Technical Report

TR-488

Operator Managed Residential/SOHO Network Architecture and Requirements

Issue: 1

Issue Date: September 2023

Notice

Issue History

Issue Number	Issue Date	Release Date	Issue Editor	Changes
1	September 2023	September 2023	Aleksandra Kozarev, MaxLinear Marcos Martinez Vazquez, MaxLinear	Original

Comments or questions about this Broadband Forum Technical Report should be directed to info@broadband-forum.org.

Editors: Aleksandra Kozarev, MaxLinear
Marcos Martinez Vazquez, MaxLinear
Mike Talbert, WNC

Broadband User Services (BUS) Work Area Directors: Jason Walls, QA Cafe
John Blackford, CommScope

Project Stream Leaders: Martin Casey, Calix
Mike Talbert, WNC

Table of Contents

Table of Figures

Table of Tables

Executive Summary

A Residential/SOHO network is the infrastructure needed for delivering Internet based services to end devices.

In general, modern residential/SOHO networks are composed of a mix of diverse connectivity and networking technology options, such as broadband wireless (Wi-Fi), broadband wireline (Ethernet, MoCA and G.hn) and IoT narrowband (Wi-Fi, Zigbee, Z-wave). These transmission technologies collaborate between themselves, creating a heterogeneous network infrastructure for distribution of content across the residential/SOHO network.

This Technical Report defines the different elements of such a heterogeneous network infrastructure. It also outlines the architectural, management, and operational aspects of the residential/SOHO network and derives requirements for the devices and technologies to cope with the needs of the delivery of Internet based services to end devices.

1 Purpose and Scope

1.1 Purpose

More than ever, Service Providers are looking to roll-out future-proofed fiber-grade services to quickly, easily, and cost-effectively deploy reliable broadband connectivity to end devices within residential and business environment using the most appropriate combination of technologies.

An important aspect of such deployments is to provide the most efficient residential/SOHO network infrastructure and components—devices, media, and services. Unfortunately, this segment has traditionally been the segment with the least amount of oversight by the service providers.

This Technical Report covers this gap by providing clarifications and insights into different aspects of the residential/SOHO infrastructure network.

1.2 Scope

This Technical Report provides insight into the following aspects of the Operator Managed Residential/SOHO Network (OMRN):

- Device classes, Topology Use Cases, Services and Connectivity Technologies
- Reference architecture of an End-to-End Service Network with examples of mapping Topology Use Cases to the reference architecture
- Management and operational aspects of an OMRN including management architecture, references to management specifications, use of an ACS, and diagnostics
- Functional and management recommendations specific to the OMRN architecture

This Technical Report also extracts from the previous mentioned points the main recommendations the heterogeneous residential/SOHO networks (and its building devices) should implement to successfully cover the necessities of service providers.

2 References and Terminology

2.1 Conventions

In this Technical Report, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found in RFC 2119 [23][15].

MUST	This word, or the term “REQUIRED”, means that the definition is an absolute requirement of the specification.
MUST 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 behavior is acceptable or even useful, but the full implications need to be understood and the case carefully weighed before implementing any behavior 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 MUST be prepared to inter-operate with another implementation that does include the option.

2.2 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.

A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

Document	Title	Source	Year
[1] TR-069 Amendment 6 Corrigendum 1	CPE WAN Management Protocol	BBF	2022
[2] TR-369 Issue: 1 Amendment 2	User Services Platform (USP), https://www.broadband-forum.org/technical-reports and https://usp.technology/specification/	BBF	2022
[3] TR-181 Issue 2 Amendment 15	Device Data Model, https://www.broadband-forum.org/technical-reports and https://usp-data-models.broadband-forum.org	BBF	2022
[4] TR-124 Issue 7	Functional Requirements for Broadband Residential Gateway Devices	BBF	2022
[5] TR-301 Issue 2 Amendment 1	Architecture and Requirements for Fiber to the Distribution Point	BBF	2022
[6] TR-419 Issue 2	Fiber Access Extension over Existing Copper Infrastructure	BBF	2022
[7] MR-419	Utilizing Existing Copper Infrastructure for Deployment of Fiber-grade Services	BBF	2021
[8] GSTP-HNAFS	Architecture, functions and services of home network	ITU-T	2021
[9] GSTP-FTTR	Use cases and requirements of fiber-to-the-room (FTTR)	ITU-T	2021
[10] GSTP-OVHN	Overview of ITU-T G.hn technology	ITU-T	2021
[11] TPLS.G-HN	Operation of G.hn technology over access and in-premises phone line medium	ITU-T	2015
[12] TP-UC-HN	Technical paper on the use of ITU-T G.hn technology for in-home networking	ITU-T	2022
[13] G.hetnet	Terminology and overview of the architecture of a Heterogeneous Home Network	ITU-T	202x

[14]	G.fin	High speed fiber-based in-premises transceivers	ITU-T	202x
[15]	G.9962 (2018) Amendment 1	Unified high-speed wire-line based home networking transceivers – Management specification	BBF	2020
[16]	IEEE 802.11-2020	IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", https://ieeexplore.ieee.org/document/9363693	IEEE	2020
[17]	Specification	Wi-Fi Data Elements Specification, Release 2.1	WFA	2021
[18]	Specification	Wi-Fi EasyMesh Specification (https://www.wi-fi.org/discover-wi-fi/specifications)	WFA	2021
[19]	Specification	Wi-Fi QoS Management Specification, (https://www.wi-fi.org/discover-wi-fi/specifications)	WFA	2021
[20]	TR-356	Alternate Management Path for Broadband	BBF	2016
[21]	Technical Paper	In-Home Wi-Fi Industry Guidelines (https://wballiance.com/resources/wba-white-papers/)	WBA	2019
[22]	White Paper	The Rise of the App-Enabled Services Gateway	BBF	2022
[23]	RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	IETF	1997
[24]	RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words	IETF	2017
[25]	TR-436	Access & Home Network O&M Automation/Intelligence	BBF	2021
[26]	TR-452.1	Quality Attenuation Measurement Architecture and Requirements	BBF	2020
[27]	TR-471	Maximum IP-Layer Capacity Metric, Related Metrics, and Measurements	BBF	2021
[28]	TR-456 Issue 2	AGF Functional Requirements	BBF	2022
[29]	TR-470 Issue 2	5G Wireless Wireline Convergence Architecture	BBF	2022
[30]	IEEE 802.3-2022	IEEE Standard for Ethernet https://ieeexplore.ieee.org/document/9844436	IEEE	2022
[31]	Specification	MoCA Home™ Networking Technology https://mocalliance.org/technology/index.php	MoCA	2022
[32]	Technical Paper	Wi-Fi Generations https://www.wi-fi.org/discover-wi-fi	WFA	2022
[33]	White paper	In-Home Wi-Fi (https://wballiance.com/resources/wba-white-papers/)	WBA	2021
[34]	Technical paper	State of Wi-Fi Reporting http://dynamicspectrumalliance.org/wp-content/uploads/2021/06/ASSIA-DSA-Summit-Presentation-v7.8.pdf		2021

2.3 Definitions

The following terminology is used throughout this Technical Report.

Term	Definition
Access Network	The Access network is specifically how the home or premise is connected to the Service Provider's network infrastructure. Access network could be Fiber, Copper or Wireless (e.g.: 5G)
Backhaul	Backhaul is the connection of network elements within the LAN and can be either wired or wireless technology. This would include connections from the RGW to Extenders / Access Points or IOT Hubs
Ethernet	Ethernet is a family of wired computer networking technologies specified by IEEE that is commonly used in local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN).
Fronthaul	Fronthaul is normally defined as the connection from an ED (or client device) to the network infrastructure within the home or premise. Usually, fronthaul is defined as the Wi-Fi interface for ED
FTTep	Broadband Forum's architecture (Fiber to the extension point) where the fiber is extended by using a copper medium without causing significant degradation in QoE compared to the FTTH.
Gateway	An Internet Gateway provides a connection between the access network and residential/SOHO network. It can be implemented as a single-box solution (residential gateway (RG) e.g., fixed network (FN-RG) or 5G residential gateway (5G-RG), cable modem or FTTx modem) or a multiple-box solution (residential gateway connected to a residential/SOHO cconnectivity network (RCN) e.g., Wi-Fi Extender or a primary Wi-Fi access point with an integrated Wi-Fi EasyMesh Controller functionality).
G.hn	HomeGrid Forum's name for the gigabit home networking technology standard and delivering broadband service over existing wiring (coax, twisted pair, powerline, and plastic optical fiber) specified in ITU-T Recommendations G.996x.
G.hn Access	Use of G.hn technology based on ITU-T Recommendations G.996x in broadband access applications, like Broadband Forum's Fiber-to-the-Extension-point (FTTep).
GiGAWire™	HomeGrid Forum's name for G.hn Access.
In-home network	Synonym for Residential/SOHO Connectivity Network
RCNMS	Residential/SOHO Connectivity Network Management System is the core of the operator managed end user network (OMRN) management system and refers to a system for managing infrastructure network (MIN), devices (ED and RCD) and services.
Home	Synonym for Residential/SOHO environment
LiFi	LiFi is wireless communication technology which utilizes light modulation to transmit data defined in ITU-T G.9991 Recommendation (G.vlc) that extends wireline G.hn networking technology and is capable of transmitting data at high speeds over the visible light, ultraviolet and infrared spectrums
MoCA Home	MoCA (Multimedia over Coax Alliance) gigabit home networking (mesh) technology standard over coaxial wiring.

MoCA Access	MoCA (Multimedia over Coax Alliance) gigabit access technology for connecting homes in an MDU over coaxial wiring.
prpl Foundation	prpl is a diverse community of Service Providers, OEMs, Silicon Vendors, ISVs, and open-source developers committed to Open-Source and Open-APIs in support of Open Gateway CPE.
Wi-Fi	Wi-Fi is a family of wireless network protocols, based on the IEEE 802.11 family of standards, which are commonly used for local area networking of devices and Internet access, allowing nearby digital devices to exchange data by radio waves.

2.4 Abbreviations

This Technical Report uses the following abbreviations:

Term	Definition
AEN	Access Extension Network
AN	Access Network
AP	Access Point
ASG	App-Enabled Services Gateway
DSCP	Differentiated Service Code Point
ENT	Extended Network Terminal
ED	End Device
FTTR	Fiber to the Room
FTTP	Fiber to the Premises
GW	Internet Gateway
IoT	Internet of Things
IPTV	Internet Protocol Television
MDU	Multiple Dwelling Unit
MIN	Managed Infrastructure Network
Multi-AP	Multiple Access Points
NT	Network Terminal
OMRN	Operator Managed Residential/SOHO Network
PAN	Personal Area Network
PCP	Port Control Protocol
PLC	Powerline Communications
PLA	Powerline adapter
PRE	Powerline Repeater/Extender
QoE	Quality of Experience
QoS	Quality of Service
RCD	Residential/SOHO Connectivity Device
RCN	Residential/SOHO Connectivity Network
RCNMS	RCN Management System
RG	Residential Gateway

SAN	Sensor Area Network
SDU	Single Dwelling Unit
SFU	Single Family Unit
SOHO	Small Office, Home Office
STB	Set Top Box
STA	Client Device (or EUD)
WMM	Wi-Fi Multi-Media
WRE	Wi-Fi Repeater/Extender

3 Technical Report Impact

3.1 Energy Efficiency

TR-488 does not explicitly define requirements for energy efficiency.

3.2 Security

Security of communications in its entirety in the Operator Managed Residential/SOHO reference architecture has a goal to enable reliable broadband connectivity to interoperable devices using the most appropriate combination of communication technologies and is considered as the highest priority from end-to-end. TR-488 does not explicitly define security requirements, instead it utilizes benefits of the widely deployed industry standards by providing an exemplary list of references.

3.3 Privacy

For an individual or group of users, privacy is the highly important asset of information to control or influence related to what data may be collected, processed, and stored and by whom, and to whom that information may be disclosed. As with the Security, TR-488 does not explicitly define privacy requirements but references other standards.

4 Operator Managed Residential/SOHO Network

This section presents typical Operator-Managed Residential/SOHO Network (OMRN) example topologies that deliver Intranet based services to end users.

To better understanding the different functional and operational requirements for the Residential/SOHO Connectivity Devices (RCD) and the connected End Devices (ED) within the End-to-End Service Network, devices are categorized into a set of device classes.

4.1 Device Classes

In general, devices are categorized by mobility type and connectivity type:

- Mobility type: Fixed vs Nomadic
- Connectivity type: Infrastructure / Residential/SOHO Connectivity Device (RCD) vs End Device (ED)

Figure 1 illustrates the various device classes (Dclass.1 – Dclass.4).

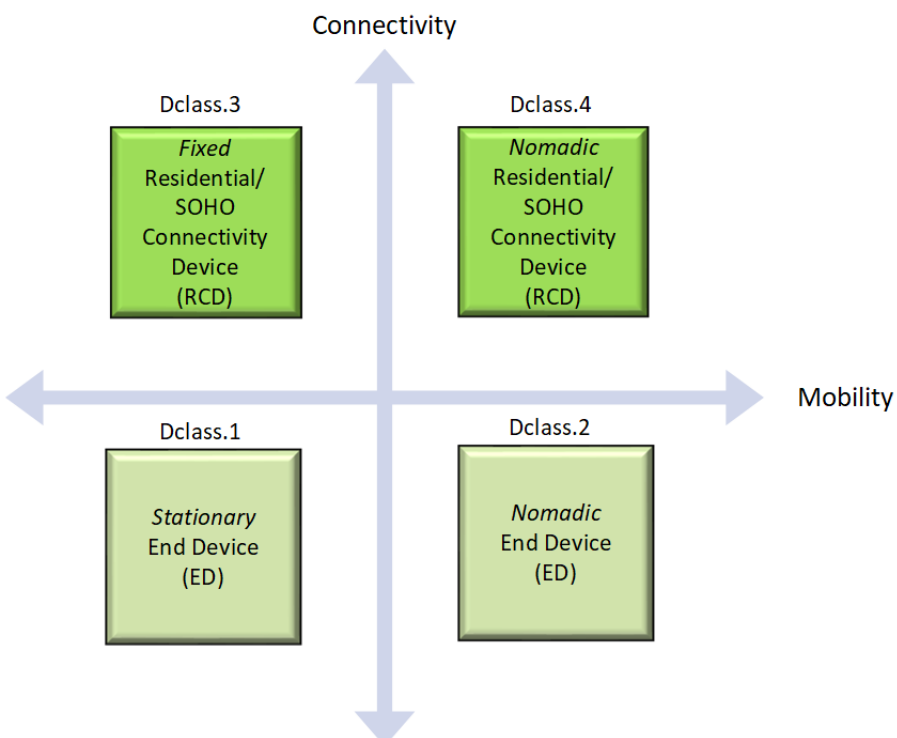

Figure 1 – Device classes

Within both mobility types, there are legacy devices that are connected via wired or wireless technology as well as gateway devices that use Internet-of-Things (IoT) protocol for communication. Sometimes the hardware specific IoT gateway communication protocol is located within the RG, or sometimes an additional hub to service as a bridge from the RG to the IoT gateway communication protocol would be required. It is commonly understood that the IoT devices can be connected directly to the RG portion of the Local Area Network (LAN), connected to the RG via additional hub or service gateway, or connected to a nomadic device that is connected to the LAN.

4.1.1 Fixed Devices

Stationary devices are normally fixed in a single location. Stationary devices that are part of the network infrastructure are either connected to the RG via a wired technology (Ethernet, G.hn, MoCA) or via a wireless technology (Wi-Fi). These types of devices are usually referred to as Switches, Access Points (AP), Wi-Fi Extenders, or Wi-Fi Repeaters and serve to extend the capabilities of the RG.

A stationary infrastructure device like a switch, wireless AP, extender or repeater do not usually move once placed inside the customer premise and optimized for signal performance.

Stationary devices also include interactive or consumption type devices that are usually in a fixed location, for example, a desktop computer or streaming media device (TV set, Set Top Box, Gaming Station, etc.).

Additionally, there could be “stationary” devices that may be moved to a different location for any number of reasons. An example of these devices could be a Gaming Station, voice assistant, or streaming media device. These devices are usually stationary due to the fact that they are not battery powered but derive their power from fixed electrical supply locations. (e.g., wall outlets).

4.1.2 Nomadic Devices

Nomadic devices are not in a fixed location but move around the customer premises, and normally are connected via a wireless technology like Wi-Fi. However, they could also be connected to an IoT specific RG communication protocol like Bluetooth, Zigbee, Zwave, etc.

Nomadic devices are usually things like tablets, mobile phones, XR glasses that do not have a defined fixed location.

4.2 Topology Use Cases

While Section 5 describes a reference network architecture for deployment of operator-grade broadband services to subscribers within the managed residential/SOHO network infrastructure, the remainder of this section is dedicated to understanding any additional level of intelligence in the end user network infrastructure that devices should utilize.

Topology use cases are important to better understand the options for optimizing the network infrastructure, but also having control of the consumers (Eds and RCDs) of that network infrastructure. An operator-managed residential/SOHO network solution should consider the following topology use cases listed in Table 1 and further described in subsequent sub-sections.

Table 1 –Topology Use Cases

Type	Use Case Name	Characteristic features	Description
1	**Direct connectivity to RG**	Best-effort type of connectivity to end devices (ED)	This use case provides the typical wireless connectivity for nomadic devices to the RG or retail IoT gateway. Fixed ED devices can also be connected to the RG through Ethernet cables or powerline/MoCA adapters.
2	**Improved connectivity to RG**	Best-effort-and-patches type of connectivity to end devices (ED) using wired or wireless Wi-Fi Repeater/Extender devices	This use case amends the direct connectivity use case in that it improves limited Wi-Fi network coverage and performance. In this case, users are typically reaching for retail or service provider Repeater/Extender devices, usually Wi-Fi but also powerline.
3	**Multi-AP Network – Retail**	Improved in-home wireless connectivity (coverage and performance) to end devices	Multi-AP Wi-Fi network is composed primarily of wireless links between a primary access point (often integrated in the RG) and

		(ED) by using Multi-AP Wi-Fi network without leveraging the existing in-home communication infrastructure.	multiple multi-band networking devices (secondary or extender access points/nodes) that create a seamless and reliable Wi-Fi connection throughout the entire home. This retail approach is most beneficial for minimizing customer installation costs being that it is easy to install and extend.
4	**Multi-AP Network – MDU**	Advanced in-home wireless connectivity (coverage and performance) to end devices (ED) by using Multi-AP Wi-Fi network and leveraging the existing in-home communication infrastructure	Multi-AP Wi-Fi network is composed of wired and wireless links between a primary access point (often integrated in the RG) and multiple multi-band networking devices (secondary or extender access points/nodes) that creates performance optimized and reliable Wi-Fi connection throughout the entire home. This approach is commonly used by service providers in multi-dwelling deployments (MDU) to ensure overall Wi-Fi network spectrum is optimally shared between fronthaul and backhaul links by employing wired backhaul technologies wherever possible, as well as control and management of multiple access points in a network.
5	**Multi-AP Network – Greenfield**	Optimized in-home wireless connectivity (coverage and performance) to end devices (ED) by using Multi-AP Wi-Fi network and building new in-home communication infrastructure	This approach is commonly used by service providers in greenfield deployments. The Wi-Fi network radio spectrum resources are optimally shared between the "backhaul" (wired and wireless) links and "fronthaul" (primarily wireless) links, in that different technology options for connecting multiple access points are available. For example, Ethernet (over Cat6 cables), fiber-to-the room (FTTR), fiber-to-the-premises (FTTP) or other multi-gigabit solutions not currently existing in premises.

4.2.1 Topology Use Case 1: Direct connectivity to RG

More details about the device classes and other characteristic features of the Use Case "Direct connectivity to RG" are given in Table 2 and in

Figure 2.

Table 2 –Topology Use Case 1 Features list

Device Classes		**Characteristic features**
End Devices (ED)	**Dclass.1 – Fixed stationary**	Connected wirelessly to the RG or through an Ethernet cable to the RG. Powerline/MoCA adapters may be used to connect sensitive devices (e.g., IPTV STB) to the RG.
	Dclass.1 – Fixed movable stationary	Connected wirelessly to the RG. Ethernet cable, powerline/MoCA adapters may be used to connect sensitive devices to the RG.
	Dclass.2 – Nomadic	All mobile devices (e.g., smartphones, Google Nest smart home devices, Amazon Alexa-enabled devices, Apple HomeKit devices, Philips Hue smart lighting devices, and

		other smart home devices) in the home are directly connected to the RG or retail IoT gateway wirelessly.
Residential/SOHO Connectivity Devices (RCD)	**Dclass.3 – Fixed**	RG or IoT gateways for connecting sensors/devices in wired SAN.
	Dclass.4 – Nomadic	IoT gateways for connecting sensors/devices in wireless SAN.
Residential/SOHO Connectivity Network (RCN)		**Characteristic features**
Wi-Fi Roaming		N/A
Wi-Fi Performance Experience		Moderate to Poor
RCN Management System (RCNMS)		Typical device and RG management by the service provider (e.g., through CWMP, USP or some other management system)

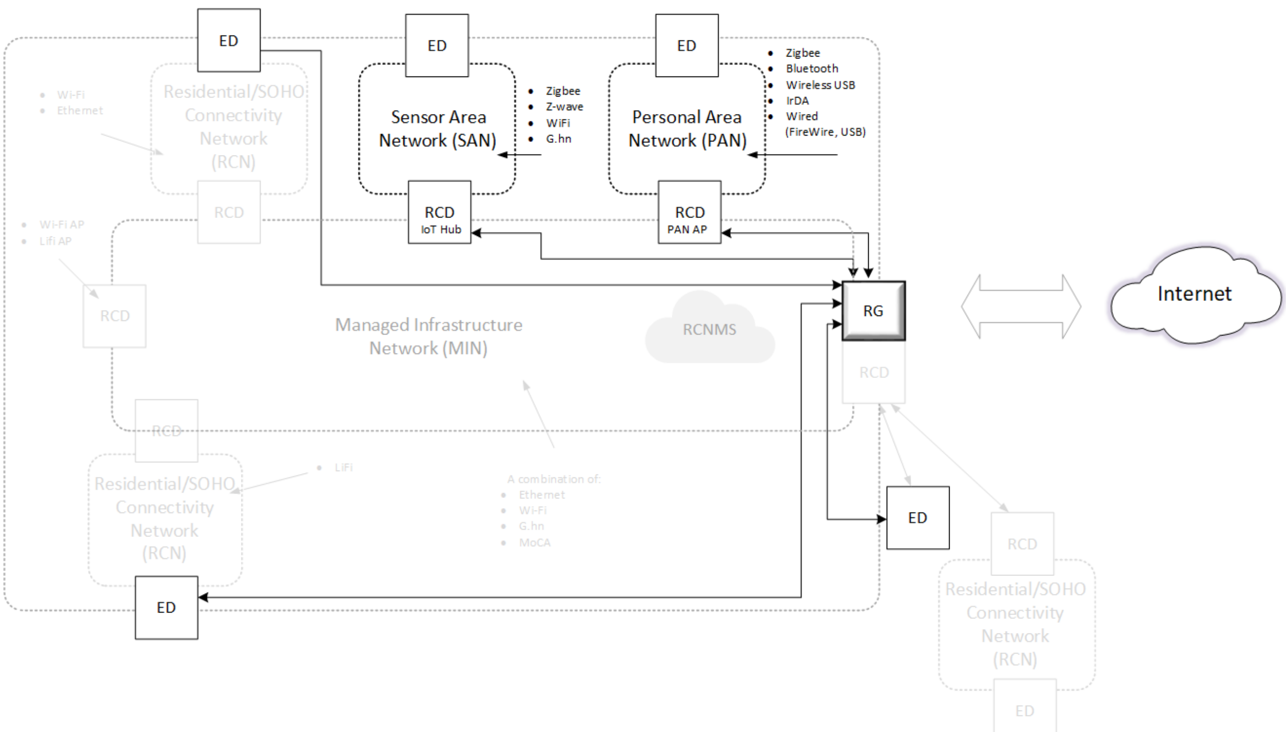

Figure 2 – Topology Use Case 1: *Direct connectivity to RG*

4.2.2 Topology Use Case 2: Improved connectivity to RG

More details about the device classes and other characteristic features of the Use Case "Improved connectivity to RG" are given in Table 3 and in Figure 3.

Table 3 – Topology Use Case 2 Features list

Device Classes		**Characteristic features**
End Devices (ED)	**Dclass.1 – Fixed stationary**	Connected wirelessly to the RG or through an Ethernet cable to the RG. Powerline/MoCA adapters may be used to connect sensitive devices (e.g., IPTV STB) to the RG.

	Dclass.1 – Fixed movable stationary	Connected wirelessly to the RG. Ethernet cable, powerline/MoCA adapters may be used to connect sensitive devices to the RG.
	Dclass.2 – Nomadic	All mobile devices (e.g., smartphones, Google Nest smart home devices, Amazon Alexa-enabled devices, Apple HomeKit devices, Philips Hue smart lighting devices, and other smart home devices) in the home are directly connected to the RG or retail IoT gateway wirelessly.
Residential/SOHO Connectivity Devices (RCD)	**Dclass.3 – Fixed**	RG or IoT gateways for connecting sensors/devices in wired SAN. Wi-Fi coverage area improved with the residential/SOHO connectivity network (RCN) by connecting retail or service provider Repeater/Extender devices, usually Wi-Fi but often Ethernet or powerline.
	Dclass.4 – Nomadic	IoT gateways for connecting sensors/devices in wireless SAN. Wi-Fi coverage area improved by connecting retail or service provider Wi-Fi Repeater/Extender devices and utilizing the RCN.
Residential/SOHO Connectivity Network (RCN)		**Characteristic features**
Wi-Fi Roaming		N/A
Wi-Fi Performance Experience		Excellent to good
RCN Management System (RCNMS)		Typical device and RG management by the service provider (e.g., through CWMP or USP). Repeaters/ Extenders (APs) should not be excluded from the RCN Management System (RCNMS) as they play a key role in the management of all connected devices.

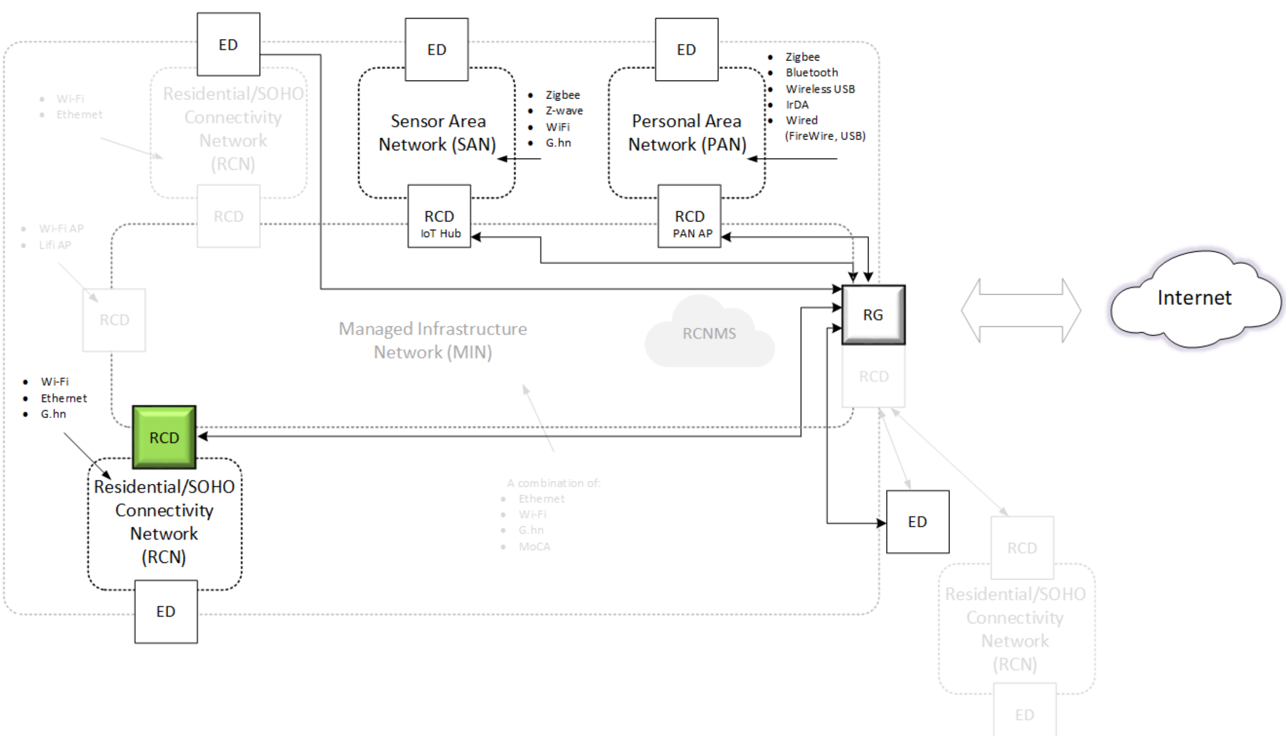

Figure 3 – Topology Use Case 2: *Improved connectivity to RG*

4.2.3 Topology Use Case 3: Multi-AP Network – Retail

More details about the device classes and other characteristic features of the Use Case “Multi-AP Network - Retail” are given in Table 4 and in Figure 4.

Table 4 –Topology Use Case 3 Features list

Device Classes		Characteristic features
End Devices (ED)	**Dclass.1 – Fixed stationary**	Mainly connected wirelessly to an AP in a multi-AP in-home network. Alternative connecting option to some wireless links through an Ethernet cable or powerline/MoCA may be used when better Wi-Fi performance is required.
	Dclass.1 – Fixed movable stationary	Mainly connected wirelessly to an AP in a multi-AP in-home network. Alternative connecting option to some wireless links through an Ethernet cable or powerline/MoCA may be used when better Wi-Fi performance is required.
	Dclass.2 – Nomadic	All mobile devices (e.g., smartphones, Google Nest smart home devices, Amazon Alexa-enabled devices, Apple HomeKit devices, Philips Hue smart lighting devices, and other smart home devices) in the home are connected wirelessly to an AP in the in-home MIN network (including the one integrated in the RGW) or retail IoT gateway wirelessly.
Residential/SOHO Connectivity Devices (RCD)	**Dclass.3 – Fixed**	Multiple access points (multi-AP) network or IoT gateways for connecting sensors/devices in wired SAN. In a multi-AP in-home network, a primary AP provides broadband access. The secondary APs are connected to the primary AP through backhaul Wi-Fi links and in this way connected to the Internet. All APs, including the primary AP, provide Wi-Fi coverage to devices in the home. Multi-AP network is composed mainly of wireless links. For better performance, Wi-Fi backhaul connections to the primary AP may be replaced with wired links to the user (e.g., Ethernet, Powerline or MoCA).
	Dclass.4 – Nomadic	Multiple access points (multi-AP) network or IoT gateways for connecting sensors/devices in wired SAN. In a multi-AP in-home network, a primary AP provides broadband access. The secondary APs are connected wirelessly to the primary AP through backhaul Wi-Fi links and in this way connected to the Internet. All APs, including the primary AP, provide Wi-Fi coverage to devices in the home.
Residential/SOHO Connectivity Network		**Characteristic features**
Wi-Fi Roaming		Seamless
Wi-Fi Performance Experience		Excellent to good
RCN Management System (RCNMS)		Needs a management function controlled by service provider either in the edge or in the cloud. Typical approaches are to either manage RCD, and possibly ED via RCD, locally in the edge (device and RG management) or to manage RCD, and possibly ED, directly in the cloud-based management system. There may be also multiple management systems, e.g., for multiple services or with multiple managing entities.

Figure **4** illustrates a case where the existing Wi-Fi router (in the RG) is replaced with a network that consists of four Wi-Fi access point units, the primary one AP and three secondary ones AP1, AP2 and AP3. Data traffic is distributed among the access points over “backhaul” wireless links represented by the dotted green lines. The most remote Access point AP3 is positioned out of range from the gateway and requires a double hop through one of the less remote access points, AP1 or AP2, over two different backhaul links. The dashed black lines in this figure represent the “fronthaul” links.

Given that in this topology there is no longer a need to switch between the obsolete Wi-Fi of the router and a Wi-Fi multi-AP, seamless connectivity of the Eds to the strongest access point is always enabled without changing connection data. Particularly in the case of older routers, this also results in enhanced Wi-Fi performance.

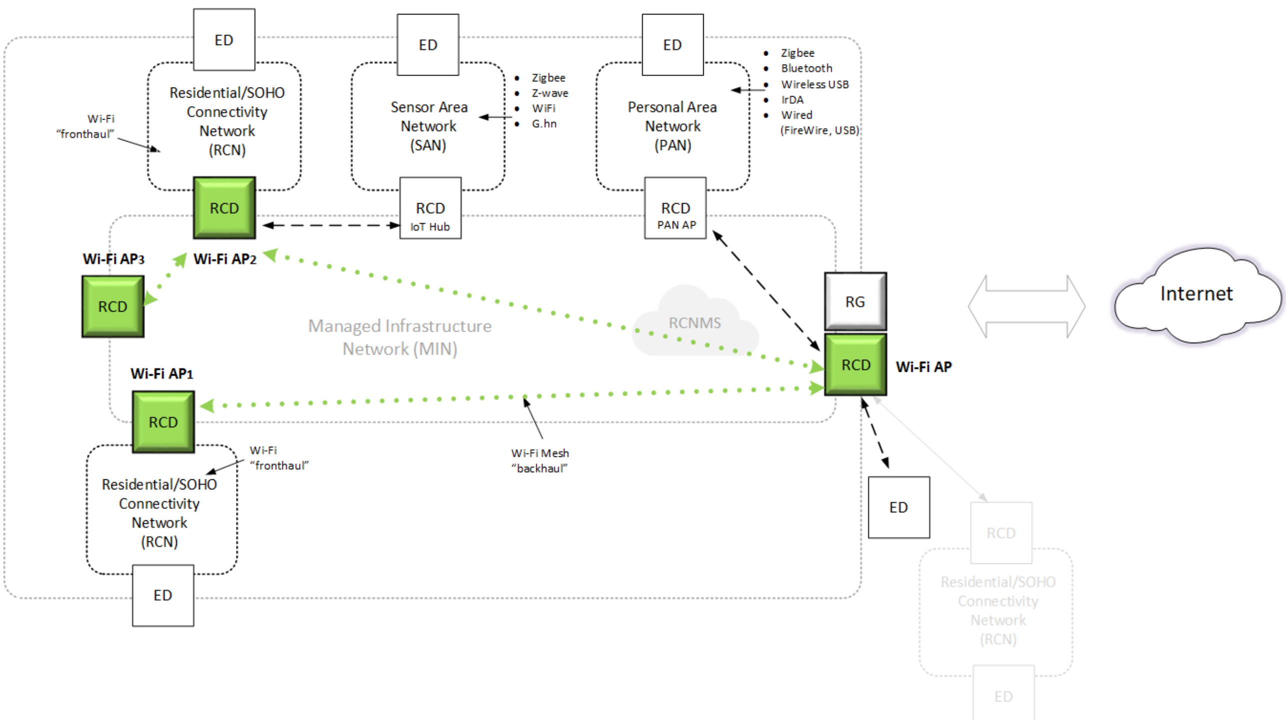

Figure 4 – Topology Use Case 3: *Multi-AP Network - Retail*

4.2.4 Topology Use Case 4: Multi-AP Network – MDU

More details about the device classes and other characteristic features of the Use Case “Multi-AP Network – MDU” are given in Table 5 and in Figure 5.

Table 5 –Topology Use Case 4 Features list

Device Classes		Characteristic features
End Devices (ED)	**Dclass.1 – Fixed stationary**	Mainly connected wirelessly to an AP in a multi-AP in-home network. Alternative connecting option to some wireless links through an Ethernet cable or powerline/MoCA may be used when better Wi-Fi performance is required.
	Dclass.1 – Fixed movable stationary	Mainly connected wirelessly to an AP in a multi-AP in-home network. Alternative connecting option to some

		wireless links through an Ethernet cable or powerline/MoCA may be used when better Wi-Fi performance is required.
	Dclass.2 – Nomadic	All mobile devices (e.g., smartphones, Google Nest smart home devices, Amazon Alexa-enabled devices, Apple HomeKit devices, Philips Hue smart lighting devices, and other smart home devices) in the home are connected wirelessly to an AP in the in-home MIN network (managed infrastructure network), including the one integrated in the RG or retail IoT gateway wirelessly.
Residential/SOHO Connectivity Devices (RCD)	**Dclass.3 – Fixed**	Multiple access points (multi-AP) or IoT gateways for connecting sensors/devices in a SAN. In a multi-AP in-home network, a primary AP provides broadband access. The secondary APs are connected to the primary AP through backhaul links and in this way connected to the Internet. All APs, including the primary AP, provide Wi-Fi coverage to devices in the home. Multi-AP network is composed of a combination of wireless backhaul links and various wired backhaul technologies, such as Ethernet, G.hn or MoCA. Unlike the Ethernet backhaul solution that requires dedicated cables for interconnections of access points, G.hn technology operates over almost any type of wiring available in residential environments, such as AC power lines, coaxial cables, and twisted-pairs (e.g., phone-line cables). Transporting backhaul traffic over the existing AC powerlines (PLC) is particularly convenient because AP devices are all AC-powered. MoCA technology is another convenient backhaul option that makes use of existing coaxial cables, which typically distribute cable television signals, to transport backhaul traffic between multiple AP devices at Ethernet-like throughput rates.
	Dclass.4 – Nomadic	Multiple access points (multi-AP) or IoT gateways for connecting sensors/devices in a SAN connected to the in-home MIN network primarily through wireless backhaul links.
Residential/SOHO Connectivity Network		**Characteristic features**
Wi-Fi Roaming		Possible
Wi-Fi Performance Experience		Excellent to good
RCN Management System (RCNMS)		By the means of its management system, in-home MIN networks utilize multiple APs able to work together and adapt to changing network conditions, thus providing extended network coverage, increased performance, capacity and effective throughput, and high-quality user experience in all areas of home with no dead spots. Industry standards, like Wi-Fi EasyMesh from the WFA and prplMesh, an open-source software implementation of a carrier-grade mesh Wi-Fi solution from the prpl Foundation, facilitate management system implementations built on a reliable multi-vendor interoperability. Cloud-based and edge-based management systems are commonly used approach by service providers, although other options, like hybrid management systems or systems with multiple managing entities, are also possible.

Figure 5 illustrates a case when the existing Wi-Fi router (in the RG) is replaced with a network that consists of four Wi-Fi access point units, the primary one AP and three secondary ones AP1, AP2 and AP3. Data traffic is distributed among the access points over two "backhaul" options, wireless and wired, on a ground-breaking G.hn basis over the existing AC powerlines. Wireless links are represented by the dotted green lines, while the wired links are represented by the dotted red lines. The most remote Access point AP3 is positioned out of range from the gateway and requires a double hop through one of the less remote access points, AP1 or AP2, over two different backhaul links. The dashed black lines in Figure 5 represent the "fronthaul" links.

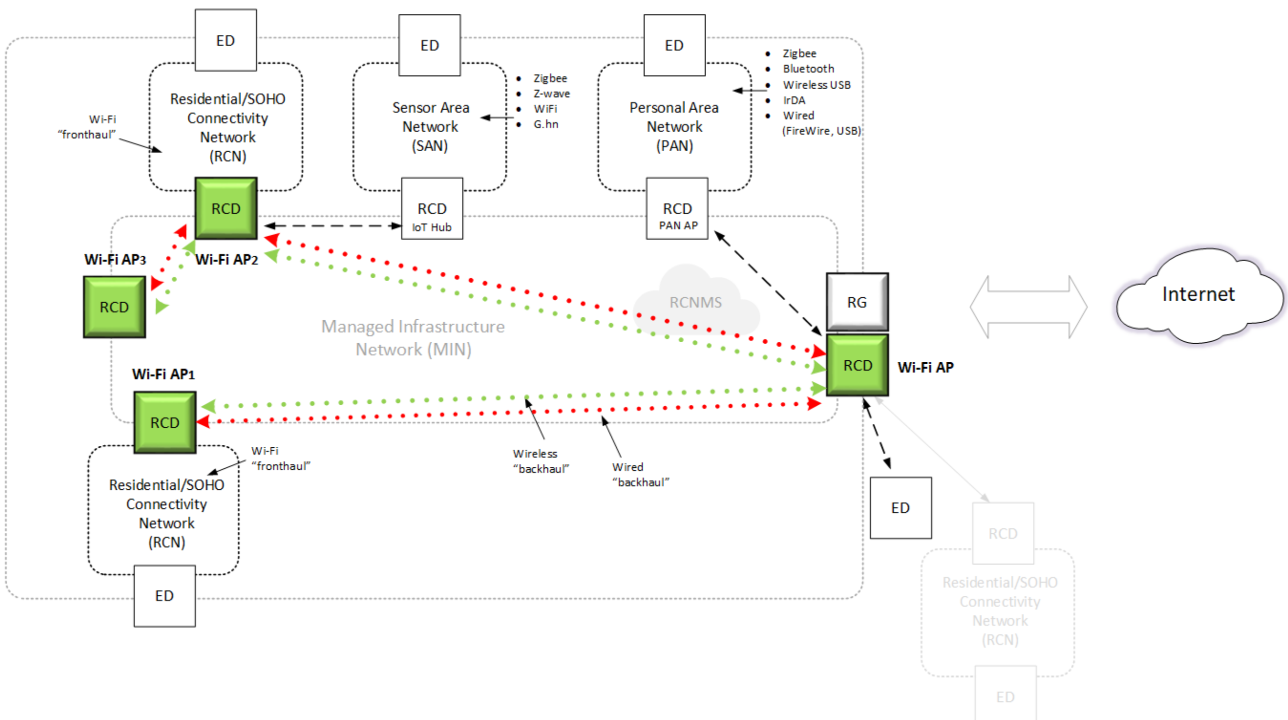

Figure 5 – Topology Use Case 4: *Multi-AP Network – MDU*

4.2.5 Topology Use Case 5: Multi-AP Network – Greenfield

More details about the device classes and other characteristic features of the Use Case "Multi-AP Network – Greenfield" are given in Table 6 and in Figure 6.

Table 6 –Topology Use Case 5 Features list

Device Classes		Characteristic features
End Devices (ED)	**Dclass.1 – Fixed stationary**	Mainly connected wirelessly to an AP in a multi-AP in-home network. Alternative connecting option to some wireless links through an Ethernet cable or powerline/MoCA may be used when better Wi-Fi performance is required.
	Dclass.1 – Fixed movable stationary	Mainly connected wirelessly to an AP in a multi-AP in-home network. Alternative connecting option to some wireless links through an Ethernet cable or

		powerline/MoCA may be used when better Wi-Fi performance is required.
	Dclass.2 – Nomadic	All mobile devices (e.g., smartphones, Google Nest smart home devices, Amazon Alexa-enabled devices, Apple HomeKit devices, Philips Hue smart lighting devices, and other smart home devices) in the home are connected wirelessly to an AP in the in-home MIN network (including the one integrated in the RGW) or retail IoT gateway wirelessly.
Residential/SOHO Connectivity Devices (RCD)	**Dclass.3 – Fixed**	Multiple access points (multi-AP) or IoT gateways for connecting sensors/devices in a SAN. In a multi-AP in-home network, a primary AP provides broadband access. The secondary APs are connected to the primary AP through backhaul links and in this way connected to the Internet. All APs, including the primary AP, provide Wi-Fi coverage to devices in the home. Backhaul links using Ethernet/Fiber-optic/next generation high speed wired technologies are building the in-home network (MIN).
	Dclass.4 – Nomadic	Multiple access points (multi-AP) or IoT gateways for connecting sensors/devices in a SAN connected to the in-home MIN network primarily through wireless backhaul links.
Residential/SOHO Connectivity Network		**Characteristic features**
Wi-Fi Roaming		Possible
Wi-Fi Performance Experience		Excellent to good
RCN Management System (RCNMS)		By the means of its management system, in-home MIN networks utilize multiple APs able to work together and adapt to changing network conditions, thus providing extended network coverage, increased performance, capacity and effective throughput, and high-quality user experience in all areas of home with no dead spots. Industry standards, like Wi-Fi EasyMesh from the WFA and prplMesh, an open-source software implementation of a carrier-grade mesh Wi-Fi solution from the prpl Foundation, facilitate management system implementations built on a reliable multi-vendor interoperability. Cloud-based and edge-based management systems are commonly used approach by service providers, although other options, like hybrid management systems or systems with multiple managing entities, are also possible.

Figure 6 illustrates a case when the existing Wi-Fi router (in the RG) is replaced with a network that consists of four Wi-Fi access point units, the primary one AP and three secondary ones AP1, AP2 and AP3. Data traffic is distributed among the access points over two backhaul options, Cat 6 Ethernet, and fiber-optic. Cat 6 Ethernet links are represented by the dotted green lines, while the fiber-optic links are represented by the dotted red lines. The most remote Access point AP3 is positioned out of range from the gateway and requires a double hop through one of the less remote access points, AP1 or AP2, over two different backhaul links. The dashed black lines in **Figure 6** represent the “fronthaul” links.

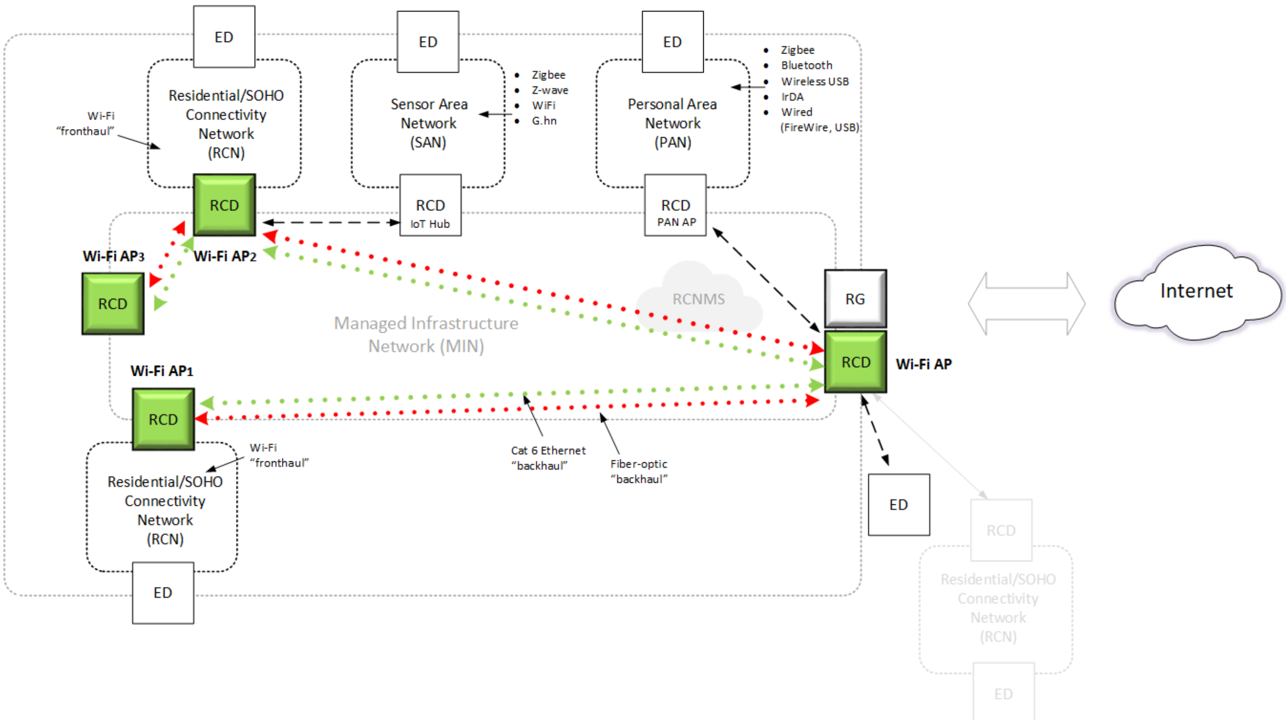

Figure 6 – Topology Use Case 5: *Multi-AP Network – Greenfield*

4.3 Services

Different types of services in the home, and more generally the operator managed residential/SOHO network (OMRN), along with their classification have been discussed in several technical papers (Architecture, functions and services of home network ITU - GSTP-HNAFS [8], Use cases and requirements of fiber-to-the-room (FTTR) – ITU GSTP-FTTR [9], Rise of the app-enabled services gateway [22], Overview of ITU-T G.hn technology – ITU GSTP-OVHN [10]), just to cite a few.

According to ITU – GSTP-HNAFS [8], the dominant services in the in-home network are background service, video service, voice service, and IoT service. Background traffic represents the bulk of data transfers and other actions related to the in-home network management system (RCNMS) that are permitted on the network but that should not impact the use of the network by other users and applications. Background services are responsible for the autonomous exchange of user plane data packets, generally in the absence of a specific user interaction with devices, which can be considered low priority in the in-home network. Video and voice services belong to the traditional services in the home, such as broadcast video over IP (IPTV) and Over-the-Top (OTT) video streaming, as well as voice service implemented using voice over Internet Protocol (VoIP). Recent trends show that cloud VR is becoming more popular within the in-home networks. Cloud VR is a new cloud computing technology for VR services. With fast and stable transport networks, VR content is stored and rendered in the cloud, and video and audio outputs are coded, compressed, and transmitted to end-user devices. Another service that is gaining in popularity is IoT, which can be provided by the operator through interconnecting and organizing sensor area networks (SAN) physical objects – "things" – that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet and operating new value-added services.

Technical Paper ITU - GSTP-FTTR [9] reveals a detailed look into use cases and requirements of fiber-to-the-room (FTTR) technology. However, many of the use cases collected in this report are notably important in general for innovation and technological development of the end-user networks: Wi-Fi backhauling, seamless roaming, smart office network services (voice, real-time camera capturing, simultaneous integration of hundreds of teleconference calls and background internet service), IoT and process automaton in smart homes, latency sensitive in-home broadband services, dynamically created network slicing services with different QoS requirements, East-West data transmission services and exchange of information between any node of the network, just to mention few of them.

Finally, just recently Broadband Forum published a white paper “The Rise of the App-Enabled Services Gateway” [22] about creating a services-based ecosystem for the residential/SOHO network. Service providers have an opportunity to grow the subscriber base to include a diverse array of differentiated residential/consumer, business, and other services such as gaming, work from home VPN, enhanced security and privacy, smart home e-Services, e-Public services, and more. See Figure 7 (A) below defining potential applications viable for such a platform.

For the last few years, the service providers have been undergoing the digital transformation of the subscriber network and shifting their focus from the gateway solution for providing Internet access to devices within the home or business, toward enabling the gateway platform by creating a services-based ecosystem. As we look at the echo system to support the App-Enabled Services Gateway (ASG), we come to understand the importance of defining the OMRN. In order to support the services-based platform, an ecosystem will need to be defined. The ecosystem may contain any, some or none of the following cloud connected function spaces as shown in Figure 7 (B). This document will not attempt to define any of the cloud connected spaces, however it will be noted that the ASG will need access from the OMRN to support this level of functionality.

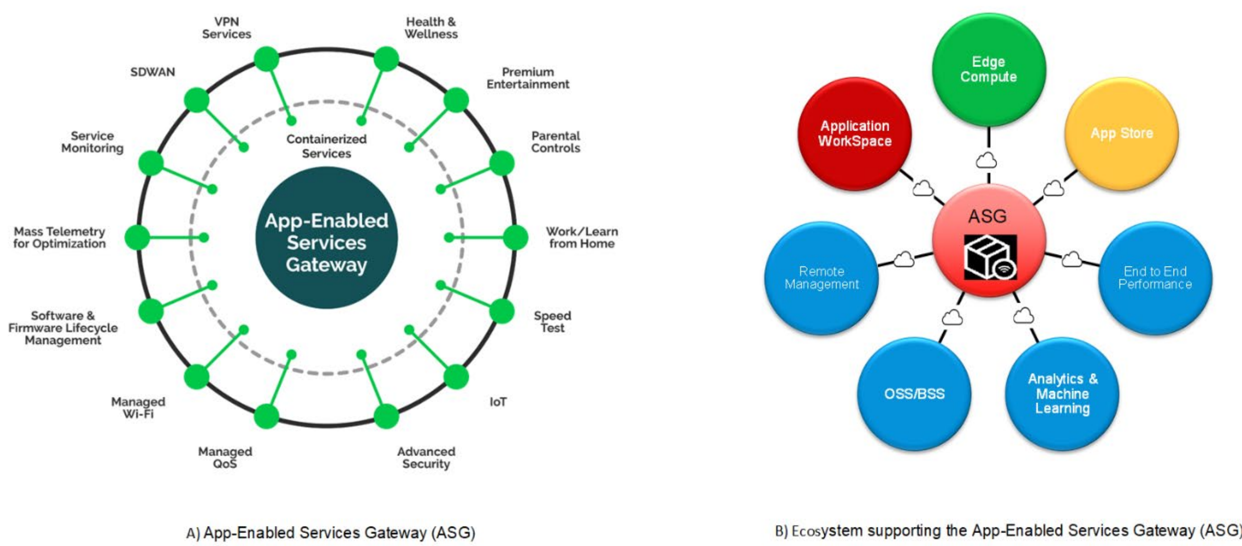

Figure 7 – App-Enabled Services Gateway (ASG) with supporting ecosystem

5 Operator-Managed Residential/SOHO Network Architecture

5.1 Reference Architecture

In this Technical Report, an overall network infrastructure for delivering Internet based services to end users is referred to as an End-to-End Service Network.

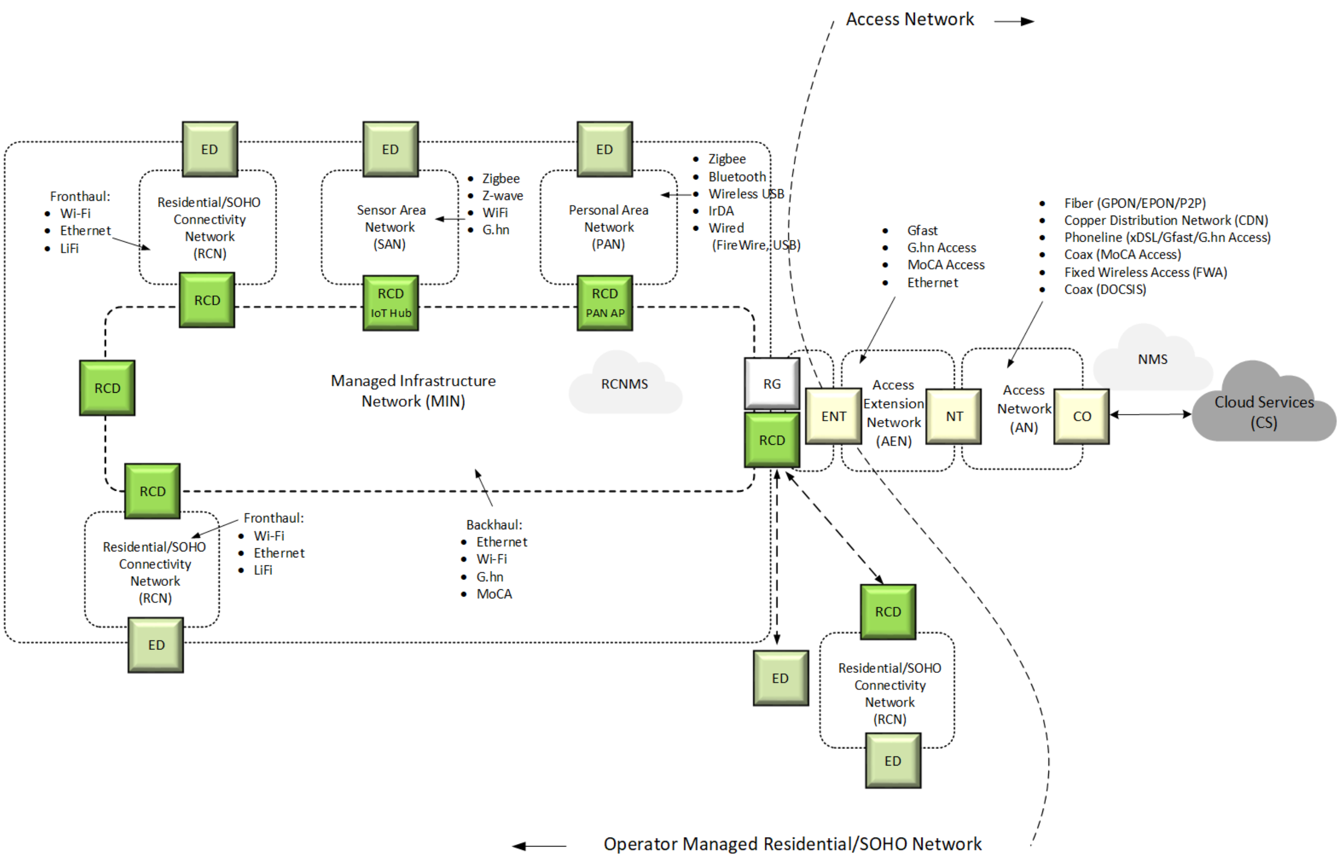

Figure 8 – End-to End Service Network

As shown in Figure 8, it encompasses the following building blocks:

1. A *Cloud Services (CS)*, which incorporates Software Defined Networking (SDN) and Network Function Virtualization (NFV), running on a cloud-like infrastructure deployed at Central Offices, providing additional computing resources and services, management functions (e.g., network management, optimization, and diagnostic functions), cloud applications and reliable and scalable computing service, etc. for the in-home networks.

2. An *Access Network (AN)*, also referred to as an outside plant, which enables physical connection from the Central Office (CO), e.g., DSLAM, OLT, DPU, GAM or fixed-wireless antenna, to the in-home network, by using various communication technologies over copper wires (xDSL, Gfast, G.hn Access), coax cables (MoCA Access, DOCSIS, G.hn Access), fiber optics (GPON, XG(S)-PON, EPON, point-to-point fiber), or over the air (4G LTE, 5G, FWA), to provide broadband access to the end user.

3. Network Terminal (NT) is the end network device of an access network, such as ONT in PON network or DSL Modem/end device in DSL network.
4. The Access Network is included in the diagram to articulate the larger view and may be optionally extended through use of an *Access Extension Network (AEN)* to reduce the cost of physical deployments by using a lower cost technology without reducing the performances. *Extended Network Terminal (ENT)*: In some cases, an additional link may be needed to build up connection between the network terminal of an access network and the in-home network entry point (by using an Extended Access Network (AEN) terminated by an Extended Network Terminal (ENT)). More detailed explanation about this architecture together with the list of use cases of the AEN is provided in BBF TR-419 [6].
5. An Internet Gateway provides a connection between the access network and residential/SOHO network. It can be implemented as a single-box solution *Residential Gateway (RG)* e.g., fixed network (FN-RG) or 5G residential gateway (5G-RG), cable modem or FTTx modem) or a multiple-box solution (residential gateway connected to a residential/SOHO cconnectivity network (RCN) e.g., Wi-Fi Extender or a primary Wi-Fi access point with an integrated Wi-Fi EasyMesh Controller functionality.
6. *Residential/SOHO Connectivity Devices (RCD)* provide connectivity to the network to End Devices (e.g., Wi-Fi AP, LiFi AP or smart home/IoT hub). In a generic sense, RG is a special case of an RCD.
7. *End Device (ED)* is an electronic device that enables dedicated service for end users and is capable of connecting to the in-home network through at least one connection interface. Some typical examples include computers, smartphones, tablets, personal digital assistants, smart TV systems, and other smart home devices.

In this document, we focus on the part of the End-to-End Service network from a demarcation line drawn through an ENT to the end devices. This is referred to as an *Operator Managed Residential/SOHO Network (OMRN)*, composed of the following types of sub-networks:

a. *Managed Infrastructure Network (MIN)*: Including Residential/SOHO Connectivity Devices (RCD) that are not directly providing a service to the user and that have as role to distribute the broadband signal through the home. For instance, the in-home infrastructure network may be a mesh network composed of an interconnection of Wi-Fi access points (AP). The interconnection can be wired or wireless. In general, an edge controller or cloud controller monitors, diagnose and manage the behavior of this in-home infrastructure network devices (owned by the service/cable provider or by the user) and the topology of the in-home infrastructure network. Typical communication technologies used in backhaul include Wi-Fi [32], G.hn ITU TP-UC-HN [12], MoCA [31] and Ethernet [30].

b. *Residential/SOHO Connectivity Network (RCN)*: Providing connectivity to the End Devices through different fronthaul technologies, typically Wi-Fi, but also light communication (LiFi), Ethernet.

c. *Personal Area Networks (PAN)* and *Sensor Area Networks (SAN)*: Providing connectivity to electronic devices within an individual person’s workspace and a connectivity for special purposes (e.g., low-cost, low-power wireless IoT networks or in-home automation).

d. *OMRN management systems* comprised of operator’s *Network Management System (NMS)* running in a network server deployed in the central office (CO) and the *RCN Management System (RCNMS)* for managing end devices, quality of service, diagnostic and maintenance functions.

5.2 Mapping Topology Use Cases to the reference architecture

5.2.1 Example 1: Use Case "Direct connectivity to RG"

Figure 9 illustrates a typical home ecosystem with a residential gateway (RG) in a living room (LR) or an office as a central point for device connectivity. Its top-level architecture is shown in Figure 10.

Figure 9 – Example 1 "Direct connectivity to RG"

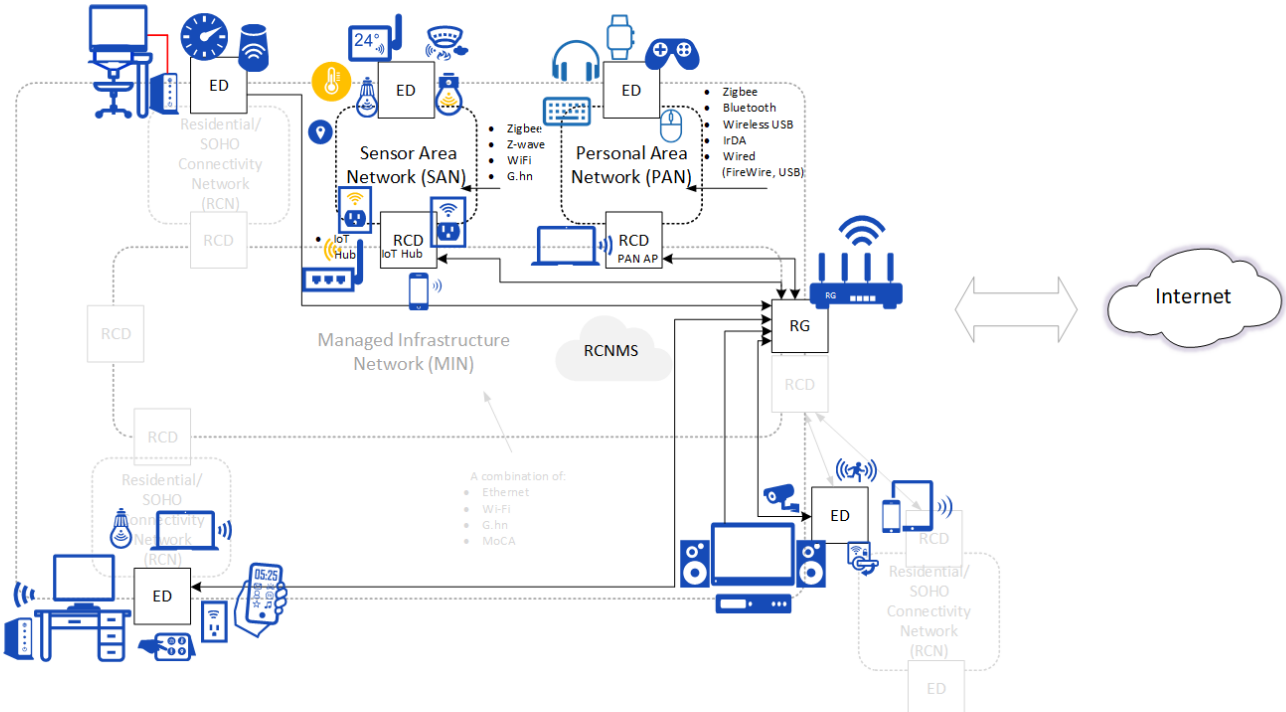

Figure 10 – Use Case "Direct connectivity to RG": Top-Level Architecture

5.2.2 Example 2: Use Case "Improved connectivity to RG

Figure 11 illustrates a typical home ecosystem with a residential gateway (RG) in a living room (LR) or an office as a central point for device connectivity and the improved Wi-Fi network performance realized through the use of a powerline Wi-Fi Repeater/Extender pair of devices. This is a common approach to broadening the coverage area of a network using electrical wiring that consists of these two components: powerline adapter (PLA) plugged into a residential gateway (RG) and the companion powerline repeater/extender (PRE) plugged to an electrical outlet. Its top-level architecture is shown in Figure 12.

Figure 11 – Example 2 "Improved connectivity to RG" utilizing Powerline Repeater/Extender

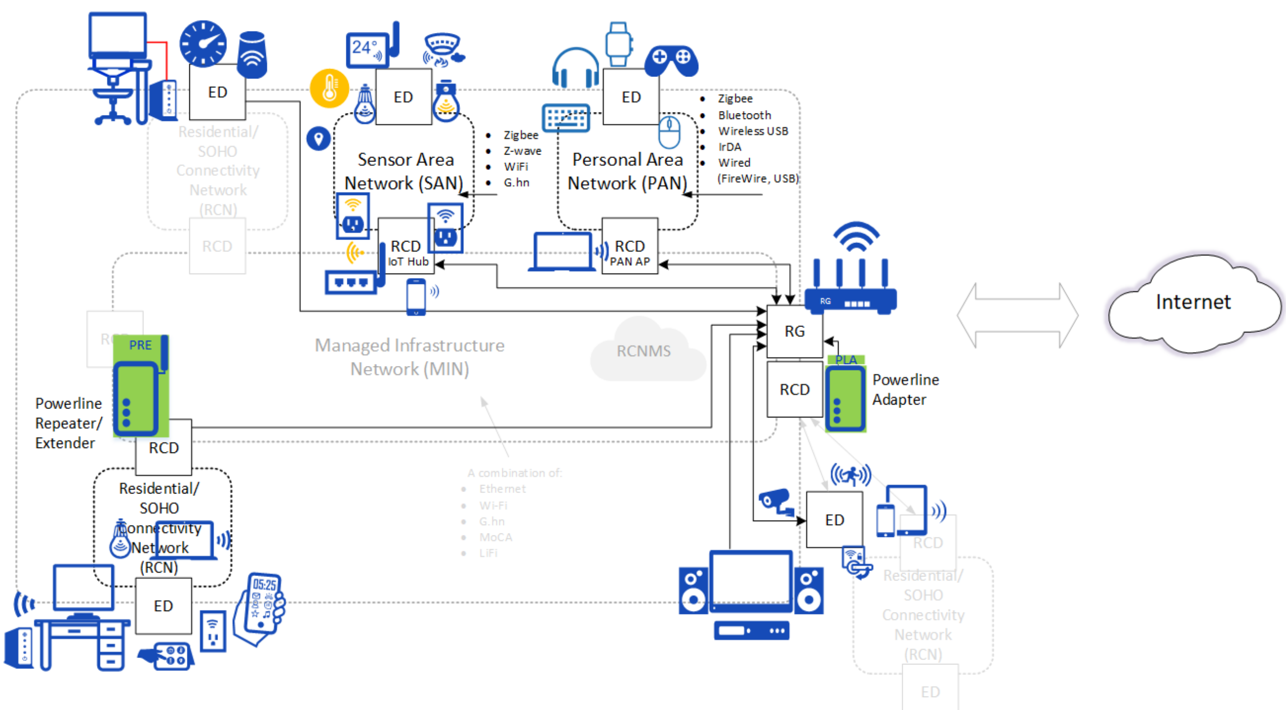

Figure 12 – Use Case "Improved connectivity to RG" utilizing Powerline Repeater/Extender: Top-Level Architecture

Another common approach for extending network coverage is shown in Figure 13. It utilizes a Wi-Fi Repeater/Extender device (WRE) that takes an existing signal from a wireless router (RG), or wireless access point, and rebroadcasts improved signal range and strength to create an extension of the network accessible to end user devices in far corners of the home, different floors, or even outside of home. Its top-level architecture is shown in Figure 14.

Figure 13 – Example 2 "Improved connectivity to RG" utilizing Wi-Fi Repeater/Extender

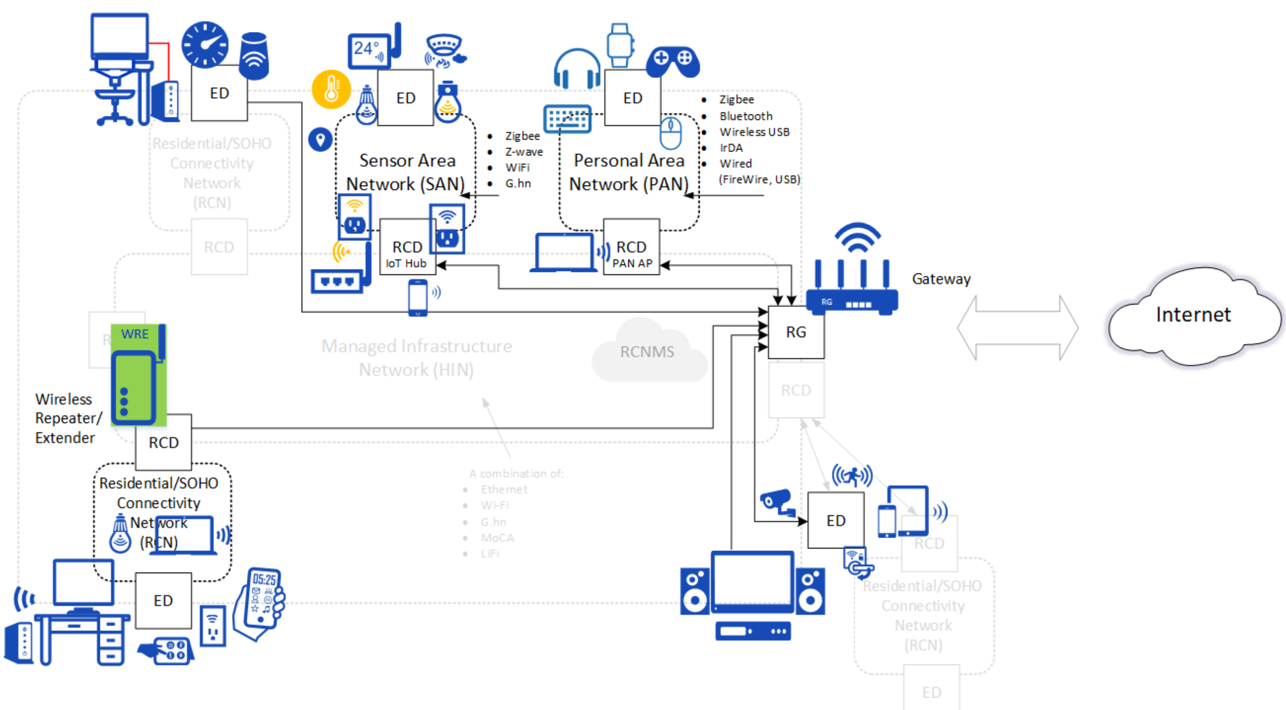

Figure 14 – Use Case "Direct connectivity to RGW" utilizing Wi-Fi Repeater/Extender: Top-Level Architecture

5.2.3 Example 3: Use Case “Multi-AP Network – Retail”

Figure 15 illustrates a typical home ecosystem with a residential gateway (RG) in a living room (LR) or an office as a central point for device connectivity and the improved Wi-Fi coverage and throughput performance through use of a network comprised of multiple Wi-Fi access points. Its top-level architecture is shown in Figure 16.

In this example the router function of RG is switched off and moved to the primary access point Wi-Fi AP, which is a common approach to enable seamless connectivity of Eds to the strongest access point without changing connection data. Nomadic Eds can then roam with a user walking from one location in the home to another having their Wi-Fi connection literally following the user from one AP to another.

As shown in Figure 15, a multi-AP network consists of four Wi-Fi access point units, the primary one AP and three secondary ones AP1, AP2 and AP3. The most remote Access point AP3 is positioned out of range from the gateway and requires a double hop through the less remote access points AP2, over two different backhaul links (AP-AP2, AP2-AP3). Data traffic is distributed among the access points over “backhaul” wireless links represented by the dashed green lines.

The dashed black lines in Figure 16 represent the “fronthaul” links. Fronthaul links are almost always Wi-Fi connections because Wi-Fi is the universal wireless interface standard for all consumer devices in a home.

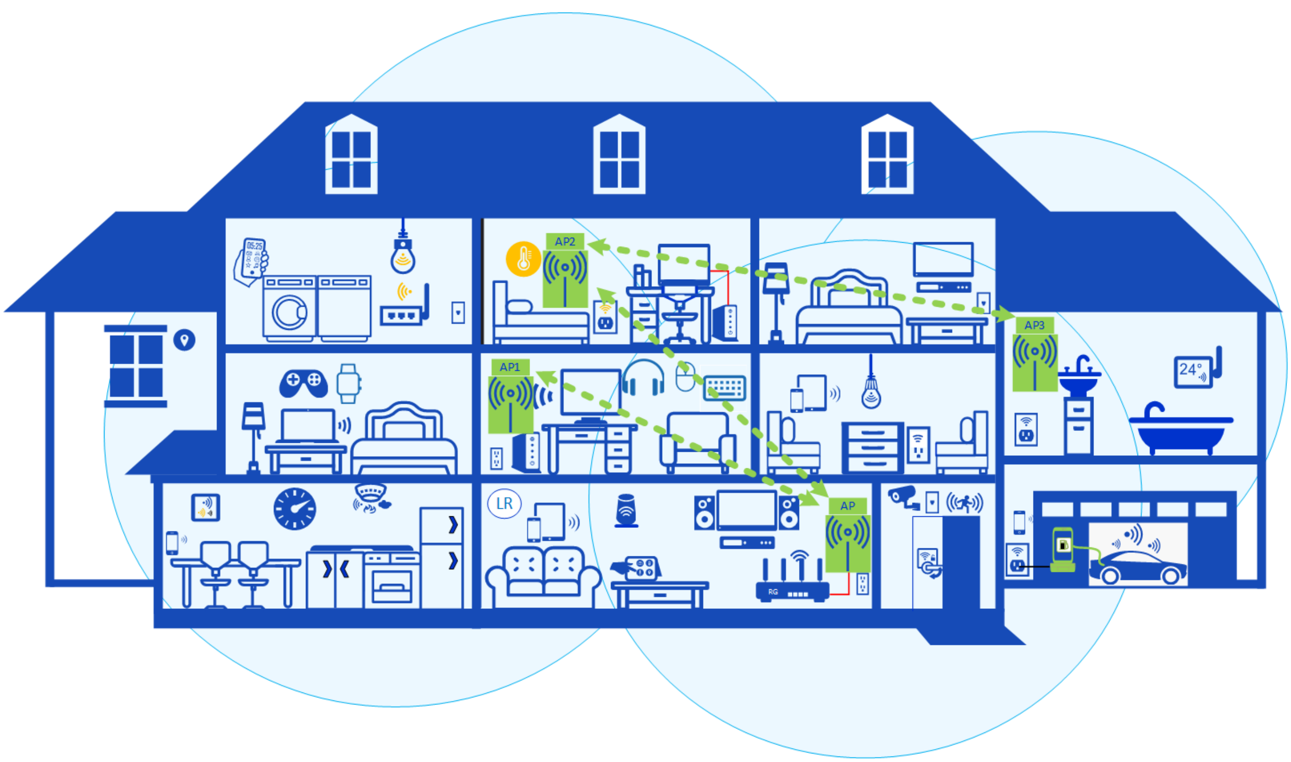

Figure 15 – Example 3 “Multi-AP Network – Retail”

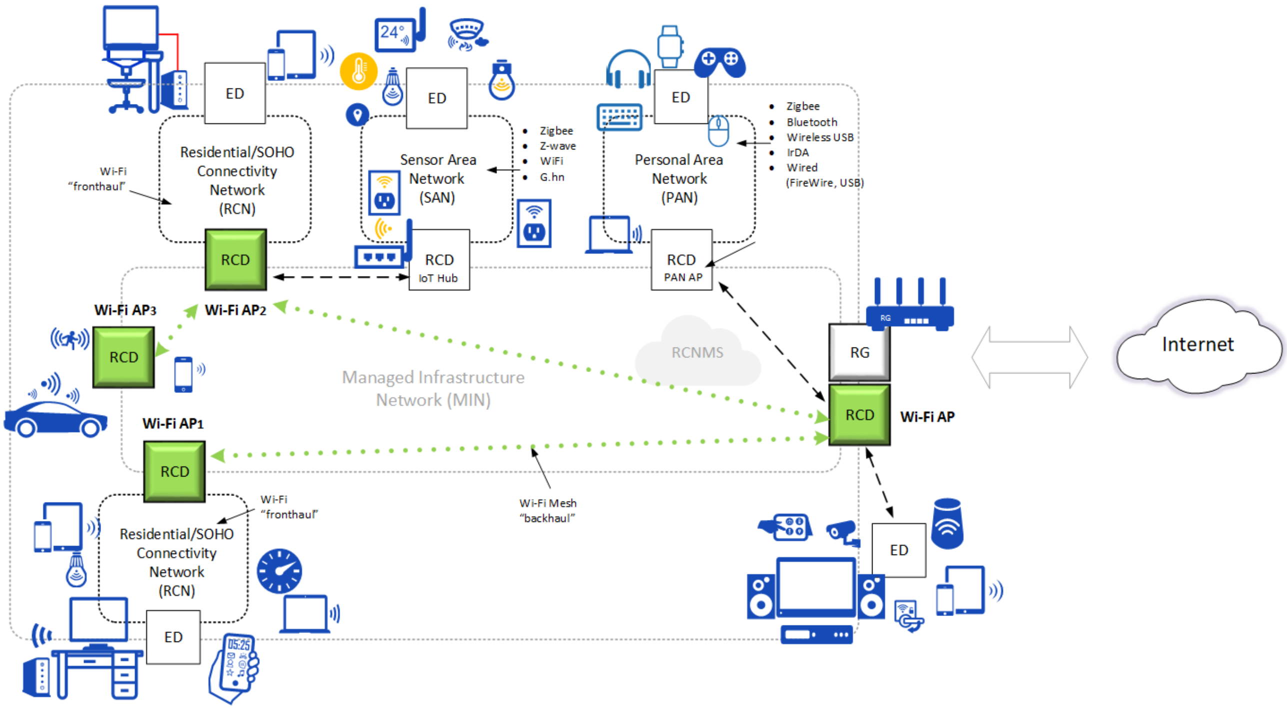

Figure 16 – Use Case "Multi-AP Network – Retail": Top-Level Architecture

5.2.4 Example 4: Use Case "Multi-AP Network – MDU"

Figure 17 illustrates a typical home ecosystem with a residential gateway (RG) in a living room (LR) or an office as a central point for device connectivity and the improved Wi-Fi coverage and throughput performance through use of a network comprised of multiple Wi-Fi access points. Its top-level architecture is shown in **Figure 18**.

The main difference between this use case and the use case "Multi-AP Network – Retail" is a variety of backhaul technology options used to link between the Wi-Fi access points. Depending on locations and density of deployments (single family units (SFU), single-dwelling units (SDU) or multi-dwelling units (MDU)), expectations for good Wi-Fi coverage (rate-at-range) everywhere in homes and a quality of experience (QoE) perception, service providers need to be able to choose which technology, wireless (Wi-Fi) or wired over the existing infrastructure (Ethernet, G.hn or MoCA) best serves end user's needs. Data traffic is distributed among the access points over wireless "backhaul" links represented by the dashed green lines and wired "backhaul" links are shown as the dashed red lines.

The dashed black lines in **Figure 18** represent the "fronthaul" links. Fronthaul links are almost always Wi-Fi connections because Wi-Fi is the universal wireless interface standard for all consumer devices in a home.

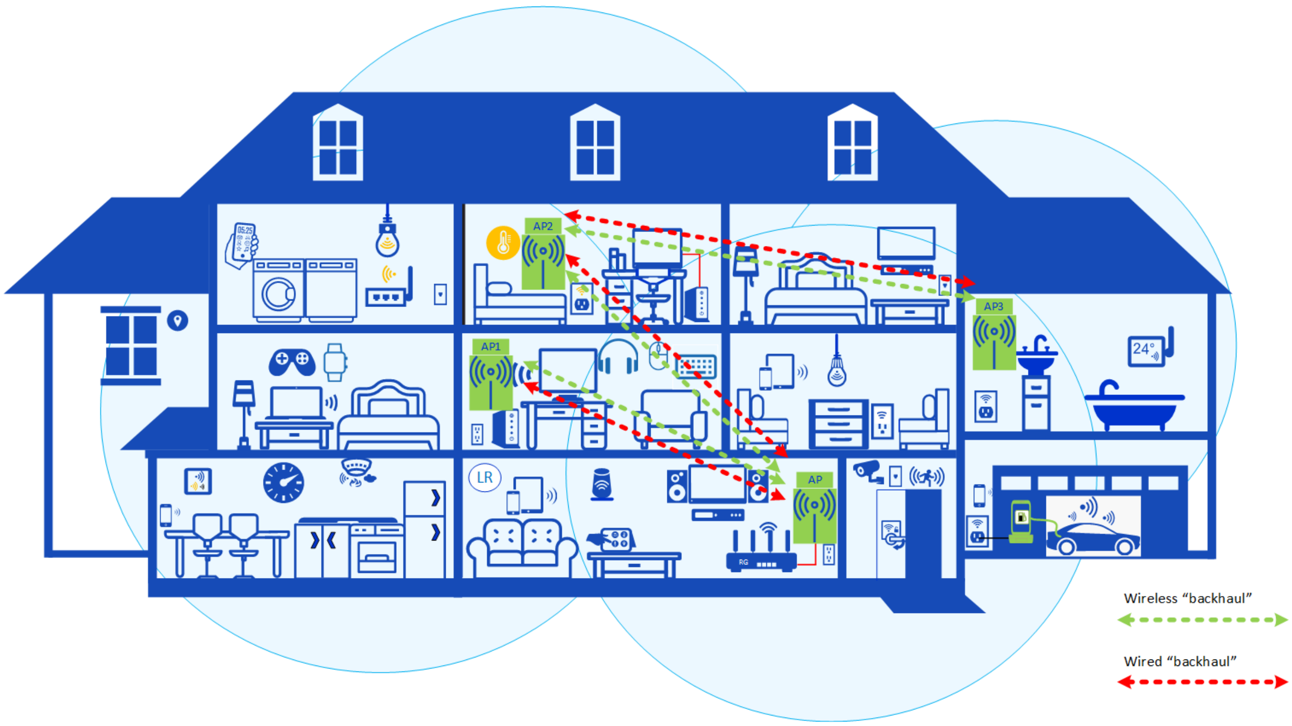

Figure 17 – Example 4 "Mesh Network – MDU"

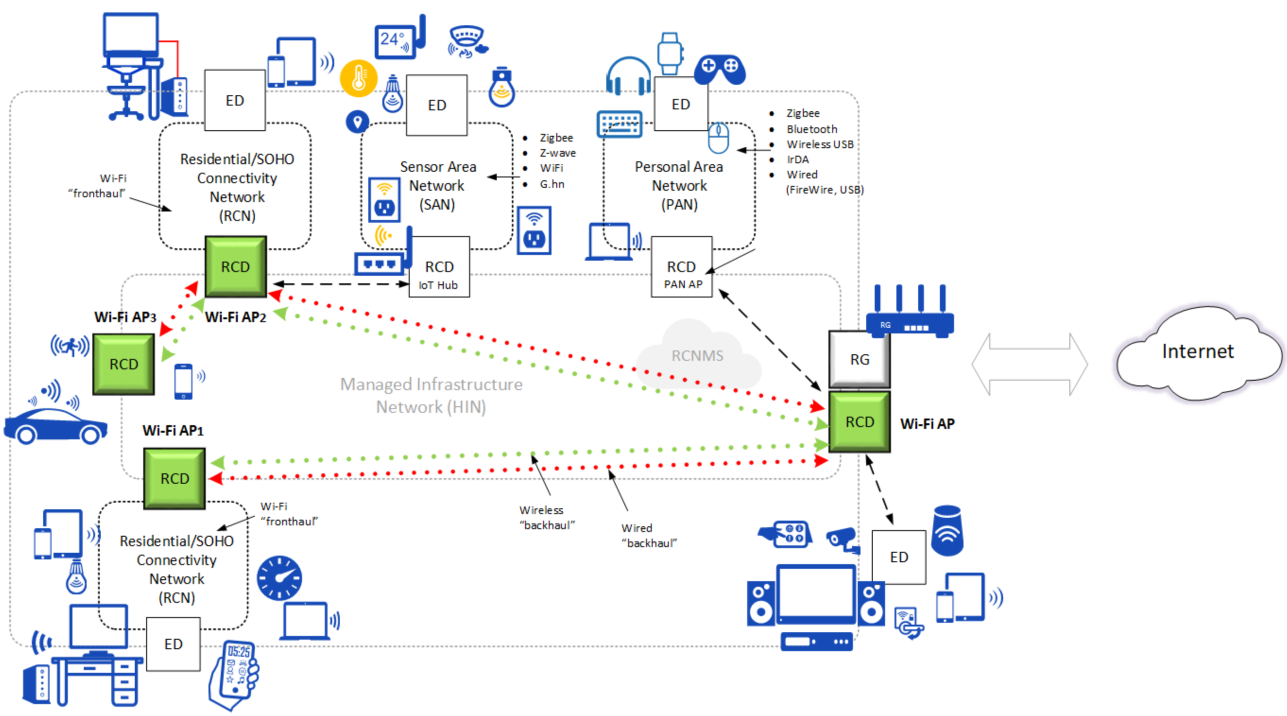

Figure 18 – Use Case "Multi-AP Network – MDU": Top-Level Architecture

5.2.5 Example 5: Use Case "Multi-AP Network – Greenfield"

Figure 19 illustrates a typical home ecosystem with a residential gateway (RG) in a living room (LR) or an office as a central point for device connectivity and the improved Wi-Fi coverage and throughput performance through use of a network comprised of multiple Wi-Fi access points. Its top-level architecture is shown in **Figure 20**.

The main difference between this use case and the use case "Multi-AP Network – MDU" is in the backhaul technology options used to link between the Wi-Fi access points. Depending on locations and density of deployments (single family units (SFU), single-dwelling units (SDU) or multi-dwelling units (MDU)), expectations for good Wi-Fi coverage (rate-at-range) everywhere in homes and a quality of experience (QoE) perception, service providers need to be able to choose which technology, Cat 6 Ethernet or fiber-optic best serves end user's needs. Data traffic is distributed among the access points over Cat 6 Ethernet backhaul links represented by the dashed green lines and fiber-optic backhaul links are shown as the dashed red lines.

The dashed black lines in **Figure 20** represent the "fronthaul" links. Fronthaul links are almost always Wi-Fi connections because Wi-Fi is the universal wireless interface standard for all consumer devices in a home.

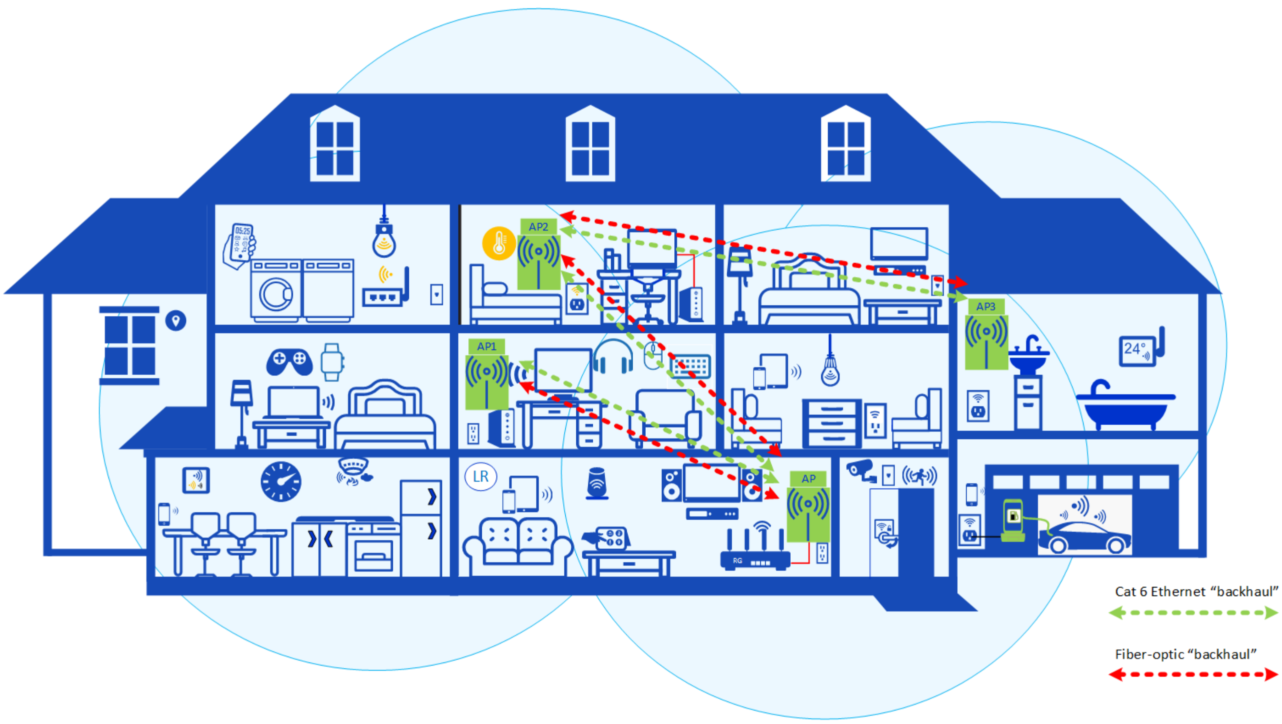

Figure 19 – Example 5 "Multi-AP Network – Greenfield"

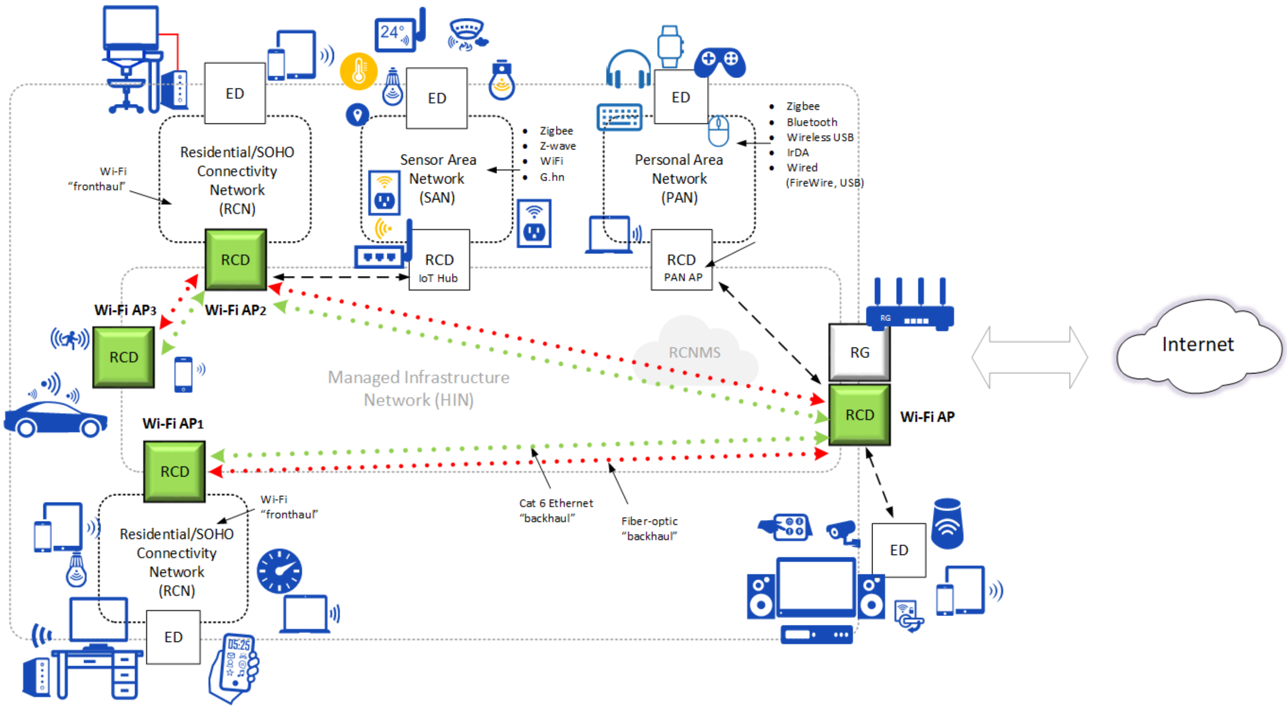

Figure 20 – Use Case "Multi-AP Network – Greenfield": Top-Level Architecture

6 Operation and Management of an Operator Managed Residential/SOHO Network

An operator-managed end-user network (OMN) solution requires the following capabilities enabled for deployment, operations, and management of the network.

6.1 Operation of the OMRN

Deployment capabilities cover the initial setup of the end-user network with a single Residential Gateway (RG). The basic deployment is where end-user devices (Eds) are directly connected to the RG as described in the Topology Use Case 1. This is the typical basic wireless best-effort approach to connecting nomadic devices to the RG or a retail IoT gateway. Fixed Eds may be connected to the RG through an Ethernet cable or powerline/MoCA adapters. Deployment of Topology Use Case 2 is similar to Use Case 1 but has a goal to improve Wi-Fi network coverage and performance by adding one or more Repeater/Extender devices (Aps), usually Wi-Fi but often powerline. In both use cases, the RG and one or more Aps for the initial setup of the network may be provided by the service provider or obtained via a retail channel.

Mesh networks typically have a local controller that controls configuration among multiple extender RCDs. Typically, this local controller is physically located in the RG. If not, then an RCD that houses the local controller can be connected over Ethernet or other connection to the RG. This connection can use signaling at layer 2 or at layer 3. Examples of layer 2 signaling are EasyMesh and IEEE 1905. Examples of layer 3 signaling are TR-69 and TR-369.

Common to all three mesh use cases is that the Wi-Fi or wired (G.hn powerline, MoCA, Ethernet or fiber optics) links between a primary access point and one or more multi-band extender access points should create a seamless and reliable Wi-Fi connection throughout the entire home. In general, installation of the network, together with onboarding end-user devices and integration of an additional extender to the existing network, delivered by the operator, should run automatically allowing deployment of network services, with a minimized effort for the user.

6.2 Management of an OMRN

An Operator Managed Residential/SOHO Network is considered managed because the operator has the ability to monitor and control aspects of RCD and certain ED (such as set-top boxes) that are part of the operator's service offering in the subscriber's network. The goal of this ability is to allow the operator to:

- Onboard new subscribers and new RCD (i.e., Customer Premises Equipment).
- Manage the life cycle of firmware and software on these managed devices to reduce mean time to deployment and resolve security issues.
- Deploy and configure value-added services using the available equipment.
- Provide near real-time network monitoring, mapping, device fingerprinting, and adjustments to ensure quality of experience.
- Provide mechanisms for customer self-care to reduce support load.
- Configure devices and services, sometimes including configuration for performance optimization.

Management in the context of the architectures defined in OMRN Use Cases is one of the most valuable opportunities for operators that can be accomplished using several architectural concepts as described in the next section.

The following specifications are among those used for the purpose of managing an OMRN:

- BBF TR-069 (CWMP) [1] has provided the protocol for subscriber network management for many years. BBF TR-369 (USP) [2], aka the User Services Platform , has improved on this using modern protocol practices and expansions in the number and kinds of RCD and ED that can be managed and controlled.
- BBF TR-181 Data Model [3] provides the data model for describing RCD and ED devices, and the proxy management of non-USP devices for comprehensive subscriber management. TR-181 includes management of Device info, User interface, Ethernet, USB, HPNA, MoCA, G.hn, UPA, Wi-Fi, ZigBee, Bridging, IP, Routing, DHCP, IEEE 802.1x, UpnP, Firewall, Femtocell, IEEE 1905, WWC, IoT, and other objects.
- BBF TR-124 [4] provides requirements for RGs.
- ITU-T G.9962 [15] defines the management specification for G.hn.
- IEEE 802.11 [16] defines a great many management parameters and capabilities, however many devices only implement a subset of these defined management parameters and capabilities.
- Wi-Fi CERTIFIED Data Elements™ [17] defines many read-only parameters for diagnostics, remote configuration, and performance management for Wi-Fi. Wi-Fi Data Elements is particularly applicable for managing Wi-Fi CERTIFIED EasyMesh™ [18] mesh networks. Wi-Fi Data Elements is part of the TR-181 data model in Device.WiFi.DataElements.
- Wi-Fi CERTIFIED QoS Management [19] provides mechanisms for assigning Wireless Multimedia (WMM) priorities across Wi-Fi networks.
- The Wireless Broadband Alliance (WBA) [21] has shown multi-AP architectures with both local hierarchical control through a gateway, and direct to cloud, as well as many other guidelines for operator management of Wi-Fi.

6.2.1 OMRN Management Architecture

The architectural concept for managing an OMRN shown in Figure 21 is built around BBF TR-369 (USP) [2], and its standardized protocol to manage, monitor, update, and control devices and user services in a residential/SOHO network. The User Services Platform is a system of Controllers and Agents that enables remote monitoring and manipulation of software and hardware capabilities of the connected RCD and ED devices.

The main Functional blocks within the OMRN management architecture are highlighted in the following sections.

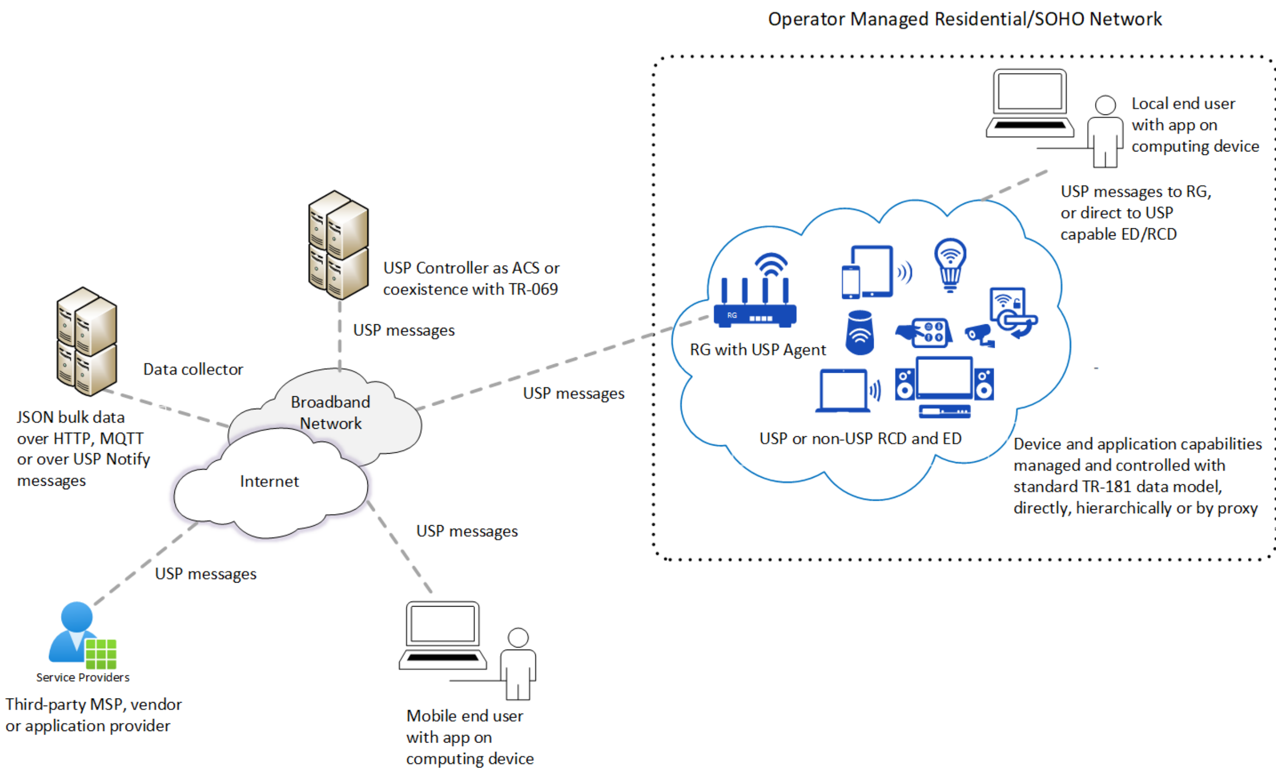

Figure 21 – Architectural Concept for Managing an OMRN

6.2.1.1 Use of Autoconfiguration Server (ACS)

BBF TR-069 (CWMP) [1] defined the concept of an Autoconfiguration Server to manage operator CPE. This became a general function on its own that is carried on in the use of a BBF TR-396 (USP) [2] Controller.

The ACS function of a USP Controller utilizes the Create, Read, Update, Delete, Operate, and Notify functions of USP to monitor and control RG, RCD, and ED via a USP Agent and an API defined in the Device:2 BBF TR-181 Data Model [3]. Devices that support these components are then able to be monitored and controlled via the ACS function.

The data model defined in TR-181 Device:2 provides an expansive list of hardware and software capabilities that can be managed and monitored by a USP Controller serving the ACS function. In the context of the OMRN architectures, this includes:

- Onboarding new RCD and ED in the OMRN,
- Deploying firmware updates and patches to RCD and ED,
- Providing the control functions to optimize quality of experience in the different OMRN architectures.

Specific to Wi-Fi in the OMRN is the use of the Wi-Fi Alliance's Data Elements (DE) set of parameters to allow for the management and optimization of the end-user 802.11 network. The Theory of Operations for the use of Data Elements as defined in TR-181 can be found in Appendix III: Wi-Fi Theory of Operation.

6.2.1.2 Bulk Data Collection

BBF TR-369 (USP) [2] Annex A defines a bulk data collection mechanism for gathering mass telemetry from one or more RCDs and Eds. This consists of a USP Agent capable of transmitting data via this mechanism and one or more data collectors. The data collector provides the resulting data to applications used to monitor and optimize the OMRN.

6.2.1.3 Hierarchical vs. Direct Access to RCD and ED

In most residential/SOHO networks, management access to non-RG RCDs, and the Eds themselves, requires communication that must cross the network boundary provided by the RG. This communication can be accomplished via either hierarchical access to these devices (i.e., communications managed or proxied by the RG that has a USP Agent) or via direct communication to these devices via their own USP Agents, as shown in Figure 22. The dashed lines in Figure 22 indicate optional interfaces to manage some ED.

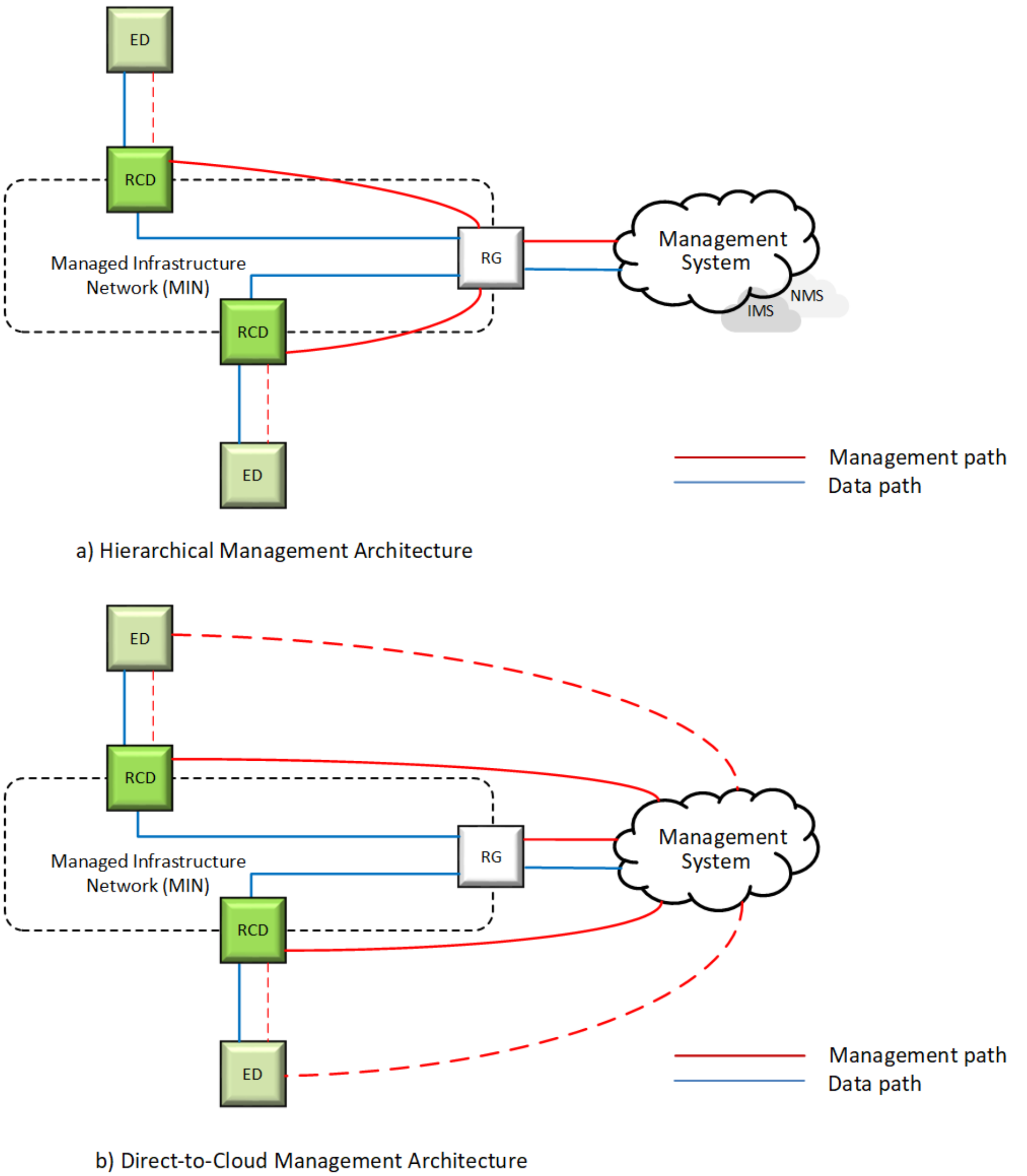

Figure 22 – Residential/SOHO Network Management Architecture

A hierarchical management architecture involves management messages going between the management system and the RG, then being translated, or otherwise sent between RG and RCD, and then possibly also sent between RCD and ED. Wi-Fi EasyMesh [18] is a good example of such a hierarchical management architecture, typically an Easy Mesh controller is contained within the RG. The EasyMesh controller on the RG translates Wi-Fi Data Elements messages from the management system and uses its own control logic to then issue layer 2 messages that traverse the LAN to RCDs. The only USP agent needed in this hierarchical architecture is at the RG.

A Direct-to-Cloud residential/SOHO network management architecture involves the RCDs being directly managed by the management system. For example, each RCD has a USP agent and communicates directly with the management system.

6.2.1.4 Distributed Management Architecture

USP supports a distributed management architecture for the OMRN. A distributed architecture means that different management functions can be controlled by different systems, even with different responsible parties. The ACS function may be broken down into several different Controllers, or different bulk data collectors may exist for specific use cases.

For example, an operator may want to employ a third-party entity to provide Wi-Fi optimization, security services, etc. This model is also conducive to app-enabled services gateways that can install third-party applications that expose components that can be managed by the application provider.

6.2.1.5 Customer Self-Care

A key use case for operators is giving end users the ability to resolve network issues on their own without the need for support intervention. In this case, providing a USP Controller on a customer's ED (such as a smartphone) that allows a self-care application to talk to the RG or another RCD or ED lets this happen while also not relying on a working WAN connection. Moreover, it can be used as a hybrid with other management architectures above to be used as failover or to provide information that could not otherwise be obtained by the ACS function directly (see TR-356 [20]).

6.2.2 Operator management functions for the OMRN

- Providing and ensuring connectivity
    - Assist with or perform client onboarding, configuring user login and security settings, setting SSIDs for private/public networks, check device and network status.
    - Assist with or perform network infrastructure onboarding and configuration including both wired and wireless connected infrastructure.
- Monitoring for performance and faults
    - Operators want visibility into the OMRN, at the service level for monitoring services and at the individual user level for monitoring broadband.
    - Passive data is gathered by the equipment and includes data rates, signal strength, interference, congestion, utilization, packet and / or bit error rates, physical layer connectivity, availability events, traffic counters and performance counters.
    - Quality of Experience Delivered (QED) as defined in TR-452.1 [26] is an increasingly important measure of latency, which is crucial for monitoring many services. The distribution of latency is an important component impacting QED, it should be considered as many endpoint devices may be sensitive to variability as well as mean latency. Jitter is also an important parameter. It may impact many endpoint devices which could be sensitive to jitter as well as latency.
    - Operators should be informed of problems when they happen by subscribing to notifications and alarms. This should allow for proactive notification of problems to the subscriber.

- Diagnostics for initial analyses by a call screener or by an automated system such as described by TR-436 [25].
    - Simple status and performance data, inventory and configuration information can be collected passively for the initial diagnostics.
- Troubleshooting to identify root causes, by a technician or automated system [25].
    - Can use highly granular data for high-tier analyses.
    - Active tests can be triggered and require sending and analyzing test signals, including throughput and latency tests. UDP speed tests, as defined in TR-471 [27] and implemented in OB-UDPST software, are most effective.
- Configuration or reconfiguration
    - Configuration of devices, networking, and services,
    - Wi-Fi configuration: channel, band and client steering, Wi-Fi 6 spatial reuse, mesh configuration.
    - Set priorities, configure scheduling, or queue management for services; perform Wi-Fi QoS Management [19].
- Virtualized management
    - Cloud management, local management (RG software), both cloud and local, edge/fog, etc.
    - Support for on-device internal services such as Wi-Fi intelligence or IoT services
- Security
- Software or firmware updates, e.g., Software Module Management in BBF TR-369 (USP) [2].
- Resource Management and Optimization
    - The subscriber's OMRN may consist of different types of physical layer components. An extender (such as different Wi-Fi or IoT radios) may offer wireless services that may not be present in the RG. The OMRN should provide for resource management and optimization of Wi-Fi, IoT radios, wired and wireless interfaces with their prospective statistics.

6.2.2.1 OMRN Performance Management and Diagnostics

This section focuses on fault and performance management. Fault and performance management are key operations for the operators and service providers. Wi-Fi residential/SOHO networks have always been the source of many faults, and operators are now expected to provide and uphold the performance of the OMRN. Fault management is the component of network management concerned with detecting, isolating, and resolving problems or malfunctioning in network operations. Properly implemented, network fault management can keep connectivity, applications and services running at an optimum level, provide fault tolerance and minimize downtime. Performance management encompasses methods that manage, enable, and ensure a network's optimal performance levels. Typically, network performance management demands the routine monitoring of quality and performance service levels for each network component and device.

The ability to manage, monitor, troubleshoot and control various connected RCD and ED devices (residential gateways, smart Wi-Fi systems, consumer electronics, IoT etc.), network resources (latency, bandwidth, throughput) and services (cloud based or running on the end devices) in an unified framework defined on standard based architecture, protocol and data model is essential for an operator to manage a residential/SOHO network for end users effectively and efficiently. BBF TR-369 (USP) [2], and its predecessor management protocol BBF TR-069 (CWMP) [1], makes use of and expands the Device:2 BBF TR-181 Data Model [3] to provide this framework and enable deployment of secure and trustworthy applications [21].

BBF TR-069 (CWMP) [1] or BBF TR-369 (USP) [2], provide the protocol for managing the OMRN. Management is typically provided through an operator-provided WAN connection to an RG. However, a second WAN connection, such as a cellular network, can serve as either an alternate management path as described in TR-356 [20] or a backup WAN connection. The second WAN connection is particularly useful when the primary WAN connection is impaired.

In recent years many reports have appeared on characterizing and improving reliability of broadband Internet access and Wi-Fi experience for residential users. Maintenance of good QoE is becoming an increasingly challenging process, as this requires that operators diligently collect and aggregate diagnostics data across very many subscriber lines. Another observable trend is that due to the growth in Wi-Fi devices, connection speeds and traffic volumes, Wi-Fi has increasing capacity demands. Deploying new Wi-Fi generations, such as Wi-Fi 6 and Wi-Fi 7, can increase Wi-Fi capacity. Also, using the new spectrum available at 6 GHz allows wider channel bandwidths with higher capacity, less congestion, and less interference. According to [33], doing so will have an immediate impact on congested networks and will lay the foundation for supporting new use cases, such as meeting ever-increasing demand for faster multi-user data rates and IoT deployments. Wi-Fi coverage (rate-at-range) is another issue that is typically addressed by deploying mesh networks such as Wi-Fi EasyMesh [18]. Optimizing the use of Wi-Fi spectrum can become a critical management task especially in dense MDU environments. One method of preserving Wi-Fi capacity is to use Wi-Fi only for fronthaul links and deploying wired backhaul technologies (e.g., G.hn or MoCA) for Wi-Fi backhaul by utilizing existing wiring wherever possible.

For OMRN, it is important to apply considerations of end-to-end QoS performing consistent QoS treatment across multiple segments of the overall network. WMM compliant Wi-Fi QoS treatments should be mapped to QoS attributes such as DSCP or PCP to offer low latency and high priority handling of Voice and Video traffic. Similarly other physical media offered QoS capabilities need to be mapped such that the differential prioritization is applied in a consistent way across multiple hops. One way of doing so is Wi-Fi QoS Management [19].

6.2.2.2 Performance Management Examples

Some basic diagnostics data with common types of faults and impairments reported in [34] are listed in Table 7. This table shows that not only are there different types of impairments, but each can be categorized into different levels as perceived from different perspectives:

- Impact on QoE as perceived by the user.
- Impact on QoS, typically a first cut categorization of service impact as perceived by a call center agent.
- The actual root cause(s), such as perceived by a technician after analyses.

Table 7 – User perception -> QoS -> Diagnostic

QoE Artifact	QoS Impact	Diagnostic root cause						
		Connectivity/ Wrong credentials	Interference	Congestion	Coverage	Legacy clients/ Poor efficiency	Misconfiguration (Channel, WMM)	High traffic/ User density
No connection	Availability	X			X		X	X
Slow speed Poor video quality	Throughput /Speed		X	X		X	X	X
Poor gaming Slow control	Latency		X	X			X	X

In Table 7, congestion is caused by shared communication with this same RCD or radio, while interference comes from communications with other RCD and external noise. Coverage issues are caused by insufficient signal power in some locations and can be identified by very low connection speeds. Legacy clients using old standard generations can use a lot of the airtime to transmit a given amount of data. High traffic or high user density can result in high congestion and interference. These issues, and others such as wrong credentials, may impact connectivity.

Typical management actions that can be performed to alleviate the impairments in Table 7 are shown below:

- Restart driver or device.
- Reset network credentials, and security protocol, also make sure the end devices are upgraded to the latest software version
- Apply adaptive radio channel allocation and selection
- Utilizing deployment of the radio resource management (RRM) solutions to increase visibility into the wireless network to mitigate issues related to interference and congestion, and to proactively manage wireless resources, e.g., dynamic frequency selection (DFS) and transmit power control (TPC) for 5GHz operation, automated frequency coordination (AFC) for 6GHz operation, or airtime fairness management (ATF)
- Avoiding interference from residential networks in close proximity using client band steering and AP steering to associate clients with different connectivity devices (RCD)
- Network loop prevention in a mesh Wi-Fi network when there are redundant connections (e.g., G.hn or Ethernet) between some APs (repeaters/extenders)
- Building the network infrastructure using standards-based state-of-the art interoperable equipment
- Network traffic prioritization using Wi-Fi QoS Management [19].
- Reallocation of the operational channels and rearrangement of the backhaul and fronthaul channels.
- Deploying new (the latest) Wi-Fi standards and certified equipment, and advanced multi-AP solutions for residential/SOHO network (e.g., Wi-Fi EasyMesh)
- Network topology control and optimization
- Preventive network diagnostics for resolving potential faults before the end users notice them.
- Utilization of wired backhaul technologies (G.hn, MoCA, Ethernet) in the managed infrastructure network (MIN) and reallocation of radio channels to fronthaul links.
- Utilization of alternate fronthaul technologies (G.hn Li-Fi, Ethernet)

End of Broadband Forum Technical Report TR-488

