In Home Wi-Fi: Multiple-AP Solutions Trial

Use Cases Scope Document

Source: Wireless Broadband Alliance
Author(s): WBA In-Home Wi-Fi
Issue date: June 2020
Version: 1.0.0
Document status: Final

ABOUT THE WIRELESS BROADBAND ALLIANCE

Founded in 2003, the vision of the Wireless Broadband Alliance (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 and organizations to achieve that vision. WBA undertakes programs and activities to address business and technical issues, as well as opportunities, for member companies.

WBA work areas include advocacy, industry guidelines, trials and certification. Its key programs include NextGen Wi-Fi, 5G, IoT, Testing & Interoperability and Roaming, with member-led Work Groups dedicated to resolving standards and technical issues to promote end-to-end services and accelerate business opportunities. WBA's membership is comprised of major operators and leading technology companies, including BSNL, Orange, Facebook, Google, HPE Aruba, Huawei, Nokia, Qualcomm, Shaw, Swisscom, Softbank, Rogers, Telstra, Telus and T-Mobile US.

The WBA **Board** includes AT&T, Boingo Wireless, Broadcom, BT, Cisco Systems, Comcast, Deutsche Telekom AG, GlobalReach Technology, Intel, KT Corporation, Reliance Jio and SK Telecom. For a complete list of current WBA members, **click here**.

Follow Wireless Broadband Alliance at:

www.twitter.com/wballiance
http://www.facebook.com/WirelessBroadbandAlliance
https://www.linkedin.com/company/wireless-broadband-alliance

CONFIDENTIALITY

Privileged/confidential information may be contained in this document and any files attached in it ('WBA Documentation').

Only WBA member companies who have signed the new WBA IPR Policy (Located at: **http://extranet.wballiance.com/apps/org/workgroup/inf_cen/document.php?document_id=2125**) and are the intended recipient are entitled to receive, review or comment on this WBA Documentation.

If you are not the intended recipient (or have received this WBA Documentation in error), please notify the sender and WBA (**pmo@wballiance.com**) immediately and delete this WBA Documentation. Any unauthorized copying, disclosure, use or distribution of this WBA Documentation is strictly forbidden.

UNDERTAKINGS AND LIMITATION OF LIABILITY

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

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

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

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

CONTENTS

1 Executive Summary 1
2 Deployment Use-Cases 2
3 DEP-1 – IoT onboarding challenges – not using Easy Connect™ 3
3.1 Use Case 3
3.2 Assumptions 3
3.3 Procedure 3
3.4 Metrics 3
4 DEP-2a – IoT onboarding challenges - using Easy Connect™ 4
4.1 Use Case 4
4.2 Assumptions 4
4.3 Procedure 4
4.4 Metrics 5
5 DEP-2b – IoT onboarding challenges - using Easy Connect™ 5
5.1 Use Case 5
6 DEP-2c – IoT onboarding challenges - using Easy Connect™ 5
6.1 Use Case 5
6.2 Assumptions 6
6.3 Procedure 6
6.4 Metrics 6
7 DEP-3 – Initial installation of a multiple AP network by an end-user 7
7.1 Use Case 7
7.2 Assumptions 7
7.3 Procedure 7
7.4 Metrics, Observations or Considerations 8
8 DEP-4 – Professional installation of multiple interconnected APs 8
8.1 Use Case 8
8.2 Assumptions 8

8.3 Procedure 9
8.4 Metrics, Observations or Considerations 9
9 DEP-5 – Channel allocation / selection 10
9.1 Use Case 10
9.2 Assumptions 10
9.3 Procedure 10
9.4 Metrics 11
10 DEP-6 – Adding an AP to an already installed system 11
10.1 Use Case 11
10.2 Assumptions 11
10.3 Procedure 12
10.4 Metrics 13
11 DEP-7 – Detecting and specifying the location of APs 13
11.1 Use Case 13
11.2 Assumptions 13
11.3 Procedure - installation 14
11.4 Procedure - optimization 14
11.5 Metrics 14
12 DEP-8 – Network loop prevention 15
12.1 Use Case 15
12.2 Assumptions 15
12.3 Procedures 15
12.4 Metrics 16
13 OPS-1 – Self-healing for fixing channel interference issues 16
13.1 Use Case 16
13.2 Assumptions 16
13.3 Procedure 16
13.4 Metrics 17
14 OPS-2 – Preventing orphaned APs 17

14.1 Use Case 17
14.2 Assumptions 17
14.3 Procedure 17
14.4 Metrics 18
15 OPS-3 – Handling orphaned APs 18
15.1 Use Case 18
15.2 Assumptions 18
15.3 Procedure 19
15.4 Metrics 19
16 OPS-4 – Handling and detection of unmanaged APs using same SSID as the managed network 19
16.1 Use Case 20
16.2 Assumptions 20
16.3 Procedure 20
16.4 Metrics 21
17 OPS-5 – Client steering 21
17.1 Use Case 21
17.2 Assumptions 21
17.3 Procedures 21
17.3.1 Single AP band steer procedure 21
17.3.2 Multi-AP AP steer procedure 22
17.4 Metrics 22
18 OPS-6 – Coordinated firmware upgrade 23
18.1 Use Case 23
18.2 Assumptions 23
18.3 Procedures 24
18.4 Metrics 24
19 OPS-7 – Network topology control/optimization 24
19.1 Use Case 24

19.2 Assumptions 25
19.3 Procedures 25
19.4 Metrics 26
20 MAN-1 – App provided to end-user 26
20.1 Use Case 26
20.2 Assumptions 26
20.3 Procedure 26
20.4 Metrics 27
21 MAN-2 – Proactive diagnostics and analytics by the operator 27
21.1 Use Case 27
21.2 Assumptions 27
21.3 Procedure 28
21.4 Metrics 28
22 MAN-3 – Topology management by the operator. 28
22.1 Use Case 28
22.2 Assumptions 29
22.3 Procedure 29
22.4 Metrics 29
23 MAN-4 – Onboarding devices to an Easy Connect™ (DPP Initiator-Configurator) AP. 29
23.1 Use Case 30
23.2 Assumptions 30
23.3 Procedure 30
23.4 Metrics, Observation or Considerations 30

1 Executive Summary

Wi-Fi is the most widespread access technology to connect to the Internet within home environments. To this end, Operators have realized that they must own Wi-Fi in the Home, provide quality of service expected by customers, and adopt best practices to overcome Wi-Fi performance challenges. WBA acknowledges Wi-Fi's widespread increase in importance to deliver a high-quality broadband service in the home and strives to be a partner in contributing to that story.

The WBA In-Home Wi-Fi workgroup aims to promote understanding and adoption of Wi-Fi standards and technologies appropriate for In-Home use to WBA members and the wider community. WBA's In-Home workgroup recently published a "current state-of-the-art" document depicting the Wi-Fi landscape and outlined industry guidelines and best practices for operators to achieve high-quality In-Home Wi-Fi. In this document the area of multiple-AP home networks was identified as the focus for the group's current work.

Multiple Access Point (AP) solutions for the enterprise have been around for many years. Where most homes relied on one AP they often now require multiple APs for reliable whole-home coverage, and the cost and simplicity of modern solutions have brought enhanced Wi-Fi capabilities In-Home.

By means of use-cases, this paper describes features that should be found in multiple-AP-capable In-Home solutions and thereby highlights some of the advantages of adopting them. The use-cases are divided into broad functional areas of Deployment, Operation, and Management/Diagnostics. Amongst the newer features covered by the use cases, the reader will find several multi-AP functionalities; as an example, using Wi-Fi CERTIFIED EasyMesh™, zero-touch onboarding, and Wi-Fi Easy Connect™™, along with diagnostic features supported by Wi-Fi CERTIFIED Data Elements™.

2 Deployment Use-Cases

The use-cases are divided into broad functional areas of 1- Deployment (DEP), 2- Ongoing Operation (OPS), and 3- Management/Diagnostics (MAN):

N	Use Case
Deployment Test Cases	
1	DEP-1 – IoT onboarding challenges – not using Easy Connect™.
2	DEP-2a – IoT onboarding challenges - using Easy Connect™.
3	DEP-2b – IoT onboarding challenges - using Easy Connect™.
4	DEP-2c – IoT onboarding challenges - using Easy Connect™.
5	DEP-3 – Initial Installation of a multiple AP network by an end-user.
6	DEP-4 – Professional installation of multiple interconnected APs.
7	DEP-5 – Channel allocation / selection.
8	DEP-6 – Adding an AP to an already installed system.
9	DEP-7 – Detecting and Specifying Location of APs.
10	DEP-8 – Network Loop Prevention.
Ongoing Operation Test Cases	
10	OPS-1 – Self-healing for fixing channel interference issues
11	OPS-2 – Preventing orphaned APs.
11	OPS-3 – Handling orphaned APs.
12	OPS-4 – Handling and detection of unmanaged APs using same SSID as the managed network.
13	OPS-5 – Client steering
12	OPS-6 – Coordinated firmware upgrade.
13	OPS-7 – Network topology control/optimization
Management and Diagnostics	
14	MAN-1 – App provided to end-user.
15	MAN-2 – Proactive diagnostics and analytics by the operator.
16	MAN-3 – Topology management by the operator.
17	MAN-4 – Onboarding devices to an Easy Connect™ (DPP Initiator-Configurator) AP.

3 DEP-1 – IoT onboarding challenges – not using Easy Connect™

Use case will consist of onboarding scenarios according to IoT device type, existing Wi-Fi network configuration, and out-of-box onboarding procedure supported by IoT device vendor.

3.1 Use Case

IoT Device Type

1. Onboarding single-band IoT device.
   Example Globe Electric Wi-Fi Smart Plug or Teckin SP10 Smart Plug
2. Onboarding dual-band IoT device.
   Example Leviton DW15P-1BW Smart Plug

3.2 Assumptions

Certain Wi-Fi network SSIDs configurations are required.

1. Onboarding IoT device on dual-band Wi-Fi network configured with a unified SSID
   a. Onboarding IoT device with band-steering enabled on Wi-Fi network
2. Onboarding IoT device on dual-band Wi-Fi network with separate SSIDs per

3.3 Procedure

1. Onboard via third-party Android or iPhone smartphone/tablet app supplied by IoT device vendor
   a. Default pairing mode requires smartphone to be on 2.4GHz band. Otherwise, need to launch AP mode and connect smartphone directly to device
      – this is the case with the Globe Electric App and Teckin App.
   b. Default pairing mode is AP mode
      – this is the case with the Leviton App.
2. Other on-boarding methods, if supported, include:
   a. WPS PBC or PIN – not supported in iOS, deprecated in Android 9+
   b. Bluetooth
   c. Amazon Wi-Fi simple setup process

3.4 Metrics

- Device is onboarded and confirmed via the third-party App, or the Routers device tables.

4 DEP-2a – IoT onboarding challenges - using Easy Connect™

Phone adding a new device/IoT to network by scanning a QR code

4.1 Use Case

A device in this scenario could be an IoT device with a QR code sticker attached to it, or a device which can display a QR code on a display (like a printer with an LCD display). This scenario is applicable when the AP is either a legacy AP without DPP support, or a DPP capable AP, although the former is the main focus due to market availability and possibly cost of implementation of a full DPP stack on IoT devices.

4.2 Assumptions

- The phone is the Initiator-Configurator
- The IoT device is the Responder-Enrolee

4.3 Procedure

1. The device has a QR code attached (e.g. a sticker on the bottom side of the device) or can display a QR code on an attached display. The device is powered up for the first time, or following a factory reset (unconfigured mode).
2. Phone scans the QR code and initiates bootstrapping.
3. Phone configures the device using DPP and provides SSID and password.
    a. In legacy AP use-case: Configuration includes WPA2 (or WPA3) password.
    b. In DPP AP use-case: Configuration includes information that allows the new device to communicate with the DPP AP and derive a network key securely.
4. With DPP R2 on both enrolee and Configurator sides, the enrolee sends its band support list with the configuration request message. It allows the phone to conclude if the enrolee supports the band of the requested network.
5. Configuration ends, and
    a. If enrolee supports DPP R1, then the session ends. The device will try to connect to the network, and there is no feedback mechanism defined.
    b. With DPP R2 on both enrolee and Configurator sides, the enrolee responds immediately with Configuration status result:
        i. STATUS_OK indicates that the configuration was accepted, and the enrolee will try to use it.

ii. STATUS_CONFIG_REJECTED indicates failure - The device does not accept the configuration and remains unconfigured.

If the enrolee responded with STATUS_OK, it would attempt to use the configuration to connect to the network. The phone remains up to 15 seconds in the DPP channel and waits for feedback. If no result is received, the feedback is “timeout”. The status result that the enrolee sends back could be:

i. STATUS_OK enrolee successfully associated to the AP and has network access

ii. STATUS_AUTH_FAILURE enrolee discovered the AP and failed to connect to the network.

iii. STATUS_INVALID_CONNECTOR enrolee received an invalid connector during network introduction - This is not applicable without DPP AKM.

iv. STATUS_NO_MATCH Received AP Connector is verified and valid, but no matching Connector could be found by enrolee - This is not applicable without DPP AKM.

v. STATUS_NO_AP enrolee failed to discover an access point.

4.4 Metrics

- Device is onboarded and confirmed via the return status, or the Routers device tables.

5 DEP-2b – IoT onboarding challenges - using Easy Connect™

5.1 Use Case

Phone adding a new AP to network by scanning a QR code

Similar to use case 1, credential type that is sent from the phone is for AP and not STA.

6 DEP-2c – IoT onboarding challenges - using Easy Connect™

6.1 Use Case

Phone joining a network by scanning the AP/Phone QR code

This use case may be applicable in two scenarios:

1. Another device is displaying a QR code or a QR code is available on a sticker or paper.
2. QR code is available on an AP supporting DPP. May not be applicable in the near future, until DPP supporting APs will be available in the market.

6.2 Assumptions

- The phone is the Initiator-Enrolee
- The AP or other phone is the Responder-Configurator

6.3 Procedure

1. The DPP AP has a QR code attached (e.g. a sticker on the bottom side or in the packing materials; a public network can possibly display a QR code in the premises), or a master phone is displaying a QR code.
2. Phone scans the QR code and initiates bootstrapping.
3. AP configures the device using DPP and derives a network key securely with the phone.
4. Phone responds with a Configuration Status immediately:
    a. STATUS_OK if configuration is valid
    b. STATUS_CONFIG_REJECTED in case of an error. Error cases could be in case there is corruption in the configuration message for example. Additionally, an error could be returned if a credential that the phone does not support was received.

    Configuration is saved and the phone tries to connect and send status feedback to the configurator. The status result that the phone sends back could be:

        i. STATUS_OK enrolee successfully associated to the AP and has network access
        ii. STATUS_AUTH_FAILURE enrolee discovered the AP and failed to connect to the network.
        iii. STATUS_INVALID_CONNECTOR enrolee received an invalid connector during network introduction - This is not applicable without DPP AKM.
        iv. STATUS_NO_MATCH Received AP Connector is verified and valid but no matching Connector could be found by enrolee - This is not applicable without DPP AKM.
        v. STATUS_NO_AP enrolee failed to discover an access point.

6.4 Metrics

- Device is onboarded and confirmed via the return status, or the Routers device tables.

7 DEP-3 – Initial installation of a multiple AP network by an end-user

To provide a naïve user with an easily achieved procedure by which a set of APs can be self-installed to provide a multiple-AP in-home network.

7.1 Use Case

A user requires a multiple-AP system for whole home coverage and has chosen to self-install it. Even though the user has existing Wi-Fi provided by their ISPs gateway, the new system may not support wireless connection with the original gateway. The user would like to be guided through the self-installation and end up with all their existing client devices connected to the new network with only a minimal amount of reconfiguration. The ultimate goal is for a 'zero-touch' installation, with the user simply placing and plugging in the Aps

7.2 Assumptions

- The APs in the multiple-AP system are not extenders, they work together to form their own standalone network requiring wired connection to the ISP modem/gateway.
- The APs are under the control of the user and not managed by the ISP, even though they may have been supplied by the ISP (except for s/w updates).

7.3 Procedure

The User purchases; or receives from the ISP; a box containing one or more APs (number chosen according to home size or other requirements), including instructions.

1. User unpacks the APs and identifies the installation instructions.
2. The user performs any pre-process actions described in the instructions.
3. The user places and powers up the APs in the positions and order specified in the instructions.
4. The user connects a Device to the network in the manner specified in the instructions.
5. If necessary, the user uses a management interface; in accordance with the instructions; to perform any necessary configuration or any customization desired by the user.
6. The user checks the connectivity of existing client devices and if necessary, reconnects them as instructed.
7. The user performs any post-install actions described in the instructions.
8. The new multiple-AP in-home network should now be operational.

7.4 Metrics, Observations or Considerations

- Are different options provided depending on how suitable the ISP modem location is for the first AP (Can it handle a bad location?)
- Are the APs all individual and interchangeable, or do they come supplied as a set
  a. If the APs are supplied as a set, do they come preconfigured to work together?
  b. Are the APs installed in a specific order and if so, how are they identified?
- Is there a management interface?
  a. What steps are required to connect to the AP management interface?
  b. Can the installation be completed without using the management interface?
- Is there a physical UI on the APs (e.g. lights, pairing button)?
  a. What form does it take and what is its purpose?
- What assistance is provided to the user when placing the APs around the home?
  a. How easy is this to use?
  b. How accurate is it?
- What steps must the user take to introduce a new AP to the network?
- Does the new system interconnect and/or interoperate with the existing gateway's Wi-Fi, or must that be disabled?
- Does the user have to re-associate all the client devices to the new network?

8 DEP-4 – Professional installation of multiple interconnected APs

A Customer orders an Internet Service with Wi-Fi, or the addition of Wi-Fi to an Internet Service.

8.1 Use Case

A user requires a multiple-AP system for whole-home coverage and has ordered the service from their ISP. The ISP sends out a specialist Wi-Fi installer to the customer's home.

The installer conducts a survey of the Wi-Fi around the home and decides how many APs to place and where to place them. After commissioning, the installer conducts further tests of the coverage and assists the customer to connect (some) devices to the new Wi-Fi network.

8.2 Assumptions

- The In-Home equipment is supplied by the ISP, not user sourced.

8.3 Procedure

The customer purchases a Wi-Fi Service and arranges an appointment for it to be installed in the home.

1) The installer may also determine any special requirements from the customer (e.g. live TV-streaming device).
2) The installer sets up a Wi-Fi source and conducts a survey of the coverage around the home.
3) Depending on the results, the installer may elect to move the ISP modem connection point.
4) The installer places and powers up the APs in the positions and order indicated by the guidance tools or expertise.
5) The installer performs any necessary configuration or customization required for the user.
6) The installer connects certain client devices to the network and shows the customer how to connect any others (that might not be in the home at the time).
7) The installer performs post-install checks to ensure that the APs are working as expected and giving acceptable coverage.
8) The installer may provide a certificate of completion along with instructions for adding further devices, etc.
9) The Operator/Service Provider continually monitors the level of service to make sure that it continues to meet any guarantees.

8.4 Metrics, Observations or Considerations

- What steps must the user take to introduce a new Client to the network?
- Does the user have any tools to view the performance of the system (such as the displaying the Service KPIs)?
- Does the network provide any extra facilities such as guest networks, or public networks?
    a. If present, how does the user manage access to the guest network?
- Does the network have any dynamic capability to reconfigure parameters if the environment changes, such as changing the channel and channel width?
- Must the user request installation of additional APs if these become necessary, or can they be self-installed?

9 DEP-5 – Channel allocation / selection

Multi-APs are installed to improve the overall user experience in a home. User experience does not solely depend on coverage but overall, on available bandwidth and hence qualitative access to services. Installation of multi-AP networks as such requires the availability of the RF medium. To efficiently access the RF medium, multi-AP networks must assign frequency slots to each of the APs to achieve the highest available medium accessibility. This frequency adjustment ability of the multi-AP network should also be applied to divert RF access in case large portions of interference affect the user experience.

9.1 Use Case

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

9.2 Assumptions

- Each AP, device, node can assess channel conditions and report those to a multi-AP management entity (e.g. Wi-Fi CERTIFIED EasyMesh™, Wi-Fi CERTIFIED Data Elements™ or proprietary variants).
- A multi-AP network embeds a management entity that can reside anywhere (e.g. embedded, edge, cloud ...) that employs a channel allocation algorithm based on data provided by the APs in the network.

9.3 Procedure

1. An end-user adds a series of extender APs to the home network
2. Each extender allocates an initial operational channel based on its own embedded logic or in a variant case, waits for the multi-AP (channel) management entity to assign an operational channel to the extender AP.
3. The multi-AP management entity periodically assesses the channel allocation after installation, based on measurement data provided by the APs in the network.
4. Based on the most recent channel assessment, the multi-AP management entity assigns the optimal operational channel to each of the extenders in the network. The definition of “optimal” shall be a configurable property of the multi-AP management entity.
5. Depending on the logic / algorithm executed by the multi-AP management entity and the capability of the extenders in the network, local (unmanaged) channel assignment may be allowed (e.g. to allow for immediate reaction to sudden interference conditions).

6. If RF conditions change (e.g. interference or OBSS is detected, devices are added or removed), the multi-AP management entity shall react by (potentially) re-assigning the channel allocations in the network (including the backhaul should it be a wireless one).

9.4 Metrics

- When RF conditions change the multi-AP, network re-assigns the operational channel(s) for the extender APs
- The extender APs deliver measurement data that characterizes the current operational channel to a multi-AP (channel) management entity
- The multi-AP management entity shall publish some sort of (periodical) channel allocation report/assessment for the whole network.
- The multi-AP management entity shall allow for updating its channel assignment policy

10 DEP-6 – Adding an AP to an already installed system

An end-user is dissatisfied with the coverage of the (existing) Wi-Fi network in his premises and wants to improve it by seamlessly adding a new AP to the network, in the form of an extender / repeater.

10.1 Use Case

A coverage extender, delivered by an operator, is installed effortlessly in the existing network by an end-user. The extender automatically integrates with the network, allowing deployment of all network services, without the further effort of an end-user. The installation mechanism applied may or may not be a WFA mechanism and as such may or may not be tailored solely to extender installation.

10.2 Assumptions

- The existing network provides a means to pair and onboard new devices, potentially in addition to the mechanisms that provided initial network setup
- At least one pairing mechanism is supported. A pairing mechanism may be a Wi-Fi CERTIFIED mechanism or vendor-proprietary one.
- It is preferable that at least one Wi-Fi CERTIFIED pairing mechanism is supported as this offers the broadest support for pairing.
- Pre-pairing of a new device is not possible
- The installation procedure must accommodate both wired and wireless installation

- In case there is a Broadband gateway in the network, this device is owned / managed by the operator that offers the extender(s).
- Onboarding of a new extender must be seamless and secure

10.3 Procedure

Two scenarios can be identified:

i. An extender is added to an existing extender network. In this network, there are already operational Wi-Fi extenders.

ii. An extender is added to a broadband gateway

The actual pairing / onboarding mechanisms may differ for both scenarios, although it is highly desirable that there is only a single pairing / onboarding flow. The installation flow (if different) must be made clear towards end-users. The onboarding flow must not be ambiguous, and end-user should not have to decide “how” to onboard (e.g. leave the choice open to perform wired or wireless onboarding).

The end-user should power on the extender and follow the predefined onboarding flow.

Several mechanisms exist for pairing extender devices to an existing network, not all mechanisms implement an equal level of security:

- Ethernet-based onboarding (e.g. no authentication)
- Wi-Fi Simple Config
- Wi-Fi Easy Connect™
- Wi-Fi EasyMesh
- Vendor proprietary implementations
    - App-based onboarding (e.g. Easy Connect™ or similar)
    - Maintenance SSID, leveraging on a default credential set
    - Cloud-provisioned onboarding (e.g. Easy Connect™ or similar)
    - Hybrid Ethernet / WSC based onboarding

Once a new extender is successfully onboarded, the end-user must be clearly made aware of the success state. In case there is an error during onboarding, the end-user must be presented with sufficient information to allow the error to be corrected or at least provide meaningful information back to a helpdesk.

An extender that reached the “onboarded” state extends the operator’s service bundle transparently. As such, an end-user establishes an expanded (operator) network instead of a gateway with an additional access point.

10.4 Metrics

- Installation success.
- Wi-Fi performance, before and after the extender is installed.
- Customer satisfaction, before and after the extender is installed.

11 DEP-7 – Detecting and specifying the location of APs

Aid a person installing Wi-Fi extenders to install the devices in a correct location and do so by providing insightful feedback. Next, inform a network owner / operator that the individual placement (location) of the network device can be optimized and provide feedback on how to achieve this task.

11.1 Use Case

A multi-AP network’s performance relates to the location of the individual nodes for each other. A correct installation is imperative to avoid issues later on. To install a network node, an end-user must be guided to the node in a suitable location by an application that assesses the installation quality. When installation has completed, a network “lives” in the environment it is operated in. As such, maintenance and optimisation is required. To achieve this, the end-user must again be guided by a similar if not identical application to reinstall or move some nodes of the network.

11.2 Assumptions

- The network provided by the operator has a means to signal feedback to an end-user about the quality of the location in which a network node has been placed
- Quality is at minimum defined as signal strength but maybe a more elaborate/complex link quality metric
- Network devices are capable of measuring signal strength (e.g. RSSI, RCPI) for example defined in Wi-Fi EasyMesh™ or Wi-Fi Data Elements™

11.3 Procedure - installation

Two scenarios can be identified for installation:

i. A proactive mechanism that leverages out-of-band techniques to position a network node

ii. A reactive mechanism that leverages purely the link measurement abilities of the network nodes

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

An alternative approach is a reactive based location search mechanism where the end-user moves around on the premises, installs the network node and checks if it has been installed in a suitable location by requesting information from a cloud service through an app or by looking at the device’s LEDs that signal the location quality. By iterating through a few locations, an end-user is likely to find a suitable location to install the network node.

11.4 Procedure - optimization

Via the installation guidance, an end-user is usually advised of a good location. This location, with respect to a full network, typically reflects a single dimension in terms of optimal location as only that location is validated, not the full installation of the network.

While the network itself has the ability to perform topology optimization, either by reconnecting backhaul connections differently in tree-type network architecture or routing packets differently in full-mesh network architecture, topology improvement by relocating device is impossible to achieve without end-user interaction.

To further improve the network, periodic reassessment of the network quality is required. Hence, a service capable of assessing network quality/performance can inform an end-user of suggested location-based optimizations. These optimizations can be communicated to the end-user in several ways, ranging from an app to an operator reaching out the end-user directly.

11.5 Metrics

- The effort needed by the end-user to perform the use case.
- Wi-Fi performance, before and after location change.
- Customer satisfaction, before and after location change.

12 DEP-8 – Network loop prevention

Installation of multi-AP networks is not a straightforward task as the goal is to extend the full service of an operator. This requires end-users or installers to be guided to handle this task correctly. However, end-users may not decide the keep the instructed installation. An end-user may have originally installed an AP via a wireless backhaul connection but decides they have too many problems with it and installs an Ethernet backhaul connection to overcome issues with the wireless backhaul. This action can create a network loop that can break the whole network instead of improving it.

12.1 Use Case

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

A Multi-AP network, as such must be able to “handle” network loops to allow end-users the freedom to install the network as they see fit while maintaining control over the network.

12.2 Assumptions

- Every AP in the network has the ability to detect a loop from being created (e.g. by monitoring the 802.1Q bridge traffic).
- Every AP in the network has the ability to break a network loop by the implementation of a loop prevention algorithm based on a standard (e.g. STP, RSTP, TRILL ...) or a proprietary mechanism (e.g. master/slave path blocking).
- Loop breaking can either be done by physically disconnecting an interface or by preventing multicast/broadcast traffic from being sent via an interface.

12.3 Procedures

The procedure is straightforward, a network that consists of a single Broadband GW (with Ethernet-LAN interface and Wi-Fi interface) is extended by installation of an additional AP. The AP is connected both via Wi-Fi and Ethernet to the Broadband GW, perhaps in a specific order. The GW-bridge and the (extender)AP-bridge run their loop prevention algorithm and decide to block one of the interfaces.

The end result is that none of the network nodes “die” and that, for example, client devices connected to Wi-Fi can still communicate with each other or the internet.

12.4 Metrics

- The network remains operational after installation of extra backhaul connections, irrespective of how many are installed
- The network does not suffer any significant degradation from increased loop traffic
- Reaction time of the algorithm

The speed with which the algorithm reacts is a metric. The reaction speed could be deemed to be annoying and hence might have to be less than a perceivable threshold (e.g., less than 30 seconds).

OPERATION USE-CASES

13 OPS-1 – Self-healing for fixing channel interference issues

When the home network’s environment changes, either through interference or congestion from new neighboring networks, it may become necessary to reallocate the channels on which the network operates. This process typically uses the same functionality as in DEP-5 – Channel allocation / , with the addition of information about the environment that has been gathered during operation.

13.1 Use Case

A nearby existing network changes channel, increasing the level of interference and congestion on the home network. The home network takes action to mitigate this.

13.2 Assumptions

- The home network is able to change channel once configured.
- The channel change will be based on the history of channel, interference and contention information collected during operation.

13.3 Procedure

See DEP-5 – Channel allocation /

13.4 Metrics

- Before-and-after measures of interference and contention. The number of channel changes over time (minimise).

14 OPS-2 – Preventing orphaned APs

Use case covers changing a network's credentials (security and/or network name) while trying to prevent wirelessly backhauled APs from dropping off the network or from having to be manually re-onboarded.

14.1 Use Case

The end-user or managing operator at the request of the end-user wishes to change the security credentials and/or the name of the existing wireless network being served by a multi-AP system (with one or more APs using a wireless backhaul), likely with attached clients.

After the change, both the end-user and the operator want the following to be true:

1. All of the APs in the system to still be connected to each other
2. All of the APs in the system to be running with the new network credentials and configuration
3. During the reconfiguration, it is OK if the Wi-Fi is not operational
4. After the reconfiguration, a notification should state that the change is complete
5. Notify the end-user and operator of any APs and STAs that are no longer attached after the procedure.

The end-user would like most of the currently attached STAs to remain attached, but they are changing the credentials because they suspect there is one unauthorized STA, so they are OK if they have to reconnect each STA.

14.2 Assumptions

- The multi-AP system is currently configured and running
- STAs attached to the system will not be attached after the change
- End-user/Operator has a method to reconfigure the network

14.3 Procedure

Follow reconfiguration procedure provided by the system

14.4 Metrics

- Number of orphaned APs after the procedure
- Number of APs operating with the new network name and credentials
- Time system needs to complete the reconfiguration
- Are there notifications (to the end-user and operator) that the reconfiguration is complete.

15 OPS-3 – Handling orphaned APs

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

15.1 Use Case

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

15.2 Assumptions

- A Multi-AP network must provide a manual way for an orphaned AP / network node to be re-onboarded to the network. Some of these techniques have been discussed in DEP-6.
- An orphaned AP / network node has been successfully connected to the network at some point in time. It is as such NOT a new device.
    - The orphaned AP / network node may have a set of “recovery” credentials to re-onboard

- A Multi-AP network may provide an automatic way for an orphaned AP / network node to be re-onboarded to the network. Some of these techniques rely on a standard (e.g. Wi-Fi CERTIFIED Easy Connect™™) or are vendor proprietary (e.g. dedicated onboarding BSSID, dedicated key ...)

15.3 Procedure

A Multi-AP network updates backhaul credentials while one of the AP / network nodes is powered down.

After the update, an end-user can access the internet and services offered by an operator as usual.

The end-user enables the previously powered down AP / network node and either is notified that the AP / network node cannot get connected to the network anymore (e.g. via an app or via LEDs) or the end-user does not notice anything as the AP / network node self-heals itself and re-onboards with the network.

In case there is no automatic recovery procedure, the end-user must be notified to take action via the regular tools with which the end-user manages its network or gets network notifications (e.g. app, LEDs).

15.4 Metrics

- The network should indicate that there is an orphaned AP / network node – existing node is not operational. Note that this may “just” be just an AP / network node that has broken down, was replaced ... An end-user may be asked to indicate the true status of an orphaned AP / node (e.g. ignore the info, delete the removed node, or mark it as orphaned).
- The network may self-heal and choose to notify the end-user
- Final State: The network “just” works when an orphaned AP / network node is either self-healed or manually healed, and the AP is onboarded to the network/controller.

16 OPS-4 – Handling and detection of unmanaged APs using same SSID as the managed network

Managed (residential) networks may suffer from the installation of an unmanaged extender AP as this allows client devices to get “trapped” in a segment of the network that likely does not offer the same QoE as the rest of the network. Such an AP is labelled as “rogue” AP.

16.1 Use Case

ISP or network operators are challenged by their customers to deliver the same service and QoE level throughout the home. It has been established that to achieve that, extenders or extender APs are required next to the broadband gateway in certain installations. Network operators invest a lot of time and money in guaranteeing full home coverage of their services by ensuring that all nodes in the in-home network deliver the offered services in a similar way. As such, all of the nodes in the in-home network are managed by the operator offering the broadband services. If end-users for some reason (e.g. cost) install standalone APs with identical network credentials, they create unmanaged and network segments in which an operator can no longer guarantee or a least try to deliver a certain level of QoE. End-users however, do not fully grasp the issue they are creating and hence still hold the network operator responsible whenever there are network QoE issues, even with rogue/unmanaged extenders installed. To try and correct such scenarios, a (managed) multi-AP network shall have the ability to identify these unmanaged or rogue network segments and where possible come up with a solution

16.2 Assumptions

- An operator managed entity is present in the multi-AP network that manages the multi-AP network.
- An operator or an operator managed entity/device in the network can learn or identify other operator managed devices. There must be a ground truth.
    a. For example, there could be a 2nd stage of onboarding where device certificates are exchanged/verified
    b. For example, an operator may require all of the devices to identify themselves via TR069 – active inform
- An operator managed entity/device in the network can perform a network discovery method (e.g. 1905.1 based, ARP based, DHCP based ...)

16.3 Procedure

1. The entity that manages the multi-AP network runs periodical identification of all network nodes present in the network.
    a. Based on the identification mechanism, a list of device MAC addresses can be collected.
    b. MAC addresses present in the network can be collected via several methods (e.g. WLAN network scan, 1905.1 device discovery, DHCP, ARP ...)

c. These MAC addresses can be correlated with MAC addresses used in the network (e.g. OUI match or full MAC address match considering that some MAC address may be a “variant” of the one that is allowed in the network such as the next iteration or a locally administered variant thereof)

2. If a rogue device is detected, the network management entity shall apply the operator managed / configured action.

   a. Actions can range from notifying the operator of the presence of a rogue AP, notifying the end-user of the presence of a rogue AP and finally block the traffic to/from such an AP.

16.4 Metrics

- A multi-AP management entity must be able to detect and report (in some way) the presence of rogue AP

17 OPS-5 – Client steering

The use case consists of testing client and AP steering behavior in a dual-band homogenous network. Both band and AP steering are tested.

17.1 Use Case

When devices move about the home the end-user and operator want each client device to roam/be steered to the best AP/band. This usually means the band/AP that reduces the airtime utilization for that client device.

17.2 Assumptions

- Dual-band (2.4 and 5 GHz) network with common SSID
- Each AP will have both 2.4 and 5 GHz radios
- For band steering – client is dual-band capable

17.3 Procedures

17.3.1 Single AP band steer procedure

1. Place client near (e.g., 2-meters from) the AP
2. Start capture mechanisms
3. Associate client to Network (letting it pick the band)

4. Start traffic stream to/from client
5. If client chose the 5 GHz band, attempt to steer the client to the 2.4 GHz band
    a. Method 1: move the client away from the AP
    b. Method 2: use the multi-AP solution's control to steer the client
6. If client picked the 2.4 GHz band, attempt to steer the client to the 5 GHz band
    a. Method 1: move the client closer to the AP
    b. Method 2: use the multi-AP solution's control to steer the client

17.3.2 Multi-AP AP steer procedure

- Place APs (2 to 4 total) according to solution's recommendation
- Place client near (e.g., 2-meters from) one AP
- Start capture mechanisms
- Associate client to Network (letting it pick the band and AP)
- Start traffic stream to/from client
- Attempt to steer the client to each of the other APs setup
    - Method 1: move the client at slow walking speed to near (e.g. within 2 meters of) another AP, wait 3 minutes for client to roam/be steered. Repeat with all remaining APs.
    - Method 2: While using method 1, use the solution's mechanism to attempt to steer the client to the new nearest AP

17.4 Metrics

- Client's association behavior
- Client's Rx/Tx RSSI/SNR/PHY rate of beginning and ending BSSs
- APs' messaging to the client during steering attempt along with APs' SNR/RSSI of client
    - 11kvr used?

18 OPS-6 – Coordinated firmware upgrade

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

Upgrading multiple devices is always tricky and requires some form of management/coordination. How complex the management function needs to be is typically influenced by properties of the APs / network nodes (e.g. dual-image storage) or the network topology (e.g. tree vs. star vs. graph).

Operators must consider that there is a network-wide upgrade procedure that ensures that ALL APs / network nodes get upgraded without risking losing devices, with minimizing the network downtime, etc.

18.1 Use Case

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

18.2 Assumptions

- There is an application either centralized in the network or in every AP / network node that is able to download new firmware.
- This mechanism should be secure, but that is outside of the scope of the use case
- There is either a centralised or decentralised protocol that coordinates when and if a firmware update can be executed. An updated protocol may be based on standards (e.g. SNMP, TR-069, Wi-Fi CERTIFIED Data Elements™) or a vendor-specific protocol.
- The update protocol checks various parameters (e.g. network busyness, topology) before triggering the update procedure.
- The update protocol controls which AP / network node updates, this can be sequential or all at once.
- All APs have the capability to be upgraded or will continue to work in a non-homogeneous firmware environment.

18.3 Procedures

A Multi-AP network is operational.

A new firmware image is presented either to a cloud server or a remote management server. Or a new firmware image is presented to a (network) GUI.

The update management function of the Multi-AP network will determine the right moment and sequence to update the APs / network nodes.

If there is, for example, a lot of network traffic, the update may be postponed or aborted. This may be signaled back to the end-user or update process.

If all conditions check out, the update management function triggers an update in accordance with the strategy of the update algorithm to ensure minimal downtime of the network.

18.4 Metrics

- All APs / nodes of the network update, reboot and come up with the new firmware
  - This is displayed in an AP's GUI or app or remote management GUI
- Downtime of the network is considerably less than when an off-line, manual update of each node is performed
- The update procedure is deferred when traffic is present to minimize the end-user impact.

19 OPS-7 – Network topology control/optimization

Multi-AP networks have to cope with several issues that span from the multi-AP nature. OPS-1 already discusses the need to react to changes in the RF conditions when operating a Multi-AP network. However, another important aspect that requires a form of self-healing and this relates to topology changes. Multi-AP networks have to handle APs/network nodes that are switched on/off or backhauls that break due to severe deterioration of the RF environment.

While Multi-AP networks may receive topology guidance from a cloud or remote management system, this guidance is not a real-time as it requires "some" data to converge to an optimal Multi-AP topology. When however there are instantaneous topology changes. The Multi-AP network must have the minimal ability to re-form itself to a pseudo-optimal topology first before being fully optimized via remote management techniques in a later phase.

19.1 Use Case

Multi-AP networks must handle dynamic topology changes. End-users frequently switch off/on devices, backhaul links deteriorate, etc. A Multi-AP system must have a minimum viable logic

to re-form the network in such a way that the overall performance remains acceptable to the end-user.

19.2 Assumptions

- A Multi-AP network implements a centralized or decentralized topology assessment and control function
    - The function may be based on standards (e.g. Wi-Fi CERTIFIED EasyMesh™ or IEEE 1905.1[a]) or on a vendor-specific mechanism
    - The function may have a visualization component to illustrate the current network topology for the end-user
- The topology assessment and control function applies a metric to allow comparing network topology “quality”
- The topology assessment and control function reacts instantaneously to a change in topology
- All APs / network nodes support functions to reconnect their backhaul connection, provided this backhaul connection can be re-connected somewhere else
- All APs / network nodes have credentials to re-connect backhauls

19.3 Procedures

A Multi-AP network is operated in a typical tree topology.

- Broadband GW → AP1/network node 1 → AP2/ network node 2
- AP1 is switched off
- verify that AP2 connects with the Broadband GW seamlessly but the backhaul speed has severely decreased
- AP1 is switched on
- verify that AP2 re-connects with AP1 iso remaining connected via a reduced connection to the Broadband GW.

Connect a STA to AP2 and check the overall throughput during the tests. When AP1 is disabled, the throughput should degrade, but once AP1 is enabled, it should remount to its original level.

19.4 Metrics

- STA performance
- Network topology overview

MANAGEMENT AND DIAGNOSTICS USE-CASES

20 MAN-1 – App provided to end-user.

An application (app) is installed on a smartphone which provides Wi-Fi information to consumers and possibly also allows some configuration such as station association control.

20.1 Use Case

The app is used in a multi-AP network. The app provides visibility into available Wi-Fi connections and the quality of the current Wi-Fi connection. The app may be accessed directly by the consumer who can then overview their Wi-Fi network, and the app may also connect to a mobile service provider who can then gain visibility into Wi-Fi offloading performance.

20.2 Assumptions

- A home has a multi-AP network.
- An app can be downloaded and installed into a smartphone.
- The app can assist with managing the multi-AP network.
- The app has a GUI accessible by a user.
- The app can provide data about the multi-AP network, such as performance, topology, connected STAs, and analysis results.
- Optionally, the app may also provide some control or configuration capabilities, such as channel change.
- Optionally, the app may also connect over the mobile network to a management system for a mobile service provider.

20.3 Procedure

1. The app is installed on a Smartphone.
2. A user accesses the app to manage the Multi-AP network.
    a. There should be multiple such interactions.
    b. Optionally, control or reconfiguration is performed via the app.

3. Optionally, the app connects over the mobile network to a management system.
    a. The app provides diagnostic data to the mobile management system.
    b. Optionally, control or reconfiguration of the multi-AP network is performed from the mobile management system through the app.

20.4 Metrics

- Usage; how much do the consumers actually use the app.
- Customer satisfaction, with and without the app.
- Data provided by the app.
- Control or reconfiguration that is possible through the app.

21 MAN-2 – Proactive diagnostics and analytics by the operator.

Multi-AP systems are monitored by the Operator and reconfigured to improve service.

21.1 Use Case

Premises with installed and running multi-AP systems are monitored by providing diagnostics to a remote management system. Diagnostics data may be in Wi-Fi CERTIFIED Data Elements™, Broadband Forum TR-181, or other data models. The quality of the delivery of broadband service through the Wi-Fi is monitored, as is the STA performance. Errors in the operation of the multi-AP system are counted, such as APs that are not onboarded to the multi-AP system, and unnecessary station disassociations. The diagnostics data can be analyzed, compared to historical data, and used to estimate QoE. Wi-Fi and broadband access speeds can be measured and compared to find bottlenecks.

Poor Wi-Fi coverage within a premise may be identified automatically by a management system. This may then invoke DEP-6 – Adding an AP to an already installed system, or DEP-7 – Detecting and specifying the location of APs.

21.2 Assumptions

- A management system can connect across a WAN to a multi-AP controller, gateway, AP or similar device.
- The management system is capable of remotely monitoring the multi-AP system and providing diagnostics data.

21.3 Procedure

1. The management system connects across a WAN to a multi-AP controller, gateway, AP or similar device(s).
2. The management system collects data from the multi-AP controller, gateway, AP or similar device(s).
3. The management may perform analyses to distil data, perform fault correlation, determine root cause, etc.
4. The diagnostics data and analyses results are read from the management system
    a. Diagnostics data and analysis results should be read under varying conditions and times.

21.4 Metrics

- Service quality diagnostics such as speed, connectivity, latency, and coverage per premises and across the entire operator's network.
  Possibly also comparisons to historical data and derived QoE estimates.
- Counts of errors such as reboots, onboarding failures, association failures.
- Broadband speed versus Wi-Fi speed
- STA performance measurements taken from Data Elements
- Counts of service disruptions due to multi-AP station steering or channel steering.
- Ability to identify premises with chronic coverage issues.
- Customer satisfaction, with and without multi-AP.

22 MAN-3 – Topology management by the operator.

Multi-AP systems are monitored by the Operator and reconfigured to improve service.

22.1 Use Case

Wi-Fi performance of each end station in a multi-AP network is affected by the topology of the multi-AP network, such as the selection of backhaul links from the agents/APs to the controller/WAN. Topology information is useful for diagnosing if a particular device such as a set-top box is connected properly. A topology map can be useful for showing multi-AP configurations. Topology optimization and backhaul steering should improve the multi-AP topology, but it may not work optimally and could cause service interruptions.

22.2 Assumptions

- There is a multi-AP network which can report topology information such as which other devices are connected to a given device in the network.
- Device identification may also be provided.
- There is a system which can provide such information across the multi-AP network.
- The topology of controller, connected APs, backhaul, stations, etc. should be provided.
- There is a way to read this data, possibly in a graphical form.

22.3 Procedure

1. A system which can gather topology data from the multi-AP system is either connected, installed or is already in a multi-AP network.
2. The system may run locally or remotely.
3. Topology data is read from the system.

   a. The topology should be varied, with the data then re-read.
5. A graphical display of the topology is optionally supplied.
6. Device ID is optionally supplied

22.4 Metrics

- End-to-end Wi-Fi throughput; before and after backhaul steering.
- Topology views.
- Device identification.
- Counts of topology re-arrangements.
- Counts of service disruptions due to backhaul steering.

23 MAN-4 – Onboarding devices to an Easy Connect™ (DPP Initiator-Configurator) AP.

The home network Service Provider provides a Smartphone App that allows the user to manage devices and access (e.g., guest access, parental controls) on a DPP enabled AP. The app is used to add DPP-enabled APs and clients, including IoT clients, to the home network.

23.1 Use Case

The home network Service Provider provides an Access Point that is a DPP Initiator - Configurator so that the home network is not reliant on a single user device for onboarding.

It also provides a Smartphone App; running on one or more smartphones; that allows the user to manage device onboarding and access (e.g. guest access, parental controls) on a DPP enabled AP. The app is used to add DPP-enabled APs and clients, including IoT clients, to the home network.

23.2 Assumptions

- The Configurator in the home network should be the AP because of the risk of reliance on the Configurator being a single (physically vulnerable) mobile device.
- A mechanism can be provided that will enable the AP to trust the device running the management App.
- A means of transferring the Configurator role to a replacement AP can be established (just as would be needed if a Smartphone were the Configurator).

23.3 Procedure

1. A user's client device (Smartphone) installs an App from the SP to manage the home network.
2. The Smartphone is onboarded to the AP (perhaps using DPP Initiator-Enrolee). It then performs an additional trust step to allow the AP to trust the identity/user of the device.
3. The Smartphone App communicates with the AP to receive information about nearby devices and allow the user to determine which DPP-enabled devices in the neighborhood should be onboarded.
4. The device App provides information to the AP (such as a scan of a barcode on an IoT device) and instructs the AP to initiate a DPP enrolment with the identified new device.
5. The new device is onboarded and returns appropriate status messages to the AP (see DEP-2).

23.4 Metrics, Observation or Considerations

- Successful onboarding of devices.
- Successful use of the management App by a second smartphone to onboard further devices.

LINKS

Globe Electric Wi-Fi Smart Plug

https://globe-electric.com/en/product/globe-electric-wi-fi-smart-plug-no-hub-required-white50114/

Teckin SP10 Smart Plug

https://www.teckinhome.com/copy-of-sp-22-1

Leviton DW15P-1BW Smart Plug

https://www.leviton.com/en/products/dw15p-1bw

Amazon Wi-Fi simple setup process

https://developer.amazon.com/docs/frustration-free-setup/understand-wi-fi-simple-setup.html

Globe Electric App

https://play.google.com/store/apps/details?id=com.globe.electric&hl=en_CA

Teckin App

https://play.google.com/store/apps/details?id=com.tuya.smartlife&hl=en_CA

Leviton App

https://play.google.com/store/apps/details?id=com.leviton.home&hl=en_CA

DOCUMENT HISTORY

VERSION	REVISION DATE	REVISED BY	DESCRIPTION OF CHANGE
1.0.0	24/04/2020	Tim J Twell (BT)	Formal approval for release

PARTICIPANT LIST

NAME	COMPANY	ROLE
John Bahr	CableLabs	Project Leader
Koen Van Oost	AirTies	Project Co-Leader
Tim Twell	BT	Project Co-Leader & Chief Editor
Ken Kerpez	ASSIA	Editorial Team
Simon Ringland	BT	Editorial Team
Hai Shalom	Google	Editorial Team
Preston Huang	Rogers	Editorial Team
Pedro Mouta	WBA	Editorial Team
Feng Wang	AT&T	Project Participant
Lawrence Masike	BOFINET	Project Participant
Thomas Derham	Broadcom	Project Participant
Chris Beg	Cognitive Systems	Project Participant
Stella Loh	Google	Project Participant
Djamel Ramoul	iBwave	Project Participant
Max Riegel	Nokia	Project Participant
Randy Sharpe	Nokia	Project Participant
George Hart	Rogers	Project Participant
Juan Pablo Ginocchio	Telecom Argentina	Project Participant
Bruno Tomas	WBA	Project Participant
Sarah Markham	WBA	Project Participant