

Validated Solution Guide

Aruba Solution TME

May 28, 2025

Table of Contents

ESP SD-WAN & Branch Deploy Document Conventions	4 4
Introduction to SD-Branch Purpose of This Guide	5 5
Aruba SD-Branch Network Deployment Overview Branch Site Requirements	8 10
Preparing to Deploy Aruba SD-Branch Network 1 Device Management with HPE GreenLake 1 Define Groups in Aruba Central 2	19 19 22
Aruba VPNC Group Configuration2Configure the VPNC Group2Configure VPNC Devices4Configure VPNC Device4Onboard VPNC to Central5	28 28 19 19 55
Deploying Branch Site	57
Aruba Branch Gateway Configuration 5 Create a Branch Gateway Group and Preprovision Gateways 5 Configure the Branch Gateway Group 5 Configure Branch Gateway at the Device Level 8	58 58 58 33
Branch Switch Configuration 9 Stacking Switches Offline 9) 0 90
Aruba Branch Access Point (AP) Configuration 10)6
SD-Branch Security 12	25
Enabling Centralized Multi-Site Fabric 12 Enabling Multi-Site Fabric 12 SD-Branch User Based Tunneling 13	2 6 28 32
Summary 14	18
Aruba Microbranch 14	19
Aruba Layer 3 Microbranch AP Configuration 15 (Optional) Routed Layer 3 Full-Tunnel Configuration 17 Monitor Microbranch AP Routing Overlay 18	74 81
Aruba Microbranch Centralized Layer 2 (CL2) Overview18User Traffic Flow in CL218	13 33
Aruba CL2 VPNC Configuration18Configure CL2 VLAN18Assign the CL2 VLAN to the VPNC LAN Port Interface18	37 37 38

Configuring CL2 Microbranch AP 19	90
Create a Microbranch AP Group	90
Configure System IP Pool	91
Set AP Device Password	92
Configure Country Code	93
Assign the System IP Pool to AP Group	94
Configure DNS and NTP	94
Configure WAN Uplink	96
Configure WAN Health Check	96
Configure the WPA3-Enterprise Wireless LAN	97
Configure Split-Tunnel in CL2	02
Configure Full-Tunnel in CL2	07
Assign a Microbranch AP to a Group	211
Assign a Microbranch AP to a Site	211
Monitor Microbranch Site Tunnels	12
Monitor Microbranch Site Routes	215
	17
	. 1 /
Verifying Aruba SD-Branch Hub Spoke Topology 2	18
Verify SD-WAN Tunnels	18
Verify Routes	19
Verify NTP	21
Verify DHCP Snooping	221
Verify Radius	22

ESP SD-WAN & Branch Deploy

This guide provides IT professionals with the prescriptive steps to deploy both SD-WAN & Branch network outlined in the Design document using the following products:

- Aruba Central
- Aruba ClearPass Policy Manager
- EdgeConnect Orchestrator
- EdgeConnect EC-US, EC-XS, EC-S-P, EC-M-H, EC-L-H
- Aruba Access Point 300, 600 and 500 Series
- Aruba Gateway 7000, 7200, and 9000 Series
- Aruba CX Switching 6100, 6200, and 6300

Document Conventions

Bold text indicates a command, navigational path, or a user interface element.

Examples:

- the show stacking command
- Navigate to Configuration > System > General
- Username: admin

Italic text indicates the definition of important terminology, user interface input, or table heading.

Examples:

- Spatial streaming is a transmission technique in MIMO wireless communication
- **Password:** *password*
- Example: Core 1 Switch

Code blocks indicates a variable for which you should substitute a value appropriate for your environment.

Example:

• Configure the NTP servers.

```
ntp server 10.2.120.98 iburst version 3
ntp server 10.2.120.99 iburst version 3
```

Introduction to SD-Branch

Software-defined branch (SD-Branch) is a technology shift toward solutions that are agile, open, and cloud-integrated. SD-Branch includes SD-WAN components that deliver a secure, service-provider-independent network with enterprise-level performance over disparate wide-area network (WAN) technologies. However, although SD-WAN solves a real IT problem, it addresses only part of the issue organizations face when dealing with distributed locations.

Organizations often roll out and operate distributed, heterogeneous networks with centralized teams. These distributed networks offer many services in addition to WAN connectivity. Branch networks require wired and wireless LANs, security and policy enforcement, and, of course, WAN interconnects. SD-Branch extends the concepts beyond SD-WAN to all elements in the branch, delivering a full-stack solution that includes SD-LAN and security that address all network connectivity needs.

When formulating the strategy for an SD-Branch rollout, Aruba recommends:

- Purchase as much WAN bandwidth as possible to alleviate potential bottlenecks during the busiest times of the day.
- Increase Internet bandwidth, instead of buying additional private bandwidth.
- Use cloud-based tools to simplify the configuration, operation, and management of the WAN.

Purpose of This Guide

This deployment guide covers the Aruba SD-Branch in the Edge Services Platform (ESP) architecture. It contains an explanation of the requirements that shaped the design and the benefits it can provide to your organization. The guide describes a single unified infrastructure that integrates access points (APs), switches, gateways, and network management with access-control and traffic-control policies. Refer to volume one of this VSG for design guidance:

Aruba VSG: SD-Branch Design

This guide assumes the reader has an equivalent knowledge of an Aruba Certified Mobility Associate or Aruba Certified Switching Associate.

Design Goals

The overall goal is to create a simple, scalable design that is easy to replicate across all sites in your network. The solution components are limited to a specific set of products to help with operations and maintenance. The key features addressed by Aruba SD-Branch include:

 Simplicity with Zero Touch Provisioning (ZTP): SD-Branch devices can be factory-shipped directly to a remote site. By automatically matching orders to an Aruba customer account, the mobile Installer app is available for third-party systems integrators to quickly install equipment. Standardized group- and device-level configurations for APs, switches, and gateways enable fast network deploymnet.

- Unified policy management: For Aruba and third-party network infrastructure, Aruba ClearPass delivers a common policy framework for multivendor wired and wireless networks. This softwaredefined approach makes it easy for the network administrator to distribute changes quickly based on corporate risk and compliance requirements. ClearPass Device Insight (CPDI) adds AI-powered device profiling to help automate discovery of the latest mobile and IOT endpoints.
- **Predictive analytics and assurance:** Aruba Central's artificial intelligence (AI), machine learning (ML), and automation capabilities identify issues and notify IT of problems with recommended changes. When shifting to a cloud-hosted model, data can be collected and crowdsourced from Aruba's installed base to take advantage of Aruba's extensive data science expertise.
- Secure WAN connectivity: Enable SD-WAN technology to support the use of the Internet to replace or augment private WAN services. Elements of the solution include: path quality monitoring (PQM) to track the available paths, stateful firewall with application fingerprinting to identify traffic flows, dynamic path selection (DPS) to use the optimal path, and centralized routing to free branch gateways (BGWs) from participating in the routing decisions. End-user identity information refines the selection of available WAN paths.
- LAN automation with dynamic segmentation: Most branch networks are needlessly complex because designs are based on a proliferation of VLANs, complex IP addressing schemes, access control lists (ACLs), and architectures tailored to the needs of automation software. The SD-Branch architecture flattens the branch into fewer subnets or even a single subnet, eliminating the dependence on static IP addressing schemes and hardwired ACLs across multiple devices. This is achieved by consolidating all policy enforcement into a single device in the branch.

Use this guide to design new networks or to optimize and upgrade existing networks. It is not intended as an exhaustive discussion of all options; it presents commonly recommended designs, features, and hardware.

Audience

This guide is written for IT professionals who need to design an Aruba SD-Branch network. These IT professionals serve in a variety of roles:

- Systems engineers who need a standard set of procedures for implementing solutions
- Project managers who create statements of work for Aruba implementations
- Aruba partners who sell technology or create implementation documentation.

Customer Use Cases

Branch networks are changing rapidly. The most pressing challenges include an increasing number of mobile and IoT devices, growing bandwidth requirements of the business, and modern users who expect connectivity for work and personal use from anywhere at any time. The teams that run these distributed networks are often shrinking while demands increase. Organizations expect new network rollouts within shorter timeframes, and IT organizations are asked to improve service levels, reduce costs, and shift spending from capital expense to operating expense.

This guide discusses the following use cases:

- Secure WAN communications using IPsec tunnels over an independent transport
- ZTP for all networking components in the branch
- Switch stacking for simplified management, high availability, and scalability
- Link aggregation for high bandwidth, redundancy, and resiliency between switches and gateways
- Wireless as the primary access method for branch employees
- Wireless and wired guest access for customers, partners, and vendors
- Consistent security for wired and wireless devices based on roles.

Aruba SD-Branch Network Deployment Overview

This section provides details for the SD-Branch deployment used in subsequent sections.

It is best practice to standardize the branch design for all sites to reap the full benefits of Aruba Central configuration. OWL Corp., however, has a requirement for two branch designs.

A pair of VPNCs (VPN concentrators) is configured to facilitate connectivity between the campus network and branch sites using IPsec tunnels and route sharing. VPNCs summarize the campus subnets to a single route of 10.0.X.X/13 and prevent advertising point-to-point links to the branches.

Each remote site has redundant branch gateways, and each gateway is connected to a single WAN transport. Switches at branch provide L2 connectivity for the APs and other client devices. Each branch site is assigned a /21 subnet from the superset address space of 10.14.X.X/16. Within the 10.14.X.X/16 address space, the 10.14.254.X/24 is reserved for Microbranch system IPs.



Figure 1: Network_Overview

Hub Site Configuration

- Gateways will be connected to the services aggregation block in the OWL campus network.
- Gateways will use OSPF to peer with the campus service aggregation.

- Gateways will have redundant connections to each aggregation block.
- Gateways will have redundant Internet and MPLS connections.
- Gateways will use eBGP for MPLS connectivity.
- The standby EdgeConnect appliance will have a lower metric than the primary to ensure route symmetry.
- EdgeConnect SD-WAN appliances will summarize campus routes before redistribution into the SD-WAN Fabric.
- Gateways will use the summary address 10.0.X.X/13 to advertise the Campus network to branch sites
- Gateways will summarize all branch sites to 10.14.X.X/16 to advertise to the Campus network.

RSVDC-VPNC1-1	VLAN	Local IP address	Port	Peer IP address	Peer Device
OSPF Uplink 1	4001	172.18.106.22/30	GE0/0/0	172.18.106.21/30	RSVCP-CR1-SS2-1
OSPF Uplink 2	4002	172.18.106.30/30	GE0/0/1	172.18.106.29/30	RSVCP-CR1-SS2-2
MPLS Uplink	2086	100.100.7.6	GE0/0/2	100.100.7.1	
Internet Uplink	2084	Static IP	GE0/0/3		
Microbranch (CL2)	101	10.8.0.2 - VRRP (10.8.0.1)			
Gateway System IP	2085	10.0.6.111/32			

RSVDC-VPNC1-2	VLAN	Local IP address	Port	Peer IP address	Peer Device
OSPF Uplink 1	4001	172.18.106.18/30	GE0/0/0	172.18.106.17/30	RSVCP-CR1-SS2-1
OSPF Uplink 2	4002	172.18.106.26/30	GE0/0/1	172.18.106.25/30	RSVCP-CR1-SS2-2
MPLS Uplink	2086	100.100.7.5	GE0/0/2	100.100.7.1	
Internet Uplink	2084	Static IP	GE0/0/3		
Microbranch (CL2)	101	10.8.0.2 - VRRP (10.8.0.1)			
Gateway System IP	2085	10.0.6.111/32			

Quantity	SKU	Description
2	9012	RJ45 console port 12 x 10/100/1000BASE-T ports 6 x PoE+ portsUSB Type A Host port 1xRJ45 console port Micro USB console port

NOTE:

The equipment listed may not be the same equipment used in the guide; however, the configuration steps are alike.

Branch Site Requirements

- Wi-Fi should be the main connection used by employees. Ethernet connections should be available for use as needed. Ensure that switchport count is available for all users
- Access points should be mounted to the ceiling, not above the ceiling tile in plenum space or behind any barrier that may cause signal reflection or attenuation.
- Wireless coverage is required.
- Employees use Office 365 and Microsoft Teams for communications, along with other business productivity apps (Salesforce, SAP, etc.).
- Sites use IoT devices such as smart thermostats, smart access control, and meeting room kiosk.
- Sites must be able to upgrade with hitless failover.
- Sites have a single MPLS 10 Mbps download 5Mbps upload and Internet connection 100 Mbps download 25Mbps upload. Both are RJ-45 drops.
- Employee and guest SSIDs must be provided.

Low Traffic Site Requirements

OWL's low traffic site have the logical topology shown below.



Low Traffic Site Characteristics

• 3750 square feet, closed office space

- Low-traffic sites to support up to 30 employees, each with a docking station and a laptop.
- 10 large workspace
- 12 small workspace
- 18 open workspaces
- 4 conference rooms
- 1 IDFs
- 1 MDF/Computer Room

Low Traffic Branch Site Configuration

- Gateway 1 will use GE0/0/0 Port for INET connectivity.
- Gateway 2 will use GE0/0/1 eBGP for MPLS connectivity.
- Gateway will use GE0/0/2 to trunk listed VLANs down to the access switches' highest ethernet port.
- Gateway will be the default gateway for the site.
- Gateway will enable RADIUS snooping.
- Gateway should be version 10.4 or higher.
- Gateway will use DHCP relay for addressing devices.
- Access switches will use the standard feature template (MOTD, RADIUS, TACACS, User-Roles, STP, etc.).
- The first 12 Ports on access switching will be reserved for the access points.
- All IOT devices will be reserved for the next 24 ports.
- Workstations will be revered for the last 12 ports (special case ports).
- Access points should have two SSIDs for Guest and Corporate access

Quantity	SKU	Description
2	9004	4 x 100/1000BASE-T ports1 x USB 3.0 portRJ45 console port Micro USB console port
2	6300F (JL663A)	48x ports 10/100/1000 BaseT ports 4x 1G/10G/25G/50G1 SFP ports 1x USB-C Console Port 1x OOBM port 1x USB Type A Host port 1x Bluetooth dongle to be used with CX Mobile App
6	Aruba 505 (R2H29A)	1.49 Gbps maximum real-world speed (HE80/HE20) WPA3 and Enhanced Open security Built-in technology that resolves sticky client issues for Wi-Fi 6 and Wi-Fi 5 devices OFDMA for enhanced multi-user efficiency IoT-ready Bluetooth 5 and Zigbee support

Required Equipment

NOTE:

The equipment listed may not be the same equipment used in the guide; however, the configuration steps are alike.

Miami Branch Details

VLAN			Default Gateway	MIABR-ECB1- 1 IP	MIABR-ECB1- 2 IP
ID	Description	Network	(VRRP)	Address	Address
100	MGMT (Gateway System IP)	10.14.0.0	10.14.0.1	10.14.0.2	10.14.0.3
101	Employee	10.14.1.0/	240.14.1.1	10.14.1.2	10.14.1.3
102	PRINTER	10.14.2.0	10.14.2.1	10.14.2.2	10.14.2.3
103	IoT (smart thermostats, smart access control, and meeting room kiosk.)	10.14.3.0,	/2 0 .14.3.1	10.14.3.2	10.14.3.3
104	Guest	10.14.4.0	10.14.4.1	10.14.4.2	10.14.4.3
105	Reject	10.14.5.0,	/20.14.5.1	10.14.5.2	10.14.5.3
106	Critical	10.14.6.0	10.14.6.1	10.14.6.2	10.14.6.3
107	Quarantine	10.14.7.0/	240.14.7.1	10.14.7.2	10.14.7.3
Sumr		10.14.0.0			

MIABR-			Peer IP	
ECB1-1	Local IP address	Port	address	Peer Device
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0,		MIABR-ECB1- CR1(STK)
MPLS Uplink		GE0/0/	′1——–	
Internet Uplink	DHCP (VLAN 4085)	GE0/0,		

MIABR-			Peer IP	
ECB1-2	Local IP address	Port	address	Peer Device
Access	Native VLAN: 100, Trunked VLAN:	GE0/0,		MIABR-ECB1-
Downlink	101,102,103,104,105,106,107			CR1(STK)

MIABR- ECB1-2	Local IP address	Port	Peer IP address	Peer Device
MPLS Uplink	MPLS (VLAN 4085)	GE0/0/	1	
Internet Uplink		GE0/0,		

MIABR-ECB1- CR1	Local IP address	Port	Peer port	Peer Device
MGMT VLAN	DHCP			
Gateway Uplink 1	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	1/1/23	GE0/0/3	MIABR- ECB1-1
Gateway Uplink 2	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	1/1/24	GE0/0/3	MIABR- ECB1-2

Huston Branch Details

		Default	HOUBR-	HOUBR-
VLAN		Gateway	ECBI-LIP	ECBI-2 IP
ID	Description	Network (VRRP)	Address	Address
100	MGMT (Gateway System IP)	10.14.8.0 10.14.8.1	10.14.8.2	10.14.8.3
101	Employee	10.14.9.0/ 20 .14.9.1	10.14.9.2	10.14.9.3
102	Printer	10.14.10.(10.14.10.1	10.14.10.2	10.14.10.3
103	IoT (smart thermostats, smart access control, and meeting room kiosk.)	10.14.11.0/209.14.11.1	10.14.11.2	10.14.11.3
104	Guest	10.14.12.(10.14.12.1	10.14.12.2	10.14.12.3
105	Reject	10.14.13.0/22414.13.1	10.14.13.2	10.14.13.3
106	Critical	10.14.14.(10.14.14.1	10.14.14.2	10.14.14.3
107	Quarantine	10.14.15.0/22414.15.1	10.14.15.2	10.14.15.3
Sumr		10.14.8.0		

HOUBR- ECB1-1	Local IP address	Port	Peer IP address	Peer Device
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0,	1/1/23	HOUBR-ECB1- CR1(STK)
MPLS Uplink		GE0/0/	/1	
Internet Uplink	DHCP (VLAN 4085)	GE0/0,		

HOUBR-			Peer IP	
ECB1-2	Local IP address	Port	address	Peer Device
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0,	1/1/24	HOUBR-ECB1- CR1(STK)
MPLS Uplink	MPLS (VLAN 4085)	GE0/0/	'1——–	
Internet Uplink		GE0/0,		

HOUBR- ECB1-CR1	Local IP address	Port	Peer port	Peer Device
MGMT VLAN	DHCP			
Gateway Uplink 1	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	1/1/23	GE0/0/2	HOUBR- ECB1-1
Gateway Uplink 2	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	1/1/24	GE0/0/2	HOUBR- ECB1-2

High Traffic Site Requirements

OWL's High traffic site have the logical topology shown below.



HIGH TRAFFIC BRANCH SITE CONFIGURATION

- All network infrastructure should use ZTP for provisioning.
- Gateway 1 will use WAN0 Port for INET connectivity.
- Gateway 2 will use WAN1 eBGP for MPLS connectivity.
- Gateways will be connected using LAN0 to enable WAN HA.
- Gateways will use LAN 1 to trunk listed VLANs down to the access switches' highest ethernet port.
- Gateways will use VRRP and be the default gateway for the site.
- Gateways will enable RADIUS snooping.
- Gateways should be version 9.2 or higher.
- Gateways will use DHCP relay for addressing devices.
- Access switches will use the standard feature template (MOTD, RADIUS, TACACS, User-Roles, STP, etc.).
- The first 12 ports on access switching will be reserved for the access points.
- All IoT devices will be reserved for the next 24 ports.
- Workstations will be reserved for the last 12 ports (special case ports).
- Access points should have two SSIDs for Guest and Corporate access

Quantity	SKU	Description
2	9004	4 x 100/1000BASE-T ports1 x USB 3.0 portRJ45 console port Micro USB console port
2	6300F (JL663A)	48x ports 10/100/1000 BaseT ports 4x 1G/10G/25G/50G1 SFP ports 1x USB-C Console Port 1x OOBM port 1x USB Type A Host port 1x Bluetooth dongle to be used with CX Mobile App
4	6200F (JL725A)	48x ports 10/100/1000 BaseT ports 4x 1G/10G SFP ports 1x USB-C Console Port 1x OOBM port 1x USB Type A Host port 1x Bluetooth dongle to be used with CX Mobile App
11	Aruba 505 (R2H29A)	1.49 Gbps maximum real-world speed (HE80/HE20) WPA3 and Enhanced Open security Built-in technology that resolves sticky client issues for Wi-Fi 6 and Wi-Fi 5 devicesOFDMA for enhanced multi-user efficiencyIoT-ready Bluetooth 5 and Zigbee support

NOTE:

The equipment listed may not be the same equipment used in the guide; however, the configuration steps are alike.

San Diego Branch Details

		Default	SANBR-ECB1-	SANBR-ECB1-
VLAN ID	Description	Network (VRRP)	Address	2 IP Address
100	MGMT (Gateway System IP)	10.14.16.(10.14.16.1	10.14.16.2	10.14.16.3
101	Employee	10.14.17.0/224.14.17.1	10.14.17.2	10.14.17.3
102	PRINTER	10.14.18. 10.14.18.1	10.14.18.2	10.14.18.3
103	IoT (smart thermostats, smart access control, and meeting room kiosk.)	10.14.19.0/122414.19.1	10.14.19.2	10.14.19.3
104	Guest	10.14.20. 10.14.20.1	10.14.20.2	10.14.20.3
105	Reject	10.14.21.0/22414.21.1	10.14.21.2	10.14.21.3
106	Critical	10.14.22. 10.14.22.1	10.14.22.2	10.14.22.3
107	Quarantine	10.14.23.0/12/414.23.1	10.14.23.2	10.14.23.3
Sumr		10.14.16.(——–		

SANBR- ECB1-1	Local IP address	Port	Peer IP address	Peer Device
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0,	1/1/23	SANBR-ECB1- CR1(STK)
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0/	31/1/24	SANBR-ECB1- CR1(STK)
MPLS Uplink		WAN1		
Internet Uplink	DHCP (VLAN 4085)	WAN0		

SANBR- ECB1-2	Local IP address	Port	Peer IP address	Peer Device
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0,	2/1/23	SANBR-ECB1- CR1(STK)
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0/	32/1/24	SANBR-ECB1- CR1(STK)
MPLS Uplink	MPLS (VLAN 4085)	WAN1		
Internet Uplink		WAN0		

San Francisco Branch Details

			Default	SFOBR-ECB1-	SFOBR-ECB1-
VLAN			Gateway	1 IP	2 IP
ID	Description	Network	(VRRP)	Address	Address
100	MGMT (Gateway System IP)	10.14.24.	10.14.24.1	10.14.24.2	10.14.24.3
101	Employee	10.14.25.	0/120414.25.1	10.14.25.2	10.14.25.3
102	PRINTER	10.14.26.	10.14.26.1	10.14.26.2	10.14.26.3
103	IoT (smart thermostats, smart access control, and meeting room kiosk.)	10.14.27.0	0/122414.27.1	10.14.27.2	10.14.27.3
104	Guest	10.14.28.	10.14.28.1	10.14.28.2	10.14.28.3
105	Reject	10.14.29.	0/122414.29.1	10.14.29.2	10.14.29.3
106	Critical	10.14.30.	10.14.30.1	10.14.30.2	10.14.30.3

		Default	SFOBR-I	ECB1- SFOBR-ECI	B1-
VLAN		Gateway	/ 1 IP	2 IP	
ID	Description	Network (VRRP)	Address	Address	
107	Quarantine	10.14.31.0/22414.31.	1 10.14.31.	2 10.14.31.3	
Sumr		10.14.24. ——-			

SFOBR- ECB1-1	Local IP address	Port	Peer IP address	Peer Device
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0,	1/1/23	SFOBR-ECB1- CR1(STK)
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0/	31/1/24	SFOBR-ECB1- CR1(STK)
MPLS Uplink		WAN1		
Internet Uplink	DHCP (VLAN 4085)	WAN0		

SFOBR- ECB1-2	Local IP address	Port	Peer IP address	Peer Device
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0,	2/1/23	SFOBR-ECB1- CR1(STK)
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0/	32/1/24	SFOBR-ECB1- CR1(STK)
MPLS Uplink	MPLS (VLAN 4085)	WAN1		
Internet Uplink		WAN0		

Preparing to Deploy Aruba SD-Branch Network

This section provides details for configuring Aruba Central to prepare for an SD-Branch deployment, including establishing interaction with HPE GreenLake.

Four requirements include: importing devices, licensing devices, creating groups, and creating site configuration.

This section also describes the fundamental differences between group and device configuration levels.

Device Management with HPE GreenLake

This section demonstrates how to applications to you HPE GreenLake account, add Aruba Central subscription keys, and add a new network device to the HPE GreenLake portal for management from Aruba Central.

The HPE GreenLake platform delivers a unified experience that enables customers to use a single dashboard to view, manage, and orchestrate the system's network, compute, storage infrastructure and related services.

Import and License Devices

To use Aruba Central, devices must be licensed and maintained in HPE GreenLake's inventory. Follow this procedure to import devices and apply the correct licenses. This article assumes that an account has been set up with HPE GreenLake and the Aruba Central application has been installed. If the prerequisite have not been complete, follow the documented process here.

Add a Subscription Key

Devices within Aruba Central require a subscription key to function. These keys grant access to various licenses, depending on the device type.

Step 1 On the HPE GreenLake top menu bar, select Manage.

Step 2 Click the Subscriptions tile.

Step 3 Click Add Device Subscription.

Step 4 In the **Add Device Subscription** window, enter the subscription key sent with the device or emailed after purchase. Click **Submit**.

Step 5 Repeat the process to continue adding subscription keys for additional devices as needed.



Figure 2: Add_Subscription_Key

Add a Device to GreenLake

Add network devices to HPE GreenLake using a .CSV file or by entering the Serial Number and MAC Address. Use the procedure below to enter the Serial Number and MAC Address. When complete, the device is assigned to Central automatically.

Step 1 On the HPE GreenLake top menu bar, select **Devices**.

Step 2 Click Add Devices.

Step 3 Select Network Devices as the Device Type, then click Next.

Step 4 On the Ownership Type list, click Serial Number & MAC Address.

Step 5 Type or paste the Serial Number and MAC Address values, then click Enter.

Step 6 Continue adding devices as needed. When finished, click Next.

Step 7 Tags are not entered in this example. Click Next.

Step 8 Review the list of devices and click Finish.

Step 9 Click Close.



Figure 3: Add_Device

Assign Subscriptions to the Devices

The following procedure assigns the subscription key to the device. This procedure demonstrates manual subscription key assignment, but the process can be automated for some device types. Instructions for the automated process can be found here.

Step 1 On the HPE GreenLake top menu bar, select Devices.

Step 2 Click the Require Subscriptions tile.

Step 3 Click the checkbox for each device to be assigned a subscription.

Step 4 Click the Actions menu.

Step 5 Click Apply Subscriptions.

Step 6 Select the Subscription Tier, then select the Subscription Key to apply.

Step 7 Click Apply Subscriptions.

Step 8 Click Finish, then click Close.

Step 9 Repeat steps 2 to 8 for additional device types that require licensing.

NOTE:

This process supports multi-select in step 3 to license multiple devices, when applying the same license.



Figure 4: Apply_Subscription

This concludes the steps performed in HPE GreenLake. After completing the above steps, the device(s) are available for use in Aruba Central.

If a device is offline, it does not appear in any Aruba Central groups. In Central, use **Device Preprovisioning** to assign a device to a group and apply appropriate group and device level configuration. After a device is connected, Central downloads the pre-provisioned configuration.

Define Groups in Aruba Central

A device's final configuration settings are defined by its group configuration, and additional devicespecific configurations, when applicable.

When creating device groups, the devices should have similar network functions so that common configurations such as VLANs, NTP, and DNS can be applied at the group level. Device-specific configurations, such as IP addresses, should be applied at the device level.

Central uses two group types: template groups and UI groups.

- Template groups are CLI-based configuration files pushed down to a device. Device-specific information can be defined using variables.
- With UI groups, all configuration is performed from the Central user interface. Device-specific configuration can be applied by selecting a particular device and configuring it individually in the user interface.

Template groups are an excellent choice when devices have overlapping configurations or when configurations do not change often. UI groups are a better choice for workflow-driven configurations and provide the flexibility to change single device configurations.

In both cases, devices in the same group must have similar configurations. If port layouts must change or the topology of the branch differs from other sites, create a unique group and configuration for that different site.



Figure 5: Configuration hierarchy

NOTE:

This graphic does not reflect the exact naming and type used in the guide. It is for reference purposes only.

Configure Device Groups

The following procedure creates a group. This guide uses the following groups and group types.

Device Type	Group Name	Group Type
VPNC	VPNC-RSVDC	UI Group
BGW, AOS-CX Switch, Access Point	BR-EC-SDB	UI Group
Micro Branch	BR-EC-MB	UI Group

Step 1 On the left navigation pane, in the Maintain section, select Organization.

Step 2 Click the Groups tab.

Step 3 Click the + (plus sign) to create a new group

Step 4 Enter a **Name** for the group, and select the appropriate checkbox in the **Group will contain** list. Follow the table above.

Step 5 Select the device Architecture and Network Role.



Step 6 Repeat Steps 3 through 5 for each group.



Create Sites

Central uses sites to group devices at the same geographical location. Sites also identify the gateways to be clustered together, and the APs and switches at the same location. This procedure creates sites, used later in this guide. This guide uses RSVDC, which is the hub location in Roseville CA. Chicago, Miami, and San Francisco are the example branch locations.

Step 1 On the Central Account Home page, launch the Network Operations app.

Step 2 In the dropdown, select All Devices.

Step 3 In the left navigation pane, in the Maintain section, select Organization.

Step 4 Click the Sites tile, then click New Site on the bottom left.

Step 5 In the Create New Site window, assign the following settings, then click Add.

- Site Name: RSVDC
- Street Address: 8000 foothills Blvd
- City: Roseville
- Country: United States
- State or Province: California
- Zip/Postal Code : 95747

Step 6 Repeat steps 4 and 5 for all remote sites. This guide uses the following sites:

Site Name
HOURBR
SANBR
MIABR
SFOBR

aruba Central						⑦ ₩ Å		

Figure 7: Adding Site

Preprovision Device in Central > Groups

Move the VPNC devices to the hub group (**VPNC-RSVDC**) and the branch gateways to the branch group (**BR-ECSDB**)

Step 1 In the Aruba Central app, set the filter to Global.

Step 2 Under Maintain, click Organization.

Step 3 Click the Device Preprovisioning tile.

Step 4 Select the device(s) to move to a selected group.

Step 5 Click the Move devices icon.

Step 6 Select the **Destination Group** from the dropdown.

Step 7 Click Move.

HPE GreenLake			
aruba Central			@ ⑦ Å
Customer: Orange TME			
II VPNC-RSV-DC			
Manage			
89 Overview			
Devices			
Eb Clients			
A Guests			
Applications			
Ø Security			
Analyze			
△ Alerts & Events			
Audit Trail			
💐 Tools			
a Reports			
- Maintáin			
Firmware			
E Organization			
Witting for internal-air central anabaseboords, com.			

Figure 8: Verify_Preprovisioning

Preprovision Device in Central > Sites

Move the VPNC devices to the hub site (**RSVDC**) and the branch gateways, switches, and access points to the branch sites (**MIABR**, **HOUBR**, **SANBR**)

Step 1 In the Aruba Central app, set the filter to Global.

Step 2 Under Maintain, click Organization.

Step 3 Click the Sites tile.

Step 4 Select the device(s) to move to a selected site.

Step 5 Drag the devices to the corresponding site.

Step 6 Click Yes to confirm the move.

NOTE:

This step requires the system MAC address of the devices to determine the site to which they are moved. If that is not plausible, devices can be moved to the correct group after a hostname has been established later in the deployment process.

HPE GreenLake					88
				۹ ۵	0 Å
🗱 BR-ECSDB 📀					
Security					
Analyze					
Audit Trail					
Nuoic Hait					
		-			
ង Organization					



Aruba VPNC Group Configuration

The VPNC is configured in two steps. First, the group level configuration includes all the common configurations such as NTP, DNS, and OSPF area. A majority of the configuration is performed at the group level. After the group is configured, device level configuration can be applied. Device level configuration includes entering device-specific information such as IP addresses, hostnames, etc.

Configure the VPNC Group

This procedure configures groups for VPNCs.

Step 1 In the Global filter dropdown, search or select the VPNC-RSVDC group.

Customer: Orange TME	
← 🙊 RSVDC-VPNC1-1	\oslash
黛 Global	
VPNC-RSVDC	×
업Groups	
VPNC-RSVDC	

Figure 10: Select Group

Step 2 On the left navigation pane, in the Manage section, select Devices.

Cu	stomer: Orange TME
ä	VPNC-RSVDC 🔿
— Ma	inage
88	Overview
0	Devices

Figure 11: Select Devices

Step 3 Select the **Gateways** tab, then click the **Config** (gear) icon in the upper right corner.

Customer: Orange TME	@ Gateways								Ih ∷≣ Summary List	Config
🛱 VPNC-RSVDC 🕓										-
- Manage	Gateways • Online 2 2	Offline Cl O	usters 0							
B Overview										
Devices	Gateways (2)								2	₹
- Series	Y Device Name	Y Model	Y IP Address	Y MAC Address	Y Serial	Firmware Version	Y Group	▼ Site	Uptime	
🖆 Clients	• 28:de:65:a7:ad:78	A9240	10.0.6.111	28:de:65:a7:ad:78	CNP5KYH001	10.4.0.0_86033	VPNC-RSVDC	RSVDC	3 hours 4 minutes	
ஃ. Guests	• 28:de:65:a7:b2:78	A9240	10.0.6.112	28:de:65:a7:b2:78	CNP5KYH00Q	10.4.0.0_86033	VPNC-RSVDC	RSVDC	3 hours 6 minutes	

Figure 12: Select Gateway

Step 4 Click Cancel, then click Exit.

Central	Guided Setup for VPNC Device 28:de:65:a7:b2:78
1 System 2 LAN 3 WAN	This wizard will guide you through the essential steps to configure the VPNCs in the Device 28:dec65:a7:b2:78. You can exit this wizard at any time by clicking cancel. You will be able to relaunch the wizard at any time as long as you have not yet completed all the steps. After completing this initial setup, you can change the settings at any time.
Tunnets & Routing	EXIT GUIDED SETUP Guided Setup will be exited and changes will be lost. You can re-enter the Guided Setup at any time to complete It. BESURE TOT
	Cancel Equin

Figure 13: Guided_Setup

Select the Hardware Model for the VPNC Group

Only one VPNC gateway model can be assigned for each group.

Step 1 On the Gateways tab, in the System section, select Model.

Step 2 In the **VPNC Model** dropdown, select the hardware model for the VPNC gateway group; for example: *A9240*.

Step 3 Use the toggle to disable **Automatic Group Clustering**, since clustering assigned at the site level.

NOTE: Clustering is required for MicroBranch and can be left enabled if needed. Exercise caution since other devices brought into the group are clustered.

HPE GreenLake						88
aruba Central	Search or ask Anuba			۹	\$	08
Customer: Orange TME			SELEC	C Survey	ry List	Carde
\$\$ VPNC-RSVDC 〇	Sarawan JA Tunnes & Routing VPN			Advanced I	· lode Gu	uided Setup
- Manage						
88 Overview	Practern Im Uns harragement Over					
Oevices	Specify the model of the VPNC devices that this group will contain. Show more					
La Clients	Per-field help					
🚓 Guests	VPNC Model A9240 -					
Applications						
Security						
- Anatyze						
🗷 Audit Trail						
🕰 Tools						
Reports						
- Maintain						
Firmware						
b Organization						
	In Automatic group clustering, all gateways belonging to the same group will act as a single gateway to allow better performance and redundancy. When disabled, each gateway operates individually. Enable automatic group					
	duzering					
© Copyright 2023 Hewlett Packard 8	merprise Development LP	Privacy Te	rms of Use Ad Choices	& Cookies Do Not Sell M	ly Personal	I information

Figure 14: hardware_selection

Step 4 Click Save Settings in the bottom right corner.

Set the VPNC Group System Time Parameters

Use this procedure to set the network time protocol (NTP) parameters and time zone to keep the VPNC clocks synchronized.

Step 1 On the Gateways tab, in the System section, select Time.

Step 2 In the **Public NTP Servers** table, click the **+** (plus sign) to add a public NTP server.

Customer: Orange TME	🙊 Gateways		
ជ VPNC-RSVDC 🛛	System LAN Tunnels & Rout	ing VPN	
- Manage			
B Overview	Platform Time DNS Ma	anagement oser	
Devices	Each gateway in the group wil	I automatically obtain its time using th	e Network Tin
□ Clients	Per-field help		
a Guests			
Applications	Public NTP Servers		+
Security	IPV4 ADDRESS/FQDN	BURST MODE	
Analyze			
∩ Alerts & Events			
Audit Trail			
A Tools		No data to display	
ш керorts			
- Maintain			
© Firmware			
😫 Organization			

Figure 15: Setting_NTP

Step 3 In the IPv4 Address/FQDN column, enter *pool.ntp.org* or other NTP server address.

Step 4 Check **Burst Mode** if this feature is supported by the NTP server. Burst mode provides faster time synchronization.

Customer: Orange TME	<u>@</u>				
법 VPNC-RSVDC 〇	System LAN Tunnels & Routing VPN				
- Manage	Platform Time DNS Management User				
Devices	Public NTP Servers	+			
□ Clients	IPV4 ADDRESS/FQDN BURST MODE				
🙁 Guests	pool.ntp.org	Î			
Applications					

Figure 16: configuring_NTP

Step 5 In the **Timezone** dropdown, choose the appropriate time zone, then click **Save Settings**.

	Gateways	
II VPNC-RSVDC	System LAN Tunnels & Routi	ng VPN
— Manage ————	Diatform Time DNS Ma	nagement User
🗄 Overview		nagement oser
Devices	Public NTP Servers	+
🗖 Clients	IPV4 ADDRESS/FQDN	BURST MODE
🙁 Guests	pool.ntp.org	Enabled
Applications		
Security		
— Analyze —		
🛕 Alerts & Events		
🛛 Audit Trail		
🖏 Tools		
💼 Reports		
— Maintain ————		
Firmware	Timezone	Inited States: America/Los Angeles (
😫 Organization		od
		Inited States:
		America/Los Angeles (UTC-08:00)

Figure 17: Timezone

Select a DNS Server for the VPNC Gateway

Specify the DNS server(s) the VPNC gateway uses to communicate with Central.

Step 1 On the Gateways tab, in the System section, select DNS.

Step 2 Select Specify DNS servers.

Step 3 In the **Domain name** text box, enter a domain name; for example: *example.local*.

Step 4 In the **Public DNS Servers** table, click the **+** (plus sign) to assign a public DNS server. For a virtual gateway VPNC, leave the default DNS provided by the cloud provider and go to step 6.

Step 5 In the **Provider** dropdown, select one of the listed providers, or select **Alternate DNS** if the desired server is not in the list.

Step 6 Click Save Settings.

HPE GreenLake		
		ବ 📮 📀 ଲି
Customer: Orange TME		
II VPNC-RSVDC		
Manage 88 Overview	Platform Time DNS Management Uter	
Devices		
🗂 Clients		
🚉 Guests	O Specify DNS servers Learn DNS configuration from DHCP	
# Applications		
Security		
- Analyze		
🗾 Audit Trail		
Reports		
Maliitain		
Firmware		
ta Organization		
		Concel Sove Settings
Copyright 2023 Hewlett Packard		

Figure 18: Configuring_DNS

NOTE:

The gateway uses this DNS server for DNS lookups. Clients do not use this DNS server.

Create a Management User Account

Create a management user account for CLI to access the gateways.

Step 1 On the Gateways tab, in the System section, select Management User.

Step 2 In the Local management users table, click the + (plus sign).

Customer: Orange TME		SELECTED GROUP TYPE VPNC	II. Summary	ill 🔞
업 VPNC-RSVDC 〇	System LAN Tunnels & Routing VPN	Ad	vanced Mode	Guided Setup
- Manage	Platform Time DNS Management User			
B Overview				
Devices	To be able to locally or remotely access the CLI console of the gateways in the group, you must either a local management user or enable centralized management user authentication using a RADIUS or TACACS Show more			
□ Clients	Per-field help			
🚉 Guests				
Applications				
Security	Local Management Users +			
- Analyze	NAME ROLE PASSWORD			



Step 3 In the Add Management User table, assign the following settings, then click Save.

- Name: admin
- **Password**: *password*
- Retype Password: password
- Role: Super user role

	Gateways
ជ VPNC-RSVDC 〇	System LAN Tunnels & Routing VPN
- Manage	Platform Time DNS Management User
🗄 Overview	
Devices	Per-tiela help
🗖 Clients	Add Management User
<u>න</u> , Guests	
Applications	Name admin
Security	Password
- Analyze	Retype password
☆ Alerts & Events	Role Super user role 👻
🗹 Audit Trail	
💐 Tools	Cancel
🔝 Reports	

Figure 20: MGMT_Name_PW



Step 4 Click **Save Settings** in the bottom right corner.

Create VLANs for Each Ethernet Port

Create five VLANs on the VPNCs including one each for WAN type of MPLS and Internet, and two for the LAN connections and OSPF peering to the campus infrastructure. The Gateway Pool VLAN is for the gateway's System IP address, configured for auto assignment.

Step 1 On the right side, click Advanced mode.

Step 2 Go to Interface, then select VLANs.

Step 3 In the VLANs table, click the + (plus sign).

Step 4 In the New VLAN window, configure the following VLANs, and click Save Settings.

VLAN Name	VLAN ID
MPLS	2086
INET	2084
GATEWAY_POOL	2085

VLAN Name	VLAN ID
OSPF_LAN_UPLINK_1	2001
OSPF_LAN_UPLINK_2	2002

NOTE:

VLANs 4080 and above are reserved. If these VLANs must be used, contact Aruba support.

HPE GreenLake		88
aruba Central		<u> </u>
Customer: Orange TME		
は VPNC-RSVDC 〇		
- Minage	Piatform Time DNS Management User	
BB Overview		
Devices		
⊈b Clients		
🚉 Guests		,
Applications		
Security		
- Analyze		
Ω Alerts & Events		
Audit Trail		
a Tools		
Reports		
Ga Firmware		
• Organization		
© Copyright 2023 Hewlett Packard E		

Figure 21: Creating_VLAN

Step 5 Verify the VLAN information in the summary table, then click **Save Settings** in the bottom right corner.

	Gateways			
LI VPNC-RSVDC	System WAN Interface Security VPN Routing High Availability Config A	udit		
— Manage ————	Ports VLANs DHCP Pool Management GRE Tunnels Bulk config	uration upload		
🗄 Overview				
Devices	Vlans			
🗖 Clients	NAME	ID(S)		
😩 Guests	GATEWAY_POOL	2085		
Applications	INET	2084		
Security	MPLS	2086		
- Analyze	OSPF_LAN_UPLINK_1	2001		
☆ Alerts & Events	OSPF_LAN_UPLINK_2	2002		
🖪 Audit Trail		1		

Figure 22: Complete_VLAN_List

Step 6 Configure the following settings on each VLAN in the IP Address Assignment section.

Interface	Enable Routing	IP Assignment	NAT Outside
MPLS	Checked	Static	
INET	Checked	Static	Checked
GATEWAY_POOL	Checked	Gateway Pool	
OSPF_LAN_UPLINK_1	Checked	Static	
OSPF_LAN_UPLINK_2	Checked	Static	

CAUTION:

DO NOT enable NAT on the **OSPF_LAN_UPLINK**, **MPLS**, or **Gateway Pool** VLANs.
HPE GreenLake			80
aruba Central			.a. 🖉 🖗 🔒
Customer: Orange TME			
업 VPNC-RSVDC 이			
- Mönage	Ports VLANs DHCP Pool Management GRE Tunnels Bulk config		
88 Overview			
Devices	Vians		
🗈 Clients			
🚉 Guests			
Applications			
Security			
- Analyze			
∯ Alerts & Events			
🔟 Audit Trail			
🔍 Tools			
Reports			
Maintain			
Firmware			
t: Organization			
© Copyright 2023 Hewlett Packard E			

Figure 23: Enable_Routing

Step 8 Enable OSPF for the *Gateway Pool*, OSPF_LAN_Uplink_1, and OSPF_LAN_Uplink_2 VLANs.

- Select the **OSPF_LAN_UPLINK_1**.
- Enable **OSPF**.
- Enter the **OSPF area**: 0.0.0.0.
- Click Save Settings.
- Repeat these steps for the **OSPF_LAN_Uplink_2** and **Gateway Pool** VLANs.



Figure 24: Enable_OSPF

Enable OSPF Globally

Although OSPF has been enabled for the VLAN, it is not enabled globally. The following procedure enables OSPF globally so the interfaces can participate in OSPF.

Step 1 On the Gateway tab in Advanced Mode, go to Routing > OSPF.

Step 2 Enable the OSPF toggle.

Step 3 Enter the Area ID: 0.0.0.0.



Figure 25: Enabling OSPF

Define the Gateway Pool

In the previous sections, the Gateway Pool VLAN was defined. However, it was not configured as a Gateway Pool. This procedure completes the Gateway Pool configuration, which automatically assigns Gateway IP Addresses.

Step 1 In **Advanced Mode**, go to **Interface** and select **Pool Management**. Expand the **Gateway Pool** option.

Step 1 Select the + (plus sign) to create a **Gateway Pool**.

Customer: Orange TME		-									
	Gateway	/s									
II VPNC-RSVDC	System	WAN	Interface	Security	VPN	Routing	High Availability	Config Audit			
Manage	Ports	VLANs		Pool M	lanagem	ent (GRE Tunnels	Bulk configuration u	pload		
E Overview						_					
Devices	> NA1	r Pools									
□ Clients	> Stat	eway Po	IAT DOI								
😩 Guests		Gatev	vay pool								
Applications		NAME							START ADDRESS	END ADD	DRESS
Security											
Analyze											
☆ Alerts & Events										10	
🛛 Audit Trail										L J	
🖏 Tools										No data to display	
n Reports		+									

Figure 26: Nav_Gateway_Pool

Step 3 Enter the pool of IP Addresses for the Gateway Pool.

- 1. Enter the Start IP address: 10.0.6.111.
- 2. Enter the End IP address: 10.0.6.120.
- 3. Click Save Settings.

Add New Gateway Pool	
Pool name:	Gateway Pool
Start IP address:	10.0.6.111
End IP address:	10.0.6.120

Figure 27: Gateway_Pool_Config

I AM HERE!!!!

Step 4 Go to Interface > VLANs.

	Gateways							
LI VPNC-RSVDC	System WAN Interface Security VPN Routing High Availability Config A	Config Audit						
— Manage ————	Ports VLANs DHCP Pool Management GRE Tunnels Bulk config	uration upload						
🗄 Overview								
Devices	Vlans							
🗖 Clients	NAME	ID(S)						
😩 Guests	GATEWAY_POOL	2085						
Applications	INET	2084						
Security	MPLS	2086						
- Analyze	OSPF_LAN_UPLINK_1	2001						
☆ Alerts & Events	OSPF_LAN_UPLINK_2	2002						
🖪 Audit Trail		1						

Figure 28: Nav_VLAN_List

Step 5 Select the Gateway Pool VLAN.

- Set the **IP Assignment** to *Gateway Pool*.
- Set the VLAN Pool to Gateway Pool.
- Click Save Settings

HPE GreenLake			
aruba Central			.a. 🖉 🔿 🔒
Customer: Orange TME			
🛱 VPNC-RSVDC 💦 🔿			
Mänago	Ports VLANs DHCP Pool Management GRE Tunnels Buik		
BB Overview Devices	Vlans		
👝 Clients			
🚉 Guests			
Applications			
Security			
Analyze			
ф. Alerts & Events			
🛛 Audit Trail			
🔦 Tools			
Reports			
- Maintain			
Firmware			
te Organization			
© Copyright 2023 Hewlett Packard E			

Figure 29: Applying Gateway Pool

Step 6 Go to System > General.

Step 7 Expand the System IP Address and select VLAN 2085 (the Gateway Pool VLAN).

Customer: Orange TME	ୁଲ Catoway
ば VPNC-RSVDC 〇	System WAN Interface Security VPN Routing High Availability Config Audit
- Manage	General Admin Certificates SNMP Logging Switching External Monitoring
B Overview	
Devices	> Basic Info
🗖 Clients	Domain Name System
<u>න</u> , Guests	> Dynamic Domain Name System
Applications	> Dynamic Domain Name System (HTTPS)
Security	V System IP Address
- Analyze	IPv4 address: VLAN 2085 V
☆ Alerts & Events	> Capacity Threshold
🛛 Audit Trail	> Location

Figure 30: Set System IP

Step 8 Click Save Settings

Assign the VLANs to the LAN Ports

After each VLAN is configured appropriately, the VLANs must be assigned to the correct ports.

Later in this guide, the VPNC is set up for One Touch Provisioning, so it is important to assign the correct port layout.

Step 1 Go to **Gateways > Config**. On the right side, click **Advanced mode**.

Step 2 Go to Interface > Ports.

Step 3 In the LAN ports/port channel table, click the + (plus sign).

Step 4 Select all the ports to be used. This example uses Ports Ge 0/0/0 - Ge 0/0/3.

HPE GreenLake		88
aruba Central		ፍ 🖉 🖉 🔒
Customer: Orange TME		SELECTED GROUP TYPE II. III III Config
ង vpnc-rsvdc 📀		Advanced Mode Guided Setup
- Manage	Platform Time DNS Management User	
88 Overview		₽
Devices		
🗈 Clients		
🚉 Guests		
Applications		
Security		
- Analyze		
Ω Alerts & Events		
🗹 Audit Trail		
🔩 Tools		
Reports		
- Maintain		
Firmware		
te Organization		
Copyright 2023 Hewlett Packard E	Phasy Terms of Use Ad	hoices & Cookies Do Not Sell My Personal Information

Figure 31: Selecting Ports

Step 5 Configure the Interface Type, VLAN ID and Description, and LLDP on each port, as shown below.

Port ID	Interface Type	VLAN ID	Description
Ge 0/0/0	LAN	2001	OSPF_LAN_UPLINK_1
Ge 0/0/1	LAN	2002	OSPF_LAN_UPLINK_2
Ge 0/0/2	WAN	2086	MPLS
Ge 0/0/3	WAN	2084	INET

NOTE:

Before registering an appliance with Central, interface Ge 0/0/1 can be reserved for One Touch Provisioning. Do not use this interface as a WAN port if DHCP addressing is required (such as an Internet circuit).

HPE GreenLake							88
aruba Central							🜻 🕐 🔒
Customer: Orange TME							
다 VPNC-RSVDC 이							
- Minago	Ports VLANS						
88 Overview							
Devices	Ports						
🖽 Clients							
🚉 Guests							
Applications							
Security							
Analyze							
ф. Alerts & Events							
🗵 Audit Tráil							
🐁 Tools							
💼 Reports	Port channel						
- Maintáin							
Firmware							
😫 Organization							



Step 6 Verify the port information in the summary table.

	Gateways									VEINC	Sumn
C VPNC-RSVDC	System WAN Int	erface Security N	/PN Routing High	Availability Config	Audit						Basic
- Manage	Ports VLANs DHCP Pool Management GRE Tunnels Bulk configuration upload										
E Overview											
Devices	Ports										
□ Clients	PORT	ТҮРЕ	\forall admin state	POLICY	MODE	\forall native vlan	γ access vlan	γ trunk vlans	TRUSTED VLANS	SPANNING TREE	DESCRIPTION
🚊 Guests	GE-0/0/0	LAN	Enabled	Not-defined	access		2001		2001	~	OSPF_LAN_UPLINK
Applications	GE-0/0/1	LAN	Enabled	Not-defined	access		2002		2002	~	OSPF_LAN_UPLINK
Security	GE-0/0/2	WAN	Enabled	Per-Session	access		2086		2086	√	MPLS
- Analyze	GE-0/0/3	WAN	Enabled	Per-Session	access		2084	-	2084	1	INET



Enable Tunnel Orchestrator Peering

In this procedure, the SD-WAN overlay orchestrator is enabled to automate establishing tunnels.

Step 1 On the Gateways tab in Basic Mode, go to Tunnels & Routing and select SD-WAN Overlay.

NOTE:

In **Advanced Mode**, go to **VPN > SD-WAN Overlay** and switch the overlay mode to orchestrated.

Step 2 Click Overlay Orchestrator Peering, then click Save Settings.

Customer: Orange TME	û Gateways	SELECTED GROUP TYPE II III III III III III III III III II	Config
법 VPNC-RSVDC 이	System LAN Tunnels & Routing VPN	Advanced Mode Guid	ided Setup
- Manage	SD-WAN Overlay Static Routing Route Maps Overlay Routing		
BB Overview			
Oevices	Enable Overlay Orchestration		
⊑a Clients	Ennuard branch internet traffic to a charific Nevt.		
알 , Guests	Hop router IP using PBR		



Configure Route Filtering

The VPNC filters out all point-to-point routes, 172.18.X.X/16, from the campus. This procedure creates a prefix list and a route map to accomplish the filtering.

Step 1 On the Gateways tab in Basic Mode, go to Tunnels & Routing and select Route Maps.

Step 2 Click the **Prefix List** dropdown, then click the **+** (plus sign) to create a new prefix list.

Step 3 Enter the following settings for the **Point-To-Point** prefix list.

- Name: PTP
- Sequence: 10
- Action: Deny
- Address: 172.18.96.0
- Mask: 255.255.224.0
- **GE:** 29

Step 4 Click the + (plus sign) to create a new prefix list. Enter the following settings for a **Catch all** prefix list.

- Name: ANY
- Sequence: 20
- Action: Permit
- Address: 0.0.0.0
- Mask: 0.0.0.0
- LE: 32

Step 5 Click Save Settings.

NOTE:

The LE and GE configurations are required to enable filtering or allow fewer specific prefixes. In this example, the point-to-point prefix list matches only network 172.18.96.0/19. It would not match the more specific route of 172.18.96.8/30.

	Gateways	5									
	System	LAN	Tunnels & Routing	VPN							
- Manage	SD-WAN	Overlay	Static Routing	Route Maps	Overlay Routing	r					
🗄 Overview						, 					
Devices	Configu	ire rout	e maps and prefix r	ules which can	be used for in an	y of the routing	protocols (OSPF,	BGP or overlay).	Show more		
_ Clients	Per-field	d help									
🚉 Guests	>	Comr	munity List								
Applications	~	Prefi	x List								
Security		Pret	fix rules								+
- Analyze		NAN	1E	SEQUENCE		ACTION	ADDRESS	MASK	GE	LE	
☆ Alerts & Events		any		20		permit	0.0.0.0	0.0.0.0		32	
🗷 Audit Trail		p2p		10		deny	172.18.96.0	255.255.224.0	29		
🖏 Tools											
🛍 Reports											
— Maintain ————											
Firmware											

Figure 35: Configure Prefix List

Step 6 Expand the **Route Map** dropdown, and click the + (plus sign) to create a new route map.

Step 7 Enter the following settings for the route map.

- Name: Block_PTP
- Sequence Number: 10
- Action: Permit

Step 8 In the Match box, click the + (plus sign) to add a match.

Step 9 Set the type to IP Address and set the value to the PTP Prefix list.

Step 10 Click the **+** (plus sign) to add another match. Set the type to **IP Address** and set the value to the **ANY** Prefix list.

Step 11 Click Save, then click Save Settings.

HPE GreenLake		
다 VPNC-RSVDC 이	System LAN Tunnels & Routing VPN	
- Manage	SD-WAN Overlay Static Routing Route Maps Overlay Routing	
Devices		
🗈 Clients		
<u>와</u> Guests	🗸 Community List	
Applications	Community list rules	
Security	NAME ACTION WELL KNOWN COMMUNITY COMMUNITY VALUE AS:NN	
- Analyze		
↓ Alerts & Events		
🗹 Audit Trail		
🖏 Tools		
	N. Beefin Liet	
t Organization	V Route Map	
		Cancel Sove Settings

Figure 36: Creating Route Map

Configure the Overlay Routing

Use this procedure to redistribute OSPF routes into the overlay so branches can reach corporate prefixes. Aruba SD-WAN automatically translates route costs between the overlay and data center to ensure symmetry.

Step 1 On the Gateways tab, in the Tunnels & Routing section, select Overlay Routing.

Step 2 On the **Overlay Routing** page, expand **Redistribution** to display the redistribution table.

Step 3 In the **Redistribution** table, click the **+** (plus sign) to create a new redistribution rule.

Step 4 In the **Source Protocol** dropdown, select *OSPF*. Static, connected, and BGP routes also are supported, though not shown in this example.

Step 5 In the **Filter** dropdown, select **Intra Area**, depending on the OSPF routes to be redistributed. Other options can be selected.

Step 6 In the **Route Map** dropdown, select the *Block_PTP* route map created in the previous procedure.

Step 7 Click Save Settings.

HPE GreenLake		
aruba Central		
Customer: Orange TME		
ង vpnc-rsvdc 📀	System LAN Tunnels & Routing VPN	
- Manage	SD WAN Overlay Static Routing Route Maps Overlay Routing	
BB Overview		
Devices		
🗈 Clients		
🔉 Guests	✓ Redistribution	
Applications	Redistribution Rules	
Security	SOURCE PROTOCOL FILTER ROUTE MAP	
- Analyze		
Alerts & Events		
Audit Trail		
a, Tools		
Reports		
Firmware	> Data Center Aggregate Routes	
• Organization		
Copyright 2023 Hewlett Packard E		

Figure 37: Redistribute Routes

Redistribute SD-WAN Routes

Step 1 In Advanced Mode, select the Routing tab.

Step 2 Select OSPF.

Step 3 Select Redistribution and click the + (plus sign).

Step 4 Select the source protocol **SDWAN Overlay**. Select the **Route Type** *E1* and set the **Cost**; in this case: *100*.

HPE GreenLake		
aruba Central		
Customer: Orange TME		
🕮 VPNC-RSVDC 💦 🔿	System WAN Interface Security VPN Routing High Availability Config Audit	
- Manage	IP Routes Policy-Based Routing NextHop Configuration RIP OSPF BGP Overlay Routing	
88 Overview		
Devices	IP routes	
🗈 Clients		
요. Guests		
Applications		
Security		
Analyze Alerts & Events		
R Audit Trail		
S. Tools		
🔊 Reports		
- Maintain	> Static Default Gateway	
Firmware		
🔓 Organization		

Step 5 Click Save Settings in the bottom right corner.

Configure Aggregation Routes

This procedure uses the DC aggregation routes to summarize the 10.X.X.X addresses in the campus into one summary address. The VPNC advertises the summary route 10.0.0.0/13 to each Branch Gateway. This is optional; however, it is recommended to summarize as much as possible to protect the route table size.

Step 1 On the Gateways tab, in the SDWAN & Routing section, select Overlay Routing.

Step 2 On the **Overlay Routing** page, expand **Data Center Aggregate Routes** to display the **DC Aggregate Routes** table.

Step 3 Uncheck **Allow branch to branch**. If selected, the VPNC becomes a transit site allowing branches to communicate through the VPNC. This is typically unwanted if all applications are centralized at the data center.

Step 4 In the **DC Aggregate Routes** table, click the **+** (plus sign) to create a new aggregate route. In this example, the 10.0.0.0/13 summary is used to summarize the corporate address space.

Step 5 In the IP Address column, enter 10.0.0.0, and in the Mask column, enter 255.248.0.0.

	Customer: Orange TME		SELECTED GROUP TYP VPNC
	업 VPNC-RSVDC 〇	System LAN Tunnels & Routing VPN	
	- Manage	SD-WAN Overlay Static Routing Route Maps Overlay Routing	
	Devices	This page allows you to configure the Overlay Routing Protocol in order to exchange routes between Gateways and VPNCs connected to the Overlay Orchestrator. Show more	
	⊑a Clients	Per-field help	
	a Guests	> Redistribution	
	Applications	✓ Data Center Aggregate Routes	
	Security	Allow branch to branch	
	- Analyze	DC Aggregate Routes	
	Д Alerts & Events	IP ADDRESS MASK	
	Audit Trail	10.0.0 255.248.0.0	
	🗞 Tools		
	💼 Reports		
	- Maintain		
	Firmware		
Step 6 Click Save Settings.	ង្ខ Organization		

Configure Static Routes

This procedure configures The VPNC gateways with the routes needed to form IPSEC tunnels over the INET and MPLS transports. The INET route is provided via a static default-gateway and the MPLS route is provided via a static route. In this example, the MPLS network can be summarized with the 100.100.7.0/24 prefix. These routes are applied at the group level, since they are the same for all gateways in the group; however, they could be applied at the device level if the next-hops differ. BGP also can be configured on the MPLS circuit to provide these routes, if desired. While the default gateway is configured as part of the OTP process of the gateway, also configure it at the group level.

In the first step illustrated below:

Step 1 In Advanced Mode select the Routing tab.

Step 2 Select IP Routes.

Step 3 Expand IP Routes.

Step 4 Click the + (plus sign) to create a new static route.

Step 5 Enter the following information to create the MPLS route. - Destination IP address: 100.100.7.0
- Destination network mask: 24 - Forwarding settings: Use Forwarding Router Address - Next hop IP address: 100.100.7.1 - Cost: 1* - Distance: 1

Step 6 Click Save Settings.

HPE GreenLake										88
aruba Central				O Search or ask Aruba					۹	۵ ۵
Customer: Orange TME	۰							SELECTED	GROUP TYPE	n 🗉 🤶
II VPNC-RSVDC O	System V		Routing High Availability Config Audit						Basi	c Mode Guided Setup
- Manage 2	IP Routes	Policy-Based Routing Next	Hop Configuration RIP OSPF BGF	P Overlay Routing						
BB Overview										
Devices	P Rou	routes								
⊑a Clients		DESTINATION IP ADDRESS	DESTINATION MASK	VINEXT HOP (FORWARDING ROUTER AL COST	DISTANCE	VIPSEC MAP NAME	NULL INTER	ACE		=
at Guests										
Applications										
Security					190					
- Analyze					No data to diretar					
Alerts & Events					the data to display					
🛛 Audit Trail	4	F								
🗞 Tools										
Reports		lew IP Route								
Birmware										
a Organization		IP version:	IPv4							
L Organization										
	5	Destination IP address:	100.100.7.0							
	_	Destination network mask:	255.255.255.0							
		Forwarding settings:	Using Forwarding Router Address 💙							
		Next hop IP address:	100.100.7.1							
		Cost:	1							
		Distance:	1							
									<u>6</u>	Save Settings
© Copyright 2023 Hewlett Packard B	interprise Devel	opment LP					Privacy T	erms of Use Ad Choices & Co	okies Do Nor Sel	My Personal Information

Figure 38: VPNC Static Route

In the second step illustrated below:

Step 1 Expand Static Default Gateway.

Step 2 Click the + (plus sign) to create a new static default gateway.

Step 3 Enter the following information to create the INET route.

- Destination IP address: Default Gateway IP
- Default Gateway IP: gateway IP of INET circuit
- Cost: 1

Step 4 Click Save Settings.

HPE GreenLake			88
	Search or asiX Anda	۹ 🌻	0 A
Customer: Orange TME		SELECTED GROUP TYPE	
업 VPNC-RSVDC 〇	University System (VM) Interface Security VPN Rewarding High Availability Config Avail	Basic Mode Guit	ided Setup
- Manage	P Rouses Policy-Based Routing Nexting Configuration RP 05FF BGP Overlap Routing		
88 Overview			
Devices	structure Sutio Default Gateway		
🗈 Clients	Static default gateway		
2. Guests	[∀] DEFAULT GATEWAY COST		-
Applications			
Security			
- Analyze			
Ω Alerts & Events	No data to daplay		
Audit Irail			
≪, Tools	2 +		
Malatala			
@ Firmware	New Default Cateway		
t Organization			
	IP version: IPv4		
	Defsuit Gateway IP IPSec Map		
	3 Default gateway IP.		
	Core .		
	> Dynamic Default Gateway		
		A Save Se	ettings
© Copyright 2023 Hewlett Packard	Privacy Terms of Privacy Terms of	Use Ad Choices & Cookies Do Not Sell My Personal I	Information

Figure 39: VPNC Default Gateway

Configure VPNC Devices

After the group level configuration is complete, assign device-level configurations. This section walks through the remaining configuration, which is unique to each VPNC. The procedure is provided for one VPNC, but it must be repeated for the second VPNC in the group. Since the devices were moved to the group using preprovisioning, this configuration is completed before the gateways come online.

Assign a VPNC Device to a Group and Site

This step should have been completed in the *Preparing to Deploy Aruba SD-Branch* chapter. If it was not, refer to the procedure here.

Configure VPNC Device

This procedure is illustrated for one VPNC, but must be repeated for the second VPNC in the group. Because the devices were moved to the group using preprovisioning, this configuration can be complete before the device comes online. Step 1 Go to the VPNC-RSVDC Group.



Figure 40: VPNC Select Group

Step 2 On the left menu, select Devices.

Cu	stomer: Orange TME
IJ	VPNC-RSVDC
— Ma	anage
88	Overview
0	Devices

Figure 41: VPNC Select Device

Step 3 In the gateway list, select the first gateway to configure. Correlate the system-mac to the device to select.

Customer: Orange TME	© Gateways									II. Summary	Config
업 VPNC-RSVDC 〇	,-										_
- Manage	Gateways 2	• Online 2	 Offline 0 	Clusters 0							
B Overview											
Devices	Gateways (2)										⊥ ⊙
U Devices	Y Device Name		Y Model	Y IP Address	Y MAC Address	▼ Serial	Firmware Version	Y Group	▼ Site	Uptime	
Clients	• 28:de:65:a7:ad:7	78	A9240	10.0.6.111	28:de:65:a7:ad:78	CNP5KYH001	10.4.0.0_86033	VPNC-RSVDC	RSVDC	3 hours 4 minutes	
🚉 Guests	• 28:de:65:a7:b2:3	78	A9240	10.0.6.112	28:de:65:a7:b2:78	CNP5KYH00Q	10.4.0.0_86033	VPNC-RSVDC	RSVDC	3 hours 6 minutes	

Figure 42: VPNC Select Group

Step 4 In the left navigation pane, select **Device**.

Customer: Orange TME					
← 🙊 28:de:65:a7:b2:78	Ø				
- Manage					
B Overview					
Q WAN					
ය. LAN					
Device					

Figure 43: VPNC Select Device 2

Step 5 In the guided setup window, click Cancel, then click EXIT.

orubo Central G	iuided Setup for VPNC Device 28:de:65:a7:b2:78
1 System	This witard will guide you through the essential steps to configure the VPNC's in the Device 28:de:65:a7:b2:78. You can exit this wizard at any time by clicking cancel. You will be able to relaunch the wizard at any time as long as you have not yet completed all the steps.
3 WAN	
(4) Tunnels & Routing	EXIT GUIDED SETUP Guided Setup will be exited and changes will be lost. You can re-enter the Guided Setup at any time to complete It.
	(везиме) сот
	Cancel

Figure 44: VPNC Cancel Guided Setup

Configure Hostname

Use this procedure to configure the hostname on the gateway.

Step 1 Go to the Gateway configuration and click Basic Mode.

Step 2 Select System > Hostname.

Step 3 Enter the Hostname.

Step 4 Click Save Settings.

HPE GreenLake				
				9 0 A
← ⊛ 28:de:65:a7:b2:78 ⊘				
	✓ Basic Info			
a LAN				
Device				
Applications				
Security				
	> Domain Name System			
	> Dynamic Domain Name System			
🖬 Audit Trail	> Dynamic Domain Name System			
🔦 Tools				
	> Location			

Figure 45: Configure Hostname

Configure the System IP for the VPNC Device

Use this procedure to define the system IP address the gateway will use for network services. Ensure that **Basic Mode** is still selected.

Step 1 Select System > System IP.

Step 2 In the VLAN Interface box, select the VLAN 2085.

	Customer: Orange TME	© Gateway	SELECTED DEVICE TYP VPNC
	← இ RSVDC-VPNC1-1 ⊘	System LAN WAN Tunnels & Routing	
	- Manage	System IP Hostname	
	B Overview		
	Q WAN	Each gateway requires a unique system IP address that is used by the gateway to communicate with network services such as VPN, RADIUS, syslog, TACACS+, and SNMP. The system IP addresses 1	or your gateways can be
	ය. LAN	Per-field help	
Step 3 Click Save Settings.	Device	VLAN Interface VLAN 2085 🔹	

Assign IP Addresses to the VLANs

Step 1 Select the LAN tab, and select VLANs.

Step 2 In the VLANs table, select the VLAN to update, then click the edit (pencil) icon.

Step 3 In the **VLAN** window, assign the following settings, then click **Save**. (These settings are for the first VPNC.)

VLAN Name	VLAN ID	IP Address	NetMask
OSPF_LAN_UPLINK_1	2001	172.18.106.18	255.255.255.252
OSPF_LAN_UPLINK_2	2002	172.18.106.26	255.255.255.252
MPLS	2086	100.100.7.5	255.255.255.240
INET	2084	X.X.X.X	X.X.X.X

HPE GreenLake		
aruba Central		<u>ዓ</u> ወ ሐ
Customer: Orange TME		
$\leftarrow @$ RSVDC-VPNC1-1 \bigcirc		
- Manage	System IP Hostname	
Q WAN		
a LAN		
Device		
🗈 Clients		
Applications		
Security		
- Analyze		
Ω Alerts & Events		
Audit Trail		
Maintain		
Firmware		
A Constitute 2027 Marchanic		

Figure 46: Configuring IP address

Step 4 Repeat steps 3 to 4 for each additional LAN uplink VLANs. The final configuration should look like the image below.

	Gateway				
$\leftarrow \ \ \mathbb{R}$ RSVDC-VPNC1-1 \bigcirc	System LAN WAN T	Funnels & Routing			
— Manage —	VLANs LAN ports				
B Overview					
Q WAN	Each gateway will requi	re one or more LAN VLANs and IP inter	faces to support infrastructure a	and client devices in your branches. Plea	se remember to atta
윪 LAN	Per-field help				
Device	VLANs				+
🗖 Clients	VLAN ID	NAME	IPV4 ADDRESS	NETMASK	
Applications	2001	OSPF_LAN_UPLINK_1	172.18.106.18	255.255.255.252	
	2002	OSPF_LAN_UPLINK_2	172.18.106.26	255.255.255.252	
Security	2084	INET			
- Analyze	2085	GATEWAY_POOL			
☆ Alerts & Events	2086	MPLS	100.100.7.5	255.255.255.240	

Figure 47: Final VLAN configuration

Configure the WAN Ports

In this procedure, configure the WAN uplinks and map them to the VLANs.

Step 1 Go to the WAN tab in Basic Mode.

Step 2 In the Uplinks table, click the + (plus sign).

Step 3 In the Add/Edit Uplink window, enter an uplink Name and select the uplink VLAN.

NOTE:

If **WAN type** is set to *Internet*, enter a public IP address or use a private address and configure 1:1 NAT translation on the internet edge firewall. If **WAN type** is set to *MPLS*, the uplink name must match between the VPNC and BGW to enable automated tunnel orchestration between gateways.

HPE GreenLake			88
aruba Cent			\$ (0) A
Customer: Orange TME			(B) Config
← ⊕ RSVDC-VPNC1-1			de Guided Setup
- Manage BB Overview	System 9 Hostname		
😔 WAN			Show more
器 LAN			
@ Device			
📼 Clients			
Applications			
Security			
Analyza			
Alerts & Events			
Audit Irali			
Reports			
- Maintain			
Firmware			
	Privacy Terms of Use Ad	Choices & Cookies Do Not Sell My R	Personal Information

NOTE:

While this example uses the name **MPLS** for the uplink, it is common to use a provider name to represent the private transport.

Onboard VPNC to Central

Static Provisioning (One Touch Provisioning)

The VPNCs in this deployment do not receive a DHCP address from any of their WAN connections, meaning they cannot communicate with Central. To register these devices with Central, One Touch Provisioning must be used. This step can be skipped if the gateways will connect to a device that assigns them a DHCP address and Internet access.

Step 1 Using the VPNC console port and a terminal, enter the settings below connect to the gateway.

- Baud rate: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Step 2 Select the **static-activate** option from the menu and follow the prompt to configure the WAN connection manually.

Auto-provisioning is in progress. It requires DHCP and Activate servers Chose one of the following options to override or debug auto-provisioning... 'enable-debug' : Disable auto-provisioning debug logs 'full-setup' : Statt full setup dialog. Provides full customization 'static-activate' : Provides customization for static or PPPOE ip assignment. Uses activate for conductor information Enter Option (partial string is acceptable): static-activate Enter Controller VLAN ID [1]: 2084 Enter Uplink port (EG 0/0/0]: EG 0/0/3 Enter Uplink port mode (access[trunk) [access]: access Enter Uplink Vlan Static IP address [192.168.1.1]: Enter Uplink Vlan Static IP address [192.168.1.1]: Enter Uplink Vlan Static IF address [192.168.1.1]: Enter Uplink Vlan Static IF address [192.168.1.1]: Enter Uplink Vlan Static IP actess [192.168.1.1]: Enter Uplink Vlan Static IP (segino) [ves]: no Do you wish to configure IFV6 address on vlan (yes]no) [ves]: no Do you wish to configure dynamic port-channel (yes]no) [no]: no Current choices are: Controller VLAN id: 2084 Uplink port: EG 0/0/3 Uplink Vlan Static IP nethod: static Uplink Vlan Static IP nethod: static Uplink Vlan Static IP Nethod: static Uplink Vlan IF address: Uplink Vlan IF dati I gate way: Domain Name Server to resolve FODN: 8.8.8.8 Option to configure VLAN interface IFV6 address: no Spanning-tree is disabled: no Do you wish to accept the changes (yes]no] Do you wish to accept the changes (yes]no]

Figure 48: Static-Activate

NOTE:

To bring up a Gateway using DHCP, see the "Configuring the Branch Gateway" section.

Deploying Branch Site

The following chapter of this guide includes procedures to configure three components of an Aruba SD-Branch site. This includes guidance on Branch Gateways, Switches and Access points.

Aruba Branch Gateway Configuration

In this set of procedures, the branch gateway (BGW) is configured in two steps. The first step is the group level configuration, where the bulk of configuration is performed. This includes all common configurations, such as NTP, DNS, and VLANs.

After the group configuration is complete, each BGW's device-specific configuration, such as hostname and IP addressing, is applied. This is applied before the device comes online with preprovisioning.

Create a Branch Gateway Group and Preprovision Gateways

Refer to the "Preparing to Deploy" section to create the branch group and move the gateways to the group.

Configure the Branch Gateway Group

Step 1 In **Global** dropdown, search or select the *BR-ECSDB* created in the "Preparing to Deploy" section.

뤛 Global	0
剑Global	
T BR-ECSDB	×
CGROUDS BR-ECSDB	

Figure 49: Select Group

Step 2 In the left navigation pane, in the **Manage** section, select **Devices**.

ä	BR-ECSDB]
— Ma	anage	
88	Overview	
0	Devices	

Figure 50: Select Devices

Step 3 Select the **Gateways** tab, then click the gear icon in the upper right corner.

Customer: Orange TME	Access Points Switches	@ Gateways		SELECTED GROUP TYPE Branch Gateway	th Summary	3 Souther
ଘ BR-ECSDB 이	System LAN WAN Tunnels	k Routing Policie		Adr	vanced Mode	Guided Setup
- Manage	Platform Time DNS Mar	agement User				
Devices	Each group will contain gatewa	s of the same mo	el (for example, 7005). Select the model of the gateways you plan on assigning to this group. Show more			

Figure 51: Select Config

Step 4 Click Cancel, then click Exit.

aruba Central	suided Setup for VPNC Device 28:de:65:a7:b2:78								
1 System	This witard will guide you through the essential steps to configure the VPNCs in the Device 28:de:65:a7:b2:78. You can exit this wizard at any time by clicking cancel. You will be able to relaunch the wizard at any time as long as you have not yet completed all the steps. After completing this initial setup, you can change the settings at any time.								
4 Tunnels & Routing	EXIT GUIDED SETUP Guided Setup will be exited and changes will be lost. You can re-enter the Guided Setup at any time to complete It.								
	IT. RESUME CXTT								
	Cancel Regin								

Figure 52: Guided_Setup

Configure Model

Use this procedure to set the gateway model. Each group can contain only a single gateway model.

Step 1 On the Gateways tab, in the System section, select Platform.

Step 2 In the **Model** dropdown select the platform you are standardizing on. In this case, **A9004** is selected.

Configure System IP Pool

Set the configuration approach to *Specify static IP address later*. This is done because the management VLAN will be used as the System IP address. Ensuring that the system IP is set to a VLAN that is trunked throughout the environment is critical for high availability and wired/wireless tunneling best practice.

HPE GreenLake			88
aruba Central	Q Search or ask Aruba	۹	¢ 🛛 🙈
Customer: Orange TME		SELECTED GROUP TYPE Branch Gateway	th :≡ 🛞 Summary List Confe
업 BR-ECSDB 〇	System LAN WAN Turnels & Routing Policies	Advan	nced Mode Guided Setup
- Manage	Platform Time DNS Management User		
88 Overview			
Devices	Each group will contain gateways of the same model (for example, 7005). Select the model of the gateways you plan on assigning to this group. Show more		
🖽 Clients	Per-field help		
a Guests	Model A5004 -		
Applications			
Security	on Ibo 9004		
Analyze			
Alerts & Events			
Audit Irail			
S Tools			
Maintain	This gateway group includes		
Firmware			
te Organization	site based auto-custering is automatically enabled to facultate LNN overlay establishment		
-	Configuration approach Define system IP address pool 💿 Specify static IP addresses later		
	 You do not define a System IP apoil. It is necessary to specify the We have a single start Person on a specific the statis or for multiple gateways area using the Buik configuration upload feature. 		



Set the System Time Parameters

Use this procedure to set the network time protocol (NTP) parameters and time zone to keep the BGW clocks synchronized.

Step 1 On the Gateways tab, in the System section, select Time.

Step 2 In the **Public NTP Servers** table, click the **+** (plus sign) to add a public NTP server.

HPE GreenLake							88
orubo Central			Q Se	earch or ask Aruba		٦	🤹 📀 Å
Customer: Orange TME	Access Points Switches	© Gateways			SELECTED GROUP TYPE Branch Gateway	th Summary	List Config
ឰ BR-ECSDB 🛛	System LAN WAN Tunne	Is & Routing Policies			Adı	vanced Mode	Guided Setup
- Manage	Platform Time DNS M	lanagement User					
BB Overview							
Devices	Each gateway in the group w	ill automatically obtain it	s time using the Network Time	e Protocol (NTP). You can either select one or more public NTP service providers (for example Google	, ntp.org etc.) or specify your own. St	low more	
🗈 Clients	Per-field help						
🚉 Guests	Public NTP Servers		+				
Applications	IPV4 ADDRESS/FQDN	BURST MODE					
Security							
- Analyze							
🗹 Audit Trail							
🖏 Tools		No data to display					
ជា Reports							
— Maintain							
Firmware							
😫 Organization							
	Timezone	Choose a timezone					
© Copyright 2023 Hewlett Packard E	interprise Development LP			Privacy Terms of	Use Ad Choices & Cookies Do N	ot Sell My Pers	onal Information

Figure 54: Setting_NTP

Step 3 In the **IPv4 Address/FQDN** column, enter *pool.ntp.org* or other NTP server address.

Step 4 Select **Burst Mode** if this feature is supported by the NTP server. Burst mode provides faster time synchronization.

HPE GreenLake							
Central			Q Searc				
Customer: Orange TME	la constante a cuitabas	<u>@</u>					
ជ BR-ECSDB 🛛	Svstem LAN WAN Tunn	els & Routing Policie	25				
Manage							
B Overview	Platform Time DNS P	Aanagement User					
Devices	Each gateway in the group w	vill automatically obta	ain its time using the Network Time Pro				
🗖 Clients	Per-field help						
😫 Guests	Public NTP Servers		+				
Applications	IPV4 ADDRESS/FQDN	BURST MODE					
Security	pool.ntp.com	Enabled					
- Analyze							
户 Alerts & Events							
🗾 Audit Trail							
ళ్ళ Tools							
🗓 Reports							
— Maintain ————							
Firmware							
ះ Organization							
	Timezone	United States: Ame	erica/Los Angeles (

Step 5 In the **Timezone** dropdown, select the time zone, then click **Save Settings**.

Figure 55: NTP Server

Set DNS Servers

Specify the DNS server(s) the BGW uses to communicate with Central.

Step 1 On the Gateways tab, in the System section, select DNS.

Step 2 Select Specify DNS servers.

Step 3 In the Domain name text box, enter a domain name (example: *example.local*).

Step 4 In the **Public DNS Servers** table, click the **+** (plus sign) to assign a public DNS server. For a virtual BGW, leave the default DNS provided by the cloud provider and go to Step 6.

Step 5 In the **Provider** dropdown, select one of the listed providers, or select **Alternate DNS** if the desired server is not in the list.



Figure 56: Configuring_DNS

Step 6 Click Save Settings.

NOTE:

The Gateway uses this DNS server for DNS lookups. Clients do not use this DNS server

Create a Management User Account

Create a management user account for CLI to access the gateways.

Step 1 On the Gateways tab, in the System section, select Management User.

Step 2 In the Local management users table, click the + (plus sign).

Customer: Orange TME	G Access Points		<u>@</u>		
┇ BR-ECSDB 〇	System LAN	WAN Tunnels	& Routing Policies		
— Manage	Platform Tim	e DNS Ma i	nagement User		
E Overview					
Devices	To be able to lo	ocally or remotel	ly access the CLI console	of the gateways in the group,	you must eith
Clients	Per-field help				
a Guests	AAA authentic	ation			
Applications		ation			
Security	Local Manag	gement Users			+
— Analyze ————	NAME	1	ROLE	PASSWORD	
☆ Alerts & Events					
🛛 Audit Trail					
🖏 Tools					
ቪ Reports					
— Maintain ————			No data to displ	ау	
Firmware					
ង Organization					

Figure 57: Add MGMT User

Step 3 In the **Add Management User** table, assign the following settings, then click **Save**. - **Name**: *admin* - **Password**: *password* - **Retype Password**: *password* - **Role**: *Super user role*

NOTE:

Create additional users with other roles as needed.

Customer: Orange TME	G Access Points		<u>@</u> Gateways	
ជ BR-ECSDB 🛛	System LAN	WAN Tunnels	& Routing Policies]
— Manage ————	Platform Tim	e DNS Man	agement User	
🗄 Overview		lp		
Devices	Fei-field fie	пр		
🗖 Clients	Add Man	agement User		
🚉 Guests				
Applications	Name		admin	
Security	Passwo	ord	•••••	•
- Analyze	Retype	password	•••••	
🛕 Alerts & Events	Role		Super	user role 💌
🛛 Audit Trail				
💐 Tools				Cancel Save
🙃 Reports				

Figure 58: MGMT_Name_PW

Step 3 Click Save Settings in the bottom left corner.

Configure VLANs

In this section, the data VLANs are configured. This configuration is at the group level, so none of these VLANs have an IP address assigned.

Step 1 On the right side, click Basic Mode.

Step 2 Go to LAN and select VLANs.

Step 3 On the **VLANs** table, click the **+** (plus sign).

Step 4 In the New VLAN window, configure the below VLANs, then click **Save Settings**. - Select **Enable DHCP relay** for VLANs 1. *10.2.120.98* 2. *10.2.120.99*

Step 5 Repeat steps for all VLANs

VLAN Name	VLAN ID
MGMT	100
Employee	101
Printer	102

VLAN Name	VLAN ID
Camera	103
Guest	104
Reject	105
Critical	106
Quarantine	107

HPE GreenLake								88
aruba Central								e o A
Customer: Orange TME								
🛱 BR-ECSDB 📀								
Manage								
88 Overview								
Devices								
🖽 Clients								
🔐 Guests								
Applications	VLANs							
Security	VLAN ID	NAME	STATIC	DYNAMIC DHCP POOL	DHCP RELAY			
– Ånalyze ————								
ф Alerts & Events								
🗾 Audit Trail								
🗞 Tools								
💼 Reports								
- Maintain								
Firmware								
😫 Organization								
								Save Settings



Configure LAN links

In this section, the LAN links are configured.

Step 1 On the right side, click **Basic Mode**.

Step 2 Go to LAN and select LAN ports.

Step 3 On the LAN Ports/Port Channels table, click the + (plus sign).

Step 4 Configure the LAN ports with the information in the below table

Name	Port	Mode	Access VLAN	Native VLAN	Allowed VLANs
GE2 Trunk to LAN	GE-0/0/2	trunk	blank	100	blank
GE3 Trunk to LAN	GE-0/0/3	trunk	blank	100	blank

HPE GreenLake									88
									@ 🔿 🖁
🛱 BR-ECSDB 📀									
- Manage	VI ANE LAN								
BB Overview									
Devices									
🖽 Clients									
🔐 Guests	LAN Ports	/Port Channel							
Applications	NAME	PORT	MODE	ACCESS VLAN	NATIVE VLAN	ALLOWED VLANS			
Security									
— Ánalyze ————									
▲ Alerts & Events									
🗾 Audit Trail									
🗞 Tools									
Crganization									
© Copyright 2023 Hewlett Packard E									

Figure 60: Configure_LAN_Ports

Configure WAN Uplinks

In this section, the WAN uplinks are configured. This configuration is at the group level, so none of these uplinks have an IP address assigned. Port 0/0/0 is used for the Internet connection and port 0/0/1 is used for MPLS. The **Uplink field** is generally the name of the service provider. For MPLS, ensure that the uplink field matches across all devices.

Step 1 On the right side, click Basic Mode.

Step 2 Go to WAN and select WAN Details.

Step 3 On the **WAN Uplinks/Ports** table, click the + (plus sign).

Step 4 In the New WAN Uplink / Port window configure the MPLS and INET uplinks.

MPLS:

- Uplink: MPLS
- WAN Type: MPLS
- WAN Speed: 10
- Source NAT: Unchecked
- Use as Back: Unchecked
- IP Addressing Method: Static
- Port: GE 0/0/1
- Secure with ACL: Unchecked

INET

- Uplink: INET
- WAN Type: INET
- WAN Speed: 20
- Source NAT: Checked
- Use as Back: Unchecked
- IP Addressing Method: DHCP
- **Port:** *GE* 0/0/0
- Secure with ACL: Checked

HPE GreenLake									
aruba Central									🕫 🔿 🖁
Customer: Orange TME									
🛱 BR-ECSDB 📀									
- Manage									
88 Overview									
Devices									
La Clients									
🔐 Guests									
Applications									
Security	WAN Uplinks/Ports								
– Ánalyze ————	UPLINK	ТҮРЕ	PORT	VLAN ID	ADDRESS	WAN SPEED	NAT	BACKUP	
🗾 Audit Trail									
🔩 Tools									
Reports									
- Maintain									
Firmware									
😫 Organization									

Figure 61: Setting WAN Uplinks

Configure the WAN Load Balancing Algorithm

Uplink utilization is recommended for use as the load balancing algorithm. This moves traffic from oversaturated links to a less used link if the bandwidth threshold is exceeded.

Step 1 On the configuration Gateways tab in Basic Mode, go to WAN and select Load Balancing.

Step 2 In the Load balancing mode list, select Uplink utilization.

Central						
Customer: Orange TME	0					
	Access I	Points	Switches		Gatew	ays
BR-EC3DB	System	LAN	WAN	Tunnels 8	& Routing	Policies
- Manage	Health	Checks	Load	Balancing	WAN D	etails
E Overview					-	
Devices	Gatew	/ays sup	port thr	ree differe	nt load-ba	lancing algoi
🗖 Clients	Per-fie	eld help				
2. Guests	Load	balanci	ing mod	e 🔿	Round ro	bin
Applications				0	Session o	ount
Security				۲	Uplink ut	ilization

Figure 62: Configure WAN Load Balancing Algorithm

Configure the Overlay and Set the VPNC Preference

Use this procedure to assign data center preferences for tunnel orchestration for the VPN concentrators (VPNCs).

Step 1 In basic mode select Tunnels & Routing, then DC Preference.

Step 2 In the **DC Preference** table, click the **+** (plus sign) to add a VPNC hub group.

Step 3 In the **Hub Group** dropdown, select a VPNC group to assign the preferred data center.

Step 4 In the **Primary VPNC** dropdown, select the primary VPNC.

Step 5 In the Secondary VPNC dropdown, select the secondary VPNC, then click Save Settings.

NOTE:

VPNCs do not appear unless they have been configured. See the "Configuring VPNC" section to configure the VPNCs.

aruba Central			Q Search or ask Aruba	
Customer: Orange TME	lo Emitados	<u>@</u>		
🛱 BR-ECSDB 🔅	System LAN WAN Tunne	Is & Routing Policies		
- Manage	DC Preference Static Routin	g Overlay Routing		
Devices	If your deployment includes	VPN Concentrators (VPNCs) deploye	d in one or more hub sites, your gateways c	an be configured to c
🗖 Clients	Per-field help			
🚉 Guests	(i) Overlay Orchestrator	peering is Enabled		
Applications	0	0		
Security	DC Preference			+
- Analyze	HUB GROUP	PRIMARY VPNC	SECONDARY VPNC	
Alerts & Events	VPNC-RSVDC	RSVDC-VPNC1-1 [28 🔻	RSVDC-VPNC1-2 [28 💌	î
🗷 Audit Trail				

Figure 63: Enabling Overlay

Step 6 Repeat steps 3 to 5 if a secondary data center is used. Groups higher in the list (with lower numbers) are treated as more preferred VPNC groups.

NOTE:
The procedures in guide do not use a second DC; this is just an example.

Enable Overlay Routes

In this procedure, branch subnets are redistributed into the VPN overlay to ensure route reachability with other sites.

Step 1 In Basic mode, select Tunnels & Routing, then Overlay Routes.

Step 3 In **Redistribute connected vlans**, select all the user VLANs and system IP VLAN for overlay redistribution, then click **Save Settings**.

				Q	Search o	r ask Aruba	
Customer: Orange TME		Acces) Points	Sv		چ Gatew	ays
IJ	BR-ECSDB	System	System LAN WAN Tunnels &		& Routing	Policies	
— M	lanage	DC Pr	eference	Statio	c Routing	Overlay	Routing
88	Overview						-
0	Devices						
ᄃ	Clients	Rec	istribute	e connect	ted vlans		
ą	Guests						
	Applications	Rec	istribute	e static ro	outes		
0	Security						
— A	nalyze						
¢	Alerts & Events						
	Audit Trail						
z	Tools						
ŵ	Reports						
— M	laintain						
٥	Firmware						
ŝ	Organization						



Enable DPI and Application Visibility

Deep packet inspection and Application Visibility must be enabled for Dynamic Path Steering and SAAS Express to function. This section describes how to enable these features.

NOTE:

This procedure will cause the gateways to reboot to apply the configuration.

Step 1 Verify that the Gateway configuration mode is in **Advanced Mode**.

Step 2 Select the Security tab, then select Applications.

Step 3 Expand the Application Visibility section.

Step 4 Check the Deep packet inspection checkbox.

Step 5 Check the App performance monitoring checkbox.

Step 6 Click Save Settings.

HPE GreenLake					88
Central		Q Search or ask Aruba			۹ 🌻 🖗 ک
Customer: Orange TME	Access Points Switches Gateways			SELECTED GROUP TYPE Branch Gateway	II. III Summary List Config
법 BR-ECSDB 〇	System WAN Interface Security VPN Routing High A	Availability Config Audit		1	Basic Mode Guided Setup
Manage	Roles Policies Aliases Applications Apply Policy	Auth Servers Role Assignment (AAA Profiles)	L2 Authentication L3 Authentication	Advanced Firewall	
8 Overview					
Devices	Application Visibility				
🗅 Clients	Firewall visibility:	✓			
😩 Guests					
Applications	4 Deep packet inspection:	~			
Security	5 App performance monitoring:	✓			
- Analyze					
Alerts & Events	Web content classification (webcc):				
Audit Trail	Drop packets during webcc miss:				
🖏 Tools					
Reports	URL to redirect blocked session:				
Maintain	IP classification and reputation:				6
& Organization					
te Organization				Cancel	Save Settings
© Copyright 2023 Hewlett Packard E	Interprise Development LP		Privacy Terms of Use	Ad Choices & Cookies Do N	Not Sell My Personal Information

Figure 65: Enable DPI & Application Visibility

NOTE:

Deep packet inspection is enabled by default at the device level, but it is best practice to also enable it at the group level.

Configure Policies for Dynamic Path Steering

The dynamic path steering (DPS) feature allows traffic routing in real-time and traffic load balancing across available uplinks based on the performance of the uplinks. DPS policies and configurations are unique to each environment, based on the organization's applications and performance needs. General guidance on developing a DPS policy can be found in the design section of the guide here. This section describes how to configure a DPS policy to select the optimal WAN path and apply forward error correction (FEC) for voice traffic.

Additional policies should be created based on application requirements.

NOTE:

While this example deployment does not utilize LTE connections, LTE is included in the below policy to facilitate the future addition of LTE uplinks without the need to modify the policy.

Create Policy

Step 1 Verify that the Gateway configuration mode is in Basic Mode.

Step 2 Select the Policies tab, then select DPS.

Step 3 Click the + (plus sign) to create a new DPS policy.
HPE				00
GreenLake		C Search or ask Aruba	Q	
Customer: Orange TME		SELECTED GROUP TYPE Branch Gateway	th :	
법 BR-ECSDB 이	System LAN WAN Tunnels & Routing Policies		dvanced Mode	Guided Setup
Manage	Roles Applications DPS 205 Secu	rity		
E Overview				
Devices	Use traffic policies to define the behavior of client t	traffic passing on the WAN. After defining the traffic rules for the policy, the minimum path quality needed for this traffic can be defined throug	gh an SLA. Show	more
□ Clients	Policies +	3		
🕰 Guests		-		
Applications				
Security				
Analyze				
☆ Alerts & Events	No data to display			
Audit Trail				
🖏 Tools				
🔝 Reports				
- Maintain				
t∰ Firmware				
le Organization			Cancel	Save Settings
© Copyright 2023 Hewlett Packard E	terprise Development LP	Privacy Terms of Use Ad Choices & Cookies Do	Not Sell My Person	hal Information

Figure 66: Create DPS Policy

Step 4 In the **Create Policy** window, assign the following settings and click **Save**.

- Policy Type: DPS
- Policy Name: Protect-Voice

HPE GreenLake		
aruba Central		Q Search
Customer: Orange TME	la Englista	<u>.</u>
ជ BR-ECSDB 📀	System LAN WAN Tunnels 8	Routing Policies
- Manage	Roles Applications DPS F	PBR QoS Security
E Overview	Per field belo	
Devices		
🗖 Clients	Create Policy	
😩 Guests	Policy Type	DPS 🗸
Applications	Policy Name	Protect-Voice
Security		
Analyze		Cancel



Identify Traffic

Step 1 Select Protect-Voice.

Step 2 Click the edit (pencil) icon in the **Traffic Rules** section.

HPE GreenLake								88
Central		Q Search or ask Aru	ba				۹	2 🕈 🎗
Customer: Orange TME	Access Points Switches Gateways					SELECTED GROUP TYPE Branch Gateway	II. Summary	III (Config
🛱 BR-ECSDB 💦	System LAN WAN Tunnels & Routing Poli	cies				A	dvanced Mode	Guided Setup
Manage	Roles Applications DPS PBR OoS S	ecurity						
B Overview		,						
Devices	Use traffic policies to define the behavior of clie	ent traffic passing on the WAN. After defi	ning the traffic rules for th	e policy, the minimu	m path quality needed for this traffi	c can be defined throug	gh an Shov	more
🗂 Clients	Every DPS policy should have primary W	'AN path and atleast one traffic rule confi	gured. And every SaaS pol	icy should have prim	nary exit profile and SLA configured.	And please select an Si	LA with loss thr	eshold
<u>ಖ</u> Guests	(i) configured If FEC Is enabled. Please review Protect-Voice.							
Applications	Policies +	Traffic Rules for Protect-Voice	/	2				
Security	1 Protect-Voice	Click pencil icon to create rules		-				
Analyze								
☆ Alerts & Events								
🗹 Audit Trail								
🖏 Tools		Actions for Protect-Voice						
🔝 Reports		SLA:	WAN Path	1				
Maintain —		Latency:	- Primary:					
Firmware		Loss:	 Last resort: 	-				
ំ Organization		Litilization					Cancel	
© Convright 2023 Hewlett Packard Er	tarnrise Devalopment I P				Privacy Tarme of Liea Ad C	hoires & Cookies Do	Not Sall My Pare	onal Information

Figure 68: Identify Traffic 1

Step 3 Click the + (plus sign) to create a new traffic specification rule.

Curctor Curctor or as Auto Curctor or as Auto Start or as	GreenLake												88
Currenter Orange TME <							Q Search	or ask Arub	Da		۹	Ģ	0 2
2 BR-ECSDB 2 BR-ECSDB Advanced Mode	Eustomer: Orange TME	Acce	6 ss Points	Switches	© Gateways				SELECTED G Branch Ga	OUP TYPE	th Summary	i List	Confi
Manage © Overview © Dovlocs © Collents & Guests @ Applications © Reports a Audit Traili > Tools > Perrors Wantardin > Promware • Organization <td>IBR-ECSDB 이</td> <td>Syste</td> <td>m LAN</td> <td>WAN Tunnels</td> <td>& Routing Polic</td> <td>ies</td> <td></td> <td></td> <td></td> <td>A</td> <td>ivanced Mode</td> <td>Gui</td> <td>ided Setup</td>	IBR-ECSDB 이	Syste	m LAN	WAN Tunnels	& Routing Polic	ies				A	ivanced Mode	Gui	ided Setup
○ Verview Use traffic policies to define the behavior of client traffic passing on the WANA. After defining the traffic rules for the policy, the minimum path quality needed for this traffic can be defined through an SLA. Path selection preference Show more © Clients © Energips plays should have primary WANA path and atleast one traffic rule configured. And every SaaS policy should have primary out profile and SLA configured. And plasse select an SLA with loss threshold configured I FEC is enabled. > Applications • Fer-field help > Arests & Events > Aduit Trail > Apports > No data to display > Application > No data to display • Ferrimer Organization	Aanage	Role	s Applic	ations DPS	PBR QoS Si	curity							
be belies be traffic policies to define the behavior of client traffic passing on the WAAA. After defining the traffic rules for the policy, the minimum path quality needed for this traffic can be defined through an SLA. Path selection preference. Show more show more show the policy and show the behavior of client traffic passing on the WAAA. After defining the traffic rules for the policy, the minimum path quality needed for this traffic can be defined through an SLA. Path selection preference. Show more show more show the policy and show	Overview												
a Clients b Clients c C	Devices	Us	e traffic pol	licies to define th	e behavior of clie	nt traffic p	bassing on the WAN. After defin	ing the trafi	ffic rules for the policy, the minimum path quality needed for this traffic can be defined through an SLA. Path s	election pr	eference Sh	iow mo	ore
Guests Guests Guests Applications Construct Total Aderts & Events Judit Trail Tools Granization Firmware Organization	3 Clients		Every D	PS policy should	have primary W	AN path ar	nd atleast one traffic rule config	ured. And e	every SaaS policy should have primary exit profile and SLA configured. And please select an SLA with loss three	hold confi	gured if FEC is	s enabl	led.
Applications y Security halfyze A klerts & Events A klerts & Events A klerts & Events A klerts & Traific Specification Rules for Process-Value Tools Roports Anitation P Firmware O opgnization	Guests		Per-field h	elp									
Security Addrt Sale Addrt Tail Tools Reports Aidents Area to display Firmware Organization	Applications												
Source Source Destination A clars & Evens Audit Trail A clars & Evens B clars & Evens <	9 Security		← Tra	ffic Specification	n Rules for Prote	ct-Voice		+	< <u>3</u>				
A Alers & Events J Aulit Tail J Aulit Tail Tools Tools No data to display	Analyze		SOURCE		DESTINATION		APPLICATION						
A ddi Trail Tools No data to diophy Reports taihtain Firmware Organization	Alerts & Events												
Tools No data to display Reports All and an and and and and and and and and	Audit Trail												
Reports aintain	Tools				No	data to displa	ay						
Cancel Sector	Reports												
Organization Cancel Series Ser	Firmware												
Cancel Service	Organization												
Cancel Investment													
Cancel Exercised													
											Cancel		

Figure 69: Identify Traffic 2

Step 4 In the Add Rules for Protect-Voice window, assign the following settings and click Save.

- Source: Any
- **Destination:** Any

- Application/Port: App Categories
- App Categories: unified-communications

HPE GreenLake				
orubo Central				Q Search or ask
Customer: Orange TME	Constants Switch	<u>@</u>		
ជ BR-ECSDB 🛛	System LAN WAN Tun	nels & Routing Policie	s	
- Manage	Roles Applications DP	5 PBR QoS Sec	urity	
Devices	Per-field help Add Rules for Protect	t-Voice		
🗖 Clients				
음 Guests	Source	Any	• •	
Applications	Destination	Any	•	
Security	Application/Port	Арр	Categories 🔹	
⚠́ Alerts & Events	App categories	searc	l-communications ×	
🛛 Audit Trail				
🖏 Tools			Cancel	Savo
Reports			Cancel	Jave

Figure 70: Identify Traffic 3

Step 5 Click the back arrow.

HPE GreenLake																					88
orubo Central			Q Search o	or ask Arul	ruba														۹	Ģ	0 2
Customer: Orange TME	G Switche	<u>e</u> Gatewaye															SELECTED G Branch Ga	ROUP TYPE	LL Summary	iiii Ust	
ය BR-ECSDB 이	System LAN WAN Tuni	nels & Routing Policies																A	dvanced Mo	de Gi	ided Setu
Manage	Roles Applications DPS	S PBR OoS Security																			
B Overview																					
Devices	Use traffic policies to defin	e the behavior of client traf	fic passing on the WAN. After definit	ing the trai	raffic ru	c rules	les fo	for the	e policy,	, the mir	nimum pa	th quality n	leeded for	his traffic c	n be define	d through	an SLA. Path s	election p	reference	Show n	nore
3 Clients	Every DPS policy sho	ould have primary WAN pat	h and atleast one traffic rule configu	gured. And	nd every	ery Sa	Saas	s polic	licy shou	uld have	e primary e	exit profile a	and SLA co	ifigured. An	d please sele	ect an SLA	with loss thre	shold cont	igured If FEG	: is ena	bled.
🔒 Guests	Please review protein	ct-voice.																			
Applications					_																
Security	5 ← Traffic Specifica	ation Rules for Protect-Void	•	+																	
Analyze	SOURCE	DESTINATION	APPLICATION																		
ት Alerts & Events	Any	нлу	Application Category unified																		
Audit Trail																					
k Tools																					
] Reports																					
Maintain																					
a Firmware																					
g Organization																					
																			Cancel	s	
© Convright 2023 Hewlett Packard I	Enterorise Development I P													Privacy	Terms of U	se Ad	Choices & Cook	ies Do	Not Sell My	Persona	Informati



Set WAN Paths

HPE _____ GreenLake 88 orubo Central Q Search or ask Aruba ۹ ¢ 🤉 🛎 SELECTED GROUP TYPE er: Orange TME ill List 🛱 BR-ECSDB System LAN WAN Tunnels & Routing Policies Applications DPS PBR QoS Security B Overview Devices _ Clients Traffic Rules for Protect-Voice 🔉 Guests ÷ All Application Category unified Applications Security Alerts & Events Actions for Protect-Voice 🗹 Audit Trail SI A. ñ WAN Path 🗞 Tools Latency: Jitter: Loss: Utilization: Secondary: Last resort: 🗊 Reports Firmware Loss Correction (FEC): Loss % with FEC: FEC Ratio: 😫 Organization Cancel Save Settin © Copyright 2023 Hewlett Packard Enterprise Development LP Privacy Terms of Use Ad Choices & Cookies Do Not Sell My Personal Information

Step 1 Select Protect-Voice and click the pencil icon next to WAN Path.

Figure 72: WAN Path 1

Step 2 In the WAN Path for Protect-Voice window, assign the following settings and click Save.

- Primary path: ALL_MPLS
- Secondary path: ALL_INET
- Last resort path: ALL_LTE

HPE GreenLake		
Central		Q Sea
Customer: Orange TME		
🛱 BR-ECSDB	System LAN WAN Tunnels & Routing Policies	
Manage	Roles Applications DPS PBR QoS Security	
Oevices	Per-field help	
🗖 Clients	WAN Path for Protect-Voice	
2 Guests	ALL_MPLS ×	
 Applications 	Primary path search	
Security	Secondary path	
Analyze	search	
☆ Alerts & Events	Last resort path	
🛛 Audit Trail	search	
🖏 Tools		
n Reports		ancel Save
Maintain		



Configure SLA

Step 1 Select Protect-Voice and click the edit (pencil) icon next to SLA.

Step 2 In the **Select SLA for Protect-Voice** window, assign the following settings and click **Save**.

- SLA: BestforVoice
- Loss Correction (FEC): Checked
- Loss % with FEC: 5
- FEC Ratio: 1:4

					Q Search or ask Aru	ıba
Customer: Orange TME	Access	Points Switches	<u>@</u> Gateways			
ជ BR-ECSDB 이	System	LAN WAN Tunne	Is & Routing Policies			
Manage	Roles	Applications DPS	PBR Oos Securit	w.		
		Applications		7		
O Devices	Pe	r-field help				
Clients	5	Select SLA for Protect-	Voice			
🙁 Guests		NAME	LATENCY (MS)	JITTER (MS)	LOSS (%)	UTILAZATION (%)
Applications		BestForSkype	50	30	1	
Security		BestForTeams	250	30	10	
Analyze		BestForVideo	150	20	1	a
↑ Alerts & Events		BestForZoom	150	40	2	-
		CriticalData-Bulk	300		5	
Audit Irail			100		-	
		Loss Correction (FEC)		\checkmark		
🔧 Tools		Loss % with FEC		5		
🔪 Tools ៊្នា Reports						
乳 Tools 記 Reports Maintain		FEC Ratio		1:4	•	

Figure 74: WAN Path 3

Step 3 Review the configuration and click Save Settings.

HPE GreenLake								88
orubo Central		Q Search o	r ask Aruba				۹	¢ 🛛 2
Customer: Orange TME	Access Points Switches Gateways					SELECTED Branch C	GROUP TYPE II. Gateway Summary	List Config
Manage	System LAN WAN Tunnels & Routing Police	25					Advanced Mode	Guided Setup
Overview	Roles Applications DPS PBR QoS Se	urity						
Devices	Use traffic policies to define the behavior of clier	t traffic passing on the WAN. After defini	ng the traffic rules fo	r the policy, the minimu	m path quality needed for this traffic c	an be defined through an SLA. Path	selection preference Sho	w more
Clients	Policies +	Traffic Rules for Protect-Voice	1					
🚉 Guests	Protect-Voice	All Application Category unified-comm	unications traffic					
Applications								
8 Security								
Analyze		Actions for Protect-Voice						
Alerts & Events		SLA: BestEpri/gice	WAN Path	1				
Audit mail		Latency: Less than 150 ms.	Primary:	ALL_MPLS				
T Reports		Jitter: Less than 30 ms. Loss: Less than 1%	Secondary: Last resort:	ALL_INET ALL LTE				
Maintain		Utilization: -						
🔅 Firmware		Loss Correction (FEC): Enabled Loss % with FEC: 5						
😫 Organization		FEC Ratio: 1:4						
								3
							Cancel	Save Settings
© Copyright 2023 Hewlett Packard E	interprise Development LP				Privacy	Terms of Use Ad Choices & Co	okies Do Not Sell My Perso	onal Information

Figure 75: Review Policy DPS

Configure Policies for SAAS Express

The SAAS Express feature allows traffic routing from the best Internet egress point based on the performance of the Internet egress points for the given application. SAAS Express policies and configurations are unique to each environment, based on the organization's applications and performance needs. General guidance developing a SAAS Express policy can be found in the design section of the guide here. This section describes how to configure a SAAS Express policy to optimize Office 365 traffic.

NOTE:

While this example deployment does not utilize LTE connections, LTE is included in the below policy to facilitate the future addition of LTE uplinks without the need to modify the policy.

Additional policies should be created based on application requirements.

Create Policy

Step 1 Verify that the Gateway configuration mode is in Basic Mode.

Step 2 Select the Policies tab, then select DPS.

Step 3 Click the + (plus sign) to create a new SAAS Express policy.



Figure 76: Create SAAS Policy

Step 4 In the Create Policy window, assign the following settings and click Save.

- Policy Type: SAAS
- Application: office365

HPE GreenLake								
orubo Central								Q Search
Customer: Orange TME		0			٩			
ג BR-ECSDB	Syst	tem LAN	WAN	Tunnels	Gatewa & Routing	Policies		
- Manage	Ro	les Appli	cations	DPS	PBR QoS	Security		
B Overview		- C-141				-		
Devices		Per-tield r	neip					
∟ ī Clients		Create	Policy					
🚉 Guests		Policy	Туре			SAAS	•	
Applications		Applic	ation			office365	•	
Security		i	Custom Express	apps can > Config"	be created (under "Global	> Applicat	ions > SaaS
- Analyze				0				
♀ Alerts & Events							_	
🗾 Audit Trail							Canc	el Save
🖏 Tools								

Figure 77: Create SAAS Policy

Configure SLA

Step 1 Select **saas_office365_wp** and click the edit (pencil) icon beside **SLA**.

orubo Central		Q Search or ask Aruba			Q
Customer: Orange TME	Access Points Switches	e cateways			SELECTEI Branch
រះ្ហា 🖾 BR-ECSDB 🔅	System LAN WAN Tunnels 8	& Routing Policies			
— Manage —	Roles Applications DPS	PBR OoS Security			
B Overview					
Devices	Use traffic policies to define the	behavior of client traffic passing on	the WAN. After defining the traffic rules for t	he policy, the minimum p	bath quality needed for this traffic can be defined through an SLA.
Clients	Every DPS policy should	have primary WAN path and atleast of	one traffic rule configured. And every SaaS pr	olicy should have primary	vexit profile and SLA configured. And please select an SLA with los
a Guests	Please review saas_omic	2305_wp.			
Applications	Policies	+ Traffic Rules for	r saas_office365_wp		
Security	Protect-Voice	All Application Ca	ategory office365_saas traffic		
- Analyze					
↓ Alerts & Events					
🛛 Audit Trail		Actions for saas	_office365_wp		
🖏 Tools		SLA:	Exit Profile:	i	
🔝 Reports		Latency:	- Primary:		
— Maintain ————		Jitter:	- Secondary:	-	
Firmware		Utilization:	- Last resort:	-	
ះ Organization					

Figure 78: Create SAAS SLA Pencil

Step 2 In the Select SLA for saas_office365_wp window, select the BestforSaaS SLA.

					G Search or ask.				Q	Č (
ner: Orange TME	0	=	<u> </u>					SELECTED GROU Branch Gatew	PTYPE II.	:=
ECSDB O	Access Points	Switches	Gateways					branch back	ay sama,	U.A.
	System LAN	WAN Tunnels 8	Routing Policies						Advanced Mode	Guideo
e	Roles Applica	tions DPS	PBR QoS Secur	ty						
erview	Per-field be	In								
vices	T CI-IICIG IIC	'P								
ents	Select SL	A for saas_office	365_wp							
ortr										
6515	SLA						+			
plications	NAME		LATENCY (MS)	JITTER (MS)	LOSS (%)	UTILAZATION (%)				
urity			50							
e	2 Be	stForSaaS	400	120	2					
rts & Events	Be	stForTeams	250	30	10					
dit Trail	L 50	strorzoom	150	40	2					
uit fran										
bls										
ports										
in										
nware						Cancel	save			
tanization										
samzauon										

Step 3 Click Save.

Figure 79: SAAS Express Create SLA

Configure Exit Profile

Step 1 Select saas_office365_wp and click the edit (pencil) icon beside Exit Profile.

HPE GreenLake													
Central				Q Search	or ask Aruba							۹	۹
Customer: Orange TME	G Access Points	E Switches	@ Gateways								SELECTED GROUP Branch Gatewa	SELECTED GROUP TYPE Branch Gateway	SELECTED GROUP TYPE II. Branch Gateway summary
I BR-ECSDB	System LAN	WAN Tunnels	& Routing Polici	s								Advan	Advanced Mode
age	Roles Applie Use traffic po	cations DPS blicles to define the	PBR QoS Se e behavior of clier	urity t traffic passing on the WAN. After defi	ning the traffic rules f	or the policy, the minim	um path quality need	de la	ed for this traffic ca	ed for this traffic can be defined thr	ed for this traffic can be defined through an SLA. Path select	ed for this traffic can be defined through an SLA. Path selection	ed for this traffic can be defined through an SLA. Path selection Show
Devices					-							-	-
Clients	Every I Please	DPS policy should review saas_offic	have primary WA e365_wp.	I path and atleast one traffic rule confi I path and atleast one traffic rule confi	gured. And every Saa	S policy should have pri	imary exit profile and	SL	A configured. And	A configured. And please select a	A configured. And please select an SLA with loss threshold	A configured. And please select an SLA with loss threshold configure	A configured. And please select an SLA with loss threshold configured if FEC is
Guests	Policies		+	Traffic Rules for saas office365 w									
Applications	Protect-	Voice		All Application Category office365_sa	as traffic								
Security	saas_offi	ice365_wp											
Analyze													
🗘 Alerts & Events													
Audit Trail				Actions for saas_office365_wp									
Tools				SLA: BestForSaaS	Exit Profile:								
Reports				Latency: Less than 400 m	s. Primary:								
Aaintain				Loss: Less than 120 m	s. Secondary: % Last resort:								
Firmware				Utilization:									
Grganization													
												Ĺ	Cancel
© Copyright 2023 Hewlett Packard 8	Enterprise Developm	tent LP						Privacy		Terms of Use	Terms of Use Ad Choices & Cookies	Terms of Use Ad Choices & Cookies Do Not	Terms of Use Ad Choices & Cookies Do Not Sell My Pers

Figure 80: SAAS Express Create Exit Profile Pencil

Step 2 In the Exit Profile for saas_office365_wp window, select the default profile BestForSaaS and click Save.

HPE GreenLake		
aruba Central		Q Search
Customer: Orange TME		<u>@</u>
ば BR-ECSDB 〇	System LAN WAN Tunnels & Ro	uting Policies
— Manage —	Roles Applications DPS PBR	OoS Security
B Overview		
Devices	Per-field help	
🗖 Clients	Exit Profile for saas_office36	5_wp
a. Guests	Name	BestForSaaS X
Applications		
Security	Primary path	search
— Analyze ————	Cocondamy wath	
☆ Alerts & Events	Secondary path	No secondary path selected
🛛 Audit Trail	Last resort path	No last resort path selected
🖏 Tools		
航 Reports		Cancel
— Maintain ————		

Figure 81: SAAS Express Create Exit Profile 1

Step 3 Review the configuration and click Save Settings.

GreenLake			
aruba Central		Q Search or ask Aruba	ې 🙎 🧟
Customer: Orange TME	arcers Points Switches	S B	LECTED GROUP TYPE
🛱 BR-ECSDB 📀	System LAN WAN Tunnels & Ro	Policies	Advanced Mode Guided
- Manage	Poles Applications DDS DDR		
BB Overview	Roles Appleadors D13 For	ou accumy	
Devices	Use traffic policies to define the bel	or of client traffic passing on the WAN. After defining the traffic rules for the policy, the minimum path quality needed for this traffic can be defined through an :	LA. Path selection preference Show more
Clients	Policies	+ Traffic Rules for saas, office365, wp	
a. Guests	Protect Voice	All Application Category office365_saas traffic	
Applications	saas_office365_wp		
Security			
Analyze			
🗘 Alerts & Events		Actions for saas_office365_wp	
🛛 Audit Trail		SLA: BestForSaaS Exit Profile: BestForSaaS	
4 Tools		Latency: Less than 400 ms. Primary: ALL_UPLINKS Jitter: Less than 120 ms. Secondary: -	
Reports		Loss: Less than 2% Last resort:	
Maintain			
Ø Firmware			
ង្ខ Organization			
			Cancel Save S
© Convright 2023 Hewlett Packard I	Enterorise Development I P	Privany Terms of Like Aid Cho	ices & Cookies Do Not Sell My Personal Info

Figure 82: SAAS Express Review Configuration

Configure Branch Gateway at the Device Level

In this section the primary Miami branch gateway is configured. This gateways can be preconfigured offline, and obtain their configuration when connected to Central. Ensure that the Branch Gateways are assigned to the group and site as demonstrated in the Preparing to Deploy section.

Start the Branch Gateway Configuration

Step 1 On the Aruba Central Account Home page, launch the Network Operations app.

Step 2 In the dropdown, select the branch gateway group containing the devices.

Step 3 In the left navigation pane, in the **Manage** section, select **Devices** and select the **Gateways** tab.

Step 4 In the **Gateways** table, select the device to configure as the primary branch gateway.

Step 5 In the Guided Setup window, click Cancel, then click Exit.

HPE GreenLake							88
aruba Central							📮 🕐 🐧
Customer: Orange TME							
⊈ Global							
- Manage							POTENTIAL ISSUES
88 Overview							
Devices							
🖽 Clients							
왔. Guests							
Applications							
Security							
🛠 Network Services							
Analyze							
▲ Alerts & Events							
🔟 Audit Trail							
🔩 Tools							
Reports							
- Launch							
App Catalog							
- Maintain							
 Himware 							
Crganization							
Copylight 2023 Hewlett Packard Enterp	onse Development LP			Privacy Ter	rms of Use Ad Choices &	Cookies Do No	Self My Personal Information

Figure 83: Starting branch configuration

Assign a Hostname

Step 1 Go to the Gateway configuration and verify that **Basic Mode** is enabled.

Step 2 Select System and Hostname.

Step 3 Click the basic info dropdown and enter the **Hostname**.

Customer: Orange TME	٩				
← ♀ R1B20A-20:4C:03: ▲	Gateway System	LAN	WAN	Tunnels & Routing	Redundancy
— Manage ————	System	IP H	ostname	e	
B Overview					
Q WAN	Hostname			MIABR-ECB1-2	
ය. LAN					
💿 Device					

Figure 84: configure Hostname

Assign IP Addresses to the VLAN

Use this procedure to assign LAN VLAN IP addresses. The DHCP relay was preconfigured at the group level.

Step 1 Ensure that the Gateway configuration mode is in **Basic Mode**.

Step 2 Select the LAN tab and select VLANs.

Step 3 In the VLANs table, select one of the VLANs, and click the edit (pencil) icon.

Step 4 In the **VLAN** window, assign the following settings, then click **Save**. (These IP address are for the Miami site)

			Default Cataway	MIABR-ECB1-	MIABR-ECB1-
	Description	Network		I IP Address	2 IP Address
	Description	NELWOIK		Address	Address
100	MGMT (Gateway System IP)	10.14.0.0	10.14.0.1	10.14.0.2	10.14.0.3
101	Employee	10.14.1.0/	2140.14.1.1	10.14.1.2	10.14.1.3
102	PRINTER	10.14.2.0	10.14.2.1	10.14.2.2	10.14.2.3
103	IoT (smart thermostats, smart access control, and meeting room kiosk.)	10.14.3.0/	′2 0 .14.3.1	10.14.3.2	10.14.3.3
104	Guest	10.14.4.0	10.14.4.1	10.14.4.2	10.14.4.3.
105	Reject	10.14.5.0/	′ 2⊕ .14.5.1	10.14.5/.2	10.14.5.3
106	Critical	10.14.6.0	10.14.6.1	10.14.6.2	10.14.6.3
107	Quarantine	10.14.7.0/	240.14.7.1	10.14.7.2	10.14.7.3
Sumr		10.14.0.0			

Step 5 Repeat step 3 and 4 for all VLANs in the table above.

HPE GreenLake			88
			ዲ 📮 😨 🖁
← 🙊 R1B20A-20:4C:03: 📐			
	System IP Hostname		
욺 LAN			
Device			
Applications			
Security			
🗹 Audit Trail			
🔩 Tools			

Figure 85: Assigning an IP to VLAN

NOTE:

Clicking **Save Settings** after changing each VLAN IP is unnecessary. All VLAN IP changes can be saved at the same time.

Configure the MPLS VLAN

The MPLS VLAN must be configured statically with an IP address and gateway. The DNS is used for health checks on the interface.

Step 1 Ensure that the Gateway configuration mode is in **Basic Mode**.

Step 2 Go to WAN and select WAN Details.

Step 3 Scroll and select the MPLS VLAN. (Be sure the local gateway VLAN is selected.)

Step 4 Enter the IPv4 Address, Gateway IP, Netmask, and DNS Servers for the MPLS VLAN.

Step 5 Click Save.



Figure 86: Configuring MPLS IP

Assign System IP Address

Use this procedure to select the Management VLAN as the system IP address.

Step 1 Ensure that the Gateway configuration mode is in **Advanced Mode**.

Step 2 In the System section, select General and expand System IP Address.

Step 3 In the dropdown, select VLAN 100.

Step 4 Click Save Settings.

HPE GreenLake			88
aruba Central	Search or ask Aruba	۹	\$ 0 A
Customer: Orange TME	© Gateway	SELECTED DEVICE TYPE Branch Gateway	Config
← ŵ MIABR-ECB1-1 ⊘	System W4N Interface Security VPN Routing High-Availability Config Audit		Basic Mode Guided Setup
- Manage	General Admin Certificates ShMP Logging Switching External Monitoring		
Q WAN	> Basic Info		
हरे LAN	Clock Domain Name System		
Device	Dynamic Domain Name System		
Clients	> Dynamic Domain Name System (HTTPS)		
Applications	MAC address: 20.4cr03b59112		
- Analyze	Ibut address		
🗹 Audit Trail	Loopback Interface Capacity Threshold		
N Iools	> Location		
Maintain			
Ø Firmware			
		Cancel	Save Settings
© Convright 2023 Hewlett Packard F	Internities Development LP Drivery Terms of Like and C	hoises & Cookies Do N	int Sell My Demonal Information

Figure 87: configure Hostname

Configure the LAN Redundancy

Step 1 Ensure that the Gateway configuration mode is in Basic Mode.

Step 2 In the Redundancy section, select Preferred Cluster Leader.

Step 3 Set the Preferred Cluster Leader to MIABR-ECB1-1.

Step 4 In the **Cluster Virtual Router IPs** table, click the **+** (plus sign).

Step 5 In the **VLAN ID** dropdown, select a LAN VLAN. The IP Address on Local and IP Address on Peer columns should autopopulate with the IP address values.

Step 6 In Virtual IP column, enter an IP address; for example, 10.14.0.1.

Step 7 Repeat steps 3 and 4 for all user VLANs.

Step 8 Click Save Settings.

NOTE:

Ensure that **Automatic Clustering** and **Auto Site** are both enabled at the group level by selecting **BR-ECSDB > Select Advanced mode High Availability > Clusters**.

HPE GreenLake								88
								🕫 🔿 🙈
← @ MIABR-ECB1-1 ⊘		els & Routing Redundancy						
	Cluster VRRP							
Device								
	Preferred Cluster Lea	ıder						
	GATEWAY		PREFFERED LEADER					
C Security								
• Security								
Audit Trail								
	Cluster Virtual Route	r IPs						
	VLAN ID	IP ADDRESS ON LOCAL	ADDRESS ON PEER	VIRTUAL IP	CLUSTER MANAGEMENT			



Configure WAN Redundancy for Specific Deployments (Optional)

If only one of each WAN transport is available at a site with redundant gateways, WAN transports can be shared over the LAN. For example, the INET circuit terminates on one gateway and the MPLS circuit terminates on another gateway. As long as the gateways are reachable over the LAN, they can share the respective WAN transports. **This configuration is not used in this deployment because the sites have redundant connections for both INET and MPLS**. In this example, site RS01 is shown, with VLAN 100 used for connectivity between the gateways. Follow these steps to configure WAN redundancy. **Step 1** Verify that the Gateway configuration mode is in **Basic Mode**.

Step 2 Select the WAN tab, then select WAN Details.

Step 3 Turn on Enable High Availability deployment.

Step 4 In the **Peer Gateway** section, select the gateway at each site.

Step 5 Ensure that all the WAN transports appear in the **WAN Uplinks / Ports** table.

NOTE:

As long as both gateways have the same site-id the peer gateway and site ID are populated automatically and grayed out.

Branch Switch Configuration

The primary function of the switch in this branch deployment is to provide power and layer 2 access to wired devices and APs. Each branch deployment should have the same physical connectivity, to minimize differences in the template. OWL has the requirement for two different switch topologies. To accommodate OWL's requirements there will be two switch templates one for the collapsed core and one for the access switch. The majority of the configuration will be the same for both switches, the only difference will be in the uplinks/Downlinks. The following section will leverage templates to configure the switches.

Templates leverage variables to apply unique configuration to switches. Variables are created by using percent sign on both sides of a string in a configuration file. This string is defined by the admin, this string will become a column in a CSV file that will need an input from the admin. Below is an example of how variables are created/formatted.

```
interface Vlan 10
ip address %VLAN_IP%
```

Switch Name	%VLAN IP% Variable Input
Example-SW-01	10.0.0.2
Example-SW-02	10.0.0.2

In advanced cases templates might need to take advantage of other template functions such as If, and else statements. If statements are also delineated by a percent sign on both sides of a string. There are a few difference between an if statement variable and a single variable. The following guide will demonstrate how to use variables to allow for flexibility within a configuration file.

Stacking Switches Offline

Before connecting the uplinks to the switches should be stacked, use the following procedure to stack switches before they connect to central.

CAUTION:

Do not connect the switch to the gateway before it is stacked otherwise it will not be able to stack offline without factory reset.

Before starting this procedure check the following:

Step 1 Ensure switches are AOS-CX 10.7 or Above

Step 2 All switches are factory default.

Step 3 Switches in the stack are using the reserved auto-stacking ports. - 24 port switches auto stack ports : 25, 26 - 48 port switches auto stack ports: 49, 50

Step 4 Switches are connected in a ring topology.

Step 5 Console connection to the switch.

After going through the checklist above the switches are ready to be stacked.

Step 1 Press the mode button until the LED displays **STK** on the switch that will be the conductor, wait for the conductor to reboot.

Step 2 On the second switch press the LED until it displays STK. Wait for the second member to boot.

NOTE:

During stacking operation, the port LEDs are displayed in three different states: Flashing green - Indicates that the member is the conductor. Flashing orange - Indicates that the member is rebooting to join the stack or offline due to error condition. Solid green - Indicates that the member joined the stack and is operational. For more information on stacking LED states, refer to the Monitoring Guide.

Configure the Access Base Features

Use this procedure to configure the access switch base features. The base features include the host name, management user account, banner MOTD, NTP, DNS, TACACS, and AAA.

In the configuration template, perform the following steps:

Step 1 Configure the switch host name.

hostname %HOSTNAME%

Step 2 Configure the management user account.

user admin group administrators password plaintext <password>

NOTE:

There must be an admin user account for CLI access to the switch.

Step 3 Configure the login banner. The banner MOTD is normally used as a legal disclaimer to notify users logging into the network that only authorized access is allowed. Consult your own legal team to define the banner MOTD. An example is shown below.

NOTE:

When setting the banner, a delineator breaks the switch from the MOTD context. In this example, the delineator is "\$".

Step 4 Configure the NTP servers and time zone.

```
ntp server 10.2.120.98 iburst version 3
ntp server 10.2.120.99 iburst version 3
clock timezone us/pacific
```

Step 5 Configure the DNS servers and domain name.

ip dns host 10.2.120.98
ip dns host 10.2.120.99
ip dns domain-name Example.local

Configure the Access VLANs

In order to provide client devices with network connectivity, access switches must have the same VLANs as the branch gateways. The access switches also have an additional layer 3 interface for the management VLAN. IGMP, DHCP snooping, and ARP inspection are enabled.

IGMP snooping prevents hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. The feature provides layer 2 switches with a mechanism to prune multicast traffic from ports that do not contain an active multicast listener.

DHCP snooping is enabled globally and enabled for each VLAN to snoop DHCP packets. DHCP snooping prevents DHCP starvation attacks and rogue DHCP servers from servicing requests on the network.

ARP inspection is enabled under the VLAN, but does not take effect unless DHCP snooping also is enabled. ARP inspection stops man-in-the-middle attacks caused by ARP cache poisoning.

In the configuration template, assign the following configuration:

VLAN ID	Description
100	MGMT VLAN
101	Employee
102	Camera
103	IOT
104	Guest
105	Reject
106	Critical
107	Quarantine

Step 1 Configure DHCP snooping globally.

dhcpv4-snooping

Step 2 Configure the access VLANs, enable DHCP/IGMP snooping, and enable ARP inspection.

```
vlan 100
name MGMT
dhcpv4-snooping
arp inspection
ip igmp snooping enable
vlan 101
name EMPLOYEE
dhcpv4-snooping
arp inspection
ip igmp snooping enable
...
vlan 107
name QUARANTINE
dhcpv4-snooping
arp inspection
ip igmp snooping enable
```

Step 3 Configure the layer 3 interface VLAN.

```
interface vlan 100
description MGMT
ip dhcp
```

NOTE:

The IP DHCP command can only be applied to one VLAN interface. The template will fail to apply if multiply Interface VLANs have this configuration.

Configure Device Profiles

Device profiles detect APs dynamically and configure the attached port properly for device management and for tagging the bridged SSIDs. This assists network operators by eliminating manual configuration of ports to which APs are connected.

Device profiles are applied in three steps. First, configure the role to identify the AP, as well as the port tagging. Second, define the LLDP group, which uses LLDP to glean the device OUI to identify if the device is an Aruba AP. Last, associate the role and LLDP group in a device profile configuration.

NOTE:

This procedure can be skipped if ClearPass is used to authenticate Aruba APs.

On each access switch, perform the following steps:

Step 1 Configure the Aruba-AP Role. Create the role, set the authentication mode, set the native VLAN, and define the allowed VLANs.

```
port-access role ARUBA-AP
auth-mode device-mode
vlan trunk native 100
vlan trunk allowed 100,101,104-107
```

Step 2 Configure the LLDP group. Create the group and identify the Aruba AP OUIs.

```
port-access lldp-group AP-LLDP-GROUP
seq 10 match vendor-oui 000b86
seq 20 match vendor-oui D8C7C8
seq 30 match vendor-oui 6CF37F
seq 40 match vendor-oui 186472
seq 50 match sys-desc ArubaOS
```

NOTE:

The LLDP group identifies the Aruba APs and sets the system-description at the end as a catchall for future APs.

Step 3 Configure the device profile. Create the profile, enable it, then associate it with the role and LLDP group created previously.

```
port-access device-profile ARUBA_AP
enable
associate role ARUBA-AP
associate lldp-group AP-LLDP-GROUP
```

Configure RADIUS

Use this procedure to configure the RADIUS servers for the access switch.

Access switches authenticate devices attempting to connect to the network. The two most common methods to authenticate users are 802.1x and MAC-based authentication. This design supports both methods, as well as dynamic authorization that allows the AAA server to change the authorization level of the device connected to the switch.

RADIUS tracking is enabled to verify the status of the client and server. The configuration also includes user roles for rejected clients and RADIUS failure scenarios.

On each access switch, perform the following steps:

Step 1 Configure the RADIUS servers, enable RADIUS dynamic authorization, and track client IP addresses with probes.

```
radius-server host 10.2.120.94 key plaintext <Password>
radius-server host 10.2.120.95 key plaintext <Password>
radius dyn-authorization enable
client track ip update-method probe
```

Step 2 Configure AAA for 802.1x and MAC authentication.

```
aaa authentication port-access dot1x authenticator
    enable
aaa authentication port-access mac-auth
    enable
```

Step 3 Configure local user roles, set the authentication mode, and set the VLAN.

```
port-access role EMPLOYEE
    reauth-period 120
    vlan access 101
port-access role CAMERA
    reauth-period 120
    vlan access 102
port-access role IOT
    reauth-period 120
    vlan access 103
port-access role GUEST
    reauth-period 120
    vlan access 104
port-access role REJECT
  reauth-period 120
 vlan access 105
port-access role CRITICAL
  reauth-period 120
 vlan access 106
port-access role QUARANTINE
    reauth-period 120
    vlan access 107
```

Step 4 Configure AAA authentication on the access ports. Set the client limit, configure 802.1x/MAC authentication, set the authentication order, and configure critical role and the rejection role. Adjust the EAPOL timeout, max requests, and max retry defaults.

```
interface 1/1/1
 description ACCESS_PORT
 no shutdown
 no routing
 vlan access 1
 aaa authentication port-access client-limit 5
 aaa authentication port-access auth-precedence dot1x mac-auth
 aaa authentication port-access critical-role CRITICAL_AUTH
 aaa authentication port-access reject-role REJECT_AUTH
 aaa authentication port-access dot1x authenticator
   eapol-timeout 30
   max-eapol-requests 1
   max-retries 1
   enable
 aaa authentication port-access mac-auth
  enable
```

NOTE:

EAPOL timeout: The amount of time the switch waits for EAP responses before identifying a packet as lost.**Max EAPOL requests**: The number of requests the interfaces can have at one time.**Max retries**: The number of times the switch tries to authenticate the device.

Configure Spanning Tree

Spanning tree is enabled globally on each access switch as a loop prevention mechanism. Supplemental features such as admin-edge, root guard, BPDU guard, and TCN guard are enabled on appropriate interfaces to ensure that spanning tree runs effectively.

On each access switch, perform the following steps:

Step 1 Configure spanning tree globally and enable Rapid Per VLAN Spanning Tree for the access VLANs.

```
spanning-tree mode rpvst
spanning-tree
spanning-tree priority 8
spanning-tree vlan 100-107 priority 15
spanning-tree vlan 100-107
```

Step 2 Configure the supplemental spanning tree features.

```
interface 1/1/1
  description ACCESS_PORT
  no shutdown
  no routing
  vlan access 1
  spanning-tree bpdu-guard
  spanning-tree port-type admin-edge
  spanning-tree root-guard
  spanning-tree tcn-guard
  loop-protect
  loop-protect action tx disable
```

Step 3 The final access port configuration should look like the following:

```
interface 1/1/1
 description ACCESS_PORT
 no shutdown
 no routing
 vlan access 1
 spanning-tree bpdu-guard
 spanning-tree port-type admin-edge
 spanning-tree root-guard
 spanning-tree tcn-guard
  loop-protect
 loop-protect action tx disable
 aaa authentication port-access client-limit 5
 aaa authentication port-access auth-precedence dot1x mac-auth
 aaa authentication port-access critical-role CRITICAL_AUTH
 aaa authentication port-access reject-role REJECT_AUTH
 aaa authentication port-access dot1x authenticator
   eapol-timeout 30
   max-eapol-requests 1
   max-retries 1
   enable
 aaa authentication port-access mac-auth
  enable
```

Step 4 Repeat the full interface configuration for each access port. The Collapsed Core switch will be stacked so ensure the stacked interface ports are used e.g 2/1/1.

Configure Access Uplink Ports

Each access switch can have an uplink connection to both BGWs or to an aggregation switch. Each uplink connected to the gateway will be a trunk with the allowed VLANs of 100-107. If the access switch is connected to an aggregation switch the switch will use a lag with the same allowed VLAN's. The native VLAN for the uplink will be VLAN 100. Each uplink has DHCP Snooping trust allowed and ARP inspection trust enabled. The section below will demonstrate how to use If statements in the template to dictate the configuration the switch will receive.

CAUTION:

If DHCP Snooping and ARP inspection trust are not enabled, clients **cannot** get an IP address and connect to the network.

For the access switch template perform the following steps:

Step 1 Configure the uplink interface, then set the native VLAN and the allowed VLANs on the trunk.

```
interface 1/1/24
  description Uplink_GW
  no shutdown
  no routing
  vlan trunk native 100
  vlan trunk allowed 100-107
```

Step 2 Configure ARP inspection trust and DHCP snooping trust.

interface 1/1/23
 description Uplink_GW
 no shutdown
 no routing
 vlan trunk native 100
 vlan trunk allowed 100-107
 arp inspection trust
 dhcpv4-snooping trust

CAUTION:

DHCP snooping and ARP inspection must be trusted on the trunk interface to allow clients to receive DHCP addresses from the centralized DHCP servers on the network.

Step 3 Configure if statement around uplink ports.

%if SITE_HAS_AGG=n% interface 1/1/23 description Uplink_to_BGW no shutdown no routing vlan trunk native 100 vlan trunk allowed 100-107 arp inspection trust dhcpv4-snooping trust interface 1/1/24 description Uplink_to_BGW no shutdown no routing vlan trunk native 100 vlan trunk allowed 100-107 arp inspection trust dhcpv4-snooping trust %endif%

Step 5 Configure the LAG.

interface lag 1
 no shutdown
 no routing
 vlan trunk native 100
 vlan trunk allowed 100-107
 lacp mode active
 lacp fallback-static
 arp inspection trust
 dhcpv4-snooping trust

Step 6 Configure the if statement around the LAG and uplinks

%if SITE_HAS_AGG=y% interface lag 1 no shutdown no routing vlan trunk native 100 vlan trunk allowed 100-107 lacp mode active lacp fallback-static arp inspection trust dhcpv4-snooping trust %endif% %if SITE_HAS_AGG=y% interface 1/1/23 no shutdown description Uplink_to_AGG lag 1 interface 1/1/24 no shutdown description Uplink_to_AGG lag 1 %endif%

Configure Collapsed Core Uplink Ports

On each access switch, perform the following steps:

Step 1 Configure the LAG's

interface lag 1 no shutdown no routing vlan trunk native 100 vlan trunk allowed 100-107 lacp mode active lacp fallback-static arp inspection trust dhcpv4-snooping trust interface lag 2 no shutdown no routing vlan trunk native 100 vlan trunk allowed 100-107 lacp mode active lacp fallback-static arp inspection trust dhcpv4-snooping trust interface lag 3 no shutdown no routing vlan trunk native 100 vlan trunk allowed 100-107 lacp mode active lacp fallback-static arp inspection trust dhcpv4-snooping trust interface lag 4 no shutdown no routing vlan trunk native 100 vlan trunk allowed 100-107 lacp mode active lacp fallback-static arp inspection trust dhcpv4-snooping trust

Step 2 Configure the uplink interfaces, then set the native VLAN and the allowed VLANs on the trunk.

interface 1/1/23 description Uplink_GW no shutdown no routing lag 1 interface 1/1/24 description Uplink_GW no shutdown no routing lag 1 interface 2/1/23 description Uplink_GW no shutdown no routing lag 2 interface 2/1/24 description Uplink_GW no shutdown no routing lag 2

Step 3 Configure downlinks to access switches

interface 1/1/1 description Uplink_GW no shutdown no routing lag 3 interface 1/1/2 description Uplink_GW no shutdown no routing lag 4 interface 2/1/1 description Uplink_GW no shutdown no routing lag 3 interface 2/1/2 description Uplink_GW no shutdown no routing lag 4

Applying the Template Configuration

After the template configuration is created, there should be two configuration files one for the access, and one collapsed core file. The only difference being the uplinks and the stacking ports configuration for the Collapsed core. This procedure walks through steps to get the configuration into Central.

Step 1 On the **Groups** page, in the **Manage Groups** section, drag the access switches from the right side to the template group on the left side.

Step 2 Go to Global > Groups. In the Groups list, select BR-ECSDB.

Step 3 On the Switches List page at the top right, click Config.



Figure 89: nav_to_sw_group_template_config

 Image: Switches
 Switches
 Second Second

Step 4 On the **Switches Template** section at the top right, click the **+** (plus sign) symbol.



Step 5 On the **Add Template** window in the **Basic Info** section, assign the following settings, then click **Next**.

- Template Name: BR-ACC
- Device Type: Aruba CX
- Model: 6200
- Part Name: All
- Version: All

ADD TEMPLATE			×
	SSICINFO Lect drvice type, model, part name and version	I	
	BASIC INFO		
	The template configuration should match the running configuration CLI order and format. TREATING THE TREATIN	 ✓ ✓ ✓ ✓ 	
CANCEL		BA	ICK NEXT

Figure 91: Low_Traffic_site_template_creation-1318605-1321132

Step 6 In the Edit Template section, paste the access configuration in the box, then click SAVE.

CAUTION:

All variables must be enclosed with percent "%" symbols.

×

ADD TEMPLATE

BASIC INFO Select device type, model, part name and version TEMPLATE Template Configuration	
MPLATE IMPORT CONFIGURATION AS TEMPLATE	Show Variables I
1 hostname %_sys_hostname%	
2 banner motd !	
3	
4 NOTICE TO USERS	
5 This is a private computer system and is the property of	
6 Aruba Networks. It is for authorized use only.	
7 users (authorized or unauthorized) have no explicit or	
8 implicit expectation of privacy while connected to this	
9 system.	
10 Any or all uses of this system and all files on this system	
11 may be intercepted, monitored, recorded, copied, audited,	
12 inspected, and disclosed to an authorized site, Aruba networks,	
13 and law enforcement personnel	
14 (foreign and domestic).	
15 By using this system, the user consents to such interception,	
INCEL	BACK



Step 7 Repeat steps 4-6 for the collapsed core with the following details - **Template Name:** *BR-AGG* - **Device Type:** *Aruba CX* - **Model:** 6300 - **Part Name:** *All* - **Version:** *All*

Upload the Access Switch Variables

Use this procedure to upload the variables for the access switches into Central.

Step 1 On the **Devices > Switches** page, select the **Variables** tab, then click **DOWNLOAD SAMPLE VARIABLES FILES**.

🚥 Switches				
Templates	Variables Configuration	Audit		
Select	the Upload/Download fi	le format and upl	load variables. Varia	ables '_sys_serial' and '_sys_lan_mac'
Upload	d/Download file format	◯ JSON	CSV	
UPL	OAD VARIABLES FILE	DOWNLOAD SAMP	LE VARIABLES FILE	
Vari	ables			
Devic	e MAC Address		Device S	erial Number

Figure 93: Download Variables

Step 2 Open the CSV file in an editor, enter the proper value for each variable, and enter **Y** in the modified column. **Save** the file on your computer.

Switch	Switch Mac	%HOSTNAME% Variable	%if SITE_HAS_AGG%	Modified
Jenat	Switch Mac	Input	variable	Moumeu
SG1AKW50LJ	44:5b:ed:37:62:c0	HOUBR-ECB-1CR1	n	γ
TW14KNK051	38:10:f0:25:6f:c0	MIABR-ECB1-CR1	n	Y
SG12KN5052	8c:85:c1:5d:c1:40	SFOBR-ECB1-CR1		Y
SG12KN505R	8c:85:c1:60:5f:00	SFOBR-ECB1-CR1		Y
SG0BKW506D	8c:85:c1:50:e0:00	SFOBR-CR1-AC1	У	Y
SG0BKW5070	8c:85:c1:50:93:c0	SFOBR-CR1-AC1	у	Y

CAUTION:

Change the **modified** column to **Y** for each device. For the Aggregation switch leave the variables that don't apply blank

Step 3 On the **Variables** tab, click **Upload Variables Files**, find the updated CSV file on your computer, then click **Open**.

 Switches					
Templates	Variables	Configuration	Audit		
Select	the Upload/	'Download fil	e format and up	oload variables. Var	iables '_sys_serial'
Uploa	d/Download	file format	⊖ json	CSV	
UPI	OAD VARIABL	ES FILE	DOWNLOAD SAMP	PLE VARIABLES FILE)



Stacking Collapsed Core Switches Offline

Before connecting the uplinks to the collapsed core, they should be stacked. Use the following procedure to stack switches before they connect to central. For the Houston and Miami sites the switches do not need to be stacked so they can be connected directly to the branch gateways.

CAUTION:

Do not connect the switch to the gateway before it is stacked otherwise it will not be able to stack offline without factory reset.

Before starting this procedure check the following:

- 1. Ensure switches are AOS-CX 10.7 or Above
- 2. All switches are factory default.
- 3. Switches in the stack are using the reserved auto-stacking ports.

- 4. Switches are connected in a ring topology.
- 5. Console connection to the switch.

After going through the checklist above the switches are ready to be stacked.

- 1. Press the mode button until the LED displays **STK** on the switch that will be the conductor, wait for the conductor to reboot.
- 2. On the second switch press the LED until it displays **STK**. Wait for the second member to boot.

NOTE:

During stacking operation, the port LEDs are displayed in three different states:Flashing green -Indicates that the member is the conductor. Flashing orange - Indicates that the member is rebooting to join the stack or offline due to error condition. Solid green - Indicates that the member joined the stack and is operational.For more information on stacking LED states, refer to the Monitoring Guide.

###

SWITCHES (5)

- 3. Connect the uplinks to the branch gateway.
- 4. Verify all switches are online and stacked. Go to **Devices > Switches > List** and verify that the switches are **In sync**.

SWITCHES	ONLINE	• OFFLINE
5	5	0

γ Device Name	Туре	Clients	Alerts	Config Status					
• SFOBR-ECB1-CR1	AOS-CX Stack	0	0	In sync					
• HOUBR-ECB1-CR1	AOS-CX	2	0	In sync					
• MIA-ECB1-CR1	AOS-CX	3	0	ln sync					
• SFOBR-CR1-AC1	AOS-CX	3	0	In sync					
• SFOBR-CR1-AC2	AOS-CX	2	0	In sync					

Figure 95: 2023-11-29_21-09-09

Aruba Branch Access Point (AP) Configuration

This section describes the creation and configuration of the AP group to support wireless service in the branches.

Open the AP Group

This procedure locates and opens the AP group

Step 1 In the Global dropdown, search or select the group you created in the previous section.

Step 2 In the left navigation pane, in the Manage section, select Devices.

Step 3 Select the AP tab, then click the gear icon in the upper right corner.



Step 4 Click Cancel, then click Exit.

Configure the WPA3-Enterprise Wireless LAN

Use this procedure to configure a WPA3-Enterprise SSID.

WPA3-Enterprise enables authentication using passwords or certificates to identify users and devices. The wireless client authenticates against a RADIUS server using an EAP-TLS exchange, and the AP acts as a relay. Both the client and the RADIUS server use certificates to verify their identities.

Step 1 From the **Access Point** page, select the **WLANs** tab. On the bottom left of the **Wireless SSIDs** table, click **(+) Add SSID**.

			System	IoT	Configuration Audit			
Wireless	s SSIDs							
NAME		SECURITY			ACCESS TYPE		TRAFFIC FORWARDING MODE	NETWORK ENABLED
						No data	to display	

Figure 96: Add SSID

Step 2 In the Create a New Network page on the General tab, expand Advance Settings.

Step 3 Configure SSID Name: EXAMPLE-CORP

Step 4 Click the + (plus sign) to expand **Broadcast/Multicast**.

- Change the **Broadcast filtering** to *All*.
- Enable DMO, and set the DMO Client Threshold to 40.

NOTE:

A **DMO Client Threshold** of 40 is the recommended initial value and should be adjusted based on actual performance.

Step 5 Click the + (plus sign) to expand Transmit Rates (Legacy Only).

- Set 2.4 GHz to Min: 5 and Max: 54.
- Set **5 GHz** to **Min:** *18* and **Max:** *54*.

Step 6 Click Next

CREATE A NEW NETWORK						
1 General ② VLANs ③ Security ④	Access 5 Summary					
Name (SSID):	EXAMPLE-CORP					
✓ Advanced Settings						
 Broadcast/Multicast 						
Broadcast filtering:	ALL					
DTIM Interval:	1 beacon					
Multicast Transmission Optimization:						
Dynamic Multicast Optimization (DMO):						
DMO channel utilization threshold:	90 %					
DMO client threshold:	40					
Transmit Rates (Legacy Only)						
2.4 GHz:	Min: 5 🔻 Max: 54 🔻					
5 GHz:	Min: 18 V Max: 54 V					
🕀 Beacon Rate						

Figure 97: General SSID Configuration

Configure SSID VLAN

On the VLANs tab, assign the following settings:

Step 1 Set the **Traffic Forwarding Mode** to *Tunnel*.

Step 2 Set the **Primary Gateway Cluster:** *UI-BGW-01-AUTO site cluster*. Leave the **Secondary Gateway Cluster:** *None (default)*.

Step 3 Set the Client VLAN Assignment: Static (default).

Step 4 Select the Employee VLAN (101).

Step 5 Click Next.
CREATE A NEW NETWORK	
1 General 2 VLANs 3 Security	Access Summary
Traffic forwarding mode:	Bridge Tunnel Mixed 없 네
Primary Gateway Cluster:	UI-BGW-01:auto site cluster
Secondary Gateway Cluster:	None
Client VLAN Assignment:	Static Dynamic
VLAN ID:	Employee(101)
> Show Named VLANs	

Figure 98: Configuring VLAN

NOTE:

When tunneling to the branch gateway, ensure the VLAN line protocol is up, by verifying that the VLAN is trunked or **forced operational state up** is configured on the branch gateway

Configure SSID Security Settings

WPA3 provides significant security improvements over WPA2 and should be used when possible. Consult relevant endpoint documentation to confirm support.

On the **Security** tab, assign the following settings:

Step 1 Security Level: Slide to Enterprise

Step 2 Key Management: WPA3 Enterprise CMM 128

CREATE A NEW NETWORK		
1 General 2 VL/	ANs 3 Security	4 Access 5 Summary
Security Level:	Enterprise Pers	rsonal Visitors Open
Key Management:		WPA3-Enterprise(CCM 128)
Primary Server:		- Select - This field is mandatory.
> Advanced Settings		

Figure 99: Enabling dot1x

Step 3 On the **Security** tab, click the **+** (plus sign) next to **Primary Server**.

Step 4 In the New Server window, assign the following settings, then click OK.

- Set Server Type to RADIUS.
- Name the server *cppm-01*
- Enter the RADIUS IP Address: 10.2.120.94
- Enter the **Shared Key:** *shared key*

NEW SERVER				×
Server Type:	RADIUS	Name:	cppm-01	
Radsec:		IP Address:	10.2.120.94	
Shared Key:		NAS IP Address:	optional	
Retype Key:		NAS Identifier:	optional	
Retry Count:	3	Auth Port:	1812	
Timeout (in secs):	5	Accounting Port:	1813	
Service Type Framed User: MAC/Captive Portal		CPPM Username:		
Password:		Retype:		
				Cancel

Figure 100: Adding Radius Server

NOTE:
It is important to record the Shared Key created above for use when configuring ClearPass
Policy Manager in the procedure below.

Step 6 Repeat the two previous steps for the second CPPM server using the appropriate values.

Step 7 Enable Load Balancing by selecting the toggle.

TE A NEW NETWORK				
General 2 VLANs	3 Securi	ty ④ Ad	ccess 5	Summary
Security Level:	0			
	Enterprise	Personal	Visitors	Open
Key Management:			WPA3-Enter	prise(CCM 128)
Primary Server:			cppm-01	🔻 + 🖍 i
Secondary Server:			cppm-02	• + 🖍 🖬
LOAD BALANCING:				



NOTE:

Best practice is to deploy 2 RADIUS servers and enable load balancing.

Step 8 On the Security tab, expand Advanced Settings and scroll down.

Step 9 Click the + (plus sign) to expand **Fast Roaming**.

Step 10 Ensure that Opportunistic Key Caching is enabled.



Step 11 Enable **802.11K**.

Configure Network Access Rules

Tunnel mode SSID restrictions are configured on the Gateway.

Step 1 On the Access tab, ensure that the Access Rules is set to Unrestricted.



Figure 102: Set Access

Step 2 On the Summary tab, review the settings and click Finish.

Configure the Visitor Wireless LAN

Use this procedure to configure a visitor SSID.

Arcess Points Radios Interfaces Security Services System IoT Configuration Audit Wireless SSIDs NAME SECURITY ACCESS TYPE TRAFFIC FORWARDING MODE NETWORK ENAB I EXAMPLE-CORP wpa3-aes-ccm-128 Unrestricted Tunnel Yes I Access Points Vireless SSIDs Vireless SSIDs Vireless SSIDs Vireless SSIDs Model SECURITY Vereless SSIDs Vireless SSIDs Vireless SSIDs Vireless SSIDs Vireless SSIDs Vereless SSIDs Vereless SSIDs Vereless SSIDs Vereless SSIDs Vereless SSIDs Vireless SSIDs Vereless SSIDs Vereless SSIDs Vereless SSIDs Vereless SSIDs Vereless SSIDs Vireless SSIDs Vereless SSIDs Vereless SSIDs Vereless SSIDs Vereless SSIDs Vereless SSIDs Vireless SSIDs Vereless SSIDs Vereless SSIDs Vereless SSIDs Vereless SSIDs Vireless SSIDs Vereless SSIDs Vereless SSIDs Vereless SSIDs Vereless SSIDs Vireless SSIDs Vereless SSIDs Vereless SSIDs Vereless SSIDs Vereless SSIDs <th></th> <th>1 0</th> <th>·</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>,</th> <th></th>		1 0	·							,	
Wireless SSIDs NAME SECURITY ACCESS TYPE TRAFFIC FORWARDING MODE NETWORK ENAB If EXAMPLE-CORP wpa3-aes-ccm-128 Unrestricted Tunnel Yes	VLANs	Access Points	Radios	Interfaces	Security	Services	System	IoT	Configuration Audit		
NAME SECURITY ACCESS TYPE TRAFFIC FORWARDING MODE NETWORK ENABLING I EXAMPLE-CORP wpa3-aes-ccm-128 Unrestricted Tunnel Yes I H Add SSID + Add SSID I H ADD SID I H ADD SID I H ADD SID I H ADD SID	Wi	ireless SSIDs									
■ EXAMPLE-CORP wpa3-aes-ccm-128 Unrestricted Tunnel Yes Ves Ves Ves Ves Ves Ves Ves		NAME			SECURITY	(ACCESS TYPE	TRAFFIC FORWARDING MODE	NETWORK ENABL
+ Add SSID	EXAMPLE-CORP			wpa3-aes	s-ccm-128			Unrestricted	Tunnel	Yes	
+ Add SSID											
+ Add SSID											
+ Add SSID											
+ Add SSID											
+ Add SSID											
+ Add SSID											
+ Add SSID											
	+	Add SSID									

Step 1 On the Access Points page, select the WLANs tab. On the bottom left of the Wireless SSIDs table,

click (+) Add SSID.

Step 2 Configure SSID Name: EXAMPLE-GUEST

Step 3 On the Create a New Network page of the General tab, expand Advance Settings.

Step 4 Click the + (plus sign) sign to expand **Broadcast/Multicast**.

- Change the **Broadcast filtering** to All.
- Enable DMO, and set the DMO Client Threshold to 40.

NOTE:

A **DMO Client Threshold** of 40 is the recommended initial value and should be adjusted based on actual performance results.

Step 5 Click the (+) sign to expand Transmit Rates (Legacy Only).

- Set 2.4 GHz to Min: 5, Max: 54.
- Set **5 GHz** to **Min:** *18*, **Max:** *54*.

CREATE A NEW NETWORK	
1 General ② VLANs ③ Security ④ Act	ccess (5) Summary
Name (SSID):	EXAMPLE-GUEST
✓ Advanced Settings	
Broadcast/Multicast	
Broadcast filtering:	ALL
DTIM Interval:	1 beacon
Multicast Transmission Optimization:	
Dynamic Multicast Optimization (DMO):	
DMO channel utilization threshold:	90 %
DMO client threshold:	40
Transmit Rates (Legacy Only)	
2.4 GHz:	Min: 5 V Max: 54 V
5 GHz:	Min: 18 V Max: 54 V

Figure 103: General SSID Configuration

Step 6 On the **General** tab, scroll down, and click the + (plus sign) to expand **Time Range Profiles**.

							٦.											
+	Ne	w Ti	me	Rang	ge Pr	ofile	e.											
	0	1	2	2		-	c	7		0	10	11	12	12	14	15	16	17
		+	-2	-	4			<u> </u>	Ŷ	9			12	15	14	15	10	Ť
MON	<u> </u>							_									_	-
TUE																		
WED																		
тни																		
FRI																		
SAT																		
SUN																		

Step 7 In the middle of the section, click (+) New Time Range Profile.

Step 8 In the New Profile window, assign the following settings, then click Save.

• Configure the **Name**: *Visitor Weekdays*.

- Ensure the **Type** is *Periodic*.
- Set **Repeat** to *Daily*.
- Set the Day Range: Monday Friday (Weekdays) (This can be changed to fit other environments).
- Set the Start Time Hours: 7, Minutes: 0.
- Set the End Time Hours: 18, Minutes: 0.

NEW PROFILE	
Name:	Guest Weekday
Туре:	Periodic
Repeat:	Daily Weekly
Day Range:	Monday - Sunday (All Days) Saturday-Sunday (Weekend)
Start Time:	Hours 7 V Minutes 0 V
End Time:	Hours 18 V Minutes 0 V
Note: The visualization is app	roximated to the hour.
0 1 2 3 4 5	6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
Cancel	

Figure 104: Configuring Time profile

Step 9 In the **Time Range Profiles** section in the Status dropdown, find the newly created profile, and select **Enabled**. At the bottom of the page, click **Next**.

Time D																							
Time Range Profile																	Sta	tus					
Guest	Guest Weekday (Periodic Weekday 07:00 - 18:00)																E	nable	ed		▼		
+ N	+ New Time Range Profile																						
Noto	The	/icual	lizativ	on is	s ann	rovir	nate	d to	the	bour													
0	1	2	3	4	5 5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
MON																							
TUE									<u> </u>			_			<u> </u>	<u> </u>							
TUE WED																							
TUE WED THU									<u> </u>		-		-	+		-	+	-					
TUE WED THU FRI																							
TUE WED THU FRI SAT																							

Figure 105: Enable Time profile

Configure VLANs

Step 1 On the **VLANs** tab, assign the following settings, then click **Next**. - Set the **Traffic Forwarding Mode** to *Tunnel*. -

Table of contents {: .text-delta } - TOC {:toc}

```
<script type="application/ld+json">
 {
    "@context": "http://schema.org",
    "@type": "Organization",
    "name": "Aruba Networks",
    "url": " https://arubanetworking.hpe.com/techdocs/VSG/",
    "description": "This section details how to use Aruba Central to ensure the
       topology is functional.",
    "keywords": {
        "WAN HA": "WAN Redundancy",
        "Clustering": "site clustering",
        "Branch gateway": "BGW"
    },
    "sameAs": [" https://en.wikipedia.org/wiki/Aruba_Networks",
        " https://www.facebook.com/arubanetworks/",
        " https://twitter.com/ArubaNetworks",
        " https://www.linkedin.com/company/aruba-a-hewlett-packard-enterprise-
           company",
        " https://www.youtube.com/c/arubanetworks/",
        " https://www.youtube.com/c/ABCNetworking",
        " https://community.arubanetworks.com/"
    ],
    "parentOrganization": {
        "@type": "Organization",
        "name": "Hewlett Packard Enterprise",
        "url": " https://www.hpe.com/us/en/home.html"
    },
    "owns": {
        "@type": "ProductGroup",
        "name": "Aruba Instant On",
        "url": " https://www.arubainstanton.com/",
        "logo": " https://www.arubainstanton.com/skin-solutionfuse-instant-on/img/
            aio-logo-drk-txt.svg",
        "description": "Let the network do the talking. Find access points and
            switches designed for small business. Get Wi-Fi up and running in
           minutes."
    },
    "address": {
        "@type": "PostalAddress",
        "addressLocality": "San Jose, CA",
        "postalCode": "95002",
        "streetAddress": "6280 America Center Dr"
    },
"faxNumber": "+1-408-752-0626",
    "telephone": "+1-408-941-4300",
    "logo": " https://arubanetworking.hpe.com/wp-content/themes/Aruba2015/images/
       aruba_hp_lockup_140x68-01.svg"
}
</script>
<script type="application/ld+json">
{
  "@context": " https://schema.org/",
  "@type": "WebSite",
   "url" : " http://arubanetworking.hpe.com/",
  "name": "Aruba Networks",
  "potentialAction": {
        "@type": "SearchAction",
        "target": " https://arubanetworking.hpe.com/gsa-search/#stq={
           search_term_string}",
        "query-input": "required name=search_term_string"
      }
}]
</script>
```

• VLAN ID: Guest(104).

CREATE A NEW NETWORK					
1 General 2 VLANs	(3) Security (4)	Access (5) Summary		
Traffic forwarding mode:		Bridge	• Tunnel	Mixed	ណ៍ – 🦾 🤖
Primary Gateway Cluster:		UI-BGW-01:auto	site cluster	▼	
Secondary Gateway Cluster:		None		▼	
Client VLAN Assignment:		• Static	Oynamic		
VLAN ID:		Guest(104) ×		▼	
> Show Named VLANs					

Figure 106: Set tunneling

NOTE:	
When tunneling to the branch gateway, ensure that the VLAN li	ne protocol is up by verifying the
VLAN is trunked or forced operational state up is configured	on the branch gateway

Configure Security

Step 1 On the **Security** tab, assign the following settings. - Set the **Security Level** to *Visitors*. - **Captive Portal Type:** *External*.

Security Level:			0
	Enterprise	Personal	Visitors Open
Access Network			
Туре:			External Captive Portal
Captive Portal Profile:			- Select - ▼ +
			This field is mandatory.
Primary Server:			- Select - V + This field is mandate
Encryption:			
Key Management:			Enhanced Open 🛛 🔻



Step 2 In the **Splash Page** section, click the + (plus sign) next to **Captive Portal Profile**.

Step 3 In the External Captive Portal-New window, assign the following settings, then click OK.

- Enter the Name: CPPM-Portal.
- Set the Authentication Type: RADIUS Authentication.
- Enter the Clearpass IP or Hostname: cppm.example.local.
- Enter the captive portal **URL:** /guest/example_guest.php.
- Verify the **Port** is 443.
- Set the **Redirect URL:** *http://arubanetworking.hpe.com*.

EXTERNAL CAPTIVE PORTAL-NEW	
Name:	CPPM-Portal
Authentication Type:	RADIUS Authentication 🛛 🔻
IP or Hostname:	cppm.example.local
URL:	/guest/example_guest.p
Port:	443
Use HTTPS:	
Captive Portal Failure:	Deny Internet
Server offload:	
Redirect URL:	https://www.arubanetw

Figure 108: Redirect configuration

Step 4 On the **Security** tab of the **Splash Page** section, click the dropdown next to **Primary Server**. Select the RADIUS server created in the WPA3 Enterprise section. Ensure THAT the **Secondary server** is se-

	Access Network	
	Туре:	External (
	Captive Portal Profile:	CPPM-Pc
	Primary Server:	cppm-01
	Secondary Server:	cppm-02
	LOAD BALANCING:	
	Encryption:	
	Key Management:	Enhanced
lected as well. Enable Load Balancing.		

Step 5 If the RADIUS server was not created in the WPA3 Section, follow the steps BELOW to configure the RADIUS Server.

Step 6 On the **Security** tab, click the **+** (plus sign) next to **Primary Server**.

Step 7 In the **New Server** window, assign the following settings, then click **OK**. - Set **Server Type** to *RADIUS*. - Name the server *cppm-01*. - Enter the RADIUS **IP address**: *10.2.120.94*. - Enter the **Shared Key**: *shared key*.

NEW SERVER				×
Server Type:	RADIUS	Vame:	cppm-01	
Radsec:		IP Address:	10.2.120.94	
Shared Key:		NAS IP Address:	optional	
Retype Key:		NAS Identifier:	optional	
Retry Count:	3	Auth Port:	1812	
Timeout (in secs):	5	Accounting Port:	1813	
Service Type Framed User: MAC/Captive Portal		CPPM Username:		
Password:		Retype:		
				Cancel

Figure 109: Adding Radius Server

NOTE:

It is important to record the **Shared Key** created above for use when configuring ClearPass Policy Manager in the procedure below.

Step 8 Repeat the two previous steps for the second CPPM server using the appropriate values.

Step 9 Enable **Load Balancing** by selecting the toggle, then click **Next**.

1 General 2 VLAN	ls 3 Securi	ty ④ A	ccess 5	Summary
Security Level:			0	
	Enterprise	Personal	Visitors	Open
cess Network				
Туре:			External Cap	tive Portal 🛛 🔻
Captive Portal Profile:			CPPM-Porta	• • + 🖍
Primary Server:			cppm-01	▼ + 🖍
Secondary Server:			cppm-02	• + 🖍 i
LOAD BALANCING:				

Figure 110: Enable Load balancing

NOTE:

The Captive Portal Profile requires information from the CPPM server on the network. For detailed steps, see *Appendix 1: How to Find ClearPass Details for the Visitor WLAN*.

Configure Access For Guest SSID

In most cases, the visitor needs access only to DHCP and DNS services, and HTTP/HTTPS access to all destinations on the Internet. To prevent access to internal resources, add an exception network and mask covering the internal IP addresses to the HTTP and HTTPS allow rules.

Step 1 On the Access tab, move the slider to Network Based.

Step 2 Select the Allow any to all destinations rule, then click the pencil icon.

Step 3 In the Access Rules window, change the action from Allow to Deny, then click OK.

Step 4 On the Access tab, select (+) Add Rule.

Step 5 In the Access Rules window, assign the settings in the table below, then click OK.

Step 6 Repeat step 4 and 5 for each row in the table.

CAUTION:

This step changes the default *allow any to all destinations* rule to a *deny any to all destinations* rule for visitor traffic. This line must always be the last entry in the Access Rules to prevent unauthorized access to internal network resources.

Example: Access rules for visitors

Rule Type	Service type	Service name	Action	Destination
Access control	Network	DHCP	Allow	10.2.120.98 (internal DHCP server)
Access control	Network	DHCP	Allow	10.2.120.99 (internal DHCP server)
Access control	Network	DNS	Allow	8.8.4.4 (well-known DNS server)
Access control	Network	DNS	Allow	8.8.8.8 (well-known DNS server)
Access control	Network	HTTP	Allow	To all destinations, except internal
Access control	Network	HTTPS	Allow	To all destinations, except internal
Access control	Network	Any	Deny	To all destinations

aruba Central	Q s	earch or ask Anuba	۵ 🧔 🔅 ۵
업 UI-AP-BR01 이	G Access Points		IL III Conte
Manage Manage B Overview Devices Clents A Clents A Clents A Security Analyze Alerts & Events A Alerts & Events A Addit Trail	Access Faints VILANS Access Faints CREATE A NEW NETWORK CREATE A NEW NETWORK CREATE A NEW NETWORK CREATE A NEW NETWORK Access rules Rock Rock Rock Rock Rock Rock Rock Rock	Configuration Audit Summary Summary Cole Based Network Based Universified Access BULES FOR SELECTED ROLES Cole Configurations Cole Based Configurations Cole Based Configurations Cole Based Configurations Cole Based Configurations Configuration Confi	Hide Advanced
Tools Reports Maintain Firmware			1 ftulets3

Figure 111: Configuring Access Control list

ccess rules		0	
	Role Based	Network Based	Unrestricted
ACCESS RULES FOR SELECTED ROLES			
Allow https except to network 10.0.0/255.0.0.0			
■ ● Allow https except to network 192.168.0.0/255.255.0.0			
■ Allow https except to network 172.16.0.0/255.240.0.0			
Allow http except to network 172.16.0.0/255.240.0.0			
Allow http except to network 192.168.0.0/255.255.0.0			
Allow http except to network 10.0.0.0/255.0.0.0			
Allow dos on server 8 8 4 4/255 255 255 255			

Step 7 Review the ACL, and select Next.

Step 8 On the **Summary** tab, review the settings, and click **Finish**.

CR	CREATE A NEW NETWORK					
	1 General 2 VLANs 3 Security 4 Access 3 Summary					
Ne	twork Summary					
	General			Security		
	ESSID	EXAMPLE-GUEST		Security Level	Captive Portal	
	Multicast Optimization	Disabled		Auth Server 1	cppm-01	
	Band	all		Auth Server 2	cppm-02	
	DTIM Interval	1 beacons		Captive Portal Profile	CPPM-Portal	
	Primary Usage	guest		Key Management	Enhanced Open	
	Inactivity Timeout	1000 secs		MAC Authentication	Disabled	
	Dynamic Multicast OPT	Enabled		VLANs		
	Content Filtering	Disabled		Traffic forwarding mode	Tunnel	
	Airtime	unlimited		Primary Gateway Cluster	UI-BGW-01:auto site cluster	
	Hide SSID	Disabled		Client VLAN Assignment	Static	
	Broadcast filtering	all		VLAN	Guest	
	Transmit Rates (legacy Only)	2.4 GHz	Min: 5Mbps	Access		
			max: э4морs	Role Assignments For Authenticated Users	Disabled	
		5 GHz	Min: 18Mbps Max: 54Mbps	ENFORCE MAC AUTH ONLY ROLE	Disabled	

Figure 112: Summary Configuration

I AM HERE!!!!

Configure the WLAN Access Points

After a branch is operational, the access points automatically create a virtual controller (VC) cluster and join the default group.

Assign the WLAN AP Group

Step 1 In the dropdown, verify that All Devices is selected.

Step 2 In the left navigation pane, in the Manage section, select Devices.

Step 3 On the **Access Points** tab, in the **Access Points** section, identify the MAC addresses of the AP and assign the AP to the **UI-AP-BR01** group.

Step 4 In the left navigation pane, in the Maintain section, select Organization.

Step 5 Drag the virtual controller into the configured AP group. All access points in the site are automatically moved to the AP group.



Figure 113: moving AP's

Assign WLAN Access Points to Site

The following procedure assigns access points to a site. Creating sites was shown in the "preparing to Deploy" section of the guide.

Step 1 Go to Organization and select Site

Step 2 Select Unassigned devices and assign the APs to the correct site. Click Yes

aruba Central	Q S	earch or ask Aruba	۹ ¢ @ # Å
	Network Structure		
Manage BR Overview @ Devices It Clients 	Croups Containe devices with common configuration into a single group to apply the same configuration Groups 0: unprovisioned devices	Sites Sites allow you to group devices based on their focution 188 Sites 9 unassociated devices	Labels Labels are logical sets of devices which can be used for a variety of monitoring and reporting purposes Labels 88 unassociated devices
Security K Network Services Analyze Alerts & Events Addit Trail	Install Manager Manage devices installation on site by installers who are using mobile app Aruba installations (Minager 1 Site installations in progress 1 Site installations 1 Quemphical 1 Authorized installers	Certificates Uplicat certificates for validating theiros or user identity during authentication 2 Certificates	
Tools Reports Maintain Firmware Organization			

Figure 114: Assigning AP's to site

Rename the Access Points

Step 1 Go to the UI-AP-BR01 group.

Step 2 Select Configuration.

Step 3 Select the AP, then click the **pencil** icon.

Step 4 Enter the new AP name. In this example, it is *RS01-AP01*. Click **Save Settings**.

aruba Central		Q Search or ask Aruba		Q	4 🛛 🏭 🖞
🕽 UI-AP-BR01 📀	Contract Con				
- Manage BB Overview	Access Points • Online • Offline Radios 2 2 0 4				
Devices	Access Points (2)				
Eb Clients					
🔉 - Guests					
# Applications					
Security					
- Analyze					
Ω Alerts & Events					
🖬 Audit Trail					
😃 Tools					
Et Penerte					
Maintain					
Firmware					



SD-Branch Security

Aruba Edgeconnect SD-Branch includes security capabilities that enable admins to centralize network policy and propagate policy across the SD-Branch Fabric .

The following sections of this guide builds on the branches configured in the configured in the following section: This section of the guide will demonstrate how to configure, UBT and Centralized Multi-Site Fabric, and how to create policies.

The topology configured in the previous section is illustrated below with the to-be configuration of the logical topology.



High Traffic Site

Low Traffic Site



Figure 116: Logical_site_topology

Enabling Centralized Multi-Site Fabric

OWL Corp. plans to implement role-based policy to simplify network policy across the SD-WAN Fabric. They have requested enabling User Based Tunneling (UBT) at each branch site, with policy extended between branches.

The following procedures will demonstrate how to change the Switch and Gateway configurations, in order to enable role-based policy with UBT and Multi-Site Fabric. UBT centralizes policy at the Branch gateway. Multi-Site Fabric enables carrying the user role policy across the WAN, with enforcement at the destination branch gateway or VPNC.

Centralized Multi-Site Fabric Requirements

- Jumbo frames enabled on all Gateway VLANs
- Removal of user VLAN's from switches and access points.
- Large MTU configured on switch VLANs (9198 MTU)
- Change switch user roles to use gateway roles instead of VLANs
- UBT-Client-VLAN: this guide uses VLAN 2000 .

NOTE:

AP configuration do not require adjustment, since APs are already set to tunnel. No additional roles are needed for access points. The gateways will proxy the RADIUS request and apply roles based on the role returned from Clearpass. The gateway role will contain the policy configured below.



Figure 117: image-20240131091215658

Policy Requirements

All devices are assigned a user role. The level of access is determined by the user role. The following policies are configured.

Role	Allowed Access
EMPLOYEE	Printers, Internal Applications, DNS, DHCP, AD, Internet
IT-ADMIN	All Network Nodes , Internet
IT-SUPP	Employees, Printers, IOT-INTERNAL, IOT-LMT-INET, IOT-NO-INET, REJECT, Internet

Role	Allowed Access
VISITOR	Internet, Captive Portal, DHCP
PRINTER	Internal Applications (Employee, IT-Admins and IT-SUPP all should be able to initiate connections to printers, but the printer should not be able to initiate connections.)
IOT-NO-INET	IOT-NO-INET
IOT-INTERNAL	Internal Applications (padlock systems, asset tracking.)
IOT-LMT-INET	SaaS (Water systems, Air Quality Monitor, Smart thermostats .)
REJECT	Internet (All devices with reject role are profiled by ClearPass.)
QUARANTINE	Internal Applications.
CRITICAL	Internet, AD, DNS.
SECURITY	Internal Applications (Security Camera DVR, RFID Database)

NOTE:

The policy examples below do not represent all established OWL policies. The instructions provide information for only policies affected by this section's requirements

Enabling Multi-Site Fabric

This section illustrates how to enable Multi-Site Fabric, enabled between specific groups. The section also detail the centralized configuration of user roles using the Global Policy Manager.

It is imperative to configure user roles within the Global Policy Manager, where the mapping of policy ID to user roles takes place. The assigned policy ID is carried between branches, allowing the propagation of policy. The Policy ID received by destination branches is also used for reverse lookups of roles configured in Global Policy Manager, ensuring the enforcement of role-to-role policies.

NOTE:

For admins who do not intend to enable Multi-Site Fabric, user roles and policies can be configured at the group level.

Configure Global Client Roles

Step 1 On the Global page, in the left menu, click Security.

Step 2 Click the Client Roles tab at the top of the page.





NOTE:

All user roles configured before Aruba Central 2.5.6 were automatically configured in Global Policy Manager. Delete roles that are not needed and skip adding the roles.

Step 3 Click the + (plus sign) in the Roles table.



Step 4 Enter the following User Role name: EMPLOYEE. Click Save.

Step 5 Repeat Steps 3 to 4 for the list of user roles below.

• IT-ADMIN

- IT-SUPP
- VISITOR
- PRINTER
- IOT-NO-INET
- IOT-INTERNAL
- IOT-LMT-INET
- REJECT
- QUARANTINE
- CRITICAL
- SECURITY

Step 6 Hover over the EMPLOYEE role that was created and click the edit (pencil) icon.

Step 7 In the Permissions table, click the edit (pencil) icon.

- Click the **PRINTER** box in **Allow Source to Destination**.
- Click Assign.
- Click Save.

Central		O Search or ask Aruba		Q New	Central
Customer: Orange TME	•	¢ Ø •	D		Ð
율 Global 🛛	RAPIDS Authenticat	ion & Policy Gateway IDS/IPS Firewall 0	lient Roles		3 nours
- Manage	Role-to-Role Policy Enforc	ement 🕖 🛈 Permission defined for roles do not appl	y.		
B Overview	ROLES (12)				+
I Devisor	y Name	Description	Policy Identifier	Permissions	
C Devices	CRITICAL		1100	0 permitted	
Clients	EMPLOYEE		100	0 permitted	
🖧 Guests	IOT-INTERNAL		700	0 permitted	
An aliantiana	IOT-LMT-INET		800	0 permitted	
Applications	IOT-NO-INET		600	0 permitted	
😌 Security	IT-ADMIN		200	0 permitted	
& Network Services	IT-SUPP		300	0 permitted	
Analan	PRINTER		500	0 permitted	
Analyze	QUARANTINE		1000	0 permitted	
Alerts & Events	REJECT		900	0 permitted	
🖬 Audit Trail	SECURITY		1200	0 permitted	
🖏 Tools	VISITOR		400	0 permitted	
🛋 Reports					
- Launch					
App Catalog	Use a switch fabric for rol	le propagation? 💿 Yes 🔵 No		h	
- Maintain					
Firmware					
រ៉ៃ Organization					

Figure 119: Assigning role to role permissions

Step 8 Repeat step 7 for the role-to-role permissions below. Application-level permissions are configured in the "Updating Gateway Configuration" section.

Role	Allowed Access
EMPLOYEE	Printers

Role	Allowed Access
IT-ADMIN	All Network Nodes
IT-SUPP	Employees, IT-ADMIN, Printers, IOT-INTERNAL, IOT-LMT-INET, IOT-NO-INET, REJECT
PRINTER	Employee, IT-Admins and IT-SUPP should all be able to initiate connections to printers but the printer should not be able initiate connections.
IOT-NO-INET	IOT-NO-INET

NOTE:

Configuring one role automatically configures other roles that are allowed to the destination.

Enable Role to Role Policy across branches

Step 9 At the bottom of the page, select *No* in Use a switch fabric for role propagation? Select No.

Step 10 Click **Branch** and click the + (plus sign.

- Select the **BR-ECSDB** group.
- Select the **VPNC-RSVDC** group.
- Click Assign.
- Click Save.

Central	Q :	Search or ask Aruba		Q New	Central 🌒 🗘 🗿 😤
Customer: Orange TME	•	Ø			Ð
요 Global	RAPIDS Authentication &	Policy Gateway IDS/IPS Firewall Client	Roles		3 nours
- Manage	Role-to-Role Policy Enforcemen	t Permission defined for roles do not apply.			
B Overview	ROLES (12)				+
	Y Name	Description	Policy Identifier	Permissions	
	CRITICAL		1100	1 permitted	
Lū Clients	EMPLOYEE		100	3 permitted	
🖧 Guests	IOT-INTERNAL		700	2 permitted	
Applications	IOT-LMT-INET		800	2 permitted	
- · · · · · ·	IOT-NO-INET		600	2 permitted	
😌 Security	IT-ADMIN		200	12 permitted	
🗞 Network Services	IT-SUPP		300	8 permitted	
- Analyze	PRINTER		500	3 permitted	
↑ Alerts & Events	QUARANTINE		1000	1 permitted	
A Alero de Veno	REJECT		900	2 permitted	
Audit Trail	SECURITY		1200	1 permitted	
🖏 Tools	VISITOR		400	1 permitted	
🛍 Reports					
- Launch					
App Catalog	Use a switch fabric for role prop	pagation? 💿 Yes 🔵 No			
- Maintain					
Firmware					
h Organization			•		
G Organization					

Figure 120: Selecting role-to-role groups-1972299

CAUTION:

Two groups must be selected or roles and policy cannot be pushed to the group. SD-Branch role propagation and role propagation across a switch fabric are mutually exclusive.

Step 12 At the top of the page, click the Role-to-Role Policy Enforcement slider.

Central	٩	Search or ask Aruba		Q	New Central 🌒 🗘 🗿 💈
Customer: Orange TME	©	Ø			<u>.</u>
ଢ Global ◯	RAPIDS Authentication & P	olicy Gateway IDS/IPS Firewall Cli	ent Roles		Jin
- Manage	Role-to-Role Policy Enforcement	•• •12			
🗄 Overview	ROLES (12)				+
	→ Name	Description	Policy Identifier	Permissions	
l Devices	CRITICAL		1100	1 permitted	
🗖 Clients	EMPLOYEE		100	3 permitted	
9 Guests	IOT-INTERNAL		700	2 permitted	
a. Ouests	IOT-LMT-INET		800	2 permitted	
Applications	IOT-NO-INET		600	3 permitted	
😌 Security	IT-ADMIN		200	13 permitted	
	IT-SUPP		300	8 permitted	

Figure 121: Enable Role-to-Role Policy-1970841

Step 13 Scroll down the page and click Save.



Figure 122: Save Settings

SD-Branch User Based Tunneling

This section demonstrates changes needed for the switch and gateway to allow UBT at a branch site. APs are already set to tunnel and do not require adjustment. No additional roles are needed for access points.

Update Switch Template Configuration

The switch template must be updated first.

Four configuration changes for the switch are required: adjusting MTU size, removing unused VLAN's, enabling UBT and adjusting user roles.

Adjusting the MTU size on the switch disrupts service and causes the switches to lose connection to the gateways. The connection is restored after gateway configuration when the MTUs match.

Step 1 In the BR-ECSDB group, click the Switch tab.

Orubo Central	Q Se	arch or ask Aruba				٩	New Central	📮 🕐 🚨
Customer: Orange TME	6	æ					th	
¤ ■ BR-ECSDB	Access Points Switches	Gateways					Juninity	Comg
	Gateways • Online	• Offline	Clusters					
- Manage	8 8	0	4					
BB Overview	Gateways (8)							.↓
Devices	Pevice Name	▼ Model	Y IP Address	MAC Address	▼ Serial	Firmware Version	Uptime	Group
Clients	HOURR-ECR1-2	A9004	10.14.8.3	20:4c:03:b7:ae:4a	CNLCKLB04X	10.5.0.1 88128	4 days 1 hour 24 minutes	BR-ECSDB
9 Cuesta	HOUBR-ECB1-1	A9004	10.14.8.2	20:4c:03:b7:ad:72	CNLCKLB04T	10.5.0.1 88128	6 days 2 hours 53 minutes	BR-ECS (1)
a duests	SFOBR-ECB1-1	A9004	10.14.24.2	20:4c:03:b7:ae:7a	CNLCKLB055	10.5.0.1_88128	4 days 1 hour 25 minutes	BR-ECSDB
Applications	SFOBR-ECB1-2	A9004	10.14.24.3	20:4c:03:b7:ac:f2	CNLCKLB03Y	10.5.0.1_88128	4 days 1 hour 22 minutes	BR-ECSDB
Security	MIABR-ECB1-2	A9004	10.14.0.3	20:4c:03:b5:98:52	TWJTKLB05L	10.5.0.1_88128	5 hours 54 minutes	BR-ECSDB
Analyze	SANBR-ECB1-1	A9004	10.14.16.2	20:4c:03:b7:ad:82	CNLCKLB04V	10.5.0.1_88128	4 days 1 hour 26 minutes	BR-ECSDB
Alerts & Events	SANBR-ECB1-2	A9004	10.14.16.3	20:4c:03:b7:ac:d2	CNLCKLB04K	10.5.0.1_88128	4 hours 11 minutes	BR-ECSDB
A AICIO & EVENO	MIABR-ECB1-1	A9004	10.14.0.2	20:4c:03:b5:91:12	TWJSKLB0Q9	10.5.0.1_88128	4 hours 16 minutes	BR-ECSDB
Audit Trail								
🖏 Tools								
刷 Reports								
Maintain								
- Maintain								
Firmware								
🔓 Organization								
							h	

Step 2 In the Switches List page at the top right, click Config.



Step 3 In the **Switches Template** section, hover over the **BR-ACC** template and click the **edit** (pencil) icon.

Orubo Central		Q 5	earch or ask Aruba			Q	New Central 🌒 🛛 🔅	0 2
Customer: Orange TME	G Access Points	Switches	@ Gateways				li ∷≣ Summary List	Conf
ជ 🖙 BR-ECSDB 🛛	Templates Var	iables Configur	ation Audit					
- Manage								
B Overview	Template	es (2)					Q +	• •
Devices	Template Na	ame		Device Type	Model	Version	Last Modified	
	BR-ACC			cx	6200	ALL	Fri, 12 Jan 2024 01:24:59 GMT 3	Ō
Clients	BR-AGG			cx	6300	ALL	Wed, 17 Jan 2024 01:34:32 GMT	
😤 Guests								
Applications								
Security								
- Analyze								
Ω Alerts & Events								-
🖬 Audit Trail								



Configuring UBT Client VLAN

The original template configuration is shown below. The following VLANs will be adjusted.

Step 1 Adjust the VLAN's configuration.

vlan 101 name EMPLOYEE dhcpv4-snooping arp inspection ip igmp snooping enable vlan 102 name CAMERA dhcpv4-snooping arp inspection ip igmp snooping enable vlan 103 name IOT dhcpv4-snooping arp inspection ip igmp snooping enable vlan 104 name VISITOR dhcpv4-snooping arp inspection ip igmp snooping enable vlan 105 name REJECT dhcpv4-snooping arp inspection ip igmp snooping enable vlan 106 name CRITICAL dhcpv4-snooping arp inspection ip igmp snooping enable vlan 107 name QUARENATINE dhcpv4-snooping arp inspection ip igmp snooping enable

Step 2 Reconfigure the VLANs as:

```
vlan 100
   name MGMT
vlan 101
   name EMPLOYEE
vlan 102
   name CAMERA
vlan 103
   name IOT
vlan 104
   name VISITOR
vlan 105
   name REJECT
vlan 106
   name CRITICAL
vlan 107
   name QUARENATINE
vlan 2000
 name UBT_CLIENT
 dhcpv4-snooping
 arp inspection
 ip igmp snooping enable
```

Step 4 Ensure VLANs are on the uplinks and the MTU is set.

interface 1/1/23 description Uplink_GW no shutdown no routing mtu 9198 vlan trunk native 100 vlan trunk allowed 100-107 arp inspection trust dhcpv4-snooping trust interface 1/1/24 description Uplink_GW no shutdown no routing mtu 9198 vlan trunk native 100 vlan trunk allowed 100-107 arp inspection trust dhcpv4-snooping trust

Step 3 Adjust the MTU on VLAN 100, so users can access the network.

```
interface vlan 100
description MGMT
ip mtu 9198
ip dhcp
```

Configure UBT

For switch-to-tunnel traffic to the gateways, the UBT VLAN must point to the gateway's IP address, which is a new variable in the template.

Step 1 Define the UBT client VLAN and create the UBT zone in the default VRF.

- UBT Client VLAN: 2000
- UBT Zone: branch

```
ubt zone branch vrf default
primary-controller ip %gateway_1_sys_ip%
backup-controller ip %gateway_2_sys_ip%
enable
ubt-client-vlan 2000
```

Adjust User Roles

The roles must be adjusted to point to the gateway roles. The names must match the names on the gateway. The gateway map the VLAN to the roles and enforces role-to-role policy. The original configuration in the template below shows the user roles to be adjusted.

```
port-access role ARUBA-AP
 auth-mode device-mode
 vlan trunk native 100
 vlan trunk allowed 100,101,104-107
port-access role REJECT
   reauth-period 120
    vlan access 105
port-access role EMPLOYEE
    reauth-period 120
    vlan access 101
port-access role PRINTER
    reauth-period 120
   vlan access 102
port-access role IOT
    reauth-period 120
    vlan access 103
port-access role GUEST
    reauth-period 120
   vlan access 104
port-access role REJECT
    reauth-period 120
    vlan access 105
port-access role CRITICAL
 reauth-period 120
  vlan access 106
port-access role QUARANTINE
    reauth-period 120
    vlan access 107
```

Step 1 Remove the **VLAN access** line from the roles displayed above and replace them with the following **VLAN access** line: - *gateway-zone zone branch gateway-role* and the respective role name.

```
port-access role EMPLOYEE
    reauth-period 120
    gateway-zone zone branch gateway-role EMPLOYEE
port-access role SECURITY
   reauth-period 120
    gateway-zone zone branch gateway-role SECURITY
port-access role IOT-NO-INET
   reauth-period 120
    gateway-zone zone branch gateway-role IOT-NO-INET
port-access role IOT-INETERNAL
    reauth-period 120
    gateway-zone zone branch gateway-role IOT-INETERNAL
port-access role IOT-LMT-INET
    reauth-period 120
    gateway-zone zone branch gateway-role IOT-LMT-INET
port-access role VISITOR
    reauth-period 120
    gateway-zone zone branch gateway-role VISITOR
port-access role INFRA-DEVICE
   reauth-period 120
  gateway-zone zone branch gateway-role INFRA-DEVICE
port-access role PRINTER
   reauth-period 120
  gateway-zone zone branch gateway-role PRINTER
port-access role IT-ADMIN
  reauth-period 120
   gateway-zone zone branch gateway-role IT-ADMIN
port-access role IT-SUPP
   reauth-period 120
   gateway-zone zone branch gateway-role IT-SUPP
port-access role REJECT
    reauth-period 120
    gateway-zone zone branch gateway-role REJECT
port-access role CRITICAL
    reauth-period 120
    vlan access 106
port-access role QUARANTINE
   reauth-period 120
   gateway-zone zone branch gateway-role QUARANTINE
```

Step 2 Remove the old VLAN's from the AP role.

```
port-access role ARUBA-AP
auth-mode device-mode
vlan trunk native 100
vlan trunk allowed 100
```

Update Gateway Configuration

The gateways require three changes to enable user based tunneling: MTU size must be increased, and both VLAN-to-role mapping and network policy must be configured in the group. This section demonstrates the process.

Adjusting VLAN MTU

Step 1 Select the Gateways tab, then click the gear icon in the upper right corner.

Customer: Orange TME	Access Points Switches Gateways	SELECTED GROUP TYPE II. 1 Seman Selected Group Type II. 1 Core					
ଘ BR-ECSDB 이	System LAN WAN Tunnels & Routing Poli	Advanced Mode Guided Setup					
Manage	Platform Time DNS Management User						
BB Overview							
Devices	Each group will contain gateways of the same model (for example, 7003). Select the model of the gateways you plan on assigning to this group. Show more						

Figure 125: bgw-select-config-2

Step 2 Select LAN. Click Lan Ports

Step 3 Hover over the GE0/0/2 interface, then select the pencil icon.

Step 5 Check the Jumbo Frames box.

Step 6 Select Save.

Step 7 Repeat steps 3-6 for the GE0/0/3 interface.

Step 8 Click Save Settings





Associate VLANs to User Roles

Roles are established within the group from global policy manager . However, these roles lack VLAN association. Consequently, during authentications, clients are assigned a role with VLAN 1 by default instead of being placed in the appropriate VLAN. The following procedure demonstrates how to associate VLANs to roles.

Step 1 Ensure the Gateway configuration is in Advanced Mode. Select the Security tab.

Step 2 Select the Roles tab.

	Q Search or ask Aruba		Q	New Central	¢ 0 2
Customer: Orange TME	\$ = \$			SELECTED GROUP TYPE	
ଘ 💷 BR-ECSDB 📀	Access Points Switches Gateways System WAN Security VPN Routing His	th Availability Config Audit		branch Gateway Sammary	Racis Mode
- Manage	Polar Polician Alistan Applications Apply Pol	line Auth Songer Pole Arrigoment (AAA Profiler)	12 Authentication 12 Authentication Advanced	Eizewall	basic wode
B Overview		icy Additiservers Role Assignment (AAA Fromes)	22 Autorentication D Autorentication Advanced	110400	
Oevices	Roles				
🗖 Clients	∀ NÂME	RULES	GLOBAL		=
🛎 Guests	ap-role	35 Rules	No		
Applications	authenticated	4 Rules	No		
Security	CRITICAL	0 Rules	Yes		
Analyze	default-iap-user-role	2 Rules	No		
	default-via-role	3 Rules	No		
🗷 Audit Trail	default-vpn-role	4 Rules	No		
🖏 Tools	+				
Reports					
Maintain					
Ø Firmware					
😫 Organization					



Step 3 Select the Critical role.

Step 4 Scroll down and select the More tab. In the more tab, set the VLAN ID and the max sessions.

- VLAN: 106
- Max Sessions: 10000

Step 5 Click Save Settings.

aruba Central		O Search or ask Aruba					۹		New Centr	al 🌒	¢ 🛛 2
Customer: Orange TME	Access Points Switches	Gateways							SELECTED GROUP TYPE Branch Gateway	il. Summary	List Config
🛱 📼 BR-ECSDB 📀	System WAN Interface Se	curity VPN Routing High	Availability Config Au	dit							Basic Mode
- Manage	Roles Policies Aliases	Applications Apply Police	Auth Servers	Role Assignment (AAA Profiles)	L2 Authentication	L3 Authentication	Advanced	Firewall			
88 Overview											
Devices	Roles										
🗈 Clients	∑ NÂME		RULES		GLOBAL						=
🚉 Guests	ap-role		35 Rules		No						
Applications	authenticated		4 Rules		No						
Security	CRITICAL		0 Rules		Yes						
- Analyze	default-iap-user-role		2 Rules		No						
Alerts & Events	default-via-role		3 Rules		No						
🗷 Audit Trail	default-vpn-role		4 Rules		No						
🖏 Tools	+										
Reports											
- Maintain											
Firmware				•							
😫 Organization											



NOTE:

The VLAN List displays VLAN IDs. Named VLANs also can be used to associate the VLAN to the user role. In the example above, the VLAN ID is used.

Step 6 Repeat steps 3 to 5 for all roles.

User Role	VLAN ID
EMPLOYEE	101
PRINTER	102
IOT-INTERNAL	103
IOT-LMT-INET	103
IOT-NO-INET	103
GUEST	104
REJECT	105
CRITICAL	106
QUARANTINE	107

Configuring Network Policy with User Roles

Global policy manager can configure only role-to-role policies. For more granular policies, such as applications or network protocols, the configuration be made in the group. This section walks through the process of configuring URL and IP-based policies specifically for the *Visitor* user role.

Role	Allowed Access	Denied Access
VISITOR	Internet, Captive Portal (cppm.example.local), DHCP/DNS(10.2.120.99/98)	RFC1918

Step 1 On the Gateway tab on the top right side, select Basic Mode.

aruba Central	Q. Search or ask Aruba	٩	New Central 🌒 🧔 🔮
Customer: Orange TME	Ø •		SELECTED GROUP TYPE II. III S
រះ្ឋ 💷 BR-ECSDB 💦	Access Points Switches Gateways System WAN Interface Security VPN Routine Hirb Availability Confir Audit		Basic Mode
- Manage	General Admin Certificates SNMP Logging Switching External Monitoring		
89 Overview			

Figure 129: select basic mode

Step 2 Select the Policies tab. Click Applications.



Figure 130: Navigation_to_polices

Step 3 Click the + (plus sign) beside Network Aliases. In the Name field, enter ad server.

Step 4 Click the **+** (plus sign) in the **User Rules** table.

Step 5 In the new row's **Type Column**, click **Name**. Scroll to select **Host**. In the **IP Address** field, enter *10.2.120.98*.

Step 6 Repeat step 4. Click Name. Scroll to select the Host. In the IP Address field, enter 10.2.120.99.

Step 7 Click Save.

Customer: Orange TME Customer: Orange TME Customer: Orange TME	Access Points Swite System LAN WAN Tr Roles Applications Gateways are effectively	thes Gateways unnels & Routing Policies DPS PBR QoS Secu			
Image Image - Manage Image BB Overview Image Image Devices Image Image Devices Image	Access Points Switc	unnels & Routing Policies DPS PBR QoS Secu			
Manage Overview Devices Clients	Roles Applications	DPS PBR QoS Secu	· _		
Overview Devices Clients	Roles Applications	DPS PBR QoS Secu			
Devices	Gateways are effectively		irity		
Clients		stateful firewalls with appl	lication inspection capabilities. As s	uch, custom application	s, network aliases
Eu cilenci	Per-field help				
a Gueste					
a queso	Network Aliases				+
Applications	NAME	ITEMS	DESCRIPTION	INVERT	
Security	any	1		false	
- Analyze	auth-facebook	3		false	
	controller	1		false	
🗹 Audit Trail	localip	1		false	
Tools	mswitch	1		false	
D Reports	private-networks	3	System defined netdestinat	false	
Maintain	Service Aliases				+
A Firmware	NAME	PROTOCOL	PORT	ALG	
g riffiware	any				
ង្ខ Organization	any-v6	255			
	svc-adp	udp	8200		
	svc-cfgm-tcp	tcp	8211		
	svc-citrix	tcp	2598		
	svc-dhcp	udp	67-68		

Figure 131: ad_network_alias

Step 7 Click the + (plus sign) beside Network Aliases. In the Name field, enter rfc1918.

Step 8 Click the + (plus sign) in the **User Rules** table.

Step 9 In the new row's **Type Column**, click **Name**. Scroll to select **Network**. Enter the first range, then repeat step 8 for the remaining ranges.

- IP/Mask: 192.168.0.0/255.255.0.0
- IP/Mask: 172.16.0.0/255.240.0.0
- IP/Mask: 10.0.0.0/255.0.0.0

Step 10 Click Save.

Cutomer Orang TME Cutomer Orang TME Cutomer Orang TME Control Cont	Constraints Switch Access Points Switch System LAN WAN Tu Roles Applications C Gateways are effectively Per-field help Network Allases NAME ad servers	Cateways Gateways PS PBR QoS Secu- stateful firewalls with app ITEMS	lication inspection capabilities	. As such, custom application	is, network aliases a
till mBR-ECSDB Manage BB Overview SB Devices Ca Clients SB Applications SG Security Analyze	Access Points Switch System LAN WAN Tu Roles Applications C Gateways are effectively Per-field help Network Aliases NAME ad servers	Annels & Routing Policies PBR QoS Secu- Stateful firewalls with app ITEMS	inity	. As such, custom application	is, network aliases a +
Manage B Overview Devices Co Clients different Applications S Security Analyze	Roles Applications C Gateways are effectively Per-field help Network Allases NAME ad servers	IPS PBR QoS Secu stateful firewalls with app	irity	. As such, custom application	is, network aliases ar +
BB Overview Image: Devices Image: Devices <t< td=""><td>Roles Applications C Gateways are effectively Per-field help Network Aliases NAME ad servers</td><td>IPS PBR QoS Secu stateful firewalls with app ITEMS</td><td>lication inspection capabilities</td><td>. As such, custom application</td><td>is, network aliases an</td></t<>	Roles Applications C Gateways are effectively Per-field help Network Aliases NAME ad servers	IPS PBR QoS Secu stateful firewalls with app ITEMS	lication inspection capabilities	. As such, custom application	is, network aliases an
Devices Clients Guests Applications Security Analyze	Gateways are effectively Per-field help Network Aliases NAME ad servers	stateful firewalls with app	lication inspection capabilities	. As such, custom application	is, network aliases ar +
Clients Guests Applications Security Analyze	Per-field help Network Allases NAME ad servers	ITEMS			+
Clients Guests Applications Security Analyze	Network Allases NAME ad servers	ITEMS			+
Guests Applications Security Analyze	Network Aliases NAME ad servers	ITEMS			+
Applications Security Analyze	NAME ad servers	ITEMS			
Security Analyze ————————————————————————————————————	ad servers		DESCRIPTION	INVERT	
Analyze		2		false	
	any	1		false	
	auth-google	2		false	-
🗷 Audit Trail	controller	1		false	
Tools	localip	1		false	
The Departs	mswitch	1		false	
ag Reports	Service Aliases				+
n flooren	NAME	PROTOCOL	PORT	ALG	
gr Firmware	any				
😫 Organization	any-v6	255			
	svc-adp	udp	8200		
	svc-cfgm-tcp	tcp	8211		
	svc-citrix	tep	2598		
	svc-dhcp	udp	67-68		

Figure 132: RFC1918

Step 11 Click the "+ (plus sign) beside **Network Aliases**. In the **Name** field, enter *captive portal*.

Step 12 Click the **+** (plus sign) in the **User Rules** table.

Step 13 With the Name field selected, enter *cppm.example.local*

Step 14 Click Save.

Step 15 Click Save Settings.

aruba Central		Q Search or a					٩	Q New Central	Q New Central	Q New Central
Customer: Orange TME	arcars Balats	(Catoway)						SELECTED GROUP TYPE Branch Gateway	SELECTED GROUP TYPE II. Branch Gateway summary	SELECTED GROUP TYPE II. III Branch Gateway summary Lat
第 @ BR-ECSDB 이	Access Points Switches	Gateways						· · · · · · · · · · · · · · · · · · ·		
Manage	system Dav WAN Tunne	Policies							Ad	Advance
PD Quencieu	Roles Applications DPS	PBR QoS Security								
DE Overview	Catourus are effectively stat	of d frequelle with applicatio	n inconstion constitution. As a	ush surrow applications potund	alianan a	nd conice places can be defined	nd convice allosses say he defined. Cherry many	nd son ise allocar say he defined. Chevy mare	nd consists allocate can be defined. Characterized	nd can ice stisses can be defined. Chevy many
Devices	Gateways are effectively stat	erui irrewaiis with applicatio	in inspection capabilities. As s	uch, custom applications, networ	anases ar	to service allases can be denned.	to service allases can be defined. Show more	la service allases can be defined. Show more	ia service allases can be defined. Show more	ia service allases can be defined. Snow more
🗈 Clients	Per-field help									
왔 Guests	Network Aliases				+					
Applications	NAME	ITEMS	DESCRIPTION	INVERT						
Security	ad servers	2	DESCRIPTION	false						
Analyze	any	1		false						
Analyze	auth-facebook	3		false						
L Alerts & Events	auth-google	2		false						
🗹 Audit Trail	controller	1		false						
🖏 Tools	mswitch	1		false						
Reports										
Maintain	Service Aliases				+					
A Firmware	NAME	PROTOCOL	PORT	ALG						
	any									
Crganization	any-v6	255								
	svc-adp	udp	8200				*	•	h	h
	svc-cootp	tro	8211							
	svc-citrix	tcp	2598							
	svc-dhcp	udp	67-68							
	are onep	oop	0.00							
									Cancel	Cancel S

Figure 133: url rule

Central		Q Search or a	sk Aruba						
Customer: Orange TME	Arcess Points Switches	<u>@</u> Gateways							
ជ 🖬 BR-ECSDB 🛛	System LAN WAN Tunn	els & Routing Policies							
— Manage —	Roles Applications DPS	PRI 16 Security							
B Overview		- Security							
Devices	Gateways are effectively stateful firewalls with application inspection capabilities. As such, custom applications, network aliases and service aliases can be defined. Show more								
🗖 Clients	Per-field help								
😩 Guests	Network Aliases			+					
Applications	NAME	ITEMS	DESCRIPTION	INVERT					
Security	ad servers	2		false					
- Analyze	any	1		false					
	auth-facebook	3		false					
Д Alerts & Events	auth-google	2		false					
🛛 Audit Trail	controller	1		false					
& Tools	localip	1		false					
- 100IS	mswitch	1		false					
Reports	Service Aliases				+				
the Planet	NAME	PROTOCOL	PORT	ALG					
t∰ Firmware	any								
ដ្ងៃ Organization	any-v6	255							
	svc-adp	udp	8200						
	svc-bootp	udp	67-69						
	svc-cfgm-tcp	tcp	8211						

Step 16 Click the Security tab next to QOS.

Figure 134: navigation_to_apply_rules

Step 17 In the Roles table, select the Visitor role.

Step 18 In the **Policies** table click the + (plus sign) symbol and enter *visitor_net_policy*.

NOTE:

The Visitor user role was created using global client roles. If the user role was not created using global client roles or if the deployment is not using multi site fabric, the User role can be created in the group by clicking the **Roles** tab on the page below.
Central	Q Search or ask Aruba	
Orange TME	(And And And And And And And And And And	
SVStem LAN WAN TH	s Gateways	
Roles Applications D	PBR QoS Security	
Each device connected to	he branch network will be associated with a user role. Define the firewall policies associated to those u	iser roles to determine which traffic to
es		
s Per-field help		
Ralas	1	
Koles		
ap-role		
default-iap-user-role		
default-via-role		
S default-vpn-role		
guest		
guest-logon		
logon		
stateful-dot1x		
switch-logen		
e sys-switch-role		
voice		
VISITOR		
IT-ADMIN		
IT-SUPP	•	
PRINTER		
IOT-INTERNAL		
IOT-LMT-INET		
IOT-NO-INET REJECT		
QUARANTINE		
CRITICAL		
SECURITY		
EMPLOYEE		



Step 20 In the **Rules** table click the **+** (plus sign) to create a new rule.

Step 21 In the Rule table, assign the following:

- Source: Any
- **Destination:** Network Alias
- **Destination Alias:** *ad server*
- Service/App: sys-svc-dns
- Action: Permit

Step 22 Click Save.

Central	Q Search or ask Aruba		٩	New Central 🌒 🛛 🧔
Orange TME				SELECTED GROUP TYPE
-ECSDB	System LAN WAN Tunnels & Routing Policies			Advance
	Roles Applications DPS PBR QoS Security			
VIEW	Each device connected to the branch network will be associated with a	user role. Define the firewall policies associated to those user roles to	determine which traffic to allow or deny through the sateway. Show more	
ces	call device connected to the pranci methodik will be associated with a	dan role, benne the mewan pointes associated to those user roles to	determine which came to show or deny chooge the gateway. Show note	
its	Per-field help			
its	Roles +	Policies +	Rules	
cations	ap-role	VISITOR_r2r_policy		
ity	authenticated	visitor_net_policy		
	default-iap-user-role		*	
	default-via-role			
s & Events	default-vpn-role			
Trail	guest			
	guest-togon			
rts	stateful-dot1x			
	switch-logon			
	sys-ap-role			
vare	sys-switch-role			
nization	voice		No data to display	
	VISITOR			
	IT-SUPP			
	PRINTER			
	IOT-INTERNAL			
	IOT-LMT-INET			
	IOT-NO-INET			
	REJECT			
	QUARANTINE			
	SECURITY			
	EMPLOYEE			
				Cancel

Figure 136: adding rules to policy

Step 23 Repeat Steps 18 to 20 to complete the table below. Then click **Save Settings**. The completed policy is illustrated below.

Source	Destination	Service	Action
Any	AD Servers	DNS	Permit
Any	AD Servers	DHCP	Permit
Any	Captive Portal	Https	Permit
Any	RFC1918	Any	Deny
Any	Any	Any	Permit

stem LAN WAN Tunnels & Routing Policies toles Applications DPS PBR QoS Security				Advanced Mode
Each device connected to the branch network will be associated v Per-field help	with a user role. Define the firewall policies assoc	iated to those user roles to	determine which traffic to allow or deny through the gateway. Show more	
Roles	Policies	+	Rules	+
ap-role	VISITOR_r2r_policy		Allow service sys-svc-dns from any to alias ad servers	
authenticated	III visitor_net_policy	Î		
default-lap-user-role			Allow service svc-bootp from any to alias ad servers	
default-via-role				
default-vpn-role			Allow service svc-https from any to alias captive portal	
guest				
guest-logon			Deny service any from any to alias rfc1918	
logon			Allow service any from any to any	
stateful-dot1x				
switch-logon				
sys-ap-role				
sys-switch-role				
voice				
VISITOR				
IT-ADMIN				
IT-SUPP				
PRINTER				
IOT-INTERNAL				
IOT-LMT-INET				
IOT-NO-INET				
REJECT				
QUARANTINE				
CRITICAL				
SECURITY				
EMPLOYEE				

21 Save Settings

Figure 137: complete visitor policy-5016929

Summary

Successful flow of information is critical for a well-run organization.

The Aruba SD-Branch design is a prescriptive solution based on best practice and tested topologies. SD-Branch facilitates building a robust WAN network to accommodates the organization's network requirements.

For users located at a headend site or at a smaller branch site, the design provides a consistent set of features and functions for reliable network access, improving user satisfaction and productivity while reducing operational expense.



Figure 138: Network_Overview

The Aruba SD-Branch design provides a consistent and scalable method of building the network, improving overall usable network bandwidth and resilience, and making the WAN easier to deploy, maintain, and troubleshoot.

Aruba Microbranch

The Microbranch architecture provides remote teleworkers and small branches with wireless connectivity and secure access to corporate resources.

Zero Touch Provisioning (ZTP) simplifies Microbranch deployment, requiring only an Internet connection to provision an AP, upgrade firmware, and deploy configuration through Aruba Central.

Microbranch supports three SSID operating models:

- **Routed Layer 3 SSIDs** optimize traffic patterns, while allowing access to internal corporate resources.
- **NATed Layer 3 SSIDs** provide access to Internet services, but do not allow access to the internal corporate network.
- Layer 2 Tunneled SSIDs forward all traffic to the data center VPNC, including Internet traffic. Note that tunneling Layer 2 traffic may introduce suboptimal traffic patterns.

Organizational requirements at Microbranch locations should be considered before choosing a deployment model. The following sections demonstrate how to configure a Microbranch AP in all three modes.

Aruba Layer 3 Microbranch AP Configuration

Layer 3 Microbranch also referred to as Distributed Layer 3 (DL3). Allows admins the ability to provide three different types of access, Routed Layer 3, Nated Layer 3 and Fully-tunneled access. This guide will demonstrate, all three types of access.

Full Tunnel uses Policy based routing and will be shown as a optional section of the guide.

This guide demonstrates how to configure two types of Microbranch SSIDs:

- *EXAMPLE-CORP* is a Routed Layer 3 SSID that provides access to corporate resources. It is assigned VLAN ID 101 and prefix 10.14.200.0/24, which is advertised to the broader campus network.
- *EXAMPLE-GUEST* is a NATed Layer 3 SSID that provides only Internet access. It is assigned VLAN 100 and prefix 192.168.0.0/24, which is only routed locally.

NOTE:

This guide uses the VPNC configured in the hub & spoke section. To configure a VPNC, review the "Deploying VPNC" section.

The illustration below shows the Microbranch topology.



Figure 139: Micro-Branch

Create a Microbranch AP Group

Step 1 In the left navigation pane, in the Maintain section, select Organization.

Step 2 In the left navigation pane, click Global, then select the Groups column heading.

Step 3 To create a **New Group**, in the upper right, click + (plus sign).

Step 4 In the Add Group window, enter a name, click the Access Point checkbox, then click Next.

Step 5 Leave *ArubaOS 10* selected in **Architecture for access points and gateways in this group**. Click the **Microbranch** radio button under **Network role of the access points in this group**, then click **Add**.



Figure 140: Creating AP Group

Configure System IP Pool

The System IP Pool assigns IP addresses to access points dynamically, as required for Microbranch AP setup.

APs use their assigned IP for the inner tunnel IP address and to source traffic such as RADIUS, TACACS+, and SNMP. The System IP Pool is applied to the Microbranch group in a future step.

Step 1 Select the Global group. In the left navigation pane, click Network Services.

Step 2 Select the IP Address Manager tab.

Step 3 In the upper right, click + (plus sign).

Step 4 In the Add System IP Pools window, enter the following: - Pool Name: System IP Pool - Start address: 10.14.254.1 - End address: 10.14.254.100

Step 5 Click Save.



Figure 141: Configuring Address Pool

Configure VLAN DHCP Pool

A **Shared DHCP Pool** is configured for later assignment to the *EXAMPLE-CORP* VLAN.

Step 1 Select the **Global** group. In the left navigation pane, select **Network Services**.

Step 2 Select the IP Address Manager tab, then select the Shared DHCP Pools tab.

Step 3 To create a DHCP pool, in the upper right, click + (plus sign).

Step 4 In the **Add Shared DHCP Pool** window, enter the following: - **Pool Name:** *EXAMPLE-CORP* - **Start address:** *10.14.200.1* - **End address:** *10.14.200.255* - **Hosts per DHCP VLAN:** *20*

Step 5 Click Save.

Central				Q Search or a				۹	🜻 🕐 🖁
ନ୍ତୁ Global ୍	OD SD-WAN OVERLAY	က် IP Address Manager	ஓ Virtual Gatew	ays Cloud Connect	ے Cloud Security (Legacy)				Config
— Manage	System IP Pools Share	ed DHCP Pools							
BB Overview	Shared DHCP Po	ols							+ 💬
Devices	Pool Name			IP Range		Hosts per DHCP VLAN	Allocated DHCP Pools		
🗖 Clients									
🚉 Guests									
Applications									
Security						*			
器 Network Services									
- Analyze									
🛛 Audit Trail									
🖏 Tools		No Rows To Show							
🗊 Reports									
- Launch									
App Catalog									
— Maintain —									
Firmware									
😫 Organization									



Set AP Device Password

Step 1 In the **Global** dropdown, search and select the Microbranch AP group created previously.

Step 2 In the left navigation pane under Manage, select Devices.

Step 3 Select the **Access Points** tab. In the upper right corner, click the **Config** (gear) icon.

Step 4 Enter a device password in the **Password** field, re-enter the password in the **Confirm password** field, then click **Set Password**.



Figure 143: AP Group Navigation

Configure Country Code

It is important to assign the proper country code to ensure that APs operate in compliance with local regulatory restrictions.

Step 1 In the UI-MICRO-AP-01 > Devices configuration panel, in the System tile, select Properties.

Step 2 In the **Set country code** field, select the appropriate country code from the dropdown.

Step 3 Click Save.

orubo Central	Q s	earch or ask Aruba	ፍ ሰ 🖲 🏭 ሐ
법 UI-MICRO-AP-01 O	55 Points		
- Manage			
88 Overview			
Devices			
🗈 Clients			
🙁 Guests			
Applications			
Security			
Analyze	• 0		
û Alerts & Events		Tunnels & Routing	Services
🗾 Audit Trail			
🔦 Tools			
Reports			
- Maintain			
Firmware			
			0 •
	Security Client Authentication		

Figure 144: configuring Country Code

Assign System IP Pool to AP Group

Step 1 In the UI-MICRO-AP-01 > Devices configuration panel, in the System tile, select IP Addressing.

Step 2 Click + (plus sign).

Step 3 In the **Select IP Address Pool** field, select the previously configured *System IP Pool*.

Step 4 Click Save.

Central	Q 2	earch or ask Aruba		۹	(<u>ව</u>
UI-MICRO-AP-01	Cess Points			th Summary	i Ust	(Config
- Manage				Configura	ation Stat	tus
BB Overview	System	WAN	LAN			
Devices	Properties Country code, DHCP	WAN Uplink Branch gateway uplinks (Ethernet, Cellular)	VLANS Virtual subnets management			
🗈 Clients	IP Addressing Select IP address pool A. IP address pool is required for tunnel traffic	Uplink Management Enforce preferred uplink	Port Profiles Wired network profiles and access control			
🚉 Guests	DNS & NTP Domain name & Time servers	WAN Health Check Monitor WAN paths performance				
Applications	Administrator					
Security						
- Analyze	• 0					
☆ Alerts & Events	Wireless	Tunnels & Routing	Services			
🗷 Audit Trail	WLAN Wretess network profiles & 351Ds	Data Center VPN concentrators priority & overlay orchestration	Real-Time Locating System integrate with external RTLS systems			
🖏 Tools	Radios Radios frequency bands, channels & transmit power	Static Routing Default & back up routes	CALEA Lawful communication interception integration			
🔝 Reports		Policy-based Routing Customize routing policies & rules	Network Integration Paio Alto Network frewall integration			
- Maintain		NextHop List				
Firmware		Network destinations routing table				
ទ្រ Organization			• 0			
	Security					
	Client Authentication Authentication servers, MPSK					
	Threats Management Wreless IDS/IPS					
	Policies & Access Control Roles, Alases, Denylisting, Custom blocked URL, Intra VLAN allowlist, Firewall Settings					



Configure DNS and NTP

Step 1 In the UI-MICRO-AP-01 > Devices configuration panel, in the System tile, select DNS & NTP.

Step 2 In the Domain Name field, enter the domain name.

Step 3 To add a DNS server, in the DNS SERVERS header, click + (plus sign).

Step 4 In the dropdown, select a DNS service.

Step 5 Click Save.

aruba Central	Q 9	earch or ask Aruba	ዓ ሷ 🖲 🚟 🖁
및 UI-MICRO-AP-01 O	ess Points		
- Manago			
BB Overview			
Devices			
🖽 Clients			
跳 Guests			
Applications			
Security			
- Analyze	• 0		
▲ Alerts & Events		Tunnels & Routing	Services
🗾 Audit Trail			
🔦 Tools			
Reports			
- Maintain			
Firmware			
			0 •
	Security		
	Manage Conclusion		

Figure 146: Configuring DNS

Step 6 Expand the **NTP** section, and click **> NTP**.

Step 7 To add a NTP server, in the PUBLIC NTP SERVERS header, click + (plus sign).

Step 8 In the new empty field, enter an NTP server name or IP address.

Step 9 In the **Timezone** field, select a timezone from the dropdown.

Step 10 Click Save.

aruba Central		Q Searc	h or askAruba	ዓ 🗘 🖲 🖩 ሐ
\$ UI-MICRO-AP-01 O	lo Iss Points			
- Manage -	DNS & NTP			
Devices				
LD Clients				
🔐 Guests				
Applications				
Security Analyze				
🖬 Audit Trail				
🖏 Tools				
Reports				
- Maintain	> NTP			
G Timware				

Figure 147: Configuring NTP

Configure WAN Uplink

The WAN uplink identifies the interface assigned a WAN IP address. Tunnel Orchestrator uses this WAN IP address to create tunnels between devices.

Step 1 In the **UI-MICRO-AP-01 > Devices** configuration panel, in the **WAN** tile, select **WAN Uplink**.

Step 2 On the right side, click + (plus sign).

Step 3 In the Uplink Name, enter the uplink interface name.

Step 4 Click Save.

aruba Central			۹ 🖉 🗮 🕅
😫 UI-MICRO-AP-01 💦 Acco	6 ass Points		
- Manage			
88 Overview			
Devices			
🗂 Clients			
음 , Guests			
Applications			
Security			
Analyze	• 0		
ф Alerts & Events		Tunnels & Routing	Services
🗷 Audit Trail			
🔩 Tools			
Reports			
- Maintain			
Firmware			
			• 0

Figure 148: Config

Configure WAN Health Check

A WAN Health Check measures latency and packet loss on WAN uplinks using ICMP or UDP probes. UDP-based probes add measurement of jitter and generation of MoS scores.

Step 1 Go to the **UI-MICRO-AP-01 > Devices** configuration panel, in the **WAN * tile, select** WAN Health Check**.

Step 2 Click the slider right of Monitor WAN health.

Step 3 Click the Custom radio button.

Step 4 In the Protocol field, click the dropdown and select UDP.

Step 5 Click Save.

Central	0	Search or ask Aruba		<mark>ዓ </mark>
업 UI-MICRO-AP-01 이	Contract Con			lli ∷≣ Summary List Config
- Manage				Configuration Status
88 Overview	System	WAN	LAN	
Devices	Country code, DHCP	WAN Uplink Branch gateway uplinks (Ethernet, Cellular)	VICANS Virtual subnets management	
⊑a Clients	IP Addressing Select IP address pool	Uplink Management Enforce preferred uplink	Port Profiles Wired network profiles and access control	
🙁 Guests	DNS & NTP Domain name & Time servers	WAN Health Check Monitor WAN paths performance		
Applications	Administrator Local device administration			
Security				
- Analyze	• 0			
Alerts & Events	Wireless	Tunnels & Routing	Services	
🗹 Audit Trail	WLAN Wireless network profiles & SSIDs	Data Center VPN concentrators priority & overlay orchestration	Real-Time Locating System Integrate with external RTLS systems	
🖏 Tools	Radios Radios frequency bandis, channels & transmit power	Static Routing Default & back up routes	CALEA Lawful communication interception integration	
Reports		Policy-based Routing Customize routing policies & rules	Network Integration Palo Alto Network firewall integration	
— Maintain ————		NextHop List		
Firmware		Lefteren v. anthrougenen in Leanurd Connect		
ង្ខ Organization			• 0	
	Security Client Authentication Anterestation traves, Mark Thread Swagement Weines DUMS Building & Access Control	۱.		
	Roles, Aliases, Denylisting, Custom blocked URL, Intra VLAN allowlist, Firewall Settings			

Figure 149: Configuring WAN Health Check

Configure Hub Site

Step 1 Go to the **UI-MICRO-AP-01 > Devices** configuration panel. In the **Tunnels & Routing** tile, select **Data Center**.

Step 2 In the Data Center header, click + (plus sign).

Step 3 In the **HUB GROUP** dropdown, select the VPNC Group configured in *Hub and Spoke Deployment*.

Step 4 In the Cluster Name dropdown, select the cluster configured in Hub and Spoke Deployment.

Step 5 Click Save.

orubo Central	Q Search or ask Aruba		Q	New Central	2 🔊 🎗
Customer: Orange TME	6			il. Summary	
ជ UI-MICRO-AP-01 〇	Access Points			Configur	ation Status
- Manage	System	WAN	LAN		
BB Overview	Properties Country code, DHCP	WAN Uplink Branch gateway uplinks (Ethernet, Cellular)	VLANs Virtual subnets management		
Devices	IP Addressing Select IP address pool	Uplink Management Enforce preferred uplink	Port Profiles Wred network profiles and access control		
Clients	DNS & NTP Domain name & Time servers	WAN Health Check Monitor WAN paths performance			
🛎 Guests	Administrator Local device administration				
Applications					
Security	• 0				
- Analyze	Wireless	Tunnels & Routing	Services		
Alerts & Events	WLAN Wireless network profiles & SSIDs	Data Center VPN concentrators priority & overlay orchestration	Real-Time Locating System Integrate with external RTLS systems		
Audit Trail	Radio Profiles RF profiles to control allowed frequency bands, channels, and power range	Static Routing Default & back up routes	CALEA Lawful communication interception integration		
🖏 Tools		Policy-based Routing	Network Integration		
Reports		Customize routing policies & rules NextHop List	Paio Also Network Trewall Integration		
Maintain		Network destinations routing table	IoT radio, Zigbee service, BLE beacon service		
Firmware				0	
😫 Organization	6le-				
	Client Authentication				
	Authentication servers, MPSK Threats Management				
	Wireless IDS/IPS		*		
	Policies & Access Control Roles, Aliases, USB port policy, Derylisting, Custom blocked URL, Intra VLAN allowlist	t, Firewall Settings			
	Certificate Store Manage certificates				

Figure 150: configure_hub-8257684

Configure VLANs

Create VLANs for the route *EXAMPLE-CORP* SSID and the *EXAMPLE-GUEST* SSID.

Step 1 Go to the **UI-MICRO-AP-01 > Devices** configuration panel, in the **LAN** tile, select **VLANs**.

Step 2 In the VLANs header, click + (plus sign).

orubo Central	Q :			۹	¢	0 A
법 UI-MICRO-AP-01 이	G Access Points			th. Summary	i List	© Config
- Manage				Configu	ration St	atus
B Overview	System	WAN	LAN			
Devices	Properties Country code, DHCP	WAN Uplink Branch gateway uplinks (Ethernet, Cellular)	VLANs Virtual subnets management			
□ Clients	IP Addressing Select IP address pool	Uplink Management Enforce preferred uplink	Port Profiles Wired network profiles and access control			
🙎 Guests	DNS & NTP Domain name & Time servers	WAN Health Check Monitor WAN paths performance				
Applications	Administrator Local device administration					
Security						
- Analyze	• 0					
Alerts & Events	Wireless	Tunnels & Routing	Services			
🗹 Audit Trail	WLAN Wreless network profiles & 35IDs	Data Center VPN concentrators priority & overlay orchestration	Real-Time Locating System Integrate with external RTLS systems			
🖏 Tools	Radios Radios frequency bands, channels & transmit power	Static Routing Default & back up routes	CALEA Lawful communication interception integration			
Reports		Policy-based Routing customize routing policies & rules	Network Integration Palo Alto Network firewall integration			
- Maintain		NextHop List				
Firmware		receiver a second country country.				
ង្ហ Organization			• 0			
	Security Client Authentication Administration Server, UP3X Threast Management Wrees 05095 Policies & Access Control Rom, Auto, Dongtorne, Contron Blocket URI, Intra VLAN albudite, Prevail Sectorys					

Figure 151: Navigating to VLAN Creation

CAUTION:

Do not use the same VLAN ID at a Microbranch site and on the VPNC. If the same VLAN ID is configured on both, a Layer 2 tunneled SSID is created operationally, even if the configuration specifies Layer 3 Routed or NATed.

Step 3 In the new VLAN form, enter the following field values. - **DHCP Profile Name:** *EXAMPLE-CORP* - **VLAN ID:** *101* - Click the **Routed** radio button - **DHCP Pool:** *EXAMPLE-CORP* - **Excluded addresses:** *5* - **Domain name:** *example.local* - **DNS Server:** *Specify Servers* - *10.2.120.98,10.2.120.99*

Step 4 Leave other fields at their default values.

Step 5 Click Save.

땳 UI-MICRO-AP-01 이	ৃত্ত Access Points
— Manage ————	← VLAN
E Overview	
Devices	EXAMPLE-CORP 101
Clients	Routed NATed
😩 Guests	DHCP Server Configuration
Applications	DHCP server comgutation DHCP pool EXAMPLE-CORP 5
Security	Apply to the beginning of the range
- Analyze	Domain Name DNS server example local Specify servers
🋕 Alerts & Events	
🛛 Audit Trail	10.2.120.98,10.2.120.99
🔏 Tools	DHCP Options
💼 Reports	
— Maintain ————	DHCP Lease Time
Firmware	720 min.
ង Organization	Summary
	IP Range 10.14.200.1 - 10.14.200.255
	Number of IPs 255 addresses - 5 first reserved
	Number of Pools 0 pools allocated - 7 remaining

Figure 152: Configure Example Corp VLAN

Step 6 In the **VLANs** header, click + (plus sign).

Step 7 In the new VLAN window, enter the following field values.

- DHCP Profile Name: EXAMPLE-GUEST
- VLAN ID: 100

- Click the **NATed** radio button
- Subnet: 192.168.0.0
- Subnet Mask: 255.255.255.0
- Domain name: example.local
- DNS Server: AP Assigned DNS Server
- Excluded addresses: 5

Step 8 Leave other fields at their default values.

Step 9 Click Save.

법 UI-MICRO-AP-01 이	ි Access Points	
— Manage ————	← VLAN	
日 Overview		
Devices	EXAMPLE-GUEST 100	
🗖 Clients	Routed NATed	
a Guests	DHCP Server Configuration	
Applications	Subnet Mask	
Security	192.168.0.0 255.255.0	
- Analyze	Domain Name DNS server	
Alerts & Events	example.local Use AP's assigned DI	NS S ▼
🖪 Audit Trail	DHCP Options Type Value	+ ō
🖏 Tools	DHCP Lease Time Excluded addresses	
💼 Reports	720 min. 5 Apply to the beginning of t	he range
— Maintain ————		
Firmware	IP Range 192.168.0.1 - 192.168.0.254	
ដ្ ធ Organization	Number of IPs 254 addresses - 5 first reserved	

Figure 153: Configure Example Guest VLAN

Configure the WPA3-Enterprise Wireless LAN

The following procedure creates a secure, routed SSID for accessing internal resources.

Step 1 Go to the UI-MICRO-AP-01 > Devices configuration panel. In the Wireless tile, select WLAN.

Step 2 Near the bottom left of the WLANs tab, click + Add SSID.

Wirele	cess Points	Radios	Interfaces	Security	Services	System	IoT	Configuration Audit			
	ess SSIDs										
NAM	1E			SECURITY	(ACCESS TYPE		TRAFFIC FORWARDING MODE	NETWORK ENABLED
									No data	to display	

Figure 154: Add SSID

Step 3 On the General tab, set the SSID Name field to EXAMPLE-CORP.

Step 4 To display additional settings, click > **Advanced Settings**.

Step 5 To expand broadcast/multicast options, click (+) **Broadcast/Multicast**.

Step 6 In the Broadcast filtering dropdown, select All.

Step 7 To expand legacy transmission rate options, click (+) Transmit Rates (Legacy Only).

Step 8 In the 2.4 GHz section, set the following values. - Min: 5 - Max: 54

Step 9 In the 5 GHz section, set the following values. - Min: 18 - Max: 54

Step 10 Click Next.



Figure 155: General Configuration

Configure SSID VLAN

On the VLANs tab, enter the following values, then click **Next**. - **Traffic forwarding mode:** *L3 Routed/-NATed*. - **Client VLAN Assignment:** *Static* - **VLAN ID**: *EXAMPLE-CORP (vlan:101)*

Create a New Network	
1 General 2 VLANs	3 Security Access Summary
Traffic forwarding mode:	L2 Forwarded L3 Routed/NATed Mixed Care Care Care Care Care Care Care Care
Client VLAN Assignment:	Static Dynamic Native VLAN
VLAN ID	EXAMPLE-CORP (vlan:101) \times To add/edit DHCP scope profile
> Show Named VLANs	
	Cancel Back Next

Figure 156: Setting VLAN

Configure SSID Security Settings

Enable 802.1X authentication and encryption on the SSID.

Step 1 To set the security level, move the **Security Level** slider to *Enterprise*.

Step 2 From the Key Management dropdown, select WPA3 Enterprise(CMM 128).

CAUTION:

Use WPA3 when possible to benefit from significant security improvements over WPA2. Consult endpoint documentation to confirm that Microbranch devices support WPA3. If devices do not support WPA3, use WPA2-Enterprise.

Create a New Network				
1 General 2 VLANs	3 Security	(4) Acc	cess 💿 Su	mmary
Security Level:	Enterprise	Personal	Visitors	Open
Radius Proxy:				
Primary Proxy Server:			Select Cluster	•
Key Management:			WPA3-Enterpris	se(CCM 128)
Primary Server:			Select	▼ + This field is mandatory.
> Advanced Settings				

Figure 157: Enabling dot1x

Step 3 To add a primary RADIUS server, beside the Primary Server field, click + (plus sign).

Step 4 In the NEW SERVER window, enter the following values, then click OK.

- Server Type: RADIUS
- Name: cppm-01
- IP Address: 10.2.120.94
- Shared Key: < Enter the RADIUS server shared key >
- Retype Key: < Re-enter the RADIUS server shared key >

NEW SERVER				×
Server Type:	RADIUS	Name:	cppm-01	
Radsec:		IP Address:	10.2.120.94	
Shared Key:		NAS IP Address:	optional	
Retype Key:		NAS Identifier:	optional	
Retry Count:	3	Auth Port:	1812	
Timeout (in secs):	5	Accounting Port:	1813	
Service Type Framed User: MAC/Captive Portal		CPPM Username:		
Password:		Retype:		
				Cancel

Figure 158: Adding Radius Server

NOTE: It is important to record the **Shared Key** for use when configuring ClearPass Policy Manager.

Step 5 To add a secondary RADIUS server, beside the **Secondary Server** field, click + (plus sign).

Step 6 Repeat step 4 with appropriate values for the secondary RADIUS server.

Step 7 To enable Load Balancing, click the slider.

0			
Enterprise	Personal	Visitors	Open
		WPA3-Enterp	orise(CCM 128)
		cppm-01	▼ + 🖍
		cppm-02	• + 🖍
	·	·	WPA3-Enterp cppm-01 cppm-02

Figure 159: Enabling Load Balancing

Step 8 Click Next.

Configure Network Access Rules

Network access rules apply policy enforcement for an SSID based on the role or IP address of a device.

Orubo Central			Q Search or as	(Aruba
ជ UI-MICRO-AP-01	ි Access Points			
Manage				
B Overview	Create a New Network		_	
Oevices	1 General 2	VLANs 3	Security	4 Access
🗖 Clients	Access rules		_	
🙁 Guests			Role Ba	sed N
Applications				tion allows ful
Security			M onrestricted op	uon allows fu
nalyze				
Alerts & Events				
Audit Trail				
🖏 Tools				
Reports				
Maintain				
Firmware				
ង្ហ Organization				

Step 1 Leave the default setting of Unrestricted, then click Next.

Step 2 On the Summary tab, review all settings and click Finish.

Configure the Visitor Wireless LAN

The following procedure creates a NATed SSID with a captive portal for guest Internet access.

Create Visitor SSID

Step 1 In the UI-MICRO-AP-01 > Devices configuration panel, in the Wireless tile, select WLAN.

WEANS	Access Points	Radios	Interfaces	Security	Services	System	IoT	Configuration Aud
Wi	ireless SSIDs							
	NAME			SECURITY	(ACCESS TYPE
	EXAMPLE-CO	ORP		wpa3-aes	-ccm-128			Unrestricted

Step 2 On the bottom left of the WLANs tab, click + Add SSID.

Step 3 On the General tab, set the SSID Name field to EXAMPLE-GUEST.

Step 4 To display additional settings, click > Advanced Settings.

Step 5 To expand broadcast/multicast options, click (+) **Broadcast/Multicast**.

Step 6 In the Broadcast filtering dropdown, select All.

Step 7 To expand legacy transmission rate options, click (+) Transmit Rates (Legacy Only).

Step 8 In the 2.4 GHz section, set the following values. - Min: 5 - Max: 54

		0
1	General (2) VLANs (3) Security	(4) Access (5) Summary
	Name (SSID):	EXAMPLE-GUEST
\sim	Advanced Settings	
Θ	Broadcast/Multicast	
	Broadcast filtering:	ALL 🔻
	DTIM Interval:	1 beacon
	Dynamic Multicast Optimization (DMO):	
	DMO channel utilization threshold:	90 96
	DMO client threshold:	
Θ	Transmit Rates (Legacy Only)	
	2.4 GHz:	Min: 5 🔻 Max: 54

Step 9 In the 5 GHz section, set the following values. - Min: 18 - Max: 54

Figure 160: General SSID Configuration

NOTE:

Setting the time range for guest access is optional. Skip steps 11-14, if not applicable.

Step 10 Click Next to skip this configuration.

Step 12 To display time range options, click (+) Time Range Profiles.

Θ	Tim	e R	ang	e Pr	ofile	25													
	+ New Time Range Profile																		
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
	MON																		
	TUE																		
	WED																		
	THU																		
	FRI																		
	SAT																		
	SUN																		

Step 13 To create a new time range, click + New Time Range Profile.

Step 14 In the NEW PROFILE window, enter the following values, then click Save.

- Name: Guest Weekdays
- **Type:** *Periodic*
- Repeat: Daily
- Day Range: Monday Friday (Weekdays)
- Start Time:
 - Hours: 7

- Minutes: 0
- End Time:
 - Hours: 18
 - Minutes: 0
- Click Save.

NEW PROFILE	
Name:	Guest Weekday
Туре:	Periodic V
Repeat:	Daily Weekly
Day Range:	Monday - Sunday (All Days) Onday - Friday (Weekdays) Saturday-Sunday (Weekend)
Start Time:	Hours 7 V Minutes 0 V
End Time:	Hours 18 V Minutes 0 V
Note: The visualization is appr	roximated to the hour.
0 1 2 3 4 5	6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
Cancel	

Figure 161: Configuring Time profile

Step 14 The new time range appears in the **Time Range Profiles** list. To enable the profile, click the **Status** dropdown beside the name, select **Enabled**, then click **Next**.

() Ne Ra	Thi	<mark>s fea</mark> Profil	ture	requ	uires	NTP.																	
() ne Ra	Thi	<mark>s fea</mark> Profil	ture	requ	uires	NTP.																	
ne Ra	inge	Profil									i This feature requires NTP.												
ne Ra	inge	Protii		Timo Dango Brofilo													~						
													Status										
Guest Weekday (Periodic Weekday 07:00 18:00)						davu	07.0/	. 10										aabla	d				
est V	VEEK	uay (r	enc	Juic	vveek	udy	07:00	J - 10	5.00)								Ľ	able	u		•		
Ne	w Tir	ne R	ang	e Pr	ofile																		
te:	The	/isua	lizat	ion i	s app	roxir	nate	d to	the h	nour	-												
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
N								<u> </u>	<u> </u>		-	-	<u> </u>	<u> </u>		-							
							_				-	-				-							
P								<u> </u>	<u> </u>	<u> </u>	-	-	<u> </u>	<u> </u>		-	<u> </u>						
(
	Ne te: 0	New Tir	New Time R	New Time Rang	New Time Range Protection is 0 1 2 3 4	New Time Range Profile te: The visualization is app 0 1 2 3 4 5	New Time Range Profile te: The visualization is approxir 0 1 2 3 4 5 6 0 1 2 3 4 5 0 1 2 3 4 5 0 1 2 3 4 5 0 1 2 3 4 0 1 2 3 4 0 1 2 3 4 0 1 2 3 4 0 1 2 3 4 0 1 2 3 4 0 1 2 3	New Time Range Profile te: The visualization is approximate 0 1 2 3 4 5 6 7	New Time Range Profile te: The visualization is approximated to 0 1 2 3 4 5 6 7 8 0 1 2 3 4 5 6 7 8 0 1 2 3 4 5 6 7 8 0 1 1 2 3 4 5 6 7 8 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	New Time Range Profile te: The visualization is approximated to the I 0 1 2 3 4 5 6 7 8 9	New Time Range Profile te: The visualization is approximated to the hour 0 1 2 3 4 5 6 7 8 9 10 0 1 2 3 4 5 6 7 8 10 0 1 2 3 4 5 6 7 8 10 0 1 2 3 4 5 6 7 8 10 0 1 2 3 4 5 6 7 8 10 0 1 2 4 5 6 7 8 10 0 1 2 4 5 6 7 8 10 0 1 2 4 5 6 7 8 10 0 1 2 4 5 6 7 8 10 0 1 2 4 5 6 7 8 10 0 1 2 4 5 6 7 8 10 0 1 2 4 5 6 7 8 10 0 1 2 4 5 6 7 8 10 0 1 2 4 5 6 7 8 10 0 1 2 4 5 6 7 8 10 0 1 2 4 5 6 7 8 10 0 1 2 4 5 6 7 8 10 0 1 2 4 5 6 7 8 10 0 1 2 4 5 6 7 8 10 0 1 2 4 5 6 7 8 10 0 1 2 4 5 6 7 8 10 0 1 2 4 5 6 7 8 10 0 1 2 4 5 6 7 8 10 0 1 2 4 5 6	New Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 V 4 5 6 7 8 9 10 11 V 4 5 6 7 8 9 10 11 V 4 5 6 7 8 9 10 11 V 4 5 6 7 8 9 10 11 V 4 5 6 7 8 9 10 11 V 4 6 6 7 8 9 10 11 V 4 6 6 7 8 9 10 11 V 4 6 6 7 8 9 10 10 V 6 6 7 <td< td=""><td>New Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 0 1 2 3 4 5 6 7 8 9 10 11 12 0 1 2 3 4 5 6 7 8 9 10 11 12 0 1 2 3 4 5 6 7 8 9 10 11 12 0 1 2 3 4 5 6 7 8 9 10 11 12 0 1<</td><td>New Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 0 1 2 3 4 5 6 7 8 9 10 11 12 13 0 1 2 3 4 5 6 7 8 9 10 11 12 13 0 1 2 3 4 5 6 7 8 9 10 11 12 13 0 1 2 3 4 5 6 7 8 9 10 11 12 13 0 1 <</td><td>New Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 1</td><td>New Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 1</td></td<> <td>New Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 1 1 1 1 1 1 14 15 16 1 1 1 1 1 1 1 1 14 15 16 1 <td< td=""><td>Lesson New Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 0 1 1 1 1 1 14 15 16 17 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 <td< td=""><td>L New Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 0 1</td><td>Lessenation of the support of the supp</td><td>L See Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 Image: see See See See See See See See See See</td><td>Letter State 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 0 1 1 1 1 1 1 1 1 10 10 10 10 10 10 10 10 10 10 10</td><td>te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22</td></td<></td></td<></td>	New Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 0 1 2 3 4 5 6 7 8 9 10 11 12 0 1 2 3 4 5 6 7 8 9 10 11 12 0 1 2 3 4 5 6 7 8 9 10 11 12 0 1 2 3 4 5 6 7 8 9 10 11 12 0 1<	New Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 0 1 2 3 4 5 6 7 8 9 10 11 12 13 0 1 2 3 4 5 6 7 8 9 10 11 12 13 0 1 2 3 4 5 6 7 8 9 10 11 12 13 0 1 2 3 4 5 6 7 8 9 10 11 12 13 0 1 <	New Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 1	New Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 1	New Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 1 1 1 1 1 1 14 15 16 1 1 1 1 1 1 1 1 14 15 16 1 <td< td=""><td>Lesson New Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 0 1 1 1 1 1 14 15 16 17 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 <td< td=""><td>L New Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 0 1</td><td>Lessenation of the support of the supp</td><td>L See Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 Image: see See See See See See See See See See</td><td>Letter State 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 0 1 1 1 1 1 1 1 1 10 10 10 10 10 10 10 10 10 10 10</td><td>te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22</td></td<></td></td<>	Lesson New Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 0 1 1 1 1 1 14 15 16 17 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 <td< td=""><td>L New Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 0 1</td><td>Lessenation of the support of the supp</td><td>L See Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 Image: see See See See See See See See See See</td><td>Letter State 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 0 1 1 1 1 1 1 1 1 10 10 10 10 10 10 10 10 10 10 10</td><td>te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22</td></td<>	L New Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 0 1	Lessenation of the support of the supp	L See Time Range Profile te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 Image: see	Letter State 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 0 1 1 1 1 1 1 1 1 10 10 10 10 10 10 10 10 10 10 10	te: The visualization is approximated to the hour. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

Figure 162: Enable Time profile

Configure VLANs

On the VLANs tab, enter the following values, then click **Next**.

- Traffic Forwarding Mode: L3 Routed/NATed.
- Client VLAN Assignment: Static

	Create a New Network	
	1 General 2 VLANs	3 Security Access 3 Summary
	Traffic forwarding mode:	L2 Forwarded I L3 Routed/NATed Mixed A
	Client VLAN Assignment:	Static Dynamic Native VLAN
	VLAN ID	EXAMPLE-GUEST (vlan:100) To add/edit DHCP scope profile
	> Show Named VLANs	
• VLAN ID: Example-Guest(100)		Cancel

Configure Security

Enable a web-based captive portal.

Step 1 To set the security level, move the **Security Level** slider to **Visitors**.

Step 2 In the Access Network section, click the Type dropdown and select External Captive Portal.

1 General 2 VLANs	3 Securit	ty ④ Ac	ccess (5) Summary
Security Level:	Enterprise	Personal	Visitors Open
Access Network			
Туре:			External Captive Portal
Captive Portal Profile:			- Select - 🔻 +
			This field is mandatory.
Primary Server:			- Select - This field is mandatory.
Encryption:			
Key Management:			Enhanced Open
> Advanced Settings			

Figure 163: enable Captive portal

Step 2 To create a captive portal profile, click the **+** (plus sign) beside the **Captive Portal Profile** dropdown.

Step 3 In the **External Captive Portal-New** window, enter the following values, then click **OK**.

- Name: CPPM-Portal
- IP or Hostname: 10.2.120.92
- **URL:** /guest/mb_guest_portal.php
- Port: 443
- **Redirect URL:** *http://arubanetworking.hpe.com*

CAUTION:

The **IP or Hostname** field cannot be set to an FQDN for Layer 3 NATed SSIDs. The DNS request from the AP will be NATed and cannot resolve the FQDN correctly.

External Captive Portal-New	
Name:	CPPM-Portal
IP or Hostname:	10.2.120.92
URL:	/guest/mb_guest_portal.ţ
Port:	443
Use HTTPS:	
Captive Portal Failure:	Deny Internet
Server offload:	
Prevent Frame Overlay:	
Redirect URL:	http://www.arubanetwor

Figure 164: Captive Portal Configuration-2928543

Step 4 To set the primary RADIUS server, click the **Primary Server** dropdown and select the previously created primary RADIUS server.

Step 5 To set the secondary RADIUS server, click the **Secondary Server** dropdown and select the previously created secondary RADIUS server.

Step 6 To enable **Load Balancing**, toggle the slider.

Step 7 Click Next.



Figure 165: Configuring Radius Servers

NOTE:

Refer to *Configure SSID Security Settings* in the *Configure the WPA3-Enterprise Wireless LAN* section to create new RADIUS servers.

Configuring Access For Guest SSID

Pre- and post-authentication roles apply access restrictions to clients associated to an SSID. The pre-authentication role *EXAMPLE-DENY* denies all access except DNS, DHCP, and web access to the CPPM server. The *EXAMPLE-GUEST* post-authentication role allows access to all destinations. It is not necessary to block guests from internal networks in the post-authentication role because clients associated to the *EXAMPLE-GUEST* SSID cannot initiate connections to internal resources.

Configure Deny Role

Step 1 On the Access tab, move the slider to Role Based

Step 2 To create a new role, in the lower left, click + Add Roll.

Step 3 In the Add Roll window, enter EXAMPLE-DENY in the Role field, then click OK.

업 UI-MICRO-AP-01 〇	C) Access Points	il. I≣ 🛞 Summary List Confg
- Manage		
88 Overview	Create a New Network	
Oevices	General 2 VLANs 3 Security 4 Access 3 Summary	
Clients	Access rules	
🚉 Guests	Role Based Network Based Unrestricted	
Applications	A Unrestricted option allows full access to the network. This may lead to potential security issues.	
Security		
- Analyze		
🗾 Audit Trail		
🗞 Tools	*	
Reports		
- Maintain		
Firmware		
t Organization		
		Cancel Back Next

Figure 166: Creating Roles

Configure Deny ACL

Step 1 In the Role tile, select EXAMPLE-DENY.

Step 2 In the Access Rules For Selected Roles tile, select Allow any to all destinations, then click the edit (pencil) icon.

ा UI-MICRO-AP-01	G Access Points	,		1 /	-	, ,	th III Summary List	Cenfig
- Manage	Create a New Network							
88 Overview								
Devices	General 2 VOANS 3 Security	Access Summary						
Clients	Access rules	0						
🚉 Guests		Role Based	Network Based	Unrestricted				
Applications	Role	Access Rules For Sel	ected Roles					
Security	EXAMPLE-DENY	Allow http to r	naster IP					
- Analyze	EXAMPLE-GUEST	Allow tcp on p	ort 4343 to master IP					
Alerts & Events	default_wired_port_profile	🖬 🔹 Allow dhcp to	all destinations					
🗹 Audit Trail	wired-SetMeUp	🖬 💿 Allow dns to a	ll destinations					
🖏 Tools								
Reports								
- Maintain								
Firmware	+ Add Role	4 Role(s) + Add Rule					4 Rule(s	5)
😫 Organization								
	Role Assignment Rules							
	Default role: EXAMPLE-GUEST							

Step 3 In the Access Rules window, click the Action dropdown, select *Denv*, then click OK.

Step 4 To configure additional access rules, click + Add Rule.

Step 5 In the Access Rules window, enter the values from the first row in the table below and click OK.

Rule Type	Service type	Service	Action	Destination	Network
Access control	Network	HTTPS/HTTP	Allow	To Particular Server	10.2.120.92
Access control	Network	DNS	Allow	To Particular Server	10.2.120.98

Rule Type	Service type	Service	Action	Destination	Network
Access control	Network	DNS	Allow	To Particular Server	10.2.120.99
Access control	Network	DHCP	Allow	To all destinations	N/A

Step 6 Repeat steps 4 and 5 for each row in the table.

aruba Central		Q Search or ask Aruba	۹	40 A
업 UI-MICRO-AP-01 이	0 Access Points		th Summary	List Config
- Manage	Create a New Network			
Devices	1 General 2 VLANs 3 Security 4 Access	Summary		
Clients	Access rules	0		
a Guests		Role Based Network Based Unrestricted		
Applications	Role	Access Rules For Selected Roles		
Ø Security	EXAMPLE-DENY	Deny any to all destinations		
- Analyze	EXAMPLE-GUEST			
	default_wired_port_profile			
Audit Trail	wired-SetMeUp	•		
🖏 Tools				
Reports				
- Maintain				
Firmware	+ Add Role 4 R	ole(s) + Add Rule		1 Rule(s)
😫 Organization				
	Role Assignment Rules			
	Default role: EXAMPLE-GUEST			

Figure 167: Configuring Access Rules

Step 7 In the Assign Pre-Authentication Role dropdown, select EXAMPLE-DENY

Step 8 Click Next.

Central		Q Search or ask Aruba	۹	۵	<u>ම</u> සි
법 UI-MICRO-AP-01 O	o is Points		il. Summary	i Ust	Config
Manage	detault_wired_port_profile	Allow ans on server 10.2.120.987255.255.255			
PD Ourselaw	wired-SetMeUp	Allow https on server 10.2:120.92/255.255.255			
BB Overview		Allow http on server 10.2.120.92/255.255.255			
🕑 Devices		Deny any to all destinations			
🚉 Guests	+ Add Role 4 Role	r(s) + Add Rule		6 Rule(s	.)
Applications					
Security	Role Assignment Rules				
- Analyze	Default role: EXAMPLE-GUEST				
Audit Trail					
🗞 Tools					
Reports					
- Maintain					
Firmware					
b Organization	+ ADD ROLE ASSIGNMENT			1 Role(s)	0
	Assign Pre-Authentication Role:	EXAMPLE-DENY			
		Cancel	Back	Next	

Figure 168: image-20220518204544679

(Optional) Routed Layer 3 Full-Tunnel Configuration

In highly secure deployments all traffic might need to be securely tunneled back to security appliances to ensure compliance, before forwarding to the appropriated destinations. The following section demonstrates how to configure a full tunnel.

To configure full-tunnel in Layer 3 Microbranch deployments, the Data Center deployment should be adjusted, and a **Policy-Based Routing (PBR)** policy should be created . With a rule stating that all traffic to any destination should be forwarded to either a VPNC or pair of VPNCs (via next hop list), through the secure IPsec tunnel. The PBR policy is then assigned to the user role(s). The users or devices who are assigned to the user role have all their user traffic forwarded to the data center via the secure tunnel.

Configure Hub Priority

Previously in the guide the hub site was configured as a site cluster which load balances based on route across the cluster, when full tunneling this can cause Asymmetric routing with a full tunnel deployment. To avoid this Manual Hub deployment should be used, this will Force the AP's to tunnel to a single gateway. If the primary gateway fails the tunnels will failover to the next gateway in the group.

Step 1 Go to the **UI-MICRO-AP-01 > Devices** configuration panel. In the **Tunnels & Routing** tile, select **Data Center**.

Step 2 In the Data Center header, hover over the configured group and select the trash can.

HPE _____ GreenLake 88 O Search or ask Art Q 👲 🔿 🔗 Orubo Central New Central er: Orange TME il. 1 Access Points ជ UI-MICRO-AP-01 Manag System WAN LAN WAN Uplink Branch gateway up Properties R Overview IP Addressing Select IP address pool Devices Uplink Mana Lo Clients DNS & NTP WAN Health Check & Guests Administrator Applications • 0 Security Wireless Tunnels & Routing Alerts & Events Data Center WLAN Real-Time Locating System 🛛 Audit Trail Static Routing CALEA S Tools Policy-based Routing Customize routing policies & rule Network Integration Reports NextHop List Eirmware • 0 🔓 Organization Security Client Authentication Threats Manage Policies & Ac © Copyright 2023 He Terms of Use Ad Choices & Cookies Do Not Sell or Share My Person

Step 3 Click Save.



Step 4 In the Tunnels & Routing tile, select Data Center.

Step 5 Select the Hubs radio button

Step 6 In the Data Center header, click + (plus sign)

Step 7 In the **HUB GROUP** dropdown, select the VPNC Group configured in *Hub and Spoke Deployment*.

Step 8 In the **Cluster Name** dropdown, select the *RSVDC-VPNC-1* configured in *Hub and Spoke Deployment*.

Step 9 In the highlighted **VPNC-RSVDC** header click + (plus sign), select *RSVDC-VPNC-2*.

Step 10 Click Save.

HPE GreenLake					88
aruba Central	Q Search or ask Aruba		۹	New Central	¢ 🛛 2
Customer: Orange TME	Access Points			th Summary	List Config
ជ UI-MICRO-AP-01 🛛	Access Forma			Configura	tion Status
- Manage	System	WAN	LAN	comgan	
BB Overview	Properties Country code, DHCP	WAN Uplink Branch gateway uplinks (Ethernet, Cellular)	VLANs Virtual subnets management		
Devices	IP Addressing Select IP address pool	Uplink Management Enforce preferred uplink	Port Profiles Wired network profiles and access control		
□ Clients	DNS & NTP Domain name & Time servers	WAN Health Check Monitor WNN paths performance			
🚨 Guests	Administrator				
Applications					
Security	• 0				
- Analyze	Wireless	Tunnels & Routing	Services		
Alerts & Events	WLAN Wreters network profiles & SSIDs	Data Center VPN concentrators priority & overlay orchestration	Real-Time Locating System Integrate with external RTLS systems		
🗹 Audit Trail	Radio Profiles	Static Routing	CALEA		
🖏 Tools	to promotive control ansarce incidentity earliest control and beauty uniffic	Policy-based Routing	Network Integration		
Reports		Customize routing policies & rules NextHop List	Paio Alto Network firewall integration		
- Maintain		Network destinations routing table	IoT radio, Zigbee service, BLE beacon service		
Ø Firmware		*		0	
នៃ Organization	for market				
	Client Authentication				
	Authentication servers, MPSK Threats Management				
	Wireless IDS/IPS				
	Roles, Aliases, USB port policy, Denylisting, Custom blocked URL, Intra VLAN allowlist, Firewall Settings				
	Certificate Store Manage certificates				
© Copyright 2023 Hewlett Packard F	nterorise Development I.P	Privary	Terms of Use Ad Choices & Cookies	Do Not Sell or Share My Pers	onal Information

Figure 170: set_manual_hub_priority

Create PBR policy for full-tunnel

Step 1 Go to the group **UI-MICRO-AP-01 > Devices** page. In the **Tunnels & Routing** tile, select **Policy-based Routing**.

Step 2 Near the top right of the Policies tab, click + (plus sign).

Step 3 Enter a PBR policy name (*eg: EXAMPLE-PBR-DL3-FULL-TUNNEL*).

orubo Central	Q Search or ask Aruba		۹	New Central	¢	02
Customer: Orange TME				il. Summary	List	(B) Contra
법 UI-MICRO-AP-01 〇	Access Points			Confi	guration	Status
- Manage	System	WAN	LAN			
B Overview	Properties Country code, DHCP	WAN Uplink Branch gateway uplinks (Ethernet, Cellular)	VLANs Virtual subnets management			
Devices	IP Addressing Select IP address pool	Uplink Management Enforce preferred uplink	Port Profiles Wired network profiles and access control			
Clients	DNS & NTP Domain name & Time servers	WAN Health Check Monitor WAN paths performance				
😫 Guests	Administrator Local device administration					
Applications						
Security	• 0					
- Analyze	Wireless	Tunnels & Routing	Services			
↓ Alerts & Events	WLAN Wireless network profiles & SSIDs	Data Center VPN concentrators priority & overlay orchestration	Real-Time Locating System			
🗹 Audit Trail	Radio Profiles PE explicit to control allowed fees used where channels and ensure came	Static Routing	CALEA			
🖏 Tools	rer promes to control anoweo requency banos, chamiero, and power range	Policy-based Routing	Network Integration			
Reports		Customize routing policies & rules	Palo Alto Network firewall integration			
- Maintain		Network destinations routing table	IoT radio, Zigbee service, BLE beacon service			
Firmware				0		
😫 Organization				0		
	Security Client Authentication					
	Authentication servers, MPSK					
	Threats Management Wireless IDS/IPS					
	Policies & Access Control Roles, Alases, USB port policy, Derylisting, Custorn blocked URL, Intra VLAN allowlist, Firewall Settings					
	Certificate Store					
	Manage certificates	*				

Figure 171: create_pbr_policy

NOTE:	
When a new PBR policy is added, a default rule to forward any traffic to internet automatically.	is created

Step 5 Mouse-over *EXAMPLE-PBR-DL3-FULL-TUNNEL* policy and click the **edit** (pencil) icon on the right.

← Policy-based routing

Policies (2)				+
Names Rules Roles				
EXAMPLE-PBR-DL3-FULL-TUNNEL	1		ľ	Ō
default policy	1			·

Figure 172: image-20230928141634927

Step 6 Mouse-over the default rule that was created automatically.

Step 7 Click the edit (pencil) icon on the right.

•	← Policy-based routing					
	EXAMPLE-PBR-DL3-FULL-TUNI	NEL - Rules (1)				
	Source	Destination	Service / Application	Action		
	= Any	Any	Any	Forward		

Figure 173: image-20230928141818901

+

Step 8 Click the EDIT RULE table. Perform either (1) or (2) based on the requirement as mentioned.

To forward all the user traffic to terminate on to a single VPNC, enter below details and click **OK** - **Source:** *Any*

- **Destination:** Any
- Service/App: Any
- Action: Forward to IPSec Map to VPNC
- **VPNC**: The VPNC to terminate traffic
- Uplink Tag: The uplink of the VPNC



Figure 174: image-20230929101758372

Policy-based routing						
EXAMPLE-PBR-DL3-FULL-TUNNEL - Rules (1)					+	
Source	Destination	Service / Application	Action			
= Any	Any	Any	Forward to IPsec map to VPNC : gw-ipsecmap-	-eth0-uplink		

Figure 175: image-20231002145937585

Step 9 To forward all the user traffic to nexthop devicesusing nexthop list, enter below details and click **OK**

• Source: Any

- **Destination:** Any
- Service/App: Any
- Action: Forward to Nexthop List
- Name of next-hop-list: < select the nexthop list name >

←	Edit Rule	
Sour Any	ce	~
Desti Any	nation	~
Servi Any	ce/App	~
Actio Forw	n ard to Nexthop List	~
Nam EXAN	e of next-hop-list /IPLE-NEXTHOP-LIST	~

Figure 176: image-20231002155648848

Step 10 Click Save.

Apply PBR Policy for Full-Tunnel to User Role

Step 1 Go to the group UI-MICRO-AP-01 > Devices page. In the Security tile, select Policies & Access Control.

Step 2 Expand the Roles section.

Step 3 Select the user role to which to apply the PBR policy.

Step 4 In the Rules window, click + (plus sign).

÷	Policies & Access Control Roles, Aliases, Denylisting, Custom blocked URL, Intra VLAN allowlist, Firewall Settings							
~ R	Y Roles							
	Roles (4)	+ 0	RULES (1)	+ 💬				
	Role		Access Rules For Selected Roles					
- [EXAMPLE-CORP		 Allow any to all destinations 					
	default_wired_port_profile							

Figure 177: image-20231002165508884

Step 5 In the ADD RULE window, enter the following values, then click OK.

- Rule Type: Policy-Based Routing
- Add Existing Policy:

ADD RULE

• Policy Name: EXAMPLE-PBR-FULL-TUNNEL

Rule Type Policy-Based Routing	~	Add existing policy Policy name EXAMPLE-PBR-DL3-FULL-TU	Add a new policy
			CANCEL

Figure 178: image-20231002165549846

Step 6 The PBR policy configured for full-tunnel is assigned to the user role.

←	Policies & Access Control Roles, Aliases, Denylisting, Custom blocked URL, Intra VLAN allowlist, Firewall Settings					
Υ R	oles					
	Roles (4)	+ 💬	RULES (2)	+ 💬		
	Role		Access Rules For Selected Roles			
- [EXAMPLE-CORP		 Allow any to all destinations 			
	default_wired_port_profile		→ Policy-Based Routing EXAMPLE-PBR-DL3-FULL-TUNNEL			

Figure 179: image-20231002165647469

Step 7 Click Save.



Assign a Microbranch AP to a Group

Step 1 In the left navigation pane, click Global, then select the Groups column heading.

Step 2 Expand the **Unprovisioned devices** group by clicking the expansion icon (>) next to its name.

Step 3 Select the Microbranch AP.

Step 4 Click the Move Devices icon.

Step 5 In the Destination Group dropdown, select UI-Micro-AP01.

Step 6 Click Move.





Assign a Microbranch AP to a Site

The following procedure assigns the VPNCs to a site.

Step 1 Go to Organization and select Site.

Step 2 Select Unassigned devices.

Step 3 Select the *Microbranch* AP on the right side, then drag the AP to the ESP-MB01 site.

Step 4 Click Yes.
orubo Central			Q Search or ask Aruba					۹	¢ 0 8
율 Global	Network Structure	Diatform Integration							
- Manage	Drag And Drop D To Select Multipl	Devices To Add To A Site le Devices Shift+Click Or Ctrl+Click							
Devices	Convert Labels	s To Sites							
Clients	▽ Site Name	∀Address	Device Count	ħ	∀Name	∀ Group	∀туре		
a Guests	All Devices		111		RSVCP-AC3-AP133	UI-WIRELESS	IAP		
Applications	Unassigned		31		AP-WDSM02-01	BR-WDSM02	IAP		
C Security	BHAM-01	1030 Lakeway Dr	2		RSVCP-AC4-AP10	CP-RSVWLAN	IAP		
security	BR-SAC01	3535 Elverta Rd	2		RSVCP-AC2-AP9	CP-RSVWLAN	IAP		
8 Network Services	DSM-DC-01	4090 Westown Pkwy	0		BR-IACITY02-AP01	BR-IACITY02	IAP		
Analyze	ESP-MB01	4199 Campus Dr	0		BR-IACITY02-AH01	BR-IACITY02	IAP		
Alerts & Events	ESP-RS01	8501 foothills blvd	6		GW-WDSM03-BR02-01	BR-WDSM03	Gateway		
Audit Trail	ESP-RS02	6280 America Center Dr, CA	2		GW-WDSM03-BR02-02	BR-WDSM03	Gateway		
🖏 Tools	ESP-RS03	27816 Jones Rd	2		RS01-AP01	UI-AP-BR01	IAP		
Reports	ESP-VPNC-DC01	3333 Scott Blvd	2	-	RSVCP-AC2-AP14	CP-RSVWLAN	IAP		
Launch	IACITY01	21 N Clinton	4		RSVCP-AC2-AP1	CP-RSVWLAN	IAP		
App Catalog	IACITY02	1660 Sycamore St	6		RS01-AP02	UI-AP-BR01	IAP		
Maintain	ME01	12 Main St.	1		20:4c:03:32:ad:b4	UI-MICRO-AP-01	IAP		
Firmware	RSVCP	8000 Foothills BLVD	42		AP-WDSM03-04	BR-WDSM03	IAP		
b Organization	SJC01	503 W. Capitol Expy	5		RSVCP-AC2-AP6	CP-RSVWLAN	IAP		
	WDSM01	925 Jordan Creek Pkwy	2		RSVCP-AC1-AP15	CP-RSVWLAN	IAP		
	WDSM02	360 Bridgewood Dr	1		BR-IACITY01-AP01	BR-IACITY01	IAP		
	WHE01	100 N. Milwaukee	4		AP-WDSM03-03	BR-WDSM03	IAP		
					BR-IACITY01-AP02	BR-IACITY01	IAP		
	New Site			16 Sites				111	Device(s)

Figure 181: Adding microbranch AP to site

Monitor Microbranch AP Routing Overlay

The route orchestrator redistributes the routes between the headend VPNCs and the Microbranch APs. All the overlay routing information such as control connections, routes advertised, routes learned, etc. can be monitored in the AP device page.

Step 1 Go to AP Group > Devices > Access Points > List.

Step 2 Select an AP.

Step 3 Under Overview, click Routing tab.

Step 4 Select Overlay tab.

Step 5 The Overlay summary table displays an overview of control connection state, number of interfaces, number of routes advertised from AP and number of routes learned by the AP

Step 6 Under the **Overlay details**, in the dropdown box, select **Routes advertised** which displays all the routes advertised from the AP.

Step 7 Under the **Overlay details**, in the dropdown box, select **Routes learned** which displays all the routes learned by the AP.

Orubo Central		0	Search or ask Aruba			٩	New Central	ے 🕫 🛱
Customer: Orange TME			Sloor Plan Performance	F P				4) 3 hour
← 🖾 20:4c:03:32:ad:b4 ⊘	Summary	Ai insignos	Plot Plan Performance	Kr Kouting				
- Manage				*				Actions 🔻
B Overview	DEVICE				NETWORK			
	AP MODEL AP-303H		COUNTRY CODE	MAC 20:4c:03:32:ad:b4	o Down	SPEED (Mbps) / DUPLEX	VLAN -	LLDP Details
E Clients	SERIAL NUMBE	ER	UPTIME	LAST REBOOT REASON	ETH1	SPEED (Mbps) / DUPLEX	VLAN	
E cients	CNG9K2R0K	N	18 Minutes 1 Second	Reboot caused by kernel panic: Out	o Down		-	
諸 LAN	10.5.0.0_876	i91	Synchronized	Dual Band	ETH2 O Down	SPEED (Mbps) / DUPLEX	VLAN	
Security					ETLIZ	SPEED (Mhore) / DLIPLEY	VII AN	
- Analyze	5.31 W		POWER NEGOTIATION 802.3 at	GROUP UI-MICRO-AP-01	o Down	-	-	
↓ Live Events	LABELS		NAME	SITE	CURRENT UPLINK	UPLINK CONNECTED TO	IP ADDRESS	
			20:4c:03:32:ad:b4	ESP-MB01	Ethernet (eth0)	HM-SW1 Port: 1/1/9	10.1.100.22 (DHCP) :: (IPv6)	
Audit Trail	LEDs on ACCES	JS POINT			PUBLIC IP ADDRESS 69.62.193.6	DNS NAME SERVERS 10.2.120.98,10.2.120.99	DEFAULT GATEWAY 10.1.100.1 (DHCP)	
🖏 Tools	NOTE 🧨				NTP SERVER			
— Maintain ————					pool.ntp.org			
Firmware								
	RADIOS		Radio 2.4 GHz		Radio	5 GHz		
	MODE		-					
	STATUS		o Down		o Dow	m		
	RADIO MAC	ADDRESS	90:4c:81:4e:bb:c0		90:4c:	81:4e:bb:d0		
	CHANNEL				-			
	POWER							

Figure 182: mb_route_table

Aruba Microbranch Centralized Layer 2 (CL2) Overview

Centralized Layer 2 (CL2) is an extension of previously introduced Remote Access Point (RAP). CL2 forwarding provides flexible options:

• All user traffic can be tunneled entirely to the data center.

CL2 is supported for both wireless and wired clients. In CL2 mode, Microbranch AP does not act as DHCP server or as a gateway for the clients. DHCP server and Default GW reside in the data center, so DHCP requests from the client are tunneled to the data center. CL2 also extends the corporate VLAN or broadcast domain to remote branches.

Common usage for CL2 includes, but is not limited to:

- Remote deployments that must perform security policy checks at the data center
- Remote deployments that require VLAN extension and DHCP scopes from the data center to the branches

The AP follows its routing table to forward traffic, so any user traffic is sent via the AP's default gateway (to the AP's WAN uplink to the ISP network).

In addition, the Overlay Route Orchestrator (ORO), that helps to advertise data center routes to APs dynamically, does not serve a role in CL2. Therefore, when using CL2, a policy must be defined to redirect or forward user traffic to the data center using Policy-Based Routing (PBR). The PBR policy action "forward to cluster" is designed specifically to enable CL2 mode to redirect traffic to VPNC clusters.

User Traffic Flow in CL2

After the user is authenticated, the VLAN configured for CL2 is assigned to the client. Two options are available to handle the user traffic flow or the APs' data forwarding decision to forward all user traffic to the data center or to forward only a select subset of user traffic to the data center:

- **Split-tunnel:** The AP tunnels only the user traffic destined to access resources at data center, while other traffic can be NATed locally to an AP WAN uplink (Internet or cellular).
- Full-tunnel: The AP tunnels all the user traffic to the data center.



Figure 183: CL2-split-full-tunnel-diagram

Split-Tunnel in CL2

The split-tunnel optimizes traffic flow by directing only corporate traffic back to the data center through the secure IPsec tunnel, while Internet application traffic can be bridged locally to the AP WAN uplink by source-NAT with AP uplink IP. This ensures that non-corporate Internet traffic does not incur the overhead of a round trip to the data center VPNCs, which decreases traffic on the WAN link and minimizes latency for voice/video applications such as Zoom, Teams, etc.

By default, all user traffic is NATed locally to the AP WAN uplink and does not allow access to corporate resources. To allow access to internal resources with CL2, engage split-tunneling by configuring **Policy-Based Routing (PBR)** policy with two or more rules. Traffic matching a PBR rule with the action "*forward to cluster*" is securely tunneled to the UDG (User Designated Gateway). If traffic does not match a PBR rule, the traffic is src-NATed with the AP uplink's IP and sent to the uplink.

Full-Tunnel in CL2

In full-tunnel mode, the Microbranch AP forwards all user traffic securely via the IPsec tunnel to the VPNC clusters at the data center instead of using its own routing table for routing decision. Full-tunneling may required to perform additional required security checks at the data center and/or to provide centralized access for all user traffic. Typical usage would include networks for banking and insurance that require scrutinizing user traffic at the data center for added security and other similar business situations.

To configure full-tunnel in CL2 Microbranch deployments, a **Policy-Based Routing (PBR)** policy is created first with a rule stating that any user traffic to any destination must be forwarded to the cluster through the secure IPsec tunnel. Traffic matching any PBR rule with the action "*forward to cluster*" is securely tunneled to the UDG (User Designated Gateway).

NOTE:

By default, all user traffic is sent to the AP's WAN uplink, so data center resources cannot be accessed. PBR rules must be configured to send authorized user traffic to the data center to access internal resources.

Determine UDG (User Designated Gateway) for Clients in CL2

For overlay cases, unlike DL3 where the routing table in AP (populated by ORO) determines the VPNC that client traffic terminates, using CL2 the AP receives the *bucket map* from the data center to map clients to the VPNC, also known as UDG (User Designated Gateway).

Any time a client sends traffic to the data center, the AP checks its bucket map, determines the client's UDG, and forwards the traffic through the pre-established IPsec tunnel to the UDG/VPNC assigned to the client. This helps with load balancing in addition to assigning clients to a specific UDG/VPNC in the data center cluster.

The screenshot below displays the bucket map that the AP receives from the data center. The client (in Station list) connected to the AP is assigned to the UDG/VPNC with index 1 and IP 172.30.28.33. The traffic from the client destined to the data center is sent via the secured IPSec tunnel to UDG/VPNC.

-MB-515- :# show overlay bucketmap						
Cluster auto_gwclu	uster_215_0 radio=0	zone=0 - Num UACs 2				
Index ArrayIdx U	UAC IP Num ST	'As				
	172.30.28.32 0					
Station List	172.30.20.33					
UAC Index Station	n Mac BSSID					
1 7E:DA:	9C:8C:					
Bucket Map						
Pucket Idy Pance	Pucket Man					
Bucket fux Range	Bucket Map					
[0-31]						
[32=63]						
[64-95]	0 0 0 0 0 0 0 0 0 0 0					
[96-127]	0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0				
[128-159]	1 1 1 1 1 1 1 1 1 1					
[160-191]	11111111111	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1				
[192-223]	11111111111	11111111111111111111111				
[224-255]	11111111111	11111111111111111111111				
	Standby Map					
[0-31]	1 1 1 1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1				
[32-63]	1 1 1 1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1				
[64-95]	1 1 1 1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1				
[96-127]	1 1 1 1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1				
[128-159]	0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0				
[160-191]	0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0				
[192-223]	<u> </u>	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0				
[224-255]	<u> </u>	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0				
Statistics:Bmap Up	pdates=5; UAC:Adds=2	<pre>2 Deletes=0; STA:Adds=0 Deletes=17 moves=0 errs=0 copies=0</pre>				

Figure 184: CL2-bucketmap

This set-up also can be observed on the **Client Details** page in the Aruba Central user interface. The UDG where the client traffic is tunneled and the UDG IP are displayed in the screenshot below.



Figure 185: CL2-client-UI

Aruba CL2 VPNC Configuration

This guide provides the configuration steps required for VPNCs at the data center for CL2 mode Microbranch deployments. VLAN ID 253 (10.20.253.0/24) is the VLAN configured on the VPNC that will be extended to the AP. *UI-MICRO-VPNC-01* is the group in which the data canter VPNCs are added.

NOTE:

This guide uses the VPNC configured in the hub and spoke section. To configure a VPNC, review the "Deploying VPNC" section. This section describes only the VPNC configurations required for CL2 mode in Microbranch deployments.

Configure CL2 VLAN

The VLAN configured in the VPNC is extended to Microbranch AP in CL2 mode deployments. The configuration of CL2 VLAN ID 253 is performed at the **VPNC group level**.

NOTE:

The DHCP server can reside in the data center to allocate the IP address for VLAN ID 253 to clients connected in CL2 mode. It should be reachable through VPNC.

Step 1 Go to the UI-MICRO-VPNC-01 > Devices > Gateways UI page.

Step 2 Select the Interfaces tab.

Step 3 Select the VLANs tab.

Step 4 In the VLANs window, click the + (plus sign) at the bottom left.

orubo Central	Q Search or	ask Aruba		Q	¢ 0 (ሐ
Customer: 1 HPE Inte	<u>်စွ</u> Gateways		SELECTED GROUP TYPE	II. Summary	iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	3 hfig
路 UI-MICRO-VPNC-01 〇	System WAN Interface Security VPN Routing	High Availability Config Audit		Basic Mode	Guided Setu	ιp
- Manage	Ports VLANs DHCP Pool Management G	RE Tunnels Bulk configuration upload				
B Overview						
Devices	Vlans					
🗖 Clients	NAME	ID(S)			≡	
😩 Guests	infra	1028				
Applications	internet-vlan	500				
Security		1				
- Analyze						
♪ Alerts & Events						
🛛 Audit Trail	+					
🖏 Tools	—					
🛍 Reports						
— Maintain ————						



Step 5 In the New VLAN window, enter: - VLAN Name: tunneled_users - VLAN ID/Range: 253

Step 6 Click Save Settings.

-	New VLAN				
G					UP OF
Sj	VLAN name:	tunneled_users			
P	VLAN ID/Range:	253	()		
l					
1				Cancel	Save Settings
	infra		1028		

Figure 187: CL2-VPNC-VLAN-New

Assign the CL2 VLAN to the VPNC LAN Port Interface

The newly created VLAN ID 253 for CL2 mode must be assigned to the VPNC LAN port interface so it can reach the DHCP server when a DHCP request comes through the tunnel.

Step 1 Go to the UI-MICRO-VPNC-01 > Devices > Gateways page.

Step 2 Select the Interfaces tab.

Step 3 Select the Ports tab.

Step 4 Select the LAN port interface (example: GE-0/0/7)

Step 5 In the port interface window, add the following: - Allowed VLANs: 253

Step 6 Click Save Settings.



Figure 188: CL2-VPNC-assign-VLAN-LAN-port-interface

Configuring CL2 Microbranch AP

This guide demonstrates the configuration of Centralized Layer 2 (CL2) mode SSID in Microbranch. *EXAMPLE-CL2* is a Centralized Layer 2 SSID providing access to both corporate resources and non-corporate resources through the Internet.

VLAN ID 253 is the tunneled user VLAN extended from the data center VPNC and assigned to the SSID (through clustering functionality). The VLAN ID 253 should be configured only in VPNC and not in the Microbranch AP.

The topology below illustrates the Microbranch.



Figure 189: CL2-Topology

Create a Microbranch AP Group

Step 1 Click the context filter Global.

Step 2 Hover over Groups column heading and click the settings icon.

Step 3 To create a New Group, in the upper right, click + (plus sign).

Step 4 In the Add Group window, enter a name. Click the Access Point checkbox, and click Next.

Step 5 Leave *ArubaOS 10* selected under **Architecture for access points and gateways in this group**. Click the **Microbranch** radio button under **Network role of the access points in this group**, then click **Add**.



Figure 190: Creating AP Group

Configure System IP Pool

The System IP Pool dynamically assigns IP addresses to access points, which is required for Microbranch AP setup. APs use the assigned IP as the system IP for the inner tunnel IP address and as a management address to source traffic such as RADIUS, TACACS+, and SNMP. The System IP Pool is applied to the Microbranch group in a future step.

Step 1 Select the Global group. In the left navigation pane, click Network Services.

Step 2 Select the IP Address Manager tab.

Step 3 In the upper right, click + (plus sign).

Step 4 In the Add System IP Pools window, enter the following: - Pool Name: System IP Pool

- Start address: 10.14.254.1
- End address: 10.14.254.100

NOTE:

The system IP pool is global and applied to all APs in the group. When designing the system IP pool size, account for all APs in the Microbranch group.

Step 5 Click SAVE.



Figure 191: Configuring Address Pool

NOTE:

Global VLAN DHCP pool is not required for Centralized Layer 2 (CL2) mode SSID. In CL2, the external DHCP server at the data center is used to define DHCP scope for the clients.

Set AP Device Password

Step 1 In the **Global** dropdown, search and select the Microbranch AP group previously created.

Step 2 In the left navigation pane under Manage, select Devices.

Step 3 Select the Access Points tab. In the upper right corner, click the config (gear) icon.

Step 4 Enter a device password in the **Password** field. Reenter the password in the **Confirm password** field, then click **Set Password**.



Figure 192: AP Group Navigation

Configure Country Code

It is important to assign the proper country code to ensure that APs operate in compliance with local regulatory restrictions.

Step 1 On the group **UI-MICRO-AP-01 > Devices** page, in the **System** tile, select **Properties**.

Step 2 In the **Set country code** field, select the appropriate country code from the dropdown.

Step 3 Click Save.

aruba Central	Q :	Search or ask Aruba	ዓ ቀ 🖲 🚟 🙈
및 UI-MICRO-AP-01 이	ess Points		
- Manage			
88 Overview			
Devices			
ҧ Clients			
음, Guests			
Applications			
Security			
Analyze	• 0		
Alerts & Events		Tunnels & Routing	Services
🗹 Audit Trail			
🖏 Tools			
Reports			
- Maintain			
Firmware			
			0 •
	Security		



Assign the System IP Pool to AP Group

Step 1 On the group UI-MICRO-AP-01 > Devices page, in the System tile, select IP Addressing.

Step 2 Click + (plus sign).

Step 3 In the **Select IP Address Pool** field, select the previously configured *System IP Pool*.

Step 4 Click Save.

aruba Central	Q 3	earch or ask Aruba		Q	¢	ා ක
업 UI-MICRO-AP-01	Access Points			llı Summary	i Ust	Config
- Manage				Configu	ration Sta	itus
B Overview	System	WAN	LAN			
Devices	Properties Country code, DHCP	WAN Uplink Branch gateway uplinks (Ethernet, Cellular)	VLANs Virtual subnets management			
Clients	IP Addressing Select IP address pool ▲ IP address pool is required for tunnel traffic	Uplink Management Enforce preferred uplink	Port Profiles Wired network profiles and access control			
2. Guests	DNS & NTP Domain name & Time servers	WAN Health Check Monitor WAN paths performance				
Applications	Administrator Local device administration					
Security						
- Analyze	• •					
☆ Alerts & Events	Wireless	Tunnels & Routing	Services			
🖬 Audit Trail	WLAN Wireless network profiles & SSIDs	Data Center VPN concentrators priority & overlay orchestration	Real-Time Locating System Integrate with external RTLS systems			
🖏 Tools	Radios Radios frequency bands, channels & transmit power	Static Routing Default & back up routes	CALEA Lawful communication interception integration			
🔝 Reports		Policy-based Routing Customize routing policies & rules	Network Integration Palo Alto Network firewall integration			
- Maintain		NextHop List				
Firmware		recents descharders rousing sacre				
😫 Organization			• 0			
	Security					
	Client Authentication Authentication servers, MPSK					
	Threats Management Wreless IDSIPS					
	Policies & Access Control Roles, Alases, Deryloting, Custom blocked URL, Intra VLAN allowlist, Firewall Settings					

Figure 194: SystemIP Pool

Configure DNS and NTP

Step 1 On the group UI-MICRO-AP-01 > Devices page, in the System tile, select DNS & NTP.

Step 2 In the Domain Name field, enter the domain name.

Step 3 To add a DNS server, in the DNS SERVERS header, click + (plus sign).

Step 4 Select a DNS service from the dropdown.

aruba Central	Q 9	arch or ask Aruba	ላ ሳ 🖲 🚟 ሐ
CUI-MICRO-AP-01	G ss Points		
Manage			
88 Overview		WAN	
Devices			
La Clients			
왔. Guests			
H Applications			
Security			
Analyze	• 0		
		Tunnels & Routing	Services
🗾 Audit Trail			
🖏 Tools			
💼 Reports			
— Maintain ————			
Ø Firmware			
			0 •

Figure 195: Configuring DNS

Step 5 To expand the **NTP** section, click **> NTP**.

Step 6 To add an NTP server, in the PUBLIC NTP SERVERS header, click + (plus sign).

Step 7 In the new empty field, enter an NTP FQDN or IP address.

Step 8 In the Timezone field, select a timezone from the dropdown.

Step 9 Click Save.

Central Central Search			۵ 🗘 🔍 ۹
🛱 UI-MICRO-AP-01 💦 🔒	Ccess Points		Ih 🔚 🍪 Summary Us Config
	← DNS & NTP ↓ DNS		
Devices			
Security			
Audit Trail			
	> NTP		

Figure 196: Configuring NTP

Configure WAN Uplink

The WAN uplink identifies the interface assigned a WAN IP address. Tunnel Orchestrator uses the WAN IP address to create tunnels between devices. The WAN Uplink name is used in the Tunnel Matching algorithm and it will try to match the same name on the other side of the tunnel. If the labels do not match, then it is attempted to match any other WAN label.

Step 1 On the group UI-MICRO-AP-01 > Devices page, in the WAN tile, select WAN Uplink.

Step 2 On the right side, click + (plus sign).

Step 3 In the Uplink Name field, enter the uplink interface name.

Step 4 Click Save.

aruba Central			۹ 🖉 📖 🖞
및 UI-MICRO-AP-01 이	55 Points		
- Manage			
88 Overview			
Devices			
En Clients			
🔐 – Guests			
Applications			
Security			
Analyze			
▲ Alerts & Events		Tunnels & Routing	Services
🛃 Audit Trail			
🔦 Tools			
Reports			
- Maintain			
Firmware			
			• 0

Figure 197: Config

Configure WAN Health Check

A WAN Health Check measures the quality of the WAN uplink. Latency and packet loss on WAN uplinks are calculated using ICMP or UDP probes. UDP-based probes add measurement of jitter and generate MoS scores.

Step 1 Go to the group UI-MICRO-AP-01 > Devices page. In the WAN tile, select WAN Health Check.

Step 2 To the right of Monitor WAN health, click the slider.

Step 3 Click the Custom radio button.

Step 4 In the **Protocol** field, click the dropdown and select *UDP*.

NOTE:

We recommend using **pqm.arubanetworks.com** as the remote FQDN (Fully Qualified Domain Names) for Health Check probes.

orubo Central	٥	Search or ask Aruba	ፍ 🗘 🔊 🖧
업 UI-MICRO-AP-01 이	ි Access Points		IL : Summary List Config
- Manage			Configuration Status
B Overview	System	WAN	LAN
Devices	Country code, DHCP	WAN UPINK Branch gateway uplinks (Ethernet, Cellular)	VERNS Virtual subnets management
_ Clients	IP Addressing Select IP address pool	Uplink Management Enforce preferred uplink	Port Profiles Wired network profiles and access control
🙁 Guests	DNS & NTP Domain name & Time servers	WAN Health Check Monitor WAN paths performance	
Applications	Administrator Local device administration		
Security			
- Analyze	• 0		
♠ Alerts & Events	Wireless	Tunnels & Routing	Services
🛛 Audit Trail	WLAN Wireless network profiles & SSIDs	Data Center VPN concentrators priority & overlay orchestration	Real-Time Locating System Integrate with external RTLS systems
🔩 Tools	Radios Radios frequency bands, channels & transmit power	Static Routing Default & back up routes	CALEA Lawful communication interception integration
Reports		Policy-based Routing Customize routing policies & rules	Network Integration Palo Ato Network firewall Integration
— Maintain —		NextHop List	
Firmware		Listena y nationario considiransi	
😫 Organization			• 0
	Security Client Authentication Authentication Firsts Management Wretes Looka Particles & Access Central Res, Values, Response Control Boosed VIL, Intra VLAV albelint, Firewal semign Particles & Access Central	×	

Figure 198: Configuring WAN Health Check

Configure the WPA3-Enterprise Wireless LAN

The following procedure creates a secure, CL2 mode SSID for accessing internal resources as well as non-internal resources.

Step 1 Go to the group UI-MICRO-AP-01 > Devices page. In the Wireless tile, select WLAN.

Step	2 Near	the bottom	left of the WLA	ANs tab, clic	k + Add SSID.
------	--------	------------	-----------------	---------------	---------------

ত ss Points					II. Summary	: List	<mark>ැලි</mark> Config	
← Wireless SSIDs								
Name (Profile)	Security	Access Type	Traffic forwarding	Network Enabled				
No data to display								
+ Add SSID						0 SS	ID(s)	

Figure 199: CL2-WLAN-SSID-Add

Step 3 On the General tab, set the SSID Name field to EXAMPLE-CL2.

Step 4 To display additional settings, click **> Advanced Settings**.

Step 5 To expand broadcast/multicast options, click (+) **Broadcast/Multicast**.

Step 6 In the Broadcast filtering dropdown, select All.

Step 7 To expand legacy transmission rate options, click (+) Transmit Rates (Legacy Only).

Step 8 In the 2.4 GHz section, assign the following values. - Min: 5 - Max: 54

Step 9 In the 5 GHz section, assign the following values. - Min: 18 - Max: 54

Step 10 Click Next.

Create a New Network

1 General 2 VLANs 3 Sec	curity 4 Access 5 Summary
Name (SSID):	EXAMPLE-CL2
 ✓ Advanced Settings 	
 Broadcast/Multicast 	
Broadcast filtering:	ALL
DTIM Interval:	1 beacon
Dynamic Multicast Optimization (DMO):	
DMO channel utilization threshold:	90 %
DMO client threshold:	6
Transmit Rates (Legacy Only)	
2.4 GHz:	Min: 5 🔻 Max: 54 🔻
5 GHz:	Min: 18 V Max: 54 V

Figure 200: CL2-WLAN-SSID-General

Configure SSID VLAN

On the VLANs tab, enter the following values, then click Next.

- Traffic forwarding mode: L2 Forwarded
- **Primary Gateway Cluster:** Select the primary *VPNC headend cluster* to terminate the L2 tunnel from drop-down menu
- **Secondary Gateway Cluster:** (optional) Select the *backup VPNC headend cluster* for VPNC redundancy from the dropdown
- Client VLAN Assignment: Static
- VLAN ID: From the dropdown, select the desired VLAN for users. Example: *tunneled_users* (*vlan:253*)

NOTE:

The VLAN ID in the dropdown are automatically populated from the selected VPNC Gateway cluster and these are the VLANs already configured on the VPNC side.

NOTE:

CL2 is dependent of having cluster on the VPNC side. In CL2, the VLAN ID and the headend VPNC clusters are selected while configuring the SSID itself without the need to configure them seperately.

Configure SSID Security Settings

Enable 802.1X authentication and encryption on the SSID.

Step 1 To set the security level, move the Security Level slider to Enterprise.

NOTE:

CL2 mode SSID uses VPNC clusters as the radius proxy when authentication is required.

Step 2 From the Key Management dropdown, select WPA3 Enterprise(CMM 128).

CAUTION:

Use WPA3 when possible to benefit from significant security improvements over WPA2. Consult the endpoint documentation to confirm that Microbranch devices support WPA3. If the devices do not support WPA3, use WPA2-Enterprise.

Create a New Network		
1 General 2 VLANs	3 Security 4 Access	5 Summary
Security Level:	Enterprise Personal V	ïsitors Open
Key Management:	WPA3-Enterprise(CCM	l 128) 🔻
Primary Server:	Select 🔻 🕂	This field is mandatory.
> Advanced Settings		

Figure 201: CL2-WLAN-SSID-Security-01

Step 3 To add a primary RADIUS server, beside the Primary Server field, click + (plus sign).

Step 4 In the NEW SERVER window, enter the following values, then click OK.

- Server Type: RADIUS
- Name: cppm-01
- IP Address: 10.2.120.94
- Shared Key: Enter the RADIUS server shared key
- **Retype Key:** *Re-enter the RADIUS server shared key*

NEW SERVER				×
Server Type:	RADIUS	Name:	cppm-01	
Radsec:		IP Address:	10.2.120.94	
Shared Key:		NAS IP Address:	optional	
Retype Key:		NAS Identifier:	optional	
Retry Count:	3	Auth Port:	1812	
Timeout (in secs):	5	Accounting Port:	1813	
Service Type Framed User:		CPPM Username:		
Password:		Retype:		
				Cancel

Figure 202: Adding Radius Server

NOTE:

It is important to record the **Shared Key** for use when configuring ClearPass Policy Manager.

Step 5 To add a secondary RADIUS server, beside the **Secondary Server** field, click + (plus sign).

Step 6 Repeat step 4 with appropriate values for the secondary RADIUS server.

Step 7 To enable Load Balancing, click the toggle.

Create a New Network	
1 General 2 VLANs	3 Security 4 Access 5 Summary
Security Level:	Enterprise Personal Visitors Open
Key Management:	WPA3-Enterprise(CCM 128)
Primary Server:	cppm-01 🔻 + 🖍 🖬
Secondary Server:	cppm-02 🔻 + 💉 💼
LOAD BALANCING:	
> Advanced Settings	
Key Management: Primary Server: Secondary Server: LOAD BALANCING:	Enterprise Personal Visitors Open WPA3-Enterprise(CCM 128) \checkmark $\boxed{ppm-01} + \checkmark$

Figure 203: CL2-WLAN-SSID-Security-02

Step 8 Click Next.

Configure Network Access Rules

Network access rules apply policy enforcement for an SSID based on the role or IP address of a device.

OFUDO Cent	ral	_		Search or a		
ជ UI-MICRO-AP-01	ි <mark>ම</mark> Access Points					
Manage	Create a N	lew Network				
BB Overview	create an					
Devices	1 Ge	eneral	2 VLANs	3 Security	4 Access	
🗖 Clients	Access	rules		-		
😩 Guests				Role B	ased Net	N
Applications				A Unrestricted o	ntion allows full a	
Security				Zanieschered o	protraions fail a	-
Analyze						
☆ Alerts & Events						
🛛 Audit Trail						
🖏 Tools						
🗈 Reports						
— Maintain —						
Firmware						
🔓 Organization						

Step 1 Leave the default setting of *Unrestricted*, then click **Next**.

Step 2 On the Summary tab, review all settings and click Finish.

CAUTION:

At this point, access to internal resources at the data center are restricted. By default in CL2 mode, the Microbranch AP routes all user traffic to its WAN uplink instead of sending them through the tunnel to the data center.

For the CL2 mode, to handle the user traffic flow at the AP and determine whether to forward all the user traffic to the data center or forward only a selective subset of user traffic to the data center, two options are available.

Step 1 Split-tunnel: The AP tunnels only the user traffic destined to access resources at the data center while other traffic can be locally NATed to the AP WAN uplink (Internet or cellular)

Step 2 Full-tunnel: The AP tunnels all user traffic to the data center

Configure Split-Tunnel in CL2

By default, all user traffic is locally NATed to the AP WAN uplink and does not have access to corporate resources. To allow access to internal resources for CL2, split-tunnel mode is activated by configuring **Policy-Based Routing (PBR)** policy with two or more rules and assigning the PBR policy to one or more user roles. The users or devices assigned to the user role(s) have their user traffic redirected accordingly either through the tunnel to the data center or broken out locally through the AP WAN uplink based on the individual rules configured in the PBR policy.

Create PBR Policy for Split-Tunnel

Step 1 Go to the group **UI-MICRO-AP-01 > Devices** page. In the **Tunnels & Routing** tile, select **Policy-based Routing**.

Step 2 Near the top right of the Policies tab, click + (plus sign).

Step 3 Enter the PBR policy **Name**, example: *EXAMPLE-PBR-SPLIT-TUNNEL*

Step 4 Click OK

Central	Q Search or a	sk Aruba		Q	¢	0	ሐ
Customer: 1 HPE Inte	access Points			II. Summary	:= List		<mark>ලා</mark> ionfig
ជ UI-MICRO-AP-01 이	Accession			Config	uration	Statu	s
 Manage Overview Devices Clients Guests Applications 	System Properties Country code, DHCP IP Addressing Select IP address pool DNS & NTP Domain name & Time servers Administrator Local device administration	WAN WAN Uplink Branch gateway uplinks (Ethernet, Cellular) Uplink Management Enforce prefered uplink WAN Health Check Monitor WAN paths performance	LAN VLANS Virtual subnets management Port Profiles Wired network profiles and access of	ontrol			
 Security Analyze Alerts & Events Audit Trail Tools Reports Maintain 	O Wireless WLAN Wireless network profiles & SSIDs Radios Radios frequency bands, channels & transmit power	Tunnels & Routing Data Center VPN concentrators priority & overlay orchestration Static Routing Default & back up routes Policy-based Routing Customize routing policies & rules NextHop List Network destinations routing table	Services Real-Time Locating System Integrate with external RTLS system CALEA Lawfu communication interception Network Integration Palo Alto Network firewall integratio	s integration			

Figure 204: CL2-PBR-Split-Tunnel-New-PBR

NOTE:

When a new PBR policy is added, a default rule to forward all traffic to internet is created automatically.

Step 5 Mouse-over *EXAMPLE-PBR-SPLIT-TUNNEL* policy.

Step 6 Click the edit (pencil) icon on the right

← Policy-based routing					
Policies (2)					
Names		Rules	Roles		
EXAMPLE-PBR-SPLIT-TUNNEL		1		Í	
default policy		1			



Step 7 Near the top right of the **Rules** tab, click + (plus sign).

Policy-based routing

EXAMPLE-PBR-SPLIT-TUNNEL - Rules (1)				
Source	Destination	Service / Application	Action	
= any	any	any	forward	

Figure 206: CL2-PBR-Split-Tunnel-add-rule

Step 8 In the ADD RULE table, enter the following values, then click OK

- Source: Any
 - Other dropdown options can be selected, such as host, network, alias, etc.
- **Destination:** Network
 - Other dropdown options can be selected, such as host, alias, any, etc.
- Network address: <eg: 10.20.253.0> (Internal resource network at Data Center to be accessed by user)
- Netmask: <eg: 255.255.255.0>
- Service/App: Any
 - Other dropdown options can be selected, such as app category, application, protocol, service, TCP, UDP, Web Category, Web Reputation etc.
- Action: Forward to Cluster

🔶 Edit Rule	
Source	
Any	~
Destination	
Network	~
10.20.253.0	
Netmask(version 4)	
255.255.255.0	
Service/App	
Any	~
Action	
Forward to Cluster	\sim

Figure 207: CL2-PBR-Split-Tunnel-rule-add-values

Step 9 The newly created rule is added to the *EXAMPLE-PBR-SPLIT-TUNNEL* policy

←	← Policy-based routing					
EX	EXAMPLE-PBR-SPLIT-TUNNEL - Rules (2)					
Sou	irce	Destination	Service / Application	Action		
=	Any	Any	Any	Forward		
=	Any	Network : 10.20.253.0 - 255.255.255.0	Any	Forward to cluster		

Figure 208: CL2-PBR-Split-Tunnel-list-rules

Step 10 Drag the newly created rule to the top and click Save

![CL2-PBR-Split-Tunnel-drag-rules](Media/cl2-pbr-split-tunnel-drag-rules.gif)

NOTE:

The order of rules in a PBR policy is important. The first rule to match the user traffic takes precedence.

Apply PBR Policy for Split-Tunnel to User Role

Step 1 Go to the group **UI-MICRO-AP-01 > Devices** page. In the **Security** tile, select **Policies & Access Control**.

Step 2 Expand the Roles section.

Step 3 Select the user role to which to apply the PBR policy

Step 4 In the Rules window, click + (plus sign)

←	Roles, Aliases, Denylisting, Custom blocked URL, Intra VLAN allowlist, Firewall Settings									
~ R	~ Roles									
	Roles (4)	+ 💬	RULES (1)	+ 💬						
	Role		Access Rules For Selected Roles							
	EXAMPLE-CL2		 Allow any to all destinations 							
	default_wired_port_profile									

Figure 209: CL2-PBR-assign-role

Step 5 In the ADD RULE window, enter the following values, then click OK.

- Rule Type: Policy-Based Routing
- Add Existing Policy:
- Policy Name: EXAMPLE-PBR-SPLIT-TUNNEL

ADD RULE



Figure 210: CL2-PBR-Split-Tunnel-assign-user-role

Step 6 The PBR policy is assigned to the user role.

← Policies & Access Con Roles, Aliases, Denylisting, C	trol Custom blocked URL, Intr	a VLAN allowlist, Firewall Settings	
~ Roles			
Roles (4)	+ 0	RULES (2)	+ 💬
Role		Access Rules For Selected Roles	
EXAMPLE-CL2		→ Policy-Based Routing EXAMPLE-PBR-SPLIT-TUNNEL	
default_wired_port_profile		 Allow any to all destinations 	



Step 7 Click Save

NOTE:

When a user is assigned a user role and the user traffic flows, all the access rules for the user role are applied first and if there is a PERMIT, the PBR policy is then applied to that specific user traffic.

Configure Full-Tunnel in CL2

To configure full-tunnel in CL2 Microbranch deployments, a **Policy-Based Routing (PBR)** policy should be created first with a rule stating that all user traffic to any destination should be forwarded to the cluster through the secure IPsec tunnel. The PBR policy is then assigned to the user role(s). The users or devices who are assigned to the user role have all their user traffic forwarded to the data center via the secure tunnel.

Create PBR policy for full-tunnel

Step 1 Go to the group **UI-MICRO-AP-01 > Devices** page. In the **Tunnels & Routing** tile, select **Policy-based Routing**.

Step 2 Near the top right of the Policies tab, click + (plus sign).

Step 3 Enter a PBR policy name (eg: EXAMPLE-PBR-FULL-TUNNEL).

Step 4 Click OK.



Figure 212: CL2-PBR-Full-Tunnel-New-PBR

NOTE:

When a new PBR policy is added, a default rule to forward any traffic to internet is created automatically.

Step 5 Mouse-over *EXAMPLE-PBR-FULL-TUNNEL* policy and click the **edit** (pencil) icon on the right.

Policy-based routing							
Policies (2)				+			
Names	Rules	Roles	_				
EXAMPLE-PBR-FULL-TUNNEL	1		1°	Ō			
default policy	1		_				



Step 6 Mouse-over the default rule that was created automatically.

Step 7 Click the edit (pencil) icon on the right.

Policy-based routing

EXAMPLE-PBR-FULL-TUNNEL - Rules (1)						
Source	Destination	Service / Application	Action			
= any	any	any	forward	ľ	Ō	

Figure 214: CL2-PBR-Full-Tunnel-edit-rule

Step 8 In the EDIT RULE table, enter the following values, then click OK.

- Source: Any
- Destination: Any
- Service/App: Any
- Action: Forward to Cluster

\leftarrow	Edit Rule	
Sour	ce	
Any		~
Dest	ination	
Any		~
Serv	ice/App	
Any		~
Actio	on	
Forv	vard to Cluster	~

Figure 215: CL2-PBR-Full-Tunnel-edit-rule-Forward-to-cluster

Step 9 The edited rule with action "forward_to_cluster" displays in the *EXAMPLE-PBR-FULL-TUNNEL* policy.

Policy-based routing								
EXAMPLE-PBR-FULL-TUNNEL - Rules (1)								
Source	Destination	Service / Application	Action					
= any	any	any	forward_to_cluster					

Figure 216: CL2-PBR-Full-Tunnel-rule-Forward-to-cluster

Step 10 Click Save.

Apply PBR Policy for Full-Tunnel to User Role

Step 1 Go to the group UI-MICRO-AP-01 > Devices page. In the Security tile, select Policies & Access Control.

Step 2 Expand the Roles section.

Step 3 Select the user role to which to apply the PBR policy.

Step 4 In the **Rules** window, click + (plus sign).

← Policies & Access Contr Roles, Aliases, Denylisting, Cus	ol tom blocked URL, Intra VLA	N allowlist, Firewall Settings	
~ Roles			
Roles (4)	+	RULES (1)	+ 💬
Role		Access Rules For Selected Roles	_
EXAMPLE-CL2		 Allow any to all destinations 	
default_wired_port_profile			

Figure 217: CL2-PBR-assign-role

Step 5 In the ADD RULE window, enter the following values, then click OK.

- Rule Type: Policy-Based Routing
- Add Existing Policy:

ADD RULE

• **Policy Name:** *EXAMPLE-PBR-FULL-TUNNEL*

Rule Type	~	Add existing policy	Add a new policy
Poincy-based Routing		Policy name EXAMPLE-PBR-FULL-TUNNEL V	
			CANCEL

Figure 218: CL2-PBR-Full-Tunnel-assign-user-role

Step 6 The PBR policy configured for full-tunnel is assigned to the user role.

÷	Policies & Access Control Roles, Aliases, Denylisting, Custo	I om blocked URL, Intra	a VLAN	allowlist, Firewall Settings	
~ Re	oles				
	Roles (4)	+ 💬	RU	JLES (2)	+ 😳
	Role		Acc	ess Rules For Selected Roles	
	EXAMPLE-CL2			→ Policy-Based Routing EXAMPLE-PBR-FULL-TUNNEL	
	default_wired_port_profile		=	Allow any to all destinations	

Figure 219: CL2-PBR-Full-Tunnel-assign-user-role-list

Step 7 Click Save.

NOTE:
When a user is assigned a user role and the user traffic flows, all the access rules for the user
role are applied first and if there is a PERMIT, the PBR policy is then applied to that specific user
traffic.

Assign a Microbranch AP to a Group

Step 1 In the left navigation pane, click Global, then select the Groups column heading.

Step 2 Expand the Unprovisioned devices group by clicking the expansion icon (>) next to its name.

Step 3 Select the Microbranch AP.

Step 4 Click the Move Devices icon.

Step 5 In the Destination Group dropdown, select UI-Micro-AP01.

Step 6 Click Move.





Assign a Microbranch AP to a Site

The following procedure assigns the APs to a site.

Step 1 Go to Organization and select Site.

Step 2 Select Unassigned devices.

Step 3 Select the Microbranch AP on the right side, then drag the AP to the **ESP-MB01** site.

Central			Q Search or ask Ar					۹ ಿ 🕈
@ Global	Network Structure	Platform Integration						
- Manage	Drag And Drop D To Select Multiple	vices To Add To A Site Devices Shift+Click Or Ctrl+Click						
Devices	Convert Labels	o Sites						
Clients	▽ Site Name	∀Address	Device Count	r	∀Name	∀ Group	∀туре	
a Guests	All Devices		111		RSVCP-AC3-AP133	UI-WIRELESS	IAP	
Applications	Unassigned		31		AP-WDSM02-01	BR-WDSM02	IAP	
Security	BHAM-01	1030 Lakeway Dr	2		RSVCP-AC4-AP10	CP-RSVWLAN	IAP	
C security	BR-SAC01	3535 Elverta Rd	2		RSVCP-AC2-AP9	CP-RSVWLAN	IAP	
8 Network Services	DSM-DC-01	4090 Westown Pkwy	0		BR-IACITY02-AP01	BR-IACITY02	IAP	
- Analyze	ESP-MB01	4199 Campus Dr	0		BR-IACITY02-AH01	BR-IACITY02	IAP	
Alerts & Events	ESP-RS01	8501 foothills blvd	6		GW-WDSM03-BR02-01	BR-WDSM03	Gateway	
🖾 Audit Trail	ESP-RS02	6280 America Center Dr, CA	2		GW-WDSM03-BR02-02	BR-WDSM03	Gateway	
🖏 Tools	ESP-RS03	27816 Jones Rd	2		RS01-AP01	UI-AP-BR01	IAP	
Reports	ESP-VPNC-DC01	3333 Scott Blvd	2	-	RSVCP-AC2-AP14	CP-RSVWLAN	IAP	
- Launch	IACITY01	21 N Clinton	4		RSVCP-AC2-AP1	CP-RSV/WLAN	IAP	
App Catalog	IACITY02	1660 Sycamore St	6		RS01-AP02	UI-AP-BR01	IAP	
— Maintain —	ME01	12 Main St.	1		20:4c:03:32:ad:b4	UI-MICRO-AP-01	IAP	
Ø Firmware	RSVCP	8000 Foothills BLVD	42		AP-WDSM03-04	BR-WDSM03	IAP	
b Organization	SJC01	503 W. Capitol Expy	5		RSVCP-AC2-AP6	CP-RSVWLAN	IAP	
	WDSM01	925 Jordan Creek Pkwy	2		RSVCP-AC1-AP15	CP-RSVWLAN	IAP	
	WDSM02	360 Bridgewood Dr	1		BR-IACITY01-AP01	BR-IACITY01	IAP	
	WHE01	100 N. Milwaukee	4		AP-WDSM03-03	BR-WDSM03	IAP	
					BR-IACITY01-AP02	BR-IACITY01	IAP	
	New Site			16 Sites				111 Device(s)

Monitor Microbranch Site Tunnels

The tunnels for the Microbranch sites can be monitored under SD-WAN overlay tab in a map view along with the tunnel details.

Step 1 Go to Global > Network Services > SD-WAN Overlay.

Step 2 Select Tunnel.

Step 3 Under Overlay Tunnel Orchestrator Topology, click Spokes tab.

Step 4 Under the Spokes Groups, select the Microbranch group where the Microbranch AP resides.

Step 5 In the search filed, select a Microbranch site (for which the tunnel details need to be viewed)

- 1. Hover over the Microbranch site pin location and view the name, total number of tunnels and their status.
- 2. Hover over the DC pin location(s) to view the headend VPNC(s) and their status.
- 3. Hover over the tunnel links between the AP and DC, and view their tunnel status.

NOTE:

The number next to the DC pin represents the data center preferences. For example: Number "1" represent primary data center cluster, "2" represents secondary data center cluster and so on.

HPE GreenLake										00
Central	٩	Search or ask Aruba					c	2		¢ 0 2
Customer	E Network Health	Q WAN Health	Summary	ِ Wi-Fi Cor	nectivity	Q Al Insights				th Summary
🕸 Global 💦		in a ricalar	Samary		incentry	, insights				
- Manage									NO ISSUES OPC	ITENTIAL ISSUES
					Nui	mber of devi	ces		W	AN
	∑ Site Name	Al Insights	Status	High Mem Usage	High CPU Usage	High CH utilization	Clients	High Noise	Uplinks Status	Tunnels Status
但 Devices	and the second	HIGH MEDIUM LOW	UP DOWN			2.4 GHz 5 GHz	CONNECTED FAILED	2.4 GHz 5 GHz	ISSUES DOWN	ISSUES DOWN
Clients	1+ 34 4	· · · · ·					iowa -	Detr	oit	uffaló
😩 Guests	- 1. 15	Salt Lake	City	(One	NE	BR.	Davenport'	Toled	Akron	
Applications	Reno	NEV.		Denver		Inited States	ALL.	IND.	OHIO 2	Harrisburg N.J.
Security	cramento	. UTA		COLO.		KANS.	Kansas City St Louis	Cincinna	w.va.	DEL
🗞 Network Services	2 CALIF		1 : -				·	KY.		
— Analyze ————	Bakersfield	Las Vegas		Santa Fe		Tulsa OKLA:	Memphis	TENN.	N.C.	Virginia Be
Alerts & Events	Los Ang	eles	1Z.	й.м.	Lubbock	0	ABK.		lanta s c	
🗷 Audit Trail		T	ucson		- CODUCK	. • Pallas	MISS.	ALĂ.	3 4 4 3	
🖏 Tools		Ensenada	Ciud	ad Juárez		TEXAS	LA. Mob	ilo		
🛍 Reports			SON.		~~~.	Houston	New Orleans		Jacksonville	

Figure 221: sdwanoverlay-tunnel-status

In CL2, the Microbranch AP establishes tunnels to all VPNCs in primary cluster as well to VPNCs in secondary cluster. In below screenshots, there are total of three IPSec tunnels established from Microbranch AP:

- Two tunnels established to the two VPNCs in primary DC.
- One tunnel established to the one VPNC in secondary DC.

HPE GreenLake						88
orubo Central	Q Sea	rch or ask Aruba			Q	4 @ &
Customer:	() SD-WAN OVERLAY	لم IP Address Manager	လ္က Virtual Gateways	ු Cloud Connect		3 hours List Config
🕸 Global 🛛 🔅	Tunnel Route	U	,			
— Manage ————			0.67			
🗄 Overview	OVERLAY TUNNEL OF	RCHESTRATOR TOPOL	.UGY	Rey-Rodriguez	×	Map Grid
Devices	Hubs	Spokes	+	Vancouver	Winnipeg 👾	ONTARIO
🗔 Clients	Spoke Groups		-	WASH MONTANA	N.D.	Quebech
ஃ. Guests	✓ Spoke Group AOS10 EC MB AP Group 1 branch	1=	6 C	Salem ORE. IDAHO * WYO.	SZD.	WIS. MICH Toronto VT
Applications	Dennis Home Office Gro 1 branch	up			I NEBR. IOWA C	Detroit N.Y. MASS
Security	EC Microbranch AP 1 branch			NEV.	United States	ILL. IND. OHIO
쁂 Network Services	MB AP group-test 0 branches			Rey-Rodriguez	OKLA.	TEN NA
— Analyze —	default 1 branch			Los Angeles ARIZ. N.M.	ARK.	S.C.
🗘 Alerts & Events				B.C.	TEXAS	Jacksonville
🛛 Audit Trail				SON. CHIH.	COA.	FLA.
🖏 Tools				BIC.S.	Mexico TAM	ulf of Bahamas exico
🛍 Reports				NA	Y. S.L.P.	Cuba

Figure 222: sdwanoverlay-tunnels-both-DC-clusters

Rey-Rodriguez-MB-AP# show crypto ipsec stats											
IPSEC STATS											
MAP NAME		IP ADDR	DEVNAME	TX/RX PACKETS	TX/RX BYTES	TX/RX DROPS	TX/RX ERRORS				
gw-ipsecmap-20:4c:	-uplink-eth0	10	tun0	449252/448863	49131332/49090320	0/0	0/0				
gw-ipsecmap-20:4c:	-uplink-eth0	10	tunl	431001/430611	47135200/47093554	0/0	0/0				
gw-ipsecmap-02:1a:	-uplink-eth0	10	tun2	449725/449317	49183020/49140660	0/0	0/0				

Figure 223: image-20230920144053194

More details about the tunnels such as tunnel endpoints, public IP, private IP, SPI, next rekey, tunnel event logs, etc. can also be viewed.

Step 1 Click the tunnel link between the Microbranch AP and the DC

Step 2 In the pop-up window, expand each row to view individual tunnel details

HPE GreenLake					00
Central	Q Search or ask Aruba			Q	¢ ∅ ≗
Customer:	③ 端 SD-WAN OVERIAY IP Address Manager	<u>ه</u> Virtual Gateways	ے Cloud Connect		-O 3 hours List Config
🗟 Global 📀	Tunnel Route	in taal datemays			
- Manage	OVERLAY TUNNEL ORCHESTRATOR TOPO	LOGY	Q Rev-Rodriguez	×	Map Grid
B Overview	the hard sectors		Regina		7 1 1
Devices	Spoke Groups	+	Vancouver	Winnipeg	ONTARIO
🗖 Clients		6	MONTANA	N.D.	Quebecry N
😤 Guests	AOS10 EC MB AP Group 1 branch	C	ORE. IDAHO 4 WYO.	sto. w	IS. MICH Toronto VT
Applications	Dennis Home Office Group 1 branch			NEBR. IOWA Chi	Cago PA.
Security	EC Microbranch AP 1 branch		COLO.	United States	ILL. IND. OHIO
🞖 Network Services	MB AP group-test 0 branches		(Rey-Rodriguez)	OKLA.	
– Analyze –	default 1 branch		Los Angeles ARIZ. N.M.	ARK.	S.C.
🏚 Alerts & Events			B.C. SON.	Houston	Jacksonville
🗷 Audit Trail			CI	0A.	
🖏 Tools			BIC.S. SIN. Mex	tico TAM	xico Havana
🛍 Reports			NAY.	S.L.P.	Cuba

Figure 224: sdwanoverlay-tunnel-details

The **control channel state** for the Microbranch AP can also be viewed by selecting the control connection as below:

Step 1 Go to Global > Network Services > SD-WAN Overlay > Tunnel > Spokes

Step 2 Under the Spokes Groups, select the Microbranch group where the Microbranch AP resides.

Step 3 In the search filed, select a **Microbanch site** (for which the control channel state need to be viewed)

Step 4 Scroll to the bottom and select Control Connections

Step 5 Expand the row to view more details

HI Global GreenLake							00
Central	Q Sea	arch or ask Aruba			۹		¢ 0 2
Customer:	(§) SD-WAN OVERLAY	ំំំ IP Address Manager	্ঞ Virtual Gateways	ු Cloud Connect		3 hours	List Config
🗟 Global 🧹 🖓	Tunnel Route	0	,				
— Manage ————							
🗄 Overview	OVERLAY TUNNEL C	RCHESTRATOR TOPO	LOGY	Q		Мар	Grid
Devices	Hubs	Spokes	+	Vançouver	- Regina Winnipeg	I ONTARIO	OUEBEC ST
🗖 Clients	Spoke Groups		-	WASH - MO	ONTANA N.D.	t.	Quebech
🙁 Guests	Y Spoke Group AOS10 EC MB AP Group	p 1≕	ି C	Salem	A SCD.	WIS. MICH	MAINEL
Applications	Dennis Home Office Gr	oup			WYO. COD 2 NEBR. IOV	Madison Detroit	N.Y. MASS
Security	EC Microbranch AP 1 branch			NEV.	United States	ILL. IND. OHIO	New York
쁂 Network Services	MB AP group-test 0 branches			CALIF: Las Vegas	OKLA.	TEN NO	
— Analyze ————	default 1 branch			Los Angeles ARIZ	N.M.	NRK. S.C.	
🏚 Alerts & Events				8.0	Ciudad Juárez TEXAS Houston	LA Jacksonville	
🗷 Audit Trail					UN. CHIH. COA.	SLA.	
🖏 Tools					SIN Mexico TAM	Gulf of Mexico	ahamas
🗈 Reports					NAY. S.L.P.	Good 🔽 Fair 🔽 Poor	🗌 Name

Figure 225: sdwanoverlay-tunnel-control-connection

Monitor Microbranch Site Routes

For each Microbranch site, the routes learnt from the Microbranch AP and the routes advertised to the Microbranch AP can be monitored in SD-WAN overlay tab as below.

Step 1 Go to Global > Network Services > SD-WAN Overlay.

Step 2 Select Routes.

Step 3 Under Overlay Tunnel Orchestrator Topology, click Spokes tab.

Step 4 Under the **Spokes Groups**, select the **Microbranch group** where the Microbranch AP resides.

Step 5 In the search filed, select a Microbranch site (for which the route details need to be viewed).

Step 6 Scroll to the bottom to view control connections details for the Microbranch AP in the above selected site.

Step 7 Under **Routes Learned** column, the number denotes the number of routes learned from this Microbranch AP.

1. Click on the number to view the actual routes learned from the Microbranch AP.

Step 8 Under **Routes Advertised** column, the number denotes the number of routes advertised to this Microbranch AP (and eventually stored in the route table).

1. Click on the number to view the actual routes advertised to the Microbranch AP.

HI Global										80
Central	٩	Search or ask Aruba						۹ ۱	New Central 🔵	¢
Customer: Pragadesh	🕒 Network Health	Q WAN Health) Summary	Wi-Fi Co	ି nnectivity	Q Al Insights				tl₁ : Summary List
🗟 Global 🆕 📀			,		,	Ū				
- Manage									NO ISSUES	TENTIAL ISSUES
					Nu	mber of devi	ces		W/	AN .
🔠 Overview	▽ Site Name	Al Insights	Status	High Mem	High CPU	High CH utilization	Clients	High Noise	Uplinks Status	Tunnels Status
Devices	'	HIGH MEDIUM LOW	UP DOWN	Üsage	Üsage	2.4 GHz 5 GHz	CONNECTED FAILED	2.4 GHz 5 GHz	NO ISSUES DOWN	NO ISSUES DOWN
🗔 Clients	+ 15 4	A				X.Y.	Madison	Detr	oit	Buffalo, N.Y. Alb
😩 Guests	-1. 75	Salt Lake	City 1	Č O ne	N E	BR.	TOWA Davenport	Toledo	Akron	AL
Applications	Reno	NEV.		Denver		United States	int.	IND.	OHIO 2	Harrisburg N.J.
Security	ramento	1999 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	"V			KANS.	Kansas City Ste Louis	2 in the	w.va.	DEL
🗞 Network Services	2 CALIF	Las Vegas	7. 1. 1. 1. 1.			Tulsă	in in	KY.		Virginia B
— Analyze ————	Bakersfield	W. L. W. L. W.		Santa Fe		OKLA:	Memoh	TENN.	N.C.	
🇘 Alerts & Events	Los Ange	les AR	iz.	й.м.	Lubbock	O	ARK.	At	anta s.c.	a feat
🛛 Audit Trail		T	ucson		÷.	Dallas	MISS.	ALA. 4	A	
🖏 Tools		B.C.	Ciud	ad Juarez			HALL M	obile	Jacksonville	
🗊 Reports			SON.	1	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	Houston	New Orleans			

Figure 226: sdwanoverlay-routes

The Microbranch uplink statistics such as WAN status, type, availability, usage, throughput, utilization, etc. can be viewed under **Global > Overview > WAN Health > List > Transport**

E	<u>_</u>		Q							th 📒
Transport Ste										
WAN Interfaces (3)										₹ ⊙
▼ Name	▼ Site	🍸 Status 🖌	🍸 Transport 🐱	▼ Carrier	∀ туре ∨	🖓 Availability 👻 🚛	Usage	Throughput	♥ Utilization ♥	▼ Loss
branch1-gw1 Branch Gateway	Branch-1	• Up	Internet	outside_inet 100.8.180.46	Primary	• 100%	1.1 GB 48.2 MB	852.6 Kbps 36.5 Kbps	• 4.3%	• 0.2%
Lab10_Microbranch_2 Microbranch	Microbranch-2	• Up	Internet	eth0 69.141.118.41	Primary	• 100%	226.2 MB	171.5 Kbps 196.9 Kbps		• 0%
wadlab_seel_gw Branch Gateway	Datacenter-2	• Up	Internet	fios_inet 100.8.180.46	Primary	• 100%	↓ 19.3 MB	14.6 Kbps 6.9 Kbps	• 0%	• 0.3%
	Retwork Health WW Transport Site WAN Interfaces G V Name branch1ger branch1ger Lab10, Microbranch, 2 Microbranch Washab set gw Branch Labes	Retwork Health WAN Health Transport Site WAN Interfaces (3) ▼ Name ▼ Site Interfaces 9 Site Interfaces Branch 1 Intel State Microbranch 2 Microbranch 2 Microbranch 2 Mach Genery Datacenter 2	Retwork Health WNH Health Summary WiFFI Conn Transport Site Site V VNAN Interfaces (3) V Site V VNAM V Site V Site V Vanch 1 get based Sensory Branch 1 * Up Up L Lablo Microbranch 2 Microbranch 2 • Up Up L Maded Genergy Datacenter 2 • Up Up L	WAN Health Wan Health WiFFI Connectivity Al Insights Transport Site WiFFI Connectivity Al Insights WAN Interfaces (3) Transport Y V Name V Site V Status v V Transport v Internet Branch-1 % Up Internet Labito Microbranch-2 Microbranch-2 Up Internet Machtorstein Datacenter-2 Up Internet	Retwork Health WAN Health Summary Parage Parage	Retwork Health VI #7 Connectivity VI #7 Conne	Retwork Health Retwork	Retwork Health View Nealth View Nealth	WAN Health Vit #I Connectivity <	Verter for the set of

Figure 227: Microbranch-WAN-Health
Validated Hardware

The following hardware and software versions were validated for this guide. For compatibility, please upgrade to the versions listed below (or higher).

Wireless Gateways

Product Name	Software Version
Aruba 7240XM	10.4
Aruba 9240	10.4
Aruba 9012	10.4
Aruba 9004	10.4

Wireless Access Points

Product Name	Software Version
Aruba AP 500 Series	10.4
Aruba AP 300 Series	10.4

Wired Access

Product Name	Software Version
Aruba CX 6400	10.10.0002
Aruba CX 6300	10.10.0002
Aruba CX 6200	10.10.0002
Aruba 3810	16.11.0005
Aruba 2930M/F	16.11.0005

Management and Orchestration

Product name	Software version
Aruba Central	2.5.6
Aruba ClearPass Policy Manager	6.9.11

Verifying Aruba SD-Branch Hub Spoke Topology

This section explains how to verify the SD-Branch topology.

Verify SD-WAN Tunnels

Check the VPNCs first because they manage the aggregation of all branch gateway tunnels.

To verify that the tunnels are up, navigate to the **UI-VPNC-SD-WAN** and select one of the VPNCs. Select **WAN** from the left navigation pane to view and verify that all tunnels are up.

Repeat this step for the second VPNC.

Verify that the following is displayed:

- Status is Up.
- Availability is trending upward or 100%.

← @ 7210-DC1-VPNC-1 ⊘	<u>₹</u> Tunnels		S 3 hours
- Manage			Actions 👻
BB Overview			
😞 WAN	TUNNELS SUMMARY		
	TOTAL UP	DOWN PEER	S ORCHESTRATED
놂 LAN	13 13	0 8	13
Device			
The Clients	Tunnels (13)		\odot
Lu chenes	Y Name IE Y Status ✓ Mode	 Source Destination 	Loss Latency Availability
Applications	> 7210-dc1-vpnc-1:inet_inet::20:4c:03:32:ad:b4:uplink-eth0 • Up ORCH		100%
Security	> 7210-dc1-vpnc-1:inet_inet::rs01-9004-1:inet_inet • Up ORCH		100%
- Analyze	7210-dc1-vpnc-1:inet_inet::rs01-9004-2:inet_inet • Up ORCH		100%
A Alerte & Events	> 7210-dc1-vpnc-1:inet_inet::rs02-9004-1:inet_inet • Up ORCH		100%
LI Alerts & Events	> 7210-dc1-vpnc-1:inet_inet::rs02-9004-2:inet_inet • Up ORCH		100%
🗷 Audit Trail	> 7210-dc1-vpnc-1:inet_inet::rs03-7004-1:inet_inet • Up ORCH		100%
🖏 Tools	> 7210-dc1-vpnc-1:inet_inet:rs03-7004-2:inet_inet • Up ORCH		100%
	7210-dc1-vpnc-1:mpls_mpls::rs01-9004-1:mpls_mpls • Up ORCH	172.17.1.26 172.17.1.14	100%
Reports	> 7210-dc1-vpnc-1:mpls_mpls::rs01-9004-2:mpls_mpls • Up ORCH	172.17.1.26 172.17.1.34	100%
- Maintain	> 7210-dc1-vpnc-1:mpls_mpls::rs02-9004-1:mpls_mpls • Up ORCH	172.17.1.26 172.17.1.2	100%
Firmware	7210-dc1-vpnc-1:mpls_mpls::rs02-9004-2:mpls_mpls • Up ORCH	172.17.1.26 172.17.1.6	100%
	7210-dc1-vpnc-1:mpls_mpls::rs03-7004-1:mpls_mpls • Up ORCH	172.17.1.26 172.17.1.18	100%
	7210-dc1-vpnc-1:mpls_mpls::rs03-7004-2:mpls_mpls • Up ORCH	172.17.1.26 172.17.1.38	100%



Click **Tools** on the left menu. Select the **Console** tab, log into the console, and use the **show crypto ipsec sa** option to see the tunnel type

Verify that the following is displayed:

- Tunnel Type is Hubandspoke.
- Flags display UTlt.

🛱 UI-VPNC-SD-WAN 🔿	ස් Network Check Device Check Comm	ands Console					
- Manage							
BB Overview	REMOTE CONSOLE						
Devices	E Console session for the device: 7210	-DC1-VPNC-1					No Session Found ▼ Q (i) C
🗖 Clients	admin@7210-DC1-VPNC-1 [11:20:33 AM] 🖌 ×	+					-
🚉 Guests	Initiator IP	Responder IP	SPI(IN/OUT)	Flags	Start Time	Tunnel Type	Inner IP
Applications			e7d04000/dbd5e800	UTlt	Feb 10 22:29:45	HubAndSpoke	10.14.254.1
Security	172.17.1.2	172.17.1.26	fb90c800/ab978800	UTlt	Feb 11 10:46:02	HubAndSpoke	
- Analyze	172.17.1.34	172.17.1.26	44e29600/27c1a600	UTlt	Feb 11 10:18:08	HubAndSpoke	
	172.17.1.18	172.17.1.26	cc725600/a8a17e00	UTlt	Feb 11 10:18:08	HubAndSpoke	
🗹 Audit Trail			6cd96e00/72320e00	UT1t	Feb 10 21:04:20	HubAndSpoke	
🔦 Tools	172.17.1.14	172.17.1.26	ae448b00/8ee8fb00	UTIt	Feb 11 10:18:04	HubAndSpoke	
鼠 Reports			a/8/1600/3481d600	UTIt	Feb 10 21:04:14	HubAndSpoke	
- Maintain	172.17.1.38	172.17.1.26	ef04700 /26f4ef00	UTlt	Feb 11 10:18:04	HubAndSpoke	
Ø Firmware			c1d5400 /c98ab400	UTlt	Feb 10 21:04:22	HubAndSpoke	
			4a364c00/5d258400	UTlt	Feb 10 21:04:12	HubAndSpoke	
	172.17.1.6	172.17.1.26	c92f0600/31ef6e00	UTlt	Feb 11 10:18:06	HubAndSpoke	
			3ef19000/a9bf8000	UT1t	Feb 10 21:04:14	HubAndSpoke	
	<pre>Flags: T = Tunnel Mode; E = Trar L = L2TP Tunnel; N = Nort l = uplink load-balance;</pre>	nsport Mode; U = UDP Encap 2el Client; C = Client; 2 = IKEv2 t = Tunnel Service; F = Reverse-Pinning Enabled					
	[2022 Feb 11 11:20:34 AM] Ssh session started						^

Figure 229: Tunnel Security association

Go to **UI-BGW-01** and select one of the Branch Gateways. Select **WAN**, then select the **Tunnels** tab.

Verify that the following is displayed:

- Status is Up
- Availability is trending upward or 100%

Central					Q Search or as	k Aruba					۹ <u>ل</u>	o 🏨 🖁
← @ RS01-9004-2 ⊘	Summary Tunnels	Path Steerin	ng									3 hours
Manage											Actions 👻	• Go Live
B Overview												
🖕 wan	TUNNELS SUMMARY											
R LAN	TOT	AL			UP		DOWN		PEERS	ORC	HESTRATED	
55 LAN	4				4		0		4		4	
Device												
□ Clients	Tunnels (4)											\odot
	▼ Name	18.	▼ Status	~	▼ Mode	~	Source	Destination	Loss	Latency	Availability	
Applications	> rs01-9004-2:inet_inet::7	210-dc1-vpnc	• Up		ORCH		172.20.1.35		0%	0.35ms	100%	
Security	> rs01-9004-2:inet_inet::7	210-dc1-vpnc	• Up		ORCH		172.20.1.35		0%	0.35ms	100%	
- Analyze	> rs01-9004-2:mpls_mpls	::7210-dc1-vpn	• Up		ORCH		172.17.1.34	172.17.1.26	0%	0.34ms	100%	
Alerts & Events	> rs01-9004-2:mpls_mpls	::7210-dc1-vpn	• Up		ORCH		172.17.1.34	172.17.1.22	0%	0.33ms	100%	
🛛 Audit Trail												
🖏 Tools												



Verify Routes

Select the **UI-VPNC-SD-WAN** group. Select one of the Branch gateways. On the **Overview** page, select the **Routing** tab.

Select **Overlay**, then change the overlay details to **Routes learned**.

Verify that summarized routes are learned using the overlay.

Ensure the following is displayed:

• Summary routes from each branch

• Availability is trending upward or 100%.

orubo Central			C	Search or ask Aruba					Q	۵ 🛛	ه ا
업 UI-VPNC-SD-WAN 이	🙊 Gateways								il. Summary	i List	Config
- Manage	Gateways Online	0 Offline	Clusters								
BB Overview	2 2	0	1								
Devices	Gateways (2)									. ↓ .	\odot
Clients	V Device Name	Y Model	Y IP Address	Y MAC Address	▼ Serial	Firmware Version	Y Group	▼ Site	Uptime		-
a. Guests	• 7210-DC1-VPNC-1	A7210	10.0.6.111	00:1a:1e:05:01:28	CV0016872	10.3.0.0_82463	UI-VPNC-SD-WAN-01	ESP-VPNC-DC01	52 days 5 hours 5	i6 minutes	
Applications	• 7210-DC1-VPNC-2	A7210	10.0.6.112	00:1a:1e:05:01:a0	CV0016870	10.3.0.0_82463	UI-VPNC-SD-WAN-01	ESP-VPNC-DC01	51 days 1 hour 37	' minutes	
Security											
- Analyze											
☆ Alerts & Events											
Audit Trail											
🖏 Tools											
Reports											
- Maintain											
Firmware											
			*								



Select the **UI-BGW-01** group. Select one of the Branch Gateways. On the **Overview** page, select the **Routing** tab.

Select **Overlay** and change the overlay details to **Routes learned**. Verify that routes are learned via using overlay.

Ensure the following is displayed:

• A summary route for the campus network is learned via the **Overlay**.

Central			C	Search or ask Aruba					ዳ ሳወ 👪 🖁
ជ UI-BGW-01 🛛	چ Gateways								ili ∷≣ 😂 Summary List Config
Manage	Gateways • Online	• Offline C	usters						
BB Overview	6 6	0	3						
Devices	Gateways (6)								₹ 💬
🗈 Clients	▼ Device Name	▼ Model	Y IP Address	Y MAC Address	Y Serial	Firmware Version	Y Group	▼ Site	Uptime
🚨 Guests	• RS01-9004-1	A9004	10.14.255.1	20:4c:03:b7:ae:7a	CNLCKLB055	10.3.0.0-beta_81639	UI-BGW-01	ESP-RS01	106 days 23 hours 27 minutes
Applications	• RS01-9004-2	A9004	10.14.255.2	20:4c:03:b7:ac:f2	CNLCKLB03Y	10.3.0.0-beta_81639	UI-BGW-01	ESP-RS01	90 days 21 hours 8 minutes
M Appleadors	• RS02-9004-1	A9004	10.14.255.3	20:4c:03:b5:98:52	TWJTKLB05L	10.3.0.0-beta_81639	UI-BGW-01	ESP-RS02	73 days 22 hours 18 minutes
Security	• RS02-9004-2	A9004	10.14.255.4	20:4c:03:b5:91:12	TWJSKLB0Q9	10.3.0.0-beta_81639	UI-BGW-01	ESP-RS02	73 days 22 hours 10 minutes
- Analyze	 RS03-7004-1 	A7005	10.14.255.5	20:4c:03:2f:f7:dc	CP0044595	10.3.0.0-beta_81639	UI-BGW-01	ESP-RS03	6 days 22 hours 23 minutes
	* RS03-7004-2	A7005	10.14.255.6	20:4c:03:2f:f4:2c	CP0044594	10.3.0.0-beta_81639	UI-BGW-01	ESP-RS03	6 days 20 hours 12 minutes
Audit Trail Audit Trail Reports Maintain Firmware		k							



Verify NTP

Verify the NTP configuration using the **show ntp status** command.

Verify that the following is displayed:

- The NTP status is enabled.
- The NTP server connections are in the default VRF.
- The reference time is correct for the timezone

These values indicate the NTP service is reachable by the switch.





Verify DHCP Snooping

Verify the DHCP Snooping and ARP inspection configurations using the **show dhcpv4-snooping statis-tics**, **show dhcpv4-snooping binding**, and **show arp inspection statistics vlan** commands.

Verify that the following is displayed:

- Packet-Type: server, Action is forward.
- Packet-Type: client, Action is forward.

The non-zero values indicate that DHCP snooping is actively forwarding traffic from servers and clients.

🛱 🕮 TG-SW-BG01 💦	R Device Check	Commands Console	
Manage	Device Type	 Consider V 	
BB Overview			
Devices	REMOTE CONSOLE		
Clients	i	vice: RS01-SW01	
🚉 Guests	admin@RS01-SW01 [09:15:45 PM] / RS01-SW01#	× +	
Applications	RS01-SW01# RS01-SW01# RS01-SW01#		
Analyze	RS01-SW01# RS01-SW01#		
Alerts & Events	RS01-SW01# show dhcpv4-sn Packet-Type Action Re	nooping statistics eason	Count
🗷 Audit Trail	server forward fr	rom trusted port	58852 94477
🔦 Tools	server drop re server drop un	eceived on untrusted port nauthorized server	0
Reports	client drop de client drop un client drop ba	ntrusted option 82 field ad DHCP release request	0
Maintain Firmware	client drop fa client drop fa	ailed verify MAC check ailed on max-binding limi	0 t 0
() THINWARE	RS01-SW01# show dhcpv4-sn	nooping binding	
	MacAddress IP 	VLAN Inter 14.1.10 101 1/1/3	face Time-Left
	RS01-SW01# show arp inspe	ection statistics vlan 10	
	VLAN Name	Forwarded Drop	 ped
	101 EMPLOYEE	113558 2	
	RS01-SW01# [] [2022 Feb 25 09:15:48 PM] Ssh session s	started	

Figure 234: Verifying DHCP-Snooping

Verify Radius

Verify the RADIUS configuration using the **show radius-server** command.

Ensure the following is displayed:

- Both servers are reachable, without a "*" before their name.
- The VRF is set to *default*.

These values indicate that the RADIUS servers are reachable in the correct VRF.



Figure 235: Verify Radius Connectivity

Verify Device Profile and Radius Authentication

Verify the device profile configuration using the **show port-access clients** and **show port-access device-profile all** commands.

Verify that the following is displayed:

- Radius Onboarding displays Success.
- The Authorization Details are applied.
- The VLAN is displayed.
- The device-profile onboarding method is a Success.
- The profile name and LLDP group state are applied

These values indicate the device profiles are applied and devices are onboarded.



Figure 236: verifying Device profiles and Radius Authentication

💢 📼 TG-SW-BG01 🛛 🔅	Network Check Device Check Commands	Console
	Device Type	~
Manage		
88 Overview		
Devices		
E Devices	REMOTE CONSOLE	
Clients	= Console session for the device: BS01-SW01	
8 Gueste		
a, duests	admin@RS01-SW01[09:15:45 PM] × +	
Applications		
Cocurity	Role : RADIUS_161250981 Status : Applied	
Security		
- Analyze	Role Information:	
▲ Alerts & Events	Name + PADTUS 161250981	
	Type : radius	
Audit Trail	Reauthentication Period	
🔦 Tools	Cached Reauthentication Period	
	Authentication Mode Session Timeout	
Reports	Client Inactivity Timeout	
- Maintain	Gateway Zone	
C Eirmwara	UBT Gateway Role UBT Gateway Clearpass Role	
e rinnware	Access VLAN	
	Native VLAN Allowed Trunk VLANs	
	Access VLAN Name	: EMPLOYE
	Allowed Trunk VLAN Names	
	VLAN Group Name	
	QOS Trust Mode	
	STP Administrative Edge Port	
	PVLAN Port Type	
	Captive Portal Profile Policy	
	[2022 Feb 25 09:15:48 PM] Ssh session started	



© Copyright 2021 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. Aruba Networks and the Aruba logo are registered trademarks of Aruba Networks, Inc. Third-party trademarks mentioned are the property of their respective owners. To view the end-user software agreement, go to: www.arubanetworks.com/assets/legal/EULA.pdf



www.arubanetworks.com

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

See Confluence for Correct Doc Title