Wireless Specifications

Wi-Fi Requirements for Cable Modem Gateways

WR-SP-WiFi-GW-I03-140311

ISSUED

DISCLAIMER

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. Any use or reliance on the information or opinion in this document is at the risk of the user, and CableLabs and its members shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, or utility of any information or opinion contained in the document.

CableLabs reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various entities, technology advances, or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein.

This document is not to be construed to suggest that any affiliated company modify or change any of its products or procedures, nor does this document represent a commitment by CableLabs or any of its members to purchase any product whether or not it meets the characteristics described in the document. Unless granted in a separate written agreement from CableLabs, nothing contained herein shall be construed to confer any license or right to any intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

Document Status Sheet

Document Control Number:	WR-SP-WiFi-GW-I03-140311			
Document Title:	Wi-Fi Requirements for Cable Modem Gateways			
Revision History:	I01 - Released 05/20/10 I02 – Released 02/16/12 I03 – Released 03/11/14			
Date:	March 11, 2014			
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 generally public document that has undergone Member and Technology Supplier review, cross-vendor interoperability, and is for Certification testing if applicable. Issued Specifications are subject to the Engineering Change Process.
Closed	A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs.

Trademarks

Contents

Figures

1 SCOPE

1.1 Introduction and Purpose

Wi-Fi is an increasingly pervasive technology used to deliver wireless broadband services to consumers and business customers. This specification details functional requirements for a cable operator managed Wi-Fi air interface that can be applied in residential, enterprise, and public cable modem gateways. These requirements can help enable Wi-Fi roaming among partner networks from cable operators and non-cable operators. Therefore, this specification identifies the essential capabilities for a cable modem with Wi-Fi functionality to comply with cable operator Wi-Fi roaming requirements.

Requirements are targeted at deployment scenarios that integrate an [802.11n] or later-generation Wi-Fi air interface with a [MULPI3.0] cable modem. This specification includes functional requirements for device management. The protocol definition for management is outside the scope of this specification.

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. As applied to this specification, requirements signified by "SHOULD" are expected to be mandatory for Wi-Fi Gateways (Wi-Fi GWs) deployed in public settings and in enterprises. On the other hand, particular circumstances driven by lower end residential deployments may prevent the full implementation of requirements signified by "SHOULD" for residential Wi-Fi GWs.
"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.

[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, 2007.

[802.11a] IEEE 802.11a: High-speed Physical Layer in the 5 GHz Band, 1999.

[802.11ac] IEEE 802.11ac (D3.0): Enhancements for Very High Throughput for Operation in Bands below 6 GHz, June 2012.

[802.11b] IEEE 802.11b: Higher-Speed Physical Layer Extension in the 2.4 GHz Band, 1999.

[802.11d] IEEE 802.11d: Amendment 3: Specification for operation in additional regulatory domains, 2001.

[802.11e] IEEE 802.11e: Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, 2005.

[802.11g] IEEE 802.11g: Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band, 2003.

[802.11i] IEEE 802.11i: Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004.

[802.11n] IEEE 802.11n: Enhancement for higher throughput, 2009.

[802.1D] IEEE 802.1D: Media Access Control (MAC) Bridges, 2004.

[802.1Q] IEEE 802.1Q: Virtual Bridged Local Area Networks, 2011.

[802.1X] IEEE 802.1X: Port-Based Network Access Control, 2011.

[MULPI3.0] Data-Over-Cable Service Interface Specifications, DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification, CM-SP-MULPIv3.0-I23-131120, November 20, 2013, Cable Television Laboratories, Inc.

[RFC 2548] IETF RFC 2548, Microsoft Vendor-specific RADIUS Attributes, March 1999.

[RFC 2784] IETF RFC 2784, Generic Routing Encapsulation (GRE), March 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 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 3646] IETF RFC 3646 DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6), December 2003.

[RFC 4372] IETF RFC 4372, Chargeable User Identity, January 2006.

[RFC 5094] IETF RFC 5094, Mobile IPv6 Vendor Specific Option, December 2007.

[RFC 5176] IETF RFC 5176, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), January 2008.

[RFC 5213] IETF RFC 5213, Proxy Mobile IPv6, August 2008.

[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.

[RFC 5844] IETF RFC 5844, IPv4 Support for Proxy Mobile IPv6, May 2010.

[RFC 5845] IETF RFC 5845, Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6, June 2010.

[RFC 5846] IETF RFC 5846, Binding Revocation for IPv6 Mobility, June 2010.

[RFC 6085] IETF RFC 6085, Address Mapping of IPv6 Multicast Packets on Ethernet, January 2011.

[RFC 6106] IETF RFC 6106, IPv6 Router Advertisement Options for DNS Configuration, November 2010.

[RFC 6540] IETF RFC 6540, IPv6 Support Required for All IP-Capable Nodes, April 2012.

[RFC 6757] IETF RFC 6757, Access Network Identifier (ANI) Option for Proxy Mobile IPv6, October 2012.

[RFC 6909] IETF RFC 6909, IPv4 Traffic Offload Selector Option for Proxy Mobile IPv6, April 2013.

[WiFi MGMT] Wi-Fi Management Interface Requirements, WR-SP-WiFi-MGMT-I04-140311, March 11, 2014, Cable Television Laboratories, Inc.

[WMM] Wi-Fi Alliance: Wi-Fi Multi-Media QoS based on 802.11e, Version 1.1.

[WPA] Wi-Fi Alliance: Wi-Fi Protected Access (WPA) Enhanced Security Implementation Based on IEEE P802.11i standard, Version 3.1, August, 2004.

[WPS] Wi-Fi Alliance: Wi-Fi Protected Setup™ Specification 1.0.

2.2 Informative References

This specification uses the following informative references.

[3GPP TS 23.402] 3GPP TS 23.402 Release 10 2, V10.7.0, Architecture for Non 3GPP Access, March 2012.

[3GPP TS 29.275] 3GPP TS 29.275 Release 9, V9.5.0, Proxy Mobile IPv6 (PMIPv6)-based Mobility and Tunneling protocols; Stage 3 Specification, June 2011.

[eRouter] IPv4 and IPv6 eRouter Specification, CM-SP-eRouter-I11-131120, November 20, 2013, Cable Television Laboratories, Inc.

[WiFi-ROAM] Wi-Fi Roaming Architecture and Interfaces Specification, WR-SP-WiFi-ROAM-I03-140311, March 11, 2014, Cable Television Laboratories, Inc.

2.3 Reference Acquisition

- 3rd Generation Partnership Project (3GPP), 650 Route des Lucioles, Sophia Antipolisn Valbonne, France, Phone: +33 4 92 94 42 00, Fax: +33 4 93 65 47 16, http://www.3gpp.org
- 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

- Internet Engineering Task Force (IETF) Secretariat, 48377 Fremont Blvd., Suite 117, Fremont, California 94538, USA, Phone: +1-510-492-4080, Fax: +1-510-492-4001, http://www.ietf.org
- Wi-Fi Alliance, https://www.wi-fi.org/

3 TERMS AND DEFINITIONS

This specification uses the following terms:

eRouter	An eSAFE device that is implemented in conjunction with the DOCSIS Embedded Cable Modem.
Multi-operator	Common agreements, requirements and operations amongst operators to support roaming.
Roaming	The use of a home network subscription to gain access to a partner network.

4 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations:

AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
AP	Access Point
APN	Access Point Name
ARP	Address Resolution Protocol
BCE	Binding Cache Entry
BRA	Binding Revocation Acknowledgement
BRI	Binding Revocation Indication BULE Binding Update List Entry
BSSID	Basic Service Set Identifier
BULE	Binding Update List Entry
CM	Cable Modem
CMTS	Cable Modem Termination System
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
GI	Guard Interval
GRE	Generic Routing Encapsulation
HFC	Hybrid Fiber Coax
HT	High Throughput
LMA	Local Mobility Anchor
MAC	Media Access Control
MAG	Mobile Access Gateway
MCS	Modulation and Coding Scheme
MIMO	Multiple-input multiple-output
MN	Mobile Node
NAI	Network Access Identifier
NS	Neighbor Solicitation
PBU	Proxy Binding Update
PDN	Packet Data Network
PEAP	Protected Extensible Authentication Protocol
PGW	Packet Data Network Gateway
PHY	Physical
PMIPv6	Proxy Mobile IPv6

RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RS	Router Solicitation
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
U-APSD	Unscheduled Automatic Power Save Delivery
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
Wi-Fi AP	Wi-Fi Fidelity Access Point
Wi-Fi GW	Wi-Fi Gateway
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup

5 OVERVIEW

The Wi-Fi GW considered in this specification integrates a [MULPI3.0] modem with an [802.11n] or later-generation air interface as illustrated in Figure 1. Other functional elements may be integrated with the cable modem as well, but are not illustrated or addressed in this document. The Wi-Fi GW requirements support residential, enterprise and public deployments. Requirements are placed on the air interface in order to support roaming among partner networks. The cable modem interface to the CMTS is defined in [MULPI3.0] specifications. Functional requirements are placed on the Wi-Fi GW management interface. An optional Remote Authentication Dial In User Service (RADIUS) client interface is specified to support Authentication, Authorization and Accounting (AAA) functions.

The Wi-Fi GW requirements apply to cable modem router CPEs. For example, the Wi-Fi requirements can be added to a number of standardized networking functions, such as those defined in [eRouter], or network functions defined in operator specifications.

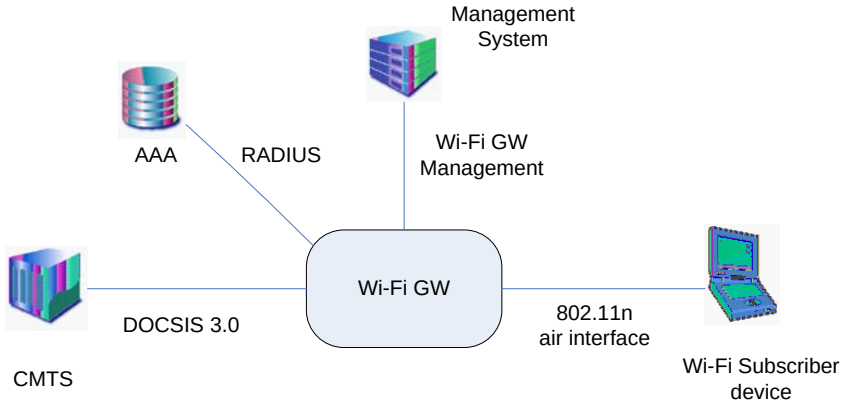

Figure 1 - Wi-Fi GW Interfaces

6 REQUIREMENTS

This section contains normative requirements on the Wi-Fi GW air interface. These requirements encourage multi-vendor interoperability on the Wi-Fi air interface. The Wi-Fi GW MUST NOT use technologies that place non-standard or proprietary requirements on the Wi-Fi subscriber devices.

The requirements apply to GWs that support [MULPI3.0] cable modems. Please see [MULPI3.0] specifications for cable modem requirements.

6.1 802.11 Air Interface Requirements

The Wi-Fi GW MUST support [802.11n] in order to provide high performance wireless data service in conjunction with DOCSIS 3.0 as described in the following subsections. The Wi-Fi GW MUST be backwards compatible with [802.11a], [802.11b], and [802.11g] subscriber devices.

The Wi-Fi GW MAY support [802.11ac] in order to further increase the performance of the wireless data service. If the Wi-Fi GW supports [802.11ac], it MUST be backwards compatible with [802.11a], [802.11b], [802.11g], and [802.11n] subscriber devices.

The Wi-Fi GW needs to support variety of access models which include clear and secured Service Set Identifiers (SSIDs.) Credentials may consist of user name and password or device certificates as determined by the home network operator. A recommended operational residential Wi-Fi GW configuration with a minimum of four SSIDs is described below.

1. A clear SSID that allows users to log into a captive web portal to gain access through the Wi-Fi GW. The SSID name may indicate the brand name of the cable operator that operates the Wi-Fi access network. Alternatively, the SSID name may be common to all roaming partner networks.
2. A secured SSID that supports secure connections for users. An operator-configured client may be required for this access. The SSID name may indicate the brand name of the cable operator that operates the Wi-Fi access network. Alternatively, the SSID name may be common to all roaming partner networks.
3. At least one operator controlled SSID that may or may not be broadcast.
4. An SSID that could be configured by the subscriber on residential GWs, or configured by the enterprise on enterprise GWs, or may be considered a spare.

At least eight SSIDs are recommended for enterprise Wi-Fi GW operations.

6.1.1 Requirements for 802.11n Wi-Fi GWs for use with DOCSIS 3.0 CMs

The [MULPI3.0] specification has significantly improved the cable modem data rate in the downstream and upstream directions compared to previous versions, through the means of channel bonding. By bonding a minimum of four channels, DOCSIS 3.0 certified CMs can achieve a minimum Physical (PHY) rate of 160 Mbps on the downstream. To fully utilize the resources available on the cable access network, the wireless air interface of the Wi-Fi GW that is integrated with a DOCSIS 3.0 certified CM will match the rate that is achievable by the CM. The newest IEEE amendment to the [802.11], wireless networking standard [802.11n], is selected because it offers a significant improvement in throughput over prior standards such as [802.11b] and [802.11g]. The Wi-Fi GW MUST support all mandatory features in the [802.11n] specification. The Wi-Fi GW SHOULD support the optional features defined in [802.11n].

The Wi-Fi GW operating in 802.11n mode MUST support the 20 MHz HT (High Throughput 20 MHz channel) mode. The Wi-Fi GW operating in 802.11n mode SHOULD optionally support the 40 MHz HT mode. If the Wi-Fi GW operating in 802.11n mode supports both 20 MHz HT and 40 MHz HT modes, the Wi-Fi GW initial default MUST be 20 MHz HT. The Wi-Fi GW MUST support the ability of the operator to configure the 20 Mhz and 40Mhz HT modes for operation.

Multiple modulation and coding scheme (MCS) parameter sets are defined by the IEEE standard, and can be adapted for varying physical environment. The Wi-Fi GW operating in 802.11n mode MUST support the following Modulation and Coding Scheme (MCS) parameter sets as defined in [802.11n]: MCS0 - MCS15 for 20 MHz HT. Under favorable physical environment, the potential PHY layer data rate can achieve a maximum of 130 Mbps, with

the use of only mandatory features. The Wi-Fi GW operating in 802.11n mode MUST be able to achieve 130 Mbps in raw bit rate.

With the use of optional features such as channel bonding, short Guard Interval (GI) and more than two spatial streams, the 802.11n is able achieve even higher PHY throughput. The Wi-Fi GW operating in 802.11n mode SHOULD support the optional features defined in [802.11n]. In particular, the use of 40 MHz channel is an optional feature that is achieved through channel bonding, and is responsible for doubling the PHY throughput from a single 20 MHz channel. The Wi-Fi GW operating in 802.11n mode MUST support MCS0 - MCS15 for 40 MHz HT if 40 MHz channel is supported.

The Wi-Fi GW SHOULD support 40 MHz channels with short Guard Interval (GI) that provides up to 300Mbps performance.

6.1.2 Interoperability

The 802.11n air interface operates in the 2.4 GHz frequency range, which it shares with legacy devices that are 802.11b and g capable, as well as 5 GHz spectrum, which it shares with 802.11a enabled devices. To ensure coexistence with legacy and new devices, the Wi-Fi GW MUST be interoperable with Wi-Fi certified [802.11b], [802.11g] and [802.11n] compliant MAC Computers, Windows-based PCs and other mobile Wi-Fi devices. The Wi-Fi GW SHOULD be interoperable with Wi-Fi certified [802.11a] devices as enabled or disabled separately by the operator provisioning. The Wi-Fi GW operating in 802.11n mode MUST support non-concurrent selective dual band mode: 2.4 GHz 11b/g/n or 5 GHz .11n, with 2.4 GHz being the default selection. The Wi-Fi GW MUST support the ability of the operator to provision which band is selected for operation. The Wi-Fi GW MUST support frame aggregation.

The [802.11n] capable Wi-Fi GW MUST support data rates with automatic fall back of 6Mbps, 36Mbps, and 48Mbps in [802.11g] modes.

Since the Wi-Fi GW is required to support multiple SSIDs, the interoperability requirement is extended to the SSID level. The 802.11n capable Wi-Fi GW MUST support both tri-mode (.11b/g/n) and single mode (e.g., .11n only) operations per SSID as defined in [802.11n]. The 802.11n capable Wi-Fi GW SHOULD support both dual-mode (.11a/n) and single mode (e.g., .11n only) operations per SSID as defined in [802.11n]. The 802.11n capable Wi-Fi GW SHOULD support the ability of the operator to configure the mode of operation using a field programmable mode lock option.

6.1.3 Channel Selection

The 802.11 standards divide the 2.4000–2.4835 GHz band into 13 channels, each with width 22 MHz but spaced only 5 MHz apart, with channel 1 centered on 2.412 GHz. Multiple wireless devices operating in the same channel in the vicinity of each other may experience co-channel interference. The Wi-Fi GW MUST support auto-channel selection by the following two methods per [802.11]: 1) measuring energy levels on the channel, and 2) monitoring for 802.11 signal structures and detecting radar pulses.

The Wi-Fi GW MUST support manual selection of a channel.

The Wi-Fi GW MUST support selection of 1, 6, and 11 channels only.

The Wi-Fi GW MUST allow the operator to select between Manual and Auto channel selection mode.

6.1.4 Antenna Requirements

Multiple-Input, Multiple-Output, or MIMO, utilizes multiple transmitter and receiver antennas to improve the system performance. The Wi-Fi GW operating in 802.11n mode MUST support MIMO Power Save by utilizing multiple antennas only on as-needed basis based on Automatic Power Save Delivery as defined in [WMM]. The Wi-Fi GW operating in 802.11n mode MUST support the minimum of 2 x 2 MIMO transmit/receive antenna array for the frequency band with four antennas in total. This is denoted as the 2 x 2 MIMO configuration.

The Wi-Fi GW operating in 802.11n mode SHOULD also support transmit beam forming that locates receiving devices and focus the signal on them.

As stated in earlier section, the Wi-Fi GW is prohibited from using any proprietary technologies that may cause interoperability issues with client devices. The Wi-Fi GW MUST NOT use proprietary beam forming technologies that place non-standard or proprietary requirements on the Wi-Fi subscriber devices.

The Wi-Fi GW antennas MUST support transmission and reception simultaneously.

The minimum specification for Wi-Fi GW antenna gain MUST be at least 4 dBi.

6.1.5 Transmit Power, Range, Receiver Sensitivity

The Wi-Fi GW MUST have a Maximum Transmit Power equal to or greater than 400 mW (26.021 dBm).

The Wi-Fi GW MUST NOT exceed the maximum limits for radiated power according to regional regulations.

6.1.6 Air interface performance

The 802.11n air interface defines a number of MCS parameter sets that can be utilized to match varying physical environment. The Wi-Fi GW MUST support dynamic link adaptation for graceful degradation when RF conditions deteriorate (e.g., switch to a lower order QAM). The Wi-Fi GW SHOULD support power management techniques to reduce interference.

6.1.7 Other Requirements

The Wi-Fi GW MUST default the user configured SSID to either on or active. The Wi-Fi GW MUST NOT allow the user to disable operator-configured SSIDs.

The Wi-Fi GW MUST comply with [802.11d].

The Wi-Fi GW MUST support IPv6-only operation per [RFC 6540]. Note that IPv6-only operation has different implications for the control plane and user traffic forwarding plane. For the control plane, IPv6-only operation means that the wireless AP will not have an IPv4 address assigned to it for management, monitoring, or transport (e.g., GRE), meaning that all interaction between the Wireless AP and the Wi-Fi core or PMIPv6 core will be over IPv6. Separately, the Wireless AP and PMIPv6 (proxy mobile IPv6) user device data plane can be configured as IPv4-only, IPv6-only, or dual-stack. This supports traffic from a variety of wireless devices. It is expected that a wireless AP using IPv6-only control plane operation will support dual-stack data plane operation. This means that any IPv4 user data will be encapsulated in IPv6 transport back to the Wi-Fi core.

6.1.8 Configurations of SSIDs

In order to provide the Wi-Fi subscriber devices the impression of multiple physical Access Points in the same area, multiple SSIDs on the same Wi-Fi GW are used. All the SSIDs configured in a single Physical Access Point share the same Radio and the Physical channel. In effect, it is possible to emulate as many Virtual Access Points as the number of SSIDs supported by the Hotspot with a single Physical Access Point. Support for multiple SSIDs is implemented in one or more of the following models:

- multiple SSIDs per beacon, single beacon, single BSSID,
- single SSID per beacon, single beacon, single BSSID,
- single SSID per beacon, multiple beacons, single BSSID,
- single SSID per beacon, multiple beacons, multiple BSSIDs.

A Base Service Set Identifier (BSSID) per [802.11] is technically equivalent to a MAC address, for most of the hotspots have their unique MAC address as their BSSID.

The Wi-Fi GW MUST support at least four SSIDs using the multiple BSSID model. The Wi-Fi GW MUST support independent remote configuration of parameters associated with each SSID. The Wi-Fi GW SHOULD support at least eight SSIDs for enterprise deployment scenarios.

The Wi-Fi GW MUST correspond each SSID to a separate MAC address (multiple BSSIDs), providing the functionality of multiple virtual APs and true traffic separation.

The Wi-Fi GW MUST provide the ability for any SSID to be configured as below:

- Operator-configured and secured SSID for use by home network subscribers. This SSID is utilized by the subscriber to access the operator's HFC network. This may be used by the operator for Fixed-Mobile Convergence applications or other purposes.

- Operator-configured and secured SSID for users. The SSID name may indicate the brand name of the cable operator that operates the Wi-Fi access network. Alternatively, the SSID name may be common to all roaming partner networks. This secured multi-operator SSID is utilized when a connection manager has been configured on the client device. The connection manager is responsible for choosing the appropriate network for the client device to connect to; be it a home operator SSID, multi-operator SSID for roaming users, or macro networks, etc., based on pre-configured criteria such as traffic type or priority. By doing so, the connection manager provides seamless connection without user intervention.
- An operator-configured clear SSID for users that leads the user to a captive sign-in portal. The SSID name may indicate the brand name of the cable operator that operates the Wi-Fi access network. Alternatively, the SSID name may be common to all roaming partner networks. The portal can be used by new users or existing subscribers to gain access to the operator Wi-Fi GW. Compared to the previous scenario, the subscribers or new users must log in through the captive portal.
- Residential subscriber or enterprise controlled SSID, managed by the subscriber via a local web page.

The Wi-Fi GW MUST support independent remote configuration of parameters associated with each SSID. The Wi-Fi GW SHOULD support independently configurable parameters on a per SSID basis that includes but is not limited to: the SSID name, security type, [WMM] enable/disable, bridge mode enable/disable, data rate supported or radio resources/bandwidth allocation (percentage of total bandwidth per SSID), SSID Broadcast on/off, authentication, and encryption. This requirement is primarily targeted for the three operator-configured SSIDs as discussed above.

For residential and enterprise configurations, the Wi-Fi GW MUST support the configuration of the user-controlled SSIDs and the associated attributes via a local web page. The Wi-Fi GW MUST provide the residential subscriber with the option of configuring their SSID.

The Wi-Fi GW MUST support the ability of the operator to configure an SSID for use by the subscriber (the subscriber controlled SSID). Furthermore, the Wi-Fi GW MUST support the ability of the operator to set the default designation of the subscriber controlled SSID; for example, to the device model number plus the last six digits of one of the wireless MAC address.

The Wi-Fi GW MUST support the configuration of the operator-controlled SSIDs and the associated attributes via remote access by the operator. The Wi-Fi GW MUST NOT allow the operator-controlled SSIDs and the associated attributes to be configured or changed by the user.

The Wi-Fi GW MUST support the capability of the operator to configure SSIDs and activate the Wi-Fi air interface operation upon attachment of Wi-Fi GW to the operator's HFC network, and without user intervention.

The operator-controlled SSIDs MAY be broadcast using a beacon. The user may choose to broadcast the subscriber-controlled SSID.

As a measure to help prevent unauthorized access to the Wi-Fi GW, client-side SSID probing suppression is used. The Wi-Fi GW MUST accept configuration from the operator to block association requests that do not specify a valid SSID. That is, the device MUST be able to block association requests that probe for "any" SSID if configured to do so.

To prevent a user from inadvertently turning off the roaming services provided by the Wi-Fi GW, fail-safe features are required for the configuration process. The Wi-Fi GW MUST prohibit the subscriber from disabling the access point radio as this would turn off all SSIDs. The Wi-Fi GW MUST provide a method for the subscriber to disable the wireless interface impacting only the subscriber's SSID. The Wi-Fi GW MUST NOT impact or provide any information regarding the operator configured SSIDs when the subscriber configures the subscriber designated SSID.

Operators can select to organize traffic from each SSID in separate Virtual Local Area Networks (VLANs) to assist in traffic priority settings and to help ensure traffic separation and traffic forwarding. The following layer 2 tagging methods are available for marking packets from any configured SSID to help form a VLAN:

- [802.1Q] Q-Tag frame encoding also known as Virtual Local Area Network (VLAN) tagging (e.g., VID)
- [802.1Q] S-Tag and C-Tag frame encodings (e.g., S-TPID S-VID,... C-TPID, C-VID,...)

The Wi-Fi GW MUST be able to assign VLAN marking per [802.1Q] based on SSID to traffic as configured by the network operator. The Wi-Fi GW MUST be able to assign S-Tags and C-Tags per [802.1Q] based on SSID to traffic as configured by the network operator.

When an SSID is configured by the operator in bridge mode configuration, the Wi-Fi GW MUST forward the traffic belonging to that SSID, directly between the SSID and the cable modem.

When an SSID is configured by the operator in router mode configuration, the Wi-Fi GW SHOULD forward the traffic belonging to that SSID, directly between the SSID and the Wi-Fi GW internal routing functions (such as an eRouter).

The Wi-Fi GW MUST present traffic from an SSID to the cable modem with the VLAN tags provisioned for that SSID even if the traffic is forwarded through a router internal to the Wi-Fi GW. i.e., the Wi-Fi GW ensures that the VLAN tags added per the SSIDs are preserved when forwarding the traffic to the cable modem from a bridge mode SSID or a router mode SSID.

6.1.9 Security Requirements

The Wi-Fi GW is designed to offer the strongest security the subscriber device can support. Therefore, the Wi-Fi GW supports Wi-Fi Alliance certified encryption and authentication methods, including Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Wi-Fi Protected Access 2 (WPA2). WPA2 supports the Advanced Encryption Standard (AES), while Temporal Key Integrity Protocol (TKIP) can be used in WPA.

The Wi-Fi GW MUST implement WPA2 per [WPA] on the air interface that supports [802.1X], Protected Extensible Authentication Protocol, (PEAP), Extensible Authentication Protocol- Tunneled Transport Layer Security (EAP-TTLS) per [RFC 5281], and Extensible Authentication Protocol - Transport Layer Security (EAP-TLS) per [RFC 5216]. The Wi-Fi GW MUST support the following security operating modes configurable per SSID: WEP (64 and 128 bit), encryption, WPA-PSK, WPA2-PSK, WPA with 802.1x, WPA2 with 802.1x, and mixed WPA(TKIP) - WPA2(AES) security mechanisms as per [802.11i] and [WPA], in bridge or router mode.

Note: WPA2 (AES) is strongly recommended to be configured on operator managed SSIDs.

The Wi-Fi GW MUST support the WPS pairing button. The Wi-Fi GW MAY support the PIN methods for initial Wi-Fi device pairing per [WPS]. It is recommended that the Wi-Fi GWs are Wi-Fi alliance certified for WPS.

The Wi-Fi GW MUST support independent configuration of security options for each SSID.

The Wi-Fi GW MUST prevent routing between private and public SSID VLANs. When VLANs are supported, the Wi-Fi GW MUST put the clients connected to each SSID in a separate VLAN and route the traffic from each VLAN transparently to the upstream network.

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

It is recommended that Wi-Fi GWs support firewall and NAT capabilities. However, firewall requirements are outside the scope of this specification.

6.1.10 Other Requirements

The Wi-Fi GW MUST utilize the Unscheduled Automatic Power Save Delivery, U-APSD, (WMM Power Save) enhancements per [WMM]. Wi-Fi GWs need to pass Wi-Fi alliance U-APSD certification.

The Wi-Fi GW SHOULD support the redirection of subscriber devices to a web page upon successful authentication and access admission as configured by the operator. This requirement is envisioned to apply to enterprise deployments where subscribers are redirected to an enterprise web page.

6.1.11 Requirements for 802.11ac Support

The following requirements are applicable to the Wi-Fi GW that supports [802.11ac]

The Wi-Fi GW MUST support the mandatory features in [802.11ac]. Additionally, the Wi-Fi GW MUST also support the following optional [802.11ac] functions:

- Short Guard Interval,

- MCS 8 and 9 (256-QAM, r=3/4, r=5/6)
- LDPC channel coding.

These PHY enhancements increase the Wi-Fi GW's capacity, reliability and range for data transmission. In particular, the Wi-Fi GW 256-QAM modulation capability can offer a maximum PHY transmission rate of 1.3 Gbps.

The Wi-Fi GW MUST support the simultaneous dual-band operations with 802.11b/g/n on the 2.4 GHz band and [802.11ac] on the 5 GHz band. This allows legacy 802.11b/g/n subscriber devices and [802.11ac] subscriber devices to operate with the Wi-Fi GW at the same time.

6.2 Generic Routing Encapsulation

This section describes Wi-Fi GW requirements to support Generic Routing Encapsulation (GRE) [RFC 2784] of layer two user traffic to and from an SSID. GRE is an optional capability for the Wi-Fi GW that operators can use to segregate and forward user traffic per SSID. A separate GRE tunnel can be established for each SSID, or traffic associated with multiple SSIDs can be combined in a single GRE tunnel. In this case, VLAN tags (802.1Q or 802.1ad) are used to separate traffic between SSIDs within the GRE tunnel. The use of GRE is transparent to the CMTS with this approach. IP transport is used to carry the GRE tunnel.

The GRE tunnel is statically provisioned on the Wi-Fi GW.

Note Layer two tagging techniques including 802.1ad, can be used in combination with GRE encapsulation. Layer two tags are encapsulated along with the balance of the user layer two packet within the GRE tunnel. VLANs are preserved with this GRE approach.

Note DSCP markings can be added by the Wi-Fi GW to provide differentiation of traffic from separate GRE tunnels as well as unique traffic flows (e.g., per SSID) within a given GRE tunnel.

6.2.1 GRE Requirements for the User Data Plane for a public SSID

The Wi-Fi GW MUST support the mapping of an IP GRE tunnel to a single SSID. The mapping supports bi-directional traffic.

The Wi-Fi GW MUST support the mapping of an IP GRE tunnel to multiple SSIDs. The mapping supports bi-directional traffic.

The Wi-Fi GW MUST support terminating 802.11, and originating 802.3 frames for forwarding upstream traffic

The Wi-Fi GW MUST support upstream forwarding as listed below:

- The destination IP address in the transport IP header MUST be set to the IP address of the GRE tunnel endpoint in the network north of the Wi-Fi GW.
- The source IP address in transport IP header MUST be set to the WAN IP address (Public IP) of Wi-Fi GW
- The protocol type in transport IP header MUST be set to "GRE" (47)
- The protocol type in GRE header MUST be set to "Transparent LAN Bridging" (0x6558).
- The Wi-Fi GW MAY insert 802.1q or 802.1ad VLAN tag corresponding to the SSID in the encapsulated (i.e., inner) 802.3 frame. The 802.1q or 802.1ad VLAN tag MAY be used to identify the SSID(s).
- The Wi-Fi GW MUST prevent user-to-user switching of frames within same SSIDs or across SSID. All traffic (including broadcast and multicast packets but excluding EAP messages for 802.1x authentication) coming in on 802.11 WLAN interfaces must be tunneled to the GRE tunnel endpoint in the network north of the Wi-Fi GW.
- The Wi-Fi GW must support applying DSCP value in the transport IP header for upstream packets. This is used to classify traffic from SSIDs into different DOCSIS service flows, based on the DSCP marking on the GRE tunnel packets. The set of DSCP markings used to map to a GRE tunnel is static.

- The Wi-Fi GW MUST support downstream forwarding as listed below:
  - The Wi-Fi GW decapsulates GRE
  - If the protocol type in GRE header is "Transparent LAN Bridging" (0x6558), then the Wi-Fi GW MUST process the 802.3 frame following the GRE header.
  - If the protocol type in GRE header is not "Transport LAN Bridging" (0x6558), then the Wi-Fi GW MUST silently drop the frame.
  - The Wi-Fi GW MAY use the VLAN-ID to locate the SSID.
  - If the decapsulated 802.3 frame contains a 802.1q or 802.1ad VLAN tag, the Wi-Fi GW MUST use the VLAN tag to locate the SSID.
  - If the decapsulated 802.3 frame does not contain 802.1q or 802.1ad VLAN tag, the Wi-Fi GW Must use the destination MAC address to locate the SSID.
- The Wi-Fi GW MUST rewrite MSS option to or less than 1390B in both TCP SYN and TCP SYN-ACK packets.

6.2.2 GRE Requirements for the Control Plane for a Public SSID

The Wi-Fi GW MUST implement DHCP relay agent in order to insert sub-options in option-82 of DHCP messages received from the client device connected to the public SSID.

The Wi-Fi GW MUST support inserting information about the AP and the SSID (e.g., AP-MAC-Address, SSID-Name, and SSID-Type i.e., "open" or "secure") on which the DHCP message is received from the client device connected to the public SSID in the circuit-ID sub-option in DHCP relay agent option option-82. Insertion of SSID in the circuit-ID sub-option MUST be configurable.

- The Wi-Fi GW MUST support inserting the MAC address of client device connected to a public SSID remote-id sub-option of DHCP option-82. Insertion of MAC address of client device in remote-id sub-option MUST be configurable.
- Remote-id MUST be a string containing MAC address of client device connected to the public in the format "xx:xx:xx:xx:xx:xx"
- The Wi-Fi GW MUST transparently forward any other options already present in DHCP (e.g., DHCP option 26 inserted by the client device).

6.3 Proxy Mobile IPv6 based Layer-3 Tunneling Support

Proxy Mobile IPv6 (PMIPv6) is a network-based mobility management protocol standardized by IETF. The base protocol is defined in [RFC 5213] and [RFC 5844]. The protocol also supports many other additional extensions for supporting various use-cases and these extensions have been published by IETF. PMIPv6 protocol is also being used in 3GPP SAE architecture, on S2a, S2b and S5/S8 interfaces, specified in [3GPP TS 23.402] and [3GPP TS 29.275].

There are two core functional entities in PMIPv6, Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG). PMIPv6 is a control-plane driven protocol, which uses the control plane signaling to establish dynamic tunnels between MAG and LMA for carrying user traffic. In PMIPv6 terminology, subscriber end devices are typically referred to as mobile nodes. LMA is responsible for maintaining the mobile node's reachability state and is the topological anchor point for the mobile node's home network. MAG is the entity that performs mobility management on behalf of a mobile node and it resides on the access-link where Mobile node is anchored.

PMIPv6 supports IPv4, IPv6 or dual-Stack client addressing. The mobile nodes attached to the Proxy Mobile IPv6 domain can be an IPv4-only, IPv6-only or a dual-stack capable nodes. Furthermore, PMIPv6 supports IPv4-only or IPv6-only transport network. All though the protocol name suggests that PMIPv6 is an IPv6-based protocol, however the protocol has complete support for IPv4-only mobile nodes and IPv4-only transport network. The protocol allows a clear migration path for allowing the operator to evolve the mobile nodes and transport network from IPv4 to IPv6 at different phases. As specified in Section 6.1.7 above, the Wi-Fi GW needs to be capable of IPv6 only operation.

PMIPv6 protocol supports the following encapsulation types for the layer-3 tunnel between the MAG and the LMA. These tunnel encapsulation types are standard layer-3 tunnels. The mobile node's traffic between the MAG and the LMA can be carried using any one of the encapsulations negotiated over the control plane signaling. However, GRE is the only encapsulation mode supported in 3GPP PGW/LMA and hence is the preferred and default encapsulation mode.

IP over GRE tunnels (preferred)

IP in IP tunnels

UDP over IP Tunnels

PMIPv6 defines a policy profile for each mobile node. This policy profile can be configured locally on the MAG, or the MAG can obtain this policy profile from AAA as part of access authentication. This profile identifies the mobile node's service parameters and the home network information, such as LMA identity. Corresponding to a mobile node, MAG finds out about the identity (IP Address or FQDN) of the mobile node's home LMA from an associated mobile node policy. In addition to the LMA identity, the policy may also contain other parameters, which will be provided to the LMA, which will help the LMA to identify the type of network access to be provided to the client, the IP addressing type (IPv4, IPv6 or Dual Stack etc.), the location information etc. A mobile node policy may be based up on a globally defined policy profile on the W-Fi GW. Policy profile can be defined on a per SSID basis as well. In addition, some or all of the parameters of the policy may be overwritten by a AAA server. This AAA server based policy override provides the flexibility to customize the policy at a per Mobile node level.

Wi-Fi gateway with PMIPv6 support may be used for the following deployment scenarios:

a) Wi-Fi Hotspot with generic IP mobility architecture using PMIPv6: In this model, the mobile access gateway (MAG) functionality on the Wi-Fi gateway will interwork with a generic [RFC 5213] compatible LMA. This is suited for MSO managed public Wi-Fi deployment scenarios, which does not require integration to a third party Mobile Operator's packet core.

b) Wi-Fi Hotspot solution which supports trusted WLAN integration with EPC: In this model PMIPv6 LMA functionality is co-located with 3GPP PDN gateway in the 3GPP core. This is suited for Mobile Data Offload scenarios over an MSO managed public Wi-Fi network, or for trusted Wireless LAN interworking with the 3GPP access.

c) Wi-Fi Hotspot solution with hybrid model: In this model, MAG functionality on the Wi-Fi GW can interwork with a generic [RFC 5213] compatible LMA as well as an LMA co-located on a PDN gateway

A logical topology of a Generic Wi-Fi Architecture using PMIPv6 is illustrated in Figure 2 below. In this architecture the MAG functionality resides on the Wi-Fi GW. Control plane signaling messages are used between the MAG and LMA to establish dynamic layer-3 data plane tunnels between the Wi-Fi GW and the LMA. LMA is the tunnel termination point on the MSO network side and typically will be co-located on a subscriber aggregation device such as BNG, which enforces Wi-Fi subscriber network and service access policies. Traffic corresponding to multiple Wi-Fi subscriber devices can be mapped to a single data plane tunnel.

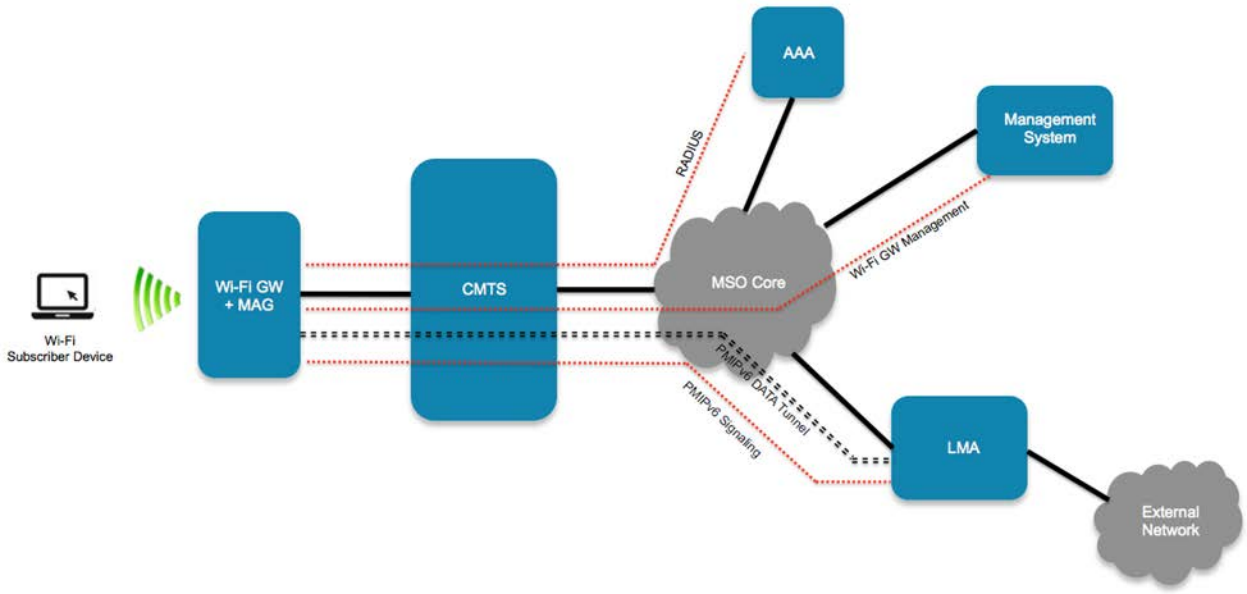

Figure 2 - PMIPv6 Architecture using Wi-Fi GW MAG

Basic protocol operation at a high level is illustrated using the call flow provided in Figure 3 below:

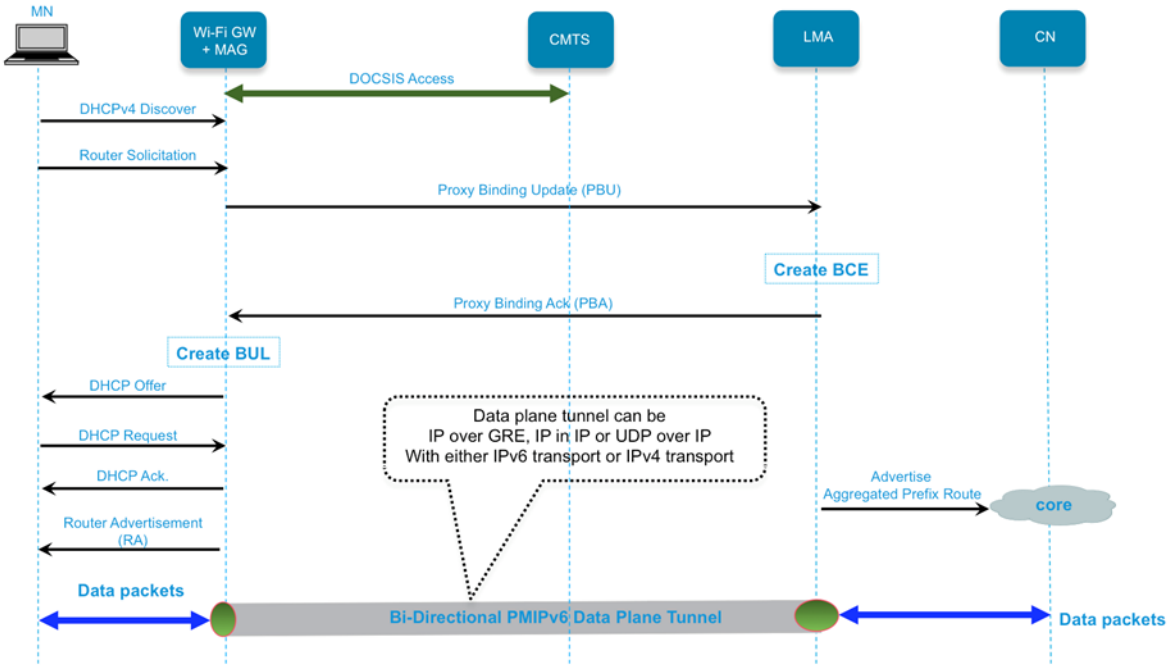

Figure 3 - Sample PMIPv6 Signaling Call Flow.

In this call flow it is assumed that client authentication is already completed. This call flow illustrates Dual Stack based client addressing. DHCP discover message from the client acts as attachment detection for the MAG. Also the client device sends a Router Solicitation Message to initiate the IPv6 address acquisition process. If 802.1X

authentication is in use, the successful completion of authentication also can trigger the PMIPv6 processing. Up on detecting the Mobile node attachment, the MAG builds a Proxy Binding Update (PBU) message. MAG uses the MN policy (derived from a Policy profile configured on the GW or downloaded from AAA server) to populate the parameters in the PBU message. Up on receiving the PBU message, the LMA assigns an IPv4 address and an IPv6 Prefix for the Mobile Node and creates a Binding Cache Entry (BCE). LMA picks up these addresses for the client either from locally defined pools or from external DHCP and DHCPv6 servers. The BCE entry associates the MAC address of the Mobile node with the IPv4 address and the IPv6 prefix. After the BCE is created, LMA sends a Proxy Binding Acknowledgement (PBA) message to the MAG. PBA message carries the IPv4 address and the IPv6 prefix for the client. It may also carry Protocol Configuration Information (PCO) such as DNS server IP address, Domain name etc. MAG uses the PBA message to build the Binding Update List (BUL) entry for the client. If there is already an existing data plane tunnel between the MAG and LMA, the MAG simply binds the new client to this tunnel. Otherwise a new tunnel will be created and the client will be associated to this tunnel. After creating the BUL entry for the client, MAG completes the address assignment through DHCP for IPv4 and SLAAC for IPv6. After the completion of IPv4 and IPv6 address assignment, subsequent data packets from the client get forwarded through the PMIPv6 data plane tunnel.

Note: Even though call flow illustrates a dual stack client, PMIPv6 supports single stack IPv4 only as well as IPv6 only addressing.

6.3.1 PMIPv6 Control Plane Requirements for the Wi-Fi GW

PMIPv6 MAG functionality on the Wi-Fi GW must support the following:

- Wi-Fi GW must support the configuration of a global PMIPv6 policy profile. This global profile will be used to generate the signaling messages towards the LMA up on a client attachment trigger on the Wi-Fi side.
- Wi-Fi GW must support configuration of Home LMA IP address or FQDN name of the Home LMA in the policy profile.
- Wi-Fi GW may support the configuration of an APN in the policy profile when interworking with a generic LMA per [RFC 5213].
- Wi-Fi GW must support the configuration of an APN in the policy profile when interworking with a 3GPP PGW/LMA over S2a PMIPv6 interface.
- Wi-Fi GW may support the configuration of a PDN type in the policy profile when interfacing with a generic LMA per [RFC 5213].
- Wi-Fi GW must support the configuration of a PDN type in the policy profile when interfacing with a 3GPP PGW/LMA over S2a PMIPv6 interface.
- Wi-Fi GW must support the configuration of PMIPv6 policy profile on a per SSID basis.
- Wi-Fi GW must support AAA override of PMIPv6 policy profile on a per client basis.
- For IPv4 clients, Wi-Fi GW must support the following client attachment triggers, a) DHCP discover, b) DHCP Request, c) Unicast ARP d) Broadcast ARP
- For IPv6 clients, Wi-Fi GW must support the following client attachment triggers, a) Router Solicitation, b) Neighbor Solicitation
- For IPv4 client addressing, Wi-Fi GW must function as a DHCPv4 server and must assign the LMA assigned IPv4 address to the client via DHCP.
- For IPv6 client addressing, Wi-Fi GW must support SLAAC and assign the LMA assigned IPv6 prefix using unicast RA.
- For IPv6 client, Wi-Fi GW should use Recursive DNS Server and DNS Search List (RDNSS) options specified in [RFC 6106] for providing the DNS information parameters in the RA messages.
- For IPv6 client, Wi-Fi GW should use DHCPv6 per [RFC 3646] to provide the DNS Recursive Name Server option to provide a list of one or more IPv6 addresses of DNS recursive name servers to which a

client's DNS resolver may send DNS queries, and Domain Search List option to specify the domain search list the client is to use when resolving hostnames with DNS.

- For IPv6 client addressing, Wi-Fi GW may support Stateful DHCPv6 server functionality and assign the LMA assigned IPv6 prefix to the client via DHCPv6.
- Wi-Fi GW must include the configured APN name in the PBU message.
- Wi-Fi GW may include an ANI in the PBU message. ANI may be configurable at the global level or per SSID basis. If no ANI is configured, Wi-Fi GW may include SSID to which the client is associated as the ANI and include in the PBU message.
- Wi-Fi GW must send a De-registration PBU message when a Wi-Fi client which has an active BUL entry is disconnected from the Radio Network.
- Wi-Fi GW must delete an existing BUL entry for a client up on receiving a BRI message from LMA. After the deletion of the BUL entry, Wi-Fi gateway must send a BRA message in response to the BRI.
- Wi-Fi GW must support the binding of multiple clients to a single PMIPv6 data plane tunnel.
- As specified in Section 6.1.7 above, the Wi-Fi GW needs to be capable of IPv6 only operation.

6.3.2 PMIPv6 Data Plane Requirements for the Wi-Fi GW

PMIPv6 MAG functionality on the Wi-Fi GW must support the following:

- Wi-Fi GW must support dynamic establishment/tear-down of layer-3 bi-directional data plane tunnel with GRE encapsulation mode.
- Wi-Fi GW may support data plane tunnels using other encapsulation options as defined in [RFC 5844] and [RFC 5845]
- Wi-Fi GW must simultaneously support multiple PMIPv6 data plane tunnels with different LMA's.
- Wi-Fi GW must support the binding of multiple mobile nodes to a single GRE tunnel. For carrying multiple mobile node traffic on a single GRE tunnel between a MAG and LMA, GRE key extension as defined in [RFC 5845] must be supported.
- Wi-Fi GW must forward all the upstream traffic from the client with an active BUL entry to the corresponding data plane tunnel.
- For IPv4 clients, Wi-Fi GW must support proxy ARP for the client's IP destination addresses in the client's home IPv4 subnet.
- For IPv4 clients, Wi-Fi GW must be able to terminate DHCP transactions and must be able to deliver the LMA assigned IP address configuration to the mobile node.
- As specified in Section 6.1.7 above, the Wi-Fi GW needs to be capable of IPv6 only operation.

6.4 Resources and Traffic Priority

The ability to define resource policies, as well as admission control procedures for various users, allows operators to ensure proper service levels to subscribers with a finite amount of network resources. For example, it may be beneficial for the operator to be able to guarantee a minimum amount of bandwidth for the subscriber to access the HFC network, and to cap the maximum bandwidth that can be used by the roaming users. The Wi-Fi GW MUST support the capability of the operator to configure the maximum resources allocated and minimum resources reserved to any SSID. If the bandwidth available for roaming subscribers on multi-operator SSIDs is exhausted, then the Wi-Fi GW MUST NOT accept any new connections for roaming or public users on the multi-operator SSID.

Traffic from roaming subscribers cannot prevent or preempt the use of the bandwidth allocated for the residential or enterprise subscriber. Therefore, the operator will need to be able to configure the Wi-Fi GW to prioritize traffic from the residential or enterprise subscriber over traffic generated from roaming subscribers. The Wi-Fi GW MUST support the ability for the operator to configure traffic priority on the air interface and WAN interface. The GW

MUST support the ability to propagate the configured traffic priority for the air interface to the DOCSIS interface as configured by the operator.

The Wi-Fi GW MUST support traffic prioritization mapped per SSID to Class of Service bits as defined by 802.1p in [802.1D] and VLAN tags as defined in [802.1Q]. The Wi-Fi GW MUST support traffic prioritization procedures and capabilities called out in [MULPI3.0].

6.5 RADIUS Client Interface

The Wi-Fi Roaming Architecture specification, [WiFi-ROAM], specifies how RADIUS is used by partner networks to support service to roaming subscribers. Operators may select to deploy RADIUS signaling clients on Wi-Fi GWs. The RADIUS interface will allow the Wi-Fi GW to interface to policy servers, AAA proxies, and AAA servers. This section defines an optional interface on the Wi-Fi GW to support RADIUS for AAA functions. If the Wi-Fi GW supports a RADIUS signaling client, then the Wi-Fi GW MUST support the RADIUS client AAA functions and mandatory attributes defined in [RFC 2865], [RFC 2866], [RFC 2869], [RFC 3579], [RFC 3580], [RFC 4372], and [RFC 5176]. If the Wi-Fi GW supports a RADIUS signaling client, the Wi-Fi GW MUST support the MS-MPPE-Send-Key and MS-MPPE-Recv-Key attributes as defined in [RFC 2548] for the sake of establishing encryption over the air per [WPA] after authentication is completed and access is granted for a subscriber device. If the Wi-Fi GW supports a RADIUS client, it MUST report its location in RADIUS Accept-Request and Accounting-Request messages per the procedures defined [RFC 5580] as configured by the operator. The Wi-Fi GW MUST support the capability of the operator to configure the reported operator and location attributes defined in [RFC 5580]. See the Wi-Fi Roaming Architecture specification [WiFi-ROAM] for further information on the use of RADIUS attributes per the RFCs listed above.

6.6 Management Interface Requirements

The following subsections include functional requirements for the Wi-Fi GW management interface. The protocol definition for the management interface is outside the scope of this specification.

6.6.1 Status and Performance Reports

The Wi-Fi GW needs to provide sufficient air interface status, fault and performance reports to the operator's network management system in order to provide the best service and customer care support for the subscriber. Reports can include the health and configuration of the Wi-Fi GW, the connection and traffic status of clients, and air interface performance data. The Wi-Fi GW MUST support the management interface, configuration and reporting requirements specified in [WiFi MGMT].

6.7 Configured Admission Control

The Wi-Fi GW MUST support operator-configured access lists to restrict access of specific users or categories of users. This list is referred to as a MAC address black list. The Wi-Fi GW MUST support a device MAC address filter list per SSID. The Wi-Fi GW MUST support subscriber access to the MAC filter list associated with the subscriber controlled SSID. The Wi-Fi GW MUST NOT allow subscriber access to the MAC filter lists associated with operator managed SSIDs.

The Wi-Fi GW MUST support the ability for the operator to configure a list of device MAC addresses that have exclusive access to an SSID on the Wi-Fi air interface. MAC addresses that are not on the list are not allowed to associate with an SSID on the Wi-Fi air interface. This list is referred to as a MAC address white list.

Appendix I Acknowledgements

CableLabs would like to thank the cable operator members of CableLabs for their support in guiding the requirements defined in this specification, as well as the vendors who helped in the review of these requirements.

Mr. Sukhjinder Singh, Wajeeh Butt - Comcast

Jennifer Andreoli-Fang, Dhawal Moghe, Jean-François Mulé, Stuart Hoggan, Phyllis O'Connell – CableLabs

Bernie McKibben, CableLabs

Appendix II Revision History

The following Engineering Changes have been incorporated in WR-SP-WiFi-GW-I02-120216.

ECN	ECN Date	Summary
WiFi-GW-N-11.0003-1	6/13/11	Inclusion of both the "Branded SSID" and the "Common Operator SSID" models in the Wi-Fi Gateway specification
WiFi-GW-N-11.0007-2	2/6/2012	802.1ad for traffic forwarding

The following Engineering Changes have been incorporated in WR-SP-WiFi-GW-I03-140311.

ECN	ECN Date	Summary	ECN Author
WiFi-GW-N-12.0010-3	9/4/2012	GRE encapsulation for traffic forwarding	McKibben
WiFi-GW-N-12.0011-1	11/5/2012	Add the support for 802.11ac	Li
WiFi-GW-N-14.0016-2	2/17/2014	PMIPv6	Coppola