Best Current Practices for
Wireless Internet Service Provider (WISP) Roaming

Purpose and Scope of this Document

This document specifies recommended Best Current Practices for Wi-Fi based Wireless Internet Service Provider (WISP) roaming.   This document does not specify a standard of any kind, but does rely on the operational application of standards-based protocols and methodologies. It is beyond the scope of WISPr to develop, monitor or enforce minimum criteria for WISP roaming. Parties to the roaming process are therefore encouraged to follow the recommendations of the WISPr guidelines, but are barred from branding their roaming products and services as Wi-Fi Alliance or WISPr compliant. Definition and adoption of various business models and commercial relationships for WISP roaming are at the discretion of individual companies. Specifically, the retail delivery of roaming service to subscribers, including services definition and charging principles, roaming tariff plans, billing methods, settlement issues and currency matters, are outside the scope of WISPr.

Abstract

WISPr was chartered by the Wi-Fi Alliance to describe the recommended operational practices, technical architecture, and Authentication, Authorization, and Accounting (AAA) framework needed to enable subscriber roaming among Wi-Fi based Wireless Internet Service Providers (WISPs). This roaming framework allows using Wi-Fi compliant devices to roam into Wi-Fi enabled hotspots for public access and services. User can be authenticated and billed (if appropriate) for service by their Home Entity (such as another service provider or corporation).

In order to facilitate compatibility with the widest possible range of legacy Wi-Fi products, it is recommended that WISPs or Hotspot Operators adopt a browser-based Universal Access Method (UAM) for Public Access Networks. The UAM allows a subscriber to access WISP services with only a Wi-Fi network interface and Internet browser on the user's device.

RADIUS is the recommended backend AAA protocol to support the access, authentication, and accounting requirements of WISP roaming.   This document describes a minimum set of RADIUS attributes needed to support basic services, fault isolation, and session/transaction accounting.

Intellectual Property Disclaimer

51 **Table of Contents**

81

82 **Table of Figures**

86

87 **1.   Introduction**

88 Since the adoption of the IEEE 802.11b standard in 1999, an increasing number of vendors have used this
89 standard in producing Wi-Fi compliant wireless LAN (WLAN) products. Pioneers of high speed Internet
90 access have built WLAN hotspots (zones of public access). Since it is difficult for a single service provider
91 to build an infrastructure that offers global access to its subscribers, roaming between service providers is
92 essential for delivering global access to customers. Roaming allows enterprises and service providers to
93 enhance their employee connectivity and service offerings by expanding their footprint to include network
94 access at Wi-Fi enabled hot spots.

95

96 WISPr was formed by the Wi-Fi Alliance to create recommendations that facilitate inter-network and inter-
97 operator roaming with Wi-Fi based access equipment. The dialup Internet roaming protocol selection criteria
98 in [RFC2477], addresses the requirements for a roaming standard but does not address the distinct
99 differences in access methods and protocol support for Wi-Fi based networks that can utilize existing
100 protocols. This document presents the recommended best current practices for enabling WISP roaming.

101

102 The figure below graphically depicts a generic model for WISP roaming, including necessary functions and
103 participants.

104

Roaming Intermediary (optional)

Authentication & Accounting Server

Home Entity

Authentication & Accounting Server

Billing

End User

Direct AAA Exchange

Roaming User

Internet

User Data

Hotspot Operator

Authentication & Accounting Server

RADIUS

PAC Gateway

Access Point

Wi-Fi

Laptop
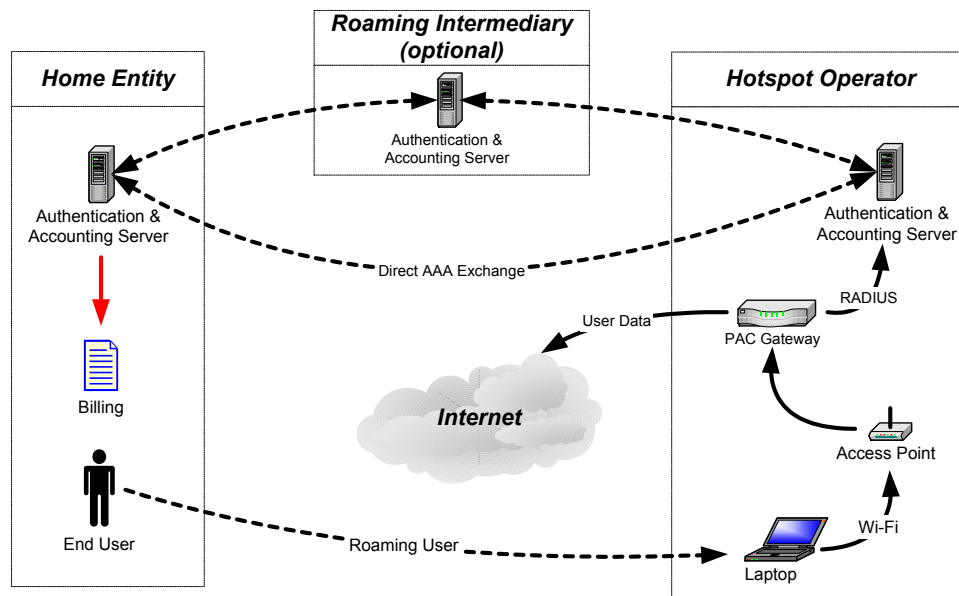
105

106   **Figure A: WISP Roaming Overview**

107

108 The participants, and all intermediaries that sit in the AAA flow, must support the recommended AAA
109 attributes. The functional objects/players in the WISP roaming model include:
110   • Hotspot Operator – Operator of Wi-Fi network for public Internet access at hotspots.
111   • Home Entity –Entity that owns account relationship with the user. The Home Entity must authenticate
112   their user to obtain roaming access at the hotspot. Examples of home entities include WISPs, other
113   service providers, and corporations.
114   • Roaming Intermediary - An optional intermediary that may facilitate AAA and financial settlement
115   between one or more WISPs and Home Entities. Examples of AAA intermediaries include Brokers
116   and Clearinghouses.

117

118 Parties that do not directly participate in the AAA framework nor have to directly support the AAA attributes
119 of the Roaming Model:
120   • User - Uses Wi-Fi Roaming at hotspots and has a billing relationship with the Home Entity.
121   • Content Provider - Content providers provide content and applications to the users of the service.   The
122   content provider and the Home Entity have a commercial relationship where the content provider takes

123   responsibility to make content accessible to the authorized users, and the Home Entity guarantees the
124   commercial terms (i.e., payment).
125 • Hotspot Property Owner - The hotspot property owner typically controls the density of potential
126   users/customers and provides the Hotspot Operator space for equipment and consumers using the
127   service. If the hotspot property owner is not a Hotspot Operator, it does not participate in the data
128   exchange required to support authentication and accounting for roaming users.
129

1.1. Terminology

131 *~ AAA ~*
132 Authentication, Authorization and Accounting. A method for transmitting roaming access requests in the
133 form of user credentials (typically user@domain and password), service authorization, and session
134 accounting details between devices and networks in a real-time manner.
135

136 *~Clearinghouse~*
137 A clearinghouse is a third party that facilitates exchange of authentication and accounting messages between
138 WISPs and home entities, and provides auditable data for settlement of roaming payments. Unlike a broker,
139 clearinghouses do not buy airtime minutes from WISPs for resale, instead providing a trusted intermediary
140 function for implementing roaming agreements made directly between WISPs and home entities.
141 Clearinghouses are typically compensated on a transaction basis for clearing and settlement services.
142

143 *~ EAP ~*
144 Extensible Authentication Protocol. A general authentication protocol used by Local and Metropolitan Area
145 Networks that supports various specific authentication mechanisms. EAP is defined in [RFC2284] and used
146 by the IEEE 802.1x Port Based Access Control protocol [8021x].
147

148 *~ Home Entity ~*
149 The entity with which the end-user has an authentication and/or billing relationship. The Home Entity need
150 not be a network provider, but must support the RADIUS functionality required to authenticate and account
151 for usage of their clients that roam. The Home Entity may also be a Hotspot Operator, a service provider that
152 hasn't deployed Wi-Fi access hotspots, an enterprise network, or an independent business entity that the end-
153 user has an account relationship with.
154

155 *~ Hotspot ~*
156 A location that provides Wi-Fi public network access to Wi-Fi enabled consumers. Examples of hotspots
157 include hotel lobbies, coffee shops, and airports.
158

159 *~ Hotspot Operator ~*
160 An entity that operates a facility consisting of a Wi-Fi public access network and participates in the
161 authentication process.
162

163 *~ IEEE 802.11 ~*
164 The Institute of Electrical and Electronic Engineers (IEEE) has developed the 802.11 family of standards for
165 wireless Ethernet local area networks operating in the 2.4 GHz ISM band and the 5 GHz UNII band. The
166 802.11 standards define the Medium Access Control (MAC) and Physical Layer (PHY) specifications for
167 wireless LANs (WLANs). The 802.11 standards define protocols for both Infrastructure Mode, where all
168 Wireless Stations communicate via at least one Access Point, and Ad-Hoc (peer-to-peer) Mode, where
169 Wireless Stations communicate directly without use of an intervening Access Point. All public and
170 enterprise WLANs operate in the Infrastructure Mode. Further information about the 802.11 family of
171 standards can be found on the IEEE802.11 web site, www.ieee802.org/11/
172

173 *~ NAI ~*
174   Network Access Identifier. As defined in [RFC2486], the NAI is the userID submitted by the client during
175 authentication and used when roaming to identify the user as well as to assist in the routing of the
176 authentication request to the user's home authentication server.
177
178

179 ~ *Public Access Control (PAC) Gateway* ~
180 The Public Access Control (PAC) Gateway may be used by Hotspot Operators to provide the access and
181 services control in their Wi-Fi network. The PAC gateway can perform several key functions for the Hotspot
182 Operator in order to support the Universal Access Methodology.
183
184 ~ *RADIUS* ~
185 An Authentication, Authorization, and Accounting protocol defined by the IETF [RFC2865, RFC2866].
186
187 ~ *Roaming* ~
188 The ability of an end-user with a Wi-Fi device to use the services of an operator other than the one with
189 which they have an account relationship. Roaming implicitly indicates a relationship between a Hotspot
190 Operator, possibly a Broker, a Home Entity and the end-user, who has an established relationship with the
191 Home Entity.
192
193 ~ *Roaming Agent* ~
194 A legal entity operating as a representative of a community of Home Entities or Hotspot Operators,
195 facilitating common legal and commercial frameworks for roaming. The agent does not become a party in
196 the roaming agreement between the Home Entities and Hotspot Operators (like Roaming Brokers do) and
197 retains a neutral position with regard to tariffs and service content offered. An agent operates a multilateral
198 roaming model and typically offers multilateral settlement services.
199
200 ~ *Roaming Broker* ~
201 An entity that provides (global) services for Home Entities and Hotspot Operators by operating as an
202 intermediary and trading broadband access between them at a fixed or transactional price (buying and re-
203 selling roaming airtime usage), and performs clearing and settlement services. Brokers may provide
204 centralized authentication services in order to compute and validate the broadband traffic.
205
206 ~ *Roaming Agreement* ~
207 An agreement for access and services between Hotspot Operators, Roaming Intermediaries, and Home
208 Entities. The agreement regulates the exchange of AAA messages that control the delivery of access at a
209 hotspot and also defines the technical and commercial conditions of such access and is a pre-requisite to
210 initiating roaming services.
211   • **Bilateral Roaming Agreement**: a roaming agreement negotiated directly between two roaming
212   parties.
213   • **Multilateral Roaming Agreement**: a roaming agreement negotiated between a Home Entity or
214   Hotspot Operator and a roaming agent.
215
216 ~ *Roaming (AAA) Intermediary* ~
217 An entity in the AAA path between the Hotspot Operator and the Home Entity. The AAA intermediaries
218 could be a clearinghouse, an aggregator, a roaming broker, or a roaming agent.
219
220 ~ *Roaming Tariff* ~
221 The various charges set by the Hotspot Operator for usage of its network by roaming users.
222
223 ~ *Secure Authentication Portal* ~
224 A web page where users of the wireless network enter their user credentials to obtain access to the network
225 using an encrypted mechanism.
226
227 ~ *Smart Client* ~
228 A software solution which resides on the user's access device that facilitates the user's connection to Public
229 Access Networks, whether via a browser, signaling protocol or other proprietary method of access.
230
231 ~ *Universal Access Method (UAM)* ~
232 The recommended methodology, described in section 2, for providing secure web-based service presentment,
233 authentication, authorization and accounting of users is a WISP network. This methodology enables any
234 standard Wi-Fi enabled TCP/IP device with a browser to gain access to the WISP network.
235

236   *~ Wi-Fi Alliance ~*
237   The Wi-Fi Alliance's mission is to certify interoperability of Wi-Fi™ (IEEE 802.11) products and to promote
238   Wi-Fi as the global wireless LAN standard across all market segments.   For more information on the Wi-Fi
239   alliance, please visit their website, http://www.wi-fi.org/.
240
241   *~ Wi-Fi™ ~*
242   A trademark of the Wi-Fi Alliance. This term refers to all Wi-Fi Alliance-certified IEEE 802.11b
243   networking products.
244
245   *~ WISP ~*
246   Wireless Internet Service Provider. WISP is a general term that can be a Home Entity allowing their users to
247   roam into a Wi-Fi hotspot or a Hotspot Operator that operates a Wi-Fi based infrastructure for public network
248   access. WISPs may also offer additional services such as location based content and services, Virtual Private
249   Networking (VPN), and Voice over IP (VoIP).
250
251   *~ WISPr ~*
252   Wireless Internet Service Provider roaming. A Wi-Fi Alliance Committee established to identify
253   recommended best practices for support of wireless roaming between providers of networks employing Wi-
254   Fi technology.

255   **1.2.   Requirements Specific Language**

256   Several words in this document are used to signify the requirements to follow the WISPr recommendations.
257   WISPr is not a standards body nor does it have any facility for enforcement. As such, a Requirements
258   Language is necessary, for the purposes of this document, only to convey levels of conviction towards the
259   parameters of the WISPr roaming specification.
260
261   The Requirements Language refers to the capabilities of standards compliant networking applications and
262   devices to fulfill the intent of the WISPr inter-network roaming specification and not towards the aspect of
263   Wi-Fi hardware compliance. These imperatives are used to communicate where compliance is actually
264   required for interoperation or limit potentially harmful behavior. The intent is not to use these imperatives to
265   impose a particular implementation, but rather to define the recommended best operational practices for the
266   delivery of WISP roaming services.
267
268   This document, as it relates to these definition of terms to describe the requirements of the WISPr
269   specification, follows the conventions as outlined in [RFC2119]:
270
271   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD,
272   "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" contained in this document are to be
273   interpreted in the following manner:
274
275   REQUIRED – This word, or the terms "MUST" or "SHALL", mean the definition is an absolute requirement
276   to follow the WISPr recommendations.
277
278   MUST NOT – This phrase, or the phrase "SHALL NOT", means the definition is an absolute prohibition to
279   follow the WISPr recommendations.
280
281   RECOMMENDED – This word, or the adjective "SHOULD", means there may exist valid reasons in
282   particular circumstances to ignore a particular item, but the full implications must be understood and
283   carefully weighed before choosing a different course.
284
285   NOT RECOMMENDED – This phrased, or the phrase "SHOULD NOT" means there may exist the valid
286   reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full
287   implications should be understood and the case carefully weighed before implementing any behavior
288   described with this label.
289
290   OPTIONAL – This word, or the adjective "MAY", means that an implementer may choose to include the
291   item because a particular business objective requires it or because they feel that it enhances the service while

292   other implementers may choose to omit the item. An implementation, which does not include a particular
293   option, MUST be prepared to interoperate with another implementation that does include the option though
294   with perhaps reduced functionality, and vice-versa.

295   **1.3.   Assumptions**

296   This document makes the following assumptions, in no particular order:
297   •   WISPs SHALL utilize Wi-Fi and/or Wi-Fi5 certified networking components.
298   •   All entities involved in roaming must support the RADIUS protocol [RFC2865, RFC2866] and
299   WISPr-defined attributes for exchange of operational and accounting data.
300   •   All issues related to WISP business models are outside the scope of WISPr. Excluded topics include:
301   services definitions and selection, roaming relationships, selection of roaming clearinghouses, charging
302   models, fees, currencies, settlement methods, billing cycles and anything related to these subjects.
303   •   Established industry standards groups are more suitable to defining inter-standard roaming practices.
304   The GSM Association (WLAN Taskforce) and IS-41 (TIA) (EIA/TIA-45 and TR-46 committees) have
305   the industry representation and technical expertise required to address inter-standard roaming. WISPr
306   will cooperate with these organizations in any future discussions of best practices for inter-standard
307   roaming.
308   •   As new technology and methodologies emerge, WISPr will consider their potential application to
309   WISP roaming.
310
311   The deployment of 802.11a wireless LANs does not offer significant technical implications on WISPr
312   because of WISPr's limited dependence on the 802.11 PHY layers. Wi-Fi products (including 802.11a and
313   802.11b) utilize the same MAC layer. The primary differences between them fall within the PHY layers and
314   include varying data rates, modulation types, and transmission frequencies. These are differences that the
315   implementer must take into account when deploying the wireless LAN.

316   **2.   Access Methods**

317   WISPr recommends the Universal Access Method (UAM) to facilitate WISP roaming. The UAM allows a
318   subscriber to access WISP services with only an Internet browser and Wi-Fi network interface on the
319   subscriber device, so that all users, regardless of device type or operating system, can participate in WISP
320   roaming. The UAM utilizes an Internet browser-based secure Authentication Portal, user credential entry,
321   and RADIUS AAA. The UAM represents the lowest common denominator for granting access to a WISP
322   network ensuring that all users can share the same experience.
323
324   The Universal Access Method may be enhanced by use of a proprietary Smart Client to simplify the user
325   experience. A Smart Client can be used to enhance the subscriber experience by providing features such as a
326   directory listing available public network access hotspots, SSID browsing, automated sign-on or single click
327   launch of additional software (like a remote Virtual Private Network client). These Smart Clients are
328   typically compatible with, and add value over and above the UAM, and are typically provided by the
329   subscriber's Home Entity. Home Entities should be mindful that requiring the use of a proprietary Smart
330   Client could restrict network access. As a result, Home Entities must ensure that use of the Smart Client does
331   not preclude roaming using the UAM.
332
333   The recently introduced IEEE 802.1x standard provides a protocol for authentication and port-based access
334   control supporting enhanced access security, but has not been widely deployed in public access
335   environments. Unlike the UAM, the 802.1x access method requires client software on the subscriber device.
336   Further discussion of the 802.1x authentication method and user experience is provided in Appendix A.

337   **2.1.   The Universal Access Method User's Experience**

338   The user experience in the following section describes a typical user experience at a Wi-Fi public access
339   hotspot using the Universal Access Methodology to control user access.
340
341   *"A user visits a public hotspot. He boots up his laptop and associates with the local Wi-Fi network by*
342   *selecting the available network or entering the correct SSID in his Wi-Fi PC Card Configuration Utility. He*
343   *then starts his browser, which, for the sake of discussion, is configured to load www.yahoo.com as his home*

344   *page. Instead of the browser loading this home page, it loads a Welcome Page from the Hotspot Operator*
345   *that allows the user to login with a username and password. Once authenticated, a Start Page appears from*
346   *the Home Entity and the user can access his original home page such as Yahoo. In addition, a smaller*
347   *window pops up detailing session information and providing a button which, when clicked, will log him out.*
348   *At this time the user can access the Internet via his wireless connection. When the user finishes, he clicks the*
349   *aforementioned logout button to disconnect from the network and continues to work on the laptop or shuts*
350   *down his laptop and leaves."*
351
352   The minimum HTML-based logon process and requirements for each page are outlined in the following
353   diagram and sections. A collection of the authentication pages provided by the Hotspot Operator may also be
354   referred to as the Secure Authentication Portal (SAP).
355
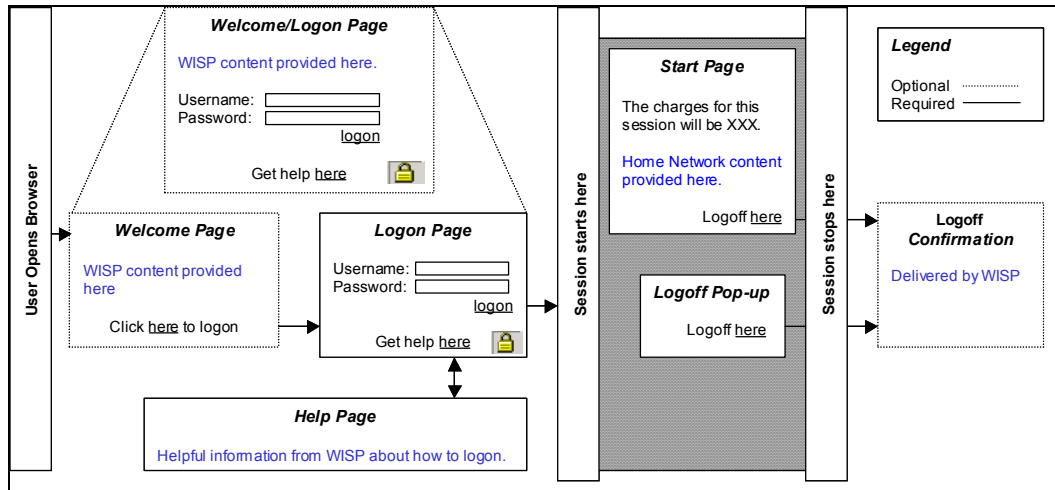
356

357   **Figure B: Universal Access Method (UAM) User Experience**
358

359   **Welcome Page**
360
361   The Welcome Page is an OPTIONAL web page provided by the Hotspot Operator. The Welcome Page is
362   the first page that is presented to the user. The Welcome Page MAY contain local content such as maps,
363   local hotel information, baggage and ticketing information, restaurants, etc. The Logon Page and the
364   Welcome Page may be the same page, but in some cases the Welcome Page may only provide a link to the
365   Logon Page or to other network access-specific pages, such as localized text pages for multi-lingual access
366   instructions. At minimum, a clearly identifiable link to the Logon Page MUST be provided on the Welcome
367   Page.
368
369   **Logon page**
370
371   The secure Logon Page is REQUIRED and is delivered by the Hotspot Operator. This page is made secure
372   by the use of SSL (Secure Socket Layer). At a minimum, the logon page MUST have space to enter the
373   user's credential. The user's credentials are the same across all WISPr-compliant networks, specifically in
374   the format of username@domain, as specified by the Network Access Identifier (NAI) [RFC2486], extended
375   by allowing the use of embedded spaces in the username, prohibiting case translation by any intermediate
376   parties, and used to assist in the routing of the authentication request. Users who are subscribers of the
377   Hotspot Operator (in this case the Hotspot Operator is the user's Home Entity) are NOT REQUIRED to enter
378   a @domain qualifier (NAI) following the username.
379
380   **Help Page**
381
382   Although the Help Page is REQUIRED, the actual content of the Help Page is at the discretion of the Hotspot
383   Operator. In order to facilitate the logon process for first time users, information on how to logon in a
384   roaming environment SHOULD be provided. Additional instructions for new user registration MAY be

385   provided here.
386
387   As with the Logon Page, language localization for the Help Page is helpful, but entirely OPTIONAL.
388
389   **Start Page**
390
391   The Start Page functionality is REQUIRED to be supported by the Hotspot Operator, but the Start Page URL
392   address is specified by the Home Entity. Upon successful authentication of a roaming user, the Hotspot
393   Operator MUST redirect the customer to the Home Entity's Start Page as specified in an AAA Vendor
394   Specific Attribute (VSA) transmitted during the user's authorization. If the Home Entity does not provide
395   the Start Page VSA, the Hotspot Operator MAY proceed to the user's originally requested URL (origin
396   server) or a default Hotspot Operator Start Page instead.
397
398   The Start Page MAY communicate information to the customer regarding roaming billing, charges that will
399   be incurred as a result of using the service. Roaming users SHOULD be able to cancel the session from this
400   page. An explicit method for logoff MUST be presented on the Start Page to allow for this function.   To
401   achieve this, the Hotspot Operator is REQUIRED to specify in an AAA Vendor Specific Attribute (VSA) the
402   explicit Logoff URL for the wireless hotspot the customer is requesting access.
403
404   **Logoff Confirmation Page**
405
406   The Logoff Confirmation Page is RECOMMENDED for explicit logoffs and delivered by the Hotspot
407   Operator. The page is intended to provide confirmation to the customer that they have been logged off and
408   MAY contain session statistics in regards to the user's closed session.
409   **2.2.   Logoff Functionality**
410   Both implicit and explicit logoff capabilities are REQUIRED to be provided by the Hotspot Operator, even if
411   they are not applicable to the local network provider's own billing methods. The reasoning behind this is that
412   different billing methods will exist from provider to provider. WISPr RECOMMENDS real-time accounting
413   via the appropriate AAA, including connection, time, and usage based information. Even though the Hotspot
414   Operator may be billing the Home Entity or customer owner in megabytes and not require the user to logoff,
415   the customer may be billed in minutes and MUST have the ability to logoff.
416
417   It is RECOMMENDED the Home Entity provide an explicit logoff method via the Start page.
418
419   **Explicit logoff**
420
421   A clear method MUST be provided by the Hotspot Operator to allow the user to logoff the visited network.
422   This explicit logoff function SHOULD be delivered in several different ways including, but not limited to:
423   1.   A hypertext link from the Start page
424   2.   A small popup window that allows the user to click a logoff button
425   3.   For PDA users, as an alternate to the popup window, a logoff web page could be bookmarked so the
426   user could return to the page to manually initiate the logoff process
427
428   **Implicit logoff**
429
430   If a user does not explicitly logoff, a session MUST be guaranteed to eventually end. This implicit logoff
431   protects the user in case of a loss of signal or some other failure. It is RECOMMENDED that the user not be
432   required to login again if they reboot their PC or end up losing signal for a short period of time. However,
433   indefinite time out periods are also undesirable because by the nature of the technology, roaming wireless
434   connections do not have a clear indication of termination of connection.
435
436   In order to more accurately measure the actual usage on the Hotspot Operator's network a Hotspot Operator
437   MUST support the idle (or inactivity) timeout specified by the Home Entity in the idle-timeout attribute. If
438   the idle-timeout attribute is not specified, then the Hotspot Operator should utilize an idle-timeout of no more
439   than five minutes. The idle period is determined by the elapsed time since the user has last transmitted a
440   packet, or is no longer accessible on the network. Once this idle-timeout period is reached, the user will have

441 their session automatically terminated and appropriate accounting mechanisms record the end of session. In
442 the case of an idle-timeout, the Acct-Session-Time sent as part of the accounting record should be reduced by
443 the length of the idle-timeout period in order to prevent the user from being overcharged.
444
445 The Home Entity MAY prohibit indefinite connections by providing a maximum session time available to its
446 roaming customers by specifying a Session-Timeout attribute in the roaming user's profile. A user exceeding
447 this time would have his access removed, an account record generated, and would be forced to re-login to
448 gain access.

449 ## 2.3. HTML/CGI Standardization

450 To facilitate connections using a Smart Client, WISPr recommends standardization of the HTML/ASP and
451 CGI mechanisms at the Secure Authentication Portal (SAP), the combination of the pages described in the
452 previous section. It is understood there are a wide variety of implementations of Login Pages and providers
453 who wish to implement a Smart Client must know the vendor and method at the hotspot for the SAP.
454 However, if a Hotspot Operator is creating a unique Authentication Portal Logon Page or modifications to
455 the Logon Page are made, care should be taken to consider the following WISPr recommendations:
456 - Form Post data variables for collecting the user credential should be in the form of "username" and
457   "password" whenever possible. As part of the username, users will be logging into the Home Entity
458   using an NAI to identify the user's home authentication server. The use of the NAI will extend the
459   "username" significantly. In accordance with the Network Access Identifier specification in
460   [RFC2486], devices that handle NAI's, such as the Secure Authentication Portal in this case, MUST
461   support an NAI length (username) of at least 72 characters.
462 - Use of standardized URLs is RECOMMENDED. When creating Logon and Logout functions, use of
463   a consistent naming convention and CGI implementation network-wide will help facilitate the
464   identification and passing of user credential information directly to the SAP by a Smart Client without
465   the need for the user to manually type in his/her credentials. All login data requirements should be
466   presentable to the hotspot in a single URL.

467 ## 3. Hotspot Operator's Network Architecture

468 As outlined in Section 2 above, the Universal Access Method enables public access connectivity to the
469 Hotspot Operator's network while allowing users to retain a billing relationship with their Home Entity. To
470 support the Universal Access Method, a Hotspot Operator must provide Wi-Fi connectivity and support
471 several key Public Access Control functions as described below.

472 ## 3.1. Public Access Control (PAC) Gateway

473 The Public Access Control (PAC) Gateway may be used by Hotspot Operators to provide the access and
474 services control in their Wi-Fi network. The PAC gateway can perform several key functions for the Hotspot
475 Operator in order to support the Universal Access Methodology. The primary PAC gateway functions may
476 include:
477 - IP Address Management
478 - Home Page Redirection
479 - Authentication and SSL Support
480 - Authorization
481 - Accounting
482 - Access Control
483 - VPN Support
484 - Mail Support
485 - Authentication Testing Facility
486
487 The PAC gateway is a logical entity, and is not necessarily a distinct network component. A range of
488 hardware and software configurations can deliver the functions of the PAC entity, such as:
489 - A stand-alone networking device,
490 - As an integrated software gateway function of another networking device such as an Access Point or
491   router, or
492 - As a distributed array of such devices in a "hybrid" network architecture.

493 **3.2. Access Points, SSID, and Hotspot Network Association**

494 Various methods have been established for facilitating the association of the user's station with the Hotspot
495 Operator's Wi-Fi Access Point. The minimum requirement for association with an Access Point in the
496 Universal Access Method is knowledge of the Hotspot Operator's network SSID. Incorrect selection of the
497 SSID may result in a confusing user experience and a failure to logon. Currently, manual configuration of
498 the Wi-Fi station with the correct SSID or "browsing" the SSID beacons are the preferred methods of SSID
499 determination.
500
501 *Client Settings*
502 To allow for easy configuration and association with the Hotspot Operator's network when roaming, WISPr
503 strongly recommends that clients set their devices to disable WEP. Since the over-the-air link is completely
504 insecure, WISPr strongly recommends the use of a VPN or other security measures to ensure the privacy of
505 data.
506
507 WISPr recommends that clients who may utilize a private WEP key should be informed of the requirement to
508 disable their WEP configuration to access a roaming network. It should be made clear that any private WEP
509 information may be lost in doing so, therefore it is highly recommended that the user note this key (often up
510 to 13 characters for 128-bit WEP encryption) so it may be replaced after the user leaves the Hotspot and
511 returns to his/her "private" environment.
512
513 *SSID*
514 Users who are unfamiliar with the configuration utilities provided by their Wi-Fi NIC manufacturer and are
515 not comfortable with manually setting the required SSID value should be encouraged to set their SSID to
516 "ANY" as supported by their Wi-Fi Configuration Utility. Use of "ANY" allows the user's station to
517 automatically associate with the "nearest" Wi-Fi network without the need for the user to configure their NIC
518 manually with the correct SSID. Implementation of this form of Wi-Fi network association support varies by
519 Wi-Fi NIC manufacturer.
520
521 If ANY is used to automatically associate with Wi-Fi networks as they are encountered, users should be
522 cautioned to be cognizant of the network login pages of the available Wi-Fi networks before transmitting
523 account information. Users should be encouraged to maintain an awareness of the networks to which their
524 station associates with and should never attempt to login or transmit their user credential (NAI) to unknown
525 networks.
526
527 Furthermore, Wi-Fi Internet Service Providers and card manufacturers should consider the following SSID
528 issues:
529 - Each Hotspot Operator SHOULD consider using a unique SSID to differentiate their Access Point
530   from other available Wi-Fi networks by incorporating the Hotspot Operator's name as part of the
531   identifier (e.g., "`ACMEWISP_NewarkAirport`") as described as part of the Location-Name AAA
532   Attribute.
533 - Inclusion of the SSID in beacon transmissions and response to the broadcast SSID (read as "wildcard
534   SSID") in probe request frames from a client (as required by the 802.11 standard) is
535   RECOMMENDED for all Hotspot Operator access points to allow for SSID browsing and implicit Wi-
536   Fi network associations by the user client station's OS or Wi-Fi Configuration Utility software.
537

538 **4. AAA**

539 RADIUS is the preferred AAA protocol for Wi-Fi roaming. As other protocols become available for
540 deployment, WISPr will review the technology and make recommendations. Regardless of the access
541 method used, the RADIUS protocol is used between entities to coordinate roaming between service partners.
542
543 Given the importance of AAA to inter-WISP roaming, WISPr seeks to clearly identify the critical aspects of
544 AAA that must be considered for a Wi-Fi roaming framework:
545 - Protection of the user's Identity and credentials
546 - Proper implementations and practices to support Accounting
547 - RADIUS protocol compliance

548   • RADIUS attribute support
549   • Informational WISPr RADIUS attributes for WISP roaming

4.1. Accounting Support

551   Specific WISP business practices related to roaming, clearinghouse, settlement and billing are not within the
552   scope of WISPr. However, the minimum technical requirements specified here are required to provide the
553   exchange of the necessary accounting data between Hotspot Operators, Intermediaries, and Home Entities to
554   assure the integrity of billing and settlement processes.
555
556   Vendors, Hotspot Operators, and Intermediaries SHOULD NOT implement partial AAA solutions (e.g. only
557   provide authentication and authorization with no accounting).   Public Access methods that do not provide
558   complete RADIUS session accounting SHOULD NOT be used in Public Access Networks unless combined
559   with the Universal Access Methodology for AAA or other manner to record usage durations in an acceptable
560   fashion.

4.2. AAA Data Exchange

562   The Hotspot Operator MUST provide the Home Entity with all generated RADIUS/AAA authorization and
563   accounting messages, including any interim accounting messages.
564
565   This document makes no requirements on the transmission path of the AAA data. The AAA data can be sent
566   on the public Internet, over a segregated private network link, or isolated within VPN tunnels. The choice of
567   transmission path is decided on a bilateral basis between operators of the RADIUS/AAA servers.
568
569   **Exchange Cycle**
570
571   Real-time delivery of RADIUS/AAA data is REQUIRED. The RADIUS/AAA accounting messages are the
572   basic usage telemetry that allow all service providers to monitor and measure usage of their subscribers. The
573   real-time delivery of RADIUS/AAA accounting messages is necessary and sufficient to support any usage
574   based business model, including Prepaid or Debit card services.
575
576   **AAA Data Exchange Integrity**
577
578   Hotspot Operators and Roaming Intermediaries should strive for 100% reliability of AAA message delivery.
579   Experience has shown that 99.9% reliability of AAA message delivery should be routinely achievable under
580   high traffic conditions.
581
582   All parties along the transmission path of the AAA data should exercise care in the engineering of the
583   communication links and the capacity of the RADIUS/AAA servers. It is a common fallacy that the reliance
584   on the UDP protocol for transporting RADIUS/AAA data is the cause of RADIUS message loss. The
585   RADIUS protocol employs its own data retransmission strategy for ensuring that packets are delivered
586   reliably over lossy communication paths. Service providers need to exercise care in properly selecting the
587   retransmission parameters appropriate for the bandwidth, path error, and path congestion characteristics
588   between RADIUS/AAA servers. Undersized RADIUS/AAA servers are a common cause for the loss of
589   RADIUS messages. Undersized RADIUS/AAA servers can reliably receive a RADIUS message and then
590   lose the message internally as its internal resources are overwhelmed by traffic. Service providers should
591   characterize the capability of their RADIUS/AAA servers so that they can anticipate and prevent conditions
592   that lead to RADIUS message loss in the servers.
593
594   **Support for Interim Accounting Messages**
595
596   Support for RADIUS Interim Accounting Messages is RECOMMENDED to minimize the impact of a lost
597   session start or stop message. It is RECOMMENDED that the Hotspot Operator support generation of
598   interim accounting messages at time intervals set by the Home Entity's RADIUS server. The interval for
599   RADIUS Interim Accounting Messages establishes the minimum measurable interval of usage. If the final
600   RADIUS Accounting Message is lost, the RADIUS Interim Accounting Message limits the maximum
601   amount of measured service delivered without supporting accounting data is limited by the RADIUS Interim

602   Accounting Message interval. [RFC2869] recommends that the interim accounting interval SHOULD NOT
603   be smaller than 600 and careful consideration should be given to its impact on network traffic. This interval
604   is considered sufficient to support many WLAN applications.
605
606   **Archiving of Accounting Data**
607
608   In order to facilitate usage audits and charging reconciliation, the parties at both ends of a RADIUS link
609   SHOULD maintain a log of RADIUS messages exchanged. Complete records of raw RADIUS message data
610   SHOULD be archived for the same periods and with the same care as invoice and accounting data. The
611   archived data must be readily available on request, but need not be accessible on-line. Local laws determine
612   the required storage time for billing-related accounting information. For example, most European countries
613   require 1-year storage of invoicing and billing data. In the United States, cellular carriers are required to
614   keep call detail and roamer settlement records for 7 years, and cellular clearinghouses keep settlement
615   summary reports for 7 years.

616   **5.   RADIUS Attribute Support**

617   RADIUS attributes provide for the critical handling of session control, accounting information, and potential
618   implementation of real-time services. As such, Hotspot Operators and Roaming Intermediaries should
619   support the broadest possible set of RADIUS attributes for various services, even though those services are
620   not offered on their networks (i.e., TCP-Clear for legacy support, Session-Timeout for pre-paid Internet
621   access and EAP for wireless security). To prevent loss of data and/or services failure, all Roaming
622   Intermediaries or RADIUS proxy systems are REQUIRED to support the RADIUS Attributes specified in
623   the following section.

624   **5.1.   Required Standard RADIUS Attributes**

625   It is RECOMMENDED that Hotspot Operators implement all RADIUS v1 attributes from 1-88 in addition to
626   supplementary attributes for control of specific NAS functions. At a minimum, WISPr REQUIRES the
627   following standard RADIUS attributes be supported for purposes of basic services, fault isolation, and
628   session/transaction accounting:
629

Required Attribute	#	Type	Auth Req	Auth Reply	Acctg Req	Comment
User-Name	1	String	X		X	User enters full NAI
User-Password	2	String	X			
NAS-IP-Address	4	Ipaddr	X		X	IP Address of the Access Gateway
Service-Type	6	Integer	X			Must be set to Login (1)
Framed-IP-Address	8	Ipaddr	X		X	IP Address of the User
Reply-Message	18	String		X		Text of reject reason if present
State	24	String	X	X		
Class	25	String		X	X	
Session-Timeout	27	Integer		X		Forced logout once timeout period reached (seconds)
Idle-Timeout	28	Integer		X		Implicit logout inactivity timeout period (seconds)
Called-Station-ID	30	String	X		X	This field should contain the MAC address or other information identifying the Access Gateway
NAS-ID	32	String	X		X	
Acct-Status-Type	40	Integer			X	1 = Start, 2 = Stop, 3 = Interim Update
Acct-Delay-Time	41	Integer			X	Delay (seconds) between Acctg Event and when Acct-Req sent (doesn't include estimated network transit time)
Acct-Input-Octets	42	Integer			X	
Acct-Output-Octets	43	Integer			X	
Acct-Session-ID	44	String	X	X	X	
Acct-Session-Time	46	Integer			X	Call duration in seconds (already compensated for idle timeout)
Acct-Input-Packets	47	Integer			X	

Required Attribute	#	Type	Auth Req	Auth Reply	Acctg Req	Comment
Acct-Output-Packets	48	Integer			X	
Acct-Terminate-Cause	49	Integer			X	1 = Explicit Logoff, 4 = Idle Timeout, 5 = Session Timeout, 6 = Admin Reset, 9 = NAS Error, 10 = NAS Request, 11 = NAS Reboot
NAS-Port-Type	61	Integer	X		X	15 = Ethernet, 19 = 802.11
Acct-Interim-Interval	85	Integer		X		Interval (seconds) to send accounting updates

630   **CHAP-Password**

631   CHAP password is not possible with the protocol described above, as there is no challenge-response phase
632   between the client and the access gateway. For this reason, the access gateway does not initiate CHAP in the
633   *Access-Request* message; therefore, the *CHAP-Password* field should not be used.

634   **NAS-Identifier**

635   The *NAS-Identifier* MAY be set to a pre-agreed value identifying the access gateway. *NAS-Identifier* is the
636   preferred attribute for location identification when *NAS-IP-Address* cannot be used for this purpose. When
637   present, *NAS-Identifier* MUST be included in both *Access-Request* and *Accounting-Request* packets.

638   **Idle-Timeout**

639   The *Idle-Timeout* field included in the *Access-Accept* must be used to set the amount of time the user is
640   allowed to stay idle before being disconnected. When the user is disconnected due to an Idle-Timeout, the
641   following *Accounting-Request* message must have the *Acct-Session-Time* reduced by the length of the *Idle-
642   Timeout* in order to prevent the user from being overcharged.

643   **NAS-Port-Type**

644   Both the *Access-Request* and *Accounting-Request* must include the *NAS-Port-Type*. The Access Gateway
645   may distinguish between Ethernet (15) and 802.11 (19) when they are present at the same venue.

646   **5.2. WISPr Vendor Specific Attributes**

647   WISPr RECOMMENDS the implementation of certain Vendor Specific Attributes (VSA). The VSA values
648   are intended to provide the Home Entity and/or Broker with information such as the user's location to
649   facilitate back-end processing of transaction data as well as to provide service-level information. WISPr has
650   obtained an IANA Private Enterprise Number (PEN) of 14122 that is registered to the Wi-Fi Alliance, which
651   will be used to pass *Vendor-Specific* attributes for use with broadband roaming services and can be utilized
652   by various vendors and providers who wish to support WISPr functionality. Any other proprietary *Vendor-
653   Specific* attributes should be propagated through the roaming network. *Vendor-Specific* attributes, which
654   should receive specific handling, are detailed below.

655

WISPr Vendor Specific Attributes	#	Type	Auth Req	Auth Reply	Acctg Req	Comment
Location-ID	1	String	X		X	Hotspot Location Identifier
Location-Name	2	String	X		X	Hotspot Location and Operator's Name
Logoff-URL	3	String	X			URL for user to perform explicit logoff
Redirection-URL	4	String		X		URL of Start Page
Bandwidth-Min-Up	5	Integer		X		Minimum Transmit Rate (b/s)
Bandwidth-Min-Down	6	Integer		X		Minimum Receive Rate (b/s)
Bandwidth-Max-Up	7	Integer		X		Maximum Transmit Rate (b/s)
Bandwidth-Max-Down	8	Integer		X		Maximum Receive Rate(b/s)
Session-Terminate-Time	9	String		X		YYYY-MM-DDThh:mm:ssTZD
Session-Terminate-End-Of-Day	10	Integer		X		Flag zero or one indicating termination rule.
Billing-Class-Of-Service	11	String		X		Text string indicating service type.

656
657   WISPr Network Location information is to be delivered in the WISPr-Location-ID and WISPr-Location-
658   Name attributes. The intent of this requirement is to provide the information regarding the user's location
659   and connection that is required by the Hotspot Operator and Home Entity for the purposes of facilitating
660   billing processes. WISPr RECOMMENDS a consistent usage of VSAs split between a standardized set of
661   VSA for billing and others to be used as a generic variable content Text Location Identifier.
662
663   *~ Location-ID ~*
664
665   A *Location-ID* value SHOULD be included in the *Access-Request* and *Accounting-Request* packet. This
666   *Location-ID* MUST be configurable for each hotspot location and be of the form:
667   `isocc=<ISO_Country_Code>,cc=<E.164_Country_Code>,ac=<E.164_Area_Code>,`
668   `network=<SSID/ZONE>`
669   Example:
670   `"isocc=us,cc=1,ac=408,network=ACMEWISP_NewarkAirport"`
671
672   *~ Location-Name ~*
673
674   The name of the Hotspot Operator and a textual description of the location SHOULD be included in the
675   *Access-Request* and *Account-Request* packet. This value MUST be configurable for each access gateway and
676   be of the form:
677   `<HOTSPOT_OPERATOR_NAME>,<Location>`
678   Example:
679   `"ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport"`
680
681   *~ Redirection-URL ~*
682
683   The *Access-Accept* packet MAY include a *Redirection-URL;* this is the URL of the Start Page that the user's
684   browser is directed to after authentication. When this value is present, the user's browser should be directed
685   to the indicated URL. This will allow the Home Entity to control the user's experience.
686
687   *~ Logoff-URL ~*
688
689   The *Access-Request* packet MUST include a *Logoff-URL.* This value is presented to allow the Home Entity
690   to provide a link on their Start Page for the user to Logoff.
691
692   *~ Bandwidth-Max-Up and Bandwidth-Max-Down ~*
693
694   These attributes specify the maximum rate at which that corresponding user is allowed to transmit (Up) and
695   receive (Down) data. Since the user may be connected to the hotspot via local LAN connection that has
696   higher bandwidth than the available WAN bandwidth out of that hotspot, when specified, the hotspot should
697   throttle down the amount of data the user can transmit and/or receive.
698
699   *~ Bandwidth-Min-Up and Bandwidth-Min-Down ~*
700
701   These attributes specify the minimum guaranteed rate at which bandwidth should be reserve for the user to
702   transmit (Up) and receive (Down) data. Support for guaranteed end-to-end Quality of Service (QoS) is
703   currently not available but being reserved for the future use and is currently only enforced for the traffic
704   flowing through that specific hotspot location.
705
706   *~ Session-Terminate-Time ~*
707
708   The *Session-Terminate-Time* VSA indicates the time when the user should be disconnected from the
709   network. The field is a text string formatted according to ISO 8601 format YYYY-MM-DDThh:mm:ssTZD.
710   If the TZD is not included, the user should be disconnected at the time specified in local time. For example, a
711   disconnect on 18 December 2001 at 7:00 PM Universal Coordinated time would be formatted as "2001-12-
712   18T19:00:00+00:00". A disconnect request for midnight local time on the same day would be formatted

713   "2001-12-18T00:00:00". If the *Session-Terminate-Time* is included, the *Session-Terminate-End-Of-Day*
714   VSA should not be sent. This attribute should be treated as an explicit logoff.
715
716   **~ *Session-Terminate-End-Of-Day* ~**
717
718   The *Session-Terminate-End-Of-Day* VSA is an integer flag of either zero or one indicating whether the user's
719   connection should be terminated at the end of its billing day. If a specified billing day is not provided, this
720   field should be ignored. This attribute should be treated as an explicit logoff.
721
722   **~ *Billing-Class-Of-Service* ~**
723   The *Billing-Class-Of-Service* is a free-form text field. It is intended to indicate service variations that would
724   require different charges even though they occurred at the same hotspot. The contents of the field should be
725   negotiated between the Home Entity or Roaming Intermediary and the Hotspot Operator and may indicate,
726   for example, the difference between service obtained in a hotel room versus service obtained in the lobby or
727   conference room.

728 **6.**   **Security**

729   WISPr REQUIRES that Hotspot Operators conform to a minimum level of security in regards to the
730   promotion and support of the following security considerations:
731
732   •   Authentication of the User and the Hotspot Operator
733   •   Protecting the User's Credentials and Information
734   •   Protecting the User's Data
735   •   Protecting the User's Station
736   •   Protecting the WISP Networks
737
738   This section describes the areas vulnerable to attack and special consideration that should be taken when
739   using the Universal Access Method. Different characteristics and challenges for protecting the user's
740   credentials from attack are addressed in Appendix A: 802.1x.

741 **6.1.**   **Authentication**

742   The Hotspot Operator MUST provide a way for a user to authenticate the network as well as a way for a
743   network to authenticate the user. In other words, mutual authentication MUST be supported:
744   •   In order for the network to authenticate the user, username and password is used.
745   •   In order for the user to authenticate the Hotspot Operator, the Login Page MUST use SSL and
746   MUST utilize a certificate for that page so the user's browser can check if the server's Fully
747   Qualified Domain Name (FQDN) is valid before the user enters their username and password.
748
749   The ability for the user to authenticate the Hotspot Operator is important for web-based user authentication
750   where a user's login attempt may be redirected to a rogue Authentication Portal that can obtain username and
751   password information. WISPr RECOMMENDS that the Hotspot Operator use Public Key Infrastructure
752   (PKI) certificate-based authentication using HTTPS (HTTP over SSL). In this case, the Hotspot Operator
753   should obtain its server certificate issued by a trusted 3rd-party Certificate Authority that performs strict
754   verification process (i.e., Class 3 authentication) against the Hotspot Operator before issuing the certificate.
755   This provides a way to find out the legal entity of the Hotspot Operator if an identity theft occurs.

756 **6.2.**   **Protecting the User's Credentials/Information**

757   The Wi-Fi Internet Service Provider MUST protect the User Credential when presented at an Authentication
758   Portal. When using Universal Access or browser-based solutions and the user is expected to enter his User
759   Credential into a Authentication Portal, the web URL handling the transmission of the request to the AAA
760   infrastructure MUST be protected, (e.g. SSL, SSH, HTML MD5 Hash, MD5 Challenge). For example, the
761   Logon Page should utilize SSL so the username and password when submitted via the Web Browser are
762   encrypted and protected. This mandatory requirement protects both the user and the Hotspot Operator from
763   account "identity theft" and session hijacking.
764

765   To protect the user name and password from being intercepted at any link between RADIUS entities, it is
766   RECOMMENDED that service providers use IPSEC or other VPN technology to protect the RADIUS
767   messages between RADIUS servers. Although RADIUS accounting messages are protected from
768   modification by the message authentication attribute, the use of IPSEC or other VPN technology can be used
769   to hide the contents of the RADIUS accounting message if desired.
770
771   It should be noted that even if IPSEC or other VPN technology is used, a service provider could only be sure
772   that the RADIUS message is protected between the sending service provider and the receiving service
773   provider. The sending service provider may not be able to assure to their users that the third-party receiving
774   service provider will similarly protect the RADIUS traffic as it is forwarded to other third-parties.
775
776   To prevent the user's identity from theft by a malicious Hotspot Operator, third-party, or system
777   administrator (such as the case if the username and password was stored in a log file at the AAA Server or
778   access gateway), it is possible for the user to use an anonymous username from their Home Entity (e.g.,
779   anonymous@MyHomeEntity.com) and use a one-time-password that could also be hashed or encrypted with
780   the users identity that only the Home Entity could identify. The use of one-time passwords also protects the
781   users who otherwise could use a simple password that is vulnerable to dictionary attacks.
782
783   These and additional security concerns are being addressed with more advanced security protocols and will
784   be revisited as appropriate technologies (like 802.1x) become more widely available.

785 **6.3.**   **Protecting the User's Traffic/Data**

786   **WEP**
787   Due to the current limitations in WEP implementations, such as the requirement of a static WEP key be
788   assigned to the access point and configured in each user's client, WEP is not useful for public access
789   networks. When technologies and methods for dynamic WEP key assignment (such as 802.1x) become more
790   widely available and supported in users clients, WISPr will revisit the support of WEP as part of its
791   recommendations. Instead, SSL is used to encrypt and protect the user's credentials during the authentication
792   phase and the user can utilize VPN software to protect subsequent traffic/data.
793
794   Fluhrer, Mantin, and Shamir have described WEP limitations that have been further validated by AT&T Labs
795   [ATT]. As per AT&T recommendations on the implementation of WEP for Hotspot Operators, WISPr
796   concurs with their conclusions:
797   •   Assume that the link layer offers no security.
798   •   Use higher-level security mechanisms such as IPSEC and SSH for security, instead of relying on WEP.
799   •   Treat all systems that are connected via 802.11 as external. Place all access points outside the firewall.
800   •   Assume that anyone within physical range can communicate on the network as a valid user. Keep in
801   mind that an adversary may utilize a sophisticated antenna with much longer range than found on a
802   typical 802.11 PC card.
803
804   **VPN Software**
805   It is highly RECOMMENDED that Home Entities promote the use of Virtual Private Network software by
806   their users to protect the privacy of all sensitive over-the-air data and Internet transactions. Use of VPN
807   software combined with a Secure Authentication Portal offsets any actual or implied limitations of WEP
808   security. In accordance with the Universal Access Method, the use of VPN Software is not required in order
809   for the user to access the hotspot's content or services, authenticate himself with a Hotspot Operator, gain
810   Internet access, or utilize Home Entity services.

811 **6.4.**   **Protecting User's Client and Home Entity**

812   It is highly RECOMMENDED that all users of WISP networks to install and employ Personal Firewall
813   software. Personal Firewalls protect the user's station from WLAN-based attacks and exploits.
814
815   It is highly RECOMMENDED to all users of WISP networks to install and employ Virus Protection agents
816   and programs to protect against WLAN-based exposure to other infected devices and hand carrying the
817   problem back to the Home Entity or private network.

818 **6.5. Protecting the WISP Network**

819 It is highly RECCOMENDED that all WISP networks employ basic firewall protections and/or security
820 methods, either on the network facilities or on the access devices themselves, to protect against intrusion and
821 internet-based Denial-of-Service attacks.
822
823 WISP roaming networks should consider their policies on SMTP restrictions and "spam" protections as it
824 relates to their user's roaming services. If a Home Entity protects their SMTP services to known IP address,
825 other means for providing mail services to roaming customers must be considered. Use of the Hotspot
826 Operator's SMTP server by roaming users is generally acceptable when identification is pre-arranged.
827 Proper DNS resolution of all DHCP addresses is RECOMMENDED to facilitate the identification of remote
828 network transactions by a Home Entity and its services.

829 **7. References**

830 [8021x] Congdon, P., Aboba, B., Moore, T., Palekar, A., Smith, A., Zorn, G., Halasz, D., Li, A.,
831   Young, A., Roese, J., "IEEE 802.1x RADIUS Usage Guidelines", IETF Internet Draft, July
832   2001.

833 [ATT]   AT&T Labs, "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP", TD-4ZCPZZ,
834   www.cs.rice.edu/~astubble/wep/, August 6, 2001.

835 [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", IETF RFC 2119,
836   March 1997.

837 [RFC2284] Blunk, L. and Vollbrecht, J., "PPP Extensible Authentication Protocol (EAP)", IETF RFC
838   2284, March 1998.

839 [RFC2477] Aboba, B. and Zorn, G., "Criteria for Evaluating Roaming Protocols", IETF RFC 2477,
840   January 1999.

841 [RFC2486] Aboba, B., Beadles, M., "The Network Access Identifier", IETF RFC 2486, January 1999.

842 [RFC2865] Rigney, C., Willens, S., Rubens, A., Simpson, W., "Remote Authentication Dial In User
843   Service (RADIUS)", IETF RFC 2865, June 2000.

844 [RFC2866] Rigney, C., "RADIUS Accounting", IETF RFC 2866, June 2000.

845 [RFC2869] Rigney, C., Willats, W., and Calhoun, P., "RADIUS Extensions", IETF RFC 2869, June
846   2000.

847 **8. Acknowledgements**

848 Thank you to the Wi-Fi Alliance board for your insight and patience.
849
850 Many of the definitions and terms contained in this document have been integrated from various IEEE and
851 IETF resources. Thank you IEEE and IETF for providing such a wealth of online information!
852
853 **Participating Wi-Fi Alliance Committee Members**
854
855 Thank you to the participating WISPr members. Group document writing is no easy task. We learned a lot
856 from each other.
857
858 The following list details the Wi-Fi Alliance membership in attendance of at least one WISPr meeting during
859 the development of this document:
860

861 • Agere Systems   863 • AMD
862 • Airwave Wireless, Inc.   864 • Askey Computer Corp.

865	• Atheros Communications	884	• Microsoft Corporation
866	• Cisco Systems	885	• Mobilestar Network Corporation
867	• Colubris Networks, Inc.	886	• NEC Corporation
868	• Compaq	887	• Nokia Networks
869	• Dell Computer Corporation	888	• Nomadix, Inc.
870	• Enterasys Networks	889	• Nortel Networks
871	• Excilan	890	• NTT
872	• Fiberlink Communications	891	• Philips
873	• Funk Software	892	• Proxim, Inc.
874	• Gemtek Systems, Inc.	893	• Sprint PCS
875	• GRIC Communications, Inc.	894	• Symbol
876	• HereUare Communications, Inc.	895	• Telia
877	• Illuminet	896	• Toshiba
878	• Intel Corporation	897	• TSI Telecommunication
879	• Interlink Networks, Inc.	898	Services, Inc.
880	• Intersil	899	• TTS-Linx
881	• iPass, Inc.	900	• Wayport
882	• Jungo Networks	901	• Woodside Networks
883	• Lucent Technologies		

902
903 **WISPr Contact Information**
904
905   The following individuals may be contacted in regards to WISPr or this document:
906
907   Butch Anton (WISPr Chair)
908   Gemtek Systems, Inc.
909   Email: butch@butch.net
910
911   Blair Bullock (WISPr Vice-Chair)
912   iPass, Inc.
913   Email: bbullock@ipass.com
914
915   Joel Short (WISPr Vice-Chair)
916   Nomadix, Inc.
917   Email: jshort@nomadix.com

918 **Appendices**
919
920   WISPr has considered several "forward-looking" technologies that may, in the future, be useful in WISP
921   roaming. Some of these technologies and protocols are simple enhancements to the base-line
922   recommendations; others are in still in the early stages of development, while some (such as IEEE
923   802.1X) are substantially complete but are not widely deployed. As such, it is impossible to make
924   distinct recommendations for the implementation of these technologies and so consideration of these
925   technologies has been placed in the appendices to follow. WISPr is committed to further exploring new
926   technologies and protocols as they emerge and evaluating the issues surrounding future WISPr
927   implementations. In order for an appendix to be formally adopted as an official WISPr recommendation
928   and moved into the main body of this document, new and substantial evidence must be introduced to
929   qualify the technology as having positive field experience in a WISP implementation as it applies to
930   roaming.

931 **Appendix A – 802.1x**

932   **Access Method User Experience**
933
934   *"The user starts his laptop (either from boot up or a resume) and provides the 802.1x networking*
935   *client with a username, a credential, and the Hotspot Operator's SSID. The wireless networking client*
936   *manages the connection to the Hotspot Operator and establishes networking service through an*
937   *existing user account. The networking client automatically starts up the users welcome page specified*
938   *by the AAA server. When the user is finished, he simply disconnects from the wireless network*
939   *explicitly through the wireless networking client or by simply shutting down his laptop. Either action*
940   *will result in immediate disconnect of his session."*
941
942   When 802.1x authentication methods are used, the user service is controlled by the AP.   See the figure
943   below, "Figure D: Authentication and Accounting Process for Roaming 802.1x Users."
944
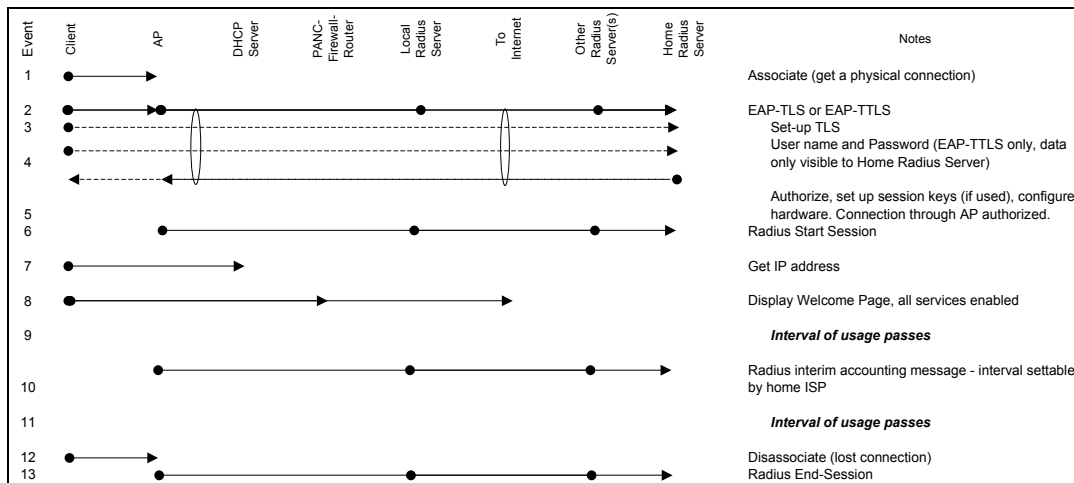
946   **Figure C: Authentication and Accounting Process for Roaming 802.1x Users**

947
948   Event 1, 2, 3: The access process will begin with the client and AP negotiating the use of an EAP
949   authentication method. In this example, the user is configured for the use of EAP-TLS or EAP-TTLS. In
950   both cases, TLS is used to authenticate the home RADIUS server. This is essential, as the user has a
951   preexisting established business (trust) relationship with their Home Entity. This step is protected from
952   unwanted interactions with the local RADIUS server or any other intermediary RADIUS server.
953

954   Event 3: If the Home Entity wishes to use EAP-TLS to authenticate users, each user must have their own
955   certificate.
956
957   Event 4: If the Home Entity wishes to use EAP-TTLS to authenticate users, the client provides the user
958   name and password protected by the TLS record phase. The use of the TLS record phase is equivalent to
959   the use of SSL for protecting web pages. Only the Home Entity is able to receive the user name and
960   password. This step is protected from unwanted interactions with the local RADIUS server or any other
961   intermediary RADIUS server.
962
963   Event 5: On successful authentication, the home RADIUS server authorizes the AP to provide a
964   connection to the client and can also provide a session specific WEP key and configure the AP with an
965   interval to change the WEP key. If this change occurs at sub-second intervals, WEP is resistant to
966   known WEP attack. It is only at this step that the client has a network connection.
967
968   Event 6: The AP acknowledges the service authorization with a RADIUS Accounting-Request message
969   containing an Acct-Status-Type Attribute with the Value field set to "Start" (1). This starts the timing of
970   the user's session.
971
972   Event 10: The AP should generate a RADIUS Accounting-Request message containing an Acct-Status-
973   Type Attribute with the Value field set to "Interim-Update" (3) at intervals specified by the home
974   RADIUS server in Event 5. When generated by the AP, this periodic accounting is created without the
975   overhead of additional authentication messages.
976
977   Event 12, 13: The AP should generate a RADIUS Accounting-Request message containing an Acct-
978   Status-Type Attribute with the Value field set to "Stop" (2) when the user's client disconnects
979   (disassociates) from the AP. This provides an accurate measure of the connection duration. If the user's
980   disconnection is due to interference or a weak signal, a new authentication process is started when a
981   connection is reestablished.

982   **802.1x Considerations**

983
984   The credentials required during the 802.1x Authentication and Accounting Process described above will
985   depend to the authentication method selected by the user or as required by the Home Entity.   The
986   following issues should be considered:
987
988   **First Time User**
989
990   The user will be required to install an 802.1x networking client to use the 802.1x authentication
991   methods. It is expected that the 802.1x client will be (a) provided as part of the networking driver when
992   they purchase an 802.11b adapter, (b) provided as part of the "dialer" from their Home Entity, (c)
993   purchased separately, or (d) provided as part of their operating system. Initially, it is expected that
994   some WISPs will be distributing the 802.1x clients to simplify identifying affiliate Hotspot Operators
995   and making the appropriate SSID entry.
996
997   **Authentication methods**
998
999   It is RECOMMENDED that the Home Entity select either 802.1x/EAP-TLS or 802.1x/EAP-TTLS.
1000   802.1x/EAP-TTLS can be used if the users are being authenticated with user names and passwords or
1001   802.1x/EAP-TLS can be used if certificates are used to authenticate the user.
1002
1003   Both methods have the identical technical requirements of the networking hardware, of the RADIUS
1004   protocols, and of any RADIUS servers that may exist between the Hotspot Operator and the Home
1005   Entity. The distinction between EAP-TLS and EAP-TTLS are handled by the user's wireless
1006   networking client and the Home Entity's RADIUS server, both managed by the Home Entity.
1007

1008   The choice of EAP-TLS or EAP-TTLS does affect the user's experience. The use of EAP-TLS
1009   requires the Home Entity to distribute certificates to each individual user. The use of the certificate and
1010   the safe keeping of the user's private key will depend of the vendor of the wireless client. In the case
1011   of EAP-TTLS, individual user certificates are not required. Instead, EAP-TTLS allows the use of
1012   passwords, tokens or other legacy authentication methods. The passwords and tokens may be the same
1013   ones in use for dial-up Internet roaming.
1014
1015   By encrypting the full NAI (user's identification), EAP-TTLS disrupts services that depend on the
1016   ability of a broker to count the number of unique NAI's serviced. Other third-party services that rely
1017   on user identification for policy enforcement and service selection will also be disrupted.
1018
1019   **Welcome Pages**
1020
1021   If specified by the RADIUS/AAA server, the 802.1x-networking client automatically launches the
1022   browser to display the welcome page. Since the RADIUS/AAA server may determine the Welcome
1023   Page URL, a rich range of welcome pages can be matched to the user's service preferences.
1024
1025   **Logoff Functionality**
1026
1027   The Hotspot Operator and the Home Entity require a means to measure the time the user is connected
1028   to the network. It is REQUIRED that the 802.1x hardware use RADIUS accounting messages to report
1029   the subscriber usage. Usage is then automatically reported with RADIUS start sessions at the
1030   completion of a successful authentication and a RADIUS stop session marks a disconnect (802.11b
1031   disassociate). The end of a session can be triggered by (a) user explicitly logging off through their
1032   wireless client, (b) a disconnect triggered by a maximum connection timer at the access, (c) a
1033   disconnect triggered by a exceeding the inactivity time limit at the access point, or (d) a loss of
1034   connection by the client going out of range.
1035
1036   **Automatically Establishing a Connection**
1037
1038   It is possible to automatically manage the connection process without user intervention. In general, a
1039   higher degree of automation is viewed as an improvement of the user's experience. However, there are
1040   a few areas that need careful consideration: (a) will the user be confronted with unexpected usage
1041   charges, (b) in a location with more than one Hotspot Operator, will the right Hotspot Operator be
1042   selected, and (c) how to prevent unauthorized network usage if the user's laptop is stolen.
1043
1044   **Support for Protocol Extensions**
1045
1046   If the roaming user is to utilize the 802.1x access method, the hotspot operator must support the 802.1x
1047   access method and the entire AAA infrastructure including the Hotspot Operator, Roaming
1048   Intermediaries, and Home Entities MUST support implementation of RADIUS/EAP protocol
1049   extensions [RFC2869], including EAP messaging as a RADIUS proxy attribute, as part of the AAA
1050   infrastructure. Guidelines for implementing RADIUS functionality over 802.1x and 802.11 solutions
1051   have been discussed in detail by various IETF working groups [8021x].

1052   **Appendix B – Re-Authentication using PANA**

1053   **Requirements for Re-Authentication using PANA**
1054
1055   Connection hijacking may be used not only to impersonate a user by taking over their connection while
1056   they're active (a user may leave without performing explicit logout), but also after they leave, an
1057   unscrupulous provider may seize that connection and hold it open in order to increase billing time. In
1058   order to prevent connection hijacking, periodical re-authentication with mutual authentication SHOULD
1059   be performed when performing usage-based accounting. In addition, the periodic re-authentication
1060   SHOULD be performed locally between client and the network, if the re-authentication is performed

1061   with a short internal (e.g., less than 5 minutes) in order not to increase AAA signaling traffic exchanged
1062   in the core network. The periodic re-authentication can also be used for detection of client
1063   disconnection. The following Working Group exists the IETF (Internet Engineering Task Force) to
1064   develop a new protocol:
1065
1066   *~ PANA ~*
1067   (Protocol for carrying Authentication for Network Access), which is able to support such a periodical
1068   and local re-authentication capability. One of the possible PANA usage scenarios is described as
1069   follows.
1070
1071   • The client obtains IP address via DHCP.
1072
1073   • The client performs PANA with the hotspot network. PANA carries EAP message as does
1074   PPP and 802.1X.
1075
1076   The EAP message carried in PANA message is extracted at the hotspot network and passed
1077   to the RADIUS entity.   Similarly, the EAP message created by the Home Entity and
1078   carried in the RADIUS message is extracted at the hotspot network and passed to PANA
1079   entity.
1080
1081   Some EAP algorithm such as EAP-GSS-IAKERB and EAP-SRP supports, in addition to
1082   authentication, distribution of a session key that is created by the Home Entity to the client.
1083   A copy of the session key is also distributed from the Home Entity to the hotspot via
1084   RADIUS.
1085
1086   • Based on the session key temporarily shared between the client and hotspot, PANA re-
1087   authentication is periodically performed between them without going all the way back to
1088   the Home Entity.
1089
1090   Note that the PANA solution can work even for a browser client if the PANA software is written in
1091   JAVA script and the client downloads the script from the hotspot via HTTP and runs it.

1092   **Appendix C – Enhancing the User Experience: The Smart Client**

1093   The Universal Access Method enables a wireless user with an ordinary web browser to log in and use the
1094   network of an arbitrary Hotspot Operator. However, the UAM User's Experience described in the
1095   Access Method section depends heavily upon the user presiding over the login process to make
1096   decisions, click buttons, and manually enter credentials into web pages. There are many situations
1097   where this amount of user interaction is undesirable. 802.1x promises to greatly simplify this process in
1098   the future, but few client platforms   currently support 802.1x. Therefore, it is important to define how a
1099   more simplified and seamless user experience can be achieved based on current client platforms.
1100
1101   If a WISP creates a customized client, that client can automatically configure the SSID, login to the
1102   WISP's network, and access other WISP-specific services without user intervention. Such a customized
1103   client can provide a "one click" experience to the user. However, if a customized client roams onto
1104   another WISP's network, it is unlikely to work correctly. Many "tacit" assumptions about how to log in
1105   to the Home Entity's network may be invalid on the WISP.
1106
1107   The solution to this problem is for WISPs to adopt common mechanisms to support a Smart Client
1108   capable of "one click" login to arbitrary WISP networks. There are two viable approaches for defining
1109   such mechanisms. One possibility is to define separate login mechanisms from the Universal Access
1110   Method, using whatever protocols are deemed appropriate. Another possibility is to use the same
1111   Universal Access Method mechanisms but to programmatically drive use of those mechanisms on the
1112   user's behalf. In other words, the Smart Client would use the same HTTP interface as an interactive user
1113   would. Because current practice already supports the Universal Access Method, WISPr recommends the

1114   latter approach.
1115
1116   Given that the Smart Client will use the UAM HTTP interface, there are some additional architectural
1117   choices to be made. Since the user is not available to guide navigation through the login pages, the
1118   Smart Client must be configured to understand the structure of the login process to complete it
1119   successfully. There are at least three possibilities:
1120
1121   • WISPs adopt a single common login process using standard, universal login and logout URLs that
1122   the WISP automatically redirects onto its site-specific URLs.
1123
1124   • WISPs standardize the login process but publish WISP-specific login and logout URLs. The
1125   Smart Client becomes responsible for obtaining and using the correct URL for the WISP. This in
1126   turn requires the Smart Client to be able to discover the identity of the WISP prior to login.
1127
1128   • The Smart Client extracts descriptive data from the welcome and/or login pages. It subsequently
1129   uses that information to configure and direct its login process. Such descriptive data would likely
1130   be encoded in XML and advertised through a reference on the welcome and/or login page.   The
1131   XML protocol is specified in The Smart Client to Access Gateway Interface Protocol Appendix.

1132   **Appendix D – The Smart Client to Access Gateway Interface Protocol**

1133   **Client Integration**

1134   This appendix discusses the third of the suggested UAM HTTP interfaces discussed in the Smart Client
1135   Appendix, allowing the Smart Client and Access Gateway to negotiate authentication URLs. This
1136   interface is implemented through the use of client-initiated, secure HTTP message exchanges. TCP
1137   connections are requested to ports 80 and 443 unless otherwise indicated. HTTP version 1.0 is specified
1138   due to its simplified header formats.
1139
1140   The following interaction diagrams represent the access procedure protocol from the perspective of the
1141   Smart Client.

1142   **Login Request: Successful Case**

```
1143    Client          Gateway          AAA
1144       |----------->|                        1. Arbitrary http GET
1145       |<-----------|                        2. Redirect Login URL
1146       |----------->|                        3. POST credentials
1147                    |---------->|            4. Auth request
1148                    |<----------|            5. Auth reply - accept
1149       |<-----------|                        6. Success Notification
1150                    |---------->|            7. Start accounting
1151                    |<----------|            8. Acknowledgment
1152           .
1153           .                                 Internet Access Enabled
1154           .
1155       |----------->|                        9. GET Logoff URL
1156                    |---------->|            10. Stop accounting
1157                    |<----------|            11. Acknowledgment
1158       |<-----------|                        12. Logoff Notification
```
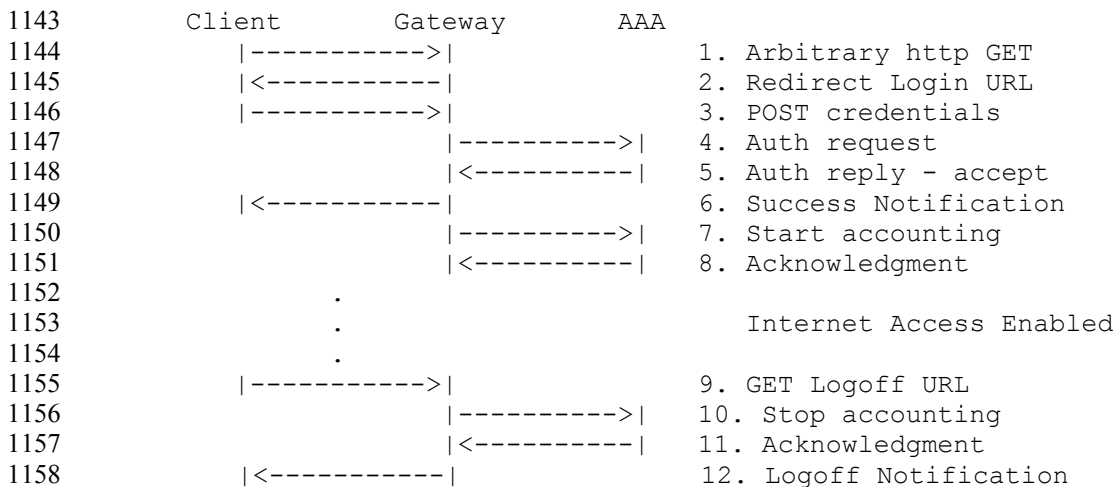
1159   **Login Request: Successful Case With Proxy Reply**

```
1160    Client          Gateway          AAA
1161       |----------->|                        1. Arbitrary http GET
1162       |<-----------|                        2. Proxy reply
1163                                                (NextURL, delay then resend)
```
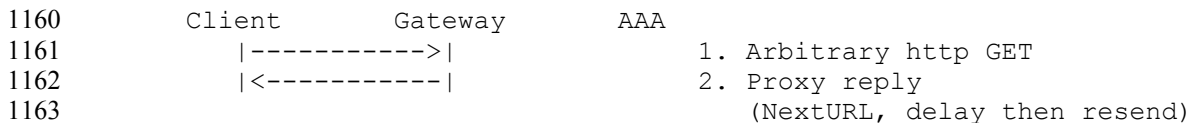
```
1164        |----------->|                      3. Http GET to NextURL
1165        |<-----------|                      4. Redirect Login URL
1166        |----------->|                      5. POST credentials
1167                     |---------->|           6. Auth request
1168                     |<----------|           7. Auth reply - accept
1169        |<-----------|                      8. Success Notification
1170                     |---------->|           9. Start accounting
1171                     |<----------|          10. Acknowledgment
1172             .
1173             .                               Internet Access Enabled
1174             .
1175        |----------->|                     11. GET Logoff URL
1176                     |---------->|          12. Stop accounting
1177                     |<----------|          13. Acknowledgment
1178        |<-----------|                     14. Logoff Notification
```

1179   **Login Request: Successful Case With Polling**

```
1180       Client        Gateway       AAA
1181        |----------->|                      1. Arbitrary http GET
1182        |<-----------|                      2. Redirect Login URL
1183        |----------->|                      3. POST credentials
1184                     |---------->|           4. Auth request
1185        |<-----------|                      5. Auth Pending
1186        |----------->|                      6. GET to polling URL
1187        |<-----------|                      7. Auth pending, delay then refresh
1188                     |<----------|           8. Auth reply - accept
1189        |----------->|                      9. GET to polling URL
1190        |<-----------|                     10. Success Notification
1191                     |---------->|          11. Start accounting
1192                     |<----------|          12. Acknowledgment
1193             .
1194             .                               Internet Access Enabled
1195             .
1196        |----------->|                     13. GET Logoff URL
1197                     |---------->|          14. Stop accounting
1198                     |<----------|          15. Acknowledgment
1199    |<-----------|                          16. Logoff Notification
```

1200   **Login Request: Reject**

```
1201       Client        Gateway       AAA
1202        |----------->|                      1. Arbitrary http GET
1203        |<-----------|                      2. Redirect Login URL
1204        |----------->|                      3. POST credentials
1205                     |---------->|           4. Auth request
1206                     |<----------|           5. Auth reply - reject
1207        |<-----------|                      6. Failure Notification
```

1208   **Login Request: Reject With Polling**

```
1209       Client        Gateway       AAA
1210        |----------->|                      1. Arbitrary http GET
1211        |<-----------|                      2. Redirect Login URL
1212        |----------->|                      3. POST credentials
1213                     |---------->|           4. Auth request
1214        |<-----------|                      5. Auth Pending
1215        |----------->|                      6. GET to polling URL
```

```
1216        |<----------|                   7. Auth pending, delay then refresh
1217                    |<----------|        8. Auth reply - reject
1218        |---------->|                    9. GET to polling URL
1219        |<----------|                   10. Reject Notification
1220
```

Protocol Specifics

The Smart Client to Access Gateway protocol is implemented using XML. Presently, no assumption of standardized URLs is made. Rather, the protocol depends on using URL Redirection. Most access gateways already provide a redirect mechanism for users attempting to access the network via a web browser. Because most browsers do not yet have XML support, it is likely that the access gateway is returning an HTML page. In order to implement the XML protocol, the gateway may implement one of the following options:

- Embed all XML tags within an HTML comment to prevent interpretation by the web browser.
- Embed XML tags on the redirect page in HTML comments which redirect the Smart Client to a URL which implements a true XML protocol.

Due to the inherent weaknesses in present implementations of WEP, SSL is used to protect the subscriber's authentication credentials. In order to further protect the subscriber from rogue access points, it is necessary to have a well-defined certificate at the access gateway that the client can verify.

The protocol messages include a proxy notification message. This is not included in the protocol description, but identified, as some access gateways require it.

All messages from the access gateway to the client will contain both response codes and message types.

The message types shall be one of the following values:

Message Type	Message Meaning
100	Initial redirect message
110	Proxy notification
120	Authentication notification
130	Logoff notification
140	Response to Authentication Poll
150	Response to Abort Login

The response code shall be one of the following values:

Response Code	Response Meaning
0	No error
50	Login succeeded (Access ACCEPT)
100	Login failed (Access REJECT)
102	RADIUS server error/timeout
105	Network Administrator Error: Does not have RADIUS enabled
150	Logoff succeeded
151	Login aborted
200	Proxy detection/repeat operation
201	Authentication pending
255	Access gateway internal error

1248   **Smart Client HTTP GET to ORIGIN SERVER**

1249   The Smart Client shall perform an HTTP GET to a valid roaming site to initiate the access sequence.
1250
1251   When the client system is already authorized for access at the access gateway, the gateway shall pass the
1252   HTTP GET through to the connected public network and return no special response. This behavior is
1253   also required whenever a subscriber attempts access using the Smart Client while already authorized for
1254   access as a result of accepting the local terms and conditions on the access location web site (i.e., the
1255   user agreed to the standard service agreement for service at the access site and the authorized service
1256   period has not yet elapsed).
1257
1258   If the subscriber should navigate to the terms & conditions page on the web site at the access location
1259   while authorized for access via the Smart Client, the access gateway shall deliver a generic "you are
1260   already logged in" or other appropriate rejection in response to an authorization attempt.
1261   When the client device is not currently authorized for access, the access gateway shall return an HTTP
1262   redirect (302) status message or an META HTTP-EQUIV="REFRESH" message. It is also possible for
1263   the access gateway to return a proxy message in reply to the initial HTTP GET operation. This will be
1264   covered in more detail below.

1265   **Redirect**

1266   When a redirect message is returned it shall contain both the address and the access procedure
1267   identification for login and logout as described in the table below. The information shall be contained
1268   within a valid HTML message, delimited appropriately with the <HTML> and </HTML> tags. The
1269   HTML message may contain other valid HTML message elements (e.g., HEAD, BODY, etc.).
1270

Required Information name	Field format/value

Access procedure	`<AccessProcedure>`
	`    {Procedure Version}`
	`</AccessProcedure>`

Location Identifier	`<AccessLocation>`
	`    {Location ID}`
	`</AccessLocation>`

Location Name	`<LocationName>`
	`    {User readable location name}`
	`</LocationName>`

Login URL	`<LoginURL>`
	`    https://<site specific login URL>`
	`</LoginURL>`

Abort Login URL	`<AbortLoginURL>`
	`    https://<site specific login URL>`
	`</AbortLoginURL>`

Message Type	`<MessageType>`
	`    100`
	`</MessageType>`

Response	`<ResponseCode>`
	`    {Response Code data}`
	`</ResponseCode>`

1271
1272
1273   The location identifier specified uniquely identifies the device through which the access will occur. If
1274   this ID is a characteristic of the physical device, replacement of the device could modify the ID received
1275   from the access location. Accordingly, any device swaps should be reported to participating roaming
1276   network providers. This should be identical to the Location-ID vendor-specific attribute that is part of
1277   the *Authentication Request.*
1278
1279   The Smart Client can use the *LocationName* to describe to the user the location being connected to.
1280

1281   When all required parameters are not present, an internal malfunction of the access gateway shall be
1282   assumed and the Smart Client shall behave as though an internal gateway response code was received.
1283

1284   The *AbortLoginURL* is used by the client to inform the access gateway that some error has occurred
1285   during the login process. When this is received by the access gateway, every attempt should be made to
1286   abort the session cleanly and to never generate an accounting record.
1287

1288   *{response code}* shall be one of the values listed in the following table:
1289

Response Code	Response Message
0	No error
105	Network Administrator Error: Does not have RADIUS enabled
255	Access Gateway internal error

1290   **Proxy**

1291   When a proxy message is returned it may contain an optional Delay parameter. The proxy message
1292   should only occur in response to either the initial HTTP GET at login, or to the initial HTTP GET to the
1293   LogoffURL. The information may be contained within a valid HTML message, delimited appropriately
1294   with the <HTML> and </HTML> tags. The HTML message may contain other valid HTML message
1295   elements (e.g., HEAD, BODY, etc.).
1296

Information name	Field format/value	Required/ Optional

Message Type	`<MessageType>`
	    110
	`</MessageType>`
		Required

Response	`<ResponseCode>`
	    {Response Code data}
	`</ResponseCode>`
		Required

Next URL	`<NextURL>`
	    http://<site specific URL>
	`</NextURL>`
		Optional

Delay in seconds	`<Delay>`
	    {Number of seconds data}
	`</Delay>`
		Optional

1297
1298   When all required parameters are not present, an internal malfunction of the access gateway shall be
1299   assumed and the Smart Client shall behave as though an access gateway internal error response code was
1300   received.
1301

1302   When it receives the proxy message, the smart client should sleep for the number of seconds specified in
1303   the Delay parameter (none if it is not present) and then resend the HTTP GET. Note: The proxy message
1304   may occur multiple times.
1305

1306   If the optional <NextURL> is present, then the Smart Client should replace the URL it is using for the
1307   HTTP GET messages to this new URL. It is possible for this URL to be updated on each successive
1308   Proxy message. The last known value will be used if no <NextURL> is present in a given Proxy
1309   Message.
1310

1311   *{response code}* shall be one of the values listed in the following table:
1312

Response Code	Response Message

200	Proxy detection/repeat operation

Authentication

The authentication phase of the protocol shall consist of an authentication request POST operation by the Smart Client followed by a HTTP 200 or HTTP 302 reply by the access gateway.

Authentication Request

The Smart Client shall send a secure HTTP POST operation to the login URL returned in the Redirect message. Since the post will be using https, it should be assumed that port 443 would be used if not specified otherwise as part of the LoginURL.

The POST parameters shall be as follows:
- **UserName**: the full user id including appropriate clearinghouse routing prefixes
- **Password**: the user's password
- **Button**: form button identifier
- **OriginatingServer**: the URL of the server to which the activation GET operation was directed

Field name	Field naming/format specification	Required/ Optional
User name input field	name="UserName" max size="128"	Required
Password input	name="Password" max size="128"	Required
Button Identifier	name="button" content="Login"	Required
Form Name	Name="FNAME" content="0" (numeral zero)	Required
Origin Server	Name="OriginatingServer" content={original server GET URL}	Required

Authentication Reply

The access gateway shall return an HTTP 200 meta refresh or HTTP 302 redirect reply to the authentication request. The reply shall contain an XML segment with the fields described in the table below. The information may be contained within a valid HTML message, delimited appropriately with the <HTML> and </HTML> tags. The HTML message may contain other valid HTML message elements (e.g., HEAD, BODY, etc.).

Information name	Field format/value	Required/ Optional

Message Type	`<MessageType>`
	`    120`
	`</MessageType>`
		Required

Response	`<ResponseCode>`
	`    {Response Code Data}`
	`</ResponseCode>`
		Required

Reply Message	`<ReplyMessage>`
	`    {Reply Message Text}`
	`</ReplyMessage>`
		Optional

Login results URL	`<LoginResultsURL>`
	`    https://<site specific login URL>`
	`</LoginResultsURL>`
		Optional

Logoff URL	`<LogoffURL>`
	`    https://<site specific logoff URL>`
	`</LogoffURL>`
		Optional*

1337   The *LogoffURL* must be present in the authentication reply if the Response (response code) is "Login
1338   succeeded". It may contain session specific information if required by the access gateway.
1339
1340   *{response code}* shall be one of the values listed in the following table:
1341

Response Code	Response Meaning
50	Login succeeded (Access ACCEPT)
100	Login failed (Access REJECT)
102	RADIUS server error/timeout
201	Authentication pending
255	Access Gateway internal error

1342

1343   The optional "*ReplyMessage*" returns text to the client that is taken from the RADIUS attribute *Reply-*
1344   *Message*. This allows the AAA server to provide a human readable reason for rejecting an authentication
1345   request.
1346
1347   The access gateway may choose to block on the authentication request and reply immediately to the user
1348   if the time-to-authenticate is expected to be low. Alternatively, if there are many concurrent
1349   authentication requests and/or the time-to-authenticate is very high, the gateway may choose to
1350   immediately return an "Authentication Pending" message causing the client to poll.
1351
1352   If the authentication reply is "Authentication Pending" (response code 201) then the Smart Client will
1353   begin polling the access gateway for the authentication results. This requires the inclusion of the optional
1354   "*LoginResultsURL*" in the authentication reply message.

1355   **Authentication Results Polling**

1356   If the authentication reply message returned "Authentication pending" then the client will enter the
1357   authentication-polling phase. The authentication-polling phase of the protocol shall consist of a series of
1358   HTTPS GET operations by the Smart Client followed by HTTP 200 or HTTP 302 replies by the access
1359   gateway. This implements an optional polling mechanism that allows the access gateway to optimize
1360   resources.

1361   **Authentication Poll**

1362   The client shall send a secure http GET to the "LoginResultsURL" that was returned in the
1363   authentication reply message. Since the post will be using https, it is assumed that port 443 will be used
1364   unless specified otherwise as part of the URL.

1365   **Response to Authentication Poll**

1366   The access gateway shall return an HTTP 200 meta refresh or HTTP 302 redirect reply to the
1367   authentication results poll. The reply shall contain an XML segment with the fields described in the table
1368   below. The information may be contained within a valid HTML message, delimited appropriately with
1369   the <HTML> and </HTML> tags. The HTML message may contain other valid HTML message
1370   elements (e.g., HEAD, BODY, etc.).
1371

Information name	Field format/value	Required/ Optional

Message Type	`<MessageType>`
	`    140`
	`</MessageType>`
		Required

Response	`<ResponseCode>`
	    `{Response Code Data}`
	`</ResponseCode>`
		Required

Reply Message	`<ReplyMessage>`
	    `{Reply Message Text}`
	`</ReplyMessage>`
		Optional

Delay in seconds	`<Delay>`
	    `{Number of seconds data}`
	`</Delay>`
		Optional

Logoff URL	`<LogoffURL>`
	    `https://<site specific logoff URL>`
	`</LogoffURL>`
		Optional

1372

1373

1374   The LogoffURL must be present in the response to authentication poll if the response (response code) is
1375   "Login succeeded". It may contain session specific information if required by the access gateway.

1376

1377   *{response code}* shall be one of the values listed in the following table:

1378

Response Code	Response Meaning
50	Login succeeded (Access ACCEPT)
100	Login failed (Access REJECT)
102	RADIUS server error/timeout
201	Authentication pending
255	Access Gateway internal error

1379

1380   If the authentication is complete, then the response to the authentication poll will contain the
1381   authentication results. If not (response code 201), then it will request the client to delay for the number
1382   of seconds specified in the "Delay" field and then resend the HTTP GET to the "LoginResultsURL".

1383   **Abort Login**

1384   In the event that a protocol problem has occurred during the login process, the client will make a GET
1385   operation to the abort login URL followed by a HTTP 200 or HTTP 302 reply by the access gateway.

1386   **Abort Login Request**

1387   To abort a login, the Smart Client shall send a HTTP GET operation to the AbortLoginURL returned in
1388   the initial redirect message.

1389   **Abort Login Reply**

1390   The access gateway shall return an HTTP 200 meta refresh or HTTP 302 redirect reply to the abort login
1391   request. The reply shall contain an XML segment with the fields described in the table below. The
1392   information may be contained within a valid HTML message, delimited appropriately with the <HTML>
1393   and </HTML> tags. The HTML message may contain other valid HTML message elements (e.g.,
1394   HEAD, BODY, etc.).

1395

Information name	Field format/value	Required/ Optional

Message Type	`<MessageType>`
	    `150`
	`</MessageType>`
		Required

Response	`<ResponseCode>`
	`    {Response Code Data}`
	`</ResponseCode>`
		Required

Logoff URL	`<LogoffURL>`
	`    https://<site specific logoff URL>`
	`</LogoffURL>`
		Optional*

1396
1397   The *LogoffURL* must be present in the abort reply if the Response (response code) is "Login succeeded".
1398   It may contain session specific information if required by the access gateway. The connection should not
1399   be terminated in this case. If the client wishes to terminate the connection then it will send a logoff
1400   request to the logoff URL.

1401
1402   *{response code}* shall be one of the values listed in the following table:
1403

Response Code	Response Meaning
50	Login succeeded (Access ACCEPT)
151	Login aborted
255	Access Gateway internal error

1404

1405   **Logoff**

1406   The logoff phase of the protocol shall consist of a GET operation to the logoff URL by the Smart Client
1407   followed by a HTTP 200 or HTTP 302 reply by the access gateway.

1408   **Logoff Request**

1409   To initiate a logoff, the Smart Client shall send a HTTP GET operation to the Logoff URL returned in
1410   either the authentication reply or authentication poll reply message.

1411   **Logoff Reply**

1412   The access gateway shall return an HTTP 200 meta refresh or HTTP 302 redirect reply to the logoff
1413   request. The reply shall contain an XML segment with the fields described in the table below. The
1414   information may be contained within a valid HTML message, delimited appropriately with the <HTML>
1415   and </HTML> tags. The HTML message may contain other valid HTML message elements (e.g.,
1416   HEAD, BODY, etc.).
1417

Information name	Field format/value	Required/ Optional
Message Type	`<MessageType>130</MessageType>`	Required
Response	`<ResponseCode>{Response Code Data}</ResponseCode>`	Required

1418
1419
1420   *{response code}* shall be one of the values listed in the following table:
1421

Response Code	Response Meaning
150	Logoff succeeded
255	Access Gateway internal error

1422

1423   **XML Schema**

1424   `<?xml version="1.0" encoding="UTF-8"?>`
1425   `<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"`
1426   `elementFormDefault="qualified" attributeFormDefault="unqualified">`

32

```
1427                    <xs:element name="WISPAccessGatewayParam">
1428                      <xs:complexType>
1429                        <xs:choice>
1430                          <xs:element name="Redirect" type="RedirectType"/>
1431                          <xs:element name="Proxy" type="ProxyType"/>
1432                          <xs:element name="AuthenticationReply"
1433                                      type="AuthenticationReplyType"/>
1434                          <xs:element name="AuthenticationPollReply"
1435                                      type="AuthenticationPollReplyType"/>
1436                          <xs:element name="LogoffReply" type="LogoffReplyType"/>
1437                          <xs:element name="AbortLoginReply" type="AbortLoginReplyType"/>
1438                        </xs:choice>
1439                      </xs:complexType>
1440                    </xs:element>
1441                    <xs:simpleType name="AbortLoginURLType">
1442                      <xs:restriction base="xs:anyURI"/>
1443                    </xs:simpleType>
1444                    <xs:simpleType name="NextURLType">
1445                      <xs:restriction base="xs:anyURI"/>
1446                    </xs:simpleType>
1447                    <xs:simpleType name="AccessProcedureType">
1448                      <xs:restriction base="xs:string"/>
1449                    </xs:simpleType>
1450                    <xs:simpleType name="AccessLocationType">
1451                      <xs:restriction base="xs:string"/>
1452                    </xs:simpleType>
1453                      <xs:simpleType name="LocationNameType">
1454                        <xs:restriction base="xs:string"/>
1455                      </xs:simpleType>
1456                    <xs:simpleType name="LoginURLType">
1457                      <xs:restriction base="xs:anyURI"/>
1458                    </xs:simpleType>
1459                    <xs:simpleType name="MessageTypeType">
1460                      <xs:restriction base="xs:integer"/>
1461                    </xs:simpleType>
1462                    <xs:simpleType name="ResponseCodeType">
1463                      <xs:restriction base="xs:integer"/>
1464                    </xs:simpleType>
1465                    <xs:simpleType name="ReplyMessageType">
1466                      <xs:restriction base="xs:string"/>
1467                    </xs:simpleType>
1468                    <xs:simpleType name="LoginResultsURLType">
1469                      <xs:restriction base="xs:anyURI"/>
1470                    </xs:simpleType>
1471                    <xs:simpleType name="LogoffURLType">
1472                      <xs:restriction base="xs:anyURI"/>
1473                    </xs:simpleType>
1474                    <xs:simpleType name="DelayType">
1475                      <xs:restriction base="xs:integer"/>
1476                    </xs:simpleType>
1477                    <xs:complexType name="RedirectType">
1478                      <xs:all>
1479                        <xs:element name="AccessProcedure" type="AccessProcedureType"/>
1480                        <xs:element name="AccessLocation" type="AccessLocationType"/>
1481                        <xs:element name="LocationName" type="LocationNameType"/>
1482                        <xs:element name="LoginURL" type="LoginURLType"/>
1483                        <xs:element name="AbortLoginURL" type="AbortLoginURLType"/>
1484                        <xs:element name="MessageType" type="MessageTypeType"/>
1485                        <xs:element name="ResponseCode" type="ResponseCodeType"/>
1486                      </xs:all>
1487                    </xs:complexType>
1488                    <xs:complexType name="ProxyType">
1489                      <xs:all>
```

33

```
1490            <xs:element name="MessageType" type="MessageTypeType"/>
1491            <xs:element name="ResponseCode" type="ResponseCodeType"/>
1492            <xs:element name="NextURL" type="NextURLType" minOccurs="0"
1493                                              maxOccurs="1"/>
1494            <xs:element name="Delay" type="DelayType" minOccurs="0"
1495                                              maxOccurs="1"/>
1496         </xs:all>
1497       </xs:complexType>
1498       <xs:complexType name="AuthenticationReplyType">
1499         <xs:all>
1500            <xs:element name="MessageType" type="MessageTypeType"/>
1501            <xs:element name="ResponseCode" type="ResponseCodeType"/>
1502            <xs:element name="ReplyMessage" type="ReplyMessageType"
1503                      minOccurs="0" maxOccurs="1"/>
1504            <xs:element name="LoginResultsURL" type="LoginResultsURLType"
1505                      minOccurs="0" maxOccurs="1"/>
1506            <xs:element name="LogoffURL" type="LogoffURLType"
1507                      minOccurs="0" maxOccurs="1"/>
1508         </xs:all>
1509       </xs:complexType>
1510       <xs:complexType name="AuthenticationPollReplyType">
1511         <xs:all>
1512            <xs:element name="MessageType" type="MessageTypeType"/>
1513            <xs:element name="ResponseCode" type="ResponseCodeType"/>
1514            <xs:element name="ReplyMessage" type="ReplyMessageType"
1515                      minOccurs="0" maxOccurs="1"/>
1516            <xs:element name="Delay" type="DelayType"
1517                      minOccurs="0" maxOccurs="1"/>
1518            <xs:element name="LogoffURL" type="LogoffURLType"
1519                      minOccurs="0" maxOccurs="1"/>
1520         </xs:all>
1521       </xs:complexType>
1522       <xs:complexType name="LogoffReplyType">
1523         <xs:sequence>
1524            <xs:element name="MessageType" type="MessageTypeType"/>
1525            <xs:element name="ResponseCode" type="ResponseCodeType"/>
1526         </xs:sequence>
1527       </xs:complexType>
1528       <xs:complexType name="AbortLoginReplyType">
1529         <xs:sequence>
1530            <xs:element name="MessageType" type="MessageTypeType"/>
1531            <xs:element name="ResponseCode" type="ResponseCodeType"/>
1532            <xs:element name="LogoffURL" type="LogoffURLType"
1533                      minOccurs="0" maxOccurs="1"/>
1534         </xs:sequence>
1535       </xs:complexType>
1536     </xs:schema>
```

1537   **Examples**

1538   The messages documented in this section are associated with their *originator*, either client or Access
1539   Gateway.

1540

1541   ***Authentication Procedure Activation [client] to port 80 at arbitrary IP address*** **(xxx.yyy.zzz.eee)**
1542   ```
         GET / HTTP/1.0<CR><LF><CR><LF>
         ```

1543

1544     ***Activation - Redirect Reply***
1545     ```
         <?xml version="1.0" encoding="UTF-8"?>
1546     <WISPAccessGatewayParam
1547         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
1548         xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccessGatewa
1549     yParam.xsd">
         ```

```
1550              <Redirect>
1551                <AccessProcedure>1.0</AccessProcedure>
1552                <AccessLocation>12</AccessLocation>
1553                <LocationName>
1554                  ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport
1555                </LocationName>
1556                <LoginURL>http://www.acmewisp.com/login/</LoginURL>
1557                <AbortLoginURL>
1558                  http://www.acmewisp.com/abortlogin/
1559                </AbortLoginURL>
1560                <MessageType>100</MessageType>
1561                <ResponseCode>0</ResponseCode>
1562              </Redirect>
1563            </WISPAccessGatewayParam>
1564
```

1565   *Activation - Proxy Reply*
```
1566            <?xml version="1.0" encoding="UTF-8"?>
1567            <WISPAccessGatewayParam
1568              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
1569              xsi:noNamespaceSchemaLocation=
1570              "http://www.acmewisp.com/WISPAccessGatewayParam.xsd">
1571              <Proxy>
1572                <MessageType>110</MessageType>
1573                <NextURL>http://www.acmewisp.com/proxypoll</NextURL>
1574                <ResponseCode>200</ResponseCode>
1575                <Delay>5</Delay>
1576              </Proxy>
1577            </WISPAccessGatewayParam>
1578
```

1579   *Authentication Request [client] via SSL*
```
1580            POST /process HTTP/1.0
1581            …
1582            <CR><LF><CR><LF>
1583            button=Login&UserName=WISP1/joseph@company.com&Password=xxxxx&FNAME=0&Orig
1584            inatingServer=http://xxx.yyy.zzz.eee/
1585            <CR><LF>
1586
```

1587   *Authentication Reply (Login Successful)*
```
1588            <?xml version="1.0" encoding="UTF-8"?>
1589            <WISPAccessGatewayParam
1590                xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
1591                xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccessGate
1592            wayParam.xsd">
1593              <AuthenticationReply>
1594                <MessageType>120</MessageType>
1595                <ResponseCode>50</ResponseCode>
1596                <ReplyMessage>Authentication Success</ReplyMessage>
1597                <LoginResultsURL>
1598                  http://www.acmewisp.com/loginresults/
1599                </LoginResultsURL>
1600                <LogoffURL>http://www.acmewisp.com/logoff/</LogoffURL>
1601              </AuthenticationReply>
1602            </WISPAccessGatewayParam>
1603
```

1604   *Authentication Reply (Login rejected)*
```
1605            <?xml version="1.0" encoding="UTF-8"?>
1606            <WISPAccessGatewayParam
1607                xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
1608                xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccessGate
1609            wayParam.xsd">
1610              <AuthenticationReply>
1611                <MessageType>120</MessageType>
```

```
1612            <ResponseCode>100</ResponseCode>
1613            <ReplyMessage>Invalid Password</ReplyMessage>
1614            <LoginResultsURL>
1615               http://www.acmewisp.com/loginresults/
1616            </LoginResultsURL>
1617            <LogoffURL>http://www.acmewisp.com/logoff/</LogoffURL>
1618          </AuthenticationReply>
1619        </WISPAccessGatewayParam>
1620
```

1621   *Authentication Reply (Login failed – unexpected RADIUS protocol error)*
```
1622        <?xml version="1.0" encoding="UTF-8"?>
1623        <WISPAccessGatewayParam
1624            xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
1625            xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccessGate
1626      wayParam.xsd">
1627          <AuthenticationReply>
1628            <MessageType>120</MessageType>
1629            <ResponseCode>102</ResponseCode>
1630            <ReplyMessage>RADIUS Error</ReplyMessage>
1631            <LoginResultsURL>
1632               http://www.acmewisp.com/loginresults/
1633            </LoginResultsURL>
1634            <LogoffURL>http://www.acmewisp.com/logoff/</LogoffURL>
1635          </AuthenticationReply>
1636        </WISPAccessGatewayParam>
1637
```

1638   *Authentication Reply (Login failed – internal access gateway error)*
```
1639        <?xml version="1.0" encoding="UTF-8"?>
1640        <WISPAccessGatewayParam
1641            xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
1642            xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccessGate
1643      wayParam.xsd">
1644          <AuthenticationReply>
1645          <MessageType>120</MessageType>
1646          <ResponseCode>255</ResponseCode>
1647            <ReplyMessage>Access Gateway Error</ReplyMessage>
1648            <LoginResultsURL>
1649     http://www.acmewisp.com/loginresults/
1650   </LoginResultsURL>
1651            <LogoffURL>http://www.acmewisp.com/logoff/</LogoffURL>
1652          </AuthenticationReply>
1653        </WISPAccessGatewayParam>
1654
```

1655   *Authentication Reply (Polling)*
```
1656
1657        <?xml version="1.0" encoding="UTF-8"?>
1658        <WISPAccessGatewayParam
1659            xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
1660            xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccessGate
1661            wayParam.xsd">
1662          <AuthenticationPollReply>
1663            <MessageType>140</MessageType>
1664            <ResponseCode>201</ResponseCode>
1665            <ReplyMessage>Authentication Pending</ReplyMessage>
1666            <Delay>5</Delay>
1667            <LogoffURL>http://www.acmewisp.com/logoff/</LogoffURL>
1668          </AuthenticationPollReply>
1669        </WISPAccessGatewayParam>
1670
```

1671   *Client-initiated Connection Termination (logoff) of Authenticated User*
```
1672        GET {Logoff_URL} <CR><LF><CR><LF>
1673
```

```
1674          Logoff Reply(Logoff Successful)
1675              <?xml version="1.0" encoding="UTF-8"?>
1676              <WISPAccessGatewayParam
1677                   xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
1678                   xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccessGate
1679                   wayParam.xsd">
1680                <LogoffReply>
1681                  <MessageType>130</MessageType>
1682                  <ResponseCode>150</ResponseCode>
1683                </LogoffReply>
1684              </WISPAccessGatewayParam>
1685
1686          Logoff Reply (Logoff failed – Access Gateway internal error)
1687
1688              <?xml version="1.0" encoding="UTF-8"?>
1689              <WISPAccessGatewayParam
1690                   xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
1691                   xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccessGate
1692                   wayParam.xsd">
1693                <LogoffReply>
1694                  <MessageType>130</MessageType>
1695                  <ResponseCode>255</ResponseCode>
1696                </LogoffReply>
1697              </WISPAccessGatewayParam>
1698
```