

May 19, 2022



EdgeConnect Microbranch Deep Dive

John Schaap, Consulting Systems Engineer EMEA

Welcome! Housekeeping.



- Listen by computer audio or dial-in



- All lines are muted during the webinar

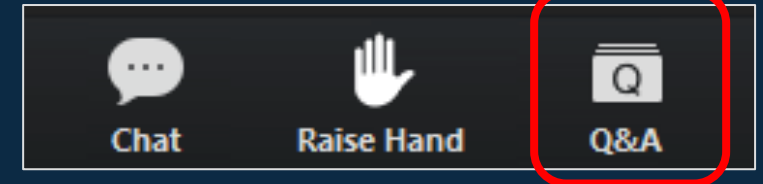


- Ask *questions* by selecting "Q&A" and to report any webinar difficulties



- Webinar is being recorded & will be emailed to all attendees

TO ASK
QUESTIONS



Partner Technical Webinar Series

Aruba AOS 10 Technical Deep Dive

Session 1: Designing Next Generation Campuses with ArubaOS 10

Thu, April 21st, 2022, 11:00 AM - 12:00 AM CET

Session 2: AOS10 Services Deep Dive

Thu, May 5th, 2022, 11:00 AM - 12:00 AM CET ([click here to register](#))

Session 3: Micro Branch Deep Dive

Thu, May 19th, 2022, 11:00 AM - 12:00 AM CET ([click here to register](#))

Session 4: Exploring Aruba SD-Branch with AOS10

Thu, June 2nd, 2022, 11:00 AM - 12:00 AM CET ([click here to register](#))



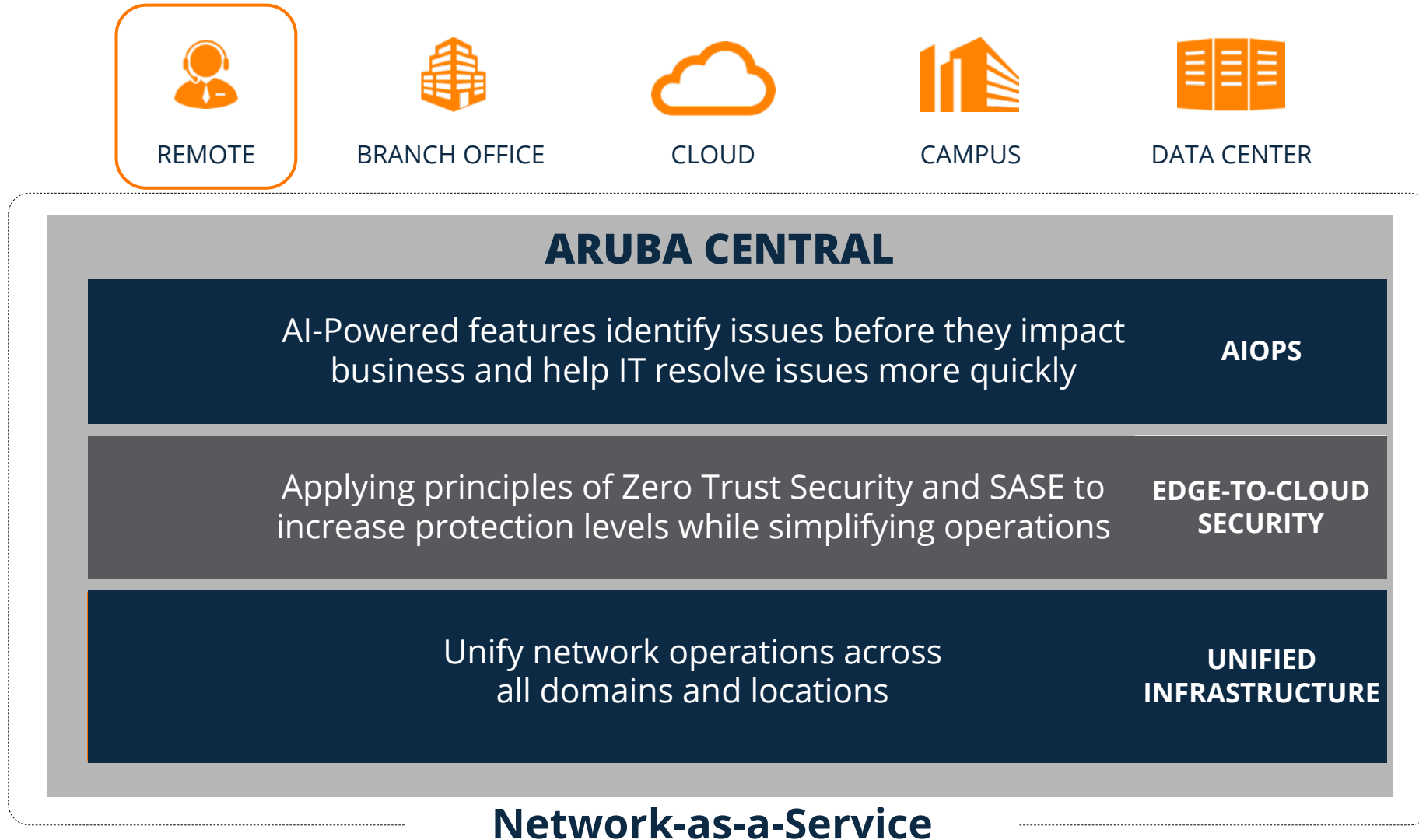
Agenda

- Aruba ESP & EdgeConnect Microbranch
- Aruba's Remote Work Solution Comparison
- WLAN Forwarding Modes & Traffic Load Balancing
- Automated Central Services Workflow
- Aruba Central Configuration Workflow
- Demo: WAN Visualization & SASE Integration
- Q & A
- Useful Resources

Agenda

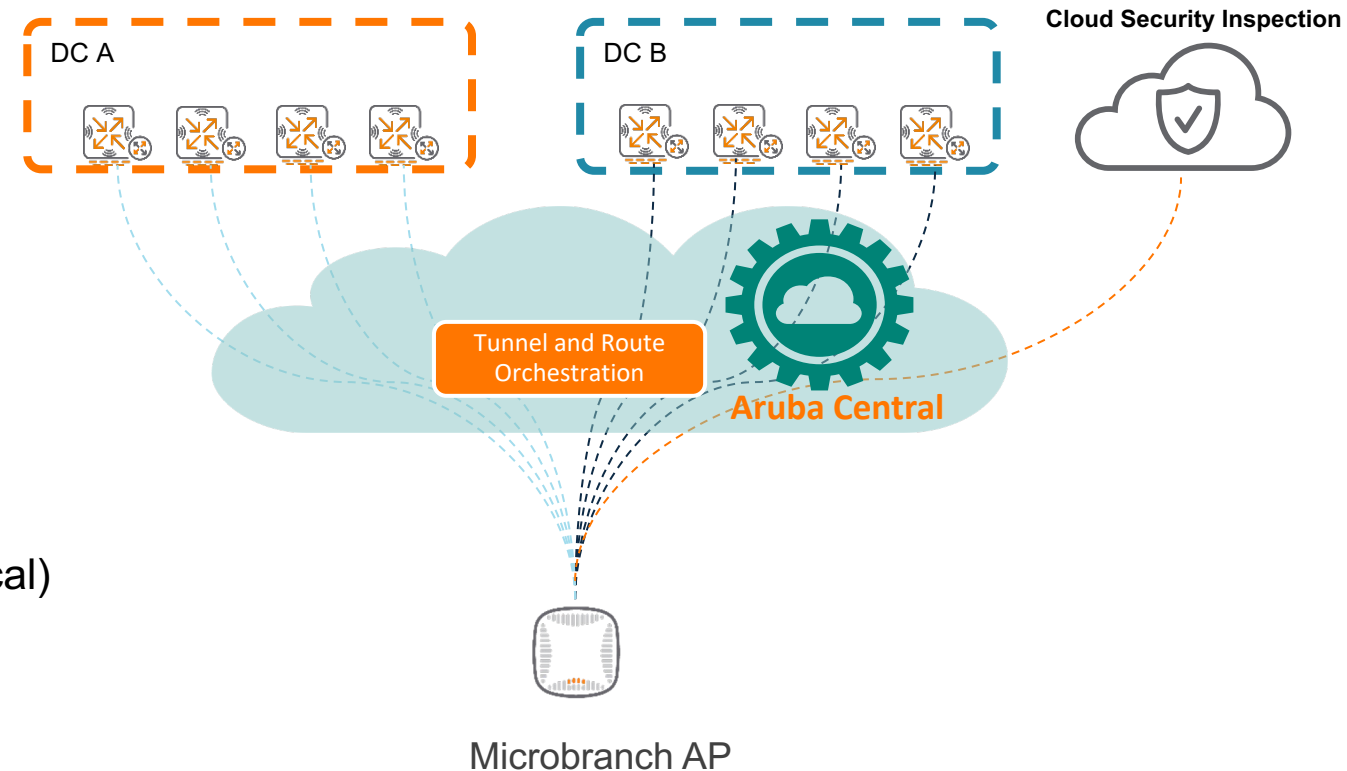
- Aruba ESP & EdgeConnect Microbranch
- Aruba's Remote Work Solution Comparison
- WLAN Forwarding Modes & Traffic Load Balancing
- Automated Central Services Workflow
- Aruba Central Configuration Workflow
- Demo: WAN Visualization & SASE Integration
- Q & A
- Useful Resources

Aruba Edge Services Platform Architecture



Introduction of EdgeConnect Microbranch

- Single AP Branch solution
- Supported by ArubaOS 10.3 and Central 2.5.4
- Max 5 headend **VPNC clusters** supported for high redundancy (**Layer 3 mode**)
- AP establishes IPsec tunnels with each VPNC for fast failover and load balancing
- Orchestrated tunnels and routes
- Centralized L2 and Routed L3 (DL3) and NATed L3 (local) modes supported
- Cloud Security Orchestration (SASE)
- PBR with 1st packet classification
- Next Generation IAP-VPN & RAP



**NO ON-PREM GATEWAY
REQUIRED**

Agenda

- Aruba ESP & EdgeConnect Microbranch
- **Aruba's Remote Work Solution Comparison**
- WLAN Forwarding Modes & Traffic Load Balancing
- Automated Central Services Workflow
- Aruba Central Configuration Workflow
- Demo: WAN Visualization & SASE Integration
- Q & A
- Useful Resources

Remote Work Solutions Comparison

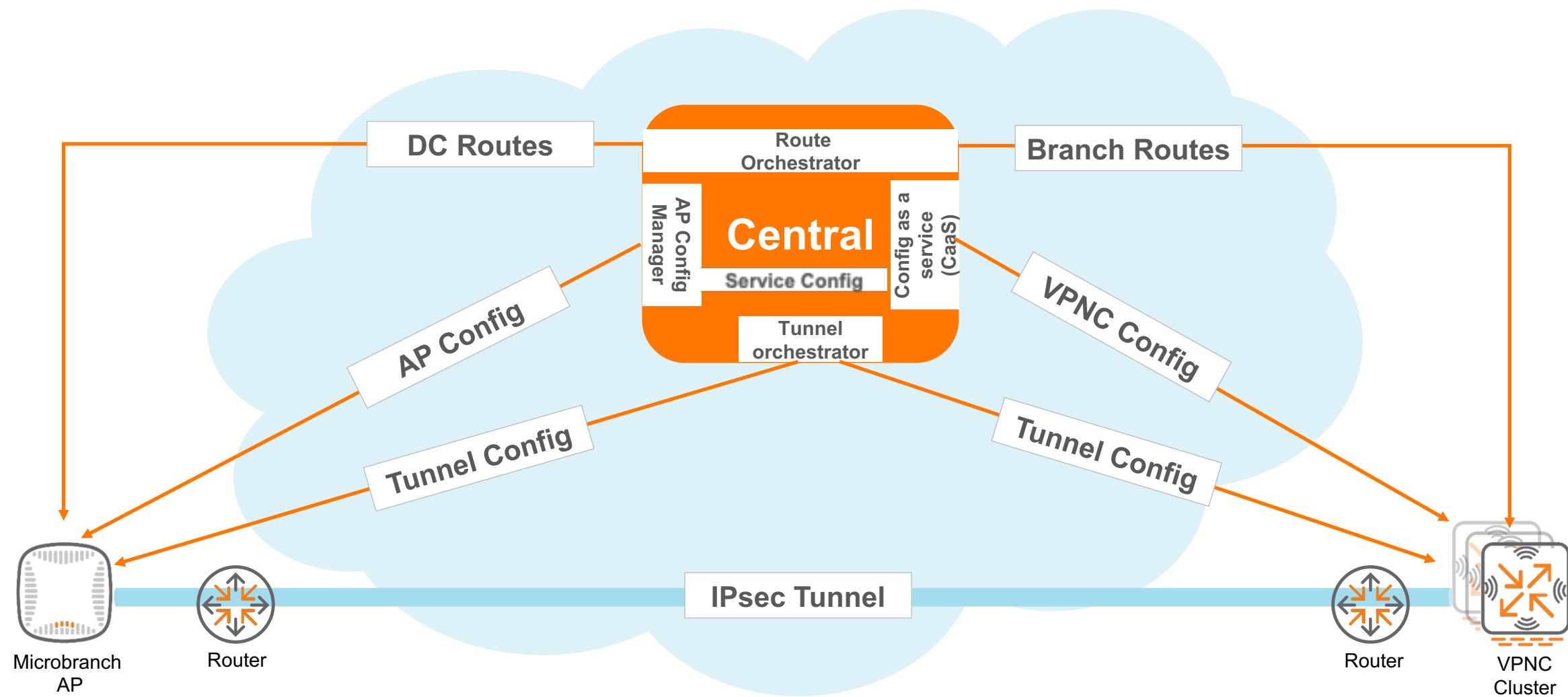
	RAP	IAP-VPN	EdgeConnect Microbranch
Supported OS	ArubaOS 8.x	ArubaOS 8.x	ArubaOS 10.3
Supported AP models	All	All	All
Deployment Type	Single AP	Single AP, Cluster	Single AP
Management	Mobility Conductor	IAP GUI, Aruba Central	Aruba Central
Ports to be open for AP	UDP 4500	UDP 4500	UDP 4500
Wireless client support	Yes	Yes	Yes
Wired client support	Yes	Yes	Yes
Static Routing	Yes	Yes	Yes
Dynamic Routing	No	No	Route Orchestrator
Policy Based Routing	Yes	Yes	Yes
Tunnel pre-establishment to all VPNCs	No (only to primary cluster/standalone)	Yes (w/ Fast Failover enabled)	Yes
Full-Tunnel	Yes	Yes	Yes
Split-Tunnel	Yes	Yes	Yes



Remote Work Solutions Comparison (Contd.)

	RAP	IAP-VPN	EdgeConnect Microbranch
Encryption nodes	Client to DC	AP to DC	AP to DC
Failover within DC	Yes	Yes	Yes
Failover between DC	Yes	Yes	Yes
Tunnel orchestration	No	No	Tunnel Orchestrator
Route orchestration	No	No	Route Orchestrator
Cloud Security vendor support	No	No	Yes

High Level Control Flow

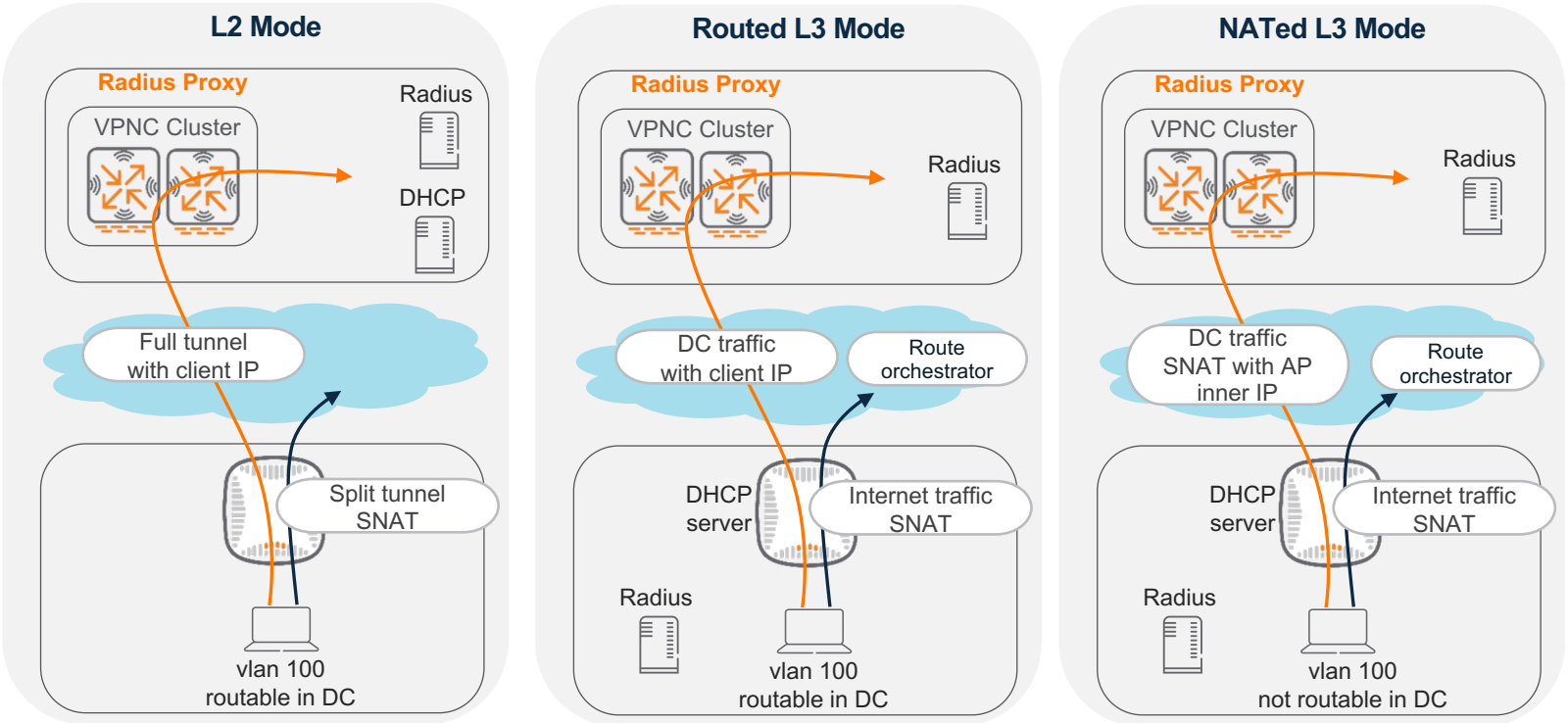


Agenda

- Aruba ESP & EdgeConnect Microbranch
- Aruba's Remote Work Solution Comparison
- **WLAN Forwarding Modes & Traffic Load Balancing**
- Automated Central Services Workflow
- Aruba Central Configuration Workflow
- Demo: WAN Visualization & SASE Integration
- Q & A
- Useful Resources

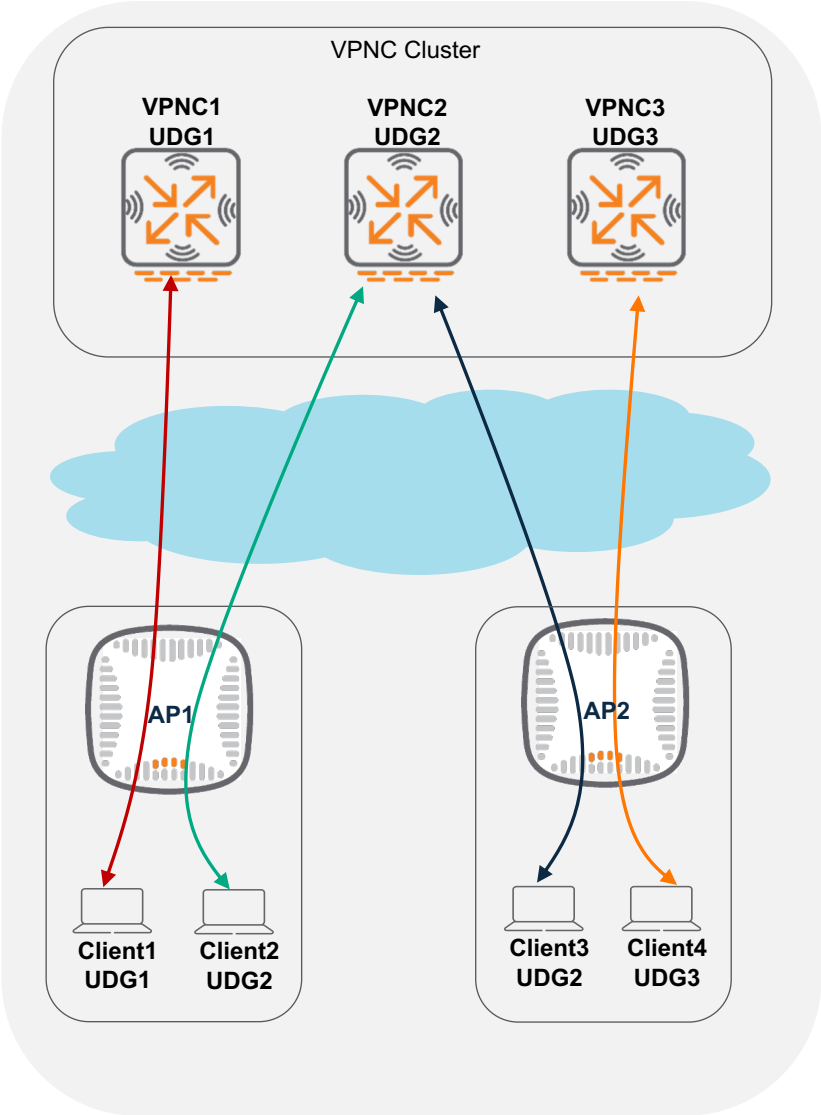
Forwarding Mode Comparison

Functions and Behaviors	L2	Routed L3	NATed L3
Route orchestrator required	No	Yes	Yes
DHCP server	VPNC or External DHCP server in DC	Microbranch AP	Microbranch AP
Client subnets routable in DC	Yes	Yes	No
Client traffic to DC	Source with client IP	Source with client IP	Source-NATed with AP inner IP
Client traffic to Internet	Full tunnel to DC source with client IP or split-tunnel with source-NATed with AP uplink IP	Source-NATed with AP uplink IP	Source-NATed with AP uplink IP
VPNC cluster as radius proxy	Yes	Optional. In mixed SSID, yes	Optional. In Mixed SSID, yes
PBR rules required for user role	Yes for DC traffic as split tunnel is default	Optional	Optional
Load balancing	Evenly distributed between VPNCs	Based on VPNC cost assigned by route orchestrator	Based on VPNC cost assigned by route orchestrator

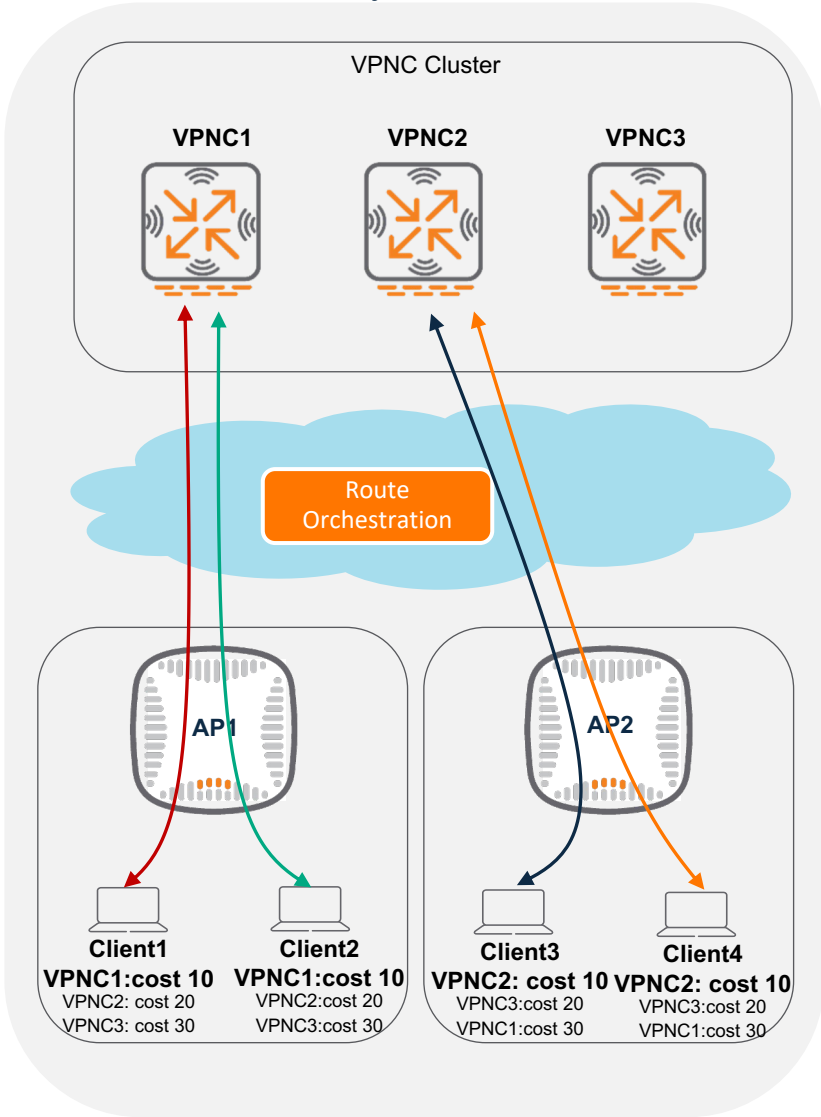


Traffic Load Balancing

L2 Mode: Client-based load balancing
All clients of one AP are distributed to different VPNCs



L3 Mode: AP-based load balancing
All clients of one AP always use same VPNC for DC traffic

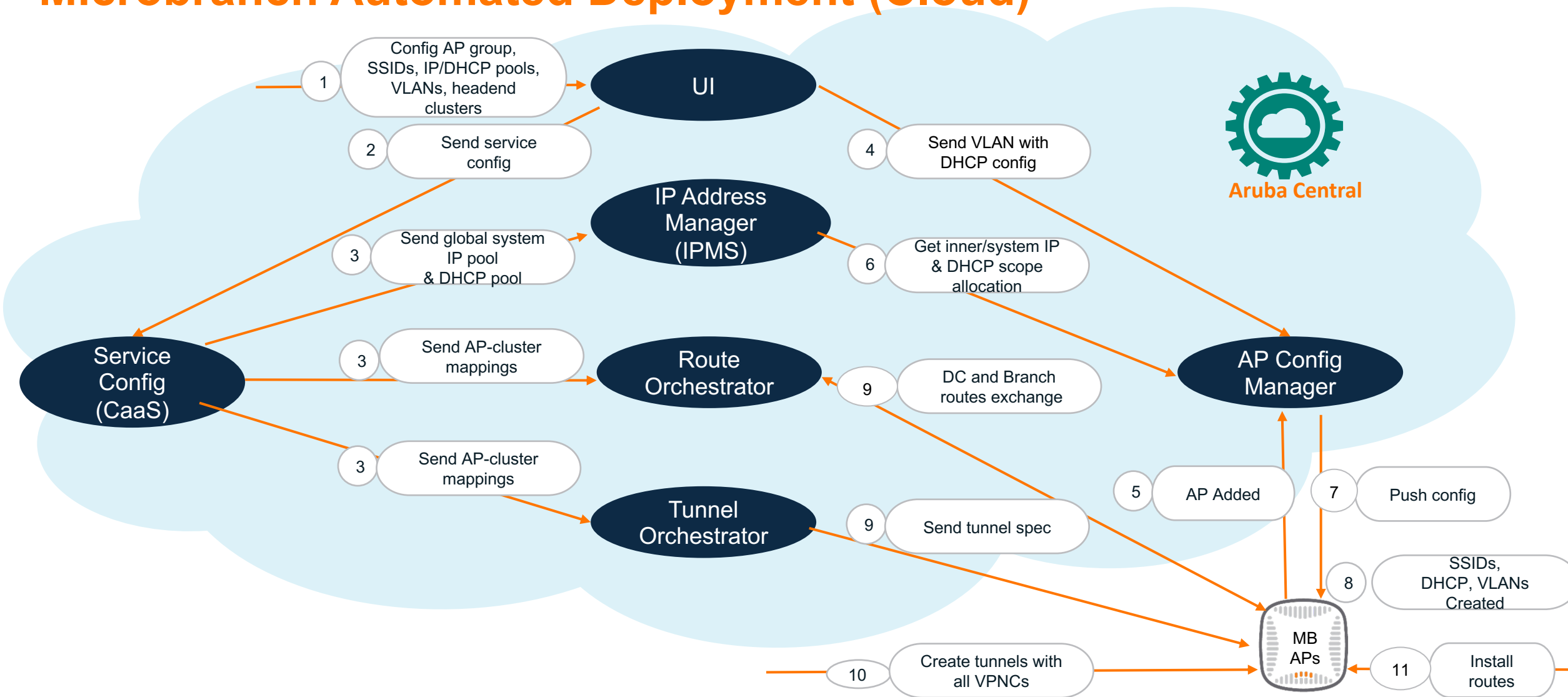


* UDG – User Designated Gateway

Agenda

- Aruba ESP & EdgeConnect Microbranch
- Aruba's Remote Work Solution Comparison
- WLAN Forwarding Modes & Traffic Load Balancing
- **Automated Central Services Workflow**
- Aruba Central Configuration Workflow
- Demo: WAN Visualization & SASE Integration
- Q & A
- Useful Resources

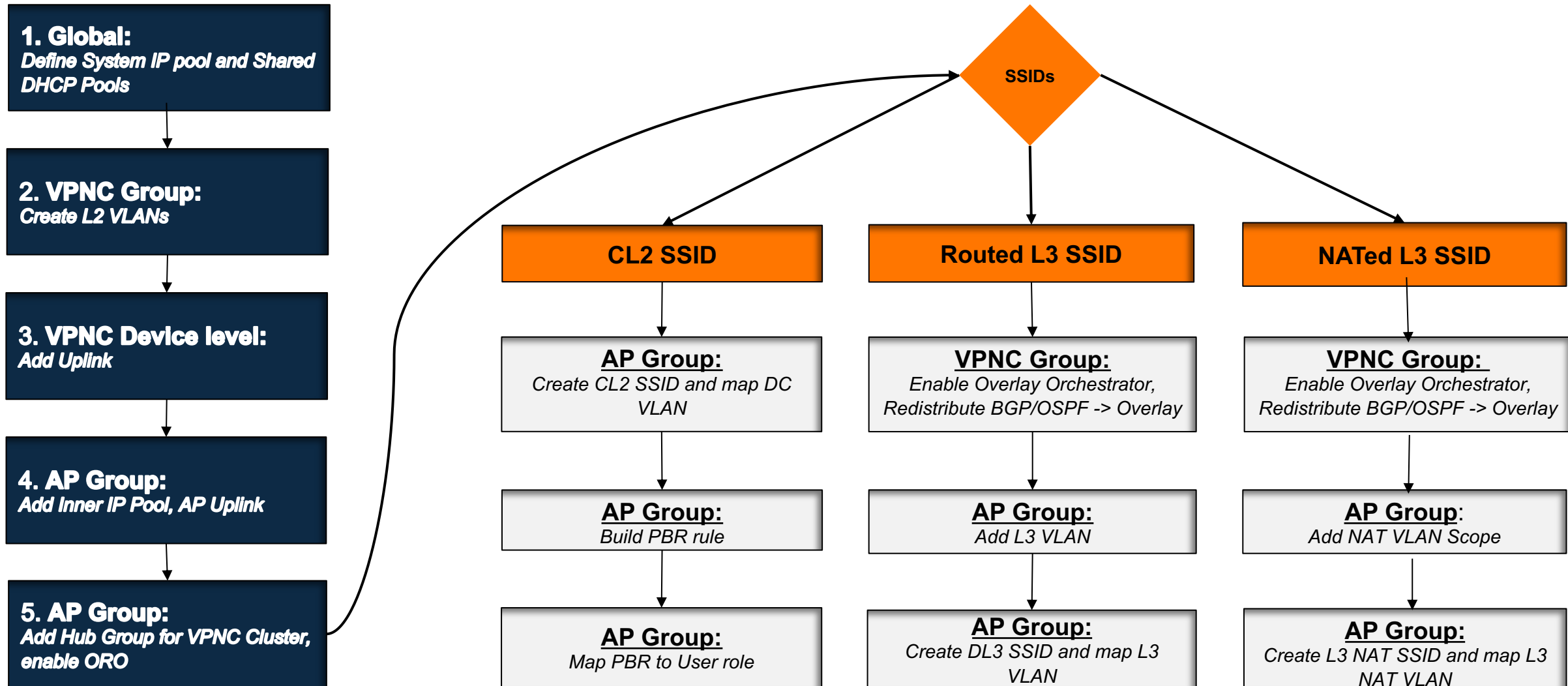
Microbranch Automated Deployment (Cloud)



Agenda

- Aruba ESP & EdgeConnect Microbranch
- Aruba's Remote Work Solution Comparison
- WLAN Forwarding Modes & Traffic Load Balancing
- Automated Central Services Workflow
- **Aruba Central Configuration Workflow**
- Demo: WAN Visualization & SASE Integration
- Q & A
- Useful Resources

Microbranch Configuration Workflow (Aruba Central UI)



Microbranch AP Inner IP

The screenshot illustrates the configuration of a Microbranch AP's inner IP address pool in WinBox. The interface is divided into several sections:

- Global** (top left): The main menu area.
- IP Address Manager** (top center): The active tab for managing IP pools.
- System IP Pools** (top right): A table listing existing IP pools. The table has columns for Pool Name, IP Range, and Allocated IP Addresses. A pool named "Microbranch AP Inner IP pool" is listed with an IP Range of 172.16.200.10 - 172.16.200.20 and 9% of addresses allocated.
- Add System IP Pools** (modal window): A form for adding a new IP pool. It includes fields for Pool Name (Microbranch AP Inner IP Pool-2), IP Range (From 172.16.200.21 to To 172.16.200.200), and a summary stating "180 IP Addresses will be assigned to the IP Pool".
- Microbranch-AP** (right sidebar): A section for configuring the AP. It includes a dropdown for "Select IP Address Pool" which is currently set to "Microbranch AP Inner IP Pool-2".
- IP Addressing** (bottom right): A detailed view of the IP pool configuration. It shows the "Select IP Address Pool" dropdown, the "IP Address Ranges" (Start from 172.16.200.21, End to 172.16.200.200), and a donut chart indicating that 0.6% of the pool is allocated.

Orange arrows indicate the flow of the configuration process: from the "Add System IP Pools" modal to the "Microbranch-AP" section, and then to the "IP Addressing" section.

IPMS – DHCP Pool Allocation Algorithm

Total IPs per site = Requested host count per site + 3
3 extra IPs=subnet address + broadcast address + default gateway

Subnet size calculation = Total IPs per site rounded to next power of 2

For example, pool: 172.16.10.0 – 172.16.10.255, host per site = 25
25+3=28, then rounded to next power of 2 is 32
then subnet size is 32,

Total number of branch subnets = range size / subnet size
In this example: 256 / 32 = 8

The example pool can be allocated to 8 APs:
172.16.10.0/27, 172.16.10.32/27, 172.16.10.64/27, 172.16.10.96/27
172.16.10.128/27, 172.16.10.160/27, 172.16.10.192/27, 172.16.10.224/27

DHCP Pool for Clients in L3 Mode

- Multiple IP ranges are supported for one DHCP pool
- Three types of DNS server supported: Specify server; Use AP's assigned DNS servers; Use AP as DNS

The screenshot shows the 'Global' management interface. The 'IP Address Manager' tab is selected. Under 'Shared DHCP Pools', a table lists the configuration for 'vlan-100'.

Pool Name	IP Range	Pool Unit Size	Allocated IP
vlan-100	192.168.100.10 - 192.168.100.250	10	0%
	192.168.101.10 - 192.168.101.250		
	192.168.102.10 - 192.168.102.250		



The screenshot shows the 'Microbranch-AP' configuration interface. The 'Access Points' tab is selected. Under 'LAN', the 'VLANs' section is highlighted.



The screenshot shows the 'Microbranch-AP' configuration interface. The 'Access Points' tab is selected. Under 'VLAN', the 'DHCP Profile Name' is 'vlan100'. The 'Routed' radio button is selected. The 'DHCP Server Configuration' is set to 'DHCP pool' and 'vlan-100'. The 'Domain Name' is 'TME-labnet.com'. The 'DNS server' is set to 'Use AP as DNS'. The 'DHCP Lease Time' is 720 minutes. The 'Summary' section shows the IP Range and the number of IP addresses and pools.

Type	Value
IP Range	192.168.100.10 - 192.168.100.250 192.168.101.10 - 192.168.101.250 192.168.102.10 - 192.168.102.250
Number of IPs	723 addresses - 0 first reserved
Number of Pools	0 pools allocated - 18 remaining

DNS Redirect

- By default, it is disabled
- AP will snoop all the DNS packets, if the FQDN domain matches any one of the domain name in redirect domain list. It will proxy the DNS request to configured redirect DNS server.
- To enable DNS redirect for L3 mode, “**Use AP as DNS**” needs to be selected under VLAN configuration

← **VLAN**

DHCP Profile Name: vlan100 VLAN ID: 100

☒ Routed ☐ NATed

DHCP Server Configuration

DHCP pool: vlan-100 Excluded addresses: 0

Domain Name: TME-labnet.com

DNS server: Use AP as DNS



Access Points

← **DNS & NTP**

✓ DNS

Domain Name:

DNS SERVERS (1) +

Provider	IP Address
User Defined	10.71.1.10

Redirect DNS: L3 routed/NAT ed tunnels

DOMAINS TO REDIRECT (1) +

Domain Name	IP Address
tmelab.net	8.8.8.8

Uplink Configuration of AP

- Configured at the group level

The screenshot displays the network configuration interface. On the left, under the 'Access Points' header, there are two main sections: 'System' and 'WAN'. The 'WAN' section is expanded, showing 'WAN Uplink' (highlighted with a red box), 'Uplink Management', and 'WAN Health Check'. An orange arrow points from the 'WAN Uplink' option to the 'Add Uplink' configuration page on the right.

Add Uplink

Uplink: uplink-eth0

VLAN: 4092

WAN type: Ethernet ▼

Speed: Auto ▼

☐ Use as backup

IP addressing method: DHCP server assigned ▼

Port assignment: Eth-0 ▼

Uplink Configuration of Each VPNC

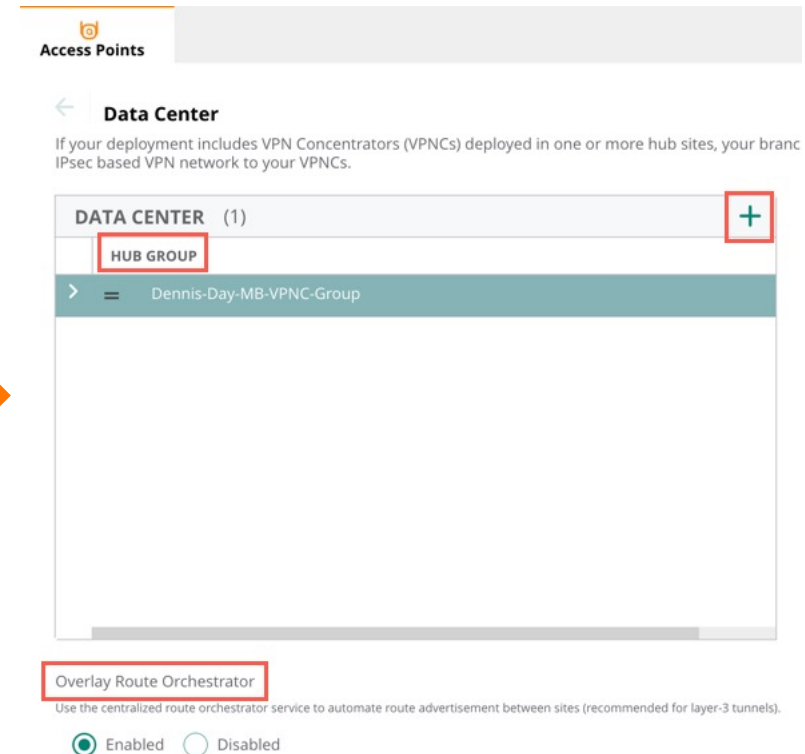
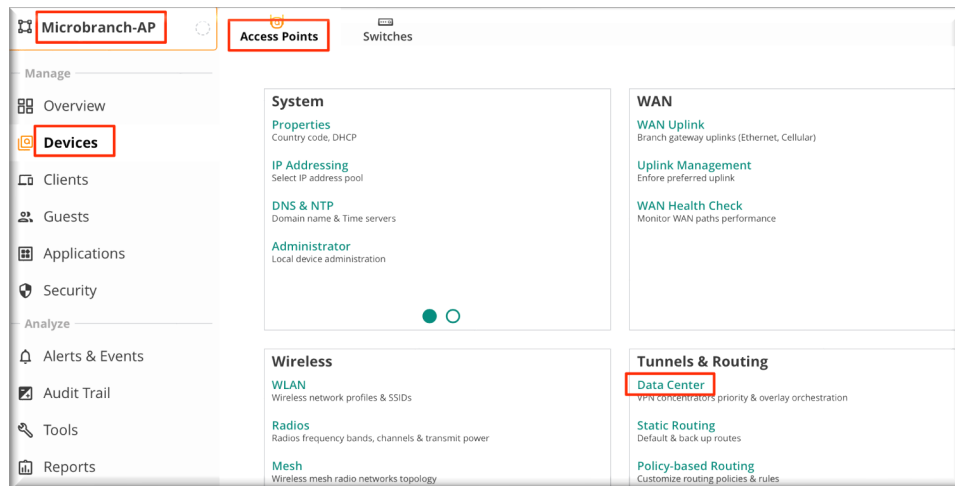
- Configured at the device level
- Public IP is required for Internet uplink

The screenshot shows the configuration interface for a device named Pod14-GW1. The left sidebar contains navigation links: Overview, WAN, LAN, Device (highlighted with a red box), Clients, Applications, and Security. The main content area is titled 'Gateway' and has tabs for System, LAN, WAN (highlighted with a red box), and Tunnels & Routing. Under the WAN tab, there is a section 'WAN Details' with a descriptive text: 'Each VPNC (Headend Gateway) connects to one or more MPLS or internet connections using WAN ports. Each connection requires...'. Below this is a link for 'Per-field help'. At the bottom, there is a table titled 'Uplinks' (highlighted with a red box) with columns: LINK, TYPE, ID, PUBLIC IP (highlighted with a red box), and PRIVATE IP. The table contains one entry: uplink1_INET, INET, 24, 108.24.65.37, and 10.71.24.11.

LINK	TYPE	ID	PUBLIC IP	PRIVATE IP
uplink1_INET	INET	24	108.24.65.37	10.71.24.11

Hub Group Configuration for L3 mode SSIDs

- For L3 SSID, the Hub Groups (VPNC clusters) are configured under Data Center, max. 5 Hub Groups are supported
- For L2 SSID, the VPNC clusters are configured under SSID. Primary and secondary clusters are supported
- L3 and L2 SSIDs cannot terminate on the same VPNC cluster



Route Orchestration for L3 mode SSIDs

- By default, Route Orchestrator assigns different costs to each DC route through different VPNCs within the clusters for next hop selection while announcing DC routes to the Microbranch APs .
- Each AP most likely gets different costs for routes through each VPNC for load balancing.

The screenshot displays the Cisco Meraki dashboard interface for configuring a device named "Dennis-Day-MB-V...". The left sidebar contains navigation options: "Manage" (with a sub-option "Overview"), "Devices", "Clients", "Guests", "Applications", and "Security". The main content area is titled "Gateways" and features a horizontal menu with tabs: "System", "WAN", "Interface", "Security", "VPN", "Routing", "High Availability", and "Config Audit". The "VPN" tab is selected and highlighted. Below this, a sub-menu includes "SD-WAN Overlay", "Cloud Security", "Site to Site", "DPD", "IKEV1", "IKEV2", and "General VPN". The "SD-WAN Overlay" option is selected. The "Overlay mode:" is set to "Orchestrated" with a green checkmark. A section titled "Overlay Orchestrator Peering" shows a status of "Running" with a green checkmark icon and a "Disable" button. An information icon (i) is located to the right of this section.

DC Aggregate Routes

- Aggregation of DC routes is highly recommended
- Every AP can have maximum 512 routes
- When “allow transit inter-branch connectivity” is enabled for specific VPNC group, the routes learnt from one branch will be advertised to other branches.

The screenshot displays the SD-WAN Overlay configuration interface. At the top, the 'Gateways' tab is selected, and the 'VPN' sub-tab is active. Below this, the 'SD-WAN Overlay' section is visible, showing the 'Overlay mode' set to 'Orchestrated'. The 'Overlay Orchestrator Peering' status is 'Running', with a 'Disable' button. The 'DC Aggregate Routes' section is expanded, showing a table with the following data:

IP ADDRESS	NETMASK
10.71.0.0	255.255.0.0

Below the table, there is a checkbox for 'Allow transit inter-branch connectivity:' which is checked. A tooltip explains: 'This will make the VPNC group as transit site and allow branch to branch traffic.'

Radius Configuration in SSID workflow

- VPNC as radius proxy is **OPTIONAL** for L3 mode SSID
- VPNC is always the radius proxy for L2 and mixed (L2 + L3) mode SSID

The screenshot displays the Microbranch-AP configuration interface. The left sidebar contains navigation links: Manage, Overview, Devices, Clients, Guests, Applications, Security, Analyze, Alerts & Events, Audit Trail, Tools, Reports, Maintain, and Firmware. The main content area is titled 'Access Points' and 'Switches'. The breadcrumb path is 'NETWORKS > CONFIGURATION > MB-DL3-SSID1'. The 'Security' tab is selected, showing a 'Security Level' slider set to 'Enterprise'. Below this, the 'Radius Proxy' section is highlighted with a red box. It includes fields for 'Primary Proxy Server' (set to 'microbranch-gw:auto_gwcl'), 'Secondary Proxy Server' (set to 'None'), and 'Key Management' (set to 'WPA3-Enterprise(CCM 128)'). At the bottom, the 'Primary Server' field is also highlighted with a red box, set to 'CloudAuth'.

Microbranch-AP

Access Points Switches

NETWORKS > CONFIGURATION > MB-DL3-SSID1

General VLANs Security Access Summary

Security Level: Enterprise Personal Visitors Open

Radius Proxy:

Primary Proxy Server: microbranch-gw:auto_gwcl

Secondary Proxy Server: None

Key Management: WPA3-Enterprise(CCM 128)

Primary Server: CloudAuth



DEMO

Key Takeaways

NO ADDITIONAL HARDWARE REQUIRED	All services delivered via AP
	On-campus experience without an appliance
	Scalability from cloud-based management
CONSISTENT SECURITY, HOME TO CAMPUS	Identity-based access control
	SASE-based cloud services
SUITED FOR ENTERPRISE	Zero-Touch Provisioning, automated onboarding
	More insights (WAN, AI)
	Unified/centralized visibility
	Ability to manage at scale

Agenda

- Aruba ESP & EdgeConnect Microbranch
- Aruba's Remote Work Solution Comparison
- WLAN Forwarding Modes & Traffic Load Balancing
- Automated Central Services Workflow
- Aruba Central Configuration Workflow
- Demo: WAN Visualization & SASE Integration
- Q & A
- Useful Resources

EdgeConnect Microbranch Resources

Arubapedia:

- Partners: https://afp.arubanetworks.com/afp/index.php/AOS_10

Validated Solution Guides:

- <https://www.arubanetworks.com/techdocs/VSG/>



Questions



Partner Resources

Portals



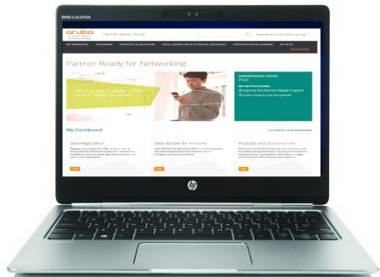
Airheads Community

[\(Click Here\)](#)



Arubapedia for Partners

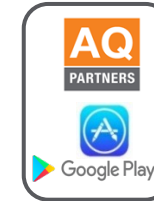
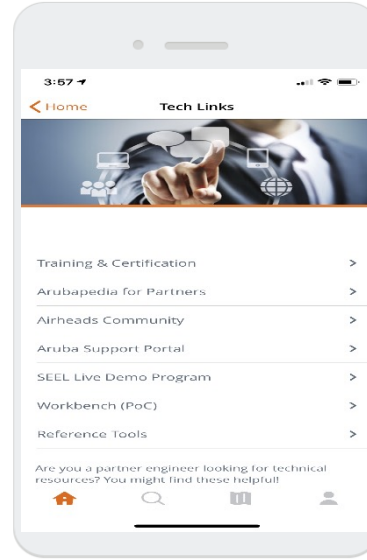
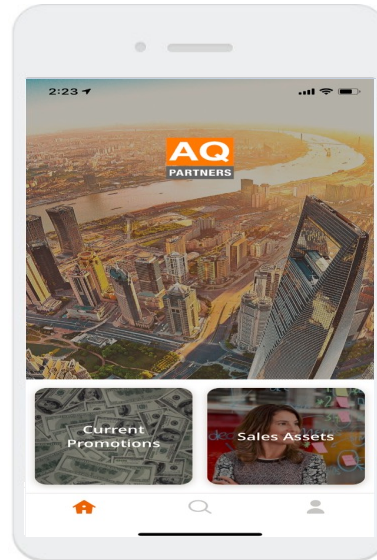
[\(Click Here\)](#)



Partner Ready for Networking portal

[\(Click Here\)](#)

Mobile App



Aruba Quotient for Partners (mobile app)
Navigate to Tech Links

Apple Store [\(Click Here\)](#)
Google Play [\(Click Here\)](#)

Live Support

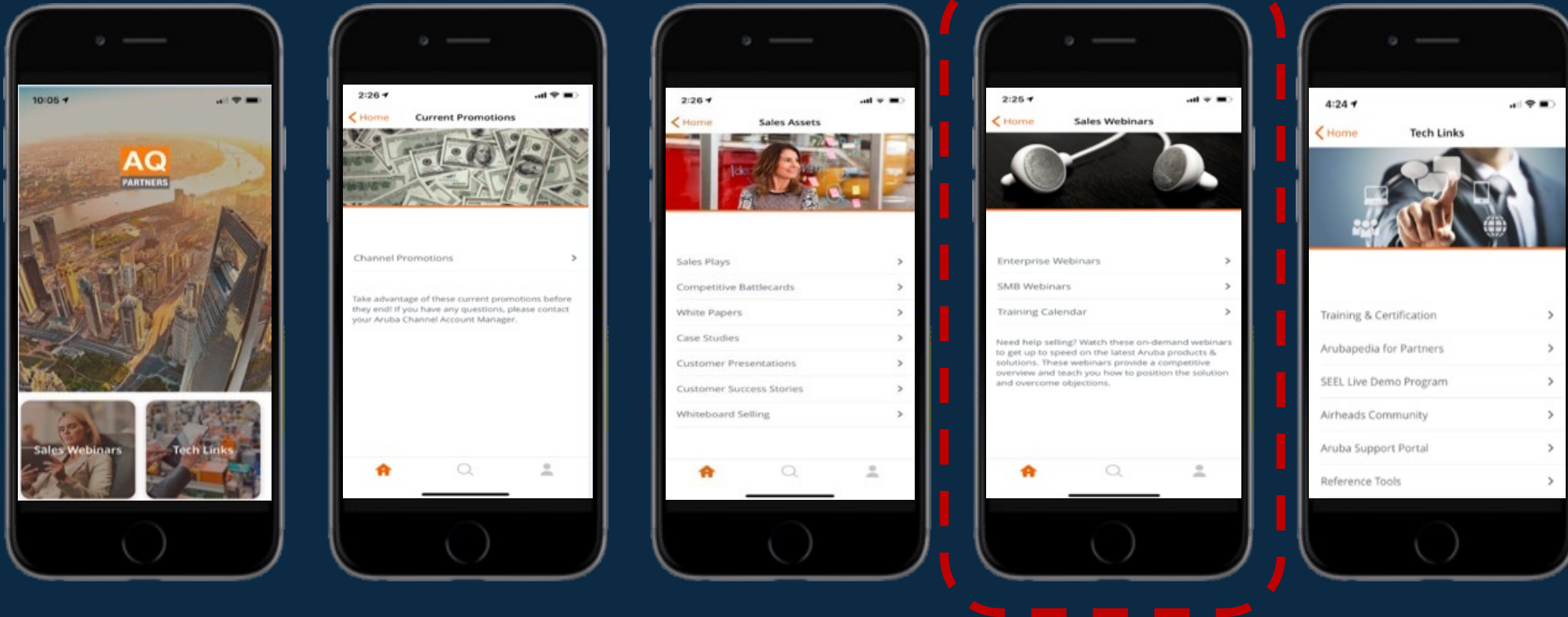


Channel SEs (CSEs)
Regional channel support

Aruba Quotient for Partners Mobile App



1. Download the free “Aruba Quotient for Partners”
2. Login with Partner Login information
3. Browse content by scrolling left and right at bottom of screen



Thank You

