Smart Home & IoT

Operator-Managed Industry Framework

Source: Wireless Broadband Alliance

Authors: WBA IoT and Smart Home Project team

Issue Date: February 2025
Version: 1.0.0
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.

For the complete list of current WBA members, click here.

Follow Wireless Broadband Alliance:

www.twitter.com/wballiance

www.facebook.com/WirelessBroadbandAlliance

www.linkedin.com/company/2919934/

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.

The images generated by DALL.E and included in this Document have been transferred to WBA by the original creator, and WBA now holds full ownership of these images. WBA reserves all rights to these images, and no further reproduction, distribution, or use of the images is permitted without WBA's explicit permission. WBA disclaims any liability for unauthorized use of the images by third parties.

Table of Contents

Figures

1. Executive Summary

The "Smart Home & IoT - Operator-Managed " Industry Framework provides a comprehensive overview of the current state and future trajectory of smart home technologies. It details the evolution of the WBA Operator Managed Wi-Fi Reference Architecture into a Smart Home implementation , highlighting the shift from basic connected homes to sophisticated NextGen Smart Homes, emphasizing the need for robust communication protocols, device interoperability, and stringent data privacy measures.

One of the primary areas of focus is the evolution of smart homes. The document traces the progression from isolated automated devices to interconnected systems that enhance user experience. It discusses the transition from Smart Home 1.0, characterized by individual device control, to Smart Home 2.0, which integrates platforms for seamless operation. The advent of NextGen Smart Homes, with advanced AI, edge computing, and sustainable energy solutions, marks a significant leap forward in the smart home landscape.

Connectivity solutions are another critical component addressed in the document. It provides a detailed exploration of Wi-Fi, Wi-Fi HaLow, IEEE 1905, BLE, and Thread as foundational technologies for smart home connectivity. Each connectivity solution is discussed in terms of its benefits and applications, highlighting their roles in creating a robust and efficient smart home network. The importance of these technologies in ensuring seamless communication between devices is emphasized.

The document also delves into device management and data models, introducing Matter, an open-source standard for device interoperability, and TR-181, a standardized data model for remote management. Other models like TR-369/USP and OCF are examined for their roles in ensuring secure and efficient device communication and management. These models are pivotal in maintaining a cohesive and functional smart home ecosystem.

In terms of practical applications, the document explores various NextGen Smart Home use-cases. Home automation is highlighted for its potential to enhance convenience and efficiency through interconnected devices. Edge computing is discussed for its ability to leverage local data processing, ensuring privacy, reduced latency, and resilience. The integration of AI in smart homes is seen as a significant advancement, enabling intelligent decision-making, predictive analytics, and enhanced security. Additionally, the document covers innovations in connected health, home security, energy monitoring, and media distribution, illustrating the broad impact of smart home technologies.

Finally, the document emphasizes the importance of deploying and managing smart home services through a standardized framework. Building on WBA's Operator Managed Wi-Fi Technical Specifications and Architecture, the group has developed a Smart home modulation that incorporates IoT components and ensure interoperability, scalability, security, and cost efficiency. The challenges posed by proprietary solutions are acknowledged, with a strong advocacy for open standards like Matter and USP/TR-181 to foster a versatile and consumer-friendly smart home ecosystem. The role of service orchestration tools, device management platforms, and developer support in implementing this standardized framework is highlighted, showcasing the collaborative effort required to achieve a unified, secure, and efficient smart home environment.

In conclusion, the "Smart Home & IoT - Operator-Managed " Industry Framework calls for collaboration among manufacturers, service providers, and regulatory bodies to adopt standardized solutions. This collective effort is deemed essential for achieving a unified, secure, and efficient smart home environment that enhances user experience and drives innovation in the industry.

2. Smart Home Evolution

The evolution of home technology has been a captivating journey, moving from simple stand-alone automation and internet-connected devices to highly integrated and intelligent systems. The progression from a "connected home" to the sophisticated "NextGen Smart Home" has fundamentally transformed our living spaces, offering unprecedented convenience and efficiency. Initially, homes were equipped with individual devices that operated largely in isolation. As technology matured, these devices began to communicate, leading to seamless interoperability and more intuitive user experiences. This overview will delve into the key stages of this evolution, shedding light on the transformative milestones of smart home technology.

2.1 Smart Home Vs. Connected Home

The terms "smart home" and "connected home" are often used interchangeably, but there are distinct differences between the two. A connected home refers to a living space where various devices, such as thermostats, lights, and security cameras, are connected to the internet and can be remotely controlled. It's a foundational step in making homes more technologically advanced. However, a smart home takes this concept a step further. In a smart home, these devices don't just connect and operate independently; they communicate with one another, share data, and can even make decisions based on that data. For example, a smart thermostat can adjust the heating based on data from a weather app and occupancy sensors. The primary distinction lies in the integration and intelligence of the system. While a connected home offers remote access and control, a smart home provides a holistic, responsive, and often automated living experience. As the technology evolves, it's crucial for consumers to understand these nuances to make informed decisions about home automation.

Figure 1 Connectivity Solutions Vs. Integrated Smart Home Experience

2.2 Smart Home 1.0

The first iteration of the smart home, often referred to as Smart Home 1.0, was a significant leap from traditional homes. This era marked the initial introduction of devices that could be controlled remotely, usually via smartphones or computers. Homeowners began integrating smart light bulbs, thermostats, and basic security systems. These devices typically operated on their own respective platforms, requiring separate apps or interfaces for control. The focus was primarily on individual device functionality rather than system-wide integration. While this phase was revolutionary in many ways, it also had its challenges. Fragmentation was a significant issue, with a myriad of devices often not communicating or working seamlessly together. However, Smart Home 1.0 laid the foundational groundwork, showcasing the potential of tech-integrated living spaces and setting the stage for the subsequent evolution of smarter, more connected homes.

2.3 Smart Home 2.0

Building on the foundation of Smart Home 1.0, the second iteration, Smart Home 2.0, aimed to address the challenges of device fragmentation and lack of interconnectivity. In this phase, there was a noticeable shift towards developing platforms and ecosystems where devices could communicate with one another. Industry giants like Apple, Google, and Amazon introduced home automation platforms, promoting interoperability between devices. Voice assistants, such as Alexa, Siri, and Google Assistant, became central hubs for controlling various smart home devices. Integration with third-party services added another layer of functionality, allowing, for example, music to play or lights to change based on user location or scheduled routines. The overall user experience improved significantly, with greater ease of use, better integration, and the beginning of true home automation. However, even with these advancements, there was still room for growth, innovation, and a move towards an even more unified home ecosystem.

2.4 Next-Generation Smart Home

The NextGen smart home represents the future of home automation, characterized by advanced AI, deeper integration, and proactive automation. In this emerging paradigm, homes will not just react to user commands but anticipate needs based on patterns, behaviors, and external data sources. Imagine a home that adjusts its temperature, lighting, and music based on the mood detected from the occupants' biometrics. Inter-device communication will be so seamless that the home will function as one cohesive unit rather than a collection of individual devices. Advanced sensors will monitor health and well-being, with potential applications in telehealth and elderly care. Furthermore, edge computing capabilities will enable quicker, more localized data processing, reducing reliance on cloud servers. The NextGen smart home will prioritize sustainability, with systems designed to optimize energy use, reduce waste, and integrate with renewable energy sources. The NextGen ecosystem will use standards to enable plug-n-play across a myriad of devices from multiple vendors, allowing innovation to flourish. As technology and innovation continue to evolve, the home of the future promises to be a space that's not just smart but truly intuitive and adaptive to its occupants' needs.

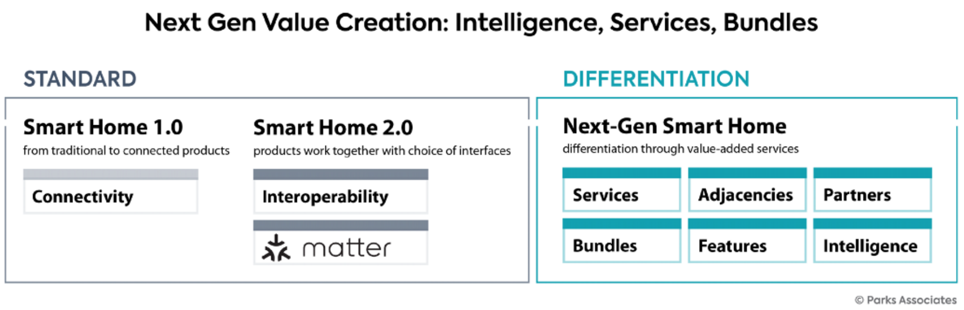

Figure 2 Next-Generation Smart Home: Parks Associates & CSA

3. Connectivity Solutions for Home Networking

In the rapidly evolving realm of smart homes, two pillars stand out: connectivity and the management and data model. Connectivity encompasses the technologies and protocols that facilitate communication between devices, ensuring smooth, instantaneous, and often autonomous operations. It's the underlying infrastructure that powers the smart ecosystem, giving life to our everyday devices, making them "smart". On the other hand, management and data models serve as the architectural blueprints. They define device behaviors, their interactions, and the frameworks for remote operations. Together, these two dimensions shape the intelligence, interoperability, and user experience of the modern smart home.

3.1 Smart Home Connectivity Solutions

The technical foundation of the smart home is rooted deeply in its connectivity infrastructure. It's through this networked layer that devices and systems communicate, collaborate, and offer users the cohesive experience of automation. From bandwidth and range to power consumption and topology, the type of connectivity chosen can greatly influence the performance, scalability, and security of the entire ecosystem. Moreover, the integration of different protocols can either simplify or complicate the deployment and maintenance of smart home systems. Each technology has its intricacies and nuances, catering to various applications, ensuring optimal performance for specific tasks.

3.2 Wi-Fi

Wi-Fi, operating in the 2.4 GHz and 5 GHz bands (and more recently in the 6 GHz with Wi-Fi 6E and Wi-Fi 7), provides broadband speeds suitable for data-intensive tasks. It's based on the IEEE 802.11 family of standards, which has seen various iterations from 802.11a to 802.11ax (Wi-Fi 6) and now 802.11be (Wi-Fi 7), each improving on speed, reliability, or efficiency. Wi-Fi's infrastructure typically consists of routers and access points, which can dynamically manage device connections based on traffic and priority. Its extensive range, often up to 100 meters in open areas, can be extended further using mesh networking solutions. The bandwidth can vary, with Wi-Fi 5 (802.11ac) supporting speeds up to 3.5 Gbps and Wi-Fi 6 (802.11ax) reaching up to 9.6 Gbps under optimal conditions. However, Wi-Fi's larger bandwidth and range sometimes come at the cost of higher power consumption. For security, Wi-Fi networks should utilize WPA3 encryption, and it's essential to keep firmware updated to prevent potential vulnerabilities. Considering the sheer volume of devices connected in a modern household, from smartphones to smart fridges, Wi-Fi's adaptability and speed remain paramount.

Wi-Fi 6 and 7 contain power-saving features such as target wake time (TWT) that are useful for IoT devices. To support time-sensitive networking, Wi-Fi scheduling can be enabled with restricted TWT (rTWT) and Orthogonal Frequency Division Multiple Access (OFDMA). Also, Wi-Fi QoS Management can provide effective prioritization over Wi-Fi.

Wi-Fi HaLow, standardized in IEEE 802.11ah, uses license-exempt 900 MHz spectra for long-range, medium speed and relatively low-power transmission. Wi-Fi HaLow is suitable for many IoT applications. Wi-Fi Direct provides peer-to-peer wireless connections between two devices to establish a direct Wi-Fi connection without needing an infrastructure network, and Wi-Fi Direct can be useful for applications such as directly connecting a VR headset to a rendering PC.

3.3 Wi-Fi HaLow

Wi-Fi HaLow, based on the IEEE 802.11ah standard, is a technology designed specifically for the Internet of Things (IoT) devices. It operates in the sub-1 GHz spectrum, offering longer range and lower power consumption compared to traditional Wi-Fi standards. With its ability to penetrate walls and other obstacles more effectively, Wi-Fi HaLow enables IoT devices to communicate over greater distances through basements, attics, and yards, making it suitable for smart home applications.

One of the key benefits of Wi-Fi HaLow is its ability to connect a wide range of IoT devices within the smart home ecosystem, including sensors, thermostats, appliances, lighting, and security cameras. Its low-power consumption allows devices to operate on battery power for extended periods, reducing the need for frequent battery replacements. In addition, Wi-Fi HaLow's longer range enables seamless connectivity throughout the home, ensuring reliable communication between devices even in remote/outdoor areas.

Use cases for Wi-Fi HaLow in the smart home include security cameras and sensors, HVAC and air quality monitors, appliances, energy management, solar power systems and EV chargers.

3.4 IEEE 1905

Per section 4.2 of IEEE 1905.1a-2014, the standard defines an abstraction layer that provides a common interface to several home network technologies: IEEE 1901 over power lines, Wi-Fi/IEEE 802.11 for wireless, Ethernet over twisted pair cable, and MoCA 1.1 over coax, and other protocols through the instantiation of Generic PHY.

The 1905.1 abstraction layer is an intermediate layer between the LLC L2 layer and underlying MAC layer(s) as illustrated in Figure 4-2 (below). The 1905.1 abstraction layer abstracts the heterogeneous MAC and PHY technologies of the converged home network by creating a single virtual MAC on top of the underlying MAC/PHY of the respective network technologies. Key features of the convergence layer include:

- Topology Discovery and change monitoring
    - 1905 Topology discovery protocol defines the current LAN topology.
    - LLDP discovery of IEEE 802.1 compatible bridges on or between 1905 devices, such as IoT gateways and hubs that may also be running Zigbee, Thread, and Bluetooth protocols.
- Diagnostics and reporting
    - Topology change notifications, device stats, and link metric reporting are used by local LAN protocol controllers to optimize network configuration and performance.
    - WAN accessible TR069/TR369 data models enable higher layer reporting of IEEE1905 and derivative data model over longer periods to enhance controller trend analysis and centralize problem remediation.
- Extensibility:
    - Other Network Technologies, including ITU-T-REC-G.9979, are supported by an extensible mechanism using an IEEE OUI and an XML-formatted documents.
    - Overlay protocols such as Wi-Fi EasyMesh are built using WFA specific extensions to IEEE 1905 and provide insight into the IEEE 802.11 operations hidden behind the 802.11 portal.
    - The Wi-Fi Data Elements data model serves as a diagnostic and remote configuration front end to the EasyMesh controller.
- Power management of interfaces
    - Enable enhanced power management (i.e. ACPI) by optimizing power usage across disparate dynamic technologies.

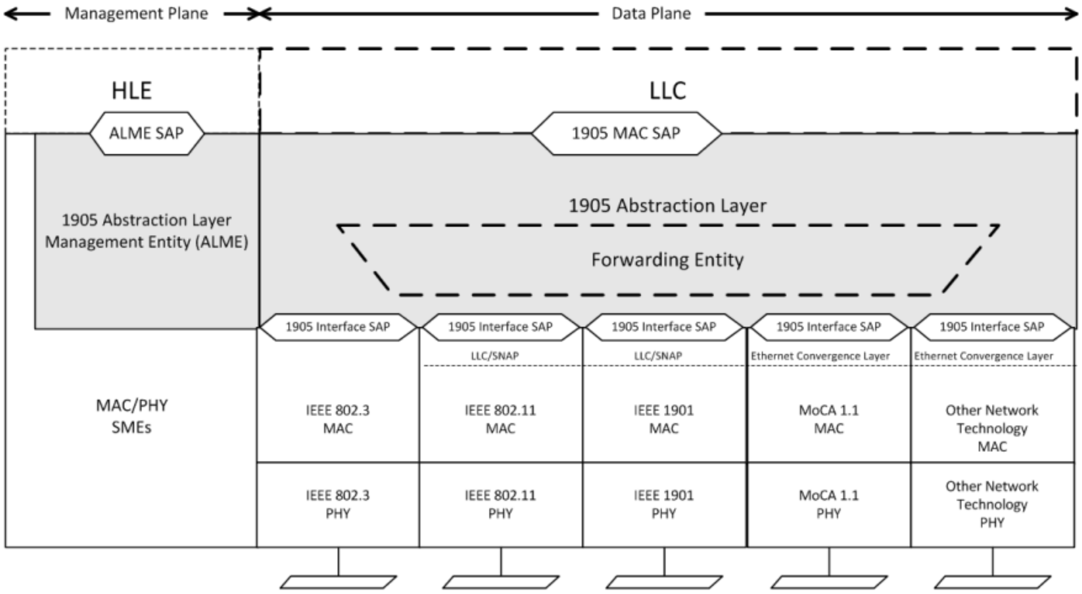

Figure 3 Abstraction Layer Model

(Source [IEEE Standard 1905.1a (2014)], *IEEE Standard for a Convergent Digital Home Network for Heterogeneous Technologies, Amendment 1: Support of new MAC/PHYs and enhancements*.)

3.5 Bluetooth Low Energy (BLE)

BLE (Bluetooth Low Energy) represents a power-conscious iteration of the standard Bluetooth protocol. Operating in the 2.4 GHz ISM band, it was introduced with Bluetooth 4.0 and was designed for short bursts of long-range communication, minimizing power usage. Technically, BLE achieves its efficiency by reducing connection times drastically — often to just a few milliseconds. The modulation rate for BLE is about 1 Mbps, which, while slower than standard Bluetooth, is optimal for its intended use-cases. Its typical range can extend up to 100 meters, but this is highly dependent on the environment and potential interference. A significant advantage of BLE is its ability to function in a "sleep mode," conserving power when not transmitting data. On the security front, BLE employs a host of features, including the Secure Simple Pairing, LE Secure Connections, and protection against passive eavesdropping. For smart homes, BLE's prominence is often seen in wearables, health monitors, and proximity sensors, where data needs are minimal, and battery conservation is critical.

3.6 Thread

Thread is an IPv6-based, low-power, wireless mesh networking protocol that's becoming increasingly popular in the smart home landscape. Operating in the 2.4 GHz frequency band, it uses 6LoWPAN, which effectively allows it to transmit IPv6 packets over IEEE 802.15.4-based networks. Data rate is typically 250 kbps. The standout feature of Thread is its mesh topology; devices, or "nodes," in a Thread network collaboratively relay data, ensuring resilience and reliability. If one node fails, the data can take an alternate path. This self-healing capability of the network enhances its robustness. Thread networks can support up to 250 devices, making them scalable for most smart home applications. Unlike hub-and-spoke models, where the central hub becomes a single point of failure, Thread's decentralized approach ensures continuous operation. For security, Thread uses AES encryption, ensuring data integrity and protection against eavesdropping. It seamlessly integrates with standard IP networks, making it compatible with existing infrastructures and cloud-based services, presenting a future-forward approach to smart home connectivity.

3.7 Device Management and Data Models

Management and data models play a pivotal role in the smart home ecosystem, ensuring consistent operation, configuration, and inter-device communication. These models serve as frameworks that define how devices behave, how they're managed remotely, and how they interact with other devices or platforms. From the protocols that dictate data transmission to standardized models ensuring device interoperability, a cohesive management strategy is essential. Each standard or protocol caters to a specific need within the smart home domain, addressing needs including remote management, inter-device communication, device classification, or communication patterns.

3.8 Matter

Previously known as "Project Connected Home over IP" (Project CHIP), Matter, by the Connectivity Standards Alliance (CSA), is an open-source, royalty-free messaging standard. Matter aims to increase compatibility among smart home products and augment the adoption of IoT devices. Built on proven technologies like Ethernet, Wi-Fi, and Thread, Matter provides a unified and consistent application programming interface (API) for building, accessing, and controlling IoT devices. Its architecture is based on an end-to-end model, emphasizing security from the device level to the cloud. By promoting interoperability among manufacturers, Matter aspires to simplify development for device makers and enhance the user experience by ensuring diverse devices can work seamlessly together.

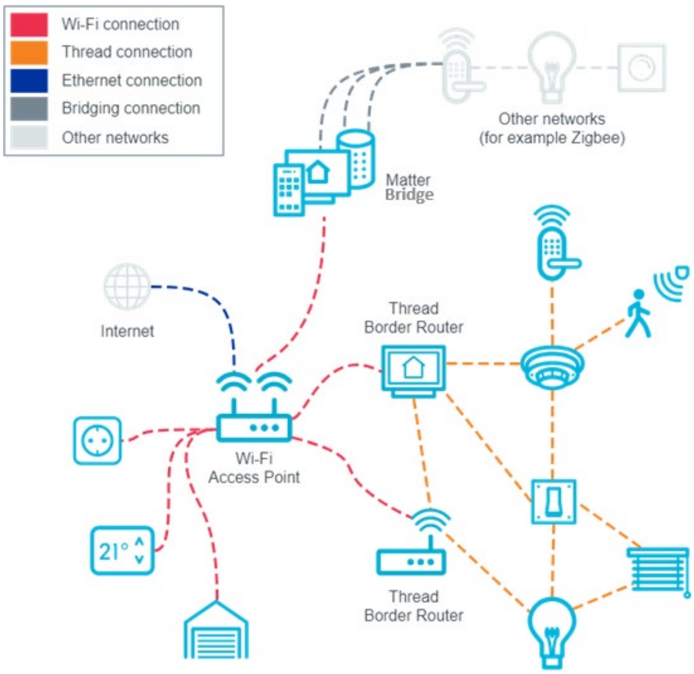

Figure 4 Matter Network

The Matter Data Model delineates a hierarchical structure where nodes, endpoints, clusters, and device types are systematically encapsulated, with nodes being the pinnacle data elements. A single Matter-enabled device, such as a lighting fixture or a smart lock, is represented by one or several nodes. These nodes coexist within a Matter fabric, a network ecosystem facilitating interoperability under a shared security framework. Within any given fabric, a device is assigned a distinct node with a unique Operational Node ID, securing its exclusive identification in that network.

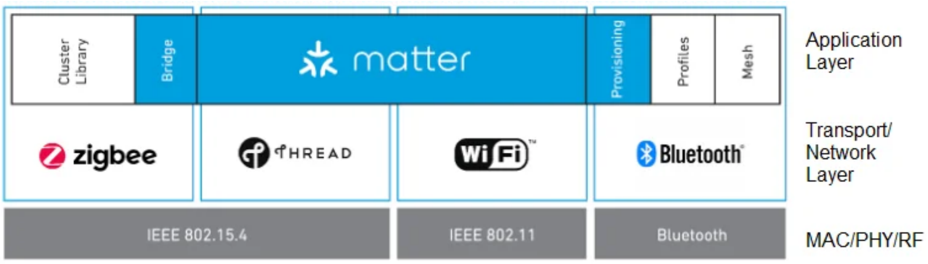

Figure 5 Matter Stack Representation

For example, a lighting device connected to an Apple HomePod fabric holds a unique node ID for that system, just as a switch within a Samsung SmartThings fabric bears an individual ID for its respective network. The same device may span multiple fabrics, as in a door lock that's part of both HomePod and SmartThings fabrics; it's depicted as two nodes with potentially unique or identical Operational Node IDs in each fabric, underscoring their operational independence. The following sections describes the Matter data model, including Nodes and Device Types:

Nodes

Nodes within the Matter ecosystem act as individual entities, each uniquely identifiable by an Operational Node ID, allowing them to be distinguished within a Matter fabric. This system facilitates the representation of one or multiple physical devices—be it sensors, lights, or other smart devices—within a singular node, granting them the ability to interact within the vast Matter network. Nodes are designed to communicate directly with one another, which promotes efficient peer-to-peer exchanges without the need for intermediary devices. Inherently, each node is endowed with a specific role, such as Commissioner, Controller, Controlee, OTA Provider, or OTA Requestor, each defining their behavior and interactions within the Matter network. For instance, a Commissioner is responsible for adding new devices to the network, creating new connections. Controllers manage other nodes by sending commands, while Controlees are at the receiving end of these commands. OTA Providers and Requestors facilitate the distribution and application of software updates throughout the network, respectively. The integration of complete application functionality into a single stack for each node streamlines communication and enhances autonomous operation. Even when nodes are part of multiple fabrics, they maintain their unique identifiers, ensuring consistent identification. A shared root of trust among nodes in a fabric bolsters the security of their interactions and data exchanges, which is pivotal for the network's integrity. Consequently, this architecture ensures that nodes are not only distinct but also function in a robust and responsive network environment, enhancing the overall resilience and efficacy of the Matter ecosystem.

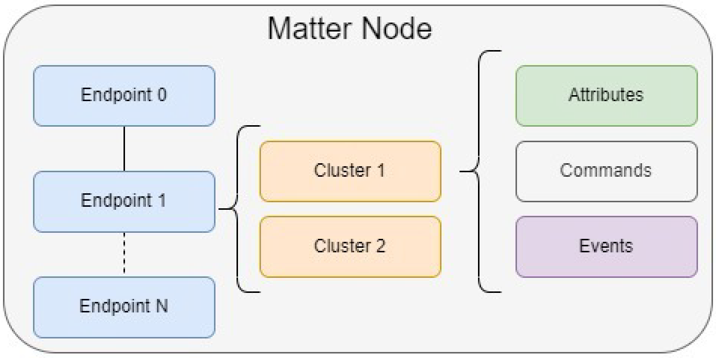

Figure 6 Matter Node Model

Endpoints

In the hierarchical structure of Matter, endpoints serve as subdivisions within nodes, organizing a node's functionality into discrete, manageable segments. These segments each represent a different aspect of the node's capabilities, such as in a smart thermostat, where separate endpoints might control heating and monitor temperature, respectively. Endpoints fall into two categories: leaf and composed. Leaf endpoints function independently, handling specific operations without reliance on other endpoints. In contrast, composed endpoints depend on other endpoints for full functionality. Endpoint 0 is unique and is always reserved for Utility Clusters, which manage foundational services including device discovery and diagnostics. Numerically distinct endpoints, beyond Endpoint 0, contain their own feature sets and operate independently, even if they share the same number across different nodes. This individual addressability enables precise management and modification of functionalities, contributing to the modularity of the Matter protocol. By aggregating clusters within endpoints, Matter allows for a comprehensive suite of features for each node, ensuring that each endpoint, with its particular role and function, contributes effectively to the performance and capabilities of the Matter device.

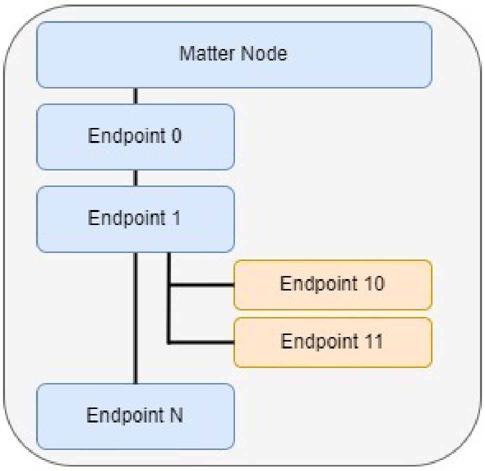

Figure 7 Matter Endpoint Model

Clusters

Clusters are the core building blocks of Matter's data model, organizing data into logical and functional groupings that underpin the operational capabilities of nodes. Within these clusters, attributes define the current state or configurations of a node, commands act as executable actions to alter these states or invoke specific functions, and events log the historical changes in a node's state for future reference. Each cluster is distinct, allowing for granular control and individual interactions within an endpoint. With the ability to handle an array of data types, from integers to strings and arrays, clusters can accommodate a wide range of functional requirements. The bidirectional nature of commands within clusters—where they can flow from client to server or vice versa—facilitates dynamic interactions, and the outcomes of these commands can vary from immediate action to acknowledgments or error statuses. Server clusters, which are stateful, hold the data and manage the states, while client clusters, being stateless, perform operations by interacting with the server clusters. This structure allows any cluster to function as a server or a client, granting nodes the versatility to store information and communicate with each other. For instance, a client cluster within a light switch can send a command to a server cluster within a light bulb to turn it on or off, showcasing the interactive and responsive nature of cluster communication. This arrangement emphasizes Matter's commitment to interoperability and flexibility, streamlining the development process and fostering the growth of smart home ecosystems.

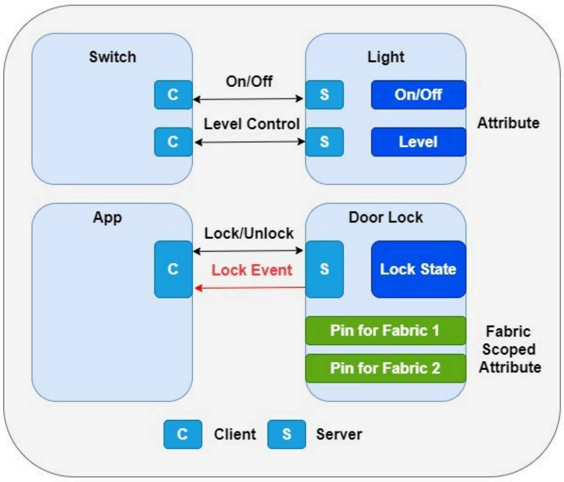

Figure 8 Matter Cluster Model

3.9 TR-181

The Broadband Forum's TR-181, also known as "Device:2", is a technical report that offers a standardized data model for various device types within the broadband home environment. TR-181 addresses a range of devices from gateways, routers, access points, other devices; as well as many technologies and protocols. Related data models in the Broadband Forum support voice over IP (VoIP) in TR-104, set-top boxes in TR-135, Network Attached Storage (NAS) in TR-140, and Femto Access Point (FAP) service in TR-196. TR-181 facilitates remote management and diagnostics, allowing service providers to ensure optimum performance, reduce maintenance costs, and quickly resolve issues. TR-181 also facilitates remote configuration through readWrite parameters, and more recently with USP-enabled commands and notifications. The TR-181 data model is supported by both the TR-369 User Services Platform and the legacy TR-69 CPE WAN Management Protocol (CWMP). TR-181 has an extensive Wi-Fi data model, as well as data models for IoTCapability, Zigbee, UPnP, DLNA, MoCA, G.hn, HomePlug, Cellular, IEEE 1905, etc. The data model is now being extended to encompass Matter and Tread. Through this standardized approach, TR-181 aids in simplifying device management in diverse broadband network environments.

3.10 TR-369 / User Services Platform (USP)

The Broadband Forum's TR-369, also known as the User Services Platform (USP), builds upon the legacy of CWMP (TR-069) but provides a more modern approach to device management. Unlike its predecessor, TR-369 is designed to manage not just broadband devices but the entire spectrum of connected devices in the home, including IoT devices. It's a platform-agnostic model that employs real-time communication, allowing devices to be managed and monitored instantaneously. Devices can interface to multiple TR-369 controllers, for example to support separate home automation and energy management services with separate controllers from separate service providers. TR-369 utilizes a message-based approach, supporting multiple Message Transfer Protocols (MTP) including MQTT, WebSockets, STOMP and now

Unix Domain Sockets (UDS), granting it the flexibility to cater to various use-cases. Regardless of the MTP, the same uniform TR-181 dataset can be carried. With its robust architecture, TR-369 paves the way for efficient device orchestration, analytics, and diagnostics in complex, multi-vendor environments. TR-369 also supports bulk data collection.

TR-369 Software Module Management (SMM) allows software modules to be distributed and instantiated from a cloud or edge. TR-369 recently added support for internal device communication with internal services or microservices using Unix Domain Sockets (UDS), Further, the App-enabled Services Gateway (ASG) is now being specified within the WBA and Broadband Forum to support apps or microservices on an in-home gateway similar to smartphone apps.

3.11 OCF Models

The Open Connectivity Foundation (OCF) is an industry consortium focused on creating a specification and sponsoring an open-source project to unlock the massive opportunity in the IoT market. Their goal is to ensure that devices from various manufacturers can securely and seamlessly interact with one another. The OCF specification covers everything from a set of device schemas, data models, and protocols to facilitate device discovery, onboarding, communication, and device-to-device interoperability. Built with a robust security framework at its core, OCF utilizes technologies like Public Key Infrastructure (PKI) and cloud-based management to ensure device integrity. By creating a unified solution and reducing market fragmentation, OCF hopes to accelerate the development and deployment of connected devices across various sectors, including the smart home, automotive, and healthcare industries.

4. NextGen Smart Home Use-Cases

4.1 Home Automation

Home automation, at its core, represents the nexus of wireless technologies, software, and interconnected systems that work in unison to enhance occupant experience. Protocols such as Wi-Fi 6, BLE 5.0, and Matter (formerly Project CHIP) serve as the underlying communication supporting home automation, making activities ranging from automated lighting control to adaptive thermostat adjustments more efficient than ever. The introduction of the Matter standard is a game-changer, providing uniform messaging and platform for IoT devices across various manufacturers to interoperate. Additionally, other protocols like Zigbee 3.0 and Z-Wave provide low-power solutions that are suitable for battery-operated devices, ensuring real-time responses without draining power. As AI-driven solutions integrate into these platforms, devices can learn and adapt to user behaviors, making anticipatory adjustments. The roll-out of 5G technology provides a high-speed, low-latency wireless WAN environment, further optimizing device-to-edge and device-to-cloud interactions. Secure protocols, from WPA3 for Wi-Fi to end-to-end encryption standards in Matter, ensure that data integrity and privacy are maintained. Cloud integrations, using platforms like AWS IoT and Google Cloud IoT Core, amplify automation capabilities by providing tools for remote device management, firmware over-the-air (FOTA) updates, and big data analytics. Voice-assistant integration using technologies like Amazon Alexa or Google Assistant also exemplify the advances in home automation, turning voice commands into actions.

Figure 9 Next Generation Home Automation

4.2 Edge Compute & Smart Home

Today's smart home IoT devices are constrained by limitations in compute power, storage capacity, and battery life. In many cases, smart home controllers, such as speakers or smart phones, rely on cloud infrastructure to execute various tasks. With proliferation of IoT devices in homes, the data they collectively generate can be astronomical. Edge computing provides the architecture to handle this data explosion, ensuring that data is processed, analyzed, and acted upon locally. The Smart Home edge device can take the form of a dedicated compute device or be integrated into Access Points, Smart TVs, smart speakers, and other devices. Various end devices including sensors, door locks, shades, thermostats, etc. feed data from the environment to these edge devices for local computing. The introduction of Smart Home Edge devices brings about several advantages:

1. **Privacy and Data Sovereignty**: Smart Home Edge devices ensure data privacy and sovereignty by keeping users' personal data local. This approach allows users to maintain ownership and control over their personal data.
2. **Reduced Latency**: For applications where low latency is critical, smart home edge computing can deliver near-real-time analysis and response, meeting users' latency demands, especially for larger workloads.
3. **Enhanced Resiliency**: Even in the event of disruptions to cloud connectivity, the network remains operational, ensuring that smart home systems continue to function.

4. **Extended Battery Life**: By shifting the compute burden from battery powered IoT devices to edge devices, the overall battery life of IoT devices is significantly extended. This ensures that IoT devices can operate longer without requiring frequent recharging or battery replacement.

Home edge computing enables a diverse range of use cases. By embracing edge devices, a significant chunk of data processing can be localized, which translates to reduced latency. Such immediate processing is especially crucial for applications requiring rapid response, like real-time video surveillance analytics, camera object classification and facial recognition, monitoring and alerting when children enter unsafe zones, assisting in fall detection for aging individuals, for quick device actuation in safety-critical scenarios. Other applications include compute offload from devices such as robot vacuum cleaners which use computer vision to map and navigate the house. Moreover, integrating solid state drives (SSDs) or fast-access memory modules into edge devices accelerates data retrieval and storage operations. Technologies like Multi-access Edge Computing (MEC) and 5G environments can also further the integration between edge devices in homes and cellular networks.

Fog computing can further extend the concept and benefits of edge computing. Fog computing envisions distributed computing, with some functions performed close to the user (e.g. running an AI model), and some functions performed further back toward the cloud (e.g., training an AI model). The fog can extend computing across in-home devices, an in-home compute server, near edge computing, far edge computing, and to the cloud.

Fog computing and Multi-access Edge Computing (MEC) significantly enhance smart home technologies by bringing cloud computing capabilities closer to the edge of the network and the users. In smart homes, fog computing allows for localized data processing, enabling immediate and responsive actions like climate control adjustments, while offloading complex data analysis to the cloud. This not only improves network efficiency and reduces latency but also enhances privacy and security by minimizing the transmission of sensitive data to the cloud. MEC further complements these benefits by providing faster communication and efficient integration of a multitude of IoT devices, thus improving the performance of smart home systems and mobile devices through reduced processing times and quicker data analysis. Telecom and network operators are central to this ecosystem, responsible for setting up and maintaining the necessary infrastructure, managing services and resources, ensuring robust security, and facilitating seamless integration with cloud services. These operators are not just infrastructure providers but also innovators, driving the development of new technologies and capabilities in fog and MEC, thereby advancing the functionality and efficiency of smart homes.

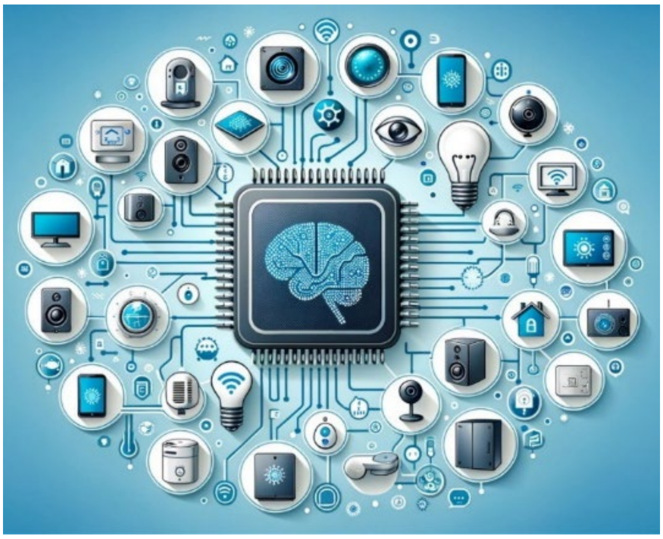

Figure 10 Edge Compute & Smart Home

4.3 AI & Smart Home

The integration of Artificial Intelligence (AI) in Smart Home Edge Computing represents a significant leap in the evolution of home automation and IoT (Internet of Things) applications. AI enhances edge computing's capabilities, offering intelligent, adaptive, and highly personalized experiences for users. Here are key aspects where AI contributes significantly:

1. Intelligent Decision Making: AI algorithms can analyze data from various IoT devices to make informed decisions. For instance, an AI system can learn a user's preferences and routines, and automatically adjust smart home devices to optimize comfort and energy usage.
2. Predictive Analytics: AI can predict future needs or potential issues in a smart home setting. For instance, it can anticipate device maintenance needs, or suggest optimal times for energy consumption based on usage patterns and utility rates.
3. Enhanced Security and Surveillance: AI-powered surveillance systems can offer advanced features like anomaly detection, facial recognition, and immediate alerting for unusual activities, enhancing home security beyond conventional systems.
4. Natural Language Processing (NLP): Smart home devices equipped with AI can understand and process human language, allowing for more natural and efficient voice commands and interactions.
5. Learning and Adaptation: AI in smart home edge devices can continuously learn from user interactions and environmental data, adapting to changes and improving its functionality over time.
6. Energy Efficiency: AI can optimize energy use by learning and predicting the best times to operate certain devices, contributing to more efficient energy management in smart homes.

Figure 11 AI & Smart Home

4.4 VAS: Connected Health and Aging in-Place

Connected health, especially in the domain of aging in-place, is witnessing profound technological advances. The foundation of this is the interplay of IoT devices, robust networking, and analytics. Devices employ sensors with MEMS technology for precision tracking of vitals. BLE, known for its low-energy footprint, is now becoming pivotal for wearable health trackers, ensuring long operational lifetimes. Concurrently, Wi-Fi 6 and 7 allow high-throughput data communication, making real-time video consultations and data-heavy transmissions hassle-free. The integration of technologies like Matter ensures device interoperability, which is especially crucial when devices from different manufacturers need to share health data seamlessly. Real-time data analysis is gaining momentum, with edge devices now having dedicated Neural Processing Units (NPUs) for on-the-fly analytics. With 5G's low latency, remote patient monitoring becomes more efficient, offering healthcare professionals almost instantaneous feedback. Moreover, the rise of AI-driven predictive health platforms can foresee potential health risks by analyzing patterns in the collected data. As health data is sensitive, advanced encryption standards, often hardware-accelerated, are being incorporated to ensure data privacy and protection.

Wi-Fi sensing processes the Channel State Information (CSI) from today's multi-antenna Wi-Fi systems to identify and classify motion and presence within a home. Wi-Fi sensing can monitor health, including with fall-detection and heart-rate monitoring. Wi-Fi sensing also applies to other applications such intruder detection for physical security.

Figure 12 Aging In-Place Use Case

4.5 VAS: Home Security & Monitoring

Modern home security hinges on the confluence of sensor technology, advanced wireless communications, and artificial intelligence. Devices are now equipped with LiDAR and infrared sensors, enabling precise motion detection and depth sensing. When paired with HD or 4K cameras, the level of surveillance detail captured is unparalleled. Fast, stable, and secure communication is non-negotiable, with Wi-Fi 6/6E and Wi-Fi 7 offering the necessary bandwidth and range, especially for high-definition video feeds. Furthermore, the integration of Matter ensures a cohesive ecosystem where security devices can intercommunicate without vendor-specific bottlenecks. AI-enhanced analytics is changing the game; not only can they identify an intruder but can also differentiate between a human and an animal, or a normal resident and a stranger, reducing false alarms. Additionally, with the Internet of Things (IoT) being at the forefront, security systems are now integrating with smart home setups, offering layered security protocols. For instance, a breached security could automatically lock all smart doors, shut windows, and alert local authorities. The decentralized processing offered by edge computing aids in immediate threat assessment, reducing dependency on cloud servers. Lastly, with 5G connectivity, homeowners can remotely access real-time video feeds with negligible latency, ensuring they're always in the know.

Figure 13 Home Security and Monitoring Use-case

4.6 VAS: Energy Monitoring & Energy Demand-Response

The quest for energy efficiency is driving profound innovations in how homes consume and respond to energy demands. Advanced sensor suites, from ultrasonic flow meters to infrared occupancy sensors, provide granular data on energy consumption. Protocols like Zigbee and Thread, known for its low-power requirement and mesh networking capability, are prevalent in smart meters and other energy monitoring devices. Real-time data analysis, enabled by Matter's standardization and edge computing principles, allows homes to adapt dynamically to changing energy needs. With the ubiquity of Wi-Fi 6/6E and Wi-Fi 7, large-scale data, like solar panel performance metrics or whole-home energy consumption trends, can be processed and shared rapidly. AI-driven optimization algorithms can now pre-emptively adjust HVAC systems based on predictive weather models or occupancy patterns, ensuring optimal energy utilization. Furthermore, with the smart grid evolution, homes can actively participate in energy demand-response, dynamically consuming, storing, or even selling back energy based on grid requirements. With 5G's assured communication, these interactions between homes and energy grids are almost instantaneous, ensuring energy stability and efficiency.

Figure 14 Home Energy Awareness and Demand-Response Use-case

4.7 VAS: Media Distribution Use-Case

In the realm of home entertainment, the media distribution paradigm is rapidly shifting towards decentralization, hyper-personalization, and high fidelity. Media devices, from smart TVs to streaming sticks to smart speakers, are now embracing Wi-Fi 6/6E and Wi-Fi 7 for their high bandwidth capability, which is especially crucial for 4K or 8K streaming. Matter's influence ensures seamless communication between media devices, creating a harmonious media ecosystem in homes. Advanced codecs, like AV1 or H.266/VVC, promise better compression rates without sacrificing visual quality, ensuring efficient network utilization. The role of edge computing is also becoming undeniable in media distribution, as locally cached content reduces streaming latency and offers immediate playback. With AI, recommendation engines are becoming smarter, often predicting user preferences and preloading content, ensuring an uninterrupted viewing experience. Additionally, advanced audio technologies, such as Dolby Atmos or DTS:X, are proliferating, and with Wi-Fi's ample bandwidth, transmitting these high-definition audio streams becomes seamless. Integration of 5G and Wi-Fi QoS Management with home media setups further elevates the experience, ensuring cloud gaming or AR/VR content is delivered with minimal lag. In essence, the convergence of these technologies is sculpting the future of home entertainment, making it more immersive and personalized than ever before.

Figure 15 Home Media Distribution Use-case

5. Deploying and Managing Smart Home Services

Smart home services are inherently multifaceted and, as the landscape evolves, the complexity of deploying and managing these services escalates. At the core, there's an interplay of various communication protocols, service orchestration tools, edge computing principles, and device management platforms, all choreographed to work in harmony.

Service orchestration in smart home environments often leans on tools like Kubernetes, primarily due to its efficacy in managing containerized applications. Kubernetes allows for easy scaling, automated rollouts/rollbacks, and self-healing capabilities, which become essential as the number of connected devices and the complexity of services surge. Device management, on the other hand, involves not just the physical devices but their digital twins in the cloud. Platforms such as Eclipse Hono stand out here, as they allow for protocol adaptation, thereby ensuring devices with diverse communication standards can coexist. Furthermore, MQTT (Message Queuing Telemetry Transport) and Websockets have gained prominence as the de facto communication protocols for many IoT devices. They're lightweight, ensuring they don’t strain the limited computational capabilities of smaller devices.

5.1 Current Proprietary Industry Solutions

The arena of proprietary smart home solutions presents a mosaic of custom protocols, specialized software frameworks, and intricate device management techniques. Let's dissect some of the big players.

Apple's HomeKit serves as an exemplar of meticulous integration, with the protocol ensuring not just device communication but prioritizing end-to-end encryption. It employs the HomeKit Accessory Protocol (HAP) over IP and Bluetooth LE. HAP ensures that data is consistent across devices, allowing for instantaneous updates and state synchronization. Apple's commitment to user privacy is echoed in the HomeKit architecture, with data staying local to the device or being encrypted while traversing networks.

Amazon's Alexa ecosystem, by contrast, leverages its might from the cloud-centric nature of AWS. Using AWS IoT Core, the Alexa system can securely communicate with connected devices, process messages, and relay appropriate instructions. The underlying MQTT protocol ensures lightweight and timely data transfer. Moreover, AWS Lambda integration means that the ecosystem can execute code in response to events, like turning on a light when you say, "Alexa, lights on."

Google's smart home framework doesn't lag behind. Utilizing technologies like Weave and Thread, Google ensures reliable, low-latency communication across devices. Weave provides a comprehensive set of device schemas, and its underlying principle ensures that devices are aware of each other's capabilities. This intelligence is crucial in creating a cohesive smart home environment.

The SmartThings ecosystem, anchored by its SmartThings Hub, leverages an open-source protocol called SmartThings Schema to facilitate communication with a myriad of devices using different protocols such as Zigbee, Z-Wave, or Wi-Fi. This protocol ensures that the hub can not only communicate with various smart devices but also send commands and status updates efficiently. The SmartThings App acts as the control center for this system, providing users the convenience of managing their smart devices remotely, establishing automated routines, and receiving important alerts. Furthermore, SmartThings Cloud API empowers developers to build custom integrations, significantly enhancing the versatility of the ecosystem.

Despite their prowess, the insular nature of these solutions often becomes a double-edged sword. While they guarantee seamless experiences within their ecosystems, they can also inadvertently stifle the synergy of cross-platform devices. The lack of a universal standard means that a device optimized for HomeKit may not communicate effectively within an Alexa-dominated environment. This absence of full interoperability can lead to inefficiencies, redundancies, and, in worst-case scenarios, total system incompatibility.

Proprietary frameworks often employ unique encryption standards, communication protocols, and API endpoints. While this ensures security and optimization within their environments, it also curtails third-party integrations. Developers, limited by these ecosystem-specific constraints, might face challenges in integrating novel technologies or creating cross-platform solutions.

While these proprietary solutions have indisputably advanced the smart home sector, the call for open, standardized frameworks is getting louder. The emerging consensus hints at a future where specialized, proprietary excellence blends seamlessly with open standards, thus nurturing a holistic, user-centric smart home landscape.

5.2 Operator-Managed Smart-Home Standardized Framework

The limitations of proprietary solutions can be overcome via standards solutions including those discussed previously here. In particular, Matter now provides standardized inter-device messaging, and USP with TR-181 provides standardized cloud control.

The standardized multi-vendor ecosystem will foster innovation from many players and support multiple service offerings. These services can be powered by a number of cloud or edge systems, seamlessly interoperating within the home environment.

Therefore, the IoT & Smart Home group has developed an implementation based on WBA's Operator Managed Wi-Fi to ensure a series of benefits and complement with the necessary IoT dimensions and modules.

This Smart Home implementation is built upon the WBA Operator Managed Wi-Fi Reference Specification and Architecture, which serves as the foundation for the solution.

5.2.1 Key Benefits of a Standardized Framework

One of the key advantages of adopting a standardized framework is its ability to ensure **interoperability**. Standardized protocols like Matter and USP/TR-181 enable devices from different manufacturers to work seamlessly together. This ensures that consumers have the freedom to choose from a wide variety of devices without worrying about compatibility issues, fostering a more versatile and consumer-friendly market.

Scalability is another significant benefit. A standardized framework allows for easy scaling of smart home systems. As new devices and services are added, they can be integrated smoothly without the need for extensive reconfiguration or additional proprietary solutions. This makes it easier for users to expand their smart home ecosystems over time.

Security is also enhanced through standardized protocols. By adhering to standardized security protocols, the smart home ecosystem can ensure that all devices and communications are secure. This reduces the risk of vulnerabilities that could be exploited in a proprietary system with inconsistent security measures, thereby protecting user data and maintaining privacy.

Flexibility and innovation are promoted within a standardized framework. Developers and manufacturers can focus on innovation rather than compatibility issues. This fosters a more dynamic and rapidly evolving market, with new features and improvements being introduced regularly, benefiting both the industry and consumers.

From an economic perspective, **cost efficiency** is a notable advantage. Standardized solutions can reduce costs for both manufacturers and consumers. Manufacturers benefit from economies of scale and reduced development costs, while consumers benefit from a competitive market with more affordable options.

Lastly, a standardized framework enhances the overall **user experience**. With a unified, interoperable system allows consumers to manage all their smart home devices through a single interface, creating a more intuitive and convenient setup. This streamlined experience can significantly improve user satisfaction and engagement with smart home technology.

5.2.2 Smart Home & IoT - Operator-Managed Framework: Overview

The diagram illustrates the architecture of a Customer Premises Equipment (CPE) Gateway Middleware system, integrated with cloud-based Unified Service Platform (USP) controllers and services. This system is designed to optimize and manage smart home devices and services.

Cloud Components:

- **Cloud USP Controllers and Services:** These include various microservices such as Provisioning/ACS, Data Collectors/Telemetry, and an Edge Microservice Orchestrator. The orchestration service is responsible for updating and maintaining edge services on the CPE.
- **Provisioning/ACS:** Manages the automated configuration and provisioning of CPE devices.
- **Data Collectors/Telemetry:** Gathers data from CPE devices for monitoring and analytics.
- **Edge Microservice Orchestrator:** Oversees the deployment, update, and maintenance of edge microservices on the CPE.

CPE Components:

- **Config DB and Config Manager**: Serve as the database and management system for CPE configuration, ensuring devices are correctly set up and maintained.
- **USP Broker with Access Controls**: Acts as an intermediary, managing communication between cloud services and edge applications, ensuring secure access and data exchange.
- **Edge Apps & Microservices**: Includes key functionalities like Matter Device Management & Controller, Matter/Smart Home Bridge, Local Scenes, and Local AI/ML processing. These applications enhance the interoperability and intelligent automation of connected devices.
- **Edge Microservices Manager**: Responsible for the deployment, execution, monitoring, and resource management of microservices on the CPE, enabling dynamic service delivery and management.

Middleware and Communication:

- **System IPC Bus/USP Internal IMTP**: Facilitates internal messaging and task processing within the CPE, ensuring efficient communication between different components.
- **Northbound APIs**: These APIs, based on TR-181 standards and Wi-Fi Alliance Data Elements (WFA DE), support communication between the CPE and cloud services, allowing for seamless

integration and management of services like EasyMesh, Matter, and OTBR (OpenThread Border Router).

- Southbound APIs: Interface with hardware components, such as Wi-Fi drivers, BLE drivers, Z-Wave/LPWAN modules, and routing accelerators, ensuring smooth operation and control of the physical network and connected devices.

External Integration:

- EasyMesh Agent and Controller: Complying with IEEE 1905.1, these components manage the mesh network, facilitating the extension of network coverage through retail extenders and ensuring a robust and seamless Wi-Fi experience.

This architecture exemplifies a robust, scalable, and secure solution for managing smart home environments, providing a seamless interface between cloud-based services and local edge devices. The integration of various standards and protocols ensures compatibility and futureproofing in a rapidly evolving IoT ecosystem.

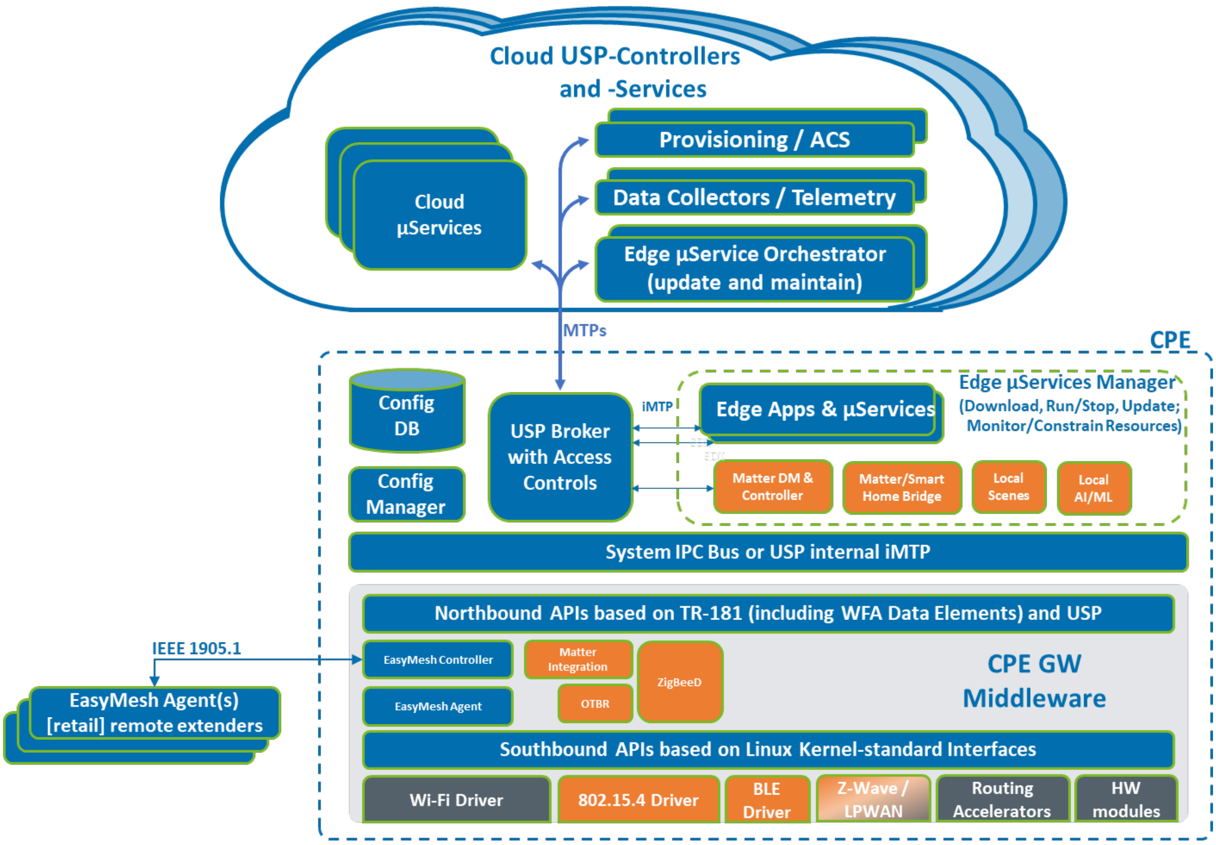

Figure 16 Smart Home & IoT - Operator-Managed Framework

The smart home integration within the CPE Gateway Middleware architecture builds on the foundational components previously outlined, enhancing the system's ability to manage and control a diverse array of connected devices. By incorporating advanced technologies like Matter, OpenThread Border Router (OTBR), and local AI/ML processing, this architecture not only supports seamless communication and interoperability among devices but also positions the CPE as a central hub for smart home management. This evolution addresses the needs discussed in industry meetings, where the focus was on ensuring hardware compatibility, flexibility in device commissioning, and reducing reliance on proprietary ecosystems. As a result, the architecture not only future-proofs smart home environments but also empowers operators to deliver more autonomous, secure, and user-friendly solutions.

1. Matter Device Management & Controller:

- **Role:** Matter, an open-source standard, ensures seamless communication between various smart home devices regardless of the manufacturer. The CPE architecture allows operators and hardware suppliers to obtain and manage Matter containers, ensuring hardware requirements are met and installation options are clearly understood. This was highlighted as crucial for ensuring that devices remain compatible and secure as the Matter Data Model evolves.
- **Implementation Strategy:** In response to evolving standards, it was suggested during discussions that the Matter Data Model block should be moved to a container rather than being embedded in firmware. This approach ensures that software requiring periodic updates remains flexible and up-to-date.

2. Matter/Smart Home Bridge:

- **Role:** The bridge acts as a crucial translation layer, enabling legacy devices to communicate with Matter-compliant devices, thus extending their usability. This component is particularly significant in providing an alternative to the dominance of proprietary smart home ecosystems by enabling the CPE to act as the central hub for commissioning and controlling devices.
- **Operator Flexibility:** As discussed, operators can use the CPE for commissioning and control, reducing reliance on phones or smart hubs typically provided by tech giants. This flexibility was emphasized as a strategic advantage for operators looking to offer independent, user-friendly smart home solutions.

3. OpenThread Border Router (OTBR):

- **Role:** OTBR facilitates communication between Thread devices and other IP-based networks, enabling seamless integration and control of low-power devices within the smart home network. The importance of BLE (Bluetooth Low Energy) support in the gateway, particularly for use cases where the CPE is intended to onboard and commission IoT devices autonomously.

4. Local AI/ML Processing:

- **Role:** Local AI/ML capabilities within the CPE enable real-time processing, enhancing the responsiveness of smart home systems. This functionality ensures that critical operations continue even if cloud connectivity is interrupted, providing a reliable and secure user experience.
- **Use Case Considerations:** Discussions also touched on the potential of the CPE architecture to support multiple use cases across different operator environments. The flexibility of the architecture allows for the deployment of various smart home scenarios, tailored to the specific needs of the user or operator.

6. Future Work

The Smart Home & IoT - Operator-Managed Industry Framework consists of two main components:

- Visualizing the future evolution of Smart Homes as a connectivity hub and how to drive better interoperability between stable and emerging technologies
- Helping residential service providers with a Managed Wi-Fi reference architecture that incorporates IoT and Matter components on its overall set of functionalities, that will allow these to develop and procure equipment vendors that are compliant with the interoperable requirements.

Ultimately, this initial deliverable from the WBA IoT & Smart Home group derives an evolving modulation of the WBA Operator Managed Wi-Fi, which we refer to as a reference implementation for the Smart Home.

The work will continue within the WBA through multiple initiatives:

- **IoT & Smart Home and Multi-Dwelling Units (MDU) Centralized Management**: A group of WBA members is preparing a program proposal (Terms of Reference – ToR) for the 2025 roadmap. The program will focus on the Smart Home environment under the emerging trend of MDU and how to guarantee best possible convergence of technologies, interoperability and viable business case for service providers, particularly focused in MDU centralized management.
- **Operator Managed Wi-Fi**: Entering its 3rd phase, the team responsible for developing the underlying reference architecture and technical functionalities specification for residential broadband Wi-Fi will now move towards compliance work, creating testing mechanisms so that autonomously or through third parties, operators and vendors are able to match advertised equipment functionality with actual delivery of such features. Further developments are expected throughout 2025.

The IoT & Smart Home Project Team invites industry players to stay engaged with the upcoming work.

Acronyms and Abbreviations

Acronym / Abbreviation	Definition
WBA	Wireless Broadband Alliance
IoT	Internet of Things
BLE	Bluetooth Low Energy
USP	User Services Platform
OCF	Open Connectivity Foundation
OMSH	Smart Home & IoT - Operator-Managed Framework
CSA	Connectivity Standards Alliance
TWT	Target Wake Time
rTWT	Restricted Target Wake Time
OFDMA	Orthogonal Frequency Division Multiple Access
QoS	Quality of Service
QoE	Quality of Experience
MoCA	Multimedia over Coax
LLC	Logical Link Control
PHY	Physical Layer
MAC	Media Access Control
LLDP	Link Layer Discovery Protocol
OUI	Organizational Unique Identifier
ACPI	Advanced Configuration and Power Interface
ALME	Abstraction Layer Management Entity
ISM	Industrial, Scientific and Medical
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Network
AES Encryption	Advanced Encryption Standard
CHIP	Project Connected Home over IP
API	Application Programming Interface
RF	Radio Frequency
OTA	Over the Air
FAP	Femto Access Point
VoIP	Voice over IP
NAS	Network Attached Storage
CWMP	CPE WAN Management Protocol
MTP	Message Transfer Protocol
UDS	Unix Domain Sockets

SMM	Software Module Management
UDS	Unix Domain Sockets
PKI	Public Key Infrastructure
FOTA	Firmware Over the Air
WPA	Wireless Protected Access
AWS	Amazon Web Services
MEC	Multi-Access Edge Computing
NLP	Natural Language Processing
NPU	Neural Processing Units
CSI	Channel State Information
LiDAR	Light Detection and ranging
HVAC	Heating, Ventilation and Air Conditioning
HAP	HomeKit Accessory Protocol
CPE	Customer Premises Equipment
MQTT	Message Queuing Telemetry Transport
IPC	InterProcess Communication
ACS	Auto Configuration Server
OTBR	OpenThread Border Router

Participant List

Name	Company	Job Role
Wael Guibene	Reliance Jio	Project Leader, Images Creator
Fatemeh Fazel	Intel	Project Co-Leader
Ken Kerpez	DZS	Editorial Team
George Hechtman	Hechtman Venture Development (HVD)	Editorial Team
Dennis Edwards	NOKIA	Editorial Team
David Barr	Prpl Foundation	Editorial Team
Amir Jalil	Aerial	Project Participant
Jessie Manik	Bell Mobility	Project Participant
Martin Casey	Calix	Project Participant
Meganathan Pooranan	Calix	Project Participant
David Grant	Charter Communications	Project Participant
Loay Kreishan	Charter Communications	Project Participant
Ruchi Kothari	Comcast	Project Participant
Gaetan Feige	Hechtman Venture Development (HVD)	Project Participant
Livia Rosu	MaxLinear	Project Participant
Dino Demetriou	Minime Labs	Project Participant
Tim Spets	NOKIA	Project Participant
Tom Van Driessche	NOKIA	Project Participant
José Martinez	RDK-m	Project Participant
Satyendra Bhaisare	Zebra Technologies	Project Participant
Pedro Mouta	WBA	Project Participant