Operator Managed Wi-Fi

Reference Architecture and Requirements

Source: Wireless Broadband Alliance

Authors: Operator Managed Wi-Fi (OMWi)

Issue Date: December 2024

Version: 2.0.0

Status: FINAL

For other publications, visit our website here

To participate in further projects, contact pmo@wballiance.com

About the Wireless Broadband Alliance

Wireless Broadband Alliance (WBA) is the global organization that connects people with the latest Wi-Fi initiatives. Founded in 2003, the vision of the WBA is to drive seamless, interoperable service experiences via Wi-Fi within the global wireless ecosystem. WBA's mission is to enable collaboration between service providers, technology companies, cities, regulators and organizations to achieve that vision.

WBA undertakes programs and activities to address business and technical challenges, while exploring opportunities for its member companies. These initiatives encompass standards development, industry guidelines, trials, certification, and advocacy. Its key programs include NextGen Wi-Fi, OpenRoaming, 5G, IoT, Smart Cities, Testing & Interoperability and Policy & Regulatory Affairs, with Member-led Work Groups dedicated to resolving standards and technical issues to promote end-to-end services and accelerate business opportunities.

Membership in the WBA includes major operators, service providers, enterprises, hardware and software vendors, and other prominent companies that support the ecosystems from around the world. The WBA Board comprises influential organizations such as Airties, AT&T, Boingo Wireless, Boldyn Networks Broadcom, BT, Charter Communications, Cisco Systems, Comcast, HFCL, Intel, Reliance Jio, Telecom Deutschland and Turk Telekom.

Follow Wireless Broadband Alliance:

www.twitter.com/wballiance

www.facebook.com/WirelessBroadbandAlliance

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 organizations 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 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.

Table of Contents

Table of Figures

Executive Summary

With the proliferation of Wi-Fi as the main method of connectivity to the Internet, the word "Wi-Fi" has become equivalent to Internet. Consequently, users' perception of Internet quality of experience (QoE) is most of the time equivalent to Wi-Fi QoE. Moreover, users do not make any distinction between the Wi-Fi service and the Internet service, and they expect their Wi-Fi issues to be resolved by the operator, i.e., Internet Service Provider (ISP). As such, Wi-Fi has become a service that should be managed, and more specifically, a service that should be managed by the operator, hence the name "operator-managed".

Several different operator-managed Wi-Fi solutions exist in the market, each utilizing different proprietary or standard methods for data collection, communication between the Customer Premises Equipment (CPE) and the cloud, remote management, mesh formation, and more. Furthermore, most commercial operator-managed Wi-Fi solutions try to solve the same problems in a different way, which yields non-interoperable and non-reusable solutions.

There are many independent standardization activities in different organizations which try to address the issues related with Wi-Fi management, and which work on new features that enable further remote management capabilities to Wi-Fi networks. As such, there is already a significant amount of work in terms of standardization of features related to remote management of Wi-Fi networks. A holistic solution for the operator-managed Wi-Fi network which incorporates the necessary standards into a reference architecture for the operators to use in their deployments is greatly needed, as it will accelerate the integration process with interoperable and reusable components that bring flexibility to deploy new value-add services.

The operator-managed Wi-Fi (OMWi) reference architecture was introduced by WBA in 2023 in collaboration with industry leaders representing leading ISPs, open-source communities, and hardware and software vendors in an effort to address the much-needed demand for a holistic solution.

WBA's OMWi provides an exemplary reference architecture that satisfies the operators' needs by combining the benefits of the available standards, such as Wi-Fi Alliance (WFA) Wi-Fi EasyMesh™ [1], Wi-Fi CERTIFIED Data Elements™ [4], and Broadband Forum (BBF) User Services Platform (USP) Data Models TR-369 [3] and TR-181 [2]. WFA EasyMesh™ can be utilized as the standard interface for Wi-Fi data collection, Wi-Fi management, configuration, and optimization of the home network. It is important to note that home networks with a standalone Gateway (without Extenders) can use WFA EasyMesh as the standard Wi-Fi data collection, management, configuration interface (API) for the Gateway.

In this second version of the WBA's OMWi reference architecture specification, WBA expands the scope of the requirements defined in the first version, and also include exemplary OMWi compliant open-source implementations from both the prpl Foundation and RDK-B in the Appendix.

1. Introduction

The key attributes that an operator-managed Wi-Fi (OMWi) solution is expected to incorporate for a seamless home network deployment can be listed as follows:

- Support for a standalone Gateway, as well as easy extension to mesh deployments,
- Installation and operation not requiring cloud connectivity,
- Wi-Fi metadata collection from the home network,
- Remote configuration of the CPEs (Gateway, router and access points) in the home network,
- Remote management of the home network,
- Flexibility for adding new features (applications) without requiring CPE firmware upgrade,
- Running microservices (i.e., applications) on the CPEs and cloud,
- Reusability and interoperability with other deployments,
- Upgrades to the latest developments in Wi-Fi standards.

Figure 1 depicts the OMWi Generic block diagram focusing on the functionality of each block while abstracting away the specific technologies used for them. As illustrated in the figure, OMWi solution puts together CPE (embedded) blocks that provide APIs to handle lower layer (southbound) and upper layer (northbound) functionalities. Also, the generic architecture illustrates that several microservices (i.e., applications) can run on the CPE, and these microservices can be downloaded from and managed by separate cloud instances which might be operated by different entities. Thus, providing a significant flexibility for the operator to deploy several different microservices which might be supplied by different service providers.

The architecture illustrated in Figure 1 depicts components that can address the key attributes listed above. In Section 3, we specify the technologies that are recommended for each of the component depicted in Figure 1.

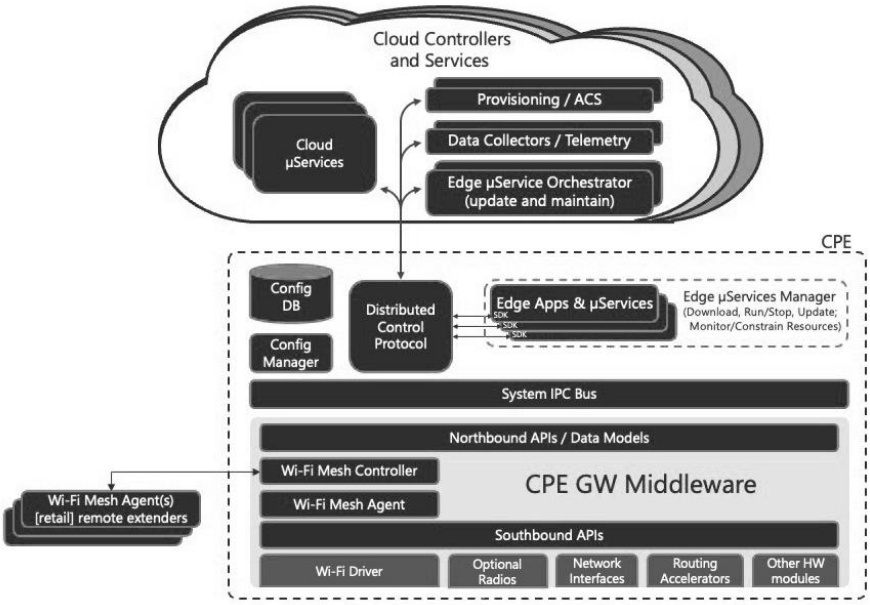

Figure 1 OMWi Generic Architecture Block Diagram

2. Terminology and References

2.1 Conventions

In this specification, several words are used to signify the requirements of the specification.

- Shall: This word, or the term "required", means that the definition is an absolute requirement of the specification.
- Shall not: This phrase means that the definition is an absolute prohibition of the specification.
- Should: This word, or the term "recommended", means that there could exist valid reasons in particular circumstances to ignore this item, but the full implications need to be understood and carefully weighed before choosing a different course.
- Should not: This phrase, or the phrase "not recommended" means that there could exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications need to be understood, and the case carefully weighed before implementing any behaviour described with this label.
- May: This word, or the term "optional", means that this item is one of an allowed set of alternatives. An implementation that does not include this option shall be prepared to inter-operate with another implementation that does include the option.

2.2 References

[1] Wi-Fi Alliance EasyMesh Release 4
[2] Broadband Forum TR-181 Issue 2: Device Data Model
[3] Broadband Forum TR-369 USP
[4] Wi-Fi Alliance Data Elements Release 2.1
[5] Prpl Foundation
[6] RDK-B

3. General Architecture

In this section, we provide an overview of the building blocks that form the OMWi Reference Architecture.

In Figure 2, we illustrate the specific technologies that are recommended to be used for the functionality blocks depicted in Figure 2. Here, it is envisioned that one or more cloud Controllers, e.g., USP Controllers [3], are utilized for remote configuration and management of the CPE, for example, through TR-181 [2] data model objects. Furthermore, microservices (applications) can run on the CPE (as edge microservices) and/or in the cloud (as cloud microservices), and edge microservices can be remotely updated and maintained through USP.

As illustrated in Figure 2, home network can be extended by adding Extenders to the Gateway using industry-standard Wi-Fi EasyMesh [1]. The mesh network can be managed and configured by using Wi-Fi EasyMesh. It is also envisioned that the home mesh network can be managed remotely using USP via the BBF TR-181 based northbound API [5].

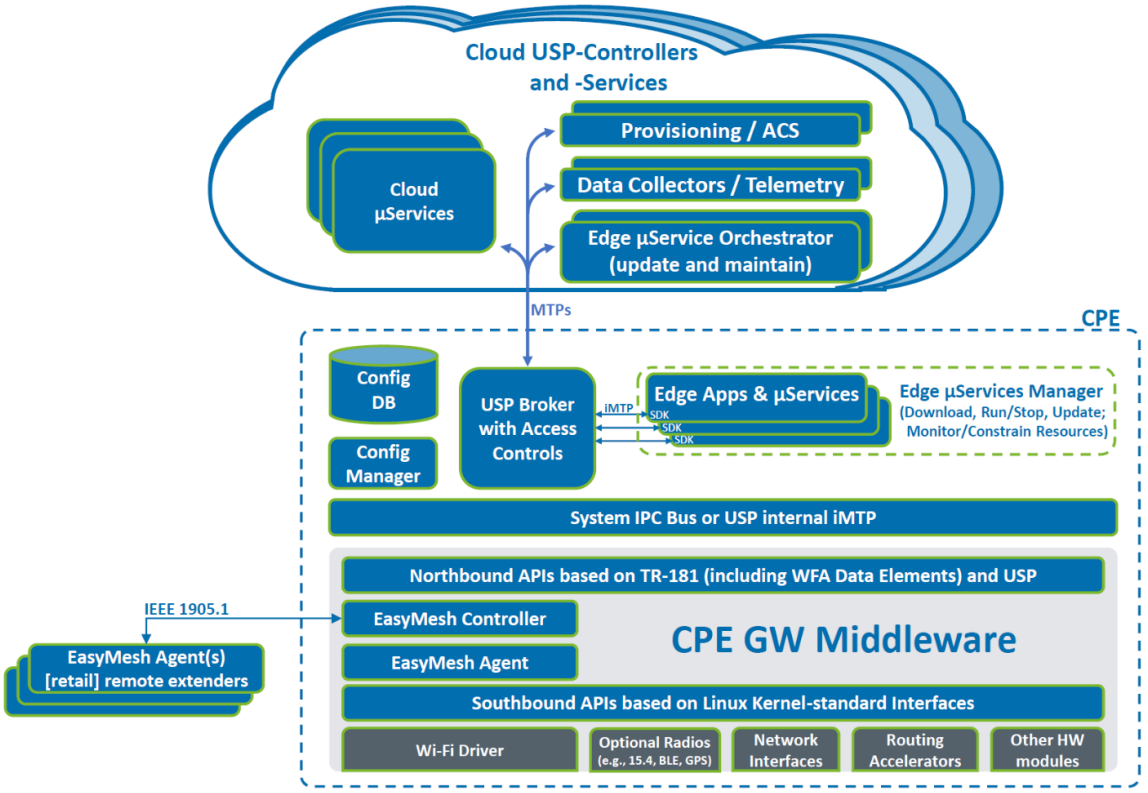

Figure 2 OMWi Reference Architecture Block Diagram

The OMWi Reference Architecture, as shown in Figure 2, defines common, standards-based components which form a common reference platform, while still allowing for value-added proprietary components implemented as edge or cloud microservices. Specifically, TR-181 [2] provides a common standard data model that enables configuration and management of the home network, and together with TR-369 [3], it enables a standard method for the management and configuration of the device and network through a standard data model. Also, WFA EasyMesh provides a standard interoperable method for setup, configuration, and management of multi-AP (mesh) networks. By leveraging WFA EasyMesh [1] together with WFA Data Elements [4] (which are also incorporated in TR-181) via a common Northbound API [5], OMWi provides proprietary microservices: a) the capacity to run value-add applications that process data supplied by the device and/or home network for analysis; and b) the necessary configuration handlers for remote configuration of the network parameters.

The OMWi architecture in a home network with a Gateway (GW) and Extender AP deployment is illustrated in Figure 3. Here, it is shown that the WFA EasyMesh Controller located in the Gateway and the WFA EasyMesh agent located in the Gateway and the WFA EasyMesh agent located in the Extender are communicating through WFA EasyMesh and IEEE 1905.1.

It is important to note that WFA EasyMesh™ is utilized as the standard interface for Wi-Fi data collection, Wi-Fi management, configuration, and optimization of the home networks with a standalone Gateway (without Extenders) as well as the networks with Extenders.

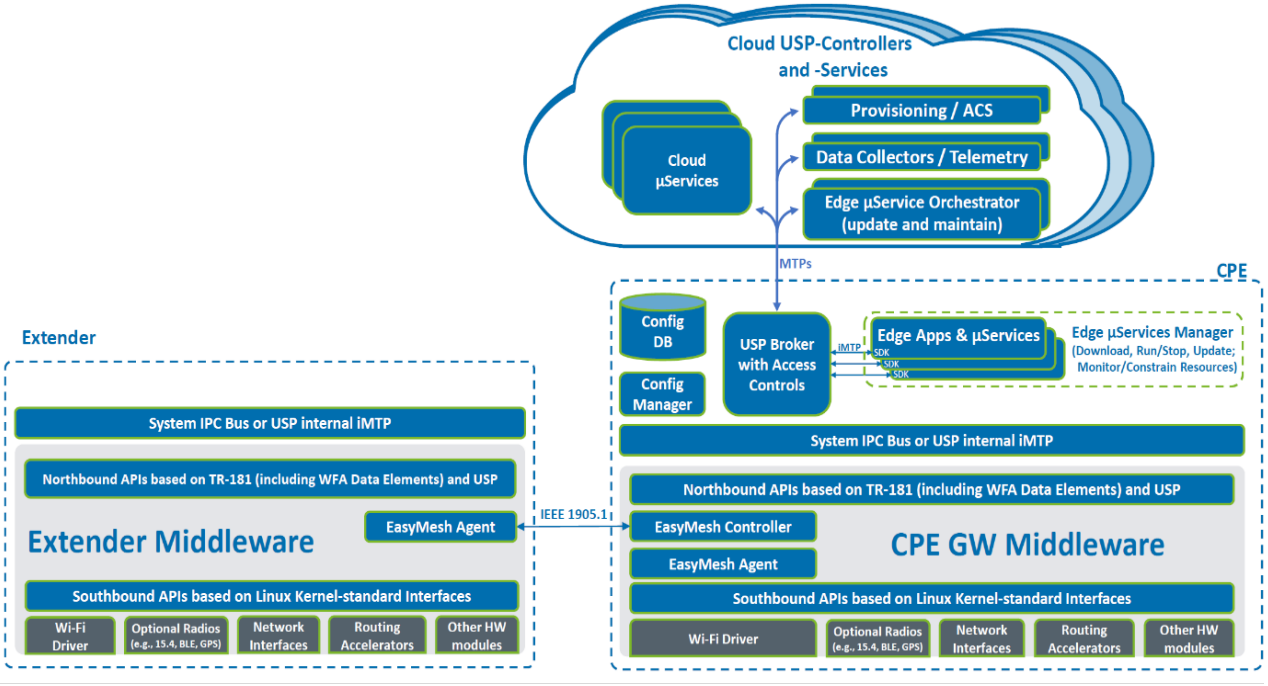

Figure 3 OMWi Architecture with Extender deployment

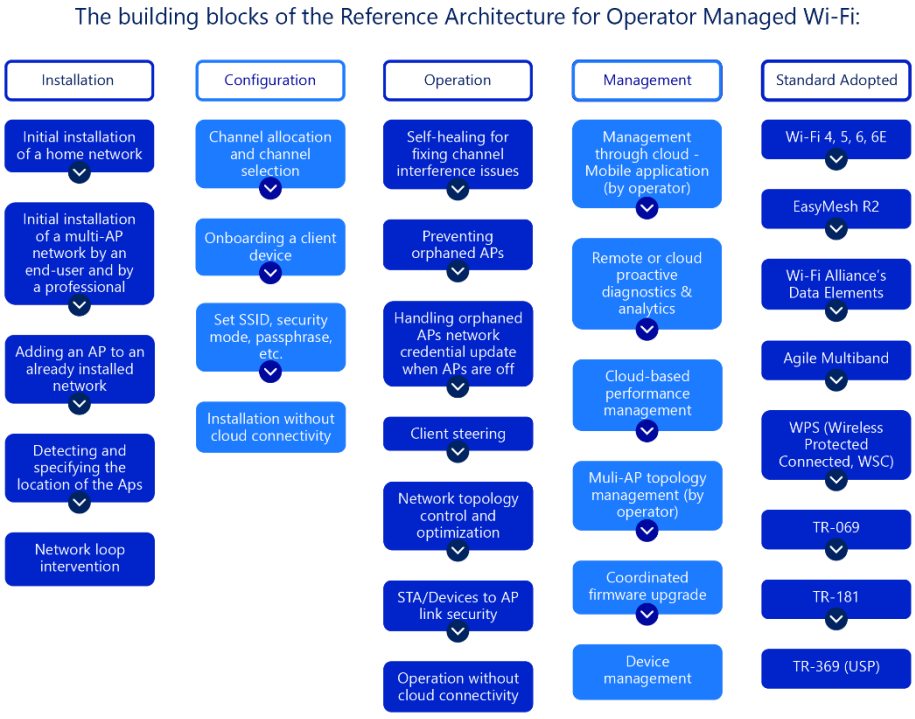

Figure 4 Building blocks of Reference Architecture for Operator Managed Wi-Fi

4. Deployment (DEP)

This section covers the OMWi recommendations for the deployment use cases.

4.1 Initial Installation of a Home Network

In this use case, a user would like to have an Internet connection setup on their premises. A standalone Gateway or a multi-AP system may be provided by the ISP according to the user's needs.

This use case covers the initial setup of a home network with either a standalone Gateway, or a Gateway with Extenders, e.g., a newly unboxed set of multi-AP devices.

DEP.R1 The provided system shall include one Gateway to sustain the Internet connection. Gateway shall support WFA EasyMesh Release 4 with at least 'Profile 2'. Note that Gateway functionality may be distributed across multiple boxes, e.g., an Internet Gateway connected to a Wi-Fi access point that has a Wi-Fi EasyMesh Controller.

DEP.R2 Gateway shall by default run the WFA EasyMesh Controller.

DEP.R3 Gateway and the Extenders shall use TR-181 data model.

DEP.R4 The provided system may have one or more Extender APs. The number of APs should be defined according to the user's needs and property features, e.g., number of floors, rooms, etc. The Extenders shall employ WFA EasyMesh agents supporting WFA EasyMesh Release 4 with at least profile 2 to be able to form a mesh (multi-AP) network.

DEP.R5 Wireless Simple Connect (WSC/WPS) shall be supported by the Gateway and the Extenders to connect APs wirelessly.

DEP.R6 Ethernet connection (WPS or Device Provisioning Protocol (DPP) - over Ethernet) shall be supported by the Gateway and the Extenders to connect APs.

DEP.R7 A physical button (on the CPEs) for initiation of the onboarding process is recommended.

DEP.R8 Wi-Fi CERTIFIED Easy Connect™ (also known as DPP) may be supported to allow for onboarding stations (STA) and APs to the network.

DEP.R9 It is recommended that an application running on a smartphone, or a tablet is used for installation of the home network. For further details on requirements of the application, refer to Section 6.1.

4.2 Initial Installation of a Multi-AP Network With an Existing Gateway (OTT Installation)

This use case provides for an easily achieved procedure so that a user can deploy a new multi-AP network on top of their existing network with an old Gateway which does not support a multi-AP connection, i.e., which does not support WFA EasyMesh.

A user requires a multi-AP system for whole-home coverage. Even though the user has existing Wi-Fi provided by their ISP's Gateway, the new system may not support wireless connection with the original Gateway. In this case there are two different solutions:

1. Extend the existing network with Extender APs; or,
2. Create a standalone network with a router and add Extender APs.

In the first case, an Extender AP is connected to the existing Gateway with an Ethernet connection and becomes the multi-AP (EasyMesh) Controller. Other Extender APs can then connect to the network wired/wirelessly via the Extender AP that serves as the EasyMesh Controller.

In the second case, a router is connected to the existing Gateway with an Ethernet connection and becomes the multi-AP (EasyMesh) Controller. Any Extender APs can connect to the network wired/wirelessly via the router that serves as the EasyMesh Controller. Here, the router forms a new network different from the existing Gateway's network.

The difference between these two scenarios stems from the capabilities of the new multi-AP systems. A system consisting of only Extenders, as in the first case, performs at the data link layer and cannot perform network operations specific to router functionality, such as IP-layer traffic classification, parental control (traffic and application based) or firewall etc. If the user/operator needs such operations, they should: a) include a router as in the second case; or b) install a Gateway that has these functions.

DEP.R10 The new routers and Extenders shall be capable of being connected to the Gateway via wired Ethernet.

DEP.R11 The added Router and Extender shall support Wi-Fi EasyMesh to be able to form a mesh (multi-AP) network. The router shall run the EasyMesh Controller.

DEP.R12 Wireless Simple Connect (WSC/WPS) shall be supported by the added CPEs (i.e., router and Extender APs) to connect APs wirelessly.

DEP.R13 Added CPEs shall support WPS or DPP over Ethernet.

DEP.R14 A physical button should exist on the added CPEs (i.e., router and Extender APs) to initiate the onboarding.

DEP.R15 Wi-Fi Easy Connect (DPP) may be supported by the added CPEs (i.e., router and Extender APs) to allow for onboarding STAs and APs to the network.

4.3 Adding an AP to an Already Installed Network

This use case covers a scenario where a user is dissatisfied with the coverage of the existing Wi-Fi network in their premises and wants to improve it by adding a new Extender AP to the network which already supports WFA EasyMesh.

An Extender, delivered by the operator, should be installable effortlessly in the existing network by the user. The Extender automatically integrates with the network allowing deployment of all network services without further effort.

DEP.R16 The installation procedure should accommodate both wired and wireless installation.

DEP.R17 Wi-Fi EasyMesh shall be supported by the added Extender to form a mesh (multi-AP) network.

DEP.R18 Wireless Simple Connect (WSC/WPS) shall be supported by the added Extender to connect APs wirelessly.

DEP.R19 Ethernet connection (WPS or DPP over Ethernet) shall be supported to connect APs.

DEP.R20 A physical button should exist to initiate the onboarding.

DEP.R21 Wi-Fi Easy Connect (DPP) may be supported by the added Extender to allow for onboarding STAs and APs to the network.

4.4 Detecting and Specifying the Location of APs to Provide Installation Guidelines via Mobile Application

This feature aims at providing users a mobile application that guides them during the installation of their home mesh network, specifically, helping them place the APs in appropriate locations such that the mesh network coverage is maximized, while also optimizing the end-to-end (STA to Gateway) throughput. Reader is referred to Section 6.1 for more information on the mobile application.

A multi-AP network's performance relies on the locations of the individual mesh nodes and a correct installation is imperative to avoid issues, such as low end-to-end throughput. To install a network node, a user should be guided to locate the node in a suitable location by an application that assesses the end-to-end (STA to Gateway) link quality. Proactive mechanisms that leverage out-of-band techniques to position a network node may be utilized.

An end-user receives a new device and depending on the installation flow supported by an operator, she can use a proactive based location search mechanism whereby a client device (e.g., smartphone) is used to move around on the premises and a "location finder" application guides the end-user to a suitable location.

An application running on a mobile device (e.g., tablet, smart phone) may be used to guide and help the user on detecting and specifying location of APs (Gateway and Extender APs).

DEP.R22 The home network system and instructions provided by the operator shall have the means to give feedback to an end-user about the quality of the location in which a network node has been placed.

DEP.R23 Instructions or guidance shall be provided to enable the user to place APs in good locations. Location recommendations may be provided by an app or Web UI. The AP may show LED colors indicating signal strength to assist placement.

DEP.R24 APs shall be capable of measuring and storing/sharing signal strength (e.g., Received Signal Strength Indicator (RSSI), Received Channel Power Indicator (RCPI)) as defined in WFA EasyMesh [1], Wi-Fi Data Elements [4] and BBF TR-181 [2].

DEP.R25 A mobile application should be able to retrieve data about signal strength, e.g., RSSI between the APs and between an AP and a connected STA, from the home network, or preferably from a cloud server. Application may use this information together with a drawing (e.g., map) of the home to provide the user with locations of the APs and the mobile device. Mobile applications may be provided with a sketch of the home by the user.

4.5 Network Loop Prevention

Network loops may occur in mesh networks when two APs have direct wireless and Ethernet links between each other. Such a scenario may occur, for example, when a user may have originally installed an AP via a wireless backhaul connection but then decides to install an Ethernet backhaul connection when issues with the wireless backhaul are encountered. Having simultaneous wireless and wired backhauls between two APs would cause a network loop, which would yield the network unusable.

Typical Extender APs offer not only a wireless backhaul but also several wired options like Ethernet (IEEE 802.3), powerline (G.HN, HomePlug) or other alternative LAN connection options. A user can easily connect a second LAN connection assuming that the network will properly use and handle it. By creating parallel LAN paths between 2 network nodes, an OSI layer-2 loop is created allowing for a storm of broadcast packets that eventually brings down the individual nodes of the network and, at the end, the network itself.

This feature aims at detecting network loops in multi-AP networks and removing them as soon as possible. A multi-AP network, as such must be able to "handle" network loops to allow users the freedom to install the network as they see fit while maintaining control over the network.

DEP.R26 Every AP in the network shall have the ability to detect a loop being created (e.g., by monitoring the IEEE 802.1Q bridge traffic).

DEP.R27 Every AP in the network shall have the ability to break a network loop by the implementation of a loop prevention algorithm based on a standard (e.g., Spanning Tree Protocol (STP), or Rapid STP (RSTP), Transparent Interconnection of Lots of Links (TRILL), etc.) or a proprietary mechanism (e.g., master/slave path blocking).

DEP.R28 Loop breaking can either be done by physically disconnecting an interface or by preventing multicast/broadcast traffic from being sent via an interface.

4.6 Channel Selection

Multi-AP networks are installed to improve the overall user experience in a home. However, user experience does not solely depend on coverage; but overall, on available bandwidth and hence qualitative access to services. Installation of multi-AP networks as such requires the availability of the Radio Frequency (RF) medium. To efficiently access the RF medium, multi-AP networks must assign frequency slots to each of the APs to achieve the highest available medium accessibility.

Standalone APs generally implement a mechanism to select "the optimal" band/channel to operate on. However, when multiple APs are installed in an environment, the optimal channel allocation can benefit from a multi-AP coordination function to allow each AP the highest available medium accessibility within the boundaries of hardware and regulatory constraints.

DEP.R29 The multi-AP system shall be able to select an operating channel at the initialization, i.e., following network installation.

DEP.R30 A simple channel selection method may be employed for the assignment of the operating channel at the start. Yet, the channel assignment for the home network shall be optimized later as sufficient

data is gathered by the EasyMesh Controller, preferably within a day. For the requirements related to channel optimization during operation, reader is referred to Section 5.1.

DEP.R31 Each AP shall assess channel conditions and shall be able to report channel conditions to the multi-AP management entity, Wi-Fi EasyMesh™ Controller.

DEP.R32 Home network shall employ a channel management entity that can gather information regarding channel quality from the EasyMesh Controller to perform channel quality assessment, and that can select the optimal channel for each AP in the home network.

DEP.R33 The channel management entity may be an edge microservice that runs on the Gateway (or master AP) or it can be a cloud microservice that runs in the cloud. In either case, the channel management entity shall have access to data collected by the EasyMesh Controller.

DEP.R34 Decision on the operating channel may be performed by the channel management entity.

DEP.R35 Channel switch shall be triggered by the EasyMesh Controller, and the EasyMesh Agents in the network shall apply the channel assignment given by the EasyMesh Controller as defined in the WFA EasyMesh specification.

4.7 Onboarding a Client Device

This feature covers the methods by which a user device that is previously not connected to the home network gains its network access.

There are various methods to provide seamless connection to clients, such as Wi-Fi Protected Setup™ (WPS), Wi-Fi Easy Connect (a.k.a. DPP), QR Code based methods, etc. Besides these technologies, entering the Service Set Identifier (SSID) and the passphrase manually is still an option.

Being a relatively old technology, WPS can still be used to onboard a client device by pushing the WPS button on the AP and the device. Considering the large number of legacy devices with WPS support in use, WPS is still a valid option for onboarding client devices.

Also, a QR code including the network credentials can be placed on the devices. These QR codes may include SSID and password information or they may direct the user to another HTML server to retrieve the credentials, etc. A mobile application can be used to read the QR code.

DEP.R36 The home network shall support Wireless Simple Connect™ (WSC/WPS) and QR Code onboarding schemes.

DEP.R37 The home network may support Wi-Fi Easy Connect.

DEP.R38 A client device should be able connect to the home network via manually entering the network credentials.

4.8 Setting SSID, Security Mode, Passphrase

Home network by default comes with credentials such as SSID, security mode, passphrase, etc., which are predetermined by the operator and set by the manufacturer. However, users may want to change these credentials according to their specific needs. Credentials may also be changed to respond to security concerns.

When a home network is deployed, the network user may want to set specific SSID, security mode and/or a passphrase different from the predefined credentials. In this case, the home network must permit the user to carry out these changes. While these changes can be made by the user locally through a mobile application or WEB UI (hosted on the Gateway), they can also be made by the operator remotely through the cloud.

DEP.R39 The network shall present a UI to let the user set the network credentials.

DEP.R40 For remote setting by the operator, a remote management system such as TR-069 or TR-369 shall be supported.

DEP.R41 The user should be provided with a mobile application, as described in Section 6.1, to be able to set and get her home network's SSID, Security mode and passphrase.

DEP.R42 It shall be possible to write the same SSID and passphrase to the Gateway and all APs and Extenders making up the home network.

DEP.R43 SSIDs shall be assignable to distinct traffic separation domains, such as private, guest, public, etc.

4.9 Installation Without Cloud Connectivity

This feature ensures that a home network can be installed without Internet (cloud) connectivity, i.e., the setup of the home shall not rely on cloud connectivity. As such, a local mechanism (that does not require connection to the Internet) should also be provided to the user for deploying a new home network or adding a new AP/network node to an existing network.

DEP.R44 Gateway and APs should be able to run a local WEB server and host a local Web UI. The IP address of the WEB UI should be provided to the user. For example, a QR code printed on the Gateway can be used to direct the user to the local Web UI.

DEP.R45 In case of mesh network, it is recommended that all APs direct to a single Web UI, which is hosted preferably by the Gateway.

DEP.R46 A mobile application (check for Section 6.1) may also be used for accessing the local server and configuring the home network.

5. Operation (OPS)

This section covers the OMWi recommendations for the operation use cases, which cover post installation home network usage scenarios.

5.1 Channel Management: Self-Healing for Fixing Channel Interference Issues

When the home network's environment changes, for example due to congestion or interference from new neighbouring networks, it may become necessary to reallocate the channels in which the network operates. This process typically uses the same functionality as described in Section DEP.R26 with the addition of information that is gathered during operation about the changing environment conditions.

The home network should periodically, or on request, check the channel efficiency and the possible other channels to be aware of the interference sources. When a nearby network changes channel or uses the channel more densely, the level of interference and congestion on the home network may increase, causing the home network to take action in an effort to mitigate the problem.

When multiple APs are installed in an environment, the optimal channel allocation can benefit from a multi-AP coordination function to allow each AP the highest available medium accessibility within the boundaries of hardware and regulatory constraints.

As stated in requirements DEP.R32 and DEP.R33, home network shall employ a channel management entity, which can be implemented as an edge or cloud microservice, that can gather information regarding channel quality from the EasyMesh Controller to perform channel quality assessment, and that can select the optimal channel for each AP in the home network.

The channel management entity shall periodically assess the channel allocation after installation. Based on the most recent channel assessment, the channel management entity shall assign the optimal operational channel to each of the Extenders in the network for both the fronthaul and the backhaul radios.

OPS.R1 The home network shall be able to change the channels once configured.

OPS.R2 Each AP, i.e., WFA EasyMesh agent, shall assess channel conditions and report the measurement results to the Wi-Fi EasyMesh Controller, as defined in the WFA EasyMesh specification.

OPS.R3 The channel assessment may be based on the current values and history of one or more parameters such as channel (medium) availability, interference, signal strength, bandwidth, number of associated devices, channels supported by clients in the network and contention information collected during operation.

OPS.R4 Home network shall employ a channel management entity that can gather information regarding channel quality from the EasyMesh Controller to perform channel quality assessment, and that can select the optimal channel for each AP in the home network.

OPS.R5 The channel management entity may be implemented as an edge microservice that runs on the Gateway (or master AP) or it may be implemented as a cloud microservice that runs in the cloud. In either case, the channel management entity shall have access to the data collected by the EasyMesh Controller.

OPS.R6 The channel management entity, implemented either as an edge or a cloud microservice, shall use a common TR-181 [2] based northbound API to communicate with the Wi-Fi EasyMesh Controller [1].

OPS.R7 Decision on the operating channel for each radio and the channel switch should be given by the channel management entity, and these decisions shall be conveyed to the WFA EasyMesh Controller via a common TR-181 based northbound API.

OPS.R8 Channel switch shall be triggered by the EasyMesh Controller using the channel change procedures as defined in the WFA EasyMesh specification.

OPS.R9 In the 5 GHz band, the APs may support Dynamic Frequency Selection (DFS) and non-DFS channels. In case DFS channels are supported, the APs shall operate in accord with the DFS rules of the operating country (e.g., FCC in the USA and ETSI in Europe).

OPS.R10 Channel switch to a DFS channel shall not cause backhaul link disruption, so off-channel scanning is recommended to clear DFS channels.

OPS.R11 Channel switching operation shall avoid wireless client disconnects. As such, Channel Switch Announcement (CSA) or Extended CSA (ECSA) shall be supported by Gateway and APs.

OPS.R12 Cloud management should also be used for longer-term channel selection, e.g., by storing performance data about previous channel selections.

5.2 Orphaned APs in a Multi-AP Network

Multi-AP networks create a strain on configuration mechanisms. The network configuration must have the ability to be changed, and the changes must be handled carefully without orphaning network nodes. In real life, however, users forget that a specific network node (e.g., in the garden patio) has been powered down when they reconfigure the network. While backhaul credentials can, for example, be managed by a remote management system that halts when not all APs are accounted for, the credential update will not be halted indefinitely, so a network device may get orphaned.

5.2.1. Preventing Orphaned APs - Reliable Network Credential Change

This feature aims at preventing wirelessly backhauled APs from dropping off the network (or from having to be manually re-onboarded) while changing network's credentials (security mode, network name, passphrase, etc.).

OPS.R13 User/operator should have a method to reconfigure the network.

OPS.R14 The backhaul and fronthaul links should have separate SSID and password, and backhaul SSID shall be hidden, as specified in Wi-Fi EasyMesh standard. It is recommended that the home network does not provide any mechanism for the user to change the Wi-Fi backhaul SSID and the password. The Wi-Fi backhaul SSID, and the password should be configurable by the operator only.

OPS.R15 The Wi-Fi backhaul credential change shall be performed such that backhaul link between two APs is not updated before both APs receive the new credentials. An exemplary method may be to start credential change from the outermost (i.e., leaves of the tree topology) AP and to continue one by one until Gateway (root of the tree topology) is reached.

5.2.2. Handling Orphaned APs - Network Credential Update When Some APs Are Off

Network devices require the ability to have their configuration updated, especially when related to security aspects, as the target is to ensure the safest network for the end-users. With multi-AP networks, extra challenges present themselves. A multi-AP network must handle the reality that not all its nodes are enabled all the time and hence may not be updated with the latest (security) configuration. When such a scenario occurs, the device that was not enabled during the configuration update will become orphaned. As such, network operators must have a re-onboarding procedure in place to allow end-users to handle such a scenario.

OPS.R16 A multi-AP network should provide a manual or automatic way for an orphaned AP/network node to be re-onboarded to the network. Some of these techniques have been discussed in Section 4.1.

Expected outcomes for handling orphaned APs are listed below.

- The network indicates that there is an orphaned AP/network node – existing node is not operational. Note that this may "just" be an AP/network node that has broken down, was replaced, etc. An end-user may be asked to indicate the true status of an orphaned AP/node (e.g., ignore the info, delete the removed node, or mark it as orphaned).
- An orphaned AP/network node that has been successfully connected to the network at some point in time is recognized again.
- The network may self-heal, by automatically reconnecting the orphaned AP, and chooses to notify the end-user.
- At the final stage, the network works again when an orphaned AP/network node is either self-healed or manually healed, and the AP is onboarded to the network/Controller.

5.3 Client Steering

This feature deals with maintaining client devices' connectivity and optimizing their end-to-end performance (Gateway to/from STA) by managing which AP and radio/band (or interface) the device is connected to. When the device is moving around the home, it may stay connected to a suboptimal AP/band, and it may be necessary to steer the client to the optimal AP/band to improve its end-to-end (throughput) performance.

A dual-band or tri-band client device may also stay connected to a suboptimal radio (e.g., 2.4 GHz radio), being suboptimal due to the limited capacity of the operating band or the interference in the operating channel; whereas it could benefit from better end-to-end performance if connected to another band. In such cases, the client may not be able to identify the better band option, and it may be necessary for the home network to steer the client to the optimal band.

OPS.R17 Client steering in a home network with APs that have dual-band or tri-band radios shall support any available combination of bands ('2.4 & 5' / '5 & 6' / '2.4 & 6' / '2.4 & 5 & 6').

OPS.R18 Client steering between bands, and client steering between APs in multi-AP networks shall be supported.

OPS.R19 Client steering between interfaces with the same SSID shall be supported.

OPS.R20 Support for client steering between interfaces with different SSID is recommended.

OPS.R21 IEEE 802.11v shall be supported on APs.

OPS.R22 IEEE 802.11k should be supported on APs.

OPS.R23 IEEE 802.11r may be supported on APs.

OPS.R24 Client steering may be managed by a client steering entity implemented as an edge microservice or a cloud microservice. In such a case, the client steering entity shall use a common TR-181 based northbound API to communicate with the Wi-Fi EasyMesh Controller.

OPS.R25 Client connection assessment for each client should be performed by, and the client steering decision should be given by the client steering entity. These decisions shall be conveyed to the WFA EasyMesh Controller via a common TR-181 based northbound API.

OPS.R26 Client steering shall be triggered by the EasyMesh Controller using the client steering procedures as defined in the WFA EasyMesh specification [1].

5.4 Network Topology Control and Optimization

Multi-AP networks must cope with several issues that span from the multi-AP nature. Section 5.1 already discusses the need to react to the changes in the RF conditions when operating a multi-AP network. However, another important aspect that requires a form of self-healing is related to topology changes. Multi-AP networks must handle APs/network nodes that are switched on/off or backhauls that break due to severe deterioration of the RF environment.

Topology can be optimized over the long term by a cloud or remote management system, or relatively rapidly by a local Controller. While multi-AP networks may receive topology guidance from a cloud or remote management system as described in Section 6.4, this guidance may not be real-time as it requires some data to converge to an optimal multi-AP topology. When, however, there are instantaneous topology changes, the multi-AP network must have the minimal ability to reform itself to a pseudo-optimal topology first before being fully optimized via remote management techniques in a later phase.

OPS.R27 A home network shall have the means to reform the network in such a way that the overall performance remains acceptable to the end-user.

OPS.R28 A home network shall implement a centralized or decentralized topology assessment and control function.

OPS.R29 The network topology assessment and control function shall use a common TR-181 based northbound API to communicate with the Wi-Fi EasyMesh Controller.

OPS.R30 Topology information shall be available and may have a visualization component to illustrate the current network topology for the end-user.

OPS.R31 The topology assessment and control function should apply a metric to allow comparing network topology "quality".

OPS.R32 The topology assessment and control function should react rapidly to disruptive changes in topology. The reaction shall be fast, minimizing the time home network is dysfunctional.

OPS.R33 All APs in the home network shall support functions to reconnect their backhaul links, provided this backhaul link can be re-connected to somewhere else.

OPS.R34 All APs/network nodes shall have necessary credentials to re-connect backhauls.

OPS.R35 The network topology assessment and control function may be implemented as a separate edge or cloud microservice. In such a case, the microservice shall use a common TR-181 based northbound API to communicate with the Wi-Fi EasyMesh

5.5 STA-AP Link Security

Client devices in a home network require secure Wi-Fi links which may be provided by utilizing standard security and encryption methods. This feature covers the required security protocols that should be supported by the fronthaul interfaces of Gateway and AP.

OPS.R36 The fronthaul interfaces in a home network shall at least support the following security schemes: WPA2 – Personal, WPA3 – Personal, WPA3 – Transition.

OPS.R37 It is recommended that backhaul Wi-Fi interfaces use WPA3-Personal security scheme.

5.6 Operation Without Cloud Connectivity

Home network must stay operational even if connectivity to the cloud servers is lost. A local mechanism (that does not require connection to cloud servers) should also be provided to the user for local management of the network. For example, Wi-Fi EasyMesh Controller shall be able to manage the topology of the network even if cloud connectivity is lost.

OPS.R38 The home network should have at least the necessary minimal set of edge microservices to maintain the home network operation when cloud connectivity is lost.

OPS.R39 The home network should have a local entity to inform the user about loss of cloud connectivity.

OPS.R40 The Gateway and the APs shall employ default parameter settings for the TR-181 data model, particularly for critical parameters that govern the operation of the home network. Thus, the home network shall not rely on getting TR-181 parameter values from a cloud service for operation of the home network.

6. Remote Management and Diagnostics (RMD) Features

This section covers the OMWi recommendations for the remote management of the home network as well as the recommendations for the diagnostics capabilities.

6.1 Management Through a Mobile Application

An application running on a smartphone or tablet may be used to provide means to manage and monitor a home network. The application provides visibility to available Wi-Fi connections and the quality of the current Wi-Fi connections in the home network.

RMD.R1 The application should provide means to onboard Extender APs to the home network.

RMD.R2 The application should provide means to onboard wireless clients, such as headless devices, e.g., printers, IoT devices, cameras.

RMD.R3 The application should provide means to control wireless client access to the home network. For example, user should be able to define Wi-Fi and Internet on/off schedules for any client in the home network using the application. It is worthwhile to note that if MAC randomization is enabled on the client devices, MAC address-based Wi-Fi access control would not work. (As a

remedy, the home network may implement a device identification method that does not rely on MAC address information.) Only where MAC-based access control is used, the user should be notified about this. Furthermore, the user may be informed that for proper operation of MAC address-based Wi-Fi access control, MAC randomization may be needed to be disabled (if the home network does not implement another device identification method).

RMD.R4 The application should provide means to name both clients and APs for ease of tracking and managing of the devices in the home network by the user.

RMD.R5 The application should provide means for troubleshooting, for example, by providing guidelines illustrating what steps to follow in case of issues.

RMD.R6 The application should provide means to configure the home network. The user should be able to set SSID and passphrase of her home network using the application. The application should allow the user to create new interfaces, such as but not limited to guest SSID.

RMD.R7 Authorization, preferably through the operator's network, should be required to run the application. Only an authorized application shall have home-network configuration privileges (e.g., setting SSID, passphrase, naming devices, etc.).

RMD.R8 The application should provide means to access data about the home network, such as data related to performance, topology, connected STAs and analysis results. The data may include RSSI, achieved throughput, transmit/receive physical layer (PHY) rate per STA, and medium availability (Clear Channel Assessment (CCA) and/or utilization) per channel.

RMD.R9 The application should be downloadable from an application store, such as Apple App Store and Google Play.

6.2 Remote or Cloud Proactive Diagnostics and Analytics by the Operator

Remote management of the home network is an essential element of an operator managed home network. Remote management consists of three components: (i) collection of diagnostics data by the CPEs and delivering of the data by the CPE to a cloud server, (ii) running analytics on the collected data to enable reactive and proactive diagnostics, (iii) management of the home network by the cloud through remote configuration of home-network parameters based on the collected data.

RMD.R10 CPEs (i.e., Gateway, router and APs) in the home network shall collect data, e.g., via WFA EasyMesh agent, that facilitate remote diagnostics of STA and AP performance, e.g., in terms of RSSI, achieved and achievable throughput, transmit/receive PHY rate, etc., and channel performance, e.g., in terms of medium availability (CCA and/or utilization).

RMD.R11 TR-181 [2] and WFA Data Elements [4] provide an extensive data model that facilitates home network diagnostics. Home network shall use TR-181 (together with WFA Data Elements) as the main data model. The operator may use vendor extensions to the data model if the data model does not address the operator's needs. The vendor extensions should support writable objects and commands for remote configuration.

RMD.R12 TR-181 should be the main common data model for collecting diagnostics data, setting and getting home-network wide parameters, running of remotely triggered functions.

RMD.R13 Frequently collected diagnostics data, for example, RSSI per STA per second, medium availability per channel per second etc., may be bundled (accumulated and/or compressed) and delivered in bundles periodically, e.g., every minute, every 10 minutes, etc., or may be delivered in terms of histograms, to the operator's cloud server to minimize communication overhead. The format used for bundling of the data and delivery of this bundled data to the cloud may be implementation specific. Note that bundling of frequently collected data and delivery of this bundle is needed, because frequent access from the cloud to local TR-181 data model for getting diagnostics data would create a significant overhead and would result in inefficient use of the communication system yielding performance degradation in terms of delayed responses, etc.

RMD.R14 Cloud diagnostics shall allow for historic data analysis. For that, the cloud server should be capable of storing the periodically collected home network data for a long term, e.g., for at least 1 month, and should allow for accessing the data for analysis when requested.

RMD.R15 Collection, processing, storage, accessing and displaying of home network diagnostics data shall comply with the data protection laws for the jurisdictions in which they operate.

RMD.R16 When the home network employs both a Gateway and Extenders, i.e., a WFA EasyMesh network, the diagnostics data shall include home-level data comprising data points for Gateway and each Extender.

RMD.R17 The diagnostics system may employ alarm events to notify the operators and the user about the critical instances that are detected during operation of the home network. The alarm events may be triggered from the CPE (i.e., Gateway, router, or AP) or from the cloud system. The alarm events may cover, for example, onboarding issues that may be encountered during onboarding of APs or clients to the network and may include descriptive guidance for the user, problematic disconnection issues, detected heavy interference, etc.

6.3 Cloud-Based Performance Management

RMD.R18 The remote management system shall be capable of running service quality diagnostics, such as but not limited to measuring speed, latency (and jitter) and coverage per home network.

RMD.R19 The remote management system shall provide means for comparison of a home network with an operator's deployment base with respect to measured Key Performance Indicators (KPIs). For this, commonality of collected data across different deployments is needed.

RMD.R20 The system should be capable of measuring Wi-Fi speed per home. The system may be capable of measuring broadband speed also, and in such cases, should be able to compare broadband and Wi-Fi speed to identify possible root causes for performance issues.

RMD.R21 Home networks with repeatedly occurring issues, e.g., coverage problems, high interference, should be detected and alarms should be fired to inform the operator in such cases.

RMD.R22 The users may be able to access the performance management data for example via a mobile application (as described in in 6.1).

6.4 Multi-AP Topology Management by the Operator

RMD.R23 The cloud-based home network management system should be able to monitor changes in the topology based on the historic long-term data collected in the cloud. The monitored topology data should allow for detecting changes at least (i) in the level of interference in the operating channel measured by each AP in the home network, (ii) link quality between the APs making up the home network.

RMD.R24 The system shall have an historic time series view of STA<->AP link quality, e.g., in terms of RSSI, transmit/receive PHY rate, expected throughput, achieved throughput. The historic view should span at least 1 month of data. The granularity of the historic view may be as low as 1 second between data points, but a reasonable separation between historic data points may be 1 minute or a few minutes.

RMD.R25 The system shall have an historic time series view of backhaul links, e.g., Gateway<->AP and AP<->AP links, in terms of RSSI, transmit/receive PHY rate, expected throughput, achieved throughput. The historic view should at least span 1 month of data, and minimum separation between consecutive data points can be as low as 1 second, but a reasonable separation may be 1 minute or a few minutes.

RMD.R26 The system should be able to determine a well-performing topology candidate for the home network and should be able to impose the determined topology to the home network. The topology changes can be realized by initiating backhaul steering request(s), as defined in WFA EasyMesh, to force the APs to form their backhaul links in the determined way. The remote system may utilize related TR-181 data model functions and parameters to trigger backhaul steering request at the home network.

RMD.R27 The system should be able to detect anomalies in the topology of a home network, e.g., missing AP, sub-optimally formed mesh network (for example, a daisy chain formed whereas a star topology would provide a better overall performance), and service disruptions. The system should be able to notify the operator and the user about the detected anomaly, and if a remedy to the anomaly is possible, such as by changing backhaul links, it should apply the remedy automatically.

RMD.R28 The remote topology management and the local home network topology management (through WFA EasyMesh Controller) should not contradict. In case of conflicting decisions from the cloud and EasyMesh Controller, the cloud decision should prevail. Yet, if the cloud decisions are not applicable to the home network due to a sudden change in the home network right after cloud decision was generated, for example, due to an AP being unavailable (e.g., switched off, temporarily unavailable due to Channel Availability Check (CAC), etc.), then EasyMesh Controller may disregard cloud decisions.

RMD.R29 The remote topology management should aim to maximize end-to-end throughput, i.e., STA to/from Gateway (with possible intermediate Extenders, when mesh is employed).

RMD.R30 The remote topology management should try to minimize topology re-arrangements to avoid possible service disruptions which may occur during reformation of backhaul links.

6.5 Coordinated Firmware Upgrade

All network devices sooner or later require their firmware to be updated for a multitude of reasons like security, bug fixing, new feature introduction. While this procedure has been worked out for broadband Gateways or standalone devices, multi-AP networks require special attention.

A multi-AP network must have the ability to update the firmware of its APs. This must be done with the least amount of impact on the end-user and the update method must be robust to avoid bricking APs.

Upgrading multiple devices is always tricky and requires some form of coordination. How complex the management function needs to be is typically influenced by properties of the APs (e.g., dual-image storage) or the network topology (e.g., tree vs. star vs. graph). Operators must consider that there is a network-wide upgrade procedure that ensures that all APs get upgraded without risking losing devices while minimizing the network downtime.

RMD.R31 There should be an application (i.e., microservice) either centralized in the network, e.g., in the Gateway, or in every AP that is able to download new firmware.

RMD.R32 There should be either a centralized or decentralized protocol that coordinates when and if a firmware update can be executed. The update protocol should be based on standards, e.g., Simple Network Management Protocol (SNMP), BBF TR-369 [3], Wi-Fi Data Elements™ [4].

RMD.R33 The update protocol should check various parameters, e.g., network business, topology, before triggering the update procedure.

RMD.R34 The update protocol should control which APs are updated. This procedure may be performed sequentially or at once.

RMD.R35 All APs should have the capability to be upgraded. Otherwise, the home network would continue to work in a non-homogeneous firmware environment.

RMD.R36 The update procedure should be deferred when traffic is present in the network so that the end-user impact can be minimized.

RMD.R37 The home network (via the implemented firmware upgrade protocol) should be able to report if a firmware upgrade was completed with success or aborted or failed due to an issue, including information such as, but not limited to, firmware version information (for previous and updated firmware), time the firmware upgrade was performed, the ID of the upgraded CPE (e.g., serial number, bridge MAC address, or any other unique identifier).

6.6 Device Management

This feature considers the necessity of remote device management. APs' Wi-Fi subsystems may need to be restarted remotely by the operator to continue their duty properly.

The operator may want to reset the Wi-Fi subsystem of the APs forming the user's home network to solve issues on the home network.

RMD.R38 A remote management system should be deployed at both ends (cloud and the AP).

RMD.R39 The management system should be one of TR-069, TR-369, or both.

RMD.R40 The management system shall allow for resetting the Wi-Fi subsystem of each AP in the home network.

7. Interoperability (IOP) Requirements

This section covers the OMWi recommendations for maintaining interoperability in the home network.

7.1 Managing a network with APs having different features

The home network must be able to be deployed, operated, and managed even if the APs/network nodes use/run different protocols, security modes, capabilities, software versions etc.

IOP.R1 The home network shall support a diversity of multiple different Wi-Fi protocols, e.g., Wi-Fi 4, Wi-Fi 5, Wi-Fi 6, Wi-Fi 6E, Wi-Fi 7.

IOP.R2 The home network shall support different security modes, e.g., WPA, WPA2, WPA3.

IOP.R3 The home network shall support different hardware configurations, e.g., a network with a mix of dual-band APs (2.4GHz + 5 GHz) and tri-band APs (2.4GHz + 5GHz + 6GHz).

IOP.R4 The home network shall support DFS.

8. Additional Applications/Services (Microservices) (MS)

Home network capabilities can be enhanced with additional applications that provide additional features to the user.

The Operator Managed Wi-Fi Reference Architecture shall allow applications to run on the Gateway or APs in the network, or in remote cloud servers.

The applications may be downloaded from cloud to the platform (Gateway or AP) or they may run in the cloud while they can utilize necessary APIs to gather data from the local devices and to execute commands on the local devices.

MS.R1 USP (TR-369) [3] may be utilized for downloading, upgrading, and maintaining the edge microservices.

MS.R2 USP may be utilized for management of cloud microservices.

MS.R3 Edge and cloud microservices should support a TR-181 [2] based common northbound API.

9. Platform/Device/Standards Requirements

In this section, we list the industry standards recommended by OMWi to be used in operator-managed residential networks, as well as the platform and the device requirements.

STD.R1 IEEE802.11n (Wi-Fi4), IEEE802.11ac (Wi-Fi5), IEEE802.ax (Wi-Fi6/6E), IEEE802.11be (Wi-Fi 7)

STD.R2 WFA Data Elements

STD.R3 WFA EasyMesh Release 2 or WFA EasyMesh Release 4 with profile 2.

STD.R4 Recommendation: WFA EasyMesh Release 6 (Wi-Fi 7)

STD.R5 WFA Wi-Fi Agile Multiband

STD.R6 WFA QoS Management

STD.R7 WFA Easy Connect (a.k.a. DPP)

STD.R8 WFA Wireless Simple Connect (WSC, a.k.a. WPS)

STD.R9 BBF TR-181

STD.R10 BBF TR-069

STD.R11 BBF USP (TR-369

Appendix

This section presents two of the prominent exemplary open-source implementations of the WBA's OMWi recommended architecture, namely the implementation from the prpl Foundation and the implementation from RDK-B [6].

It is worthwhile to note that prpl and RDK-B have their own flavours of the OMWi recommended architecture and might include additional components on top of OMWi architecture while they comply with the baseline requirements of the OMWi reference architecture.

9.1 prpl Foundation's Implementation

The prpl Foundation [5] is a broad community developing open-source CPE software that is fully compliant with open industry standards and open APIs, including WBA's OMWi. "prplWare" software components are designed and developed to be platform-independent and hence portable to any Linux-based router operating system, including field-deployments on RDK-B, other proprietary operating systems, and prpl's own prplOS. The prplWare software is developed on and for carrier-grade hardware with next-gen state-of-the-art SoCs.

Figure 5 depicts the prplWare Service Delivery Platform architecture, showing an identical match, component-by-component, with OMWi's Reference Architecture Recommendations in Figure 2, including the key industry-standardized components (e.g., WFA's EasyMesh & Data Elements, as well as BBF's TR-181 and USP with its various MTPs). The purple-colored blocks are prplWare components that are publicly available in free open-source. The USP-Broker component is depicted as both purple & green because that component is jointly developed by prpl and BBF [3] and is also available as free open-source.

The App Store enables operators to securely deploy innovative 3rd-party Apps & µServices onto CPE devices after they have been deployed in the field (i.e., without a traditional firmware update). A wide variety of innovative 3rd-party apps & µservices are gathered and curated as an App Store in the cloud, to be orchestrated by the deploying operator. From the cloud, they can be dynamically downloaded into the CPE to execute inside unprivileged containers where they run securely isolated from each other and from the core gateway middleware. The prpl LCM component manages the lifecycle of containerized apps & services, including the functions listed there and secure version-update maintenance over time. An SDK software-development kit provides a framework for facilitating development of innovative applications that may need intensive or real-time access to the device Data Model via the USP-Broker (which enforces role-based access controls for strong security).

Containerized apps & µservices can not only *consume* the device's Data Model, they can also Register their own objects into the device's Data Model via the USP-Broker. In this way, the prpl High-Level API becomes dynamic, allowing apps & µservices to interact with each other via the Data Model and via USP & iMTPs. The entire Data Model is also accessible from the cloud via USP, making the service delivery platform fully remotely manageable by the operator.

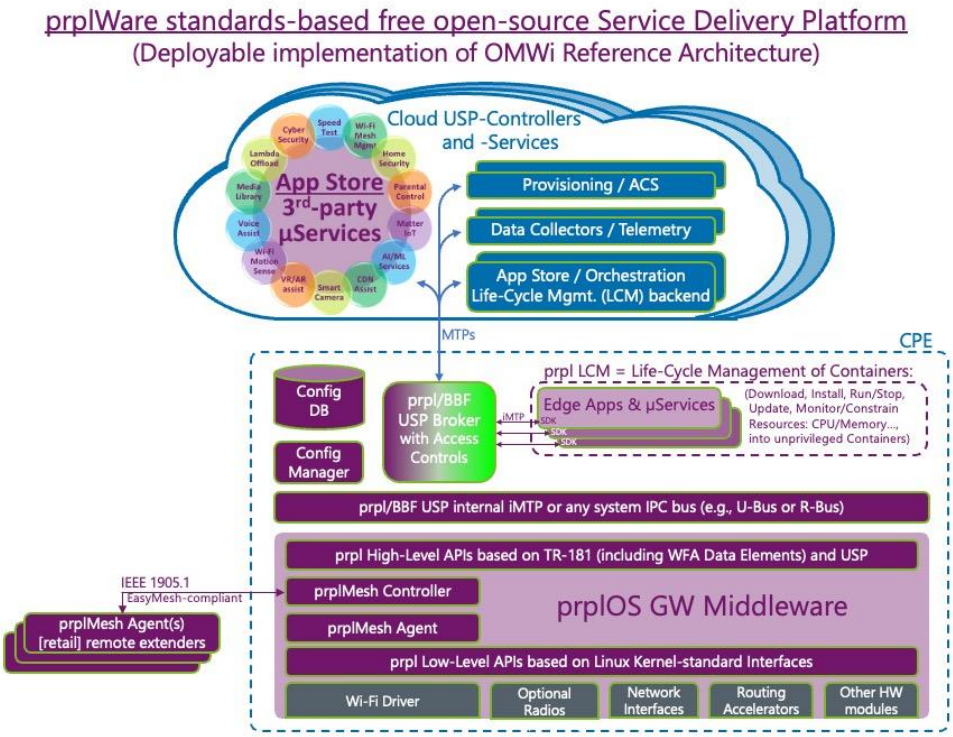

Figure 5: ppl Architecture Closely Matches, Component-by-Component, OMWi Reference Architecture from Figure 2

9.2 RDK-B's Implementation

RDK-B is the broadband-specific implementation of the Reference Design Kit (RDK). It is designed to standardize and accelerate the deployment of broadband services for service providers, with a standardized software stack that can be used across different hardware platforms and vendors ensuring consistency and interoperability while allowing for customization to add unique features.

RDK-B includes a variety of components playing key roles in the implementation of the WBA's OMWi:

1. RBUS (RDK-Bus) is an integral component of the RDK-B architecture. It is a middleware communication framework designed to facilitate efficient inter-process communication (IPC) within the RDK-B environment. RBUS provides via RBUS API's the northbound API's necessary to manage the internal representation of TR181 data model.
2. CCSP is the former IPC used for communication between RDK-B components, RBUS provides backwards compatibility for components that still make use of the CCSP API's as TR181 northbound management.
3. Hardware abstraction layer (HAL) in RDK-B abstract the hardware specifics to RDK-B components, the abstraction lays on top of the kernel but it will abstract proprietary drivers when necessary, allowing portability across different hardware platforms.
4. Protocol agents are RDK-B components that provide the interconnection between the CPE and different backend management implementations using different remote management protocols. RDK-B supports the main standard remote management protocols such as USP, TR69 or SNMP. In addition to standard remote management protocols support, RDK offers their own open-source management framework called Xmidt/WebPa, a fully end to end open-source framework, where in addition to the protocol agent implementation in the CPE, offers as well as open source, all the necessary components to implement

the management service at the backend. As part of the complete management implementation, WEBpa implements a translation service that provides a RESTful interface for TR-181 management-based devices. WEBpa uses as protocol message definition WRP (web routing protocol), a simple and fast framework based on the msgpack open-source project.

- DAC/Dobby is a lightweight and secure container management solution designed for embedded systems, particularly those used in broadband and video devices. It is a part of the RDK-B (Broadband) and RDK-V (Video) software stacks, providing a way to run applications and services in isolated environments to enhance security, manageability, and resource efficiency.
- Easy Mesh controller is part of the RDK-B landscape, and the first draft of fully portable RDK-B EasyMesh agent will be available during 2025. Current deployments in RDK-B for EasyMesh use the standard RDK-B controller in combination with EasyMesh agents provided by SoC vendors like Broadcom or Qualcomm.

Figure 6 illustrates the RDK-B Architecture in comparison to the WBA's OMWi reference architecture.

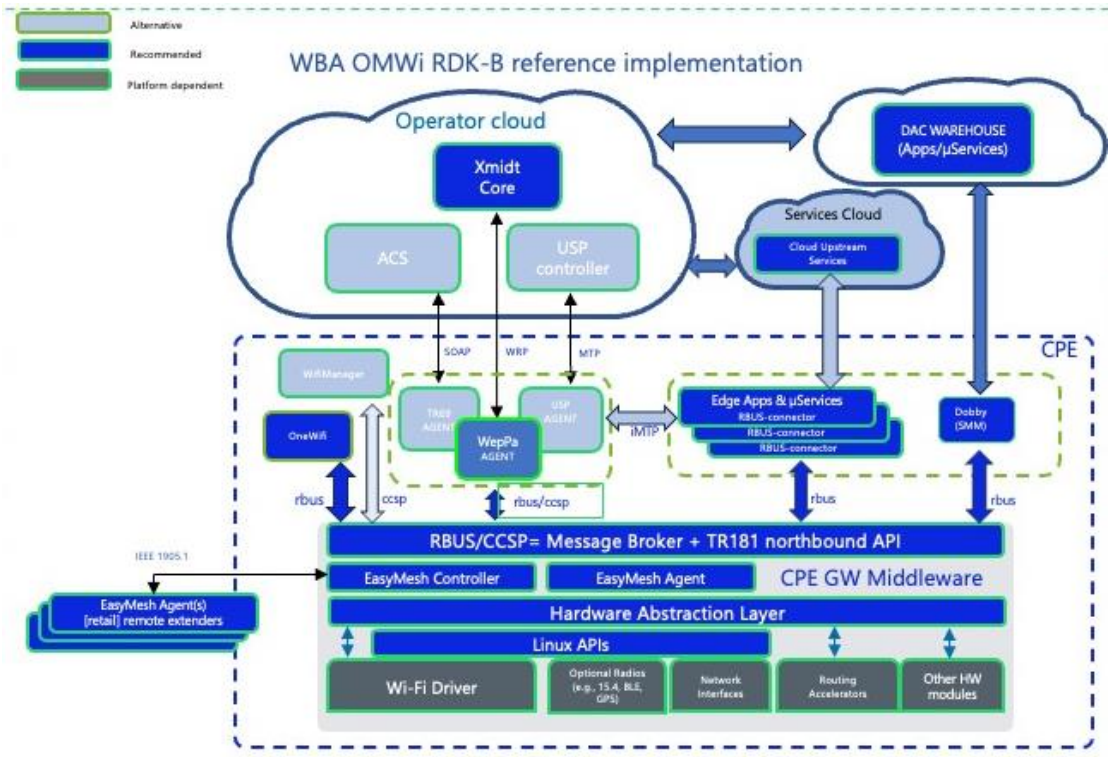

Figure 6: RDK-B Architecture

Links

1. RDK-B (https://wiki.rdkcentral.com/display/RDK/RDK+Broadband+Documentation)

2. XMIDT (https://xmidt.io/docs/introduction/overview/)

3. WEBpa (https://xmidt.io/docs/webpa/overview/)

4. WRP (https://xmidt.io/docs/wrp/overview/)

5. msgpack (https://msgpack.org/)

Acronyms and Abbreviations

Acronym / Abbreviation	Definition
AP	Access Point
API	Application Programming Interface
BBF	Broadband-Forum.org
CAC	Channel Availability Check
CCA	Clear Channel Assessment
CPE	Customer Premises Equipment
DAC	Downloadable Application Containers
DFS	Dynamic Frequency Selection
DPP	Device Provisioning Protocol
GUI	Graphical User Interface
GW	Gateway
iMTP	"internal" MTP used by containerized apps & µservices
IPC	Inter-Process Communication
ISP	Internet Service Provider
KPI	Key Performance Indicator
LCM	Life-Cycle Management of containerized apps & µservices
MTP	Message Transfer Protocol
OBSS	Overlapping Basic Service Sets
OSI	Open Systems Interconnection
OTT	Over the Top
prpl	prplFoundation.org
RDK-B	Reference design kit for broadband
SDK	Software Development Kit
SoC	System-on-a-Chip
STA	Station
UI	User Interface
U-Bus	a specific IPC mechanism
USP	User Services Platform
WFA	Wi-Fi Alliance = Wi-Fi.org
WPS	Wireless Protected Setup
WSC	Wireless Simple Connect
WRP	Web Routing Protocol

Participant List

Name	Company	Role
Sarper Gokturk	Airties	Project Leader & Chief Editor
Tom Van Driessche	Nokia	Project Co-leader
Pedro Caldeira dos Santos	Deutsche Telekom	Project Co-Leader
David Barr	Prpl Foundation	Project Co-Leader
Wouter Cloetens	Deutsche Telekom	Editorial Team
João Freitas	Deutsche Telekom	Editorial Team
Ken Kerpez	DZS	Editorial Team
Richard Lyda	Hotwire Communications	Editorial Team
Aleksandra Kozarev	MaxLinear	Editorial Team
Jeongmin Noh	LG U+	Editorial Team
Bill McFarland	Plume	Editorial Team
Jose Ramon Diaz Martinez	RDK	Editorial Team
Irfan Acar	Airties	Project Participant
Murat Guven	Airties	Project Participant
Ugur Ozcan	Airties	Project Participant
Metin Taskin	Airties	Project Participant
Omer Topal	Airties	Project Participant
Paul Plofchan	Amazon	Project Participant
Ravi Saxena	Aruba, an HPE company	Project Participant
Stuart Strickland	Aruba, an HPE company	Project Participant
Prince Boafo	AT&T	Project Participant
Kevin Franzen	AT&T	Project Participant
Jim Sturges	AT&T	Project Participant
Jessie Manik	Bell Mobility	Project Participant
Romin Jain	Boingo Wireless	Project Participant
Jonathan Campbell	Boldyn Networks	Project Participant
Florin Baboescu	Broadcom	Project Participant
Simon Ringland	BT	Project Participant
Tim Twell	BT	Project Participant
Steve Arendt	CableLabs	Project Participant
Zack Foreman	CableLabs	Project Participant
John Bahr	CableLabs	Project Participant
Tucker Polomik	CableLabs	Project Participant
Lili Hervieu	CableLabs	Project Participant
Josh Redmore	CableLabs	Project Participant
Luther Smith	CableLabs	Project Participant
Martin Casey	Calix	Project Participant
Sandeep Agrawal	CDOT	Project Participant
Tim Bleidorn	Charter Communications	Project Participant
Scott Dotto	Charter Communications	Project Participant
Kyle Johnson	Charter Communications	Project Participant
Loay Kreishan	Charter Communications	Project Participant

Dave Moran	Charter Communications	Project Participant
Shahid Ajmeri	Cisco	Project Participant
Steven Chung	Cisco	Project Participant
Mark Grayson	Cisco	Project Participant
Sri Gundavelli	Cisco	Project Participant
Paul Polakos	Cisco	Project Participant
Ruchi Kothari	Comcast	Project Participant
Brian Epstein	Comcast	Project Participant
John Hart	Comcast	Project Participant
Robert Jaksa	Comcast	Project Participant
Hussain Zaheer Syed	Comcast	Project Participant
Charles Cheevers	CommScope	Project Participant
Mark Hamilton	CommScope	Project Participant
David Lee	CommScope	Project Participant
Kurt Lumbatis	CommScope	Project Participant
Saurabh Mathur	CommScope	Project Participant
Scott Voegele	CommScope	Project Participant
Ian Wheelock	CommScope	Project Participant
Derrick Smith	Cox Communications	Project Participant
Angelos Mavridis	Deutsche Telekom	Project Participant
Sascha Dech	Deutsche Telekom	Project Participant
Bryan Wills	Deutsche Telekom	Project Participant
Hideaki Goto	Eduroam	Project Participant
Natalia Ermakova	ER-Telecom	Project Participant
Blaz Vavpetic	Galgus	Project Participant
Richard Zhou	Google	Project Participant
Yariv Bargil	Heights Telecom	Project Participant
Christian Gabetta	Heights Telecom	Project Participant
Richard Lyda	Hotwire Communications	Project Participant
John Belstner	Intel Corporation	Project Participant
Necati Canpolat	Intel Corporation	Project Participant
Dibakar Das	Intel Corporation	Project Participant
Mythili Hegde	Intel Corporation	Project Participant
Ingolf Karls	Intel Corporation	Project Participant
Valerie Parker	Intel Corporation	Project Participant
Rajendra Patil	Jio	Project Participant
Ravi Sinha	Jio	Project Participant
Wael Guibene	Jio	Project Participant
Tim Colleran	LEVL	Project Participant
Livia Rosu	MaxLinear	Project Participant
Gabor Bajko	MediaTek	Project Participant
James Chiang	MediaTek	Project Participant
Yonggang Fang	MediaTek	Project Participant
Justin Cardones	Meta	Project Participant
Michael Tseytlin	Meta	Project Participant
Dennis Edwards	Nokia	Project Participant
Thirumurthy Rajamanickam	Nokia	Project Participant

Max Riegel	Nokia	Project Participant
Randy Sharpe	Nokia	Project Participant
Tim Spets	Nokia	Project Participant
David Valerdi	Nokia	Project Participant
Thierry Van de Velde	Nokia	Project Participant
Luo Ye	Nokia	Project Participant
Jean-Michel BONNAMY	Orange	Project Participant
John Danner	Pavlov Media	Project Participant
Eran Dor	Pavlov Media	Project Participant
Subir Das	Peraton Labs	Project Participant
Hans Liu	Plume	Project Participant
Vasudevan Nagendra	Plume	Project Participant
Saurabh Verma	Rakuten Mobile	Project Participant
George Hart	Rogers	Project Participant
Betty Cockrell	Single Digits	Project Participant
Michael Sym	Single Digits	Project Participant
Sami Susiaho	SKY - Comcast Group	Project Participant
Gabriele Marruco	SKY Itália	Project Participant
Federico Lazzarin	SKY Itália	Project Participant
Kishore Rajasekharuni	STL	Project Participant
Edward Sun	Sun Global Broadband	Project Participant
Les Goldman	Syniverse	Project Participant
Brendan Malay	Telus	Project Participant
Samson Okulaja	Telus	Project Participant
Troy Cross	Tessares	Project Participant
Nicolas Keukeleire	Tessares	Project Participant
Burak Dogan	Turkcell	Project Participant
Dan Friedman	Viasat	Project Participant
Majid Mahmood	Viasat	Project Participant
Thad Mazurczyk	Viasat	Project Participant
Pedro Mouta	WBA	Project Participant
Bruno Tomás	WBA	Project Participant