ARUBA VALIDATED DESIGN



ARUBA SD-BRANCH

Design & Deployment Guide

August 2020

Table of Contents

Document Conventions	1
Introduction	2
Purpose of This Guide	2
Customer Use Cases	4
SD-Branch Design	5
SD-Branch Architecture	9
Aruba SD-WAN	.19
Aruba SD-LAN	.34
SD-Branch Components	. 38
Deploying the SD-Branch	47
Aruba Central	.48
SD-Branch Network Configuration Overview	.51
Preparing to Deploy the SD-Branch Network	.53
Configuring the VPNC Group	. 59
Configuring the VPNC Devices	.78
Configuring the Branch Gateway Group—One Branch Gateway per Branch	.92
Configuring a Branch Gateway Device—One Branch Gateway per Branch	116
Configuring the Branch Gateway Group for High Availability—Two Branch Gateways Per Branch	123
Configuring a Branch Gateway Device—Two Branch Gateways per Branch	146
Configuring the Branch Switch UI Group	164
Configuring the Device Switch UI Group	171
Configuring the Branch Access Points Group	174
Configuring the WLAN Access Points	184
Summary1	86
What's New in This Version1	87

Document Conventions

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

- the **show stacking** command
- Navigate to Configuration > System > General
- click Save

Italic text indicates the definition of important terminology. Example:

• Spatial streaming is a transmission technique in MIMO wireless communication

Blue text indicates a variable for which you should substitute a value appropriate for your environment. Example:

• stacking member 2 priority 250

Highlighting indicates emphasis. Example:

• ip address 10.4.20.2/22

Note Notes contain asides or tips.

Caution Cautions warn you about circumstances that could cause a failure.

Introduction

Software-defined branch (SD-Branch) is a technology shift towards 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 only addresses 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 besides just WAN connectivity. Branch networks need 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 you are formulating the strategy for your SD-Branch rollout, Aruba recommends that you:

- 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 guide covers the Aruba SD-Branch design, including reference architectures along with their associated hardware and software components. It contains an explanation of the requirements that shaped the design and the benefits it provides 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.

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—SD-Branch devices can be factory-shipped directly to a remote site by automatically matching orders to an Aruba customer account, and a mobile Installer app is available for third-party systems integrators to quickly install equipment. Combined with configuration hierarchy, which assigns APs, switches, and gateways to site-specific configurations, networks are brought up very quickly.
- Unified policy management—For Aruba and third-party network infrastructure, Aruba ClearPass delivers a common policy framework for multivendor wired and wireless networks. This software-defined 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 while recommending changes. When you shift to a cloud-hosted model, data is collected and crowdsourced from Aruba's large installed base while taking advantage of Aruba's 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 offload the branch gateways (BGWs) from participating in the routing decisions. You can also use end-user identity information when selecting the 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 that are tailored to the needs of automation software. The SD-Branch architecture seeks to flatten 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.

You can 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 but rather to present 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 can fill 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 not getting any bigger and often, they are shrinking. Organizations expect new network rollouts to be complete in 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

SD-Branch Design

This guide addresses the most common uses cases of an SD-Branch solution. If you are planning a more complex project that is not covered in this guide, contact an Aruba or partner SE/CSE for design verification. The Aruba SD-Branch design consists of the following elements:

- Aruba Central—Flexible policy, configuration, and monitoring capabilities allow an organization to simplify network operations by providing zero-touch provisioning and customizable templates in order to quickly deploy BGWs, switches, and APs. Aruba Central provides centralized management for historical data reports, monitoring for PCI compliance, and troubleshooting for regional and global locations. It also gives you key insights into WAN health and optimization to help IT determine the best link to send traffic to corporate data centers or to the Internet based on per-user, per-device, or per-application policies.
- Aruba ClearPass—Allows network security policies to be automatically assigned based on user or device role from a central location. This capability ensures that policies are consistent, eliminating the chance of devices having old configurations and minimizing human-introduced errors. The network identifies, authenticates, and grants trust based on the user or device role.
- Aruba headend gateways—The Aruba 7200 Series, virtual gateways, and certain Aruba 7000 Series platforms can act as headend gateways, or *VPN concentrators* (VPNCs), for SD-Branch designs. BGWs establish VPN tunnels to one or more VPNCs over multiple providers networks. High availability options support multiple VPNCs deployed at a single site or deployed in pairs at multiple sites for the highest availability. The VPNC supports active/standby or active/active uplinks from the branch locations.
- Aruba virtual gateways—The virtual gateway simplifies branch network deployments for organizations that are migrating to Infrastructure as a Service (IaaS) providers such as Amazon Web Services and Microsoft Azure. They provide the ability to directly connect a branch to cloud instances, improving access to the resources hosted in a public cloud. The virtual gateway supports resilient connectivity by using multiple transport links and delivers centralized policy management across the branch, data center, and cloud endpoints.
- Aruba branch gateways—The Aruba 9000 Series, 7200 Series, and 7000 Series can operate as BGWs to optimize and control WAN, LAN, and cloud security services. The BGW provides routing, firewall, security, URL filtering, and WAN optimization. With support for multiple WAN connection types, the BGW routes traffic over the most efficient link based on availability, application, user, and link health. This allows organizations to take advantage of high-speed, low-cost broadband links to supplement or replace traditional WAN links such as MPLS.

- Aruba access switches—The Aruba 2930F, 2930M, 3810M, and 5400R family of switches connect wired devices to the branch network, such as APs, workstations, medical devices, multi-function printers, point-of-sale devices, and other devices that don't support Wi-Fi or that do need higher performance than a wireless connection can provide. The access layer also provides PoE to devices such as APs, IP phones, and IP cameras. You can use the switches standalone or in a stacked configuration, depending on the number of ports needed at each location.
- Aruba access points—Aruba AP-5xx models are dual radio 802.11ax Wi-Fi 6 APs and the AP-3xx models are dual radio 802.11ac Wave 2 Wi-Fi 5 APs that support different throughput and client loads. With Aruba's controllerless model called *Instant*, there is no central controller, and the controller functions are distributed among the APs. Instant is typically used in branch sites and scales up to 128 APs per cluster. In this type of design, you normally see less than 50 APs per cluster at each remote site.
- Aruba threat detection—Aruba's role-based Intrusion Detection System and Intrusion Prevention System (IDPS) capabilities are available in the 9000 series gateways. Aruba IDPS allows an organization to set security policies on individual- or role-based access to branch endpoints. It analyzes data packets entering the network and acts quickly to prevent threats in real time. All identified threats are logged for correlation analysis.

You can find a complete list of Aruba Central-supported hardware in the components area at the end of this section.

The following figure shows an example SD-Branch design with a headend site, an IaaS data center, cloud security providers, and several remote locations, each depicting different branch deployment models.

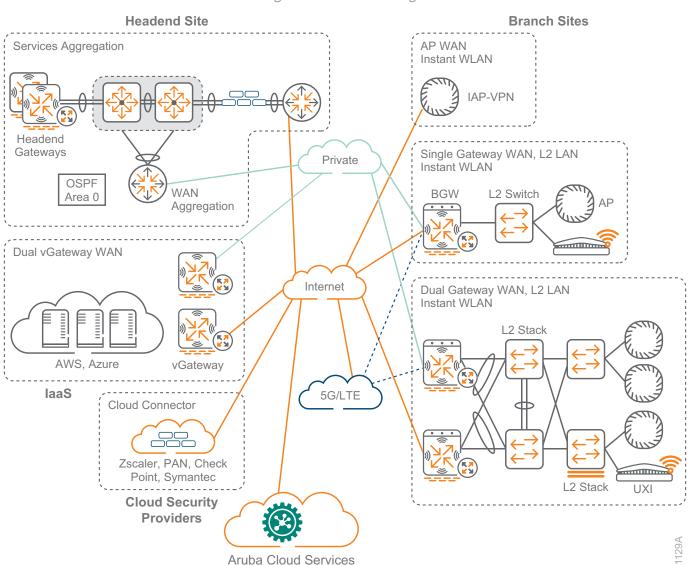


Figure 1 SD-Branch design

The Aruba SD-Branch solution provides network access for employees, wireless Internet access for guests, and connectivity for IoT devices. Regardless of their location on the network, wired and wireless devices have the same experience when connecting to their services.

The Aruba SD-Branch includes the following key features and capabilities:

- **Stateful firewall**—Context-aware, role-based data adapted from Aruba WLAN to dynamically apply policy from RF to WAN Information on user, device, application, and location can enhance visibility and security.
- **Dynamic segmentation**—With centralized policy for WAN, wired, and wireless, IT can extend consistent policies across the entire distributed branch footprint. This provides a simple and secure way to configure network devices and onboard IoT endpoints without additional overhead.
- **Traffic analysis**—Gain rich application awareness into over 3,000 applications across 21 categories. Web Content Classification provides protection from malicious or unauthorized web URLs and includes geolocation filtering and IP reputation.
- **Deep packet inspection (DPI)**—Monitors application usage and performance while optimizing bandwidth, priority, and network paths in real time, including apps that are encrypted or appear as web traffic. DPI is vital to understanding usage patterns that might require changes to network design and capacity.
- **Installer app and zero-touch provisioning**—Simplify on-site deployment with ZTP through cloud-based Aruba Central and deploy new branches more efficiently with a task-oriented Install Manager dashboard, as well as the installer app for mobile devices.
- Health check—The BGW can actively and passively monitor established TCP connections for latency, jitter, packet loss, and throughput.
- **Policy-based routing (PBR)**—You can route traffic across private or public WAN uplinks based on application or user role (examples: guest or employee), in addition to traditional destination-based routing.
- **Dynamic path selection**—When multiple WAN links exist, DPS helps choose the best available path for an application based on characteristics like throughput, latency, jitter, packet loss, and uplink utilization.
- **SaaS optimization**—When accessing cloud-based applications from a branch location with multiple transports, software-as-a-service (SaaS) optimization dynamically chooses the best-performing path based on real-time information.
- WAN optimization—To improve overall bandwidth efficiency, the BGW can enable IP payload compression on the IPsec sessions between the branch and headend gateways. Compression efficiency varies depending on the traffic type, but real-world scenarios typically show 40-60% bandwidth savings.

- **Private or Internet WAN**—The BGW can support multiple uplinks, such as Internet broadband, existing MPLS, metro Ethernet, and cellular connectivity, with multiple transport overlays across uplinks. You can route traffic destined for the Internet locally, and you can route traffic destined for the data center either over private WAN or any available Internet path.
- Third-party integration—To reduce local branch complexity, integration with cloud services provided by firewall vendors such as Zscaler, Palo Alto Networks, Check Point, and UCC applications such as Microsoft Skype for Business makes extending security easier and more reliable across the distributed enterprise.

SD-BRANCH ARCHITECTURE

WANs are the key component for branch office employees to communicate with their co-workers and customers. Applications have moved to centralized data centers and cloud-based providers. Businesses depend on their network to maintain a competitive edge and the WAN is one of the highest monthly costs of the network.

Aruba SD-Branch allows an organization to implement the most cost-effective option at each branch-site location by providing flexible alternatives to traditional private WAN offerings. Traffic can use any available bandwidth to and from each location while maintaining the service level agreements defined by the network administrator. The Aruba SD-Branch architecture is built in layers, as shown in the following figure.



Figure 2 SD-Branch architecture

Connectivity Layer

Starting from the bottom in the figure, the *connectivity layer* is the foundation for the SD-Branch architecture. It forms the underlay network between locations in an organization, and in a WAN setting, the transport links can be private or public depending on the type of service available at each location. Gateways provide flexible connectivity in a variety of form factors. At the branch location, they perform the LAN integration for the wired and wireless devices, and the WAN access for the public and private networks. At the headend location, they allow high speed connectivity to the campus and data center environments. Gateways use advanced routing to direct the traffic to and from each location. The switches and access points form the campus network at each location and connect to the gateway for the WAN services. There are several different branch sizes, and each of them has a recommended wired and wireless design based on their requirements.

Policy Layer

The *policy layer* runs over the top of the connectivity layer and allows organizations to securely transport traffic between sites. VPN tunnels are established between branch and headend gateways to create an SD-WAN overlay network. *Headend sites* are typically corporate headquarters, private data centers, or laaS data centers hosted in the cloud, and they include one or more headend gateways. *Branch sites* are remote locations that include one or more branch gateways. Larger deployments might include additional headend sites, providing path diversity and application redundancy in the event of a primary site failure.

A flexible transport design uses secure policy overlay tunnels to simplify the WAN deployment. The tunnels for public and private WAN connections reduce complexity for your routing and security, regardless of the underlying networks. The tunnels also provide flexibility by allowing an organization to choose different service provider options based on availability and cost for each location, while maintaining a common overlay network.

Services Layer

The *services layer* is where the operations team interacts with the network. It provides significant capabilities leveraging AI, ML, and location-based services for network visibility and insights into how the network is performing. By leveraging a common data lake in the cloud, Aruba Central can correlate cross-domain events and display multiple dimensions of information in context, unlocking powerful capabilities around automated root cause analysis while providing robust analytics.

Headend Site Design

The recommended headend site design consists of a pair of redundant gateways to terminate the IPsec tunnels from the BGWs. Additional headend sites are supported, and you can deploy them by using the techniques described in this guide.

Physical Gateways

The physical gateways connect to the services aggregation layer, and we recommend LACP for uplink port redundancy or equal-cost multi-path routing for L3 redundancy. The gateways terminate the IPsec tunnels from the private WAN by using private IP addresses and from the Internet by using static NAT addresses on the firewall.

The following figure shows an example headend site with a pair of physical gateways using LACP.

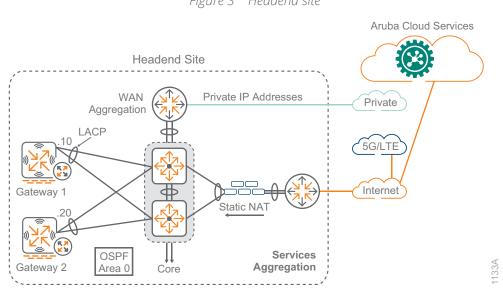


Figure 3 Headend site

The gateways are configured with static IP addresses, which allows the BGWs to reliably connect to them using established addresses.

Virtual Gateways

The IaaS public cloud environment is for many companies a "foreign" element in their network. Services rely on cloud-provider tools that are not like those in the companies' own data center. To alleviate the management and operational concerns, something more advanced than a simple virtual machine offered through the marketplace is desirable.

The Aruba SD-Branch solution automates the deployment and configuration of a virtual gateway (vGW) in public cloud environments like Amazon Web Services (AWS) and Microsoft Azure. Aruba Central handles the whole lifecycle of the vGW, from the initial startup and provisioning, through the regular management and the failover between them in high availability scenarios.

Aruba BGWs support standard IPsec tunnels and could therefore establish direct communication with the IaaS provider's own VPN concentrators. However, cloud VPN termination points do not support the advanced SD-Branch capabilities equivalent to those of an Aruba vGW. The most critical features are as follows:

- Orchestrated tunnels—Aruba Central automates the establishment of IPsec tunnels from all BGWs to all relevant VPNCs, including the vGW.
- Orchestrated routing—Aruba Central automates the exchange of routes across the SD-WAN, to and from the vGW location.
- **Reverse path pinning**—The vGW ensures the traffic always returns through the same WAN path, allowing BGWs to perform DPS, PBR, and uplink load-balancing as needed.
- End-to-end visibility—Allows you to manage all SD-Branch network devices under a single pane of glass in the cloud.

The following figure shows a pair of virtual gateways in an IaaS public cloud environment.

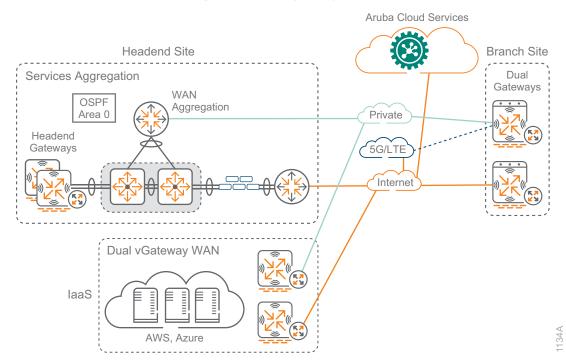


Figure 4 Virtual gateways in IaaS

From the perspective of the SD-WAN network in an IaaS environment, deployments are differentiated between those where each Virtual Network (VNET) or Virtual Private Cloud (VPC) is treated as a separate node of the SD-WAN and those where there are multiple VNET/VPCs accessible through a single SD-WAN node. When there are multiple VNET/VPCs, you place the vGW into the transit or edge VNET/VPC. The vGW communicates with the VHUB/TGW, as shown in the right side of the following figure.

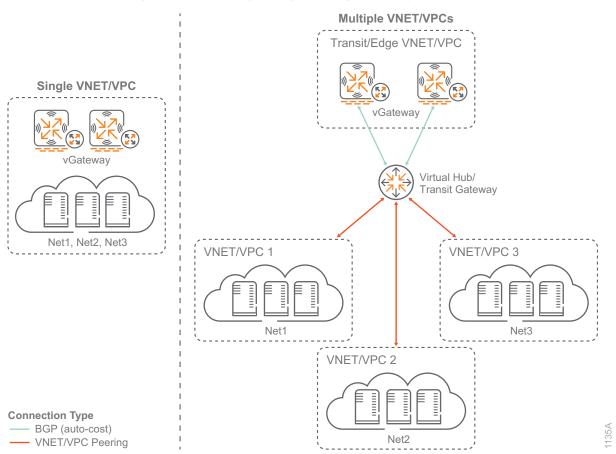


Figure 5 laaS deployment types—single vs multiple VNET/VPCs

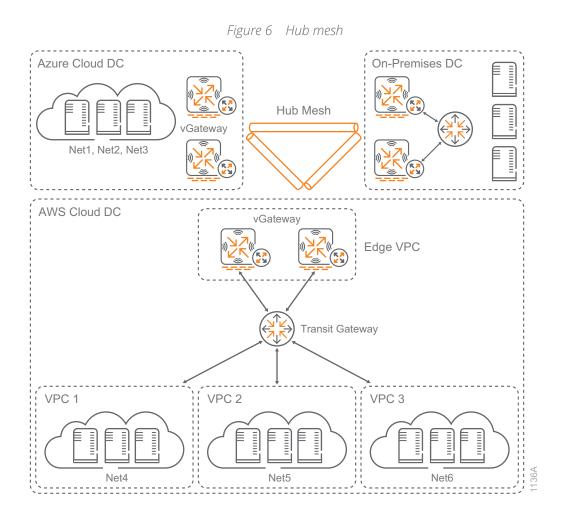
The use of the vGW to connect the SD-WAN environment to the laaS environment is highly encouraged, as it truly brings the public-cloud data center into the SD-WAN network as if it were any other headend location.

Hub Mesh

Aruba supports mesh topologies between on-premises hubs (physical gateways) and/or cloud hubs (virtual gateways). In a mesh topology, all or a portion of your hub sites are connected to each other through site-tosite IPsec tunnels. Using a mesh, you can connect any type of hub and create an overlay network between your data centers.

The mesh topology is highly redundant because it creates a mesh of tunnels over all available uplinks and uses BGP mechanisms to exchange routes between each peer. For easier identification of the hubs and a simplified configuration, it is recommended that you use a loopback address on each hub and source the site-to-site tunnels and the BGP peering from the loopback address. You can route-map match prefixes received or advertised by the peer, and you can modify them to control what is advertised between the hub locations.

You can configure up to eight hub sites in a mesh topology. Each hub site can be in only one mesh topology at a time.



Branch Site Design

A branch site with two WAN interfaces is a common use case, but you can use the same techniques for other options. For example, you can deploy a single BGW or dual BGWs, depending on the business criticality of the location. You can add up to four active and one standby LTE uplink per branch location. The goal of all SD-WAN designs is to choose the best WAN path for each different class of traffic. After choosing the best path based on current WAN conditions, you create flexible rules to allow your traffic to efficiently pass over the available paths.

The first option is the SD-WAN Private and Internet, which uses private WAN paired with Internet. In this option, the private WAN handles the critical traffic because you have SLA guarantees from your service providers for certain applications. The secondary traffic classes use the public WAN available at each location.

The second option is the SD-WAN Dual Internet, which uses two Internet services. With this option, you select one of the Internet paths as the preferred path. You can select the provider that has more direct connections to each of your branch sites, or you can choose the one with the most bandwidth. The secondary traffic classes use the remaining Internet bandwidth available at each location.

Branch Gateway Options

This guide highlights several branch-site designs, and they provide different levels of service and redundancy using diverse WAN transports tied to the specific requirements for each site. Single gateway designs provide uplink resiliency and dual gateway designs provide uplink and gateway resiliency. Both can optionally add 5G/LTE uplinks for a path of last resort. The following figure shows common branch-site options.

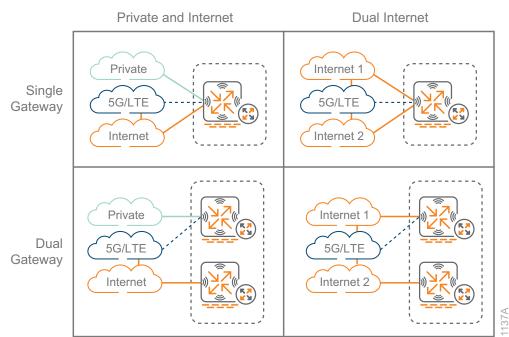
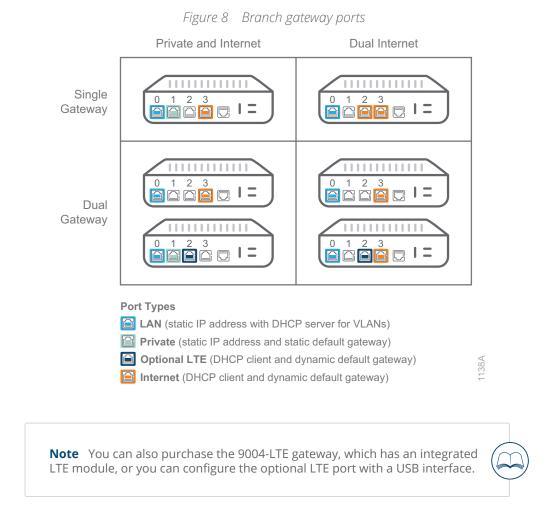


Figure 7 Branch gateway options

Branch Gateway Ports

You should use the physical ports on a BGW in a uniform manner across your network. This provides consistency between your branches and reduces the number of groups required. The examples shown in the following figure are focused on the Aruba 7005 BGWs because it has the fewest number of physical ports, but the same port arrangement principles are used for the rest of the BGWs in the portfolio. The idea is to pick a common set of ports that work for as many of your branch configurations as possible.

The following figure highlights port arrangements on the Aruba 7005 BGWs for the different branch site options mentioned previously.



It is very important the physical port types on gateways at dual-gateway sites share the same characteristics, because both gateways must be added to the same group for routing, DPS, and PBR configurations. If a port type defined at the group-level is not needed at certain branches, you should disable it at the device-level to prevent it from showing as down in the Monitoring and Reports application. All four examples in Figure 8 use the physical ports in a similar fashion as noted below:

- Port 0/0/0—LAN with static IP addresses and DHCP servers for VLANs
- Port 0/0/1—Private WAN with static IP address and default gateway
- Port 0/0/2—Public WAN (LTE or secondary INET) with DHCP client and dynamic default gateway
- Port 0/0/3—Public WAN (primary INET) with DHCP client and dynamic default gateway

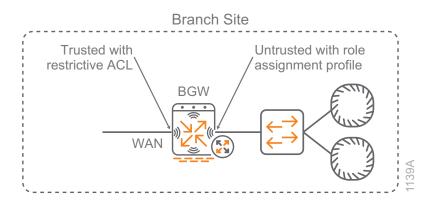
Because the port arrangements for each of the groups are aligned configuration-wise, you can configure an initial group and then copy it to the new groups to save time during the group configuration procedures. The port types you choose do not have to align with the choices above, but they should match the common port arrangements for your environment.

Trusted vs Untrusted

Unlike traditional perimeter firewalls, the trusted interface feature in an Aruba gateway's role-based firewall refers to whether there is a user-session for all traffic coming through an interface with the potential for role assignment policies. The two options are as follows:

- The gateway does not keep user-sessions for traffic coming through trusted interfaces.
- The gateway maintains user-sessions for all devices coming from untrusted interfaces. This means you must assign a role assignment (AAA) profile to all VLANs attached to untrusted interfaces, regardless of whether you plan to enable role assignments.

You achieve the best combination of security and visibility when LAN-facing interfaces are marked as untrusted with an associated role-assignment profile and WAN-facing interfaces are marked as trusted with a restrictive policy applied to them.





Note When you use the Basic setup mode in Aruba Central, the interfaces are correctly configured for trust based on how their WAN or LAN designations.

The gateway determines if traffic is trusted by first selecting the trust status of the port and then the trust status of the VLANs attached to the port. In case of a discrepancy, the untrusted status always takes precedence.

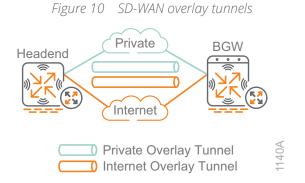
Policy Layer

The Aruba SD-Branch solution implements standards-based VPN tunnels. To simplify the SD-WAN overlay tunnel establishment, the Aruba gateways leverage factory installed trusted platform module (TPM) certificates for mutual authentication. The TPM certificates are installed on each Aruba gateway at the factory; however, end-user certificates are also supported.

The SD-WAN overlay tunnel is initiated from the BGW and terminates on a gateway using network address translation-traversal for the Internet paths. The only firewall port that you need to open between a headend gateway and a BGW for a tunnel to establish is UDP destination port 4500. You can terminate the tunnels directly on the headend gateway or NAT them via an intermediate device, such as an edge firewall for the Internet WAN connection.

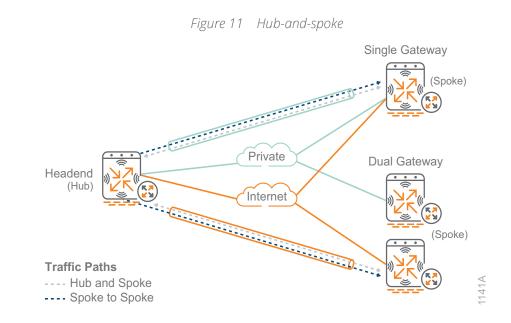
For private WANs, the tunnels are typically terminated on a headend gateway by using a VLAN interface assigned with a private IPv4 address. You can either terminate Internet-based WAN services on a gateway using a public IPv4 address or a private IPv4 address. This depends on your organization's data center architecture.

You establish the SD-WAN overlay tunnel through the connectivity underlay network to a gateway at the headend site. Each BGW establishes one tunnel to each headend for every WAN service in the deployment. The following figure shows an example of a single BGW at a branch site establishing one tunnel over the private WAN and one tunnel over the Internet WAN service.



Hub-and-Spoke

The Aruba SD-Branch solution supports a hub-and-spoke topology where the SD-WAN overlay tunnels are established between headend gateways (hubs) and BGWs (spokes). With a hub-and-spoke design, the DPS policies, routing, and PBR rules you configure for each branch group determine the branch traffic that is selected and forwarded to the gateways via the overlay tunnels. The gateways at the headend sites provide routing and forwarding for hub-to-spoke and spoke-to-spoke traffic.



Most SD-Branch deployments include at least one headend site with one or more gateways installed that terminate VPN tunnels initiated from BGWs installed at the branch sites. The number of gateways that are deployed in each headend site is dependent on the deployment size and redundancy needs. The most basic SD-Branch deployment consists of one gateway installed at a headend site that services all the BGWs installed at branch sites. L2 or L3 redundancy are available by installing a backup gateway at the headend site, but L3 redundancy is recommended due to faster failover times.

Larger SD-Branch deployments can include additional headend sites, providing redundancy in the event of a primary hub failure. A typical large deployment consists of a primary and secondary headend with L3 redundant gateways at each site. More complex topologies using additional headend sites are also supported. For example, your deployment might include a cloud-based data center hosting a specific application or service using virtual gateways.

ARUBA SD-WAN

The Aruba SD-Branch solution provides a centralized control plane function (offered from Aruba Central) that is based on a cloud-native, multi-tenant architecture that automatically scales to a customer's network growth. In previous SD-Branch deployments, the network administrator had to configure IPsec tunnels between branch and headend gateways, interface types, public IP addresses of the VPNCs and the IKE parameters. When using a tunnel through a common Internet service provider, the uplink on BGW and the public IP address on the VPNC was manually configured.

The configuration workflows were cumbersome and prone to misconfigurations that often-delayed deployments and led to unnecessary calls to TAC. There was no support for dynamic protocols or orchestrated routes through the overlay tunnels. Static routes pointing to each data center were configured with different costs in order to provide redundancy in case of a failure. For large deployments, which might have hundreds of locations, static routes were not scalable or easy to administer.

SD-WAN Orchestrator

To simplify the configuration, Aruba introduced SD-WAN Orchestrator to automatically setup IPsec tunnels and configure dynamic routing between the BGWs and headend VPNC. Overlay Tunnel and Route Orchestrator processes run in Central to automate the existing workflows.

The Aruba SD-WAN Orchestrator provides the following features:

- The IPSec overlay is automatically created through tunnel orchestration.
- Reachability information is propagated through route orchestration, and route redistribution is done through a single group configuration.
- Routing policies are set with a simple hub preference at the group level and route redistribution at the headend ensures symmetry.
- Individual devices do not need to be configured with the overlay topology and routing policy because they are done at group level for all devices.
- When a new BGW is added to a group, it dynamically learns the overlay topology and orchestration creates the tunnels and route policy.
- Changing the path preference is done by changing hub preference setting and routing costs are translated into the data center routing process.
- Scalability is built into the orchestration, which helps an organization build a robust routing design.

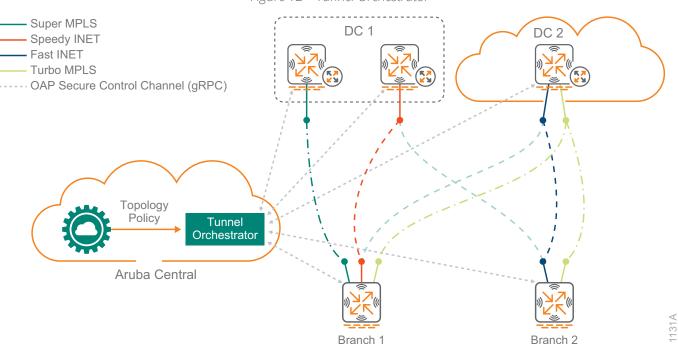
Tunnel Orchestrator

In order to build an SD-WAN network, the first step is to bring up a policy overlay network that is independent of the underlying WAN circuits. In order to do this, the administrator identifies the uplink interfaces in all gateways with their corresponding service provider. After the information is entered, SD-WAN Orchestrator establishes the overlay tunnels according to the defined policy. The main functions of Aruba Overlay Tunnel Orchestrator include:

- Discovering the public/private IP addresses and uplinks attributes
- Exchanging keys and sending keys to devices
- Building IPsec tunnels
- Refreshing keying material before old keys expire

Aruba Overlay Tunnel Orchestrator removes the complexity and scalability issues associated with configuring IPsec tunnels. It also eliminates the need to specify Internet Key Exchange (IKE)-related information. With SD-WAN Orchestrator, Aruba simplifies the configuration of one of the most complex tasks when bringing up an SD-WAN service.

SD-WAN Orchestrator sends the topology policy to Tunnel Orchestrator and, based on interface type and provider name, it automatically establishes the tunnels. If the interface type is MPLS, the names must match for the orchestrator to build the tunnels. If the interface type is INET, the orchestrator prefers names that match, but tunnels are also built for non-matching Internet providers names as shown in the following figure. In the figure, the tunnel orchestrator establishes an Overlay Agent Protocol (OAP) secure control channel using Google RPC to each BGW and VPNC.





Route Orchestrator

Aruba Route Orchestrator enables the distribution of routing information across all sites including branches and headend. It provides route distribution across sites in a dynamic way according to the topology and routing segmentation policy configurations.

The main functions of Aruba Route Orchestrator include:

- Learning routes from headend and branch sites
- Advertising routes across the SD-WAN network with appropriate costs
- Redistributing routes into the LAN side with appropriate costs

SD-WAN Orchestrator's goal is to build the SD-WAN overlay and provide dynamic routing with minimal intervention from the user's side. The network behind the gateways can be a simple L2 with connected subnets or a more complex L3 environment running OSPF or BGP routing.

In the following figure, Route Orchestrator acts like a BGP route reflector to collect and redistribute the routing information from each gateway using the routing policy defined in Aruba Central.

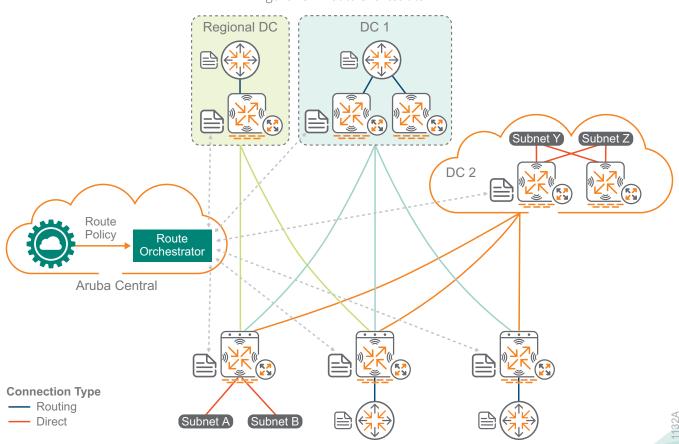
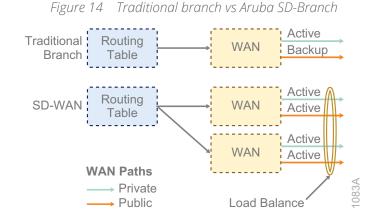


Figure 13 Route Orchestrator

Traditional Branch

With traditional branch solutions, traffic is routed using the information from the routing table over a single active WAN path, and other paths are backup links that are used only when the active link becomes unavailable. The Aruba SD-Branch solution sends traffic simultaneously over multiple active WAN paths. The paths can be different types with unequal bandwidths, and they can also span a second gateway device. The following figure compares traditional branch solutions with Aruba SD-Branch.



To further enhance the Aruba SD-Branch solution, routing is manipulated using SLAs to ensure compliance with defined thresholds and preferred WAN paths are chosen on a dynamic basis. The three areas where path selection decisions are made are as follows:

- **Routing table**—If special treatment is not required, traffic is forwarded from the routing table.
- **Dynamic path selection**—If SLAs are required and the preferred paths are in the routing table, DPS dynamically selects the best available WAN path.
- **Policy-based routing**—If the preferred WAN paths are not available in the routing table or you want to specify a path for traffic, PBR overrides the available WAN paths using next hop lists.

If the traffic has a simple path without specific requirements, it can follow the routing table. However, most SD-WAN customers want to use SLAs to provide a better user experience for their real-time traffic while pushing their background traffic to lower performing WAN paths. If SLAs are needed and the preferred WAN paths are available in the routing table, a DPS policy is required. If the preferred WAN paths are not in the routing table or you want to steer to a specific set of equal cost paths, a PBR policy with a next-hop list is required.

The administrator decision tree shown below helps you determine when DPS and PBR policies are needed in your environment. PBR policies take precedence over entries in the routing table, so you should only use them when required.

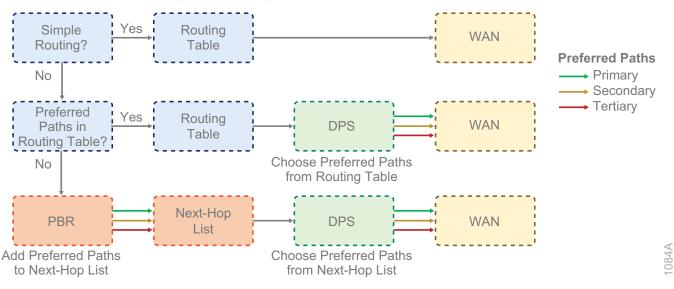


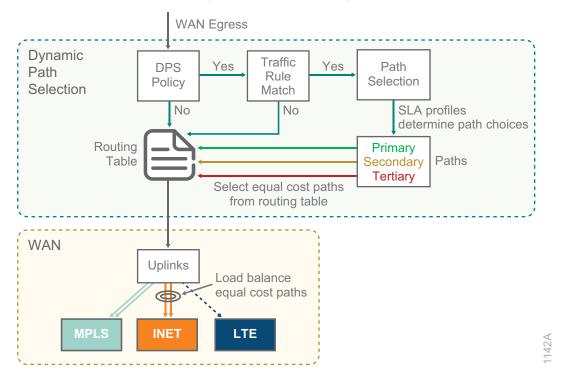
Figure 15 Routing, DPS, and PBR administrator decision tree

Dynamic Path Selection

Using health-monitoring information, DPS can intelligently route traffic based on policy, ensuring that applications are sent over the paths most appropriate to their needs. Based on user-defined criteria, DPS allows branch gateways to select the best path for an application to take across the WAN. The network administrator can define service-level agreements (SLAs) for an application based on values such as latency, jitter, packet loss, and uplink utilization, and the gateway makes a path selection based on which available link meets the SLA criteria.

The selected forwarding path can be a single WAN uplink, or traffic can be load-balanced across a group of WAN uplinks. The destination IP address of the traffic determines if the traffic is steered towards a VPN tunnel or forwarded directly to the Internet at the branch location. The DPS policy selects an uplink, and the gateway's routing table or PBR rules determines the next hop.

Figure 16 DPS on WAN egress



Load Balancing

When DPS selects a group of WAN uplinks, the gateway performs a load-balancing action. The load-balancing algorithm determines how sessions are distributed between the active WAN uplinks in the group.

Branch gateways support the following load-balancing algorithms:

- **Round robin**—Sequentially distributes outbound traffic between each active WAN uplink. This is the simplest algorithm to configure and implement but might result in uneven traffic distribution over time.
- Session count—Distributes outbound traffic between active WAN uplinks based on the number of sessions managed by each link. This algorithm attempts to ensure that the session count on each active WAN uplink is within 5% of the other active WAN uplinks.
- Uplink utilization—Distributes traffic between active WAN uplinks based on each uplink's utilization percentage. Uplink utilization considers the link speed to calculate the utilization for a given link and allows a maximum bandwidth percentage threshold to be defined. After the bandwidth threshold percentage has been exceeded, that WAN uplink is no longer considered available.

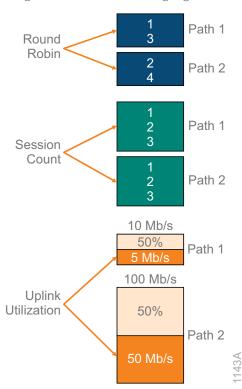


Figure 17 Load-balancing algorithms

Aruba recommends the uplink utilization algorithm because it accounts for the WAN service speed when making path selection.

Health Checks

You must enable health checks in order to determine the path availability of each WAN uplink and policy overlay tunnel. When health checks are enabled, the gateway sends UDP or ICMP probes to an IP or FQDN of a host to determine if the connectivity underlay paths are available to accommodate traffic. The BGW also sends probes to all VPNCs to determine if the policy overlay paths are available for traffic. The primary use case for health checks is to verify the WAN underlay and overlay networks are operational which prevents branch traffic from being forwarded into a black hole.

When the defined health check host is not reachable over a WAN uplink, the default gateway associated with the WAN uplink is removed from the gateway's routing table. This prevents the WAN uplink from being used for branch traffic that is NAT'd to the Internet or management traffic that is destined for Central. Any established VPN tunnels continue to operate if the VPNC is reachable over the WAN uplink. Aruba Gateways monitor the state of every WAN circuit by probing their default-gateway, the tunnel destination to each headend gateway as well as a service in the cloud to assess the health and status of every uplink. The following criteria are used:

- There must be a default-gateway defined for every WAN interface for it to be considered a valid uplink. A higher cost can be associated if the default-gateway shouldn't be used, but it must exist for the health check to work.
- BGWs send probes to headend gateway destinations through all uplinks in order to measure the health and state of the policy overlay tunnels.
- BGWs send probes to a health check service. In order to avoid black-holing Internet traffic, the gateway prevents connectivity underlay communication through uplinks marked as "unreachable" by the health check probes. Because they have their own probes, overlay traffic continues to work without impact

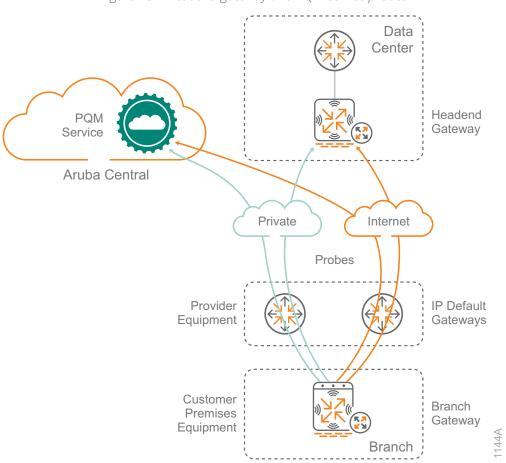


Figure 18 Headend gateway and PQM service probes

Aruba PQM Service

As part of the SD-Branch solution, Aruba provides a global Path Quality Monitoring (PQM) service that gateways can probe to measure the quality of the uplinks. This global service consists on a set of nodes that respond to ICMP/UDP probes from gateways managed by Aruba Central. All other traffic is throttled to avoid DoS attacks.

This service is maintained by the Aruba Cloud Operations team. On top of the regular monitoring of all the PQM nodes and the authoritative DNS, Aruba has distributed probes all over the world probing pqm. arubanetworks.com every five minutes. These probes are constantly reporting latency, packet loss, and which PQM node is responding to the Aruba Cloud Operations dashboard. This provides not just monitoring of the instances but a true 24x7 monitoring of the PQM service.

The Aruba SD-Branch solution relies on control-plane communication between BGWs and VPNCs, which allows the SD-WAN orchestrator to negotiate tunnels and establish routes. At least two paths of communication are recommended between the gateways and Aruba Central. This becomes even more important when dealing with Internet, LTE or VSAT circuits that are not be as reliable as an enterprise-grade MPLS network. You can achieve a second path to Aruba Central by configuring a static default route with a higher cost pointing to the private WAN overlay tunnel, which is routed over the headend site's DMZ out to the Internet.

Policy-Based Routing

Some advanced deployments might require PBR to override destination-based routes when traffic must be forwarded over a specific WAN path. If needed, PBR policies override the routing table for both underlay and overlay traffic. For example, if you want all traffic from your corporate users to go through the hub-site location, you apply a PBR rule pointing to the overlay tunnels. The gateway can use multiple paths by setting the same priority in a next-hop list and applying the PBR policy to the relevant user roles. If more than one active path is available, the gateway selects them using a combination of DPS and load-balancing.

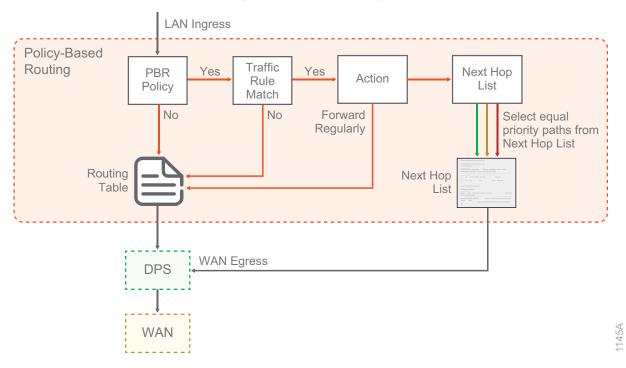


Figure 19 PBR on LAN ingress

Common use cases where PBR policies are implemented include:

- All employee Internet traffic must be routed to the hub-site location to provide additional policy checks.
- Traffic from a specific subset of clients' needs to be forwarded out a specific WAN path.
- Integration with third-party SaaS or unified threat management providers—such as Check Point, Palo Alto Networks, or Zscaler—where certain traffic needs to be steered through a cloud-based security provider.

Reverse-Path Pinning

When a path selection is made for sessions destined for the corporate network through a VPN tunnel, the reverse traffic must take the same WAN path to prevent connectivity problems caused by asymmetric routing issues. Reverse-path pinning allows the hub gateway to choose the same WAN path for each active session to and from the branch. This is important because the branch gateway selects paths based on performance and SLAs. Reverse-path pinning is performed for corporate sessions originating from the branch destined to the data center, as well as sessions originating from the hub towards the branches.

A session destined for a branch from the hub site is handled as follows:

- The VPNC gateway selects an available WAN path using equal-cost multi-path routing.
- If the WAN path matches the preferred path defined in the DPS policy, then no additional steering is required.
- If the WAN path does not match the preferred path defined in the DPS policy, the branch gateway sends the return session over the preferred path. Upon receipt of the traffic from the new path, the VPNC steers the outbound session to the preferred path to maintain symmetry.

The following figure shows traffic from a branch location over the private WAN overlay tunnel and the reverse path pinning feature on the VPNC returns the traffic on the same path to enforce symmetry.

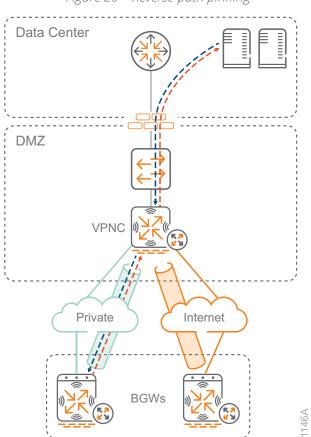


Figure 20 Reverse-path pinning

Cloud Security Providers

Security is an integral part of the Aruba SD-Branch solution. The solution is built from the ground up to be completely policy-driven using a role-based model. In most deployments, the BGW is directly connected to the Internet, requiring very robust hardening policies. The Aruba SD-Branch solution begins with the hardening of the operating system, adds signature-based device profiling with ClearPass and supports the integration with best-of-breed security partners by using on-premises appliances or cloud-based services.

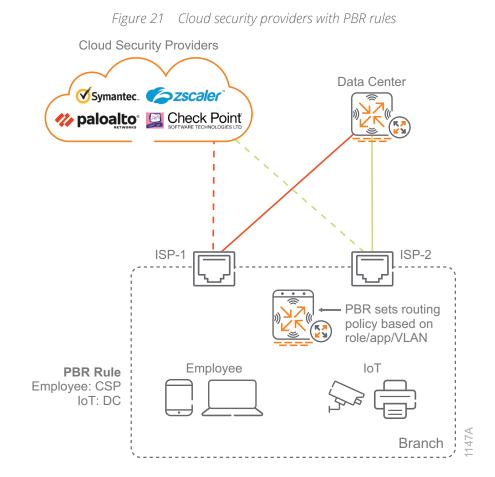
The BGW has a hardened operating system that includes the following security features:

- Secure boot—TPM-signed software image that heavily restricts communications until the BGW receives its initial configuration from Aruba Central
- Secure zero touch provisioning—Leverages the TPM to securely communicate with Aruba Central
- AES 256 encryption—To secure the SD-WAN policy overlay tunnels
- **Role-based stateful firewall**—Support for scalable configuration using firewall aliases, ALGs, and role-based policies
- Deep packet inspection—Capacity to identify close to 3200 applications
- Web content and reputation filtering—WebRoot's ML technology to classify content, reputation, and geolocation for billions of URLs
- Aruba threat detection—IPS/IDS available in the 9000 series gateways

The Aruba SD-Branch solution integrates with ClearPass Policy Manager to form a true policy-driven branch. This model dynamically assigns policies based on users and devices, as opposed to the traditional way of assigning policies manually based on VLANs, IP addresses. and ports. You can enhance the policy-driven branch by leveraging integrations with partners in the ClearPass Exchange. You can push device identification further by integrating with Aruba Device Insight for advanced AI/ML-based profiling.

Aruba SD-Branch can also integrate with best-of-breed third-party security infrastructure partners to offer enterprise-grade advanced threat protection in a scalable manner. The integration with cloud-based security offerings from third party companies provides an extremely simple and scalable solution for advanced threat protection in branch networks.

To secure your Internet traffic, the BGW redirects selected traffic through a cloud-based security platform. This enables best-of-breed security, with services like advanced threat protection or data loss prevention, without the need to increase the footprint in branch locations. In the following figure, a PBR rule sends the employee Internet traffic to the cloud security provider for threat mitigation, and the IoT traffic goes straight to the data center.



SaaS Express

As more businesses deploy SD-WAN to take advantage of inexpensive broadband Internet services and also adopt software-as-a-service (SaaS) applications such as Office 365, Box, Slack, and Zendesk, operations teams must ensure the users at a branch site can seamlessly and securely connect to their applications in the cloud with the best possible performance. The Aruba SaaS Express feature enables the discovery of the SaaS application servers, monitors application performance, and steers traffic to the best available servers in order to provide an improved user experience.

The SaaS Express feature offers the following benefits:

- Real-time probe measurement to determine the optimal ISP for user traffic
- Ability to choose the best network path for SaaS applications in order to optimize the user experience
- Improved service reliability with multiple network paths and dynamic traffic-steering

SaaS Application Profile Parameter

The BGW supports a set of applications and application categories in the DPI library. The built-in application profiles include a set of SaaS applications; for example, Adobe, Dropbox, Amazon, Google, Salesforce, Slack, Webex, etc. If a SaaS application is not available in the list, the network administrator can configure their own.

Each SaaS application profile includes the following elements:

- Name—Name of the SaaS application
- FQDN—A list of domain URLs bound to the SaaS application
- Exit profile—Traffic steering policy for determining an optimal path exit
- SLA—Threshold profile for measuring path quality and performance
- Health check probe URI—URI to use for probes to determine the best available path

HTTP and DNS Probes

Aruba BGWs send HTTP requests to each SaaS application over every available path. They calculate the average packet loss and latency for each path in order to determine the one with the best performance. When a user requests access to a SaaS application, the BGW dynamically steers the application traffic to the best available path.

When a client requests SaaS application access, the BGW intercepts the DNS query acting as a proxy and forwards the query to the DNS server to resolve into IP addresses. Using the type of SaaS application and the location of DNS caching servers for a given ISP, the BGW determines the best available uplink. This means traffic is automatically steered to the best performing SaaS servers, rather than statically defining them based on a best-guess geographic location.

Traffic Steering and Path Selection

Network administrators can use a WAN policy with path steering based on key performance indicators, such as jitter, latency, and packet loss, to attach the policy to each SaaS application profile. By default, the BGW includes a Best for SaaS SLA profile, which is used for SaaS application profiles. Network administrators can also use a custom SaaS policy for steering their SaaS application traffic. The following figure illustrates SaaS traffic steering and path selection from a branch site with dual Internet circuits.

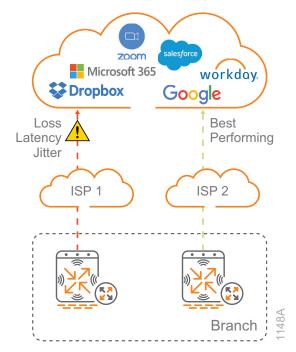


Figure 22 SaaS Express traffic steering and path selection

ARUBA SD-LAN

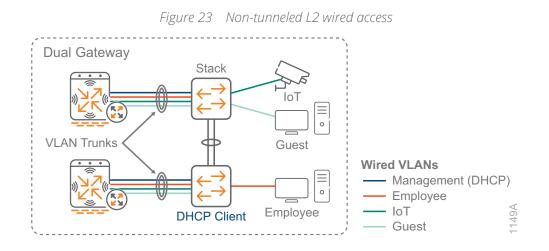
The Aruba SD-Branch solution provides a centralized control plane function offered from Aruba Central that is based on a cloud-native, multi-tenant architecture that automatically scales to a customer's network growth. After the SD-WAN is deployed, the SD-LAN behind the branch gateway is next.

Non-Tunneled L2 Wired Access

To handle complex topologies with more IP subnets, branch sites use non-tunneled L2 switching for simple wired designs and L3 switching. If micro-segmentation is needed, traffic can be tunneled from the wired switches and APs to offer additional security.

In this design, the BGW provides L3 services for the site. The switches use VLANs for segmentation, which allows you to configure your access switches identically to further reduces the complexity of the design. Using the same switch hardware and feature configurations saves money due to lower operational costs and maintaining fewer sets of spares.

The access switch is trunked to the BGW to map the VLANs between them. The BGW acts as the IP default gateway for each of the IP subnets and provides DHCP services to the end devices. DHCP can also be centralized at the headend location. The switch obtains its IP address by using a DHCP client on the management VLAN.



Non-Tunneled L3 Wired Access

In this design, the L3 aggregation switch provides layer-3 services for the site. The L2 access switches use multiple VLANs that are trunked to the aggregation switches to map the VLANs between them. The aggregation switches acts as the IP default gateway for each of the IP subnets and provides DHCP services to the end devices. DHCP can also be centralized at the headend location. The L2 access switch obtains its IP address using a DHCP client on the management VLAN. The aggregation switches are routed to the BGWs using L3 ports. The guest VLAN uses a second set of ports to provide L2 access to the BGWs for direct access to the Internet.

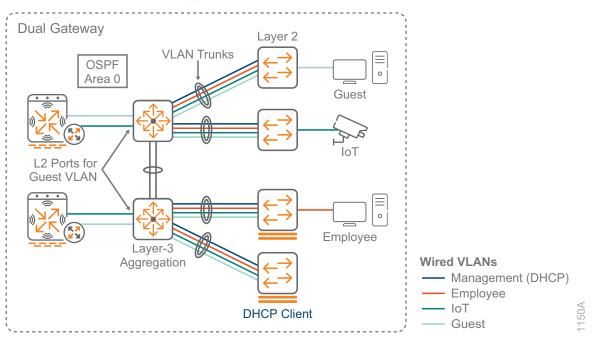


Figure 24 Non-tunneled L3 wired access

Non-Tunneled Wireless Access

Aruba Instant is a controllerless wireless architecture that is easy to set up and that supports robust security features. It includes automatic RF management to ensure the best Wi-Fi connection and granular visibility into applications, which helps prioritize business-critical data, limit or block non-business data, and keep malicious actors off your network. This design is well suited for deployments where tunneled traffic is not needed. Unlike solutions that require a separate management system, an Aruba Instant cluster distributes certain functions across the APs in the cluster and elects a single AP to act as a virtual controller for the remaining configuration functions, which are managed by Central.

APs are staggered into different switches within a stack in order to minimize disruption during software upgrades or unexpected switch outages. The switches use device profiles to automatically place the APs into the management VLAN and the APs use a DHCP client to obtain their IP addresses. Dynamic trunks are created between the APs and the L2 switches that map to the SSIDs and are passed through to the BGW for L3 termination.

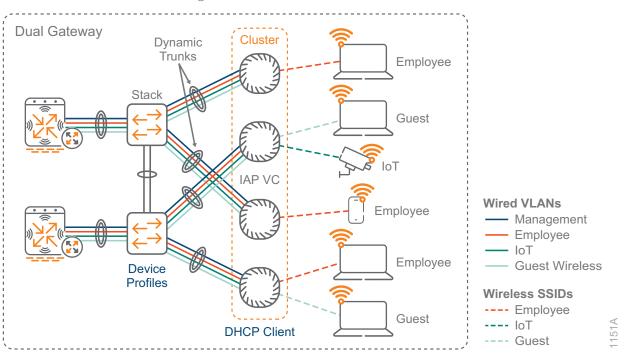
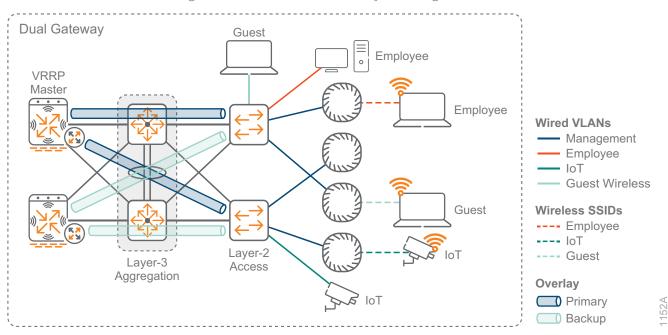


Figure 25 Non-tunneled L2 wireless access

Tunneled Access with Dynamic Segmentation

In this design, the user VLANs from the access switches, and APs are tunneled to the BGWs for L3 termination. Device profiles are used on the switches to automatically configure the AP ports for the management underlay VLAN and the SSID VLANs are dynamically trunked. Role-based access is configured for all ports on the switch and port-based mode is used for APs. Tunneled traffic is always untrusted, which means you must apply an AAA profile to the VLAN. Each VLAN can have a separate AAA profile with a different initial role in the BGW.





SD-BRANCH COMPONENTS

This section discusses the recommended components for an SD-Branch solution. Not every component is required for a valid SD-Branch deployment. The only hard requirements are a branch location with multiple WAN paths and Aruba Central for the management.

Gateway Components

The gateway offers organizations a reliable, high performance option with support for multiple WAN connections. From a routing standpoint, this provides IT with insight into the traffic flowing in and out of a site, regardless of the uplink. A headend gateway is needed for VPN tunnel termination in private data center and campus routing scenarios. A virtual gateway is needed for network deployments using cloud providers. A branch gateway provides direct access to the Internet at a remote site, as well as secure tunnel access to corporate resources at the headend location.

Headend Gateway

The headend gateway acts as a VPN concentrator terminating VPN tunnels, and it provides routing into the data center or campus environments using OSPF or BGP. The headend gateway participates in the SD-WAN fabric overlay topology by terminating the tunnels from the BGWs. The headend gateway is a software function that runs on the Aruba 7200 series appliances, the 9000 series appliances, and some of the Aruba 7000 series appliances. The following table details the headend gateway scaling.

Table 1 Headend gateway scaling

Platform	Max tunnels	Max IKE learned routes	Max routes in forwarding table	WAN compression	Crypto throughput	Firewall sessions
7280	8192	32,768	32,768	10 Gbps	50 Gbps	2M
7240XM	6144	32,768	32,768	10 Gbps	30 Gbps	2M
7220	4096	16,384	16,384	10 Gbps	21 Gbps	2M
7210	1024	8096	8192	10 Gbps	8 Gbps	2M
7030	512	3000	4096	2.5 Gbps	2.6 Gbps	128K
7010/7024	256	1500	4096	2.5 Gbps	2.6 Gbps	64K
9004/9012	512	3000	4096	2.5 Gbps	4 Gbps	64K

Virtual Gateway

The virtual gateway extends the SD-WAN overlay services to the public cloud infrastructure. Virtual gateways function as VPN concentrators and terminate tunnels from branch gateways, Instant APs and, VIA clients. Like the hardware VPN concentrators, virtual gateways support routing, security, and tunneling features. Virtual gateways are supported in Amazon Web Services and in Microsoft Azure. The following table details the virtual gateway scaling.

Table 2 Virtual gateway scaling

Platform	Max tunnels	Max IKE learned routes	Max routes in forwarding table	Crypto throughput	Firewall sessions
vGW-4G	8192	32,768	131,072	4 Gbps	6M
vGW-2G	4096	16,384	65,536	2 Gbps	256K
vGW-500M	1600	8096	2048	500 Mbps	64K

Branch Gateway

The branch gateway is the appliance at each remote site that connects to WAN uplinks and participates as an endpoint in the SD-WAN overlay fabric. The branch gateway provides the dynamic segmentation by acting as a policy-enforcement point for wired, wireless, security, and WAN policies including routing. The gateway functions include stateful firewall, web content classification, hybrid WAN connectivity, IPsec VPN, QoS, and WAN path monitoring and selection. The branch gateway is a software function that runs on the Aruba 7200, 9000 and 7000 series appliances.

The following table details the branch gateway scaling.

Platform	Client devices	Firewall throughput	Crypto throughput	Active firewall sessions	Firewall sessions per second	Tunneled node ports
7240XM	32,768	40 Gbps	30 Gbps	2M	800K	Pending QA
7220	24,576	40 Gbps	20 Gbps	2M	500K	Pending QA
7210	16,384	20 Gbps	6 Gbps	2M	350K	Pending QA
7030	4096	8 Gbps	2.6 Gbps	128K	65K	2048
7010/7024	2048	4 Gbps	2.6 Gbps	64K	64K	1024
9004/9012	2048	7 Gbps	4 Gbps	64K	32K	2048
7005/7008	1024	2 Gbps	1.2 Gbps	64K	63K	512

Table 3 Branch gateway scaling

For a complete list of Aruba Central-supported gateways, see Aruba Central Supported Gateways.

Microbranch

For very small and micro branch deployments, Aruba does not require a traditional branch gateway. You can deploy an Instant AP cluster at a small branch or home office location without a gateway. In this design, the Instant AP acting as a virtual controller establishes secure connections with the VPN concentrators at each headend or data center location. The Instant cluster provides Wi-Fi connectivity to the end devices and secure WAN access to corporate resources.

For a complete list of Aruba Central-supported Instant APs, see <u>Aruba Central Supported Instant APs</u>.

Wired Components

The wired LAN in the SD-Branch uses a layer-2 or layer-3 design. Although there are many hardware choices that work at the access layer in the network, this design focuses on products that are the most common and easily supported options in each layer of the network, with general guidance on which option to choose.

Access Switches

The access layer connects wired devices to the network, such as APs, workstations, multi-function printers, and other devices that don't support Wi-Fi or need higher performance than a wireless connection can provide. The access layer also provides PoE to devices such as APs, IP phones, and IP cameras.

The following features are common across the Aruba access switches:

- Support for security and network management with Aruba ClearPass and Aruba Central
- REST APIs for automation
- PoE for APs, IP phones, and IoT devices

The number of ports needed in an access closet and the performance required determine which access switch model is the best fit for your network.

Aruba 5400R—The Aruba 5400R chassis supports a variety of interface modules that provide copper and fiber interfaces in different speeds and densities. At the access layer, the switch supports up to 96 HP Smart Rate Multi-Gigabit or 288 1-GbE ports with PoE+. This switch is ideal for organizations that need large numbers of access ports in high-density areas of their network (majority of access closets with 96+ ports). Features:

- Layer-3 modular switch with VSF stacking, tunnel node, ACLs, robust QoS, low latency, and resiliency
- HPE Smart Rate for high-speed multi-gigabit bandwidth (IEEE 802.3bz) and PoE+
- Scalable line-rate 40 GbE for wireless traffic aggregation

Aruba 3810M—The Aruba 3810M is available with either 24 or 48 1-GbE access ports with PoE+ (30W) on each port and either 4 SPF+ ports or 2 40-GbE ports on an optional expansion module. The 3810M is also available in a model with 40 1-GbE ports and 8 HPE Smart Rate ports capable of 1, 2.5, 5, or 10 GbE. The 3810M supports backplane stacking with up to 10 switches in a single stack and advanced layer-3 services. It also supports meshed stacking. This switch is ideal for organizations that have larger access closets requiring larger switch stacks, are deploying or planning on deploying 802.11ac Wave 2 APs and want a switch with high performance and room for future growth. Features:

- Layer-3 switch with backplane stacking, tunnel node, ACLs, robust QoS, low latency, and resiliency
- HPE Smart Rate for high-speed multi-gigabit bandwidth (IEEE 802.3bz) and PoE+
- Modular line-rate 10-GbE and 40-GbE ports for wireless aggregation

Aruba 2930M—The Aruba 2930M is available with either 24 or 48 1-GbE access ports with PoE+ (30W) on each port and either 4 SPF+ ports or 2 40-GbE ports on an optional expansion module. The 2930M is also available in a model with 40 1-GbE ports and 8 HPE Smart Rate ports capable of 1, 2.5, 5, or 10 GbE. The 2930M supports backplane stacking with up to 10 switches in a single stack and dynamic layer-3 services. This switch is designed for organizations wanting to create a digital workplace optimized for mobile users with an integrated wired and wireless access network. Features:

- Layer-3 switch with backplane stacking, tunnel node, ACLs, and robust QoS
- HPE Smart Rate for high-speed multi-gigabit bandwidth (IEEE 802.3bz) and up to 1440 W PoE+
- Modular 10-GbE or 40-GbE uplinks
- Models with 24 ports of HPE Smart Rate with IEEE 802.3bz

Aruba 2930F—The Aruba 2930F is available with either 24 or 48 1-GbE access ports and 370W PoE+. The switch supports Virtual Switching Framework (VSF), allowing you to stack up to 8 switches using available front ports. Although the 2930F supports basic layer-3 features, it is typically deployed as a layer-2 switch. This switch is ideal for organizations that have smaller access closets requiring only one or two switches, are looking for good performance, and who can accept a limited feature set in return for lower cost. Features:

- Layer-3 switch with VSF stacking, tunnel node, ACLs, and robust QoS
- Convenient built-in 1GbE or 10GbE uplinks and up to 740 W PoE+

Aggregation Switches

The aggregation layer provides connectivity for all access layer switches and connects to the branch gateways. The aggregation layer is responsible for layer-3 routing in this design, and it handles all traffic between networks on the LAN and traffic leaving the LAN for the WAN or the Internet. For high availability, the aggregation layer consists of a pair of switches acting as a single switch. If a switch fails or needs to be taken out of service for maintenance, the other switch continues forwarding traffic without interruption to the LAN services.

The following features are common across the aggregation switches:

- HPE Smart Rate for high-speed multi-gigabit bandwidth (IEEE 802.3bz) and PoE+
- Support for security and network management with Aruba ClearPass and Aruba Central
- REST APIs for the software-defined network

Aruba 5400R—The Aruba 5400R chassis supports a variety of interface modules that provide copper and fiber interfaces in different speeds and densities. The switch supports up to 96 10-GbE ports (SFP+ and 10GBASE-T), 96 HP Smart Rate Multi-Gigabit, or 288 1-GbE ports with PoE+. This switch is ideal for organizations that need to aggregate many access switches and might need to connect servers, firewalls, or other network appliances directly to the aggregation layer. The 5400R chassis includes the following features:

- Layer-3 modular switch with VSF stacking, static routing, RIP, OSPF, ACLs, robust QoS, policy-based routing, low latency, and resiliency
- Scalable line-rate 40GbE for wireless traffic aggregation

Aruba 3810M—The Aruba 3810M is available in a 16 port SFP+ and a two-module slot model. The module slots allow for an additional 8 SFP+ or 2 40-GbE ports. This switch is ideal for organizations with a small LAN who to aggregate 1 or 10-GbE connected access switches. The 3810 includes the following features:

- Layer-3 switch with backplane stacking, static routing, RIP, OSPF, ACLs, robust QoS, policy-based routing, low latency, and resiliency
- Modular line-rate 10-GbE and 40-GbE ports for wireless aggregation

For a complete list of Aruba Central-supported switches, see <u>Aruba Central Supported Switches</u>.

Wireless Components

With Aruba's controllerless model called *Instant*, there is no central controller and the controller functions are distributed among the APs. Instant is typically used in smaller networks or branch sites and scales up to 128 APs per cluster. In this design, we recommend deploying Aruba Instant with up to 50 APs. If you are planning to install more than 50 Instant APs, please contact an Aruba or partner SE/CSE for verification of your design.

Access Points

There are currently two series of Aruba access points: the latest generation 5xx series 802.11ax APs and the 3xx series 802.11ac Wave 2 APs. Details about currently available models are listed below; they support different throughput and client loads to meet different deployment needs.

The last digit in the model number denotes the antenna type. If the number is 4, then the AP has connectors for external antennas. If the number is 5, then the AP has internal antennas. For example, IAP-334 has external antennas and IAP-335 has internal antennas. In most office deployments, internal antenna models are preferred.

The following features are common across the current Aruba 5xx and 3xx APs:

- Unified AP for either controller-based or controllerless deployment modes
- Hitless PoE failover between both Ethernet ports (dual Ethernet models only)
- Built-in Bluetooth Low-Energy radio
- Advanced Cellular Coexistence to minimize interference from cellular networks
- Support for security and network management with Aruba ClearPass and Aruba Central
- Application visibility for QoS and traffic control
- Enhanced security with WPA3 and Enhanced Open

Aruba 5xx Series Access Point Options

The Aruba 5xx Series of campus access points support 802.11ax to efficiently and simultaneously serve multiple clients and traffic types in dense environments. These APs offer increased data rates for both individual device and overall system while delivering high performance and throughput in environments where mobile and IoT density is a growing concern.

Aruba 5xx common capabilities:

- Dual uplink ports with LACP support for redundancy and increased capacity
- Bluetooth 5 and Zigbee radios for location and IoT use-cases
- Green AP mode for energy savings up to 70%

Aruba 550 Series Access Points—The Aruba 550 Series APs are ideal for extreme high-density environments, such as public venues, higher education, hotels, and enterprise offices. The 550 series supports maximum data rates of 4.8Gbps in the 5GHz band and 1,150Mbps in the 2.4GHz band (for an aggregate peak rate of 5.95Gbps). The Aruba 550 series requires ArubaOS and Aruba InstantOS 8.5 software, and its features include:

- Dual-radio (8x8 + 4x4 MIMO)
- Optional tri-radio mode* with two 5GHz and one 2.4GHz radio (all 4x4 MIMO)
- Dual 5G HPE Smart Rate ports
- Al-powered features for wireless RF and client connectivity optimization
- Up to 1024 associated client devices per radio (recommended active 200) *

*Some 5xx features are not supported in the initial release but will be enabled in future software releases.

Aruba 530 Series Access Points—The Aruba 530 Series APs are ideal for very high-density environments, such as higher education, K12, retail branches, hotels, and digital workplaces. The 530 series supports maximum data rates of 2.4Gbps in the 5GHz band and 1,150Mbps in the 2.4GHz band (for an aggregate peak rate of 3.55Gbps). The Aruba 530 series requires ArubaOS and Aruba InstantOS 8.5 software, and its features include:

- Dual-radio (dual 4x4 MIMO)
- Dual 5G HPE Smart Rate ports
- Al-powered features for wireless RF and client connectivity optimization
- Up to 1024 associated client devices per radio (recommended active 200)*

*Some 5xx features are not supported in the initial release but will be enabled in future software releases.

Aruba 510 Series Access Points—The Aruba 510 Series APs are ideal for high-density environments, such as schools, retail branches, hotels, and enterprise offices. The 510 series supports maximum data rates of 2.4Gbps in the 5GHz band and 575Mbps in the 2.4GHz band (for an aggregate peak data rate of 2.975Gbps). The Aruba 510 series requires ArubaOS and Aruba InstantOS 8.4 software, and its features include:

- Dual-radio (4x4 + 2x2 MIMO)
- Single 2.5G HPE Smart Rate and Gigabit Ethernet uplink ports
- Up to 256 associated client devices per radio

Aruba 3xx Series Access Point Options

Aruba 340 Series Access Points—The Aruba 340 Series is the highest performance AP and supports HPE Smart Rate uplink, so it can use the full performance of 3.5 Gbps on two 5-GHz bands or 1.7 Gbps in the 5-GHz band and 800Mbps in the 2.4-GHz band, for a combined bandwidth of 2.5 Gbps. This model is ideal for organizations that require very high density and next-generation performance for auditoriums, high-density office environments, or public venues. The Aruba 340 series requires ArubaOS and Aruba InstantOS 8.3 software.

- Dual radio 4x4 802.11ac AP with MU-MIMO
- Optional dual 5-GHz mode supported, where the 2.4-GHz radio is converted to a second 5-GHz radio
- Antenna polarization diversity for optimized RF performance
- HPE Smart Rate and Gigabit Ethernet uplink ports with Link Aggregation Control Protocol (LACP) support for increased capacity
- Hitless PoE failover between both Ethernet ports

Aruba 330 Series Access Points—The Aruba 330 Series is a high-performance AP and supports HPE Smart Rate uplink, so it can use the full performance of 1.7 Gbps in 5-GHz band and 600Mbps in 2.4-GHz band for a combined bandwidth of 2.3 Gbps. This model is ideal for organizations that require high density and next-generation performance for auditoriums, high-density office environments, or public venues.

- Antenna polarization diversity for optimized RF performance
- HPE Smart Rate and Gigabit Ethernet uplink ports with LACP support for increased capacity
- Hitless PoE failover between both Ethernet ports

Aruba 310 Series Access Points—The Aruba 310 Series is a medium-performance AP that supports 1.7 Gbps in the 5GHz band and 300 Mbps in the 2.4-GHz band with a single Gigabit Ethernet uplink. This model is ideal for organizations that need to support medium-density environments, such as schools, retail branches, hotels, and enterprise offices that don't require multi-gigabit performance.

Aruba 300 Series Access Points—The Aruba 300 Series is an entry-level AP that supports 1.3 Gbps in the 5-GHz band and 300 Mbps in the 2.4-GHz band with a single Gigabit Ethernet uplink. This model is ideal for organizations with medium-density environments, organizations that want the latest technology but don't need the higher level of performance.

For a complete list of Aruba Central-supported Instant APs, see Aruba Central Supported Instant APs.

Deploying the SD-Branch

The Aruba SD-Branch design provides SD-WAN, wired, and wireless connectivity for branch users. The SD-WAN interconnects the corporate site with the remote-site locations, making it a critical part of the network. Modern WAN networks require a flexible and scalable design to support mission-critical applications and real-time multimedia communications from any location on the corporate network. Access to cloud-based services from each branch location is also critical to the success of keeping the network running as efficiently as possible.

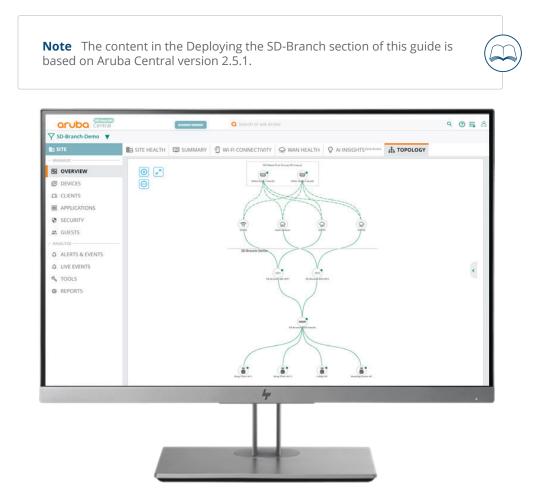
The SD-Branch design:

- Combines SD-WAN, wireless, and wired infrastructure with cloud-based orchestration
- Provides location-independent network access to improve employee and guest productivity
- Simplifies setup with zero-touch provisioning and plug-and-play branch deployment
- Provides wireless connectivity to hard-to-wire locations, eliminating the need for costly construction
- Simplifies configuring, managing, and operating, by using cloud-based controls

Simple, repeatable designs are easier to deploy, manage, and maintain. This design shows recommended deployment options and general guidance for which options to use.

ARUBA CENTRAL

Aruba Central is a cloud-based platform that enables you to configure, manage and monitor your Aruba SD-Branch network. Designed as a software-as-a-service subscription-based set of applications, Central provides a standard web-based interface that allows you to work on your network from anywhere. The hierarchical configurations provide operational efficiency; the monitoring and alerting streamlines day-2 operations, and the historical data reporting helps with auditing and troubleshooting.



Aruba Central Account Home Page

The Aruba Central account home page provides access to the Network Operations application, which is a dashboard for configuration, monitoring, reporting, and troubleshooting.

The home page also provides access to global settings. In this guide, we use the following global setting areas:

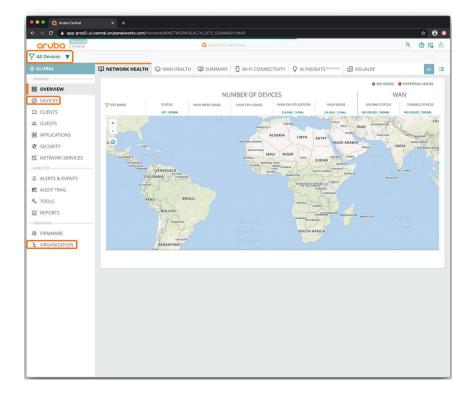
- Key Management
- Device Inventory
- Subscription Assignment

ACCOUNT HOME Manage your Network Inventory, Subscrip	tions, and User Access. Use any of the followi	ng apps to make Aruba work better for you.	
APPS			
Network Operations Manage your wired, wireless, and WAN infrastructure	ClearPass Device Insight Discover and Profile devices connected to the network		
GLOBAL SETTINGS			
USERS AND ROLES Manage user access	KEY MANAGEMENT Manage your subscription keys	DEVICE INVENTORY Manage the Dences in your invertory	
SUBSCRIPTION ASSIGNMENT Assign and modify device and service subscriptions	DATA COLLECTORS Manage on premoe data collectors	AUDIT TRAIL View audit-trail logs	
SINGLE SIGN ON Create and manage SAME. Profiles	API GATEWAY Access API Gateway and manage access tekens	WEBHOOKS Manage Webhook end pointes	

Aruba Central Network Operations App

The Aruba Central Network Operations app is the main application for configuring, monitoring, reporting, and troubleshooting your network. You use the navigation bar on the left to change the context of the main screen. In this guide, we focus on configuration and use the following areas:

- Filter drop-down list—Used to select the devices, groups, sites, or labels that you need to configure or monitor.
- Devices—Used to manage and configure access points, switches, and gateways.
- **Organization**—Used to manage groups, sites, and labels.



Groups are the parent level for a hierarchical network configuration. You use groups to apply common parameters to a group of devices.

Sites group all devices into a single location. You use sites to monitor devices, not to configure them.

Labels provide additional user-defined context for monitoring devices. You can assign a single device with up to five labels.

SD-BRANCH NETWORK CONFIGURATION OVERVIEW

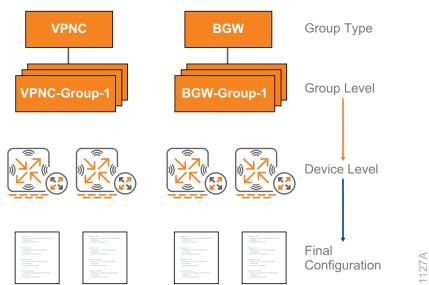


Figure 27 SD-Branch network configuration

To configure the SD-Branch network, you need to:

- 1. Verify that all devices are listed in the inventory and have licenses assigned to them.
- 2. Plan how you want to organize the device groups. We recommend that you keep the number of groups to a minimum. While a single group can be used to combine gateway, switching, and wireless configurations, keeping them separated can provide more flexibility for the assignment of configurations to the devices.
- 3. Configure the sites, data center, and remote. Sites represent the physical locations where you have installed the equipment.
- 4. Configure the VPNC groups and devices. When you implement redundant data centers, use one group per data center.
- 5. Bring the VPNC devices online. You can perform one-touch provisioning by using a console or you can use the local GUI to download the device's final configuration from Central.
- 6. Configure the branch device groups. In this guide, we use separate groups for branch gateways, switches, and APs.
- 7. Assign devices to sites and groups. You can complete this step by using the Install Manager app at the installation site (not covered in this guide) or you can allow your Central admin to assign them before installing the equipment.

8. Configure the branch devices. All branch devices support zero-touch provisioning when you use DHCP-assigned IP addresses. If you use static IP addresses, you can implement one-touch provision by using the GUI or you can use CLI to get the device online and connected to Central.

Note You must assign a group to a device prior to configuring the device.



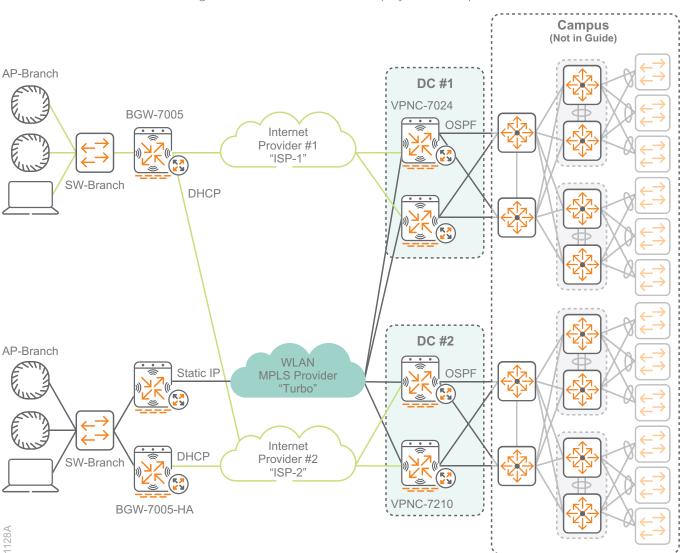


Figure 28 SD-Branch network deployment examples

Procedures

Preparing to Deploy the SD-Branch Network

- 1.1 Add Your Devices to the Device Inventory Manually
- 1.2 Configure the Device Subscription Keys
- 1.3 Assign Subscriptions to the Devices Manually
- 1.4 Define the Device Sites

We recommend that you complete the steps in this section prior to configuring the network devices.

1.1 Add Your Devices to the Device Inventory Manually

Aruba Central automatically adds each device you purchase to the device inventory in your Central account. You also have the option of manually adding a device by using the MAC address and serial number of the device. **Step 1:** On the Aruba Central Account Home page, select **Device Inventory**, and then click **Add Devices**.

DEVICE INVENTORY View the devices in your inventory and manually add devices here.
view the devices in your inventory and manually add devices here.
VIEW DEVICES
Approximation of the second secon
CP0025951 20:4C:03:12:6E:58 controller(Gateway) 192.168.1.203 Aruba7005 7005-US JW634A default ③
• CP0025992 20:4C03:12:6FA0 controller(Gateway) 10.8.255.200 7005-R511 7005-US JW634A BGW-Dual-INET 📀
• CP0025999 20:4C:03:12:6F:D8 controller(Gateway) 10.8.255.2 7005-R51 7005-US JW634A BGW-Single 🥥
• CP0026016 20:4C:03:12:70:60 controller(Gateway) 10.8.255.21 7005-R55-2 7005-US JW634A 8GW-Dual 📀
• CP0026019 20:4C:03:12:70:78 controller(Gateway) 10.8.255.22 7005-R52 7005-US JW634A BGW-Dual 🥥
• CP0041614 20:4C:03:2F:98:8C controller(Gateway) 10.8.255.23 7005-R55 7005-U5 JW634A BGW-Dual 🥥
• CP0041652 20:4C:03:2F:9A:34 controller(Gateway) 10.8.255.1 7005-R54 7005-U5 JW634A BGW-Single 🥥
• CP0044588 20:4C:03:2F:F8:C4 controller(Gateway) 10.8.255.20 7005-R52-2 7005-US JW634A 8GW-Dual 🥥
• CP0044594 20:4C:03:2F:F4:2C controller(Gateway) 10.8.255:40 7005-R53-2 7005-U5 JW634A BGW-Dual-4 🥥
• CP0044595 20:4C:03:2F:F7:DC controller(Gateway) 10.8.255.41 7005-R53 7005-US JW634A BGW-Dual-4 🥥
• CP0046727 20.4C:03:39:5D:0C controller(Gateway) 7005-USF1 JW636A - 0
• CP0046739 20:4C:03:39:51:7C controller(Gateway) 7005-USF1 JW636A O
• CP0046977 20:4C:03:39:5F:94 controller(Gateway) 7005-USF1 JW636A - O
• CP0047911 20:4C:03:39:85:24 controller(Gateway) 107.15.154.110 Aruba7005 7005-US JW634A default 🥥
• CP0047912 20.4C:03:39:73:1C controller(Gateway) 10.8.255.242 7005-R512 7005-US JW634A BGW-Single-N 🥥
• CP0047915 20:4C:03:39:7B:EC controller(Gateway) 7005-US JW634A 🥥
• CP0048213 20:4C:03:39:76:94 controller(Gateway) 7005-US JW634A ⊘

Step 2: In the Add Devices dialog box, enter the serial number and MAC address for each device that you need to add to the device inventory list, and then click **Done**.

ADD DEVIC Add up to 4 devices by enter device	CES ring the Serial Number and MAC Address for each
SERIAL NUMBER	MAC ADDRESS
	Done

You can also use this page to assign new and offline devices to configuration groups.

1.2 Configure the Device Subscription Keys

After you have added the devices to the inventory, you need to add subscription keys for the devices so you can configure and manage them in Aruba Central.

Aruba provides several subscription options. For more information, see the Aruba SD-WAN Ordering Guide.

Step 1: On the Aruba Central Account Home page, select **Key Management**.

 ● ● ● ● Aruba Central ← → C ● portal-prod2.cent 	× + tral.arubanetworks.com/platform/frontend/			x ∔ 0	:		
Orubo Central				() III /	8		
	OUNT HOME e your Network Inventory, Subscriptions	, and User Access. Use any of the following a	ipps to make Aruba work better for you.				
APP	s						
3	Network Operations Metwork Operations Metwork wreles, and WAN infrastructure	ClearPass Device Insight Discover and Profile devices connected to the network					
	LAUNCH	LAUNCH					
GLO	GLOBAL SETTINGS						
USE	RS AND ROLES	KEY MANAGEMENT Manage your subscription keys	DEVICE INVENTORY Manage the Dences in your inventory				
SUB	SCRIPTION ASSIGNMENT and modify device and service subscriptions.	DATA COLLECTORS Manage on premise data collectors	AUDIT TRAIL View audit-trail tops				
SINC	GLE SIGN ON and manage SAML Profiles	API GATEWAY Access AR Gateway and manage access tokens	WEBHOOKS Manage Vyeshook and points				

Step 2: In the **Key Management** dialog box, enter your subscription key, and then click **Add Subscription**.

KEY MANAGEMENT View and manage your subscription keys here. When you order new subscription keys, Aruba sends an email containing the keys to the
address listed on the order.
Already received your ARUBA Central subscription key? Add the subscription key to activate your account now! SUBSCRIPTION KEY ADD SUBSCRIPTION

Note The Key Management page also displays the status and expiration dates for existing licenses.

1.3 Assign Subscriptions to the Devices Manually

After adding your subscription keys, you must assign a subscription to each device for configuration and management. Central allows you to automatically assign device licenses by using the Auto Subscribe option.

Alternatively, you can manually assign subscription keys to gateways by using the following steps:

Step 1: On the Aruba Central Account Home page, select Subscription Assignment.

Step 2: In the Gateway Subscriptions section, select a gateway.

Step 3: In the Assignment column for the gateway, select a subscription from the drop-down list to assign it to the gateway.

A GO TO ACCOU					
	PTION ASSIGNM				
Use the options belo	ow to assign Foundation and Net	work Service subscriptions to	devices.		
DEVICE SUBSCR					
A device manageme	nt subscription entitles the subs	tribed device to be managed	in Aruba Central and	l enables most functionality.	
Auto Subsc You must select	ribe OFF devices beice to assign subscriptions to the	em			
DEVICES (0 TO I	BE SUBSCRIBED 0 TO BE	UNSUBSCRIBED)			
	♥ SERIAL NUM		C ADDRESS	Y MODEL	
YES	CV0016892	00:14	:1E:05:0E:70	7210-US	
🖬 YES	CNDDJSSTDQ	20:46	i:CD:C0:38:D6	IAP-305-US	
YES	CNDDJSSTDX	20:A6	i:CD:C0:38:E2	IAP-305-US	
MES YES	CNHLK9W0P	x 00:4E	:35:C4:9A:5E	AP-535-US	
YES YES	CN93HKZ48Y	38:21	:C7:BA:F0:00	2930F	
N0	CP0047912	20:40	:03:39:73:10	7005-US	
N0	CK0234513	40:E3	:D6:C1:34:6C	IAP-215-US	
NO NO	CT0338957	94:84	1:0F:C6:58:18	IAP-225-US	
DEVICE ASSIGNMEN	muties the subscribed Gateway d			BCODITIONS	
			\		
APPER AND APPER	SERIAL NUMBER	Y MAC ADDRESS		GROUP	
ASSIGNMENT		001415050575			
Unassigned	CV0016892 CP0047912	00:1A:1E:05:0E:70	7210-US	R/SW/Single Nation	
Unassigned Foundation	♥ CP0047912	20:40:03:39:73:10	7210-US 7005-US	BGW-Single-Nelson default	- i -
Unassigned Foundation Foundation	♥ CP0047912		7210-US	BGW-Single-Nelson default	1
Unassigned Foundation	CP0047912 CP0047911	20:4C:03:39:73:1C 20:4C:03:39:85:24	7210-US 7005-US 7005-US		1
Unassigned Foundation Foundation Unassigned	CP0047912 CP0047911 CP0002586	20:40:03:39:73:10 20:40:03:39:85:24 00:08:86:88:92:48	7210-US 7005-US 7005-US 7005-US	default	ł.
Unassigned Foundation Foundation Unassigned Foundation	CP0047912 CP0047911 CP002586 CP0025951	20.4C:03:39:73:1C 20:4C:03:39:85:24 00:08:86:88:92:48 20:4C:03:12:68:58	7210-US 7005-US 7005-US 7005-US 7005-US	default	ł
Unassigned Foundation Foundation Unassigned Foundation Foundation	CP0047912 CP0047911 CP0047911 CP002586 CP0025951 CP0001664	20:4C:03:39:73:1C 20:4C:03:39:35:24 00:08:86:88:92:48 20:4C:03:12:56:58 00:08:86:88:75:78	7210-US 7005-US 7005-US 7005-US 7005-US 7005-US	default	
Unassigned Foundation Unassigned Foundation Foundation Foundation	CP0047912 CP0047911 CP002586 CP0025951 CP000564 CP0047915	20.4C0339731C 20.4C03398524 000886895248 20.4C0312.6E58 00.08.8687578 20.4C0319788C	7210-US 7005-US 7005-US 7005-US 7005-US 7005-US 7005-US	default	

Step 4: Click Go To Account Home.

1.4 Define the Device Sites

Aruba Central uses sites to organize devices by the geographical locations in which you install them.

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

Step 2: In the filter drop-down list, select **All Devices**.

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

Step 4: On the Sites and Labels tab, click New Site.

aruba Central		Q Se					۹ 🔿 👯
All Devices 🔻							
GLOBAL	🛱 GROUPS 📿	SITES AND LABELS	CATES 🔝 INSTALL MANA	AGER			
MANAGE							
8 OVERVIEW	SITES AN	ID LABELS					
DEVICES	Labels are logical	sets of devices which can be use	d for a variety of monitorin	g and reporting p	urposes. Each d	evice can be asso	ciated with up to five
CLIENTS		can apply to as many devices as					
GUESTS	Sites allow you to	group devices based on the locat	ion context.				
APPLICATIONS	MANAGE SITE	The second s					
SECURITY		DEVICES TO ADD TO A SITE PLE DEVICES SHIFT+CLICK OR CTRI	+CLICK			Labels	Sites
NETWORK SERVICES	CONVERT LABEL		- CLICK				
NALYZE							
ALERTS & EVENTS	SITE NAME		DEVICE COU		∀ NAME	∀ GROUP	∀ TYPE
AUDIT TRAIL	ALL DEVICES		35		RS11-2930F	SW-Branch	SWITCH
TOOLS	UNASSIGNED		8		RS15-2930F-1	BGW-Dual-RS	SWITCH
REPORTS	Data Center #2	7025 Kit Creek Road	2		RS15-2930F-1	BGW-Dual-RS	SWITCH
INTAIN	HQ Roseville	8000 Foothills Blvd	2		R53-2930F	SW-Branch	SWITCH
FIRMWARE	Remote Site 1	1234 Any Street	2		RS12-2930F	SW-Branch	SWITCH
ORGANIZATION	Remote Site 11	9999 Forest Lake Drive	2		20:a6:cd:c0:3	default	IAP
ORGANIZATION	Remote Site 12	1122 Inlet View Drive	3		20:a6:cd:c0:3	AP-Branch	IAP
	Remote Site 15	11137 Bayberry Hills Drive	7		20;a6;cd;c0;3,	AP-Branch	IAP
	Remote Site 2	5678 Main Street	4	5946	38:17:c3:c0:5	AP-Branch	IAP
	Remote Site 3	1122 South Lane	3	DRAG	R\$15-AP-515-1	BGW-Dual-RS	IAP
	Remote Site 4	3344 North Street	1		RS15-AP-515-2	BGW-Dual-RS	IAP
	Remote Site 5	31753 Bretton Road	1		R\$12-555-1	AP-RS12	LAP
					RS15-AP-555-1	BGW-Dual-RS	IAP
					JW634A-20:4	BGW-7005	Gateway
					R\$15-7005-1	BGW-Dual-RS	Gateway
					RS11-7005	BGW-7005	Gateway
					R\$1-7005	BGW-7005	Gateway
					JW634A-20:4	BGW-7005-HA	Gateway

Step 5: In the Create New Site dialog box, implement the following settings:

- Site Name—New Site
- Street Address—123 Street
- City—Santa Clara
- County—United States
- State or Province—California
- Zip/Postal Code—95054

Step 6: Click Add.

CREATE NEW SITE
SITE NAME
New Site
123 Street
СІТҮ
Santa Clara
United States
California
ZIP/POSTAL CODE
95054
Add

Procedures

Configuring the VPNC Group

- 2.1 Create a New VPNC Group
- 2.2 Select the Hardware Model of the VPNC Group
- 2.3 Set the VPNC Group System Time Parameters
- 2.4 Select a DNS Server for the VPNC Gateway
- 2.5 Create a Management User Account
- 2.6 Create VLANs for Each Ethernet Port
- 2.7 Assign the VLANs to the LAN Ports
- 2.8 Enable Tunnel Orchestrator Peering
- 2.9 Configure the Overlay Routing

Aruba Central uses a two-level hierarchy for configuration tasks. A device's final configuration is a combination of the group configuration along with the device-specific configuration. Aruba recommends that you create groups for devices that have similar deployment parameters and that you use groups for most device configuration. You configure device-specific configurations, like IP addresses and routing, at the VPNC device level. Aruba recommends that you fully configure the gateways at the group and device level before connecting to the network to prevent partial configurations from creating connectivity issues .

2.1 Create a New VPNC Group

Use this procedure to create a group and assign it to the VPNC group type. Use one group per data center.

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

Step 2: In the filter drop-down list, select All Devices.

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

Step 4: On the Groups tab, click New Group.

ROUPS oup in Aruba Centr		2 CERTIFICATES	I INSTALL MANAGER	2				
ROUPS oup in Aruba Centr		CERTIFICATES	INSTALL MANAGER	ę				
oup in Aruba Centr	al acts like a pri							
oup in Aruba Centr	al acts like a pri							
		imany configuration	n container for device	s. You can combine dev	ices with co	mmon configurati	ion requirements into a	
e group and apply t			all the devices in the g		ices widt co	inition configuration	on requirements into a	
NAGE GROUPS	5							
		HES BETWEEN GROP	UPS					
ELECT MULTIPLE DE	VICES SHIFT+CLI	ICK OR CTRL+CLICK						
			1.221012.21	En	1	Income of	1	
	595							
				Sacramento,Unite				1
				Sarramento Linite				
	1	13 (500 000)						143
	G AND DROP CLUST	G.AND DADP CLUSTES AND SWITCH ELECT MULTIPLE DEVESSIFIET CLU OUP NAME DEVESS SIGNARD DEVIL 2 SIGNARD DEVIL 2 2330F.Single 2 2330F.Single 2 2330F.Single 2 2330F.Single 2 2330F.Single 2 2030F.Single 2 2030F.Single 2 POLIA 4 POLIA 2 POLIA 2 POLIA 2 POLIA 3 POLIANTET 3	G AND DRP CLUSTES AND SHITH-IS BETWEEN CRID ELECT MULTIFLE DEVICES SHIFT-CLUCK OR CTRL-CLUCK COMMENTO DEVICES COMMENTO DEVICES 2007-Single 2 23057-Single 2 23055-Single 2 23055-Single 2 23055-Single 2 23055-Single 2 2004 4 4 0-0-0-14 2 2004 1 2 0-0-0-14 3 3 0 0-0-0-14 3 3 0 0-0-0-14 3 0 0-0-0-14 3 0 0-0-0-14 3 0 0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0	G AND DONC CLUSTERS AND SNITCHES EXTINCENT CROUPS ELECT MULTIPLE DEVICES SNIFTCHES EXTINCENT CROUPS CONNECTED EVIL 24 2007 NUME DEVICES 23007 Sniple 2 23007 Sniple 2 23007 Sniple 2 23004 Status 4 2004 Status 4 2005 Status 4 2005 Status 4 2005 Status 4 2005 Status 4 2005 Status 4 2005 Status 4 2006 Status 4 20	GAND DROP CLUSTERS AND SMITCHES BETWEEN GROUPS ELECT MULTIFLE DENCES SHIT-LICK ORC CTRL-CLOCK VILME VILCOLTON CONNECT DROVE 2 2006-R512 Springunited Soles SSIGNED DRVENS 0 2006-R512 Springunited Soles 2006 Signer 2 2006-R52 Springunited Soles 2006 Signer 2 2006-R52 - 2006 Signer 2 2006-R52 - Poulid 2 2006-R52 - Poulid 2 3006-R53 - Poulid 3 3010-R51 Secremento_Unitia	GAND DROP CLUSTERS AND SWITCHES BETWEEN GROUPS ELECT MULTIFLE DEVICES SHITCHCLOCK OF CITAL-CLUCK CONNECTE DAVIE 2 2007-MILE DEVICE 2 2007-SNIE	GAND DROP CLUSTES AND STRUCTURES EXTYRETED GROUPS BLECT MULTIPLE DEVICES SHEFT-CLUCK ON CTRL+ CUCK COMULTION DEVICES COMULTION DEVICES Station Station DEVICES 23005 Single 2 20005 Single 3 3 20005 Single 3 3 Single(Single) <th< td=""><td>GAND DROP CLUSTERS AND SWITCHES RETWEEN GROUPS ELECT MULTIFIC DEVECTS SHIT-LCUCK OF CIFE/CLUCK VIANE VI</td></th<>	GAND DROP CLUSTERS AND SWITCHES RETWEEN GROUPS ELECT MULTIFIC DEVECTS SHIT-LCUCK OF CIFE/CLUCK VIANE VI

Step 5: In the Create New Group dialog box, implement the following settings:

- Group Name—VPNC-7210
- Switch—Unselect
- Password—password
- Confirm Password—password

Step 6: Click Add Group.

CREATE NEW GROUP	×
CROUP NAME VPNC-7210	
Use the group as Template group by selecting the device i IAP AND GATEWAY Group password settings i PASSWORD	
CONFIRM PASSWORD	
Cancel Add Group	

Step 7: In filter drop-down list, select the group you created in Step 5.

Step 8: In the left navigation pane, in the Manage section, select **Devices**.

Step 9: Select the **Gateways** tab, and then click the gear icon in the upper right corner.

🗢 🗢 💿 Aruba Central	× +				
← → C 🔒 app-prod2-ui.	central.arubanetworks.com/front	tend/#/GATEWAY/LIST			아 ☆ ± 은 :
aruba Central		Q :	learch or ask Aruba		۵ 🛯 🚜
▼ VPNC-7210 ▼					
1 GROUP	ACCESS POINTS		YS		💷 ıl. 🛞
- MANAGE			_		
88 OVERVIEW	GATEWAYS . UP	O DOWN			
	0 0	0			
E& CLIENTS	GATEWAYS				₹ ⊖
A GUESTS		IF MODEL	FIRMWARE VERSION	UPTIME	IP ADDRESS
# APPLICATIONS					
SECURITY					
- ANALYZE					
ALERTS & EVENTS					
AUDIT TRAIL					
TOOLS					
REPORTS					
- MAINTAIN					
FIRMWARE					
			No data to display right no	v	

Step 10: In the Set Group Type dialog box, select VPNC, and then click Save Settings.

						ave a mix of Gat	eway and VPNC devic
Group is configured	_		/PNC group the	en it cannot be	e changed.		
Branch Gateway		VPNC					

For educational purposes, the next step exits the guided setup.

Step 11: Click Cancel, and then click Exit.

EXIT G	UIDED SETUP
A	Guided Setup will be exited and changes will be lost. You can re-enter the Guided Setup at any time to complete it.
	RESUME

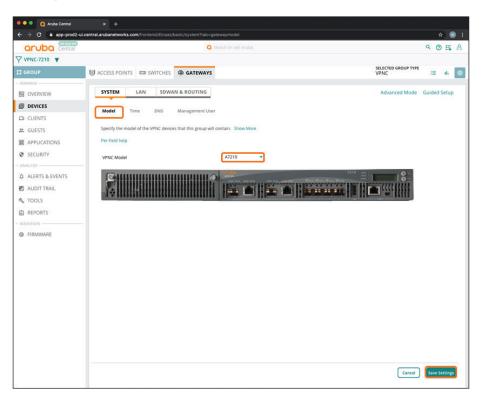
2.2 Select the Hardware Model of the VPNC Group

You can have only one VPNC gateway model per group.

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

Step 2: In the **VPNC Model** drop-down list, select the hardware model for the VPNC gateway group (example: **A7210**).

Step 3: Click Save Settings.



2.3 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.

orubo Central			Q Searc						9 6	0 11	ക
VPNC-7210 ¥								SELECTED GROUP TYPE			
GROUP	ACCESS POINTS	SWITCHES						VPNC	:=	16	6
MANAGE	SYSTEM	LAN SDW/	AN & ROUTING								_
8 OVERVIEW	STSTEM	3044	IN & ROOTING					Advanced Mode	Guided	setup	1
DEVICES	Model Tim	e DNS	Management User								
b CLIENTS		_									
& GUESTS		ay in the group w	III automatically obtain its t	ime using the Netw	ork Time Proto	ocol (NTP). You can ei	ther select one or	more public NTP service	Show M	lore	
APPLICATIONS	Per-field help										
SECURITY	Public NTP Ser	vers			+						
INALYZE	IPV4 ADDRESS/FQ	DN	BURST MODE								
ALERTS & EVENTS											
AUDIT TRAIL			No data to display								
TOOLS											
REPORTS											
MAINTAIN											
FIRMWARE	Timezone	Choose	e a timezone								

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

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

Step 5: In the **Timezone** drop-down list, choose your time zone, and then click **Save Settings**.

PUBLIC NTP SERVERS			+
IPV4 ADDRESS/FQDN	BURST MODE		
pool.ntp.org			
Timezone	Primary: Etc/GMT-7 (UTC+07:00)		
		Cancel	Save Settings

2.4 Select a DNS Server for the VPNC Gateway

 → C 	k.contral.arubanetworks.com/frontend/#/caas/basic/system?tab×dns	* (
aruba Central	Q Search or ask Aruba	۹ 🔿 🔢
VPNC-7210 🔻		
GROUP	🗑 ACCESS POINTS 📼 SWITCHES 🙊 GATEWAYS	i= 4.
MANAGE	SYSTEM LAN SDWAN & ROUTING Advanced Mode	
OVERVIEW	SYSTEM LAN SDWAN & ROUTING Advanced Mode	Guided Setup
B DEVICES	Model Time DNS Management User	
Th CLIENTS	Each branch gateway in the group requires Domain Name System (DNS) configuration to be able to successfully resolve FQDNs and be able communicate with cloud services such as Aruba	Show More
GUESTS	Each branch gateway in the group requires Domain Name System (DNS) contiguration to be able to successfully resolve FQDNs and be able communicate with cloud services such as Aruba Per-field help	anow more
APPLICATIONS		
SECURITY	Specify DNS servers Elearn DNS configuration from ISP	
ANALYZE ALERTS & EVENTS		
audit trail		
TOOLS		
REPORTS		
MAINTAIN		
FIRMWARE		

You must specify the DNS server(s) that the VPNC gateway uses to communicate to Aruba 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 gateway VPNC, leave the default DNS provided by the cloud provider and go to Step 6.

Step 5: In the **Provider** drop-down list, pick one of the providers listed or select **Alternate DNS** if the desired server is not in the list.

Step 6: Click Save Settings.

Specify DNS servers	O Learn DNS configuration from ISP	
Domain name (Optional)	example.local	
Public DNS Servers		+
PROVIDER	IPV4 ADDRESS	
Google	8.8.8.8.8.4.4	
		Cancel Save Settings

2.5 Create a Management User Account

You must have a management user account to use 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.

	central.arubanetworks.com/fr	or restroy my case of passicle									* 8	9 8
aruba Central			Q							9 6	0	6
▼ VPNC-7210 ▼									SELECTED GROUP TYP			_
C GROUP	ACCESS POINTS	SWITCHES	GATEWAYS						VPNC	=	4.	۲
MANAGE	SYSTEM LA	N SDWAN & F	OUTING						Advanced Mode	Guided	Setup	
BB OVERVIEW									Nuvanceu moue	Guideo	Secup	
DEVICES	Model Time	DNS Man	agement Use									
Eb CLIENTS				-								
& GUESTS		r remotely access the	CLI console of	the gateways in	the group, yo	u must eit	her configure eit	her a local mana	gement user or enable	Show M	ore	
APPLICATIONS	Per-field help											
SECURITY												
ANALYZE	AAA authentication											
ALERTS & EVENTS	Local manageme	nt users				+						
AUDIT TRAIL	NAME	ROLE		PASSWORD		_						
TOOLS												
REPORTS		No	data to display									
MAINTAIN												
G FIRMWARE												

Step 3: In the Add Management User table, implement the following settings:

- Name—admin
- Password—password
- Retype Password—password

Step 4: Role—Super user role

Step 5: Click Save.

Add management user	
Name	admin
Password	
Retype Password	
Role	Super user role 🔻

Step 6: Click Save Settings.

2.6 Create VLANs for Each Ethernet Port

Step 1: On the Gateways tab, in the LAN section, select **VLANs**.

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

		in the state of the state of	basic/lan?tab=virtual					e (
aruba Central				O Search or ask Aruba			۹ ()	
7 VPNC-7210 🔻						SELECTED GROUP TYP		
GROUP	ACCESS POINTS	SWITCHES	GATEWAYS			VPNC		4
MANAGE	SYSTEM	LAN SDW/	N & ROUTING			Advanced Mode		
OVERVIEW	313161	DAN SDW	a a Rooting			Advanced Mode	Guided	setup
DEVICES	VLANS LAP	V Ports						
E& CLIENTS								
CUESTS		require one or mo	e LAN VLANs and IP I	nterfaces to support infrastructure an	d client devices in your branches. E	ach VLAN will either be statically or	Show Mo	re
# APPLICATIONS	Per-field help							
SECURITY	VLANs					+		
ANALYZE	VLAN ID		NAME	IPV4 ADDRESS	NETMASK			
ALERTS & EVENTS								
AUDIT TRAIL				No data to display				
TOOLS								
REPORTS								
MAINTAIN								
FIRMWARE								

Step 3: In the New VLAN dialog box, implement the following settings:

- Name—**GE_0_0_0**
- VLAN ID-100

Step 4: Click Save.

Step 5: Repeat Step 2 - Step 4 for each VPNC port you intend to use.

New VLAN	
Name	GE_0_0_0
VLAN ID	100
IPV4 ADDRESS (Optional)	
Netmask (Optional)	
	Cancel Save

Step 6: Verify the VLAN information in the summary table, and then click **Save Settings**.

VLAN ID	NAME	IPV4 ADDRESS	NETMASK	
			Records to the second second	
100	GE_0_0_0			
101	GE_0_0_1			
102	GE_0_0_2			
103	GE_0_0_3			
				Save Settings

2.7 Assign the VLANs to the LAN Ports

Step 1: On the Gateways tab, in the LAN section, select **LAN Ports**.

Step 2: In the LAN ports/port channel table, click the plus (+) sign.

aruba Central				Q Search or ask A					0	0	<u>۾</u>
VPNC-7210 🔻								SELECTED GROUP TYPE			
SROUP	ACCESS POINTS	SWITCHES	A GATEWAYS					VPNC		4.	۲
OVERVIEW	SYSTEM	LAN SDWA	N & ROUTING					Advanced Mode	Guide	d Setu	p
DEVICES											
CLIENTS	VLANS LA	N Ports									
GUESTS	LAN VLANS can b	e assigned to one or	r more ports on your	gateways in the grou	up. The gateway por	ts that are available fo	or assignment in this step v	vill be dependent on the	Show I	Aore	
APPLICATIONS	Per-field help										
SECURITY	LAN ports/po	rt channel					+				
IALYZE	NAME	PORT	MODE	ACCESS VLAN	NATIVE VLAN	ALLOWED VLANS					
ALERTS & EVENTS											
AUDIT TRAIL			,	No data to display							
TOOLS											
REPORTS											
FIRMWARE											

Step 3: In the New LAN port/port channel dialog box, implement the following settings:

- Name—WAN_Uplink1
- Port—GE-0/0/0
- Access VLAN—100:GE_0_0_0

Step 4: Click Save.

Step 5: Repeat Step 2 - Step 4 for each VPNC port you intend to use.

New LAN port / portchannel	
Name	WAN_Uplink1
Port	GE-0/0/0
VLAN mode (Optional)	Access 🔹
Access VLAN (Optional)	100 : GE_0_0_0 🔻
	Cancel

Step 6: Verify the port information in the summary table, and then click Save Settings.

LAN ports/port channel								
NAME	PORT	MODE	ACCESS VLAN	NATIVE VLAN	ALLOWED VLANS			
WAN_Uplink1	GE-0/0/0	access	100					
WAN_Uplink2	GE-0/0/1	access	101					
LAN_Uplink1	GE-0/0/2	access	102					
_AN_Uplink2	GE-0/0/3	access	103					

2.8 Enable Tunnel Orchestrator Peering

In this procedure, you enable SD-WAN overlay orchestrator peering to automate tunnel establishment.

Step 1: On the Gateways tab, in the SDWAN & Routing section, select SD-WAN Overlay.

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

🔍 🔍 🔍 🧕 😋 Aruba Central	× +	
← → C a app-prod2-ui.c	central.arubanetworks.com/frontend/#/caas/basic/vpnrouting?tab=sdwanoverlay	x 🚯 :
aruba Central	Q Search or ask Aruba	۹ 🔊 📖 🖁
▼ VPNC-7210 ▼		
🗱 GROUP	The switches GATEWAYS SELECTED GROUP TYPE VPNC	ii 11. 🛞
- MANAGE		
88 OVERVIEW	SYSTEM LAN SDWAN & ROUTING Advanced Mode	Guided Setup
DEVICES	SD-WAN Overlay Static Routing Route Maps Overlay Routing	
LT CLIENTS	and the stand start webs are indicated in and the start of the start o	
& GUESTS	Overlay Orchestrator Peering	
# APPLICATIONS		
SECURITY		
- ANALYZE		
ALERTS & EVENTS		
AUDIT TRAIL		
S TOOLS		
REPORTS		
- MAINTAIN		
FIRMWARE		
	Cancel	Save Settings

2.9 Create a New Route Map

(Optional)

Use this procedure to create a route map. You can use this route map to control redistribution of specific overlay prefixes into OSPF.

Step 1: On the Gateways tab, in the SDWAN & Routing section, select Route Maps.

Step 2: On the Route Maps page, expand **Route Maps** to display the route maps table.

Step 3: In the Route maps table, click the plus (+) sign.

🗧 🔍 🔍 💽 Aruba Central	× +	
← → C app-prod2-ul	.central.arubanetworks.com;frontend/#/caas/basic/vpnrouting?tab=routemaps	\$ 🖲 E
aruba Central	Search or ask Aruba	۹ 🛛 📖 🖁
▼ VPNC-7210 ▼		
🛱 GROUP	🗑 ACCESS POINTS 💷 SWITCHES 🙊 GATEWAYS	
- MANAGE		
88 OVERVIEW	SYSTEM LAN SDWAN & ROUTING Advance	ed Mode Guided Setup
	SD-WAN Overlay Static Routing Route Maps Overlay Routing	
CLIENTS		
🔐 GUESTS	Configure route maps and prefix rules which can be used for in any of the routing protocols (OSPF, BGP or overlay). Show More	
# APPLICATIONS	Per-field help	
SECURITY	> Community List Rules	
- ANALYZE	> Prefix Lists	
ALERTS & EVENTS	v Route Maps	
M AUDIT TRAIL		
S TOOLS	Route Maps	
REPORTS	NAME SEQUENCE ACTION MATCH SET	
- MAINTAIN		
FIRMWARE	No data to display	
3		

Step 4: In the Add/Edit Route map dialog box, implement the desired filters. This example permits all prefixes:

- Name—RM_All
- Sequence number—1
- Action—Permit

Step 5: Click Save.

dd/Edit Route map		
Name	RM_AII	
Sequence number	1	
Action	Permit 🝷	
Match		+
ТҮРЕ	VALUE	
Set		+
ТҮРЕ	VALUE	
	No data to display	
		Cancel

2.10 Configure the Overlay Routing

Use this procedure to redistribute OSPF routes into the overlay so that branches can reach corporate prefixes.

Note Aruba SD-WAN automatically translates routing costs between the overlay and data center to ensure symmetry. For more information, see the Aruba SD-WAN Orchestrator tech note.

Step 1: On the Gateways tab, in the SDWAN & 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.

••• C Auda Contral x +				
🗲 🔿 🕐 🔹 app-prod2-ui.central.arubanetworks.com/frontend/#/casa/basic/vprrouting?tab=overlayvprogroup	ľ.,	*	=r (1
Central Q Search or ask Aruba		a (a
∇ VPNC-7210 ▼				
ti group 🔯 access points 📼 switches 🙊 gateways	JP TYPE	:=	16	۲
- MANA55				
88 OVERVIEW SYSTEM LAN SDWAN & ROUTING Advanced 1	Mode (suided	Setup	
DEVICES SD-WAN Overlay Static Routing Route Maps Overlay Route Maps				
C CLIENTS				
# GUESTS This page allows you to configure the Overlay Routing Protocol in order to exchange routes between Branch Gateways and VPNCs connected to the Overlay Orchestrate	ar. Show I	More		
APPLICATIONS Per-field help				
SECURITY Redistribution				
- ANALYZE REDISTRIBUTION RULES +				
ALERTS & EVENTS SOURCE PROTOCOL FILTER ROUTE MAP				
AUDIT TRAIL				
TOOLS No data to display				
E REPORTS				
- MAINTAIN				
FIRMWARE				
> Data Center Aggregate Routes				

Step 4: In the Source Protocol drop-down list, select **OSPF**. Static, connected, and BGP routes are also supported but not shown in this example.

Step 5: In the Filter drop-down list, select **Intra Area**, **Inter Area**, **External Type-1**, and **External Type 2** if all types of OSPF routes need to be redistributed.

Step 6: In the Route Map drop-down list, select the new route-map you created in Procedure 2.9 (Example: **RM_AII**).

Step 7: Click Save Settings.

Redistribution rules			+
SOURCE PROTOCOL	FILTER	ROUTE MAP	
OSPF 🗸	Intra Area		
	Inter Area		
	External Type-1		
	External Type-2		
Data Center Aggregat	e Routes	Canc	el Save Setting

Step 8: On the Gateways tab, in the SDWAN & Routing section, select Overlay Routing.

Step 9: On the Overlay Routing page, expand **Data Center Aggregate Routes** to display the DC Aggregate Routes table.

Step 10: Unselect **Allow branch to branch**. Clear this option to send only the data center summary route and not send specific prefixes from other branches.

	il.central.arubanetworks.com/trontend/#/caas/basic/vpnrouting?tab=overlayvpncgroup	* 😁 :
	Q Search or ask Aruba	۹ 🛛 📖 👌
NC-7210 ¥		SELECTED GROUP TYPE
OUP	ACCESS POINTS SWITCHES R GATEWAYS	VPNC III II.
AGE	SYSTEM LAN SDWAN & ROUTING	Advanced Mode Guided Setup
DEVICES		
LIENTS	SD-WAN Overlay Static Routing Route Maps Overlay Routing	
GUESTS	This page allows you to configure the Overlay Routing Protocol in order to exchange routes between Branch Gateways and VPNCs connected to the	e Overlay Orchestrator. Show More
PPLICATIONS	Per-field help	
ECURITY	> Redistribution	
YZE	✓ Data Center Aggregate Routes	
LERTS & EVENTS	Allow branch to branch	
UDIT TRAIL		
OOLS	DC Aggregate Routes +	
REPORTS	IP ADDRESS MASK	
ITAIN	- No data to display	
IRMWARE		

Step 11: In the **DC Aggregate Routes** table, click the plus (+) sign to create a new aggregate route. We use 10.0.0.0/8 in this example to represent corporate prefixes.

Step 12: In the IP Address column, enter 10.0.0.0, and then in the Mask column, enter 255.0.0.0.

Step 13: Click Save Settings.

The example in the screenshot below aggregates all OSPF routes into the overlay by using a single 10.0.0.0/8 prefix.

~	Data Center Agg	regate Route	s			
	Allow branch to branc	h				
	DC Aggregate Rou	tes			+	
	IP ADDRESS		MASK			
	10.0.0.0		255.0.0.0)		
				Cancel	Save Settings	

Procedures

Configuring the VPNC Devices

- 3.1 Assign a VPNC Device to a Group
- 3.2 Initiate the VPNC Device Configuration
- 3.3 Configure the IP Address for the VPNC Device
- 3.4 Assign a Hostname to the VPNC Device
- 3.5 Assign IP Addresses to the VLANs
- 3.6 Configure the WAN Providers
- 3.7 Configure the Default Route to the Internet
- 3.8 Configure OSPF Routing to the LAN
- 3.9 Enable One-Touch Provisioning on the VPNC Device

Repeat this set of procedures for each VPNC.

3.1 Assign a VPNC Device to a Group

In this procedure, you assign the VPNC device(s) to a group. Use one VPNC group per data center.

Step 1: On Aruba Central Account Home page, select **Device Inventory**.

Step 2: In the View Devices table, select the VPNC gateways, and then click **Assign Group**.

GO TO ACCO	DUNT HOME								
DEVICE I	NVENTO	RY							
			devices have						
view the devices i	n your inventory an	d manually add	devices here.						
VIEW DEVICE	s								
▼ SERIAL NUM		TYPE	IP ADDRESS	NAME	WODEL	PART NUMB	GROUP	▼subscr =	
CV0016872	00:1A:1E:05:01:28	controller(G	-		7210-US	JW744A	-	- 8	
CV0016870								100 L.	
CNHJKD58Y6	F4:2E:7F:C7:8E:B8	lap	10.8.56.107	RS15-AP-515-2	AP-515-US	Q9H63A	BGW-Du	0	
 CNHJKD58Y5 	F4:2E:7F:C7:7D:F2	iap	10.8.56.106	RS15-AP-515-1	AP-515-US	Q9H63A	BGW-Du_	0	
• CNHPK9Y01Q	80:8D:87:C0:15:F9	lap	10.8.56.104	R\$15-AP-555-1	AP-555-US	JZ357A	BGW-Du	0	
 CV0016892 	00:1A:1E:05:0E:70	controller(G			7210-US	JW744A		0	
CNDDJSSTDQ	20:A6:CD:C0:38:	iap	10.8.0.2	AP305-D6	IAP-305-US	JX946A	default	0	
CNDDJSSTDX	20:A6:CD:C0:38:E2	iap	10.8.0.4	AP305-E2	IAP-305-US	JK946A	default	0	
• CNHLK9W0PX	00:4E:35:C4:9A:5E	lap	192.168.1.156	IAP535-RS12	AP-535-US	JZ337A	default		
• CN93HKZ48Y	38:21:C7:BA:F0:00	switch			2930F	JL258A		0	
• CP0047912	20:4C:03:39:73:1C	controller(G			7005-US	JW634A		0	
• CK0234513	40:E3:D6:C1:34:6C	iap			IAP-215-US	IAP-215-US		0	
• CT0338957	94:84:0F:C6:58:18	iap			IAP-225-US	IAP-225-US			
CN85HKZ0KZ	94:F1:28:8C:D2:A0	switch		RS15-2930F-1	2930F	JL258A	BGW-Du	0	
• CP0047911	20:40:03:39:85:24	controller(G	10.8.255.211	R\$15-7005-2	7005-US	JW634A	BGW-Du	0	
	20:A6:CD:C0:36:2E	iap	10.8.16.11	20:a6:cd:c0:36:2e	IAP-305-US	JX946A	default	0	
 CNDDJSST1R 		iap			IAP-305-US	JX946A		0	
CNDDJSST1R CNDRJSSDWH	20:A6:CD:C3:0A:								
	20:A6:CD:C3:0A: 20:A6:CD:C0:37:62	lap			IAP-305-US	JX946A			

Step 3: In the **Assign a Group to the Select Device** dialog box, select one of the VPNC groups you created in Procedure 2.1 (example: **VPNC-7210**).

TG 2930F-Single	
TG 2930M-Stack	
TG 3810M-Single	
AP-Branch	
AP-RS12	
BGW-7005	
BGW-7005-HA	
BGW-Dual-RS15	
default	
SW-Branch	
VPNC-7024	
VPNC-7210	
Cancel	Assign Device(s)

Step 4: Click Assign device(s), and then click OK.



3.2 Initiate the VPNC Device Configuration

Step 1: In the filter drop-down list, select the gateway that you want to configure.

aruba Central	Q Search or a	k Aruba Q 🕥 👪
VPNC-7210 V		• 1
Q REFINE FILTER LISTING		
GATEWAYS ONLY (8) default default VPNC-7024 VPNC-7024 VPNC-7024	Andu2100,12,46,28 Andu2100,12,24,40 0 Cl 2014 275440 275440	Clients Count
VPNC-7210 BGW-Dual-RS15 BGW-Dual-RS15	JW744A-0011A1E05/01A0 R515-7005-1 R515-7005-2	~
APPLICATIONS SECURITY	No data to display right now	No data to display right now
ALERTS & EVENTS	Bandwidth Usage Per Network	Client Count Per Network
AUDIT TRAIL		
TOOLS	ter ter	
MAINTAIN	No data to display right now	No data to display right now
FIRMWARE	Top APs By Usage	Top Clients By Usage
	No data to display right now	No data to display right new
	Top IAP Clusters By Usage	Top IAP Clusters By Clients
	No data to display right now	Ho data to display right new
	WLAN	
	NAME IF CLIENTS	TYPE SECURITY

GATEWAYS ONLY (8)			
default	Aruba7005_12_6E_28		
default	Aruba7005_12_6F_A0		
VPNC-7024	DC1-7024-1		
VPNC-7024	DC1-7024-2		
VPNC-7210	JW744A-00:1A:1E:05:01:28		
VPNC-7210	JW744A-00:1A:1E:05:01:A0	Jun	
BGW-Dual-RS15	RS15-7005-1	6	
BGW-Dual-RS15	RS15-7005-2		

For educational purposes, the next step exits the guided setup.

Step 2: In the guided setup dialog box, click **Cancel**, and then click **EXIT**.

Central	Guided Setup for VPNC Device JW744A-00:1A:1E:05:01:A0
1 System	This wizard will guide you through the essential steps to configure the VPNCs in the Device JW744A-00:1A:1E:05:01:A0.
2 LAN	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	After completing this initial setup, you can change the settings at any time.
4 SDWAN & Routing	
	Cancel Begin
EXIT GU	IDED SETUP
A	Guided Setup will be exited and changes will be lost. You can re-enter the Guided Setup at any time to complete it.
	RESUME

3.3 Configure the IP Address for the VPNC Device

Use this procedure to define the system IP address that the gateway will use for network services.

Step 1: On the Gateway Tab, in the SYSTEM section, select **System IP**.

Step 2: In the IPV4 Address box, enter the system IP address (example: **10.4.255.3**), and then in the Netmask box, enter **255.255.255.255**.

Step 3: Click Save Settings.

aruba Central	Q Search or ask Aruba		9 0	H &
JW744A-00:1A:1E:0				
GATEWAY	l GATEWAY	SELECTED DEVICE TYPE VPNC		4
MANAGE				
OVERVIEW	SYSTEM LAN WAN SDWAN & ROUTING	Advanced Mode	Guided Se	tup
DEVICE	System IP Hostname			
CLIENTS				
APPLICATIONS	Each branch gateway requires a unique system IP address that is used by the gatewa	y to communicate with network services such as VPN, RADIUS, syslog, TACACS+, and	Show More	
NALYZE	Per-field help			
ALERTS & EVENTS	IPv4 Address 10.4.255.3			
AUDIT TRAIL	Netmask 255.255.255			
TOOLS	110100x 233232323			
REPORTS				
AINTAIN				
FIRMWARE				

3.4 Assign a Hostname to the VPNC Device

Step 1: On the Gateways tab, in the **SYSTEM** section, select **Hostname**.

Step 2: In the Hostname box, enter a name (example: DC2-7210-1), and then click Save Settings.

🗢 🗢 💿 🙆 Aruba Central	x +				
← → C a app-prod2-ul.c	entral.arubanetworks.com/Trontend/#/caas/basic/system?tab=hostname		*	8	1
aruba Central	Q Search or ask Aruba	۹	0:	. 8	5
▼ JW744A-00:1A:1E:0 ▼					
🞇 GROUP	TACCESS POINTS SKITCHES GATEWAYS	18	i 1	4	₿
MANAGE					
B OVERVIEW	SYSTEM LAN WAN SDWAN & ROUTING Advanced Mode	Guide	ed Set	up	
DEVICES	System IP Hostname				
E8 CLIENTS					
SUESTS	Hostname DC2-7210-1				
APPLICATIONS					
SECURITY					
- ANALYZE					
A ALERTS & EVENTS					
AUDIT TRAIL					
S TOOLS					
REPORTS					
- MAINTAIN					
FIRMWARE					
	Cancel	Save	Setti	ngs	
		-			

3.5 Assign IP Addresses to the VLANs

Step 1: On the Gateway tab, in the LAN section, select VLANs.

Step 2: In the VLANs table, select the VLAN you want to update, and then click the pencil icon.

SYSTEM LAN WAN SDWAN & ROUTING Advanced Mode Guid VLANS LAN Ports Each gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Per-field help VLANS + HPM ADDESS NTMAK +	C GATEWAY VPNC STSTEM LAN WAN SDWAN & ROUTING Advanced Ma VLANs LAN Ports Lan Construction Lan Ports Construction Construction	VINC Advanced Mode Guided Setur Cture and client devices in your branches. Each YLAN will either be statically or Show More +	Id GATEWAY SULCETO DUNCE THE SYSTEM LAN VLANS LAN VLANS LAN Each gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Per-field help VLANS VLANS VLANS	Image: Structure of the static of the sta
SYSTEM LAN WAN SOWAN & ROUTING Advanced Mode Guid VLANS LAN Port Each gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Show Per-field help + VLANS + VLANS NETWASK	X X	Advanced Mode Guided Setu cture and client devices in your branches. Each VLAN will either be statically or Show More	SYSTEM LAN WAN SDWAN & ROUTING Advanced Mode VLANS LAN Ports Each gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Per-field help VTS VLANS + VLANS MAM IPV ADDRESS NTMAKK	SYSTEM LAN WAN SDWAN & ROUTING Advanced Mode Guided Se VLNN LAN Ports Each guteway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Show More Per-field help * * VLANS * *
VLANS LAN Ports Each gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Show Per-field help + VLANS + VLANS IPV4 aboltsS	VLANS LAN Ports LAN Ports Each gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Per-field help EVENTS VLANS +	cture and client devices in your branches. Each VLAN will either be statically or Show More	VLANS LAN Points Each gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Per-fields help. 1 NTS VLANS + VLAND NAME IPVI ADDRESS INTIMASK	VLANS LAN Ports Each gazeway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Per-field help Show More VLANS + VLANS + VLANS IPVI ADDEESS NTMARK IPVI ADDEESS
Each gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Per-field help VLANS + VLANS + VLANS NETWARK	ONS Each gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Per-field help EVENTS VLANS +	+	Each gateway will require one or more LAN VLANs and IP Interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Per-field help VLANS VLANS VLANS VLAN ID NAME IPV4 ADDRESS NETMASK	Each gazeway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Per-feele help VLANS + VLANS IPV4 ADDRESS NTMAXX 10 0.0000 IPV4 ADDRESS NTMAXX
Each gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Per-field help VLANS + VLANS + VLANS NETWARK	Each gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Per-field help ENTS	+	Each gateway will require one or more LAN VLANs and IP Interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Per-field help VLANS VLANS VLANS VLAN ID NAME IPV4 ADDRESS NETMASK	Each gazeway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Per-feele help VLANS + VLANS IPV4 ADDRESS NTMAXX 10 0.0000 IPV4 ADDRESS NTMAXX
VLANS + VLAN ID NAME UV4 ADDRESS INITIALIX	Per-field help	+	VIS VLANS + VLANS + VLAN ID NAME IPVY ADDASSS INTIMASK	Per-felshelp VLANS VLAND NAME INVA ADDRESS NETMASK INV INV
VLANS + YLAN ID NAME IPV4 ADDRESS INITIALIX	TS		VLANS + VLAN ID NAME UV4 ADDRESS INCTIMASIC	VLANS + VLAN ID NLINE IPV4 ADDRESS INTIMASE 10 02.0.0 IEIC
VLANS + VLAN ID NAME IV4 ADDRESS NETMASK			VLANS + VLAN ID NAME IPV4 ADDR55 NETMASK	VLAN 10 NAME IPVLADORESS NETMACK
VLAN ID NAME IPV4 ADDRESS NETMASK			VLAN ID NAME IPV4 ADDRESS NETMASK	VLAN 10 NAME IPVLADORESS NETMACK
100 66.0.0.0	VLAN ID NAME IPV4 ADDRESS NETMASK			
101 GL0.0.1				
				102 0E_0_0_2
				103 GE.0.0.3
	103 GEO.0.3		103 GE 0 0 3	
103 GE_0.0.3	105 00000			103 G£.0,0,3
				103 66.0.0.3
	66.0.0.3		GE 0.0.3	
103 GE_0_0_3				103 GE.0.0.3
102 GE_0.0.2	102 GE_0_0_2		102 GE,0,0,2	102 GE_0.0.2
				102 0E_0_0_2

Step 3: In the VLAN dialog box, implement the following settings:

- IPv4 Address—172.17.1.200
- Netmask—255.255.255.0

Step 4: Click Save.

VLAN - GE_0_0_0(100)	
Name	GE_0_0_0
VLAN ID	100
IPV4 ADDRESS	172.17.1.200
Netmask	255.255.255.0
(Condox	
	Cancel Save

Step 5: Repeat Step 2 - Step 4 for each additional LAN uplink VLANs.

Step 6: In the VLANs table, verify your changes, and then click **Save Settings**.

VLANS			
VLAN ID	NAME	IPV4 ADDRESS	NETMASK
100	GE_0_0_0	172.17.1.200	255.255.255.0
101	GE_0_0_1	66.60.164.125	255.255.255.224
102	GE_0_0_2	10.4.150.1	255.255.255.252
103	GE_0_0_3	10.4.150.5	255.255.255.252
4087	SystemIP_4087	10.4.255.3	255.255.255.255

3.6 Configure the WAN Providers

In this procedure, you configure the WAN uplinks (providers) and map them to the VLANs.

Step 1: On the Gateways tab, in the **WAN** section, select **WAN Details**.

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

COLDO Central Q © 11 A V IV7444-00:1A:1E0. V 11 GROUP © ACCESS POINTS D SWITCHES @ GATEWARS	🔍 🔍 🔍 Aruba Central	× +									
W17444-00:14:150 V Ct GOUP © Access POINTS SWITCHS @ GATEWARS SULCTO DEVICE TYPE BB OVERVIEW © Access POINTS SWITCHS @ GATEWARS Advanced Mode Guided Setup © DEVICES Edit VPNC (Headend Gateway) connects to one or more MPIS or internet connections using WAN ports. Each connection requires a WAN port to be configured. The 50-WAN. Show More Image: Configured and Conf	← → C 🌢 app-prod2-ul.ce	ntral.arubanetworks.co	m/frontend/#/caas/	basic/wan?tab=wa	nPorts					* (8
Clearing Clear	aruba Central				Q Search or ask Arub				٩	0 11	6
CROUP © ACCESS POINTS © SWITCHES © CREWAYS VPNC III IIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	∑ JW744A-00:1A:1E:0 ▼										
BIL Description BIL VEXAN EXANUTING Advanced Mode Guided Setup BIL VEXANUE VEXANUE CLENTS VEXANUE Control ALCENTS Each VPNC (Headend Guideway) connects to one or more MPLS or internet connections using WAN ports. Each connection requires a WIN port to be configured. The SD-WANI Show More ALCENTS Each VPNC (Headend Guideway) connects to one or more MPLS or internet connections using WAN ports. Each connection requires a WIN port to be configured. The SD-WANI Show More ALMENTS SECURITY ALLERTS & EVENTS Internet connection provide a provide provide a provide provide a provide a provide a provide	🞇 GROUP	ACCESS POINTS	SWITCHES	@ GATEWAY	s			VPNC	:=	11.	۲
B OKNEW CUENTS CUENTS CUENTS CUENTS ALAZETS & EVENTS ALAZETS & EVENTS ALAZETS ALAZETS CUENTS ALAZETS CUENTS ALAZETS CUENTS	- MANAGE	0107514			a pourrais						
CLIENTS CLIENTS CLI		STSTEM	LAN	SDWAN	& ROUTING			Advanced Mode	Guide	d Setu	p
Each VFNC (Headend Gateway) connects to one or more MFLS or interret connections using WAN ports. Each connection requires a WAN port to be configured. The SD-WAN. Show More AULTRES AUL		WAN Details	1								
APPLICATIONS UPLINKS Image: Control of the state of			•								
O SECURITY INIX YYPE IP PUBLIC IP PARTATE IP ALALERTS & EVENTS		Each VPNC (Hea	dend Gateway) conr	ects to one or mo	re MPLS or internet conne	tions using WAN ports. E	ach connection requires a W	AN port to be configured. The SD-WAN	Show	More	
ADALYTE CALL CONTRACT		UPLINKS					+				
Q. ALERTS & EVENTS No data to display ZI AUDIT TRAIL		LINK	TYPE	ID	PUBLIC IP	PRIVATE IP					
AUDIT TRAIL AUDIT TRAIL AUDIT TRAIL AUDIT TRAIL AUDIT TRAIL AUDIT TRAIL											
tools in reports Miniman in the second secon					No data to display						
I REPORTS											
MAINTAIN											
• FIRMWARE											
	Ø FIRMWARE										

Step 3: In the Add/Edit Uplink dialog box, implement the following settings:

- Uplink Name—Turbo
- Interface VLAN ID—VLAN 100
- WAN type—MPLS or Internet

Note If you set **WAN type** to **Internet**, you must enter a public IP address to enable 1:1 NAT translation at the internet firewall. If you set **WAN type** to **MPLS**, the uplink name must match the MPLS providers on the branch gateways to enable automated tunnel orchestration between gateways.

Step 4: Click Save.

Add/Edit Uplink	
Uplink	Turbo
Interface VLAN ID	VLAN 100 -
WAN type	MPLS 🔻
Private IP	172.17.1.200
	Cancel Save
Add/Edit Uplink	
Add/Edit Uplink	Speedy
-	Speedy VLAN 101
Uplink	
Interface VLAN ID	VLAN 101

Step 5: In the Uplinks table, review your changes, and then click **Save Settings**.

UPLINKS					1
LINK	ТҮРЕ	ID	PUBLIC IP	PRIVATE IP	
Turbo_MPLS	MPLS	100	-	172.17.1.200	
Speedy_INET	INET	101	66.60.164.125	66.60.164.125	

3.7 Configure the Default Route to the Internet

Step 1: On the Gateways tab, in the SDWAN & Routing section, select **Static Routing**.

Step 2: In the **Default Routes** table, click the plus (+) sign to add a default route toward the internet provider.

🔍 🔍 🔍 🧟 Aruba Central	× +								
← → C 🍙 app-prod2-ui.	central.arubanetworks.com/front	end/#/caas/basic/vpnrouting?t	ab=staticoverlayrouting					*) I
aruba Central			Q Search or ask Arr				9 6) :::	8
▼ JW744A-00:1A:1E:0 ▼									
1 GROUP	ACCESS POINTS					SELECTED DEVICE TYPE VPNC	:=	46	۲
- MANAGE									_
88 OVERVIEW	SYSTEM LAN	WAN SDWAN	ROUTING			Advanced Mode	Guided	Setup	
	SD-WAN Overlay	Static Routing Route M	aps OSPF	BGP Overlay Routing					
LD CLIENTS	L								
A GUESTS	Configure default and st	atic routes that apply to all Bran	ch Gateways in this gro	up. Show More					
# APPLICATIONS	Per-field help								
SECURITY	DEFAULT ROUTES	+							
- ANALYZE	NEXT HOP	COST							
ALERTS & EVENTS									
AUDIT TRAIL	No da	ta to display							
S TOOLS									
REPORTS									
- MAINTAIN									
FIRMWARE	STATIC ROUTES				+				
	DESTINATION IP	DESTINATION MASK	TYPE	NEXT HOP	COST				
			No data to display						
						Cancel	Save S	etting	gs

Step 3: In Next Hop column, enter the default gateway (example: 66.60.164.97).

Step 4: In the Cost column, enter 1.

DEFAULT ROUTES	+	
NEXT HOP	соѕт	
66.60.164.97	1]

Step 5: Click Save Settings.

3.8 Configure OSPF Routing to the LAN

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

	Q Search or ask Aruba	۹	0	 8
JW744A-00:1A:1E:0 ¥ GROUP MANAGE MANAGE B8 OVERVIEW Ø Ø DEVICES CLIENTS C GUESTS #	ACCESS POINTS SWITCHES GATEWAYS STSTEM LAN WAN SDWAN & ROUTING Advanced Mod SD-WAN Overlay Static Routing Route Maps OSFF BGP Overlay Routing This page allows you to configure the Open Shortest Path First (05FF) routing protocol in order to exchange routes between the VPNC and an upstream router. Show More	e Gui	i≣ ided S	
APPLICATIONS SECURITY AMALYZE AURTTS & EVENTS AURTT RAIL ATOLS AURTTRAIL FOOLS ARPORTS MAUNTAIN FIRMWARE	v General Enable OSPF Interface Redistribution			

Step 2: Under General, click the **Enable OSPF** slider.

Step 3: In the Router ID box, select the System ID interface for OSPF Router ID (example: 10.4.255.3).

Step 4: In the Area ID box, define the OSPF area (example: 0.0.0.0).

🗸 General	
Enable OSPF	
Default originate	
Router ID	10.4.255.3 ×
Area ID	0.0.0.0

Step 5: Click Save Settings.

Step 6: Repeat these steps, if necessary.

Step 7: On the OSPF page, expand **Interface**.

Step 8: In the VLANs table, click the plus (+) sign.

	Seneral nterface				
	VLANS				+
	VLAN	AREA ID	COST	HELLO INTERVAL	
		No data to displa	y		
> F	Redistribution				

Step 9: Enable OSPF on each of the LAN uplinks and System IP interfaces, define area ID, and adjust the OSPF metrics, if desired, and then click **Save Settings**.

VLANS				+
VLAN	AREA ID	COST	HELLO INTERVAL	
GE_0_0_2 102 (10.4.150.1)	0.0.0.0	1	10	
GE_0_0_3 103 (10.4.150.5)	0.0.00	1	10	
SystemIP_4087 4087 (10.4.25	0.0.0.0	1	10	

Step 10: Expand Redistribution.

🗧 🔍 🌒 👩 Aruba Central	x +			
← → C app-prod2-ui.	central.arubanetworks.com/frontend/#/caas/basic/vpnrouting?tab=ospf		8	
aruba Central	Search or ask Aruba	9 0		8
▼ JW744A-00:1A:1E:0 ▼				
II GROUP	G ACCESS POINTS SWITCHES C GATEWAYS	100.00		۲
If GROUP MARADE BO OVERVIEW ID DEVICES LS CLIENTS LS GUESTS ID ADDETS ID ADDETS ID ADDETS ADDIT TAIL ID REPORTS ID REPORTS ID REPORTS	Access Points SWITCHES Access Points Advanced Mode SWITCHE SWITCHES Advanced Mode SWITCHES SWITCHES SWITCHES Advanced Mode SUMAN Overlay Static Routing Route Maps OSPF BGP Overlay Routing This page allows you to configure the Open Shortest Path First (OSPF) routing protocol in order to exchange routes between the VPNC and an upstream router. Show More Per field hep Sourcess KEDISTRIBUTION NULLS SOURCE RADIDECOL INITIR ROUTE TYPE ROUTE MAP COST No data to digplay:			
	Geneel	Save Set	tings	Î

Step 11: In the **Redistribution Rules** table, click the plus (+) sign.

Step 12: In Source Protocol drop-down list, select SDWAN Overlay.

Step 13: For Route Type, select E1 using the drop-down.

Step 14: In the **Route Map** drop-down list, select none or the route map you created at the group level in optional Procedure 2.9 (example: **rm_all**).

REDISTRIBUTION RULES								
FILTER	ROUTE TYPE	ROUTE MAP	COST					
	E1	rm_all	1					
	FILTER							

Step 15: Click Save Settings.

3.9 Enable One-Touch Provisioning on the VPNC Device

Use this procedure to connect the VPNC device to the network and execute an initial script to enable one-touch provisioning.

Step 1: Using the VPNC console port and the settings below for your terminal software, select the **static-activate** option from the menu to enable one-touch provisioning by using a static IP address.

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

```
Auto-provisioning is in progress. It requires DHCP and Activate servers
Choose one of the following options to override or debug auto-provisioning...
    'enable-debug' : Enable auto-provisioning debug logs
'disable-debug' : Disable auto-provisioning debug logs
    'mini-setup'
                          : Start mini setup dialog. Provides minimal customization and requires DHCP
server
    'full-setup' : Start full setup dialog. Provides full customization
'static-activate' : Provides customization for static or PPPOE ip assignment. Uses activate for
master information
Enter Option (partial string is acceptable): static-activate
Enter Controller VLAN ID [1]: 101
Enter Uplink port [GE 0/0/0]: GE 0/0/1
Enter Uplink port mode (access|trunk) [access]:
Enter Uplink Vlan IP assignment method (static|pppoe) [static]:
Enter Uplink Vlan Static IP address [192.168.1.1]: 66.60.164.125
Enter Uplink Vlan Static IP netmask [255.255.255.0]: 255.255.255.224
Enter IP default gateway [none]: 66.60.164.97
Enter DNS IF address [none]: 8.8.8.8
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
Do you want to disable spanning tree (yes|no)? [no]:
Do you want to configure dynamic port-channel (yes|no) [no]:
Current choices are:
Controller VLAN id: 101
Uplink port: GE 0/0/1
Uplink port mode: access
Uplink Vlan IP assignment method: static
Uplink Vlan static IP Address: 66.60.164.125
Uplink Vlan static IP net-mask: 255.255.255.224
Uplink Vlan IP default gateway: 66.60.164.97
Domain Name Server to resolve FQDN: 8.8.8.8
Option to configure VLAN interface IPV6 address: no
Spanning-tree is disabled: no
Do you wish to accept the changes (yes|no) yes
```

Procedures

Configuring the Branch Gateway Group—One Branch Gateway per Branch

- 4.1 Create a New Branch Gateway Group
- 4.2 Create the System IP Address Pool for the Branch Gateway Group
- 4.3 Select the Hardware Model of the Gateway Group
- 4.4 Select the Branch Gateway Group Time Zone
- 4.5 Configure the DNS Servers for the Branch Gateway Group
- 4.6 Create a Management User Account for the Branch Gateways
- 4.7 Configure VLANs for the Branch Network Devices and Users
- 4.8 Configure the LAN Ports for the Branch Gateway
- 4.9 Configure WAN Health Checks
- 4.10 Configure the WAN Load Balancing Algorithm
- 4.11 Define the WAN Service Providers
- 4.12 Specify the SD-WAN Data Center Preferences
- 4.13 Configure the SD-WAN Overlay Routing
- 4.14 Configure Role-Based Policies for the Branch Gateways

4.1 Create a New Branch Gateway Group

In this procedure, you create a branch gateway group and assign a branch gateway group type to the group.

Step 1: In filter drop-down list, select **All Devices**, and then in the left navigation bar, under maintain, select **ORGANIZATION**.

Step 2: Select the Groups tab, and then click New Group.

				a					۹ 💿
GLOBAL	GROUPS	SITES AND LA	BELS Ø	CERTIFICATES	INSTALL MANAGER				
ANAGE OVERVIEW DEVICES CLIENTS GUESTS	group and a	Aruba Central acts apply the same cor GROUPS	nfiguration s	ettings to all th	ion container for devices. You c ie devices in the group.	an combine devices	with comm	non configuration n	equirements into a single
SECURITY		DROP CLUSTERS AN MULTIPLE DEVICES							
NETWORK SERVICES	▼ GROUP N	AME DEV	NCES		√ NAME	VLOCATION	TYPE	V SERIAL W	V MAC ADDRESS
ALYZE	ALL CONN	CTED DEVI 19		1	Aruba-2930F-8G-P	Spring,United States	HPPC	CN79HKZ081	f4:03:43:fb:75:c0
ALERTS & EVENTS	A CONTRACT OF A CONTRACT	ED DEVICES 0			Aruba7005_12_6E	Spring,United States	MC	CP0025945	20:4c:03:12:6e:28
AUDIT TRAIL	TG 2930F-	Single 0			Aruba7005_12_6F	Spring,United States	MC	CP0025992	20:4c:03:12:6f:a0
TOOLS	TG 2930M	-Stack 0			DC1-7024-1	Sacramento,United	MC	CZ0000091	00:0b:86:bb:bb:a7
REPORTS	TG 3810M	-Single 0			L DC1-7024-2	Sacramento,United	MC	CZ0001699	00:0b:86:bb:ff:a7
INTAIN	BGW-Dual-I	IS15 S			DC2-7210-1	Sacramento,United	MC	CV0016870	00:1a:1e:05:01:a0
FIRMWARE	default	7			DC2-7210-2	Sacramento,United	MC	CV0016872	00:1a:1e:05:01:28
ORGANIZATION	SW-3810-G	RP 1			HP-2920-48G-POEP		HPPC	SG82JQP24L	04:09:73:b3:df:40
	SW-BRANCI	H-GRP 2			IAP-Thomas1	Sacramento,United	VC	CNDDJSST1R	20:a6:cd:c0:36:2e
	New Grou	r jako Grava		11 Group(s)					19 Device(s)

Step 3: In the Create New Group dialog box, implement the following settings:

- Group Name—BGW-7005
- Switch—Unselect
- Password—password
- Confirm Password—password

Step 4: Click Add Group.

	NEW G			
GROUP NAME BGW-7005			-	
Use the group a	s Template group	by selecting t	he device 🚺	
IAP AND GA	ATEWAY		SWITCH	
Group password	l settings 🚺			
CONFIRM PASSWORD			-	
Cancel			Add G	roup

Note If you intend to use the Install Manager App, assign the group to the sites at this point.

Step 5: In the filter drop-down list, select **BGW-7005**.

Step 6: In the left navigation pane, in the Manage section, click **Devices**.

Step 7: Select the **Gateways** tab, and then click the gear icon in top right.

🔍 🔍 🔍 🌊 Aruba Central	× +				
← → C 🌲 app-prod2-ui.	.central.arubanetworks.com/frontend/#/GATE	WAY/LIST			* 🙂 E
aruba Central		Q Search			۹ 🛛 🟭 🖧
Y BGW-7005 V					
11 GROUP	access points 📼 switches				💷 ıl. 🛞
- MANAGE					
88 OVERVIEW	GATEWAYS UP O DOWN				
	0 0 0				
LT& CLIENTS	GATEWAYS				Ŧ Θ
SUESTS	♥ DEVICE NAME IF	MODEL	FIRMWARE VERSION	UPTIME	IP ADDRESS
# APPLICATIONS					
- ANALYZE					
ALERTS & EVENTS					
AUDIT TRAIL					
S TOOLS					
REPORTS					
- MAINTAIN					
FIRMWARE					
			No data to display right	now	

Step 8: In the Set Group Type dialog box, select **Branch Gateway**, and then click **Save Settings**.



For educational purposes, the next step exits the guided setup.

Step 9: In the Guided Setup dialog box, click Cancel, and then click Exit.

aruba Central	Guided Setup for Branch Gateway Group BGW-7005
1 System	This wizard will guide you through the essential steps to configure the branch gateways in the Group BGW-7005.
2 LAN	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	After completing this initial setup, you can change the settings at any time.
4 SDWAN & Routing	
5 Policies	Cancel Begin
EXIT GU	IIDED SETUP
	Guided Setup will be exited and changes will be lost.
	You can re-enter the Guided Setup at any time to complete it.
	RESUME

4.2 Create the System IP Address Pool for the Branch Gateway Group

Use this procedure to define the system IP address pool that the gateway will use for network services.

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

 C • C • spo-prod2-ul central andaretworks.com/itorited/l/casi/basic/system/hab-gateway/opcol C • D • D • C • spo-prod2-ul central andaretworks.com/itorited/l/casi/basic/system/hab-gateway/opcol C • D • D • C • Spo-prod2-ul central andaretworks.com/itorited/l/casi/basic/system/hab-gateway/opcol C • D • D • C • Spo-prod2-ul central andaretworks.com/itorited/l/casi/basic/system/hab-gateway/opcol C • D • D • C • Spo-prod2-ul central andaretworks.com/itorited/l/casi/basic/system/hab-gateway/opcol C • D • D • C • Spo-prod2-ul central andaretworks.com/itorited/l/casi/basic/system/hab-gateway/opcol C • D • D • D • D • D • D • D • D • D •	*) D II	® : (
	0 1	8
11 GROUP TACCESS POINTS SWITCHES & GATEWAYS	4.	۲
- MANAGE		
88 OVERVIEW SYSTEM LAN WAN SDWAN & ROUTING POLICIES Advanced Mode Guided	Setu	P
DEVICES System IP Model Time DNS Management User		
ID CUENTS		
GUESTS Each branch gateway requires a unique system IP address that is used by the gateway to communicate with network services such as VPN, RADIUS, systog, TACACS+, and Show M	ore	
APPLICATIONS Per-field help		
SECURITY Configuration approach Define system IP address pool Specify static IP addresses later		
- ANALYZE		
ALERTS & EVENTS If you do not define a System IP pool, it is necessary to specify the VLAN interface and system IP setting on a per-device basis or for		
AUDIT TRAIL multiple gateways once using the Burk configuration upload feature.		
 tools 		
C REPORTS		
- MARTAN		
© FIRMWARE		

Step 2: Select Define system IP address pool.

Step 3: In Assign the Start IP address box, enter 10.8.255.1.

Step 4: In the End IP address box, enter 10.8.255.20, and then click Save Settings.

Note The system IP ac be in a routable space.	ldress is used for gatew	ay management and needs to	
Configuration approach	Define system IP address pool	O Specify static IP addresses later	
Start IP address	10.8.255.1		
End IP address	10.8.255.20		
Gateway pool size	20 Gateways		
Vlan	4087	Cancel Save Settings	J

Step 5: In the Warning dialog box, click **Yes**. When you move the gateways to a group, the gateways need to reboot to complete the group configuration.

Warning	
Gateway will be rebooted on savin	g changes. Do you want to proceed?
	No Yes

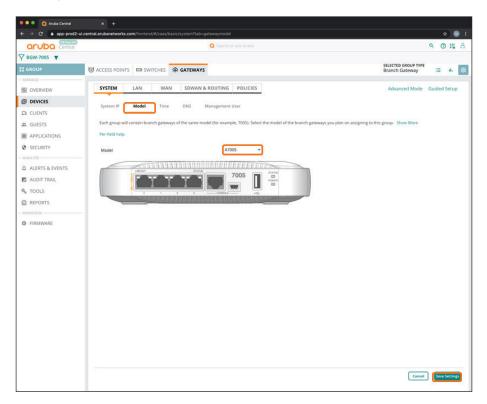
4.3 Select the Hardware Model of the Gateway Group

You can have only one gateway model per branch in the gateway group.

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

Step 2: In the **Model** drop-down list, select the hardware model for the branch gateway(s) in the group (example: **A7005**).

Step 3: Click Save Settings.



4.4 Select the Branch Gateway Group Time Zone

Use this procedure to set the NTP parameters and time zone to keep the branch gateway 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.

• • • • Aruba Central	× +					
	i.central.arubanetworks.com/fronte	nd/#/caas/basic/system?tab=time		د م رو	-	
Central		G Search of ask Aruba		4 6	110	0
II GROUP	🗑 ACCESS POINTS 📼 SI	A CATCHANE	SELECTED GROUP TYPE			0
- MANAGE -	C ACCESS POINTS	WITCHES SE GALEWATS	Branch Gateway	-	46	ψ
88 OVERVIEW	SYSTEM LAN	WAN SDWAN & ROUTING POLICIES	Advanced Mode	Guided	Setup	
LD CLIENTS	System IP Model	Time DNS Management User				
2. GUESTS	Each branch gateway in th	e group will automatically obtain its time using the Netwo	rk Time Protocol (NTP). You can either select one or more public NTP service providers (for	Show Mo	re	
# APPLICATIONS	Per-field help					
SECURITY	Public NTP Servers		+			
- ANALYZE	IPV4 ADDRESS/FQDN	BURST MODE				
ALERTS & EVENTS						
AUDIT TRAIL		No data to display				
S TOOLS						
MAINTAIN						
FIRMWARE	Timezone	Choose a timezone				

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

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

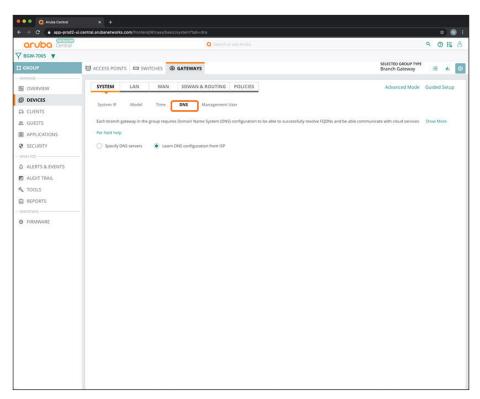
Step 5: In the Timezone drop-down list, choose your timezone, and then click Save Settings.

V4 ADDRESS/FQDN	BURST MODE		
ool.ntp.org			
ezone	Choose a timezone		

4.5 Configure the DNS Servers for the Branch Gateway Group

You must specify the DNS server(s) that the gateway uses to communicate to Aruba Central.

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



Step 2: Click 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.

Step 5: In the **Provider** drop-down list, select one of the providers listed or manually configure the desired DNS server(s). This server needs to be reachable when the device comes up for connectivity to Central.

Step 6: Click Save Settings.

ROVIDER	IPV4 ADDRESS	
ioogle 🔹	8.8.8.8,8.8.4.4	

4.6 Create a Management User Account for the Branch Gateways

You must have a management user account to use 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.

GROUP CACCESS POINTS SWITCHES GATEWAYS SUICHES 0 VEXVIEW SYSTEM LAN WAN & ROUTING POLICIES Advanced Mode Guided Seture 0 VEXVIEW SYSTEM LAN WAN & ROUTING POLICIES Advanced Mode Guided Seture 0 VEXVIEW System IP Model Time DHS Management User Stoow More 0 VEXVIEW Source Perified help No Stoow More Stoow More 1 APPLICATIONS Perified help Advanced mode Seture Stoow More 1 APPLICATIONS Perified help MAA authentication Stoow More 1 AUDIT TRAIL Non Gate to digity No Gate to digity No Gate to digity		aruba Central	Q Search or ask Aruba	۹ 🔿 🏭
GROUP © ACCESS POINTS © MITCHES © GATEWAYS Branch Gateway E 4. WARE System IP LAN WAN SDWAN & ROUTING POLICIES Advanced Mode Guided Seture 0 CLENTS System IP Model Time DNS Management User South Area Show More 0 CLENTS To be able to locally or remotely access the CLI console of the gateways in the group, you must either configure either a local management user or enable centralized Show More APPLICATIONS SisCURITY AdvanchedIndeb Model Show More ALERTS & REVENTS A authentication Advanced Mode Show More I AUDIT TRAIL Nos Gas to digity No Gas to digity No Gas to digity		3GW-7005 🔻		
IVENUEW SYSTEM LAN WAN SDWAIN & ROUTING POLICIES Advanced Mode Guided Setup IVENUES System IP Model Time DNS Management User IVENUES To be able to locably or remotely access the CU console of the gateways in the group, you must either configure either a local management user or enable centralized Show More APPLICATIONS Perfect help State to locably or remotely access the CU console of the gateways in the group, you must either configure either a local management user or enable centralized Show More APPLICATIONS Perfect help Advantertication Show More IVENUE Callering Advantertication Show More IVENUE IVENUE IVENUE IVENUE IVENUE IVENUE IVENUE IVENUE	BB OVERVEW SYSTEM LAN WAN SDWAN & ROUTING POLICIES Advanced Mode Guided S CB CLENTS System IP Model Time DNS Management User AL CLESTS To be able to locally or remotely access the CLI conside of the gateways in the group, you must either configure either a local management user or enable centralated Show More A APPLICATIONS Perified help Store field help Store field help S SCURITY Advanced Mode Local management users + A Advanced Mode Store field help Store field help Store field help S SCURITY Local management users + A Advanced Mode Store field help Store field help S ALERTS & EVENTS Local management users + A Model No. Gate to diplay Massexob Management users + + Management users +	ROUP	🗇 ACCESS POINTS 🛤 SWITCHES 🙊 GATEWAYS	SELECTED GROUP TYPE Branch Gateway 🗄 🖬
SPENCES System IP Model Time DNS Management User System IP Model Time DNS Management User GUESTS GUESTS GUESTS APPLICATIONS Perfield help Security AAA authentication Im Local management users Local management users Im Name Refield help Security ALERTS Local management users Im No data to digity No data to digity	BOVICES System IP Model Time DNS Management User Social CleMTS CleMTS CleMTS CleMTS CleMTS Addet to locally or remotely access the CLI console of the gateways in the group, you must either configure either a local management user or enable centralized Social Model Addet te Addet te CleMTS Addet te Addet Addet te Addet Addet Addet te Addet Addet te Addet Ad			
CUENTS System IP Model Time Dis Management User CUENTS To be able to locally or remotely access the CU console of the gateways in the group, you must either configure either a local management user or enable centralized Show More APPLICATIONS Perfetch help Advantagement user or enable centralized Show More I SECURITY Advantagement users Imagement users Imagement users ALERTS Local management users Imagement users Imagement users I REPORTS No data to display No data to display	CLENTS System IP Model Time DNS Management User GUESTS GUESTS To be able to locally or remotely access the CLI console of the gateways in the group, you must either configure either a local management user or enable centralized Show More Per-field help ACLENTS Accel management users CLICATIONS Reform S AUDIT TRAIL Name ROLE PASSWORD No deal to display		SYSTEM LAN WAN SDWAN & ROUTING POLICIES	Advanced Mode Guided Setup
GUESTS To be able to locally or remotely access the GU console of the gateways in the group, you must either configure either a local management user or enable centralized Show More J APPLICATIONS Perifield help Addatatatatatatatatatatatatatatatatatata	COUSTS To be able to locally or remotely access the CLI console of the gateways in the group, you must either configure either a local management user or enable centralized Show More Per-fetch help Control AAA authentication AAAA authentication AAA authentication AAA authentication AAA authentication AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		System IP Model Time DNS Management User	
APPLICATIONS Per-field help SECURITY AAA authentication AAAA authentication AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	APPLICATIONS Per-field help SECURITY AAA authentication ALERTS & EVENTS L Cocat management users L AUDIT TRAIL , TOOLS REPORTS			
A A Authentication A A Authentication A	A ALEMANDA SCIENTINA ALERTS & EVENTS LOCAI management users I AUDIT TRAIL NAME ROLE PASSWORD I I AUDIT TRAIL NAME ROLE INO data to display			I management user or enable centralized Show More
AALVEE AAA duthentication C	ALIZET ALIVET AL		Pentied help	
ALER'S & EVENTS Local management users AUDIT TRAIL NAME ROLE TOOLS REPORTS No diak to display	ALER'S & EVEN'S Lecal management users AUDIT TRAIL NAME ROLE TOOLS		AAA authentication	
AUDIT TRAIL AUDIT TRAILAUD	AUDIT TRAIL AUDIT TRAIL TOOLS REPORTS No data to display			
TOOLS REPORTS No data to display	TOOLS REPORTS No data to display			
REPORTS No data to display	REPORTS No data to display		NAME ROLE PASSWORD	
NITANN	NITAIN		No data to display	
FIRMWARE	FIRMWARE		-	
		FIRMWARE		

Step 3: In the Add Management User dialog box, implement the following settings:

- Name—admin
- Password—password
- Retype Password—password
- Role—Super user role

Step 4: Click Save.

 can add additional users wi users are optional.	th other roles as needed. These	
Add management user		
Name	admin	
Password		
Retype Password		
Role	Super user role 🔻	
	Cancel	

Step 5: Click Save Settings.

4.7 Configure VLANs for the Branch Network Devices and Users

In this procedure, you define the VLANs for the branch network devices and users as well as assign subnets at the device level.

Step 1: On the Gateways tab, in the LAN section, select **VLANs**.

Step 2: Select IP DHCP server.

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

In this example, we create VLAN 1 for management. VLAN 1 is recommended for plug and play of the switches and APs in the branch.

•••	Aruba Central	× +									
$\leftarrow \rightarrow$	C app-prod2-ui.c	central.arubanetworks.com//ro	ntend/#/caas/basic/lan?tat						\$		
or				O Search or ask Aru				٩	0:		ക
∀ BGW	/-7005 🔻										
11 GRO	UP	access points	SWITCHES @ GATE	WAYS			SELECTED GROUP TYPE Branch Gateway				۲
- MANAG	it									1	
88 OV	ERVIEW	SYSTEM LAN	WAN SDV	WAN & ROUTING POLIC	IES		Advanced Mode	Guid	ed Set	up	
@ DE	VICES	VLANS LAN PO									
LE CLI	ENTS										
St. GU	IESTS	Each branch gateway w	ill require one or more LA	NVLANs and IP interfaces to su	pport infrastructure and client o	devices in your branches. Each VLAN	will either be statically or	Show	More		
II AP	PLICATIONS	Per-field help									
SEC SEC	CURITY	IP DHCP server									
- ANALY	ZE					_	-				
Q ALI	ERTS & EVENTS	VLANs				L					
🗹 AU	DIT TRAIL	4087	NAME SystemiP_4087	STATIC	DYNAMIC DHCP POOL	DHCP RELAY Disabled					
S TO	OLS		.,								
REI REI	PORTS										
- MAINTA	AIN										
@ FIR	MWARE										
										_	
							Cancel	5	ive Sett	tings	
2											_

Step 4: In the New VLAN dialog box, implement the following settings:

- Name—Management
- VLAN ID-1
- IP addressing mode—Static

Step 5: Click Save.

Name	Management
/LAN ID	1
P addressing mode	Static 🔹
PV4 ADDRESS (Optional)	
Netmask (Optional)	
Act as DHCP server	
Enable DHCP relay	

Step 6: Repeat Step 3 - Step 5 for each additional user VLAN. For example, an **Employee** VLAN.

Step 7: Click Save Settings.

VLANs					+
VLAN ID	NAME	STATIC	DYNAMIC DHCP POOL	DHCP RELAY	
4087	SystemIP_4087	· *	8	Disabled	
1	Management	×	¥.	Disabled	
20	Employee			Disabled	

4.8 Configure the LAN Ports for the Branch Gateway

Assign the LAN ports that the downstream switches use and permit the user and management VLANs.

Step 1: On the Gateways tab, in the LAN section, select **LAN Ports**.

Step 2: In the LAN ports/port channel table, click the plus (+) sign.

Central				Q Search or ask)					9 0	0 114
GW-7005 ▼ ROUP	O ACCESS POINTS	SWITCHES	@ GATEWAYS					SELECTED GROUP TYPE Branch Gateway		4.
OVERVIEW	SYSTEM	LAN WAR	N SDWAN &	ROUTING PO	LICIES			Advanced Mode	Guided	Setup
DEVICES	VLANS A	IN Ports								
CLIENTS	YDANS U	N Ports								
GUESTS	LAN VLANS can b	e assigned to one or	more ports on you	r gateways in the gro	up. The gateway por	rts that are available fo	or assignment in this step w	vill be dependent on the	Show M	ore
APPLICATIONS	Per-field help									
SECURITY	LAN ports/po	et channel					+			
LYZE	NAME	PORT	MODE	ACCESS VLAN	NATIVE VLAN	ALLOWED VLANS				
LERTS & EVENTS				Action for		ALLONIO TONIO				
UDIT TRAIL				No data to display						
DOLS										
EPORTS										
VTAIN										
FIRMWARE										

Step 3: In the New LAN port/port channel dialog box, enter a name for the new port (example: LAN).

Step 4: In the Port drop-down list, select a physical port on the gateway (example: GE-0/0/0).

Step 5: In the VLAN mode drop-down list, select **Trunk**.

Step 6: In the **Native VLAN** drop-down list, select the management VLAN you created in Procedure 4.7 (example: **1 : Management**).

Step 7: In the **Allowed VLAN** box, enter the VLAN IDs for the VLANs allowed towards LAN, and then click **Save**.

Step 8: Repeat Step 2 - Step 7 for each additional LAN port that you need to configure.

lew LAN port / portchannel	
Name	LAN
Port	GE-0/0/0
VLAN mode (Optional)	Trunk
Native VLAN (Optional)	1 : Management 🔻
Allowed VLAN (Optional)	1,20
	Cancel Save

Step 9: Click Save Settings.

4.9 Configure WAN Health Checks

For more information, see Enabling WAN Health Check Probes.

Step 1: On the Gateways tab, in the WAN section, select **Health Checks**.

aruba Central		Q Search			۹ (D III	8
BGW-7005 T	C ACCESS POINTS	GATEWAYS		SELECTED GROUP TYPE Branch Gateway	:=	а.	
MANAGE -	Gracessrounds - Smith			branch Gateway			
OVERVIEW	SYSTEM LAN	WAN SDWAN & ROUTING	POLICIES	Advanced Mode	Guideo	d Setu	р
DEVICES	Health Checks Load Bala	ancing WAN Details					
D CLIENTS		incing which because					
GUESTS	IP health checks are used by the	gateways to determine WAN path av	ailability and measure WAN path per	formance. The responses to these health check probes are used by	Show N	tore	
APPLICATIONS	Per-field help						
SECURITY		-					
ANALYZE	Enable health checks						
ALERTS & EVENTS	Health check destination	•					
AUDIT TRAIL	We recommended you to:	select health check destination as Ar	uba cloud.				
TOOLS	Health check probe mode	Ping 👻					
REPORTS							
MAINTAIN							
FIRMWARE							

Step 2: In the Health check destination drop-down list, select **Aruba cloud**.

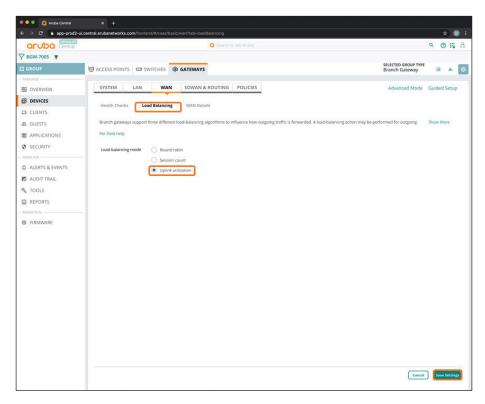
Step 3: Click Save Settings.

Health Checks	Load Balancing	WAN Detail	s		
IP health checks are Per-field help	used by the gateways	s to determine W.	AN pa	ath availabi	lity and measure
Enable health chec	ks				
Health check destir	nation	Aruba cloud	•		
Health check probe	mode	Ping	•		
				Cancel	Save Settings

4.10 Configure the WAN Load Balancing Algorithm

Step 1: On the Gateways tab, in the WAN section, select Load Balancing.

Step 2: In Load balancing mode list, select Uplink utilization, and then click Save Settings.



4.11 Define the WAN Service Providers

In this example, we use a single gateway with dual internet connections.

Step 1: On the Gateways tab, in the WAN section, select WAN Details.

Step 2: In the WAN Uplinks/Ports table, click the plus (+) sign.

orubo Central	Q Search or ask Aruba Q (D III	å
BGW-7005 ¥			
GROUP	ACCESS POINTS SKITCHES & GATEWAYS	d.	۲
AANAGE	SYSTEM LAN WAN SDWAN & ROUTING POLICIES Advanced Mode Guidee		
8 OVERVIEW	Advanced Mode Guider	1 Setup	
DEVICES	Health Checks Load Balancing WAN Details		
CLIENTS			
GUESTS	Each branch gateway connects to one or more Internet, MPLS and cellular based WAN services using WAN ports. A gateway can support a maximum of four Wired WAN links Show N	lore	
APPLICATIONS	Per-field help		
SECURITY	Enable HA deployment		
NALYZE			
ALERTS & EVENTS	WAN Uplinks / Ports +		
AUDIT TRAIL	UPLINK TYPE PORT VLAN ID ADDRESS SPEED NAT BACKUP		
TOOLS			
REPORTS	No diata to display		
AAINTAIN			
FIRMWARE			

Step 3: In the Add/Edit wan port dialog box, implement the following settings:

- Uplink—ISP-1
- WAN—Internet
- WAN speed—200
- Port—GE-0/0/3

VAN CONNECTION		
Uplink	ISP-1	
WAN type	Internet	•
WAN speed	200	Mbps
Source NAT	>	
Use as backup		
IP addressing method	DHCP	-
Only four uplinks was port assignment		ssing method
Only four uplinks v can be created WAN PORT ASSIGNM Port		ssing method

Add/Edit wan port	
WAN CONNECTION	ISP-2
WAN type	Internet 🔹
WAN speed	100 Mbps
Source NAT	\checkmark
Use as backup	
IP addressing method	DHCP -
Only four uplinks with l can be created	DHCP IP addressing method
WAN PORT ASSIGNMENT Port	GE-0/0/2
Secure with ACL	\checkmark
	Cancel

Step 4: Click Save.

Step 5: Repeat Step 2 - Step 4 for each dual uplink.

WAN Uplinks / Ports							+	
UPLINK	ТҮРЕ	PORT	VLAN ID	ADDRESS	SPEED	NAT	BACKUP	
isp-2_inet	INET	GE-0/0/2	4085	DHCP	100 Mbps	Enabled	Disabled	
isp-1_inet	INET	GE-0/0/3	4086	DHCP	200 Mbps	Enabled	Disabled	

4.12 Specify the SD-WAN Data Center Preferences

Use this procedure to assign the data center preferences for route orchestration toward the VPN concentrators.

Step 1: On the Gateways tab, in the SDWAN & Routing section, select **DC Preferences**.

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

	x + Leentral.aubanetworks.com/frontend/#/cass(basic/ypreouting?tsb+yprhubs		*	8
aruba Central	Q Search or ask Aruba	2 (0	8
∀ BGW-7005 ▼				
11 GROUP	CACCESS POINTS C SWITCHES C GATEWAYS	:=	ıl.	۲
- MANAGE -	SYSTEM LAN WAN SDWAN & ROUTING POLICIES Advanced Mode G			
88 OVERVIEW	SYSTEM LAN WAN SDWAN & ROUTING POLICIES Advanced Mode G	uide	Setu	p
	DC Preference Static Routing Overlay Routing			
2. GUESTS	If your deployment includes VPN Concentrators (VPNCs) deployed in one or more hub sites, your branch gateways can be configured to create a hub-n-spoke IPsec based VPN SI	how N	ore	
APPLICATIONS	Per-field help			
SECURITY				
- ANALYZE	Overlay Orchestrator Peering : Disabled			
ALERTS & EVENTS	Overlay orchestration will be enabled once DC preference is configured			
AUDIT TRAIL	DC Preference +			
TOOLS	HUB GROUP PRIMARY VPNC SECONDARY VPNC			
REPORTS				
- MAINTAIN	No data to display			
G FIRMWARE				
1				

Step 3: In the **Hub Group** drop-down list, select a VPNC group for the preferred data center (example: **VPNC-7210**).

Step 4: In the Primary VPNC drop-down list, select the primary VPNC.

Step 5: In the Secondary VPNC drop-down list, select the secondary VPNC.

Step 6: Repeat Step 2 - Step 5 if a secondary data center is used.

Step 7: Click Save Settings.

our deployment includes	VPN Concentrators (VPNCs) depl	loyed in one or more hub sites, your branch gatew	vays can be configured to
r-field help			
Overlay Orchestrator P	Peering : Disabled		
 Overlay orchestration 	will be enabled once DC prefere	ence is configured	
			+
DC Preference			
	PRIMARY VPNC	SECONDARY VPNC	
DC Preference HUB GROUP VPNC-7210	PRIMARY VPNC		
HUB GROUP			
IUB GROUP			

Aruba Central automatically enables overlay orchestrator peering after you click Save Settings.

DC Preference					
HUB GROUP	PRIMARY VPNC	SECONDARY VPNC			
WPNC-7210	DC2-7210-1 [00:1a:1e:05:01:a0]	DC2-7210-2 [00:1a:1e:05:01:28]			
WPNC-7024	DC1-7024-1 [00:0b:86:bb:bb:a7]	DC1-7024-2 [00:0b:86:bb:ff:a7]			

4.13 Configure the SD-WAN Overlay Routing

You should redistribute branch subnets in the VPN overlay to enable the dynamic routing functionality at the headend site.

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

oruba Central	Q Search or	ask Aruba 🔍 💿 👪 🖧
7 BGW-7005 🔻		
GROUP	🗟 ACCESS POINTS 📼 SWITCHES 🙊 GATEWAYS	SELECTED GROUP TYPE Branch Gateway 🗄 II.
MANAGE	SYSTEM LAN WAN SDWAN & ROUTING	POLICIES Advanced Mode Guided Setup
OVERVIEW	STSTEM LAN WAN SOWAN & ROUTING	POLICIES Advanced Mode Guided Setup
DEVICES	DC Preference Static Routing Overlay Routing	
E& CLIENTS		
& GUESTS	Redistribute connected vlans Select VLANs	
# APPLICATIONS	Redistribute static route	
SECURITY		
ANALYZE		
ALERTS & EVENTS		
AUDIT TRAIL		
TOOLS		
REPORTS		
FIRMWARE		
B FIRMWARE		

Step 2: In the **Redistribute connected vlans** box, select all of the user VLANs and system IP VLAN for overlay redistribution.

Step 3: Click Save Settings.

DC Preference Static Routing	Overlay Routing
Redistribute connected vlans	(Vian 1 X) (Vian 20 X) (Vian 4087 X) search
Redistribute static route	
	Cancel Save Settings

4.14 Configure Role-Based Policies for the Branch Gateways

Use this procedure to define the policies for user VLANs to allow network access.

Step 1: On the Gateways tab, in the Policies section, select **Roles**.

🔍 🔍 💽 🧟 Aruba Central \leftrightarrow \rightarrow C \bullet app-prod2-* 🕒 i aruba 0 5 ۹ 👁 🏭 🖁 ▼ BGW-7005 ▼ 🛱 GROUP TACCESS POINTS SWITCHES GATEWAYS i≣ n. ⊗ SYSTEM LAN WAN SDWAN & ROUTING POLICIES 88 OVERVIEW Guided Setup DEVICES Roles Applications DPS QOS Security LD CLIENTS Each user or device connected to the bra signed, it can be used in traffic and security po St. GUESTS Per-field help APPLICATIONS SECURITY + Roles Role assignment (+) ap-role authenticated default-via-role default-vpn-role VLAN NAME ALERTS & EVENTS AUDIT TRAIL & TOOLS guest guest-logon REPORTS G FIRMWARE

Step 2: In the Role assignment table, click the plus (+) sign.

Step 3: In the Role assignment dialog box, implement the following settings:

- VLAN ID—Management (1)
- Initial Role—authenticated
- Authentication—Disable this option

Step 4: Click Save.

Role assignment		
VLAN ID	Management (1) 🔻	
Initial Role	authenticated	
Authentication		
		Cancel

Step 5: Repeat Step 2 - Step 4 for all of the user VLANs (example: Employee).

ROLE ASS	IGNMENT			+
VLAN	NAME	AUTHENTICATION	ROLE	
1	Management	Disabled	authenticated	
20	Employee	Disabled	authenticated	

Procedures

Configuring a Branch Gateway Device—One Branch Gateway per Branch

- 5.1 Assign a Device to a Branch Gateway Group
- 5.2 Initiate the Branch Gateway Device Configuration
- 5.3 Assign a Hostname to the Branch Gateway Device
- 5.4 Assign IP Addresses to the VLANs

5.1 Assign a Device to a Branch Gateway Group

Use this procedure to assign a device to a branch gateway group to inherit global configurations.

Step 1: On the Aruba Central Account Home page, select **Device Inventory**.

Step 2: In the View Devices table, select a branch gateway, and then click **Assign Group**.

SO TO ACCO	OUNT HOME								
	NVENTO	2V							
View the devices i	n your inventory an	d manually add	I devices here.						
VIEW DEVICE									
	MAC ADDRESS	TYPE	IP ADDRESS	NAME	Y MODEL	PART NUMB	GROUP	▼ SUBSCF 💻	
								~	
CNDDJSSTDQ	20:A6:CD:C0:38:	iap	10.8.0.2	AP305-D6	IAP-305-US	JX946A	default		
CNDDJSSTDX	20:A6:CD:C0:38:E2	iap	10.8.0.4	AP305-E2	IAP-305-US	JX946A	default		
CNDDJSSTDY	20:A6:CD:C0:38:E4	iap			IAP-305-US	JX946A IX946A			
CNDRJSSDV0	20:A6:CD:C3:0A:	iap			IAP-305-US	JX946A JX946A		0	
CNDRJSSDWH CNDRJSSDWP	20:A6:CD:C3:0A:	lap lap			IAP-305-US	JX946A JX946A		0	
CNDRJSSDWP CNFDK513T2	38:17:C3:C0:53:8A	iap	10.8.0.3	AP345-8A	AP-345-US	JX946A JZ033A	default	0	
CNEDK51312 CNEJKD58Y5	58:17:C3:C0:53:8A F4:2E:7F:C7:7D:F2	iap	10.8.56.106	AP345-8A R\$15-AP-515-1	AP-345-US	09H63A	BGW-Du_	0	
CNHJKD58Y5 CNHJKD58Y6	F4:2E:7F:C7:8E:B8	iap	10.8.56.105	RS15-AP-515-1	AP-S15-US	Q9H63A	BGW-Du_	0	
CNHLK9W0PX	00:4E:35:C4:9A:5E	iap	192,168,1,156	IAP535-RS12	AP-535-US	IZ337A	default	0	
 CNHPK9Y01Q 	80:8D:87:C0:15:F9	iap	10.8.56.104	R\$15-AP-555-1	AP-555-US	JZ357A	BGW-Du	0	
 CP0001664 	00:0B:86:B8:75:78	controller(G			7005-US	7005-US		0	
 CP0002586 	00:08:86:88:92:48	controller(G			7005-US	7005-US		0	
 CP0015098 	00:08:86:8F:59:60	controller(G			7005-US	JW634A		õ	
 CP0025945 	20:40:03:12:6E:28	controller(G			7005-US	JW634A		Ø	
• CP0025951	20:40:03:12:66:58	controller(G	10.8.255.210	RS15-7005-1	7005-US	JW634A	BGW-Du	0	
• CP0025992	20:4C:03:12:6F:A0	controller(G	-	ile	7005-US	JW634A		0	
• CP0025999	20:4C:03:12:6F:D8	controller(G	11	2	7005-US	JW634A		0	
 CP0026016 	20:40:03:12:70:60	controller(G			7005-US	JW634A			

Step 3: In the **Assign a Group to the Select Device** dialog box, select the Branch Gateway group you created in Procedure 4.1 (example: **BGW-7005**).

GROUP NAME	
TG 2930F-Single	
TG 2930M-Stack	
TG 3810M-Single	
BGW-7005	
BGW-7005-HA	
BGW-Dual-RS15	
default	
SW-3810-GRP	
SW-BRANCH-GRP	
VPNC-7024	
VPNC-7210	

Step 4: Click Assign device(s), and then click OK.



5.2 Initiate the Branch Gateway Device Configuration

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

Step 2: In the filter drop-down list, select the branch gateway group you created in Procedure 4.1 (example: **BGW-7005**).

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

Step 4: In the **Gateways** table, select the device you intend to configure.

🔍 🔍 🔍 🧕 Aruba Central								
← → C a app-prod2	-ui.central.arubanetworks.com/frontend/#/	GATEWAY/LIST				\$		
aruba Central			Q Search or ask Aruba			۹ (۵		8
▼ BGW-7005 ▼								
11 GROUP	access points 📼 switch					:=	њ.	8
- MANAGE								
88 OVERVIEW		OWN						
		1						
E& CLIENTS	GATEWAYS						Ł	0
& GUESTS		IF MODEL	FIRMWARE VERSION	UPTIME	IP ADDRESS			
# APPLICATIONS	o JW634A-20:4C:03:12:6F:A0	JW634A	Unknown					
SECURITY								
- ANALYZE								
ALERTS & EVENTS								
AUDIT TRAIL								
S TOOLS								
REPORTS								
- MAINTAIN								
FIRMWARE								

For educational purposes, the next step exits the guided setup.

Step 5: In the Guided Setup dialog box, click Cancel, and then click Exit.

aruba Central	Guided Setup for Branch Gateway Device
1 System	This wizard will guide you through the essential steps to configure the branch gateways in the Device .
2 LAN	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	After completing this initial setup, you can change the settings at any time.
4 SDWAN & Routing	
5 Redundancy	Cancel



5.3 Assign a Hostname to the Branch Gateway Device

Step 1: On the Gateway tab, in the System section, select **Hostname**.

Step 2: In the Hostname box, enter a name (example: RS11-7005-1), and then click Save Settings.

oruba Central	Q Search or ask Aruba	۹ 🔿 🏭
BGW-7005 🔻	JW634A-20:4C:03:12:6F:A0 ×	
GATEWAY	🗇 GATEWAY	SELECTED DEVICE TYPE Branch Gateway
IANAGE		
OVERVIEW	SYSTEM LAN WAN SDWAN & ROUTING REDUNDANCY	Advanced Mode Guided Setup
DEVICE	System IP Hostname	
CLIENTS		
APPLICATIONS	Hostname RS11-7005-1	
ALYZE		
ALERTS & EVENTS		
AUDIT TRAIL		
TOOLS		
REPORTS		
FIRMWARE		
FIRMIWARE		

5.4 Assign IP Addresses to the VLANs

In this procedure, you assign IP addresses, and define the DHCP scope, for the management and user VLANs.

Step 1: On the Gateway tab, in the LAN section, select VLANs.

Step 2: In the VLANS table, select the **Management** VLAN, and then click the pencil icon.

		EWAY StLETED DIVICE TWY Branch Gateway GE SYSTEM VERVIEW SYSTEM VERVIEW SYSTEM VIANS LAN VIANS LAN Ports VIANS LAN Po	EWAY SILECTED DIVICE TYPE Branch Gateway GE SYSTEM VERVIEW SYSTEM UNN SDWAN & ROUTING REDUNDANCY Advanced Mode GUIDED VIANS LAN Ports Stateway UNN LAN Ports Each branch gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Show More Per-field help IP DHCP server VLANS 1 Management 20 Employee 20 Employee 20 Employee 20 Employee 20 Employee 305 Vun, 686 20 Engloyee 305 20 State 20 Engloyee 305 20 Engloyee 305 20 Engloyee 305 306 307	EWAY SILECTED DIVICE TYPE Branch Gateway GE SYSTEM VERVIEW SYSTEM UNN SDWAN & ROUTING REDUNDANCY Advanced Mode GUIDE SUBJECTION LAN Ports LAN Ports <th>ruba Centra</th> <th></th> <th></th> <th>Q Search or ask A</th> <th></th> <th></th> <th></th> <th>۹ @ :</th> <th>16 6</th>	ruba Centra			Q Search or ask A				۹ @ :	16 6
CATEWAY C GATEWAY C GATEW		EWAY IS GATEWAY Branch Gateway GE Get Comparison Advanced Mode Guided Setue VERVIEW VIANS LAN WAN SDWAN & ROUTING REDUNDANCY Advanced Mode Guided Setue VIANS LAN WAN SDWAN & ROUTING REDUNDANCY Advanced Mode Guided Setue VIANS LAN Port Feer field help Feer field help Feer field help Feer field help VIANS VIANS VIANS STATIC DYNAMIC DICP Pool DicP MELAY Feer field help 20 Engingere - Disabled Guided Setue Feer field help 20 Engingere - Disabled Feer field help	EWAX © GATEWAX Branch Gateway GL GL GL SYSTEM VERVIEW SYSTEM VAN SDWAN & ROUTING VENCE VLANS VENTS Lan Ports Each branch gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or SRew More ZEL Per-field help IP DHCP server VLANID NAME 20 Engingee 20 Enging	VEWAY © GATEWAY Branch Gateway GL GL GL SYSTEM VERVIEW SYSTEM VENCE VLANS VENTS Seach branch gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Sector State Per-field help IP DHCP server IP DHCP server VLANID NAME 20 Employee	W-7005 V	JW634A-20:4C:03:12	2:6F:A0 ×						
g OVERVIEW SYSTEM LAN WAN SDWAN & ROUTING REDUNDANCY Advanced Mode Guil g DEVICE VLANS LAN Ports LAN Ports Each branch gateway will require one or more LAN VLANS and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Shot g AppLiCATIONS Each branch gateway will require one or more LAN VLANS and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Shot g Audort TRAIL IP DHCP server IP IP DHCP server IP g REPORTS VLANS Static DYNAMIC DHCP FOOL DHCP RELAY	or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Show More	VERVIEW SYSTEM LAN WAN SDWAN & ROUTING REDUNDANCY Advanced Mode Guided Setu VERVIEW VLAN LAN NAN SDWAN & ROUTING REDUNDANCY Advanced Mode Guided Setu VERVIEW VLAN LAN Port Store	VERVIEW SYSTEM LAN WAN SDWAN & ROUTING REDUNDANCY Advanced Mode Guided Sets VERVIEW VLANS LAN Ports LAN Ports Redundance	VERVIEW SYSTEM LAN WAN SDWAN & ROUTING REDUNDANCY Advanced Mode Guided Set VERVIEW VLANS LAN Ports LAN Ports Redundance <	TEWAY	GATEWAY					SELECTED DEVICE TYPE Branch Gateway		1
VEX.NEW VEX.NS LAN Ports CLIENTS APPLICATIONS Each branch gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Sho will vizit Per-field help Per-field help ALERTS & EVENTS IP DHCP server AUDIT TRAIL VLANS TOOLS VLANS REPORTS NAME	or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Show More	VILANS VILANS LAN Ports IENTS Each branch gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Show More ZZ	VLANS VLANS LENTS PublicAttions ZZE Fer-field help LERTS & EVENTS JDIT TRAIL JDIT TRAIL Policy server VLANS Static UNAND NAME Static Drivanic ObcP Pool Dir Gradied Image meet 20 Engingele 20 Engingele </td <td>VLANS VLANS LENTS Per-field help Per-field help IP DHCP server VLANS TATIC VLANS I ANN Static 20 Engingee 20 Engingee</td> <td>AGE</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	VLANS VLANS LENTS Per-field help Per-field help IP DHCP server VLANS TATIC VLANS I ANN Static 20 Engingee	AGE								
CLIENTS LAN Ports CLIENTS LAN Ports CLIENTS LAN Particle branch gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Sho NUTZE Per-field help ALERTS & EVENTS AUDIT TRAIL TOOLS REPORTS LAN ID NAME STATIC DYNAMIC DHCP FOOL DHCP RELAY	e - Deabled	ILENTS LAN Ports	LENTS Each branch gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Show More Per-field help IP DHCP server IP DHCP server VLANS IP DHCP Server IP D	VLANS VLANS LAN Ports spelicAtions Each branch gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Show More vertications Per-field help IP DHCP server Image: Show More vertications VLANS Show More Image: Show More vertications Image: Show More Image: Show More Image: Show More vertications Image: Show More Image: Show More Image: Show More vertications Image: Show More Image: Show More Image: Show More vertications Image: Show More Image: Show More Image: Show More vertications Image: Show More Image: Show More Image: Show More vertications Image: Show More Image: Show More Image: Show More vertications Image: Show More Image: Show More Image: Show More vertications Image: Show More Image: Show More Image: Show More vertications Image: Show More Image: Show More Image: Show More vertications Image: Show More Image: Show More Image: Show More vertications Image: Show More Image: Show More Image: Show More vertications	OVERVIEW	SYSTEM LA	N WAN SDV	VAN & ROUTING RED	UNDANCY		Advanced Mode	Guided Set	up
CLEENTS Each branch gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Sho VIZE Per-field help ALERTS & EVENTS IP DHCP server VIZE VLANS TOOLS YLAN ID NAME STATE DYNAMIC DHCP Pool DHCP RELAY	STATIC DYNAMIC DHCP POOL DHCP RELAY ment - Dealed re - Dealed	LENTS Each branch gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or "Show More Perfield help Zet Perfield help LENTS & EVENTS DDIT TRAIL DOOLS AMM I AMM Static DYNAMIC Dic/ Pols 1 Market Static 20 Engingere - 20 Engingere - </td <td>LIENTS Each branch gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Show More Perfield help LIENTS & EVENTS DDIT TRAIL DOOLS REPORTS I Name Static DYNAMIC DHCP Pool VLANS Name 20 Engisyee 20 Engisyee<</td> <td>UENTS Each branch gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Show More Perfield help LERTS & EVENTS DDIT TRAIL DOOLS REPORTS IP DHCP server IP VLANS NAME STATIC DYNAMIC DHCP POOL DHCP RLAY 1 Margement I Databled 20 Employee - Databled 20 Employee - Databled</td> <td>DEVICE</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	LIENTS Each branch gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Show More Perfield help LIENTS & EVENTS DDIT TRAIL DOOLS REPORTS I Name Static DYNAMIC DHCP Pool VLANS Name 20 Engisyee 20 Engisyee<	UENTS Each branch gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Show More Perfield help LERTS & EVENTS DDIT TRAIL DOOLS REPORTS IP DHCP server IP VLANS NAME STATIC DYNAMIC DHCP POOL DHCP RLAY 1 Margement I Databled 20 Employee - Databled 20 Employee - Databled	DEVICE								
VIZE - Per-field help VIZE SE EVENTS IVIDIT TRAIL VILANS - + VILANS - + VILANIO NAME STATE DYNAMIC DHCP FOLL DHCP RELAY	STATIC DYNAMIC DHCP POOL DHCP RELAY ment - Dealed re - Dealed	VALUATION Per-field help VDIT TRAIL IP DHCP server VLANS VLANS VLANID NAME 20 Employee 20 Employee 20 Employee 405 Van, 6056 4066 Van, 6056	VILANIOS Per-field help JDIT TRAIL IP DHCP server JDIT TRAIL VILANIO VILANIO NAME 1 Margement 20 Engioyee 20 Engioyee 405 Vulanids 4065 Vulanids	VILANIOS Per-field help JDIT TRAIL IP DHCP server JOIS VILANIO VLANIO NAME 20 Engioyee 20 Engioyee 20 Engioyee 405 Vulanids 4065 Vulanids	LIENTS	VLANS	orts						
VZZ Per-field help LERTS & EVENTS IP DHCP server VLANS + VLANS + VLAN ID NAME STATIC DYNAMIC DHCP FOL DHCP RELAY	et a builded build because and a builded build because a builded build b	Value NAME Static Dividend Value Modgement - - Value Modgement - - Value Modgement - - Value Modgement - - Value Value - - Value Value - - Value Value - - Value Value - -	VILAN ID NAME STATIC DVXAMIC OHCP Pool DHCP RELAY VILAN ID NAME STATIC DVXAMIC OHCP Pool DHCP RELAY VILAN ID NAME STATIC DVXAMIC OHCP Pool DHCP RELAY VILAN ID NAME STATIC DVXAMIC OHCP Pool DHCP RELAY VILAN ID NAME STATIC DVXAMIC OHCP Pool DHCP RELAY VILAN ID NAME STATIC DVXAMIC OHCP Pool DHCP RELAY VILAN ID NAME STATIC DVXAMIC OHCP Pool DHCP RELAY VILAN ID NAME STATIC DVXAMIC OHCP Pool DHCP RELAY VILAN ID NAME STATIC DVXAMIC OHCP Pool DHCP RELAY VILAN ID NAME STATIC DVXAMIC OHCP Pool DHCP RELAY VILAN ID NAME STATIC DVXAMIC OHCP Pool DHCP RELAY VILAN ID NAME STATIC DVXAMIC OHCP Pool DHCP RELAY VILAN ID NAME STATIC DVXAMIC OHCP POOL DHCP RELAY	VILAN ID NAME STATIC DVIANIC DICP FOOL DICP RELAY VILAN ID NAME STATIC DVIANIC DICP FOOL DICP RELAY VILAN ID NAME STATIC DVIANIC DICP FOOL DICP RELAY VILAN ID NAME STATIC DVIANIC DICP FOOL DICP RELAY VILAN ID NAME STATIC DVIANIC DICP FOOL DICP RELAY VILAN ID NAME STATIC DVIANIC DICP FOOL DICP RELAY VILAN ID NAME STATIC DVIANIC DICP FOOL DICP RELAY VILAN ID NAME STATIC DVIANIC DICP FOOL DICP RELAY VILAN ID NAME STATIC DVIANIC DICP FOOL DICP RELAY VILAN ID NAME STATIC DVIANIC DICP FOOL DICP RELAY VILAN ID NAME STATIC DVIANIC DICP FOOL DICP RELAY VILAN ID NAME STATIC DVIANIC DICP FOOL DICP RELAY VILAN ID NAME STATIC DVIANIC DICP FOOL DICP RELAY	PPLICATIONS	Each branch gateway	will require one or more LA	VLANs and IP interfaces to	support infrastructure and client	devices in your branches. Each V	LAN will either be statically or	Show More	
LERTS & EVENTS UDIT TRAIL OOLS VLANS + EPORTS VLAN ID NAME STATIC DYNAMIC DHCP FOOL DHCP RELAY	STATIC DYNAMIC DHCP POOL DHCP RELAY mmet - Deabled Image: Comparison of the point	ERTS & EVENTS JDIT TRAIL JOLS AIN AIN AIN AIN AIN AIN AIN AIN	IP DHCP server IP DHCP server VLAN ID VLAN ID VLAN ID NAME 1 Margement 20 Engloyee 20 Engloyee 405 Vun,4056 4065 Vun,4056	IP DHCP server IP DHCP server VLAN ID VLAN ID VLAN ID NAME 1 Margement 20 Engloge 20 Engloge 405 Vun, 4056 4065 Vun, 4056		Per-field help							
IP DHCP server IP VUDIT TRAIL VLANS OOLS YLAN ID VIAN ID NAME STATIC DYNAMIC DHCP FOOL DHCP RELAY	et a builded build because and a builded build because a builded build b	IP DHCP server Import VLANS VLANS VLANID NAME VLANID NAME 1 Margeneet 20 Engipyeet 20 Engipyeet 405 Van, 4056 4066 Van, 4056	IP DHCP server Image: market of the server Image: mark	IP DHCP server Image: market of the server VLANS VLANS VLAN ID NAME SPORTS Market of the server 1 Market of the server 20 Engloyeet 20 Engloyeet 405 Van, 4056 4056 Van, 4056		i crincia neip							
VLANS + EPORTS VLAN ID NAME STATIC DYNAMIC DHCP POOL DHCP RELAY	STATIC DYNAMIC DHCP POOL DHCP RELAY mmet - Deabled Image: Comparison of the point	VLANS + PORTS NAME NAME STATIC DPIXAMIC DHCP POOL DHCP ATLAY AIM 1 Movagement - Deadledt Deadledt AIM 20 Employee - Deadledt Deadledt 405S Van, 4056 - Deabledt - Deabledt	VLANS YLANS + VLAN ID NAME STATC DYNAMIC ChCP POOL DHCP RLIAY 1 Margement - Drawled Drawled 20 Brighyse - Drawled Drawled 4055 Vun_4066 - Drawled -	VLANS VLANS PYNAMIC DICP POOL DHCP RLAY VLAN ID NAME STATC DYNAMIC DICP POOL DHCP RLAY 1 Margement - Doubled Doubled 20 Brighysek - Doubled Doubled 4065 Van, 4066 - Doubled Doubled		IP DHCP server	>						
COLS VLAN ID NAME STATIC DYNAMIC DHCP POOL DHCP RELAY	et a builded build because and a builded build because a builded build b	VAN ID NAME STATIC DYNAMIC DICP FOOL DICP FLAY IPORTS 1 Jack I Disability AMM 20 Indigeneeit I Disability MWARE 4065 Vuin, 6066 I Disability	VLAN ID NAME STATIC DYNAMIC DHCP POL DHCP RLAY PPORTS 1 Management - Catabled 20 Employee - Catabled 20 Employee - Disabled 405 Van, 4056 - Disabled	VLAN ID NAME STATC DYNAMIC DHCP POL DHCP RLaY PPORTS 1 Management - - Dashed 20 Employee - - Dashed RMWARE 4065 Van, 4086 - Dashed	UDIT TRAIL	VIANS					+		
EPORTS CONTRACTOR OF	ment - Dashted	I Maragement - Disabled AMI 20 Employee - Disabled RMWARE 4085 Value085 - Disabled 4086 Value086 - Disabled	I Management Obselved TAUN 20 Employee - Disabled RMWARE 4085 Vain_4085 - Disabled 4086 Vain_4086 - Disabled	I Management Disabled TANN 20 Employee - Disabled RMWARE 4085 Vain_4085 - Disabled 4086 Vain_4086 - Disabled	OOLS								
1 Management , Dishled 🗍 🖍	ve - Disabled	All 20 Employee - Disabled RMVARE 4085 Van_4085 - - Disabled 4086 Van_4086 - Disabled	ZAIN 20 Employee - Disabled RMWARE 4085 Van_4085 - Disabled 4066 Van_4086 - Disabled	ZAIN 20 Employee - Disabled RMWARE 4085 Van, 4085 - Disabled 4066 Van, 4086 - Disabled	EPORTS	VLAN ID		STATIC	DYNAMIC DHEP POOL				
	15 · Disabled	4086 Van,4086 - Disabled	4086 Van, 4086 · · Disabled	4086 Van, 4086 · · Disabled	FAIN	20							
RMWARE 4085 · · Disabled					RMWARE	4085	Vlan_4085		(A)	Disabled			
		4087 System®_4087 - Disabled	4087 System®,4087 - Disabled	4087 System®,4087 - Disabled									
	8 4087 Dirabled					4087	SystemIP_4087	3		Disabled			
	2 4797 Dirablad					4087	SystemIP_4087	1		Disabled			
							appenning and a			and and a second s			
4087 System#_4087 Disadeed	anna - manura												
4087 Systemin, 4087 • • Disabled													
4087 Systemin, 4087 • • Disabled	2007 · · · · · · · · · · · · · · · · · ·												
4087 systemic, 4087 • • Disabled													
KOR? Systemine_KOR? • • Disabled													
4087 systemine_6087 + + Disabled													
4087 system/#_4087 • • Diadoled													
4087 system/#_6087 • • Disabled													
4087 systemme_4087 - + Disabled													
4087 systemme_4087 - + Disabled													

Step 3: In the VLAN - Management dialog box, implement the following settings:

- IPV4 Address—10.8.40.1
- Netmask—255.255.255.0
- Act as DHCP server—Enable this option
- Default router—10.8.40.1
- Domain name—example.local
- DNS server type—Public DNS Server
- DNS Service Provider—Google

Name	Management
VLAN ID	1
IP addressing mode	Static 🝷
IPV4 ADDRESS	10.8.40.1
Netmask	255.255.255.0
Act as DHCP server	
Network	10.8.40.0
Netmask	255.255.255.0
Default router (Optional)	10.8.40.1
Domain name (Optional)	example.local
DNS server type	Public DNS Servir 🔻
DNS Service Provider	Google 👻
Enable DHCP relay	

Step 4: Click Save.

Step 5: Repeat Step 2 - Step 4 for any additional VLANs (example: Employee).

VLANS					+
VLAN ID	NAME	STATIC	DYNAMIC DHCP POOL	DHCP RELAY	
1	Management	10.8.40.1 / 24	20 20	Disabled	
20	Employee	10.8.41.1 / 24		Disabled	
4085	Vlan_4085			Disabled	
4086	Vlan_4086		22	Disabled	
4087	SystemIP_4087	1	12	Disabled	

Procedures

Configuring the Branch Gateway Group for High Availability—Two Branch Gateways Per Branch

- 6.1 Create a New Branch Gateway Group
- 6.2 Create the System IP Address Pool for the Branch Gateway Group
- 6.3 Select the Hardware Model of the Gateway Group
- 6.4 Select the Branch Gateway Group Time Zone
- 6.5 Configure the DNS Servers for the Branch Gateway Group
- 6.6 Create a Management User Account for the Branch Gateways
- 6.7 Configure VLANs for the Branch Network Devices and Users
- 6.8 Configure the LAN Ports for the Branch Gateway
- 6.9 Configure WAN Health Checks
- 6.10 Configure the WAN Load Balancing Algorithm
- 6.11 Configure the WAN Service Providers
- 6.12 Specify the SD-WAN Data Center Preferences
- 6.13 Configure the SD-WAN Overlay Routing
- 6.14 Configure Role-Based Policies for the Branch Gateways

In this set of procedures, we configure a branch gateway group that can be used for sites that include two branch gateways for high availability.

6.1 Create a New Branch Gateway Group

In this procedure, you create a branch gateway group and assign a type to the branch gateway group.

Step 1: In filter drop-down list, select All devices, and then in the left navigation pane, select Organization.

Step 2: On the Groups tab, click New Group.

KIGRAL El GROUPS SITES AND LABELS CERTIFICATES INSTALL MANAGER MOVE OVERVIEW GROUPS A group in Auba Central acts like a primary configuration container for devices. You can combine devices with common configuration requirements into a single group in Auba Central acts like a primary configuration container for devices. You can combine devices with common configuration requirements into a single group in Auba Central acts like a primary configuration central net for devices. You can combine devices with common configuration requirements into a single group in Auba Central acts like a primary configuration central net for devices. You can combine devices with common configuration requirements into a single group in Auba Central acts like a primary configuration central net for devices. You can combine devices with common configuration requirements into a single group in Auba Central acts like a primary configuration central net for devices. You can combine devices with common configuration requirements into a single group in Auba Central acts like a primary configuration central net for devices. You can combine devices with common configuration requirements into a single group in Auba Central acts like a primary configuration central net for devices. ManAGE GROUPS ANVAT DBMG AND DROP CLISTERS AND SWITCHES BETWEEN GROUPS Primary Configuration central net for devices. YucAtION Y the Y SERVEL # YucAcADDRESC ALICONNECTED DEVICES 0 Vication YucAtION Y the Zentral Acts like Auba Zentral A	aruba Central			٥					۹ (۵	1
Number OverAntige Second State Value Value <th>All Devices V</th> <th>Pe coours discus</th> <th></th> <th>A crossecure</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	All Devices V	Pe coours discus		A crossecure						
OWNERVEW DEVICES CLEATS GROUPS Arguing and apply the same configuration container for devices. You can combine devices with common configuration requirements into a single group and apply the same configuration returns to all the devices. In the group. GUESTS Applications Security MARGE GROUPS DBM AND DROP CLEATERS AND SWITCHES BETWEEN GROUPS TO SELECT MULTIPLE DEVICES SHIFT-CLICK OR CTRL+CLICK SECURITY NEWWORK SERVICES ALTATE ALEATS & EVENTS ALEATS & EVENTS ALIGN SERVICES VCACID INVEX VIACES VIACES VIACES And ADD TORAL VIACES VIACES <t< th=""><th></th><th>LL GROUPS C SITE</th><th>S AND LABELS</th><th>CERTIFICATES</th><th>INSTALL MANAGER</th><th></th><th></th><th></th><th></th><th></th></t<>		LL GROUPS C SITE	S AND LABELS	CERTIFICATES	INSTALL MANAGER					
DIVICES A group in Aruba Central acts like a primary configuration container for devices. You can combine devices with common configuration requirements into a single group and apply the same configuration requirements into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same configuration requirements. Into a single group and apply the same config		CROURC								
CLIENTS group and apply the same configuration settings to all the devices in the group. GUESTS MANAGE GROUPS AppLications DRAG AND DROP CLUSTERS AND SWITCHE'S BETWEEN GROUPS' TO SELECT MULTIPLE DEVICES SHIPT-CLUCK OR CTRL+CLUCK Vince Vince <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>2</td></t<>										2
Annage MANAGE GROUPS AppLications DRAG AND DROP CLUSTERS AND SINCHES BETWEEN BODUPS to SELECT MULTIPLE DEVICES SHIPT-CLUCK OR CTRL-CLUCK NETWORKSERVICES Value DRVCS Vinces <						an combine devices	with comm	on configuration n	equirements into a singi	5
APPLICATIONS SECURITY DRAG AND DROP CLUSTERS AND SWITCHES BETWEEN GROUPS TO SELECT MULTIPLE DEVECES SHIPT-CLUCK OR CTRL-CLUCK NETWORK SERVICES VINCES VINCES <th< td=""><td></td><td></td><td>20</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></th<>			20							
XI-LICATIONS TO SELECT MULTIPLE DEVECES SHEFT-CLICK OR CTRL-CLICK SECURITY Onces VIANO				TCHES BETWEEN GR	OUPS					
VCROUP HAME DIVCES VLMAF VLMAF VLOATION VTMP VSRUL VMAA <address< th=""> ALVET ALL CONTACTED DEV/C. 19 Auba-2004640-R. SpringUnited States Andas CV79H2021 40.03.13.65.00 ALDET TABL TO 23004-Sank 0 Auba-200512.62.83 SpringUnited States AC C902592 204:0312.64.20 TOOLS To 23004-Sank 0 C017094-21 Saramento.United KC C9002592 204:0312.64.20 REPORTS To 23004-Sank 0 C017094-21 Saramento.United KC C900091 0008.88bcbbha7 REPORTS To 33004-Sank 0 C017094-21 Saramento.United KC C9001697 001.11:60512.6 REPORTS 5 C00048715 5 C012701-0 Saramento.United KC C9001697 001.11:60512.0 REPORTS 6fault 7 C00048715 5 C001471 001.11:60512.0 001.11:60512.0 001.11:60512.0 001.11:60512.0 001.11:60512.0 001.11:60512.0 001.11:</address<>										
ALIZ ALI CONNECTED DIVIC. 19 Auba-20064G-Pe. SpringUnited States Auba-2. O/179H2031 H03.43/b/7.50 ALERTS & EVENTS UNASSIGNID DIVICIS 0 Auba-2. SpringUnited States Auba-2. O/7995294 403.43/b/7.50 AUDIT TRAIL To 23305-Single 0 Auba-2. SpringUnited States KC CP025945 204.c03.12.64.20 TOOLS To 23305-Single 0 0 0.00.858.bbb.304 00.00.858.bbb.304 REPORTS To 3810M-Single 0 0.00.858.bbb.304 0.00.858.bbb.304 0.00.858.bbb.304 INTAIN B0W-7005 0 0.00.858.bbb.304 0.00.858.bbb.304 0.00.858.bbb.304 REPORTS To 3804M-5010 0.00.878.bbb.304 0.00.858.bbb.304 0.00.858.bbb.304 REPORTS B0W-7005 0.00.878.bbb.304 0.00.858.bbb.304 0.00.858.bbb.304 0.00.858.bbb.304 REPORTS B0W-7005 0.00.878.bbb.304 0.00.858.bbb.304 0.00.858.bbb.304 REPORTS B0W-7005 0.00.878.bbb.304 <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>										
ALECTONNEL Deficience Deficience <thdeficience< th=""> Deficience Deficien</thdeficience<>		GROUP NAME	DEVICES		∀ NAME	V LOCATION	Y TYPE	Y SERIAL #		
Multiality Derivation Outcome Control Multiality Derivation M		ALL CONNECTED DEVIC			Aruba-2930F-8G-Po	Spring,United States	Aruba S	CN79HKZ081	f4:03:43:fb:75:c0	1
No. 2009		UNASSIGNED DEVICES	0		Aruba7005_12_6E_28	Spring,United States	MC	CP0025945	20:4c:03:12:6e:28	l
REPORTS 10 0<	AUDIT TRAIL	TG 2930F-Single	0		Aruba7005_12_6F_A0	Spring,United States	MC	CP0025992	20:4c:03:12:6f:a0	l
NIXAM D6W 7005 0 0 DC2-7210-1 Satzmente_Ubited MC CV016870 001.tr1c6050120 FIRMWARE B0W AbaJ-8515 5 DC2-7210-2 Satzmente_Ubited MC CV016872 001.tr1c6050120 DRGANIZATION default 7 DC2-7210-2 Satzmente_Ubited MC CV016872 0.tr1c1c6050120 SW 3810-GRP 1 DC2-7210-2 Satzmente_Ubited MP CV0016872 0.tr1c1c6050120 WP-Thomas1 Satzmente_Ubited MP CV0050571R 20.abcctc03620420	TOOLS	TG 2930M-Stack	0		DC1-7024-1	Sacramento,United	MC	CZ0000091	00:0b:86:bb:bb:a7	l
FIRMWARE B0W-Dual-R515 S - Company DC2-7210-2 Sacramenta_United MC W001672 0111:10:50312 ORGANIZATION default 7 HP-2320:460;POEP - Company Aulub S 562(3)724.2 0409:733:33:460 SW3810.0RP 1 MP-Thomas1 Sacramenta_United MP CND05ST1R 2026cdc0202e	REPORTS	TG 3810M-Single	0		← DC1-7024-2	Sacramento,United	MC	CZ0001699	00:0b:86:bb:ff:a7	
ORGANIZATION default 7 HP-320-486-POEP - Anba S SGR3(P24L) 6409/338.3450.069 SM3310 GBP 1 MP-Tomas1 Saramente_United MP Obj055T1R 29.46cd:00.262	NINTAIN	- BGW-7005	0		DC2-7210-1	Sacramento,United	MC	CV0016870	00;1a:1e:05:01:a0	
WW3810-GRP 1 MP-Thomas1 Sacramenta,United WP CND0jST1R 20a6cdx03/62e	FIRMWARE	BGW-Dual-RS15	5		DC2-7210-2	Sacramento,United	MC	CV0016872	00:1a:1e:05:01:28	
	ORGANIZATION	default	7		HP-2920-48G-POEP		Aruba S	SG82JQP24L	04:09:73:b3:df:40	
Even Crosp 12 Group(s) 12 Group(s) 19 Devices		SW-3810-GRP	1		IAP-Thomas1	Sacramento,United	IAP	CNDDJSST1R	20:a6:cd:c0:36:2e	
		Clone selected Group		12 (1000)(5)					19 Denia	

Step 3: In the Create New group dialog box, implement the following settings:

- Group Name—BGW-7005-HA
- Switch—Unselect this option
- Password—password
- Confirm Password—password

Step 4: Click Add Group.

GROUP NAME BGW-7005-H	A		
Use the grou	ıp as Template group		
	O GATEWAY	SWIT	сн
PASSWORD	87 - 1225F		
CONFIRM PASSWOR	D		

Note If you intend to use the Install Manager App, assign the group to the sites at this point.

Step 5: In the filter drop-down list, select **BGW-7005-HA**.

Step 6: In the left navigation pane, in the Manage section, select **Devices**.

Step 7: Select the **Gateways** tab, and then click the gear icon in top right.

🗧 🔍 🔍 💽 Aruba Central	× +							
← → C 🌲 app-prod2-ui.	.central.arubanetworks.com/frontend/#/GATEWAY/LIST							÷
aruba Central		Q Search or ask Aruba			c	0		8
▼ BGW-7005-HA								
II GROUP	🔯 ACCESS POINTS 📼 SWITCHES 👰 GA	TEWAYS				=	•	۲
- MANAGE						_		_
88 OVERVIEW	GATEWAYS . UP O DOWN							
E& CLIENTS	GATEWAYS						1 6	Э
2 GUESTS	♥ DEVICE NAME IF MODEL	FIRMWAREV	ERSION	E	P ADDRESS			
I APPLICATIONS								
SECURITY								
- ANALYZE								
ALERTS & EVENTS								
AUDIT TRAIL								
A TOOLS								
REPORTS								
- MAINTAIN								
FIRMWARE								
		No data	to display right now					

Step 8: In the Set Group Type dialog box, select **Branch Gateway**, and then click **Save Settings**.



For educational purposes, the next step exits the guided setup.

Step 9: In the Guided Setup dialog box, click Cancel, and then click Exit.

ruba Central	Guided Setup for Branch Gateway Group BGW-7005-HA
1 System	This wizard will guide you through the essential steps to configure
T	the branch gateways in the Group BGW-7005-HA.
2 LAN	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	After completing this initial setup, you can change the settings at any time.
4 SDWAN & Routing	
5 Policies	Cancel
EXIT GUIDE	D SETUP ded Setup will be exited and changes will be lost.
	i can re-enter the Guided Setup at any time to complete it.
	RESUME

6.2 Create the System IP Address Pool for the Branch Gateway Group

Use this procedure to define the system IP address pool that the gateway will use for network services.

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

Step 2: Select Define system IP address pool.

🗢 🔍 💿 🔹 Aruba Central				
\leftrightarrow \rightarrow \mathbb{C} \textcircled{a} app-prod2-ul	central.arubanetworks.com/frontend/#/caas/basic/system?tab=gateway/opool		* (8 1
aruba Central	Search or ask Aruba	9 6	0 11	8
▼ BGW-7005-HA ▼				
C GROUP	CESS POINTS SWITCHES CATEWAYS	:=	16	۲
- MANAGE				
88 OVERVIEW	SYSTEM LAN WAN SDWAN & ROUTING POLICIES Advanced Mode C	Juided	Setu	P
DEVICES	System IP Model Time DNS Management User			
CLIENTS				
SUESTS	Each branch 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	Show M	ore	
APPLICATIONS	Per-field help			
SECURITY	Configuration approach O Define system IP address pool Specify static IP addresses later			
- ANALYZE				
ALERTS & EVENTS	If you do not define a System IP pool, it is necessary to specify the VLAN interface and system IP setting on a per-device basis or for			
AUDIT TRAIL	multiple gateways once using the Bulk configuration upload feature.			
S TOOLS				
REPORTS				
- MAINTAIN				
FIRMWARE				
2				

Step 3: In the Start IP address box, enter 10.8.255.21.

Step 4: In the End IP address box, enter 10.8.255.60, and then click Save Settings.

Configuration approach	Define system IP address pool	O Specify static IP addresses later
Start IP address	10.8.255.21	
End IP address	10.8.255.60	
Gateway pool size	40 Gateways	
Vlan	4087	
		Cancel Save Settings

Step 5: In the Warning dialog box, click **Yes**. When you move gateways to a group, the gateways need to reboot to complete the group configuration.

Warning	
Gateway will be rebooted on saving	g changes. Do you want to proceed?
	No Yes

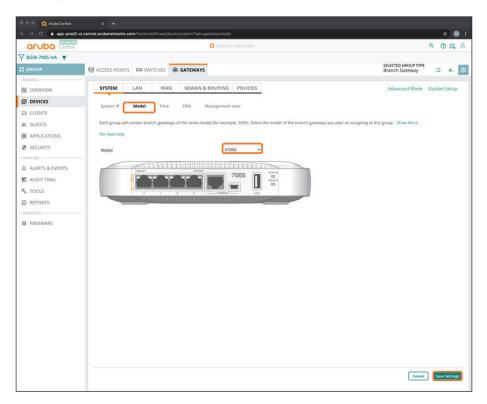
6.3 Select the Hardware Model of the Gateway Group

You can have only one gateway model per branch in the gateway group.

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

Step 2: In the Model drop-down list, select the hardware model for the branch gateway(s) in the group (example: **A7005**).

Step 3: Click Save Settings.



6.4 Select the Branch Gateway Group Time Zone

Use this procedure to set the NTP parameters and time zone to keep the branch gateway 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.

aruba Central		Q Search or ask Arub		9 0		8
7 BGW-7005-HA 🔻						
I GROUP	🗑 ACCESS POINTS 📼 S		SELECTED GROUP TYPE Branch Gateway	:=	di.	0
MANAGE						
BB OVERVIEW	SYSTEM LAN	WAN SDWAN & ROUTING POLICE	ES Advanced Mode	Guided	Setup	
DEVICES	System IP Model	Time DNS Management User				
E& CLIENTS						
SUESTS		e group will automatically obtain its time using the Netv	ork Time Protocol (NTP). You can either select one or more public NTP service providers (for	Show Mo	ire	
# APPLICATIONS	Per-field help					
SECURITY	Public NTP Servers		+			
ANALYZE	IPV4 ADDRESS/FQDN	BURST MODE				
AUDIT TRAIL						
TOOLS		No data to display				
REPORTS						
MAINTAIN						
FIRMWARE	Timezone	Choose a timezone				

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

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

Step 5: In the **Timezone** drop-down list, choose your timezone, and then click **Save Settings**.

V4 ADDRESS/FQDN	BURST MODE		
ool.ntp.org			
mezone	Choose a timezone		
ince office	choose a annezone		

6.5 Configure the DNS Servers for the Branch Gateway Group

You must specify the DNS server(s) that the gateway uses to communicate to Aruba Central.

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

🔍 🔍 🔍 💽 Aruba Central	x +				
← → ♂ ▲ app-prod2-ui.	central.arubanetworks.com/frontend/#/caas/basic/system?tab=dns			_	
oruba Central	Q Search or ask Aruba	۹	0		ል
∀ BGW-7005-HA ▼					
II GROUP	Maccess POINTS SWITCHES & GATEWAYS Branch Gateway		=	d.	۲
- MANAGE					
88 OVERVIEW	SYSTEM LAN WAN SDWAN & ROUTING POLICIES Advanced Mode	Gui	ded Se	etup	
	System IP Model Time DNS Management User				
LD CLIENTS					
a GUESTS	Each branch gateway in the group requires Domain Name System (DNS) configuration to be able to successfully resolve FQDNs and be able communicate with cloud services	Sho	w More	•	
APPLICATIONS	Per-field help				
SECURITY	Specify DNS servers Evann DNS configuration from ISP				
- ANALYZE					
ALERTS & EVENTS					
AUDIT TRAIL					
S TOOLS					
REPORTS					
- MAINTAIN					
FIRMWARE					

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.

Step 5: In the **Provider** drop-down list, select one of the providers listed or manually configure the desired DNS server(s).

Step 6: Click Save Settings.

ublic DNS Servers		$\left(+ \right)$
ROVIDER	IPV4 ADDRESS	
oogle 🔻	8.8.8,8.8.4.4	

6.6 Create a Management User Account for the Branch Gateways

In this procedure, you create a local management user account so you can use CLI to access the gateway.

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

Step 2: In the **Local Management User** table, click the plus (+) sign.

aruba Central				Q Search or ask Arul				٩	0	
BGW-7005-HA 🔻										
GROUP	ACCESS POINTS	SWITCHES	@ GATEWAYS				SELECTED GROUP T Branch Gateway			a d
ANAGE										
OVERVIEW	SYSTEM	LAN WAT	SDWAN &	ROUTING POLIC	IES		Advanced Mo	ide Gui	ded Se	tup
DEVICES	System IP	Model Time	DNS	Management User						
CLIENTS										
GUESTS	To be able to loca	illy or remotely acces	s the CLI console of	f the gateways in the gro	up, you must eith	er configure either a local manag	gement user or enable centralized	Sho	w More	
APPLICATIONS	Per-field help									
SECURITY		ion 🕥								
ALYZE	AAA authenticati	ion 🖉								
ALERTS & EVENTS	Local manage	ement users			+					
AUDIT TRAIL	NAME	ROLE		PASSWORD						
TOOLS										
REPORTS			No data to display							
AINTAIN										
FIRMWARE										

Step 3: In the Add Management User dialog box, implement the following settings:

- Name—admin
- Password—password
- Retype Password—password
- Role—Super user role

Step 4: Click Save.

Note You can add additional users with other roles as needed. These additional users are optional.



Step 5: Click Save Settings.

Add management user	
Name	admin
Password	
Retype Password	
Role	Super user role 🔻
	Cancel Save

6.7 Configure VLANs for the Branch Network Devices and Users

Use this procedure to define the VLANS for the branch network devices and users, as well as assign subnets at the device level.

Step 1: On the Gateways tab, in the LAN section, select VLANs.

Step 2: Select IP DHCP server.

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

In this example, we create a native VLAN 1 for management.	
--	--

🔍 🔍 🔍 💽 Aruba Central	× +										
← → C (à app-prod2-ui,	central.arubanetworks.co	m /frontend/#/caas/bas	sic/lan?tab=virtualLans						\$		
aruba Central			Q Search					٩	0:	. 6	8
▼ BGW-7005-HA ▼											
C GROUP	@ ACCESS POINTS	SWITCHES	SATEWAYS				SELECTED GROUP TYPE Branch Gateway		= a		۲
- MANAGE											
88 OVERVIEW	SYSTEM	LAN WAN	SDWAN & ROUTING	POLICIES			Advanced Mode	Guid	ed Set	up	
@ DEVICES	VLANS LA	IN Ports									
CLIENTS	The state of the s	or Ports									
SUESTS	Each branch gate	way will require one or	more LAN VLANs and IP inter	faces to support	infrastructure and client of	devices in your branches. Each	VLAN will either be statically or	Show	More		
# APPLICATIONS	Per-field help										
	IP DHCP server										
- ANALYZE		9									
ALERTS & EVENTS	VLANs						+				
AUDIT TRAIL	4087	NAME SystemIP_4	STATIC		DYNAMIC DHCP POOL	DHCP RELAY Disabled					
A TOOLS		Syntema				U.L.U.L.					
REPORTS											
- MAINTAIN											
FIRMWARE											
										_	
							Cancel	1	ave Sett	ings	

Step 4: In the New VLAN dialog box, implement the following settings:

- Name—Management
- VLAN ID-1
- IP addressing mode—Static.

Step 5: Click Save.

Step 6: Repeat Step 3 - Step 5 for each additional user VLAN. For example, an Employee VLAN.

New VLAN	
Name	Management
VLAN ID	1
IP addressing mode	Static 🔻
IPV4 ADDRESS (Optional)	
Netmask (Optional)	
Act as DHCP server	
Enable DHCP relay	
	Cancel

Step 7: Click Save Settings.

VLANs					+
VLAN ID	NAME	STATIC	DYNAMIC DHCP POOL	DHCP RELAY	
4087	SystemIP_4087	· *	8	Disabled	
1	Management	×	¥.	Disabled	
20	Employee			Disabled	

6.8 Configure the LAN Ports for the Branch Gateway

Assign the LAN ports that the downstream switches use and permit user and management VLANs.

Step 1: On the Gateways tab, in the LAN section, select LAN Ports.

Step 2: In the **LAN ports/port channel** table, click the plus (+) sign.

Central				Q Search or ask /					9 0	0	1
GW-7005-HA 🔻	O ACCESS POINTS	SWITCHES	@ GATEWAYS	1				SELECTED GROUP TYPE Branch Gateway	:=	а.	
OVERVIEW	SYSTEM	LAN WA	N SDWAN 8	ROUTING PO	LICIES			Advanced Mode	Guideo	l Setu	up
DEVICES	VLANS	AN Ports									
CLIENTS	YDANS D	an Ports									
GUESTS	LAN VLANS can I	be assigned to one o	r more ports on you	or gateways in the gro	up. The gateway por	rts that are available fo	or assignment in this step	will be dependent on the	Show N	lore	
APPLICATIONS	Per-field help										
SECURITY	LAN ports/p	ort channel					+				
LYZE	NAME	PORT	MODE	ACCESS VLAN	NATIVE VLAN	ALLOWED VLANS	U				
LERTS & EVENTS											
UDIT TRAIL				No data to display							
OOLS EPORTS											
FIRMWARE											

Step 3: In the New LAN port/port channel dialog box, in the Name box, enter a name for the new port (example: LAN).

Step 4: In the Port drop-down list, select a physical port on the gateway (example: GE-0/0/0).

Step 5: In the VLAN mode drop-down list, select **Trunk**.

Step 6: In the **Native VLAN** drop-down box, select the management VLAN you created in Procedure 6.7 (example: **1 : Management**).

Step 7: In the **Allowed VLAN** box, enter the VLAN IDs for the VLANs allowed towards the LAN.

Step 8: Repeat Step 2 - Step 7 for each additional LAN port that you need to configure.

ew LAN port / portchannel	
Name	LAN
Port	GE-0/0/0
VLAN mode (Optional)	Trunk
Native VLAN (Optional)	1 : Management 🔻
Allowed VLAN (Optional)	1,20
	Cancel

Step 9: Click Save, and then click Save Settings.

6.9 Configure WAN Health Checks

Step 1: On the Gateways tab, in the WAN section, select **Health Checks**.

Aruba Central				
	central.arubanetworks.com/frontend/#/caas/basic/wan?tab=healthCheck			8 :
	Search or ask Aruba	٩	0 #	• A
▼ BGW-7005-HA ▼		SELECTED GROUP TYPE		
🗱 GROUP	TO ACCESS POINTS SWITCHES A GATEWAYS	Branch Gateway	i= 6.	۲
- MANAGE	SYSTEM LAN WAN SDWAN & ROUTING POLICIES	Advanced Mode Gu		
88 OVERVIEW	STSTEM LAW WAN SUWAN & ROUTING POLICIES	Advanced Mode Gu	ided Sett	qu
DEVICES	Health Checks Load Balancing WAN Details			
CLIENTS				
🚉 GUESTS	IP health checks are used by the gateways to determine WAN path availability and measure WAN path performance. Th	he responses to these health check probes are used by Sho	ow More	
APPLICATIONS	Per-field help			
SECURITY	Enable health checks			
ANALYZE				
ALERTS & EVENTS	Health check destination			
AUDIT TRAIL	We recommended you to select health check destination as Aruba cloud.			
S TOOLS	Health check probe mode Ping -			
REPORTS				
MAINTAIN				
FIRMWARE				

Step 2: In the Health check destination drop-down list, select **Aruba cloud**.



Health Checks	Load Balancing	WAN Detai	ls	
IP health checks are Per-field help	used by the gateways	s to determine W	/AN path availab	ility and measure
Enable health checl	<5			
Health check destin	ation	Aruba cloud	•	
Health check probe	mode	Ping	•	
			Cancel	Save Settings

6.10 Configure the WAN Load Balancing Algorithm

Step 1: On the Gateways tab, in the WAN section, select Load Balancing.

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

Step 3: Click Save Settings.

aruba Central	Q Search or ask Aruba	۹	0 #	8
▼ BGW-7005-HA ▼				
🛱 GROUP	🗑 ACCESS POINTS 📼 SWITCHES 🙊 GATEWAYS SELECTED GROUP TYPE Branch Gateway		- iii	6
- MANAGE				
88 OVERVIEW	SYSTEM LAN WAN SDWAN & ROUTING POLICIES Advanced Mode	Guide	d Setu	p
@ DEVICES	Health Checks Load Balancing WAN Details			
E& CLIENTS				
2. GUESTS	Branch gateways support three different load-balancing algorithms to influence how outgoing traffic is forwarded. A load-balancing action may be performed for outgoing	Show	More	
I APPLICATIONS	Per-field help			
SECURITY	Load balancing mode O Round robin			
ANALYZE	- O Session count			
ALERTS & EVENTS	Uplink utilization			
AUDIT TRAIL				
Nools				
REPORTS				
- MAINTAIN				
FIRMWARE				

6.11 Configure the WAN Service Providers

In this procedure, you enable high availability (HA) and configure the WAN service providers. We use a dual gateway with internet and MPLS WAN for HA.

Step 1: On the Gateways tab, in the WAN section, select WAN Details.

Step 2: Click the Enable HA Deployment slider.

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

🔍 🔍 🔍 Aruba Central	x +		
← → C a app-prod2-ul.	central.arubanetworks.com/frontend/#/caas/basic/wan?tab=wanPorts	*	8
aruba Central	Q Search or ask Aruba	۹ 🕲 🗄	. 8
▼ BGW-7005-HA ▼			
🛱 GROUP	ACCESS POINTS SWITCHES & GATEWAYS	:= d.	
- MANAGE			
88 OVERVIEW	SYSTEM LAN WAN SDWAN & ROUTING POLICIES Advanced Mode	Guided Setu	IP.
DEVICES	Health Checks Load Balancing WAN Details		
LD CLIENTS			
& GUESTS	Each branch gateway connects to one or more Internet, MPLS and cellular based WAN services using WAN ports. A gateway can support a maximum of four Wired WAN links	Show More	
APPLICATIONS	Per-field help		
SECURITY			
- ANALYZE	Enable HA deployment		
A ALERTS & EVENTS	WAN Uplinks / Ports +		
AUDIT TRAIL	UPLINK TYPE VLAN ID ADDRESS SPEED NAT BACKUP		
S TOOLS			
REPORTS	No data to display		
- MAINTAIN			
FIRMWARE			
			_
	Cancel	Save Setti	ngs
			-

Step 4: In the Add/Edit WAN port dialog box, implement the following settings:

• Uplink—Turbo

Note If you choose an MPLS WAN, the uplink name must match the name used at the VPNCs to enable automated tunnel orchestration between gateways.

- WAN type—MPLS
- WAN speed—500
- Source NAT—Unselect this option
- Secure with ACL—Unselect this option

Step 5: Click Save.

Step 6: Repeat Step 3 - Step 5 for each WAN provider.

dd/Edit wan port		
WAN CONNECTION		
Uplink	Turbo	
WAN type	MPLS	-
WAN speed	500	Mbp
Source NAT		
Use as backup		
IP addressing method	DHCP	*
Only four uplinks v can be created	with DHCP IP addressin	g method
WAN PORT ASSIGNM Create port attributes onl of WAN port must be don	ly for HA deployments.	Assignm
Port (Optional)		•
Secure with ACL		
	Cancel	Save
dd/Edit was nort	Cancel	Savi
ldd/Edit wan port	Cancel	Sav
WAN CONNECTION) Sav
	ISP-1	Sav
WAN CONNECTION) Sav
WAN CONNECTION	ISP-1	
WAN CONNECTION Uplink WAN type	ISP-1 Internet	
WAN CONNECTION Uplink WAN type WAN speed	ISP-1 Internet 200	
WAN CONNECTION Uplink WAN type WAN speed Source NAT	ISP-1 Internet 200	
WAN CONNECTION Uplink WAN type WAN speed Source NAT Use as backup IP addressing method	ISP-1 Internet 200	Mbp
WAN CONNECTION Uplink WAN type WAN speed Source NAT Use as backup IP addressing method	ISP-1 Internet 200 INCP INCP With DHCP IP addressin	Mbp g method

These screenshots illustrate a dual gateway with an internet and an MPLS WAN provider.

6.12 Specify the SD-WAN Data Center Preferences

Use this procedure to assign data center preferences for tunnel orchestration toward the VPN concentrators.

Cancel

Step 1: On the Gateways tab, in the SDWAN & Routing section, select DC Preferences.

Secure with ACL

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

Central		Q Search or				9 0	14	8
SW-7005-HA 🔻	Ø ACCESS POINTS ■ SWI				SELECTED GROUP TYPE		4.	
wer	O ACCESS POINTS C SWI	CHES SHE WATE			Branch Gateway			8
OVERVIEW	SYSTEM LAN	WAN SDWAN & ROUTING	POLICIES		Advanced Mode	Guided	Setup	
DEVICES	DC Preference Static	Routing Overlay Routing						
CLIENTS	DC Preference Statio	Routing Overlay Routing						
GUESTS	If your deployment includes	/PN Concentrators (VPNCs) deployed in one	or more hub sites, your branch ga	teways can be configured to create a h	ub-n-spoke IPsec based VPN	Show Me	ore	
APPLICATIONS	Per-field help							
ECURITY	Overlay Orchestrator P	eering : Disabled						
Y2E								
ALERTS & EVENTS				-				
AUDIT TRAIL	DC Preference			+				
DOLS	HUB GROUP	PRIMARY VPNC	SECONDARY VPNC	0.0				
EPORTS								
ITAIN		No data to display						
FIRMWARE								

Step 3: In the **Hub Group** drop-down list, select a VPNC group to assign the preferred data center (example: **VPNC-7210**).

Step 4: In the **Primary VPNC** drop-down list, select the primary VPNC.

Step 5: In the **Secondary VPNC** drop-down list, select the secondary VPNC.

Step 6: Repeat Step 2 - Step 5 if a secondary data center is used.

Step 7: Click Save Settings.

	CRouting Overlay Routing	red in one or more hub sites, your branch gate	units can be configured to
r-field help	ven concentrators (vencs) deploj	red in one of more nub sites, your branch gate	ways can be conligured to
Overlay Orchestrator	Peering : Disabled		
 Overlay orchestration 	will be enabled once DC preference	e is configured	
DC Preference			+
HUB GROUP	PRIMARY VPNC	SECONDARY VPNC	
VPNC-7210	DC2-7210-1 (00:1a:1 -	DC2-7210-2 (00:1a:1 -	

Aruba Central automatically enables overlay orchestrator peering after you click Save Settings.

DC Preference			+
HUB GROUP	PRIMARY VPNC	SECONDARY VPNC	
WPNC-7210	DC2-7210-1 [00:1a:1e:05:01:a0]	DC2-7210-2 [00:1a:1e:05:01:28]	
WPNC-7024	DC1-7024-1 [00:0b:86:bb:bb:a7]	DC1-7024-2 [00:0b:86:bb:ff:a7]	

6.13 Configure the SD-WAN Overlay Routing

In this procedure, you redistribute the branch subnets in the VPN overlay to enable the dynamic routing functionality at the headend site.

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

	x 🛚 🕅
Q Search or ask	cAruba 🔍 🕲 🛄 🗍
	SELECTED GROUP TYPE
ACCESS POINTS SWITCHES GATEWAYS	Branch Gateway 🗉 🔒 🛞
	OLICIES Advanced Mode Guided Setup
STSTEM DATE WARE SDIVER & ROUTING P	Advanced Mode Guided Setup
DC Preference Static Routing Overlay Routing	
Redistribute connected vlans Select VLANs	
Redistribute static route	
	ol central and/aneleokit economice 2/least/basic/person/og/tablesesid/person/og/tablese Person/og/tablesesid/person/og/tablesesid/person/og/tablesesid/person/og/tablesesid/person/og/tablesesid/person/og/tablesesid/person/og/tablesesid/person/og/tablesesid/person/og/tablesesid/person/og/tablesesid/person/og/tablesesid/perso

Step 2: In the **Redistribute connected vlans** box, select all of the user VLANs and system IP VLAN for overlay redistribution.

Step 3: Click Save Settings.

DC Preference	Static Routing	Overlay Routing
Redistribute connect	ed vlans	Vian 1 X Vian 20 X Vian 4087 X search
Redistribute static ro	oute	
		Cancel Save Settings

6.14 Configure Role-Based Policies for the Branch Gateways

Use this procedure to define the policies for the user VLANs to allow network access.

Step 1: On the Gateways tab, in the Policies section, select **Roles**.

Step 2: In the **Role assignment** table, click the plus (+) sign.

aruba Central			Q Sea	rch or ask Aruba				٩	0 :	۵.
▼ BGW-7005-HA ▼	G ACCESS POINTS 🗖 SWITCHE						SELECTED GROUP TYPE Branch Gateway	1		
OVERVIEW DEVICES CLIENTS GUESTS GUESTS		DPS QOS	AN & ROUTII		role. Once the role h	as been assigned, it can be use	Advanced Mode			νp
O SECURITY ALTER ALTER	Parts + united - united -	Role assigned assigne	nament NAME	AFERICATON	101					

Step 3: In the Role assignment dialog box, implement the following settings:

- VLAN ID—Management (1)
- Initial Role—authenticated
- Authentication—Disable this option

Step 4: Click Save.

Role assignment		
VLAN ID	Management (1) 🔻	
Initial Role	authenticated	
Authentication		
		Cancel

Step 5: Repeat Step 2 - Step 4 for all of the user VLANs.

ROLE ASS	IGNMENT			+
VLAN	NAME	AUTHENTICATION	ROLE	
1	Management	Disabled	authenticated	
20	Employee	Disabled	authenticated	

Procedures

Configuring a Branch Gateway Device—Two Branch Gateways per Branch

- 7.1 Assign the Branch Gateway Devices to a Group
- 7.2 Initiate the Primary Branch Gateway Configuration
- 7.3 Assign a Hostname to the Primary Branch Gateway Device
- 7.4 Assign IP Addresses to the VLAN
- 7.5 Set the DHCP Scope
- 7.6 Initiate the Secondary Branch Gateway Configuration
- 7.7 Assign a Hostname to the Secondary Branch Gateway
- 7.8 Assign IP Addresses to the VLANs
- 7.9 Set the DHCP Scope
- 7.10 Specify the WAN Ports
- 7.11 Assign a Default Route for MPLS
- 7.12 Configure the LAN Redundancy

7.1 Assign the Branch Gateway Devices to a Group

Step 1: On the Aruba Central Account Home page, select Device Inventory.

Step 2: In the View Devices table, select two branch gateways, and then click **Assign Group**.

	UNT HOME								
DEVICE I	NVENTO	Y							
View the devices in			devices here.						
VIEW DEVICES	5								
♥ SERIAL NUM_	Y MAC ADDRESS	Y TYPE	IP ADDRESS	NAME	WODEL	▼ PART NUMB	GROUP	♥ SUBSCF ≡	
• CP0044588	20:4C:03:2F:F8:C4	controller(G			7005-US	JW634A		0	
CP0044594	20:4C:03:2F:F4:2C	controller(G	=	14 C	7005-US	JW634A	-	0	
CP0044595	20:4C:03:2F:F7:DC	controller(G	-	-	7005-US	JW634A	-	in the	
• CP0046727	20:4C:03:39:5D:0C	controller(G			7005-USF1	JW636A		0	
• CP0046739	20:40:03:39:51:70	controller(G			7005-USF1	JW636A		0	
• CP0046977	20:40:03:39:5F:94	controller(G			7005-USF1	JW636A		0	
• CP0047911	20:40:03:39:85:24	controller(G	10.8.255.211	R\$15-7005-2	7005-US	JW634A	BGW-Du	0	
• CP0047912	20:40:03:39:73:10	controller(G	10.8.255.4	RS12-7005	7005-US	JW634A	BGW-70	0	
• CP0047915	20:4C:03:39:7B:EC	controller(G			7005-US	JW634A		0	
• CP0048213	20:40:03:39:76:94	controller(G			7005-US	JW634A			
• CT0338957	94:84:0F:C6:58:18	iap			IAP-225-US	IAP-225-US		0	
• CV0016870	00:1A:1E:05:01:A0	controller(V	10.4.255.3	DC2-7210-1	7210-US	JW744A	VPNC-72	0	
• CV0016872	00:1A:1E:05:01:28	controller(V	10.4.255.4	DC2-7210-2	7210-US	JW744A	VPNC-72	0	
• CV0016892	00:1A:1E:05:0E:70	controller(G			7210-US	JW744A		0	
• CZ0000091	00:08:86:88:88:	controller(V	10.2.255.2	DC1-7024-1	7024-US	7024-US	VPNC-70	0	
• CZ0001699	00:08:86:88:FF:A7	controller(V	10.2.255.3	DC1-7024-2	7024-US	7024-US	VPNC-70	0	
SG70GYW01J	EC:EB:88:17:F3:00	switch	10.8.0.3	RS1-3810-1	3810	JL073A	SW-381	0	
SG7BGYW0C8	EC:EB:88:F5:1C:00	switch	10.8.12.3	RS4-3810-1	3810	JL073A	SW-BRA	0	
SG82jQP23W	04:09:73:85:D3:40	switch			2930M	JL323A		0	

Step 3: In the Assign a Group to the Selected Devices dialog box, select the Branch Gateway group you created in Procedure 6.1 (example: **BGW-7005-HA**).

7 group name	
TG 2930F-Single	
TG 2930M-Stack	
TG 3810M-Single	
BGW-7005	
BGW-7005-HA	
BGW-Dual-RS15	
default	
SW-3810-GRP	
SW-BRANCH-GRP	
VPNC-7024	
VPNC-7210	

Step 4: Click Assign device(s), and then click OK.



7.2 Initiate the Primary Branch Gateway Configuration

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

Step 2: In the filter drop-down list, select the branch gateway group you assigned the devices to in Procedure 7.1 (example: **BGW-7005-HA**).

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

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

🔍 🔍 🔍 💽 Aruba Central							
← → C · app-prod2-u	i.central.arubanetworks.com/frontend/#/GATEWAY/						
		Q Search or ask	Aruba			2 0	щ <u>А</u>
▼ BGW-7005-HA ▼							
11 GROUP	🗑 ACCESS POINTS 📼 SWITCHES 👰	GATEWAYS					ı. ©
- MANAGE							
89 OVERVIEW	GATEWAYS . UP O DOWN						
	2 0 2						
LD CLIENTS	GATEWAYS						± ⊖
A GUESTS	P DEVICE NAME IF MOD	EL	FIRMWARE VERSION	UPTIME	IP ADDRESS		
	o jW634A-20:4C:03:2F:F4:2C JW63	4A.	Unknown				
# APPLICATIONS	o jW634A-20:4C:03:2F:F7:DC JW63-	4A	Unknown				
SECURITY SECURITY							
- ANALYZE							
ALERTS & EVENTS							
AUDIT TRAIL							
S TOOLS							
REPORTS							
- MAINTAIN							
G FIRMWARE							
OF PIRMYDARE							
Í.							
Í.							

For educational purposes, the next step exits the guided setup.

Step 5: In the Guided Setup dialog box, click Cancel, and then click Exit.

orubo Central	Guided Setup for Branch Gateway Device
1 System	This wizard will guide you through the essential steps to configure the branch gateways in the Device .
2 LAN	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	After completing this initial setup, you can change the settings at any time.
4 SDWAN & Routing	
5 Redundancy	Cancel Begin



7.3 Assign a Hostname to the Primary Branch Gateway Device

Step 1: On the Gateway tab, in the System section, select **Hostname**.

Step 2: In the Hostname box, enter a name (example: RS3-7005-1), and then click Save Settings.

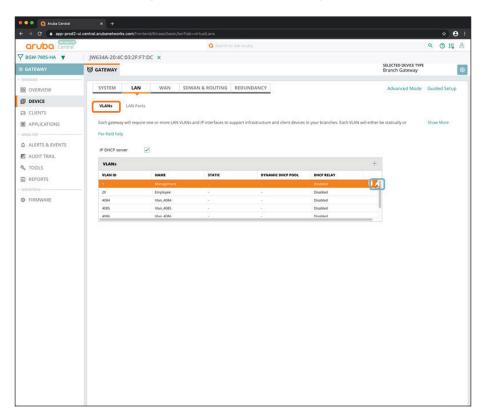
🔍 🔍 🧕 🔯 Aruba Central	× +				
← → C ▲ app-prod2	-ui.central.arubanetworks.com/frontend/#/caas/basic/system?tab=hostname			*	e :
oruba Central	Q Searc			۹ 🕲 🗉	: 8
∀ BGW-7005-НА ▼	JW634A-20:4C:03:2F:F7:DC ×				
@ GATEWAY	G GATEWAY		SELECTED DEVICE TYPE Branch Gateway		۲
- MANAGE					
88 OVERVIEW	SYSTEM LAN WAN SDWAN & ROUTING	3 REDUNDANCY	Advanced Mode	Guided Setu	up
DEVICE	System IP Hostname				
CLIENTS					
APPLICATIONS	Hostname RS3-7005-1				
ANALYZE					
TOOLS					
REPORTS					
MAINTAIN					
G FIRMWARE					
			Cancel	Save Setti	ines

7.4 Assign IP Addresses to the VLAN

Use this procedure to assign LAN VLAN IP addresses and set the DHCP scope for the management and user LANs.

Step 1: On the Gateway tab, in the LAN section, select VLANs.

Step 2: In the VLANs table, select Management, and then click the pencil icon.



Step 3: In the VLAN - Management dialog box, implement the following settings:

- IPV4 Address—10.8.8.2
- Act as DHCP server—Enable this option
- DNS server type—Public DNS Server
- DNS Service Provider—Google

Name	Management
VLAN ID	1
P addressing mode	Static 💌
PV4 ADDRESS	10.8.8.2
Netmask	255.255.255.0
Act as DHCP server	
Network	10.8.8.0
Netmask	255.255.255.0
Default router (Optional)	10.8.8.1
Domain name (Optional)	example.local
DNS server type	Public DNS Servir 💌
DNS Service Provider	Google 🔻
Enable DHCP relay	

Step 4: Click Save.

Step 5: Repeat Step 2 - Step 4 for any additional VLANs (example: Employee).

Step 6: Click Save Settings.

VLANs					+
VLAN ID	NAME	STATIC	DYNAMIC DHCP POOL	DHCP RELAY	
1	Management	10.8.8.2 / 24		Disabled	1
20	Employee	10.8.9.2 / 24	2	Disabled	
4084	Vlan_4084	12.5	5 1	Disabled	
4085	Vlan_4085			Disabled	
4086	Vlan 4086			Disabled	

7.5 Set the DHCP Scope

Step 1: On the Gateway tab, in the LAN section, select **VLANs**.

Step 2: Click Advanced Mode.

aruba Centra	D		Q Search or ask A	ruba			۹ 🔿 📖	
BGW-7005-HA 🔻	JW634A-20:4C:03:2F	F7:DC ×						
GATEWAY	G GATEWAY					SELECTED DEVICE T Branch Gateway	YPE	I
MANAGE								
8 OVERVIEW	SYSTEM LA	WAN SDV	VAN & ROUTING RED	UNDANCY		Advanced Moo	de Guided Setu	p
DEVICE	VLANS LAN P	vits						
b CLIENTS								
APPLICATIONS	Each gateway will req	aire one or more LAN VLANs	and IP interfaces to support	infrastructure and client devices	in your branches. Each VL	AN will either be statically or	Show More	
NALYZE	Per-field help							
ALERTS & EVENTS								
AUDIT TRAIL	IP DHCP server							
TOOLS	VLANS					+		
REPORTS	VLAN ID	NAME	STATIC	DYNAMIC DHCP POOL	DHCP RELAY			
AINTAIN	1	Management	10.8.8.2/24		Disabled			
FIRMWARE	20 4084	Employee Vian_4084	10.8.9.2724		Disabled			
PIRMITIPAL	4085	Vian_4085			Disabled			
	4386	Vian 4086			Disabled			

Step 3: Select the **Interface** tab, and then select **DHCP**.

Step 4: In the **IP excluded address range** table, click the plus (+) sign.

IP DHCP server:	~		
IP DHCP server.			
Pool configuration			
IP VERSION	∀NAME	VNETWORK	VDEFAULT ROUTER
IPv4	vlan_1	10.8.8.0	10.8.8.1
IPv4	vlan_20	10.8.9.0	10.8.9.1
IP excluded address	range		
IP EXCLUDED ADDRESS	L.		

Step 5: Enter the IP address ranges that you want to exclude from the DHCP scopes.

IP excluded address range	
IP EXCLUDED ADDRESS	
10.8.8.2 10.8.8.9	
10.8.9.2 10.8.9.9	

Step 6: Click Save Settings to return to Basic Mode.

7.6 Initiate the Secondary Branch Gateway Configuration

Step 1: In the filter drop-down list, select the branch gateway group you assigned the devices to in Procedure 7.1 (example **BGW-7005-HA**).

Step 2: In the left navigation pane, in the Manage section, select **Devices**, and then select the **Gateways** tab.

Step 3: In the **Gateways** table, select the device you intend to configure as the secondary branch gateway.

Control and	🔍 🔍 🔍 💽 Aruba Central								
V BOX YODSHA Y CACESS FONTS SWITCHS CACESS FONTS SWITCHS CATEWAYS CATEWAYS<	← → C 🔒 app-prod2-ui	.central.arubanetworks.com/front						*	
V BOX YODSHA Y CACESS FONTS SWITCHS CACESS FONTS SWITCHS CATEWAYS CATEWAYS<			0	Search or ask Aruba			۹ (3 II	8
It accust VEX.CESS POINTS SWITCHS A CERTARY It accust It accust </th <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>									
CATTINATS Operation Cattorian Constraint Cattorian <			A CATRUNE						~
Bit Oversite/// CATEWAYS L/B CODOTS CLEARIS CLEARIS <thclearis< th=""> CLEARIS C</thclearis<>		G ACCESS FORMES	initicities in GATEMATS						
2 2		GATEWAYS	0.0000						
□ CUENTS CATINANS PADOELS PADOELS <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>									
X CUISTS V DOILS FRAMAR VERIOR UPME PADDESS III APFLICATIONS IMDAMA CUERDINAL MIDIAA Uthowini Implement									~
MCUSIS DMMANDAMENDIATION MMSAAA Latione © MANDAMENDIATION MMSAAA Latione Image: Contemportant	LD CLIENTS							ٹ	0
Mill APPLICATIONIS 9 (MISUA 2014C0319772C) MISSUA Unitation © SECURIT -	AL GUESTS		120 P00 P00 P00		UPTIME	IP ADDRESS			
SECURITY ANALIZIS ALTERTS & EVENTS ALTERTS & EVENTS ALTERTS ALTERTS ALTERTS ALTERTS ALT	# APPLICATIONS								
ALERTS & EVENTS ALERTS & EVENTS ALERTS AUTOLS DEPORTS EXAMPLEM	SECURITY								
ALERTS & EVENTS ALERTS & EVENTS ALERTS AUTOLS DEPORTS EXAMPLEM									
AUDIT TRAIL A TOOLS REPORTS AUDITION									
 ▲ TOOLS ■ REPORTS = HANYTERI 									
© REPORTS									
- MANYTAIN	S TOOLS								
	REPORTS								
© FIRMWARE	- MAINTAIN								
	FIRMWARE								

For educational purposes, the next step exits the guided setup.

Step 4: In the Guided Setup dialog box, click **Cancel**, and then click **Exit**.

aruba Central	Guided Setup for Branch Gateway Device
1 System	This wizard will guide you through the essential steps to configure the branch gateways in the Device .
2 LAN	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	After completing this initial setup, you can change the settings at any time.
4 SDWAN & Routing	
5 Redundancy	

EXIT G	UIDED SETUP
A	Guided Setup will be exited and changes will be lost. You can re-enter the Guided Setup at any time to complete it.
	RESUME

7.7 Assign a Hostname to the Secondary Branch Gateway

Step 1: On the Gateway tab, in the System section, select **Hostname**.

Step 2: In the Hostname box, enter a name (example: RS3-7005-2), and then click Save Settings.

aruba Centra	Search or ask Aruba	۹ 🔿 🎬
BGW-7005-HA ▼	JW634A-20:4C:03:2F:F4:2C ×	
GATEWAY	G GATEWAY	SELECTED DEVICE TYPE Branch Gateway
ANAGE		
OVERVIEW	SYSTEM LAN WAN SDWAN & ROUTING REDUNDANCY	Advanced Mode Guided Setup
DEVICE	System IP Hostname	
CLIENTS		
APPLICATIONS	Hostname RS3-7005-2	
ALYZE		
ALERTS & EVENTS		
AUDIT TRAIL		
TOOLS		
REPORTS		
NTAIN		
FIRMWARE		

7.8 Assign IP Addresses to the VLANs

Step 1: On the Gateway tab, in the LAN section, select VLANs.

Step 2: In the VLANs table, select **Management**, and then click the pencil icon.

Central			Q Search or ask				9 (ש 📫
GW-7005-HA 🔻	JW634A-20:4C:03:2F	:F4:2C ×						
	GATEWAY					SELECTED DEVICE TYPE Branch Gateway		
CAGE								
OVERVIEW	SYSTEM LA	N WAN SD	WAN & ROUTING REE	UNDANCY		Advanced Mode	Guideo	Setup
DEVICE	VLANS LAN P							
UENTS	VLANS DAN P	orts						
APPLICATIONS	Each gateway will rec	uire one or more LAN VLAN	is and IP interfaces to suppor	t infrastructure and client devices	in your branches. Each VLAN will	either be statically or	Show N	lore
	Per-field help							
LERTS & EVENTS								
AUDIT TRAIL	IP DHCP server							
	VLANS					+		
OOLS	VLAN ID	NAME	STATIC	DYNAMIC DHCP FOOL	DHCP RELAY			
EPORTS	1	Management			Disabled			
ITAIN	20	Employee		1	Disabled			
IRMWARE	4084	Vlan_4084			Disabled			
						-1		
					The second se			
	4085 4196	Vian_4085 Vian_4086			Disabled Disabled			

Step 3: In the VLAN - Management dialog box, implement the following settings:

- IPV4 Address—10.8.8.3
- Act as DHCP server—Enable this option
- DNS server type—Public DNS Server
- DNS Service Provider—Google

Name	Management
VLAN ID	1
IP addressing mode	Static 💌
IPV4 ADDRESS	10.8.8.3
Netmask	255.255.255.0
Act as DHCP server	
Network	10.8.8.0
Netmask	255.255.255.0
Default router (Optional)	10.8.8.1
Domain name (Optional)	example.local
DNS server type	Public DNS Servix 💌
DNS Service Provider	Google
Enable DHCP relay	
Enable DHCP relay	

Step 4: Click Save.

Step 5: Repeat Step 2 - Step 4 for each additional VLAN (example: Employee).

Step 6: Click Save Settings.

VLANS					+
VLAN ID	NAME	STATIC	DYNAMIC DHCP POOL	DHCP RELAY	
1	Management	10.8.8.3 / 24		Disabled	
20	Employee	10.8.9.3 / 24	101 101	Disabled	
4084	Vlan_4084		-11) 	Disabled	
4085	Vlan_4085	*	10	Disabled	
4086	Vlan 4086			Disabled	

7.9 Set the DHCP Scope

Step 1: On the Gateway tab, in the LAN section, select VLANs.

Step 2: Click Advanced Mode.

aruba Central				Q Search	or ask Aruba			۹ 🔿 📖	8
BGW-7005-HA	JW634A-20:40	-03-2F-F4-20	×	-					
GATEWAY	G GATEWAY						SELECTED DEVICE TYPE Branch Gateway		0
ANAGE	Guarcia						bianch Gateway		-
OVERVIEW	SYSTEM	LAN	WAN	SDWAN & ROUTING	REDUNDANCY		Advanced Mode	Guided Setup	
DEVICE									
CLIENTS	VLANs	LAN Ports							
APPLICATIONS	Each gateway	Each gateway will require one or more LAN VLANs and IP interfaces to support infrastructure and client devices in your branches. Each VLAN will either be statically or Sho							
ALYZE	Per-field help								
ALERTS & EVENTS									
AUDIT TRAIL	IP DHCP ser	ver 🗸							
TOOLS	VLANS						+		
REPORTS	VLAN ID		NAME	STATIC	DYNAMIC DHCP POO	L DHCP RELAY			
INTAIN	1		Management	10.8.8.3 / 24		Disabled			
FIRMWARE	20		Employee Vian,4084	10.8.9.3724		Disabled			
	4085		Van_4085			Disabled			
			Vian 4086			Disabled			
	4086		and all the						
	4096								
	4095								
	4095								

Step 3: Select the **Interface** tab, and then select **DHCP**.

Step 4: In the **IP excluded address range** table, click the plus (+) sign.

CP Server IP DHCP server:	~		
Pool configuration	1		
IP VERSION	VNAME	VNETWORK	VDEFAULT ROUTER
IPv4	vlan_1	10.8.8.0	10.8.8.1
IPv4	vlan_20	10.8.9.0	10.8.9.1
IP excluded addres			

Step 5: Enter the IP address ranges that you want to exclude from the DHCP scopes.

IP excluded address range								
IP EXCLUDED ADDRE	ss							
10.8.8.2 10.8.8.9								
10.8.9.2 10.8.9.9								

Step 6: Click Save Settings to return to Basic Mode.

7.10 Specify the WAN Ports

Step 1: On the Gateways tab, in the WAN section, select WAN Details.

aruba Central					Q Search o						9 1	3 11
3GW-7005-HA 🔻	JW634A-20:40	:03:2F:F4:20	×									
ATEWAY	GATEWAY									SELECTED DEVICE TYPE Branch Gateway		
NAGE	-											
OVERVIEW	SYSTEM	LAN	WAN	SDWAN	& ROUTING	REDUNDANCY				Advanced Mode	Guide	d Setup
DEVICE	Health Chec	ks Load	Balancing	WAN DO	tails							
CLIENTS	- A CONTRACTOR		and an									
APPLICATIONS	Each branch (gateway conne	cts to one or	more interne	t, MPLS and cellu	ilar based WAN servi	ces using WA	N ports. A gat	eway can support	a maximum of four Wired WAN links	Show N	Nore
ULYZE	-	a set a better a s	3									
ALERTS & EVENTS	Enable High	Availability dep	noyment									
AUDIT TRAIL	WAN UPL	INKS / PORTS							+			
TOOLS	UPLINK	TYPE	PORT	VLAN ID	ADDRESS	SPEED	NAT	BACKUP				
REPORTS	turbo_mpls isp-2_inet	MPLS INET	GE-un	4084	DHCP	500 Mbps 200 Mbps	Disabled Enabled	Disabled				
NTAIN	isp-1_inet	INET	GE-un_	4085	DHCP	200 Mbps 200 Mbps	Enabled	Disabled				
FIRMWARE												

Step 2: Click **Enable High Availability deployment** to allow the workflow to configure both gateways in the HA pair.

Step 3: In the Peer gateway drop-down list, select the primary gateway device (example: RS3-7005-1).

Step 4: In the **HA VLAN** drop-down list, select the **Management** VLAN ID. The Local VLAN IP/netmask and the Peer VLAN IP/netmask addresses should auto-populate.

nable High Availability deployment		
Local gateway	RS3-7005-2 (20	:4c:03:2f:f4:2c)
Peer gateway	RS3-7005-1 (20):4 🗸
Site ID (Optional)	Type to searc	h or add
is installed at the same site being redistributed into ove HA will not work.		
HA VLAN	1	*
Local VLAN IP/netmask	10.8.8.3	255.255.255.0

Step 5: In the **WAN Uplinks/Ports** table, select one of the physical ports you added in Procedure 6.11 (examples: **Turbo** or **ISP-1**) to assign to the local WAN uplink for the primary gateway.

Step 6: In the Add/Edit wan port dialog box, implement the following settings:

- Port—GE-0/0/2
- IP addressing method—Static or DHCP
- Secure with ACL—Select this option only for Internet WAN

Add/Edit wan port	
Gateway	Local Peer
WAN CONNECTION	
Uplink	turbo_mpls
WAN type	MPLS 💌
WAN speed	500 Mbps
Source NAT	
Use as backup	
IP addressing method	Static 🔹
Static IPv4 addresses for be either pre-provision using Bulk configuration device.	or each branch gateway must ied using OTP, provisioned on upload or modified per
IPv4 address:	172.17.1.105
Netmask:	255.255.255.0
WAN PORT ASSIGNMENT	
Port	GE-0/0/2 🔻
Secure with ACL	
	Cancel Save

Step 8: Repeat Step 5 - Step 7 to assign the remote (peer) WAN uplink for the primary gateway.

Add/Edit wan port	
Gateway	🔘 Local 💿 Peer
WAN CONNECTION	
Uplink	isp-1_inet
WAN type	Internet 💌
WAN speed	200 Mbps
Source NAT	\checkmark
Use as backup	
IP addressing method	DHCP -
Only four uplinks wi can be created	th DHCP IP addressing method
WAN PORT ASSIGNME	NT
Port	GE-0/0/3 👻
Secure with ACL	\checkmark
	Cancel

Step 9: Click Save Settings.

Step 10: In the **WAN Uplinks/Ports** table, verify that the WAN ports have been allocated to both gateways.

← → C ▲ app-prod2-u	i.central.arubanetworks.co	om/frontend/#/caas/l	asic/wan	?tab=wanPorts									*	8
aruba Central				٩								۹	0 :::	8
🖓 BGW-7005-НА 🔻	JW634A-20:4C:03	3:2F:F4:2C ×												
🕸 GATEWAY	GATEWAY									SELECTED DEVIS Branch Gates	LE TYPE way			10
- MANAGE														
88 OVERVIEW	SYSTEM	LAN WA	N S	DWAN & ROU	TING R	EDUNDANCY	-			Advanced I	Mode	Guide	d Setu	p
Ø DEVICE	Health Checks	Load Balancin		VAN Details										
LD CLIENTS				and become										
I APPLICATIONS	Each branch gate	eway connects to one	or more	Internet, MPLS a	ind cellular	based WAN serv	ices using W/	AN ports. A g	ateway can s	upport a maximum of four Wired WAN	links	Show	More	
ANALYZE				-										
ALERTS & EVENTS	Enable High Ava	ilability deployment												
AUDIT TRAIL	Local gateway			R53-7005-2 (20)	40:03:21:14:2	(c)								
S TOOLS	Peer gateway			RS3-7005-1 (20:	4 -									
REPORTS	Site ID			Type to search	or add									
MAINTAIN	Site to													
Ø FIRMWARE														
	HA VLAN			1	*									
	Local VLAN IP	/netmask		10.8.8.3	255.3	55.255.0								
	Peer VLAN IP	netmask		10.8.8.2	255.3	155.255.0								
	Local/	Peer should have atle	ast one p	hysical uplink pr	ort									
	WAN UPLI	NKS / PORTS								+				
	GATEWAY	UPLINK	TYPE	PORT	VLAN ID	ADDRESS	SPEED	NAT	BACKUP					
	Local	turbo_mpls	MPLS	GE-und	4084	DHCP	500 M	Disabled	Disabled					
	LOCA													
	Local	isp-2_inet	INET	GE-und	4085	DHCP	200 M	Enabled	Disabled					
			INET INET MPLS	GE-und GE-und	4085 4086 4084	DHCP DHCP DHCP	200 M 200 M	Enabled Enabled Disabled	Disabled Disabled					

7.11 Assign a Default Route for MPLS

Step 1: On the Gateway tab, in the SDWAN & ROUTING section, select Static Routing.

Step 2: In the **Default Routes** table, click the plus (+) sign to create a new static route.

a
۲

Step 3: In the **Type** column, enter a name for the new route (example: **Nexthop**).

Step 4: In the Next Hop/VPNC column, enter the IP address for the route (example: 172.17.1.1).

Step 5: Click Save Settings.

Default Routes							
ТҮРЕ	NEXT HOP/VPNC	UPLINK	соят				
Nexthop	172.17.1.1		1				

7.12 Configure the LAN Redundancy

Step 1: On the Gateway tab, in the Redundancy section, select VRRP.

Step 2: In the **VRRP interfaces** table, click the plus (+) sign.

🗧 🔍 🌒 👩 Aruba Central	× +											
← → C 🌢 app-prod2-ui.	.central.arubanetworks	.com/frontend/i	#/caas/basic/r	edundancy?tab=vr	rrp						* 6	•
				0						٩	0 11	8
▼ BGW-7005-HA ▼	JW634A-20:4C:	03:2F:F4:2C	×									
🙊 GATEWAY	GATEWAY								Branch Gateway			۲
- MANAGE												
88 OVERVIEW	SYSTEM	LAN	WAN	SDWAN & ROU	UTING REDUNE	ANCY			Advanced Mode	Guide	d Setup	6
B DEVICE	VRRP											
CLIENTS							8	3				
APPLICATIONS		allows you to s	et up 2 gatewa	iys to share the sar	me Virtual IP function	ing as the default gate	eway for the associated VI	AN, so if one goes dow	n the other becomes	Show	More	
ANALYZE ALERTS & EVENTS	Per-field help											
AUDIT TRAIL	VRRP IN	TERFACES						+				
S TOOLS	VLAN ID		IP ADDRESS	ON LOCAL	P ADDRESS ON PEER	VIRTUAL IP	MASTER					
REPORTS												
- MAINTAIN					No data to dis	olay						
FIRMWARE												
14												

Step 3: In the **VLAN ID** drop-down list, select a LAN VLAN. The IP Address on Local and IP Address on Peer columns should auto-populate with the IP address values.

Step 4: In Virtual IP column, enter an IP address (typically .1 is used). For example, **10.8.8.1**.

Step 5: In the **Master** column, select which gateway you intend to use as the VRRP master.

VRRP INTERFACES										
VLAN ID	IP ADDRESS ON LOCAL	IP ADDRESS ON PEER	VIRTUAL IP	MASTER						
1 🔹	10.8.8.3/24	10.8.8.2/24	10.8.8.1	🔵 Local 💽 Peer						

Step 6: Repeat Step 2 - Step 4 for all user VLANs.

Step 7: Click Save Settings.

VRRP INTERFACES									
VLAN ID	IP ADDRESS ON LOCAL	IP ADDRESS ON PEER	VIRTUAL IP	MASTER					
1	10.8.8.3/24	10.8.8.2/24	10.8.8.1	peer					
20	10.8.9.3/24	10.8.9.2/24	10.8.9.1	peer					

Procedures

Configuring the Branch Switch UI Group

- 8.1 Create the Branch Switch UI Group
- 8.2 Configure the Switch VLANs
- 8.3 Configure the Uplinks for the VLANs

For branch switches, you can create a single UI group that includes different hardware models. You can configure common items like VLANs and uplink ports at the group level, and configure other settings, such as VLAN assignments at the user ports, at the device level.

8.1 Create the Branch Switch UI Group

Step 1: In the filter drop-down list, select **All Devices**, and then in the left navigation pane, select **Groups** or **Organization**.

Step 2: On the Groups tab, click New Group.

	♥ TYPE ed Aruba S Aruba S.	SERIAL # CN87HKW227	Prequirements into a single
A DECKES B OVERNEW B OPICKS C CLIENTS C CLIEN	♥ TYPE ed Aruba S Aruba S.	SERIAL # CN87HKW227	♥ MAC ADDRESS
VEX.NORK SERVICES ♥ GROUP NAME DIVICES ♥ ILOCATION ALLCONNECTED DEV.L 26 Aruba-2300-24G.P. Sacramenta,Uhino ALLCONNECTED DEV.L 26 Aruba-2300-24G.P. Sacramenta,Uhino ALLCONNECTED DEV.L 26 Aruba-2300-24G.P. Sacramenta,Uhino ALLCONNECTED DEV.LS 0 Aruba-2300-24G.P. Spring,Uhited 52a ALLCONNECTED DEV.LS 0 Aruba-2300-8G.P. Spring,Uhited 52a ALDOIS 100 2330-MStack 0 Aruba-3810M-24G.S. Sacramenta,Uhito REPORTS 000 3310-MStrogle 0 Aruba-3810M-24G.S. Sacramenta,Uhito BRV7005 4 DC1-702+1 Sacramenta,Uhito Sacramenta,Uhito BRV7005-HA 4 DC1-702+2 Sacramenta,Uhito	ed Aruba S. tes Aruba S.	. CN87HKW227	
ALL CONNECTED DIV. 30 À ALLOT TAAIL UNASSIGNED DIVICES 0 À ALDIT TAAIL 12 23005-fosgle 0 À ADDIT TAAIL 12 23005-fosgle 0 À TODIS 16 29300-450-PL Conway,United Status B REPORTS 10 31310M Single 0 B REVINS 10 30310M Single 0 Ø REPORTS 10 3000-500-540 -PL Scaramenta,United Status Ø REPORTS 10 3000-500-540 -PL Scaramenta,United Status Ø REPORTS 10 3000-5000-540 -PL Scaramenta,United Status	ed Aruba S. tes Aruba S.	. CN87HKW227	
ALERTS & EVENTS UNASSIGNED DEVICES 0 Auto-2306-Mage Spring United 52x A UDIT TRAIL 10 2306-Mage 0 Auto-2306-Mage Spring United 52x A UDIT TRAIL 10 2306-Mage 0 Auto-2306-Mage Spring United 52x A TODLS 10 2306-Mage 0 Auto-2306-Mage Spring United 52x A REPORTS 10 3810M-Single 0 Auto-3810M-24G- Spring United 52x MURITAIN BOW-7005 4 0 Del-3024-1 Spring United 52x FIRMWARE BOW-7005+MA 4 DCI-7024-2 Spring United 52x	tes Aruba S.		
AUDIT TRAIL TEC 2930F-Single 0 Audust 2930F-Bingle 0 Audust 2930F-Single 0 Audust 2930F-Bingle 0 Audust 2930F-Bingle ConwayUnited 3 TODLS TE 2930F-Single 0 Audust 2930F-Bingle Secaramenta,United 3 Audust 2930F-Bingle Secaramenta,United 3 Audust 2930F-Bingle Secaramenta,United 3 Audust 2930F-Bingle Secaramenta,United 3 Secaramenta,			
TODLS Top 2004-50ack 0 Aruba 38104-24G Sazamento,Union D REPORTS 10 38104-5ingle 0 Aruba 38104-24G Sazamento,Union D REMOVARE BGW-7005-14A 4	tat Aruba S.		f4:03:43:fb:75:c0
INEPORTS 16 38104-Single 0 Aruba-38104-24G. Sacramento,Lion MINTAIN BGW-7005 4 DC1-7024-1 Sacramento,Lion FIRMWARE BGW-7005-HA 4 DC1-7024-2 Sacramento,Lion			38:21:c7:ba:f0:00
алитили BGW-7005 4 DC1-7028-1 Sacramenta.Unite D FIRAMWARE BGW-7005-HA 4 DC1-7028-2 Sacramenta.Unite			ec:eb:b8:17:f3:00
FIRMWARE BGW-7005+HA 4 DC1-7024-2 Sacramento,Unitit			ec:eb:b8:f5:1c:00
		CZ0000091	00:0b:86:bb:bb:a7
CORGANIZATION BGW-Dual-RS15 5 DC2-7210-1 Sacramento,Unito		CZ0001699	00:0b:86:bb:ff:a7
		CV0016870	00:1a:1e:05:01:a0
default 9 DC2-7210-2 Sacramento,Unite	ed MC	CV0016872	00:1a:1e:05:01:28

Step 3: In the Create New Group dialog box, implement the following settings:

- Group Name—SW-Branch
- Switch—Unselect this option
- Password—password
- Confirm Password—password

Step 4: Click Add Group.

	CREATE NEW GROUP	
	GROUP NAME SW-Branch Use the group as Template group by selecting the device 1 LAP AND GATEWAY Group password settings 1 PASSBOOD	
	Contrast Add Group	
Note If you inten sites at this point.	d to use the Install Manager App, assign the group to the	(

Use the following steps to navigate to the switch UI group configuration menu.

Step 5: In the filter drop-down list, select the new group you created for the branch switches (example: **SW-Branch**).

Step 6: In the left navigation pane, in the Manage section, select **Devices**.

Step 7: Select the **Switches** tab, and then click the gear icon in top right.

●●● Aruba Central ← → C ● app-prod2-u	× +	/frontend/#/SWITCH/LIST					× 0 :
			Q Search o	or ask Aruba			۹ 🛛 📖 👌
SW-Branch							
GROUP	ACCESS POINTS	SWITCHES 🙊 GA	TEWAYS				💷 a. 🚳
- MANAGE	-						
BB OVERVIEW	SWITCHES .	UP O DOWN					
	_						
LD CLIENTS	T DEVICE NAME	CLIENTS	ALERTS	Y MODEL	CONFIG STATUS	LAST SEEN	USAGE
at GUESTS							
APPLICATIONS							
SECURITY							
ALERTS & EVENTS							
AUDIT TRAIL							
TOOLS							
REPORTS							
- MAINTAIN -							
G FIRMWARE							
∀ SW-Branch ▼							
CROUP	ACCESS POINTS	SWITCHES A GA	TEWAYS				i ii 🛞
- MANAGE 89 OVERVIEW	SWITCHES STACKS	INTERFACE SECURITY SY	STEM IP SETTINGS IG	SMP CONFIGURATION AUDIT			
OVERVIEW DEVICES							
	Switches						
A GUESTS	HOSTNAME	IP ASSIGNMENT	IP ADDRESS	DEFAULT GATEWAY	MAC ADDRESS	LOCATION	CONTACT
I APPLICATIONS							
SECURITY				-1.			
- ANALYZE				()			
ALERTS & EVENTS							
AUDIT TRAIL							
TOOLS							
REPORTS							
- MAINTAIN -							
FIRMWARE							

8.2 Configure the Switch VLANs

Step 1: On the Switches tab, in the Interface section, select **VLANs**.

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

(TTTTTTT)		rks.com/frontend/#/CC								* 6
Uba Central				Q Search or ask	Aruba				٩	0 :::
Branch 🔻										Эзно
UP	ACCESS PO		ES @ GATEWAYS							ii 6.
t	SWITCHES ST	ACKS INTERFACE S	ECURITY SYSTEM	P SETTINGS IGMP	CONFIGURATION AUDIT					
ERVIEW		_				8				
VICES	Ports PoE 1	Trunk Groups VLANs	Spanning Tree Loop	Protection						
ENTS										1 VLANS
STS	VLANs	Settings								
CATIONS	VLANS									(+
RITY										
	10	NAME DEFAULT_VLAN	IP ASSIGNMENT	IP ADDRESS	TAGGED PORTS	UNTAGGED POR 1-52	DHCP HELPER IP	VOICE	јимво Х	
EVENTS		DEMOLI_YON				1-52		^	<u>^</u>	
AIL										
RTS										
RE										
		Relay Settings								
	> DHCP I	keiay sectings								
	> DHCP I	keiay sectings								
	> DHCP I	relay sectings								

Step 3: In the New VLANs dialog box, implement the following settings:

- ID-20
- Name—Employee

Step 4: Click OK, and then click Save Settings.

VLANs	×
ID	20
Name	Employee
IP Assignment	Disabled V
DHCP Server	
DHCP Helper IP	
Voice	
Cancel	ОК

8.3 Configure the Uplinks for the VLANs

Step 1: On the Switches tab, in the Interface section, select **VLANs**.

Step 2: In the **VLANs** table, select the VLAN you configured in Procedure 8.2 (example: **Employee**), and then click the pencil icon.

🔍 🔍 💽 Aruba Central											
← → C a app-prod2-ui.	.central.arubanetwo	orks.com/frontend/#/CC	NFIGHPVLANS							* 8	
aruba Central				Q Search or ask /	Aruba					2 1 11	8
										Э з ной	RS
11 GROUP	O ACCESS PC		S 🙊 GATEWAYS							10 A.	۲
- MANAGE	SWITCHES ST	TACKS INTERFACE S	ECURITY SYSTEM	P SETTINGS IGMP	CONFIGURATION AUDIT						_
88 OVERVIEW	1										
	Ports PoE	Trunk Groups	Spanning Tree Loop	Protection							
LD CLIENTS										2 VLANS	
A GUESTS	VLAN:	s Settings									
APPLICATIONS	VLAN									+	
SECURITY											
- ANALYZE	1D	DEFAULT_VLAN	IP ASSIGNMENT	IP ADDRESS	TAGGED PORTS	UNTAGGED POR	DHCP HELPER IP			-	
ALERTS & EVENTS	20	Employee	-		-	-	-		_		
AUDIT TRAIL											
S TOOLS											
REPORTS											
@ FIRMWARE											
	> DHCP	Relay Settings									
javascript:											

Step 3: In the VLAN Port Mode section, in the **Ports** table, select the uplink ports for the branch gateway(s).

Step 4: In the Select Port Mode drop-down list, select Tagged, and then click OK.

ts			Trunk Groups		
PORT	PORT MODE	TRUNK GROUP =		PORT MODE	=
	None				
2	None	-			
3	None	-			
4	None	-	(*	III E	
5	None		+		
6	None		No dat	ta to display	
7	None				

Step 5: Click Save Settings.

Procedures

Configuring the Device Switch UI Group

- 9.1 Assign a Switch Device to a Switch UI Group
- 9.2 Configure the Device Switch Hostname

In the case of branch switches a single UI group that includes different models can be created. Common items like VLANs and uplink port configurations can be done at the group level while VLAN assignments at the user ports can be configured at the device level.

9.1 Assign a Switch Device to a Switch UI Group

Step 1: On the Aruba Central Account Home page, select Device Inventory.

Step 2: In the View Devices table, select a switch, and then click **Assign Group**.

GO TO ACCO	UNT HOME							
DEVICE II	NVENTOR	Y						
View the devices in	your inventory and i	manually add	devices here.					
VIEW DEVICES								
♥ SERIAL NUMBER	T MAC ADDRESS	TYPE	IP ADDRESS	NAME	Y MODEL	PART NUMBER	GROUP	♥ SUBSCRII
CNDDJSST1R	20:A6:CD:C0:36:2E	iap	10.8.16.11	20:a6:cd:c0:36:2e	IAP-305-US	JX946A	default	0
CNDDJSST6Q	20:A6:CD:C0:37:62	iap			IAP-305-US	JX946A		0
CNDDJSSTDQ	20:A6:CD:C0:38:D6	iap	10.8.0.5	AP305-D6	IAP-305-US	JX946A	default	0
CNDDJSSTDX	20:A6:CD:C0:38:E2	iap	10.8.0.6	AP305-E2	IAP-305-US	JX946A	default	0
CNDDJSSTDY	20:A6:CD:C0:38:E4	iap			IAP-305-US	JX946A		0
CNDRJSSDV0	20:A6:CD:C3:0A:32	iap			IAP-305-US	JX946A		0
CNDRJSSDWH	20:A6:CD:C3:0A:8E	iap			IAP-305-US	JX946A		0
CNDRJSSDWP	20:A6:CD:C3:0A:9A	iap			IAP-305-US	JX946A		0
CNFDK513T2	38:17:C3:C0:53:8A	iap	10.8.0.4	AP345-8A	AP-345-US	JZ033A	default	
 CN93HKZ48Y 	38:21:C7:BA:F0:00	switch	10.8.44.2	R\$12-2930F	2930F	JL258A	SW-Branch	0
• CK0234513	40:E3:D6:C1:34:6C	lap			IAP-215-US	IAP-215-US		0
CNHPK9Y01Q	80:8D:87:C0:15:F9	lap	10.8.56.104	R\$15-AP-555-1	AP-555-US	J2357A	BGW-Dua	0
• CT0338957	94:84:0F:C6:58:18	iap			IAP-225-US	IAP-225-US		0
 CN85HKZ0KZ 	94:F1:28:8C:D2:A0	switch		R\$15-2930F-1	2930F	JL258A	BGW-Dua	0
CN87HKW227	88.83:03:38:AA:C0	switch			2930F	JL255A		12
CN80HKZ05H	B8:83:03:D7:66:80	switch	10.8.56.103	R\$15-2930F-1	2930F	JL258A	BGW-Dua	0
SG70GYW01J	EC:EB:B8:17:F3:00	switch	10.8.0.3	Aruba-3810M-24G	3810	JL073A	default	0
SG7BGYW0C8	EC:EB:B8:F5:1C:00	switch	10.8.12.3	Aruba-3810M-24G	3810	JL073A	default	0
• CN79HKZ081	F4:03:43:F8:75:C0	switch	10.8.40.4	Aruba-2930F-8G-P	2930F	JL258A	default	0
CNHJKD58Y5	F4:2E:7F:C7:7D:F2	iap	10.8.56.106	R\$15-AP-515-1	AP-S15-US	Q9H63A	BGW-Dua	0
CNHJKD58Y6	F4:2E:7F:C7:8E:88	iap	10.8.56.107	RS15-AP-515-2	AP-515-US	Q9H63A	BGW-Dua	0
								53 Device(s)

Step 3: In the Assign a Group to the Select Device dialog box, select the switch UI group you created in Procedure 8.1 (example: **SW-Branch**).

7 GROUP NAME	
TG 2930F-Single	
TG 2930M-Stack	
TG 3810M-Single	
BGW-7005	
BGW-7005-HA	
BGW-Dual-RS15	
default	
SW-Branch	
VPNC-7024	
VPNC-7210	

Step 4: Click Assign device(s), and then click OK.



9.2 Configure the Device Switch Hostname

Step 1: On the Aruba Central Account home page, launch the **Networks Operations** app.

Step 2: In the filter drop-down list, select the switch UI group you created in Procedure 8.1 (example: **SW-Branch**).

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

Step 4: In the **Switches** table, select the switch you intend to configure, and then click the pencil icon.

🔍 🔍 🔍 Arub	a Central × +							
← → ♂ ●	app-prod2-ui.central.arubanetworks	.com/frontend/#/CONFIGHPSWITC	HES					* 🖰 i
aruba	Central		Q Sec				۹ (۵ 🚜 🕈
SW-Branch								
C GROUP	G ACCESS POINT		EWAYS				:=	a. 💿
- MANAGE	SWITCHES STAC	S INTERFACE SECURITY SYST	TM IP SETTINGS IGMP	CONFIGURATION AUDIT				_
88 OVERVIEW								
DEVICES							2.5%	vitches
LD CLIENTS	Switches							
# GUESTS								-
	IS HOSTNAME RS12-2930F	IP ASSIGNMENT DHCP	IP ADDRESS 10.8.44.2	DEFAULT GATEWAY 10.8.44.1	MAC ADDRESS 38:21:c7:ba:f0:00	LOCATION	CONTACT	_
SECURITY	JL255A-88:83:0		10.0.44.2	10.0.44,1	B8:83:03:38:AA:C0			
- ANALYZE		CONTRACTOR AND						
ALERTS & EV	ENTS							
AUDIT TRAIL								
S TOOLS								
REPORTS	5 10 25 5	0 Per Page					K < > >	Page: 1/1
- MAINTAIN								50 E
FIRMWARE								

Step 5: In the Edit Switches dialog box, in the **Hostname** box, enter a name (example: **RS3-2930F**).

Step 6: Click OK.

EDIT SWITCHES		×
Hostname	RS3-2930F	
IP Assignment	DHCP V	
Location		
Contact		
Cancel	0	к

Step 7: Click Save Settings.

Procedures Configuring the Branch Access Points Group 10.1 Create the Access Point Group 10.2 Create A New Network: SSID General Settings 10.3 Create a New Network: Client VLANs 10.4 Create a New Network: WLAN Security 10.5 Specify the Radio Settings

10.1 Create the Access Point Group

Step 1: In the filter drop-down list, select **All Devices**, and then in the left navigation bar, select **Groups** or **Organization**.

Step 2: On the Groups tab, click New Group.

	GROUPS 🖉 SITES AN							۹ (5 #
SLOBAL									2 -4
WAGE		DIABELS CERTIFICA		MANAGER					
OVEDVEEN		v centric							
OVERVIEW	GROUPS								
DEVICES		acts like a primary config	uration container	for devices. You can combi	ine devices with commo	n configurat	tion requirements in	to a single group and ap	ply
CLIENTS	the same configuration se								
GUESTS	MANAGE GROUPS								
APPLICATIONS	DRAG AND DROP CLUSTER								
SECURITY	TO SELECT MULTIPLE DEVI	CES SHIFT+CLICK OR CTRL	+CLICK						
NETWORK SERVICES	GROUP NAME	DEVICES		▽ NAME		▼ TYPE	▼ SERIAL #	▼ MAC ADDRESS	
ALYZE	ALL CONNECTED DEVICES	30	1	Aruba-3810M-24G-Po_	Sacramento.United St	Aruba S	SG7BGYW0C8	eceb:b8:f5:1c00	ĥ
ALERTS & EVENTS	UNASSIGNED DEVICES	0		DC1-7024-1	Sacramento, United St	MC	C20000091	00:0b:86:bb:bb:a7	1
AUDIT TRAIL	TG 2930F-Single	0		DC1-7024-2	Sacramento, United St	MC	CZ0001699	00:0b:86:bb:ff:a7	J.
TOOLS	TG 2930M-Stack	2		DC2-7210-1	Sacramento, United St	MC	CV0016870	00:1a:1e:05:01:a0	
REPORTS	TG 3810M-Single	0	+	DC2-7210-2	Sacramento, United St	МС	CV0016872	00:1a:1e:05:01:28	
INTAIN	BGW-7005	4		HP-2920-48G-POEP		Aruba S	SG82JQP24L	04:09:73:b3:df:40	
FIRMWARE	BGW-7005-HA	6		IAP-Thomas1	Sacramento,United St	IAP	CNDDJSST1R	20:a6:cd:c0:36:2e	
ORGANIZATION	BGW-Dual-RS15	5		IAP535-VC-RS12	Conway,United States	IAP	CNHLK9W0PX	00:4e:35:c4:9a:5e	
	default	5		Instant-RS1	Sacramento, United St	IAP	CNFDK513T2	38:17:c3:c0:53:8a	
	New Group		10 Group(s)					30 Devi	ce(s)

Step 3: In the Create New Group dialog box, implement the following settings:

- Group Name—AP-Branch
- Switch—Unselect this option
- Password—password
- Confirm Password—password

Step 4: Click Add Group.

Use the group as Template group by selecting the device ()
Group password settings
CONFIRM PASSWORD
Cancel Add Group

Use the following steps to navigate to the AP group configuration menu.

Step 5: In the filter drop-down list, select the group you created for the branch access points in Procedure 10.1 (example: **AP-Branch**).

Step 6: In the left navigation pane, in the Manage section, click **Devices**.

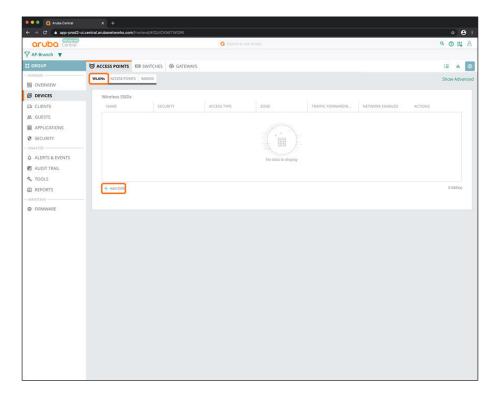
Step 7: Select the **Access Points** tab, and then click the gear icon in the top right.

→ C A app-prod2-u	+ ×	Ifrontendia								* (
	commanandoanetworks.com	errontenapa	(Wellclat	-	Search or ask Ar					۹ 🔊 📖
AP-Branch					Search or ask w					~ © :::
GROUP	図 ACCESS POINTS	SWIT	CHES @ GATE	WAYS						1
IANAGE	-									-
B OVERVIEW	ACCESS POINTS	• UP		DIOS						
DEVICES	0	0	0	0						
b CLIENTS	ACCESS POINTS									₹ €
GUESTS				RADIO 1		RADIO 2				
APPLICATIONS		1	CHANNEL	POWER (DBM)	CHANNEL	POWER (DBM)	▼ IP ADDRESS IF	Y MODEL	11" FIRM	WARE VERSION
SECURITY										
VALYZE										
ALERTS & EVENTS										
AUDIT TRAIL										
TOOLS										
REPORTS										
INTAIN										
FIRMWARE										
						No data to displa	iy.			

Step 8: Notice the group name in the filter and that the gear icon is selected.

11 GROUP	access points	SWITCHES @ GATEWA	AYS					ii 16 🛞
- MANAGE 88 OVERVIEW	WLANS ACCESS POINTS	ADIOS						Show Advanced
	Wireless SSIDs							
L CLIENTS	NAME	SECURITY	ACCESS TYPE	ZONE	TRAFFIC FORWARDIN	NETWORK ENABLED	ACTIONS	
A GUESTS								
# APPLICATIONS								
SECURITY								
- ANALYZE								
ALERTS & EVENTS				No data to displ	ay			
AUDIT TRAIL								
S TOOLS								
REPORTS	+ Add SSID							0 SSID(s)
- MAINTAIN								
FIRMWARE								

10.2 Create A New Network: SSID General Settings



Step 1: On the Access Points tab, in the WLANs section, click **Add SSID**.

Step 2: In the Create a New Network dialog box, in the General section, enter an SSID name (example: **Example-Employee**).

Step 3: Click Next.

1 General Name (SSID):	VLANs	3 Security	Access	Summary Example-Employee	
> Advanced Se	ettings				
				Cancel	Nex

10.3 Create a New Network: Client VLANs

The client VLANs need to match the switch and branch gateway VLANs in order to establish connectivity. The branch switch ports that connect to the access points must allow the VLANs and configure the access point (AP) ports on the switches as tagged.

Step 1: In the Create a New Network dialog box, in the VLANs section, select Static.

CREATE A NEW NETWORK		
1 General 2 VLANs 3 Security 4 Access	Summary	
Client IP Assignment:	Instant AP assigned External DHCP server assigned	
Client VLAN Assignment:	Static Dynamic Native VLAN	
VLAN ID:	•	
> Show Named VLANs		
		Cancel Back Next
		Cancel Back NEXT

Step 2: Click Show Named VLANs, and then click Add Named VLAN.

V Hide Named VLANs	VLAN	ACTIONS	
	-()		
	No data to display		
+ Add Named VLAN			0 Named VLAN(s)

Step 3: In the Add Named VLAN dialog box, implement the following settings:

- VLAN Name—Employee
- VLAN-20

ADD NAMED VLAN		×
VLAN Name:	VLAN:	
Employee	20]
Cancel		ОК

Step 4: Click OK.

REATE A NEW NETWORK	
1 General 2 VLANS 3 Security 4 Access	5 Summary
Client IP Assignment:	Instant AP assigned External DHCP server assigned
Client VLAN Assignment:	Static Dynamic Native VLAN
VLAN ID:	Employee T

Step 5: In the VLAN ID drop-down list, select the VLAN you created (example: Employee), and then click Next.

10.4 Create a New Network: WLAN Security

Option 1: Passphrase Authentication

Use the following steps to enable authentication by using a WPA3 personal passphrase.

Step 1: In the Create a New Network dialog box, in the Security section, click **Personal**.

Step 2: In the **Passphrase** box, enter a password, and then in the **Retype** box, re-enter the password.

General 2 VLANs 3 Security	Access Summary
Security Level:	Enterprise Personal Captive Portal
Key Management:	WPA3-Personal
Passphrase Format:	8-63 chars
Passphrase:	
Retype:	······

Step 3: Click Advanced Settings.

Step 4: Click Fast Roaming, and then select 802.11k and 802.11v

Step 5: Click Next.

~	Advanced Settings	
	MAC Authentication:	
	Blacklisting:	
	Max Authentication Failures:	0
	Enforce DHCP:	
	WPA3 Transition:	
	Use IP for Calling Station ID:	
	Called Station ID Include SSID:	
	Sast Roaming	
	802.11k:	
	802.11v:	
		Cancel Back Next

Option 2: Username and Password Authentication

In this procedure, you enable WPA3 Enterprise authentication.

Step 1: In the Create a New Network dialog box, in the Security section, click **Enterprise**.

Step 2: In the **Primary Server** drop-down list, select a server, and then click the plus (+) sign to define the authentication server parameters.

Step 3: Click Advanced Settings, and then click Fast Roaming.

1 General 2 VLANs 3 Security	Access (5) Summary
Security Level:	Enterprise Personal Captive Portal Open
Key Management:	WPA3-Enterprise(CCM 128)
Primary Server:	InternalServer 🔻 🕂
Users:	0 Users Manage Users
	Only registered users of type ' Employee ' will be able to access thi network.
Advanced Settings	

Step 4: Select 802.11k and 802.11v.

✓ Advanced Settings	
MAC Authentication:	
Blacklisting:	
Max Authentication Failures:	0
Enforce DHCP:	
WPA3 Transition:	
Use IP for Calling Station ID:	
Called Station ID Include SSID:	
Fast Roaming	
802.11k:	
802.11v:	
	Cancel Back Next

Step 5: Click Next.

CREATE A NEW NETWORK		
1 General 2 VLANs 3 S	security Access 3 Summary	
Access rules	Role Based Network Based Unrestricted	
	Unrestricted option allows full access to the network. This may lead to potential security issues.	
Downloadable Role:		
		Cancel Back Next

Step 6: On the Access tab, click Next, and then on the Summary tab, click Finish.

10.5 Specify the Radio Settings

Step 1: On the Access Points tab, select Radios.

Step 2: In the Client Control section, implement the following settings:

- Airtime Fairness Mode—Fair Access
- **ClientMatch**—Enable this option
- ClientMatch Threshold—30

Step 3: If you use multiple access points in the sites, use the slider to disable 80 MHz Support.

🔍 🔍 🔍 Aruba Central	× +		
← → C 🔒 app-prod2-u	i.central.arubanetworks.com/frontend/#/RF		* 🛛 :
aruba Central		Q Search or ask Aruba	۹ 🕲 📖 👌
Y AP-Branch V			
II GROUP	ACCESS POINTS SWITCHES	@ GATEWAYS	i= n. 🙁
- MANAGE	WLANS ACCESS POINTS RADIOS		Show Advanced
88 OVERVIEW			
	RF		
LD CLIENTS	✓ Adaptive Radio Management	(ARM)	
2. GUESTS	Client Control		
# APPLICATIONS			
SECURITY	Band Steering Mode:	Prefer 5 GHz	
- ANALYZE	Airtime Fairness Mode:	Fair Access	
ALERTS & EVENTS	ClientMatch:		
AUDIT TRAIL			
S TOOLS	ClientMatch Calculating Interval:	3 seconds	
REPORTS	ClientMatch Neighbor Matching:	60 %	
MAINTAIN FIRMWARE	ClientMatch Threshold:	30	
	Spectrum Load Balancing Mode:	Channel	
	Access Point Control		
	Customize Valid Channels:		
	Min Transmit Power:	9 V	
	Max Transmit Power:	Max 🔻	
	Client Aware:		
	Scanning:		
	Wide Channel Bands:	5 GHz 🛛 🔻	
	80 MHz Support:		
	> Radio		
25			

Step 4: Expand **Radio**, and then in the 5 GHz band table, click the plus (+) sign.

Step 5: In the MIN/MAX Power column, enter 15/18 for walled-office environments.

2.4 GHz band +			+	5 GHz band			+
NAME	ZONE	MIN/MAX POWER		NAME	ZONE	MIN/MAX POWER	=
default		6/9		default		15/18	

Procedures

Configuring the WLAN Access Points

11.1 Assign the WLAN AP Group

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

11.1 Assign the WLAN AP Group

Step 1: In the filter drop-down list, 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 virtual controller clusters and assign the virtual controller clusters to the AP group you created in Procedure 10.1 (example: **AP-Branch**).

Central					Q Search or ask A						۹ ()	
II Devices 🔻												
LOBAL	🗇 ACCESS POINTS 📼 S	WITCH	ES @ GATEV	VAYS								
NAGE												
OVERVIEW	ACCESS POINTS	0	NOWN RAD									
DEVICES	8 7		1 1	7								
CLIENTS	ACCESS POINTS										J.	
GUESTS				ADIO 1		RADIO 2						
		18	CHANNEL	POWER (DBM)	CHANNEL	POWER (DBM)	♥ IP ADDRESS IF	Y MODEL		112	FIRMWARE VERSION	
APPLICATIONS	© 20:a6:cd:c0:36:2e (VC)						10.8.16.11	AP-305	CNDD)SST1R		8.6.0.2_73853	
SECURITY	 RS15-AP-555-1 (VC) 		149 (80 MHz)	18	1 (20 MHz)	9	10.8.56.104	AP-555	CNHPK9Y01Q		8.6.0.3_74788	
NETWORK SERVICES	 RS15-AP-515-1 		52 (80 MHz)	18	6 (20 MHz)	9	10.8.56.106	AP-515	CNH5KD58Y5		8.6.0.3_74788	
LYZE	 R\$15-AP-\$15-2 20:a6:cd:c0:38:e2 (VC) 		100 (80 MHz)	18	11 (20 MHz) 11 (20 MHz)	9 24	10.8.56.107	AP-515 AP-305	CNH(KD58Y6 CNDD)(SSTDX		8.6.0.3_74788 8.5.0.5_73491	
ALERTS & EVENTS	 20:a6:cd:c0:38:62 (VC) 20:a6:cd:c0:38:66 					24		AP-305 AP-305			8.5.0.5,73491	
AUDIT TRAIL	+ R\$12-555-1 (VC)		149 (80 MHz)	18	6 (20 MHz)	9		AP-535	CNHLK9W0PX		8.6.0.4,74969	
TOOLS	+ 38:17:c3:c0:53:8a				6 (20 MHz)		10.8.0.4	AP-345	CNFDK513T2		8.5.0.5,73491	
FIRMWARE												
IRGANIZATION												
DRGANIZATION												
DRGANIZATION												
ORGANIZATION												
DRGANIZATION												
DRGANIZATION												
DRGANIZATION												
ORGANIZATION												
ORGANIZATION												
ORGANIZATION												
ORGANIZATION												

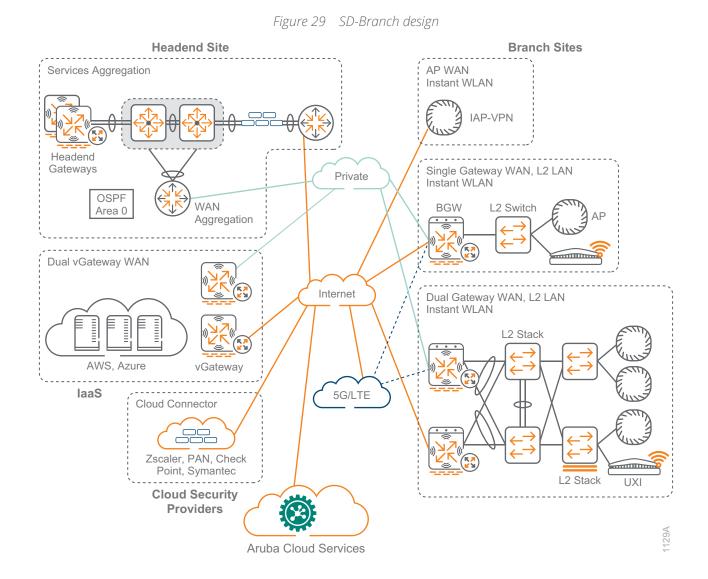
Step 4: In the left navigation pane, in the Maintain section, select **Organization**.

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

& NETWORK SERVICES	V GROUP NAME	DEVICES		V NAME	V LOCATION	TYPE	▼ SERIAL #		1
ANALYZE	TG 2930F-Single	0		RS15-7005-2	Raleigh,United States	MC	CP0047911	20:4c:03:39:85:24	
ALERTS & EVENTS	TG 2930M-Stack	2		IAP-Thomas1	Sacramento,United Sta	LAP	CNDDJSST1R	20:a6:cd:c0:36:2e	
AUDIT TRAIL	TG 3810M-Single	0		Instant-RS1	Sacramento,United Sta	IAP	CNDDJSSTDX	20:a6:cd:c0:38:e2	
S TOOLS	AP-Branch	0		R512-2930F	Conway, United States	Aruba S	CN93HKZ48Y	38:21:c7:ba:f0:00	
REPORTS	AP-RS12	1	1.12	RS15_VC	Raleigh,United States	IAP	CNHPK9Y01Q	80:8d;b7:c0:15:f9	
MAINTAIN	BGW-7005	5		R\$15-2930F-1	Raleigh,United States	Aruba S	CN85HKZ0KZ	94:f1:28:8cid2:a0	
G FIRMWARE	BGW-7005-HA	6		R\$3-2930F	Sacramento,United Sta	Aruba S	CN87HKW227	b8:83:03:38:aa:c0	
	BGW-Dual-RS15	5		R\$15-2930F-1	Raleigh, United States	Aruba S	CN80HKZ05H	b8:83:03:d7:66:80	
	default	4		R51-3810	Sacramento, United Sta	Aruba S	SG70GYW01J	ec:eb:b8:17:f3:00	

Summary

The flow of information is a critical component to a well-run organization. The Aruba SD-Branch design is a prescriptive solution based on best practices and tested topologies. This allows you to build a robust WAN network that accommodates your organization's requirements. Whether users are located at a headend site or a smaller branch site, this design provides a consistent set of features and functionality for network access, which helps improve user satisfaction and productivity while reducing operational expense.



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

What's New in This Version

The following changes have been made since Aruba last published this guide:

- SD-WAN Orchestrator components Tunnel Orchestrator and Route Orchestrator
- Aruba virtual gateways for Amazon Web Services and Microsoft Azure
- Support for single and multiple VNET/VPCs
- Hub mesh topologies
- Dynamic Path Selection and Policy Based Routing comparison
- Reverse path pinning
- Health checks and Aruba Path Quality Monitoring service
- Third-party cloud-security providers
- SaaS optimization with SaaS Express
- SD-LAN design with two-tier LAN support and dynamic segmentation
- Aruba 9000 gateways and Aruba 500 access points
- Aruba threat detection with IDS/IPS

© Copyright 2020 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



You can use the <u>feedback form</u> to send suggestions and comments about this guide.



B-000601A-20A-1 08/20 a00103243enw