Spectralink VIEW Certified Configuration Guide

Aruba
A Hewlett Packard Enterprise Company

Aruba Controllers (Series) 600, 3200, 3400, 3600, 6000, 7000, 7100, 7200
Aruba APs AP-68, AP-9x, AP-10x, AP-11x, AP-12x, AP-13x, AP-20x, AP-21x, AP-22x, AP-27x
Copyright Notice

© 2005-2017 Spectralink Corporation All rights reserved. Spectralink™, the Spectralink logo and the names and marks associated with Spectralink’s products are trademarks and/or service marks of Spectralink Corporation and are common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient’s personal use, without the express written permission of Spectralink.

All rights reserved under the International and pan-American Copyright Conventions. No part of this manual, or the software described herein, may be reproduced or transmitted in any form or by any means, or translated into another language or format, in whole or in part, without the express written permission of Spectralink Corporation.

Do not remove (or allow any third party to remove) any product identification, copyright or other notices.

Notice

Spectralink Corporation has prepared this document for use by Spectralink personnel and customers. The drawings and specifications contained herein are the property of Spectralink and shall be neither reproduced in whole or in part without the prior written approval of Spectralink, nor be implied to grant any license to make, use, or sell equipment manufactured in accordance herewith.

Spectralink reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult Spectralink to determine whether any such changes have been made.

NO REPRESENTATION OR OTHER AFFIRMATION OF FACT CONTAINED IN THIS DOCUMENT INCLUDING BUT NOT LIMITED TO STATEMENTS REGARDING CAPACITY, RESPONSE-TIME PERFORMANCE, SUITABILITY FOR USE, OR PERFORMANCE OF PRODUCTS DESCRIBED HEREIN SHALL BE DEEMED TO BE A WARRANTY BY SPECTRALINK FOR ANY PURPOSE, OR GIVE RISE TO ANY LIABILITY OF SPECTRALINK WHATSOEVER.

Contact Information

<table>
<thead>
<tr>
<th>US Location</th>
<th>Denmark Location</th>
<th>UK Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>+1 800-775-5330</td>
<td>+45 7560 2850</td>
<td>+44 (0) 20 3284 1536</td>
</tr>
<tr>
<td>Spectralink Corporation</td>
<td>Spectralink Europe ApS</td>
<td>Spectralink Europe UK</td>
</tr>
<tr>
<td>2560 55th Street</td>
<td>Bygholm Soepark 21 E Stuen</td>
<td>329 Bracknell, Doncastle Road</td>
</tr>
<tr>
<td>Boulder, CO 80301</td>
<td>8700 Horsens</td>
<td>Bracknell, Berkshire, RG12 8PE</td>
</tr>
<tr>
<td>USA</td>
<td>Denmark</td>
<td>United Kingdom</td>
</tr>
<tr>
<td><a href="mailto:info@spectralink.com">info@spectralink.com</a></td>
<td><a href="mailto:infoemea@spectralink.com">infoemea@spectralink.com</a></td>
<td><a href="mailto:infoemea@spectralink.com">infoemea@spectralink.com</a></td>
</tr>
</tbody>
</table>
Contents

Introduction .................................................................................................................. 5
Certified Product Summary .......................................................................................... 5
Known Limitations ....................................................................................................... 6
Spectralink References ............................................................................................... 7
  Support Documents .................................................................................................. 7
  White Papers ........................................................................................................... 8
Product Support .......................................................................................................... 8

Chapter 1: Overview .................................................................................................. 9
  Command, Comment, and Screen Text Key .............................................................. 9
  Network Topology ..................................................................................................... 10

Chapter 2: Initial Administrative Setup ................................................................. 11
  Connecting to the Mobility Controller .................................................................... 11
    Via console ............................................................................................................. 11
    Via the Command Line Interface (CLI) ................................................................. 11
    Via the Web interface (WebUI) .............................................................................. 12
  Initializing the Controller ......................................................................................... 14
  Licensing the Controller ........................................................................................... 16

Chapter 3: Configure the Environment .................................................................... 19
  Logical and Physical Interfaces ................................................................................ 19
    Using CLI ............................................................................................................... 19
    On the WebUI ......................................................................................................... 20
  Creating Firewall Roles and Policies ...................................................................... 24
  Creating a Syslog Policy ........................................................................................... 25
    On CLI ..................................................................................................................... 25
    On WebUI ............................................................................................................... 25
  Creating User-Role and Assigning Firewall Rules to the Role ............................... 27
    Creating a User-Role Derivation Rule ................................................................ 27
    On CLI ..................................................................................................................... 27
    On WebUI ............................................................................................................... 27
    Assigning Firewall Rules to the Role .................................................................. 28
    On CLI ..................................................................................................................... 28
    On WebUI ............................................................................................................... 29

Chapter 4: Configure Wireless Security .................................................................... 31
  Configuration Steps for None, WEP, WPA-PSK or WPA2-PSK Security ............... 31
Creating an Authentication Profile for controller-based authentication............................31
Use the next four statements if using an external Radius server .................................31
Configuration Steps for WPA2-Enterprise Security .........................................................37
Defining an 802.1X authentication server ....................................................................37
Create a Server Group and Add the RADIUS Server ....................................................39
Using CLI ........................................................................................................................39
Using WebUI ...................................................................................................................39
Creating an 802.1X Authentication Profile .................................................................40
Using CLI ........................................................................................................................40
Using WebUI ...................................................................................................................40
Creating an Authentication Profile ...............................................................................42
Using CLI ........................................................................................................................42
Using WebUI ...................................................................................................................42

Chapter 5: Configure Wireless LAN ................................................................. 44
On CLI ............................................................................................................................44
On WebUI .......................................................................................................................54
Introduction

Spectralink’s Voice Interoperability for Enterprise Wireless (VIEW) Certification Program is designed to ensure interoperability and high performance between PIVOT™ by Spectralink® (PIVOT) and 84-Series Wireless Telephones and WLAN infrastructure products.

The products listed below have been tested in Spectralink’s lab and have passed VIEW Certification.

Certified Product Summary

<table>
<thead>
<tr>
<th>Manufacturer:</th>
<th>Aruba Networks: <a href="http://www.arubanetworks.com">www.arubanetworks.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Certified products:</td>
<td>Controllers (Series): Aruba 600, 3200, 3400, 3600, 6000, 7000, 7100, 7200</td>
</tr>
<tr>
<td></td>
<td>Access Points: Aruba AP-8, 9x, 10x, 11x, 12x, 13x, 20x, 21x, 22x, 27x</td>
</tr>
<tr>
<td>AP Radio(s):</td>
<td>2.4 GHz (802.11b/g/n), 5 GHz (802.11a/n)</td>
</tr>
<tr>
<td>Security:</td>
<td>None, WEP, WPA-PSK, WPA2-PSK, WPA2-Enterprise (EAP-FAST and PEAPv0/MSCHAPv2)</td>
</tr>
<tr>
<td>QoS:</td>
<td>Wi-Fi Standard for Spectralink 84-Series and PIVOT</td>
</tr>
<tr>
<td>AP/controller software version approved:</td>
<td>6.5.1.2 for 20x, 21x, 22x, 27x</td>
</tr>
<tr>
<td></td>
<td>6.3.1.9 for 68, 9x, 105, 11x, 12x, 13x</td>
</tr>
<tr>
<td></td>
<td>6.4.2.3 for 13x, 22x, 27x</td>
</tr>
<tr>
<td>Network topology</td>
<td>Switched Ethernet (recommended)</td>
</tr>
<tr>
<td>Handset* models tested:</td>
<td>PIVOT models</td>
</tr>
<tr>
<td>AP radio mode:</td>
<td>802.11b</td>
</tr>
<tr>
<td>Meets VIEW minimum call capacity per AP:**</td>
<td>8</td>
</tr>
</tbody>
</table>
Handset* models tested: Spectralink 8440/8441/8450/8452/8453 Wireless Telephone

<table>
<thead>
<tr>
<th>AP radio mode:</th>
<th>802.11b</th>
<th>802.11 b/g</th>
<th>802.11b/g/n</th>
<th>802.11a, a/n, a/n/ac</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meets VIEW minimum call capacity per AP:**</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>10</td>
</tr>
</tbody>
</table>

*Spectralink handset models and their OEM derivates are verified compatible with the WLAN hardware and software identified in the table. Throughout the remainder of this document they will be referred to collectively as “Spectralink wireless telephones”, “phones” or “handsets. When necessary to differentiate, the 8440, 8441 (8440 with personal alarm hardware), 8450 (with 1D bar code reader), 8452 (with 1D and 2D bar code reader), and 8453 (8452 with personal alarm hardware) handsets will be referred to collectively as the 84-Series handsets. All PIVOT models will be referred to collectively as PIVOT handsets.

** Maximum calls tested per the VIEW Certification Test Plan. The certified product may actually support a higher number of maximum calls.

**Known Limitations**

The following limitations were discovered during VIEW testing of this product:

- 1Mb/s and 2Mb/s data rates must be disabled to meet maximum call capacity.
- All handsets operating on a given AP radio must have the same QoS setting. The APs must be configured to enable the corresponding features to support the handset QoS setting.
- Heavy multicast, broadcast or push-to-talk (PTT) traffic may impair voice quality.
- Paired-channel deployment is not recommended on the 2.4 GHz radio by Aruba.
- The Client Match features, if enabled, may cause audio dropouts on the Spectralink handsets. The White Paper: *Best Practices Guide to Deploying Spectralink 84-Series Handsets* has more information about cell design. If ARM is on, it is recommended to check the VOIP Aware and Client Aware options.
- 802.11r is not implemented on the Spectralink products
- Phones manufactured recently or set to factory defaults with a PIVOT version of 2.4 or later or an 84-series version after 5.3 will have 802.11n disabled.
- If 802.11n is turned on, A-MPDU aggregation (an 802.11n feature) should be disabled in SSIDs used by the handsets. The handsets do not support this feature and there is an incompatibility in the Aruba implementation which causes poor handset performance.
**Spectralink References**

All Spectralink documents are available at [http://support.spectralink.com](http://support.spectralink.com).

---

**To go to a specific product page**

Select the Product Category and Product Type from the dropdown lists and then select the product from the next page. All resources for that particular product are displayed by default under the All tab. Documents, downloads and other resources are sorted by the date they were created so the most recently created resource is at the top of the list. You can further sort the list by the tabs across the top of the list to find exactly what you are looking for. Click the title to open the link.

**Support Documents**

*PIVOT by Spectralink Deployment Guide*  The Deployment Guide provides sequential information for provisioning and deploying the smartphones. It covers deployment using QNC and CMS as well as manual deployment.
**PIVOT by Spectralink Configuration Guide**  The PIVOT Configuration Guide provides detailed information about PIVOT menu items that have been developed specifically for the PIVOT smartphone.

The *Spectralink 84-Series Wireless Telephone Administration Guide* provides a comprehensive list of every parameter available on Spectralink 84-Series Wireless Telephones.

*Spectralink 84-Series Wireless Telephone Deployment Guide* This document introduces deployment concepts and the methods of provisioning the 84-Series handsets in any type of facility. It is the fundamental text and a prerequisite to this Administration Guide, especially for administrators who are new to the Spectralink 84-Series handsets or who may wish a refresher course.

The *Web Configuration Utility User Guide* is used for troubleshooting in certain isolated cases as explained in the text.

*Best Practices for Deploying Spectralink 87-Series PIVOT Handsets* provides detailed information on wireless LAN layout, network infrastructure, QoS, security and subnets.

**White Papers**


For the Spectralink 84-Series Wireless Telephones, please refer to *Best Practices Guide for Deploying Spectralink 84-Series Handsets* for detailed information on wireless LAN layout, network infrastructure, QoS, security and subnets.

For additional details on RF deployment please see *The challenges of ensuring excellent voice quality in a Wi-Fi workplace* and *Deploying Enterprise-Grade Wi-Fi Telephony*.

These White Papers identify issues and solutions based on Spectralink’s extensive experience in enterprise-class Wi-Fi telephony. It provides recommendations for ensuring that a network environment is adequately optimized for use with Spectralink Wireless Telephones.

**Product Support**

Note: **RADIUS server configuration**

This document does not cover the steps involved to configure a RADIUS server required for using WPA2-Enterprise security types.

If you encounter difficulties or have questions regarding the configuration process, please contact Aruba customer service at: [http://www.arubanetworks.com/support.php](http://www.arubanetworks.com/support.php) or Spectralink at support.spectralink.com.
Chapter 1: Overview

**Command, Comment, and Screen Text Key**

In the sections below you will find commands, comments, prompts, system responses, or other screen-displayed information involved in the configuration process. This key explains the text styles and symbols used to denote them.

<table>
<thead>
<tr>
<th>Text Style</th>
<th>Denotes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>xxxxxxxxx</td>
<td>Typed command</td>
</tr>
<tr>
<td>&lt;xxxxxxxxx&gt;</td>
<td>Encryption key, domain name or other information specific to your system that needs to be entered</td>
</tr>
<tr>
<td>(xxxxxxxxx)</td>
<td>Comment about a command or set of commands</td>
</tr>
<tr>
<td>xxxxxxxxx</td>
<td>Prompt, system response or other displayed information</td>
</tr>
</tbody>
</table>
**Network Topology**

The following configuration was tested during VIEW Certification.

Note: Example configuration shown
This is a modified diagram and not all components are shown for every system type.
Chapter 2: Initial Administrative Setup

Connecting to the Mobility Controller

Via console

Using a standard RS-232 cable, connect the Aruba mobility controller to the serial port of a terminal or PC.

Run a terminal emulation program (such as HyperTerminal™) or use a VT-100 terminal with the following configuration:

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bits per second</td>
<td>9600</td>
</tr>
<tr>
<td>Data bits</td>
<td>8</td>
</tr>
<tr>
<td>Parity</td>
<td>None</td>
</tr>
<tr>
<td>Stop bits</td>
<td>1</td>
</tr>
<tr>
<td>Flow control</td>
<td>None</td>
</tr>
</tbody>
</table>

Use this mode of connection during the initialization phase of the controller to configure login credentials.

1. Press Enter to display the Aruba mobility controller login screen.
2. Enter the default login: **admin** and the default password: **admin**. These are case sensitive.
3. Enter **enable** and the default password: **enable** to get into the command mode.

Via the Command Line Interface (CLI)

By default, only SSH (Secure Shell) access to the switch (mobility controller) is permitted.

1. From a management system that has network connectivity to the switch, connect to the switch using SSH
   
   `ssh admin@<switch IP address>`

2. Enter the admin password at the password prompt.
   Type enable at the > prompt to enter the enable mode.
3. Type the enable password when prompted for a password.
Via the Web interface (WebUI)

Once the connectivity to the switch is verified, open a Web browser and enter the switch’s IP address in the navigator bar.

The switch can be accessed using http at [http://<switch IP Address>]
or https at [https://<switch IP Address>].

The user is prompted with the username and password configured (in the example above, the username/password configured is **admin/admin**). On successful login the following Monitoring screen is displayed versions 6.4 and 6.3:

![Monitoring screen](image)

For versions 6.5+, the Dashboard tab is displayed:
Dashboard for versions 6.5+
Initializing the Controller

When powered up, the controller will present the following screen on the serial console. Please fill in basic network details when prompted. The following is a sample of the information presenting which may vary depending on the controller model and software version:

Example

<<< Welcome to Aruba Networks - Aruba A651 >>>

Performing CompactFlash fast test... Checking for file system... Passed.
Reboot Cause: User reboot.
Restoring the database... done.
Generating SSH Keys...... done.
Reading configuration from factory-default.cfg

************************ Welcome to the Aruba651 setup dialo************************
This dialog will help you to set the basic configuration for the switch.
These settings, except for the Country Code, can later be changed from the
Command Line Interface or Graphical User Interface.

Commands: <Enter> Submit input or use [default value], <ctrl-I> Help
<ctrl-B> Back, <ctrl-F> Forward, <ctrl-A> Line begin, <ctrl-E> Line end
<ctrl-D> Delete, <BackSpace> Delete back, <ctrl-K> Delete to end of line
<ctrl-P> Previous question <ctrl-X> Restart beginning

Enter System name [Aruba651]
Enter VLAN 1 interface IP address [172.16.0.254]: <Controller IP>
Enter VLAN 1 interface subnet mask [255.255.255.0]: <Subnet Mask>
Enter IP Default gateway [none]: <Default GW IP address>
Enter Switch Role, (master|local) [master]
This controller is restricted to Country code US for United States, please confirm (yes|no)?: yes
Enter Time Zone [PST-8:0]
Enter Time in GMT [15:39:55]
Enter Date (MM/DD/YYYY) [4/21/2009]
Enter Password for admin login (up to 32 chars): *****
Re-type Password for admin login: *****
Enter Password for enable mode (up to 15 chars): *****
Re-type Password for enable mode: *****
Do you wish to shutdown all the ports (yes|no)? [no]: no

Current choices are

System name: Aruba651
VLAN 1 interface IP address: <IP Address>
VLAN 1 interface subnet mask: <Subnet Mask>
IP Default gateway: <Default Gateway>
Switch Role: master
Time Zone: PST-8:0
Ports shutdown: no

If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no): yes
Creating configuration... Done.

System will now restart!
Licensing the Controller

A license for the Next Generation Policy Enforcement Firewall Module must be installed for the firewall features and Spectralink voice prioritization to work. Please contact your local Aruba representative. License Management can be performed using the License Wizard of the WebUI.

You will need
- The Serial Number of the Mobility Controller.
- The License Certificate Number of the service to be activated (Please contact your local Aruba team).

Obtain the license Key from: https://licensing.arubanetworks.com

On the WebUI
1. Click the Configuration tab.
2. On the tabs list, click Licenses.
3. Click Add by Add New License Key (scroll down to see option).
4. Enter the license Key in the space provided and click OK.
5. Repeat 3 and 4 for all the licenses desired.
6. Click Save Configuration.
7. Verify that the licenses show up on the table in the same screen.
8. Centralized Licensing and a license server may also be used. See the Aruba User’s Guide for details.
Installing the license

To obtain license keys via the web:
- Licensing web: [https://license.arubanetworks.com](https://license.arubanetworks.com)
- You will need the following:
  - The serial number of the switch or supervisor module
  - The license certificate number of the service you wish to activate
  - The serial number to use for this switch or AC3002154

User License Usage:
- License Limit: 8192
- License Used: 0
- License Available: 8192
- License Exceeded: 0

AP Licenses:
- Total: 32
- Remaining: 31

License Table:

<table>
<thead>
<tr>
<th>License Type</th>
<th>Key</th>
<th>Installed</th>
<th>Expires</th>
<th>Flages</th>
<th>Service Type</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Generation Policy Enforcement Firewall Module</td>
<td>2011-08-03 16:54:54</td>
<td>Never</td>
<td>E</td>
<td>Next Generation Policy Enforcement Firewall Module: 32</td>
<td>DELETE</td>
<td></td>
</tr>
</tbody>
</table>

Flags: A = auto-generated; E = enabled; R = robust required to activate

Add New License Key

Save Report | Export Database | Import Database
### Version 6.5

**License Information**

#### Service Status and Current Limits

<table>
<thead>
<tr>
<th>Service</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Points</td>
<td>16</td>
</tr>
<tr>
<td>RF Protect</td>
<td>0</td>
</tr>
<tr>
<td>VPN Server Module</td>
<td>4096</td>
</tr>
<tr>
<td>xSec Module</td>
<td>0</td>
</tr>
<tr>
<td>Next Generation Policy Enforcement Firewall Module</td>
<td>16</td>
</tr>
<tr>
<td>Advanced Cryptography</td>
<td>0</td>
</tr>
<tr>
<td>WebCC</td>
<td>0</td>
</tr>
<tr>
<td>Beta AP</td>
<td>0</td>
</tr>
<tr>
<td>RF Protect</td>
<td>DISABLED</td>
</tr>
<tr>
<td>Policy Enforcement Firewall</td>
<td>ENABLED</td>
</tr>
<tr>
<td>VPN Server</td>
<td>ENABLED</td>
</tr>
<tr>
<td>xSec Module</td>
<td>DISABLED</td>
</tr>
<tr>
<td>Policy Enforcement Firewall for VPN users</td>
<td>DISABLED</td>
</tr>
<tr>
<td>Advanced Cryptography</td>
<td>DISABLED</td>
</tr>
<tr>
<td>Maritime Regulatory Domain</td>
<td>DISABLED</td>
</tr>
<tr>
<td>WebCC</td>
<td>DISABLED</td>
</tr>
<tr>
<td>Beta AP</td>
<td>DISABLED</td>
</tr>
</tbody>
</table>

#### AP Licenses

<table>
<thead>
<tr>
<th>License Type</th>
<th>Alphabetical</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Licenses</td>
<td>16</td>
</tr>
<tr>
<td>RLM Licenses</td>
<td>16</td>
</tr>
<tr>
<td>Overall AP License Limit</td>
<td>16</td>
</tr>
</tbody>
</table>

#### AP Usage

<table>
<thead>
<tr>
<th>Usage Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active CAs</td>
<td>2</td>
</tr>
<tr>
<td>Standby CAs</td>
<td>0</td>
</tr>
<tr>
<td>RAs</td>
<td>0</td>
</tr>
<tr>
<td>Remote-node APs</td>
<td>0</td>
</tr>
<tr>
<td>Tunneled nodes</td>
<td>0</td>
</tr>
<tr>
<td>Total APs</td>
<td>2</td>
</tr>
</tbody>
</table>

#### Remaining AP Capacity

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAs</td>
<td>14</td>
</tr>
<tr>
<td>RAs</td>
<td>14</td>
</tr>
</tbody>
</table>

### License Table

<table>
<thead>
<tr>
<th>License</th>
<th>Key</th>
<th>Installed</th>
<th>Expires (Grace period expires)</th>
<th>Flags</th>
<th>Service Type</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>E656FC7D1D-57d9f8f0-d758d8ef-c9b8ca8b-e9de5e2b3c5</td>
<td>2016-06-27 12:22:39</td>
<td>Never</td>
<td>E</td>
<td>Access Points: 32</td>
<td>Delete</td>
<td></td>
</tr>
<tr>
<td>S/jedixa-77x21f-p-f0d9a2-c7-f0g8bo-e9de5e2b3c5</td>
<td>2016-06-27 12:22:31</td>
<td>Never</td>
<td>E</td>
<td>Next Generation Policy Enforcement Firewall Module: 32</td>
<td>Delete</td>
<td></td>
</tr>
</tbody>
</table>

**License Type**
- A - auto-generated
- E - enabled
- S - Subscription
- R - rollout required to activate

Add New License Key

Save Report | Export Database | Import Database
Chapter 3: Configure the Environment

Logical and Physical Interfaces

This section defines the Layer 2/3 framework that connects the Spectralink phones with the WLAN Mobility Controller (MC) and the Access Points. The requirement is that the phones and Spectralink infrastructure be connected over Layer-2 and have the L2 subnet span across L3 switching/routing fabric.

The steps involved are

1. Define a VLAN for voice on the WLAN.
2. Define the IP parameters for the VLAN.
3. Enable IGMP for use in the Push-to-talk function in the handsets.
4. Turn on the use of proxy ARP.
5. Define the DHCP server for the phones to get their IP addresses.
6. Define the physical port assignment on the MC. Most deployments have the MC uplinked to a Layer-3 switch which performs routing functions.

These parameters can be easily defined using the Controller Wizard on the WebUI.

Using CLI

IP Interfaces, VLAN configuration

(Aruba651) #configure terminal
(Aruba651) (config) #vlan <vlan ID>
(Aruba651) (config) #interface <vlan ID>
(Aruba651) (config-subif) #ip igmp proxy <port(s) in use for PTT>
(Aruba651) (config-subif) #ip local-proxy-arp
(Aruba651) (config-subif)#ip helper-address <DHCP server / helper for the VLAN>
(Aruba651) (config-subif)#write m
(Aruba651) (config-subif)#end

Physical Port Assignment

The uplink is configured as follows

(Aruba651) (config) #interface gigabitethernet <slot/port>
(Aruba651) (config-if)#trusted
(Aruba651) (config-if)#no shutdown
(Aruba651) (config-if)#switchport mode trunk
(Aruba651) (config-if)#switchport trunk allowed vlan <VLAN IDs>

Uplink Security Definition

For 6.5, add:
(Aruba7502) (config-if)#trusted
(Aruba7502) (config-if)#trusted vlan <x-xxxx>
(Aruba7502) (config-if)#ip access-group “uplink-firewall” session
(Aruba651) (config-if)#write memory

On the WebUI

1. Click the **Configuration** tab.
2. On the left pane, click **Controller** under **WIZARDS**.
3. The **Basic Info** and **Licenses** fields should be auto-filled from the previous steps. Click **Next** on both to arrive at the **VLANs and IP Interfaces** page.
4. Highlight the default VLAN line and click on it. (Other VLAN’s may be entered here: see Aruba documentation for details.)
5. Enter details for the VLAN on which the phones are desired – VLAN ID, VLAN-Name.
   a. Click the drop-down to enter an IP address for the VLAN interface on the controller and the subnet mask. (Please bear in mind that L2 connectivity is required for the phones to reach the voice server and gateway).
   b. Click to choose the ports assigned to the VLAN (default is all available ports).
   c. Specify details on how the phones are expected to get their IP addresses. This drop-down offers the option of static IP assignment (**None**), DHCP using the in-built DHCP server (**Act as server**) and DHCP using an external DHCP server (**Relay to external**).

Version 6.3, 6.4
### Version 6.5

<table>
<thead>
<tr>
<th>Name</th>
<th>VLANs (on this controller)</th>
<th>IP address/netmask</th>
<th>IPv6 address</th>
<th>Enable NAT</th>
<th>Port Members</th>
<th>DHCP settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td></td>
<td>172.29.109.168/255.255.255.0</td>
<td></td>
<td></td>
<td></td>
<td>Relay to external</td>
</tr>
</tbody>
</table>

6. Click Save Configuration

7. Click Next to proceed to Connectivity assignment.
   a. Enter the IP address for the Default Gateway or pick Dynamic if the default gateway will be provided by DHCP, DNS, or router infrastructure.
   b. Click Next.

8. Version 6.5 only. Define policies and behavior for Uplink. On **Uplink for {Controller Name}**
   i. To define which ports of the controller are used for Uplink, click on **Edit** and move them to the **Selected** column.
ii Enable Uplink FireWall and define uplink-firewall policies as desired. See Aruba documentation for details.

iii Select which protocols are to be used for Management Interfaces.

c Define the VLAN/Prot relationship.

9 By default, all ports are on VLAN 1.

a To change port configuration, click the corresponding row.

b If the controller has a single uplink to the wired network, check the Trunk Mode box for the port and include the VLANs to be trunked on that port.

c If the controller has only one uplink, STP should be disabled.

10 Click Next twice, then click finish to save the changes to the configuration.

11 Enable igmp and local proxy ARP on the VLAN(s).

a Navigate to Configuration>NETWORK>IP.

b For each VLAN that supports handsets:

i Click on Edit in the row representing the VLAN.
ii  Click on the **Enable IGMP** radio button.

iii  Ensure that **Enable IGMP Snooping** is unchecked.

iv  Check the **Enable IGMP Proxy** radio button.

v  Check the interfaces/ports that will have PTT multicast traffic flowing through them.
Creating Firewall Roles and Policies

The Aruba MC has an application-aware stateful firewall that can assign prioritization to Spectralink voice traffic once it knows that a certain wireless client is a Spectralink handset. This is accomplished by the following steps:

1. Create a user role that the phones should be assigned to.
2. Create the syslog policy.
3. Assign firewall policies to the role.
4. Create a user-derivation rule that dictates how a client should be identified as a Spectralink voice phone. In this case it is easiest to classify based on the leading octets of the MAC OUI (00:90:7a).
5. Finally, create an AAA-profile that ties the user-derivation rule with the appropriate firewall rules.
Creating a Syslog Policy

On CLI

(Aruba651) (config) #ip access-list session syslog
(Aruba651) (config-sess-syslog) #any any svc-syslog permit

On WebUI

1. Click the Configuration tab.
2. Click Access Control.
3. Click Policies.
4. Click Add.
5. Set the Policy name to syslog, the policy type to Session/
6. Click on Add under Rules.
7. Set the Service/Application to service, the service name to svc-syslog (udp-514), and the action to permit.
8 Click **Add**, then **Apply**.
**Creating User-Role and Assigning Firewall Rules to the Role**

Creating a User-Role Derivation Rule

**On CLI**

```plaintext
(Aruba651) (config) # aaa derivation-rules user spectralink-derivation

(Aruba651) (user-rule) # set role condition macaddr starts-with 00:90:7a set-value spectralink

(Aruba651) (user-rule) # write memory
```

**On WebUI**

1. Click the **Configuration** tab.
2. Click **Authentication**.
3. Click **User Rules** and click **Add**.
4. Type a name for the user rules, such as spectralink-derivation.
5. Click **Add**.
6. Click the newly entered name in the tree in the left column.
7. Click **Add**.
8. Fill the following parameters
   a. **Set Type** – Role
   b. **Rule Type** – MAC Address
   c. **Condition** – starts with
   d. **Value** – 00:90:7a
   e. **Roles** – <select role created for phones> (spectralink in this example).
9. On the right hand side, under Misc. Configuration, ensure that Enable Deep Packet Inspection is not checked if WMM CaC is to be used.
10. Click **Add** and then **Apply**.
11. Click **Save Configuration**.
Assigning Firewall Rules to the Role

On CLI

(Aruba651) (config) #user-role spectralink

Disable deep packet inspection if WMM CaC is to be used.

(Aruba651) (config) #dpi disable

(Aruba651) (config-role) #access-list session sip-acl position 1
(Aruba651) (config-role) #access-list session tftp-acl position 2
(Aruba651) (config-role) #access-list session icmp-acl position 3
(Aruba651) (config-role) #access-list session dhcp-acl position 4
(Aruba651) (config-role) #access-list session syslog position 5
(Aruba651) (config-role) #access-list session dns-acl position 6
(Aruba651) (config-role) #access-list session lync-acl position 7
(Aruba651) (config-role) #access-list session http-acl position 8
(Aruba651) (config-role) #access-list session https-acl position 9
(Aruba651) (config-role) #access-list session ntp-acl position 10
(Aruba651) (config-role) #access-list session ftp-acl position 11
Admin Tip: Enter applications in firewall list
Ensure that applications installed on the phone are entered into the firewall list for the Spectralink role as needed. ipv6 services are not shown here and may need to be added.

On WebUI

1. Click the Configuration tab.
2. Click Access Control.
3. Click on the User Roles tab.
4. Click on the spectralink role defined above.
5. Click on Edit.
7. Click the Choose from configured policies radio-button.
8. From the drop down list select, sip-acl, tftp-acl, icmp-acl, dhcp-acl, dns-acl, lync-acl, http-acl, https-acl, ntp-acl, ftp-acl, and syslog policies to the list, clicking Done after each selection and repeating from step 5.
9. Click Apply at the bottom of the page.
10. Click Save Configuration.

Admin Tip: Enter applications in firewall list
Ensure that applications installed on the phone are entered into the firewall list for the Spectralink role as needed.
### Security > User Roles > Add Role

**Role Name**

<table>
<thead>
<tr>
<th>Name</th>
<th>Role Owner</th>
<th>AP Group</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Re-authorization Interval**

- **Disabled**
- **Change** (in doubles, re-authorization takes place when less authentication is performed)

**Role VLAN ID**

- **Not Assigned**
- **Assigned**

**Bandwidth Contract**

- **Upstream Not Enhanced**
- **Downstream Not Enhanced**

**Network Access**

- **Pre-Login**
- **Post-Login**
Chapter 4: Configure Wireless Security

Configuration Steps for None, WEP, WPA-PSK or WPA2-PSK Security

Creating an Authentication Profile for controller-based authentication

On CLI

(Aruba651) (config) # aaa authentication dot1x default

Use the next four statements if using an external Radius server

(Aruba651) (802.1X Authentication Profile "default") #termination enable
(Aruba651) (802.1X Authentication Profile "default") #termination eap-type eap-tls
(Aruba651) (802.1X Authentication Profile "default") #termination eap-type eap-peap
(Aruba651) (802.1X Authentication Profile "default") #termination inner-eap-type eap-mschapv2
(Aruba651) (802.1X Authentication Profile “default”) #exit

(Aruba651) (config) aaa authentication dot1x "spectralink-psk"
(Aruba651) (802.1X Authentication Profile “spectralink-psk”) #machine-authentication machine-default-role spectralink
(Aruba651) (802.1X Authentication Profile “spectralink-psk”) #machine-authentication user-default-role spectralink
(Aruba651) (802.1X Authentication Profile “spectralink-psk”) #timer idrequest_period 65535
#exit

(Aruba651) #configure terminal aaa profile spectralink-aaa
(Aruba651) (AAA Profile "spectralink-aaa") #initial-role authenticated
(Aruba651) (AAA Profile "spectralink-aaa") #authentication-dot1x spectralink-psk
On WebUI

1. Navigate to Configuration and Authentication.
2. Click the L2-Authentication tab.
3. Click 802.1X Authentication Profile in the middle-pane to expand the tree and click default.
   a. On the right pane, check Termination. (Check these values if using an external Radius server.)
   b. For Termination EAP-Type, click eap-peap and eap-tls.
   c. For Termination Inner EAP-Type, check eap-mschapv2.
   d. Click Apply.

4. Navigate to Configuration>Authentication>L2 Authentication and click 802.1X Authentication Profile in the middle pane.

5. On the right pane, enter a name for the new profile such as spectralink-psk and click Add
   a. On the left pane under 802.1X Authentication, click on the name just created.
   b. On the right pane, unclick all radio boxes. Enter the role spectralink in the dropdown for the Machine Authentication default roles as shown:
c Click on the **Advanced** pane and enter 65535 for the **Interval between Identity Requests** as shown:
d Touch **Apply**

6 Click the **AAA Profiles** page and on the right-pane, click **Add**.

7 Assign a name to the AAA profile (Ex. spectralink-aaa) and click **Add**.

   a Click the newly created profile name.

   b Set the **Initial role** to **authenticated**.

   c Set the **MAC Authentication Default Role** and the **802.1X Authentication Default Role** to the role created for Spectralink phones, i.e. spectralink.
d) Drop-down the list against **User derivation rules** and select the role created for the Spectralink phones.

e) Click **Apply**.

### Security > Authentication > Profiles

<table>
<thead>
<tr>
<th>AAA Profile</th>
<th>spectralink-aaa</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial role</td>
<td>authenticated</td>
</tr>
<tr>
<td>MAC Authentication Default Role</td>
<td>spectralink</td>
</tr>
<tr>
<td>802.1X Authentication Default Role</td>
<td>spectralink</td>
</tr>
<tr>
<td>Download Role from CPPM</td>
<td></td>
</tr>
<tr>
<td>Set username from dhcp option 12</td>
<td></td>
</tr>
<tr>
<td>L2 Authentication Fail Through</td>
<td></td>
</tr>
<tr>
<td>Multiple Server Accounting</td>
<td></td>
</tr>
<tr>
<td>User idle timeout</td>
<td></td>
</tr>
<tr>
<td>Max IPv4 for wireless user</td>
<td>2</td>
</tr>
<tr>
<td>RADIUS Interim Accounting</td>
<td></td>
</tr>
<tr>
<td>User derivation rules</td>
<td>spectralink-derivation</td>
</tr>
<tr>
<td>Wired to Wireless Roaming</td>
<td>1</td>
</tr>
<tr>
<td>SIP authentication role</td>
<td>--NONE--</td>
</tr>
<tr>
<td>Device Type Classification</td>
<td>1</td>
</tr>
<tr>
<td>Enforce DHCP</td>
<td></td>
</tr>
<tr>
<td>PAN Firewall Integration</td>
<td></td>
</tr>
<tr>
<td>Open SSID radius accounting</td>
<td></td>
</tr>
</tbody>
</table>

8) Click on **802.1X Authentication** underneath the **spectralink-aaa** profile entry.

a) From the dropdown list by **802.1X Authentication Profile**, select the profile just created, i.e **spectralink-psk**

b) Click **apply**.

9) Click **Save Configuration**.
**Security > Authentication > Profiles**

### Basic
- **Max authentication failures**: 0
- **Enforce Machine Authentication**: [ ]
- **Machine Authentication**: Default: [ ]
- **Cache Timeout**: 24 [h]
- **Blacklist on Machine Authentication Failure**: [ ]
- **Machine Authentication**: Default: [ ]
- **Interval between Identity Requests**: 65535 [sec]
- **Quiet Period after Failed Authentication**: 30 [sec]
- **Reauthentication Interval**: 84400 [sec]
- **Use Server provided Reauthentication Interval**: [ ]
- **Use the termination-action attribute from the Server**: [ ]
- **Multicast Key Rotation Time Interval**: 1800 [sec]
- **Unicast Key Rotation Time Interval**: 900 [sec]
- **Authentication Server Retry Interval**: 5 [sec]
- **Authentication Server Retry Count**: 0
- **Pramed MTU**: 1100 [bytes]
- **Number of times ID-Requests are retried**: 5
- **Maximum Number of Reauthentication Attempts**: 3
- **Maximum number of times Held State can be bypassed**: 0
- **Dynamic WEP Key Message Retry Count**: 1
- **Dynamic WEP Key Size**: 128 [bits]
- **Interval between WPA/WPA2 Key Messages**: 1000 [msec]
- **Delay between EAP-Success and WPA2 Unicast Key Exchange**: 0 [msec]
- **Delay between WPA/WPA2 Unicast Key and Group Key Exchange**: 0 [msec]
- **Time interval after which the PMKSA will be deleted**: 8 [h]
- **Delete Keycache upon user deletion**: [ ]
- **WPA/WPA2 Key Message Retry Count**: 9
- **Multicast Key Rotation**: [ ]
- **Unicast Key Rotation**: [ ]

<table>
<thead>
<tr>
<th>Commands</th>
<th>View Commands</th>
</tr>
</thead>
</table>

---

**Spectralink VIEW Certified Configuration Guide: Aruba, a Hewlett Packard Enterprise company**
**Configuration Steps for WPA2-Enterprise Security**

**Defining an 802.1X authentication server**

**On CLI**

(Aruba651) (config) #aaa authentication-server radius <server-name>

(Aruba651) (RADIUS Server "spectralink-dot1x") #host <server IP>

(Aruba651) (RADIUS Server "spectralink-dot1x") #key <RADIUS secret>

(Aruba651) (RADIUS Server "spectralink-dot1x") #write memory

**On WebUI**

1. Navigate to Configuration > Authentication > Servers.
2. Click RADIUS Server, name server profile (Ex. Spectralink-dot1x) and click Add.
3. Click the newly created instance to configure.
4. Input the IP address of the external RADIUS server and the pre-shared key.

![Settings: Define Aruba Controller on Radius with the same secret](image)

The Aruba mobility controller should be defined as a dot1x client on the RADIUS server and configured with the same secret as in step 4 above.

5. Click Apply and Save Configuration.
Settings: Define OKC on the 84-Series

Fast roaming must be set to **Opportunistic Key Caching** (OKC) on the handset when WPA2-Enterprise is in use. It is enabled by default on the controller. PIVOT handsets automatically detect the type of fast roaming necessary.
Create a Server Group and Add the RADIUS Server

Using CLI

(Aruba651) #configure terminal
(Aruba651) (config) #aaa server-group < Server Name >
(Ex. Spectralink)
(Aruba651) (Server Group "Spectralink") # auth-server "Spectralink-dot1x" position 1
(Aruba651) (Config) #aaa profile "Spectralink-dot1x"
(Aruba651) (AAA Profile ""Spectralink-dot1x") #dot1x-server-group "Spectralink"

Using WebUI

1. Navigate to Configuration and Authentication.
2. Click the Servers tab. Click the Server Group.
3. In the right pane click Add and create a new server group (Ex. Spectralink).
4. Click the newly created server group.
5. Click New under Servers tab.
6. Assign the required RADIUS server under Server Name, click Add Server and Apply button.
7. Click Save Configuration.
Creating an 802.1X Authentication Profile

Using CLI

(Aruba651) (config) #aaa authentication dot1x <profile-name>

If termination is required (the Radius server is external)

(Aruba651) (802.1X Authentication Profile "spectralink-dot1x")
#termination enable
(Aruba651) (802.1X Authentication Profile "spectralink-dot1x")
#machine-authentication machine-default-role spectralink
(Aruba651) (802.1X Authentication Profile "spectralink-dot1x")
#machine-authentication user-default-role spectralink
(Aruba651) (802.1X Authentication Profile "spectralink-dot1x")
#termination eap-type eap-peap
(Aruba651) (802.1X Authentication Profile "spectralink-dot1x")
#termination eap-type eap-tls
(Aruba651) (802.1X Authentication Profile "spectralink-dot1x")
#termination inner-eap-type eap-mschapv2
(Aruba651) (802.1X Authentication Profile "spectralink-dot1x") #wpa-fast-handover
(Aruba651) (802.1X Authentication Profile "spectralink-dot1x")
#voice-aware

Using WebUI

1. Navigate to Configuration and Authentication.
2. Click the L2 Authentication tab.
3. Click 802.1X Authentication.
4. Fill in a name and click Add and create a new profile (Ex. spectralink-dot1x).
5. Click the newly created name under 802.1X Authentication.
6. Click on the Advanced tab:
   a. Click the newly created instance and enable termination. Specify the Termination EAP-Type to be eap-peap and eap-tls and the Inner-EAP-Type to be eap-mschapv2.
   b. Set the Machine Authentication: Default Machine Role and Machine Authentication: Default User Role to the role defined for spectralink phones, i.e. spectralink.
   c. Ensure that Opportunistic Key Caching and Validate PMKID are checked.
d For version 6.5+: **WPA Fast-Handover** may be checked if the SSID is shared with other phones that support 802.11r.

e For version 6.5+ ensure that **Disable rekey and reauthentication for clients on call** is checked.

7 Click **Apply** and **Save Configuration**.
Creating an Authentication Profile

Using CLI

(Aruba651) #configure terminal aaa profile <profile-name>
(Aruba651) (AAA Profile "spectralink-dot1x") #authentication-dot1x <
name of 802.1x profile created above, i.e. spectralink-dot1x >
(Aruba651) (AAA Profile "spectralink-dot1x") #dot1x-server-group
<dot1x authentication server name>
(Aruba651) (AAA Profile "spectralink-dot1x") #mac-default-roled
<spectralink user defined role>
(Aruba651) (AAA Profile "spectralink-dot1x") #dot1x-default-role
<spectralink user define role>
(Aruba651) (AAA Profile "spectralink-dot1x") #user-derivation-rules
"spectralink-derivation"

Using WebUI

1. Navigate to Configuration and Authentication.
2. Click the AAA Profiles tab.
3. Click Add and create a new profile (Ex. spectralink-dot1x).
4. Click on the name of the newly created profile on the left pane.
   a. Change the User derivation rules (Ex. spectralink-derivation) to the user-role created for the phones.
   b. Change the Mac Authentication Default Role and the 802.1X Authentication Default Role to the user role created for the phones.
   c. Click 802.1X Authentication Profile and specify the newly created profile.
5. On the left pane, click under the newly created name on 802.1X Authentication. Select the 802.1X Authentication Profile created in the last section (i.e. spectralink-dot1x) from the dropdown list.
6. On the left pane, click under the newly created name on 802.1X Authentication Server Group and enter the name created in the section above for the Radius server group.
7. Click Apply and Save Configuration.
Chapter 5: Configure Wireless LAN

This section defines the wireless network parameters that are most aptly suited to the Spectralink phones.

It is required to have separate SSID for the Spectralink phones and other data clients. Also, certain parameters need to be modified to allow seamless interoperability of Spectralink phones in and out of call with Aruba’s Adaptive Radio Management (ARM) mechanism. Aruba OS accomplishes this by creating independent profiles for the SSID definition, radio definition and ARM definitions before tying them together to an AP-group on which they would operate. This way, all APs configured to be part of the AP-group will have the same operational parameters. The steps in this procedure are below

1. Create an SSID profile – each SSID profile is characterized by the ESSID and the authentication-encryption scheme.
2. Create a VOIP CaC profile that defines the bandwidth limits for calls per AP.
3. Create a HT-SSID profile (with 802.11n features enabled or disabled as appropriate for the deployed network) and assign the HT-SSID to the SSID profile.
4. Create a Virtual-AP profile that ties the SSID profile and authentication profile (created in the previous section) with a VLAN on the wired-side.
5. Create a Traffic Management Profile that allocates all of the bandwidth tracked by bandwidth control to the virtual AP profile defined for voice. (Other clients will have their own virtual AP profiles with their own tracking.)
6. Create Radio-profiles for the 2.4 GHz and 5 GHz radio. This would include ARM and HT-Radio profile settings. In this example, we modify the default radio profiles which are assigned to the Virtual-AP automatically.
7. Associate the Virtual-AP with an AP-group.

The WLAN configuration for 802.1X authentication is identical to that for PSK-based authentication except for the following 2 points

- In Creating a SSID-profile, encryption (opmode) on the SSID should be set to wpa2-aes.
- The AAA profile for the Virtual-AP should be set to the newly created dot1x profile (spectralink-dot1x).

On CLI

Creating a SSID-profile

(Aruba651) #configure terminal wlan ssid-profile view
For None (open network – no security) #opmode opensystem
For WEP

(Aruba651) (SSID Profile "view") #opmode static-wep
(Aruba651) (SSID Profile "view") #weptxkey <index 1-4>
(Aruba651) (SSID Profile "view") #wepkey<index> <"string of hex characters”>

For WPA-PSK

(Aruba651) (SSID Profile "view") #opmode wpa-psk-tkip
(Aruba651) (SSID Profile "view") #wpa-passphrase <"passphrase”>

For WPA2-PSK

(Aruba651) (SSID Profile "view") #opmode wpa2-aes-psk
(Aruba651) (SSID Profile "view") #wpa-passphrase < "passphrase”>

For all

(Aruba651) (SSID Profile "view") #dtim-period 1
(Aruba651) (SSID Profile "view") #wmm
(Aruba651) (SSID Profile "view") #wmm-uapsd
(Aruba651) (SSID Profile "view") #max-retries 8
(Aruba651) (SSID Profile "view") #max-tx-fail 0
(Aruba651) (SSID Profile "view") #wmm-vi-dscp 40
(Aruba651) (SSID Profile "view") #wmm-vo-dscp 46
(Aruba651) (SSID Profile "view") #wmm-be-dscp 0
(Aruba651) (SSID Profile "view") #wmm-bk-dscp 0
(Aruba651) (SSID Profile "view") #no wmm-override-dscp-mapping
(Aruba651) (SSID Profile "view") #wmm-ts-min-inact-in 0
(Aruba651) (SSID Profile "view") #no strict-svp
(Aruba651) (SSID Profile "view") #essid view
(Aruba651) (SSID Profile "view") #a-tx-rates 6 9 12 18 24 36 48 54
(Aruba651) (SSID Profile "view") #g-basic-rates 5 11
(Aruba651) (SSID Profile "view") #g-tx-rates 5 6 11 12 18 24 36 48 54
(Aruba651) (SSID Profile "view") #max-tx-fail 0
Creating a Virtual-AP

(Aruba651) #configure terminal wlan virtual-ap spectralink-vap
(Aruba651) (Virtual AP Profile “spectralink-vap”)#no broadcast-filter arp
(Aruba651) (Virtual AP Profile “spectralink-vap”)#vlan 1

Creating a VoIP CAC profile

In the CLI commands below, use the bandwidth from the table below that corresponds to the codec the phones on the network will be using. As described in Spectralink 84-Series Wireless Telephone Administration Guide, the 84-Series handsets support the codecs shown in the table below. If the configuration is not changed from the default described in the reference, the codec used will be the one shown first in the table that is supported by the other side of the call. The 84-Series handsets can be configured to add the optional codecs shown in the table. This feature is used when communicating with desksets with high definition audio.

Choose the bandwidth from the table below that is the smallest number needed to support the type of phones or codecs expected so that the number of calls will be limited to what the AP can support.

WMM-AC is supported on PIVOT handsets running R1.5 and later.

84-Series, PIVOT handset Codecs

<table>
<thead>
<tr>
<th>Codec</th>
<th>Radio</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.722</td>
<td>5.0 GHz</td>
<td>3200</td>
</tr>
<tr>
<td>G.722</td>
<td>2.4 GHz</td>
<td>2000</td>
</tr>
<tr>
<td>G.722.1 (32 kbps)</td>
<td>5.0 GHz</td>
<td>2000</td>
</tr>
<tr>
<td>G.722.1 (32 kbps)</td>
<td>2.4 GHz</td>
<td>1600</td>
</tr>
<tr>
<td>G.711Mu-law</td>
<td>5.0 GHz</td>
<td>3200</td>
</tr>
<tr>
<td>G.711Mu-law</td>
<td>2.4 GHz</td>
<td>2400</td>
</tr>
<tr>
<td>G.711A-law</td>
<td>5.0 GHz</td>
<td>3200</td>
</tr>
<tr>
<td>G.711A-law</td>
<td>2.4 GHz</td>
<td>2400</td>
</tr>
<tr>
<td>G.729AB</td>
<td>5.0 GHz</td>
<td>1200</td>
</tr>
</tbody>
</table>
**Codec** | **Radio** | **Bandwidth**
---|---|---
G.729AB | 2.4 GHz | 1000

**Generally disable deep packet inspection if CAC is enabled**

(Aruba651)# configure terminal
(Aruba651)# voice alg-based-cac disable
(Aruba651)# wlan voip-cac-profile "8400_g"
(Aruba651)(VoIP Call Admission Control profile "8400_g")#call-admission-control
(Aruba651)(VoIP Call Admission Control profile "8400_g")#bandwidth-cac
(Aruba651)(VoIP Call Admission Control profile "8400_g")#bandwidth-capacity 2400
(Aruba651)(VoIP Call Admission Control profile "8400_g")#wmm-tspec-enforcement-period 3
(Aruba651)(VoIP Call Admission Control profile "8400_g")#send-sip-status-code client none
(Aruba651)(VoIP Call Admission Control profile "8400_g")#send-sip-status-code server none

**Changing AP EDCA profile**

(Aruba651) #configure terminal wlan edca-parameter-profile ap AC_ON
(Aruba651) # video acm 1
(Aruba651) # voice acm 1

Or

(Aruba651) #configure terminal wlan edca-parameter-profile ap AC_OFF
(Aruba651) # video acm 0
(Aruba651) # voice acm 0

**Changing station EDCA profile**

(Aruba651) #configure terminal wlan edca-parameter-profile station AC_ON
(Aruba651) # video acm 1
(Aruba651) # voice acm 1

Or

(Aruba651) # configure terminal wlan edca-parameter-profile station AC_OFF
(Aruba651) # video acm 0
(Aruba651) # voice acm 0

**HT-SSID profile (disable 802.11n network)**

(Aruba651) # configure terminal wlan ht-ssid-profile ht-disabled
(Aruba651) (High-throughput SSID profile "ht-disabled") # no high-throughput-enable
(Aruba651) (High-throughput SSID profile "ht-disabled") # no 40MHz-enable
(Aruba651) (High-throughput SSID profile "ht-disabled") # no 80MHz-enable
(Aruba651) (High-throughput SSID profile "ht-disabled") # no mpdu-agg

**HT-SSID profile (enable 802.11n network)**

(Aruba651) # configure terminal wlan ht-ssid-profile ht-enabled
(Aruba651) (High-throughput SSID profile "ht-enabled") # high-throughput-enable

For 12x and 13x APs, set the maximum number of MSDUs in an A-MSDU on best-effort AC and the maximum number of MSDUs in an A-MSDU on background AC both to 10. For 11n APs with model numbers smaller than 12x, set these values to 3.

Set the Maximum number of MSDUs in an A-MSDU on video AC and Maximum number of MSDUs in an A-MSDU on voice AC both to 3.

**Admin Tip: A-MSDU Aggregation Settings**

The AP-125 and AP-135 and newer AP’s can process 10 packets per background and best effort aggregation. Older 11n AP’s have better performance with a setting of 3 packets per background and best effort aggregation. Voice and video should remain with 3 packets per aggregation to avoid audible/visible latency issues.

**Admin Tip: Disable A-MPDU on handset SSIDs**

The Spectralink handsets do not implement A-MPDU aggregation. They cause extra traffic by declining Block ACK requests. It eliminates extra traffic to disable A-MPDU traffic on SSIDs used for handset traffic.
Admin Tip: 802.11n and A-MSDU and A-MPDU settings

The A-MSDU and A-MPDU settings described in this section are not necessary for a phone with 802.11n disabled.

Spectralink PIVOT phone software R2.4 and above disables 802.11n by default. Therefore after a factory reset, 802.11n will be disabled in phones running R2.4 and above. A simple update from an earlier version will not disable 802.11n. Only a factory reset will reset the default to disabled. Check to see if 802.11n is disabled by navigating to Admin menu> Developer options> Disable 802.11n. Yes means 802.11n is disabled.

For the 84-Series, R5.3 and above disables 802.11n along with phones manufactured after a certain date. Check to see if 802.11n is disabled by navigating to Settings> Status> Diagnostics> WiFi Stats> [Press the Next softkey to get to the screen] [2/6] General Information. It will say 802.11n= Disabled. If it needs to be changed, edit the following parameter either in the wireless.cfg file or if using CMS, as a custom setting. The parameter is device.wifi.dot11n.enabled. Yes is 1, No is 0.

(Aruba651) (High-throughput SSID profile "ht-enabled") #max-tx-a-msdu-count-be <3 or 10, depending on AP model>
(Aruba651) (High-throughput SSID profile "ht-enabled") #max-tx-a-msdu-count-bk <3 or 10, depending on AP model>
(Aruba651) (High-throughput SSID profile "ht-enabled") #max-tx-a-msdu-count-vi 3
(Aruba651) (High-throughput SSID profile "ht-enabled") #max-tx-a-msdu-count-vo 3
(Aruba651) (High-throughput SSID profile "ht-enabled") #no mpdu-agg

For 80 MHz network
(Aruba 3600) (High-throughput SSID profile "ht-enabled") #80-MHz-enable

Note: the AP must be power cycled for the 80 MHz setting to take effect.

For 40 MHz network:
(Aruba651) (High-throughput SSID profile "ht-enabled") #40MHz-enable
(Aruba 3600) (High-throughput SSID profile "ht-enabled") #no 80-MHz-enable

For 20 MHz network
(Aruba651) (High-throughput SSID profile "ht-enabled") #no 40MHz-enable
(Aruba651) (High-throughput SSID profile "ht-enabled") #no 80MHz-enable
(Aruba651) (High-throughput SSID profile "ht-enabled")

**Admin Tip: Paired channel recommendation**

40 MHz (paired) channels are not recommended by Aruba on the 2.4 GHz radio band.

(Aruba651) (High-throughput SSID profile "ht-enabled") #mpdu-agg
If WEP or no security is desired to be allowed (Aruba651) (High-throughput SSID profile “ht-enabled”) #allow-weak-encryption

**Assigning HT-SSID and EDCA profiles to the SSID-Profile**

(Aruba651) #configure terminal wlan ssid-profile view
(Aruba651) (SSID Profile "view") #ht-ssid-profile <ht-disabled or ht-enabled>
(Aruba651) (SSID Profile "view") #edca-parameters-profile station <AC_OFF or AC_ON>
(Aruba651) (SSID Profile "view") #edca-parameters-profile ap <AC_OFF or AC_ON>

**Adding the aaa-profile and the ssid-profile to the virtual-ap profile**

(Aruba651) (config) #wlan virtual-ap spectralink-vap
(Aruba651) (Virtual AP profile "spectralink-vap") #aaa-profile spectralink-aaa
(Aruba651) (Virtual AP profile "spectralink-vap") #ssid-profile spectralink-dot1x

**Creating Radio profiles**

In most cases, one can use the default Radio-profile, HT-Radio profile and ARM profile and modify them as required. If there are multiple AP-groups on the network that require different radio profiles, please refer to the ArubaOS User Guide to create and assign radio-profiles to AP-Groups.

**5 GHz Radio settings**

(Aruba651) (config) #rf dot11a-radio-profile default

Enable or disable 5 GHz radio

(Aruba651) (802.11a radio profile “default”) #<no> radio-enable

Choose a channel
Enable 80 MHz or not

(Aruba651) (802.11a radio profile “default”)#<no> very-high-throughput enable

Enable 40 MHz or not

(Aruba651) (802.11a radio profile “default”)#<no> high-throughput enable

Admin Tip: Transmit Power

For setting up the Transmit Power, please consult your facility’s RF site survey, designed for voice traffic, to determine if you have sufficient coverage to support all data rates. Spectralink Wireless Telephones require the following minimum dBm reading to support the corresponding Mandatory data rate setting in the access point.

<table>
<thead>
<tr>
<th>802.11 Radio Standard</th>
<th>Minimum Available Signal Strength (RSSI)</th>
<th>Maximum &quot;Mandatory&quot; Data Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a</td>
<td>-67 dBm</td>
<td>6 Mb/s</td>
</tr>
<tr>
<td></td>
<td>-50 dBm</td>
<td>54 Mb/s</td>
</tr>
</tbody>
</table>

Web Info: RF Deployment reference

For additional details on RF deployment please see the Deploying Enterprise-Grade Wi-Fi Telephony White Paper.

(Aruba651) (802.11a radio profile “default”)#tx-power <transmit EIRP in .5 dBm increments)

(Aruba651) (802.11a radio profile “default”)#no spectrum-load-balancing

If DFS channels (shared with radar) are used on 802.11a/n radio, the following commands to alter the default radio profile or other defined radio profile will be necessary

(Aruba651) (802.11a radio-profile “default”) #csa
(Aruba651) (802.11a radio-profile “default”) #csa-count 4
(Aruba651) (802.11a radio-profile “default”) #dot11h

2.4 GHz Radio settings
(Aruba651) (config) #rf dot11g-radio-profile default

Enable or disable 2.4 GHz radio
(Aruba651) (802.11g radio profile “default”)#<no> radio-enable

Choose a channel
(Aruba651) (802.11g radio profile “default”)#channel <desired channel>

Disable 40 MHz
(Aruba651) (802.11b radio profile “default”)#<no> high-throughput enable

Admin Tip: Transmit Power
For setting up the Transmit Power, please consult your facility’s RF site survey, designed for voice traffic, to determine if you have sufficient coverage to support all data rates. Spectralink Wireless Telephones require the following minimum dBm reading to support the corresponding Mandatory data rate setting in the access point.

<table>
<thead>
<tr>
<th>802.11 Radio Standard</th>
<th>Minimum Available Signal Strength (RSSI)</th>
<th>Maximum &quot;Mandatory&quot; Data Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11b</td>
<td>-65 dBm</td>
<td>11 Mb/s</td>
</tr>
<tr>
<td>802.11g</td>
<td>-67 dBm</td>
<td>6 Mb/s</td>
</tr>
<tr>
<td>802.11g</td>
<td>-47 dBm</td>
<td>54 Mb/s</td>
</tr>
</tbody>
</table>

Web Info: RF Deployment reference
For additional details on RF deployment please see the Deploying Enterprise-Grade Wi-Fi Telephony White Paper.

(Aruba651) (802.11g radio profile “default”)#tx-power <transmit EIRP in .5 dBm increments)
(Aruba651) (802.11g radio profile “default”)#no spectrum-load-balancing

Assigning the HT Radio Profiles to the Virtual AP
(Aruba651)# config terminal wlan virtual-ap spectralink-vap
(Aruba651) (Virtual AP profile "spectralink-vap") #configure
terminal rf ht-radio-profile default-g
(Aruba651) (Virtual AP profile "spectralink-vap") #configure
terminal rf ht-radio-profile default-a

Creating an ARM profile
(Aruba 3600) #configure terminal rf arm-profile default
(Aruba 3600) (Adaptive Radio Management (ARM) profile “default”) 
#assignment <disable or maintain >
(Aruba 3600) (Adaptive Radio Management (ARM) profile “default”) #
voip-aware-scan
(Aruba 3600) (Adaptive Radio Management (ARM) profile “default”) #
40MHz-allowed a-only
(Aruba 3600) (Adaptive Radio Management (ARM) profile “default”) #
client-aware
(Aruba 3600) (Adaptive Radio Management (ARM) profile “default”) #
no active-scan
(Aruba 3600) (Adaptive Radio Management (ARM) profile “default”) #
ota-updates
(Aruba 3600) (Adaptive Radio Management (ARM) profile “default”) #
scanning
(Aruba 3600) (Adaptive Radio Management (ARM) profile “default”) #
multi-band-scan
(Aruba 3600) (Adaptive Radio Management (ARM) profile “default”) #
voip-aware-scan
(Aruba 3600) (Adaptive Radio Management (ARM) profile “default”) #
power-save-aware scan
(Aruba 3600) (Adaptive Radio Management (ARM) profile “default”) #
video-aware-scan
(Aruba 3600) (Adaptive Radio Management (ARM) profile “default”) #
no client-match
(Aruba 3600) (Adaptive Radio Management (ARM) profile “default”) #
write memory

Assigning properties to an AP-Group

Virtual AP assignment
(Aruba651) #configure terminal ap-group default
(Aruba651) (AP group "default") #virtual-ap spectralink-vap
(Aruba651) (AP group "default") #voip-cac-profile "8400_g"

Normally, one would have to assign the Radio-profile to an AP-Group. But this example uses the default radio profiles which are assigned to the default AP-Group automatically.

On WebUI

Creating a Virtual-AP

1. Navigate to Configuration and AP Configuration.
2. Click Edit against the default AP-Group.
3. Click Wireless LAN and Virtual AP.
4. Click Add.
5. On the right-pane, select NEW under Add a profile and enter a profile name (Ex., spectralink-vap) and click Add.
6. Click on the newly entered name and enter the following options
   a. Check Virtual AP enable.
   b. Allowed band – all (or select a band, if the design calls for voice on only one band).
   c. Select the VLAN where the voice handsets would reside.
   d. In the right pane, uncheck Convert Broadcast ARP requests to unicast.
   e. Click Apply.
### Versions 6.3, 6.4

#### Configuration > AP Group > Edit "default"

<table>
<thead>
<tr>
<th>Profiles</th>
<th>Profile Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless LAN</td>
<td>Virtual AP enable</td>
</tr>
<tr>
<td></td>
<td>VLAN</td>
</tr>
<tr>
<td></td>
<td>Forward mode</td>
</tr>
<tr>
<td></td>
<td>Allowed band</td>
</tr>
<tr>
<td></td>
<td>Band Steering</td>
</tr>
<tr>
<td></td>
<td>Steering Mode</td>
</tr>
<tr>
<td></td>
<td>Dynamic Multicast Optimization (DMO)</td>
</tr>
<tr>
<td></td>
<td>Dynamic Multicast Optimization (DMO) Threshold</td>
</tr>
<tr>
<td></td>
<td>Drop Broadcast and Multicast</td>
</tr>
<tr>
<td></td>
<td>Convert Broadcast ARP requests to unicast</td>
</tr>
<tr>
<td></td>
<td>Authentication Failure Blacklist Time</td>
</tr>
<tr>
<td></td>
<td>Blacklist Time</td>
</tr>
<tr>
<td></td>
<td>Deny inter user traffic</td>
</tr>
<tr>
<td></td>
<td>Deny time range</td>
</tr>
<tr>
<td></td>
<td>DoS Prevention</td>
</tr>
<tr>
<td></td>
<td>HA Discovery on-association</td>
</tr>
<tr>
<td></td>
<td>Mobile IP</td>
</tr>
<tr>
<td></td>
<td>Preserve Client VLAN</td>
</tr>
<tr>
<td></td>
<td>QoS QoE VLAN</td>
</tr>
<tr>
<td></td>
<td>QoS QoE VLAN 0</td>
</tr>
<tr>
<td></td>
<td>Remote-AP Operation</td>
</tr>
<tr>
<td></td>
<td>Station Blacklisting</td>
</tr>
<tr>
<td></td>
<td>Strict Compliance</td>
</tr>
<tr>
<td></td>
<td>VLAN Mobility</td>
</tr>
</tbody>
</table>

---

**Dashboard**

- **WIZARDS**
  - AP
  - Controller
  - Campus WLAN
  - Remote AP
  - AirWave
- **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
    - Threshold
    - ADVANCED SERVICES
      - Redundancy
      - AirGroup
      - IP Mobility
      - Stateful Firewall
Creating a SSID-profile

1. Click the newly created virtual-ap in the left-hand Virtual AP list.

2. Click **SSID profile**.
   
   a. On the right pane, select **NEW** and enter an SSID-profile name (Ex., spectralink).
   
   b. Enter the desired SSID-name.
   
   c. When Spectralink phones are configured for None (not recommended, but useful for provisioning), under **Network Authentication**, select **None**, and under **Encryption**, select **Open**.
   
   d. When Spectralink phones are configured for WEP, under **Network Authentication**, select **None**, and under **Encryption**, select **WEP**. For the 40 Bits key on the Spectralink phone, use the 64-bit key Aruba setting, entering 10 hex digits. For the
104-bit key on the Spectralink phone, use the 128-bit key Aruba setting, entering 26 hex digits.

e  WPA-PSK is no longer available through the Web GUI. It must be entered with the following cli commands:

(Aruba651) #configure terminal wlan ssid-profile view
(Aruba651) (SSID Profile “view”) #opmode wpa-psk-tkip
(Aruba651) (SSID Profile “view”) #wpa-passphrase <“passphrase”>

f  When Spectralink phones are configured for WPA2-PSK under Network Authentication, select WPA2-PSK and Open under Encryption. Enter a preshared key in either Hex or as a passphrase.

g  When Spectralink phones are configured for WPA2-Enterprise, under Network Authentication select WPA and AES under Encryption.

h  Click Apply

3  Click the Advanced tab on the right pane and make the following changes

a  DTIM Interval – 1

b  802.11g transmit rates – check 5, 6, 9, 11, 12, 18, 24, 36, 48, 54.

c  802.11g basic rates – check 5, 11

d  802.11a transmit rates – check, 6, 9, 12, 18, 24, 36, 48, 54.

e  802.11a basic rates – check 6, 12, 24

f  Check Wireless Multimedia (WMM).

g  Check Wireless Multimedia U-APSD (WMM-UAPSD) Powersave

h  Set Max Transmit Attempts to 8.

i  Set DSCP mapping for WMM voice AC to 46 to match Spectralink phone setting

j  Set DSCP mapping for WMM video AC to 40 to match Spectralink phone setting

k  Set WMM TSPEC inactivity interval to 3600000 msec, or when available, 0.

l  Set DSCP mapping for WMM best-effort AC to 0.

m  Set DSCP mapping for background AC to 0.

n  Ensure that Override DSCP mappings for WMM clients is NOT checked.

o  Ensure that Maximum Transmit Failures is set to 0 to disable deauthentication of the handsets when acks are not received.

p  Ensure that Enable OKC is checked, if the option is given in the controller software version in use
q Ensure that **Enable Management Frame Protection** and **Require Management Frame Protection** are unchecked where the options are available.

r Ensure that **Strict Spectralink Voice Protocol (SVP)** is unchecked.

4 Click **Apply** and **Save Configuration**.

**Versions 6.3, 6.4**
### Spectralink VIEW Certified Configuration Guide: Aruba, a Hewlett Packard Enterprise company

#### Configuration > AP Group > Edit "default"

<table>
<thead>
<tr>
<th>Profiles</th>
<th>Profile Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Station Access Time 1000 sec</td>
</tr>
<tr>
<td></td>
<td>Max Transmit Attempts 8</td>
</tr>
<tr>
<td></td>
<td>RTS Threshold 1333 bytes</td>
</tr>
<tr>
<td></td>
<td>Short Pendable 10</td>
</tr>
<tr>
<td></td>
<td>Max Associations 84</td>
</tr>
<tr>
<td></td>
<td>Wireless Multimedia (MM) 10</td>
</tr>
<tr>
<td></td>
<td>Wireless Multimedia UAPSD (WMM-UAPSD) PowerShine 0</td>
</tr>
<tr>
<td></td>
<td>WMM TPSC Min Inactivity Interval 1500000 mc</td>
</tr>
<tr>
<td></td>
<td>Override DSCP mappings for WMM clients 0</td>
</tr>
<tr>
<td></td>
<td>DSCP mapping for video AC 48</td>
</tr>
<tr>
<td></td>
<td>DSCP mapping for video AC 40</td>
</tr>
<tr>
<td></td>
<td>DSCP mapping for video AC 0</td>
</tr>
<tr>
<td></td>
<td>DSCP mapping for WMM background AC 0</td>
</tr>
<tr>
<td></td>
<td>Multiple Tx Transmit Counters 0</td>
</tr>
<tr>
<td></td>
<td>Mode SSD 0</td>
</tr>
<tr>
<td></td>
<td>DSCP Overwrite Protocols 0</td>
</tr>
<tr>
<td></td>
<td>Local Probe Request Threshold (DB) 10</td>
</tr>
<tr>
<td></td>
<td>Disable Probe Retry 10</td>
</tr>
<tr>
<td></td>
<td>Battery Boost 0</td>
</tr>
<tr>
<td></td>
<td>WEP Key 1 Encryption 0</td>
</tr>
<tr>
<td></td>
<td>WEP Key 2 Encryption 0</td>
</tr>
</tbody>
</table>

#### Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Apply</th>
<th>View Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5  Click **EDCA Parameters AP profile** and select the profile for the Spectralink phones from the dropdown.

6  Change **ACM field** under the **Video and Voice AC** to 1.
7. Click **EDCA Parameters Station** profile and select the profile for the Spectralink phones from the dropdown (Ex. Default If it is not desired to use the default EDCA Parameters profile, a new profile can be created, as shown in the example.)

Change **ACM field** under **Video and Voice AC** to 1 only if PIVOT handsets are not present in the network.

8. Click **Apply** and **Save Configuration**.
Creating a VoIP CAC Profile

In the VoIP Call Admission Control Profile screen below, use the bandwidth from the table below that corresponds to the codec the phones on the network will be using. As described in Spectralink 84-Series Wireless Telephone Administration Guide, the 84-Series handsets support the codecs shown in the table below. If the configuration is not changed from the default described in the reference, the codec used will be the one shown first in the table that is supported by the other side of the call. The 84-Series handsets can be configured to add the optional codecs shown in the table. This feature is used when communicating with desksets with high definition audio.

Choose the bandwidth from the table below that is the smallest number needed to support the type of phones or codecs expected so that the number of calls will be limited to what the AP can support.

8000 Series Phones

<table>
<thead>
<tr>
<th>Codec</th>
<th>Radio</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>5.0 GHz</td>
<td>1500</td>
</tr>
<tr>
<td>All</td>
<td>2.4 GHz</td>
<td>1100</td>
</tr>
</tbody>
</table>
### 84-Series handsets Default Codecs (in priority order)

<table>
<thead>
<tr>
<th>Codec</th>
<th>Radio</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.722</td>
<td>5.0 GHz</td>
<td>3200</td>
</tr>
<tr>
<td>G.722</td>
<td>2.4 GHz</td>
<td>2000</td>
</tr>
<tr>
<td>G.722.1 (32 kbps)</td>
<td>5.0 GHz</td>
<td>2000</td>
</tr>
<tr>
<td>G.722.1 (32 kbps)</td>
<td>2.4 GHz</td>
<td>1600</td>
</tr>
<tr>
<td>G.711Mu-law</td>
<td>5.0 GHz</td>
<td>3200</td>
</tr>
<tr>
<td>G.711Mu-law</td>
<td>2.4 GHz</td>
<td>2400</td>
</tr>
<tr>
<td>G.711A-law</td>
<td>5.0 GHz</td>
<td>3200</td>
</tr>
<tr>
<td>G.711A-law</td>
<td>2.4 GHz</td>
<td>2400</td>
</tr>
<tr>
<td>G.729AB</td>
<td>5.0 GHz</td>
<td>1200</td>
</tr>
<tr>
<td>G.729AB</td>
<td>2.4 GHz</td>
<td>1000</td>
</tr>
</tbody>
</table>

### 84-Series handsets Configurable Codecs

<table>
<thead>
<tr>
<th>Codec</th>
<th>Radio</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.722.1 (16 kbps)</td>
<td>5.0 GHz</td>
<td>1400</td>
</tr>
<tr>
<td>G.722.1 (16 kbps)</td>
<td>2.4 GHz</td>
<td>1000</td>
</tr>
<tr>
<td>G.722.1 (24 kbps)</td>
<td>5.0 GHz</td>
<td>1800</td>
</tr>
<tr>
<td>G.722.1 (24 kbps)</td>
<td>2.4 GHz</td>
<td>1400</td>
</tr>
<tr>
<td>L16.8 (128 kbps)</td>
<td>5.0 GHz</td>
<td>6000</td>
</tr>
<tr>
<td>L16.8 (128 kbps)</td>
<td>2.4 GHz</td>
<td>4700</td>
</tr>
<tr>
<td>L16.16 (256 kbps)</td>
<td>5.0 GHz</td>
<td>5800</td>
</tr>
<tr>
<td>L16.16 (256 kbps)</td>
<td>2.4 GHz</td>
<td>4400</td>
</tr>
</tbody>
</table>
1 Note: this command disables deep packet inspection for SIP and must be used from the cli for proper WMM Access Control (TSPEC) operation. No GUI equivalent is currently available:

(Aruba651)# configure terminal
(Aruba651)# voice alg-based-cac disable

2 Click **AP Configuration**.

3 Click **QoS**.

4 On the right pane, select **NEW** and enter a Cac profile name (Ex., 8400_g).

5 Click **Apply**.

6 Click the newly created profile name
   a Click **VoIP Call Admission Control Profile**.
   b Check **VoIP Call Admission Control**, **Enable only WMM-AC CAC**, and **VoIP Bandwidth based CAC**.
   c Enter the bandwidth from the table in the **VoIP Bandwidth Capacity (kbps)** as described above.
   d Uncheck **VOIP TSPEC Enforcement**, **VoIP Send SIP 100 Trying**, and **VoIP Disconnect Extra Call**.
   e Select **none** from the **VoIP Drop SIP…** dropdown lists.
   f Click **Apply** and **Save Configuration**.
Creating a High Throughput SSID profile for an 802.11n-disabled network

1. Click High Throughput SSID Profile.
2. Drop down on the right pane and select NEW. Provide name (Ex., ht-disabled).
3. Modify the following
   a. Uncheck High Throughput enable.
4. Click Apply.
Creating a High-Throughput SSID profile for an 802.11n-enabled network

1. Click **High-Throughput SSID Profile**.

2. On the right pane, click on the **Advanced** tab.

3. Drop down on the right-pane and select **NEW**. Provide name (Ex., ht-enable-80).

4. Modify the following
   a. Check **High-Throughput enable**.
   b. Check **40 MHz channel usage** or uncheck for 20 MHz usage.
   c. Check **Very High throughput enable (SSID)** and **80 MHz channel usage (VHT)** if available or uncheck not to use 80 MHz. Note: the AP must be power cycled for the 80 MHz setting to take effect.

5. Click **Save Configuration**.
Admin Tip: Paired channel recommendation
40 MHz (paired) channels are not recommended by Aruba on the 2.4 GHz radio band.

d Ensure that Temporal Diversity Enable is unchecked.
e Uncheck MPDU Aggregation.

Admin Tip: Disable A-MPDU on handset SSIDs
The Spectralink handsets do not implement A-MPDU aggregation. They cause extra traffic by declining Block ACK requests. It eliminates extra traffic to disable A-MPDU traffic on SSIDs used for handset traffic.

Admin Tip: 802.11n and A-MSDU and A-MPDU settings
The A-MSDU and A-MPDU settings described in this section are not necessary for a phone with 802.11n disabled.

Spectralink PIVOT phone software R2.4 and above disables 802.11n by default. Therefore after a factory reset, 802.11n will be disabled in phones running R2.4 and above. A simple update from an earlier version will not disable 802.11n. Only a factory reset will reset the default to disabled. Check to see if 802.11n is disabled by navigating to Admin menu> Developer options> Disable 802.11n. Yes means 802.11n is disabled.

For the 84-Series, R5.3 and above disables 802.11n along with phones manufactured after a certain date. Check to see if 802.11n is disabled by navigating to Settings> Status> Diagnostics> WiFi Stats> [Press the Next softkey to get to the screen] [2/6] General Information. It will say 802.11n= Disabled. If it needs to be changed, edit the following parameter either in the wireless.cfg file or if using CMS, as a custom setting The parameter is device.wifi.dot11n.enabled. Yes is 1, No is 0.

f Check Legacy Stations. Note: this is not necessary if there are no non-11n devices in the network.
g Check Short guard interval in 20 MHz mode.
h Check Short guard interval in 40 MHz mode.
i For 12x and 13x AP’s, set the Maximum number of MSDUs in an A-MSDU on best-effort AC and the Maximum number of MSDU’s in an A-MSDU on background AC both to 10. For 11n AP’s with model numbers smaller than 12x, set these values to 3.
j Set the **Maximum number of MSDUs in an A-MSDU on video AC** and **Maximum number of MSDUs in an A-MSDU on voice AC** both to 3.

---

**Admin Tip: A-MSDU Aggregation Settings**

The AP-125 and AP-135 and newer AP’s can process 10 packets per background and best effort aggregation. Older 11n AP’s have better performance with a setting of 3 packets per background and best effort aggregation. Voice and video should remain with 3 packets per aggregation to avoid audible/visible latency issues.

---

5 Click **Apply**.

---

6 Click **Save Configuration**.

**Assigning an AAA-profile**

1 Click **AAA Profile** on the middle pane and select the AAA profile created for the voice devices (spectralink-aaa for non-enterprise security or spectralink-dot1x for enterprise security).

2 Click **Apply** and **Save Configuration**.
Assigning a 5 GHz Radio-profile

1. Click RF Management under the Virtual AP.
2. Click 802.11a radio-profile.
3. Click the Advanced tab.
   a. Click Radio enable to turn the 802.11a radio on.
   b. In the default profile on the right-pane, enter a 5 GHz channel.
   c. Clear or set the High throughput enable (radio) according to whether the radio is 802.11n-enabled mode or not.
   d. Choose a Transmit EIRP chosen to support the site survey plan and the maximum mandatory data rate as described immediately below.
Admin Tip: Transmit Power
For setting up the Transmit Power, please consult your facility’s RF site survey, designed for voice traffic, to determine if you have sufficient coverage to support all data rates. Spectralink Wireless Telephones require the following minimum dBm reading to support the corresponding Mandatory data rate setting in the access point.

<table>
<thead>
<tr>
<th>802.11 Radio Standard</th>
<th>Minimum Available Signal Strength (RSSI)</th>
<th>Maximum &quot;Mandatory&quot; Data Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a</td>
<td>-67 dBm</td>
<td>6 Mb/s</td>
</tr>
<tr>
<td></td>
<td>-50 dBm</td>
<td>54 Mb/s</td>
</tr>
</tbody>
</table>

Web Info: RF Deployment reference
For additional details on RF deployment please see the Deploying Enterprise-Grade Wi-Fi Telephony White Paper.

e If DFS channels are to be used (channels shared with radar applications)
f Click Advertise 802.11d and 802.11h Capabilities
g Click Enable CSA.
h Set CSA Count to 4.
i Ensure that Spectrum Load Balancing is unchecked.
4 Click Apply.
5 Click Adaptive Radio Management (ARM) profile and then the Advanced tab.

6 Enter the settings as follows
   a Ensure that Assignment is set to disable or maintain.
   b Set Allowed bands for 40MHz channels to a-only.
   c Check Client Aware.
   d Ensure that Active Scan is not checked.
   e Ensure that ARM Over the Air Updates, Scanning, Multi Band Scan, VoIP Aware Scan, Power Save Aware Scan, and Video Aware Scan are checked.
   f Ensure that Client Match is NOT checked.

7 Click Apply and Save Configuration.
8. **Click High-Throughput Radio profile** (default-a).
   
a. Ensure that CSD override is not checked.

b. **Click Apply** and **Save Configuration**.
Assigning a 2.4 GHz Radio-profile

1. Click **802.11g radio-profile**.

2. Click the **Advanced** tab.
   
   a. Click **Radio enable** to turn the 802.11g radio on.
   
   b. In the default profile on the right-pane, enter a 2.4 GHz channel.
   
   c. Clear or set the High throughput enable (radio) according to whether the radio is 802.11n-enabled mode or not. Use only a 20 MHz width.
   
   d. Choose a Transmit EIRP chosen to support the site survey plan and the maximum mandatory data rate as described immediately below.
Admin Tip: Transmit Power
For setting up the Transmit Power, please consult your facility’s RF site survey, designed for voice traffic, to determine if you have sufficient coverage to support all data rates. Spectralink Wireless Telephones require the following minimum dBm reading to support the corresponding Mandatory data rate setting in the access point.

<table>
<thead>
<tr>
<th>802.11 Radio Standard</th>
<th>Minimum Available Signal Strength (RSSI)</th>
<th>Maximum &quot;Mandatory&quot; Data Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11b</td>
<td>-65 dBm</td>
<td>11 Mb/s</td>
</tr>
<tr>
<td>802.11g</td>
<td>-67 dBm</td>
<td>6 Mb/s</td>
</tr>
<tr>
<td>802.11g</td>
<td>-47 dBm</td>
<td>54 Mb/s</td>
</tr>
</tbody>
</table>

Web Info: RF Deployment reference
For additional details on RF deployment please see the Deploying Enterprise-Grade Wi-Fi Telephony White Paper.
3. Click **Adaptive Radio Management (ARM) profile** and then the **Advanced** tab.

4. Enter the settings as follows:
   - **a.** Ensure that **Assignment** is set to **disable** or **maintain**.
   - **b.** Set **Allowed bands for 40MHz channels** to **a-only**.
   - **c.** Check **Client Aware**.
   - **d.** Ensure that **Active Scan** is not checked.
   - **e.** Ensure that **ARM Over the Air Updates, Scanning, Multi Band Scan, VoIP Aware Scan, Power Save Aware Scan**, and **Video Aware Scan** are checked.
   - **f.** Ensure that **Client Match** is NOT checked.
5. Click High-Throughput Radio profile (default-g) and then the Advanced tab.
   a. Ensure that CSD override is not checked.
   b. Click Apply.

6. Click Save Configuration.
At this point, the Mobility Controller is ready to provide Spectralink voice services.

****END OF DOCUMENT****