

DEPLOYMENT GUIDE - ARUBA INSTANT MESH

USING ARUBA INSTANT AP VIRTUAL CONTROLLER MESH

When needing to stand up a quick, easy to deploy temporary, tactical, or permanent deployment of Wi-Fi over an open area that is lacking wired connectivity for the coverage area required, Aruba's Instant APs can be deployed easily using Instant Mesh within a Virtual Controller (VC) to wirelessly extend coverage to remote areas that are outside of the wired range of the network or to areas that are difficult to pull wired network drops to. Instant Mesh can be used just to extend wireless coverage to clients in and around the areas where the APs are deployed or can provide wired connectivity using the mesh radios to backhaul traffic over the mesh back to the LAN.

TABLE OF CONTENTS

What Is Mesh?	1
How to set Instant Mesh within a Virtual Cluster (VC)	2
Initial Staging of APs	2
Setting proper RF settings for Outdoor APs	4
Creating the Wireless User SSIDs	5
Mesh Setup	7
Mesh Setup with Wired Backhaul	9
Conclusion	11
Appendix – Universal AP (UAP) Setup	12

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.



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 Instant Mesh, including Point to Multi-Point in both a hub and spoke (Figure 2) as well as linear multi-hop mesh (Figure 3) below.

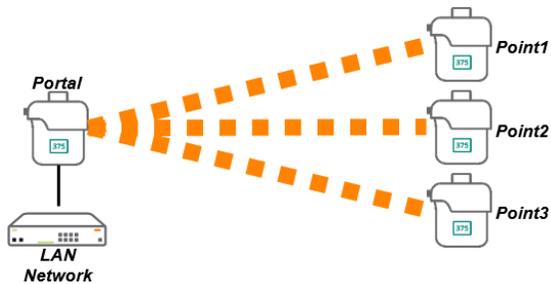


Figure 2

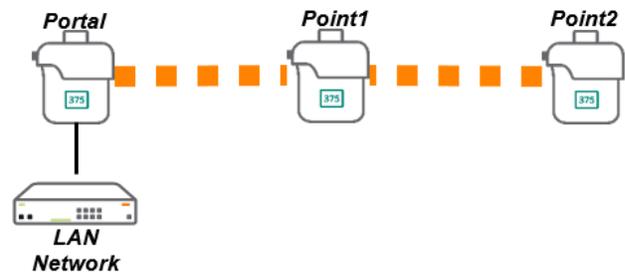


Figure 3

With Aruba Instant, 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. Aruba Instant has a hard limit of up to 8 mesh points per portal and 2 hops in the mesh topology, but each mesh point in the cluster adds latency and lowers overall throughput, so keeping the mesh point count low helps ensure adequate performance.

HOW TO SET INSTANT MESH WITHIN A VIRTUAL CLUSTER (VC)

The following process makes a few assumptions necessary to support an Instant mesh solution. Other considerations can be taken into account but are outside the scope of this document. Assumptions include:

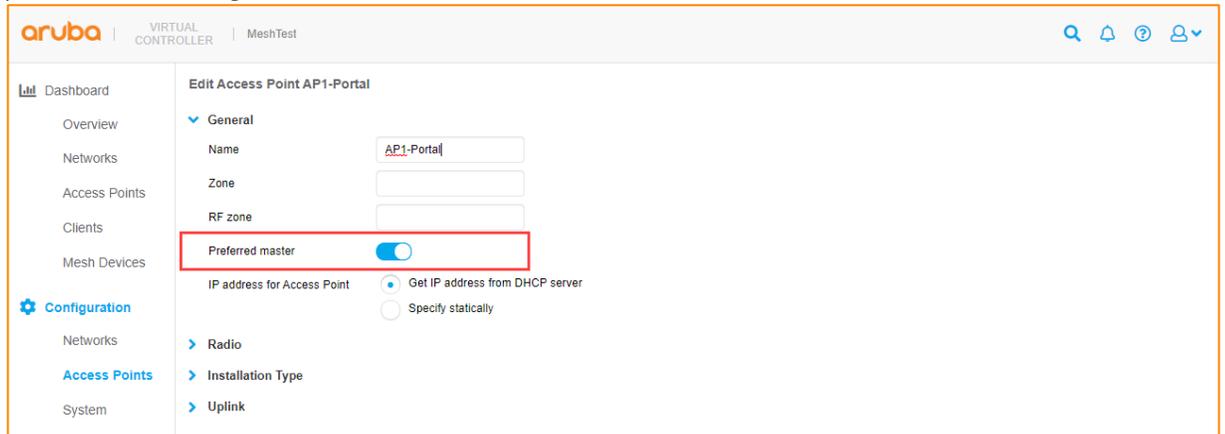
- The network where these APs are deployed are the only Instant APs on that L2 network/VLAN.
- All APs within the same Virtual Controller (VC) are of the same platform and family (AP-360 family, AP-370 family, AP-387 Point-to-Point solution, etc.).
- All APs are part of the mesh. This mesh network will not be able to backhaul other Instant APs not part of the mesh and should be handled with a specific design to accommodate that requirement. Please consult your Aruba SE or Partner.
- DHCP services are available either to/from the main LAN/network or provided via the gateway or routers for this network.
- Instant OS version 8.5 or 8.6 or later.
- If there are any other deviations or accommodations that need to be made, please consult your Aruba SE or Partner.

INITIAL STAGING OF APs

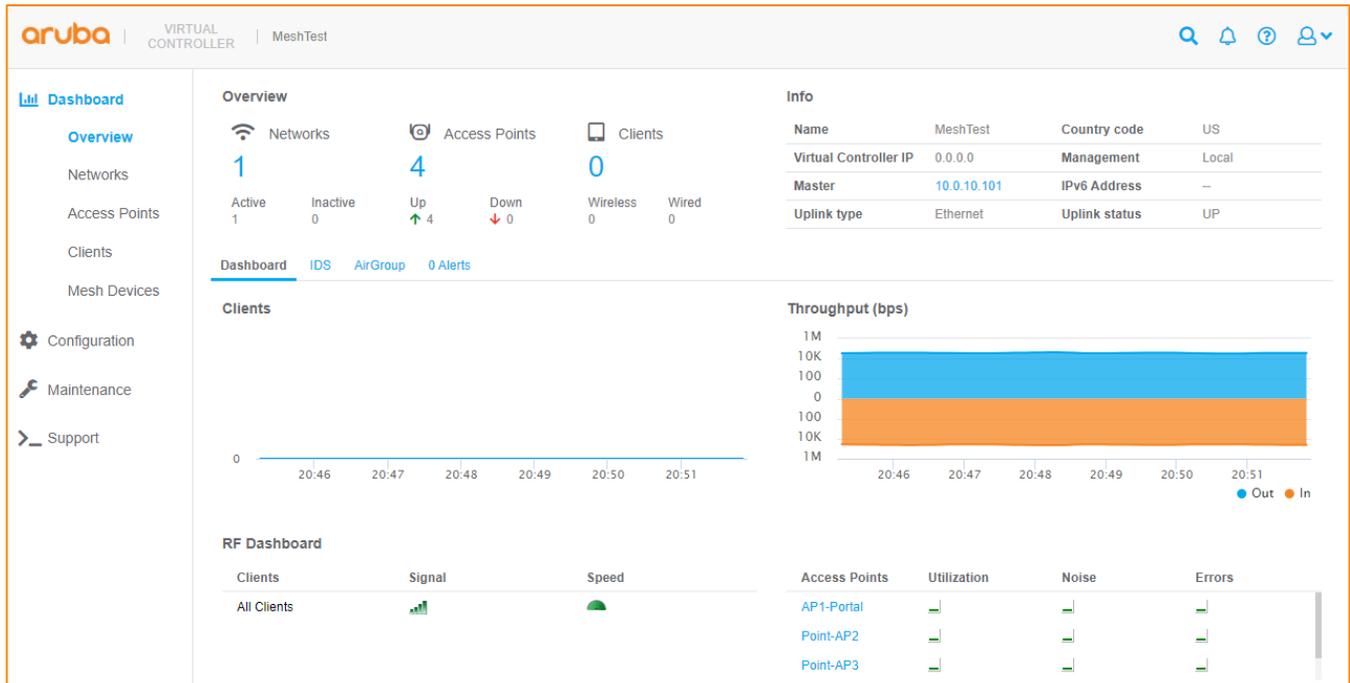
While this deployment guide is starting from the assumption of a new deployment, the following steps can be taken if this is to extend, grow, or modify an existing Instant AP deployment. Some of the steps can be ignored below if there is an existing deployment (making system and password changes, naming APs, etc.).

1. Connect all the APs to the same network (same VLAN) to allow them to come up as an IAP Cluster and allow them to pull an IP address. You can see what the IP address of one of the APs are either by connecting to the DHCP server to see which IP address was assigned to the AP's MAC address, or connecting to the AP's serial console, logging in with either 'admin'/'admin' or the 'admin'/'serial number' of the AP, depending on code version. Once all the APs are connected, they will upgrade to the same code version. You can also connect with a wireless client to the 'SetMeUp' SSID being broadcast.

- a. Note, the default Instant admin password is 'admin' up until Instant OS 8.4. Starting in 8.5, new APs or APs factory defaulted will require the password to be the AP's serial number (either the single AP or any AP's serial number that is part of the VC).
2. Connect to one of the APs, log in with 'admin' and do the following under 'Configuration':
 - a. Under 'System > General' - Change the system name to a name that makes sense for the deployment.
 - b. Under 'System > Admin' - Change the 'admin' password to something secure.
 - c. Under 'Access Points' - Change the name of the APs from their default MAC address to a name that indicates function and location (usually role and where the AP will be placed).
 - d. For the AP designated as a portal AP, configure the portal as a 'preferred master' to prevent a mesh point from becoming the VC master.



3. Under 'Maintenance > Firmware' - Upgrade the IAPs to the latest 8.5.0.6 or 8.6.0.2 version.
4. Under 'Maintenance > Reboot' - Reboot all the IAPs.
5. When done, the IAP VC should look like the below image.



Note: If new APs are being deployed, and the Universal AP (UAP) provisioning page displays when setting up the AP, please see the bottom of this document for the UAP provisioning steps in 'Appendix: Universal AP (UAP) Setup'.

SETTING PROPER RF SETTINGS FOR OUTDOOR APs

When APs are located outdoors, or when supporting mesh deployments, generally the AP's radios need to be set at or near maximum power to ensure maximum range and signal at longer distances. As such, the RF settings need to be modified for the outdoor APs to properly support outdoor environments.

1. Go to 'Configuration > RF' to access the RF settings of the APs within the IAP VC.
2. At the bottom of the page, click on 'Show Advanced Options'.
3. Set the minimum transmit power at 30dB and turn off 80Mhz support (if 160Mhz support is also visible, support for 160Mhz should also be disabled). The 'Customize Channels' can also be checked to ensure all available channels are selected.

4. If there is a need to set custom radio channel and power profiles, the 'Radio' tab can be selected and custom radio-specific power settings can be applied as well.
5. Click 'Save'.

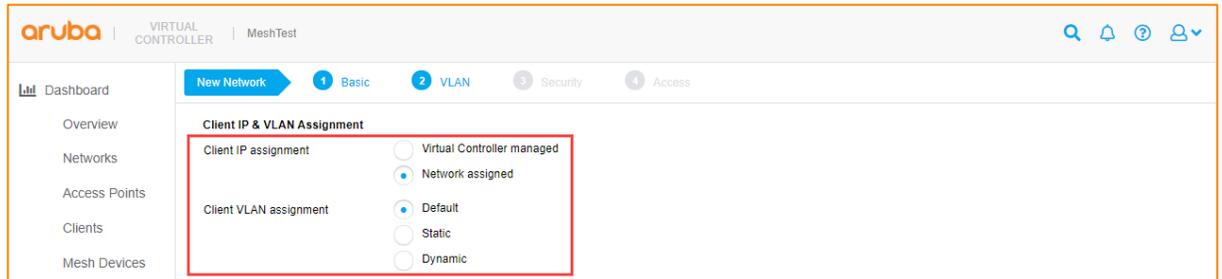
CREATING THE WIRELESS USER SSIDS

Once all the IAPs have rebooted after initial staging, the user WLAN SSIDs can be configured.

6. Under 'Configuration > Networks' - Create the necessary WLAN SSIDs to support the end users by clicking the blue '+' sign.
7. The name of the SSID will be the Wi-Fi SSID that is broadcast by the AP. Select type as 'Wireless' and the primary usage can be 'Employee' for employee access. There is also a primary usage of 'Guest' that will allow an SSID to serve guest clients behind a NAT from the VC that will be separated from the main VLAN the IAPs are running on.

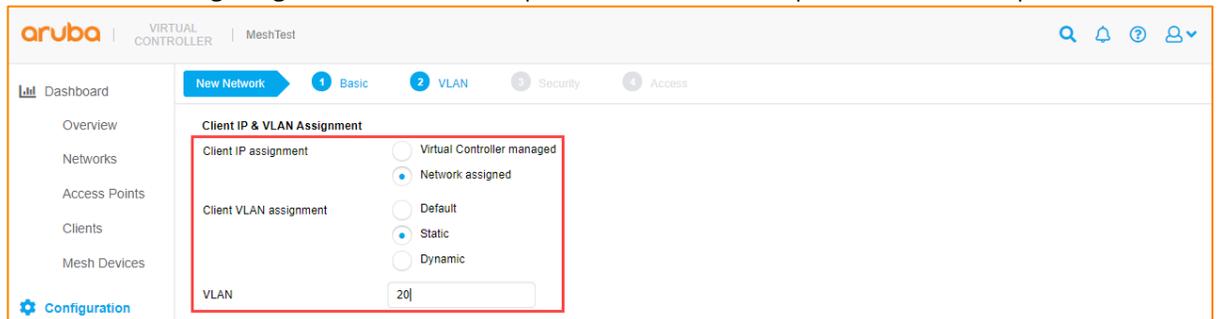
8. Under 'Advanced', any advanced settings can be configured, if necessary.

9. Define the network assignments to the SSID, depending on how they are connected to the network.
 - a. 'Virtual Controller managed' - will create a NAT'd network for the clients to connect to the network, generally used for 'Guest' networks.
 - b. 'Network Assigned > Default' - will assign the clients an IP address on the same untagged L2 network the APs are connected to.



The screenshot shows the Aruba Virtual Controller interface for 'MeshTest'. The 'New Network' wizard is on the 'VLAN' step. The 'Client IP & VLAN Assignment' section is highlighted with a red box. It shows two radio button options for 'Client IP assignment': 'Virtual Controller managed' (unselected) and 'Network assigned' (selected). For 'Client VLAN assignment', there are four radio button options: 'Default' (selected), 'Static', and 'Dynamic' (unselected).

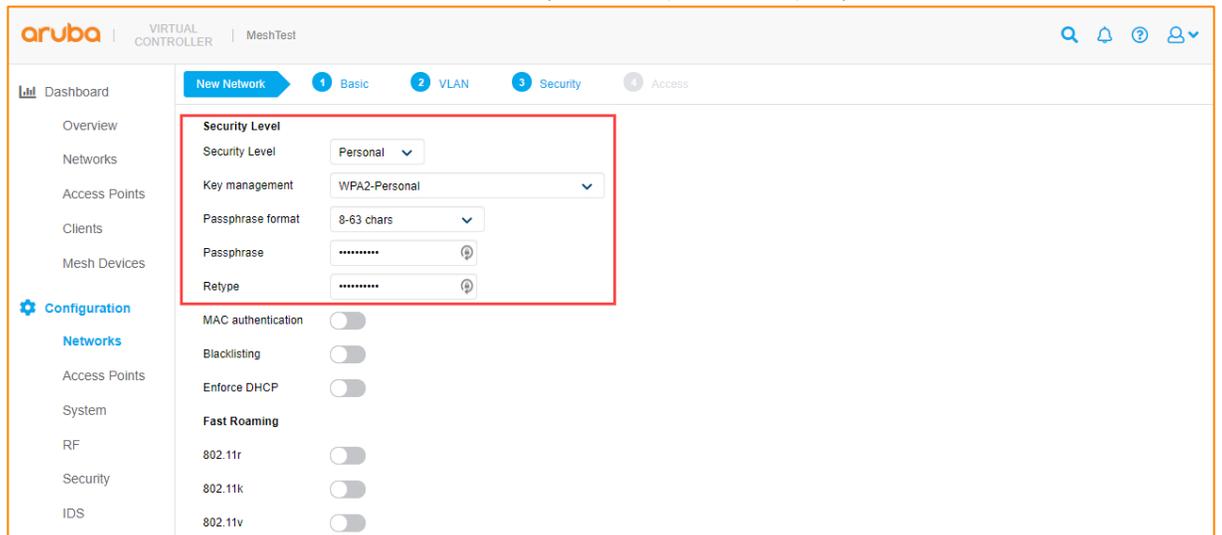
- c. 'Network Assigned > Static' - allows clients to be assigned to a specific VLAN that is tagged to the AP's uplink ports on the switch they are connected to. Note that the IAPs all run in bridge mode, so if a static VLAN is being assigned for a client SSID, please ensure all the requisite VLANs are in place.



This screenshot is similar to the previous one, but the 'Client VLAN assignment' is now set to 'Static'. Additionally, a 'VLAN' input field is visible at the bottom of the configuration area, containing the value '20'.

10. Create the security settings on the SSID.

- a. 'Personal' defines a non-RADIUS WLAN solution (WPA2-PSK, WPA3-PSK, etc).



The screenshot shows the 'Security' step of the 'New Network' wizard. The 'Security Level' section is highlighted with a red box. It includes a dropdown menu for 'Security Level' set to 'Personal', a dropdown for 'Key management' set to 'WPA2-Personal', a dropdown for 'Passphrase format' set to '8-63 chars', and two password input fields for 'Passphrase' and 'Retype'. Below this section, there are several toggle switches for 'MAC authentication', 'Blacklisting', 'Enforce DHCP', and 'Fast Roaming' (with sub-toggles for 802.11r, 802.11k, and 802.11v).

- b. 'Enterprise' defines a RADIUS-based solution (WPA2-ENT, WPA3-ENT, etc.), and requires an already setup RADIUS server to authenticate the users. Please ensure all RADIUS settings required for the environment are set correctly, and this network and the APs are added to the RADIUS server to authenticate users.

The screenshot shows the 'New Network' configuration page in the Aruba Virtual Controller. The 'Security' tab is active, and the 'Security Level' section is highlighted with a red box. The configuration includes:

- Security Level: Enterprise
- Key management: WPA2-Enterprise
- Authentication server 1: EnterpriseRadius
- Authentication server 2: -- Select Server --
- EAP offload: Disabled
- Reauth interval: 0 min.
- Authentication survivability: Disabled
- MAC authentication:
 - Perform MAC authentication before 802.1X: Disabled
 - MAC authentication fail-thru: Disabled
- Accounting: Disabled

11. Define the firewall policy to be applied to the wireless clients, if a policy needs to be applied. The IAPs support both role-based policies as well as network-based policies. Please consult the [Instant User Guide](#) for details on creating a role or network-based policy. In this instance, we are creating an unrestricted network policy.

The screenshot shows the 'New Network' configuration page in the Aruba Virtual Controller, specifically the 'Access' tab. The 'Access Rules' section is highlighted with a red box. The configuration includes:

- Access Rules: Unrestricted
- Download roles: Disabled

Below the dropdown, it states: "No restrictions on access based on destination or type of traffic"

MESH SETUP

1. Go to 'Configuration > System' and click on 'Show Advanced Options'.
2. Find 'Extended SSID' and disable it (it should turn from blue to grey). Disabling 'Extended SSID' allows the APs to broadcast the required mesh SSID.

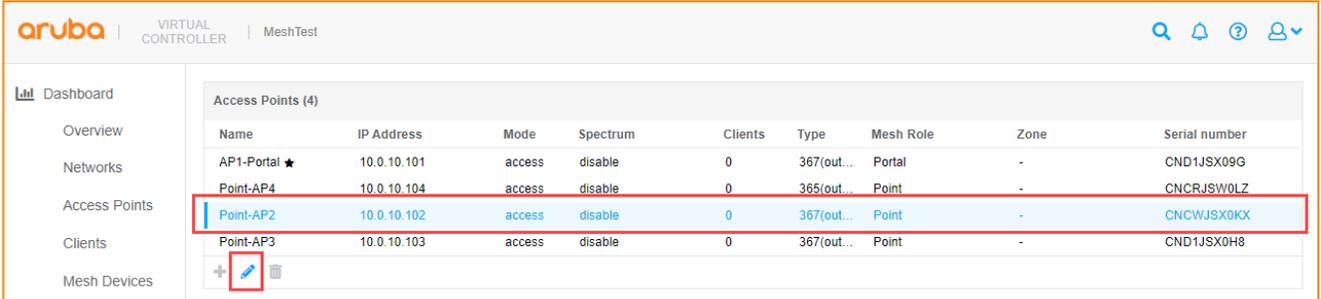
The screenshot shows the Aruba Virtual Controller configuration interface for a device named 'MeshTest'. The left sidebar contains navigation options: Dashboard, Configuration (with sub-items: Networks, Access Points, System, RF, Security, IDS, Routing, Tunneling, Services, DHCP Server), Maintenance (with sub-items: About, Firmware, Configuration, Certificates, Reboot, Convert, Regulatory, Option 82 XML), and Support. The main configuration area is under the 'General' tab. Various settings are visible, including Name (MeshTest), System location, Virtual Controller IP (0.0.0.0), and several toggle switches. The 'Extended SSID' toggle switch is highlighted with a red rectangular box.

3. Click 'Save' in the bottom right. It will prompt that the APs should be rebooted, but do not reboot them yet and close the prompt.
4. Go to 'Configuration > Access Points' and click on each AP that will be deployed as a mesh point (aka an access point that will not be connected to the LAN).

The screenshot shows the 'Access Points (4)' table in the Aruba Virtual Controller configuration interface. The table has the following columns: Name, IP Address, Mode, Spectrum, Clients, Type, Mesh Role, Zone, and Serial number. The row for 'Point-AP4' is highlighted with a red rectangular box.

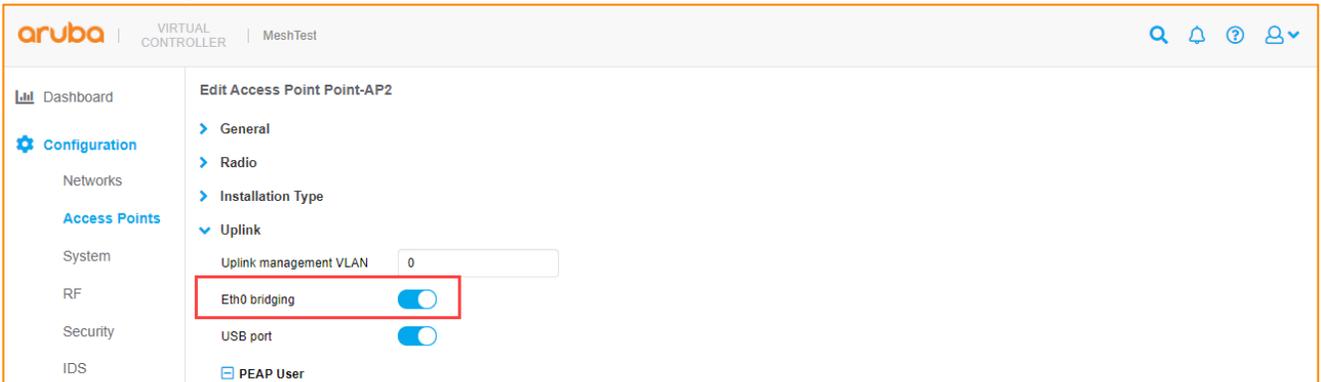
Name	IP Address	Mode	Spectrum	Clients	Type	Mesh Role	Zone	Serial number
AP1-Portal ★	10.0.10.101	access	disable	0	367(out...	N/A	-	CND1JSX09G
Point-AP4	10.0.10.104	access	disable	0	365(out...	N/A	-	CNCRJSW0LZ
Point-AP3	10.0.10.103	access	disable	0	367(out...	N/A	-	CND1JSX0H8
Point-AP2	10.0.10.102	access	disable	0	367(out...	N/A	-	CNCWJSX0KX

5. Click on each AP that should be a mesh point, until it turns blue, then click on the pencil to 'edit' that AP's config.



Name	IP Address	Mode	Spectrum	Clients	Type	Mesh Role	Zone	Serial number
AP1-Portal	10.0.10.101	access	disable	0	367(out...)	Portal	-	CND1JSX09G
Point-AP4	10.0.10.104	access	disable	0	365(out...)	Point	-	CNCRJSW0LZ
Point-AP2	10.0.10.102	access	disable	0	367(out...)	Point	-	CNCWJSX0KX
Point-AP3	10.0.10.103	access	disable	0	367(out...)	Point	-	CND1JSX0H8

- Click on 'Uplink' and select 'Eth0 Bridging' to enable it (aka it should turn blue) to tell the mesh point to use wireless as the uplink.



Edit Access Point Point-AP2

- General
- Radio
- Installation Type
- Uplink
 - Uplink management VLAN: 0
 - Eth0 bridging**
 - USB port
 - PEAP User

- Click 'Save'. It will prompt to reboot the AP again, but ignore that message and close the prompt.
- Repeat steps 5-7 for each AP that needs to be configured as a mesh point.
- Once all planned mesh points have had Eth0-bridging enabled, go to 'Maintenance > Reboot' and reboot the VC.

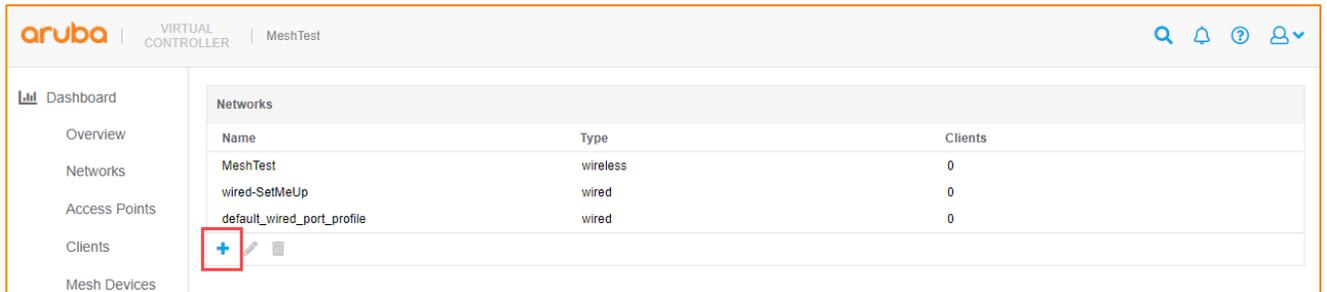
Important Note: Once the APs have been rebooted, they need to be disconnected from the wired network to prevent a network loop. If the mesh point is left wired to the LAN and the mesh uplink forms, a loop could form that would bring down the network.

Once all the APs have been rebooted, with the portal AP up and active, the mesh point APs will connect to the portal to bridge their traffic over the mesh link. In the VC, once logged in, go to 'Mesh Devices' to see all the mesh APs up, network stats, etc.

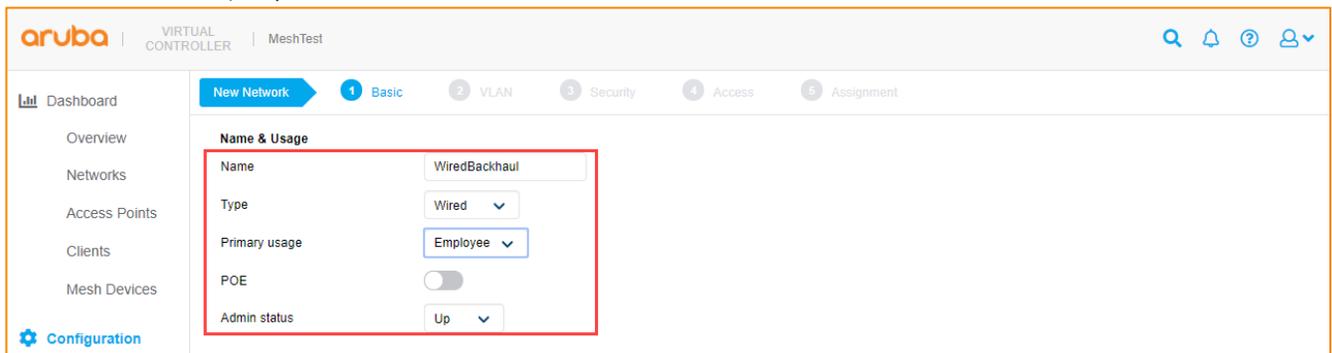
MESH SETUP WITH WIRED BACKHAUL

If there is a need to connect a 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.

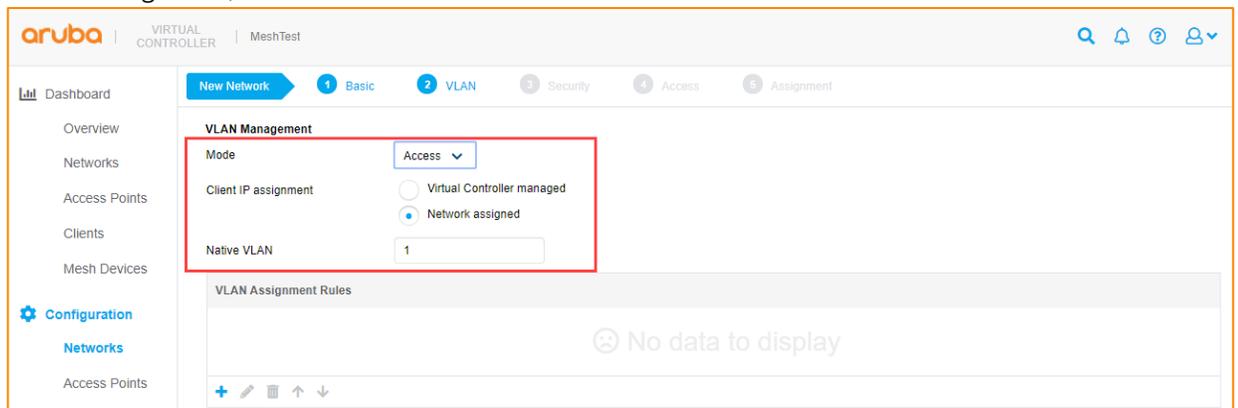
- On the VC, click on 'Configuration > Networks', click on the blue '+' sign to add a new wired network profile.



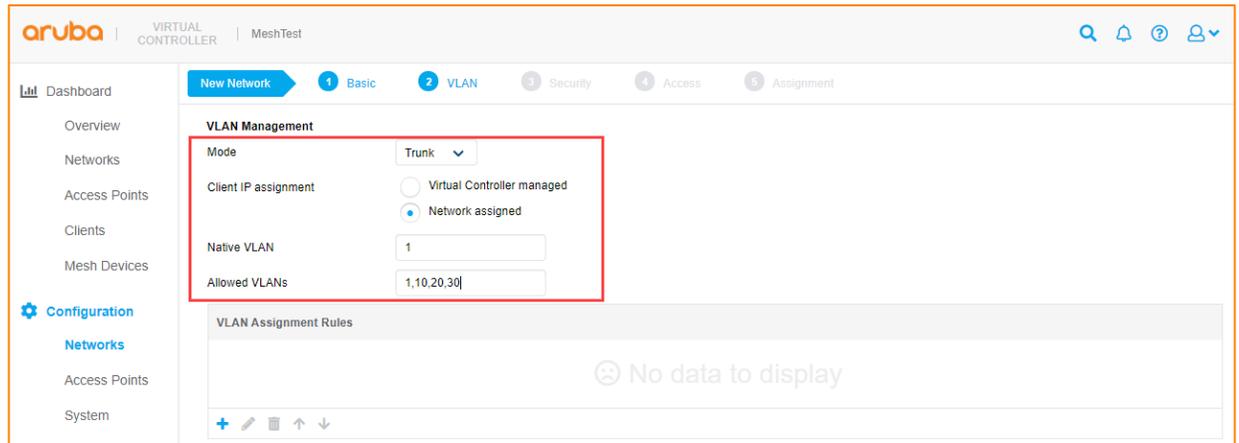
- Name the new wired profile with something that makes sense to this location (aka 'ParkingLotWiredNetwork' or 'RemoteMeshWired', etc).



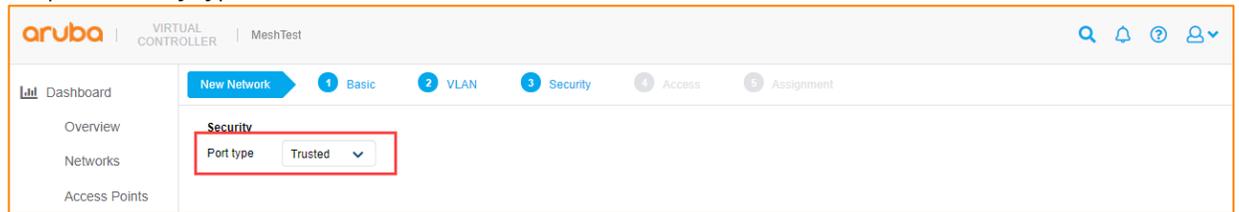
- Set the type to 'Wired', primary usage to 'Employee', and admin status as 'Up'.
- Define the wired port settings similar to what you have on the switched network that the portal is connected to:
 - If the portal is on a flat single VLAN, then 'access' mode can be set, with 'Network Assigned' set for the client IP assignment, and native VLAN set to '1'.



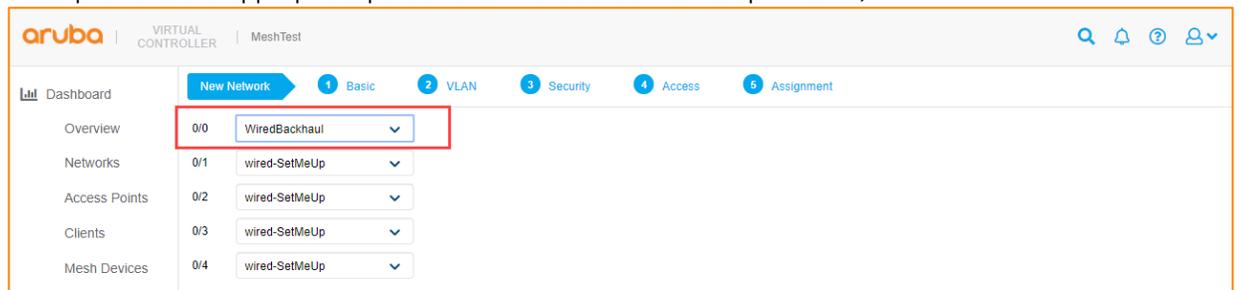
- If the portal is connected to a trunk port to carry multiple VLANs, either for the client SSIDs or specific VLANs of wired VLAN traffic, set the mode to 'Trunk', define native VLAN as 1, and add in the trunked VLANs the mesh should carry back from the remote switch to the portal.



- c. Set port-security type to 'Trusted' and click 'Next'.

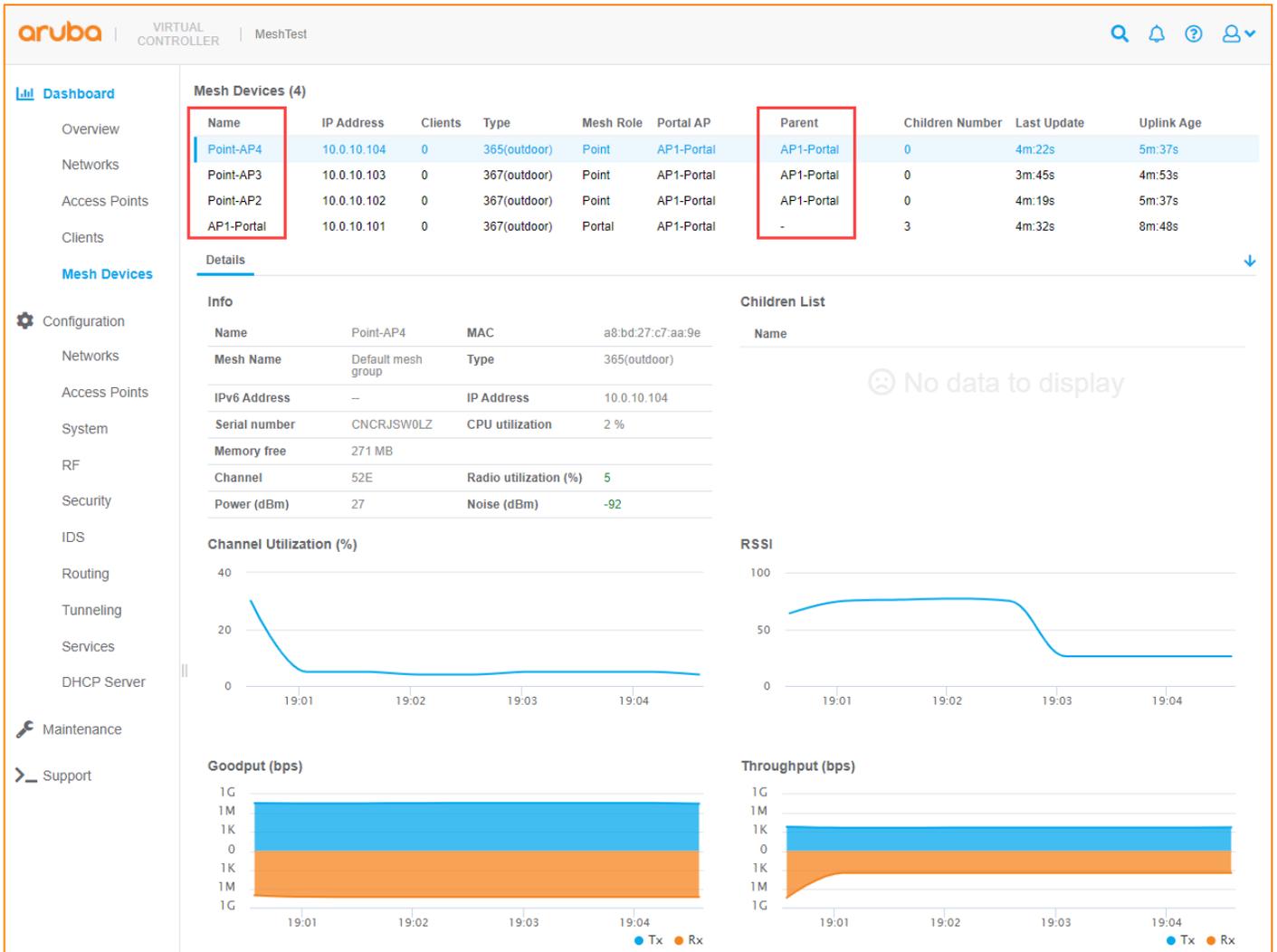


- d. There are no access rules to define, so click 'Next'.
- e. Assign the new wired port profile to Ethernet port '0/0' (if you have multi-port APs, assign the new wired profile to the appropriate port on the AP that the switch is uplinked to).



- f. Click 'Finish'.

5. Once done, all APs on that Virtual Controller cluster will be configured for that new wired port profile on all mesh points where Eth0-Bridging is enabled.



CONCLUSION

Using the information in this document, a quick and capable Instant-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

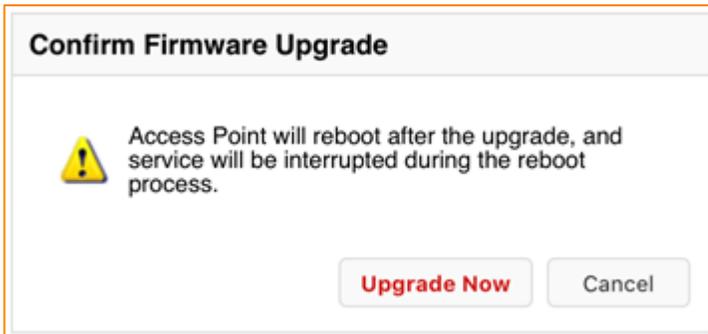
- <https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/EntryId/28815/Default.aspx>

APPENDIX - UNIVERSAL AP (UAP) SETUP

Most modern Aruba APs are 'Universal APs' (UAPs) which allows the access point to automatically determine if it should deploy as an Instant AP (IAP) or as a controller-based Campus AP (CAP). In cases where there is not an already existing Instant or Campus deployment, and if there is not a provisioning rule in Activate, or the UAP cannot reach the internet, the APs can come up with the UAP provisioning screen. If that happens for a new deployment, the following steps will walk through how to provision the UAP as an Instant AP (IAP). After provisioning the UAP as an IAP, the steps in this document can then be followed.

1. Log in to the AP using 'admin/admin'.
2. The provisioning page will display. If loading Instant OS, download from <https://asp.arubanetworks.com> the appropriate AP image named in the image file type (in the below example, the image name is 'Scorpio').

3. Once the file is loaded, the UAP will prompt to confirm the firmware upgrade.



4. Once the Instant OS is loaded, the UAP will reboot and will come up with the Instant OS login.
 - a. If the OS version is 8.4 and previous, the login will be 'admin/admin'.
 - b. If the OS version is 8.5 and later, the login will be 'admin/<serial number>'.

03.30.20