DEPLOYMENT GUIDE – ARUBAOS 8.X CONTROLLER MESH

EXTENDING CONTROLLER-BASED NETWORKS WITH MESH

Extending a controller-based network to areas without network access is a common use case where network access is critical yet the cost or ability to extend the wired LAN is either cost prohibitive or not possible due to logistics, limited deployment timeframes and/or the LAN extension is temporary. Using AOS controller-based access points (APs) to build a mesh network to extend both wireless and wired backhaul capabilities can be done with minimal effort while still providing the security and manageability of a large campus WLAN.

The assumption of this document is that the mesh setup is being deployed on an already existing ArubaOS campus deployment. If there is a need to stand up a new ArubaOS campus deployment, or on a new standalone controller, please go to https://asp.arubanetworks.com to download the user guides for setting up a Mobility Master (MM) or standalone Mobility Controller (MC).

TABLE OF CONTENTS

What Is Mesh? 1
How to setup mesh within an AOS8 Mobility Master (MM) or controller deployment 3
Initial Controller Configuration 3
Creating the mesh settings in the new AP group 5
Enabling Loop Protection before deploying mesh 7
Initial staging and provisioning of mesh APs 9
Enabling wired backhaul over the mesh points 13
Conclusion 14

WHAT IS MESH?

Aruba's mesh solution is a technology that allows APs to talk to other APs for the purpose of providing Wi-Fi links over the APs to carry wired or wireless client traffic from Mesh Points located away from the wired network, back to the Mesh Portal which is connected to the LAN. In addition to extending the network, APs supporting mesh can also be deployed in configurable mesh clusters so that APs can be grouped together within a large topology and the Mesh Cluster configuration controls which mesh APs can talk to other mesh APs.

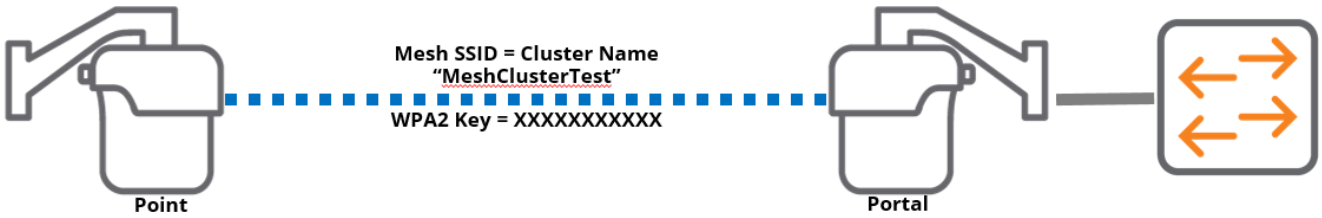


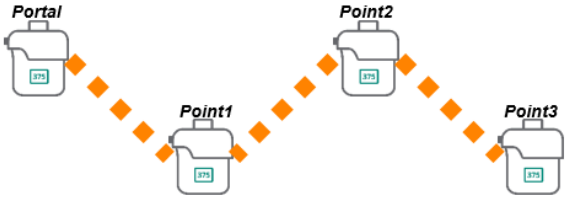
Figure 1

Aruba's mesh supports several topologies, where a mesh portal can support one or more mesh points if necessary. Figure 1 shows a simple Point-to-Point with a single mesh portal and a single mesh point. However, other topologies are supported with an ArubaOS controller-based mesh deployment, including Point to Multi-Point in both a hub and spoke, as well as linear multi-hop mesh in either single-channel or multi-channel topologies below. See Figure 2 below for example topologies.

- **Point to Point (PtP)**

- **Point to Multi-Point (PtMP)**

- **Single-Channel Multi-Hop Mesh**



- **Multi-Channel Multi-Hop Mesh**

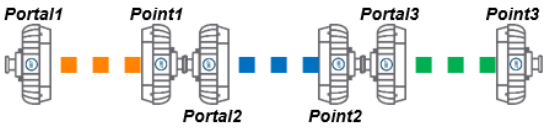
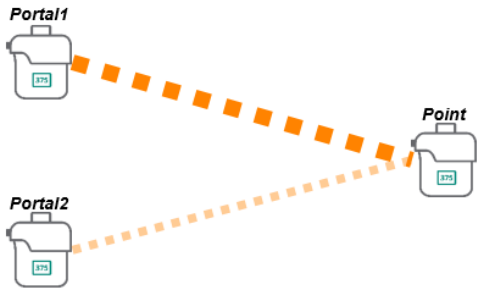


Figure 2

Additionally, using ArubaOS controller-based mesh, mesh-cluster redundancy can be deployed for high availability requirements, as ArubaOS controller-based mesh allows for the configuration of separate mesh clusters. In Figure 3, for PtP redundancy, two portals in the same mesh cluster can be deployed to service one or more mesh points, so that if one portal goes down or gets blocked, the point can move to another portal. For PtMP redundancy, one or more portals can serve as a backup mesh cluster for mesh points, so that if one mesh cluster's portal goes down or gets blocked, the second cluster's portal can take over and serve those mesh points.

- **Point to Point (PtP) Redundancy**



- **Point to Multi-Point (PtMP) Redundancy**

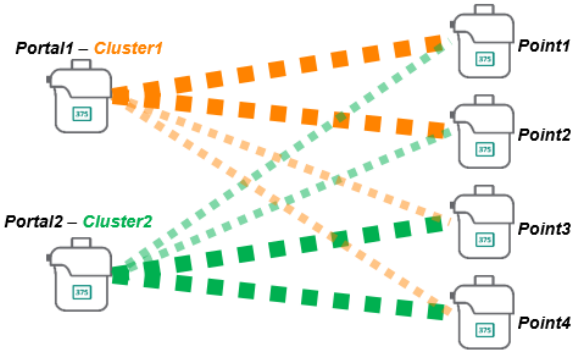


Figure 3

In terms of deployment topologies, it is recommended that there be no more than 3-4 mesh points per portal for general applications, with no more than 2 hops in the mesh topology design. ArubaOS however will allow for more but as more mesh points are added, or as more hops occur within the mesh, overall performance goes down due to the additional overhead of having more APs on the same mesh backhaul.

HOW TO SET MESH WITHIN AN AOS8 MOBILITY MASTER (MM) OR CONTROLLER DEPLOYMENT

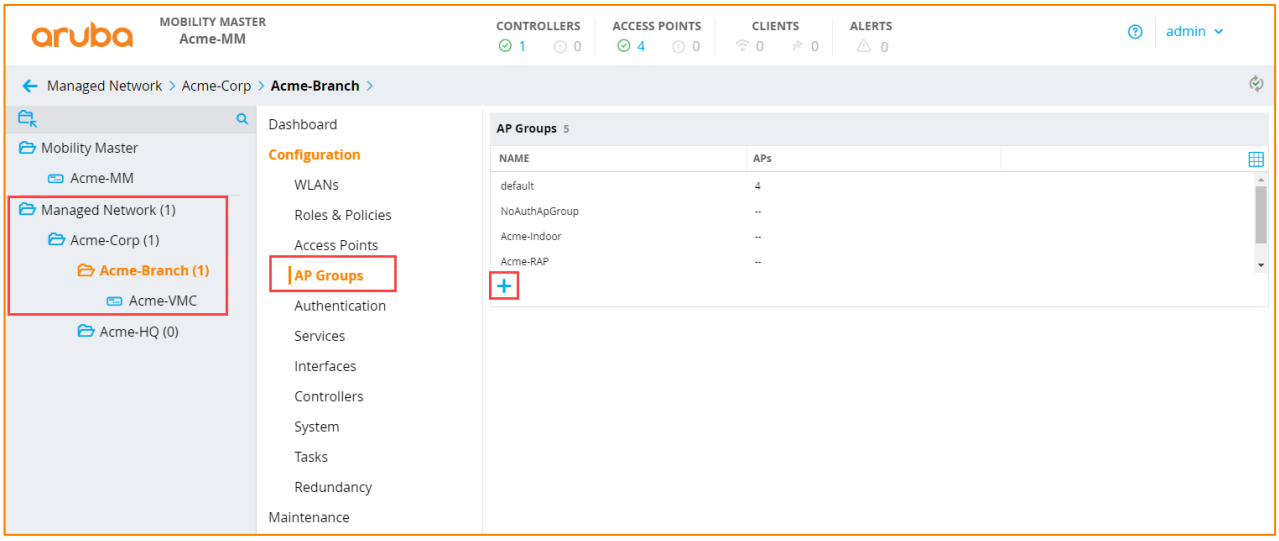
The following process makes a few assumptions necessary to support mesh with AOS 8. Note that while this document focused on a Mobility Master (MM) deployment, the same procedures are used for standalone or non-MM based controller deployments. Other considerations can be taken into account but are outside the scope of this document. Assumptions are:

- A Mobility Master (MM) with Mobility Controllers (MC) are already deployed on the network, and generally are already configured for the core WLAN services required (client WLAN SSIDs, network resources, RADIUS servers, etc.)
- APs that are being deployed are first brought up on the wired network for AP provisioning, using the same controller discovery processes already in place (DHCP Opt 43/60, DNS, etc.)
- A new AP group will be created to accommodate these new APs supporting mesh
- All mesh portals will have network access to the MCs on the core network/LAN
- The ArubaOS version will be AOS 8.x or later. For the purposes of this document, all screenshots are captured using ArubaOS 8.6.0.3

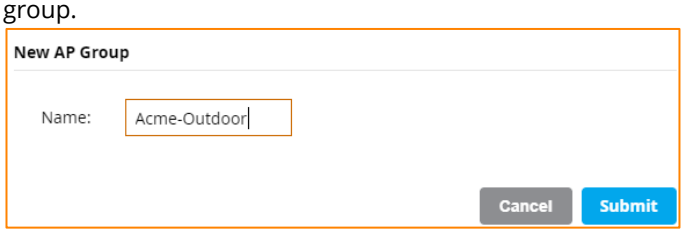
INITIAL CONTROLLER CONFIGURATION

With ArubaOS controller-based deployments, AP groups should be configured before the APs are brought up and provisioned. Either new AP groups specific for mesh can be created so that there is a new group to put these new mesh APs in to, or an existing AP group can be modified to support mesh. It is recommended to create a new AP group for mesh APs due to the need to modify the radio settings to accommodate the outdoor environment that these APs will operate in. As such, the following steps will assume that a new AP group will be created. However, if an existing group is planned to be modified, the same steps can be walked through and only modify the relevant elements in the guide.

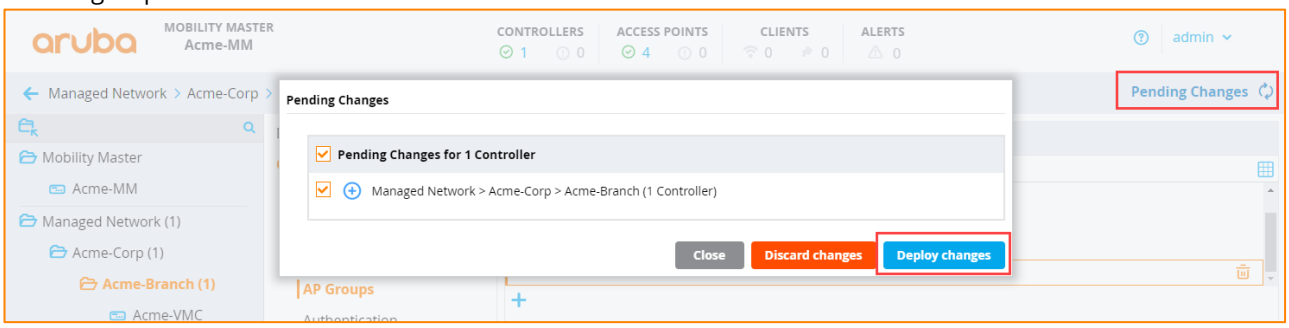
1. Log in to the MM or MC
2. In the MM, navigate to the node in the hierarchy where the MCs are and where the APs will be terminated. Note, configuration changes should be made in the parent node/folder, not on the individual mobility controllers, especially in cases where there are MCs in a cluster supporting APs and clients.
3. In the folder where the MCs are located, navigate to ‘Configuration > AP Groups’ and click on the blue ‘+’ sign to create a new AP group.



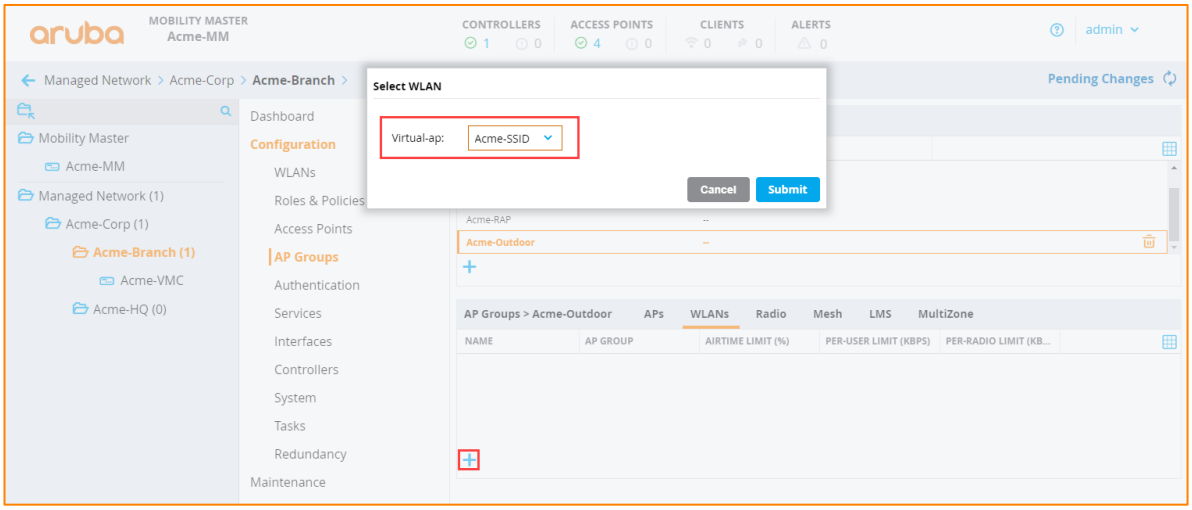
4. A prompt will pop up to name the group. Name the group in accordance with your standard naming conventions, making sure to indicate that this is for mesh for new outdoor APs. Click 'Submit' to create the new group.



5. Once done, in the top right click 'Pending Changes' and then in the pop-up click 'Deploy Changes' to create the new AP group. Then click 'Close' in the confirmation box.

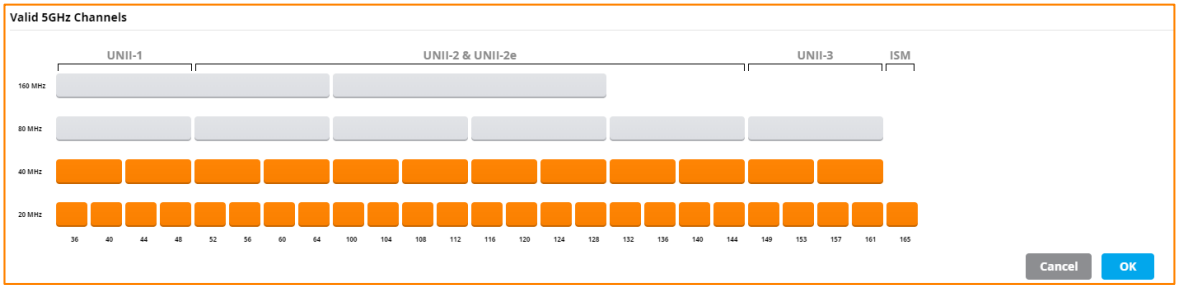


6. Once created, from the 'AP Groups' page, click on the newly created AP group. A new page will load with multiple tabs to configure.
    a. The APs tab will currently be blank. Once APs are provisioned into this group, APs that are a member of this group will appear here. For now, this being blank is fine.
    b. The 'WLANs' tab is where existing WLANs in that node exist. If there are WLANs to assign to this new AP group, click the blue '+' sign and select which WLANs to add to this group. Click 'Submit' when done adding one or more WLANs to this group.

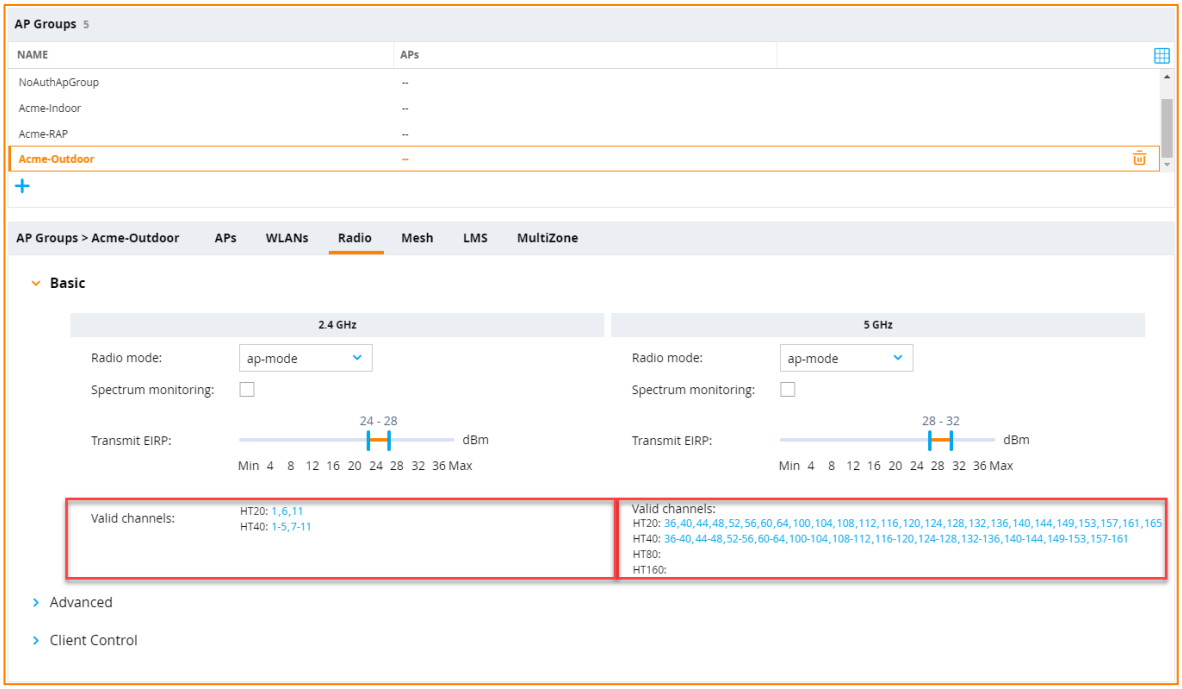


c. Click on the 'Radio' tab. If these are going to be outdoor APs located outdoors, to ensure strong signal for larger outdoor areas, the 'Transmit EIRP' should be raised. Consult with your WLAN engineer if these values are not clear, but generally it's recommended to set the 2.4Ghz radio to '24-28dBm' EIRP, and the 5Ghz radio to '28-32dBm' in the 'Transmit EIRP' settings. If unsure, please consult with your WLAN engineer.

d. Additionally, on the 'Radio' tab, the 'Valid Channels' should be set. The 2.4Ghz radios should only be configured for HT20 with channels 1, 6, and 11 configured. For the 5Ghz radio, this can be specific to the deployment but for the purposes of this guide, we will enable only 40Mhz wide channels and enable Dynamic Frequency Selection (DFS) channels. Please consult your local WLAN engineer, partner, or Aruba SE if this is not clear, or if the area in question has special considerations in terms of DFS. Proximity to airports, naval ports, hospitals with helicopter pads, etc. should generally avoid DFS channels to prevent WLAN disruption. When clicking on the 'Valid Channels' a pop-up will appear. To enable or disable channels, just click in the bubbles to enable (turns orange) or disable (turns grey).



e. Once finished on the 'Radio' tab, there should be a transmit power setting with the new allowed 'valid channels' defined for this new AP group. Click 'Submit' in the lower-right to apply the new changes.

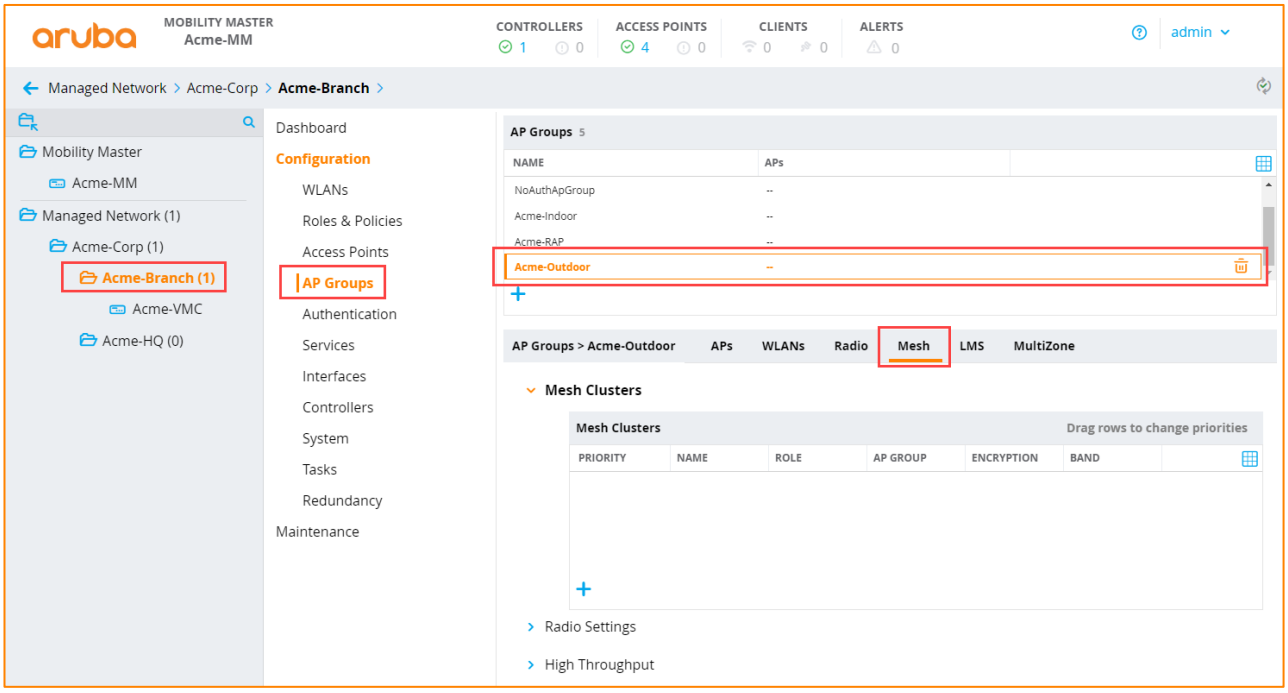


f. Once done modifying the WLAN and Radio settings, click on 'Pending Changes' and 'Deploy Changes' as before.

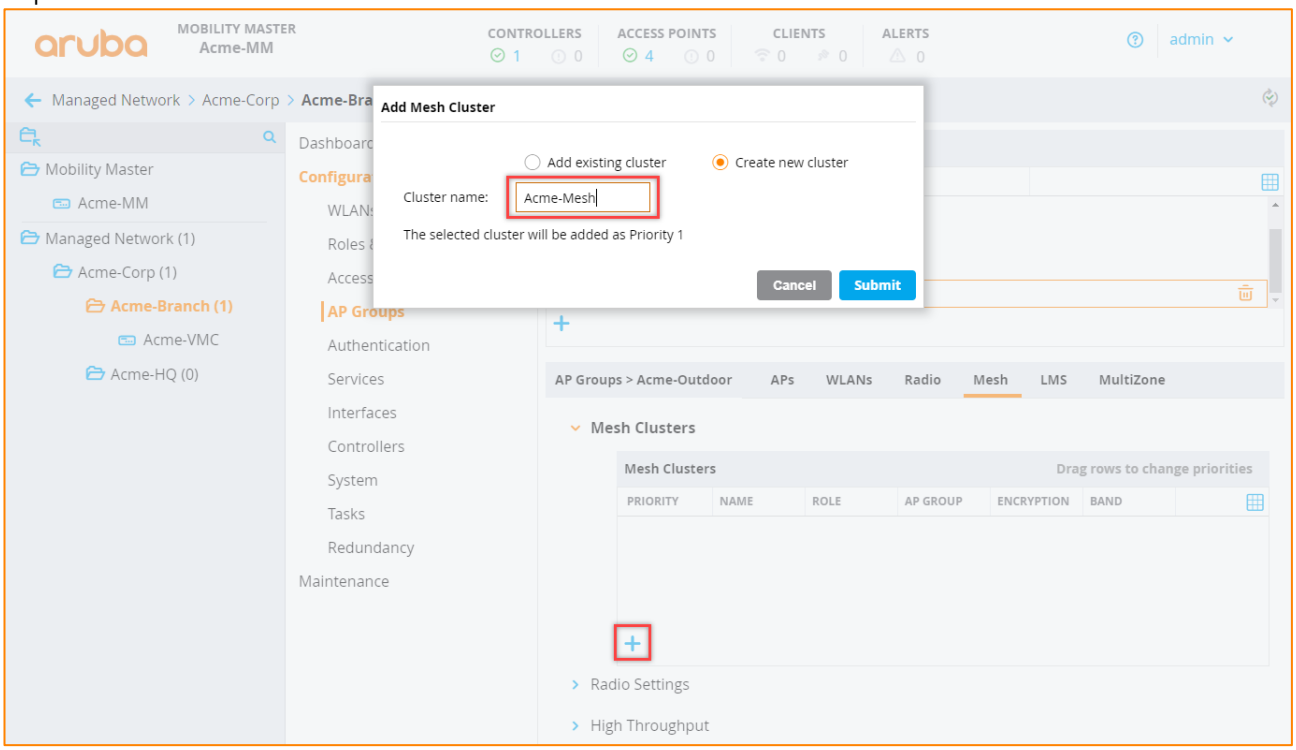
CREATING THE MESH SETTINGS IN THE NEW AP GROUP

With the new AP group complete, the mesh settings that are required can now be created in the new AP group.

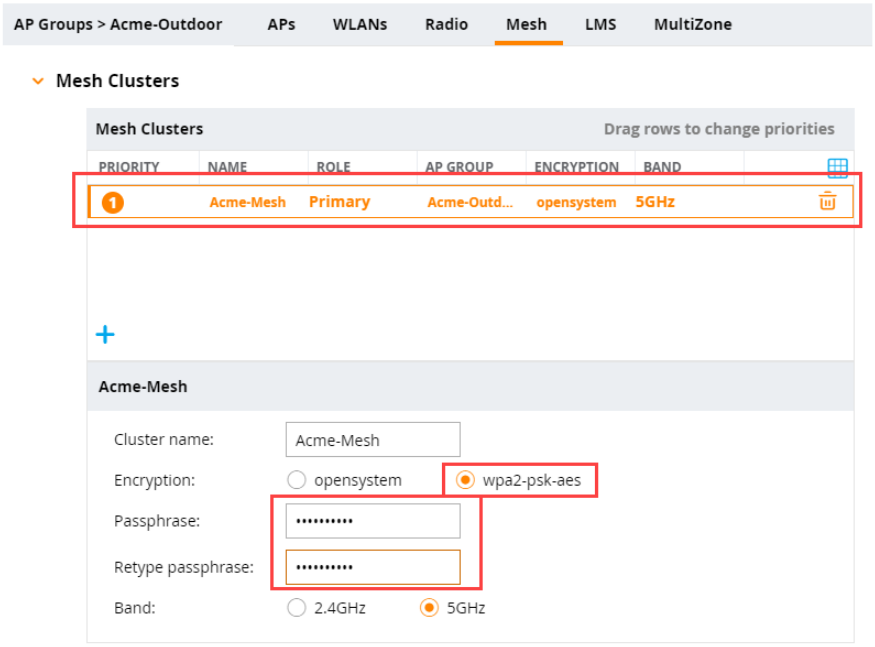
1. Go to the folder in the hierarchy where the new AP group was created and go to 'Configuration > AP Groups' and click on the new AP group that was created. Then click on the 'Mesh' tab.



2. Once the Mesh tab loads, it should show the 'Mesh Clusters' configuration page. To create a new mesh cluster configuration for a new AP group, click on the blue '+' sign to create a new mesh cluster for this AP group. A popup will appear with 'Create new cluster'. Give the new cluster a name that fits within the naming convention required. Click 'Submit'.

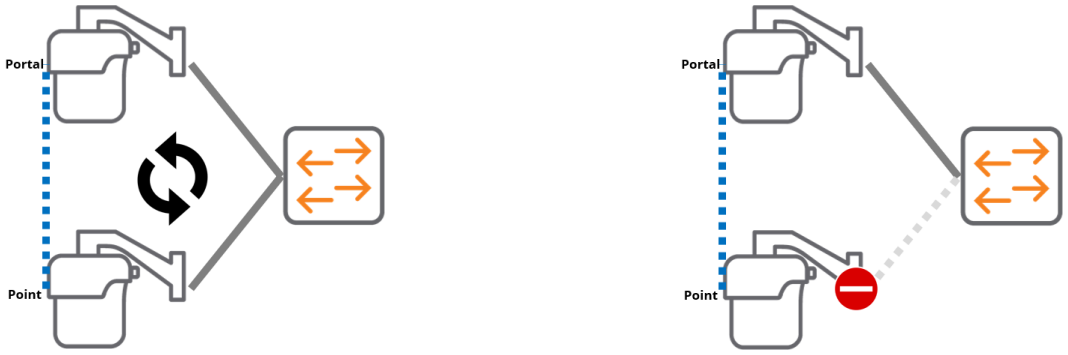


3. Once the new mesh cluster is created, the new mesh cluster will show up in the mesh clusters page with a green priority of '1'. This indicates it is the primary mesh cluster for this AP group. If other mesh clusters are configured within this AP group for redundancy purposes, make sure that they are prioritized correctly within the AP group. To modify the newly created mesh cluster to use encryption, click on the new mesh cluster, change the encryption to 'WPA2-PSK-AES' and enter a passphrase for the encryption. Click 'Submit', then as before click 'Pending Changes' and then 'Deploy Changes' to write the change to the MM and MCs. Then click 'Close'.



ENABLING LOOP PROTECTION BEFORE DEPLOYING MESH

At this point, the new AP group has enough information that will allow a properly provisioned AP to participate in Mesh. However, there is a risk that if a mesh portal and point are provisioned while both are connected to the same network, if that happens there could be a condition that a loop on the network forms (since there will be multiple paths from the point to the wired uplink network). To mitigate this risk, the new mesh AP group can enable loop protection. Loop protection on the AP group system settings monitors the wired traffic in and out of a mesh point's interface and if it sees its own traffic coming in and out of the wired interface as well as the wireless uplink, it will disable the mesh point's wired interface for a period of time, and then release the interface to continue monitoring. The steps below walk through enabling loop protection on the new mesh AP group. Figure 4 below shows a mesh PtP with and without loop protection.



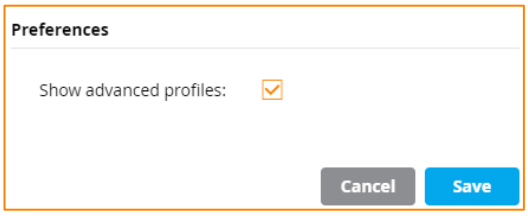
Without 'Loop Protection' enabled

With 'Loop Protection' enabled

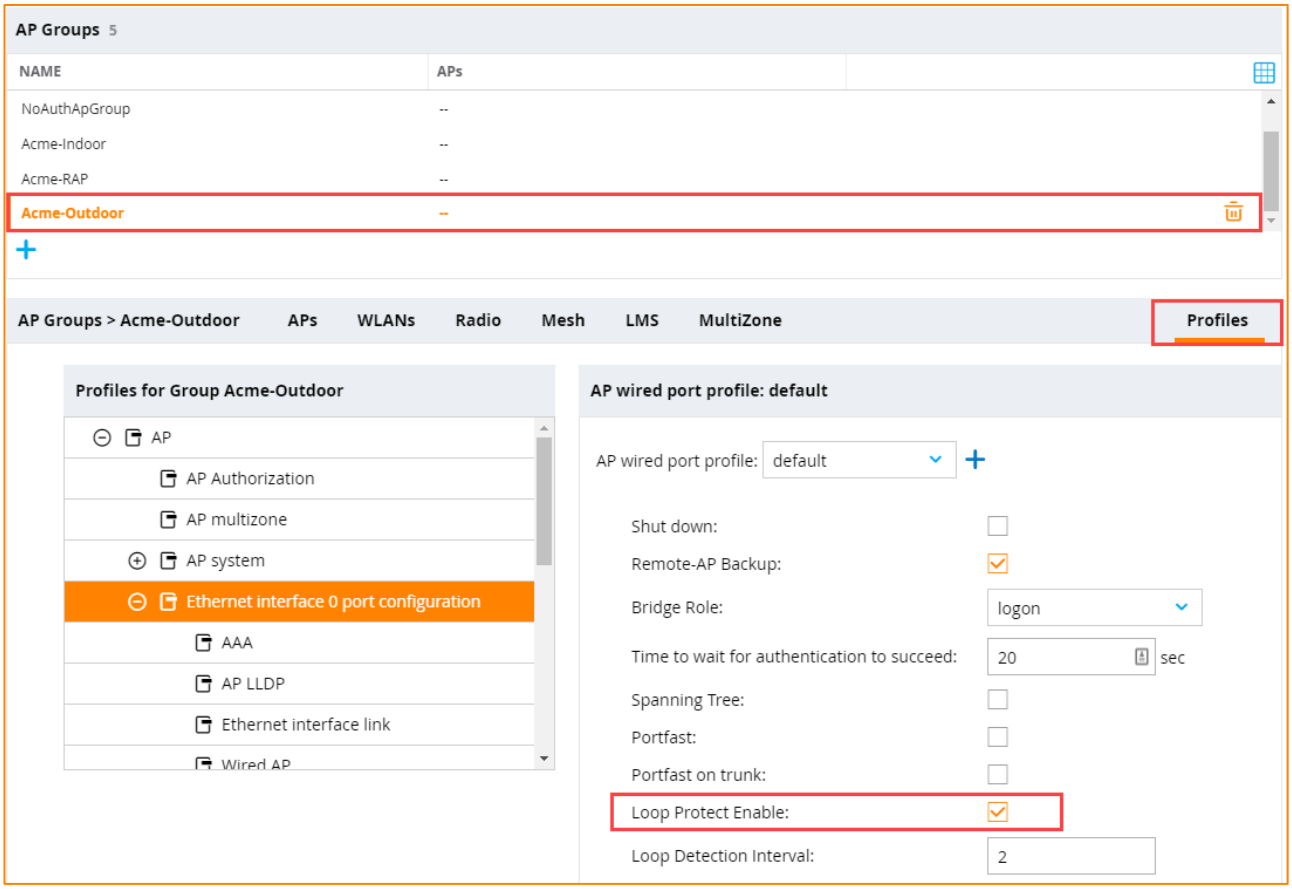
Figure 4

To enable Loop Protection on the new mesh AP group:

1. If 'Show advanced profiles' is not already enabled, go to the top right, click on the 'admin' account (or name of the account logged in), click 'Preferences', and in the pop-up check the 'Show advanced profiles' checkbox. Click 'Save'.



2. Go to the node or folder containing the controllers where the AP group was configured, and go to 'Configuration > AP Groups', click on the newly created mesh AP group, and click on the 'Profiles' tab.
3. Within the 'Profiles' menu on the left side, navigate to 'AP > Ethernet interface 0 port configuration', and check the box next to 'Loop Protect Enable'. Do this for any active interfaces to be used by the mesh point. Then click 'Submit' when done. Then as before, click on 'Pending Changes' followed by 'Submit Changes' to write the config to the MM and MCs.



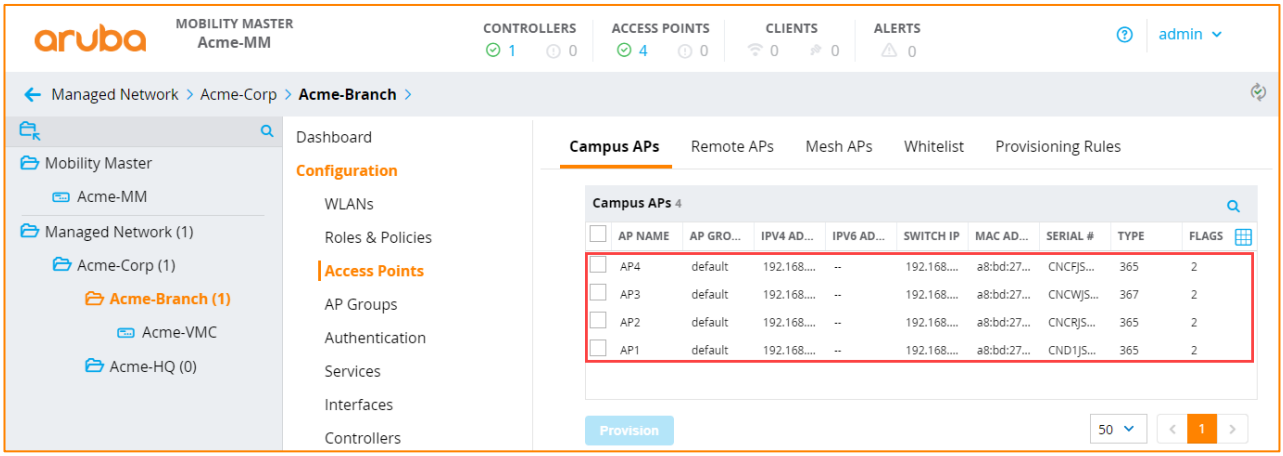
Now any mesh points deployed in this AP group will have Loop Protection enabled on any active wired interface on the AP.

NOTE: Some vendor's switches use BPDU Guard that will trigger loop protect mode. If connecting remote switches to the mesh points, it is advised to disable any BPDU guard functionality on that switch.

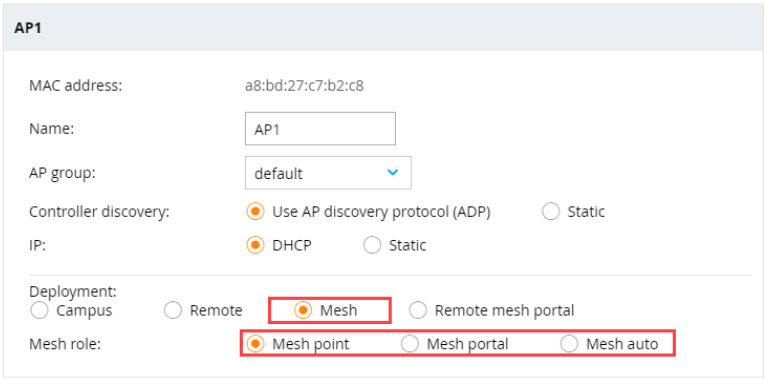
INITIAL STAGING AND PROVISOINING OF MESH APS

Once the AP group is established, with the appropriate RF settings changed, the WLAN configured, and the new mesh cluster configuration established, the MM or controller is ready to provision the APs.

1. Connect all the APs to the network to allow the controller discovery to occur. The APs should discover the controllers via the Aruba Discovery Protocols (ADP) upgrade code and show up on the MM or MCs ready to be provisioned.
2. Clicking back into the node or folder on the hierarchy where the controllers are located, the APs should now show up under 'Configuration > Access Points'. If they are new APs, the AP name will be the wired MAC address and the group will be 'default'. If they are already existing APs being re-provisioned for mesh, they will need to be found in the existing AP list.



3. When provisioning an AP, there are a minimum of two pieces of information that needs to be defined on the AP. First is the AP name, the second is the AP group. Additionally, however, if the APs are doing mesh, we also need to assign a mesh role. There are three roles available when provisioning a mesh AP. When an AP is provisioned as a mesh AP, what defines the role is whether the 'uplink' back to the controller is over the wire or over the wireless. Mesh portals use the wired interface for uplink and mesh points use the wireless interface for uplink to the controller.



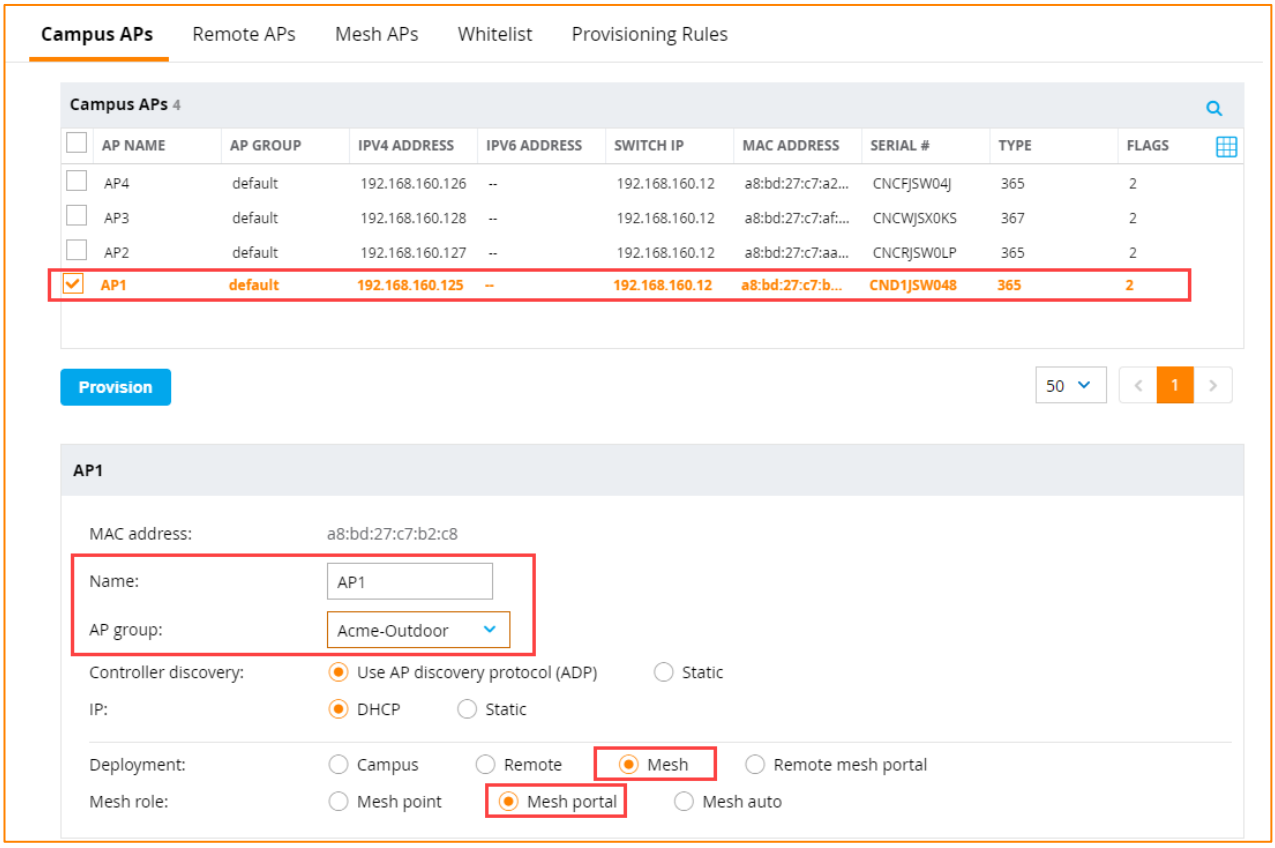
   a. Mesh Role: Portal – This setting enables the AP to broadcast the mesh SSID that will be used by the mesh points and locks the uplink to the wired interface. If the deployment ensures the AP will always be a portal, define the role as 'Portal'.

   b. Mesh Role: Point – This setting enables the AP to use ONLY the wireless interface for uplink, by scanning for the mesh SSID broadcast by a nearby portal or point. If the deployment ensures the AP will never have a wired uplink to the controllers, define the mesh role as 'Point'.

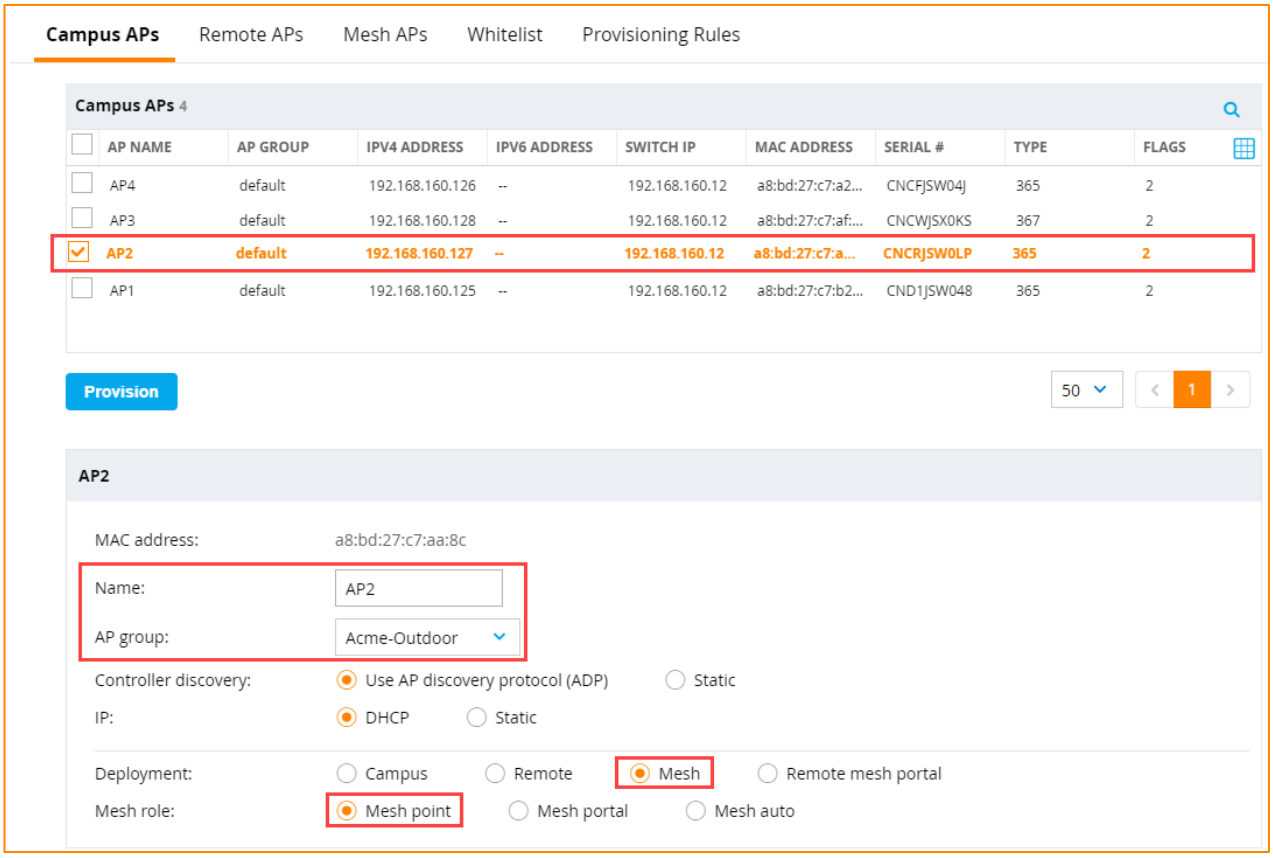
   c. Mesh Role: Auto – This setting enables the AP to become a mesh portal OR a mesh point, by testing uplink detection. The tradeoff is that a mesh AP provisioned as 'auto' will first try the wired uplink first, then reboot to try wireless uplink, and go back and forth until uplink is detected. This can result in 'auto' provisioned mesh APs taking longer to come up when rebooted but allows for flexibility in deploying in uses case where wired uplink is not certain.

NOTE: In general, all APs should be on the wire before provisioning, so they can connect to the controller. There is no mechanism to provision mesh points without first connecting to the MC.

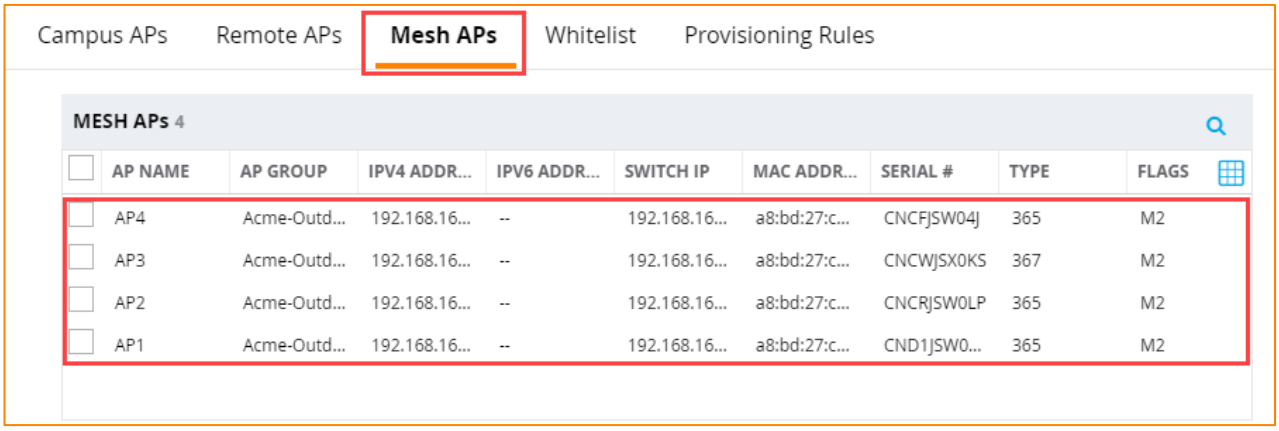
4. With the APs up on the MM or controller, pick the AP designated to be the portal to be provisioned first. Click on the AP to be provisioned and click the blue 'Provision' button.
5. In the AP provisioning window, enter the AP name, assign the new mesh AP group that was created as the 'AP group', and check the 'Mesh' radio button along with the 'Portal'. Verify all fields are set correctly, and then click 'Submit'. The controller will then send those new settings to the AP and the AP will reboot. At this point, the portal is complete, and it can be deployed.



6. As the portal is being deployed and is rebooting, provision the next AP that will be a mesh point. As before, click on the AP to be provisioned, click the blue 'Provision' button, and enter the new AP name and assign it the new mesh group. Select the 'Mesh' radio button and select 'Mesh point'. 'Mesh auto' is also an option as well if the deployment calls for it, noting the above conditions as it pertains to the 'Mesh auto' role. Click 'Submit' to re-provision the AP.



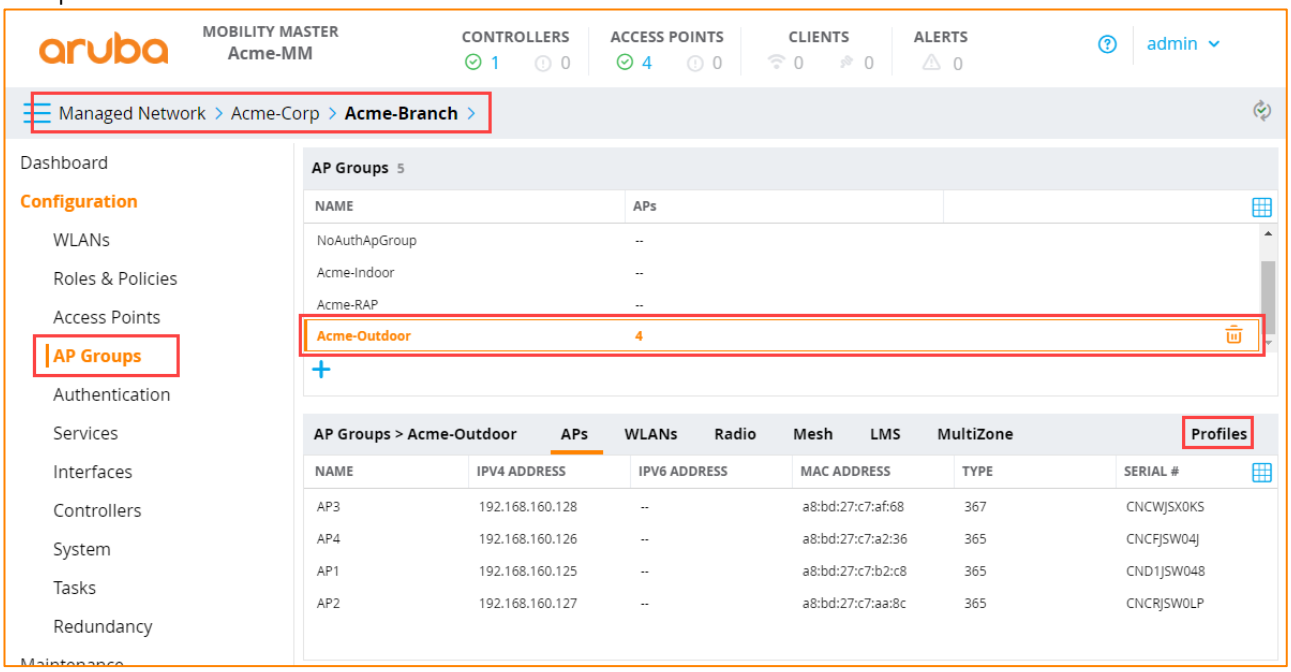
7. It is important that once a mesh point is provisioned, once it downloads the config and reboots, that the AP be disconnected from the network and deployed, ***or as is always a best practice***, powered up separately on a power injector or external switch to come up as a test before the AP is deployed. While loop protect was enabled before, the risk of a network loop should be minimized as much as possible.
8. Once the portal and all points have been re-provisioned correctly, and if they are being tested in the lab or in the staging area before deployment ***as a best practice***, verify that the portal(s) and point(s) come up and are working as expected before going out to install and deploy the APs. Once all APs have been tested and found to be working correctly, this part of the configuration is now done. All mesh APs will show up in 'Configuration > Access Points – Mesh APs' tab.



ENABLING WIRED BACKHAUL OVER THE MESH POINTS

If there is a need to connect a wired device or switch to a mesh point to backhaul wired network traffic from the remote switch on the mesh point back to the main LAN or internet, perform the following steps.

1. In the folder or node that contains the mobility controllers, go to 'Configuration > AP Groups > New Mesh AP Group' and click on the 'Profiles' tab.



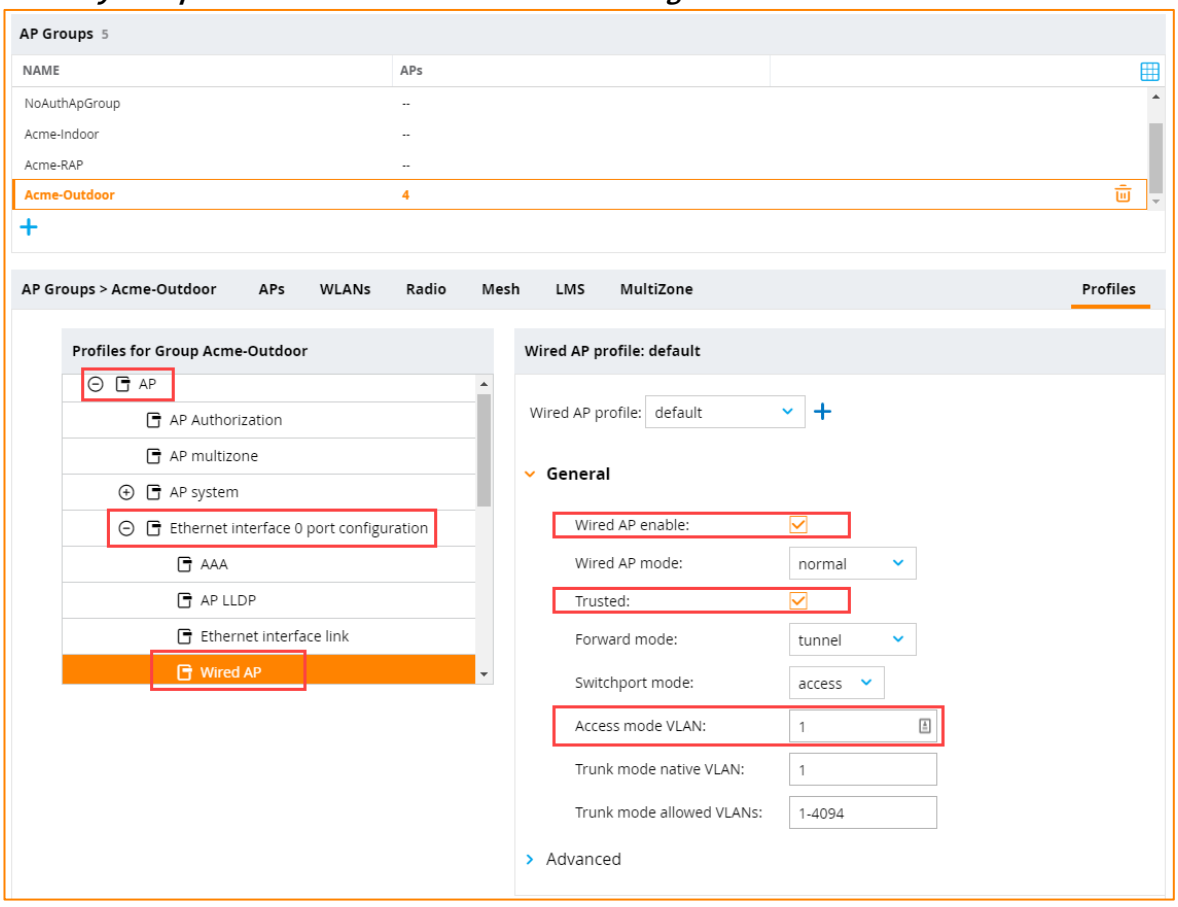
2. Within 'Profiles', go to 'AP > Ethernet interface 0 port configuration > Wired AP'. This is where the AP interfaces can be configured to serve as a wired backhaul interface over the mesh back to the portal. Check the box next to 'Wired AP Enable' to enable the interface, check the box next to 'Trusted' to mark the port as trusted. In terms of 'Forward mode', there are two options.
    a. Tunnel – will encapsulate the wired traffic inside a GRE tunnel back to the controller. This is the safest option as it removes the portal AP's wired uplink switch port configuration from consideration in handling the wired traffic, which requires ensuring that all mesh APs have the same wired port bridge

configuration. This in effect means all wired backhaul traffic VLANs should be configured and exist on the controllers terminating the APs.

b. Bridge – Wired traffic between the mesh point and mesh portal are purely bridged, meaning untagged traffic into the mesh point go out the portal untagged, and any wired tagged traffic must match the tag on the portal's switch port. As such, running in bridge mode requires that the switch port configs in terms of tagged and untagged VLANs must match on both sides.

3. Depending on the wired config requirements, configure the port config (access or trunk, specific VLANs, etc.) to match the Forward mode and switch configuration (if relevant). In the image below, this network runs over VLAN 160 but because the port config is a flat access layer, VLAN 1 can be the default native VLAN. Click 'Submit', then 'Pending Changes' and 'Deploy Changes' to write the configuration change to the controller.

   a. ***Note: If defining a native VLAN other than VLAN 1 on a trunk port with native VLAN support, the AP system profile's 'Native VLAND ID' must be configured to match.***



Enabling wired traffic backhaul over mesh, especially on any deployment with multiple VLANs can be challenging. In cases where wired backhaul support from switches connected to the mesh point is required, please follow proper staging guidelines to ensure testing and a working configuration is verified before hanging the mesh points ***as a best practice***.

CONCLUSION

Using the information in this document, a quick and capable ArubaOS controller-based mesh network can be deployed in a rapid fashion to provide quick, reliable coverage in hard to reach areas. The logistics of a setup still have to be solved, including WAN or Internet traffic and how the clients and devices get out to the internet, power solutions for the hardware in use in a parking lot, or remote facility, what infrastructure would be required to mount the APs to (tripods, light poles, stationary vehicles or trailers, etc. are all viable with creative solutions) and Aruba's AP mounts are very simple, fast, and easy to use.

Please use the following links to find supporting documentation on Aruba's products, and if there are any questions, please reach out to your Aruba SE or Partner for more information.

Aruba Access Points

- https://www.arubanetworks.com/products/networking/access-points/

Outdoor AP Mounting Brackets

- https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/EntryId/28815/Default.aspx

03.30.20

aruba
a Hewlett Packard Enterprise company
www.arubanetworks.com

3333 Scott Blvd. | Santa Clara, CA 95054
1.844.472.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | info@arubanetworks.com