Wireless Broadband Alliance

Driving next generation Wi-Fi experience

Carrier Wi-Fi Guidelines

The WBA Vision

Source: Carrier Wi-Fi Working Group
Author: Carrier Wi-Fi Working Group
Issue date: 07 February 2014
Version: 1.0
Document status: Final

About the Wireless Broadband Alliance

Founded in 2003, the aim of the Wireless Broadband Alliance (WBA) is to secure an outstanding user experience through the global deployment of next generation Wi-Fi. In order to make this a reality, the WBA is currently championing various initiatives in the Wi-Fi ecosystem including Next Generation Hotspot (NGH) trials, Wi-Fi Roaming and its Interoperability Compliance Program (ICP). Today, membership includes major fixed operators such as BT, Comcast and Time Warner Cable; seven of the top 10 mobile operator groups (by revenue) and leading technology companies such as Cisco, Google and Intel. WBA member operators collectively serve more than 1 billion subscribers and operate more than 5 million hotspots globally. The WBA Board includes Arqiva, AT&T, Boingo Wireless, BT, China Mobile, Cisco Systems, Comcast, iPass, KT Corporation, NTT DOCOMO, Orange and Ruckus Wireless.

Follow Wireless Broadband Alliance at:

www.twitter.com/wballiance
http://www.facebook.com/WirelessBroadbandAlliance
http://www.linkedin.com/groups?mostPopular=&gid=50482
https://plus.google.com/106744820987466669966/posts

© Copyright 2014 Wireless Broadband Alliance Ltd ("WBA"). All rights reserved. While every effort is made to ensure the information in this report is accurate, the WBA does not accept liability for any errors or mistakes which may arise in relation to the material. All copyright material and trademarks used in this report are the property of their respective owners.

Undertakings And Limitation of Liability

This Document and all the information contained in this Document is provided on an 'as is' basis without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for particular purpose, or non-infringement. In addition, the WBA (and all other organisations who may have contributed to this document) makes no representations or warranties about the accuracy, completeness, or suitability for any purpose of the information. The information may contain technical inaccuracies or typographical errors. All liabilities of the WBA (and all other organisations who may have contributed to this document) howsoever arising for any such inaccuracies, errors, incompleteness, suitability, merchantability, fitness and non-infringement are expressly excluded to the fullest extent permitted by law. None of the contributors make any representation or offer to license any of their intellectual property rights to the other, or to any third party. Nothing in this information or communication shall be relied on by any recipient.

The WBA also disclaims any responsibility for identifying the existence of or for evaluating the applicability of any claimed copyrights, patents, patent applications, or other intellectual property rights, and will take no position on the validity or scope of any such rights. The WBA takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any effort to identify any such rights.

Neither the WBA nor any of the other organisations who may have contributed to this document will be liable for loss or damage arising out of or in connection with the use of this information. This is a comprehensive limitation of liability that applies to all damages of any kind, including (without limitation) compensatory, direct, indirect or consequential damages, loss of data, income or profit, loss of or damage to property and claims of third-parties.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

Contents

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

Tables

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

Figures

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

Executive Summary

Carrier Wi-Fi is seen by operators as an important step forward to improve the user experience of customers, in particular because Wi-Fi is increasingly being used to deliver new services, and also for its role in cellular offload.

This paper examines Carrier Wi-Fi in the following sections:

- Section 1 discusses the WBA motivation for, and method of, developing this paper.
- Section 2 introduces terminology used in the paper.
- Section 3 very briefly touches on business drivers and the market for Carrier Wi-Fi. Operators need revenue sources with Wi-Fi services that are brand-worthy. Subscribers will expect Carrier Wi-Fi to exceed their experiences from legacy Wi-Fi offerings.
- Section 4 discusses three basic high level attributes of a Carrier Wi-Fi Network (CWLAN): consistent user experience; integrated end-to-end network capabilities; and network management. These attributes are discussed from the point of view of the user of the CWLAN and the operator deploying the CWLAN.
- Section 5 describes the technical functionality of a CWLAN required to provide the basic attributes described in Section 4. Example topics include automated network discovery and attachment, efficient standardized radio resource management, network quality, and integration of Wi-Fi into carrier networks.
- Section 6 analyses the gaps in the existing standards and certifications that need to be filled in order to provide coverage of the functionality described in Section 5. Recommendations for specification work or certification development have been identified. Actions should be considered within the WBA, WFA, IETF and BBF.
- Section 7 proposes a roadmap of actions to be taken to close the gaps identified in Section 6.
- Section 8 discusses the concept of a specific Carrier Wi-Fi Certification Program.
- Section 9 identifies specific liaisons to be sent by the WBA to begin implementation of the roadmap described in Section 7.
- The Annex describes the state of existing standards and certification in the Wi-Fi industry. Certification programs have proved to be important in bringing together the industry, to align the user experience and behavior of devices and network to offer consistency and a better user experience.

Devices are worth a special mention. While Devices are not actually deployed by the Operator, they are an important part of the Carrier Wi-Fi ecosystem. If they do not support the functions and features of CWLAN, then the operator's customers and users will not benefit from the enhanced behavior and service delivery of a CWLAN. Hence the paper also talks about the features that Carrier Wi-Fi devices need to support.

It is expected that as this paper is received by other industry bodies, they will give feedback and suggestions to the WBA on how to progress Carrier Wi-Fi development, and also detail potential work they will carry out relevant to Carrier Wi-Fi. It is therefore envisaged that there will be later versions of this paper that will include the feedback and progress of work in other industry bodies.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

1. Introduction and Overview

There is currently much discussion in the industry about Carrier Wi-Fi. However, the term has a different meaning depending on who is taking part in the discussion and where the topic is being discussed. These differences in understanding means there is no clear shared vision of Carrier Wi-Fi amongst operators and vendors, or of the steps needed to achieve a shared vision.

The WBA, in working on this topic, is trying to bring together all parties in the Wi-Fi industry into one vision that defines Carrier Wi-Fi, with the goal of creating a shared industry definition. This will allow the industry to develop a CWLAN ecosystem and subsequently to give the Wi-Fi consumer, when connected to a carrier-managed Wi-Fi network, the best user experience possible at that time and in that location.

This whitepaper is written by the WBA members and is their definition and agreed understanding as to what is meant by the term 'Carrier Wi-Fi'. This includes terms such as 'Carrier Grade Wi-Fi' and 'Carrier Defined Wi-Fi' as well as other possible variations on this theme. It does however exclude the work in the new IEEE study group on High Efficiency Wi-Fi (HEW), although a relationship between CWLAN and HEW may exist at some point in the future.

In preparing this paper the WBA has spoken to other relevant industry bodies as well as Standard Developing Organizations (SDOs) and included their views on the topic where they have provided them. Later versions of this paper may include views not available at the time of the whitepaper's initial publication.

Many different companies and industry bodies seem to have different views on Carrier Wi-Fi. This paper gives a clear and unified vision by all the relevant parties on what constitutes Carrier Wi-Fi. This will be shared amongst other industry bodies so that the entire community is working together in the same direction.

As always, at the heart of this project is the wish to serve the Wi-Fi customer when they are connected to a carrier-managed Wi-Fi network, to improve and enhance their user experience and to deliver to them the services they desire, where and when they desire those services.

By defining this vision the industry can work together to build the ecosystem required, and to put in place the building blocks for the industry to deliver that shared vision.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

2. Definitions

2.1 Carrier Wi-Fi Local Area Network (CWLAN)

CWLAN is a set of guidelines and best-practices that distinguish carrier-operated public Wi-Fi networks from consumer and enterprise networks. The intent of the program is to develop and publish an industry consensus regarding the characteristics of Carrier Wi-Fi. Those attributes include:

a. Features that must be supported by the infrastructure and the terminal devices built for carrier networks
b. The network architectures and implementation methods that support operator-managed Wi-Fi services
c. User experiences and operational best-practices typical of service provider networks

2.2 Trusted and Untrusted CWLAN

Within the scope of interconnection of a CWLAN with a 3GPP EPC network in a home operator network, it is the home operator's policy decision if a CWLAN is considered as Trusted or Untrusted. Whether a CWLAN is considered trusted is determined by the Home operator of the user, based on operational conditions, security, confidentiality and reliability criteria determined by Home operators.

Furthermore the Roaming Agreement between the Home operator and the Visited operator deploying the CWLAN can determine the criteria for considering a CWLAN as Trusted or Untrusted.

2.3 Next Generation Hotspot (NGH)

NGH is a set of capabilities, including enhanced network discovery and automatic authentication defined by the Wi-Fi Alliance Hotspot 2.0 Technical Specification [3] and support of WRIX [11], to deliver a set of features that enhance the Wi-Fi user experience.

The WBA has specified NGH, and tested it in a 'real world' environment that includes end user devices, and Wi-Fi network infrastructure including back office systems, operator requirements for NGH. NGH is an element of the Interoperability Compliance Program and of CWLAN.

2.4 Interoperability Compliance Program (ICP)

ICP is an accreditation program that facilitates Wi-Fi roaming relationships. It offers Wi-Fi service providers the opportunity to self-identify network capabilities, and provides them with a convenient means to present themselves to prospective access partners using an industry-recognized framework and terminology. Support for NGH is a requirement for ICP compliance at the Premier tier, but not at the Standard or Advanced tiers. Networks recognized as meeting ICP standards may also exhibit attributes of Carrier Wi-Fi.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

3. Business Drivers and Market Opportunities

In today's market, mobile and fixed operators view Carrier Wi-Fi to be a business imperative in order to meet subscriber demand for wireless data, reduce subscription churn, and increase subscriptions. Subscribers of Carrier-managed public Wi-Fi services expect accessibility and performance exceeding that of 'existing legacy Wi-Fi', while operators of Carrier Wi-Fi need revenue generating services (e.g. subscriptions, premium experiences, amenity services, wholesale access), with networks and technology that are brand-worthy. Therefore Carrier Wi-Fi must provide the capabilities and interoperability required to ensure that users turn to Carrier-managed Wi-Fi for wireless data services, rather than competing options.

Operator-managed Wi-Fi is an immediate market opportunity in developed economies. This market opportunity is expected to grow substantially; specific opportunities include:

- Enhance the value of devices already targeted for the service provider market
- Expand the portfolio of devices that can connect to carrier networks
- Improve connectivity for Cloud services
- Augment Consumer Electronic devices with embedded connectivity
- Expand service area to subscribers with 100-plus Wi-Fi roaming partner networks

Standardized Carrier Wi-Fi capabilities are needed to ensure Wi-Fi networks can reliably scale to take advantage of the market opportunity.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

4. Basic Attributes

There are three basic high-level attributes that need to be provided by a Carrier Wi-Fi network: consistent user experience; a fully integrated end-to-end network; and network management capabilities.

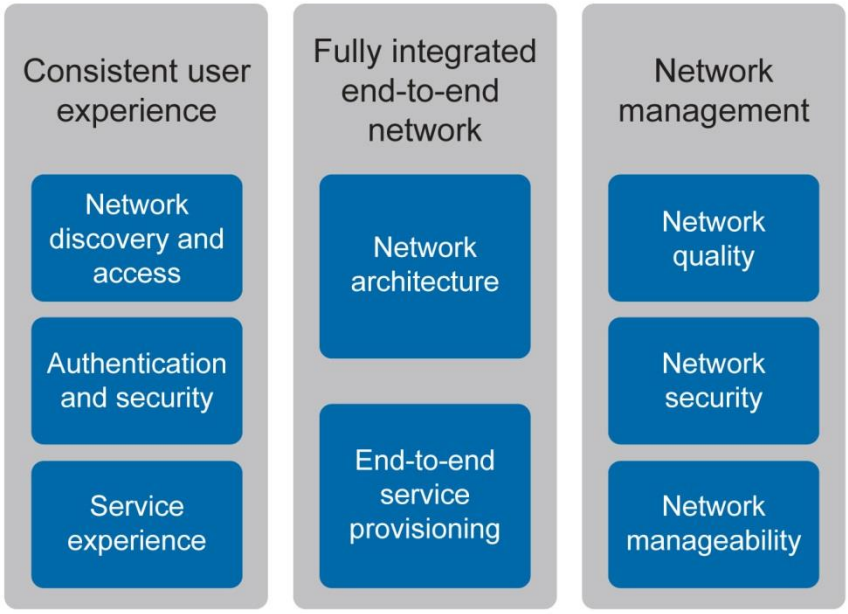


Figure 4–1 CWLAN Basic Attributes

4.1 Consistent User Experience

In Carrier-managed Wi-Fi networks, users expect an accessibility, service and performance level exceeding that provided by 'existing legacy Wi-Fi'. They expect devices to automatically manage network selection and authentication. They expect secure networks where they have confidence that their data will not be intercepted. Also, there may no longer be a need for the user to distinguish between Wi-Fi and cellular connections, for data traffic in particular.

To meet these user expectations, operators need to support interoperability and roaming across Wi-Fi networks, consistent user experiences across hotspots, and session continuity within the Wi-Fi network. As a longer term goal, operators with cellular access may need to support session continuity between their Wi-Fi and cellular access networks, which is dependent on the relevant standards and implementations being available in networks and devices.

4.1.1 Network Discovery and Access:

Carrier Wi-Fi devices and networks will to need support automated network discovery and selection of home and partner operator networks. Hotspot 2.0 is a technology that can be deployed to provide these capabilities. Admission control onto the network will be influenced by coverage and network load.

4.1.2 Authentication and Security:

Strong authentication methods must be employed before a subscriber is authorized to access network services. Multiple credential types can be used for authentication, including SIM and non-SIM credentials. Protection of credentials must be assured. Over the air

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

encryption to industry standards is required to provide the user confidentiality. Assurance of user data integrity is also required.

4.1.3 Service Experience:

Quality of Experience must be managed by the operator to achieve service experience levels expected by the user. This includes: network reliability that provides expected throughput targets; Operator-supported mobility across access points (AP) within the Wi-Fi network to ensure a seamless user experience; mobility support between Wi-Fi and cellular access to provide connectivity to the best network available and provide an ubiquitous service; and support of multi advanced service differentiation (such as the ability to support premium video) and mobile multi-media across APs. Underlying these technical attributes is the need for radio conformance to radio protocols and air interface interoperability of devices and APs.

4.2 Fully Integrated End-to-End Network

To provide superior value to customers, the CWLAN needs to provide the ability to connect users via the most appropriate technology available for the requested service, as well as interoperability between devices and networks, and interoperability and roaming between Wi-Fi networks.

4.2.1 Network Architecture:

The CWLAN architecture needs to support integration into the operator's network with standard interfaces, for example leveraging GRE and GTP. This could include the set of capabilities that 3GPP defines as required for 'trusted non-3GPP access'. IPv6 needs to be supported for devices, but also on all network nodes and network interfaces. The CWLAN architecture needs to support integration into the carrier network cloud architecture for economical large scale deployments. The network architecture should allow operators to share Wi-Fi resources.

The CWLAN architecture should support inter-network interconnect for roaming on a massive scale (hundreds of roaming partner networks.) This requires interoperability compliance to industry roaming specifications. One example of interconnection for roaming is the WBA's specification WRIX--i [11] RADIUS [34] interface for authentication, admission, accounting and home network-initiated disconnection per subscriber session. This could lead to supporting a very large number of simultaneous access requests; potentially thousands to tens of thousands.

4.2.2 End-to-End Service Provisioning

Ease of service subscription and provisioning for new subscribers is essential, by means such as support of the WFA Hotspot 2.0 specification [4]. The network and mobile device needs to support operator policy provisioning and enforcement that is granular to the subscriber service. The network must provide accounting and charging for home network and roaming subscribers. End-to-End service provisioning includes manageable service layer APIs.

Provisioning required for regulatory requirements, for example lawful interception, is needed.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

4.3 Network Management

To provide a consistent user experience and managed quality of service (QoS), the Carrier Wi-Fi network needs to be manageable by the operator using existing standards and techniques adopted by the industry. Operators need to manage policies and to support QoS with measureable results, including in highly dense interference environments. Network faults need to be automatically detected and reported to the operator's management system.

4.3.1 Network Quality:

Effective and dynamic radio resource management is essential to realize network quality. Radio resource management on a massive scale (hundreds of thousands to millions of APs) requires conformance to radio protocol standards across vendor products. Dynamic load sharing across multi-band operations is needed as well as the use of interference mitigation techniques in dense deployments. Operators need to manage their networks to optimize coverage, throughput and other Key Performance Indicators (KPIs).

4.3.2 Network Security:

Network integrity with strong intrusion prevention and detection methods are needed for Carrier Wi-Fi networks. Network management must be executed via secure access.

4.3.3 Network Manageability:

Interoperability of management systems for the CWLAN is essential in order to provide End-to-End management of the Wi-Fi network and to provide command and control capabilities from a Network Management Centre, for successful network operations to meet the network's management metrics.

Network manageability starts with standards-based provisioning of devices, APs and infrastructure. This includes auto-configuration and remote configuration methods.

Network manageability includes automated troubleshooting and network optimization to help ensure reliable network performance to measureable KPIs. Load Management with optimal resource allocation are essential capabilities. Load and traffic conditions need to be reported to the Network Management Centre in a timely basis.

Management capabilities to support regulatory compliance are mandatory.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

5. Functional Requirements

This section describes the functional requirements of Carrier Wi-Fi, based on the basic attributes described in section 4. The requirements are grouped as follows:

a. Carrier Wi-Fi Access Network

- Describes the logical architecture of the CWLAN, and the functional requirements for the APs and WLAN Access Controllers (ACs)

b. Network to Network components

- Describes the functional requirements of logical components required for inter-network roaming of subscribers among partner operators

c. Network Management System

- Describes the functionality required by the network management system to enable the operator to configure and manage the CWLAN

d. WLAN Service Servers

- Describes the functional requirements of servers that may be needed to provide operator required services to the CLWAN

e. Interworking with 3GPP Networks

- Describes the functional requirements that are needed in a CWLAN to support operator networks providing services to customers with 3GPP devices and subscriptions

f. Devices

- Describes the functional requirements of user devices within the CWLAN, such as smartphones, tablets, laptops or other user devices with a Wi-Fi interface

Some of the requirements in this section are already available in certification programs, such as those maintained by the WFA. This section needs to be read in conjunction with the Gap Analysis (Section 6) to fully appreciate the current state of what networks can achieve today and what the WBA would like to see of Carrier Wi-Fi networks in the future.

In the requirement tables in this section, the use of the term ‘SHALL’ means that it is a mandatory requirement, while ‘MAY’ means that it is an optional requirement.

5.1 Carrier Wi-Fi Access Network (CWLAN)

5.1.1 Network Architecture

Figure 5–1 below illustrates high level logical architectures for CWLANs, comprising of the following logical components: the AP complex, which may include only APs, or APs and ACs; the CWLAN Network Management System (CWLAN NMS); CWLAN Service Servers (CWLAN SS); Network-to-Network Components (NNCs); and Authentication, Authorization and Accounting (AAA) elements.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

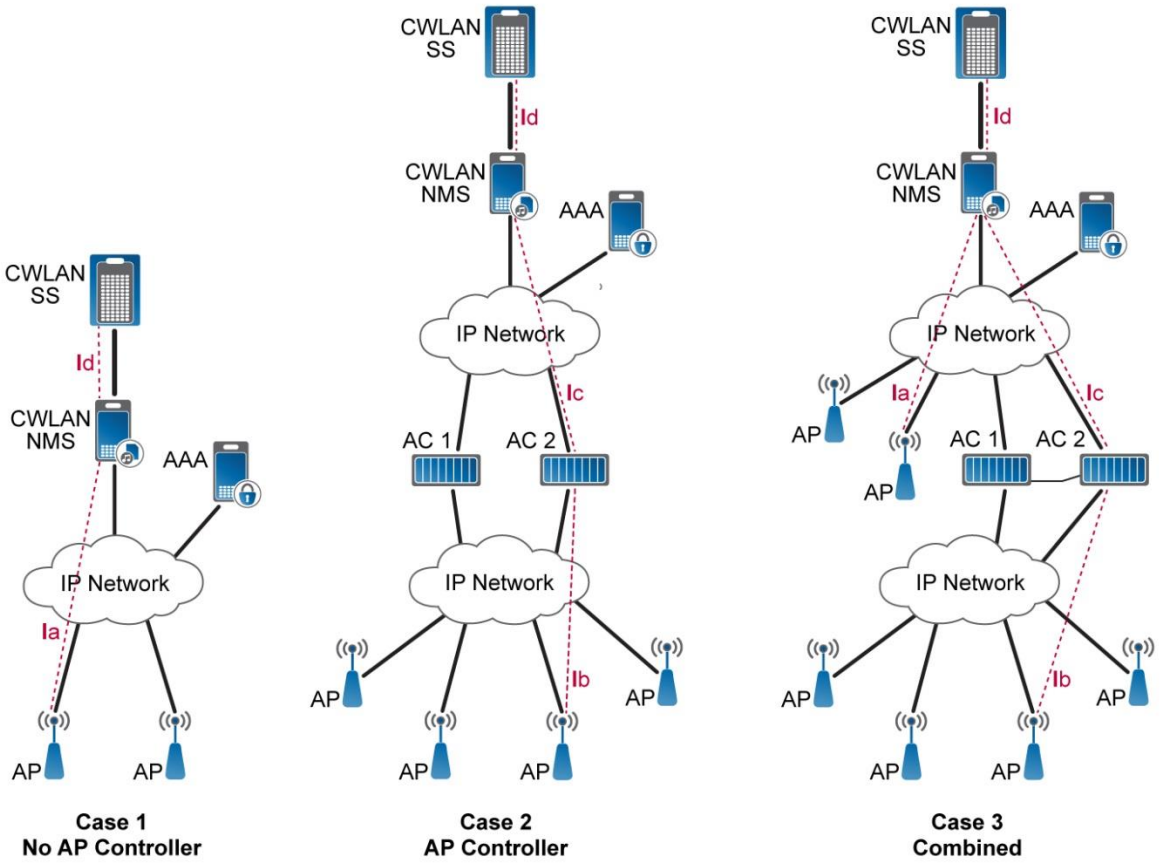


Figure 5–1 CWLAN Logical Network Architectures

The CWLAN NMS provides configuration, fault and performance management for each CWLAN network element including APs and ACs. The CWLAN SS is an application layer Service Server, such as a Wi-Fi Self Organizing Network (SON) system or ANQP server. The CWLAN NMS and CWLAN SS need to be compatible to APs and ACs from multiple vendors. The interface between the CWLAN NMS and CWLAN SS, (interface Id in Figure 5–1) can be implemented using TR-069 or other protocols.

The CWLAN SHALL implement one of three logical network architectures in Figure 5–1:

- In case 1, autonomous APs are used, so there are no ACs in the CWLAN. APs from different vendors are required to communicate directly with WLAN NMS and AAA servers. Ia is the interface between the AP and the CWLAN NMS, which can be implemented using TR-069, NETCONF [38] or SNMP.
- In case 2, all APs are managed by ACs. ACs from different vendors are required to communicate directly with CWLAN NMS and AAA servers. Ib is the interface between AP and AC, although the protocol used on the interface is out of the scope of this document. Ic is the interface between AC and CWLAN NMS, which can be implemented using TR-069 or other protocols.
- Case 3 is a combination of Case 1 and Case 2, where some of the APs are autonomous, and others are managed through ACs. IP Network 1 and IP Network 2 can be in the same physical domain but the logical path of each interface may be different.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

The CWLAN MAY integrate into the operator's core network. This can include core network architectures. Examples of technologies used to connect to fixed and mobile cores may include GRE, CAPWAP and 3GPP-defined reference points. The initial release of this document does not mandate a specific interconnection into a fixed or mobile core network. The architecture represents the scenario of a W-Fi network deployed by a single operator excluding inter-operator roaming.

Req ID	Requirement
5.1.1.1	CWLAN SHALL have one of three Wi-Fi network architectures in Figure 5–1

Table 5–1 Network Architecture

5.1.2 Network Manageability

The CWLAN provides full visibility and control of the network condition to the operator through the use of standardized network management interfaces, Ia and Ic in Figure 5–1. Network management interfaces provide means for troubleshooting, planning and optimization of network resources. The CWLAN SHALL support a standardized protocol for the network management interface. The data model for the proper management of the CWLAN needs to be developed. The CWLAN MAY support NETCONF [38] or SNMPv3 [40] for the network management interface. If possible, the NETCONF data model and SNMP MIB should be based on the data model used with TR-069 [41] which needs to be developed. The CWLAN MAY support a means of auto-configuration that includes the ability to discover network configuration servers, retrieve initial configuration files and invoke an initial configuration suitable for operation.

Given the increasing amount of subscribers and traffic on Wi-Fi networks, it is important for the CWLAN to properly and gracefully address Wi-Fi overload conditions. Therefore, the CWLAN reports to the NOC when the load over the thresholds configured by the operator are exceeded. The CWLAN SHALL report the APs, bands, and channels that have exceeded the overload thresholds configured by the operator at the time the thresholds are exceeded. In response to overload conditions, the CWLAN SHALL reject new device associations, MAY reduce downlink and uplink throughout, MAY reallocate resources to SSIDs and devices, and MAY reallocate throughput to SSIDs and devices as configured by the operator. The CWLAN SHALL ensure that Basic Service Set (BSS) load is communicated to devices on the air interface per IEEE 802.11-2012.

Req ID	Requirement
5.1.2.1	CWLAN SHALL support a standardized protocol for the network management interface, such as TR-069, CAPWAP, NETCONF or SNMPv3
5.1.2.2	CWLAN MAY support a means of auto-configuration including initial configuration
5.1.2.3	CWLAN SHALL support APs reporting threshold overload
5.1.2.4	CWLAN SHALL reject new device associations during overloads
5.1.2.5	CWLAN SHALL communicate BSS load to devices via the air interface per IEEE 802.11-2012

Table 5–2 Network Manageability

5.1.3 Network Quality

The network quality of the CWLAN is assured with radio physical layer and protocol interface conformance to standards, effective operator radio resource management, high levels of interoperability with certified devices, and support of KPIs.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

In the CWLAN, operators SHALL have the means to manage radio resources, including the ability to, but not limited to, manage the following list of parameters below. The CWLAN SHALL provide means to manage these parameters through standardized interfaces.

- Transmit power
- MCS rates
- MIMO and MU-MIMO configurations
- Beam forming configurations
- Channel bandwidth
- Maximum throughput per device
- Carrier sense thresholds
- Multi Band configuration and steering of devices, which can include dynamic traffic load sharing across bands
- Subscriber and service-driven dynamic load balancing among APs, bands and channels
- Channel assignments
- Interference avoidance and mitigation for higher density deployments

The CWLAN SHALL support the operator's ability to collect and monitor the KPIs listed below. (Note that KPI value ranges may need to be targeted to certain services):

- Received signal strength from devices
- Noise and interference levels
- Packet error rates and packet loss rates
- Throughput of uplink and downlink per device
- Device location
- Load threshold indicators
- Channel utilization
- Band utilization
- Rogue AP detection
- Neighbor AP detection
- Delays, latencies and jitter for traffic uplink and downlink

Req ID	Requirement
5.1.3.1	CWLAN SHALL support WFA Wi-Fi CERTIFIED™ n and/or Wi-Fi CERTIFIED™ ac (Based on IEEE 802.11ac D3.0)
5.1.3.2	CWLAN SHALL support radio resources management, using both automatic and manual methods, as listed in section 5.1.3
5.1.3.3	CWLAN SHALL support the measurement and reading of KPIs by operators as listed in section 5.1.3

Table 5–3 Table Title

5.1.4 Network Discovery and Access

Operator-managed automatic network discovery and access makes it easier for subscribers to take advantage of operator-provided services. The CWLAN AP complex SHALL be WFA Passpoint™ certified [4] in support of automated network discovery and selection.

Operators are able to manage admission and access on CWLAN networks based upon a number of parameters, allowing operators to provide better services to more subscribers. CWLAN AP complexes SHALL enforce admission control of subscriber devices based upon network load thresholds determined by the network operator. Admissions can be denied if the Wi-Fi network load thresholds are exceeded. Also, the CWLAN AP complex SHALL

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

enforce access of subscriber devices based upon the subscription type associated with the device, as determined by the operator. For example, higher service tier subscribers or subscribers with certain credential types may be offered access to more operator-managed APs or more Wi-Fi networks than other subscribers.

Responsive service is an important characteristic of CWLAN networks. It helps encourage subscribers to continue to use operator-provided services. Therefore, in the future when it is available, the CWLAN AP complex may support 802.11ai, Fast Initial Link Setup, to help provide responsive admission for subscribers.

Req ID	Requirement
5.1.4.1	The CWLAN AP complex SHALL be WFA Passpoint™ certified
5.1.4.2	CWLAN AP complex SHALL enforce access control of subscriber devices based upon network load thresholds determined by the network operator
5.1.4.3	CWLAN AP complex SHALL enforce access of subscriber devices based upon the subscription type associated with the device as determined by the operator
5.1.4.4	CWLAN AP complex MAY support interworking with 3GPP using the 802.11 defined 3GPP Cellular Network ANQP-element (as described in 802.11-2012 section 8.4.4.11), and the 3GPP Cellular Network Procedure (as defined in 802.11-2012 section 10.24.3.2.5)

Table 5–4 Network Discovery and Access

5.1.5 Authentication and Security

CWLAN SHALL use all NGH Network Authentication and Security features. It is essential that a CWLAN SHALL ensure that user credentials are securely stored.

Req ID	Requirement
5.1.5.1	CWLAN SHALL use all NGH Network Authentication and Security features [9]
5.1.5.2	The CWLAN SHALL provide for the secure storage of user credentials

Table 5–5 Authentication and Security

5.1.6 Service Experience

The CWLAN includes a number of capabilities for operators to deliver a managed service experience to subscribers, including what operators need to meet the standard for reliable throughput rates, transport for multi-media and differentiated services, and reduced interruption of service as a device moves among APs in the network.

The CWLAN SHALL support resource management such that the operator can set and maintain reliable minimum downlink and uplink throughput levels to subscriber devices as defined by the operator. The CWLAN SHALL support multi-media services through the use of QoS management driven upon the media authorized for exchange (downlink or uplink) to the subscriber device. The CWLAN SHALL support differentiated services by allowing the operator to set packet forwarding priorities and throughput levels per operator policy for each differentiated service.

The CWLAN SHALL support BSS Transition Management as defined in 802.11-2012 section 10.23.6, to facilitate efficient device transitions between APs within the Extended Service Set (ESS) in order to reduce interruption in services.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

The CWLAN SHALL support Fast BSS Transition as defined in 802.11-2012 section 12, to facilitate transfer of the security context parameters from one AP to another for faster over-the-air cryptographic establishment, avoiding full authentication procedures across APs.

Future work in CWLAN requirements will address the service experience as the subscriber device moves among CWLAN and cellular access networks.

Req ID	Requirement
5.1.6.1	The CWLAN SHALL support resource management such that the operator can set and maintain reliable minimum downlink and uplink throughput levels to subscriber devices as defined by the operator
5.1.6.2	The CWLAN SHALL support multi-media services through the use of QoS management
5.1.6.3	The CWLAN SHALL support differentiated services
5.1.6.4	CWLAN SHALL support BSS Transition Management as defined in 802.11-2012 section 10.23.6
5.1.6.5	CWLAN SHALL support Fast BSS Transition as defined in 802.11-2012 section 12

Table 5–6 Service Experience

5.1.7 Network Security

The CWLAN includes security measures to ensure the integrity of the network and services provided by the network. The CWLAN SHALL support secure access and authentication across network elements as configured by the operator. The CWLAN SHALL provide the means for the operator to manage intrusion prevention, detection and response mechanisms. The CWLAN SHALL provide the means to check the integrity of transmissions across network components. The CWLAN SHALL support confidentiality of transmissions between network elements as configured by the network operator. The CWLAN SHALL support methods to mitigate Denial of Service (DoS) attacks. The CWLAN SHALL provide proper traffic forwarding and packet filtering to ensure the security of subscriber device traffic.

Req ID	Requirement
5.1.7.1	CWLAN SHALL support operator configured secure access and authentication across network elements
5.1.7.2	CWLAN SHALL support network intrusion prevention, detection and response mechanisms
5.1.7.3	CWLAN SHALL support integrity checking of transmissions across network components
5.1.7.4	CWLAN SHALL support confidentiality of transmissions between network elements
5.1.7.5	CWLAN SHALL support methods to mitigate DoS attacks
5.1.7.6	CWLAN SHALL support traffic forwarding
5.1.7.7	CWLAN MAY support traffic packet filtering

Table 5–7 Network Security

5.1.8 IP Addressing

Operators will deploy IPv6 in order to support a range of new features that IPv6 provides, and also to help prevent potential IPv4 address exhaustion. The CWLAN needs to be IPv6-ready and support IPv4, IPv6 and dual stack clients. See the WBA ‘NGH Operator Guidelines, IPv6 for Carrier Wi-Fi’ for IPv6 requirements applicable to the CWLAN and other portions of the Wi-Fi network.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

Req ID	Requirement
5.1.8.1	The CWLAN SHALL support IPv6 as per the WBA document 'NGH Operator Guidelines, IPv6 for Carrier Wi-Fi'[10]

Table 5–8 IP Addressing

5.1.9 End-to-End Service Provisioning

The CWLAN enforces configured traffic flow parameters for operator-provided applications and services. Therefore, the CWLAN SHALL enforce the following traffic flow parameters as configured by the operator over standardized interfaces:

- Resource allocation limits or ranges to SSIDs on an AP
- Traffic priorities per SSID
- Traffic priorities per device based on operator-provided service or application
- Throughput maximums per SSID on an AP that supports multiple SSIDs
- Throughput maximums per device
- Traffic priority and maximum throughputs based on subscription type:
  - E.g. Gold, Silver access priority etc.
  - Home or roaming subscription

Req ID	Requirement
5.1.9.1	CWLAN SHALL support standard traffic flow parameters configured by the operator over standardized management or policy interfaces
5.1.9.2	CWLAN SHALL support traffic flow parameters enforcement

Table 5–9 End-to-End Service Provisioning

5.2 Network to Network Components

Network-to-network components (NNCs) support a number of capabilities for inter-network roaming of subscribers among partner operators. Interfaces between networks SHALL support authentication, authorization, accounting, data usage analysis and financial settlement. Wi-Fi service location also SHALL be supported through the use of a common data model and standardized data exchange methodology.

The NNCs SHALL support WRIX-i [11] for Authentication, Authorization and Accounting (AAA) when inter-network roaming is agreed between two operators. See WRIX-i for requirements that address RADIUS profiles, security and reliability on the inter-network AAA interface. The NNCs SHALL support WRIX-d [11] and WRIX-f [11] when data usage analysis and financial settlement are agreed between partner operators.

The NNCs SHALL support WRIX-L [11] for the exchange of Wi-Fi service location information when location services are agreed between partner operators.

Operators who agree to any of the internetwork roaming capabilities listed above are encouraged to certify their networks via the WBA ICP.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

Req ID	Requirement
5.2.0.1	The CWLAN NNCs SHALL support WRIX-i for Authentication, Authorization and Accounting (AAA)
5.2.0.2	The CWLAN NNCs SHALL support WRIX-d and WRIX-f
5.2.0.3	The CWLAN NNCs SHALL support WRIX-L
5.2.0.4	CWLAN operators MAY certify their networks using the WBA ICP program

Table 5–10 Network to Network Components

5.3 Network Management System (NMS)

5.3.1 General Requirements

The CWLAN NMS SHALL be capable of operating in all three of the logical architectures presented in Figure 5–1, which requires it to be able to interoperate with CWLAN network elements from multiple vendors. The CWLAN NMS SHALL provide the method by which CWLAN SS can configure and control CWLAN functions. For example, CWLAN SS can change the configuration of an AP via the CWLAN NMS, using the interfaces illustrated in Figure 5–1.

Req ID	Requirement
5.3.1.1	CWLAN NMS SHALL be able to interoperate with CWLAN components from multiple vendors
5.3.1.2	CWLAN NMS SHALL provide the method by which CWLAN SS configures and controls CWLAN functions

Table 5–11 General Requirements

5.3.2 Account Management

Based on installation location, equipment type, and capacity of CWLAN, different administrators need to have separate authorities to monitor and control CWLANs. The CWLAN NMS SHALL be able to support the creation various types of administrative accounts and provision these accounts with appropriate authority to manage all or a subset of CWLANs.

Req ID	Requirement
5.3.2.1	CWLAN NMS SHALL be able to create various types of administrator accounts with varying level of authority

Table 5–12 Account Management

5.3.3 Configuration Management

The CWLAN NMS SHALL be able to get and/or set the various configuration of CWLANs, including:

- Installation configuration: Installation location, date, status, zone/site name
- Network node profile such as manufacturer/supplier name, type, id, model name
- Network configuration: IP address, wireless/wired MAC address, type of backhaul
- Version configuration: hardware and software version, firmware update
- NMS configuration: IP address of NMS, account information for NMS, interface type
- Wi-Fi MAC configuration: SSID, beacon interval, RTS/CTS exchange threshold, fragmentation threshold, guard interval, frame aggregation, retry count, WMM
- RF configuration: the number and bandwidth of channel, RF power

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

Req ID	Requirement
5.3.3.1	CWLAN NMS SHALL be able to get and/or set the various configuration of CWLANs

Table 5–13 Configuration Management

5.3.4 Fault/Event Management

The CWLAN NMS SHALL be able to detect the status of CWLAN components, and display alarms according to severity level or a range of severity levels, including:

- Out of service (OOS)
- Power on/off status
- Configuration mismatch
- Traffic volume level
- Authentication fail level
- Malicious APs or STA detected

Req ID	Requirement
5.3.4.1	CWLAN NMS SHALL be able to detect the status of CWLAN components and display alarms

Table 5–14 Fault/Event Management

5.3.5 Performance Management

The CWLAN NMS SHALL provide the capabilities and standard interfaces to manage the CWLAN KPIs as described in section 5.1.3.

Req ID	Requirement
5.3.5.1	CWLAN NMS SHALL provide the capabilities and standard interfaces to manage the CWLAN KPIs

Table 5–15 Performance Management

5.3.6 Security Management

The CWLAN NMS systems SHALL support mutual authentication, integrity protection and confidentiality on all network management interfaces between the CWLAN NMS and the CWLAN elements.

Req ID	Requirement
5.3.6.1	The CWLAN NMS systems SHALL support mutual authentication, integrity protection and confidentiality on all network management interfaces between the CWLAN NMS and the CWLAN network elements

Table 5–16 Security Management

5.4 Wi-Fi Services and Applications

5.4.1 Wi-Fi Self Organizing Networks (Wi-Fi SON)

Carrier Wi-Fi networks may be large in scale, comprising of hundreds of thousands or millions of operator-managed APs. Self-organizing methods are required for the efficient management of Wi-Fi access when large numbers of APs are involved. Wi-Fi SON approaches can include techniques supported by each AP for immediate response to air interface conditions. Wi-Fi SON approaches can also include central SON servers that

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

provide the high level management of specific parameters based upon a wider view of the Wi-Fi network than may be available to individual APs.

The use of a Wi-Fi SON server is optional in a CWLAN, but if used operators need a standardized interface for centralized control of SON parameters. (See Figure 5–1 in section 5.1.1 for the placement of the CWLAN SON Server (CWLAN SS) in the CWLAN architecture.) The standardized interface at the CWLAN SON Server should support a number of operator or vendor-determined SON algorithms executed on the CWLAN SS. The interface should also support the use of a CWLAN controller and radio control functions local at each AP.

The goal of the architecture is to provide operators with a centralized Wi-Fi SON control, based on a wide view of the Wi-Fi access network, while maintaining vendor innovation at the CWLAN SS, CWLAN controller or CWLAN AP.

The CWLAN SS interface SHALL support the exchange of parameters as shown in Table 5–17and Table 5–18 below. This document does not mandate a specific timeframe for the exchange of information to and from the CWLAN SS, but it is expected that parameter updates are read by the CWLAN SS from each AP at a rate of around once per hour. It is expected that the CWLAN SS responds accordingly and applies new parameters as needed. The CWLAN SS interface SHALL support standardized protocols such as TR-069 framework, NETCONF, or SNMPv3.

Information from APs	Periodic/ On Demand	Mandatory/Optional
Neighbor Information by Channel Scan	Both	Mandatory
- SSID		
- Channel Number and Bandwidth		
- RSSI		
Number of Associated Users	Both	Mandatory
Channel Numbers and Bandwidth in Use	On Demand	Mandatory
Supported Channel Number & Bandwidth	On Demand	Mandatory
RF Power in Use	On Demand	Mandatory
Supported RF Power Range	On Demand	Mandatory
Beacon RF Power Range	On Demand	Mandatory
Supported Beacon MCS Level	On Demand	Mandatory
Operation Mode (b/g/a/n/ac) in Use	On Demand	Mandatory
Supported Operation Mode (b/g/a/n/ac)	On Demand	Mandatory
Carrier Sense Threshold in Use	On Demand	Mandatory
Supported Carrier Sense Threshold Range	On Demand	Optional
Channel Utilization	Both	Optional
Number of Received/Sent Bytes	Both	Mandatory
Number of Received/Sent Packets	Both	Mandatory
Throughput	Both	Optional
Traffic (Http, TCP) Quality of STA	Both	Optional

Table 5–17 Wi-Fi SON Parameters read by the WLAN SS for Each AP

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

Commands to APs	Mandatory/Optional
Channel Numbers and Bandwidth	Mandatory
RF Power	Mandatory
Beacon MCS Level	Mandatory
Operation Mode (b/g/a/n/ac)	Mandatory
Carrier Sense Threshold	Mandatory
Maximum Associated STA for Admission Control	Optional
Maximum Packet Retry Count	Optional
RTS/CTS Exchange	Optional
Frame Aggregation Level	Optional
Data MCS Level (Auto, Fixed)	Optional
Noise/Interference Immunity Level	Optional
LNA Bypass	Optional

Table 5–18 Wi-Fi SON Parameters Applied by the WLAN SS to Each AP

Req ID	Requirement
5.4.1.1	CWLAN MAY use a CWLAN Son Server
5.4.1.2	CWLAN SS interface SHALL support the exchange of parameters in tables 5-2 and 5-3
5.4.1.3	CWLAN SS interface SHALL support protocols consistent with the TR-069 framework, SNMP or other standardized protocol as per Req ID 5.1.2

Table 5–19 Wi-Fi Self Organizing Networks (Wi-Fi SON)

5.5 Interworking with 3GPP Networks

For an improved user experience the interworking of CWLAN with 3GPP networks is an option. The CWLAN MAY support integration into the 3GPP mobile operator network or may interwork with 3GPP networks of other operators acting as a home network. It shall be noted that in order to support such scenarios the CWLAN shall fulfil and support the requirements defined by 3GPP. 3GPP includes some mandatory and other optional requirements, hence this section shall be intended to define conditional requirements applicable only in the case that interworking with a 3GPP mobile network is supported.

Req ID	Requirement
5.5.0.1	CWLAN MAY support integration into the 3GPP mobile operator network or MAY interwork with 3GPP network of other operator network acting as a home network

Table 5–20 Interworking with 3GPP Networks

5.5.1 Network Architecture for 3GPP interworking

Currently the CWLAN may be connected to a 3GPP network for enabling access to the CLWAN for a Mobile Operator's subscribers. The user with a mobile subscription is authenticated using the (U)SIM performing EAP-SIM, EAP-AKA or EAP-AKA' authentication. After obtaining access to the CWLAN, the user can connect directly to the Internet and traffic is accounted as specified in WRIX. These specifications enable authentication, admission, accounting and home network initiated disconnection per subscriber session. The scenario is shown in Figure 5–2 and in 3GPP terminology is called Non-seamless WLAN offload (NSWO).

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

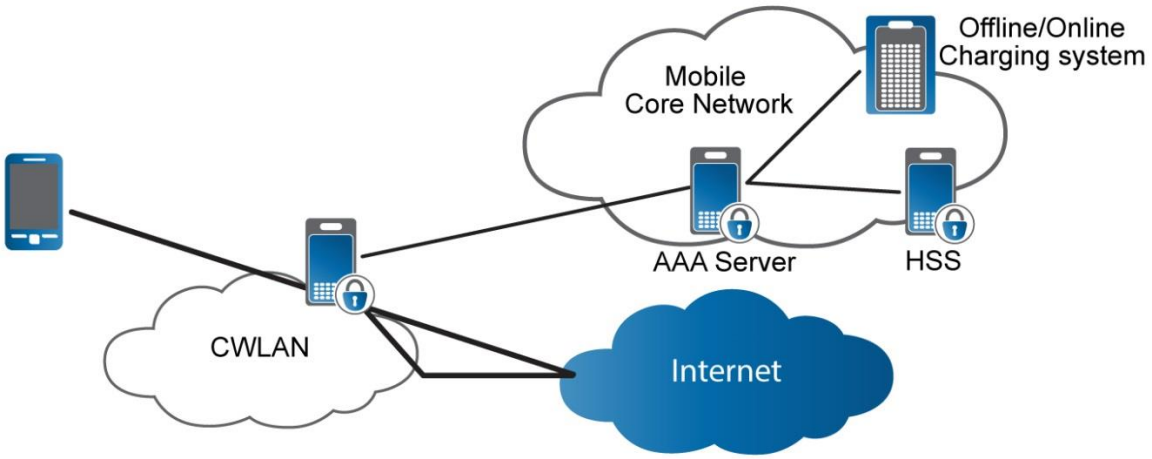


Figure 5–2 3GPP device connected to CWLAN accessing directly to the Internet

The 3GPP specifications enable the additional scenario where the mobile customer can access services provided by mobile operator through the 3GPP core network when connected to the CWLAN, i.e. the user traffic is routed from CWLAN to the Mobile Core Network. The 3GPP User Equipment (UE) can still maintain the connection on the 3GPP access network, and to the services provided via the Packet Data Network (PDN) connection according to the UE and the network capability. Furthermore, session mobility between the 3GPP access network and the CWLAN, and vice-versa, may be supported.

In order to enable access to mobile services via the interconnected mobile network, the CWLAN shall support the routing of traffic towards the 3GPP Evolved Packet Core (EPC).

3GPP defines three mobility solutions, called from the reference point name S2a, S2b and S2c. Figure 5–3 depicts the scenario where all PDN connections are moved or established on the CWLAN for consideration during various mobility solutions.

The third solution with S2c is based on DSMIPv6 and requires the support of a Mobile IP client embedded in the device, but at this point there is no indication of future support of this feature, so this solution is not being considered further in this document.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

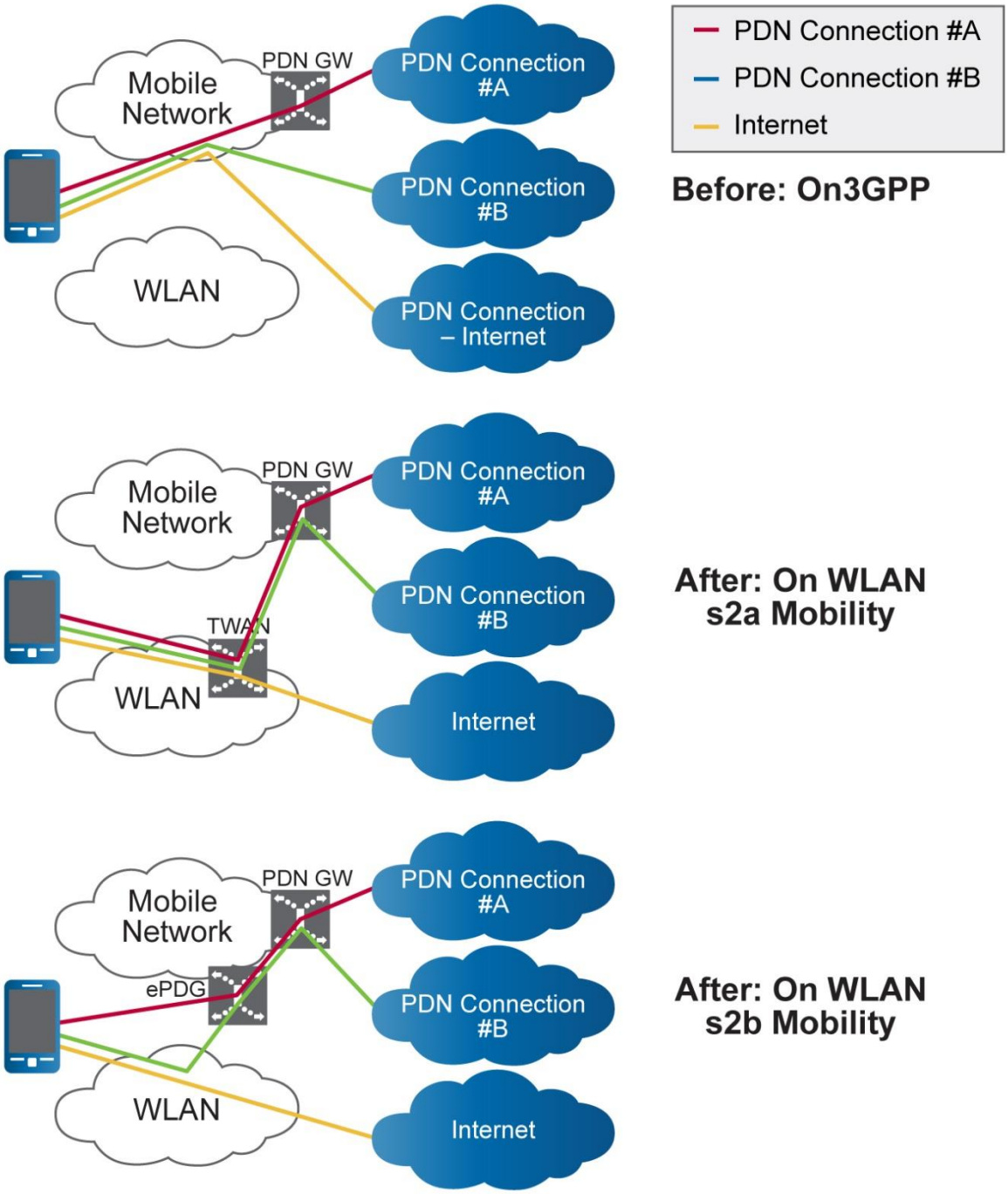


Figure 5–3 Inter-system mobility scenario with 3GPP device connected to 3GPP EPC and directly to the Internet via CWLAN

The S2a solution is based on deployment of a Trusted Gateway (TWAG) in the CWLAN where the S2a interface shall be GTP. The communication between the TWAG and the UE is based on the establishment of a point-to-point link. The CWLAN may support interworking with 3GPP EPC based on S2a. If S2a is supported, then the CWLAN SHALL support requirements as defined in 3GPP TS 23.402 and specifically as defined in TS 23.402 [13], TS 24.302 [28], TS 29.273 [21], TS 29.274 [22], TS 29.281 [23], TS 29.275[24]:

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

- EAP-based authentication
- TWAG
- Support point-to-point link between 3GPP UE and TWAG
- GTP as roaming interface between the TWAG and the PDN Gateway

The solution defined by 3GPP in Rel-11 has the following limitations:

- The handover between the CWLAN and the 3GPP access with IP preservation, i.e. session continuity, is not supported.
- The 3GPP UE can only have one PDN connection or Non-seamless WLAN offloaded connection, which is signaled by the home network during the authentication in AAA message exchange on the STa reference point.
- In a CWLAN, for a given UE simultaneous access to the EPC through S2a,non-seamless offload is not supported.

At the time when this guideline is published, 3GPP is working on Rel-12 to improve the solution for removing the above limitations.

The S2b solution is based on the deployment of the ePDG network element within the 3GPP EPC. The UE, after having obtained access to the CWLAN and after receiving an IP address, performs the establishment of an IKEv2 tunnel with a selected ePDG performing EAP-AKA authentication as part of the IKEv2 tunnel authentication. After the establishment of the tunnel the user traffic and any control signaling specific for supporting mobile procedures is exchanged within the IKEv2 tunnel, so is not accessible and transparent to the CWLAN. The S2b support is defined in 3GPP specifications TS 23.402[13], TS 33.402[26], TS 24.302[28], and TS 29.273[21].

In order to support the S2a based solution, the CWLAN shall be considered as a trusted access network by the home operator, while S2b solution can be support by a CWLAN but is considered Untrusted. (See the definition in Section 2.2 of Trusted and Untrusted CWLAN.)

3GPP specifications enable several different scenarios of connection and routing traffic via 3GPP and/or WLAN networks, Figure 5–4 shows the scenario called Multi Access PDN Connectivity (MAPCON), where the 3GPP UE is simultaneously connected to 3GPP access and the CWLAN, with some PDN connections maintained on the 3GPP access network, while other PDN connections are on CWLAN.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

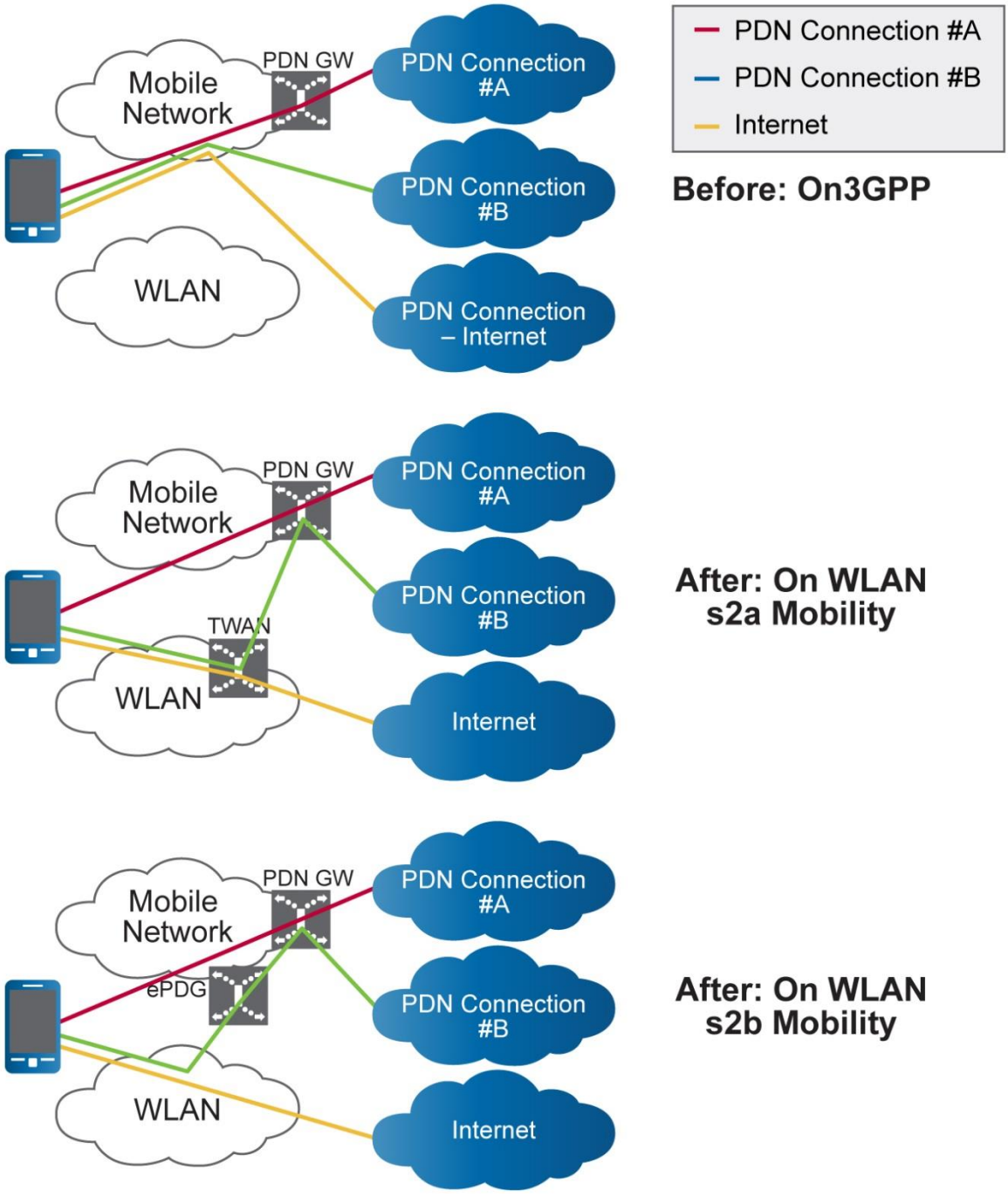


Figure 5–4 Inter-system mobility scenario with Multi-Access PDN connection support (MAPCOM) where a 3GPP device is connected to 3GPP EPC simultaneously via 3GPP and CWLAN and directly to the Internet via CWLAN

Finally Figure 5–5 shows a Non-Seamless WLAN Offload scenario where some IP flows belonging to PDN connections are moved to the CWLAN and consequently the traffic is no longer directed towards the 3GPP EPC network. Furthermore in this scenario the handoff is not seamless, i.e. the IP address is changed from those assigned for PDN Connection to those assigned locally by the CWLAN.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

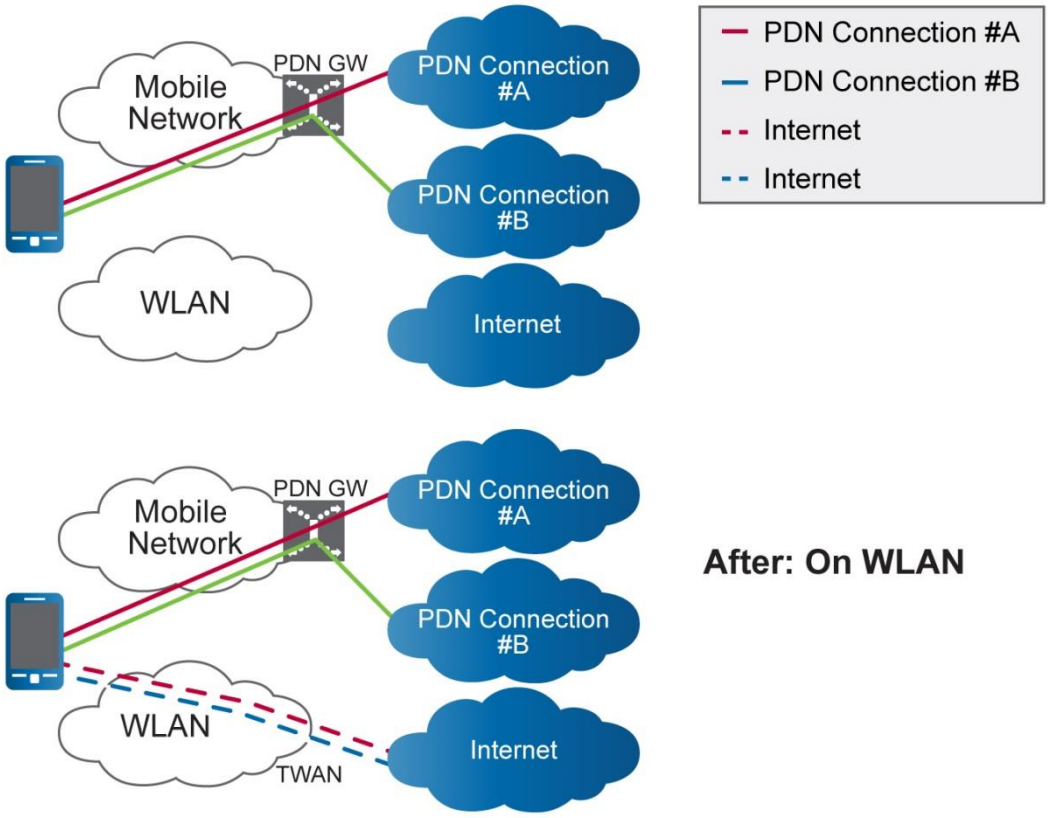


Figure 5–5 Non-Seamless IP Flow mobility scenario where some IP flows on a PDN connection are selectively offloaded from 3GPP access to CWLAN

5.5.2 CWLAN APs, AP controllers Requirements

On the support of interconnection within a 3GPP network, for S2b based solutions there are no additional requirements for APs and AP controllers.

For the support of S2a-based scenario the APs and the AP controllers shall support the establishment of a direct point-to-point link between the UE and the TWAG as specified by 3GPP TS 23.402, TS 24.302, for example configuration of bridge mode, SoftGRE or other solutions.

Req ID	Requirement
5.5.2.1	If supporting S2a based interworking with 3GPP the APs and the AP controllers SHALL support the establishment of direct point-to-point links between the UE and the TWAG as specified by 3GPP TS 23.402

Table 5–21 CWLAN APs, AP controllers Requirements

5.5.3 Network to network Components

Wi-Fi networks almost exclusively use RADIUS for AAA. However 3GPP has specified the use of Diameter in Release 6 and later. Some 3GPP specified attributes are only available in Diameter and have no RADIUS equivalent. Currently no specification exists to manage

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

this difference of usage in RADIUS and Diameter. With the growing use of Wi-Fi as a cellular offload solution, a standard for translation between RADIUS and Diameter is needed.

In order to support S2b solutions, the requirements in the following are applicable:

- The CWLAN SHALL support the routing of the traffic towards the 3GPP ePDG network element located in the 3GPP mobile Evolved Packet Network of the home service provider
- The CWLAN MUST allow the transit of IPsec protocol traffic from the 3GPP UE towards the 3GPP ePDG

In order to support S2a solutions, the requirements in the following are applicable:

- The CWLAN MUST support the TWAG as specified in TS 23.402, TS 24.303
- The CWLAN MUST support the S2a interface towards the Home mobile operator based on GTP as defined in TS 23.402, TS 29.274 and TS 29.281

Req ID	Requirement
5.5.3.1	If supporting S2b-based interworking with 3GPP the CWLAN SHALL support the routing of the traffic towards the 3GPP ePDG network element located in the 3GPP EPC of the home service provider
5.5.3.2	If supporting S2b-based interworking with 3GPP the CWLAN SHALL allow the transit of IPsec protocol traffic from the 3GPP UE towards the 3GPP ePDG
5.5.3.3	If supporting S2a-based interworking with 3GPP the CWLAN SHALL support the TWAG as specified in TS 23.402, TS 24.303[29]
5.5.3.4	If supporting S2a-based interworking with 3GPP the CWLAN SHALL support the s2a interface towards the Home mobile operator based on GTP as defined in TS 23.402, TS 29.274 and TS 29.281
5.5.3.5	To support standardized accounting, authentication and authorization methods between 3GPP and Wi-Fi networks, the CWLAN SHALL support a standard method of translation between RADIUS and Diameter

Table 5–22 Network to network Components

5.6 Devices

Devices are an important part of the Carrier Wi-Fi ecosystem. They need to be able to support and utilize the features present in a CWLAN to provide customers with the full benefits of CWLANs deployed by operators.

The GSMA Terminal Steering Group (TSG) has released the latest version of its document 'GSMA Minimal Wi-Fi Capabilities of Terminals, (TS.22) version 2' to the industry. This document is for SIM-based dual-mode devices. As this document defines 3GPP operators' expectations of device behavior with Wi-Fi networks, the WBA does not wish to duplicate the work of the GSMA TSG but to instead reference the document as reflecting the expectations of 3GPP operators when it comes to the requirements of devices as part of a Carrier Wi-Fi ecosystem. It should be remembered that the TS22 document will evolve when other 3GPP-specific aspects, such as ANDSF, support of traffic routing to 3GPP EPC, and session continuity, as well as new WFA Certification programs become available, and Operators develop their Wi-Fi network objectives further.

However, there is still a need to address the requirements of devices, such as tablets, that are Wi-Fi-only devices. Many of the Wi-Fi network behavior characteristics of non-SIM-based devices will need to be identical to those of SIM-based dual-mode devices. The main differences are likely to be the type of authentication used, and network discovery and access restricted to Wi-Fi networks only.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

There may still be aspects of a Carrier Wi-Fi ecosystem that are not addressed by the current GSMA TSG document of device requirements.

It should be noted that this document references only current WFA releases of certification programs. As existing WFA programs have new releases in the future then it can generally be assumed that the latest WFA certification release is that one that SHALL be supported in the device.

5.6.1 Network Discovery and Access

The CWLAN Device SHALL be WFA Passpoint™ certified in support of automated network discovery and selection. The CWLAN Device SHALL automatically execute network selection by taking into account, as provisioned by the operator, the home network realm, 3GPP information, Roaming Consortium information, roaming partner list priority and BSS load as reported by the AP SSID.

In the case of a 3GPP UE (e.g. smartphone) and if interworking with 3GPP core network is supported by CWLAN, in order to enable CWLAN selection and traffic steering between (possibly simultaneous) connections to a 3GPP radio access and to a WLAN, the network and discovery policy MAY include 3GPP Release 12 or later ANDSF policy. In Release 12 ANDSF network selection supersedes the Passpoint network selection, but uses the ANQP network selection information provided by Passpoint-enabled networks. This is to support selective offload for some applications and services.

Wi-Fi-only devices will normally be provisioned using Hotspot 2.0 Specification Release 2 procedures (when available) or proprietary techniques used by the Wi-Fi network provider.

When the CWLAN uses ANDSF, the CWLAN dual-mode device MAY be provisioned using ANDSF mechanisms, or the ANDSF policies may be provisioned in the CWLAN device by other means.

Req ID	Requirement
5.6.1.1	The CWLAN Device SHALL be WFA Passpoint™ certified
5.6.1.2	CWLAN Device SHALL automatically execute network selection

Table 5–23 Network Discovery and Access

5.6.2 Authentication and Security

The CWLAN Device SHALL be WFA Passpoint™ certified and hence support the current industry best practice for accepted authentication. The device SHALL support the security features specified in the WFA Passpoint™ Certification.

Req ID	Requirement
5.6.2.1	The CWLAN Device SHALL support the security features specified in the WFA Passpoint™ Certification
5.6.2.2	CWLAN Device SHALL provide secure storage of user credentials

Table 5–24 Authentication and Security

5.6.3 Service Experience

The CWLAN Device SHALL have a mechanism for evaluating the service experience being provided to the user via the AP with which it is currently associated, versus the experience that would be provided if the device was associated with another AP within the same ESS on the list of APs in range. The list will be updated, and the evaluation performed with a

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

frequency that SHALL provide the user with the best continuous service experience, as resulting from the device's evaluation. For example, the device will scan for APs with a frequency that minimizes the impact on its battery life and the WLAN overhead traffic, while allowing the device to be able to evaluate the service experience improvements available by switching to another AP in a timely manner, thus minimizing the service degradation experienced by the user prior to switching to another AP.

The CWLAN Device SHALL support fast and seamless transition between APs within the same ESS.

Req ID	Requirement
5.6.3.1	CLWAN device SHALL maintain a list of all APs within range
5.6.3.2	CWLAN device SHALL have a mechanism for evaluation of the service experience provided by all APs with the same BSSID within range, and SHALL associate with the AP which provides the best service experience according to its evaluation
5.6.3.3	CWLAN Device SHALL support 802.11-2012 parameters as in section 5.1.3, Req ID 5.1.3,4,5, and 6
5.6.3.4	The CWLAN Device SHALL support fast and seamless transition between APs within the same ESS

Table 5–25 Service Experience

5.6.4 Network Quality and Reliability

The CWLAN device will need to be able to support the network quality and reliability features in section 5.1.3. The CWLAN device SHALL use appropriate signaling to establish and maintain service and not exhibit excessive signaling behavior. (Specific signaling behaviors will need to be defined.)

Req ID	Requirement
5.6.4.1	CWLAN device will need to be able to support the CWLAN network quality and reliability features
5.6.4.2	The CWLAN device SHALL use appropriate signalling to establish and maintain service and not exhibit excessive signalling behaviour.

Table 5–26 Network Quality and Reliability

5.6.5 Network Security

The CWLAN device will need to be able to support the network security features in section 5.1.7.

Req ID	Requirement
5.6.5.1	CWLAN device SHALL support the CWLAN network security in section5.1.7, in addition to features in existing WFA certifications such as Passpoint™

Table 5–27 Network Security

5.6.6 Network Manageability

The CWLAN device will need to be able to support the network manageability features in section 5.3. Possible features could include network managed in-band channel switching as well as multiband switching, for example between the 2.4Ghz and 5GHz band. This could be based on features such as network load or the service requested on the device either automatically or by the end user.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

Req ID	Requirement
5.6.6.1	The CWLAN device SHALL support the network manageability features of the CWLAN network in section 5.3

Table 5–28 Network Manageability

5.6.7 End-to-End Service Provisioning

The CWLAN device will need to be able to support the network End-to-End service provisioning features in section 5.1.9. These features may in the future be part of a certification program. This could include support of policies based on subscription type such, as Gold or Silver access priority.

Req ID	Requirement
5.6.7.1	The CWLAN device will need to be able to support the network End-to-End service provisioning features in section 5.1.9. These features may in the future be part of a certification program. This could include support of policies based on subscription type such as Gold or Silver access priority

Table 5–29 End-to-End Service Provisioning

5.6.8 3GPP Interworking Device Requirements

For the device to support Wi-Fi-to-3GPP interworking, the device may support ANDSF and may also support other 3GPP capabilities required for the support of the interfaces S2a and S2b as defined by 3GPP. This is out of scope of this paper.

Req ID	Requirement
5.6.8.1	In order to support session continuity between the 3GPP network and the CWLAN, the CWLAN, the mobile network and the device SHALL support at least one common mobility solution, i.e. 3GPP s2a or S2b
5.6.8.2	The CWLAN 3GPP UE Device MAY support ANDSF

Table 5–30 3GPP Interworking Device Requirements

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

6. Gap Analysis

This section contains gap analysis based upon the Carrier Wi-Fi requirements documented in section 5. Each gap in the following sections is analyzed with respect to three aspects:

- Gaps in specification: new specification, a profile to an existing specification, or an extension to a specification is needed to help meet Carrier Wi-Fi requirements
- Gaps in certification and test programs: a new certification program needs to be developed, or an existing certification program is insufficient and needs to be enhanced or replaced
- Timeframe considerations: certain gaps may present an immediate problem for operators, while others can be addressed in the longer term evolution of technology. Therefore, the gap analysis recommends general timeframes for the development of work plans to close the gaps

6.1 Gap Analysis: CWLAN

6.1.1 Fast BSS Transitions Across APs on the same ESS:

- Gaps in specification: The specification already exists in IEEE 802.11-2012
- Gaps in certification and test programs: The WFA Voice Enterprise Certification program includes, among other requirements, the fast transition portions of 802.11-2012. A certification program for the fast transition capabilities on APs should be developed. This feature needs to be added to a more appropriate certification program, such as WFA Passpoint™, and/or as a standalone certification
- Timeframe considerations: Operators are considering WFA Passpoint™ deployments in the near term, many with APs providing continuous radio coverage over wide areas where devices are mobile. Note that BSS fast transitions need to apply across WFA Passpoint™ SSIDs of the same network operator

6.1.2 Authentication for Secure SSIDs with User Name and Password:

- Gaps in specification: The WFA HS 2.0 Technical Specification mandates EAP-TTLS MSCHAPv2 for user name and password. MSCHAPv2 requires the use of MD4 hash, which is a weak security mechanism, and complicates the secure storage of credentials in the network. An alternative to EAP-TTLS MSCHAPv2 for user name and password that supports the storage of credentials protected with current and future hash algorithms of strong security strength is required for CWLAN. The means to provision and use the authentication alternative to EAP-TTLS MSCHAPv2, it needs to be mandated in the HS2.0 Technical Specification and supported by the CWLAN authentication infrastructure
- Gaps in certification and test programs: WFA Passpoint™ certifications should be updated to include alternatives to EAP-TTLS MSCHAPv2 for user name and password. CWLAN infrastructure needs to be tested to support the alternative authentication mechanism
- Timeframe considerations: Operators are currently using less secure techniques to protect their credential databases until an alternative to EAP-TTLS MSCHAPv2 is selected for device certifications. Therefore, an alternative to EAP-TTLS MSCHAPv2 should be identified for orderly inclusion in future WFA Passpoint™ product releases and certification test updates

6.1.3 Channel Selection Within and Across Bands

- Gaps in specification: A method needs to be specified to require a device to move to a specific channel within a frequency band or to a specific frequency band. Operators need to direct devices for purposes such as load balancing and service requirements

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

- Gaps in certification and test programs: CWLAN tests are needed to ensure support of network-driven channel selection within and across bands
- Timeframe considerations: Operators are currently experiencing excessive loads in 2.4Ghz bands. Dual band devices often stay on 2.4Ghz even when a 5Ghz service is also available. Therefore, a specification and product certification for channel selection across frequency bands without impacting the 802.11 air interface protocol is needed immediately. Additional, more sophisticated channel selection in multi-band environments that impact the air interface, may be needed in the longer term.

6.1.4 Management of Resources

- Gaps in specification: Standardized interfaces and data models are needed for operators to manage air interface parameters with KPIs as described in section 5.1.3
- Gaps in certification and test programs: Compliance tests need to be developed to ensure the CWLAN elements support standardized interfaces for the management of air interface parameters and KPIs
- Timeframe considerations: Operators have an immediate need for more effective air interface management of CWLAN from multiple vendors with standard interfaces. Compliance tests are needed in the near term.

6.1.5 Management of Overload Conditions

- Gaps in specification: Standardized interfaces and data models are needed for operators to set overload thresholds on the CWLAN, and for the NMS to receive reports when thresholds are exceeded. The CWLAN needs to reject new associations during overload conditions and report the association rejections. The CWLAN needs to support standardized interfaces for the operator to provision policy for resource reallocation to devices during overload conditions
- Gaps in certification and test programs: A CWLAN test program needs to be developed to ensure support for the management of overload conditions
- Timeframe considerations: The need for the graceful management of overload conditions will increase as traffic demands continue to increase. These capabilities need to be implemented when appropriate on future product releases

6.1.6 Traffic Flow Parameter Management in the CWLAN

- Gaps in specification: Operators have an immediate need for the CWLAN to enforce operator provisioned traffic flow parameters with standardized interfaces as described in section 5.1.9. Specifications need to be developed to support these traffic flow management capabilities.
- Gaps in certification and test programs: Compliance tests need to be developed to ensure that the CWLAN applies traffic flow management parameters with standardized interfaces as defined in section 5.1.9
- Timeframe considerations: Vendor solutions exist for the management of traffic flow parameter capabilities described in section 5.1.9. Operators, however, need standardized interfaces for multivendor deployments in large networks. Vendor products need to migrate toward standardized interfaces for policy enforcement when appropriate

6.1.7 Interference Management

- Gaps in specification: Wi-Fi networks suffer degraded performance due to interference from a range of sources as listed below. No specific gaps in CWLAN specifications are

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

identified here, however, studies should be conducted to determine if further specification can help operators better mitigate interference.

- Interference with other wireless networks or devices using unlicensed spectrum
- Interference with other wireless networks or devices using licensed spectrum
- Interference from other Wi-Fi networks. For example, interference can be exacerbated when high transmit power levels are used unnecessarily
- Interference across channels on the same AP
- Gaps in certification and test programs: Potential tests are for further study
- Timeframe considerations: The need for interference management grows as more Wi-Fi networks are deployed and user traffic levels increase. A target timeframe for potential solutions is for further study

6.1.8 Additional Gaps to be Addressed Within a Longer Timeframe

- Fast Initial Link Setup: Fast Initial Link Setup promises to substantially reduce the time required to attach to secure SSIDs while increasing the battery life of devices. Specifications and test programs for CWLAN support of Fast Initial Link Setup needs to be developed

6.2 Gap Analysis: Network to Network Components

6.2.1 Inter-network Reporting of Accounting Records When Devices Move Across APs

- Gaps in specification: Session maintenance across secure SSIDs can be influenced by fast transition mechanisms, for example key caching. These techniques can avoid authentication messaging and help maintain a session as a device moves across secure SSIDs. Accounting record guidelines should be developed for scenarios where devices move across APs to help ensure consistency of reporting across networks. For example, the use of Start, Interim and Stop records, and updates in AP location parameters should be explained. These guidelines can be considered for WRIX-i
- Gaps in certification and test programs: Tests for accounting records produced as a device moves across APs can be considered for the WBA ICP
- Timeframe considerations: Guidelines and test programs are needed in the near term when the deployment of WFA Passpoint™ with internetwork roaming becomes prevalent

6.2.2 RADIUS to Diameter Interworking

- Gaps in specification: Wi-Fi networks almost exclusively use RADIUS for AAA. However, 3GPP has specified the use of Diameter in Release 6 and later. Some 3GPP-specified attributes are only available in Diameter and no RADIUS equivalent. Currently no specification exists to manage this difference of usage in RADIUS and Diameter
- Gaps in certification and test programs: No tests have been specified to test for conversion of Diameter only attributes to RADIUS based attributes. The industry needs to define solutions
- Timeframe considerations: This gap needs to be addressed in the short to medium term as operators begin to support 3GPP offload to Wi-Fi networks, and increasing as 3GPP operators deploy Diameter in their networks

6.2.3 RADIUS Attributes

- Gap in specifications: None

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

- Gaps in certification and test programs: There is no certification to validate that CWLAN equipment, including devices, generates and handles RADIUS attributes correctly
- Timeframe considerations: This is an issue in the market today

6.2.4 GTP Interface for 3GPP Interworking

- Gap in specification: The 3GPP interworking scenario described in section 5.5. includes the S2a-based solution, which foresees the usage of an s2a reference point based on GTP as the roaming interface between a visited operator deploying CWLAN and a home operator with 3GPP EPC. This scenario is not currently foreseen in any WLAN roaming guideline in WBA or GSMA
- Gaps in certification and test programs: The test of GTP as a roaming interface should be considered for a potential phase of NHG trial in case of support of s2a based 3GPP interworking scenario
- Timeframe considerations: This gap needs to be addressed in the medium term

6.2.5 Additional Gaps to be Addressed Within a Longer Timeframe

- Initial Wi-Fi roaming deployments will likely route user traffic to the internet locally in the visited network. Eventually home network operators will want to deliver applications, content and services to roaming subscribers using inter-network policy transfer and enforcement. Specifications and test procedures need to be developed to support user traffic forwarding to the home network with inter-network policy interfaces.

6.3 Gap Analysis: Network Management System

- At this time no gaps have been identified in the specifications for Network Management Systems.

6.4 Gap Analysis: Wi-Fi Services and Applications

6.4.1 Wi-Fi SON

- Gaps in specification: The motivation and architecture for Wi-Fi SON is described in section 5.4.1. Standard interfaces and data models are needed to exchange the Wi-Fi SON parameters that are identified in this document. The SON parameters need to be exchanged on standard interfaces between (1) the SON Server and NMS, (2) between the NMS and AP, (3) and between the NMS and AC. Wi-Fi SON server algorithms and AC radio resource algorithms are not intended to be standardized in order to allow operators and vendors freedom to develop optimizations
- Gaps in certification and test programs: Compliance tests for the Wi-Fi SON interface and parameter exchange listed above need to be developed
- Timeframe considerations: Operators have already deployed large Wi-Fi networks that could benefit from SON approaches. The need for standardized SON interfaces continues to grow as networks become even larger and increase in density. Standardize SON interfaces will also allow operators to manage radio resources when deploying APs from multiple vendors. Operators need standard Wi-Fi SON interfaces in the near term

6.5 Gap Analysis: Devices

This section contains the gap analysis applied to Wi-Fi devices to be compatible with Carrier Wi-Fi networks.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

6.5.1 AP Selection for Improved Uplink and Downlink Performance:

- Gaps in specification: Some devices, sometime referred to as 'sticky devices', remain associated to an AP when the uplink and/or downlink radio link performance has degraded, even though there is another AP available to which they could transition. A specification is needed that requires devices to select an AP with improved radio conditions available within the same ESS in an appropriate timeframe
- Gaps in certification and test programs: A device compliancy test is needed to ensure devices move onto the APs for better uplink and downlink performance
- Timeframe considerations: This is an issue currently being experienced by subscribers, which is therefore generating calls to customer care centers. Resolution is needed immediately

6.5.2 Fast BSS Transitions Across APs on the same ESS:

- Gaps in specification: The specification already exists in IEEE 802.11-2012
- Gaps in certification and test programs: The WFA Voice Enterprise Certification program includes, among other requirements, the fast transition portions of 802.11-2012. A certification program for the fast transitions capabilities on APs should be developed. This feature needs to be added to a more appropriate certification program, such as WFA Passpoint™, and/or as standalone certification
- Timeframe considerations: Operators are considering WFA Passpoint™ deployments in the near term, many with APs providing continuous radio coverage over wide areas. Note that fast transitions need to apply across WFA Passpoint™ SSIDs of the same network operator

6.5.3 Devices with Appropriate Signalling Behaviour:

- Gaps in specification: Certain Wi-Fi devices produce inappropriate or unneeded levels of signaling. For example, a specific device type produces a multitude of unneeded DHCP requests. A device behavior guideline is needed for the appropriate use of signaling, including DHCP
- Gaps in certification and test programs: A compliancy test for appropriate device signaling behavior needs to be developed
- Timeframe considerations: This is an issue currently being experienced by subscribers and generating calls to customer care centers. Resolution is needed immediately

6.5.4 Private and Public SSID selection:

- Gaps in specification: Operator APs may be deployed with a combination of private and public SSIDs. The WFA Hotspot 2.0 specification and the 3GPP ANDSF may provide for appropriate selection among public and private SSIDs, but there is no specification that mandates the use of the device UI to be able to place specific private SSID names in higher priority than WFA Passpoint™ or other public SSIDs
- Gaps in certification and test programs: A device compliancy test needs to be developed to ensure devices allow users to prioritize their private or certainly public SSIDs
- Timeframe considerations: A device compliancy test is needed in the near term

6.5.5 Device Utilization of WFA Passpoint™ features:

- Gaps in specification: The WFA Hotspot 2.0 Technical Specification addresses the air interface, and the provisioning of operator policy, on devices. Device behavior guidelines or specifications are needed to outline how the subscriber interacts with

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

Passpoint features, or how devices can better utilize Passpoint features. Examples are shown listed below

- Gaps in certification and test programs: While the WFA Passpoint™ certification test program checks the syntax of the air interface 802.11 messages, testing for how devices utilize Passpoint features is not completely addressed. A device certification program needs to be developed to test for device compliance of all mandatory Passpoint features, examples include:
    - The selection of SSID based upon roaming consortium OI
    - Device requirements that support the subscribers ability to select the subscription used for Wi-Fi access
    - Device requirements to display Passpoint features of interest to the user such as Operator Friendly Name and Venue
- Timeframe considerations: Proper utilization of Passpoint features by devices is in the near term needed when Passpoint networks become widespread

6.5.6 Authentication for Secure SSIDs with User Name and Password:

- Gaps in specification: The WFA Hotspot 2.0 Technical Specification mandates EAP-TTLS MSCHAPv2 for user name and password. MSCHAPv2 requires the use of MD4 hash, which is a weak security mechanism, and complicates the secure storage of credentials in the network and on the device. An alternative to EAP-TTLS MSCHAPv2 for user name and password which supports the storage of credentials protected with current and future hash algorithms of strong security strength is required for CWLAN. The means to provision and use the authentication alternative to EAP-TTLS MSCHAPv2 needs to be mandated in the WFA Hotspot 2.0 Technical Specification on and supported on devices
- Gaps in certification and test programs: WFA Passpoint™ certification should be updated to include alternatives to EAP-TTLS MSCHAPv2 for user name and password
- Timeframe considerations: Operators are currently using alternative, less secure techniques to protect their credential data bases until an alternative to EAP-TTLS MSCHAPv2 is selected for device certifications. Therefore, the alternative to EAP-TTLS MSCHAPv2 should be identified for orderly inclusion in future WEA Passpoint™ certified product releases and certification test updates

6.5.7 Channel Selection Within and Across Bands

- Gaps in specification: A method needs to be specified to require a device to move to a specific channel within a frequency band or to a specific frequency band. Operators need to direct devices for purposes such as load balancing and service requirements
- Gaps in certification and test programs: Device compliancy tests are needed to ensure devices support network driven channel selection within and across bands
- Timeframe considerations: Operators are currently experiencing excessive load in 2.4Ghz bands. Dual-band devices often stay on 2.4Ghz even when 5Ghz service is also available. Therefore, a specification and product certifications for channel selection across frequency bands without impacting the 802.11 air interface protocol is needed immediately. Additional more sophisticated channel selection in multi-band environments that impact the air interface may be needed in the longer term

6.5.8 Additional Gaps to be Addressed Within a Longer Timeframe

- Seamless mobility across RATs: Procedures that support seamless mobility across Wi-Fi and other carrier radio access need to be developed

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

- Fast Initial Link Setup: Fast Initial Link Setup promises to substantially reduce the time required to attach to secure SSIDs while increasing battery life. Specifications and test programs for devices to support Fast Initial Link Setup need to be developed

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

7. Recommended Actions

Section 7 provides a gap analysis between CWLAN functional requirements included in this document and existing Wi-Fi specifications, test programs and certain products. The following tables recommend specific actions to be taken by the WBA to move toward closure of these gaps.

GAP	Req ID	Recommended Actions	Requested Support	Time Frame
BSS Fast Transitions	5.1.6.4, 5.1.6.5	Liaison to WFA for a new BSS fast transition certification	WFA	2014
Authentication with user name & password	5.1.5.1	Liaison to WFA to motivate updates in Passpoint specifications and related certifications	WFA	2015
Channel Selection across bands	5.1.3.1, 5.1.3.2	Liaison to WFA to motivate specifications and certification programs	WFA	2014
Management of resources	5.1.3.1, 5.1.3.2	WBA to develop a data model that should be sent via liaison to other bodies, such as the BBF, for detailed protocol specification	WBA, BBF, IETF	2014-2015
Management of overload conditions	5.1.2.1, 5.1.2.3, 5.1.2.4	WBA to develop guidelines and data models for the management of overload conditions. These should be sent to other bodes for detailed protocol specification.	WBA, BBF, IETF	2014-2015
Traffic Flow Parameter management	5.1.9.1, 5.1.9.2	WBA to develop a data model that should be sent via liaison to other bodies, such as the BBF, for detailed protocol specification of the management interface.	WBA, BBF, IETF	2015
Interference Management	5.1.3.2, 5.1.3.3	WBA to complete a detailed study of interference problems and recommendations for mitigation. This may trigger liaisons to the IEEE or WFA depending upon recommendations	WBA	2015

Table 7–1 Recommended Actions: CWLAN

GAP	Req ID	Recommended Actions	Requested Support	Time Frame
Accounting Correlation Across APs	5.2.0.1, 5.2.0.2, 5.2.0.3, 5.2.0.4	REWG to consider guidelines for accounting data as a device moves across APs. WRIX specifications may be updated. The WBA ICP may also be updated.	WBA	2014
AAA protocol for 3GPP interworking with EPC	5.5.2.5	WBA Roaming guideline and GSMA to analyses the scenario and to propose solution, for example to revise the roaming specification in WBA and GSMA for introducing the support of Diameter or to propose to 3GPP to specify the support of Radius taking into account needed 3GPP extension	WBA, GSMA	2014
RADIUS Attributes	5.2.0.1	A certification program is needed to validate that CWLAN equipment generates and handles RADIUS attributes correctly	WBA	2014
GTP as roaming interface for 3GPP interworking with EPC	5.5.2.4	WBA Roaming guideline and GSMA to consider the enhancement of roaming guideline with support of GTP for enabling the s2a based 3GPP interworking	WBA, GSMA	Mid-Term

Table 7–2 Recommended Actions: Network to Network Components

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

GAP	Req ID	Recommended Actions	Requested Support	Time Frame
Standardized interfaces for Wi-Fi SON parameters	5.4.1.1, 5.4.1.2, 5.4.1.3	It is recommended that the WBA produce guidelines and a standard data model for Wi-Fi SON interfaces. The data model should be sent to other forums, such as the BBF, via liaison for specific protocol work	WBA, BBF	2014

Table 7–3 Recommended Actions: Wi-Fi SON

GAP	Req ID	Recommended Actions	Requested Support	Time Frame
AP selection for improved performance	5.6.3.1, 5.6.3.2, 5.6.3.3	WBA should publish guidelines on device selection of APs for improved uplink performance. The DCP should test per the guidelines	WBA	2014
BSS Fast Transitions	5.6.3.4	Liaison to WFA to motivate greater adoption of fast transition certifications	WFA	2014
Appropriate Signaling Behavior	5.6.4.2	WBA should publish device guidelines for appropriate signaling behavior from devices. (DHCP is one example) The DCP should test per the guidelines	WBA	2014
Private SSID Selection	5.6.1.2	The WBA should publish guidelines that require devices to allow subscribers to directly prioritize their private SSIDs over Passpoint SSIDs. The DCP should test per these guidelines	WBA	2014
Utilization of Passpoint	5.6.1.1, 5.6.1.2	The WBA should publish guidelines on device behavior with Passpoint features. The DCP should test per these guidelines	WBA	2014
Authentication with user name & password	5.6.2.2	Liaison to WFA to motivate updates in Passpoint specifications and related certifications	WFA	2015
Channel Selection across bands	5.6.3.3	Liaison to WFA to motivate specifications and certification programs	WFA	2014

Table 7–4 Recommended Actions: Devices Compatible with CWLAN

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

8. Carrier Wi-Fi Certification Programs

There are already existing certification programs and recommendations available that cover various aspects of Carrier Wi-Fi. This includes the WFA Passpoint™ Certification and the WBA ICP program. However, there are also other aspects of Carrier Wi-Fi that would benefit from being part of a certification process.

There are at least two possible solutions to developing a Carrier Wi-Fi Certification. One way would be to define a list of certification programs that together make up the minimum set of requirements to be considered a Carrier Wi-Fi network. Secondly, there could be a Carrier Wi-Fi Certification program that consists of a variety of tests that a network has to satisfy to be considered as Carrier Class Wi-Fi.

An alternative approach would be for the WBA ICP program to define a set of certification programs that an Operator has to meet to be considered as Carrier Class Wi-Fi. The Operator would need to demonstrate it is meeting and continuing to satisfy these requirements, in order to be given Carrier Class Wi-Fi status and to maintain that status.

Initially this would consist of a set of certification programs and recommendations, however there would initially be many gaps in that set of certifications. Over time the gaps would be addressed and replaced with expanded or new certification programs.

Finally we would finish with Carrier Wi-Fi clearly defined by a set of industry-recognized certification programs and standardized, industry-recognized compliancy programs for good practices.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

9. Next Steps for WBA

The WBA will liaise this completed document to the following bodies: 3GPP; Broadband Forum; CableLabs; GSMA; IEEE; NGMN; Small Cell Forum; Wi-Fi Alliance.

The WBA will ask for their feedback and opinions on this topic, based on this document. Any relevant feedback received could be included in any later versions of this document.

The WBA will initiate new work that could help towards developing Carrier Wi-Fi. This may be a new specific program but also more likely may have an impact on existing programs such as the NGH Operator Guidelines, NGH Trial and ICP programs.

In addition, where work has been identified in section 7, Recommended Actions, the WBA will liaise with the suggested bodies, with the intention of working with those bodies to initiate work programs to satisfy the shortfalls identified in making Carrier Wi-Fi a reality.

The WBA will take an active role in coordinating Carrier Wi-Fi activity in the industry and will become the reference point for Carrier W-Fi work.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

References

Ref	Document Number	Title
[1]	GSMA IR.61	WLAN Roaming Guidelines (Inter-Operator Handbook)
[2]	IEEE Std 802.11-2012,	Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.
[3]	Hotspot 2.0 MRD	Wi-Fi Alliance Marketing Requirements Document that specifies an industry specification approach to announcement, authentication and security for public hotspots in a way that is transparent to the user
[4]	Hotspot 2.0 Release 1 Specification	Wi-Fi Alliance Release 1 specification for the WFA Passpoint™ Certification Program
[5]	IETF RFC 6241	Network Configuration Protocol (NETCONF)
[6]	BBF TR-069	CPE WAN Management Protocol
[7]	IETF RFC 4515	Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification
[8]	IETF RFC 3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
[9]	WBA NGH Security	White Paper on Next Generation Hotspot Security
[10]	WBA IPv6 Paper	Whitepaper on IPv6 deployment, WOG-IPv6-v1.0-01182014.docx
[11]	WRIX-i, WRIX-d, WRIX-f, WRIX-L	Wireless Broadband Alliance standards document that deals with the respective aspects of inter-operator data exchange as identified by the single letter subject area suffix: -i for Interchange deals with Walled Garden and AAA aspects; -d for Data deals with the exchange of summary usage data in the clearing process; -f for Financial deals with the financial aspects of the settlement process
[12]	3GPP TS 23.234	3GPP system to Wireless Local Area Network (WLAN) interworking; System description
[13]	3GPP TS 23.402	Architecture enhancements for non-3GPP accesses
[14]	3GPP TR 23.839	Support for BBF Accesses Interworking
[15]	3GPP TR 23.139	3GPP system - fixed broadband access network interworking; Stage 2
[16]	GSMA IR.62	End-to-End WLAN Roaming Test Cases
[17]	IETF RFC 4187	Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)
[18]	IETF RFC 5448	Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')
[19]	802.1X	IEEE Standard for port-based Network Access Control
[20]	IETF RFC 5555	Mobile IPv6 Support for Dual Stack Hosts and Routers
[21]	3GPP TS 29.273	Evolved Packet System (EPS); 3GPP EPS AAA interfaces
[22]	3GPP TS 29.274	3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C); Stage 3
[23]	3GPP TS 29.281	General Packet Radio System (GPRS) Tunneling Protocol User Plane (GTPv1-U)
[24]	3GPP TS 29.275	Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunneling protocols; Stage 3
[25]	3GPP TS 23.261	IP flow mobility and seamless Wireless Local Area Network (WLAN) offload; Stage 2
[26]	3GPP TS 33.402	Security Aspects of non-3GPP Accesses
[27]	3GPP TS 23.122	Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode
[28]	3GPP TS 24.302	Access to the 3GPP EPC via non-3GPP access networks
[29]	3GPP TS 24.303	Mobility management based on Dual-Stack Mobile IPv6; Stage 3
[30]	IETF RFC 3588	Diameter Base Protocol
[31]	IETF RFC 4186	Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)
[32]	IETF RFC 5216	The EAP-TLS Authentication Protocol
[33]	IETF RFC 5281	Extensible Authentication Protocol Tunneled Transport Layer Security

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

Ref	Document Number	Title
		Authenticated Protocol Version 0 (EAP-TTLSv0)
[34]	IETF RFC 2865	Remote Authentication Dial In User Service (RADIUS)
[35]	IETF RFC 3535	Overview of the 2002 IAB Network Management Workshop
[36]	3GPP TS 24.312	Access Network Discovery and Selection Function (ANDSF) Management Object (MO)
[37]	GSMA TS22	GSMA Minimal Wi-Fi Capabilities of Terminals, version 2
[38]	IETF RFC 6421	Network Configuration Protocol (NETCONF)
[39]	WFA Operator Best Practices for AAA Interface Deployment	Wi-Fi CERTIFIED Passpoint™ (Release 1), Operator Best Practices for AAA Interface Deployment, DRAFT Version 1.1, October 2012
[40]	IETF RFC 3411–RFC 3418	Simple Network Management Protocol v3
[41]	BBF TR-069	CPE WAN Management Protocol. TR-069 Amendment 5. Broadband Forum. January 2014

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

Appendix

A. WBA Industry Partner Bodies - Who Does What Now

This section describes the work being carried out by other industry bodies that is directly or indirectly connected to the features of Carrier Wi-Fi. It also describes a high level an overview of these industry bodies. As part of the process of writing this paper these bodies were asked directly for their opinion of their own work that is related to Carrier Wi-Fi. They will also be asked to comment on the contents of this WBA paper on Carrier Wi-Fi.

A.1 WBA

i. Organization Overview

Founded in 2003, the aim of the Wireless Broadband Alliance (WBA) is to secure an outstanding user experience through the global deployment of next generation Wi-Fi. The WBA and its industry leading members are dedicated to delivering this quality experience through technology innovation, interoperability and robust security:

- Business: Develops enablers for seamless connectivity and user experience across technologies, devices and operators
- Industry Engagement: Promote the adoption and benefits of Wi-Fi as a complementary service to other wireless broadband network services and champion WBA's engagements and the wider ecosystem
- Roaming: Lead and support development of roaming related technical specifications, guidelines, frameworks and best practices

ii. Carrier Wi-Fi Relevant Work

Within the WBA itself, there are work items that are relevant to Carrier Wi-Fi:

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

- Interoperability Compliancy Program: WBA operator members use a tool called Wi-Fi Roaming Compliancy Check to promote their compliancy and roaming capabilities in the community
- GSMA / WBA Joint Roaming Task Force (phase 3): The task force is expected to reconvene in 2014 to discuss Wi-Fi roaming issues, including WRIX Specifications
- Small Cell Forum / WBA joint work group: Studies issues relevant to integrated small cell / Wi-Fi networks
- WBA Roaming Enhancements work group: Maintains WRIX-i (Interconnect), WRIX-l (Location), WRIX-d (Data Clearing), and WRIX-f (Financial Settlement)
- NGH Trial work group: Facilitates operator conducted trials of Wi-Fi network NGH functionality

A.2 WFA

iii. Organization Overview

Wi-Fi Alliance® is a global non-profit industry association of companies devoted to Wi-Fi seamless connectivity. The Wi-Fi CERTIFIED™ program was launched in March 2000. It provides a widely recognized designation of interoperability and quality, and it helps to ensure that Wi-Fi-enabled products deliver the best user experience. Wi-Fi Alliance has certified more than 15,000 products.

iv. Carrier Wi-Fi Relevant Work

The following existing WFA core certifications are relevant to Carrier Wi-Fi:

- Wi-Fi products based on IEEE radio standards: 802.11a, 802.11b, 802.11g in single, dual mode (802.11b and 802.11g) or multi-band (2.4GHz and 5GHz) products. Now also required by CTIA for Wi-Fi enabled handsets seeking CTIA certification
- WPA2™ (Wi-Fi Protected Access 2): Wi-Fi wireless network security - offer government-grade security mechanisms for personal and enterprise
- EAP (Extensible Authentication Protocol): An authentication mechanism used to validate the identity of network devices (for enterprise devices)
- Protected Management Frames: Wi-Fi CERTIFIED WPA2 with Protected Management Frames extends WPA2 protection to unicast and multicast management action frames, which will play an increasing role in emerging applications
- Wi-Fi CERTIFIED n: Supports the IEEE 802.11n ratified standard. This test program also includes Wi-Fi Multimedia (WMM) testing
- Wi-Fi CERTIFIED ac: The first generation of Wi-Fi that can deliver up to gigabit per second data rates. Based on IEEE 802.11ac, this program requires devices to successfully pass all certified n tests

The following existing WFA optional certifications are relevant to Carrier Wi-Fi:

- Passpoint™: (Release 1) Enables mobile devices to automatically discover and connect to Wi-Fi networks. Passpoint also automatically configures industry-standard WPA2™ security protections without user intervention. Passpoint certifies products which implement technology defined in the Wi-Fi Alliance Hotspot 2.0 Technical Specification.
- Wi-Fi Protected Setup™: Facilitates easy set up of security features using a Personal Identification Number (PIN) or other defined methods within the Wi-Fi device. Wi-Fi Protected Setup certifies products which implement technology defined in the Wi-Fi Simple Configuration Technical Specification

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

- WMM® (Wi-Fi Multimedia™): Support for multimedia content over Wi-Fi networks enabling Wi-Fi networks to prioritize traffic generated by different applications using QoS mechanisms. WMM certifies products which implement technology defined in the WMM Technical Specification
- WMM-Power Save: Power savings for multimedia content over Wi-Fi networks - helps conserve battery life while using voice and multimedia applications by managing the time the device spends in sleep mode
- Voice-Personal: Voice over Wi-Fi - extends beyond interoperability testing to test the performance of products and help ensure that they deliver good voice quality over the Wi-Fi link
- CWG-RF: For converged devices with both Wi-Fi and cellular technology - provides detailed information about the performance of the Wi-Fi radio in a converged handset, as well as how the cellular and Wi-Fi radios interact with one another. Now mandatory for Wi-Fi enabled handsets seeking CTIA certification
- Voice-Enterprise: Supports a good experience with voice applications over Wi-Fi, enabling fast transitions between access points and providing management. Voice-Enterprise builds on the Voice-Personal certification features
- WMM-Admission Control: Enhanced bandwidth management tools to optimize the delivery of voice and other traffic in Wi-Fi® networks. WMM-Admission Control certifies products which implement technology defined in WMM Technical Specification

A.3 CableLabs

v. Organization Overview

Founded in 1988 by cable operating companies, Cable Television Laboratories, Inc. (CableLabs®) is a non-profit research and development consortium that is dedicated to pursuing new cable telecommunications technologies and to helping its cable operator members integrate those technical advancements into their business objectives.

Cable operators have deployed and operate large scale Wi-Fi networks. Therefore, CableLabs has a number of active wireless projects that include technical assessments of emerging technologies, specification work on how to integrate Wi-Fi with cable networks, and Wi-Fi interoperability tests.

CableLabs works within the wireless forums such as the IEEE, WBA, WFA and 3GPP as needed to ensure cable operator requirements are incorporated into WLAN specifications and certification programs. Publicly available CableLabs specifications include operator managed Wi-Fi requirements for integrated cable modems, and network to network interfaces to support inter-network Wi-Fi roaming.

vi. Carrier Wi-Fi Relevant Work

Current areas of focus include Passpoint, IPv6, community Wi-Fi scenarios, operator methods to manage massive Wi-Fi deployments, mobile device evolution and inter-network roaming.

A.4 GSMA

vii. Organization Overview

The GSM family of technologies has provided the world with mobile communications since 1991. In over twenty years of development, GSM has been continually enhanced to provide

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

platforms that deliver an increasingly broad range of mobile services as demand grows. Mobile technologies and standards managed by GSMA include:

- GSM :An open, digital cellular technology used for transmitting mobile voice and data services
- GPRS: A very widely deployed wireless data service, available now with most GSM networks
- EDGE: GSM Evolution (EDGE) technology provides up to three times the data capacity of GPRS
- WCDMA: The air interface for one of the International Telecommunications Union's family of third-generation (3G) mobile communications systems
- HSPA: The set of technologies that enables operators to upgrade their existing 3G/WCDMA networks to carry more traffic and at faster speeds
- LTE: Designed to be backwards-compatible with GSM and HSPA, Long Term Evolution uses the OFDMA air interface, in combination with other technologies, to offer high throughput speeds and high capacity
- GSM Roaming: The ability for a customer to make and receive calls, send and receive data, or access other services when travelling outside the coverage area of their home network

viii. Carrier Wi-Fi Relevant Work

Terminal Steering Group (TSG) Wi-Fi Working Group (TSGWIF)

TSG facilitates operator and vendor alignment to drive terminal related matters for the benefit of the entire mobile ecosystem. It manages/coordinates terminal capability requirements activities within GSMA and beyond.

The TSGWIFI working group documents key principles for the support of usability, authentication, connection management and performance handling on the terminal and from those derives functional recommendations for the client/terminal/OS to be supported as well as inputs for further progress and specification in OMA, WFA & WBA, 3GPP related to the connection manager, the network support and the hotspot specifications.

Latest specification: TS.22 "Recommendations for Minimal Wi-Fi Capabilities of Terminals", Version 2, published September 2013. (http://www.gsma.com/newsroom/wp-content/uploads/2012/06/TS.22-v2.0.pdf)

Inter-Working, Roaming Expert Group (IREG)

IREG specifies technical, operational and performance issues supporting international roaming, taking into account 3G GSM evolutions. IREG focuses on the study, from compatibility and interoperability perspective, of the signaling and inter-working of roaming issues between Public Land Mobile Networks (PLMNs), Public Switched Telephone Networks (PSTNs), Integrated Services Digital Networks (ISDNs) and Public Packet Switched Networks (PPDNs) modes, to define, guidelines and test procedures for voice and data services.

Latest specification: IR.61 " WLAN Roaming Guidelines (Inter-Operator Handbook)", Version 6.0, published 25 October 2013.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

Transferred Account Data Interchange Group (TADIG)

Transferred Account Procedures (TAP) have supported Wi-Fi since 2003, however the TAP specification has since recently been reviewed and updated to bring in line with WBA Format WRIX-D.

Latest specification: TD.57 “Transferred Account Procedure”, Version 3.120, published 1 May 2013.

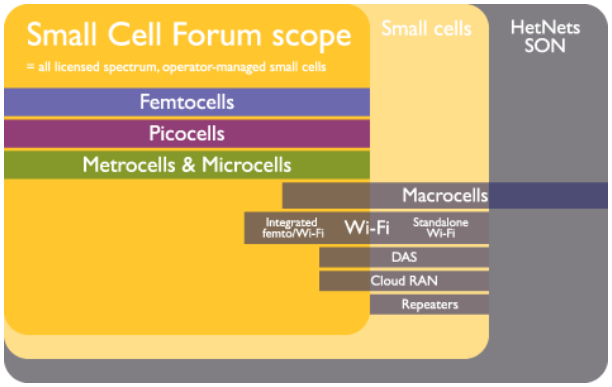
A.5 Small Cell Forum (SCF)

ix. Organization Overview

Overview text & diagram attribution: http://www.smallcellforum.org

The Small Cell Forum supports the wide-scale adoption of small cells. The mission of SCF is to accelerate small cell adoption to change the shape of mobile networks and maximize the potential of the mobile internet.

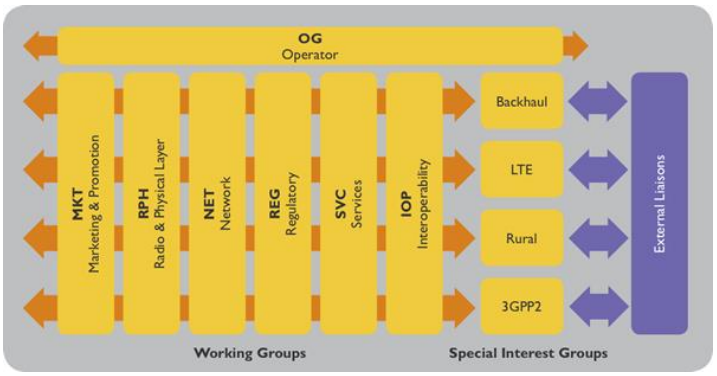
The scope of the work incorporates all small cell technology that uses licensed spectrum and is managed by a carrier, concerned with the multiple ways in which licensed small cells can be deployed by carriers across network architectures including metro femto, rural femto, metrocells, picocells and microcells.



In some areas SCF cooperates with organizations where they overlap or integrate with small cells, such as the interworking of unlicensed technologies such as Wi-Fi. Other areas may also be represented in SCF work-streams where they overlap with small cell technology (for example this may include HetNet, SON, Cloud RAN and DAS).

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

Small Cell Forum work-streams:



x. Carrier Wi-Fi Relevant Work

- The potential to simplify Wi-Fi APs by placing some of their current functions (e.g. authenticator) in a more centralized controller

A.6 3GPP

xi. Organization Overview

The 3rd Generation Partnership Project (3GPP) has six telecommunications standard development partner organizations (ARIB, ATIS, CCSA, ETSI, TTA, TTC), working to produce the Technical Reports(TR) and Technical Specifications (TS) that define 3GPP technologies:

- Global System for Mobile communication (GSM) including evolved radio access technologies General Packet Radio Service (GPRS) and Enhanced Data rates for GSM Evolution (EDGE)
- Universal Terrestrial Radio Access (UTRA) both Frequency Division Duplex (FDD) and Time Division Duplex (TDD) modes
- Evolved Universal Terrestrial Access Network (E-UTRAN, also known as LTE) ,and the Evolved Packet Core (EPC)

The four Technical Specification Groups (TSG) in 3GPP are:

a. Radio Access Networks (RAN)
b. Service & Systems Aspects (SA)
c. Core Network & Terminals (CT)
d. GSM EDGE Radio Access Networks (GERAN)

xii. Carrier Wi-Fi Relevant Work

- Several features have already been specified from Rel-6 for interworking with GPRS network and from Rel-8 for enabling the connection of a 3GPP UE from the so called Non-3GPP accesses, that include WLAN, to the 3GPP EPC mobile core network. The specifications enables authentication, session continuity between 3GPP and WLAN over S2c and S2b interfaces, interworking with Fixed Broadband access, charging, etc.
- Further enhancements on WLAN interworking are on-going in 3GPP Release 12 which is scheduled to complete in June 2014 include:

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

- WLAN Network Selection for 3GPP Terminals: It aims to enhance existing 3GPP solutions for network selection for WLAN by taking into account of operator' policies for network discovery and network selection and WFA Hotspot 2.0 solutions
- S2a Mobility based On GTP and WLAN access to EPC: The solution allows a GTP option to enable network-based mobility through the trusted WLAN access via the EPC
- Optimized Offloading to WLAN in 3GPP-RAT mobility: It aims to enable the differentiation of 3GPP RATs (e.g. E-UTRAN versus UTRAN, GERAN vs. UTRAN) with respect to WLAN, according to operators' policies
- Network Management for 3GPP Interworking WLAN: It is to define the Management Information Objects and Performance Management data for the completed the 3GPP WLAN Interworking functions and interfaces

WLAN / 3GPP Radio Interworking

3GPP RAN is working on study RP-122038 on WLAN/3GPP Radio Interworking. The objectives of this study are to evaluate LTE-WLAN and UTRA-WLAN interworking procedures while improving seamless and non-seamless mobility. The study applies solely to WLAN APs deployed and controlled by cellular operators and their partners. The study covers both collocated and non-collocated H{e}NBs/eNBs/NodeBs and WLAN APs. Also the study takes into account existing IEEE 802.11 specifications.

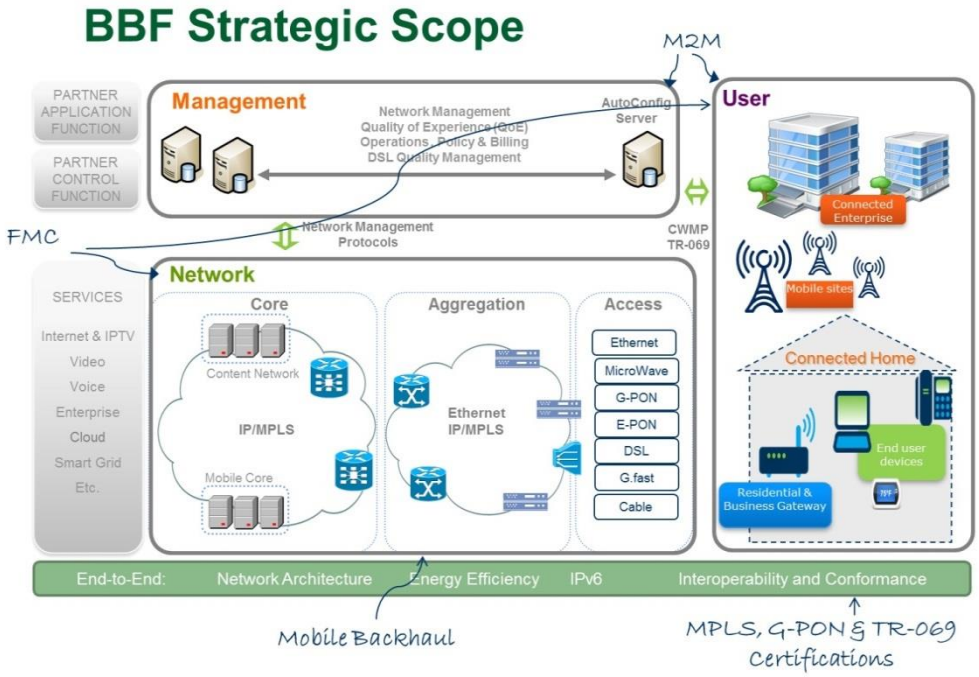
A.7 Broadband Forum (BBF)

xiii. Organization Overview

Overview text & diagram attribution: ***http://www.broadband-forum.org/***

The BBF is drives broadband wire-line solutions empowering converged packet networks to better meet the needs of vendors, service providers and their customers. The BBF develops multi-service broadband packet networking specifications addressing interoperability, architecture and management. Their work enables home, business and converged broadband services, encompassing customer, access and backbone networks.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance



The Broadband Forum packages technical reports into distinct Broadband Suite Releases:

- 1.0 provides the technical reports needed to deliver basic high speed internet access over ADSL
- 2.0 increases the speed by including ADSL2/2plus specifications and addressing the remote management requirements of the networked home
- 3.0 brings fiber and bonded options into the mix, and provides specifications that ensure quality IPTV deployment and management
- 3.1 adds VDSL2 specifications
- 3.2 specifies the next generation home networking and management platform
- 4.0 provides integration and migration solutions for network and management support of the new numbering protocol- IPv6
- 4.1 offers tools and techniques for enhancing service delivery and support of the Connected Home
- 5.0 provides the architecture, management and testing tools needed to ensure interoperability in PON deployments
- 6.0 offers a package of 4G/LTE Ready Mobile Backhaul specifications and resources
- 6.1 provides a Super-fast Broadband kit of tools to optimize DSL capabilities (vectoring, bonding, splitters, etc) and the latest in DSL Quality Management
- 6.2 Fibre Interoperability Suite expands the BBF.247 ONU certification program to address new VLAN profiles and functionality test, and offers a companion OLT/ONU interoperability test plan

xiv. Carrier Wi-Fi Relevant Work

BBF is in progress of developing a working text, WT-321, entitled “Public Wi-Fi Access in Multi-service Broadband Networks”. Following are the content of sections “scope” and “Purpose” of this document, liaised to the WBA by the BBF on 19-Sept-2013:

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

Purpose

Since the introduction of mobile devices that include Wi-Fi, there has been an increasing interest in improving Broadband Forum's multi-service broadband architecture to incorporate the public Wi-Fi access. The rise in the use of smartphones at public hotspots has accelerated this interest. As the popularity of Wi-Fi enabled devices along with access to Internet and other data services continues to increase, an emerging ecosystem is taking shape where applications are developed largely independently of access types. There is increased desire to provide network capabilities that offer better user experiences and more efficient network utilization for these devices and this is becoming a requirement for operators that wish to provide superior user experiences.

Scope

The WT-321 scope includes, use cases, physical and logical architecture and functional and/or nodal requirements for public Wi-Fi access capabilities that are used nomadically as part of a broadband network. Architecture includes data, signaling, and management, as well as functional decomposition and placement into network nodes. Functional and nodal requirements will be considered for the following: Wi-Fi Access Point (AP), Residential Gateway (RG), CAPWAP Access Controller (AC), Broadband Network Gateway (BNG). The scope also includes potential interactions with PDP and/or Authentication Authorization Accounting Server (AAA).

WT-321 covers requirements on:

- The potential to simplify Wi-Fi APs by placing some of their current functions (e.g. authenticator) in a more centralized controller
- Retain the current capability for a single physical AP to host multiple Wi-Fi providers and services
- Vetting the use of CAPWAP as the protocol supporting centralization of AP control, and then building upon this or the chosen protocol as necessary
- AP control (including authentication and management) deployed as an overlay over the broadband access - regardless of type
- Traffic management of AP broadband access supporting both aggregate traffic management between Wi-Fi service providers and also per-subscriber traffic management
- Support for both co-located and also separated AC and BNG
- Mutual authentication between APs and ACs
- Authentication of attaching devices using the AP or AC as the authenticator
- Security mechanisms including key management
- Reliability mechanisms
- The support of location based services
- Client connection management, including choice of AP
- Interoperability between the AP and AC
- The interface between an AC and broadband network. Wider SDO Inputs

A.8 IEEE Standards Association (IEEE-SA)

xv. Organization Overview

IEEE-SA develops and maintains standards in cross a wide range of engineering domains, driving the functionality, capabilities and interoperability of a wide range of products and services.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

The IEEE-SA standards development process is open to IEEE-SA members and non-members. However, IEEE-SA membership is required to participate in additional balloting and participation opportunities. IEEE-SA members are the driving force behind the development of standards, providing technical expertise and innovation, driving global participation, and pursuing the on-going advancement and promotion of new concepts.

xvi. Carrier Wi-Fi Relevant Work

The IEEE 802 standards deal with local area networks (LAN) and metropolitan area networks (MAN). There are many Working Groups with 802, relevant Carrier Wi-Fi areas include:

- 802.1 Bridging and Network Management
- 802.1X Port Based Authentication
- 802.11 WLAN
- IEEE 802.11 High Efficiency Wireless (HEW) Study Group
- IEEE 802.11ai Fast Link Setup draft

A.9 IETF

xvii. Organization Overview

The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.

The IETF's standards development work is organized into eight Areas:

e. Applications
f. General
g. Internet
h. Operations & Management
i. Real-time Applications & Infrastructure
j. Routing
k. Security
l. Transport

Within each Area there are multiple Working Groups (WG). Each WG has one or more chairs who manage the work, and a written charter defining what the work is and when it is due. There are more than one hundred WGs. The WGs produce Internet Drafts (I-Ds) which often lead to the publication of an Internet standard as a Request For Comments (RFC).

The IETF is a completely open forum, there is no formal membership. Participating accept the IETF's rules, including the rules about intellectual property (patents, copyrights and trademarks).and participate as individuals, and never as company representatives.

xviii. Carrier Wi-Fi Relevant Work

- NETCONF (RFC 6241) : The “Network Configuration” working group in the Operations & Management Area of the IETF maintains the Network Configuration Protocol (NETCONF)
- SNMP (RFC 5343): The “Operations & Management” working group in the Operations & Management Area maintains the Simple Network Management Protocol (SNMP)

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

- RADIUS (RFC 3535): The “RADIUS Extensions” working group in the Operations & Management Area maintains the Remote Authentication Dial In User Service (RADIUS)
- Diameter (RFC 6733): The “Diameter Maintenance & Extensions” working group in the Operations & Management Area work group maintains Diameter (which is so named because it is an extension of RADIUS)

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

Acronyms And Abbreviations

Term	Description
3G	Third Generation Cellular network standard providing wide area voice and data service as defined by the International Telecommunications Union (www.itu.int)
3GPP	3rd Generation Partnership Project (www.3gpp.org)
4G	Fourth Generation Cellular network standard providing provisions for very high speed data traffic, with all traffic, including voice traffic, handled as packet switched, Internet Protocol traffic, as defined by the International Telecommunications Union (www.itu.int)
802.1X	IEEE Standard for port-based Network Access Control
AAA	Authentication, Authorization and Accounting, core functions commonly implemented through protocols like RADIUS [58] and Diameter [54]
ANDSF	Access Network Discovery and Selection Function
ANQP	Access Network Querying Protocol
AP	Access Point
API	Access Programming Interface
BSS	When one access point (AP) is connected to a wired network and a set of wireless stations, it is referred to as a Basic Service Set (BSS).
BSSID	Basic Service Set Identification
CAPWAP	Control And Provisioning of Wireless Access Points (RFC 5415)
CWLAN	Carrier Wi-Fi
Diameter	Authentication, authorization and accounting protocol for computer networks, and a successor to RADIUS [58]. (IETF RFC 3588 [54])
DoS	Denial of Service
DSMIPv6	Dual Stack Mobile IPv6
EAP	Extensible Authentication Protocol or EAP is used to pass the authentication information between the supplicant (e.g. the Wi-Fi device) and the authentication server (usually a radius server). The actual authentication is defined and handled by the EAP type.
EAP-AKA	Authentication method used with EAP to support authentication using a USIM, providing USIM Authentication and Key Agreement, as standardized in RFC 4187 [10]
EAP-AKA'	Authentication method used with EAP to support authentication of EAP-AKA [10] on networks that are not 3GPP compliant for 3GPP compliant devices, i.e. a device with a USIM wanting to authenticate on a Wi-Fi network would use EAP-AKA', as standardized in RFC 5448 [13]
EAP-SIM	Authentication method used with EAP to support authentication using a SIM, as standardized in RFC 4186 [55]
EAP-TLS	Authentication method used with EAP to support authentication through Transport Layer Security, in which secure digital certificates are used to mutually identify a user and a server's identity, as standardized in RFC 5216 [56]
EAP-TTLS	Authentication method used with EAP to support authentication through Tunneled Transport Layer Security, in which secure digital certificates are used to identify a server's identity (and optionally, a device's or user's identity), establish a tunnel, and then allow for user identification over the encrypted tunnel, as standardized in RFC 5281 [57] , Note that there is often an inner EAP method used with EAP-TTLS, such as MSCHAPv2
eNB or eNodeB	Evolved NodeB
ePDG	Evolved Packet Data Gateway
ESS	Extended Service Set: A set of two or more BSSs that form a single sub network.
GRE	Generic Routing Encapsulation
GSM	Global System for Mobility, generic name for a series of standards and associated operating practices commonly used in cellular equipment and networks to assure

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

Term	Description
	global mobility for users. These standards and associated processes are maintained by the GSMA.
GSMA	GSM Association, industry group made up of cellular network operators and associated companies that furthers the use and interoperation of the technology and plays an active role in setting standards for the industry. (www.gsma.org)
GTP	GPRS Tunneling Protocol
HLR	Home Location Register
HSS	Home Subscriber Server
ICP	WBA's Interoperability Compliance Program
IEEE 802.11	Institute of Electrical and Electronics Engineers LAN/MAN Standards committee 802 - Working Group 11 is a standard for implementing wireless local area network (WLAN) computer communication (*http://www.ieee802.org/11/)*
IEEE HEW	Institute of Electrical and Electronics Engineers High Efficiency WLAN, IEEE HEW Study Group http://www.ieee802.org/11/Reports/hew_update.htm
IETF	Internet Engineering Task Force, a body for the development and promotion of standards for and related to the Internet. (www.ietf.org)
IPv6	Internet Protocol version 6
LWAPP	Lightweight Access Point Protocol
MAPCON	Multi Access PDN Connectivity
MAC	Media Access Control Address
MCS	Modulation and Coding Scheme
MIMOM	Multiple-Input and Multiple-Output
MU-MIMO	Multi-User MIMO
NB	Node B
NGH	Next Generation Hotspot
NMS	Network Management System
NOC	Network Operations Centre
OMA DM	Device management protocol specified by the Open Mobile Alliance (OMA) Device Management (DM) Working Group and the Data Synchronization (DS) Working Group
PDG	Packet Data Gateway
PDN	Packet Data Network
PMF	Protected Management Frames (see IEEE 802.11-2012)
QoE	Quality of Experience
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service, a commonly used service for Authentication of user identity, Authorization of user service, and Accounting for service usage, as defined in IETF RFC 2865 [58] and its many associated RFCs (tools.ietf.org/html/rfc2865)
RAN	Radio Access Network
RAT	Radio Access Technology
RF	Radio Frequency
RFC	Request For Comments, the acronym used to identify IETF standards.
RRM	Radio Resource Management
RTS/CTS	Request To Send (RTS); applies on situations where Data Terminal Equipment requests the is prepare to receive data. Clear to Send (CTS); indicates the Data Communication Equipment is ready to accept data.
SDO	Standard Developing Organization
SIM	Subscriber Identity Module, earlier a chip-based module that provides the identity for a mobile subscriber which is included in mobile phones using the GSM system. Nowadays an application that resides in UICC
SNMPv3	Simple Network Management Protocol v3 IETF RFC 3411–RFC 3418
SON	Self-Organizing Network

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

Term	Description
SS7	Signaling System No. 7 set of telephony signaling protocol
SSID	Service Set identification
STA	Station, WFA term for UE or AP
TAP	Transferred Account Procedure
TPC	Transmit Power Control
TWAG	Trusted Wireless Access Gateway
UE	User Equipment, 3GPP terminology for devices and terminals
UICC	Universal Integrated Circuit Card is the smart card used in mobile terminals in GSM and UMTS networks
USIM	Authentication application that resides on UICC and provides AKA authentication for UMTS networks
VLR	Visitor Location Register
WBA	Wireless Broadband Alliance, industry group made up of primarily Wi-Fi network operators and equipment vendors to further the use of wireless technologies. (www.wballiance.org)
WFA	Wi-Fi Alliance (www.wi-fi.org)
Wi-Fi	Originally called Wireless Fidelity, Wi-Fi is a wireless air interface/technology that allows an electronic device to exchange data wirelessly over a computer network, including high-speed Internet connections
WISPr	Wireless Internet Service Provider roaming
WLAN	Wireless Local Access Network
WLAN SS	WLAN SON Sever
WMM	Wi-Fi Multimedia
WPA2	Wi-Fi Protected Access II
WRIX	Wireless Roaming Intermediary Exchange, a series of recommendations and operating procedures defined by the WBA to assist in the facilitation of roaming traffic on public Wi-Fi hotspots. WRIX-I defined the interchange portion, dealing with operation aspects of hotspot operation and AAA. WRIX-d deals with data exchange of traffic related information, and WRIX-f deals with financial aspects of settlement and clearing. WRIX–I deals with the maintenance and exchange of location information

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

Document History

Version	Revision date	Revised by	Description of change
0.03	7 August 2013	Orange & CableLabs	Sec 2, 3, 5 added
0.04	8 August 2013	Orange & CableLabs	Sec 5 + Refs & Acronyms added
0.05-0.16	August to December 2013	Various	Other Secs added
0.20	20 December 2013	Orange	Draft version for Final comments
0.29	6 February 2014	Orange et al	Final version after all comments addressed
0.30	7 February	Orange	Editorial Review

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance

Participant List

Company
Accuris Networks
AT&T
BSG Wireless
BskyB
BT
CableLabs
China Mobile
Cisco Systems
Comcast
Ericsson
Huawei
Intel Corporation
NTT DOCOMO
Orange
Qualcomm
Ruckus Wireless
SK Telecom
Time Warner Cable
Towerstream

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2014 Wireless Broadband Alliance