aruba
a Hewlett Packard Enterprise company

Aruba Central Managed IAP-VPN Solution for Teleworkers and Home Offices

Copyright Information

Open-Source Code

Certain Aruba products include Open-Source software code developed by third parties, including software code subject to the GNU General Public License ("GPL"), GNU Lesser General Public License ("LGPL"), or other Open Source Licenses.

The Open-Source code used can be found at this site:
http://www.arubanetworks.com/open_source

Revision History

The following table lists the revisions of this document:

Table 1 Revision History

Revision	Change Description	Revision Date
Revision 01	Initial Release	Mar, 2020
Revision 02	Added Network Recommendations section	Nov, 2020
Revision 03	Added the Terminology Change section	Mar, 2021
Revision 04	Added new security enhancements for teleworkers	Aug, 2021

aruba
a Hewlett Packard Enterprise company

www.arubanetworks.com
3333 Scott Boulevard
Santa Clara, CA 95054
Phone: 1-800-WIFI-LAN (+800-943-4526)
Fax 408.227.4550

Objectives

This document will provide an overview of the IAP-VPN architecture including Instant APs and VPN Concentrators, Data center architecture and various forwarding modes of operation. Steps for device provisioniong and IAP-VPN configuration using Aruba Central are also provided. In addition, this document also covers the security recommendations and best practices for teleworker Instant APs along with various use cases.

Table of Contents

Terminology Change

As part of advancing HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our HPE culture and moving forward, Aruba will replace racially insensitive terms and instead use the following new language:

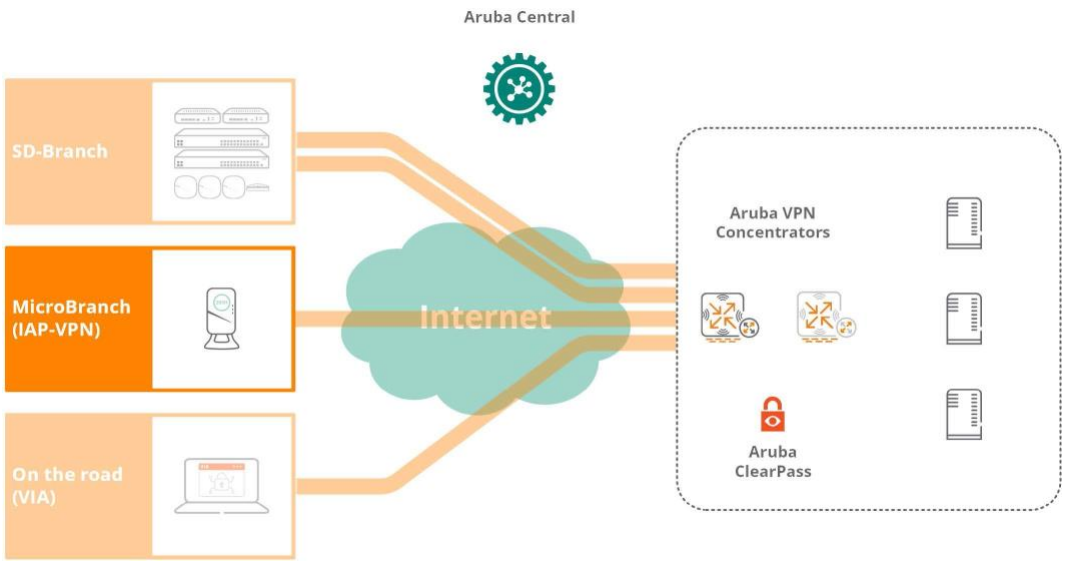
Usage	Old Language	New Language
Campus Access Points + Controllers	Master-Slave	Conductor-Member
Instant Access Points	Master-Slave	Conductor-Member
Switch Stack	Master-Slave	Conductor-Member
Wireless LAN Controller	Mobility Master	Mobility Conductor
Firewall Configuration	Blacklist, Whitelist	Denylist, Allowlist
Types of Hackers	Black Hat, White Hat	Unethical, Ethical

Solution Overview

Remote offices and teleworkers generally have a need for secure communication with the centralized corporate network. For branch offices, this secure connectivity is typically provided through solutions such as SD-WAN, where overlay networks are established over private WANs, MPLS networks or the public Internet. In contrast, remote teleworkers require the same secure connectivity to the corporate network but are limited to public Internet connectivity options. Each teleworker connects to the Internet via last-mile options based on their geographic location and service provider.

The Aruba SD-Branch solution seeks to provide a complete suite of solutions for all the needs in a distributed enterprise. From the road warrior that needs VPN connectivity to access corporate resources to the larger branches, that may need redundant gateways as well as the complete cloud-managed LAN/WLAN. This, of course, includes the case of micro-branches such as a small office or a teleworker office, where the branch network could be built with as little as a single AP using IAP-VPN technology.

Figure 1 *Aruba SD-Branch Solution*



Aruba Instant is a powerful platform which is fully capable of providing secure wireless connectivity to either remote branch offices or teleworkers.

- Branch Offices – Typically employ multiple Instant APs (IAPs) depending on the number of users and the size of the branch.
- Teleworkers – Typically employ a single IAP single per teleworker. The model of IAP is dependent on the available connectivity options.

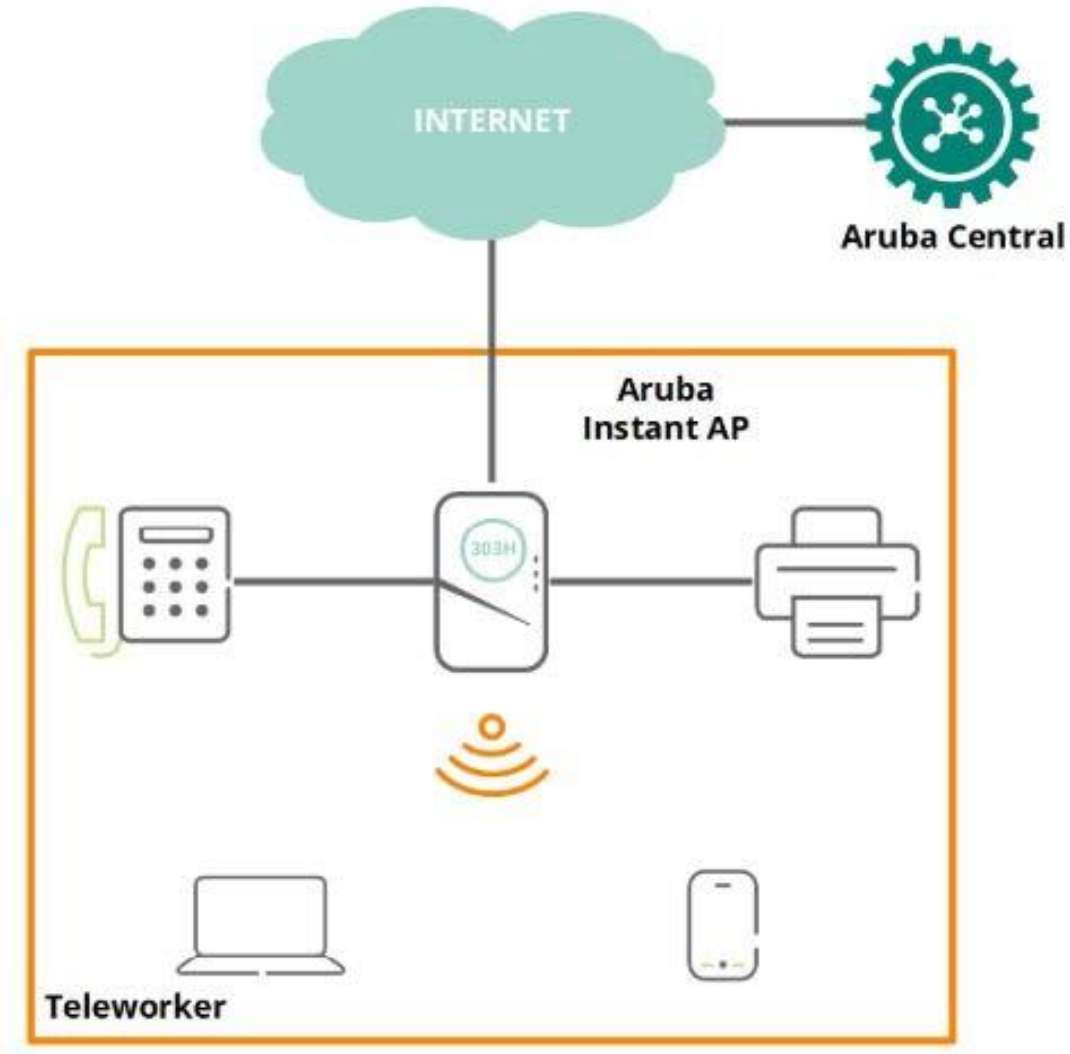
Aruba Instant is designed to alleviate the complexity associated with deploying site-to-site IPsec VPNs through native VPN capabilities and zero-touch provisioning. These attributes greatly reduce the challenges thatnormally come along with deploying IPsec VPN by reducing deployment costs and eliminating the complexity that is normally associated with traditional IPsec VPN branch or teleworker deployments. When a VPN is configured, the IAP creates a VPN tunnel over the Internet to a VPN Concentrator (VPNC) deployed in a corporate office data center. The VPNC exclusively functions as a VPN endpoint and does not supply the IAP with any configuration. Aruba Central provides all management, configuration and monitoring of both the IAPs and VPNCs.

Network Services

With an IAP VPN-based solution, enterprises can quickly and easily extend corporate network services to remote teleworkers over a secure VPN connection. Depending on the IAP model they deploy, organizations can offer employees Wi-Fi and wired connectivity options and provide the same connection experience as employees working in the corporate office.

- Wi-Fi – Provides secure authenticated access to corporate, employee and BYOD SSIDs.
- Wired – Connects desktop PCs, VoIP phones or telepresence devices. Supports MAC and 802.1X authentication.

Figure 2 *Seamless Network Services*



The types of radios and port configurations that are available differ by the model of Access Point. For deployment flexibility, Aruba offers Wi-Fi 5 and Wi-Fi 6 AP models in a variety of configurations and form factors. **While any Aruba AP can be considered, for remote teleworker deployments, the 203R, 203H, 303H, 503H and 505H models are generally preferred as these models can be easily placed on a desk and offer additional Ethernet ports.** The 203R, 303H and 505H also provide 802.3af PoE (or 802.3at PoE if E1 alone is used in 505H) to power a VoIP phone, if required. Your implementation may include a single AP model or different AP models. Both deployment options are fully supported with this solution, allowing you to deploy the AP model that works best for each teleworker's needs.

Solution Architecture

The IAP VPN tunnel architecture includes the following three components:

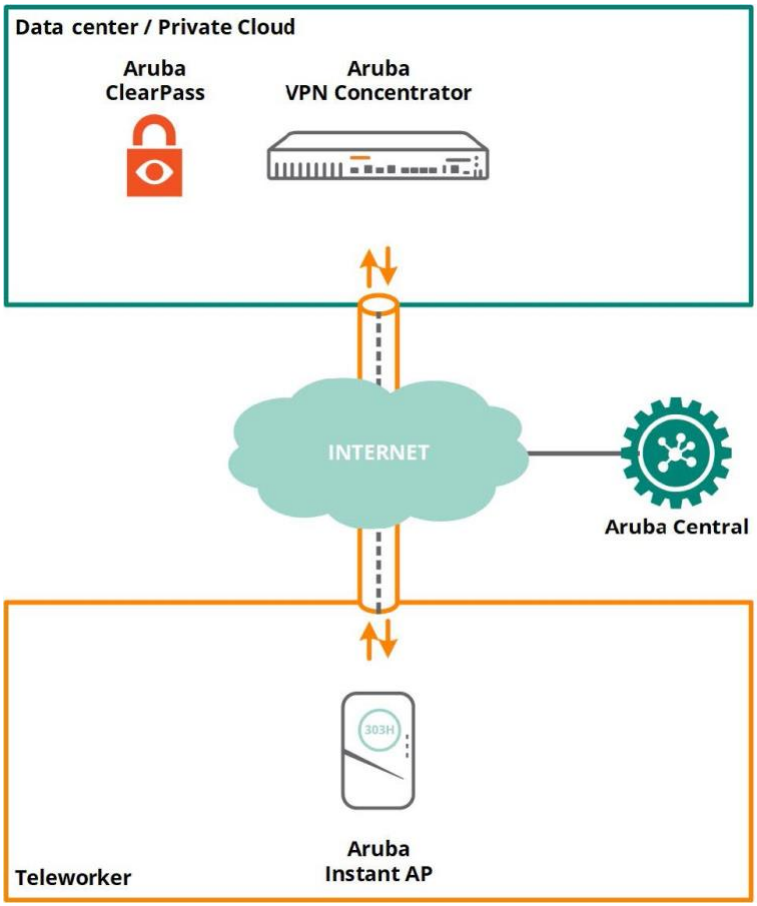
1. Aruba Central – Provides configuration, management, monitoring and insights for the solution.
2. Instant APs – For this guide, it is assumed that one IAP is deployed at each teleworker site.
3. VPN Concentrators – One or more VPNCs are deployed in data centers.

NOTE: Data center deployment options are captured in a later section

The IAP at the teleworker site serves as the VPN endpoint, and the gateway located in the datacenter serves as the VPN concentrator. When an IAP is set up for a VPN, it forms an IPsec tunnel to a gateway in the data center to secure sensitive corporate data.

IPsec authentication and authorization between the VPNC and the IAP is based on a allowlist configured in Aruba Central. From the VPNCs perspective, the IAPs that form the VPN tunnels are considered VPN clients. The VPNCs purpose in this scenario is to terminate VPN tunnels as well as route or switch VPN traffic into the data center. The IAP creates an IPsec or GRE VPN tunnel from the remote site to the VPNC. The VPNC only acts as an IPsec or GRE VPN endpoint. It does not provide any configuration or management for the IAP. The figure below provides a visual depiction of the IAP VPN tunnel architecture:

Figure 3 *IAM Solution Architecture*



Forwarding Modes

Instant APs support four forwarding modes to accommodate various branch use-cases. Each forwarding mode determines whether the DHCP server and default gateway for the clients reside in the branch or in the data center. (These modes do not determine the firewall processing or traffic forwarding functionality.) The IAP enables different DHCP pools (various assignment modes) and allocate IP subnets for each branch. The VPNC allows different traffic forwarding modes from clients on a VLAN based on the DHCP scope configured on the Instant AP.

For the remote teleworker solution, Aruba recommends the centralized Layer 2 or distributed Layer 3 forwarding modes. Both of these forwarding options are simple to deploy, easy to manage, and securely extend the corporate IP network to the remote teleworker clients. Unlike other remote access solutions that rely on NAT translation, the remote teleworker devices are assigned an IP address from the corporate network. This provides several benefits:

- IT staff can apply policies in the data center to determine which applications teleworkers can access the same way as if they are in the office.
- IT teams can provide support for remote teleworkers by permitting remote access into managed assets.
- Real-time voice and video communications are permitted over the VPN network

NOTE: Data center deployment options are captured in a later section. A full description of each forwarding mode is captured in the Aruba Instant Validated Reference Design v2.0 guide. While the local, distributed Layer 2 and centralized Layer 3 modes are valid for remote teleworker deployments, the centralized Layer 2 and distributed Layer 3 forwarding modes are the most commonly deployed

Centralized Layer 2

Centralized Layer 2 forwarding extends the corporate VLAN or broadcast domain to remote teleworkers. The DHCP server and default gateway for the remote clients reside in the datacenter. Depending on the datacenter architecture, either the VPNC or an upstream router acts as the gateway for clients. DHCP services are provided by the existing corporate DHCP / IP Address Management (IPAM) system.

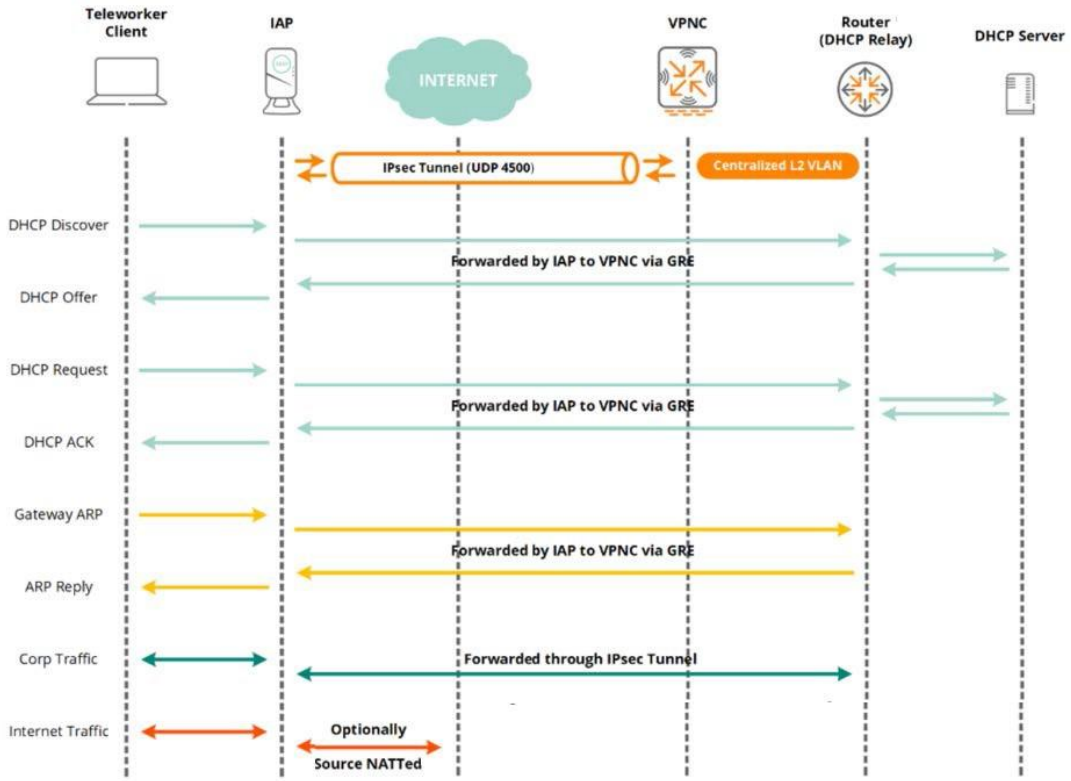
A centralized Layer 2 deployment offers two options for forwarding remote teleworker traffic:

- **Full-Tunnel Mode** – All traffic is forwarded by the IAP through the IPsec tunnel to the default gateway in the data center. This option is typically selected by organizations that prefer to exercise more control over traffic by having it forwarded to the datacenter for additional inspection.
- **Split-Tunnel** – All corporate traffic is forwarded by the IAP through the IPsec tunnel to the default gateway in the data center while Internet traffic is NAT translated and forwarded locally. This option is preferred by organizations that utilize cloud hosted applications thus offloading overhead from the corporate network or where full control / inspection over Internet traffic is less of a concern.

Deciding which mode to implement will primarily depend on your organizations security policy. It is important to note that these forwarding options are defined per Centralized L2 DHCP scope / VLAN in Central. This allows the forwarding behavior to be assigned on a per-client basis based on VLAN assignments from AAA. This provides full flexibility by allowing administrators to require full-tunnel mode for some client devices while permitting split-tunneling for others. The IAP provides deep packet inspection and full control as to which teleworker traffic is permitted or denied for each path, regardless of which forwarding mode is selected.

An overview of the centralized Layer 2 forwarding architecture is provided in the figure below. Centralized Layer 2 forwarding is the simplest forwarding option to implement as the corporate subnet resides in the datacenter. No routing is performed between the IAP and VPNC, however the inner-IP and centralized Layer 2 subnets are typically advertised by the datacenter router into the datacenter using OSPFv2 or BGP4. Static routing is also an option for smaller environments. All teleworker traffic is encapsulated in GRE inside an IPsec tunnel to the datacenter. The VLAN, IP subnet, DHCP server and default gateway all reside in the datacenter.

Figure 4 ***Centralized Layer 2 Forwarding Mode***



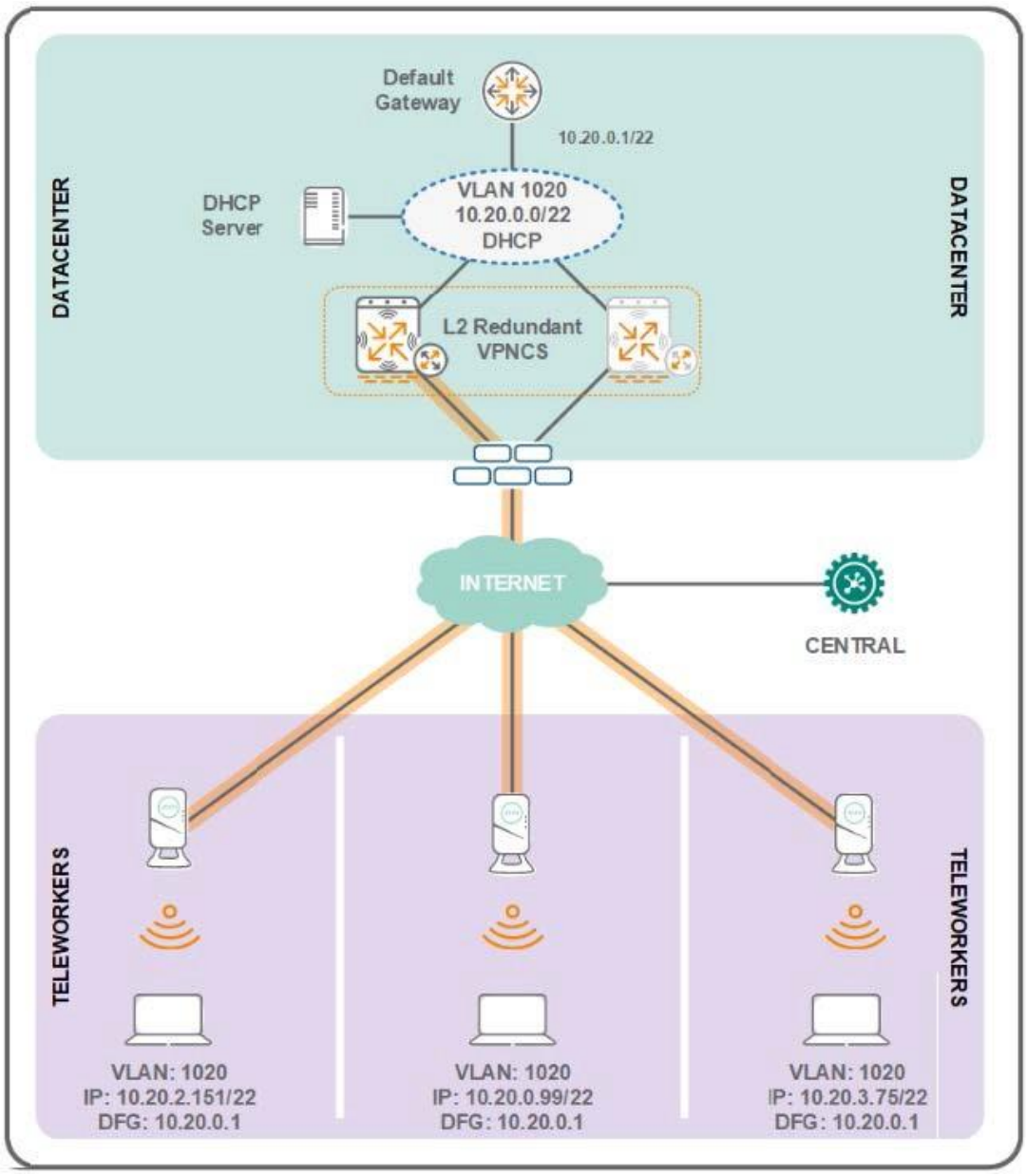
Use Case Example

You're required to support 256 remote teleworkers with up to three client devices per site (768 total clients). To accommodate the immediate requirements and provide room for growth:

1. A centralized VLAN 1020 has been defined in the data center with the subnet 10.20.0.0/22. It will accommodate up to 1,000 client devices.
2. A DHCP scope is configured on the DHCP server with the appropriate DHCP options.
3. A Centralized Layer 2 DHCP scope is created in the AP Group in Central that defines the VLAN ID and optionally enables split-tunneling.
4. The Centralized Layer 2 DHCP scope is assigned to WLAN and if required wired port profiles.

An example topology and address allocation is provided in the following figure:

Figure 5 *Centralized Layer 2 Deployment*



Distributed Layer 3

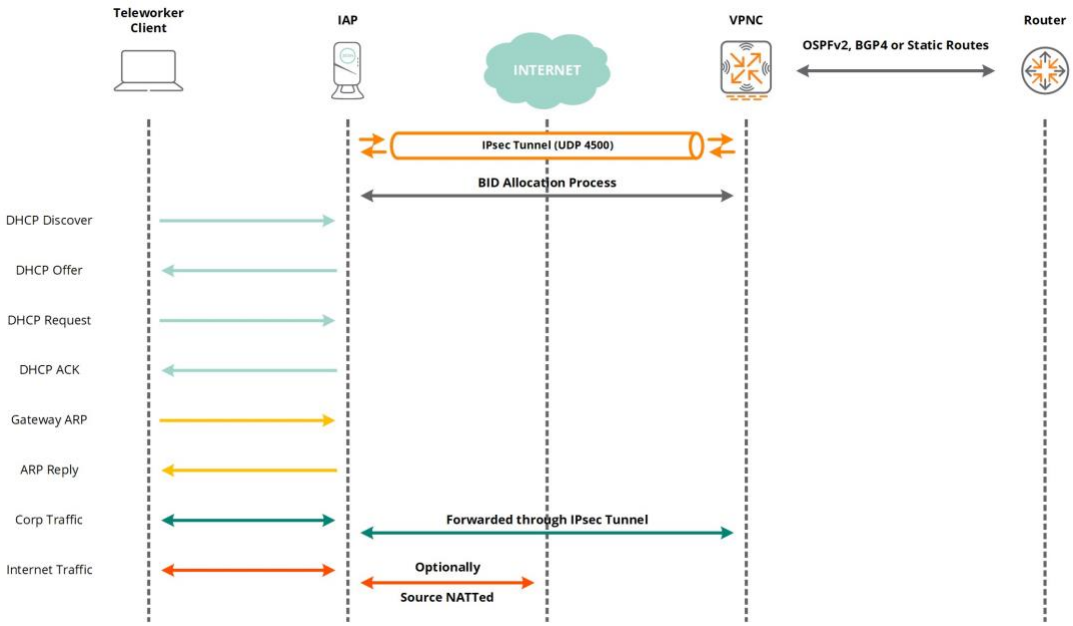
Distributed Layer 3 forwarding differs from centralized Layer 2 forwarding by assigning a dedicated subnet for each teleworker site which is used by clients. However, unlike traditional branch deployment which often requires manual subnet assignments for each site, this process is fully automated. This is achieved by establishing a main subnet for all the teleworkers upon which smaller subnets are sub-allocated to each IAP. Enabling automation in this manner eliminates the cost and the complexity associated with a classic site- to-site VPN routed deployment.

With Distributed Layer 3 forwarding, the IAP manages the dedicated subnet in addition to serving as the DHCP server and default gateway for clients. Client traffic destined for datacenter resources is routed to the VPNC through the IPsec tunnel, which then routes the traffic to the appropriate corporate destination. When an IAP registers with the VPNC a route is automatically added to enable the routing of traffic from the corporate network to clients on the

local subnet of the branch. The routes from each teleworker site are redistributed into the datacenter using OSPFV2 and BGP4. Static routing is also supported for smaller deployments.

Any traffic destined for the Internet or a local destination is source NATed using the local IP address of the IAP and locally bridged. The WLAN controller in the datacenter is aware of the Layer 3 subnet at each branch and can redistribute these routes to upstream datacenter routers using OSPFv2 or BGP4. All client traffic can be forwarded through the IPsec tunnel or bridged locally if required.

Figure 6 *Distributed L3 Forwarding Mode*



One important aspect of a Distributed Layer 3 deployment model is subnet allocation. Each IAP is allocated with a small pool of addresses from a main subnet that is defined in Aruba Central. The main subnet is scoped based on the number of IAPs and addresses that need to be supported.

Table 2: *Distributed L3 Pool Examples*

Number of IAPs	Example IP Range	Required Clients per Branch	Resulting IAP Subnet Size	Available Addresses per IAP
128	10.200.0.0 – 10.200.1.255 (/23)	1	/30	2
256	10.200.0.0 – 10.200.7.255 (/21)	2	/29	6
512	10.200.0.0 – 10.200.15.255 (/20)	3	/29	6

Each subnet is assigned to IAPs on a first come first serve basis using the BID process. Once a subnet has been allocated to an IAP, it is persistent. Once a pool has been registered, it is added as a route in the VPNC which can be redistributed into the datacenter using OSPFv2 or BGP4 for reachability. Route costs are utilized when multiple datacenters and VPNCs are deployed.

> **NOTE:** Subnet allocation follows standard CIDR allocation rules. When entering the number of clients for each branch, Central will add an additional IP for the IAP. For example, entering 6 will results in a /28 subnet being allocated, as 7 addresses are required and this cannot be satisfied with a /29 subnet.

NOTE: DHCP options can be configured with the Distributed L3 forwarding mode to support VoIP phone, if required.

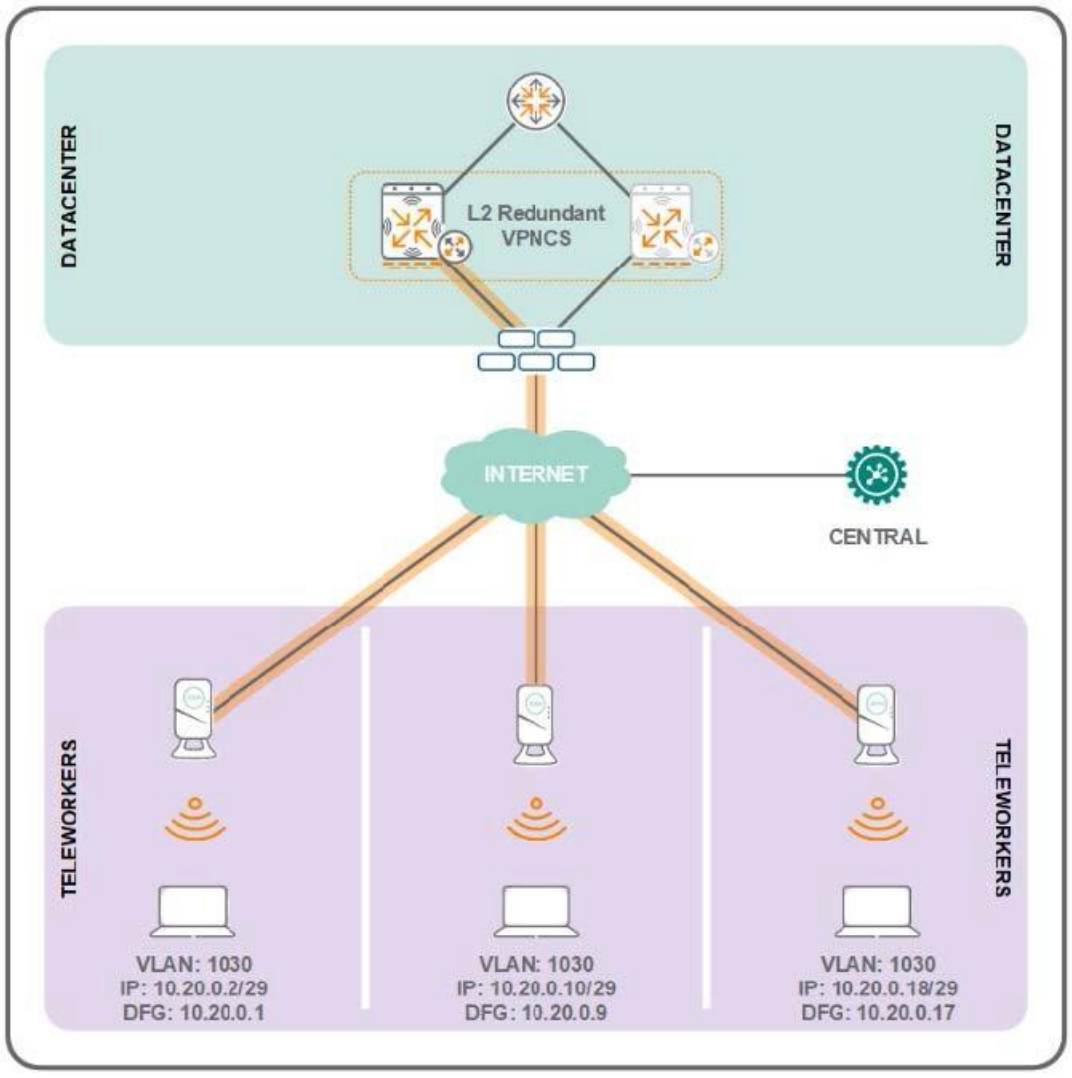
Use Case Example

This example requires support for 200 remote teleworkers with up to four client devices per site. To accommodate the immediate requirements and provide room for growth:

- A distributed Layer 3 Layer 2 DHCP scope is created in the AP Group to allocate a /29 subnet per branch:
  - VLAN ID: 1020
  - IP Range: 10.20.0.0 – 10.20.7.255 (/21)
  - Clients per branch: 4
- The distributed Layer 3 scope is assigned to the WLAN (and wired port profiles, if required).

An example topology and resulting subnet allocation is provided in the following figure:

Figure 7 *Distributed Layer 3 Deployment Example*

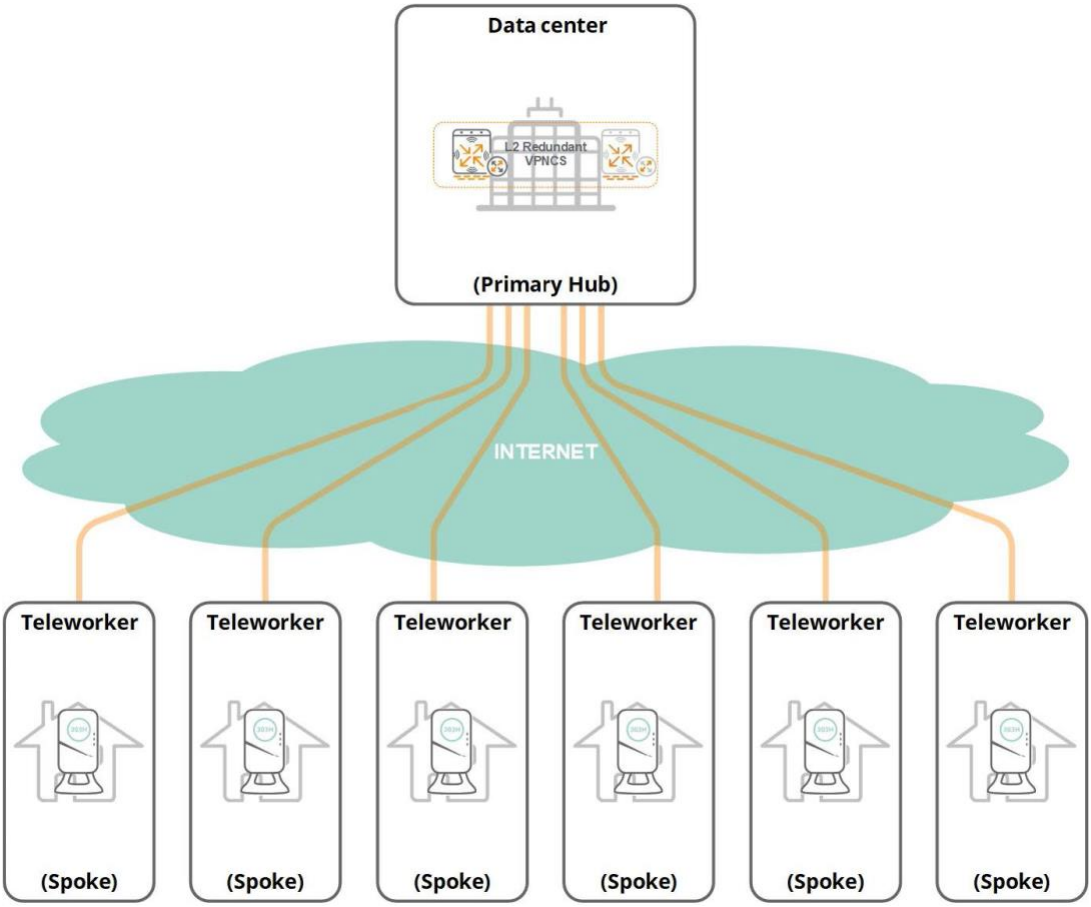


Data Center Architectures

With the IAP VPN solution, VPN tunnels are established from the IAPs to VPNCs to create an overlay network. This overlay network is used to securely transport traffic forwarded between the teleworkers and data centers. Data centers typically consist of corporate headquarters or computer rooms that include one or more VPN Concentrators. Larger organizations may include additional data centers that provide additional layers of redundancy in the event of any primary data center failures.

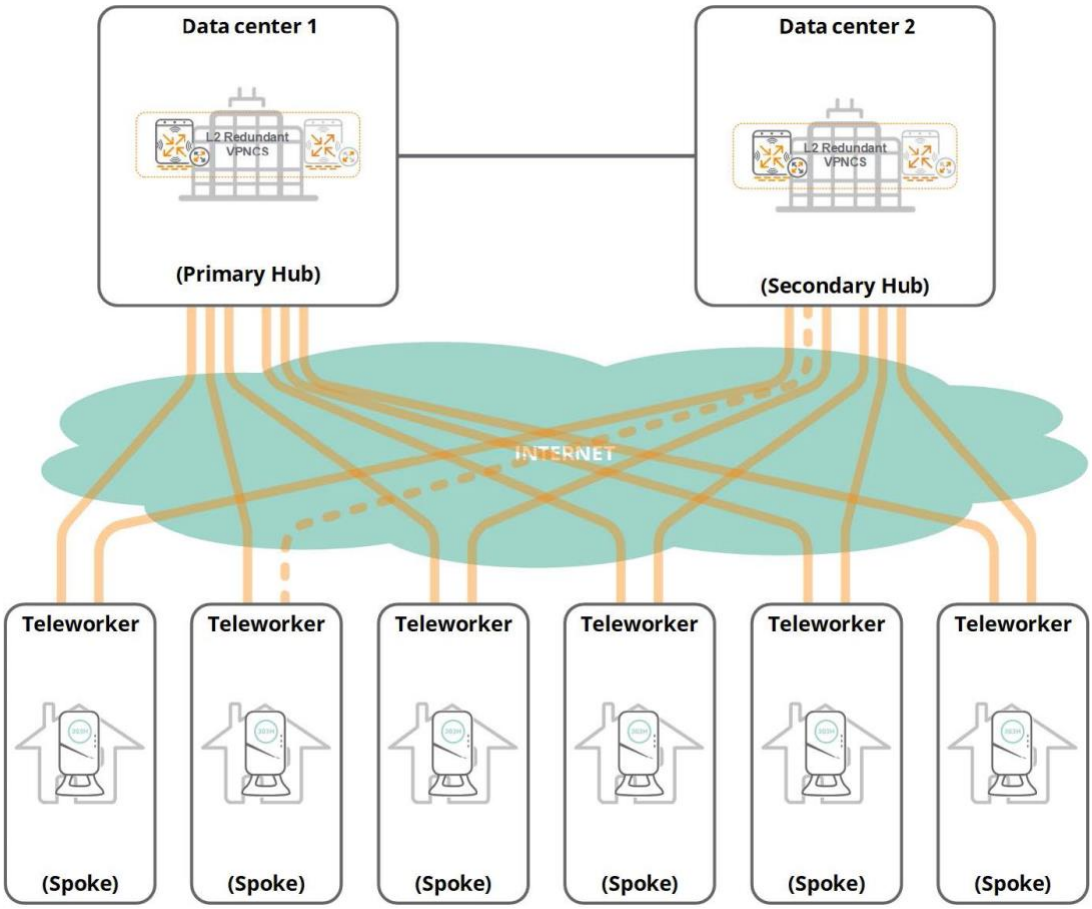
The Aruba IAP VPN solution supports a hub-and-spoke architecture where the VPN tunnels are established between IAPs (spokes) and VPNCs (hubs). All IAP VPN deployments include at least one hub site, with one or more VPNCs installed, that terminates IPsec based VPN tunnels initiated from the IAPs installed at the teleworkers homes. The number of VPNCs that are deployed in each hub site depend upon the size and redundancy needs of the deployment. The most basic IAP VPN deployment consists of one VPNC installed at a hub site that services all the IAPs. An optional layer 2 redundancy is provided by installing a second VPNC at the hub site.

Figure 8 *Single Data Center*



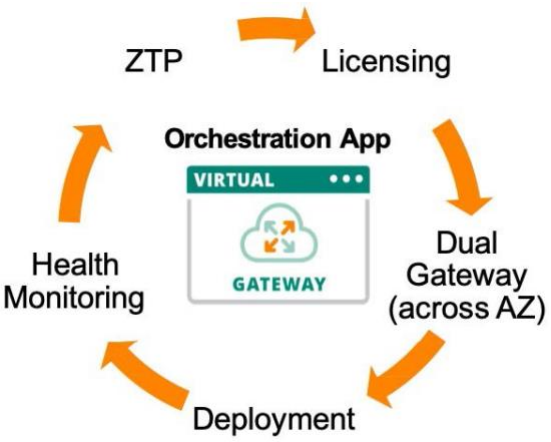
Larger IAP VPN deployments often include a secondary hub site providing additional failover and recovery in the event of a primary hub failure. The most typical deployments consist of a primary and secondary hub each with standalone or layer 2 redundant VPNCs.

Figure 9 *Dual Data Centers*



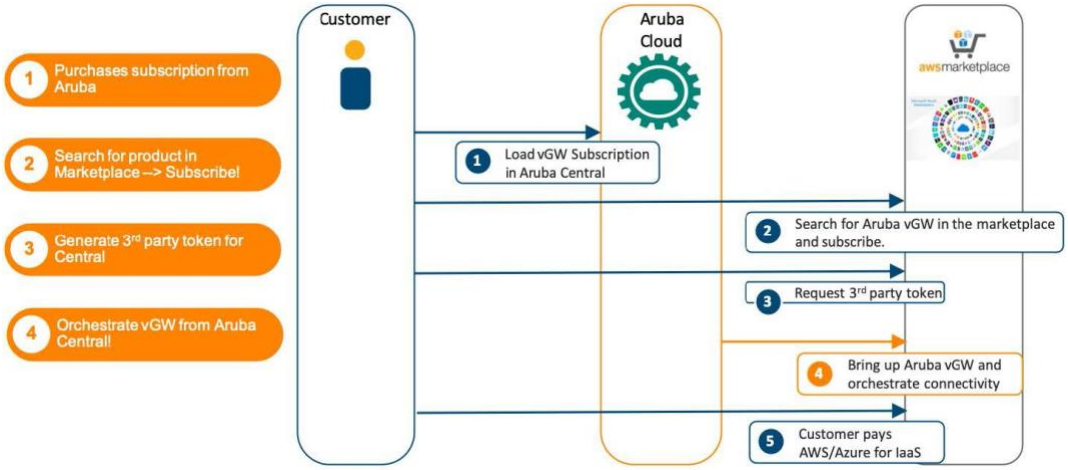
Finally, the Aruba Micro-Branch Solution can also leverage Headend Gateways (or VPN Concentrators) in Public Cloud environments such as AWS or Azure. In such environments, Aruba Central can handle the full life cycle of the Aruba Virtual Gateways (Aruba VPNCs in AWS or Azure): from the initial bring up and provisioning through the regular management (as if it were another VPNC in the network), and to even handle failover in HA scenarios.

Figure 10 *Functions Performed by the Virtual Gateway Orchestration Application*



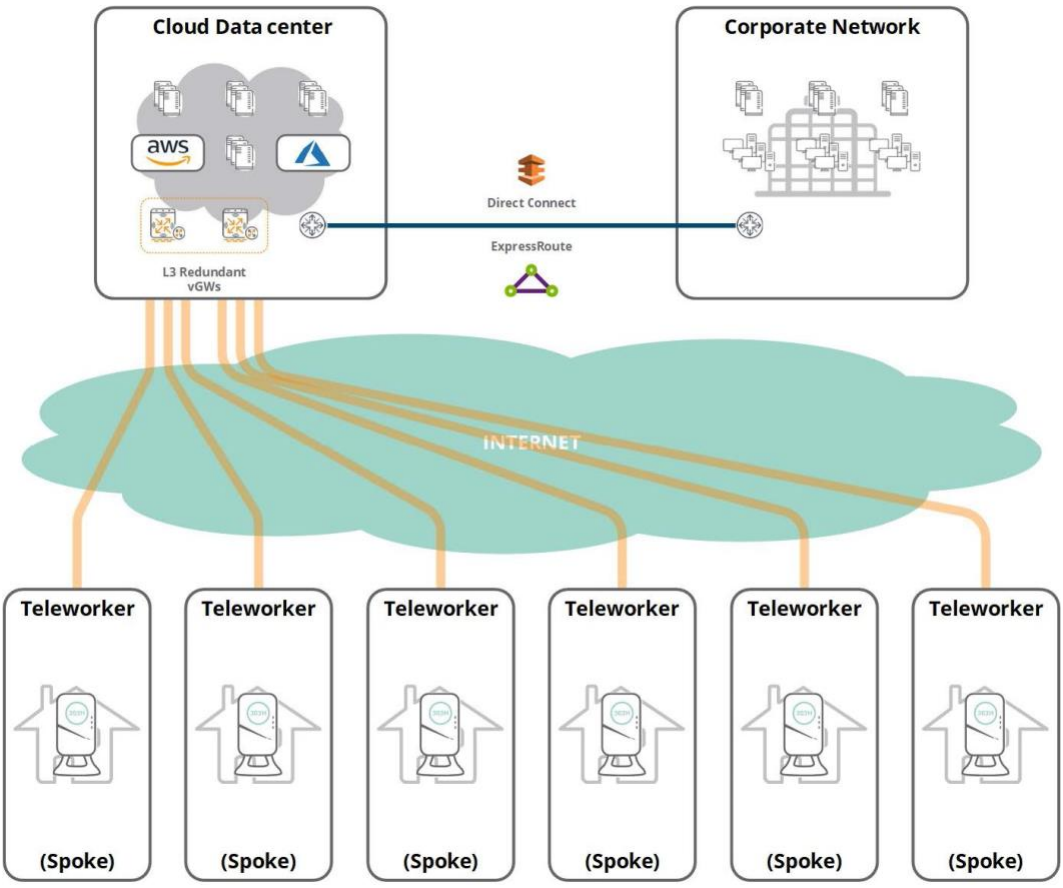
In this process, Aruba Central connects to the customer AWS or Azure account to have visibility over it and provision the VM together with the necessary interfaces, subnets, elastic-IP mappings, and so on. This provides an accelerated mechanism to enable connectivity, as no hardware needs to be installed in the Data Center and all actions can be performed through APIs connecting from Aruba Central to AWS or Azure.

Figure 11 *Aruba Virtual Gateway Provisioning*



In summary, Aruba Virtual Gateways would behave like Aruba VPNCs deployed in the customer's Public Cloud.

Figure 12 *Public Cloud*

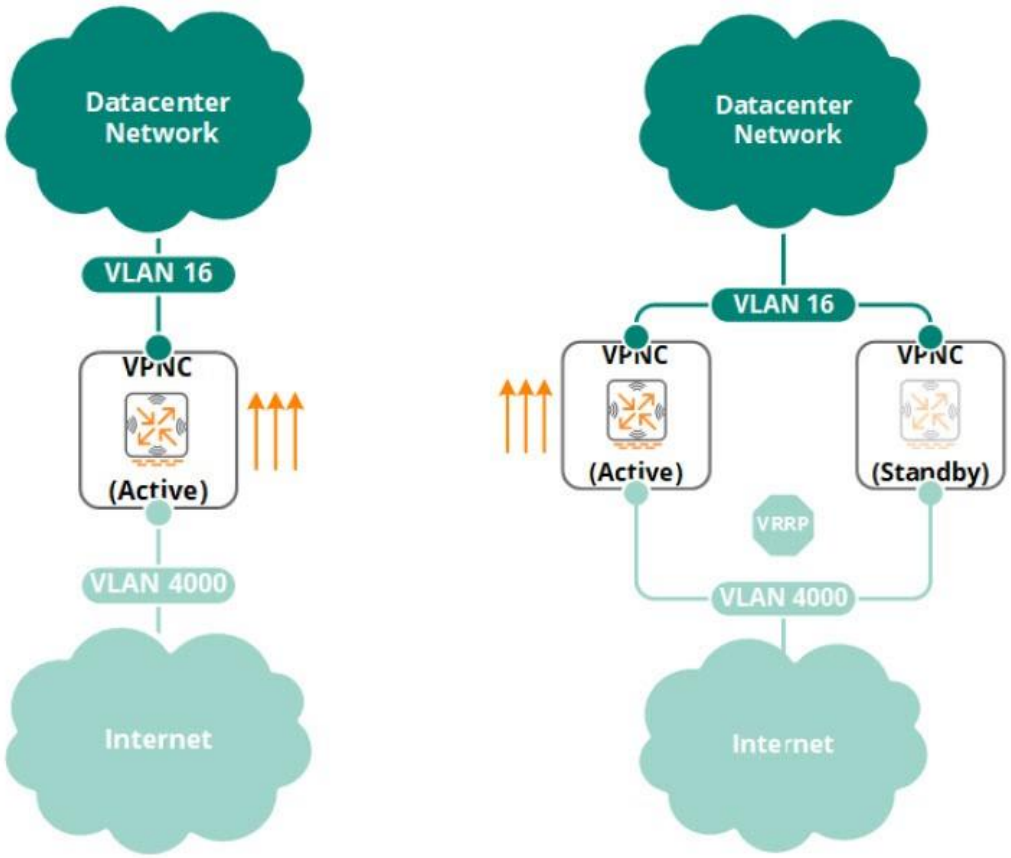


NOTE: Additional details on Virtual Gateway Orchestration and Public Cloud integration can be found in Tech Notes as well as the Aruba Central documentation.

L2 Redundancy

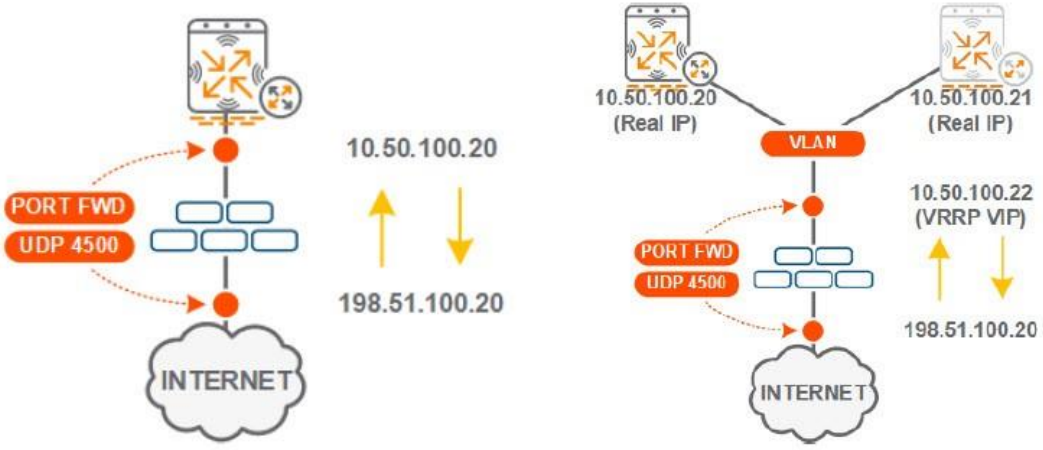
Each hub site can consist of a standalone VPNC or a Layer 2 redundant pair of VPNCs. When Layer 2 redundancy is enabled, one VPNC operates in an active role and the second VPNC operates in a standby role. The standby VPNC only assumes an active role in the event of an active VPNC failure. Failover is provided using the Virtual Router Redundancy Protocol (VRRP) where the active VPNC is assigned the highest VRRP priority. It is important to note that the standby VPNC does not terminate any VPN tunnels or advertise branch routes through OSPFv2 or BGP4 until it transitions to an active state. If an L2 failover occurs, all the VPN tunnels from the teleworker IAPs are torn down and re-established to the standby VPNC (typically, 20 to 30 tunnels per second).

Figure 13 *VPNC Redundancy Examples—Standalone VPNC and L2 Redunandant VPNC*



When L2 redundant VPNCs are deployed, the VPN tunnels from the IAPs are terminated on the VRRP virtual IP rather than the real IP of the VPNC that is the VRRP master. (The VNPC that is the VRRP master terminates the VPN tunnels and forwards the traffic during normal operation.) As most VPNCs are deployed behind an Internet edge firewall, a port-forwarding rule is configured to permit UDP4500 traffic from an outside public IP address to the VRRP virtual IP.

Figure 14 *Examples of Port Forwarding—Standalone VPNC and L2 Redundant VPNC*



L3 Redundancy

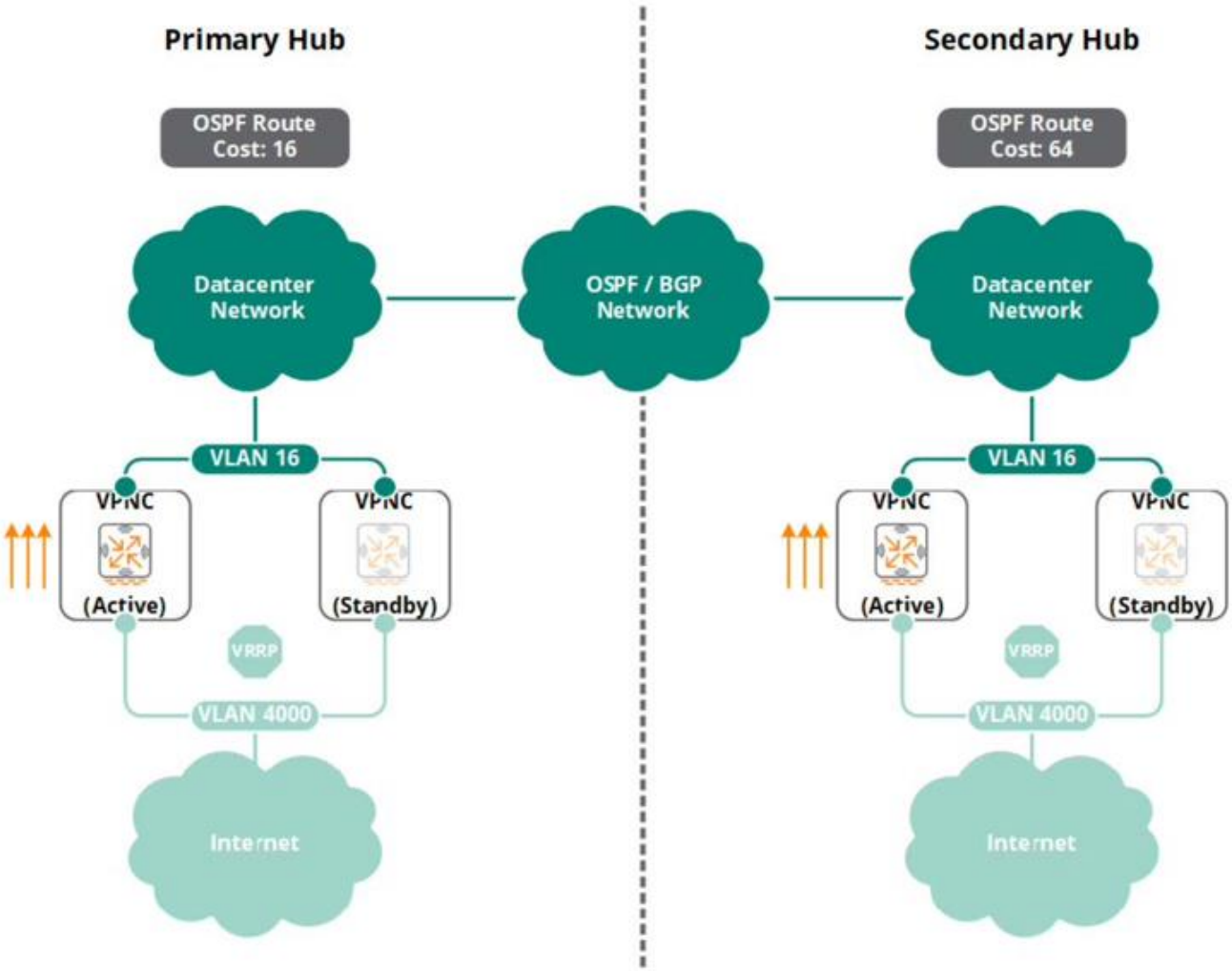
Larger IAP VPN deployments may include a secondary hub site for additional failover and recovery. The secondary hub site can include a standalone or L2 redundant pair of VPNCs as required. This deployment model is often referred to as Layer 3 redundancy since OSPFv2 or BGP4 route costs in the corporate network are used to determine which hub site is actively forwarding traffic to the teleworker sites.

In an L3 redundancy deployment, each IAP has a VPN tunnel established to the primary and secondary hub sites. The VPNCs in each hub are configured with route policies that redistribute the teleworker subnets into the datacenter network via OSPFv2 or BGP4 at different route costs. The hub that advertises the teleworker routes at the lowest cost being the preferred path.

> **NOTE:** In this model, it is important to note that while the IAPs establish active VPN tunnels to both hubs, only one hub is actively forwarding traffic for the IAPs at any given time. The ability to simultaneously forward traffic to both hubs at the same time is not supported with the IAP VPN.

Each hub is therefore assigned a primary or secondary role. The designated VPNCs in each hub advertise the branch routes into OSPFv2 or BGP4 at different route costs. The VPNCs in the primary hub advertise 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 (Figure X). If the primary hub fails or becomes unreachable, the VPN tunnels are already established to the secondary hub site. During a failover, the OSPF/BGP routers will re-converge so that the teleworker routes are reachable via the secondary hub with a typical re-convergence occurring in under 1 minute (depending on the IGP configuration).

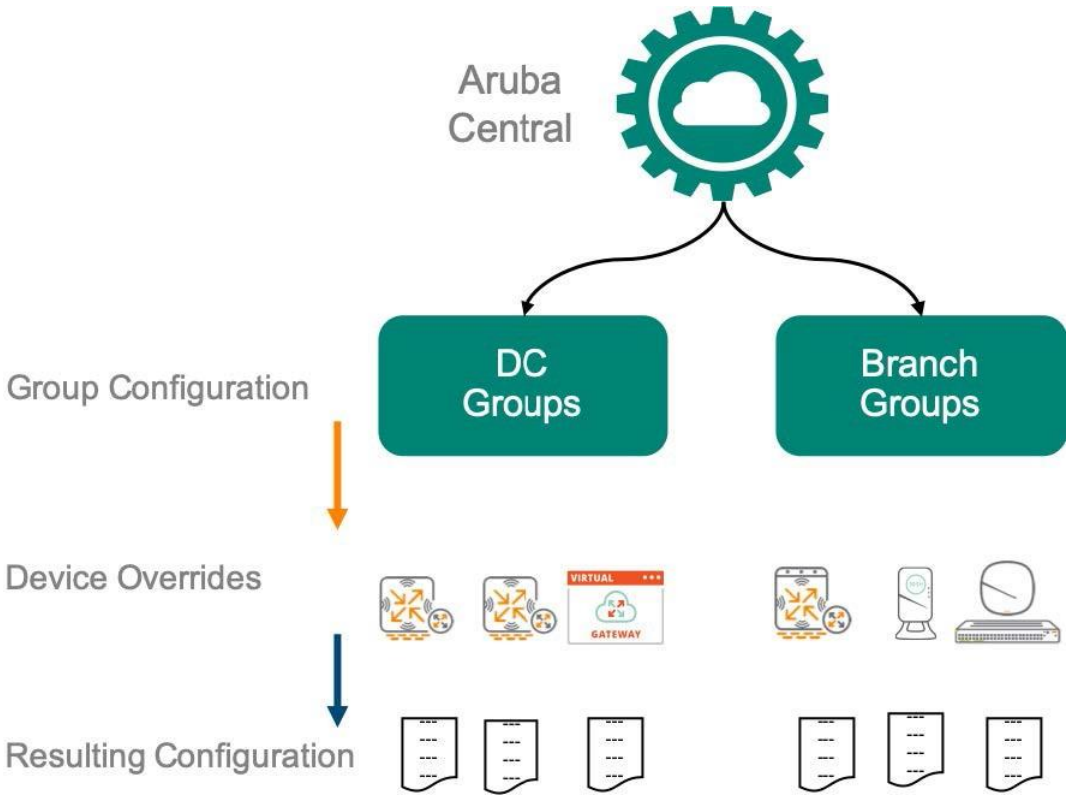
Figure 15 *Layer 3 Failover*



Configuration in Aruba Central

Aruba Central uses a hierarchical configuration model where configurations applied at the group level filter down to all the devices in the group. Specific overrides, like hostnames, IP addresses or specific routing configurations are generally overridden at the device level.

Figure 16 *Central Configuration Hierarchy*



For a micro-branch environment, Aruba recommends having different groups for each data center site and for each type of branch site. Different branch types or geographical locations with different RF regulations also have their own recommendations.

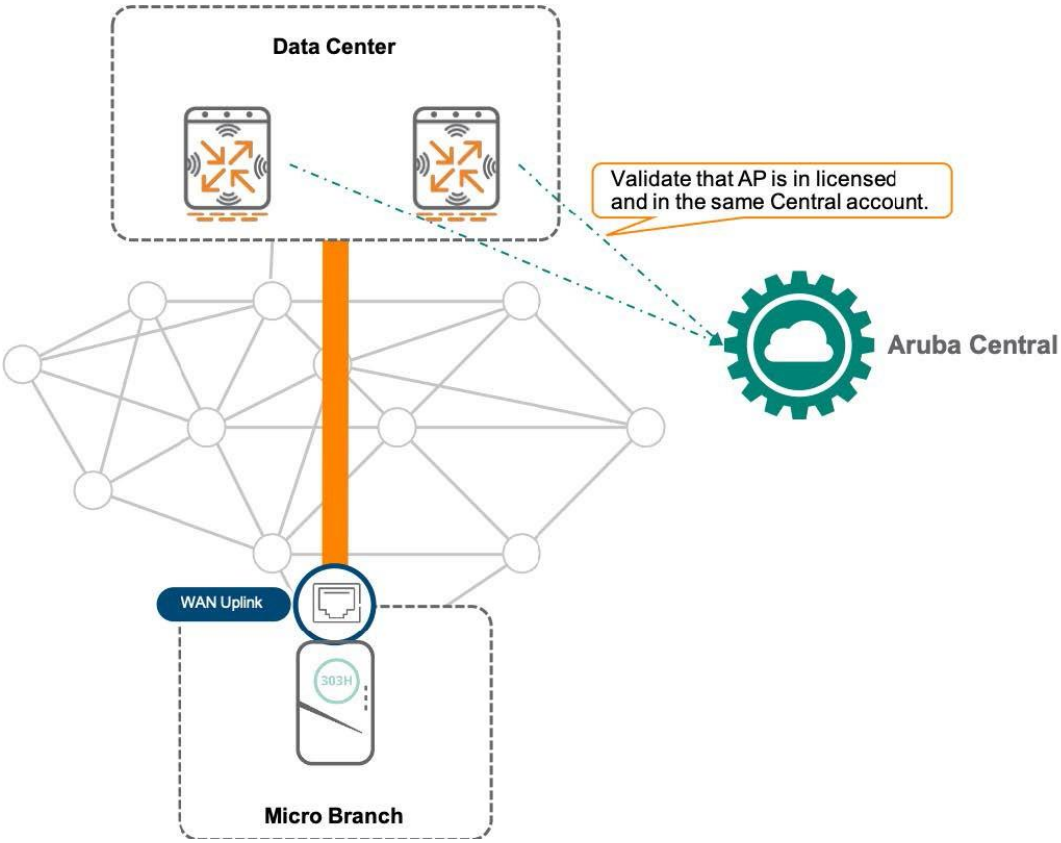
Headend Gateway Configuration

The configuration of Aruba Headend Gateways, also referred to as VPN Concentrators (VPNCs), to terminate micro-branch tunnels consists of three elements: authentication, dynamic IP assignment, and route redistribution.

Authentication

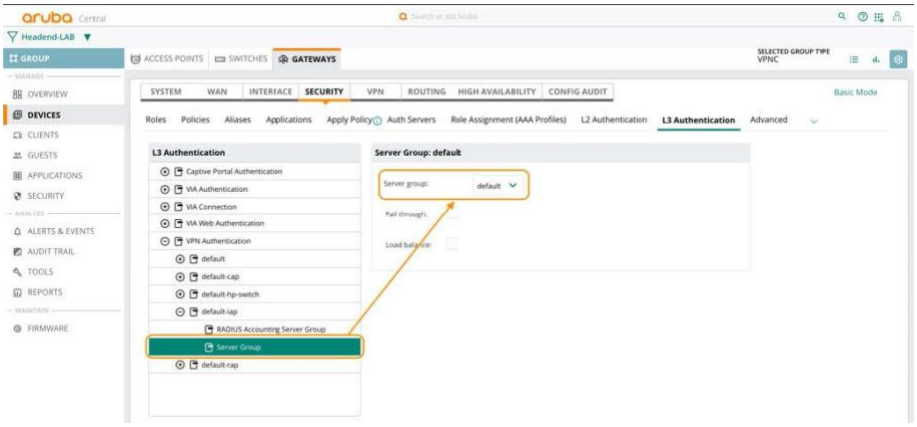
Aruba APs identify themselves using their factory TPM certificate, which has the device's MAC address as the CN. The first step in authentication is to have VPNC accept incoming connection from the IAPs. When both the Headend Gateway and the AP are managed by the same Central account, allowlisting happens automatically. Upon receiving the connection request, the VPNC validates with Central that the AP is licensed and in the same Central account.

Figure 17 *Tunnel Authentication*



To configure, validate that the VPNC group is using the default setup to authenticate IAP-VPN tunnels. This is the default configuration and typically does not require any changes. For verification, the settings can be found under **Headend > Devices > Gateways > Security > L3 Authentication > VPN Authentication > default-iap > Server Group.**

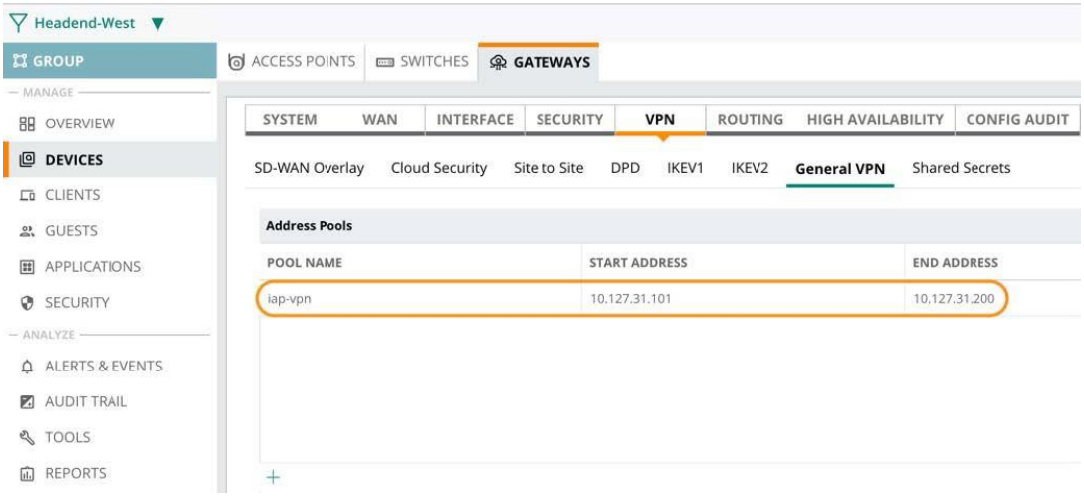
Figure 18 *IAP Tunnel Allowlisting*



Dynamic IP Assignment

When connecting to the VPNC, APs behave like dynamic VPN clients. This means that they are assigned a pool of Inner IP addresses, which can be configured in **Headend > Devices > Gateways> VPN > General VPN.**

Figure 19 *Inner IP Pool Configuration*



This pool of IP addresses is used by IAPs and client devices in source-NATed subnets in the IAPs to reach the rest of the network. Therefore, the pool of IP addresses should be routable.

Figure 20 *Inner IP Address Allocation*

The inner IP pool is advertised to the rest of the network as branch subnets are advertised. Aruba recommends setting the same IP pools in all VPNCs and leveraging routing costs to ensure that the primary VPNCs advertise these subnets with higher priority.

> **NOTE:** For IAPs using ArubaOS version prior to 8.4, make sure you check the IAP-VPN Backwards compatible box.

Route Redistribution

The Aruba Micro-Branch architecture can work in layer 2 (L2) mode, where VLANs are L2 extended from the APs to the VPNC, or in layer 3 (L3) mode, where branch subnets are advertised upstream as part of the tunnel negotiation. When working in L3 mode, branch subnets should be redistributed into a dynamic routing protocol. Use the following methods to redistribute branch subnets into a dynamic routing protocol:

OSPF:

1. Enable OSPF and set the area to be used with the upstream router.
2. Enable the interface VLANs to be used in the OSPF process.
3. Redistribute IAP-VPN overlay routes into OSPF.

BGP:

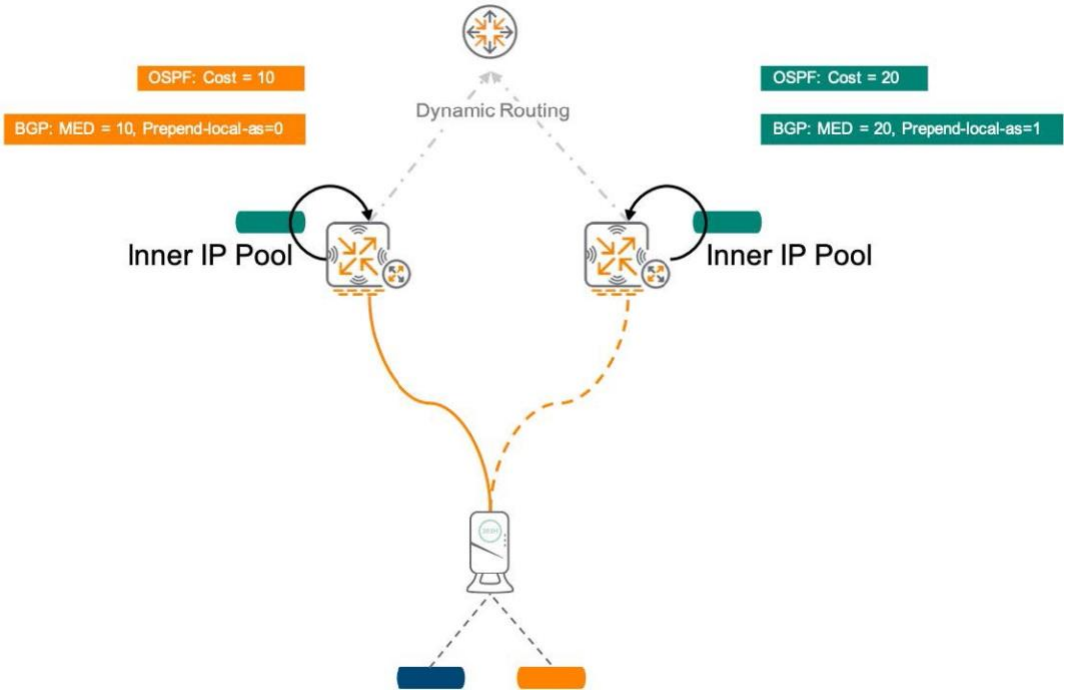
1. Enable BGP globally and set the AS number.
2. Create the necessary BGP neighbors.

3. Redistrube IAP-VPN overlay routes into BGP

NOTE: ArubaOS follows RFC1812, which describes that in the absence of a route map, no routes should be learned from a neighboring eBGP router.

In order to maintain traffic symmetry, ensure that routes are redistributed with a higher cost from the active VPNC than from the backup. The following figure shows an example of this route redistribution:

Figure 21 *Route Redistribution Example*



Micro-Branch Group Configuration

The Aruba Micro-Branch solution is designed to have a scalable configuration scheme. All configurations should be applied at the group level, with the exception of the AP hostnames, which can be handled as part of the provisioning process. Once APs are the right group, they are configured from the **Micro-Branch > Devices > Access Points** configuration page.

Tunnel Establishment

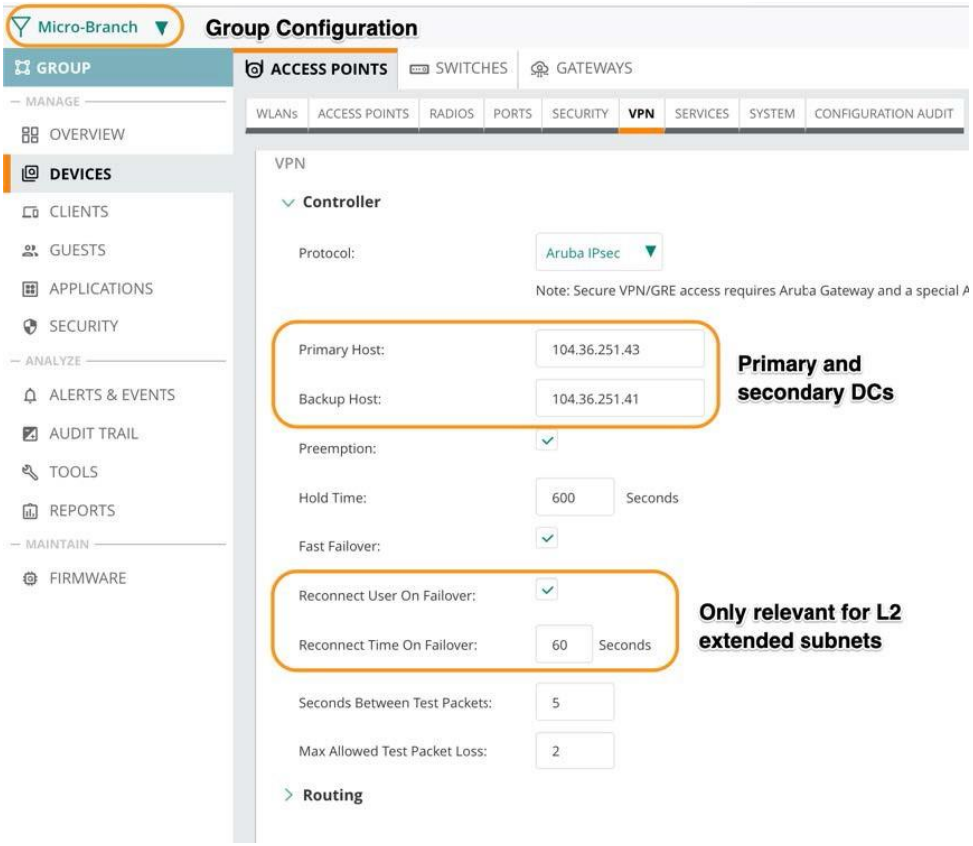
Access points bring up tunnels to the VPNCs using their TPM as authentication to automate them. The configurations are done in **Micro-Branch > Devices > Access Points > Configuration > VPN**. The following are some reference configurations:

Protocol: Aruba IPSec.

- Set the primary and secondary hosts (these should be the Outer IPs of the VPNCs).
- Preemption enabled with the default hold time of 600 seconds.

- Fast failover enabled, resulting in having tunnels to both VPNCs preemptively established.
- Reconnect user on failover with a reconnect time of 60 seconds. In the case of an L2 extension, this disconnects all WLAN users from the network to ensure that they get an IP from the subnet in the secondary DC.

Figure 22 *Tunnel Configuration*



Once the tunnels are established, either L2 VLAN extension or L3 routing can be selected based on each VLAN.

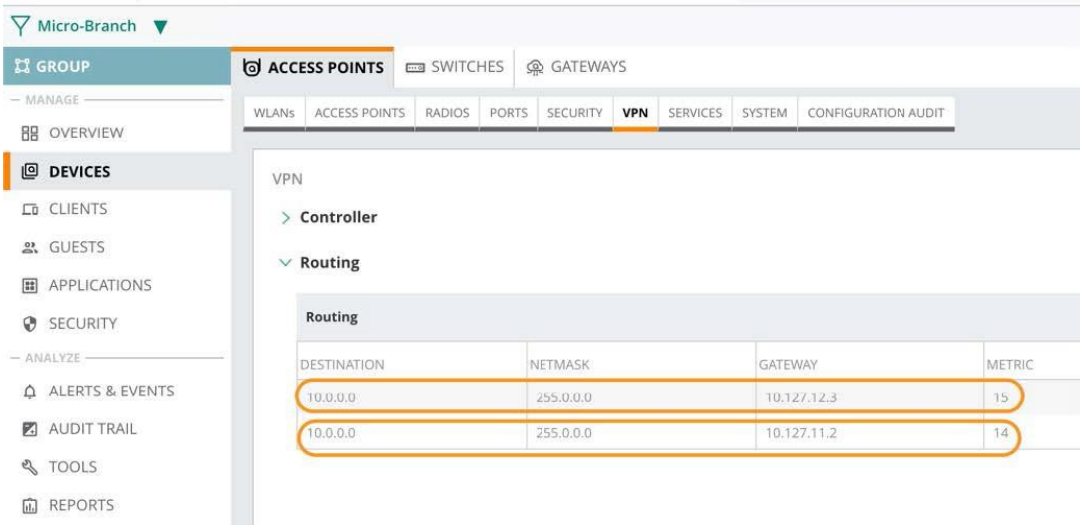
Routing

An AP acting as a Micro-Branch can forward traffic through the tunnel or source-NAT it through its default gateway. The destinations for which traffic should be tunneled can be selected in **Micro-Branch > Devices > Access Points > VPN > Routing**. Keep the following in mind when setting the routes:

- Routes pointing to the tunnels should point to the physical IP of the VPNCs, not the Outer IP NATted by the firewall. In case there is a pair of VPNC with VRRP enable, point routes with different metrics to the physical address of the VPNCs.
- Select 0.0.0.0/0 as the destination network for full-tunnel configuration.
- Select 0.0.0.0 as the gateway to exclude a destination subnet from being tunneled.

NOTE: This behavior applies to L3 routed branch subnet and L2 extended VLANs that are configured in Split-Tunnel mode.

Figure 23 *Routing Configuration*



NOTE: To find the physical IP addresses of the VPNCs to be set in the routing tables of the IAPs, go to the **Gateway Details** page and select the **LAN** tab.

Split DNS Configuration

Split DNS is enabled by default in the Micro-Branch architecture to enable users to reach Internet destinations closest to their location. The enterprise domain setting in the AP configuration specifies the domains for which DNS resolution must be forwarded to the default DNS server of the client.

For example, if the enterprise domain is configured for arubanetworks.com, the DNS resolution for host names in the arubanetworks.com domain are forwarded to the default DNS server of the client. The DNS resolution for host names in all other domains is redirected to the local DNS server of the IAP.

Under **Micro-Branch > Devices > Access Points > System > Enterprise Domains**, type the enterprise domains for which DNS requests would be sent to the corporate DNS servers. For all other domains, the DNS server obtained by the IAP is used. To have all DNS requests go to the corporate server, enter an asterisk (*).

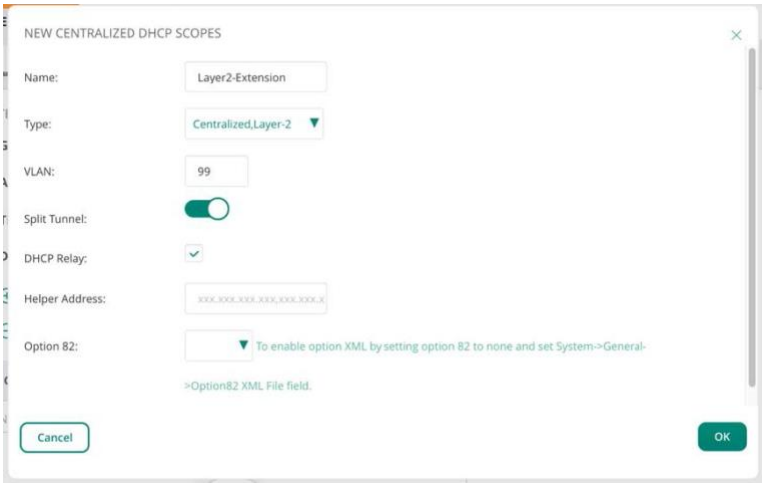
Modes of Operation

Setting the modes of operation is done based on each VLAN. In **Micro-Branch** > **Devices** > **Access Points** > **System** > **DHCP**, create the Local, L2, or L3 subnets and DHCP scopes to be used. Centralized modes assume the existence of a corporate DHCP server to which requests are relayed. In distributed modes, the AP acts as the DHCP server. The two most common modes are L2 centralized mode and L3 distributed mode

L2 Centralized Mode

When working in L2 centralized mode, a common subnet spans across all the locations. DHCP requests are related by the AP to the DHCP server. In order to preserve scalability, the Headend Gateways do not flood all broadcast and unknown multicast traffic to the rest of the branches. When there is an L2 extension of a VLAN across multiple locations in this mode, traffic can be source-NATed. Define an L2-Centralized VLAN in a Micro-Branch group in **Micro-Branch > Devices > Access Points > System > DHCP.**

Figure 24 *Extended L2 VLAN Configuration*



NOTE: When Split-Tunnel is enabled, the AP source-NATs all traffic that is not set to be forwarded through the IPSec tunnel, as defined in the routing configuration.

L3 Distributed Mode

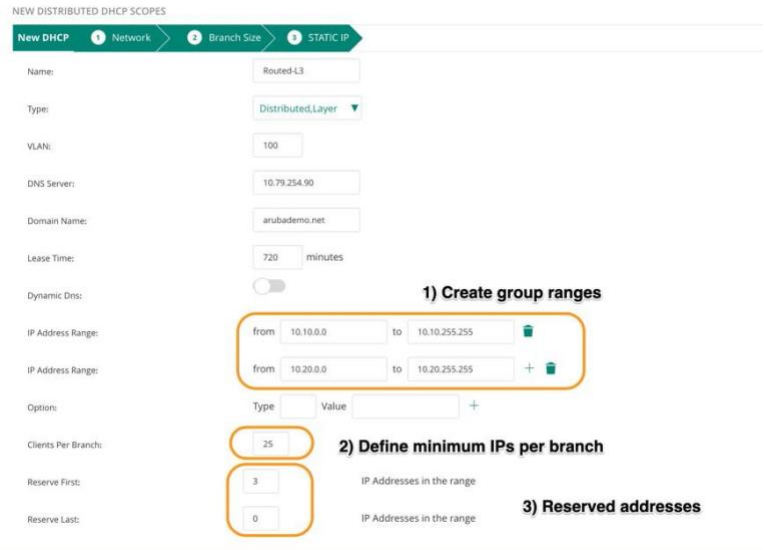
When working in L3 centralized mode, a common range (or set of ranges) of IP addresses is distributed across the branch subnets. This range is sliced into smaller subnets and allocated to the different APs by the VPNC. Once the larger group range is selected, the number of hosts per branch and the number of reserved IPs, the VPNC allocates subnets to the APs.

For the example in the following figure, there are a total of 31 addresses as follows:

- 25 hosts
- 3 reserved addresses
- 1 access point IP address
- 1 network IP
- 1 broadcast IP

This results in the VPNC allocation 27 branch subnets to all the APs in the group for VLAN 100.

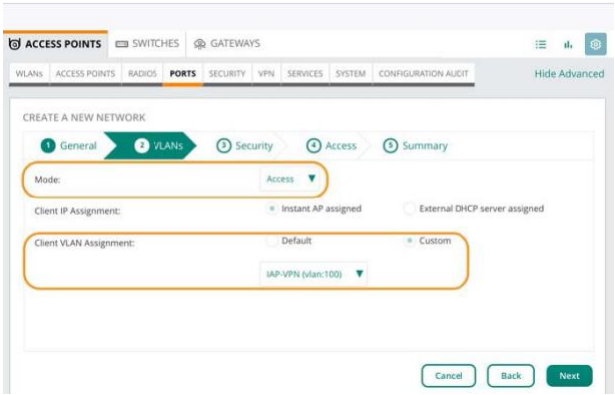
Figure 25 *Routed L3 Network Example*



Applying Tunneled Networks

Once the route is created for a given VLAN, it can be used in the SSID or Port Profile configuration under **Micro-Branch > Devices > Access Points > Configuration**. To apply VLANs to WLANs, navigate to **Micro- Branch > Devices > Access Points > WLAN**. To apply VLANs to ports, navigate to **Micro-Branch > Devices > Access Points > Ports**.

Figure 26 *Assigning VLANs to SSIDs and Ports*

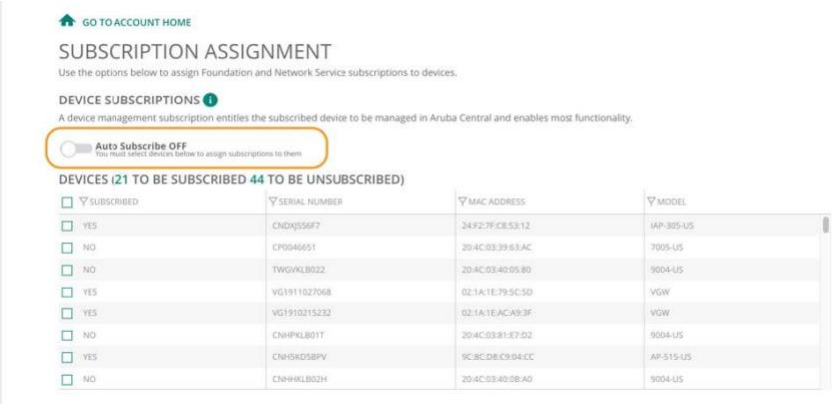


NOTE: Aruba recommends all teleworker ports to be treated as untrusted and to apply 802.1X authentication on wired and wireless subnets to ensure non-corporate devices are not connected to the network. Details on how to configure Network Profiles as well as AAA and Security Profiles can be found in the Aruba Central documentation.

Device Provisioning

Aruba Central helps streamline IT operations by providing a true zero-touch deployment. Devices can be shipped directly to remote locations, such as teleworker offices, and installed by non-technical personnel because devices are added to the customer's Device Inventory in Aruba Central as soon as a purchase order for any number of (n) devices, are received by Aruba. Once the devices are added to the Device Inventory in Aruba Central, they can be manually or automatically assigned a Central subscription in the Aruba Central Account Home.

Figure 27 *Aruba Central Account Home*



If an Aruba Central subscription is assigned to a device, it automatically connects to Aruba Central as soon as it has network connectivity and Internet access. This allows the device to download its configuration and to be managed by Aruba Central. The Aruba Installation Management service simplifies and automates site deployments and helps IT administrators manage site installations with ease. Detailed information about this process is available in the Aruba Central Documentation Portal.

Administrator Workflow

Install Manager on the Aruba Central portal. For more information, refer to the Aruba Central Documentation Portal.

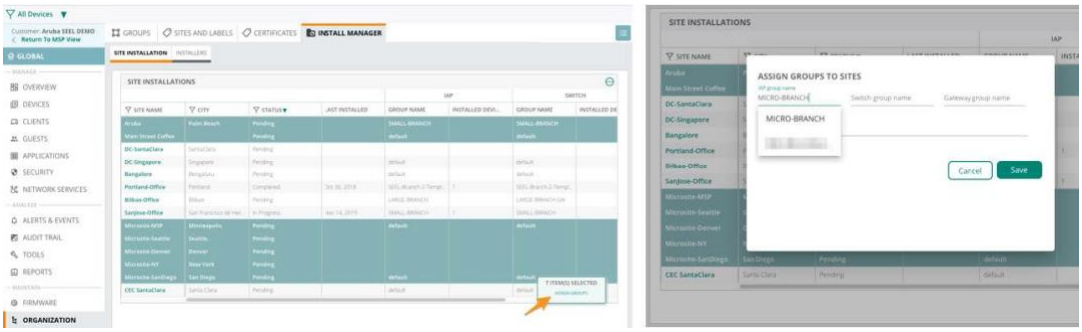
Site Creation

This part of the process is an optional step that allows installers to assign the name and location of the installation sites. Assigning names and locations to all of the sites simplifies day-to-day operations and can be done in bulk using a CSV file or through the Aruba Central API. For more information, refer to the Managing Sites section of the Aruba Central Documentation Portal.

Associate Configuration to Sites

Once the sites are created, they can be configured through the Install Manager workflow on the **All Devices > Global > Organization > Install Manager > Site Installation** page.

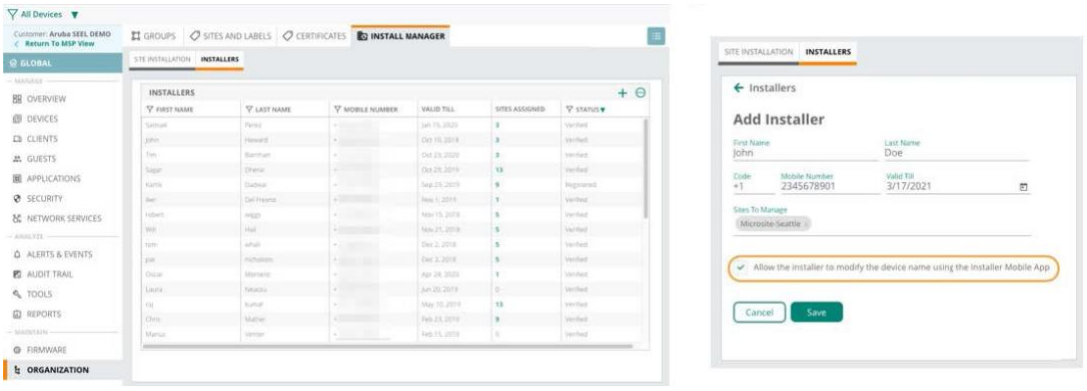
Figure 28 *Assigning Groups to Sites on the Site Installation Page*



Invite Installers

Since Aruba Central provides a true zero-touch deployment, anyone at the remote site can be an installer. Installers can be added and assigned to their respective locations on the **All Devices > Global > Organization > Install Manager > Installers** page.

Figure 29 *Installers Page*



Once an installer is added, they can provision the devices.

Provisioning

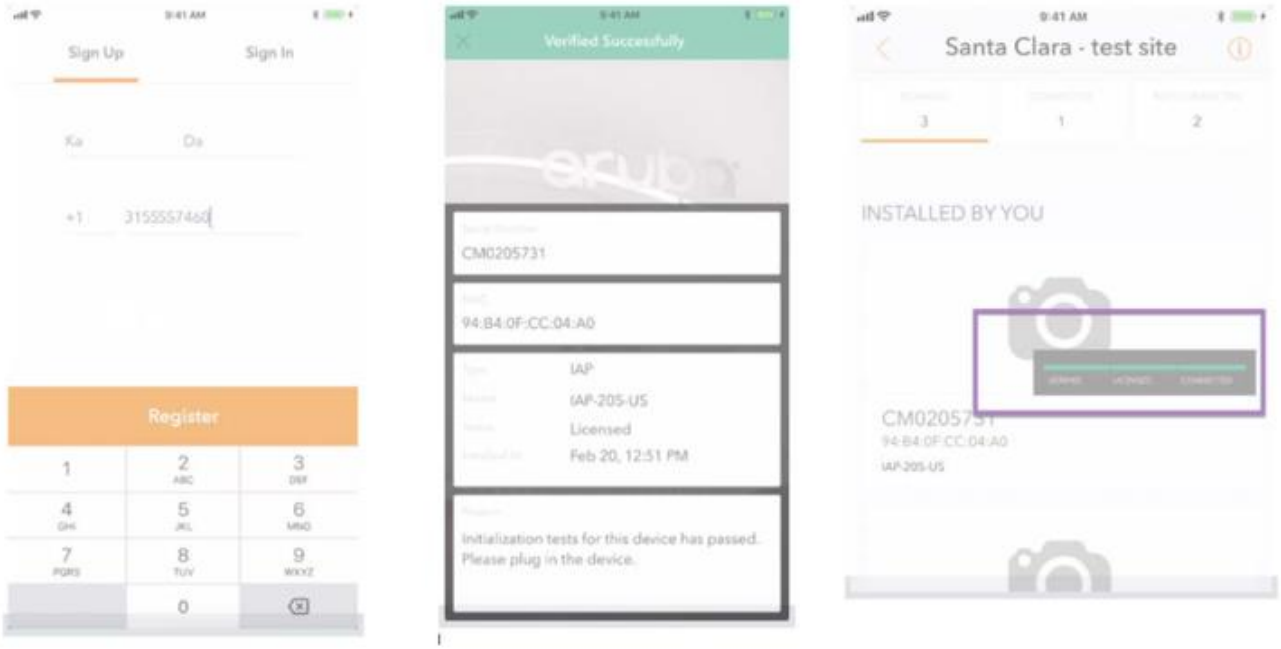
Once an installer is added, they receive a text message with a prompt to download the mobile app for provisioning. Once the mobile app is downloaded, the installer can use the following steps to provision the devices:

1. **Log in to the application** using an OTP sent in a text message.
2. **Click on the site** where the AP will be installed.
3. **Scan the barcode** with the serial number and (optionally) set the name of the AP.

Once an AP is scanned, it is ready to connect to the network. The AP automatically connects with Aruba Central, receives its configuration, and brings up a secure corporate network at the teleworker site.

The mobile app allows installers to view all of the devices that have been scanned on site, as well as devices that are connected or not connected.

Figure 30 *Installer workflow*



Network Recommendations

The following section details the network recommendations and security knobs required for teleworkers in distributed layer 3 deployments. The recommendations in this section of the document are best practices to secure a teleworker's IAP in any kind of network environment. Many of the scenarios described in this section might not actually take place in a typical teleworker's network. These configurations are also not configured by default because many of them would interfere with the clustering capabilities of the IAP. Following these best practices in a single-AP teleworker deployment ensures that the uplink port on the IAP is placed in the most restrictive and secure configuration state. And this also allows the IAP to be safely placed in any kind of teleworker's environment.

It is recommended to use IAPs in standalone mode or single-ap mode while deploying as a single AP remote teleworker solution. This ensures that the IAP does not form clusters with other unauthorized Aruba APs present in the network.

In addition to the configuration and deployment scenarios mentioned before, the following section details on additional recommendations and security knobs for Distributed Layer 3 deployments for a single IAP in standalone mode or single-ap mode. Once the AP is up, configure the standalone mode or single-ap mode by navigating to **the IAP-group > Devices > Access Points > Config > System > General > Swarm mode** configuration page.

Figure 31 *Standalone configuration of IAP at group level*

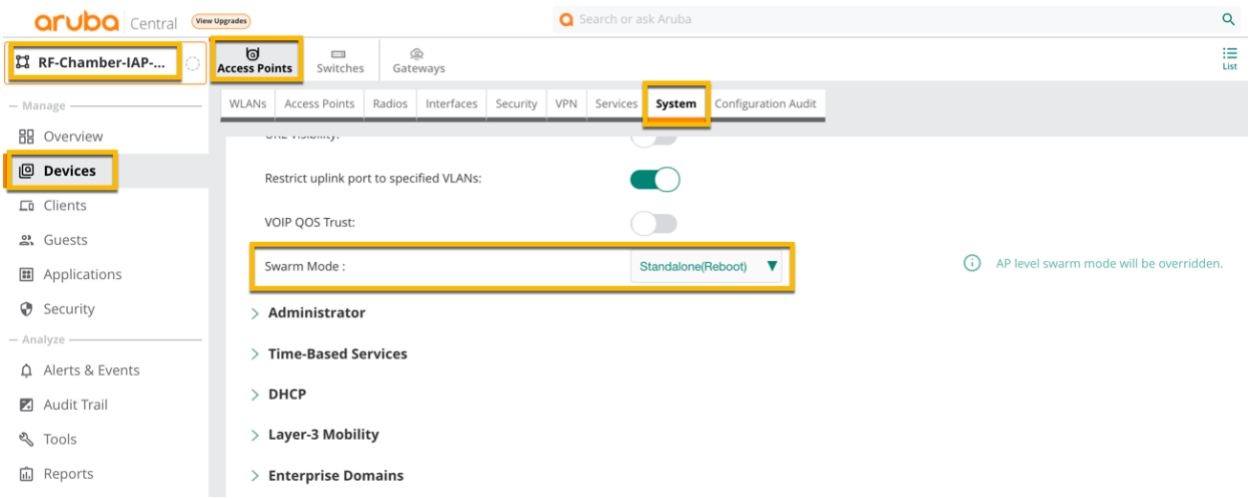
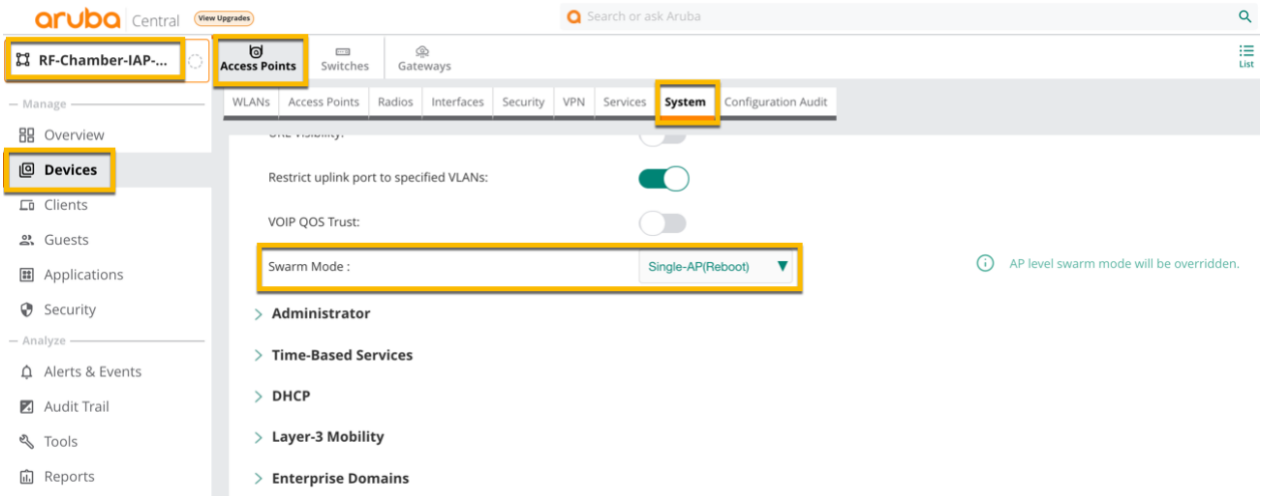
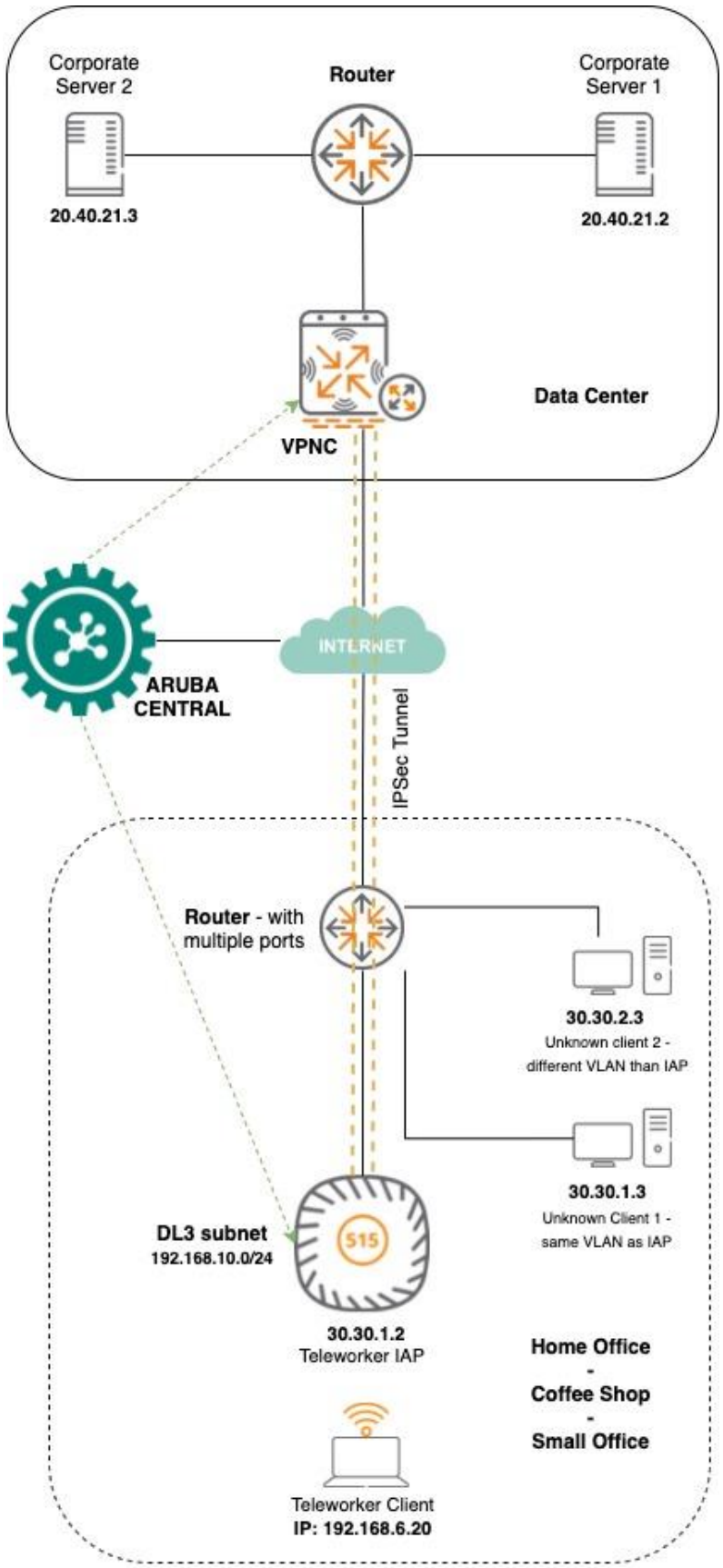


Figure 32 *Single-ap configuration of IAP at group level*



The following figure is a reference diagram for the following use cases:



NOTE: In the following use cases, IAP local uplink network denotes the LAN network of the teleworker router. For example, in the above diagram, IAP local uplink network comprises of unknown client 1, unknown client 2 and teleworker IAP.

Table 3: *Required Feature Matrix for Use Cases*

Required Features / Config Knobs for Use Cases	Management Subnets	Inbound Firewall rules	UI Knob	Access Rules	Auto Topology Rules	Enterprise Domains
Block all local Management access to Teleworker's IAP	N/A	N/A	WebUI Access	N/A	N/A	N/A
Restrict Management access of a Teleworker's IAP to a specific network	Yes	N/A	N/A	N/A	N/A	N/A
Block all inbound traffic to Teleworker's IAP	Yes	Yes	N/A	N/A	N/A	N/A
Allow arbitrary access from corporate to teleworker IAP through tunnel	N/A	Yes	Tunnel trusted	N/A	N/A	N/A
Block Corporate access from IAP local uplink network	N/A	Yes	N/A	N/A	N/A	N/A
Disallow non- native VLAN tagged traffic from uplink side	N/A	N/A	Restrict uplink port to specified VLANs	N/A	N/A	N/A
Block Teleworker client's access to IAP local uplink network	N/A	N/A	N/A	Yes	N/A	N/A
Block Teleworker client's access to IP addresses reserved for IAP	N/A	N/A	N/A	Yes	N/A	N/A
Block automatic cluster formation messages from non-teleworker Aruba APs	N/A	N/A	N/A	N/A	Yes	N/A

Block roaming, mobility control packets to be sent/received in uplink port	N/A	N/A	Single-ap mode	N/A	N/A	N/A
Forward all DNS traffic to the DNS server assigned to the teleworker client	N/A	N/A	N/A	N/A	N/A	Yes

Use Case 1: Block all local management access to Teleworker's IAP

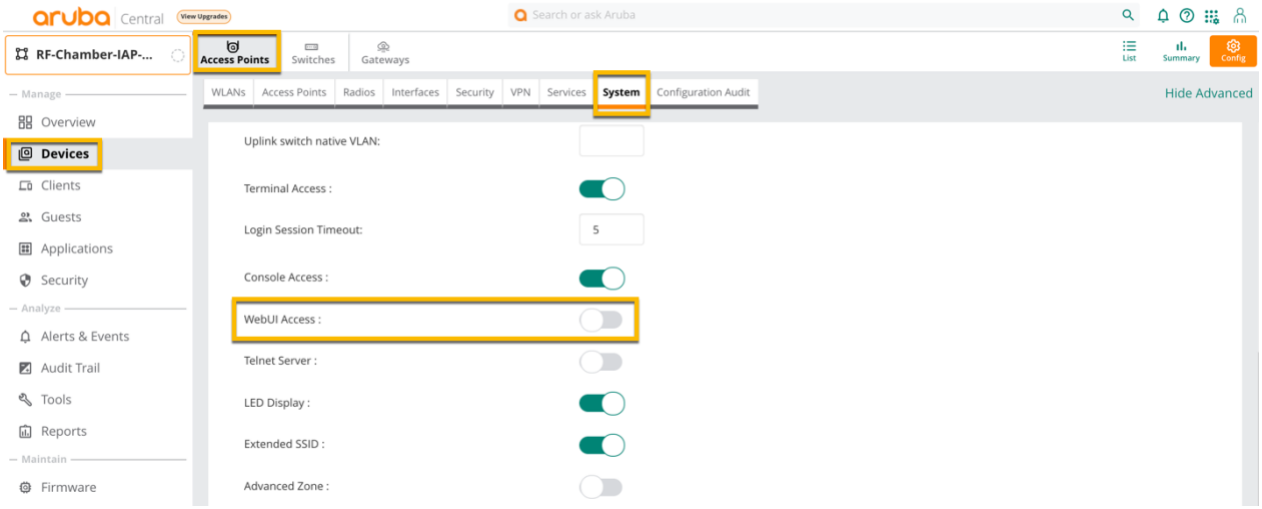
By default, any device on the teleworker's IAP local uplink network can have management access to the IAP (by providing the correct login credentials). Although the AP login credentials are secret, some administrators may want to completely manage the IAP only through Central and block all management access (such as SSH, WebUI) especially when managing the IAP remotely.

Configuration

Navigate to **IAP-Group > Devices > Access Points > Config > System > General and 'disable' the WebUI Access**. By disabling 'WebUI Access', the AP Web UI access and any communication via HTTPS or SSH received by the IAP through the uplink port will be blocked.

> **NOTE:** Management access from Central will not be affected by this configuration. However, if central connection is down, the teleworker IAP cannot be managed until the connection to central is up.

Figure 33 *Block Management Access*



Verification

After disabling WebUI access, management access of teleworker's IAP through WebUI or SSH will be blocked

NOTE: This will only block the management access to the teleworker IAP whereas other access like ping, etc. to teleworker's IAP will continue to work.

The remote console access to the teleworker IAP through Central will also be blocked. However, teleworker IAP can be accessed through its physical console port.

Use Case 2: Restrict management access of a Teleworker's IAP to specific network

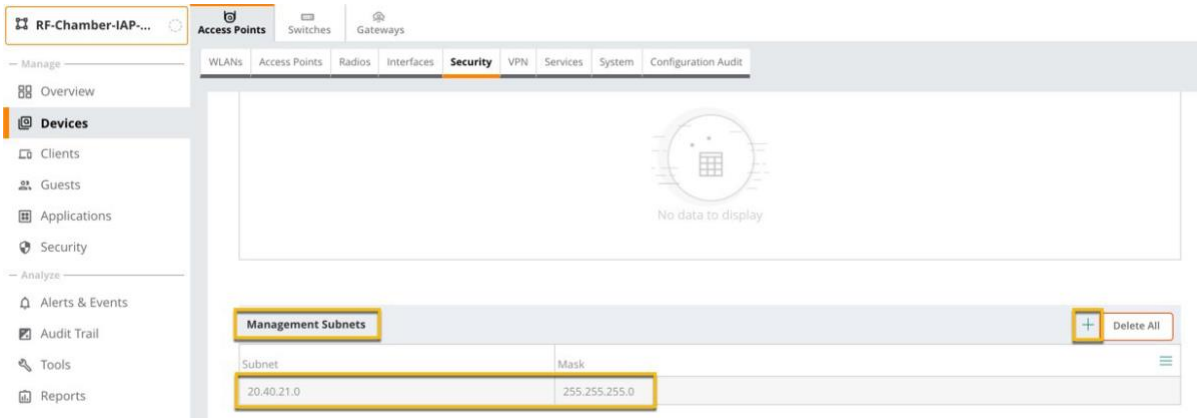
By default, any device on the teleworker's IAP local uplink network can have management access to the IAP (by providing the correct login credentials). Although the AP login credentials are secret, some administrators may want to restrict the management access (such as SSH, WebUI) to specific network and allow only certain subnets to manage the teleworker's IAP (unlike completely blocking the management access as seen in the previous use case).

NOTE: Management access from Central will not be affected by this configuration.

Configuration

Navigate to **IAP-Group > Devices > Access Points > Config > Security > Wireless IDS/IPS > Firewall Settings > Management Subnets** and click **+** to add subnet(s) that are allowed to manage the teleworker's IAPs.

Figure 34 *Configuring Management Subnets*



Verification

After configuring Management Subnets, management access to the teleworker's IAP will be restricted only to the configured subnets.

NOTE: This will only block the management access to the teleworker IAP whereas other access like ping, etc. to teleworker IAP will still continue to work.

Use Case 3: Block inbound traffic to Teleworker's IAP

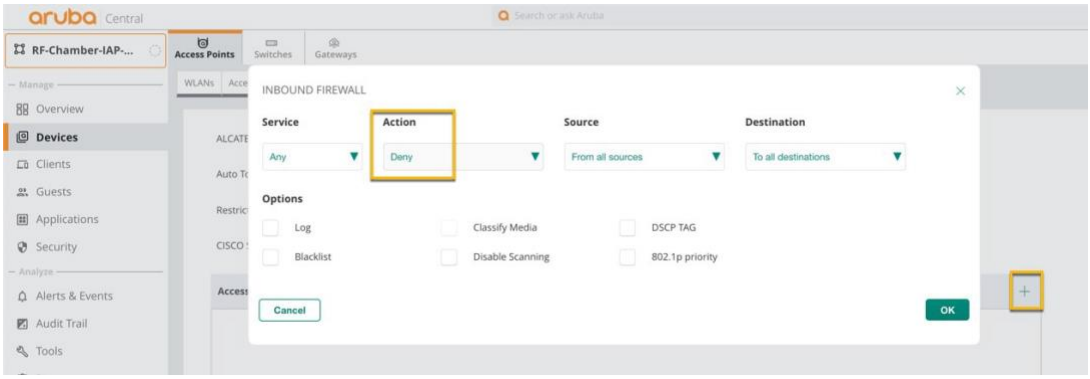
By default, any device on the teleworker's IAP local uplink network as well as from the corporate network can have access to the IAP (i.e Ping, Telnet, SSH, WebUI, etc. by providing the correct credentials). Any device in the IAP local uplink network using IAP as the gateway can access the corporate resources. To block this, inbound firewall rules need to be added and Management access to teleworker IAP should be blocked. This also ensures that the incoming traffic from the IAP's local non-native VLANs is blocked

> **NOTE:** Inbound firewall rule blocks everything apart from SSH and WebUI management access. Restricting the management access blocks all the management access.

Configuration

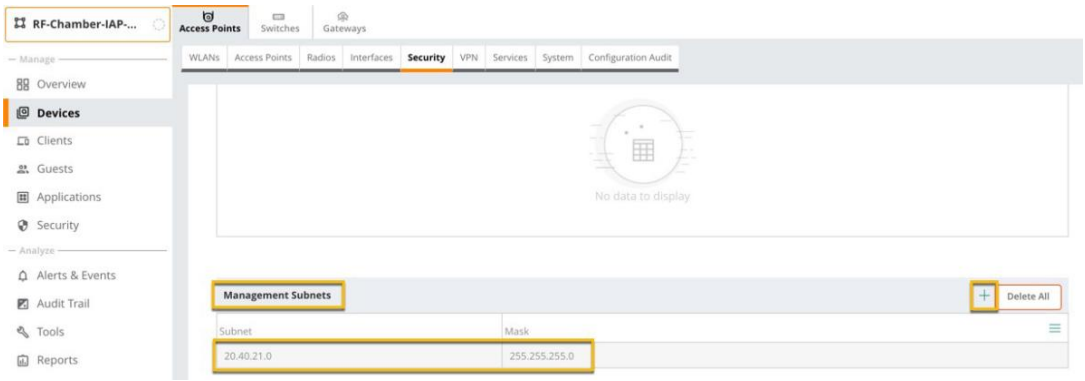
Navigate to **IAP-Group > Devices > Access Points > Config > Security > Wireless IDS/IPS > Firewall Settings** and add a rule as shown below:

Figure 35 *Configuring Inbound Firewall Rule*



Navigate to **IAP-Group > Devices > Access Points > Config > Security > Wireless IDS/IPS > Firewall Settings > Management Subnets**, click + to add a dummy subnet (Central will still access the Teleworker IAP)

Figure 36 *Configuring Management Subnets*



NOTE: IAP may be accessed via SSH or WebUI if the management subnet configured in Central is accidentally present in the IAP local uplink network.

Verification

After configuring inbound firewall rule, any access to the teleworker's IAP and the clients associated with this IAP will be restricted from IAP local uplink network and from the corporate network

NOTE: Teleworker clients behind the IAP can still access the corporate network with this configuration.

Use Case 4: Allow arbitrary access from Corporate to Teleworker IAP through tunnel

By default, any device on the teleworker's IAP local uplink network as well as from the corporate network can have access to the IAP (i.e Ping, Telnet, SSH, WebUI, etc. by providing the correct credentials). To block this, inbound firewall rules need to be added. If required, specific management subnets can be configured to restrict management access to the IAP.

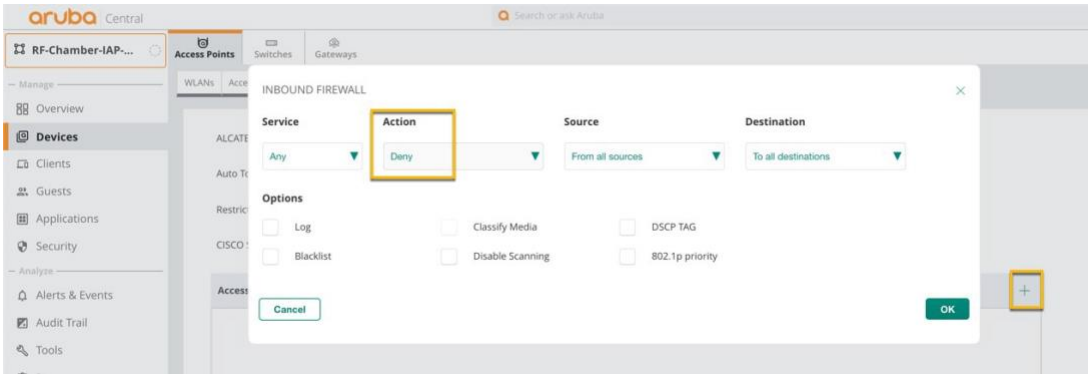
Adding inbound firewall rules might also block access from corporate to teleworker IAP and the associated clients. To avoid this and to allow arbitrary access from corporate to teleworker IAP and associated clients through tunnel, 'Tunnel Trusted' knob can be enabled

NOTE: Inbound firewall rule blocks everything apart from SSH and WebUI management access. Restricting the management access blocks all the management access.

Configuration

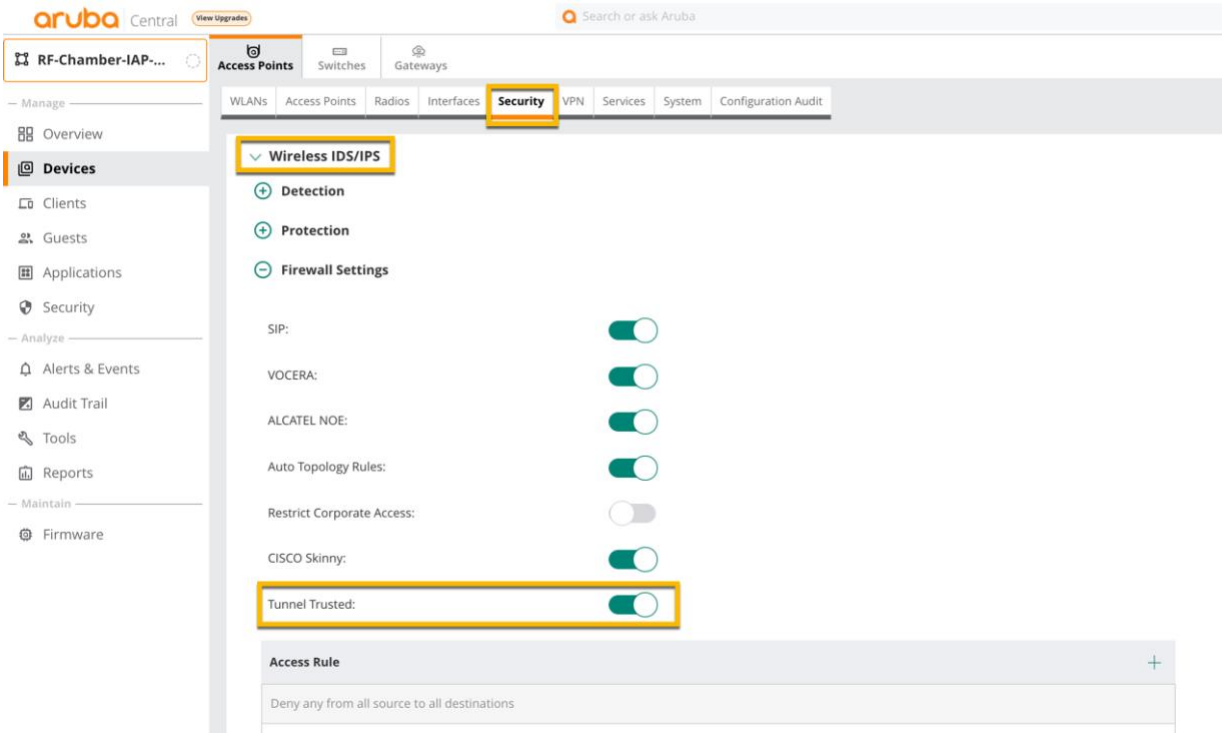
Navigate to **IAP-Group > Devices > Access Points > Config > Security > Wireless IDS/IPS > Firewall Settings** and add a rule as shown below:

Figure 37 *Configuring Inbound Firewall Rule*



Navigate to **IAP-Group > Devices > Access Points > Config > Security > Wireless IDS/IPS > Firewall Settings > Enable 'Tunnel Trusted'**

Figure 38 *Configuring Tunnel Trusted*



NOTE: IAP may be accessed via SSH or WebUI if the management subnet configured in Central is accidentally present in the IAP local uplink network.

Verification

After configuring inbound firewall rule and enabling 'Tunnel Trusted', access to the teleworker's IAP and the clients associated with this IAP will be allowed from the corporate network

NOTE: Teleworker clients behind the IAP can still access the corporate network with this configuration.

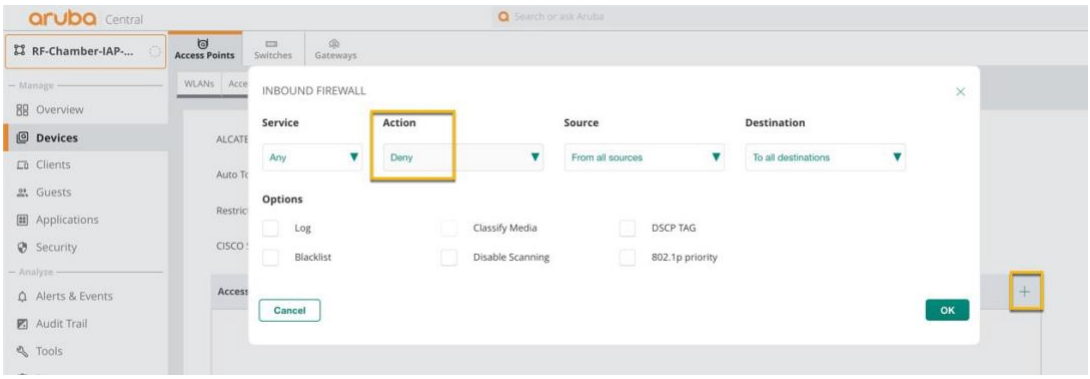
Use Case 5: Block Corporate Access from IAP Local Uplink Network

Any device in the IAP local uplink network using IAP as the gateway can access the corporate resources. To block this, enable inbound firewall rule. This restricts access to corporate network from the uplink port of the IAP.

Configuration

Navigate to **IAP-Group > Devices > Access Points > Config > Security > Wireless IDS/IPS > Firewall Settings** and add a rule as shown below:

Figure 39 *Configuring Inbound Firewall Rule*



Verification

After configuring inbound firewall rule, access to corporate resources will be blocked for unauthorized devices on IAP's local uplink network.

Use Case 6: Disallow non-native VLAN tagged Traffic from Uplink side

By default, the IAP's physical uplink is a trunk port with allowed-all vlans. To allow only the native VLAN traffic and to block all non-native VLAN tagged traffic on the IAP's uplink port, a new wired port profile with the recommended configurations need to be created and the knob **Restrict uplink port to specified VLANs** should be enabled.

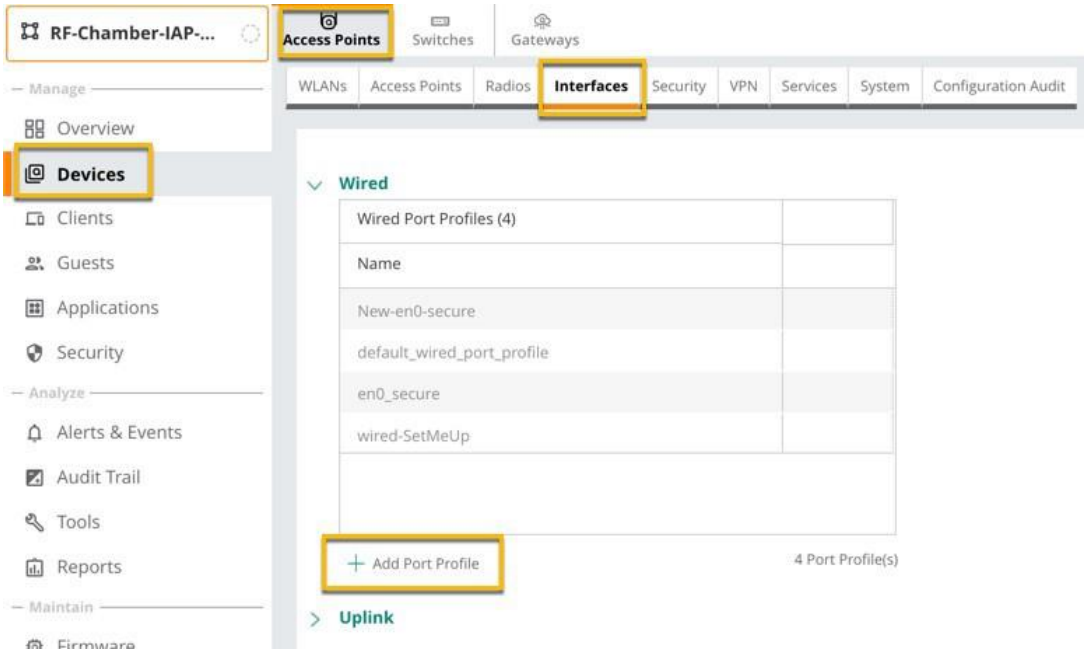
> **NOTE:** IAP should be rebooted for this configuration to take effect.

Configuration

Navigate to **IAP-Group > Devices > Access Points > Config > Interfaces > Wired,** click **Add Port profile** and provide the following information:

- Name: New-en0-secure
- Ports: enet0
- Allowed vlan: 1
- Leave other options with default values

Figure 40 *Adding a wired port profile*



In the following image, ‘enet0’ refers the E0 port on the teleworker's IAP which is the uplink port.

Figure 41 *Binding uplink port to wired port profile*

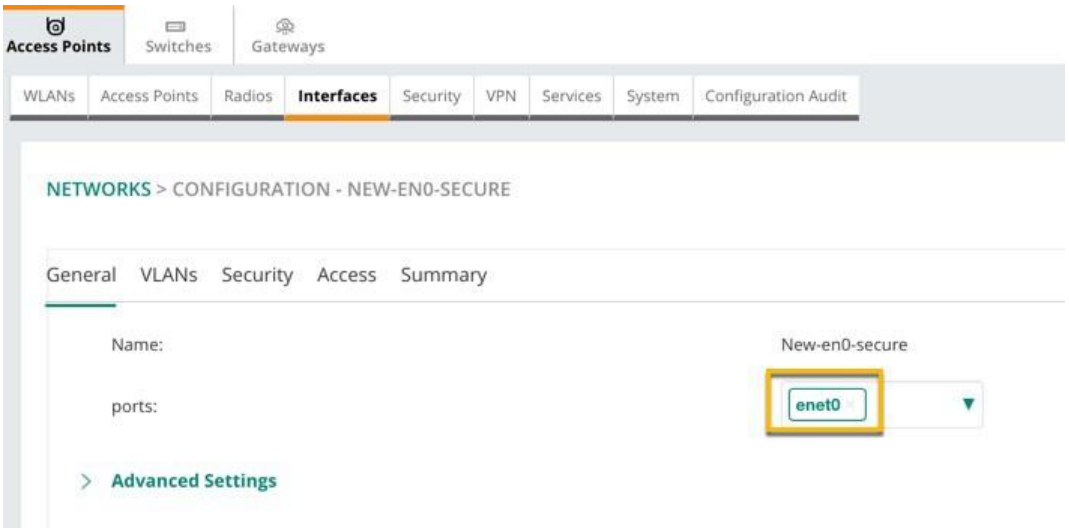
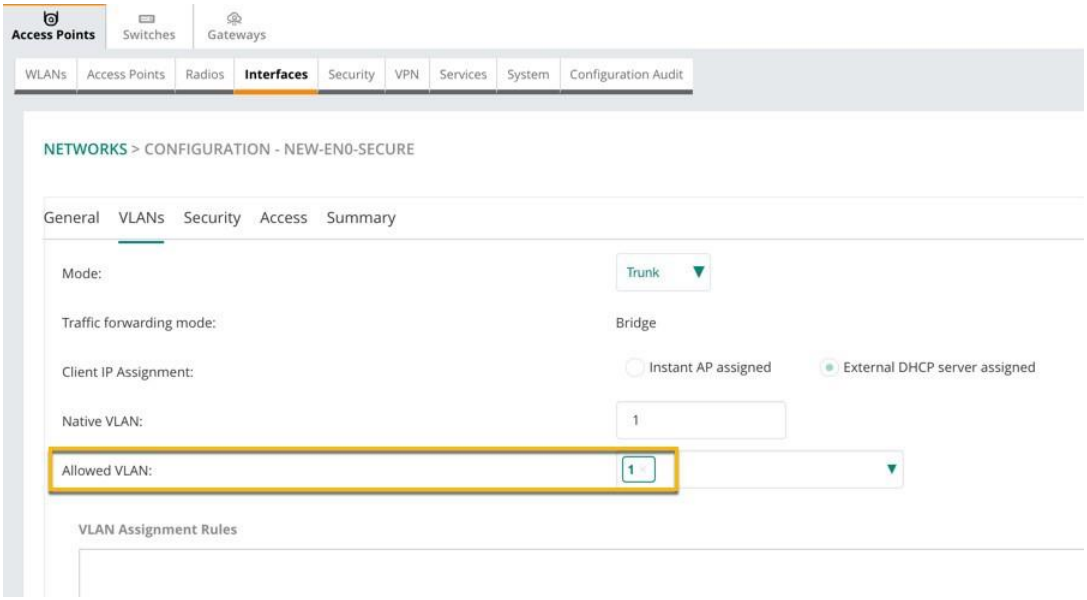
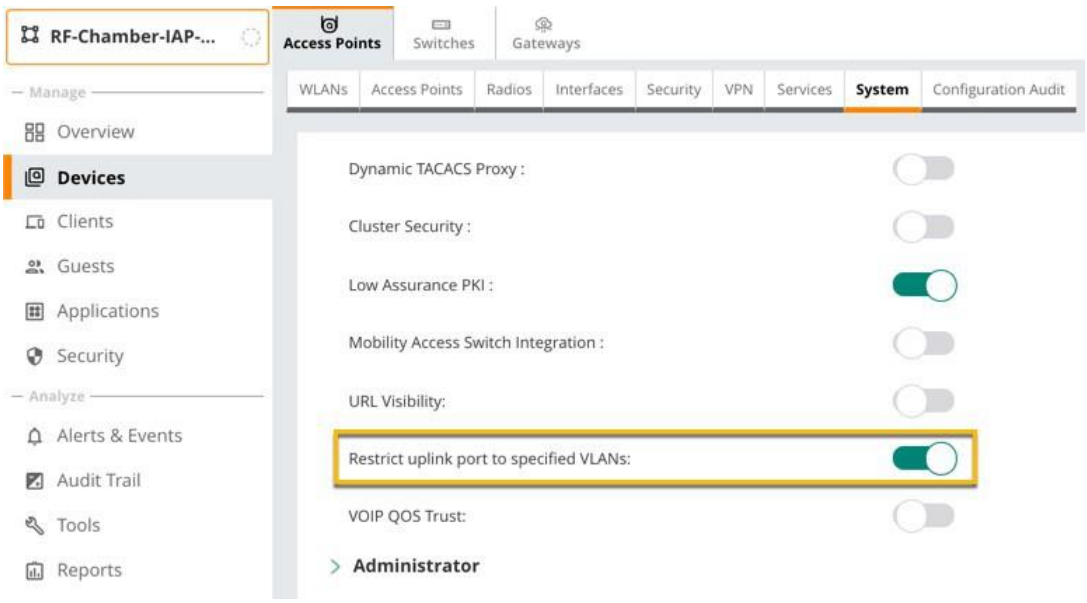


Figure 42 *Configuring Allowed vlan for wired port profile*



Navigate to **IAP-Group > Devices > Access Points > Config > System** and enable **Restrict Uplink port to specified VLANs.**

Figure 43 *Enabling Restrict Uplink port to specified VLANs*



Navigate to **IAP (device) > Overview > Action**, click **Reboot AP** to reboot the teleworker's IAP. This is required for the above mentioned configuration to take effect.

Figure 44 *Rebooting Teleworker's IAP*

Use Case 7: Block Teleworker Client's Access to IAP Local Uplink Network

By default, the teleworker's clients can access IAP's local uplink network like home printers, IoT devices etc. To block this, an ACL should be set on the teleworker wireless SSID configuration to deny this traffic.

Configuration

The ACL rule can be set as Network-Based access rule in the SSID configuration. Navigate to **SSID > Access > Network-based > New Access Rule,** select **Deny** for **Action** and **to AP network** for **Destination.**

Figure 45 ***Configuring Access Rule***

Verification

After configuring access rules, the teleworker's clients will not be able to access the IAP's local uplink network.

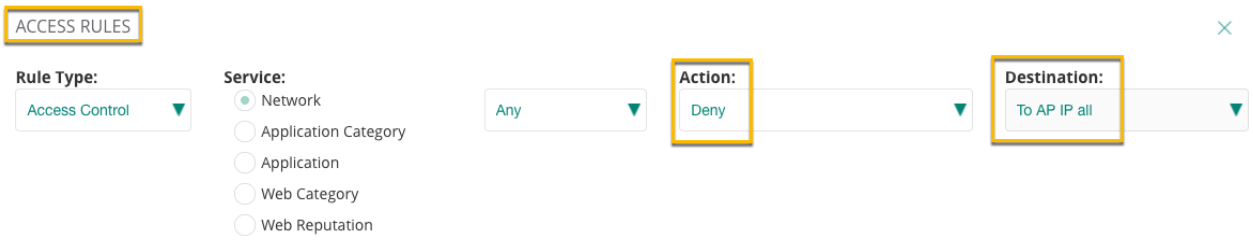
Use Case 8: Block Teleworker's Client Access to IP Addresses Reserved for the IAP

By default, the teleworker's clients can access the IP addresses reserved for the IAP. To block this, an ACL can be set on the teleworker wireless SSID configuration to deny the traffic to the alias 'apip-all'. The 'apip-all' is an alias that includes all IP address used by the IAP such as br0 IP, DHCP scope, magic-vlan, etc.

Configuration

The ACL rule can be set as Network-Based access rule in the SSID configuration. Navigate to **SSID > Access > Network-based > New Access Rule,** select **Deny** for **Action** and **To AP IP all** for **Destination.**

Figure 46 ***Configuring Access Rule***



Verification

After configuring access rules, the teleworker's clients will not be able to access the IP addresses reserved for the IAP.

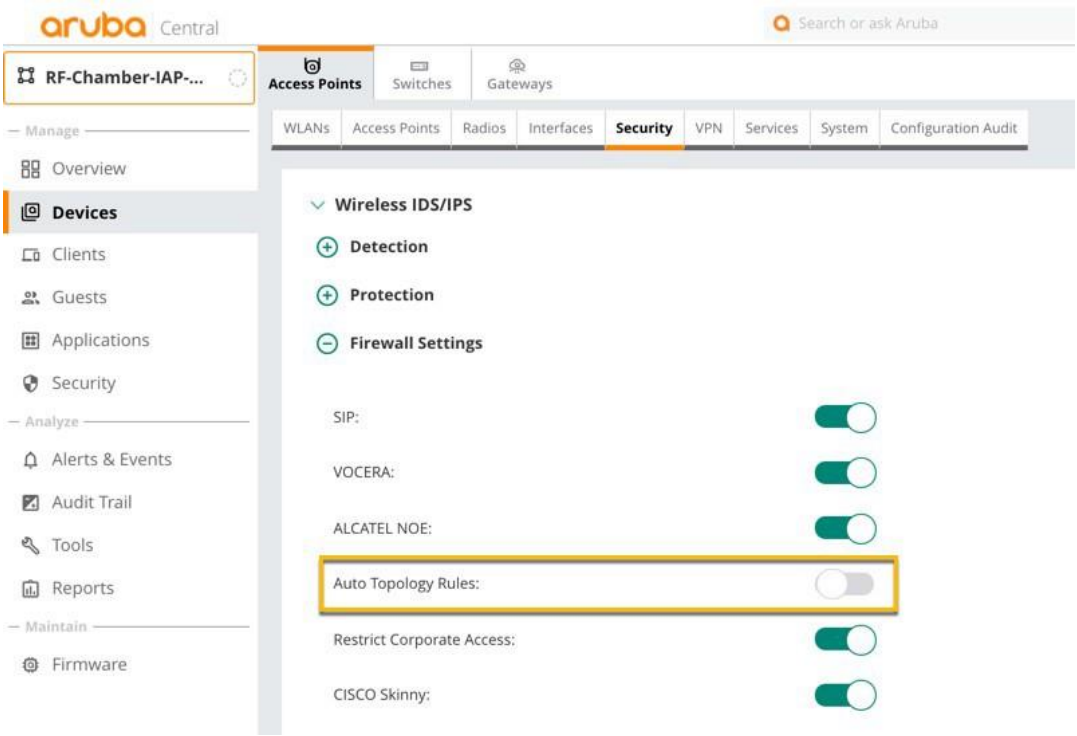
Use Case 9: Block Automatic Cluster Formation Messages from Non-Teleworker Aruba APs

Auto Topology is a feature that automatically adds ACL rules into the firewall. This ensures that any kind of control-plane messages required for the automatic cluster formation are never blocked and auto topology is enabled by default. However, this feature can be disabled when customers prefer full control on the security policy rather than accepting automatic ACL rules. This will block fake PAPI traffic from attackers. To deny auto topology communication outside the Instant AP subnet, the inbound firewall settings must also be enabled.

Configuration

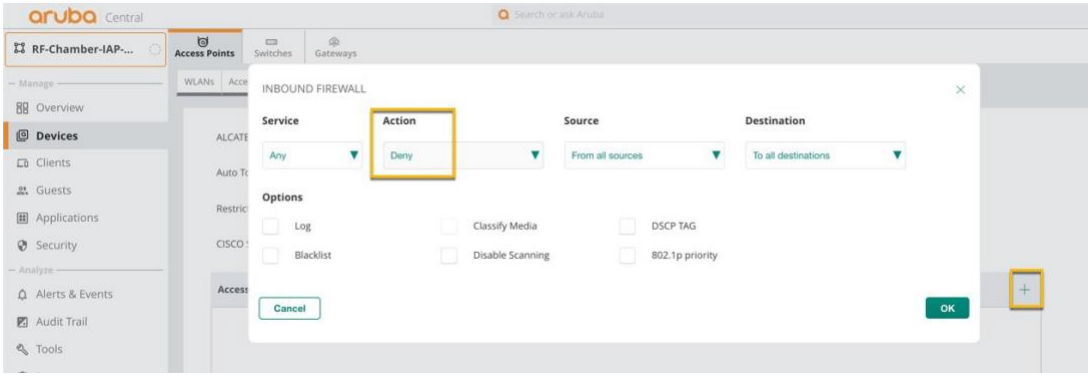
Navigate to **AP-Group > Devices > Access Points > Config > Security > Wireless IDS/IPS > Firewall Settings.** Select **Disabled** for **Auto topology rules.**

Figure 47 *Disabling Auto topology Rules*



Navigate to **IAP-Group > Devices > Access Points > Config > Security > Wireless IDS/IPS > Firewall Settings** and add a rule as shown below:

Figure 48 *Configuring Inbound Firewall Rule*



Use Case 10: Block Roaming, Mobility Control Packets to be Sent/Received in Uplink Port

By default, the access point can send or receive management frames such as mobility packets, roaming packets, hierarchy beacons through its uplink port. To prevent this, the standalone teleworker IAP can be configured as “single-ap” mode. Single-ap mode is a new deployment mode suitable for deployments with single teleworker access point.

Configuration

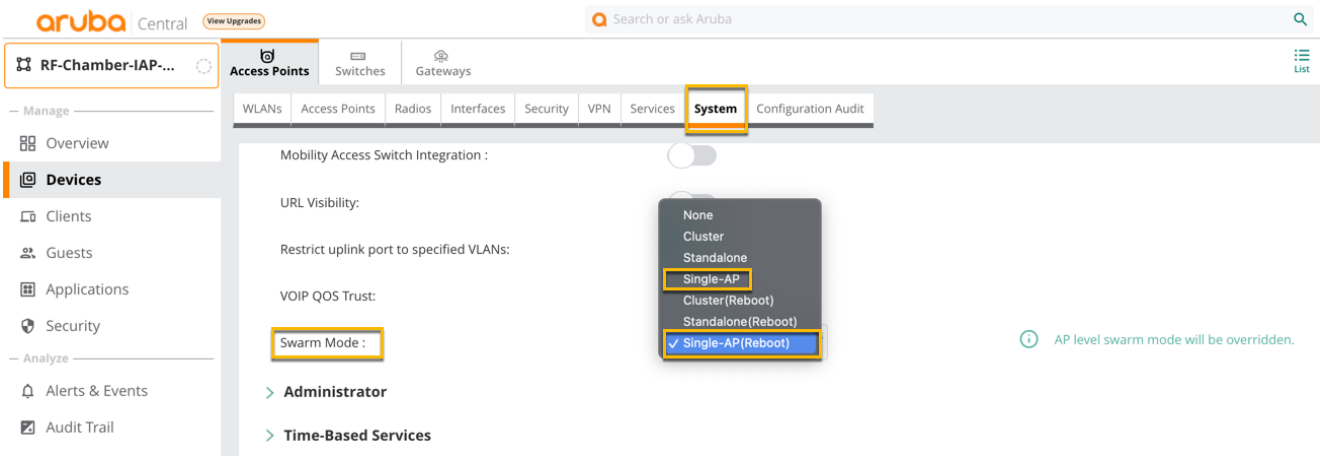
Single-ap mode can be configured either at group level or at AP level. When configured in group mode, the IAP level swarm mode will be overridden.

Group-level:

Navigate to **AP-Group > Devices > Access Points > Config > System > General**. In Swarm Mode, select either one:

- **Single-AP(Reboot)** – to configure single-ap mode and automatically reboot IAP
- **Single-AP** – to configure single-ap mode but user must manually reboot IAP to take effect

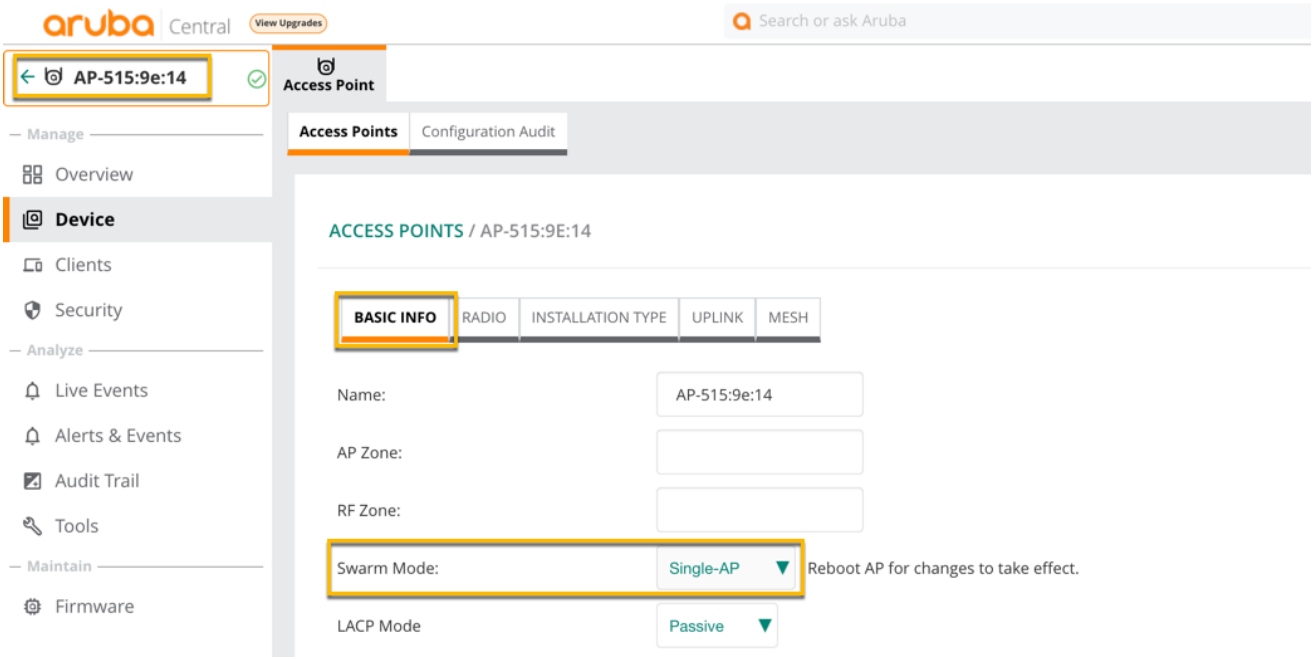
Figure 49 *Configuring Single-ap swarm mode in AP-group level*



AP-level:

Navigate to **AP-Group > Devices > Access Points > Click the Access point to be configured > Device > Access Points > Edit > Basic Info**. In Swarm Mode, select **'Single-AP'**

Figure 50 *Configuring Single-ap swarm mode in AP level*



Navigate to **IAP (device) > Overview > Action**, click **Reboot AP** to reboot the teleworker's IAP. This is required for the above-mentioned configuration to take effect.

Figure 51 *Rebooting Teleworker's IAP*

NOTE: IAP should be rebooted for this configuration to take effect.

Use Case 11: Forward all DNS traffic to the DNS server Assigned to the Teleworker's Client

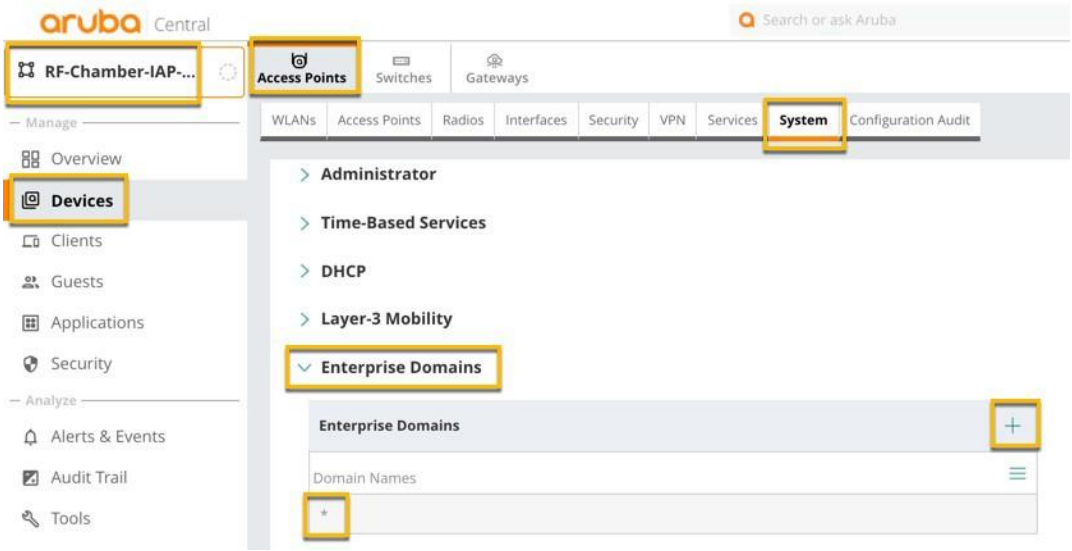
The enterprise domain setting in the AP configuration specifies the domains for which DNS resolution must be forwarded to the default DNS server of the client.

For example, if the enterprise domain is configured for arubanetworks.com, the DNS resolution for host names in the arubanetworks.com domain are forwarded to the default DNS server of the client. The DNS resolution for host names in all other domains is redirected to the local DNS server of the IAP.

Configuration

To ensure all DNS requests go to the DNS server assigned to the teleworker client, enter an asterisk (*) in enterprise domain. Navigate to **IAP-Group > Devices > Access Points > Config > System > Enterprise Domains**, click **+** and all **(*)**.

Figure 52 *Configuring Enterprise Domain Names*



Verification

It can be observed that before adding asterisk (*) in an enterprise domain, if a teleworker user tries to access non-corporate resources such as www.google.com, the datapath session (*show datapath session | include <client IP>*) in VPNC will not display the DNS query as the teleworker local DNS server will be used. After adding asterisk (*) in an enterprise domain, the datapath session in VPNC will display the DNS query as all the DNS queries are sent to the corporate server.

Appendix A - Important Considerations

Central Licenses

When devices are managed by Central, the following licenses are required for the teleworker service:

- Headend gateways require at least the Foundation base license.
- APs require a Foundation license.

Headend Gateway Sizing

Table 2 below outlines scalability numbers for each gateway model for an IAP VPN deployment. The table assumes the following definitions:

- IAP VPN Tunnels – The number of IAP remote teleworker branches that can be terminated by the gateway
- Route Limit – The number of Layer 3 routes supported by the gateway
- User Limit - For L2 extended VLANs.
- VLAN Limit – The number of VLANs supported by the gateway

Table 5: *VPNC Scaling*

Platform	IAP Tunnel	Route Limit	User Limit (L2 mode)	VLAN Limit
Virtual Gateway (AWS)				
VGW-4G	4,096	32,000	N/A	4,096
VGW-2G	2,048	16,000	N/A	4,096
VGW-500M	512	1,700	N/A	256
Virtual Gateway (Azure)				
VGW-4G	4,096	32,000	N/A	4,096
VGW-2G	2,048	32,000	N/A	4,096
VGW-500M	512	1,700	N/A	256
9000 Series				
9004	128	8,192	1,792	4,094
9012	128	8,192	1,792	4,094

Platform	IAP Tunnel	Route Limit	User Limit (L2 mode)	VLAN Limit
7200 Series				
7210	2,048	16,384	12,288	4,094
7220	4,096	16,384	16,384	4,094
7240XM	8,192	32,769	16,384	4,094
7280	8,192	32,769	16,384	4,094
7000 Series				
7005	64	4,096	896	4,094
7008	64	4,096	896	4,094
7010	128	4,096	1,792	4,094
7024	128	4,096	1,792	4,094
7030	256	8,192	3,584	4,094