

# **DEPLOYMENT GUIDE – ARUBA MESH WITH CENTRAL** USING ARUBA CENTRAL WITH INSTANT ACCESS POINTS

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 Central with Instant Access Points (APs) can be implemented. Using Central for cloud management and Instant Mesh within a Virtual Controller (VC), it's easy 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. Central and 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. Additionally, the APs reporting up to Central allow for remote monitoring and management of the deployed networks via the cloud.

# **TABLE OF CONTENTS**

What Is Mesh?	.1
How to set Instant Mesh within a Virtual Cluster (VC) managed by Central	.2
Initial Staging of Central	.2
Configure the New Mesh AP Group Settings	.5
Assigning APs to the Newly Created Central Group1	11
Configuring the APs in Central1	13
Configure the Mesh Points 1	17
Mesh Setup with Wired Backhaul	8
Conclusion	22

# 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 multihop mesh (Figure 3) below.



With Central and 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) MANAGED BY CENTRAL

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

- On the network where these new APs are deployed, these are the only Instant APs on that L2 network/VLAN, and the APs will have access to Central in the cloud.
- 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 configured are part of the mesh and are in the same group within Central. 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, and all devices have access to the Internet for Central management
- Instant OS version 8.5 or 8.6 or later under Central
- If there are any other deviations or accommodations that need to be made, please consult your Aruba SE or Partner

# **INITIAL STAGING OF CENTRAL**

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 Central with Instant AP deployment. Because this guide is assuming a new deployment in Central, there are some steps to follow first within Central before connecting and configuring the APs. In addition, Central allows for most of the configuration to be deployed before the APs are brought up, allowing for more rapid staging of hardware once on site.

1. Log in to Central and click on the account where the new APs will be deployed

SELECT ACCOUNT	
۹ Search	
Acme Mesh Demo CID: ad2240ef8b7b46f09096f6569533c19c	
4	Þ

2. When logging in for the first time, there will be a prompt to add new devices to the Central account. This can be done now within the prompt or can wait until later on in the staging process.

GET STARTED WITH AR		~	KIT WORKFLOW
ADD DEVICES	ADD DEVIC Add up to 100 devices by er Address for each device	ES Attended of the Serial Number and MAC	your devices via the mobile app. They appear here.
VIEW DEVICES ♡ TYPE	serial number CNFFK80007 Device added successfully	AAC ADDRESS A8:bd:27:cf:f6:08	7 MODEL
	SERIAL NUMBER CNFFK8101S Device added successfully	MAC ADDRESS a8:bd:27:cf:f8:ae	
	SERIAL NUMBER CNFFK81020 Device added successfully	a8:bd:27:cf:f8:ea	
	SERIAL NUMBER CNFFK80003 Device added successfully	a8:bd:27:cf:f5:e0	
		MAC ADDRESS	
CANCEL	ADD MORE DEVICES	DONE	

 After adding devices, or after skipping this step to add the devices later, the 'Account Home' page will be displayed. This is the main page used for adding licenses, subscriptions and devices to the Central account. Assuming the Subscriptions and the Device Inventory has been added, click on 'Network Operations' to log into the Central management dashboard

the central manageme		
ACCOUNT HOME Manage your Network Inventory, Subscripti better for you.	ions, and User Access. Use any of the followi	ng apps to make Aruba work
APPS		
Network Operations Manage your wired, wireless, and WAN infrastructure	ClearPass Device Insight Discover and Profile devices connected to the network	
LAUNCH	GET STARTED	
GLOBAL SETTINGS		
USERS AND ROLES Manage user access	KEY MANAGEMENT Manage your subscription keys	
DEVICE INVENTORY Manage the Devices in your inventory	SUBSCRIPTION ASSIGNMENT Assign and modify device and service subscriptions	
AUDIT TRAIL View audit-trail logs	SINGLE SIGN ON Create and manage SAML Profiles	
API GATEWAY Access API Gateway and manage access tokens	WEBHOOKS Manage Webhook end points	

4. Once logged in to the main page, in the top-left, click on 'All Groups' and click on the 'Groups' link with the gear icon. This will open up the 'Groups' page where a new group will be created for the new mesh APs.

Central	Q Search or ask Aruba	۹ 🛛 🚟 🖧
	WI-FI NNECTIVITY	Q AI Early CISUALRF II ∷≡
ALL DEVICES		NO ISSUES     POTENTIAL ISSUES
GROUPS ®	CES	WAN
default	HIGH CH UTILIZA	TION HIGH NOISE UPLINKS STATUS TUNNELS STATUS
LD CLIENTS UP DOWN	2.4 GHz 5 GHz	2.4 GHz 5 GHz NO ISSUES DOWN NO ISSUES DOWN
APPLICATIONS     +	O c e a n	SYRIA IRAQ IRAN AFGHANISTAN
SECURITY Sargasso	ALGERIA	BYA EGYPT KUWAIT PAKISTAN NEP
쓚 NETWORK SERVICES	WESTERN SAHARA MAURITANIA	SAUDI ARABIA OMAN INDIA

5. In the 'Create New Group' prompt, enter a name for the new mesh AP group, uncheck 'IAP and Gateway' as well as 'Switches' as we are not creating any template groups. Enter a password for the new group as this will be the password applied to the individual devices within that group should they need to be accessed.

CREATE NEW GROUP	>
group name Acme Mesh	
Use the group as Template group by selecting the device ()	
Group password settings	
CONFIRM PASSWORD	
Cancel Add Group	

6. With the new mesh AP group created, mouse over the new mesh AP group and click on the 'Config' button to open the Group Configuration page.



# **CONFIGURE THE NEW MESH AP GROUP SETTINGS**

With the new mesh AP group created under Central, the following steps will go through creating the group settings so that once the new APs are brought up in Central and assigned to the mesh AP group, it can more quickly inherit the settings to make the deployment go faster.

1. Inside the new AP group, under Access Points, click on the 'WLANs' tab and click the "+ Add SSID" button in the lower-left

aruba Central		Q Sea	rch or ask Aruba				۹ 🕐 🏭 🕅
√ Acme Mesh							
🛱 GROUP	ACCESS POINTS	SWITCHES	n GATEWAYS				⊞ ılı 🕸
- MANAGE	WLANS ACCESS POINTS	RADIOS					Show Advanced
B OVERVIEW							
DEVICES	Wireless SSIDs						
CLIENTS	NAME	SECURITY	ACCESS TYPE	ZONE	TRAFFIC FO	NETWORK	ACTIONS
APPLICATIONS							
SECURITY				FA			
- ANALYZE							
ALERTS & EVENTS				₹ ■ 差			
AUDIT TRAIL				No data to display			
🖏 tools							
REPORTS							
MAINTAIN	+ Add SSID						0 SSID(s)
FIRMWARE							

<b>Orubo</b> Central	Q Search or ask Aruba	۵ 🗰 🛍
√ Acme Mesh		
🛱 GROUP	ත් ACCESS POINTS 📼 SWITCHES 🙊 GATEWAYS	⊞ th 🕸
MANAGE	WLANS ACCESS POINTS RADIOS	Show Advanced
CVERVIEW		
DEVICES	CREATE A NEW NETWORK	
CLIENTS	1 General (2) VLANs (3) Security (4) Access (5) Summary	
APPLICATIONS		
SECURITY	Name (SSID):	
- ANALYZE	Advanced Settings	
	/ nounced sectings	
AUDIT TRAIL		
🖏 tools		
REPORTS		Cancel Next
- MAINTAIN		
FIRMWARE		

2. Create the SSID(s) to be used by the clients for this deployment and click 'Next'

3. Configure the VLAN and network settings for the user SSID being created. Note this configuration is ultimately decided by how the APs are uplinked to the network. If an SSID needs to be in a trunked VLAN on the AP's uplink port, then the appropriate VLAN settings should be applied. In this example, the users will be on the same flat VLAN as the APs. Click 'Next' when done.

<b>Orubo</b> Central	🔾 Search or ask Aruba
ជ GROUP	🔯 ACCESS POINTS 📼 SWITCHES 🙊 GATEWAYS 😑 11. 😵
MANAGE	WLANS ACCESS POINTS RADIOS Show Advanced
B OVERVIEW	
	CREATE A NEW NETWORK
CLIENTS	1 General 2 VLANs (3) Security (4) Access (5) Summary
APPLICATIONS	
SECURITY	Client IP Assignment: Instant AP assigned External DHCP server assigned
- ANALYZE	Client VLAN Assignment: Static Dynamic Native VLAN
AUDIT TRAIL	
🖏 tools	
REPORTS	Cancel Back Next
- MAINTAIN	
FIRMWARE	

4. Configure the appropriate security settings required for this new SSID. The below example is a WPA3-PSK SSID, but if other security settings are required (Open, WPA2-PSK, RADIUS-based solutions, etc.), please set accordingly. Click 'Next'

<b>Central</b>	<b>Q</b> s	jearch or ask Aruba	۹ 🛛 🗰 🖞
√ Acme Mesh			
ଘ group	O ACCESS POINTS SWITCHES	GATEWAYS	⊞ ılı 🐵
- MANAGE	WLANS ACCESS POINTS RADIOS		Show Advanced
H OVERVIEW			
DEVICES	CREATE A NEW NETWORK		
CLIENTS	1 General 2 VLANs	s 3 Security 4 Access 5 Summary	
APPLICATIONS			
SECURITY			
- ANALYZE	Security Level:	O	
ALERTS & EVENTS		Enterprise Personal Captive Portal Open	
AUDIT TRAIL			
🖏 TOOLS	Ver Managements		
🔝 REPORTS	key Management:	WPAS-Personal V	
- MAINTAIN	Passphrase Format:	8-63 chars 🔻	
FIRMWARE	Passphrase:		
	Retype:		
	> Advanced Settings		
		Cancel	Back

5. Apply any SSID Access Rules required. The below example is open to all traffic, but if a specific security policy is required, please configure accordingly. Click 'Next'

Central	Q Search or ask Aruba	۹ 💿 腸 🖞
ដ្ឋ GROUP	🗑 ACCESS POINTS 📼 SWITCHES 🏩 GATEWAYS	⊞ di 🚳
- MANAGE	WLANS ACCESS POINTS RADIOS	Show Advanced
DEVICES	CREATE A NEW NETWORK	
ED CLIENTS     APPLICATIONS     SECURITY     ANALYZE     ALERTS & EVENTS     ALERTS & EVENTS     AUDIT TRAIL     TOOLS     REPORTS     MAINTAIN     FIRMWARE	General 2 YLANs 3 Security Cecess Summary   Access rules   Role Based Network Based Unrestricted   Unrestricted option allows full access to the network. This may lead to potential security issues.   Downloadable   Role:	el Back Next

6. Review all elements configured for the new SSID in the 'Summary' page, if it all looks correct, click 'Finish'. Once 'Finish' is clicked, a popup will indicate the SSID was created.



7. Next, click on the 'Radios' tab. Because in most cases for an outdoor AP mesh deployment, the APs being outdoors requires higher power levels to ensure range and coverage. As such, the 'Radio' settings should be modified so that ARM applies a higher power level to the APs radios. On the 'Radios' page, under 'Access Point Control', set the Min Transmit Power to '24' and the Max Transmit Power to 'Max'. Additionally, disable 80Mhz wide channels as well as 160Mhz wide channels if present.



8. Additionally, within the 'Radio' tab, click on 'Radio' tab, and on the 5Ghz band modify the 'default' 5Ghz radio profile by clicking on the pencil icon.

aruba Central			Q Search or ask Aru	ba				۵ 🕲 腸
√ Acme Mesh								
ଘ GROUP	C ACCESS POINT	s 📼 switches	GATEWAYS					։≘ մե 🛞
- MANAGE	WLANS ACCESS PC	NINTS RADIOS						Show Advanced
DEVICES	RF							
CLIENTS	> Adaptive R	adio Managemer	nt(ARM)					
APPLICATIONS	✓ Radio							
SECURITY								
- ANALYZE	2.4 GHz band	I		+	5 GHz band			+
ALERTS & EVENTS	NAME	ZONE	MIN/MAX PO	=	NAME	ZONE	MIN/MAX PO	=
AUDIT TRAIL	default		6/9		default		12/18	
🖏 tools								

9. Check the 'Custom ARM Power Range' and modify the maximum and minimum to match Step 7.

DEFAULT	۷.	×
Channel Switch Announcement Count:	0	
Background Spectrum Monitoring:		
Customize ARM Power Range:		
Min Transmit Power:	24	
Max Transmit Power:	Max V	
Enable 11ac:		
Smart antenna:		
ARM/WIDS Override:	Off V	
Const		Sava
		Save

10. Next, the new Group 'System' configurations need to be applied. This consists of assigning a country code and time zone to the 'System' settings in the group. Additionally, because the APs in this group will be doing mesh, the 'Extended SSID' should be disabled. Once done, click 'Save Settings'.

aruba Central		Q Search or ask Aru	ba		۹ 🕲 腸					
\nother										
멻 GROUP	🖯 ACCESS POINTS 📼 SWITCH	ies 🙊 gateways			i≣ di 🚳					
- MANAGE	WLANS ACCESS POINTS RADIOS	PORTS SECURITY VPN SER	VICES SYSTEM CONFIGURATIO	N AUDIT	Hide Advanced					
B OVERVIEW										
	SYSTEM									
CLIENTS	∨ General									
APPLICATIONS	Matual Cantuallan									
SECURITY	Virtual Controller									
- ANALYZE	NAME	NAME IP ADDRESS IPV6 ADDRESS COUNTRY CODE								
ALERTS & EVENTS										
AUDIT TRAIL										
S TOOLS			玉囲左							
REPORTS			No data to display right now							
			1 7 6							
	Set Country code for group :	US - Ur	ited States	•						
		Reboot A	P for changes to take effect.							
	Timezone :	Pacific-	Time UTC-08	•						
		The selecter	d country observes Daylight Savings Tir	ne						
	Telnet Server :									
	LED Display :		)							
	Extended SSID :		]							
	Advanced Zone :									

11. The last step in staging the Central group settings is to set 'Manage Firmware Compliance' for the devices assigned to this group. This will save some time so that once APs are assigned to this group, Central will automatically upgrade them to the specified version. Back on the main page under the new Central 'Group', click on 'Firmware', and go to the 'Access Points' tab. In the top-right, there is a 'Manage Firmware Compliance' link and once clicked, a popup will appear to define the group to apply the compliance policy to, as well as which version to apply. Once done, click 'Save and Upgrade'. No APs will be in this group once clicked, so there won't be anything to actually upgrade. But if APs are assigned to that group, they will start to upgrade.

aruba Central			Q Search or as				۹ 🕐 🏭 🖁
\overline Acme Mesh     \overline							3 HOURS
멻 GROUP	C ACCESS POINTS	SWITCH - M	AS 📼 SWITCH - A	RUBA 🧟 GATEWAYS			
MANAGE							
B OVERVIEW	Filter By Upgrade Stat	us				🐯 Manag	ge Firmware Compliance
DEVICES	Show All	<b></b>					
CLIENTS	ACCESS POINTS						
APPLICATIONS	NAME	APS	FIRMWARE VERS	RECOMMENDED VER	UPGRADE STATUS		COMPLIANCE STATUS
SECURITY							
- ANALYZE							
ALERTS & EVENTS							
AUDIT TRAIL							
🖏 tools							
REPORTS							
- MAINTAIN	1 /	-			_		
© FIRMWARE		Manage	firmware complian	ce			
		Groups ACME ME	SH		•		
		Firmware Ve	rsion				
		8.6.0.3_74	4788		<b>T</b>		
		Now	U Later Date				
				Cancel Save and U	Jpgrade		

# ASSIGNING APS TO THE NEWLY CREATED CENTRAL GROUP

With the new Central group defined and pre-staging settings applied, the APs can now be assigned to the new group from the 'default' group where new APs show up in Central.

 From the 'Global > All Devices' page in Central, go to 'Organization' in the lower-left and click on the 'Groups' tab. The newly deployed APs will show up in the 'default' group and will be visible in the right pane. Click and drag the Virtual Controller (VC) from the right pane into the newly created Central group.



2. A confirmation dialogue box will appear to confirm the move.



3. Once moved, the new Central group will reflect the new device(s) in the group. Click on the 'Config' button.



4. Clicking on the 'Firmware' link in the lower left should show the newly added APs upgrading to the firmware version defined in the 'Manage Firmware Compliance' in a previous step. If so, wait for the APs to finish upgrading before moving on.

# **CONFIGURING THE APS IN CENTRAL**

After the firmware is finished upgrading to the specified version, the APs are ready to be configured. This includes naming the APs, setting any AP specific configuration elements, and configuring the mesh points.

 Go to the new Central group, click on 'Devices', and under 'Access Points', the new APs should show up with the default Virtual Controller (VC) name and the AP names should be their wired MAC address. To start, click on 'Show Advanced' and click on the 'System' tab. The default 'SetMeUp' Virtual Controller (VC) should be present. Click on the pencil to edit the VC.

orubo Central		Q Search or ask	Aruba		۹ 🛛 🟭 🖞
\not Acme Mesh     ▼					
😭 GROUP	O ACCESS POINTS SWITCHE	s 🙊 gateways			ii ii 😵
- MANAGE	WLANS ACCESS POINTS RADIOS F	PORTS SECURITY VPN S	ERVICES SYSTEM CC	ONFIGURATION AUDIT	Hide Advanced
E OVERVIEW	· · · · · · · · · · · · · · · · · · ·				
DEVICES	SYSTEM				
CLIENTS	∨ General				
APPLICATIONS					
SECURITY	Virtual Controller				
- ANALYZE	NAME	IP ADDRESS	IPV6 ADDRESS	COUNTRY CODE	=
ALERTS & EVENTS	SetMeUp-CF:F8:AE			US	
AUDIT TRAIL	5 10 25 50 Per Page				K < > > Page: 1/1
🖏 tools					
REPORTS	Set Country code for group :	US -	United States	<b>v</b>	
- MAINTAIN	Timezone :	Paci	fic-Time UTC-08	•	
FIRMWARE		The sele	cted country observes Daylig	ght Savings Time	
	Preferred Band :	All	▼		

2. A pop-up will appear to name the VC and assign a virtual IP to the cluster (optional). Click 'OK' when done.

EDIT IP ADDRESS	×
Name :	AcmeMeshCluster
IP Address :	192.168.170.99
IPv6 Address :	)00000000C
G	) IPv6 Management should be enabled.
Country Code :	
US - United States	▼
Cancel	ок

3. Once the 'System' settings are done, go back to the 'Access Points' tab and click on the AP that will be designated the portal. Once highlighted, click the pencil icon.

Central				Q Search or ask Arub	3				۵ 🗰 🕺		
\overline Acme Mesh     \overline											
멻 GROUP	🗟 ACCESS POINTS 📼 SWITCHES 🙊 GATEWAYS 🗄 11. 🚳										
- MANAGE	WLANS ACCESS POINTS RADIOS Show Advanced										
B OVERVIEW			_								
	ACCESS POINTS 4Access Points										
CLIENTS	Arross Daints										
APPLICATIONS											
SECURITY	NAME	VC NAME	STATUS	IP ADDRESS	IP ASSIGN	MODE	TYPE	2.4 GHz (C	5 GHz (Cha		
- ANALYZE	• a8:bd:27	SetMeUp-C	Online	192.168.170.114	DHCP	access	AP-375	Auto	Auto		
▲ ALERTS & EVENTS	• a8:bd:27	SetMeUp-C	Online	192.168.170.111	DHCP	access	AP-375	Auto	Auto 🖉		
🗖 AUDIT TRAII	• a8:bd:27	SetMeUp-C	Online	192.168.170.112	DHCP	access	AP-377	Auto	Auto		
A TOOLS	• a8:bd:27	SetMeUp-C	Online	192.168.170.113	DHCP	access	AP-377	Auto	Auto		
TOULS	5 10 25 5	50 Per Page							< < > >  Page: 1/1		
REPORTS											
- MAINTAIN											
FIRMWARE											

4. Name the portal in accordance with your naming convention to identify this AP as the portal. Additionally, the portal should be defined as the "Preferred Master" to ensure the VC master is on the wired network. Click 'Submit when done.

Central		Q Search or ask Aruba	۹ 🕲 腸
🛱 GROUP	access points SWITCHES	A GATEWAYS	⊞ II. 🕸
- MANAGE	WLANS ACCESS POINTS RADIOS		Show Advanced
OVERVIEW			
DEVICES	ACCESS POINTS / A8:BD:27:CF:F6	08	
CLIENTS	✓ Basic Info		
APPLICATIONS	News		
SECURITY	Name:	APT	
- ANALYZE	AP Zone:		
ALERTS & EVENTS	PE Profile:		
AUDIT TRAIL	ki Hone.		
🖏 tools	Swarm Mode:	Cluster 🔻	
REPORTS	Preferred Master:		
- MAINTAIN		Reboot AP for changes to take effect.	
FIRMWARE	IP Address For Access Point:	Get IP Address from DHCP server	
		Static	

5. There will be a prompt to reboot the AP, and it will ask if it should load the AP details page to reboot the AP. For now, click 'Cancel'.



6. Do the same thing for the APs that will be designated as the mesh point(s). Click on the APs that will be designated as mesh points, name them, and click 'Submit'

Central		Q Search or ask Aruba	۹ 🕲 👪 🗂
CI GROUP	ACCESS POINTS SWITCHES	A GATEWAYS	Ш db 🚳
- MANAGE	WLANS ACCESS POINTS RADIOS		Show Advanced
OVERVIEW			
	ACCESS POINTS / A8:BD:27:CF:F8:	AE	
CLIENTS	→ Basic Info		
APPLICATIONS			
SECURITY	Name:	AP2	
- ANALYZE	AP Zone:		
ALERTS & EVENTS	95 P. (1		
AUDIT TRAIL	RF Profile:		
🖏 tools	Swarm Mode:	Cluster 🔻	
REPORTS	Preferred Master		
- MAINTAIN	increment mosteri		
FIRMWARE	IP Address For Access Point:	Get IP Address from DHCP server	
		Static	

7. Once done, all APs should show up in the AP list with the proper name.

Central		Q Search or ask Aruba									പ്പ
🛱 GROUP	O ACCESS POINTS	WITCHES	GATEWAY	/S					≣	di.	ŝ
MANAGE											
OVERVIEW	ACCESS POINTS . UP	o DO	WN RADIO	S							
DEVICES	4 *		0	_							
CLIENTS	ACCESS POINTS								4	. OO	
			RAD	10 1	RAD	010 2					
AFFEICATIONS		1= C	CHANNEL	POWER (DBM)	CHANNEL	POWER (DBM)	Y IP ADDRESS ↓=			∀ SER	ы.
SECURITY	• AP1	1	40 (40 MHz)	15	1 (20 MHz)	9	192.168.170.111	AP-375		CNFFK8	30
- ANALYZE	• AP2 (VC)	1	08 (40 MHz)	18	6 (20 MHz)	9	192.168.170.112	AP-377		CNFFK8	31
ALERTS & EVENTS	• AP3	1	16 (40 MHz)	15	6 (20 MHz)	9	192.168.170.113	AP-377		CNFFK8	31
AUDIT TRAIL	• AP4	6	50 (40 MHz)	18	11 (20 MHz)	9	192.168.170.114	AP-375		CNFFK8	30

8. Once it's verified that all APs are named correctly, click on the current VC AP (identified by the "(VC)" label next to the AP). Once the page loads, in the top-right, there is an 'Actions' dropdown, select 'Reboot Swarm'.

Central		0	Search or ask Aruba				९ 🕐 🏭 🖁
	AP2 ×						S HOURS
ACCESS POINTS	SUMMARY						
	No downtime in the last	: 20 Minutes	DEVICE HEALTH • Good		RADIO 1 (5 GHz) • Good	RADIO 2 (2.4 GHz) • Good	VIRTUAL CONTROLLER
	ACCESS POINT DETAILS	AI INSIGHTS Early Access	USAGE	RF	TUNNELS	LOCATION	ACTIONS GO LIVE
<ul> <li>ANALYZE</li> <li>Δ ALERTS &amp; EVENTS</li> </ul>	DEVICE AP MODEL AP-377	COUNTRY CO	DE		NETWORK	SPEED (Mbps) / DUPLEX	
<ul> <li>AUDIT TRAIL</li> <li>TOOLS</li> </ul>	MAC a8:bd:27:cf:f8:ae	SERIAL NUME CNFFK8101	BER S		ETH1 O Down	SPEED (Mbps) / DUPLEX	CONSOLE VLAN



9. Once all the APs have rebooted, the designated VC AP should be identified as the 'VC' AP. The next steps will configure the mesh points.

aruba Central			Q Sea	rch or ask Aruba				م	0	<b>u</b> 8
\not \not \not \not \not \not \not \										
😭 GROUP	access points	SWITCHE	S 🙊 GATEWA	YS .					i 1	I. ®
- MANAGE										
OVERVIEW	ACCESS POINTS	• UP • D	OWN RADIC	S						
DEVICES	4	-	° 0	_						
CLIENTS	ACCESS POINTS								⊥	$\odot$
			RA	DIO 1		RADIO 2				
		1=	CHANNEL	POWER (DBM)	CHANNEL	POWER (DBM)	Y IP ADDRESS ↓=		Y	SERI.
SECURITY	• AP1 (VC)		44 (40 MHz)	12	6 (20 MHz)	9	192.168.170.111	AP-375	CI	VFFK80
- ANALYZE	• AP2		52 (40 MHz)	12	11 (20 MHz)	9	192.168.170.112	AP-377	Cl	VFFK81
ALERTS & EVENTS	• AP4		108 (40 MHz)	12	6 (20 MHz)	9	192.168.170.114	AP-375	CI	VFFK80
AUDIT TRAIL	• AP3		60 (40 MHz)	12	1 (20 MHz)	9	192.168.170.113	AP-377	CN	VFFK81

### **CONFIGURE THE MESH POINTS**

1. Once the APs have rebooted, the mesh points are ready to be configured to operate with mesh. For the APs to be configured as mesh points, click on each AP and click the pencil icon to edit the AP.

<b>aruba</b> Central		🝳 Search or ask Aruba									
🛱 GROUP	🞯 ACCESS P	J ACCESS POINTS									
- MANAGE	WLANS ACC	WLANS ACCESS POINTS RADIOS Show Advanced									
DEVICES	ACCESS PO	ACCESS POINTS 4 Access Points									
CLIENTS	Access Poi	nts									
APPLICATIONS											
SECURITY	NAME	VC NAME	STATUS	IP ADDRESS	IP ASSIGN	MODE	TYPE	2.4 GHz (	5 GHz (Ch 📃		
- ANALYZE	• AP4	AcmeMes	Online	192.168.1	DHCP	access	AP-375	Auto	Auto		
Δ ALERTS & EVENTS	• AP1	AcmeMes	Online	192.168.1	DHCP	access	AP-375	Auto	Auto		
	AP2	AcmeMes		192.168.1	DHCP				Auto 🖉		
AUDII IRAIL	<ul> <li>AP3</li> </ul>	AcmeMes	Online	192.168.1	DHCP	access	AP-377	Auto	Auto		
🖏 tools	5 10 25	50 Per Page									
REPORTS									rage. 1/1		

2. Enable 'Eth0 Bridging' on the mesh point and once done click 'Submit'.

aruba Central	Q Search or ask Aruba		Q	?:	<b>::</b> A	
ជ្ជ GROUP	🗑 ACCESS POINTS 📼 S	SWITCHES		:	:≣ il	. 🕸
- MANAGE	WLANS ACCESS POINTS RA	RADIOS		SI	how Ad	lvanced
DEVICES	ACCESS POINTS / AP2					
CLIENTS	> Basic Info					
APPLICATIONS	> Radio					
SECURITY ANALYZE ————————————————————————————————————	> Installation Type					
ALERTS & EVENTS	$\vee$ Uplink					
AUDIT TRAIL	Uplink Management	0				
🖏 TOOLS	VLAN:					
REPORTS     MAINTAIN	Preferred Uplink:	1				
🔅 FIRMWARE	Eth0 Bridging:					
	T a d d c n b a h	The eth0 port a an active netwo the eth0 bridgin could cause inau network. Are yo bridging mode r and then recom has taken effect	ppears to be currently connected to rk device. Please note that changing ig mode while the port is in active use divertent issues in your wired u sure you want to change the eth0 now? If not, please disconnect eth0 nect it after the new bridging mode 			

3. Once submitted, a popup will prompt to reboot the AP and will redirect to the AP details page. Click 'Cancel' as we will configure all the points and then reboot them all together. However, if you want to reload the AP to deploy as they are configured one by one, reboot the AP and once it reboots, disconnect from the network and power up off the network to ensure that it comes up as a mesh AP before taking it to its final location.

NOTE: As there can be a slight delay between submitting a change from Central to the AP, and then the AP writing the actual command into its configuration, it is a best practice to wait at least 1-2 minutes after making a configuration change before rebooting and disconnecting the AP from the network. Otherwise, the configuration for 'Eth0 Bridging' may not get written to the AP and as a result, the AP may not come up on mesh until it's reconnected to the network to fully inherit its config.

Please reboot the access point for the changes to take effect. You can reboot the device from the access point details page. Do you want to go to the access point details page now?

<b>Orubo</b> Central		Q Search	or ask Aruba			۵ 🕲 🗰
\nother Acme Mesh     \nother      \no	AP2 ×					S HOURS
ତ୍ତି ACCESS POINTS	SUMMARY					
- MANAGE		1	DEVICE HEALTH	RADIO 1 (5 GHz)	RADIO 2 (2.4 GHz)	VIRTUAL CONTROLLER
	No downtime in the	e last 22 Minutes	• Good	• Good	• Good	AcmeMeshCluster
CLIENTS	ACCESS POINT DETAI	ILS				ACTIONS V GO LIVE
- ANALYZE	OVERVIEW	AI INSIGHTS Early Access	USAGE	RF	LOCATION	REBOOT AP
	DEMOS			NETHODY		REBOOT SWARM
AUDIT TRAIL	AP MODEL	COUNTRY COL	DE	ETHO	SPEED (Mbp	TECH SUPPORT
🖏 TOOLS	AP-377	US		• Up	1000 / Full	CONSOLE
- -	MAC a8:bd:27:cf:f8:ae	SERIAL NUMBI CNFFK81015	ER S	VLAN Trunk (1)	LLDP Details	

4. Once all the mesh point APs have been configured, the resulting network should have the portal AP up along with all mesh points up in Central.

#### **MESH SETUP WITH WIRED BACKHAUL**

If there is a need to connect a switch or a wired device 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 Central, in the newly created Central group, click on 'Devices' and then 'Show Advanced' under 'Access Points' and click on 'Ports' to show the 'Wired Port Profile' settings for the APs.

<b>Orubo</b> Central		Q Search or ask Aruba			۹ 🛛 👪 🕅
√ Acme Mesh					
멻 GROUP	🗑 ACCESS POINTS 📼 SWITCHES 🗣	GATEWAYS			⊞ ılı 🛞
- MANAGE	WLANS ACCESS POINTS RADIOS PORTS	SECURITY VPN SERVICES SYSTEM CONFIGL	RATION AUDIT		Hide Advanced
B OVERVIEW					
DEVICES	Wired Port Profiles				
CLIENTS	NAME	TYPE	ACCESS TYPE	ACTIONS	
APPLICATIONS	default_wired_port_profile	Mixed traffic	unrestricted		
SECURITY	wired-SetMeUp	Mixed traffic	network-based		
- ANALYZE					
ALERTS & EVENTS					
AUDIT TRAIL					
🖏 tools					
REPORTS					
- MAINTAIN	+ Add Port Profile				2 Port Profile(s)
FIRMWARE	Port Profiles Assignments				
	Ethernet 0/0:	default_wired_port_profile			
	Ethernet 0/1:	wired-SetMeUp			
	Ethernet 0/2:	wired-SetMeUp			
	Ethernet 0/3:	wired-SetMeUp			
	Ethernet 0/4:	wired-SetMeUp			

2. Create a new 'Wired Port Profile' that will be assigned to the APs in this Central group. Provide a name to use for this new profile and click 'Next'.

Central	Q Search or ask Aruba	۵ 🗰 🗂
Y Acme Mesh		
🛱 GROUP	O ACCESS POINTS SWITCHES A GATEWAYS	≡ n ®
- MANAGE	WLANS ACCESS POINTS RADIOS PORTS SECURITY VPN SERVICES SYSTEM CONFIGURATION AUDIT	Hide Advanced
B OVERVIEW		
DEVICES	CREATE A NEW NETWORK	
CLIENTS	1 General (2) VLANS (3) Security (4) Access (5) Summary	
APPLICATIONS		
SECURITY	Port Profile Name: Acme Wired Backhaul	
- ANALYZE	Advantal Cation	
Д ALERTS & EVENTS	> Auvanced Settings	
AUDIT TRAIL		
🔦 TOOLS		
REPORTS		Cancel Next
- MAINTAIN		
FIRMWARE		

3. Configure the network settings for the AP's wired port. Note this will depend on the wired network uplink config on the portal's side as well as the mesh point side. Because Instant Mesh bridges, the network settings should match on each side for the AP's uplink and downlink interfaces. By default, the setting is 'Trunk' mode, native VLAN of '1', and 'all' VLANs are allowed to ensure maximum compatibility. Set as required for your site. Click 'Next'.

orubo Central	Q Search or a	ask Aruba		۵ 🗰 🙈
🛱 GROUP	ⓓ ACCESS POINTS			⊞ 1h 🛞
- MANAGE	WLANS ACCESS POINTS RADIOS PORTS SECURITY VPN SERVICES SY	STEM CONFIGURATION AUDIT		Hide Advanced
B OVERVIEW				
DEVICES	CREATE A NEW NETWORK			
🗂 CLIENTS	1 General 2 VLANS 3 Security 4 Acc	ess (5) Summary		
APPLICATIONS				1
SECURITY	Mode:	Trunk 🔻		
- ANALYZE	Client IP Assignment:	<ul> <li>Instant AP assigned</li> </ul>	External DHCP server assigned	
ALERTS & EVENTS	Client VI AN Assignment	Default	Custom	
AUDIT TRAIL	Circle VENA Assignment			
🖏 TOOLS	Allowed VLAN:	all ×	Ŧ	
REPORTS				
- MAINTAIN				
FIRMWARE				
			(	Cancel Back Next

4. If necessary, created a wired security profile to apply to the wired port. Otherwise, set security to 'Open and mark as 'Trusted' to ensure all traffic is allowed over the mesh link. Click 'Next'.

Central	Q Search or ask Aruba	۵ 🗰 🕜 ۹
\not \not \not \not \not \not \not \		
😫 GROUP	O ACCESS POINTS SWITCHES A GATEWAYS	⊞ th 🛞
- MANAGE	WLANS         ACCESS POINTS         RADIOS         PORTS         SECURITY         VPN         SERVICES         SYSTEM         CONFIGURATION AUDIT	Hide Advanced
DEVICES	CREATE A NEW NETWORK	
CI CLIENTS  APPLICATIONS  SECURITY  ANALYZE  ALERTS & EVENTS  AUDIT TRAIL  A TOOLS  REPORTS  MAINTAIN  FIRMWARE	General VLANs   Security Access   Security Level:     802.1X Authentication   MAC Authentication   Captive Portal   Open     Mac Authentication   Captive Portal   Open     Port Type Trusted :     Advanced Settings	
	Cancel Bac	k Next

5. A Summary page will appear to verify all settings. If all settings are correct, click 'Finish'.

aruba Central		Q Search or ask Aruba		۹ 🛛 🗰 🖁
√ Acme Mesh				
ដ្ឋ GROUP	O ACCESS POINTS SWITCHES	GATEWAYS     GATEWAYS     GATEWAYS     GATEWAYS     Second seco		⊞ th 😵
- MANAGE	WLANS ACCESS POINTS RADIOS PORTS	SECURITY VPN SERVICES SYSTEM CC	INFIGURATION AUDIT	Hide Advanced
B OVERVIEW		<b>-</b>		
DEVICES	CREATE A NEW NETWORK			
CLIENTS	1 General 2 VLANs	3 Security 4 Access	5 Summary	
APPLICATIONS	Network Summary			
SECURITY	GENERAL		VLAN	
ALERTS & EVENTS	NAME	Acme Wired Backhaul	VLAN MODE	trunk
AUDIT TRAIL	SPEED	auto	CLIENT IP ASSIGNMENT	Instant AP Assigned
🖏 tools	DUPLEX	auto	Client VLAN Assignment	Default
REPORTS	PRIMARY USAGE	employee	ALLOWED VLANS	all
- MAINTAIN	POE	Enabled	CECHDITY	
FIRMWARE	ADMIN STATUS	Up	SECORITY	
	CONTENT FILTERING	Disabled	MAC AUTHENTICATION	Disabled
	UPLINK	Disabled	ACCESS	
			Role Assignments For Authenticated Users	Disabled
			ENFORCE MAC AUTH ONLY ROLE	Disabled
			ASSIGN PRE-AUTHENTICATION ROLE	Disabled
			ENFORCE MACHINE AUTHENTICATION	Disabled
				Cancel Back Finish

6. Once the 'Wired Port Profile' is created, the new wired port profile needs to be applied to the APs on the appropriate Ethernet interface of the AP. For single port APs, this would be 'Ethernet 0/0'. If this is a multi-port AP, it should be applied to the port where the wired port profile should apply.

aruba Central		Q Search or ask Aruba			۵ 🗰 🕺
\nother Acme Mesh     \nother \n					
🕽 GROUP	🗑 ACCESS POINTS 📼 SWITCHES				ii 🗈 🕼
MANAGE	WLANS ACCESS POINTS RADIOS PO	RTS SECURITY VPN SERVICES SYSTEM COM	FIGURATION AUDIT		Hide Advanced
B OVERVIEW					
DEVICES	Wired Port Profiles				
LT CLIENTS	NAME	TYPE	ACCESS TYPE	ACTIONS	
APPLICATIONS	Acme Wired Backhaul	Mixed traffic	unrestricted		
SECURITY	default_wired_port_profile	Mixed traffic	unrestricted		
- ANALYZE	wired-SetMeUp	Mixed traffic	network-based		
AUDIT TRAIL					
🔦 TOOLS					
REPORTS					
- MAINTAIN	- + Add Port Profile				3 Port Profile(s)
FIRMWARE	Port Profiles Assignments				
	Ethernet 0/0:	default_wired_port_profile			
		Acme Wired Backhaul			
	Ethernet 0/1:	default_wired_port_profile wired-SetMeUp			
	Ethernet 0/2:	wired-SetMeUp			
	Ethernet 0/3:	wired-SetMeUp 🔻			
	Ethernet 0/4:	wired-SetMeUp 🔻			

At this point, there should be a mesh portal with one or more mesh points up and active and connected to Central. Additionally, if wired backhaul was enabled, the mesh points should also be providing wired network services out of the mesh points' wired interface. This should all be tested in a lab or on a bench in a controlled environment before physically deploying the AP. This would include making sure all APs are up, that all settings are applied and correct, and that if wired backhaul services are offered, that clients, switches and devices have wired access over the mesh points to the main LAN.

#### **CONCLUSION**

Using the information in this document, a quick and capable Central managed Instant-based mesh network can be deployed in a rapid fashion to provide quick, reliable coverage in hard to reach areas, while also allowing for remote monitoring and management of the network. 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, and what infrastructure would be required to mount the APs to (tripods, light poles, stationary vehicles or trailers, etc. are all viable with creative solutions). 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

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

**Outdoor AP Mounting Brackets** 

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



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