

SD-Branch Fundamentals Guide

Version 1.1.1

Authors:

Kevin Marshall
Andrew Tanguay

Contributors:

Samuel Perez
Meggie Yao

Copyright Information

Copyright © 2018 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US \$10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA



www.arubanetworks.com

3333 Scott Blvd

Santa Clara, CA 95054

Phone: 1-800-WIFI-LAN (+800-943-4526)

Fax 408.227.4550

Contents

Revision History	4
About This Guide	5
Overview	5
Intended Audience	5
Scope	5
Conventions	6
Introduction	10
SD-Branch Overview.....	10
Solution Elements.....	11
Features.....	13
Aruba Central	15
Device Inventory	15
Subscription Assignment	17
Organization	20
Provisioning	33
Prerequisites.....	33
Automatic Provisioning	33
One Touch Provisioning.....	40
Bulk Configuration Upload.....	42
Aruba Gateways	44
VLANs and Interfaces	44
Wide Area Networks.....	78
Virtual Private Networks	96
Routing	109
Reference Topologies	136
Data Center Topologies.....	136
Branch Topologies.....	205
Appendix	228
Platforms and Scaling.....	228
Protocols and Ports	229

Revision History

The following table lists the revisions of this document:

Revision	Date	Change Description
1.1.1	03/13/2019	Minor edits to Aruba Gateways chapter
1.1.0	11/26/2018	Minor revisions made to entire document based on initial feedback
1.0.0	10/19/2018	Initial Publication

Table 0-1 *Revision History*

About This Guide

Overview

Aruba Fundamentals Guides are best practice recommendation documents specifically designed to demonstrate the efficacy of Aruba products and to enable customers who deploy Aruba solutions to achieve optimal results. This document is not only intended to serve as a deployment guide but also to provide descriptions of Aruba technology, recommendations for product selections, network design decisions, configuration procedures, and best practices. The cumulative Aruba documentation suite for ArubaOS 8 comprises a reference model for understanding Aruba technology and designs for common customer deployment scenarios. Our customers rely on these proven designs to rapidly deploy Aruba solutions in their production environments with the assurance that they will perform and scale as expected.

Intended Audience

This guide is intended for administrators who are responsible for deploying and configuring Aruba Software-Defined Branch (SD-Branch) solutions on customer premises. This is a base design guide for ArubaOS and it is assumed that readers have at least a working understanding of fundamental wireless concepts such as Software-Defined Wide Area Networks (SD-WAN) as well as Aruba technology.

Scope

The Validated Reference Design series documents focus on particular aspects of Aruba technologies and deployment models. Together these guides provide a structured framework to understand and deploy Aruba Wireless Local Area Networks (WLANs). The VRD series has four document categories:

- **Foundation** guides explain the core technologies of an Aruba WLAN. These guides also describe different aspects of planning, operation, and troubleshooting deployments
- **Base Design** guides describe the most common deployment models, recommendations, and configurations
- **Application** guides build on the base designs. These guides deliver specific information that is relevant to deploying particular applications such as voice, video, or outdoor campus extension.
- **Specialty Deployment** guides involve deployments in conditions that differ significantly from the common base design deployment models, such as high-density WLAN deployments.

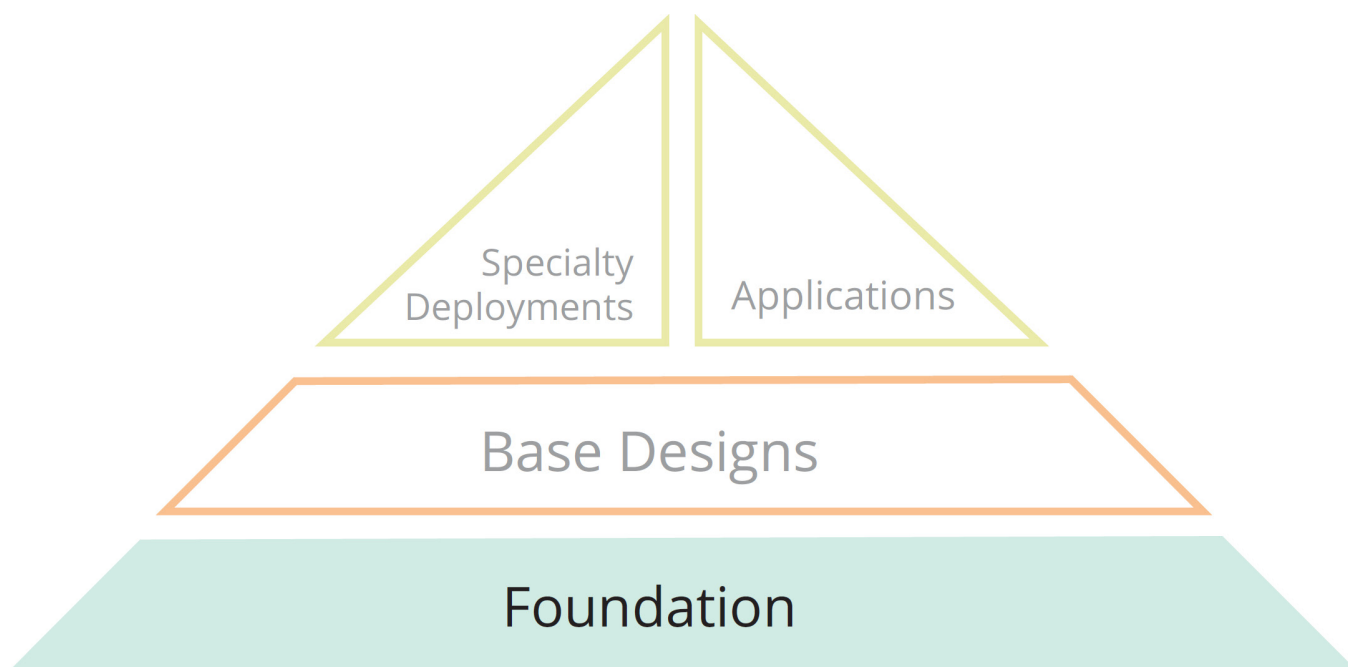


Figure 0-1 Aruba Reference Architectures

The SD-Branch Fundamentals Guide is considered a Foundation level document within the VRD core technology series.

Conventions

Typographical Conventions

The following conventions are used throughout this manual to emphasize important concepts:

Style Type	Description
<i>Italics</i>	Italics are used to emphasize important terms and to mark the titles of books.
Bolded words	Bolded words indicate an option that should be selected in the Web user interface (WebUI). The angled brackets indicate that the choices are part of a path in the UI.
Command Text	Command text in this font will appear inside of a box and indicates commands that can be entered into the Command Line Interface (CLI).
<Arguments>	In the command examples, italicized text within single angle brackets represents items that should be replaced with information appropriate to a specific situation. For example: # send <text message>

	In this example, a user would type “send” at the system prompt exactly as shown, followed by the text of the message being sent. Do not type the angle brackets.
[Optional]	Command examples enclosed in brackets are optional. Do not type the brackets.
{Item A Item B}	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

Table 0-2 *Typographical Conventions*

Informational Icons

The following informational icons are used throughout this guide:



Indicates helpful suggestions, pertinent information, and important things to remember.



Indicates a risk of damage to hardware or loss of data.



Indicates a risk of personal injury or death.

Acronym List

Acronym	Definition
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
AP	Access Point
BGW	Branch Gateway
CLI	Command Line Interface
CPU	Central Processing Unit
DC	Data Center
DLNA	Digital Living Network Alliance
DNS	Domain Name Service
DHCP	Dynamic Host Configuration Protocol

DPD	Dead Peer Detection
DPI	Deep Packet Inspection
DPS	Dynamic Path Selection
ECMP	Equal-cost Multi-path routing
FQDN	Fully-qualified Domain Name
GRE	Generic Routing Encapsulation
HA	High Availability
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IAP	Instant Access Point
IDF	Intermediate Distribution Frame
IGP	Interior Gateway Protocol
IKE	Internet Key Exchange
IKEv2	Internet Key Exchange Protocol Version 2
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISP	Internet Service Provider
LAN	Local Area Network
LAG	Link Aggregation Group
LSA	Link State Advertisement
MAC	Media Access Control
NAS	Network Access Server
NAT	Network Address Translation
NAT-T	Network Address Translation-Traversal
OTP	One Touch Provisioning
PAT	Port Address Translation
PBR	Policy-based Routing
PPPoE	Point-to-Point Protocol over Ethernet

PQM	Path Quality Monitoring
QoS	Quality of Service
RACL	Route Access Control List
RADIUS	Remote Authentication Dial In User Service
RAP	Remote Access Point
SACL	Session Access Control List
SD	Software-defined
SD-WAN	Software-defined Wide Area Network
SDN	Software Defined Network
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
TACACS+	Terminal Access Controller Access Control System Plus
TCP	Transmission Control Protocol
TPM	Trusted Platform Module
URL	Uniform Resource Locator
VIA	Virtual Internet Access
VIP	Virtual Internet Protocol address
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VPNC	Virtual Private Network Concentrator
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WebUI	Web User Interface
WLAN	Wireless Local Area Network
ZTP	Zero-touch Provisioning

Introduction

The primary purpose of this fundamentals guide is to provide readers with a foundation knowledge of the key concepts required to understand and successfully deploy an Aruba SD-Branch solution. This guide provides details for adding, configuring, managing and organizing devices in Aruba Central as well as detailed overviews of each key feature and configuration option available in the Aruba Gateway Application.

This guide also includes a reference architecture chapter that provides topologies and configuration details for common data center (DC) and branch topologies. Each reference architecture is tested and validated by Aruba SD-Branch experts as well as Aruba customers in the field. Each topology can be referenced and modified to suit specific deployment environments.

SD-Branch Overview

Software-defined wide area networking (SD-WAN) is a technology shift towards solutions that are more agile, open, and cloud integrated. SD-WAN solutions should deliver a secure, service provider independent network with enterprise level performance over different WAN technologies.

However, while SD-WAN solves a real IT problem, it only addresses one of the problems faced when dealing with distributed locations. Organizations often roll out and operate distributed, heterogeneous networks with small, centralized teams. These distributed networks offer many services besides just WAN connectivity. Branch networks need wired and wireless local area network (LAN), security and policy enforcement, and of course, WAN interconnect.

The software defined branch extends the concepts around SD-WAN to all elements in the branch, delivering a full-stack solution that addresses wired and wireless LAN, security and policy enforcement, and, of course, WAN connectivity.

The key pain points addressed by Aruba SD-Branch include:

- **WAN Connectivity** – Allows SD-WAN technology to support the use of the Internet to replace or augment MPLS services. Elements of the SD-WAN solution include Path Quality Monitoring (PQM) to track the quality of the available paths, stateful firewall with Application Fingerprinting to identify traffic flow, dynamic path selection (DPS) to always select the optimal path; and Centralized Routing to offload the branch gateways from participating in routing. In addition, user identity information can also be used when selecting from the available paths.
- **LAN Security and Automation** – Modern branch deployments can be excessively complex as designs are usually based on a proliferation of Virtual Local Area Networks (VLANs), complex Internet Protocol (IP) addressing schemes, access control lists (ACLs) distributed across multiple devices in the branch, and architectures that are tailored to the needs of automation software rather than the automation software adapting to the architecture.

The Aruba SD-Branch architecture flattens the branch into fewer subnets by consolidating all policy enforcement into a single device. Doing so eliminates dependence on static IP addressing schemes and hardwired ACLs across multiple devices.

- **Branch Onboarding and Lifecycle Management** – Small centralized teams are often forced to leverage third party companies for installations. Different companies may also be required in each geography requiring the corporate team to work with these third-party installers to bring remote locations online. This model presents significant logistical as well as technical challenges. Aruba’s SD-branch architecture has been developed with the objective of enabling Zero Touch Provisioning (ZTP) for all branch devices which allows hundreds of locations to be brought up per week. ZTP coupled with a scalable cloud-based management platform allows for organizations to set up, modify, and maintain networks in a quick and agile manner.

Solution Elements

Aruba SD-Branch consists of the following elements:

- **Aruba Central** – With flexible policy, configuration, and monitoring capabilities, organizations can simplify network operations by providing zero-touch provisioning and customizable templates. Central allows teams to quickly deploy branch networks, centralize management for Aruba Gateways, provide historical data reports, monitor for PCI compliance, and troubleshoot regional as well as global locations. Key insight into WAN health and optimization helps IT determine the best link and routes for traffic destined for corporate data centers or for the Internet. Path selection can be based on per-user, per-device, or per-application policies.
- **Provisioning** – Leverages Aruba Activate, Aruba Central, and the new Aruba Installer mobile application to simplify and streamline the deployment of new Aruba devices across branch sites. Aruba’s innovative provisioning approach allows devices to be quickly and easily deployed by contractors or non-IT staff. To deploy a new branch the installer simply scans the new Aruba devices, connects the required Ethernet cables, and provides power. Zero touch provisioning over the Internet takes care of the rest.
- **Aruba Gateways**
 - **Headend Gateways** – An Aruba 7000 Series or 7200 Series device acts as a headend gateway, or virtual private network concentrator (VPNC) for all branch offices. Branch Gateways (BGWs) establish secure Internet Protocol security (IPsec) tunnels to one or more headend gateways over the Internet or other untrusted networks. High Availability options support either multiple headend gateways deployed at a single site or headend gateways deployed in pairs at multiple sites for the highest availability.

The headend gateways support active/standby or active/active uplinks out of the branch. The most widely deployed topology is the dual hub-and-spoke where branches are multi-homed to a primary and backup data center. The headend gateway would sit

at the hub site data center and can be deployed in an active/standby or active/active configuration. Any of the headend gateways can perform the function of VPNC at the hub site. These devices offer high-performance and support a large number of tunnels to aggregate data traffic from hundreds to thousands of branches.

- **Branch Gateways** – The Aruba 7000 Series is a versatile family of hardware that can operate as an SD-Branch gateway at the branch to optimize and control WAN, LAN, and cloud security services. The branch gateway provides features such as routing, firewall, security, Uniform Resource Locator (URL) filtering, and compression.

With support for multiple WAN connection types, the branch gateway routes traffic over the most efficient link based on availability, application, user-role, and link health. This allows organizations to take advantage of high-speed, lower-cost broadband links to supplement or replace traditional WAN links such as MPLS.

Aruba SD-Branch supports specific models of 70XX and 72XX Aruba Gateways operating as VPNCs and all models of 7X00 operating as BGWs. Table 1-1 provides a matrix of which Aruba Gateway models can be deployed in each role:

Platform	VPN Concentrator	Branch Gateway
70XX Series		
7005	No	Yes
7008	No	Yes
7010	Yes	Yes
7024	Yes	Yes
7030	Yes	Yes
72XX Series		
7205	No	No
7210	Yes	No
7220	Yes	No
7240XM	Yes	No
7280	No	No

Table 1-1 Aruba Gateway Support by Role

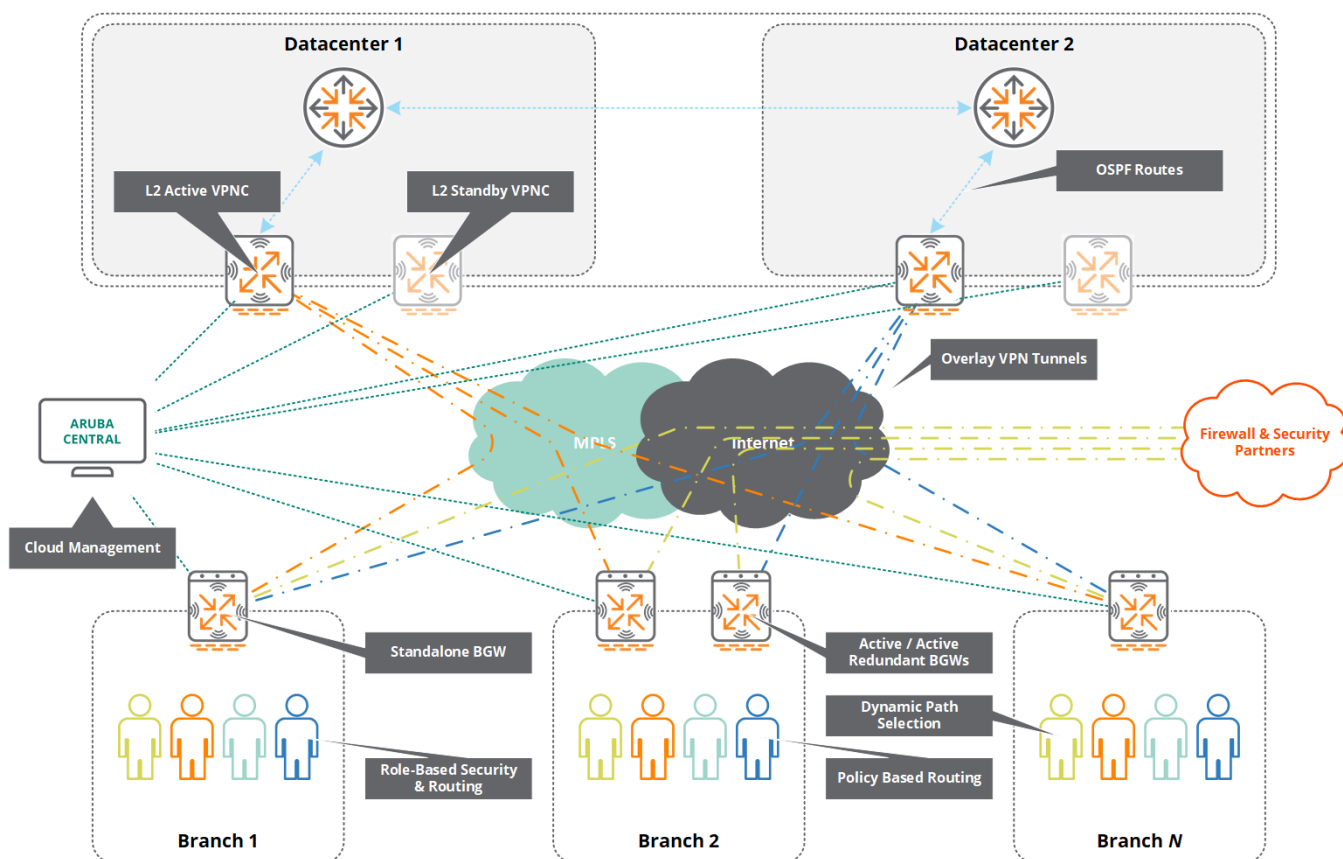


Figure 1-1 Solution Overview

Features

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

- Stateful Firewall** – Introduces context-aware, and role-based data adapted from the Aruba WLAN to dynamically apply policies based on user, device, application, and location to greatly enhance visibility and security.
- Dynamic Segmentation** – With centralized policy control for WAN, WLAN, and LAN, 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 2,600 applications across 21 categories. WebCC provides protection from malicious or unauthorized web URLs.
- Deep Packet Inspection (DPI)** – Monitors application usage and performance while optimizing bandwidth, priority, and network paths in real time, including applications that are encrypted or masquerade as web traffic. DPI is vital to understanding usage patterns that may require changes to network design and capacity.

- **Installer App and Zero-Touch Provisioning (ZTP)** – 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.
- **Adaptive Quality of Service (QoS)** – Monitors the uplink throughput and adjusts QoS policy based on measured throughput.
- **Path Quality Monitoring (PQM)** – The branch gateway can actively and passively monitor established Transmission Control Protocol (TCP) connections for latency, jitter, packet loss, and throughput.
- **Policy-Based Routing (PBR)** – Traffic can be routed across private or public WAN uplinks based on application or user role (e.g. guest or employee), in addition to traditional destination-based routing.
- **Dynamic Path Selection (DPS)** – When multiple WAN links exist, DPS will help choose the best available path for an application based on characteristics like throughput, latency, jitter, and packet loss.
- **WAN Compression** – To improve overall bandwidth efficiency, the branch gateway can enable data 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.
- **Hybrid WAN** – The branch gateway can support multiple uplinks with multiple transport overlays such as Internet broadband, existing MPLS, and cellular connectivity. Traffic destined for the Internet can be routed locally, while traffic destined for the data center can either be routed over MPLS 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, CheckPoint and UCC applications such as Microsoft Skype for Business make extending security and QoS easier and more reliable across the distributed enterprise.

Aruba Central

Aruba Central provides simple, cost-effective, wireless, wired and WAN management for Aruba Instant APs, switches, and gateways. Central also offers value added services such as customized guest access along with detailed location and service assurance analytics. Simple, functional, workflow-driven features simplify traditional management tasks, allowing administrators to focus less on infrastructure and more on value creation.

Device Inventory

Each purchased Aruba device is automatically added to the device inventory in the Central account. The device inventory can include Aruba gateways, Aruba Instant Access Points (IAPs) and ArubaOS switches. A purchased device may be manually added if it does not show up in the device inventory. Aruba Central supports two recommended methods for adding devices into the device inventory:

1. Add a maximum of 32 devices using Media Access Control (MAC) addresses and serial numbers
2. Retrieve devices associated with an Aruba Activate account

Aruba recommends using the cloud activation key to manually add devices into a Central account. This method allows for the manual addition of multiple devices without restrictions.

The screenshot displays the Aruba Central interface for the Device Inventory page. On the left, there is a navigation sidebar with options like Manage Groups, Device Inventory, Key Management, Subscription Assignment, Cluster Management, Labels and Sites, Users & Roles, and Certificates. The main content area is titled 'DEVICE INVENTORY' and features three buttons: 'ADD BY MAC/SN', 'ADD WITH CLOUD ACTIVATION KEY', and 'ADD USING ACTIVATE'. Below these buttons is a table with the following columns: SERIAL #, MAC, TYPE, IP, NAME, MODEL, PART NUMBER, GROUP, and STATUS. The table contains 17 rows of device information, all of which are marked as 'Subscribed'.

SERIAL #	MAC	TYPE	IP	NAME	MODEL	PART NUMBER	GROUP	STATUS
CNF5JSP09N	20:4C:03:21:D8:7C	controller(Gateway)	10.90.170.1	INTROSPECT-GW	7008-RW	JX927A	DEMO-INTROS...	Subscribed
CG0010488	00:0B:86:DD:07:20	controller(Gateway)	10.90.76.1	Aruba7010_DD_07_20	7010-RW	7010-RW	Paul #02	Subscribed
CP0008002	00:0B:86:BE:87:F8	controller(Gateway)	--	7005-RW-00:0B:86:BE...	7005-RW	7005-RW	PGallant	Subscribed
CP0025949	20:4C:03:12:6E:48	controller(Gateway)	--	JW634A-20:4C:03:12:6...	7005-US	JW634A	Amish	Subscribed
CNF4K9T03D	38:17:C3:C8:01:88	iap	--	--	AP-303-US	JZ321A	--	Subscribed
CND4JSW19K	C8:85:AD:C8:65:80	iap	--	--	AP-365-US	JX967A	--	Subscribed
CNC7J0Y249	A8:BD:27:C4:B2:2E	iap	--	--	IAP-335-US	IAP-335-US	default	Subscribed
CT0471732	94:B4:0F:CA:63:BE	iap	--	--	IAP-225-US	JW242A	--	Subscribed
CM0205462	94:B4:0F:CC:02:86	iap	10.70.160.107	94:b4:0fcc:02:86	IAP-205-US	IAP-205-US	TME-Roopesh...	Subscribed
CM0186995	94:B4:0F:CB:72:40	iap	--	--	IAP-205-RW	IAP-205-RW	EMEA-ATM-18	Subscribed
CR0000037	00:0B:86:B4:AE:67	controller(VPNC)	192.168.220.10	vpnc-01.arubatme.com	7030-US	7030-US	CentralPerk#5...	Subscribed
CN71HKZ25D	F4:03:43:07:99:40	switch	10.90.101.2	EMEA-MV-ASW-B01	2930F	JL258A	EMEA-ATM-18	Subscribed
CM0166718	AC:A3:1E:C4:B9:56	iap	--	--	IAP-205-US	IAP-205-US	--	Subscribed
CNCJ0Y1YB	A8:BD:27:C6:13:72	iap	--	--	IAP-335-US	JW825A	--	Subscribed
BB0001750	00:1A:1E:00:62:40	controller(VPNC)	10.67.70.30	EMEA-CSE-VPNC-02	7220-US	7220-US	EMEA-CSE-VPNC	Subscribed
BB0001789	00:1A:1E:00:64:30	controller(VPNC)	10.67.70.20	EMEA-CSE-VPNC-01	7220-US	7220-US	EMEA-CSE-VPNC	Subscribed
CN7344K73RX	E4:03:43:07:99:30	switch	10.70.10.214	Aruba 7030E R/C DnEG	7030E	IL258A	default	Subscribed

Figure 2-1 Device Inventory Page

MAC Address/Serial Number

Aruba Central allows manual addition up to 32 devices into the device inventory by entering MAC Addresses and Serial Numbers. This option can be invoked by navigating to **Global Settings > Device Inventory** in the Central Web-based User Interface (WebUI), selecting the blue **ADD BY MAC/SN** button, and entering the MAC Addresses and Serial Numbers of the devices. Once the 32 device limit has been reached, additional devices will need to be added using the Cloud Activation Key.

ADD DEVICES

Central supports adding up to 32 total devices manually.

SERIAL NUMBER	MAC ADDRESS
SERIAL NUMBER	MAC ADDRESS
SERIAL NUMBER	MAC ADDRESS
SERIAL NUMBER	MAC ADDRESS
SERIAL NUMBER	MAC ADDRESS
+ 5 more rows	
OK	

Figure 2-2 Adding Devices Manually



If the devices are present in Aruba Activate, they must be moved into the “default” Activate folder before they can be added to the Central device inventory.



The MAC Address and Serial Number for each Aruba device can be obtained from either the Aruba device packaging or the sticker on the device itself.

Aruba Activate

Central permits retrieval of multiple devices associated with a separate Activate user account. This option can be invoked by navigating to **Global Settings > Device Inventory** in the Central WebUI, selecting the blue **ADD USING ARUBA ACTIVATE** button, and providing valid Aruba Activate credentials. This is the recommended method when devices need to be added to the Central inventory that exist in an Activate account that is not currently linked to the Central account. When Aruba Activate credentials are used to synchronize the Central account, all devices in the default Activate folder will appear in in the Central device inventory.

ACTIVATE

When you use your Aruba Activate credentials to synchronize your Central account, all devices in your default Activate folder will appear in your Central device inventory.

The screenshot shows a form titled "ACTIVATE". It has two input fields: "ACTIVATE USER NAME" and "PASSWORD". Below the fields are two buttons: a blue "Add" button and a white "Cancel" button with a blue border.

Figure 2-3 Adding Devices via Activate



Adding devices through Activate will only add devices that have been placed into the “default” Activate folder.



Devices can be automatically added to Central through Activate however only one set of Activate credentials may be entered for device importation. Once Activate credentials have been added to Central only devices from that account may be imported using Activate.

Subscription Assignment

Central offers two categories of licenses for IAPs and ArubaOS switches:

- **Device Management** – A device management subscription entitles IAPs and ArubaOS switches to be managed in Aruba Central and enables most functionality. One device management subscription is required for each IAP and ArubaOS Switch.
- **Network Service** – A Network Service subscription permits IAPs to participate in Cloud Guest networks, to be included in Presence Analytics, and to be monitored through Clarity. One subscription is required for each IAP to enable a particular network service.

Aruba’s SD-Branch solution introduces three new subscription licenses for Aruba Central which allow Aruba Gateways to be managed by Central and enable base SD-Branch functionality:

- **Foundation 72XX** – Allows 72XX Series Aruba Gateways to operate as VPNs. One subscription is required for each 72XX Series Aruba Gateway.
- **Foundation 70XX** – Allows 70XX Series Aruba Gateways to operate as Branch Gateways (BGWs) or VPNs. One subscription is required for each 70XX Series Aruba Gateway.
- **Foundation-Base Capacity** – Allows 7005/7008 Aruba Gateways to operate as Branch Gateways (BGWs) supporting a maximum of 75 clients (defined by MAC addresses). One subscription is required for each 7005/7008 Aruba Gateway.

Each Gateway operating as a VPNC or BGW requires a foundation subscription license. Central allows device management and foundation subscription keys to either be automatically or manually assigned. Automatic subscription applies keys on a first come first served basis, while manual subscription requires manual selection and license application for each device.



Regardless of whether or not Auto-Subscribe is enabled, any subscribed device that has an expired subscription will automatically be assigned a new valid subscription (if available). Available subscriptions can be viewed on the **Key Management** page.



When Auto-Subscribe is enabled, each gateway will be automatically assigned a device management license and not a foundation license. If a gateway has been assigned a device management license it will be automatically removed when you assign a foundation license assigned in its place.

Auto Subscription

Aruba Central will automatically assign a device management subscription key to IAPs and ArubaOS Switches in the inventory by default. This feature can be controlled by navigating to **GLOBAL SETTINGS > Subscription Assignment > DEVICE SUBSCRIPTIONS** and toggling the **AUTO SUBSCRIBE DEVICE SUBSCRIPTION KEYS** option. Aruba recommends using auto subscription as a best practice since it eliminates the need to manually assign device management subscription keys to devices.

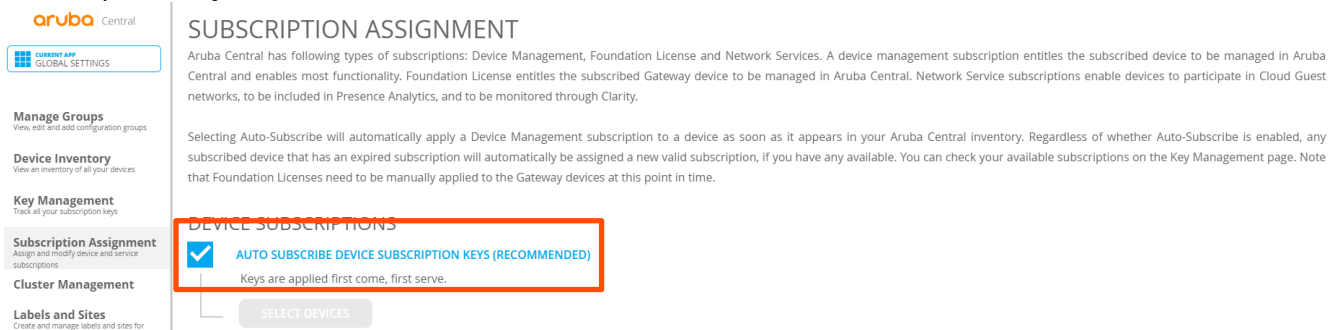


Figure 2-4 Enabling the Auto Subscription Feature

Manual Subscription

If automatic subscription is disabled then device management subscription keys must be manually assigned to each managed device. There are two ways to manually assign device subscriptions for IAPs and ArubaOS Switches:

1. Navigate to **GLOBAL SETTINGS > Subscription Assignment > NETWORK SERVICE SUBSCRIPTIONS** and dragging the new device into the **ALL DEVICES** group.
2. Click the **SELECT DEVICES** button under **GLOBAL SETTINGS > Subscription Assignment > DEVICE SUBSCRIPTIONS** and then select **SUBSCRIBED**.



Device management subscriptions can also be unassigned this way if required.

APPLY SUBSCRIPTIONS

with auto-apply disabled, you'll need to manually select which devices you'll manage in Aruba Central

<input type="checkbox"/> SUBSCRIBED	SERIAL #	MAC	MODEL
<input checked="" type="checkbox"/> YES	CNF4K9T03D	38:17:C3:C8:01:88	AP-303-US
<input checked="" type="checkbox"/> YES	CND4JSW19K	C8:B5:AD:C8:65:80	AP-365-US
<input checked="" type="checkbox"/> YES	CNC7J0Y249	A8:BD:27:C4:B2:2E	IAP-335-US
<input checked="" type="checkbox"/> YES	CT0471732	94:B4:0F:CA:63:BE	IAP-225-US
<input checked="" type="checkbox"/> YES	CM0205462	94:B4:0F:CC:02:86	IAP-205-US
<input checked="" type="checkbox"/> YES	CM0186995	94:B4:0F:CB:72:40	IAP-205-RW
<input checked="" type="checkbox"/> YES	CR0000037	00:0B:86:B4:AE:67	7030-US
<input checked="" type="checkbox"/> YES	CN71HKZ25D	F4:03:43:07:99:40	2930F

0 to be subscribed 0 to be unsubscribed Total number of devices: 114

Figure 2-5 Manual Subscription Assignment Using "Select Devices"

NETWORK SERVICE SUBSCRIPTIONS

DRAG AND DROP DEVICE(S) ONTO A SERVICE TO ASSIGN
 TO SELECT MULTIPLE DEVICES SHIFT+CLICK OR CTRL+CLICK
 TO REMOVE MULTIPLE DEVICES FROM A SERVICE, USE BATCH REMOVE

SUBSCRIPTIONS	DEVICES
ALL DEVICES	114
NO SUBSCRIPTIONS	74
Clarity	33
Cloud Guest	17
Presence Analytics	32
UCC	16

500 TOTAL SUBSCRIPTIONS
388 AVAILABLE

SERIAL #	NAME	TYPE	LOCATION	SERVICES
CNF5JSP09N	INTROSPECT-GW	boc	Waterloo, Canada	0
CG0010488	Aruba7010_DD_07_20	boc	Québec, Canada	0
CP0008002	7005-RW-00:0B:86:BE:87:...	boc	-	0
CP0025949	JW634A-20:4C:03:12:6E:48	boc	-	0
CNF4K9T03D	--	iap	-	0
CND4JSW19K	--	iap	-	0
CNC7J0Y249	--	iap	-	0
CT0471732	--	iap	-	0
CM0205462	94:b4:0f:cc:02:86	iap	Fremont, United States	1 (Clarity)
CM0186995	--	iap	-	0

BATCH REMOVE SUBSCRIPTIONS 114 Device(s)

Figure 2-6 Manual Subscription Assignment Using "Drag and Drop"

Foundation subscriptions can be manually assigned to individual gateways by navigating to **GLOBAL SETTINGS > Subscription Assignment > GATEWAY SUBSCRIPTIONS**, selecting the appropriate device, and choosing either the **Foundation-Base** or **Foundation** subscription from the **ASSIGNMENT** column.

GATEWAY SUBSCRIPTIONS

DEVICE ASSIGNMENT

ASSIGN SUBSCRIPTIONS TO YOUR GATEWAYS HERE. SELECT MULTIPLE GATEWAYS TO BATCH ASSIGN SUBSCRIPTIONS. BASE CAPACITY SUBSCRIPTIONS MAY ONLY BE APPLIED TO MODEL 7005 GATEWAYS.

ASSIGNMENT	SERIAL NUMBER	MAC ADDR	MODEL	GROUP
UNASSIGNED	CV0009902	00:1A:1E:03:71:78	7210-US	
UNASSIGNED	CG0002796	00:0B:86:9A:0B:D7	7010-RW	
UNASSIGNED	CG0002698	00:0B:86:9A:1A:D7	7010-RW	
UNASSIGNED	CP0015869	00:0B:86:BF:6F:E8	7005-RW	
UNASSIGNED	CG0003032	00:0B:86:9A:79:B7	7010-RW	
UNASSIGNED	CG0010382	00:0B:86:DC:F8:00	7010-RW	
UNASSIGNED	BA0001388	00:1A:1E:00:21:80	7210-US	
UNASSIGNED	CZ0000060	00:0B:86:8B:B7:07	7024-US	

Figure 2-7 Manual Foundation Subscription Assignment for Gateways

Foundation-Base or Foundation subscriptions can be optionally assigned to multiple Aruba Gateways by holding down the Control key, clicking on two or more Aruba Gateways, and then selecting **BATCH ASSIGNMENT**.

GATEWAY SUBSCRIPTIONS

DEVICE ASSIGNMENT

ASSIGN SUBSCRIPTIONS TO YOUR GATEWAYS HERE. SELECT MULTIPLE GATEWAYS TO BATCH ASSIGN SUBSCRIPTIONS. BASE CAPACITY SUBSCRIPTIONS MAY ONLY BE APPLIED TO MODEL 7005 GATEWAYS.

ASSIGNMENT	SERIAL NUMBER	MAC ADDR	MODEL	GROUP
UNASSIGNED	CNF5JP09N	20:4C:03:21:D8:7C	7008-RW	DEMO-INTROSPECT
UNASSIGNED	CG0010488	00:0B:86:DD:07:20	7010-RW	Paul #02
UNASSIGNED	CP0008002	00:0B:86:BE:87:F8	7005-RW	PGallant
UNASSIGNED	CP0025949	20:4C:03:12:6E:A8	7005-US	Amish
UNASSIGNED	CR0000037	00:0B:86:84:AE:67	7030-US	CentralPerk#523-SD-WAN-DC
UNASSIGNED	BB0001750	00:1A:1E:00:62:40	7220-US	EMEA-CSE-VPNC
UNASSIGNED	BB0001789	00:1A:1E:00:64:30	7220-US	EMEA-CSE-VPNC
UNASSIGNED	CR0010661	00:0B:86:87:09:37	7030-RW	CentralPerk#5150-Branch
UNASSIGNED	CP0028987	20:4C:03:19:D0:14	7005-RW	

BATCH ASSIGNMENT

29 Devices
0 Remaining Subscriptions for Foundation-Base Capacity
0 Remaining Subscriptions for Foundation

Figure 2-8 Gateway Foundation Subscription Batch Assignment Option

Organization

The fundamental aggregation and grouping elements in Aruba Central are as follows:

- Groups
- Devices
- Sites
- Labels

The filter in Central determines the scope of devices and users that are selected in each Central application. The filter can be used to select a group, device, site, or label.

The **Monitoring and Reports** application is opened by default with the **All Groups** filter selected upon initially connecting to Central. The **All Groups** filter scope includes all the devices and users in the network. The scope can be further refined within an application by selecting a group, device, site, or label (Figure 2-9).

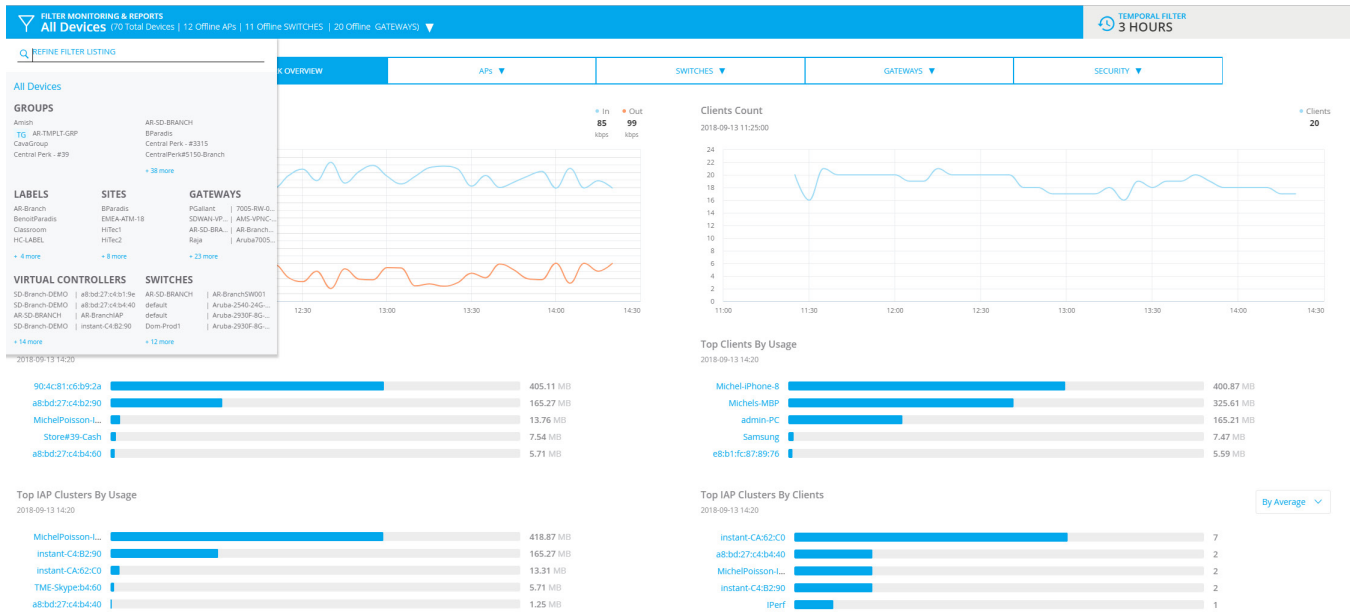


Figure 2-9 Monitoring and Reports Filter

There are some restrictions as to which filters are display and can be selected per application:

- **Monitoring & Reports** – Supports the selection of a Device, Group, Site or Label
- **Wireless Management** – Supports the selection of a Device or Group
- **Wired Management** – Supports the selection of a Device or Group
- **Gateway Management** – Supports the selection of a Device or Group
- **Maintenance** – Supports the selection of a Device, Group or Label
- **Install Manager** – Supports the selection of a Site

Configuration tasks can usually only be performed against groups or devices meaning that a group or device can only be selected when using the wired, wireless, or gateway management applications. Monitoring, reporting, and maintenance can be performed against groups, devices, or labels. Sites are specific to SD-Branch and can only be selected in the **Monitoring & Reports** and **Install Manager** applications.

Groups

Central supports allocating devices to groups for scalable configuration, monitoring, and maintenance. A group in Central is a primary configuration element that acts as a container. Groups should be thought of as a superset of one or several devices that share common configuration parameters.

Device groups provide the following functions and benefits:

- **Combine different types of devices under a common group** – E.g., a single group may be created for all branches that includes gateways, IAPs, and switches. Central allows configuration management of these devices in separate applications (i.e. Gateway Management, Wireless Management, and Wired Management) within the group.
- **Assign multiple devices to a single group** – E.g., a group could consist of multiple BGWs of the same model sharing the same switchport, VLAN, WAN, and VPN configuration settings.
- **Manage common configuration settings of devices at the group level** – Quickly modify or push new configuration changes across multiple devices. E.g., deploying a new WAN policy to support a new application across all BGWs.

Each managed device in Aruba Central must be assigned to a group. Devices may be assigned to groups using the **GLOBAL SETTINGS** application in the **Device Inventory** or **Manage Groups** pages.

Group Operations

Central allows various functions to be performed at the All Groups or individual group levels. The following list shows the most common tasks performed at a group level:

- **Configuration** – Add, modify, or delete configuration parameters for devices in a group
- **User Management** – Control user access to device groups and group operations based the type of user role
- **Device Status and Health Monitoring** – View device health and performance for devices in a specific group
- **Report Generation** – Run reports per group
- **Alerts and Notifications** – View and configure notification settings per group
- **Firmware Upgrades** – Enforce firmware compliance across all devices in a group

Tasks that are not performed at a group level include device-specific configurations such as assigning static IP addresses and hostnames. Device-specific parameters may be learned by Central upon onboarding a new gateway if manual provisioning is employed, or can be provisioned prior to adding a gateway using bulk provisioning.

VPNC Groups

VPNC groups include one or more Aruba Gateways operating as VPN Concentrators. The group type must be set to **VPNC** the first time the group is selected in the **Gateway Management** application (Figure 2-10). Groups marked as VPNC may only contain VPNCs and must not include gateways deployed in branches.

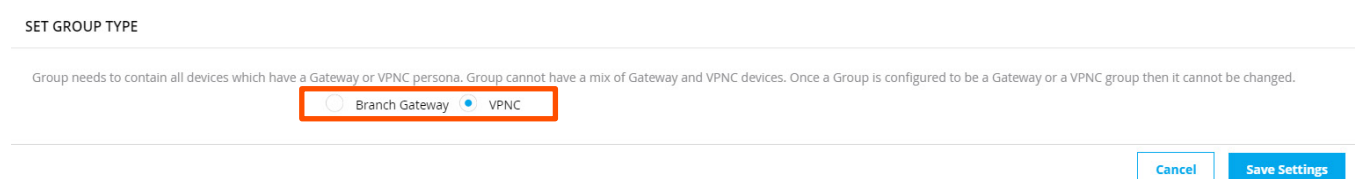


Figure 2-10 Designating a VPNC Group

VPNC groups include one or more gateways operating as VPNCs. The group type must be designated as a **VPNC** the first time it is selected in the **Gateway Management** application (Figure 2-11). Groups marked as VPNC can only contain VPNCs and must not include gateways deployed in branches.

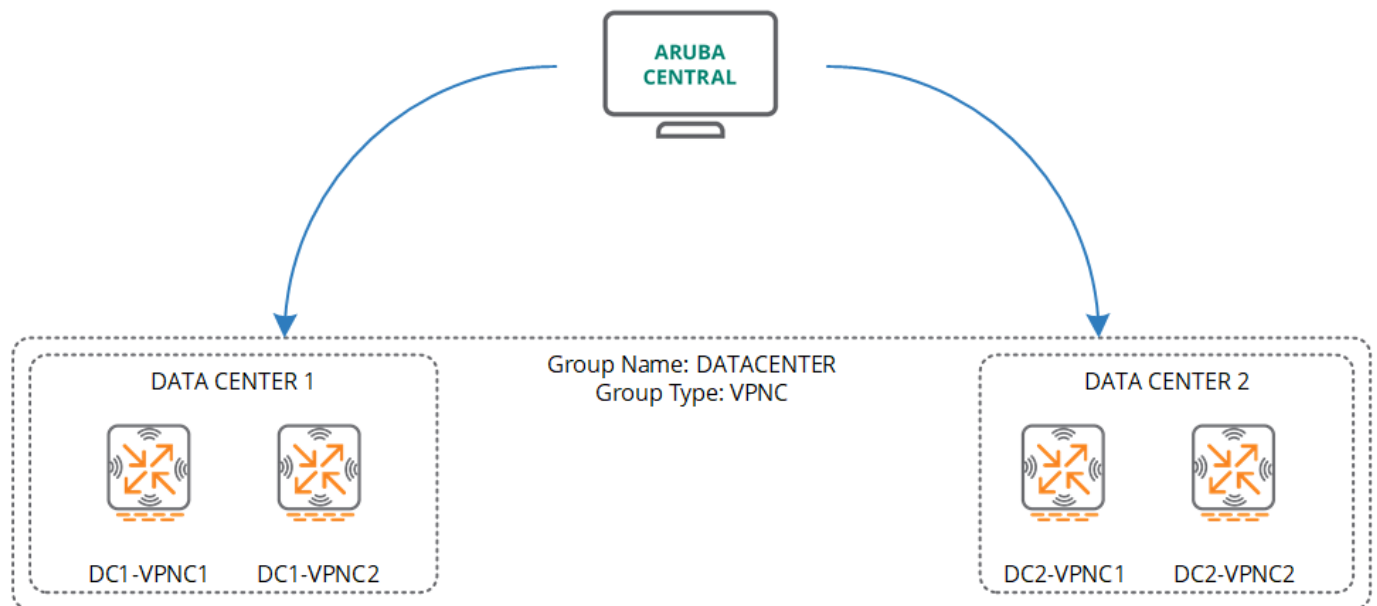


Figure 2-11 VPNC Group Sample Architecture

Branch Groups

Branch groups can include gateways, switches and/or IAPs. The group type must be designated **Branch Gateway** the first time it is selected in the **Gateway Management** application (Figure 2-12). Groups marked as **Branch Gateway** must not include gateways operating as VPNs.

SET GROUP TYPE

Group needs to contain all devices which have a Gateway or VPN persona. Group cannot have a mix of Gateway and VPN devices. Once a Group is configured to be a Gateway or a VPN group then it cannot be changed.

Branch Gateway VPN

Cancel Save Settings

Figure 2-12 Designating a Branch Group

Determining the number of groups requiring implementation for branch sites can be challenging. There is no right or wrong answer and the approach taken will be specific to each organization's requirements and business needs.

Aruba recommends creating separate groups for different types of branch sites in the following scenarios:

1. The deployment supports branch sites with unique configuration needs. E.g., a retailer with stores consisting of multiple brands where each brand requires different Service Set Identifiers (SSIDs), Roles, and VLAN assignments.
2. The deployment includes small and medium branches where each branch implements different gateway and switch models. E.g., small branches which include Aruba 7005 gateways with 24-port Switches while the medium branches include Aruba 7008 gateways and 48-port Switches.
3. The deployment includes branch sites across multiple regions and time zones. Separation may be helpful to accommodate different maintenance windows in each region.
4. An organization wishes to reduce the risk when new configuration changes are applied. E.g., a deployment includes test sites where new configurations are tested and vetted prior to being rolled out across all the branch sites.

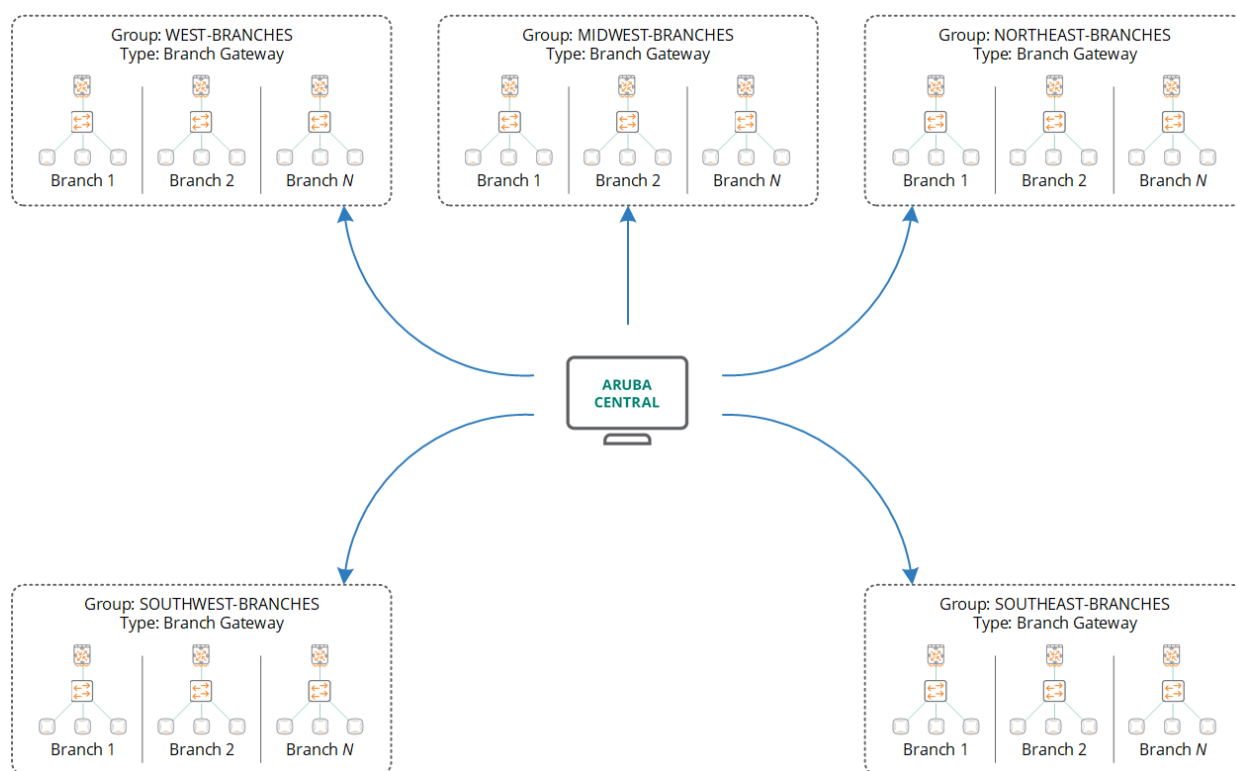


Figure 2-13 Branch Group Sample Architecture

If a deployment is relatively small and the branches consist of common hardware and configurations, then Aruba recommends implementing a single group to configure, manage, and monitor gateways, switches, and IAPs across all branch sites. Additional groups may be created and branch devices may be moved in the future as the number of branches increase or business needs evolve.

Assigning Devices to Groups

Aruba Central has two methods for assigning new devices into groups:

1. Device Inventory Page
2. Manage Groups Page

Device Inventory

New devices may be assigned to a group and existing devices can be moved to a new group under **Device Inventory** in the **Global Settings** application. New devices can be assigned to a group by selecting one or more devices in the table then selecting **Assign Group**. Multiple devices may be selected in the table by holding the Shift or Control keys while selecting devices.

1. Select the device(s) which need to be assigned or need to be reassigned to a new group.
2. Click **Assign Group**. This will display the **Assign a Group to the Selected Devices** window.

DEVICE INVENTORY

SERIAL #	MAC	TYPE	IP	NAME	MODEL	PART NUMBER	GROUP	STATUS
CNF55P09M	204C:0321:D8:7C	controller(Gateway)	10.90.170.1	INTROSPECT-GW	7008-RW	J9327A	DEMO-INTROSPECT	Subscribed
CO0010488	00:0B:86:0D:07:20	controller(Gateway)	10.90.76.1	Aruba7010_DD_07_20	7010-RW	7010-RW	Paul #02	Subscribed
CP0008002	00:0B:86:BE:87:F8	controller(Gateway)	--	7005-RW-00:0B:86:BE:87:F8	7005-RW	7005-RW	PGallant	Subscribed
CP0025949	204C:0312:6E:48	controller(Gateway)	--	JW634A:204C:0312:6E:48	7005-US	JW634A	Amish	Subscribed
CNF4K91030	38:17:C3:C8:01:88	lap	--	--	AF-3003-US	J2321A	--	Subscribed
CND49W179K	CB:85:AD:CB:85:89	lap	--	--	AP-360-US	J9076A	--	Subscribed
CNC70Y049	A8:8D:27:C4:82:2E	lap	--	--	IAP-335-US	IAP-335-US	default	Subscribed
CT0471732	94:84:0F:CA:63:BE	lap	--	--	IAP-225-US	JW424A	--	Subscribed
CM0205462	94:84:0F:CC:02:86	lap	10.70.160.107	94b4d0fcc0286	IAP-205-US	IAP-205-US	TME-Roopesh-Skype	Subscribed
CM0186995	94:84:0F:CB:72:40	lap	--	--	IAP-205-RW	IAP-205-RW	EMEA-ATM-18	Subscribed
CR0000237	00:0B:86:8A:AE:67	controller(VPN)	192.168.220.10	vprc-01.arubatme.com	7030-US	7030-US	CentralPerk#523-SD-WANL...	Subscribed
CN71HK22SD	F4:03:43:07:99:40	switch	10.90.101.2	EMEA-MV-ASW-801	2930F	JL258A	EMEA-ATM-18	Subscribed
CM0166718	ACA3:1E:C4:89:56	lap	--	--	IAP-205-US	IAP-205-US	--	Subscribed
CNC9J0Y1YB	A8:8D:27:C6:13:72	lap	--	--	IAP-335-US	JW825A	--	Subscribed
BB0001750	00:1A:1E:00:62:40	controller(VPN)	10.67.70.30	EMEA-CSE-VPN-02	7220-US	7220-US	EMEA-CSE-VPN	Subscribed
BB0001789	00:1A:1E:00:64:30	controller(VPN)	10.67.70.20	EMEA-CSE-VPN-01	7220-US	7220-US	EMEA-CSE-VPN	Subscribed
CN71HK21EX	F4:03:43:07:87:30	switch	10.70.18.214	Aruba-2930F-BG-PoEP-25FPP	2930F	JL258A	default	Subscribed
CN730YLWFP	80:5A:DA:1E:87:10	switch	10.90.33.7	SD-WAN-2530	2530YB	JL070A	SD-Branch-DEMO	Subscribed
CR0010661	00:0B:86:87:09:37	controller(Gateway)	10.1.90.50	Branch-5150	7030-RW	7030-RW	CentralPerk#5150-Branch	Subscribed
CNK02887	204C:0319:D6:14	controller(Gateway)	--	--	7005-RW	JW633A	--	Subscribed
CND9581M	2046:CD:0C:1F:2	lap	10.90.58.226	Branch#P001	IAP-305-RW	J9045A	AR-SD-BRANCH	Subscribed
CNC69P018	204C:030A:5E:90	controller(Gateway)	10.90.255.240	TME_OAK_7008	7008-US	J9028A	SD-Branch-DEMO	Subscribed
CP0007868	00:0B:86:BE:83:CB	controller(Gateway)	10.90.101.1	Aruba7005-MV	7005-RW	7005-RW	EMEA-ATM-18	Subscribed
CR0012735	204C:0306:ED:F0	controller(Gateway)	10.76.135.66	Peacock-Workbench	7030-US	7030-US	Peacock-WorkBench	Subscribed
CNC69P003	204C:030A:83:20	controller(Gateway)	192.168.10.1	Branch-1-7008-8320	7008-US	J9028A	unprovisioned	Subscribed
CP0032000	204C:031A:34:3C	controller(Gateway)	172.16.5.1	Peacock-Branch-05	7005-RW	JW633A	CentralPerk#523-SD-WANL...	Subscribed

ASSIGN GROUP

Figure 2-14 Assigning Devices to Groups Using the Device Inventory Page

- Select the name of the group where the selected devices need to be assigned. Click **Assign Device(s)**.

ASSIGN A GROUP TO THE SELECTED DEVICE ✕

GROUP NAME

default

Central Perk - #523

Central Perk - #3315

Central Perk - #39

Paul #01

Paul #02

Dom-Prod1

TG TME Demo Switch Stack

TG TME Demo Switch 5400

Doms-AviGS

MichelPoisson

Assign Device(s)

Cancel

Figure 2-15 Assigning Devices to Groups Using the Device Inventory Page (Cont.)

Manage Groups Page

Devices may be moved to a new group by navigating to **Global Settings > Manage Groups**. The table on the left side of the page provides a list of groups while the table on the right displays the device membership for the selected group. To move devices into a new group in the **Managed Groups** page:

1. Click on the group name where the device(s) that need to be moved reside.
2. Select the device(s) the need to be moved. Note that multiple devices may be selected by holding the Shift or Control keys.
3. Drag then drop the selected device(s) to the new group.

GROUPS
A group is the primary configuration element in Aruba Central. Aruba IAPs are automatically organized into clusters, which allows IAPs to work together as a virtual WLAN controller. Group policies will be automatically applied as you add switches and IAP clusters to a group.

MANAGE GROUPS
DRAG AND DROP CLUSTERS AND SWITCHES BETWEEN GROUPS
TO SELECT MULTIPLE DEVICES SHIFT+CLICK OR CTRL+CLICK

GROUP NAME	DEVICES
ALL CONNECTED DEVICES	61
UNASSIGNED DEVICES	3
Amish	1
AR-SD-BRANCH	3
TG AR-TMPLT-GRP	0
BParadis	1
CavaGroup	0
Central Perk - #3315	3
Central Perk - #29	1
CentralPerk#5150-Branch	1
CentralPerk#5150-DC-01	2
Central Perk - #523	4
CentralPerk#523-SD-WAN-Branch	3
CentralPerk#523-SD-WAN-DC	3
default	5
DEMO-INTROSPECT	1
Dom-Prod1	1
Doms-AVIGS	1
Elie-Group	0
EMEA-ATM-18	2
EMEA-CSE-Branch	0
EMEA-CSE-VPNC	2
EMEA-MV-ASW	0
EMEA-MV-BGW	0
Fuzzy's	0
TG HOLD	1

NAME	LOCATION	TYPE	SERIAL #	MAC ADDR.
Aruba-2540-24G-45FPP	Fremont,United States	Aruba Switch	CHWA1YH032	94:1B:82:55:e1:c0
Aruba-2930F-8G-PoP-254FPP	San Francisco,United States	Aruba Switch	CH71HK21BK	f43343378730
SetMeUp-18F554	San Jose,United States	IAP	CHD0K2958	20:4c:02:18:f5:54
SetMeUp-C730FE	Waterloo,Canada	IAP	CHCM0T0C3	34:fc:b9:c7:90:fe
SetMeUp-CB-2100	Minooka,United States	IAP	CHCV55246	34:fc:b9:c7:90:fe

Figure 2-16 Assigning Devices to Groups Using the Manage Groups Page

Group Requirements and Recommendations

The number of groups that are defined in Aruba Central will be specific to each organization and deployment. At a minimum, Aruba Central requires one group to be defined for VPNCs and one group to be defined for BGWs. The role of each group (Branch or VPNC) is determined when devices are initially assigned to their groups.

The number of groups that defined in Central will influence how the Aruba devices are configured, managed, and monitored. Considerations that will influence those decisions include:

1. The number of data centers that will include VPNCs
2. The number of branches in the deployment and their location
3. The different branch deployment models requiring support

Device Level Configuration

Aruba Central provides two levels of configuration hierarchy. A device's final configuration is a result of configuration that is applied at the device level along with configuration that is applied at a group level. Most configuration parameters performed at the device level will override the configuration performed at the group level. The exceptions to that rule are reordering of entries in ACLs or the removal of group level configurations. If the same configuration is performed at both device and group levels, the configuration performed at the device level will be applied. Since configurations can be applied at two levels, some best practices need to be defined. Aruba recommends performing the bulk of the configuration using groups unless specific device level configuration is required. Common configuration parameters which will be applied to the device level include:

1. Hostnames
2. VLAN or Loopback Interfaces with Static Internet Protocol Version 4 (IPv4) Addresses
3. Local DHCP Pools
4. OSPF Router IDs
5. VRRP Priorities
6. Redundant Gateway Peer Configuration
7. Marking ports as WAN in active-active redundant gateway deployments
8. Manual override of firewall aliases (if more scalable mechanisms can't be used)
9. Uplink configuration inherited from Zero Touch Provisioning
10. Configuration defined using the Full-Setup
11. Bulk configuration imported from the CSV

Each device in Central will have some device level configuration. The amount of device level configuration that is learned by Central is dependent on how the device is provisioned. Usually, each configuration parameter defined during the full-setup for a device or each field that is populated in the bulk provisioning CSV will be added as a device level configuration parameter. There are also some best practices that should be followed when determining which configuration parameters to apply at the group level vs. the device level. Configuration parameters that should never be applied to a group include device static IP addresses, loopback interfaces, OSPF router IDs, and local dynamic host configuration protocol (DHCP) pools. These parameters are device specific and may result in unpredictable behavior or un-reachable devices.

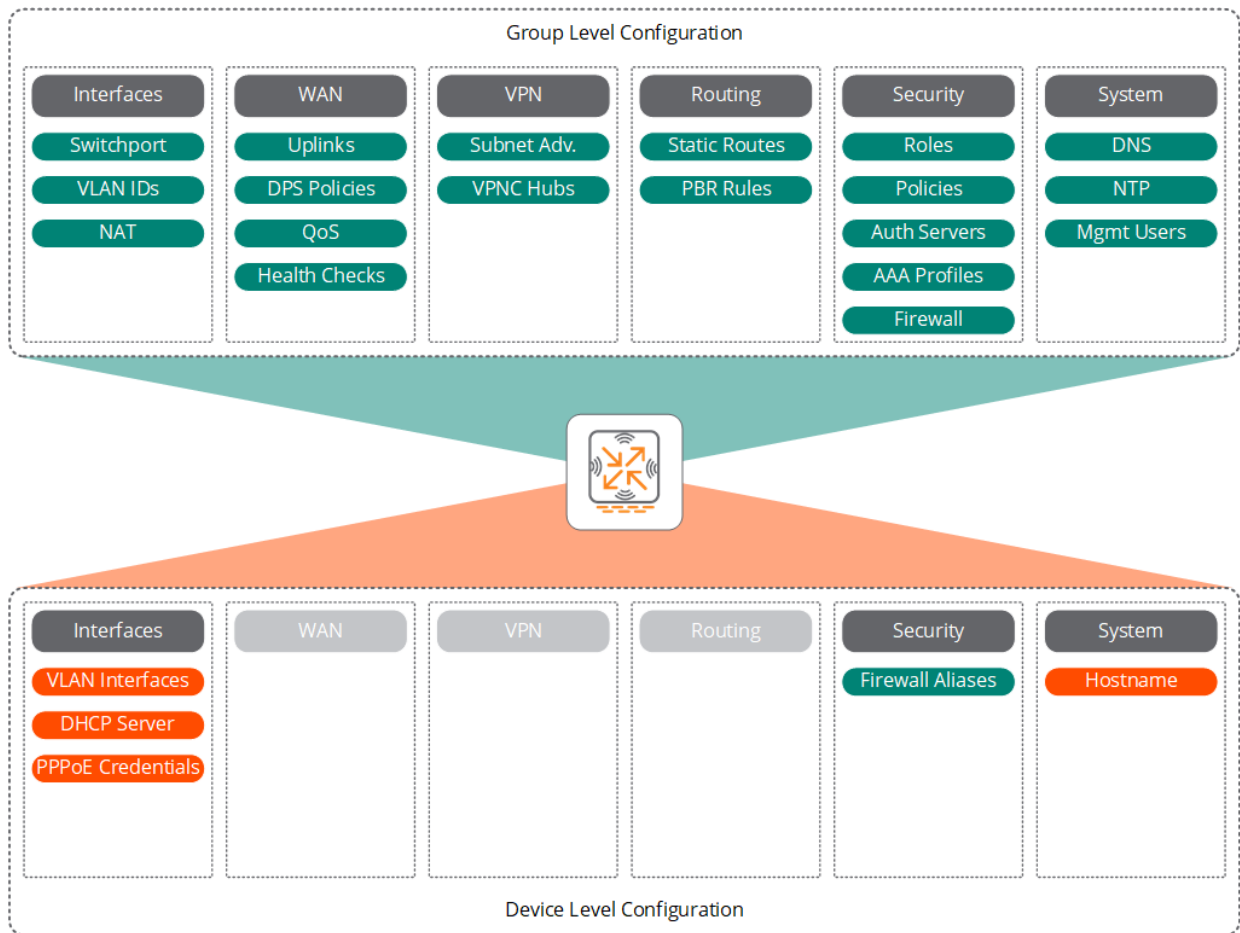


Figure 2-17 Device Level vs. Group Level Configuration

Labels

Labels provide an additional useful grouping method in Aruba Central to further simplify the monitoring, maintenance, and reporting of branch devices and users. Labels provide an orthogonal way of organizing devices for administrative purposes without impacting the configuration hierarchy.

Each Aruba device in Central can be assigned one or more labels. This could be a single label to indicate a region name or multiple labels to indicate city, state, country or even service provider. A label may then be selected as a filter in the **Monitoring & Reports** and **Maintenance** applications to select a specific target group of devices. E.g., selecting a city would allow an administrator to monitor and generate reports for all the clients and devices across all sites assigned to the selected city.

The number of labels defined and assigned to devices will be specific to an organization's monitoring, maintenance, and reporting needs.



Aruba Central allows a maximum of 5 labels to be assigned per device.

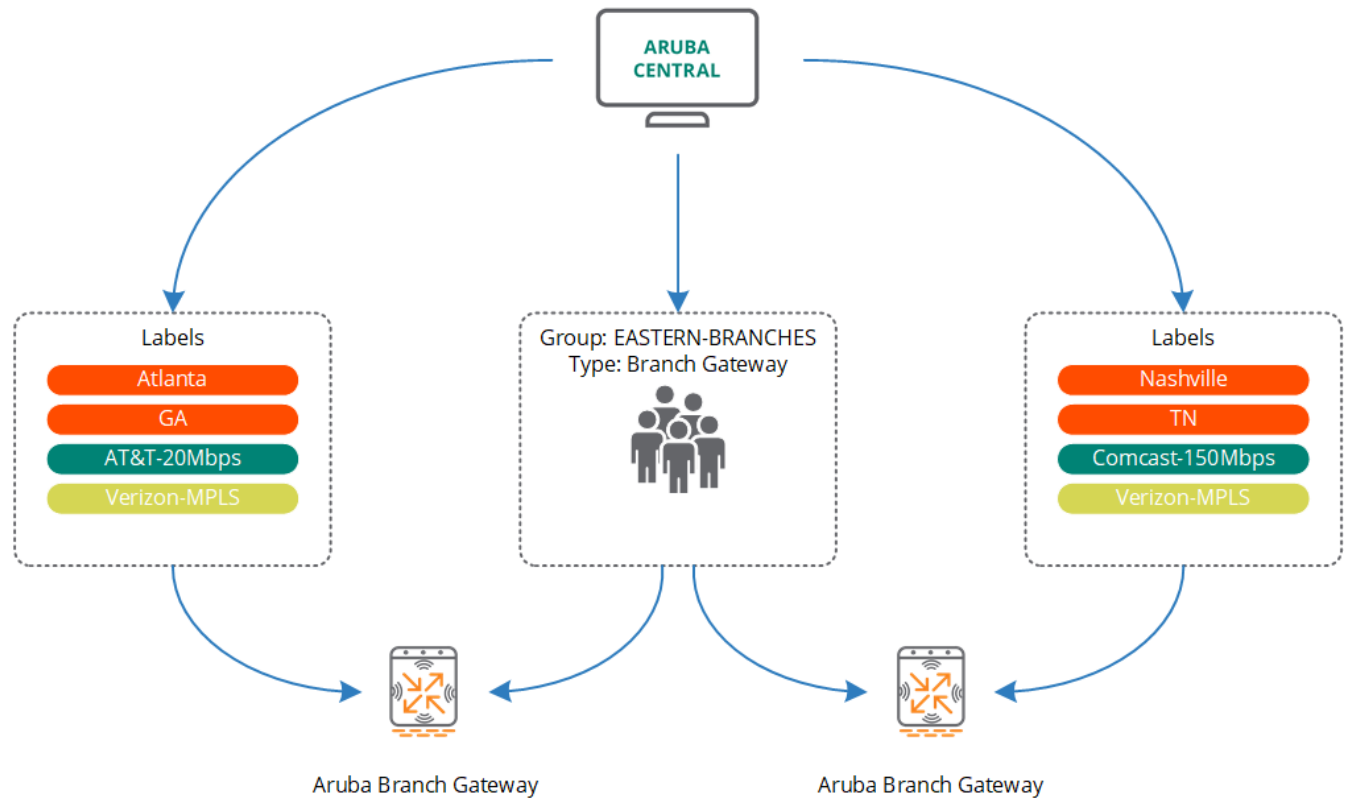


Figure 2-18 Label Usage Example

It is important to note that labels are not used for device configuration. The configuration of devices will be handled using the group-device hierarchy. Labels are primarily used as a mechanism to simplify monitoring, maintenance, and reporting tasks. Effectively, labels provide a tool that makes it easier to keep track of data center and branch devices without the need for creating separate groups.

Labels are created and managed by the following process:

1. Navigate to **Global Settings > Labels and Sites**
2. Ensure that the blue slider in the upper right hand corner of the page is moved over to Labels
3. Click the **Add Label** button in the bottom left hand corner

Each label must include a unique name. Devices are assigned to labels by dragging and dropping one or more devices from the list on the right to the respective label on the left. Multiple devices can be selected at the same time by holding the Shift or Control keys while selecting the devices.

LABELS AND SITES

Labels are logical sets of devices which can be used for a variety of monitoring and reporting purposes. Each device can be associated with up to five labels, and a label can apply to as many devices as you want. Sites allow you to group devices based on the location context

MANAGE LABELS

DRAG AND DROP DEVICE(S) ONTO A LABEL TO ASSIGN
TO SELECT MULTIPLE DEVICES SHIFT+CLICK OR CTRL+CLICK
TO REMOVE MULTIPLE DEVICES FROM A LABEL, USE "BATCH REMOVE"

▼ LABEL NAME	DEVICE COUNT
ALL DEVICES	84
UNASSIGNED	78
Label	0
Label	1
Label	2
Label	1
Label	1
Label	1
Label	1

7 Labels

Labels Sites

▼ NAME	GROUP	▼ TYPE	LABELS
Label	Label	CONTROLLER	0
Label	Label	CONTROLLER	0
Label	Label	CONTROLLER	0
Label	Label	CONTROLLER	0
Label	Label	SWITCH	0
Label	Label	IAP	2
Label	Label	CONTROLLER	0
Label	Label	CONTROLLER	0
Label	Label	CONTROLLER	0
Label	Label	CONTROLLER	0
Label	Label	CONTROLLER	0

84 Device(s)

Figure 2-19 Label Management

Sites

Sites are a specific type of label in Central that groups and organizes devices by their location. Each site can contain Aruba Gateways, Switches, and IAPs. Aruba recommends that creating one site for each branch location. Each site includes the name and physical address of the site, and is used by Central to provide monitoring, maintenance and reporting at a branch level. Sites are also used by the Install Manager application for assigning installers and monitoring the status of each branch sites installation.

Sites are created and managed by navigating to **Global Settings > Labels and Sites**. Toggle the blue slider in the upper right hand corner of the page from **Labels** to **Sites** to display the Site options.

Sites can be manually added one at a time or bulk added using a CSV file. The bulk upload option allows a maximum of 1,000 sites to be uploaded at a time. A template file can be downloaded by selecting the **Bulk Upload** icon.

LABELS AND SITES

Labels are logical sets of devices which can be used for a variety of monitoring and reporting purposes. Each device can be associated with up to five labels, and a label can apply to as many devices as you want. Sites allow you to group devices based on the location context.

MANAGE SITES

DRAG AND DROP DEVICES TO ADD TO A SITE
TO SELECT MULTIPLE DEVICES SHIFT+CLICK OR CTRL+CLICK

[CONVERT LABELS TO SITES](#) OR [CREATE SITES USING EXISTING GROUPS](#)

SITE NAME	ADDRESS	DEVICE COUNT
ALL DEVICES		84
UNASSIGNED		83
TENNESSEE-OFFICE	1001 Nashville, TN	1

NAME	GROUP	TYPE
TENNESSEE-OFFICE	TENNESSEE-OFFICE	CONTROLLER
ALPHA-APAC-001	ALPHA-APAC-001	CONTROLLER
ALPHA-APAC-002	ALPHA-APAC-002	CONTROLLER
ALPHA-APAC-003	ALPHA-APAC-003	CONTROLLER
ALPHA-APAC-004	ALPHA-APAC-004	CONTROLLER
ALPHA-APAC-005	ALPHA-APAC-005	CONTROLLER
ALPHA-APAC-006	ALPHA-APAC-006	CONTROLLER
ALPHA-APAC-007	ALPHA-APAC-007	CONTROLLER
ALPHA-APAC-008	ALPHA-APAC-008	CONTROLLER
ALPHA-APAC-009	ALPHA-APAC-009	CONTROLLER
ALPHA-APAC-010	ALPHA-APAC-010	CONTROLLER
ALPHA-APAC-011	ALPHA-APAC-011	CONTROLLER
ALPHA-APAC-012	ALPHA-APAC-012	CONTROLLER
ALPHA-APAC-013	ALPHA-APAC-013	CONTROLLER
ALPHA-APAC-014	ALPHA-APAC-014	CONTROLLER
ALPHA-APAC-015	ALPHA-APAC-015	CONTROLLER
ALPHA-APAC-016	ALPHA-APAC-016	CONTROLLER
ALPHA-APAC-017	ALPHA-APAC-017	CONTROLLER
ALPHA-APAC-018	ALPHA-APAC-018	CONTROLLER
ALPHA-APAC-019	ALPHA-APAC-019	CONTROLLER
ALPHA-APAC-020	ALPHA-APAC-020	CONTROLLER
ALPHA-APAC-021	ALPHA-APAC-021	CONTROLLER
ALPHA-APAC-022	ALPHA-APAC-022	CONTROLLER
ALPHA-APAC-023	ALPHA-APAC-023	CONTROLLER
ALPHA-APAC-024	ALPHA-APAC-024	CONTROLLER
ALPHA-APAC-025	ALPHA-APAC-025	CONTROLLER
ALPHA-APAC-026	ALPHA-APAC-026	CONTROLLER
ALPHA-APAC-027	ALPHA-APAC-027	CONTROLLER
ALPHA-APAC-028	ALPHA-APAC-028	CONTROLLER
ALPHA-APAC-029	ALPHA-APAC-029	CONTROLLER
ALPHA-APAC-030	ALPHA-APAC-030	CONTROLLER
ALPHA-APAC-031	ALPHA-APAC-031	CONTROLLER
ALPHA-APAC-032	ALPHA-APAC-032	CONTROLLER
ALPHA-APAC-033	ALPHA-APAC-033	CONTROLLER
ALPHA-APAC-034	ALPHA-APAC-034	CONTROLLER
ALPHA-APAC-035	ALPHA-APAC-035	CONTROLLER
ALPHA-APAC-036	ALPHA-APAC-036	CONTROLLER
ALPHA-APAC-037	ALPHA-APAC-037	CONTROLLER
ALPHA-APAC-038	ALPHA-APAC-038	CONTROLLER
ALPHA-APAC-039	ALPHA-APAC-039	CONTROLLER
ALPHA-APAC-040	ALPHA-APAC-040	CONTROLLER
ALPHA-APAC-041	ALPHA-APAC-041	CONTROLLER
ALPHA-APAC-042	ALPHA-APAC-042	CONTROLLER
ALPHA-APAC-043	ALPHA-APAC-043	CONTROLLER
ALPHA-APAC-044	ALPHA-APAC-044	CONTROLLER
ALPHA-APAC-045	ALPHA-APAC-045	CONTROLLER
ALPHA-APAC-046	ALPHA-APAC-046	CONTROLLER
ALPHA-APAC-047	ALPHA-APAC-047	CONTROLLER
ALPHA-APAC-048	ALPHA-APAC-048	CONTROLLER
ALPHA-APAC-049	ALPHA-APAC-049	CONTROLLER
ALPHA-APAC-050	ALPHA-APAC-050	CONTROLLER
ALPHA-APAC-051	ALPHA-APAC-051	CONTROLLER
ALPHA-APAC-052	ALPHA-APAC-052	CONTROLLER
ALPHA-APAC-053	ALPHA-APAC-053	CONTROLLER
ALPHA-APAC-054	ALPHA-APAC-054	CONTROLLER
ALPHA-APAC-055	ALPHA-APAC-055	CONTROLLER
ALPHA-APAC-056	ALPHA-APAC-056	CONTROLLER
ALPHA-APAC-057	ALPHA-APAC-057	CONTROLLER
ALPHA-APAC-058	ALPHA-APAC-058	CONTROLLER
ALPHA-APAC-059	ALPHA-APAC-059	CONTROLLER
ALPHA-APAC-060	ALPHA-APAC-060	CONTROLLER
ALPHA-APAC-061	ALPHA-APAC-061	CONTROLLER
ALPHA-APAC-062	ALPHA-APAC-062	CONTROLLER
ALPHA-APAC-063	ALPHA-APAC-063	CONTROLLER
ALPHA-APAC-064	ALPHA-APAC-064	CONTROLLER
ALPHA-APAC-065	ALPHA-APAC-065	CONTROLLER
ALPHA-APAC-066	ALPHA-APAC-066	CONTROLLER
ALPHA-APAC-067	ALPHA-APAC-067	CONTROLLER
ALPHA-APAC-068	ALPHA-APAC-068	CONTROLLER
ALPHA-APAC-069	ALPHA-APAC-069	CONTROLLER
ALPHA-APAC-070	ALPHA-APAC-070	CONTROLLER
ALPHA-APAC-071	ALPHA-APAC-071	CONTROLLER
ALPHA-APAC-072	ALPHA-APAC-072	CONTROLLER
ALPHA-APAC-073	ALPHA-APAC-073	CONTROLLER
ALPHA-APAC-074	ALPHA-APAC-074	CONTROLLER
ALPHA-APAC-075	ALPHA-APAC-075	CONTROLLER
ALPHA-APAC-076	ALPHA-APAC-076	CONTROLLER
ALPHA-APAC-077	ALPHA-APAC-077	CONTROLLER
ALPHA-APAC-078	ALPHA-APAC-078	CONTROLLER
ALPHA-APAC-079	ALPHA-APAC-079	CONTROLLER
ALPHA-APAC-080	ALPHA-APAC-080	CONTROLLER
ALPHA-APAC-081	ALPHA-APAC-081	CONTROLLER
ALPHA-APAC-082	ALPHA-APAC-082	CONTROLLER
ALPHA-APAC-083	ALPHA-APAC-083	CONTROLLER
ALPHA-APAC-084	ALPHA-APAC-084	CONTROLLER
ALPHA-APAC-085	ALPHA-APAC-085	CONTROLLER
ALPHA-APAC-086	ALPHA-APAC-086	CONTROLLER
ALPHA-APAC-087	ALPHA-APAC-087	CONTROLLER
ALPHA-APAC-088	ALPHA-APAC-088	CONTROLLER
ALPHA-APAC-089	ALPHA-APAC-089	CONTROLLER
ALPHA-APAC-090	ALPHA-APAC-090	CONTROLLER
ALPHA-APAC-091	ALPHA-APAC-091	CONTROLLER
ALPHA-APAC-092	ALPHA-APAC-092	CONTROLLER
ALPHA-APAC-093	ALPHA-APAC-093	CONTROLLER
ALPHA-APAC-094	ALPHA-APAC-094	CONTROLLER
ALPHA-APAC-095	ALPHA-APAC-095	CONTROLLER
ALPHA-APAC-096	ALPHA-APAC-096	CONTROLLER
ALPHA-APAC-097	ALPHA-APAC-097	CONTROLLER
ALPHA-APAC-098	ALPHA-APAC-098	CONTROLLER
ALPHA-APAC-099	ALPHA-APAC-099	CONTROLLER
ALPHA-APAC-100	ALPHA-APAC-100	CONTROLLER

Figure 2-20 Site Management

Devices can either be manually assigned to a site using Drag and Drop or be assigned by the installer via the Aruba Install Manager mobile application. The application simplifies deployments as it allows organizations to designate an installer for each branch site who can then scan the new Aruba devices. Each scanned Aruba Gateway, Switch, and IAP is automatically geotagged and assigned to the correct site and group.

Aruba Central provides a convenient option to convert existing labels or groups into sites for existing deployments. Both methods allow a CSV file to be downloaded which contains all of the existing labels or groups. Each CSV contains address fields that must be populated before uploading the CSV file back into Central.

The conversion of labels is a one way process and cannot be undone. All the historical data for each converted label will be retained, but will only be available when monitoring and reporting for a site. The converted labels and assignments will be removed. The conversion of groups into sites will leave existing groups unchanged. The conversion process will simply create a new site for each group and will automatically assign all the devices in each group to their respective sites.

Provisioning

Aruba Gateways operating as VPNCs or BGWs can either be automatically or manually provisioned. Most deployments will implement manual provisioning for VPNCs and automatic provisioning for BGWs using ZTP. Automatic provisioning is preferred for BGWs as it simplifies and streamlines branch deployments.

Prerequisites

The following steps must be performed in Aruba Central server before provisioning Aruba Gateways, Aruba IAPs, or ArubaOS switches:

1. The device must be present in the Central device inventory. For most deployments this will be automatic as each newly purchased Aruba device will be added automatically.
2. The device must be subscribed and licensed. Aruba recommends enabling **Auto Subscribe** to automate device management subscription assignments to IAPs and Switches. Additionally each Gateway must be assigned a foundation or foundation-base license.

To streamline the provisioning process of Aruba Gateways in branch locations, each BGW must be assigned a system-ip. The system-ip can be automatically assigned using configuration applied to each BGW group or be applied on a per device basis using bulk configuration.



For additional details on the system-ip please refer to the [System IP](#) section.

Automatic Provisioning

Most Aruba devices deployed in branches will be automatically provisioned. New Aruba Gateways are connected to the Internet and will automatically obtain IP addressing, reach out to Aruba Activate for firmware upgrades (if required), and then be redirected to Aruba Central where their configuration resides. Any device level configuration uploaded using bulk configuration combined with a BGW group configuration is pushed and applied to that gateway.

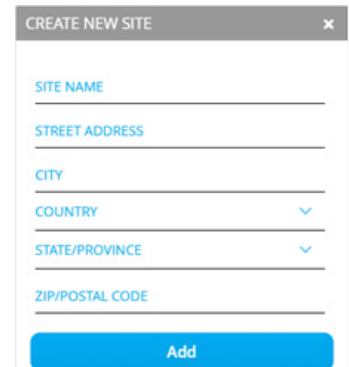
The Aruba Gateways must be assigned to a BGW group prior to communicating with Central in order for automatic provisioning to occur. The group assignment can be performed manually in Central or automatically using the Install Manager application.

Install Manager

Aruba offers the Install Manager application in Aruba Central to automate the provisioning of new devices for new branch sites along with a corresponding mobile application available for Android and Apple iOS devices. The Install Manager application in Central is used by IT staff to assign installers to each new branch site, configure the gateway, IAPs and ArubaOS Switch group assignments as well as monitor the deployment status.

A typical Install Manager provisioning workflow consists of the following steps:

1. IT staff will create a new site or import multiple sites under **Labels and Sites**.



CREATE NEW SITE

SITE NAME

STREET ADDRESS

CITY

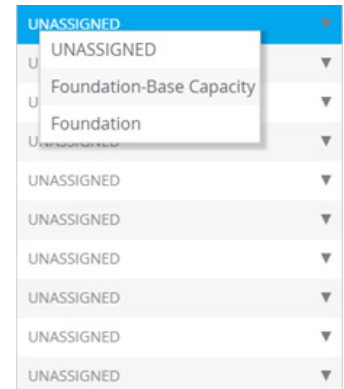
COUNTRY

STATE/PROVINCE

ZIP/POSTAL CODE

Add

2. If auto-subscription is disabled IT staff will assign the device and foundation subscriptions to the new devices under **Subscription Assignment**.



UNASSIGNED

UNASSIGNED

Foundation-Base Capacity

Foundation

UNASSIGNED

UNASSIGNED

UNASSIGNED

UNASSIGNED

UNASSIGNED

UNASSIGNED

UNASSIGNED

3. Navigate to **Install Manager** and configure the IAP, switch, and gateway group assignments for each site.



Edit Mode

IAP GROUP NAME

DEMO-BRANCH-GW

SWITCH GROUP NAME

DEMO-BRANCH-GW

GATEWAY GROUP NAME

DEMO-BRANCH-GW

ADDITIONAL NOTES

SAVE

- IT staff assign an existing installer to a site or add a new installer and assign a site under **Installers**. The installer's first name, last name, mobile phone number, site assignments, expiration date, and expiration time are configured.

ADD INSTALLER

First Name Agent	Last Name Smith	
CODE +1	Mobile Number 555-555-1212	Valid Till 08/16/2018
× DEMO-BRANCH1 × DEMO-BRANCH2 ×		

SAVE

CANCEL

- Once on-site, the installer opens the Aruba Installer application, selects **Sign Up**, and enters their first name, last name, and mobile phone number. The information entered must match the installer configuration in Central. The installer selects **Register** to complete the registration process.

Verizon 10:12 100%

Sign Up Sign In

Agent Smith

+1 5555551212

Register

- The installer selects **Sign In** and enters their mobile phone number, then selects **Get OTP** to receive a one-time password via a SMS text message. The password is valid for 5 minutes and the installer must enter it to login and proceed. The password can be resent if required.

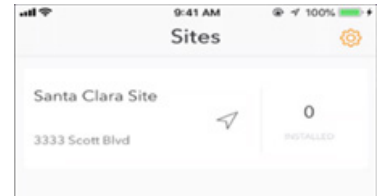
Verizon 10:13 100%

Sign Up Sign In

+1 5555551212

Get OTP

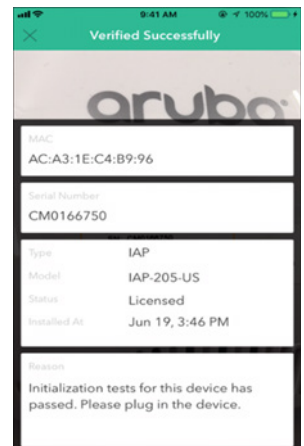
- The application will display a list of sites the installer has been assigned once they have signed in. The installer will select the appropriate site.



- The installer scans the serial number and MAC address barcodes of each Aruba device which is in turn sent to Aruba Central.



- If verification is successful, the installer will see a "Verified Successfully" message. The device's MAC address, serial number, information, and licensing status is displayed.



- Once the devices have been connected to the network, the installer can view the status of each device. If installation was successful, the verified, licensed, and connected statuses will show as green.



Zero Touch Provisioning

Aruba devices can be automatically provisioned by Aruba Central using Zero Touch Provisioning. With ZTP, Aruba gateways, IAPs, and ArubaOS switches are able to automatically communicate with Central and download their group configuration without any user interaction. Each managed Aruba device can be manually assigned to their respective group in Central under **Global Settings > Manage Groups** or by assigning groups per site in advance under Site Installations in the Install Manager application. Unlike Aruba switches and IAPs, the group assignment for gateways must be performed prior to ZTP. This is required so that Central knows the role (BGW or VPNC) of the gateway. The group type must also be selected or the group type will display as “unprovisioned”.

ZTP is the preferred method for deploying new branch devices as it eliminates the requirements for any on-site user interaction and configuration. An on-site installer can simply connect the Aruba devices and the ZTP process will automatically onboard and provision each branch device. While ZTP may be used to provision VPNCs in the data center, One Touch provisioning is often preferred as VPNCs typically require static IPv4 addresses along with specific VLAN and switchport configuration.

When deploying a new branch site, it is important to remember that any IAPs and ArubaOS switches at the branch will only be able to complete their ZTP process and receive their group configuration once the gateway(s) are provisioned and online. The IAPs and switches will not be able to communicate with Central until they are able to obtain IP addressing and domain name server (DNS) information from their respective gateway(s).

In order for a gateway to successfully perform ZTP, one or more ZTP ports must be connected to a WAN service that provides the following:

1. DHCP addressing
2. DHCP options 3 (Router) and 5 (Name Server)
3. Internet access

The WAN services at the branch can provide the gateway with either public or private RFC-1918 IPv4 addressing. Private IPv4 addressing is typically offered by intermediate CPE modems or gateways. If multiple WAN services are connected to the gateway, each WAN service must provide a non-overlapping IPv4 address. This may occur if multiple CPE modems or gateways are connected which provide RFC-1918 addressing since most vendors default to a common 192.168.0.0/24 address space.

WAN services can be connected to any switchport on an Aruba gateway except for Gigabit Ethernet 0/0/1 which is reserved for One Touch Provisioning (OTP). If the gateway is connected to multiple WAN services it will attempt to perform ZTP over each service until it is successful. The first WAN service that responds to the DHCP discover message will be selected first.

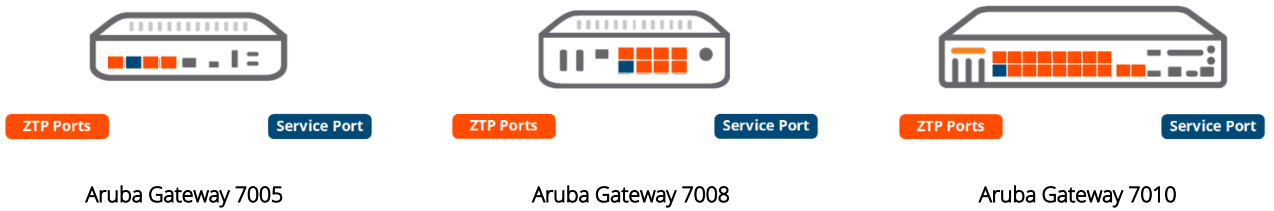


Figure 3-1 ZTP Port Locations



The last copper port on the gateway is reserved for ZTP if it is running the firmware image shipped from the factory.

The ZTP process is broken into three phases:

1. The gateway will attempt to obtain an IPv4 address via DHCP out of VLAN 4094 which is assigned to the ZTP enabled switchports.
2. The gateway will resolve the Activate fully-qualified domain name (FQDN) and establish an HTTP Secure (HTTPS) session to Activate. The gateway provides Activate with its serial number, MAC address, and model. Aruba Activate authenticates the device and redirects the gateway to Central.

Aruba Activate will trigger a firmware upgrade if one is required. The gateway will reboot and restart the ZTP process upon upgrading.

3. The gateway will resolve the Aruba Central FQDN and establish a HTTPS session to Central. The gateway provides Central with its serial number, MAC Address, model and certificate. Central authenticates the device and pushes the required firmware image (if required) along with group configuration.

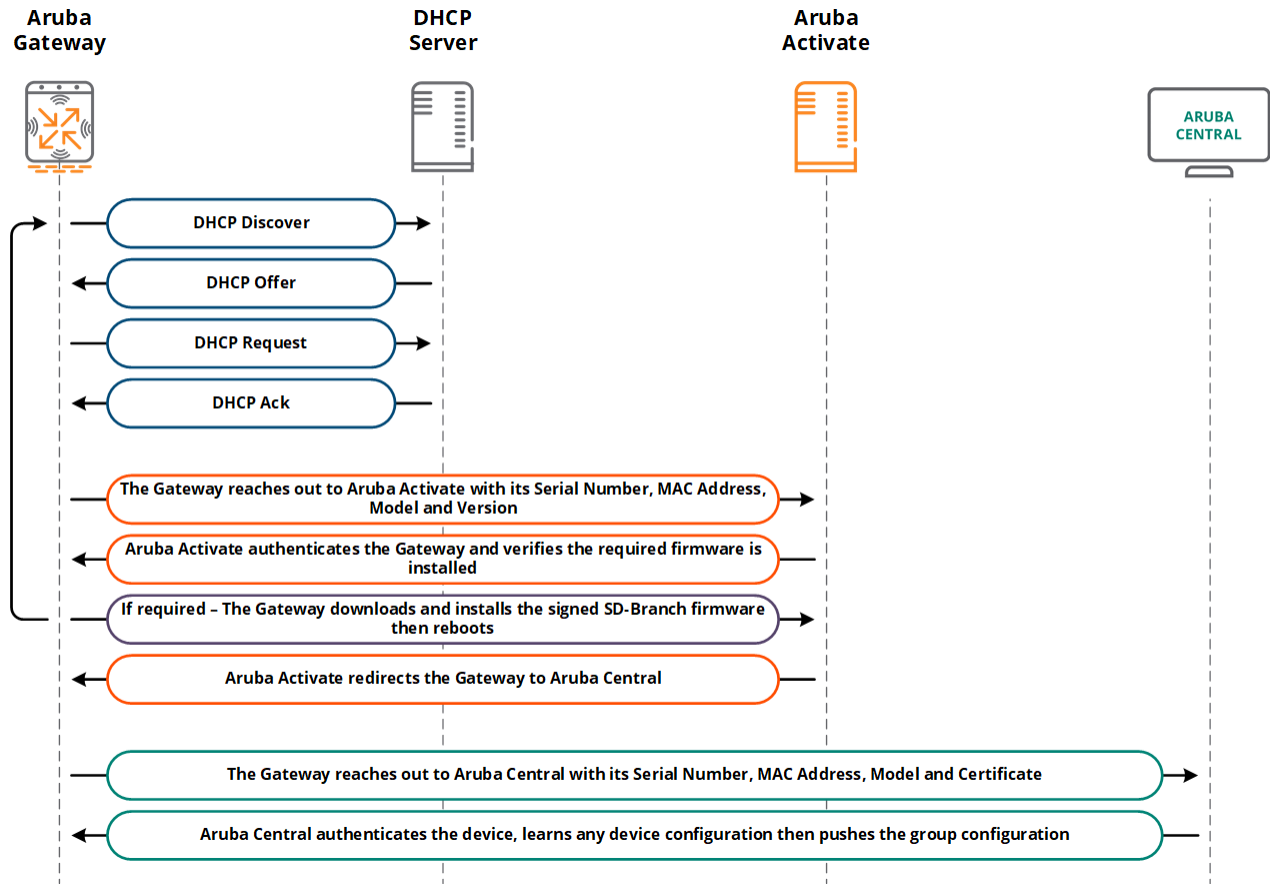


Figure 3-2 ZTP and Auto-Upgrade Process



The Aruba gateway has to resolve the Aruba Activate server FQDN <https://device.arubanetworks.com> during the ZTP process as well as the Aruba Central URL assigned by the Activate server, otherwise the ZTP provisioning process will fail.



The automatic firmware upgrade from Activate is supported for Aruba gateways running the factory firmware with image 6.5.1.4 and above. If the gateway is running ArubaOS 8.0 or above then a manual firmware upgrade is required.

One Touch Provisioning

ZTP is the preferred method for deploying gateways that dynamically obtain their IP addressing from an Internet Service Provider (ISP). The gateway is connected to the Internet services, obtains an IPv4 address then communicates with Aruba Central to obtain its configuration.

There may be circumstances where a gateway requires additional configuration before it can communicate with Central. E.g., the gateway may require:

1. Static addressing
2. Point-to-Point Protocol over Ethernet (PPPoE) credentials to initiate the Internet service
3. Specific VLAN configuration

To account for these deployment scenarios, Aruba offers a “one touch provisioning” feature for gateways which can be accessed using either the serial console or web user interface. The OTP feature is only available for gateways in their factory default state and cannot be accessed once a gateway has received its configuration from Central.

Web User Interface

OTP using the web user interface allows static IP addressing and PPPoE credentials to be configured on Aruba gateways. The web user interface is the recommended option for BGW deployments when static IP addressing or PPPoE credentials are required for the BGW to communicate with Central. This configuration is typically performed by the installer.

OTP is performed on a gateway via the WebUI using the following procedure:

1. Boot the Aruba Gateway.
2. Once the Aruba Gateway is booted, connect a PC or workstation to the **Ge0/0/1** port. The PC or workstation must be configured to obtain its IPv4 address using DHCP.
3. Open a Web browser and connect to **https://172.16.0.254**. The controller contains a default server certificate to validate the device on the network. At the **Security Alert**, click **Yes** to proceed with the **Setup Wizard**. The alert will vary by web browser.
4. Select the **By connecting to activate/central** provisioning method and then click **Next**.

The WebUI provides an option to configure a WAN uplink with a static IP addressing as well as configure PPPoE credentials. Examples of each configuration are provided in figure 3-3:

How will the controller connect to Activate/Central?

Static IP Address PPPoE

Interface:

IP address:

Network mask:

Default gateway:

DNS server:

How will the controller connect to Activate/Central?

Static IP Address PPPoE

Interface:

Username:

Password:

Retype password:

Figure 3-3 One Touch Provisioning using Static IP and PPPoE

Serial Console

One touch provisioning using the serial console allows static IP addressing, PPPoE credentials, and specific VLAN configurations to be configured on gateways. The serial console is recommended when a VPNC or BGW requires more advanced configurations such as requiring a specific VLAN IDs or trunk configurations.

OTP can be performed on a gateway via the serial console using the following procedure:

1. Configure a terminal or terminal emulation program to use the following communication settings:

Baud Rate	Data Bits	Parity	Stop Bits	Flow Control
9600	8	None	1	None

2. Connect the terminal or workstation to the serial port on the controller using an RS-232 serial cable. All accessory kits shipped with Aruba gateways contain an RJ-45 cable and DB-9 to RJ-45 adapter. It may be necessary to use a USB adapter to connect the serial cable to the terminal or workstation.
3. Boot the gateway.
4. After the gateway has booted the following screen should appear. The OTP setup is activated by typing **static-activate** followed by the **enter** key:

```
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 customi-
zation and requires DHCP server
  'full-setup'         : Start full setup dialog. Provides full customiza-
tion
  'static-activate'   : Provides customization for static or PPPOE ip as-
signment.
Enter Option (partial string is acceptable): static-activate
```

The serial console allows a static IP address and PPPoE credentials as well as specific VLAN configuration to be configured. The following examples demonstrate typical one touch configurations that can be performed using the serial console:

- BGW implementing PPPoE on a specific access VLAN and port:

```
Enter Controller VLAN ID [1]: 4092
Enter Uplink port [GE 0/0/0]: GE 0/0/3
Enter Uplink port mode (access|trunk) [access]:
Enter Uplink Vlan IP assignment method (static|pppoe) [static]: pppoe
Enter Uplink Vlan PPPoE username: username
Enter Uplink Vlan PPPoE password: *****
Re-enter Uplink Vlan PPPoE password: *****
Do you want to configure port-channel (yes|no) [no]: no
```

- VPNC requiring static addressing and an 802.1Q tagged VLAN:

```
Enter Controller VLAN ID [1]: 4001
Enter Uplink port [GE 0/0/0]:
Enter Uplink port mode (access|trunk) [access]: trunk
Enter Native VLAN ID [1]: 1
Enter Uplink Vlan IP assignment method (static|pppoe) [static]: static
Enter Uplink Vlan Static IP address [192.168.1.1]: 192.168.120.20
Enter Uplink Vlan Static IP netmask [255.255.255.0]: 255.255.255.0
Enter IP default gateway [none]: 192.168.120.1
Enter DNS IP address [none]: 1.1.1.1
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
Do you want to configure port-channel (yes|no) [no]: no
```

Bulk Configuration Upload

When bulk configuration upload is used, an Aruba Gateways configuration is populated in advance in a CSV template file and then uploaded to Central. All configuration defined in the template for a device is applied to the respective VPNC or BGW device configuration. Bulk configuration upload is incremental and allows new configurations or changes to be uploaded into Central at any time.

Bulk configuration upload requires the sample device template file to be downloaded, populated with the correct values, and then uploaded back into Central. The device template can be downloaded by navigating to **Gateway Management > Interfaces > Bulk configuration upload** and selecting the **Download Sample File** option. Doing so will download an empty CSV template file that includes headers and descriptions only. Selecting the **Download Device Template** option will download a CSV template file that includes the headers, descriptions, and will be prepopulated with the MAC addresses and group assignments of existing gateways (Figure 3-4):

The screenshot shows the Aruba Central Gateway Management interface. The left sidebar contains navigation options: Search Current App, Interfaces, WAN, VPN, Routing, Security, and System. The main content area is titled 'FILTER GATEWAY MANAGEMENT TME_OAK_7008' and includes tabs for Ports, VLANs, DHCP, Pool Management, GRE Tunnels, and Bulk configuration upload. Under 'Bulk configuration upload', there is a 'Previous bulk configuration' section showing a successful status with 1 device processed. Below this is an 'Upload Section' with a 'File to upload:' field and three buttons: 'Browse', 'Download Sample File', and 'Download Device Template'. The 'Download Sample File' and 'Download Device Template' buttons are highlighted with a red box.

Figure 3-4 Bulk Configuration Upload

Parameters that can be configured and uploaded using the template file include:

- Hostnames
- VLAN Configuration
- DHCP Pools
- PPPoE Credentials
- Gateway Redundancy
- VRRP Configuration
- System IP Configuration

Pre-provisioning a new gateway using the bulk configuration upload method requires populating at least the **MAC Address**, **Group**, **Model**, and **Hostname** fields. The population of the remaining fields will be dependent on the individual VPNC or BGW configuration requirements. E.g., deploying a VPNC or BGW using static IP address assignments will necessitate population of the **VLAN Id**, **VLAN IP**, **VLAN Subnet** and **Controller VLAN** fields (Figure 3-5):

	A	B	C	D	E	F	G	V	W	X	AG
35	MAC Address	Group	Model	Hostname	VLAN Id	VLAN IP	VLAN Subnet	VLAN Id	VLAN IP	VLAN Subnet	Controller VLAN
36	00:0b:86:b8:66:e8	DEMO-BRANCH-GW	A7005	DEMO-BR1-GW1	10	192.168.88.1	255.255.255.128	11	192.168.88.129	255.255.255.128	10
37	00:0b:86:be:63:e8	DEMO-BRANCH-GW	A7005	DEMO-BR2-GW1	10	192.168.89.1	255.255.255.128	11	192.168.89.129	255.255.255.128	10

Figure 3-5 Bulk Configuration Template Pre Provisioning Example

Aruba Gateways

This section provides a detailed overview of the fundamental configuration parameters required to configure Aruba Gateways within the Gateway Management application. The intent of this section is to provide an explanation of each key configuration element with usage examples. This section does not provide step-by-step configuration examples but is organized to follow a typical configuration workflow.

VLANs and Interfaces

VLAN Interfaces

A VLAN interface is a Virtual LAN (VLAN) represented by one IPv4 address to the routing and bridging system. The VLAN interface provides the layer 3 processing of packets from all switch ports associated with a given VLAN. All Aruba gateways operating as VPNCs or BGWs will implement one or more VLAN interfaces depending on the data center or branch topology:

- **Data center** – One or more VLAN interfaces to terminate VPN tunnels and forward overlay traffic.
- **Branch** – Two or more VLAN interfaces to initiate VPN tunnels (WAN) and support users.

VLAN interfaces can be configured at the device or group level. Typically individual VLAN IDs, routing, and DHCP relay options are configured using groups while static addresses or PPPoE credentials are configured per device. VLAN interfaces using dynamic address assignments via DHCP typically are configured per group.

Figure 4-1 provides example VLAN interface usage within a data center and branch:

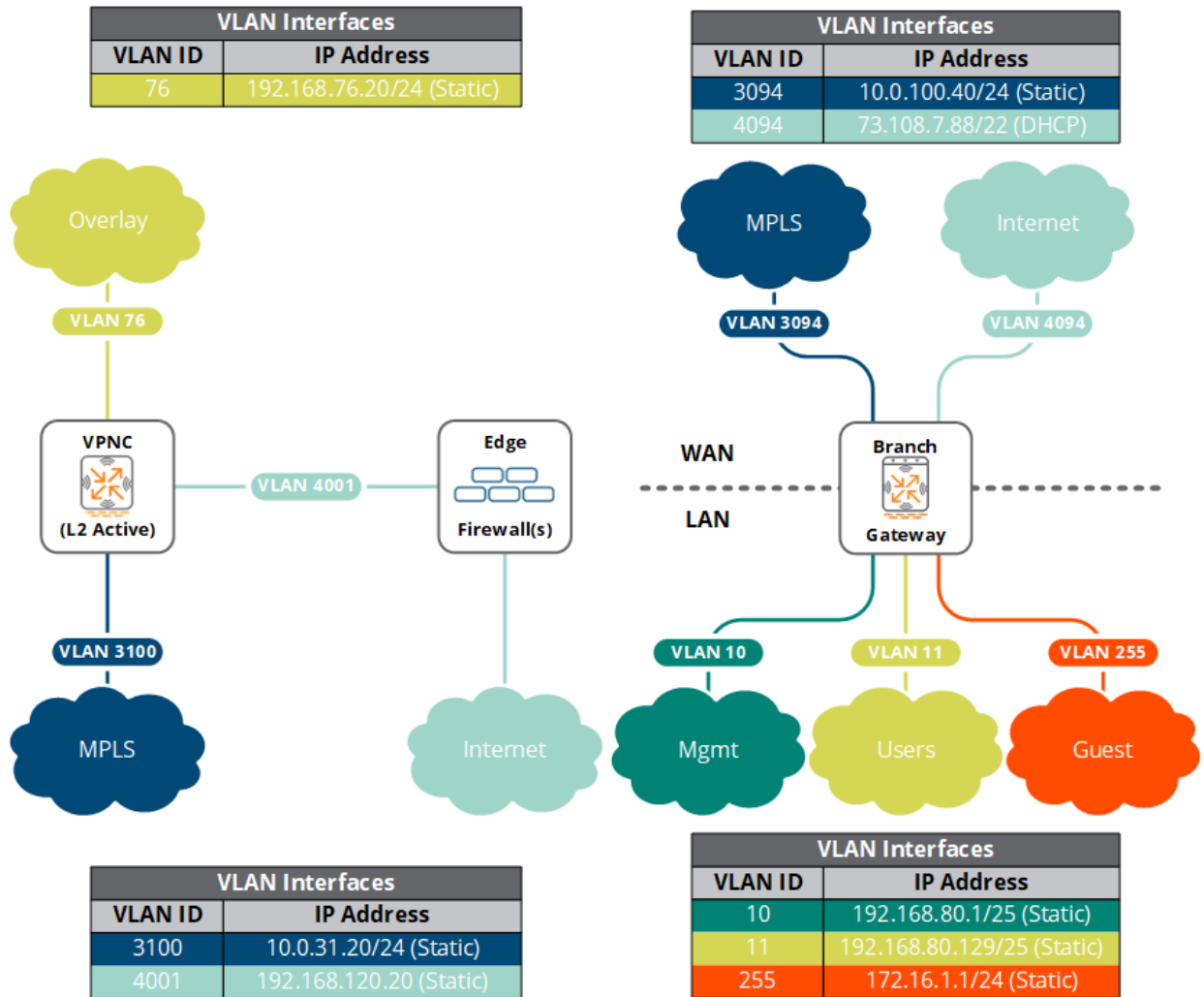


Figure 4-1 VLAN Interfaces for VPNC (Left) and BGW (Right) Deployments

VLAN interfaces are configured by navigating to **Gateway Management > Interfaces > VLANs**. A **VLAN name** and **VLAN ID** must be configured before any IPv4 address configuration can be applied. A new VLAN can be created by selecting the blue **Plus (+)** icon. As a best practice, Aruba does not recommend including spaces for VLAN names:

aruba Central

CURRENT APP
GATEWAY MANAGEMENT

Q Search Current App
Find devices, clients and networks

Interfaces
Set Interfaces, DHCP, NAT parameters

WAN
Set uplink, path steering policies

VPN
Set IPSec encryption parameters

Routing
Set routing parameters

Security
Set advanced security parameters

System
Manage advanced system settings

High Availability
Set redundancy parameters

Configuration Audit
Review Configuration status

FILTER GATEWAY MANAGEMENT
TME_OAK_7008 (1 Total Devices | 0 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS) ▼

Ports **VLANs** DHCP Pool Management GRE Tunnels Bulk configuration upload

VLANs	
NAME	ID(S)
employee	2
guest	99
iot	3
Mgmt	1
system-ip	3333
--	169-170,4094
+	

New VLAN

VLAN name:

VLAN ID/Range:

Figure 4-2 VLAN Interface Configuration

Once the VLAN ID has been created it can be selected which will display its IPv4 configuration. Configuration parameters that can be applied include:

- **Enable Routing** – Must be enabled for the VLAN interface to process layer 3 packets. This parameter is typically enabled per VPNC or BGW group.
- **IP assignment** – Determines how the VLAN interface is addressed:
 - **Static** – The VLAN interface is statically assigned an address per device. Static addressing can be applied during gateway provisioning, bulk configuration upload, or be manually assigned post-provisioning in Central.
 - **DHCP** – The VLAN interface is dynamically assigned an address using DHCP. This option is typically utilized for Internet-based WAN uplinks in BGWs and is configured per BGW group.
 - **PPPoE** – The VLAN interface is dynamically assigned an address using PPPoE. This option is typically utilized for Internet-based WAN uplinks for xDSL deployments and is configured per BGW group. The individual PPPoE credentials are typically pre-provisioned per device using bulk configuration upload or static activate.

- **Dynamic DHCP Pool** – The VLAN interface is dynamically assigned an address from Aruba Central. The VLAN interface and users in each branch are assigned addressing from a subnet allocated from a larger CIDR range configured per BGW group.
- **Gateway Pool** – The VLAN interface is dynamically assigned a host address from Central. The VLAN interface is dedicated for system-ip use. The gateway pool is configured per VPNC or per BGW group.
- **Network Address Translation (NAT) Outside** – Enabled for Internet WAN uplinks when local Internet access is permitted. This parameter is typically enabled per VPNC or per BGW group.

The VLAN interfaces for VPNCs can be configured at either the device or VPNC group level. Most deployments will configure VLAN names and IDs at the VPNC group level and assign static addresses per VPNC device. Aruba does not recommend implementing dynamic addressing for VPNCs as the IPv4 addresses need to be known.

To simplify branch deployments, all VLAN interface configuration for BGWs is typically performed per BGW group with any static addressing being pre-provisioned using bulk configuration upload. VLAN interface addressing for LANs can also be automated using dynamic DHCP pools which are configured per BGW group.



For each Aruba Gateway one VLAN interface will be selected as the system-ip which is used to communicate with external systems such as Remote Authentication Dial In User Service (RADIUS), syslog, Terminal Access Controller Access Control System Plus (TACACS+), and Simple Network Management Protocol (SNMP). Recommendations and best practices for configuring the system-ip is covered in detail in the [System IP](#) section of this document.

Static IP Addressing

Static IP addresses are assigned to individual VLAN interfaces on VPNCs or BGWs per device. Static IPv4 address assignments can be performed using a number of methods:

1. Static IPv4 addresses are configured on gateways using Full Setup or Static Activate. The configured addresses are learned by Central and applied to the configuration for each device.
2. Static IPv4 addresses are pre-provisioned using bulk configuration upload. The CSV template allows for pre-provisioning of one or more VLAN interfaces and DHCP pools. The system-ip address can also be provisioned.
3. Static IPv4 addresses are configured in Central post provisioning. The VLANs are configured and enabled for IP routing per group while the static IP addresses are configured per device.

The addressing method will be specific to each deployment. VPNCs will typically be provisioned using One Touch Provisioning where the VLAN interface and static IPv4 address is configuration and learned. BGWs will typically be pre-provisioned using bulk configuration upload. Per device address assignments are only performed for smaller deployments consisting of a few BGWs.

Per Device

There are certain instances where an existing IPv4 address needs to be changed or a new VLAN interface and IPv4 address configured. As a best practice Aruba recommends creating the VLAN ID and Name at the group level then then assigning the static IP addresses at the device level:

- **Group** - Enable routing and set the IP assignment to Static.
- **Device** - Assign the IPv4 address and Netmask. A DHCP server may be optionally enabled and configured for LAN interfaces on BGWs.



The exception would be for guest VLAN interfaces that are common and internal to each branch. The VLAN ID, Name, and static IPv4 address configuration can all be performed at the group level.

To modify the IPv4 configuration for a VLAN interface navigate to the **Gateway Management > Interfaces > VLANs** and click on the VLAN IDs that require modification under the **VLANs** list. Selecting the appropriate ID from the VLAN IDs list that appears will provide access to **IP Address Assignment** where parameters such as IP routing and toggling between static and dynamic IP assignment can be configured:

The screenshot displays the configuration for an IPv4 Port Member. The 'IP Address Assignment' section is highlighted with a red border. It includes the following settings:

- Enable routing:
- IP assignment: Static (dropdown menu)
- IPv4 address: 192.168.88.1
- Netmask: 255.255.255.128
- Act as DHCP server:
- Relay to external:
- MTU: 1500
- Suppress ARP:
- VLAN status:
- NAT inside:
- NAT outside:
- Admin state:

Figure 4-3 VLAN Interface Static IP Address Assignment

Figure 4-3 shows the group and device configuration for a BGW's VLAN 10 LAN interface. In this example the VLAN ID and Name are configured under the BGW group. IP routing is **enabled** and the **IP assignment** is set to **Static**. The IPv4 address and Netmask assignment are performed at the device level. Additional configuration such as enabling the DHCP server (not shown) may optionally be performed if required.

Bulk Configuration Upload

VPNC or BGW VLAN interfaces can be configured using the bulk configuration template and then be uploaded to Central. Bulk configuration can be used to pre-provision new VPNCs or BGWs prior to deployment or incrementally apply new configurations or changes to existing VPNCs or BGWs at any time.

The **MAC Address**, **VLAN Id**, **VLAN IP**, and **VLAN Subnet** fields need to be populated to configure one or more VLAN interfaces on a gateway. The template provides the option to define two VLAN interfaces by default. Additional fields such as **Group**, **Model**, and **Hostname** fields being required for new gateways without a group assignment.

Figure 4-4 shows a template example that configures two VLAN interfaces for two BGWs. In this example VLAN interfaces **10** and **11** are configured on each BGW with static IPv4 addresses assigned. VLAN interface 10 is also assigned as the system-IP for each BGW. Additional columns showing other configurations are hidden for clarity:

	A	B	C	D	E	F	G	V	W	X	AG
35	MAC Address	Group	Model	Hostname	VLAN Id	VLAN IP	VLAN Subnet	VLAN Id	VLAN IP	VLAN Subnet	Controller VLAN
36	00:0b:86:b8:66:e8	DEMO-BRANCH-GW	A7005	DEMO-BR1-GW1	10	192.168.88.1	255.255.255.128	11	192.168.88.129	255.255.255.128	0
37	00:0b:86:be:63:e8	DEMO-BRANCH-GW	A7005	DEMO-BR2-GW1	10	192.168.89.1	255.255.255.128	11	192.168.89.129	255.255.255.128	0

Figure 4-4 Static IP Bulk Configuration for VLAN Interfaces Upload Template Example

The template includes columns to support two VLAN interfaces as well as optional DHCP pools. If a single VLAN interface is required, only the first **VLAN Id**, **VLAN IP**, and **VLAN Subnet** fields need to be populated. If a deployment requires more than two VLAN interfaces:

1. More CSV fields may be added to the end of the header. E.g., adding additional VLAN Id, VLAN IP, and VLAN Subnet fields.
2. The template file works in an incremental way, meaning that new configurations can be added by modifying the template file then re-uploading it into Central. E.g., additional VLAN interfaces could be added by modifying the VLAN Id, VLAN IP, and VLAN subnet column values then re-uploading the template to Central.

DHCP Addressing

BGWs with VLAN interfaces connected to Internet WAN services can be configured to dynamically obtain IPv4 addressing from an ISP's DHCP server. This configuration is typically performed per BGW group when the group includes the VLAN ID, Name, routing, IPv4 assignment, and NAT configuration.

The configuration is performed per BGW group by navigating to **Gateway Management > Interfaces > VLANs**. The IPv4 configuration for a VLAN is accessed by selecting a **VLAN ID** which exposes the IPv4 configuration. Figure 4-5 shows the group configuration for a BGW's VLAN 4094 VLAN interface that connects to an ISP. In this example, IP routing is **enabled** and the **IP assignment** is set to **DHCP**. **IP NAT outside** is also enabled to facilitate the translation and forwarding of Internet traffic from employees and guests:

The screenshot shows the configuration page for IPv4 Port Members. Under the 'IP Address Assignment' section, the following settings are visible:

- Enable routing:** (highlighted with a red box)
- IP assignment:** DHCP (dropdown menu)
- Client ID:** (empty text field)
- MTU:** 1500 (text field)
- VLAN status:**
- NAT inside:**
- NAT outside:** (highlighted with a red box)
- Admin state:**

Figure 4-5 VLAN Interface DHCP Address Assignment

PPPoE Addressing

BGWs with VLAN interfaces connected to xDSL based Internet WAN services can be configured to dynamically obtain IPv4 addressing from the ISP using the PPPoE protocol. The PPPoE configuration can be performed at the BGW group or per BGW device depending on if common or unique credentials that are supplied:

- **Common PPPoE Credentials** – All the VLAN interface configuration can be performed at the group level.
- **Unique PPPoE Credentials** – If unique PPPoE credentials are required per branch the configuration must be performed at both the BGW group and device level. The PPPoE credentials can also be provisioned on the BGW during installation using Static Activate or be pre-provisioned using bulk configuration upload.

Many service providers in the United States will require unique PPPoE credentials to be configured per branch and will therefore require a unique PPPoE username and password to be configured per BGW. The VLAN interface configuration will be performed per BGW group while the individual PPPoE credentials are configured per device.

While PPPoE credentials can be pre-provisioned using bulk configuration upload, the BGW will typically require the xDSL Internet WAN service to communicate with Aruba Central to be provisioned. If this is the case, the PPPoE credentials would be entered by the installer using One Time Provisioning during the initial Aruba Gateway setup.

Per Device

There are certain instances where existing PPPoE credentials needs to be changed or a new VLAN interface supporting PPPoE needs to be deployed. This performed per device by navigating to **Gateway Management > Interfaces > VLANs**. As a best practice Aruba recommends creating the VLAN ID and Name at the group level then then assigning the PPPoE credentials per device:

- **Group** – Enable routing, set the IP assignment to PPPoE, and define a PPPoE username. Optionally enable NAT outside.
- **Device** – Assign the PPPoE username and password.

The PPPoE configuration for a VLAN interface is accessed by selecting a **VLAN ID** at the device or group which exposes the IPv4 configuration. Figure 4-6 shows the group and device configuration for a BGWs VLAN 4094 LAN interface. In this example the VLAN ID and Name are configured under the BGW group. IP routing is **enabled** and the **IP assignment** is set to **PPPoE**. **IP NAT outside** is also enabled to facilitate the translation and forwarding of Internet traffic from employees and guests. The individual PPPoE credentials being configured or changed at the device level:

The screenshot displays the configuration page for IPv4 Port Members. Under the 'IP Address Assignment' section, the following settings are visible:

- Enable routing:
- IP assignment: PPPoE (dropdown menu)
- Service name: (empty text field)
- User name: CHANGEME (text field)
- Password: (masked text field)
- Retype password: (masked text field)
- MTU: 1500 (text field)
- VLAN status:
- NAT inside:
- NAT outside:
- Admin state:

Figure 4-6 VLAN Interface PPPoE IP Address Assignment

Bulk Configuration Upload

A BGW's PPPoE configuration can be configured or modified using the bulk configuration template (**Gateway Management > Interfaces > Bulk configuration upload**) and then uploaded to Central. The bulk configuration template file provides the necessary columns to provide the **PPPoE username**, **PPPoE password**, and optional **PPPoE service name** for a VLAN interface. The PPPoE parameters are assigned directly after the **VLAN Id** assigned to the WAN VLAN interface.

Figure 4-7 shows a template example which configures the PPPoE credentials on a WAN VLAN interface for two BGWs. For this example the WAN VLAN interface is set to **4094** and each BGW is configured with a unique **PPPoE username** and **PPPoE password**. Additional columns showing other configurations are hidden for clarity:

	A	B	C	D	E	I	J
1	MAC Address	Group	Model	Hostname	VLAN Id	PPPoE Username	PPPoE Password
2	00:0b:86:b8:66:e8	DEMO-BRANCH-GA7005		DEMO-BR1-GW1	4094	br1username	*****
3	00:0b:86:be:63:e8	DEMO-BRANCH-GA7005		DEMO-BR1-GW2	4094	br2username	*****

Figure 4-7 PPPoE Bulk Configuration for VLAN Interfaces Upload Template Example



Bulk configuration upload can also be used to update existing PPPoE credentials by selecting **Download Device Template** (which includes all the existing BGWs in the group) modifying the PPPoE credentials and then uploading the CSV back to Aruba Central.

Dynamic DHCP Pools

Dynamic DHCP pools provide a convenient way to automate addressing of LAN VLAN interfaces at branch sites. With Dynamic DHCP, Central can automatically allocate a subnet to a LAN VLAN interface on a BGW from a dynamic pool of addresses configured within the BGW group. In each branch, the BGW is allocated the first address from the subnet while the remaining addresses are allocated to users.

As with a normal DHCP pool, one dynamic pool is required per LAN VLAN interface that requires dynamic addressing. Each dynamic pool consists of a CIDR block of addresses of which smaller subnets are allocated to VLAN interfaces per BGW on a first come, first serve basis. Each subnet is allocated as each BGW within the group is provisioned.

For each dynamic DHCP pool, the primary CIDR block is sized accordingly to support the number of BGWs assigned to the group as well as the number of host addresses required per branch. One important thing to remember is that the number of host addresses assigned from each dynamic pool is consistent across all the BGWs in the group. For example if the dynamic pool is configured to allocate 25 host addresses to each branch, a /27 subnet is assigned to each BGW regardless if all the addresses are utilized.

Figure 4-8 provides an example dynamic DHCP pool configuration for three BGW groups supporting two VLAN interfaces. Each BGW group supporting between 200 – 245 BGWs. For this example VLAN 10 is used for device management while VLAN 11 is used for employees. The

maximum number of managed devices per branch is 8 devices (including the BGW) while the maximum number of employee devices is 18.

To accommodate these requirements:

- VLAN 10** – The managed devices dynamic pool in each group are allocated a /20 CIDR range of addresses. The dynamic pool is configured to allocate 13 host addresses with one additional host address is automatically assigned to the each BGW in the group (14 total). This configuration will allocate a /28 to each branch. The BGWs VLAN 10 interface assuming the first address from the assigned subnet.
- VLAN 11** – The employee devices dynamic pool in each group is allocated a /19 CIDR range of addresses. The dynamic pool is configured to allocate 29 host addresses with one additional host address is automatically assigned to the each BGW in the group (30 total). This configuration will allocate a /27 to each branch. The BGWs VLAN 11 interface assuming the first address from the assigned subnet.

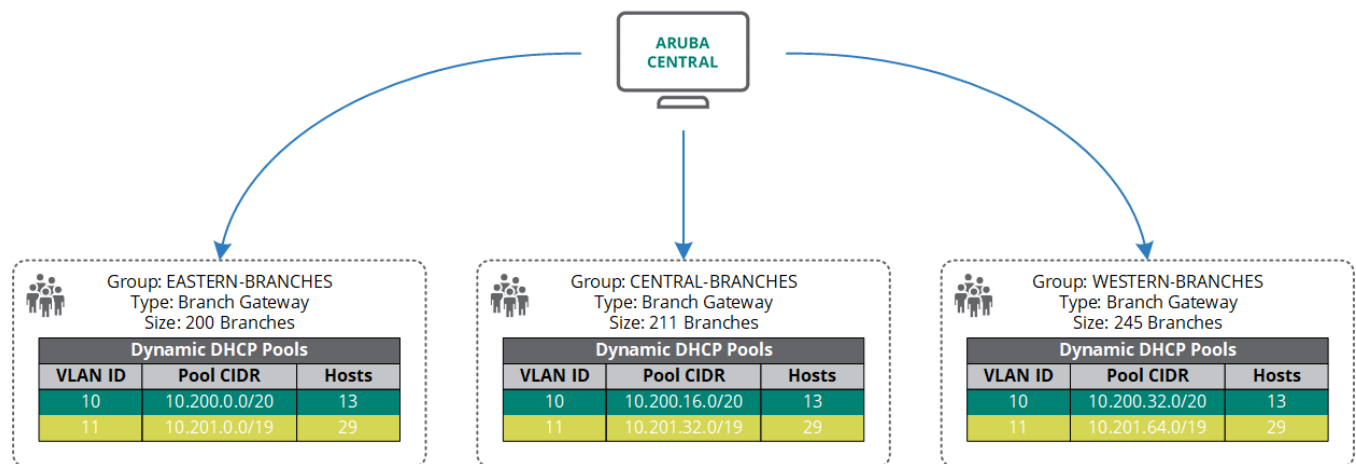


Figure 4-8 Dynamic DHCP Pool Deployment Example



Once a subnet has been allocated to a BGW, the subnet is sticky and will not change.

A dynamic DHCP pool can be created by navigating to **Gateway Management > Interfaces > DHCP**. Under **Pool Configuration** select the **Plus (+)** icon. The IPv4 DHCP server option also needs to be enabled:

FILTER GATEWAY MANAGEMENT
SD-Branch-DEMO (7 Total Devices | 0 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS) Selected Group Type is BG

Ports VLANs **DHCP** Pool Management GRE Tunnels Bulk configuration upload

▼ DHCP Server

IPv4 DHCP server:

Pool Configuration				
IP VERSION	NAME	NETWORK	DEFAULT ROUTER	
IPv4	vlan_1	--	192.168.1.1	
IPv4	vlan_99	192.168.99.0	192.168.99.1	

+

Figure 4-9 Gateway DHCP Pool Example

The following parameters must be configured for each dynamic DHCP pool:

1. **Pool Name** – The name of the pool that will be assigned to the dedicated VLAN interface.
2. **Network IP address type** – Dynamic.
3. **Starting network IPv4 address** – The first IPv4 address for the CIDR range.
4. **Ending network IPv4 address** – The last IPv4 address for the CIDR range.
5. **Hosts** – The number of hosts from the range to assign per BGW.

In the following example (Figure 4-10) a dynamic DHCP pool named **management-pool** has been configured which will be assigned to the management VLAN interface on a BGW group. In this scenario the BGW group has a total of 256 BGWs each requiring 13 management host addresses to be assigned per branch (14 host addresses including the BGW). To accommodate this requirement, the CIDR range 10.200.0.0/20 is allocated to the BGW group of which 13 hosts (/28) are assigned to each BGW. Additional DHCP options such as DNS Server(s) and Domain Name are also assigned (not shown).



Do not include the BGW when determining the host pool size. In the above example, allocating 13 hosts to the dynamic pool will result in a total of 14 host addresses being allocated (1 BGW + 13 hosts). Configuring the dynamic pool to allocate 14 host addresses would result in a /27 being allocated to each branch.

To add a dynamic DHCP pool, navigate to **Gateway Management > Interfaces > DHCP > DHCP Server > Pool Configuration** and click the blue **Plus (+)** icon. Clicking the icon will open the **Add New Pool Configuration** window where parameters administrators can select options related to the DHCP pool:

The screenshot shows the 'Add New Pool Configuration' window in the SD-Branch-DEMO interface. The window has a header with a filter icon and the text 'FILTER GATEWAY MANAGEMENT SD-Branch-DEMO (7 Total Devices | 5 Offline APs | 1 Offline SWITCHES | 1 Offline GATEWAYS)'. Below the header are navigation tabs: Ports, VLANs, DHCP (selected), Pool Management, GRE Tunnels, and Bulk configuration upload. The main content area is titled 'Add New Pool Configuration' and contains the following fields:

- IP version: IPv4 (dropdown)
- Pool name: management-pool
- Network IP address type: Dynamic (dropdown)
- Starting network IPv4 address: 10.200.0.0
- Ending network IPv4 address: 10.200.15.255
- Hosts: 13

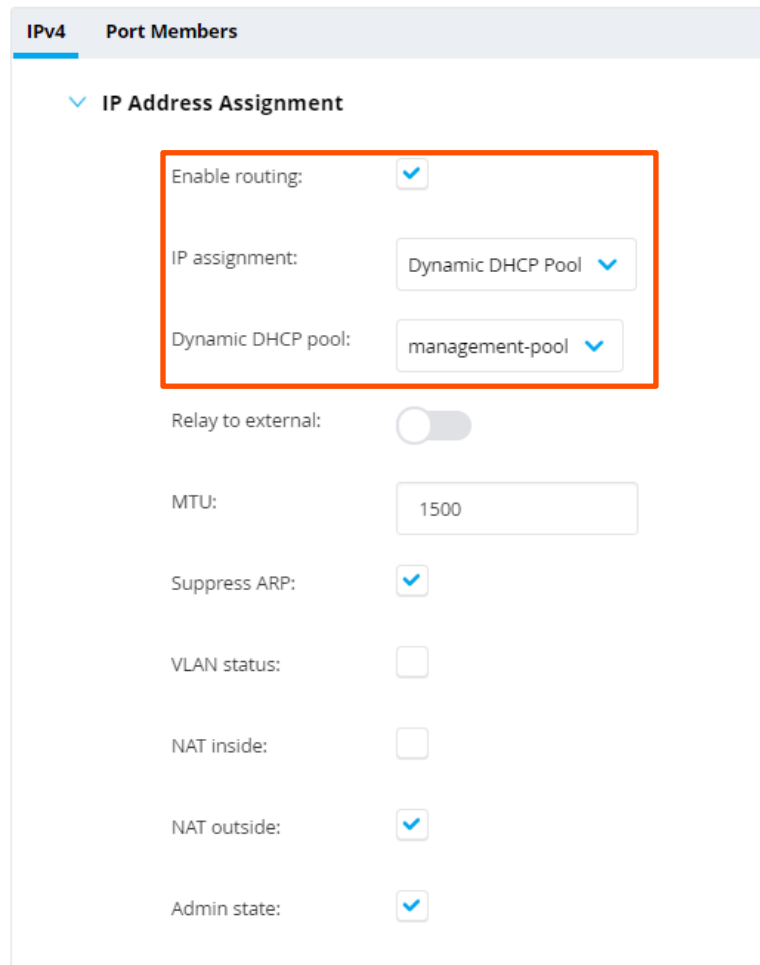
A red box highlights the Pool name, Network IP address type, Starting network IPv4 address, Ending network IPv4 address, and Hosts fields.

Figure 4-10 Dynamic DHCP Pool Configuration Example

Dynamic DHCP pools are assigned to LAN VLAN Interfaces within the group. Each LAN VLAN interface requiring a separate dynamic DHCP pool to be defined. An administrator can assign a DHCP Pool to a VLAN interface by navigating to **Gateway Management > Interfaces > VLANs** and performing the following steps:

1. Select the appropriate VLAN name under **VLANs > Name**
2. Select a VLAN ID under **VLAN IDs > ID**
3. Under **IPv4 > IP Address Assignment** check **Enable Routing** box
4. Set the **IP assignment** option to **Dynamic DHCP Pool**
5. Select the pool name using the **Dynamic DHCP Pool** drop-down

In this example the pool named **management-pool** has been assigned to VLAN interface 10. An example dynamic DHCP pool assignment is provided in Figure 4-11:



The screenshot shows the configuration page for a VLAN interface under the 'IPv4 Port Members' section. The 'IP Address Assignment' section is highlighted with a red box. The configuration includes:

- Enable routing:
- IP assignment: Dynamic DHCP Pool (dropdown)
- Dynamic DHCP pool: management-pool (dropdown)
- Relay to external:
- MTU: 1500
- Suppress ARP:
- VLAN status:
- NAT inside:
- NAT outside:
- Admin state:

Figure 4-11 Assigning Dynamic DHCP Pool to a VLAN Interface

System IP

The system-ip is a critical configuration element for each gateway operating as a VPNC or BGW. Each gateway uses one VLAN interface as its system-ip. By default this interface is used by the Aruba Gateway to communicate with network services such as RADIUS, syslog, TACACS+, and SNMP.

The VLAN interface selected for the system-ip on each gateway must have an IPv4 address assigned for the gateway to be fully functional. A gateway will not fully initialize unless the assigned VLAN interface is active and operational. Central does not allow the assignment of VLAN interfaces that are configured to dynamically obtain addressing from Internet service providers using DHCP or PPPoE for the system-ip.



Central will not apply any device or group level configurations to a new gateway unless the pending configuration includes the system-ip VLAN interface assignment. The system-ip must be provisioned in Central for all new Aruba Gateways being added to Central using either Gateway Pools, Bulk Configuration Upload, Dynamic DHCP Pools or Manual Assignment.

The Aruba SD-Branch solution supports the following methods for system-ip assignment:

- **VLAN Interfaces using Gateway Pools** – Central automatically allocates a host address to a dedicated VLAN interface from a range of addresses configured per group.
- **VLAN Interfaces using Bulk Configuration Upload** – VPNC or BGW device configuration is populated in Central using bulk configuration upload. The VLAN interface configuration and system-ip assignment is provisioned using a .CSV file that is uploaded to Central before the device is connected.
- **Manual VLAN Interface Assignment** – The system-ip is manually configured per device. The VPNC or BGW device configuration must be present in Central before the manual system-ip assignment can be made.
- **VLAN Interfaces using Dynamic DHCP Pools** – Central automatically allocates a subnet to a LAN VLAN interface on a BGW from a dynamic pool of addresses configured per BGW group. The BGW is allocated the first address in the subnet while the remaining addresses are allocated to users.

The system-ip must be configured using one of the above methods for all gateways. If no system-ip configuration is performed then Central will not push any pending device or group configuration to the gateways. The gateways will be stuck in a pending configuration state until the system-ip configuration is performed.



Changing the system-ip configuration for an existing device or group will require a reboot.

Gateway Pools

Aruba Central uses Gateway Pools to automatically allocate a host address to a dedicated VLAN interface from a preconfigured range of addresses for each group. Each pool includes a unique name along with start and end IPv4 addresses. The range of addresses defined for each pool must be non-overlapping.

Aruba recommends one Gateway Pool be configured per group since they are configured and applied to VLAN interfaces on a per group basis. The Gateway Pool must include enough IPv4 addresses to support all the Aruba Gateways assigned to the group. While a group can support multiple Gateway Pools, the Gateway Pool to VLAN Interface assignment would need to be performed at the device level.

Gateway Pools are created by navigating to **Gateway Management > Interfaces > Pool Management**, expanding **Gateway Pool**, and then select the **Plus (+)** icon:

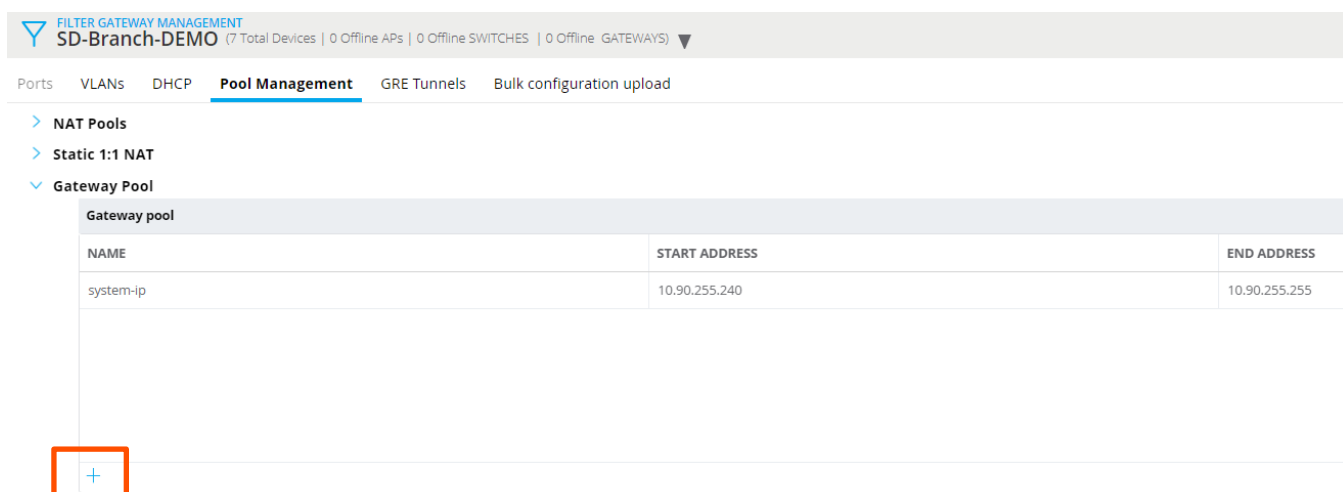


Figure 4-12 Creating Gateway Pools

For each Gateway Pool the following parameters must be configured (Figure 4-13):

1. **Pool Name** – The name of the pool that will be assigned to the dedicated VLAN interface
2. **Start IPv4 Address** – The first IPv4 address for the range
3. **End IPv4 Address** – The last IPv4 address for the range

The screenshot shows the 'Add New Gateway Pool' configuration form with the following values:

- Pool name: Sample Pool
- Start IP address: 172.16.200.1
- End IP address: 172.16.255.254

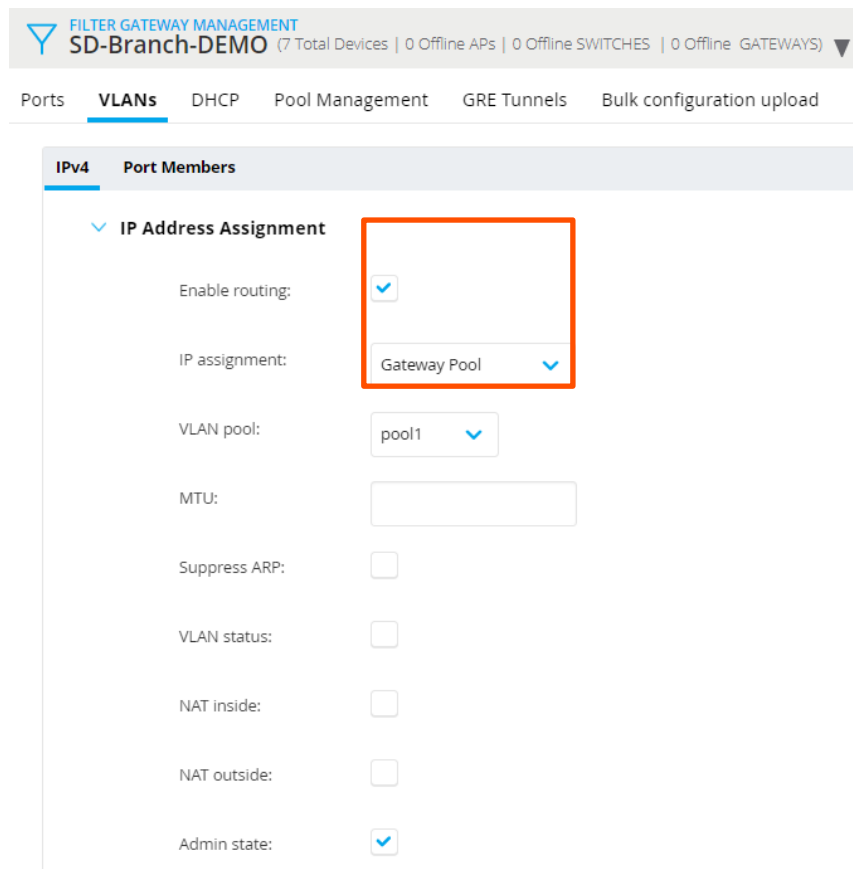
Figure 4-13 Gateway Pool Configuration

Gateway Pools are assigned to a VLAN Interface within the group that is dedicated for system-ip use. Aruba recommends using a VLAN ID that is easily identifiable and will not be confused with other VLANs configured for LAN or WAN use. An administrator can assign a Gateway Pool to a VLAN interface by performing the following steps:

1. Create a new dedicated VLAN ID. For example a **VLAN ID 3333** named **SYSTEM-IP** has been created.
2. Navigate to **Gateway Management > Interfaces > VLANs**

3. Select the appropriate VLAN under **VLANs**
4. Select the VLAN ID again under **VLAN IDs**
5. Configure the following parameters under **IPv4**:
 - Set the **Enable Routing** option to **enable**
 - Set the **IP assignment** option to **Gateway Pool**
 - Using the **VLAN Pool** drop-down, select the **Gateway Pool** name

In this example the pool named **pool1** has been assigned. An example of gateway pool assignment is provided in Figure 4-14:



The screenshot shows the configuration page for 'IPv4 Port Members' in the 'SD-Branch-DEMO' environment. The 'IP Address Assignment' section is expanded, and the 'IP assignment' dropdown menu is highlighted with a red box, showing 'Gateway Pool' selected. Other settings include 'Enable routing' (checked), 'VLAN pool' (pool1), and 'Admin state' (checked).

Figure 4-14 Gateway Pool Assignment

The final configuration step is to assign the VLAN interface as the system-ip. The VLAN interface is assigned by navigating to **Gateway Management > System > General > System IP Address**. Expand **System IP Address** and select the VLAN Interface from the drop down list (Figure 4-15). In this example **VLAN 3333** has been assigned:

- > Basic Info
- > Clock
- > Domain Name System
- > Dynamic Domain Name System

System IP Address

IPv4 address:

- > Capacity Threshold

Figure 4-15 System IP Address Assignment with Gateway Pools

Bulk Configuration Upload

VPNC or BGW VLAN interface configuration and system-ip can be configured using the bulk configuration template then be uploaded to Central. Bulk configuration can be used to pre-provision a VLAN interface and system-ip for new VPNCs or BGWs prior to deployment or change the system-ip on existing VPNCs or BGWs at any time. Changing the system-ip for existing devices requires a reboot.

To configure a system-ip on a gateway, populate the **MAC Address**, and **Controller VLAN** fields. The selected VLAN interface must have a static address or dynamic DHCP address assigned. A new VLAN interface is configured by populating the **VLAN ID**, **VLAN IP** and **VLAN Subnet** fields.

Figure 4-16 shows a template example that configures two VLAN interfaces for two BGWs. In this example VLAN interfaces **10** and **11** are configured on each BGW with static IPv4 addresses assigned. VLAN interface **10** is assigned as the system-ip for each BGW. Additional columns showing other configurations are hidden for clarity:

	A	B	C	D	E	F	G	V	W	X	AG
35	MAC Address	Group	Model	Hostname	VLAN Id	VLAN IP	VLAN Subnet	VLAN Id	VLAN IP	VLAN Subnet	Controller VLAN
36	00:0b:86:b8:66:e8	DEMO-BRANCH-GW	A7005	DEMO-BR1-GW	10	192.168.88.1	255.255.255.128	11	192.168.88.129	255.255.255.128	10
37	00:0b:86:be:63:e8	DEMO-BRANCH-GW	A7005	DEMO-BR2-GW	10	192.168.89.1	255.255.255.128	11	192.168.89.129	255.255.255.128	10

Figure 4-16 System IP Bulk Configuration Upload Template Example

Once the bulk configuration template has been uploaded to Central, the device configuration for each BGW in the template will include the hostnames, VLAN interfaces, static IPv4 address assignments, and the system-ip assignments. When the two BGWs first communicate with Central, their device and group configuration will be pushed and applied. The BGWs will reboot and come up using the VLAN 10 interface as their system-ip.

Dynamic DHCP Pools

Central uses dynamic DHCP pools to automatically allocate a subnet to a LAN VLAN interface on a BGW from a dynamic pool of addresses configured per BGW group. In each branch, the BGW is allocated the first address from the subnet while the remaining addresses are assigned to host devices (see VLAN interfaces section for more details). Dynamic DHCP pools providing a convenient way to automate addressing of LAN VLAN interfaces at branch sites.

If dynamic DHCP pools have been implemented in BGW groups then one of the dynamically addressed VLAN interfaces can be selected as the system-ip. Most deployments will select the management VLAN interface for this purpose. It's important to remember that addressing is non-deterministic and the branch subnet allocation is first come, first serve as each BGW is provisioned.

The VLAN interface enabled for dynamic addressing is assigned by navigating to **Gateway Management > System > General > System IP Address**. Expand **System IP Address** and select the VLAN Interface from the drop down list (Figure 4-17). In this example the management VLAN 99 has been assigned as the system-ip for the BGW group. Notice that no IPv4 address is listed for the VLAN interface as the addressing is dynamically assigned from Aruba Central:

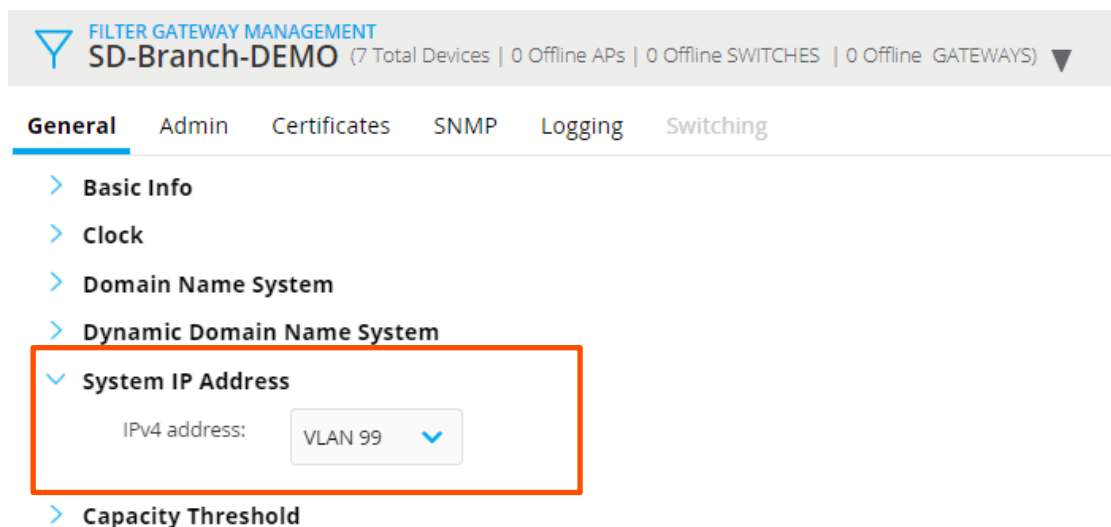


Figure 4-17 System IP Address Assignment with Dynamic DHCP Pools

Manual Assignment

A VLAN interface can be manually assigned as the system-ip to a device or group by navigating to **Gateway Management > System > General > System IP Address**. Expand **System IP Address** and select the VLAN Interface from the drop down list (Figure 4-18). In order to appear as an option in the drop down the VLAN interface must be enabled for IP routing and be configured with either a static address, gateway pool, or dynamic DHCP pool. Central will not permit selection of a VLAN interface that has been configured to use DHCP or PPPoE addressing:

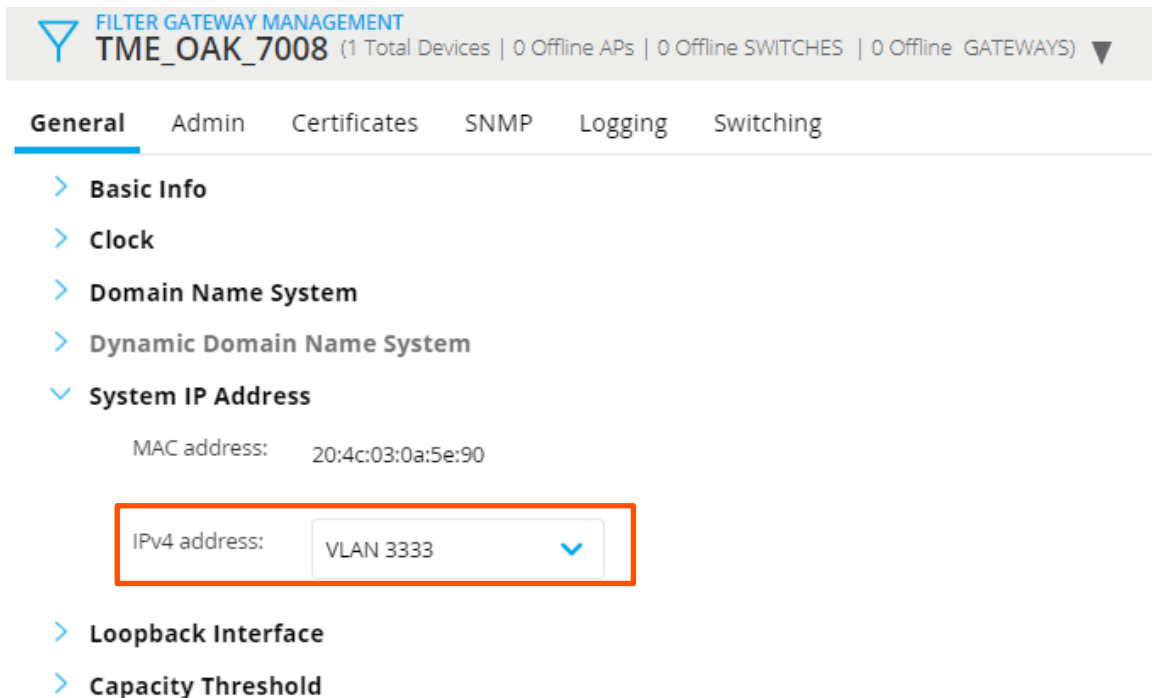


Figure 4-18 Manual System IP Assignment

Ports

Aruba gateways are connected to network devices and WAN services using Ethernet ports. Each port can be configured to be a member of a single VLAN (access) or multiple VLANs (trunk). The number of Ethernet ports and VLANs that are required for each SD-branch deployment is dependent on the data center and branch topology (refer to the [Reference Topologies](#) section of this document for additional information).

Port configuration is usually performed per VPNC or BGW group as it allows the port configuration such as mode, VLAN membership, trust, and policy assignments to be applied to all the VPNCs or BGWs in the group. If group configuration is used for ports they must be added prior to the configuration taking place. The number of ports added depends on the gateway model assigned to the group. Aruba does not recommend assigning different gateway models to a single group

due to the discrepancies in port numbers that are supported per platform. E.g., assigning 7005 and 7008s to a BGW group would not be recommended.

Ports are added to a VPNC or BGW group by navigating to **Gateway Management > Interfaces > Ports**. Click the blue **Plus (+)** icon and then select the number of ports requiring configuration based on the gateway model (Figure 4-19). In the example below four ports are being added to a BGW group supporting consisting of 7005 series Aruba Gateways:

The screenshot shows the 'FILTER GATEWAY MANAGEMENT' interface for 'SD-Branch-DEMO'. The 'Ports' tab is active, displaying a table of ports. A plus icon in the bottom left of the table is highlighted with an orange box. An orange arrow points from this icon to the 'New Port' configuration dialog. In the dialog, the text states: 'Gateway models support up to a maximum of 26 ports, so you can create and configure upto 26 ports. Select the ports you wish to configure based on the device model.' There is an unchecked checkbox for 'All 26 configurable ports'. Below it, four ports are listed with checked checkboxes: GE-0/0/0, GE-0/0/1, GE-0/0/2, and GE-0/0/3. These four ports are enclosed in an orange box. At the bottom right of the dialog are 'Cancel' and 'Save Settings' buttons.

PORT	TYPE	ADMIN S	TRUSTED	POLICY	MODE	NATIVE V	ACCESS	TRUNK V	TRUSTED V	SPANNING	DESCRIPTI
GE-0/0/0	LAN	Enabled	--	Not-definec	trunk	2	--	2-3,99	1-2,4-98,10	✓	GE0/0/0
GE-0/0/1	--	Enabled	--	Not-definec	access	--	1	--	--	✓	GE0/0/1
GE-0/0/2	--	Enabled	--	Not-definec	access	--	1	--	--	✓	GE0/0/2
GE-0/0/3	--	Enabled	--	Not-definec	access	--	1	--	--	✓	GE0/0/3
GE-0/0/4	--	Enabled	--	Not-definec	access	--	1	--	--	✓	GE0/0/4
GE-0/0/5	--	Enabled	--	Not-definec	access	--	1	--	--	✓	GE0/0/5

Figure 4-19 Adding Ports to a Group

Trust

Each port and VLAN on a gateway can be configured as Trusted or Untrusted. The Trust parameter determines how the gateway processes incoming user traffic. When a port or VLAN is configured as Untrusted, the gateway will track the user sessions for each IPv4 address. User devices are assigned a predefined role that determines which session ACLs will be applied to incoming and outgoing user traffic. The trust configuration for each port and VLAN will depend on the role of the gateway and what is connected to that port. Aruba recommends the following trust configuration for VPNC and BGW ports:

- **VPNCs** – Configure all ports and VLANs as **Trusted**
- **BGWs** – Configure all WAN ports and VLANs as **Trusted**
- **BGWs** – Configure all LAN ports as **Untrusted**

There is no reason to track the user sessions on VPNCs, therefore all ports and VLANs are configured as **Trusted**. This also applies to BGW and VPNC ports that are directly connected to WAN services. If a VPNC or BGW is directly connected to a public WAN service, Aruba recommends configuring and assigning a restrictive session ACL to the port. Aruba recommends configuring all BGW LAN ports as **Untrusted**. This will result in the BGW tracking all the user sessions for all internal IPv4 addresses. Each LAN VLAN requires its own AAA profile. Each AAA profile can trigger MAC, 802.1X, or captive portal authentication as well as determine an initial role assignment. Device and user authentication is completely optional.

Navigate to **Gateway Management > Interfaces > Ports**. Selecting the desired port will open a window below where the desired settings can be applied. Figure 4-20 provides the example configuration for a WAN port on a BGW. In this example the port and Access VLAN are configured as **Trusted**:

Trust:

Policy: Per-Session Internet-sacl

Mode: Access

VLAN: 4094

VLAN trust:

Policy > internet-sacl Rules					Drag rows to re-order
IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	
IPv4	any	any	svc-dhcp	permit	
IPv4	vpnc	any	any	permit	
IPv4	any	any	any	deny	

Figure 4-20 BGW WAN Uplink Port Configuration Example

A restrictive session ACL named **internet-sacl** is assigned to port in the above example since it connects to a public WAN service. The restricted session ACL applies the following conditions:

1. Permits DHCP for IPv4 addressing.
2. Permits all IP communication with the VPNC alias. The VPNC alias includes the public host IPv4 addresses of each VPN peer.
3. Denies and logs all other traffic.

Figure 4-21 provides a sample configuration for a LAN port on a BGW. In this example the port is configured as **Untrusted** while the branch VLANs are configured as **Trusted**:

The screenshot shows the configuration for a BGW LAN port. The 'Trust' setting is set to 'Untrusted' (indicated by a red box around the 'Untrusted' radio button). The 'Policy' is 'Not-defined', 'Mode' is 'Trunk', 'Native VLAN' is '10', and 'Allowed VLANs' is 'Allow specified VLANs'. Below these settings is a table with two columns: 'VLAN' and 'TRUSTED'. The table contains one entry: '10-11,255' in the 'VLAN' column and 'Trusted' in the 'TRUSTED' column. A '+' sign is visible at the bottom left of the table, indicating that more entries can be added.

VLAN	TRUSTED
10-11,255	Trusted

Figure 4-21 BGW LAN Port Configuration Example

Each VLAN in the above example is assigned an AAA Profile that determines the initial role for each host. AAA Profiles are configured per BGW group by navigating to **Gateway Management > Security > Role Assignment (AAA Profiles)**. Each AAA Profile includes an initial role assignment and optional authentication options. The example has the following configuration:

- **VLAN 10** – Is assigned a AAA Profile named **management** which assigns the initial role of **authenticated**.
- **VLAN 11** – Is assigned a AAA Profile named **employee** which assigns the initial role of **authenticated**.
- **VLAN 12** – Is assigned a AAA Profile named **guest** which assigns the initial role of **guest-logon**.

Figure 4-22 provides the AAA Profile example for the employee VLAN:

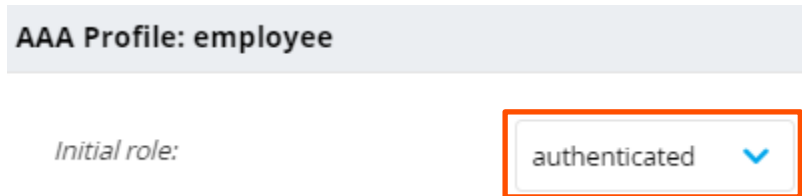


Figure 4-22 AAA Profile Configuration

The AAA profiles are assigned to VLANs per BGW group by navigating to **Gateway Management > Interfaces > VLANs**. Select the **VLAN Name**, **VLAN ID**, and then expand **Other Option**. The AAA profile is assigned using the **AAA profile** drop-down.

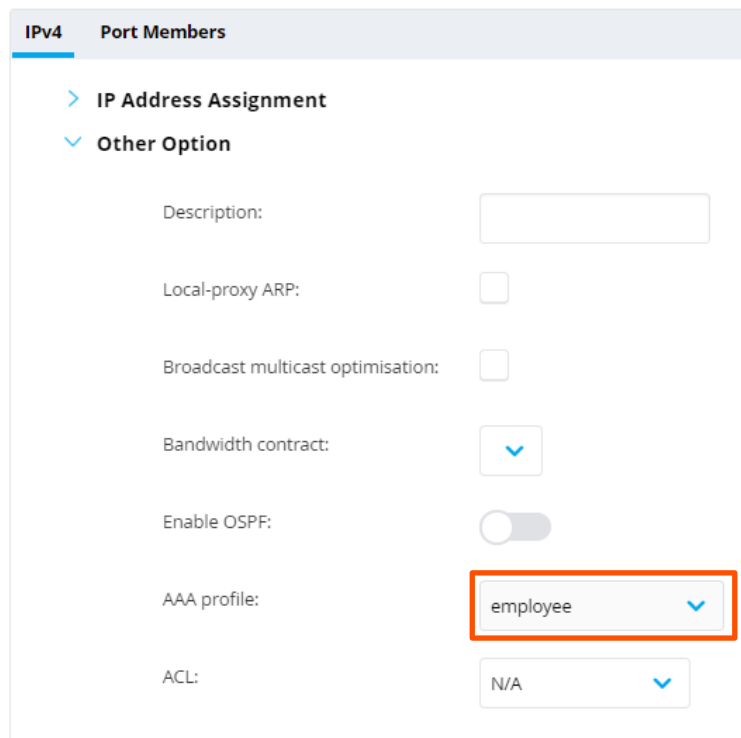


Figure 4-23 AAA Profile Port Assignment

VLAN Modes

Each port can be configured as either an access or a trunk port. Access ports carry traffic from a single VLAN while trunk ports can carry traffic from multiple VLANs. The mode configured for each port on VPNCs and BGWs will depend on the data center and branch topology. Most SD-Branch deployments will have a VLAN mode configuration similar to the following:

- **VPNCs** – Generally connected to the data center network using trunk ports. This can be a single port or multiple ports configured in a link aggregation group (LAG).
- **BGWs** – Are generally connected to one or more ArubaOS Switches using trunk ports and WAN services using access ports.

The Aruba SD-Branch solution is highly flexible and allows VPNCs and BGWs to be configured based on business and redundancy needs. E.g., a VPNC may be simultaneously connected to multiple devices in the data center such as an aggregation switch and edge-firewall while BGWs may be connected to an ArubaOS-Switch using multiple trunk ports with link aggregation or failover via spanning-tree protocol. There is no right or wrong way to connect gateways so long as networking best practices are followed.

The mode of a port on a VPNC or BGW group is configured by navigating to **Gateway Management > Interfaces > Ports**. Selecting the desired port will expose the port configuration options. Which VLAN options are available will depend on whether the mode is set to **Access** or **Trunk**:

Access Mode	Trunk Mode
VLAN – Select the individual VLAN ID to assign to the port.	<p>Native VLAN – Select the untagged VLAN assigned to the port (default 1).</p> <p>Allowed VLANs – Select Allow specified VLANs or Allow all. When assigning specific VLANs, all VLANs will be 802.1Q tagged on the port except for the native VLAN. Each allowed VLAN must be designated as Trusted or Untrusted.</p>

Table 4-1 Port VLAN Mode Configuration Options

Figure 4-24 shows an access port configuration in a BGW group connected to an MPLS WAN service. In this example, GE-0/0/2 is configured as an access port and assigned VLAN 3094. The GE-0/0/2 port connects to an existing MPLS-CE router installed at each branch site. A BGW port can be designated an access port by navigating to **Gateway Management > Interfaces > Ports**, selecting the desired port from the **Ports** list, and selecting **Access** from the drop down list under **Mode**. Both the port and the VLAN are trusted in this example:

Trust:

Policy:

Mode:

VLAN:

VLAN trust:

Figure 4-24 BGW Access Port Example

Figure 4-25 shows a trunk port configuration in a VPNC group that connects each L2 redundant VPNC to a data center aggregation switch. In this example GE-0/0/0 has been configured as a trunk port using native VLAN1 and specific VLANs 66, 3000, and 4000. A port can be designated as a trunk port by following the same process as an access port with the exception of selecting **Trunk** under the **Mode** option instead of **Access**. Both the port and the VLANs are trusted in this example:

Mode: Trunk ▾

Native VLAN: 1 ▾

Allowed VLANs: Allow specified VLANs ▾

VLAN	TRUSTED	
66,3000,4000	Trusted	✎ 🗑
+		

Figure 4-25 VPNC Trunk Port Example



The Native VLAN is not included in the Allow specified VLAN list so the port will discard any untagged traffic.

Branch Client Addressing

Clients at branch sites will either implement static IPv4 addressing or require dynamic addressing to be provided by a DHCP server. Aruba supports the following dynamic addressing methods for dynamic addressing in the branch:

1. **Centralized DHCP Server(s)** – LAN VLAN interfaces on the BGWs are configured with an IP-helper addresses pointing to centralized DHCP server(s) in the data center. All DHCP transactions are forwarded to the centralized DHCP server(s) through the VPN tunnels.
2. **Distributed DHCP Server(s)** – LAN VLAN interfaces on the BGWs are configured with an IP-helper address pointing to a local DHCP server deployed at each branch. All DHCP transactions are forwarded to the local DHCP server(s) through the BGW.
3. **Dynamic DHCP Pools** – Each BGW group is configured with one or more dynamic DHCP pools that are referenced by each BGW's VLAN interfaces (one per VLAN). Each dynamic DHCP pool is allocated a large CIDR range of addresses (example /20) of which a smaller

subnet is allocated to each branch (example /27). The BGW is assigned the first address from the subnet while hosts are assigned the remaining addresses. Addressing is non deterministic as each subnet is allocated on a first come, first served basis.

4. **Internal DHCP Server** – Each BGW is configured with local DHCP pools, exclusion ranges, and options for each VLAN. This configuration is performed per device since the DHCP configuration is typically unique per BGW. The DHCP configuration can be performed in Central (per BGW) or be configured using bulk configuration during provisioning.

Centralized and Local DHCP Servers

One or more DHCP addresses can be configured per VLAN interface for branches requiring dynamic host addressing using either centralized or local DHCP servers. The helper address defines the DHCP server IP address used for DHCP discover and request messages.

The VLAN interface on the BGW must be configured to use static IP addressing or a dynamic DHCP pool in order for DHCP helper addresses to be supported. The VLAN interface is configured per BGW group while the address assignments are typically configured in advance through a bulk configuration update. The DHCP server addresses that are configured must be reachable from the BGW either locally or through the overlay network. DHCP relay configuration is performed for each BGW group through the following steps:

1. Navigate to **Gateway Management > Interfaces > VLANs**
2. Select the **VLAN Name** then **VLAN ID** to expose the IPv4 configuration for that interface
3. Set the Relay to external slider to **On**
4. Click the **Plus (+)** icon to add one or more DHCP server IPv4 addresses (Figure 4-26)

In this example two DHCP servers have been defined so that are both reachable through the overlay network:



Figure 4-26 Configuring DHCP Relay



DHCP relay can be configured even if the BGW is providing DHCP services to devices. The DHCP messages can be used by some AAA servers such as Aruba ClearPass to profile client devices.

Dynamic DHCP Pools

Dynamic DHCP pools provide a convenient way to automate addressing of LAN VLAN interfaces for branch sites. Central uses dynamic DHCP to automatically allocate a subnet for each LAN VLAN interface on a BGW from a pool of addresses configured within each BGW group. Each BGW in the group is allocated a subnet on a first come, first served basis. The first address in the subnet is allocated to the VLAN interface on the BGW while the remaining addresses are allocated to hosts.

When using dynamic DHCP pools for host addressing, it's important to remember to size each subnet accordingly. Each dynamic pool is configured per BGW group, therefore the size of each allocated subnet is the same for each BGW in the group. The configuration must provide enough resources for the hosts requiring support today as well as provide room for growth in the future. When planning the network configuration it is important to keep in mind that one host address from the subnet is assigned to the VLAN interface on the BGW.

If the number of hosts per branch is highly variable for a deployment it may be advantageous to deploy multiple BGW groups. Each BGW group could include the necessary dynamic DHCP pool configuration to match the expected hosts for each class of branch (small, medium, large, etc.). This is the recommended approach to optimize address usage and minimize address waste.

If a single BGW group is implemented then the dynamic DHCP pool for each VLAN must be appropriately sized to accommodate the largest host count across all branches. E.g., if a branch deployment includes 120 sites and the largest employee host count at a single branch is 52, the dynamic DHCP pool hosts configuration for BGW group would be set to support 61 hosts (a /26 network provides a block size of 64 addresses, 2 are consumed for the network and broadcast, and one is reserved for the BGW). This will ensure the largest branch has adequate host addresses to support the 52 employees while reserving 9 additional host addresses for future growth.



Dynamic addressing using dynamic DHCP pools is covered in detail in the [VLAN Interfaces > Dynamic DHCP Pools](#) section of this document.

Integrated DHCP Server

Many SD-Branch deployments will implement an integrated DHCP server on the BGW to provide dynamic address assignment for hosts within the branch. The integrated DHCP server requires the VLAN interfaces on the BGW to be statically addressed. The configuration is unique to each BGW, therefore the VLAN interface and DHCP server pool configuration is performed per BGW at the device level. The configuration can be performed directly within Central or be performed through a bulk configuration upload.

The number of host addresses supported by the integrated DHCP server on a gateway is determined by the gateway hardware platform. Larger platforms will support more addresses than smaller platforms:

- **7005/7008** – Supports a maximum of 1,000 host addresses
- **7010/7024** – Supports a maximum of 2,000 host addresses
- **7030** – Supports a maximum of 4,000 host addresses

The integrated DHCP server is configured using one of three methods. The method that is used will depend on configuration needs and the DHCP options required:

- **Per VLAN Interface** – Allows configuration of basic DHCP server parameters directly on the VLAN interface. Each configuration results in a pool being automatically configured which can be modified as needed.
- **Per Pool** – Allows creation of more advanced configurations including pools, exclusions, and options.
- **Bulk Configuration Upload** – Allows configuration of basic DHCP server parameters and options for each VLAN interface in a CSV file that is uploaded to Central. The uploaded configuration results in pools being automatically configured which can be modified as needed.

Per VLAN Interface

Enabling the DHCP server per VLAN interface creates a basic configuration that provides clients with the minimum information required to communicate over the intermediate network. The integrated DHCP server is enabled on an individual BGW using the following steps:

1. Navigate to **Gateway Management > Interfaces > VLANs**
2. Select the **VLAN Name** then **VLAN ID** to expose the IPv4 configuration
3. Activate the **Act as DHCP server** slider and then define the following parameters:
 - **Pool Name** – A unique name for the DHCP pool (example “management”).
 - **Network** – The network prefix for the DHCP pool (e.g. “192.168.88.0”). This must match the subnet assigned to the VLAN interface.
 - **Netmask** – The network mask for the DHCP pool (e.g. “255.255.255.128”). The netmask must match the subnet assigned to the VLAN interface.
 - **Default Router** – The IPv4 address of the BGWs VLAN interface (e.g. “192.168.88.1”).
 - **DNS Servers** – One or more DNS server IPv4 addresses separated by spaces (e.g. “192.168.10.2 192.168.10.3”)

Figure 4-27 shows an example of a DHCP server configuration on a BGW. Note that the minimum amount of options are configured under the VLAN interface. If additional DHCP options need to be defined or exclusions made they can be configured by selecting the DHCP tab once the configuration has been applied:

The screenshot shows the 'IPv4 Port Members' configuration page. Under the 'IP Address Assignment' section, the 'Act as DHCP server' toggle is turned on and highlighted with a red box. Below it, a table of DHCP pool settings is also highlighted with a red box:

Network:	192.168.88.0
Netmask:	255.255.255.128
Pool name:	vlan_10
Default router:	192.168.88.1
DNS servers:	192.168.10.2 192.168.10.1

Multiple DNS Servers should be separated by spaces

Figure 4-27 Enabling the DHCP Server for a VLAN Interface



Configuring DHCP under the VLAN interface will automatically enable the IPv4 DHCP server on the BGW. No additional configuration is required unless addresses need to be excluded or additional options defined.

Per Pool

An administrator can create Individual DHCP pools, exclude addresses, or configure options by navigating to **Gateway Management > Interfaces > DHCP**. If no existing DHCP server configuration is applied, the **IPv4 DHCP server** parameter will be disabled and no pools will be defined. New pools may be added by clicking the blue **Plus (+)** icon. Existing pools are modified by selecting them from the table (Figure 4-28):

FILTER GATEWAY MANAGEMENT
Branch-5150 (1 Total Devices | 0 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS) Selected Device Type is BG

Ports VLANs **DHCP** Pool Management GRE Tunnels Bulk configuration upload

▼ DHCP Server
IPv4 DHCP server:

Pool Configuration				
IP VERSION	NAME	NETWORK	DEFAULT ROUTER	
IPv4	ap	10.51.10.0	10.51.10.1	
IPv4	ap-arubatme.com	10.51.11.0	10.51.11.1	
IPv4	vlan_15	10.51.15.0	10.51.15.1	
+				

Figure 4-28 Individual DHCP Pool Creation

Aruba recommends configuring the following parameters for each DHCP pool:

- **Pool Name** – A unique name for the DHCP pool (e.g. “management”).
- **Network IP address type** – Must be set to **Static**.
- **Network IP address** – The network prefix for the DHCP pool (e.g. “192.168.88.0”). This must match the subnet assigned to the VLAN interface.
- **Network IP mask** – The network mask for the DHCP pool (e.g. “255.255.255.128”). This must match the subnet assigned to the VLAN interface.
- **Default Router** – The IPv4 address of the VLAN interface on the BGW (e.g. “192.168.88.1”).
- **Import DNS from DHCP/PPPoE** – Enable if using DNS servers assigned by an ISP.
- **DNS Servers** – One or more DNS server IPv4 addresses separated by spaces (e.g. “192.168.10.2 192.168.10.3”)
- **Domain Name** – The DNS domain name for the organization (e.g. “arubanetworks.com”).
- **Lease Time** – The number of days, hours, minutes, and seconds each lease is valid.

Figure 4-29 shows an example of a DHCP pool configuration on a BGW. The pool configuration includes more DHCP options such as domain name, lease time and vendor specific DHCP options:

Pool Configuration > vlan_10

IP version: IPv4

Pool name: vlan_10

Network IP address type: Static

Network IP address: 192.168.88.0

Network IP mask: 255.255.255.128

Default routers: 192.168.88.1 (Multiple Default Routers should be separated by spaces)

Import DNS address from DHCP/PPPoE:

DNS servers: 192.168.10.2 192.168.10. (Multiple DNS Servers should be separated by spaces)

Domain name: arubanetworks.com

Import WINS server from DHCP/PPPoE:

WINS: (Multiple WINS Servers should be separated by spaces)

Lease time: 1 Days 0 Hours 0 Mins 0 Seconds

Pool type: -None-

OPTION	IP/TEXT	VALUE
150	ip	192.168.10.15

Option: +

Figure 4-29 DHCP Pool Configuration

Bulk Configuration Upload

Bulk configuration allows configuration for a VPNC or BGW to be pre-populated in a CSV file, uploaded to Central, and applied to the device configurations. This method allows an administrator to define the VLAN interfaces, IPv4 addresses, and DHCP pools in the CSV file for each VPNC or BGW prior to deployment. This can either be performed as one touch or incremental configuration.

Using bulk configuration upload requires an administrator to download the sample device template file, populate it with the appropriate information, and then upload the template back to Central. The device template can be downloaded by navigating to **Gateway Management > Interfaces > Bulk configuration upload**. If BGWs are already present in Central, select the blue **Download Device Template** option which will include the MAC addresses and groups for all existing devices.

To configure integrated DHCP services using the configuration template, for each VLAN interface the following columns must be populated:

- **VLAN Id** – The VLAN ID of the VLAN interface.
- **VLAN IP** – The IPv4 address assigned to the VLAN interface.
- **VLAN Subnet** – The Network Mask for VLAN interface.
 - **DHCP Pool Name** – A unique name for the DHCP pool.
- **DHCP Network** – The network prefix for the DHCP pool. This must match the subnet assigned to the VLAN interface.
 - **DHCP Mask** – The network mask for the DHCP pool. This must match the subnet assigned to the VLAN interface.
- **DHCP DNS Server** – One or more DNS server IPv4 addresses separated by spaces.
- **DHCP Domain Name** – The organizational DNS domain name.
- **DHCP Default Gateway** – The IPv4 address of the BGWs VLAN interface.

Figure 4-30 shows an example of a completed device template that includes the configuration for a single VLAN interface. Additional VLAN interfaces and associated DHCP configuration be provided by additional columns in the template:

	A	B	C	D	E	F	G	O	P	Q	R	S	T
35	MAC Address	Group	Model	Hostname	VLAN Id	VLAN IP	VLAN Subnet	DHCP Pool Name	DHCP Network	DHCP Mask	DNS Server 1	Domain Name	DHCP Default Ro
36	00:0b:86:b8:66:e8	DEMO-BRANCH-GA7005		DEMO-BR1-GW1	10	192.168.88.1	255.255.255.128	management	192.168.88.0	255.255.255.128	192.168.10.2	192.1arubanetworks.cc	192.168.88.1
37	00:0b:86:be:63:e8	DEMO-BRANCH-GA7005		DEMO-BR2-GW1	10	192.168.89.1	255.255.255.128	management	192.168.89.0	255.255.255.128	192.168.10.2	192.1arubanetworks.cc	192.168.89.1

Figure 4-30 DHCP Bulk Configuration Template Example

Excluded Addresses

There might be instances where it is advantageous to exclude ranges of addresses in certain branches for hosts using static addressing. This can be performed by navigating to **Gateway Management > Interfaces > DHCP > IPv4 Excluded Address Range**. By default, each DHCP pool will only exclude the host address of the VLAN interface on the BGW. To prevent the DHCP server from allocating specific ranges of addresses those addresses must be explicitly excluded. An exclusion can be added by selecting the blue **Plus (+)** icon at the bottom of the **IPv4 Excluded Address Range** table.

Figure 4-31 shows an example of excluded addresses for the management VLAN on the BGW. In this example the management VLAN interface is assigned the 192.168.88.0/25 subnet which is also used to manage ArubaOS-Switches and IAPs. To prevent the integrated DHCP server from assigning conflicting addresses, an exclusion has been configured on the BGW for the 192.168.88.1 – 192.168.88.19 range:

IPv4 Excluded Address Range

IPv4 EXCLUDED ADDRESS

192.168.88.1 192.168.88.19

+

Figure 4-31 DHCP Pool Excluded Addresses



Excluded ranges can also be configured for each pool using the bulk configuration template by adding the DHCP Exclude Start IP and DHCP Exclude End IP columns for each pool. The columns must be placed immediately next to the DHCP Default Router 1 column for each pool.

Wide Area Networks

Health Checks

Health checks must be enabled to determine the path availability of each WAN uplink. When enabled, the gateway will send UDP or ICMP probes to an IP or FQDN of a host to determine if the path is available to accommodate traffic. The primary use case for health checks are to verify that each ISP's network is operational and prevent branch traffic from being forwarded into a black hole.

Health checks are enabled per branch group by navigating to **Gateway Management > WAN > Health Check**. At a minimum a remote host IP or FQDN and the probe mode must be defined (Figure 4-32):

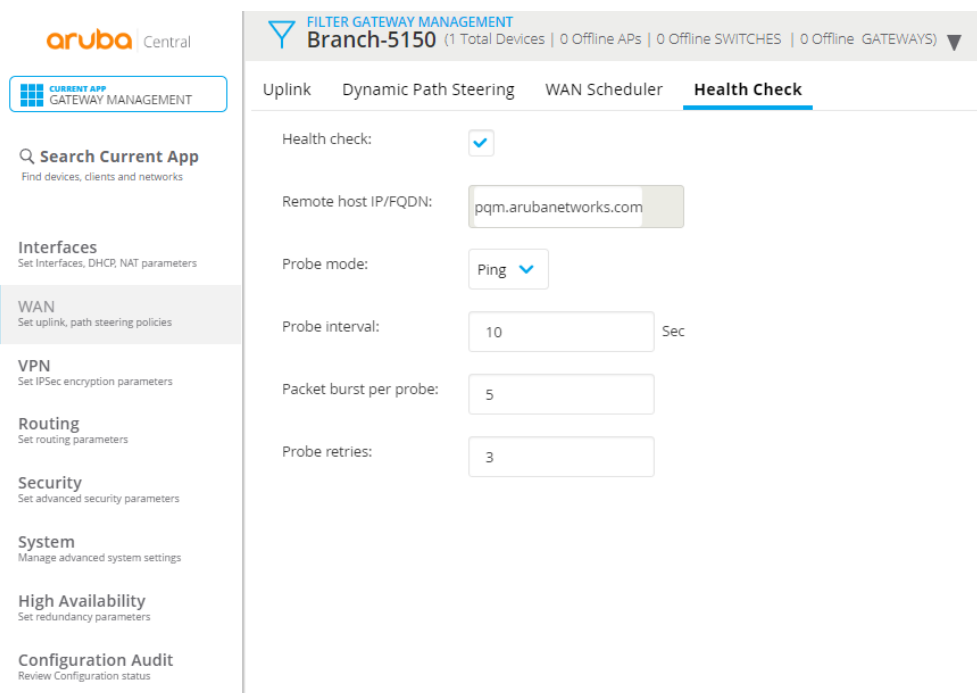


Figure 4-32 Enabling Health Checks

Aruba recommends using **pqm.arubanetworks.com** as the health-check remote host. This Aruba host can support either ICMP or UDP probes. UDP probe support is provided to accommodate internet environments where ICMP is not permitted out the branch. Any reachable IP or FQDN may be used, however the probe mode must be set to ICMP and the destination host must be reliable. As with SLA probes, Aruba does not recommend using Google DNS (8.8.8.8 or 8.8.4.4) or well-known public IP addresses as destinations since these services tend to throttle ICMP requests during peak congestion times.

When the defined health check IP or FQDN is not reachable over a WAN uplink, the default gateway associated with the WAN uplink is removed from the gateway's routing table. This will prevent the WAN uplink from being used for branch traffic that is NATed to the Internet or

management and control traffic that is destined for Central. Any established VPN tunnels will continue to operate as long as the VPNC is reachable over the WAN uplink.

BGWs also implement a few additional methods of determining link viability. When combined with the health check, this allows gateways in branches to verify first hop reachability, service provider path availability, data center reachability, and VPN tunnel failures:

1. **Default Gateway Monitoring** – The first hop router of WAN uplink is monitored via ARP and ICMP for reachability. This is used to detect last-mile failures or service provider router issues.
2. **VPNC Monitoring** – VPNC reachability and availability are monitored via Internet Key Exchange (IKE) dead peer detection (DPD). This is enabled by default under **Gateway Management > VPN > DPD**.

WAN and VPNC availability for each gateway can be seen in the **Monitoring and Reports** application. The **Network Health** view provides summary and per WAN uplink views.

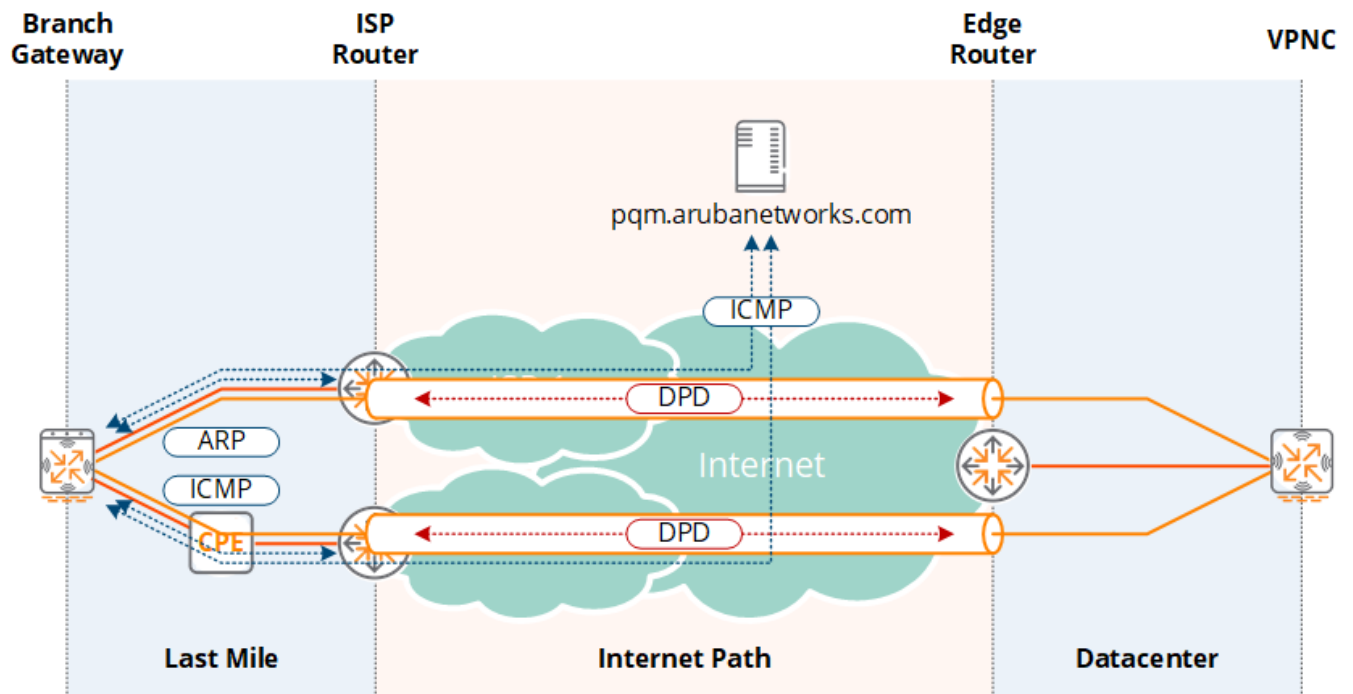


Figure 4-33 End-to-End Internet Monitoring



Aruba provides pqm.arubanetworks.com as a health-check host that can support either ICMP or UDP probes. UDP probes maybe required when ICMP is not permitted as well as to measure jitter.

Uplinks

Aruba gateways deployed in branches will include one or more physical ports that are connected to WAN services upon which the VPN network is established. These are referred to as WAN uplinks. The most common branch deployments include different types of WAN uplinks. The Aruba SD-Branch solution is flexible and can accommodate different combinations of WAN services. The primary limiting factor for the number of wired WAN uplinks on a gateway is the number of available Ethernet ports. E.g., smaller gateways such as the 7005 feature four Ethernet ports which are used for both WAN and LAN connectivity. Aruba branch gateways are currently limited to a maximum of 4 wired WAN uplinks plus one USB LTE modem (which can be either active or backup). A single physical port can also be configured to support multiple WAN uplinks if an external L2 breakout switch is employed, however special care must be taken to ensure the ZTP VLAN is untagged.

The most common types of WAN services that can be deployed include:

Private WAN	Internet
<ul style="list-style-type: none">• MPLS• Metro Ethernet• Point-to-Point Leased Lines• Packet Switched Networks (ATM, Frame Relay, etc.)	<ul style="list-style-type: none">• Cable (DOCSIS)• DSL (ADSL, HDSL, VDSL, etc.)• Fiber to the Home• Satellite Internet• Wireless Internet

Table 4-2 *Types of WAN Uplinks*

Aruba gateways can connect to any WAN service that provides an Ethernet handoff. A WAN service can either be directly connect to the gateway with no additional hardware or require an external router or CPE device (such as a modem). LTE services can be connected using a compatible USB modem or via Ethernet using an external LTE gateway. WAN services such as MPLS implementing leased lines will require an external router.

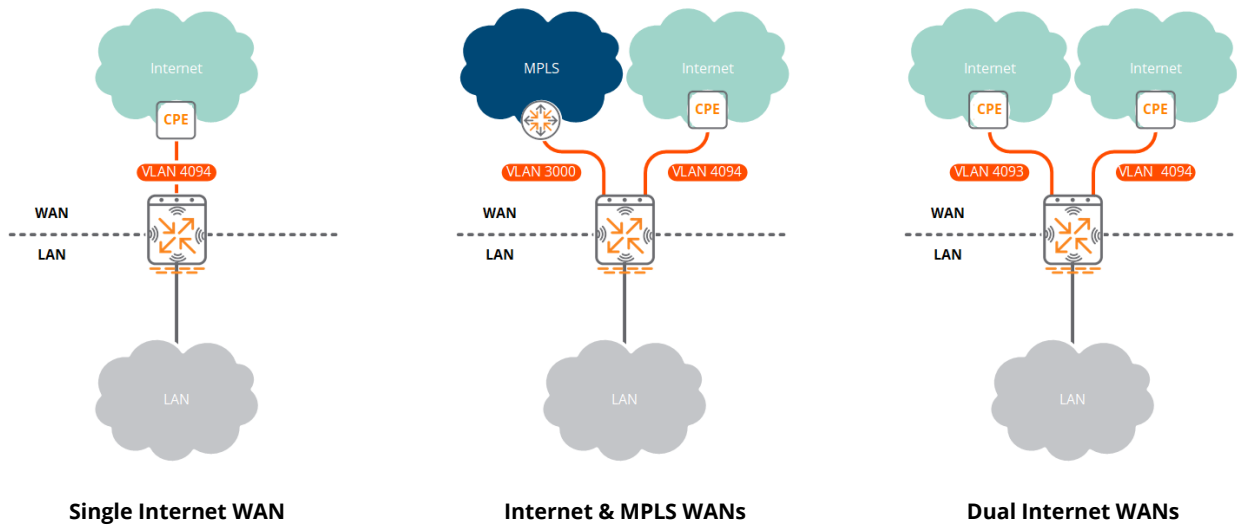


Figure 4-34 WAN Uplink Examples

How branches are connected will be unique to an organization’s business requirements, geographic locations, and availability needs. A deployment may include Internet and MPLS WAN services provided by common tier 1 service providers or WAN services from multiple service providers based on each branch’s location and service availability. BGWs are primarily configured using groups and different types of WAN options available at branch sites will influence the numbers of groups that are defined.

Link Type

Each WAN service that connects to a BGW requires an uplink to be defined. One of the key parameters that must be assigned to each WAN uplink is the link type. The link type value is used to identify groups of similar uplinks in DPS policies when a load balancing action is required. Each WAN uplink requires one of the following link types to be assigned:

- MPLS
- INET
- LTE
- Metro-Ethernet

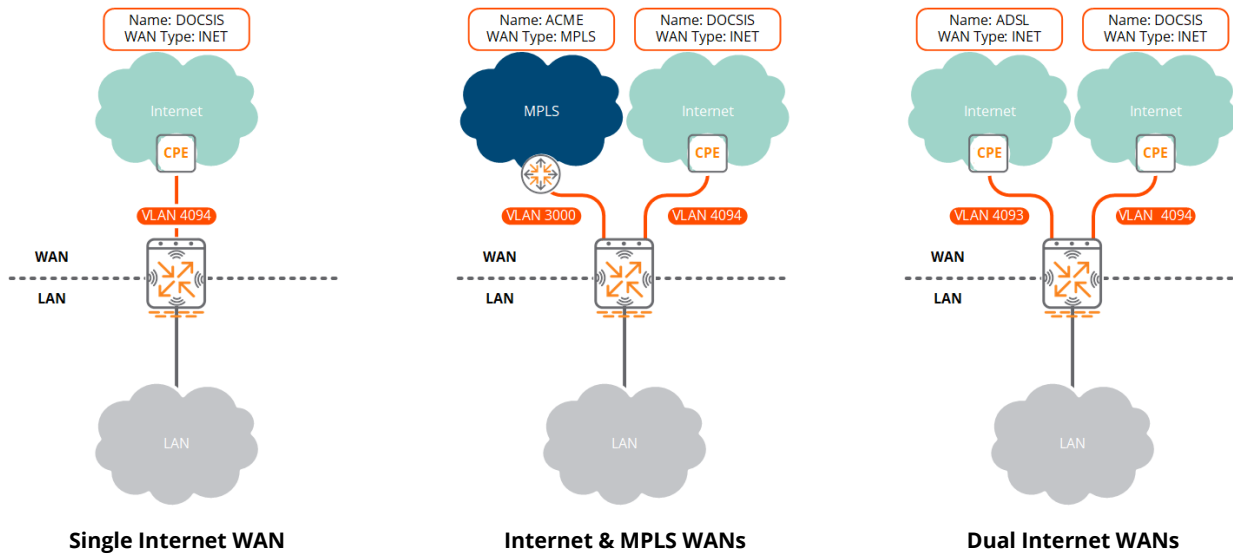


Figure 4-35 WAN Uplink Type Examples

DPS policies provide special path selection tags that allow the primary, secondary, and tertiary paths to be groups of uplinks. The path selection tags allow administrators to select groups of links of a specific type (INET, MPLS, etc.) or all uplinks. When one of these tags is used for path selection in a DPS policy, traffic is load balanced between the active WAN uplinks using that link type. E.g., if the primary path selection for the DPS policy is set to **ALL_INET**, traffic that matches the DPS policy will be load balanced between active WAN uplink interfaces with the link type **INET**. These special path selection tags include:

- ALL_UPLINKS
- ALL_INET
- ALL_MPLS
- ALL_METRO
- ALL_LTE

The **ALL_UPLINKS** path selection tag is unique and applies to all active WAN uplinks. When the **ALL_UPLINKS** tag is used in a DPS policy, traffic will be load balanced traffic across all active WAN uplinks regardless of their link type.

Adding WAN Uplinks

WAN uplinks are defined per branch group by navigating to **Gateway Management > WAN > Uplink** (the Uplink tab is selected by default). This page displays compression and load balancing configuration along with a table containing the WAN uplinks that have been defined for the group. New uplinks are added by selecting the blue **Plus (+)** icon (Figure 4-36). Each branch gateway can support a maximum of four wired WAN uplinks plus one USB LTE modem (either active or backup):

FILTER GATEWAY MANAGEMENT
Branch-5150 (1 Total Devices | 0 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS) ▼

Uplink Dynamic Path Steering WAN Scheduler Health Check

Compression:

Loadbalancing mode: Round robin ▼

Uplink VLANs

LINK	ID	OPERATION STATE	BACKUP LINK	WEIGHT
Wan_INET	4094	✓		10

+

Figure 4-36 WAN Uplink Configuration

Each WAN uplink requires the following mandatory configuration:

1. **Link Type** – Used for load balancing
2. **Link Name** – Unique identifier for the WAN uplink
3. **Interface VLAN ID** – The VLAN interface assigned to the WAN uplink

Aruba recommends assigning a unique link name to each WAN uplink that clearly represents the WAN service type. This could be the service provider name or the connection type. Central will automatically append a suffix to the name which includes the link type. E.g., naming a WAN uplink “ACME” and setting the type to ‘MPLS’ will result in the name “ACME_MPLS”. Therefore it is not recommended to name links MPLS or Internet as this will result in confusing duplicate names such as “Internet_INET”.

The **Interface VLAN ID** requires the existence of VLAN and VLAN interface for the branch group prior to creating an uplink. Each WAN uplink should be assigned a unique VLAN interface. Two uplinks cannot be assigned to the same VLAN ID.

Add Uplink

Link type: MPLS ▼

Link name: ACME

Interface VLAN ID: 255 ▼

Figure 4-37 Adding a WAN Uplink

Backup Links

When adding a new uplink, administrators can optionally specify the WAN uplink as a backup link. Unlike normal WAN uplinks, a backup link will not transition into an operational state until all higher weighted WAN uplinks fail. Failure conditions include physical failures such as an Ethernet link loss or path failures detected by health-check probes. Backup links are especially useful for branch deployments implementing LTE or dial-up services which should only be activated as a last resort (Figure 4-38).

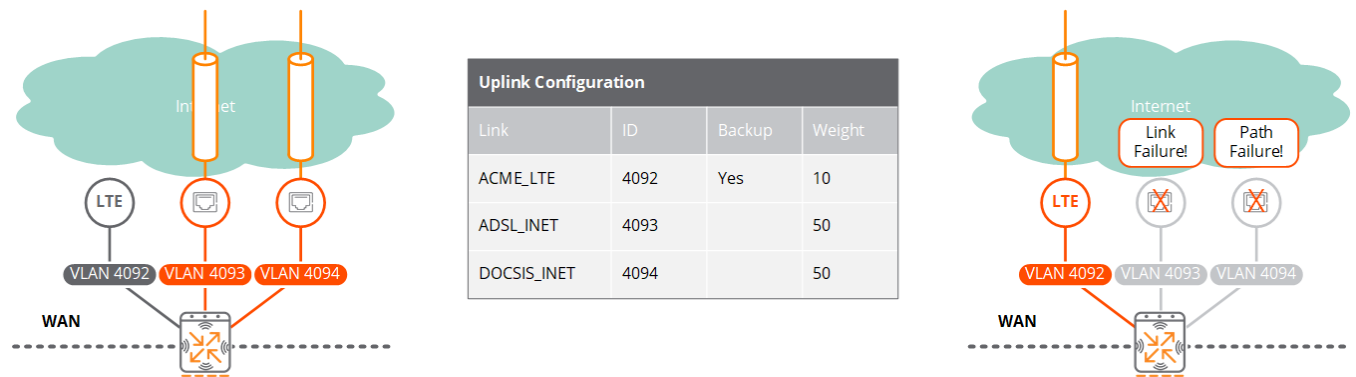


Figure 4-38 Backup Link Usage Example

One advantage of setting a WAN uplink as a backup link is that the gateway will not forward any traffic out the backup link during normal operation. The WAN uplink will obtain an IPv4 address but not forward any branch traffic out the uplink until it transitions to an operational state. This includes establishing a VPN tunnel and sending probes.

A WAN uplink can be designated as a backup link when adding a new uplink or by modifying an existing uplink by selecting the **Use only as backup link** checkbox option (Figure 4-39). There are no restrictions on which types uplinks can be selected as backup links or on how many backup links can be defined. Any uplink can be configured as a backup link as long as the uplink configuration includes one non-backup link.



If a deployment includes multiple backup links the backup links can be weighted so that there is a primary and secondary backup link. A backup link will only become active if all other active uplinks fail.

The screenshot shows the 'Add Uplink' configuration form with the following fields and values:

- Link type: LTE
- Link name: ACME
- Connection type: USB (selected)
- Interface VLAN ID: 4095 (with a note: This VLAN is reserved for LTE USB)
- Use only as backup link: (highlighted with a red box)
- Weight: 10

Figure 4-39 Backup Link Configuration Example

General Uplink Parameters

WAN Compression

WAN compression is enabled by default and applies to IP traffic that is encapsulated and forwarded through the VPN tunnels established between gateways. WAN compression is not applied to IP traffic forwarded directly to the Internet or to IP traffic forwarded through VPN tunnels established to non-Aruba gateways.

WAN compression attempts to reduce the size of the IP payload to optimize the WAN bandwidth between the branch and corporate networks. The compression efficiency varies depending on the traffic type, but real-world scenarios typically achieve a 40-60% increase in bandwidth efficiency. Dynamic compression is used for the IP payload to achieve a high compression ratio. No compression is applied to data such as image files that might already be in a compressed format as data of this nature does not compress well and may even increase in size. Dynamic compression is also not applied to encrypted traffic such as HTTPS or VPN sessions forwarded through the overlay network.



Load Balancing Algorithm Selection

Most branch deployments will implement one or more DPS policies to determine how the WAN paths are selected for branch users accessing applications in the corporate office or internet. Each DPS policy can select primary, secondary, and tertiary WAN paths which can be individual WAN uplinks or a group of WAN uplinks. When a group of WAN uplinks are selected the gateway will perform a load balancing action. Matched traffic will be distributed between the active WAN uplinks in the group. The load balancing algorithm determines how sessions are distributed between the active WAN uplinks in the group (Figure 4-40).

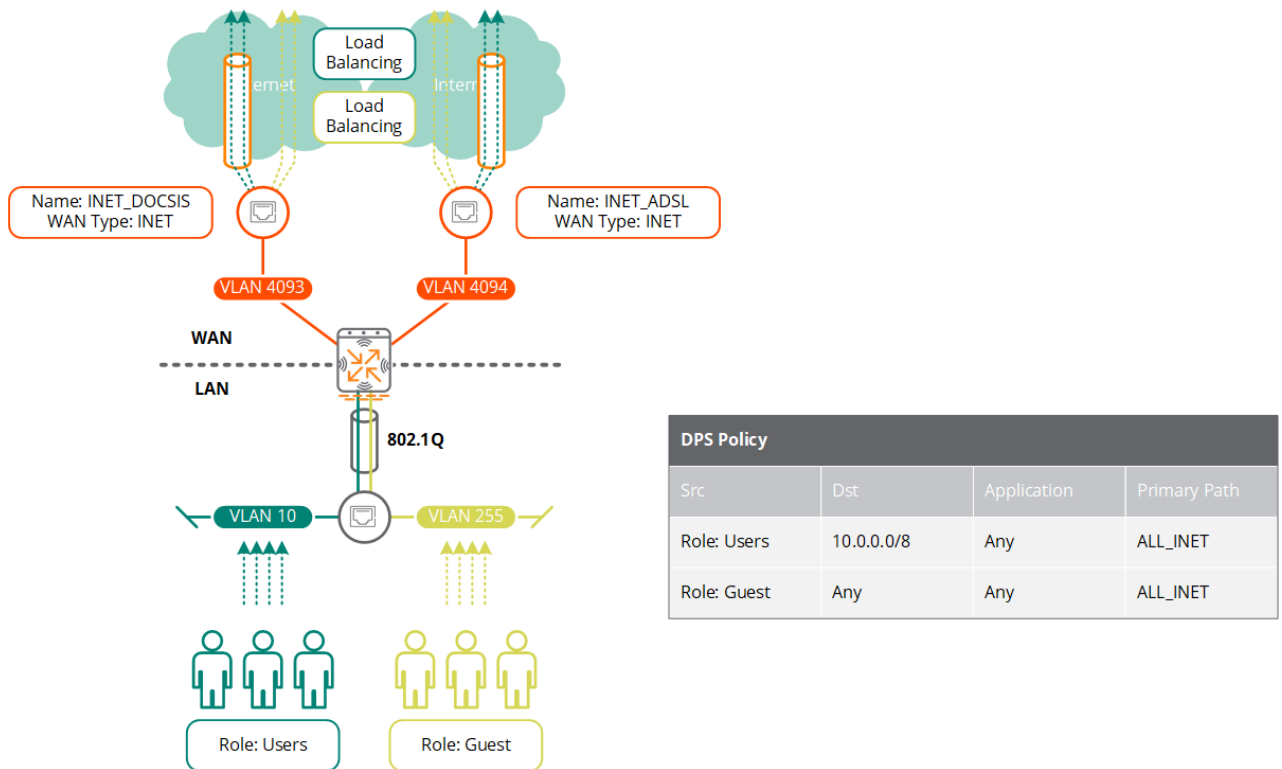


Figure 4-40 Load Balancing with DPS Policy Example

A load balancing action may also be performed if no matching DPS policy is defined when two or more paths exist to the destination. E.g., the gateway has two Internet WAN uplinks and no DPS policy has been defined for guest users to access the Internet. The gateway in the branch will load balance the guest user Internet traffic between the Internet WAN paths using the selected algorithm (Figure 4-41).

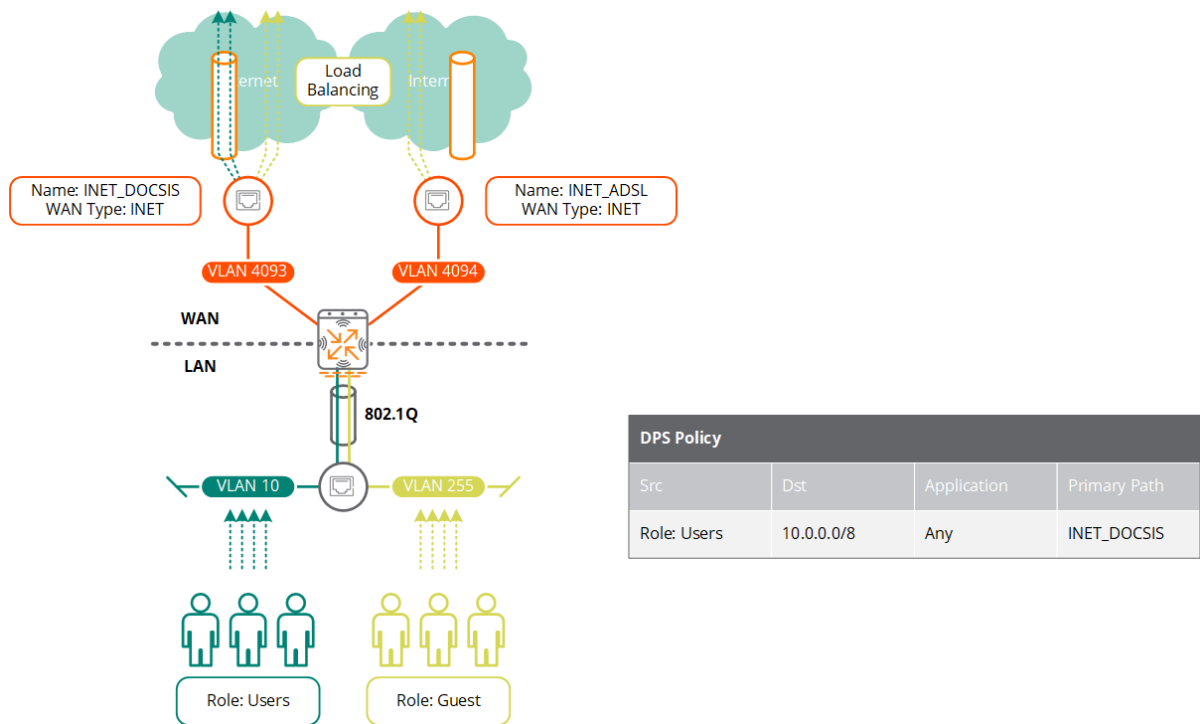


Figure 4-41 Load Balancing Without DPS Policy

Aruba gateways support three load balancing algorithms with the Round Robin algorithm selected by default. Aruba recommends implementing the Uplink Utilization algorithm for most deployments which accounts for the WAN service speed when making path selection. However, administrators should select the appropriate load-balancing algorithm that best meets the needs of their organization. The load balancing mode for an uplink can be selected by navigating to **Gateway Management > WAN > Uplink** and selecting the desired algorithm from the drop down list under **Loadbalancing mode**.

Round Robin Algorithm

The Round Robin algorithm sequentially distributes outbound traffic between each active WAN uplink. E.g., INET_ISP-A, INET_ISP-B, INET_ISP-A, INET_ISP-B etc. Round Robin is the simplest algorithm to configure and implement, but may result in uneven traffic distribution over time.

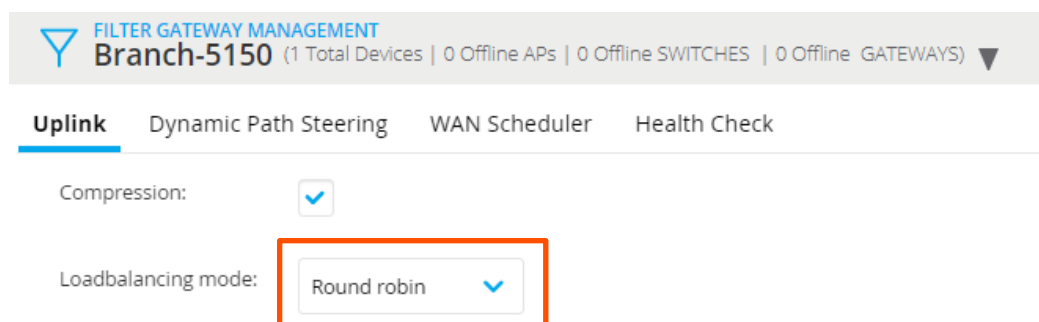
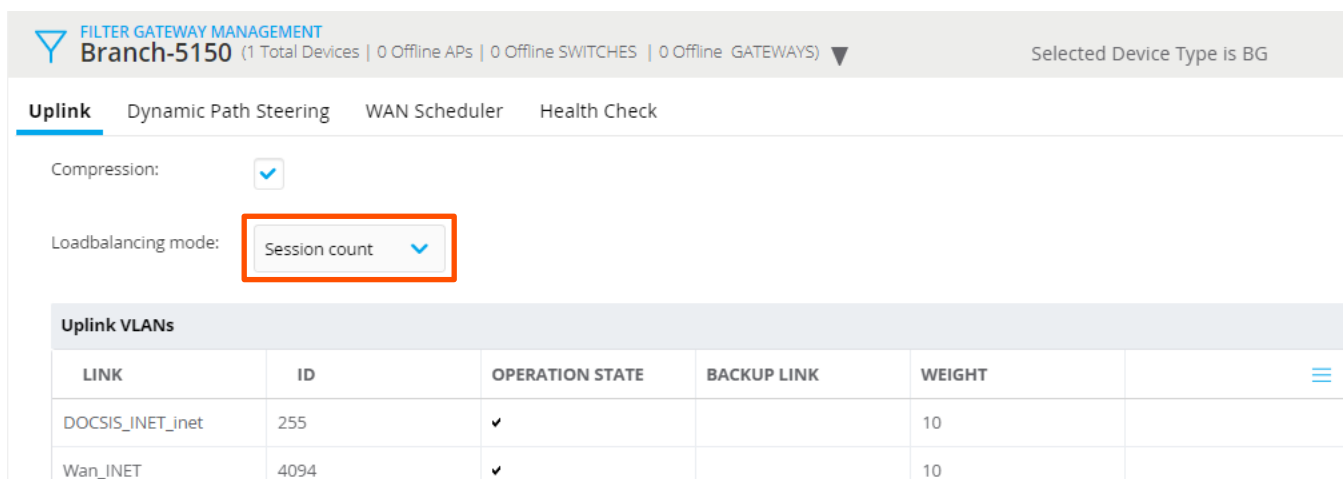


Figure 4-42 Selecting Round Robin as the Load Balancing Algorithm

Session Count Algorithm

The Session Count algorithm distributes outbound traffic between active WAN uplinks based on the number of sessions managed by each link. The algorithm will attempt to ensure that the session count on each active WAN uplink is within 5% of the other active WAN uplinks.

The session count algorithm optionally allows for weights to be assigned to each WAN uplink. E.g., assigning a weight of 80 to INET_ISP-A and a weight of 20 to INET_ISP-B would result in an 8:2 (i.e. 4:1) session ratio where for every 4 sessions forwarded out INET_ISP-A would result in 1 session being forwarded out INET_ISP-B.



Filter Gateway Management
Branch-5150 (1 Total Devices | 0 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS) Selected Device Type is BG

Uplink Dynamic Path Steering WAN Scheduler Health Check

Compression:

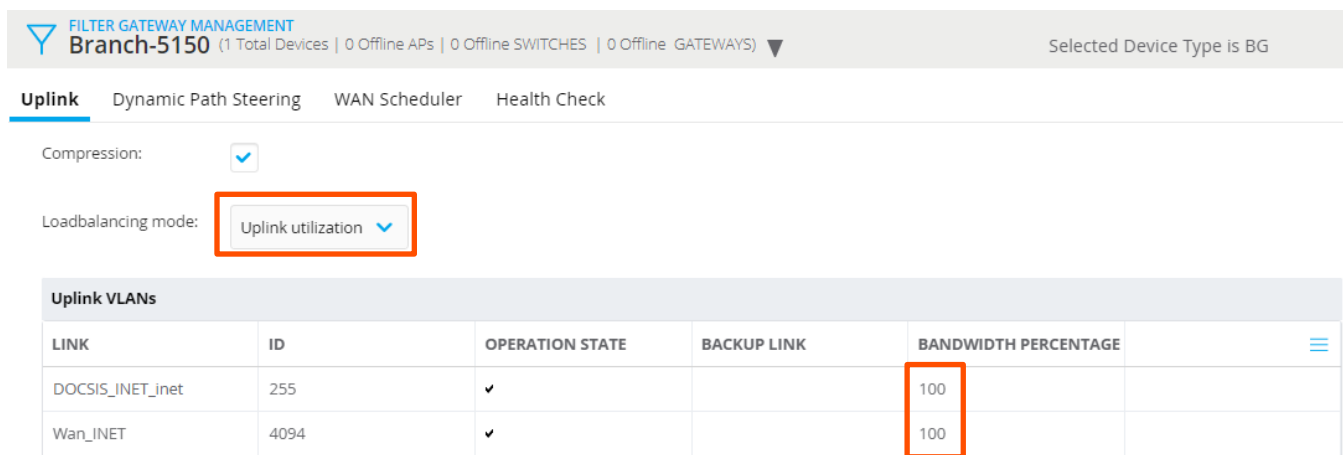
Loadbalancing mode: **Session count**

Uplink VLANs					
LINK	ID	OPERATION STATE	BACKUP LINK	WEIGHT	
DOCSIS_INET_inet	255	✓		10	
Wan_INET	4094	✓		10	

Figure 4-43 Selecting Session Count as the Load Balancing Algorithm

Uplink Utilization Algorithm

The Uplink Utilization algorithm 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. Once the bandwidth threshold has been exceeded, that WAN uplink is no longer considered available.



Filter Gateway Management
Branch-5150 (1 Total Devices | 0 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS) Selected Device Type is BG

Uplink Dynamic Path Steering WAN Scheduler Health Check

Compression:

Loadbalancing mode: **Uplink utilization**

Uplink VLANs					
LINK	ID	OPERATION STATE	BACKUP LINK	BANDWIDTH PERCENTAGE	
DOCSIS_INET_inet	255	✓		100	
Wan_INET	4094	✓		100	

Figure 4-44 Selecting Uplink Utilization as the Load Balancing Algorithm

A link speed to each WAN uplink in order for the uplink utilization algorithm to work correctly. The WAN link speed is calculated based on the negotiated speed of the Ethernet port by default. However, if the WAN service speed is lower than the negotiated PHY rate, the upload WAN speed must be defined for each WAN uplink so that the algorithm can correctly calculate the utilization.

Dynamic Path Selection

Aruba gateways can implement DPS policies to determine the WAN uplinks that are selected for specific users, applications, and destinations. The selected forwarding path could be a single WAN uplink or traffic could be load balanced between a group of WAN uplinks. The destination IP address of the traffic will determine if the traffic is steered towards a VPN tunnel or forwarded directly to the Internet. The DPS policy effectively selects an uplink and the gateway's routing table or policy based routing (PBR) rules will determine the next hop. DPS policies are defined per branch group by navigating to **Gateway Management > WAN > Dynamic Path Steering**. A new DPS policy is created by clicking the blue **Plus (+)** icon.

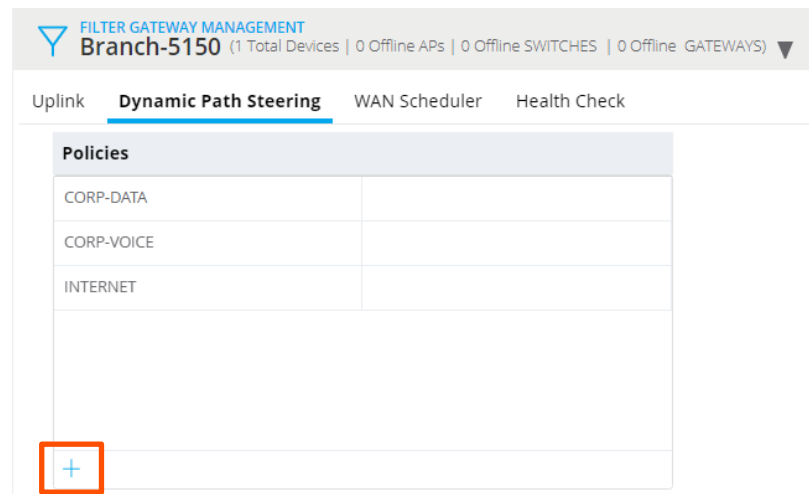


Figure 4-45 Configuring Dynamic Path Steering

Each DPS policy requires the following configuration to be defined:

1. A unique name that identifies the DPS policy
2. One or more traffic specification rules to identify the traffic matching the DPS policy
3. Optional SLA profile which influences WAN path selection for interesting traffic based on the WAN performance of each path.
4. Path selection which determines the primary, secondary, and last resort WAN uplinks that should be used

Each DPS policy is evaluated in order (highest to lowest) in a similar manner to IP access control lists. When a branch client accesses a new application the first DPS policy with a matching traffic specification rule will be selected for that session. The gateway will then make an appropriate path

selection from the primary, secondary, and last resort path based on SLA thresholds and WAN uplink availability.

If no traffic specification rules in any DPS policy are matched for the session, the traffic is subjected to normal routing will be forwarding based on the gateway's routing table or PBR rules (if defined). If multiple paths exist to the destination IP address then the gateway will load balance the traffic based on the selected load balancing algorithm.

Aruba recommends creating DPS policies that group specific applications to preferred path selections. Most branches will include multiple WAN uplinks which are better suited for specific applications. E.g., the MPLS network may offer the best performance for transactional or real-time applications while the high-speed Internet connection is adequate to support bulk data and web based applications.

Traffic Specification Rules

Each DPS policy includes one or more traffic specification rules which determine the interesting traffic that must be matched for the DPS policy to be applied. The traffic specification rules are evaluated in order from highest to lowest. Aruba recommends defining the most specific rules first and least specific rules last in a similar manner to configuring an ACL. Each DPS policy can support a maximum of 64 traffic specification rules. Traffic specification rules can be defined for each DPS policy through the following steps:

1. Navigate to **Gateway Management > WAN > Dynamic Path Steering**
2. Select the appropriate policy under **Policies** and click on the blue pencil icon under the **Traffic Specification Rules** window that appears
3. Click the blue **Plus (+)** icon under **Traffic Specification Rules for <<policy name>> Policy**

Source	Destination	Application
<ul style="list-style-type: none"> • Any • User • Host • Network • User Role 	<ul style="list-style-type: none"> • Any • Host • Network 	<ul style="list-style-type: none"> • Any • Application Name • Application Category • Web Category / Reputation • UDP Port(s) • TCP Port(s) • Service

Table 4-3 Traffic Specification Rule Elements

One useful feature when defining traffic specification rules is the ability to match based on user roles. When dynamic segmentation is deployed in a branch, the traffic from each wired and wireless device is tunneled to the BGW where it is assigned a role and associated policies. Defining traffic specification rules based on user roles can greatly simplify the overall creation and management of DPS policies as it eliminates the need for creating branch-specific rules that match on source IP addresses or networks:

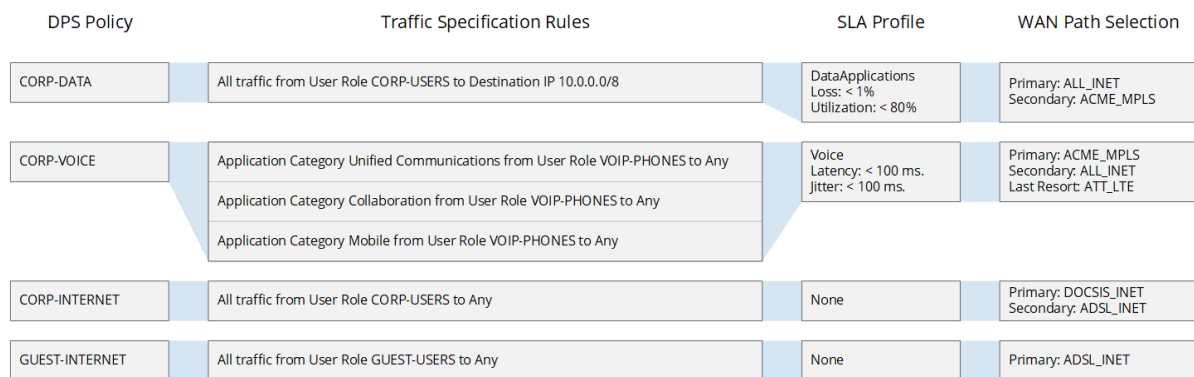


Figure 4-46 DPS Policy Example with User Roles



Traffic specification rules using Application Categories and Web Categories or Web Reputations require the appropriate firewall features to be enabled in the BGW group. These features can be enabled by navigating to **Gateway Management > Security > Applications > Application Visibility**.

DPS policies created for corporate traffic that is reachable over the VPN network should include the corporate network as the destination (for example **10.0.0.0/8** or **172.16.0.0/20**). This follows the more specific to least specific policy order recommendation and will ensure that the correct DPS policy is selected. DPS policies for sessions destined to the internet will require a destination of **Any**. The exception would be for sessions destined for a cloud or SaaS provider where a specific destination can be defined. Most cloud providers will publish their CIDR blocks for each geographic region and zone.

SLA Profiles

Each DPS policy can optionally be assigned an SLA profile that influences path selection for both new and existing sessions defined in the policy. When a SLA profile is assigned the gateway will monitor each of the primary and secondary WAN paths defined in the policy to ensure that the performance of each uplink meets the latency, jitter, loss, and utilization thresholds in the assigned SLA profile. The gateway utilizes UDP or ICMP probes to the VPNC or user defined FQDN to monitor each WAN path.

If the WAN path exceeds one or more of the defined thresholds in the SLA profile it is considered in violation of the policy. Existing as well as new sessions on the affected WAN path will be moved

to an alternative path that meets the defined thresholds. Depending on the WAN path configuration, one of the following options will occur for the sessions:

1. Moved to an alternative primary WAN path (if multiple primary paths are defined)
2. Moved to the secondary WAN path

If no primary or secondary WAN paths are available that meet the defined thresholds then traffic is load balanced between the available WAN paths.

The gateways include three default SLA profiles (Table 4-4) which can be used as default or be modified to suit a deployment's requirements. Administrators may also create and assign custom SLA profiles if desired. The default SLA policies can be used to address most use cases:

Name	Latency (ms)	Jitter (ms)	Loss (%)	Utilization (%)
BestForInternet	-	-	1	80
BestForVoice	100	100	-	-
HighlyAvailable	150	150	-	-

Table 4-4 Default SLA Profiles

Each SLA profile allows for definition one or more threshold values. The SLA profile may consist of a single threshold or multiple thresholds as required. Each threshold value defines a ceiling that must be reached before the WAN path is considered in violation of the SLA. E.g., if the SLA profile includes a packet loss threshold of 1% and the WAN path is reporting a 2% loss, the WAN path will be considered in violation. If the loss threshold is 5% and the WAN path is reporting a 2% loss, the WAN path will not be considered in violation.

No SLA profile is assigned by default when creating a new DPS policy. The SLA profile in the DPS policy will display **SLA:NA**. A SLA profile can be assigned to the DPS policy by selecting the **blue pencil** icon in the **SLA** box. One of the default SLA profiles may be selected or custom SLA profiles may be added by clicking the blue **Plus (+)** icon at the bottom of the newly opened box (Figure 4-47).

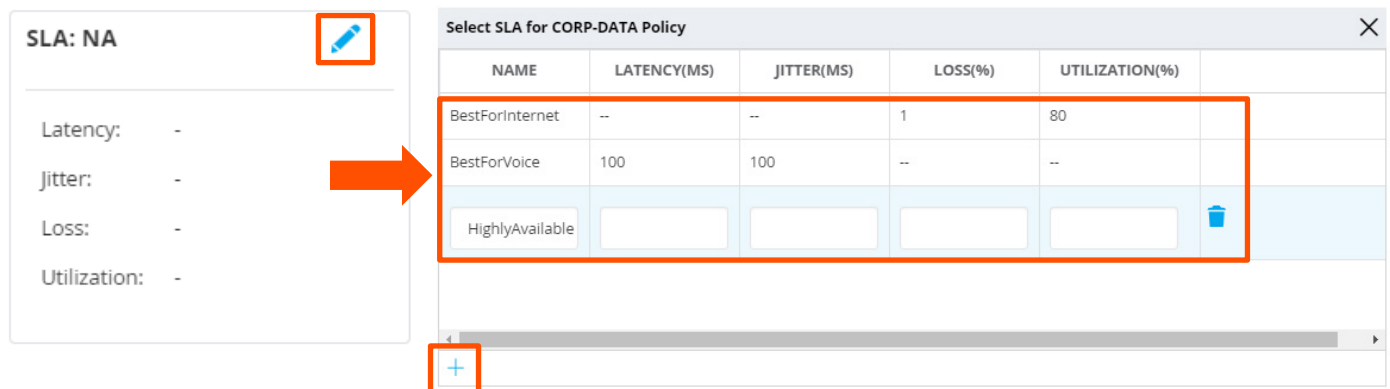


Figure 4-47 Configuring SLA Profiles



SLA policies include a corresponding probe profile that determines how the performance for each WAN path is measured. The probe configuration is fixed in the initial release and uses ICMP probes to the VPNC to measure path performance. Probe settings can be viewed or configured under **Gateway Management > WAN > Health Check**.

Path Selection

DPS policies allow assignment of primary, secondary, and last resort WAN paths. The WAN uplinks assigned to the primary path are preferred over the WAN uplinks assigned to the secondary path. WAN links assigned as last resort are only selected if the primary and secondary WAN uplinks are unavailable. The backup path is typically used for backup links such as LTE. Primary, secondary, and tertiary WAN paths can be assigned in a DPS policy by navigating to **Gateway Management > WAN > Dynamic Path Steering**, selecting the desired DPS policy, and clicking the **blue pencil** icon under **WAN Path Selection**. This will display the **WAN Path Selection** dialog for the policy. One or more links may be assigned to the primary, secondary, and last resort paths by selecting the **blue pencil** icon next to each path and then assigning one or more links from the available links list (Figure 4-48):

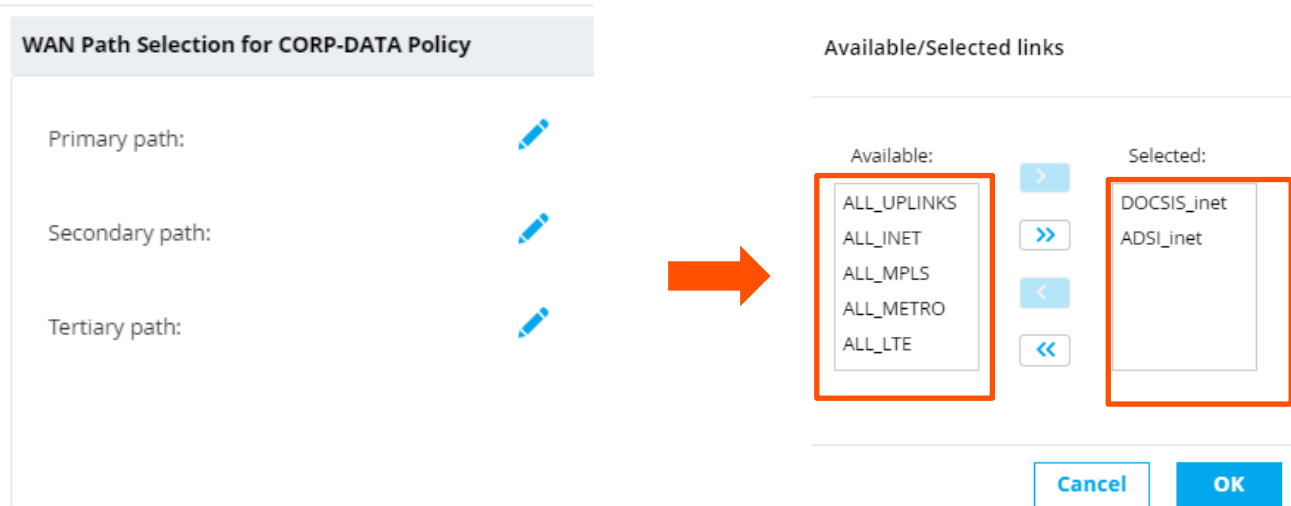


Figure 4-48 WAN Path Selection Configuration

The primary, secondary, and last resort paths can consist of a single link, a group of links, or special link tags. Each DPS policy must include at least one link assigned to the primary path:

- **Single Link** – DPS will only use the selected link, e.g. ACME_MPLS.
- **Multiple Links** – DPS will load-balance traffic between the links using the selected load balancing algorithm, e.g. DOCSIS_INET and ADSL_INET.
- **Special Link Tags** – DPS will load-balance traffic between links of the same type using the selected load-balancing algorithm, e.g. ALL_INET.

It is important to note that when several links are marked as primary the branch gateway will load balance across all of the links that meet the SLA defined in the DPS configuration. If any of the links stop meeting the defined SLA they will be “dropped” from the load balancing group until the link is compliant with the policy for a period of 3 minutes.

Reverse Path Pinning

When a path selection is made for sessions destined for the corporate network through a VPN tunnel, the reverse path of the traffic must take same WAN path to prevent firewall and routing issues. One key feature of the Aruba SD-Branch solution is the ability of gateways operating as VPNCs to follow the WAN paths for each active session to and from the branches. This is important as the BGWs in the branches select paths based on performance and will switch paths in the event that SLAs on WAN uplinks are violated. The peer VPNC must be able to detect these changes and alter the return path of the impacted sessions accordingly.

This capability is referred to as reverse path pinning and is performed automatically by each gateway operating as a VPNC. Reverse path pinning is performed for corporate sessions originating from the branch destined to the data center as well as sessions originating from the data center towards the branches.

The VPNC terminating the VPN overlay tunnels will follow the path selection made by the branch gateway for each session. When a branch gateway selects a path for an application, the VPNC will use the same VPN tunnel for the return traffic. E.g., if a voice call is initiated from a branch to the corporate office and the MPLS path is selected, the VPNC will ensure the return path for the voice call is also sent via the MPLS VPN tunnel.

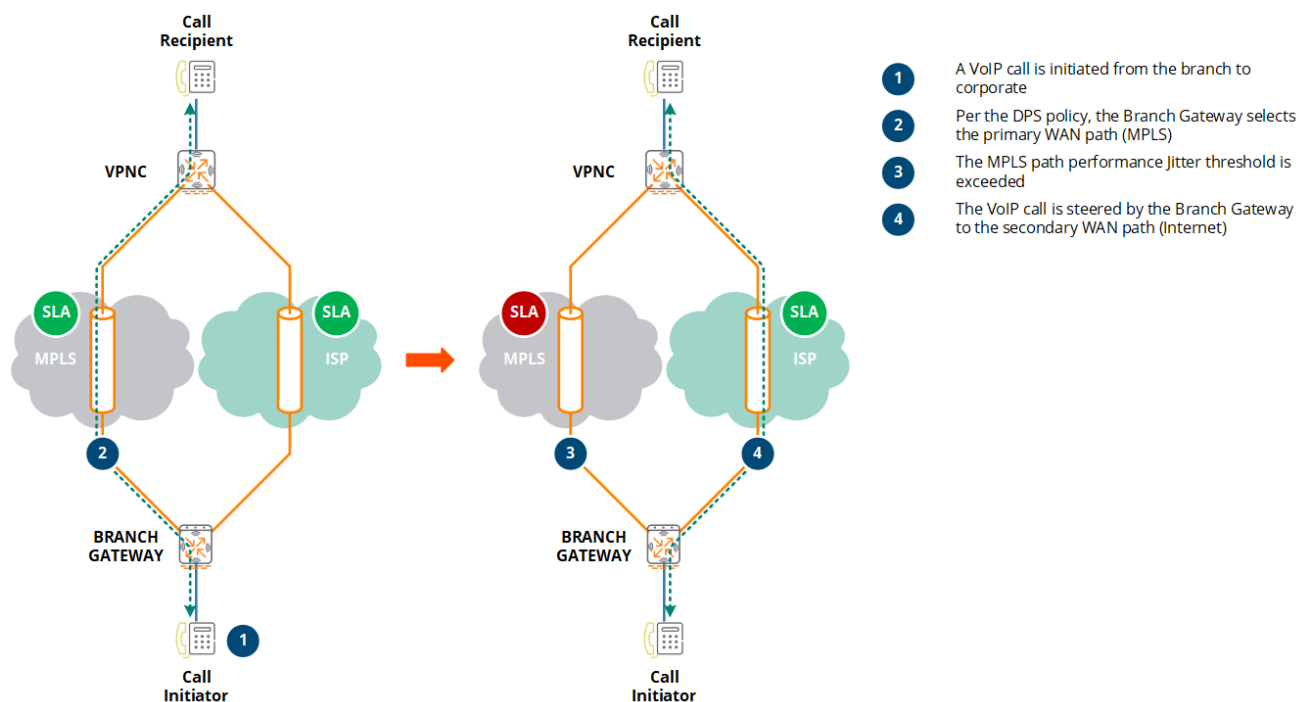


Figure 4-49 Reverse Path Pinning – Branch to VPNC

If the SLA for the MPLS path degrades and violates the assigned SLA, the gateway in the branch will steer the voice traffic to a backup path (e.g., Internet). The VPNC will detect this change and

will switch the return path of the voice traffic to the VPN tunnel for the new selected path with minimum interruption to the voice call as displayed in Figure 4-49.

When a session destined for a branch is initiated from corporate, the VPNC will initially select an available WAN path using equal-cost multi-path routing (ECMP):

1. If the VPNC selects a WAN path that matches the primary path defined in the DPS policy at the branch and the WAN path performance for the primary path meets the SLA then no additional steering is required.
2. If the VPNC selects a WAN path that does not match the primary path defined in the DPS policy, the gateway in the branch will send the return session over the primary WAN path. The VPNC will then steer the session to the preferred path.

Assume a VoIP call is initiated from the corporate site to a branch. The VPNC uses ECMP and selects the Internet WAN path which is received by the gateway in the branch. The DPS policy for the voice traffic is configured to use MPLS as the primary WAN path and the MPLS WAN path meets the defined SLA thresholds. The gateway in the branch will forward the return session over the primary MPLS WAN path. The VPNC will detect that the ingress and egress sessions do not match and will immediately switch the session to the MPLS WAN path (Figure 4-50).

If the MPLS WAN path does not meet the defined SLA thresholds, the gateway in the branch would forward the return session over the Internet WAN path. No additional path steering would be required.

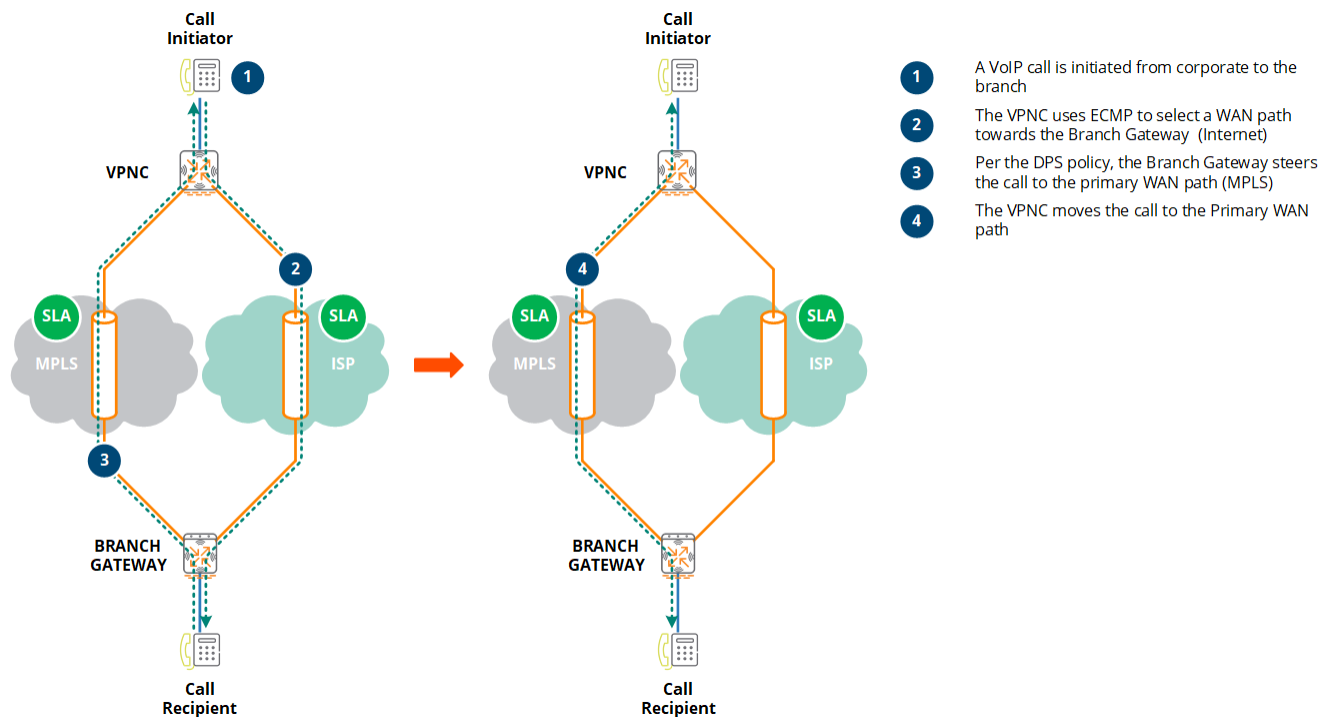


Figure 4-50 Reverse Path Pinning - VPNC to Branch

Virtual Private Networks

VPN tunnels are established between gateways to create an overlay network. The overlay network is used to securely transport traffic forwarded between hub and branch sites. Hub sites are typically corporate headquarters or data centers that include one or more gateways operating in a VPNC role while branch sites include one or more gateways operating as BGWs. Larger deployments may include additional hub sites providing redundancy in the event of a primary hub site failure.

Architecture

The Aruba SD-Branch solution supports a hub and spoke architecture where VPN tunnels are established between VPNCs (hubs) and BGWs (spokes). The establishment of VPN tunnels directly between VPNCs and BGWs is not supported in this initial release.

With a hub and spoke architecture the DPS policies, static routes, and PBR rules configured for each branch group in Central determine the branch traffic that is selected and forwarded to the VPNCs via the VPN tunnels. The VPNCs at the hub sites provide routing and forwarding for hub to spoke, spoke to hub, and spoke to spoke traffic.

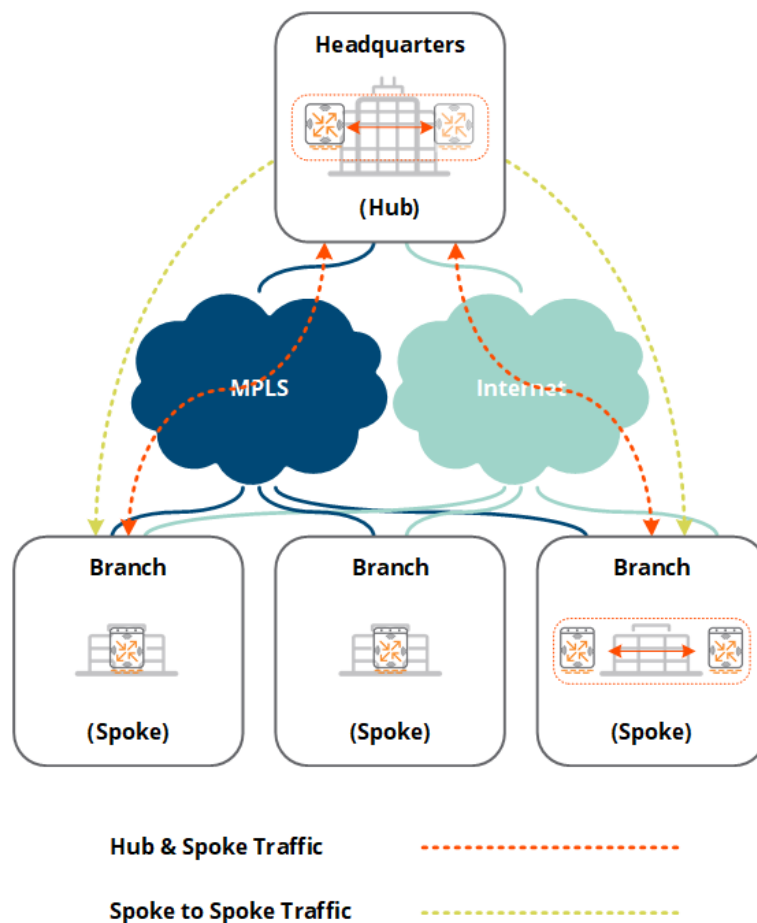


Figure 4-51 Hub and Spoke – Single Hub Example

All SD-Branch deployments will include at least one hub site with one or more VPNCs which terminate IPsec based VPN tunnels initiated from the BGWs installed at the branch sites. The number of VPNCs that are deployed in each hub site will be dependent on the deployment size and redundancy needs. The most basic SD-Branch deployment will consist of one VPNC installed at a hub site that services all the BGWs installed at branch sites. Optional layer 2 redundancy is provided by installing a second VPNC at the hub site.

Larger SD-Branch deployments will include additional hub sites providing additional redundancy in the event of a primary hub failure. The most common deployment consists of a primary and secondary hub, each with two layer 2 redundant VPNCs (Figure 4-52). More complex topologies utilizing additional hub sites are also supported. E.g., a deployment may include a third data center hosting a specific application or service.

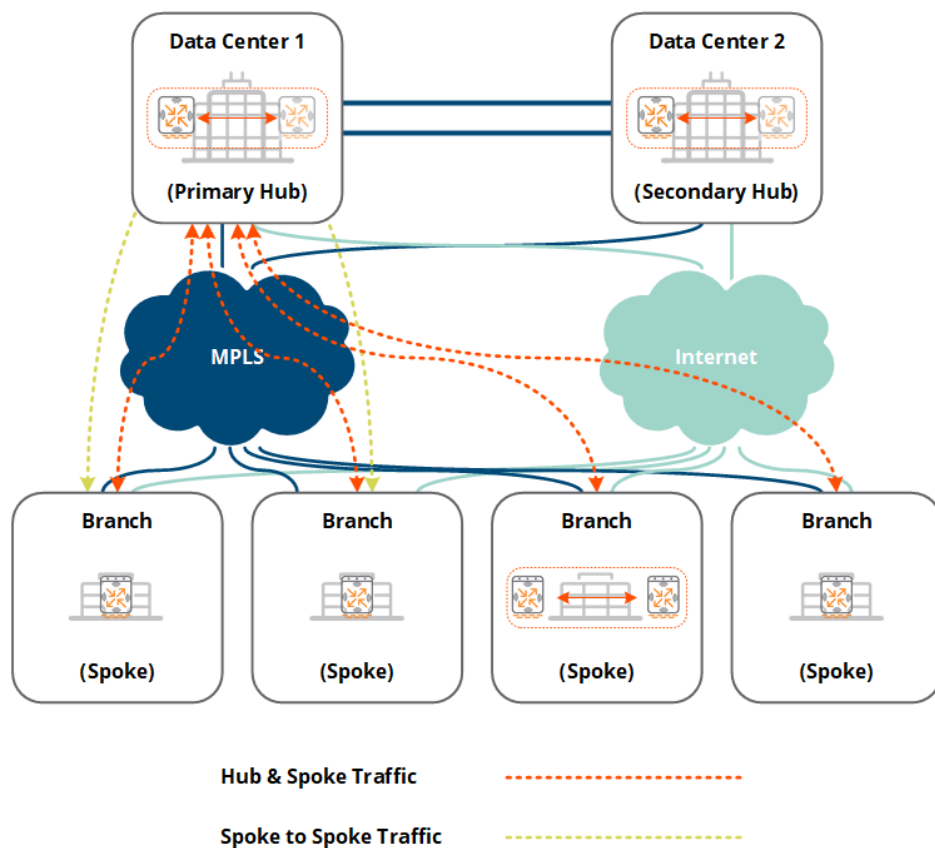


Figure 4-52 Hub and Spoke – Dual Hub Example

VPN Tunnels

The Aruba SD-Branch solution implements IPsec VPN tunnels based on Internet Key Exchange Protocol Version 2 (IKEv2). Aruba gateways leverage factory installed Trusted Platform Module (TPM) certificates for mutual authentication to simplify and automate overlay tunnel

establishment. TPM factory certificates are installed on each gateway at the factory, however user uploaded certificates are supported if required.

Each overlay IPsec VPN tunnel is initiated from a BGW and terminates on a VPNC in a hub using Network Address Translation-Transversal (NAT-T). The only protocol and port that needs to be open for an overlay IPsec VPN tunnel to be established between a VPNC and a BGW is UDP destination port 4500. The VPN tunnels can either be terminated directly on the VPNC without modification or be NATed via an intermediate device such as an edge firewall installed between the Internet WAN and the VPNC.

The VPN tunnels over MPLS based WANs will typically terminate on a VPNC using a VLAN interface assigned a private IPv4 address. Internet based WAN services can either be directly terminated on a VPNC using a VLAN interface assigned a public IPv4 address or a VLAN interface assigned a private IPv4 address. This will depend on the data center architecture.

Each IPsec VPN tunnel is established over the underlay network to a VPNC in the hub sites. The number of VPN tunnels that are established will depend on the number of WAN services used at each site. Most deployments will typically utilize MPLS and Internet WAN services. Each BGW will usually establish one VPN tunnel to each hub per WAN service (Figure 4-53).

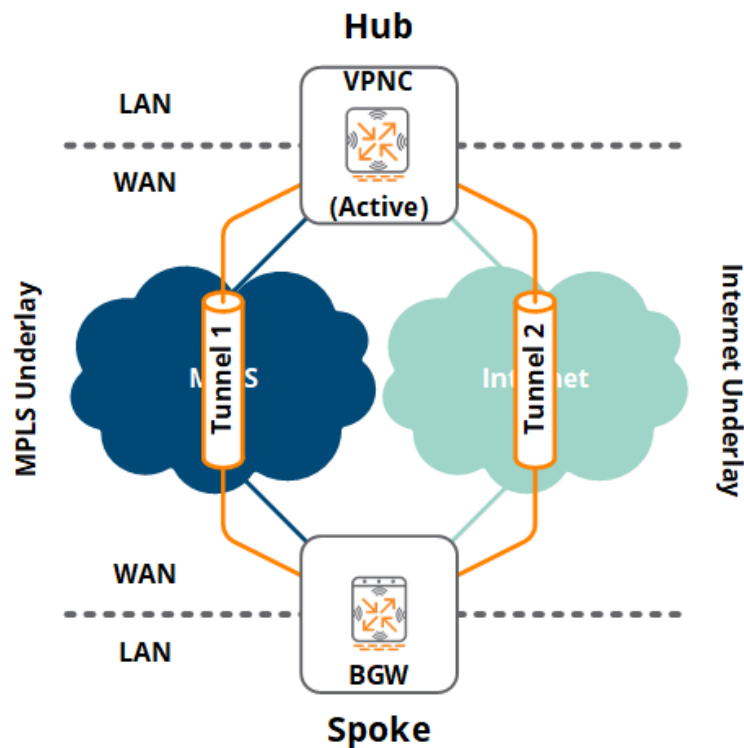


Figure 4-53 VPN Tunnel Example

When the Internet WAN at the hub site is protected by an edge firewall it must be configured appropriately to permit VPN tunnel establishment. The VPNC can either be assigned a RFC-1918

private IPv4 address or a public IPv4 address. The firewall configuration that is required depends on the address assigned to the VPNC (Figure 4-54):

- **RFC-1918 Private Addressing** – The edge firewall must be configured to permit inbound UDP 4500 traffic and translate UDP port 4500 to the private IPv4 address assigned to the VPNC. Most firewall vendors refer to this as port address translation (PAT).
- **Public Addressing** – The edge firewall must be configured to permit inbound UDP 4500 traffic destined to the public IPv4 address assigned to the VPNC.

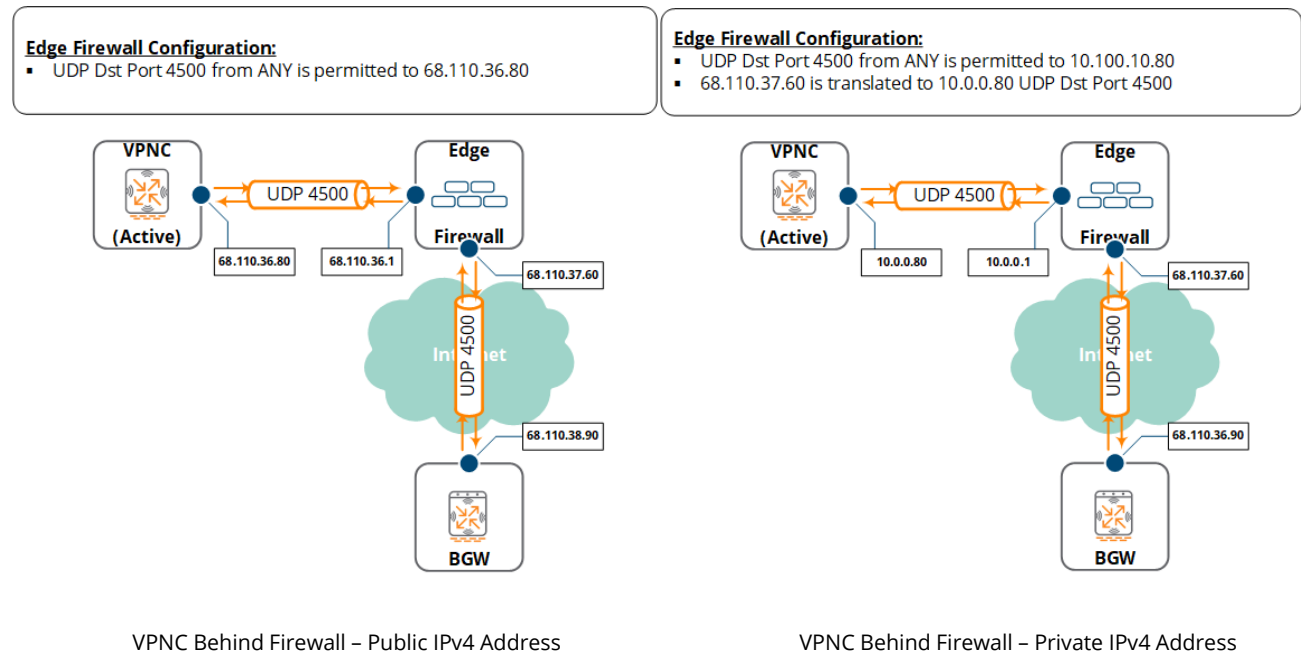


Figure 4-54 VPN Tunnels with Firewalls and NAT

Most BGWs implement DHCP for Internet WAN services and the public IPv4 addresses of the BGWs are not typically known. Aruba recommends configuring the edge firewalls to permit inbound UDP 4500 sessions from any source to accommodate dynamic addressing. The destination will either be the public or private IPv4 address assigned to the VPNC. If the source IPv4 addresses of the BGWs are known (i.e. static) the edge firewall can be configured to only permit UDP 4500 traffic from the specific source IPv4 addresses.

VPN tunnels are configured in Central by navigating to **Gateway Management**, selecting a VPNC or BGW group, and then selecting **VPN**. It's important to note that the VPN configuration options are different depending on whether a VPNC or BGW group is selected. This is the primary reason why the group type must be set as a VPNC or BGW when a group is first selected (please refer back to the [Groups](#) section of this document).



Aruba VPN tunnels implement AES128 encryption with SHA1 hashing and DH Group 2 for phase 1 and AES256 encryption with SHA1 authentication for phase 2.

VPNC Configuration

The only configuration required for VPNCs is determining which BGWs should terminate VPN tunnels. This is achieved by whitelisting which can either be manual or automatic. Aruba recommends performing this configuration at a group level so that the whitelist configuration is applied across all the VPNCs in the group.

To manually whitelist devices for a VPNC group navigate to **Gateway Management > VPN > Hub and Spoke**. Click on the blue **Plus (+)** icon and select the name and MAC address of the BGW that should be whitelisted from the drop-down list. A BGW can be found by running a search for its MAC address if the deployment includes a large number of gateways. Once the BGW has been manually added to the whitelist the BGW will be able to establish VPN tunnels to the VPNCs in the group. The disadvantage of manual whitelisting is that if the BGW is not present in the Central inventory and assigned to a BGW group the VPNC's MAC address must be manually typed.

The screenshot shows the 'FILTER GATEWAY MANAGEMENT' interface for 'CentralPerk#52...'. The top right corner indicates 'Selected Group Type is VPNC'. The main navigation bar includes 'Hub And Spoke', 'Site to Site', 'Cloud Security', 'DPD', 'IKEV1', 'IKEV2', 'Dynamic VPN IP Pool', and 'Shared Secrets'. The 'Hub And Spoke' section is active, displaying a table of gateways. A dropdown menu is open, showing a list of gateway names and MAC addresses, including 'Branch-5150 (00:0b:86:b7:09:37)', 'TEST-VPNC-01 (00:0b:86:b5:36:27)', and 'TEST-VPNC-02 (20:4c:03:06:f2:f0)'. Below the dropdown is an input field for 'Enter New MAC address'.

Gateway Name (MAC Address)	Certificate	Whitelist
Peacock-Branch-02 (20:4c:03:0a:79:40)	Factory Cert	--
Branch-1-7008-8320 (20:4c:03:0a:83:20)	Factory Cert	--
Peacock-Branch-05 (20:4c:03:1a:34:3c)	Factory Cert	--
Peacock-Branch-01 (20:4c:03:21:ad:ac)	Factory Cert	--
Peacock-BGW-IntroSpect (20:4c:03:21:b2:ac)	Factory Cert	--

Figure 4-55 Manual Whitelisting

Automatic whitelisting offers a much more streamlined process for whitelisting BGWs compared to manual whitelisting. Automatic whitelisting is enabled per VPNC group by navigating to **Gateway Management > VPN > Hub and Spoke**, selecting the **Automatically whitelist branch gateways** slider, and defining a passphrase. When enabled, the VPNC can terminate VPN tunnels initiated from BGWs present in the Central account as well as BGWs in other Central accounts.

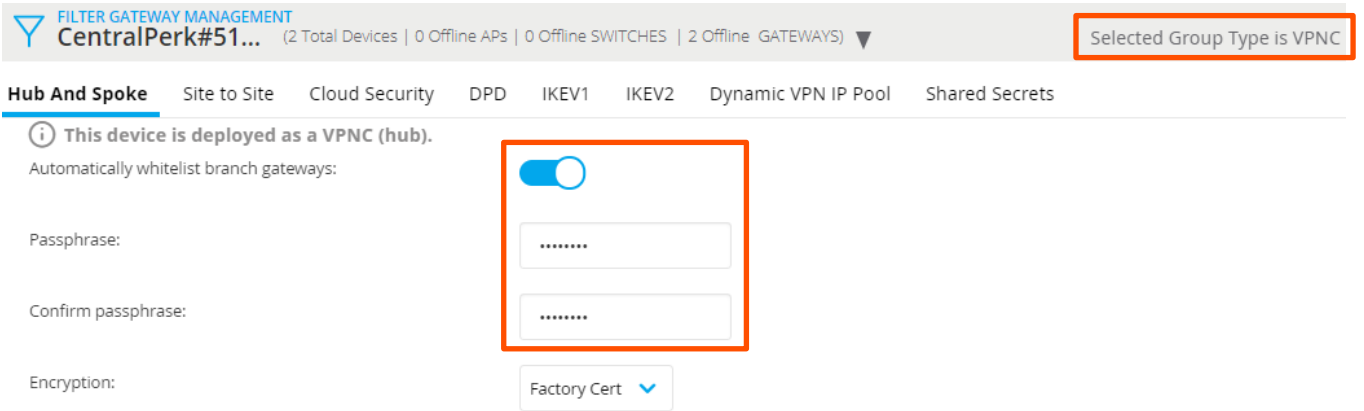


Figure 4-56 Automatic BGW Whitelisting

To prevent undesirable VPN tunnels from being established to the VPNCs in the group, automatic whitelisting employs passphrase protection. The VPNCs will only accept VPN tunnels from BGWs that are configured with the correct passphrase. It's important to note that the passphrase is not used for the VPN tunnel establishment itself. The VPN tunnels still utilize TPM with factory or user uploaded certificates for mutual authentication and establishment.

Branch Gateway Configuration

The VPN configuration for a BGW group requires an administrator to define each VPNC peer and interface where a VPN tunnel will be initiated. The number of VPNC peers that have been defined in the BGW group is dependent on how many hub sites and WAN services that have been deployed. A basic SD-Branch deployment utilizing one hub and two WAN services will require two VPNC peers to be defined. A more advanced SD-Branch deployment consisting of two hubs and two WAN services will require four VPNC peers to be defined. If the deployment includes LTE backup links then additional entries will need to be defined as well.

As previously mentioned, the VPNCs can be provisioned to either manually or automatically whitelist BGWs. If the VPNCs are configured to automatically whitelist BGWs, then the BGW group requires a similar configuration for the VPNCs to match. Navigate to **Gateway Management > VPN > Hub and Spoke**, activate the **Connect automatically to VPNC** slider, and enter the same passphrase configured for the VPNC group (Figure 4-57). Failing to perform this step will prevent the VPN tunnels from being established. This configuration step is not required if manual whitelisting has been employed.

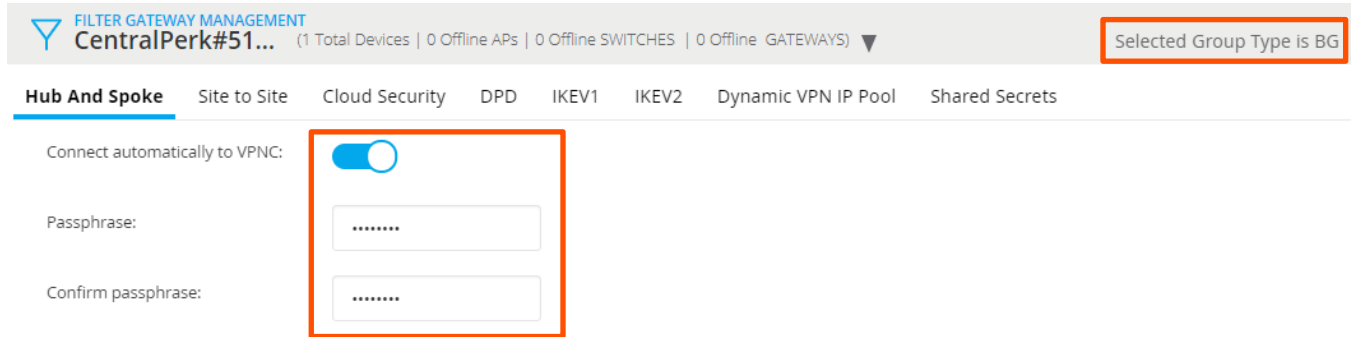


Figure 4-57 Configuring BGWs to Automatically Connect to VPNC

A VPNC peer can be created by clicking the blue **Plus (+)** icon. The exact configuration entered will depend on whether the VPNC peer is standalone or is configured as a layer 2 redundant pair. A standalone VPNC peer requires the following configuration:

- **Primary VPNC** – Select the name and MAC address of the active VPNC from the dropdown list. A search may be performed for the MAC address of the VPNC as well.
- **IP Address** – The IP Address of the VPNC interface that will terminate the VPN tunnel. If an intermediate firewall is configured for PAT then the public IPv4 address of the firewall that is translating the address to the private IPv4 address on the VPNC must be entered.
- **Source VLAN** – The WAN uplink VLAN interface on the BGW where the VPN tunnel will be initiated.

If the VPNCs are configured as a layer 2 redundant pair then the following configuration needs to be entered:

- **Primary VPNC** – Select the name and MAC address of the active VPNC from the dropdown list. A search may be performed for the MAC address of the VPNC as well.
- **Secondary VPNC** – Select name and MAC address of the standby VPNCs from the dropdown list. A search may be performed for the MAC address of the VPNC as well.
- **IP Address** – The Virtual Router Redundancy protocol (VRRP) virtual IP Address of the VPNC interface that will terminate the VPN tunnel. If an intermediate firewall is configured for PAT then the public IPv4 address of the firewall that is translating the address to the private IPv4 address on the VPNC must be entered.
- **Source VLAN** – The WAN uplink VLAN interface on the BGW where the VPN tunnel will be initiated.

Figure 4-58 provides a sample VPN peer configuration for a single hub site implementing layer 2 redundant VPNCs. The BGW group configuration includes two VPN peers that will configure the BGWs in the group to establish VPN tunnels to the active VPNC using the underlay MPLS and Internet WAN services.

FILTER GATEWAY MANAGEMENT
 DEMO-BRANCH-... (2 Total Devices | 0 Offline APS | 0 Offline SWITCHES | 1 Offline GATEWAYS) ▼ Selected Group Type is BG

Hub And Spoke Site to Site DPD IKEV1 IKEV2 Dynamic VPN IP Pool Shared Secrets

Connect automatically to VPN:

Advertise branch subnets to hub:

Advertise branch VLANs:

HUB			BRANCH GATEWAY		
PRIMARY VPNC	BACKUP VPNC	IP ADDRESS	SOURCE VLAN	ENCRYPTION	CA CERT
DEMO-VPNC1 (20:4c:03:0a:5d:70)	DEMO-VPNC2 (20:4c:03:0a:89:f0)	10.0.0.42	3094	Factory Cert	--
DEMO-VPNC1 (20:4c:03:0a:5d:70)	DEMO-VPNC2 (20:4c:03:0a:89:f0)	101.0.0.42	4094	Factory Cert	--

Choose an option ...
 DEMO-VPNC1 (20:4c:03:0a:5d:70)
 DEMO-VPNC2 (20:4c:03:0a:89:f0)
 vpnc1 (00:1a:1e:00:ec:50)
 Enter New Primary VPNC

Figure 4-58 VPNC Peer Configuration

Each VPNC peer includes a Primary and Backup VPNC along with the VRRP virtual IPv4 addresses configured on the VPNCs. This configuration will result in the following:

- One VPN tunnel will be established to the peer VRRP virtual IPv4 address 10.0.0.42 via the MPLS WAN uplink VLAN 3094.
- One VPN tunnel will be established to the peer VRRP virtual IPv4 address 101.0.0.42 via the Internet WAN uplink VLAN 4094.



If automatic whitelisting is employed and the target VPNC is not present in the Central account then the MAC addresses in the Primary VPNC and (if required) Secondary VPNC fields must be entered manually.

Figure 4-59 demonstrates the usage of source VLANs when the VPNC peer IP addresses are reachable over single and multiple WAN uplinks. In the left example the VPNC peer IP address is reachable over the Internet from both WAN uplinks on the BGW. One VPN tunnel is configured in the BGW group with the source VLANs set to 4093 and 4094. This configuration will result in two VPN tunnels being established from the BGW to the VPNC (one VPN tunnel per WAN uplink).

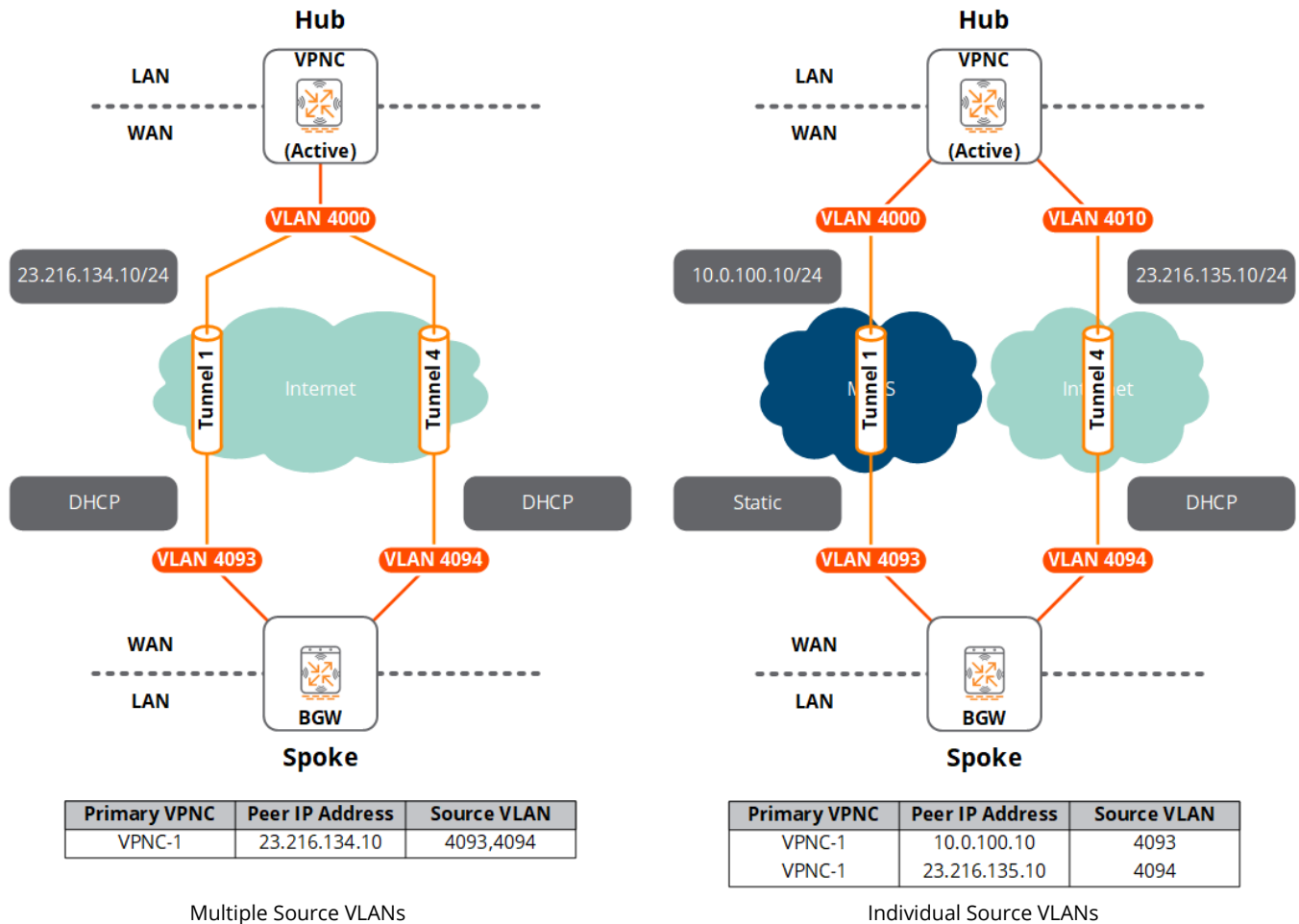


Figure 4-59 Source VLAN Usage Examples

In the example on the right the VPNC has separate VLAN interfaces configured to support multiple isolated WAN services (MPLS and Internet). The BGW can only reach the MPLS and Internet interfaces through their respective WAN uplinks. The Internet WAN uplink cannot reach the VPNC's MPLS VLAN interface and vice versa. To support this topology two VPN tunnels are configured in the BGW group with the source VLANs set to the VLAN interface connected to each respective WAN service:

- **MPLS VPN Tunnel** – Configured with the source VLAN 4093
- **Internet VPN Tunnel** – Configured with the source VLAN 4094

This VPN configuration will result in two VPN tunnels being established from the BGW to the VPNC, one tunnel initiated over the MPLS WAN uplink and one over the Internet WAN uplink.

VPNC Redundancy Options

VPNCs can either be deployed as standalone devices or as layer 2 redundant pairs. When layer 2 redundancy is enabled, one VPNC operates in an active role while the second VPNC operates in a standby role. The standby VPNC only assumes an active role in the event of an active VPNC failure. It's important to note that the standby VPNC does not terminate any VPN tunnels or advertise branch routes via OSPF until it transitions to an active state.

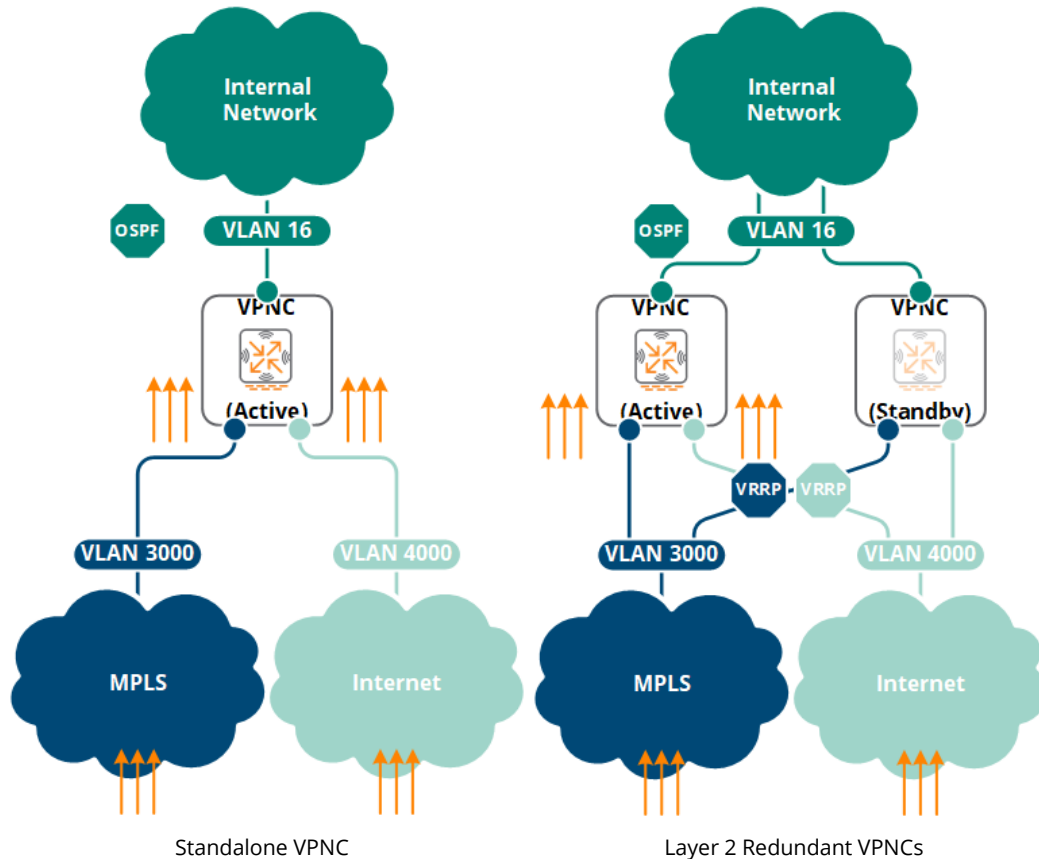


Figure 4-60 Standalone vs. Layer 2 Redundant VPNCs

VPNCs deployed using layer 2 redundancy leverage VRRP on each WAN VLAN interface for failover. The VRRP priorities are assigned so that one VPNC assumes an active role while the second VPNC assumes a standby role. The active VPNC terminates the VPN tunnels during normal operation and advertises the branch routes into the internal network via OSPF. The standby VPNC will only assume an active role if the active VPNC fails or becomes unreachable.

If the active VPNC fails or is taken out of service for maintenance, the VPN tunnels will be re-established to the standby VPNC at a rate of 20-30 tunnels per second. The standby VPNC will advertise the branch routes into OSPF as the VPN tunnels are brought back up. The failover and convergence times are dependent on the configured VPN DPD timers and the number of tunnels that need to be reestablished. For reference, a typical layer 2 failover for 6,000 tunnels occurs in under 5 minutes.

If multiple hubs are deployed each hub site can contain a standalone VPNC or a layer 2 redundant pair of VPNCs. Aruba supports layer 3 failover for these deployments where the VPN tunnels are established to VPNCs deployed at each hub site. In this redundancy model the branch groups in Central are configured with multiple VPN peers. The VPN tunnels are established from each BGW to their designated VPNCs in each hub site.

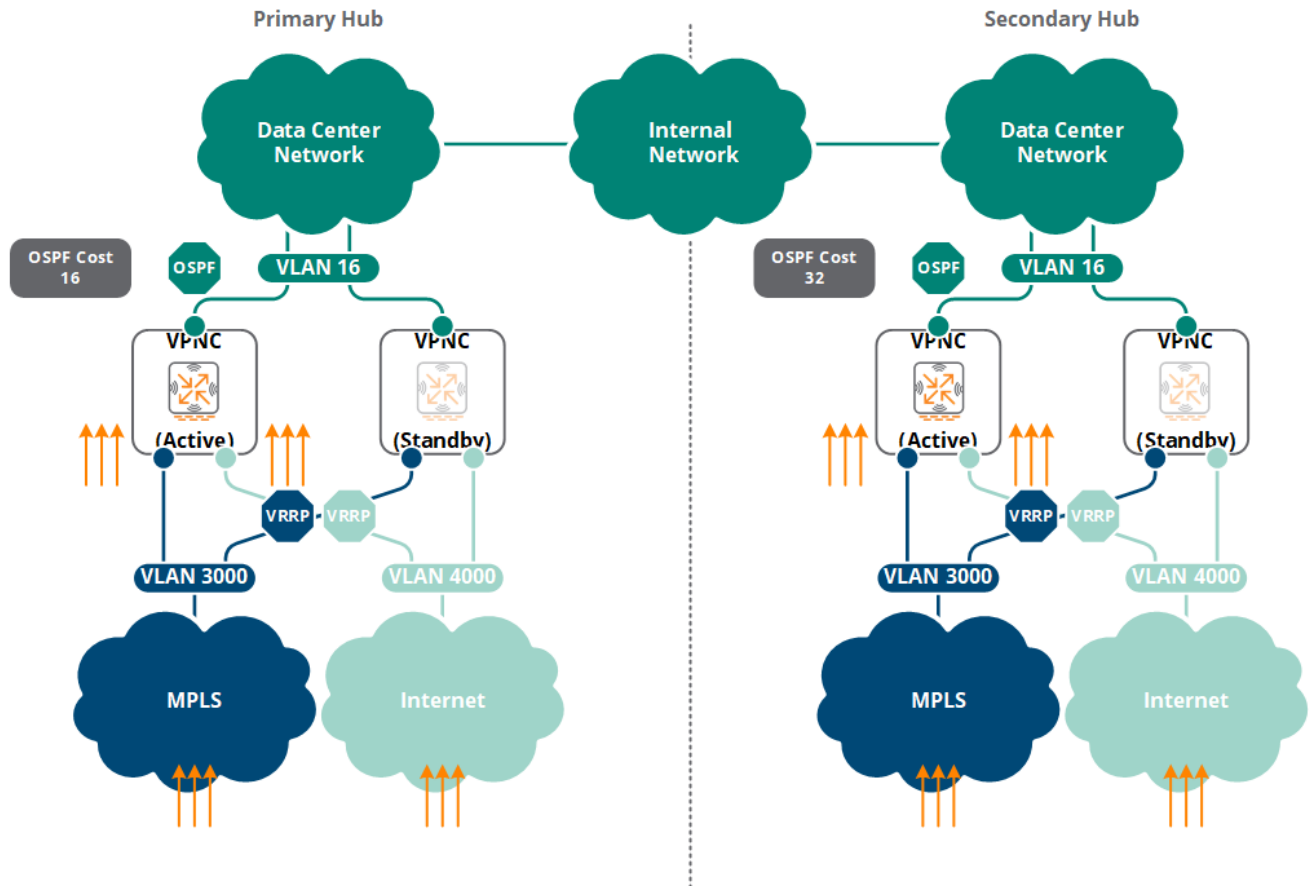


Figure 4-61 Layer 3 Failover between Hub Sites



Please refer to the [Reference Topologies](#) section for supported and validated reference architectures.

Each hub is assigned either a primary or secondary role. The designated VPNCs in each hub advertise the branch routes into OSPF at different route costs. The VPNCs in the primary hub advertising the branch routes at a lower route cost than the VPNCs in the secondary hub. The VPNCs in the primary hub forward hub to spoke, spoke to hub, and spoke to spoke traffic during normal operation. The VPN tunnels are already established to the secondary site in the event that the primary hub fails or becomes unreachable. The OSPF routes will converge so that the branch routes are reachable through the secondary hub. A typical reconvergence occurs in under 1 minute depending on the interior gateway protocol (IGP) configuration.

VPNC Scaling

The number of VPNCs deployed per hub will be influenced by the following factors:

- Hardware model of the VPNCs
- Number of branches deployed
- Number of active WAN uplinks
- Number of branch subnets that are advertised to the VPNC

A deployment may include a standalone VPNC or a layer 2 redundant pair of VPNCs servicing all BGWs. In the case of large deployments there may be pools of VPNCs where standalone or layer 2 redundant pairs of VPNCs service BGWs from specific regions. The table below outlines how many tunnels will be established from each gateway based on the number of VPNC peers and active WAN links:

VPNC Peers	Active WAN Links	Tunnels
1	1	1
2	2	4
1	3	3

Table 4-5 Typical VPNC Scalability

Each BGW will usually establish one VPN tunnel to each configured VPNC peer per active WAN uplink. A BGW with two active WAN uplinks and two configured VPNC peers will establish a total of four VPN tunnels (one VPN tunnel per active WAN uplink to each VPNC peer). A BGW with three active WAN uplinks and one configured VPNC peer will establish three VPN tunnels (one VPN tunnel per active WAN uplink to the VPNC peer).

The total number of VPN tunnels a VPNC can support is determined by the model. Platforms such as the 7210 can support a total of 1,000 tunnels while the 7240 can support 6,000. The number of branches supported by each VPNC platform can be quickly calculated by dividing the total number of tunnels by the number of active WAN uplinks enabled on branches. E.g., a 7210 can support a total of 500 branch sites when two active WAN uplinks are enabled per branch.

An additional consideration when determining which model of VPNC to deploy at hub sites are the total number of routes supported by each platform. The branch VLAN interfaces (subnets) that are advertised to VPNC hubs from branches can be specified based on the BGW group configuration. The routes are exchanged using IKEv2 extensions and will be learned by the VPNCs as overlay routes. In addition to the branch routes, the BGW will also advertise its system-ip address which is installed as a host route on the VPNC. One host route is created per WAN uplink. This is an important consideration when determining scaling as the system-ip will consume route entry resources. E.g., a BGW with two active WAN uplinks that is configured to advertise 2 VLAN interfaces will advertise a total 6 branch routes to the VPNC (3 routes per WAN uplink).

If the IPv4 subnets assigned to the VLAN interfaces on each BGW are contiguous, then the BGW can optionally send summarized routes to the VPNC. E.g., if a BGW is configured with local networks 192.168.88.0/25 and 192.168.88.128/25, the BGW will advertise the single summarized route of 192.168.88.0/24 rather than two individual routes. Implementing contiguous address space in branches and using route summarization reduces the overall number of routes each VPNC peer must learn and therefore provides greater ability to scale. Using the same example as the one mentioned above, a BGW with two active WAN uplinks that is configured to advertise two VLAN interfaces (contiguous addresses) will generate two total summarized routes on the VPNC as opposed to four non-summarized routes. Aruba recommends assigning contiguous address space to branches whenever possible.



The [Appendix](#) section of this document provides a list of supported VPNC platforms with scaling information.

Tunnel Modes

The Aruba SD-Branch solution supports both split tunneling and full tunneling modes. The tunneling method selected for a deployment will be dependent on organizational business and policy requirements:

- **Split Tunneling** – Traffic destined for the corporate network or other branches is forwarded out over the VPN tunnel(s). Traffic destined for the Internet is NATed by the BGW and forwarded out locally.
- **Full Tunnel** – All traffic is forwarded out via the VPN tunnel(s). This includes traffic destined to the corporate network, other branches, or Internet.

A BGW group can be configured to support either split tunnel or full tunnel modes or a combination of both modes (Figure 4-62):

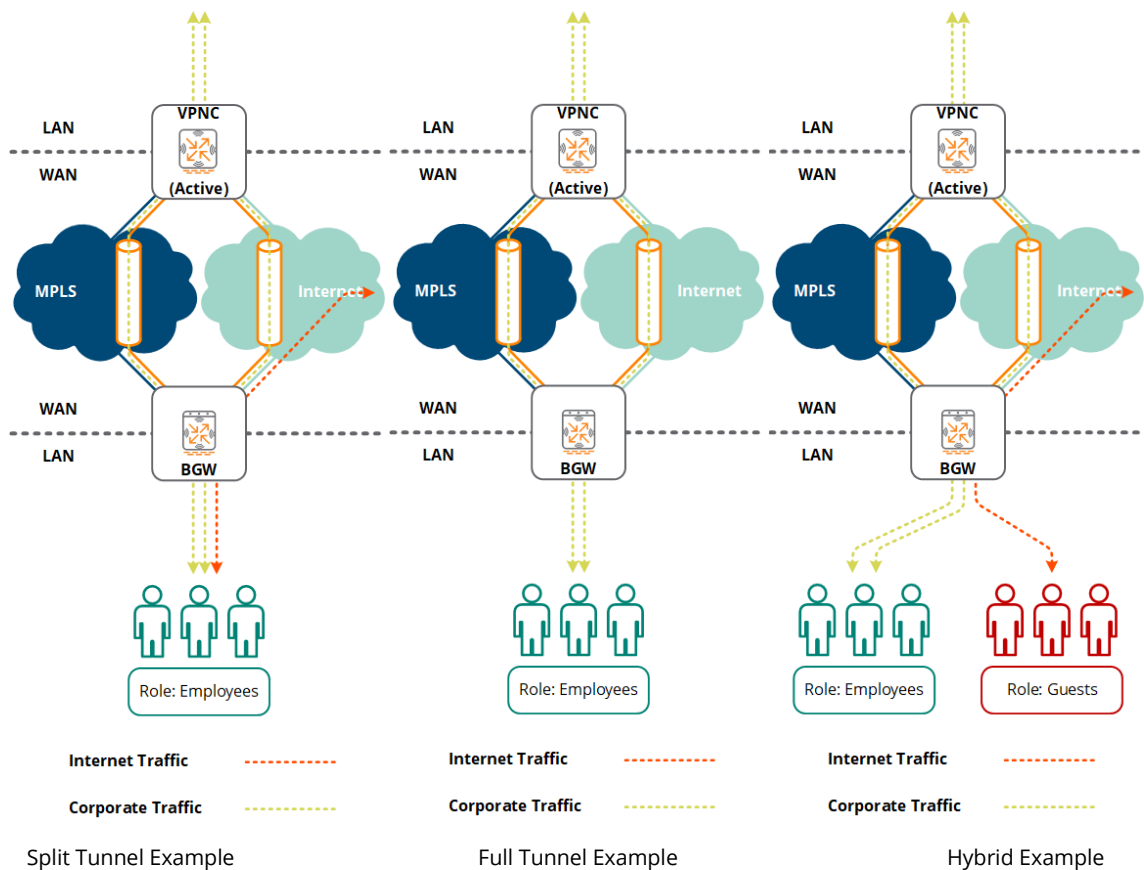


Figure 4-62 VPN Tunnel Modes

To support full tunnel mode, the BGWs leverage PBR rules to override the routing table on the BGW and forward traffic destined for the Internet via one or more VPN tunnel(s). The PBR rules determine which sessions are to be matched and forwarded to the VPN tunnels as well as which sessions are to be ignored and routed normally. The VPNC in the hub site may also require PBR rules to be defined depending on how the VPNC is deployed and connected to the Internet (see the [Reference Topologies](#) section for additional details).

Routing

Aruba's SD-Branch solution leverages WAN services that interconnect hub and spoke sites to establish VPN tunnels which encapsulate and forward corporate traffic. Each WAN service is referred to as the underlay network while the VPN tunnels form the overlay network.

Reachability and forwarding through the underlay and overlay networks is achieved using IP routing on gateways. The VPNCs and BGWs each implement their own routing tables to determine the next-hop for each IP packet on its way to the desired destination. The routing tables on the BGWs consist of default gateways and static routes while the routing tables on VPNCs consist of default gateways, static, IKEv2, and OSPF routes (Figure 4-63).

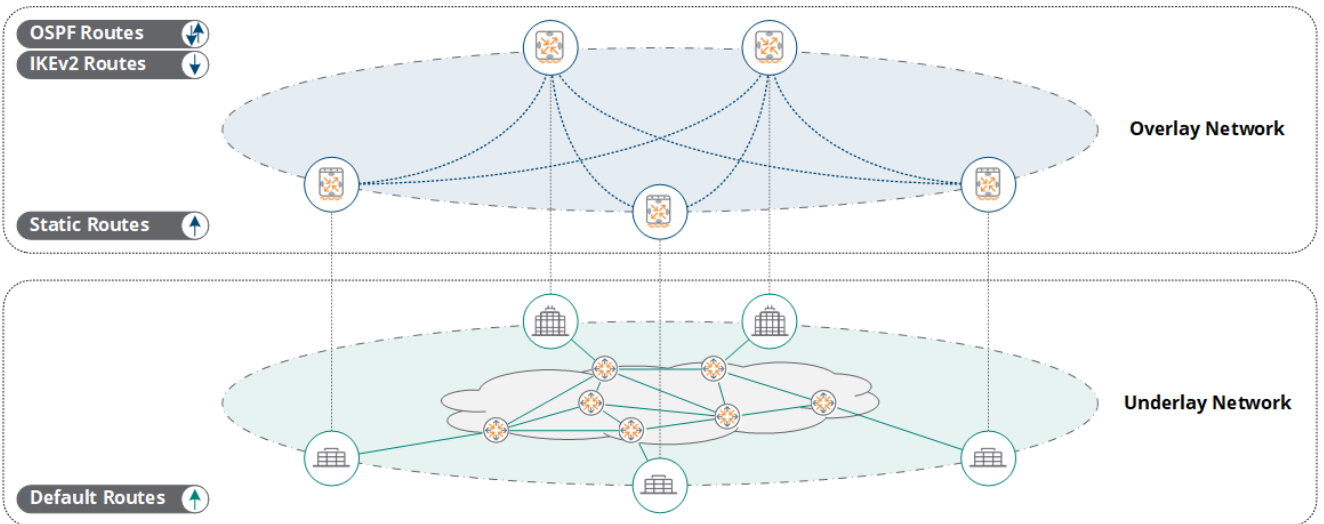


Figure 4-63 Underlay vs. Overlay Routing

Underlay Routing

For the VPN tunnels to be established, the VLAN interfaces on the BGWs and VPNCs connected to each WAN service must be reachable over each WAN service. To provide IP reachability through each WAN service a combination of default gateways and static routes are required. The types of routes that are implemented are determined by the WAN service:

- **Internet WAN Services** – Requires default gateways to be defined on both VPNCs and BGWs. These are manually configured on VPNCs and dynamically learned on BGWs from each from the ISP via DHCP or PPPoE.
- **MPLS / Private WAN Services** – Requires static default routes on BGWs and static routes on VPNCs. These are manually configured on both VPNCs and BGWs.

Figure 4-64 provides an example of the underlay routes required for a typical SD-Branch deployment utilizing MPLS and Internet WAN services. In this example reachability between BGWs and VPNCs over the Internet WAN service is achieved by defining a static default gateway on the VPNCs and dynamically learning default gateways on BGWs via DHCP. Reachability over the MPLS WAN service is achieved by defining static routes on the VPNCs and static default gateways on the BGWs.

A default gateway is required on each BGW for MPLS networks. The default gateway must be defined with a cost of 15 or higher and is required for the VPN tunnels to establish.



A default gateway is required on each BGW for MPLS networks. The default gateway must be defined with a cost of 15 or higher and is required for the VPN tunnels to establish.

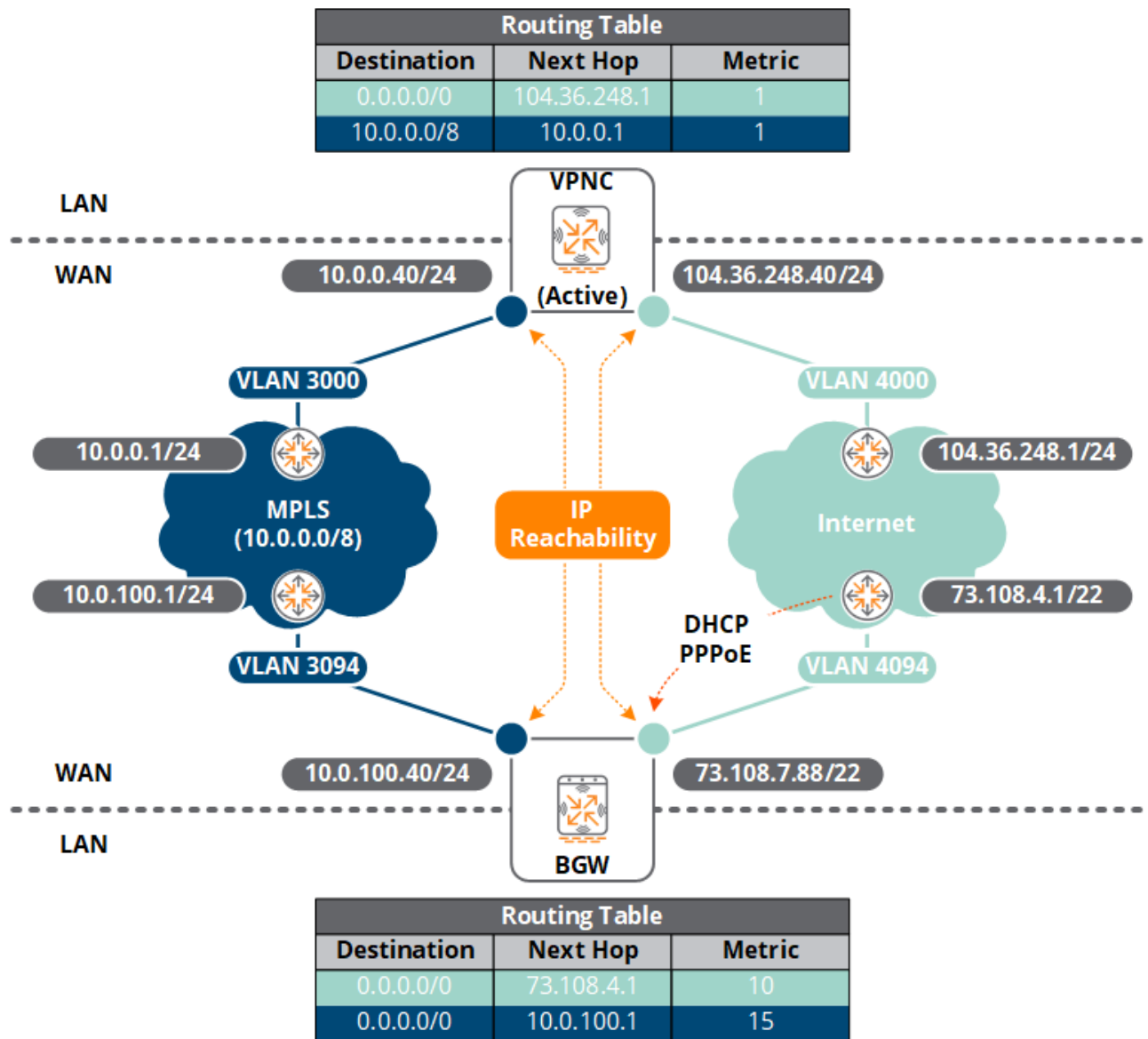


Figure 4-64 Underlay Routes Example

For deployments implementing multiple Internet WAN services, Aruba gateways can support and install multiple default gateways (see reference architectures section). BGWs implementing multiple Internet WAN services will load-balance or steer sessions out the respective Internet WAN uplinks based on the configured DPS and PBR policies. VPNCs typically implement a single default route and leverage the stateful packet inspection (SPI) firewall to pin each VPN tunnel to the correct VLAN interface. The SPI firewall on the VPNCs ensuring the return traffic for each incoming UDP 4500 session is sent out the same VLAN interface it was received.

Static Default Gateways

Static default gateways are required for all deployments implementing Internet based WAN services. The default gateway is statically defined on VPNCs and dynamically derived on the BGWs from the Internet Service Provider (ISP) via DHCP or PPPoE. BGWs requiring static default gateways if static addresses are assigned.

A static default gateway is also required on BGWs connecting to MPLS WAN or private WAN services. The static default gateway is required by the uplink manager to allow the VPN tunnel to be initiated out the MPLS WAN uplink.

The static default gateway configuration is performed at the device level since default gateways are typically unique to each BGW and VPNC. However, there are some circumstances where the default gateways can be defined at the group level. E.g., if the deployment includes L2 redundant VPNCs that share a common gateway or if the BGWs connect to CPE modems implementing the same RFC-1918 addresses space requiring static addressing. Static default gateways are defined per device by navigating to **Gateway Management > Routing > IP Routes > Static Default Gateway**. A new default gateway can be added to a device by selecting the blue **Plus (+)** icon (Figure 4-65). A next-hop IPv4 address and a cost must be specified for each default gateway:

The screenshot shows the 'Static Default Gateway' configuration page. At the top, there is a filter bar for 'mis5150-vpnc-01' with device status indicators. Below this are navigation tabs for 'IP Routes', 'Policy-Based Routing', 'NextHop Configuration', and 'OSPF'. The 'IP Routes' tab is active, and the 'Static Default Gateway' sub-tab is selected. A table lists the current static default gateway configuration:

IP ADDRESS	COST	IPVERSION
10.1.85.1	1	IPv4

Below the table, a red box highlights a plus sign icon. An arrow points from this icon to a 'New IP Default' form. The form contains the following fields:

- IP version: IPv4 (selected)
- IP address: (empty text input field)
- Cost: 1

Figure 4-65 Static Default Gateway Configuration

Dynamically learned default gateways on BGWs from DHCP, LTE or PPPoE will be installed in the route table with a default cost of 10 by default. These default costs can be optionally modified by navigating to **Gateway Management > Routing > IP Routes > Dynamic Default Gateway**. If a deployment includes BGWs with multiple Internet based WAN services implementing both dynamic and static addressing, Aruba recommends defining the static default gateways at a cost equal to the dynamically learned default gateway(s) so that both default gateways will be installed in the BGW's routing table.

BGWs connecting to MPLS WAN services require a static default gateway to be defined pointing to the MPLS-CE router. Aruba recommends defining the static default gateway with a cost of 15 or higher (Figure 4-66). If a static default gateway is not defined, the VPN tunnel will not be initiated to the VPNC over the MPLS WAN service.

▼ Static Default Gateway

Static Default Gateway			
IP ADDRESS	COST	IPVERSION	
10.1.85.1	15	IPv4	

Figure 4-66 MPLS Default Gateway Example

Static Routes

Static routes may be required on the VPNCs to provide reachability through the MPLS network for deployments including MPLS WAN services. Most MPLS networks will implement an organizationally unique block of CIDR addresses (e.g., 10.100.0.0/16) allowing a single static route to be defined. Most MPLS networks implement a contiguous block of addresses to promote summarization.

The static routes must be defined at the device level since the next-hop MPLS-CE routers are unique to each device. The exceptions are L2 redundant VPNCs where the routes can be optionally configured at the group level. Static routes can be defined at the device or group level by navigating to **GATEWAY MANAGEMENT > Routing > IP Routes** and selecting the blue **Plus (+)** icon (Figure 4-67):

The screenshot displays the 'IP Routes' configuration page for a device named 'mis5150-vpnc-01'. The page includes a navigation menu with 'IP Routes' selected. Below the menu, there is a table of existing IP routes:

DESTINATION IP ADDRESS	DESTINATION MASK	NEXT HOP (FORWARDING)	COST	IPSEC MAP NAME	NULL INTERFACE
10.0.0.0	255.0.0.0	10.0.0.1	--	--	--
192.168.0.0	255.255.240.0	192.168.66.1	--	--	--
192.168.64.0	255.255.192.0	192.168.66.1	--	--	--

A blue plus icon (+) is highlighted in a red box below the table. Below this icon is the 'New IP Route' form, which is also partially highlighted with a red box. The form includes the following fields:

- IP version: IPv4 (selected)
- Destination IP address: [text input]
- Destination network mask: [text input]
- Forwarding settings: Using Forwarding Router Address (selected)
- Next hop IP address: [text input]
- Cost: [text input]

Figure 4-67 Static IP Routes – VPNC

Static routes are not required on the BGWs to provide reachability through the MPLS network. The BGW will use the static default gateway to initiate the VPN tunnel to the destination VLAN interface on the VPNCs. The VPNCs optionally use static route(s) for the return path.

Overlay Routing

Once the overlay network has been established routing is required to provide reachability. The VPNCs require routes to know which networks are reachable through each BGW (including system-ips) as well as which networks are reachable through peer corporate routers. The BGWs require routes to know which corporate networks are reachable through each VPNC hub. To simplify overlay routing and provide scaling, the Aruba SD-Branch solution implements a combination of dynamic and static routing:

1. BGWs are configured with static routes to determine which destination networks are reachable through the VPN tunnels. One static route is defined per VPNC peer per WAN uplink.
2. The BGWs are configured to advertise internal LAN networks to each L2 active VPNC peer using Aruba IKEv2 extensions. Each advertised LAN is installed as an IKEv2 route on each L2 active VPNC (one route per active WAN uplink).
3. The VPNCs participate in OSPF and learn corporate routes from neighboring OSPF routers as well as redistribute IKEv2 overlay routes to neighboring OSPF routers. IKEv2 routes are redistributed as OSPF External Type 2 routes.

Figure 4-68 provides an example of the overlay routes for a typical SD-Branch deployment utilizing MPLS and Internet WAN services:

Routing Table		
Destination	Next Hop	Metric
192.168.80.0/25	bgw-mpls	66
192.168.80.0/25	bgw-inet	66
192.168.80.128/25	bgw-mpls	66
192.168.80.128/25	bgw-inet	66

Routing Table		
Destination	Next Hop	Metric
192.168.0.0/20	vpnc-mpls	1
192.168.0.0/20	vpnc-inet	1

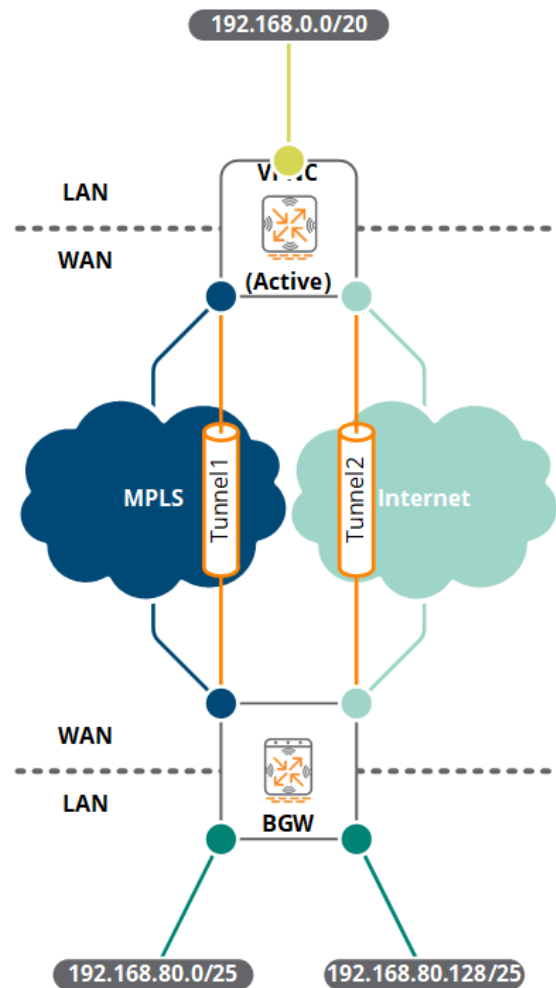


Figure 4-68 *Overlay Routes Example*

Aruba recommends implementing the dynamic overlay routing model as it allows the VPNCs to dynamically learn the branch LAN routes and seamlessly redistribute them into the corporate network. However, smaller deployments with single data centers may elect to implement static routes on corporate routers to provide reachability to the branch networks.

In Figure 4-68 each BGW is advertising two LAN networks (192.168.80.0/25 and 192.168.80.128) to a VPNC which are installed as IKEv2 overlay routes. Since two WAN uplinks are implemented the VPNC will learn the routes through each WAN uplink and will learn and install a total of four routes.

The BGW implements two static routes to reach the 192.168.0.0/20 network which are configured at the group level: one static route using the MPLS WAN uplink and one static route implementing the Internet WAN uplink. This configuration results in two overlay static routes being installed in the BGW routing table with the next-hop pointing to the appropriate VPNC and WAN uplink.

BGW Subnet Advertisement

Aruba recommends configuring the BGWs to advertise the branch networks to the VPNC hubs using Aruba IKEv2 extensions for all SD-Branch deployments. The IKEv2 extensions provide a seamless mechanism that allows each L2 active VPNCs to dynamically learn branch routes without requiring definition of static routes. Scaling will be dependent on the hardware platform selected for the VPNCs. The learned IKEv2 routes are typically redistributed to neighboring routers via OSPF.

Aruba recommends only advertising the networks supporting hosts that need to communicate through the overlay network. For most deployments this consists of management, user, voice, and IoT VLANs. It is not recommended to include guest VLANs unless full tunnel mode is required.

The configuration for branch network advertisement using Aruba IKEv2 extensions is performed per BGW group by navigating to **Gateway Management > VPN > Hub And Spoke**, setting the **Advertise branch subnets to hub** slider to **On**, and then under **Advertise branch VLANs** specify each VLAN interface that will be advertised to the VPNC hubs (Figure 4-69):

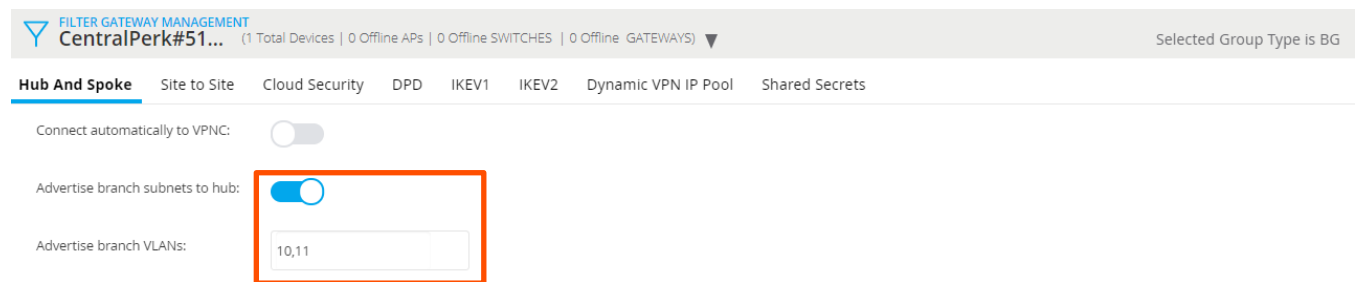


Figure 4-69 Branch VLAN Advertisement

One important thing to note is that a BGW can only advertise networks associated to its VLAN interfaces. Each specified VLAN interface must be configured with an IPv4 address and be up for the associated subnet to be advertised. A VLAN interface can be statically addressed or dynamically assigned using a dynamic DHCP pool. A BGW cannot redistribute static routes or dynamically learned routes learned from OSPF to a VPNC.



When advertising branch networks to a VPNC each BGW will also advertise its system-ip address out of each WAN uplink. The system-ip address is local to the VPNC and is not redistributed into OSPF unless the VLAN interface assigned as the system-ip is explicitly advertised.

BGW Route Summarization

To further optimize the number of routes that are advertised to VPNC hubs Aruba supports route summarization which can optionally be enabled per BGW group. Route summarization provides the ability to reduce the total number of IKEv2 routes that are advertised to VPNC hubs from each BGW when contiguous address space is allocated and implemented in branch sites.

E.g., if a BGW is configured with the local networks 192.168.88.0/25 and 192.168.88.128/25:

- **Without Summarization** – The BGW will advertise both 192.168.88.0/25 and 192.168.88.128/25 networks out of each active WAN uplink.
- **With Summarization** – The BGW will advertise the single summarized route 192.168.88.0/24 out of each active WAN uplink.

As demonstrated above, route summarization can dramatically reduce the number of overlay IKEv2 route entries that are learned and installed on VPNCs. If the VPNCs are redistributing the routes into OSPF that can also reduce the number of routing entries that are redistributed to neighboring OSPF routers. For that reason Aruba recommends assigning contiguous address space to branches whenever possible.

Router summarization can be configured per BGW group by navigating to **Gateway Management > VPN > Hub And Spoke** and setting the **Advertise branch subnets to hub** slider to **On** (Figure 4-70):

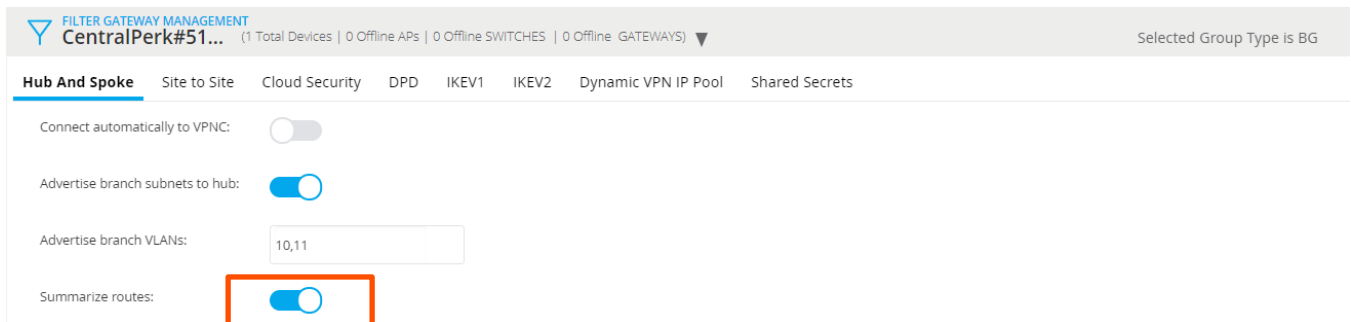


Figure 4-70 Enabling Branch VLAN Summarization

Route summarization is also an important consideration for large SD-Branch deployments since each VPNC hardware platform can only scale to support a specific number of IKEv2 overlay routes. Consider a SD-Branch deployment for 1,000 branch sites where each BGW implements 2 active WAN uplinks and advertises 4 networks. Without route summarization this deployment would result in 8,000 IKEv2 overlay routes being advertised and learned by each VPNC:

- **Calculation:** $1,000 \times 2 \times 4 = 8,000$ (Total Branch Route Entries)

With route summarization, the number of advertised IKEv2 routes could be reduced to 2,000 with each BGW advertising 1 summarized IKEv2 route per WAN uplink instead of 4 IKEv2 non-summarized routes per WAN uplink:

- **Calculation:** $1,000 \times 2 \times 1 = 2,000$ (Total Branch Route Entries)

Even if only some of the branch networks are contiguous, summarization can still reduce the overall number of IKEv2 routes that are advertised, learned, and redistributed. E.g., if two of the four branch networks are contiguous, then summarization can still reduce the overall number of IKEv2 routes by 2,000. The BGW would advertise 3 IKEv2 routes per WAN uplink (2 non-summarized and 1 summarized):

- **Calculation:** $1,000 \times 2 \times 3 = 6,000$ (Total Branch Route Entries)

Static Routes

In the majority of Aruba SD-Branch deployments static overlay routes are only required on the BGWs which are configured at per BGW group. VPNCs will dynamically learn the branch LAN routes via IKEv2 extensions, no static overlay routes are required.

Each SD-Branch deployment will require definition of static routes per BGW group so that the branches can reach the corporate network(s) via the VPN tunnels. The number of static routes that are required will depend on the addressing scheme employed, the number of WAN uplinks, and the number of VPNC hub sites. Each BGW group will require one static route to be defined per WAN uplink and VPNC hub for each remote network that needs to be reached from the branches through the overlay network.

The following steps must be performed when defining static routes through the overlay network:

1. Enter the destination IP address and network mask
2. Select the forwarding setting **Using IPsec Tunnel to VPNC**
3. Select a **VPNC name** from the drop-down list that will be the next hop
4. Select a **WAN uplink name** from the drop-down list that will be the outgoing overlay path for the route

Static routes are defined at the group level by navigating to **Gateway Management > Routing > IP Routes**. The same route must be defined for each destination per WAN uplink including backup links. Figure 4-71 provides an example of a BGW group implementing a single VPNC hub with two WAN uplinks. In this example two static routes have been defined to reach the **192.168.0.0/16** network through the VPNC named **DEMO-VPNC1** for both the MPLS and Internet WAN uplinks.

IP version:	<input type="text" value="IPv4"/>	IP version:	<input type="text" value="IPv4"/>
Destination IP address:	<input type="text" value="192.168.0.0"/>	Destination IP address:	<input type="text" value="192.168.0.0"/>
Destination network mask:	<input type="text" value="255.255.0.0"/>	Destination network mask:	<input type="text" value="255.255.0.0"/>
Forwarding settings:	<input type="text" value="Using IPSec Tunnel to VPNC"/>	Forwarding settings:	<input type="text" value="Using IPSec Tunnel to VPNC"/>
VPNC:	<input type="text" value="DEMO-VPNC1 (20:4c:03:0a:5d:70)"/>	VPNC:	<input type="text" value="DEMO-VPNC1 (20:4c:03:0a:5d:70)"/>
Uplink:	<input type="text" value="STARK_mpls"/>	Uplink:	<input type="text" value="DUFF_inet"/>
Cost:	<input type="text" value="1"/>	Cost:	<input type="text" value="1"/>

Overlay Route Example – MPLS Path
Overlay Route Example – Internet Path

Figure 4-71 *Overlay Static Route Configuration Example – Single VPNC Hub*

If a deployment includes multiple VPNC hub sites then the static routes to each VPNC hub site need to be defined at different costs. One VPNC hub site would be designated as a primary hub while the second VPNC hub site would be designated as a secondary hub site. Aruba recommends using the default cost (1) for routes pointing to the primary hub site and using a cost of 10 or higher for routes pointing to the secondary hub site. The BGW will install the lower cost routes until the VPN overlay tunnels to the primary VPNC hub site fail at which time the higher cost routes will be installed.

Figure 4-72 provides an example overlay static route configuration for a dual VPNC hub deployment. In this example:

1. Two overlay static routes have been defined to reach **192.168.0.0/16** corporate network through the primary VPNC named **DEMO-VPNC1** through the MPLS and Internet WAN paths using the default cost **1**.
2. Two overlay static routes have been defined to reach **192.168.0.0/16** network through the secondary VPNC named **DEMO-VPNC2** through the MPLS and Internet WAN paths using a cost of 10.

The lower cost routes to the primary VPNC hub are installed during normal operation:

IP version:	<input type="text" value="IPv4"/>	IP version:	<input type="text" value="IPv4"/>
Destination IP address:	<input type="text" value="192.168.0.0"/>	Destination IP address:	<input type="text" value="192.168.0.0"/>
Destination network mask:	<input type="text" value="255.255.0.0"/>	Destination network mask:	<input type="text" value="255.255.0.0"/>
Forwarding settings:	<input type="text" value="Using IPSec Tunnel to VPNC"/>	Forwarding settings:	<input type="text" value="Using IPSec Tunnel to VPNC"/>
VPNC:	<input type="text" value="DEMO-VPNC1 (20:4c:03:0a:5d:70)"/>	VPNC:	<input type="text" value="DEMO-VPNC1 (20:4c:03:0a:5d:70)"/>
Uplink:	<input type="text" value="STARK_mpls"/>	Uplink:	<input type="text" value="DUFF_inet"/>
Cost:	<input type="text" value="1"/>	Cost:	<input type="text" value="1"/>
VPNC Primary Hub – MPLS Path		VPNC Primary Hub – Internet Path	
IP version:	<input type="text" value="IPv4"/>	IP version:	<input type="text" value="IPv4"/>
Destination IP address:	<input type="text" value="192.168.0.0"/>	Destination IP address:	<input type="text" value="192.168.0.0"/>
Destination network mask:	<input type="text" value="255.255.0.0"/>	Destination network mask:	<input type="text" value="255.255.0.0"/>
Forwarding settings:	<input type="text" value="Using IPSec Tunnel to VPNC"/>	Forwarding settings:	<input type="text" value="Using IPSec Tunnel to VPNC"/>
VPNC:	<input type="text" value="DEMO-VPNC2 (20:4c:03:0a:70:5d)"/>	VPNC:	<input type="text" value="DEMO-VPNC2 (20:4c:03:0a:70:5d)"/>
Uplink:	<input type="text" value="STARK_mpls"/>	Uplink:	<input type="text" value="DUFF_inet"/>
Cost:	<input type="text" value="10"/>	Cost:	<input type="text" value="10"/>
VPNC Secondary Hub – MPLS Path		VPNC Secondary Hub – Internet Path	

Figure 4-72 *Overlay Static Route Configuration Example – Multiple VPNC Hubs*

Data Center Routing

Once the overlay routing has been configured between BGWs and VPNCs, routers and firewalls in the data center and corporate network will need to know how to reach the branch networks behind VPNCs. Depending on the deployment architecture, an administrator can either implement static routes or leverage dynamic routing via OSPF. Small deployments with single VPNC hub sites typically implementing static routes while larger deployments with multiple VPNC hub sites implementing OSPF.

Static Routes

While this guide is not intended to provide a detailed overview of how to implement static routing across all routers and firewalls in the data center and corporate network, this section provides an overview of how static routing can be implemented to provide branch reachability for single hub site deployments using standalone and L2 redundant VPNCs. Static routing is not recommended for multiple VPNC hub deployments as additional mechanisms such as IP SLA need to be

implemented on routers to provide dynamic failover between primary and secondary hub sites. That topic is out of the scope of this guide.

Most SD-Branch deployments will allocate a large CIDR block of addresses for the branch sites which are subnetted and allocated to each branch site as smaller blocks. Allocating one or more contiguous CIDR blocks of addresses to branches simplifies static routing in the data center and corporate networks as it requires a smaller number of static routes to be defined. Static routes are required on the first-hop router or firewall that connects to the VPNCs as well as the core and any intermediate aggregation layers.

One static route needs to be defined on the first-hop router or firewall for each branch CIDR range pointing to the connected VLAN interface on the VPNC (Figure 4-73). In this example a standalone VPNC and first-hop router or firewall are interconnected over VLAN 16. A single static route is defined on the first-hop router or firewall to reach the branch CIDR range 192.168.64.0/18 through the VPNCs VLAN 16 interface 192.168.16.40:

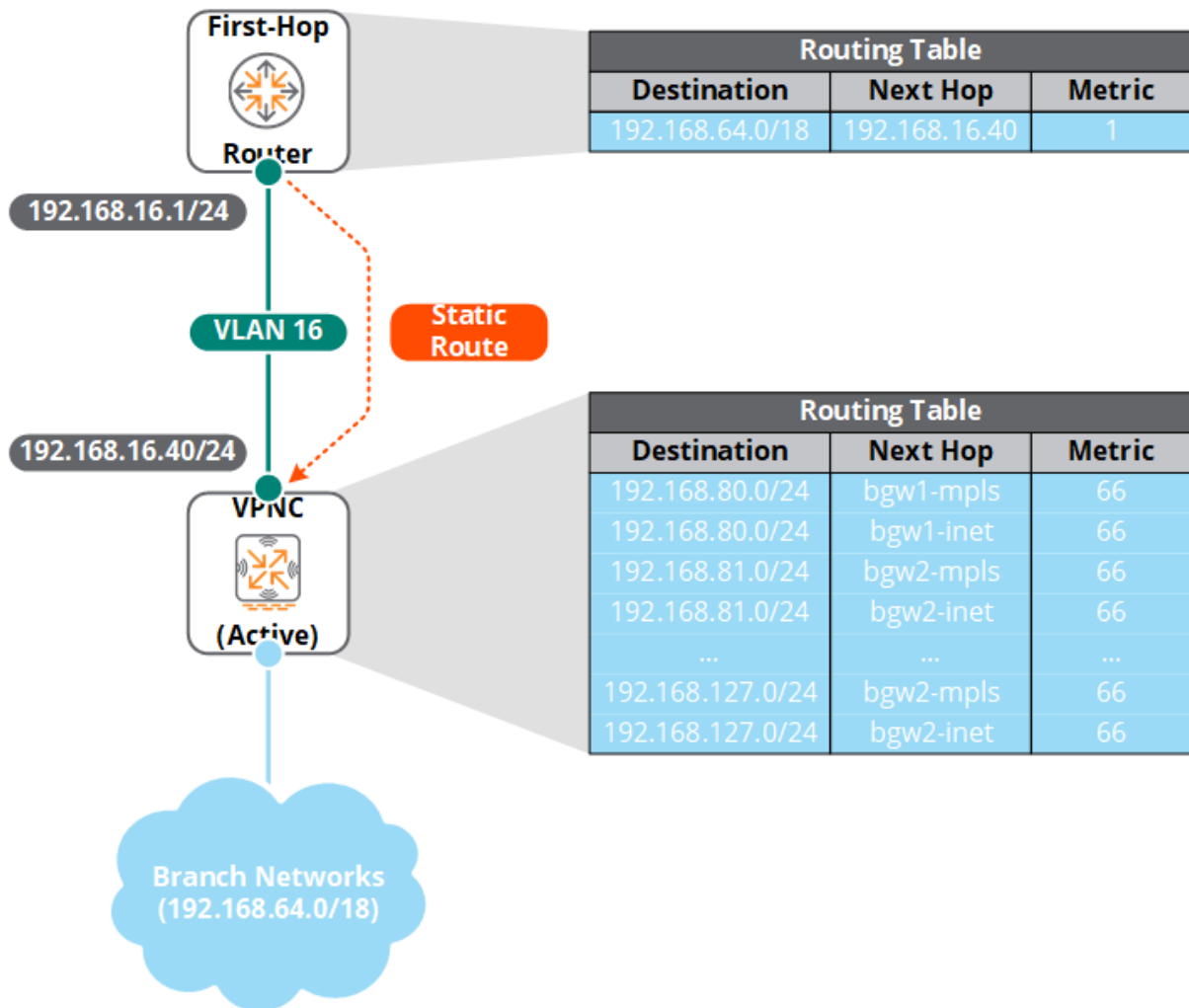


Figure 4-73 Data Center Static Route Example – Standalone VPNC

For L2 redundant VPNC deployments, additional configuration is required as VRRP needs to be configured and enabled on the VLAN interfaces that connect to the first-hop router or firewall. The VRRP virtual IP (VIP) is used as the next-hop for any static routes defined on the first-hop router or firewall. VRRP is required for this configuration as the VRRP VIP is shared between the L2 active and L2 standby VPNCs allowing the static routes to function regardless of the VRRP role of each VPNC.

During normal operation, the L2 active VPNC will terminate the overlay IPsec VPN tunnels from the BGWs and will receive and install the IKEv2 routes in its routing table. The L2 standby VPNC will not terminate any tunnels or install any routes unless it transitions to an L2 active role. Any static routes defined on the first-hop router or firewall will be forwarded to the L2 active VPNC (Figure 4-74).

In this example the L2 redundant VPNCs and the first-hop device are interconnected over VLAN 16. The VLAN 16 interfaces on the VPNC are configured with real IP addresses and the VRRP VIP 192.168.16.42. A single static route is defined on the first-hop device to reach the branch CIDR range 192.168.64.0/18 through the VRRP VIP:

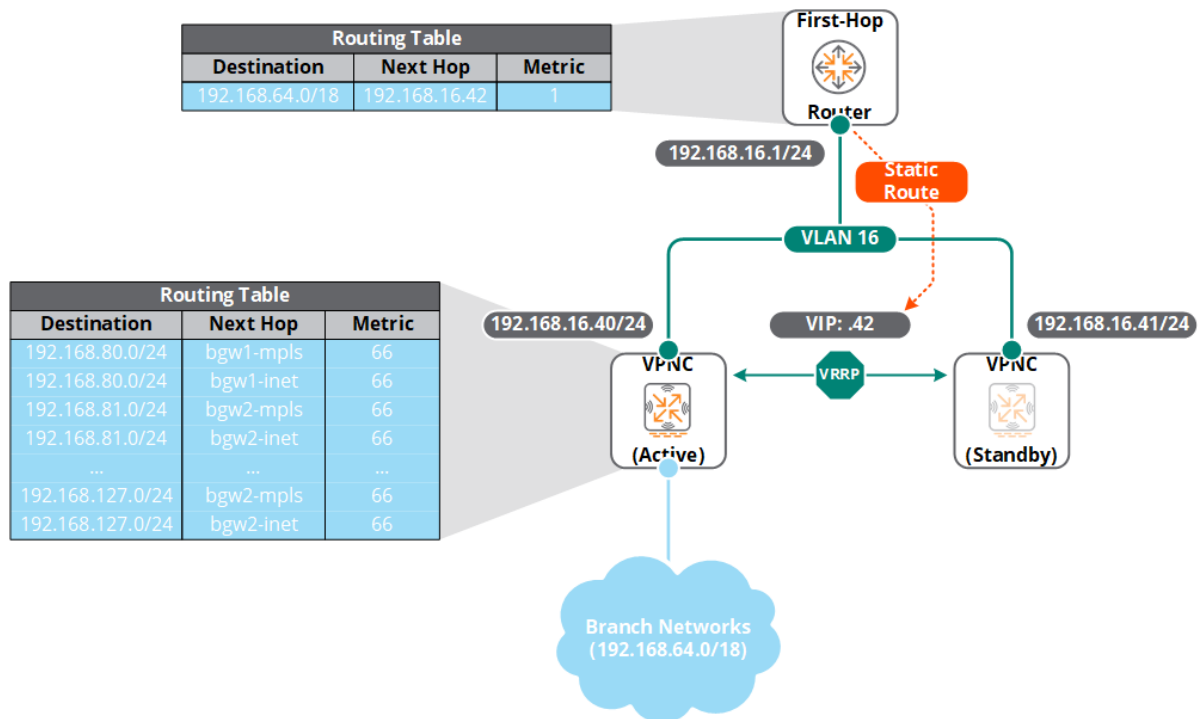


Figure 4-74 Data Center Static Route Example – L2 Redundant VPNCs



In order the configuration shown above to work VRRP tracking needs to be enabled so that the VRRP state of the VLAN interfaces that connect to the data center and WAN services are consistent. Routing issues will occur if the VRRP roles (active/standby) differ between the data center and WAN VLAN interfaces.

OSPF

For large SD-Branch deployments Aruba recommends implementing OSPF between the VPNCs and first-hop devices to dynamically exchange branch and corporate routes. OSPF is preferred for large SD-Branch deployments as it greatly simplifies router configuration and provides the ability to support failover when multiple VPNC hub sites are deployed. OSPF can not only be used to advertise branch networks into an OSPF area but can also be used by VPNCs to learn corporate routes. Aruba Gateways support OSPFv2 and can be configured to participate in Normal, NSSA, and Stub areas. The OSPF configuration and configuration will be unique to the data center architecture and requirements. Most deployments connect VPNCs to Normal OSPF areas either behind routers or firewalls in the data center.

The following points must be considered before configuring and enabling OSPF on VPNCs:

1. Aruba recommends configuring and enabling the loopback interfaces on each VPNC. This configuration is performed at the device level. The loopback interface can be used as a VPNC's system-ip as well as the OSPF router ID.
2. Perform the appropriate configuration on OSPF routers in the area to ensure that no VPNC is elected as a designated router (DR). The VPNCs will effectively operate as border routers.
3. The VPNCs are configured to redistribute IKEv2 overlay routes at a specific cost. VPNCs at the primary hub site redistributing IKEv2 overlay routes at a lower cost than the VPNCs at the secondary hub site.
4. IKEv2 overlay routes are redistributed into the OSPF areas as OSPF external type 2 routes. By default the VPNC will redistribute the IKEv2 overlay routes as they are learnt from the BGWs (summarized or non-summarized). If additional route summarization is required, this can be optionally enabled on the VPNCs.
5. A VPNC will not redistribute any learned BGWs system-ip's into the OSPF area for purposes of optimization. The VPNCs will suppress the host routes and only redistribute branch routes.

OSPF Configuration

OSPF configuration for a VPNC is device specific and is therefore performed at the device level. OSPF is enabled on a VPNC via global and per VLAN interface configuration. The OSPF global configuration determines the router-id, areas, redistribution, and summarization while the per VLAN interface configuration determines area membership.

Global OSPF configuration is performed per VPNC device by navigating to **Gateway Management > Routing > OSPF**. The following must be configured at a minimum (Figure 4-75):

1. Globally Enable OSPF.
2. Enter a router ID. This is the IPv4 address assigned to the VPNCs loopback interface.
3. Define an OSPF area(s) and set the type.

FILTER GATEWAY MANAGEMENT
CentralPerk#51... (2 Total Devices | 0 Offline APs | 0 Offline SWITCHES | 2 Offline GATEWAYS) Selected Group Type is VPNC

IP Routes Policy-Based Routing NextHop Configuration **OSPF**

Enable OSPF:

Default information:

Configured router ID: 192.168.0.40

Area	NETWORK	STUB	NO-SUMMARY	DEFAULT COST	NSSA	DEFAULT INFORMATIK	NO REDISTRIBUTION	NO LSA SUMMARY
	0.0.0.0	--	--	--	--	--	--	--

Figure 4-75 OSPF Global Configuration

After the global OSPF configuration is defined, the VLAN interface needs to be associated with an OSPF area and OSPF must be enabled. This configuration step is performed per VPNC device by navigating to **Gateway Management > Interfaces > VLANs**, and selecting a **VLAN ID**. The OSPF configuration is provided in the IPv4 configuration for per VLAN interface by selecting **Other Option** (Figure 4-76):

VLANs > DC1-INTERNET **VLAN IDs**

ID	IPv4 ADDRESS	NAT	PORT MEMBERS	ADMIN STATE	OPERATIONAL STATE	DHCP SETTINGS
4000	101.0.0.40/255.255.255.0	--	0/0/0	Enabled	--	None

IPv4 Port Members

> IP Address Assignment

Other Option

Description:

Local-proxy ARP:

Broadcast multicast optimisation:

Bandwidth contract:

Enable OSPF:

Area network (eg. 0.0.0.0): 0.0.0.0

Figure 4-76 OSPF VLAN Interface Configuration

Overlay Route Redistribution

For the VPNCs to redistribute IKEv2 overlay routes into the configured OSPF area, the **Redistribute Overlay Routes** option must be enabled and a route cost needs to be defined. Once enabled, the VPNC will redistribute the IKEv2 overlay routes into the OSPF area as External Type 2 routes at the defined cost value. The VPNC will redistribute all the IKEv2 overlay routes (except system-ip host routes) as learned from each BGW (summarized or non-summarized) by default. These can be further summarized by the VPNC prior to advertisement if required.

The following points need to be considered before configuring IKEv2 overlay route redistribution:

1. If the deployment includes L2 redundant VPNCs Aruba recommends setting the same redistribution cost on both the L2 active and L2 standby VPNCs. Only the L2 active VPNC will redistribute IKEv2 routes during normal operation, however both VPNCs will establish OSPF neighbor adjacencies.
2. If the deployment includes multiple VPNC hub sites then different redistribution costs must be specified for each hub. This is to prevent asymmetrical routing from occurring as the BGWs will establish VPN tunnels to each hub site. Aruba recommends designating one hub as primary and one hub as secondary. The redistributed route cost for the primary hub site is lower than the redistributed route cost for the secondary hub site.

Figure 4-77 shows a typical OSPF configuration for a single VPNC hub implementing L2 redundant VPNCs. The OSPF configuration and requirements for a standalone VPNC are identical to L2 redundant VPNCs. In this example the L2 active and L2 standby VPNCs are configured to redistribute IKEv2 routes into a normal OSPF area with a cost of 16. During normal operation the L2 active VPNC redistributing the IKEv2 overlay branch routes into the OSPF area. The routes are redistributed and installed on the neighboring OSPF routers as External Type 2 routes:

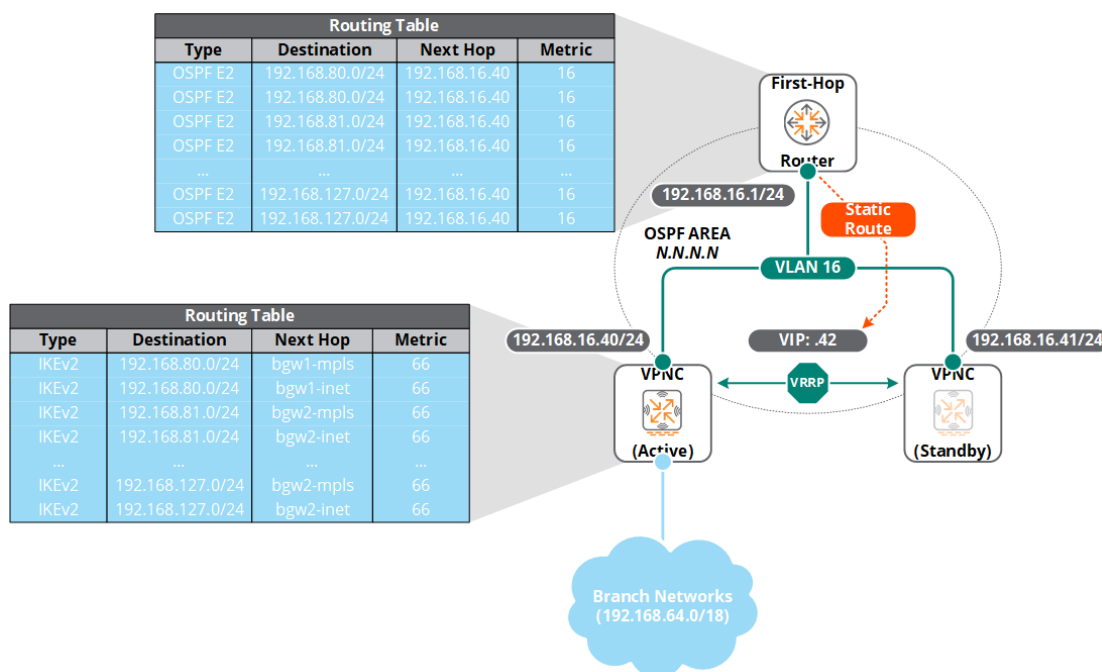


Figure 4-77 Single Hub OSPF Example – L2 Redundant VPNCs

When multiple VPNC hubs are deployed, each hub is designated as a primary or secondary hub site and will redistribute the IKEv2 routes into their respective OSPF area(s) at different costs. The VPNCs in the primary hub site re-distributing the IKEv2 overlay routes at a lower cost than the VPNCs in the secondary hub. Using different OSPF route costs for each hub is required to prevent asymmetrical routing and ensure hub to spoke traffic is forwarded to the correct VPNC. Spoke to hub traffic is forwarded to the correct hub site using static routes configured per BGW group.

The route costs defined for VPNCs for each of the hub sites will be dependent on the network topology and OSPF configuration. The redistribution costs must be set appropriately to ensure the L2 active VPNC in the primary hub is the preferred routing path during normal operation.

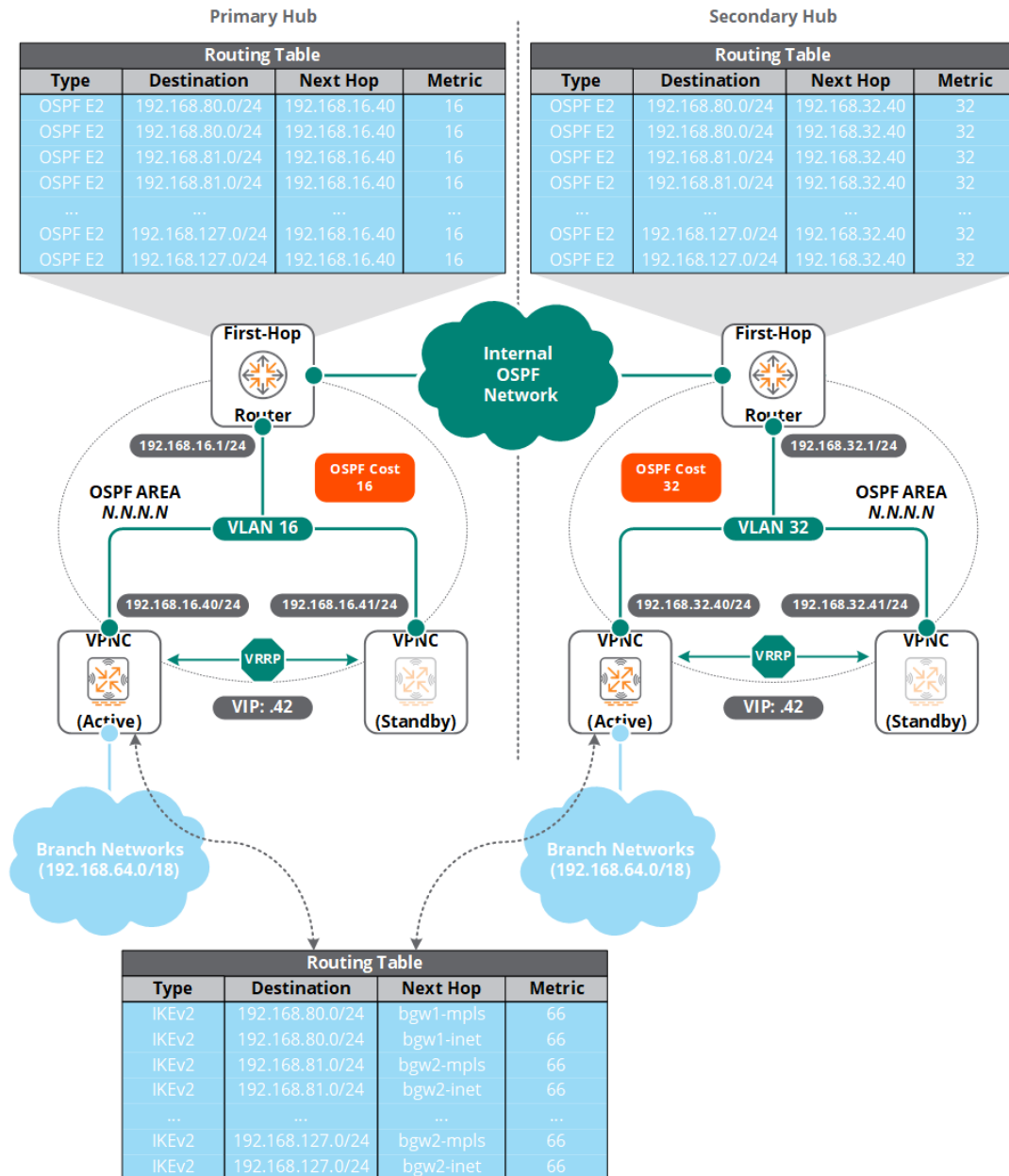


Figure 4-78 Dual Hub OSPF Example – L2 Redundant VPNCs

Figure 4-79 shows an example of OSPF configuration for a dual VPNC hub implementing L2 redundant VPNCs. In this example the primary hub VPNCs are configured to redistribute IKEv2 overlay routes at a cost of 16 while the secondary hub VPNCs are configured to redistribute IKEv2 overlay routes at a cost of 32. During normal operation the L2 active VPNC in the primary hub site is the preferred routing path to reach the branches. If the primary hub site fails, OSPF will reconverge and the L2 active VPNC in the secondary hub will become the preferred routing path.

IKEv2 route redistribution is enabled per VPNC device by navigating to **Gateway Management > Routing > OSPF** and enabling the **Redistribute overlay routes** option. A route cost must be specified for each VPNC. In the below example a route cost of **16** is specified:

The screenshot shows the OSPF configuration page for a VPNC. The page has a header with 'FILTER GATEWAY MANAGEMENT' and 'CentralPerk#51...' (with subtext '(2 Total Devices | 0 Offline APs | 0 Offline SWITCHES | 2 Offline GATEWAYS)'). The 'Selected Group Type is VPNC' is shown in the top right. The main navigation tabs are 'IP Routes', 'Policy-Based Routing', 'NextHop Configuration', and 'OSPF' (which is selected). The configuration options are: 'Enable OSPF' (checked), 'Default information' (unchecked), 'Configured router ID' (192.168.0.40), 'Redistribute VLAN ID' (empty), 'Redistribute overlay routes' (checked, highlighted with an orange box), and 'Cost for overlay routes' (16, also highlighted with an orange box).

Figure 4-79 IKEv2 Overlay Route Redistribution Configuration

Overlay Route Summarization

By default a VPNC will redistribute IKEv2 overlay routes into OSPF as they were received from each BGW. The received overlay routes will either be summarized or not by the BGW before being advertised and installed in the VPNCs routing table. Even when summarization is performed by BGWs, a VPNC's routing table may still contain a large number of IKEv2 overlay routes. It may not be desirable to redistribute these routes directly into the OSPF area but rather configure the VPNC to summarize them before advertisement.

A key feature of the OSPF protocol is the ability to summarize routes at boundaries. Since the VPNCs operate as border routers within an autonomous system, the overlay routes can be summarized by the VPNCs before being advertised into the OSPF area. Summarization reduces the amount of link state advertisement (LSA) flooding within an area as well as reduces link state database (LSDB) and route table sizes. The result is lower memory and central processing unit (CPU) utilization on the OSPF routers.

Summarization is enabled per VPNC device or group by navigating to **Gateway Management > Routing > OSPF**. The routes which need to be summarized by each VPNC can be configured in the **Overlay Route Summary Table** by clicking the blue **Plus (+)** icon. Each summarized route entry includes the CIDR **Network**, **Netmask**, and **Cost** (Figure 4-80).

Cost for overlay routes:

Route Costs Metrics

Overlay Route Summary Table		
NETWORK	NETMASK	COST
192.168.64.0	255.255.192.0	16
+		

Figure 4-80 OSPF IKEv2 Route Summarization Configuration

In the above example the VPNCs have been configured to advertise the summarized route 192.168.64.0/18 into the OSPF area at a cost of 16. The defined CIDR range covers all the networks assigned to the LAN VLAN interfaces on the BGWs. Once configured, the L2 active VPNC will advertise the defined summarized route into the OSPF area as opposed to 128 individual /25 branch routes. The route cost for each summarized route matches the global cost for overlay routes.

When multiple VPNC hubs are deployed, the same rules are followed where the summarization route costs in the primary VPNC hub are lower than the summarization route cost for the secondary VPNC hub. E.g., a summarization route cost of 16 for the primary VPNC hub and 32 for the secondary VPNC hub. The route costs used will be dependent on the network topology and OSPF configuration.

One consideration that needs to be made prior to enabling summarization on the VPNC is how it impacts BGWs during a L3 failover. If summarization is enabled, the primary and secondary VPNCs will advertise a summary route into each data center at different costs compared to redistributing the individual branch networks. If a subset of the BGWs cannot reach the primary VPNCs then the higher cost routes to reach the impacted individual branch networks via the secondary VPNCs will not be installed on the OSPF routers since the lower cost summary route via the primary VPNC will still be present in the routing tables of the OSPF routers.

The only way to support layer 3 failover for individual branches is to redistribute the individual branch networks into the OSPF areas. The branch networks are summarized by the BGWs before being advertised to the VPNCs.

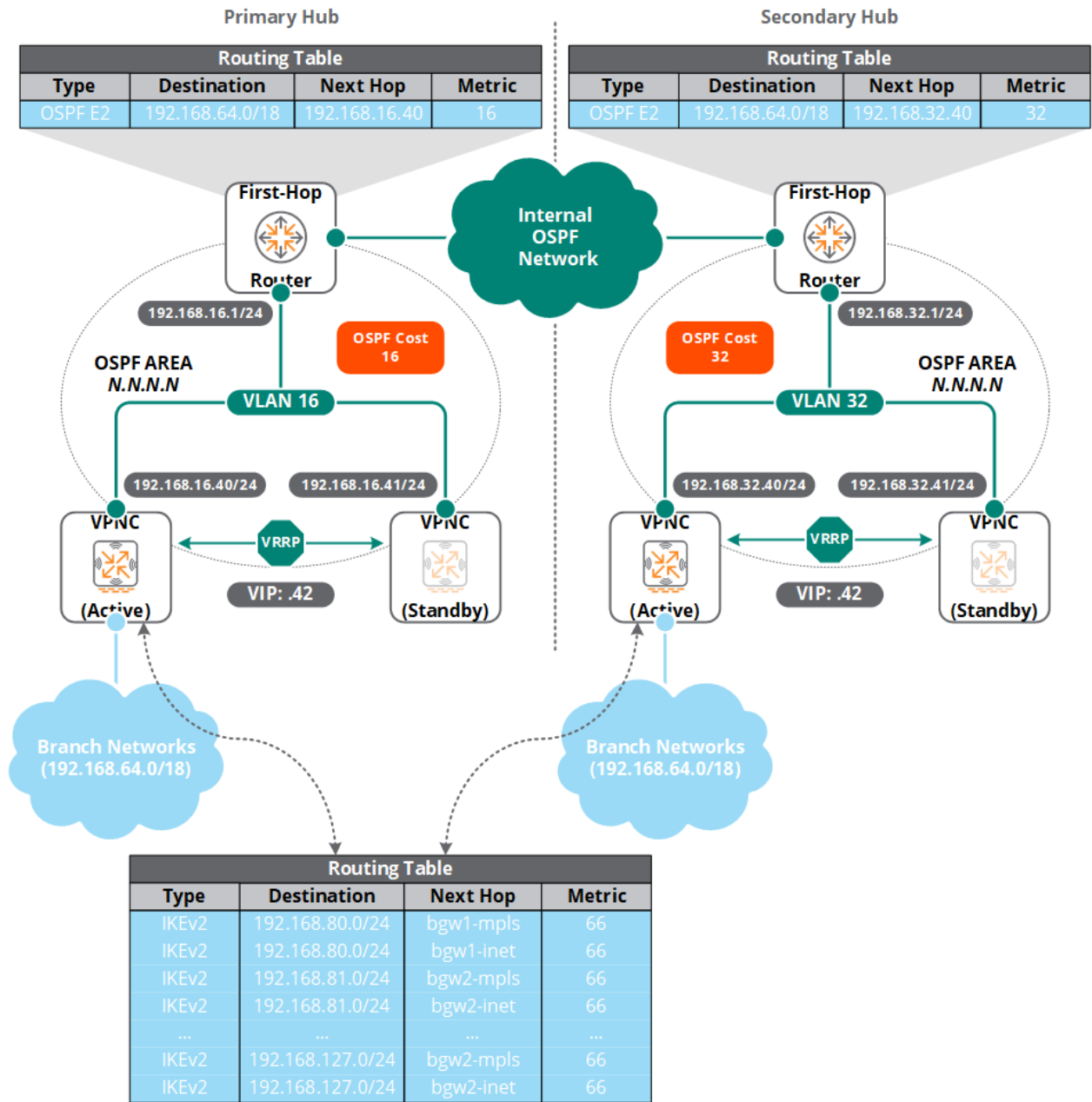


Figure 4-81 Dual Hub OSPF Summarization Example – L2 Redundant VPNCs

Policy Based Routing

All SD-Branch deployments will leverage destination based routing to forward underlay and overlay traffic, however more advanced deployments may require Policy Based Routing (PBR) to be implemented to override destination based routing when certain traffic needs to be forwarded to a specific next-hop. PBR policies can be used to override destination based routing for both underlay and overlay traffic.

Common use cases where PBR policies are implemented include:

1. Deployments where traffic from a specific subset of client's needs to be forwarded out a specific WAN uplink. E.g., guest user traffic is forwarded out a specific Internet WAN uplink.
2. Deployments requiring full-tunnel mode. E.g., a corporate security policy that requires all Internet traffic from employees to be forwarded through a hub site where it can be further inspected.
3. Deployments integrating with 3rd party SaaS or UTM providers such as Checkpoint, Palo Alto, or Zscaler where certain traffic needs to be steered through an on-prem appliance or cloud service.

A PBR configuration consists of PBR policies and next-hop lists. The PBR policy determining the traffic is routed normally and which traffic is matched and forwarded to the nexthop list. The next-hop list determines the next-hop router IP, site-to-site tunnel, or VPN tunnel the traffic is forwarded to (Figure 4-82).

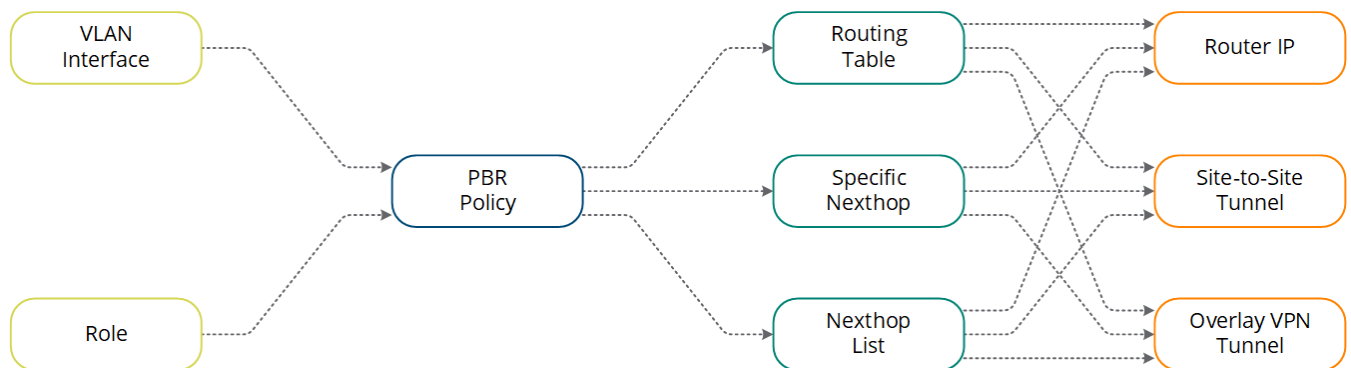


Figure 4-82 PBR Elements

PBR Policies

PBR policies include an ordered list of rules and actions that determine how traffic is forwarded. The action for each rule can either forward traffic normally, forward traffic to a specific next-hop, or forward traffic to multiple next-hops using a next-hop list:

- **Forward Regularly** – Matched traffic is forwarded normally using the VPNCs or BGWs routing table
- **Forward to IPsec Map** – Matched traffic is forwarded to a specified site-to-site tunnel
- **Forward to VPNC** – Matched traffic is forwarded to a specified VPN tunnel
- **Forward to Next-hop List** – Matched traffic is forwarded to destinations defined in the next-hop list consisting of multiple next-hop destinations

The action selected will depend on organizational requirements. Most SD-Branch deployments implementing PBR policies in branches select the Forward to Next-hop List option since it allows multiple next-hop routers or VPN tunnels to be utilized for load-balancing and failover purposes. A typical use case would be when full-tunnel mode is required for employees.

A PBR policy and its rules are typically configured per VPNC or BGW group by navigating to **Gateway Management > Routing > Policy-Based Routing**. Each PBR policy must have a unique name and contain at least one rule.

When defining rules in a PBR policy, Aruba recommends defining the most specific rules first and the least specific rules last. As with firewall rules, PBR rules are evaluated in order, the first matched rule and action will be selected. This is demonstrated in Figure 4-83 where PBR policy rules are defined in a BGW group to provide full-tunnel mode to employees. In this example the most specific rule matching corporate traffic (destination 192.168.0.0/16) is defined before the rule matching Internet traffic (destination any). This rule order ensures that traffic destined to a local or corporate network is routed normally and not matched by the forward to next-hop list rule. If the least specific rule was placed first, all traffic would match that rule and the second more specific rule would be ignored.

IP Routes **Policy-Based Routing** NextHop Configuration OSPF

Policies			
NAME	RULES COUNT	POLICY USAGE	
full-tunnel	2	--	
master-boc-traffic	0	--	
uplink-lb-cfg-racl	0	--	
uplink-lb-sys-racl	0	--	
+			

Policy > full-tunnel Rules					Drag rows to re-order
IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	
IPv4	any	192.168.0.0 255.255.0.0	any	forward	
IPv4	any	any	any	route next-hop-list overlay-network	
+					

Figure 4-83 Policy Based Routing Configuration Example

Next-hop Lists

PBR requires a next-hop list to be configured which is referenced by the PBR policy. The next-hop list defines the router IPv4 addresses, IPsec maps, or VPN tunnels where matched traffic will be forwarded. Each next-hop list can include either a single next-hop entry or multiple next-hop entries. When multiple next-hop entries are defined a priority can be specified that determines preference. The next-hop entry with the highest priority will be preferred.

Next-hop lists are configured per VPNC or BGW group by navigating to **Gateway Management > Routing > Next-hop Configuration**. A unique **Name** needs to be specified for the next-hop list as well as minimum of one device. Each entry type requires a specific configuration:

- **IP / DHCP** – Requires specification of the VLAN Interface (DHCP) or the next-hop router IP along with a priority
- **IPsec Map** – Requires selection of a site-to-site IPsec Map name and a priority
- **VPNC** – Requires selection of a VPNC name, uplink and a priority.

Figure 4-84 provides an example of each next-hop type:

Add NextHop IP/DHCP	Add New IPsec Map	Add New IPsec Map
NextHop: <input type="radio"/> IP <input checked="" type="radio"/> DHCP	Forward settings: Using Site-to-Site IPsec	Forward settings: Using IPsec Tunnel to VPNC
VLAN ID: 4094	Using site-to-site: zscaler	Using IPsec tunnel to: DEMO-VPNC1 (20:4c:03:0a:5d:70)
Priority: 128	IPsec: zscaler	VPNC: DEMO-VPNC1 (20:4c:03:0a:5d:70)
	Priority: 128	Uplink: STARK_mpls
		Priority: 128
IP Next-hop Example	IPsec Map Next-hop Example	VPNC Next-hop Example

Figure 4-84 Next-hop Entry Examples



The next-hop configuration for a VPNC includes all of the options listed above except for the section of a VPNC device as a next-hop. Most VPNC configurations implement IP based next-hop entries to enable full-tunnel mode depending on the data center topology.

The priorities defined for each next-hop IP, IPsec map, or VPN tunnel influence the next-hop that is selected for the matched traffic. If the next-hop entries are defined with different priorities then entry with the highest priority will be selected unless the device or tunnel is unreachable. If two or more next-hop entries are defined with equal priorities then the matched traffic will either be load-balanced or steered based on DPS policies. The next-hop configuration provides the uplink

manager or DPS with a list of available next-hop devices that can be used for underlay or overlay routing.

Figure 4-85 provides an example next-hop configuration for BGW group to implement full-tunnel for employees. In this example the BGW has two WAN uplinks and a primary and secondary VPNC hub. Four VPNC next-hop entries are defined in the next-hop list at different priorities. Two entries are for the VPN tunnels to the primary VPNC hub and two entries are for the for the VPN tunnels to the secondary VPNC hub. The priorities for the VPN tunnels to the primary VPNC hub are higher than the priorities to the secondary VPNC hub.

During normal operation, the PBR policy will select the higher priority VPN tunnels. Traffic is either load-balanced between tunnels or steered using DPS. If the primary VPNC hub becomes unreachable then the matched traffic is switched to the lower priority VPN tunnels.

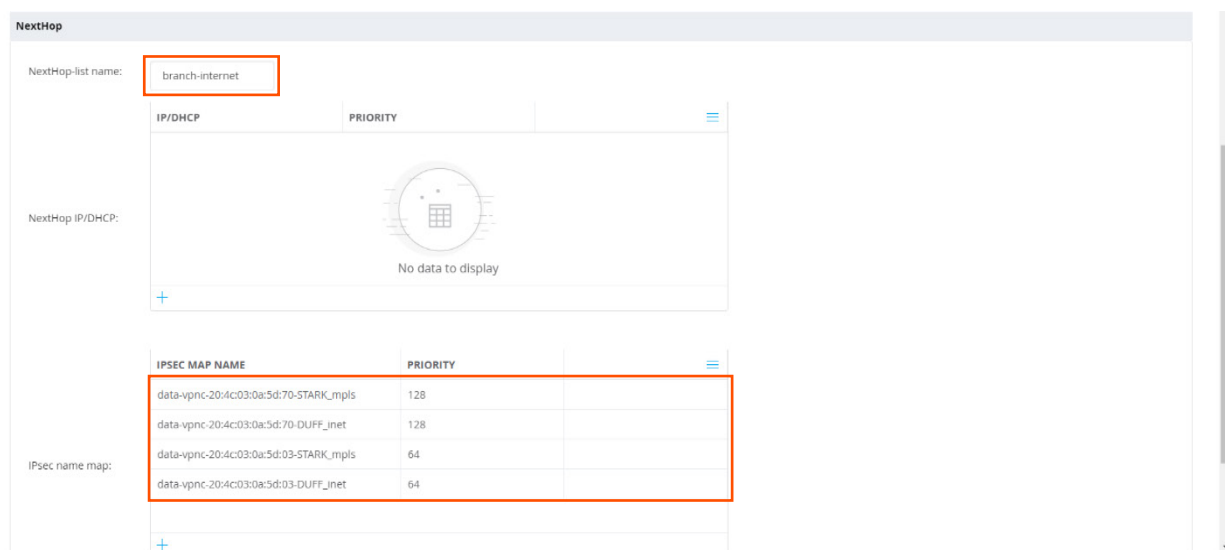


Figure 4-85 Next-hop List Configuration Example

PBR Assignment

In order for a PBR policy to be active it must be applied to a traffic path. Where the PBR policy is applied will be different for a VPNC than for a BGW. For BGWs, the PBR policies are applied to user traffic received by a BGW before the traffic is forwarded out the underlay or overlay network. The PBR policies can either be applied to a VLAN interface or a user role. For VPNCs the PBR policies are applied to user traffic received through the VPN tunnel. A use case would be branch traffic destined for the Internet that needs to be forwarded to a specific firewall or router in the data center. The requirement for implementing a PBR policy on VPNCs is dependent on the data center topology (see reference architectures section X).

VLAN Interfaces

PBR policies are typically assigned to VLAN interfaces per BGW group by navigating to **Gateway Management > Interfaces > VLANs** and choosing a **VLAN ID**. The ACL configuration is provided in the **IPv4** configuration for per VLAN interface by selecting **Other Option**. The PBR policy is assigned in the **ACL** drop-down menu (Figure 4-86):

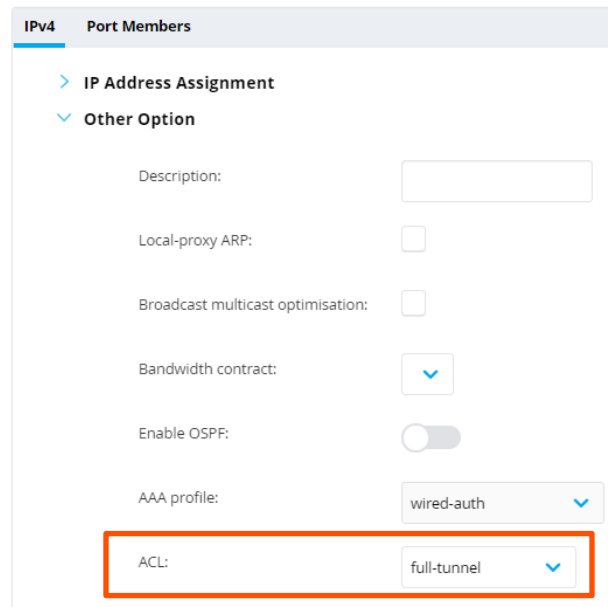


Figure 4-86 Assigning a PBR Policy to a VLAN Interface

User Roles

PBR policies are typically assigned to user roles per BGW group by navigating to **Gateway Management > Security > Roles**. Select the role name that will be assigned to the PBR policy and then select **Show Advanced View**. Select the blue **Plus (+)** icon:

1. Select **Add an existing policy**
2. Set the **Policy type** to **Route**
3. Select the PBR policy in the **Policy name** drop-down menu

An example of a PBR policy being assigned to a user role is provided in Figure 4-87:

FILTER GATEWAY MANAGEMENT
CentralPerk#51... (1 Total Devices | 0 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS) ▼ Selected Group Type is BG

Roles Policies Aliases Applications Apply Policies Auth Servers AAA Profiles L2 Authentication L3 Authentication Advanced Firewall

Roles 12

NAME	RULES	
ap-role	35 Rules	
authenticated	6 Rules	
default-via-role	3 Rules	
default-vpn-role	4 Rules	
guest	11 Rules	
guest-logon	27 Rules	

authenticated Policies Bandwidth More

NAME	RULES COUNT	TYPE	POLICY USAGE
ra-guard	1	session	ap-role, authenticated, default-vpn-role, gu
v6-allowall	1	session	authenticated, default-via-role, default-vpn-
allowall	2	session	authenticated, default-via-role, default-vpn-
apprf-authenticated-sacl	0	session	authenticated
global-sacl	0	session	authenticated, default-via-role, default-vpn-
full-tunnel	2	routing	authenticated

Figure 4-87 Assigning a PBR Policy to a User Role

VPN Tunnels

PBR policies can be assigned per VPNC device or per VPNC group. A PBR policy can be assigned to a VPNC by navigating to **Gateway Management > VPN > Hub And Spoke**. The PBR policy is assigned using the Route ACL drop-down menu (Figure 4-88):

ACL types:

Route ACL: ▼

Session ACL: ▼

Figure 4-88 Assigning a PBR Policy to VPN Tunnels

Reference Topologies

This section provides tested and validated reference topologies for both data centers and branches which can be followed to implement an end-to-end Aruba SD-Branch solution. The reference topologies for data centers and branches are intended to be combined based on existing data center topology and business requirements. Aruba supports various data center and branch topologies that not captured in this section. E.g., data center topologies implementing dual Internet WAN services. If an Aruba SD-Branch deployment requires a data center or branch topology, please engage an Aruba account team.

Data Center Topologies

The following section provides an overview and details for the tested and validated data center topologies that can be referenced to implement Aruba gateways in data center(s). This guide provides the configuration requirements and detailed examples for each reference topology:

1. VLANs and VLAN Interfaces
2. Layer 2 redundancy
3. Underlay and overlay routing
4. Layer 3 redundancy (dual data centers)

For each reference topology, detailed diagrams are provided to visualize the configurations, session paths, and routing. Implementation details are provided for a single data center design with dual data center implementation details being provided at the end of each section. This approach is taken as a dual data center implementation is a mirror of a single data center design with only minor routing changes.

While the primary focus of this section centers on the configuration and connectivity requirements for the standalone or L2 redundant VPNCs, the relevant configuration for the edge firewalls, core/aggregation switches, and zones used to validate this topology are provided for convenience.

Internet Only with Single Network Zone

The following topology represents the simplest deployment model where a standalone VPNC or L2 redundant pair of VPNCs implement a single VLAN interface to connect to an edge firewall in a single data center. This can be considered as a one-armed design where the VPN tunnel termination and the forwarding of branch traffic are both performed by the standalone or L2 active VPNC using a single IP interface.

This topology is typically followed for Aruba SD-Branch deployments using Internet based WAN services where the data center connects to one or two ISPs. For simplification purposes this

section focuses on a single ISP design. Each BGW initiates a VPN tunnel to the standalone/L2 active VPNC to establish the overlay network:

1. **Internet VPN Tunnels (UDP 4500)** – All Internet VPN tunnels are terminated by the VLAN 4001 interface on the standalone/L2 active VPNC
2. **Branch Traffic** – All deencapsulated branch traffic is transmitted and received by the VLAN 4001 interface on the standalone/L2 active VPNC
3. **Full-Tunnel Mode** – If implemented, all branch traffic destined to the Internet is transmitted and received by the VLAN 4001 interface on the standalone/L2 active VPNC

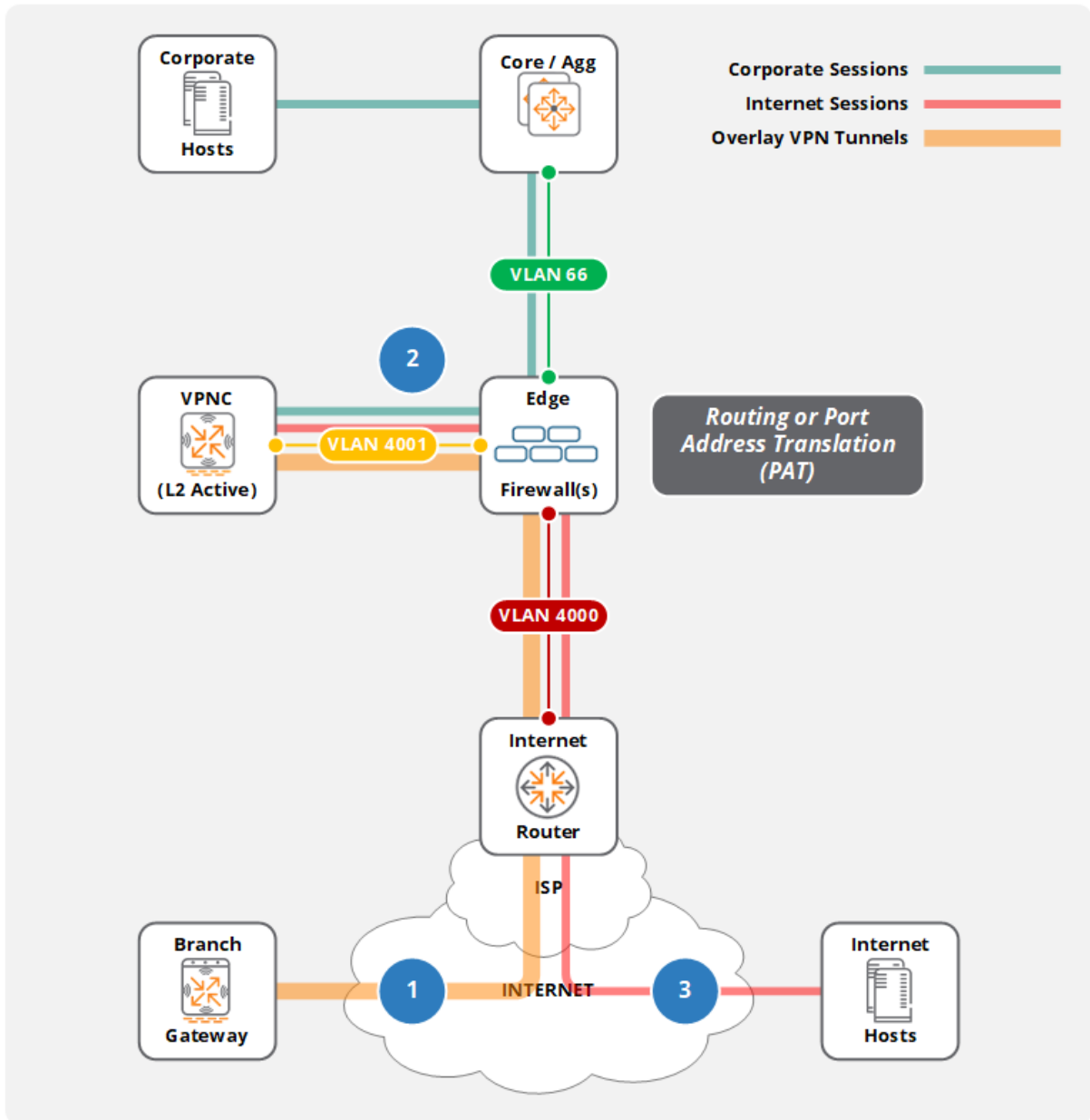


Figure 5-1 Flow Diagram

Figure 5-2 provides the logical topology which will be used in this section. The network is separated into three zones that are interconnected using an edge firewall to better explain the concepts, configurations, and traffic flows. This topology can support standalone VPNC or L2 redundant VPNCs that are connected to an edge firewall in the VPNC zone using one VLAN Interface:

- **VLAN 4001** – Used to terminate VPN tunnels from the Internet as well as transmit/receive deencapsulated traffic from the branches.

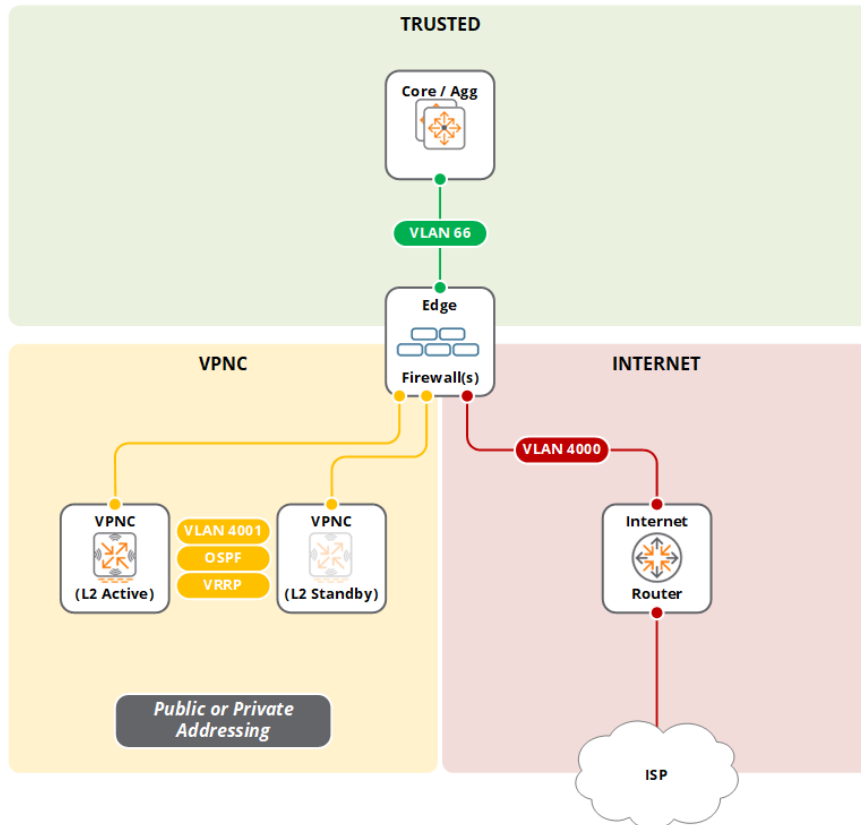


Figure 5-2 Reference Topology

CIDR Allocation

To better understand the address allocation for each zone as well as the underlay/overlay routing later in this section it is important to provide an overview of the CIDR addressing scheme that has been used for this reference architecture. Contiguous ranges of addresses are allocated to the corporate network and branches to simplify routing:

- **Corporate** - The corporate network is allocated the 192.168.0.0/17 CIDR range. For this reference topology the following address space is used from the network block of VLAN 66 – 192.168.66.0/24.
- **Branch** - All branch networks are allocated from the 192.168.128.0/17 CIDR range. This includes system IP addresses, management VLAN interfaces, and user VLAN interfaces.

- **Internet** - The Internet Service Provider (ISP) has been allocated the 23.216.134.0/24 CIDR range.

Virtual LANs

Several VLANs are required to ensure connectivity between devices in the different zones of this topology:

- **VPNCs to VPNC Zone** - One VLAN is required to connect the standalone/L2 redundant VPNCs to the edge firewall. In this example VLAN 4001 is used.
- **Edge Firewall to Trusted Zone** - One VLAN is used to connect the edge firewall to the core/aggregation layer in the trusted zone. In this example VLAN 66 is used.
- **Edge Firewall to Internet Zone** - One VLAN is used to connect the edge firewall to the Internet router. In this example VLAN 4000 is used.

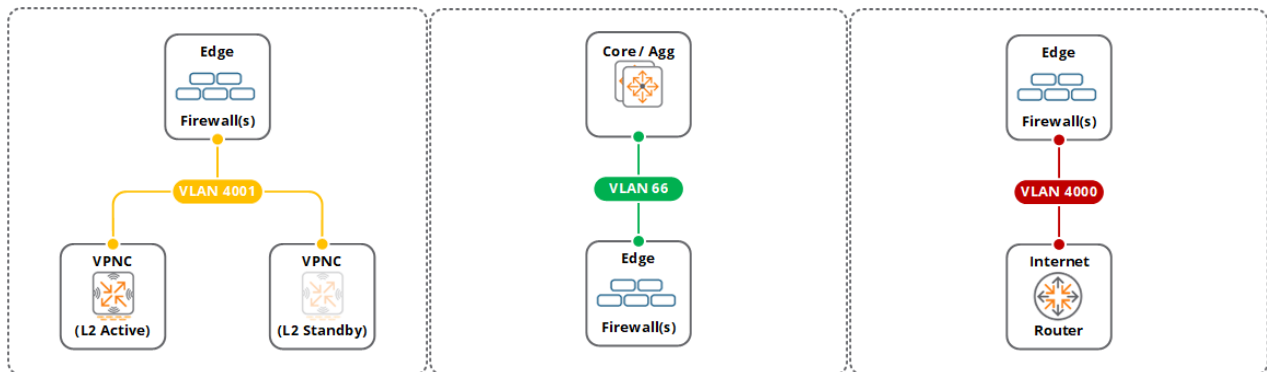


Figure 5-3 Internet Only with Single Network Zone Topology VLANs



If the edge firewall implements routed ports instead of VLAN interfaces then adjust the configuration accordingly. If the edge firewall implements routed ports and the deployment requires L2 redundant VPNCs, a layer 2 aggregation switch will need to be deployed to connect the VPNCs.

Ports

This reference topology can support connecting the standalone or L2 redundant VPNCs using a single port or multiple ports. When a single port is implemented it is configured as a trunk with each VLAN 802.1Q tagged out the port. The standalone or L2 redundant VPNCs are typically connected to a L2 aggregation switch. If multiple ports are implemented, each port is configured with a specific VLAN and connected to its respective peer device such as an edge firewall or the core/aggregation layer. The VPNCs support standards based link aggregation allowing multiple ports to be assigned to a LAG group if additional bandwidth and fault-tolerance is required. A single LAG may be connected to a L2 aggregation switch or multiple LAGs connected to different peer devices as port-density allows.

As a best practice Aruba recommends the following:

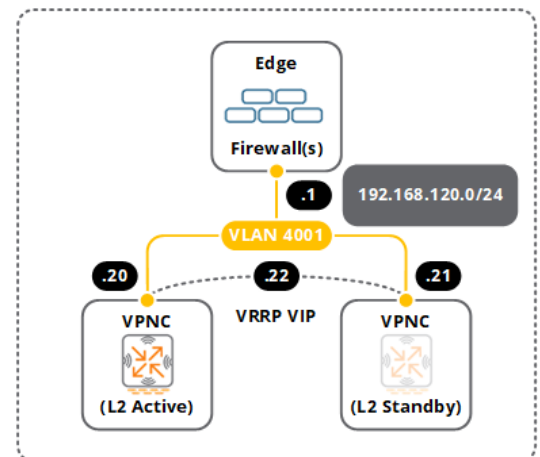
1. Configure each port or LAG as a trunk and 802.1Q tagging each VLAN. Using trunk ports or LAGs on the VPNCs allows additional VLANs to be added in the future with no interruption to existing underlay or overlay traffic.
2. Configure the ports/LAGs and VLANs as trusted. The VPNC will not be performing any L2 or L3 authentication for the overlay traffic.

VLAN Interfaces

This reference topology consists of IP interfaces in different zones that utilize public as well as private addressing.

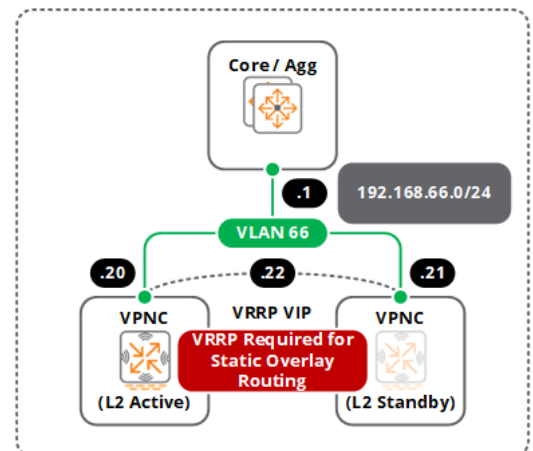
VPNC to Edge Firewall (VPNC Zone)

- Internet underlay VLAN interface
- Can be public or private addressing
- Public address space is allocated by the ISP
- In this example the standalone/L2 redundant VPNCs are connected to the edge firewall in the VPNC zone using the **192.168.120.0/24** private network
- VPNC Address Requirements:
 - Standalone VPNC – 1 address
 - L2 Redundant VPNCs – 3 addresses (2 host and 1 VRRP)



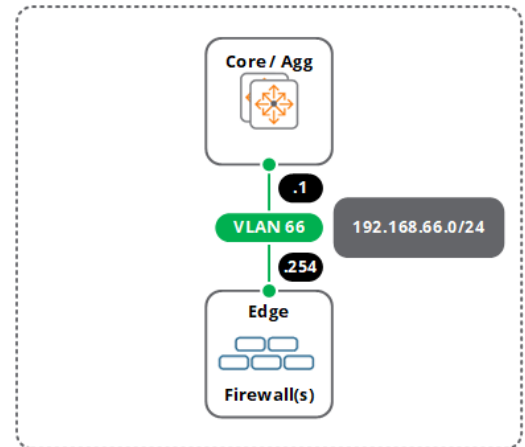
VPNC to Core/Aggregation Layer (Trusted Zone)

- Overlay traffic VLAN interface
- In this example the standalone/L2 redundant VPNCs are connected to the core/aggregation layer in trusted zone using the **192.168.66.0/24** network
- VPNC Address Requirements:
 - Standalone VPNC – 1 address
 - L2 Redundant VPNCs (Static Overlay) – 3 addresses (2 host and 1 VRRP)
 - L2 Redundant VPNCs (OSPF) – 2 addresses



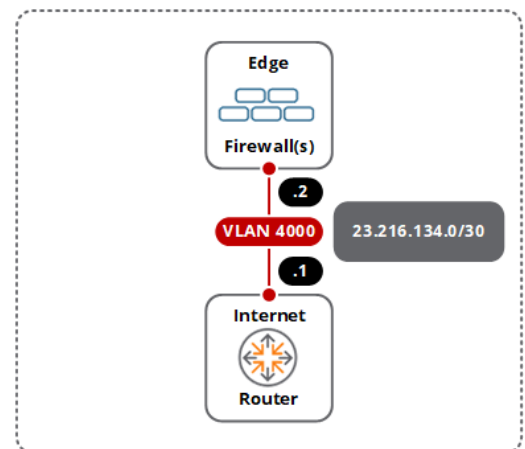
Edge Firewall to Core/Aggregation Layer (Trusted Zone)

- Core/aggregation layer to edge firewall interconnect VLAN
- In this example the edge firewall are is connected to the core/aggregation layer in trusted zone using the **192.168.66.0/24** network
- Address requirements are deployment specific



Edge Firewall to Internet Router (Internet Zone)

- Edge firewall to Internet router interconnect VLAN or routed interfaces
- Requires public addressing assigned by the ISP
- In this example edge firewall is connected to the Internet router in the Internet zone using the **23.216.134.0/30** network
- Address requirements will be deployment specific



L2 Redundancy

This reference topology can support a standalone VPNC or pair of L2 redundant VPNCs. When a L2 redundant pair of VPNCs is deployed, VRRP is enabled on the VLAN interfaces that terminate the VPN tunnels. For this reference architecture this would include VLAN 4001. One VPNC in the pair is active and terminates the VPN tunnels and forwards the overlay traffic during normal operation. The second VPNC in the pair operating as a standby unit. The forwarding of traffic is performed by the active VPNCs host IP address and not the virtual IP address.

L2 redundancy leverages VRRP where the assigned VRRP priority determines the role of each VPNC. The VPNC assigned the highest priority assumes an active role while the VPNC assigned the lowest priority assuming a standby role. Each L2 redundant pair of VPNCs requires a host address along with virtual address that is shared between the VPNCs. The VRRP virtual IP interface is used to terminate the VPN tunnels as well as provide underlay and overlay routing during normal operation.

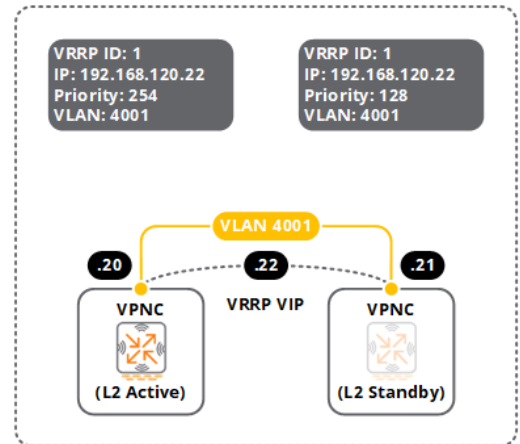
For this topology VRRP will be enabled on one of the VLAN interfaces for VLAN 4001 that terminates the VPN tunnels initiated over the Internet WAN services and carries overlay traffic:

Active VPNC (Internet underlay VLAN interface)

- VLAN Interface 4001
- A unique common VRRP ID within the broadcast domain (VRRP ID 1 in this example)
- Assigned the highest VRRP priority 254

Standby VPNC (Internet underlay VLAN interface)

- VLAN Interface 4001
- A unique common VRRP ID within the broadcast domain (VRRP ID 1 in this example)
- Assigned the VRRP priority 128



Routing

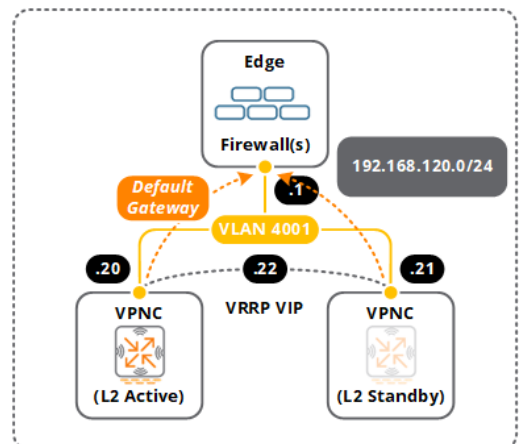
Underlay Routing

For this reference topology underlay routing is achieved on the standalone/L2 redundant VPNCs by defining default gateways and static routes. The default gateway configuration provides reachability to the Internet while static routes provide reachability to the MPLS network.

The routing configuration required for the edge firewall and Internet router will be dependent on the Internet architecture. Each device either implements dynamic routing such as BGP or default routes.

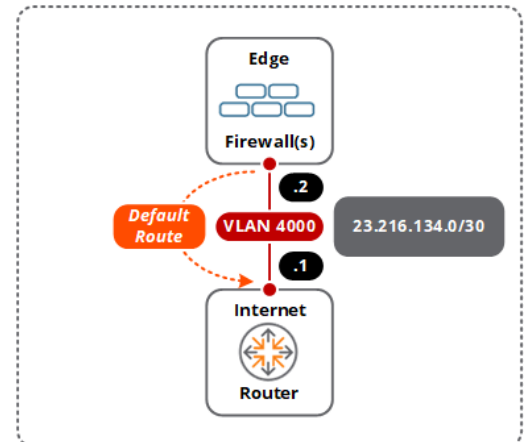
VPNC (Internet Reachability)

- Each VPNC requires a default gateway to be configured to provide reachability to the Internet
- The next-hop router address is the host address assigned to the edge firewall in the VPNC zone
- In this example each VPNC is configured to use **192.168.120.1** as their default gateway



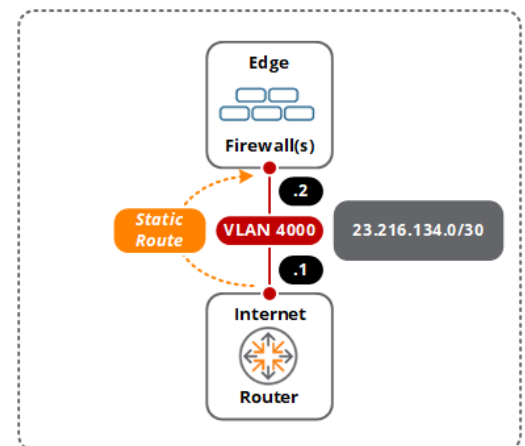
Edge Firewall (Internet Reachability)

- Requires a default route to provide reachability to the Internet (can be dynamically learned via BGP or statically defined)
- The next-hop router address is the address assigned to the Internet router in the Internet zone
- In this example the edge firewall has a static default route configured as **23.216.134.1**



Internet Router (VPNC Zone Reachability)

- If public addressing is implemented in the VPNC zone then the Internet router must be able to reach the public network behind the edge firewall.
- This can either be dynamically learned via BGP or statically defined
- The next-hop router address is the address assigned to the edge firewall in the Internet zone
- The standalone/L2 redundant VPNCs in this example do not implement public addressing so no routes are required on the Internet router



Overlay Routing

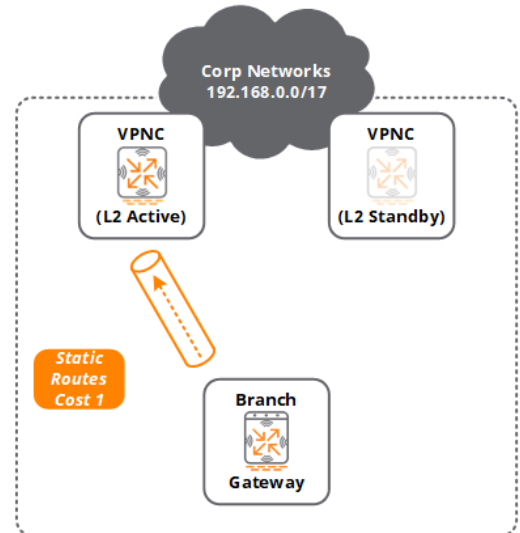
This reference topology can support static or dynamic routing to provide reachability between the corporate and branch networks through the overlay network. Static routing is typically implemented for smaller deployments where dynamic routing has not been implemented in the core/aggregation layers. Dynamic routing using OSPF provides the most flexibility since individual branch routes or a summary of the branch routes are automatically advertised and redistributed to the edge firewall and core/aggregation layers.

Static Routing

SD-Branch deployments implementing static routing require administrators to configure static routes on the standalone/L2 redundant VPNCs, edge firewall, and core/aggregation layers to provide reachability between the corporate and branch networks:

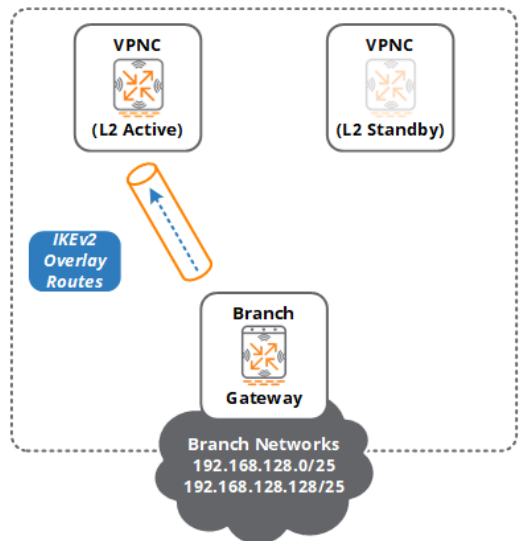
BGW (Corporate Network Reachability)

- Each BGW group is configured with static routes to reach the corporate networks using the Internet VPN tunnels established to the standalone/L2 redundant VPNCs
- In this example the static route cost to reach the corporate network **192.168.0.0/27** through the standalone/L2 redundant VPNCs for each VPN tunnel is defined as **1**



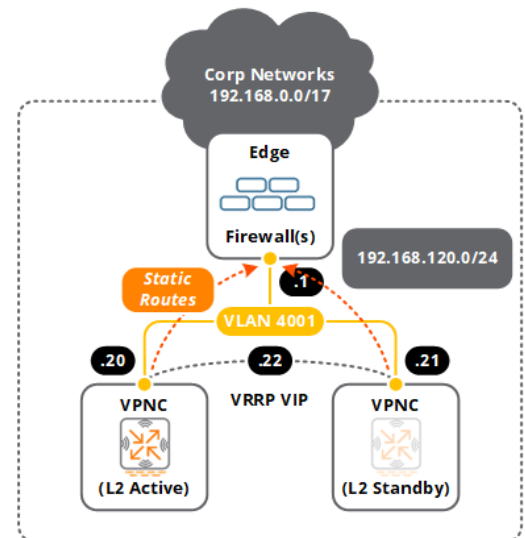
VPNC (Branch Network Reachability)

- Per Aruba best practices, each branch gateway is configured to advertise their local branch networks to the standalone/L2 active VPNC through the VPN tunnels using Aruba IKEv2 extensions.
- This eliminates the need for defining static routes to reach the remote branch network on the VPNCs



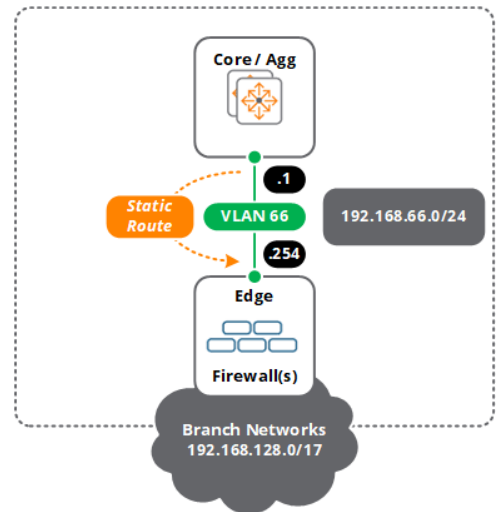
VPNC (Corporate Network Reachability)

- Requires static routes to reach the corporate networks through the edge firewall
- In this example one static route is defined on the standalone/L2 redundant VPNCs to reach the **192.168.0.0/17** network through the edge firewall via **192.168.120.1**



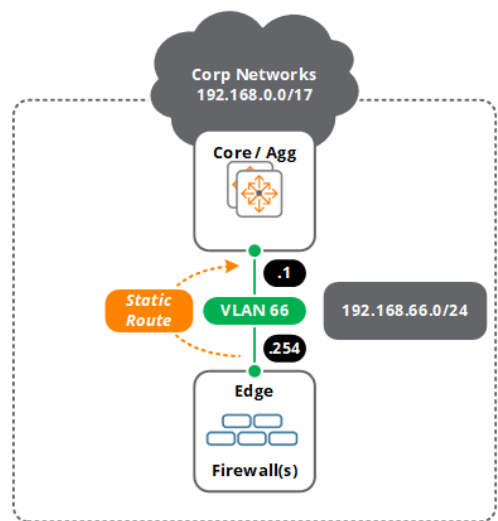
Core/Aggregation (Branch Network Reachability)

- Requires static routes to reach the branch networks through the edge firewall
- In this example one static route is defined on the core/aggregation layer to reach the **192.168.128.0/17** branch networks through the edge firewall via **192.168.66.254**



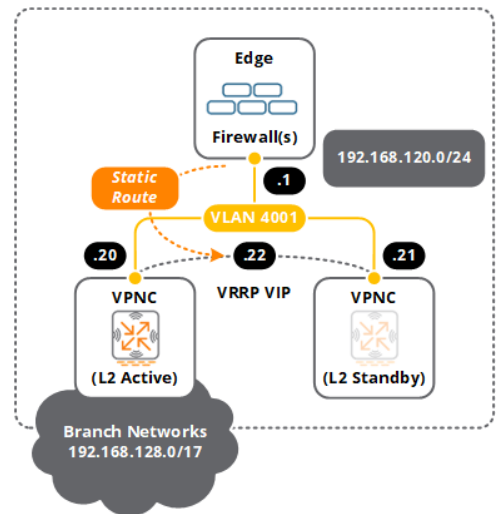
Edge Firewall (Corporate Network Reachability)

- Requires static routes to reach the corporate networks through the core/aggregation layer.
- In this example one static route is defined on edge firewall to reach the **192.168.0.0/17** network through the core/aggregation layer via **192.168.66.1**



Edge Firewall (Branch Network Reachability)

- Requires static routes to reach the branch networks through the standalone/L2 redundant VPNCs
- In this example one static route is defined on edge firewall to reach the **192.168.128.0/17** branch networks through the L2 redundant VPNCs via the VRRP virtual IP **192.168.120.22**



Dynamic Routing (OSPF)

Dynamic routing requires OSPF to be configured on the core/aggregation switches, edge firewall, and VPNCs. The OSPF configuration for each device and zone is organizationally specific. When OSPF is enabled and configured the standalone or L2 active VPNC will automatically redistribute connected branch routes in the trusted network using the overlay traffic VLAN. The routes are learned by the edge firewall and core/aggregation layers.

Branch routes can be redistributed into the OSPF area in two ways:

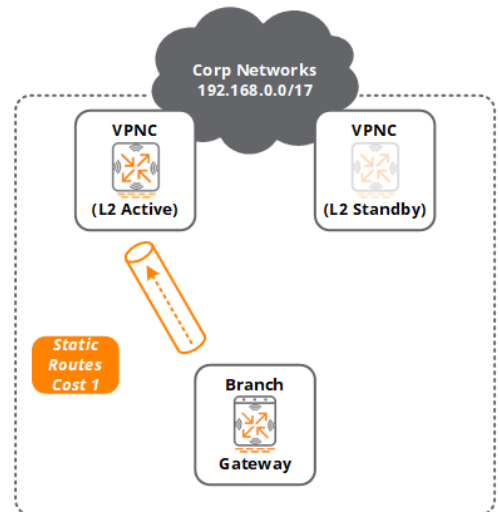
1. Individual branch routes can be redistributed into the OSPF area at a configured cost as learned by the standalone/L2 active VPNC. Each route is installed by the OSPF routers as External Type 2 routes at the specified cost.
2. One or more summary routes for can be redistributed into the OSPF area at a configured cost by the standalone/L2 active VPNC. Each summary route being installed by the OSPF routers as External Type 2 routes at the specified cost.



For large SD-Branch deployments utilizing a single data center Aruba recommends configuring summary routes as this will consume less CPU and memory resources on the OSPF routers in the network.

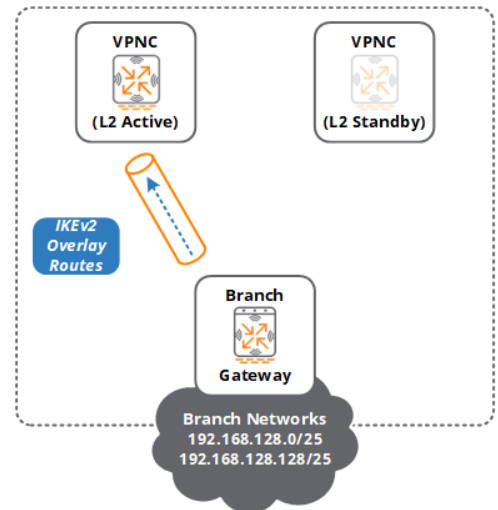
BGW (Corporate Network Reachability)

- Each BGW group is configured with static routes to reach the corporate networks using the MPLS and Internet VPN tunnels established to the standalone/L2 redundant VPNCs.
- In this example the static route costs to reach the corporate network **192.168.0.0/27** through the standalone/L2 redundant VPNCs for each VPN tunnel is defined at a cost of **1**



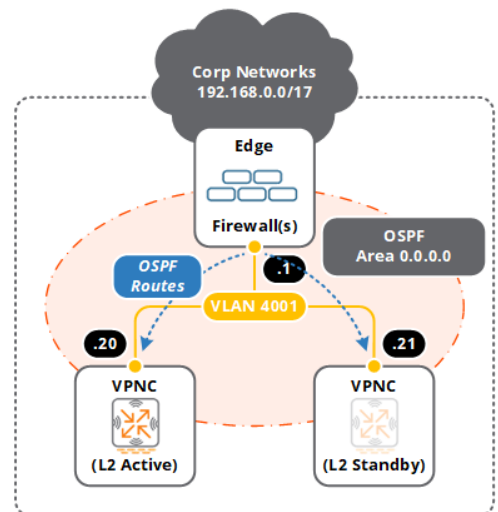
VPNC (Branch Network Reachability)

- Per Aruba best practices, each branch gateway is configured to advertise their local branch networks to the standalone/L2 active VPNC through the VPN tunnels using Aruba IKEv2 extensions.
- This eliminates the need for defining static routes to reach the remote branch network on the VPNCs



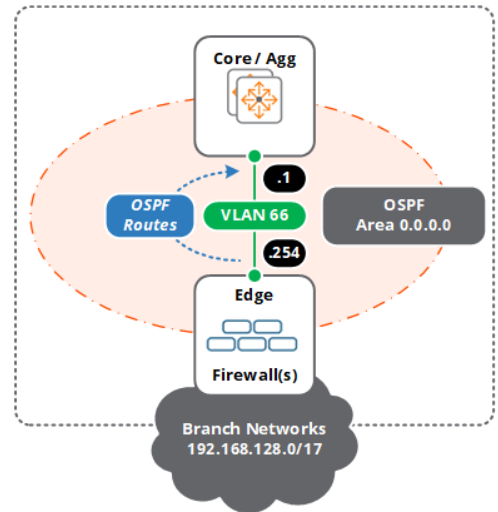
VPNC (Corporate Network Reachability)

- The VPNCs use OSPF routing to reach the corporate networks through the edge firewall
- The corporate network routes are either individual routes or summarized routes
- The VPNCs and edge firewall interfaces in VLAN 4001 are configured for the same OSPF area and type (example normal Area **0.0.0.0**)
- In this example the standalone/L2 redundant VPNCs learn a summarized **192.168.0.0/17** corporate network OSPF route from the edge firewall via **192.168.120.1**



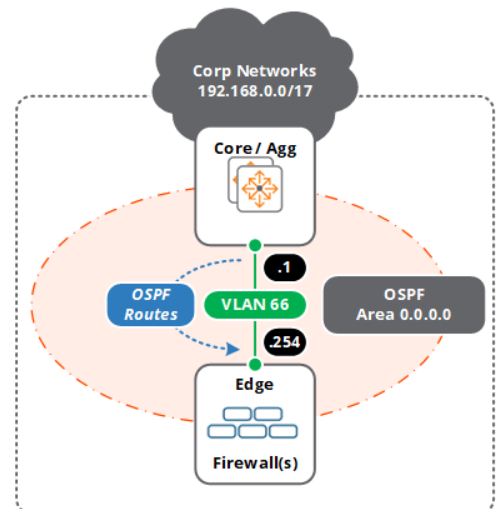
Core/Aggregation (Branch Network Reachability)

- The core/aggregation layer uses OSPF routing to reach the branch networks through the edge firewall.
- The branch network routes are either individual or summarized
- The edge firewall and core/aggregation switch interfaces in VLAN 66 are configured for the same OSPF area and type (example normal Area **0.0.0.0**)
- In this example the core/aggregation layer switches learn a summarized **192.168.128.0/17** branch network route from the edge firewall via **192.168.66.254**.
- The summarized branch route being installed as an OSPF type 2 route



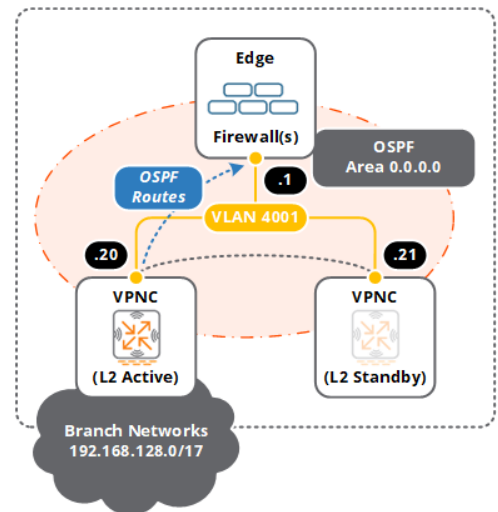
Edge Firewall (Corporate Network Reachability)

- The edge firewall uses OSPF routing to reach the corporate networks through the core/aggregation layer. The corporate network routes are either individual or summarized
- The edge firewall and core/aggregation switch interfaces in VLAN 66 are configured for the same OSPF area and type (example normal Area **0.0.0.0**)
- In this example the edge firewall learns the summarized **192.168.0.0/17** corporate route via **192.168.66.1**



Edge Firewall (Branch Network Reachability)

- The edge firewall uses OSPF routing to reach the branch networks through the standalone/L2 redundant VPNCs
- The branch network routes are either individual or summarized
- The edge firewall and standalone/L2 redundant VPNC interfaces in VLAN 4001 are configured for the same OSPF area and type (example normal Area **0.0.0.0**)
- In this example the edge firewall learns the summarized **192.168.0.0/17** branch route from the L2 active VPNC via **192.168.120.20**
- The summarized branch route being installed as an OSPF type 2 route



As a best practice, Aruba recommends configuring a loopback interface per VPNC that is used as the OSPF router ID. The core / aggregation layer switch operating as the designated router.

Dual Data Center

This reference topology can be deployed in a dual data center environment where a mirror of the standalone/L2 redundant VPNCs are deployed in a second data center. L2 redundancy (if enabled) is provided within each data center while L3 redundancy is provided between data centers.

When considering a dual data center design, it is important to note that only one data center will actively forward traffic during normal operation. The standalone/L2 redundant VPNCs in one data center are primary while the standalone/L2 redundant VPNCs in the second data center are secondary. This configuration is required as OSPF is utilized in each data center to determine the active branch traffic path during normal operation. The OSPF external type 2 routes via the primary standalone/L2 active VPNC are installed by the OSPF routers in the corporate network during normal operation.

This dual data center design requires the following:

1. The corporate network must implement a dynamic routing protocol such as OSPF. If another IGP is implemented, the OSPF routes must be redistributed into the IGP at the appropriate costs.
2. Overlay routing between the VPNCs and the core/aggregation layer must implement OSPF. The branch routes are advertised as external type 2 routes at specific costs by the standalone/L2 active VPNC into each data center. The route cost determines which data center is primary and which data center is secondary. The redistributed or summary route cost for the primary data center is lower than the redistributed or summary route cost in the secondary data center.

- Each BGW group requires the overlay static routes to reach the corporate network to be defined at different costs. The overlay static routes using the Internet VPN tunnels established to the primary standalone/L2 redundant VPNCs must be configured at a lower cost than the static routes using the Internet VPN tunnels established to the secondary standalone/L2 redundant VPNCs.

Figure 5-4 shows an example of a dual data center topology where a L2 redundant pair of VPNCs are deployed per data center. Each data center includes Internet WAN services, core/aggregation layers, and edge firewalls. The standalone/L2 active VPNCs learn the corporate network routes using OSPF while redistributing branch network routes into the respective data centers at different costs:

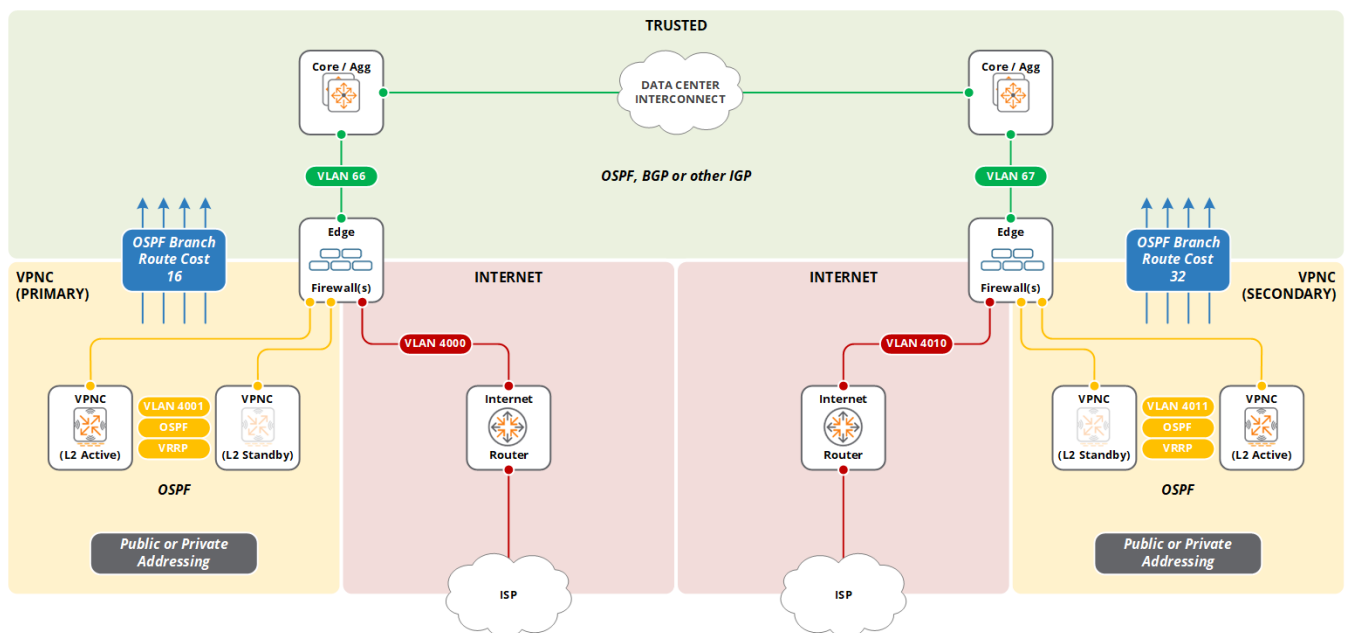


Figure 5-4 Dual Data Center Reference Topology

For this reference topology the standalone/L2 active VPNCs in each data center are connected to their respective edge firewall and core/aggregation switch using one VLAN interface:

- VLAN 4001/4011** – Connected to the VPNC zone in the respective data centers terminating the VPN tunnels from the Internet and transmitting and receiving overlay traffic. VPN tunnels are established to both standalone/L2 active VPNCs in each data center during normal operation. VLAN 4001 is used to transmit and receive overlay traffic during normal operation while VLAN 4011 is used during a L3 failover.

Figure 5-5 provides the flow paths for the VPN tunnels and overlay traffic:

1. **Internet VPN Tunnels (UDP 4500)** – All Internet VPN tunnels are terminated by the VLAN interface on the standalone/L2 active VPNC in each data center. This example uses VLANs 4001 and 4011.
2. **Overlay Corporate Traffic** – All overlay corporate traffic is transmitted and received by the overlay traffic VLAN interface on the primary standalone/L2 active VPNC. In this example VLAN 4001 redistributes the individual/summary the branch routes into the OSPF network at the lowest cost.
3. **Overlay Internet Traffic** – If full-tunnel mode is implemented, all overlay internet traffic is transmitted and received by the overlay traffic VLAN interface on the primary standalone/L2 active VPNC. In this example VLAN 4001 redistributes the individual/summary the branch routes into the OSPF network at the lowest cost.

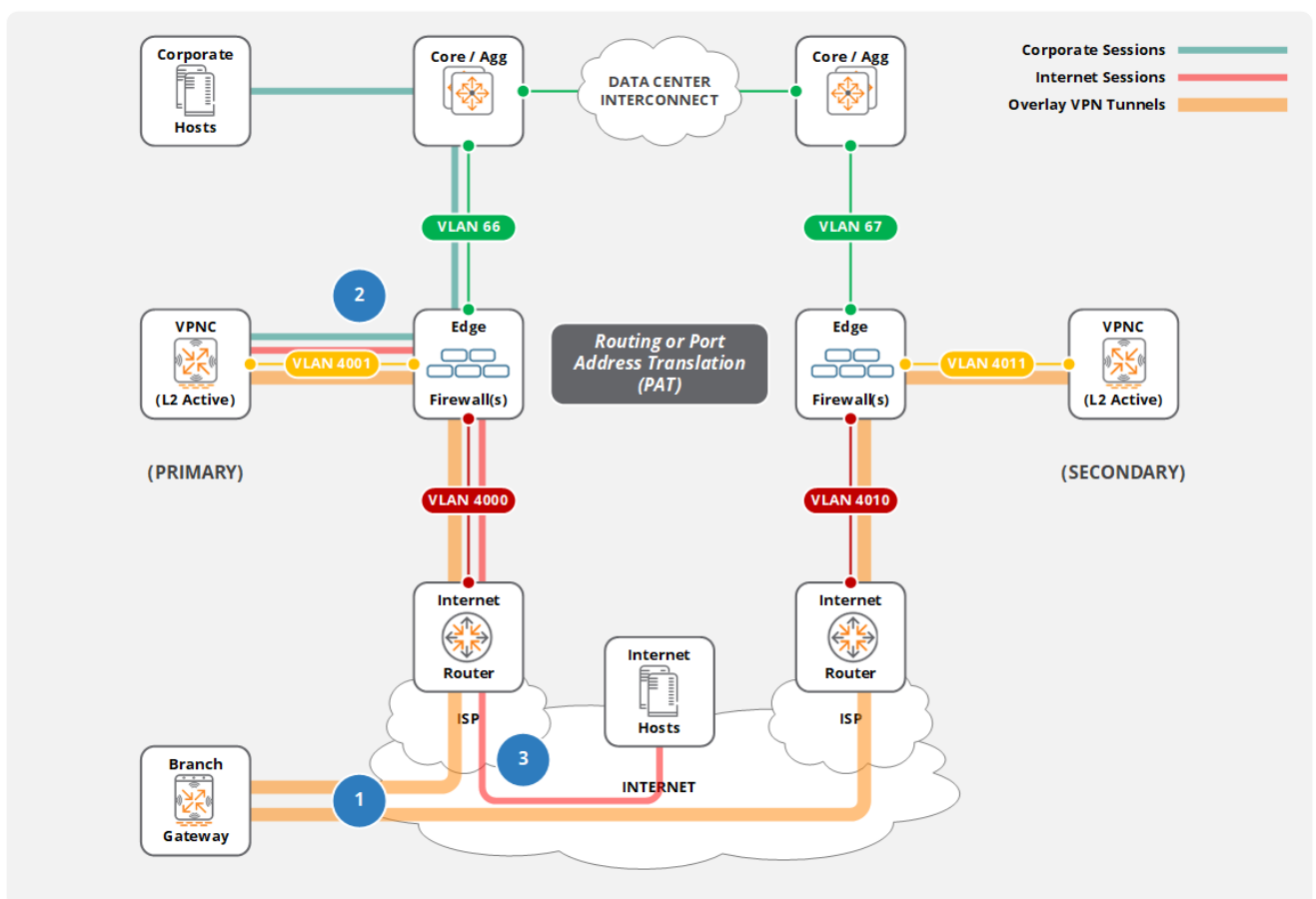


Figure 5-5 Flow Diagram

Overlay Routing

This section provides the overlay route implementation details required to support a dual data center design. As with a single data center deployment, the core/aggregation layers and edge firewalls in each data center need to be capable of reaching the branch networks from VPNCs. Likewise, the edge firewalls and VPNCs need to know how to reach the corporate networks from

the core/aggregation layers. This is achieved using dynamic routing where OSPF is required between the VPNCs and the edge firewall.

In a dual data center design, the standalone/L2 redundant VPNCs in one data center are designated primary while the standalone/L2 redundant VPNCs in the second data center are designated secondary. The primary standalone/L2 redundant VPNCs forward and receive overlay traffic during normal operation. This is achieved by configuring different cost overlay static overlay routes in each BGW group along with different OSPF redistribution route costs on the VPNCs:

1. The static overlay routes configured on the BGWs to reach the corporate networks through the VPN tunnels terminate on the primary standalone/L2 redundant VPNCs use a low cost (e.g., 1)
2. The static overlay routes configured on the BGWs to reach the corporate networks through the VPN tunnels terminate on the secondary standalone/L2 redundant VPNCs use a higher cost (e.g., 10)
3. The primary standalone/L2 redundant VPNCs are configured to redistribute the individual or summary branch routes into the OSPF network at a low cost (e.g., 16)
4. The secondary standalone/L2 redundant VPNCs are configured to redistribute the individual or summary branch routes to the OSPF network at a higher cost (e.g., 32)

During normal operation the BGWs will forward all overlay traffic through the VPN tunnels terminating on the primary standalone/L2 active VPNC. Since the OSPF redistributed route cost from the primary standalone/L2 active VPNC is lower than the OSPF redistributed route cost on the secondary standalone/L2 active VPNC all return overlay traffic is forwarded to the primary standalone/L2 active VPNC.

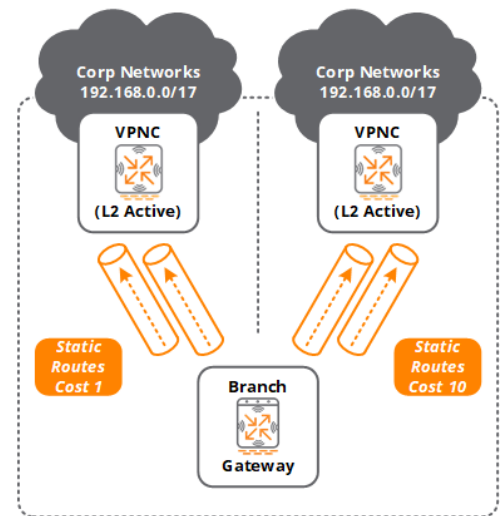
If an L2 failover occurs, the primary L2 standby VPNC will transition to an active role and terminate the VPN tunnels. The new L2 active VPNC will redistribute the branch networks to the OSPF network and will become the new path for the overlay traffic. Each branch network will be redistributed to OSPF at the same cost.

An L3 failover will occur if both VPN tunnels on a BGW established to the primary standalone/L2 redundant VPNC go down. The impacted BGWs will update their routing table to install the higher cost static routes pointing to the VPN tunnels established to secondary standalone/L2 active VPNC. All overlay traffic from the BGW destined to the corporate network will be forwarded using new routes. The OSPF routers in the corporate network will reconverge and install the higher cost routes for the impacted BGWs. The return path for the overlay traffic using the secondary standalone/L2 active VPNC.

Since an L3 failover may occur for a subset of BGWs, Aruba does not recommend configuring the VPNCs to send summarized routes. This allows the OSPF routers to install more specific routes to reach the BGWs during an L3 failover. Aruba does recommend to enabling summarization in the BGWs so that each BGW sends a summarized route for its branch networks using Aruba IKEv2 extensions.

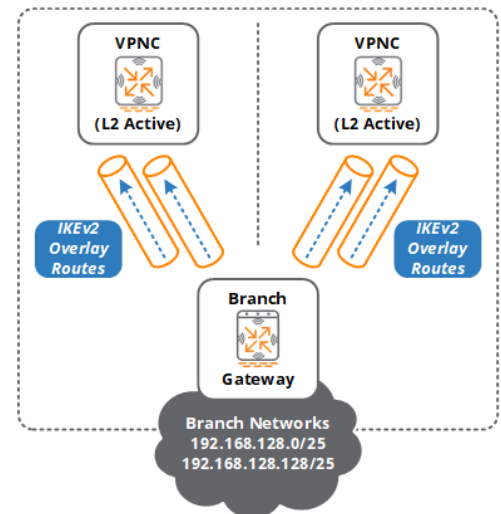
BGW (Corporate Network Reachability)

- Each BGW group is configured with static routes to reach the corporate networks using the MPLS and Internet VPN tunnels established to the primary and secondary standalone/L2 redundant VPNCs
- In this example the static route costs to reach the corporate network **192.168.0.0/27** through the primary standalone/L2 redundant VPNCs for each VPN tunnel are defined as **1**
- The static route costs to reach the corporate network **192.168.0.0/27** through the secondary standalone/L2 redundant VPNCs for each VPN tunnel are defined as **10**



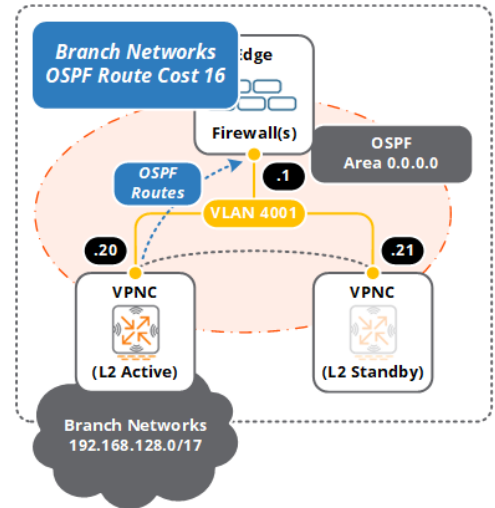
VPNC (Branch Network Reachability)

Per Aruba best practices, each branch gateway is configured to advertise their local branch networks to each standalone/L2 active VPNC through the VPN tunnels using Aruba IKEv2 extensions. This eliminates the need for defining static routes to reach the remote branch network on the VPNCs.



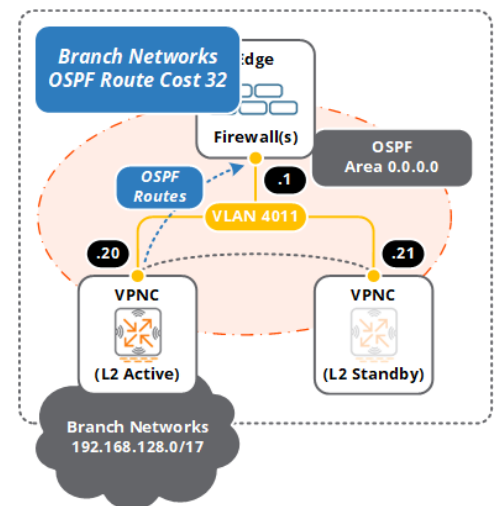
Edge Firewall (Branch Network Reachability) – Primary Data Center

- The edge firewall uses OSPF routing on the overlay traffic VLAN to reach the branch networks through the primary or secondary standalone/L2 active VPNC
- The VPNCs and edge firewall interfaces in VLAN 4001 are configured for the same OSPF area and type (e.g., normal Area **0.0.0.0**)
- In this example the edge firewall receives individual branch routes from the primary standalone/L2 active VPNC via **192.168.120.20** at a cost of **16**
- Each redistributed branch route is installed as an OSPF type 2 route by the OSPF routers in the network



Edge Firewall (Branch Network Reachability) – Secondary Data Center

- The edge firewall uses OSPF routing on the overlay traffic VLAN to reach the branch networks through the primary or secondary standalone/L2 active VPNC
- The VPNCs and edge firewall interfaces in VLAN 4011 are configured for the same OSPF area and type (e.g., normal Area **0.0.0.0**)
- In this example the core/aggregation layer switches discover individual branch routes from the secondary standalone/L2 active VPNC via **192.168.121.20** at a cost of **32**
- Branch routes redistributed by the secondary standalone/L2 active VPNC are not installed by the OSPF routers during normal operation since a lower cost route via the primary standalone/L2 redundant VPNC (cost 16) is installed



Internet Only with Multiple Network Zones

The following topology differs from the previous topology where the standalone VPNC or L2 redundant pair of VPNCs implement separate VLAN interfaces. The first VLAN interface connects the VPNCs to the edge firewall for Internet VPN tunnel termination while a second VLAN interface connects to a core/aggregation layer to forward branch traffic.

The primary difference in this reference design is that the branch traffic is transmitted and received using dedicated VLAN interface. All routing between the corporate and branch networks is also provided by this VLAN interface. The VLAN interface can either be directly connected to the core/aggregation layer or be indirectly connected through a user firewall. For simplicity no user firewall is shown.

This topology is typically followed for Aruba SD-Branch deployments using Internet based WAN services where the data center connects to one or two ISPs. For simplification this section focuses on a single ISP design. Each BGW initiates a VPN tunnel to the standalone/L2 active VPNC to establish the overlay network:

1. **Internet VPN Tunnels (UDP 4500)** – All Internet VPN tunnels are terminated by the VLAN 4001 interface on the standalone/L2 active VPNC
2. **Branch Traffic** – All deencapsulated branch traffic is transmitted and received by the VLAN 66 interface on the standalone/L2 active VPNC
3. **Full-Tunnel Mode** – If implemented, all branch traffic destined to the Internet is transmitted and received by the VLAN 66 interface on the standalone/L2 active VPNC. The Internet traffic taking the same path as corporate users.

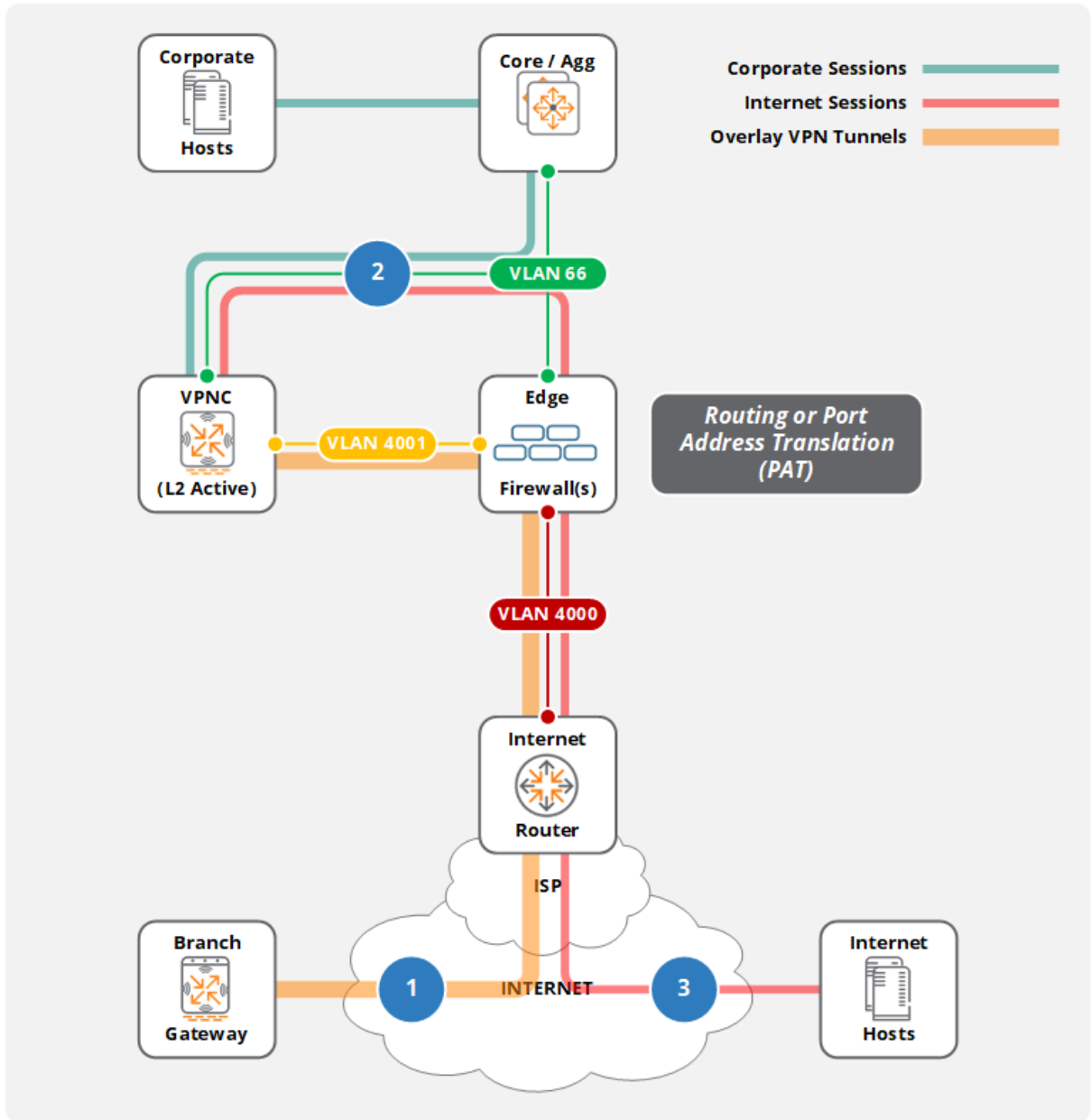


Figure 5-6 Flow Diagram

Figure 5-7 provides the logical topology which will be used in this section. To better explain the concepts, configurations and traffic flows for the network are separated into three zones that are interconnected using an edge firewall. This topology can support standalone VPNC or L2 redundant VPNCs that are connected to both the core/aggregation layers and edge firewall using two VLAN Interfaces:

- **VLAN 66** – Used to transmit/receive deencapsulated traffic from the branches
- **VLAN 4001** – Used to terminate VPN tunnels from the Internet

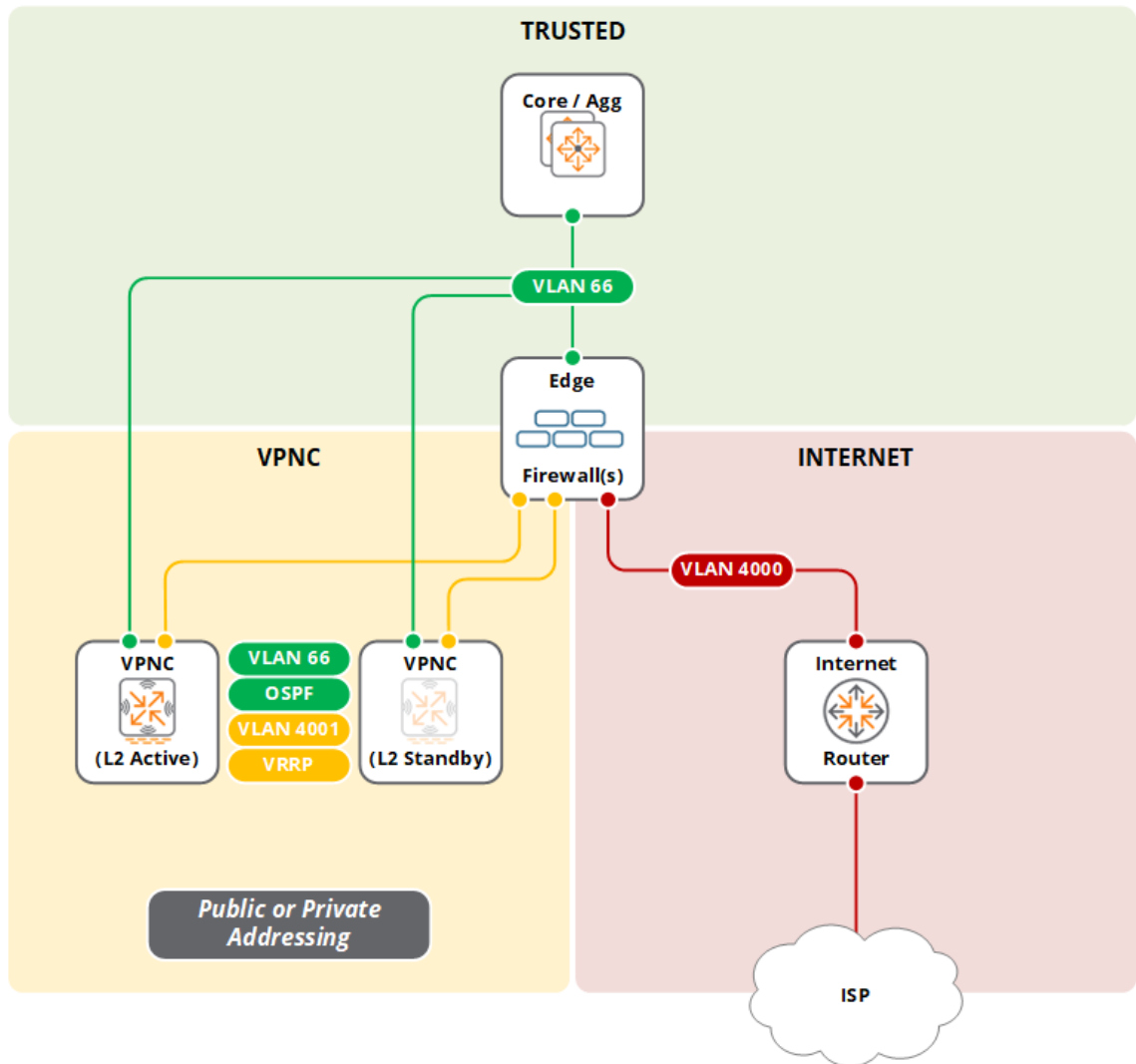


Figure 5-7 Reference Topology

For this reference topology administrators can optionally install a user firewall between the VPNC and trusted zones if required. The additional firewall(s) provide inspection of the branch traffic transmitted and received between the VPNC and trusted zones. The addition of the user firewall will require the appropriate static routing/OSPF configuration to be performed to provide reachability between the corporate and branch networks.

CIDR Allocation

To better understand the address allocation for each zone as well as the underlay/overlay routing later in this section, it is important to provide an overview of the CIDR addressing scheme that has been used for this reference architecture. To simplify routing, contiguous ranges of addresses are allocated to the corporate network and branches:

Corporate

The corporate network is allocated the **192.168.0.0/17** CIDR range. For this reference topology the following address space is used:

- **VLAN 66** – 192.168.66.0/24
- **VLAN 120** – 192.168.120.0/24

Branch

All branch networks are allocated addresses from the **192.168.128.0/17** CIDR range. This includes system IP addresses, management VLAN interfaces, and user VLAN interfaces.

Internet

The ISP has allocated the **23.216.134.0/24** CIDR range.

Virtual LANs

Several VLANs are required to ensure connectivity between devices in the different zones of this topology:

- **VPNCs to VPNC Zone** - One VLAN is required to connect the standalone/L2 redundant VPNCs to the edge firewall (VLAN 4001)
- **Edge Firewall/VPNCs to Trusted Zone** - One VLAN is used to connect the edge firewall and standalone/L2 redundant VPNCs to the core/aggregation layer in the trusted zone (VLAN 66)
- **Edge Firewall to Internet Zone** - One VLAN is used to connect the edge firewall to the Internet router (VLAN 4000)

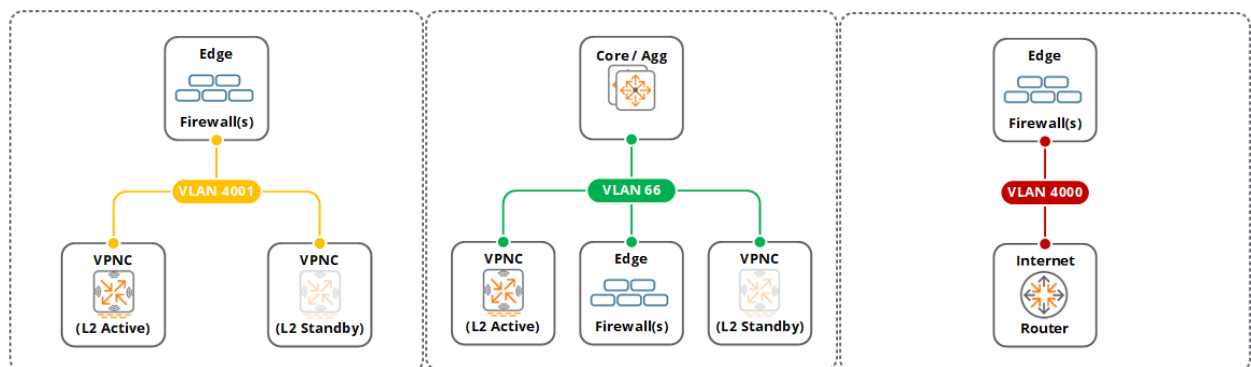


Figure 5-8 Internet Only with Multiple Network Zones VLANs



If the edge firewall implements routed ports instead of VLAN interfaces then the configuration needs to be adjusted accordingly. If the edge firewall implements routed ports and the deployment requires L2 redundant VPNCs then a layer 2 aggregation switch needs to be deployed to connect the VPNCs.

Ports

This reference topology can support connecting the standalone or L2 redundant VPNCs using either a single port or multiple ports. When a single port is implemented it is configured as a trunk with each VLAN receiving 802.1Q tags. The standalone or L2 redundant VPNCs are typically connected to a L2 aggregation switch. If multiple ports are implemented, each port is configured with a specific VLAN and connected to its respective peer device such as an edge firewall or the core/aggregation layer.

If additional bandwidth and fault-tolerance is required, the VPNCs supports standards based link aggregation allowing multiple ports to be assigned to a LAG group. A single LAG may be connected to a L2 aggregation switch or multiple LAGs connected to different peer devices as port-density allows.

As a best practice Aruba recommends the following:

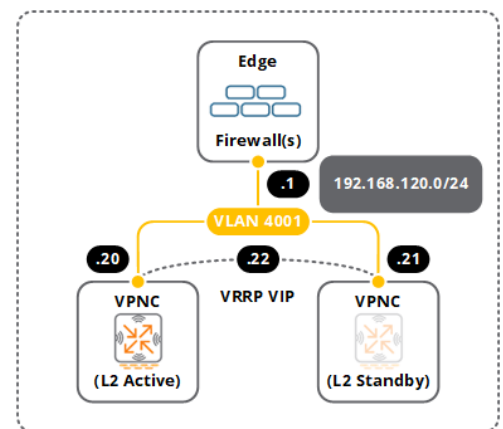
1. Configure each port or LAG as a trunk and implement 802.1Q tagging on each VLAN. Using trunk ports or LAGs on the VPNCs allows additional VLANs to be added in the future with no interruption to existing underlay or overlay traffic.
2. Configure the ports/LAGs and VLANs as trusted. The VPNC will not perform any L2 or L3 authentication for the overlay traffic.

VLAN Interfaces

This reference topology consists of IP interfaces in each zone which utilize public and private addressing:

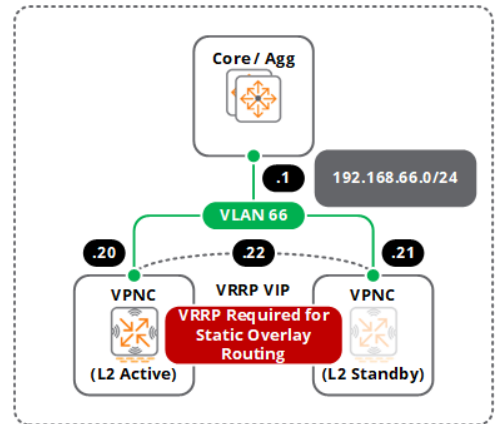
VPNC to Edge Firewall (VPNC Zone)

- Internet underlay VLAN interface
- Can be public or private addressing.
- Public address space is allocated by the ISP
- In this example the standalone/L2 redundant VPNCs are connected to the edge firewall in the VPNC zone using the **192.168.120.0/24** private network
- VPNC Address Requirements:
 - Standalone VPNC – 1 Address
 - L2 Redundant VPNCs – 3 x Addresses (2 host and 1 VRRP)



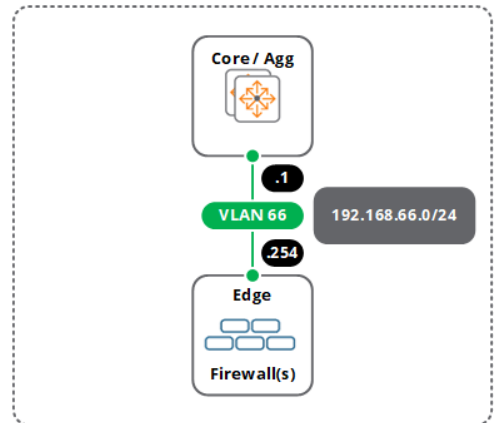
VPNC to Core/Aggregation Layer (Trusted Zone)

- Overlay traffic VLAN interface
- In this example the standalone/L2 redundant VPNCs are connected to the core/aggregation layer in trusted zone using the **192.168.66.0/24** network
- VPNC address requirements:
 - Standalone VPNC – 1 address
 - L2 Redundant VPNCs (Static Overlay) – 3 addresses (2 host and 1 VRRP)
 - L2 Redundant VPNCs (OSPF) – 2 addresses



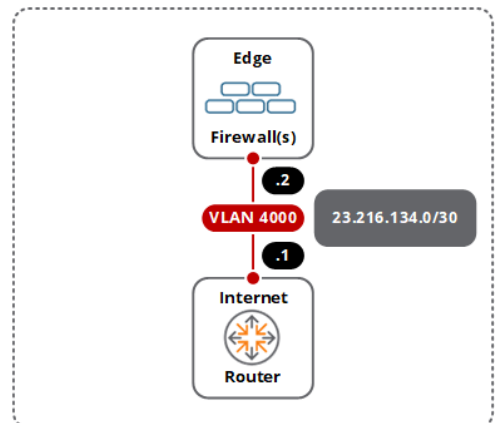
Edge Firewall to Core/Aggregation Layer (Trusted Zone)

- Core/Aggregation layer to edge firewall interconnect VLAN
- In this example the edge firewall are is connected to the core/aggregation layer in trusted zone using the **192.168.66.0/24** network
- Address requirements will be deployment specific



Edge Firewall to Internet Router (Internet Zone)

- Edge firewall to Internet router interconnect VLAN or routed interfaces
- Requires public addressing assigned by the ISP
- In this example edge firewall is connected to the Internet router in the Internet zone using the **23.216.134.0/30** network
- Address requirements will be deployment specific



L2 Redundancy

This reference topology can support a standalone VPNC or pair of L2 redundant VPNCs. When a L2 redundant pair of VPNCs is deployed VRRP is enabled on the VLAN interfaces that terminate the VPN tunnels. For this reference architecture this would include VLAN 4001. One VPNC in the pair is active and terminates the VPN tunnels and forwards the overlay traffic during normal operation. The second VPNC in the pair operates as a standby unit. The forwarding of traffic is performed by the active VPNCs host IP address and not the virtual IP address.

L2 redundancy leverages VRRP where the assigned VRRP priority determines the role of each VPNC. The VPNC assigned the highest priority assumes an active role while the VPNC assigned the lowest priority assumes a standby role. Each L2 redundant pair of VPNCs requires a host address along with virtual address that is shared between the VPNCs. The VRRP virtual IP interface is used to terminate the VPN tunnels as well as provide underlay and overlay routing during normal operation.

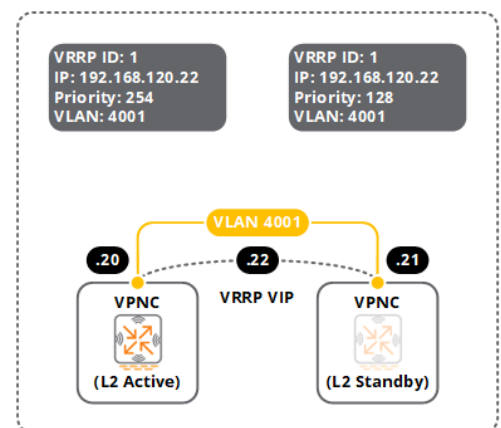
For this topology VRRP will be enabled on the VLAN interfaces for VLAN 4001 which terminate the VPN tunnels initiated over the Internet WAN services and carry overlay traffic:

Active VPNC (Internet underlay VLAN interface)

- VLAN Interface **400**
- A unique common VRRP ID within the broadcast domain (in this example **1**)
- Assigned the highest VRRP priority of **254**

Standby VPNC (Internet underlay VLAN interface)

- VLAN Interface **4001**
- A unique common VRRP ID within the broadcast domain (in this example **1**)
- Assigned the VRRP priority **128**



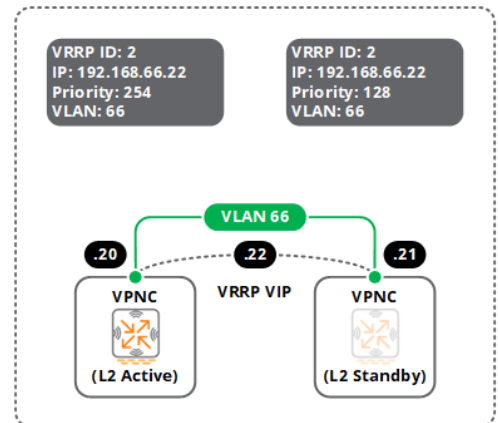
If a deployment includes L2 redundant VPNCs and overlay routing is using static routes, VRRP is also required on the overlay traffic VLAN interface. This is to provide the core/aggregation layer with a single next-hop IPv4 address for the overlay static routes. This greatly simplifies the static overlay routing configuration on the core/aggregation layer.

Active VPNC (Overlay VLAN Interface)

- VLAN Interface **66**
- A unique common VRRP ID within the broadcast domain (in this example **3**)
- Assigned the highest VRRP priority **254**

Standby VPNC (Overlay VLAN Interface)

- VLAN Interface **66**
- A unique common VRRP ID within the broadcast domain (in this example **3**)
- Is assigned the VRRP priority **128**



Routing

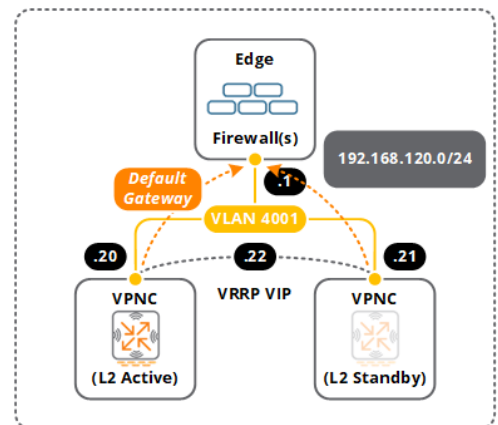
Underlay Routing

For this reference topology underlay routing is achieved on the standalone/L2 redundant VPNCs by defining default gateways and static routes. The default gateway configuration provides reachability to the Internet while static routes provide reachability to the MPLS network.

The routing configuration required for the edge firewall and Internet router will be dependent on the Internet architecture. Each device either implements dynamic routing such as BGP or implements default routes.

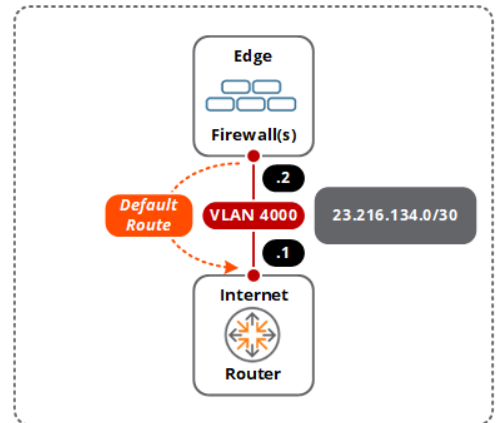
VPNC (Internet Reachability)

- Each VPNC requires a default gateway to be configured to provide reachability to the Internet
- The next-hop router address is the host address assigned to the edge firewall in the VPNC zone
- In this example each VPNC is configured to use **192.168.120.1** as their default gateway



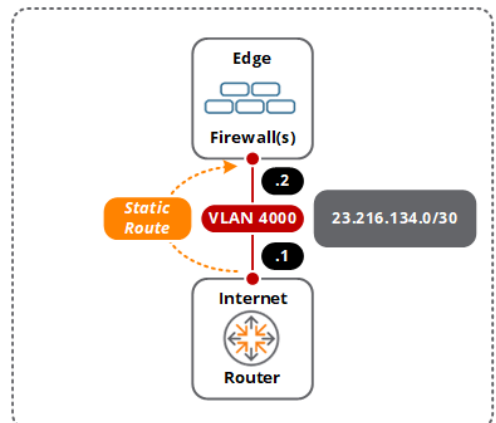
Edge Firewall (Internet Reachability)

- Requires a default route to provide reachability to the Internet
- Can either be dynamically learned via BGP or statically defined
- The next-hop router address is the address assigned to the Internet router in the Internet zone
- In this example the edge firewall has a static default route configured to **23.216.134.1**



Internet Router (VPNC Zone Reachability)

- If public addressing is implemented in the VPNC zone then the Internet router must know how to reach the public network behind the edge firewall
- Can either be dynamically learned via BGP or statically defined
- The next-hop router address is the address assigned to the edge firewall in the Internet zone
- As the standalone/L2 redundant VPNCs in this example do not implement public addressing, no routes are required on the Internet router



Overlay Routing

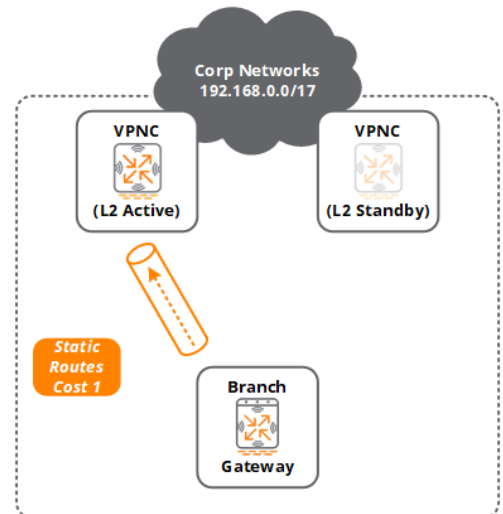
This reference topology can support static or dynamic routing to provide reachability between the corporate and branch networks through the overlay network. Static routing is typically implemented for smaller deployments where dynamic routing is not implemented in the core/aggregation layers. Dynamic routing using OSPF provides the most flexibility as individual branch routes or a summary of the branch routes are automatically advertised and redistributed to the edge firewall and core/aggregation layers.

Static Routing

SD-Branch deployments implementing static routing require configuration of static routes on the standalone/L2 redundant VPNCs, edge firewall, and core/aggregation layers to provide reachability between the corporate and branch networks.

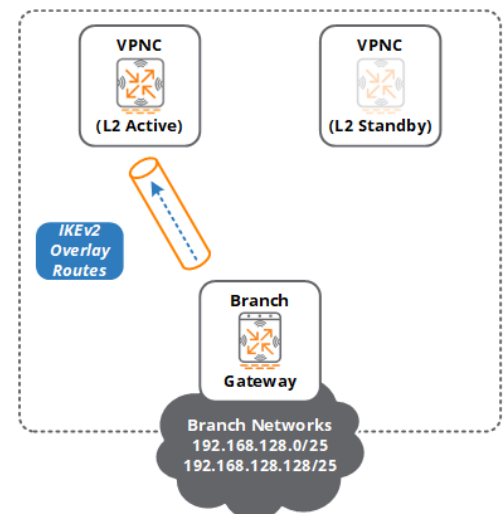
BGW (Corporate Network Reachability)

- Each BGW group is configured with static routes to reach the corporate networks using the Internet VPN tunnels established to the standalone/L2 redundant VPNCs
- In this example the static route cost to reach the corporate network **192.168.0.0/27** through the standalone/L2 redundant VPNCs for each VPN tunnel is defined as **1**



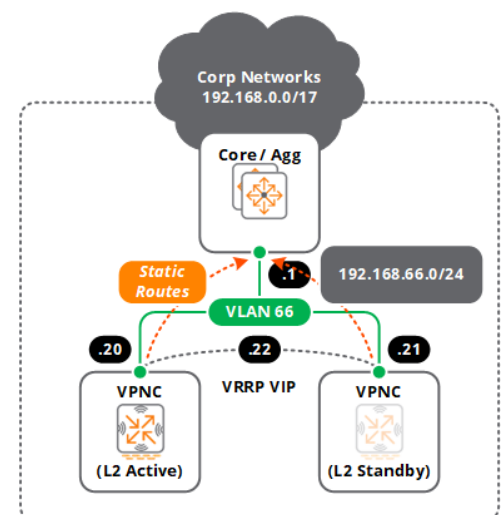
VPNC (Branch Network Reachability)

- Per Aruba best practices, each branch gateway is configured to advertise their local branch networks to the standalone/L2 active VPNC through the VPN tunnels using Aruba IKEv2 extensions
- This eliminates the need for defining static routes to reach the remote branch network on the VPNCs



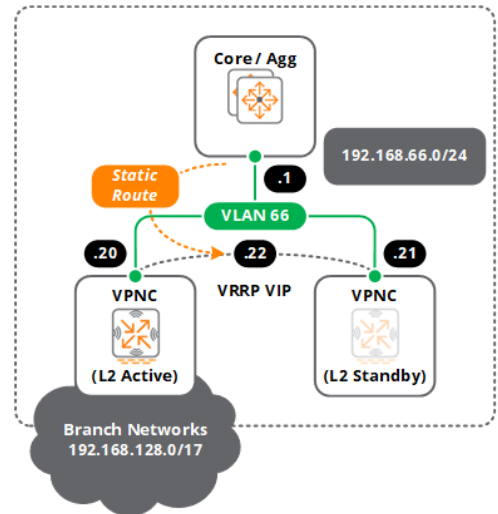
VPNC (Corporate Network Reachability)

- Requires static routes to reach the corporate networks through the core/aggregation layer
- In this example one static route is defined on the standalone/L2 redundant VPNCs to reach the **192.168.0.0/17** network through the core/distribution switch via **192.168.66.1**



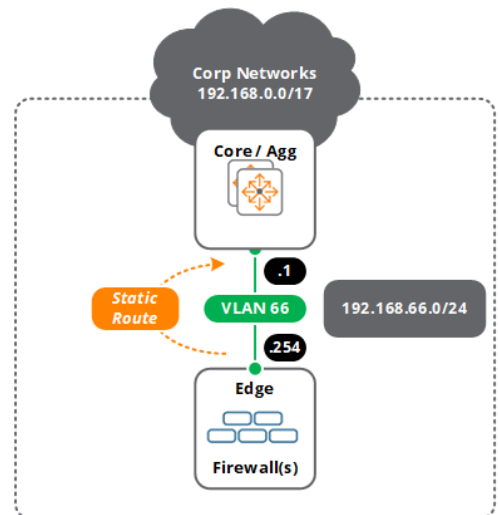
Core/Aggregation (Branch Network Reachability)

- Requires static routes to reach the branch networks through the standalone/L2 redundant VPNCs
- In this example one static route is defined on the core/aggregation layer to reach the **192.168.128.0/17** branch networks through the L2 redundant VPNCs via the VRRP virtual IP **192.168.66.22**



Edge Firewall (Corporate Network Reachability)

- Requires static routes to reach the corporate networks through the core/aggregation layer
- In this example one static route is defined on edge firewall to reach the **192.168.0.0/17** network through the core/aggregation layer via **192.168.66.1**



Dynamic Routing (OSPF)

Dynamic routing requires OSPF to be configured on the core/aggregation switches, edge firewall, and VPNCs. The OSPF configuration for each device and zone is specific to each organization. When OSPF is enabled and configured, the standalone or L2 active VPNC will automatically redistribute connected branch routes in the trusted network using the overlay traffic VLAN which will be learned by the edge firewall and core/aggregation layers.

Branch routes can be redistributed into the OSPF area in two ways:

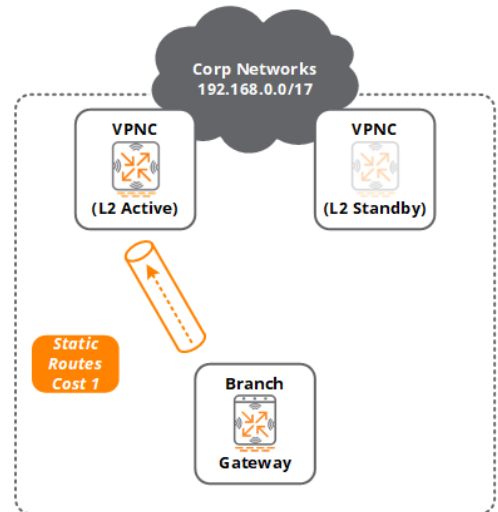
1. Individual branch routes can be redistributed to the OSPF area at a configured cost learned by the standalone/L2 active VPNC. Each route is installed by the OSPF routers as External Type 2 routes at the specified cost.

- One or more summary routes can be redistributed to the OSPF area at a configured cost by the standalone/L2 active VPNC. Each summary route is installed by the OSPF routers as External Type 2 routes at the specified cost.

For large SD-Branch deployments utilizing a single data center, Aruba recommends configuring summary routes as doing so will consume less CPU and memory resources on the OSPF routers in the network.

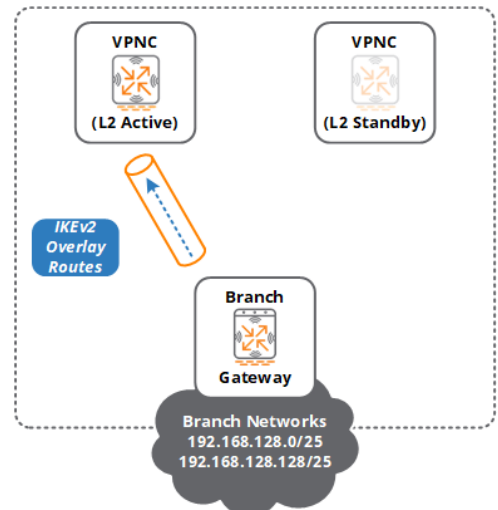
BGW (Corporate Network Reachability)

- Each BGW group is configured with static routes to reach the corporate networks using the MPLS and Internet VPN tunnels established to the standalone/L2 redundant VPNCs
- In this example the static route cost to reach the corporate network **192.168.0.0/27** through the standalone/L2 redundant VPNCs for each VPN tunnel is defined as **1**



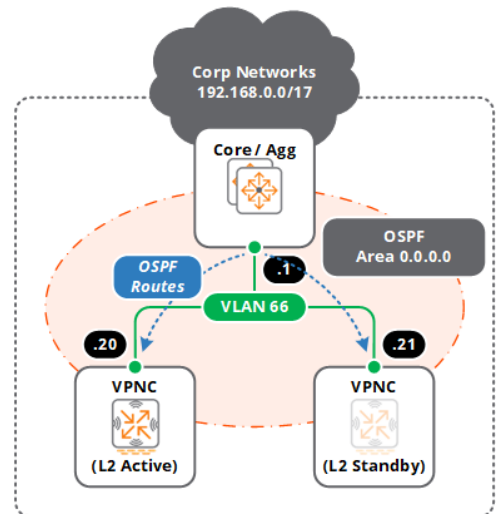
VPNC (Branch Network Reachability)

- Per Aruba best practices, each branch gateway is configured to advertise their local branch networks to the standalone/L2 active VPNC through the VPN tunnels using Aruba IKEv2 extensions
- This eliminates the need for defining static routes to reach the remote branch network on the VPNCs



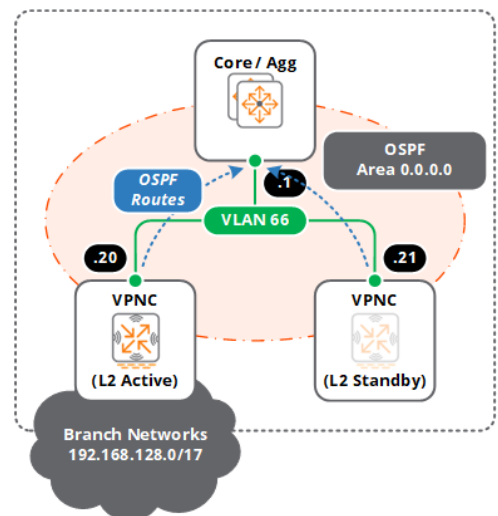
VPNC (Corporate Network Reachability)

- The VPNCs use OSPF routing on the overlay traffic VLAN to reach the corporate networks through the core/aggregation layer. The corporate network routes are either individual or summarized
- The VPNCs and core/aggregation layer switch interfaces in VLAN 66 are configured for the same OSPF area and type (e.g., normal Area **0.0.0.0**)
- In this example the standalone/L2 redundant VPNCs learn a summarized **192.168.0.0/17** corporate network OSPF route from the core/aggregation layer via **192.168.66.1**



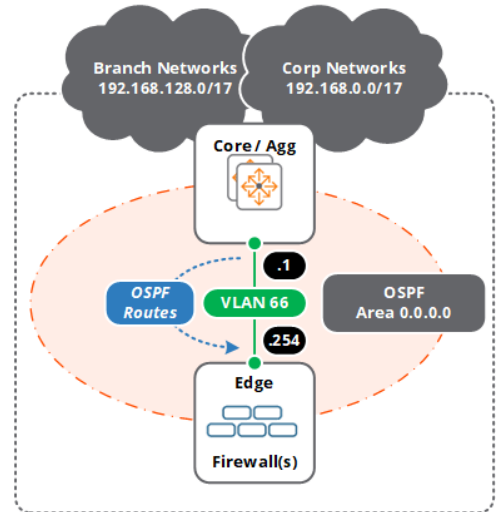
Core/Aggregation (Branch Network Reachability)

- The core/aggregation layer uses OSPF routing to reach the branch networks through the edge firewall. The branch network routes are either individual or summarized
- The VPNCs and core/aggregation layer switch interfaces in VLAN 66 are configured for the same OSPF area and type (example normal Area **0.0.0.0**)
- In this example the core/aggregation layer switches learn a summarized **192.168.128.0/17** branch network route from the L2 active VPNC via **192.168.66.20**.
- The summarized branch route is installed as an OSPF type 2 route



Edge Firewall (Corporate + Branch Network Reachability)

- The core/aggregation layer uses OSPF routing on the interconnect VLAN to reach the corporate and branch networks through the core/aggregation layer
- The corporate and branch network routes are either individual summarized
- The edge firewall and core/aggregation switch interfaces in VLAN 66 are configured for the same OSPF area and type (e.g., normal Area **0.0.0.0**)
- In this example the edge firewall learns the summarized **192.168.0.0/17** corporate route and **192.168.0.0/17** branch route via **192.168.66.1**. The summarized branch route is installed as an OSPF type 2 route.



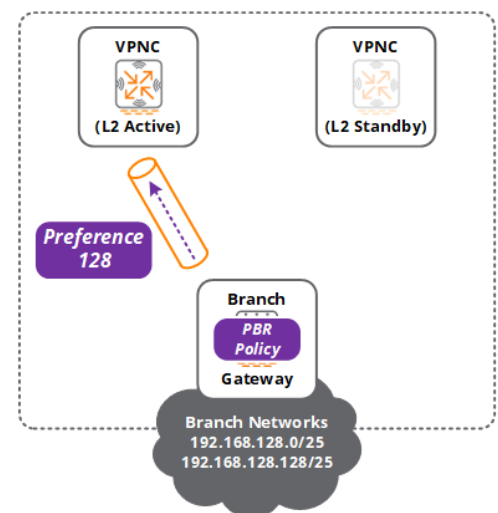
As a best practice, Aruba recommends configuring a loopback interface per VPNC that is used as the OSPF router ID. The core/aggregation layer switch operates as the designated router.

Policy Based Routing (PBR)

If full tunnel mode is required for one or more branch network, a PBR policy must be configured and applied to the VPN tunnels on the standalone/L2 redundant VPNCs. The PBR policy is required to forward branch overlay traffic destined to the Internet through the core/aggregation layer to ensure symmetrical routing.

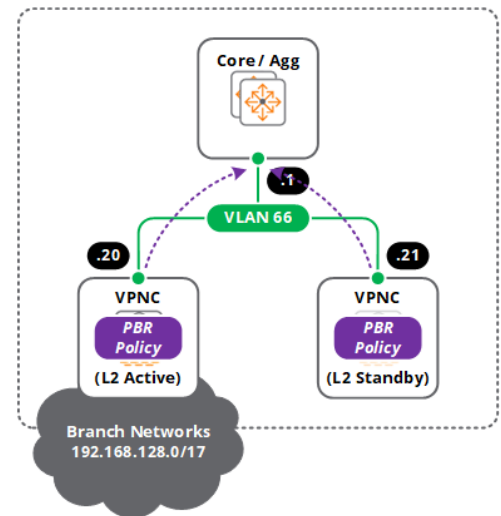
Branch Gateway

- Each BGW group is configured with a route ACL (RACL) and next-hop list that forwards branch traffic destined to the Internet via the Internet VPN tunnels established to the standalone/L2 redundant VPNCs
- In this example the RACL and next-hop list is configured to:
 - Forward branch traffic from **192.168.128.0/17** destined to the corporate network **192.168.0.0/17** normally
 - Forward branch traffic from **192.168.128.0/17** destined to **any** using a next-hop list
 - The next-hop list includes the VPN tunnel established to the standalone/L2 redundant VPNC using the default preference
- The RACL can be applied to user sessions in the BGP group using roles or AAA policy



Virtual Private Network Concentrator

- A route ACL (RACL) is configured on the standalone/L2 redundant VPNCs with the following rules:
 - Route traffic received from the branch networks destined to the corporate networks normally (e.g., example source **192.168.128.0/17** destined to **192.168.0.0/17**)
 - Forward traffic received from the branch networks destined to the Internet to the core/aggregation layer (e.g., source **192.168.128.0/17** destined to **any** via **192.168.66.1**)



PBR is required on the VPNC in this scenario to prevent symmetrical routing. By default the standalone/L2 redundant VPNCs will use the default gateway information and forward the branch traffic destined to the Internet directly to the edge firewall. As the edge firewall is only capable of reaching the branch networks through the core/aggregation layer, all return traffic will be forwarded to the core/aggregation layer which is different than the outgoing session path.



If full tunnel mode is required, the edge firewalls will also need to learn the branch route through the core/aggregation layer or directly from the standalone/L2 redundant VPNCs.

Dual Data Center

This reference topology can be deployed in a dual data center environment where a mirror of the standalone/L2 redundant VPNCs are deployed in a second data center. L2 redundancy (if enabled) is provided within each data center while L3 redundancy is provided between data centers.

When considering a dual data center design, it is important to note that only one data center will actively forward traffic during normal operation. The standalone/L2 redundant VPNCs in one data center are primary while the standalone/L2 redundant VPNCs in the second data center are secondary. This is required as OSPF is utilized in each data center to determine the active branch traffic path during normal operation. The OSPF external type 2 routes via the primary standalone/L2 active VPNC are installed by the OSPF routers in the corporate network during normal operation.

This dual data center design requires:

1. The corporate network must implement a dynamic routing protocol such as OSPF. If another IGP is implemented, the OSPF routes must be redistributed into the IGP at the appropriate costs.
2. Overlay routing between the VPNCs and the core/aggregation layer must implement OSPF. The branch routes need to be advertised as external type 2 routes at specific costs by the

standalone/L2 active VPNC into each data center. The route cost determines which data center is primary and which data center is secondary. The redistributed or summary route cost for the primary data center is lower than the redistributed or summary route cost in the secondary data center.

- Each BGW group requires the overlay static routes to reach the corporate network to be defined at different costs. The overlay static routes use the Internet VPN tunnels established to the primary standalone/L2 redundant VPNCs configured at a lower cost than the static routes using the Internet VPN tunnels established to the secondary standalone/L2 redundant VPNCs.

Figure 5-9 shows an example dual data center topology where a L2 redundant pair of VPNCs are deployed per data center. Each data center includes Internet WAN services, core/aggregation layers, and edge firewalls. The standalone/L2 active VPNCs learn the corporate network routes using OSPF while redistributing branch network routes into the respective data centers are different costs:

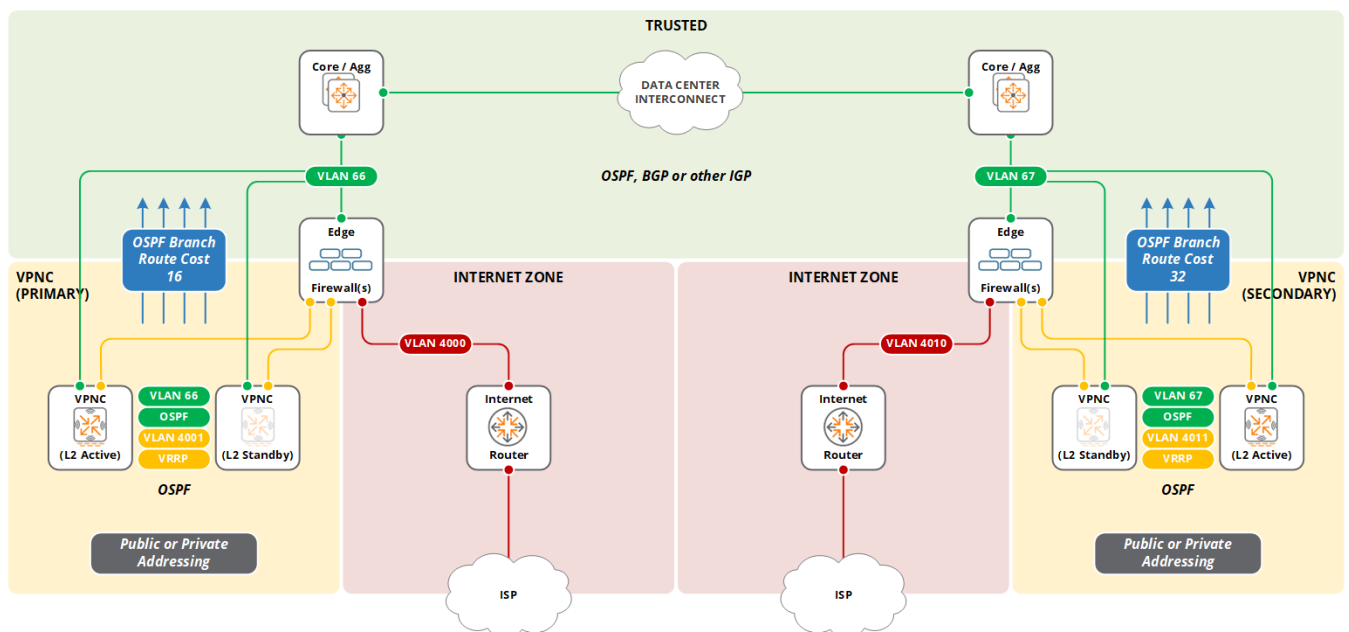


Figure 5-9 Dual Data Center Reference Topology

For this reference topology the standalone/L2 active VPNCs in each data center are connected to their respective edge firewall and core/aggregation switch using two VLAN interfaces:

- VLAN 66/67** – Connects to the trusted zone in each respective data center transmitting and receiving overlay traffic. VLAN 66 is used during normal operation while VLAN 67 is used during a L3 failover.
- VLAN 4001/4011** – Connects to the VPNC zone in the respective data centers terminating the VPN tunnels from the Internet. VPN tunnels are established to both standalone/L2 active VPNCs in each data center during normal operation.

Figure 5-10 demonstrates the flow paths for the VPN tunnels and overlay traffic:

1. **Internet VPN Tunnels (UDP 4500)** – All Internet VPN tunnels are terminated by the VLAN interface on the standalone/L2 active VPNC in each data center. In this example VLAN 4001 and 4011.
2. **Overlay Corporate Traffic** – All overlay corporate traffic is transmitted and received by the overlay traffic VLAN interface on the primary standalone/L2 active VPNC. In this example VLAN 66 redistributes the branch routes to the OSPF network at the lowest cost.
3. **Overlay Internet Traffic** – If full-tunnel mode is implemented, all overlay internet traffic is transmitted and received by the overlay traffic VLAN interface on the primary standalone/L2 active VPNC. In this example VLAN 66 redistributes the branch routes to the OSPF network at the lowest cost.

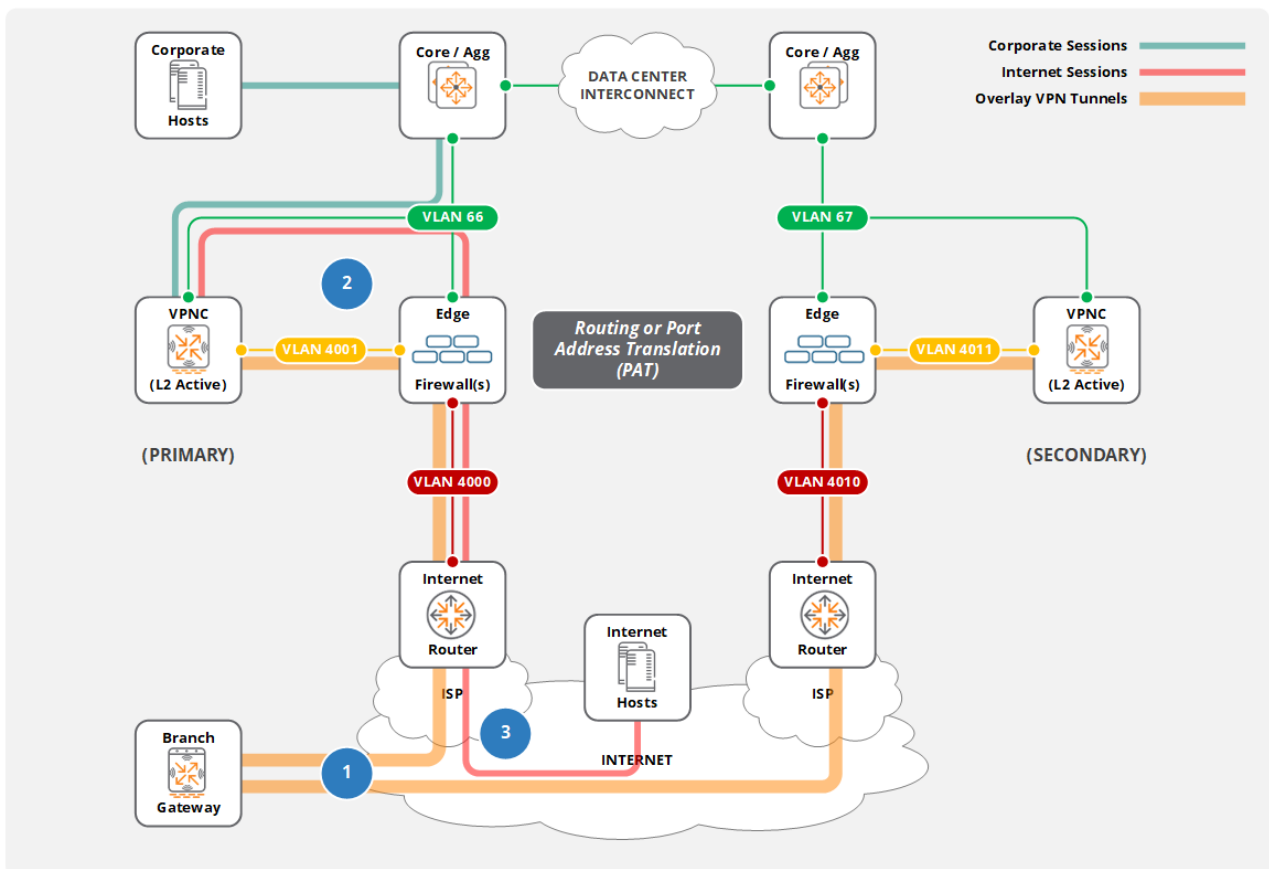


Figure 5-10 Dual Data Center Flow Diagram

Overlay Routing

This section provides the overlay route implementation details required to support a dual data center design. As with a single data center deployment, the core/aggregation layers and edge firewalls in each data center need to learn how to reach the branch networks from VPNCs. Likewise, the edge firewalls and VPNCs need to know how to reach the corporate networks from the core/aggregation layers. This is achieved using dynamic routing where OSPF is required between the VPNCs and the edge firewall.

In a dual data center design, the standalone/L2 redundant VPNCs in one data center are designated primary while the standalone/L2 redundant VPNCs in the second data center are designated secondary. The primary standalone/L2 redundant VPNCs forward and receive overlay traffic during normal operation. This is achieved by configuring different cost overlay static overlay routes in each BGW group along with different OSPF redistribution route costs on the VPNCs:

1. The static overlay routes configured on the BGWs to reach the corporate networks through the VPN tunnels terminated on the primary standalone/L2 redundant VPNCs using a low cost (e.g. 1)
2. The static overlay routes are configured on the BGWs to reach the corporate networks through the VPN tunnels terminated on the secondary standalone/L2 redundant VPNCs using a higher cost (e.g. 10)
3. The primary standalone/L2 redundant VPNCs are configured to redistribute the individual or summary branch routes into the OSPF network at a low cost (e.g. 16)
4. The secondary standalone/L2 redundant VPNCs are configured to redistribute the individual or summary branch routes into the OSPF network at a higher cost (e.g. 32)

During normal operation the BGWs will forward all overlay traffic through the VPN tunnels terminating on the primary standalone/L2 active VPNC. Since the OSPF redistributed route cost from the primary standalone/L2 active VPNC is lower than the OSPF redistributed route cost on the secondary standalone/L2 active VPNC, all return overlay traffic is forwarded to the primary standalone/L2 active VPNC.

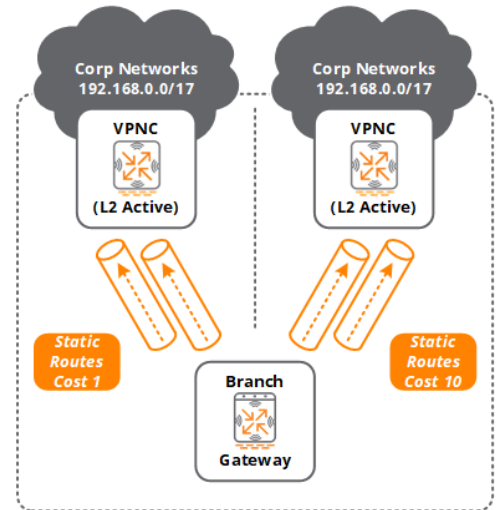
If an L2 failover occurs, the primary L2 standby VPNC will transition to an active role and terminate the VPN tunnels. The new L2 active VPNC will redistribute the branch networks into the OSPF network and will become the new path for the overlay traffic. Each branch network will be redistributed to OSPF at the same cost.

An L3 failover will occur if both VPN tunnels on a BGW established to the primary standalone/L2 redundant VPNC go down. The impacted BGWs will update their routing table to install the higher cost static routes pointing to the VPN tunnels established to secondary standalone/L2 active VPNC. All overlay traffic from the BGW destined to the corporate network will be forwarded using new routes. The OSPF routers in the corporate network will re-converge and install the higher cost routes for the impacted BGWs. The return path for the overlay traffic will use the secondary standalone/L2 active VPNC.

As an L3 failover may occur for a subset of BGWs, it is not recommended to configure the VPNCs to send summarized routes. This allows the OSPF routers to install more specific routes to reach the BGWs during a L3 failover. Aruba does recommend enabling summarization on the BGWs so that each BGW sends a summarized route for its branch networks using Aruba IKEv2 extensions.

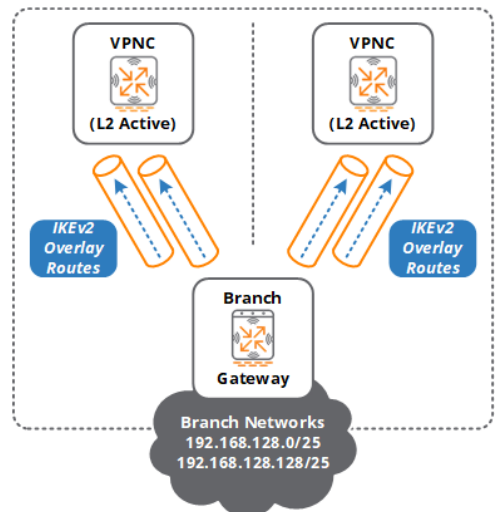
BGW (Corporate Network Reachability)

- Each BGW group is configured with static routes to reach the corporate networks using the MPLS and Internet VPN tunnels established to the primary and secondary standalone/L2 redundant VPNCs
- In this example the static route costs to reach the corporate network **192.168.0.0/27** through the primary standalone/L2 redundant VPNCs for each VPN tunnel are defined as **1**
- The static route costs to reach the corporate network **192.168.0.0/27** through the secondary standalone/L2 redundant VPNCs for each VPN tunnel are defined as **10**



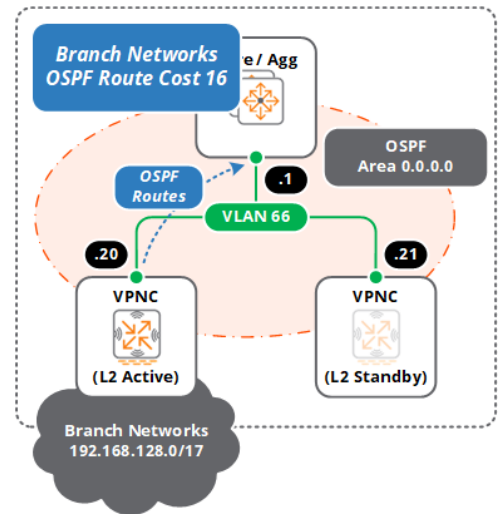
VPNC (Branch Network Reachability)

- Per Aruba best practices, each branch gateway is configured to advertise their local branch networks to each standalone/L2 active VPNC through the VPN tunnels using Aruba IKEv2 extensions
- This eliminates the need for defining static routes to reach the remote branch network on the VPNCs



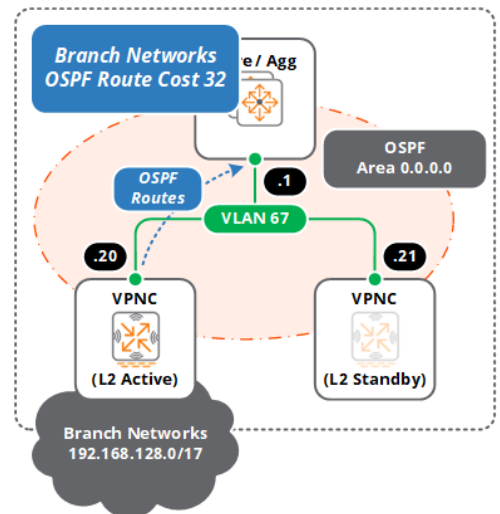
Core/Aggregation (Branch Network Reachability) – Primary Data Center

- The core/aggregation layer uses OSPF routing on the overlay traffic VLAN to reach the branch networks through the primary or secondary standalone/L2 active VPNC
- The VPNCs and core/aggregation switch interfaces in VLAN 66 are configured for the same OSPF area and type (e.g., normal Area **0.0.0.0**)
- In this example the core/aggregation switches learn individual branch routes from the primary standalone/L2 active VPNC via **192.168.66.20** at a cost of **16**
- Each redistributed branch route is installed as an OSPF type 2 route by the OSPF routers in the network



Core/Aggregation (Branch Network Reachability) – Secondary Data Center

- The core/aggregation layer uses OSPF routing on the overlay traffic VLAN to reach the branch networks through the primary or secondary standalone/L2 active VPNC (individual branch routes are preferred)
- The VPNCs and core/aggregation switch interfaces in VLAN 67 are configured for the same OSPF area and type (e.g., normal Area **0.0.0.0**)
- In this example the core/aggregation layer switches learn individual branch routes from the secondary standalone/L2 active VPNC via **192.168.121.20** at a cost of **32**
- Branch routes redistributed by the secondary standalone/L2 active VPNC are not installed by the OSPF routers during normal operation as a lower cost route via the primary standalone/L2 redundant VPNC (cost 16) is installed



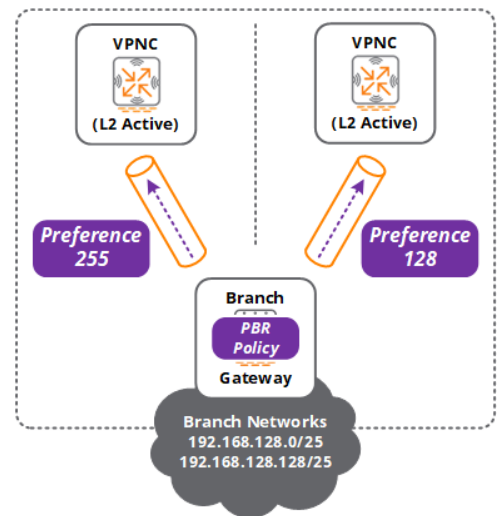
Policy Based Routing (PBR)

If full tunnel mode is required for one or more branch network, a PBR policy must be configured and applied to the VPN tunnels on the standalone/L2 redundant VPNCs. The PBR policy is required to forward branch overlay traffic destined to the Internet through the core/aggregation layer to ensure symmetrical routing.

As dual data centers are deployed, the next-hop list configured in the BGW group includes both the primary and secondary VPN tunnels. The next-hop configuration for the VPN tunnel established to the primary standalone/L2 redundant VPNCs is configured with a higher priority than the VPN tunnel established to the secondary standalone/L2 redundant VPNCs.

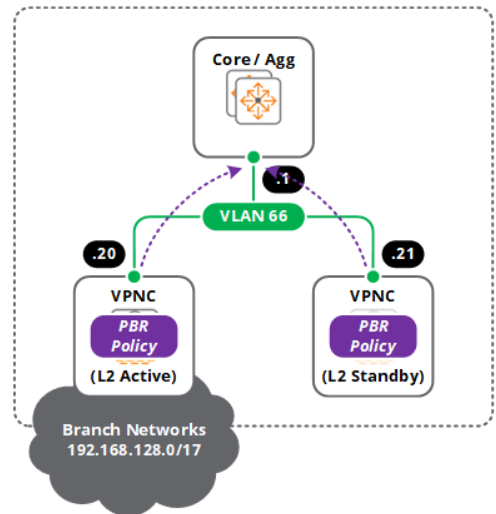
Branch Gateway

- Each BGW group is configured with an RACL and next-hop list that forwards branch traffic destined to the Internet via the Internet VPN tunnels established to the standalone/L2 redundant VPNCs
- In this example the RACL and next-hop list is configured to:
 - Forward branch traffic from **192.168.128.0/17** destined to the corporate network **192.168.0.0/17** normally
 - Forward branch traffic from **192.168.128.0/17** destined to **any** using a next-hop list
 - The next-hop list includes the VPN tunnels established to the primary and secondary standalone/L2 redundant VPNCs using different preferences:
 - The preference for VPN tunnels established to the primary standalone/L2 redundant VPNC is **255**
 - The preference for the VPN tunnels established to the secondary standalone/L2 redundant VPNC is **128**
- The RACL can be applied to user sessions in the BGP group using roles or AAA policy



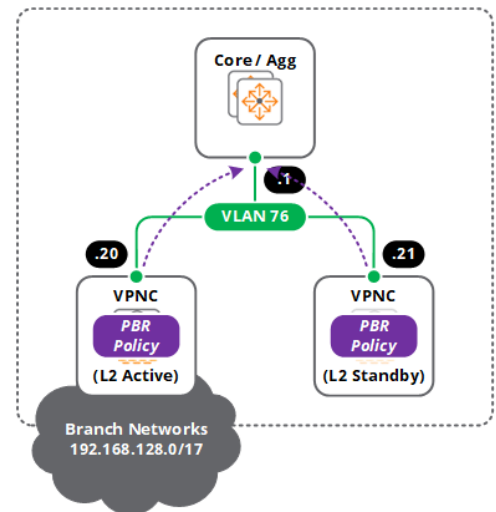
VPNC – Primary Data Center

- An ACL is configured on the standalone/L2 redundant VPNCs with the following rules:
 - Route traffic received from the branch networks destined to the corporate networks normally (e.g., source **192.168.128.0/17** destined to **192.168.0.0/17**)
 - Forward traffic received from the branch networks destined to the Internet to the core/aggregation layer (e.g., source **192.168.128.0/17** destined to **any** via **192.168.66.1**)



VPNC – Secondary Data Center

- An ACL is configured on the standalone/L2 redundant VPNCs with the following rules:
 - Route traffic received from the branch networks destined to the corporate networks normally (e.g., source **192.168.128.0/17** destined to **192.168.0.0/17**)
 - Forward traffic received from the branch networks destined to the Internet to the core/aggregation layer (e.g., source **192.168.128.0/17** destined to **any** via **192.168.76.1**)



PBR is required on the VPNC in this scenario to prevent symmetrical routing. By default the standalone/L2 redundant VPNCs will use the default gateway information and forward the branch traffic destined to the Internet directly to the edge firewall. As the edge firewall is only capable of reaching the branch networks through the core/aggregation layer, all return traffic will be forwarded to the core/aggregation layer which is different than the outgoing session path.



If full tunnel mode is required, the edge firewalls in each data center will also need to learn the branch route either through the core/aggregation layer or directly from the standalone/L2 redundant VPNCs.

Internet and MPLS with Multiple Network Zones

The following topology differs from the previous topology where the standalone VPNC or L2 redundant pair of VPNCs include an additional VLAN interface to support a MPLS network. For this design the first VLAN interface connects the VPNCs to the edge firewall for Internet VPN tunnel termination, the second VLAN connects the VPNCs to a core/aggregation layer for MPLS VPN tunnel termination, and the third VLAN interface connects to a core/aggregation layer to forward branch traffic.

The primary goal of this reference design is to separate the underlay and overlay traffic. The VPNCs implement dedicated VLAN interfaces to terminate the VPN tunnels from the separate Internet and MPLS WAN services while branch traffic is transmitted and received out a dedicated VLAN interface.

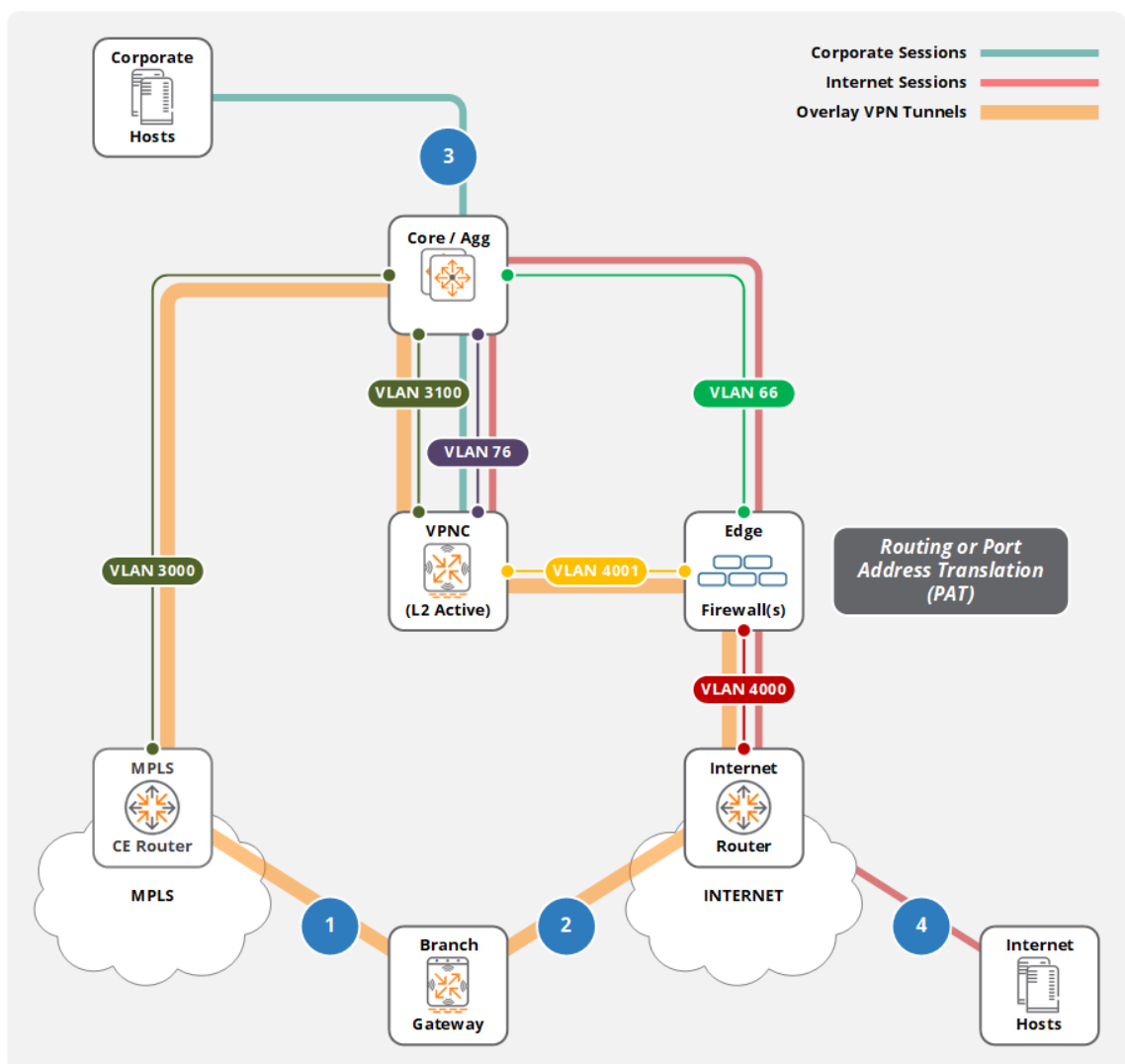


Figure 5-11 Internet and MPLS with Multiple Network Zones Flow Diagram

This topology is typically followed for Aruba SD-Branch deployments using Internet based WAN services where the data center connects to one or two ISPs. For simplification this section focuses on a single ISP design. Each BGW initiates a VPN tunnel to the standalone/L2 active VPNC to establish the overlay network:

1. **MPLS VPN Tunnels (UDP 4500)** – All MPLS VPN tunnels are terminated by the VLAN 3100 interface on the standalone/L2 active VPNC
2. **Internet VPN Tunnels (UDP 4500)** – All VPN tunnels from the Internet are terminated by the VLAN 4001 interface on the standalone/L2 active VPNC
3. **Branch Traffic** – All deencapsulated branch traffic is transmitted and received by the VLAN 76 interface on the standalone/L2 active VPNC
4. **Full-Tunnel Mode** – If implemented, all branch traffic destined to the Internet is transmitted and received by the VLAN 76 interface on the standalone/L2 active VPNC (the Internet traffic takes the same path as corporate users)

As with the previous design, the dedicated VLAN interface used for branch traffic is also used to provide IP routing between the corporate and branch networks. The branch user traffic can also be sent by a VLAN interface either directly connected to the core/aggregation layer or be indirectly connected through a user firewall. For simplification no user firewall is shown.

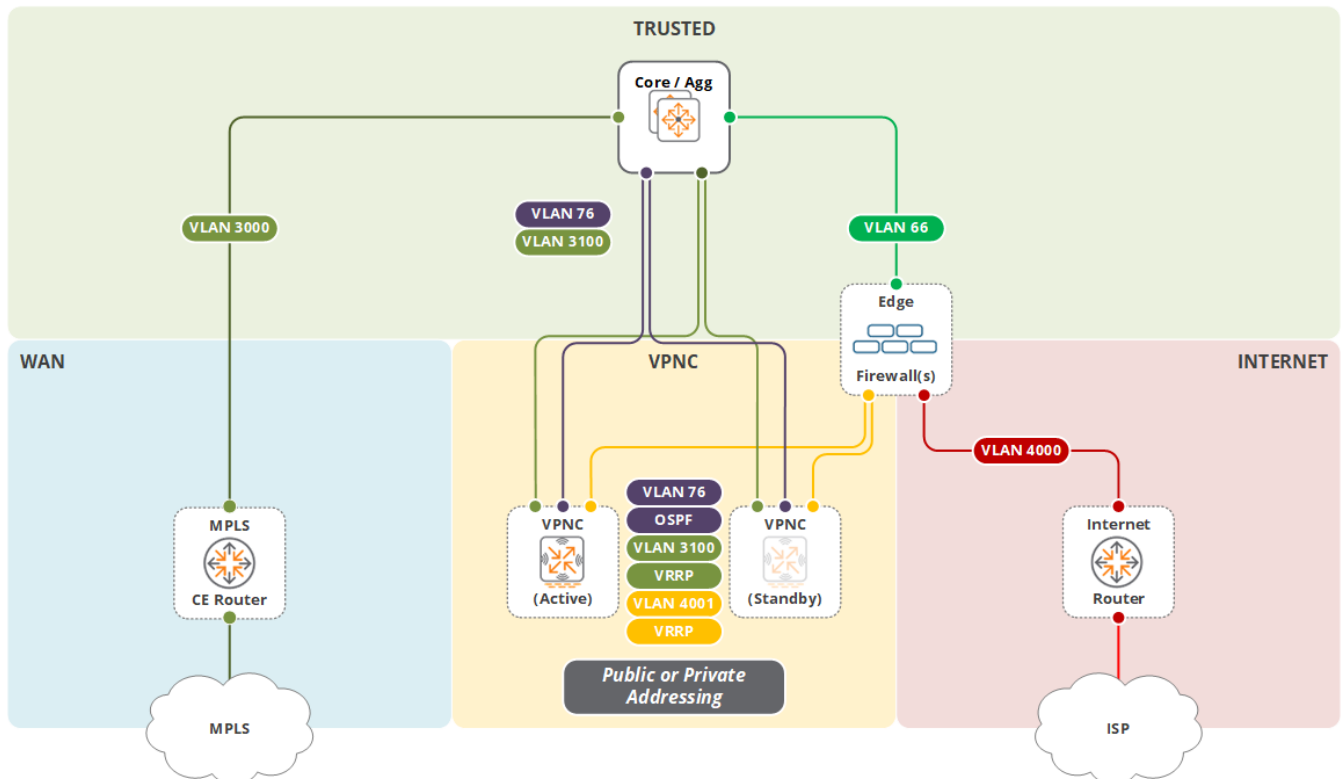


Figure 5-12 Internet and MPLS with Multiple Network Zones Single DC Reference Topology

Figure 5-12 provides the logical topology which will be used in this section. To better explain the concepts, configurations, and traffic flows the network is separated into three zones that are interconnected using an edge firewall. This topology can support standalone VPNC or L2 redundant VPNCs that are connected to both the core/aggregation layers and edge firewall using three VLAN Interfaces:

- **VLAN 76** – Used for deencapsulated traffic from the branches
- **VLAN 3100** – Used to terminate VPN tunnels from the MPLS network
- **VLAN 4001** – Used to terminate VPN tunnels from the Internet



For this reference topology a user firewall may optionally be installed between the VPNC and trusted zones if required. The additional firewall(s) providing inspection of the branch traffic transmitted and received between the VPNC and trusted zones. The addition of the user firewall will require the appropriate static routing/OSPF configuration to be performed to provide reachability between the corporate and branch networks.

CIDR Allocation

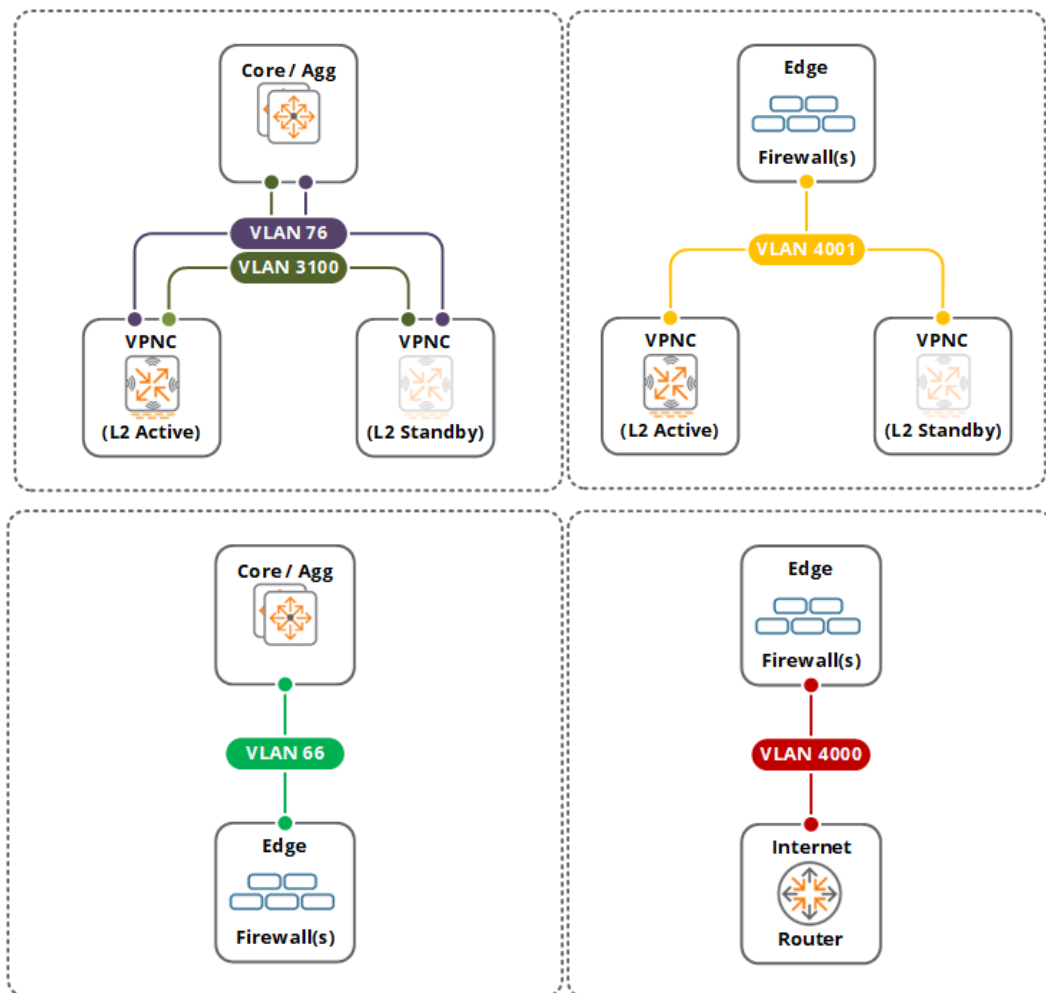
To better understand the address allocation for each zone as well as the underlay/overlay routing later in this section, it is important to provide an overview of the CIDR addressing scheme that has been used for this reference architecture. To simplify routing, contiguous ranges of addresses are allocated to the corporate network and branches:

- **Corporate** - The corporate network is allocated the **192.168.0.0/17** CIDR range. For this reference topology the following address space is used from this network block:
 - **VLAN 66** – 192.168.66.0/24
 - **VLAN 76** – 192.168.76.0/24
 - **VLAN 120** – 192.168.120.0/24
- **Branch** - All branch networks are allocated from the 192.168.128.0/17 CIDR range. This includes system IP addresses, management VLAN interfaces and user VLAN interfaces.
- **MPLS** - The MPLS WAN is allocated the 10.0.0.0/8 network by the MPLS service provider.
- **Internet** - The Internet Service Provider (ISP) has allocated the 23.216.134.0/24 CIDR range.

Virtual LANs

This reference topology requires three VLANs to connect the standalone/L2 redundant VPNCs to the VPNC and trusted zone. The VPNC zone requires one VLAN while the trusted zone requires two VLANs:

- **VPNCs to Trusted Zone** - Two VLANs are required to connect the standalone/L2 redundant VPNCs to the core/aggregation layer, in this example VLANs **76** and **3100**
- **VPNCs to VPNC Zone** - One VLAN is required to connect the standalone/L2 redundant VPNCs to the edge firewall, in this example VLAN **4001**
- **Edge Firewall to Trusted Zone** - One VLAN is used to connect the edge firewall to the core/aggregation layer in the trusted zone, in this example VLAN **66**
- **Edge Firewall to Internet Zone** - One VLAN is used to connect the edge firewall to the Internet router, in this example VLAN **4000**



If the edge firewall implements routed ports instead of VLAN interfaces, then adjust the configuration accordingly. If the edge firewall implements routed ports and the deployment requires L2 redundant VPNCs, a layer 2 aggregation switch needs to be deployed to connect the VPNCs.

Ports

This reference topology can support connecting the standalone or L2 redundant VPNCs using a single port or multiple ports. When a single port is implemented it is configured as a trunk that applies 802.1Q tags for each VLAN. The standalone or L2 redundant VPNCs are typically connected to a L2 aggregation switch. If multiple ports are implemented, each port is configured with a specific VLAN and connected to its respective peer device such as an edge firewall or the core/aggregation layer.

If additional bandwidth and fault tolerance is required, the VPNCs support standards based link aggregation allowing multiple ports to be assigned to a LAG group. A single LAG may be implemented to connect to an L2 aggregation switch or multiple LAGs connected to different peer devices as port-density allows.

As a best practice Aruba recommends the following:

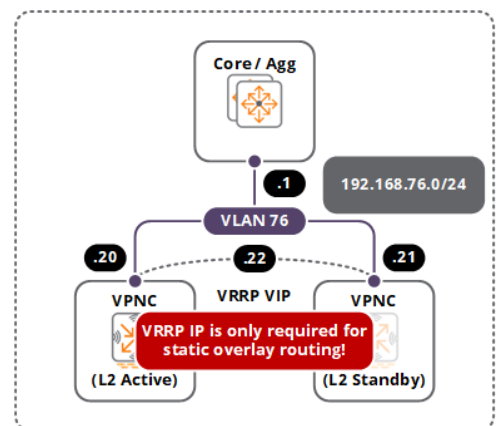
1. Configuring each port or LAG as a trunk and 802.1Q tagging each VLAN. Using trunk ports or LAGs on the VPNCs allows additional VLANs to be added in the future with no interruption to existing underlay or overlay traffic.
2. Configuring the ports/LAGs and VLANs as trusted. The VPNC will not be performing any L2 or L3 authentication for the overlay traffic.

VLAN Interfaces

This reference topology consists of IP interfaces in each zone that utilize public and private addressing:

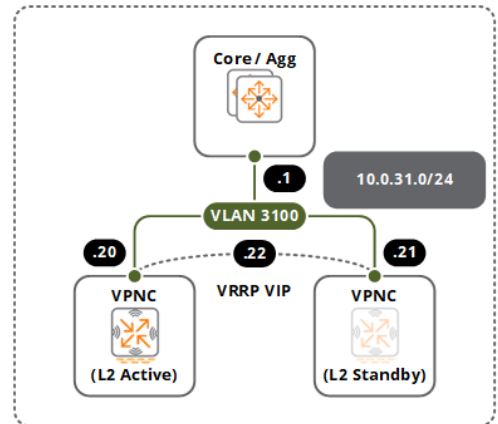
VPNC to Core/Aggregation Layer (Trusted Zone)

- Overlay traffic VLAN interface
- In this example the standalone or L2 redundant VPNCs is connected to the core/aggregation layer in trusted zone using the **192.168.76.0/24** network
- VPNC Address Requirements:
 - Standalone VPNC – 1 address
 - L2 Redundant VPNCs (Static Routing) – 3 addresses (2 host and 1 VRRP)
 - L2 Redundant VPNCs (OSPF) – 2 addresses



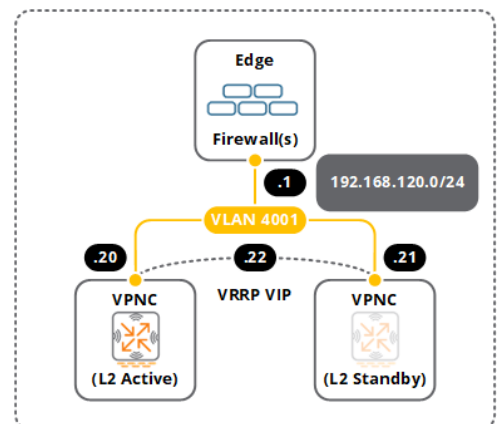
VPNC to Core/Aggregation Layer (Trusted Zone)

- MPLS underlay VLAN interface
- In this example the standalone or L2 redundant VPNCs are connected to the core/aggregation layer in trusted zone using the **10.0.0.31.0/24** network
- VPNC Address Requirements:
 - Standalone VPNC – 1 address
 - L2 Redundant VPNCs – 3 addresses (2 host and 1 VRRP)



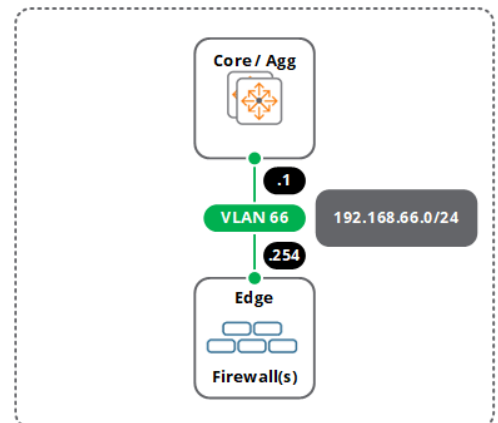
VPNC to Edge Firewall (VPNC Zone)

- Internet underlay VLAN interface
- Can be public or private addressing
- Public address space is allocated by the ISP
- In this example the standalone/L2 redundant VPNCs are connected to the edge firewall in the VPNC zone using the **192.168.120.0/24** private network
- VPNC Address Requirements:
 - **Standalone VPNC** – 1 address
 - **L2 Redundant VPNCs** – 3 addresses (2 host and 1 VRRP)



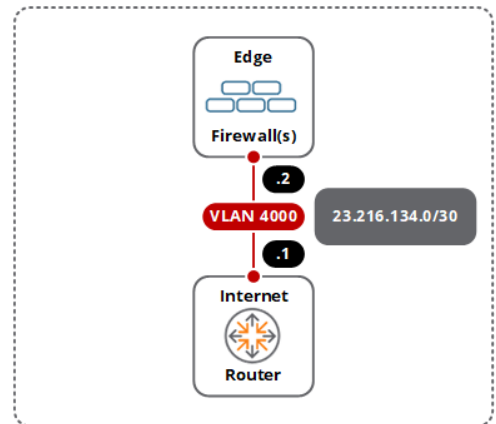
Edge Firewall to Core/Aggregation Layer (Trusted Zone)

- Core/aggregation layer to edge firewall interconnect VLAN
- In this example the edge firewall is connected to the core/aggregation layer in trusted zone using the **192.168.66.0/24** network
- Address requirements will be deployment specific



Edge Firewall to Internet Router (Internet Zone)

- Edge firewall to Internet router interconnect VLAN or routed interfaces
- Requires public addressing assigned by the ISP
- In this example edge firewall is connected to the Internet router in the Internet zone using the **23.216.134.0/30** network
- Address requirements will be dependent on your specific deployment



L2 Redundancy

This reference topology can support a standalone VPNC or pair of L2 redundant VPNCs. When an L2 redundant pair of VPNCs is deployed, VRRP is enabled on the VLAN interfaces that terminate the VPN tunnels. For this reference architecture this would include VLANs 3100 and 4001. One VPNC in the pair is active and terminates the VPN tunnels as well as forwards the overlay traffic during normal operation. The second VPNC in the pair operates as a standby unit. Traffic forwarding is performed by the active VPNC's host IP address and not the virtual IP address.

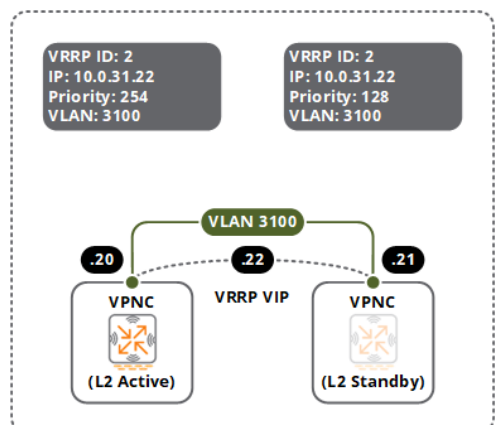
L2 redundancy leverages VRRP where the assigned VRRP priority determines the role of each VPNC. The VPNC assigned the highest priority assumes an active role while the VPNC assigned the lowest priority assumes a standby role. Each L2 redundant pair of VPNCs requires a host address along with virtual address that is shared between the VPNCs. The VRRP virtual IP interface is used to terminate the VPN tunnels as well as provide underlay and overlay routing during normal operation. VRRP is enabled on the VLAN interfaces for VLANs 3100 and 4001 that terminate the VPN tunnels initiated over the MPLS and Internet WAN services:

Active VPNC (MPLS underlay VLAN interface)

- VLAN Interface **3100**
- A unique common VRRP ID within the broadcast domain (in this example **1**)
- Assigned the highest VRRP priority **254**

Standby VPNC (MPLS underlay VLAN interface)

- VLAN Interface **3100**
- A unique common VRRP ID within the broadcast domain (in this example **1**)
- Assigned the VRRP priority **128**

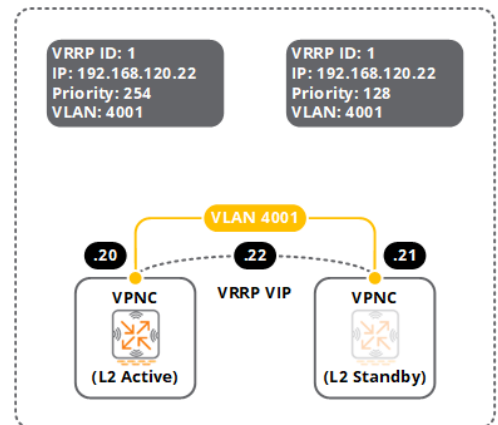


Active VPNC (Internet Underlay VLAN Interface)

- VLAN Interface **4001**
- A unique common VRRP ID within the broadcast domain (in this example **1**)
- Assigned the highest VRRP priority **254**

Standby VPNC (Internet Underlay VLAN Interface)

- VLAN Interface **4001**
- A unique common VRRP ID within the broadcast domain (in this example **1**)
- Assigned the VRRP priority **128**



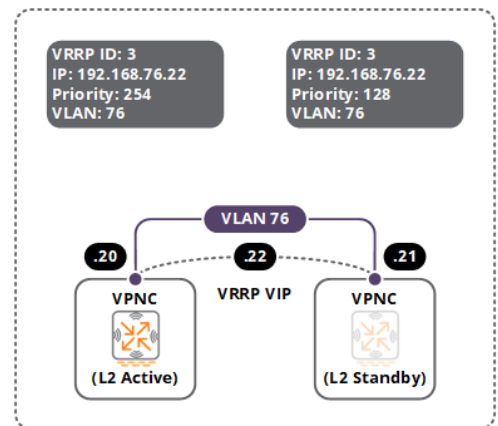
If the deployment includes L2 redundant VPNCs and overlay routing is using static routes then VRRP is also required on the overlay traffic VLAN interface. This is to provide the core/aggregation layer with a single next-hop IPv4 address for the overlay static routes. This greatly simplifies the static overlay routing configuration on the core/aggregation layer.

Active VPNC (Overlay VLAN Interface)

- VLAN Interface **76**
- A unique common VRRP ID within the broadcast domain (in this example **3**)
- Assigned the highest VRRP priority **254**

Standby VPNC (Overlay VLAN Interface)

- VLAN Interface **76**
- A unique common VRRP ID within the broadcast domain (in this example **3**)
- Assigned the VRRP priority **128**



Routing

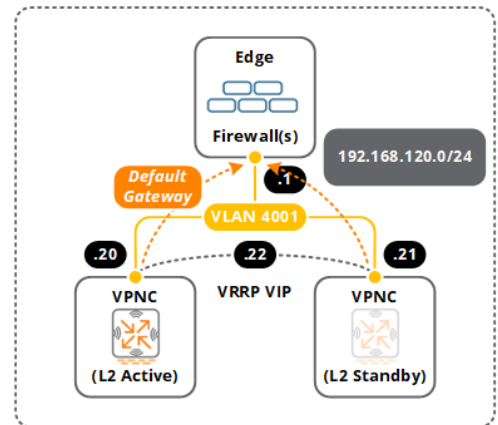
Underlay Routing

For this reference topology underlay routing is achieved on the standalone/L2 redundant VPNCs by defining default gateways and static routes. The default gateway configuration provides reachability to the Internet while static routes providing reachability to the MPLS network.

The routing configuration required for the edge firewall and Internet router will be dependent on the Internet architecture. Each device either implements dynamic routing such as BGP or implements default routes.

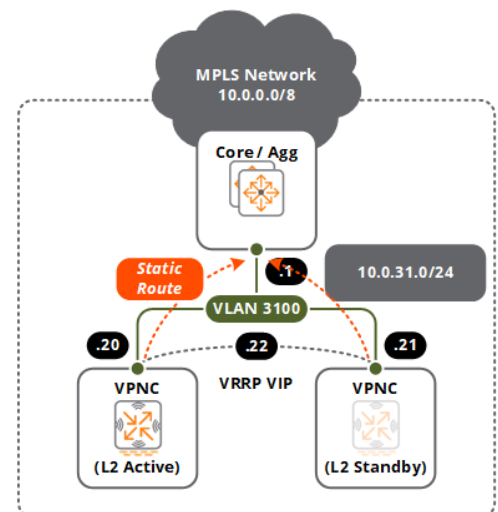
VPNC (Internet Reachability)

- Each VPNC requires a default gateway to be configured to provide reachability to the Internet.
- The next-hop router address is the host address assigned to the edge firewall in the VPNC zone
- In this example each VPNC is configured to use **192.168.120.1** as the default gateway



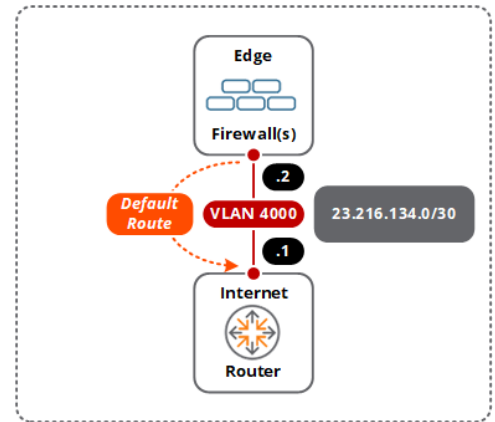
VPNC (MPLS Reachability)

- Each VPNC requires static routes to reach the MPLS network
- The next-hop router address is the host address assigned to the core/aggregation layer
- In this example each VPNC is configured with a single static route to reach the **10.0.0.0/8** network via **10.0.31.1**



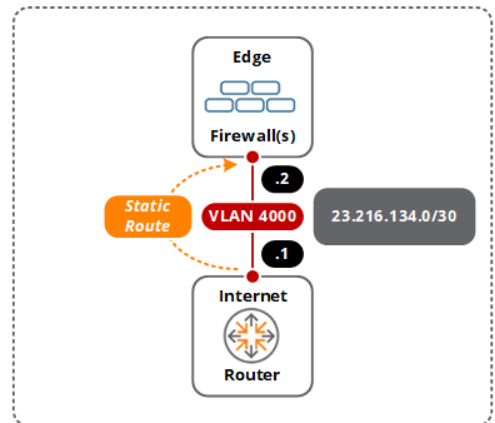
Edge Firewall (Internet Reachability)

- Requires a default route to provide reachability to the Internet
- This could either be dynamically learned via BGP or statically defined
- The next-hop router address is the address assigned to the Internet router in the Internet zone
- In this example the edge firewall has a static default route configured to **23.216.134.1**



Internet Router (VPNC Zone Reachability)

- If public addressing is implemented in the VPNC zone, the Internet Router must be able to reach the public network behind the edge firewall
- This can either be dynamically learned via BGP or statically defined
- The next-hop router address is the address assigned to the edge firewall in the Internet zone
- As the standalone/L2 redundant VPNCs in this example does not implement public addressing, no routes are required on the Internet router



Overlay Routing

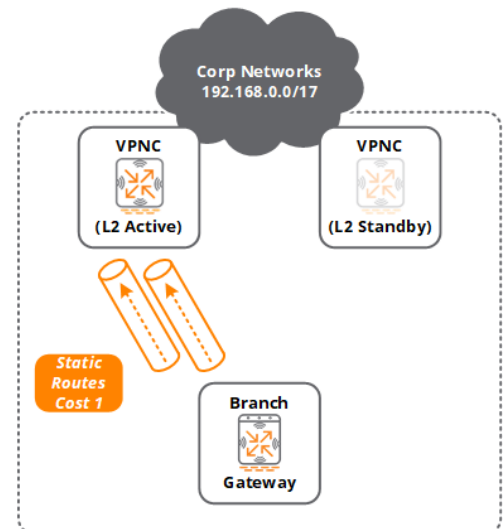
This reference topology can support static or dynamic routing to provide reachability between the corporate and branch networks through the overlay network. Static routing is typically implemented for smaller deployments where dynamic routing has not been implemented in the core/aggregation layers. Dynamic routing using OSPF provides the most flexibility as individual branch routes or a summary of the branch routes are automatically advertised and redistributed to the edge firewall and core/aggregation layers.

Static Routing

SD-Branch deployments implementing static routing requires configuration of static routes on the standalone/L2 redundant VPNCs, edge firewall, and core/aggregation layers to provide reachability between the corporate and branch networks:

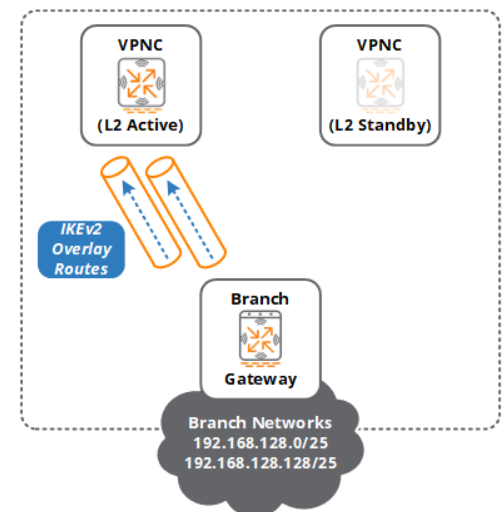
BGW (Corporate Network Reachability)

- Each BGW group is configured with static routes to reach the corporate networks using the MPLS and Internet VPN tunnels established to the standalone/L2 redundant VPNCs
- In this example the static route costs to reach the corporate network **192.168.0.0/27** through the standalone/L2 redundant VPNCs for each VPN tunnel are defined as **1**



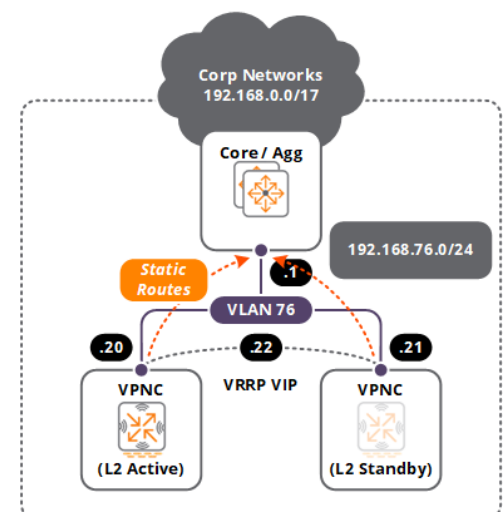
VPNC (Branch Network Reachability)

- Per Aruba best practices, each branch gateway is configured to advertise their local branch networks to the standalone/L2 active VPNC through the VPN tunnels using Aruba IKEv2 extensions
- This eliminates the need for defining static routes to reach the remote branch network on the VPNCs



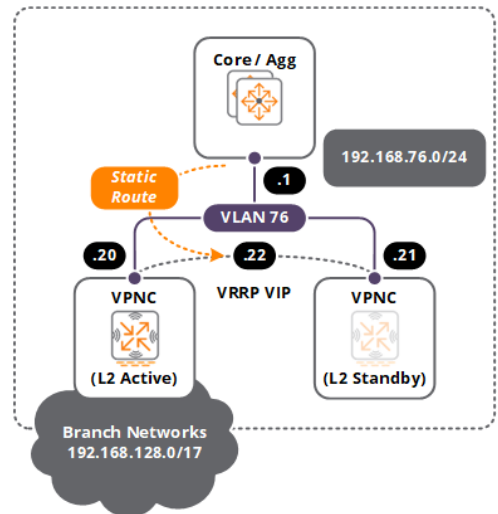
VPNC (Corporate Network Reachability)

- Requires static routes to reach the corporate networks through the core/aggregation layer
- In this example one static route is defined on the standalone/L2 redundant VPNCs to reach the **192.168.0.0/17** network through the core/aggregation layer via **192.168.76.1**



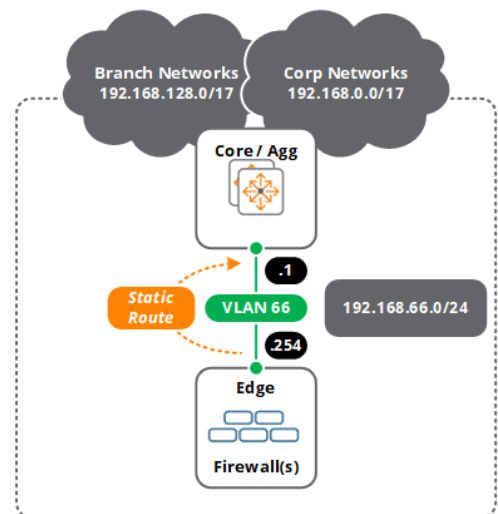
Core/Aggregation (Branch Network Reachability)

- Requires static routes to reach the branch networks through the standalone/L2 redundant VPNCs
- The next-hop router IP address will either be the host address of the standalone VPNC or the VRRP virtual IP address of the L2 redundant VPNCs
- In this example one static route is defined on the core/aggregation layer to reach the **192.168.128.0/17** branch networks through the L2 redundant VPNCs via the VRRP virtual IP **192.168.76.22**



Edge Firewall (Corporate/Branch Network Reachability)

- Requires static routes to reach both the corporate and branch networks through the core/aggregation layer
- In this example two static routes are defined on edge firewall to reach the **192.168.0.0/17** and **192.168.128.0/17** networks through the core/aggregation layer via **192.168.66.1**



Dynamic Routing (OSPF)

Dynamic routing requires OSPF to be configured on the core/aggregation switches, edge firewall, and VPNCs. The OSPF configuration for each device and zone is specific to each organization. When OSPF is enabled and configured, the standalone or L2 active VPNC will automatically redistribute connected branch routes in the trusted network using the overlay traffic VLAN which will be learned by the edge firewall and core/aggregation layers.

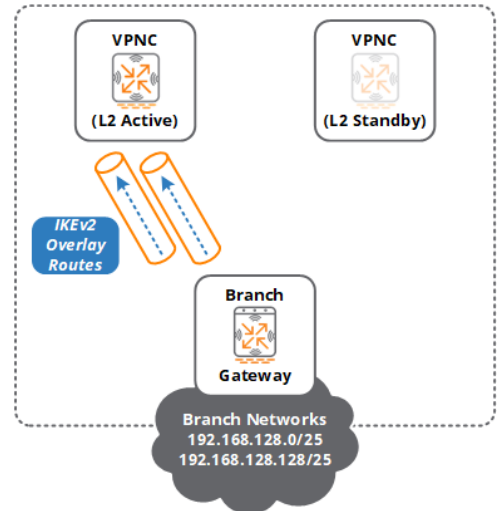
Branch routes can be redistributed into the OSPF area in two ways:

1. Individual branch routes can be redistributed into the OSPF area at a configured cost learned by the standalone/L2 active VPNC. Each route is installed by the OSPF routers as External Type 2 routes at the specified cost.
2. One or more summary routes for can be redistributed into the OSPF area at a configured cost by the standalone/L2 active VPNC. Each summary route is installed by the OSPF routers as External Type 2 routes at the specified cost.

For large SD-Branch deployments utilizing a single data center, Aruba recommends configuring summary routes as this will consume less CPU and memory resources on the OSPF routers in the network.

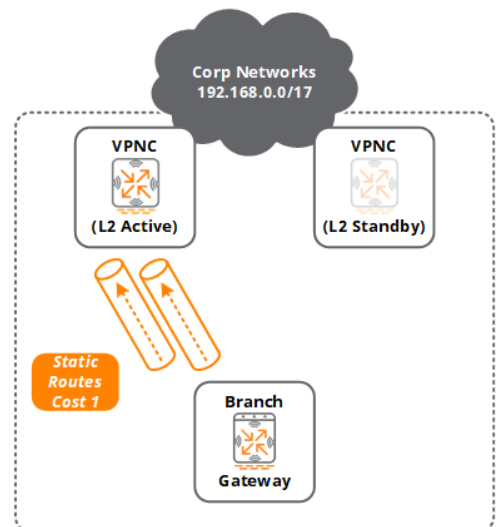
BGW (Corporate Network Reachability)

- Each BGW group is configured with static routes to reach the corporate networks using the MPLS and Internet VPN tunnels established to the standalone/L2 redundant VPNCs
- In this example the static route costs to reach the corporate network **192.168.0.0/27** through the standalone/L2 redundant VPNCs for each VPN tunnel are at a cost of **1**



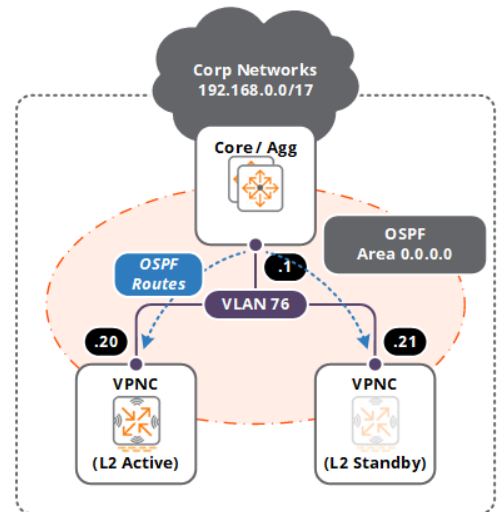
VPNC (Branch Network Reachability)

- Per Aruba best practices, each branch gateway is configured to advertise local branch networks to the standalone/L2 active VPNC through the VPN tunnels using Aruba IKEv2 extensions
- This eliminates the need for defining static routes to reach the remote branch network on the VPNCs



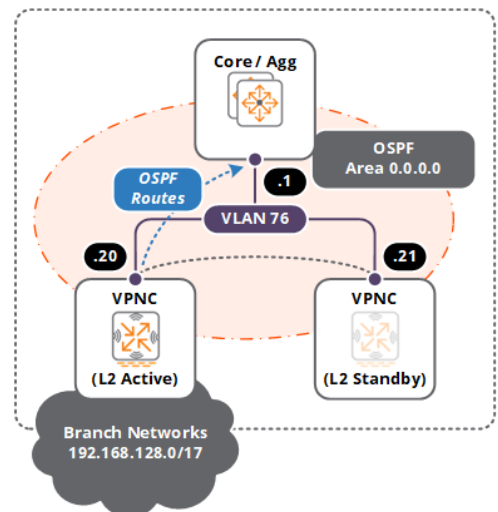
VPNC (Corporate Network Reachability)

- The VPNCs use OSPF routing on the overlay traffic VLAN to reach the corporate networks through the core/aggregation layer
- The corporate network routes are either individual or summarized
- The VPNCs and core/aggregation switch interfaces in VLAN 3100 are configured for the same OSPF area and type (example normal Area **0.0.0.0**)
- In this example the standalone/L2 redundant VPNCs learn a summarized **192.168.0.0/17** corporate network OSPF route from the core/aggregation switch via **192.168.76.1**



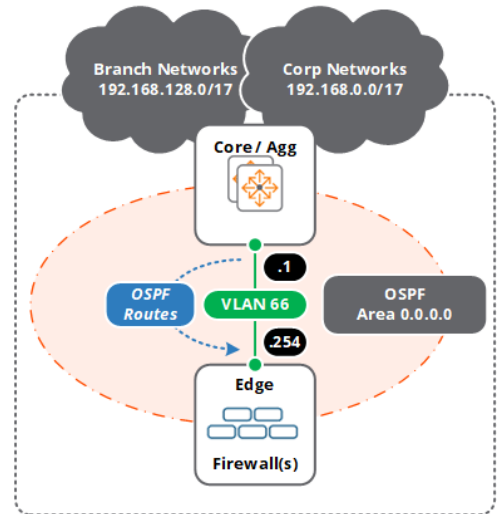
Core/Aggregation (Branch Network Reachability)

- The core/aggregation layer uses OSPF routing on the overlay traffic VLAN to reach the branch networks through the standalone/L2 active VPNC
- The branch network routes are either individual or summarized
- The VPNCs and core/aggregation switch interfaces in VLAN 3100 are configured for the same OSPF area and type (example normal Area **0.0.0.0**)
- In this example the core/aggregation layer switches learn a summarized **192.168.128.0/17** branch network route from the standalone/L2 active VPNC via **192.168.76.20**
- The summarized branch route is installed as an OSPF type 2 route



Edge Firewall (Corporate/Branch Network Reachability)

- The core/aggregation layer uses OSPF routing on the interconnect VLAN to reach the corporate and branch networks through the core/aggregation layer
- The corporate and branch network routes are either individual or summarized
- The edge firewall and core/aggregation switch interfaces in VLAN 66 are configured for the same OSPF area and type (example normal Area **0.0.0.0**)
- In this example the edge firewall learns the summarized **192.168.0.0/17** corporate route and **192.168.0.0/17** branch route via **192.168.66.1**
- The summarized branch route is installed as an OSPF type 2 route



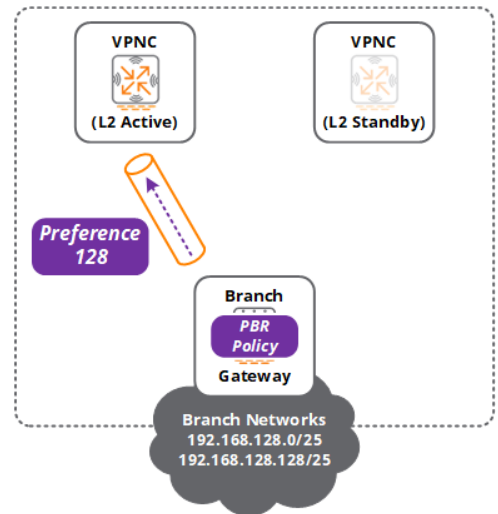
As a best practice, Aruba recommends configuring a loopback interface per VPNC that is used as the OSPF router ID. The core/aggregation layer switch operating as the designated router.

Policy Based Routing (PBR)

If full tunnel mode is required for one or more branch network, a PBR policy must be configured and applied to the VPN tunnels on the standalone/L2 redundant VPNCs. The PBR policy is required to forward branch overlay traffic destined to the Internet through the core/aggregation layer to ensure symmetrical routing.

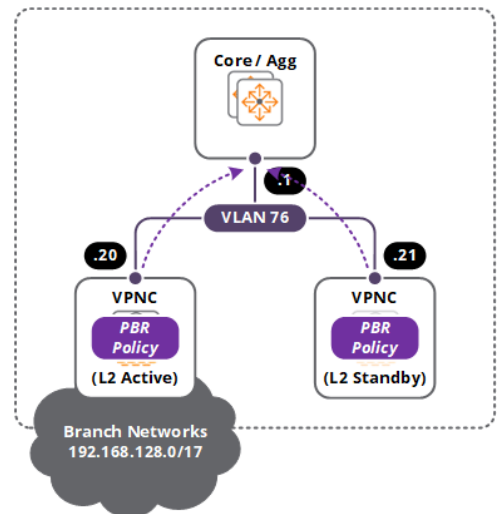
BGW

- Each BGW group is configured with an RAACL and next-hop list that forwards branch traffic destined to the Internet via the Internet VPN tunnels established to the standalone/L2 redundant VPNCs
- In this example the RAACL and next-hop list is configured to:
 - Forward branch traffic from **192.168.128.0/17** destined to the corporate network **192.168.0.0/17** normally
 - Forward branch traffic from **192.168.128.0/17** destined to **any** using a next-hop list
 - The next-hop list includes the VPN tunnel established to the standalone/L2 redundant VPNC using the default preference
- The RAACL can be applied to user sessions in the BGP group using roles or AAA policy



VPNC

- An RAACL is configured on the standalone/L2 redundant VPNCs with the following rules:
 - Route traffic received from the branch networks destined to the corporate networks normally (e.g., source **192.168.128.0/17** destined to **192.168.0.0/17**)
 - Forward traffic received from the branch networks destined to the Internet to the core/aggregation layer (e.g. source **192.168.128.0/17** destined to **any** via **192.168.76.1**)



PBR is required on the VPNC in this scenario to prevent symmetrical routing. By default the standalone/L2 redundant VPNCs will use the default gateway information and forward the branch traffic destined to the Internet directly to the edge firewall. As the edge firewall is only capable of reaching the branch networks through the core/aggregation layer, all return traffic will be forwarded to the core/aggregation layer which is different than the outgoing session path.

Dual Data Center

This reference topology can be deployed in a dual data center environment where a mirror of the standalone/L2 redundant VPNCs are deployed in a second data center. L2 redundancy (if enabled) is provided within each data center while L3 redundancy is provided between data centers.

When considering a dual data center design, it is important to note that only one data center will actively forward traffic during normal operation. The standalone/L2 redundant VPNCs in one data center are primary while the standalone/L2 redundant VPNCs in the second data center are secondary. This is required as OSPF is utilized in each data center to determine the active branch traffic path during normal operation. The OSPF external type 2 routes via the primary standalone/L2 active VPNC are installed by the OSPF routers in the corporate network during normal operation.

This dual data center design requires:

1. The corporate network must implement a dynamic routing protocol such as OSPF. If another IGP is implemented, the OSPF routes must be redistributed into the IGP at the appropriate costs.
2. Overlay routing between the VPNCs and the core/aggregation layer must implement OSPF. The branch routes are advertised as external type 2 routes at specific costs by the standalone/L2 active VPNC into each data center. The route cost determines which data center is primary and which data center is secondary. The redistributed or summery route cost for the primary data center must be lower than the redistributed or summery route cost in the secondary data center.
3. Each BGW group requires the overlay static routes to reach the corporate network to be defined at different costs. The overlay static routes using the MPLS and Internet VPN tunnels established to the primary standalone/L2 redundant VPNCs must be configured at a lower cost than the static routes using the MPLS and Internet VPN tunnels established to the secondary standalone/L2 redundant VPNCs.

Figure 5-13 shows an example dual data center topology where a L2 redundant pair of VPNCs are deployed per data center. Each data center including MPLS and Internet WAN services, core/aggregation layers, and edge firewalls. The standalone/L2 active VPNCs learn the corporate network routes using OSPF while redistributing branch network routes into the respective data centers at different costs:

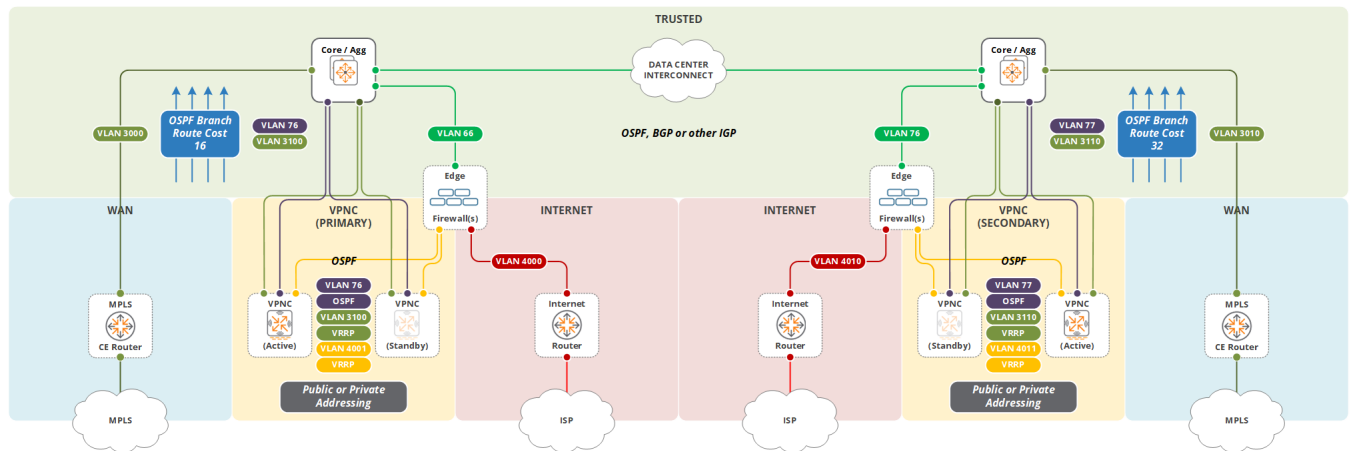


Figure 5-13 Internet and MPLS with Multiple Network Zones Dual DC Reference Topology

For this reference topology, the standalone/L2 active VPNC in each data center is connected to their respective edge firewall and core/aggregation switch using three VLAN interfaces:

- **VLANs 76/77** – Connect to the trusted zone in the respective data centers transmitting and receiving overlay traffic. VLAN 76 is used during normal operation while VLAN 77 is used during a L3 failover.
- **VLANs 4001/4011** – Connect to the VPNC zone in their respective data centers terminating the VPN tunnels from the Internet. VPN tunnels are established to both standalone/L2 active VPNCs in each data center during normal operation.
- **VLANs 3100/3110** – Connect to the trusted zone in their respective data centers terminating the VPN tunnels from the MPLS network. VPN tunnels are established to both standalone/L2 active VPNCs in each data center during normal operation.

Figure 5-14 provides the flow paths for the VPN tunnels and overlay traffic:

1. **MPLS VPN Tunnels (UDP 4500)** – All MPLS VPN tunnels are terminated by the MPLS VLAN interfaces on the standalone/L2 active VPNC in each data center, in this example VLANs 3100 and 3110.
2. **Internet VPN Tunnels (UDP 4500)** – All Internet VPN tunnels are terminated by the Internet VLAN interfaces on the standalone/L2 active VPNC in each data center, in this example VLANs 4001 and 4011.
3. **Overlay Corporate Traffic** – All overlay corporate traffic is transmitted and received by the overlay traffic VLAN interface on the primary standalone/L2 active VPNC. In this example VLAN 76 redistributes the branch routes to the OSPF network at the lowest cost.
4. **Overlay Internet Traffic** – If full-tunnel mode is implemented, all overlay internet traffic is carried by the overlay traffic VLAN interface on the primary standalone/L2 active VPNC. In this example VLAN 76 which redistributes the individual/summary the branch routes into the OSPF network at the lowest cost.

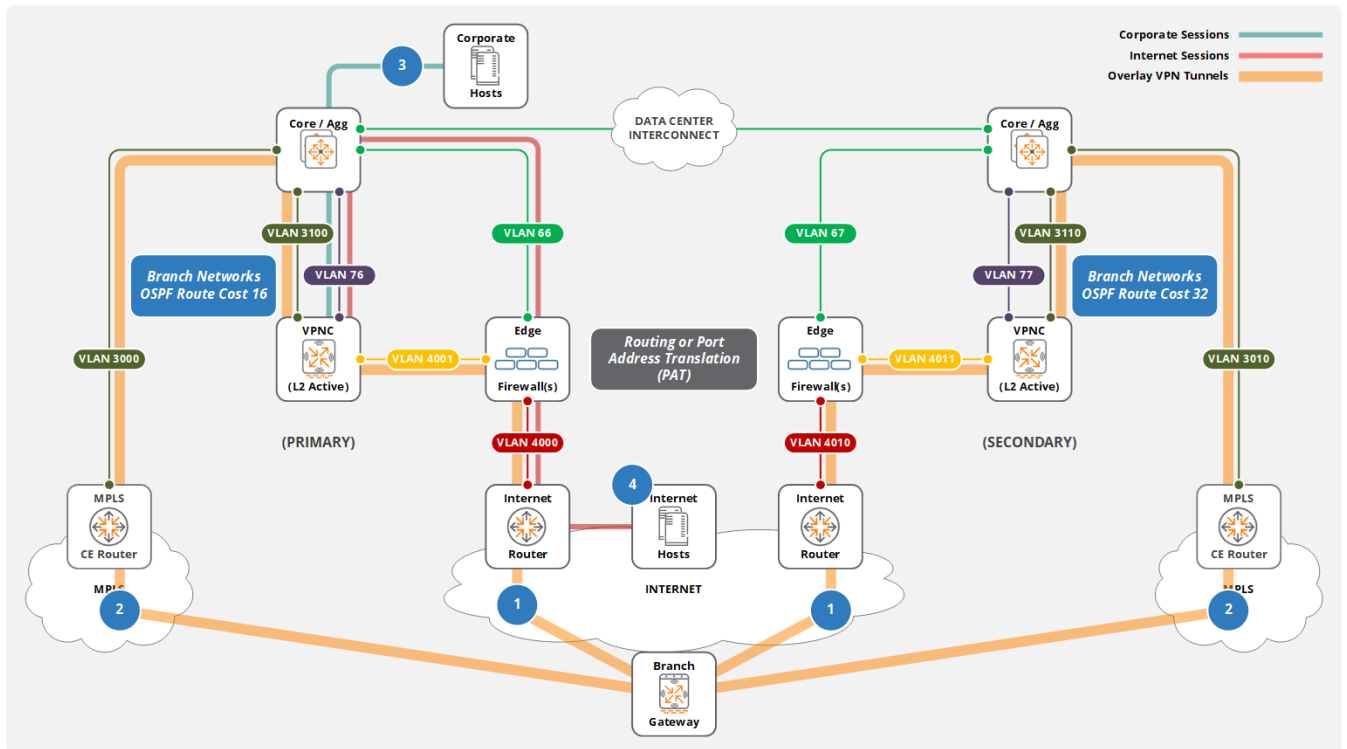


Figure 5-14 Internet and MPLS with Multiple Network Zones Dual DC Flow Diagram

Overlay Routing

This section provides the overlay route implementation details required support a dual data center design. As with a single data center deployment, the core/aggregation layers and edge firewalls in each data center need to learn how to reach the branch networks from VPNCs. Likewise, the edge firewalls and VPNCs need to be capable of reaching the corporate networks from the core/aggregation layers. This is achieved using dynamic routing where OSPF is required between the VPNCs and the core/aggregation layers.

In a dual data center design, the standalone/L2 redundant VPNCs in one data center are designated primary while the standalone/L2 redundant VPNCs in the second data center are designated secondary. The primary standalone/L2 redundant VPNCs forward and receive overlay traffic during normal operation. This is achieved by configuring different overlay static route costs in each BGW group along with different OSPF redistribution route costs on the VPNCs:

1. The static overlay routes are configured on the BGWs to reach the corporate networks through the VPN tunnels and terminate on the primary standalone/L2 redundant VPNCs using a low cost (e.g., 1)
2. The static overlay routes configured on the BGWs to reach the corporate networks through the VPN tunnels terminate on the secondary standalone/L2 redundant VPNCs use a higher cost (e.g., 10)

3. The primary standalone/L2 redundant VPNCs are configured to redistribute the individual or summary branch routes to the OSPF network at a low cost (e.g., 16)
4. The secondary standalone/L2 redundant VPNCs are configured to redistribute the individual or summary branch routes into the OSPF network at a higher cost (e.g., 32)

During normal operation the BGWs will forward all overlay traffic through the VPN tunnels terminating on the primary standalone/L2 active VPNC. Since the OSPF redistributed route cost from the primary standalone/L2 active VPNC is lower than the OSPF redistributed route cost on the secondary standalone/L2 active VPNC all return overlay traffic is forwarded to the primary.

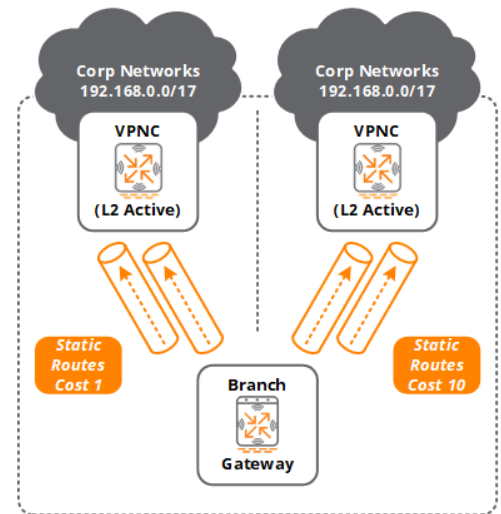
If an L2 failover occurs, the primary L2 standby VPNC will transition to an active role and terminate the VPN tunnels. The new L2 active VPNC will redistribute the branch networks to the OSPF network and will become the new path for the overlay traffic. Each branch network will be redistributed to OSPF at the same cost.

An L3 failover will occur if both VPN tunnels on a BGW established to the primary standalone/L2 redundant VPNC go down. The impacted BGWs will update their routing table to install the higher cost static routes pointing to the VPN tunnels established to secondary standalone/L2 active VPNC. All overlay traffic from the BGW destined to the corporate network will be forwarded using new routes. The OSPF routers in the corporate network will reconverge and install the higher cost routes for the impacted BGWs. The return path for the overlay traffic will use the secondary standalone L2 active VPNC.

As an L3 failover may occur for a subset of BGWs, Aruba does not recommend configuring the VPNCs to send summarized routes. This allows the OSPF routers to install more specific routes to reach the BGWs during a L3 failover. It is however recommended to enable summarization in the BGWs so that each BGW sends a summarized route for its branch networks using Aruba IKEv2 extensions.

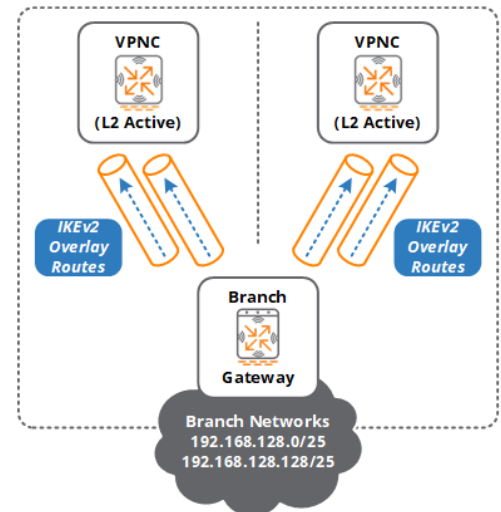
BGW (Corporate Network Reachability)

- Each BGW group is configured with static routes to reach the corporate networks using the MPLS and Internet VPN tunnels established to the primary and secondary standalone/L2 redundant VPNCs
- In this example the static route costs to reach the corporate network **192.168.0.0/27** through the primary standalone/L2 redundant VPNCs for each VPN tunnel are defined with a cost of **1**
- The static route costs to reach the corporate network **192.168.0.0/27** through the secondary standalone/L2 redundant VPNCs for each VPN tunnel are defined with a cost of **10**



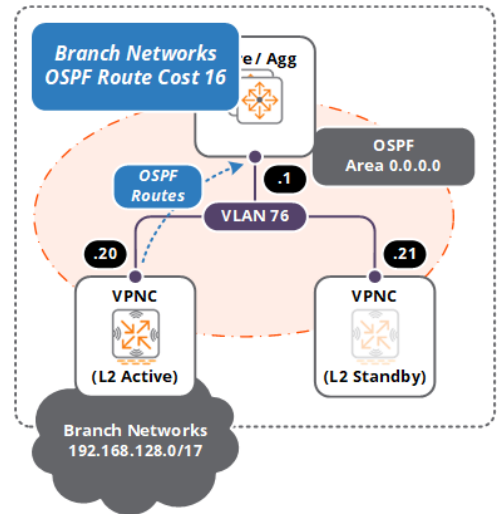
VPNC (Branch Network Reachability)

- Per Aruba best practices, each branch gateway is configured to advertise their local branch networks to each standalone/L2 active VPNC through the VPN tunnels using Aruba IKEv2 extensions
- This eliminates the need for defining static routes to reach the remote branch network on the VPNCs



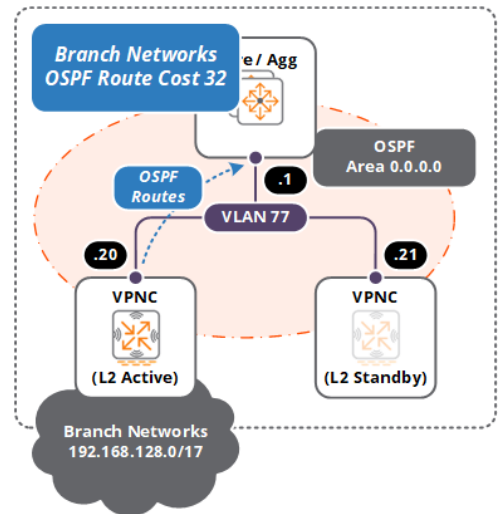
Core/Aggregation (Branch Network Reachability) – Primary Data Center

- The core/aggregation layer uses OSPF routing on the overlay traffic VLAN to reach the branch networks through the primary or secondary standalone/L2 active VPNC
- The VPNCs and core/aggregation switch interfaces in VLAN 3100 are configured for the same OSPF area and type (example normal Area **0.0.0.0**)
- In this example the core/aggregation layer switches learn individual branch routes from the primary standalone/L2 active VPNC via **192.168.76.20** at a cost of **16**
- Each redistributed branch route is installed as an OSPF type 2 route by the OSPF routers in the network



Core / Aggregation (Branch Network Reachability) – Secondary Data Center

- The core/aggregation layer uses OSPF routing on the overlay traffic VLAN to reach the branch networks through the primary or secondary standalone/L2 active VPNC
- The VPNCs and core/aggregation switch interfaces in VLAN 3110 are configured for the same OSPF area and type (example normal Area **0.0.0.0**)
- In this example the core/aggregation layer switches learn individual branch routes from the secondary standalone/L2 active VPNC via **192.168.77.20** at a cost of **32**
- Each branch route redistributed by the secondary standalone/L2 active VPNC is not installed by the OSPF routers during normal operation as a lower cost route via the primary standalone/L2 redundant VPNC (cost 16) is installed



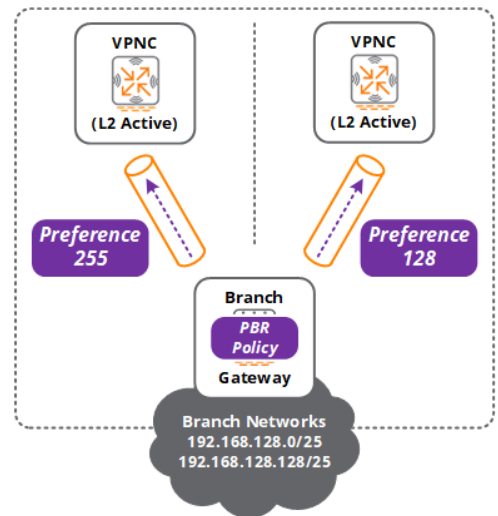
Policy Based Routing (PBR)

If full tunnel mode is required for one or more branch network, a PBR policy must be configured and applied to the VPN tunnels on the standalone/L2 redundant VPNCs. The PBR policy is required to forward branch overlay traffic destined to the Internet through the core/aggregation layer to ensure symmetrical routing.

As dual data centers are deployed, the next-hop list configured in the BGW group includes both the primary and secondary VPN tunnels. The next-hop configuration for the VPN tunnel established to the primary standalone/L2 redundant VPNCs is configured with a higher priority than the VPN tunnel established to the secondary standalone/L2 redundant VPNCs.

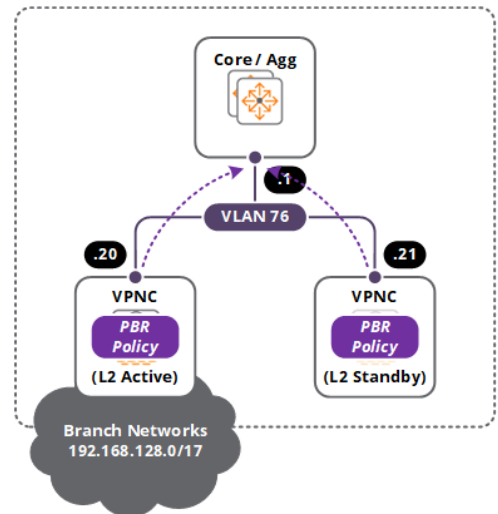
BGW

- Each BGW group is configured with an RACL and next-hop list that forwards branch traffic destined to the Internet via the Internet VPN tunnels established to the standalone/L2 redundant VPNCs
- In this example the RACL and next-hop list is configured to:
 - Forward branch traffic from **192.168.128.0/17** destined to the corporate network **192.168.0.0/17** normally
 - Forward branch traffic from **192.168.128.0/17** destined to **any** using a next-hop list
 - The next-hop list includes the VPN tunnels established to the primary and secondary standalone/L2 redundant VPNCs using different preferences:
 - The preference for VPN tunnels established to the primary standalone/L2 redundant VPNC using **255**
 - The preference for the VPN tunnels established to the secondary standalone/L2 redundant VPNC using **128**
- The RACL can be applied to user sessions in the BGP group using roles or AAA policy



VPNC – Primary Data Center

- An RAACL is configured on the standalone/L2 redundant VPNCs with the following rules:
 - Route traffic received from the branch networks destined to the corporate networks normally (e.g., example source **192.168.128.0/17** destined to **192.168.0.0/17**)
 - Forward traffic received from the branch networks destined to the Internet to the core/aggregation layer (e.g., source **192.168.128.0/17** destined to **any** via **192.168.76.1**)



VPNC – Secondary Data Center

- An RAACL is configured on the standalone/L2 redundant VPNCs with the following rules:
 - Route traffic received from the branch networks destined to the corporate networks normally (e.g., source **192.168.128.0/17** destined to **192.168.0.0/17**)
 - Forward traffic received from the branch networks destined to the Internet to the core/aggregation layer (e.g., source **192.168.128.0/17** destined to **any** via **192.168.77.1**)



PBR is required on the VPNC in this scenario to prevent symmetrical routing. By default the standalone/L2 redundant VPNCs will use the default gateway information and forward the branch traffic destined to the Internet directly to the edge firewall. As the edge firewall is only capable of reaching the branch networks through the core/aggregation layer, all return traffic will be forwarded to the core or aggregation layer which is different than the outgoing session path.



If full tunnel mode is required, the edge firewalls in each data center will also need to learn the branch route through the core/aggregation layer or directly from the standalone or L2 redundant VPNCs.

Edge Firewall

The edge firewall configuration will differ depending on whether public or private addressing is assigned to the VPNC zone. Each vendor's firewall configuration and architecture is unique, so the following section provides a high level overview of the firewall policies and NAT configuration that is required to support each reference architecture.

Topology Independent

The VPNCs use the VLAN interface in the VPNC zone to communicate with Central for management and configuration. At a minimum each VPNC must be able to resolve FQDNs via DNS from their assigned name servers and be able to establish a HTTPs based web-socket to Aruba Central.

VPNC Zone to Internet Zone

- To permit communication with Central for management/configuration and firmware updates, the following sessions must be permitted from the host address of each standalone/L2 redundant VPNC connected to the VPNC zone:
 - **Firmware Upgrades** – A permit rule to allow outgoing hypertext transfer protocol (HTTP) TCP sessions using port 80 from each to ***.arubanetworks.com** and ***.cloudfront.net**
 - **Management/Configuration** – A permit rule to allow outgoing HTTPS (TCP 443) sessions to ***.arubanetworks.com** and ***.cloudfront.net**
- If external network services are implanted, the following sessions must be permitted from the host address of each standalone/L2 redundant VPNC connected to the VPNC zone:
 - **Name Services** – A permit rule to allow DNS (UDP 53) sessions to each configured external name server
 - **Time Services** – A permit rule to allow NTP (123) sessions to each configured external time server

When the VPNC zone implements public addressing, the edge firewall must be configured to permit the Internet VPN tunnels to be established to the standalone/L2 redundant VPNCs in the VPNC zone:

Internet Zone to VPNC Zone (Public Addressing)

- **Standalone VPNC** – A permit rule to allow **NAT-T** (UDP 4500) sessions from **any** source destined to the **host** IP address assigned to the standalone VPNC VLAN interface in the VPNC zone
- **L2 Redundant VPNCs** – A permit rule to allow **NAT-T** (UDP 4500 sessions from **any** source destined to the **VRRP virtual** IP address assigned to the L2 redundant VPNCs in the VPNC zone

When the VPNC zone implements private addressing, the edge firewall must be configured to permit and port-forward the VPN tunnels to the standalone/L2 redundant VPNCs in the VPNC zone:

Internet Zone to VPNC Zone (Private Addressing)

- **Standalone VPNC**
 - A port forwarding policy is required to translate and forward **NAT-T** (UDP 4500) traffic received on the edge firewalls Internet Zone interface to the **host** IP address assigned to the standalone VPNC in the VPNC zone
 - A corresponding permit rule to allow the port forwarded session is required (please refer to the firewall documentation as this configuration varies by firewall vendor)
- **L2 Redundant VPNCs**
 - A port forwarding policy is required to translate and forward NAT-T (UDP 4500) traffic received on the edge firewalls Internet Zone interface to the VRRP virtual IP address assigned to the L2 redundant VPNCs in the VPNC zone
 - A corresponding permit rule to allow the port forwarded session is required (please refer to the firewall documentation as this configuration varies by firewall vendor)
- **Standalone / L2 Redundant VPNCs**
 - A NAT policy to translate outgoing Internet sessions from the host address of each standalone / L2 redundant VPNC connected to the VPNC zone to permit communications with Aruba Central and external network services (if required).

Reference Topology 1

As the overlay traffic transmitted and received from the standalone/L2 redundant VPNCs terminates directly on the edge firewall, the edge firewall must include the necessary firewall policies to permit branch managed devices and branch users access to specific services and hosts in the corporate network. The policies defined will be specific to each environment. The following provides example flows that need to be considered:

Branch Managed Devices to Corporate Network Services

Managed devices in the branches (Aruba BGWs, Aruba IAPs and Aruba Switches) may require access to network services hosted in the data center. Permit rules will be required for managed devices to access:

- AAA Servers (RADIUS/TACACS)
- Logging Servers (Syslog etc.)
- Time Servers (NTP)
- Name Servers (DNS)
- Utility Servers (FTP / TFTP / SFTP etc.)

Branch Users to Corporate Network Services

Users in branches will require access to network services hosted in the data center. Permit rules will be required for branch to access the following:

- Time Servers (NTP)
- Name Servers (DNS)
- User Directory Servers (AD / LDAP etc)
- File and Print Servers
- Internet Proxy Servers
- Unified Communication Servers (Messaging / Voice / Video etc.)

Branch Users to Corporate Users

Users in branches may require peer-to-peer communications to hosts on the corporate network. Permit rules will be required for branch to access the following:

- Peer-to-Peer file sharing
- Desktop screen sharing (Remote Desktop/LogMeIn etc.)
- Unified Communications (Messaging/Voice/Video etc.)

Full Tunnel Mode

If full tunnel mode is implemented for branch users, the edge firewall must be configured to permit outgoing access to the Internet from the respective source branch networks. This will include firewall policies to permit the sessions as well as NAT policies to translate the outgoing Internet sessions to the edge firewalls public IP Interface or NAT pool. A NAT pool is desirable for larger deployments consuming more than 65,535 TCP/UDP sessions.

Branch Topologies

The following section provides an overview and details for the tested and validated branch topologies that can be referenced to implement Aruba BGWs in branches. For each reference topology this guide provides the configuration requirements detailed and examples for:

1. VLANs and VLAN Interfaces
2. WAN uplinks
3. VPN tunnels
4. Underlay and overlay routing
5. Dynamic Path Selection

A reference topology is provided for both standalone and redundant BGWs. As it is impossible to accommodate every design permutation, typical topologies and configurations are provided for each topology which can be modified to suit business requirements. For each reference topology, detailed diagrams are provided to visualize the configurations, session paths and routing.

Standalone Branch Gateway

The following reference topology can be considered for branches implementing:

- A standalone branch gateway
- Internet and MPLS based WAN services
- Optional 3G/4G backup

Figure 5-15 provides the branch reference topology that will be discussed in this section. For simplicity the branch network is separated into LAN and WAN. All configuration is performed per BGW group unless specifically noted.

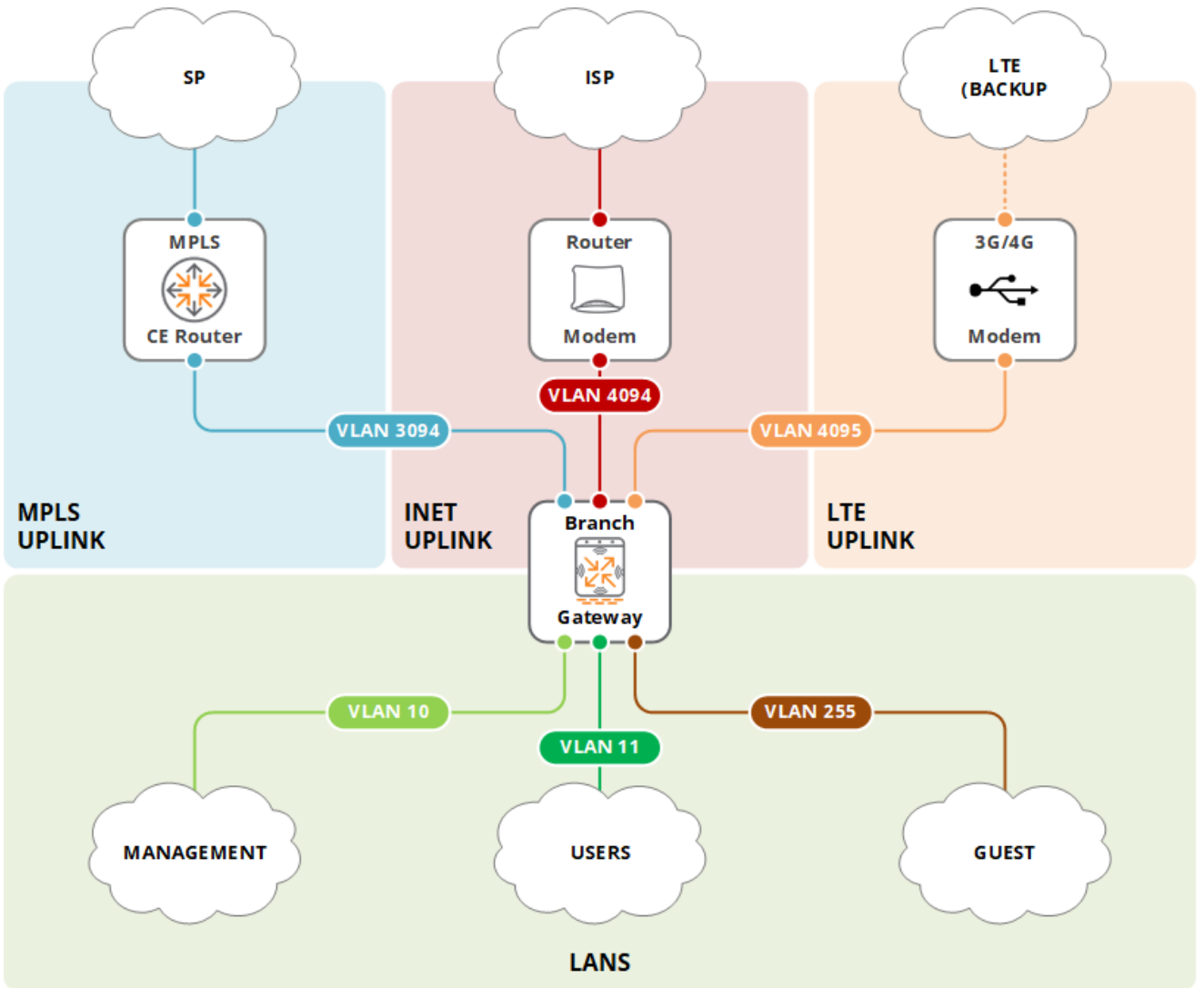


Figure 5-15 Standalone Branch Gateway Topology Example

Virtual LANs

This branch reference topology requires five VLANs which are used to connect the BGWs to the Internet and MPLS WAN services and provide connectivity to managed devices, corporate users and guests:

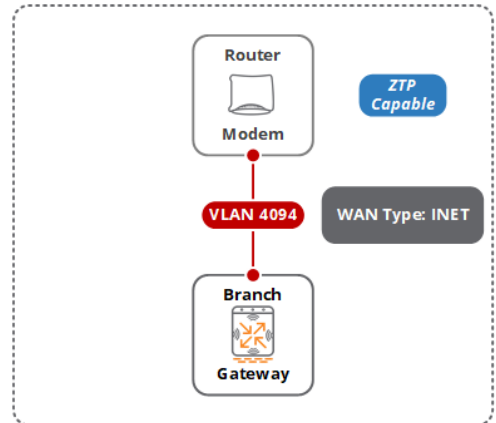
- **WAN** – Two VLANs are configured to support the MPLS and Internet WAN services. The USB LTE modem using an internal non-configurable VLAN. Each WAN uplink requires a dedicated VLAN ID and Interface.
- **LAN** – Three VLANs are configured to support managed devices, corporate users and guests.

Wide Area Network

This reference topology requires three VLANs to connect the BGWs to the Internet, MPLS, and LTE based WAN services:

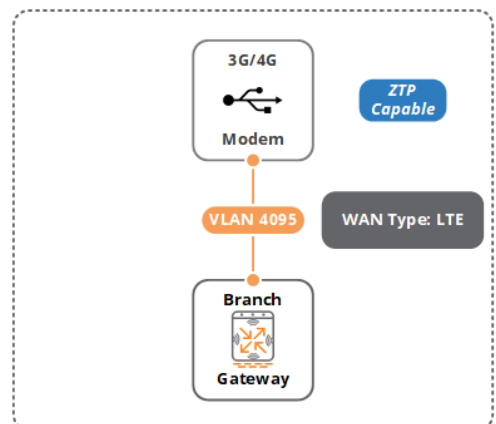
Internet WAN Uplink

- One VLAN is required to connect the BGWs to the CPE modem via Ethernet
- In this example the default **VLAN 4094** is assigned
- VLAN 4094 is enabled for zero touch provisioning (ZTP) by default and is assigned to each switchport except Ge0/0/1 on un-provisioned BGWs



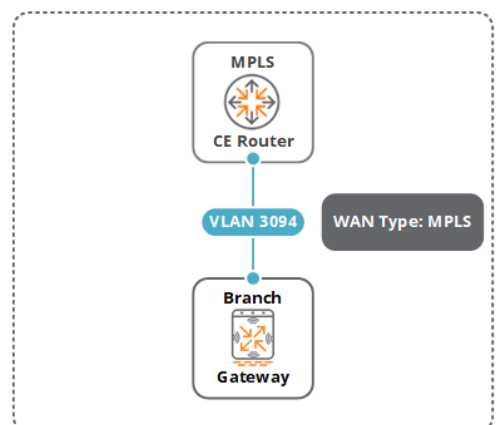
LTE WAN Uplink

- One VLAN is required to connect the BGWs to the USB based 3G/4G modem providing backup
- In this example the non-configurable internal **VLAN 4095** is assigned
- A BGW can perform zero touch provisioning using LTE if required



MPLS WAN Uplink

- One VLAN is required to connect the BGWs to the MPLS CE router via Ethernet
- In this example **VLAN 3094** is assigned



If a branch deployment implements an Ethernet based 3G/4G adaptor it will require a normal VLAN (1-4094) to be assigned.



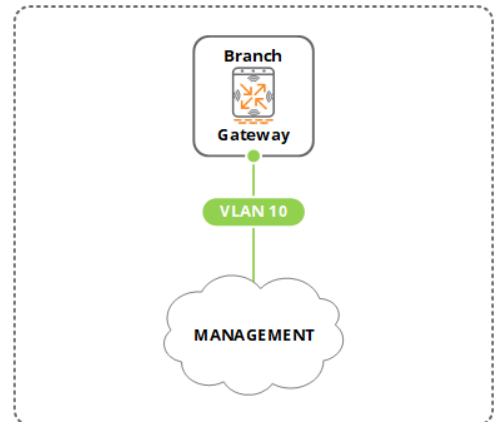
WAN services can be added and substituted as required.

Local Area Network

This reference topology requires three VLANs to connect branch devices, users, and guests:

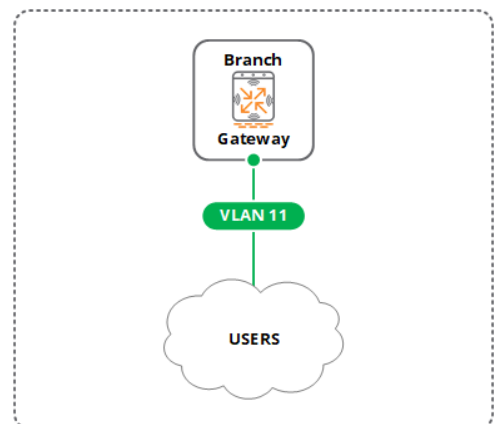
Management VLAN

- One VLAN is required to connect the managed devices such as IAPs and ArubaOS switches to the branch gateways
- This VLAN will be used to manage the devices as well as support the generic routing encapsulation (GRE) tunnels used for port-based tunneling (if enabled)
- In this example **VLAN 10** is assigned



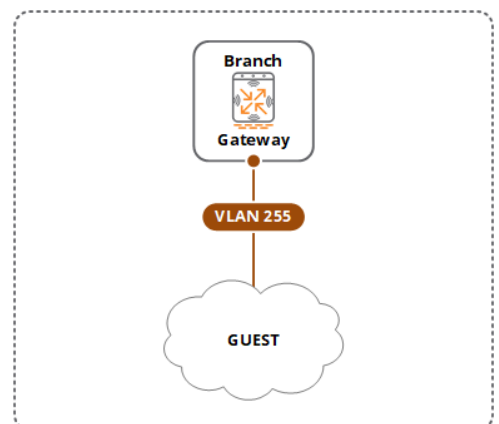
Corp User VLAN

- One VLAN is required to connect the corporate users to the branch gateways
- All corporate users will be assigned this VLAN with an appropriate role
- In this example **VLAN 11** is assigned



Guest User VLAN

- One VLAN is required to connect the guest users to the branch gateways
- All guest users will be assigned this VLAN with an appropriate role
- In this example **VLAN 255** is assigned

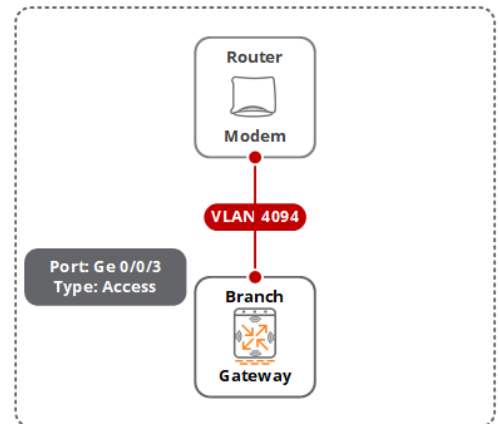


Ports

This reference topology requires three ports to connect the BGWs to the Internet and MPLS WAN services as well as an ArubaOS switch:

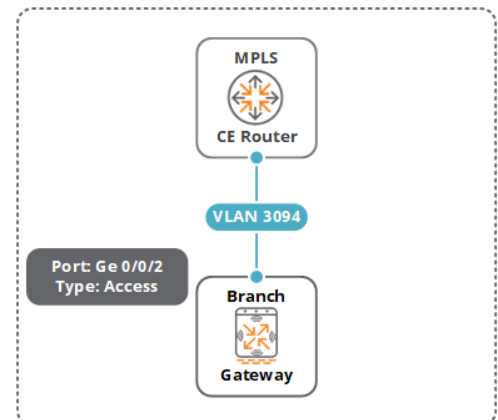
Internet WAN Uplink

- One access port is required to connect the BGW to the Internet CPE modem
- In this example **VLAN 4094** is assigned to the access port **Ge0/0/3**. The port and VLAN are **Trusted**



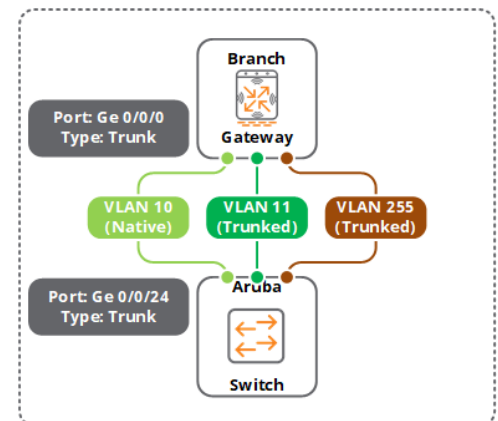
MPLS WAN Uplink

- One access port is required to connect the BGW to the MPLS-CE router
- In this example **VLAN 3094** is assigned to the access port **Ge0/0/2**. The port and VLAN are **Trusted**



LAN Uplink

- One trunk port is required to connect the BGW to an ArubaOS switch to support the management, corporate user and guest VLAN
- In this example the ArubaOS-Switch is connected to **Ge0/0/0** which is **Untrusted**
 - **VLAN 10** – Assigned as the **Native VLAN**. Add a AAA policy to the VLAN to set the initial role (e.g., **management-role**).
 - **VLAN 11** – Assigned as a **Trunked VLAN**. Add an AAA policy to the VLAN to set the initial role (e.g., **login-role**).
 - **VLAN 255** – Assigned as a **Trunked VLAN**. Add an AAA policy to the VLAN to set the initial role (e.g., **guest-logon**).





The device management VLAN 10 is untagged to allow the un-configured ArubaOS switch to perform ZTP. The unconfigured switch will require manual configuration if all the VLANs are trunked.



The initial roles assigned to the management VLAN in this example include the necessary rules to permit DHCP, DNS, NTP, and communication with Central. The default roles assigned to the corporate user and guest VLANs are specific to environmental and security policy requirements. Default roles are shown in the above example.

VLAN Interfaces

This branch reference topology implements both static and dynamic addressing.

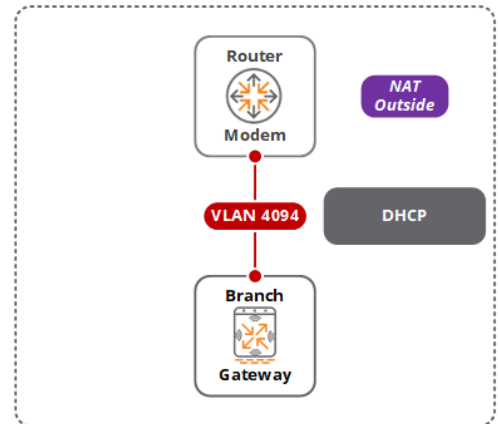
Wide Area Network

The Internet and MPLS WAN services require both dynamic and static addressing:

- **Internet WAN** – Assigned a dynamic IPv4 address from the Internet Service provider via DHCP
- **MPLS WAN** – Assigned a static IPv4 address

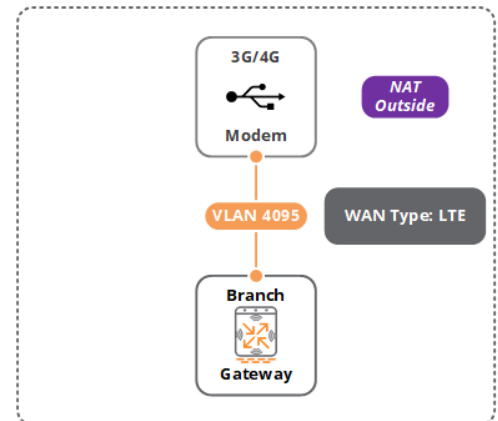
Internet WAN Uplink

- A VLAN interface for **VLAN 4094** is configured per BGW group with the following parameters:
 - Enable routing is **Enabled**
 - IP assignment is set to **DHCP**
 - NAT outside is **Enabled**



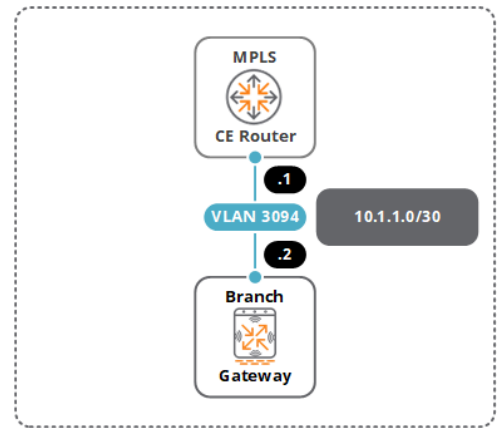
LTE WAN Uplink

- No additional configuration is required. By default the internal **VLAN 4095** is configured with the following parameters:
 - Enable routing is **Enabled**
 - IP assignment is set to **DHCP**
 - NAT outside is **Enabled**



MPLS WAN Uplink

- A VLAN interface for **VLAN 3094** is configured per BGW group with the following parameters:
 - Enable routing is **Enabled**
 - IP assignment is set to **Static**
 - NAT outside is **Disabled**
- The individual **IPv4 address** and **Netmask** assignments are applied to each BGW at the device level
- In this example the MPLS IPv4 address **10.1.1.0/30** has been statically assigned at the device level to an individual BGW



If the deployment includes an Internet WAN service that requires PPPoE, the VLAN interface is created per BGW group with the IP assignment set to PPPoE. The PPPoE credentials can either be provisioned in Central (device level) or learned from the BGW during ZTP.

Local Area Network

IP addressing for LAN based VLAN interfaces can be statically or dynamically assigned:

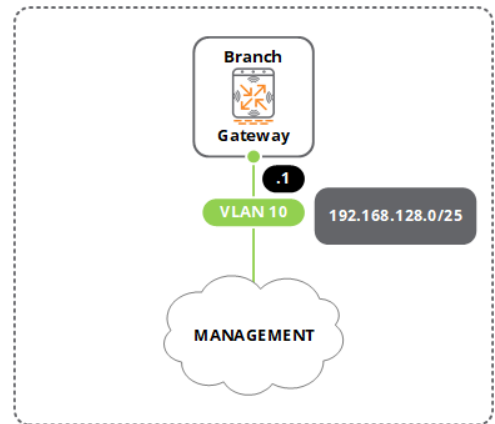
1. Static address assignment using bulk configuration upload. The uploaded bulk configuration file includes the LAN VLAN IDs and associated IP addresses and netmasks.
2. Static address assignment using group and device level configuration. The VLAN interfaces are configured per BGW group while the individual IPv4 address and netmask assignments are applied to each BGW at the device level.
3. Dynamic address assignment using Dynamic DHCP pools assigned to BGW groups. A large pool of addresses is created for each VLAN allocating a specific number of host addresses per BGW. The VLAN interfaces are configured to obtain IP addressing from the respective dynamic DHCP pools. Each BGW is allocated IP addressing on a first come first served basis.

For this reference topology static address assignment for the management and corporate user VLANs was applied to each BGW using bulk configuration upload. The VLAN interfaces were configured at the group level with bulk configuration applying the per BGW device address assignments.

The VLAN interface for the guest users uses a common IPv4 address and netmask in this example as this broadcast domain is local to each BGW and not accessible via the overlay network. If full tunnel mode is required for guest users, a unique subnet is required per BGW:

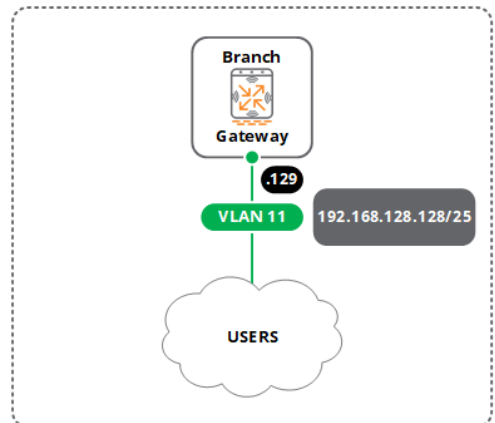
Management

- A VLAN interface for **VLAN 10** is configured per BGW group with the following parameters:
 - Enable routing is **Enabled**
 - IP assignment is set to **Static**
- The individual **IPv4 address** and **Netmask** assignments are applied to each BGW at the device level using bulk provisioning
- In this example the host IPv4 address **192.168.128.1/25** has been assigned using bulk configuration to an individual BGW



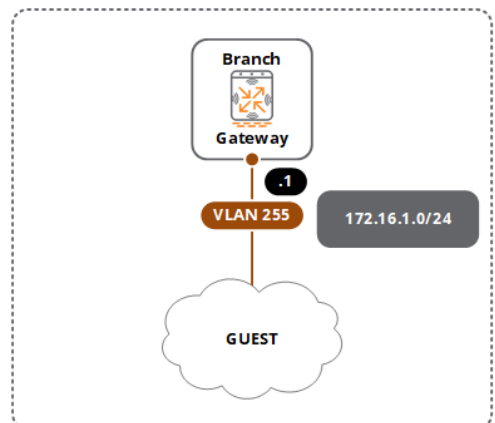
Users

- A VLAN interface for **VLAN 11** is configured per BGW group with the following parameters:
 - Enable routing is **Enabled**
 - IP assignment is set to **Static**
- The individual **IPv4 address** and **Netmask** assignments are applied to each BGW at the device level using bulk provisioning
- In this example the host IPv4 address **192.168.128.129/25** has been assigned using bulk configuration to an individual BGW



Guest

- A VLAN interface for **VLAN 255** is configured per BGW group with the following parameters:
 - Enable routing is **Enabled**
 - IP assignment is set to **Static**
 - IPv4 Address is set to **172.16.1.1**
 - Netmask is set to **255.255.255.0**



User DHCP Pools

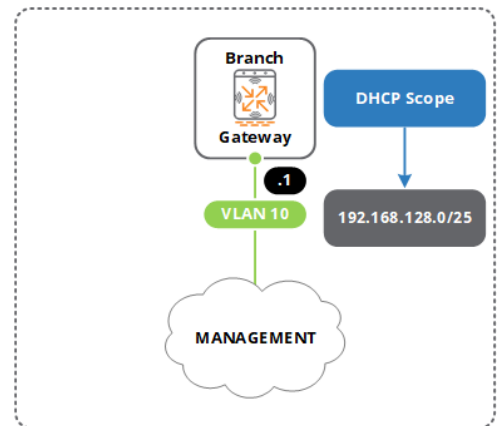
For this reference topology IP addresses are dynamically assigned to managed devices, corporate users, and guest users using the integrated DHCP server on each BGW. For this example three DHCP scopes are required:

- **Managed devices and Corporate Users** – As the IP addressing for the managed devices and corporate user VLAN at each branch is unique, the configuration is performed per BGW at the device level. Each BGW is configured with two DHCP scopes, exclusion ranges and options using Aruba Central or bulk configuration.
- **Guest Users** – As the IP addressing for the guest VLAN is the same for each branch, the DHCP scope, exclusion ranges and options for the branch users are configured per BGW group. The BGW group is also employed to globally enable the DHCP server.

Management (Device)

A DHCP scope, options and exclusion range is defined for **VLAN 10** per BGW:

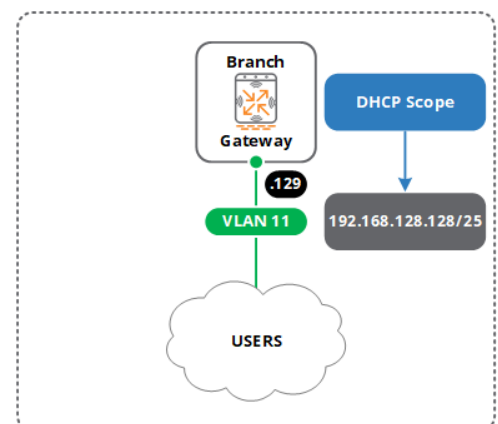
- Exclusion Range – **192.168.128.1 – 192.168.128.10**
- Network – **192.168.128.0/25**
- Option 3 (Router) – **192.168.128.1**
- Option 6 (Name Server) – **192.168.10.2, 192.168.10.3**
- Option 15 (Domain Name) – **arubanetworks.local**



Users (Device)

A DHCP scope, options and exclusion range is defined for **VLAN 11** per BGW:

- Exclusion Range – **192.168.128.129 – 192.168.128.138**
- Network – **192.168.128.128/25**
- Option 3 (Router) – **192.168.128.129**
- Option 6 (Name Server) – **192.168.10.2, 192.168.10.3**
- Option 15 (Domain Name) – **arubanetworks.local**



Guest (Group)

A DHCP scope, options and exclusion range is defined for **VLAN 255** per BGW group:

- Exclusion Range – **172.16.1.1 – 172.16.1.100**
- Network – **172.16.1.0/24**
- Option 3 (Router) – **172.16.1.1**
- Option 6 (Name Server) – **1.1.1.1**
- Option 15 (Domain Name) – **arubanetworks.local**



The integrated DHCP server on each Aruba Gateway can maintain support a specific number client devices. The 7005/7008 can support 1,000, the 7010/7024 can support 2,000, and the 7030 can support 4,000.

System

System IP Address

Each BGW requires a System IP address to be defined with is set to a common VLAN interface that is present on each BGW. The System IP address is a critical component of a BGW as it defines the VLAN interface that is used to communicate with other systems (RADIUS, Syslog, TACACS+, SNMP, etc.). The system IP address can be set to an existing VLAN interface or a dedicated VLAN interface. Most BGW deployments utilize an existing VLAN interface.

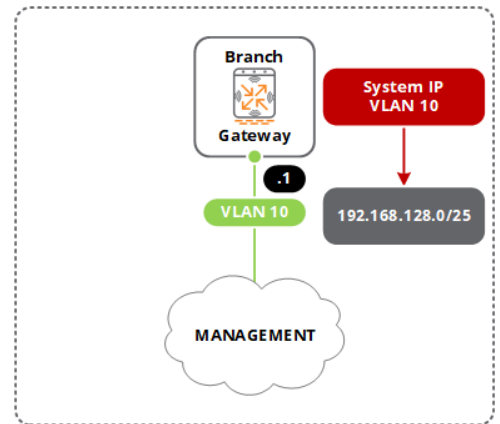
By default, the System IP address of each BGW will be set to the first VLAN interface created on the BGW. If the BGW performs ZTP, **VLAN 4094** is selected. As a best practice Aruba recommends using a LAN VLAN interface over a WAN VLAN interface as the IPv4 addressing will not change preventing unnecessary reboots. If the System IP address changes during normal operation, the BGW must reboot.

The System IP address can be set to an existing VLAN interface used by one of the branch LANs or an administrator can optionally create a dedicated VLAN interface that dynamically obtains host addressing from a Gateway Pool that is assigned to the BGW group. One Gateway Pool is required per BGW group. The Gateway Pool option is preferred when no bulk configuration is being performed.

For this branch reference architecture, the VLAN interface addressing for each LAN is assigned to each BGW using bulk configuration. The bulk configuration each BGW assigning the management and user VLAN IDs and per VLAN interface addressing. To simplify the System IP configuration, the bulk configuration template includes a **Controller VLAN** field that allows specification of the VLAN ID for the VLAN interface the BGW will use as its System IP. The bulk configuration is applied during the provisioning process. Once the device and group level configuration has been applied, the BGW will reboot using its new configuration and System IP:

System IP Address

The VLAN interface for **VLAN 10** is selected as the System IP using bulk configuration. In this example the BGW will use **192.168.128.1** as its System IP address.



Domain Name Services and Time

As a best practice Aruba recommends configuring a primary and secondary name server IP as well as two or more NTP time servers for each BGW group. This recommendation ensures that the BGWs are configured with the correct time and date and also ensures the BGWs can resolve critical FQDNs such as **central.arubanetworks.com** and **pqm.arubanetworks.com**:

1. **Name Servers** – Aruba recommends configuring public name server IP addresses as it allows the BGWs to resolve FQDNs in the event that the overlay network is unavailable. E.g., Google or Cloudflare DNS.
2. **Time Servers** – Aruba recommends defining two or more NTP server IP addresses whenever possible. E.g., Google NTP servers `time1.google.com` (216.239.35.0) and `time2.google.com` (216.239.35.4).

Wide Area Network

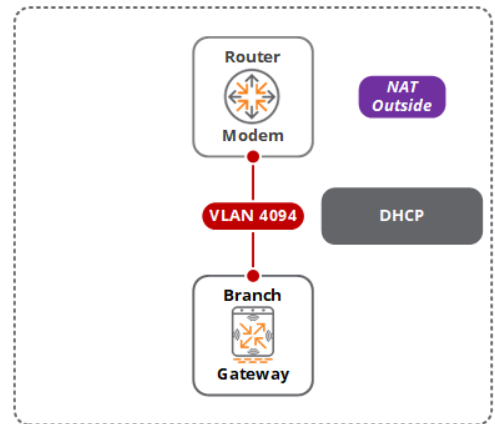
Uplinks

This branch reference topology implements three WAN services that require WAN uplinks to be configured. The WAN uplink ties each WAN VLAN interface to a WAN type, determines the operation state, and assigns a friendly name. For this topology a WAN uplink will need to be configured for the Internet, MPLS, and LTE WAN services. The LTE WAN uplink is marked as a backup link that will only be activated in the event of both Internet and MPLS WAN service failures:

Internet WAN Uplink

One WAN uplink is required for the Internet WAN service using the following parameters:

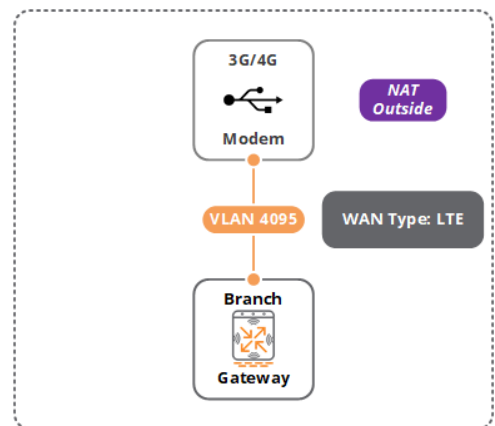
- Link type set to **INET**
- Link name set to **ACME**
- Interface VLAN ID set to **4094**



LTE WAN Uplink

One WAN uplink is required for the LTE backup service using the following parameters:

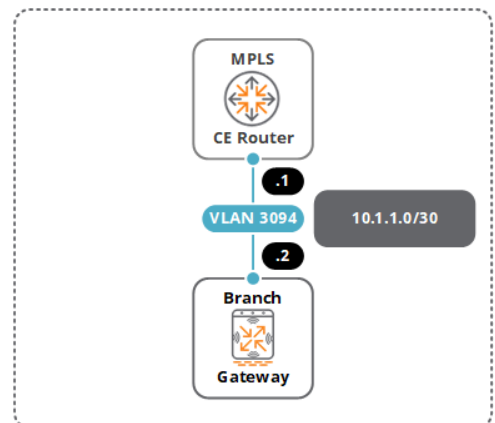
- Link type set to **LTE**
- Link name set to **ACME**
- Use only a backup link is **Enabled**



MPLS WAN Uplink

One WAN uplink is required for the MPLS WAN service using the following parameters:

- Link type set to **MPLS**
- Link name set to **ACME**
- Interface VLAN ID set to **3094**



As a best practice Aruba does not recommend naming the links after their type such as Internet or MPLS as the link type will automatically be appended. E.g., the above naming will result in the three WAN uplinks being labeled **ACME_INET**, **ACME_LTE**, and **ACME_MPLS**.

Health Checks

As a best practice Aruba recommends enabling IP health checks and defining a remote host IP/FQDN for each BGW group. For convenience Aruba provides a free cloud hosted health-check responder **pqm.arubanetworks.com** that can respond to ICMP and UDP probes from Aruba BGWs. The health check is used to monitor the availability and health of Internet based WAN paths.

The PQM service is a distributed cloud hosted probe responder service that is deployed across multiple regions including North America, Europe, and Asia. The PQM service will respond to ICMP or UDP probes from any source, however responses to non-whitelisted BGWs will be throttled to protect against DoS attacks.



As the health-check IP/FQDN will not typically be reachable over the MPLS WAN service, the health-check will show as failed. This will not impact the VPN tunnel establishment or overlay traffic forwarded over the MPLS WAN service.

Virtual Private Network

This branch reference topology implements an Internet and MPLS WAN service that will be used during normal operation. The BGW will initiate VPN tunnels over each WAN service to one or more VPNCs to create an overlay network upon which traffic is encapsulated and forwarded. The number of VPN tunnels that are established will be dependent on whether there is a single or dual data center:

- **Single Data Center** – The BGW will establish a total of two VPN tunnels:
 - One VPN tunnel established to a standalone/L2 redundant VPNCs via the Internet WAN
 - One VPN tunnel established to the standalone/L2 redundant VPNCs via the MPLS WAN
- **Dual Data Centers** – The BGW will establish a total of four VPN tunnels:
 - One VPN tunnel established to the primary standalone/L2 redundant VPNCs via the Internet WAN
 - One VPN tunnel established to the primary standalone/L2 redundant VPNCs via the MPLS WAN
 - One VPN tunnel established to the secondary standalone/L2 redundant VPNCs via the Internet WAN
 - One VPN tunnel established to the secondary standalone/L2 redundant VPNCs via the MPLS WAN

As the LTE WAN uplink is configured for backup only, no VPN tunnel will be established during normal operation. The LTE WAN service is only activated in the event that both the Internet and MPLS WAN uplinks fail. As the LTE WAN service is internet based, the VPN tunnel(s) will be

terminated by the same VLAN interface on the VPNCs as the Internet WAN service. The VPN hubs configured per BGW group will be dependent on the number of data centers deployed as well as whether there are standalone or L2 redundant VPNCs. This reference architecture assumes that two data centers are deployed, each with L2 redundant VPNCs.

Each VPN hub configuration requires the following mandatory parameters:

- **Primary VPNC** – Drop down selection of the name and MAC address of the L2 active VPNC assigned to a VPNC group. Alternatively the MAC address may be manually entered if **Connect automatically to VPNC** is enabled and a passphrase is defined.
- **Secondary VPNC** – Drop down selection of the name and MAC address of the L2 standby VPNC assigned to a VPNC group. Alternatively the MAC address may be manually entered if **Connect automatically to VPNC** is enabled and a passphrase is defined.
- **IP Address** – The VRRP virtual IPv4 address assigned to the Internet or MPLS underlay VLAN interfaces on the L2 redundant VPNCs.
- **Source VLAN** – The WAN VLAN interface on the BGW that the VPN tunnel is initiated out.



For the data center topology 3, the Internet WAN services terminate on VLAN interfaces connected to the VPNC zone. Each edge firewall is configured to port-forward UDP 4500 traffic received on its public interface to the respective private VRRP virtual IP addresses assigned to the primary and secondary L2 redundant VPNCs.

The following examples show VPN configuration for the BGW group using the IP addressing assigned to the edge firewalls and L2 redundant VPNCs in data center topology 3:

Internet WAN Uplink (Primary Data Center)

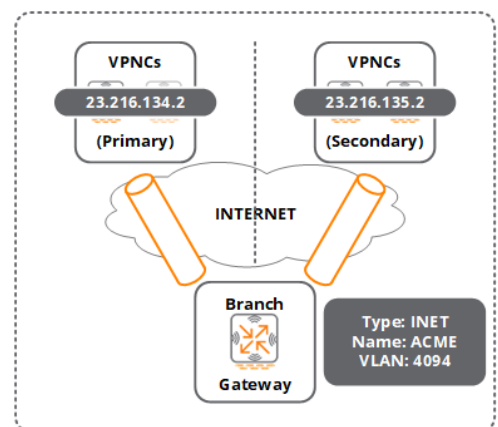
One hub entry is configured with the following parameters:

- **Primary VPNC** – Example **20:4c:03:0a:5d:70**
- **Secondary VPNC** – Example **20:4c:03:0a:89:f0**
- **IP Address** – Example **23.216.134.2** (translated Address)
- **Source VLAN** – Example **4094**

Internet WAN Uplink (Secondary Data Center)

One hub entry is configured with the following parameters:

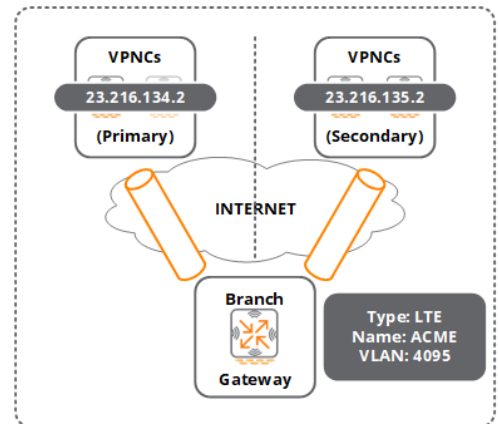
- **Primary VPNC** – Example **20:4c:03:0a:3a:2a**
- **Secondary VPNC** – Example **20:4c:03:0a:27:5d**
- **IP Address** – Example **23.216.135.2** (translated Address).
- **Source VLAN** – Example **4094**



LTE WAN Uplink (Primary Data Center)

One hub entry is configured with the following parameters:

- **Primary VPNC** – Example **20:4c:03:0a:5d:70**
- **Secondary VPNC** – Example **20:4c:03:0a:89:f0**
- **IP Address** – Example **23.216.134.2** (translated address)
- **Source VLAN** – Example **4095**



LTE WAN Uplink (Secondary Data Center)

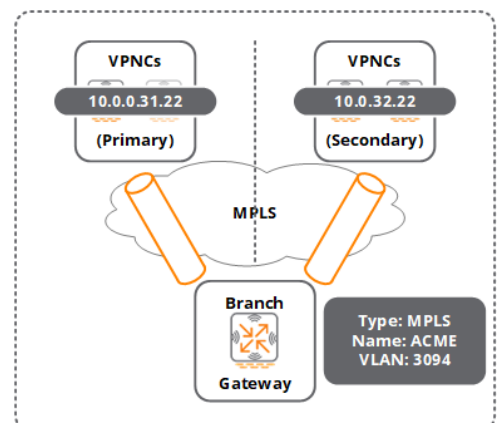
One hub entry is configured with the following parameters:

- **Primary VPNC** – Example **20:4c:03:0a:3a:2a**
- **Secondary VPNC** – Example **20:4c:03:0a:27:5d**
- **IP Address** – Example **23.216.135.2** (translated address)
- **Source VLAN** – Example **4095**

MPLS WAN Uplink (Primary Data Center)

One hub entry is configured with the following parameters:

- **Primary VPNC** – Example **20:4c:03:0a:5d:70**
- **Secondary VPNC** – Example **20:4c:03:0a:89:f0**
- **IP Address** – Example **10.0.31.22**
- **Source VLAN** – Example **3094**



MPLS WAN Uplink (Secondary Data Center)

One hub entry is configured with the following parameters:

- **Primary VPNC** – Example **20:4c:03:0a:3a:2a**
- **Secondary VPNC** – Example **20:4c:03:0a:27:5d**
- **IP Address** – Example **10.0.32.22**
- **Source VLAN** – Example **3094**

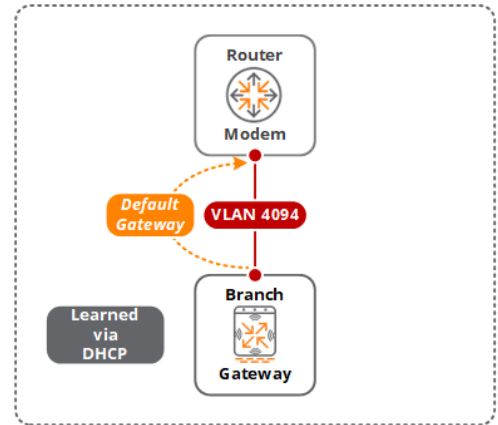
Routing

Underlay Routing

This branch reference topology implements default gateways for the Internet, MPLS and backup LTE WAN services to provide underlay routing. The default gateways for the Internet and backup LTE WAN services are dynamically learned from DHCP while the default gateway for the MPLS WAN service is statically defined per BGW at a device level:

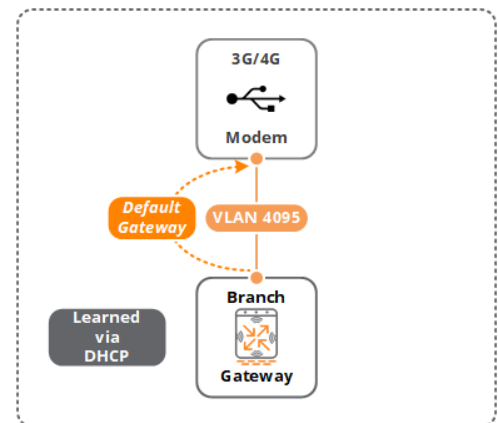
Internet WAN Uplink

- Dynamically learns the default gateway from the Internet Service Provider (ISP) using DHCP or PPPoE
- By default the dynamically learned default gateway will be installed at a cost of **10**



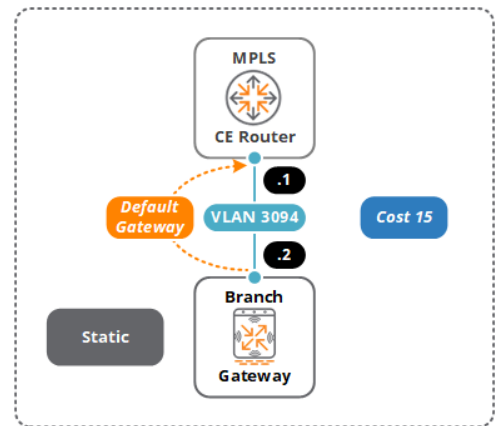
LTE WAN Uplink

- Dynamically learns the default gateway from the 3G/4G cellular provider using DHCP
- By default the dynamically learned default gateway will be installed at a cost of **10**



MPLS WAN Uplink

- As the MPLS-CE router is unique per branch site, the default gateway pointing to the MPLS-CE router is manually configured on each BGW at the device level.
- The default gateway must be defined at a cost of 15 (or higher)
- In this example a default gateway using the MPLS-CE router IP **10.1.1.1** has been statically assigned at the device level using a cost of **15**



Failure to configure a static default gateway for the MPLS WAN uplink will result in the VPN tunnels not being established through the MPLS WAN service.

Overlay Routing

This branch reference topology implements an Internet and MPLS WAN services that during normal operation are used to initiate VPN tunnels to the primary and secondary data centers to establish the overlay network. A combination of static routing and the advertisement of branch VLANs is used to provide reachability between the branch and corporate networks:

- **Static Overlay Routes** – Configured per BGW group to determine each WAN uplink for branch to corporate reachability through each VPN tunnel.
- **VLAN Advertisements** – Per Aruba best practices are configured per BGW group to advertise individual or summarized branch networks to the each standalone/L2 active VPNC using Aruba IKEv2 extensions. This is to permit corporate to branch reachability through each VPN tunnel.

The number of static routes that configured in the BGW group will be dependent on the number of WAN uplinks and data centers. One static route is required for each corporate network that needs to be reached through each VPN tunnel to each data center.

When multiple data centers are deployed, the overlay static routes are configured using different costs. This configuration is required to prevent asymmetrical routing between the BGWs and the VPNCs. Static corporate routes through the primary standalone/L2 redundant VPNCs are configured with a lower cost than the same corporate routes through the secondary standalone/L2 redundant VPNCs. The higher cost routes are only installed if the VPN tunnels to the primary standalone / L2 redundant VPNCs are not available or go down.

As this branch topology implements a backup LTE WAN service, static routes are also required to reach the corporate networks through each VPN tunnel established over the LTE WAN. These static routes will be defined at the same route cost than the Internet and MPLS WAN routes, however these routes will only be installed in the event that the backup LTE WAN interface becomes active.

The following provides an example static overlay route configuration performed per BGW group required to reach the **192.168.0.0/17** corporate network through the VPN tunnels established to the primary and secondary L2 redundant VPNCs. Since it is also desirable to reach other branch networks (**192.168.128.0/17**) through the VPNCs, the overlay static routes will be defined to reach the **192.168.0.0/16** network to include both the corporate and branch CIDR ranges. The BGW group will require six overlay static routes to be configured:

Overlay Routes (Primary Data Center)

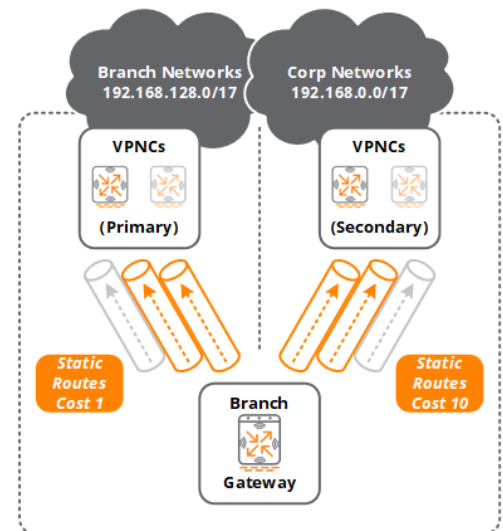
Requires three overlay routes to be configured reach the destination **192.168.0.0/16** corporate network through each VPN tunnel established to the primary L2 redundant VPNCs at a cost of **1**:

- **Overlay Route 1** – Via the Internet WAN uplink
- **Overlay Route 2** – Via the MPLS WAN uplink
- **Overlay Route 3** – Via the LTE WAN uplink

Overlay Routes (Secondary Data Center)

Requires three overlay routes to be configured reach the destination **192.168.0.0/16** corporate network through each VPN tunnel established to the secondary L2 redundant VPNCs at a cost of **10**:

- **Overlay Route 1** – Via the Internet WAN uplink
- **Overlay Route 2** – Via the MPLS WAN uplink
- **Overlay Route 3** – Via the LTE WAN uplink



Dynamic Path Steering

This branch reference topology implements dynamic path steering (DPS) to select the overlay paths each corporate traffic types. Each DPS policy includes:

1. **Traffic Selection Rules** – Determines what traffic is matched for the policy to be selected
2. **Optional SLA** – Determines the SLA that must be met for the Primary, Secondary, and Tertiary WAN paths to be considered
3. **WAN Path Selection** – The Primary, Secondary, and Tertiary WAN paths that can be considered for the matched traffic

The DPS policies defined and configured for BGW groups will be specific to each environment, traffic types, and the SLA requirements for each traffic type. For this example, four DPS policies are defined in the BGW group to select overlay traffic paths for voice, corporate data, corporate Internet, and guest Internet:

- **Corporate Voice** – IP Phones at the branches are assigned the user-role **voice**. All VoIP traffic destined to the corporate network or other branches (**192.168.0.0/16**) will prefer the MPLS path unless the SLA is not met upon which the Internet path is selected. The backup LTE path is selected if both the MPLS and Internet paths are down.
- **Corporate Data** – Employees are assigned the user-role **employee**. All employee bulk data traffic destined to the corporate network or other branches (**192.168.0.0/16**) will prefer the Internet path unless the SLA is not met upon which the MPLS path is selected. The backup LTE path is selected if both the MPLS and Internet paths are down.
- **Corporate Internet** – Employees are assigned the user-role **employee**. All employee traffic destined to the Internet will prefer the Internet path. The backup LTE path is assigned as a tertiary path which will be selected if both the Internet and MPLS paths are down. The backup LTE path is selected if the Internet path is down. No SLA is assigned.
- **Guest Internet** – Guests are assigned the user-role **guest**. All guest traffic destined to the Internet will prefer the Internet path. No backup path or SLA is assigned.

The following table provides the DPS policy that will be configured for each BGW group

Policy	Traffic Selection	SLA	WAN Path Selection
CORP-VOICE	Src: user-role = voice Dst: 192.168.0.0/16	SLA: BestForVoice	Primary: ACME_mpls Secondary: ACME_inet Tertiary: ACME_lte
CORP-DATA	Src: user-role = employee Dst: 192.168.0.0/16	SLA: HighlyAvailable	Primary: ACME_inet Secondary: ACME_mpls Tertiary: ACME_lte
CORP-INTERNET	Src: user-role = employee Dst: Any	SLA: None	Primary: ACME_inet Secondary: ACME_lte
GUEST-INTERNET	Src: user-role = guest Dst: Any	SLA: None	Primary: ACME_inet

Table 5-1 DPS Policies for BGW Groups



In the above example the selected MPLS, Internet, and LTE paths for each DPS policy include the prefix **ACME** which was defined in the WAN uplinks section. The suffix indicates the WAN type.

Policy Based Routing

If full tunnel mode is required for one or more branch networks, a PBR policy and next-hop list must be configured on the BGW group to determine which branch traffic is routed normally and which branch traffic is selected and forwarded to data center through the overlay network.

The next-hop configuration defined in the BGW group will be dependent on the number of WAN uplinks the BGW supports and if the deployment includes a single data center or dual data center:

- **Single Data Center** – The nexthop configuration will include each VPN tunnel established to the standalone/L2 redundant VPNCs at an equal priority. The DPS policy selecting the appropriate path.
- **Dual Data Center** – The next-hop configuration will include each VPN tunnel established to the primary standalone/L2 redundant VPNCs at a higher priority than each VPN tunnel established to the secondary standalone/L2 redundant VPNCs. The DPS policy selecting the appropriate path.

This branch reference topology establishes tunnels to primary and secondary L2 redundant VPNCs, six next-hop entries are required to forward the selected traffic to the primary and secondary VPNCs though the Internet, MPLS, and backup LTE VPN tunnels:

PBR Policy

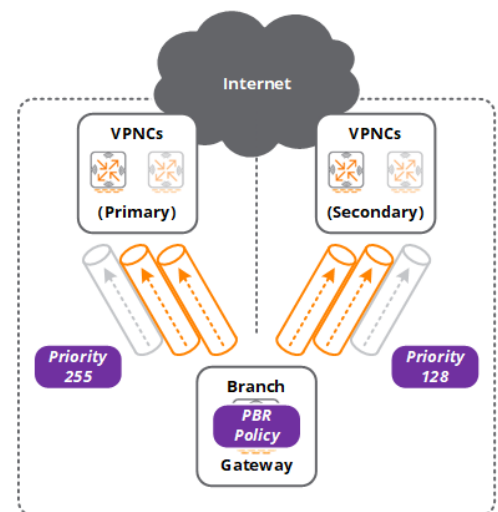
A PBR policy is configured per BGW group with the following rules:

- **Rule 1** – Matches traffic from **any** source to the destination **192.168.0.0/16** with a **forward** action. This rule is required to ignore traffic destined to the corporate and branch networks.
- **Rule 2** – Matches traffic from **any** source to the destination **any** with the action to route to the configured next-hop list.

Next-hop List (Primary Data Center)

Includes three next-hop IPsec MAP entries:

- **Next-hop 1** – The VPN tunnel to the primary L2 redundant VPNCs established over the MPLS WAN path with the priority **255**.
- **Next-hop 2** – The VPN tunnel to the primary L2 redundant VPNCs established over the Internet WAN path with the priority **255**.
- **Next-hop 3** – The VPN tunnel to the primary L2 redundant VPNCs established over the backup LTE WAN path with the priority **255**.



Next-hop List (Secondary Data Center)

Includes three next-hop IPsec MAP entries:

- **Next-hop 1** – The VPN tunnel to the secondary L2 redundant VPNCs established over the MPLS WAN path with the priority **128**.
- **Next-hop 2** – The VPN tunnel to the secondary L2 redundant VPNCs established over the Internet WAN path with the priority **128**.
- **Next-hop 3** – The VPN tunnel to the primary L2 redundant VPNCs established over the backup LTE WAN path with the secondary **128**.

Internet WAN Session ACL

By default the Internet WAN uplink will permit all incoming sessions received from the Internet. To protect the branch, Aruba recommends configuring a session ACL (SACL) in Central that is applied to the Internet WAN uplink port to restrict the incoming traffic that is allowed into the BGW. At a minimum the SACL should include:

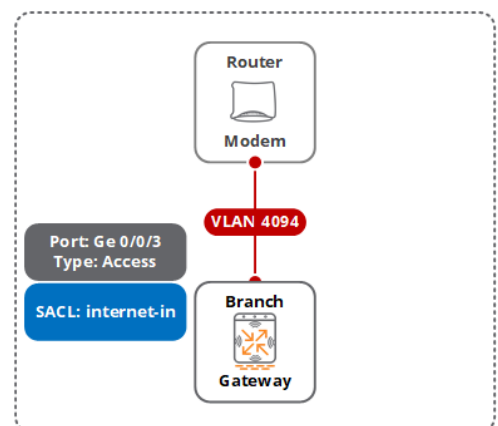
1. A permit rule to allow DHCP. This is required to allow the VLAN interface to obtain IP addressing from the Internet Service Providers DHCP server.
2. One or more permit rules to allow incoming traffic from each VPNC peer. This rule is recommended to permit UDP probes from the BGW and allow SSH access.
3. One rule to deny and log all other incoming traffic.

Additional permit rules may be added as required. For example if BGWs are terminating VPN connections from (Virtual Internet Access) VIA clients or Remote Access Points (RAPs) the necessary permit rules need to be added to allow HTTPS and NAT-T protocols. The following provides an example SACL named internet-in that is applied to the Ge0/0/3 ports for each BGW group:

Internet Session ACL

For this example the SACL will include three permit rules and one deny rule:

- **Rule 1** – Permits the service **svc-dhcp** from **any** source to **any** destination
- **Rule 2** – Permits all IP traffic from the host **23.216.134.2** (public IP of the primary L2 redundant VPNCs)
- **Rule 3** – Permits all IP traffic from host **23.216.135.2** (public IP of the secondary L2 redundant VPNCs)
- **Rule 4** – Denies and logs all other incoming traffic



Port-Based Tunneling

The configuration requirements for port-based tunneling in the branch is provided in a separate tech note that includes the details for configuring the ArubaOS switches, gateways, and the policies in Aruba ClearPass. This section highlights the branch VLAN differences and considerations when port-based tunneling is enabled.

In a typical branch deployment, the management, employee, and guest VLANs are trunked between the Aruba Branch Gateways, ArubaOS switches and IAPs:

1. Interconnect ports between Aruba devices are configured as trunk ports. The management VLAN is assigned as a Native VLAN while the employee and guest VLANs are tagged.
2. WLANs statically or dynamically assign employees and guest wireless users to their respect VLANs. The employee WLAN mapping users to VLAN 11 while the guest WLAN mapping users to VLAN 255. The users are assigned to their respective roles using AAA.
3. Management, employee and guest VLANs are either statically assigned to access ports or dynamically assigned using MAC or 802.1X based authentication from ClearPass.

Figure 5-16 depicts a sample topology consisting of management, employee, and guest VLAN assignments in an example branch deployment:

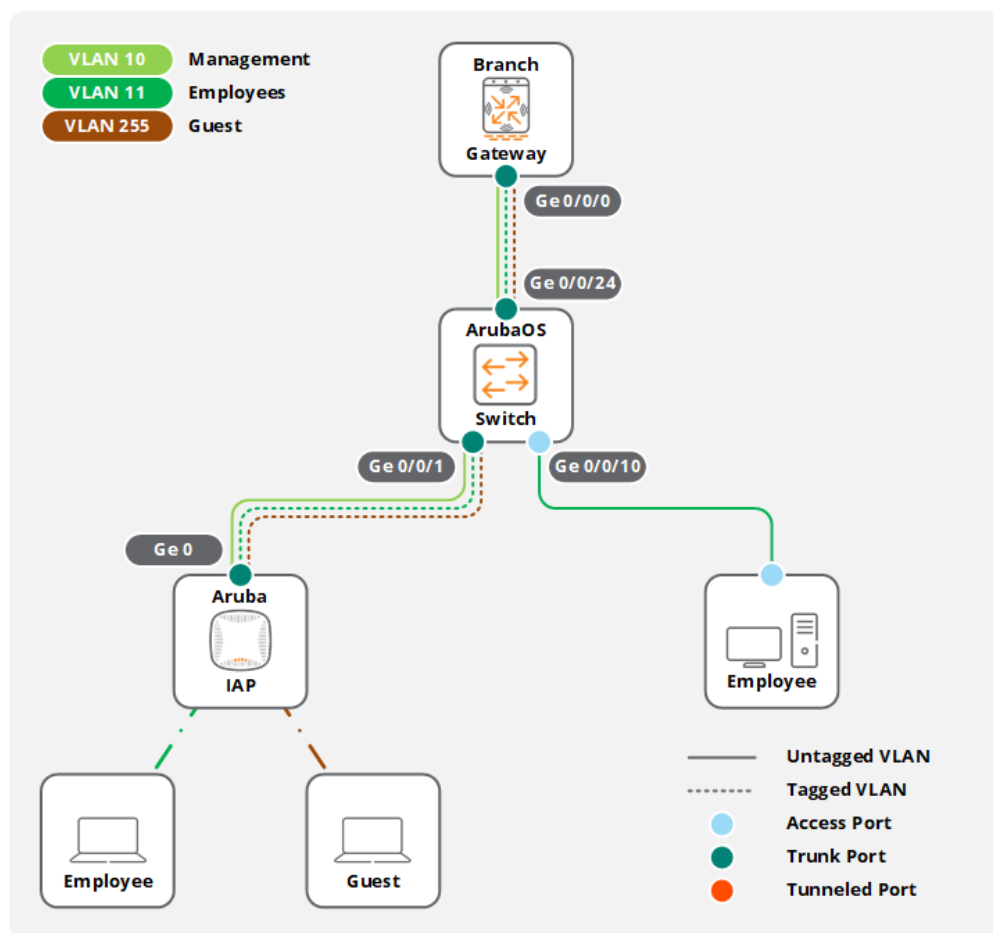


Figure 5-16 VLANs – Non Tunneled Ports

When port-based tunneling is enabled in a branch, all the VLANs from a tunneled port on an ArubaOS switches are encapsulated and forwarded by the ArubaOS switch to the BGW through a GRE tunnel. Each tunnel port establishing one GRE tunnel to the BGW. The BGW terminates all the VLANs in the branch (non-tunneled and tunneled) and includes a VLAN interface for each VLAN. The BGW assigning roles and applying policies to employee and guest devices.

One requirement for port-based tunneling is that a VLAN assigned to one or more normal ports on an ArubaOS-Switch cannot be tunneled to the BGW. A branch VLAN is either tunneled or non-tunneled. This requires a new VLAN design as the management VLAN previously used to manage the IAPs cannot be tunneled. The non-tunneled management VLAN is utilized to manage the ArubaOS switches and establish the GRE tunnels.

To provide management for the IAPs and support the cluster, a new IAP management VLAN is required. The new VLAN design tunneling the IAP management, employee and guest VLAN between the ArubaOS switches and the BGWs in the branch. The IAP management VLAN assigned as the native VLAN while the employee and guest VLANs are tagged (Figure 5-17):

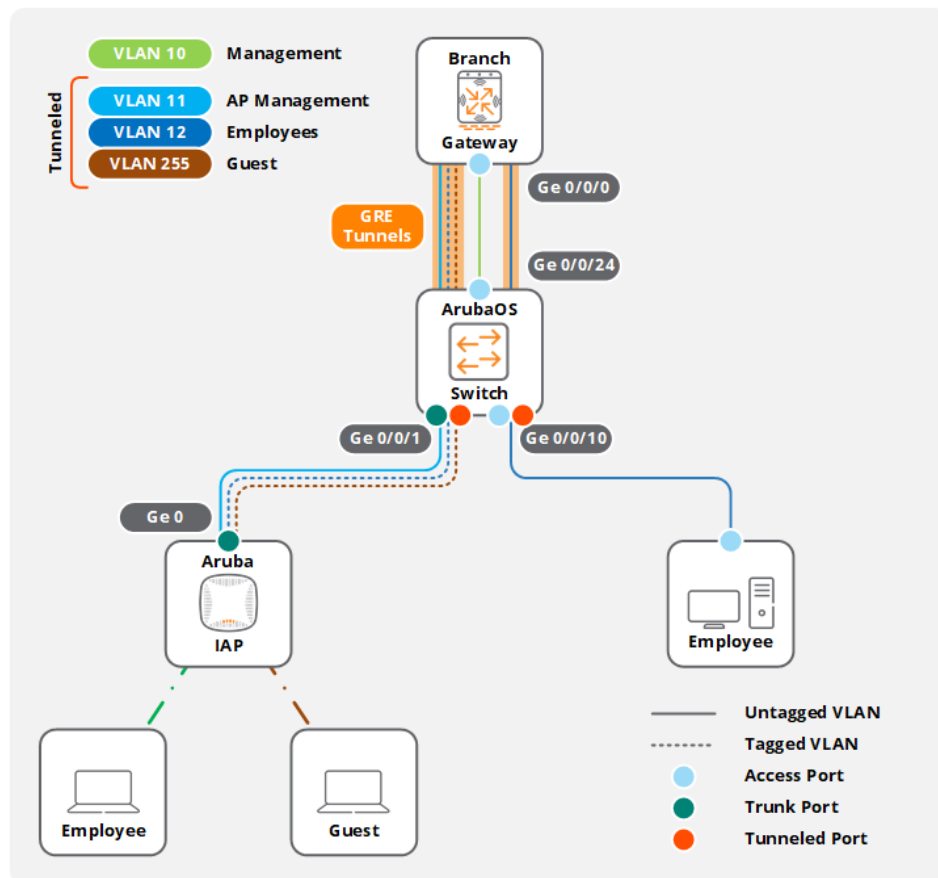


Figure 5-17 VLANs – Tunneled Ports

Appendix

Platforms and Scaling

Platform	Max VPN Tunnels	Max IKEV2 Learned Routes	Max OSPF Advertised Routes	Max WAN Compression Performance	Max Crypto Performance
7200 Series					
7210	1,024	6,000	6,000	10 Gbps	8 Gbps
7220	4,096	20,000	20,000	10 Gbps	21 Gbps
7240XM	6,144	30,000	30,000	10 Gbps	28 Gbps
7000 Series					
7010	512	3,000	3,000	2.5 Gbps	2.6 Gbps
7024	512	3,000	3,000	2.5 Gbps	2.6 Gbps
7030	512	6,000	6,000	2.5 Gbps	2.6 Gbps

Table 6-1 VPN Concentrators

Platform	Max Clients	Max Firewall Throughput	Max Active Firewall Sessions	Max Tunneled Node Ports	Max Crypto Performance
7005	1,024	2 Gbps	16,384	512	1.2 Gbps
7008	1,024	2 Gbps	16,384	512	1.2 Gbps
7010	2,048	4 Gbps	32,768	1,024	2.6 Gbps
7024	2,048	4 Gbps	32,768	1,024	2.6 Gbps
7030	4,096	8 Gbps	65,535	2,048	2.6 Gbps

Table 6-2 Branch Gateways

Protocols and Ports

Source	Destination	Protocol	Port	Usage
All Aruba Devices	*.arubanetworks.com	6	80	Cloud Firmware Upgrades
All Aruba Devices	*.arubanetworks.com	6	443	Cloud Management
BGWs / IAPs	aruba.brightcloud.com	6	443	Web Content Classification (WebCC)
BGW (WAN Interfaces)	VPNC	17	4500	IPsec Tunnels using NAT-T
BGW (WAN Interfaces)	Health Check IP/FQDN	1	-	ICMP Probes
BGW (WAN Interfaces)	Health Check IP/FQDN	17	4500	UDP Probes
BGW (WAN Interfaces)	Any	17	67-68	DHCP
BGW (WAN Interfaces)	Public DNS Server IP(s)	17	53	Domain Name System
BGW (WAN Interfaces)	Public NTP Server IP(s)/FQDN(s)	17	123	Network Time Server

Table 6-3 Mandatory Aruba Device Communications

Source	Destination	Protocol	Port	Usage
BGW (System IP)	AAA Server IP(s)	17	1812-1813	RADIUS Authentication/Accounting
AAA Server IP(s)	BGW (System IPs)	17	3799	RADIUS Change of Authorization
BGW (System IPs)	TACACS+ Server IP(s)	6	49	TACACS+ Authentication/Accounting
BGW (System IPs)	Syslog Server IP(s)	17	514	Syslog Logging
BGW (System IPs)	SNMP Server IP(s)	17	161	SNMP Agent
BGW (System IPs)	SNMP Trap Receiver IP(s)	17	162	SNMP Traps
BGW (LAN Interface)	ArubaOS-Switch	47	-	Per-Port Tunnels / Per-User Tunnels

Table 6-4 Other Aruba Device Communications (typically through VPN tunnels)