



Aruba Remote Access Point (RAP) Networks

Version 8



Copyright

© 2012 Aruba Networks, Inc. AirWave®, Aruba Networks®, Aruba Mobility Management System®, Bluescanner, For Wireless That Works®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFprotect®, The All Wireless Workplace Is Now Open For Business, Green Island, and The Mobile Edge Company® are trademarks of Aruba Networks, Inc. All rights reserved. Aruba Networks reserves the right to change, modify, transfer, or otherwise revise this publication and the product specifications without notice. While Aruba uses commercially reasonable efforts to ensure the accuracy of the specifications contained in this document, Aruba will assume no responsibility for any errors or omissions.

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

Legal Notice

ARUBA DISCLAIMS ANY AND ALL OTHER REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, ACCURACY AND QUIET ENJOYMENT. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF ARUBA EXCEED THE AMOUNTS ACTUALLY PAID TO ARUBA UNDER ANY APPLICABLE WRITTEN AGREEMENT OR FOR ARUBA PRODUCTS OR SERVICES PURCHASED DIRECTLY FROM ARUBA, WHICHEVER IS LESS.

Warning and Disclaimer

This guide is designed to provide information about wireless networking, which includes Aruba Network products. Though Aruba uses commercially reasonable efforts to ensure the accuracy of the specifications contained in this document, this guide and the information in it is provided on an "as is" basis. Aruba assumes no liability or responsibility for any errors or omissions.

ARUBA DISCLAIMS ANY AND ALL OTHER REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, ACCURACY, AND QUIET ENJOYMENT. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF ARUBA EXCEED THE AMOUNTS ACTUALLY PAID TO ARUBA UNDER ANY APPLICABLE WRITTEN AGREEMENT OR FOR ARUBA PRODUCTS OR SERVICES PURCHASED DIRECTLY FROM ARUBA, WHICHEVER IS LESS.

Aruba Networks reserves the right to change, modify, transfer, or otherwise revise this publication and the product specifications without notice.



www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Table of Contents

Chapter 1:	Introduction	8
	Reference Material	9
	Icons Used in this Guide	10
Chapter 2:	Virtual Branch Networks	11
	Aruba Virtual Branch Network Solution	11
Chapter 3:	Remote Deployments	13
	Logical Architecture of Aruba Remote Networks	15
	RAP Operation	18
	Key Components of the Architecture	19
	Master Controllers	19
	RAPs	20
	AMs	20
	Firewall Ports	20
Chapter 4:	All-Master Design for Remote Networks	21
	Controller Licenses	21
	Licensing Master Mobility Controllers	21
	Certificates	22
Chapter 5:	VLAN Design and Recommendations	23
	VLAN Pooling	25
Chapter 6:	Redundancy	27
	Master Redundancy	27
Chapter 7:	Configuring VPN Server on the Controller	37
	Configuring the VPN Server on the Controller	37
	RAP Bootstrapping	37
	VPN Server Configuration	38
	Configuring the VPN Authentication Profiles	42
Chapter 8:	Configuring AP Group for RAPs	45
	Alias	46
	Configuration Profiles	47
	AP Groups	48

Chapter 9:	Fixed Telecommuter Solution	50
	Requirements of Fixed Telecommuter Solution	50
	Creating AP Group for RAPs in Fixed Telecommuter Deployments	50
Chapter 10:	Configuring the Remote Employee Role	52
	Configuring the common-dhcp Policy	53
	Configuring the sip-session-allow Policy	54
	Configuring the remote-employee Policy	56
	Configuring the remote-employee Role	57
Chapter 11:	Remote Employee VAP	59
	Forwarding Modes	60
	Tunnel Mode	60
	Split-Tunnel Mode	60
	Bridge Mode	61
	Decrypt-Tunnel Mode	61
	RAP Operation Modes	61
	API/AM Data and Control Tunnels	62
	RAP/AP Tunnels	62
	Remote Employee SSID Profile	63
	Configuring the Remote Employee SSID Profile	64
	Configuring Wi-Fi Multimedia	64
	Configuring the Remote Employee AAA Profile	67
	Authentication Server and Server Groups	67
	Configuring the Server Group for 802.1X Authentication	68
	Configuring the Remote Employee AAA Profile	70
	Configuring the Remote Employee VAP Profile	73
Chapter 12:	Configuring the Guest Role and VAP for Fixed Telecommuter Deployment	75
	Configuring the guest-home-access Policy	76
	Configuring the Guest Role for Fixed Telecommuter Deployments	77
	Configuring the Guest SSID for Fixed Telecommuter Deployments	78
	Configuring the Guest AAA Profile for Fixed Telecommuter Deployments	80
	Configuring the Guest VAP Profiles for Fixed Telecommuter Deployments	82
Chapter 13:	Micro Branch Office Solution	84
	Requirements of Micro Branch Office Deployments	84
	Creating AP Group for RAPs in Micro Branch Office Deployments	84
	Remote Employee Role and VAP Profile for Micro Branch Office Deployments	85

Chapter 14:	Configuring the Guest Roles and VAP Profile for Micro Branch Office Deployments	86
	Configuring the clearpass-guest Policy	88
	Configuring the guest-branch-logon-access Policy	90
	Configuring the block-internal-access Policy for the Guest Role	91
	Configuring the auth-guest-access Policy	92
	Configuring the drop-and-log Policy	94
	Configuring the Initial Guest Role	95
	Configuring the Authenticated Guest Role	96
	Maximum User Sessions for Guest Role	98
	Configuring the Guest SSID Profile for Micro Branch Office Deployments	100
	Configuring the Server Group for Guest Authentication	101
	Configuring the Captive Portal Authentication Profile for Guest WLAN	102
	Configuring the Guest AAA Profile for Micro Branch Office Deployments	105
	Configuring the Guest VAP Profile for Micro Branch Office Deployments	106
Chapter 15:	Configuring the Radio Profiles	108
	Configuring the ARM Profile	108
	Configuring the 802.11a and 802.11g Radio Profiles	113
Chapter 16:	Configuring the AP System Profiles	116
	RF Band	116
	Native VLAN and Remote-AP DHCP Server	117
	RAP Uplink Bandwidth Reservation	119
	Configuring the Uplink Bandwidth Reservation	120
	Remote-AP Local Network Access	122
	Corporate DNS Domain	123
	Configuring the AP System Profile	124
Chapter 17:	Configuring the QoS	127
Chapter 18:	RAP Wired Ports	128
	Configuring the Wired AP Profile	129
	AAA Profile for Wired Ports	132
	Remote Application Role	132
	Configuring the tftp-session-allow Policy	132
	Configuring the Remote Application Role	133
	Corporate AAA Profile for Wired Ports	134
	Guest AAA Profile for Wired Ports	138

	AP Wired Port Profile	139
	Wired Ports for Printer in Micro Branch Office Deployments	141
	Disabling the Wired Ports	142
Chapter 19:	RAP 3G Uplink	144
Chapter 20:	Configuring the AP Group for Telecommuter and Micro Branch Office Deployments	149
	AP-Specific Configuration	153
Chapter 21:	AP Group for Dedicated Air Monitors	155
	Configuring the AM Scanning Profile	156
	Configuring the 802.11a and 802.11g Radio Profiles	158
	Configuring the AP Groups for Air Monitors	160
Chapter 22:	Fallback/Backup Mode for Wireless SSIDs and Wired Ports	162
Chapter 23:	Wireless Intrusion Prevention (IDS Profiles) of RFProtect	166
Chapter 24:	Spectrum Analysis	172
Chapter 25:	RAP Provisioning	176
	Zero-Touch Provisioning	176
	IT Team Tasks for Zero-Touch Provisioning	176
	Onsite Tasks for Zero-Touch Provisioning	177
	Preprovisioning	179
	IT Team Tasks for Preprovisioning	179
	Onsite Tasks for Preprovisioning	181
	Onsite RAP Deployment	181
Chapter 26:	Wide-Area Network Considerations	182
	Bandwidth Constraints	182
	Latency Constraints	182
	3G Wireless Constraints	183
	Recommendations for Minimizing Constraints	183
Chapter 27:	Logging	185
Chapter 28:	AirWave	188
	WMS Offload	189
Chapter 29:	ClearPass Guest	190

Appendix A: Regulatory Compliance	191
Regulatory Compliance for International Deployments	191
AP Compliance	191
Controller Compliance	191
Recommendations for International Deployments	192
Appendix B: RAP Control Traffic	193
Appendix C: Geographical Redundancy for RAP Deployments	194
Geographical Redundancy Design	194
Geographical Redundancy for Global RAP Deployments	197
Recommendations for Geographical Redundancy	198
Appendix D: Broadcast and Multicast Mitigation Features	201
Broadcast-filter ARP (Global Firewall Knob)	201
Drop Broadcast and Multicast (VAP Knob)	203
Convert Broadcast ARP Requests to Unicast (VAP Knob)	204
Broadcast (Wired AP Knob)	205
Suppress-ARP (VLAN Knob)	207
BC-MC Optimization (VLAN Knob)	208
Local-proxy-ARP (VLAN Knob)	209
Appendix E: Contacting Aruba Networks	213
Contacting Aruba Networks	213

Chapter 1: Introduction

The Aruba Validated Reference Design (VRD) series is a collection of technology deployment guides that include descriptions of Aruba technology, recommendations for product selections, network design decisions, configuration procedures, and best practices for deployment. Together these guides comprise a reference model for understanding Aruba technology and designs for common customer deployment scenarios. Each Aruba VRD network design has been constructed in a lab environment and thoroughly tested by Aruba engineers. Our customers use these proven designs to rapidly deploy Aruba solutions in production with the assurance that they will perform and scale as expected.

The VRD series focuses on particular aspects of Aruba technologies and deployment models. Together the guides provide a structured framework to understand and deploy Aruba wireless LANs (WLANs). The VRD series has four types of guides:

- **Foundation:** These guides explain the core technologies of an Aruba WLAN. The guides also describe different aspects of planning, operation, and troubleshooting deployments.
- **Base Design:** These guides describe the most common deployment models, recommendations, and configurations.
- **Applications:** These guides are built 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 Deployments:** These guides involve deployments in conditions that differ significantly from the common base design deployment models, such as high-density WLAN deployments.

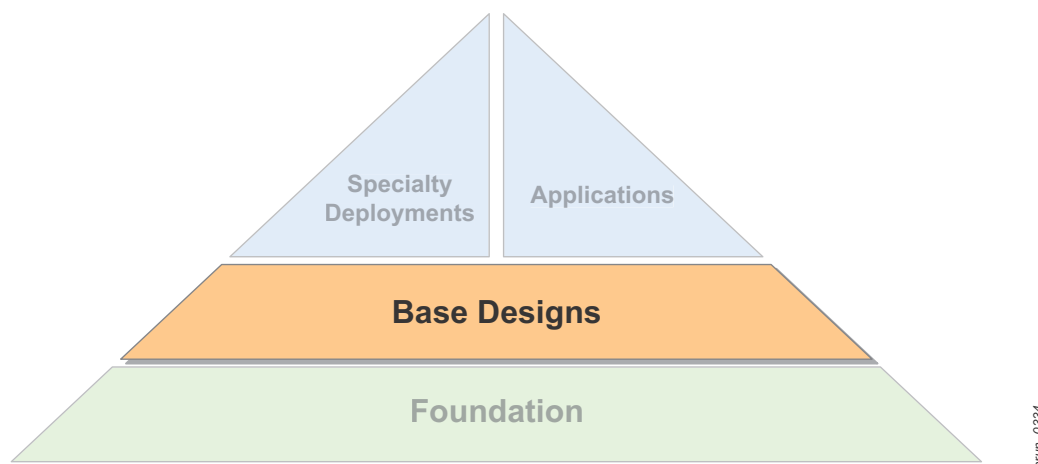


Figure 1 VRD Core Technologies

This guide covers the deployment of Aruba remote access points (RAP) in fixed telecommuter and micro branch office sites, and it is considered part of the base designs guides within the VRD core technologies series. This guide covers the design recommendations for remote network deployment and it explains the various configurations needed to implement a secure, high-performance virtual branch office (VBN) solution with Aruba RAPs.

This guide describes these specific topics:

- recommended remote network design
- controller redundancy and licensing
- VLAN design for remote networks
- configuration of AP groups for fixed telecommuter and micro-branch office deployments
- RAP provisioning

Table 1 lists the current software versions for this guide.

Table 1 Aruba Software Versions

Product	Version
ArubaOS™ (mobility controllers)	6.1
ArubaOS (mobility access switch)	7.1
Aruba Instant™	1.1
MeshOS	4.2
AirWave	7.5
ClearPass Guest (AmigopodOS)	3.9

Reference Material

This guide is a base designs guide, and therefore it will not cover the fundamental wireless concepts. This guide helps a wireless engineer configure and deploy the Aruba RAP solution. Readers should have a good understanding of wireless concepts and the Aruba technology that are explained in the foundation-level guides.

- For information on indoor MIMO WLANs, see the *Aruba 802.11n Networks Validated Reference Design*, available on the Aruba website at <http://www.arubanetworks.com/vrd/>
- For information on Aruba Mobility Controllers and deployment models, see the *Aruba Mobility Controllers and Deployment Models Validated Reference Design*, available on the Aruba website at <http://www.arubanetworks.com/vrd/>
- For specific deployment configuration details, or for deployment models for 802.11a/b/g networks, see the 3.X series of VRDs on the Aruba website at <http://www.arubanetworks.com/vrd/>. The existing VRDs will be updated to follow this new format.
- The complete suite of Aruba technical documentation is available for download from the Aruba support site. These documents present complete, detailed feature and functionality explanations beyond the scope of the VRD series. The Aruba support site is located at: <https://support.arubanetworks.com/>. This site requires a user login and is for current Aruba customers with support contracts.
- For more training on Aruba products or to learn about Aruba certifications, visit the Aruba training and certification page on our website. This page contains links to class descriptions, calendars, and test descriptions: <http://www.arubanetworks.com/training.php/>

- Aruba hosts a user forum site and user meetings called Airheads Social. The forum contains discussions of deployments, products, and troubleshooting tips. Airheads Online is an invaluable resource that allows network administrators to interact with each other and Aruba experts. Announcements for Airheads in person meetings are also available on the site: <http://community.arubanetworks.com/>
- The VRD series assumes a working knowledge of Wi-Fi®, and more specifically dependent AP, or controller based, architectures. For more information about wireless technology fundamentals, visit the Certified Wireless Network Professional (CWNP) site at <http://www.cwnp.com/>

Icons Used in this Guide

Figure 2 shows the icons that are used in this guide to represent various components of the system.

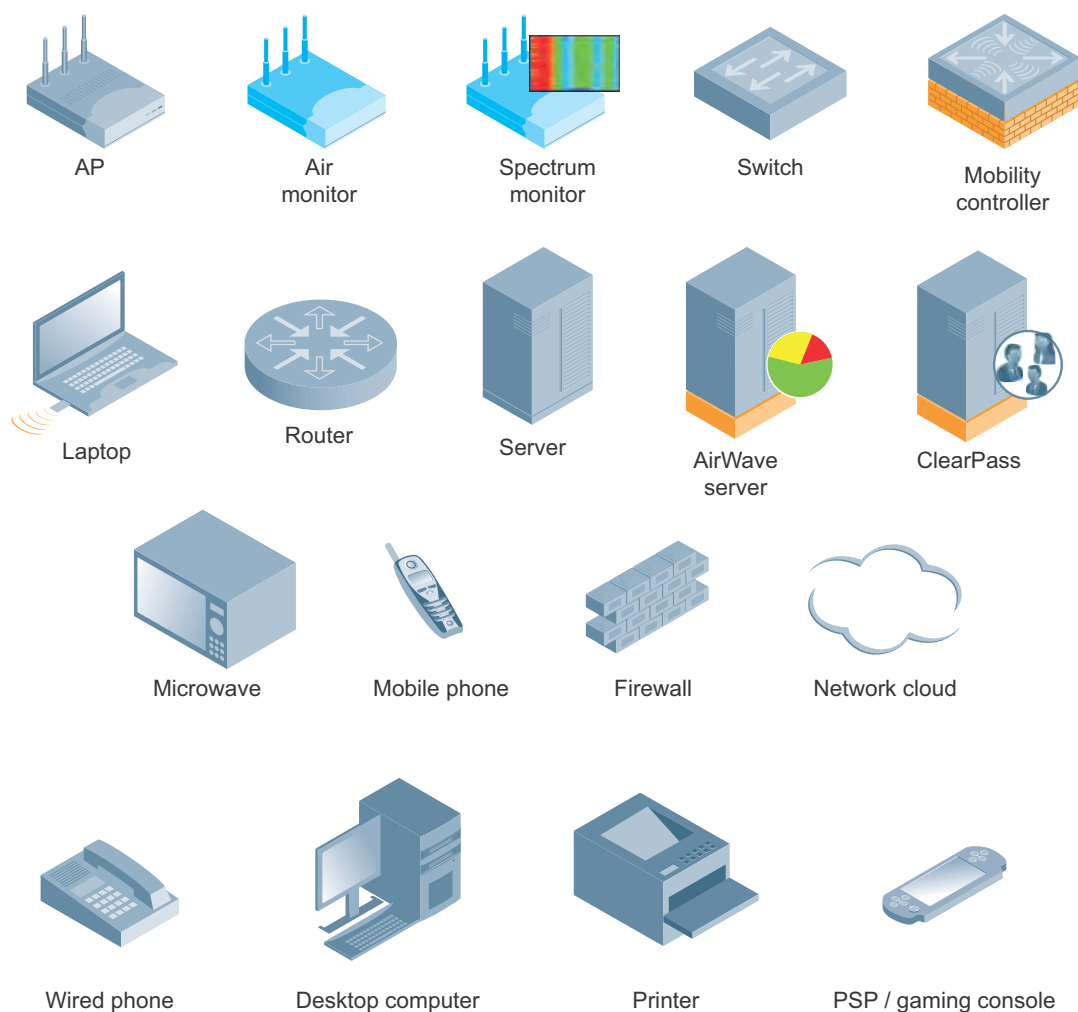


Figure 2 VRD icon set

arun_1078

Chapter 2: Virtual Branch Networks

Users who work from locations other than the organization's primary campus, headquarters facility, or large regional office are called "remote users." Remote users typically work from home offices, small satellite offices, medium-sized branch offices, or on the road from hotels, hot spots, or customer locations. Each of these remote locations has different connectivity, capacity, and usage requirements. In general, we can categorize the remote deployments as follows:

- Fixed telecommuter deployment: a remote worker at home with a few devices
- Micro branch office deployment: a branch office that can be served with a single AP and a few wired ports
- Small and medium branch office deployment: a branch office with less than 250 devices
- Large or regional branch office deployments: a branch office with 250 or more devices and with more complex requirements than a traditional branch office
- Mobile access: secure access to a single device, such as a laptop, by using a virtual private network (VPN) client

IT organizations traditionally have served each category using a different remote network architecture. For example, micro branches used a branch office router to interconnect an IP subnet at the remote site to the corporate network core, while telecommuters with only a single PC or laptop could be served with a software VPN client.

Branch office routers may have been acceptable when there were few mobile workers or mobile devices, however, today's proliferation of mobile devices and users renders them too costly and complex to be satisfactory. Aruba remote network solutions blend the simplicity of a centralized network-based VPN with the flexibility of sophisticated role-based access control to deliver a solution that is economical to deploy and easy to support.

Aruba Virtual Branch Network Solution

The Aruba virtual branch network (VBN) architecture delivers comprehensive IP network services to multidevice and multiuser sites and is simpler to deploy, use, and maintain than the simplest of software VPN solution available in the market. VBN includes four primary components:

- Remote access points (RAPs) extend the corporate LAN to any remote location by enabling seamless wired or wireless data and voice wherever a user finds an Internet-enabled Ethernet port or 3G cellular connection. RAPs are ideally suited for micro remote offices, home offices, telecommuters, mobile executives, and for business continuity applications.
- The Virtual Internet Access (VIA) client for PCs and laptops is a hybrid IPsec/SSL VPN that scans network connections and automatically establishes a VPN connection back to the corporate if the user is connected to an untrusted network. VIA offers a zero-touch end-user experience – just plug and play – and removes the complexity associated with configuring VPN clients on end user devices.
- The Aruba Instant solution uses the virtual controller technology embedded in a standard access point (AP) to create a campus or remote wireless network. Stateful redundancy and enterprise-

grade security and performance make Aruba Instant ideal for small, medium and even large sized branch offices.

- The remote node solution serves the needs of large branch and regional offices. With this solution, the deployment of branch office controllers is as simple as the zero-touch RAP provisioning model. Simply enter the fully qualified domain name (FQDN) of the remote node master controller located at the headquarters, and the remaining provisioning is handled automatically.

Chapter 3: Remote Deployments

The Aruba RAP and VIA solutions cater to the needs of all fixed telecommuter, micro, and mobile access deployments. In these deployments, the Aruba VIA agents and RAPs typically terminate on the master mobility controllers in the network demilitarized zone (DMZ). Similar to the way that campus-based APs and air monitors (AMs) are terminated, the mobility controllers terminate these remote devices coming in over the Internet with IPsec-protected sessions. The Aruba VBN architecture was built to provide high availability. Redundancy may be configured at the controller, at the RAP, or in both places. An all-master design is recommended for remote deployments. For information on other designs such as the master-local design, see the [Aruba Mobility Controllers Validated Reference Design](#). Figure 3 depicts a typical Aruba remote access deployment that provides fixed telecommuter, micro branch office, and mobile access solutions.

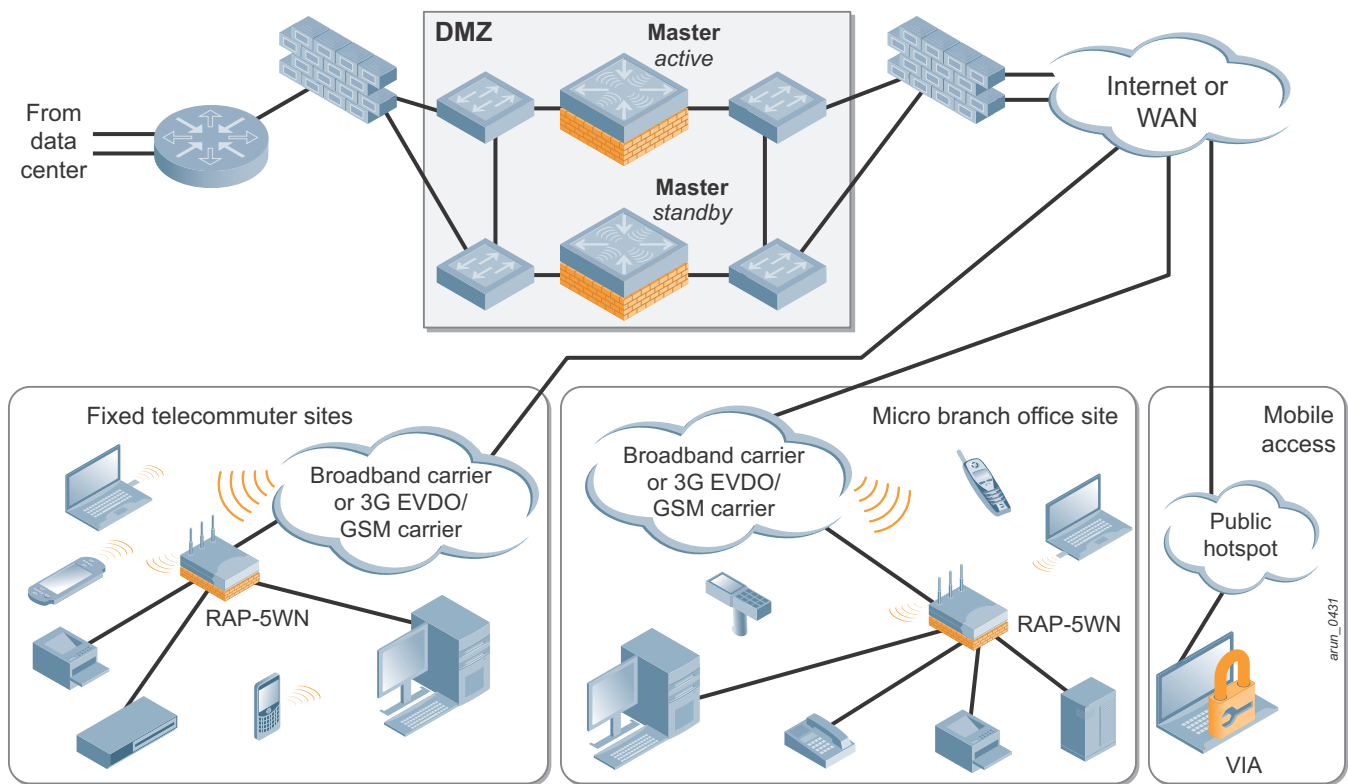


Figure 3 Typical remote deployment with redundancy

This VRD explains the design and configuration of the Aruba RAP solution for remote sites that can be served by a single RAP. [Figure 4](#) shows the remote access deployment explained in this VRD.

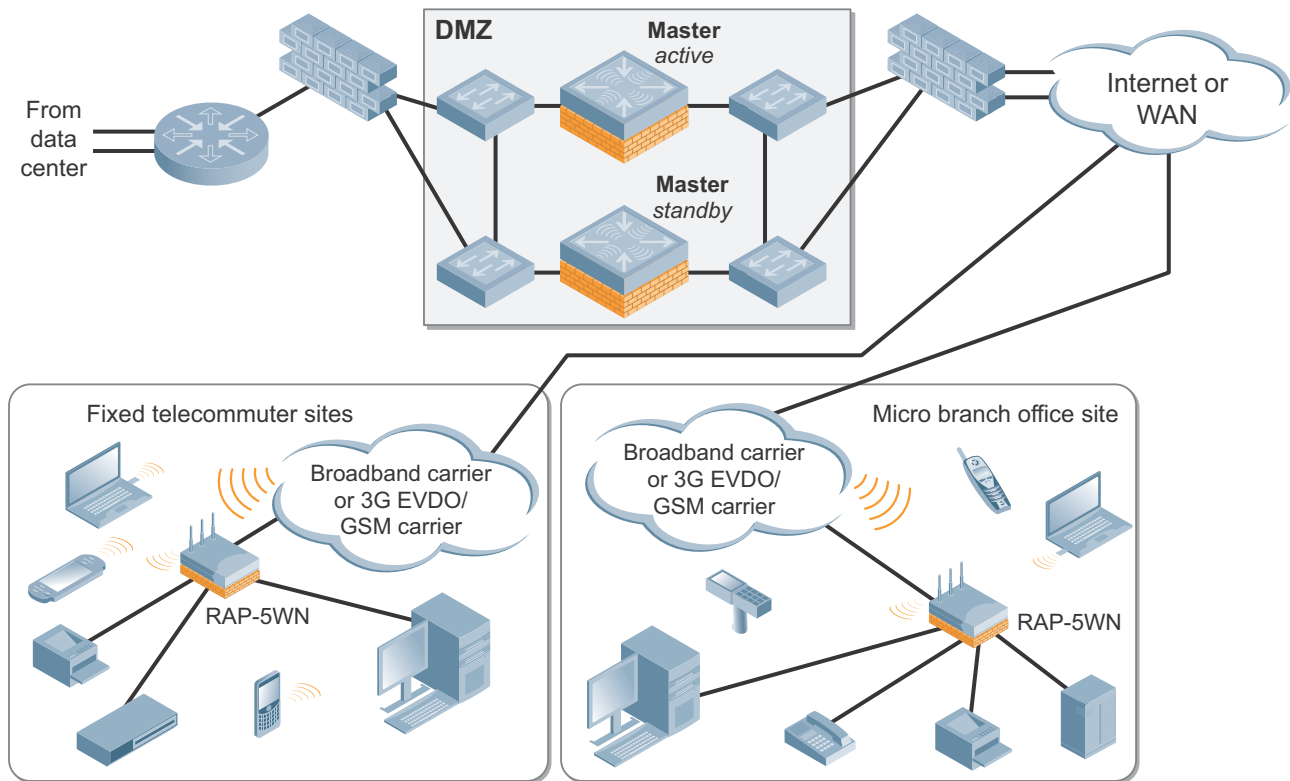


Figure 4 Single RAP deployments



CAUTION

RAPs should never be deployed in succession. In other words, the uplink port of one RAP should not be connected to the Ethernet port of another RAP to share the WAN uplink. This deployment model is not supported by the Aruba RAP solution. For example, if RAP-1 is connected through RAP-2, the IPsec tunnel of RAP-1 will be formed within the IPsec tunnel of RAP-2 and this causes double encryption and decryption of traffic between the controller and RAP-1. The double IPsec encryption and decryption of traffic affects the performance by increasing the fragmentation and delay.

Figure 5 shows the RAP behind a RAP deployment that is not supported by Aruba.

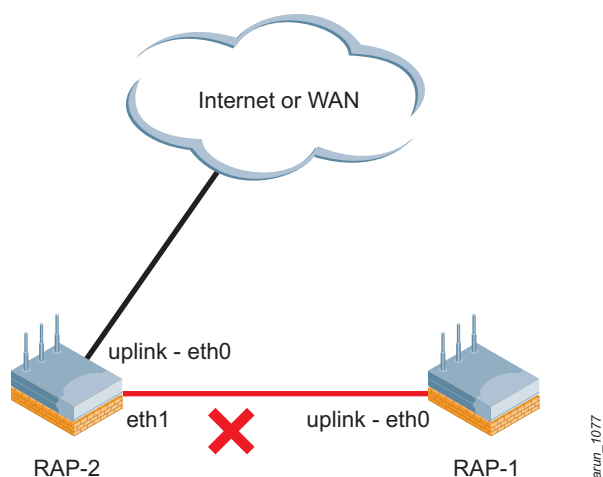


Figure 5 RAP behind a RAP (not supported)

Logical Architecture of Aruba Remote Networks

Figure 6 shows the logical operating model of the Aruba remote network design.

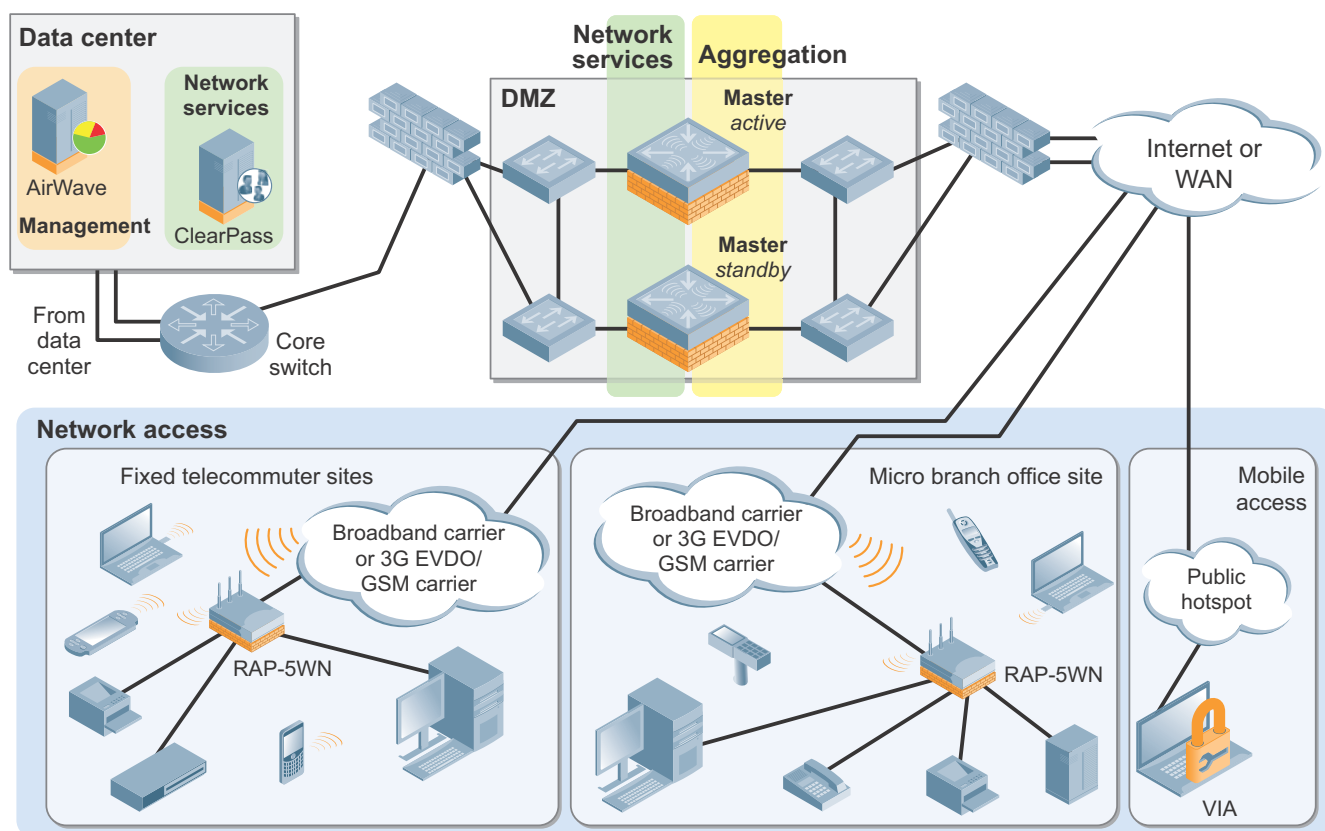


Figure 6 Aruba remote networks logical architecture

Aruba remote networks have a logical four-tier operating model that consists of these four layers:

- **Management:** The management layer consists of AirWave®. AirWave provides a single point of management for the network, including reporting, centralized configuration, and troubleshooting.
- **Network services:** The network services layer consists of master mobility controllers and Clearpass. In remote networks, the master mobility controller in the DMZ acts as a hybrid that belongs to the network services and aggregation layers. The master controllers provide a control plane for the Aruba remote networks. The control plane does not directly deal with user traffic or APs. Instead, the control plane provides services such as whitelist coordination, valid AP lists, CPsec certificates, RFProtect™ coordination, and RADIUS or AAA proxy. ClearPass consists of ClearPass Policy Manager and ClearPass Guest. The ClearPass Policy Manager (CPPM) provides advanced authentication, authorization and accounting (AAA) services and ClearPass Guest offers secure and flexible visitor management services.
- **Aggregation:** The aggregation layer is the interconnect point where the AP, AM, spectrum monitor (SM), and VIA traffic aggregates. In remote networks, the master controller in the DMZ act as aggregation layer controller and terminates all the RAPs and VIA. Secure IPsec-encrypted, generic route encapsulation (GRE) tunnels from RAPs and VIA terminate on controllers at the aggregation layer. These secure tunnels carry traffic back and forth between the controller and the RAPs. This method provides a logical point for enforcement of roles and policies on remote traffic that enters or exits the corporate LAN.
- **Network access:** The network access layer is comprised of RAPs and VIA, which work together with the aggregation layer controllers to overlay the VBN over the WAN. RAPs offer a choice of three different traffic forwarding modes. Tunnel forwarding mode backhauls all traffic to the aggregation layer for processing. When split-tunnel or bridge forwarding modes are used, firewall access control lists (ACLs) in the RAP provide the front line of policy enforcement. All bridge mode traffic with the exception of 802.1X authentication traffic is bridged to the local LAN segment or the Internet and does not reach the aggregation layer. With split-tunnel mode, the traffic destined to the local segment and Internet is bridged locally and only the traffic destined to the corporate network is forwarded to the aggregation layer. RAPs can also serve as AMs and SMs. VIA can operate either in tunnel or split-tunnel forwarding mode.

An example network is used to explain the Aruba VBN solution presented in [Figure 3](#). All networks parameters, screenshots, and command line interface (CLI) examples shown in this VRD are from the VRD example network. For details about the network parameters, design, and setup of the entire VRD example network, see the [Base Designs Lab Setup for Validated Reference Design](#).

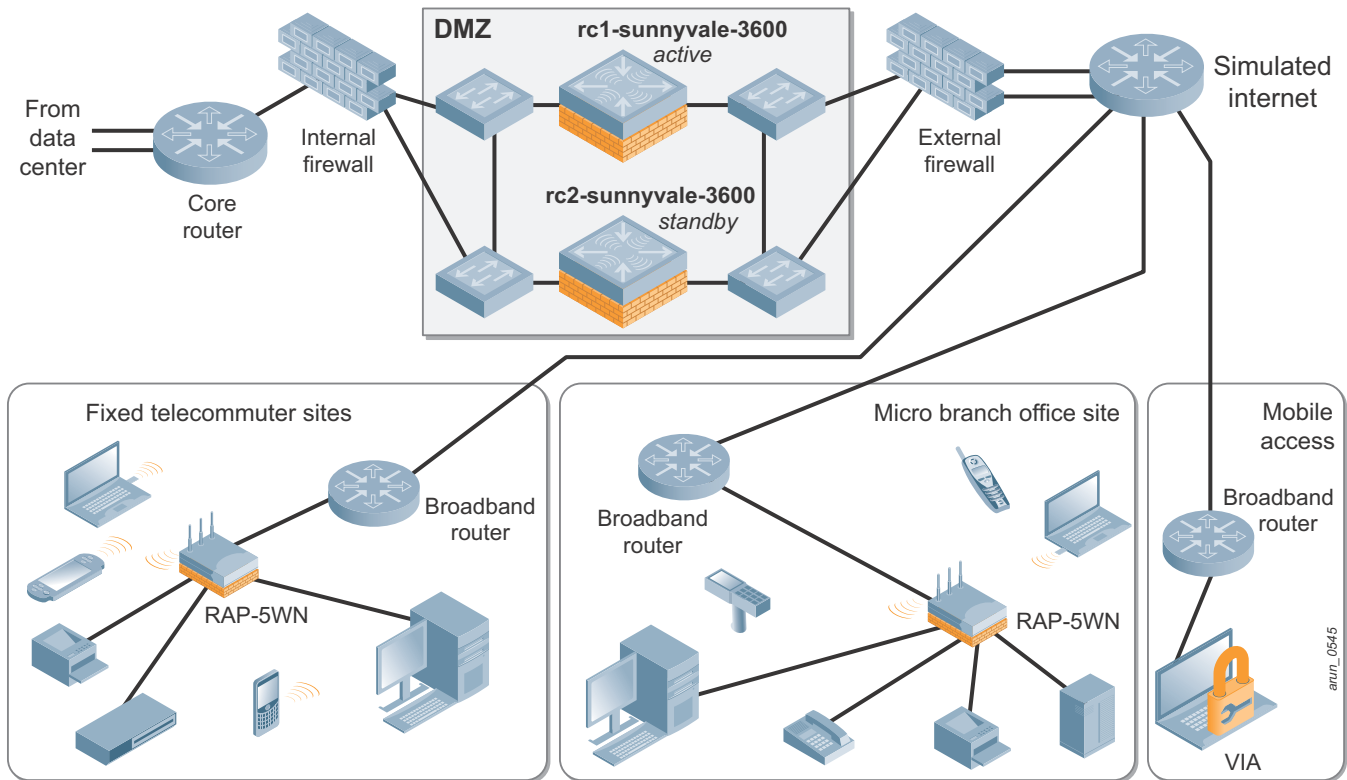


Figure 7 VRD example network for remote deployments

This VRD describes how to configure these solutions:

- **Fixed telecommuter solution using RAPs:** This solution addresses all the needs of telecommuter deployments. It is designed to provide these types of access:
 - Secure wired and wireless access to corporate users and devices by extending the corporate network into employee homes.
 - Local network and Internet access to family members and personal devices
- **Micro branch office solution using RAPs:** This solution addresses all the needs of micro branch office deployments. It is designed to provide these types of access:
 - Secure wired and wireless access to corporate users and devices.
 - Internet access (HTTP/HTTPS) to guest users through captive portal authentication.

For configuration of mobile hotspot solution using VIA, see the [Aruba Virtual Intranet Access \(VIA\) Application Note](#).

RAP Operation

These steps explain how a RAP connects to a controller and how users and devices connect to the corporate network through the RAP.

1. A RAP initiates an IPsec connection to the specified FQDN or public IP address of the controller in the DMZ over any public network. This connection is analogous to the VPN connection initiated by a VPN client on a laptop or desktop to a VPN concentrator. However, for a RAP, there is no single user to be authenticated. Instead, the RAP itself is authenticated on the controller either by using a preprovisioned user name and password on the RAP or by using certificates installed on the RAP. After the RAP is authenticated, the controller assigns an inner IP address to the RAP and an IPsec tunnel is established.
2. A key difference between the Aruba VBN solution and a branch router network is that all configurations are centralized and uploaded to the RAP in real time. No remote configuration is required. After RAP authentication is completed by the controller and the IPsec tunnel has been established, all communication between the controller and the RAP occurs through this secure channel. This encrypted tunnel is now used to download and upgrade the image on the RAP and then to push the RAP configuration from the controller to the RAP. This configuration includes all security settings, firewall roles and policies, wired port policies, and wireless LAN (WLAN) policies. This process is referred to as “bootstrapping” the RAP.
3. After the RAP has bootstrapped successfully to a controller, the RAP applies the configuration it has received to the wired ports and wireless interfaces. Users and devices can now connect to the wired ports and wireless Service Set Identifiers (SSIDs) configured on the RAP during the bootstrap process. The wired ports and RAPs can be configured to provide role-based access control (RBAC). For information on the authentication and encryption types supported on the ArubaOS, see the [Aruba 802.11n Networks Validated Reference Design](#).

The deployment scenario in this VRD portrays the needs of most remote deployments. However, the requirements of each organization are different. Your network may differ from the VRD example network in these ways:

- VLAN and IP parameters
- user density and VLAN pools
- availability, redundancy, and performance requirements
- type of devices on the network
- applications running on the network
- user role requirements
- authentication and encryption requirements
- SSID requirements
- quality of service (QoS) requirements
- intrusion detection and intrusion prevention requirements
- mobility requirements
- network management requirements

Adjust the network parameters and Aruba configurations shown in this VRD to meet your needs.

Key Components of the Architecture

The three key components of this reference model are:

- master controllers
- RAPs
- AMs

Master Controllers

Depending on the size of the remote deployment, any mobility controller can be chosen as the master controller. The master controllers should be deployed in pairs for redundancy. When controllers like MMC-3600 that does not have redundant power supplies are used as the master controllers, it is recommended that you connect each appliance to discrete power sources. When M3 are used as master controllers, each controller in a redundant pair should have its own MMC-6000 chassis. So, two MMC-6000 chassis can accommodate four pairs of redundant controllers. The MMC-6000 chassis should contain redundant power supplies connected to discrete power sources.



M3 controllers that are redundant should not be placed in the same chassis, because a chassis failure will cause the redundancy architecture to fail.

Selecting the proper mobility controller for the deployment depends on a number of factors, including forwarding mode, usage model, and AP count. Take these factors into account to select the proper mobility controller for the application:

- AP count
- user count
- VIA users
- forwarding modes
- data throughput
- mobility controller role

Aruba recommends that VIA and RAP deployments are separated onto different mobility controllers to simplify configuration, deployment, and troubleshooting. When the same controller is used for RAP and VIA termination, the proper calculation of total user count, RAP count, and IPsec tunnels consumed by RAPs/VIA are essential to choose the right controller for your deployment. Remember that the number of supported VIA clients also depends on the configuration of SSL fallback. VIA clients count against the IPsec tunnel limit, but in instances where SSL fallback is enabled, two tunnels must be constructed for each VIA client. For more information on controller selection, see the [Aruba Mobility Controllers Validated Reference Design](#).

RAPs

Aruba offers a wide range of 802.11n APs. Any AP can be configured as a RAP. However, only devices designated with a RAP part number are capable of zero-touch provisioning. The number of radios available, antenna type, MIMO capability, port density, 3G backup capability, and spectrum capability of the APs vary.



APs such as the AP-9x, AP-105, AP-12x and AP-13x series are designed to be mounted on the ceiling to provide the required coverage.

See the Aruba [AP product line matrix](#) to choose the most appropriate AP for your deployment.

AMs

Fixed telecommuter deployments do not require AMs. However, some high-security micro branch office deployments might require dedicated AMs. Dedicated AMs provide full-time surveillance of the air. AMs perform many of the intrusion detection system (IDS) duties for the network, including rogue AP containment. Use the AP-105 as AMs, because these are dual-radio APs with full spectrum analysis support. For details on the spectrum capabilities of all the Aruba APs, see the Aruba [AP product line matrix](#).

Firewall Ports

RAPs connect to the controller on UDP port 4500 for establishing the IPsec connection. So this port should be opened on all the firewalls leading up to the controllers in the DMZ.

Chapter 4: All-Master Design for Remote Networks

An all-master design flattens the network hierarchy and is suitable for remote deployments. An all-master design requires fewer controllers than a master/local design. Though a master/local design is more suitable for campus deployments, the all-master design is the recommended deployment model for remote solutions. In an all-master design, when the network grows past a single pair of redundant controllers, AirWave is recommended. When the WLAN management system (WMS) offload is enabled on the master controllers, AirWave becomes the central point of configuration and monitoring. For information on the limitations of using an all-master design in campus deployments, see the [Aruba Mobility Controllers Validated Reference Design](#).

Controller Licenses

The ArubaOS™ base operating system contains many features and extensive functionality for the WLAN network. Aruba uses a licensing mechanism to enable the additional features and to enable AP capacity on controllers. The controller licensing depends on the AP density and the features needed to operate and secure your network. For more details about Aruba licenses, see [Aruba Mobility Controllers and Deployment Models Validated Reference Design](#).

Licensing Master Mobility Controllers

Licensing unlocks the configuration capabilities on the system. Master mobility controllers used in the remote deployment terminate VAs and APs. So the master mobility controller should be licensed based on these two requirements:

- functionalities required
- number of devices terminated

Only the functionality that is being enabled must be licensed. For example, xSec is deployed primarily only in Federal Government and military installations, and it is not required unless it will be in use at the organization. Master mobility controllers are normally deployed in the active-standby redundancy model, described in [Chapter 6: Redundancy](#). Mobility controllers should be licensed at the maximum expected capacity for that mobility controller. For instance, in a failover scenario, the backup controller must be licensed to accept all the APs that it could potentially host if a failure occurs. As with any system component, it is never a good idea to run the system at maximum capacity and leave no room for future growth. As a general best practice, do not load a controller over 80% of its capacity. In the active-standby redundancy model used for master controllers, the backup master controller should be licensed to the same capacity as the active master controller to accommodate the entire load during failovers. For more information on licensing, see the [Aruba Mobility Controllers Validated Reference Design](#).

In the example network, the master controllers in the DMZ are designed for active-standby redundancy. Table 2 lists the licenses that are used by the active and the standby master controllers in the example network.

Table 2 Master Controller Licensing in the Example Network

License	Capacity rc1-sunnyvale-3600 master controller (preferred active controller)	Capacity rc2-sunnyvale-3600 master controller (preferred standby controller)
AP Capacity	102	102
PEF-NG	102	102
RFPProtect	102	102



The PEFV license is required for every controller in the network that terminates VIA clients. The PEFV license is purchased as a single license that enables the functionality up to the full user capacity of a controller.

Certificates

The Aruba controller comes with a default server certificate. This certificate demonstrates the secure login process of the controller for captive portal, secure shell (SSH), and WebUI management access. This certificate is not for use in a production network. Aruba strongly recommends that you replace this certificate with a unique certificate that is issued to the organization or its domain by a trusted certificate authority (CA).

To receive a custom certificate from a trusted CA, generate a Certificate Signing Request (CSR) on the controller and submit it to the CA. After you receive the digitally signed certificate from the CA, import it to the controller. For more details about generating the CSR and importing certificates, see “Managing Certificates” in the *ArubaOS 6.1 User Guide* available on the Aruba support site.

Chapter 5: VLAN Design and Recommendations

On an Aruba controller at the aggregation layer, VLANs are used in two logically different places:

- the access side of the controller where the APs terminate their GRE tunnels
- the user access side

VLANs are used on the access side of the controller where the APs terminate their GRE tunnels. These VLANs carry traffic between the APs and the controllers. In Aruba VBN networks, the RAPs and VIA connect to the controller through a WAN link. After the initial authentication of the RAPs and VIA, they are assigned an inner IP address. This IP address is assigned from the address pool specified in the VPN server configuration of the controller. For details on configuring VPN server on the controller, see [Chapter 7: Configuring VPN Server on the Controller](#). The controller assigns the inner IP address from the configured pool, so the IP subnets or VLANs defined in this pool must be managed by the controller and these subnets do not require DHCP services. Make sure that the DHCP services are disabled for the IP subnets used in the VPN address pool. In addition to these requirements, the VLANs used in the VPN address pool should be a part of a routable corporate subnet.

VLANs are also used on the user access side. On the user access side, user VLANs exist and traffic flows to and from the users. During authentication, a process that is called “role derivation” assigns the proper VLAN to each user and forwards traffic to the wired network if allowed. For remote networks, the controller in the DMZ or the core switch in the internal network can be made the default gateway for user VLANs. If the DMZ controllers are used as the gateway, the VLAN design recommendations are these:

- Configure Virtual Router Redundancy Protocol (VRRP) for each user VLAN used between a pair of master controllers configured in active-standby redundancy. For details on the active-standby redundancy supported by the master controllers, see [Chapter 6: Redundancy](#).
- Use distinct user VLANs for each pair of controllers. In other words, the user VLANs should be unique to a pair of redundant controllers because it is always important to restrict the broadcast domain to a single pair of redundant master controllers.
- Use a corporate DHCP server to provide DHCP services for the corporate employee networks.
- Ensure that the user VLANs are routable from the internal network.
- Ensure that the subnets used for VPN address pool are routable from the internal network else the VIA clients will not be able to reach corporate destinations and vice-versa.
- When captive portal authentication is required at remote sites, the controllers must be the default gateway and DHCP server for the guest VLAN. For details on configuring captive portal authentication at remote sites, see [Chapter 14: Configuring the Guest Roles and VAP Profile for Micro Branch Office Deployments](#).
- Static routing or Open Shortest Path First (OSPF) can be enabled between the DMZ controllers and the core switch to achieve the required routing. Using OSPF simplifies the configuration.
- OSPF injects a route only for those VLANs whose operational state is up. The presence of a user on a VLAN changes its operational state to up. However, the operational state of the VLAN used in the VPN address pool for RAPs and VIA is not changed to the up state by the presence of a RAP or VIA client. If you need OSPF to inject routes for VLANs that are used as the VPN

address pool, manually change their operational state to up. Alternatively, static routes can be used for these VLAN.

- In an active-standby redundancy model, OSPF routes are injected only by the master of the VRRP instance

If the core switch is used as the gateway, the VLAN design recommendations are these:

- Ensure user VLAN redundancy at the core layer. This can be achieved by using VRRP or any other proprietary technology supported by the core switches.
- Use distinct user VLANs for each pair of controllers because it is always important to restrict the broadcast domain to a single pair of redundant master controllers.
- Ensure that the subnets used for the VPN address pool are routable from the internal network. If they are not, the VIA clients will not be able to reach corporate destinations and vice-versa.
- When captive portal authentication is required at remote sites, the controllers must be the default gateway and DHCP server for the guest VLAN.
- Static routing or OSPF can be enabled between the DMZ controllers and the core switch to have the required accessibility to the VPN address pool.
- OSPF injects a route only for those VLANs whose operational state is up. The operational state of the VLAN used in the VPN address pool for RAPs and VIA is not changed to the up state by the presence of a RAP or VIA client. If you need OSPF to inject routes for VLANs that are used as the VPN address pool, manually change their operational state to up. Alternatively, static routes can be used for these VLAN.
- In an active-standby redundancy model, OSPF routes are injected only by the master of the VRRP instance.



The DHCP services are not synced between the active and standby controller. So do not use the master controller as the DHCP server for the employee network.



If multicast services are required between the corporate headquarters and the remote sites, then the controller must not be the default gateway. In this situation, the upstream router that has multicast routing support should be the default gateway.

VLAN Pooling

The Aruba VLAN pooling feature allows a set of VLANs to be assigned to a designated group of users. VLAN pooling is tied to the virtual AP (VAP). Each VAP on a physical AP can have different VLANs or VLAN pools. VLAN pooling is supported only on tunnel and bridge mode VAPs. VAPs and wired ports in split-tunnel mode, which is the most common forwarding mode in remote deployments, do not support VLAN pooling. For more details about VLAN pooling, see the [Aruba Mobility Controllers Validated Reference Design](#).

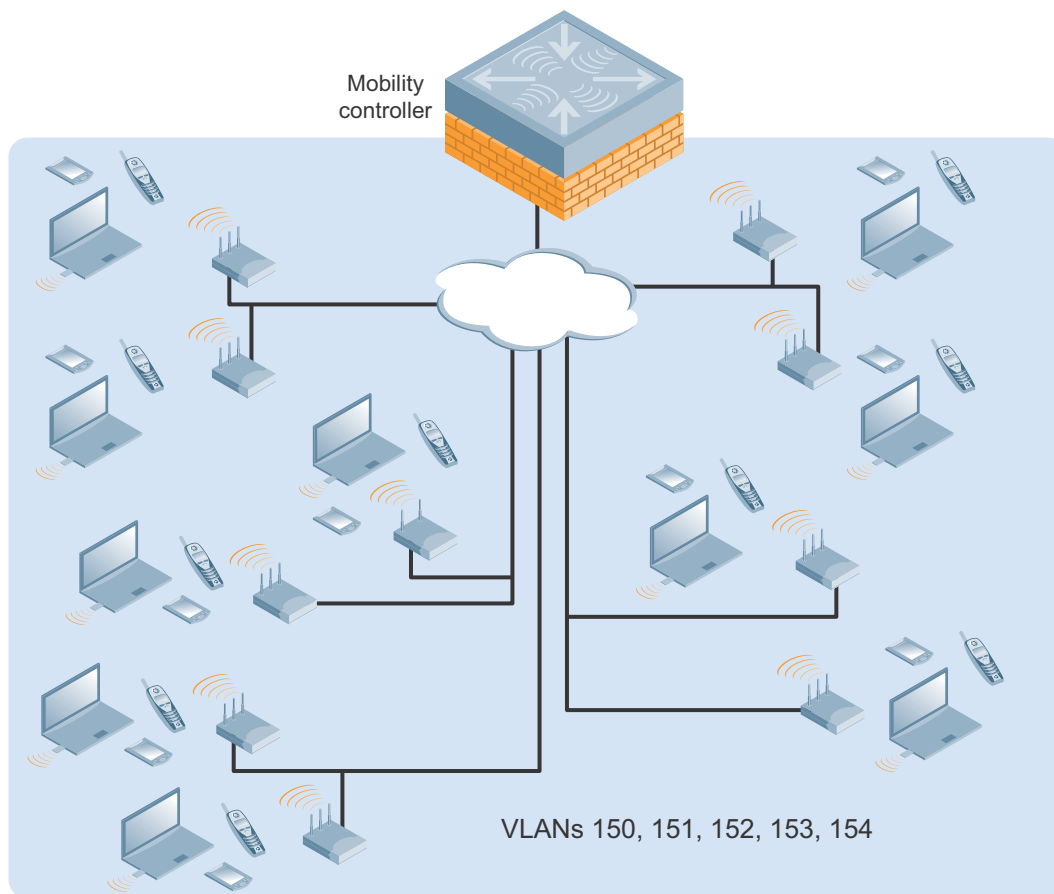


Figure 8 VLAN pools distribute users across VLANs

RAPs extend the corporate Layer 2 network to remote sites. By default, extending a Layer 2 VLAN to a remote location might increase the WAN bandwidth consumption by flooding the broadcast traffic on that VLAN to the remote site. The ArubaOS has several features to limit the flood of broadcast and multicast traffic. For information and recommendations on these features, see [Appendix D: Broadcast and Multicast Mitigation Features](#). WAN bandwidth consumed by broadcast and multicast floods can be further reduced by the use of small IP subnets for user VLANs. In RAP deployments, Aruba recommends the use of small user VLANs (a VLAN for every 64-100 remote devices), whenever possible. Network administrators can achieve this by creating a separate AP group, which does not share its user VLANs with other AP groups, for each set of RAPs that serve a total of 64-100 remote

devices. Though this design increases the number of AP groups and access VLANs, it greatly minimizes the WAN bandwidth consumed by broadcast and multicast floods.



In VLAN pooling, a user is placed into a particular VLAN based on the output of a hash algorithm that uses the media access control (MAC) address of the client. VLANs assigned based on the hashing algorithm cannot be known before connecting to the network. In networks that use VLAN pooling, the clients with static IP addressing might not work because of the possible mismatch between the statically assigned IP and the VLAN assigned by the hashing algorithm. To avoid the possibility of a mismatch in the IP and VLAN configuration, Aruba recommends that static IP addressing should not be used when VLAN Pooling is enabled.

The example network uses the DMZ master controllers as the default gateway for the user VLANs and VRRP is enabled for all user VLANs. OSPF is enabled on the DMZ controllers. The VPN address pool used for RAPs is routable from the internal network. The corporate DHCP server is used to provide DHCP services to the VLANs used for employee network.

Table 3 lists the VLANs that are used in the example network.

Table 3 VLANs in the Example Network

VLANs	IP subnet	DHCP Server	VLANs
131	10.169.131.0/24	static IP	Used for management interface of controllers.
135	10.169.135.0 /24	corporate DHCP server	Used for spit-tunnel VAPs and wired ports in a fixed telecommuter deployment.
136	10.169.136.0 /24	—	Used for VPN address pool.
172	172.16.0.0 / 24	—	Represents the DMZ interface of the controllers.
188	192.168.188.0 /24	RAP	RAP DHCP server VLAN (configured in AP system Profile). Used for the guest network in fixed telecommuter deployments.
700	192.169.70.0 / 24 (rc1-sunnyvale-3600) 192.168.71.0/24 (rc2-sunnyvale-3600)	Controller	Used for guest networks, which provide captive portal authentication, in micro branch office deployments. For details, see Chapter 14: Configuring the Guest Roles and VAP Profile for Micro Branch Office Deployments .

Chapter 6: Redundancy

Aruba offers several redundancy models for controller redundancy. The Aruba redundancy solutions can be implemented using VRRP or backup local management switch (LMS) IP. Use VRRP, which operates at Layer 2, for redundancy whenever possible. For more details about the various redundancy models and when to use backup LMS IP, see the [Aruba Mobility Controllers Validated Reference Design](#).

Master Redundancy

To achieve high availability of the master controller, use the master redundancy model. In this scenario, two controllers are used: one controller is configured as the active master and the other controller acts as standby master. This setup is known as active-standby redundancy. The two controllers run a VRRP instance between them and the database and RF planning diagram is synchronized periodically. The synchronization period is a configurable parameter with a recommended setting of 30 minutes between synchronizations. Aruba recommends active-standby redundancy for the master controllers in the DMZ.

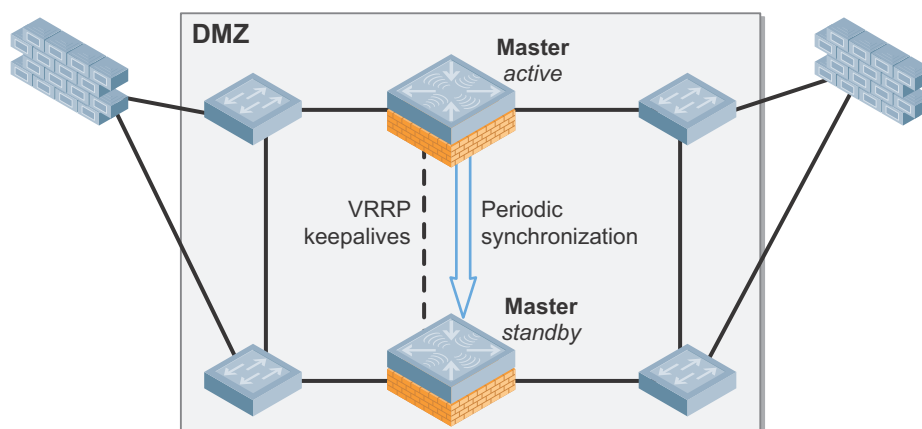


Figure 9 Active-standby redundancy

In this configuration, one controller is always the active master controller and the other is always the standby master controller. When the active controller fails, the standby controller becomes the active master. Aruba controllers support other redundancy models. For more details, see the [Aruba Mobility Controllers Validated Reference Design](#).

In remote networks, the master controllers are in the DMZ and they can be deployed as the default gateway for the user VLANs. In this case, the master controllers have multiple VRRP instances. Each VRRP instance between two controllers determines which controller is the master of that VRRP instance. However, the actual master redundancy, which is the process of electing the master and the backup controller in the active-standby redundancy model, is based on the state of a single VRRP

instance chosen for the purpose. The example network uses active-standby redundancy and has multiple VRRP instances, such as those for internal network, DMZ network, and user VLANs.



The database synchronization synchronizes details such as the AP groups, user roles, profiles, server groups, and internal database to the backup controller. However, details such as the VLAN, IP parameters, VPN address pools, DHCP server parameters and licenses are not synched during database synchronization. Routing parameters such as OSPF and static routes are also not synched during database synchronization. The network administrators should configure these parameters on both the active and standby controllers.

Between redundant controllers deployed in the active-standby redundancy model, it is important to ensure that one controller remains the master of all the VRRP instances at any given time. Network administrators can track the priority of the VRRP instances between controllers to ensure that one controller remains the master of all the VRRP instances. ArubaOS allows you to track VRRP based on these parameters:

- **Time:** When a VRRP instance A is tracked based on time, the priority of that VRRP instance can be increased by X for every Y minutes. Time-based tracking is used whenever only one VRRP instance is between the redundant controllers.
- **State of another VRRP instance:** When VRRP instance A is tracked based on the state of VRRP instance B, the priority of VRRP instance A can be increased by X if VRRP instance B is the master. VRRP tracking based on the state of another VRRP instance is used whenever multiple VRRP instances exist between redundant controllers.
- **State of a VLAN ID:** When VRRP instance A is tracked based on the state of a VLAN ID, the priority of VRRP instance A can be decreased by X if that VLAN ID is the operationally down. VRRP tracking based on the state of a VLAN ID is used whenever multiple VRRP instances exist between redundant controllers. The operational state of a VLAN is up if the associated physical port is up or if a user is on that VLAN. However, the VLAN used as the controller IP is up even if the associated physical port is down and no users are on that VLAN.
- **State of a physical interface:** When VRRP instance A is tracked based on the state of a physical interface, the priority of VRRP instance A can be decreased by X if the operational state of that physical interface is down. VRRP tracking based on the state of a physical interface is used whenever multiple VRRP instances exist between redundant controllers.

In the example network, all the VRRP instances are tracked based on the state of VRRP-172, which is the VRRP instance between the interfaces connected to the external firewall. Pre-emption is disabled on VRRP-172 but is enabled on all the tracked interfaces. The master redundancy is determined based on VRRP-131.

Table 4 through Table 7 summarize the VRRP instances and the database synchronization used for master redundancy in the example network.

Table 4 Master Redundancy Setup

VRRP ID	VRRP IP	Active Controller	Standby Controller	Enable Router Pre-emption	Tracking VRRP Master State ID	Tracking VRRP Master State Priority
131	10.169.131.8	rc1-sunnyvale-3600 (priority 110)	rc2-sunnyvale-3600 (priority 100)	enabled	172	20
135	10.169.135.8	rc1-sunnyvale-3600 (priority 110)	rc2-sunnyvale-3600 (priority 100)	enabled	172	20
172	172.16.1.8	rc1-sunnyvale-3600 (priority 110)	rc2-sunnyvale-3600 (priority 100)	disabled		

Table 5 Master Redundancy Setting on rc1-sunnyvale-3600

Master-VRRP	Peer's IP Address	Peer's IPsec Key
131	10.169.130.7	*****

Table 6 Master Redundancy Setting on rc2-sunnyvale-3600

Master-VRRP	Peer's IP Address	Peer's IPsec Key
131	10.169.130.6	*****

Table 7 Database Synchronization Parameters

Enable Periodic Database Synchronization	Database Synchronization Period in Minutes	Include RF Plan Data
enabled	30	enabled

The reason for tracking all the VRRP instances based on the VRRP instance between the interfaces of the controllers connected to the external firewall can be explained using [Figure 10](#).

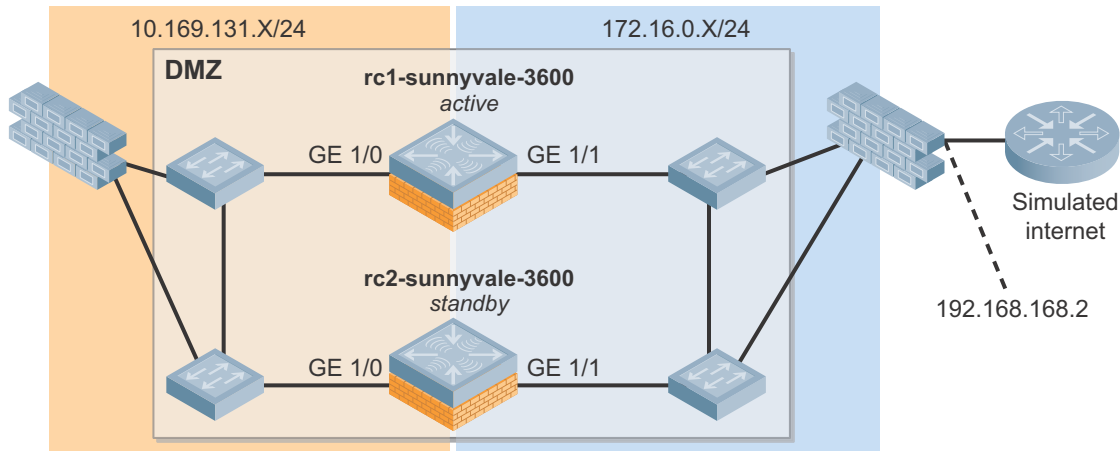


Figure 10 DMZ-setup

Consider the following setup for the [Figure 10](#):

- GE 1/0 on rc1-sunnyvale-3600 belongs to VLAN 131 with IP 10.169.131.6.
- GE 1/0 on rc2-sunnyvale-3600 belongs to VLAN 131 with IP 10.169.131.7.
- Virtual IP (VIP) for VRRP-131 between the VLAN 131 on rc1-sunnyvale-3600 and rc2-sunnyvale-3600 is 10.169.131.8.
- VRRP-131 is used to track master redundancy.
- GE 1/1 on rc1-sunnyvale-3600 belongs to VLAN 172 with IP 172.16.0.6.
- GE 1/1 on rc2-sunnyvale-3600 belongs to VLAN 172 with IP 172.16.0.7.
- VIP for VRRP-172 between VLAN 172 on rc1-sunnyvale-3600 and rc2-sunnyvale-3600 is 172.16.0.8.
- VRRP-135 and other such VRRP instances are used to provide user VLAN redundancy.
- The controller rc1-sunnyvale-3600 has higher VRRP priority for all the VRRP instances and is the preferred master.

When the GE1/1 of rc1-sunnyvale-3600 fails, rc2-sunnyvale-3600 becomes the master for VRRP-172. The master state of all the other VRRP instances including VRRP-131 is tracked based on VRRP-172, so the VRRP priority of rc2-sunnyvale-3600 for all the VRRP interfaces exceeds that of rc1-sunnyvale-3600. Pre-emption is enabled on all the tracked interfaces, so rc2-sunnyvale-3600 becomes the master for all the VRRP instances, including VRRP-131, which defines master redundancy.

There may be situations when the GE 1/0 of rc1-sunnyvale-3600 fails, in this case the rc2-sunnyvale-3600, becomes the master for VRRP-131, but rc1-sunnyvale-3600 will remain the master for all other VRRP interfaces. When this occurs, the RAPs come up but the users will not be able to reach to internal network. Whenever remote users have this type of connectivity issue to the internal network, follow this troubleshooting step: login through the VRRP instance that determines master redundancy (VIP of the VRRP-131 in the above example) and ensure that a single controller is the master for all VRRP instances.

In this example, if the VRRP of all the interfaces are tacked based on VRRP-131 and if GE 1/1 of rc1-sunnyvale-3600 fails, none of the RAPs come up. This happens because rc2-sunnyvale is the master for VRRP-172, but it is still the backup controller because rc1-sunnyvale-3600 is still the master for VRRP-131.

CLI

rc1-sunnyvale-3600

```
!  
master-redundancy  
master-vrrp 131  
peer-ip-address 10.169.130.7 ipsec *****  
!  
vrrp 131  
    priority 110  
    ip address 10.169.131.8  
    description "preferred-master"  
    vlan 131  
    preempt delay 0  
    tracking vrrp-master-state 172 add 20  
    no shutdown  
!  
vrrp 135  
    priority 110  
    ip address 10.169.135.8  
    description "user-VLAN-master"  
    vlan 135  
    preempt delay 0  
    tracking vrrp-master-state 172 add 20  
    no shutdown  
!  
vrrp 172  
    priority 110  
    ip address 172.16.1.8  
    description "DMZ-ip-master"  
    vlan 172  
    no shutdown  
!
```

rc2-sunnyvale 3600

```
!  
master-redundancy  
master-vrrp 131  
peer-ip-address 10.169.131.6 ipsec *****  
!  
vrrp 131  
    priority 110  
    ip address 10.169.131.8  
    description "preferred-backup"  
    vlan 131  
    preempt delay 0  
    tracking vrrp-master-state 172 add 20  
    no shutdown  
!  
vrrp 135  
    priority 110  
    ip address 10.169.135.1  
    description "user-VLAN-backup"  
    vlan 135  
    preempt delay 0  
    tracking vrrp-master-state 172 add 20  
    no shutdown  
!  
vrrp 172  
    priority 110  
    ip address 172.16.1.8  
    description "DMZ-ip-backup"  
    vlan 172  
    no shutdown  
!
```

WebUI Screenshot

oring

Configuration

Diagnostics

Maintenance

Plan

Save Configuration

Advanced Services > Redundancy > Edit (131)

1

Edit Virtual Router

Virtual Router Id

131

Advertisement Interval (secs)

1

Authentication Password

ype NONE *****

Description

preferred-master

IP Address

10.169.131.8

Enable Router Pre-emption

☒ Delay 0

Priority

110

Admin State

UP

VLAN

131

Tracking Master Up Time

Tracking Master Up Time Priority

Tracking VRRP Master State ID

172

Tracking VRRP Master State Priority

20

Tracking VLAN

VLAN Id	Subtract	Actions
New		

Tracking Interface

Interface	Subtract	Actions
New		

Figure 11 VRRP-131 setup

Aruba Networks, Inc.

Redundancy | 33

Configuration

Diagnostics

Maintenance

Plan

Save Configuration

Advanced Services > Redundancy > Edit (135)

Virtual Router Id

Advertisement Interval (secs)

Authentication Password

Description

IP Address

Enable Router Pre-emption

Priority

Admin State

VLAN

Tracking Master Up Time

Tracking Master Up Time Priority

Tracking VRRP Master State ID

Tracking VRRP Master State Priority

135

1

ype NONE *****

user-VLAN-maste

10.169.135.1

☒

 Delay 0

110

UP

135

172

20

Tracking VLAN

VLAN Id	Subtract	Actions
New		

Tracking Interface

Interface	Subtract	Actions
New		

Figure 12 VRRP-135 setup

Configuration

Diagnostics

Maintenance

Plan

Save Configuration

Advanced Services > Redundancy > Edit (172)

Virtual Router Id

Advertisement Interval (secs)

Authentication Password

Description

IP Address

Enable Router Pre-emption

Priority

Admin State

VLAN

Tracking Master Up Time

Tracking Master Up Time Priority

Tracking VRRP Master State ID

Tracking VRRP Master State Priority

172

1

ype NONE *****

DMZ-ip-master

172.16.1.8

☐ Delay

110

UP

172

Tracking VLAN

VLAN Id	Subtract	Actions
New		

Tracking Interface

Interface	Subtract	Actions
New		

Figure 13 VRRP-172 setup

MOBILITY CONTROLLER | rc1-sunnyvale-3600

ring **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Logout admin](#)

Advanced Services > Redundancy

Virtual Router Table

Router Name	IP Address	VLAN	Admin State	Operational State	Action
131	10.169.131.8	131	UP	MASTER	Edit Delete
135	10.169.135.8	135	UP	MASTER	Edit Delete
172	172.16.1.8	172	UP	MASTER	Edit Delete

[Add](#)

Database Synchronization Parameters

Enable periodic database synchronization ☒Database synchronization period in minutes Include RF Plan data ☒

Master Redundancy

Master VRRP	131
Peer's IP Address	10.169.131.7
Peer's IPsec Key	
Retype Peer's IPsec Key	

[Apply](#)

Figure 14 rc1-sunnyvale-3600 VRRP setup

MOBILITY CONTROLLER | rc2-sunnyvale-3600

toring **Configuration** Diagnostics Maintenance Master Switch [Save Configuration](#) [Logout admin](#)

Advanced Services > Redundancy

Virtual Router Table

Router Name	IP Address	VLAN	Admin State	Operational State	Action
131	10.169.131.8	131	UP	BACKUP	Edit Delete
135	10.169.135.1	135	UP	INIT	Edit Delete
172	172.16.1.8	172	UP	BACKUP	Edit Delete

[Add](#)

Database Synchronization Parameters

Enable periodic database synchronization ☒Database synchronization period in minutes Include RF Plan data ☒[Apply](#)

Commands

[View Commands](#)

Figure 15 rc2-sunnyvale-3600 VRRP setup

Chapter 7: Configuring VPN Server on the Controller

Several tasks are involved in configuring a VPN solution using RAPs. In general, all the tasks necessary to deploy a RAP solution can be consolidated into these four major steps:

- Configuring the VPN server on the controller
- Configuring the AP group for RAPs
- RAP Provisioning
 - Zero-touch provisioning
 - Preprovisioning
- Onsite RAP Deployment

This chapter explains the configuration of the VPN server on the controller. The other tasks required to deploy the RAP solution are covered in the following chapters.

Configuring the VPN Server on the Controller

The RAPs, VIA and third-party VPN clients connect to the controller through the public Internet. So, the communication between the RAPs/VIA/third-party VPN clients and the controller is secured using the VPN technology. The VPN server portion of the VPN design is represented by the controller while the third-party VPN clients, the RAPs, and VIA agents represent the VPN clients that request access to the VPN server.

RAP Bootstrapping

Before you configure the VPN settings, it is important to understand the phases of the RAP bootstrapping process:

1. The RAP obtains an IP address on the wired interface (Eth 0) by using DHCP. In remote deployment scenarios, the IP address is typically provided by the Internet service provider (ISP) when directly connected to the Internet.
2. The RAP can be provided with an FQDN or a static IP of the master controller. If a FQDN is used, the RAP resolves the host name by using the DNS service provided by the ISP.
3. The RAP attempts to form an IPsec connection to the master controller through the Ethernet interface.
 - a. Depending on the provisioning type, either the RAP's certificate or Internet Key Exchange (IKE) PSK is used to complete IKE phase 1 negotiation.
 - b. XAuth, which is an extension to the IKE phase 1, is used to authenticate the RAP. If IKE PSK is used, XAUTH authenticates with username and password. If authentication is successful, the RAP gets an inner IP address and an IKE SA is established between it and the controller. If certificate is used, XAUTH authenticates the MAC address in the CERT against the RAP whitelist. If authentication is successful, the RAP gets an inner IP address and an IKE SA is established between it and the controller.

4. An IPsec SA is then established between the RAP and the controller.

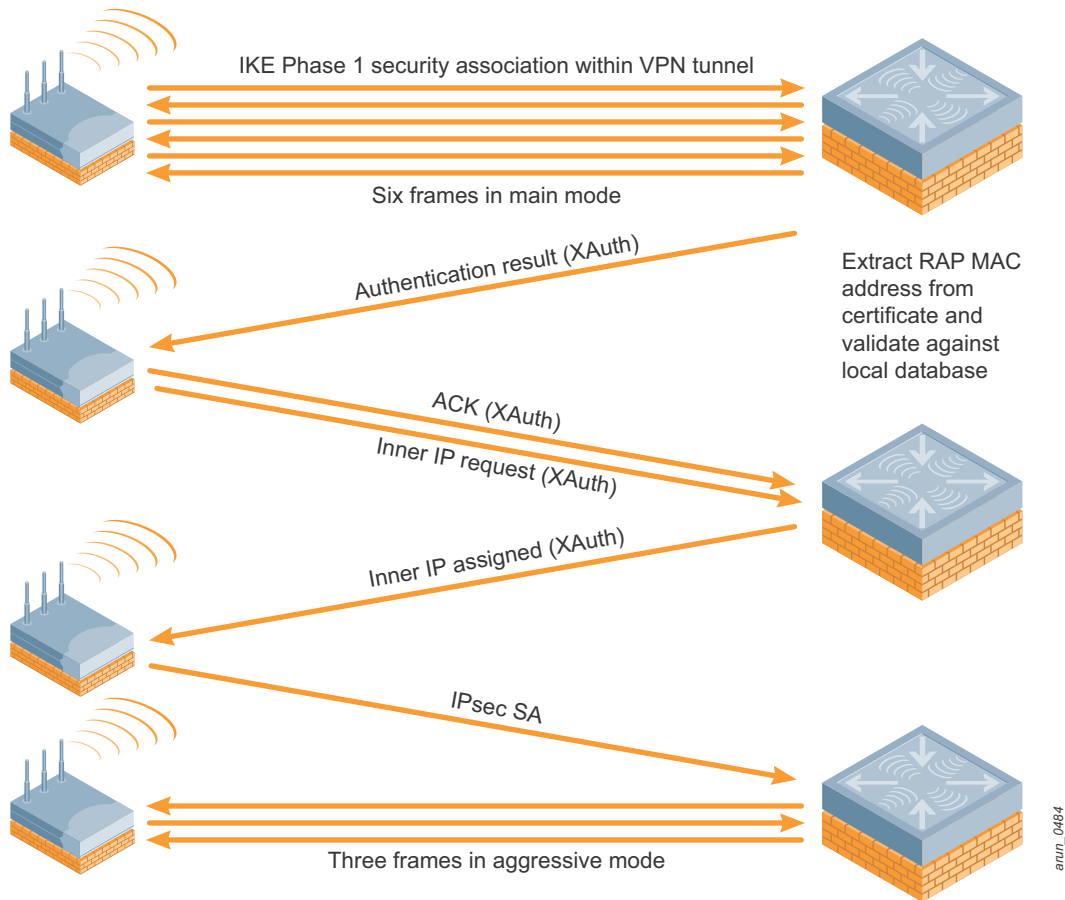


Figure 16 RAP bootstrapping

5. The master controller provides the RAP with the IP addresses of the controller (LMS and backup LMS IP) on which it should terminate. In remote deployments where the master also terminates RAPs, this is the same controller.
6. One or more IPsec-encrypted GRE tunnels are formed between the RAP and the designated controller depending on the configuration. For information on the various tunnels formed by a RAP, see [AP/AM Data and Control Tunnels on page 62](#).



In ArubaOS 6.1 and later, RAPs provisioned using certificates implement IKE version 2 instead of the IKE version 1 that was used in the prior releases.

VPN Server Configuration

At the minimum, these parameters should be configured in the VPN server of the controller:

- L2TP and XAUTH parameters (required only for VIA and third-party VPN clients)
- address pools
- IKE aggressive group name
- IKE shared secret

L2TP and XAUTH Parameters

The L2TP and XAUTH settings available in the VPN server module of the ArubaOS are applicable only for VIA and third-party VPN clients. RAPs use XAUTH by default and this cannot be altered. The enable L2TP and enable XAUTH parameters do not affect the behavior of RAPs. For RAP deployments, the L2TP and XAUTH settings can be omitted.

By default, IKEv1 VIA clients use XAUTH with IPsec tunnel mode to establish secure VPN connections to the controller. So, if VIA clients are terminated on the controller, the enable XAUTH parameter should be enabled. If any third-party L2TP clients are terminated on the controller, the enable L2TP should be enabled. The DNS server options of the L2TP/XAUTH parameters must be configured, with the appropriate corporate DNS servers, for use by VIA and other third-party VPN clients that connect to the controller. Without the DNS server information, VIA cannot resolve the DNS queries for tunneled networks. DNS configuration is required only for VIA and third-party VPN client deployments. Remember that VIA supports multiple authentication methods and IKE versions. For more details on VIA, see the [Aruba Virtual Intranet Access \(VIA\) Application Note](#).

Address Pools

Every RAP, VIA, and third-party VPN client that authenticates successfully to the VPN server module of the controller is given a valid inner IP address and DNS server information. This inner IP address is issued from the address pool that is configured in the VPN server. More than one pool can be configured and there is no need to assign more addresses in the pool than the number of remote APs or VIA clients in the network.

If only a single pool is configured, all the VPN clients (RAPs, VIA, and other third-party clients) are issued an inner IP address from the same pool. When multiple address pools are configured, the controller can be configured to use distinct VPN pools for RAPs, VIA, and third-party VPN clients. This configuration can be achieved by appending a VPN pool to the role assigned to the RAPs, VIA and third-party VPN clients. However, the ability to define a distinct VPN address pool for RAPs depends on whether CPSEC is enabled or not. For more details, see [Default Role for Authenticated RAPs on page 44](#)”

When distinct VPN pools are not defined, the controller automatically uses the first pool in the VPN address pool. When this pool expires, the next pool in the list is used and so on. Remember that if the VPN address pool is exhausted, new RAPs or VIA clients cannot establish the IPsec tunnel until the required number of IP addresses are added to the pool. In the example network, the remote-pool is used for the inner IP address of the RAPs.



CAUTION

Like the VLAN and IP parameters, the VPN address pools are not synced from the active controller to the standby controller during database synchronization. Create VPN address pools individually on both the active and standby master controllers. The VPN pools used on the active and the backup controller are not required to be the same.

IKE Aggressive Group Name

IKE aggressive group name is a feature used by certain legacy VPN clients that require an aggressive mode group name. This parameter is not used by RAPs or VIA. However, this field cannot be empty and requires a value. The default value is “changeme”. In the example network, the IKE aggressive group name is set to the default value.

IKE Shared Secret

For VIA and RAPs that are preprovisioned using PSK, a part of the IPsec process requires the VPN client to present a shared secret. Aruba allows you to configure keys that are specific to a subnet or you can specify a global key. The example network uses a global key. To make the IKE key global, specify 0.0.0.0 for the subnet and subnet mask length fields. Remember, for VIA using IKE version 1 with PSK and RAPs provisioned using PSK, IKE shared secret should be configured for the IPsec tunnel to be established.



The IKE security association (SA) and IPsec SA parameters can be customized.

CLI

```
!  
crypto isakmp key "*****" address 0.0.0.0 netmask 0.0.0.0  
!  
crypto isakmp groupname Changeme  
!  
ip local pool "remote-pool" 10.169.136.50 10.169.136.254  
!
```

WebUI Screenshot

ABILITY CONTROLLER | rc1-sunnyvale-3600

g **Configuration** Diagnostics Maintenance Plan [Save Configuration](#)

Advanced Services > VPN Services > IPSEC

IPSEC PPTP Dialers Emulate VPN Servers Site-To-Site VIA Advanced

L2TP and XAUTH Parameters

Enable L2TP ☐

Enable XAuth ☐

Authentication Protocols ☐ PAP ☐ EAP ☐ CHAP ☐ MSCHAP ☐ MSCHAPv2

Primary DNS Server 10.169.130.4

Secondary DNS Server 0.0.0.0

Primary WINS Server 0.0.0.0

Secondary WINS Server 0.0.0.0

Address Pools

Pool Name	Start Address	End Address	Action
remote-pool	10.169.136.50	10.169.136.254	Edit Delete
			Edit Delete

[Add](#)

Source NAT

Enable Source NAT ☐

NAT Pool

NAT-T

Enable NAT-T ☐

Aggressive Mode

IKE Aggressive Group Name changename (Only needed for XAUTH)

IKE Server Certificate

IKE Server Certificate Assigned for VPN-Client --NONE--

CA Certificate Assigned for VPN-Clients

CA Certificate	Action
None found	

[Add](#)

IKE Shared Secrets

Subnet	Subnet Mask Length	Key	Action
0.0.0.0	0	*****	Edit Delete

[Add](#)

IKE Policies

Version	Priority	Encryption	Hash	Authentication	PRF	Group	Lifetime(s)
v1	20	AES256	SHA	PRE-SHARE	--	GROUP 2	[300 - 86400]
v1	Default	3DES	SHA	PRE-SHARE	--	GROUP 2	[300 - 86400]
v1	Default RAP 10002	AES256	SHA	RSA	--	GROUP 2	[300 - 86400]
v1	Default RAP 10003	AES256	SHA	PRE-SHARE	--	GROUP 2	[300 - 86400]
v2	Default RAP 10004	AES256	SHA	RSA	PRF-HMAC-SHA1	GROUP 2	[300 - 86400]
v1	Default Cluster	AES256	SHA	PRE-SHARE	--	GROUP 2	[300 - 86400]

Figure 17 VPN server configuration

Configuring the VPN Authentication Profiles

When the VPN clients (RAPs, VIA, and third-party VPN clients) submit authentication credentials, the VPN server on the controller has to validate them against an authentication server and assign a user role to the authenticated clients. The VPN authentication profiles in the ArubaOS define the user role assigned for authenticated VPN clients, an authentication server, and the server group to which the authentication server belongs. The three predefined VPN authentication profiles are:

- default: for VIA and third-party VPN clients
- default-cap: for campus APs (CAPs)
- default-rap: for RAPs

These three profiles allow the use of different authentication servers, user roles, and IP pools for VIA clients, CAPs, and RAPs.



Additional VPN profiles cannot be added. The default and default-rap profiles are configurable, but the default-cap profile cannot be edited.

Authentication Servers

RAPs can be provisioned either using the zero-touch provisioning or preprovisioning. The authentication servers used for authenticating the RAPs itself depends on the type of provisioning. For details on these provisioning methods, see [Chapter 24: Spectrum Analysis](#).

While preprovisioning the RAPs, you configure IPsec settings for the RAPs, including the username and password. This username and password must be validated by an authentication server before the RAPs are allowed to establish a VPN tunnel to the controller. In this case, the authentication server can be any type of server supported by the controller such as RADIUS, LDAP, TACACS servers, or the internal database of the controller.

For zero-touch provisioning, the RAP whitelist is used instead of the username and password for authenticating the RAPs. When zero-touch provisioning is used, the authentication server can be only the internal database of the controller. If an organization needs to terminate preprovisioned and zero-touch provisioned RAPs on the same controller, then only the internal database of the controller can be used as the authentication server for RAPs.

For VIA and third-party VPN clients, any authentication server supported on the controller can be used. The example network uses an internal database for RAPs.

Table 8 summarizes the allowed combination of authentication servers if you need to deploy VPN clients, RAPs using PSK, RAPs using certificates, and CAPs on the same controller.

Table 8 Server Combination for VPN Authentication Profiles

Controller	Authentication Server Used for VIA and Third-Party VPN Clients	Authentication Server Used for RAPs Using PSK	Authentication Server Used for RAPs Using Certificates	CAP
Controller A	External AAA server 1	LocalDB	LocalDB-AP	CPSEC-whitelist
Controller B	External AAA server 1	External AAA server 1	not supported	CPSEC-whitelist
Controller C	External AAA server 1	External AAA server 2	not supported	CPSEC-whitelist
Controller D	LocalDB	LocalDB	LocalDB-AP	CPSEC-whitelist
Controller E	LocalDB	External AAA server 1	not supported	CPSEC-whitelist

Table 8 shows that if the internal database is used as the authentication server for default-rap profile, RAPs using PSK and those using certificates can be supported on the same controller. However, if an external server is used as the authentication server for default-rap profile, only RAPs using PSK can be supported on that controller. It also clear from the Table 8 that the authentication servers used for VIA and third-party VPN clients do not influence whether both RAPs using PSK and certificates can be supported on the same controller. Campus controllers using control plane security (CPSEC) use the CPSEC-whitelist by default and this cannot be modified.

Table 9 summarizes the authentication server used in the example network for the default-rap VPN authentication profile.

Table 9 Authentication Server Used for RAPs

VPN Authentication Profile	Authentication Server Group	Authentication Server
default-rap	default	internal

Default Role for Authenticated RAPs

The role that is assigned to the RAP after it has established an IPsec connection and after it has successfully authenticated to the controller is dependent on CPsec. If CPsec is disabled on the controller, the RAP is assigned the ap-role (predefined role) for its internal IP address and the logon role to its default IP address (IP address that initiated the IPsec connection). If CPsec is enabled on the controller, it is assigned the sys-ap-role (predefined role) for its internal IP address and the logon role to its default IP address (IP address that initiated the IPsec connection). The default role that is assigned to RAPs is not configurable. VPN address pools can be appended to the ap-role but not to the sys-ap-role.



The check certificate common name against AAA server parameter is responsible for authenticating the MAC address of certificate based RAPs against the RAP whitelist. If this is disabled, RAPs will be authorized even if their MAC addresses are absent in the RAP whitelist. Aruba recommends that you enable this parameter in all deployments to ensure that only authorized RAPs connect to the controller.

CLI

```
!
aaa authentication vpn "default-rap"
    server-group "default"
    cert-cn-lookup
!
```

WebUI Screenshot

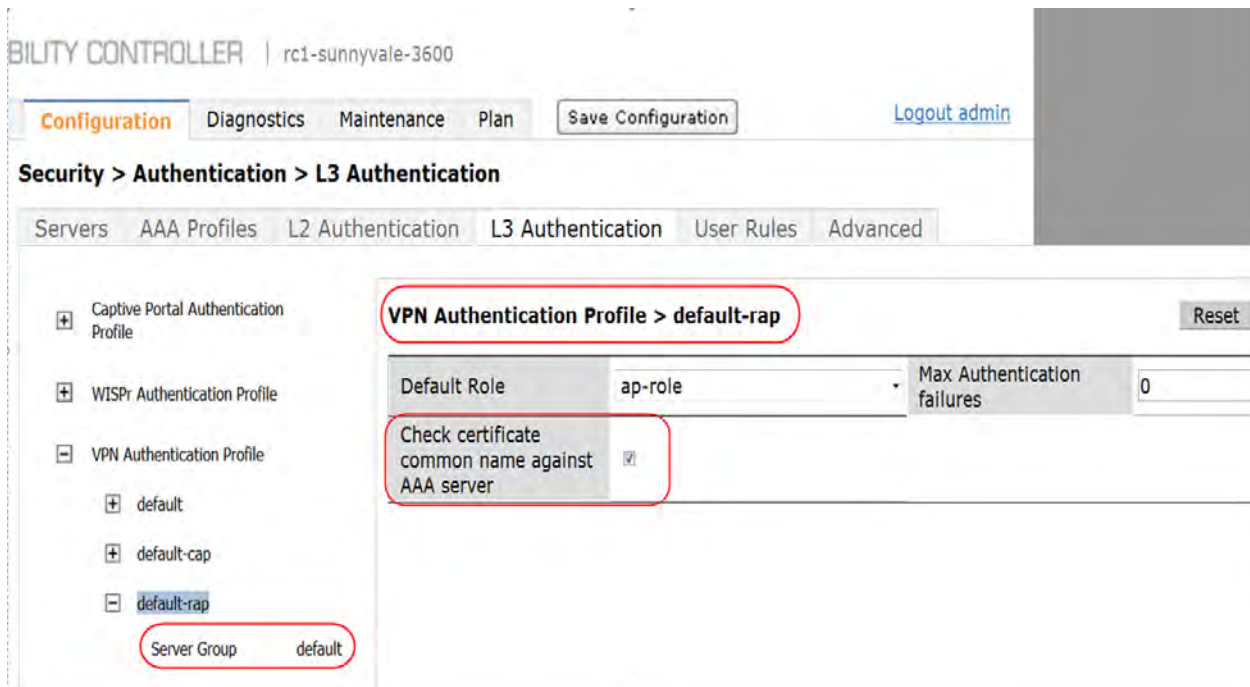


Figure 18 VPN authentication profile for RAPs

Chapter 8: Configuring AP Group for RAPs

In the Aruba user-centric network, every client is associated with a user role. The user roles that are enforced through the firewall policies determine the network privileges of a user. A policy is a set of rules that applies to the traffic that passes through the Aruba devices. The rules and policies are processed in a top-down fashion, so the position of a rule within a policy and the position of a policy within a role determine the functionality of the user role. When you construct a role, you must define the rules and policies in the proper order.

The Policy Enforcement Firewall-Next Generation (PEF-NG) license is essential to exploit the identity-based security features on the Aruba controller. The PEF-NG license also adds a set of predefined policies on the controller, which can be used or modified as required.



Modifying the predefined policies is not recommended. If necessary, create a new policy by cloning the predefined policy and then customize it.

The types of user roles and policies vary between organizations and the example network defines roles and policies that are implemented in most common cases. In the example network, the following roles are used:

- remote employee role
- remote application role (used for wired phones. For details, see [Remote Application Role on page 132.](#))
- guest-home role
- guest-branch-logon role
- auth-guest role

Figure 19 summarizes the user roles used in the example network and all the policies associated with each of those roles.

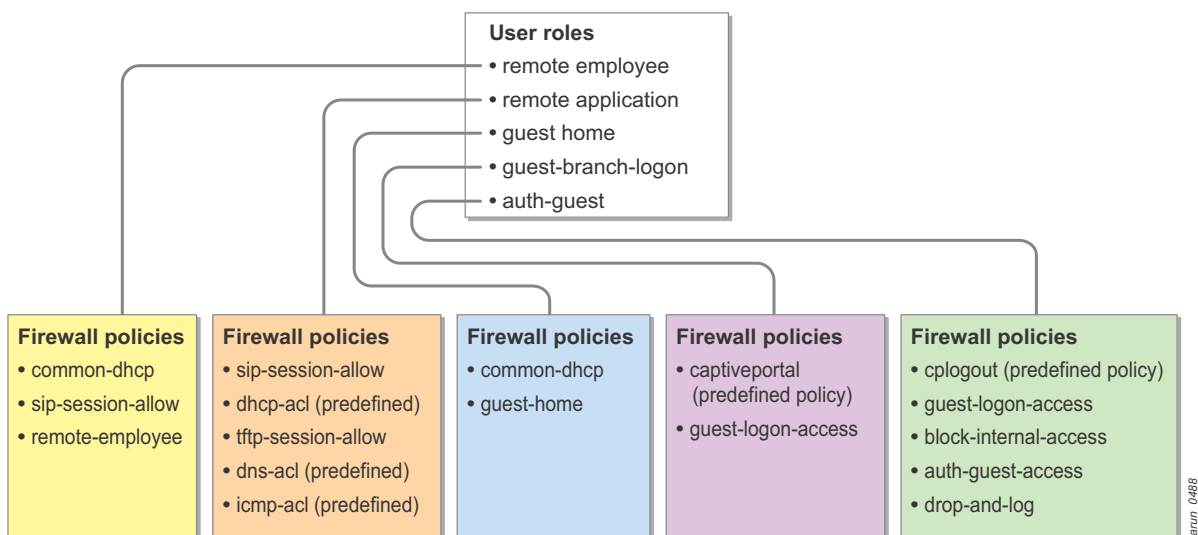


Figure 19 User roles used in the example network

Alias

The alias feature in the ArubaOS can be used to group several hosts or networks. Use this feature when several rules have protocols and actions common to multiple hosts or networks. An alias simplifies a firewall policy by reducing the number of ACL entries. An alias allows you to configure a list of domain names and IP addresses. The IP addresses can be added by host, network, or range. When the invert parameter of an alias is enabled, the rules that use that alias are applied to all the IP addresses and domains except those specified in the alias. For more information about the alias feature, see the *ArubaOS 6.1 User Guide* available on the Aruba support site.

Table 10 lists the aliases that are used in the example network.

Table 10 Aliases

Alias Name	Purpose	IP Address or Range
public-DNS	Defines the public DNS servers	Host 8.8.8.8 216.87.84.209 (In the example network, a simulated Internet is used. So, a DNS server with IP address 192.168.168.168 was created and used as the public DNS server.)
internal-network	Defines the private IPv4 address range	Network 10.0.0.0/8
guest-network	Defines the guest subnet	192.168.188.0/24 192.168.70.0/24
sip-server	Defines the SIP servers in the network	Host 10.169.130.33
tftp-server	Defines the TFTP servers in the network	Host 10.169.130.11
dns-servers	Defines the internal DNS servers	Host 10.169.130.4
clearpass-guest	Defines the ClearPass Guest server	Host 10.169.130.50

Configuration Profiles

Configuration profiles allow different aspects of the Aruba WLAN to be grouped into different configuration sets. Each profile is essentially a partial configuration. SSID profiles, radio profiles, and AAA profiles are just some of the available choices. For more information about these profiles, see the [Aruba 802.11n Networks Validated Reference Design](#) and [ArubaOS 6.1 User Guide](#).

Figure 20 shows an overview of the profile structure and high-level overview of an AP group.

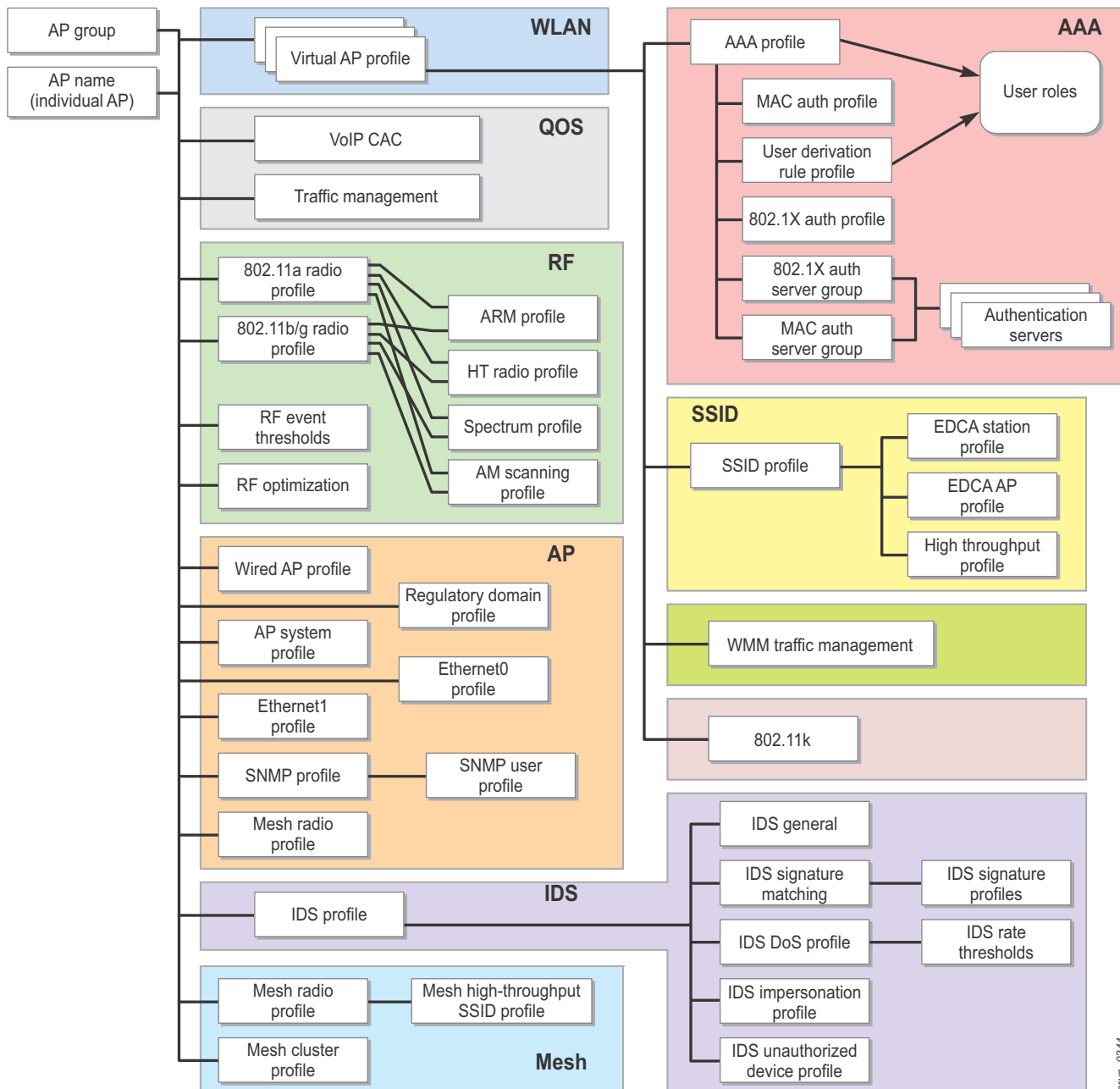


Figure 20 High-level overview of an AP group

AP Groups

An AP group is a unique combination of configuration profiles. In general, all profiles can be assigned to an AP group to create a complete configuration. This flexibility in configuration allows arbitrary groupings of APs such as All Headquarter APs, All Lobby APs, or All AMs, with different configurations for each. Configuration profiles provide flexibility and convenience to wireless network managers who create AP groups. An AP group must include a minimum number of profiles, in particular, a VAP profile.



Each AP, AM, SM, and RAP can be a part of only one AP group at any one time. This limitation eliminates the need to merge possibly contradictory configurations and prevents multiple VAPs with the same SSID from being enabled on the same physical AP.

The example network uses the following two AP groups:

- telecommuter
- micro-branch-office

Figure 21 summarizes the profiles used for the telecommuter and micro-branch-office AP groups.

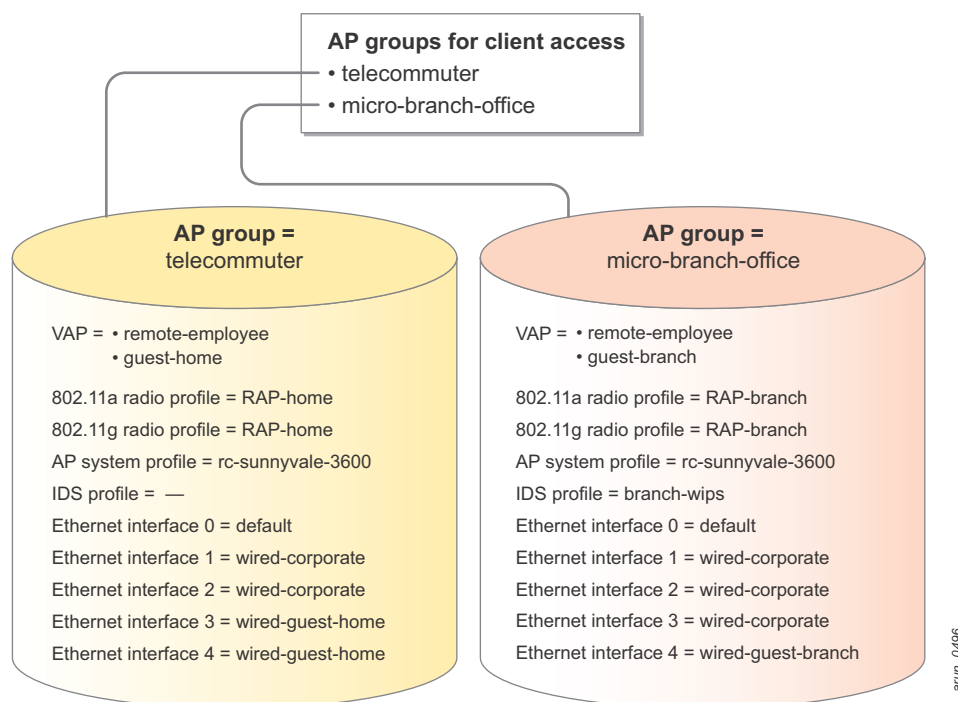


Figure 21 AP groups for client access

Figure 22 summarizes the configuration profiles used by these AP groups in the example network. The chapters that follow explain how to configure each of these profiles and why they are necessary.

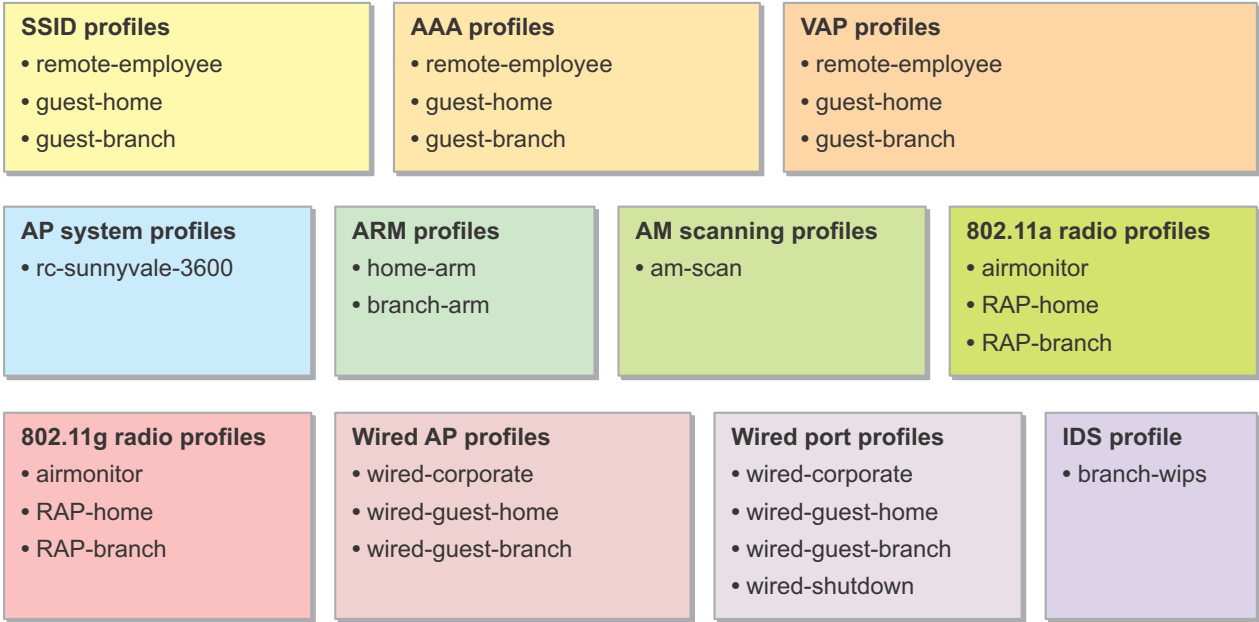


Figure 22 All the profiles configured in the example network

Chapter 9: Fixed Telecommuter Solution

Organizations with many fixed telecommuters typically have a requirement to extend a fully functional secure wired or wireless footprint (or both) into the employee home. Deploying a teleworker or branch office router at each employee premise is not a viable solution due to the cost and complexity involved. The Aruba RAP solution shatters the cost and complexity barrier involved with the traditional remote networking solutions used for fixed telecommuter deployments.

The Aruba remote network solution using RAPs fully meets the needs of remote employees and families. By leveraging the built-in firewall in the Aruba RAP, the enterprise can provide secure and QoS-enabled wired and wireless services needed by fixed telecommuters to do their jobs. In addition, by harnessing the built-in bridging capabilities of the Aruba solution, families can be online without imposing any additional IT management cost.

Requirements of Fixed Telecommuter Solution

The requirements of fixed telecommuter solutions are these:

- secure wired and wireless access to remote home office employees
- secure access to corporate resources at the enterprise HQ
- secure and reliable VoIP services through the centralized PBX at the HQ
- QoS for latency-sensitive applications, such as voice
- Internet access for family members
- wired access for local devices, such as family printers and fax machines

Creating AP Group for RAPs in Fixed Telecommuter Deployments

Most telecommuters who work from home offices require these services:

- wired and wireless access to PCs and laptops to securely connect the corporate resources
- wired and wireless access to VoIP phones to securely connect to the corporate voice server
- wired and wireless access for family members and guests so that they can reach the Internet without the need for an additional Internet connection
- wired ports and wireless access for home printers and fax machines shared by the employees and the family members in a secure manner without compromising the corporate security policy

Apart from broadcasting SSIDs to which the users can connect, the RAPs have Ethernet ports that the users can access. These ports provide the wired access required for telecommuters. Just like the SSIDs, these ports can be secured using the same authentication methods and servers while being configured to operate in various forwarding modes such as tunnel, split-tunnel, and bridge.

To create an AP group for the RAPs, you need to configure these roles and profiles:

- firewall policies and user roles (required)
- SSID profiles (required)
- server groups, AAA profiles (required)

- VAP profiles (required)
- Adaptive Radio Management (ARM) profile (optional, but recommended)
- 802.11a radio profile (required)
- 802.11g radio profile (required)
- AP system profile (required)
- wired AP profile (required)
- wired port profile (required)
- IDS profile (optional)

The next few chapters explain the configuration of telecommuter and micro-branch-office AP groups. The RAPs issued to telecommuters working from home offices belong to the telecommuter AP group. The RAPs used in micro branch offices belong to the micro-branch-office AP group.

The RAPs in the telecommuter AP group perform these actions:

- Broadcast employee SSID with split-tunnel forwarding mode and 802.1X authentication (WPA2-Enterprise).
- Broadcast guest SSID with bridge forwarding mode and PSK (WPA2-PSK).
- Provide wired employee access on wired port 1 and 2. Both ports provide 802.1X authentication and MAC authentication simultaneously.
 - Successful 802.1X authentication assigns an employee role.
 - Successful MAC authentication assigns an application role.
- Provide wired guest access (open authentication via bridge forwarding mode) on wired port 3 and 4.
- Allow employee users to reach the shared printer on the guest VLAN or local network through a one-way ACL.

Chapter 10: Configuring the Remote Employee Role

The main purpose of a RAP is to provide employee users with the same privileges that they have when connected directly to the campus network and to secure that connectivity. The user data to and from the corporate resources is always secure because it is forwarded only through the IPsec connection between the RAP and the controller.

Users who successfully authenticate to the employee SSID that is broadcasted by the RAP must be able to access all the resources in the corporate site as if they are directly connected to the campus network. To achieve this access, any remote employee user traffic that is destined to corporate network must be forwarded to the controller through the IPsec tunnel. The remote employees also need connectivity to the Internet. It is not desirable to route all traffic destined to the Internet to the controller and then back to the Internet. This path wastes the expensive Internet bandwidth resources available at the corporate site. So, any traffic from an employee user that is destined to the Internet and not to the corporate network should be forwarded directly to the Internet. In addition, the remote employee user must also be allowed to access the local resources such as the printers that will be a part of the guest network. To allow the employee users to access the local resources, the remote employee user role must be designed to allow access to the local resources using a one-way ACL. This one-way ACL ensures that the devices in the guest network don't reach the employee network.

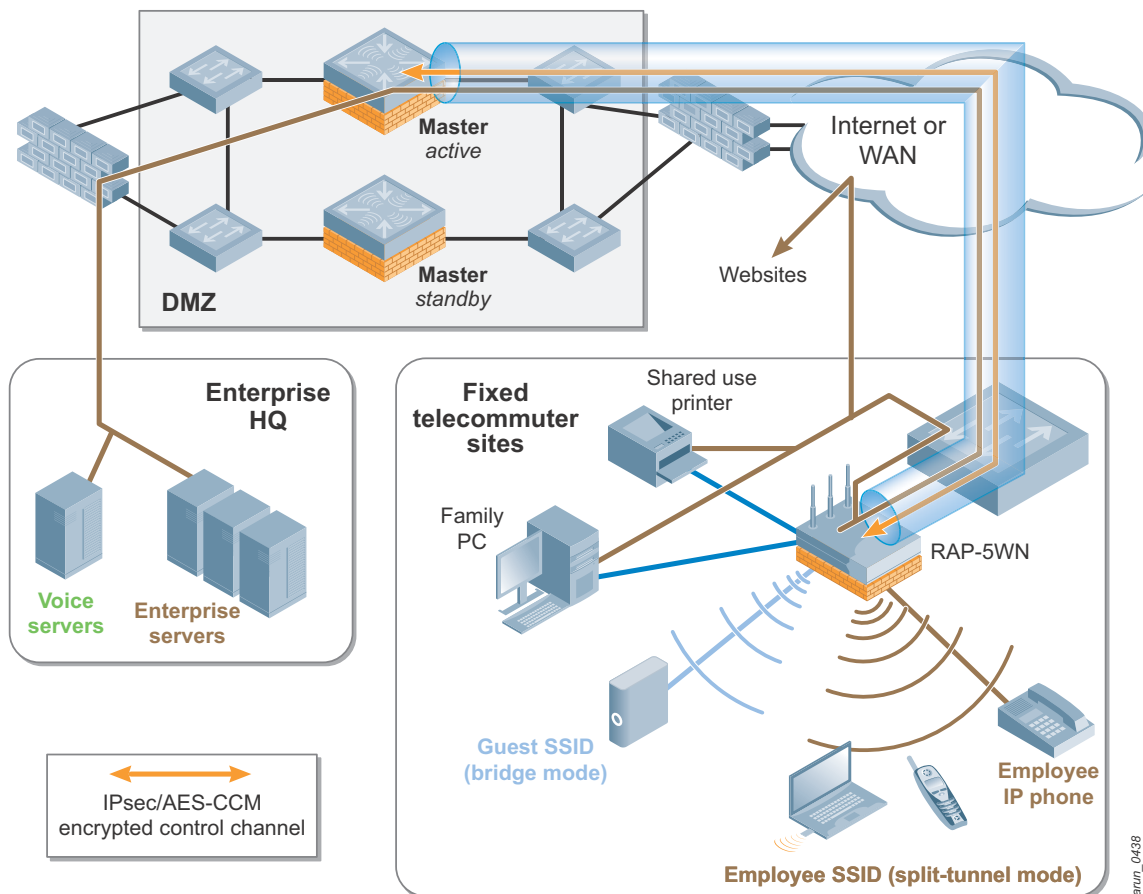


Figure 23 Remote employee network

Before you configure the remote employee role, first you must create the policy associated with it. The remote employee role in the example network contains these policies

- common-dhcp
- sip-session-allow
- remote-employee



CAUTION

In RAP deployments, which provide VoIP services through a central PBX server, 911 calls should not be made from VoIP phones unless an E911 solution has been implemented. In the absence of an E911 solution such as RedSky, the 911 calls might be routed to the wrong location. To comply with the rules of FCC or your respective local regulatory bodies, Aruba strongly recommends the use of E911 or a similar solution for your VoIP deployments.

Configuring the common-dhcp Policy

The common-dhcp policy, which is used in the remote-employee role, denies users from activating their personal DHCP servers on the network but allows legitimate DHCP services.



NOTE

Remember, the order of rules within a policy determines the behavior of the policy.

Table 11 summarizes the rules used for the common-dhcp policy.

Table 11 Rules Used for the common-dhcp Policy

Rule Number	Source	Destination	Service	Action	Purpose
1	user	any	UDP min port = 68 max port = 68	drop	This rule drops responses from a personal DHCP server, which prevents the clients from acting as DHCP servers.
2	any	any	service svc-dhcp (udp 67 68)	permit	This rule allows clients to request and discover a DHCP IP address over the network. The DHCP server on the network does not fall under the user category, so its response on port 68 is not dropped by the first rule. The first two rules guarantee that DHCP is processed only by legitimate DHCP servers on the network.

CLI Configuration

```
!
ip access-list session common-dhcp
user any udp 68 deny
any any svc-dhcp permit
!
```

WebUI Screenshot

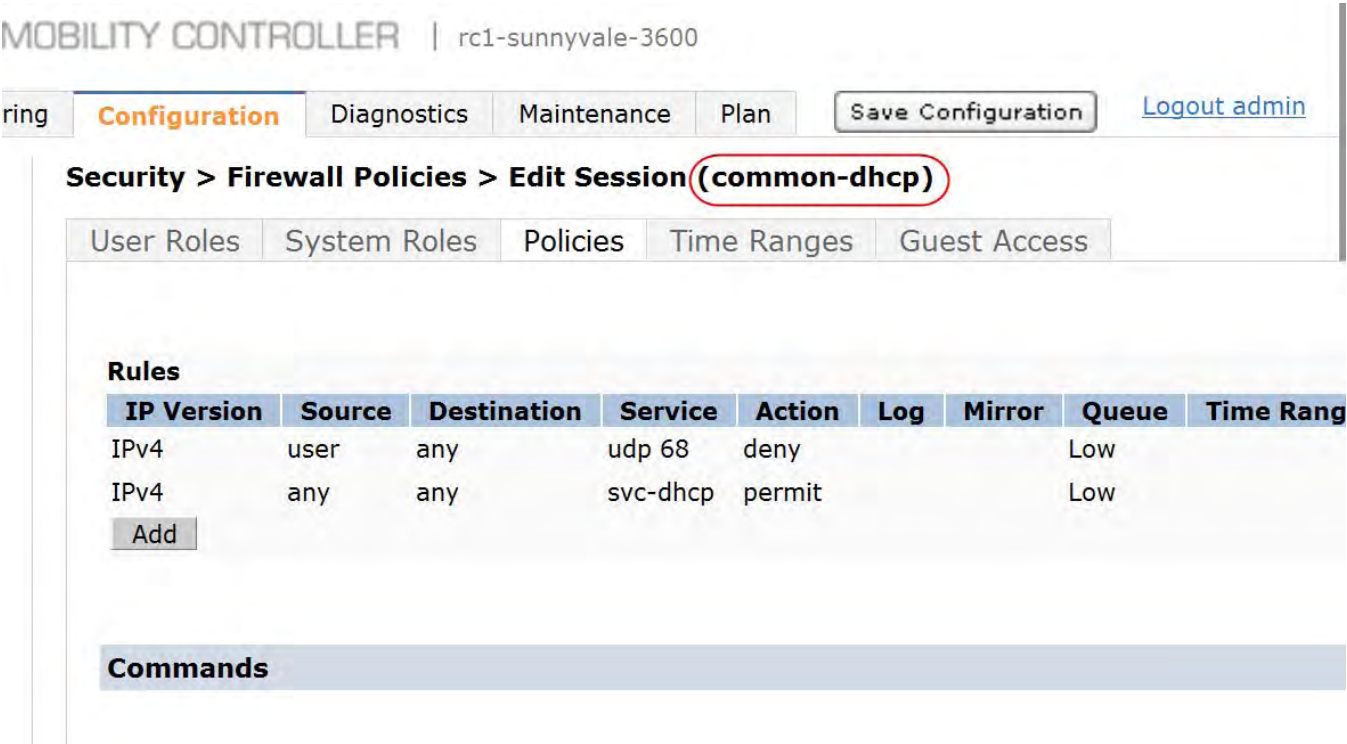


Figure 24 common-dhcp policy

Configuring the sip-session-allow Policy

The sip-session-allow policy prioritizes SIP traffic and allows SIP services only between the user and the corporate PBX and servers that provide voice service. If the organization supports protocols such as NOE from Alcatel Lucent, H.323, SCCP, Vocera, and others for voice communication, policies should be created to prioritize them.

Table 12 summarizes the rules used for the sip-session-allow policy.

Table 12 Rules Used for the sip-session-allow Policy

Rule Number	Source	Destination	Service	Action	Queue	Purpose
1	user	alias sip-server	service svc-sip-udp	permit	high	Allows SIP sessions between users and SIP servers using the UDP protocol
2	user	alias sip-server	service svc-sip-tcp	permit	high	Allows SIP sessions between users and SIP servers using the TCP protocol

Table 12 Rules Used for the sip-session-allow Policy (Continued)

Rule Number	Source	Destination	Service	Action	Queue	Purpose
3	alias sip-server	user	service svc-sip-udp	permit	high	Allows SIP sessions between SIP servers and users using the UDP protocol
4	alias sip-server	user	service svc-sip-tcp	permit	high	Allows SIP sessions between SIP servers and users using the TCP protocol

CLI Configuration

```

!
ip access-list session sip-session-allow
  user alias sip-server svc-sip-udp permit queue high
  user alias sip-server svc-sip-tcp permit queue high
  alias sip-server user svc-sip-udp permit queue high
  alias sip-server user svc-sip-tcp permit queue high
!

```

WebUI Screenshot

BILITY CONTROLLER | rc1-sunnyvale-3600

Configuration | Diagnostics | Maintenance | Plan | [Save Configuration](#) | [Logout admin](#)

Security > Firewall Policies > Edit Session (sip-session-allow)

User Roles | System Roles | Policies | Time Ranges | Guest Access

Rules

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	Pause ARM Sca
IPv4	user	sip-server	svc-sip-udp	permit			High		
IPv4	user	sip-server	svc-sip-tcp	permit			High		
IPv4	sip-server	user	svc-sip-udp	permit			High		
IPv4	sip-server	user	svc-sip-tcp	permit			High		

[Add](#)

Commands

Figure 25 sip-session-allow policy

Configuring the remote-employee Policy

The remote-employee policy used in the remote-employee role does the following things:

- Allows any service between the user and the corporate network. The corporate network IP range is defined by the internal-network alias.
- Locally bridges any traffic that is not destined to the corporate network using route source-NAT function. The source-NATing is performed based on the destination of the noncorporate traffic. If the traffic is bound to the Internet or the network managed by the home router, then the source-NATing is performed using the RAP IP address obtained from the ISP or home router. If the traffic is bound to a local subnet for which the RAP is the DHCP server or gateway, then the source-NATing is performed using the gateway IP address of this local subnet.
- Ensures that the devices in other networks, such as the guest network, cannot access the employee network.

Table 13 summarizes the rules used for the remote-employee policy.

Table 13 Rules Used for the remote-employee Policy

Rule Number	Source	Destination	Service	Action	Purpose
1	alias internal-network	alias internal-network	any	permit	This rule allows all types of traffic between the user and corporate network. The traffic can be initiated either by the user or the devices in the corporate network. The “permit” action implies tunneling, which is used for corporate traffic. Any traffic that meets the requirements of this rule is forwarded to the controller through the tunnel.
2	user	any	any	route scr-nat	This rule ensures that users can reach the Internet and local resources. The “route scr-nat” action properly source-NATs the traffic depending on the destination and eliminates the need to define static NAT pools. If the traffic is bound to the Internet, then the source-NATing is performed using the RAP IP address obtained from the ISP or home router. If the traffic is bound to a local subnet for which the RAP is the DHCP server or gateway, then the source-NATing is performed using the gateway IP of this local subnet. Placing this rule at the end ensures that “route scr-nat” action is performed only on the noncorporate traffic. The rules 1 and 2 indicate that access from another network to the employee network is denied.



If you do not want to allow the corporate resources to initiate connections to the users, then change the first rule in the remote-employee policy to “user alias internal-network any permit”.

CLI Configuration

```
!
ip access-list session remote-employee
  alias internal-network alias internal-network any permit
  user any any route src-nat
!
```

WebUI Screenshot

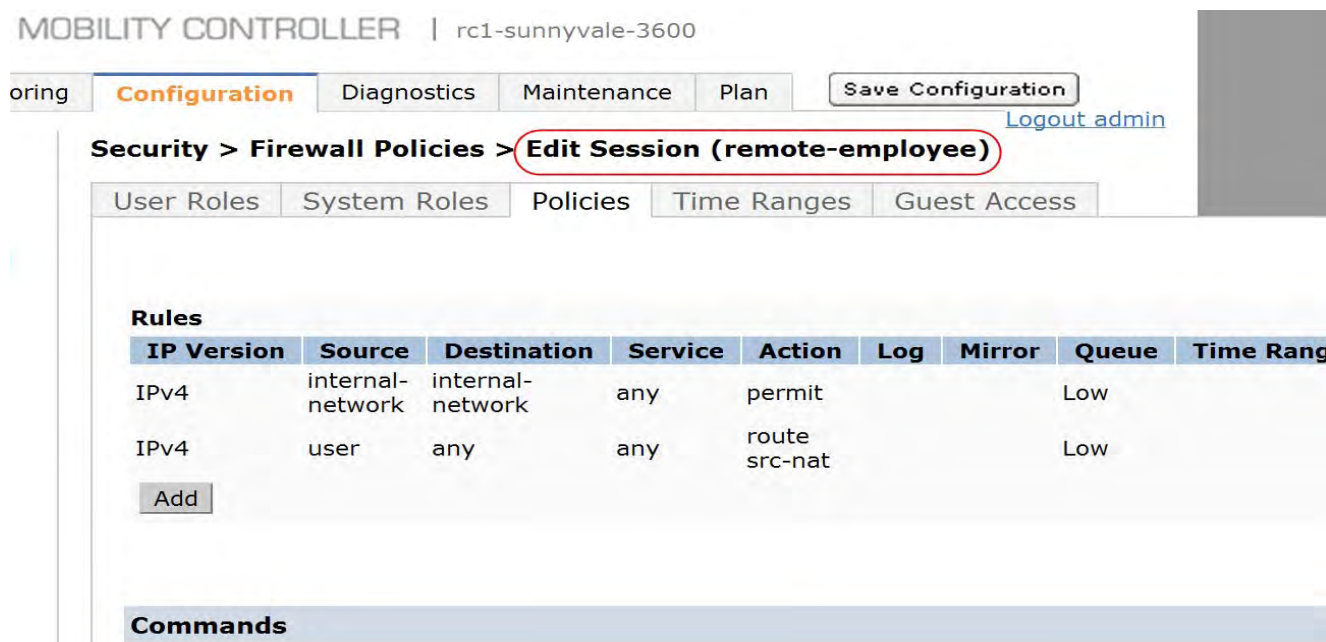


Figure 26 remote-employee policy

Configuring the remote-employee Role

The remote-employee role is designed to allow the users unrestricted access to all the corporate resources. Traffic that is destined to the corporate network is forwarded to the controller through the IPsec tunnel. Any other traffic that is destined to the Internet or to the devices on the local bridged network of the RAP is sourced-NATed by the RAP based on the traffic destination. To create the desired employee role, you must order the essential firewall policies properly.

Table 14 summarizes the policies used in the remote-employee role.

Table 14 Policies Used in the remote-employee Role

Policy Number	Policy Name	Purpose
1	common-dhcp	This policy denies personal DHCP servers but allows legitimate DHCP services. For details, see Configuring the common-dhcp Policy on page 53 .
2	sip-session-allow	This policy enables the SIP application layer gateway (ALG) and provides voice traffic priority using the high-priority queue. For details, see "Configuring the sip-session-allow Policy on page 54" .

Table 14 Policies Used in the remote-employee Role (Continued)

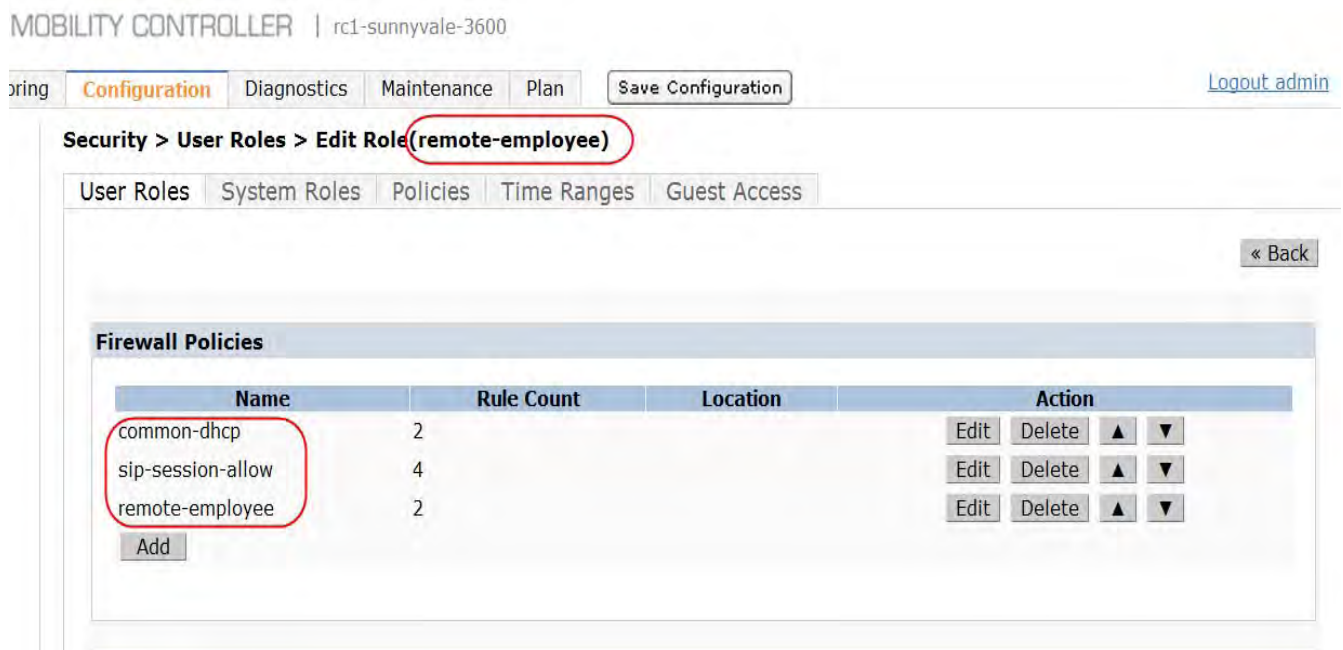
Policy Number	Policy Name	Purpose
3	remote-employee	This policy tunnels the traffic destined to corporate network through the IPsec tunnel to the controller but appropriately source-NATs all other traffic based on the destination of the traffic. It also denies access to corporate network from other networks. For details, see Configuring the remote-employee Policy on page 56 .

CLI Configuration

```

!
user-role remote-employee
  access-list session common-dhcp
  access-list session sip-session-allow
  access-list session remote-employee
!

```

WebUI Screenshot**Figure 27 remote-employee role**

Chapter 11: Remote Employee VAP

A typical home AP advertises only one SSID, so even with a dual-radio AP, only two WLANs can be formed. Ideally, in these situations the number of physical APs is proportional to the number of WLANs supported. Aruba solves this issue with the concept of virtual APs (VAPs). VAPs are logical entities that are present within a physical AP.

Physical Aruba APs, unlike typical home APs, are often configured to appear as more than one physical AP. This configuration provides the necessary authentication and encryption combinations without collocating excessive amounts of APs in the same physical area.

The VAPs share the same channel and power settings on the radio, but each appears as a separate AP with its own SSID (ESSID) and MAC address (BSSID).

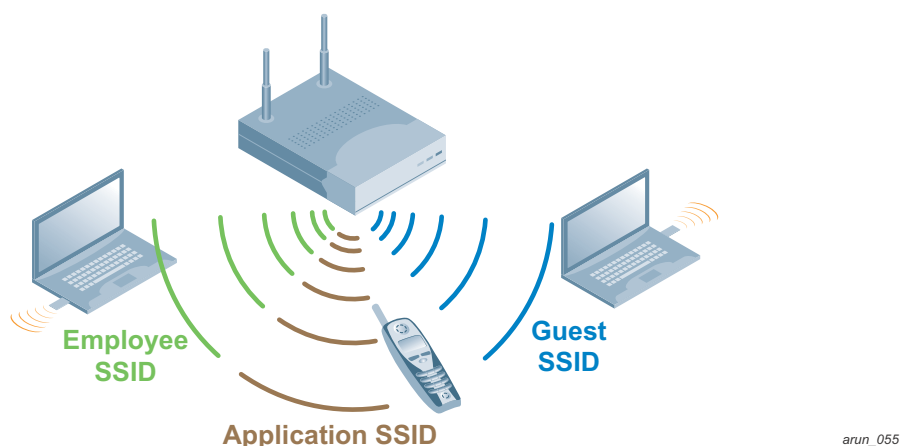


Figure 28 A typical set of VAPs on one physical AP

Aruba supports up to eight BSSIDs per radio on the AP, with a maximum of 16 VAPs per physical AP. The maximum total number of BSSIDs that are supported across the WLAN is a function of the mobility controller model. For more on these limitations, see the mobility controller matrix and AP matrix on the Aruba networks public site at <http://www.arubanetworks.com>.



Aruba does not recommend running an AP with the maximum number of VAPs available. Each VAP acts like a real AP and is required to beacon like any other AP. This beaconing consumes valuable airtime that would otherwise be used by clients to transmit data on the channel. Aruba recommends that you leverage the smaller numbers of SSIDs and user roles and deploy a new SSID only when a new encryption or authentication type is required.



The BSSIDs assigned to the SSIDs on a physical AP are generated from the MAC address of the physical AP. All the BSSIDs are generated by an algorithm. The BSSID assigned to each SSID is random. Whenever an AP reboots, the BSSID to SSID mapping may change. In certain situations, an SSID may be temporarily disabled for maintenance. When this SSID is enabled again, the BSSID assigned to it might not be the same as before.

The VAP profile is a container that holds an SSID profile, AAA profile, 802.11k profile, and Wi-Fi Multimedia™ (WMM®) traffic management profile. At minimum, each VAP profile must have an SSID and AAA profile. The VAP profile also has other configurable features, such as band steering, forwarding modes, dynamic multicast optimization, fast roaming, and DoS prevention. For more details on VAP profiles, see the [Aruba 802.11n Networks Validated Reference Design](#).

Table 15 summarizes the VAP profiles used in the example network.

Table 15 VAP Profiles Used in the Example Network

VAP Profile	AP Group	VLAN	Forwarding Mode	Remote-AP Operation Mode
remote-employee	telecommuter and micro-branch-office	135	split-tunnel	standard
guest-home	telecommuter	900	bridge	always
guest-branch	micro-branch-office	700	split-tunnel	standard

Forwarding Modes

The forwarding modes parameter in the VAP profile controls how user traffic is handled, including where decryption occurs and where role-based firewall policies are applied. A RAP can operate in tunnel, decrypt-tunnel, split-tunnel, or bridge forwarding modes.

Tunnel Mode

The RAP is set up to forward all traffic to the DMZ controller within an IPsec tunnel. All traffic is encrypted and decrypted at the controller, and user-based firewall roles are enforced at the controller. The AP does not decrypt the traffic, so IPsec re-encryption is not performed for wireless traffic unless the double-encryption is enabled. Only an IPsec authentication header (AH) is placed on the packet. The wired traffic from the tunnel mode wired ports of a RAP is always encrypted in the IPsec tunnel back to the controller. All ALGs in the ArubaOS are available in the tunnel forwarding mode. For the entire list of ALGs available in ArubaOS, see the *Aruba 6.1 User Guide* available at the Aruba support site.

Split-Tunnel Mode

When the RAP is configured in split-tunnel mode, the Aruba firewall operates inside the RAP as well as in the controller. The RAP performs decryption of wireless traffic and this allows role-based forwarding policies to be applied at the RAP. Both the wired and wireless traffic that it is bound for a noncorporate address is bridged locally and the corporate-bound traffic is encrypted in the IPsec

tunnel back to the controller. All ALGs in the ArubaOS are available in the split-tunnel forwarding mode.

Bridge Mode

All WLAN traffic is bridged locally at the AP to allow access to local devices on the LAN, such as printers and local servers. In bridge mode the Aruba firewall operates at the RAP and even though a secure tunnel exists, users will not be able to access centralized resources. The IPsec tunnel is used only for control plane traffic and 802.1X exchanges. ALGs of the ArubaOS are not available in bridge forwarding mode.

Decrypt-Tunnel Mode

RAPs are deployed across the Internet and when decrypt-tunnel mode is enabled, the traffic is tunneled back to the controller in clear text (IPsec AH with null encryption) unless double-encryption is enabled. Decrypt-tunnel mode is not recommended for deployment on RAPs except where an existing VPN is in place to secure traffic. All application layer gateways (ALGs) in the ArubaOS are available in the decrypt-tunnel forwarding mode.

For more details on forwarding modes, see the [Aruba Deployment Models Validated Reference Design](#).

RAP Operation Modes

Each wired port and wireless SSID on a RAP has a forwarding mode and an operating mode. The RAP operating mode in the VAP profile governs AP availability when the controller is not reachable. The RAP operating mode has a corresponding impact on the authentication types supported. For tunnel and split-tunnel modes, the Standard operating mode applies. For bridge mode, the network engineer has choice of three additional operating modes. [Table 16](#) summarizes the different operating modes.

Table 16 RAP Operation Modes

	Standard	Persistent	Backup	Always
Description	Classic Aruba thin AP operation	Provides SSID continuity during temporary controller outages	Provides a backup SSID for local access only when controller is unreachable	Provides an SSID that is always available for local access
Forwarding Modes	● tunnel ● split-tunnel ● bridge	bridge	bridge	bridge
ESSID Availability	Up only when controller is reachable.	Must reach controller to come up; stays up if connectivity is temporarily disrupted.	Up only when controller cannot be reached.	Always up when the AP is up, regardless of controller reachability.
Supported Authentication Modes	802.1X supported	802.1X supported	PSK ESSID only	PSK ESSID only
SSID Configuration	Obtained from controller	Obtained from controller	Stored in AP flash memory	Stored in AP flash memory

AP/AM Data and Control Tunnels

Aruba APs, AMs, and SMs maintain a variety of data and control tunnels with the controller on which it terminates. In remote deployments, this is the active master controllers in the DMZ. It is important for network engineers to understand the various types of tunnels and where they terminate inside Aruba architecture.

RAP/AP Tunnels

Figure 29 shows a RAP configuration with a mix of wired ports, wireless SSIDs, and forwarding modes that various client devices use to connect. Data from the client devices is tunneled through to the controller in the DMZ using IPsec-encrypted GRE data tunnels. In addition, Aruba Process Application Programming Interface (PAPI) control channels to the master are also used for image and configuration download, heartbeats, air monitoring, and spectrum monitoring functions.

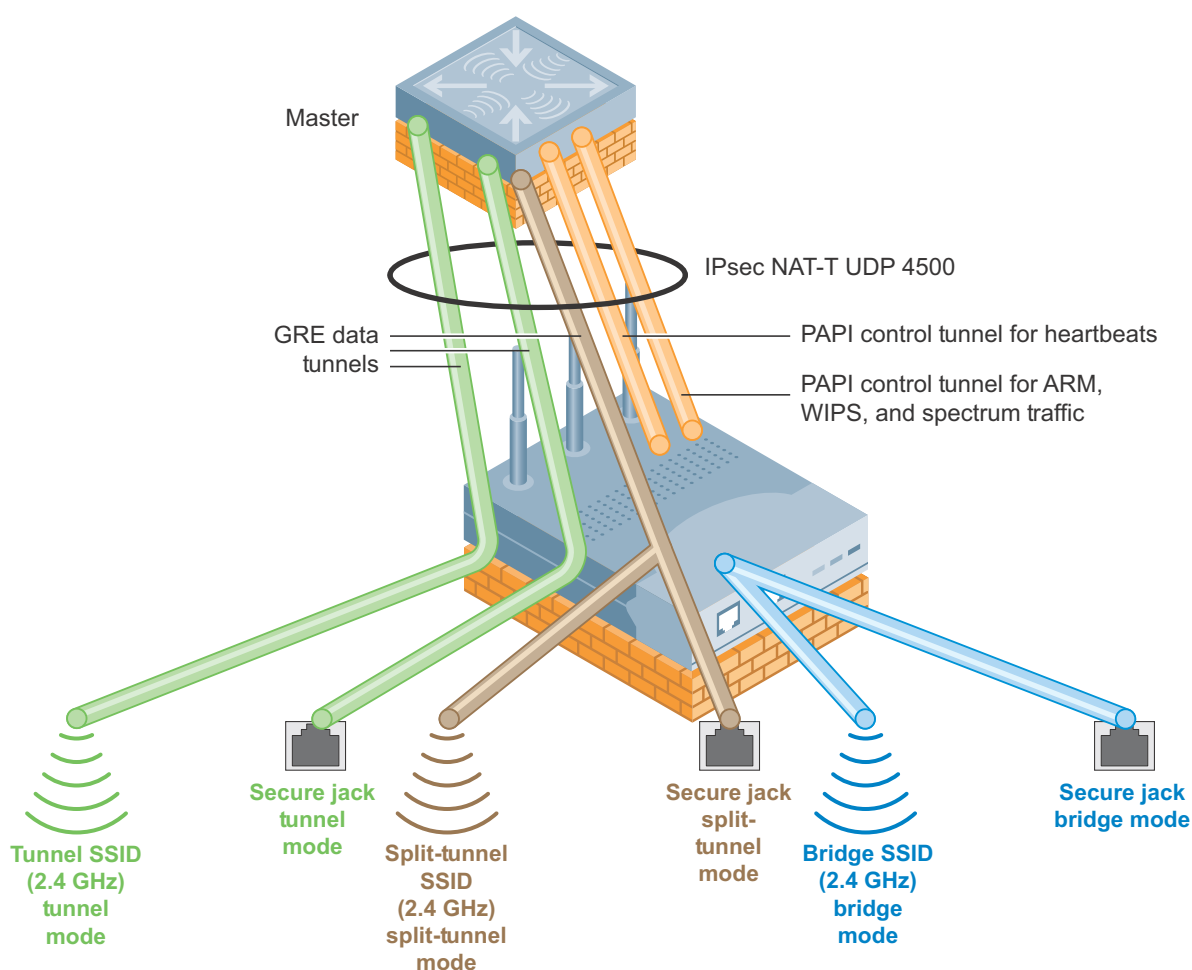


Figure 29 RAP tunnels

The number of IPsec-encrypted GRE tunnels that the RAP constructs depends on the forwarding mode on each SSID and wired port.

- **Tunnel/Decrypt-tunnel mode:** One GRE tunnel per SSID per wireless radio, plus one GRE tunnel per wired port.
- **Split-tunnel mode:** The user data traffic from all split-tunnel wired ports and wireless SSIDs are multiplexed onto a single IPsec-encrypted GRE tunnel after the decrypt and encrypt process. However, every split-tunnel VAP and wired port configured for 802.1X forms a separate IPsec-encrypted GRE tunnel to the controller. This tunnel is used only for 802.1X exchanges.
- **Bridge mode:** The user data traffic is never forwarded to the controller, so there is no IPsec-encrypted GRE tunnel to the controller for data traffic. However, each bridge mode SSID configured for 802.1X forms a GRE tunnel back to the controller on which the RAP terminates. This tunnel is used only for 802.1X exchanges.

The number of PAPI control channels constructed by a RAP, dedicated AM, or SM is two. One is used for heartbeats (GRE + PAPI keepalives). The other is used for image and configuration download, ARM, WIPS, and spectrum monitoring functions.



ArubaOS 6.0 and later introduces an optimization to reduce the WAN bandwidth required by APs. Instead of exchanging one heartbeat (GRE keepalives) per tunnel, the RAP exchanges one heartbeat per AP. The PAPI keepalives are sent once every 10 minutes and are used only for time synchronization. The time interval between keepalives is not configurable. Excluding user-traffic, a pre ArubaOS 6.0 RAP with three BSSIDs requires approximately 9 kb/s of consistent bandwidth. With ArubaOS 6.0 and later, the same RAP requires just 3 kb/s.

Remote Employee SSID Profile

The SSID is the network or WLAN that any client sees. An SSID profile defines parameters, such as name of the network, authentication type for the network, basic rates, transmit rates, SSID cloaking, and certain WMM settings for the network.

Aruba offers different flavors of the Advanced Encryption Standard (AES), Temporal Key Integrity Protocol (TKIP), and wired equivalent privacy (WEP) encryption. AES is the most secure and recommended encryption method. Most modern devices are AES capable and AES should be the default encryption method. Use TKIP only when devices that are not AES-capable are present. In these situations, use a separate SSID for devices that are capable only of TKIP. It is important to understand that several vulnerabilities have been reported with TKIP. Avoid using WEP, because it can be cracked in less than 5 minutes with generally available tools. Aruba also supports a host of authentication methods such as 802.1X, captive portal, PSK, and WEP. For information on SSID profile, various the authentication and encryption supported, and WMM settings see the [Aruba 802.11n Networks Validated Reference Design](#).

Configuring the Remote Employee SSID Profile

In any deployment, the employee SSID should have the strongest authentication and encryption. The users that authenticate successfully to the employee SSID are assigned the employee user role, which grants access to internal resources. In the example network, the remote employee SSID uses WPA2, which provides 802.1X authentication and AES encryption.

Aruba has these recommendations for your remote employee SSID:

1. Always use 802.1X for authentication and AES for encryption for the employee network. Every corporate device that is capable of 802.1X should use the employee SSID.
2. In remote deployments, do not use SSIDs with PSK for authentication except for guest networks.
3. As per the 802.11 standard, an AP beacons periodically to advertise an SSID it broadcasts. The APs should beacon separately for every SSID they broadcast. As the number of SSIDs increases, more air time is used for beaconing. Limiting the number of SSIDs increases performance, because the valuable airtime is used for serving the clients instead of for beaconing. Instead of multiple SSIDs, deploy a new SSID only when a new encryption or authentication type is required.
4. In some remote branch office deployments, certain legacy handheld scanners and IP cameras might not be 802.1X capable. In these cases, create separate SSIDs for these devices and assign a user role that restricts these devices only to the services that they require. Remember that PSK is susceptible to social engineering attacks and offline dictionary attacks. The passphrase or key that is used should be at least 20 characters. To protect against social engineering attacks, the passphrase or the key should not be distributed to everyone. Only the network administrators should know the passphrase. Aruba recommends that these devices be replaced immediately with those that are 802.1X capable.
5. All the wireless IP phones distributed to the remote employee should be 802.1X capable. Do not deploy wireless IP phones that are capable only on PSK in remote sites.

Configuring Wi-Fi Multimedia

Wi-Fi Multimedia™ (WMM®) is a Wi-Fi Alliance® certification program that is based on the IEEE 802.11e amendment. WMM ensures QoS for latency-sensitive traffic in the air. WMM divides the traffic into four queues or access categories:

- voice
- video
- best effort
- background

The traffic is prioritized based on the queue it belongs to. The order of priority is voice > video > best effort > background. Like WMM for QoS in air, QoS on the wired side of the network is dictated by the DiffServ Code Point (DSCP) and 802.1p tagging. To ensure end-to-end QoS on the network, consider these requirements:

- The DSCP tags should translate to appropriate WMM access categories and vice-versa. The Aruba infrastructure ensures this translation between WMM and DSCP/802.1p markings when the traffic moves across wired and wireless mediums.

- All devices in the network under your control should be capable of and configured for QoS support. The devices that are between the RAP and the mobility controller must recognize and prioritize DSCP-marked traffic through the network. However, RAPs are deployed across WAN links, so there is no guarantee that the WAN will respect the DSCP markings unless you have a service level agreement (SLA) with the ISP. Similarly, the core must respect the DSCP marks from the mobility controller to the multimedia servers.

For more information about the mapping between WMM access categories, DSCP tags, and other QoS functionalities, see the [Aruba 802.11n Networks Validated Reference Design](#).

Enable WMM to prioritize latency-sensitive applications. In the example network, the WMM parameter is enabled on the remote-employee SSID to prioritize latency-sensitive traffic, such as voice, over the standard data traffic. The DSCP-to-WMM mapping is a configurable parameter that is available within the SSID profile. In the example network, the DSCP-to-WMM mapping values are set to the defaults. The Aruba default DSCP-to-WMM mapping values match the default DSCP settings of most vendors. Alter the Aruba defaults only if they vary from your existing DSCP settings. [Table 17](#) summarizes the remote-employee SSID profile used in the example network.

Table 17 remote-employee SSID Profile

SSID Profile	Network Name (SSID)	Authentication	Encryption	WMM	Purpose
remote-employee	employee	WPA2	AES	enabled	All remote employees and corporate devices such as wireless IP phones will use this SSID.

CLI

```

!
wlan ssid-profile "remote-employee"
    essid "employee"
    opmode wpa2-aes
wmm
!

```

WebUI Screenshot

The screenshot shows the Aruba WebUI configuration page for the 'remote-employee' SSID profile. The page is divided into two main sections: 'Profiles' on the left and 'Profile Details' on the right. The 'Profiles' section lists various profiles, including 'remote-employee', which is currently selected. The 'Profile Details' section shows the configuration for the 'remote-employee' profile, with the 'Basic' tab selected. The 'Network' section shows the 'Network Name (SSID)' set to 'employee'. The '802.11 Security' section shows the 'Network Authentication' set to 'WPA2' and the 'Encryption' set to 'AES'. The 'Keys' section is also visible.

Configuration | Diagnostics | Maintenance | Plan | [Save Configuration](#) | [Logout admin](#)

Advanced Services > All Profile Management

Profiles

- AP
- RF Management
- Wireless LAN
 - 802.11K Profile
 - SSID Profile
 - application
 - backup SSID
 - corp-app
 - corp-employee
 - default
 - employee
 - guest-branch
 - guest-home
 - guestnet
 - remote-employee**
 - EDCA Parameters Station profile
 - EDCA Parameters AP profile
 - High throughput SSID Profile

Profile Details

SSID Profile > remote-employee | [Show Reference](#) | [Save As](#) | [Reset](#)

Basic | Advanced

Network

Network Name (SSID) | employee

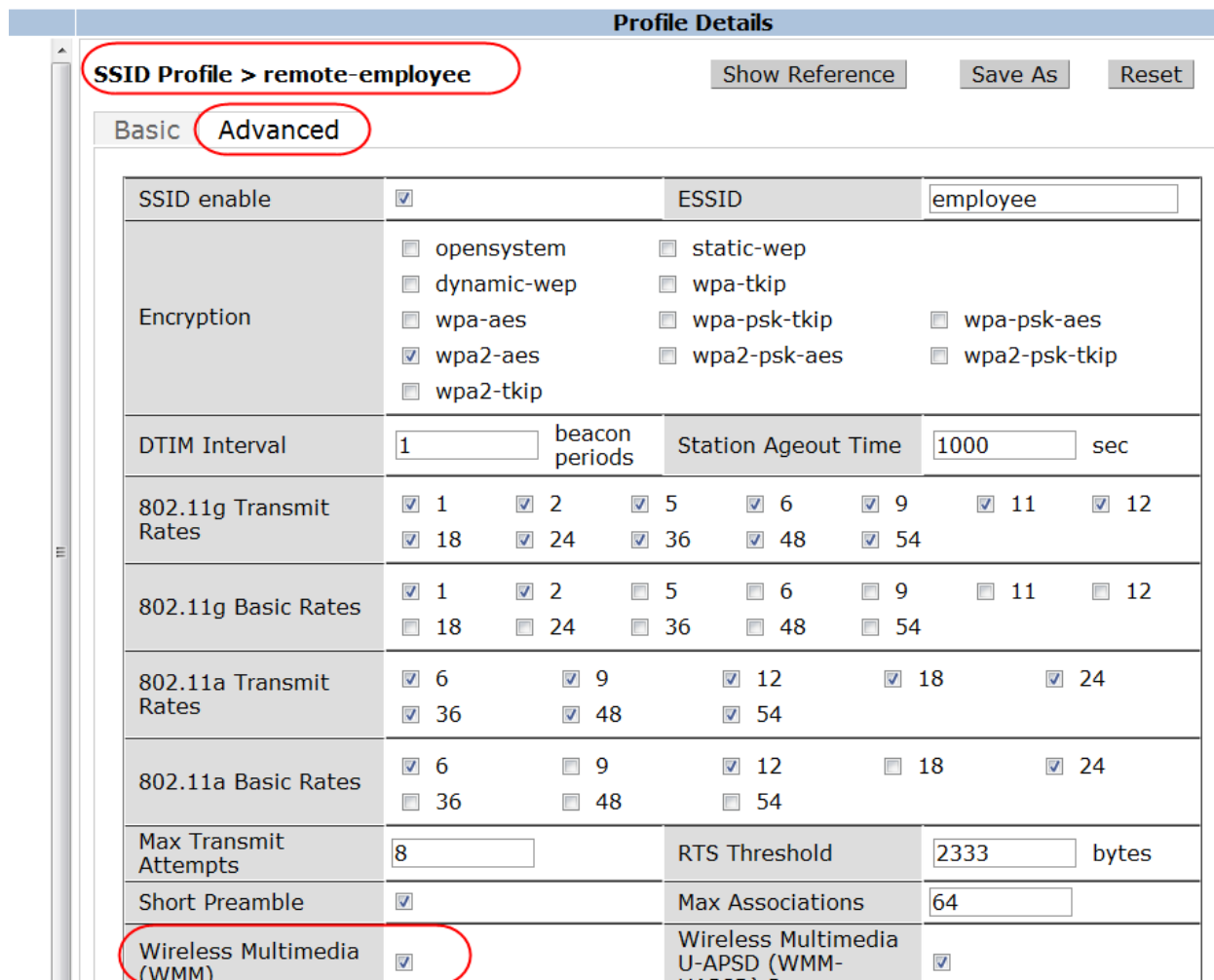
802.11 Security

Network Authentication | ☐ None | ☐ 802.1x/WEP | ☐ WPA | ☐ WPA-PSK | ☒ WPA2 | ☐ WPA2-PSK

Encryption | ☒ AES

Keys

Figure 30 remote-employee SSID



Profile Details

SSID Profile > remote-employee Show Reference Save As Reset

Basic **Advanced**

SSID enable	☒	ESSID	employee
Encryption	☐ opensystem ☐ dynamic-wep ☐ wpa-aes ☒ wpa2-aes ☐ wpa2-tpk	☐ static-wep ☐ wpa-tpk ☐ wpa-psk-tpk ☐ wpa2-psk-aes ☐ wpa2-psk-tpk	☐ wpa-psk-aes ☐ wpa2-psk-tpk
DTIM Interval	1 beacon periods	Station Ageout Time	1000 sec
802.11g Transmit Rates	☒ 1 ☒ 2 ☒ 5 ☒ 6 ☒ 9 ☒ 11 ☒ 12 ☒ 18 ☒ 24 ☒ 36 ☒ 48 ☒ 54		
802.11g Basic Rates	☒ 1 ☒ 2 ☐ 5 ☐ 6 ☐ 9 ☐ 11 ☐ 12 ☐ 18 ☐ 24 ☐ 36 ☐ 48 ☐ 54		
802.11a Transmit Rates	☒ 6 ☒ 9 ☒ 12 ☒ 18 ☒ 24 ☒ 36 ☒ 48 ☒ 54		
802.11a Basic Rates	☒ 6 ☐ 9 ☒ 12 ☐ 18 ☒ 24 ☐ 36 ☐ 48 ☐ 54		
Max Transmit Attempts	8	RTS Threshold	2333 bytes
Short Preamble	☒	Max Associations	64
Wireless Multimedia (WMM)	☒	Wireless Multimedia U-APSD (WMM-URPS)	☒

Figure 31 WMM enabled for remote-employee SSID (available on the Advanced tab of the SSID profile)

Configuring the Remote Employee AAA Profile

The AAA profiles define how users are authenticated. Based on the authentication type, the AAA profile determines the preauthentication user role for unauthenticated clients (initial role) and post-authentication user role for successfully authenticated clients (default role). The AAA profile also defines the server group that is used for the defined authentication method and RADIUS accounting.

Authentication Server and Server Groups

For authentication, ArubaOS can use the internal database or external authentication servers such as RADIUS, LDAP, TACACS+, and Windows server. A server group is a collection of servers used for authentication. In case of 802.1X authentication, the external RADIUS server or servers used for 802.1X authentication for a particular WLAN are grouped together as a server group. By default, the first server on the list is used for authentication unless it is unavailable. A server group can have

different authentication servers. For example, you can create a server group that uses an LDAP server as a backup for a RADIUS server.

If a server group has more than one server, the “fail-through” feature can be used to authenticate the users with the other servers in the list if authentication with the first server fails. If enabled, the fail-through feature tries to authenticate the users against all the servers in the list until the authentication is successful or until all the servers have been tried. When this feature is disabled, only the first authentication server in the list is used for authenticating the users unless that server is unreachable. Aruba recommends that you consider these facts before you enable this feature:

- Fail-through authentication is not supported for 802.1X authentication in server groups that consist of external EAP compliant RADIUS servers, unless authentication is terminated on the controller (AAA FastConnect).
- This feature causes an excessive processing load on the controller if the server group list is large. Use dynamic server selection in these situations. For more details about dynamic server selection, see the *ArubaOS 6.1 User Guide* available at the Aruba support site.
- RSA RADIUS server and certain other servers lock out the controller if multiple authentication failures occur. Do not enable fail-through authentication if these servers are in use.

Configuring the Server Group for 802.1X Authentication

To successfully authenticate the users to the employee network, the credentials provided by them should be validated against the authentication server in the server group. The example network uses the server group named NPS for 802.1X authentication of the employee users. A RADIUS server called NPS1 is defined and added to the NPS server group. For details on 802.1X/EAP process, see the [Aruba 802.11n Networks Validated Reference Design](#).



If the RADIUS server is configured to return specific attributes for the users after authentication, then the server-derived role that corresponds to the returned attributes can be configured under server groups. For information about configuring a server-derived role, see the *ArubaOS 6.1 User Guide* available on the Aruba support site.

CLI

```
!  
aaa authentication-server radius "NPS1"  
    host "10.169.130.20"  
    key *****  
    timeout 30  
!  
  
aaa server-group "NPS"  
    auth-server NPS1  
!
```

WebUI Screenshot

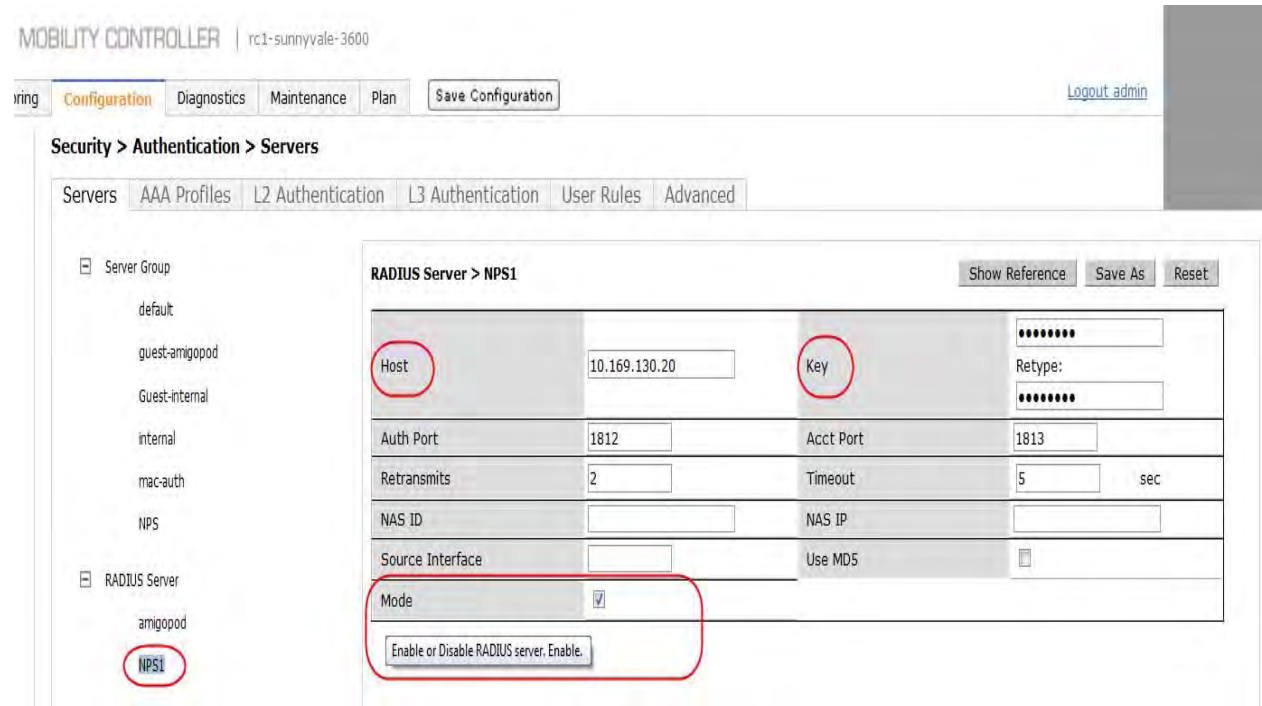


Figure 32 NPS1 RADIUS server

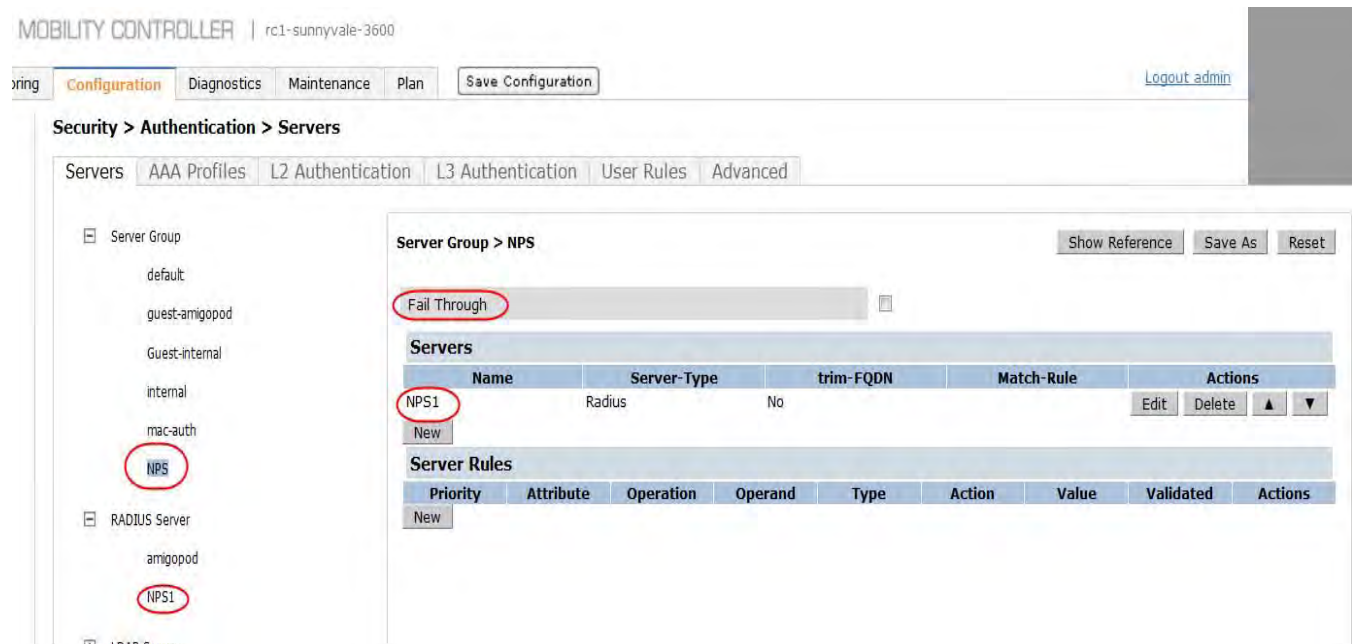


Figure 33 NPS server group

Configuring the Remote Employee AAA Profile

A AAA profile named remote-employee is used for the employee WLAN. First create a AAA profile called remote-employee and then configure the following parameters in it:

- Default role for 802.1X authentication: [Configuring the remote-employee Role on page 57](#)
- 802.1X authentication server group: NPS
- 802.1X profile:
 - Create the “remote-employee-dot1x” 802.1X profile.
 - Enable termination. (By default, the termination EAP type is EAP-PEAP and the termination inner EAP type is EAP-MSCHAPv2.)



Aruba recommends 802.1X termination on the controller. This feature, also known as AAA FastConnect™, offloads the cryptographic portion of 802.1X/EAP authentication exchange to the controller, which reduces the load on the RADIUS server. This feature is very useful when the authentication server is not 802.1X capable, such as an LDAP server. For details about AAA FastConnect, see the [Aruba 802.11n Networks Validated Reference Design](#).

CLI

```
!  
aaa authentication dot1x "remote-employee-dot1x"  
    termination enable  
    termination eap-type eap-peap  
    termination inner-eap-type eap-mschapv2  
!  
aaa profile "remote-employee"  
    initial-role "guest"  
    authentication-dot1x "remote-employee-dot1x"  
    dot1x-default-role "remote-employee"  
    dot1x-server-group "NPS"  
!
```

WebUI Screenshot

MOBILITY CONTROLLER | rc1-sunnyvale-3600

oring **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Logout admin](#)

Advanced Services > All Profile Management

Profiles	Profile Details																
- default-dot1x-psk - default-mac-auth - default-open - default-xml-api - employee - guest-branch - guest-home - guestnet - NoAuthAAAProfile remote-employee - MAC Authentication Profile - MAC Authentication Server Group 802.1X Authentication Profile remote-employee-dot1x 802.1X Authentication Server Group NPS - RADIUS Accounting Server Group - XML API server - RFC 3576 server	802.1X Authentication Profile > remote-employee-dot1x Show Reference Save As Reset Basic Advanced <table border="1"><tbody><tr><td>Max authentication failures</td><td>0</td></tr><tr><td>Enforce Machine Authentication</td><td>☐</td></tr><tr><td>Machine Authentication: Default Machine Role</td><td>guest</td></tr><tr><td>Machine Authentication: Default User Role</td><td>guest</td></tr><tr><td>Reauthentication</td><td>☐</td></tr><tr><td>Termination</td><td>☒</td></tr><tr><td>Termination EAP-Type</td><td>☐ eap-tls ☒ eap-peap</td></tr><tr><td>Termination Inner EAP-Type</td><td>☒ eap-mschapv2 ☐ eap-gtc</td></tr></tbody></table>	Max authentication failures	0	Enforce Machine Authentication	☐	Machine Authentication: Default Machine Role	guest	Machine Authentication: Default User Role	guest	Reauthentication	☐	Termination	☒	Termination EAP-Type	☐ eap-tls ☒ eap-peap	Termination Inner EAP-Type	☒ eap-mschapv2 ☐ eap-gtc
Max authentication failures	0																
Enforce Machine Authentication	☐																
Machine Authentication: Default Machine Role	guest																
Machine Authentication: Default User Role	guest																
Reauthentication	☐																
Termination	☒																
Termination EAP-Type	☐ eap-tls ☒ eap-peap																
Termination Inner EAP-Type	☒ eap-mschapv2 ☐ eap-gtc																

Figure 34 remote-employee-dot1x 802.1X authentication profile

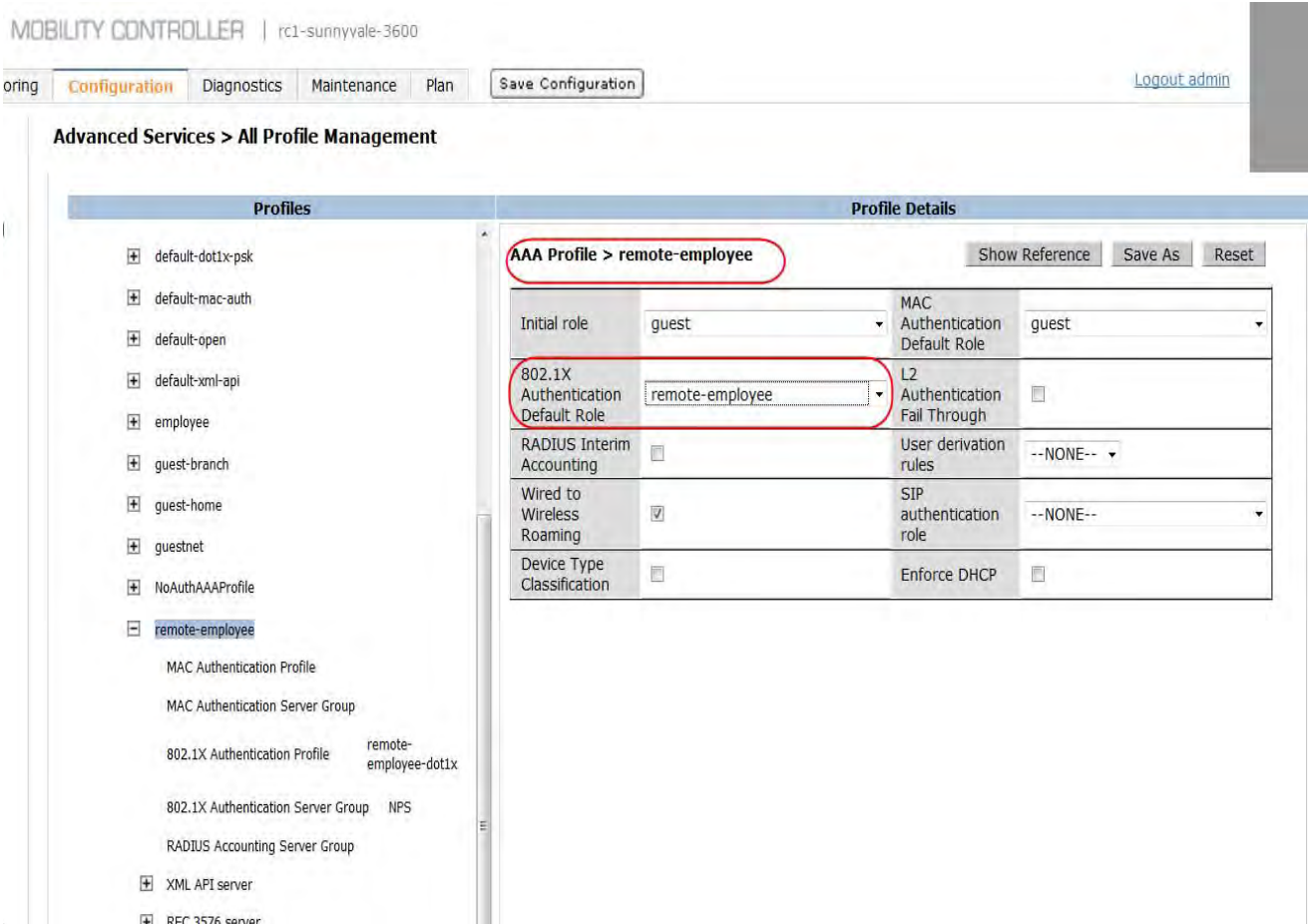


Figure 35 remote-employee AAA profile

Configuring the Remote Employee VAP Profile

Remote employees need access to corporate resources as well as the Internet. It is not desirable to tunnel noncorporate traffic back to the controller in the DMZ and then to the Internet. The RAP should dynamically forward the traffic based on the destination, which can be achieved using the split-tunnel forwarding mode. In the example network, the employee VAP is configured to operate in split-tunnel forwarding mode. In the example network, all remote employee devices including the wireless IP phones (802.1X capable) connect to employee SSID. [Table 18](#) summarizes the remote-employee VAP profile used in the example network.

Table 18 remote-employee VAP Profile

VAP Profile	VLAN	Forwarding Mode	Remote-AP Operation	AAA Profile	SSID Profile
remote-employee	135	split-tunnel	standard	remote-employee	remote-employee

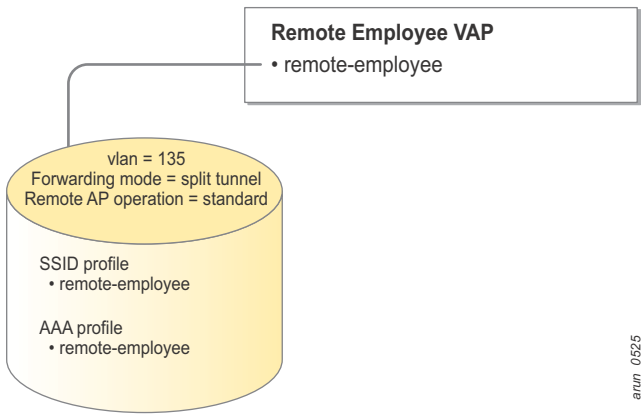


Figure 36 Remote employee VAP

CLI

```
!  
wlan virtual-ap "remote-employee"  
  aaa-profile "remote-employee"  
  ssid-profile "remote-employee"  
  vap-enable  
  vlan 135  
  forward-mode split-tunnel  
  rap-operation standard  
  band-steering  
!
```


WebUI Screenshot

Aruba Mobility Controller | rc1-sunnyvale-3600

Configuration | Diagnostics | Maintenance | Plan | [Save Configuration](#) | [Logout admin](#)

Advanced Services > All Profile Management

Profiles	Profile Details																																																
- AP - RF Management - Wireless LAN 802.11K Profile - SSID Profile - High-throughput SSID profile - Virtual AP profile - default - guest-branch - guest-home - remote-application - remote-backup remote-employee - AAA Profile remote-employee 802.11K Profile default - SSID Profile remote-employee - WMM Traffic Management Profile	Virtual AP profile > remote-employee Show Reference Save As R <table border="1"> <tr> <td>Virtual AP enable</td> <td>☒</td> <td>Allowed band</td> <td>all</td> </tr> <tr> <td>VLAN</td> <td>135</td> <td>Forward mode</td> <td>split-tunnel</td> </tr> <tr> <td>Deny time range</td> <td>--NONE--</td> <td>Mobile IP</td> <td>☒</td> </tr> <tr> <td>HA Discovery on-association</td> <td>☐</td> <td>DoS Prevention</td> <td>☐</td> </tr> <tr> <td>Station Blacklisting</td> <td>☒</td> <td>Blacklist Time</td> <td>3600 sec</td> </tr> <tr> <td>Dynamic Multicast Optimization (DMO)</td> <td>☐</td> <td>Dynamic Multicast Optimization (DMO) Threshold</td> <td>6</td> </tr> <tr> <td>Authentication Failure Blacklist Time</td> <td>3600 sec</td> <td>Multi Association</td> <td>☐</td> </tr> <tr> <td>Strict Compliance</td> <td>☐</td> <td>VLAN Mobility</td> <td>☐</td> </tr> <tr> <td>Preserve Client VLAN</td> <td>☐</td> <td>Remote-AP Operation</td> <td>standard</td> </tr> <tr> <td>Drop Broadcast and Multicast</td> <td>☐</td> <td>Convert Broadcast ARP requests to unicast</td> <td>☐</td> </tr> <tr> <td>Deny inter user traffic</td> <td>☐</td> <td>Band Steering</td> <td>☒</td> </tr> <tr> <td>Steering Mode</td> <td>prefer-5ghz</td> <td></td> <td></td> </tr> </table>	Virtual AP enable	☒	Allowed band	all	VLAN	135	Forward mode	split-tunnel	Deny time range	--NONE--	Mobile IP	☒	HA Discovery on-association	☐	DoS Prevention	☐	Station Blacklisting	☒	Blacklist Time	3600 sec	Dynamic Multicast Optimization (DMO)	☐	Dynamic Multicast Optimization (DMO) Threshold	6	Authentication Failure Blacklist Time	3600 sec	Multi Association	☐	Strict Compliance	☐	VLAN Mobility	☐	Preserve Client VLAN	☐	Remote-AP Operation	standard	Drop Broadcast and Multicast	☐	Convert Broadcast ARP requests to unicast	☐	Deny inter user traffic	☐	Band Steering	☒	Steering Mode	prefer-5ghz		
Virtual AP enable	☒	Allowed band	all																																														
VLAN	135	Forward mode	split-tunnel																																														
Deny time range	--NONE--	Mobile IP	☒																																														
HA Discovery on-association	☐	DoS Prevention	☐																																														
Station Blacklisting	☒	Blacklist Time	3600 sec																																														
Dynamic Multicast Optimization (DMO)	☐	Dynamic Multicast Optimization (DMO) Threshold	6																																														
Authentication Failure Blacklist Time	3600 sec	Multi Association	☐																																														
Strict Compliance	☐	VLAN Mobility	☐																																														
Preserve Client VLAN	☐	Remote-AP Operation	standard																																														
Drop Broadcast and Multicast	☐	Convert Broadcast ARP requests to unicast	☐																																														
Deny inter user traffic	☐	Band Steering	☒																																														
Steering Mode	prefer-5ghz																																																

Figure 37 remote-employee VAP profile

Chapter 12: Configuring the Guest Role and VAP for Fixed Telecommuter Deployment

In fixed telecommuter deployments, family members and other personal devices need access to the Internet. The family members and personal devices need a separate WLAN because they cannot connect to the employee network, which uses 802.1X. The traffic from the family members is always destined either to the Internet or to the local devices such as a family printer. So the RAPs should locally bridge all the traffic on the guest WLAN. The remote users on the employee network need access to local devices like family printers, so the guest network should be accessible by the corporate users. However, the access to corporate network from the guest network is always denied.

Unlike campus and branch office deployments, the guest access in fixed telecommuter deployments is different. In these types of deployments, the Internet service is not provided by the organization and hence the guest users (alias home users) are not restricted to what services they use on the Internet. The main purpose of the guest network in these deployments is to eliminate the need for a separate device, such as a wireless router, to provide Internet access for home users and local devices.

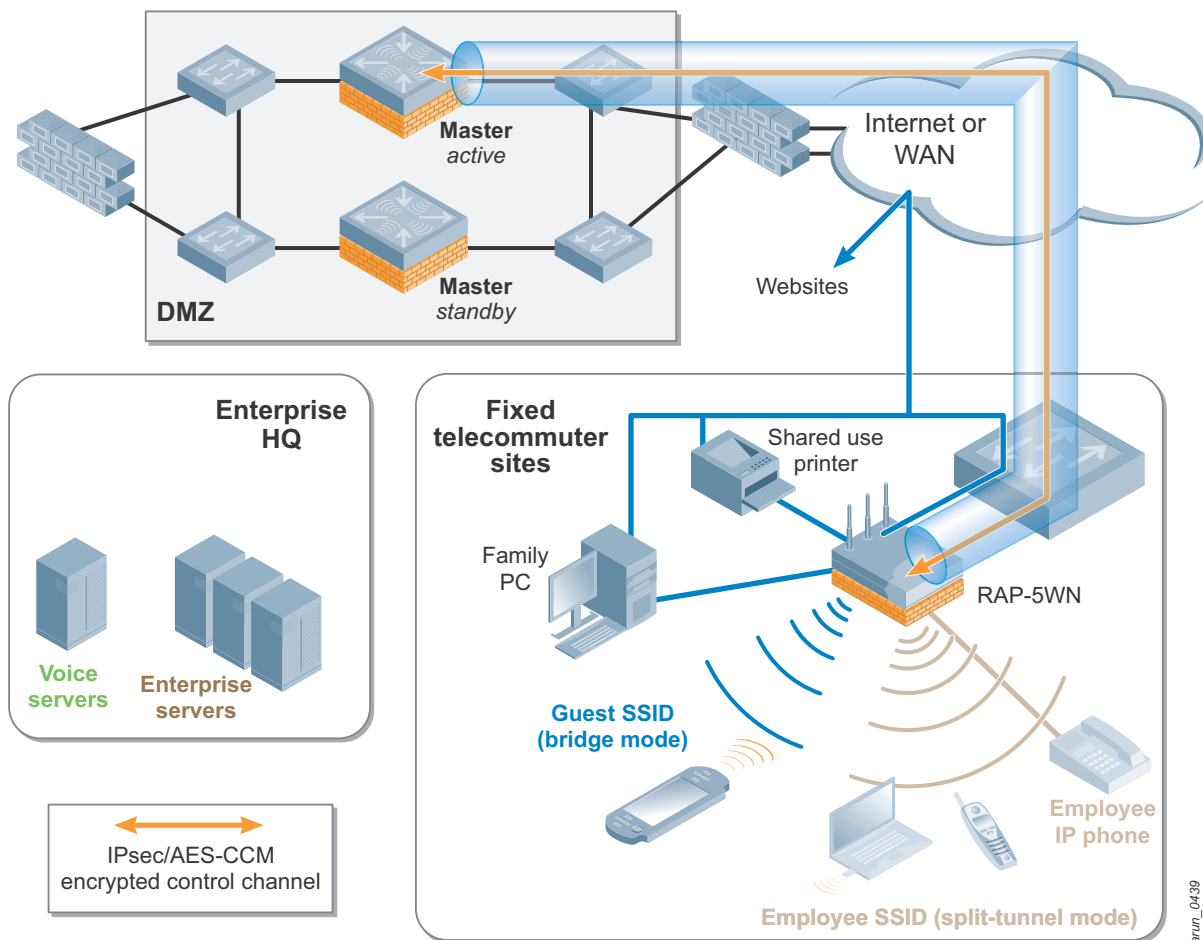


Figure 38 Guest network in fixed telecommuter deployments

The guest role in fixed telecommuter deployments is built to serve the requirements already described. Before you configure the guest role for fixed telecommuter deployments, first you must create the policy associated with it. In the example network, the guest role for telecommuter deployment has these policies:

- common-dhcp (For details, see “[Configuring the common-dhcp Policy.](#)”)
- guest-home

Configuring the guest-home-access Policy

The guest-home-access policy is part of the guest role assigned to guest users in a fixed telecommuter solution. The guest-home policy is designed to do the following things:

- Allow employee users access the guest network.
- Allow traffic between guest users to be bridged locally.
- Deny traffic from guest network to employee network.
- Source-NAT traffic to any other destination based on the traffic destination.

[Table 19](#) summarizes the rules used for the guest-home policy.

Table 19 Rules Used for the guest-home Policy

Rule Number	Source	Destination	Service	Action	Purpose
1	alias internal-network	alias guest-network	any	permit	This rule allows traffic from the employee network to the guest network.
2	alias guest-network	alias guest-network	any	permit	This rule allows traffic between guest users to be bridged locally without the need for source-NATing.
3	user	any	any	route scr-nat	This rule ensures that traffic to any other destination is source-NATed according to the destination of the traffic.

CLI

```
!
ip access-list session guest-home
  alias internal-network alias guest-network any permit
  alias guest-network alias guest-network any permit
  user any any route src-nat
!
```

WebUI Screenshot

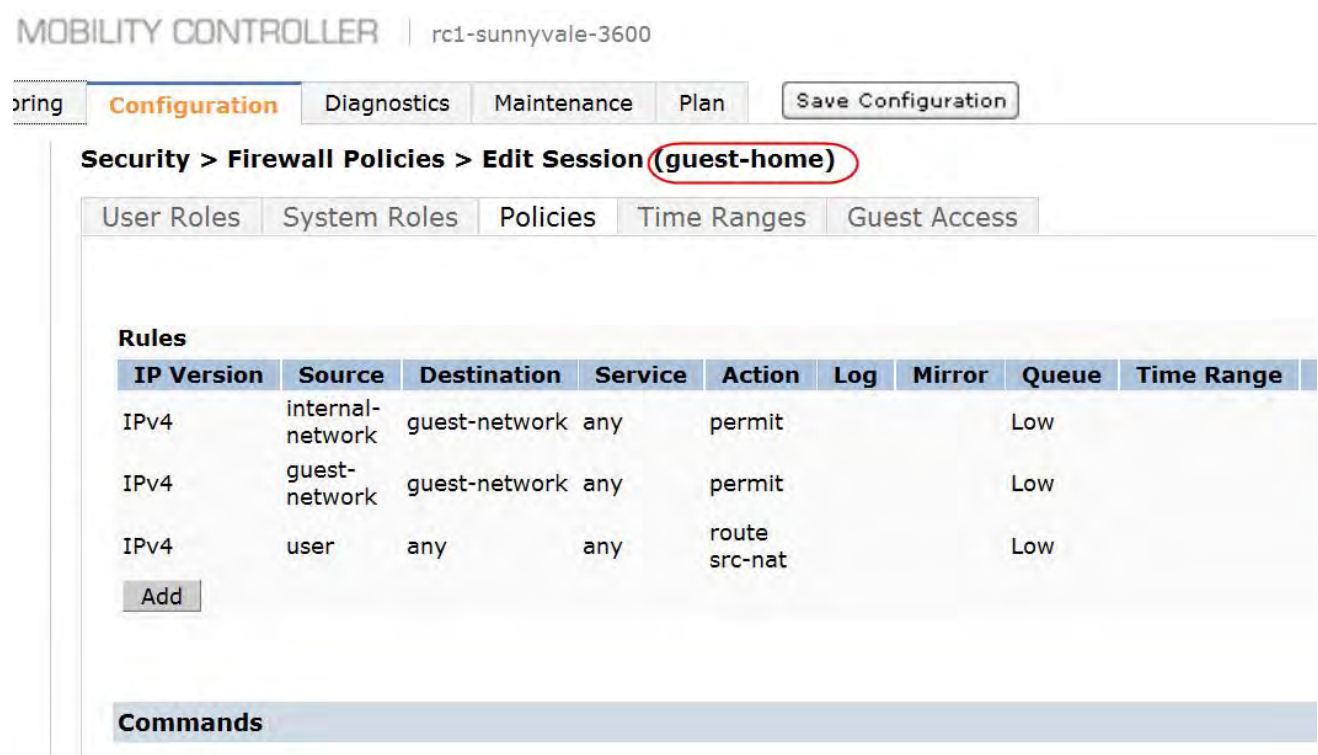


Figure 39 guest-home policy

Configuring the Guest Role for Fixed Telecommuter Deployments

The guest role is assigned to users who successfully authenticate to the guest WLAN. After all the required policies are configured, place the required firewall policies in correct order to create the guest role. Remember, the order of policies determines the behavior of a user role.

In the example network, the guest role used in fixed telecommuter deployments is named guest-home. Table 20 summarizes the order of the policies in the guest-home user role.

Table 20 guest-home User Role

Policy Number	Policy Name	Purpose
1	common-dhcp	This policy denies personal DHCP servers but allows legitimate DHCP services. For details, see “Common-dhcp Policy.”
2	guest-home	This policy allows access from corporate network to guest network and source-NATs all other traffic based on the destination of the traffic. For details see, “guest-home Policy.”

CLI

```
!
user-role guest-home
  access-list session common-dhcp
  access-list session guest-home
!
```

WebUI Screenshot

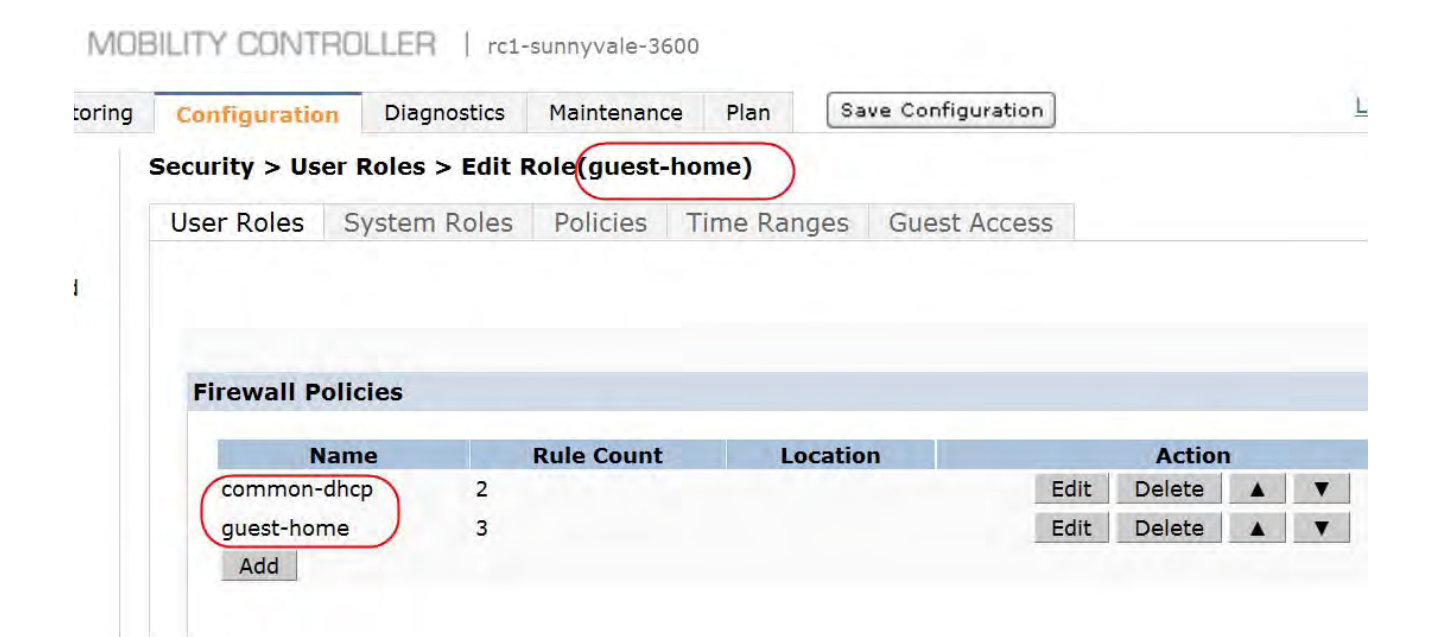


Figure 40 guest-home user role

Configuring the Guest SSID for Fixed Telecommuter Deployments

For wireless access at home, a person normally uses a wireless router. In most cases, the home wireless network is secured with PSK to prevent against wireless eavesdropping. If the wireless network is not secure, malicious users can use simple protocol analyzers to eavesdrop on wireless traffic that is not encrypted by protocols like HTTPS and IPsec. Moreover, an unsecure network is also open to wardriving. So, the guest network in fixed telecommuter deployments should be secured.

The guest SSID in fixed telecommuter deployments usually is designed to use WPA2-PSK for authentication and AES for encryption. PSK should be distributed to the employees, so all employees should be educated about the importance of key management. Organizations that expect their employees to use their own wireless routers for home user wireless access can neglect the implementation of the guest WLAN. Even in these cases, organizations need to provide a wired port for guest access to plug in the wireless router and switches because most users have only a single broadband connection. For configuration of wired ports on a RAP, see [Chapter 18: RAP Wired Ports](#).

The guest SSID in the example network uses WPA2-PSK for authentication and AES for encryption. Table 21 summarizes the guest SSID used in the example network.

Table 21 guest-home SSID Profile

SSID Profile	Network Name (SSID)	Authentication	Encryption	WMM	Purpose
guest-home	guest	WPA2-PSK	AES	--	Provides wireless access to home user and wireless printers in fixed telecommuter deployments.

```
!
wlan ssid-profile "guest-home"
  essid "guest"
  opmode wpa2-psk-aes
  wpa-passphrase *****
!
```

WebUI Screenshot

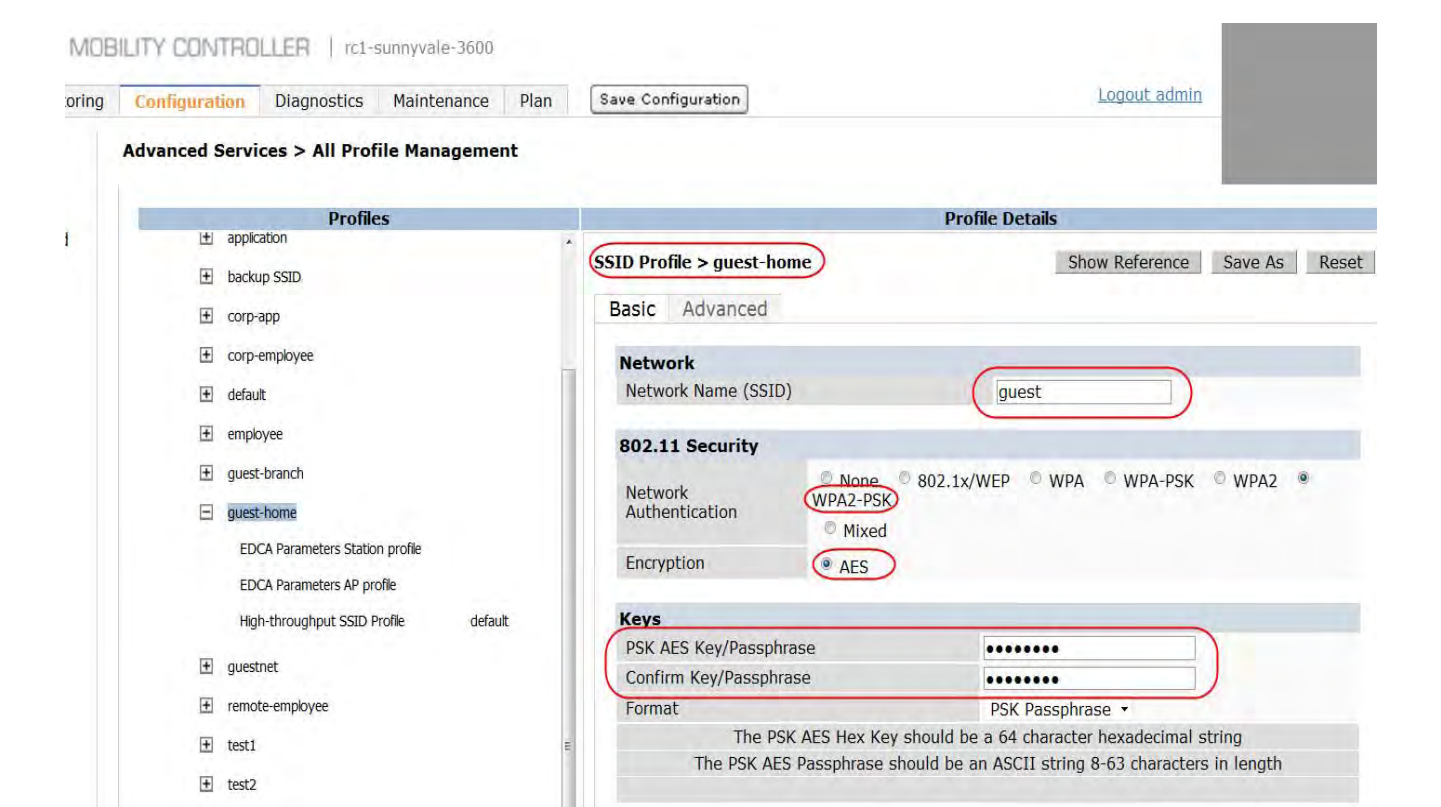


Figure 41 guest-home SSID profile

Configuring the Guest AAA Profile for Fixed Telecommuter Deployments

In the example network, a AAA profile named guest-home is used for the guest WLAN of fixed telecommuter deployments. PSK is used for authentication, so the default role that is assigned to authenticated users is specified in the initial role parameter of the AAA profile. To reduce the number of profiles, Aruba has included the default-psk profile within the 802.1X profile. The profiles are combined because the dynamic key generation process of a WPA™/WPA2 PSK process is similar to that key generation process of 802.1X/EAP. The PSK passphrase is run through an algorithm that converts it into a pairwise master key (PMK). This PMK is used in the four-way handshake process to generate the dynamic encryption keys. Select the predefined profile named default-psk as the 802.1X profile when PSK is used for authentication.

The following parameters are configured in the guest-home AAA profile:

- Initial Role: guest-home role
- 802.1X Profile: default-psk (predefined)



If you do not assign an 802.1X profile in the AAA profile that is used for PSK, connectivity issues may occur.

CLI

```
!  
aaa profile "guest-home"  
    initial-role "guest-home"  
    authentication-dot1x "default-psk"  
!
```


WebUI Screenshot

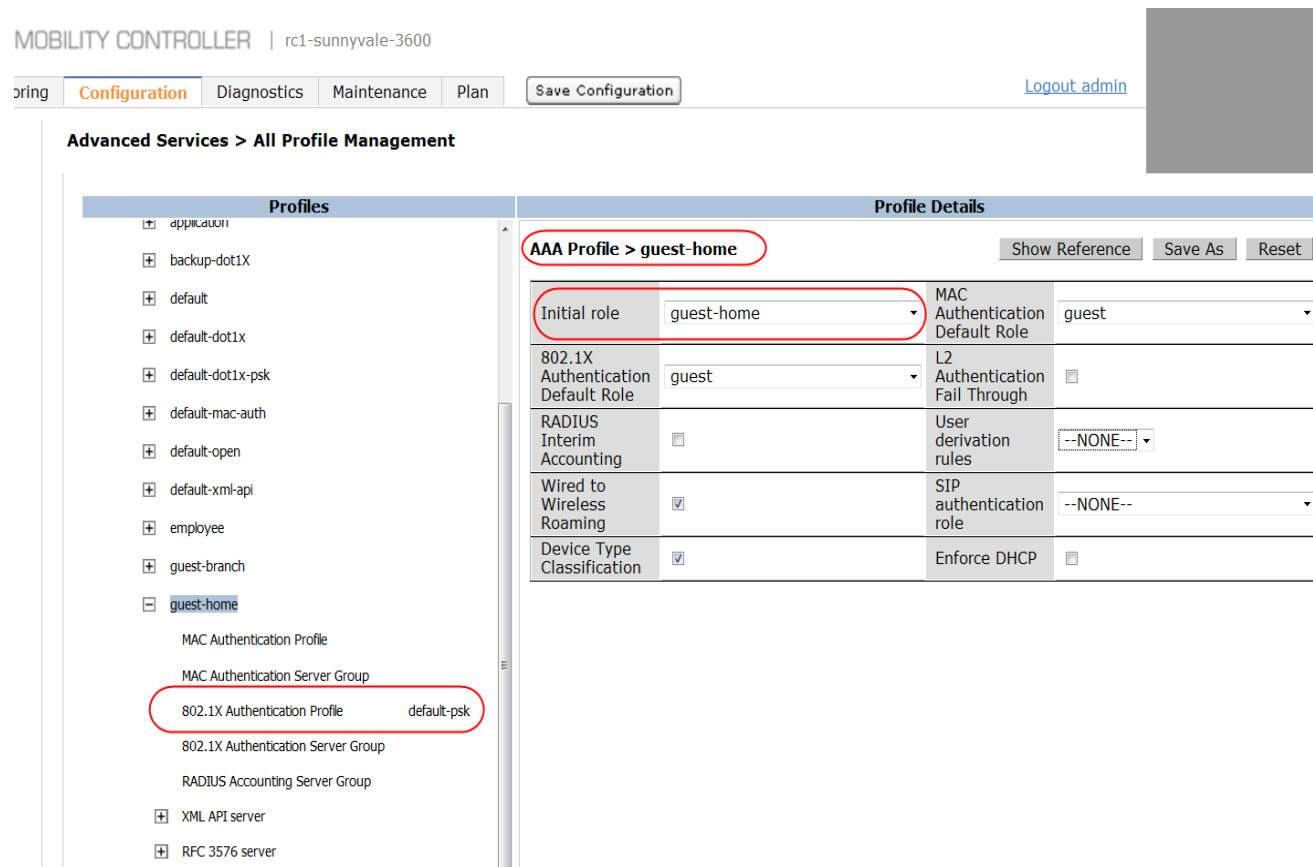


Figure 42 guest-home AAA profile

Configuring the Guest VAP Profiles for Fixed Telecommuter Deployments

All the traffic from the home users is destined either to the Internet or to local devices such as family printers. In this case, the RAP needs to bridge the traffic locally and there is no need for a data plane to controller in the DMZ as the traffic should never be destined to the corporate network. This can be achieved using the bridge forwarding mode. In the example network the guest VAP used in fixed telecommuter deployments is configured to operate in bridge forwarding mode. The VLAN configuration for bridge mode SSIDs is slightly different. For details about VLAN configuration for bridge forwarding mode, see [Chapter 16: Configuring the AP System Profiles](#).

Table 22 summarizes the guest VAP profile used in the example network for telecommuter deployments.

Table 22 guest-home VAP Profile

VAP Profile	VLAN	Forwarding Mode	Remote-AP Operation	AAA Profile	SSID Profile
guest-home	188	bridge	always	guest-home	guest-home

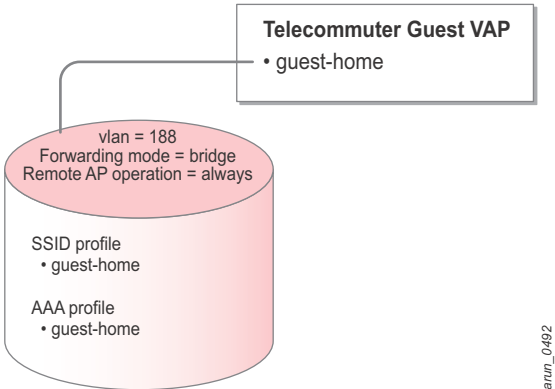


Figure 43 Telecommuter guest VAP

CLI

```
!
wlan virtual-ap "guest-home"
  aaa-profile "guest-home"
  ssid-profile "guest-home"
  vap-enable
  vlan 188
  forward-mode bridge
  rap-operation always
  band-steering
!
```

WebUI Screenshot

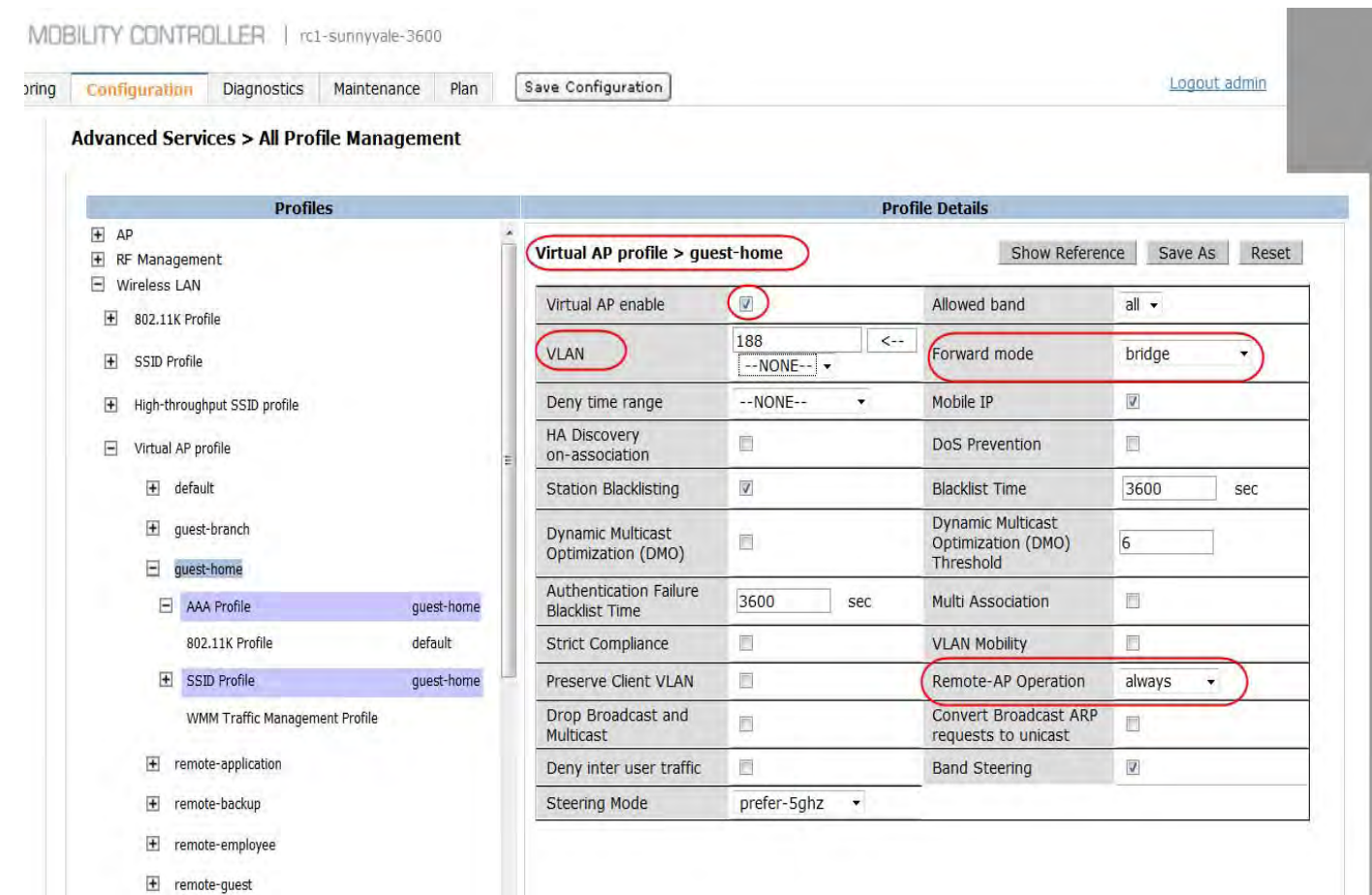


Figure 44 guest-home VAP profile

Chapter 13: Micro Branch Office Solution

Historically, most branch offices have received less-sophisticated and lower-performance network technology and IT services than workers on the enterprise core network. Paradoxically, the configuration and management costs have been much higher as a whole for the remote sites. The focus of the Aruba virtual branch network (VBN) architecture is to maintain the simplicity and ease-of-use of a software VPN solution and deliver full IP network services to multidevice, multiuser offices. This architecture shatters the cost and complexity barriers that exist today in establishing new remote offices for multiple devices and users.

The Aruba RAP solution fully meets the needs of the micro branch offices. Enterprises can leverage the built-in firewall in the RAP to provide the secure wired and wireless services needed by branch office employees, as well as Internet access for their guests.

Requirements of Micro Branch Office Deployments

Micro branch office solutions have these requirements:

- secure wireless and wired access to branch office employees
- secure access to corporate resources at the enterprise HQ
- secure and reliable VoIP services through the centralized PBX at the HQ
- QoS for latency sensitive applications, such as voice
- guest access through captive portal

Creating AP Group for RAPs in Micro Branch Office Deployments

The RAPs used in micro branch office deployments should be configured to provide these services:

- wired and wireless access to employee PCs and laptops to securely connect to the corporate resources
- wired and wireless access to employee VoIP phones to securely connect to the corporate voice server
- wireless guest access to provide Internet connectivity using specific protocols such as HTTP/HTTPS
- wired ports for branch office printers and fax machines without compromising the corporate security policy

In the example network, an AP group called micro-branch-office is created for branch office deployments. All the RAPs deployed in micro branch offices setup belong to the micro-branch-office AP group.

The RAPs in the micro-branch-office AP group perform these actions:

- Broadcast employee SSID with split-tunnel forwarding mode and 802.1X authentication (WPA2-Enterprise).
- Broadcast guest SSID with split-tunnel forwarding mode and captive portal authentication.

- Provide wired employee access on wired port 1, 2, and 3. All three ports provide 802.1X authentication and MAC authentication simultaneously:
 - Successful 802.1X authentication assigns employee role.
 - Successful MAC authentication assigns application role.
- Provide wired guest access (captive portal authentication via split-tunnel forwarding mode) on wired port 4.

Remote Employee Role and VAP Profile for Micro Branch Office Deployments

In most cases, the access privileges of employees and the requirements of employee WLAN in home office and branch office deployments are the same. For configuration of the remote employee WLAN, see [Chapter 10: Configuring the Remote Employee Role](#) and [Chapter 11: Remote Employee VAP](#).

In certain branch office deployments, the security policy of an organization may want to deny employees from accessing the guest network. In such situations, create a rule in the remote-employee policy that denies access from corporate users to guest network and append it as the second rule in the remote-employee policy. [Table 23](#) summarizes the remote-employee policy for deployments that deny access from corporate network to guest network.

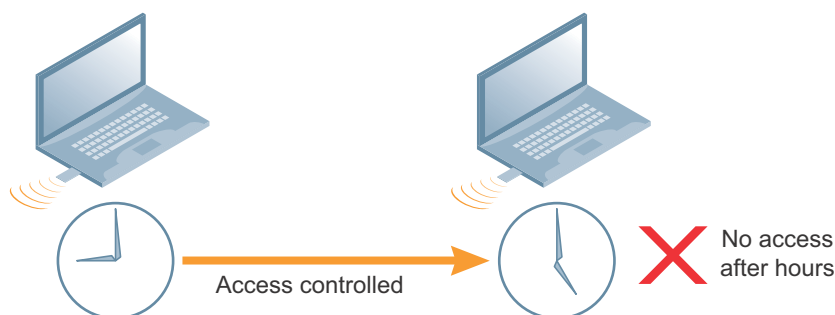
Table 23 Alternative remote-employee Role for Micro Branch Office Deployments

Rule Number	Source	Destination	Service	Action	Purpose
1	alias internal-network	alias internal-network	any	permit	This rule allows all types of traffic between the user and corporate network. The traffic can be initiated either by the user or the devices in the corporate network. The “permit” action implies tunneling, which is used for corporate traffic. Any traffic that meets the requirements of this rule is forwarded to the controller through the tunnel.
2	alias internal-network	alias guest-network	any	deny	This rule denies traffic from corporate network to guest network.
3	user	any	any	route scr-nat	This rule ensures that users can reach the Internet and local resources. The “route scr-nat” action properly source-NATs the traffic depending on the destination and eliminates the need to define static NAT pools. If the traffic is bound to the Internet, then the source-NATing is performed using the RAP IP address obtained from the ISP or home router. If the traffic is bound to a local subnet for which the RAP is the DHCP server or gateway, then the source-NATing is performed using the gateway IP of this local subnet. Placing this rule at the end ensures that “route scr-nat” action is performed only on the noncorporate traffic. The rules 1 through 3 indicate that access from another network to the employee network is denied.

Chapter 14: Configuring the Guest Roles and VAP Profile for Micro Branch Office Deployments

Just like in enterprise networks, the guest usage in micro branch offices requires the following special considerations:

- Guest users must be separated from employee users by VLANs in the network.
- Guests must be limited not only in where they may go, but also by what network protocols and ports they may use to access resources.
- Guests should be allowed to access only the local resources that are required for IP connectivity. These resources include DHCP and possibly DNS, if an outside DNS server is not available. Aruba recommends the use of Public DNS for guest DNS services.
- All other internal resources should be off limits for the guest. This restriction is achieved usually by denying any internal address space to the guest user.
- A time-of-day restriction policy should also be used to allow guests to access the network only during normal working hours, because they should be using the network only while conducting official business. Accounts should be set to expire when their local work is completed, typically at the end of each business day.



arun_060

Figure 45 Guest access has a time limit

Unlike employees, the guest users typically log in through a captive portal. Usually, guests are assigned two different roles. One role is assigned when they associate to the guest SSID and the other is assigned when they authenticate successfully through the captive portal. Only the guests who successfully authenticate are allowed to use the services needed to connect to the Internet.

Guest authentication and management can be provided through the internal resources of the Aruba controller or through *ClearPass Guest*. The internal resources of the Aruba controller can be used for visitor management in small deployments. However, Aruba recommends the use of *ClearPass Guest* for visitor management in large remote deployments that have many branch sites. For information on deploying the Aruba controller for visitor management, see the *Guest Access on ArubaOS Application Note*. For more information on the special features and deployment scenarios of *ClearPass Guest*, see the *ClearPass Guest deployment guide* available at the Aruba support site. This VRD explains only the configurations required on the Aruba controller when *ClearPass Guest* is used for visitor management.

Regardless of the forwarding mode, all the settings that are related to captive portal reside at the controller and are not pushed to the RAPs. So to present the guest users with the captive portal page,

they have to connect to the controller. Hence in remote deployments, the guest network at branch offices cannot be deployed in bridge forwarding mode if captive portal authentication is required.

The guest network at branch offices is usually deployed in split-tunnel forwarding mode for captive portal authentication. In this case, user roles are used to achieve the same behavior as bridge forwarding mode while providing captive portal authentication. The initial role assigned to the guests allows them to reach the captive portal page through the controller. After the guests pass the captive portal authentication, the authenticated role that is assigned to them can be designed to behave like a bridge forwarding mode.



NOTE

The user VLAN on a VAP configured for captive portal authentication must have an L3 interface on the controller. For captive portal authentication, it is recommended that the controller be the default gateway for users. If you need to use an external gateway, create an L3 interface on the controller for that user VLAN. The example network uses the controller as the DHCP server and default gateway for the guest VLAN. The guest VLANs that are local to a controller should be source-NATed by the controller.

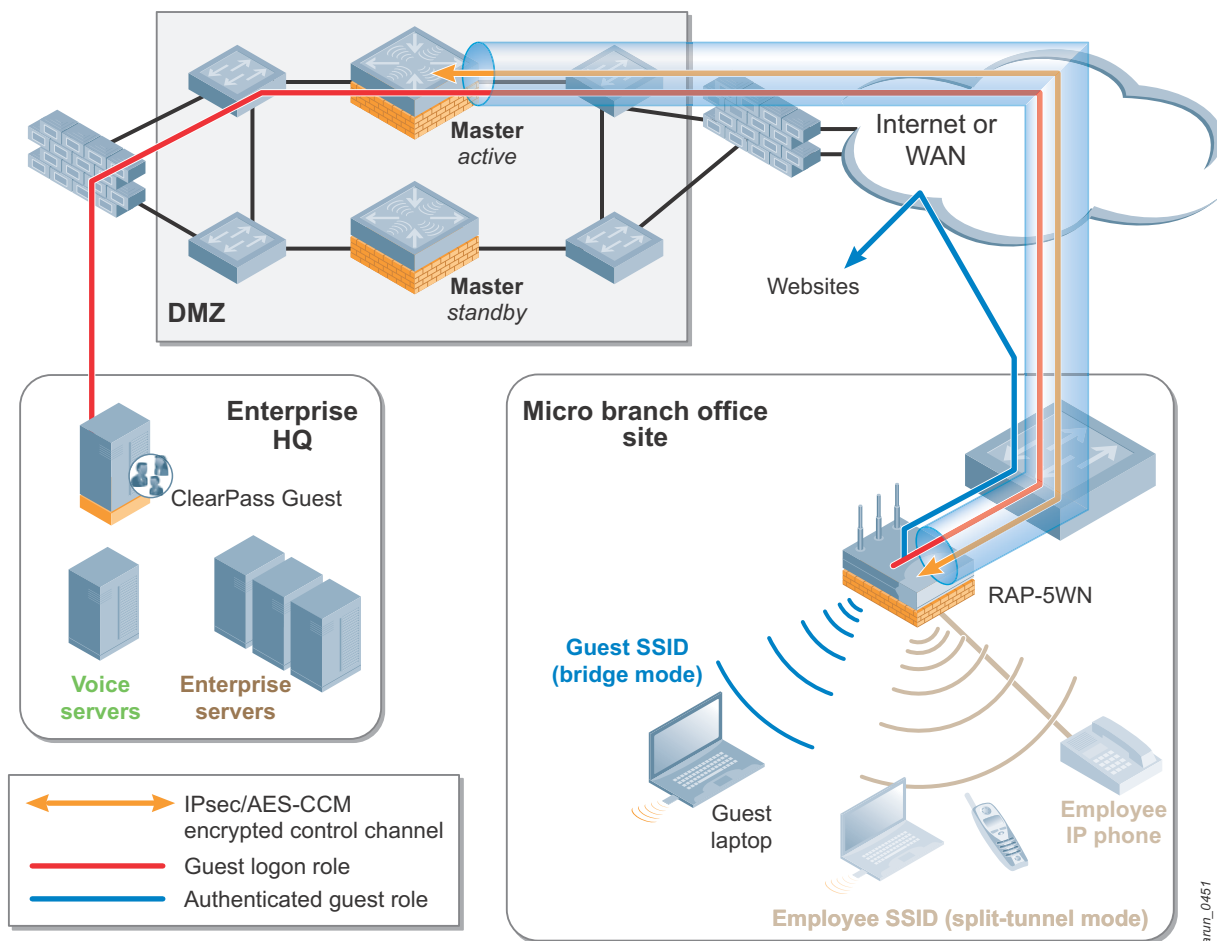


Figure 46 Remote guest network with captive portal authentication

The example network uses the guest-branch-logon role as the initial role and the auth-guest role for authenticated guests. Before you configure these two roles, first create the policies that are associated with them.

The guest-branch-logon role uses these policies:

- clearpass-guest
- captiveportal (predefined policy)
- guest-branch-logon-access

The auth-guest role uses these policies:

- cplogout (predefined policy)
- guest-branch-logon-access
- block-internal-access
- auth-guest-access
- drop-and-log

Configuring the clearpass-guest Policy

The clearpass-guest policy allows HTTP and HTTPS traffic only to the ClearPass Guest server that is defined in the clearpass-guest alias. This policy is used in the preauthenticated role and allows the client-based HTTP and HTTPS traffic to reach the hosted captive portal pages on the ClearPass Guest appliance.

A time range is used to allow users to associate to the guest network only during certain hours of the day. A time range called working-hours is created and used in the example network.

Table 24 summarizes the rules used by the clearpass-guestpolicy.

Table 24 ClearPass Guest Policy

Rule Number	Source	Destination	Service	Time range	Action	Purpose
1	user	alias clearpass-guest	service svc-http	working-hours	permit	This rule allows HTTP traffic from the users to ClearPass Guest server. The permitted traffic is source-NATed by the controller.
2	user	alias clearpass-guest	service svc-https	working-hours	permit	This rule allows HTTPS traffic from the users to ClearPass Guest server. The permitted traffic is source-NATed by the controller.

CLI Configuration

```

!
time-range "working-hours" periodic Weekday 07:30 to 17:30
!
ip access-list session clearpass-guest
  user  alias clearpass-guest svc-http permit time-range "working-hours"
  user  alias clearpass-guest svc-https permit time-range "working-hours"
!

```

WebUI Screenshot

MOBILITY CONTROLLER | rc1-sunnyvale-3600

Configuration | Diagnostics | Maintenance | Plan | [Save Configuration](#) | [Logout admin](#)

Security > Access Control > TimeRange > Edit Time Range(working-hours) | [« Back](#)

User Roles | System Roles | Policies | Time Ranges | Guest Access

Name:

Type: ☐ Absolute ☒ Periodic

Start Day	Start Time	End Day	End Time	Actions
weekday	07:00		17:30	Delete

[Add](#)

[Apply](#)

Commands | [View Commands](#)

Figure 47 Time range

MOBILITY CONTROLLER | rc1-sunnyvale-3600

Configuration | Diagnostics | Maintenance | Plan | [Save Configuration](#) | [Logout admin](#)

Security > Firewall Policies > Edit Session (clearpass-guest)

User Roles | System Roles | Policies | Time Ranges | Guest Access

Rules

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time Range
IPv4	user	clearpass-guest	svc-http	permit			Low	working-hours
IPv4	user	clearpass-guest	svc-https	permit			Low	working-hours

[Add](#)

Figure 48 clearpass-guest policy

Configuring the guest-branch-logon-access Policy

The guest-branch-logon-access policy is similar to the predefined logon-control policy, but it is much more restrictive. The guest-branch-logon-access policy is a part of the guest-branch-logon and auth-guest roles. The rules defined in this policy allow these exchanges:

- Allow DHCP exchanges between the user and the DHCP server during business hours, but block other users from responding to DHCP requests.
- Allow DNS exchanges between the user and the public DNS server during business hours. Traffic is source-NATed using the IP interface of the controller for the guest VLAN.

Guest users are denied access to the internal network, so the public-DNS alias is used. All the DNS queries of the guest users are forwarded to these public DNS servers.

Table 25 summarizes the rules used by the guest-branch-logon-access policy.

Table 25 Rules Used by the guest-branch-logon-access Policy

Rule Number	Source	Destination	Service	Time range	Action	Purpose
1	user	any	UDP min port = 68 max port = 68		drop	This rule drops responses from a personal DHCP server. This action prevents the clients from acting as DHCP servers. (This rule should be active always and not just during the working hours.)
2	any	any	service svc-dhcp (udp 67 68)	working-hours	permit	This rule allows clients to request and discover DHCP IP addresses over the network. The DHCP server on the network does not fall under the user category. Therefore, its response on port 68 is not dropped by the first rule. The first two rules guarantee that DHCP is processed only by legitimate DHCP servers on the network.
3	any	alias public-DNS	service svc-dns (udp 53)	working-hours	permit	This rule allows DNS queries only to the DNS servers that are defined in the public-DNS alias.

CLI Configuration

```
!
ip access-list session guest-logon-access
  user any udp 68 deny
  any any svc-dhcp permit time-range "working-hours"
  user alias public-dns svc-dns permit time-range "working-hours"
!
```

WebUI Screenshot

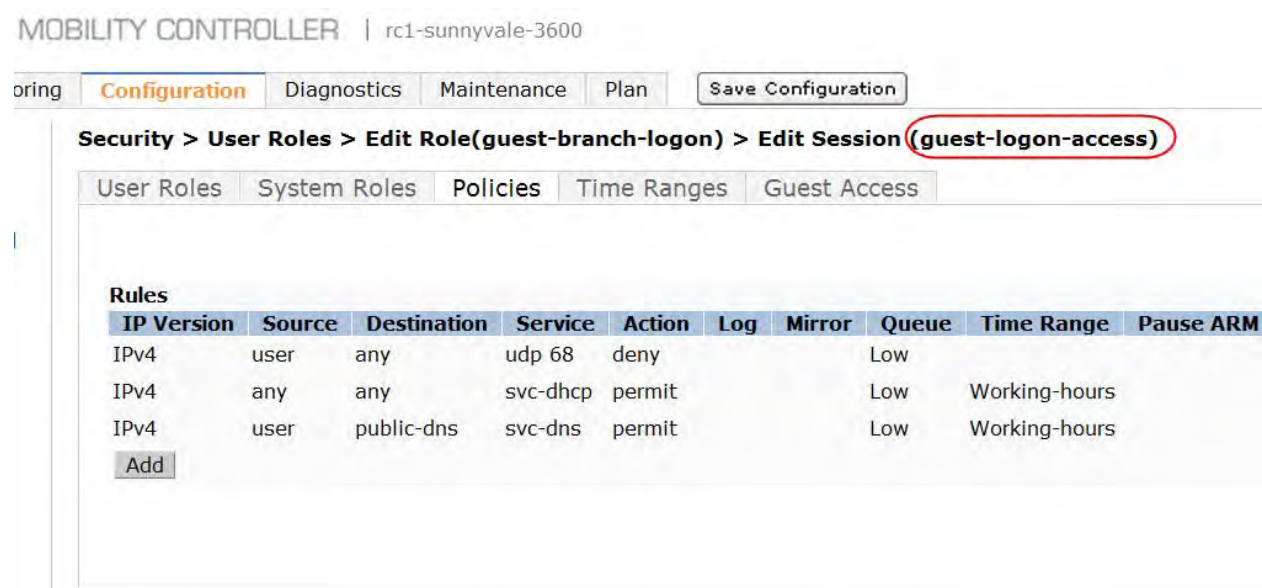


Figure 49 guest-logon-access policy

Configuring the block-internal-access Policy for the Guest Role

The internal resources of an organization should be available only to employees or to the trusted groups. Guest users are not part of the trusted entity, so they must be denied access to all internal resources. As the name implies, the block-internal-access policy denies access to all internal resources. This policy is a part of the auth-guest role.

Table 26 summarizes the rule used by the block-internal-access policy.

Table 26 Rule Used by the block-internal-access Policy

Rule Number	Source	Destination	Service	Action	Purpose
1	user	alias internal-network	any	drop	This rule denies access to all the addresses that are in the internal- network alias.

CLI Configuration

```
!  
ip access-list session block-internal-access  
  user alias internal-Network any deny  
!
```

WebUI Screenshot

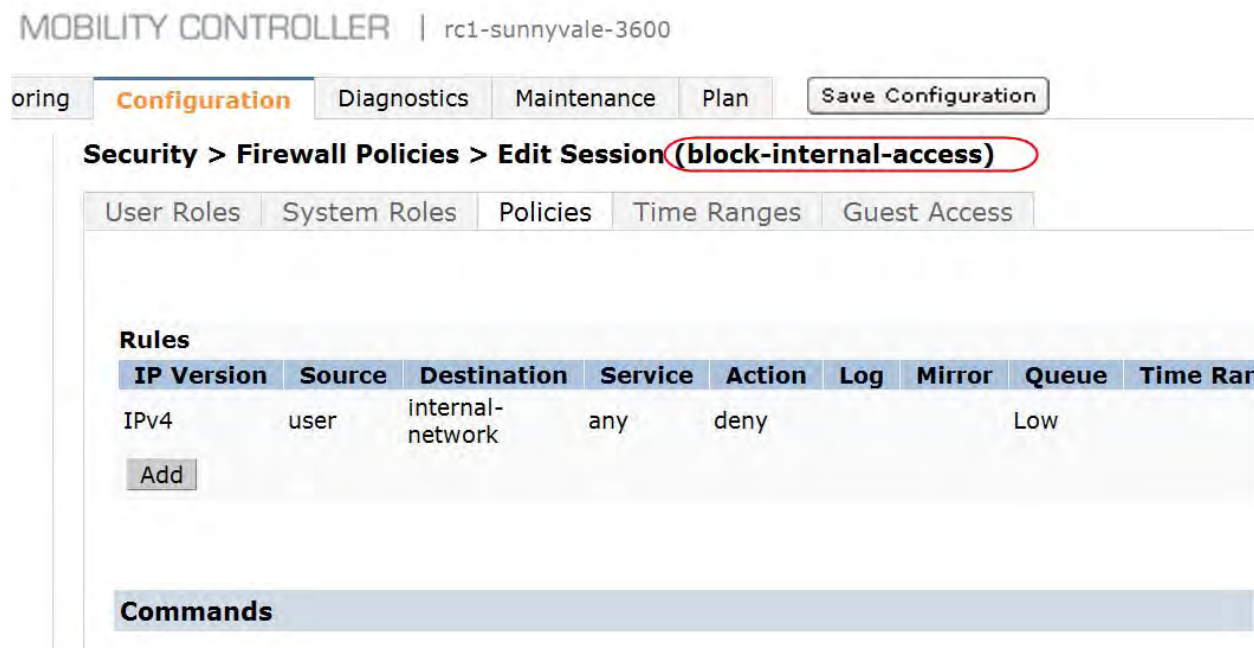


Figure 50 *block-internal-access policy*

Configuring the auth-guest-access Policy

The most important purpose of the auth-guest-access policy is to define the protocols and ports that the users are allowed to access. This policy is an integral part of the auth-guest role. The auth-guest-access policy allows HTTP and HTTPS traffic to go to any destination from the user during business hours. The traffic is route source-NATed using the IP address obtained by the RAP from ISP.



NOTE

If you want your guest users to use their IPsec clients, create rules in this policy that allows the use of ports 4500 (for IPsec NAT-T) and 500 (for IKE).

Table 27 summarizes the rules used by the auth-guest-access policy.

Table 27 Rules Used by the auth-guest-access Policy

Rule Number	Source	Destination	Service	Time range	Action	Purpose
1	user	any	service svc-http	working-hours	route scr-nat	This rule allows HTTP traffic from the users to any destination. The permitted traffic is route source-NATed by the RAP. The HTTP traffic that is bound to the Internet is source-NATed using the RAP IP address obtained from the ISP or home router.
2	user	any	service svc-https	working-hours	route scr-nat	This rule allows HTTPS traffic from the users to any destination. The permitted traffic is route source-NATed by the RAP. The HTTPS traffic that is bound to the Internet is source-NATed using the RAP IP address obtained from the ISP or home router.

CLI Configuration

```
!
ip access-list session auth-guest-access
  user any svc-http route src-nat time-range working-hours
  user any svc-https route src-nat time-range working-hours
!
```

WebUI Screenshot

MOBILITY CONTROLLER | rc1-sunnyvale-3600

oring **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Logout](#)

Security > Firewall Policies > Edit Session (auth-guest-access)

User Roles System Roles Policies Time Ranges Guest Access

Rules

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	P
IPv4	user	any	svc-http	route src-nat			Low	Working-hours	
IPv4	user	any	svc-https	route src-nat			Low	Working-hours	

[Add](#)

Figure 51 auth-guest-access policy

Configuring the drop-and-log Policy

The drop-and-log policy denies all traffic and records the network access attempt.



The logging function in this policy increases your syslog repository. If you do not require logging, ignore this policy.

Table 28 summarizes the rule used by the drop-and-log policy.

Table 28 Rule Used by the drop-and-log Policy

Rule Number	Source	Destination	Service	Action	Log	Purpose
1	user	any	any	deny	yes	This rule denies access to all services on the network and logs the network access attempt.

CLI Configuration

```
!
ip access-list session drop-and-log
  user any any deny log
!
```

WebUI Screenshot



Figure 52 drop-and-log policy

Configuring the Initial Guest Role

The guest-branch-logon role is the first role that is assigned to the users when they associate with the guest SSID. A user in this role has access only to the DHCP and DNS services. Unlike 802.1X/EAP, captive portal is a Layer 3 type authentication. A user who associates to the guest SSID is given an IP address and related DNS information even before he authenticates himself. When this user opens the browser and tries to access a web page, the guest-branch-logon role directs him to a captive portal page. The captive portal page requires login credentials. The captive portal authentication profile that is appended to this role specifies the captive portal login page and other configurable parameters, such as the default role, the authentication server, and the welcome page. To create and add the captive portal authentication profile to this initial guest role, see [“Configuring the Captive Portal Authentication Profile for Guest WLAN on page 102.”](#) Table 29 summarizes the policies used in the guest-branch-logon role.

Table 29 Policies Used in the guest-branch-logon Role

Policy Number	Policy Name	Purpose
1	clearpass-guest	Allows the client-based HTTP and HTTPS traffic to reach the hosted captive portal pages on the ClearPass Guest appliance. If this policy is not used in the guest-branch-logon role, the guest users cannot proceed to the login page on the ClearPass Guest. The preauthenticated guest logon policy usually is designed to deny all traffic other than DHCP and DNS traffic. For details, see Configuring the clearpass-guest Policy on page 88.
2	captiveportal (predefined policy)	Initiates captive portal authentication. This predefined policy redirects any HTTP or HTTPS traffic to port 8080, 8081, or 8088 of the controller. When the controller sees traffic on these ports, it checks the captive portal authentication profile that is associated with the current role of the user and processes the values specified on this profile.
3	guest-branch-logon-access	Allows DHCP and DNS services. For details, see Configuring the guest-branch-logon-access Policy on page 90.

CLI Configuration

```

!
user-role guest-branch-logon
  access-list session clearpass-guest
  access-list session captiveportal
  access-list session guest-logon-access
!

```

WebUI Screenshot

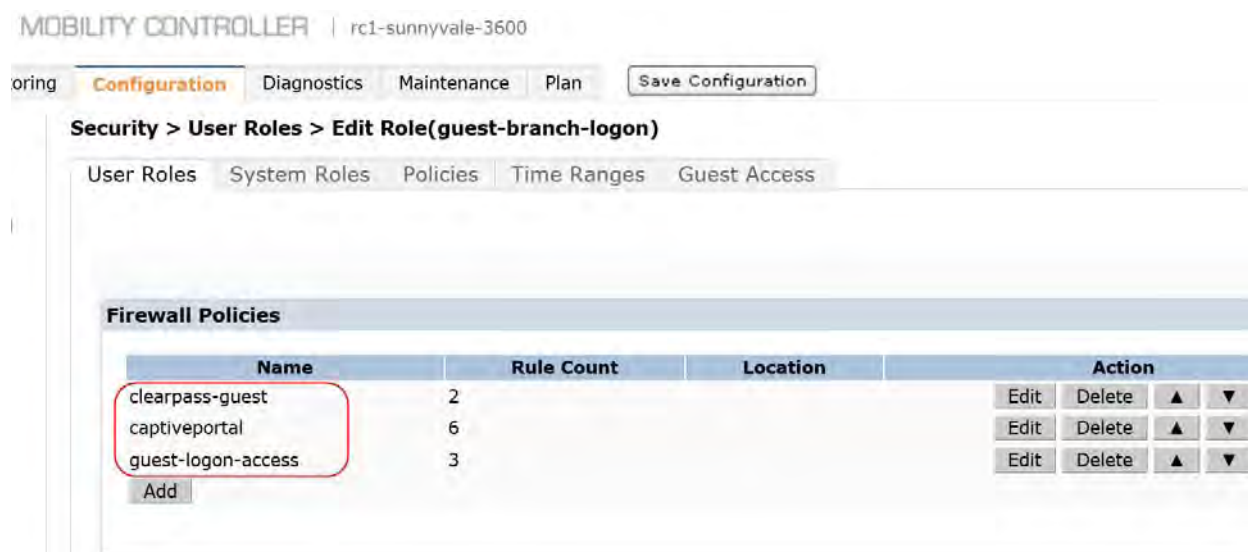


Figure 53 *guest-branch-logon role*

Configuring the Authenticated Guest Role

The auth-guest role is the role that is assigned to guest users after they authenticate successfully through the captive portal. This role is the default role in the captive portal authentication profile. In addition to restricting the network access to business hours, this role allows only HTTP and HTTPS services to access the Internet. The traffic from the users in this role is route source-NATed by the RAP and so it never reaches the controller. This role emulates the behavior of the bridge forwarding mode.

If an organization wants its guest users to use the printers in the internal network, a separate policy must be created that allows user traffic to an alias called printers. This alias must include only the IP address of the printers that the guests are allowed to use. Place this policy in the auth-guest user role just above the block-internal-access policy.

Table 30 summarizes the policies used in the auth-guest role.

Table 30 Policies Used in the auth-guest Role

Policy Number	Policy Name	Purpose
1	cplogout (predefined policy)	Redirects web traffic to the port 8081 of the controller. This redirection makes the controller present the logout window. This predefined policy must be placed before the policy that allows web access.
2	guest-branch-logon-access	Denies personal DHCP servers and provides legitimate DHCP services and DNS.
3	block-internal-access	Blocks access to internal network. This policy should be placed before the next policy that allows HTTP and HTTPS service, otherwise guest users will have access to the internal websites.

Table 30 Policies Used in the auth-guest Role (Continued)

Policy Number	Policy Name	Purpose
4	auth-guest-access	Allows HTTP and HTTPS services to any destination.
5	drop-and-log	Denies all services and logs the network access attempt. Any traffic that does not match the previous policies encounters this policy.

CLI Configuration

```

!
user-role auth-guest
  access-list session clogout
  access-list session guest-logon-access
  access-list session block-internal-access
  access-list session auth-guest-access
  access-list session drop-and-log
!

```

WebUI Screenshot

MOBILITY CONTROLLER | rc1-sunnyvale-3600

oring **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Logout admin](#)

Security > User Roles > Edit Role(auth-guest)

User Roles System Roles Policies Time Ranges Guest Access

« Back

Firewall Policies

Name	Rule Count	Location	Action
clogout	1		Edit Delete ▲ ▼
guest-logon-access	3		Edit Delete ▲ ▼
block-internal-access	1		Edit Delete ▲ ▼
auth-guest-access	2		Edit Delete ▲ ▼
drop-and-log	1		Edit Delete ▲ ▼

Add

Figure 54 auth-guest role

Maximum User Sessions for Guest Role

Though it is a very small possibility, a malicious user can connect to the guest network and initiate a denial of service (DoS) attack by using up all of the 65535 sessions available. To defend against such an attack, restrict the maximum number of sessions per user in a role. Aruba recommends that you restrict the maximum sessions per user in the guest role to 128. This limitation should be placed on all the roles used in the guest network.

The example network restricts the maximum sessions per user in the guest role to 128. This value is applied to the guest-branch-logon and auth-guest roles.

CLI

```
!  
user-role guest-branch-logon  
    max-sessions 128  
!  
user-role auth-guest  
    max-sessions 128  
!
```

WebUI Screenshot

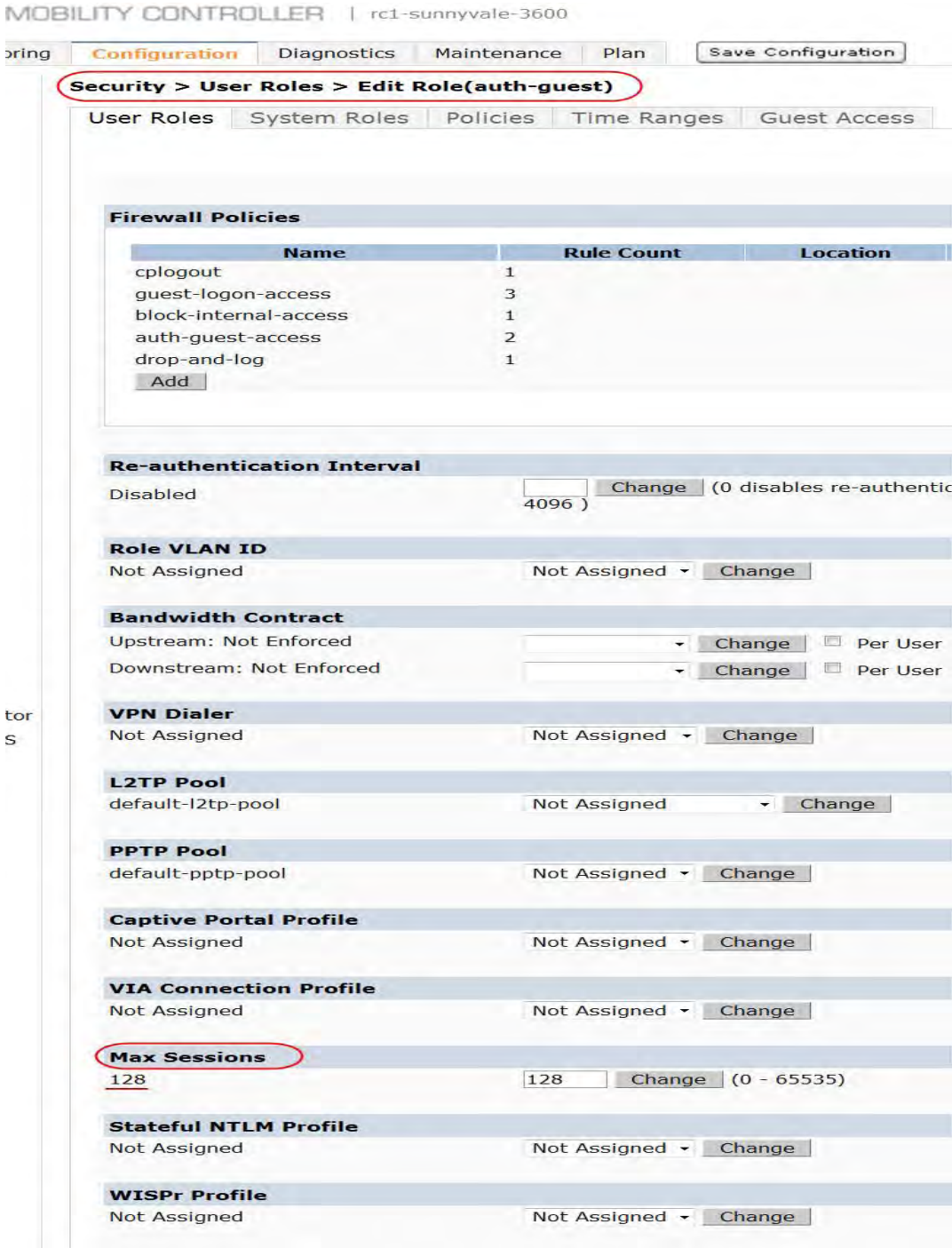


Figure 55 Maximum guest user sessions

Configuring the Guest SSID Profile for Micro Branch Office Deployments

The guest SSID does not provide any Layer 2 authentication and encryption. The Layer 2 authentication type used is open. In open authentication, hello messages are exchanged with the client before it is allowed to associate and obtain necessary IP information. All the user traffic is unencrypted. This WLAN uses captive portal to authenticate the users. The users that associate to this SSID are placed in the guest VLAN. Captive portal (with open Layer 2 authentication) should never be used for employee authentication, because captive portal does not provide encryption. The wireless traffic is visible to anyone doing a passive packet capture unless the data is encrypted by higher-layer protocols such as HTTPS and IPsec.

Table 31 summarizes the guest-branch SSID profile.

Table 31 guest-branch SSID Profile

SSID Profile	Network Name (SSID)	Authentication	Encryption	WMM	Purpose
guest-branch	guest	open	none	--	guest users (Captive portal is a Layer 3 authentication type.)

CLI Configuration

```
!
wlan ssid-profile "guest-branch"
  essid "guest"
  opmode opensystem
!
```

WebUI Screenshot

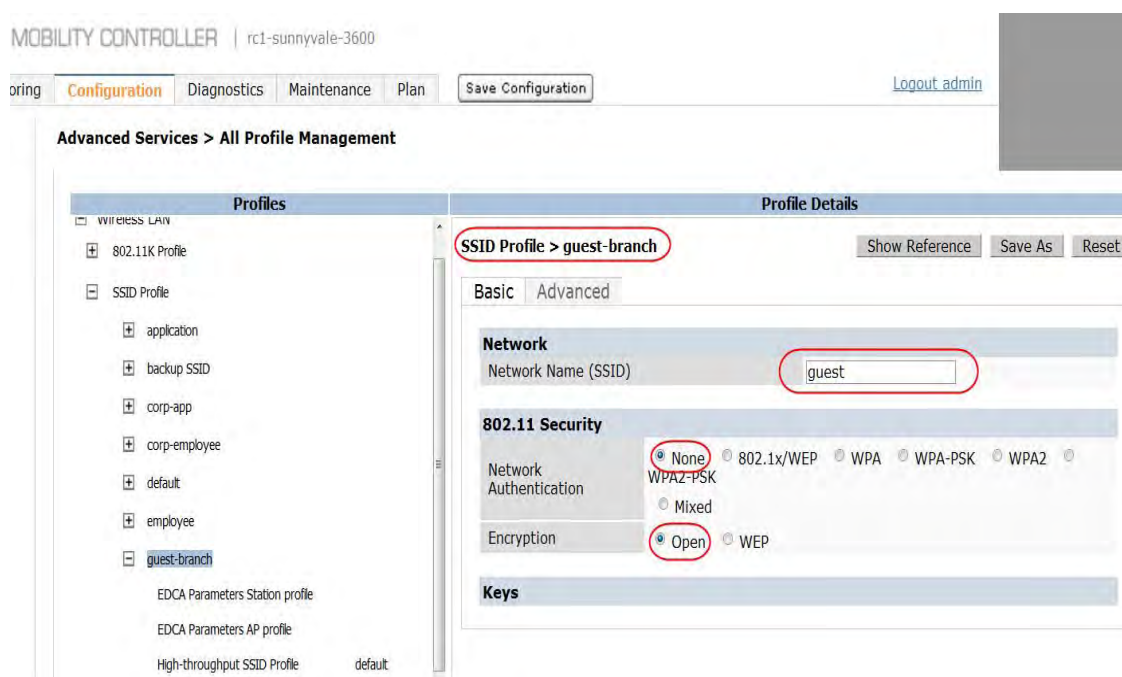


Figure 56 guest-branch SSID profile

Configuring the Server Group for Guest Authentication

The core of ClearPass Guest is a RADIUS server that uses the default ports of 1812 for authentication and 1813 for accounting. In the example network, a RADIUS server called clearpass-guest is defined and added to a newly created server group called clearpass-guest. The clearpass-guest server group is used as the server group for captive portal authentication.

CLI Configuration

```
!
aaa authentication-server radius " clearpass-guest "
    host "10.169.130.50"
    key *****
!
aaa server-group " clearpass-guest "
    auth-server clearpass-guest
!
```

WebUI Screenshot

The screenshot shows the Aruba Mobility Controller web interface. The breadcrumb navigation is **Security > Authentication > Servers**. The left sidebar shows a tree view with **Server Group** expanded, containing **amigopod** and **clearpass-guest** (highlighted with a red circle). Below it are **NPS1**, **LDAP Server**, **Internal DB**, and **Tacacs Accounting Server**. The main panel is titled **RADIUS Server > clearpass-guest** and contains a configuration table. The **Host** field is set to **10.169.130.50** and the **Key** field is masked with dots and labeled **Retype:** (both highlighted with red circles). Other fields include **Auth Port** (1812), **Acct Port** (1813), **Retransmits** (3), **Timeout** (5 sec), **NAS ID**, **NAS IP**, **Source Interface**, **Use MDS** (checkbox), **Use IP address for calling station ID** (checkbox), and **Mode** (dropdown menu, highlighted with a red circle). Buttons for **Show Reference**, **Save As**, and **Reset** are at the top right of the configuration area.

Host	10.169.130.50	Key	Retype: *****
Auth Port	1812	Acct Port	1813
Retransmits	3	Timeout	5 sec
NAS ID		NAS IP	
Source Interface		Use MDS	☐
Use IP address for calling station ID	☐	Mode	g

Figure 57 clearpass-guest RADIUS server



Figure 58 *clearpass-guest server group*

Configuring the Captive Portal Authentication Profile for Guest WLAN

As discussed earlier, to authenticate the users that are associated with the guest SSID via captive portal, you must define and attach a captive portal profile to the initial role assigned to the guest users. Configurable parameters such as the default role, login page, welcome page, and others are available in a captive portal profile.

The following parameters are configured in the guest-branch captive portal authentication profile used in the example network:

- User Login is enabled: A username and password is necessary to pass captive portal authentication when user login is enabled. Users authenticating through user login are assigned the role specified in the default role field of the captive portal profile.
- The default role is **auth-guest**: This role is assigned to users after authentication.
- Guest login is disabled: The captive portal does not request any credentials and the users can login by providing a valid email address. Users authenticating through guest login are assigned the role specified in the default guest role field of the captive portal profile. When both user login and guest login is enabled, users can login using either credentials or valid email address.
- Configure the login page: The value specified here is the URL to the login page hosted on the ClearPass Guest server. In the example network, this value is set to https://10.169.130.50/Aruba_login.php. When users in the initial guest role try to access Internet through HTTP or HTTPS protocol, they are redirected to the login page specified in this field.
- Configure the welcome pages (optional): The value specified here can be the URL to the welcome page hosted on the ClearPass Guest server, the default value, or any other external page like www.arubanetworks.com. In the example network, this value is set to www.arubanetworks.com/vrd. The welcome page specified in this field is displayed after successful authentication.
- All other parameters use the default values. For details on the other parameters of the captive portal profile, see the [Guest Access with ArubaOS Application Note](#).

For details about configuration of ClearPass Guest and its integration with Aruba controllers, see the *ClearPass Guest deployment guide* available at [Aruba support site](#).

CLI Configuration

```
!
aaa authentication captive-portal "guest-branch"
  default-role "auth-guest"
  user-login
  server-group "clearpass-guest"
  login-page "https://10.169.130.50/Aruba_login.php"
  welcome-page "http://www.arubanetworks.com/vrd"
!
```

WebUI Screenshot

The screenshot shows the Aruba WebUI configuration page for the 'Captive Portal Authentication Profile > guest-branch'. The left sidebar lists various authentication profiles, with 'Captive Portal Authentication Profile' expanded to show 'default' and 'guest-branch'. The 'guest-branch' profile is selected, and its configuration is displayed in the main area. The configuration includes fields for Default Role, Redirect Pause, Guest Login, Use HTTP for authentication, Logon wait maximum wait, Max Authentication failures, Use CHAP (non-standard), Welcome page, Add switch IP address in the redirection URL, White List, Black List, and Show the acceptable use policy page. The 'User Login' checkbox is checked, and the 'Login page' is set to 'https://10.169.130.50'.

Captive Portal Authentication Profile > guest-branch			
Default Role	auth-guest	Default Guest Role	guest
Redirect Pause	10 sec	User Login	☒
Guest Login	☐	Logout popup window	☒
Use HTTP for authentication	☐	Logon wait minimum wait	5 sec
Logon wait maximum wait	10 sec	logon wait CPU utilization threshold	60 %
Max Authentication failures	0	Show FQDN	☐
Use CHAP (non-standard)	☐	Login page	https://10.169.130.50
Welcome page	www.arubanetworks.com/vrd	Show Welcome Page	☒
Add switch IP address in the redirection URL	☐	Allow only one active user session	☐
White List		Black List	
Show the acceptable use policy page	☐		

Figure 59 guest-branch captive portal profile

After you have configured the captive portal profile, append it to the initial role, which is the guest-branch-logon role in the example network.

CLI Configuration

```
!
user-role guest-branch-logon
  captive-portal guest-branch
!
```

WebUI Screenshot

Security > User Roles > Edit Role(guest-branch-logon)

User Roles System Roles Policies Time Ranges Guest Access « Back

Firewall Policies

Name	Rule Count	Location	Action
clearpass-guest	2		Edit Delete ▲ ▼
captiveportal	6		Edit Delete ▲ ▼
guest-logon-access	3		Edit Delete ▲ ▼
block-internal-access	1		Edit Delete ▲ ▼

Add

Re-authentication Interval

Disabled Change (0 disables re-authentication. A positive value enables authentication 0 - 4096)

Role VLAN ID

Not Assigned Not Assigned ▼ Change

Bandwidth Contract

Upstream: Not Enforced Change ☐ Per User

Downstream: Not Enforced Change ☐ Per User

VPN Dialer

Not Assigned Not Assigned ▼ Change

L2TP Pool

default-l2tp-pool Not Assigned ▼ Change

PPTP Pool

default-pptp-pool Not Assigned ▼ Change

Captive Portal Profile

guest-branch guest-branch ▼ Change

Figure 60 Appending captive portal profile to initial guest role

Configuring the Guest AAA Profile for Micro Branch Office Deployments

Any user that accesses the network through the guest SSID is assigned the initial role that is specified in the guest AAA profile. The example network uses the guest-branch-logon role as the initial role. This initial role is designed to allow DHCP and DNS, so the user gets an IP address. When the user opens up a browser, the user does a DNS lookup for his homepage. The guest-branch-logon role permits DNS, so the homepage URL is resolved. When the user requests that page via HTTP/HTTPS, the captive portal ACL in the guest-branch-logon role redirects that traffic to the controller on port 8080, 8081, or 8088. When the controller sees the traffic on one of these ports, it checks the current role of the user, which is the guest-branch-logon role. The controller implements the parameters that are specified in the captive portal authentication profile that is tied to this role. After the user authenticates, the user is placed in an auth-guest role, which is the default role specified in the captive portal authentication profile.

A AAA profile named guest-branch is used for the guest WLAN. In the guest-branch AAA profile, configure the **guest-branch-logon role** as the initial role.

CLI Configuration

```
!  
aaa profile "guest-branch"  
    initial-role "guest-branch-logon"  
!
```

WebUI Screenshot

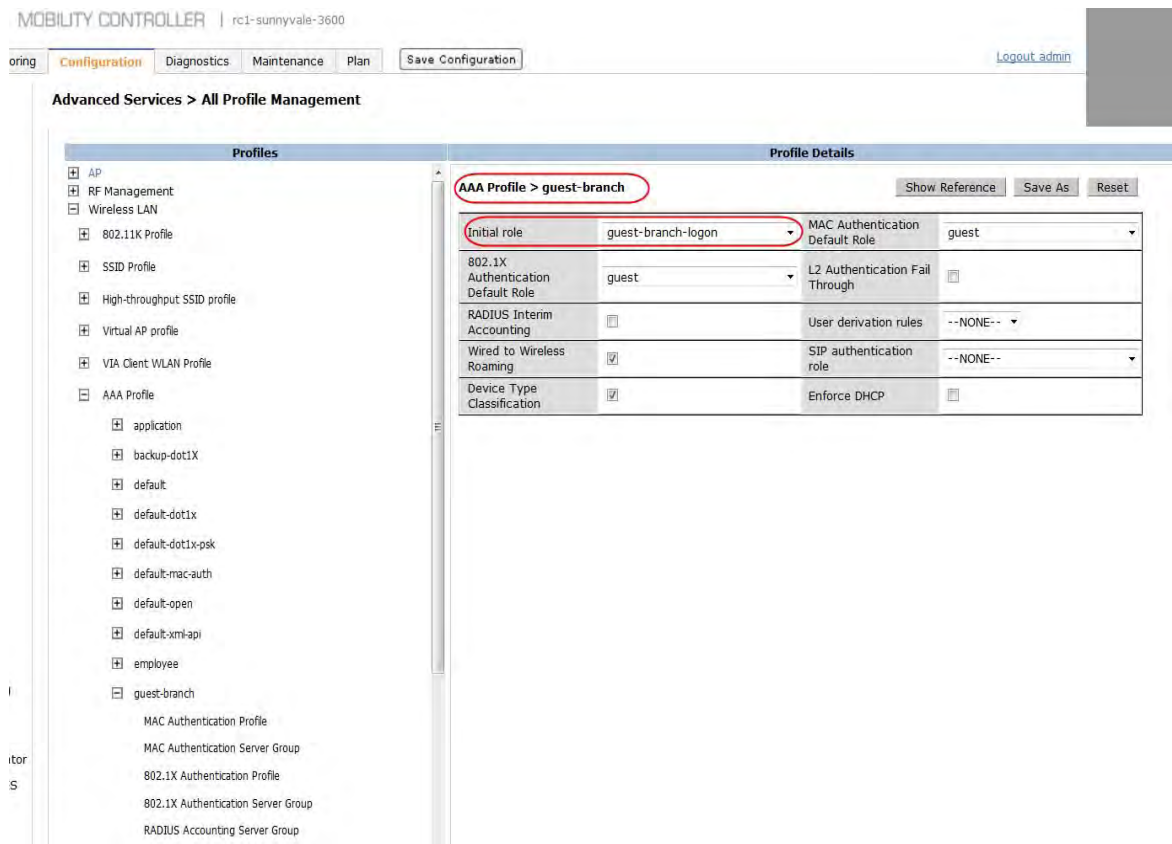


Figure 61 guest-branch AAA profile

Configuring the Guest VAP Profile for Micro Branch Office Deployments

The VAP used for guest WLAN in branch office is deployed in split-tunnel forwarding mode to provide captive portal authentication. A guest VAP profile named guest-branch is used in the example network. Figure 62 summarizes the guest VAP profile used in the example network.

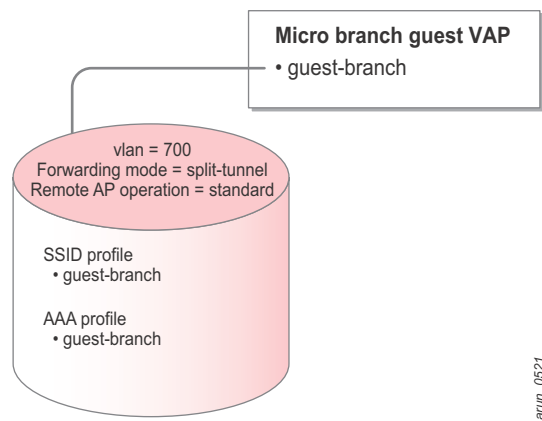


Figure 62 Micro branch office guest VAP

Table 32 lists the parameters that are configured for the guest-branch VAP profile.

Table 32 guest-branch VAP Profile

VAP Profile	VLAN	Forwarding Mode	Remote-AP Operation	AAA Profile	SSID Profile
guest-branch	700 (scr-NATed)	split-tunnel	standard	guest-branch	guest-branch



In the example network, the VLAN used for the guest network that provides captive portal authentication is source-NATed and the controller is the default gateway for this VLAN.

CLI Configuration

```
!
wlan virtual-ap "guest-branch"
  aaa-profile "guest-branch"
  ssid-profile "guest-branch"
  vlan 700
  forward-mode split-tunnel
  rap-operation standard
!
```

WebUI Screenshot

The screenshot shows the Aruba Mobility Controller web interface. The top navigation bar includes 'Configuration', 'Diagnostics', 'Maintenance', and 'Plan'. The 'Configuration' tab is active, and the 'Advanced Services > All Profile Management' section is selected. On the left, the 'Profiles' tree shows 'Virtual AP profile' expanded, with 'guest-branch' selected. The 'Profile Details' pane on the right shows the configuration for 'Virtual AP profile > guest-branch'. Key settings are highlighted with red circles: 'Virtual AP enable' is checked, 'VLAN' is set to 700, 'Forward mode' is set to 'split-tunnel', 'Remote-AP Operation' is set to 'standard', and the 'AAA Profile' and 'SSID Profile' are both set to 'guest-branch' in the left pane.

Figure 63 guest-branch VAP profile

Chapter 15: Configuring the Radio Profiles

The 802.11a and 802.11g radio profiles form the core of RF management. The various profiles and options under RF management allow you to configure these things:

- radio tuning and calibration
- AP load balancing
- coverage hole detection
- received signal strength indicator (RSSI) metrics

Primarily, the 802.11a and 802.11g radio profiles determine the mode in which an AP radio operates. A radio can be made to operate in one of the following three predefined modes:

- ap-mode (for typical APs)
- am-mode (for AMs)
- spectrum-mode (for SMs)

The 802.11a and 802.11g profiles are independent of each other. So, a dual-radio AP can be configured to behave as an AM in one spectrum band and function as a regular AP in the other band. In addition to the basic radio settings, the 802.11a and 802.11g radio profiles within an AP group include these profiles:

- ARM profile (required only for client access APs)
- high-throughput radio profile
- spectrum profile (required only for dedicated SMs)
- AM scanning profile (required only for AMs)

Though the radio profiles provide numerous options, not all are used in fixed telecommuter or micro branch office deployments. In these deployments, which have a single RAP per site, options such as spectrum load balancing and mode-aware ARM are not usable.

Configuring the ARM Profile

The Aruba Adaptive Radio Management (ARM) feature is a set of tools that allow the WLAN infrastructure to make decisions about radio resources and client connections without manual intervention by network administrators or client-side software.

The ARM algorithms and services use the information that APs and AMs gather when they scan the RF environment. The infrastructure has a network-wide view of APs and clients, and this information is used to make adjustments to provide an optimal client experience.

The Aruba ARM feature provides the following functionalities:

- channel and power setting
- client-aware ARM
- voice-aware scanning
- video-aware scanning

- rogue-aware scanning
- load-aware scanning
- band steering
- spectrum load balancing
- mode-aware ARM
- adjusting receive sensitivity
- local probe request threshold
- station handoff assist
- multiband feature
- reducing rate adaptation
- dynamic multicast optimization (DMO)
- fair access

The entire ARM feature set is not available in one place. Most features are configurable in the ARM profile. Band steering and DMO, which are defined per VAP, are available under VAP profiles. Fair access is in the traffic management profile. Spectrum load balancing and receive sensitivity options are defined within the 802.11a and 802.11g profiles. For detailed information on ARM, its features, and its advantages over traditional methods, see the [Aruba 802.11n Networks Validated Reference Design](#).

In fixed telecommuter and micro branch office deployments, which have a single RAP per site, some ARM features such as spectrum load balancing, mode-aware ARM, local probe request threshold and station handoff assist are not very useful. Similarly, if single-radio RAPs are deployed, which is often the case, then features like band steering cannot be used. Depending on your RAP selection, some ARM features may not be useful. However, ARM is essential in RAP deployments because it helps to optimize the client experience by dynamically altering the operating channel of the RAPs to get around the sources of interference (Wi-Fi or non-Wi-Fi). The scanning data collected is also useful in wireless intrusion detection and prevention.



The scanning feature in the ARM profile should be enabled. Do not disable the scanning feature unless you want to disable ARM and manually configure AP channel and transmission power.



The multiband feature in the ARM profile should be enabled for single-radio RAP deployments that require rogue scanning in the 2.4 and 5 GHz bands. If disabled, single-radio APs scan only the primary operating band.

Table 33 summarizes the recommended ARM settings for single-RAP deployments.

Table 33 ARM Recommendation Matrix

Feature	Fixed Telecommuter and Micro Branch Office Deployments (one RAP per site)
ARM Assignment	single band (default, for dual-radio RAPs) multiband (for single-radio RAPs)
Client-Aware ARM	enabled
Voice-Aware Scanning	enabled
Video-Aware Scanning	enabled
Load-Aware Scanning	10 Mb/s (default)
Power-Save-Aware Scanning	disabled
Rogue-Aware Scanning	disabled, except for high-security environments
Band Steering	enabled, prefer 5 GHz (default) (N/A for single-radio RAPs)
Spectrum Load Balancing	disabled (N/A for single-RAP deployments)
Mode-Aware ARM	disabled
Adjusting Receive Sensitivity	disabled
Local Probe Request Threshold	disabled
Station Handoff Assist	disabled
Multiband	enabled (for single-radio APs to perform rogue scanning in both 2.4 and 5GHz bands) N/A for dual-radio APs
Intelligent Rate Adaptation	always on, not configurable
Dynamic Multicast Optimization	disabled
Fair Access	enabled

The ARM profile is required only for APs that participate in ARM and not for the dedicated AMs or SMs. The scan-mode parameter in the ARM profile determines the scanning capabilities on an AP. This value can be set to:

- all-reg-domain: Scans all the channels in a spectrum band.
- reg-domain: Scans only the legal channels in a band. The legal channels in a band are determined by the local regulatory body.

The ARM requirements of a fixed telecommuter deployment vary from that of a micro branch office deployment. In fixed telecommuter deployments, where all the SSIDs and wired ports are secured, rogue scanning and containment is usually disabled. So, the multiband feature, which scans for rogues in the 2.4 and 5 GHz bands for single radio APs, can be disabled in this deployment. In micro branch office deployments, which might require rogue discovery and containment, the multiband feature should be enabled if single-radio APs are used. Enabling the multiband feature on single-radio APs does not impact the WAN bandwidth consumption. An organization should properly understand and

define its security policy for each type of deployment before deciding the type of scanning mode and turning on or off the various ARM features. For the details on ARM bandwidth requirement for RAP deployments, see [Appendix B: RAP Control Traffic](#).

The example network, which has single radio dual band RAPs, uses two ARM profiles named home-arm (for fixed telecommuter deployment) and branch-arm (for micro branch office deployments). These profiles use the recommended ARM settings specified in the ARM matrix, but in home-arm profile, the multiband feature is disabled. The fixed telecommuter setup in the example network has rogue detection and containment disabled and so the ARM scanning is used only for choosing the most optimal operating channel in the primary band of operation. The scan-mode is set as reg-domain for home-arm profile and is set as all-reg-domain for branch-arm profile.



If dual radio APs are deployed as RAPs, the multiband feature can be ignored and the ARM assignment must be set to single-band.

CLI Configuration

```
!  
rf arm-profile "branch-arm"  
  assignment multi-band  
  max-tx-power 3  
  min-tx-power 127  
  voip-aware-scan  
  scan-mode all-reg-domain  
!  
rf arm-profile "home-arm"  
  assignment multi-band  
  max-tx-power 3  
  min-tx-power 127  
  no multi-band-scan  
  voip-aware-scan  
  scan-mode reg-domain  
!
```

WebUI Screenshot

MOBILITY CONTROLLER | rc1-sunnyvale-3600

Configuration Diagnostics Maintenance Plan Save Configuration Logout admin

Advanced Services > All Profile Management

Profiles	Profile Details			
- AP - RF Management 802.11a radio profile 802.11g radio profile - Adaptive Radio Management (ARM) profile branch-arm - default - home-arm - test - High-throughput radio profile - Spectrum profile - RF Optimization Profile - RF Event Thresholds Profile - AM Scanning profile - Wireless LAN - Mesh - QoS - IDS - Other Profiles	Adaptive Radio Management (ARM) profile > Show Reference Save As Reset			
	Assignment	multi-band	Allowed bands for 40MHz channels	a-only
	Client Aware	☒	Max Tx EIRP	3
	Min Tx EIRP	127	Multi Band Scan	☒
	Rogue AP Aware	☐	Scan Interval	10 sec
	Active Scan	☐	Scanning	☒
	Scan Time	110 msec	VoIP Aware Scan	☒
	Power Save Aware Scan	☐	Video Aware Scan	☒
	Ideal Coverage Index	10	Acceptable Coverage Index	4
	Free Channel Index	25	Backoff Time	240 sec
	Error Rate Threshold	50 %	Error Rate Wait Time	30 sec
	Noise Threshold	75 -dBm	Noise Wait Time	120 sec
	Minimum Scan Time	8	Load aware Scan Threshold	1250000 Bps
	Mode Aware Arm	☐	Scan Mode	all-reg-domain

Figure 64 branch-arm ARM profile

MOBILITY CONTROLLER | rc1-sunnyvale-3600

Configuration Diagnostics Maintenance Plan Save Configuration Logout admin

Advanced Services > All Profile Management

Profiles	Profile Details			
- AP - RF Management 802.11a radio profile 802.11g radio profile - Adaptive Radio Management (ARM) profile - branch-arm - default home-arm - test - High-throughput radio profile - Spectrum profile - RF Optimization Profile - RF Event Thresholds Profile - AM Scanning profile - Wireless LAN - Mesh - QoS - IDS - Other Profiles	Adaptive Radio Management (ARM) profile > Show Reference Save As Reset			
	Assignment	multi-band	Allowed bands for 40MHz channels	a-only
	Client Aware	☒	Max Tx EIRP	3
	Min Tx EIRP	127	Multi Band Scan	☐
	Rogue AP Aware	☐	Scan Interval	10 sec
	Active Scan	☐	Scanning	☒
	Scan Time	110 msec	VoIP Aware Scan	☒
	Power Save Aware Scan	☐	Video Aware Scan	☒
	Ideal Coverage Index	10	Acceptable Coverage Index	4
	Free Channel Index	25	Backoff Time	240 sec
	Error Rate Threshold	50 %	Error Rate Wait Time	30 sec
	Noise Threshold	75 -dBm	Noise Wait Time	120 sec
	Minimum Scan Time	8	Load aware Scan Threshold	1250000 Bps
	Mode Aware Arm	☐	Scan Mode	reg-domain

Figure 65 home-arm ARM profile

Configuring the 802.11a and 802.11g Radio Profiles

The 802.11a and 802.11g radio profiles dictate the operation of the 5 GHz and 2.4 GHz radios respectively. Figure 66 summarizes the radio profiles used for the remote-home and the remote-branch AP groups in the example network.

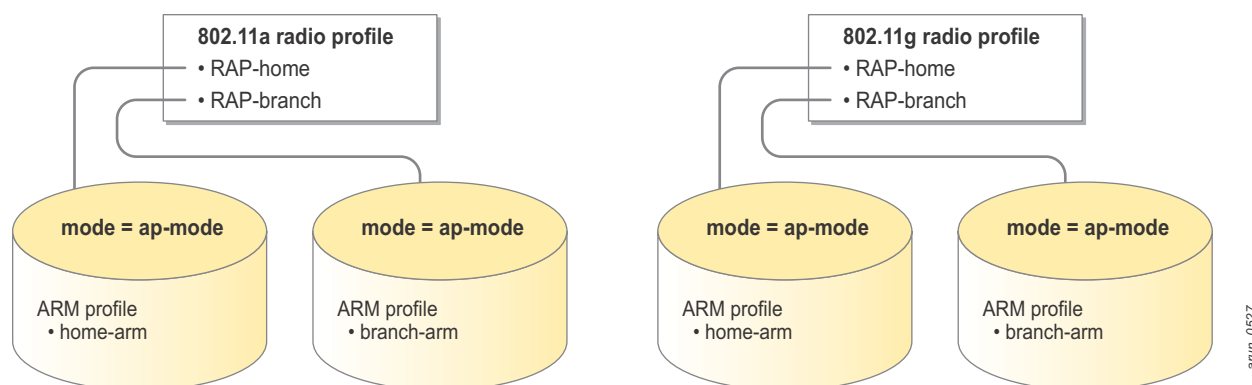


Figure 66 Radio profiles of client access AP groups

Table 34 summarizes the 802.11a and 802.11g radio profiles used in the example network by the AP groups built for fixed telecommuter and micro branch office deployments.

Table 34 Radio Profiles of Client Access AP Groups

Profile Type	Profile Name	Mode	ARM Profile	AM Scanning Profile	Purpose
802.11a radio profile	RAP-home	ap-mode	home-arm	—	Makes the 5 GHz radio function as a typical AP.
802.11g radio profile	RAP-home	ap-mode	home-arm	—	Makes the 2.4 GHz radio function as a typical AP.
802.11a radio profile	RAP-branch	ap-mode	branch-arm	—	Makes the 5 GHz radio function as a typical AP.
802.11g radio profile	RAP-branch	ap-mode	branch-arm	—	Makes the 2.4 GHz radio function as a typical AP.



Ensure that the ARM/WIDS override parameter is disabled. If this option is enabled, it will disable ARM and Wireless IDS. The behavior of dedicated AMs is not affected by this parameter.

CLI Configuration

```

!
rf dot11a-radio-profile "RAP-branch"
  mode ap-mode
  arm-profile "branch-arm"
!
rf dot11a-radio-profile "RAP-home"
  mode ap-mode
  arm-profile "home-arm"
!
!
rf dot11g-radio-profile "RAP-branch"
  mode ap-mode
  arm-profile "branch-arm"
!
rf dot11g-radio-profile "RAP-home"
  mode ap-mode
  arm-profile "home-arm"
!

```

WebUI Screenshot

MOBILITY CONTROLLER | rc1-sunnyvale-3600

oring **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Logout admin](#)

Advanced Services > All Profile Management

Profiles	Profile Details																																																				
- AP - RF Management 802.11a radio profile - airmonitor - AP - default - RAP RAP-branch - Adaptive Radio Management (ARM) Profile: branch-arm - High-throughput Radio Profile: default-a - Spectrum Monitoring Profile: default-a - AM Scanning Profile: default - RAP-home 802.11g radio profile - airmonitor - AP - default - RAP - RAP-branch - RAP-home - Adaptive Radio Management (ARM) profile - High-throughput radio profile - Spectrum profile	802.11a radio profile > RAP-branch Show Reference Save As Reset <table border="1"> <tr> <td>Radio enable</td> <td>☒</td> <td>Mode</td> <td>ap-mode</td> </tr> <tr> <td>High throughput enable (radio)</td> <td>☒</td> <td>Channel</td> <td>Secondary Channel: ☐ None ☐ Above ☐ Below</td> </tr> <tr> <td>Beacon Period</td> <td>100 msec</td> <td>Beacon Regulate</td> <td>☐</td> </tr> <tr> <td>Transmit EIRP</td> <td>15</td> <td>Advertise 802.11d and 802.11h Capabilities</td> <td>☐</td> </tr> <tr> <td>TPC Power</td> <td>15</td> <td>Spectrum load balancing</td> <td>☐</td> </tr> <tr> <td>Spectrum Load balancing mode</td> <td>channel</td> <td>Spectrum load balancing update interval (sec)</td> <td>30 seconds</td> </tr> <tr> <td>Spectrum load balancing threshold (%)</td> <td>20 percent</td> <td>Advertized regulatory max EIRP</td> <td>0</td> </tr> <tr> <td>Spectrum Load Balancing domain</td> <td></td> <td>RX Sensitivity Tuning Based Channel Reuse</td> <td>disable</td> </tr> <tr> <td>RX Sensitivity Threshold</td> <td>0 -dBm</td> <td>Non 802.11 Interference Immunity</td> <td>Level-2</td> </tr> <tr> <td>Enable CSA</td> <td>☐</td> <td>CSA Count</td> <td>4</td> </tr> <tr> <td>Management Frame Throttle interval</td> <td>1 sec</td> <td>Management Frame Throttle Limit</td> <td>20</td> </tr> <tr> <td>ARM/WIDS Override</td> <td>☐</td> <td>Maximum Distance</td> <td>0 meters</td> </tr> <tr> <td>Spectrum Monitoring</td> <td>☐</td> <td></td> <td></td> </tr> </table>	Radio enable	☒	Mode	ap-mode	High throughput enable (radio)	☒	Channel	Secondary Channel: ☐ None ☐ Above ☐ Below	Beacon Period	100 msec	Beacon Regulate	☐	Transmit EIRP	15	Advertise 802.11d and 802.11h Capabilities	☐	TPC Power	15	Spectrum load balancing	☐	Spectrum Load balancing mode	channel	Spectrum load balancing update interval (sec)	30 seconds	Spectrum load balancing threshold (%)	20 percent	Advertized regulatory max EIRP	0	Spectrum Load Balancing domain		RX Sensitivity Tuning Based Channel Reuse	disable	RX Sensitivity Threshold	0 -dBm	Non 802.11 Interference Immunity	Level-2	Enable CSA	☐	CSA Count	4	Management Frame Throttle interval	1 sec	Management Frame Throttle Limit	20	ARM/WIDS Override	☐	Maximum Distance	0 meters	Spectrum Monitoring	☐		
Radio enable	☒	Mode	ap-mode																																																		
High throughput enable (radio)	☒	Channel	Secondary Channel: ☐ None ☐ Above ☐ Below																																																		
Beacon Period	100 msec	Beacon Regulate	☐																																																		
Transmit EIRP	15	Advertise 802.11d and 802.11h Capabilities	☐																																																		
TPC Power	15	Spectrum load balancing	☐																																																		
Spectrum Load balancing mode	channel	Spectrum load balancing update interval (sec)	30 seconds																																																		
Spectrum load balancing threshold (%)	20 percent	Advertized regulatory max EIRP	0																																																		
Spectrum Load Balancing domain		RX Sensitivity Tuning Based Channel Reuse	disable																																																		
RX Sensitivity Threshold	0 -dBm	Non 802.11 Interference Immunity	Level-2																																																		
Enable CSA	☐	CSA Count	4																																																		
Management Frame Throttle interval	1 sec	Management Frame Throttle Limit	20																																																		
ARM/WIDS Override	☐	Maximum Distance	0 meters																																																		
Spectrum Monitoring	☐																																																				

Figure 67 RAP-branch 802.11a radio profile

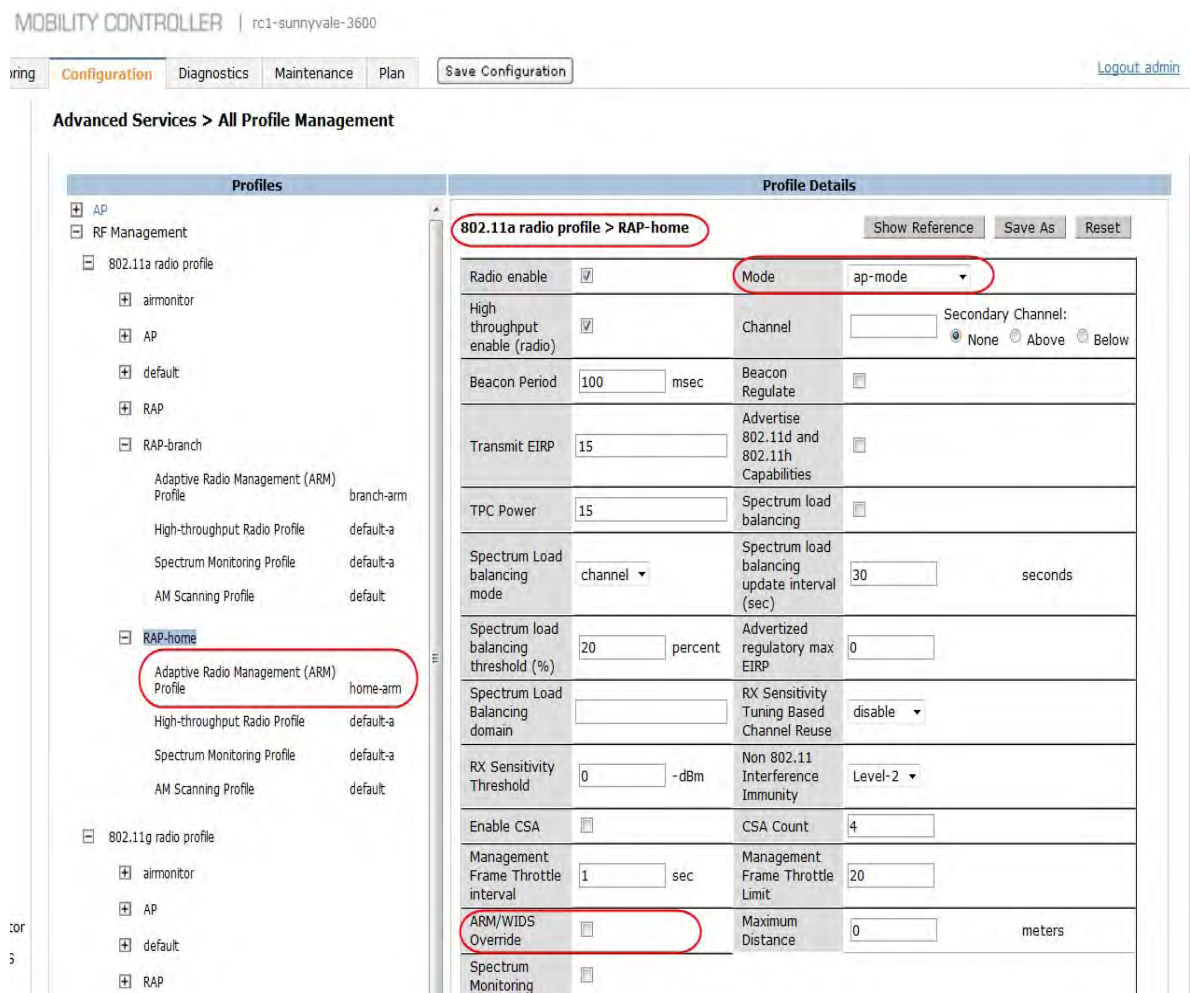


Figure 68 RAP-home 802.11a radio profile

Chapter 16: Configuring the AP System Profiles

The AP system profile defines these kinds of options:

- LMS and backup LMS IP
- real-time location services (RTLS) server values
- number of consecutive missed heartbeats on a GRE tunnel before an AP bootstraps
- remote-AP DHCP server
- primary band of operation for single-radio, dual-band APs

In Aruba terminology, the LMS is the controller that manages the AP and its traffic. In a typical deployment, when an AP boots up for the first time, it contacts the master controller. The master uses the `lms-ip` parameter to direct the AP to the mobility controller on which it should terminate its GRE tunnel. The `lms-ip` parameter is contained in the AP system profile of the AP group that is assigned to that AP. If the backup LMS IP address is defined, it is used by the AP when the original controller becomes unreachable. For remote network deployments, the LMS IP address should be the public IP address of the controller. In other words, the IP address defined as the LMS IP address in the AP system profile of the AP group used for RAPs should be reachable from the public Internet without the need for any tunneling.

The example network does not use a backup LMS IP address because the VRRP between the master controllers addresses the redundancy issue. For information about the advantages of VRRP and the use cases for the backup LMS IP address, see the [Aruba Mobility Controllers Validated Reference Design](#). For information on configuring geographical redundancy, see [Appendix C: Geographical Redundancy for RAP Deployments](#).

RF Band

A single-radio, dual-band AP is capable of operating in the 2.4 and 5 GHz bands, but at any given time it can operate in only one of these two bands. The RF band parameter defines the primary band in which a single-radio, dual-band AP should operate. This parameter can be set to these values:

- a – The 5 GHz band is the primary band for operation.
- g – The 2.4 GHz band is the primary band for operation.

Remember that a radio operating in the 2.4 GHz band has more coverage than a 5 GHz radio. However, the 5 GHz band has more channels and less interference, but all devices are not capable of

5 GHz. The network administrators should consider such RF factors before choosing the primary band of operation.



When the multiband feature is selected in the ARM assignment parameter of the ARM profile, the RF band setting is neglected. By default, ARM selects the 2.4 GHz band as the primary band for single-radio APs. In deployments with more than one AP, ARM automatically switches a single-radio AP to operate in the 5 GHz band if the other APs in the area provide the required coverage in 2.4 GHz band. If you want your single radio dual band APs to operate in a specific band, configure the ARM assignment to single-band and set the RF band parameter to the preferred band.

Native VLAN and Remote-AP DHCP Server

For VAPs and wired ports that operate in the bridge forwarding mode, the DHCP server cannot be deployed at the Headquarters behind the master controllers in the DMZ. The DHCP has to be local to the site. The native VLAN and remote-AP DHCP parameters in the AP system profile define the DHCP services that are required for the clients connected to a bridge mode VAP or wired port.

In deployments that have a local DHCP server, the native VLAN parameter is used. The frames on the native VLAN are not tagged with 802.1q tags, so the native VLAN ID in the AP system profile of an AP-group determines if bridged traffic is tagged or not. If the native VLAN ID value matches the VLAN value in the bridged VAP or wired AP profile, then the traffic is not tagged. If the native VLAN ID value does not match the VLAN value in the bridged VAP or wired AP profile, then the traffic is tagged with the VLAN ID that is specified in the bridged VAP or wired AP profile. [Table 35](#) shows some examples of when the bridge mode traffic is tagged.

Table 35 Bridge-mode VLANs

AP Uplink Port Type	VLAN of the AP Uplink	Native VLAN in AP System Profile	VLAN in the Bridge VAP Profile	VLAN from Which the Bridge Users Get IP Addresses
access	1	10	10	The native VLAN in the AP system profile matches the VLAN ID in the VAP profile, so the traffic is untagged. Hence, users get IP addresses from VLAN 1.
access	1	10	20	The native VLAN in the AP system profile does not match the VLAN ID in the VAP profile, so the traffic is tagged as VLAN 20. Users do not get an IP address and they cannot pass traffic because the uplink switch will drop all the 802.1Q tagged packets received on access ports.
trunk	1 (native VLAN)	10	100	The native VLAN in the AP system profile does not match the VLAN ID in the VAP profile, so the traffic is tagged as VLAN 100. Hence, the users get IP addresses from VLAN 100 and all the user traffic forwarded through the uplink trunk is tagged with VLAN 100.

Table 35 Bridge-mode VLANs (Continued)

AP Uplink Port Type	VLAN of the AP Uplink	Native VLAN in AP System Profile	VLAN in the Bridge VAP Profile	VLAN from Which the Bridge Users Get IP Addresses
trunk	1 (native VLAN)	10	20	The native VLAN in the AP system profile does not match the VLAN ID in the VAP profile, so the traffic is tagged as VLAN 20. Hence, the users get IP addresses from VLAN 20 and all the user traffic forwarded through the uplink trunk is tagged with VLAN 20.
trunk	30 (native VLAN)	20	20	The native VLAN in the AP system profile matches the VLAN ID in the VAP profile, so the traffic is untagged. Hence, users get IP addresses from VLAN 30 and all the user traffic forwarded through the uplink trunk is untagged.

In deployments where a local DHCP server is not available, a RAP can be the DHCP server for all the bridge mode users. The various remote DHCP parameters in the AP system profile define the DHCP server used for the bridge mode users. The remote DHCP parameters available in the AP system profile are these:

- remote-AP DHCP server VLAN
- remote-AP DHCP server ID
- remote-AP DHCP default router
- remote-AP DHCP DNS server
- remote-AP DHCP pool start
- remote-AP DHCP pool end
- remote-AP DHCP pool netmask
- remote-AP DHCP lease time

If the value of the remote-AP DHCP server VLAN parameter in the AP system profile of the AP group of a RAP matches the VLAN value in a bridge mode VAP or wired port profile, then that RAP acts as the DHCP server for all the clients connected to this bridge mode VAP or wired port.

RAP Uplink Bandwidth Reservation

In RAPs that operate in split-tunnel and bridge forwarding modes, the Uplink Bandwidth Reservation (UBR) feature allows you to reserve and prioritize uplink bandwidth traffic to provide higher QoS for specific applications, traffic, or ports. UBR is achieved by applying bandwidth reservation on session ACLs. UBR is not available for tunnel and decrypt-tunnel forwarding modes because the AP does not inspect the traffic from VAPs and wired ports that operate in these modes. For more information on UBR, see the [Aruba 802.11n Networks Validated Reference Design](#). Figure 69 shows the operation of PEF-NG and UBR modules of a RAP on split-tunnel and bridge mode traffic.

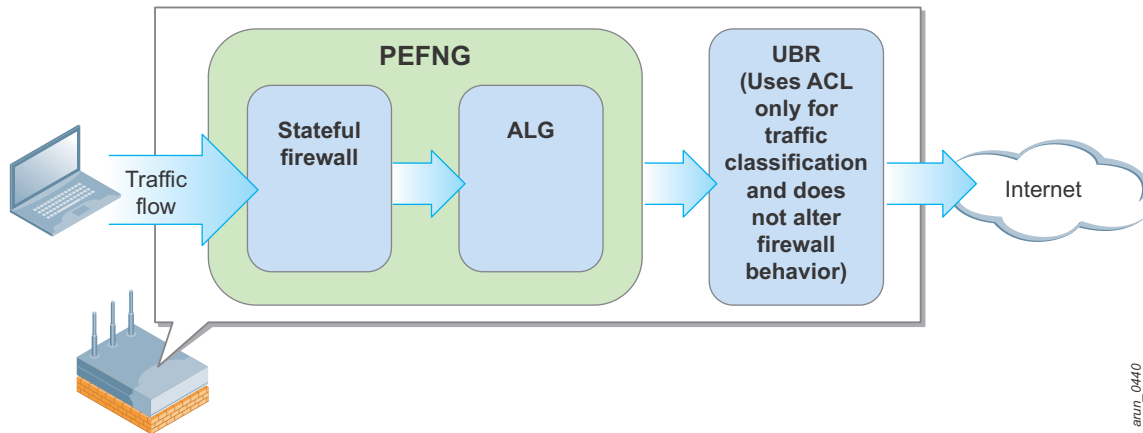


Figure 69 Traffic inspection on a RAP for split-tunnel and bridge forwarding modes

The UBR module applies traffic classification only to the egress traffic from the bridge and split-tunnel VAPs and wired ports. The PEF-NG module and the UBR module are independent of each other. For split-tunnel mode VAPs and wired ports, the ALG of the PEF-NG module dynamically opens and closes the ports (based on the configured policies) as per the needs of an application. The ports that are opened dynamically by the ALG are not communicated to the UBR. So UBR is unaware of the ports that are opened dynamically for an application. To prioritize the traffic on these dynamically opened ports, UBR requires a session ACL that prioritizes the entire range of UDP/TCP ports utilized by the application.

One of the many ALGs available in the Aruba infrastructure is the Session Initiation Protocol (SIP) ALG. Due to the presence of the SIP ALG, the **sip-session-allow policy** used in the remote-employee and **remote-application** user roles has only these rules:

```

user alias sip-server svc-sip-udp permit queue high
user alias sip-server svc-sip-tcp permit queue high
alias sip-server user svc-sip-udp permit queue high
alias sip-server user svc-sip-tcp permit queue high
  
```

These rules allow and prioritize the SIP traffic that is generated during the initial call setup. The RTP and RTCP ports that are assigned to the voice clients to pass traffic after the call has been established are dynamically learned and opened by the SIP ALG. When the call ends, the SIP ALG closes these dynamically opened ports. The ALGs simplify the firewall policies. The ALGs also improve the security at any given time by dynamically opening only the ports that are required rather than keeping all the allowed ports open at all times.

The example network has a voice deployment using an Asterisk server. The Asterisk server is configured to assign ports from the range 10000 to 20000 as Real-Time Transport Protocol (RTP) and Real-Time Transport Control Protocol (RTCP) ports for the voice calls. When user A calls user B, the Asterisk server assigns RTP and RTCP ports from this range to user A and B. In the example network, consider the following situation:

1. Remote voice user A is connected to the split-tunnel wired port of the RAP in location 1.
2. Remote employee user B is connected to the split-tunnel employee SSID of the RAP in location 2.
3. User A initiates a voice call to user B.
4. The sip-session-allow policy allows and prioritizes the SIP traffic between the users and the SIP server.
5. For this call, the Asterisk server assigns ports 10010 and 10011 as the destination RTP and RTCP ports for user A and ports 12010 and 12011 as the destination RTP and RTCP ports for user B.
6. The ALG on the RAP in location 1 (also known as ALG-Lite) dynamically opens sessions to allow voice data traffic to ports 10010 and 10011.
7. The ALG on the RAP in location 2 dynamically opens sessions to allow voice data traffic to ports 12010 and 12011.
8. The call is established between user A and B.
9. The ALG on the RAPs updates the controller with the call stats.
10. When the call is ended, these ports are closed by the ALG of the respective RAPs.

In this situation, the ports that are dynamically opened by the RAP are not communicated to the UBR. So if the sip-session-allow policy is used as the session ACL for UBR, the traffic classification is applied only to the SIP traffic. The actual RTP data is not prioritized because the UBR module on the RAP is unaware of the dynamically opened RTP and RTCP ports. So, the ALGs available in the ArubaOS cannot be used as UBR session ACLs. Therefore, the session ACL that is used for UBR should include the entire range of ports that is used by the application. In the example network, this range is UDP ports 10000 - 20000, which is used by the Asterisk server. The UBR uses the session ACL strictly for traffic classification and does not open all the specified ports. So, the UBR module does not open any security holes. Only the PEF-NG module can open or close the ports.



Aruba recommends that you check with your voice-solution vendor about the ports used by your VoIP solution.

Configuring the Uplink Bandwidth Reservation

UBR requires that the remote-AP uplink total bandwidth parameter be configured. The UBR feature is disabled if remote-AP uplink total bandwidth is set to 0. It is important to configure the correct uplink bandwidth for these reasons:

- If the actual uplink bandwidth is 2 Mb/s and the remote-AP uplink total bandwidth parameter is 5 Mb/s with 128 kb/s reserved for voice traffic, then the UBR traffic classification is useless. If the user pushes 5 Mb/s of torrent traffic and 100 kb/s of voice traffic, then the RAP allows all the voice traffic and 4.9 Mb/s of torrent traffic. However, the actual uplink is less, so the Internet

router randomly drops the traffic without considering whether it is voice or data. So the application that is prioritized might have poor performance.

- If the actual uplink bandwidth is 10 Mb/s and the remote-AP uplink total bandwidth parameter is 5 Mb/s, then the full uplink bandwidth is not available for the user. The reason is that the RAP shapes the traffic for 5 Mb/s. So even if the uplink is capable of 10 Mb/s, only a maximum of 5 Mb/s of traffic is pushed to the uplink at any time.

UBR can be configured to reserve a portion of the uplink bandwidth for up to three classes of traffic using session ACLs. A priority value of 1 - 3 can be set to each of the three traffic classes, with 1 representing the highest priority. The classified and unclassified traffics are segregated into multiple queues. The priority values determine how often these queues are dequeued. All unclassified traffic has the least priority.



Traffic from all the tunnel and decrypt tunnel mode VAPs and wired ports on a RAP is regarded as unclassified traffic.

Deploying the UBR feature is simple for micro branch office deployments because the network administrators have the knowledge about the uplink bandwidth at the various branch offices. For fixed telecommuter deployments, the uplink bandwidth available varies amongst users. So, for fixed telecommuter deployments the network administrators may configure different AP groups for the most common residential uplink bandwidths. The user RAPs can then be assigned the appropriate AP group based on the information provided by the employees about their Internet bandwidth at home.



For the UBR feature to function as expected, the RAPs at the remote sites must be deployed as recommended in [Onsite RAP Deployment on page 181](#).

In the example network, UBR is used to reserve a portion of the uplink bandwidth for voice traffic. The example network uses a session ACL named bw-uplink-reserve for UBR. The bw-uplink-reserve ACL is assigned an UBR priority of 1. [Table 36](#) summarizes all the rules used in the bw-uplink-reserve policy.

Table 36 Rules Used in the bw-uplink-reserve Policy

Rule Number	Source	Destination	Service	Action
1	user	alias sip-server	service svc-sip-udp	permit
2	user	alias sip-server	service svc-sip-tcp	permit
3	alias sip-server	user	service svc-sip-udp	permit
4	alias sip-server	user	service svc-sip-tcp	permit
5	user	internal-network	permit	udp 10000-20000

CLI

```
!
ip access-list session bw-uplink-reserve
  user alias sip-server svc-sip-udp permit
  user alias sip-server svc-sip-tcp permit
  alias sip-server user svc-sip-udp permit
  alias sip-server user svc-sip-tcp permit
  user alias internal-network udp 10000 20000 permit
!
```

WebUI Screenshot

The screenshot shows the Aruba WebUI Configuration page. The breadcrumb path is **Security > Firewall Policies > Edit Session (bw-uplink-reserve)**. The left sidebar shows the navigation menu with **Access Control** highlighted under the **SECURITY** section. The main content area displays the **Rules** table for the selected session.

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time
IPv4	user	sip-server	svc-sip-udp	permit				
IPv4	user	sip-server	svc-sip-tcp	permit				
IPv4	sip-server	user	svc-sip-udp	permit				
IPv4	sip-server	user	svc-sip-tcp	permit				
IPv4	user	internal-network	udp 10000-20000	permit				

Below the table is an **Add** button. At the bottom of the configuration area is a **Commands** section.

Remote-AP Local Network Access

The remote-AP local network access feature allows local network access between clients connected to a RAP without routing the traffic back to the controller. When two clients that are connected to a split-tunnel SSID or wired port are on the same VLAN, the traffic between them always is switched locally. However, if these two clients are on different VLANs, the traffic is routed via the controller. When remote-AP local network access is enabled, the RAP switches the traffic locally instead of routing the traffic back and forth through the controller. Similarly, for bridge mode clients on different VLANs, the remote-AP local network access feature switches the traffic locally instead of forwarding it to the upstream router when the “user any any route src-nat” firewall rule is triggered.

In the example network, the remote-AP local network access feature is enabled. Enabling the remote AP local network access parameters eliminates the need for the “alias *guest network alias guest network* any permit” rule in the guest-home policy.

Corporate DNS Domain

In many enterprises, DNS resolution of certain hosts depends on the location of the client. For example, when a computer is connected to the internal corporate network, the IP address of the mail server is resolved to an internal (private) IP address. If the computer is connected to the Internet, the same hostname (FQDN) is resolved to a public IP address. A RAP normally receives the IP address of the local DNS server from the ISP router or the local DHCP server when the AP boots up. However, in most cases, the internal corporate network has DNS servers. Therefore, the corporate DNS server is given to clients that are associated to split-tunnel SSIDs because these clients obtain IP addresses from a DHCP server on the corporate network. A RAP can intercept DNS queries from SSIDs and wired ports in split-tunnel mode and redirect these queries based on the domain. The corporate DNS domain feature available in the AP system-profile provides this functionality. When the corporate DNS domain field contains no entries, all the DNS queries of a split-tunnel user are forwarded to the controller. However, when a domain is specified in this field, all the DNS queries except for that domain are redirected to the local DNS of the RAP (obtained from the ISP). In the example network, the corporate DNS domain feature is configured to tunnel all DNS queries to the corporate DNS server if the domain name ends with “arubanetworks.com”. All other DNS queries are forwarded to the local DNS server.



For split-tunnel captive portal deployments, the DNS query for the FQDN of the redirected captive portal page should go through the controller if this FQDN is not public. When corporate domain DNS feature is used, ensure that the DNS queries for the captive portal page go through the controller.

Configuring the AP System Profile

The AP system profile that is used in the example network is:

- rc-sunnyvale-3600

Only the parameters such as the lms-ip, RF band, native VLAN, remote-AP DHCP server, remote-AP local network access, and RAP uplink bandwidth reservation are configured in this AP system profile. All other parameters are unaltered from their defaults.

Table 37 summarizes the parameters that are configured in the AP system profile used by the example network.

Table 37 Parameters for AP System Profile rc-sunnyvale-3600

Parameters for AP System Profile rc-sunnyvale-3600	Settings	
LMS IP	192.168.168.2 (In the example network, a simulated Internet is used. So the public IP of the controller is set to 192.168.168.2. In real deployments, the LMS and backup LMS IPs addresses will belong to the public IP space.)	
backup LMS IP	--	
RF band	g	
native VLAN ID	1	
remote-AP DHCP server VLAN	188	
remote-AP DHCP server ID	192.168.188.1	
remote-AP DHCP default router	192.168.188.1	
remote-AP DHCP DNS server	8.8.8.8 (If this parameter is not defined, the DNS server assigned to the RAP by the ISP router becomes the DNS server for the clients.)	
remote-AP DHCP pool start	192.168.188.50	
remote-AP DHCP pool end	192.168.188.254	
remote-AP DHCP pool netmask	255.255.255.0	
remote-AP DHCP lease time	0	
remote-AP uplink total bandwidth	10000 Kb/s	
remote-AP bw reservation 1	aclname	bw-uplink-reserve-voice
	bwvalue	1000 (this value represents Kb/s)
	prio	1
remote-AP bw reservation 2	--	
remote-AP bw reservation 3	--	
corporate DNS domain	arubanetworks.com	
remote-AP local network access	enabled	

CLI Configuration

```
!  
ap system-profile "rc-sunnyvale-3600"  
  lms-ip 192.168.168.2  
  rf-band a  
  rap-dhcp-server-vlan 188  
  rap-dhcp-server-id 192.168.188.1  
  rap-dhcp-default-router 192.168.188.1  
  rap-dhcp-pool-start 192.168.188.50  
  rap-dhcp-pool-end 192.168.188.254  
  rap-bw-total 10000  
  rap-bw-resv-1 acl "bw-uplink-reserve" 1000 priority 1  
  dns-domain "arubanetworks.com"  
  rap-local-network-access  
!
```

WebUI Screenshot

UTILITY CONTROLLER | rc1-sunnyvale-3600

Configuration Diagnostics Maintenance Plan Save Configuration Logout admin

Advanced Services > All Profile Management

Profiles	Profile Details																																																																																
- AP - AP system profile - default - rc-sunnyvale-3600 - rc1-sunnyvale-3600 - Regulatory Domain profile - Wired AP profile - AP Ethernet Link profile - AP wired port profile - AP Authorization profile - EDCA Parameters profile (Station) - EDCA Parameters profile (AP) - Spectrum Local Override Profile - RF Management - Wireless LAN - Mesh - QoS - IDS - Other Profiles	AP system profile > rc-sunnyvale-3600 Show Reference Save <table border="1"> <tr> <td>LMS IP</td> <td>192.168.168.2</td> <td>LMS IPv6</td> <td></td> </tr> <tr> <td>Backup LMS IP</td> <td></td> <td>Backup LMS IPv6</td> <td></td> </tr> <tr> <td>LMS Preemption</td> <td>☐</td> <td>LMS Hold-down Period</td> <td>600</td> </tr> <tr> <td>Number of IPSEC retries</td> <td>360</td> <td>LED operating mode (11n APs only)</td> <td>normal</td> </tr> <tr> <td>RF Band</td> <td>a</td> <td>Double Encrypt</td> <td>☐</td> </tr> <tr> <td>Root AP</td> <td>☐</td> <td>Native VLAN ID</td> <td>1</td> </tr> <tr> <td>SAP MTU</td> <td></td> <td>bytes</td> <td>Bootstrap threshold</td> </tr> <tr> <td>Request Retry Interval</td> <td>10</td> <td>sec</td> <td>Maximum Request Retries</td> </tr> <tr> <td>Dump Server</td> <td></td> <td>Telnet</td> <td>☐</td> </tr> <tr> <td>SNMP sysContact</td> <td></td> <td>AeroScout RTLS Server</td> <td>addr port</td> </tr> <tr> <td>RF Band for AM mode scanning</td> <td>all</td> <td>RTLS Server configuration</td> <td>addr port frequency key Retype:</td> </tr> <tr> <td>Remote-AP DHCP Server VLAN</td> <td>188</td> <td>Remote-AP DHCP Server Id</td> <td>192.168.188.1</td> </tr> <tr> <td>Remote-AP DHCP Default Router</td> <td>192.168.188.1</td> <td>Remote-AP DHCP DNS Server</td> <td>Delete Add</td> </tr> <tr> <td>Remote-AP DHCP Pool Start</td> <td>192.168.188.50</td> <td>Remote-AP DHCP Pool End</td> <td>192.168.188.254</td> </tr> <tr> <td>Remote-AP DHCP Pool Netmask</td> <td>255.255.255.0</td> <td>Remote-AP DHCP Lease Time</td> <td>0</td> </tr> <tr> <td>Remote-AP uplink total bandwidth</td> <td>10000</td> <td>kbps</td> <td>Remote-AP bw reservation 1</td> </tr> <tr> <td>Remote-AP bw reservation 2</td> <td>aclname bwvalue prio</td> <td>Remote-AP bw reservation 3</td> <td>aclname bwvalue prio</td> </tr> <tr> <td>Heartbeat DSCP</td> <td>0</td> <td>Session ACL</td> <td>ap-uplink-acl</td> </tr> <tr> <td>Corporate DNS Domain</td> <td>rde.arubanetworks.com arubanetworks.com Delete Add</td> <td>Maintenance Mode</td> <td>☐</td> </tr> <tr> <td>Remote-AP Local Network Access</td> <td>☒</td> <td></td> <td></td> </tr> </table>	LMS IP	192.168.168.2	LMS IPv6		Backup LMS IP		Backup LMS IPv6		LMS Preemption	☐	LMS Hold-down Period	600	Number of IPSEC retries	360	LED operating mode (11n APs only)	normal	RF Band	a	Double Encrypt	☐	Root AP	☐	Native VLAN ID	1	SAP MTU		bytes	Bootstrap threshold	Request Retry Interval	10	sec	Maximum Request Retries	Dump Server		Telnet	☐	SNMP sysContact		AeroScout RTLS Server	addr port	RF Band for AM mode scanning	all	RTLS Server configuration	addr port frequency key Retype:	Remote-AP DHCP Server VLAN	188	Remote-AP DHCP Server Id	192.168.188.1	Remote-AP DHCP Default Router	192.168.188.1	Remote-AP DHCP DNS Server	Delete Add	Remote-AP DHCP Pool Start	192.168.188.50	Remote-AP DHCP Pool End	192.168.188.254	Remote-AP DHCP Pool Netmask	255.255.255.0	Remote-AP DHCP Lease Time	0	Remote-AP uplink total bandwidth	10000	kbps	Remote-AP bw reservation 1	Remote-AP bw reservation 2	aclname bwvalue prio	Remote-AP bw reservation 3	aclname bwvalue prio	Heartbeat DSCP	0	Session ACL	ap-uplink-acl	Corporate DNS Domain	rde.arubanetworks.com arubanetworks.com Delete Add	Maintenance Mode	☐	Remote-AP Local Network Access	☒		
LMS IP	192.168.168.2	LMS IPv6																																																																															
Backup LMS IP		Backup LMS IPv6																																																																															
LMS Preemption	☐	LMS Hold-down Period	600																																																																														
Number of IPSEC retries	360	LED operating mode (11n APs only)	normal																																																																														
RF Band	a	Double Encrypt	☐																																																																														
Root AP	☐	Native VLAN ID	1																																																																														
SAP MTU		bytes	Bootstrap threshold																																																																														
Request Retry Interval	10	sec	Maximum Request Retries																																																																														
Dump Server		Telnet	☐																																																																														
SNMP sysContact		AeroScout RTLS Server	addr port																																																																														
RF Band for AM mode scanning	all	RTLS Server configuration	addr port frequency key Retype:																																																																														
Remote-AP DHCP Server VLAN	188	Remote-AP DHCP Server Id	192.168.188.1																																																																														
Remote-AP DHCP Default Router	192.168.188.1	Remote-AP DHCP DNS Server	Delete Add																																																																														
Remote-AP DHCP Pool Start	192.168.188.50	Remote-AP DHCP Pool End	192.168.188.254																																																																														
Remote-AP DHCP Pool Netmask	255.255.255.0	Remote-AP DHCP Lease Time	0																																																																														
Remote-AP uplink total bandwidth	10000	kbps	Remote-AP bw reservation 1																																																																														
Remote-AP bw reservation 2	aclname bwvalue prio	Remote-AP bw reservation 3	aclname bwvalue prio																																																																														
Heartbeat DSCP	0	Session ACL	ap-uplink-acl																																																																														
Corporate DNS Domain	rde.arubanetworks.com arubanetworks.com Delete Add	Maintenance Mode	☐																																																																														
Remote-AP Local Network Access	☒																																																																																

Figure 70 rc-sunnyvale-3600 AP system profile

Chapter 17: Configuring the QoS

The WMM and DSCP parameters discussed in the SSID profile can always be used to provide QoS for latency-sensitive applications as long as the network devices between a controller and a RAP respect the DSCP tags. The RAP always prioritizes traffic in the air depending on the WMM settings, type of traffic, and ACLs. Additionally, network administrators must also limit the number of voice calls on a RAP to provide QoS for voice.

Theoretically, based on a pure bandwidth perspective, an 802.11n AP can support hundreds of simultaneous voice calls. But in practice, the limiting factor is contention for the wireless medium. The 802.11 technology uses a collision-avoidance algorithm that makes timely access to the wireless media a challenge for delay-sensitive devices. Even with prioritization enabled for voice traffic, as the number of simultaneous voice clients increases, the contention increases, which delays the access to the wireless medium. Due to this limitation, the number of simultaneous voice calls that a single AP must process must be limited. In micro branch office deployments (single RAP deployments), the number of simultaneous wireless voice calls must not be more than 12 in mixed 802.11 client environments. If the number of simultaneous wireless voice calls is over 15 calls, the quality of the voice communication might be poor. In a pure 802.11n environment where all the voice clients are 802.11n-capable, the number of simultaneous voice calls can be up to 20. Wired phones are not affected by this limitation. Aruba recommends that network administrators strongly consider this factor for their micro branch office deployments. If your branch office deployments have a high number of wireless voice phones, consider other Aruba solutions, such as Aruba Instant and remote nodes using the 600 series branch controllers.

Chapter 18: RAP Wired Ports

On any Aruba RAP that offers at least two Ethernet ports, the additional port can be configured for bridging or secure jack operation. This configuration provides maximum flexibility and allows for local wired access at remote sites. Just like a wireless SSID, the additional Ethernet ports on a RAP can be configured for all the authentication types and forwarding modes available. In a WLAN, a single SSID cannot be configured to provide 802.1X and MAC authentication simultaneously, but this limitation does not apply to a wired port. A wired port can be configured to provide 802.1X authentication and MAC authentication simultaneously, which allows better utilization of the available wired ports.



Do not configure 802.1X and MAC authentication on the same SSID. Doing so causes client connectivity issues.

On any RAP, Eth 0 is always the uplink port. The remaining ports can be configured to provide the required functionality. To configure a wired port on a RAP you should create and apply an AP wired port profile to the desired Ethernet port. The wired port profile is a container that holds other profiles, such as the wired AP profile, Ethernet interface link profile, and AAA profile. So, the configuration of a wired port on a RAP requires these profiles:

- **AP wired port profile:** Enables or disables a port and also defines other parameters such as remote-AP backup
- **Wired AP profile:** Defines the switchport mode and the forwarding mode of a port
- **Ethernet interface link profile:** Defines speed and duplex values of a port
- **AAA profile:** Defines the authentication types, authentication servers, and the default user role for authenticated user and unauthenticated users

The example network uses RAP-5WN, which has five Ethernet ports (Eth 0 – 4). For fixed telecommuter deployment of the example network, the Ethernet ports (Eth 1 -4) are configured for these functionalities:

1. Wired port 1 provides 802.1X authentication and MAC authentication simultaneously via split-tunnel forwarding mode.
 - Successful 802.1X authentication assigns employee role to clients.
 - Successful MAC authentication assigns application role to clients.
2. Wired port 2 provides 802.1X authentication and MAC authentication simultaneously via split-tunnel forwarding mode.
 - Successful 802.1X authentication assigns employee role to clients.
 - Successful MAC authentication assigns application role to clients.
3. Wired port 3 provides wired guest access (open authentication via bridge forwarding mode).
4. Wired port 4 provides wired guest access (open authentication via bridge forwarding mode).

For micro branch office deployment of the example network, the Ethernet ports (Eth 1 -4) are configured for these functionalities:

1. Wired port 1 provides 802.1X authentication and MAC authentication simultaneously via split-tunnel forwarding mode.
 - Successful 802.1X authentication assigns the employee role to clients.
 - Successful MAC authentication assigns the application role to clients.
2. Wired port 2 provides 802.1X authentication and MAC authentication simultaneously via split-tunnel forwarding mode.
 - Successful 802.1X authentication assigns the employee role to clients.
 - Successful MAC authentication assigns the application role to clients.
3. Wired port 3 provides 802.1X authentication and MAC authentication simultaneously via split-tunnel forwarding mode.
 - Successful 802.1X authentication assigns the employee role to clients.
 - Successful MAC authentication assigns the application role to clients.
4. Wired port 4 provides wired guest access (captive portal authentication via split-tunnel forwarding mode).

Configuring the Wired AP Profile

The wired AP profile assigned to a port defines the port type (access or trunk port), allowed VLANs, and the forwarding mode. [Table 38](#) summarizes the wired AP profiles used in the example network.

Table 38 **Wired AP Profiles**

Profile Name	Wired AP	Forward Mode	Switchport Mode	Access Mode VLAN
wired-corporate	enable	split-tunnel	access	135
wired-guest-home	enable	bridge	access	188
wired-guest-branch	enable	split-tunnel	access	700



A secure jack is wired port secured with an authentication type such as 802.1X. The wired port profile enables or disables a port, but the wired AP profile determines the behavior of the port. The wired AP enable feature in the wired AP profile should be turned on for AP to perform the secure jack operation.

CLI

```

!
ap wired-ap-profile "wired-corporate"
    wired-ap-enable
    forward-mode split-tunnel
    switchport access vlan 135
!
ap wired-ap-profile "wired-guest-branch"
    wired-ap-enable
    forward-mode split-tunnel
    switchport access vlan 700
!
ap wired-ap-profile "wired-guest-home"
    wired-ap-enable
    forward-mode bridge
    switchport access vlan 188
!

```

WebUI Screenshot

MOBILITY CONTROLLER | rcl-sunnyvale-3600

ring **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Logout admin](#)

Advanced Services > All Profile Management

Profiles	Profile Details
- AP - AP system profile - Regulatory Domain profile - Wired AP profile - default - NoAuthWiredAp - wired-application - wired-corporate - wired-employee - wired-guest - wired-guest-branch - wired-guest-home - wired-instant - AP Ethernet Link profile - AP wired port profile - AP Authorization profile	Wired AP profile > wired-corporate Show Reference Save As Reset Wired AP enable ☒ Forward mode split-tunnel Switchport mode access Access mode VLAN 135 <-- 135 Trunk mode native VLAN 1 <-- 1 Trunk mode allowed VLANs 1-4094 <-- --NONE-- Trusted ☐ Broadcast ☒

Figure 71 *wired-corporate wired AP profile*

MOBILITY CONTROLLER | rc1-sunnyvale-3600

g **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Logout admin](#)

Advanced Services > All Profile Management

Profiles	Profile Details																
- AP - AP system profile - Regulatory Domain profile - Wired AP profile - default - NoAuthWiredAp - wired-application - wired-corporate - wired-employee - wired-guest - wired-guest-branch - wired-guest-home	Wired AP profile > wired-guest-home Show Reference Save As Reset <table><tr><td>Wired AP enable</td><td>☒</td><td>Forward mode</td><td>bridge</td></tr><tr><td>Switchport mode</td><td>access</td><td>Access mode VLAN</td><td>188</td></tr><tr><td>Trunk mode native VLAN</td><td>1</td><td>Trunk mode allowed VLANs</td><td>1-4094</td></tr><tr><td>Trusted</td><td>☐</td><td>Broadcast</td><td>☒</td></tr></table>	Wired AP enable	☒	Forward mode	bridge	Switchport mode	access	Access mode VLAN	188	Trunk mode native VLAN	1	Trunk mode allowed VLANs	1-4094	Trusted	☐	Broadcast	☒
Wired AP enable	☒	Forward mode	bridge														
Switchport mode	access	Access mode VLAN	188														
Trunk mode native VLAN	1	Trunk mode allowed VLANs	1-4094														
Trusted	☐	Broadcast	☒														

Figure 72 *wired-guest-home wired AP profile*

MOBILITY CONTROLLER | rc1-sunnyvale-3600

oring **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Logout admin](#)

Advanced Services > All Profile Management

Profiles	Profile Details																
- AP - AP system profile - Regulatory Domain profile - Wired AP profile - default - NoAuthWiredAp - wired-application - wired-corporate - wired-employee - wired-guest - wired-guest-branch	Wired AP profile > wired-guest-branch Show Reference Save As Reset <table><tr><td>Wired AP enable</td><td>☒</td><td>Forward mode</td><td>split-tunnel</td></tr><tr><td>Switchport mode</td><td>access</td><td>Access mode VLAN</td><td>700</td></tr><tr><td>Trunk mode native VLAN</td><td>1</td><td>Trunk mode allowed VLANs</td><td>1-4094</td></tr><tr><td>Trusted</td><td>☐</td><td>Broadcast</td><td>☒</td></tr></table>	Wired AP enable	☒	Forward mode	split-tunnel	Switchport mode	access	Access mode VLAN	700	Trunk mode native VLAN	1	Trunk mode allowed VLANs	1-4094	Trusted	☐	Broadcast	☒
Wired AP enable	☒	Forward mode	split-tunnel														
Switchport mode	access	Access mode VLAN	700														
Trunk mode native VLAN	1	Trunk mode allowed VLANs	1-4094														
Trusted	☐	Broadcast	☒														

Figure 73 *wired-guest-branch wired AP profile*

AAA Profile for Wired Ports

A single wired port can provide 802.1X and MAC authentication simultaneously. In many deployments, wired voice phones are distributed to employees. Most wired phones are not capable of 802.1X authentication and the only method of authentication for these phones is MAC authentication. MAC authentication is not secure because the MAC address can be spoofed easily, but still it provides some level of security by preventing nonhackers from accessing the corporate network. The default user role assigned for devices that successfully pass MAC authentication should strictly restrict them only to the services they require. In the example network, the wired voice phones that pass MAC authentication are assigned a user role that restricts their access only to the voice server in the corporate headquarters.

Remote Application Role

In the example network, the application role is assigned to every wired phone that passes MAC authentication. The application role prioritizes voice traffic and restricts the wired phones only to the SIP servers in the network. The application role in the example network uses the following policies:

- sip-session-allow (For details, see [Configuring the sip-session-allow Policy on page 54.](#))
- dhcp-acl (predefined)
- tftp-session-allow
- dns-acl (predefined)
- icmp-acl (predefined)

Configuring the tftp-session-allow Policy

The tftp-session-allow policy allows only TFTP services between the user and TFTP servers. This policy is required if the wired phones use TFTP service for tasks such as configuration download. Some phones use HTTP/HTTPS instead of TFTP for such tasks. In these cases, this firewall policy should be modified as required.

[Table 39](#) summarizes the rules used for the tftp-session-allow policy.

Table 39 Rules Used for the tftp-session-allow Policy

Rule Number	Source	Destination	Service	Action	Purpose
1	user	alias tftp-server	service svc-tftp	permit	Allows TFTP sessions between the user and TFTP servers.

CLI Configuration

```
!  
ip access-list session tftp-session-allow  
  user alias tftp-server svc-tftp permit  
!
```

WebUI Screenshot



Figure 74 tftp-session-allow policy

Configuring the Remote Application Role

To create the desired remote application role, you must put the essential firewall policies in the proper order. The remote authentication role restricts the devices only to the services required for their operation.

Table 40 summarizes the order of the policies in the application role that is used by the example network.

Table 40 Order of the Policies in the remote-application Role

Policy Number	Policy Name	Purpose
1	sip-session-allow	Allows SIP service. For details, see Configuring the sip-session-allow Policy on page 54 .
2	dhcp-acl (predefined)	Allows DHCP service.
3	tftp-session-allow	Allows TFTP service. For details, see Configuring the tftp-session-allow Policy on page 132 .
4	dns-acl (predefined)	Allows DNS service.
5	icmp-acl (predefined)	Allows ICMP across the network.

CLI Configuration

```

!
user-role remote-application
  access-list session sip-session-allow
  access-list session dhcp-acl
  access-list session tftp-session-allow
  access-list session dns-acl
  access-list session icmp-acl
!

```

WebUI Screenshot

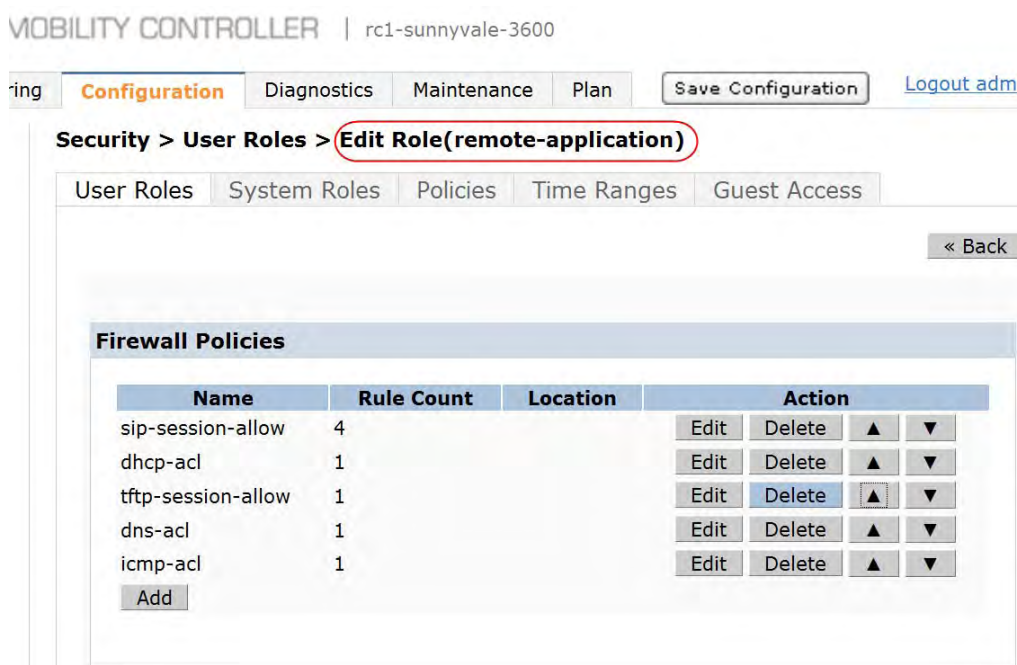


Figure 75 remote-application role

Corporate AAA Profile for Wired Ports

In the example network, a AAA profile named wired-corporate is assigned to wired ports on RAPs to provide corporate access. The wired-corporate AAA profile is design to assign different user roles based on the type of authentication. A user who successfully authenticates through 802.1X is assigned the remote employee role, but the device that passes MAC authentication is assigned the remote application role.

Configuring the Server Group for MAC Authentication

For MAC authentication, the example network uses the internal database of the controller. A server group called mac-auth is created. The mac-auth server group includes the internal database. The

MAC address of all the wired phones distributed to the remote users is added to the internal database of the master controller in the DMZ.



To add MAC addresses to the internal database of the controller, create a user account on the controller's internal database with both username and password set to the MAC address of the device. The format of MAC addresses added to the internal database depends on the delimiter configuration in the MAC authentication profile of the associated AAA profile.

CLI Configuration

```
!
aaa server-group "mac-auth"
    auth-server Internal
!
local-userdb add username 001a735497a6 password 001a735497a6
!
```

WebUI Screenshot

ILITY CONTROLLER | rc1-sunnyvale-3600

Configuration | Diagnostics | Maintenance | Plan | [Save Configuration](#) | [Logout admin](#)

Security > Authentication > Servers

Servers | AAA Profiles | L2 Authentication | L3 Authentication | User Rules | Advanced

Server Group

- default
- guest-amigopod
- Guest-internal
- internal
- mac-auth
- NPS
- + RADIUS Server
- + LDAP Server
- + Internal DB

Server Group > mac-auth | [Show Reference](#) | [Save As](#) | [Reset](#)

Fail Through ☐

Servers

Name	Server-Type	trim-FQDN	Match-Rule	Actions
Internal	Internal	No		Edit Delete ▲ ▼

[New](#)

Server Rules

Priority	Attribute	Operation	Operand	Type	Action	Value	Validated	Actions
New								

Figure 76 Server group for MAC authentication

The screenshot shows the Aruba Configuration web interface. The top navigation bar includes 'Dashboard', 'Monitoring', 'Configuration' (highlighted), 'Diagnostics', 'Maintenance', and 'Plan'. A 'Save Configuration' button is on the right. The left sidebar lists various configuration wizards and categories: WIZARDS (AP Wizard, Controller Wizard, WLAN/LAN Wizard, License Wizard, WIP Wizard), NETWORK (Controller, VLANs, Ports, Cellular Profile, IP), SECURITY (Authentication, Access Control), and WIRELESS (AP Configuration, AP Installation). The 'Authentication' category is expanded, showing 'Security > Authentication > Servers'. The 'Servers' tab is active, with sub-tabs for 'AAA Profiles', 'L2 Authentication', 'L3 Authentication', 'User Rules', and 'Advanced'. A list of server types is shown on the left: Server Group, RADIUS Server, LDAP Server, Internal DB (highlighted with a red circle), Tacacs Accounting Server, TACACS Server, XML API Server, RFC 3576 Server, and Windows Server. The 'Internal DB' configuration form is displayed on the right. It includes fields for 'User Name' and 'Password', both containing the MAC address '001a735497a6'. The 'Generate' buttons are visible next to these fields. Other fields include 'Role' (a dropdown), 'E-mail', 'Enabled' (checked), 'Expiration' (with options for 'Entry does not expire', 'Set Expiry time (mins)', and 'Set Expiry Date (mm/dd/yyyy)'), and 'Static Inner IP Address (for RAPs only)'.

Figure 77 Adding MAC address to internal database

Configuring the Corporate AAA Profile for Wired Ports

In the example network, a AAA profile called wired-corporate is created with the following parameters:

- **Initial role:** deny all (This role should deny all traffic.)
- **Default role for 802.1X authentication:** remote-employee role (see [Configuring the remote-employee Role on page 57](#))
- **802.1X authentication server group:** NPS
- **802.1X profile:**
 - Create the remote-employee-dot1x 802.1X profile.
 - Enable termination. (By default, the termination EAP-type is EAP-PEAP and the termination inner EAP type is EAP-MSCHAPv2.)
- **Default role for MAC Authentication:** remote-application role
- **MAC Authentication Server Group:** mac-auth
- **MAC Authentication Profile:** default (The defaults for delimiter and case fields, which determine the MAC address format, are none and lowercase respectively.)
- **L2 Authentication Fail Through:** enabled (When this option is enabled, if one authentication methods fails authentication is continued using the other authentication methods. 802.1X authentication is enforced before authenticating with MAC authentication.)

CLI

```

!
aaa profile "wired-corporate"
  initial-role "denyall"
  authentication-mac "default"
  mac-default-role "remote-application"
  mac-server-group "mac-auth"
  authentication-dot1x "remote-employee-dot1x"
  dot1x-default-role "remote-employee"
  dot1x-server-group "NPS"
  l2-auth-fail-through
!

```

WebUI Screenshot

MOBILITY CONTROLLER | rc1-sunnyvale-3600

ring **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Logout admin](#)

Advanced Services > All Profile Management

Profiles	Profile Details																				
- wired-application - wired-authenticated wired-corporate - MAC Authentication Profile default - MAC Authentication Server Group mac-auth 802.1X Authentication Profile remote-employee-dot1x 802.1X Authentication Server Group NPS - RADIUS Accounting Server Group - XML API server - RFC 3576 server	AAA Profile > wired-corporate Show Reference Save As Reset <table border="1"> <tbody> <tr> <td>Initial role</td> <td>denyall</td> <td>MAC Authentication Default Role</td> <td>remote-application</td> </tr> <tr> <td>802.1X Authentication Default Role</td> <td>remote-employee</td> <td>L2 Authentication Fail Through</td> <td>☒</td> </tr> <tr> <td>RADIUS Interim Accounting</td> <td>☐</td> <td>User derivation rules</td> <td>--NONE--</td> </tr> <tr> <td>Wired to Wireless Roaming</td> <td>☒</td> <td>SIP authentication role</td> <td>--NONE--</td> </tr> <tr> <td>Device Type Classification</td> <td>☒</td> <td>Enforce DHCP</td> <td>☐</td> </tr> </tbody> </table>	Initial role	denyall	MAC Authentication Default Role	remote-application	802.1X Authentication Default Role	remote-employee	L2 Authentication Fail Through	☒	RADIUS Interim Accounting	☐	User derivation rules	--NONE--	Wired to Wireless Roaming	☒	SIP authentication role	--NONE--	Device Type Classification	☒	Enforce DHCP	☐
Initial role	denyall	MAC Authentication Default Role	remote-application																		
802.1X Authentication Default Role	remote-employee	L2 Authentication Fail Through	☒																		
RADIUS Interim Accounting	☐	User derivation rules	--NONE--																		
Wired to Wireless Roaming	☒	SIP authentication role	--NONE--																		
Device Type Classification	☒	Enforce DHCP	☐																		

Figure 78 **wired-corporate AAA profile**

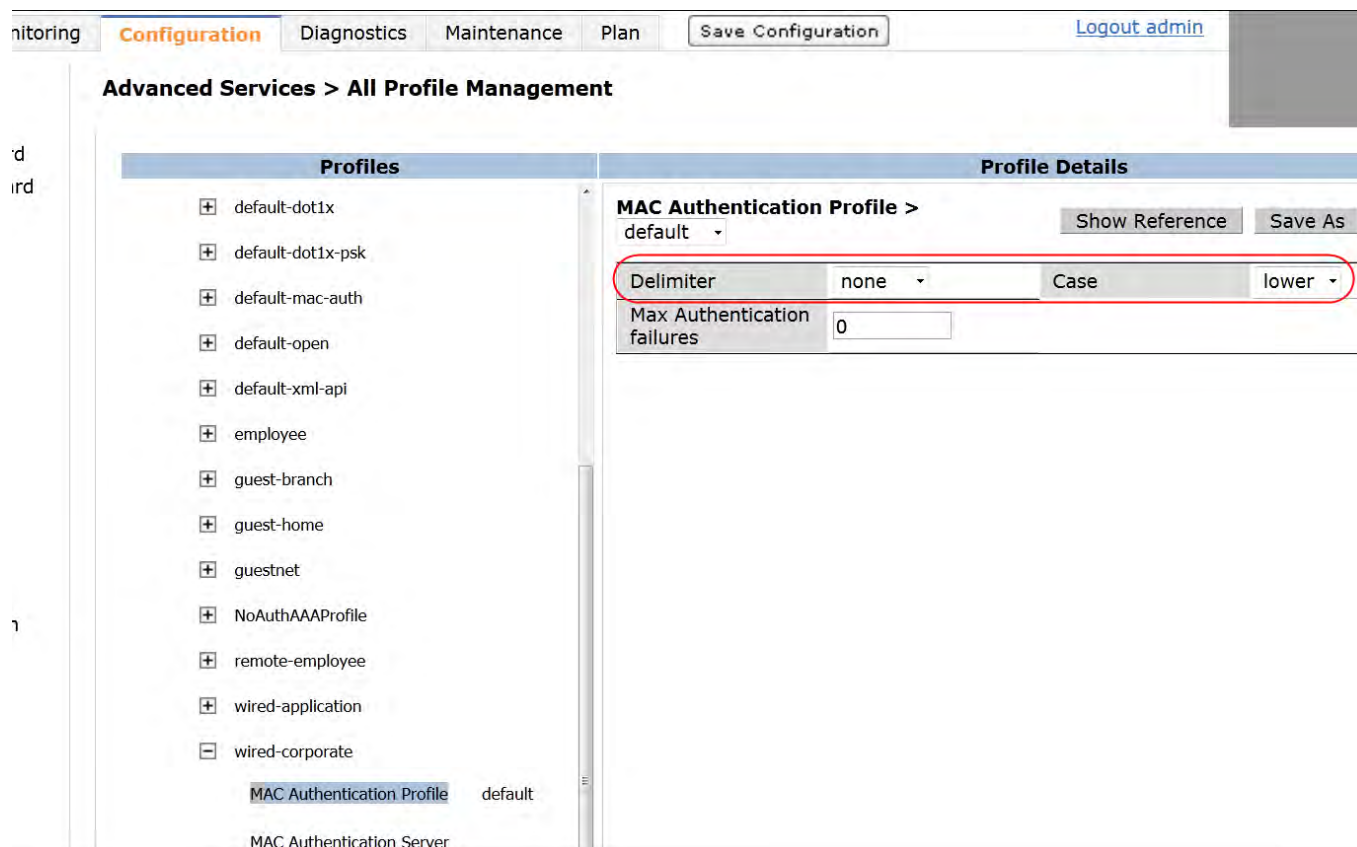


Figure 79 MAC authentication profile – delimiter configuration

Guest AAA Profile for Wired Ports

As discussed before, the guest access requirement for fixed telecommuter deployment is different from that of a micro branch office deployment. The wired port for fixed telecommuter deployment is configured for local access and connectivity to the Internet. The wired port for micro branch office deployment is configured to provide HTTPS/HTTP services to the Internet using captive portal authentication.

In most cases, the AAA profile used for guest WLAN can be reused for guest access on wired ports because the default user roles and authentication servers used for guest access is the same irrespective of the communication medium. In the example network, the **guest-home AAA profile** is used for wired access in fixed telecommuter deployments and the **guest-branch AAA profile** is used for wired access in micro branch office deployments. Most micro branch office deployments do not require wired access for guests, so for such deployments, the configuration of the wired port for captive portal authentication can be neglected.

AP Wired Port Profile

The wired port profile enables or disables a port and also contains the AAA profile, wired AP profile, and the Ethernet interface link profile. The remote AP backup feature of the wired AP profile allows local connectivity on a port when the controller is not reachable. When the connectivity to the controller is lost, the remote AP backup feature converts a port to bridge forwarding mode no matter what its original forwarding mode was. The clients receive an IP address from the DHCP server of the remote AP and the client has complete access to the RAP uplink network. Firewall policies cannot be applied on the clients that are connected to a port in remote AP backup mode.

In the example network, these wired port profiles are used:

- **wired-corporate:** Configures a wired port in split-tunnel forwarding mode with 802.1X and MAC authentication
- **wired-guest-home:** Configures a wired port in bridge forwarding mode with no authentication for local access
- **wired-guest-branch:** Configures a wired port in split-tunnel forwarding mode with captive portal authentication

Table 41 summarizes the wired port profiles used in the example network.

Table 41 Wired Port Profiles

Profile Name	Shutdown	Remote-AP Backup	Wired AP Profile	Ethernet Interface Link Profile	AAA Profile
wired-corporate	disable	enabled	wired-corporate	default	wired-corporate
wired-guest-home	disable	enabled	wired-guest-home	default	guest-home
wired-guest-branch	disable	disabled	wired-guest-branch	default	guest-branch

CLI

```

!
ap wired-port-profile "wired-corporate"
    wired-ap-profile "wired-corporate"
    rap-backup
    aaa-profile "wired-corporate"
!
ap wired-port-profile "wired-guest-branch"
    wired-ap-profile "wired-guest-branch"
    no rap-backup
    aaa-profile "guest-branch"
!
ap wired-port-profile "wired-guest-home"
    wired-ap-profile "wired-guest-home"
    rap-backup
    aaa-profile "guest-home"
!

```

WebUI Screenshot

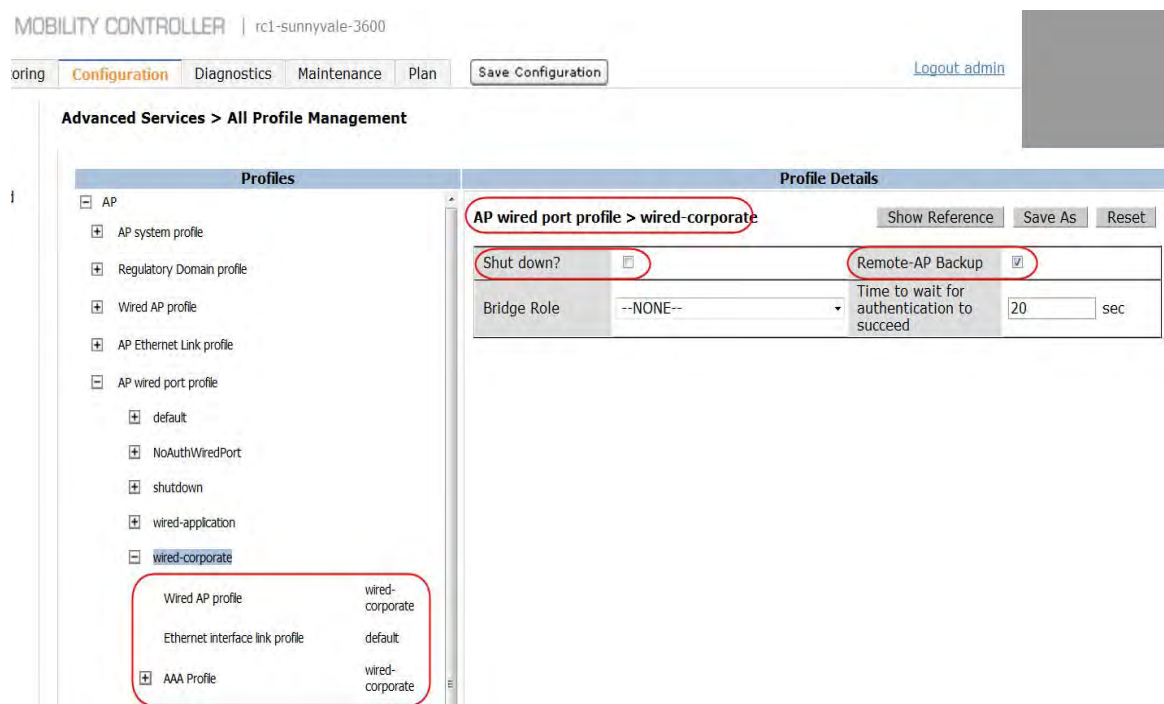


Figure 80 *wired-corporate wired port profile*

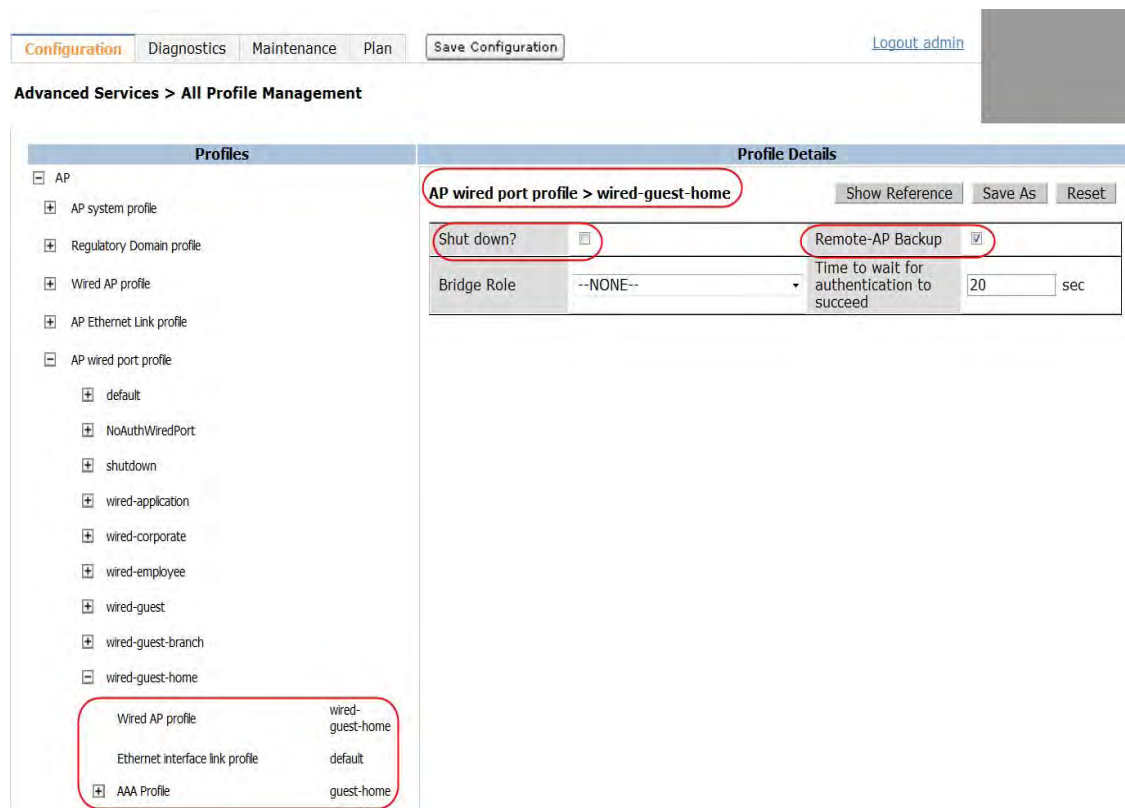


Figure 81 *wired-guest-home wired port profile*

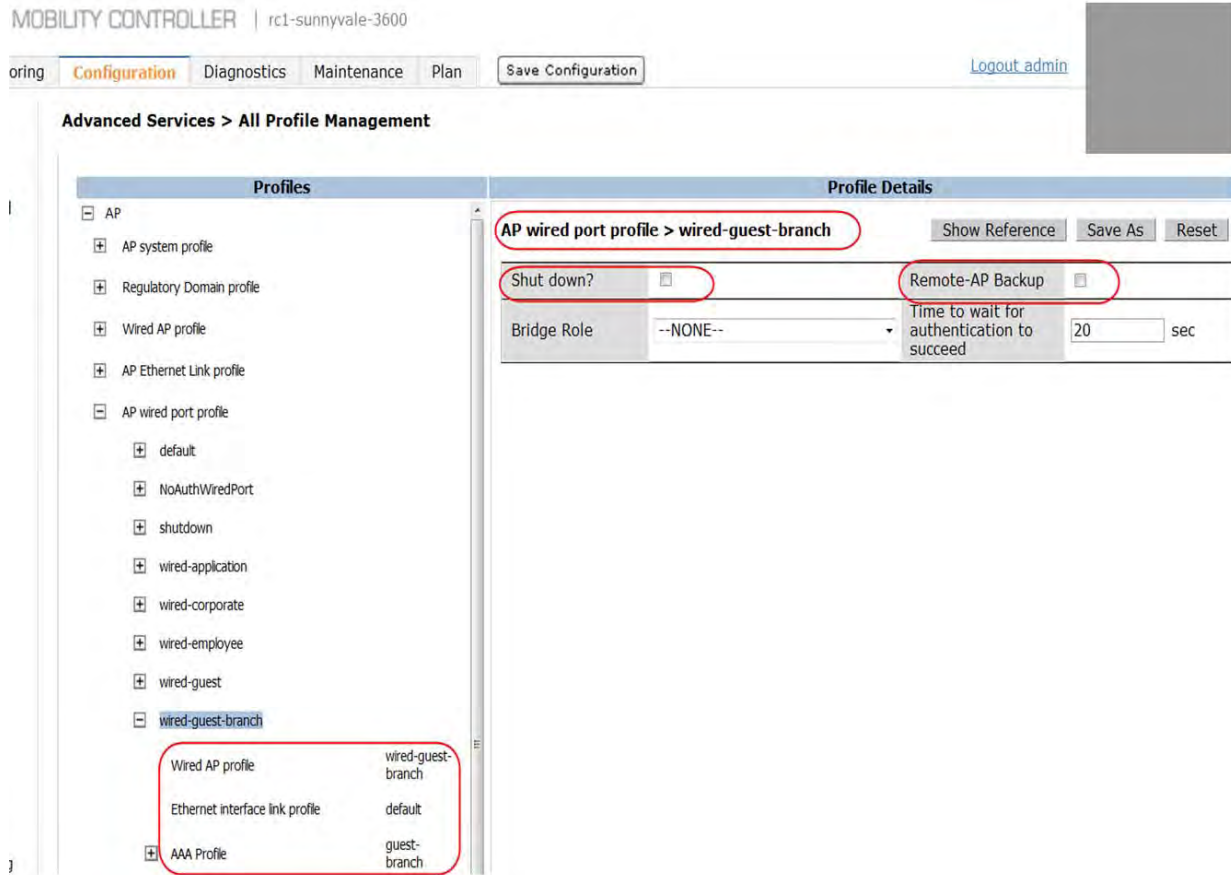


Figure 82 *wired-guest-branch wired port profile*

Wired Ports for Printer in Micro Branch Office Deployments

Most branch offices deploy printers for employee use. A wired port on a RAP can be configured specifically for use by printers. The needs of every organization are different. Some organizations might require central management of printers from the corporate headquarters, but others might allow local printers at branch office. Similarly, some organizations provide print services only to employees, but others allow guests to use the printers. So, if you require central management and employee-only access to printers, then consider these options:

- Deploy the printers on a separate VLAN.
- Configure the wired port used for a printer in tunnel forwarding mode.
- Assign a user role to the printer that restricts its access only to the printer server and required protocols.
- Remember, that when the print server is at the corporate headquarters, all the branch office print jobs must traverse the tunnel, which consumes WAN bandwidth.

In deployments where you do not require central management, consider these configurations:

- Deploy the printers on a separate VLAN.
- Configure the wired port used for a printer in bridge forwarding mode.
- Assign a user role to the printer that restricts its access only to the required protocols and services.
- Depending on the requirements, modify the user roles to allow printer access to everyone or only to the employees.

Depending on the requirements and security policies of their organization, the network administrators should choose the most appropriate configuration for the wired port used for printers.

Disabling the Wired Ports

Sometimes one or more wired ports in a RAP may need to be shut down. This is especially true if you are deploying dedicate+a wired port profile named wired-shutdown to disable any unused ports. [Table 42](#) summarizes the parameters of the wired-shutdown profile.

Table 42 Wired Port Profile to Disable Ports

Profile Name	Shutdown	Remote-AP Backup	Wired AP Profile	Ethernet Interface Link Profile	AAA Profile
wired-shutdown	enabled	disabled	default	default	default

CLI

```
!  
ap wired-port-profile "wired-shutdown"  
  shutdown  
!
```


WebUI Screenshot

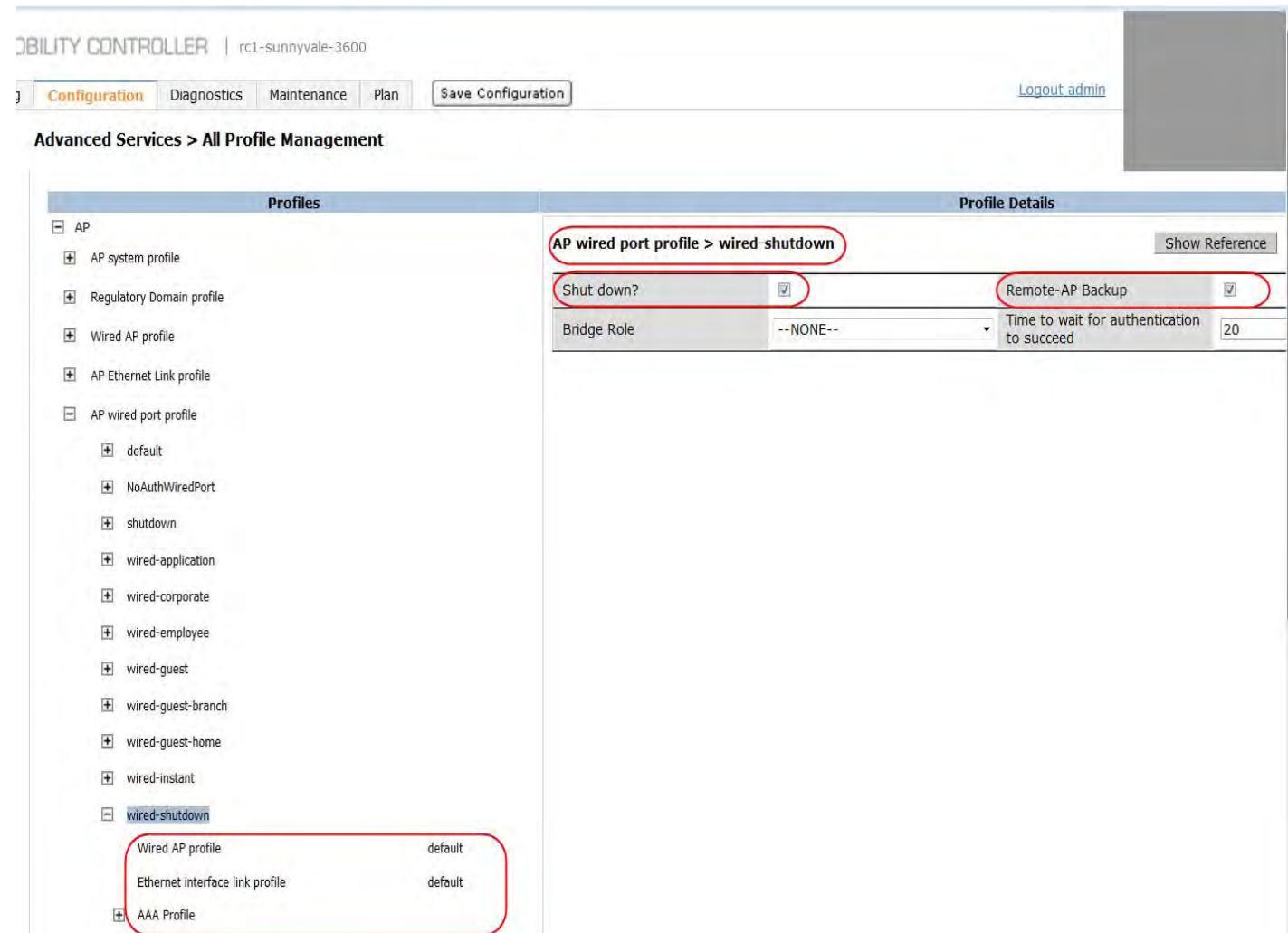


Figure 83 wired-shutdown wired port profile

Chapter 19: RAP 3G Uplink

In addition to the regular Ethernet uplink, Aruba RAP-5 and RAP-5WN support the 3G uplink. The 3G uplink on these RAPs can be used as a primary connection (in areas where no wired connectivity is available) or as a backup to the primary Ethernet link. The RAP-5 and RAP-5WN have a USB port to plug in the 3G USB modem. When 3G is used as the uplink, network administrators must calculate properly the total data usage to subscribe to the right data plan. Remember that the total data usage on a RAP is the sum of user traffic and the control traffic between RAP and the controller. 3G constraints such as uplink latency and bandwidth should also be considered. For details on 3G constraints, see [Chapter 26: Wide-Area Network Considerations](#).

The characteristics of the 3G USB modem provided by the service providers vary. The RAPs should be configured with some basic details such as the 3G service type and USB device type. These details can be configured on a per RAP basis or per AP group basis. If all RAPs that belong to an AP group have the same 3G service and USB, then a provisioning profile can be used to push the information related to the 3G service to all those RAPs. The provisioning profile of the ArubaOS defines the parameters that are required for Point-to-Point Protocol over Ethernet (PPPoE) and 3G uplink configurations. For configuring the provisioning profile for 3G uplink, depending on your 3G service provider, you should have some or all of the following information regarding the 3G USB and service:

- device type (required to install the appropriate driver)
- TTY device path
- device identifier
- initialization string
- dial string
- USB user name
- USB password



ArubaOS has a predefined configuration for 3G USB modems that works for the most common modems in the United States. If your modem is not in the list of devices, you need the above mentioned information. The predefined USB devices cannot be used in the provisioning profile. They are available for use only for individual AP specific provisioning. For information on the recommended 3G modems for RAPs, see the [interoperability](#) section on the Aruba Website



Assign a provisioning profile only if all the RAPs in an AP group have the same USB settings. If they do not, configure the 3G parameters individually for each RAP using AP provisioning. A provisioning profile can also be assigned to each RAP separately using the AP-specific configuration. For information on AP-specific configuration, see [AP-Specific Configuration on page 153](#).

When you configure the 3G uplink, specify the link priority. The priority value determines the primary and backup link. By default, the Ethernet link has the higher priority. The link with the highest priority value becomes the primary. If the priority values of the Ethernet and 3G uplinks are the same, the Ethernet link has the higher priority.

When the primary link is down, the RAP automatically switches to the backup link. The primary link is considered to be down if the link is physically disconnected or if the controller is unreachable due to connectivity issues in the intermediate WAN. If the physical link is down, the RAP immediately switches to the backup link. However, if the controller is unreachable due WAN issues, the RAP attempts twice to reconnect to the controller using the primary link before it switches to the backup link. Even after the RAP successfully establishes a connection to the controller through the backup link, it periodically (every 170 seconds) checks the status of the primary link. If the primary link is up, the RAP automatically tears down the backup link and establishes the IPsec connection to the controller through the primary uplink.



When the priority values of the Ethernet and 3G uplinks are the same, auto-preemption to the primary link is disabled.

The example network uses the provisioning profile named 3G-uplink, which is configured to use the 3G uplink as the backup link. [Table 43](#) summarizes the parameters of the 3G-uplink provisioning profile used in the example network.

Table 43 3G-uplink provisioning profile

Remote AP	Master IP	ISP	USB model	USB Device Identifier	USB Link Type	Link Priority Ethernet	Link Priority Cellular
enabled	branch.rde.arubanetworks.com	Verizon	UM175 (Pantech)	0x106c 3714	type=acm	20	10

CLI

```

!
ap provisioning-profile "3G-uplink"
  remote-ap
  master set branch.rde.arubanetworks.com
  usb-type acm
  usb-dev 0x106c 3714
  link-priority-ethernet 20
  link-priority-cellular 10
  reprovision
!

```

WebUI Screenshot

ng **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Logout admin](#)

Wireless > AP Installation > Provisioning Profiles

Provisioning Provisioning Profile RAP Whitelist Campus AP Whitelist

Provisioning Profiles

3G-uplink
default

Provision Profile Parameters for 3G-uplink

Remote-AP ☒ Master IP/FQDN Set branch.rde.aruba

PPPOE User Name PPPOE Password Retype:

PPPOE Service Name USB User Name

USB Password Retype: USB Device Type acm

USB Device Identifier 0x106c 3714 USB Dial String

USB Initialization String USB TTY device data path

USB TTY device control path Link Priority Ethernet 20

Link Priority Cellular 10 Uplink VLAN 0

Figure 84 3G-uplink provisioning profile

Provisioning 3G USB Settings on a per AP Basis

Configuration Diagnostics Maintenance Plan [Save Configuration](#) [Logout admin](#)

Wireless > AP Installation > Provisioning

Provisioning Provisioning Profile RAP Whitelist Campus AP Whitelist

Search [Search](#)

☐	AP Name ▲	AP Group ▲	AP IP ▲	AP Type ▲	AP MAC Address ▲	AP Serial Number ▲	Flags ▲	Status ▲
☒	RAP-telecommuter 1	small-branch-office	10.169.136.53	RAP-5WN	00:0b:86:66:7a:d1	AG0006347	Rc2	Up 19d:15h:28m:37s
☐	remote-AM-branch	remote-AM	10.169.136.55	105	00:24:6c:c0:12:b5	AL0004633	R	Up 19d:15h:28m:31s
☐	rap5	telecommuter	10.169.136.71	RAP-5WN	00:0b:86:66:8a:2b	AG0007133	Rc2	Up 3d:19h:13m:1s

1 | 1-3 of 3 10

Flags: U = Unprovisioned; N = Duplicate name; G = No such group; L = Unlicensed; I = Inactive; H = Using 802.11n license; D = Dirty or no config; X = Maintenance Mode; P = PPPoE AP; B = Built-in AP; R = Remote AP; R- = Remote AP requires Auth; C = Cellular RAP; c = CERT-based RAP; 2=Using IKE version 2; M = Mesh node; Y = Mesh Recovery;

[Provision](#)

Figure 85 Choosing an AP for provisioning

ring **Configuration** Diagnostics Maintenance Plan **Save Configuration**

Wireless > AP Installation > Provision

Provisioning Provisioning Profile RAP Whitelist Campus AP Whitelist

AP Parameters
AP Group: telecommuter

AP Installation Mode
☒ Default ☐ Indoor ☐ Outdoor

Antenna Parameters
Antenna Selection
☒ Internal/Included Antenna ☐ External Antenna

Authentication Method
Remote AP ☒ Yes ☐ No
Remote AP Authentication Method ☐ Pre-shared Key ☒ Certificate
IKE PSK: Confirm IKE PSK:
User credential assignment ☒ Use Automatic Generation ☐ Global User Name/Password ☐ per AP User Name/Password
User Name: Generate
Password: Generate Confirm Password:
☐ PPPoE Parameters
Service Name:
User Name:
Password: Confirm Password:
CHAP Secret: Confirm CHAP Secret:

Master Discovery
☐ Use AP Discovery Protocol
☐ Host Controller IP Address Master Controller IP Address/DNS name
☒ Host Controller Name aruba-master Master Controller IP Address/DNS name 192.168

IP Settings
Uplink Vlan: 0
☒ Obtain IP Address Using DHCP
☐ Use the following IP Address
IP Address: Subnet Mask:
Gateway IP Address:
DNS IP Address: Domain Name:
IPv6 Address/Prefix-length:
Gateway IPv6 Address:
DNS IPv6 Address:

FQLN Mapper
Remove FQLN: ☐
Campus: N/A Building: N/A Floor:

USB Settings
☒ USB Parameters
Device: Mercury Sierra Compass 885 (ATT) TTY Device Data Path: ttyUSB4
Path: Initialization String:
Device Identifier: Device Type: sierra-gsm
Dial String: PPP Username:
PPP Password: Confirm PPP Password:
Link Priority: 0 Link Priority Cellular: 0

AP List

AP IP Address	AP Name	AP Group	SNMP System Location	Mesh Role	AP Type
10.169.136.71	rap5	telecommuter		none	RAP-5WN

Apply and

Figure 86 Setting USB parameters using AP provisioning

3G USB modems can also be provisioned onsite using the RAP console. All the USB parameters required for a 3G USB modem should be entered into the default RAP console (<https://rapconsole.arubanetworks.com>) by the onsite user. For information on logging into to default RAP console, see [Chapter 25: RAP Provisioning](#).



The "Remote Access Point Setup" form is shown with the "USB" tab selected and circled in red. The form includes fields for "Device" (set to "Other (Any)"), "Device Type" (set to "any"), "Initialization String", "PPP Username", "PPP Password", "TTY Device Path", "Device Identifier", "Dial String", "Modeswitch", "Link Priority Cellular" (set to 0), and "Link Priority Ethernet" (set to 0). There are "Save", "Clear", and "Continue" buttons at the bottom.

Figure 87 **Provisioning RAP onsite**

Chapter 20: Configuring the AP Group for Telecommuter and Micro Branch Office Deployments

An AP group is a unique collection of configuration profiles. After you have configured all the required profiles, it is easy to form an AP group. To form an AP group, simply mix-and-match profiles based on the requirements.

The telecommuter AP group is used for all RAPs in fixed telecommuter deployments and the micro-branch-office AP group is used for RAPs of the micro branch office deployments.

[Table 44](#) summarizes the two AP groups that are used to provide client access in the example network and the profiles associated with each of these AP groups.

Table 44 AP Groups for Telecommuter and Micro Branch Office Deployments

Profile Categories	Profile Type	telecommuter AP Group Profiles Used	Micro-branch-office AP Group Profiles Used
Wireless LAN	VAP profile	remote-employee guest-home	remote-employee guest-branch
RF Management	802.11a radio profile	RAP-home	RAP-branch
	802.11g radio profile	RAP-home	RAP-branch
AP	AP system profile	rc-sunnyvale-3600	rc-sunnyvale-3600
	Ethernet interface 0 port configuration	default	default
	Ethernet interface 1 port configuration	wired-corporate	wired-corporate
	Ethernet interface 2 port configuration	wired-corporate	wired-corporate
	Ethernet interface 3 port configuration	wired-guest-home	wired-corporate
	Ethernet interface 4 port configuration	wired-guest-home	wired-guest-branch
	Provisioning Profile	—	3G-uplink
IDS	IDS profile (use the wizard)	—	branch-wips [Created using the wizard. See Chapter 23: Wireless Intrusion Prevention (IDS Profiles) of RFProtect.]

CLI

```
!  
ap-group "micro-branch-office"  
    virtual-ap "remote-employee"  
    virtual-ap "guest-branch"  
    dot11a-radio-profile "RAP-branch"  
    dot11g-radio-profile "RAP-branch"  
    enet1-port-profile "wired-corporate"  
    enet2-port-profile "wired-corporate"  
    enet3-port-profile "wired-corporate"  
    enet4-port-profile "wired-guest-branch"  
    ap-system-profile "rc-sunnyvale-3600"  
    provisioning-profile "3G-uplink"  
    ids-profile "branch-wips"  
!  
ap-group "telecommuter"  
    virtual-ap "remote-employee"  
    virtual-ap "guest-home"  
    dot11a-radio-profile "RAP-home"  
    dot11g-radio-profile "RAP-home"  
    enet1-port-profile "wired-corporate"  
    enet2-port-profile "wired-corporate"  
    enet3-port-profile "wired-guest-home"  
    enet4-port-profile "wired-guest-home"  
    ap-system-profile "rc-sunnyvale-3600"  
!
```


WebUI Screenshot

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan [Save Configuration](#)

WIZARDS
 AP Wizard
 Controller Wizard
 WLAN/LAN Wizard
 License Wizard
 WIP Wizard

NETWORK
 Controller
 VLANs
 Ports
 Cellular Profile
IP

SECURITY
 Authentication
 Access Control

WIRELESS
> AP Configuration

MANAGEMENT
 General
 Administration
 Certificates
 SNMP
 Logging
 Clock
 Guest Provisioning
 Captive Portal
 SMTP
 Bandwidth Calculator

Configuration > AP Group > Edit "telecommuter"

Profiles	
☐ Wireless LAN	
☐ Virtual AP	
☐ remote-employee	
☐ guest-home	
☐ RF Management	
☐ 802.11a radio profile	<u>RAP-home</u>
☐ 802.11g radio profile	<u>RAP-home</u>
RF Optimization profile	default
RF Event Thresholds profile	default
☐ AP	
☐ Ethernet interface 0 port configuration	<u>default</u>
☐ Ethernet interface 1 port configuration	<u>wired-corporate</u>
☐ Ethernet interface 2 port configuration	<u>wired-corporate</u>
☐ Ethernet interface 3 port configuration	<u>wired-guest-home</u>
☐ <u>Ethernet interface 4 port configuration</u>	<u>wired-guest-home</u>
AP system profile	<u>rc-sunnyvale-3600</u>
Regulatory Domain profile	default
Provisioning profile	
AP authorization profile	
☐ QOS	
☐ IDS	
☐ Mesh	

Figure 88 Telecommuter AP group

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan Save Configuration

WIZARDS
 AP Wizard
 Controller Wizard
 WLAN/LAN Wizard
 License Wizard
 WIP Wizard

NETWORK
 Controller
 VLANs
 Ports
 Cellular Profile
 IP

SECURITY
 Authentication
 Access Control

WIRELESS
> AP Configuration
 AP Installation

MANAGEMENT
 General
 Administration
 Certificates
 SNMP
 Logging
 Clock
 Guest Provisioning
 Captive Portal
 SMTP
 Bandwidth Calculator

ADVANCED SERVICES

Configuration > AP Group > Edit "micro-branch-office"

Profiles	
Wireless LAN	
Virtual AP	
remote-employee	
guest-branch	
RF Management	
802.11a radio profile	RAP-branch
802.11g radio profile	RAP-branch
RF Optimization profile	default
RF Event Thresholds profile	default
AP	
Ethernet interface 0 port configuration	default
Ethernet interface 1 port configuration	wired-corporate
Ethernet interface 2 port configuration	wired-corporate
Ethernet interface 3 port configuration	wired-corporate
Ethernet interface 4 port configuration	wired-guest-branch
AP system profile	rc-sunnyvale-3600
Regulatory Domain profile	default
Provisioning profile	3G-uplink
AP authorization profile	
QOS	
IDS	
IDS profile	branch-wips

Figure 89 Micro-branch-office AP group

AP-Specific Configuration

AP-specific configuration allows the network administrators to make changes to specific APs in an AP group rather than applying the changes to the entire AP group. AP-specific configuration is very useful for changing a number of settings such as the SSID settings, 3G USB settings, or the radio settings of a few APs in an AP group with hundreds of APs. If AP-specific configuration is used for an AP, the AP inherits all the profiles and settings of the AP group it belongs to and plus or minus the AP-specific settings. All the profiles and settings available for an AP group are also available for AP-specific configuration.

Consider an AP group that uses a provisioning profile named 3g-uplink for all its RAPs. If the 3G settings of a RAP, say RAP-1, in this AP group have to be changed, the network administrators can use the AP-specific configuration to push a new provisioning profile to RAP-1. RAP-1 inherits all the profiles and settings of the AP group it belongs to, except for the new provisioning profile that is specific to it.

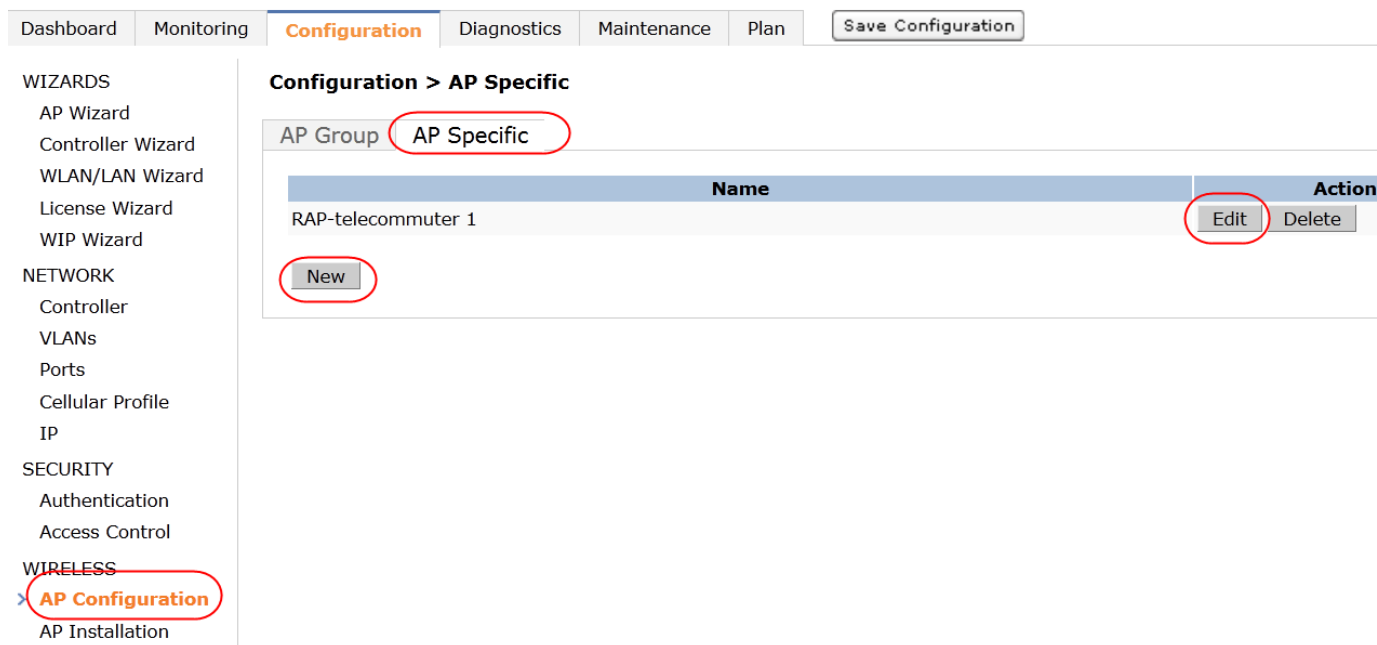


Figure 90 Add an AP to the AP Specific configuration list

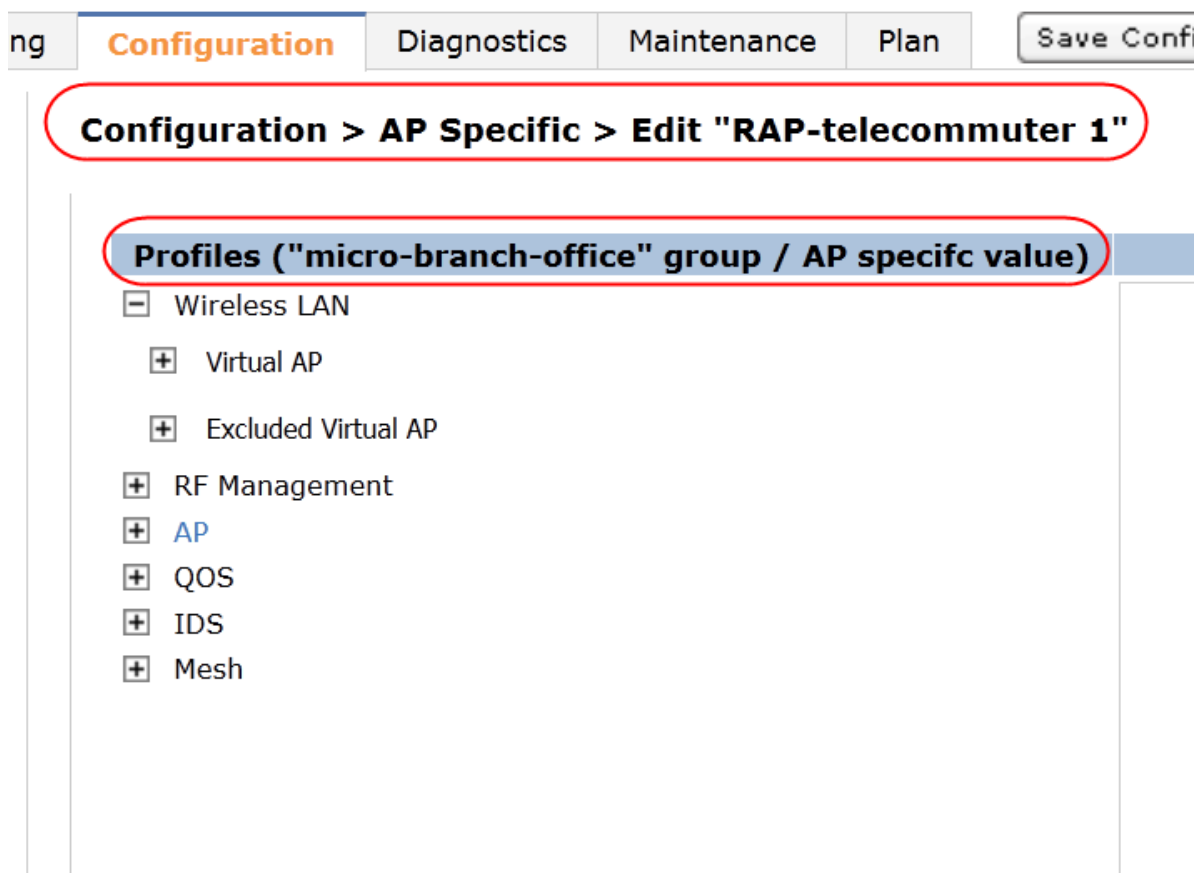


Figure 91 *Edit the AP-specific configurations for an AP*

Chapter 21: AP Group for Dedicated Air Monitors

The air monitor (AM) does not provide service to any clients, so VAP profiles and QoS profiles are not used by AP groups that are built for AMs. To create an AP group for AMs, you need these profiles:

- AM scanning profile
- 802.11a radio profile
- 802.11g radio profile
- AP system profile
- IDS profile

This chapter explains the configuration of the remote-AM AP group for AMs in micro branch office sites.

Figure 92 summarizes the AP groups used for AMs in the example network.

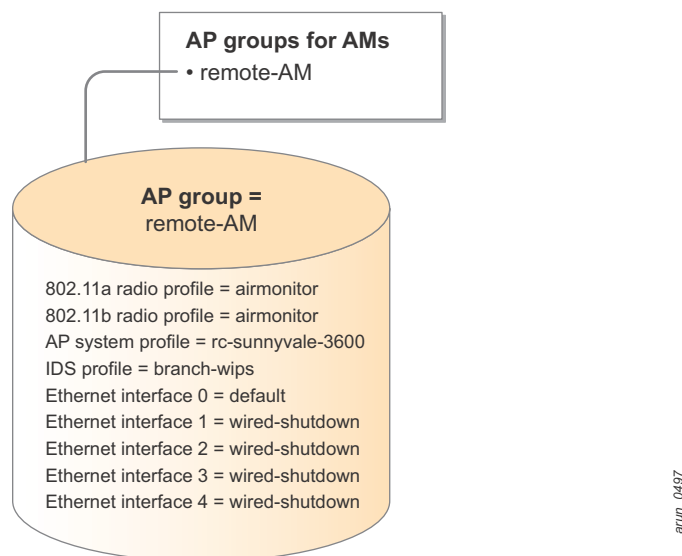


Figure 92 **AP groups for AMs**

Configuring the AM Scanning Profile

The RFProtect feature set that was introduced in ArubaOS 6.0 provides the TotalWatch™ scanning tool. When you add the RFProtect license, TotalWatch is enabled by default. TotalWatch extends the scanning capabilities of an AM to all the 14 channels in the 2.4 GHz and to the entire 4.9 – 5.895 GHz spectrum in 5 MHz increments.



Only rogues on legal channels are contained wirelessly, but rogues on any channel can be contained using wired containment. All rogues that are detected wirelessly are reported, but wireless containment can be enforced only against rogues that operate within the regulatory domain. APs and AMs cannot transmit, even to contain rogues, outside of the legal regulatory domain channels they are operating in without violating local law. The 4.9 GHz range is reserved for public safety applications in most regulatory domains. The open source hardware drivers and software-defined radios in many consumer-grade APs mean that a malicious user could program an AP to operate illegally in this range. Aruba AMs scan this range and report back any rogue AP found operating on this band. However, due to regulatory restrictions, the AM cannot contain the device using wireless containment.

For more information about TotalWatch, see the [Aruba 802.11n Networks Validated Reference Design](#).

The AM scanning profile defines all the settings that are related to TotalWatch. The scanning profile applies only to radios operating as dedicated AMs and determines their scanning capabilities. The scanning capabilities of a radio operating in AP mode are determined by the scan-mode parameter in the ARM profile. Aruba recommends that you do not change the following four parameters of this profile under any circumstances, unless specifically advised by the Aruba Technical Assistance Center (TAC) team:

- Dwell time: active channels
- Dwell time: regulatory domain channels
- Dwell time: nonregulatory domain channels
- Dwell time: rare channels

The scan-mode parameter in this profile determines the range of channels that are scanned by an AM. Aruba recommends that you set this value to rare for all AMs. If you set this value to rare on AMs, the AMs scan the 4.9 GHz range and the entire 2.4 GHz and 5 GHz range.

The example network uses the AM scanning profile named am-scan for the AMs. [Table 45](#) summarizes the AM scanning profile that is used.

Table 45 AM Scanning Profile Used in Example Network

AM Scanning Profile Name	Scan Mode	Purpose
am-scan	rare	Used for all AMs. Scans all the 14 channels in the 2.4 GHz and the entire 4.9 – 5.895 GHz spectrum in 5 MHz increments.

CLI Configuration

MC1-Sunnyvale-3600

```
!  
rf am-scan-profile "am-scan"  
  scan-mode rare  
!
```

WebUI Screenshot

MC1-Sunnyvale-3600

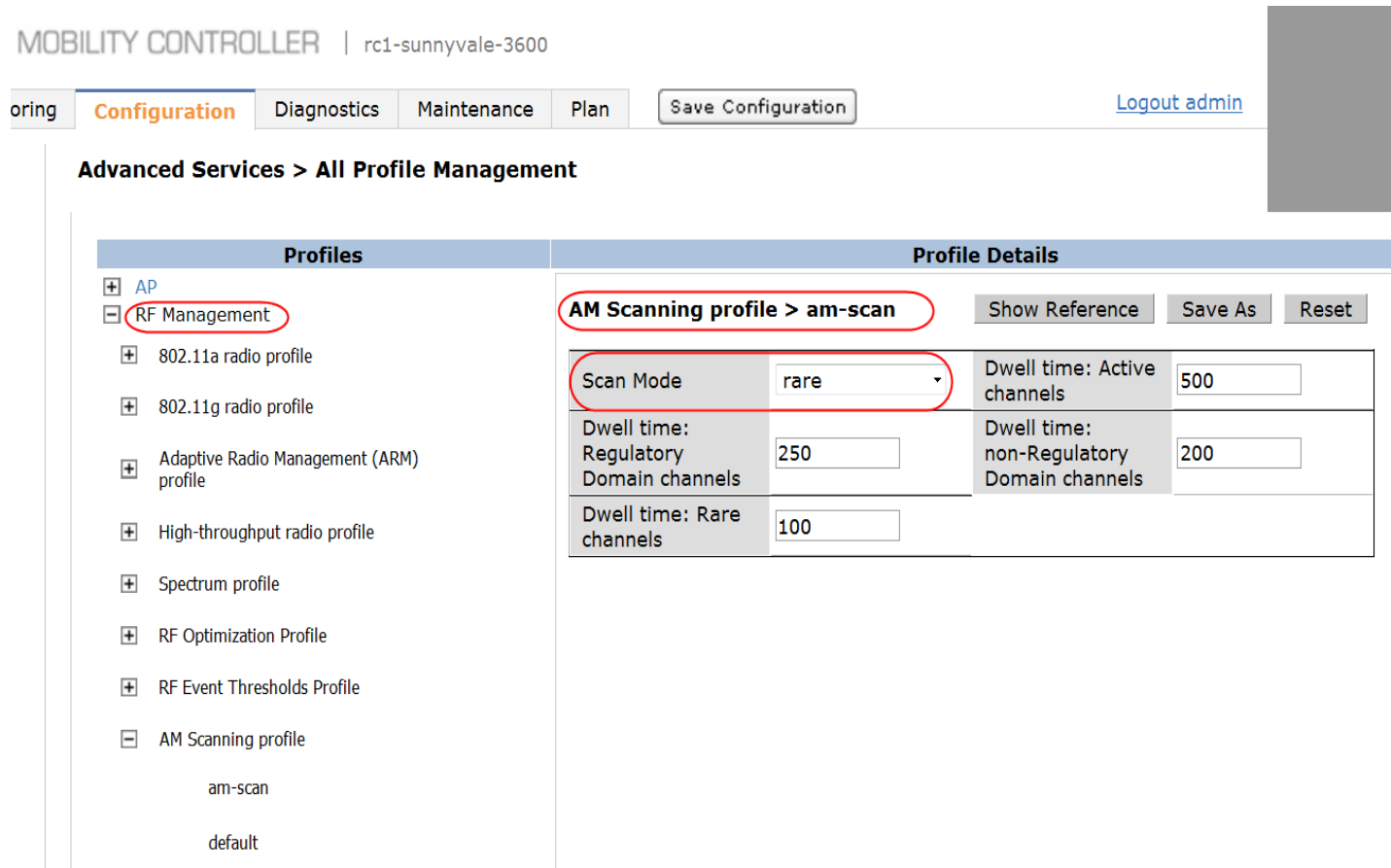


Figure 93 am-scan AM scanning profile

Configuring the 802.11a and 802.11g Radio Profiles

For AMs, the mode parameter in the 802.11a and 802.11g radio profiles is set to am-mode. [Figure 94](#) summarizes the radio profiles used in the example network for the AP groups that are built for AMs.

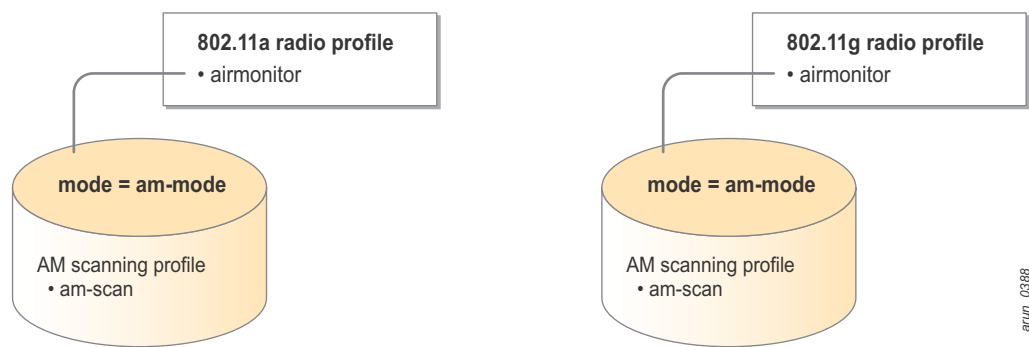


Figure 94 Radio profiles for the AP groups built for AMs

[Table 46](#) summarizes the 802.11a and 802.11g radio profiles used in the example network by the AP groups built for AMs.

Table 46 Radio Profiles of AP Groups Used for AMs

Profile Type	Profile Name	Mode	ARM Profile	AM Scanning Profile	Purpose
802.11a radio profile	airmonitor	am-mode	—	am-scan	Makes the 5 GHz radio function as an AM
802.11g radio profile	airmonitor	am-mode	—	am-scan	Makes the 2.4 GHz radio function as an AM

CLI Configuration

MC1-Sunnyvale-3600

```
!  
rf dot11a-radio-profile "airmonitor"  
  mode am-mode  
  am-scan-profile "am-scan"  
!  
rf dot11g-radio-profile "airmonitor"  
  mode am-mode  
  am-scan-profile "am-scan"  
!
```

WebUI Screenshot

MC1-Sunnyvale-3600

MOBILITY CONTROLLER | rc1-sunnyvale-3600

ring **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Logout a](#)

Advanced Services > All Profile Management

Profiles	Profile Details																																																				
- AP - RF Management 802.11a radio profile airmonitor - Adaptive Radio Management (ARM) Profile default - High-throughput Radio Profile default-a - Spectrum Monitoring Profile default-a - AM Scanning Profile am-scan	802.11a radio profile > airmonitor Show Reference Save As Reset <table border="1"><tbody><tr><td>Radio enable</td><td>☒</td><td>Mode</td><td>am-mode</td></tr><tr><td>High throughput enable (radio)</td><td>☒</td><td>Channel</td><td> Secondary Channel: ☒ None ☐ Above ☐ Below</td></tr><tr><td>Beacon Period</td><td>100 msec</td><td>Beacon Regulate</td><td>☐</td></tr><tr><td>Transmit EIRP</td><td>15</td><td>Advertise 802.11d and 802.11h Capabilities</td><td>☐</td></tr><tr><td>TPC Power</td><td>15</td><td>Spectrum load balancing</td><td>☐</td></tr><tr><td>Spectrum Load balancing mode</td><td>channel</td><td>Spectrum load balancing update interval (sec)</td><td>30 seconds</td></tr><tr><td>Spectrum load balancing threshold (%)</td><td>20 percent</td><td>Advertized regulatory max EIRP</td><td>0</td></tr><tr><td>Spectrum Load Balancing domain</td><td></td><td>RX Sensitivity Tuning Based Channel Reuse</td><td>disable</td></tr><tr><td>RX Sensitivity Threshold</td><td>0 -dBm</td><td>Non 802.11 Interference Immunity</td><td>Level-2</td></tr><tr><td>Enable CSA</td><td>☐</td><td>CSA Count</td><td>4</td></tr><tr><td>Management Frame Throttle interval</td><td>1 sec</td><td>Management Frame Throttle Limit</td><td>20</td></tr><tr><td>ARM/WIDS Override</td><td>☐</td><td>Maximum Distance</td><td>0 meters</td></tr><tr><td>Spectrum Monitoring</td><td>☐</td><td></td><td></td></tr></tbody></table>	Radio enable	☒	Mode	am-mode	High throughput enable (radio)	☒	Channel	Secondary Channel: ☒ None ☐ Above ☐ Below	Beacon Period	100 msec	Beacon Regulate	☐	Transmit EIRP	15	Advertise 802.11d and 802.11h Capabilities	☐	TPC Power	15	Spectrum load balancing	☐	Spectrum Load balancing mode	channel	Spectrum load balancing update interval (sec)	30 seconds	Spectrum load balancing threshold (%)	20 percent	Advertized regulatory max EIRP	0	Spectrum Load Balancing domain		RX Sensitivity Tuning Based Channel Reuse	disable	RX Sensitivity Threshold	0 -dBm	Non 802.11 Interference Immunity	Level-2	Enable CSA	☐	CSA Count	4	Management Frame Throttle interval	1 sec	Management Frame Throttle Limit	20	ARM/WIDS Override	☐	Maximum Distance	0 meters	Spectrum Monitoring	☐		
Radio enable	☒	Mode	am-mode																																																		
High throughput enable (radio)	☒	Channel	Secondary Channel: ☒ None ☐ Above ☐ Below																																																		
Beacon Period	100 msec	Beacon Regulate	☐																																																		
Transmit EIRP	15	Advertise 802.11d and 802.11h Capabilities	☐																																																		
TPC Power	15	Spectrum load balancing	☐																																																		
Spectrum Load balancing mode	channel	Spectrum load balancing update interval (sec)	30 seconds																																																		
Spectrum load balancing threshold (%)	20 percent	Advertized regulatory max EIRP	0																																																		
Spectrum Load Balancing domain		RX Sensitivity Tuning Based Channel Reuse	disable																																																		
RX Sensitivity Threshold	0 -dBm	Non 802.11 Interference Immunity	Level-2																																																		
Enable CSA	☐	CSA Count	4																																																		
Management Frame Throttle interval	1 sec	Management Frame Throttle Limit	20																																																		
ARM/WIDS Override	☐	Maximum Distance	0 meters																																																		
Spectrum Monitoring	☐																																																				

or

- AP
 - default
 - RAP
 - RAP-branch
 - RAP-home
- 802.11g radio profile
- Adaptive Radio Management (ARM) profile
- High-throughput radio profile
- Spectrum profile
- RF Optimization Profile
- RF Event Thresholds Profile
- AM Scanning profile
- Wireless LAN
- Mesh
- QoS

Configuring the AP Groups for Air Monitors

In the example network, a separate AP group named remote-AM is used for the dedicated AMs of the micro branch office deployment. [Table 47](#) summarizes the profiles used by the remote-AM AP group.

Table 47 remote-AM AP Groups

Profile Categories	Profile Type	remote-AM AP Group Profiles Used
Wireless LAN	VAP profile	—
RF Management	802.11a radio profile	airmonitor
	802.11g radio profile	airmonitor
AP	AP system profile	rc-sunnyvale-3600. For details, see Chapter 16: Configuring the AP System Profiles .
	Ethernet interface 0 port configuration	default
	Ethernet interface 1 port configuration	wired-shutdown
	Ethernet interface 2 port configuration	wired-shutdown
	Ethernet interface 3 port configuration	wired-shutdown
	Ethernet interface 4 port configuration	wired-shutdown
IDS	IDS profile (use the wizard)	branch-wips (Created using the wizard. See Chapter 23: Wireless Intrusion Prevention (IDS Profiles) of RFProtect .)

CLI

```

!
ap-group "remote-AM"
  dot11a-radio-profile "airmonitor"
  dot11g-radio-profile "airmonitor"
  enet1-port-profile "wired-shutdown"
  enet2-port-profile "wired-shutdown"
  enet3-port-profile "wired-shutdown"
  enet4-port-profile "wired-shutdown"
  ap-system-profile "rc-sunnyvale-3600"
  ids-profile "branch-wips"
!

```

WebUI Screenshot

MOBILITY CONTROLLER | rc1-sunnyvale-3600

Configuration | Diagnostics | Maintenance | Plan | Save Configuration

Configuration > AP Group > Edit "remote-AM"

Profiles	
[-] Wireless LAN	
[-] Virtual AP	
[-] RF Management	
[-] 802.11a radio profile	<u>airmonitor</u>
Adaptive Radio Management (ARM) Profile	default
High-throughput Radio Profile	default-a
Spectrum Monitoring Profile	default-a
AM Scanning Profile	<u>am-scan</u>
[-] 802.11g radio profile	<u>airmonitor</u>
Adaptive Radio Management (ARM) Profile	default
High-throughput Radio Profile	default-g
Spectrum Monitoring Profile	default-g
AM Scanning Profile	<u>am-scan</u>
RF Optimization profile	default
RF Event Thresholds profile	default
[-] AP	
[+] Ethernet interface 0 port configuration	<u>default</u>
[+] Ethernet interface 1 port configuration	<u>wired-shutdown</u>
[+] Ethernet interface 2 port configuration	<u>wired-shutdown</u>
[+] Ethernet interface 3 port configuration	wired-shutdown
[+] Ethernet interface 4 port configuration	<u>wired-shutdown</u>
AP system profile	<u>rc-sunnyvale-3600</u>
Regulatory Domain profile	default
Provisioning profile	
AP authorization profile	
[+] QOS	
[-] IDS	
[+] IDS profile	<u>branch-wips</u>
[+] Mesh	

Figure 95 remote-AM AP group

Chapter 22: Fallback/Backup Mode for Wireless SSIDs and Wired Ports

A VAP can be configured to operate in backup mode. A backup VAP is enabled only when the connectivity to the LMS and the backup LMS controller is lost. As soon as the RAP resumes connectivity to the controller, the backup VAP is disabled. The backup SSID operates in bridge mode. The RAP stores the configuration information, which allows it to broadcast the backup SSID when the connectivity to the controller is lost. A backup SSID can be open or it can use PSK. 802.1X is not supported in backup mode.



While operating in fallback mode, the RAP periodically retries its IPsec tunnel to the controller. If tunnel establishment is successful, the RAP immediately brings up the standard RAP profile.

The backup mode is very useful for telecommuter solutions, especially when the RAP is connected to a network that has a captive portal. When a travelling employee connects the RAP to the wired port of a hotel network that uses captive portal, the RAP will not be able to connect to the controller. So, the RAP broadcasts the backup SSID. The user can now connect to the backup SSID and when he opens a web browser, the captive portal page is displayed. From perspective of the hotel's captive portal, the traffic originates from the MAC address and IP address of the RAP because the RAP is configured to Src-NAT the user traffic. After the user authenticates to the captive portal, the RAP can establish a connection the controller. After the connectivity to the controller is established, the RAP disables the backup SSID, broadcasts the standard SSIDs, and enables the configured wired ports. For details on backup mode for wired ports, see [Chapter 18: RAP Wired Ports](#)



The user role assigned to the authenticated clients of the backup SSID should source-NAT all user traffic, except DHCP. For example, create a backup-user role with a policy that uses **any any svc-dhcp permit** followed by **any any any route src-nat rule**. Also, use the internal DCP server of the RAP to provide DHCP services for users on backup SSID.

Table 48 through Table 50 show the parameters used to configure a sample backup mode VAP.

Table 48 Sample backup SSID Profile

SSID Profile	Network Name (SSID)	Authentication	Encryption
backup SSID	backup	WPA2-PSK	AES

Table 49 Sample backup AAA Profile

AAA Profile	Initial Role	802.1X Profile
backup	backup-user	default-psk (predefined)



Whenever PSK is used for authentication, the default role that is assigned to authenticated users is specified in the initial role parameter of the AAA profile. To reduce the number of profiles, Aruba has included the default-psk profile within the 802.1X profile. The profiles are combined because the dynamic key generation process of a WPA™/WPA2 PSK process is similar to that key generation process of 802.1X/EAP. The PSK passphrase is run through an algorithm that converts it into a pairwise master key (PMK). This PMK is used in the four-way handshake process to generate the dynamic encryption keys. Select the predefined profile named default-psk as the 802.1X profile when PSK is used for authentication.

Table 50 Sample backup VAP Profile

VAP Profile	VLAN	Forward Mode	Remote AP Operation	AAA Profile	SSID Profile
backup	188 (RAP's internal DHCP server is used for this VAP)	bridge	backup	backup	backup SSID

CLI

```

!
wlan ssid-profile "backup SSID"
  essid "backup"
  opmode wpa2-psk-aes
  wpa-passphrase *****
!
aaa profile "backup"
  initial-role "backup-user"
  authentication-dot1x "default-psk"
!
wlan virtual-ap "backup"
  aaa-profile "backup"
  ssid-profile "backup SSID"
  vlan 188
  forward-mode bridge
  rap-operation backup
!

```

WebUI Screenshot

Advanced Services > All Profile Management

The screenshot displays the Aruba WebUI configuration page for 'All Profile Management'. The left sidebar shows a tree view of profiles, with 'SSID Profile' expanded and 'backup SSID' selected. The main panel shows the 'Profile Details' for 'backup SSID'. The 'Basic' tab is active, showing the 'Network' section with 'Network Name (SSID)' set to 'backup'. The '802.11 Security' section shows 'WPA2-PSK' selected for authentication and 'AES' for encryption. The 'Keys' section shows 'PSK AES Key/Passphrase' and 'Confirm Key/Passphrase' fields, both containing masked text. The 'Format' dropdown is set to 'PSK Passphrase'. A note at the bottom states: 'The PSK AES Hex Key should be a 64 character hexadecimal string' and 'The PSK AES Passphrase should be an ASCII string 8-63 characters in length'.

Figure 96 Sample backup SSID profile

Advanced Services > All Profile Management

Profiles		Profile Details																					
- AP - RF Management - Wireless LAN 802.11K Profile - SSID Profile - High-throughput SSID profile - Virtual AP profile - VIA Client WLAN Profile - AAA Profile - application backup - MAC Authentication Profile - MAC Authentication Server Group 802.1X Authentication Profile default-psk 802.1X Authentication Server Group - RADIUS Accounting Server Group		AAA Profile > backup Show Reference Save As <table> <tr> <td>Initial role</td> <td>backup-user</td> <td>MAC Authentication Default Role</td> <td>guest</td> </tr> <tr> <td>802.1X Authentication Default Role</td> <td>guest</td> <td>L2 Authentication Fail Through</td> <td>☐</td> </tr> <tr> <td>RADIUS Interim Accounting</td> <td>☐</td> <td>User derivation rules</td> <td>--NONE--</td> </tr> <tr> <td>Wired to Wireless Roaming</td> <td>☒</td> <td>SIP authentication role</td> <td>--NONE--</td> </tr> <tr> <td>Device Type Classification</td> <td>☒</td> <td>Enforce DHCP</td> <td>☐</td> </tr> </table>		Initial role	backup-user	MAC Authentication Default Role	guest	802.1X Authentication Default Role	guest	L2 Authentication Fail Through	☐	RADIUS Interim Accounting	☐	User derivation rules	--NONE--	Wired to Wireless Roaming	☒	SIP authentication role	--NONE--	Device Type Classification	☒	Enforce DHCP	☐
Initial role	backup-user	MAC Authentication Default Role	guest																				
802.1X Authentication Default Role	guest	L2 Authentication Fail Through	☐																				
RADIUS Interim Accounting	☐	User derivation rules	--NONE--																				
Wired to Wireless Roaming	☒	SIP authentication role	--NONE--																				
Device Type Classification	☒	Enforce DHCP	☐																				

Figure 97 Sample backup AAA profile

Advanced Services > All Profile Management

Profiles		Profile Details																																																	
- AP - RF Management - Wireless LAN 802.11K Profile - SSID Profile - High-throughput SSID profile - Virtual AP profile - default - guest-branch - guest-home - remote-application backup AAA Profile backup 802.11K Profile default SSID Profile backup SSID - EDCA Parameters Station profile - EDCA Parameters AP profile - High-throughput SSID Profile default		Virtual AP profile > backup Show Reference Save As Reset <table> <tr> <td>Virtual AP enable</td> <td>☒</td> <td>Allowed band</td> <td>all</td> </tr> <tr> <td>VLAN</td> <td>188</td> <td>Forward mode</td> <td>bridge</td> </tr> <tr> <td>Deny time range</td> <td>--NONE--</td> <td>Mobile IP</td> <td>☒</td> </tr> <tr> <td>HA Discovery on-association</td> <td>☐</td> <td>DoS Prevention</td> <td>☐</td> </tr> <tr> <td>Station Blacklisting</td> <td>☒</td> <td>Blacklist Time</td> <td>3600 sec</td> </tr> <tr> <td>Dynamic Multicast Optimization (DMO)</td> <td>☐</td> <td>Dynamic Multicast Optimization (DMO) Threshold</td> <td>6</td> </tr> <tr> <td>Authentication Failure Blacklist Time</td> <td>3600 sec</td> <td>Multi Association</td> <td>☐</td> </tr> <tr> <td>Strict Compliance</td> <td>☐</td> <td>VLAN Mobility</td> <td>☐</td> </tr> <tr> <td>Preserve Client VLAN</td> <td>☐</td> <td>Remote-AP Operation</td> <td>backup</td> </tr> <tr> <td>Drop Broadcast and Multicast</td> <td>☐</td> <td>Convert Broadcast ARP requests to unicast</td> <td>☐</td> </tr> <tr> <td>Deny inter user traffic</td> <td>☐</td> <td>Band Steering</td> <td>☐</td> </tr> <tr> <td>Steering Mode</td> <td>prefer-5ghz</td> <td></td> <td></td> </tr> </table>		Virtual AP enable	☒	Allowed band	all	VLAN	188	Forward mode	bridge	Deny time range	--NONE--	Mobile IP	☒	HA Discovery on-association	☐	DoS Prevention	☐	Station Blacklisting	☒	Blacklist Time	3600 sec	Dynamic Multicast Optimization (DMO)	☐	Dynamic Multicast Optimization (DMO) Threshold	6	Authentication Failure Blacklist Time	3600 sec	Multi Association	☐	Strict Compliance	☐	VLAN Mobility	☐	Preserve Client VLAN	☐	Remote-AP Operation	backup	Drop Broadcast and Multicast	☐	Convert Broadcast ARP requests to unicast	☐	Deny inter user traffic	☐	Band Steering	☐	Steering Mode	prefer-5ghz		
Virtual AP enable	☒	Allowed band	all																																																
VLAN	188	Forward mode	bridge																																																
Deny time range	--NONE--	Mobile IP	☒																																																
HA Discovery on-association	☐	DoS Prevention	☐																																																
Station Blacklisting	☒	Blacklist Time	3600 sec																																																
Dynamic Multicast Optimization (DMO)	☐	Dynamic Multicast Optimization (DMO) Threshold	6																																																
Authentication Failure Blacklist Time	3600 sec	Multi Association	☐																																																
Strict Compliance	☐	VLAN Mobility	☐																																																
Preserve Client VLAN	☐	Remote-AP Operation	backup																																																
Drop Broadcast and Multicast	☐	Convert Broadcast ARP requests to unicast	☐																																																
Deny inter user traffic	☐	Band Steering	☐																																																
Steering Mode	prefer-5ghz																																																		

Figure 98 Sample backup VAP profile

Chapter 23: Wireless Intrusion Prevention (IDS Profiles) of RFProtect

In any wireless network, it is important to protect the network against wireless attacks. Wireless security must be used in many regulated industries such as:

- healthcare
- federal government
- payment card industry

The ArubaOS wireless intrusion prevention (WIP) feature of the RFProtect software module provides a wide range of intrusion detection and intrusion prevention capabilities.

The RFProtect feature set of ArubaOS 6 and later also includes a patented containment called tarpitting. For more details on tarpitting and other RFProtect features, see the [Aruba 802.11n Networks Validated Reference Design](#). The intrusion detection system (IDS) profiles define all the possible WIP settings. Wireless security can be a complex topic with many different options, and it can be difficult to manage the wide range of IDS profiles available. To make things easier for users, Aruba developed a set of powerful wizards. Aruba wizards provide reasonable default values and help a user step through the available configuration options. You select a default template that provides an acceptable level of security for the network or a customized set of options. The wizard simplifies the selection of security options and helps to eliminate errors in the configuration. Aruba recommends the use of the WIP wizard for WIP configuration.

The WIP wizard provides the options to enable, define, or change the following items:

- rule-based rogue classification
- WIP policy creation and assignment to AP groups
- detection options for infrastructure attacks
- detection options for WLAN clients attacks
- protection options for infrastructure attacks
- protection options for WLAN clients attacks

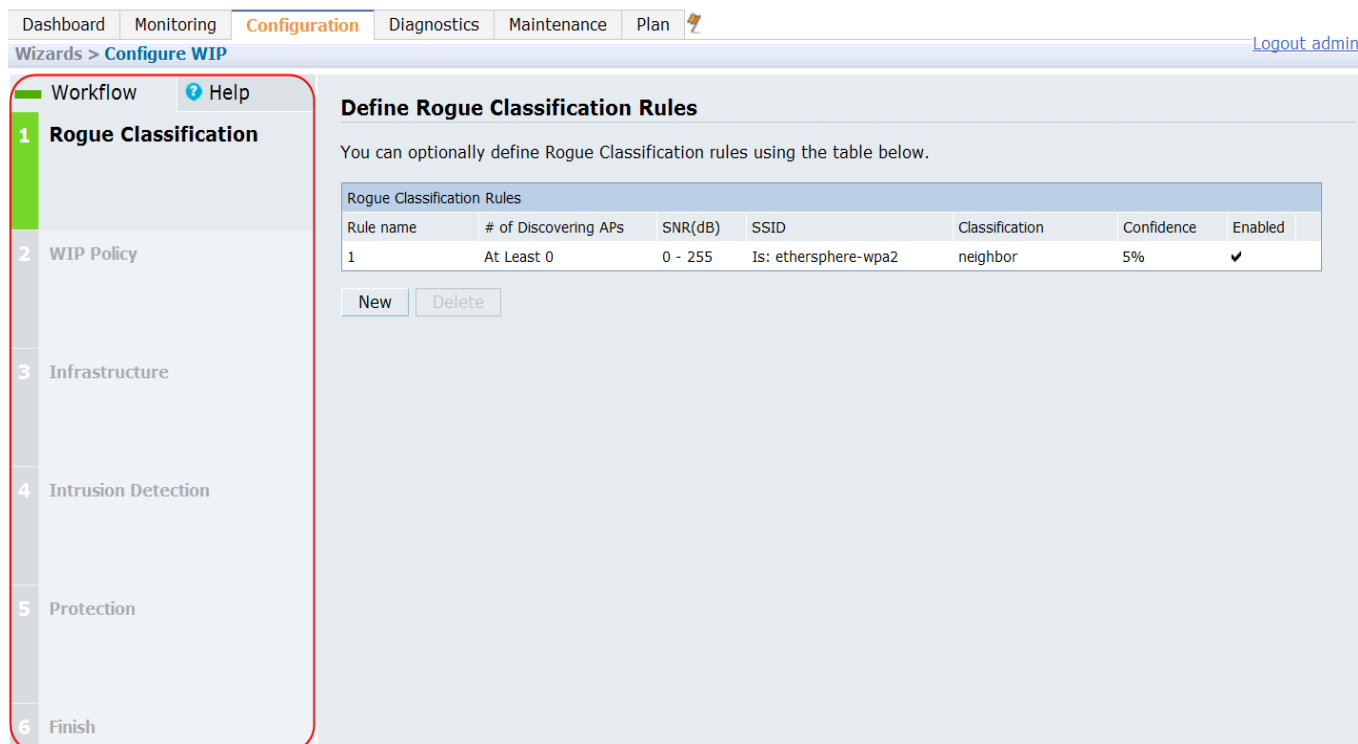


Figure 99 Configuration options in the WIP wizard

In rule-based classification, an AP is classified as a suspected rogue or as a neighbor depending on the user-defined rules. The AP classification rules can be specified by the SSID of the AP, signal-to-noise ratio (SNR) of the AP, or the number of APs that can see that AP. The rule-based classification is very useful for differentiating neighbors and rogues.

The detection setting on the wizard for the infrastructure and the client can be turned off or set to a predefined high, medium, or low level. The wizard also allows custom settings. The high detection setting enables all the detection mechanisms applicable. The medium setting enables some important detection mechanisms, and the low setting enables only the most critical detection mechanisms.

The protection settings for infrastructure have the same option as the detection settings, but the protection settings for clients can be set only to low or high.

Security requirements of remote deployments vary. Rule-based classification in remote networks can be extremely cumbersome and might even be impossible in most cases. This difficulty is due to the complexity of identifying and defining the neighboring networks at various branch sites. In most fixed telecommuter deployments, WIP features such as rogue containment and detection can be turned off to reduce the number of false alarms. The WIP requirements of branch office deployments are very organization-specific. Aruba recommends that you turn on all the critical attacks that are defined in the lowest setting and then customize it to meet the needs of your network. If you turn on all the WIP features, too many alarms can interfere with the performance of your network and your neighboring WLANs. Consult an RF security expert and the Legal department to determine the security needs and legal implications, if any.

The example network uses the branch-wips profile. The branch-WIPS profile used for branch office deployment of the example network has the low setting for all the detection and protecting options, and it uses the default containment settings. The example network does not use WIPS for fixed-

telecommuter deployment. For details about the configuration of WIPS, see the *ArubaOS 6.1 User Guide* available on the Aruba support site.



Only rogues on legal channels are contained. TotalWatch detects and reports all the rogue APs, but action can be taken only against rogues that operate within the regulatory domain. Remember to consult with your legal team before enabling containment.

Sample Screenshots

- Security summary result in the absence of a rule for rule-based classification



Figure 100 Security summary in the absence of a rule

- Security summary result on the example network after defining a rule that classifies the ethersphere-wpa2 network as a neighbor

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan  [Logout admin](#)

Wizards > **Configure WIP**

Workflow  Help

1 Rogue Classification

2 WIP Policy

Define Rogue Classification Rules

You can optionally define Rogue Classification rules using the table below.

Rogue Classification Rules						
Rule name	# of Discovering APs	SNR(dB)	SSID	Classification	Confidence	Enabled
1	At Least 0	0 - 255	Is: ethersphere-wpa2	neighbor	5%	☒

[New](#) [Delete](#)

Figure 101 Defining a rule to identify neighbors

ARUBA MOILITY CONTROLLER | Monitoring > Security Summary

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan  Last updated: 10:02:45 am | [? | Logout admin](#)

Performance Usage **> Security** Potential Issues WLANs Access Points Clients

Discovered APs & Clients

AP Classification	Active APs	Associated Clients
Rogue	0	0
Suspected Rogue	7	0
Interfering	142	23
Neighbor	93	48
Valid	14	0
Manually Contained	0	0
Total	256	71

Events

		Last 4 hrs	Last 24 hrs	All
Containment	Infrastructure	8	8	42
	Client	0	0	1
	Total	8	8	43
Detection	Low	0	0	0
	Med	10	14	161
	High	0	0	87
	Total	10	14	248

Discovered Access Points: AP Classification = Neighbor, Active = Yes

BSSID	Band	PHY Type	SSID	Channel	Clients	AP Classification	Encryption	Marked to Contain
00:24:6c:06:37:a8	5 GHz	a-HT40	ethersphere-wpa2	149	0	Neighbor	WPA	No
00:24:6c:06:44:f0	2.4 GHz	g-HT	ethersphere-wpa2	1	0	Neighbor	WPA	No
00:24:6c:06:44:f8	5 GHz	a-HT40	ethersphere-wpa2	149	0	Neighbor	WPA	No
00:24:6c:06:4d:b0	2.4 GHz	g-HT	ethersphere-wpa2	1	0	Neighbor	WPA	No
00:24:6c:06:4d:b8	5 GHz	a-HT40	ethersphere-wpa2	149	1	Neighbor	WPA	No
00:24:6c:06:51:78	5 GHz	a	ethersphere-wpa2	149	0	Neighbor	WEP/WPA	No

Figure 102 Security summary after defining a rule to identify neighbors

- Applying the WIP policy to an AP group

Dashboard | Monitoring | **Configuration** | Diagnostics | Maintenance | Plan | [Logout admin](#)

Wizards > **Configure WIP**

Workflow | ? Help

- 1 Rogue Classification
- 2 WIP Policy**
- 3 Infrastructure
- 4 Intrusion Detection
- 5 Protection
- 6 Finish

Specify WIP Policy to Configure

Specify WIP policy to configure in this Wizard, and which AP Groups the policy is assigned to. [More...](#)

WIPS Policies	Policy branch-wips is assigned to these AP Groups
branch-wips	remote-AM
default	small-branch-office

New Clone Delete Add Remove

Back Next Cancel

Figure 103 Applying the branch-wips policy to AP groups

- In the IDS wizard, the valid SSIDs list is automatically populated with all unique SSIDs configured in SSID profiles and any unique cluster names configured in AP mesh cluster profiles. Only the SSIDs that are not present on the controller should be added.

Dashboard | Monitoring | **Configuration** | Diagnostics | Maintenance | Plan | [Logout admin](#)

Wizards > **Configure WIP**

Workflow | ? Help

- 1 Rogue Classification
- 2 WIP Policy
- 3 Infrastructure
- 4 Intrusion Detection**
- 5 Protection
- 6 Finish

Configure Intrusion Detection for Policy **branch-wips**

Use the sliders to set the desired level of intrusion detection, or click "Allow custom settings" to enable/disable specific detection features. NOTE: The higher the level of intrusion detection, the more alerts will be generated. [More...](#)

Intrusion Detection for Infrastructure: [Allow custom settings](#)

High
Medium
Low
Off

☒ Detect Adhoc Network Using Valid SSID

Add SSID Remove SSID

Intrusion Detection for Clients: [Allow custom settings](#)

Back Next Cancel

Figure 104 Adding a valid SSID for the Detect Adhoc Networks feature

The screenshot shows the Aruba Configuration Wizard for WIP Policy. The top navigation bar includes Dashboard, Monitoring, Configuration (selected), Diagnostics, Maintenance, and Plan. A 'Logout admin' link is in the top right. The left sidebar shows a workflow with five steps: 1. Rogue Classification, 2. WIP Policy, 3. Infrastructure, 4. Intrusion Detection, and 5. Protection (selected). The main content area is titled 'Configure Protection for Policy branch-wips'. It contains instructions: 'Use the sliders to set the desired level of infrastructure protection, or click "Allow custom settings" to enable/disable specific protection features. [More...](#)'. Under 'Protection for Infrastructure:', there is a slider set to 'Low' and a link to 'Allow custom settings'. A list of protection features is shown: 'Protect Misconfigured AP', 'Protect From Adhoc Networks', and 'Protect SSID' (checked). Below this list is an input field for an SSID, with 'Add SSID' and 'Remove' buttons. Under 'Protection for Clients:', there is a link to 'Allow custom settings'.

Figure 105 Adding a valid SSID for the SSID protection feature

Chapter 24: Spectrum Analysis

Wi-Fi operates in the unlicensed but regulated RF bands of the 2.4 and 5 GHz spectrums. These bands are unlicensed, so anyone can use them as long as they follow the rules and regulations of the unlicensed spectrum. So, the possible sources of interference are large. In most cases, the presence of an interfering device is the main reason for WLAN performance degradation. ArubaOS 6.1 offers spectrum analysis. Spectrum analysis is an RF troubleshooting tool that identifies, classifies, and finds sources of RF interference and provides a true visualization of the RF environment.

Spectrum analysis requires that you deploy APs as spectrum monitors (SMs). When in SM mode, an AP does not serve clients or take part in rogue AP containment. Instead, the AP samples the RF band and provides data to the mobility controller. On the WebUI of the mobility controller, a spectrum dashboard displays the data that is collected by the SM. The data is displayed as a series of graphs on a user-customizable dashboard. This data is streamed to the client and can be recorded for later analysis. For more details about the spectrum dashboard and the basics of spectrum analysis, see the [Aruba 802.11n Networks Validated Reference Design](#) and the [Managing and Optimizing RF Spectrum for Aruba WLANs Application Note](#).

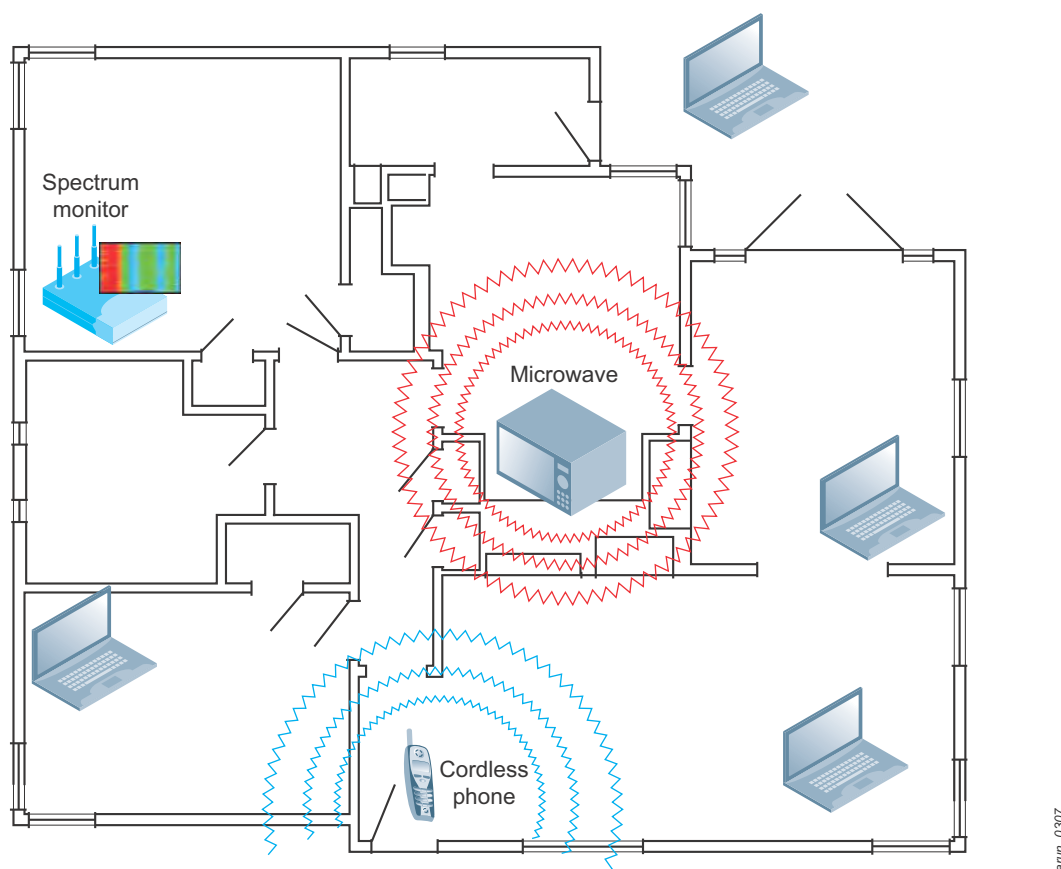


Figure 106 An active SM detects interference from non-Wi-Fi sources

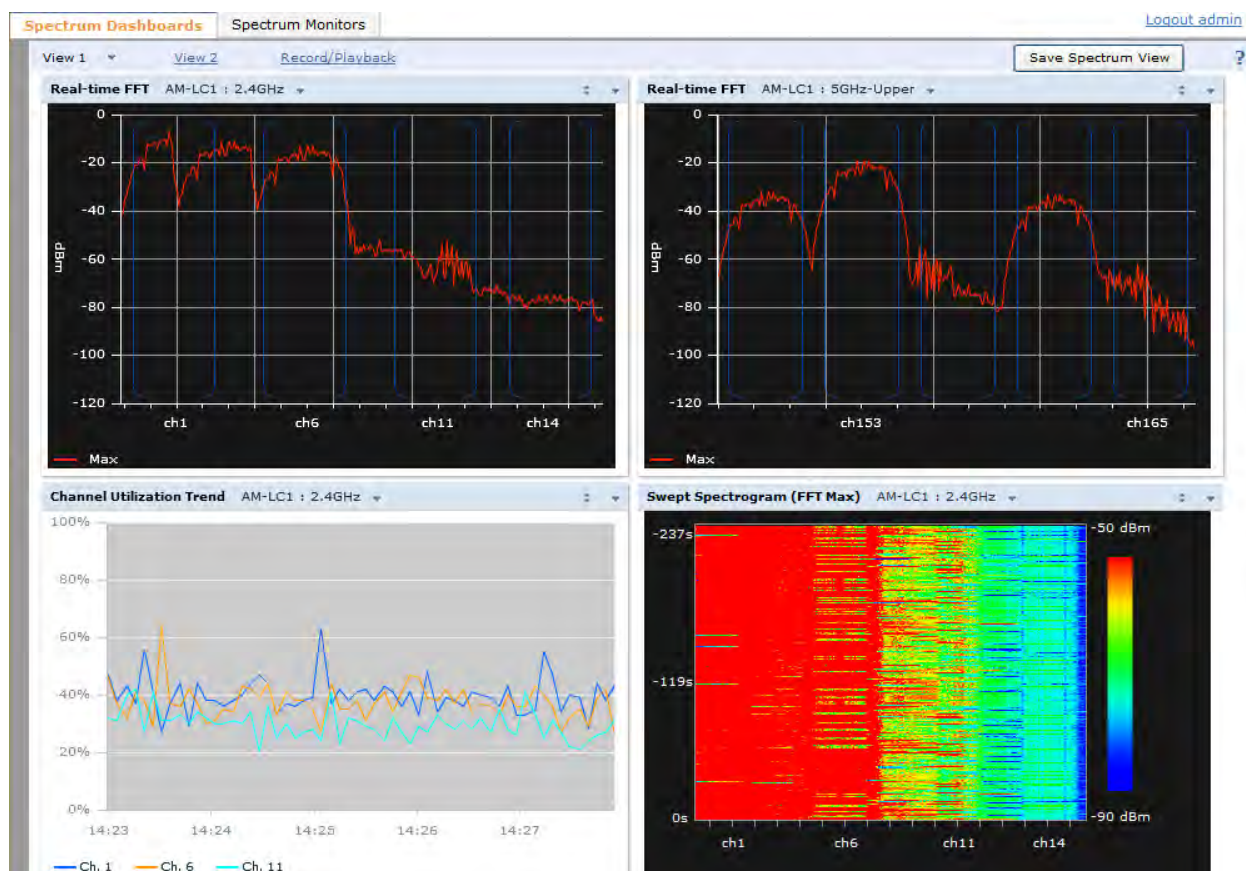


Figure 107 Sample spectrum dashboard

Spectrum analysis is not required for fixed telecommuter deployment, but some branch office deployments might require it. Most organizations use spectrum analysis only during troubleshooting, but some need spectrum analysis capabilities on a permanent basis. If you need spectrum analysis to be enabled always, deploy RAPs as dedicated SM at the remote site. In these situations, use a separate AP group with the 802.11a and 802.11g radio modes set to spectrum-mode.

When you use spectrum analysis on a temporary basis to troubleshoot client problems, you can convert a RAP or remote AM temporarily to an SM. You need not create a separate AP group or change the radio modes. Use the spectrum local override profile to convert an AP or AM into an SM. The AP functions as an SM until that AP is removed from the spectrum local override profile. When it is removed from that profile, the AP reverts back to its original configuration. The spectrum profile (used for dedicated SMs) and the spectrum local override profile also require that you specify the band to be scanned. A dual-radio AP can scan the 2.4 GHz band and one of the 5 GHz bands at the same time. However, a single-radio, dual-band AP can monitor only one band at a time.

When you change an AP radio to an SM using the local override profile, make this change through the WebUI or CLI of the controller that terminates the AP. In remote deployments, this controller is usually the master controller in the DMZ.



Remember that not all AP models are fully spectrum-capable. If full-spectrum analysis is required at remote sites, deploy spectrum-capable APs, such as AP-105, as dedicated AMs (use spectrum local override for SM capabilities) or dedicated SMs. When APs such as 105 and 9x series are deployed at remote sites, use preprovisioning. RAP-5WN and 12X series of APs have limited spectrum support. Graphs such as real time FFT, FFT duty cycle, swept spectrum, and interface source classification are not available on RAP-5WN and 12X series APs.

The example network uses spectrum analysis for temporary troubleshooting, so it uses the spectrum local override profile. In the example network, a remote AM is changed to an SM when the name of the remote AM (remote-AM-branch) is added to the spectrum local override profile on the rc1-sunnyvale-3600 controller. One radio on remote-AM-branch is set to monitor the 2.4 GHz band, and the other is set to monitor the 5 GHz upper band. When you remove remote-AM-branch from the spectrum-local override profile, it becomes an AM again.



When a client is subscribed to SM on the 2 GHz and 5 GHz bands, up to 45 Kb/s of additional WAN bandwidth is consumed, depending on the number of interferers in the environment. When no clients are subscribed, an SM just sends scanning updates to the controller, which requires less than 4 Kb/s of uplink bandwidth. Consider your WAN bandwidth availability and economics before turning on spectrum monitoring.

CLI Configuration

```
!  
ap spectrum local-override  
override ap-name remote-AM-branch spectrum-band 2ghz  
override ap-name remote-AM-branch spectrum-band 5ghz-upper  
!
```

WebUI Screenshot

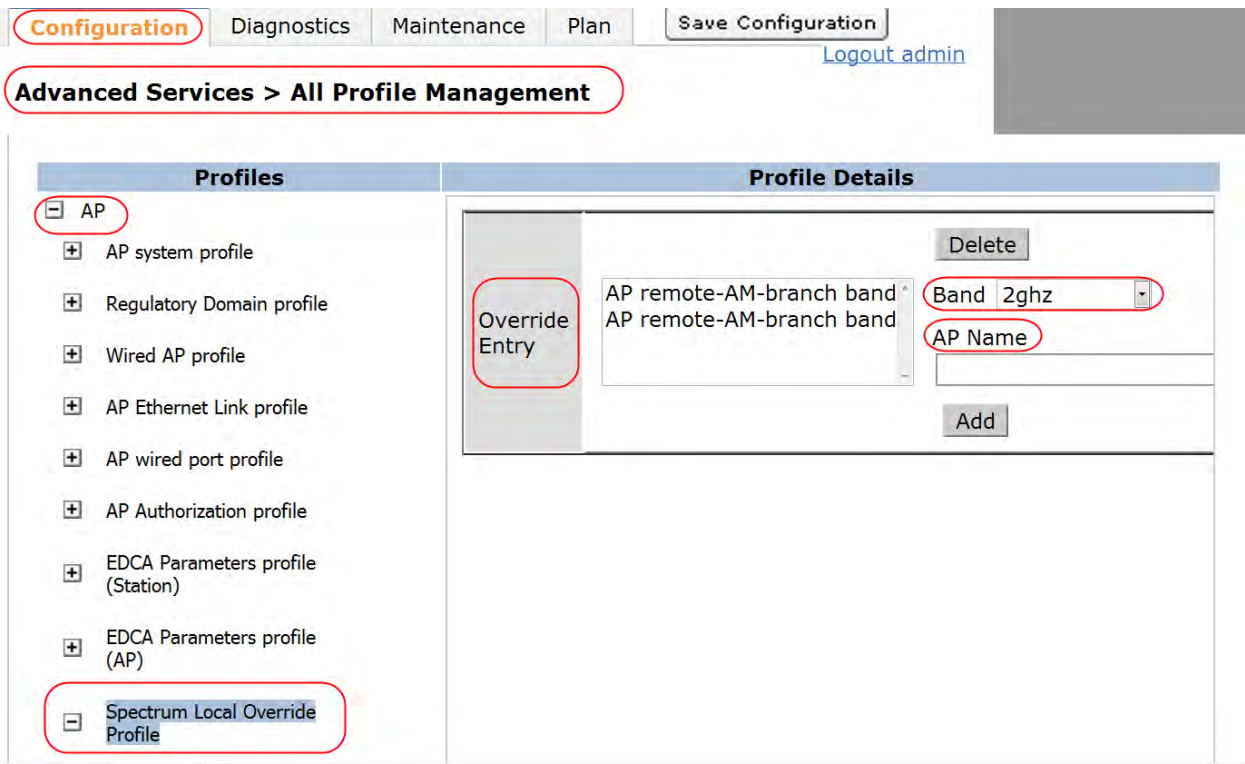


Figure 108 Spectrum local override profile

Chapter 25: RAP Provisioning

The RAPs can be provisioned using either preprovisioning or zero-touch provisioning. Not all APs support zero-touch provisioning. If you need zero-touch provisioning, choose the APs that support it. Aruba customers can adopt either of two provisioning methods as a best practice for remote network deployments. The choice depends on whether you want to allocate resources need for preprovisioning or whether the end user can or should be expected to perform certain simple tasks to activate an Aruba RAP.

Zero-Touch Provisioning

The Aruba RAP-5 and RAP-5WN include Trusted Platform Modules (TPM) that is preloaded with a unique security key at the factory. The RAP-2WG includes a security certificate that is stored in flash memory. All three of these RAP models also include a provisioning software image that includes the zero-touch feature. When combined with the controller that also includes a TPM and key, a low-cost provisioning model becomes possible. This model is particularly attractive for telecommuter deployments.

Aruba calls this zero-touch provisioning, which means that the IT organization simply preprograms the MAC address of each authorized RAP into a whitelist on the master controller and then ships the RAP to the end user. The IT professional can do this without having to plug the RAP into the controller, and the RAP remains in its packaging untouched. When the RAP arrives at the site, the end user simply enters the IP address or hostname of the controller into the provisioning screen on the RAP. The RAP automatically exchanges keys with the controller and completes the provisioning process with no further manual intervention. An optional one-time successful RADIUS authentication step may also be used for extra security. For configuring the optional one-time successful RADIUS authentication, see the *Aruba 6.1 user guide* available at the support site.

Zero-touch provisioning allows RAPs to be shipped directly to each site location, as opposed to being shipped first to a staging center. MAC address documentation and controller whitelist configuration can be performed when the APs arrive at the remote site. The customer avoids paying to ship and house the APs for the staging process.

IT Team Tasks for Zero-Touch Provisioning

The following tasks must be performed by the IT team for zero-touch provisioning:

1. Make a list of MAC addresses of the RAPs shipped to the remote sites.
2. Add the list to the RAP whitelist of the master controller in the DMZ and assign the appropriate AP groups, USB, and PPPoE settings for each RAP.



The RAP whitelist on a controller supports a maximum of 4096 entries.

CLI

```

!
local-userdb-ap add mac-address 00:0b:86:66:12:c1 ap-group micro-branch-office ap-name RAP-branch1 full-name branch1
!

```

WebUI Screenshot

The screenshot shows the Aruba Mobility Controller web interface. The breadcrumb navigation path is **Wireless > AP Installation > RAP Whitelist**, which is highlighted with a red box. Below this, there are tabs for Provisioning, Provisioning Profile, RAP Whitelist (selected), and Campus AP Whitelist. A search bar is present above a table. The table lists two entries:

	AP MAC Address	User Name	AP Group	AP Name	Description	Revoked	IP-Address
☐	00:0b:86:66:12:c1	branch 1	small-branch-office	RAP-branch1			0.0.0.0
☐	00:0b:86:66:7a:d1	telecommuter 1	telecommuter	RAP-telecommuter 1			0.0.0.0

A 'New' button is located at the bottom left of the table.

Figure 109 Adding RAPs to the RAP whitelist

Onsite Tasks for Zero-Touch Provisioning

The following simple tasks must be performed on site for zero-touch provisioning:

1. Connect Eth 0 of the RAP to the uplink. Connect a desktop or laptop to any other Ethernet port on the RAP. The PC receives an IP address from the RAP internal DHCP server.
2. Open a web browser and navigate to any URL. The browser is redirected automatically to an Aruba management web page inside the AP that requests the IP address or FQDN of the master controller in the DMZ.
3. Enter the hostname or IP address provided in the installation documentation. The RAP connects to the master controller. Then the following events occur:
 - The master controller verifies that the RAP appears in a whitelist, and to what AP group the device belongs.
 - If authenticated, the RAP updates its software image, if necessary, and downloads its configuration.
4. The RAP reboots and begins offering the expected services over the air and on secure wired ports. For detailed information about the bootstrapping process, see [RAP Bootstrapping on page 37](#).

WebUI Screenshot



Remote Access Point Provisioning
Copyright (c) 2002-2011, Aruba Networks, Inc.

Device	RAP-2WG	Uplink	
Type	RAP-2WG	Interface	Port 0
Wired MAC address	00:0B:86:C3:73:23	Link Status	UP
Serial #	AH0006791	IP address	192.168.171.70
Software Version	ArubaOS Version 6.1.0.0 Build# 28106	Port speed	100Mb/s

Remote Access Point Setup

Enter the IP address or hostname of the Aruba Master Controller for this Remote Access Point:

[Hide Advanced Settings](#)

Static IP

PPPoE

IP Address:

Netmask:

Gateway:

Primary DNS:

Domain:

Save

Clear

Continue

Figure 110 RAP-2 console



Remote Access Point Provisioning
Copyright (c) 2002-2011, Aruba Networks, Inc.

Device	RAP-3WG	Uplink	
Type	RAP-3WG	Interface	Port 0
Wired MAC address	00:0B:86:65:8A:2B	Link Status	UP
Serial #	AG0007133	IP address	192.168.171.99
Software Version	ArubaOS Version 3.0.4.2 Build# 38773	Port speed	1000Mb/s

Remote Access Point Setup

Enter the IP address or hostname of the Aruba Master Controller for this Remote Access Point:

[Hide Advanced Settings](#)

Static IP

PPPoE

USB

Device: Other (Any)

Device: any

Type:

Initialization String:

PPP Username:

PPP Password:

TTY Device Path:

Device Identifier:

Dial String:

Modeswitch:

Link Priority Cellular:

Link Priority Ethernet:

Save

Clear

Continue

Figure 111 RAP-5 console

Preprovisioning

APs such as the 105, 13X, and 12X series have a factory installed certificate, but they do not have provisioning image. To provision these APs using certificates and RAP whitelist, you must console into the AP. An alternate for APs that do not have a provisioning image or factory certificates is preprovisioning. Aruba recommends preprovisioning for APs without the preloaded provisioning image.



APs without factory certificate can be preprovisioned only.

IT Team Tasks for Preprovisioning

The following tasks must be performed by the IT team for preprovisioning.

1. Select a staging center and ensure that the staging center has secure Layer 2 connectivity to the DMZ controller.
2. Connect the AP to the DMZ controller through the LAN network. If ADP is used, ensure that no other controllers are between the RAPs and the DMZ controller.
3. After the RAP comes up on the controller, assign the unit to the proper AP group and choose an authentication method. PSKs and certificates are supported. If certificates are used, add the RAP to the RAP whitelist. Aruba supports bulk provisioning of large numbers of RAPs at the same time. After provisioning is complete, the RAP can be disconnected and prepared for shipment.



Ensure that the user name and password that are used during the RAP provision (used for preprovisioning with PSK) are added to the authentication server that is used in the default-rap VPN authentication profile.

WebUI Screenshot

MOBILITY CONTROLLER | rc1-sunnyvale-3600

Configuration | Diagnostics | Maintenance | Plan | Save Configuration

Wireless > AP Installation > Provision

Provisioning | Provisioning Profile | RAP Whitelist | Campus AP Whitelist

AP Parameters

AP Group: small-branch-office

AP Installation Mode

Default | Indoor | Outdoor

Antenna Parameters

Antenna Selection: Internal/Included Antenna | External Antenna

Authentication Method

Remote AP: Yes | No

Remote AP Authentication Method: Pre-shared Key | Certificate

IKE PSK: [] Confirm IKE PSK: []

User credential assignment

Use Automatic Generation | Global User Name/Password per AP User Name/Password

User Name: [] Password: [] Generate Confirm Password: []

PPPoE Parameters

Service Name: [] User Name: [] Password: [] CHAP Secret: [] Confirm Password: [] Confirm CHAP Secret: []

Master Discovery

Use AP Discovery Protocol: []

Host Controller IP Address: [] Master Controller IP Address/DNS name: []

Host Controller Name: branch.rde.arubanetwor Master Controller IP Address/DNS name: []

IP Settings

Uplink Vlan: 0

Obtain IP Address Using DHCP: []

Use the following IP Address

IP Address: [] Subnet Mask: []

Gateway IP Address: []

DNS IP Address: [] Domain Name: []

IPv6 Address/Prefix-length: []

Gateway IPv6 Address: []

DNS IPv6 Address: []

FQLN Mapper

Remove FQLN: []

Campus: N/A Building: N/A Floor: []

USB Settings

USB Parameters: []

Device: Mercury Sierra Compass 885 (ATT) TTY Device Data Path: ttyUS

Path: [] Initialization String: []

Device Identifier: [] Device Type: sierra

Dial String: [] PPP Username: []

PPP Password: [] Confirm PPP Password: []

Link Priority: 0 Link Priority Cellular: 0

AP List

AP IP Address	AP Name	AP Group	SNMP System Location	Mesh Role	AP
10.169.138.52	RAP-branch1	small-branch-office	[]	none	RAP-

Apply

Figure 112 Preprovisioning

Onsite Tasks for Preprovisioning

At the remote site, connect the RAP to the WAN service provider customer-premises equipment (CPE) device using the Eth0 uplink port. If 3G wireless is being used, plug in the 3G modem into the USB port on the RAP.

Onsite RAP Deployment

Figure 113 shows the recommended RAP deployment model at remote sites.

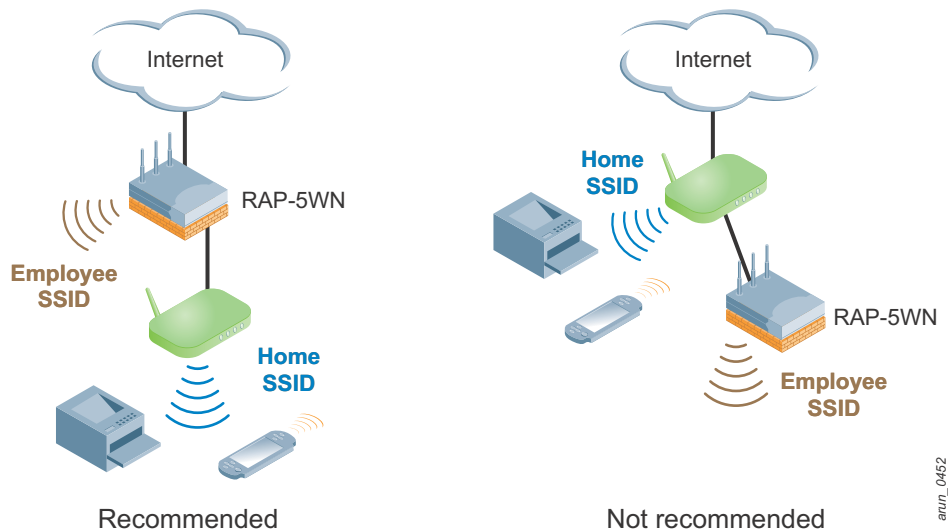


Figure 113 Recommended onsite RAP deployment

To reap the benefits of the traffic classification features on a RAP, Aruba recommends that you connect the RAP directly to the WAN uplink and not to a home router. Most home routers are not capable of QoS and traffic classification. When the RAP is deployed behind a home router, the home router does not honor RAP traffic classification, which affects the performance of latency-sensitive applications. Connect the RAP directly to the WAN uplink to ensure that the user traffic entering the WAN network is prioritized appropriately. To provide the best end user experience, the IT team must educate the employees about the recommended onsite deployment model.

Chapter 26: Wide-Area Network Considerations

The speed and latency of the connection between the RAP and the controller have a significant impact on the applications that can be supported on the RAP. Typical fixed telecommuter applications include office productivity suites, VoIP, and video conferencing. Branch offices, in addition, may utilize remote server or batch upload applications. In addition to the user data traffic, the RAPs may require up to 64 Kb/s or more for all the control traffic, depending on various factors such as ARM scanning, number of SSIDs, forwarding modes, and active spectrum analysis clients. Based on the data usage, Aruba recommends a broadband connection of 1 Mb/s or higher with latency of 100 ms or less. Remember, that a RAP control channel consumes more bandwidth during image and configuration download than during regular operation.

Bandwidth Constraints

Specific design guidelines and controller configurations are needed to maximize performance for low-speed links such as ISDN, fractional T1/E1, and many Frame Relay WAN connections. RAPs and controllers transmit heartbeat or keepalive packets between themselves to achieve high reliability and fast failover in the event of a network or controller outage. Depending on the forwarding modes in use, failure to receive these heartbeat packets can cause RAPs to rebootstrap and reestablish tunnels with the controllers. During the bootstrap process, the AP shuts off all radios for approximately 20 ms, and all clients must reassociate. If a low-speed link is saturated, heartbeat packets can be dropped, which causes the RAP to rebootstrap. This activity is the primary cause of connectivity problems for APs connected across low-speed links.

There are no hard rules to categorize what works and does not work. A number of Aruba customers have deployed RAPs across 256 Kb/s WAN links without difficulty, because packet loss is low and the throughput requirements are not high. Other customers with unpredictable traffic loads have experienced some problems due to RAP heartbeat timeouts. Customers with a low-speed link requirement must analyze and test realistic traffic patterns before deployment to minimize risk of link saturation.

Latency Constraints

When you deploy RAPs across high-latency links of 100 ms or greater, special considerations are needed to cope with the timing constraints of some client devices. Certain wireless clients are known to have very tight timing requirements that cause the association process to time out if an association response is not received within 100 ms. Check with your device vendor for the latest versions of firmware and drivers that are designed to be less sensitive to WAN latency. Aruba recommends that customers who need tunnel forwarding mode should test high-latency links to confirm that timing issues will not become a problem. The split-tunnel and bridge forwarding modes help to reduce or eliminate certain WAN traffic and delays.

3G Wireless Constraints

The minimum signal level that must be received by the handset for it to “see” the primary common pilot channel (CPICH) within a coverage area is a function of multiple factors including:

- the transmitter power of the base station
- the receiver sensitivity of the 3G modem
- the separation distance between the 3G modem and the base station
- carrier frequencies
- antenna heights of the base station
- terrain features such as buildings, tall structures, trees, lakes, and other bodies of water
- the width of the streets traversed by the 3G modem
- the angle at which the signal is incident at the receiving antenna

Typically, 3G service providers engineer their networks so that across the entire stated coverage area to a better-than-99% probability, a 3G modem will “see” the signal when the receiver sensitivity of the 3G modem is < -90 dBm. Many 3G modems have indicators of signal strength, usually colored bars that provide information about the 3G signal detected by the modem receiver. In environments where signal strength is insufficient for the modem receiver to detect (absence of bars or other signal strength indicators) or to lock onto (blinking bars or other indicators) for sustained transmission and reception, reception can be increased by using external antennas. These antennas are typically neither tested nor endorsed by the 3G modem vendors or the 3G service providers, but are available as after-market accessories.

Recommendations for Minimizing Constraints

Aruba recommends the following best practices when deploying RAPs across low-speed or high-latency links:

- Adjust the RAP bootstrap-threshold if the network experiences packet loss. The RAP will recover more slowly in the event of a failure, but it will be more tolerant to loss of heartbeat packets. The default (recommended) bootstrap-threshold for RAPs is 30. Increase the bootstrap threshold to a higher value than 30 (60 max). At this point, Aruba recommends that you upgrade the WAN link.



Even if the bootstrap threshold parameter in the AP system profile is set to a low value, the default minimum bootstrap-threshold value for RAPs is 30. The bootstrap-threshold for CAPs can be set to a minimum of 1. The default (recommended) bootstrap-threshold value for CAPs is 8.

- Limit the number of tunnel mode SSIDs to reduce the amount of traffic being tunneled back to the controller. In split-tunnel mode, only the traffic that is destined to the corporate network is tunneled back.
- For 3G modem locations, Aruba recommends that you complete a 3G wireless site survey prior to deployment. Simply plug the same USB modem into a laptop at each location and verify that the signal strength meets minimum requirements. Make sure that all client devices install the

most current firmware and driver updates from device manufacturers to reduce the sensitivity to link latency.

- Before subscribing to 3G service or DSL service that have data usage limits, calculate your data requirements (RAP control traffic + data usage) and subscribe to the appropriate package to avoid any overuse penalties.
- If high-latency causes association issues with certain handheld devices or barcode scanners, check with device manufacturer for recent firmware and driver updates.

Chapter 27: Logging

Almost all network deployments use syslog servers. A syslog server is the central repository for all the event notification messages that various network devices generate. This information is useful for troubleshooting network problems and mitigating security threats. The Aruba controller can use any of the Local Facility (0-7) to send the syslog messages. The logging level determines how often and how many notifications are sent to the syslog server. Logging all the notification messages can overwhelm the logs and may make debugging difficult. Logging all the messages also increases the traffic on the wired network. Consider these factors before you decide on the logging level. Configure syslog settings on all the controllers from which you need logs.

The example network uses the default logging level of warnings. The warnings level forwards all warning notifications to the syslog server.



To view logs on the controller, the appropriate logging level should be chosen and enabled.

CLI Configuration

```
!  
logging level warnings network subcat all  
logging level warnings security subcat all  
logging level warnings system subcat all  
logging level warnings user subcat all  
logging level warnings wireless subcat all  
logging facility local7  
logging 10.169.130.5 severity warnings  
!
```


WebUI Screenshot

Dashboard

Monitoring

Configuration

Diagnostics

Maintenance

Plan

Save Configuration

Logout admin

WIZARDS

AP Wizard

Controller Wizard

WLAN/LAN Wizard

License Wizard

WIP Wizard

NETWORK

Controller

VLANs

Ports

Cellular Profile

IP

SECURITY

Authentication

Access Control

WIRELESS

AP Configuration

AP Installation

MANAGEMENT

General

Administration

Certificates

SNMP

Logging

Management > Logging Servers

Servers

Levels

Logging Facility

Logging Facility

local1

Logging Servers

IP Address	Category	Logging Facility	Severity	Actions
10.169.130.5	All	local7	warnings	Edit Delete
New				

Apply

Operation Performed Successfully

Commands

View Commands

Figure 114 Sample logging

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan [Save Configuration](#)

WIZARDS
 AP Wizard
 Controller Wizard
 WLAN/LAN Wizard
 License Wizard
 WIP Wizard

NETWORK
 Controller
 VLANs
 Ports
 Cellular Profile
 IP

SECURITY
 Authentication
 Access Control

WIRELESS
 AP Configuration
 AP Installation

MANAGEMENT
 General
 Administration
 Certificates
 SNMP
> Logging
 Clock
 Guest Provisioning
 Captive Portal
 SMTP
 Bandwidth Calculator

ADVANCED SERVICES
 Redundancy
 IP Mobility
 Stateful Firewall
 External Services
 VPN Services
 Wired Access
 Wireless
 All Profiles

Management > Logging Levels

Servers **Levels**

Select All	Category/SubCategory	Logging Level
☒	Network logs	warnings
☒	all	N/A
☐	packet-dump	N/A
☐	mobility	N/A
☐	dhcp	N/A
☒	System logs	warnings
☐	all	N/A
☐	configuration	N/A
☐	messages	N/A
☐	snmp	N/A
☐	webserver	N/A
☐	ap	N/A
☐	Security logs	debugging
☐	all	N/A
☐	aaa	N/A
☐	firewall	N/A
☐	packet-trace	N/A
☐	mobility	N/A
☐	vpn	debugging
☐	dot1x	N/A
☐	ike	debugging
☐	webserver	N/A
☐	ntlm	N/A
☐	kerberos	N/A
☐	ids	warnings
☐	ids-ap	warnings
☐	cpsec	N/A
☐	db	N/A
☒	Wireless logs	warnings
☐	all	N/A
☒	User logs	debugging
☐	all	debugging
☐	captive-portal	N/A
☐		N/A
☐		N/A
☐		N/A
☐		N/A
☐		N/A

Alerts
 Critical
 Debugging
 Emergencies
 Errors
 Informational
 N/A
 Notifications
Warnings

Logging Level N/A **Done** **Cancel**

Figure 115 Logging Levels

Chapter 28: AirWave

As the remote network grows beyond a single pair of redundant master controller, Aruba recommends that you use AirWave. When the WLAN management system (WMS) is offloaded from the controller to the AirWave, configuration and monitoring can be done from a central point. To simplify the job of the network administrator, use the AirWave system any time more than one pair of redundant master controllers exists in the network. The AirWave system provides a consolidated view of all components and users on the network in a single, flexible console. AirWave provides network-wide configuration, advanced reporting, and trending features, which allow network administrators to interface with a single tool to plan, configure, and troubleshoot the network.

For organizations that have campus and remote network deployments, AirWave becomes even more important. AirWave provides centralized configuration management and allows network administrators to track client devices, identify rogue devices, plan new deployments, and visualize RF coverage patterns with an intuitive and seamless user interface. For more details about AirWave and how to set it up, see the *AirWave User Guide* available at the Aruba support site.

AirWave monitors Aruba devices using SNMP polling. The SNMP agent of the Aruba controllers must be set up to respond to these SNMP polls and send SNMP traps to AirWave. AirWave also requires Telnet or SSH credentials and the enable password to acquire license and serial information from controllers. Configure the SNMP settings on all the controllers that must be monitored by AirWave.



The community string on the Aruba controllers must match that on AirWave.

CLI Configuration

```
!  
snmp-server community public  
snmp-server enable trap  
snmp-server host 10.169.130.2 version 2c public udp-port 162  
!
```

WebUI Screenshot

MOBILITY CONTROLLER | rc1-sunnyvale-3600

toring **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Logout adm](#)

Management > SNMP

System Group

Host Name: rc1-sunnyvale-3600

System Contact: James

System Location: DMZ

Read Community Strings: public [Add](#) [Delete](#)

Enable Trap Generation: ☒

Trap Receivers

IP Address	SNMP Version	SECURITY NAME	UDP Port	Type	Retry	Timeout	Action
10.169.130.2	SNMPv2c	public	162	Trap	N/A	N/A	Delete

[Add](#)

SNMPV3 Users

User	Authentication Protocol	Privacy Protocol	Type	Action
Add				

[Apply](#)

Commands [View Commands](#)

Figure 116 Sample SNMP configuration

WMS Offload

The simplest way to configure WMS offload on master controllers is through AirWave. In this method, the WMS offload configuration resides in the AirWave. No special configuration is needed on the master controller to offload the WMS database. When WMS offload is enabled on AirWave, a set of commands are pushed via SSH to all Aruba Master Controllers to offload WMS. AirWave creates a new SNMPv3 user on the controllers. AirWave must have read/write access to the controllers to push these commands.

Another method for configuring WMS offload involves these two steps:

- Enable WMS and create a SNMPv3 user on the master controller through the CLI.
- Add the SNMPv3 user and the related master controller information to the AirWave.

For details on these WMS offload methods, see the *AirWave User Guide* and *AirWave and Aruba Best Practices Guide*.

Chapter 29: ClearPass Guest

Increasingly, visitors require online access to perform their work, and visitor management has become a standard requirement for most networks. On large remote networks deployments with hundreds of visitor each day, managing guest accounts is an unnecessary overhead for IT. To reduce the complexity and operational cost of visitor management, use the ClearPass Guest solution. ClearPass Guest is a unified visitor management solution with a fully functional RADIUS server and external captive portal support. The ClearPass Guest solution provides the most intuitive and flexible way to manage external visitors to an Aruba wireless network. ClearPass Guest directly links the guest accounts to security policies configured on the Aruba controller. ClearPass Guest ensures that network administrators control the underlying security policy related to guest network access, but nontechnical staff can easily and securely manage the day-to-day administration of guest accounts. If required, ClearPass Guest can also be configured to provide self-registration for guests and employee mobile devices. ClearPass Guest also offers fully customizable captive portal pages and powerful logging and reporting capabilities. For more information on the special features and deployment scenarios of ClearPass Guest, see the *ClearPass Guest deployment guide* available at the Aruba support site.

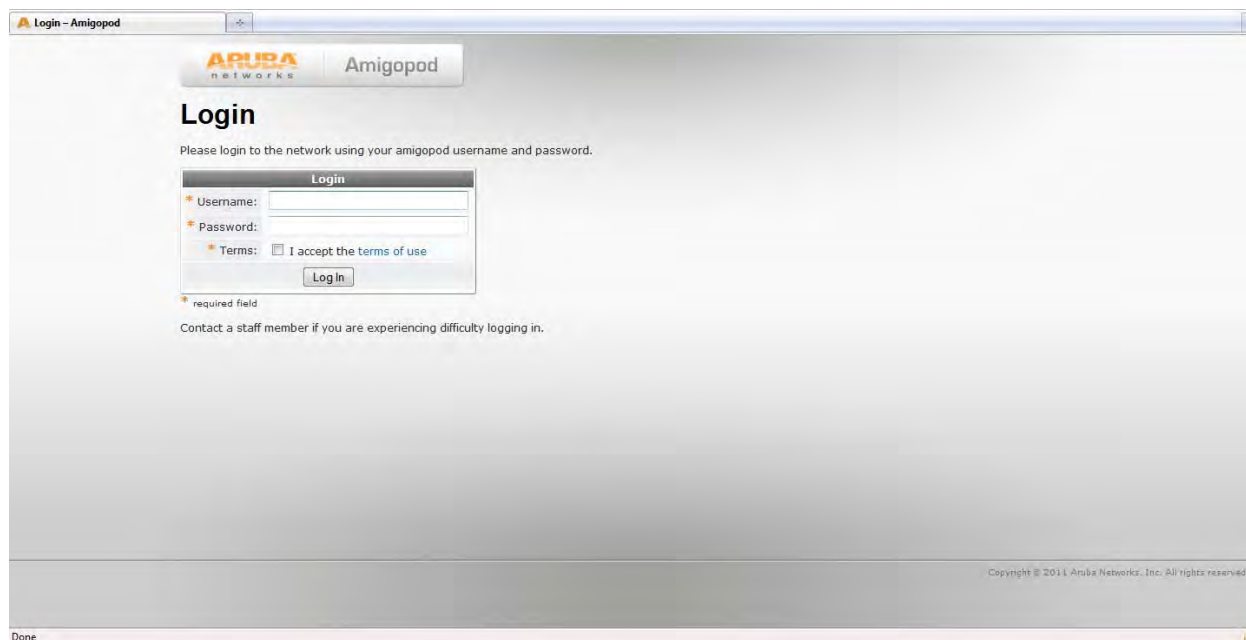


Figure 117 **Default ClearPass Guest login page (customizable)**

Appendix A: Regulatory Compliance

Regulatory Compliance for International Deployments

AP radios must meet government regulatory compliance requirements in the countries where they are installed. The geographical areas of the world for regulatory compliance purposes are broken down as follows:

- USA
- Israel
- Rest of World (ROW)

This section provides guidance on how to design international fixed telecommuter and micro-branch-office solutions. In addition, certain Aruba controller models are prohibited from being shipped to or operated in other countries.

AP Compliance

RAPs must be assigned proper country codes to comply with local regulatory requirements. AP radios must comply with specific limits on channel use and transmit power established by regulatory bodies in the countries where they are installed.

This requirement is accomplished through the AP Group feature. Each Aruba RAP is assigned to one AP group. The AP group is assigned a country code, which determines the regulatory rules applied to the AP radio, including the 802.11 wireless transmission spectrum. Most countries impose penalties and sanctions for operators of wireless networks with devices set to improper transmission spectrums.

Aruba uses Software Defined Radio (SDR) technology so that any of its APs can be used in any country that has granted approval. Aruba RAPs are approved for operations in more than 100 countries. There is no need to keep different AP models for different countries because the country code can be changed as needed and is enforced by the Aruba controller.



Note that the RAP-5, RAP-5WN, and RAP-2WG can be ordered as US and ROW (Rest of World) models based on local electrical requirements. This is not related to radio regulatory compliance, which is managed at the controller.

Controller Compliance

When ordering an Aruba controller, customers specify a geographic region: United States, Israel, or ROW. Aruba controllers sold in the United States or Israel are physically restricted from managing RAPs in other regulatory domains. Administrators cannot assign another regulatory domain to the RAPs that terminate at these controllers. However, a ROW controller can properly manage RAPs from any unrestricted country and enforce the correct regulatory radio rules.

For example, a US-based controller may not terminate or manage RAPs based in Canada or Mexico, nor can it failover using Virtual Router Redundancy Protocol (VRRP) to a non-US controller. But a ROW controller may failover to an identically configured ROW controller for redundancy purposes.

A single Aruba ROW controller can manage RAPs in France, Germany, Italy, and Spain as long as the APs in each country are properly assigned to separate AP groups. Each AP group must be assigned an RF management profile with the appropriate regulatory domain profile. The regulatory domain profile must define the correct country code corresponding to the physical location of the APs.

Recommendations for International Deployments

Use this checklist to verify that your Aruba design complies with the host country laws and regulations:

1. Review all controllers that participate in VRRP clusters to confirm that all models have identical country SKUs.
2. Review all RAPs that terminate on US-based controllers and make sure that they are all in the US.
3. Review all RAPs that terminate on Israel-based controllers and verify that they are all in Israel.
4. Make lists of all RAPs by country to create Regulatory Domain profiles.
5. Purchase any additional controllers necessary to achieve regulatory compliance.

Appendix B: RAP Control Traffic

Table 51 summarizes the approximate control traffic generated by the RAP depending on factors such as number of SSIDs, forwarding modes, ARM, and spectrum.

Table 51 RAP Control Traffic

Modes of Operation	Bandwidth Requirement (Kb/s) (ArubaOS 6.0 and later)
Radio OFF (heartbeat traffic)	3
AM-mode	5
Spectrum mode	9
Spectrum mode with two active spectrum analysis clients (clean environment)	20
Spectrum mode with two active spectrum analysis clients (high interference environment)	45
1 tunnel/split-tunnel SSID - no scanning	3.2
1 tunnel/split-tunnel SSID - scanning	3.3
3 tunnel/split-tunnel I SSID - no scanning	3.5
3 tunnel SSIDs/split-tunnel - scanning	3.7
3 bridge SSID - no scanning	2.8
3 bridge SSID - scanning	3.1

Appendix C: Geographical Redundancy for RAP Deployments

Today, most organizations have a distributed workforce with several satellite offices and remote workers. So, it is more important to ensure that a natural disaster or calamity in one region does not affect the everyday productivity of the employees in other regions. To ensure redundancy and high availability of resources, some organizations deploy geographically separate data centers to provide redundancy. Like the geographically redundant web and DNS services, the Aruba RAP solution can also be configured to provide geographical redundancy. When you deploy redundant controllers in geographically redundant data centers, the RAPs always have a backup controller if the primary data center is affected by catastrophic events.

As discussed earlier, redundancy using VRRP requires Layer 2 connectivity between the redundant controllers. Layer 2 connectivity is not guaranteed in case of geographically redundant data centers, so Aruba recommends the use of LMS and backup LMS configuration to provide geographical redundancy. In LMS and backup LMS deployments, the RAPs are configured with two controllers. The LMS IP address that is specified in the AP system profile represents the primary controller of the RAPs, and the backup LMS IP address in the AP system profile represents the backup controller. If the primary controller becomes unreachable, the RAPs will try connecting to the backup controller specified by the backup LMS IP address. A controller is considered unreachable if the number of heartbeats missed by a RAP exceeds the bootstrap threshold defined in the AP system profile. The LMS and backup LMS controllers should be configured individually because they do not sync configuration or database. Remember that AirWave can be used as a central point of configuration for all the controllers.



In RAP deployments, the IP addresses of the LMS and backup LMS should belong to the public IP address space. If the primary and backup controllers are unreachable, the RAP tries to reestablish the IPsec connection. The number of IPsec retries before a RAP reboots is specified by the “number of IPsec retries” parameter of the AP system profile (default value is 360). When the “number of IPsec retries” value is exceeded, the RAP reboots and tries to connect to the FQDN or IP address of the master controller specified in the RAP console page during the zero-touch provisioning.

Geographical Redundancy Design

The most important thing to remember when you design geographical redundancy is regulatory compliance. Network administrators should ensure that all the APs and controllers meet the necessary regulatory compliances discussed in [Appendix A: Regulatory Compliance](#). It is simple to provide geographical redundancy for RAP deployments that are contained to a single LMS and backup LMS controller pair. In these deployments, the network administrators can assign the RAPs to an AP group that defines one controller as LMS and the other as the backup LMS controller. The key requirements that should be considered in these deployments are these:

- The AP radios should comply with appropriate local regulatory domain. Based on the location of a RAP, it should be assigned an AP group with the appropriate regulatory domain profile. For information on AP compliance, see [Appendix A: Regulatory Compliance](#).

- The controller should comply with the regulatory requirements. Based on the geographical location of the deployments, controllers with the appropriate country code should be used to terminate the RAPs. A controller with country code United States (US) cannot terminate RAPs from rest of the world. For information on controller compliance, see [Appendix A: Regulatory Compliance](#).
- The backup LMS controller should belong to the same country code as the LMS controller. For example, a ROW controller cannot be used as a backup LMS controller if the LMS controller and RAPs are in the US. However, a ROW controller in London can be used as a backup LMS controller for the RAPs in India as long as the RAPs are assigned an AP group with appropriate local regulatory domain settings.
- The RAP whitelist should be imported manually to the LMS and backup LMS controllers because the whitelist is not shared between them.

For recommendations on AP group configurations on the LMS and backup LMS controllers, see [Recommendations for Geographical Redundancy](#) on page 198.

[Figure 118](#) and [Figure 119](#) are examples of geographically redundant LMS and backup LMS controllers that meet the required controller and AP compliance.

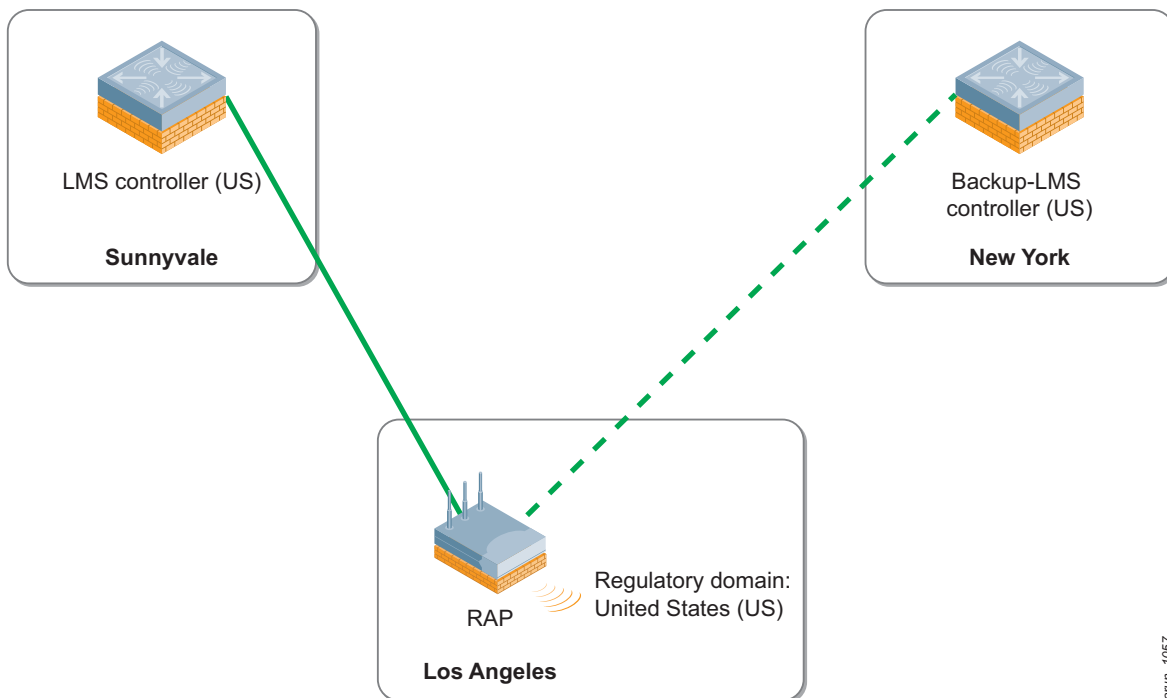


Figure 118 **Geographical redundancy - US**

arun_1057

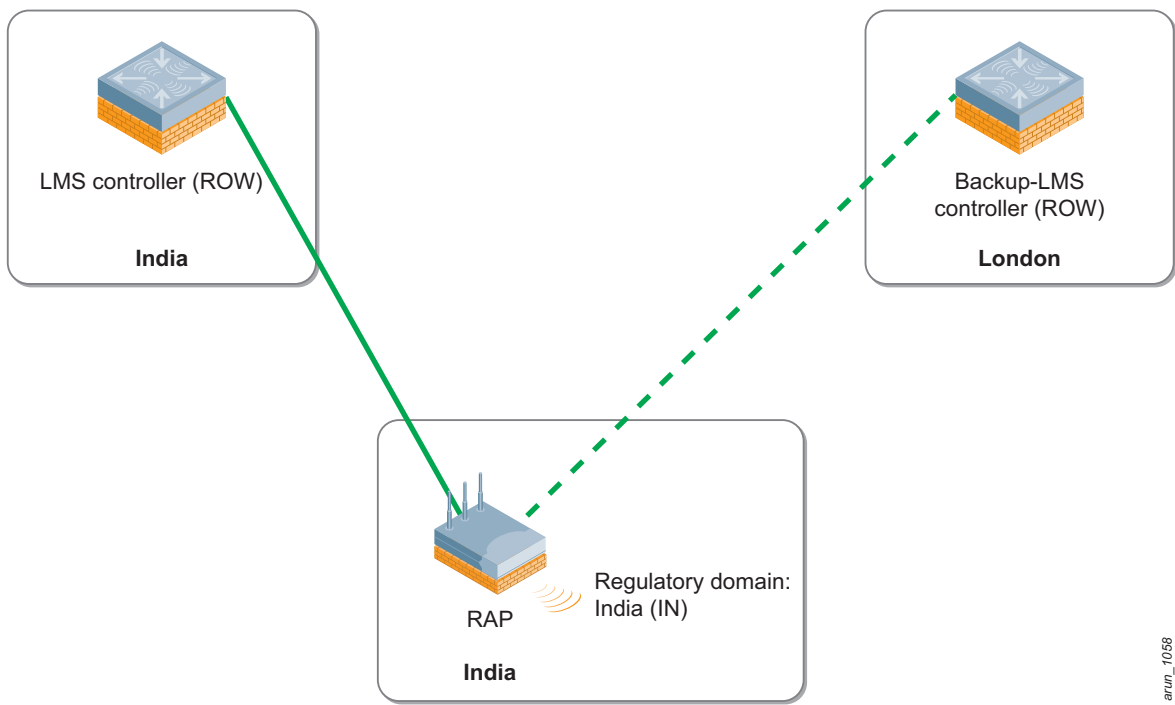


Figure 119 Geographical redundancy - ROW

Figure 120 shows a geographically redundant LMS and backup LMS deployment that fails the required controller compliance.

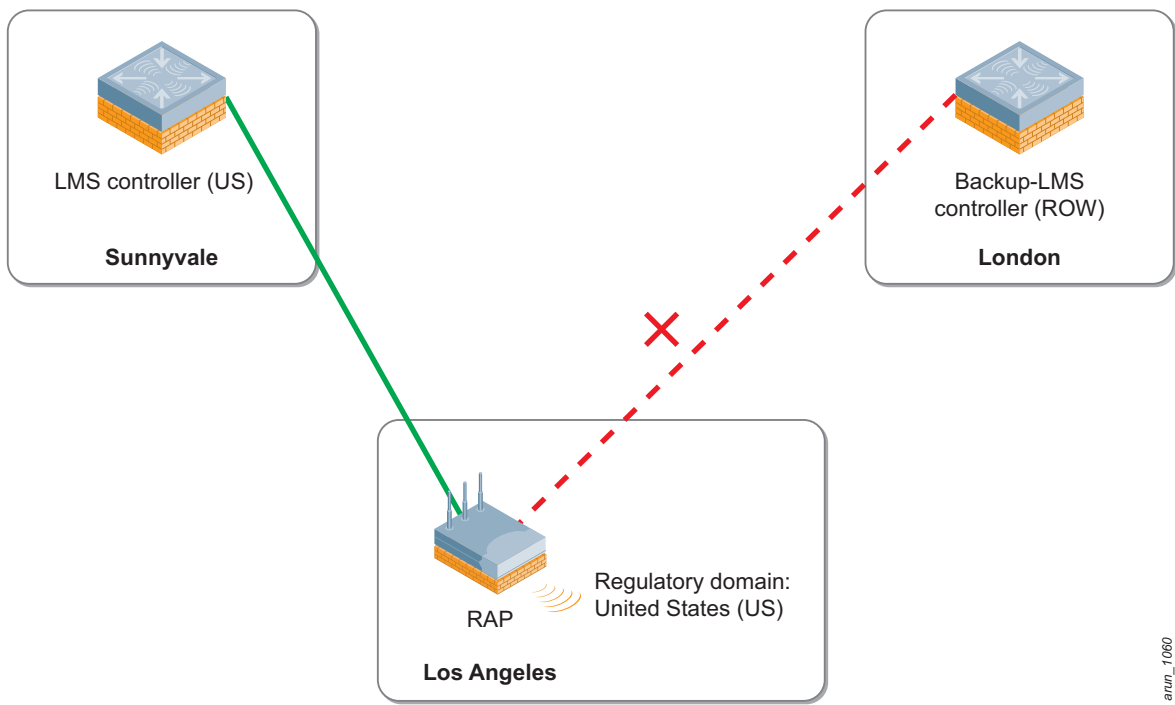


Figure 120 Controller compliance failure

Geographical Redundancy for Global RAP Deployments

Certain RAP deployments, especially those of large multi-national organizations, span the entire globe. To provide geographical redundancy for such global RAP deployments, you must plan properly in terms of DNS and regulatory compliance of controllers and RAPs.

DNS Design for Geographical Redundancy

Intelligent planning of DNS is important to ensure that RAPs connect to the appropriate controller, based on their physical location, and comply with all the regulatory requirements. Whenever a RAP is rebooted, the RAP sends a DNS query for the FQDN that is entered in the RAP console page during zero-touch provisioning (or the FQDN used during preprovisioning). When this DNS query is received, the corporate DNS server should be able to intelligently predict the physical location of the RAP and redirect it to an appropriate controller that meets all the controller compliance requirements. For example, the DNS server should not respond with the IP address of the controller in London if the query originated from a RAP in US. The ultimate goal of DNS in these RAP deployments is to steer the RAP to a controller that meets all the controller compliance requirements discussed in [Appendix A: Regulatory Compliance](#). Several DNS service providers sell these capabilities. Organizations can also deploy their own in-house DNS-based global load balancing services to terminate RAPs on appropriate controllers.



Legal penalties and sanctions might be imposed on network administrators and organizations that do not meet the required regulatory compliance.

Regional location of RAPs can be used as a factor for load balancing RAPs between the LMS and backup LMS controllers that meet the required regulatory compliance. For example, the DNS solution can be configured to respond with IP address of the controller in New York if the request is from a RAP in the eastern region of US. If the request is from a RAP in the west of US, the DNS can be configured to respond with the IP address of the controller in Los Angeles.



The DNS sever can be configured to respond with multiple IP addresses for DNS resolution. If a RAP receives multiple IP addresses for a DNS resolution of the remote controller's FQDN, the RAP will try to connect to the first IP address in the list. If the RAP is unable to connect to this IP twice in succession, it will try the next IP in the list.

Planning AP Groups

A successful DNS resolution should direct a RAP to a controller that meets all the required controller compliance. After the FQDN of the remote controller is resolved, a RAP tries to connect to the controller and authenticate itself. If the RAP is authenticated successfully, the controller assigns the AP group defined for that RAP in the RAP whitelist database. Network administrators must ensure that the AP group that is assigned to a RAP has the appropriate regulatory domain profile to meet the required AP compliance. For instance, a RAP located in India that terminates on a ROW controller in London should be assigned an AP group with a regulatory domain profile for India (IN). Like the LMS controller, the backup LMS controller should also assign an AP group that has the appropriate regulatory domain profile.

Figure 121 shows a geographically redundant LMS and backup LMS deployment that fails controller AP compliance when a RAP connects to the backup LMS controller.

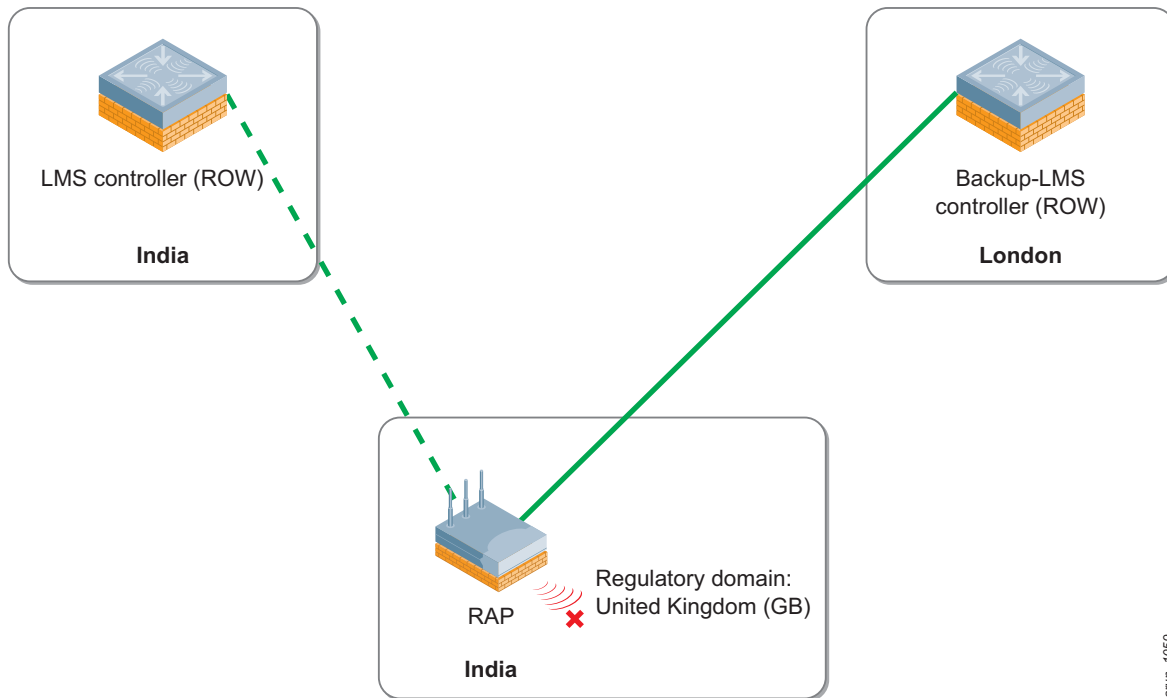


Figure 121 AP compliance failure

Recommendations for Geographical Redundancy

Consider the following key requirements when you implement geographical redundancy for global RAP deployments:

- Use intelligent DNS services and FQDN (instead of the IP address of the remote controller) in the RAP console page to direct the RAPs to controllers that meet the required controller compliance.



An alternative method is to use a different FQDN for users in different locations. For instance, users in US use rap-us.arubanetworks.com, and the users in India use rap-india.arubanetworks.com as the FQDN on the RAP console page. In deployments that use this method, if a user in the US travels to India with his RAP, the user has to reset the RAP and provision it with a different FQDN to redirect the RAP to an appropriate controller. This method also increases the management overhead.

- Based on the physical location of a RAP, an AP group with the appropriate regulatory domain profile should be assigned to RAPs to meet the required AP compliance.
- Every RAP in the RAP whitelist is assigned an AP group and at any given time an authorized/ authenticated AP on a controller can be assigned only one AP group. To comply with the regulatory domain requirements, the LMS and backup LMS controllers used for a RAP user in one regulatory domain cannot be used as the LMS and backup LMS pair when the same RAP user temporarily travels to a new regulatory domain. For example, assume that controller X and

an AP group with the regulatory domain profile for India (IN) represent the LMS controller and AP group for RAPs in India. If a RAP user in India travels to London and connects his RAP, the RAP should now terminate at a different LMS controller, which assigns an AP group with the regulatory domain profile for United Kingdom (GB). If this RAP is redirected back to the original controller X, the radios on the RAP will be operating with the wrong regulatory domain settings. Remember that Legal penalties and sanctions might be imposed on network administrators and organizations that do not meet the required regulatory compliance. In some small organizations with occasional travelers, the IT team may opt to manually change the AP group for traveling users based on their itinerary, but this increases the management overhead.

- The RAP whitelist should be imported manually to the LMS and backup LMS controllers because the whitelist is not shared between them.
- The backup LMS controller should belong to the same country code as the LMS controller.
- When a RAP moves to the backup LMS controller, it authenticates itself to the backup controller and downloads the configuration again. So, the AP group that is assigned to RAPs on the backup controller should have the appropriate regulatory domain profile configuration to meet the required AP compliance.
- Except when LMS preemption is enabled, a RAP can be assigned different AP groups on the LMS and backup LMS controllers. In other words, the AP group name used for a RAP on the LMS controller can be different from the AP group name used for the same RAP on the backup LMS controller except when LMS preemption is enabled. For the ease of management and troubleshooting, Aruba strongly recommends that you use the same AP group for a RAP on the LMS and backup LMS controller.
- When preemption is enabled, the name of the AP group that is assigned to a RAP on the LMS and backup LMS controller should be the same. This is because, when a RAP moves back to the LMS controller due to LMS preemption, it queries the LMS controller for the same AP group it used on the backup LMS controller. If the AP group that is assigned to a RAP on the backup LMS controller is not available on the LMS controller, the preempted RAP cannot be assigned an AP group by the LMS controller and the RAP will be unavailable until it is rebooted.
- LMS preemption is disabled by default and this is the recommended setting because it causes an outage during the preemption. A recommended method to move all the RAPs back to the LMS controller is to reboot the backup LMS controller during a maintenance window to force the clients back to the LMS controller.
- The configuration of an AP group that is assigned to a RAP on the backup LMS controller can be different than the configuration of the AP group that is assigned to the same RAP on the LMS controller. It is rare to extend VLANs across geographically separate data centers, so a common configuration change in the AP group that is used for a RAP on the backup LMS controller is the VLAN configuration of VAPs and wired ports.
- The AP group that is assigned to a RAP on the backup LMS controller can also have different profiles than the AP group that is assigned to the same RAP on the LMS controller. However, the need for such changes is uncommon in most deployments.
- Organizations that want to load balance RAPs between a pair of LMS and backup LMS controllers should use the RAP whitelist to split the RAP load between two separate AP groups with reversed LMS/backup LMS configuration. One AP group should have controller X as LMS and controller Y as backup LMS. The other AP group should have controller Y as LMS and controller X as backup LMS.

Figure 122 shows the controller and AP compliance that should be met when a mobile RAP user travels across regulatory boundaries.

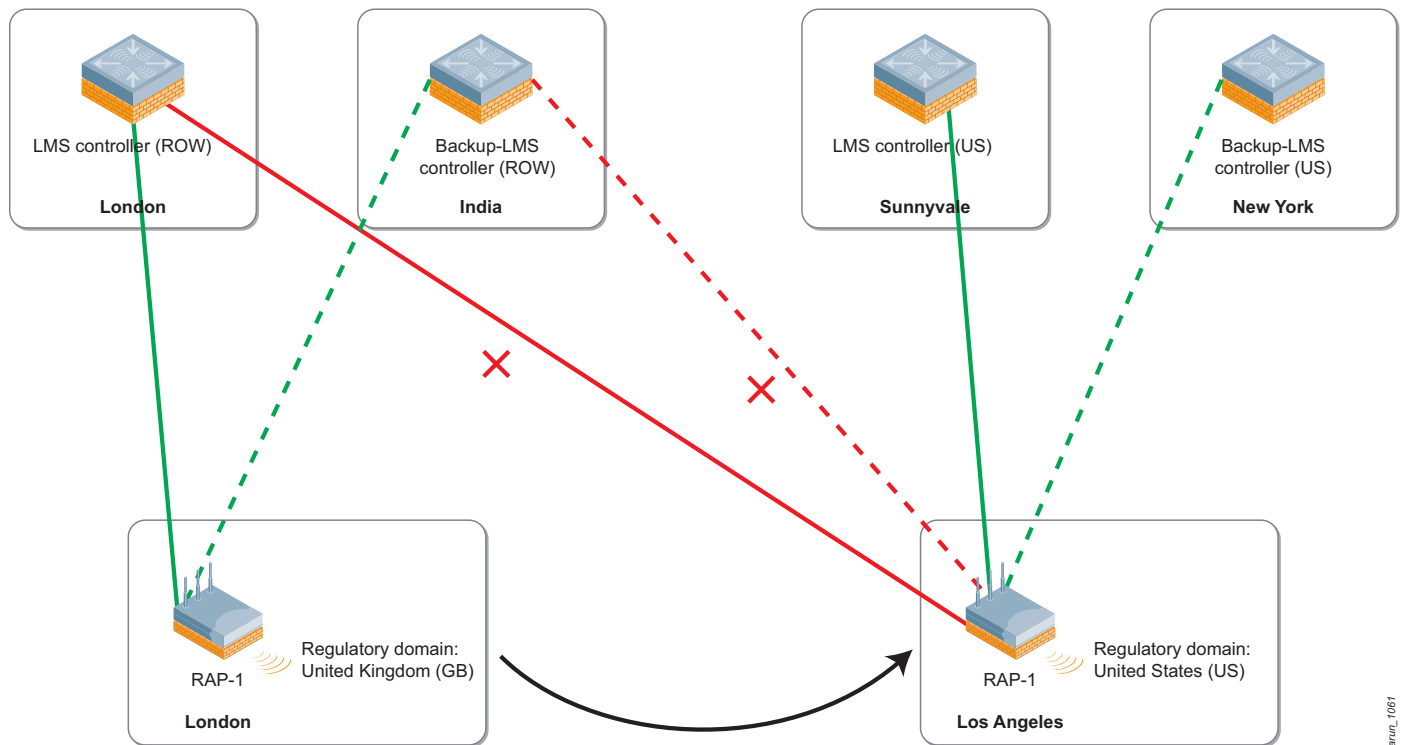


Figure 122 Compliance requirements (global RAP deployments)



If required, any LMS or backup LMS controller can be configured to have a redundant backup controller in its datacenter using the VRRP based active-standby redundancy model. This implementation adds an additional layer of redundancy.

Appendix D: Broadcast and Multicast Mitigation Features

For certain remote deployments, one of the main priorities is to conserve the expensive WAN bandwidth. RAPs extend the corporate LAN to remote locations. By default, extending a Layer 2 VLAN to the remote location floods the broadcast traffic on that VLAN to the remote site and increases the WAN bandwidth consumption. Some applications that organizations use might require the broadcast and multicast traffic to be flooded to the remote location. But in most deployments, certain types of broadcast traffic, such as Address Resolution Protocol (ARP), can be converted to unicast to minimize the WAN bandwidth and conserve the air time. ArubaOS has several knobs to reduce the flood of broadcast and multicast traffic to remote sites:

- Broadcast-filter ARP (global firewall knob)
- Drop Broadcast and Multicast (VAP knob)
- Convert Broadcast ARP Requests to Unicast (VAP knob)
- Broadcast (wired AP knob)
- Suppress-ARP (VLAN knob)
- BCMC Optimization (VLAN knob)
- Local-proxy-ARP (VLAN knob)

Some of these knobs must be enabled or disabled depending on your network requirements. This appendix provides the best practice recommendation for these knobs in remote deployments. Apart from these knobs, firewall policies in ArubaOS can also be used to deny certain unnecessary chatty protocols that might saturate the WAN link.



ArubaOS version 6.1.3.2 and later is recommended for broadcast and multicast mitigation in RAP deployments.

Broadcast-filter ARP (Global Firewall Knob)

This knob enables ARP conversion on all VLANs. If this knob is enabled, all the broadcast ARPs that are destined to wireless clients that are part of the user table and station table are converted to unicast ARP requests.



Aruba strongly recommends that you disable this knob in all deployments. This knob will be deprecated in future ArubaOS releases and network administrators instead should use the knob that is available on VAP profiles called Convert Broadcast ARP Requests to Unicast.

CLI

```
(config) # no firewall broadcast-filter arp
```

WebUI Screenshot

Dashboard
Monitoring
Configuration
Diagnostics
Maintenance
Plan
Save Configuration

WIZARDS
AP Wizard
Controller Wizard
WLAN/LAN Wizard
License Wizard
WIP Wizard
NETWORK
Controller
VLANs
Ports
Cellular Profile
IP
SECURITY
Authentication
Access Control
WIRELESS
AP Configuration
AP Installation
MANAGEMENT
General
Administration
Certificates
SNMP
Logging
Clock
Guest Provisioning
Captive Portal
SMTP
Bandwidth Calculator

Advanced Services > Stateful Firewall > Global Settings

Global Setting
White List BW Contracts
Network Services
Destination
BW Contracts Exception List

	IPv4
Monitor Ping Attack (per sec)	
Monitor TCP SYN Attack rate (per sec)	
Monitor IP Session Attack (per sec)	
Monitor/Police CP Attack rate (per sec)	
Deny Inter User Bridging	☐
Deny Inter User Traffic	☐
Deny All IP Fragments	☐
Enforce TCP Handshake Before Allowing Data	☐
Prohibit IP Spoofing	☒
Prohibit RST Replay Attack	☐
Log ICMP Errors	☐
Stateful SIP Processing	☒
Allow Tri-session with DNAT	☐
Session Mirror Destination	IP Address: Port:
Session Idle Timeout (sec)	
Disable FTP server	☐
GRE Call ID Processing	☐
Per-packet Logging	☐
Broadcast-filter ARP	☐

Figure 123 Broadcast-filter ARP (global firewall knob)

Drop Broadcast and Multicast (VAP Knob)

If the Drop Broadcast and Multicast knob is enabled, it drops all broadcasts and multicasts on a VAP except DHCP. In ArubaOS 6.1.3.1 and earlier, broadcast DHCP frames that are destined to wireless clients (that is, broadcast DHCP offers/ACKs) are converted to unicast DHCP frames over the air by the Drop Broadcast and Multicast knob. In ArubaOS 6.1.3.2 and later, the function that converts broadcast DHCP offers/ACKs to unicast DHCP frames over the air is part of the Convert Broadcast ARP Requests to Unicast knob.

CLI

```
!  
wlan virtual-ap "remote-employee"  
  
    broadcast-filter all  
!
```

WebUI Screenshot

The screenshot shows the Aruba WebUI Configuration page for 'Advanced Services > All Profile Management'. The left sidebar lists various profiles, including 'Virtual AP profile' with sub-profiles like 'default', 'guest-branch', 'guest-home', 'remote-application', 'remote-backup', and 'remote-employee'. The 'remote-employee' profile is selected, and its details are shown on the right. The 'Drop Broadcast and Multicast' knob is highlighted with a red circle. Other settings include 'Virtual AP enable' (checked), 'VLAN' (135), 'Forward mode' (split-tunnel), 'Mobile IP' (checked), 'Blacklist Time' (3600 sec), 'Dynamic Multicast Optimization (DMO)' (unchecked), 'Authentication Failure Blacklist Time' (3600 sec), 'Multi Association' (unchecked), 'VLAN Mobility' (unchecked), 'Remote-AP Operation' (standard), 'Convert Broadcast ARP requests to unicast' (checked), and 'Deny inter user traffic' (unchecked).

Profiles		Profile Details																																													
+ AP + RF Management - Wireless LAN + 802.11K Profile + SSID Profile + High-throughput SSID profile - Virtual AP profile + default + guest-branch + guest-home + remote-application + remote-backup - remote-employee + AAA Profile (remote-employee) 802.11K Profile (default) + SSID Profile (remote-employee) - WMM Traffic Management Profile		Virtual AP profile > remote-employee <a>Show Reference <a>Save As <a>Reset <table> <tr> <td>Virtual AP enable</td> <td>☒</td> <td>Allowed band</td> <td>all</td> </tr> <tr> <td>VLAN</td> <td>135</td> <td>Forward mode</td> <td>split-tunnel</td> </tr> <tr> <td>Deny time range</td> <td>--NONE--</td> <td>Mobile IP</td> <td>☒</td> </tr> <tr> <td>HA Discovery on-association</td> <td>☐</td> <td>DoS Prevention</td> <td>☐</td> </tr> <tr> <td>Station Blacklisting</td> <td>☒</td> <td>Blacklist Time</td> <td>3600 sec</td> </tr> <tr> <td>Dynamic Multicast Optimization (DMO)</td> <td>☐</td> <td>Dynamic Multicast Optimization (DMO) Threshold</td> <td>6</td> </tr> <tr> <td>Authentication Failure Blacklist Time</td> <td>3600 sec</td> <td>Multi Association</td> <td>☐</td> </tr> <tr> <td>Strict Compliance</td> <td>☐</td> <td>VLAN Mobility</td> <td>☐</td> </tr> <tr> <td>Preserve Client VLAN</td> <td>☐</td> <td>Remote-AP Operation</td> <td>standard</td> </tr> <tr> <td>Drop Broadcast and Multicast</td> <td>☐</td> <td>Convert Broadcast ARP requests to unicast</td> <td>☒</td> </tr> <tr> <td>Disable conversion multicast RA</td> <td>☐</td> <td>Deny inter user traffic</td> <td>☐</td> </tr> </table>		Virtual AP enable	☒	Allowed band	all	VLAN	135	Forward mode	split-tunnel	Deny time range	--NONE--	Mobile IP	☒	HA Discovery on-association	☐	DoS Prevention	☐	Station Blacklisting	☒	Blacklist Time	3600 sec	Dynamic Multicast Optimization (DMO)	☐	Dynamic Multicast Optimization (DMO) Threshold	6	Authentication Failure Blacklist Time	3600 sec	Multi Association	☐	Strict Compliance	☐	VLAN Mobility	☐	Preserve Client VLAN	☐	Remote-AP Operation	standard	Drop Broadcast and Multicast	☐	Convert Broadcast ARP requests to unicast	☒	Disable conversion multicast RA	☐	Deny inter user traffic	☐
Virtual AP enable	☒	Allowed band	all																																												
VLAN	135	Forward mode	split-tunnel																																												
Deny time range	--NONE--	Mobile IP	☒																																												
HA Discovery on-association	☐	DoS Prevention	☐																																												
Station Blacklisting	☒	Blacklist Time	3600 sec																																												
Dynamic Multicast Optimization (DMO)	☐	Dynamic Multicast Optimization (DMO) Threshold	6																																												
Authentication Failure Blacklist Time	3600 sec	Multi Association	☐																																												
Strict Compliance	☐	VLAN Mobility	☐																																												
Preserve Client VLAN	☐	Remote-AP Operation	standard																																												
Drop Broadcast and Multicast	☐	Convert Broadcast ARP requests to unicast	☒																																												
Disable conversion multicast RA	☐	Deny inter user traffic	☐																																												

Figure 124 Drop Broadcast and Multicast (VAP knob)

Convert Broadcast ARP Requests to Unicast (VAP Knob)

The Convert Broadcast ARP Requests to Unicast knob enables ARP conversion on a per VAP basis. If this knob is enabled on a VAP, all the broadcast ARPs that are destined to wireless clients that are part of the user table and station table are converted to unicast ARP requests.

CLI

```
!
wlan virtual-ap "remote-employee"

    broadcast-filter arp

!
```

WebUI Screenshot

ing **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Logout](#)

Advanced Services > All Profile Management

Profiles	Profile Details																																												
+ AP + RF Management - Wireless LAN + 802.11K Profile + SSID Profile + High-throughput SSID profile - Virtual AP profile + default + guest-branch + guest-home + remote-application + remote-backup - remote-employee + AAA Profile remote-employee 802.11K Profile default + SSID Profile remote-employee - WMM Traffic Management Profile	Virtual AP profile > remote-employee Show Reference Save As Reset <table border="1"> <tr> <td>Virtual AP enable</td> <td>☒</td> <td>Allowed band</td> <td>all ▾</td> </tr> <tr> <td>VLAN</td> <td>135 <-- 135 ▾</td> <td>Forward mode</td> <td>split-tunnel ▾</td> </tr> <tr> <td>Deny time range</td> <td>--NONE-- ▾</td> <td>Mobile IP</td> <td>☒</td> </tr> <tr> <td>HA Discovery on-association</td> <td>☐</td> <td>DoS Prevention</td> <td>☐</td> </tr> <tr> <td>Station Blacklisting</td> <td>☒</td> <td>Blacklist Time</td> <td>3600 sec</td> </tr> <tr> <td>Dynamic Multicast Optimization (DMO)</td> <td>☐</td> <td>Dynamic Multicast Optimization (DMO) Threshold</td> <td>6</td> </tr> <tr> <td>Authentication Failure Blacklist Time</td> <td>3600 sec</td> <td>Multi Association</td> <td>☐</td> </tr> <tr> <td>Strict Compliance</td> <td>☐</td> <td>VLAN Mobility</td> <td>☐</td> </tr> <tr> <td>Preserve Client VLAN</td> <td>☐</td> <td>Remote-AP Operation</td> <td>standard ▾</td> </tr> <tr> <td>Drop Broadcast and Multicast</td> <td>☐</td> <td>Convert Broadcast ARP requests to unicast</td> <td>☒</td> </tr> <tr> <td>Disable conversion multicast RA</td> <td>☐</td> <td>Deny inter user traffic</td> <td>☐</td> </tr> </table>	Virtual AP enable	☒	Allowed band	all ▾	VLAN	135 <-- 135 ▾	Forward mode	split-tunnel ▾	Deny time range	--NONE-- ▾	Mobile IP	☒	HA Discovery on-association	☐	DoS Prevention	☐	Station Blacklisting	☒	Blacklist Time	3600 sec	Dynamic Multicast Optimization (DMO)	☐	Dynamic Multicast Optimization (DMO) Threshold	6	Authentication Failure Blacklist Time	3600 sec	Multi Association	☐	Strict Compliance	☐	VLAN Mobility	☐	Preserve Client VLAN	☐	Remote-AP Operation	standard ▾	Drop Broadcast and Multicast	☐	Convert Broadcast ARP requests to unicast	☒	Disable conversion multicast RA	☐	Deny inter user traffic	☐
Virtual AP enable	☒	Allowed band	all ▾																																										
VLAN	135 <-- 135 ▾	Forward mode	split-tunnel ▾																																										
Deny time range	--NONE-- ▾	Mobile IP	☒																																										
HA Discovery on-association	☐	DoS Prevention	☐																																										
Station Blacklisting	☒	Blacklist Time	3600 sec																																										
Dynamic Multicast Optimization (DMO)	☐	Dynamic Multicast Optimization (DMO) Threshold	6																																										
Authentication Failure Blacklist Time	3600 sec	Multi Association	☐																																										
Strict Compliance	☐	VLAN Mobility	☐																																										
Preserve Client VLAN	☐	Remote-AP Operation	standard ▾																																										
Drop Broadcast and Multicast	☐	Convert Broadcast ARP requests to unicast	☒																																										
Disable conversion multicast RA	☐	Deny inter user traffic	☐																																										

nutil/setup.html?task=configure-profile-remote-employee-decrypt-tunnel

Figure 125 Convert Broadcast ARP Requests to Unicast (VAP knob)

Broadcast (Wired AP Knob)

When the Broadcast knob is disabled, flooded traffic from other wired APs (in tunnel and split-tunnel forwarding modes) and VAPs (in Tunnel, Decrypt Tunnel, and Split Tunnel forwarding modes) are not flooded to this wired AP. For this action to work, the wired AP, where the Broadcast knob is set to disable, must be in the tunnel forwarding mode. In other words, this knob is effective only on wired ports in tunnel mode.



NOTE

If you disable this knob on a wired port, broadcast traffic, including ARP requests, is dropped. If this traffic is dropped, communication might be broken between users/phones on this port and the users/phones on other VAPs or wired ports that are on the same VLAN.

CLI

```
!
ap wired-ap-profile "wired-employee"

    broadcast

!
```

WebUI Screenshot

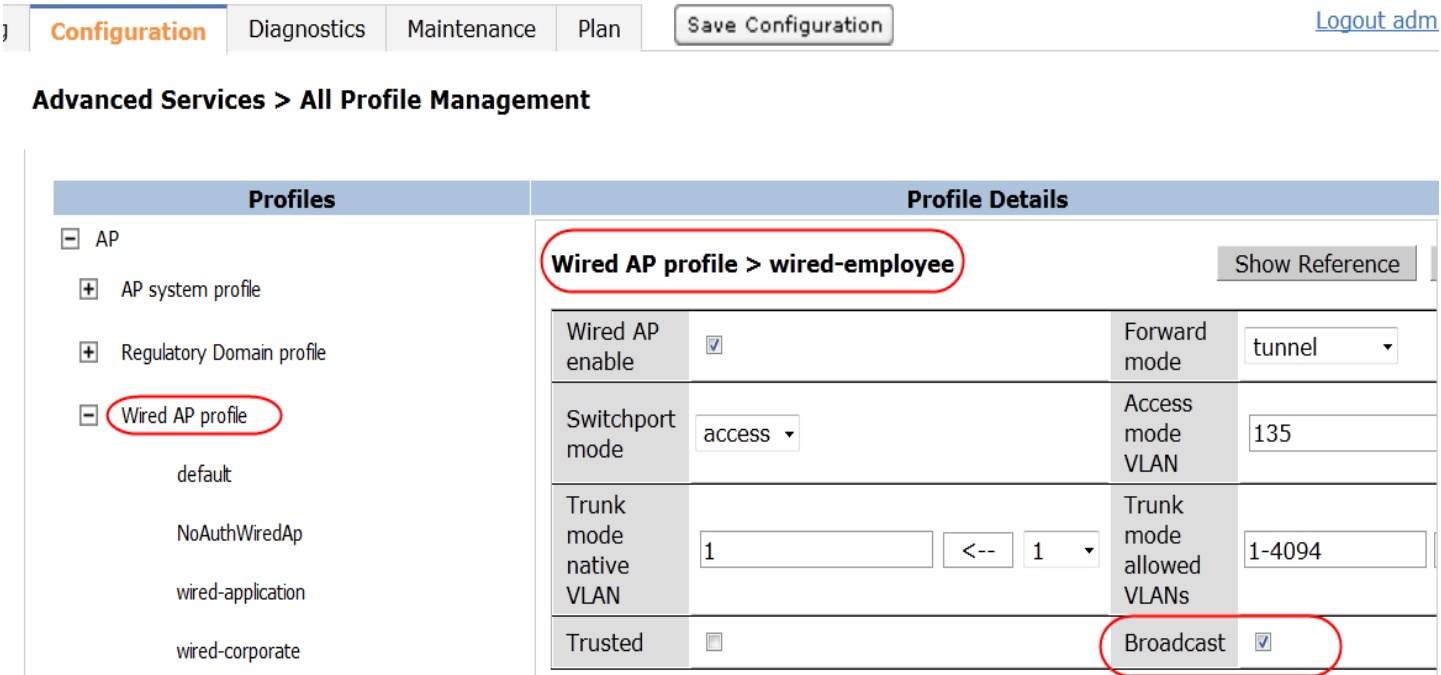


Figure 126 Broadcast (wired AP knob)

Suppress-ARP (VLAN Knob)

When the Suppress-ARP knob is enabled, it stops the flooding of unknown ARP requests to tunnel or decrypt-tunnel VAPs that are in the same VLAN on which the unknown ARP request was received. Flooding is stopped regardless of the type of ingress port (that is, LAN port, wired AP, or VAP) on which the unknown ARP request was received. The unknown ARP request is still flooded out of LAN ports, wired APs (tunnel/trusted, tunnel/untrusted, and split-tunnel) and split-tunnel VAPs. In ArubaOS 6.1.3.2 and later, gratuitous ARPs are not dropped by the Suppress-ARP knob and the knob is effective only on tunnel or decrypt-tunnel VAPs that have the Convert Broadcast ARP Requests to Unicast knob enabled.



An ARP request is considered unknown by the controller if the target IP in the ARP request has no corresponding IP/MAC address pair in the data path user table. In ArubaOS 6.1.3.1 and earlier, the Suppress-ARP feature drops gratuitous ARPs on all wireless tunnels and enabling the Suppress-ARP knob automatically enables the Local-proxy-ARP knob.

CLI

```
!  
interface vlan 131  
  
    suppress-arp  
!
```

BC-MC Optimization (VLAN Knob)

The BC-MC Optimization knob drops all the broadcast and multicast frames on a VLAN (wired and wireless interfaces) except for ARP, DHCP, IPv6 router advertisement, IPv6 neighbor solicitation, and VRRP traffic.

CLI

```
!
interface vlan 131

    bcmc-optimization
!
```

WebUI Screenshot

The screenshot shows the Aruba WebUI configuration page for editing VLAN 131. The breadcrumb navigation path is **Network > IP > IP Interface > Edit VLAN (131)**, which is circled in red. The page includes tabs for Configuration, Diagnostics, Maintenance, and Plan, along with a 'Save Configuration' button and a 'Logout admin' link.

The configuration form is divided into several sections:

- IP version:** IPv4
- VLAN ID:** 131
- Details:**
 - ☐ Obtain an IP address from DHCP
 - ☐ Client ID
 - ☐ Obtain an IP address with PPPoE
 - Service name
 - Username
 - Password
 - Confirm Password
 - ☒ Use the following IP address
 - IP Address: 10.169.131.6
 - Net Mask: 255.255.255.0
 - Uplink Priority: 0
- DHCP Helper Addresses:**
 - No Helper Addresses
 - Add button
 - Option-82: None
- IGMP:**
 - Enable IGMP: ☐
 - Snooping: ☐
 - Proxy: ☐
 - ☒ Interface: Gigabitethernet 1/0
 - ☐ Port-Channel ID: 0
- NAT:**
 - Enable source NAT for this VLAN: ☐
- Inter-VLAN Routing:**
 - Enable Inter-VLAN Routing: ☒
- MLD:**
 - Enable MLD Snooping: ☐
- BCMC (Broadcast-Multicast) Optimization:** (highlighted with a red circle)
 - Enable BCMC Optimization: ☐
- OSPF:**

Figure 127 BCMC Optimization (VLAN knob)

Local-proxy-ARP (VLAN Knob)

If the Local-proxy-ARP knob is enabled on a VLAN, the controller will proxy-ARP with target's MAC address when an ARP request is received on a Layer 2 VLAN (no IP address configured on the VLAN interface). However, if the target IP address is a known user on a Layer 3 VLAN (IP address configured on the VLAN interface), the controller responds with its MAC address instead.



A known user is considered someone who the controller is aware of either through route cache or user table.

CLI

```
!  
interface vlan 131  
  
    ip local-proxy-arp  
!
```

Table 52 and Table 53 summarize the recommendations for the broadcast and multicast optimization knobs in remote deployments.

Table 52 Broadcast Suppression Features Based on Wired Ports and VAPs

Broadcast Suppression Features based on Wired Ports and VAPs	RAPs					
	Tunnel Mode Trusted (Wireless tunnels are always untrusted.)	Tunnel Mode Untrusted		Decrypt-tunnel Mode (This mode is not available for wired ports.)	Split-tunnel Mode (Split-tunnels are always untrusted.)	
	Wired	Wired	Wireless	Wireless	Wired	Wireless
Broadcast-filter ARP (Global Firewall Knob) Note: This knob functions only for wireless users. Remember that this knob will be deprecated in future releases. Caution: Aruba strongly recommends that you disable this knob in all deployments. Network administrators should use the Convert Broadcast ARP Requests to Unicast knob instead.	N/A		Recommended: Disable [Default: Disabled]		N/A	
Drop Broadcast and Multicast (VAP Knob) Note: If this knob is enabled, the Convert Broadcast ARP Requests to Unicast knob should also be enabled or all the ARP traffic will be dropped. Note: If clients do not require multicast services, then enable this knob. Note: In ArubaOS 6.1.3.1 and earlier, the Drop Broadcast and Multicast knob converts broadcast DHCP offers/ACKs to unicast frames over the air. However, starting with ArubaOS 6.1.3.2, the Convert Broadcast ARP Requests to Unicast knob will convert broadcast DHCP offers/ACKs to unicast frames over the air.	N/A		Recommended: Disable [Default: Disabled]		N/A	

Table 52 Broadcast Suppression Features Based on Wired Ports and VAPs (Continued)

Broadcast Suppression Features based on Wired Ports and VAPs	RAPs					
	Tunnel Mode Trusted (Wireless tunnels are always untrusted.)	Tunnel Mode Untrusted		Decrypt-tunnel Mode (This mode is not available for wired ports.)	Split-tunnel Mode (Split-tunnels are always untrusted.)	
	Wired	Wired	Wireless	Wireless	Wired	Wireless
Convert Broadcast ARP Requests to Unicast (Virtual-AP Knob) Note: This knob can be enabled individually and does not require the Drop Broadcast and Multicast knob to function. Note: Starting with ArubaOS 6.1.3.2, the Convert Broadcast ARP Requests to Unicast knob converts broadcast DHCP offers/ACKs to unicast frames over the air.	N/A		Recommended: Enable [Default (6.1.3.1 and earlier): Disabled] [Default (6.1.3.2 and later): Enabled]		N/A	
Broadcast (Wired-AP Knob) Note: This knob is applicable only for wired ports in tunnel mode. If it is enabled on a wired port (box checked in WebUI), all broadcasts from other tunnels are flooded to this wired port. If it is disabled (box unchecked in WebUI), the broadcasts from other tunnels are not flooded. Caution: If you disable this knob on a wired port, communication might be broken between users/phones on this port and the users/phones on other VAPs or wired ports that are on the same VLAN.	Recommended: Enable [Default: Enabled]		N/A		N/A	

Table 53 Broadcast Suppression Features Based on VLANs

Broadcast Suppression Features Based on VLANs	RAPs					
	Tunnel Mode Trusted (Wireless tunnels are always untrusted.)	Tunnel Mode Untrusted		Decrypt-tunnel Mode (This mode is not available for wired ports.)	Split-tunnel Mode (Split-tunnels are always untrusted.)	
	Wired	Wired	Wireless	Wireless	Wired	Wireless
Suppress-ARP (VLAN Knob) Note: In ArubaOS 6.1.3.1 and earlier, enabling this knob automatically enables the Local-proxy-ARP knob. In ArubaOS 6.1.3.2 and later, enabling this knob does not automatically enable the Local-proxy-ARP knob. Note: In ArubaOS 6.1.3.2 and later, the Suppress-ARP knob is effective only on tunnel or decrypt-tunnel with the Convert Broadcast ARP Requests to Unicast knob enabled.	N/A		(ArubaOS 6.1.3.1 and earlier) Recommended: Disable [Default: Disabled] (ArubaOS 6.1.3.2 and later) Recommended: Enable [Default: Enabled]		N/A	
BCMC Optimization (VLAN Knob) Note: If clients do not require multicast services, it is recommended to enable this knob, especially in RAP deployments.	Recommended: Disable [Default: Disabled]					
Local-proxy-ARP (VLAN Knob) Note: Local-Proxy-ARP should not be enabled on a Layer 3 VLAN if ARP inspection is enabled on an upstream router, or if the VLAN is configured on multiple controllers.	Recommended: Disable [Default: Disabled]					

Appendix E: Contacting Aruba Networks

Contacting Aruba Networks

Web Site Support	
Main Site	http://www.arubanetworks.com
Support Site	https://support.arubanetworks.com
Software Licensing Site	https://licensing.arubanetworks.com/login.php
Wireless Security Incident Response Team (WSIRT)	http://www.arubanetworks.com/support/wsirt.php
Support Emails	
Americas and APAC	support@arubanetworks.com
EMEA	emea_support@arubanetworks.com
WSIRT Email Please email details of any security problem found in an Aruba product.	wsirt@arubanetworks.com

Validated Reference Design Contact and User Forum	
Validated Reference Designs	http://www.arubanetworks.com/vrd
VRD Contact Email	referencedesign@arubanetworks.com
AirHeads Online User Forum	http://community.arubanetworks.com

Telephone Support	
Aruba Corporate	+1 (408) 227-4500
FAX	+1 (408) 227-4550
Support	
● United States	+1-800-WI-FI-LAN (800-943-4526)
● Universal Free Phone Service Numbers (UFIN):	
■ Australia	Reach: 1300 4 ARUBA (27822)
■ United States	1 800 9434526 1 650 3856589
■ Canada	1 800 9434526 1 650 3856589
■ United Kingdom	BT: 0 825 494 34526 MCL: 0 825 494 34526

Telephone Support

● Universal Free Phone Service Numbers (UIFN):

■ Japan	IDC: 10 810 494 34526 * Select fixed phones IDC: 0061 010 812 494 34526 * Any fixed, mobile & payphone KDD: 10 813 494 34526 * Select fixed phones JT: 10 815 494 34526 * Select fixed phones JT: 0041 010 816 494 34526 * Any fixed, mobile & payphone
■ Korea	DACOM: 2 819 494 34526 KT: 1 820 494 34526 ONSE: 8 821 494 34526
■ Singapore	Singapore Telecom: 1 822 494 34526
■ Taiwan (U)	CHT-I: 0 824 494 34526
■ Belgium	Belgacom: 0 827 494 34526
■ Israel	Bezeq: 14 807 494 34526 Barack ITC: 13 808 494 34526
■ Ireland	EIRCOM: 0 806 494 34526
■ Hong Kong	HKTI: 1 805 494 34526
■ Germany	Deutsche Telekom: 0 804 494 34526
■ France	France Telecom: 0 803 494 34526
■ China (P)	China Telecom South: 0 801 494 34526 China Netcom Group: 0 802 494 34526
■ Saudi Arabia	800 8445708
■ UAE	800 04416077
■ Egypt	2510-0200 8885177267 * within Cairo 02-2510-0200 8885177267 * outside Cairo
■ India	91 044 66768150