In-Home Wi-Fi

Industry Guidelines

Source: In-Home Wi-Fi Workgroup
Author(s): WBA Members
Issue date: January 2019
Version: Version 1.0

WIRELESS BROADBAND ALLIANCE
DRIVING NEXT WIRELESS EXPERIENCE

ABOUT THE WIRELESS BROADBAND ALLIANCE

Founded in 2003, the mission of the Wireless Broadband Alliance (WBA) is to resolve business issues and enable collaborative opportunities for service providers, enterprises and cities, enabling them to enhance the customer experience on Wi-Fi and significant adjacent technologies. Building on our heritage of NGH and carrier Wi-Fi, the WBA will continue to drive and support the adoption of Next Generation Wi-Fi services across the entire public Wi-Fi ecosystem, having a focus on four major programmes: Carrier Wi-Fi Services, Next Generation Wireless & 5G, IoT, and Connected Cities. Today, membership includes major fixed operators such as BT, Comcast and Charter Communication; seven of the top 10 mobile operator groups (by revenue) and leading technology companies such as Cisco, Microsoft, Huawei Technologies, Google and Intel. WBA member operators collectively serve more than 2 billion subscribers and operate more than 30 million hotspots globally.

The WBA Board includes AT&T, Boingo Wireless, BT, Cisco Systems, Comcast, Intel, KT Corporation, Liberty Global, NTT DOCOMO and Orange. For a complete list of current WBA members, please **click here**.

Follow Wireless Broadband Alliance at:

www.twitter.com/wballiance

http://www.facebook.com/WirelessBroadbandAlliance

https://www.linkedin.com/company/wireless-broadband-alliance

UNDERTAKINGS AND LIMITATION OF LIABILITY

This Document and all the information contained in this Document is provided on an 'as is' basis without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for particular purpose, or non-infringement.

In addition, the WBA (and all other organisations who may have contributed to this document) makes no representations or warranties about the accuracy, completeness, or suitability for any purpose of the information. The information may contain technical inaccuracies or typographical errors. All liabilities of the WBA (and all other organisations who may have contributed to this document) howsoever arising for any such inaccuracies, errors, incompleteness, suitability, merchantability, fitness and non-infringement are expressly excluded to the fullest extent permitted by law. None of the contributors make any representation or offer to license any of their intellectual property rights to the other, or to any third party. Nothing in this information or communication shall be relied on by any recipient.

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

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

CONTENTS

1 Background / Ecosystem definition 1

1.1 Background & Motivation 1

1.2 Scope 2

1.3 Current Ecosystem 3

2 Operator Use Cases and Services Requirements 4

2.1 In-Home Wi-Fi Deployment Models 4

2.2 Mapping of In-Home Wi-Fi features and Operator requirements to various deployment models 5

2.2.1 Private Home Network 5

2.2.2 Community Wi-Fi Network 6

2.2.3 Guest Network 7

2.2.4 Content Distribution Network 8

2.2.5 Neutral Host (e.g. Mobile Offload) 9

2.2.6 Corporate Teleworker 10

2.2.7 Utility IOT Network 11

2.3 Current Gaps 11

2.3.1 Cloud RRM 12

2.3.2 Separation of Multiple SSIDs in Multi-AP (Mesh) Environments 12

2.3.3 Ethernet Backhaul security in a Multi-AP Environment 12

2.3.4 Better Onboarding experience 12

2.3.5 QoS (Traffic Prioritization) 13

3 Deployment / Architecture options 13

3.1 Single AP 13

3.2 A Multi-AP Network 14

4 Guidelines / Recommendations 16

4.1 End-to-end security 16

4.1.1 In-Home Security Threats and Security Attack Vectors 16

4.1.2 Wi-Fi Client to Wi-Fi AP link protection 17

4.1.3 Multi-AP Backhaul link protection 17

4.1.4 Multi-AP Control and Management connection between Agents and Controller protection 19
4.1.5 Operator Network protection 19
4.2 Coordination of radio usage or RRM 19
4.2.1 RRM Features 19
4.2.1.1 Band steering (Intra-AP steering) 19
4.2.1.2 AP Steering (Inter-AP Steering) 20
4.2.1.3 Channel selection management 21
4.2.1.4 QoS Management 22
4.2.1.5 Airtime Management 22
4.2.1.6 AP Transmit Power management 23
4.2.1.7 Topology Setup and Self-Healing 23
4.2.2 RRM Implementation Location Options 24
4.2.2.1 Cloud-based 24
4.2.2.2 AP/Gateway-based 25
4.2.2.3 Hybrid-based 25
4.3 Onboarding Devices 25
4.3.1 AP Onboarding 25
4.3.1.1 Operator Provided APs 25
4.3.1.2 Retail Purchased APs 26
4.3.2 Client Device Onboarding 26
4.3.3 Onboarding Best Practices 26
4.4 Deployment guidelines 27
4.4.1 AP Location 27
4.4.2 AP Orientation 27
5 Performance Testing 28
5.1 Wi-Fi Performance Testing Efforts from Other Organizations 28
5.2 Typical In-Home Wi-Fi Performance Test Cases 29
6 Future Evolution 29
6.1 Protect backhaul link with Cloud WPA 29
7 Summary and Conclusions 31

FIGURES

Figure 1. Single AP Network Entities 13
Figure 2. Multi-AP Network Entities in with a local RRM approach 15
Figure 3. Multi-AP Network Entities in a cloud RRM approach 15
Figure 4. Multi-AP Network Entities in a hybrid RRM approach 16
Figure 5. In-Home Cyber and Physical Security threat attack vectors 17
Figure 6. Protect multi-AP backhaul with additional security layer 18
Figure 7. Protect Multi-AP backhaul with Cloud WPA 30

Executive Summary

Wi-Fi is the most widespread access technology to connect to the Internet within home environments. To this end, Operators have realized that they must own Wi-Fi in the Home, and provide quality of service expected by customers, and adopt best practices to overcome Wi-Fi performance challenges. These include a growing number of devices in the home, Wi-Fi interference and congestion, especially challenging in dense deployments, and the lack of smart Wi-Fi network optimization mechanisms and insights to tackle these areas.

This whitepaper introduces the current background and motivations towards the In-Home ecosystem, embracing Multi AP configurations. In addition, this paper assesses and proposes the different cases and service requirements considered in the operator sector, based on the diverse set of architecture options and network types in use. It also describes key technical and deployment challenges that an operator typically encounters in managing large In-Home Wi-Fi networks.

Furthermore in this paper, WBA has proposed key guidelines and recommendations for different functional areas such as end-to-end security, coordination of radio resource management, device onboarding and management, as well as deployment. There is also a focus on the performance testing within the home Wi-Fi environments surveying the work carried out by different organizations and suggesting a set of performance test cases in home Wi-Fi scenarios.

Finally, this paper identifies future lines of work and possible directions the In-Home Wi-Fi network may take.

1 Background / Ecosystem definition

1.1 Background & Motivation

Wi-Fi has been deployed within the home for more than 15 years. It was originally introduced as an after-market product consisting of standalone Wi-Fi Access Points (AP), purchased, installed and maintained by the consumer. This was eventually followed by Operators integrating a Wi-Fi AP with their home gateways to provide additional capability to their customers. During this period, we also saw the rise of the prosumer, aiming to bypass the Operators home Wi-Fi solution with Wi-Fi repeaters and range extenders to overcome Wi-Fi coverage and performance issues. Furthermore, Operators are increasingly providing multi-AP options, with ease of installation, geared to provide whole-home coverage, either locally or centrally managed from the operator's cloud.

Today, Wi-Fi is the most widespread access technology to access the Internet within home environments. Its unlicensed spectrum and inexpensive cost of deployment make it an easy way to provide Internet connectivity to a varying number of clients in many scenarios of our daily life, e.g. hotels, coffee shops, airports, transportation systems, etc. The number of Wi-Fi

connected devices in homes have doubled[1] in the last few years, together with the explosion of streaming services which have increased the need for larger bandwidths. In addition, these devices present very different connection, bandwidth and security requirements, making it challenging to coordinate and guarantee the adequate performance of these devices throughout the whole house.

Additionally, home conditions vary significantly from one home to another. The size of the home, ranging from smaller homes, to the larger ones or multi-dwelling units (MDU), coupled with the material of the walls, the number of floors, and the level of interference are among the numerous factors that can hinder Operators in offering Wi-Fi with an acceptable level of quality to the entire home. This motivates the need for smarter home Wi-Fi networks to improve and enhance the performance in these scenarios, solving the home coverage problem, addressing congestion, interference issues and providing an optimal quality of service uniformly around the house.

From the operator's perspective, the lack of insight into the customers Wi-Fi quality of experience, and ability to proactively remediate Wi-Fi issues leads to a large number of customer service calls, which translates into huge costs for the operator. With the intention of keeping their customers satisfied, Operators are leveraging Wi-Fi analytics to optimize solution configuration and assist with equipment localization, while providing customers with a comprehensive insight into what is going on within their network. To that aim, Operators are moving towards a multiple Wi-Fi Access Point (AP) strategy for homes, especially in single-family homes with bigger floor space and multiple levels. In the near future, we expect to see home deployment configurations where a gateway (usually consisting of modem, AP and router functionality) provides broadband connectivity, and one or more extender/mesh APs are deployed to provide consistent coverage across the home. The primary AP connects to, or is collocated with, the gateway, and the extenders/mesh APs connect back to the gateway router (wirelessly or via wired means) and rely on it for the broadband connection.

1.2 Scope

This white paper aims to perform an operator focused assessment of the current home Wi-Fi problem space discussing the current and planned industry efforts to address known challenges while also exposing gaps which could benefit from additional industry collaboration. To that aim, this paper’s focus areas will include: operator deployment models and services requirements related with In-Home Wi-Fi and respective gaps; technology options to improve the performance of In-Home Wi-Fi provided by Operators; and guidelines to be used by Operators to improve the In-Home Wi-Fi experience.

[1] In 2014 FON concluded that there were 7 devices per household
LG seeing 12 devices per household

1.3 Current Ecosystem

There are multiple software solutions on the market which aim to enhance multi-AP wireless networks with varying levels of intelligence and automation. These software solutions, sometimes referred to as Wi-Fi SON (Self-Optimizing Networks), optimize the Wi-Fi channels to alleviate interference and congestion, especially in dense Wi-Fi deployments, additionally, SON intelligent Wi-Fi systems aim to steer devices to the best AP in the home, and orchestrate the seamless roaming between APs, to optimize coverage and performance.

From the standardization point of view, several organizations are providing certifications, guidelines and Open-Source projects to unify this environment and facilitate multi-AP deployments.

The Wi-Fi Alliance has stepped into this space to provide a standardized architecture and communication mechanism to facilitate the deployments of multi-AP scenarios. The Wi-Fi Alliance has created a certification program, branded as Wi-Fi Easy Mesh™ (Easy Mesh). It defines an architecture with a controller and agents running on access points that work together to enable easy multi-AP setup and mobility within a multi-AP deployment. A goal of Easy Mesh is to enable multi-vendor interoperability. The controller can run on one of the access points, the Gateway or in the cloud, or even a combination of these, and communicates to the agents on the access points to manage multi-AP operation.

The Easy Mesh standard does not define the algorithms that determine, for example, when to steer a device or how to allocate the best Wi-Fi channels to APs. These aspects are the domain of SON algorithms, and the standard leaves room for vendors to innovate and add value here. As an analogy, Wi-Fi standards define the “road system”, while Easy Mesh provides the traffic rules, and the Controller SON algorithms provide the navigation system that places a vehicle on the right road at the right time.

The Broadband Forum (BBF) and the Prpl Foundation have started a joint project to develop an open source implementation of Easy Mesh that is focused on extending the BBF’s open source implementation of IEEE 1905.1a, while also creating requirements to extend and enhance Easy Mesh’ capabilities for use in operator managed home networks. This project is open to all companies, whether they are members of either BBF or Prpl Foundation or not.

In addition to Multi-AP, BBF created a project stream “Wi-Fi In-premises” in 2016 addressing Wi-Fi user experience supported by Operators and their fast-growing Wi-Fi deployments. The active efforts in the project stream are in the areas of Wi-Fi management (TR-181), Wi-Fi performance testing (WT-398), Wi-Fi installation & diagnostics (SD-401) and In-home video support over Wi-Fi (SD-410 & WT-434).

Lastly, CableLabs has been working in the area of wired Proactive Network Management (PNM) for many years and have now brought that concept to wireless with Wi-Fi PNM. PNM detects and resolves impending failure conditions before problems become customer-impacting. After conducting a 7-country field trial of Wi-Fi PNM, CableLabs and their Wi-Fi

Alliance member vendors and operator partners helped create the Wi-Fi Alliance Data Elements program. This program has built a standardized data model that encompass the key performance indicators (KPI's) necessary to remotely troubleshoot Wi-Fi. Standardized troubleshooting reduces CAPEX and OPEX, while spurring innovation in big data analytics.

2 Operator Use Cases and Services Requirements

This section will use in-home Wi-Fi deployment models to establish architecture options (AP deployment), network types and the main use cases to perform an assessment of requirements aimed at further improving the in-home Wi-Fi experience.

2.1 In-Home Wi-Fi Deployment Models

In addition to the home's Private Wi-Fi network, over the past years, Operators have implemented a set of traditional deployment models, while new deployment models are also being considered. The deployment models are served concurrently from the home's Wi-Fi hardware. Each deployment model represents an isolated network that is identified by a Network Name (SSID). We start by highlighting deployment model uses followed by mapping requirements to each deployment model.

Traditional In-Home Wi-Fi Network Deployment Models:

- Private Home Network – fulfils the main consumer use case of providing Internet access to devices in the home.
- Community Wi-Fi – a service provided by the Operator, leveraging home Wi-Fi APs to provide out-of-home Internet access for participating customers. Operators brand the service under different names e.g. Wi-Fi for All, Home Spots, etc.
- Guest Network – allows the customer to establish an additional Wi-Fi network for guests having differing access parameters, and differing connectivity policy, compared to the Private Home Network.
- Content Distribution Network (CDN) – Operators who also provide entertainment services enable an additional SSID to logically separate related traffic to specialized devices (e.g. Set-top Boxes) in the home, to more simply establish end to end QoS.

Potential New / emerging In-Home Wi-Fi Network Deployment Models:

- Utility IOT network – in this case the Operator acts as a Neutral Host with strict isolation and security requirements for Utility traffic.
- Neutral Host - implements a wholesale business model where an Operator enables access to Virtual Operators through the network equipment it has installed at a subscriber's home. e.g. Mobile Offload, IoT On-Boarding, etc.
- Corporate Teleworker - a special case of Neutral Host to enable access to an enterprise network without launching a VPN Client on an employee's device.

It's also possible that many of these deployment models (e.g. Neutral Host, Corporate Teleworker, Utility IOT network, Community Wi-Fi) leverage a common SSID, helping to

alleviate the proliferation of SSIDs in home APs, drawing on station isolation, client authorization based VLAN mapping and station specific RRM/QoS policies.

2.2 Mapping of In-Home Wi-Fi features and Operator requirements to various deployment models

2.2.1 Private Home Network

This is the primary deployment model and provides Wi-Fi access to subscriber's devices in the home.

Category	Features and Operator requirements
Use Case Setup	Always enabled out-of-the-box in Single AP/Multi-AP home network. Home User may choose the Network Name (SSID), Wi-Fi Client Security and credentials, or use the operator specified credentials.
Client On-Boarding	Home user selects network by name, and inputs Credential Home User invokes Wi-Fi Protected Setup™ (Protected Setup) mode and follows connection guidelines Home User invokes Wi-Fi Easy Connect™ (Easy Connect) mode and follows connection guidelines
Wi-Fi Client Security	Recommended: WPA2™ Personal, WPA3™ Personal Not recommended: No Wi-Fi security, WEP, WPA™ Personal
Wi-Fi Easy Mesh support	Supported by Wi-Fi Easy Mesh™ (release 1). Wi-Fi backhaul secured with WPA2 Personal. Ethernet backhaul - no security
Wi-Fi Radio Resource Management (RRM)	Recommended: Wi-Fi Agile Multiband™ and Wi-Fi Optimized Connectivity™: mandates the use 802.11 k/v/u/r to ensure device interoperability for client steering and fast roaming. Easy Mesh: Enables coordinated RRM and client steering in multiple AP networks, via local and cloud-based algorithms Desirable: Cloud based controller to enhance RRM capability used to interface and extend Easy Mesh capabilities by use of Wi-Fi telemetry providing deeper insights than available on a local controller. Additionally, Single AP and Multi AP channel optimization via SON algorithm of Wi-Fi analytics is advantageous vs. local AP's Auto Channel Selection(ACS) in terms of achieving optimal Wi-Fi performance.
Traffic forwarding between Clients	Single AP network: traffic is switched by the AP locally Wi-Fi Easy Mesh network: traffic is switched by Home Gateway (HGW) APs and non-HGW APs. Desirable: Layer 2 policy enforced at APs, which restricts access for certain clients as applied by the customer. E.g. Kids devices can't reach IoT devices
Constraints imposed by operator	Does not apply
Applicable Wi-Fi Alliance Certifications	Wi-Fi 4, 5, 6; WPA2 Personal, WPA3 Personal, Wi-Fi Protected Setup™, Easy Connect, Agile Multiband, Easy Mesh

2.2.2 Community Wi-Fi Network

Prevalent use case, where the operator provides an out-of-home Wi-Fi service by enabling an additional Community SSID from Home Gateways, by tunneling traffic to a services gateway, provides authentication and access to the Internet.

Category	Features and Operator requirements
Use Case Setup	Pre-provisioned by operator: Network name (SSID), Security mode. Home User may have option to opt-in/out.
Client On-Boarding	Operators set the procedure (e.g. Captive Portal or pre-provisioned by operator on subscriber device using operator app)
Wi-Fi Client Security	Not Recommended: No Wi-Fi Security Recommended: WPA2 Enterprise, WPA3 Enterprise with subscriber's User ID/Password and one of Authentication methods (e.g. EAP-SIM, EAP-AKA, EAP-PEAP, EAP-TTLS) or using Passpoint™
Wi-Fi Easy Mesh support	HGW APs: Community Wi-Fi is supported on Home Gateway (HGW) Wi-Fi AP by operator Non HGW APs: While desirable/required by Operators, Community Wi-Fi is currently not supported by Wi-Fi Easy Mesh (R1) on non-HGW APs.
Wi-Fi RRM	Recommended: Wi-Fi Agile Multiband and Wi-Fi Optimized Connectivity: Enables interoperable client steering and fast roaming between Community Wi-Fi APs in different homes. Desirable: Cloud based RRM interfaces and optimizes RRM and client steering capabilities. Channel optimization via SON algorithm is biased towards the private SSID, nevertheless SON RRM will limit interference between adjacent APs in different homes and improve the performance across the Community Wi-Fi footprint.
Traffic forwarding between Clients	Traffic between devices is switched by Wireless Access Gateway (WAG) in operator network
Constraints imposed by operator	Operator may limit throughput per user Operator may limit number of users per Basic Service Set (BSS) (HGW) Operator may enforce QoS prioritization to limit airtime utilization of Community Wi-Fi traffic Operator could add other constraints (e.g. Time based, frequency based, volume based)
Applicable Wi-Fi Alliance Certifications	Wi-Fi 4, 5, 6; WPA2 Enterprise, WPA3 Enterprise, Agile Multiband, Passpoint (future), Wi-Fi Optimized Connectivity™

2.2.3 Guest Network

Emerging use case, whereby the customer will locally configure an additional SSID on the Gateway (GW) or non-GW APs and configure the Guest User's access to local devices and Internet privileges.

Category	Features and Operator requirements
Use Case Setup	Home User enables Guest Network using the AP's user interface (UI). Home User chooses Guest Network Name (SSID), Wi-Fi Client Security and credential.
Client On-Boarding	Guest selects network by name, selects Security mode and inputs Credential Guest invokes Wi-Fi Protected Setup mode and follows connection guidelines Guest invokes Wi-Fi Easy Connect mode and follows connection guidelines
Wi-Fi Client Security	Recommended: WPA2 Personal, WPA3 Personal Not Recommended: No Wi-Fi Security, WEP, WPA-Personal
Wi-Fi Easy Mesh support	Support for Guest SSID across Multi AP environments is required by Operators, however this use case is currently not supported by Wi-Fi Easy Mesh (R1) but can be supported on the HGW.
Wi-Fi RRM	Recommended: Wi-Fi Agile Multiband and WFA's Wi-Fi Optimized Connectivity: Enables interoperable client steering and fast roaming. Wi-Fi Easy Mesh: Enables coordinated Client Steering in multiple AP networks, via local or cloud-based algorithm. Desirable: Cloud based RRM interfaces and optimizes client steering capabilities by use of Wi-Fi telemetry which provide deeper insights than available on local APs. Additionally, Single AP and Multi AP channel optimization via SON algorithm of Wi-Fi analytics is advantageous vs. local AP's ACS (Auto Channel Selection) in terms of achieving optimal Wi-Fi performance.
Traffic forwarding between Clients	Consumer controls Wi-Fi Client access through the APs Configuration UI. It may be desirable to isolate Guest network traffic by disabling local traffic switching while still granting the Guest user access to only specific devices on the Private Home Network (e.g. Printer) Desirable: A further step may be to logically separate Guest traffic, using VLANs and dedicated subnets to provide traffic isolation.
Constraints imposed by operator	Home User may limit number of users, user connection time, throughput per user.
Applicable Wi-Fi Alliance Certifications	Wi-Fi 4, 5, 6; WPA2 Personal, WPA3 Personal, Protected Setup, Easy Connect, Agile Multiband, Optimized Connectivity

2.2.4 Content Distribution Network

A Wi-Fi network which provides dedicated access for an operator's specialized devices in the home, such as set-top-boxes (STB), establishing end to end logical separation, and simplified approach to QoS across Wi-Fi access and broadband access.

Category	Features and Operator requirements
Use Case Setup	Optional: The operator may choose to Pre-provisioned: Network name (SSID), SSID Broadcast/Hidden SSID, Security mode.
Client On-Boarding	Specialized Clients are pre-provisioned with config information and credentials to connect to the network over Wi-Fi
Wi-Fi Client Security	Optional: WPA2 Personal, WPA3 Personal can be used, where the SSID Name and Pre-Shared key are pre-provisioned or configured during the on-boarding process. Recommended: WPA2 Enterprise/WPA3 Enterprise (future) with subscriber's UserID/Password and one of Authentication methods (EAP-PEAP, EAP-TTLS, EAP-TLS) - to be verified
Wi-Fi Easy Mesh support	Wi-Fi Easy Mesh (R1), provides support from the Home Gateway only
Wi-Fi RRM	Recommended: Wi-Fi Agile Multiband and Wi-Fi Optimized Connectivity: mandates the use 802.11 k/v/u/r to ensure device interoperability for client steering and fast roaming. Wi-Fi Easy Mesh: Enables coordinated RRM and client steering in multiple AP networks, via local and cloud-based algorithms Desirable: Cloud based controller to enhance RRM capability used to interface and extend Easy Mesh capabilities by use of Wi-Fi telemetry providing deeper insights than available on a local controller. Additionally, Single AP and Multi AP channel optimization via SON algorithm of Wi-Fi analytics is advantageous vs. local AP's ACS (Auto Channel Selection) in terms of achieving optimal Wi-Fi performance. The specialized device i.e. STB, is managed by the operator using device management protocol (e.g. TR-069) and intelligent AP selection may further enhance performance.
Traffic forwarding between Clients	The operator may desire that such traffic is logically separated from the Private SSID, with no local switching capability. However, the SSID may be used for device on-boarding only, in which case, then local traffic switching is supported and the operator may enable traffic forwarding between some device categories (e.g. DVR and STB)
Wi-Fi Performance constraints imposed by operator	Key driver for Operators is to provide preferential QoS to these specialized devices with the aim of assuring video distribution over Wi-Fi. Operators may draw upon 802.11 standard approach Wi-Fi Multimedia™ (WMM (802.11e)), or by proprietary means of scheduling 802.11 MAC Layer resources to allocate commensurate air time to the respective end points. Furthermore, service awareness enhances Wi-Fi policy enforcement, to align client steering and channel selection policy to avoid service interruptions and determine that sufficient capacity is available.
Applicable Wi-Fi Alliance Certifications	WI-Fi 4, 5; WPA2 Enterprise, WPA3 Enterprise, Agile Multiband, Passpoint (future), Optimized Connectivity

2.2.5 Neutral Host (e.g. Mobile Offload)

Operators, acting as a Neutral host, provide visited network facilities, whereby customers of participating wholesale Operators are given Wi-Fi access, by means of a secure SSID or Hotspot 2.0/ Passpoint enabled on the home gateway, and proxying authentication back to the respective home operator, with Internet access routed via the visited Operators network, or via the home network operator, using tunneling.

Category	Features and Operator requirements
Use Case Setup	Host operator establishes visited network facility, configures wholesale operator SSID / Hotspot 2.0 on Home Gateways, and establishes proxy for authentication traffic and data traffic to reach the wholesale operator's core network.
Client On-Boarding	The wholesale operator is responsible for provisioning customer devices using well known procedures (e.g. MNO can update carrier file, or an App can be used to configure the handset with certificates and credentials
Wi-Fi Client Security	WPA2 Enterprise/WPA3 Enterprise (future) with subscriber's UserID/Password and one of Authentication methods (EAP-PEAP, EAP-TTLS) or EAP-SIM/AKA or Passpoint
Wi-Fi Easy Mesh support	Easy Mesh (R1) supports such use cases via the Home Gateway only. Nonetheless this is a requirement for Operators on non-Home Gateway APs as well.
Wi-Fi RRM	Recommended: Wi-Fi Agile Multiband and Wi-Fi Optimized Connectivity: enables interoperable client steering and fast roaming between Wi-Fi APs configured as Neutral hosts, which may lie in different homes. Desirable: Cloud based RRM may be used to influence and optimize client steering capabilities. Channel optimization via SON algorithm is biased towards the private SSID, nevertheless SON RRM will limit interference between APs in different homes, and improve the performance across the Neutral Host Wi-Fi footprint
Traffic forwarding between Clients	Traffic forwarding between clients is always disabled by Operators. There exist 2 Internet Access models 1) Traffic is forwarded by Trusted Wireless Access Gateway (TWAG) in operator network to Wholesale operator core network, for Internet routing 2) Traffic is routed via the Neutral Host WAG to the Internet
Constraints imposed by Operator	Neutral Host operator will apply constraints to bias the Private SSID, agreed to with the Wholesale operator: • Operator may limit throughput per user • Operator may limit number of users per BSS (HGW) • Operator may enforce QoS prioritization to limit airtime utilization of Community Wi-Fi traffic. • Operator could add other constraints (e.g. Time based, frequency based, volume based)
Applicable Wi-Fi Alliance Certifications	Wi-Fi 4, 5; WPA2 Enterprise, WPA3 Enterprise, Agile Multiband, Optimized Connectivity, Passpoint

2.2.6 Corporate Teleworker

Operator provides a visited network facility for an enterprise service to be extended via the home APs, and the related authentication traffic and data traffic is proxied to the respective enterprise's back office, with the operator providing aggregation services.

Category	Features and Operator requirements
Use Case Setup	Host operator establishes visited network facility, configures Enterprises SSID / Hotspot 2.0 on the respective employees Home Gateways / APs only, and establishes proxy for authentication traffic and data traffic to reach the enterprise's back-office network.
Client On-Boarding	The user's respective enterprise / employer is responsible for provisioning customer devices using via an App to configure the handset with SSID, realm, certificates and credentials
Wi-Fi Client Security	WPA2 Enterprise/WPA3 Enterprise with subscriber's UserID/Password and one of Authentication methods (EAP-PEAP, EAP-TTLS)
Wi-Fi Easy Mesh support	Easy Mesh (R1) supports such use cases via the Home Gateway only. Nonetheless this is a requirement for Operators.
Wi-Fi RRM	Recommended: Wi-Fi Agile Multiband and Wi-Fi Optimized Connectivity: Enables interoperable client steering and fast roaming between Wi-Fi APs within the same home. Desirable: Cloud based RRM may be used to influence and optimize client steering capabilities. Channel optimization via SON algorithm is biased towards the private SSID, and expectation is that the Corporate Teleworker SSID will be enabled within the employee's respective home only – not across an operator's footprint.
Traffic forwarding between Clients	Traffic forwarding between clients is always disabled by Operators. Traffic is forwarded by Trusted Wireless Access Gateway (TWAG) in operator network to enterprise operator core network, for Internet routing
Wi-Fi Performance constraints imposed by operator	The host operator will apply constraints to bias the Private SSID, agreed to with the enterprise operator: • Operator may limit throughput per user • Operator may limit number of users per BSS (HGW) • Operator may enforce QoS prioritization to limit airtime utilization of Community Wi-Fi traffic. • Operator could add other constraints (e.g. Time based, frequency based, volume based)
Applicable Wi-Fi Alliance Certifications	Wi-Fi 4, 5; WPA2 Enterprise, WPA3 Enterprise, Agile Multiband, Optimized Connectivity, Passpoint

2.2.7 Utility IOT Network

Operator provides a visited network facility for a Utility company to access and manage meters (Gas, Electricity, Water, and Security) or gain access to other sensors and assets within the customer's home, by relaying authentication traffic and data traffic to the Utility Company's respective enterprise's back office systems.

Category	Features and Operator requirements
Use Case Setup	Host operator establishes visited network facility, configure Utility SSID / Hotspot 2.0 on the respective employees Home Gateways / APs only, and establishes proxy for authentication traffic and data traffic to reach the respective Utility company's Back Office network.
Client On-Boarding	The Utility is responsible for provisioning customer devices with SSID, certificates, realm, and credentials, to reach their respective network.
Wi-Fi Client Security	WPA2 Enterprise/WPA3 Enterprise with subscriber's UserID/Password and one of Authentication methods (e.g. EAP-SIM, EAP-PEAP, EAP-TTLS)
Wi-Fi Easy Mesh support	Easy Mesh R1 supports such use cases via the Home Gateway only. Nonetheless this is a requirement for Operators.
Wi-Fi RRM	Recommended: Wi-Fi Agile Multiband and Wi-Fi Optimized Connectivity: Enables interoperable client steering and fast roaming between Wi-Fi APs within the same home. Desirable: Cloud based RRM may be used to influence and optimize WFA client steering capabilities. Channel optimization via SON algorithm is biased towards the private SSID.
Traffic forwarding between Clients	Traffic switching between Utility IOT devices is not allowed.
Wi-Fi Performance limitations imposed by operator	Operator controls number of Utility IOT devices per Home, throughput per home based on agreement with Utility company.
Applicable Wi-Fi Alliance Certifications	Wi-Fi 4, 5; WPA2 Enterprise, WPA3 Enterprise, Agile Multiband, Optimized Connectivity, Passpoint.

2.3 Current Gaps

Wi-Fi has been the subject of significant transformation in recent years led by standards groups, IEEE, Wi-Fi Alliance, Wireless Broadband Alliance, BBF, along with CableLabs and many industry players, materially improving performance, and interoperability, and fuelling its mass adoption. In-Home Wi-Fi lags in its ability to adopt recent standards as Operators and their OEM partners are dependent on the mass commoditization of Wi-Fi components to offer consumers advanced CPE solutions at competitive price points. The enterprise segment, being less economically constrained, has, more or less, taken full advantage of standardization and resulted in broad support for key use cases and deployment models.

In-Home Wi-Fi on the other hand, must innovate in a way which delivers on the performance and interoperability requirements, but at the right price, which leaves a number of gaps being undertaken by industry bodies.

2.3.1 Cloud RRM

As Multi-AP solutions take hold, they will further contribute to greater AP density in residential settings, and the importance of centralized coordination of radio resources, to optimize Wi-Fi performance, by intelligently managing the Wi-Fi channel, and orchestrating client device steering policy will become mandatory. Today in MDUs (Multi Dwelling Units) customers are exposed to numerous uncoordinated SSIDs / BSSIDs and ever-changing channel configuration, resulting in the inefficient use of spectrum and this effect will become equally dominant in urban, suburban and rural context over time. While Operators are moving to adopt closed RRM solutions for their own footprint of APs, the coordination between Operators seems far-fetched at this point in time, but perhaps presents a gap in maximizing efficient use of spectrum? Easy Mesh (R1) and the Wi-Fi Alliance Data Elements provide the framework for coordinated Cloud RRM but agreeing on the RRM algorithms themselves amongst industry peers could also further enhance the potential of in-home Wi-Fi, enabling Operators to adopt the optimal RRM approaches.

2.3.2 Separation of Multiple SSIDs in Multi-AP (Mesh) Environments

Easy Mesh (R1) lacks full support for secondary SSIDs in Multi-AP environments. While there is support for multiple SSIDs, there is no defined method for providing logical separation of a secondary SSIDs traffic. This has led to vendors using a variety of protocols to support this requirement, from VPNs, GRE (Generic Routing Encapsulation), and VLAN.

2.3.3 Ethernet Backhaul security in a Multi-AP Environment

Additionally, Easy Mesh (R1), does not provide a secure means of backhauling an SSID's traffic over Ethernet. For example, Community Wi-Fi makes use of GRE tunnels to isolate traffic from the Home GW to the Wireless Access Gateway (via the Broadband Access Network), however, enabling the Community Wi-Fi SSID from non-HGW APs, presents a security risk, in that traffic could be intercepted and user sessions compromised, on the LAN side of the HGW.

2.3.4 Better Onboarding experience

Setup of the Multi-AP network, including both the HGW and non-HGW APs must be zero touch to the customer. Today this is solved for using Wi-Fi Protected Setup (WPS) or proprietary provisioning, perhaps using a Smart Phone app, conceived by vendors or Operators but is often not zero touch. This issue extends to Wi-Fi devices, and especially IoT devices, which in many cases lack a screen, presents an on-boarding challenge and a

customer experience hurdle which the operator bears the fall-out, in dealing with more calls & trucks. EasyConnect contains some possible solutions and should be leveraged to reduce the touch points for the customer.

2.3.5 QoS (Traffic Prioritization)

While there are standardised methods to provide traffic prioritisation such as Wi-Fi MultiMedia (WMM), Operators require a means to ensure that 1st party devices, such asSTB's, which are more and more Wi-Fi connected, are given adequate air time to support video streaming services. Equally, where there are multiple SSIDs, the Operators will seek to bias the customer private SSID over community SSID, and WMM is insufficient, so a blunter instrument is required.

3 Deployment / Architecture options

In the home, the two basic architectures for hardware deployment are Single AP and Multi-AP, discussed in the following sections.

3.1 Single AP

In this type of deployment, a single AP provides coverage in the whole home. The AP provides broadband access to the user (i.e., supports the broadband interface into the Internet), and provides Wi-Fi coverage to user devices in the home. This deployment type is typically sufficient for smaller or medium-sized homes, especially single-level, multi-dwelling units. Even with a single AP, the different radios on the AP can be used to balance between capacity and coverage. For example, devices with strong coverage can be placed on the 5GHz radio to obtain maximum bandwidth; devices with weaker coverage can stay on 2.4GHz, which has a longer coverage range. This single AP architecture is presented in **Figure 1**.

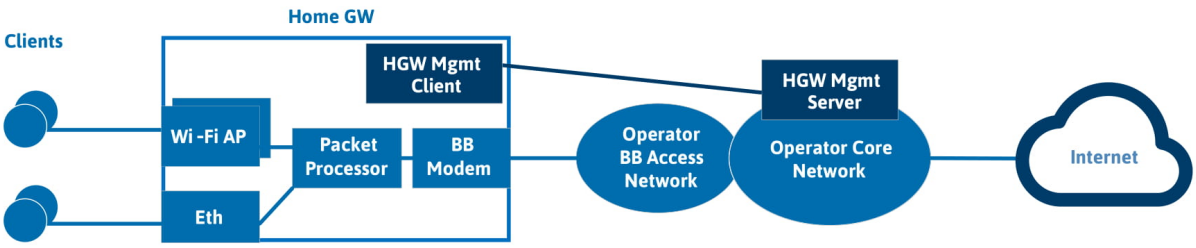

Figure 1. Single AP Network Entities

3.2 A Multi-AP Network

In a multi-AP home network, a primary AP provides broadband access, i.e. is the interface to the Internet. Additional secondary or extender APs can be deployed to provide broader coverage in the home. The extender APs connect to the Internet via the primary AP, using wired, PLC (Power Line Communication), Ethernet, MoCA (Coax Connection), or Wi-Fi backhaul connections to the primary AP. All APs, including the primary AP, provide Wi-Fi coverage to devices in the home. This type of architecture is suitable for larger homes, especially multi-level dwellings.

In a multi-AP network, APs are placed strategically within the home to optimize Wi-Fi coverage and to minimize the presence of coverage gaps. To that aim, AP placement is a critical task in this kind of deployment. Users must be assisted to perform this operation, either via truck roll, or self-care tools provided by the operator.

In the case where Wi-Fi is used for backhaul that is shared with Client fronthaul access, the channel management scheme must take into account backhaul bandwidth needs, in addition to the needs of devices connecting on the fronthaul access side. Client steering schemes are required to move devices automatically between APs, as they first associate and later move around the house. Additionally, APs in this architecture must support optimal inter-AP routing, i.e. be able to route data packets over the best links to and from the Internet ingress / egress point (i.e. the primary AP).

In a multi-AP network, we find different architectures to enable Radio Resource Management (RRM) procedures. For instance, **Figure 2** presents the scenario where all the RRM actions take place locally within APs, with no centralized cloud functions. This architecture facilitates a more rapid response to changing RF conditions, however, acts on less data to make RRM decisions. Meanwhile **Figure 3** introduces the scenario where the RRM procedures occur at a cloud-based location in a centralized approach. Finally, **Figure 4** presents an overall hybrid approach, where actions can happen both locally and at cloud side. For example, real-time decisions such as Dynamic Frequency Selection (DFS) are controlled locally, while long-term decisions of capacity optimization could be handled by a cloud Controller.

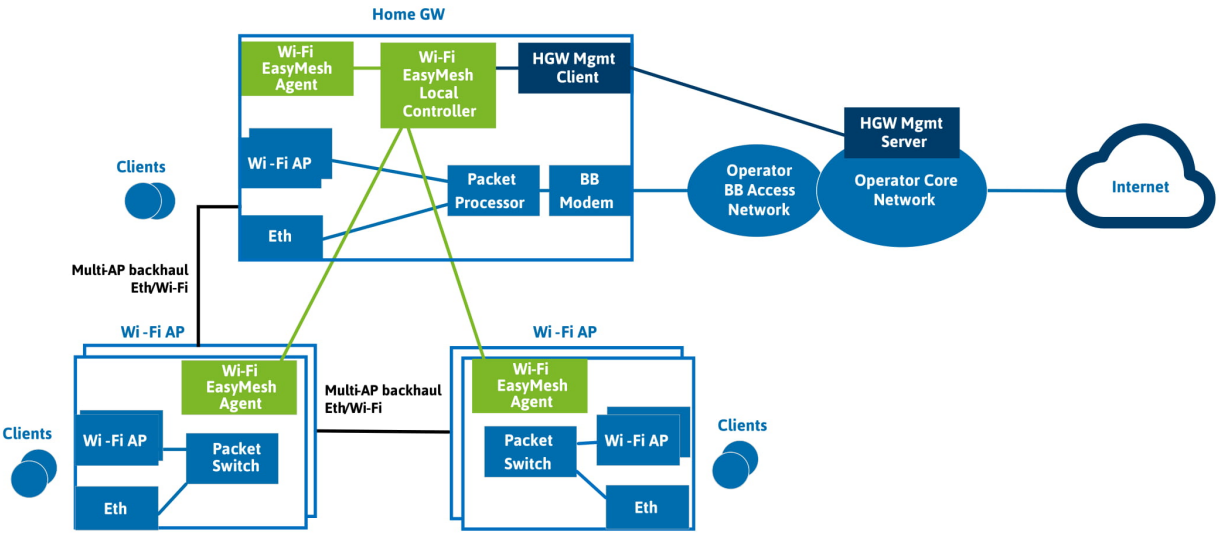

Figure 2. Multi-AP Network Entities in with a local RRM approach

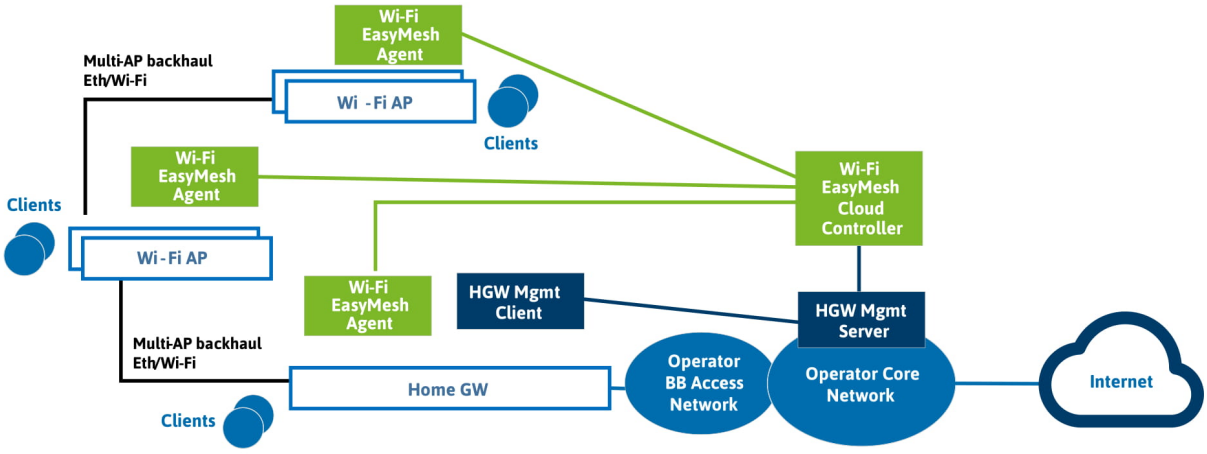

Figure 3. Multi-AP Network Entities in a cloud RRM approach

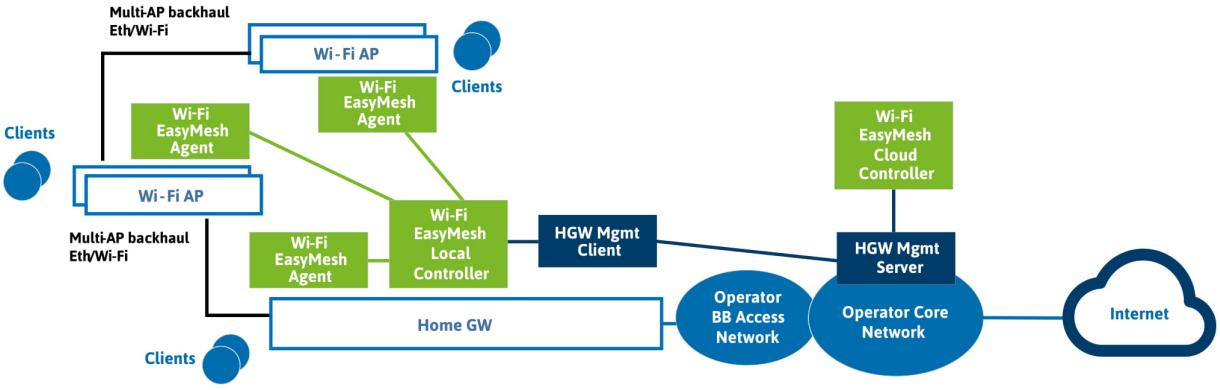

Figure 4. Multi-AP Network Entities in a hybrid RRM approach

4 Guidelines / Recommendations

4.1 End-to-end security

4.1.1 In-Home Security Threats and Security Attack Vectors

Security attacks on In-Home Wi-Fi networks seek to compromise customers sensitive information as they are connected to internet services, by installing malware, or by mounting (Distributed Denial-of-Service (DDOS) attacks using In-Home network computing resources. Cyber, physical and adjacent security attacks are the most serious security threats for the In-Home network.

Cyber-attacks are initiated by malware installed on home network devices using known software exploits. Cyber-attacks are mitigated, or better, prevented, by good hardware and software design practices, strong authentication and well considered privacy policy and timely device software upgrade procedures.

Physical security attacks are associated with an In-Home attacker tampering with hardware or software of the network equipment installed by the operator.

An adjacent attack consists of gaining access and visibility of the Home APs Wi-Fi traffic, either private or Community Wi-Fi/Neutral Host traffic passing through the In-Home network over Ethernet or Wi-Fi. These are generally known as man in the middle attacks, where a would be attacker spoofs the GW, and draws on known attack vectors to compromise devices as they consume internet services (e.g. 2017 KRACK vulnerability)

Mitigating or preventing security attacks on in home networks requires the operator to supervise local and Internet bound flows for malicious activity. The best practices to avoid attacks include: implementing a set of hardware and software design guidelines, using strong authenticated Wi-Fi link layer security, protecting unencrypted communication between

Access Points and Residential GW with additional layer of security or relocating privacy functionality of the Community Wi-Fi/Neutral Host traffic from In-Home Wi-Fi Access Points to the secured environment in the operator's network. Additionally, Operators may seek to implement a security agent within their managed APs, to monitor for abnormal behavior, and offer the customer the ability to block such traffic.

In Figure 5 we illustrate potential security attack vectors that can apply to different entities in the In-Home network.

- Devices: Client devices, Wi-Fi Access Points and Home Gateway
- Links: Client - Wi-Fi AP and backhaul (between Wi-Fi APs/Home GW)
- Control and Management connection between Wi-Fi Easy Mesh Agents and Controller

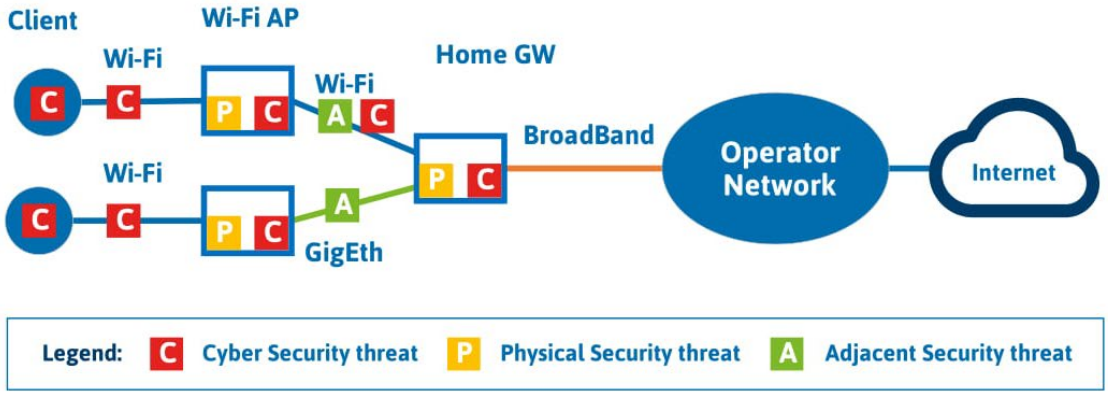

Figure 5. In-Home Cyber and Physical Security threat attack vectors

4.1.2 Wi-Fi Client to Wi-Fi AP link protection

Wi-Fi client to Wi-Fi AP link protection is achieved through combination of strong Wi-Fi authentication and privacy. It is recommended to deploy WPA2 or WPA3 Enterprise security for Community Wi-Fi/Neutral Host connections and use WPA3 Personal Security for Home and Guest network use cases, as well as the use of Wi-Fi EasyConnect to provision IoT devices.

4.1.3 Multi-AP Backhaul link protection

As we saw in the use case discussion (Section 2) Multi-AP backhaul protection for In-Home is not well supported by standards, and subject to operator and vendor proprietary implementations. The home traffic and community Wi-Fi/neutral host traffic on Wi-Fi AP links can be exposed to cyber security, and adjacent security attacks:

- Lack of isolation (logical separation) between traffic that belongs to different SSIDs/Use cases transported over Wi-Fi backhaul link: backhaul link is protected with WPA2-Personal security, using Passphrase set by home user or the operator. However, Easy Mesh supports separate fronthaul and backhaul SSIDs which can have different passphrases; the latter should be generated by the Controller (e.g. randomly generated, long high entropy) to strengthen backhaul security.
- All traffic is transported without a specific security mechanism over Ethernet links

If the Operators wish to deploy Easy Mesh (R1) and needs to use Public SSIDs across APs in that network beyond the Gateway, then they need to add proprietary features on all those APs. One method (shown in Figure 6) is to add a strong security layer (authentication and privacy) to the traffic belonging to a specific Community Wi-Fi use case/SSID that is transported over backhaul link. In section 6.1 (Future Evolution) we discuss a new architectural approach termed Cloud WPA.

Further options to secure Community Wi-Fi / Neutral host traffic on non HGW APs is to add a security layer over backhaul links. Using MACSec or implementing secured IPSec or DTLS tunnel from Wi-Fi AP to the service gateway residing in the operator's network/datacenter is one solution that has been implemented in Enterprise and Public Wi-Fi products.

A further consideration for enhancing security for Community Wi-Fi / Neutral host, which currently use non-encrypted GRE tunneling, requires overcoming a limitation in today's Home GW APs. To achieve performance of 10's to 100's Mbps of Community Wi-Fi/Neutral Host traffic, the Wi-Fi APs will have to include hardware accelerator for encryption integrated with the packet processor.

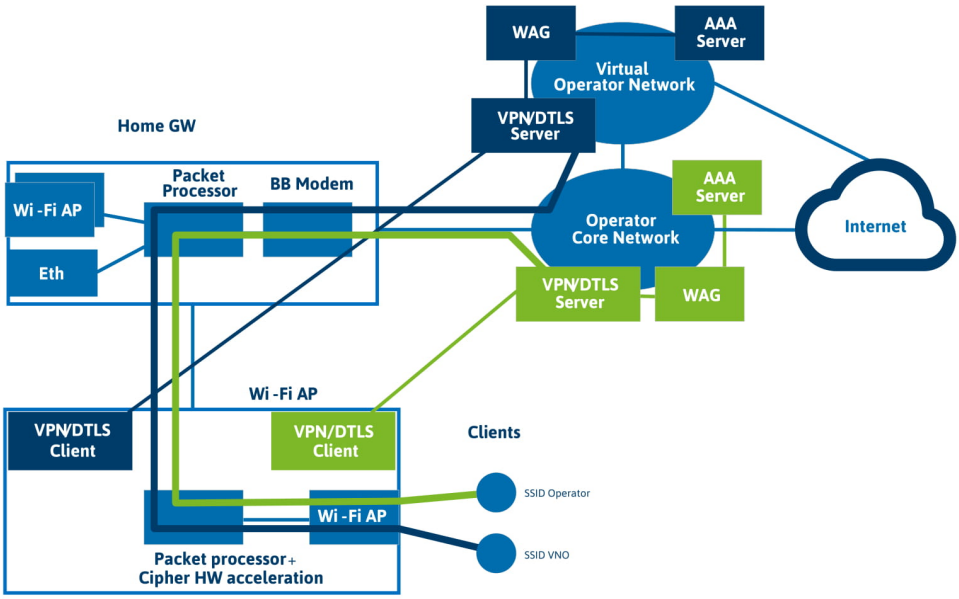

Figure 6. Protect multi-AP backhaul with additional security layer

4.1.4 Multi-AP Control and Management connection between Agents and Controller protection

Protecting the Control and Management connections between Wi-Fi Easy Mesh Agents and Controller is critical. To that aim we propose as an enhancement for future versions of the Easy Mesh standard using strong authentication and Security, such as TLS or DTLS, mutually authenticated with unique client-side certificates.

4.1.5 Operator Network protection

Security threats and protection in the operator network are not unique to the Home and are addressed in other WBA documents as well [1], [2]. This applies to security assessments Operators will carry out in implementing Cloud RRM or other device management platforms (i.e. TR-69, WebPA).

4.2 Coordination of radio usage or RRM

4.2.1 RRM Features

In the following sections, we define the RRM features that are important for In-Home Wi-Fi networks, especially those that contain multiple APs.

4.2.1.1 Band steering (Intra-AP steering)

The goal of band steering is to move clients from a congested radio on an AP to the other radio on the same AP, or to balance load across the two radios, while still providing the required capacity to all devices. For example, if the 2.4GHz channel on an AP is congested, clients on 2.4GHz can be moved to 5GHz to alleviate congestion.

The current standards that can be used for band steering of clients are IEEE 802.11 and Wi-Fi Agile Multiband™. Agile Multiband (which leverages IEEE802.11v features) provides a ranked list and steers 802.11v/MBO (Multiband Operations) devices using a BSS Transition Management (BTM) Request. Agile Multiband also defines deterministic client behaviour upon receipt of a BTM request. Easy Mesh uses this same BTM for steering but it also identifies and handles legacy (non-11v/Agile Multiband) devices, that cannot be steered using BTM Requests, by forcing disassociation/deauthentication and suppressing probes.

The following are typical conditions and recommendations for steering clients (from the source radio to the target radio):

- The source radio's channel is congested, e.g. channel utilization exceeds a prescribed threshold.
- The target radio has sufficient available headroom to accommodate the load from the clients being moved.
- Care should be taken to ensure that each client being moved will have good enough coverage on the target radio.

- Agile Multiband should be leveraged to steer a client to one of a targeted set of radios. Using Agile Multiband, the client is provided with a ranked list of radios to move to. Non-11v/Agile Multiband compatible clients can also be supported with Agile Multiband as Agile Multiband APs will identify the capabilities of each client and will steer legacy clients using disassociation/deauthentication and probe suppression.
- The band steering mechanism should be designed to minimize disruption to ongoing connections and data traffic.
- Agile Multiband defines deterministic behaviour of clients when certain types of BSS Transition Management Requests are received, allowing a network to efficiently steer them.

4.2.1.2 AP Steering (Inter-AP Steering)

The goal of AP steering is to steer a client to the best AP, whether that is the AP with a better RSSI (Received Signal Strength Indication) or an AP with a better capability of serving the client (e.g. due to lower airtime utilization, greater backhaul capacity). While band steering happens between radios on the same AP, AP steering happens between radios on different APs.

The same standards used for band steering apply for AP steering: IEEE 802.11v, Agile Multiband and Easy Mesh.

Another type of steering that can be helpful in the home is network steering of devices to the private SSID (e.g. if the device comes into the house and chooses to stay on the Community Wi-Fi SSID instead of the private SSID, both served from the home APs). In this case, the AP using available steering mechanism, will not allow for the AP to join the Community SSID.

The following are typical conditions and recommendations for steering clients (from the source AP to the target AP):

- Appropriate coverage (e.g. signal strength) thresholds should be applied to detect poor coverage for a client device, also noting that uplink and downlink RSSIs may be very different due to DL/UL transmit power imbalances between APs and the client.
- Agile Multiband should be leveraged to steer a client to one of a targeted set of radios. Using Agile Multiband, the client is provided with a ranked list of radios to move to. Non-11v/Agile Multiband clients can also be supported with Agile Multiband as Agile Multiband APs will identify the capabilities of each client and will steer legacy clients using disassociation/deauthentication and probe suppression.
- The client steering mechanism must be designed to minimize disruption to ongoing connections and data traffic.
- Hysteresis should be applied to ensure clients are not steered too frequently.
- Checks should be done to ensure the target AP is not congested.
- Network steering should take into account that client devices implement their own roaming algorithms, and the objective of network steering should be to support / backup those mechanisms (e.g. push client to roam if it does not do so on its own).

- Sticky clients (i.e. clients that do not respond to client steering requests and stay on the same radio) should be detected and handled appropriately (e.g. choose not to steer clients that have repeatedly not responded to steering requests). Easy Mesh provides feedback on client steering responses and results to the Controller to help it identify such cases.
- Agile Multiband defines deterministic behaviour of clients when certain types of BSS Transition Management Requests are received, allowing a network to efficiently steer them.
- The system should be able to detect whether a steering action is successful or not, i.e. whether the client has moved to the target radio. Steering analytics should be provided that provide the operator visibility into steering actions taken and success rates. Again, Easy Mesh provides feedback on client steering responses and results to the Controller to help it identify such cases. In the end, there should not be a negative impact on the customer experience due to network-initiated steering.

4.2.1.3 Channel selection management

Channel management is used to mitigate congestion, noise and interference in a real-time fashion, and to optimize Wi-Fi operation. A congested channel results in poor Wi-Fi performance, often showing up in the form of high retry rates, reflected in key KPIs – high latency and jitter, low throughput etc.

The goal of channel management is to move an AP's radio from a congested channel to a more optimal one. Channel management should include the following functionalities:

- Channel management should take place (a) on AP restart, to select the best channels available; and (b) periodically, in response to changing congestion / interference / noise conditions.
- A candidate channel evaluation mechanism (i.e. Off Channel Scan) to assess channels other than the one the radio is currently on (i.e. non-operating channels). This can be done by the radio in the background during normal operation, to determine candidate channels to switch to if needed.
- A trigger mechanism to determine whether a change of channel is needed. This should be done by examining congestion / noise / interference metrics to determine whether the radio's current channel conditions are poor enough to warrant a channel change.
- If the algorithm decides a channel change is needed, it should leverage the candidate channel information to select an optimal channel to switch to, also taking into account the channels (OpClasses) that associated client devices actually support. This is something that Agile Multiband can gather from client devices (i.e. client support for 2.4GHz channel 13, or 5GHz DFS Channels).
- Channel selection may be constrained in a multi-AP scenario where the fronthaul and backhaul of an AP share a radio. Easy Mesh allows Controllers to gather this kind of information.
- The Channel Switch Announcement (CSA) capability (based on 802.11h) must be used, to steer connected clients to the AP's new channel without disruption.

- The channel change mechanism must be designed to minimize disruption to ongoing connections and data traffic.
- Channel management should handle scenarios where there are changes in noise. In such a scenario, the system can pick any available alternate channel. However, short bursts of interference/noise may not be a good criterion for changing channels.
- Hysteresis should be used to ensure that a radio's channel is not changed too often, and that not too many APs in a neighbourhood undergo channel changes at one time. Widespread channel changes can have ping-pong and ripple effects through the system and can compromise system performance.
- For 802.11ac (on 5GHz), channel management must handle bonded operation, i.e. the use of 40, 80 and 160 MHz bonded channel configurations. In these cases, channel management must be able to select the best channel set to operate on, as well as the optimal primary channel to use within the channel set. The 802.11ac recommendation of aligning primary channels of overlapped bonded BSSs should be followed.
- Channel management analytics (e.g. channel change histories, success rates, performance improvement, reduction in interference etc.) should be available to the operator.
- Operational parameters for channel management, i.e. thresholds, frequency of operation etc. should be configurable by the operator.

4.2.1.4 QoS Management

QoS management provides latency-sensitive, or other designated important, traffic priority handling through the network. QoS management should provide the following:

- System should support handling and mapping of Differentiated Services Code Point (DSCP) markings from operator to Wi-Fi Multimedia (WMM) Access Categories (ACs).
- System should support mirroring of QoS between DL and UL streams.
- APs should support WMM

4.2.1.5 Airtime Management

The goal of airtime management is to apportion Wi-Fi airtime in a desired fashion across SSIDs and client devices. Airtime management should be supported at two levels:

- Across SSIDs, e.g. across a Public SSID and a Private SSID, potentially to ensure that the Private SSID's quality of service is not compromised.
- Across client devices, to ensure a desired apportioning of Wi-Fi bandwidth across clients.

Inter-SSID airtime management should support the following:

- Allocation of airtime (e.g. percentage values) across the operational SSIDs.
- Queueing scheme should be supported, i.e. allocation of airtime to the SSIDs by the AP strictly as per the configured airtime allocations.
- Fair queueing scheme should be supported, i.e. reallocation of unused airtime (by one or more SSIDs) to other SSIDs to ensure airtime is used optimally overall.
- Monitoring capability to enable the operator to monitor actual airtime allocation and usage.

Client level airtime management should support the following:

- Allocation of airtime (e.g. percentage values) across client devices.
- Strict queueing scheme should be supported, i.e. allocation of airtime to clients by the AP strictly as per the configured airtime allocations.
- Fair queueing scheme should be supported, i.e. reallocation of unused airtime (by one or more clients) to other clients to ensure airtime is used optimally overall.
- Monitoring capability to enable the operator to monitor actual airtime allocation and usage.

4.2.1.6 AP Transmit Power management

Power management in a Wi-Fi system should achieve two goals:

- Real-time AP Transmit power adjustments to optimize coverage, capacity and performance.
- Power reduction to reduce interference / congestion and possibly, improve performance.

Power management to optimize coverage, capacity and performance needs to factor in the level of coverage an AP is providing to its clients, e.g. what signal strengths / Signal-to-Noise (SNR) levels a critical mass of its clients is experiencing.

In dense deployment environments with potentially high interference, power reductions may be applied to reduce interference. This must be balanced with the need to provide individual clients good coverage. In addition, in the case of Overlapped BSS (OBSS) interference, a trade-off between same-network co-channel multi-AP operation vs. neighbouring networks (e.g. in an MDU) should be taken into account.

Operational settings for power management must be configurable by the operator. In addition, the operator must have the ability to manually set / change an AP's transmit power level via the operations interface.

4.2.1.7 Topology Setup and Self-Healing

In a multi-AP deployment, the following topology self-provisioning and self-healing capabilities should be supported:

- When Wi-Fi backhaul is used, and in the absence of a dedicated Backhaul radio, the system should select the best radio (e.g. 2.4 or 5 GHz) for backhaul connectivity between a primary and secondary AP (primary and extender), or between extender APs in a daisy-chain or mesh configuration. Dedicated backhauls radios could be an area in which the anticipated 6 GHz spectrum could be very useful.
- When Wi-Fi backhaul is used, the system should be able to switch the radio used for backhaul (e.g. 2.4 or 5 GHz) based on performance. For example, if the backhaul exhibits poor performance or becomes unavailable, the system could automatically switch to another radio for the backhaul.

- If an extender AP's connectivity to its upstream AP is unavailable, the extender AP must be able to route through a different AP to the gateway to ensure connectivity and data service are maintained.

4.2.2 RRM Implementation Location Options

Radio Resource Management features can be grouped into two main "timing" categories: real-time, policy enforcement aligned with LAN side events and non-real-time, policy governing Wi-Fi system configuration. For example, steering (Band and AP) needs to happen in real-time corresponding and in response to the movements of the clients in the network. Channel selection, as another example, however, would only need to happen at a frequency that would depend on determination that a problem has arisen, and might only happen once per day, or even less frequently.

These timing categories influence the location where it makes sense to implement each RRM feature. For example, non-real-time features could easily be implemented in a cloud-based control function as any latency would not affect the feature performance. Real-time feature performance is heavily dependent on low-latencies between the control function and the APs in the home. Low-latencies are not an issue if the feature is implemented in the local Gateway or an AP. However, if implemented in the cloud, real-time features require a low-latency cloud connection. Easy Mesh allows RRM features to be implemented either locally or in the cloud.

The next sections explain more about the different implementation location options for RRM algorithms.

4.2.2.1 Cloud-based

For many of the Wi-Fi RRM functions, cloud-based location of the RRM algorithms makes sense. A centralized approach may be better to support procedures that work across APs from different manufacturers and across different home networks. A cloud-based approach is able to coordinate across different APs (with different chipsets) more effectively.
For example, multiple APs in a home or an MDU with different chipsets could have different RRM approaches. For one thing, the way these APs change channels, bands, power levels etc. could be quite different – one platform could be aggressive, the other conservative.
A cloud-based solution can harmonize this operation and offer a better coordinated experience compared with an AP-based one.

A centralized approach can also drive a much more holistic RRM strategy, taking into account a collective "neighbourhood" view of the APs involved. A controller-based solution, on the other hand, would tend to optimize for its own AP, potentially without having control over the other APs, especially APs with different chipsets. A cloud-based approach has more historical information and may be better at making the best RF optimization decisions, aggregating information across all APs in a given neighbourhood when these networks are operated by the same operator. It can take action on one AP, knowing exactly what other

APs are doing, knowing the impact of the change on other APs, and what the algorithm intends to do with the other APs. If the homes in the neighbourhood are managed by different Operators, there may still be some advantage derived from collecting the knowledge from the APs managed by the operator. This aggregation is what the Wi-Fi Alliance Data Elements work area is looking to enable.

A cloud-based algorithmic location is beneficial for RRM functions that can benefit from a holistic macro network view across multiple homes, i.e. channel management, power control or inter-AP steering.

4.2.2.2 AP/Gateway-based

Certain RRM functions can benefit from being located on a local Gateway or AP. These are algorithms that need to act in rapid response to changing RF conditions. Examples of these are band and client steering functions, whose execution is better located in the Gateway/AP (although configuration and policy can come from the cloud server). These functions are also likely to be more frequently executed than channel management functions for example; hence locating the execution of these in a local AP or in the Gateway also reduces control traffic requirements between the Gateway/AP and cloud server.

Also, mirroring of RRM functions that may make sense to be in the cloud, onto the local Gateway/AP, allows for these functions to continue to operate in the case of a cloud control outage.

4.2.2.3 Hybrid-based

An overall hybrid approach is also practical. This includes locating functions that do not need low-latency connections between the actors (AP) and the algorithm in the cloud, whilst positioning frequently executed, fast-acting functions in the AP. It can also make sense to mirror some cloud functionality locally for redundancy purposes.

4.3 Onboarding Devices

4.3.1 AP Onboarding

Onboarding capabilities must include the ability to seamlessly bring on board end user devices as well as APs deployed on customer premises.

4.3.1.1 Operator Provided APs

AP onboarding must be close to zero-touch from an end user perspective. For operator provided devices this is possible with operator pre-provisioning of new APs prior to shipment to the end user.

4.3.1.2 Retail Purchased APs

Practically speaking, some level of light-touch / user control in onboarding is unavoidable for retail purchased APs. At the very least, the user may need to flag to the management system that a new AP has been added. Users could scan a barcode on a new AP using the operator's app linked to the existing network management system / controller. Also, the operator can provide an online portal where the user enters device IDs to register devices. Hence, onboarding will, by its very nature, involve a hybrid approach – mostly zero-touch, but with some user control added.

4.3.2 Client Device Onboarding

The Wi-Fi management system must also provide means for onboarding end user client devices and operator provided/managed client devices. This is necessary from multiple angles:

- Enable new devices to seamlessly connect to the network and access Wi-Fi service
- Enable operator to control what devices are allowed to connect to the network
- Prevent unauthorized use of a Wi-Fi network, e.g. prevent a user from connecting their device to a neighbour's Wi-Fi network and, in effect, accessing "free" service
- Enable the operator to control operator provided/managed devices and provide them with the appropriate quality of service.

As with APs, onboarding of operator provided/managed client devices can be made zero-touch by having the devices pre-provisioned Zero-touch (or light-touch) onboarding becomes critical, when large-scale Wi-Fi managed client deployments are considered.

Users are likely to have large numbers of home devices in the near future, especially with the uptake of IoT. Seamless onboarding procedures will be necessary for the operator to help ease service adoption – as involving too many manual steps will make on-boarding un-scalable and drive support calls & truck rolls. With end-user provided client devices the customer should be able to leverage the capabilities of the device to use standards like Wi-Fi Easy Connect™ (scanning a barcode) or WPS (pushing a button) to onboard devices. For example, for headless devices, WPS is a light-touch, while for a device with a camera, scanning a barcode is fairly light-touch.

4.3.3 Onboarding Best Practices

The following onboarding guidelines should be applied:

- Onboarding must be automated and seamless, to the extent possible – from the perspective of end-users and the operator.
- The process must minimize manual end-user or operator involvement.
- The onboarding process must be scalable operationally, to support millions of deployed homes and their connected devices.

4.4 Deployment guidelines

4.4.1 AP Location

In-Home Wi-Fi deployment for Operators typically falls into three categories: self-install, light-touch install, heavy-touch install. Self-install is, of course, when the subscriber installs the Wi-Fi Access Point(s). Light-touch install is typically a single truck roll with the installer simply placing the AP at the broadband point of entry into the house, or wherever the subscriber asks for it or somewhere near the center of the house. Heavy-touch install is characterized by an active or passive Wi-Fi site survey to place the AP(s) in near optimal locations.

Each has their benefits and drawbacks for Operators as seen in the table below:

	Self-install	Light-touch Install	Heavy-touch Install
Cost	Lowest	Medium	High
Wi-Fi Quality	(Possibly) Lowest	Medium	High

As alluded to above, AP location is often the single most important factor in determining Wi-Fi user experience. As demonstrated in most commercial buildings, mounting the AP on the ceiling gives the best Wi-Fi coverage and highest line-of-sight (LOS) probability. While this is often difficult in retrofit installs, Wi-Fi Alliance has a program (Wi-Fi Home Experience) that is working to certify floor plans with pre-wired ceiling mounted AP locations.

There are a few other key best practices for AP placement in the home that should be considered:

In single family homes (SFH):

- Single AP – place the AP in center of living space
- Multiple APs – place the APs with overlapping coverage (e.g. -65dBm or better) if wired backhauls; while higher overlap may be required if APs are using wireless backhauls

In Multi-Dwelling Units (MDUs)

- Do not place APs in adjacent units back to back (with the adjoining unit wall in between)

4.4.2 AP Orientation

Although it would be best if AP Orientation didn't matter, it can sometimes greatly affect the Wi-Fi coverage in the home. Some APs have non-uniform radiation patterns and Operators should test APs before deciding to deploy.

If APs are deployed with non-uniform radiation patterns, even if installers are aware and account for this pattern (which is difficult without doing a detailed site-survey), the subscriber may subsequently rotate the AP not knowing the ramifications and Wi-Fi coverage may suffer.

5 Performance Testing

To meet the ever-increasing consumer requirements for In-Home Wi-Fi, Operators must ensure that they supply devices performing in their expected ways. In this section, we summarise the efforts that have been done among various organizations, and suggest typical performance test cases for in home scenarios.

5.1 Wi-Fi Performance Testing Efforts from Other Organizations

Organization	Action	Scope	Note
Broadband Forum (BBF)	Wi-Fi In-premises Performance Testing (Ongoing work named WT-398 within BBF)	Define a set of tests on baseline capability, coverage, RF capability, Multiple client Stations (STA) support, and stability/Robustness, etc.	1. Give pass/fail criteria under different tests 2. Support till 802.11ac (Wi-Fi 5) 3. Plan to measure Wi-Fi via Video Service
CableLabs/Kyrio	Wi-Fi In-premises and chamber performance testing for APs, Multi-AP systems and STAs	TRP/TIS testing (APs/STAs); AP Throughput performance (load, per channel testing, co/adjacent channel performance, Rate v. Range, 360-deg performance); Multi-AP throughput/roaming/steering tests	1. Focus on performance 2. Support up to 11ac wave 2 (Wi-Fi 5)
CTIA	Test Plan for RF performance Evaluation of Wi-Fi Mobile Converged Device Version 2.0.2 Oct. 2015）	RF performance testing for Wi-Fi mobile converged devices	1. Focus on compatibility of cellular and Wi-Fi 2. Support till 802.11n (Wi-Fi 4) 3. No performance criteria
Home Gateway Initiative (HGI)	2014 Home Gateway Test Plan （Published in May 2016）	Define a set of functional tests based on HGI technical documents related with Wi-Fi	1. HGI ceases working and some work have moved to other SDOs 2. Support till 802.11n (Wi-Fi 4)

IEEE	Established a task group in 2004 but ceased in 2008	Evaluate 802.11 wireless performance	Low participation at that time
Wi-Fi Alliance	Develop technical specifications and certification programs to improve Wi-Fi performance	Both 802.11 standards and proprietary solutions	Perform some performance testing (PHY features) and interoperability testing for other features

5.2 Typical In-Home Wi-Fi Performance Test Cases

Category	Test Case	Description
RF	Receiver Sensitivity	Measure the ability to receive and demodulate weak signals.
Basic	Max Connection	Verify the maximum number of connections while work as normal.
Basic	Max Throughput	Measure the maximum throughput that the device support.
Basic	Airtime Fairness and Qos	Guarantee the fairness of air usage and QoS support among Wi-Fi devices.
Coverage	Penetration	Measure the performance after penetrating walls or obstacles.
Coverage	Range vs. Rate	Measure the performance under different distances.
Coverage	Spatial Consistency	Measure the performance under different orientations.
Multi-STA	Multi-STA Support	Guarantee the device functions under dynamic change of connections.
Multi-STA	MU-MIMO and SU TxBF	Test the MU-MIMO and SU TxBF (Transmit beamforming) support of the Wi-Fi device.
Stability	Long Term /Robust	Verify the functionality under long term and extreme cases.
Stability	Interference	Verify the performance with existence of Wi-Fi or other interference.
Function	Supported Functions	Verify the support of Automatic Channel Selection, Transmit Power Control, Band/AP/SSID Steering, etc.

6 Future Evolution

6.1 Protect backhaul link with Cloud WPA

One possible method of protecting a backhaul link in the home, when backhaul traffic is transmitted over an unencrypted link (e.g. Ethernet), in a Multi-AP system is using a cloud Wi-Fi Protected Access® (WPA) architecture. In this architecture the Wi-Fi-level security of client connections associated to Community Wi-Fi/Neutral Host SSID (both control and data

plane) is relocated from the physical Wi-Fi AP to the Virtual Network Function (VNF) deployed in the operator network. Wi-Fi AP is configured to pass-through 802.11 traffic coming from the clients connected to this SSID without interpretation. Cloud WPA traffic is flowing between Wi-Fi AP and VNF in the IP tunnel.

Cloud WPA architecture does not impose new compute requirements on Wi-Fi AP and could be implemented on existing AP hardware as a software upgrade.

In Cloud WPA architecture, client connection's Master Session Keys (MSK) and Pairwise Master Key (PTKs) stay in the secured environment of operator's network and are not transferred to Wi-Fi AP. This prevents physical, adjacent and cyber security attacks on Community Wi-Fi/Neutral Host in-home traffic.

ARRIS, Telenet and Intel have developed Cloud WPA architecture and have conducted benchmarking and user experience testing in multiple lab trials [2]. The tests show that architecture is sound, integrates well in the Operator network, is compatible with existing client devices on the market and does not impact user experience.

The implementation of Cloud WPA architecture as Xeon-Server based Virtual Network Function (VNF) has been contributed to the open source community at https://01.org/cloudwpa.

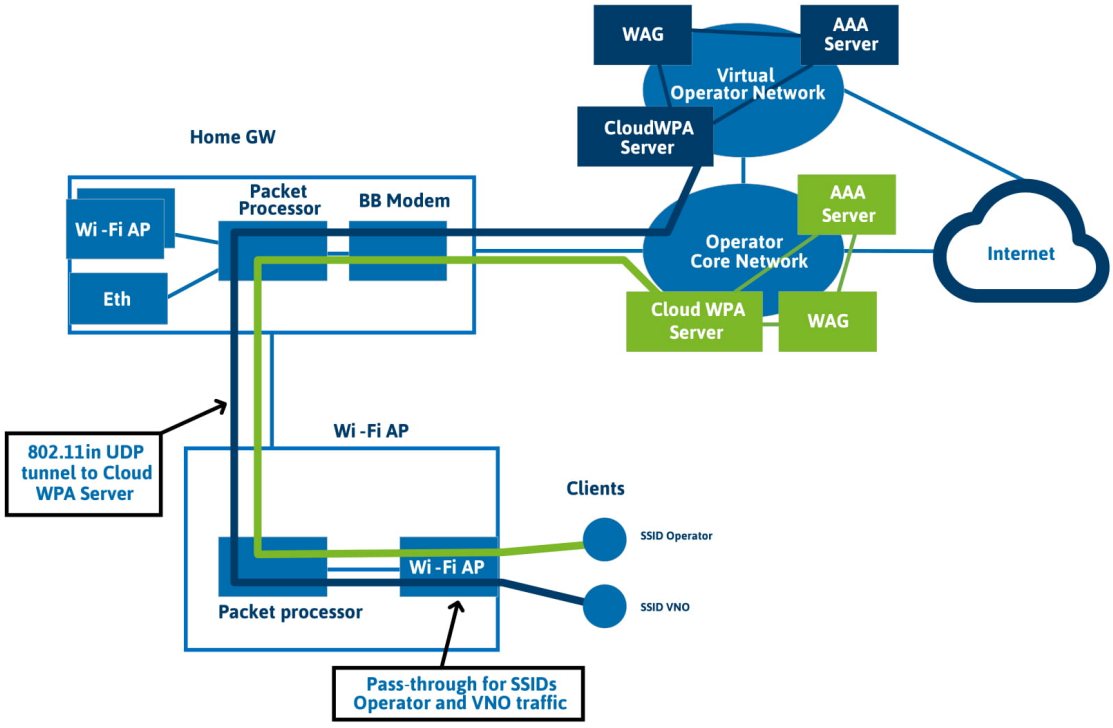

Figure 7. Protect Multi-AP backhaul with Cloud WPA

7 Summary and Conclusions

Operators are facing ever growing demand from home user consumption, which is driving performance requirements from streaming video traffic, larger number of connected devices, Smart Home IoT and VR services, offset by unmanaged multi AP home Wi-Fi networks across different home sizes. The counterbalance of different demands, coupled with the unique home environments, creates a challenge for Operators, which can lead to customer dissatisfaction from poor Wi-Fi quality, which ultimately leads, to churn.

Currently, several approaches are paving the way for improving in-home Wi-Fi performance, addressing a variety of service and architecture requirements, which without adoption for standards will conversely introduce additional interworking issues within home Wi-Fi networks.

Even though the efforts on a standardized approach are proving the most effective solution to achieve broad consensus on how to configure and manage the home environment, there are still certain points yet to be addressed by the current standardization frameworks, such as the network optimization algorithms and AP placement.

In order to solve some of these challenges, WBA members will be assessing programs in the following areas as next steps:

- **Multi-AP Solutions Trial**

With the rise of a Multi-AP solutions and the concept of mesh networks, there is a growing demand for interoperability. This trial would be supported on a set of operator defined use cases and a WBA Test Plan with the goal of proving that Operator's services and requirements work flawlessly in a real operating environment, such as in roaming scenarios, adding AP's on the fly, deploying multiple SSIDs, interaction between different manufacturers, amongst others.

- **Performance Testing Guidelines for In-Home Networks**

Another area to explore is creating a set of test cases and testing guidelines for Operators across the globe to help them confirm and guarantee that the equipment they're using and the way they're deploying Wi-Fi in the home environment can meet performance KPIs, defined by industry

- **Scaling-up In-Home Networks in the IoT era**

A set of necessary adjustments to a home network in order to guarantee the quality of experience remains unaffected in the scenario of deployment and provisioning of IoT devices; a reality that is expected to become more and more relevant in the forthcoming years. Specific use cases and requirements are in development to be defined and currently an identified gap.

- **Delivering 5G Services over an In-Home Network**

With the rise of 5G technology and associated possibilities, it will be mandatory to understand how these work and function in the in-home Wi-Fi environment, with emphasis on permutations arising from networks and its equipment.

- **Wi-Fi & 5G Roaming**

Finally, address roaming between Wi-Fi and 5G networks in the home environment. Naturally, this would involve, a clear understanding the role of 5G services in the home– but would be mostly focused on the technical convergence and coexistence of both options for the end-user and how the network capability could enhance current challenges and use cases.

To participate in the above mentioned initiatives and programs please contact the WBA PMO (pmo@wballiance.com).

REFERENCES

1. Security Development Lifecycle https://www.microsoft.com/en-us/sdl
2. New Approach to delivering Secured Community Wi-Fi, ARRIS-Telenet-Intel, 2018 https://www.intel.com/content/www/us/en/smart-home/connected-home/deploying-cloud-based-wpa2-residential-hotspots.html
3. Securing Wi-Fi Hostpots, WBA 2012
4. White Paper on Next Generation Hotspot Security, WBA 2013
5. Wi-Fi 6, Enhanced 802.11ax - Overview Use Cases Features 5G Context, WBA 2018

PARTICIPANT LIST

NAME	COMPANY	ROLE
John Bahr	CableLabs	Project Leader
Andrew Marchant	Liberty Global	Chief Editor & Project Co-Leader
José Pablo Salvador	Fon	Project Co-Leader
Artur Zaks	Intel	Project Co-Leader
Thomas Durham	Broadcom	Editorial Team Member
Xu Han	Huawei	Editorial Team Member
Peter Joyce	Liberty Global	Editorial Team Member
Nigel Bird	Orange	Editorial Team Member
Mark Hamilton	Ruckus Wireless	Editorial Team Member
Bruno Tomás	WBA	Editorial Team Member
Pedro Mouta	WBA	Editorial Team Member
Feng Wang	AT&T	Project Participant
Simon Ringland	BT	Project Participant
Tim Twell	BT	Project Participant
Praveen Srivastava	Charter	Project Participant
Chris Beg	Cognitive Systems	Project Participant
Chris Jeblonski	Comcast	Project Participant
Cole Reinwand	Comcast	Project Participant
Olakunle Ekundare	Comcast	Project Participant
Natalia Ermakova	Enforta	Project Participant
Tirtho Deb	iBwave	Project Participant
Stephen Kelly	Liberty Global	Project Participant
Max Riegel	Nokia	Project Participant
Michael Timmers	Nokia	Project Participant
George Hart	Rogers	Project Participant
Dzung Tran	Smith Micro	Project Participant
Kanwal Sangha	Shaw Communications	Project Participant