IEEE P802.11
Wireless LANs

802.11

Liaison statement from WBA on Community Wi-Fi **

Date: 2014-11-03

Author(s):

Name	Company	Address	Phone	email
Adrian Stephens	Intel Corporation			Adrian.p.stephens@intel.com

Abstract

This document contains a liaison from the Wireless Broadband Alliance (WBA).

From: Tiago Rodrigues
Sent: Monday, September 15, 2014 4:16 AM
To: Bruce Kraemer
Subject: FW: Liaison statement to IEEE

Dear Bruce,

See in attach a liaison statement to IEEE.
The LS is to share with IEEE the WBA Community Wi-Fi white paper.

Let me know if you have any additional question.

Best Regards,
Tiago Rodrigues

** Certain names may be claimed as the property of others.

www.wballiance.com
Wireless Broadband Alliance
3 Tai Seng Drive
#04-01
Singapore 535216
E-mail contactus@wballiance.com

Wireless
Broadband Alliance
Driving next generation Wi-Fi experience

3rd November 2014

Adrian P Stephens
IEEE 802.11 Working Group Chair
IEEE Operations Center
445 Hoes Lane
Piscataway, NJ 08854-4141 USA

Dear Dr Stephens,

I am authorized to grant permission to use the material in connection with the IEEE Project noted below, including public review of the material.

P802.11 – Wireless LANs

WBA Community Wi-Fi White Paper V1.0, post entire document on the 802.11 document server.

Non-exclusive, irrevocable, royalty-free permission to use this material is granted for world rights distribution, with permission to modify and reprint in all future revisions and editions of the resulting draft and approved IEEE standard, and in derivative works based on the standard, in all media known or hereinafter known.

Yours sincerely,

Tiago Rio Machado Rodrigues
Senior Director - PMO & Membership Services

The following acknowledgment requirements should be met:
Include an acknowledgment in the front matter and use the standard IEEE attribution footnote as shown: Community Wi-Fi White Paper reprinted with permission from WBA ©2014

Wireless
Broadband Alliance
Driving next generation Wi-Fi experience

Community Wi-Fi White Paper

Source: **WBA**
Author: WBA
Issue date: 12 September 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 including 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 one billion subscribers and operate more than 10 million hotspots globally. The WBA Board includes Arqiva, AT&T, Boingo Wireless, BT, 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

More information about WBA: contactus@wballiance.com

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 organizations who may have contributed to this document) make 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 organizations 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 organizations 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.

Contents

Tables

Figures

Executive Summary

Wi-Fi is becoming the access network of choice for both communication service providers (CSPs) and consumers alike. Because of this surge, the last few years have seen renewed interest in large scale Wi-Fi deployments from CSPs.

Many CSPs across the world are deploying public Wi-Fi hotspots to meet the demands of their customers. Yet while deploying dedicated public Wi-Fi hotspots is a great way to provide public Wi-Fi services to customers in areas such as malls, stadiums, and parks, they may not be the most economical tool to provide similar services in residential neighborhoods and sparsely populated areas.

CSPs are complementing their public Wi-Fi hotspot deployments by using existing Wi-Fi assets, for instance residential or small and medium business (SMB) Wi-Fi gateways, to provide public Wi-Fi services to customers in residential neighborhoods, as the so-called Community Wi-Fi. This allows CSPs to use an existing residential broadband connection as backhaul for both public and private Wi-Fi services.

While the concept of Community Wi-Fi networks is relatively new, there are a number of network deployments in operation globally. Community Wi-Fi networks are actively being deployed across Europe, North America and East Asia by a variety of operators including cellular, over the top, and broadband service providers.

In order to offer Community Wi-Fi services, an operator enables a residential Wi-Fi GW with two Wi-Fi service set Identifiers (SSIDs), consisting of a private SSID (i.e., the residential Wi-Fi network) and public SSID (i.e., the Community Wi-Fi network). These public SSIDs need to be operator brand worthy. Therefore, public SSIDs in community Wi-Fi deployments should meet the carrier Wi-Fi requirements contained in the Carrier Wi-Fi Guidelines document (available at WBA website: http://www.wballiance.com/resource-center/wba-white-papers/).The requirements address a range of feature sets focused on user experience, security, Passpoint support, resource management, 3GPP aspects and network management.

The main motivations for developing this whitepaper are to:

- Document Community Wi-Fi service levels, network architecture, and implementation details
- Identify challenges and technology gaps
- Learn and document experience from current Community Wi-Fi deployment
- Enable operators to offer consistent and predictable customer experience

Considerations and Challenges

There is a vast array of implementation choices that a CSP faces when deploying Community Wi-Fi. This whitepaper splits these choices into three primary service levels corresponding with:

- What is achievable today with little to no infrastructure modification
- What is technically achievable today (but may require substantial hardware/software rollout)
- What could be achievable in the future if all technological gaps are addressed

Additionally, Community Wi-Fi relies on a varied array of interconnected devices to provide the desired public access, with expected high levels of security and accountability, all while preserving the private user's subscribed level of service.

At the same time, operators pursuing Community Wi-Fi are equally interested in deploying architecture and interfaces that allow for network scalability (e.g., millions of access points (APs) and tens of millions of client devices), multi-vendor interoperability, and a consistent user experience.

This whitepaper reviews the following considerations:

- Dimensioning of the network and understanding Community Wi-Fi use cases, call flows, and architectural options
- Preference for a distributed architecture so that user data traffic can break out at the edge as well as separation of control plane and data plane
- Traffic separation/bandwidth control of private and public SSID traffic
- A radio resource management (RRM)
- Network management system and servicing network components in the core network such as authentication, authorization, and accounting (AAA), Wi-Fi controllers, and session routers
- IPv6 considerations
- CPE provisioning and management
- Radio frequency (RF) optimization
- Cellular interworking
- Session mobility
- Security and privacy

Gap Analysis

The result of the gap analysis is based upon the topics discussed in this paper. 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 Community 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 long-term evolution of technology. Therefore, the gap analysis recommends general timeframes for the development of work plans to close the gaps

Next Steps

The WBA will liaise this 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 later versions of this document.

In addition, where gaps have been identified, 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 this Community Wi-Fi paper.

1. Introduction

Wi-Fi is becoming the access network of choice for both CSPs and consumers alike. This fast moving trend has motivated a renewed interest in large scale Wi-Fi deployment by CSPs over recent years.

There are a number of factors influencing this phenomenon. For example, more than ever, consumer electronics manufacturers are shipping products that are Wi-Fi enabled. Even the products that support connectivity using 3GPP and 3GPP2 include support for Wi-Fi. Additionally, consumer preferences are evolving as well, as more consumers are demanding 24/7 Internet access everywhere.

Many CSPs across the world are deploying public Wi-Fi hotspots to meet the demands of their customers. Yet while deploying dedicated public Wi-Fi hotspots is a great way to provide Wi-Fi services to customers in areas such as malls, stadiums, and parks, they may not be the most economical tool to provide similar services in residential neighborhoods and sparsely populated areas.

CSPs are complementing their public Wi-Fi hotspot deployments by using existing Wi-Fi assets, for instance residential and SMB Wi-Fi gateways, to provide public Wi-Fi services to customers in residential neighborhoods, as the so-called Community Wi-Fi. This allows CSPs to use an existing residential broadband connection as backhaul for both public and private Wi-Fi services. Private Wi-Fi is for exclusive use by the ‘broadband customer’ who is paying for broadband services to their home. The public Wi-Fi is a resource for the operator to provide services to other customers. The use of residential and SMB Wi-Fi assets in this manner not only opens up new opportunities, but also challenges, for all service providers involved. This whitepaper documents the challenges, solutions, gap analysis and experiences relevant to the use of residential and SMB Wi-Fi gateways to offer both private and public Wi-Fi services.

1.1 Motivation

While the concept of Community Wi-Fi networks is relatively new, at the time of writing there are a number of Community Wi-Fi network deployments in operation globally. Community Wi-Fi networks are actively being deployed across Europe, North America and East Asia by a variety of operators including cellular, over the top, and broadband service providers. Some Community Wi-Fi networks report as many as 12 million Community Wi-Fi active and deployed APs. Additionally, it is projected that the number of Community Wi-Fi networks is going to grow in the near future.

A few examples of operators deploying Community Wi-Fi networks include:

Figure 1:1 Example List of Operators Deploying Community Wi-Fi

The main motivations for developing this whitepaper in WBA are to:

- Document Community Wi-Fi network architecture and implementation details
- Document Community Wi-Fi service levels
- Identify challenges and technology gaps

- Learn and document experience from current Community Wi-Fi deployments.
- Also, enable operators to offer consistent and predictable customer experience by deploying
- Highly scalable architecture and protocols
- Reliable, and secure network access
- Manageable networks
- Networks that support expandable business opportunities (e.g., cellular data offload, retail)

2. Definition and Use Cases

This section intends to provide a definition and potential application areas of this technology. Also, the alignment with WBA work in areas such as Carrier Wi-Fi is addressed.

2.1 Definition

Community Wi-Fi networks allow operators to offer Wi-Fi network access to their on-the-go subscribers by using existing residential and SMB Wi-Fi infrastructure. Operators can also use this coverage to offer services to retail and roaming partner operators' subscribers.

The residential subscribers accessing the network from inside their homes have prioritized access to Wi-Fi and backhaul resources. Roaming and on-the-go subscribers are only allowed to use Wi-Fi network capacity that is not currently used by the subscriber at home. The residential Wi-Fi infrastructure is configured in a manner that allows both residential and visitor subscribers to access Wi-Fi resources simultaneously in a manner that affords security, privacy, and service quality for both.

In order to offer Community Wi-Fi services, an operator enables a residential Wi-Fi gateway with two Wi-Fi SSIDs, consisting of a private SSID (i.e., the residential Wi-Fi network) and public SSID (i.e., the Community Wi-Fi network). Where "user" is defined as the end service subscriber, and "operator" is defined as the CSP. The table below defines the basic characteristics of private and public SSID in the current context:

	Private SSID	Public SSID
Purpose	Private SSID on the residential gateway is for exclusive use by the "broadband customer" paying for broadband services for that residence	Public SSID on the residential gateway is for the operator to provide services to other customers
SSID Configuration	Preconfigured by operator and/or configured by customer	Operator managed/configured SSID
Admission Control	Residential customer controls access on private SSID	Operator controls access on public SSID
Traffic Separation	Customers on the public SSID on the same residential GW are not allowed to communicate directly with the devices on the private SSID	Two users on the public SSID are not allowed to communicate with each other directly. Additionally, users on the public SSID cannot directly communicate with the devices on the private SSID
Security	Customer may or may not enable authentication/encryption	All users of the Community Wi-Fi services shall use network authentications such as WPA2-PSK, WPA2-ENTERPRISE, or web authentication (assuming a secured Wi-Fi interface)
Services	Operator uses the private SSID to offer services (e.g., voice, video) to the broadband customer	Operators may offer different services to different customers on the public SSID

	Private SSID	Public SSID
Protection of traffic on private SSID	Different priority to traffic on the private SSID than the traffic on public SSID	Different Quality of Service (QoS) profiles to different customers or groups of customers on public SSID
QoS on the Backhaul network	Since both private and public SSID are hosted on a single residential gateway, the same physical network is used to backhaul traffic on both private and public SSID. Different treatment (e.g., QoS, forwarding) of traffic from public and private SSID	Since both private and public SSID are hosted on a single residential gateway, the same physical network is used to backhaul traffic on both private and public SSID. Different treatment (e.g., QoS, forwarding) of traffic from public and private SSID
Accounting	No need for per user accounting on private SSID	Per user accounting is a requirement

Table 2:1 Basic Characteristics of Private and Public SSID

2.2 Wireless Broadband Alliance Carrier Wi-Fi Guidelines and Community Wi-Fi

Public SSIDs that are managed by operators on residential or enterprise APs share a common goal with public SSIDs on metropolitan (metro) APs; the need to be operator brand worthy. Therefore, public SSIDs in Community Wi-Fi deployments should meet the carrier Wi-Fi requirements contained in the WBA Carrier Wi-Fi Guidelines document. The requirements address a range of feature sets focused on user experience, security, Passpoint, resource management, 3GPP aspects and network management. Please see the WBA Carrier Wi-Fi Guidelines document for a full description of the functional requirements.

3. Implementation considerations

Building out a network has many challenges, while the construction of a community Wi-Fi deployment is in many ways even more challenging because of the need to balance public and private networks, service levels and technologies. From traffic management and prioritization between public and private SSIDs, covering access network QoS, gateway QoS, radio resource allocation and QoS, to network architecture and interfaces, including architecture deployment models, cellular interworking model, and IPv4 and IPv6 based non-tunnelled architectures, to scalability challenges and network security and privacy, CSPs are faced with a gamut of problems to overcome in bringing community Wi-Fi to the masses. This section seeks to cover the implementation choices for CSPs.

There are a vast array of implementation choices that a CSP faces when deploying Community Wi-Fi. This section aims to cover the following implementation choices:

- Service Levels, containing three different implementation scenarios
- Network architecture and interfaces, including architecture deployment models, cellular interworking model, and IPv4 and IPv6 based non-tunnelled architectures
- Network scalability challenges
- Traffic separation between private and public networks, and traffic forwarding
- Traffic management and prioritization between public and private SSIDs, covering access network QoS, gateway QoS, radio resource allocation and QoS
- Network selection and operator policy implementation, either client-centric or infrastructure-centric
- CPE provisioning and management, to remotely provision, manage and monitor the CPE
- RF optimization, to manage and minimize radio interference
- Radio conformance
- Cellular interworking requirements, including service continuity
- IPv6 requirements

- Session mobility, including continuity scenarios within a single operator, and when interconnected to a mobile network
- Network security and privacy
- Location information requirements
- Lawful intercept
- Hotspot 2.0 (HS2.0) implementation, including device provisioning, roaming and network enablement

3.1 Service Levels

3.1.1 Introduction

This section defines three primary service levels corresponding with what is:

- Achievable today with little to no infrastructure modification
- Technically achievable today but may require substantial hardware/software rollout
- What could be achievable in the future if all technological gaps are addressed

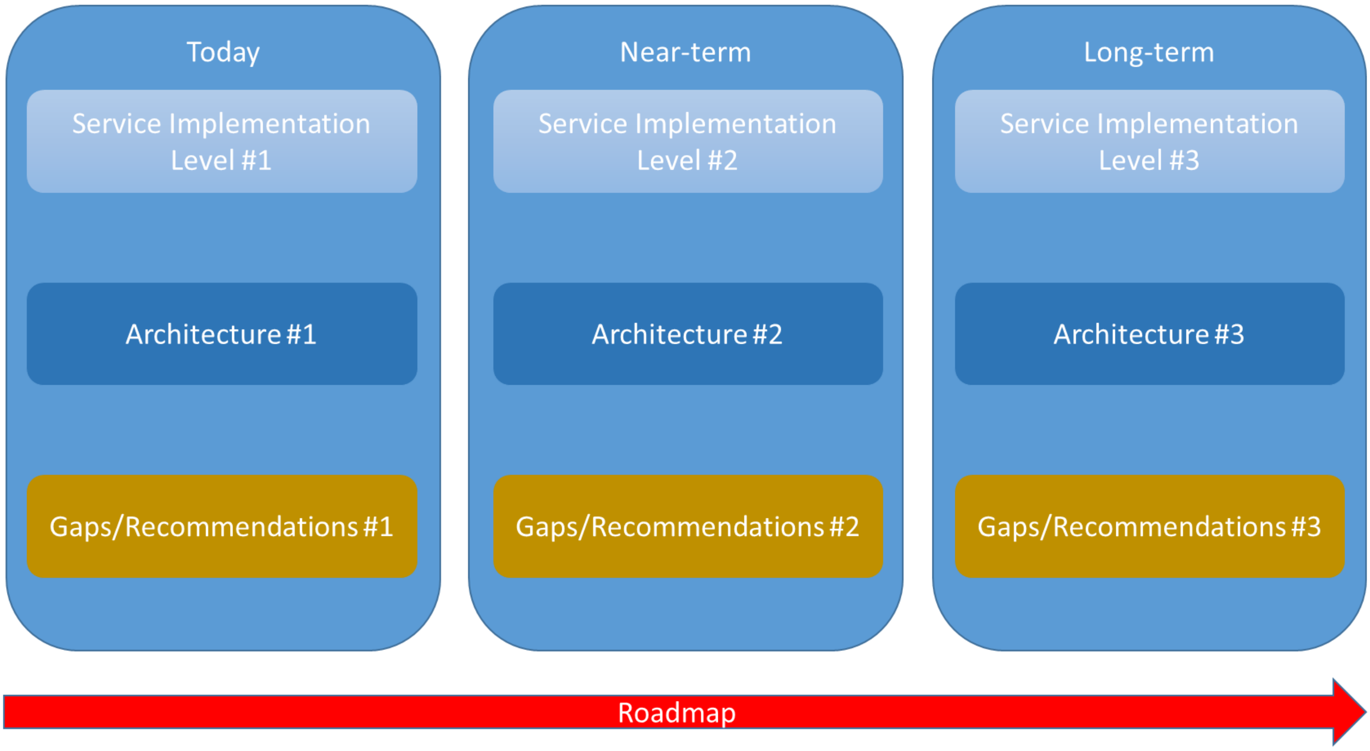


Figure 3:1 Service Implementation Level

3.1.2 Service Implementation Level 1

This is what can be deployed today in the majority of CSP networks:

Feature	Status
Architecture	See Figure 3:2 in section 3.2.2 - Community Wi-Fi Architecture #2
Network selection	Manual network selection or user device application
QoS	Wi-Fi multimedia (WMM)/802.11e, access network prioritization (e.g., Data Over Cable Service Interface Specification (DOCSIS) service flow), wireless access gateway (WAG) QoS, static admission

Feature	Status
	control. Upstream QoS cannot be guaranteed
Traffic separation and forwarding	Generic routing encapsulation (GRE), SoftGRE
Security	Open SSID with web authentication and Media Access Control (MAC) caching, peer-to-peer blocking
Session mobility	Non-seamless mobility between two Community Wi-Fi APs
IPv4 or IPv6	IPv4
RF optimization	None
Customer premises equipment (CPE) provisioning and management	Simple Network Management Protocol - Management Information Base (SNMP MIBs) or other proprietary methods
Radio conformance	No carrier Wi-Fi certification
Cellular interworking	None
Gaps	Hotspot location information may be utilized, but there is no standard for this information currently.

Table 3:1 Service implementation level 1

3.1.3 Service Implementation Level 2

This is what can potentially be deployed in the near future on top of service implementation Level 1:

Feature	Status
Architecture	See Figure 3:2 and Figure 3:4 in section 3.2.2 – Community Wi-Fi Architecture #2
Network selection	HS2.0 release 1, network-side service selection, manual network selection, user device application
QoS	Context aware prioritization (e.g., application type, location, user subscription, etc.), transmission control protocol (TCP) throttling, dynamic admission control, WMM/802.11e, access network prioritization (e.g. DOCSIS service flow), static admission control
Traffic separation and forwarding	GRE, SoftGRE, PMIP
Security	Secure SSID (WPA2-Personal / Enterprise), intrusion detection system/intrusion prevention system (IDS/IPS), open SSID with captive portal and MAC authentication peer-to-peer blocking
Session mobility	Mobility between Community Wi-Fi and Hotspot Wi-Fi, and between two Community Wi-Fi APs
IPv4 or IPv6	IPv4 and IPv6
RF optimization	Automatic channel selection on the AP, dual band dual concurrent (DBDC), self-organizing network (SON)
CPE provisioning and management	SNMP MIBs, TR-069 with standardized data model (see Annex A), Dynamic Host Control Protocol (DHCP), Trivial File Transfer Protocol (TFTP)
Radio conformance	Initial carrier Wi-Fi certifications (WFA)
Cellular interworking	Roaming (authentication and accounting only, no session mobility)
Gaps	Dynamic admission control, context aware QoS, management MIBs and data models

Table 3:2 Service Implementation Level 2

3.1.4 Service Implementation Level 3

This is what could be deployed in the long term on top of service implementation Level 1 and 2:

Feature	Status
Architecture	See Figure 3:5 in section 3.2.3 – Interworking with Mobile Network
Network selection	HS2.0 release 2, solution for public vs. private SSID prioritization, whitelist/blacklist, manual network selection, user device application, 3GPP access network discovery and selection function (ANDSF)
QoS	Full public and private application-aware QoS, airtime fairness, context aware prioritization, band steering, TCP throttling, dynamic admission control, WMM/802.11e, access network prioritization (e.g., DOCSIS service flow), WAG QoS, static admission control
Traffic separation and forwarding	SoftGRE or PMIP
Security	Secure SSID, IDS/IPS, open SSID with web authentication and MAC caching, peer-to-peer blocking
Session mobility	Full session retention in any roam between public, private, and 3GPP plus 802.11r and 802.11k
IPv4 or IPv6	Client-side IPv4 and IPv6, with IPv6 only infrastructure
RF optimization	Automatic channel selection on the AP, DBDC, SON
CPE provisioning and management	TR-069 only. Since TR-069 can handle more management tasks, we expect SNMP usage to decrease
Radio conformance	Full carrier Wi-Fi certification
Cellular interworking	Full seamless mobility
Gaps	Airtime fairness-based QoS, session mobility, hotspot location via augmented reality, carrier Wi-Fi certification, full session retention

Table 3:3 Service Implementation Level 3

3.2 Network Architecture and Interfaces

3.2.1 Introduction

Community Wi-Fi relies on a varied array of interconnected devices to provide the desired public access, with the expected levels of security and accountability, all while preserving the private user’s subscribed level of service. Operators pursuing Community Wi-Fi are interested in deploying architecture and interfaces that allow for network scalability (e.g., millions of APs and tens of millions of client devices), multi-vendor interoperability, and a consistent user experience. Additionally, there is the future goal of interworking and transparent session mobility between 3GPP and Wi-Fi networks.

3.2.2 Network Architecture Overview

In general, the Community Wi-Fi infrastructure model consists of split public/private wireless access, a tunnel between the public SSID and the CSP core, and the associated AAA related services. Radio resource management (RRM) is also highly desirable, especially in dense residential or retail deployments where significant co-channel and adjacent-channel interference is prevalent.

Managing the co-existence of the public and private networks is one of the primary technical challenges in Community Wi-Fi networks. There are two current technologies that can be used for wired traffic segregation and management – SoftGRE and PMIP. Both offer a secure tunnel back to the CSP core, and PMIP has the additional benefit of session mobility over a wider range of networks. The PMIP tunnel exists at Layer 3 between the mobile access gateway (MAG) (located in the CPE) and the local mobility anchor (LMA), allowing for secure and isolated traffic flow between the wireless station (STA) and the CSP core. In a mobile session, the STA will connect to a different MAG which is also tunneled back to the original LMA, thus preserving the existing IP settings.

There are a number of deployment models that require different network architecture, and each of these models can introduce unique challenges. These factors and associated challenges are described below:

		Public SSID	Private SSID
Scenarios for broadcasting SSID on Residential Wi-Fi Gateway	1	Standalone	
	2	Embedded	
	3	Standalone	Embedded
	4	Standalone	Standalone

Use a standalone residential Wi-Fi gateway to enable both public and private SSID. Both over the top (OTT) Community Wi-Fi network service providers and broadband network service providers can use this model

Use an embedded residential Wi-Fi gateway to enable both public and private SSID. This is a very common deployment model for Community Wi-Fi networks when the same operator provides both residential high speed Internet and Community Wi-Fi services

Use a separate standalone residential Wi-Fi gateway for public SSID and use an embedded residential Wi-Fi gateway for private SSID. This model may be more common in scenarios where the operators providing high speed Internet services and Community Wi-Fi network services are logically separate

Use a separate standalone residential Wi-Fi gateway for public SSID and a separate standalone residential Wi-Fi gateway for private SSID

Having both SSIDs on a single radio can help in dense environments with extensive co-channel and adjacent-channel interference, while discrete radios could offer the opportunity to have public and private split onto different bands, thus eliminating any airtime fairness issues.

Discrete public and private radios would also have the added benefit of allowing more user-configurable options for the private SSID (such as channel and TX power) since the RRM server must have full control over the public radio. Community Wi-Fi should also follow all architecture recommendations in section 5.1 of the WBA Carrier Wi-Fi Guideline document 9.

Additionally, the ‘Wi-Fi Requirements for Cable Modem Gateways’ document is available from CableLabs 10 , which details functional requirements for a cable operator managed Wi-Fi air interface that can be applied in residential, enterprise, and public cable modem gateways. CableLabs also maintains a Wi-Fi roaming specification, which includes requirements to help enable Wi-Fi roaming among partner networks from cable operators and non-cable operators.

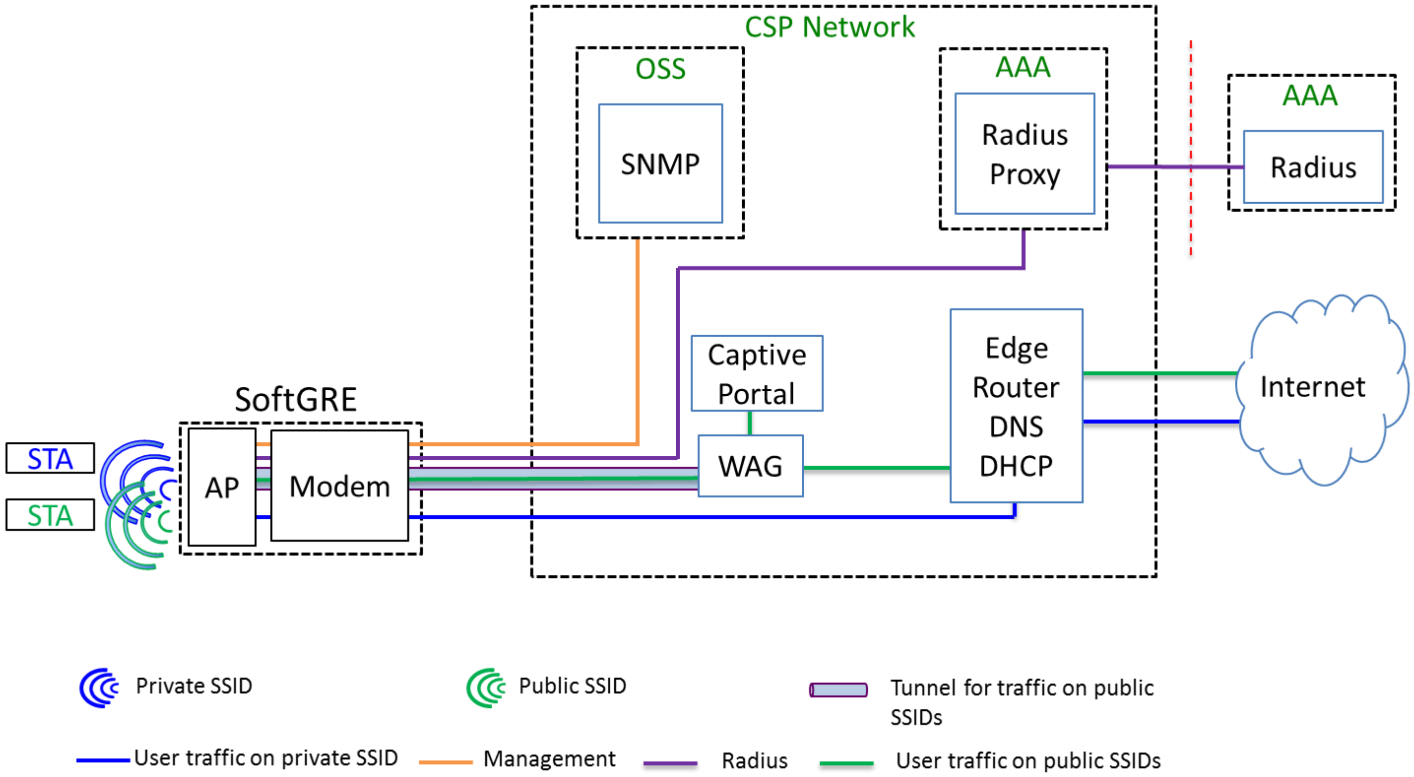


Figure 3:2 Community Wi-Fi Network Architecture (Architecture#1 – Generic)

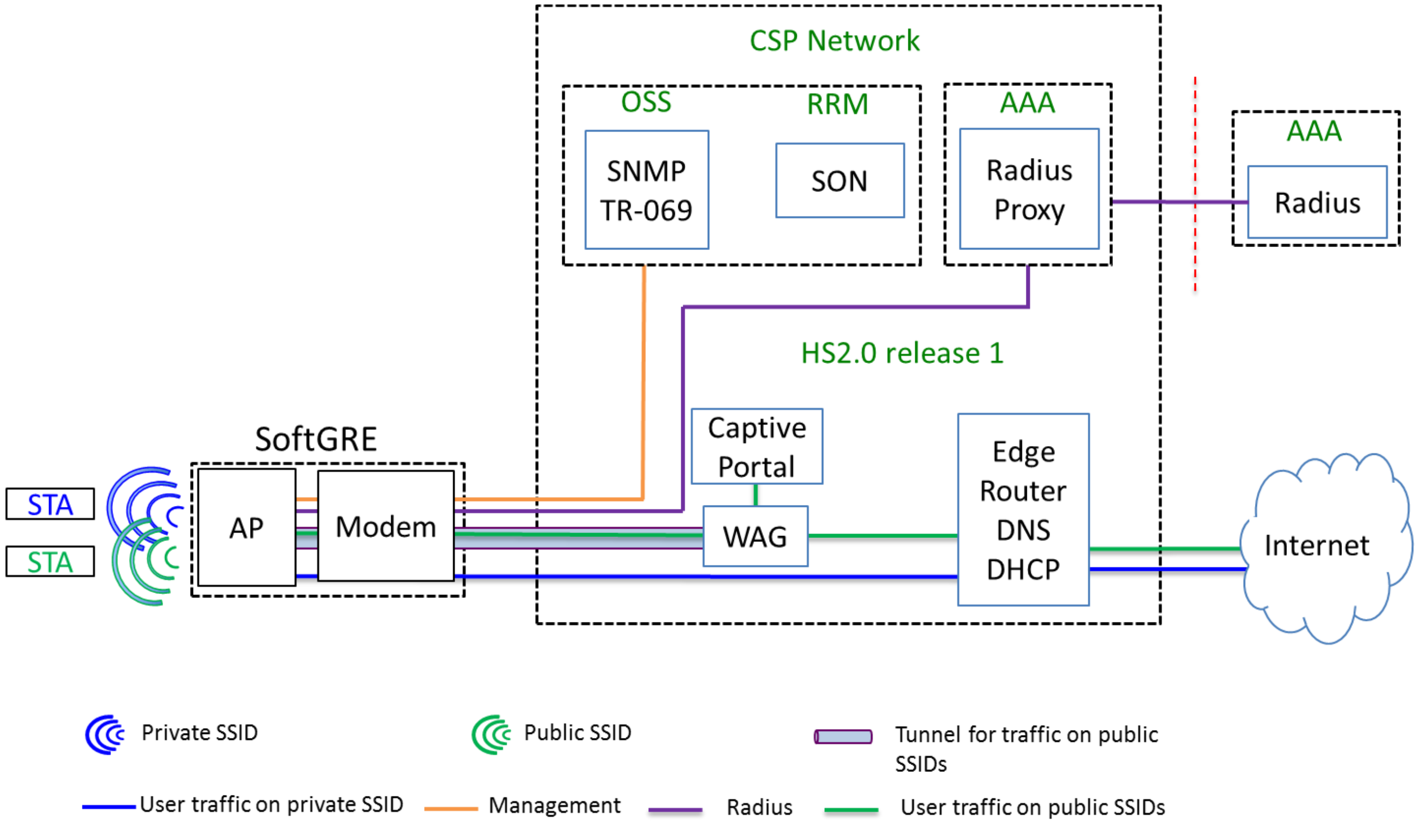


Figure 3:3 Community Wi-Fi Network Architecture (Architecture#2 – SoftGRE option)

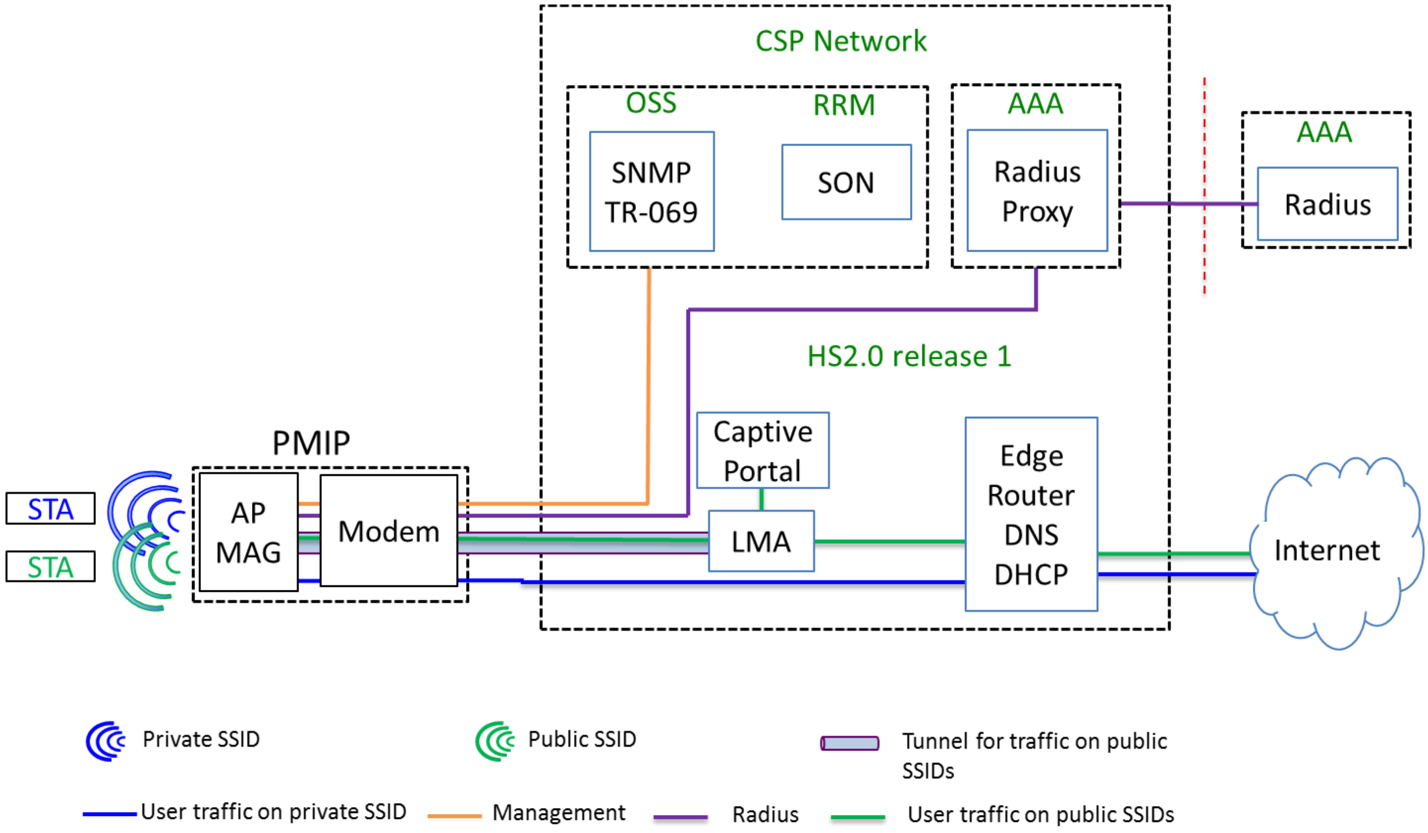


Figure 3:4 Community Wi-Fi Network Architecture (Architecture#3 – PMIP option)

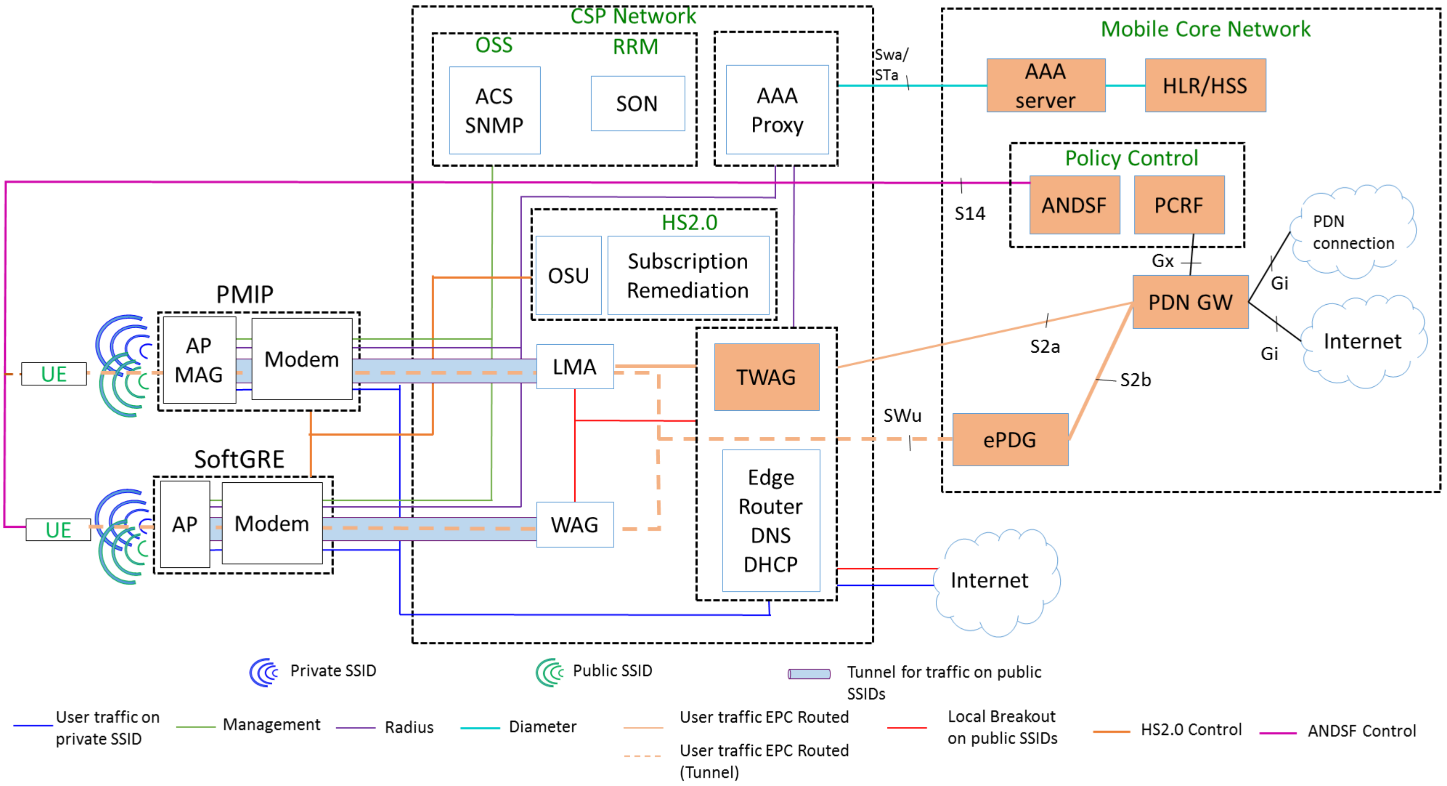


Figure 3:5 Community Wi-Fi Network Architecture Interworking with Mobile Network (Architecture #3)

3.2.3 IPv4 based non-tunneled architecture

Tunneled architectures allow for easy traffic separation and forwarding, but in many cases a tunnel may not be practical or achievable. IPv4 can be used for secure (for the users), non-tunneled, internet access with few compromises. Of primary concern is the ability to keep public and private traffic segregated.

This can be accomplished through the use of separate service flows. NAT and DHCP from the CPE can provide user devices with SSID-specific IP addresses, which will allow for the mapping of an IP address to a service flow. Not only will this keep the traffic logically separated, it can also make use of the existing service flow QoS mechanisms in order to always prioritize the private bandwidth above the public. The use of a captive portal on the public SSID allows for secure and authenticated public Internet access.

One issue with the use of IPv4 is that methods such as NAT are required to accommodate the scale needed, and this makes the tracking of individual devices more difficult. One possible solution is to tie the user to the authentication method. Accounting can still take place as these messages are generated by the CPE and sent to the CSP core.

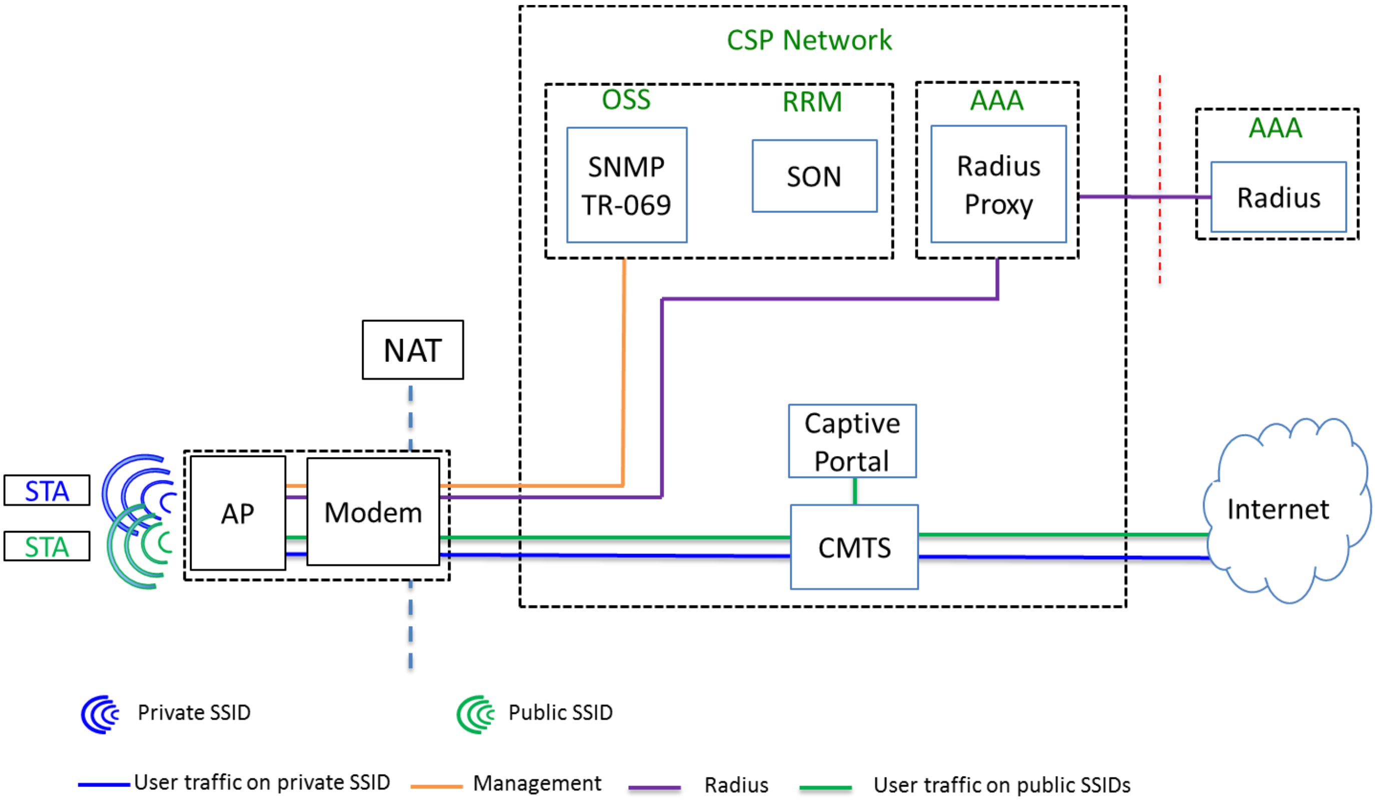


Figure 3:6 IPv4 Tuneless architecture

3.2.4 IPv6 based non-tunneled architecture

As stated in section 3.11, a fully IPv6 network enables alternative non-tunneled architectures. In a tunneled solution, user traffic goes on top of a SoftGRE tunnel up to the WAG. The user device and the WAG are connected under the same network segment. They are in the layer 2 of the TCP/IP network stack. Thus, the MAC broadcast domain is extended from the user device to the WAG. On the contrary, in an IPv6 non-tunneled solution, user traffic goes through the operator network directly to the Internet. There is no extra layer where the user traffic is encapsulated.

Regarding the accounting, in a non-tunneled architecture, accounting messages are generated by the access point by following RFC 2866, while the WAG is normally generating these messages in a tunneled solution, even though the AP is still capable of doing so.

Similarly to tunneled architectures, when the user is connected to the private interface the traffic is directly forwarded to the Internet. However, IPv6 also enables lawful interception and traffic accounting of users connected to the private network. This can be performed by the routing equipment in the operator core network, based on the IPv6 delegated prefix.

On the other hand, when different users are connected to the public network, the mechanism is slightly different. First, the traffic will be restricted to a walled garden area until the user gets Internet access. The user is, for instance, redirected to a captive portal for a web based authentication or will perform the first EAP authentication. During this transaction, the IPv6 public address will be logged together with the identity of the user.

Even if the user device has several IPv6 addresses, all of them will be logged in the backend in order to enable the lawful intercept. Furthermore, user accounting can be also performed separately from the traffic in the private interface without the need for tunnels. In both cases, the differentiation is made by considering logged and unlogged public IPv6 addresses. The ones related to the public interface have been previously logged at the backend, unlike in private interface case.

The following step in the authentication sequence involves the Radius server. Radius messages will be routed directly from the CPEs to the Radius server without the need for tunnels. Once the session is accepted, the user traffic will go through the operator network with a unique and identifiable public IPv6 address.

A reference architecture for IPv6 entangles the following network elements:

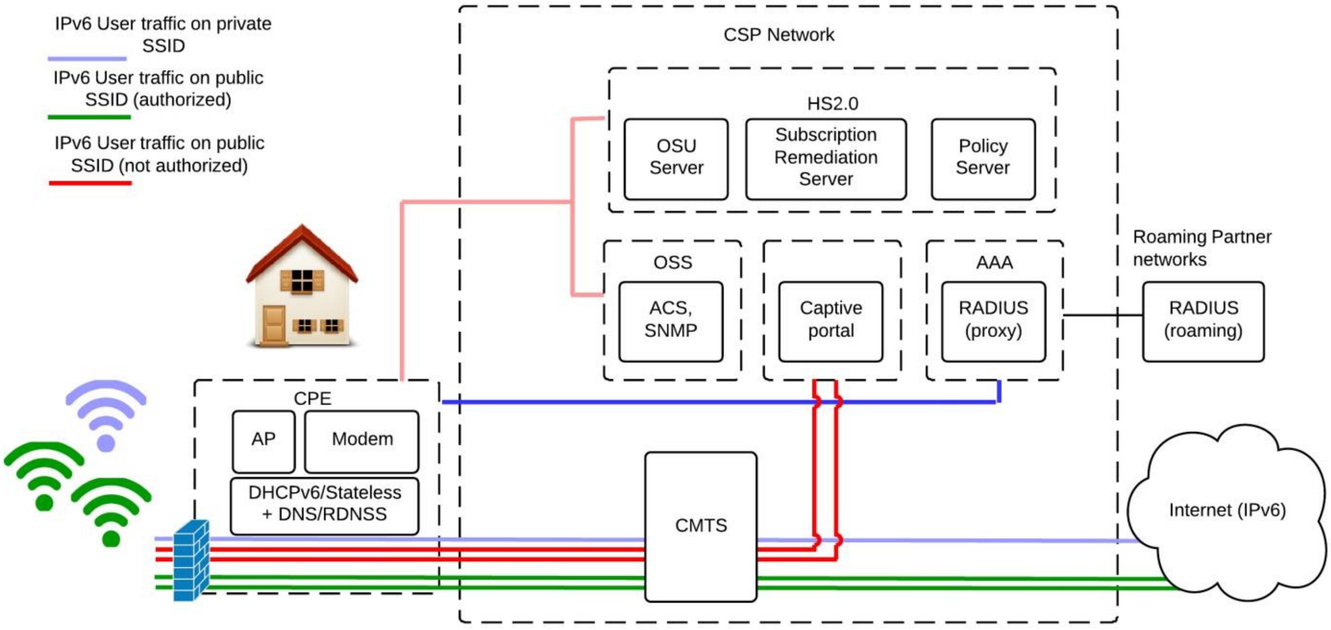

IPv6 User traffic on private SSID
IPv6 User traffic on public SSID (authorized)
IPv6 User traffic on public SSID (not authorized)
CSP Network
HS2.0
OSU Server
Subscription Remediation Server
Policy Server
OSS
ACS, SNMP
Captive portal
AAA
RADIUS (proxy)
Roaming Partner networks
RADIUS (roaming)
CPE
AP
Modem
DHCPv6/Stateless + DNS/RDNSS
CMTS
Internet (IPv6)

Figure 3:7 Community Wi-Fi Network Architecture - Non-tunneled IPv6

3.3 Network Scalability

In a wireless system, scalability issues can exist anywhere in different segmentations of the network such as air interface, backhaul, long haul, and core network, and in different layers from access stratum and network stratum, as well as in different planes of control and data. Scalability problems directly impact CAPEX/OPEX, QoS, SLA, revenue, and most importantly the customer experience, therefore it is important to identify and solve issues.

Community Wi-Fi systems have several unique scalability challenges:

- Since a large number of APs may exist in a specific geographical region, how to scale (at the right cost) the backhaul and core network functions to support the signaling as well as data volume can be a challenge
- Dense AP deployment can occur, such as when in a multiple dwelling unit (MDU) residence. There is not much control at the site over where and how the AP can be placed, therefore radio interference could be severe in some cases, creating scalability

issues for access. Additionally if Passpoint is available in such overlapping coverage areas, redundant signaling will occur from devices for ANQP, which can cause Passpoint signaling scalability issues

- A large number of IP addresses will be consumed by the APs in residential or business gateways, as well as by the accessing devices
- Potential bursty user behavior; for business areas, the office hours should be peak time while for residential areas, the evening should be peak time. Those schedules are expected to start/stop at a similar time creating a sharp burst/drop
- Mobility events for dense AP areas can be significant when subscribers move between APs or hand over between Wi-Fi and cellular at community hotspots, creating potential signaling challenges
- Network security can be a concern for the residence or business hosting Community Wi-Fi public SSID
- Community Wi-Fi SSIDs contend for same access network resources as private SSID, so traffic separation and traffic engineering becomes more important than typical best-effort Community Wi-Fi itself

To work with those challenges, below implementation considerations should be considered:

- Dimensioning of the network shall be warranted for designing of the network. This often involves complicated network modeling and traffic engineering exercises, tangled with various business and financial requirements. The planning will require the understanding of the Community Wi-Fi use cases, call flows, and architectural options

To support the increasing throughput capability from Wi-Fi APs and low latency requirement from services offered over Wi-Fi, the network design should prefer a distributed architecture:

- User data traffic can break out to the Internet at the very edge, and this needs to be balanced with the mobility domain that on the contrary requires data aggregation/anchor point for users
- Separation of the control plane and data plane should be considered, and if needed different QoS can be applied for the two sets of traffic. In addition, the control and data plane separation can enable scaling of the control and data independently to avoid unbalanced control and data volume from the same physical network components
- Traffic separation/bandwidth control of private and public SSID traffic shall be applied at the point of access, i.e., the AP. Private SSID traffic should be given a higher priority over the public SSID and it is also necessary that the public SSID gets capped for capacity/bandwidth so its overrun will not cause service degradation or even service disruption to the private SSID. The separation can bring security benefits as well, by which the public SSID users have neither visibility nor ways to inject into the private SSID traffic, assuming the air interface of the private SSID is always protected via 802.11i
- A RRM capability should be introduced as part of the architecture to minimize the radio interference and increase spectrum efficiency at the physical hotspot locations, ultimately increase the efficiency of the network and scalability

The network management system and servicing network components in the core network such as AAA, Wi-Fi controllers, and session routers which shall be scalable to accommodate the signaling (e.g, 802.11 associations, Network Management System (NMS) counter feeds, Radius, DHCP, Access Network Query Protocol (ANQP)) from large number of APs and bursty access requests from users during peak hours. The individual techniques to scale these systems vary greatly and are not in the scope of this document

- IPv6 should be considered throughout the Wi-Fi system in order to reduce the dependency on IPv4 addresses and avoid the complexity for managing scarce IPv4 addresses. The IPv6 Operator Guideline is available for reference at 2.

3.4 Traffic Separation and Forwarding

Traffic separation between private and public networks and traffic forwarding are crucial requirements to be considered when designing a Community Wi-Fi network. Main and common requirements regarding this topic are:

- Traffic separation between private and public networks and among users within the public network
- A user connected to their private SSID will not have any visibility or access to public SSID traffic
- A user connected to the public SSID will not have any visibility or access to private SSID traffic or any connected devices (e.g., network printer, disk, etc.)
- A user connected to the public SSID will not have visibility or access to the public SSIDs other users' traffic
- The system should allow for user identification and traffic differentiation from one user to another in the public network (e.g., for lawful interception purposes).

Traffic forwarding -

- Private and public traffic will be separated in the backhaul
- Downstream traffic will not be flooded on both public and private networks

In order to fulfill these requirements, there are several solutions. These solutions show different design considerations that have an impact on different aspects, such as IPv4 addresses consumption, CPE implementation complexity, user identification, traffic separation layer, etc.

For instance, the separation of the public and private network can be tackled through a packet filtering system i.e., a firewall. Different policy rules can be configured in the firewall. In this case, the rule would be to forbid the traffic forwarding between both sub-networks - private and public - based on the IP address range of each one.

Additionally, traffic separation among users within the public network can be performed in the link layer (Layer 2) or in the network layer (Layer 3) of the OSI protocol stack. In the first case (Layer 2), users cannot communicate directly among each other because Layer 2 frames, which show a link layer address different from the one the router has, will be dropped by the wireless chipset itself. The wireless chipset needs to be properly configured to enable that function (i.e., "isolation mode"). In the second case (Layer 3), a firewall policy can be configured to forbid traffic among users of the same sub-network except for the communication between the user and the router.

Finally, the requirements related to traffic forwarding can be fulfilled by using tunneling protocols (e.g., L2TP, SoftGRE, etc.). For example, the public traffic is forwarded directly over tunnels per new user connecting to the public network. The tunnel servers can also log the necessary legal interception data. On the other hand, the private network traffic can directly go through the ISP access network, without the need for tunneling the traffic for each connection in the private network, because subscribers are normally subject to a legal contract with the operator.

3.4.1 GRE overview

GRE per RFC2784 defines a protocol encapsulation of an arbitrary protocol over another arbitrary network layer. A GRE encapsulated packet has the form of Delivery header, GRE header and Payload Packet.

Layer 2 Wi-Fi roaming traffic is encapsulated between the Wi-Fi GW and WAG within a GRE tunnel. A single GRE tunnel is used per public SSID. Traffic separation of roaming traffic from the residential subscriber traffic is provided by the GRE encapsulation. The GRE tunnel can be assigned service profile-based QoS on the backhaul network, using IP classifiers, in order to establish a separate traffic priority for the public SSID. The controller provides a RADIUS client interface to the AAA and generates usage based accounting. Stateless GRE is proposed for less overhead on the AP and better scaling. Tunnel and subscriber context are auto-created such that the GRE control plane signaling is avoided. This helps the proposed architecture to scale and reduces the amount of GRE provisioning needed. The tunnel context only exists if one or more roaming Wi-Fi subscriber is admitted to the network, further helping the proposed architecture to scale.

See section 4.2 and 5.1.1 of the WBA Carrier Wi-Fi Guidelines document for more details on tunneling.

3.4.2 Dual Stack PMIPv6 overview

Although PMIP was developed primarily for mobility, Mobile Internet Protocol (MIP)also provides traffic separation, security and usage accounting reports per roamer for massive scale deployments. Therefore, PMIPv6 is considered here as both a mobile architecture and as a general approach to traffic forwarding. The support for mobility is beneficial for Wi-Fi subscribers.

Mobile IP strives to provide transparent routing of packets for mobile nodes. Applications are shielded from changes in local IP addresses through the use of mobile tunnels. MIP is widely present in 3GPP-EPC, 3GPP2 and WiMAX cellular specifications. Furthermore, MIP infrastructure can also provide authentication and per user traffic accounting. MIP has a number of variants, however, dual stack PMIPv6 per RFC5844 is considered for the traffic forwarding. Dual stack PMIPv6 can support IPv4 and IPv6 clients with an IPv6 infrastructure. Full mobility is supported without the need to place mobility requirements on the client.

PMIPv6 is implemented by two network functions, the MAG and the LMA. Mobility tunnels are established between these functions. The MAG tracks the mobile node, executes mobility signaling on behalf of the mobile node and provides usage based accounting. The LMA acts as the anchor for the tunnels. The LMA binds the Change of Address (CoA) address with the mobile’s Home IP address, tunnels packets toward mobile node CoA, and provides usage based accounting. PMIPv6 operates at Layer 3 and also relies on GRE.

The access network first authenticates and admits the device. Upon network admittance, the MAG locates a remote network LMA based on the device ID (MAC address or Network Access Identifier (NAI)), or assigns a local LMA. The MAG can then register the device with the LMA and create a mobile tunnel to the LMA. The MAG sends a router advertisement to the device and appears as the device’s default gateway. Layer 3 service establishment is complete.

3.5 Traffic Management and Prioritization

Community Wi-Fi networks make use of residential Wi-Fi gateways to offer services to guest and home subscribers. The objective is to offer guest subscriber access to Wi-Fi network resources that are not currently being used by the subscriber at home.

The challenge of traffic management and prioritization on public and private SSID is fundamental to offering Community Wi-Fi services. This becomes even more challenging to operators that use a single gateway and Wi-Fi radio to enable both public and private SSID.

Furthermore, this resource allocation problem becomes more prevalent as access network data rates continue to grow. The deployment of high data rate DOCSIS 3.0, 3.1, or Fiber To The Home (FTTH) services in the near future will challenge even unimpaired Wi-Fi networks to support the aggregate throughput offered by the access network. Specifically, as access network data rates increase from tens of megabits per second (Mbps) to hundreds of Mbps, the likelihood that the Wi-Fi channel is the bottleneck increases dramatically. Single radio deployments compound this problem by dividing the channel resources between two or more networks. Therefore, it is imperative that deployed devices support traffic management and prioritization methods capable of providing effective resource management even in the scenario where the aggregate Wi-Fi channel throughput has dropped below the access network provisioned data rates. In this scenario, access network traffic management methods e.g., rate limited DOCSIS service flows, no longer have the ability to control resources on the Wi-Fi channel.

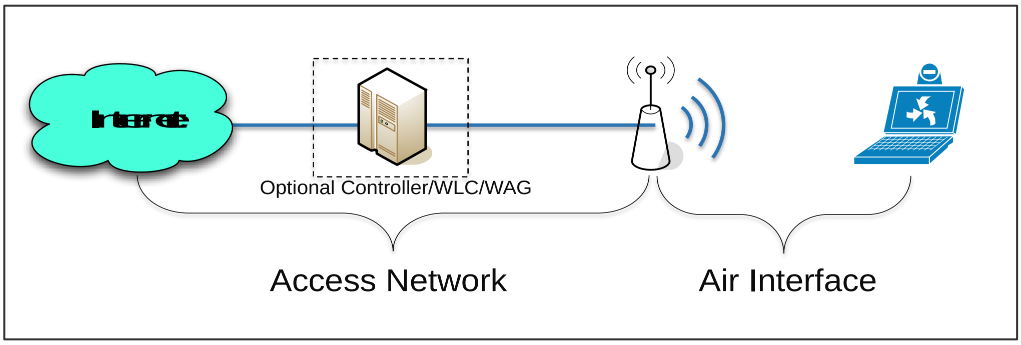


Figure 3:8 QoS Location Options

As show in Figure 3:8 above, there are two network segments that can enforce QoS mechanisms; the access network and the air interface. This section first discusses the traffic management and prioritization options for the access network. Next, this section covers the fundamental mechanisms underlying Wi-Fi resource management. This section also identifies technologies gaps in this area and reviews some possible solutions.

See section 5.1.3 and 5.1.6 of the WBA Carrier Wi-Fi Guideline document for more details on network quality.

3.5.1 Access Network QoS

The one primary traffic management and prioritization method available to Community Wi-Fi operators is the DOCSIS access network. When the air interface aggregate throughput is greater than the access network provisioned data rates, the resource allocation on the access network and the air interface can be controlled via DOCSIS service flows.

The first step is to separate the traffic from each SSID onto a separate service flow. DOCSIS service flows allow traffic filtering via a set of well-known traffic classifiers including IP addresses, IP subnets, TCP/UDP port numbers, 802.1Q (VLAN) tags, and 802.1ah tags. DOCSIS service flows allow filtering on source values, destination values, or both for all of the applicable traffic classifier parameters. One last option available to cable modems with embedded Wi-Fi interfaces is to use the cable modem interface mask (CMIM) assigned to the Wi-Fi radio or possibly to each SSID for traffic classification. For more information on CMIMs refer to the eDOCSIS specification 3.

Once the traffic from each SSID is classified onto separate service flows, DOCSIS has a rich set of QoS tools available to network operators. The first tool is a simple rate limiting function. By configuring parameters such as Peak Rate, Max Sustained Rate, and Max Traffic Burst on each service flow, aggregate throughput to each SSID can be controlled with precision.

In addition to rate control, DOCSIS offers Traffic Priority levels that are designed to indicate to the traffic scheduler relative priority between Best Effort service flows. Using Traffic Priority, in times of resource congestion in the access network, the higher priority service flow will get bandwidth before the lower priority flow. Finally, if absolute QoS is needed, for example if the service offered is a constant bit rate (CBR) service, DOCSIS offers the unsolicited grant service (UGS) service flow type with offers fixed rate guaranteed bandwidth across the access network. For more on these topics consult the MAC and Upper Layer Protocol Interface Specification for DOCSIS 3.0 4.

Using the above referenced tools, operators can configure access network QoS, at the MAC layer, to suit their needs. As mentioned above, this method is effective provided the air interface throughput is greater than the access network throughput. If the air interface throughput ever drops below the DOCSIS configured rate limits, the access network can no longer control the resource allocations and other methods must be used.

3.5.2 Wireless Access Gateway QoS

A second option for traffic management and prioritization available to Community Wi-Fi operators is to use a WAG or similar network side controller. In such a scenario, traffic is controlled at the IP layer or above. Using TCP session tracking or other deep packet inspection (DPI) techniques, the controller can influence the application layer resource usage. An example of this would be solutions that can delay or drop TCP acknowledgement (ACK) frames to reduce the throughput of a TCP connection, and thus the resource usage of that client. This method, while indirect, allows for a network side solution where a single device can manage resources across a wider array of deployed devices. Numerous variations on this solution may exist.

Similar to traffic management and prioritization on the access network, this method is effective provided the air interface throughput is greater than the access network throughput. In some scenarios, the indirect resource usage control will not be able to prevent clients from using resources at the lower layers. For example dropping TCP ACK frames on connections with long round trip times can trigger retransmissions prior to a rate reduction. These short term increases in air resource usage may negatively impact the private network user experience. In addition, this method may not have access to traffic from the private SSID. Due to this constraint the ability to fully manage the resources is limited. Ultimately, the ideal traffic management and prioritization solution for the Community Wi-Fi use case would operate on the air interface.

3.5.3 Wi-Fi Resource Allocation Fundamentals

In the single radio scenario under standard distributed coordination function (DCF) channel access rules, the allocation of the shared wireless channel resource, or airtime, between the private network and the public network is primarily a function of two variables: the number of active STAs on each network; and the physical layer rate used by each active STA.

The DCF was designed to provide equi-probable channel access to all STAs in the network. Thus, assuming all STAs have the same physical layer rate (or modulation and coding scheme (MCS) for .11n networks), all STAs get an equal allocation of the airtime. In a multi-network single radio environment, this means both public and private STAs have equal airtime. If the public network has more active users than the private network, the public network will use more of the shared airtime than the private network. In heavily skewed cases i.e., 4-1 or 5-1 public to private active users, the private network may no longer be able reach the access network provisioned data rates due to limited airtime.

The second variable governing airtime allocation is the physical layer rate used by each STA to send data over the wireless link. The physical layer rate used by an STA determines the amount of time the STA will hold the shared channel once it has gained access. For example, an STA sending a maximum size data frame (ignoring DCF Interframe Space (DIFS),Short Interframe Space (SIFS), ACKs for now) takes 9.8 milliseconds of airtime at a physical layer rate of 6.5 Mbps (MCS 0) versus just 0.55 ms at 130 Mbps (MCS 15). This means an STA at the edge of the coverage area, which can only achieve an MCS 0 link, will use approximately 20 times the airtime of a STA very close to the AP! This ignores other static overheads that slightly skew the numbers, but their effects are static and do not significantly affect the end results.

Taken together, these two variables can compound to result in the public network using the vast majority of the shared airtime resource. If there are more public users than private active on the network, and they are farther from the AP, the public network will absolutely dominate the airtime usage. This behavior, combined with increasing access network data rates, makes it very likely the private network will be unable to achieve the access network provisioned data rates.

Testing was performed (by Joey Padden of CableLabs) with a single radio device supporting two networks with the setup shown in Figure 3:9 below.

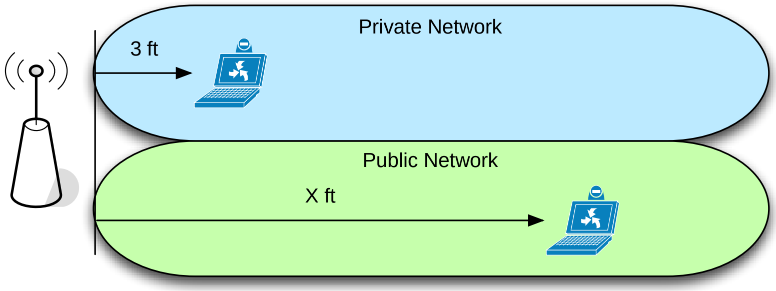


Figure 3:9 Unfair Airtime Testing Topology

To test the effect on user level throughput, two STAs were joined to a single AP supporting two networks. Upstream throughput tests were performed as the STA on the public network distance to the AP was varied.

Figure 3:10 below illustrates the results of this test. The ‘private’ network in blue was provisioned with an upstream data rate on the access network of 30 Mbps. The ‘public’ network in black was provisioned with an upstream data rate on the access network of 10 Mbps. The solid lines show the throughput of a single STA active on each network. When

both STAs are three feet from the AP, both STAs achieve a link using MCS 15 (130Mbps) and both networks are able to achieve the provisioned upstream throughput on the access network. However, when the STA on the public network is moved to 50 feet from the access point (dotted lines), the link rate for the public STA drops to MCS 4 (39Mbps) and the airtime used by the public STA has a negative impact on the private STA throughput.

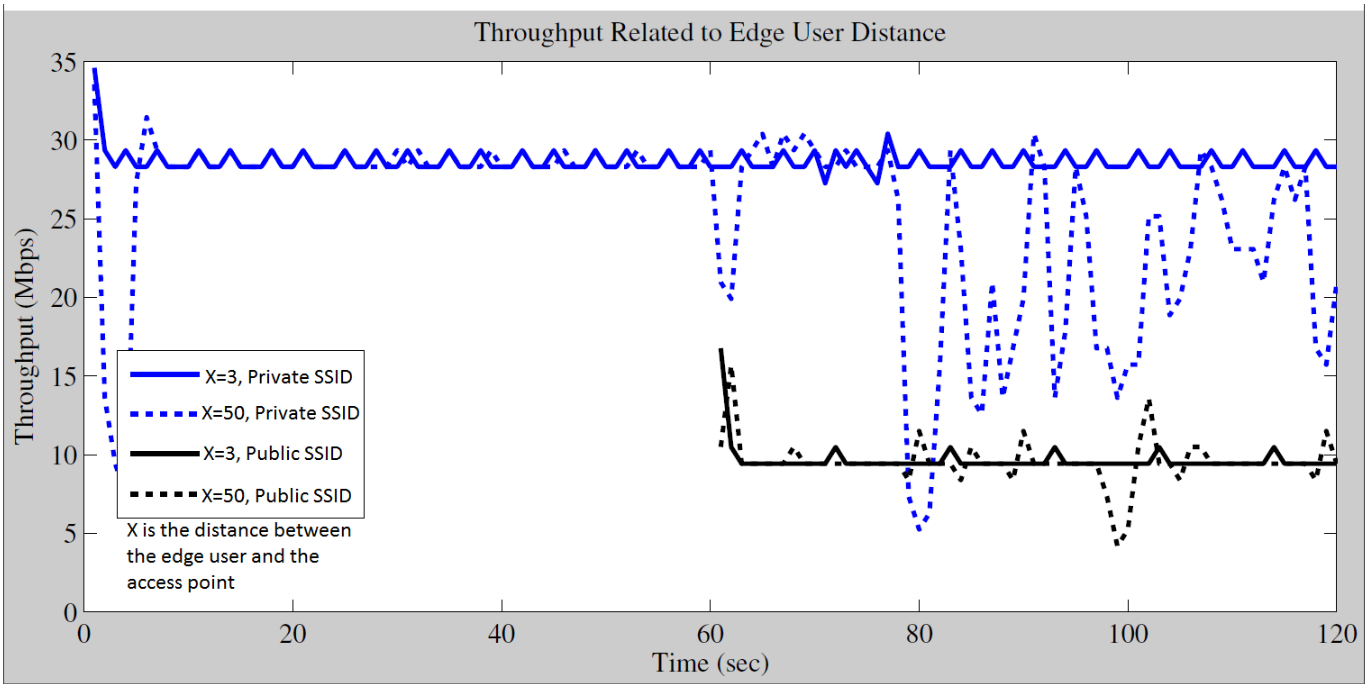


Figure 3:10 Unfair Airtime Throughput Test Results

3.5.4 Wi-Fi QoS Options

In the downstream direction, access points that implement an airtime fairness algorithm can effectively manage this problem. Private network packets can be given priority access to the channel because the AP is in complete control of which downstream packets from internal queues make it to the air interface first. Multiple vendors implement such algorithms.

However, in the upstream direction the CSMA/CA algorithm controls channel access. Currently, as stated above, the DCF provides equi-probable access to all STAs. The only tool currently available for QoS on the air interface, WMM/802.11e, is application-centric, not network or user-centric. The following sections will discuss the design and functional gaps of WMM.

3.5.4.1 Wi-Fi Multimedia Basics

Wi-Fi Multimedia (WMM) allows for the creation of multiple access categories (ACs) that are generally mapped to specific application types: Voice, Video, Best Effort, and Background. Each AC has a specific CSMA/CA parameter set that governs the channel access success probability. Figure 3:11 below shows the default parameter set defined in the WMM specifications.

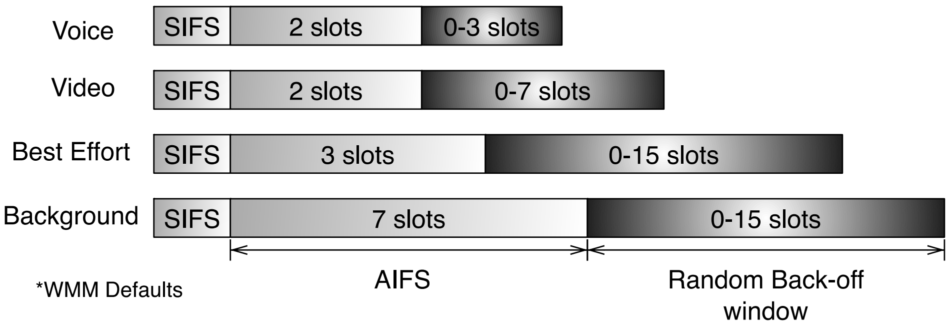


Figure 3:11 WMM Default QoS Parameter Set

The specification allows for the Arbitration Interframe Space (AIFS)and Contention Window Minimum (CWmin) (starting size of the random back window) to be configured on a per AC basis, thus creating differentiation between the ACs. Traffic is mapped to ACs based on the Internet Engineering Task Force (IETF) DiffServ field in the IP packet header. Using this method, applications can mark their traffic for four levels of priority over the Wi-Fi interface.

3.5.4.2 Wi-Fi Multimedia Shortcomings for Community Wi-Fi

The design of WMM includes two implicit assumptions: high priority traffic needs relatively low bandwidth; and applications need QoS, not users or STAs. Both of these assumptions are not applicable to the Community Wi-Fi use case.

In Community Wi-Fi, all applications on a given STA, or set of STAs, need priority access. Using WMM to accomplish this would require mapping all traffic from those STAs to a single high priority AC e.g., Voice AC. In this configuration, it is easy for high priority high bandwidth STAs to completely starve the lower priority STAs from getting any airtime. The WMM specification created two methods to ameliorate the starvation problem, Transmit Opportunity (TXOP) and WMM-Admission Control (WMM-AC).

TXOP is an AC parameter that defines the maximum length burst an STA can send in that AC. This effectively controls the airtime of an STA once it has gained access to the channel. However, as the STA count in a high priority AC grows, even setting the TXOP to a reasonable level does not prevent that AC from dominating the airtime. In the Community Wi-Fi use case, if the private network STAs were assigned statically to the voice or video AC, even with TXOP set to a reasonable level, there would be a high probability that the public network would have severely limited bandwidth anytime an STA was active on the private network.

The second mechanism created for airtime resource control is WMM-AC. In this function, an STA wishing to start a high priority flow sends a request to the AP for permission to use the AC of interest. If the AP determines that there are sufficient resources to fulfill the request, admission is granted and the STA can begin using that AC. The request format includes the nominal frame size, the mean data rate, and other parameters that are tailored to support a single flow for a specific application e.g., voice traffic has 218 byte packets and a constant bit rate of 64 kbps. However, in the Community Wi-Fi use case, the user of an STA may be web surfing, transferring files, or using a variety of connected applications simultaneously. Thus, nominal packet size and data rate may change from moment to moment making WMM-AC ill-suited to managing access to the AC.

Considering the aforementioned limitations on checks and balances in WMM, static assignment of private network STAs to a high priority AC will not resolve the upstream airtime fairness issue.

3.5.4.3 Potential Solution

A number of researchers in the academic community have identified problems with the Wi-Fi MAC layer that are related to the problem described above in 5, 6, 7, and many other studies. One common approach in the solutions proposed, such as the Idle Sense method described by Heusse et al. in 8, is to redefine the MAC layer of the Wi-Fi STA and AP. This approach poses huge logistical problems for deployment. The many millions of Wi-Fi devices currently deployed would all need, at minimum, software updates to support the new channel access method. In addition, such solutions need to work or offer some benefit in the case where the network is a heterogeneous mix of STAs supporting the new MAC and STAs supporting the DCF MAC. This particular restriction allows for acceptable performance during a phased roll out while all clients slowly transition to the new MAC. However, this restriction is hard to accommodate and many proposed algorithms, such as the Idle Sense algorithm in 8, do not work as designed when operating in heterogeneous networks.

One possible solution that could be used to prevent uncontrolled resource imbalance would be dynamic adjustment of the WMM parameter CWmin within the parameter sets advertised in the beacon frames for each SSID. The three key parameters a control algorithm would need to consider include the desired aggregate throughput of the private network, the number of active STAs in each network, and the MCS (or legacy Physical Layer (PHY)rate) used by each STA in the network. Using these parameters, a control algorithm in the AP could then intelligently manage the channel access probability ratio via adjusting CWmin for the public network relative to the private network, such that the airtime resource usage achieves the desired ratio. Variations of this solution have been proposed and tested by vendors as well as in academia with good success.

The highlight of this approach is that it is fully implemented in the AP software, using information the AP has readily available and requires no change to STAs. The majority of STAs made in the last five to seven years have implemented support for WMM. Furthermore, if the public network is always de-prioritized with respect to the private network, this method has no negative impact on adjacent networks.

The main limitations to this approach are increased channel access delay for the public network and decreased aggregate throughput for networks with high STA counts. Specifically, as the WMM parameter CWmin is increased, channel access delay goes up for STAs using that parameter set. Therefore, in extreme cases where the public network is highly de-prioritized, the performance of the public network may degrade to unusable levels. Also, there is a well-documented decrease in overall network performance as the number of STAs increases to large numbers. However, this behavior is no worse than in standard DCF controlled Wi-Fi networks.

3.5.5 Public SSID Admission Control

Public SSID oversubscription can result in a negative user experience not only for the public subscribers, but for the private subscriber as well, if the two SSIDs are on the same radio. Having a large number of public users, most likely at the edge of the cell, will severely impact the airtime available for the private user. Refer back to section 3.5.3 for a detailed description of the airtime fairness problem and how it impacts QoS on the private SSID.

Community Wi-Fi networks should support a mechanism for limiting the number of public subscribers attached to a single access point. See section 5.1.4 of the WBA Carrier Wi-Fi guidelines document for related requirements.

3.6 Network Selection and Operator Policy

A Community Wi-Fi operator should be able to implement and deploy a policy that makes the end user device preferentially connect to their private SSID when at home, even when the public SSID is available. Additionally, it is desirable for the device to be able to automatically connect to the public SSID when the user is roaming. See section 5.6.1 of the WBA Carrier Wi-Fi Guidelines document for more details on network selection.

3.6.1 Client Centric Solutions

The implementation of these policies usually relies on a client installed on the device. The client may be a downloadable application, or a native functionality integrated in the firmware (e.g., HS2.0). In the very basic approach, these applications can prioritize SSID’s. In the case of Community Wi-Fi, the private SSID must be prioritized over the public for those scenarios where both are available.

The flexibility for policy implementation depends on the device operating system. There are operating systems that allow a wide bundle of options to control network selection at user level. In these cases, operators may develop their own applications to apply their policies. In other cases, collaboration between the operating system provider and/or device manufacturer may be required to implement a customized policy.

3.6.1.1 Hotspot 2.0

WFA Passpoint supports network discovery and selection with operator policy management capabilities. However, the specification does not currently cover the private over public network prioritization case directly (there are some mechanisms for prioritizing multiple networks). Both APs (private and public) would have to be Passpoint-enabled in order to be managed by the policy server. The private network is not meant to be an operator-controlled network, so handling the private network as Passpoint enabled is not practical. The Passpoint specification states that a prioritized list of preferred networks should be capable of being presented to the user for manual selection of the network with which to connect. This may open a door for having Passpoint implementations in devices that allow users to set up prioritization beyond only Passpoint networks, though, of course, out of network side control. These are gaps future Passpoint releases might support to fully cover Community Wi-Fi network selection and operator policy use cases.

3.6.1.2 3GPP ANDSF

3GPP ANDSF is a cellular technology standard that allows an operator to provide a list of rules for selection of preferred access networks (including Wi-Fi) and for traffic steering among accesses (3GPP and Wi-Fi), with the granularity of a single IP flow. ANDSF covers the prioritization between the network access, i.e., 3GPP and the WLAN SSIDs, both when the user is in their home network or in a roaming scenario. The ANDSF allows the definition of different policy for different location, where the location may be identified by specific radio parameters such as 3GPP cell ID, 3GPP location area, etc. The ANDSF enables easy selection and traffic steering between the mobile network and the Community Wi-Fi network (public SSID). These capabilities enable SSID prioritization, but the provisioning of such a specific policy for each user demands deploying complex provisioning procedures. 3GPP specifications indicates that user preference in selection always takes precedence on automatic selection based on ANDSF, but how such capability is provided to the user is left to implementation decision on the device; for example the operating system implementation and connection manager. However, ANDSF is a function specified as part of a 3GPP compliant mobile core network (e.g., evolved packet core (EPC) network) which in 3GPP Release 12, was somewhat aligned with HS2.0 policies. This architecture also requires support for ANDSF related functionality in the client devices. Non-3GPP operators may not be able to use this architecture.

3.6.2 Infrastructure Centric Solutions

An infrastructure driven network policy can also be used to influence a client in joining one network over the other.

3.6.2.1 MAC Address Filtering

A Community Wi-Fi AP can dynamically create a MAC address-based white/black filter list. As part of this, AP would remember the MAC address of all devices that were successful in joining the network using the private SSID. Based on this MAC filter list, the Community Wi-Fi AP should not allow a client device to join the network using the public SSID if the client device was previously successful in joining the network using the private SSID. Basic operation:

- An AP creates a MAC address filter list of all devices that were successful in connecting to the AP using the private SSID
- When a client device tries to connect using the public SSID, the AP checks this filter list
- If the device MAC address isn’t in the filter list, the AP will allow the device to connect
- If the device MAC address is in the list, the AP blocks the device from connecting using the public SSID
- The filter list is erased every time the AP is rebooted

This solution can work but there are unknowns such as:

- What will the client device do? Will it try to join the private SSID? How long does it wait before joining the private SSID?
- How many times will it try to connect to the public SSID?
- Will the device delay or no longer try the public SSID outside the home?
- What impact does this have on customer experience?

3.6.2.2 Interworking IE

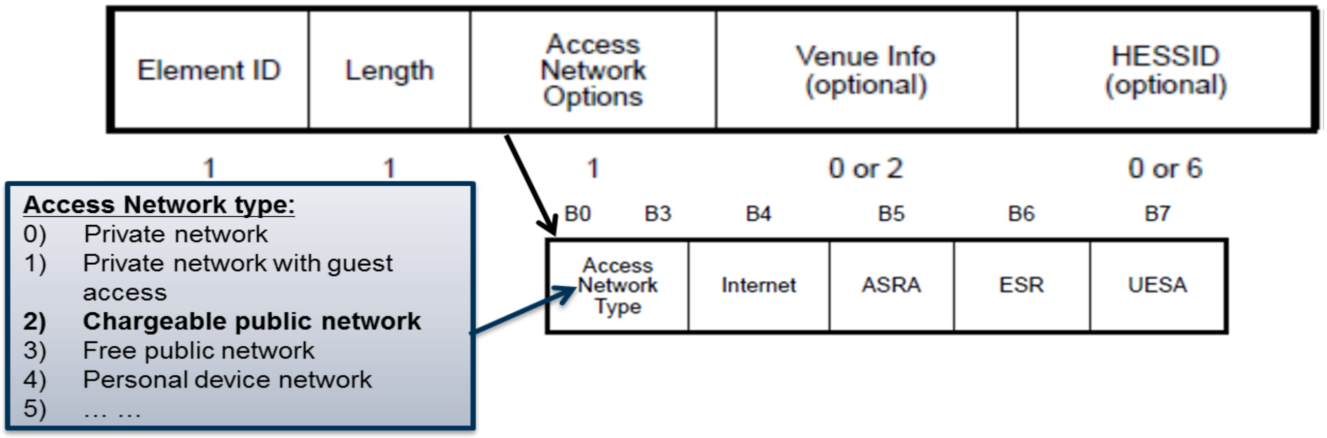


Figure 3:12 Interworking IE illustration

The interworking information element (IE) can be used to steer a client to an appropriate WLAN, but this is a limited use case and requires support on both the client and infrastructure. Operators may broadcast an interworking IE with Access Network Type = 2, which signifies a chargeable public network. The client will treat this Access Network Type as a hotspot, which will give it a lower priority than a known private network in the same location. The AP can broadcast this IE on a per-SSID basis, enabling clients to make network selection decisions based on the access network type. Refer to section 8.4.2.94 of the IEEE 802.11-2012 spec for further information.

3.6.2.3 Wi-Fi Beacon and Probe

One suggested proposal is that a Community Wi-Fi AP could be configured with beacon rates in such a way that the private SSID is more likely to be selected over the public SSID.

This solution is unlikely to be successful. A mobile device builds a roaming table of BSSIDs (????DEFINE????), and beacon rate is not recorded nor factored into the decision algorithm. The device will do a full scan of all configured channels and SSIDs, so regardless of how long the beacon interval is, all matching and active BSSIDs will become part of the table. This scan is also usually on the order of a full second or two, meaning you'd have to have the public beacon rate significantly above that for it to even potentially matter (tens of seconds). At that point there is the real risk that a public user would not see the public SSID and there is no possibility of roaming seamlessly between public SSIDs. Considering that multicast and broadcast traffic is transmitted at a multiple of the beacon rate (the DTIM), beacon restriction would also effectively limit traffic to unicast only.

3.6.3 Wi-Fi Core Network Based Solutions

The network (e.g., AAA) recognizes home users' devices and prevents them from connecting to the public SSID on their residential Wi-Fi gateway. In this solution, the subscriber request to join is rejected during the authentication phase. In the case of a MAC Address Filtering solution, the subscriber request to join the network is rejected at the Wi-Fi association phase.

3.7 CPE Provisioning and Management

As described across this document, a Community Wi-Fi strongly relies on specific functionalities implemented in CPE's or access points. The operator of the Community Wi-Fi needs to have the tools to remotely provision, manage and monitor these functionalities.

Provisioning and management solutions available in the market are mainly based on information exchange between the CPE, acting as a client, and an operation and management platform, acting as the server. These solutions also allow performing a bundle of management actions remotely. According to this, a first classification can be made:

- **Configuration parameters** are those that can be set, read, changed, from the operation and management platform into the CPE firmware for configuration provisioning purposes.
- **Monitoring parameters** are those that the CPE firmware provides to the operation and management platform for monitoring purposes.
- **Management actions** are those that can be executed remotely by the operation and management platform, for instance, reboot, factory reset, firmware download and upgrade, etc.

While there is not a significant difference between Community Wi-Fi and other Wi-Fi networks in the case of management actions (further than public SSID activation/deactivation), a Community Wi-Fi requires additional specific configuration and monitoring parameters:

Examples of Configuration parameters -

- Maximum number of associated users to public and private signals
- Maximum number of logged in users to public and private signals
- Public SSID management (e.g., name, activation), EAP SSID, etc.
- Whitelisting in the public network

Examples of Monitoring parameters -

- Service Status (e.g., CPE accessible from management platform and public signal up and running)
- Number of associated users
- Number of authenticated users
- Rogue Wi-Fi APs
- Downlink / Uplink throughput
- Link status

In addition to the ones listed above, there is a group of parameters regarding Radius Location (RFC5580[1]) and Radius servers that are relevant for Community Wi-Fi operation and are part of CPE configuration, though they are also related to other type of Wi-Fi networks. These are, for instance, Operator-Name, Location-Information, Location-Data, Basic-Location-Policy-Rules, Location-Capable, RADIUSAuthServer (host name, port, secret, etc.), RADIUSAcctServer, etc.

There is a relatively large range of existing solutions that can be used to provide remote CPE management and provisioning capabilities for a Community Wi-Fi operator. Although there are proprietary solutions, the following table covers the two most popular standard ones:

Solution	Description

[1] https://www.ietf.org/rfc/rfc5580.txt

TR-069[2]	TR-069 defines an application layer protocol for remote management of CPEs. The protocol is defined by a non-profit organization, the Broadband Forum[3], also known as DSL forum. TR-069 enables the bidirectional configuration and setting of parameters. However, TR-069 shows some drawbacks when used as a monitoring protocol, because of the overhead of the protocol. TR-069 uses HTTPs as the security layer.
SNMP[4]	SNMP enables to set and read parameters remotely. The protocol is defined by the IETF. SNMP defines a complex parameter tree architecture, which makes it less appropriate than TR-069. It is also less secure than TR-069 since the security relays on UDP and the Community Name. SNMP is normally used in LAN environments or when devices are connected through VPNs.

Table 3:4 Existing Remote CPE Management and Provisioning Solutions for Community Wi-Fi Operators

Radius might also be considered a monitoring protocol, since several statistics can be derived from the logs collected during the authorization, authentication and accounting stages. However, it falls out of scope of this section because Radius does not show management and provisioning capabilities.

The election among these solutions will depend on different factors. Generally, the operator will try to integrate Community Wi-Fi-specific management and provisioning capabilities into their current CPE management system to avoid having to deal with a plurality of systems. Among the solutions described above, TR-069 is the most common one. It is a powerful enough solution and a good candidate to cope with CPE provisioning and management requirements for Community Wi-Fi.

TR-069 defines two main entities: the client (e.g., in the CPE) and the auto configuration server (ACS). Between the ACS and the client, sets of parameters or data models are exchanged/synchronized. In the case of a Community Wi-Fi, a new data model needs to be defined for specific parameters. The Broadband Forum last data model template is defined in ‘TR-106 Amendment’ 5 document. Taking into account the format of the parameters described in the template, Community Wi-Fi vendor specific parameters can be defined. The Broadband Forum also provides some reference guides depending on the kind of device to manage (e.g., Internet gateway, femto-access point, a storage device or a DSL-Home gateway). These guides cover some relevant parameters that should be included in the TR-069 data model. The operator can consider these guides as a starting point for the definition of the Community Wi-Fi data model.

Annex A of this document provides a list of management object descriptions to consider for support on Wi-Fi GW for Community Wi-Fi.

See section 5.1.2 of the WBA Carrier Wi-Fi Guideline document for more details on network management.

3.8 RF Optimization

Given Wi-Fi uses unlicensed spectrum, interference is a significant factor. Although the interference in 5GHz band is not as bad as it is in 2.4GHz band today, it is expected to get worse as more and more 802.11ac devices are deployed. There are many sources of interference, including microwave ovens, cordless phones, Bluetooth, and other nearby Wi-Fi systems.

Sources of interference are many and dynamic in nature. To manage interference, operators should consider the following additional tools:

- Support for ACS at boot up and during operation

[2] http://www.broadband-forum.org/cwmp.php
[3] http://www.broadband-forum.org/
[4] SNMPv3 is defined by IETF RFC’s 3410, 3411, 3412, 3413, 3414, 3415, 3416, 3417 & 3418.
[5] http://www.broadband-forum.org/technical/download/TR-106_Amendment-7.pdf

- Support for DBDC with support for multiband steering
- Support for RRM and SON
- Site surveying and recording the interference environment at installation time to help with troubleshooting the post-installation environmental changes that degrade performance.

3.8.1 Automatic Channel Selection

APs supporting ACS, constantly sense the presence and amount of interference around them. APs then use this information to select and use a channel with better operating conditions.

Since the channel conditions can change with time, it is recommended that the AP should be capable of performing automatic channel selection at boot up and during run time. The channel selection must be done carefully with consideration to a number of factors such as the transmit power for each band and DFS requirements.

3.8.2 Dual Band Dual Concurrent and Multiband Steering

Wi-Fi APs could be classified into four categories based on the frequency band in which they operate.

- 2.4 GHz only: Supports 2.4 GHz band only
- 5 GHz only: Supports 5 GHz band only
- Dual Band switchable (DB switchable): Supports both 2.4 and 5 GHz bands, but not concurrently
- DBDC: Supports both 2.4 and 5 GHz bands concurrently

While DBDC is not a requirement for Community Wi-Fi, DBDC would allow operators to use separate bands for public and private SSID. For example, use 5 GHz for private SSID and 2.4 GHz for public SSID. With DBDC, support for multiband steering is an important consideration. Multiband steering should allow operators to load balance between bands dynamically.

Multiband steering is an active work item in the Wi-Fi Alliance (WFA). See section 6.1.7 of the WBA Carrier Wi-Fi Guideline document for more details on RF management.

3.8.3 Radio Resource Management (RRM) and Self Organizing Network (SON)

In addition to ACS, DBDC, and site survey, operators should also consider the use of RRM/SON for interference mitigation and performance improvement especially in dense Wi-Fi deployments.

Community 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 the Wi-Fi resources with large numbers of APs. 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 placing centralized SON servers in the cloud or network that provide a high level management of specific parameters based upon a wider view of the Wi-Fi network that may not be available to individual APs. The goal of the RRM/SON is to provide operators with a centralized Wi-Fi SON control based on a wide view of the Wi-Fi access network, which consists of wireless controllers as well as standalone APs from different vendors.

Readers should refer to section 5.4.1 of the WBA Carrier Wi-Fi Guideline document for more details on RRM/SON requirements.

3.8.4 Non-Optimal Client Basic Service Set (BSS) Transition (a.k.a. AP Stickiness)

The model of an optimally efficient Extended Service Set Identification (ESSID) would include wireless clients that quickly transition to the best AP in order to always take advantage of the highest available data rate/MCS. This would not only benefit this specific wireless client, but all other clients in the same BSSID as lower data rates mean fewer transmission opportunities. Unfortunately, many wireless clients prefer to hang onto an AP until they are forced to transition by increasing retries/missed packets/etc. The easiest way to control this behavior is to disable the lower data rates (e.g., 1, 2, and 5.5 in an 802.11b network), which will force all attached clients to only use the highest rate. The primary downside to this approach is the need for far greater AP density as the cell sizes will be significantly reduced. Alternatively, a vendor could create a vendor specific de-authentication algorithm in the AP, which could look at the quality of the received signal (Received Signal Strength Indicator (RSSI), bit error rates, retries, etc.) and disassociate the wireless station when one of the thresholds is crossed. This could have a detrimental effect on Real-time Protocol (RTP) dependent applications, like VoIP, as the mobile client would have to perform a panic transition to get back onto the WLAN.

3.9 Radio Conformance

With recent convergence in the industry for mobile-fixed interoperability it is relevant to depict possible scenarios that define Community Wi-Fi interworking with other networks, such as cellular. As Community Wi-Fi deployments increase, radio conformance issues may become prevalent and the need for radio conformance will be necessary . To that end, the Groupe Speciale Mobile Association, International Telecommunication Union, and Wi-Fi Alliance are responsible for defining and certifying radio conformance.

3.10 Cellular Interworking

Community Wi-Fi by nature is a Wi-Fi hotspot for a visiting user, either at home or a business location. A valued user for those locations most likely will be relatively stationary within the hotspot for a reasonably long period of time, from a few minutes to several hours. In certain locations and conditions, the user may wish to not consume their mobile data quota in the case of mobile subscription caps, and common multi-mode mobile devices already build a lower route metric (higher priority) for Wi-Fi when it is available. As Wi-Fi coverage grows, the necessity to provide consistent service quality and interfaces for users across different access networks grows simultaneously.

Interworking between Wi-Fi and cellular networks should happen in many aspects to enable or enhance the services:

3.10.1 Create mutual trust domains

Network access over the Community Wi-Fi network needs to have the same level of security as a cellular network. This can mean:

When on Wi-Fi, the user shall be authenticated and authorized using strong protected authentication mechanism such as 802.1x/extensible authentication protocol (EAP), which is also a better user experience when the authentication and authorization can be serviced from one system for both Wi-Fi and cellular accesses using unified ID and authentication backend system. EAP-SIM/AKA on Wi-Fi and SIM/AKA on cellular is a good example that the same authentication and key management backend can be reused on both systems.

The 802.11i protected air interface for Wi-Fi provides strong session integrity and confidentiality, equivalent to the available mechanisms on cellular, such as Packet Data Convergence Protocol (PDCP)layer protection used in long term evolution (LTE) systems (as defined in 3GPP TS 33.401).

Community Wi-Fi APs have the capability to backhaul data traffic to centrally managed core network when needed. The backhaul can be protected optionally, such as using VPN technologies or secure tunneling (control and provisioning of wireless access points (CAPWAP) etc.). Some underlying transport provides additional security such as the DOCSIS Baseline Privacy Interface (BPI). In some cases, Wi-Fi AP even shares the same backhaul transport with a cellular base station. Wi-Fi and cellular networks in a lot of cases use the same common backhaul technologies (Carrier Ethernet, fiber, DOCSIS, etc.) and the approaches to secure the backhaul (for example, IPsec in the 3GPP TS 33.402 Network Domain Security (NDS) and applicable in Wi-Fi backhaul as well). In many Wi-Fi as well as cellular practices, protection for the backhaul is optional considering that backhaul is typically a closely managed transport, and signaling already has built-in security. Therefore Wi-Fi and cellular networks are attributed with equivalent levels of security at the backhaul segment.

Community Wi-Fi network is a managed and monitored carrier network, similar to the cellular system. The Community Wi-Fi control plane and data plane can be aggregated in a managed Wi-Fi core network that can provide proper management and security before passing those areas off to cellular networks.

Whether a network is trusted is typically a case by case decision, to be made by the interworking parties. However the argument here is that the Community Wi-Fi network can be categorized as a trusted network for a cellular system or vice versa due to the analogous security architecture between the two access networks. Being a trusted domain to each other, services from either network can be integrated or expanded easily to the other network. It should also be noted that the interconnection between the Community Wi-Fi and the mobile network can be based on the so-called untrusted model, where the evolved packet network (ePDG) border network element provides additional security feature before allowing the access to the mobile core network of the user connected via Community Wi-Fi. More is discussed in following sections.

3.10.2 Enable Service Continuity

Cellular wireless systems have been evolving and data service revenue is in steady increase against traditional voice and SMS. Among cellular provided services, some have been successfully transformed in the past few years into data oriented services, such as what has occurred for messaging services, which have become increasingly data network focused, from the handsets all the way to the application services.

Service continuity in cellular wireless systems when devices are moving into 3GPP coverage is provided natively by 3GPP procedures. On one hand Release 8, the 3GPP wireless system, provides the capability to support mobility between the 3GPP access and the non-3GPP access, guaranteeing session continuity when devices move between APs or if the session is moved between 3GPP and WLAN interfaces. 3GPP specifications define mechanisms at the network layer for supporting mobility for IP-based services (e.g., email, browsing, etc.).

On the other hand some traditional cellular services are still going through changes to enable integration with packet switched accesses. One of the major changes is the shift to voice over LTE (VoLTE) for support of voice and accessory services over data connections with IMS systems. 3GPP TS 23.237 [x1] and TS 23.292 [x2] defines the voice call continuity (VCC) service (compared to earlier version: TS 23.206 [x3] VCC) between legacy 2G/3G circuit switched (CS) and packet switched (PS), covering the dual radio PS-CS VCC and Single Radio Voice Call Continuity (SRVCC)PS-CS VCC use cases. The VCC system requires the enhancement on the UE and MSC to interwork with the IMS SCC application services; it also requires compatible interfaces on visiting and home IP multimedia subsystems (IMS). IMS session continuity enables media sessions to move the IMS session, and consequently the services supported, between different IP interfaces with different IP addresses assigned to each of them.

Community Wi-Fi as a managed carrier Wi-Fi system is a data network that can be used for voice services. To support service continuity, the interworking between Wi-Fi and cellular services may use the mechanisms described below:

- Mechanisms to discover the network relationships in a timely manner: Passpoint comes into picture allowing the broadcast of cellular network roaming relations on Wi-Fi
- A policy to effectively manage the network handover for voice services is required, which needs to take into account the user preference, in-call situation, quality of the networks, location and user speed etc. Mobile devices may be able to use 3GPP-defined ANDSF to obtain a device/user level policies, while the current HS2.0 release does not cover the scenario for 3GPP/WLAN interworking
- Wi-Fi systems should map the QoS levels and admission control mechanisms available in the latest cellular technology, so that during the transfer of packet data network (PDN) connection or flow context, the corresponding QoS level can be properly applied in the destination access. The most recent QoS technology on Wi-Fi is WMM (802.11e and later part of 802.11-2007) which is designed to prioritize real time voice and video services. WMM is not necessarily defining an end to end solution. What is available is in the latest 3GPP standards, where the Minimum Guaranteed Bit Rate (GBR), Maximum guaranteed Bit Rate (MBR)and QoS Class Identifier (QCI), Address Resolution Protocol (ARP)concepts are fully standardized and the implementation is clear how to tie each bearer from user equipment (UE) all the way to network and how the QoS settings are mapped layer to layer. In more detail, the differences between Wi-Fi and LTE QoS exist in that Wi-Fi does not provide guaranteed bit rate; Wi-Fi defines four access categories and eight QoS levels, but has no definition of latency and packet loss rate constraints for these categories, while 3GPP standardize nine QCI with corresponding latency and packet loss constraints while definition of additional QCIs is left to the operator to decide. If a differentiated user service plan needs to be applied on Wi-Fi, e.g., a gold vs. silver voice plan, the Wi-Fi network does not define standards as to how this can be achieved; it is subject to the individual Wi-Fi vendor to implement the classifier to translate the user profile and network settings to applicable Layer 2, Layer 3 and QoS settings, as well as WMM priorities on the RAN. The QoS interworking has been standardized in 3GPP and BBF respectively in 3GPP TS 23.139 [x], TS 23.203 [y] and in BBF TR-203 [z], TR-291[v].
- In some cases, continuity of an IP session may be desired. The approach to maintain IP mobility between the two access networks is defined in 3GPP TS 23.402 [y]. The interworking for a trusted scenario is based on S2a and STa interfaces combined with Trusted Wireless Access Gateway (TWAG) introduced in Release 11 and further enhanced in Release 12. The interworking for an untrusted scenario is based on combination of S2b, SWa interfaces and ePDG.
- The interworking for a trusted model is based on deployment of a TWAG in the Community Wi-Fi architecture, with the S2a interface based on GPRS Tunneling Protocol (GTP) and the STa interface between the fixed AAA proxy and AAA server in

mobile core network. In release 11, specification for the communication between the TWAG and the UE is based on the establishment of a point-to-point link, yet the support of protocol control between the UE and TWAG is out of the scope of Release 11 and is subject to individual implementation. If a trusted model is supported the Community Wi-Fi will support the requirements, as defined in 3GPP TS 23.402 [x], 3GPP TS 24.302 [x], 3GPP TS 29.273 [x], 3GPP TS 29.274 [x], 3GPP TS 29.281 [x], 3GPP TS 29.275[x], 3GPP TS 23.139 [j], BBF TR-203 [x], BBF TR-291 [x]:

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

- The handover between the Community Wi-Fi 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
- For a given UE simultaneous access to the 3GPP EPC through S2a and non-seamless offload (i.e., direct connection to internet from CPS network) is not supported

The above limitations have been addressed in Release 12 where the new control WLAN Control Protocol (WLCP) between the UE and the TWAG has been defined in TS 23.402. This control protocol transports all signaling between the UE and the mobile core network via the TWAG, enabling the support of all mobile capability, such as dynamic establishment of PDN connection and related mechanisms. The WLCP protocol is transported over IP. It is important to point out that it is assumed that TWAG is the first router, i.e., CPE and AP shall be configured to have a L2 point-to-point connection between the UE and the TWAG.

Release 12 introduced three operational modes:

- Transparent Connection mode where the trusted WLAN may set up non-seamless WLAN offload or an S2a tunnel without explicit request from the UE
- Single Connection mode where only a single connection either for non-seamless WLAN offload or for PDN connectivity is supported between a UE and a trusted WLAN. This connection can be negotiated during authentication over TWAN. The Single Connection mode represents the Release 11 solution
- Multi-connection mode where a single or multiple connections at a time are supported between a UE and a trusted WLAN. One connection can be used for non-seamless WLAN offload and one or more simultaneous connections can be used for PDN connectivity

The EAP-AKA’ protocol has been extended for supporting Release12 Trusted scenario, as specified in TS 23.402 and TS 33.402, to support the negotiation of the connection mode to be supported.

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 Community Wi-Fi and after receiving an IP address, performs the establishment of an IKEv2 tunnel with a selected ePDG (SWu interface) 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 Community Wi-Fi. Optionally a IKEv2 Mobility and Multihoming Protocol (MOBIKE) feature can be used to support the mobility between different APs providing connectivity to the same ePDG. The S2b support and corresponding procedures are defined by the 3GPP specifications TS 23.402[Y1], TS 33.402[y2], TS 24.302[y3], TS 29.273 [y4] and by the Broadband Forum TR-291.

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.

These alternative scenarios were previously analyzed in GSMA–WBA Wi-Fi roaming Task Force White Paper on session continuity with IP address preservation (July 2013).

The IP mobility solution enables PDN connections to move from one access to the other (e.g., from 3GPP to WLAN) when the UE moves between accesses. In addition the solutions enable the UE to be connected directly to the Internet from the Community Wi-Fi without sending traffic via the 3GPP EPC. This scenario is called non-seamless WLAN offload (NSWO) since a new IP addresses is assigned and the service may be required to be re-established. The NSWO traffic can be supported in parallel with the routed EPC.

Interworking with 3GPP networks:

- Simultaneous access to both Wi-Fi and cellular radio is enabled by 3GPP specifications. The first capability is called Multi Access PDN Connectivity (MAPCON), when the 3GPP UE is simultaneously connected with some PDN connections maintained on the 3GPP access network, while other PDN connections are on WLAN. The second is called IP flow mobility (IFOM), when the UE is connected to the same PDN connection via both accesses and the single IP flow can be moved from one access to the other. 3GPP is currently addressing the support of IFOM for both s2a and s2b interface.
- Simultaneous access to the same application via both Wi-Fi and cellular radio is now under study with the usage of Multipath TCP (MPTCP, see IETF RFC 6824[v]) to enhance the integration of multiple access networks at the TCP level to create bundled bandwidth, as well as non-breaking reliabilities when the device is in any available network coverage.
- Integration of the Community Wi-Fi and cellular networks can be reflected in location based service as well, where detection of location can be through GPS, cellular, Wi-Fi whichever is best available and the location information collected could be aggregated into a single platform for application to benefit from.
- If the Community Wi-Fi user traffic is to be locally offloaded (NSWO), and in the situation of having the same carrier delivering the mobile and access, the operator can opt for a convergent control plane solution. This means that instead of establishing a tunnel from the fixed edge to the mobile edge as described previously, the operator could extend the policy and charging interfaces (Diameter Gx and Diameter Gy/Gz interfaces) towards the fixed domain. This simplifies the control plane of both accesses and reduces the time to market of new commercial offers. For instance, with a convergent solution it would be possible for the Community Wi-Fi user to use the mobile data subscription consumption limits in the Wi-Fi access. This solution was developed by 3GPP in collaboration with BBF and details could be found in the Release 12 of the 3GPP TS 23.203 and in the BBF WT-300 (still work in progress by the time of this writing).

See section 5.5 of the WBA Carrier Wi-Fi Guideline document for more details on interworking with 3GPP networks.

3.11 IPv6

In a SoftGRE-based Community Wi-Fi network architecture, all traffic (including device provisioning,) to and from a client on the public SSID is tunneled from the AP to the WAG in the service provider's Wi-Fi core network, with the AP acting as a bridge and tunnel source point. The AP should support configuration of tunnels for this implementation.

Alternatively, there are other Community Wi-Fi network architectures that do not require tunnels. IPv6 was designed to support a large number of IP addresses. This enables the allocation of a public IP address to every device in a network. In contrast to IPv4, where devices behind Network Address Translation (NAT)may not be identifiable from the Internet, in IPv6 every device will have its own digital identifier across the network. This fact allows tracking users' sessions from the Community Wi-Fi core network without the need of tunnels. The same equipment in the core network in charge of user session tracking can be used to provide, for instance, QoS. Note that, during the transition period from IPv4 to IPv6, there should be a distinction between the tunneled IPv4 traffic and the non-tunneled IPv6 traffic in the network topology of the Community Wi-Fi. The AP would route IPv4 traffic to tunnel concentrators while the IPv6 traffic would not be tunneled.

Many operators are actively transitioning their network to support IPv6. These operators have a strong interest in deploying Community Wi-Fi AP devices that support IPv6-only and dual-stack for the backhaul between the AP and the Wi-Fi core for user's IPv4 or IPv6 traffic. The examples of backhaul technologies include GRE over IPv6, PMIPv6, and CAPWAP over IPv6. The AP device should be able to support IPv4-only, IPv6-only or dual-stack client devices on the public SSID.

Similar to the Community Wi-Fi AP device, the WAG should support both IPv6 and IPv4 for traffic backhaul between the AP and WAG. Since a single WAG device most likely will support connections to multiple (e.g., millions) APs that may have different levels of IPv6 support, the tunnel endpoint at the WAG should be configurable in IPv6-only mode for some APs, IPv4-only mode for some APs and dual-stack mode for some APs. The AP device should be able to support IPv4-only, IPv6-only or dual-stack client devices on the public SSID.

Both DHCPv6 and stateless auto-configuration should be allowed by client devices to obtain an IPv6 address. Stateless auto-configuration refers to the case where the client configures its IPv6 address from the prefix in the Router Advertisement (RA) message that it receives from the edge router in the provider's core network.

The Community Wi-Fi network should allow the operators to enable and disable the IPv6 RA Flags Options ([RFC 5175]): A, M, and O. The A flag (Address Configuration Flag), when set to 1 in the RA message, is used to indicate that the prefix can be used for stateless address configuration (SLAAC). The M flag (Managed Address Configuration Flag), when set to 1 in RA message, is use to indicate that DHCPv6 is available for IPv6 address allocation. The O flag (Other Configuration Flag), when set to 1 in the RA message, is used to indicate that other configuration information (ex: DNS server IPv6 address) is available through DHCPv6.

Both Recursive DNS Server (RDNSS)and DNS Search List (DNSSL)should be supported in order for the client device to obtain DNS server information using the methods defined in RFC 6106.

The selection of the right IPv6 addressing model for clients in the Community Wi-Fi network is important. The following two IPv6 addressing models should be considered for the clients in the Community Wi-Fi network:

- Unique-Prefix Model - As per this addressing model, network prefix(es) assigned to a client device on the public SSID are for its exclusive use and no other client device on the same public

SSID shares an address from that prefix. There could be multiple unique IPv6 prefixes assigned to each client device on the public SSID. This is the same model that 3GPP uses for their UEs

- Shared-Prefix model - The IPv6 prefix that is assigned to the client devices on the public SSID is a shared prefix. There can be more than one client device on the public SSID that can be using IPv6 addresses from that prefix. Even in the shared-prefix model, the network prefix used for the clients on the private SSID is completely different from the network prefix used for the clients on the public SSID

The following table provides a discussion on pros and cons of using Unique and Shared prefix model for the Community Wi-Fi networks. Community Wi-Fi networks should allow operators to choose either of the two addressing model for clients on the public SSID.

	Pros	Cons
Unique Prefix model	Potentially reduced link local multicast traffic Clients are unable to find the MAC or IP of neighbors via standards ARP/ND Traffic between clients is required to go through a router	Inefficient use of address space
Shared prefix model	Stateful DHCP, Stateless DHCP or - Stateless Address Autoconfiguration (SLAAC) with RDNSS can be used to assign shared prefix	Clients are allowed to find the MAC or IP of neighbors via standards ARP/ND (if no Layer 2 filtering) Clients can communicate with each other directly through the AP (if no Layer2 filtering) Compared to unique prefix model, higher link local multicast traffic

Additionally, the Community Wi-Fi network should allow operators to perform management operations using either IPv6 or IPv4. In the long run, the Community Wi-Fi network should allow operators to use IPv6-only on the CPE devices for management operations.

While this section provides IPv6 consideration specific to Community Wi-Fi networks, the ‘WBA Wi-Fi Operator Guidelines - IPv6 for Carrier Wi-Fi’ explores the use cases and deployment considerations for IPv6 in carrier Wi-Fi network in much detail.

3.12 Session Mobility

3.12.1 Session Mobility within a Community Wi-Fi network operated by a single operator

In this scenario of session mobility, an on-the-go subscriber of the MSO should be able to connect to the public SSID broadcast from one home and seamlessly transition to the public SSID from another home as the user travels away from the first home towards the other.

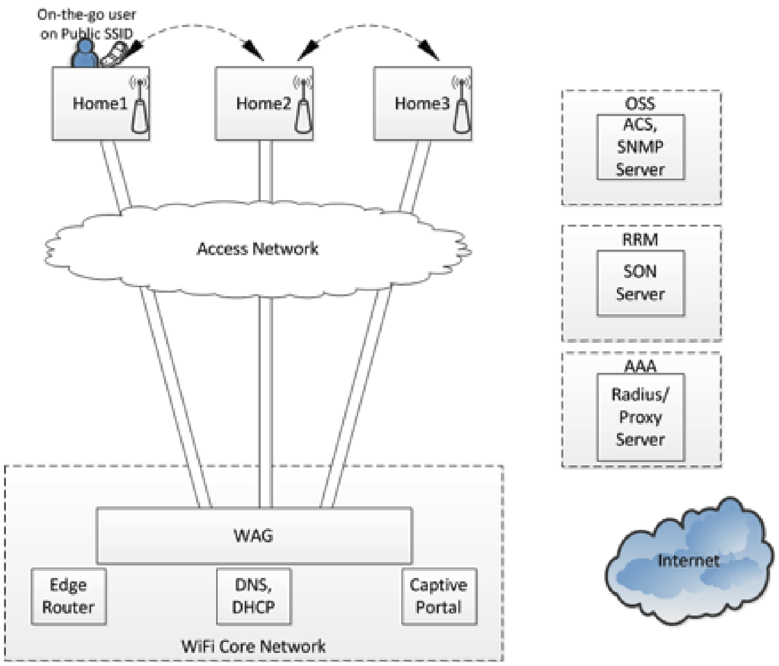


Figure 3:13 Session Mobility within Community Wi-Fi Network - Single Operator

It is assumed that all the APs in this scenario are serviced by a single MSO and connect to the same Wi-Fi core network via a SoftGRE (or CAPWAP) tunnel through the provider's access network. To maintain a session while the user is transitioning from one AP to another, it is important that the IP addresses used do not change through the session between the two APs involved in the handoff. Also, in the case of IPv4 addressing, the NAT bindings of the client with the AP should be maintained across different APs in the network. Provisioning in IPv6 can be done through any of the methods- DHCPv6 (stateful), SLAAC, or DHCPv6 with SLAAC (stateless), with the RAs sent by the Edge Router in the Wi-Fi core.

Since the Wi-Fi core network handles all provisioning and all the APs are connected to the same WAG, the provider's network should maintain the session as the transition happens. Also, in case of a failure of one WAG, the tunnels should be configured for a seamless failover mechanism for continuous connectivity.

3.12.2 Session Mobility between Community Wi-Fi and Hotspot networks operated by a single operator

For the case when the user is moving from one AP to another within a Community Wi-Fi network, seamless connectivity can be accomplished between the APs, as described in the section above. Similarly, for user session mobility from a Community Wi-Fi network to a Hotspot network provided by the MSO, the TCP session should be maintained during the transition, which requires that the source and destination IP addresses be maintained. For this, communication between the WAG and WC is essential, as shown below. The user is provisioned by the provisioning servers in the Wi-Fi core network via a SoftGRE tunnel between the WC and the WAG. This way, both the networks are aware of the IP addresses assigned to the clients and as they move from one network to another, seamless transition is possible.

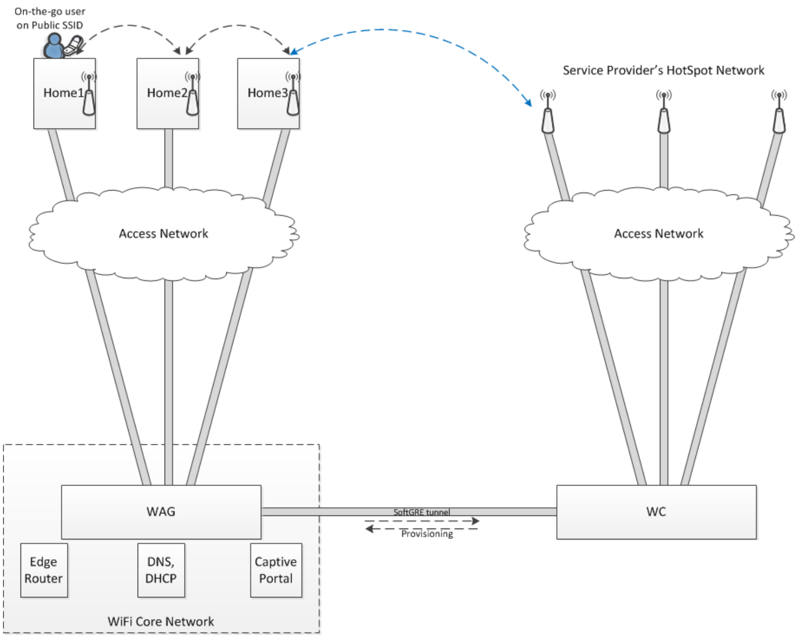


Figure 3:14 Session Mobility between Community Wi-Fi and Hotspot - Single Operator

3.12.3 Session Mobility between Private and Public SSID in the Community Wi-Fi Network operated by a single operator

When a user on the public SSID is moving from one AP to another in a Community Wi-Fi network, the user session is maintained by maintaining the source and destination IP addresses. This may be done via the Mobility Anchor in the Wi-Fi core network of the service provider. However, in the case when a user is moving from a public SSID to a private SSID, maintaining the session might be more challenging.

Traffic to and from each client on the public SSID goes through the tunnel (SoftGRE, CAPWAP, L2TP, etc.) with the AP only acting as a bridge between the client and the Wi-Fi core network. Therefore, all provisioning for clients is done from the backend servers in the Wi-Fi core, not by the AP. On the other hand, a client on the private SSID is provisioned by the router in the AP, based on the address space assigned to it by the service provider. Due to all provisioning for the private and public clients being performed by separate entities in the network, user mobility poses a challenge that needs addressing. A similar problem exists with user authentication where the clients are authenticated by different entities in the public and private SSIDs.

One potential solution to this problem is for the provisioning of both public and private clients to be handled by a single entity; the WAG. When provisioning, messages of even the private clients are tunneled across the network to the WAG, which can act as a mobility anchor transitioning the IP session when the client is in the presence of both networks, public and private. Separate tunnels created for traffic on the public and private SSIDs dynamically address this issue as illustrated in the diagram below:

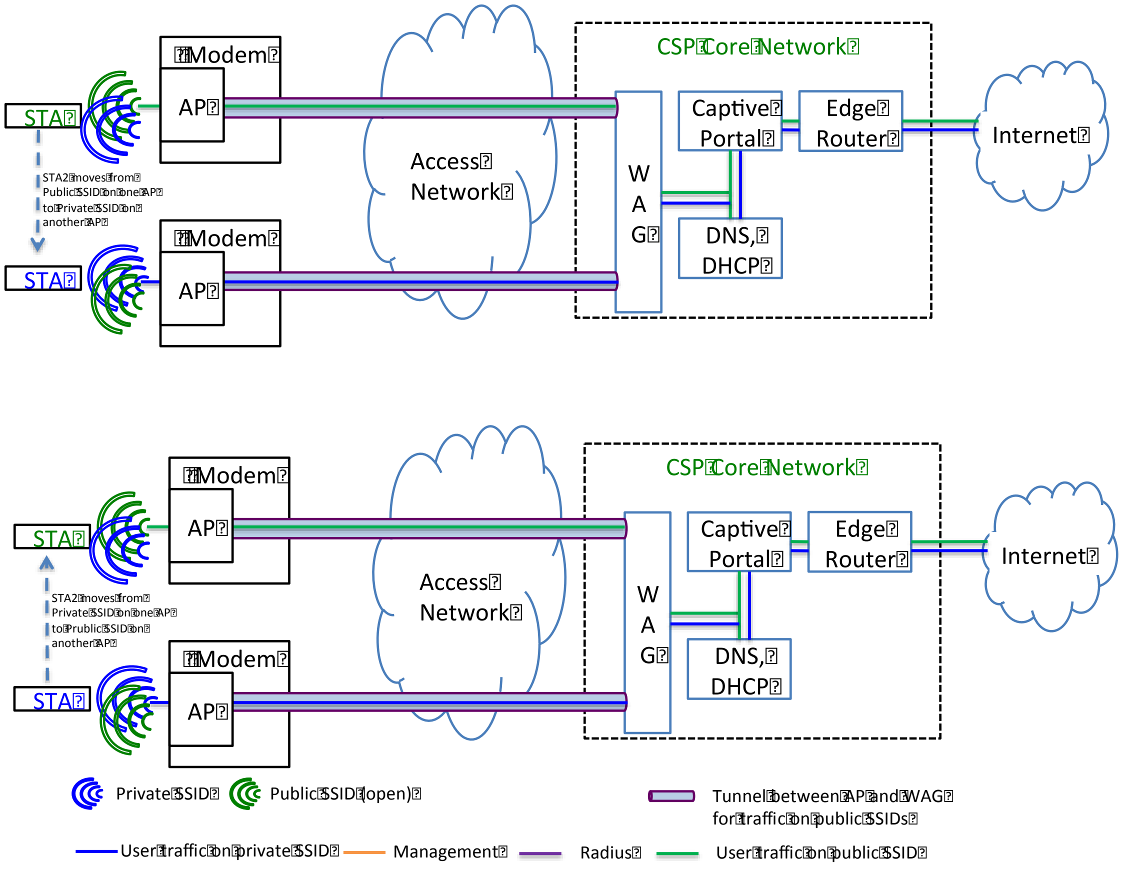

CSP Core Network
Modem
AP
STA
STA2 moves from Public SSID on one AP to Private SSID on another AP
Modem
AP
STA
Access Network
W A G
Captive Portal
Edge Router
DNS, DHCP
Internet
CSP Core Network
Modem
AP
STA
STA2 moves from Private SSID on one AP to Prublic SSID on another AP
Modem
AP
STA
Access Network
W A G
Captive Portal
Edge Router
DNS, DHCP
Internet
Private SSID
Public SSID (open)
Tunnel between AP and WAG for traffic on public SSIDs
User traffic on private SSID
Management
Radius
User traffic on public SSID

Figure 3:15 Session Mobility between Private and Public SSID in Community Wi-Fi - Single Operator

Currently no specification addresses the requirements for this use case implementation. This is a gap that needs to be addressed. The above illustration is just one proposed high level solution to the problem at hand. The objective of this section is to throw light on the current gap that exists in the deployment of Community Wi-Fi and stir discussion on the issue to come up with a near to long term solution to the problem.

3.12.4 Session Mobility for a mobile customer in Community Wi-Fi network interconnected to a mobile core network

In the case that Community Wi-Fi does not have contiguous coverage, the 3GPP interworking solution enables the handoff between different Community Wi-Fi by the means of an intermediate handoff to mobile coverage. Furthermore, if APs of the same Community Wi-Fi have overlapping coverage, the 3GPP interworking solution enables handoff between APs thanks to usage of TWAG or ePDG.

The interworking scenario between the Community Wi-Fi and the mobile core network is described in clause 3.9.

It should be noted that this solution enables the handoff only for the 3GPP devices.

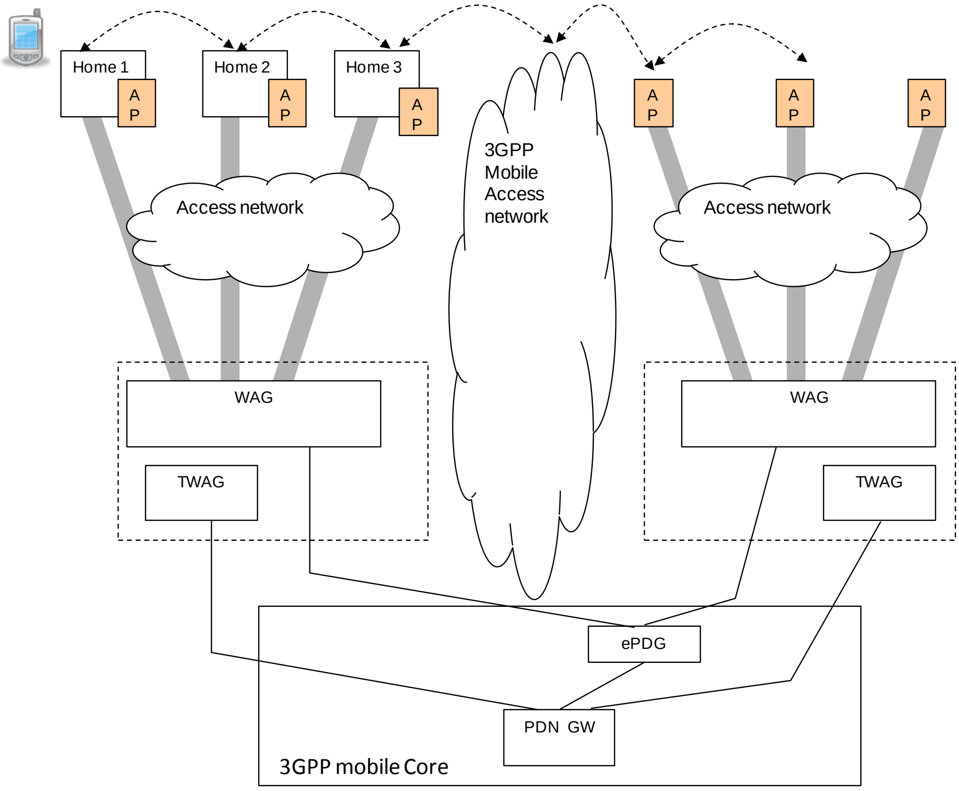


Figure 3:16 Mobile Customer Session Mobility in Community Wi-Fi - Mobile Core Network

3.12.5 802.11r – Fast BSS Transition

In order to provide a seamless user experience, real time mobile applications such as voice and video require the ability to quickly transition from one BSSID to another. 802.11r defines standard key-caching mechanisms that greatly reduce the transition time by way of reducing the number of steps during the association handshake. Key caching is typically managed and directed by a wireless LAN controller, so it may not be achievable for some standalone AP deployment scenarios. Community Wi-Fi network architectures are generally deployed without a wireless LAN controller. Currently, there are no standards or documents that define Fast BSS transition in Community Wi-Fi networks.

802.11k and other RRM solutions can assist in fast transition by informing the client of neighboring access points. See 5.4.1 of the WBA Carrier Wi-Fi Guideline document for more details on RRM/SON requirements.

3.13 Network Security and Privacy

Network security within Community Wi-Fi must address numerous issues including:

- Keeping the private SSID traffic secure from the public SSID users
- Keeping the public SSID traffic secure from both the private SSID users and from wireless attacks or interception
- Man in the Middle attacks pose an increased treat to Community Wi-Fi, in that the public SSID is known, standard, and widely deployed. A user may be less suspicious by seeing the same SSID that they are used to seeing elsewhere
- Isolating the public SSID users from seeing each other’s traffic

- Authenticating the public SSID users and allowing appropriate network access
- Intrusion detection and prevention (IDS / IPS)

Securing the private SSID traffic is addressed partially at the user configuration level, in that the private subscriber can specify and maintain whatever level of supported wireless security they would like (e.g., WPA2-PSK). Similarly, traffic on the public SSID is managed by the CSP picking an appropriate level of wireless security (e.g. WPA2-ENTERPRISE). Public/private traffic isolation can be managed by several wire-side technologies and configurations such as:

- Enable peer-to-peer blocking at the AP
- Tunneling the private traffic from the AP to the CSP core. An LMA or WAG are both appropriate termination points for the tunnel [See section 3.3]
- Use separate IPv4 subnet and IPv6 prefix for clients on private and public SSID
- Use unique IPv6 prefix for each client on the public SSID

Standard authentication technologies exist that can be used for Community Wi-Fi, such as EAP-SIM or EAP-TTLS. Not only does authentication prevent unauthorized access, it is also critical for accounting and billing (AAA). HS2.0 will also be able to manage authentication and network access.

Community Wi-Fi security should also follow the WBA Carrier Wi-Fi guidelines (section 5.1.7) **9** regarding security.

3.13.1 Open SSID

One currently deployed method of allowing public Wi-Fi access is with a captive portal on an open SSID. The public user would associate with the open SSID and be presented with the credential/payment webpage. Upon successful registration, the user's device would then have full internet access. MAC caching may be available that would allow the user's device to reconnect without needing to repeat the registration process, but this is not recommended since MAC caching may be subject to MAC spoofing attacks. Since an open SSID is unencrypted, users must rely on application-layer security (e.g., HTTPS).

3.13.2 Secure SSID

In the future, we expect to see more public Wi-Fi access via secure and encrypted SSIDs. The user may be redirected from an open SSID with a captive portal, or they may have an existing subscriber agreement that allows them access to the secured SSID. Operators can use methods such as EAP-TTLS to enable the secure SSID.

3.14 Community Wi-Fi Hotspot Location Information

As it happens in other type of networks, Community Wi-Fi hotspots location information is relevant for a plurality of services that ranges from Radius to ANDSF and advanced location based services. In contrast to carrier Wi-Fi, Community Wi-Fi networks deployments are emergent (non-planned). The topology is continuously changing and evolving. This fact adds complexity to hotspot location information management requiring, for instance, a system able to provide updated topologies and hotspot location maps.

On the other hand, Community Wi-Fi hotspots are commonly residential and linked to a broadband subscription with an ISP. There is a contract between the ISP and the subscriber. This contract requires the exchange of subscriber personal information which is subject to data protection legislation. Among this data, the subscriber address is provided. Although there are different methods (e.g., IP address geolocation data, Wi-Fi signals based, etc.) to derive hotspot location without user intervention, this is considered intrusive and against certain legislations. Thus, it is normally assumed that the contract subscriber address corresponds to the location of the hotspot. As this is personal information, the subscriber must accept in the contract that this information might be available publicly or to third parties and systems. Of course, this approach is also impacting the accuracy of hotspot location, since contract address to hotspot location correspondence might not be accurate or updated.

3.15 Lawful Intercept

Lawful intercept is an important consideration and should be addressed in the architecture design for Community Wi-Fi networks. Since the traffic in on the public SSID is tunneled to the WAG and the tunnel may be encrypted, the WAG may be the most logical point for lawful intercept. Radius/AAA is also an important piece of lawful intercept, as this is the point in the network where a local or roaming user can potentially be identified.

The detailed architectures and requirements on how to support lawful intercept in Community Wi-Fi networks are outside of the scope of this document.

3.16 Hotspot 2.0

The application of HS2.0 technology in Community Wi-Fi will provide for much more than automatic network discovery and selection. HS2.0 will allow users to self provision, allow operators to commoditize the access network, allow operators to maintain device subscription, and facilitate device roaming with partnered operators.

3.16.1 Community Wi-Fi Device Provisioning

As Community Wi-Fi networks are deployed by operators, one of the challenges will be to ensure subscriber devices are provisioned correctly. Devices can be provisioned manually or via online sign up (OSU) in HS2.0 Release 2, which facilitates loading device configurations from the CSP. This includes prioritizing manually configured home versus HS2.0 roaming or visited networks, priority of visited networks based on operator agreements, and network selection based on network load. HS2.0 additionally allows operators to perform subscription remediation in the event of changes in either policies or subscription. The use of the OSU service, depending on how the operator chooses to implement it, can enable the user to self-install the device configuration on new devices.

3.16.2 Community Wi-Fi Roaming

Based on use of the ANQP elements NAI Realm, 3GPP Cellular Network, and Roaming Consortium IDs, HS2.0 devices can determine which network to use from all available HS2.0 enabled SSIDs. Using information in the device subscription configuration, the device can determine if the home network is available, and if not it will roam to a Community Wi-Fi SSID. The device subscription configuration will allow an operator to prioritize roaming partners based on agreements between the operators or other related factors. HS2.0 will allow a user’s device to connect to the visited network without any manual user action.

3.16.3 Monetizing Community Wi-Fi

Through the use of the HS2.0 online sign up (OSU) server, the operator will able to monetize the Community Wi-Fi network. This is done by allowing a non-subscriber of the operator or partnered operators to purchase services on the Community Wi-Fi network. This can be for short periods of time, such as a few hours, to longer periods, such as a week or a month.

3.16.4 HS2.0 Load Attributes

HS2.0 AP loading attributes can be used by a device to aid in determining which access network to use in cases where the network providers are of equal priority. This will allow for a better user experience in cases where one network has more available bandwidth than another.

3.16.5 Enabling HS2.0 on Community Wi-Fi

HS2.0 requires CPE hardware and firmware that supports HS2.0 functionality, along with CSP infrastructure, such as the OSU server, Policy server, and Remediation Server. In addition, the user must have a mobile device that supports HS2.0. HS2.0 Release 2 is backward compatible with HS2.0 Release 1 so a mixture of devices could be used on the same HS2.0 provisioned network.

The AP will need to be configured with the HS2.0 attributes and have HS2.0 enabled. The full list of attributes can be found in the WBA HS2.0 Release 2 specification. These attributes include the elements used for network selection, Roaming Consortium IDs, NAI Realms, and 3GPP networks. It is worth noting that any combination of one or more of these elements may be used depending on roaming agreements and partnerships. Other elements include Operator Friendly Name, Domain, Icons, OSU server, etc.

The CSP must install and configure AAA, OSU, Policy, and Remediation servers. The AAA server is used for Radius functions for authentication and accounting. The OSU server is used for the OSU functions. The Policy server is used to administer the policies used in the device subscription configuration. The Remediation server is used to signal the AAA server when Remediation is needed and to perform the remediation process.

The OSU server can be configured to create device subscriptions based on the policies and networks selection needs of the operator. The OSU server can be used simply to provision subscriber devices or for advanced commoditization of the Community Wi-Fi network.

The Policy server will be configured based on the policies the operator wishes to enforce. These policies should be established prior to enabling HS2.0.

The Remediation server is accessed when remediation is needed, such as when there is a change in the service agreement with the end user or updates to roaming partners.

3.16.6 HS2.0 Challenges

With HS2.0 deployments there are several challenges that CSPs need to address. These include:

- Ensuring that the hardware and firmware of deployed CPE supports HS2.0
- Getting the network servers deployed and tested before enabling HS2.0
- Helping users to get mobile devices provisioned for HS2.0. The OSU function in Release 2 will help simplify this process, but there is no standard method defined in Release 1
- A large percentage of currently deployed CPE can only support one SSID. In such cases there is no capability to offer Community Wi-Fi, which requires a minimum of two SSIDs. OSU further expands the need to a minimum of three SSIDs, including the private SSID

4. High Priority Challenges for Community Wi-Fi deployments

To enhance the quality of experience of subscribers using Community Wi-Fi networks, operators need to enable a number of features in their networks. Including such features, however, implies additional costs and operators may choose to prioritize the features that they deem to be most important for their customers' quality of experience while bringing their cost to an acceptable level. For this purpose, operators may perform a cost-benefit analysis to identify such higher priority features. In this Section, we use the results of a WBA member survey (details of which can be found in Appendix A) on Community Wi-Fi and present a classification of Community Wi-Fi features from operators' perspective in terms of their importance and ranking. These classifications also provide insight on what the higher priority challenges are that operators need to deal with in their Community Wi-Fi network deployments.

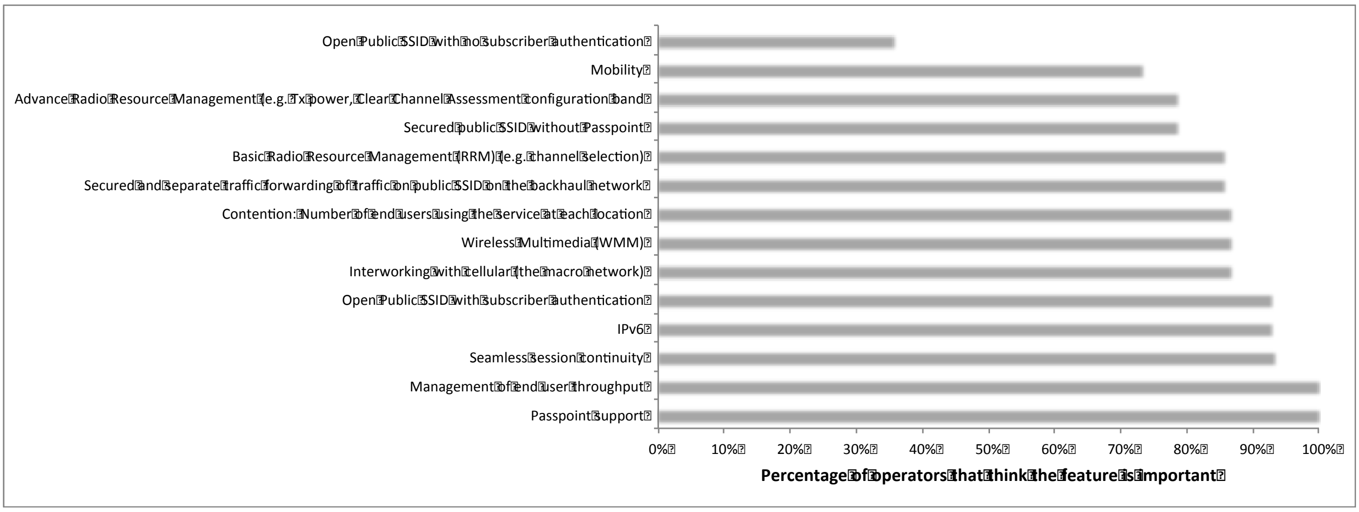


Figure 4:1 Percentage of Operators that Think a Given Community Wi-Fi Feature is Important

Figure 17 presents the percentage of operators that think a given Community Wi-Fi feature is important. The survey results show that all of the participating operators think that Paspoint and management of end user throughput are important for Community Wi-Fi.

5. Gap Analysis

This section contains gap analysis based upon the topics discussed in section 3 of this paper. 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 Community 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 long term evolution of technology. Therefore, the gap analysis recommends general timeframes for the development of work plans to close the gaps, e.g., immediate, short term, long term and no immediate concern.

5.1 Traffic Management and Prioritization on the Air Interface

- Gaps in specification: The 802.11-2012 specification provides features for application specific traffic priority functions, however lacks features for STA or groups of STAs to get QoS for all traffic. This feature is important to Community Wi-Fi because the air interface is the resource that needs to be controlled and direct control is always the most effective. A specification from some standards body should be created to address this issue

- Gaps in certification and test programs: Currently, no certification or test programs exist which cover this topic. A test program should be implemented in the near term to highlight the inability of current solutions to fully address the need. After any specification work is completed, a certification program should follow to document adherence to the specification
- Timeframe considerations: This is a short term problem that needs to be addressed quickly. Product deployment is underway and these products will have a multi-year lifetime in the field. The time is now to add air interface QoS so that as deployments continue, the products being deployed can adequately support the growth of access network data rates over the air interface

5.2 Admission Control

- Gaps in specification: While controller-based WLANs have the ability to dynamically restrict access to an SSID, the standalone nature of currently deployed subscriber access points lacks this ability. The solution will either be to attach the access points to a controller or create a method of static admission control, perhaps by simply limiting the number of public SSID users. A static limit will not be able to address fluctuations in available bandwidth, and therefore may not be adequate
- Gaps in certification and test programs: There are no admission control certifications beyond 802.11e/WMM, and that is only relevant when prioritizing application specific traffic within a single BSSID
- Timeframe considerations: This is a short term concern as public SSID oversubscription could render the private SSID (i.e., the service the home subscriber is paying for) useless

5.3 Admission Control Notification

- Gaps in specification: When a Community Wi-Fi user is denied access to the public SSID due to admission control limits they currently receive no feedback or explanation of this denial. This is not very user-friendly and could result in significant user frustration at their inability to connect
- Gaps in certification and test programs: There is no standard mechanism for CSP generated real time user feedback
- Timeframe considerations: This is a short term concern and should go hand-in-hand with the development of admission control

5.4 Session Mobility

- Gaps in specification: While 802.11k and 802.11r can assist a mobile device to quickly transition between BSSIDs in a single SSID, there is no standard for roaming between different networks (e.g., Hotspot to 3GPP, Community Wi-Fi to private, etc.)
- Gaps in certification and test programs: There are no applicable certifications or tests related to session mobility
- Timeframe considerations: This is a long term gap, as there is no current expectation of active session retention while roaming among all variations of wireless network connectivity

5.5 802.11r – Fast Transition

- Gaps in specification: 802.11r specifies a mechanism for a STA using some form of WPA to be able to transition to another access point without having to repeat the full association handshake and network access authentication process. It does this by caching the previous key, distributing that key to the new access point, and simulating a re-association, which is far shorter. While this is easy to achieve in a WLAN Controller deployment, the standalone nature of Community Wi-Fi doesn't yet have a solution for key caching and distribution

- Gaps in certification and test programs: Key caching and fast roaming is understood well enough that there should not be any gaps in certification or testing, assuming a solution can be found for non-controller environments
- Timeframe Considerations: This is not an immediate problem as it will only become relevant when applications using real time protocols (e.g., VoIP) are expected to seamlessly function while roaming between public SSIDs

5.6 Non-Optimal Client BSS Transition (a.k.a. Stickiness)

- Gaps in specification: There is no specification that covers forcing a mobile client to follow a certain data rate, however there is standard AP functionality that can achieve this result, such as disabling lower data rates/MCS values. 802.11k can provide a client with a list of APs, but cannot influence at what point the client will transition. Additionally, there is limited client support for 802.11k currently
- Gaps in certification and test programs: While there is no certification (since there is no specification), testing is fairly straightforward and easy to validate. A specification and related certification program needs to be developed
- Timeframe considerations: This is a long term concern and will only become a serious problem when Community Wi-Fi deployments achieve enough density to where inter-BSSID transition becomes commonplace

5.7 Network Selection

- Gaps in specification: While HS2.0 has the ability for a wireless device to connect to a network automatically, there remains the gap of prioritizing the private SSID over the public SSID. AP-based network steering via admission control could be deployed, but the specific implementation would have to be established.
- Gaps in certification and test programs: There is no certification program for network selection between private and public SSIDs, and a test program will have to be created.
- Timeframe considerations: This is an immediate concern, as the user device MUST always choose their specific private SSID over the public, otherwise they will not have access to their home resources (e.g., printers, local file servers, etc.)

5.7.1 Network Selection via Interworking IE

- Gaps in specification: Interworking is covered by 802.11u/HS2.0/Passpoint, however these require the user device to be compliant
- Gaps in certification and test programs: The WFA Passpoint certification program may cover this
- Timeframe considerations: This is a short term problem that may be resolved organically with the adoption of Passpoint

5.8 Wi-Fi Gateway Management

- Gaps in specification: There are currently no specifications that define the management interface and objects to manage Community Wi-Fi networks. Annex A of this paper provides some guidance on what data needs to be managed in Community Wi-Fi networks
- Gaps in certification and test programs: There is no current certification program
- Timeframe considerations: This is a short term problem, as CSPs are already beginning to roll out Community Wi-Fi

5.9 Gaps from Carrier Wi-Fi Guidelines

In addition to the gaps specified above, many of the gaps identified in the Carrier Wi-Fi Guidelines 9 document are also applicable to Community Wi-Fi. These include:

- Authentication for secure SSIDs with user name and password
- Channel selection within and across bands
- Management of resources
- Management of overload conditions
- Traffic flow parameter management in the CWLAN
- Interference management
- Additional gaps to be addressed within a longer timeframe
- Inter-network reporting of accounting records when devices move across APs
- RADIUS to diameter interworking
- RADIUS attributes
- GTP interface for 3GPP interworking
- Wi-Fi SON
- Devices with appropriate signaling behavior
- Private and public SSID selection
- Device utilization of WFA Passpoint features
- Authentication for secure SSIDs with username and password
- Channel selection within and across bands

5.10 Recommendations and Next Steps to be Driven by WBA

The WBA will drive the following tasks/activities:

- Liaise this completed document to the following bodies: 3GPP; Broadband Forum; CableLabs; GSMA; IEEE; NGMN; Small Cell Forum; Wi-Fi Alliance
- Ask liaised forums for their feedback and opinions on this topic, based on this document. Any relevant feedback received could be included in later versions of this document
- In addition, where gaps have been identified in section 5, 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 this Community Wi-Fi paper
- Take an active role in coordinating Community Wi-Fi activity in the industry and will become the reference point for Community Wi-Fi work
- Consider hosting Community Wi-Fi interoperability trials that bring together device vendors, infrastructure suppliers, and operators

Generate network management specifications or guidelines to close gaps in specifications as explained above, when needed

Generate device behavior specifications or guidelines to close gaps in specifications as explained above, when needed

- Consider launching a Community Wi-Fi compliancy program for devices and APs

6. Case Studies

6.1 Case Study#1 (Comcast)

6.1.1 Comcast Community Wi-Fi Service

Comcast is the largest cable services provider in the United States, with over 20 million high speed Internet customers.

As part of its high speed Internet service package, Comcast enables its customers to get Internet access outside the home using a Community Wi-Fi network (xfinitywifi) deployed in Comcast markets.

6.1.2 Comcast Community Wi-Fi Devices

Comcast is able to take advantage of the existing deployed CPE that currently provides high speed Internet and other services (including private Wi-Fi, VoIP, Home Security) to its customers.

The CPE is integrated into units consisting of cable modem, eMTA, eRouter, and 802.11n radio. The CPE is delivered across multiple vendors, models, and firmware variants.

By applying a software upgrade to the CPE, Comcast is able to additionally provide a Community Wi-Fi public hotspot at that location.

6.1.3 Comcast Community Wi-Fi Network Core

Comcast's Community Wi-Fi CPE uses SoftGRE tunnels to bridge the xfinitywifi traffic over the Comcast Hybrid Fiber-Coaxial (HFC) plant to the WLAN gateway core.

In order to minimize traffic latency and core network load, the WLAN gateways are located on the natural egress path of the traffic to the Internet.

Utilizing the WLAN gateway core allows Comcast to keep the Community Wi-Fi CPE 'feature light' while providing functionality (such as captive portal, authentication, accounting, lawful intercept, parental control, watermarking, QoS,) through a powerful WLAN gateway core.

6.1.4 Key Issues & Challenges – Scale:

6.1.4.1 Tunnel Architecture

Maintaining stateful Layer 2 tunnels between the AP and the WLAN gateway is a common limiting factor of the WLAN gateway capacity.

- Comcast chose to utilize SoftGRE tunnels as a tunneling protocol for the Community Wi-Fi solution for the following reasons:
- GRE is a very lightweight encapsulation
- Only the Community Wi-Fi CPE end of the tunnel needs to be configured
- No WLAN gateway heartbeat is needed to maintain the tunnel
- The tunnel is only established when traffic is being passed
- WLAN gateway's maximum tunnel capacity is aligned to the number of Community Wi-Fi CPE in use, rather than the number of Community Wi-Fi CPE configured

6.1.4.2 Migrant users

On customer devices leaving the network shortly after connecting:

- Comcast mitigates this issue by using shorter DHCP lease time to clear these sessions off the WLAN gateway and reduce effective managed concurrency
- Many client devices connect to the Community Wi-Fi service without either authenticating or sending data traffic
- Comcast mitigates this issue by not committing full WLAN gateway subscriber resources until clients are authenticated and actually passing traffic

6.1.4.3 Density and Proximity

As the deployment model for Comcast's Community Wi-Fi is defined by where they have existing CPE, rather than a designed Wi-Fi deployment, they have a mix of very sparse coverage (farmhouse with no close neighbors,) and very dense coverage (MDU with many horizontally and vertically adjacent CPE). In the dense scenario, this could be a blend of multiple vendor CPE devices.

A RRM solution that can work across the different vendor CPE variant is necessary to effectively optimize the Community Wi-Fi experience.

6.1.4.4 Operations and Management

Increased operational complexity with managing multi-vendor solution due to:

- Differences in features and functionalities (capabilities or development maturity)
- Differences in minimum performance level
- Vendor-specific management interfaces

Driving the vendor community towards vendor agnostic interfaces and consistent features with a predictable behavior model is critical to minimize the complexity of their OSS platforms. This will aid in the simplification and automation of Wi-Fi testing.

6.1.4.5 Network Selection

The client devices in the customer home will occasionally prefer xfinitywifi SSID over private secure SSID. As a result, the customer may not be able to connect to home devices (e.g., a printer).

6.1.4.6 Traffic Segregation

It is important that the Community Wi-Fi service does not degrade the security or experience of the home user.

Comcast segregates public and private traffic by VLAN at the eRouter and by DOCSIS service flow at the cable modem.

6.1.4.7 QOS and Prioritization

Comcast is evaluating Wi-Fi radio packet prioritization techniques for protection of the shared radio resource.

6.2 Case Study#2 (Belgacom Fon)

Fon is a company founded in 2006 with the goal of blanketing the world with Wi-Fi that is free for everyone. Currently, it has more than 12 million hotspots in 170 countries across the globe and partnerships with world’s leading telecommunication companies. Fon lets fixed line broadband operators extend their Wi-Fi offering outside the home or business. By building Fon technology into their CPEs (existing DSL or cable modems with Wi-Fi), they create a Fon Spot and give subscribers access to Fon global Wi-Fi network by default. Under this approach, there is no need for a second router or special configuration by users. Integration is fast and easy.

Headquartered in Brussels, Belgacom is the leading telecommunication operator in Belgium, with 45% of the country’s fixed line market. The company’s focus is to continuously invest in cutting edge technology, so it can offer its private and professional customers telephony (fixed and mobile), Internet and television services around the clock, irrespective of location or device. Belgacom’s goal is to anticipate future needs of customers; staying ahead of the curve by always adopting the best telecommunication technology available.

Belgium has one of the world’s most competitive telecommunications markets. With high Internet penetration and usage of mobile broadband throughout, deploying a Wi-Fi community was the obvious strategic choice for Belgacom. To be able to continue to compete in this increasingly dynamic market, Belgacom had to find an attractive and CAPEX-light Wi-Fi service that would not only attract more customers, but would ensure that existing customers would remain loyal to the telecommunication companies. It was also important for Belgacom to be able to bring its services to market before the competition. With an increasing amount of connected devices and customers expecting connectivity wherever they go, it became clear to Belgacom that providing customers with Internet access wherever they go could give Belgacom the competitive edge it was looking for.

In November 2011, Belgacom launched a partnership with Fon to create Belgium’s largest Wi-Fi network, giving its customers ubiquitous access throughout the country.

To achieve this, Fon implemented its signal-splitting technology right into Belgacom’s wireless modem, the B-box. This allows Belgacom customers to broadcast two Wi-Fi signals: a private one, which is for their household only; and a public one shared with all other sharing Belgacom customers and Fon members. This allowed Belgacom to quickly create a large Wi-Fi network with hundreds of thousands of users. A simple registration process gives Belgacom customers access to Fon’s entire global Wi-Fi network.

Today, Belgacom has over 600,000 hotspots all over Belgium. This means that thanks to its partnership with Fon, Belgacom’s customers are always close to an Internet connection and can enjoy their Wi-Fi-enabled devices to the fullest wherever they go.

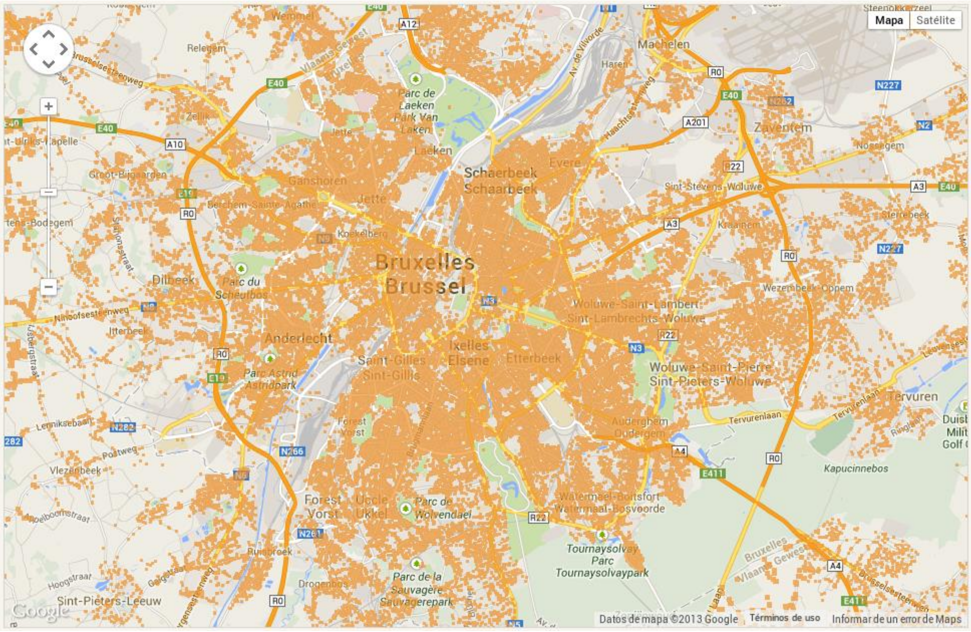


Figure18 Belgacom Fon spots in Brussels area.

In addition to Wi-Fi access in Belgium, Belgacom Internet customers have access to all of Fon's millions of hotspots around the world, allowing them to experience their fixed Internet experience from anywhere in the world.

6.3 Case Study#3 (BT)

BT Wi-Fi is the UK's largest Wi-Fi network, with more than five million hotspots across the UK and Ireland at high street brands, hotels, cafes, transport hubs, thousands of independent businesses, and homes.

The Community Wi-Fi part of this network is a key part of BT's overall Wi-Fi strategy. It is composed of both residential and business hubs which broadcast public SSIDs as part of the auto opt-in service that BT provides to its broadband customers.

A single BT platform operates the whole Wi-Fi network; however several vendors produce the end routers which are installed. The service is completely self contained, in that within the hubs all traffic is both logically and physically separated from the 'customers' traffic. This is done for several important reasons, firstly to provide separation on a service level from the customer, secondly to make sure that the customer is not charged for any public traffic on their provided broadband.

BT entered early into the hub Wi-Fi marketplace and the fully managed service with a healthy growth in deployments, functionality, and throughput. Last year BT launched the Hub 5, which is now the standard wireless router across both consumer and business broadband and fiber products. It is a feature-rich dual-frequency 802.11ac compliant unit which features many BT innovations to work with the growing customer base and the rollout of fiber into these locations

6.4 Case Study#4 (Portugal Telecom)

6.4.1 Portugal Telecom MEO Wi-Fi Hotspot

Portugal Telecom (PT) 3Play service is called MEO and started in 2007 with services based on DSL providing IPTV services, VoIP and high speed internet (HSI). In 2009 MEO deployed a FTTH network to one million houses. In January 2013, PT presented a new MEO service including a full rebranding and the launch of the first quadruple play offer, a truly fixed-mobile convergent service, including TV, internet, landline telephone and mobile, named M4O.

MEO Wi-Fi service brings wireless Internet access to MEO customers in more than 300,000 hotspots in Portugal and millions of partnerships around the world.

MEO Wi-Fi Premium Hotspots

Available at public spaces, hotels, restaurants, shopping centers, post offices, gas stations, stadiums, conference centers among many others.

MEO Wi-Fi Community Hotspots

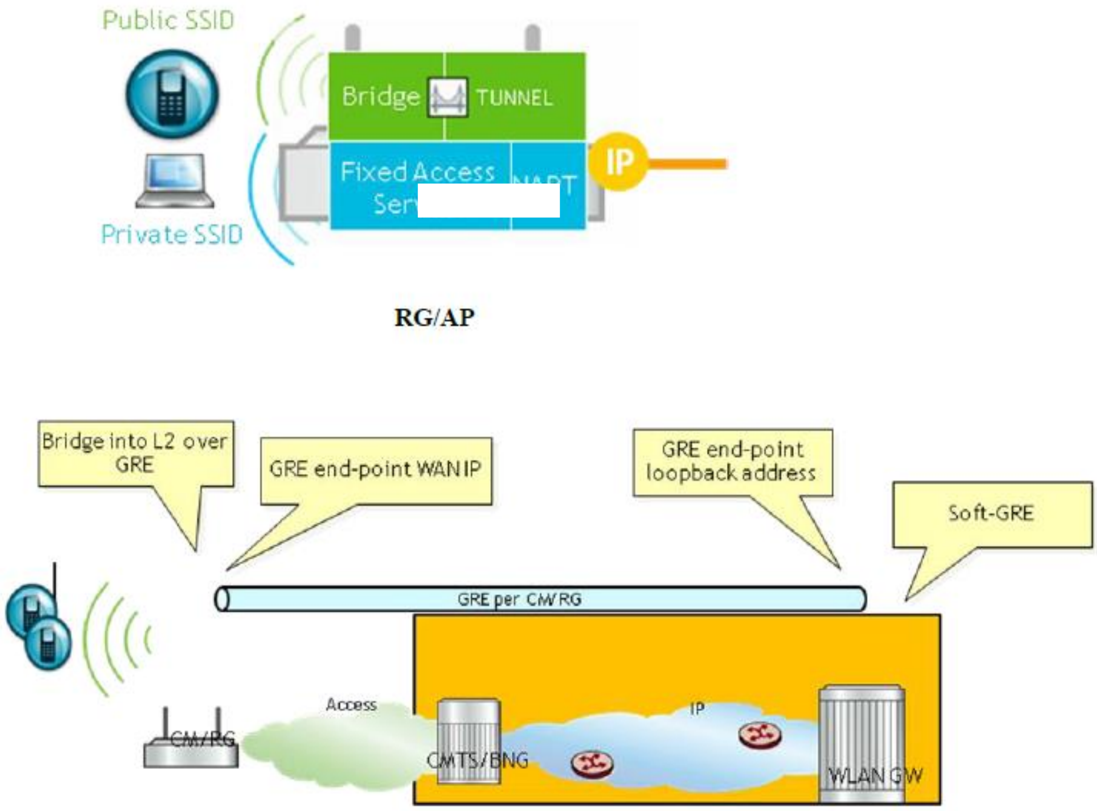
When sharing their MEO hotspot with other customers, MEO customers gain access to the whole hotspots base. The community is currently based on Fiber MEO customers only.

6.4.2 Portugal Telecom Wi-Fi Hotspot

Due to the wide number of customers, Portugal Telecom Wi-Fi community hotspots feature is highly valued. Using the CPEs that currently provide IPTV service, VoIP, and HIS, Portugal Telecom was able to deliver a community-based Wi-Fi hotspot.

Portugal Telecom MEO CPEs are basically MAGs with integrated DSL modem and Gigabit WAN port connecting to DSL or optical network terminator (ONT). On the wireless side they have an 802.11g/n radio connection supporting both private and public SSIDs.

MEO Wi-Fi Community Hotspots are available to all customers, but are enabled only for Fiber MEO customers, ensuring that customers' quality of experience is not impacted.



RG/AP

Figure 6:1 Community Wi-Fi Reference Architecture (Portugal Telecom)

Portugal Telecom's CPEs uses GRE tunnels to bridge the traffic over the FTTH network to the WLAN gateway core. Using the WLAN gateway core allows the CPE to work without the full load of this service over it and it is not affected by the requirements of the MEO Wi-Fi service, such as the authentication process, MEO Portal, accounting and others.

The deployment and provisioning of MEO Wi-Fi Community Hotspot consists basically on the configuration of the GRE tunnel and the added Wi-Fi network with 'MEO-Wi-Fi' SSID. All the traffic of this hotspot goes through the GRE tunnel established between Portugal Telecom´s WLAN gateway and the new access point.

6.4.3 Key Issues & Challenges – Scale:

6.4.3.1 Capacity per hotspot

Depending on the nearby area, (urban/rural) Wi-Fi community hotspots may be overloaded with multiple connected devices. Bearing this in mind, in order to guarantee a good Wi-Fi experience for Community Hotspot users and the customer devices, Portugal Telecom limited the number of hosts a hotspot can address. Limiting the number of hosts connected to each MEO Wi-Fi Community hotspot will ensure that the customer´s private wireless spectrum is not fully loaded by hotspot traffic and that each hotspot user will also have a good Wi-Fi user experience.

6.4.3.2 Operations and Management

Until a standard for these types of Community Wi-Fi Hotspots solutions is achieved, the need for support from the CPE vendors is mandatory.

The lack of normalization on these implementations causes an increased work to fully design, deploy and manage customizations to each of the CPEs Portugal Telecom provides for MEO service, mainly on:

Scripts customization for the deployment of CPEs Community Wi-Fi hotspot configuration (GRE tunnel set-up, public SSID, etc)

Added tests for Portugal Telecom´s CPE Technical Acceptance in new CPE models regarding the Community Wi-Fi hotspot service

Added operations to manage or change any Community Wi-Fi hotspot configuration on the CPEs

Management protocols such as TR-069 might be a solution to help manage these networks and a must to fully develop and evolve the Community Wi-Fi service.

6.4.3.3 QoS and Prioritization

As mentioned in this work, the shared radio interface and packet QoS is a topic where so much work has to be fulfilled.

Portugal Telecom´s Community Wi-Fi hotspot implementation uses the same radio interface as the customers' private Wi-Fi network causing the customer´s private Wi-Fi network to be on the same channel and with the same range than the Community Wi-Fi hotspot.

Since hotspot users and customer´s devices will use the same channel and there is no QoS and prioritization at the physical RF level, the customer might notice a decrease on the bandwidth offered to his devices, because they will all operate in the same radio channel.

This is aggravated if the customer lives in dense residential areas, where the number of both Wi-Fi private networks and hotspots coexists increasing the number of devices using the same radio channel.

6.4.3.4 Community Hotspot User Experience

As mentioned in section 7.4.3.1 because Portugal Telecom needs to guarantee a minimal QoS for hotspot users and the customer's private Wi-Fi network, the number of users a hotspot can address has been limited. This means that if a hotspot is full, the next user will not be able to connect to the hotspot. A good improvement to customer experience would be the development of a way to inform this user that the hotspot is full and that it is not possible to connect at that moment.

6.4.3.5 Wi-Fi hotspots vs. Wi-Fi Private networks

Since the radio interface on the CPE is the same for the customer Wi-Fi network and Community Wi-Fi hotspot users, when a customer has both networks authorized on his devices, sometimes they connect to the hotspot instead of the customers Wi-Fi network.

This also depends on the devices and OS', but some solutions could be evaluated to ensure that whenever clients have good signal from private Wi-Fi networks, they should preferably connect to it, instead of connecting to the public Wi-Fi network.

To address this, Portugal Telecom's solution was to develop an Android and iOS app to manage the wireless networks on these devices, ensuring the user to connect preferably to private networks over the MEO Hotspots whenever possible and to login automatically on the hotspot, providing the customer a seamless experience between private and public wireless networks.

References

1 Wi-Fi Requirements for Cable Modem Gateways, WR-SP-WiFi-GW-I03-140311, March 11, 2014, Cable Television Laboratories, Inc.

2 IPv6 for Carrier Wi-Fi: Wi-Fi Operator Guidelines, February 10, 2014, Wireless Broadband Alliance.

3 eDOCSIS™ Specification, CM-SP-eDOCSIS-I22-110623, June 23, 2011, Cable Television Laboratories, Inc.

4 DOCSIS 3.0, MAC and Upper Layer Protocols Interface Specification, CM-SP-MULPIv3.0-I24-140403, Cable Television Laboratories, Inc.

5 M. Heusse, F. Rousseau, G. Berger-Sabbatel, and A. Duda. Performance anomaly of 802.11b. In *INFOCOM*, April 2003.

6 Tinnirello, Ilenia, Giuseppe Bianchi, and Luca Scalia. Performance evaluation of differentiated access mechanisms effectiveness in 802.11 networks. In *GLOBECOM* '04. IEEE. Vol. 5. IEEE, 2004.

7 Kumar, Anurag, et al. New insights from a fixed point analysis of single cell IEEE 802.11 WLANs. In *INFOCOM* 2005. Vol. 3. IEEE, 2005.

8 Heusse, Martin, et al. Idle sense: an optimal access method for high throughput and fairness in rate diverse wireless LANs. In *ACM SIGCOMM*. Vol. 35. No. 4. ACM, 2005.

9 Carrier Wi-Fi Guidelines, February 7, 2014, Wireless Broadband Alliance.

10 Wi-Fi Provisioning Framework Specification, WR-SP-WiFi-MGMT-I04-140311, March 11, 2014, Cable Television Laboratories, Inc.

Annex A - Management Requirements

The following table provides a list of management functions, via TR-069 and/or SNMP, that operators deploying community Wi-Fi would like to see Community Wi-Fi APs to support.

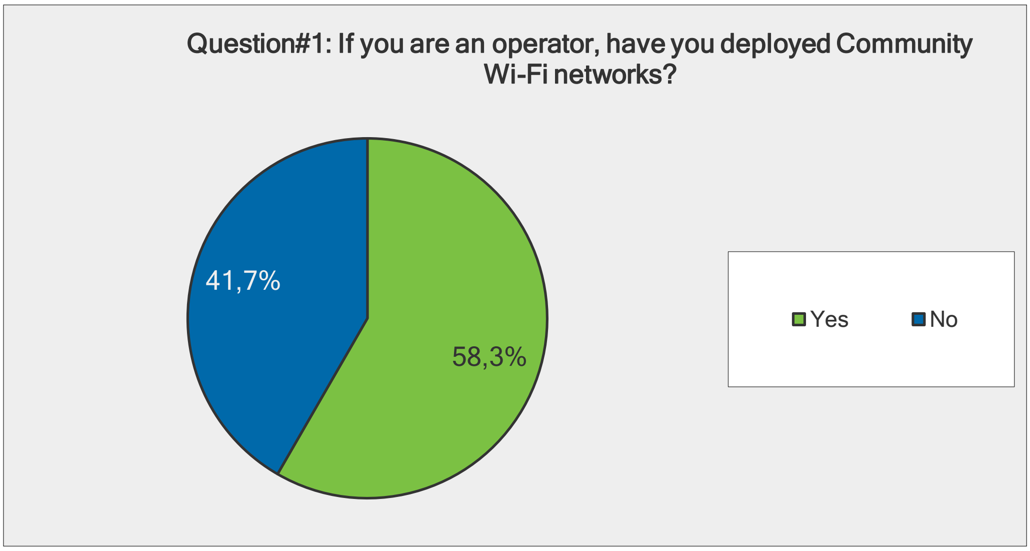
Device/Scope	Requirement /Function
Internet GW Device	Reset GW component(s) to factory default setting
	Change and apply management settings to either an individual component or all GW components
	Report WAN and LAN facing IP Addresses and interface (e.g., ifIndex)
SSID (general)	Access mode (e.g., allow/disallow device association based on MAC Address)
	MSS clamping
	Enable/disable a BSS
	Report BSSID (i.e., MAC)
	Set and report maximum sessions/connections on a single BSS
	Provision SSIDs as 'private' or 'public'
SSID/AP (Hotspot2.0)	Enable/disable Hotspot2.0
	EAP method
	Icon location of binary for storage/download
	Generic advertisement service (GAS) settings
	Roaming consortium information
	HESSID
	Access network query protocol (ANQP) settings
	IP address type
	NAI realms
	3GPP cellular network
	Domain name
	Country
	HotSpotCapabilityList
	Operator friendly name
	Online sign up
	Enable downstream forwarding of group-addressed frames (DGAF)
	Enable P2P cross-connect
	QoS mapping for interworking services
	Enable additional step required for access (ASRA)
	Enable management frame protection
	Enable BSS transition management
Tunneling (e.g. L2oGRE)	Enable/disable tunnel
	Primary tunnel endpoint address type
	Primary tunnel endpoint address
	Secondary tunnel endpoint address (failover)
	Enable/disable fragmentation
	Enable/disable failover
	Enable/disable tunnel 'keepalive'
	Keepalive interval
	Keepalive retries on timeouts
	Reset tunnel
	Primary tunnel status

Device/Scope	Requirement /Function
	Secondary tunnel status
	Enable/disable insertion of DHCP options for associated device traffic to be tunneled. (e.g., MAC address and SSID)
	Enable/disable VLAN tagging frames before placing on tunnel
Packet Classification	Classification is utilized to determine what policies are applied to upstream and downstream frames before placing on or removing from a tunnel
	SSID/IfIndex
	Source MAC
	Source MAC mask
	Destination MAC
	Destination MAC mask
	Address type
	Source IP address
	Source IP prefix length
	Destination IP address
	Destination IP prefix length
	Internet protocol
	Source port number start
	Source port number end
	Destination port number start
	Destination port number end
Policies	Add VLAN tag
	DSCP marking
	Tunnel or drop frame

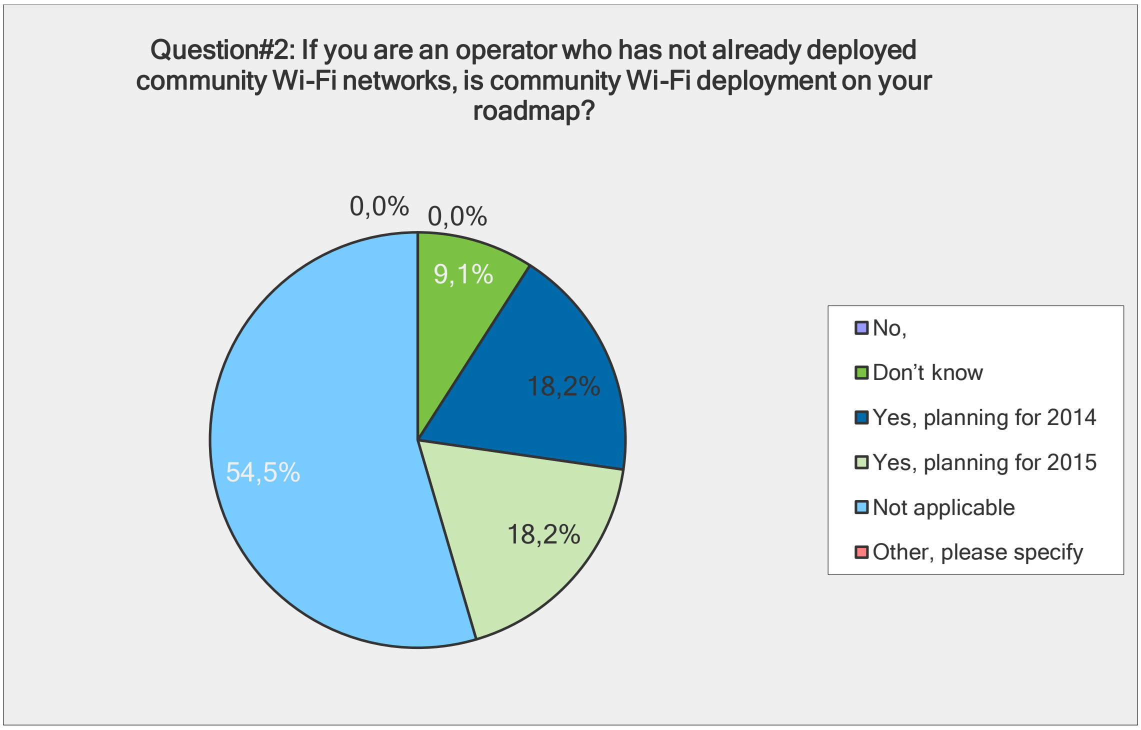
Annex B - Survey Results

In order to obtain a baseline of current Community Wi-Fi deployments, a survey was sent out to various MSOs and vendors. The survey got a total of 17 responses. 75% were from operators and 25% from vendors. The questions used in the survey are shown below, followed by the responses.

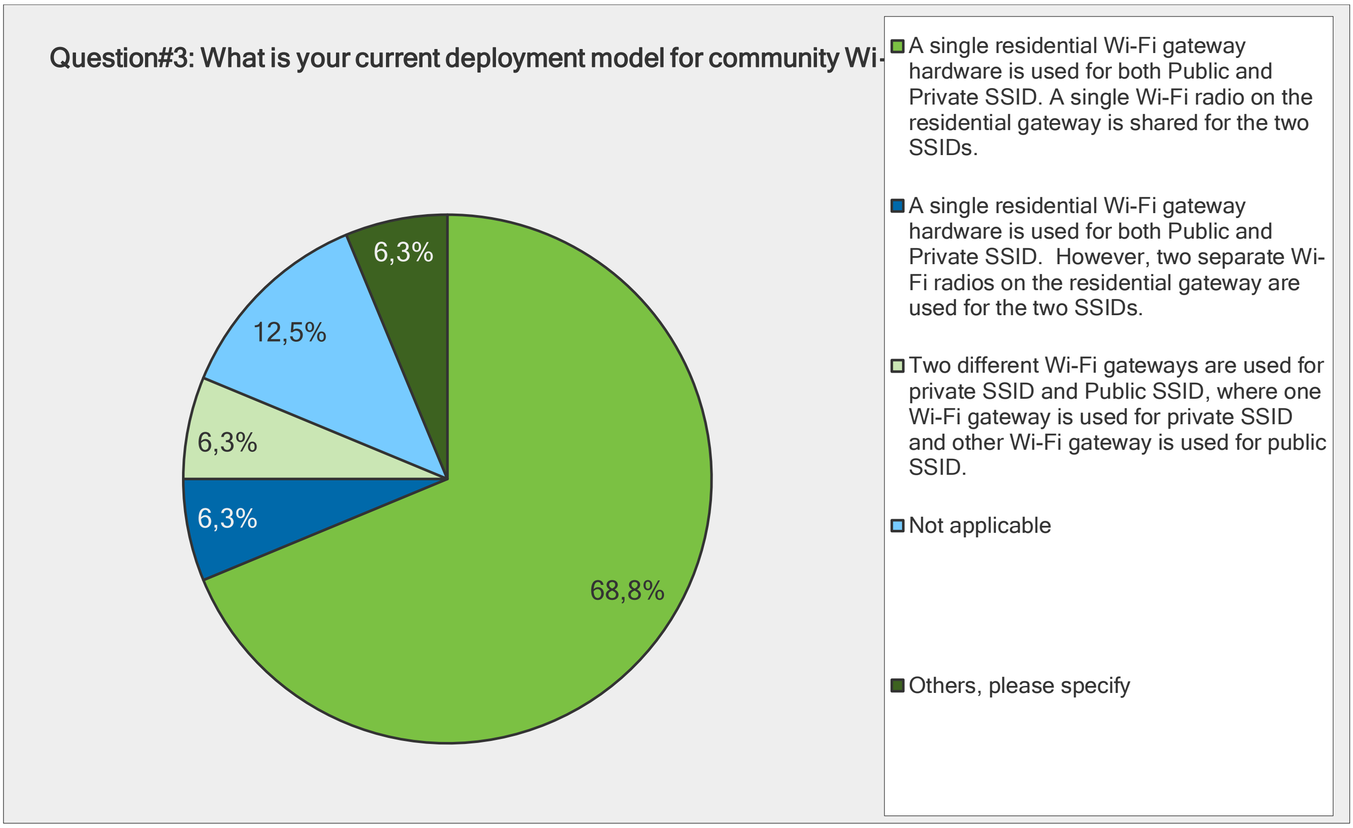
Question#1: If you are an operator, have you deployed Community Wi-Fi networks?



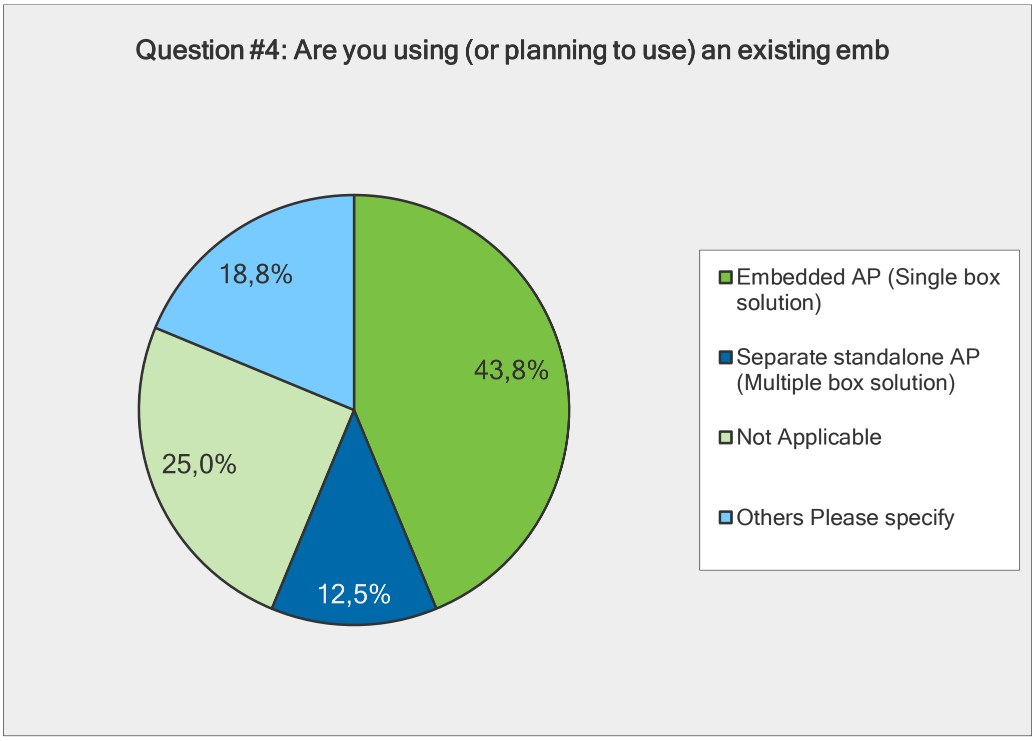
Question#2: If you are an operator who has not already deployed Community Wi-Fi networks, is Community Wi-Fi deployment on your roadmap?



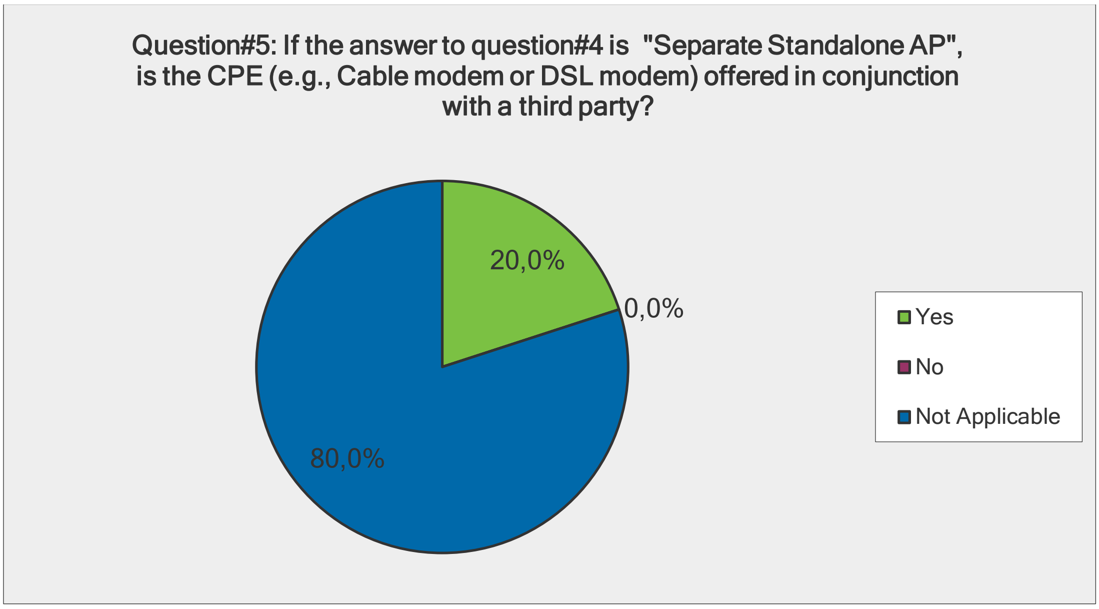
Question#3: What is your current deployment model for Community Wi-Fi?



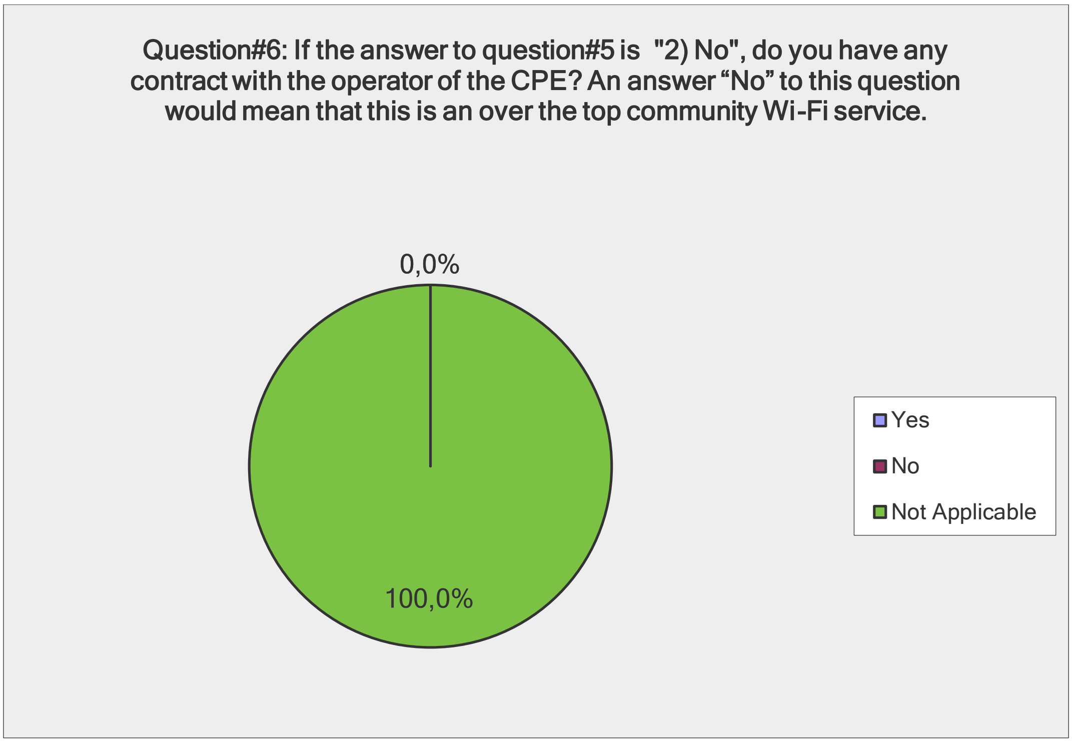
Question #4: Are you using (or planning to use) an existing embedded Wi-Fi AP or a separate standalone Wi-Fi AP to deploy Community Wi-Fi? This could be defined as either a single or multiple box solution. An embedded AP would be a single piece of hardware that could manage both the Wi-Fi and broadband connectivity.



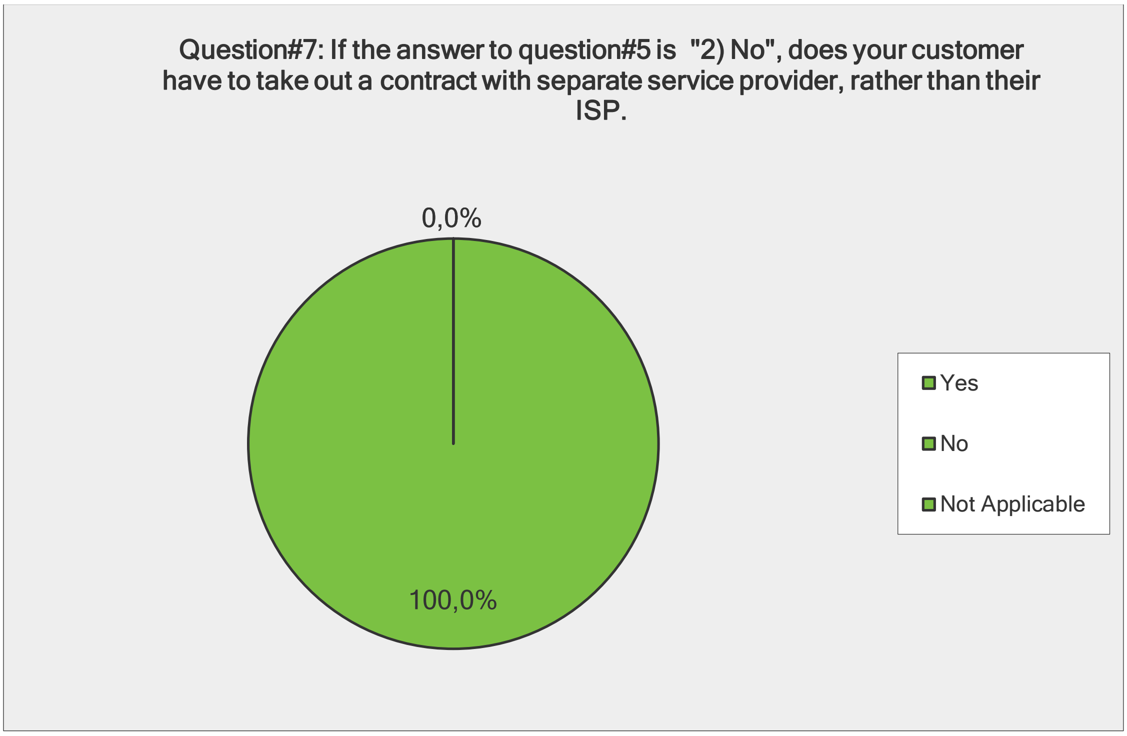
Question#5: If the answer to question#4 is "Separate Standalone AP", is the CPE (e.g., cable modem or DSL modem) offered in conjunction with a third party?



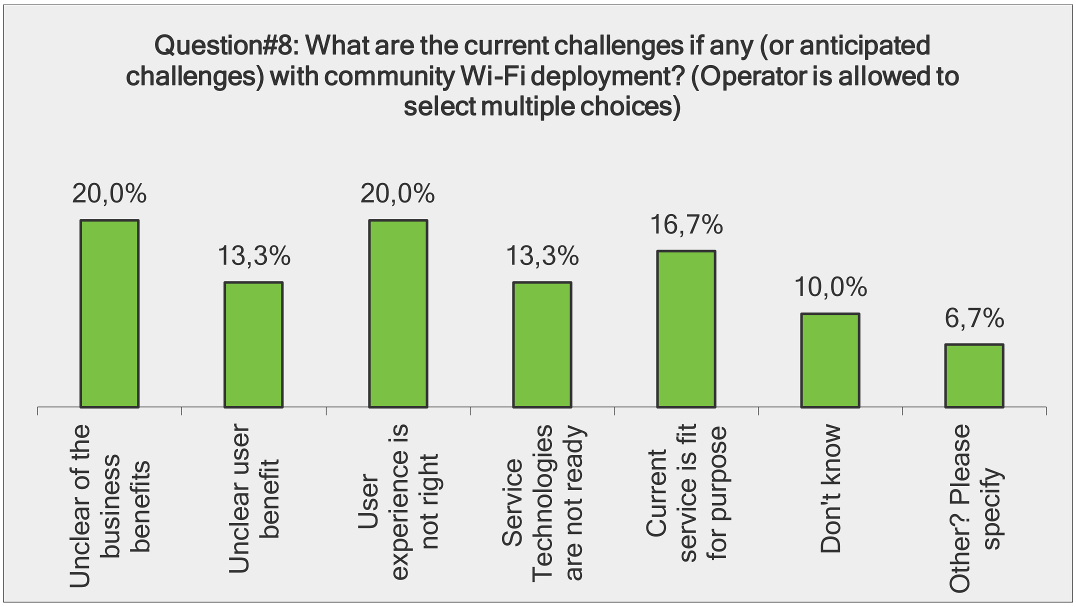
Question#6: If the answer to question#5 is "2) No", do you have any contract with the operator of the CPE? An answer “No” to this question would mean that this is an over the top Community Wi-Fi service.



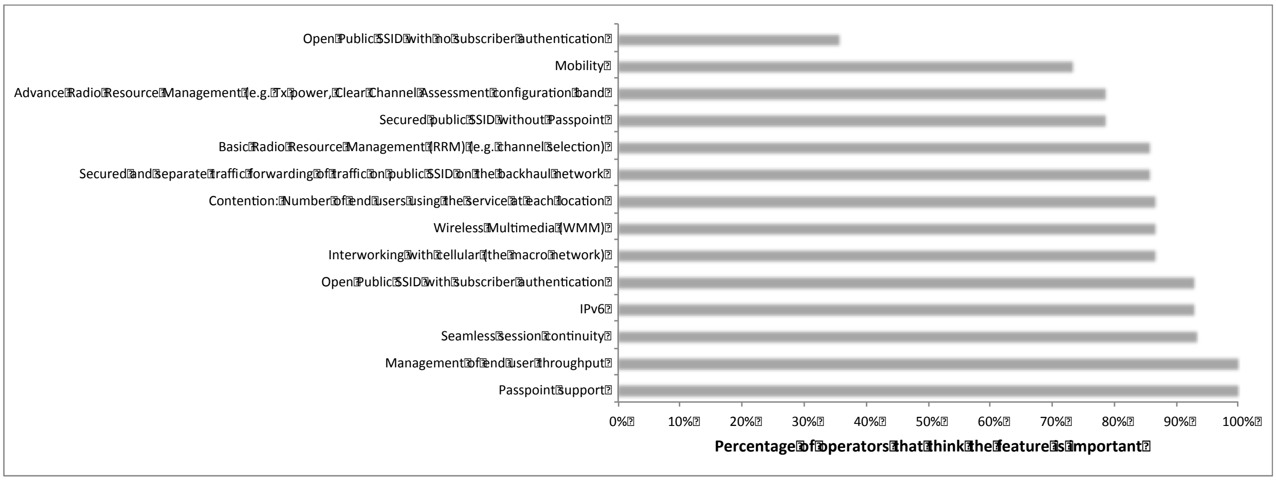
Question#7: If the answer to question#5 is "2) No", does your customer have to take out a contract with separate service provider, rather than their ISP?



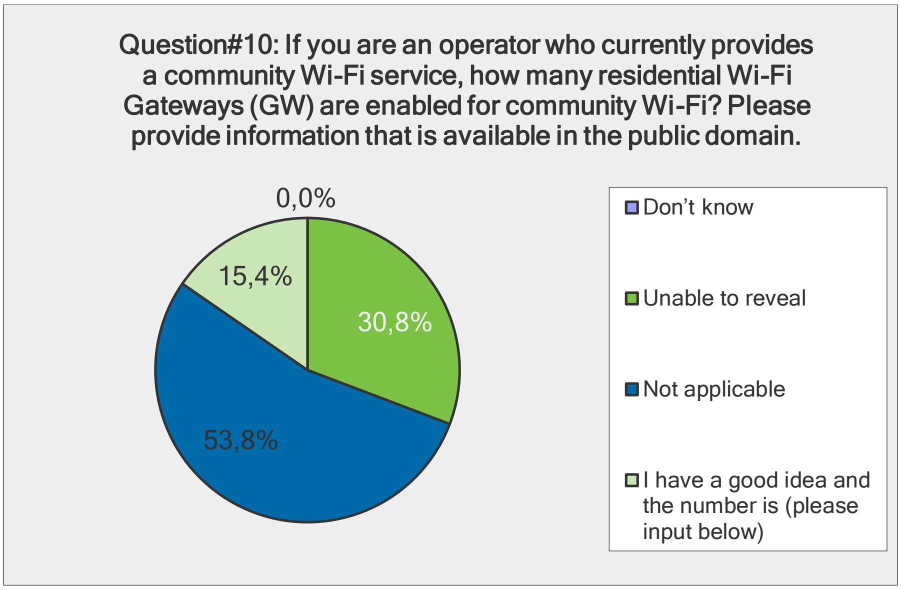
Question#8: What are the current challenges if any (or anticipated challenges) with Community Wi-Fi deployment? (Operator is allowed to select multiple choices)



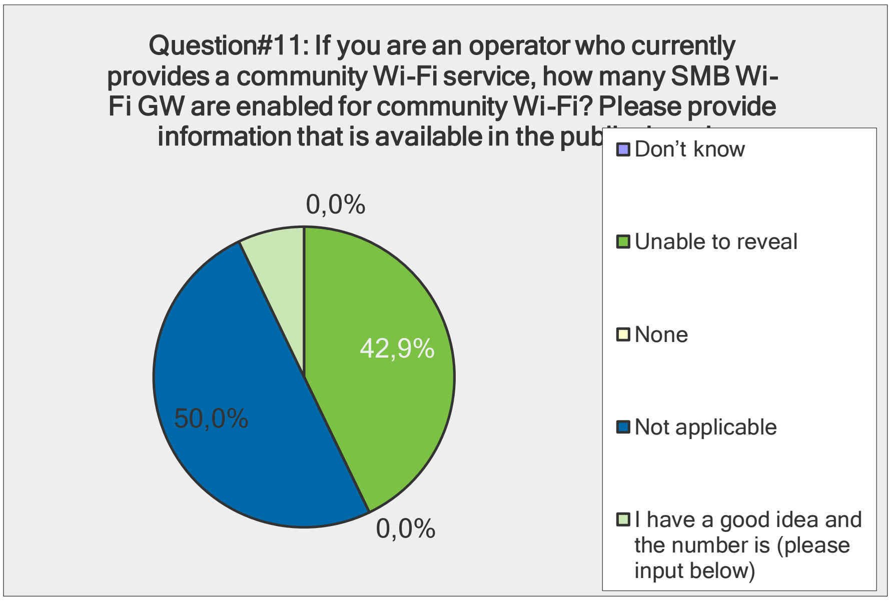
Question#9: What are the most important features that you would like to see in Community Wi-Fi products? Please also provide relative ranking for each of the below mentioned features whereas 15 represents the highest rank while 1 represents the lowest rank.



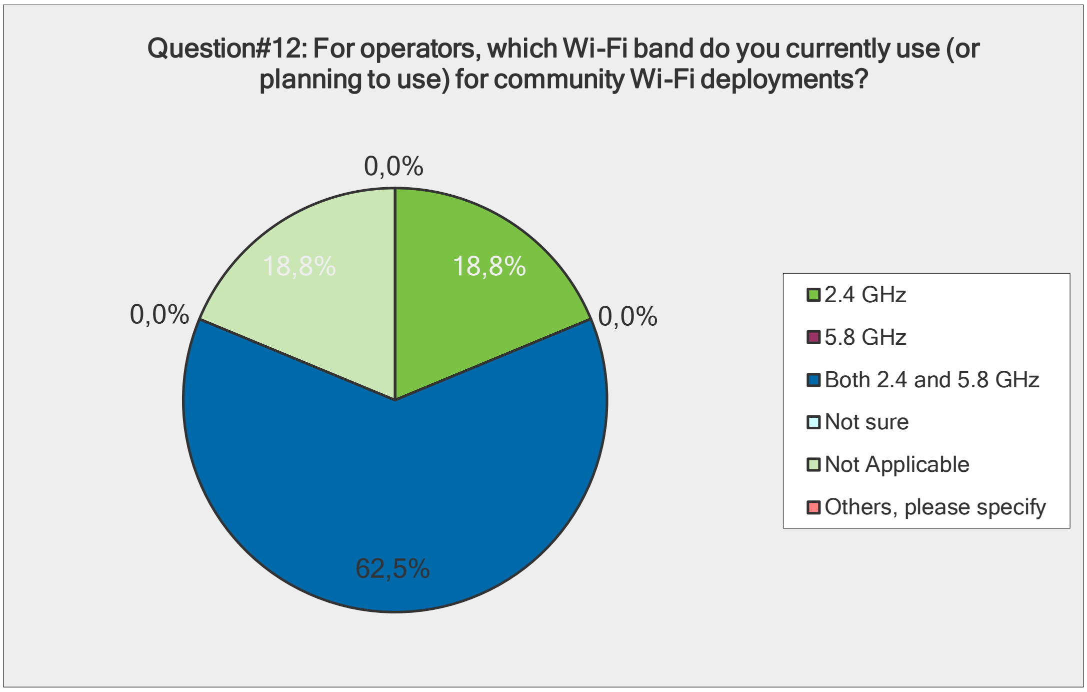
Question#10: If you are an operator who currently provides a Community Wi-Fi service, how many residential Wi-Fi gateways are enabled for Community Wi-Fi? Please provide information that is available in the public domain.



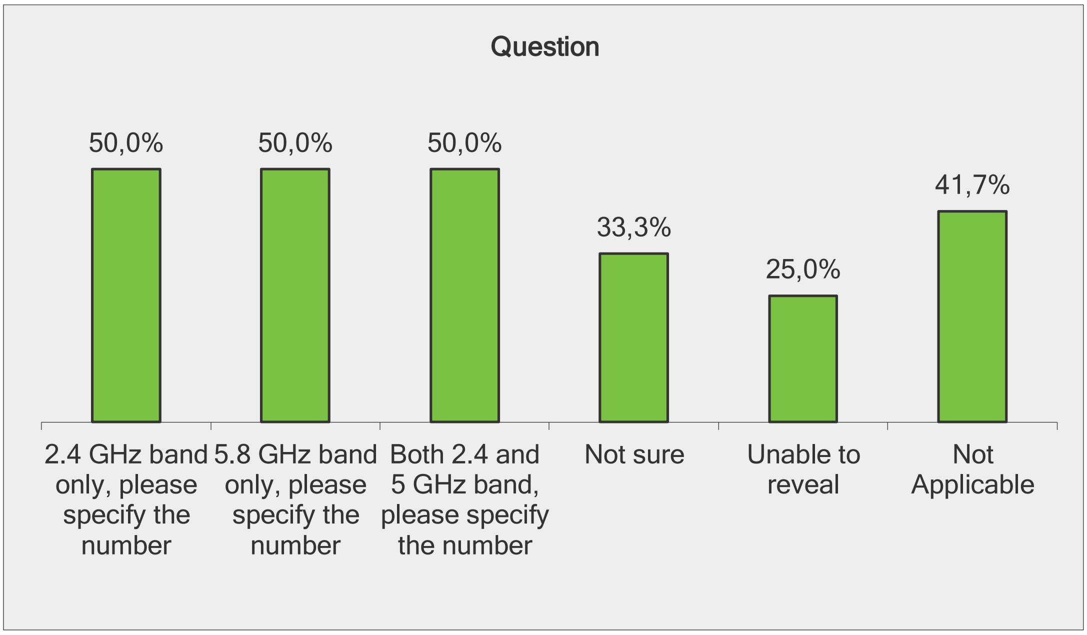
Question#11: If you are an operator who currently provides a Community Wi-Fi service, how many SMB Wi-Fi gateways are enabled for Community Wi-Fi? Please provide information that is available in the public domain



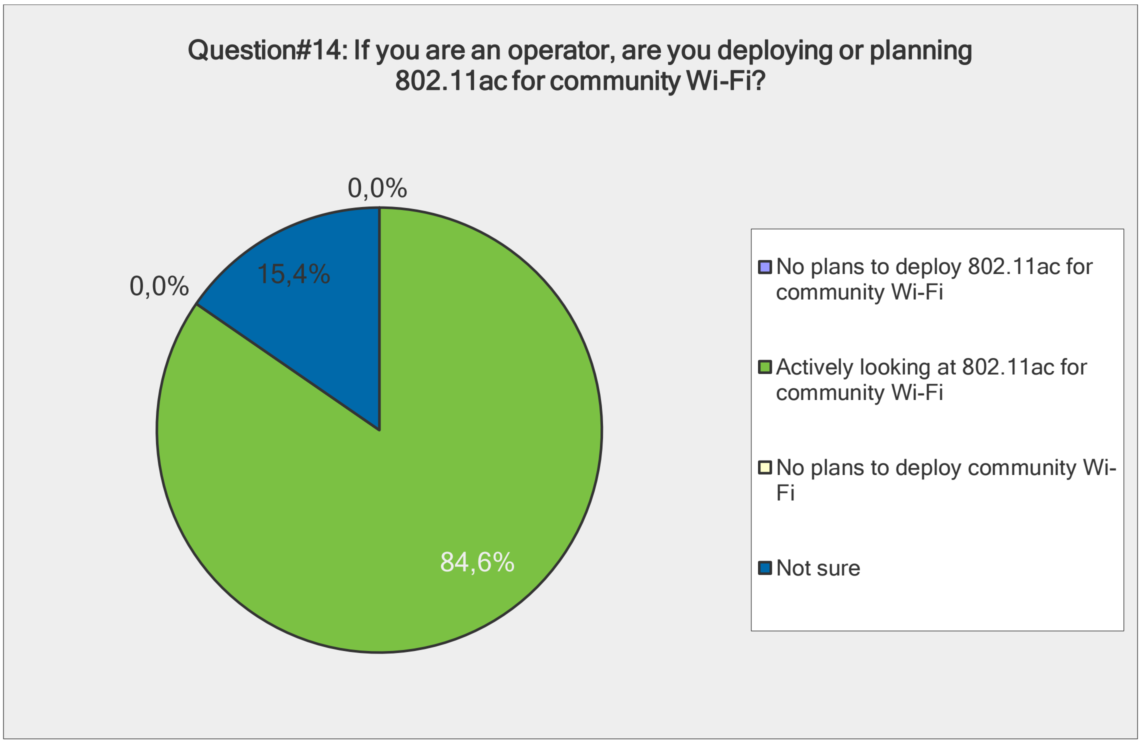
Question#12: For operators, which Wi-Fi band do you currently use (or planning to use) for Community Wi-Fi deployments?



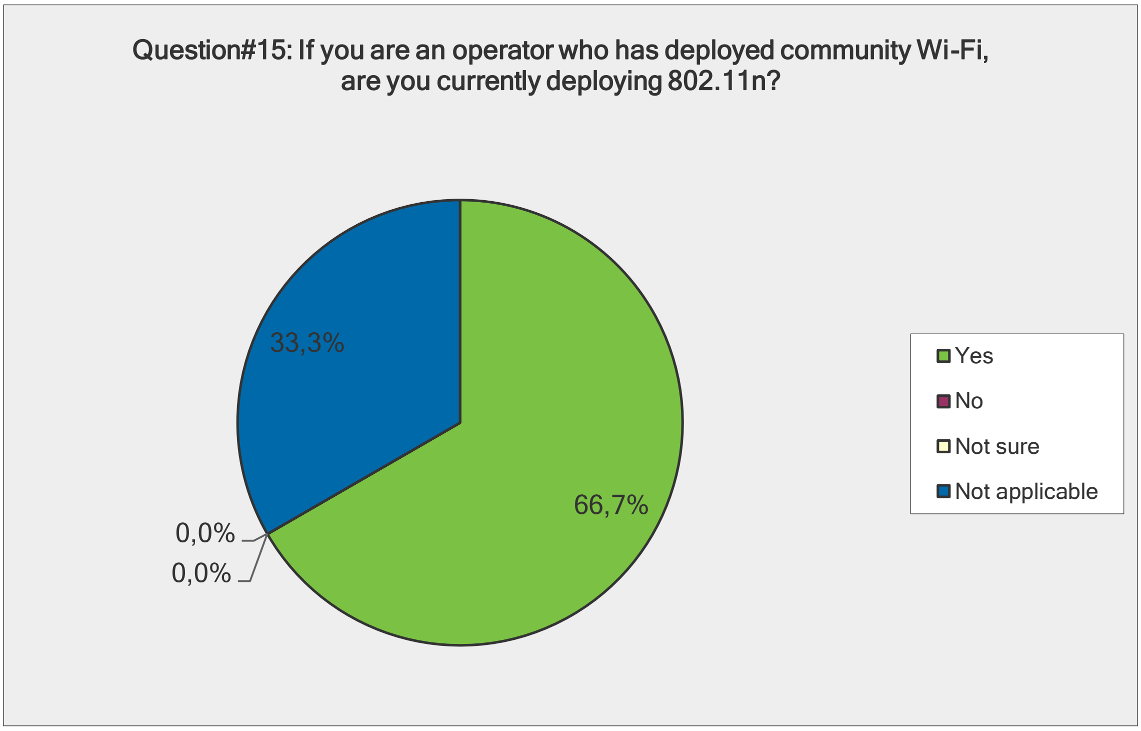
Question#13: If you are an operator with a current Community Wi-Fi deployment, what percentage of your current deployment supports the following?



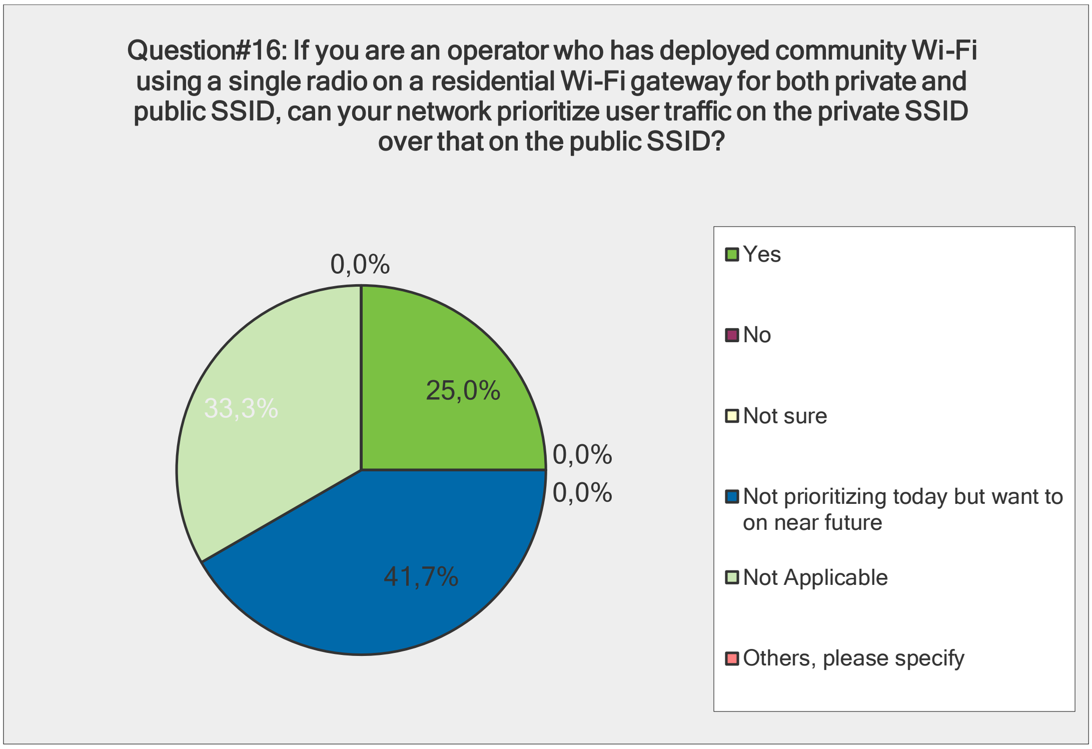
Question#14: If you are an operator, are you deploying or planning 802.11ac for Community Wi-Fi?



Question#15: If you are an operator who has deployed Community Wi-Fi, are you currently deploying 802.11n?



Question#16: If you are an operator who has deployed Community Wi-Fi using a single radio on a residential Wi-Fi gateway for both private and public SSID, can your network prioritize user traffic on the private SSID over that on the public SSID?

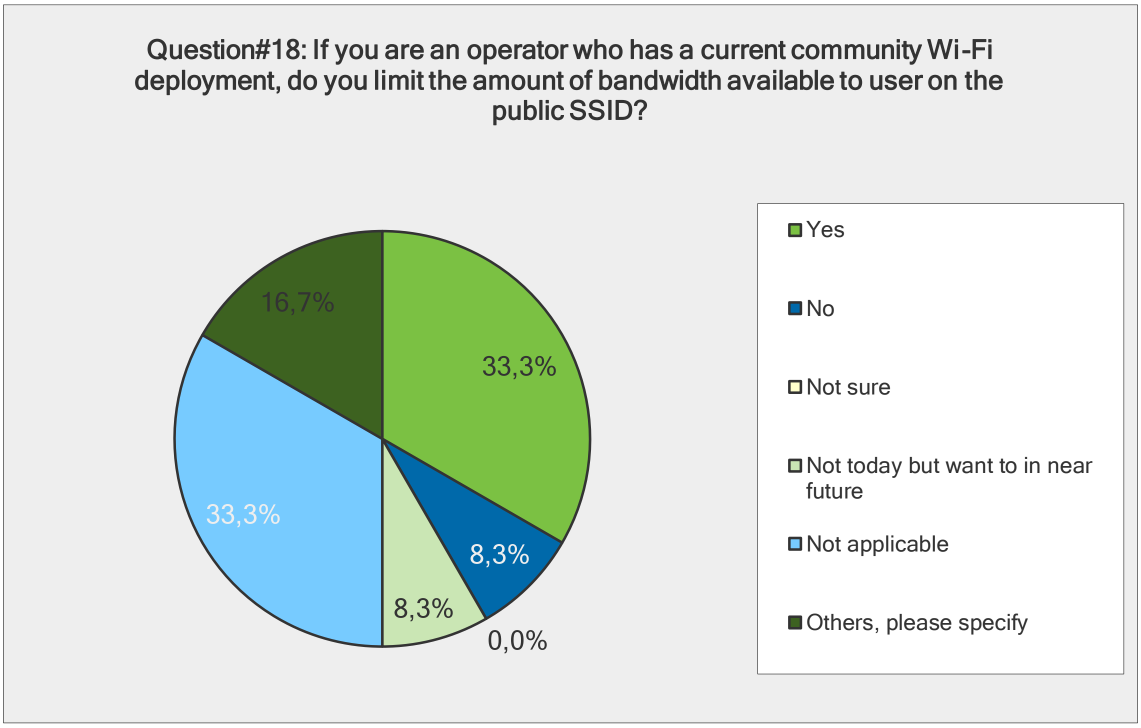


Question#17: if in current or planned Community Wi-Fi deployments user traffic on the private SSID is assigned a higher priority, or if you believe that this should be the deployment model, what technology and method should be used?

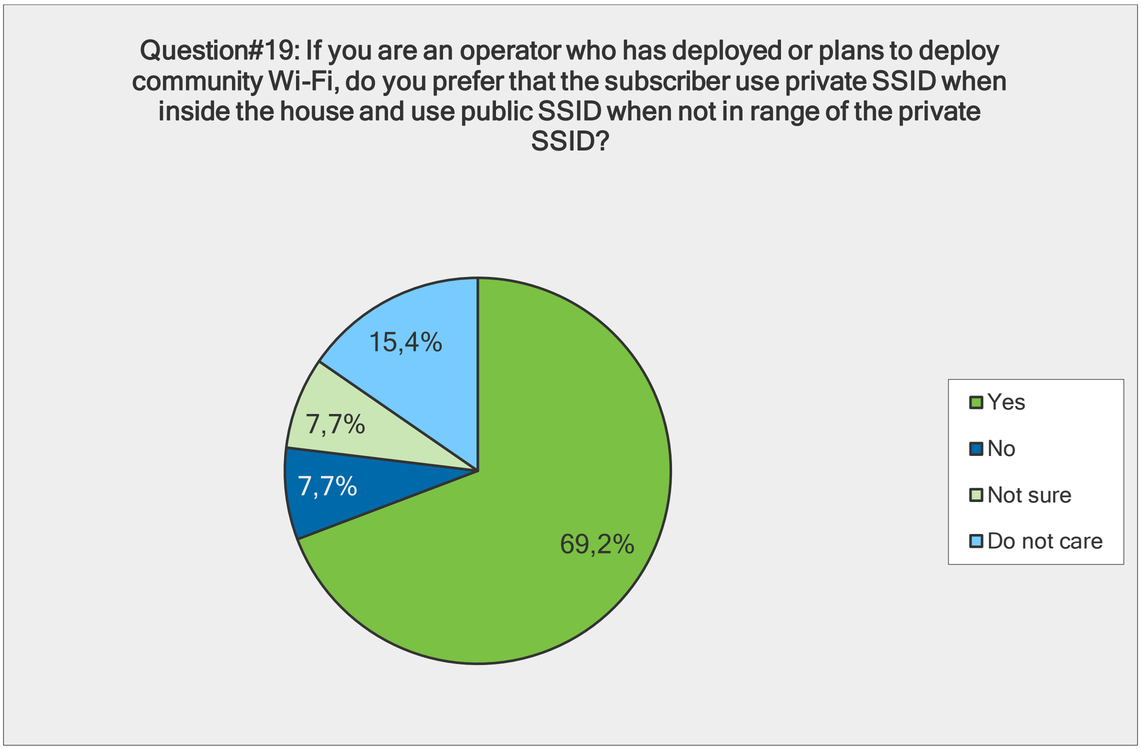
- IP QoS
- Traffic management should be deployed and also some technologies which can drive user to connect the particular SSID first will be useful
- Band Steering Airtime Fairness WMM Backhaul QoS at the WAG
- AP traffic policing on a per SSID basis can be used to limit rate and/or total traffic consumption (in either direction). Downlink traffic policing for the public SSID can also be performed by the core network
- Most AP vendors already support the ability to either prioritize one SSID over another or to rate limit the SSID or users on specific SSIDs. These policies can be managed using Radius attributes
- In order to facilitate the connection of portable devices, such as smartphone and tablets in the user's own house, the private SSID (i.e., those related to fixed line,) should take precedence and enable automatic selection of appropriate SSID in various scenarios (both private and public) for the usage of HS2.0 and ANDSF for 3GPP/WLAN smartphone. Furthermore for 3GPP-enabled devices additional technical solutions based on tighter integration between WLAN and 3GPP (e.g., RAN based integration) can provide additional benefits for ensuring a better user experience

- In the apple tech notes there is a precedent for priorities of private SSIDs being higher than all other SSIDs; refer to note http://support.apple.com/kb/HT5965
- An open standards-based solution
- Private SSID is provided with a higher priority using a variety of technologies
- Exploring strict queuing per SSID/VLAN. Interested in other approaches
- 802.11e, backhaul VLAN QoS priority

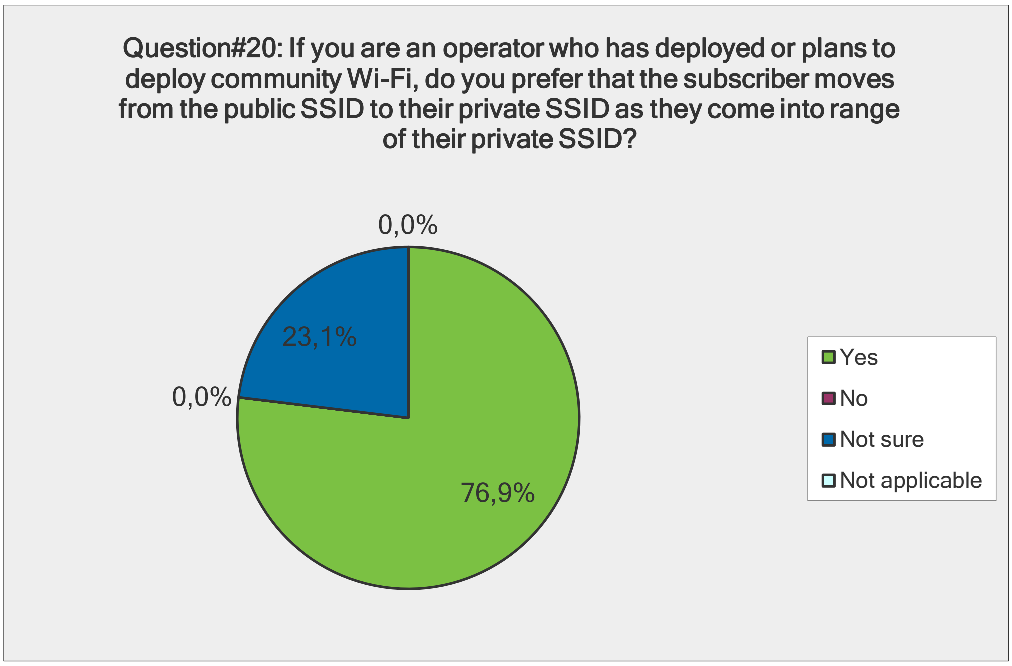
Question#18: If you are an operator who has a current Community Wi-Fi deployment, do you limit the amount of bandwidth available to user on the public SSID?



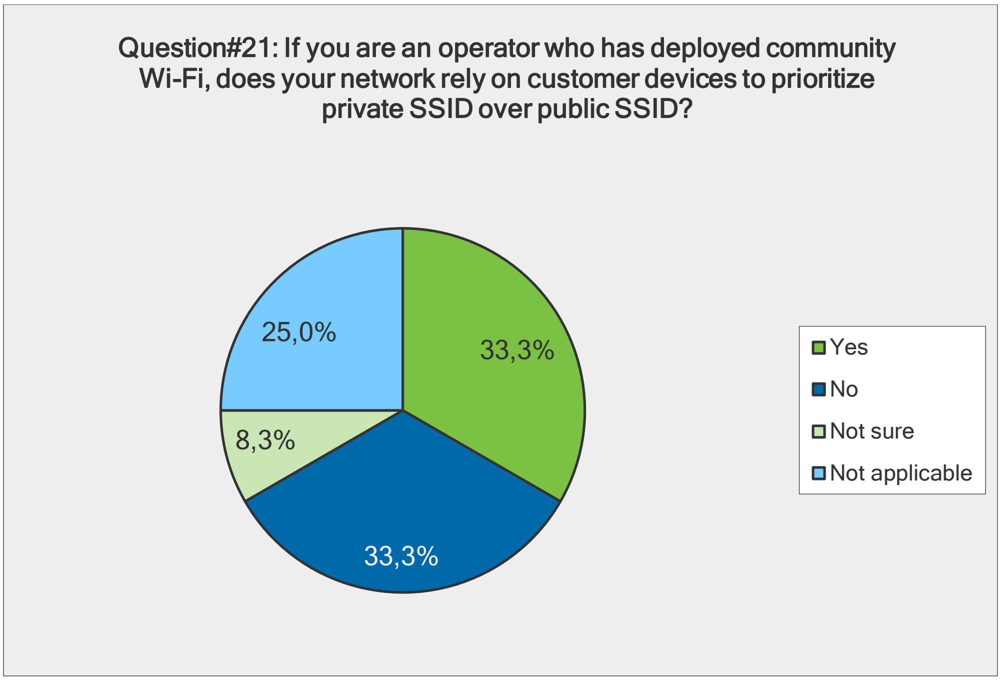
Question#19: If you are an operator who has deployed or plans to deploy Community Wi-Fi, do you prefer that the subscriber use private SSID when inside the house and use public SSID when not in range of the private SSID?



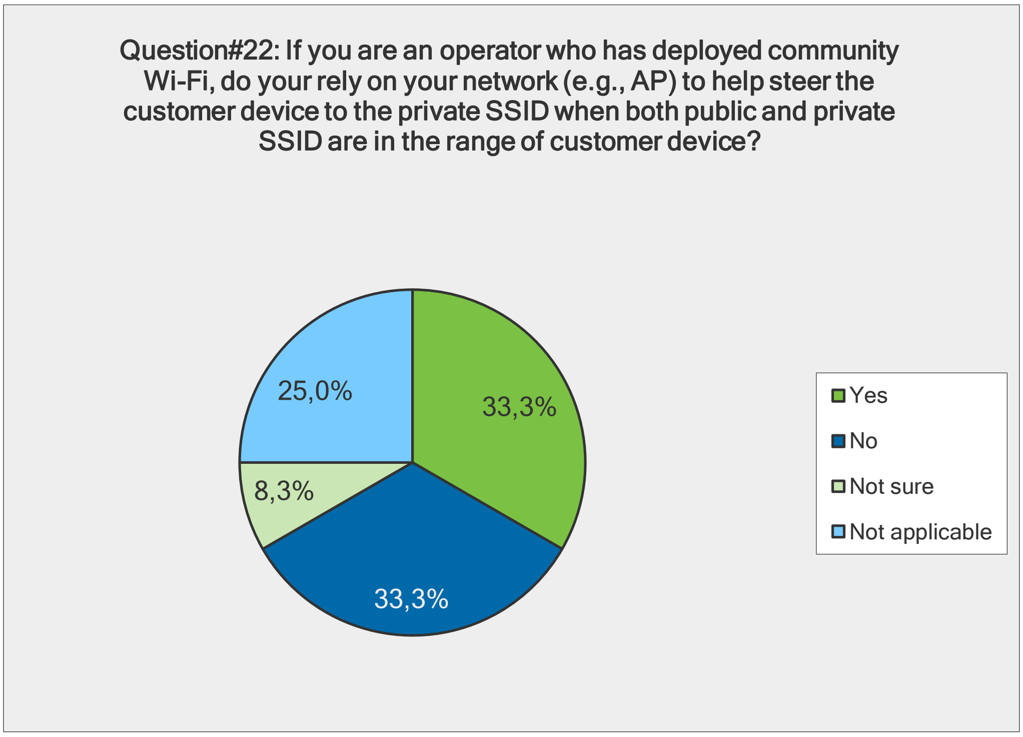
Question#20: If you are an operator who has deployed or plans to deploy Community Wi-Fi, do you prefer that the subscriber moves from the public SSID to their private SSID as they come into range of their private SSID?



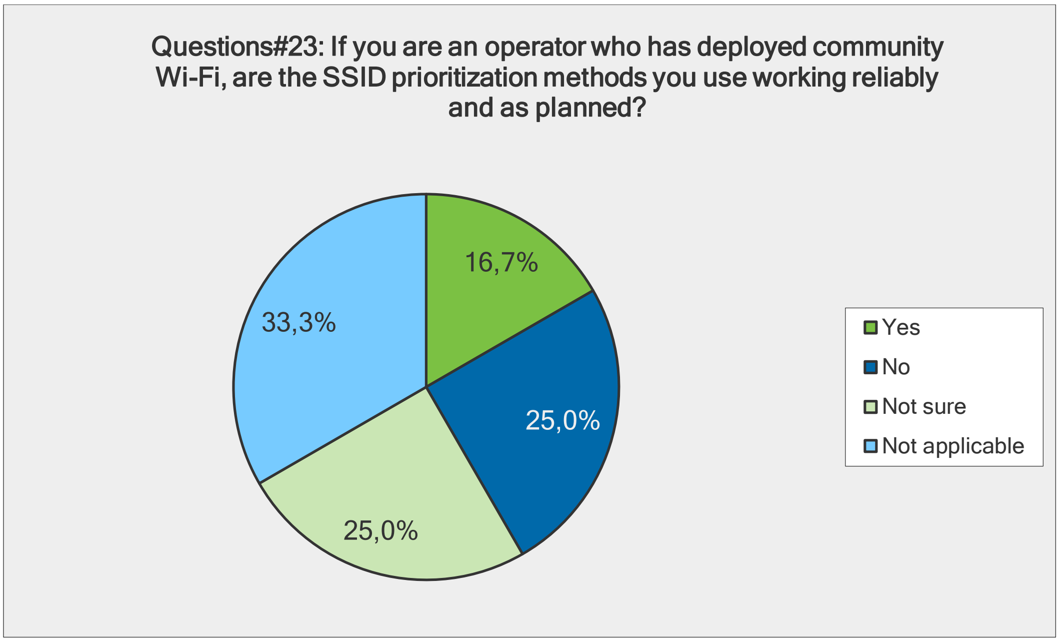
Question#21: If you are an operator who has deployed Community Wi-Fi, does your network rely on customer devices to prioritize private SSID over public SSID?



Question#22: If you are an operator who has deployed Community Wi-Fi, do you rely on your network (e.g., AP) to help steer the customer device to the private SSID when both public and private SSID are in the range of customer device?



Questions#23: If you are an operator who has deployed Community Wi-Fi, are the SSID prioritization methods you use working reliably and as planned?



Question#24: What method or technology is used or being considered to make sure that the customer device connects to the network using the correct Wi-Fi SSID?

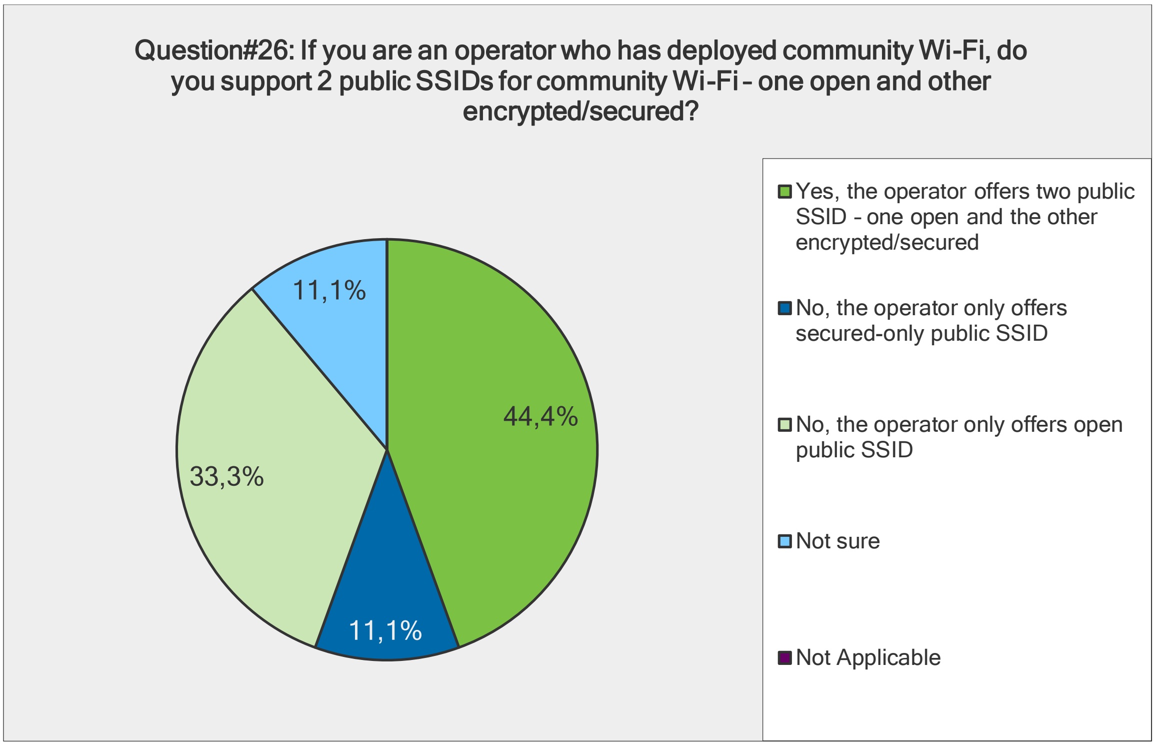
- Passpoint/NGH, Whitelist/Blacklist, WMM, Connection Managers
- Automatic network selection can be: pre provisioned by the user and/or operator on the device; delivered to the device by the operator using MDM; delivered more dynamically by the operator using e.g., 3GPP ANDSF policy automatic network discovery can be based on SSID, BSSID, HESSID; HS2.0 parameters
- Passpoint with EAP-TLS/TTLS/SIM/AKA.
- There are several mechanisms to support this. Most can happen as part of the authentication process
- The selection of correct SSID depends on the user needs, user subscription, operator business model (e.g., different price model, differentiation per services, etc.), network conditions, user device capability, etc. These broad and different conditions should be taken into consideration; hence different sets of features shall be combined to ensure that appropriate SSID is selected. The basic capabilities in device and network are Passpoint, ANDSF, and 3GPP indication for operator-integrated network. Based on the use cases, other features may be needed
- Passpoint Release 1 and Release 2 MSAP
- An open standards-based solution
- Variety of technologies based on the network

Question#25: What network element in operator's Community Wi-Fi network represents a bottleneck in the context of network scalability?

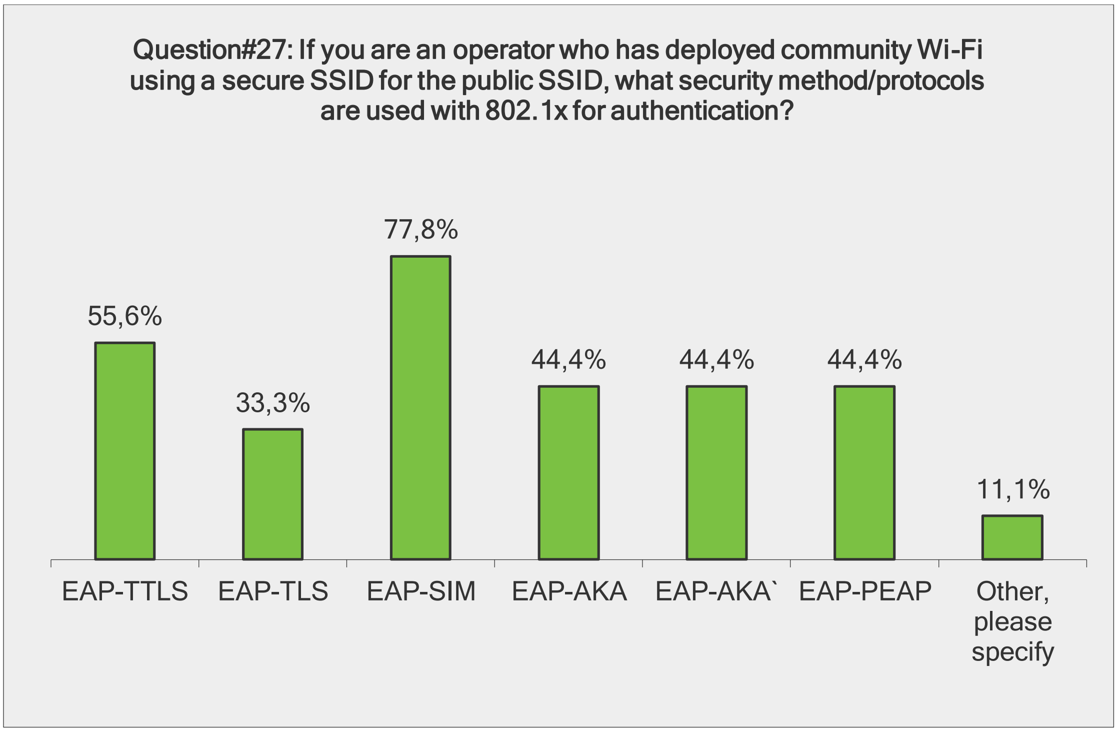
- Broadband backhaul

- Tunnel concentrator, WLAN GW, residential GW, shared Wi-Fi radio, Wi-Fi
- Too many RADIUS requests
- Depends upon implementation
- Tunnel termination g
- IP addresses
- DHCP server; tunnel management system

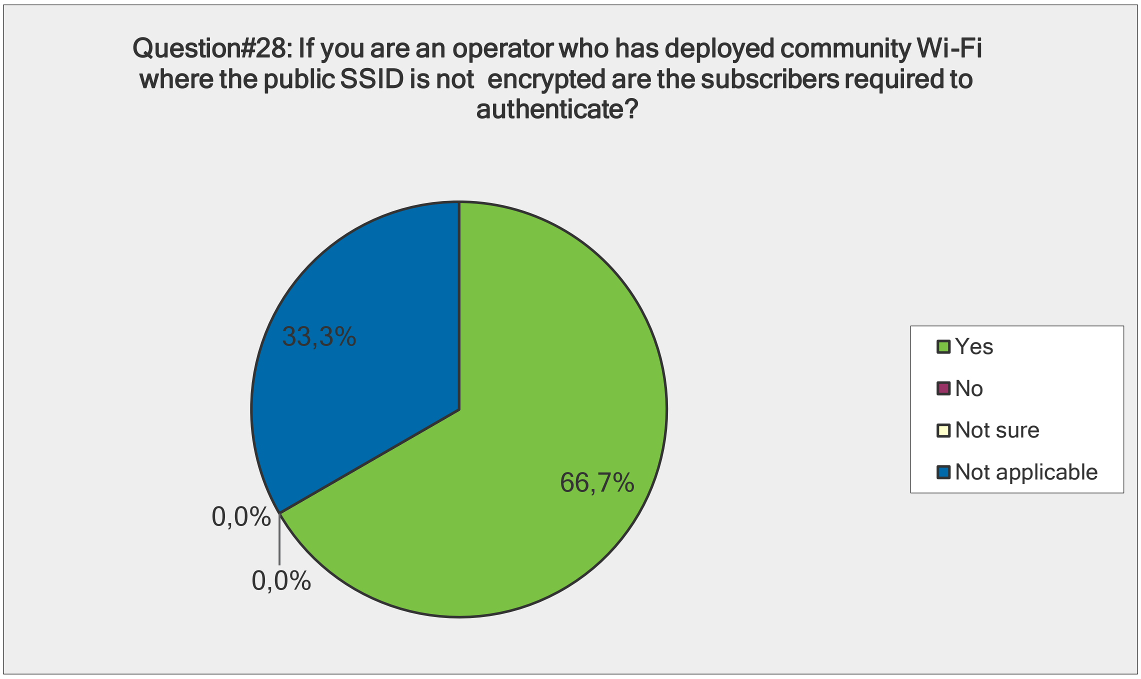
Question#26: If you are an operator who has deployed Community Wi-Fi, do you support two public SSIDs for Community Wi-Fi – one open and other encrypted/secured?



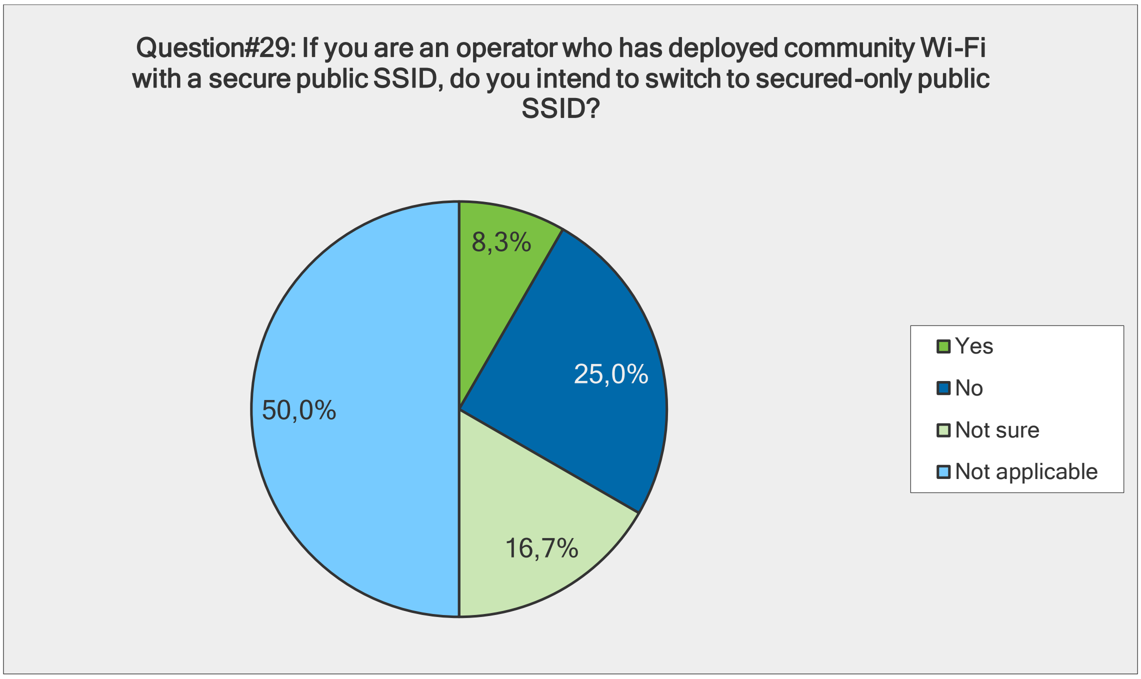
Question#27: If you are an operator who has deployed Community Wi-Fi using a secure SSID for the public SSID, what security method/protocols are used with 802.1x for authentication?



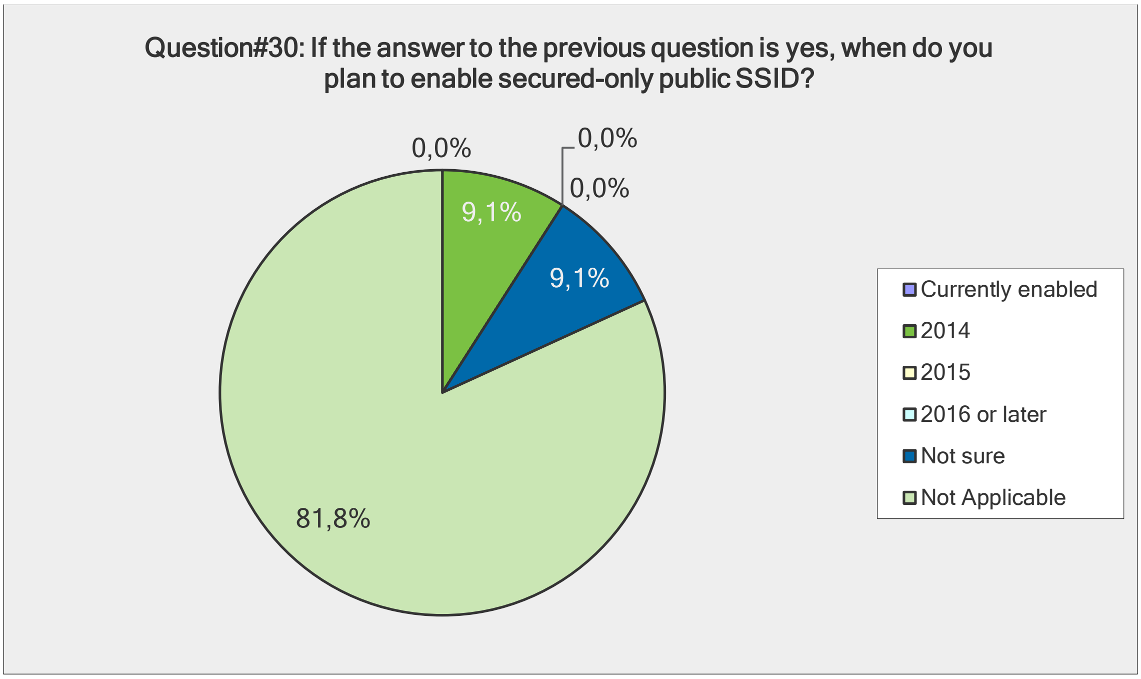
Question#28: If you are an operator who has deployed Community Wi-Fi where the public SSID is not encrypted are the subscribers required to authenticate?



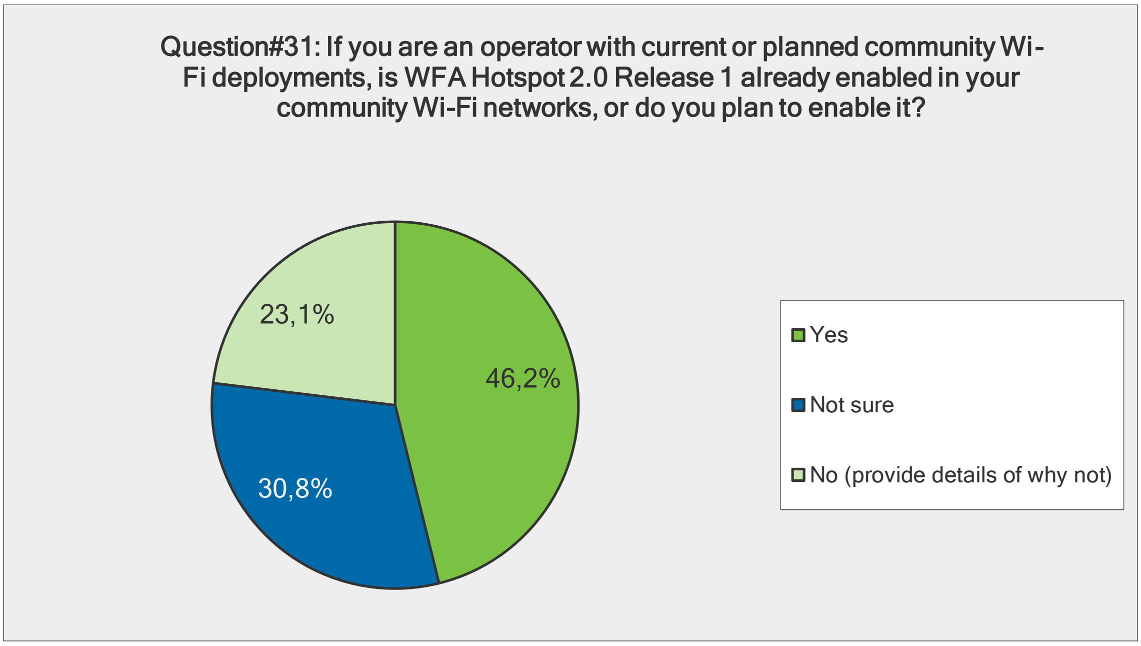
Question#29: If you are an operator who has deployed Community Wi-Fi with a secure public SSID, do you intend to switch to secured-only public SSID?



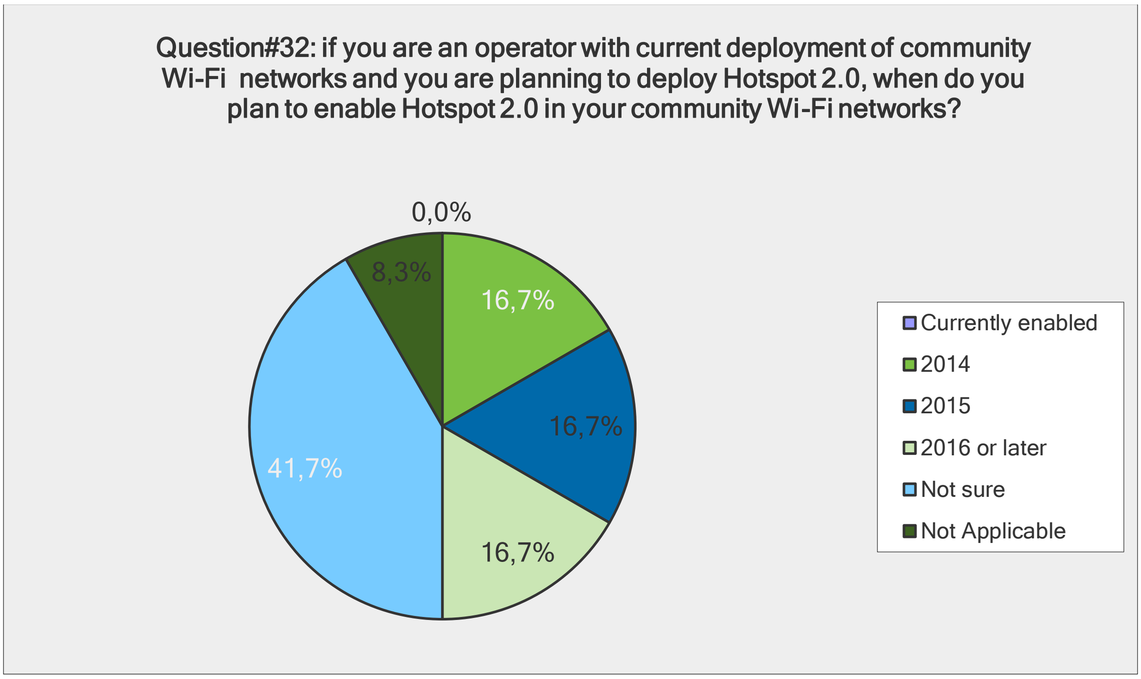
Question#30: If the answer to the previous question is yes, when do you plan to enable secured-only public SSID?



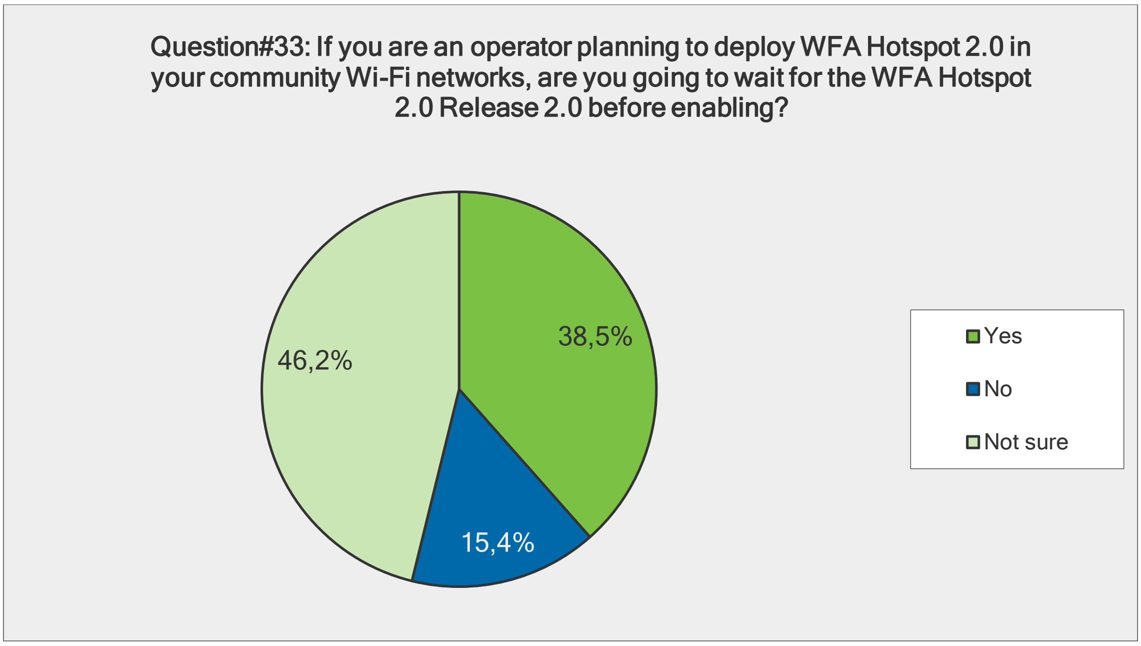
Question#31: If you are an operator with current or planned Community Wi-Fi deployments, is WFA HS2.0 Release 1 already enabled in your Community Wi-Fi networks, or do you plan to enable it?



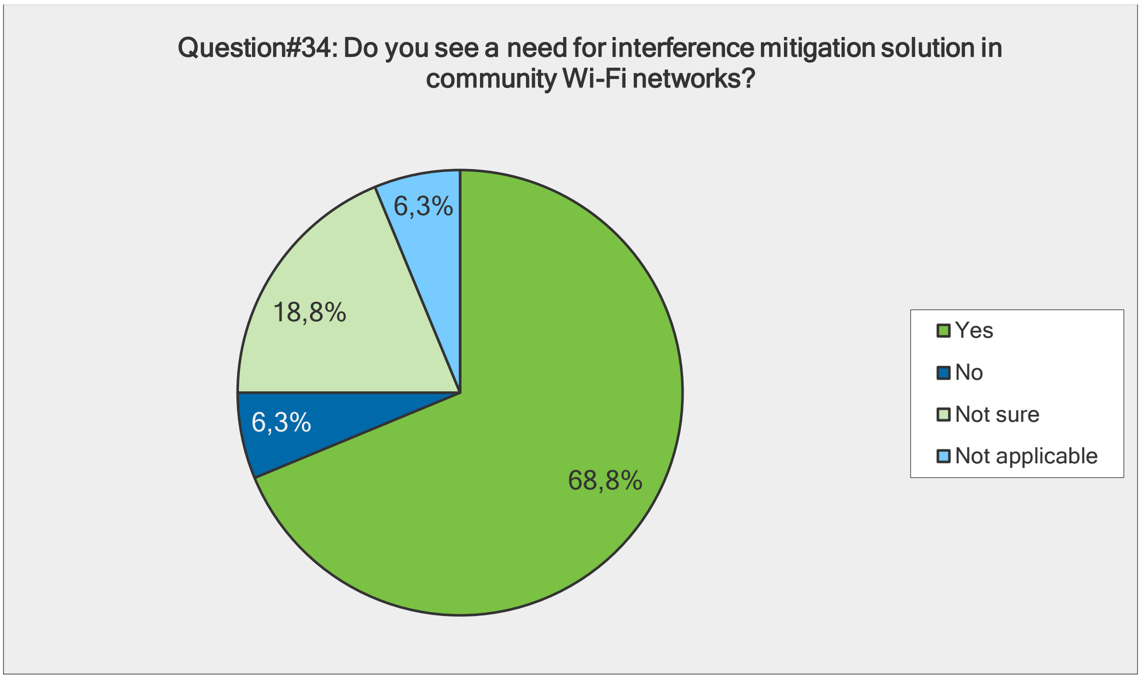
Question#32: if you are an operator with current deployment of Community Wi-Fi networks and you are planning to deploy HS2.0, when do you plan to enable HS2.0 in your Community Wi-Fi networks?



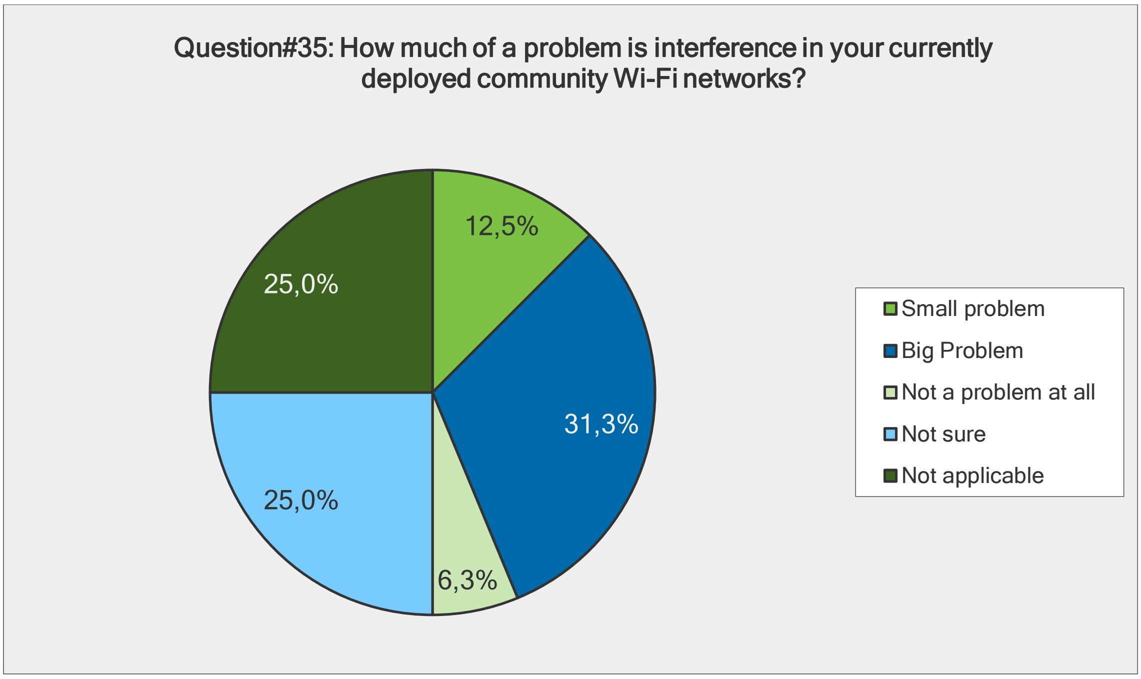
Question#33: If you are an operator planning to deploy WFA HS2.0 in your Community Wi-Fi networks, are you going to wait for the WFA HS2.0 Release 2.0 before enabling?



Question#34: Do you see a need for interference mitigation solution in Community Wi-Fi networks?



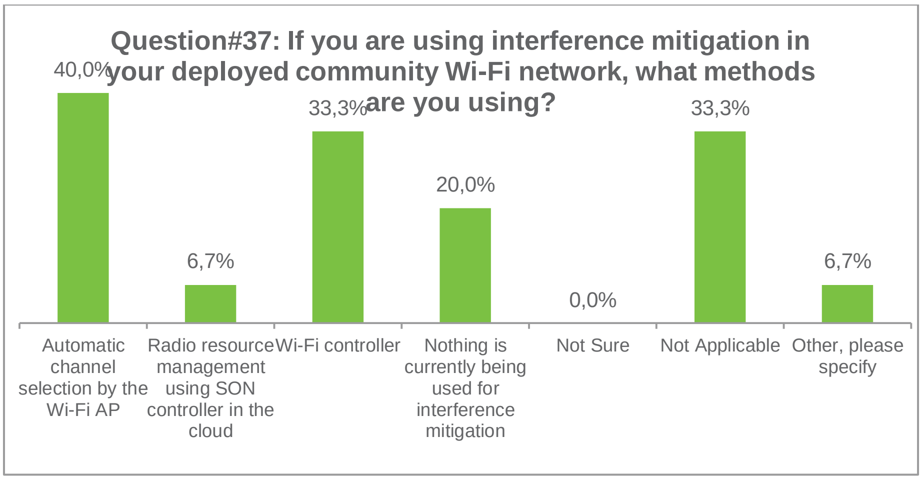
Question#35: How much of a problem is interference in your currently deployed Community Wi-Fi networks?



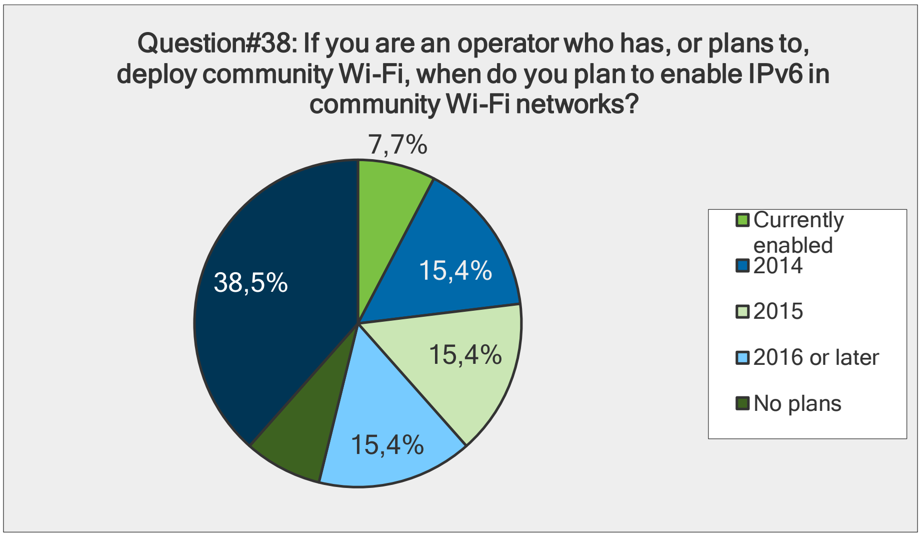
Question#36: “If you answered “small problem” or “big problem” to the previous question, what are the major sources of interference in your Community Wi-Fi networks?

- Neighboring networks
- Interference from other operators, other parties, and so on
- Co-Channel interference from other Wi-Fi networks Adjacent Channel interference from other Wi-Fi networks Alternate Channel interference from other Wi-Fi networks Microwave oven Cordless Phone
- Too many APs on the same channel
- Microwave ovens, video cameras, surveillance systems etc., Bluetooth and other carriers in the 2.4G band
- Number of Hotspots deployed can give rise to interference and we have deployed channel management to alleviate some of the issues

Question#37: If you are using interference mitigation in your deployed Community Wi-Fi network, what methods are you using?



Question#38: If you are an operator who has, or plans to, deploy Community Wi-Fi, when do you plan to enable IPv6 in Community Wi-Fi networks?

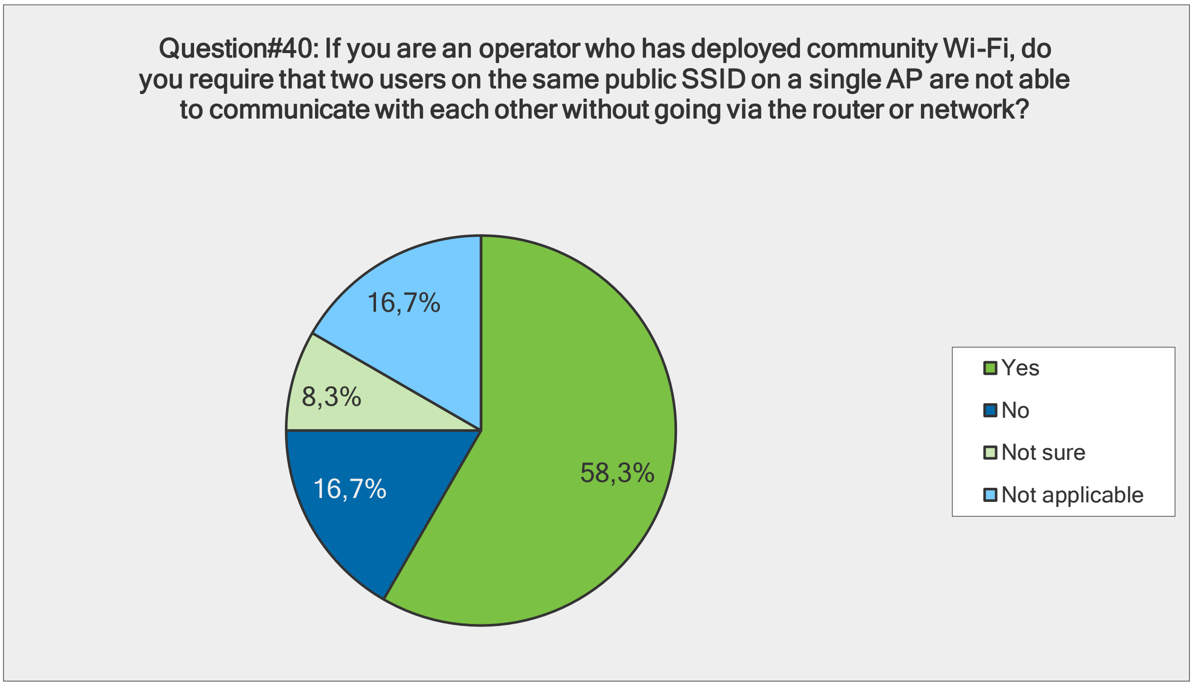


Question#39: What technology and method are using, or do you think should be used, to keep users on the public SSID from accessing the devices and service (e.g., printer) on the private SSID network?

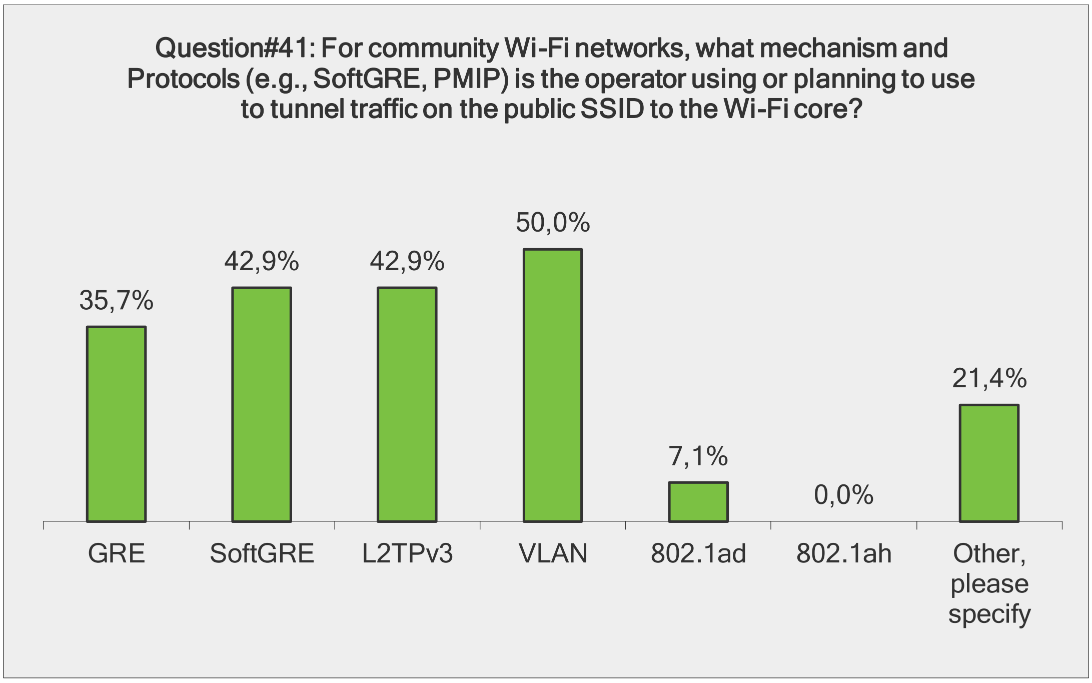
- Complete network separation
- SoftGRE VLAN DOCSIS Service Flow
- True ‘Virtual AP’ capability can provide complete separation of the data for each SSID if the APs implement segregated bridging per SSID. All traffic to the public SSID should only be tunneled to the core network Peer to peer communication should be blocked to prevent unwanted communication within the public SSID
- WLAN to softGRE tunnel over DOCSIS technique should be sufficient

- Segregate the traffic from public SSID with tunneling mechanism toward the BNG/BRAS without enabling local routing in RG
- The public SSID should be completely isolated from the public SSID. An open standards solution should be provided
- Secure and separate services provide isolation
- Firewall
- VLAN separation

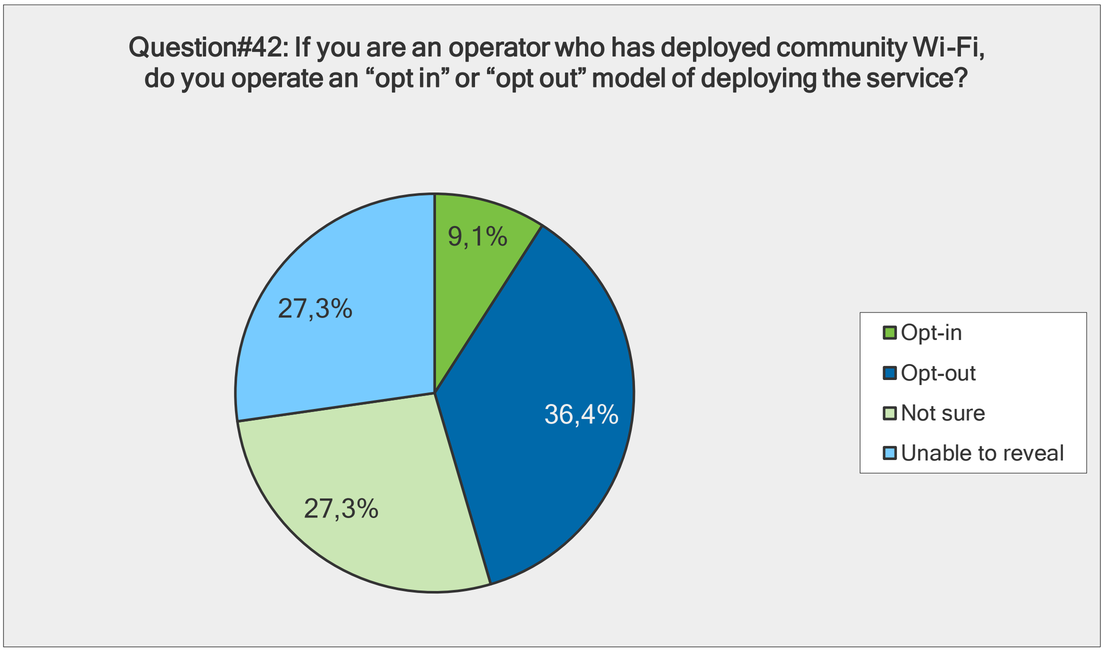
Question#40: If you are an operator who has deployed Community Wi-Fi, do you require that two users on the same public SSID on a single AP are not able to communicate with each other without going via the router or network?



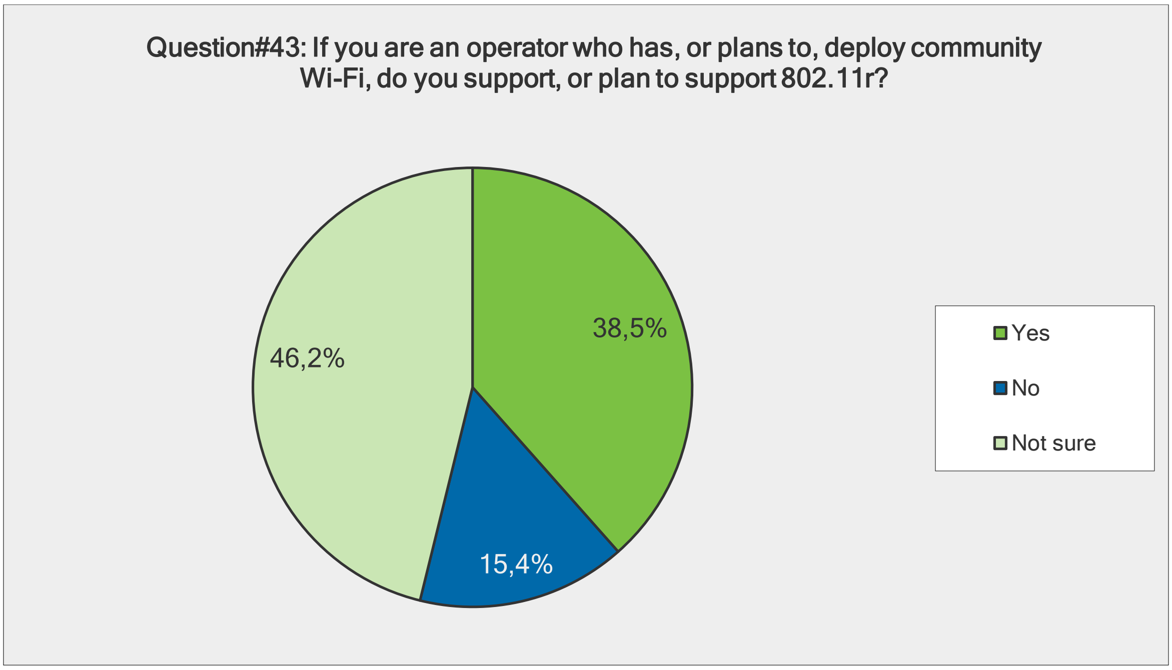
Question#41: For Community Wi-Fi networks, what mechanism and Protocols (e.g., SoftGRE, PMIP) is the operator using or planning to use to tunnel traffic on the public SSID to the Wi-Fi core?



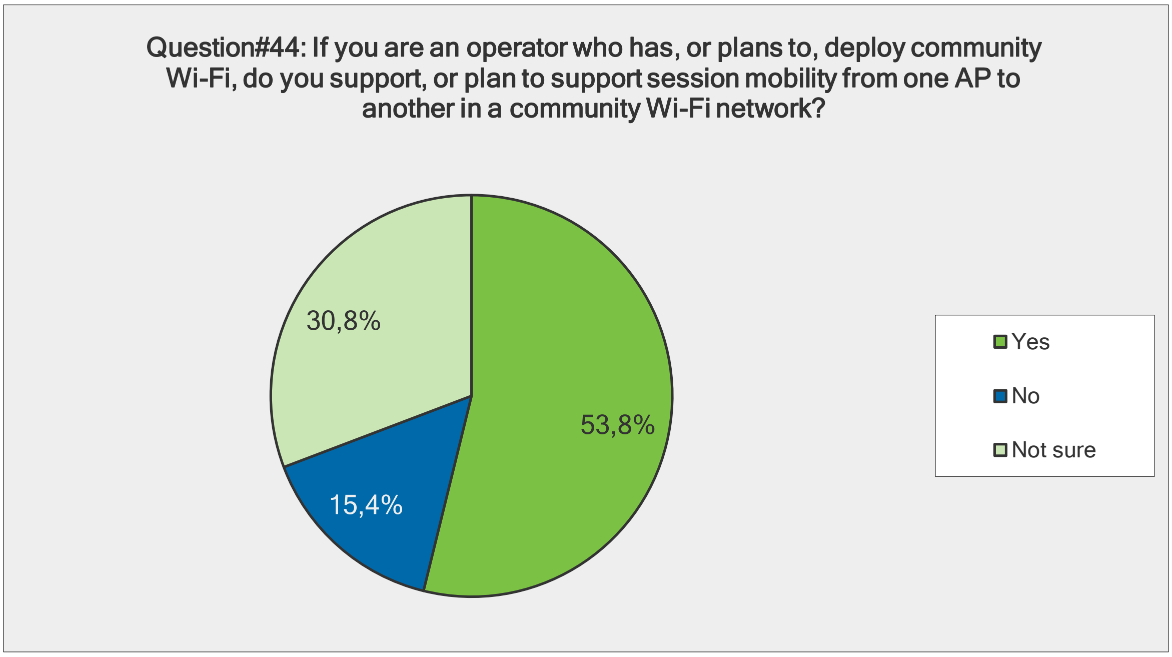
Question#42: If you are an operator who has deployed Community Wi-Fi, do you operate an “opt in” or “opt out” model of deploying the service?



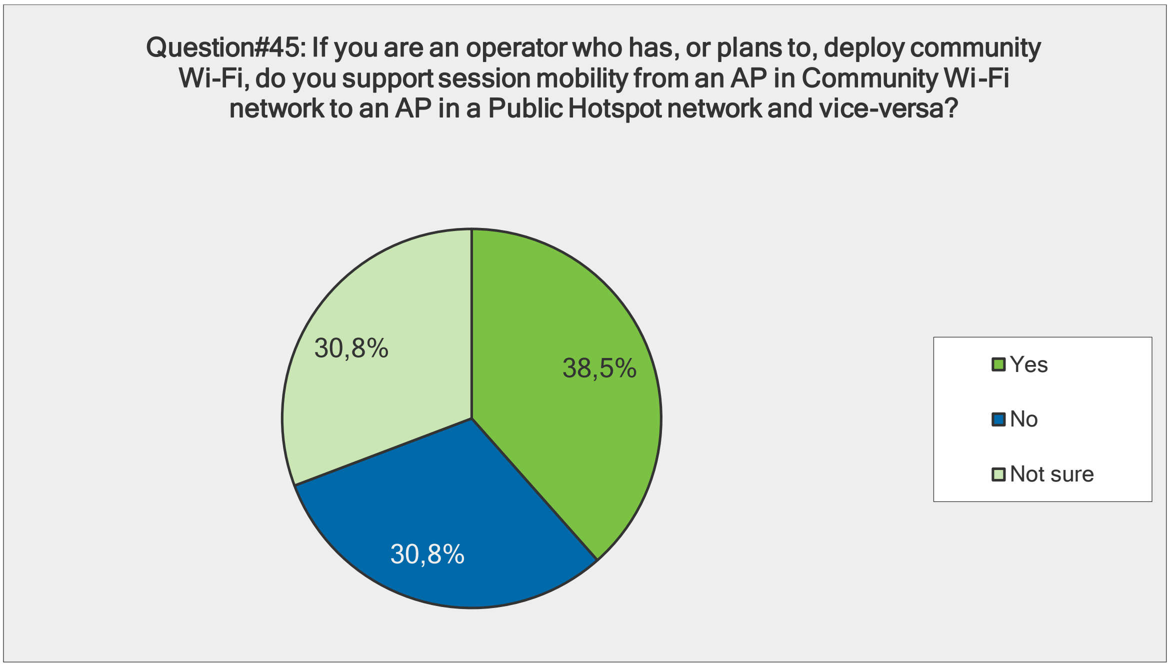
Question#43: If you are an operator who has, or plans to, deploy Community Wi-Fi, do you support, or plan to support 802.11r?



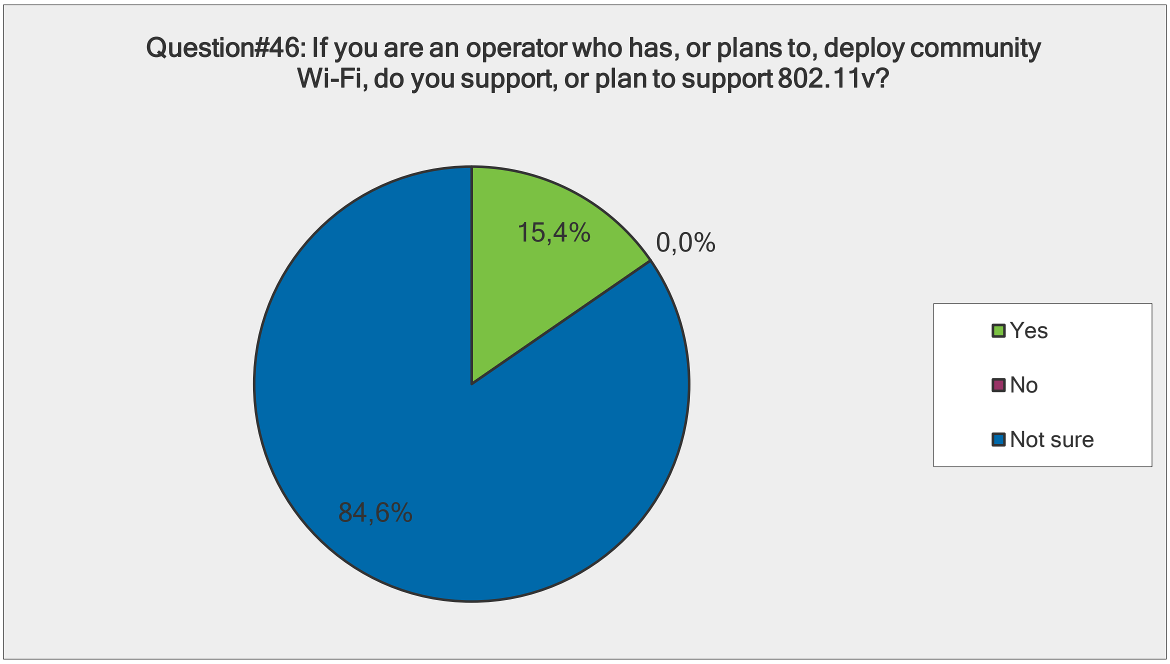
Question#44: If you are an operator who has, or plans to, deploy Community Wi-Fi, do you support, or plan to support session mobility from one AP to another in a Community Wi-Fi network?



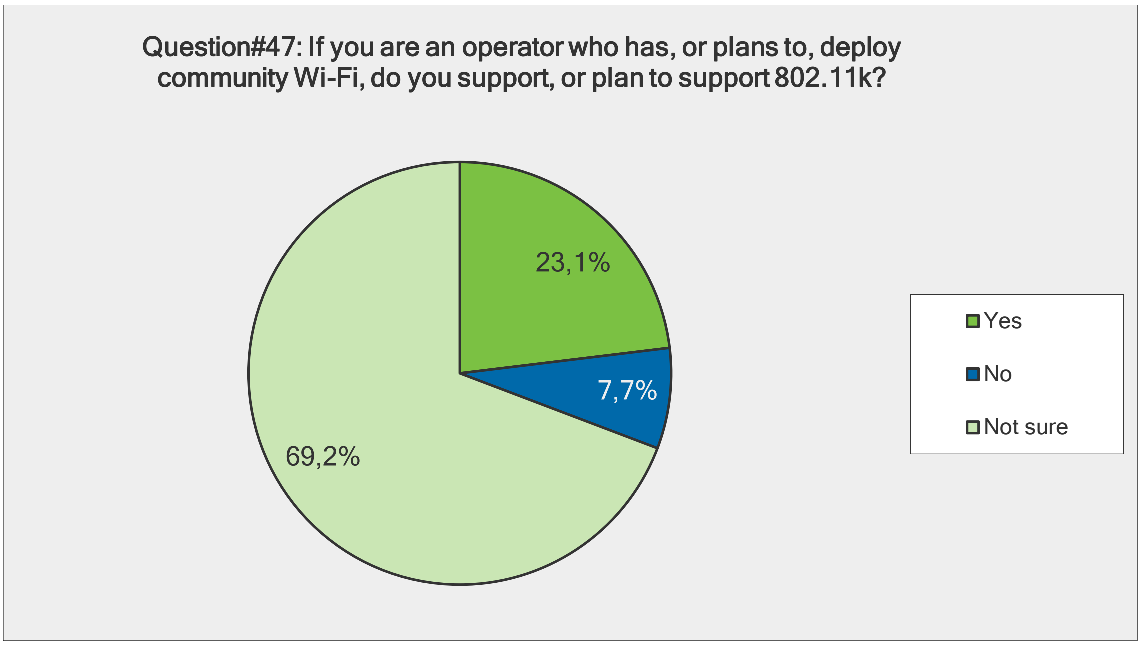
Question#45: If you are an operator who has, or plans to, deploy Community Wi-Fi, do you support session mobility from an AP in Community Wi-Fi network to an AP in a Public Hotspot network and vice-versa?



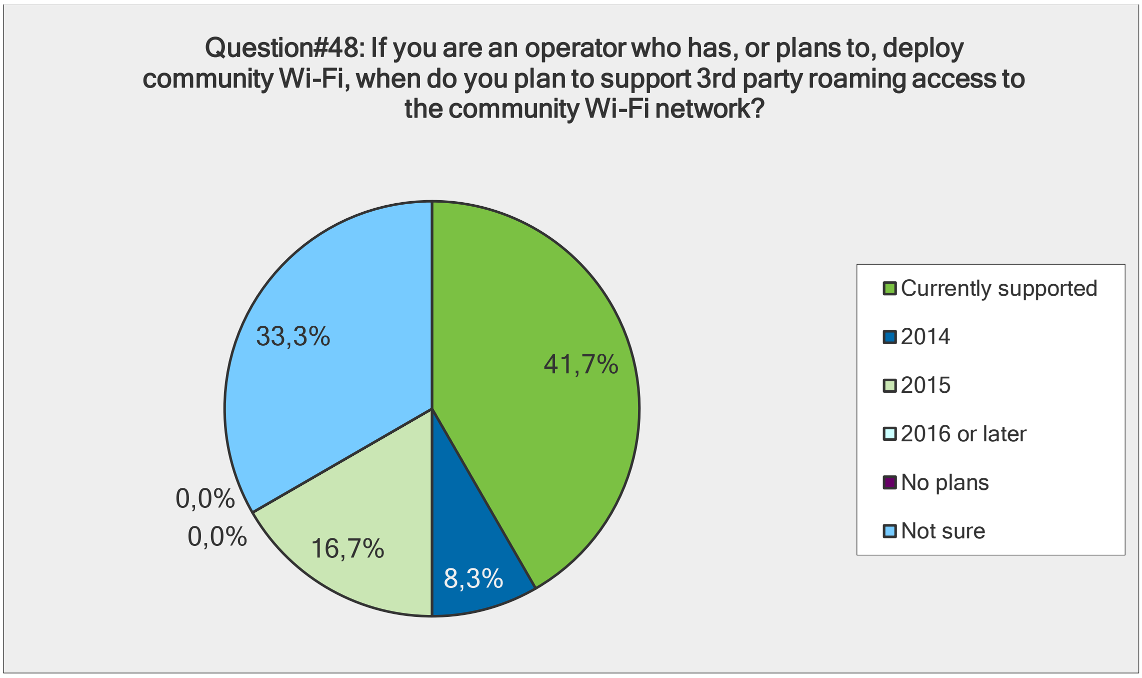
Question#46: If you are an operator who has, or plans to, deploy Community Wi-Fi, do you support, or plan to support 802.11v?



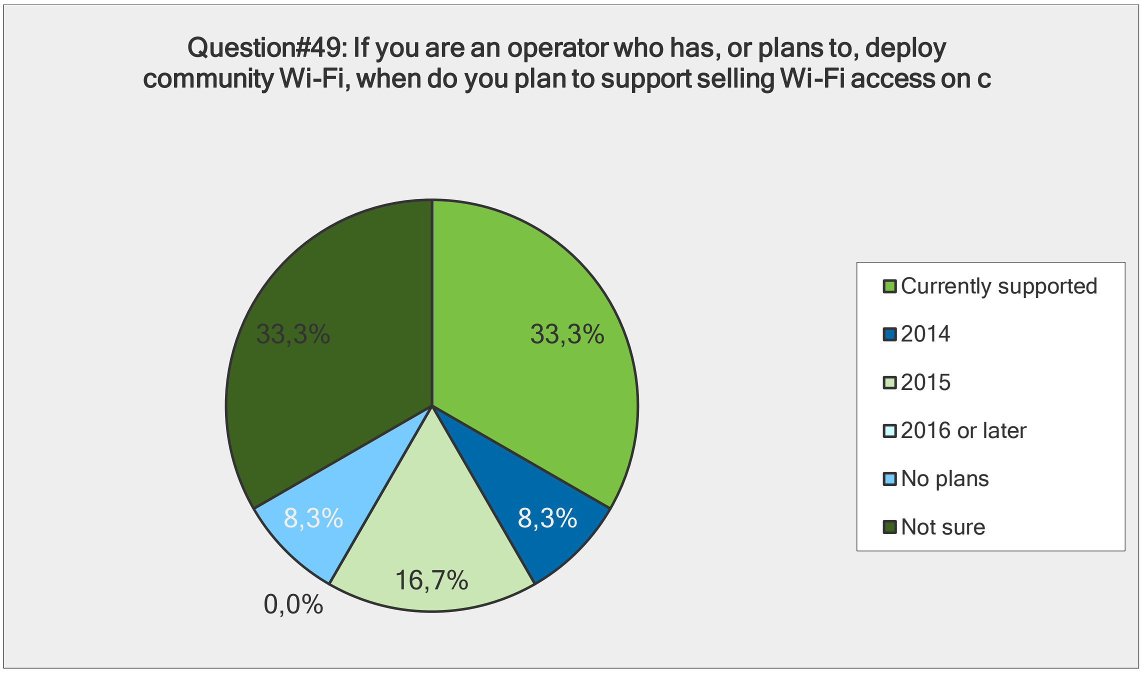
Question#47: If you are an operator who has, or plans to, deploy Community Wi-Fi, do you support, or plan to support 802.11k?



Question#48: If you are an operator who has, or plans to, deploy Community Wi-Fi, when do you plan to support 3rd party roaming access to the Community Wi-Fi network?



Question#49: If you are an operator who has, or plans to, deploy Community Wi-Fi, when do you plan to support selling Wi-Fi access on Community Wi-Fi network to retail customers? A retail customer is someone who buys Wi-Fi services from operator for a fixed (e.g., 2 hours) duration at a time. In other words, a retail customer is not a subscriber of the operator or third party roaming partner.



Question#50: Do you have any additional comment on the Wi-Fi Community deployment?

- Traffic Prioritization, Network Selection, Mobility, Security, RF Conformance, RF performance, Passpoint, Traffic separation, CPE Management, Radio Resource Management are important to operators for Community Wi-Fi deployments

- Network selection between Wi-Fi and Cellular networks is an important issue that needs to be solved. Other issues include mobility (Wi-Fi to Wi-Fi, Wi-Fi to Cellular, etc.), QoS, prioritization of private vs. public traffic. Policy management and provisioning (e.g., on the device) for network selection, mobility, etc., needs to supported/provided as well

Annex C – Use Cases and Recommendations

The following is a list of use cases and recommendations for Community Wi-Fi. The actual implementation may vary, but this should assist in ensuring the basic features are addressed.

Community Wi-Fi Service Use Cases

Network Discovery

Req.	Description
1.1	Network Discovery, Selection and Access USER SHOULD be able to discover, select, and attach to private and public Wi-Fi networks

Connection Establishment

2.1	Connect to a Home Service Provider's Residential Wi-Fi Network USER SHOULD be able to connect to their private SSID without any user intervention
2.2	Connect to a Home Service Provider's Community Wi-Fi Network USER SHOULD be able to connect to their Home Service Provider's public SSID without any user intervention
2.3	Informed Network Selection when Residential and Community Wi-Fi Networks are Available After the initial device configuration, USER SHOULD connect to the private SSID without any further user intervention OPERATOR SHOULD support the capability to prevent the USER from accessing the public SSID from their home

Quality of Service

3.1	Guaranteed QoS for Community Wi-Fi Network Connections OPERATOR MAY assign guaranteed QoS on the public SSID Private SSID traffic will get its maximum allocated bandwidth, with the remainder available for the public SSID
3.2	Guaranteed QoS for Residential Wi-Fi Network Connections OPERATOR MAY assign guaranteed QoS on the private SSID Private SSID traffic will get its maximum allocated bandwidth, with the remainder available for the public SSID

Security

4.1	Residential Wi-Fi Network Security A private SSID USER SHOULD NOT have any visibility of the public SSID traffic and its users
4.2	Community Wi-Fi Network Security A public SSID USER SHOULD NOT have any visibility of the private SSID traffic, its users, or any connected devices (e.g., network printers, network storage etc.) Public SSID USERS SHOULD NOT have direct access to, or visibility of each other

Mobility

5.1	Residential Wi-Fi to Community Wi-Fi Handoff: Seamless Session Continuity USER MAY be able to have their current session remain active when roaming from their private SSID to a public SSID
5.2	Community Wi-Fi to Residential Wi-Fi Handoff: Seamless Session Continuity

	USER MAY be able to have their current session remain active when roaming from a public SSID to their private SSID Note: Per requirement 2.3, when the USER is connected to its private SSID, the user session SHOULD not be moved to the public SSID provided by the same residential GW
5.3	Inter-Network Roaming USER MAY be able to have their current session remain active when roaming between different operator networks

Roaming

6.1	Connect to a Visited Service Provider's Community Wi-Fi Hotspot where the VSP has a roaming agreement with the HSP A roaming partner USER SHOULD be able to connect to a Visited Service Provider's public SSID without user intervention, provided the HSP and VSP have a roaming agreement

Community Wi-Fi Management Use Cases

Subscription Management

7.1	Subscribe to Community Wi-Fi Service USER SHOULD be able to subscribe to the Community Wi-Fi service by contacting their service provider or via a self-service management portal
7.2	Unsubscribe from Community Wi-Fi Service USER SHOULD be able to unsubscribe from the Community Wi-Fi Service by contacting their service provider or via a self-service management portal or application
7.3	Default Subscription State for Community Wi-Fi Service OPERATER SHOULD define the default subscription state based on their subscription policy. As such, a USER SHOULD or SHOULD NOT be automatically subscribed to the Community Wi-Fi Service

Policy Management

8.1	Home Subscriber Service Access Policy OPERATOR SHOULD be able to define a set of services that a Community Wi-Fi subscriber is able to access
8.2	Roaming Subscriber Service Access Policy OPERATOR SHOULD be able to define a set of services that a Community Wi-Fi roaming partner subscriber is able to access
8.3	Guest User Service Access Policy OPERATOR SHOULD be able to define a set of services that a guest user (i.e., a temporary subscriber) is able to access

State Management

9.1	Enable Community Wi-Fi Access OPERATOR SHOULD be able to enable access to the public SSID on a residential Wi-Fi Access Point independent of private SSID access
9.2	Disable Community Wi-Fi Access OPERATOR SHOULD be able to disable access to the public SSID on a residential Wi-Fi Access Point independent of private SSID access USER SHOULD be able to opt-out of the public SSID. This will completely disable the Community Wi-Fi SSID on their CPE and may prevent them from accessing other public SSIDs.
9.3	Enable Residential Wi-Fi Access OPERATOR SHOULD be able to enable access to the private SSID on a residential Wi-Fi Access Point independent of public SSID access

	USER SHOULD be able to enable access to the private SSID without affecting access to the public SSID
9.4	Disable Residential Wi-Fi Access OPERATOR SHOULD be able to disable access to the private SSID on a residential Wi-Fi Access Point independent of public SSID access USER SHOULD be able to disable access to the private SSID without affecting access to the public SSID
9.5	Wi-Fi Access Point Power Off If a user powers off their Wi-Fi Access Point, access to the private SSID and the public SSID will be lost. However, the configuration SHOULD NOT be lost
9.6	Wi-Fi Access Point Power On / Restart When a user powers on (or restarts) their Wi-Fi Access Point, access to the private SSID and the public SSID SHOULD be restored from the saved configuration
9.7	Wi-Fi Access Point Power On – Default Configuration OPERATOR SHOULD be able to specify the default configuration for the Wi-Fi AP. This applies to both the configuration of the private SSID and the public SSID

Notifications

10.1	Subscription Change Notifications OPERATOR SHOULD be notified when a user subscribes or unsubscribes to Community Wi-Fi
10.2	State Change Notifications OPERATOR SHOULD be notified whenever access to the public SSID changes state e.g. is enabled or disabled along with a reason for the state change. A reason may be operator action, access point failure, access point power off, etc.
10.3	Filtering OPERATOR SHOULD be able to filter notifications e.g. by notification type

Fault Management

11.1	Fault Detection This is out of the scope of Community Wi-Fi
11.2	Filtering OPERATOR SHOULD be able to filter notifications e.g. by notification type

Performance Management

12.1	Residential Wi-Fi Network Performance OPERATOR SHOULD be able to monitor the Wi-Fi network performance of residential user activity (e.g. on a device by device basis) on an individual basis and as an aggregate Performance metrics may be based on class of service
12.2	Community Wi-Fi Network Performance OPERATOR SHOULD be able to monitor the Wi-Fi network performance of Community Wi-Fi user activity, on an individual basis, and as an aggregate This may include home network subscribers, visiting network subscribers, and potentially guest users Additionally, performance metrics may be broken out by location Performance metrics may be based on class of service
12.3	Network Performance Notifications OPERATOR SHOULD be notified when pre-determined performance metric thresholds are crossed
12.4	Admission Control OPERATOR SHOULD be able to control the number of public subscribers associated with the access point. This will help to ensure adequate bandwidth

Accounting Management

13.1	Community Wi-Fi Accounting Records OPERATOR SHOULD be able to classify by: User Location Device User class Home service provider subscriber Guest Roaming partner subscriber Additionally, OPERATOR MAY use WRIX for accounting.

Security Management

14.1	Allowed Actions USER SHOULD be able to manage their Wi-Fi Access Point in the following ways: Users can turn it on Users can turn it off Users can restart it USER SHOULD be able to manage the private SSID in the following ways: Users can configure the private SSID and associated parameters Users can view the performance of the private SSID Users can view faults associated with the private SSID
14.2	Disallowed Actions USER SHOULD NOT be able to view or configure the public SSID and associated parameters, or perform any other management functions with respect to the public SSID
14.3	Allowed Actions OPERATOR SHOULD be able to manage a public SSID in the following ways: Operator can configure the public SSID and associated parameters Operator can view the performance of the public SSID Operator can view faults associated with the public SSID Operator can view changes to the configuration of the public SSID OPERATOR SHOULD be able to manage the residential Wi-Fi AP in the following ways: Operator can configure the private SSID and associated parameters Operator can view the performance of the private SSID Operator can view faults associated with the private SSID Operator can view changes to the configuration of the private SSID
14.4	Disallowed Actions None
14.5	Lawful Intercept The operator SHOULD enable access for a Law Enforcement Agency (LEA) to perform electronic surveillance as mandated by applicable local laws and regulations

Acronyms, Abbreviations, and Definitions

Acronym or Abbreviation	Definition
3GPP	3rd Generation Partnership Project. The standards group responsible for 3G GSM technology
3GPP2	3rd Generation Partnership Project 2. The standards group responsible for 3G CDMA technology
802.11e	An IEEE Wireless LAN QoS standard amendment that includes queue prioritization, admission control, and power-save specifications
802.11i	An IEEE Wireless LAN security standard amendment which replaces the deprecated WEP and allows for up to AES-level encryption
802.11k	An IEEE Wireless LAN standard amendment for radio resource management
802.11r	An IEEE Wireless LAN standard amendment for fast BSS transition
802.11u	An IEEE Wireless LAN standard amendment for interworking. Hotspot 2.0 / Passpoint is based off of this standard
802.1x	An IEEE network standard for port-based admission control
AAA	Authentication, Authorization and Accounting. A security architecture for distributed systems for controlling which users are allowed access to which services, and tracking which resources they have used
AC	Access Category
ACK	Acknowledgement
ACS	Automatic Configuration Server. A server for managing the configuration of CPE
ACS	Automatic Channel Selection
AIFS	Arbitration Interframe Space
ANDSF	Access Network Discovery and Selection function. The server provides to the UE the policy for performing the selection of the WLAN network and traffic steering among the 3GPP and WLAN accesses
ANQP	Access Network Query Protocol
AP	Access Point. A device that allows wireless stations to connect to a wired network using Wi-Fi
ARP	Address Resolution Protocol
BRAS	Broadband remote access server. A router that exists between a CSP core and a remote access device like a DSLAM
BPI	Baseline Privacy Interface
BSS	Basic Service Set
BSSID	Basic Service Set Identification
CAPWAP	Control And Provisioning of Wireless Access Points. A standard networking protocol that allows a wireless LAN controller to manage a group of wireless access points
CBR	Constant Bit Rate
CMTS	Cable Modem Termination System. A piece of equipment that terminates the cable modem signal in the CSP's core
CPE	Customer Premises Equipment. Any device located at the customer premises that is connected to the carrier's central equipment
CSP	Communications Service Provider. A company or organization that offers digital information transportation services
COA	Change of Address
CMIM	Cable Modem Interface Mask
CWmin	Contention Window Minimum
DBDC	Dual Band Dual Concurrent
DCF	Distributed Coordination Function
DHCP	Dynamic Host Control Protocol
DIFS	DCF Interframe Space

Acronym or Abbreviation	Definition
DNSSL	DNS Search List
DOCSIS	Data Over Cable Service Interface Specification
DPI	Deep Packet Inspection
DSLAM	Digital Subscriber Line Access Multiplexer. A device that concatenates multiple DSL lines into a single network trunk
DSMIPv6	Dual-stack Mobile Internet Protocol version 6
EAP	Extensible Authentication Protocol. A framework for network authentication, typically used in Wi-Fi
EAP-SIM	Extensible Authentication Protocol – Subscriber Information Module. A network authentication framework that is based off the subscriber information contained in a SIM chip
eMTA	Embedded Multimedia Terminal Adapter. A cable modem and VoIP adapter bundled into a single device.
EPC	Evolved Packet Core
ePDG	Evolved Packet Network. The gateway located in 3GPP EPC network terminated the s2b interface towards the PDN GW and the SWu toward the UE providing traffic forwarding, perform admission control, IP address assignment, etc.
ESSID	Extended Service Set Identification
FTTH	Fiber To The Home
GBR	Minimum Guaranteed Bit Rate
GRE / SoftGRE	Generic Routing Encapsulation. A tunneling protocol used to encapsulate point-to-point network traffic. SoftGRE refers to a stateless implementation of GRE where the tunnels are created dynamically on an as-needed basis
GTP	GPRS Tunneling Protocol
HLR/HSS	Home Location Register\Home Subscriber Server. The server stores the user subscription profile.
HS2.0	Hotspot 2.0
IETF	Internet Engineering Task Force
IFOM	IP Flow Mobility
IMS	IP Multimedia Subsystem
IPS / IDS	Intrusion Prevention / Detection System. A security system that can detect or actively prevent network intrusions
LMA	Local Mobility Anchor. The home agent for the mobile node in the Proxy Mobile IPv6 domain.MAC
Media Access Control	
MBR	Maximum guaranteed Bit Rate
MAG	Mobile Access Gateway. The access router for the mobile node (STA)
MAPCON	Multi Access PDN Connectivity
MCS	Modulation and Coding Scheme. The likely data rate achievable by your Wi-Fi connection, calculated by summarizing the coding type, modulation rate, number of spatial streams, and channel width
MIP	Mobile Internet Protocol
MOBIKE	IKEv2 Mobility and Multihoming Protocol
Modem	Modulator / Demodulator. The CPE that is used to connect the subscriber with the CSP network / Internet.
MPTCP	Multipath TCP
NAT	Network Address Translation
ND	Non-Duplex
NDS	Network Domain Security
NAI	Network Access Identifier
NMS	Network Management System

Acronym or Abbreviation	Definition
NSWO	Non-Seamless WLAN Offload
OSS	Operations Support System. The infrastructure in control of network configuration, fault management, and service provisioning
PCRF	Policy and Charging Rules Function. The 3GPP EPC entity responsible for the QoS and Charging coordination per subscriber. It does that by downloading the rules associated to the corresponding subscriber to the PDN GW
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PDN GW	Packet Data Network Gateway- The gateway provides several functionalities, such as Ip address assignment, traffic routing, terminating control interface, service authorization, QoS enforcement, accounting, etc.
PHY	Physical Layer
PMIP	Proxy Mobile IPv6. A network-based mobility management protocol that supports a number of access technologies such as 3GPP and Wi-Fi
PPPoE	Point-to-point protocol over Ethernet. A layer 2 protocol used to create a direct connection between two nodes over Ethernet
QCI	QoS Class Identifier
QoS	Quality of Service. The prioritizing of network traffic based on content or destination.
RA	Router Advertisement
RDNSS	Recursive DNS Server
RRM	Radio Resource Management. The centralized management server responsible for controlling AP RF characteristics such as channel, transmit power, and data rates
RSSI	Received Signal Strength Indicator
RTP	Real-time Protocol
SIFS	Short Interframe Space
SLAAC	Stateless Address Autoconfiguration
SNMP MIB	Simple Network Management Protocol
Management Information Base	
SoftGRE	Soft Generic Routing Encapsulation
SON Self-Organizing Network. An automation technology used to provide RRM	
SRVCC	Single Radio Voice Call Continuity
STA	Wireless station. A device that has the capability to use the 802.11 protocol. For example, a station may be a laptop, a desktop PC, tablet, or Wi-Fi phone
SSID	Service Set Identification. The human-readable Wi-Fi network name
TCP	Transmission Control Protocol. A transport-layer protocol used for connection-oriented, reliable network communications
TFTP	Trivial File Transfer Protocol
TIS	Total Isotropic Sensitivity. The 3-dimentional spherical sensitivity of an antenna/receiver system
TR-069	Technical Report 069. A technical specification defining an application layer protocol for remote management of end-user devices
TRP	Total Radiated Power. The power level of the transmitter as measured at the receiving antenna in an actively connected system
Tunnel	One of several encapsulation protocols (e.g., GRE) used to isolate and securely deliver the public traffic to the WAG
TWAG	Trusted Wireless Access Gateway. The gateway located in the CSP network provides the connection to the mobile core network via s2a interface, terminated the 3GPP control protocol from the UE, acts as first router, etc.
TXOP	Transmit Opportunity
UDP	User Datagram Protocol

Acronym or Abbreviation	Definition
UE	User Equipment. A device that has the capability to use IEEE 802.11 and 3GPP protocols using mobile credential (e.g., USIM). For example, a user equipment may be a smartphone or a tablet
UGS	Unsolicited Grant Service
VCC	Voice Call Continuity
VLAN	Virtual Local Area Network. A virtual broadcast domain used for network traffic isolation
VoIP	Voice over Internet Protocol. A group of technologies that enable the transmission of voice over standard networking protocols
VoLTE	Voice Over LTE
WAG	Wireless Access Gateway. Allows access to the MSO network / Internet for public SSID subscribers
WFA	Wi-Fi Alliance
WLCP	Wireless LAN Control Protocol
WMM	Wi-Fi MultiMedia
WMM-AC	WMM Admission Control
WPA	Wi-Fi Protected Access. See 802.11i
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 defines 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–l deals with the maintenance and exchange of location information

Participant List

Company
Accuris Networks
AT&T
BIGLOBE
BSG Wireless
BT
CableLabs
China Mobile
Cisco Systems
Comcast
Cox Communications
Ericsson
FON Wireless
Gemalto
Huawei
Meteor Network
NSN
NTT DOCOMO
Orange
Portugal Telecom (MEO)
Ruckus Wireless
Shaw Communications
Time Warner Cable