

Wireless Specifications

Wi-Fi Roaming Architecture and Interfaces Specification

WR-SP-WiFi-ROAM-I01-100729

ISSUED

Notice

This CableLabs Wireless specification is the result of a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. for the benefit of the cable industry and its customers. This document may contain references to other documents not owned or controlled by CableLabs. Use and understanding of this document may require access to such other documents. Designing, manufacturing, distributing, using, selling, or servicing products, or providing services, based on this document may require intellectual property licenses from third parties for technology referenced in this document. The Intellectual property contained in this specification is governed under the CableLabs' PacketCable™ Contribution and License Agreement for Intellectual Property.

Neither CableLabs nor any member company is responsible to any party for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document, or any document referenced herein. This document is furnished on an "AS IS" basis and neither CableLabs nor its members provides any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein.

© Copyright 2010 Cable Television Laboratories, Inc.
All rights reserved.

Document Status Sheet

Document Control Number:	WR-SP-WiFi-ROAM-I01-100729			
Document Title:	Wi-Fi Roaming Architecture and Interfaces Specification			
Revision History:	I01 – Released 07/29/10			
Date:	July 29, 2010			
Status:	Work in Progress	Draft	Issued	Closed
Distribution Restrictions:	Author Only	CL/Member	CL/Member/Vendor	Public

Key to Document Status Codes

Work in Progress	An incomplete document, designed to guide discussion and generate feedback that may include several alternative requirements for consideration.
Draft	A document in specification format considered largely complete, but lacking review by Members and vendors. Drafts are susceptible to substantial change during the review process.
Issued	A stable document, which has undergone rigorous member and vendor review and is suitable for product design and development, cross-vendor interoperability, and for certification testing.
Closed	A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs.

Trademarks

CableLabs[®], DOCSIS[®], EuroDOCSIS[™], eDOCSIS[™], M-CMTS[™], PacketCable[™], EuroPacketCable[™], PCMM[™], CableHome[®], CableOffice[™], OpenCable[™], OCAP[™], CableCARD[™], M-Card[™], DCAS[™], tru2way[™], and CablePC[™] are trademarks of Cable Television Laboratories, Inc.

Contents

1	SCOPE	1
1.1	Introduction and Purpose.....	1
1.2	Requirements.....	1
2	REFERENCES	2
2.1	Normative References.....	2
2.2	Informative References.....	3
2.3	Reference Acquisition.....	3
3	TERMS AND DEFINITIONS	4
4	ABBREVIATIONS AND ACRONYMS	5
5	OVERVIEW	6
5.1	Technical Overview.....	6
5.2	Roaming Architecture.....	7
5.2.1	<i>Phase 1 Architecture View</i>	7
5.2.2	<i>Roaming Reference Interfaces</i>	8
5.2.3	<i>Functional Components</i>	9
6	ROAMING ARCHITECTURE REQUIREMENTS	11
6.1	802.11 Air Interface.....	11
6.2	Interface Requirements for Access via clear SSID and Portal Sign In.....	11
6.2.1	<i>Subscriber Device Requirements Portal Sign In</i>	11
6.2.2	<i>Network Requirements for Portal Sign in Over Clear SSID</i>	11
6.2.3	<i>Interface Requirements – RADIUS</i>	11
6.2.4	<i>Access GW Requirements</i>	12
6.3	Interface Requirements for Access via Secure SSID Requirements.....	12
6.3.1	<i>User Name and Password Authentication via EAP-TTLS over a Secured SSID</i>	13
6.3.2	<i>Certificate Authentication via EAP-TLS over a Secured SSID</i>	14
6.4	Session Termination.....	15
6.5	Location Reports.....	15
6.5.1	<i>RFC5580 Location Reporting</i>	16
6.6	Post-Login Redirection.....	16
6.7	Accounting.....	16
6.8	Network to Network RADIUS Interface Requirements.....	18
6.8.1	<i>RADIUS Interface</i>	18
6.8.2	<i>Internetwork RADIUS Authentication Attributes</i>	18
6.8.3	<i>Internetwork RADIUS Accounting Attributes</i>	27
	APPENDIX I INFORMATIVE FLOWS	30
I.1	Portal Sign via Clear SSID.....	30
I.2	EAP-TTLS Username/Password Authentication.....	31
I.3	EAP-TLS Certificate Authentication.....	34
	APPENDIX II ACKNOWLEDGEMENTS	37

Figures

Figure 1 - Architecture View7
Figure 2 - Roaming Architecture Specified Interfaces8
Figure 3 - Subscriber Sign In on a Captive Portal via a Clear SSID30
Figure 4 - Authentication with EAP-TTLS32
Figure 5 - MSCHAPv2 Username/Password Authentication within EAP-TTLS34
Figure 6 - Authentication within EAP-TLS35

Tables

Table 1 - Roaming Architecture Reference Points9
Table 2 - RADIUS Authentication Attributes: Request and Challenge19
Table 3 - RADIUS Authentication Attributes: Accept and Reject22
Table 4 - RADIUS Authentication Attributes: CoA and Disconnect25
Table 5 - RADIUS Accounting Attributes28

1 SCOPE

1.1 Introduction and Purpose

Wi-Fi is a pervasive technology which enhances the user experience by allowing mobile consumption of rich multi-media content and access to data. This document specifies architecture requirements for best effort data roaming among cable operator Wi-Fi networks. Roaming allows a subscriber to use their operator subscription to gain connectivity to the Internet using a roaming partner Wi-Fi network.

The principal focus of this document is roaming among cable operator Wi-Fi networks; however, the model presented here may also be applied to non-cable operator Wi-Fi networks as well. Attention is placed on the inter-network interfaces and functional requirements needed among cable operators for roaming, while allowing operators flexibility on implementations internal to their network. Requirements are applicable to Wi-Fi clients, Wi-Fi gateways (GWs), and network systems.

1.2 Requirements

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

"MUST"	This word means that the item is an absolute requirement of this specification.
"MUST NOT"	This phrase means that the item is an absolute prohibition of this specification.
"SHOULD"	This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.
"SHOULD NOT"	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
"MAY"	This word means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

2 REFERENCES

2.1 Normative References

In order to claim compliance with this specification, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this specification. Notwithstanding, intellectual property rights may be required to use or implement such normative references.

- [IEEE 802.11] IEEE 802.11: Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, June 2007.
- [IEEE 802.11b] IEEE 802.11b: Higher-Speed Physical Layer Extension in the 2.4 GHz Band, June 2003.
- [IEEE 802.11g] IEEE 802.11g: Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band, June 2003.
- [IEEE 802.11i] IEEE 802.11i: Amendment 6: Medium Access Control (MAC) Security Enhancements, July 2004.
- [IEEE 802.11n] IEEE P802.11n/D9.0: Draft amendment 5: Enhancement for higher throughput, March 2009.
- [IEEE 802.1X] IEEE 802.1X: Port-Based Network Access Control (PNAC), December 2004.
- [RFC 2548] IETF RFC 2548, Microsoft Vendor-specific RADIUS Attributes, March 1999.
- [RFC 2616] IETF RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1, June 1999.
- [RFC 2818] IETF RFC 2818, HTTP over TLS, May 2000.
- [RFC 2865] IETF RFC 2865, Remote Authentication Dial In User Service (RADIUS), June 2000.
- [RFC 2866] IETF RFC 2866, RADIUS Accounting, June 2000.
- [RFC 2869] IETF RFC 2869, RADIUS Extensions, June 2000.
- [RFC 3576] IETF RFC 3597, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), July 2003.
- [RFC 3579] IETF RFC 3579, RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP), September 2003.
- [RFC 3580] IETF RFC 3580, IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines, September 2003.
- [RFC 4282] IETF RFC 4282, The Network Access Identifier, December 2005.
- [RFC 4301] IETF RFC 4301, Security Architecture for the Internet Protocol, December 2005.
- [RFC 4346] IETF RFC 4346, The Transport Layer Security (TLS) Protocol, V1.1, April 2006.
- [RFC 4372] IETF RFC 4372, Chargeable User Identity, January 2006.
- [RFC 5080] IETF RFC 5080, Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes, December 2007.
- [RFC 5216] IETF RFC 5216, The EAP-TLS Authentication Protocol, March 2008.
- [RFC 5281] IETF RFC 5281, Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0), August 2008.
- [RFC 5580] IETF RFC 5580, Carrying Location Objects in RADIUS and Diameter, August 2009.

- [WPA] Wi-Fi Alliance: Wi-Fi Protected Access (WPA) Enhanced Security Implementation Based on IEEE P802.11i standard, Version 3.1, August, 2004.
- [X.509] ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997.

2.2 Informative References

This specification uses the following informative references.

- [RFC 2759] Microsoft PPP CHAP Extensions, Version 2, January 2000.

2.3 Reference Acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone +1-303-661-9100; Fax +1-303-661-9199; <http://www.cablelabs.com>
- Institute of Electrical and Electronics Engineers, (IEEE), <http://www.ieee.org/web/standards/home/index.html>
- International Telecommunications Union, (ITU), Place des Nations, CH-1211, Geneva 20, Switzerland; Phone +41-22-730-51-11; Fax +41-22-733-7256, <http://www.itu.int>
- Internet Engineering Task Force (IETF) Secretariat, 46000 Center Oak Plaza, Sterling, VA 20166, Phone +1-571-434-3500, Fax +1-571-434-3535, <http://www.ietf.org>
- Wi-Fi Alliance, https://www.wi-fi.org/knowledge_center_overview.php?type=4

3 TERMS AND DEFINITIONS

This specification uses the following terms:

Best Effort Data Service	The subscriber is offered IP data network connectivity without an assured performance or Quality of Service (QoS) level.
Home Network	The home network holds the subscriber's subscription profile for Wi-Fi and other services. The home network is not related to a residential network or the subscriber's home.
Off-line charging	Off-line charging refers to charging and accounting requirements that do not affect, in real-time, the service rendered to the subscriber.
Roaming	The use of a home network subscription to gain access to a partner network.
Roaming Partner Network	A network that allows access for subscribers from another network based on a roaming agreement between the networks.
Visited Network	A roaming partner network that is providing Wi-Fi access for the subscriber.
Wi-Fi Network	The network providing Wi-Fi service to the subscriber, be it a home or visited network.

4 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations:

AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
AP	Access Point
AVP	Attribute Value Pair
CHAP	Challenge Handshake Authentication Protocol
CMTS	Cable Modem Termination System
CoA	Change of Authorization, when used for RADIUS
CUID	Changeable User Identity
DOCSIS®	Data-Over-Cable Service Interface Specifications
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol - Tunneled Transport Layer Security
eCM	Embedded Cable Modem
GW	Gateway
HTML	Hypertext Mark-up Language
HTTps	Hypertext Transfer Protocol Secure
MD5	Message-Digest algorithm 5
MSCHAPv2	Microsoft Challenge-Handshake Authentication Protocol version 2
MTU	Maximum Transmission Unit
NAI	Network Access Identifier
NTP	Network Time Protocol
PAP	Password Authentication Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comments
SSID	Service Set Identifier
STA	Station
TKIP	Temporal Key Integrity Protocol
URL	Uniform Resource Locator
Wi-Fi	Wireless Fidelity
Wi-Fi-GW	Wireless Fidelity Gateway
WPA	Wi-Fi Protected Access
XHTML	Extensible Hypertext Markup Language

5 OVERVIEW

5.1 Technical Overview

This document identifies a wireless roaming architecture where cable subscribers are able to access best effort high speed data connectivity to the Internet through roaming partner networks. The roaming partner network provides IP address management and traffic routing for roaming subscribers. The high speed data service is provided to Wi-Fi enabled devices with full browsers such as Windows and Mac OS PCs, and highly capable mobile devices. Browsers may include Microsoft Internet Explorer, Firefox, and Safari. Operator configured clients are not required, but may be deployed as members see fit. A subscriber may be able to sign in multiple devices onto a visited network as controlled by the home network operator.

Subscribers gain access to a visited network by using their home operator subscription. All visited networks support subscriber access via a web portal sign in with username and password for roamers as a minimum requirement. Cable operators have the option to deploy additional methods for network access with operator configured secure clients, for example, with [WPA]. The visited network proxies credentials to the home network, where the home network then performs subscriber authentication and device authorization. Upon successful initial authentication, the subscriber device can be redirected to a home network hosted welcome page if the home network provides the page Uniform Resource Locator (URL) to the visited network. Alternatively, the subscriber may be redirected to a local enterprise web page upon successful authentication.

The service is intended to support roamers in a visited network for a pre-determined length of time such that the roamer is not forced to sign in repeatedly during the configured time period, even when moving between visited network Access Points (AP)s. A roamer session may end due to session or idle time outs. The time values are set (1) by a RADIUS attribute sent from the home network to the visited network, (2) visited network local policy if a home network attribute is not received or (3) visited network policy that may override larger values received by the home network. The application and enforcement for these time outs are set between two network operators as part of their roaming agreement. A roamer session may also end by explicit request from the home network, or due to the client failing to request an IP address refresh.

This document requires an operator configured and managed Wireless Fidelity Gateway (Wi-Fi GW) to enable service. The Wi-Fi GW requirements here are focused on roaming, however a complete set of requirements need to define the Wi-Fi GW are out of the scope of this specification. Operator managed Wi-Fi GWs may be deployed in residences, enterprises or in public settings. Therefore, the architecture allows the operator to control and limit the resources afforded to roamed-in traffic in order to ensure appropriate service to home operator network subscribers. Visited network AP Service Set Identifier (SSID) configurations can include:

1. A clear (unencrypted) SSID common to all partner networks that allows roamers to log into a captive sign in web portal.
2. An optional secured SSID common to all partner network that supports secure connections for roamers. An operator configured client may be required for this access.
3. At least one home operator controlled SSID, that may or may not be broadcast.
4. An SSID that could be configured by the subscriber on residential APs, or configured by the enterprise on enterprise APs. This may be considered a spare SSID.

The two SSID configurations used by roaming subscribers are addressed in this document. Additional SSIDs may be used by the home network subscriber and by the serving operator for a variety of purposes.

Visited networks report time duration and traffic volume accounting data to the home network for each roamer on their network. The visited network provides an accounting report upon session end, and also provides interim reports as needed to accurately convey traffic volume usage or a subscriber transition to a new AP location.

An important architecture requirement is that the inter-operator network interfaces needed for data service roaming will be open and based on readily available standards commonly used in the Wi-Fi industry in order to encourage multi-vendor interoperability. Interoperable interfaces are specified between the client and visited network, and operator network to network interfaces. Vendor-specific solutions are avoided.

While focused on inter-cable operator roaming, the architecture should readily support roaming with regional or nation wide Wi-Fi networks that are not operated by cable operators.

Security aspects are an important aspect of the Wi-Fi Roaming architecture. The architecture protects the network from various denial of service, network disruption, theft-of-service attacks. The architecture provides support for confidentiality, authentication, integrity, and access control mechanisms across inter-network interfaces as provisioned by the operator.

5.2 Roaming Architecture

5.2.1 Phase 1 Architecture View

The following diagram illustrates the Phase 1 architecture view and network relationships.

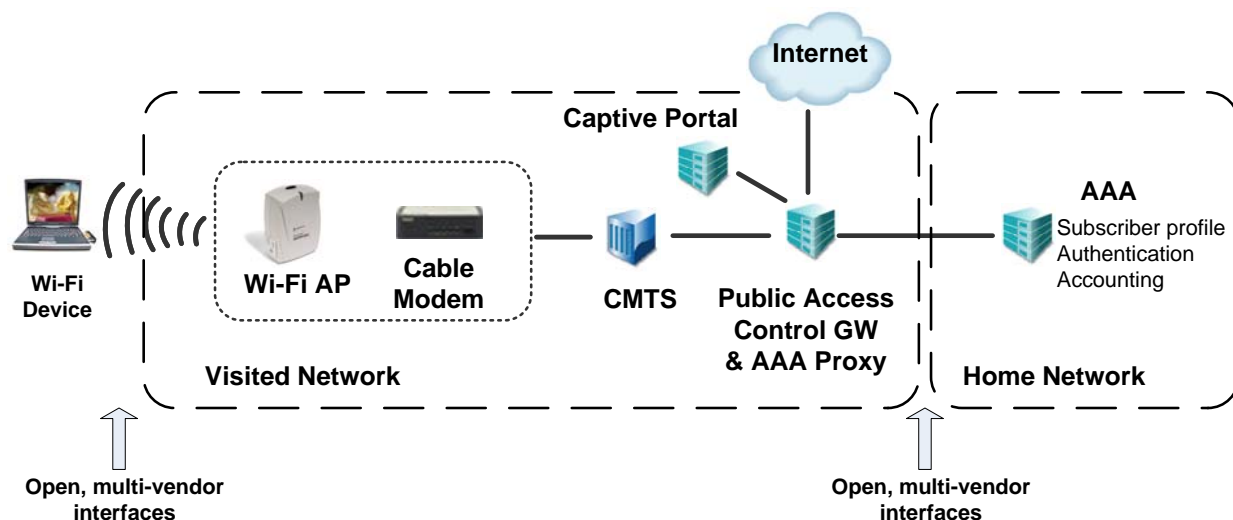


Figure 1 - Architecture View

As seen from Figure 1, the roaming architecture specifies requirements for the open interfaces between three elements:

1. The Wi-Fi device for the roaming subscriber.
2. The Wi-Fi visited network.
3. The Wi-Fi home network.

The roles of the visited network are to:

- provide best effort data connectivity between the 802.11 roaming device and the Internet for a time duration established during authentication and enforced by the visited network operator;
- act as an authentication proxy to the home network, and complete device admission based on home network authorization;

- provide accounting reports to the home network;
- provide confidentiality of subscriber traffic over the Wi-Fi air interface if configured by the visited network operator and supported by the client.

The roles of the home network are to:

- provision subscriber service and provide customer care;
- execute authentication and provide device authorization for subscriber service while on visited networks;
- collect accounting data from the visited network for billing purposes.

Figure 1 illustrates a number of functions needed within the visited network including the Wi-Fi GW that supplies the air interface, and the Data-Over-Cable Service Interface Specifications (DOCSIS) cable modem with the Cable Modem Termination System (CMTS) that supplies network connectivity. The functional elements portrayed may be distributed in the network or integrated into a single product. A Public Access Control GW supports routing of user traffic to the internet for authenticated subscribers. The AAA proxy supports an interface to the home network for Authentication, Authorization, and Accounting (AAA). A client for AAA signaling is supported at either the Wi-Fi GW or Access Control Gateway as determined by the operator. These functions are illustrated for information only since the roaming architecture does not decompose intra-operator network interface requirements to network elements internal to an operator network.

5.2.2 Roaming Reference Interfaces

The following diagram highlights the interfaces specified for the roaming architecture.

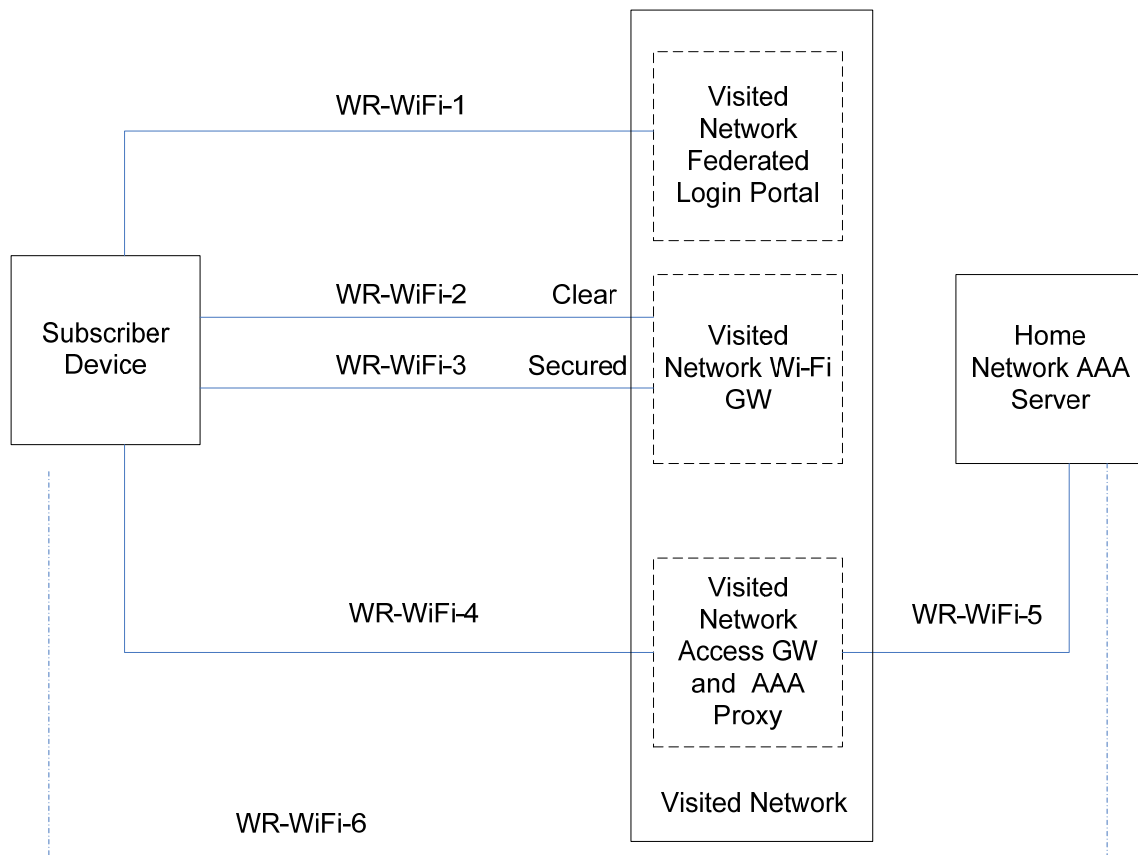


Figure 2 - Roaming Architecture Specified Interfaces

The interfaces identified in the roaming architecture support roaming for best effort data service. The interfaces are specified to ensure multi-vendor interoperability and enable a consistent subscriber experience on visited networks. Note that not all network interfaces are illustrated, but only those essential to inter-operator roaming. The functional elements shown in Figure 2 may be combined or distributed within network element deployments.

Table 1 - Roaming Architecture Reference Points

Reference Point	Network Elements	Description
WR-WiFi-1	Subscriber Device – Visited Network (portal)	This interface is used by the roaming subscriber to sign into a captive portal via the clear SSID. The interface is Hypertext Transfer Protocol Secure (HTTPS), Hypertext Mark-up Language (HTML).
WR-WiFi-2	Subscriber Device – Visited network (clear SSID)	This interface is the 802.11 air interface between the subscriber device and a clear SSID. 802.11n is used on this interface. This SSID may lead subscribers to the sign in portal.
WR-WiFi-3	Subscriber Device – Visited network (secure SSID)	This interface is the 802.11 air interface between the subscriber device and secure SSID. In addition to 802.11n, this interface also requires Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) encryption and authentication functions as specified by Wi-Fi Protected Access 2 (WPA2).
WR-WiFi-4	Subscriber Device- Visited network (authentication proxy)	This optional interface is used for Extensible Authentication Protocol (EAP) based authentication needed for the secure SSID. The visited network provides a proxy server for the client.
WR-WiFi-5	Visited Network – Home Network	This interface is used by the visited network to proxy credentials to the home network for authentication and device authorization. The home network uses this interface to authorize service on partner networks for its subscribers and to indicate authentication success to the visited network. This interface is also used to report accounting data from the visited to the home networks. The interface is RADIUS secured with IPsec. A security association needs to be maintained between the visited and home network on this interface.
WR-WiFi-6	Client-Home Network	This interface between the client and home AAA server is passed through the visited network. It is used for a home network selected authentication protocol, for example, Extensible Authentication Protocol - Transport Layer Security (EAP-TLS) or Extensible Authentication Protocol - Tunneled Transport Layer Security (EAP-TTLS). This interface is used in conjunction with WR-WiFi-5. The home AAA authenticates the client with this interface, after authentication is requested via RADIUS on the WR-WiFi-5 interface. RADIUS attributes are passed on WR-WiFi-5 that set the terms of authorization.

5.2.3 Functional Components

As can be seen from the architecture diagram in Figure 2, the roaming architecture includes a number of functional components that are described in the following subsections. Implementations internal to an operator network are out of scope. Therefore, the level of combination, integration, or distribution of the components described below is also out of scope.

5.2.3.1 Subscriber Devices

Subscriber devices provide the user interface for the subscriber. They enable portability via the 802.11 air interface towards the network. They also support interfaces to the login portal and visited network proxy for authentication

and device admission. The subscriber device also interfaces to the visited network access GW, which provides for subscriber traffic connectivity to the internet. The subscriber device also interfaces to the home AAA proxy for authentication protocols that are tunneled through the visited network.

5.2.3.2 Wi-Fi Gateway

The Wi-Fi Gateway (GW) provides the 802.11 air interface for the subscriber device. The GW integrates an 802.11 Access Point (AP) with a DOCSIS cable modem. Clear and secured SSIDs are provided. The Wi-Fi GW redirects initial service requests via the clear SSID to the captive portal. Depending upon operator deployment preference, the Wi-Fi GW may also provide a RADIUS signaling client in support of AAA functions. The Wi-Fi GW blocks unauthorized traffic.

5.2.3.3 Public Access Gateway

The Public Access Gateway provides an interface to the internet for roamed in subscriber traffic. Depending upon operator deployment preference, the Public Access Gateway GW may also provide Wi-Fi controller functions, a RADIUS signaling client in support of AAA functions, and redirection capabilities.

5.2.3.4 Visited Network AAA Proxy

The visited network AAA proxy locates the home network AAA server and routes roamed in subscriber AAA signaling and usage reports to the home network AAA server. The visited network AAA proxy establishes a security association with the home AAA server.

5.2.3.5 Home Network AAA Server

The home network AAA server contains the subscriber profile of Wi-Fi subscribers. It receives AAA signaling from the visited AAA proxy and authenticates the subscriber. It also receives usages reports from the visited network AAA proxy. The home network AAA server establishes a security association with the visited network AAA proxy.

5.2.3.6 Captive Portal

The captive portal provides a sign in web page for roamed in subscribers. The captive portal sends user credentials to a network component that provides the AAA RADIUS client. Depending upon operator deployment preferences, the captive portal may also redirect subscriber devices after successful authentication. Content displayed to the user during sign in may be provided or hosted by the visited network, or a combination of visited and home networks. The organization of content displayed to the user is beyond the scope of this specification.

5.2.3.7 CMTS

The CMTS controls access and use of the DOCSIS access network.

6 ROAMING ARCHITECTURE REQUIREMENTS

6.1 802.11 Air Interface

For wireless access, the subscriber device MUST support Wi-Fi Alliance certified 802.11b per [IEEE 802.11b], 802.11 g per [IEEE 802.11g] or 802.11n per [IEEE 802.11n] for wireless interfaces to the visited network. The Wi-Fi GW MUST support Wi-Fi Alliance certified 802.11b, g or n for wireless interfaces to the subscriber device per IEEE specifications [IEEE 802.11], [IEEE 802.11b], [IEEE 802.11g], and [IEEE 802.11n]. Additional device and network requirements are contained in the subsections below.

6.2 Interface Requirements for Access via clear SSID and Portal Sign In

This section includes interface requirements for subscribers to attach to the visited network Wi-Fi GW via a clear SSID that leads to a captive portal. Subscribers then sign into the portal web page for authentication and authorization.

6.2.1 Subscriber Device Requirements Portal Sign In

The subscriber device client MUST support an industry standard full browser with HTML and Extensible Hypertext Markup Language (XHTML), such as Internet Explorer 7.0 or Firefox 5.0, Safari, etc., to allow subscribers to login into a web portal with their user name and password. PDA and smart phones with capable web browser may also be used.

6.2.2 Network Requirements for Portal Sign in Over Clear SSID

The visited network Wi-Fi GW MUST provide a clear SSID with a pre-determined SSID name to allow roamers to sign in for access via a secure web page. This requirement may only apply to public deployments.

The subscriber initially selects the clear SSID on their native laptop connection manager, and the subscriber device attempts an 802.11 association with the visited network. After initial selection, the clear SSID may be added to the subscriber device connection manager wireless network list such that associations are automatically attempted. Upon an association attempt from a subscriber device, the visited network Access GW MUST provide an IP address to the unauthorized subscriber device for the sake of redirection to a log in portal without providing connectivity to the Internet or network services. The subscriber then launches a web browser. The visited network Access GW MUST direct the subscriber device to the login portal and establish a secured HTTPS [RFC 2818] connection between the subscriber device and portal server for subscriber login upon an initial HTTP [RFC 2616] request.

6.2.3 Interface Requirements – RADIUS

Upon the visited network portal receiving a user name and password entry from the subscriber, the visited network AAA proxy MUST initiate a RADIUS session and Access-Request to the home network AAA server per [RFC 2865] that contains the User-Name and User-Password attributes. The interface between the portal and AAA proxy is out of scope for this specification. See Section 6.8 for further RADIUS protocol requirements. The visited network AAA proxy MUST locate and route the RADIUS session to the home network based on the realm contained in the user name per Network Access Identifier (NAI) [RFC 4282]. The home network AAA MUST authenticate the subscriber based on user name password or reject the request. Upon receiving a RADIUS Access-Accept (authentication complete) from the home network AAA server, the visited network Access GW provides Internet access for the roaming subscriber device and begin to collect and report accounting data as described in Section 6.7. The interface between the visited network Access GW is out of scope of this document.

6.2.4 Access GW Requirements

The Access GW MUST redirect the residential subscriber device to a home network URL if provided by the home network. For business locations, the Access GW MUST have the functionality to redirect to a business splash page upon successful authentication if provisioned to do so by the network operator. The visited network MUST maintain internet connectivity without requiring subsequent user name and password for the duration of the session. See Section 6.4 for session end requirements.

The visited network Access GW MUST redirect the subscriber device back to the login portal upon the next service request after a session end. The visited network AAA proxy reports accounting data at certain intervals and after session end as specified in Section 6.7.

6.2.4.1 Login Portal Requirements

The captive login portal is a secure sign in web page that each operator within the federation hosts as a means for roaming subscribers from other networks to sign in for access. Subscribers enter their home network managed user name and password in order to gain access to the visited Wi-Fi network. After authentication the subscriber may be redirected to a predetermined web site as provided by the home network. If login takes place in a business location, subscribers may be redirected to local business splash page determined by the visited network customer. An operational goal for the login portal is that subscribers are offered a familiar experience on the portal sign in regardless of the visited network hosting the portal. This operational requirement does not dictate that all portals are identical among roaming partner networks, but it does impose a consistent set of qualities that each portal should achieve. This section provides a minimum set of requirements for the portal design to help ensure a consistent subscriber experience on any sign in portal site.

The portal MUST support a field for subscribers to select their home network provider. Upon selection of the home network provider, the portal MUST populate the sign in page with "Forgot Password" and "Helpdesk" hyperlinks that lead subscribers to home network customer care resources.

The portal MUST support HTTPS, HTML and XHTML to provide a secure sign in web page. The portal MUST support a field for subscribers to enter their user name. The minimum user name length is set by the home network. The portal web page MUST allow user name entries up to 253 characters in length.

The portal MUST support a field for subscribers to enter their password. The minimum password length is set by the home network. The portal web page MUST allow password entries up to 128 characters in length.

After successful subscriber authentication, the portal MUST redirect the subscriber device to a home network page URL if provided by the home network. Alternatively in enterprise deployments and upon successful subscriber authentication, the portal MUST redirect the subscriber device to a local enterprise web page.

The Wi-Fi GW MUST block further authentication attempts and user device traffic after a visited network operator configured number of failed sign in attempts. Furthermore, the Wi-Fi GW MUST block non-HTTP traffic from reaching the web portal prior to successful completion of the authentication.

6.3 Interface Requirements for Access via Secure SSID Requirements

Networks may support a second access model with a secured SSID that provides encryption of subscriber traffic over the air. This section defines interface requirements for secured access. The client provides credentials to the secured SSID. Home network providers may select user name and password, or MAC address and certificates, for client credentials. Protocol specifics are provided in subsequent sections. It is recommended that an operator configured client be used for access with secured SSIDs.

The subscriber device SHOULD support Wi-Fi Alliance certified WPA and WPA2 interfaces per [WPA] with EAP per [RFC 3576] for a secure over the air connection to the visited network. The subscriber device, visited network

Wi-Fi GW, and AAA proxy SHOULD support [IEEE 802.11i] and [IEEE 802.1X] EAP authentication methods as supported by [WPA]. These are the minimum requirements for security.

The subscriber device MUST allow the operator to set the multi-operator secure SSID to a higher priority network selection than the multi-operator clear SSID when the client supports an operator configured connection manager.

The visited network Wi-Fi GW SHOULD, as configured by the visited network operator, provide a secured SSID with a multi-operator secure SSID name to provide subscriber traffic encryption over the air interface to operator configured WPA and WPA2 enabled clients. If configured to do so by the operator, the Wi-Fi GW secure SSID MUST support AES per (recommended) or TKIP per [WPA]. Authentication alternatives via the secure SSID are contained in the sections below.

The visited network proxies credentials to the home network, which then executes authentication and authorization.

6.3.1 User Name and Password Authentication via EAP-TTLS over a Secured SSID

The following subsections include requirements to support authentication for roamers via EAP-TTLS authentication. EAP-TTLS allows the client to authenticate the home network AAA server via a server certificate. It also allows an inner authentication protocol to be tunneled via a secure over the air connection through to the home network for the subscriber to be authenticated by the home network using home network authentication methods. These requirements assume that EAP-TTLS establishes a TLS tunnel between the client and the home network AAA server. An informative flow diagram that illustrates these requirements is found in Appendix I.

The Client and home AAA server MUST support EAP-TTLSv0 [RFC 5281]. The visited network AAA proxy MUST proxy EAP-TTLS messages encapsulated in RADIUS to and from the home AAA server per [RFC 3579]. The client MUST report the username of a maximum 253 octets to the Wi-Fi network in the NAI format described in [RFC 4282]. The client MUST report the user password of 128 octets maximum length to the visited network.

The first step in EAP-TTLS is the establishment of transport layer security between the Client and the home network AAA server. The Client and home network AAA server MUST support version 1.1 [RFC 4346].

If user name privacy is supported, then the Client MUST send an anonymous username in the initial EAP-Response/Identity message that contains only the user's home domain information. Otherwise, the Client MUST send their user name in the initial EAP-Response/Identify message. Until the TLS tunnel is established in Phase 1, all data can be transmitted in the clear and so no unique user information is transmitted before the tunnel is established in order to provide user name privacy. The visited network AAA proxy MUST use the domain name portion of the user-name to locate the home network AAA server.

If the home network responds with an EAP Start message that includes a method other than EAP-TTLS, the Client MUST respond with a NAK and MUST set the Desired Auth Type to EAP-TTLS. The home network AAA server then MUST begin the EAP-TTLS authentication process, or it MUST reject the Client if EAP-TTLS is not supported.

In EAP-TTLS Phase 1, the home network AAA server (TTLS Server) MUST provide an [X.509] certificate to allow the Client to authenticate the home network AAA server. The Client SHOULD NOT provide credentials for the visited network AAA proxy to authenticate the Client. The Client MUST parse the server's X.509 certificate and extract the domain name of the service provider. If the domain name is not acceptable (e.g., does not match a preconfigured list of domains), the Client MUST reject the authentication. The client device MUST allow the operator to configure root authority information such that the client can authenticate the network during the EAP-TTLS process.

In EAP-TTLS Phase 2, the Client MUST provide credentials that allow the home network AAA server to authenticate the Client. Since the home network AAA server created a TLS tunnel to the Client in Phase 1, the visited network continues to transparently forward the encapsulated EAP messages in the TLS tunnel between the home network AAA server and the Client.

The visited network AAA proxy MUST support passing credentials between the Client and the home network using the EAP-TTLS specification [RFC 5281].

EAP-TTLS establishes a secure over-the-air link for passing credentials between the Client and the home network AAA server. Since the TLS tunnel exists between the Client and the home network AAA server, EAP-TTLS does not rely on special security within the visited network to protect the user credentials.

Both Client and home network AAA server SHOULD support the EAP-TTLS session resumption method per [RFC 5281]. If the home network AAA server does not support EAP-TTLS session resumption, it MUST follow normal EAP-TTLS mechanisms to reject the request and the Client MUST initiate a new EAP-TTLS session.

Upon authentication success, the home AAA server MUST send a RADIUS Access-Accept Success message to the visited network AAA proxy to authorize device admission. Upon successful authentication, the Wi-Fi AP MUST apply traffic encryption procedures with the client per [WPA]. AES is preferred. The home network AAA server MUST generate the key material that is used to encrypt the traffic and include key material in the RADIUS Access-Accept message. If the home network AAA server is unable to authenticate the Client, the home network MUST send a RADIUS Access-Reject message and the visited network MUST deny access to the Client.

6.3.2 Certificate Authentication via EAP-TLS over a Secured SSID

The following subsections include requirements to support authentication for roamers via EAP-TLS authentication. These requirements support the EAP-TLS session to be established between the client and the home network AAA server. The visited network AAA proxy passes EAP-TLS between the client and home network AAA server with RADIUS encapsulated EAP. An informative flow diagram that illustrates these requirements is found in Appendix I.

If configured to do so by the operator, the visited network Wi-Fi GW and AAA proxy MUST support EAP-TLS [RFC 5216] for MAC address and [X.509] certificate authentication. The Client, visited network Wi-Fi AP and AAA Proxy MUST support 802.1X [IEEE 802.1X] EAP authentication methods.

The Client and home network AAA MUST support TLS version 1.1 [RFC 4346].

The subscriber device MUST allow the operator to configure client X.509 certificates in the subscriber device. The subscriber device MUST allow the operator to configure root authority information such that the client can authenticate the network during the EAP-TLS process. The subscriber device SHOULD allow the operator to configure a user ID that may be anonymous, but includes a home network realm. The realm can be used by the visited network to route AAA requests to the home network.

If user name privacy is supported, the Client MUST send an anonymous username in the initial EAP-Request/Identity message that contains only the subscriber's home domain information. The visited network AAA proxy MUST use the home network realm to locate the home network AAA server. The visited network AAA proxy MUST encapsulate the EAP Request/Identity message in a RADIUS Access-Request message to be sent to home AAA server per [RFC 3579]. If the home AAA server decides to initiate EAP-TLS, it MUST initiate the EAP-TLS sequence messages to the client per [RFC 5216] and encapsulate these EAP messages in RADIUS for transport to the visited network AAA proxy.

The home network AAA MUST provide an X.509 certificate. The Client MUST parse the server's X.509 certificate and extract the domain name of the service provider. If the domain name is not acceptable (e.g., does not match a preconfigured list of domains), the Client MUST reject the authentication. The client device MUST allow the operator to configure root authority information such that the client can authenticate the network during the EAP-TLS process.

The Client MUST provide an [X.509] certificate to the home network AAA server that allows the home network AAA server to authenticate the Client per [RFC 5216].

The visited network AAA proxy MUST support interoperability between EAP-TLS [RFC 5216] messages over [IEEE 802.1X] with the visited network to EAP-TLS messages encapsulated within RADIUS with the home network AAA server per [RFC 3579].

Upon authentication success, the home AAA server MUST send a RADIUS Access-Success message to the visited network AAA proxy to authorize device admission. The home AAA server MUST include a master key for traffic encryption in the visited network. If the visited network AAA proxy receives the master key from the home AAA server, the Wi-Fi GW MUST apply traffic encryption procedures with the client per [WPA] as provisioned by the operator. AES encryption is recommended.

6.4 Session Termination

The visited network Access GW MUST detect a session end due to a session time out:

- per the smaller time period of a visited network session time out or home network session timeout provided by the home network per [RFC 2865] upon successful authentication, or,
- the session time out value provided by the home network per [RFC 2865] upon successful authentication.

The visited network Access GW MUST detect a session end when due to an idle time out:

- per the smaller time period of a visited network inactivity time out or home network inactivity time out provided by the home network per [RFC 2865] upon successful authentication, or
- the idle time out value provided by the home network per [RFC 2865] upon successful authentication.

The visited network Access GW MUST detect a session end when the subscriber device fails to request a renewal of the assigned IP address.

The visited network Access GW MUST detect a session end upon an explicit request from the home network via a RADIUS Change of Authorization (CoA) or Disconnect request per [RFC 3576].

6.5 Location Reports

The roaming architecture supports location reports for use by the visited or home network for the sake of location based services, location dependant subscriber access and location dependent charging. This section focuses on location reports from the visited to the home network for roaming subscribers. The visited network SHOULD report the location of the Wi-Fi GW servicing the roaming subscriber device to the home network (1) upon authentication request and (2) upon subscriber device transitions among Wi-Fi GWs as the device moves. The format of the location attributes are defined in Section 6.8.

The visited network AAA proxy MUST send the location of the Wi-Fi GW that is currently serving the Client in all Accounting-Request messages and MUST send an Accounting-Request message to the home network AAA server every time that the Client moves to a new Wi-Fi GW location.

The visited network AAA proxy MUST use [RFC 5580] based location reporting. Note that the location may be determined by other network components in the network, such as the Wi-Fi GW or a GW controller, which is outside the scope of the specification. This specification requires that any location reports between the visited network AAA proxy to home network AAA server are compliant with [RFC 5580].

It is recommended the Location ID in location Attribute Value Pairs (AVP)s indicate the embedded Cable Modem (eCM) address.

6.5.1 RFC5580 Location Reporting

[RFC 5580] location reporting is the default location reporting mechanism.

[RFC 5580] defines RADIUS attributes to be used for location reporting. If RFC 5580 location reporting is used, the visited network AAA proxy MUST support the rules and procedures specified in [RFC 5580].

Location information is required to be transmitted in accounting messages. If there is an out-of-band agreement between the home and visited networks (such as a roaming agreement to implement location reporting per [RFC 5580]), then the visited network AAA proxy MUST report the location of the AP being used to serve the subscriber in the Access-Request message to the AAA home server. If there is not an out-of-band agreement between the home and visited networks to implement [RFC 5580] location reporting, the home network AAA server MUST include the Requested-Location-Info attribute and MAY include the Basic-Location-Policy-Rules and Extended-Location-Policy-Rules attributes in the Access-Accept message that concludes the authentication session. The home AAA server MAY request location in an Access-Challenge.

The visited network AAA proxy MUST include the [RFC 5580] attributes in the Accounting-Request messages (start, stop, and interim) that are sent to the home AAA server.

6.6 Post-Login Redirection

If a Redirection URL is provided by the home network, the visited network Wi-Fi GW MUST send a redirect the Client's browser to that URL at the conclusion of the authentication session. The network element selected by the network operator to invoke and generate the redirection message is outside the scope of this document.

If access is granted via a Wi-Fi GW that is provisioned to operate as an enterprise GW, then the Wi-Fi GW MUST redirect the Client to a local enterprise web page upon successful completion of the authentication process.

6.7 Accounting

This section specifies accounting requirements on the interface between the visited and the home network. The methods of usage data collection in the visited network and how it is used in the visited and home network are outside the scope of this section. The accounting data needs to be sufficient to support the home network to bill the client for service while it is roaming. Furthermore, the accounting data reports may need to support different Internetwork revenue agreements between the network operators.

The visited network AAA proxy reports offline charging data to the home AAA server. Offline charging reports support post-paid subscriptions in which the data reported does not affect subscriber service in real time. The reported data includes the device MAC address, session time duration, volume usage and location reports at the end of a session.

To meet the needs discussed above, the following accounting requirements apply:

1. The visited network AAA proxy MUST use RADIUS accounting per [RFC 2866], [RFC 2869], and [RFC 5080] to transfer accounting data to the home network. See Section 6.8.3 for RADIUS attribute requirements.
2. The visited network AAA proxy and the home network AAA server MUST support off-line charging. Off-line charging refers to charging and accounting requirements that do not affect, in real-time, the service rendered to the subscriber.
3. Since the visited network AAA proxy may not have access to an authenticated User-name or Calling/Called-Station-ID, the RADIUS Class attribute per [RFC 2865] or the Chargeable User Identity (CUID) per [RFC 4372] will be used to allow the home network AAA server to correlate accounting records with the newly completed authentication session. Either the Class attribute or the CUID is used as described below.

- a. If required by roaming agreement, the home network AAA server **MUST** send a unique Class attribute in the Access-Accept message. If the visited network AAA proxy receives a Class attribute from the home AAA server, the visited network AAA proxy **MUST** include the unmodified Class attribute in all Accounting-Request messages (start, stop, and interim).
 - b. If required by roaming agreement, the home network AAA server **MUST** send a unique CUID attribute in the Access-Accept message. If the visited network AAA proxy receives a CUID attribute from the home AAA server, the visited network AAA proxy **MUST** include the CUID attribute in all Accounting-Request messages (start, stop, and interim).
4. In addition to the username or device identifiers used for authentication and device authorization, the visited network AAA proxy **MUST** include the MAC address of the AP, the MAC address of the subscriber device if available, AP location and IP address in usage reports, as required to meet regulatory and fraud detection needs. The visited network AAA proxy **MUST** send interim reports to update AP location when the subscriber device moves among Wi-Fi GWs. The accounting records need to be capable of storing this additional information.
 5. The location of the Wi-Fi GW serving the Client **MUST** be included in all Accounting-Request messages sent by the visited network AAA proxy to the home network AAA server.
 6. The visited network AAA proxy **MUST** provide the session start date and time in a start accounting request to the home AAA server.
 7. The visited network AAA **MUST** report a stop accounting request to the home AAA server when the session ends as specified in Section 6.4.
 8. The visited network AAA proxy **MUST** provide the volume of subscriber data transported.
 9. Interim usage reports **SHOULD** be generated periodically based on a reporting time period sent from the home network in RADIUS attributes per [RFC 2869]. For long duration data sessions, it is recommended interim records be created at least once per day. Interim reports may also be generated when large traffic volume thresholds are exceeded and when a subscriber device changes AP location.
 10. If an internal counter exceeds its maximum value before an interim data record would be created, the visited network AAA proxy **MUST** generate an additional interim record and the counter **MUST** be restarted.
 11. Since interim and stop RADIUS records are cumulative, if a data value will exceed the maximum size that the visited network is able to store, the visited network AAA proxy **MUST** follow a stop record by creating a start record to continue billing for the session per [RFC 2869] and [RFC 5080].
 12. If either the visited or home network operator uses time-of-day, day-of-week, day-of-year or other time specific billing, interim accounting records **MUST** be created and sent by the visited network AAA proxy at the time that the interval changes.
 13. The visited network AAA proxy **MUST** include a time stamp attribute in all accounting records per [RFC 2869].

If required by the roaming agreement between operators, the visited network AAA proxy **MUST** send Interim Accounting reports to the home AAA server for the following conditions:

- an interim report period indicated by the RADIUS Acct-Interim-Interval (85) attribute per [RFC 2869] sent by the home network;
- traffic volume attribute rollover;
- change in AP location.

6.8 Network to Network RADIUS Interface Requirements

6.8.1 RADIUS Interface

The WR-WiFi-5 interface resides between the visited network AAA proxy and the home network AAA server. This interface is used for authentication, device admission, and accounting. The visited network AAA proxy **MUST** transport authentication, device admission, and accounting messages to the home network AAA server via RADIUS secured by IPsec encryption per [RFC 4301]. The home network AAA server **MUST** transport authentication, device admission and accounting messages visited network AAA proxy via RADIUS secured by IPsec encryption per [RFC 4301]. Sections below illustrate the RADIUS attributes and referenced RFCs used on this interface.

6.8.2 Internetwork RADIUS Authentication Attributes

The table below lists the RADIUS attributes used for authentication and device admission. The attributes selected are designed to support multiple operational models:

- Subscriber sign in via a captive portal
- The subscriber device presents user name and password credentials via EAP-TTLS
- The subscriber device presents device certificates credentials via EAP-TLS

Attributes that are operational model dependant are indicated so in the table. Whereas the visited network AAA proxy **MUST** support the attributes for the login portal, EAP-TTLS and EAP-TLS, the home AAA server **MUST** support at least one authentication type and **MAY** support more authentication types as configured by the home network operator. The home operator selects which authentication protocols are used at the home AAA server.

The attributes listed below can be used by the home network to request service termination with the Disconnect message or a change in access conditions with the Change of Authorization (CoA) message per [RFC 3576].

The visited network AAA proxy **MUST** support the message types and mandatory attributes listed in Table 2, Table 3, and Table 4 per the procedures in [RFC 2865], [RFC 3576], and [RFC 3580] for authentication, device admission and session termination.

The home network AAA server **MUST** support the message types and mandatory attributes listed in Table 2, Table 3, and Table 4 per the procedures in [RFC 2865], [RFC 3576], and [RFC 3580] for authentication, device admission and session termination

The visited network AAA proxy **MAY** support the optional attributes listed in Table 2, Table 3, and Table 4 per the procedures in [RFC 2865], [RFC 3576], and [RFC 3580] for authentication, device admission and session termination.

The home network AAA server **MAY** support the optional attributes listed in Table 2, Table 3, and Table 4 per the procedures in [RFC 2865], [RFC 3576], and [RFC 3580] for authentication, device admission and session termination.

The type values in the following tables are taken from RFC unless otherwise indicated.

Table 2 - RADIUS Authentication Attributes: Request and Challenge

Attribute Name	Type	Description from [RFC 2548], [RFC 2865], [RFC 3576], [RFC 3579], [RFC 3580], [RFC 4372], and [RFC 5580]	Access Request			Access Challenge		
			Login	EAP-TTLS	EAP-TLS	Login	EAP-TTLS	EAP-TLS
User-Name	1	This Attribute indicates the name of the user to be authenticated.	MUST	MUST	MUST	-	-	-
User-Password	2	This Attribute indicates the password of the user to be authenticated, or the user's input following an Access Challenge.	MUST	-	-	-	-	-
CHAP-Password	3	This Attribute indicates the response value provided by a Challenge-Handshake Authentication Protocol (CHAP) user in response to the challenge.	MUST	MUST be used for CHAPv2 within EAP-TTLS	-	-	-	-
NAS-IP-Address	4	This Attribute indicates the identifying IP Address of the NAS which is requesting authentication of the user.	MUST be present if NAS-Identifier is not present	MUST be present if NAS-Identifier is not present	MUST be present if NAS-Identifier is not present	-	-	-
NAS-Port	5	This Attribute indicates the physical port number of the NAS which is authenticating the user. Note: This is using "port" in its sense of a physical connection on the NAS, not in the sense of a TCP or UDP port number.	MUST	MUST	MUST	-	-	-
Service Type	6	This Attribute indicates the type of service the user has requested, or the type of service to be provided. This is set to 'login'.	MUST	MUST	MUST	-	-	-
Framed-Protocol	7	This Attribute indicates the framing to be used for framed access.	MAY	MAY	MAY	-	-	-
Framed-MTU	12	Frame-MTU sets the max Maximum Transmission Unit (MTU) size and is recommended to be used when transferring EAP within RADIUS since packet sizes with EAP may exceed some AAA proxy to home AAA link MTUs.	MAY	MAY	MAY	-	-	-
Reply-Message	18	This Attribute indicates text which MAY be displayed to the user. When used in an Access-Accept, it is the success message. When used in an Access-Reject, it is the failure message. When used in an Access-Challenge, it MAY indicate a dialog message to prompt the user for a response.	-	-	-	MAY	MAY	MAY

Attribute Name	Type	Description from [RFC 2548], [RFC 2865], [RFC 3576], [RFC 3579], [RFC 3580], [RFC 4372], and [RFC 5580]	Access Request			Access Challenge		
			Login	EAP-TTLS	EAP-TLS	Login	EAP-TTLS	EAP-TLS
Class	25	This Attribute is available to be sent by the server to the client in an Access-Accept. It MUST be sent unmodified by the client to the accounting server as part of the Accounting-Request packet. The client MUST NOT interpret the attribute locally.	-	-	-	-	-	-
MS-MPPE-Send-Key	26/ 16	MS vendor specific attribute contains a session key for use by the Microsoft Point-to-Point Encryption Protocol (MPPE). This key is intended for encrypting packets sent from the NAS to the remote host.	-	-	-	-	-	-
MS-MPPE-Recv-Key	26/ 17	MS vendor specific attribute contains a session key for use by the Microsoft Point-to-Point Encryption Protocol (MPPE). This key is intended for encrypting packets received by the NAS from the remote host.	-	-	-	-	-	-
Session-Time-Out	27	This Attribute from the home network requests the maximum number of seconds of service to be provided to the user before termination of the session or prompt. (Value of 120 minutes is recommended.)	-	-	-	MAY	MAY	MAY
Idle-Timeout	28	This Attribute from the home network requests the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt (A value of 20 minutes is recommended.)	-	-	-	MAY	MAY	MAY
Calling-Station-ID	31	For IEEE 802.1X Authenticators, this attribute can be used to store the Supplicant MAC address in ASCII format (upper case only). This attribute MUST be set to the MAC address seen on the device air interface.	MUST	MUST	MUST	-	-	-
NAS-Identifier	32	This Attribute contains a string identifying the NAS originating the Access-Request. The format MUST be the fully qualified domain name of the NAS.	MUST be present if NAS-IP address is not present	MUST be present if NAS-IP address is not present	MUST be present if NAS-IP address is not present	-	-	-

Attribute Name	Type	Description from [RFC 2548], [RFC 2865], [RFC 3576], [RFC 3579], [RFC 3580], [RFC 4372], and [RFC 5580]	Access Request			Access Challenge		
			Login	EAP-TTLS	EAP-TLS	Login	EAP-TTLS	EAP-TLS
Acct-Session-Id	44	This attribute is a unique Accounting ID to make it easy to match start and stop records in a log file. If sent in the Access-Request, then the same value MUST be used in the Accounting-Request messages.	MAY	MAY	MAY	-	-	-
Event-Time-Stamp	55	Time the event or message was generated.	MUST	MUST	MUST			
CHAP-Challenge	60	This Attribute contains the CHAP Challenge sent by the NAS to a PPP Challenge-Handshake Authentication Protocol (CHAP) user.	MUST	MUST be used for CHAPv2 within EAP-TTLS	-	-	-	-
NAS-Port-Type	61	This Attribute indicates the type of the physical port of the NAS which is authenticating the user. For example, value = 19 indicates 802.11 and value =17 indicates cable.	MAY	MAY	MAY	-	-	-
EAP Message	79	The EAP-Message attribute is used to encapsulate EAP packets for transmission from the IEEE 802.1X Authenticator to the Authentication Server.	-	MUST	MUST	-	MUST	MUST
Message-Authenticator	80	The Message-Authenticator attribute MUST be used to protect packets within a RADIUS/EAP conversation.	-	MUST	MUST	-	MUST	MUST
Chargeable-User-Identity	89	Requests that the home AAA server provide a Chargeable User Identity in the Access-Accept.	MAY	MAY	MAY	-	-	-
Error-cause	101	It is possible that the NAS cannot honor Disconnect-Request or CoA-Request messages for some reason. The Error-Cause Attribute provides more detail on the cause of the problem. Values between 200-299 represent successful completion and MAY be sent in the CoA or Disconnect ACK.	-	-	-	-	-	-
Operator-Name [RFC 5580]	126	This attribute carries the operator namespace identifier and the operator name.	MUST when agreed out-of-band	MUST when agreed out-of-band	MUST when agreed out-of-band	-	-	-
Location-Information [RFC 5580]	127	Provides meta-data about the location information, such as sighting time, time-to-live, location-determination method, etc.	MUST when agreed out-of-band	MUST when agreed out-of-band	MUST when agreed out-of-band	-	-	-
Location-Data [RFC 5580]	128	Location data in either the Civic Location or the Geospatial Location format.	MUST when agreed out-of-band	MUST when agreed out-of-band	MUST when agreed out-of-band	-	-	-

The Phase 1 roaming architecture includes the options of EAP-TLS and EAP-TTLS between the mobile client and the home AAA server. In this scenario, the visited network AAA needs to retrieve the keying material from the home AAA server to help establish encryption over the air between the client and the visited network. The MS-MPPE attributes (Send and Recv) per [RFC 2548] are listed here for this purpose.

It is recommended the Location ID location AVPs indicate the eCM address.

Table 3 - RADIUS Authentication Attributes: Accept and Reject

Attribute Name	Type	Description from [RFC 2548], [RFC 2865], [RFC 3576], [RFC 3579], [RFC 3580], [RFC 4372], and [RFC 5580]	Access Accept			Access Reject		
			login	EAP-TTLS	EAP-TLS	login	EAP-TTLS	EAP-TLS
User-Name	1	This Attribute indicates the name of the user to be authenticated.	MAY	MAY	MAY	-	-	-
User-Password	2	This Attribute indicates the password of the user to be authenticated, or the user's input following an Access Challenge.	-	-	-	-	-	-
CHAP-Password	3	This Attribute indicates the response value provided by a Challenge-Handshake Authentication Protocol (CHAP) user in response to the challenge.	-	-	-	-	-	-
NAS-IP-Address	4	This Attribute indicates the identifying IP Address of the NAS which is requesting authentication of the user.	-	-	-	-	-	-
NAS-Port	5	This attribute indicates the physical port number of the NAS which is authenticating the user.	-	-	-	-	-	-
Service Type	6	This Attribute indicates the type of service the user has requested, or the type of service to be provided. This is set to 'login'.	MAY	MAY	MAY	-	-	-
Framed-Protocol	7	This Attribute indicates the framing to be used for framed access.	MAY	MAY	MAY	-	-	-
Framed-MTU	12	Frame-MTU sets the max MTU size and is recommended to be used when transferring EAP within RADIUS since packet sizes with EAP may exceed some AAA proxy to home AAA link MTUs.	MAY	MAY	MAY	-	-	-
Reply-Message	18	This Attribute indicates text which MAY be displayed to the user. When used in an Access-Accept, it is the success message. When used in an Access-Reject, it is the failure message. When used in an Access-Challenge, it MAY indicate a dialog message to prompt the user for a response.	MAY	MAY	MAY	MUST	MUST	MUST

Attribute Name	Type	Description from [RFC 2548], [RFC 2865], [RFC 3576], [RFC 3579], [RFC 3580], [RFC 4372], and [RFC 5580]	Access Accept			Access Reject		
			login	EAP-TTLS	EAP-TLS	login	EAP-TTLS	EAP-TLS
Class	25	This Attribute is available to be sent by the server to the client in an Access-Accept. It MUST be sent unmodified by the client to the accounting server as part of the Accounting-Request packet. The client MUST NOT interpret the attribute locally.	MUST	MUST	MUST	-	-	-
MS-MPPE-Send-Key	26/ 16	MS vendor specific attribute contains a session key for use by the Microsoft Point-to-Point Encryption Protocol (MPPE). This key is intended for encrypting packets sent from the NAS to the remote host.	-	-	MUST	-	-	-
MS-MPPE-Recv-Key	26/ 17	MS vendor specific attribute contains a session key for use by the Microsoft Point-to-Point Encryption Protocol (MPPE). This key is intended for encrypting packets received by the NAS from the remote host.	-	-	MUST	-	-	-
Session-Time-Out (A value of 120 minutes is recommended)	27	This Attribute from the home network requests the maximum number of seconds of service to be provided to the user before termination of the session or prompt.	MUST	MUST	MUST	-	-	-
Idle-Timeout (A value of 20 minutes is recommended)	28	This Attribute from the home network requests the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt.	MUST	MUST	MUST	-	-	-
Termination-Action	29	This Attribute indicates what action the NAS should take when the specified service is completed. This can be used to instruct the client to attempt a re-authentication or an access-request.	MAY	MAY	MAY	-	-	-
Calling-Station-ID	31	For IEEE 802.1X Authenticators, this attribute can be used to store the Supplicant MAC address in ASCII format (upper case only).	-	-	-	-	-	-
NAS-Identifier	32	This Attribute contains a string identifying the NAS originating the Access-Request. The format MUST be the fully qualified domain name of the NAS.	-	-	-	-	-	-
Acct-Session-ID	44	This attribute is a unique Accounting ID. If sent in the Access-Request, then the same value MUST be used in the Accounting-Request.	-	-	-	-	-	-
Event-Time-Stamp	55	Time the event or message was generated.	-	-	-	-	-	-

Attribute Name	Type	Description from [RFC 2548], [RFC 2865], [RFC 3576], [RFC 3579], [RFC 3580], [RFC 4372], and [RFC 5580]	Access Accept			Access Reject		
			login	EAP-TTLS	EAP-TLS	login	EAP-TTLS	EAP-TLS
CHAP-Challenge	60	This Attribute contains the CHAP Challenge sent by the NAS to a PPP Challenge-Handshake Authentication Protocol (CHAP) user.	-	-	-	-	-	-
NAS-Port-Type	61	This Attribute indicates the type of the physical port of the NAS which is authenticating the user. For example, value = 19 indicates 802.11 and value = 17 indicates cable.	-	-	-	-	-	-
EAP Message	79	The EAP-Message attribute is used to encapsulate EAP packets for transmission from the IEEE 802.1X Authenticator to the Authentication Server.	-	MUST when EAP is invoked	MUST when EAP is invoked	-	MUST when EAP is invoked	MUST when EAP is invoked
Message-Authenticator	80	The Message-Authenticator attribute MUST be used to protect packets within a RADIUS/EAP conversation.	-	MUST when EAP is invoked	MUST when EAP is invoked	-	MUST when EAP is invoked	MUST when EAP is invoked
Acct-Interim-Interval	85	This attribute indicates the number of seconds between each interim update in seconds for this specific session.	MUST if accounting is supported	MUST if accounting is supported	MUST if accounting is supported	-	-	-
Chargeable-User-Identity	89	The home AAA server provides a Chargeable User Identity that the client and use to correlate accounting requests.	MUST if present in Access-Request	MUST if present in Access-Request	MUST if present in Access-Request	-	-	-
Error-cause	101	It is possible that the NAS cannot honor Disconnect-Request or CoA-Request messages for some reason. The Error-Cause Attribute provides more detail on the cause of the problem. Values between 200-299 represent successful completion and MAY be sent in the CoA or Disconnect ACK.	-	-	-	-	-	-
Requested-Location-Info ([RFC 5580] location reporting option)	132	Allows the RADIUS server to indicate which location information about which entity it wants to receive. It MUST be transmitted if location is required and there is no agreed out-of-band mandate to transfer the location information.	MUST (see comment)	MUST (see comment)	MUST (see comment)	-	-	-
Basic-Location-Policy-Rules ([RFC 5580] location reporting option)	129	Policy rules control the distribution of location information.	MAY	MAY	MAY	-	-	-
Extended-Location-Policy-Rules ([RFC 5580] location reporting option)	130	Contains a URI that indicates where the richer rule set can be found.	MAY	MAY	MAY	-	-	-

Table 4 - RADIUS Authentication Attributes: CoA and Disconnect

Attribute Name	Type	Description from [RFC 2548], [RFC 2865], [RFC 3576], [RFC 3579], [RFC 3580], [RFC 4372], and [RFC 5580]	CoA or Disconnect Request			CoA or Disconnect ACK/NAK		
			login	EAP-TTLS	EAP-TLS	login	EAP-TTLS	EAP-TLS
User-Name	1	This Attribute indicates the name of the user to be authenticated.	MUST	MUST	MUST	-	-	-
User-Password	2	This Attribute indicates the password of the user to be authenticated, or the user's input following an Access Challenge.	-	-	-	-	-	-
CHAP-Password	3	This Attribute indicates the response value provided by a Challenge-Handshake Authentication Protocol (CHAP) user in response to the challenge.	-	-	-	-	-	-
NAS-IP-Address	4	This Attribute indicates the identifying IP Address of the NAS which is requesting authentication of the user.	MAY	MAY	MAY	-	-	-
NAS-Port	5	This Attribute indicates the physical port number of the NAS which is authenticating the user. Note: This is using "port" in its sense of a physical connection on the NAS, not in the sense of a TCP or UDP port number.	-	-	-	-	-	-
Service Type	6	This Attribute indicates the type of service the user has requested, or the type of service to be provided. This is set to 'login'.	MAY	MAY	MAY	MAY	MAY	MAY
Framed-MTU	12	Frame-MTU sets the max MTU size and is recommended to be used when transferring EAP within RADIUS since packet sizes with EAP may exceed some AAA proxy to home AAA link MTUs.	MAY	MAY	MAY	-	-	-
Reply-Message	18	This Attribute indicates text which MAY be displayed to the user. When used in an Access-Accept, it is the success message. When used in an Access-Reject, it is the failure message. When used in an Access-Challenge, it MAY indicate a dialog message to prompt the user for a response.	MAY	MAY	MAY	-	-	-
MS-MPPE-Send-Key	26/ 16	MS vendor specific attribute contains a session key for use by the Microsoft Point-to-Point Encryption Protocol (MPPE). This key is intended for encrypting packets sent from the NAS to the remote host.	-	-	-	-	-	-
MS-MPPE-Recv-Key	26/ 17	MS vendor specific attribute contains a session key for use by the Microsoft Point-to-Point Encryption Protocol (MPPE). This key is intended for encrypting packets received by the NAS from the remote host.	-	-	-	-	-	-
Session-Time-Out (A value of 120 minutes is recommended)	27	This Attribute from the home network requests the maximum number of seconds of service to be provided to the user before termination of the session or prompt.	MAY	MAY	MAY	-	-	-

Attribute Name	Type	Description from [RFC 2548], [RFC 2865], [RFC 3576], [RFC 3579], [RFC 3580], [RFC 4372], and [RFC 5580]	CoA or Disconnect Request			CoA or Disconnect ACK/NAK		
			login	EAP-TTLS	EAP-TLS	login	EAP-TTLS	EAP-TLS
Idle-Timeout (A value of 20 minutes is recommended)	28	This Attribute from the home network requests the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt.	MAY	MAY	MAY	-	-	-
Calling-Station-ID	31	For IEEE 802.1X Authenticators, this attribute can be used to store the Supplicant MAC address in ASCII format (upper case only). For user login, this is set to the device MAC address seen on the air interface.	MAY	MAY	MAY	-	-	-
NAS-Identifier	32	This Attribute contains a string identifying the NAS originating the Access-Request. The format MUST be the fully qualified domain name of the NAS.	MAY	MAY	MAY	-	-	-
Acct-Session-ID	44	This attribute is a unique Accounting ID to make it easy to match start, interim and stop records in a log file.	MAY	MAY	MAY	-	-	-
Event-Time-Stamp	55	Time the event or message was generated.	MUST	MUST	MUST	-	-	-
CHAP-Challenge	60	This Attribute contains the CHAP Challenge sent by the NAS to a PPP Challenge-Handshake Authentication Protocol (CHAP) user.	-	-	-	-	-	-
NAS-Port-Type	61	This Attribute indicates the type of the physical port of the NAS which is authenticating the user. For example, value = 19 indicates 802.11 and value =17 indicates cable	MAY	MAY	MAY	-	-	-
EAP Message	79	The EAP-Message attribute is used to encapsulate EAP packets for transmission from the IEEE 802.1X Authenticator to the Authentication Server.	-	MAY	MAY	-	MAY	MAY
Message-Authenticator	80	The Message-Authenticator attribute MUST be used to protect packets within a RADIUS/EAP conversation.	-	MAY	MAY	-	MAY	MAY
Error-cause	101	It is possible that the NAS cannot honor Disconnect-Request or CoA-Request messages for some reason. The Error-Cause Attribute provides more detail on the cause of the problem. Values between 200-299 represent successful completion and MAY be sent in the CoA or Disconnect ACK.	-	-	-	MAY	MAY	MAY
Requested-Location-Info ([RFC 5580] location reporting option)	132	Allows the RADIUS server to indicate which location information about which entity it wants to receive.	MAY	MAY	MAY	-	-	-
Basic-Location-Policy-Rules ([RFC 5580] location reporting option)	129	Policy rules control the distribution of location information.	MAY	MAY	MAY	-	-	-

Attribute Name	Type	Description from [RFC 2548], [RFC 2865], [RFC 3576], [RFC 3579], [RFC 3580], [RFC 4372], and [RFC 5580]	CoA or Disconnect Request			CoA or Disconnect ACK/NAK		
			login	EAP-TTLS	EAP-TLS	login	EAP-TTLS	EAP-TLS
Extended-Location-Policy-Rules ([RFC 5580] location reporting option)	130	It contains a URI that indicates where the richer rule set can be found.	MAY	MAY	MAY	-	-	-
Redirection-URL ([RFC 5580] location reporting option)	26/14122, 4	Returned by the home network upon a successful authentication attempt by a roaming customer, containing the URL of a post-login "welcome" page to present to the user.	MAY	MAY	MAY	-	-	-

6.8.3 Internetwork RADIUS Accounting Attributes

Standard RADIUS attributes have been defined for accounting. These are in addition to the various AVPs that are defined for authorization and authentication. In addition to the RADIUS accounting attributes specified below, User-Name and Calling-Station-ID AVPs **MUST** per [RFC 2865] be included in the Accounting Request. Furthermore, an Accounting-Request **MUST** contain either a NAS-IP-Address or a NAS-Identifier (or both) per [RFC 2865]. Table 5 below lists the attributes and specifies which the visit network needs to support for accounting messages. The attributes are selected to provide time duration and volume accounting reporting, and allow for interim reports as needed.

The visited network AAA proxy and the home network AAA server **MUST** support the message types and mandatory attributes listed in Table 5, per the procedures in [RFC 2866] and [RFC 2869] for accounting.

The visited network AAA proxy and the home network AAA server **MAY** support the optional attributes listed in Table 5 per the procedures in [RFC 2866] and [RFC 2869] for accounting.

The Wi-Fi GW and the visited network AAA proxy may use vendor specific attributes in the RADIUS accounting messages that are transmitted within the visited network. The visited network AAA proxy **SHOULD NOT** include vendor specific attributes in the RADIUS accounting messages that are transmitted between the visited network AAA proxy and the home network AAA server.

The Class attribute is used to correlate an accounting session with an authentication session. The User-Name, Calling-Station-ID and Called-Station-ID that are known in the visited network will not be authenticated. The home network AAA server can not rely on the validity of these attributes in the accounting record. Based upon the operator's roaming agreement, the home network AAA server **MUST** send the Class attribute in the Access-Accept message per [RFC 2865] and the visited network AAA proxy **MUST** include the received Class attribute value in the Accounting-Request messages.

The CUID is an alternative to the Class Attribute used to correlate an accounting session with an authentication session. The home AAA server **MUST** send the CUID in an Access-Accept if the CUID is requested in the Access-Request per [RFC 5580]. The visited AAA proxy **MUST** include the CUID value received in the Access-Accept in Accounting-Request messages.

Location information is mandatory in all Accounting-Request messages and so the visited network AAA proxy **MUST** include the [RFC 5580] location parameters in all Accounting-Request message for a single Acct-Session-ID.

Table 5 - RADIUS Accounting Attributes

Attribute Name	Type	Description from [RFC 2866], [RFC 2869], [RFC 4372], and [RFC 5580]	Request
Class	25	This Attribute is available to be sent by the server to the client in an Access-Accept and MUST be sent unmodified by the client to the accounting server as part of the Accounting-Request packet if accounting is supported. The client MUST NOT interpret the attribute locally.	MUST
Acct-Status-Type	40	This attribute indicates whether this Accounting-Request marks the beginning of the user service (Start), the end (Stop), or is an interim report (Interim-Update).	MUST
Acct-Delay-Time	41	This attribute indicates how many seconds the client has been trying to send this record for.	If needed
Acct-Input-Octets	42	This attribute indicates how many octets have been received from the port over the course of this service being provided.	MUST
Acct-Output-Octets	43	This attribute indicates how many octets have been sent to the port in the course of delivering this service.	MUST
Acct-Session-Id	44	This attribute is a unique Accounting ID to make it easy to match start, interim and stop records in a log file.	MUST
Acct-Authentic	45	This attribute MAY be included in an Accounting-Request to indicate how the user was authenticated, whether by RADIUS, the NAS itself, or another remote authentication protocol.	MAY
Acct-Session-Time	46	This attribute indicates how many seconds the user has received service for.	MUST
Acct-Input-Packets	47	This attribute indicates how many packets have been received from the port over the course of this service being provided to a Framed User, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.	MAY
Acct-Output-Packets	48	This attribute indicates how many packets have been sent to the port in the course of delivering this service to a Framed User, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.	MAY
Acct-Terminate-Cause	49	This attribute indicates how the session was terminated. RFC2866 defines enumerated values, such as 1 = user request, 4 = idle time out, 5 = session time out, 10 = NAS request, etc.	MUST
Acct-Input-Gigawords	52	This attribute indicates how many times the Acct-Input-Octets counter has wrapped around 2^{32} over the course of this service being provided.	MUST
Acct-Output-Gigawords	53	This attribute indicates how many times the Acct-Output-Octets counter has wrapped around 2^{32} in the course of delivering this service.	MUST
Event-Timestamp	55	This attribute is included in an Accounting-Request packet to record the time that this event occurred on the NAS, in seconds since January 1, 1970 00:00 UTC.	MUST
Chargeable User Identity	89	This attribute is included in all Accounting-Requests in order to correlate Start, Interim and Stop records.	MUST if received in Access-Accept
Operator Name (RFC5580)	126	This attribute carries the operator namespace identifier and the operator name.	MUST
Location-Information ([RFC 5580] location reporting option)	127	Provides metadata about the location information, such as sighting time, time-to-live, location-determination method, etc.	MUST
Location-Data ([RFC 5580] location reporting option)	128	Location data in either the Civic Location or the Geospatial Location format	MUST
Basic-Location-Policy-Rules ([RFC 5580] location reporting option)	129	Policy rules control the distribution of location information.	MUST only if received in Access-Accept message

Attribute Name	Type	Description from [RFC 2866], [RFC 2869], [RFC 4372], and [RFC 5580]	Request
Extended-Location-Policy-Rules ([RFC 5580] location reporting option)	130	Contains a URI that indicates where the richer rule set can be found.	MUST only if received in Access-Accept message

Note: No attributes should be found in Accounting-Response packets.

It is recommended that that Acct-Session-ID be in the format username@operator.com-sessionstart_in_utc. It is recommended that the home and visited networks support Network Time Protocol (NTP) in a manner to support time synchronization for the sake of accurate roaming events and accounting data.

It is recommended the Location ID location AVPs indicate the eCM address.

Appendix I Informative Flows

I.1 Portal Sign via Clear SSID

The following flow diagram illustrates the use of a secure captive web portal sign in via a clear SSID. Best effort unsecured internet connectivity is provided upon successful authentication.

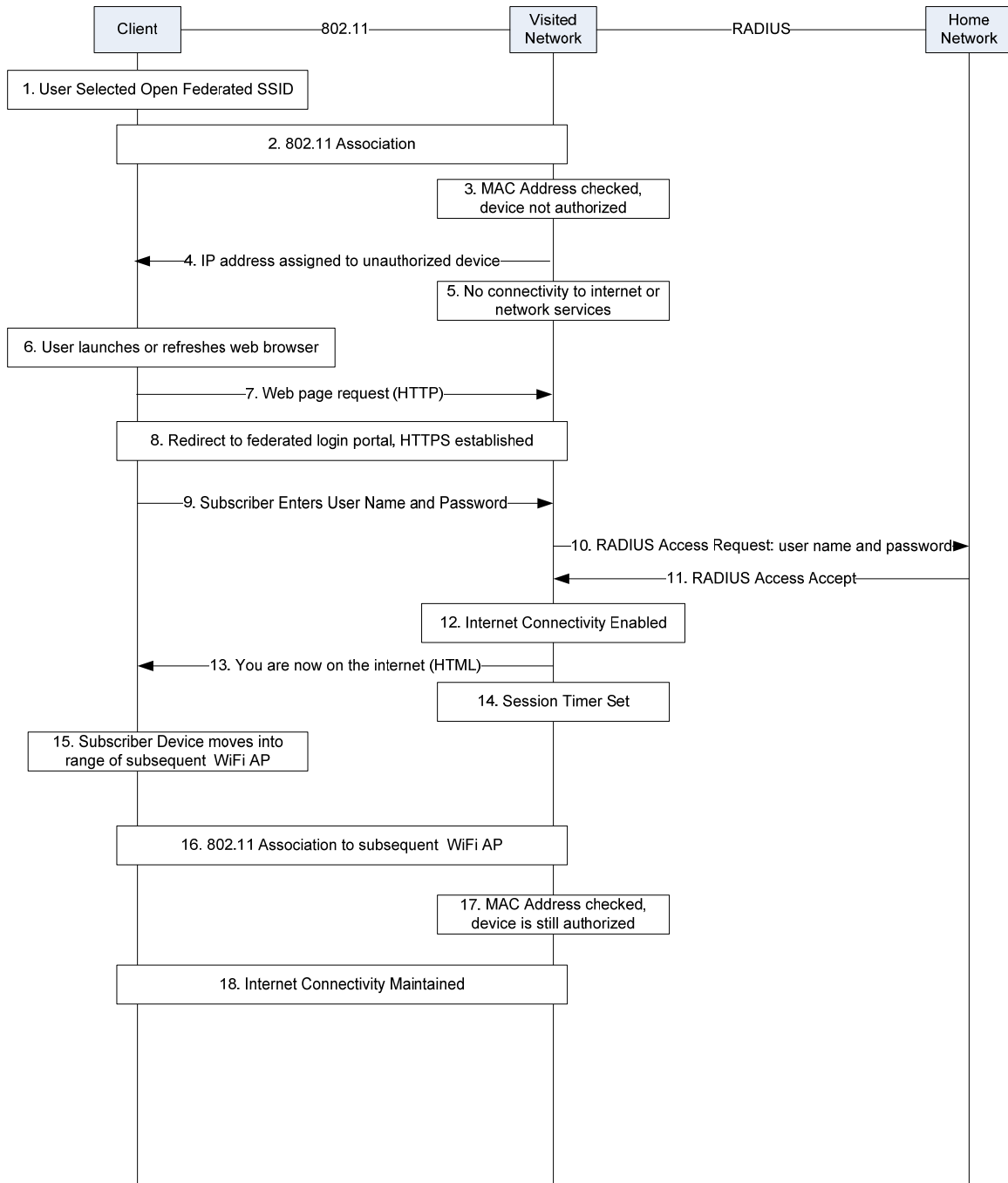


Figure 3 - Subscriber Sign In on a Captive Portal via a Clear SSID

I.2 EAP-TTLS Username/Password Authentication

In this example, EAP-TTLS is used to enable username password authentication between a client on the subscriber's device and the subscriber's home network. TTLS (Tunneled Transport Layer Security) is used to create a secure connection through the visited network to the home network to tunnel username/password authentication messages between the client and home network AAA server.

EAP-TTLS [RFC 5281] authentication begins when the 802.11 association steps have been completed. At this point, the Wi-Fi GW in visited network begins an 802.1X EAP authentication process. For EAP-TTLS, this process involves two phases. Phase 1 uses the TLS handshake protocol to authenticate the TTLS server (home network AAA server) in the home network to the client. The client and the TTLS server share keying material and agree on a TLS record layer cipher suite to secure the remaining EAP-TTLS communication messages. Since Phase 1 involves unsecure communications, the subscriber credentials are not passed to the TTLS server, only sufficient credentials (e.g., realm) to allow the visited network to locate the home network. In Phase 2, it is recommended that the subscriber and the home network AAA server perform mutual authentication. In Phase 2, the air interface is secured by the TLS tunnel established in Phase 1. The visited network acts as an EAP messaging pass through and uses EAP over RADIUS to connect to the AAA server in the home network. Since the visited network is a pass through in Phase 2, it is agnostic to the authentication method such as, Microsoft Challenge-Handshake Authentication Protocol version 2 (MSCHAPv2), Password Authentication Protocol (PAP), or Message-Digest algorithm 5 (MD5) used.

The EAP-TTLS specifications identify 4 logical functional elements that implement the EAP-TTLS authentication and security functions: Client, Access Point, TTLS Server and Home AAA server. The Access Point resides in the visited network and the TTLS Server and AAA/H Server reside in the home network in the flows shown below.

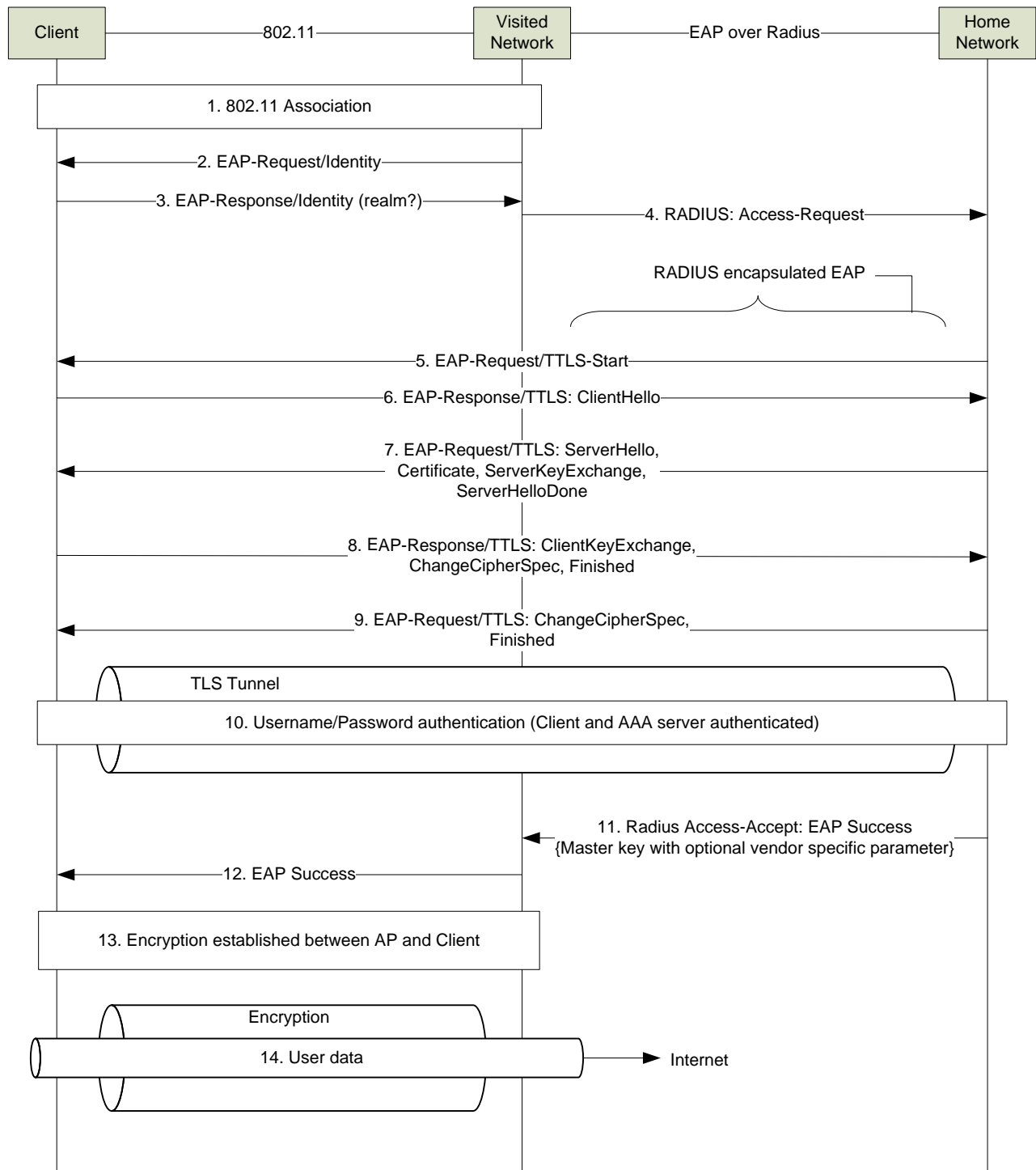


Figure 4 - Authentication with EAP-TTLS

1. The Client Station (STA) initiates normal 802.11 messaging to begin association with the SSID. During the association process, the Client STA learns that 802.1X authentication is used as the visited network AP's security policy. When this stage completes, the connection between the client and the AP is in the 802.1X Controlled Port Blocked state.

2. The AP in the visited network, following standard 802.1X authentication, sends an EAP-Request/Identity message to begin the authentication process.
3. The Client responds with an EAP-Response/Identity message. Since this messaging is still being transmitted in the clear, the identity should only include the realm and not the full username. Based on the information in the response, the Wi-Fi GW will pass this message on to the visited network AAA proxy.
4. The visited network AAA proxy uses the realm to locate the home network AAA server that will perform the EAP-TTLS server functions. It sends the EAP response encapsulated in a RADIUS Access-Request message.
5. At this point, the EAP-TTLS authentication process begins. The home network AAA server sends an EAP-TTLS/Start message that the visited network forwards to the Client. The EAP-TTLS/Start includes information to negotiate TTLS version and may include additional AVPs, such as, the server identity to allow the client to resume a prior session.

Note: The home network AAA server may not know which form of EAP processing is configured or preferred by the client and may send a start message for a different EAP method, such as, EAP-TLS. If this is the case, the Client will send an EAP-Response containing a Nak and the Desired Auth Type attribute set to EAP-TTLS. At this time, the TTLS server will send the EAP-TTLS/Start message.

6. At this point a standard TLS [RFC 4346] sequence is initiated to authenticate the home network AAA server with the client and to setup a secure path between the Client and the home network AAA server. The Client sends a response containing the TLS ClientHello message. The ClientHello contains information on supported TLS version, cipher suites, and compression methods. The visited network passes this through to the home network AAA server.
7. The home network AAA server responds with a set of TLS messages that contain the ServerHello, its X.509 certificate, a ServerKeyExchange and the ServerHelloDone. The visited network forwards this to the Client. The ServerHello has the agreed TLS version, cipher suite and compression method that will be used. The ServerKeyExchange defines the algorithm and creates the initial server key. It is expected that the server and client will support WPA at a minimum and should support WPA2 level security. The ServerKeyExchange is only sent if the X.509 certificate is for signing only.
8. After the Client has validated the certificate, the client key exchange message is sent, and the content of that message will depend on the public key algorithm selected between the client hello and the server hello. At this point, a change cipher spec message is sent by the client, and the client copies the pending Cipher Spec into the current Cipher Spec. The client then immediately sends the finished message under the new algorithms, keys, and secrets.
9. In response, the home network AAA server will send its own ChangeCipherSpec message, transfer the pending to the current Cipher Spec, and send its Finished message under the new Cipher Spec. At this point, the handshake is complete, and the client and server may begin to exchange application layer data.
10. The Client now has a secure tunnel to the home network AAA server and begins a subscriber authentication sequence. The subscriber authentication information is carried in EAP-TTLS message AVPs between the Client and the home network AAA Server. Since the visited network acts as a message pass through point, different home networks may employ different authentication mechanisms (e.g., MSCHAPv2, PAP, or MD5). See below for the case where MSCHAPv2 is used for the username/password authentication.
11. The home network AAA server distributes data connection keying information to the visited network in the message that carries the final EAP-Success indication.
12. The visited network forwards the EAP Success message to the Client.
13. At this point, the subscriber device and networks have authenticated each other and a data encryption mechanism is established between the Wi-Fi GW and the Client using the data connection keying information that was included in the EAP Success message.
14. Subscriber data is now transported between the Client and the Wi-Fi GW via an encrypted link. Within the visited network and the Internet, no encryption has been established by this process.

Step 10 in Figure 4 allows the home network AAA servers to use different mechanisms to authenticate the user after the initial TLS association is performed to create a secure tunnel to complete the user authentication. The flow shown below illustrates how MSCHAPv2 [RFC 2759] can be used by the client and the home network AAA server to allow user and home network authentication. This flow will show the EAP-TTLS messaging between the client and the visited network and the RADIUS messaging between the visited network and the home network. In the visited network, the over the air messages are protected by the TLS tunnel that has been established. Between the visited network and the home network, a form of security, such as, IPsec is used to transfer the RADIUS messages.

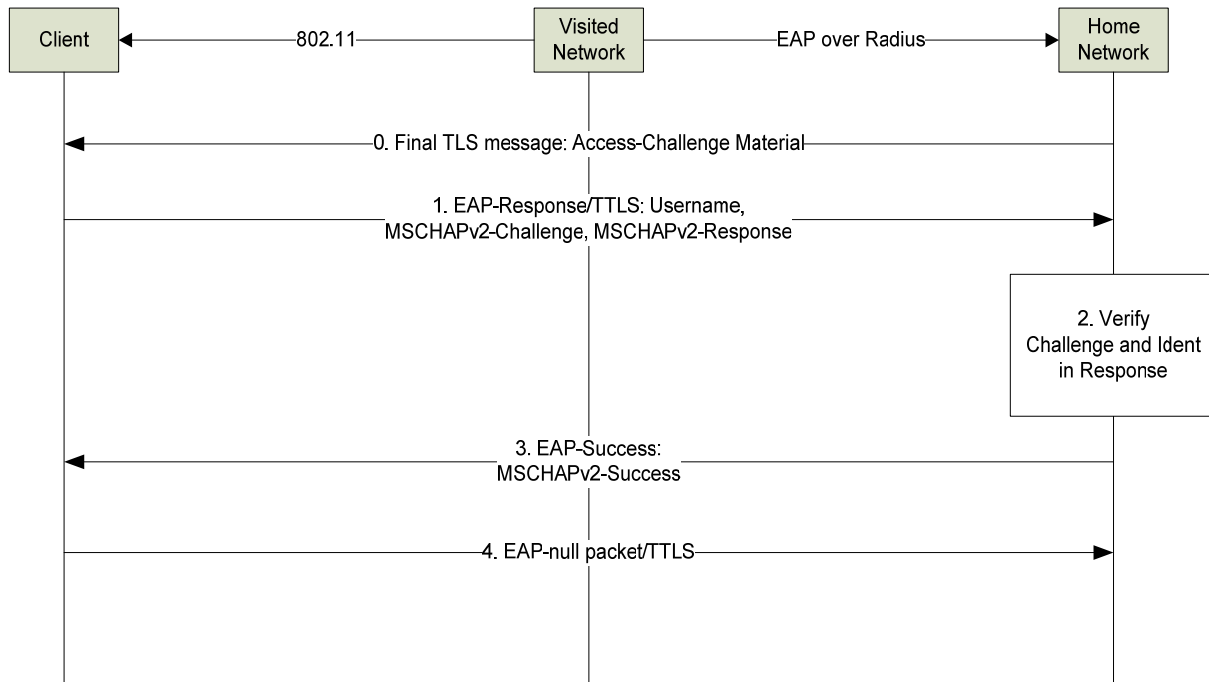


Figure 5 - MSCHAPv2 Username/Password Authentication within EAP-TTLS

0. At the final step of the TLS procedure, the home network AAA server will send challenge material to the Client. This will be used by the Client to initiate the MSCHAPv2 authentication between the Client and the Home Network AAA server.
1. The Client initiates the MSCHAPv2 authentication by sending its complete username, its MSCHAPv2 Challenge, and an MSCHAPv2 Response to the challenge materials.
2. The home network AAA server verifies the material and authenticates the user.
3. It returns a MSCHAPv2 Success message that contains the response to the challenge from the Client.
4. Once the Client has authenticated the AAA server, it sends an EAP-TTLS null packet to inform the home network AAA server that the MSCHAPv2 authentication has succeeded.

I.3 EAP-TLS Certificate Authentication

EAP-TLS is used to enable mutual authentication between a client on the subscriber's device and the authentication server through the use of X.509 certificates. The authentication server selected for the roaming architecture is the home AAA server. The client X.509 certificates may be a device certificate or a subscription certificate.

EAP-TLS [RFC 5216] authentication begins when the 802.11 association steps have been completed. At this point, the Wi-Fi GW in visited network begins an 802.1X EAP authentication process. The visited network initiates an EAP-Request Identity to the client. The client responds with an EAP-Response that includes an anonymous user name parameter with the realm of the home network. Based on the realm, the visited network knows where to route

to reach the home network AAA server. The home network AAA server determines the authentication processed used, and in this case, initiates EAP-TLS. EAP-TLS is then established directly between the client and the home network AAA. EAP-TLS packets are carried over 802.1X and 802.11 on the air interface, and then carried over RADIUS between the visited network AAA proxy and home network AAA server. (The connection between the Wi-Fi GW and the AAA proxy may be 802.1X or RADIUS.) The home AAA server authenticates the subscriber device with the certificate it receives, and the subscriber device authenticates the network with the server certificate it receives. The subscriber device is granted high speed data service to the air interface, with encryption over the air interface after the EAP authentication process is completed.

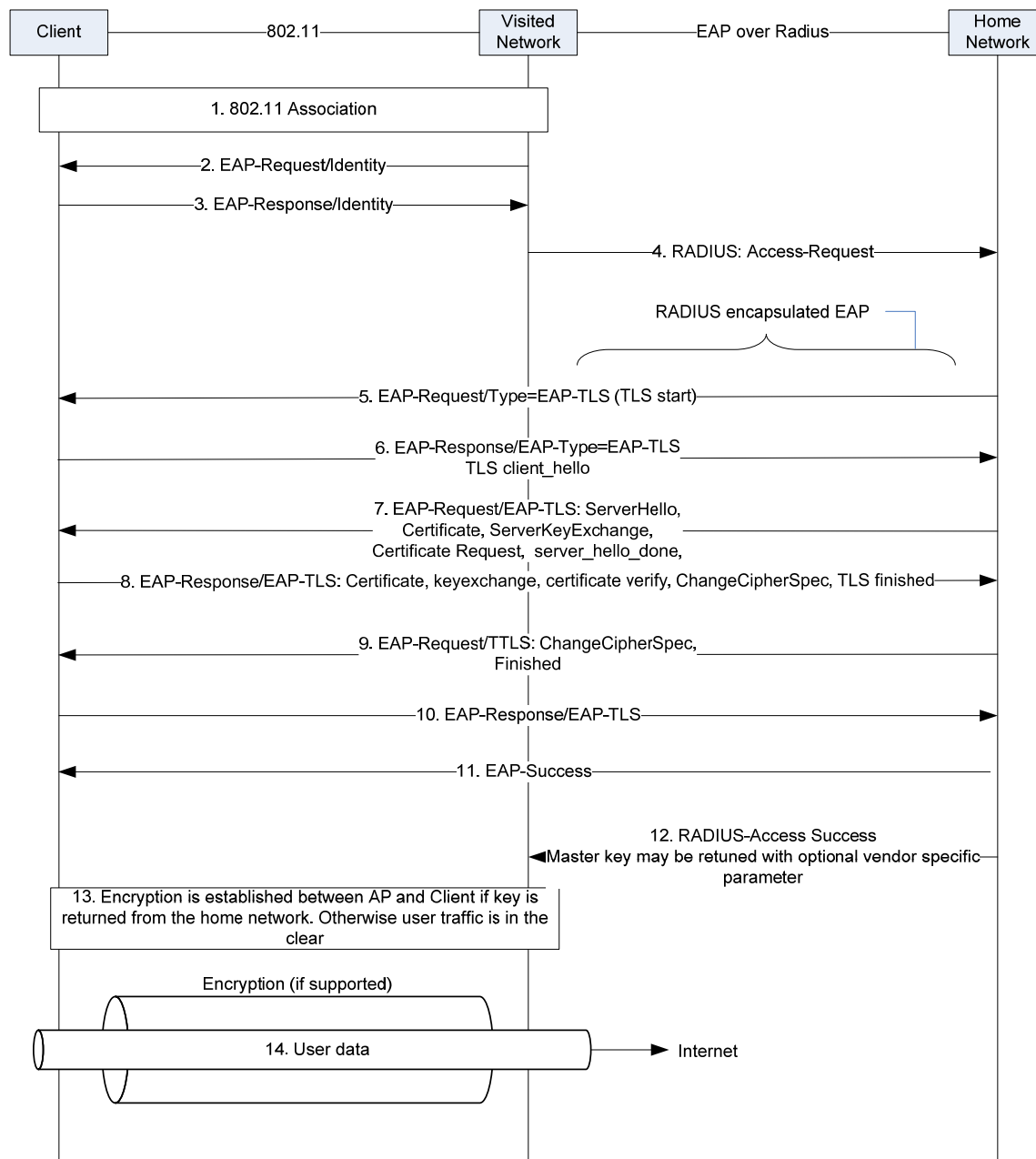


Figure 6 - Authentication within EAP-TLS

1. The Client STA initiates normal 802.11 messaging to begin association with the SSID. During the association process, the Client STA learns that 802.1X authentication is used as the visited network AP’s security policy.

When this stage completes, the connection between the client and the Wi-Fi GW is in the 802.1X Controlled Port Blocked state.

2. The Wi-Fi GW in the visited network, following standard 802.1X authentication, sends an EAP-Request/Identity message to begin the authentication process.
3. The Client responds with an EAP-Response/Identity message. Since this messaging is still being transmitted in the clear, it is recommended that the identity only include the realm and not the full username. Based on the information in the response, the AP will pass this message on to the EAP-TLS server (AAA server) in the home network.

Note: The realm is used by the visited network AAA server to locate the home network AAA server.

4. The visited network AAA proxy sends a RADIUS access-request message to the home AAA that encapsulates the EAP-Response from the client.
5. At this point, the EAP-TLS authentication process begins. The home AAA server sends an EAP-TLS/Start message that the Wi-Fi GW forwards to the Client. Messages 5 thru 11 are all passed transparently through the visited network to the Client. The visited network AAA proxy encapsulates or de-encapsulates the EAP-TLS attributes in the RADIUS messages and forwards the attributes between the home network and the Client.
6. At this point a standard TLS [RFC 4346] sequence is initiated to authenticate the AAA server with the client, and the client with the home AAA server and to setup a secure path between the Client and the AP. The Client sends a response containing the TLS ClientHello message. The ClientHello contains information on supported TLS version, cipher suites, and compression methods. The AP passes this through towards the home AAA server.
7. The home AAA server responds with a set of TLS messages that contain the ServerHello, its X.509 certificate, a ServerKeyExchange and the ServerHelloDone. The AP forwards this to the Client. The ServerHello has the agreed TLS version, cipher suite and compression method that will be used. The ServerKeyExchange defines the algorithm and creates the initial server key. It is expected that the server and client will support WPA at a minimum and should support WPA2 level security. The ServerKeyExchange is only sent if the X.509 certificate is for signing only.
8. After the Client has validated the certificate, the client key exchange message is sent which includes the client certificate to be sent to the AAA server. The content of that message will also depend on the public key algorithm selected between the client hello and the server hello. At this point, a change cipher spec message is sent by the client, and the client copies the pending Cipher Spec into the current Cipher Spec. The client then immediately sends the finished message under the new algorithms, keys, and secrets.
9. The AAA server then authenticates the client based on the certificate received. In response, the AAA server will send its own ChangeCipherSpec message, transfer the pending to the current Cipher Spec, and send its Finished message under the new Cipher Spec.
10. The client provides a final response to the AAA server.
11. The AAA server acknowledges that the EAP process is successful.
12. At this point, the handshake is complete, and the AAA server sends a RADIUS Access Success message to the visited network AAA server with standard IETF attributes. If encryption is to be supported, the home AAA server needs to return the cipher key to the visited network AAA proxy in the RADIUS Access-Accept message. Having the key retrieved from the home AAA server, the visited network is able to establish encryption over the air interface.
13. At this point the subscriber device and networks have authenticated each other. If the visited network AAA proxy receives the master key from the visited network, data encryption mechanism is established between the Wi-Fi GW and the Client.
14. Subscriber data is now transported between the Client and the Wi-Fi GW and onto the Internet via the visited network.

