Wireless Specifications

Wi-Fi Requirements for Cable Modem Gateways

WR-SP-WiFi-GW-I06-250801

ISSUED

DISCLAIMER

Document Status Sheet

Document Control Number	WR-SP-WiFi-GW-I06-250801			
Document Title	Wi-Fi Requirements for Cable Modem Gateways			
Revision History	I01 – Released 05/20/2010 I02 – Released 02/16/2012 I03 – Released 03/11/2014 I04 – Released 12/01/2014 I05 – Released 05/15/2015 I06 – Released 08/01/2025			
Date	August 1, 2025			
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; may include several alternative requirements for consideration.

Draft A document that is considered largely complete but is undergoing review by members and vendors. Drafts are susceptible to substantial change during the review process.

Issued A public document that has undergone rigorous member and vendor review, supports cross-vendor interoperability, and is suitable for certification/qualification testing. Issued specifications are subject to the Engineering Change process.

Closed A static document that has been reviewed, tested, validated, and closed to further Engineering Change requests to the specification through CableLabs.

Trademarks

Table of Contents

List of Figures

List of Tables

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 [802.11n] and [802.11ax] Wi-Fi air interfaces on the 2.4 GHz frequency band and [802.11ac] and [802.11ax] Wi-Fi air interfaces on the 5 GHz frequency band with a [MULPI4.0] cable modem. In addition, these requirements are also targeted at deployment scenarios that have a standalone access point (AP) with the same Wi-Fi air interfaces. 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.

"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, for example, a particular marketplace requires it or because it enhances the product; 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.

At the time of publication, the editions indicated were valid. All references are subject to revision, and parties to agreement based on this specification are encouraged to investigate the possibility of applying the most recent editions of the documents listed below. References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific. For a non-specific reference, the latest version applies.

[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, 2012

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

[802.11ac] IEEE 802.11ac: Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz, December 2013

[802.11ax] IEEE 802.11ax 2021: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN, 2021

[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: 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: Amendment 5: Enhancement for Higher Throughput, 2009

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

[802.1Q] IEEE 802.1Q: Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks, 2011

[802.1X] IEEE 802.1X: Port-Based Network Access Control, 2010

[CANN DHCP Reg] CableLabs' DHCP Options Registry, CL-SP-CANN-DHCP-Reg-I17-220831, Cable Television Laboratories, Inc. https://account.cablelabs.com/server/alfresco/4966ca26-2cee-40ef-932f-280e869758a5

[HS2.0] Hotspot 2.0 Specification Phase 1 Version 0.41, 2012

[MULPI4.0] DOCSIS 4.0 MAC and Upper Layer Protocols Interface Specification, CM-SP-MULPIv4.0-I09-250627, June 27, 2025, Cable Television Laboratories, Inc.

[RFC 2131] IETF RFC 2131, Dynamic Host Configuration Protocol, March 1997

[RFC 2132] IETF RFC 2132, DHCP Options and BOOTP Vendor Extensions, March 1997

[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 3315] IETF RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), 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 3646] IETF RFC 3646 DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6), December 2003

[RFC 4014] IETF RFC 4014, Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) RelayAgent Information Option, February 2005

[RFC 4282]	IETF RFC 4282, The Network Access Identifier, December 2005
[RFC 4372]	IETF RFC 4372, Chargeable User Identity, January 2006
[RFC 4594]	IETF RFC 4594, Configuration Guidelines for DiffServ Service Classes, August 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
[RFC 7170]	IETF RFC 7170, Tunnel Extensible Authentication Protocol (TEAP) Version 1, May 2014
[RFC 9190]	IETF RFC 9190, EAP TLS 1.3: Using the Extensible Authentication Protocol with TLS 1.3, February 2022
[WiFi MGMT]	WiFi Provisioning Framework Specification, WR-SP-WiFi-MGMT-I09-220621, June 21, 2022, Cable Television Laboratories, Inc.
[WMM]	Wi-Fi Alliance: Wi-Fi Multi-Media QoS based on 802.11e, Version 1.1
[WPA3]	Wi-Fi Alliance: Wi-Fi Protected Access 3, Version 3.4, October 2024
[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-I22-240503, May 3, 2024, Cable Television Laboratories, Inc.
[RFC 3947]	IETF RFC 3947, Negotiation of NAT-traversal in the IKE, January 2005
[RFC 3948]	IETF RFC 3948, ESP Encapsulation of the IPS ESP Packets, January 2005
[RFC 4301]	IETF RFC 4301, Security Architecture for the Internet Protocol, December 2005
[RFC 5996]	IETF RFC 5996, Internet Key Exchange Protocol Version 2 (IKEv2), September 2010
[WiFi-ROAM]	Wi-Fi Roaming Architecture and Interfaces Specification, WR-SP-WiFi-ROAM-I04-141201, December 1, 2014, Cable Television Laboratories, Inc.

2.3 Reference Acquisition

- 3GPP: The 3rd Generation Partnership Project, c/o ETSI, 650 Route des Lucioles, 06921 Sophia Antipolis CEDEX, France; www.3gpp.org
- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone: +1 303-661-9100; Fax: +1 303-661-9199; www.cablelabs.com
- IEEE: Institute of Electrical and Electronics Engineers, 3 Park Avenue, 17th Floor, New York, NY 10016-5997; Phone: +1 212-419-7900; Fax: +1 212-752-4929; www.ieee.org
- IETF: Internet Engineering Task Force Secretariat, c/o Association Management Solutions, LLC (AMS), Fremont, CA 94538; Phone: +1 510-492-4080, Fax: +1 510-492-4001; http://www.ietf.org
- Wi-Fi Alliance, 10900-A Stonelake Boulevard, Suite 195, Austin, TX 78759; Phone: +1 512-498-9434 (498-WIFI); Fax: +1 512-498-9435; 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
ACS	auto configuration server
AES	Advanced Encryption Standard
ANI	access network identifier
AP	access point
APN	access point name
ARP	Address Resolution Protocol
BCE	binding cache entry
BRA	binding revocation acknowledgement
BRI	binding revocation indication
BSSID	basic service set identifier
BULE	binding update list entry
CM	cable modem
CMTS	cable modem termination system
DFS	dynamic frequency selection
DNS	domain name system
DOCSIS®	Data-Over-Cable Service Interface Specifications
DSCP	differentiated services (DiffServ) code point
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol - Tunneled Transport Layer Security
eSAFE	embedded service/application functional entity
FQDN	fully qualified domain name
GI	guard interval
GRE	generic routing encapsulation
GW	gateway
HFC	hybrid fiber-coax
HT	high throughput
LDPC	low density parity check
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
PBA	proxy binding acknowledgement
PBU	proxy binding update
PCO	protocol configuration options
PDN	packet data network

PEAP	Protected Extensible Authentication Protocol
PGW	packet data network gateway
PHY	Physical Layer
PMIPv6	Proxy Mobile IPv6
RA	router advertisement
RADIUS	Remote Authentication Dial In User Service
RRM	radio resource management
RS	router solicitation
SLAAC	stateless address autoconfiguration
SON	self-organizing network
SSID	service set identifier
STA	station
STBC	space time block code
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
VSA	vendor-specific attribute
WEP	wired equivalent privacy
Wi-Fi	wireless fidelity
Wi-Fi AP	Wi-Fi access point
Wi-Fi GW	Wi-Fi gateway
WMM	Wi-Fi multimedia
WPA	Wi-Fi Protected Access
WPA3	Wi-Fi Protected Access 3
WPA3-TM	WPA3 transition mode
WPA3-PCM	WPA3 personal compatibility mode
WPS	Wi-Fi Protected Setup

5 OVERVIEW

One configuration of the Wi-Fi GW considered in this specification integrates a [MULPI4.0] modem with an [802.11n] and [802.11ax] air interface on the 2.4 GHz frequency band and an [802.11ac] and [802.11ax] air interface on the 5 GHz frequency band, as illustrated in Figure 1. Other functional elements also may be integrated with the cable modem, but they 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 [MULPI4.0]. 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 integrated 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.

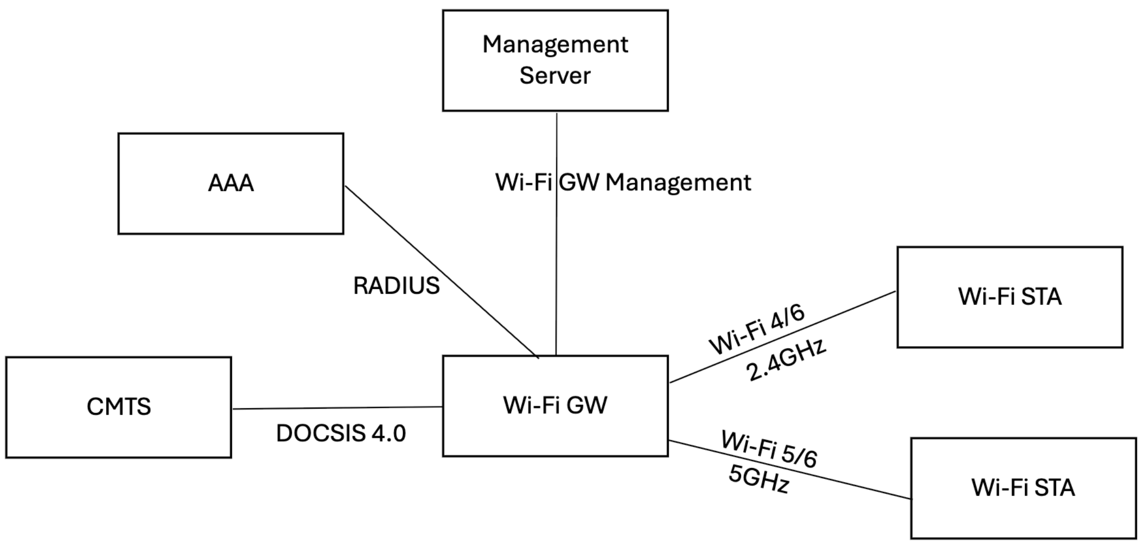

Figure 1 - Integrated Wi-Fi GW Interfaces

Another configuration of the Wi-Fi GW considered in this specification is a standalone AP with an [802.11n] and [802.11ax] air interface on the 2.4 GHz frequency band and an [802.11ac] and [802.11ax] air interface on the 5 GHz frequency band. The standalone GW is illustrated in Figure 2.

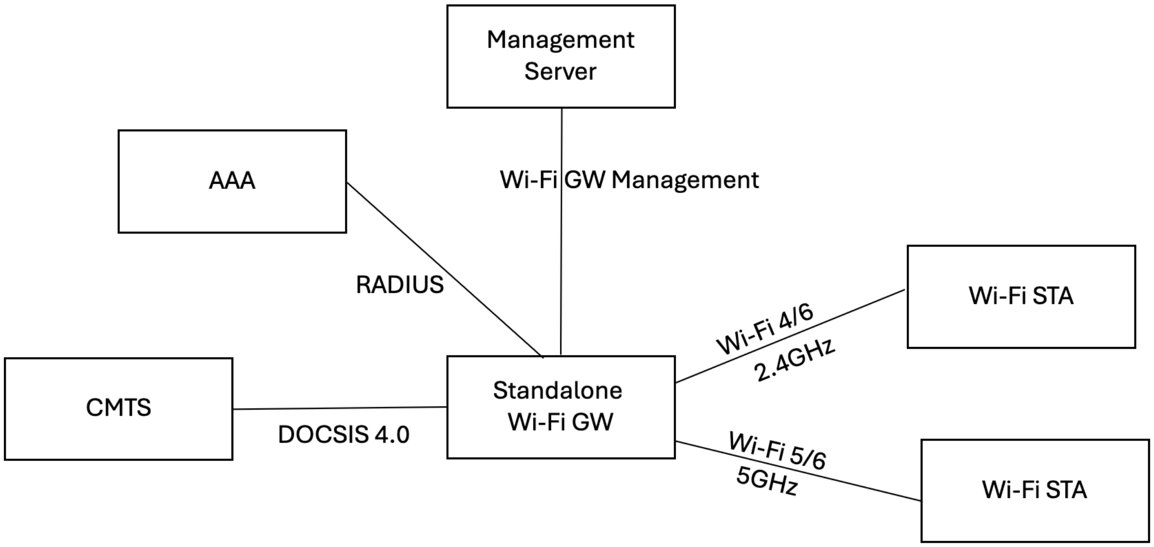

Figure 2 - Wi-Fi GW Interfaces for a Standalone Wi-Fi GW

In this document, without specific qualification, the term "Wi-Fi GW" refers to both the Wi-Fi GW and the standalone Wi-Fi GW.

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 DOCSIS 4.0 cable modems. The [MULPI4.0] 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 and OFDM and OFDMA technology. By bonding a minimum of five OFDM channels and 32 SC-QAM channels in the downstream and up to seven OFDMA channels and four SC-QAM channels in the upstream, DOCSIS 4.0 certified CMs can achieve up to 10 Gbps on the downstream and 6 Gbps on the upstream. To fully utilize the resources available on the cable access network, the wireless air interfaces of the Wi-Fi GW that is integrated with a DOCSIS 4.0 certified CM will match the rate that is achievable by the CM. Please see [MULPI4.0] for cable modem requirements.

6.1 802.11 Air Interface Requirements

In order to provide high performance wireless data service in conjunction with DOCSIS4.0as described in the following subsections, the Wi-Fi GW MUST support concurrent dual-band operations, with [802.11n] and [802.11ax] operating on the 2.4 GHz frequency band and [802.11ac] and [802.11ax] on the 5 GHz frequency band.

The Wi-Fi GW needs to support a 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. An 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 Support

The following requirements are applicable to the Wi-Fi GW's [802.11n] interface on the 2.4 GHz frequency band.

The Wi-Fi GW MUST support all mandatory features of the [802.11n] specification.

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 40 MHz 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 environments. The Wi-Fi GW operating in 802.11n mode MUST support the following MCS parameter sets as defined in [802.11n]: MCS0 - MCS23 for 20 MHz HT. Under favorable physical environments, 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 the 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 - MCS23 for 40 MHz HT if the 40 MHz channel is supported.

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

6.1.2 Requirements for 802.11ac Support

The following requirements are applicable to the Wi-Fi GW's [802.11ac] interface on the 5 GHz band.

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

- Short guard interval
- MCS 8 and 9 (256-QAM, r=3/4, r=5/6)
- Low density parity check (LDPC) channel coding
- Explicit transmit beamforming (TxBF)

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 MAY support MU-MIMO. The Wi-Fi GW MAY support space time blocking (STBC). The Wi-Fi GW MAY support 160 MHz and 80 Mhz+80 MHz channel widths.

The Wi-Fi GW SHOULD implement appropriate mechanisms to ensure overlap BSS (OBSS) coexistence in both the 2.4 GHz and 5 GHz frequency bands.

6.1.3 Requirements for Wi-Fi 6 Support

The following requirements are applicable to the Wi-Fi GW's [802.11ax] interface on the 2.4 GHz and 5 GHz frequency bands. The table below gives a list of all the Mandatory (M), Conditionally Mandatory (CM), and Optional (O) capabilities for a Wi-Fi GW to support [802.11ax]. For detailed definitions of each of these capabilities , refer to the following WFA documents.

MRD r1	https://www.wi-fi.org/system/files/members/Wi-Fi%206%20MRD%20v1.6.pdf
Wi-Fi 6 at 6 GHz	https://www.wi-fi.org/system/files/members/MRD_Wi-Fi-6-at-6-GHz_v1.4.pdf
MRD r2	https://www.wi-fi.org/system/files/members/Wi-Fi_6_R2_MRD_v1.2_0.pdf

Mandatory	Conditionally Mandatory	Optional
4 antenna support	LDPC Rx	Dynamic MU SMPS
A-MPDU with A-MSDU	LDPC Tx	MU-RTS trigger frame
Basic trigger frame in HE MU PPDU		Preamble puncturing
Beamforming sounding		UL extended range
Broadcast target wake time		
BSRP trigger frame		
Co-located BSS		
Compressed block Ack Rx(buffer size 256)		
Compressed block Ack Tx(buffer size 256)		
DL MU PPDU multi-tone (multiple resource units)		
DL MU-MIMO		
DL OFDMA		

Mandatory	Conditionally Mandatory	Optional
Extended sleep		
Extended sleep time		
Individual target wake time		
M-BSSID		
M-BSSID control frames		
MCS 8-9 Rx		
MCS 8-9Tx		
MCS 10-11 Rx		
MCS 10-11 Tx		
MU EDCA parameter set element		
MU-BAR trigger frame		
Multiple M-BSSID		
Operating mode control field		
Operating mode indication		
Operating mode subfield in A-Control Field		
Operating Mode UL MU Rx		
SU beamformee		
SU beamformer		
SU-MIMO		
Target wake time information frames		
TXOP RTS threshold		
UL MU control		
UL MU-MIMO		
UL OFDMA		

6.1.4 Interoperability

The Wi-Fi GW's [802.11ax] interface operating on the 2.4 GHz frequency band shares with legacy devices that are 802.11b, g, and n capable. 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 Wi-Fi devices on the 2.4 GHz frequency band. The Wi-Fi GW MUST support frame aggregation.

The [802.11ax] interface on the 2.4 GHz frequency band MUST support data rates with automatic fall back of 6 Mbps, 12 Mbps, and 24 Mbps in [802.11g] modes.

Because the Wi-Fi GW is required to support multiple SSIDs, the interoperability requirement is extended to the SSID level. The Wi-Fi GW's 802.11n interface on the 2.4 GHz frequency band MUST support both tri-mode (.11b/g/n) and single mode (e.g., .11n only) operations per SSID as defined in [802.11n]. It SHOULD also support the ability of the operator to configure the mode of operation using a field programmable mode lock option.

The Wi-Fi GW's [802.11ax] interface on the 5 GHz frequency band MUST meet all interoperability requirements mandated in [802.11ac]. The Wi-Fi GW SHOULD be interoperable with Wi-Fi certified [802.11a] and [802.11n] devices as enabled or disabled separately by the operator provisioning.

The Wi-Fi GW SHOULD support disassociating any associated client Wi-Fi device as soon as its average MCS, measured during an operator defined time interval, drops below an operator-defined threshold.

6.1.5 Channel Selection

The Wi-Fi GW MUST support auto channel selection by the following two methods per [802.11] during initialization and normal operation: (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 for the 2.4 GHz frequency band.

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

The Wi-Fi GW SHOULD let MSOs provide a means for their subscribers to select between the Manual and Auto channel selection modes (e.g., through a configuration web page). If Wi-Fi GW supports this feature, it MUST reject manual configuration of channels that cannot be used.

6.1.6 Antenna Requirements

Multiple-input, multiple-output (MIMO) utilizes multiple transmitter and receiver antennas to improve system performance. The Wi-Fi GW MUST support MIMO Power Save by utilizing multiple antennas only on an as-needed basis based on Automatic Power Save Delivery as defined in [WMM]. The Wi-Fi GW MUST support the minimum of 3x3 MIMO. It SHOULD support 4x4 MIMO. The Wi-Fi GW MUST support three spatial streams with 3x3:3 configuration and two spatial streams with 3x3:2 configuration. If the Wi-Fi GW supports 4x4 MIMO, it MUST support three spatial streams with 4x4:3 configuration and two spatial streams with 4x4:2 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.

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.

6.1.7 Transmit Power, Range, Receiver Sensitivity

The Wi-Fi GW MUST have a conducted aggregate maximum transmit power equal to or greater than 4 dB below the maximum transmit power per country regulatory body code (e.g., 400 mW or 26 dBmV for FCC regulated devices) with a 0 to - 3 dB tolerance across all channels in the 2.4 GHz band.

The Wi-Fi GW MUST have a conducted aggregate maximum transmit power equal to or greater than 4 dB below the maximum transmit power per country regulatory body code with a 0 to - 3 dB tolerance across all channels in the 5 GHz UNIFI bands. The Wi-Fi GW MUST NOT exceed the maximum limits for radiated power according to regional regulations.

Figure 3 below illustrates the percent reduction in area covered at an 802.11n MCS7 data rate at 2.4 GHz as conducted TX power decreases with constant 6 dB. Antenna using free space path loss equation with path loss coefficient of 35 (Path Loss = 20logF + 35 log -28).

For example, conducted TX power of 26 dBm will amount to a 60% area coverage of 65 Mbps when compared to area coverage at 30 dBm TX power FCC 'not to exceed' TX power limit.

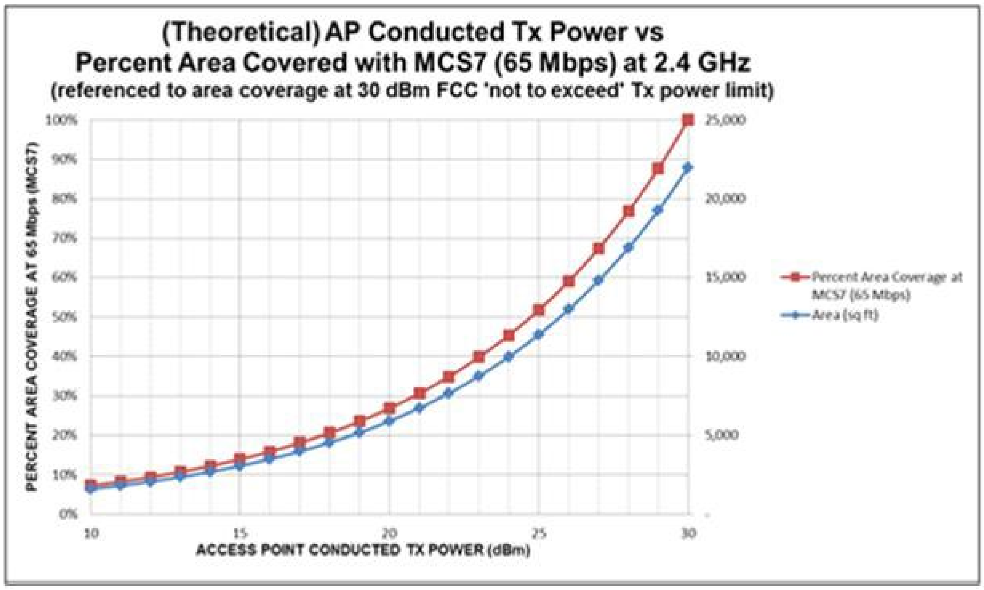

Figure 3 - Theoretical AP Conducted TX Power vs. Percent Area Covered with MCS7 (65 Mbps) at 2.4 GHz

6.1.8 Air Interface Performance

The 802.11n air interface defines a number of MCS parameter sets that can be utilized to match varying physical environments. 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.

6.1.9 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.

6.1.10 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; and
- 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 need to 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 MUST support the following independently configurable parameters on a per SSID basis: the SSID name, security type, [WMM] enable/disable, bridge mode enable/disable, NAT 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 addresses.

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 provide a method for the subscriber to disable the wireless interface impacting only the subscriber's SSID. The Wi-Fi GW SHOULD let MSOs provide a means for their subscribers to shut down each radio interface and, thus, disable all the SSIDSs, including the operator-configured ones (e.g., through a local configuration webpage). The Wi-Fi GW MUST NOT impact or provide any information regarding the operator-configured SSIDs when the subscriber configures the subscriber-designated SSID.

The Wi-Fi GW MUST provide the ability to read out the state of each radio interface (turned on/shut down) by the operator.

The Wi-Fi GW MUST support configuring a maximum number of associated client Wi-Fi devices on a per-SSID basis. When a client Wi-Fi device tries to associate on an SSID where the limit has been reached, the Wi-Fi GW MUST deny the association.

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.

6.1.11 Security Requirements

The Wi-Fi GW is designed to offer and negotiate the strongest security that the subscriber device can support. Use of Wired Equivalent Privacy (WEP) is deprecated. Use of Wi-Fi Protected Access (WPA) is discouraged. Therefore, the Wi-Fi GW supports the recommended Wi-Fi Alliance certified encryption and authentication methods, including Wi-Fi Protected Access 3 (WPA3) and Wi-Fi Protected Access 2 (WPA2).

The Wi-Fi GW MUST support configuring the following security operating modes as specified in [WPA3] on a per-SSID basis:

- WPA2-Personal Only mode
- WPA3-Personal Only mode
- WPA3-Personal Transition mode
- WPA3-Personal Compatibility mode
- WPA3-Enterprise Only mode
- WPA3-Enterprise Transition mode

When configured to operate in WPA3-Enterprise Only mode or WPA3-Enterprise Transition mode, the Wi-Fi GW MUST support the following EAP methods:

- Protected Extensible Authentication Protocol (PEAP)
- Extensible Authentication Protocol - Tunneled Transport Layer Security (EAP-TTLS) as per [RFC 5281]
- Extensible Authentication Protocol - Transport Layer Security (EAP-TLS) as per [RFC 5216]
- Extensible Authentication Protocol - Transport Layer Security 1.3 (EAP-TLS 1.3) as per [RFC 9190]

When configured to operate in WPA3-Enterprise Only mode or WPA3-Enterprise Transition mode, the Wi-Fi GW SHOULD support the following EAP method:

- Tunnel Extensible Authentication Protocol (TEAP) Version 1 as per [RFC 7170]

The Wi-Fi GW SHOULD support the WPS pairing button. The use of the PIN methods for initial Wi-Fi device pairing per [WPS] is discouraged. 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 allow putting 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 allow bridging of SSIDs by assigning to the same VLAN.

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.

6.1.12 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.

The Wi-Fi GW SHOULD support a mechanism to trigger a neighbor report. When the neighbor report is triggered on a Wi-Fi GW that supports it, either by a timing constraint or by a manual trigger, the Wi-Fi GW MUST perform a neighbor report in a MIB table.

The Wi-Fi GW that supports a neighbor report MUST support clearing the results from a previous neighbor report.

The Wi-Fi GW SHOULD support a mechanism to trigger a client report that includes information about the currently connected/associated client devices. If supported, the Wi-Fi GW SHOULD report the information listed per the [WiFi MGMT], section 6.2 Management Interface Protocol Requirements (Table 2), the "AssociatedDevice" data model.

The Wi-Fi GW SHOULD have the capability to scan the channel spectrum, calculate the available channel spectrum capacity per bandwidth (e.g., 20, 40, 80 MHz), and detect non-Wi-Fi interfaces. Additionally, the Wi-Fi GW SHOULD detect and classify the signal source (Bluetooth, Wi-Fi, ZigBee, cordless phone, microwave oven, radar, other). For the purpose of signal classification, the Wi-Fi GW does not need to be able to decode those signals but only to understand their type by examining their spectral signatures or other methods. If Wi-Fi GW has this channel diagnostic capability, it MAY use the same radio for spectrum analysis and for serving client devices or it MAY use different radios. If Wi-Fi GW has this channel diagnostic capability, it MUST support remote enabling or disabling of this capability. If Wi-Fi GW has this channel diagnostic capability, it MUST be able to support the management of this feature per the [WiFi MGMT] "Device.WiFi.ChannelWiFiDiagnostics" data model and the corresponding SNMP MIBs.

6.2 Generic Routing Encapsulation

This section describes Wi-Fi GW requirements to support generic routing encapsulation (GRE) [RFC 2784] of layer 2 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 broadband access network 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 2 tagging techniques, including 802.1ad, can be used in combination with GRE encapsulation. Layer 2 tags are encapsulated along with the balance of the user layer 2 packet within the GRE tunnel. VLANs are preserved with this GRE approach.

NOTE: Differentiated services code point (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.
- For the integrated Wi-Fi GW, the source IP address in transport IP header MUST be set to the WAN IP address (public IP).
- For the standalone Wi-Fi GW, the source IP address MAY be set by a NAT entity in the connected external broadband access device (e.g., cable gateway).
- 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. For the integrated Wi-Fi GW, this can be used to classify traffic from SSIDs into different DOCSIS service flows based on the DSCP marking on the GRE tunnel packets. For the standalone Wi-Fi GW, the DSCP marking can be used by any network node along with the GRE tunnel data path for QoS treatment. 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 the 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 IPv4-only, IPv6-only, or dual-stack capable nodes. Furthermore, PMIPv6 supports a IPv4-only or IPv6-only transport network. Though the protocol name suggests that PMIPv6 is an IPv6-based protocol, the protocol has complete support for IPv4-only mobile nodes and an 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 6.1.9 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; therefore, it 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. The 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 upon a globally defined policy profile on the W-Fi GW. Policy profile also can be defined on a per SSID basis. 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 GW 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 GW will interwork with a generic [RFC 5213] compatible LMA. This is suited for MSO-managed public Wi-Fi deployment scenarios, which do not require integration to a third-party mobile operator's packet core.

b) Wi-Fi hotspot solution that supports trusted WLAN integration with EPC—In this model, PMIPv6 LMA functionality is co-located with the 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 4 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.

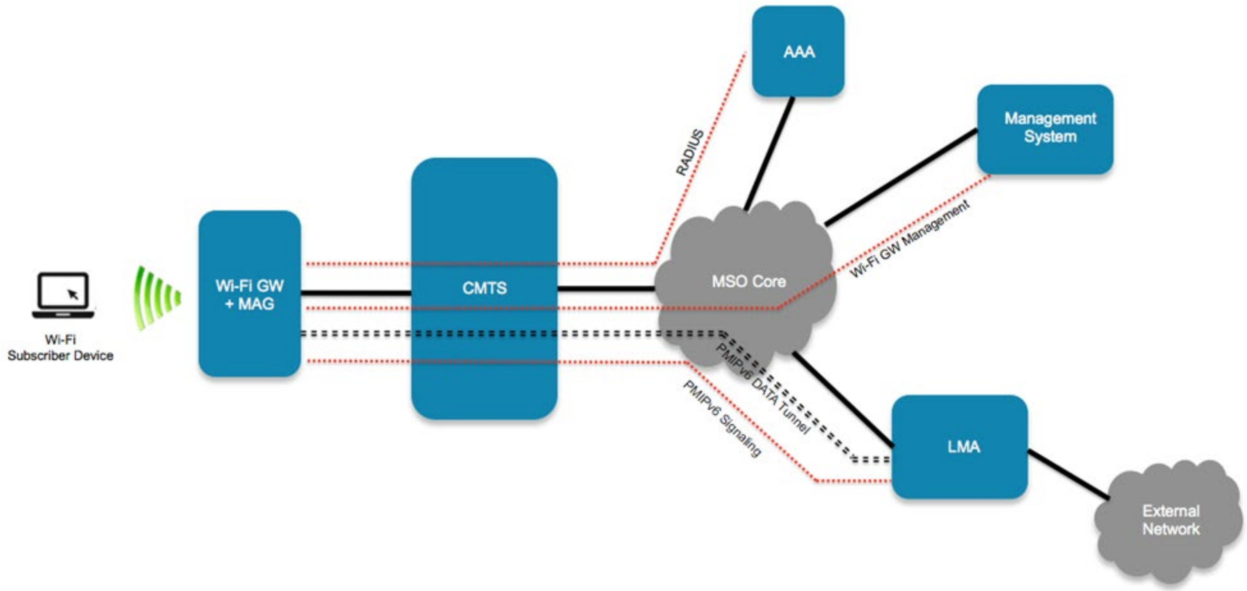

Figure 4 - PMIPv6 Architecture Using Wi-Fi GW MAG

Basic protocol operation at a high level is illustrated using the call flow provided in Figure 5 below.

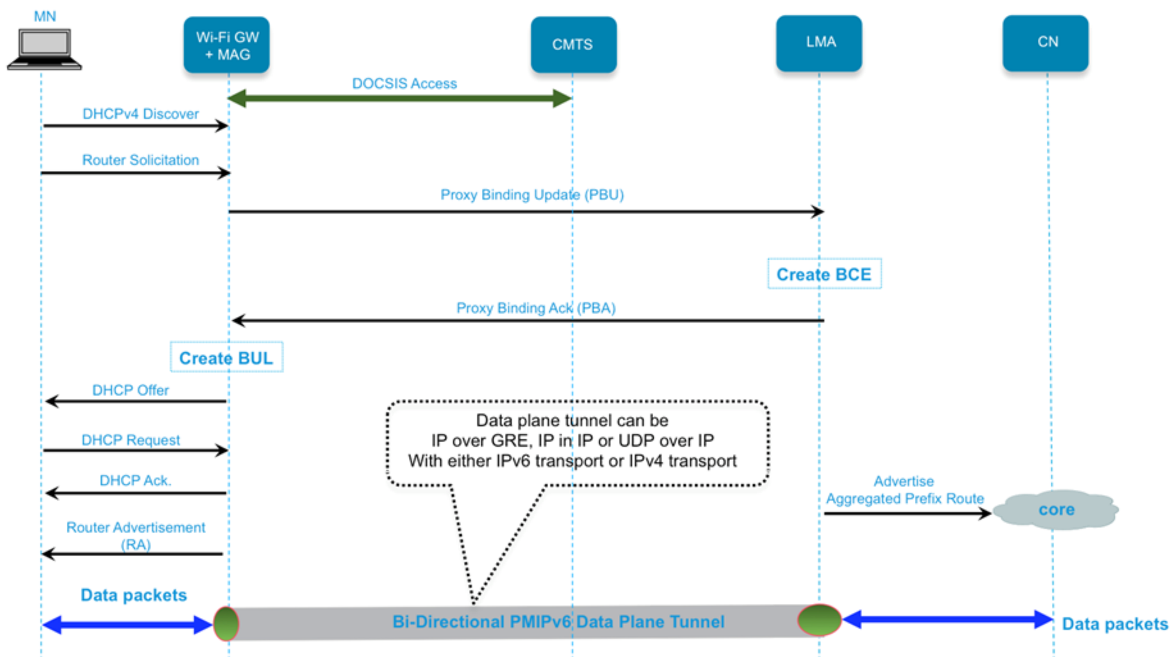

Figure 5 - Sample PMIPv6 Signaling Call Flow

In this call flow, it is assumed that client authentication is already completed. This call flow illustrates dual stack-based client addressing. A 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. Upon detecting the mobile node attachment, the MAG builds a proxy binding update (PBU) message. The 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. Upon 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). The 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, the LMA sends a proxy binding acknowledgement (PBA) message to the MAG. The PBA message carries the IPv4 address and the IPv6 prefix for the client. It may also carry protocol configuration information (PCO) such as domain name system (DNS) server IP address, domain name, etc. The 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, the MAG completes the address assignment through DHCP for IPv4 and stateless address autoconfiguration (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

A Wi-Fi GW that implements PMIPv6 MAG functionality will support the following:

- The Wi-Fi GW MUST support the configuration of a global PMIPv6 policy profile. This global profile will be used to generate the signaling messages toward the LMA upon a client attachment trigger on the Wi-Fi side.
- The Wi-Fi GW MUST support configuration of a home LMA IP address or FQDN name of the home LMA in the policy profile.
- The Wi-Fi GW may support the configuration of an APN in the policy profile when interworking with a generic LMA per [RFC 5213].
- The Wi-Fi GW MUST support the configuration of an APN in the policy profile when interworking with a 3GPP PGW/LMA over the S2a PMIPv6 interface.
- The Wi-Fi GW may support the configuration of a PDN type in the policy profile when interfacing with a generic LMA per [RFC 5213].
- The Wi-Fi GW MUST support the configuration of a PDN type in the policy profile when interfacing with a 3GPP PGW/LMA over the S2a PMIPv6 interface.
- The Wi-Fi GW MUST support the configuration of PMIPv6 policy profile on a per-SSID basis.
- The Wi-Fi GW MUST support AAA override of PMIPv6 policy profile on a per-client basis.
- For IPv4 clients, the Wi-Fi GW MUST support the following client attachment triggers: (a) DHCP discover, (b) DHCP request, (c) Unicast ARP, and (d) broadcast ARP.
- For IPv6 clients, the Wi-Fi GW MUST support the following client attachment triggers: (a) router solicitation and (b) neighbor solicitation.
- For IPv4 client addressing, the 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, the Wi-Fi GW MUST support SLAAC and assign the LMA-assigned IPv6 prefix using unicast RA.
- For IPv6 client, the Wi-Fi GW should use the 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, the 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 should also use the domain search list option to specify the domain search list the client is to use when resolving host names with DNS.

- For IPv6 client addressing, the Wi-Fi GW may support stateful DHCPv6 server functionality and assign the LMA-assigned IPv6 prefix to the client via DHCPv6.
- The Wi-Fi GW MUST include the configured APN name in the PBU message.
- The Wi-Fi GW may include an access network identifier (ANI) in the PBU message. ANI may be configurable at the global level or on a per-SSID basis. If no ANI is configured, the Wi-Fi GW may include the SSID to which the client is associated as the ANI and include it in the PBU message.
- The Wi-Fi GW MUST send a de-registration PBU message when a Wi-Fi client that has an active BUL entry is disconnected from the radio network.
- The Wi-Fi GW MUST delete an existing BUL entry for a client upon receiving a BRI message from LMA. After the deletion of the BUL entry, the Wi-Fi GW must send a BRA message in response to the BRI.
- The Wi-Fi GW MUST support the binding of multiple clients to a single PMIPv6 data plane tunnel.
- As specified in Section 6.1.9 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

A Wi-Fi GW that implements PMIPv6 MAG functionality will support the following:

- The Wi-Fi GW MUST support dynamic establishment/tear-down of layer 3 bi-directional data plane tunnel with GRE encapsulation mode.
- The Wi-Fi GW may support data plane tunnels using other encapsulation options as defined in [RFC 5844] and [RFC 5845]
- The Wi-Fi GW MUST simultaneously support multiple PMIPv6 data plane tunnels with different LMAs.
- The 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.
- The 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, the Wi-Fi GW MUST support proxy ARP for the client's IP destination addresses in the client's home IPv4 subnet.
- For IPv4 clients, the 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 6.1.9 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. The bandwidth from the broadband service provider termination device to a standalone AP can be negotiated in advance.

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 broadband interface as configured by the operator.

The Wi-Fi GW MUST support traffic prioritization mapped per SSID to a specific class of service bits as defined by 802.1p in [802.1D] and follow the VLAN tags as defined in [802.1Q]. The Wi-Fi GW MUST support all the traffic prioritization procedures and capabilities called out in the IEEE 802.11 specification.

6.5 RADIUS Client Interface

The Wi-Fi Roaming Architecture and Interfaces 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. 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 [WiFi-ROAM] for further information on the use of RADIUS attributes per the RFCs listed above.

The Wi-Fi GW MUST support the RADIUS session-timeout attribute as defined in [RFC 2865] and MUST disassociate the client Wi-Fi device if the session is expired.

Following [RFC 4282], the Wi-Fi GW MUST support a network access identifier (NAI) length of at least 72 octets.

DHCPv4 (see [RFC 2131] and [RFC 4014]) is used to obtain the IPv4 configuration data for standalone APs. DHCPv6 (see [RFC 3315]) is used to obtain the IPv6 configuration data for standalone APs. The standalone AP RADIUS information can be pre-configured or can be obtained through DHCP. If pre-configuration is absent, the standalone AP MUST request RADIUS server option, inside the DHCP message as per [RFC 4014]. Additionally, if pre-configuration is absent, the standalone AP MUST request CL_V4OPTION_RADIUS_SERVER (7) as defined in [CANN DHCP Reg] when provisioning in IPv4. If pre-configuration is absent, the standalone AP MUST request CL_V6OPTION_RADIUS_SERVER (41) as defined in [CANN DHCP Reg].

To avoid dependency on broadband service providers, the DHCP server SHOULD provide RADIUS with a server IP address rather than FQDN. For accounting purposes, the standalone AP MUST perform reachability tests to the RADIUS server at short intervals. The reachability tests can be constant ICMP message exchanges at regular intervals or any proprietary method that allows verifying message exchange between standalone AP and RADIUS server IP address.

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].

6.6.2 Wi-Fi Radio Resource Management

This section describes Wi-Fi GW requirements for supporting RRM/SON functionality. The objective of Wi-Fi SON is to manage large numbers of APs in dense deployments while reducing operational costs. SON capabilities periodically update AP settings, such as transmit power levels, in order to increase user traffic throughput and reduce interference among neighboring APs. Wi-Fi SON approaches MAY include techniques supported by each AP for immediate response to air interface conditions and support for a central SON server that provides the high level management of specific parameters. The Wi-Fi GW MUST support read and write parameters as defined in [WiFi MGMT]. The use of a Wi-Fi SON server is optional in an MSO network, but if used, the operators need a standardized interface for centralized control of RRM/SON parameters to and from a Wi-Fi GW. The standardized interface at the northbound interface of the Wi-Fi GW MUST support either TR-069 or SNMP for network management interface. If TR-069 is used, the Wi-Fi GW MUST support one interface to an auto configuration server (ACS) and MAY support an additional northbound interface.

The standalone AP MUST support TR-069-based configuration. The standalone AP MAY support SNMP-based configuration. The standalone AP TR-069 ACS information can be pre-configured or can be obtained through DHCP. If pre-configuration is absent, the standalone AP MUST request DHCPv4 option CL_V4OPTION_ACS_SERVER (6) as defined in [CANN DHCP Reg] in order to receive TR-069 ACS information when provisioning in IPv4. If pre-configuration is absent and the standalone AP is provisioning in IPv6, the standalone AP MUST request DHCPv6 option CL_V6OPTION_ACS_SERVER (40) as defined in [CANN DHCP Reg].

In addition to the above DHCP options, the standalone AP MUST request DNS option 6 as defined in [RFC 2131] when provisioning in DHCPv4. When provisioning in DHCPv6, the standalone AP MUST request DNS option 23 as defined in [RFC 3315].

In the case of standalone Wi-Fi GW, if TR-069 server is not reachable, the operator hotspot SSID(s) MUST be disabled.

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.

6.8 +Hotspot 2.0

The Wi-Fi GW SHOULD support Hotspot 2.0 (HS2.0) to enable the use of HS2.0 for the discovery and selection of the access network. The use of HS2.0 will allow a HS2.0-enabled STA (station) with the HS2.0 credentials to automatically select and connect to an enabled WLAN on the gateway as defined by the STA credentials. There are two parts of the HS2.0 specification that will need to be included in the Wi-Fi GW to enable support for HS2.0 on the Wi-Fi GW. These apply to both a residential and enterprise gateway equally. Through provisioning, HS2.0 can be enabled as needed or disabled if HS2.0 is not intended to be used.

To support HS2.0, all requirements defined in Section 2.1, Required Capabilities of APs, and Section 2.3, Requirements for Hotspot Operators, of the HS2.0 Release 1 specification, [HS2.0] MUST be supported on the AP. The requirements on the Wi-Fi GW are to ensure the Wi-Fi GW can support the HS2.0 functionality. The requirements for the hotspot operator are to ensure the Wi-Fi GW can be controlled and serve as a hotspot for the operator that is deploying the Wi-Fi GW.

6.9 Community Wi-Fi

Community Wi-Fi comprises a public SSID, which is configured on a Wi-Fi GW, in order to provide Internet access to subscribers while outside of their home networks. The following section defines the requirements necessary to enable support for community Wi-Fi beyond what has been listed above.

6.9.1 Traffic Prioritization

The Wi-Fi GW MUST support the traffic prioritization procedures and capabilities called out in [WMM].

The Wi-Fi GW MUST support downstream DSCP to WMM traffic priority mapping. The default values are as listed in Table 1 and MAY be configurable by the operator. Upstream DSCP values MAY be copied by the Wi-Fi GW to the tunnel header in order to provide continuous classification and prioritization.

Table 1 - DSCP to WMM Mapping

DSCP Traffic Type	DSCP Value	WMM
Control	56 (0x38)	VO (Voice)
Audio	46 (0x2E)	VO (Voice)
Video	40 (0x28)	VI (Video)
Best Effort	0 (0x00)	BE (Best Effort)
Excellent Effort	24 (0x18)	BE (Best Effort)
Background	8 (0x08)	BK (Background)

The Wi-Fi GW MUST support the ability to prioritize traffic on a per-SSID basis in the downstream direction. The Wi-Fi GW SHOULD support the ability to prioritize traffic on a per-SSID basis in the upstream direction.

6.9.2 SSID Prioritization

The Wi-Fi GW MUST support the ability to steer a user device to their private SSID when available. This is necessary to ensure the user has access to any local network devices (e.g., printers, file servers, media renderers), as well as providing the user with their expected level of service.

6.9.2.1 Admission Control

Wi-Fi admission control MUST be available (per Section 6.7) and could be leveraged for network selection by blacklisting the user from the public SSID. The Wi-Fi GW SHOULD, upon a client associating with the private SSID, add the client's MAC address to the public SSID blacklist table. Upon the client associating to any SSID for which the functionality is configured, the Wi-Fi GW SHOULD check a local blacklist and allow or deny the association based on its presence in the blacklist. The blacklist SHOULD be able to hold at least 64 entries, and SHOULD be configurable to clear the list upon reboot or when manually ordered to do so. The Wi-Fi GW SHOULD list the entries in the blacklist table, via any local or remote management interface.

6.9.2.2 Interworking Information Element

The interworking information element (IE) MAY also be used to steer a client to a preferred network by broadcasting an access network type, which can be weighted based on the service. Operators may broadcast an interworking IE with Access Network Type = 2, which signifies a chargeable public network. The client will treat this access network type as a hotspot, which will give it a lower priority than a known private network in the same location. The Wi-Fi GW MUST broadcast this IE on the public SSID, enabling clients to make network selection decisions based on the access network type. Refer to Section 8.4.2.94 of [802.11] for further information.

6.9.3 Considerations for Standalone Wi-Fi GW

When standalone Wi-Fi GWs are used for community Wi-Fi, there is a security/privacy risk introduced, as the Ethernet link between the standalone AP and the broadband access is unsecure.

The standalone Wi-Fi GW SHOULD use IPSec in tunnel mode for connectivity to the core network. If this architecture is used, Wi-Fi GW SHOULD support:

- IPSec in ESP tunnel mode,
- UDP encapsulation for NAT traversal (NAT-T) of IPSec, and
- pre-shared keys (PSK) or the dynamic key exchange mechanism via IKEv2.

Appendix I Acknowledgements

On behalf of the cable industry and our member companies, 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.

Contributor	Company Affiliation
Carol Ansley, Kurt Lumbatis, Dan Torbet	Arris
Rajat Ghai	Benu Networks
Gordon Li, John McQueen	Broadcom
Jennifer Andreoli-Fang, John Berg, Stephen Burroughs, Lili Hervieu, Stuart Hoggan, Neeharika Jesukumar, James Kim, Bernie McKibben, Dhawal Moghe, Jean-François Mulé, Phyllis O'Connell, Josh Redmore, Joey Padden, Mark Poletti, Vikas Sarawat, Luther Smith, Darshak Thakore	CableLabs
Sri Gundavelli, Charles Moreman	Cisco
Wajeeh Butt, Sukhijinder Singh	Comcast
Brent Bischoff, Baw Chng	Cox
Satish Mudugere	Intel
Praveen Srivastava, Roger Stafford	TWC
Gordon Verhagen	Ziggo

Appendix II Revision History

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

ECN Identifier	Accepted Date	Title of EC	Author
WiFi-GW-N-11.0003-1	6/13/11	Inclusion of both the "Branded SSID" and the "Common Operator SSID" models	Moghe
WiFi-GW-N-11.0007-2	2/6/2012	802.1ad for traffic forwarding	McKibben

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

ECN Identifier	Accepted Date	Title of EC	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

The following Engineering Changes have been incorporated into WR-SP-WiFi-GW-I04-141201.

ECN Identifier	Accepted Date	Title of EC	Author
WiFi-GW-N-14.0018-1	8/11/2014	Incorporation of Hotspot2.0	Smith
WiFi-GW-N-14.0019-1	8/11/2014	Wi-Fi Radio Resource Management	Allanki
WiFi-GW-N-14.0020-1	8/11/2014	Additional 802.11ac requirements for Wi-Fi GW	Li
WiFi-GW-N-14.0021-3	9/22/2014	Incorporation of Community Wi-Fi	Redmore
WiFi-GW-N-14.0024-5	10/20/2014	Additional Air Interface Requirements	Babaei
WiFi-GW-N-14.0025-3	10/27/2014	RF Performance	Poletti
WiFi-GW-N-14.0026-3	11/3/2014	Adding requirements for spectrum analysis capability	Babaei

The following Engineering Change was incorporated into WR-SP-WiFi-GW-I05-150515.

ECN Identifier	Accepted Date	Title of EC	Author
WiFi-GW-N-15.0027-2	4/20/2015	Adding requirements for Wi-Fi GW with Stand-alone AP	Babaei

The following Engineering Change was incorporated into WR-SP-WiFi-GW-I06-250801.

ECN Identifier	Accepted Date	Title of EC	Author
WiFi-GW-N-25.0037-1	6/25/2025	Adding support for Wi-Fi 6	Jesukumar

✻ ✻ ✻