Wireless Specifications

Wi-Fi Requirements for Cable Modem Gateways

WR-SP-WiFi-GW-I02-120216

ISSUED

Document Status Sheet

Document Control Number:	WR-SP-WiFi-GW-I02-120216			
Document Title:	Wi-Fi Requirements for Cable Modem Gateways			
Revision History:	I01 - Released 05/20/10 I02 – Released 02/16/12			
Date:	February 16, 2012			
Status:	~~Work in Progress~~	~~Draft~~	**Issued**	~~Closed~~
Distribution Restrictions:	~~Author Only~~	~~CL/Member~~	~~CL/ Member/ Vendor~~	**Public**

Key to Document Status Codes

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

Trademarks

Contents

1 SCOPE 1

1.1 Introduction and Purpose 1
1.2 Requirements 1

2 REFERENCES 2

2.1 Normative References 2
2.2 Informative References 3
2.3 Reference Acquisition 3

3 TERMS AND DEFINITIONS 4

4 ABBREVIATIONS AND ACRONYMS 5

5 OVERVIEW 6

6 REQUIREMENTS 7

6.1 802.11 Air Interface Requirements 7
6.1.1 Requirements for 802.11n Wi-Fi GWs for use with DOCSIS 3.0 CMs 7
6.1.2 Interoperability 8
6.1.3 Channel Selection 8
6.1.4 Antenna Requirements 9
6.1.5 Transmit Power, Range, Receiver Sensitivity 9
6.1.6 Air interface performance 9
6.1.7 Other Requirements 9
6.1.8 Configurations of SSIDs 9
6.1.9 Security Requirements 11
6.1.10 Other Requirements 12
6.2 Resources and Traffic Priority 12
6.3 RADIUS Client Interface 12
6.4 Management Interface Requirements 12
6.4.1 Status and Performance Reports 13
6.5 Configured Admission Control 13

APPENDIX I ACKNOWLEDGEMENTS 14

APPENDIX II REVISION HISTORY 15

Figures

Figure 1 - Wi-Fi GW Interfaces 6

This page left blank intentionally.

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] 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.

[802.11b] 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-I17-111117, November 17, 2011, Cable Television Laboratories, Inc.

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

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

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

[WiFi MGMT] Wi-Fi Management Interface Requirements, WR-SP-WiFi-MGMT-I02-120216, February 16, 2012, 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.

[eRouter] IPv4 and IPv6 eRouter Specification, CM-SP-eRouter-I07-111117, November 17, 2011, Cable Television Laboratories, Inc.

[WiFi-ROAM] Wi-Fi Roaming Architecture and Interfaces Specification, WR-SP-WiFi-ROAM- I02-120216, February 16, 2012, Cable Television Laboratories, Inc.

2.3 Reference Acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027;
  Phone +1-303-661-9100; Fax +1-303-661-9199; http://www.cablelabs.com
- Institute of Electrical and Electronics Engineers, (IEEE), http://www.ieee.org/web/standards/home/index.html
- 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/knowledge_center_overview.php?type=4

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
BSSID	Basic Service Set Identifier
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
HFC	Hybrid Fiber Coax
HT	High Throughput
MAC	Media Access Control
MCS	Modulation and Coding Scheme
MIMO	Multiple-input multiple-output
PEAP	Protected Extensible Authentication Protocol
PHY	Physical
RADIUS	Remote Authentication Dial In User Service
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] 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.

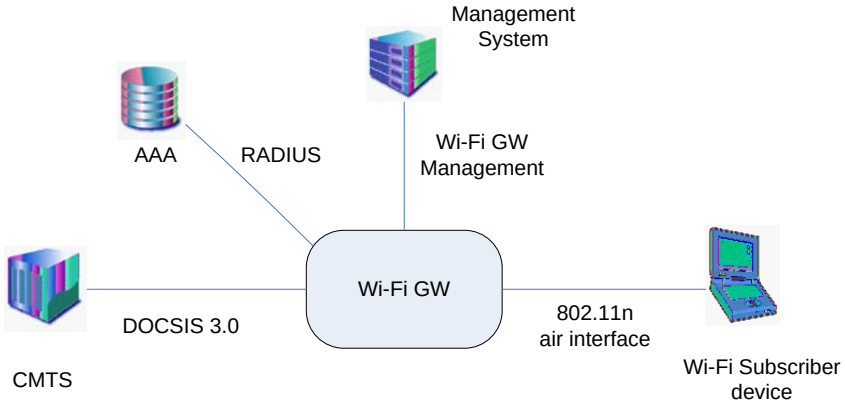

Figure 1 - Wi-Fi GW Interfaces

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 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].

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.

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.

6.2 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].

6.3 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.

6.4 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.

6.4.1 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].

6.5 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 Change has 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