April 2021

ONBOARDING AND PROVISIONING AUTOMATION FOR MESH ACCESS POINTS

Vincent Cuissard

Samuel Pasquier

Alessandro Erta

Luca Bisti

Amine Choukir

See next page for additional authors

Inventor(s)
Vincent Cuissard, Samuel Pasquier, Alessandro Erta, Luca Bisti, Amine Choukir, and Domenico Ficara

ONBOARDING AND PROVISIONING AUTOMATION FOR MESH ACCESS POINTS

AUTHORS:
Vincent Cuissard
Samuel Pasquier
Alessandro Erta
Luca Bisti
Amine Choukir
Domenico Ficara

ABSTRACT

Mesh networks can be implemented in many different scenarios in which direct cabling of access points may not be practical or may not make financial sense. For example, in Internet of Things (IoT) deployments, access points may be located far from each other with very limited physical access. Presented herein are techniques to leverage hardware and software features available on mesh access points to avoid manual configuration in the field.

DETAILED DESCRIPTION

It can be difficult to provide direct cabling for wireless access points (APs) within many mesh network environments due to cost and/or practical implications. One environment in which mesh networks are especially relevant involves IoT deployments. In an IoT environment, APs can be located far from each other with very limited physical access. For example, some APs may be several kilometer/miles away from each other and can involve hours to days to reach and are usually not reachable by knowledgeable Information Technology (IT) personnel. This implies that, once installed, the expectation is that equipment is to involve no/very little manual intervention and has to work over its expected lifetime in such a way. Any failure (e.g., a configuration mistake, etc.) can be critical and can require physical access to AP(s).

This proposal provides techniques to leverage hardware (HW) and software (SW) features available on mesh APs to avoid manual configurations of such devices in the field. In particular, a mesh access point is able to switch from an AP operating role to a station (STA) role when not configured. Broadly, techniques herein involve a "Provisioning Mesh

AP service" that can be provided by operating mesh nodes through Access Network Query Protocol (ANQP) or a dedicated Service Set Identifier (SSID) in order to onboard non-configured mesh nodes. Non-configured mesh nodes can be configured to search for the "Provisioning Mesh AP service" on any available Wi-Fi network (or dedicated SSID). Once connected to the service, the non-configured nodes can communicate with a Plug-and-Play (PnP) server to obtain their configuration and can then switch to the operating mode once their configuration is complete. Each time a new mesh node is configured, it automatically increases the provisioning coverage area.

Consider various devices and terminologies that can be utilized to facilitate techniques of this proposal.

- RAP: Root Access Point - This is an access point with a wired uplink (to facilitate reachability to a Wireless Local Area Network (LAN) Controller (WLC) / wider network) and a wireless downlink (to facilitate wider network / WLC reachability to children)
- MAP: Mesh Access Point - This is an access point with wireless uplink (to facilitate reachability to WLC / wider network) and a wireless downlink (to facilitate wider network / WLC reachability to children)
- PnP server: Server that implements a PnP procedure to provide device onboarding for Day-0 / Day-1 processes. In some instances, a network orchestrator or network manager may implement PnP server functionality.

In order to leverage the HW/SW features available on mesh access points in order to avoid manual configurations in the field, each operating MAP/RAP will broadcast a provisioning SSID. When a RAP first boots after Day-0, it will be able to join the WLC, thus starting its RAP role. When a MAP first boot after Day-1, it will start scanning for the provisioning SSID. When available, the MAP will join this provisioning SSID as a wireless client and will be able to talk with the PnP server. The PnP server will then send the MAP its full configuration and the MAP will reboot and start its MAP role.

By utilizing the techniques of this proposal, all the MAPs/RAPs will get their Day-1 configuration automatically. Of course, a provisioning convergence time may be observed, especially for MAPs that are mesh-tree-leaves, since all the parent MAPs are the

first to be Day-1 provisioned. For cases of configuration or operating mode failures, MAPs can automatically, after a configuration timer, restart the Day-1 phase operations in order to fetch a new configuration (e.g., degraded mode, radio slot update, etc.).

Regarding onboarding security, techniques herein do not mandate the use of Open SSID, although the use of Open SSID is not precluded by the techniques of this proposal. In the case of a Pre-Shared Key (PSK) or Dot1X SSID implementation, credential material can be provisioned in a staging area before equipment deployment in the field and especially in remote areas. This would secure the link between non-managed mesh nodes and the current provisioned mesh infrastructure. In some instances, credential material could also be provided as part of the staging configuration and not part of the PnP configuration such that it cannot be lost upon Day-0 – Day-n workflows. It should be noted that network access control methods such as Media Access Control (MAC) Address Bypass (MAB) can be used so that every device can be whitelisted on an Authentication, Authorization, and Accounting (AAA) server.

Figure 1, below, illustrates an example operational flow involving Day-0 operations.

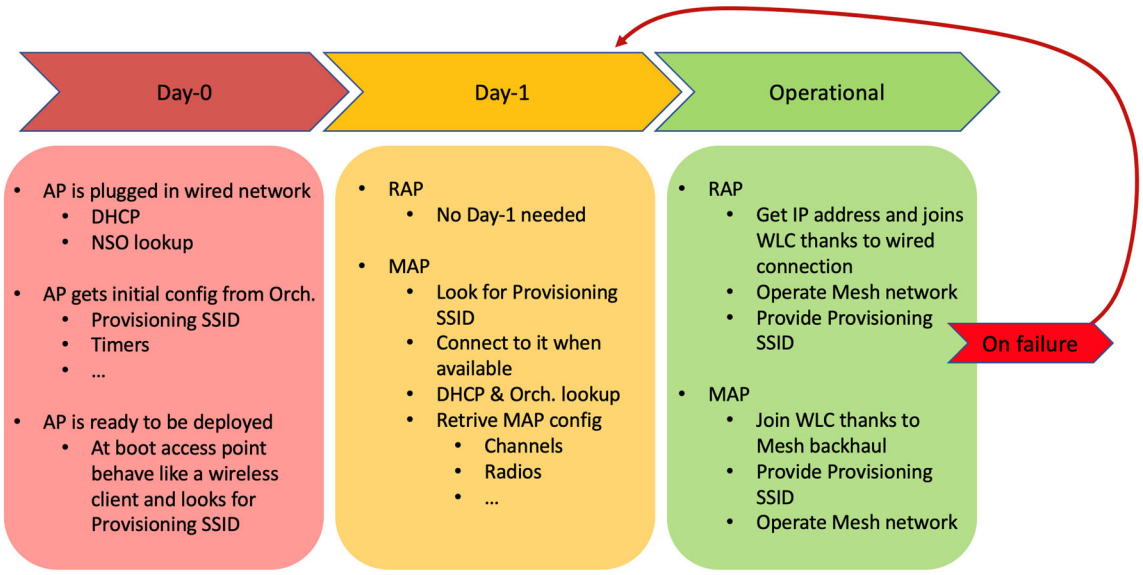

Figure 1: Example Operational Flow Involving Day-0 Operations

Figure 2, below, illustrates another example operational flow for instances in which Day-0 operations can be skipped if defaults are good enough.

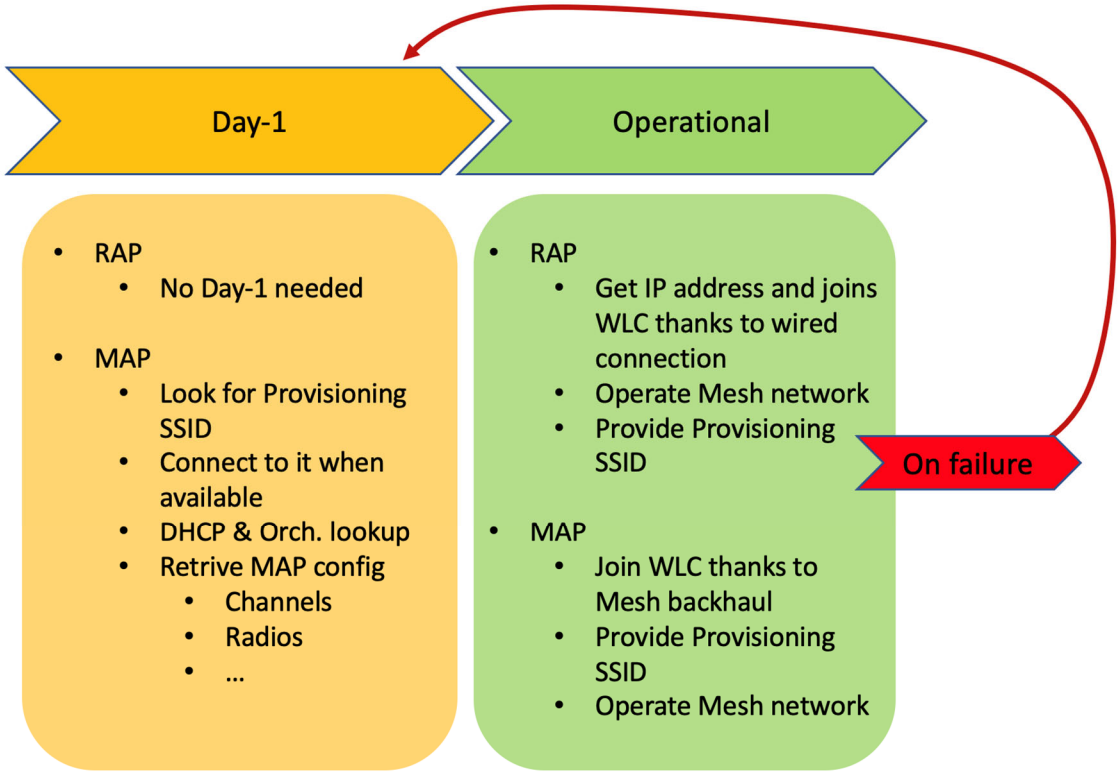

Figure 2: Example Operational Flow Skipping Day-0 Operations

For the example operational flow as illustrated in Figure 2, consider that, out of the factory, all mesh access points can, after a Dynamic Host Configuration Protocol (DHCP) timeout, switch to the provisioning wireless client mode and start scanning for the Provisioning Mesh Access Point service (e.g., via ANQP). If such service is provided by an open network (or a Hotspot network), the mesh access point can join the network and start the PnP procedure with a PnP public server. The PnP public server will then proxy to a private PnP server based on MAC entries (e.g., global account), as is typically performed for switches and routers. Using a Hotspot network provides for the ability to alleviate an open network, which may provide added security/authentication during Day-1 operations, if needed. In some instances, technologies such as OpenRoaming can be leveraged to facilitate authentication.

Utilizing the techniques as illustrated in Figure 2, a MAP can obtain its Day-1 configuration from its mesh network or any other network that provides a Provisioning Mesh AP service over an open network (or a Hotspot network). In some instances, it is

even possible to expose such a service from a smartphone to speed up the Day-1 configuration of equipment after its installation.

Regarding Day-2 and subsequent Day-n operations, the PnP server is only used to bootstrap Day-0 and Day-1 configurations, whereas Day-2, etc. configurations can be handled by a WLC. For instances in which a device is misconfigured, the device can restart in a bootstrap mode and perform Day-1 operations again to obtain its configuration.

Consider a deployment flow, as discussed in further detail through Figures 3–7, below for the operational flow involving Day-0 operations, as shown in Figure 2, above. The deployment flow shown below is similar to the operational flow that does not involve Day-0 operations, however, such a flow would further involve integration of a public PnP server. The deployment flow shown below in Figures 3–7 involves a network orchestrator, nevertheless, techniques herein can also be implemented in other PnP solutions.

To begin, consider that a customer receives RAPs and MAPs from a manufacturer such that the Day-0 configuration is to be performed. In this example, the customer creates entries in the network orchestrator database based on device MAC addresses and applies the requested classification (RAP, MAP, etc.). The network orchestrator will update the Remote Authentication Dial-In User Service (RADIUS) authentication server/WLC to allow the MAC addresses of the devices. The devices can then be deployed in the field to await Day-1 configuration, as shown below in Figure 3, in which all the RAPs are awaiting wired Internet Protocol (IP) addresses (via DHCP) and the MAPs are in the wireless client mode looking for the "Provisioning SSID."

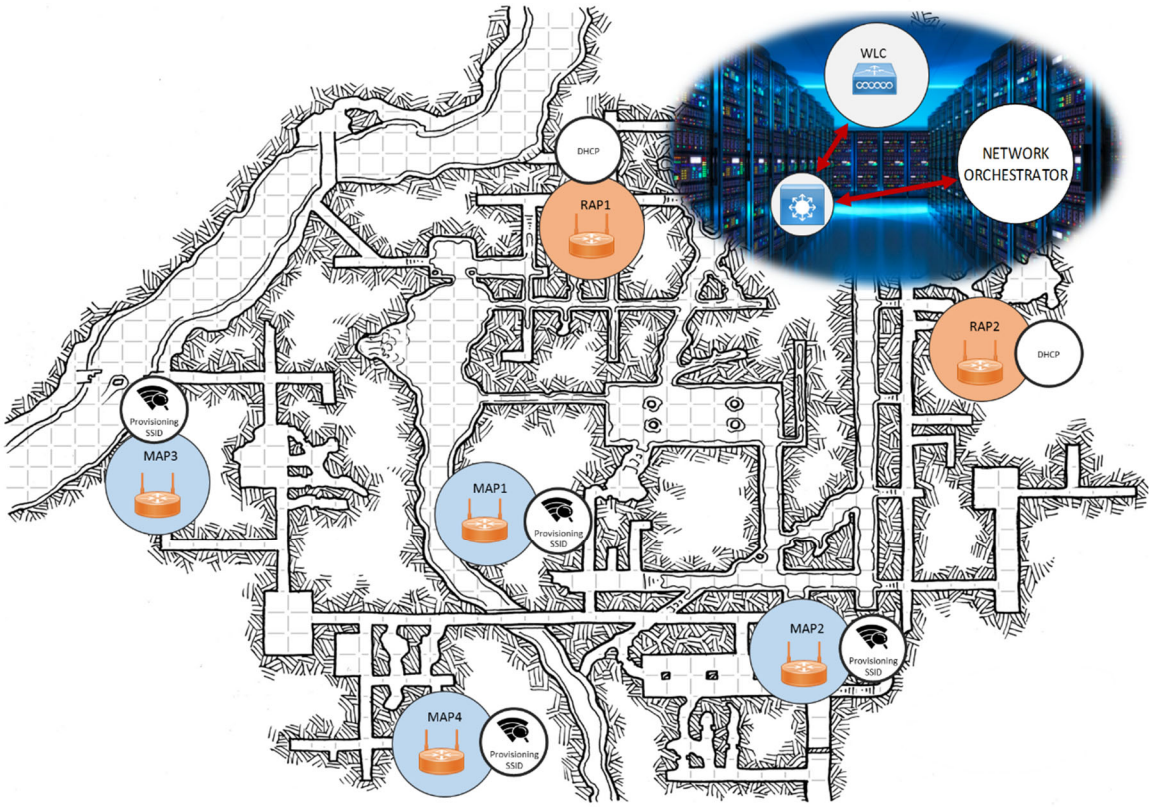

Figure 3: Example Day-1 Deployment

Next, as shown in Figure 4, consider that the RAPs have received their IP addresses, joined the WLC, and the WLC has configured the RAPs such that they are operating the mesh network (e.g., providing backhaul and client access) and broadcasting the "Provisioning SSID" in order to onboard new mesh nodes.

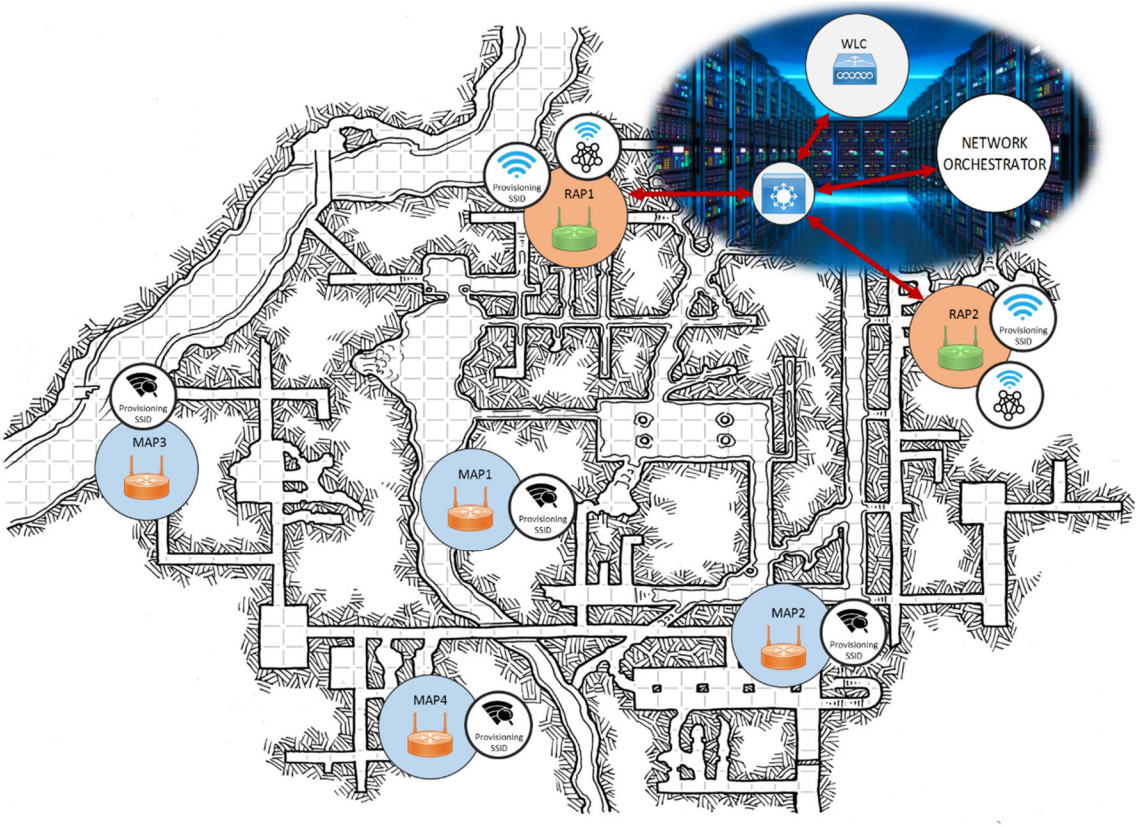

Figure 4: RAPs Broadcast "Provisioning SSID"

As illustrated in Figure 5, below, some of the MAPs start Day-1 phase operations such that MAPs that are in the wireless coverage of RAPs (e.g., MAP1 and MAP2) are able to join the "Provisioning SSID," obtain their IP addresses, and start the Day-1 operations with the network orchestrator.

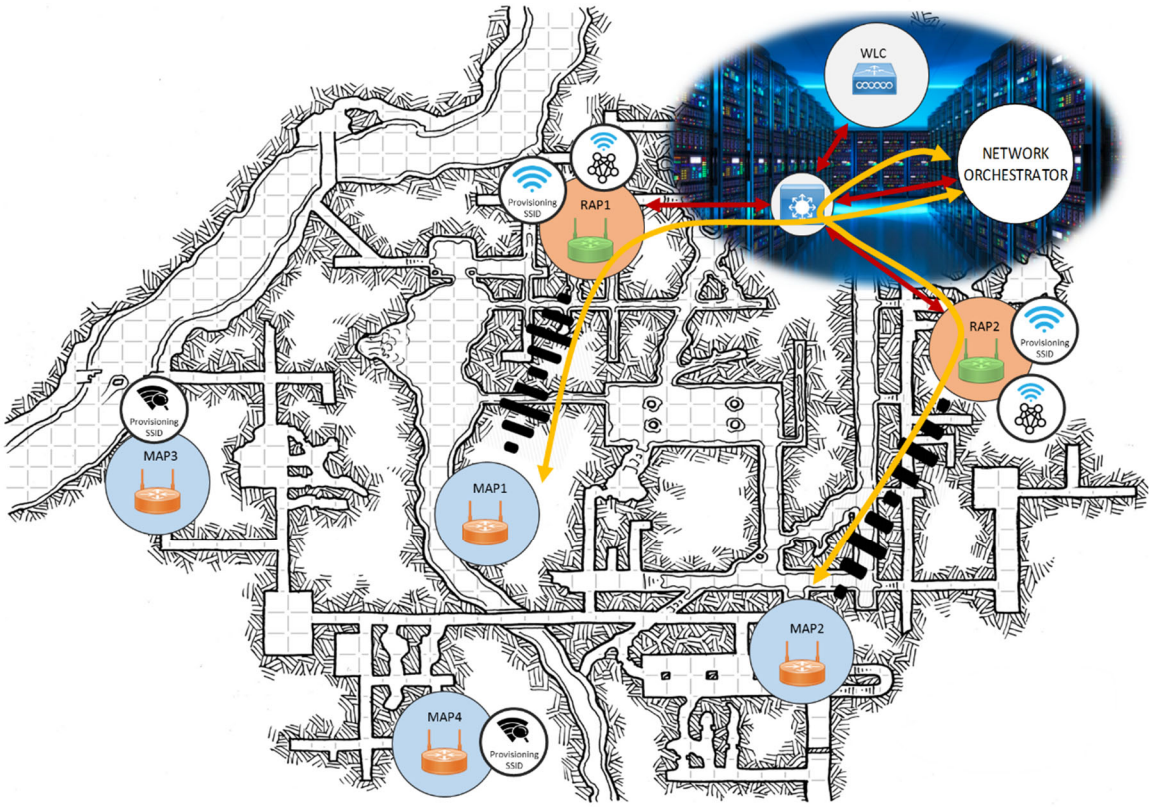

Figure 5: Day-1 Phase Operations for MAP1 and MAP2 within Coverage of RAPs

Thereafter, MAP1 and MAP2 are operational such that they join the WLC (through the wireless mesh backhaul) and are operating in the mesh network (e.g., providing backhaul and client access) and broadcasting the "Provisioning SSID" in order to onboard new mesh nodes. For example, MAP3 and MAP4 are now able to join the "Provisioning SSID" and start their Day-1 phase operations, as shown in Figure 6, below.

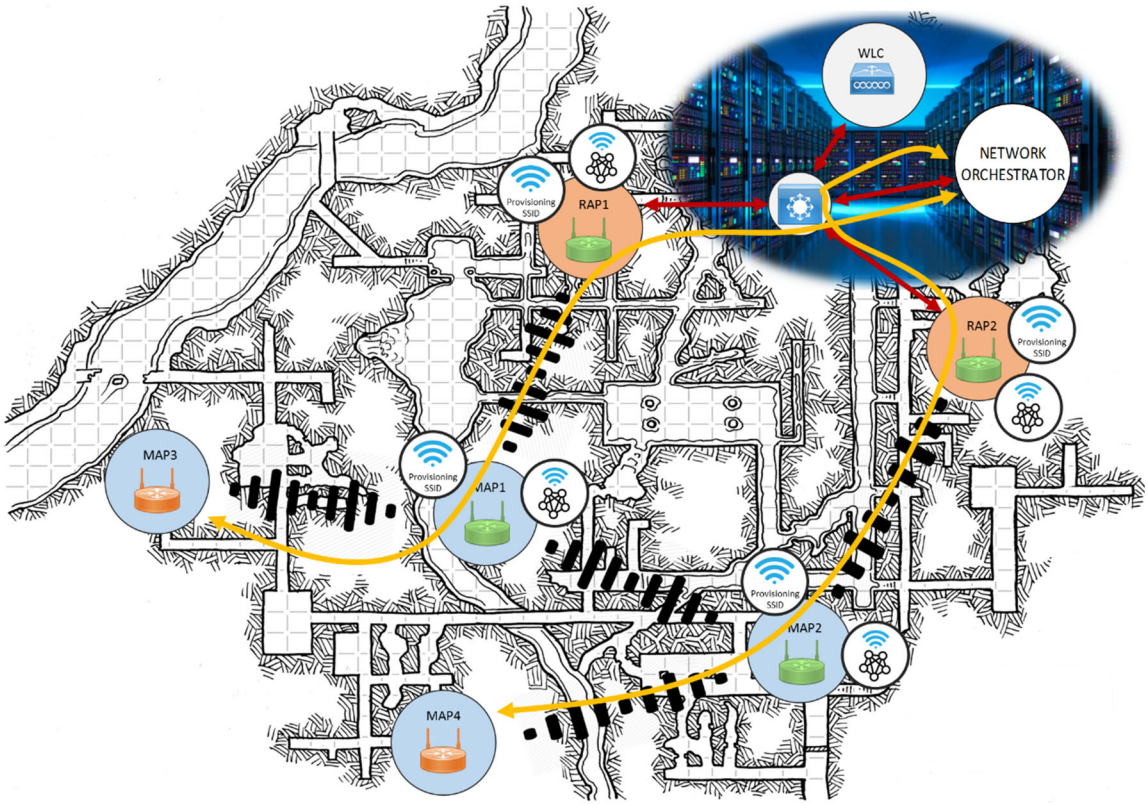

Figure 6: Day-1 Phase Operations for MAP3 and MAP4

Following completion of the Day-1 for MAP3 and MAP4, the network is operational, as illustrated below in Figure 7.

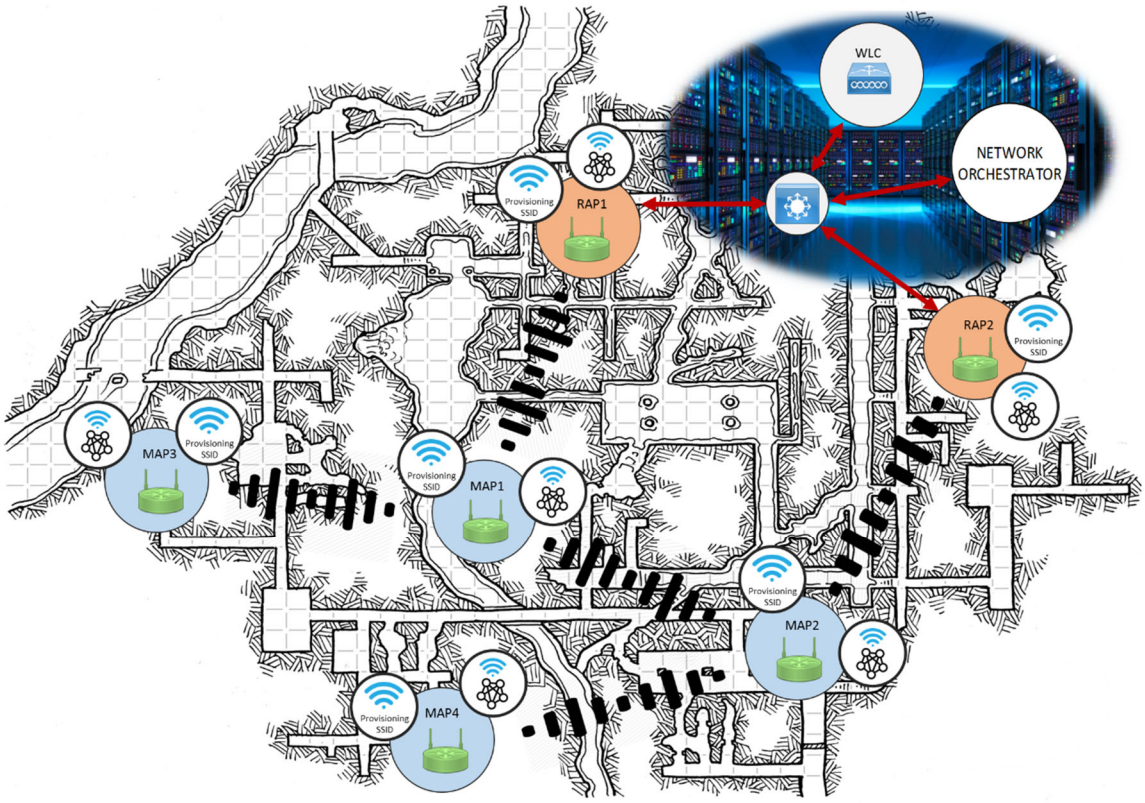

Figure 7: Network is Operational

In summary, techniques herein facilitate a "Provisioning Mesh AP service" that can be provided by operating mesh nodes through ANPQ (or dedicated SSID) to onboard non-configured mesh nodes. Non-configured mesh nodes look for "Provisioning Mesh AP service" on any available Wi-Fi network (or dedicated SSID). Once connected, the non-configured mesh nodes can communicate with a PnP server to obtain their configuration. Advantageously, the techniques herein provide for utilizing an omni-role AP that can intelligently change its wireless behavior to sometimes operate as a client and sometimes operate as an AP, which has not previously been covered in other solutions and is the heart of techniques described herein. Without such an omni-role AP, ANQP and PnP, which provides the framework to exchange configuration information between a device and the PnP server, alone may be incapable of solving the configuration problems as addressed herein. Thus, the techniques herein provide for building an underlay link and increasing coverage provided by operating devices such that each newly configured device takes part in the network and thereby increases the provisioning coverage area.