



Polycom VIEW Certified Configuration Guide

Cisco

**2100/4400/5500 Series WLC (Wireless LAN Controller),
WiSM (Wireless Services Module) and 3750G Integrated WLC
with 104x, 113x, 114x, 120x, 123x, 124x, 125x, 126x, 350x, 360x APs**

Trademarks

©2012, Polycom, Inc. All rights reserved.

POLYCOM®, the Polycom "Triangles" logo and the names and marks associated with Polycom products are trademarks and/or service marks of Polycom, Inc. and are registered and/or 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 Polycom.

Disclaimer

While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

Limitation of Liability

Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.

Customer Feedback

We are striving to improve the quality of our documentation and we appreciate your feedback. Email your opinions and comments to VoiceDocumentationFeedback@polycom.com.



Visit support.polycom.com for software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.

Contents

- Introduction.....5**
 - Certified Product Summary 5
 - Known Limitations 6
 - Polycom References..... 6
 - Product Support..... 7

- Chapter 1: Configuration for Wi-Fi Standard QoS or CCXv4 Operation9**
 - Overview 9
 - Network Topology 10
 - Configuring a New Controller Starting from Factory Defaults..... 11
 - Connecting to the Controller Via a Browser 11
 - Installing Software 12
 - Controller Setup..... 13
 - Connecting APs 14
 - AP Configuration 16
 - Configuration for handsets running in 802.11b , b/g mixed mode, g only mode in 8020/8030 phones or 2.4 GHz in 8400 phones 16*
 - Configuring 802.11n..... 22*
 - Configuration for handsets running in 802.11a mode in the 8020/8030 phones and using the 5 GHz radio in the 8400 series phones 23*
 - Configuring 802.11n:..... 27*
 - Setting up the SSID..... 29
 - Setting up the EDCA parameters profile..... 33
 - Configuration for handsets running in 802.11b/g mode, 802.11b and b/g mixed mode, or 802.11 g only mode in 8020/8030 phones or 2.4 GHz in 8400 phones 33*

- Chapter 2: Configuration for SVP Operation.....35**
 - Introduction 35
 - Network Topology 35
 - Configuring a New Controller Starting from Factory Defaults..... 36
 - Connecting to the Controller via a Browser 37
 - Installing Software 38
 - Controller Setup..... 39
 - Connecting APs 40
 - AP Configuration 42

Configuration for handsets running in 802.11b & b/g mixed and g only mode with 7.0 and 7.2 versions of controller software..... 42

Configuration for handsets running in 802.11a mode..... 47

Setting up the SSID..... 51

Appendix A55

Introduction

Polycom’s Voice Interoperability for Enterprise Wireless (VIEW) Certification Program is designed to ensure interoperability and high performance between SpectraLink 8440/8450/8452 and 8020/8030 Wireless Telephones and WLAN infrastructure products.

The products listed below have been thoroughly tested in Polycom’s lab and have passed VIEW Certification. This guide describes the configuration of Cisco 2100/4400/5500 Series WLC (Wireless LAN Controller), WiSM (Wireless Services Module) and 3750G Integrated WLC with 104x, 113x, 114x, 120x, 123x, 124x, 125x, 126x, 350x, and 360x APs with SpectraLink wireless telephones.

Certified Product Summary

<i>Manufacturer:</i>	<i>Cisco Systems: www.cisco.com</i>			
Certified products:	Controllers:	APs:	123x	360x
	2100, 4400, 5500 Series WLC (Wireless LAN Controller)	104x	124x	
	3750G Integrated WLC	113x	125x	
	WiSM (Wireless Services Module)	114x	126x	
		120x	350x	
AP Radio(s):	2.4 GHz (802.11b/g/n), 5 GHz (802.11a/n)			
Security:	None, WEP, WPA-PSK, WPA2-PSK, WPA2-Enterprise (EAP-FAST and PEAPv0/MSCHAPv2) with CCKM (Cisco Centralized Key Management)** and OKC			
QoS:	Wi-Fi Standard for SpectraLink 8440/8450/8452 and 8020/8030 SVP for SpectraLink 8020/8030			
AP and WLC software version tested:	6.0.202.0 for 113x, 114x, 120x, 123x, 124x, and 125x APs 7.0.220.0 for 104x, 113x, 114x, 120x, 123x, 124x, 125x, 126x and 350x APs 7.2.103.0 for 104x, 113x, 114x, 120x, 123x, 124x, 125x, 126x, 350x and 360x APs			
Handset* models tested:	SpectraLink 8440/8450/8452 Wireless Telephone			
Handset radio mode:	802.11b	802.11b/g	802.11bgn	802.11a & 802.11an
Meets VIEW minimum call capacity per AP:	6 calls	10 calls	8 calls	10 calls
Handset models tested:	SpectraLink 8020/8030 Wireless Telephone			

Manufacturer:	Cisco Systems: www.cisco.com	
Handset radio mode:	802.11b & b/g mixed. 802.11 g only	802.11a
Meets VIEW minimum call capacity per AP:	6 (Wi-Fi Standard QoS)** 8 calls (SVP)	8 (Wi-Fi Standard QoS) ** 12 calls (SVP)
Network topology:	Switched Ethernet (recommended)	

*SpectraLink handset models and their OEM derivatives 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”. The 8440, 8450 (with 1D bar code reader), and 8452 (with 1D and 2D bar code reader) handsets will be referred to collectively as the 8400 handsets.

** Only Release 3.0 capable SpectraLink 8020/8030 handsets support WPA2-Enterprise, Wi-Fi Standard QoS, and CCXv4 (Cisco Compatible Extensions). Release 3.0 capable phone types connect to PBX’s that support IP telephony. Release 3.0 capabilities are not available for SpectraLink 8020/8030 handsets connecting to PBXs using the TDM protocol through a SpectraLink Telephony Gateway (phone type 30 on the 8020/8030).

Known Limitations

- SpectraLink 8400 handsets must be configured with 802.11n mode disabled when used with Cisco AP 114x and 125x with versions prior to 6.0.202.0. See Appendix A for configuration steps.
- Heavy multicast, broadcast or push-to-talk (PTT) traffic may impair voice quality.
- When SpectraLink Voice Priority (SVP) is enabled for SpectraLink 8020/8030 in the EDCA parameters setting, the 802.11n capabilities will be disabled on that radio when using Cisco 6.0 software versions (see Section 1: Configuring for SVP Operation → AP Configuration). It is therefore recommended to deploy handsets using SVP on a different radio than 802.11n clients.

Polycom References

Please refer to the Polycom *Deploying Enterprise-Grade Wi-Fi Telephony* white paper, available at http://www.polycom.com/products/voice/wireless_solutions/wifi_communications/handsets/SpectraLink_8020_wireless.html. This document covers the security, coverage, capacity and QoS considerations necessary for ensuring excellent voice quality with enterprise Wi-Fi networks.

For more detailed information on wireless LAN layout, network infrastructure, QoS, security and subnets, please see the *Best Practices Guide to Network Design Considerations for SpectraLink Wireless Telephones*, available at <http://support.polycom.com/PolycomService/support/us/support/voice/wi-fi/index.html>. This document identifies issues and solutions based on Polycom’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: Converting autonomous APs to Lightweight mode

This document does not cover the steps involved in converting autonomous APs to Lightweight mode such that they can be controlled by the Cisco WLCs. Please contact Cisco's Customer Support at www.cisco.com for instructions on this procedure. Once the APs are converted, this document can be used to provision APs.



Note: RADIUS server configuration

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

- Installation and configuration guides for Cisco Wireless LAN Controllers can be found on Cisco's website.
- To convert Autonomous APs to Lightweight mode, go to:
http://www.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwappnote.html
- For other assistance, contact either Cisco's or Polycom's customer service at:
www.cisco.com or www.polycom.com

Chapter 1: Configuration for Wi-Fi Standard QoS or CCXv4 Operation

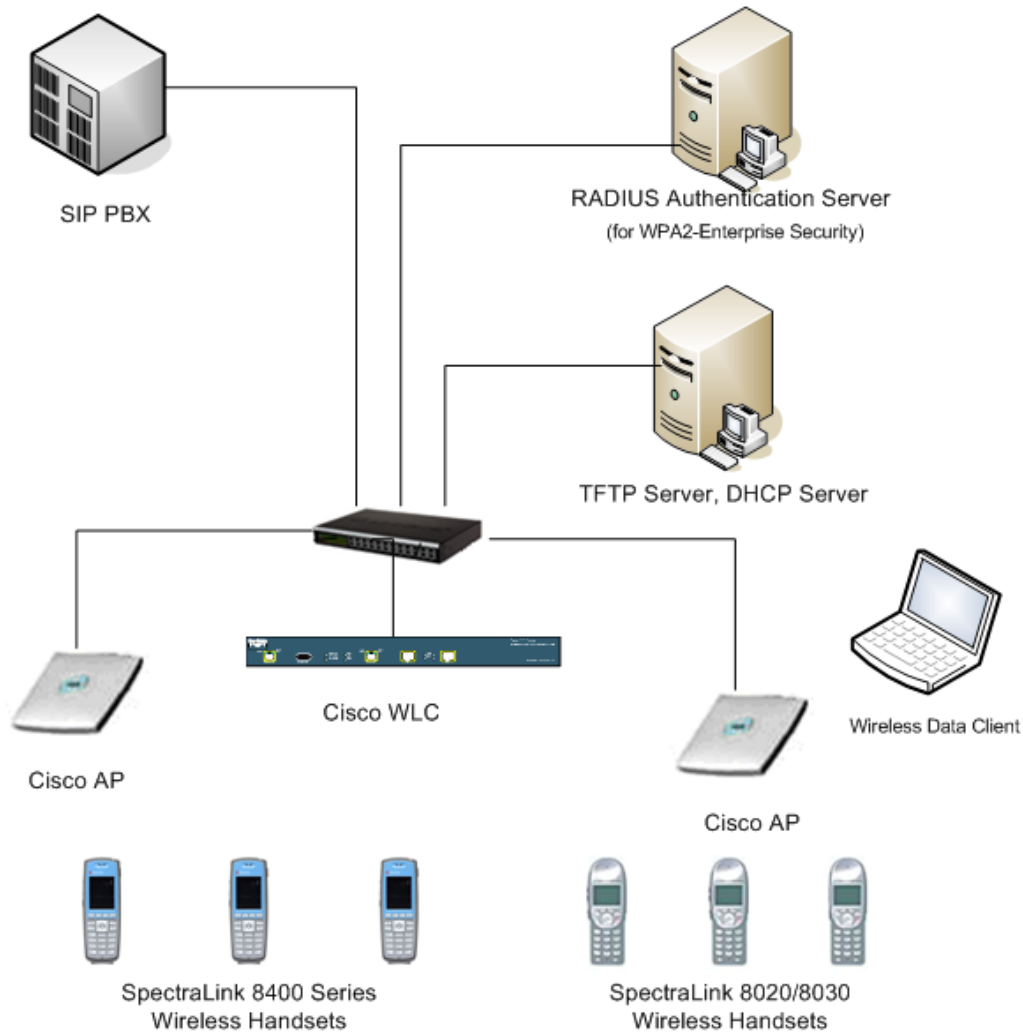
Overview

SpectralLink 8020/8030 phones can be configured with Wi-Fi Standard QoS from the WLAN Settings menu using either the Custom or CCX selection.

- If the Custom menu is selected, QoS Wi-Fi Standard is selected from the QoS submenu.
- If the CCX menu is selected from the WLAN Settings menu, Wi-Fi Standard QoS is used automatically without any further menu selections.

SpectralLink 8400 phones only support Wi-Fi Standard QoS. The phones are compatible with both networks configured with CCX (Cisco Compatible Extensions) and networks that are not configured with CCX, but they have not been CCX certified.

Network Topology



Note: Example configuration shown

This configuration is not applicable to all customer environments.

Configuring a New Controller Starting from Factory Defaults

Initial provisioning of the controller is done via the command line interface (CLI).

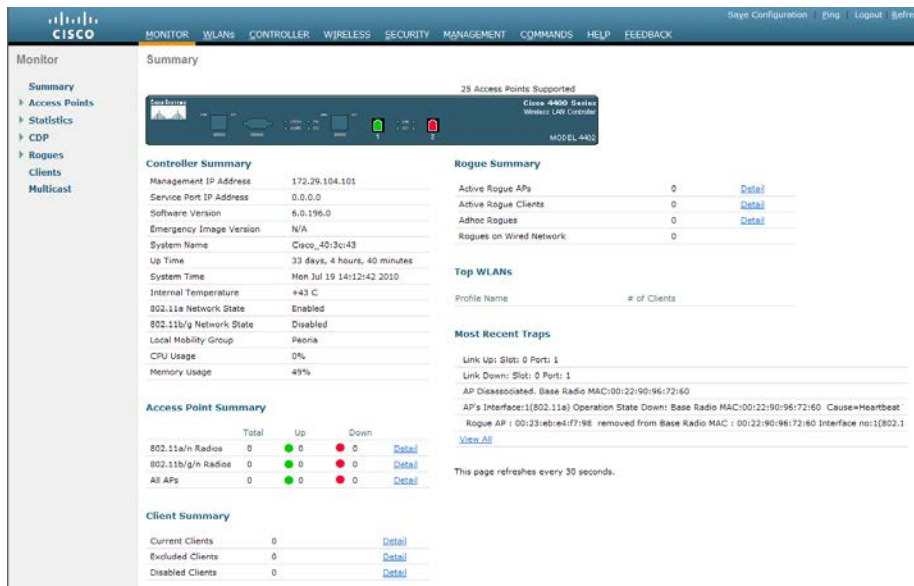
- 1 Connect a null modem serial cable between the console port of the controller and the serial port of a PC.
- 2 Open a terminal program, such as Hyper Terminal, and configure the port settings to 9600 baud, no parity, 8 data bits and 1 stop bit.
- 3 Power-on the controller. Status of the controller's boot process will appear as the controller is powering up. Once the controller is running, it will prompt you to run the Startup Wizard.
- 4 The Startup Wizard provides for an easy means to perform initial controller setup and provisioning. Refer to the *Installation and Startup Guide* for the Cisco 4400 Series WLC, or other appropriate controller, found at Cisco's website. This document contains a detailed explanation of using the Startup Wizard for the 4400:
<http://www.cisco.com/en/US/docs/wireless/controller/4400/quick/guide/ctrlv32.html#wp34023>
- 5 Once the controller has been configured via the Startup Wizard, the remaining configuration can be configured through the switch-web interface using a Web browser (Cisco recommends using MS IE 6.0+).
- 6 If necessary, the controller can be reset to factory defaults. To reset the WLC to factory default, you must reboot, then type **Recover-config** at the CLI. This only works before the first time a user logs in via the console.

A few advanced commands must be set from the command line interface after the rest of the controller has been configured. These are noted in the instructions below.

Connecting to the Controller Via a Browser

- 1 Connect to the WLC by pointing your internet browser to the URL: `https<IP_Addr>` (where `<IP_Addr>` is the IP address of the management interface of the WLC).
- 2 Click the **Login** prompt. The default **User Name** and **Password** is **admin**.

Once logged in properly, a page similar to the one below displays.



Installing Software

- 1 To check the installed version of software, listed in the **Product Summary**, click **Monitor** from the main menu.
- 2 In the navigation pane, click **Summary**. The heading labeled **Software Version** shows the current software version.
- 3 Download the appropriate software for your model of controller from the Cisco website.
- 4 Set up a Trivial File Transfer Protocol (TFTP) server running on a PC to download the file to the controller.
- 5 From the main menu, click **Commands**.
- 6 In the navigation pane, click **Download File**.
- 7 Fill in the download parameters:
 - a For **File Type**, select **Code**.
 - b For **TFTP Server**, type in the IP Address of the TFTP server.
 - c Add the **File Path** (this is the path in the TFTP server's root directory and not the system path where the TFTP server is located) and **File Name** of the firmware file to download.

(Note the example simply uses the /designator for the root TFTP directory.) Point the TFTP server to the code.

- 8 Click **Download** and allow a few minutes for the download to complete.

- 9 Reboot the Controller.

Controller Setup

The initial setup of the controller is shown below.



Note: Example only

The setup instructions outlined in this document are for the configuration shown in the diagram only. Your configuration may differ, and the appropriate adjustments must be made.



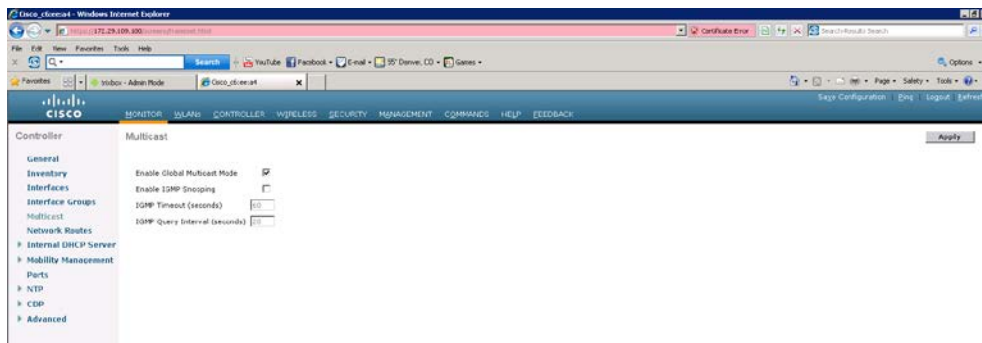
Note: The WLC will provision the APs

It is not necessary to configure each AP individually. The WLC is capable of provisioning the APs.

- 1 From the main menu, click **Controller**.
- 2 Set the **AP Multicast Mode** to **Multicast** and enter a multicast IP address that is currently not being used on your network for the **Multicast Group Address**.
- 3 Click the **Apply** button.

- 4 Click **Multicast** from the options on the left side of the screen
- 5 Select **Enable Global Multicast Mode** checkbox

6 Click the **Apply** button.



7 Click **Save Configuration**.

Connecting APs

As the APs are connected to the network, they should automatically find the controller via the CAPWAP discovery algorithms. The Dynamic Host Configuration Protocol (DHCP) server will assign each AP an IP address.



Note: DHCP server

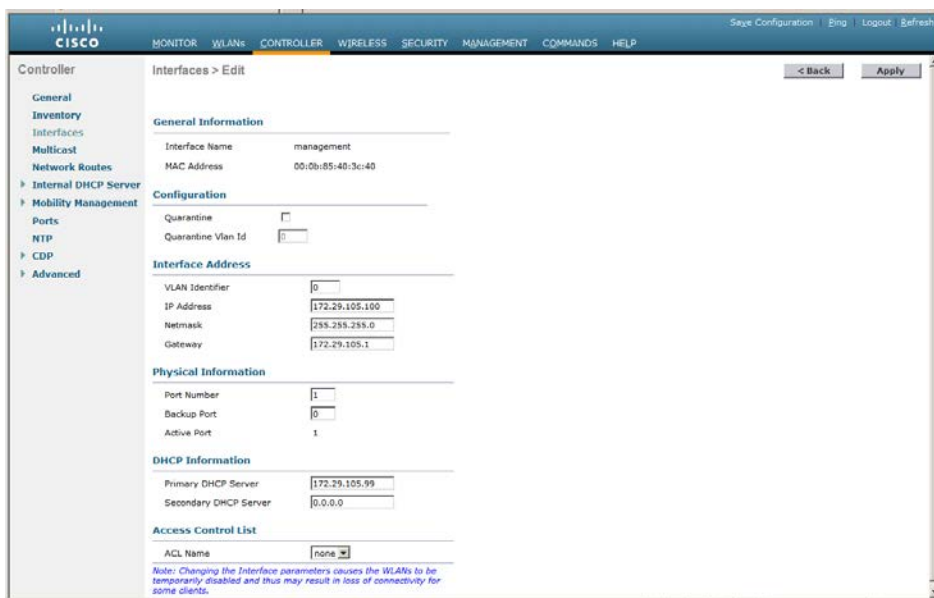
You can configure a DHCP server to run on a remote PC for a small deployment. However, for large-scale deployments, an enterprise-grade DHCP server must be used.

The **ap-manager** and **management** interfaces' configuration should include the DHCP server you have configured. Alternately, you can configure the DHCP server internally on the controller to hand out leases to the connected clients. (Note: The WLC's DHCP server does not lease addresses to the AP.) The instructions for doing so are included at the end of this document.

- 1 From the main menu, click **Controller**.
- 2 In the navigation pane, click **Interfaces**. Verify that the proper IP addresses are assigned to the interfaces.
- 3 Under **Interface Name** click **management**. Note: the screenshots are from a Cisco 4400. The 2100 does not contain a service-port interface. The 5500 does not contain an ap-manager interface. If the interface is not present on the model being configured, no values need to be entered.



- 4 Under **DHCP Information**, enter the IP address of the **Primary DHCP Server**.
- 5 Repeat this step for the **ap-manager** interface, if present on the model configured.
- 6 Click the **Apply** button and save the changes.



- 7 Under service-port, (if present), enter a valid IP Address and Netmask in a different subnet than the management interface.
- 8 Click the **Apply** button and save the changes.



AP Configuration



Note: QoS

All handsets operating on a given AP radio must have the same QoS setting. All APs supporting the handsets must be configured to enable the corresponding features.

- 1 Power-on and connect the APs to the network. Wait a few minutes for the APs to find the controller.
- 2 Verify the APs are associated to the WLC.
- 3 From the main menu, click **Monitor**.

The screenshot shows the Cisco WLC Monitor interface. The main content area is titled 'Summary' and displays '12 Access Points Supported'. It includes a 'Controller Summary' table with fields like Management IP Address (172.29.105.100), Service Port IP Address (0.0.0.0), Software Version (6.0.188.0), and System Name (Cisco_40:3c:143). There is also a 'Rogue Summary' table showing Active Rogue APs (67), Active Rogue Clients (2), and Adhoc Rogues (0). An 'Access Point Summary' table shows 1 up and 1 down for 802.11a/n Radios, and 1 up and 0 down for 802.11b/g/n Radios. A 'Client Summary' table shows 3 Current Clients, 0 Excluded Clients, and 0 Disabled Clients. The interface also features a 'Most Recent Traps' section listing detected rogue APs and clients.

Configuration for handsets running in 802.11b , b/g mixed mode, g only mode in 8020/8030 phones or 2.4 GHz in 8400 phones

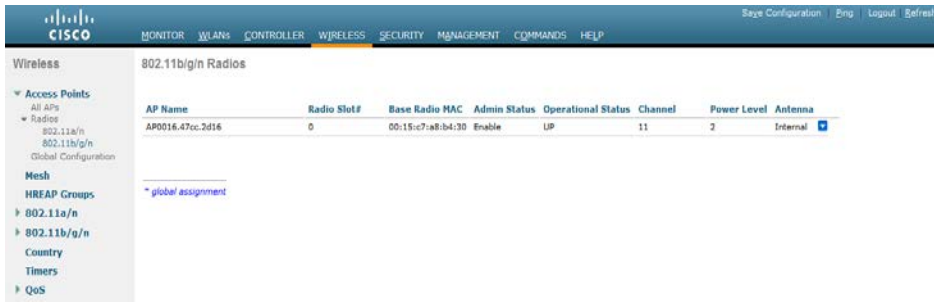


Note: When to use g-only

When 8020/8030 phones are set to g only mode, they support the higher g data rates. In g only mode, however, the handset will not detect 802.11b clients and will not provide protection. G only mode in these handsets should be used only if there is no possibility of an 802.11b client or the network will experience data corruption.

- 1 From the main menu, click **Wireless**.

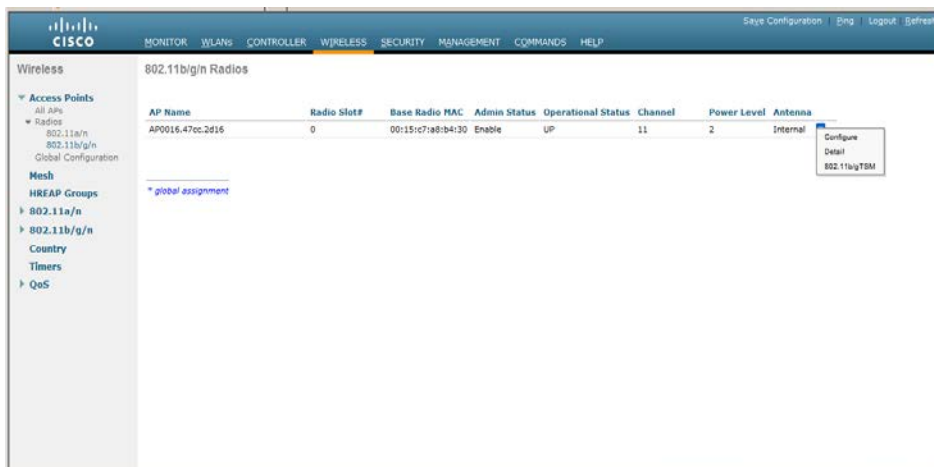
- 2 In the navigation pane, under **Access Points** click **Radios**, then select **802.11b/g/n**. All the APs that are connected should be listed, showing their **Operational Status** as **UP**.



The screenshot shows the Cisco Wireless Configuration interface. The left navigation pane is expanded to 'Access Points' > 'Radios' > '802.11b/g/n'. The main content area displays a table of 802.11b/g/n Radios. The table has the following columns: AP Name, Radio Slot#, Base Radio MAC, Admin Status, Operational Status, Channel, Power Level, and Antenna. One row is visible with the following data:

AP Name	Radio Slot#	Base Radio MAC	Admin Status	Operational Status	Channel	Power Level	Antenna
AP0016.47cc.2d16	0	00:15:c7:a8:b4:30	Enable	UP	11	2	Internal

- 3 Select **Configure** from the drop-down list for the access point you wish to change. Set the parameters for that AP:



The screenshot shows the same Cisco Wireless Configuration interface as above. A 'Configure' button is now visible in the 'Antenna' column of the table row, indicating that the configuration page for that specific radio is being accessed.

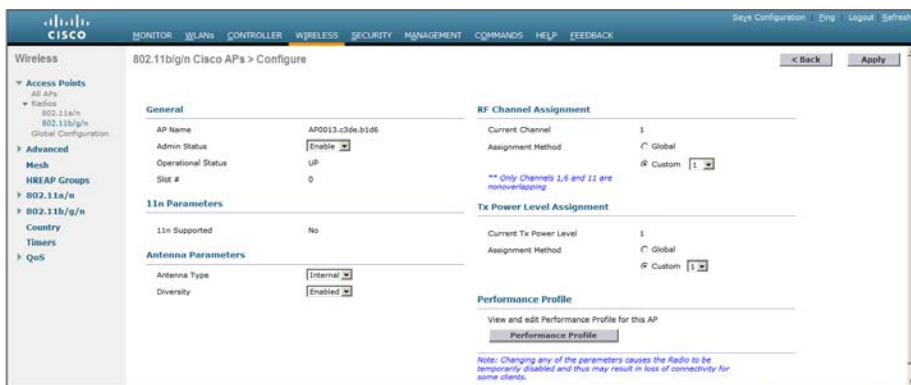


Note: Power and channel settings

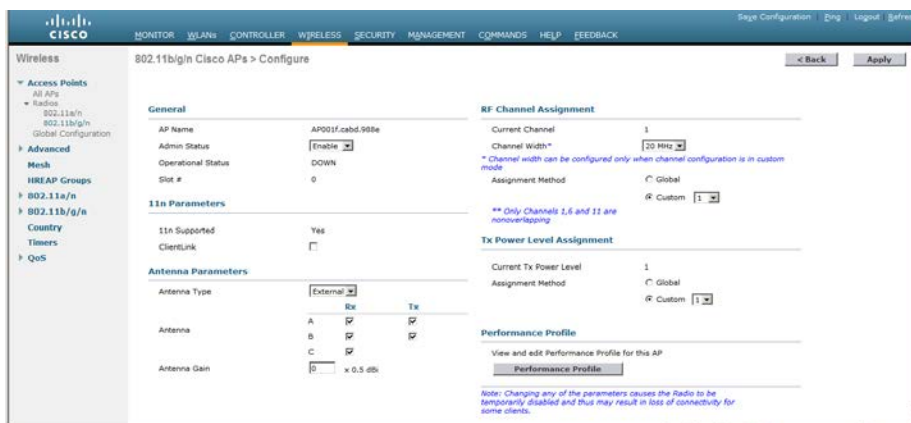
Global settings for **RF Channel Assignment** and **Tx Power Level Assignment** were not tested. For **Custom Tx Power** and **RF Channel** settings please consult your facility's RF site survey — optimized for wireless voice traffic — to determine correct power and channel settings for each AP using only channels **1**, **6** and **11**.

- a Set **Admin Status** to **Enable**.
- b Configure any other settings that might be relevant to your deployment as needed.
- c Click the **Apply** button to save all changes.

Screenshot for 113x, 120x, 123x and 124x series access points:



Screenshot for 104x, 114x, 125x, 126x, 350x, and 360x series access points (1040 has only 2 antennas):



- 4 In the navigation pane under **802.11b/g/n**, click **Network**. Set network parameters as follows:
 - a Set **802.11b/g Network Status** to **Disable**. The radio will be re-enabled after setting radio parameters.



Note: Data Rates

For setting up the **Data Rates**, 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.

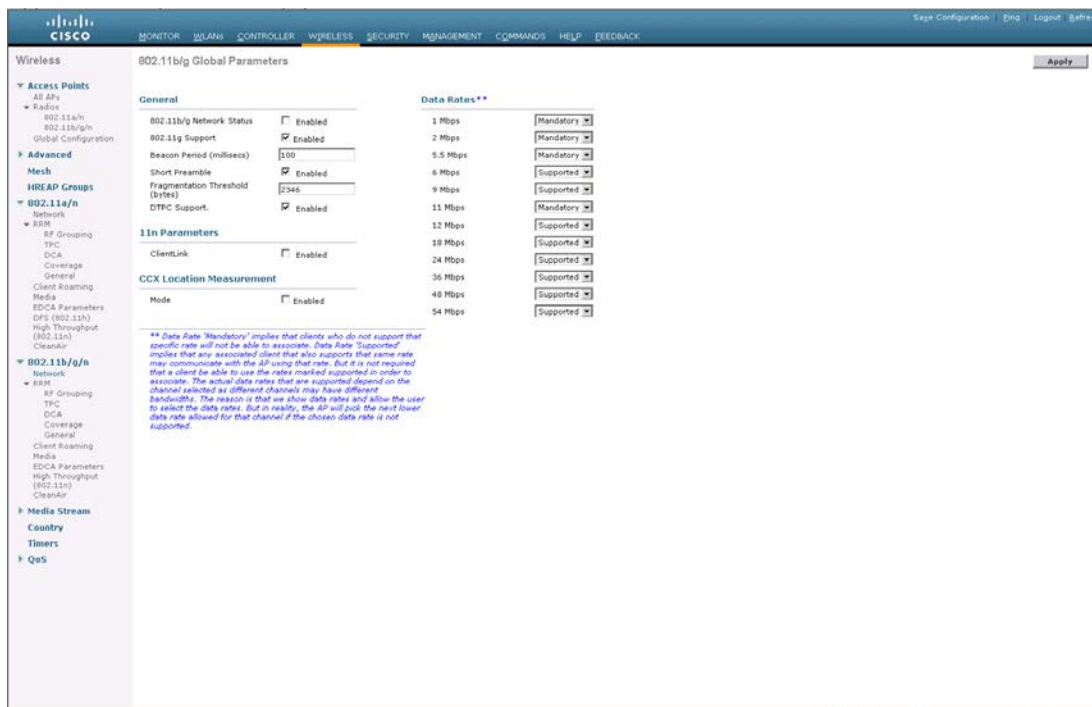
802.11 Radio Standard	Minimum Available Signal Strength (RSSI)	Maximum "Mandatory" Data Rate
802.11b	-70 dBm	1 Mb/s
	-60 dBm	11 Mb/s
802.11g	-63 dBm	6 Mb/s
	-47 dBm	54 Mb/s
802.11a	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s



Note: RF Deployment reference

For additional details on RF deployment please see the *Deploying Enterprise-Grade Wi-Fi Telephony* white paper and the *Best Practices Guide to Network Design Considerations for SpectraLink Wireless Telephone*.

- b** Use the default **Fragmentation Threshold** (2346 bytes).
- c** Set the **Beacon Period** to **100**.
- d** The handsets do not support dynamic power and will not utilize the information element that is set when DTPC Support is enabled. The handset power should be configured to match the highest transmit power of the APs.
- e** Click the **Apply** button to save the settings.



Note: Enable Admission Control

Admission Control (ACM) must be enabled on both the Voice and Video AC when the handset is configured for Admission Control Mandatory.

- 5 For Cisco 6.0, in the navigation pane under 802.11b/g/n, select **Voice**.
For Cisco 7.0, in the navigation pane under 802.11 b/g/n, select **Media**, then select the **Voice** tab.
- 6 Select the **Admission Control (ACM)** checkbox. Set the Max RF Bandwidth to **20** to limit the bandwidth allocated to handsets to a value tested to provide good performance.



Note: Disable WLAN before changing Admission Control settings.

Any WLAN using the network must be disabled before changing Admission Control settings.

- 7 For Cisco 6.0, in the navigation pane under 802.11b/g/n, select **Video**. For Cisco 7.0, in the navigation pane under 802.11b/g/n, select **Media**, then select the **Video** tab.
- 8 Select the **Admission Control (ACM)** checkbox. Set the Max RF Bandwidth for Video to **5**.



Note: Disable WLAN before changing Admission Control settings.

Any WLAN using the network must be disabled before changing Admission Control settings.

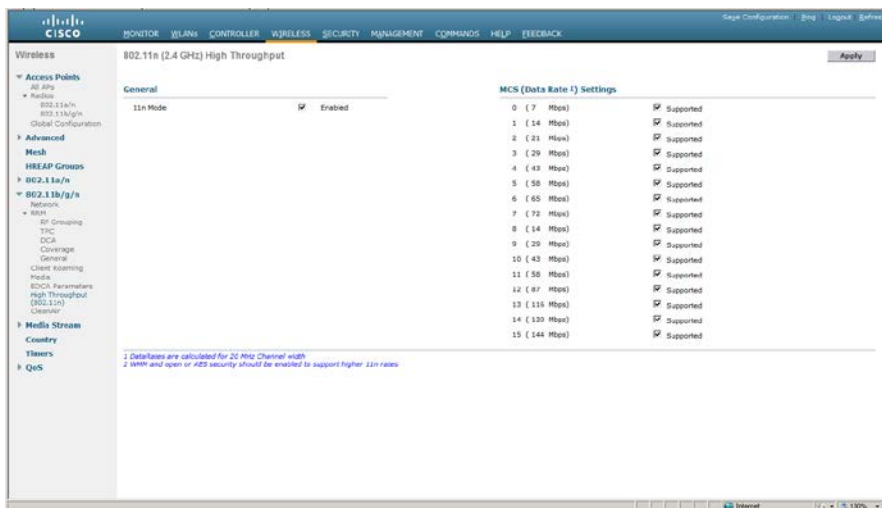
- 9 Click the **Apply** button to save the settings.
- 10 In the navigation pane under 802.11b/g/n, select **Network**.

11 Enable 802.11b/g Network Status and 802.11g Support if SpectraLink Wireless Telephones are configured for 802.11b & b/g mixed or g only mode in 8020/8030 phones or 2.4 GHz in 8400 phones.

12 Click the **Apply** button to save the settings.

Configuring 802.11n

1 For Cisco versions 6.0.202.0 or 7.0.220.0, in the navigation pane under 802.11 b/g/n, select **High Throughput (802.11n)**. Check the radio box to enable 11n mode and allow all data rates to be supported.



2 Disable msdu aggregation:

3 Connect to the CLI as described in the section “Configuring a New Controller Starting from Factory Defaults”.

4 Enter the commands:

```
config 802.11b 11n support a-msdu tx priority all disable
save config
```

5 Click the **Apply** button to save the settings.

6 In the navigation pane under **802.11b/g/n**, select **Network**.

7 For **802.11b/g Network Status**, click the **Enabled** check box.



Note: Configuring 802.11n with versions prior to 6.0.202.0

SpectraLink 8400 handsets must be configured with the 802.11n mode disabled when used with Cisco AP 114x and 125x with versions prior to 6.0.202.0. See Appendix A for configuration steps.

Configuration for handsets running in 802.11a mode in the 8020/8030 phones and using the 5 GHz radio in the 8400 series phones

- 1 From the main menu, click **Wireless**.
- 2 In the navigation pane, under **Access Points** click **Radios**, then select **802.11a /n**. All the APs that are connected should be listed, showing their **Operational Status** as **UP**.
- 3 Select **Configure** from the drop-down list for the access point you wish to change. Set the parameters for that AP:

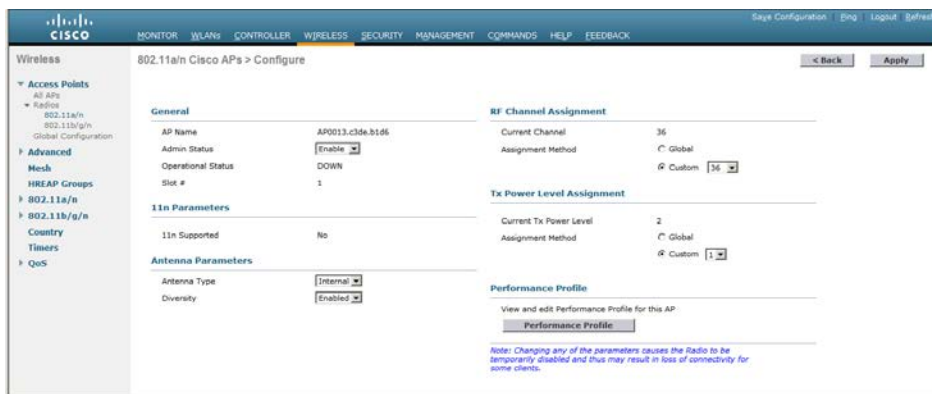


Note: Power and channel settings

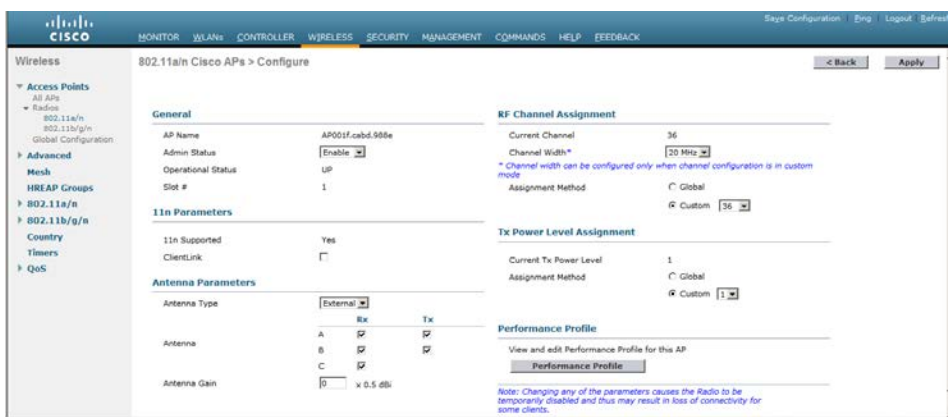
Global settings for **RF Channel Assignment** and **Tx Power Level Assignment** were not tested. For **Custom Tx Power** and **RF Channel** settings please consult your facility's RF site survey — optimized for wireless voice traffic — to determine correct power and channel settings for each AP using non-overlapping channels.

- a Set **Admin Status** to **Enable**.
- b Configure any other settings that might be relevant to your deployment as needed.
- c Click the **Apply** button to save all changes.

Screenshot for 113x, 120x, 123x and 124x series access points:



Screenshot for 104x, 114x, 125x, 126x, 350x, and 360x series access points (1040 has only 2 antennas):



- 4 In the navigation pane under **802.11a/n**, click **Network**. Set the network parameters as follows:
 - a Set **802.11a Network Status** to **Disable**; the radio will be re-enabled after setting radio parameters
 - b For setting up the **Data Rates**, please consult your facility’s RF site survey, designed for voice traffic, to determine if you have sufficient coverage to support all data rates. The handset requires the following minimum dBm reading to support the corresponding **Mandatory** data rate setting in the access point.

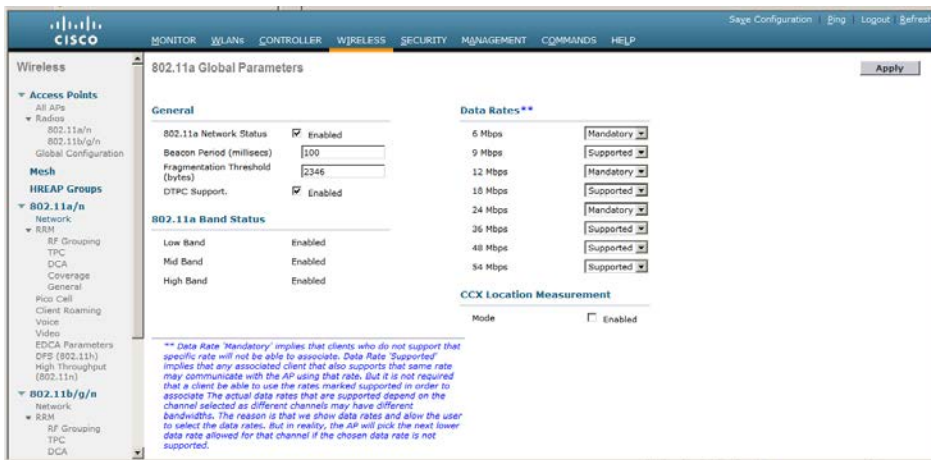
802.11 Radio Standard	Minimum Available Signal Strength (RSSI)	Maximum "Mandatory" Data Rate
802.11b	-70 dBm	1 Mb/s
	-60 dBm	11 Mb/s
802.11g	-63 dBm	6 Mb/s
	-47 dBm	54 Mb/s
802.11a	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s



Note: Add Title Here

For additional details on RF deployment please see the *Deploying Enterprise-Grade Wi-Fi Telephony* white paper and the *Best Practices Guide to Network Design Considerations for SpectraLink Wireless Telephony*.

- c Use the default **Fragmentation Threshold** (2346 bytes).
- d Set the **Beacon Period** to **100**.
- e SpectraLink Wireless Telephones do not support dynamic power and will not utilize the information element that is set when **DTPC support** is enabled. The handset power should be configured to match the highest transmit power of the APs.
- f Click the **Apply** button to save the settings.



- If DFS channels are used in the deployed network, in the navigation pane under 802.11a/n, select DFS (802.11h). Check the Channel Announcement radio box to cause the AP to advertise Spectrum Management. If the AP does not advertise Spectrum Management, Polycom phones will not connect on DFS channels (bandwidth shared with radar facilities).



Note: Admission Control

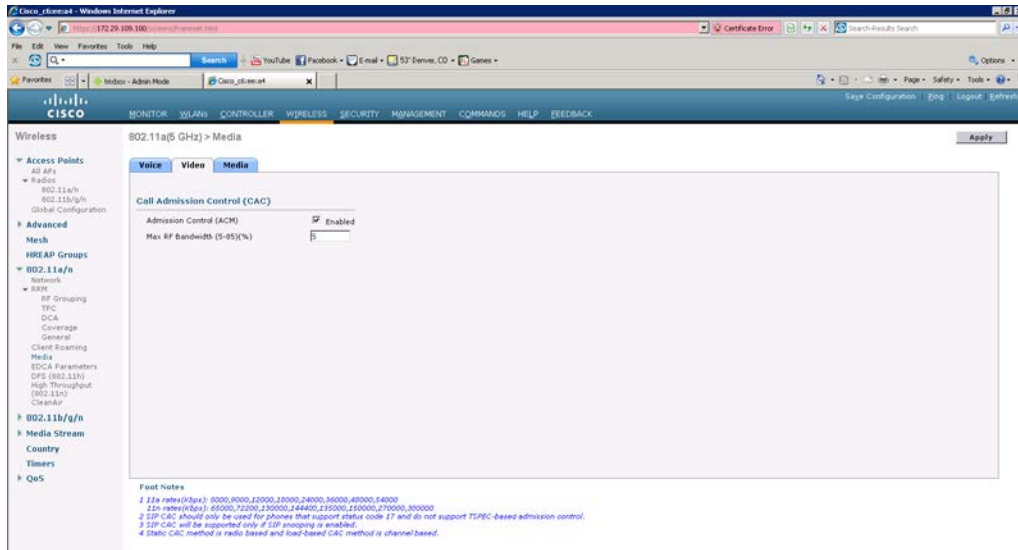
Admission Control (ACM) must be enabled on both the Voice and Video AC when the handset is configured for Admission Control Mandatory.

- For Cisco 6.0, in the navigation pane under 802.11a/n, select **Voice**.
For Cisco 7.0, in the navigation pane underneath 802.11 a/n, select **Media**, then select the **Voice** tab.
- Select the **Admission Control (ACM)** checkbox. (This step is optional if the handset is configured with Admission Control set to Optional, this setting must match setting in Video). Set the Max RF Bandwidth to **15** to limit the bandwidth allocated to handsets to a value tested to provide good performance.

Font Notes

- 1 11e rates(kbps): 6000,9000,12000,18000,24000,36000,48000,64000
- 2 11n rates(kbps): 65000,72000,130000,144400,135000,120000,170000,300000
- 3 SIP CAC should only be used for phones that support either code 17 and do not support TSPC-based admission control.
- 4 SIP CAC will be supported only if SIP snooping is enabled.
- 5 Static CAC method is radio based and load-based CAC method is channel based.

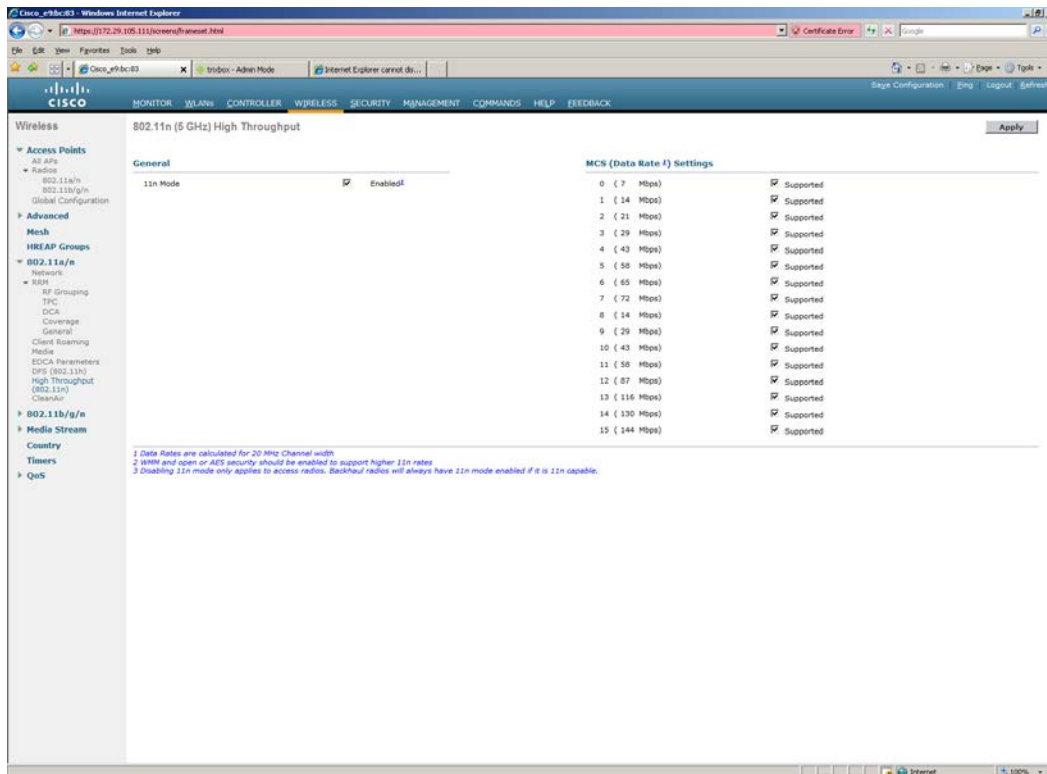
- For Cisco 6.0, in the navigation pane under 802.11a/n, select **Video**.
For Cisco 7.0, in the navigation pane under 802.11a/n, select **Media**, then select the **Video** tab.
- Select the **Admission Control (ACM)** checkbox. (This step is optional if the handset is configured with Admission Control set to Optional, this setting must match setting in Voice)



10 Click the **Apply** button to save the settings.

Configuring 802.11n:

- 1 For Cisco versions 6.0.202.0 or 7.0.220.0, in the navigation pane under 802.11 a/n, select High Throughput (802.11n). Check the radio box to enable 11n mode and allow all data rates to be supported.



- 2 Disable msdu aggregation:

- 3 Connect to the CLI as described in the section “Configuring a New Controller Starting from Factory Defaults”.
- 4 Enter the commands:

```
config 802.11a 11nsupport a-msdu tx priority all disable  
save config
```
- 5 In the navigation pane under **802.11a/n**, select **Network**.
- 6 For **802.11a Network Status**, click the **Enabled** check box.
- 7 Click the **Apply** button to save the settings.



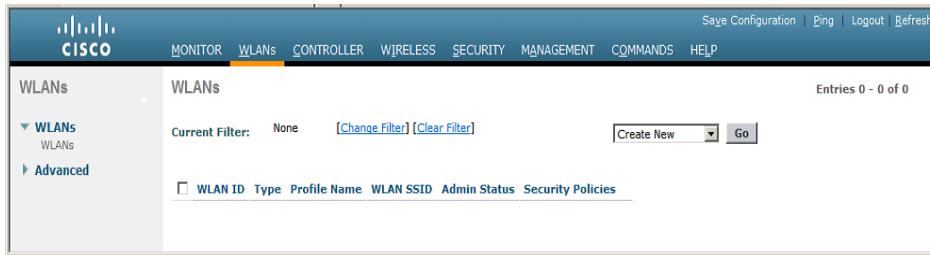
Note: Add Title Here

SpectraLink 8400 handsets must be configured with the 802.11n mode disabled when used with Cisco AP 114x and 125x with versions prior to 6.0.202.0. See Appendix A for configuration steps.

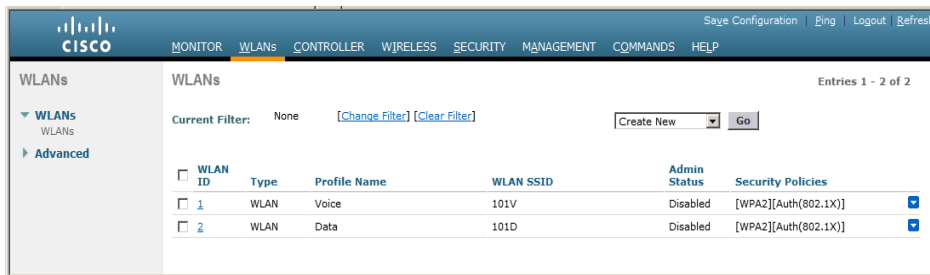
Setting up the SSID

Voice and data must be on separate SSIDs to prioritize voice traffic. The voice SSID must be set to **Platinum** for **Quality of Service** and the data SSID must be set to **Silver** for **Quality of Service**.

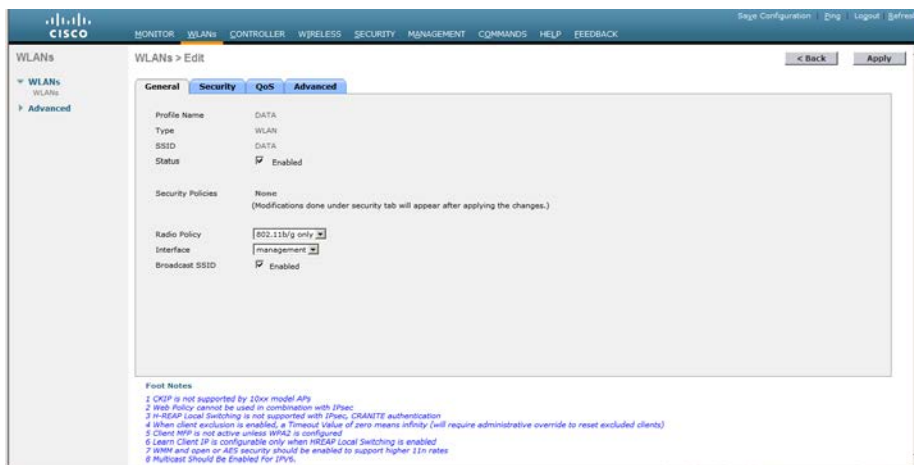
- 1 From the main menu, click **WLANs**.
- 2 In the **WLANs** screen, select Create New from the drop down list and click Go.



- 3 Enter the **Profile Name** and **SSID**.
- 4 Click the **Apply** button twice.

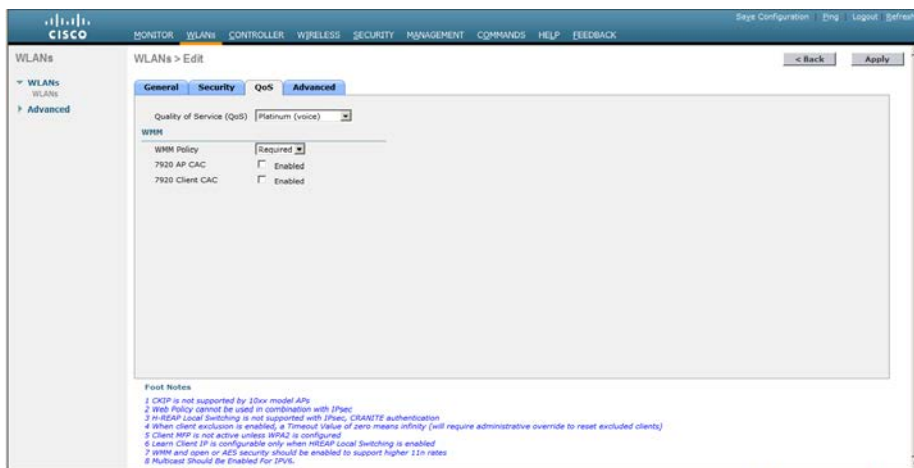


- 5 Select the **Profile Name** for the voice SSID.
- 6 Under the **General** tab, verify the **Radio Policy** corresponds to the SpectraLink Wireless Telephone configuration.
 - When **Radio Policy** is configured for **802.11b/g only**, the handsets should be configured for **802.11b & b/g mixed** in 8020/8030 phones and 2.4 GHz in 8400 phones.
 - When **Radio Policy** is configured for **802.11a only**, the handsets should be configured for **802.11a** in 8020/8030 phones and 5 GHz in 8400 phones.
 - When **Radio Policy** is configured for **802.11g only**, the handsets should be configured for **802.11g only** in 8020/8030 phones and 2.4 GHz in 8400 phones.
 - When **Radio Policy** is configured for **All**, the handsets may be configured to any of the settings required.
- 7 For **Status**, select the **Enabled** check box.



8 Under the **QoS** tab, set **Quality of Service** to **Platinum**. This is the required setting for voice traffic.

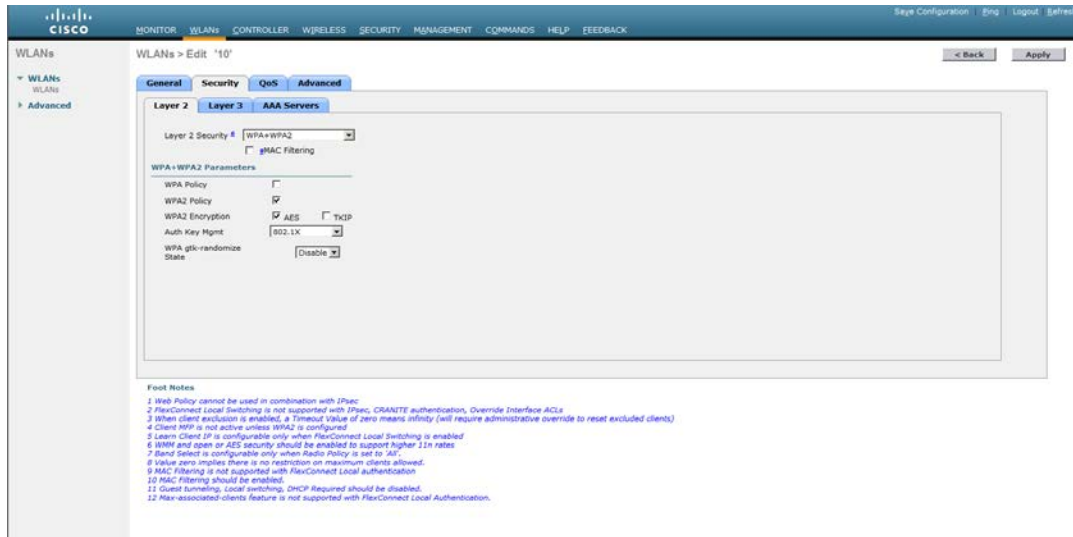
9 Set **WMM Policy** to **Required**.



10 Under the **Security** tab, at **Layer 2 Security** select the desired security policy from the drop-down list.

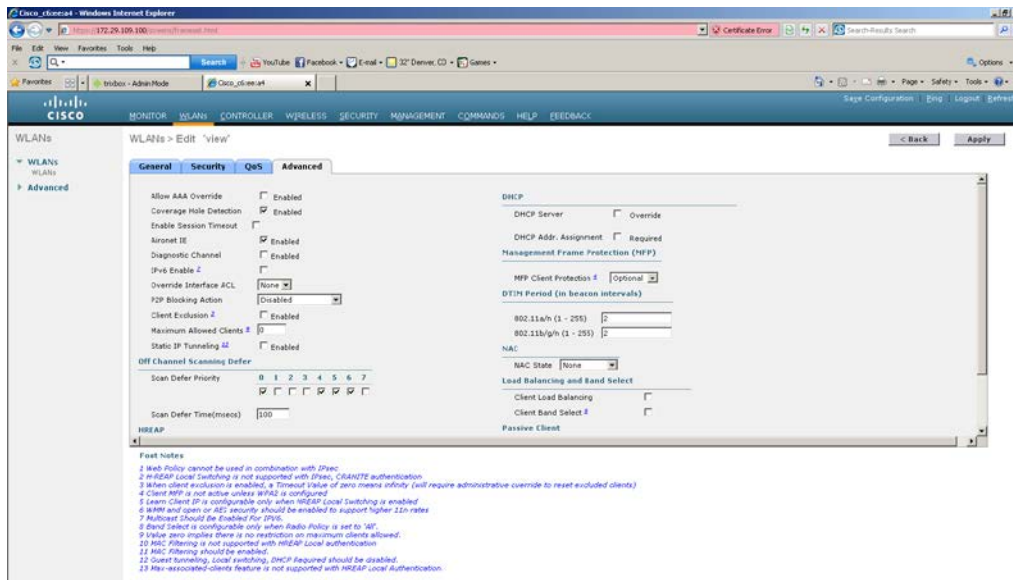
- For WPA2-PSK, under **WPA+WPA2 Parameters**:
 1. Select the **WPA2-Policy** check box.
 2. Select the **AES** check box for **WPA2-Encryption**.
 3. At **Auth Key Mgmt** select **PSK** from the drop-down list.
 4. If present (version 7.2.103.0), ensure that **WPA gtk-randomize State** is set to **Disable**.
- For WPA-PSK, under **WPA+WPA2 Parameters**:
 1. Select the **WPA-Policy** check box.
 2. Select the **TKIP** check box for **WPA Encryption**.

3. At **Auth Key Mgmt** select **PSK** from the drop-down list. The PSK Format may be selected as **ASCII** or **HEX** for both WPA-PSK and WPA2-PSK policies.
 4. If present (version 7.2.103.0), ensure that **WPA gtk-randomize State** is set to **Disable**.
- For WPA2-Enterprise (802.1X), select **WPA+WPA2 Parameters**:
 1. Select the **WPA2 Policy** check box.
 2. Select the **AES** check box for **WPA2 Encryption**.
 3. At **Auth Key Mgmt**, select **802.1X+CCKM** from the drop-down list.
 4. If present (version 7.2.103.0), ensure that **WPA gtk-randomize State** is set to **Disable**.



11 Under the **Advanced** tab

- a Set the **DTIM** to **2** for the radio that corresponds to the SpectraLink Wireless phone configuration.
- b Ensure the **Enable Session Timeout** box is unchecked and that **Client Exclusion** is disabled.
- c Uncheck the **Client Load Balancing** and **Client Band Select** boxes.
- d Check off-channel scanning defer for the 0 priority class (prevents contention between off-channel scanning and PTT).

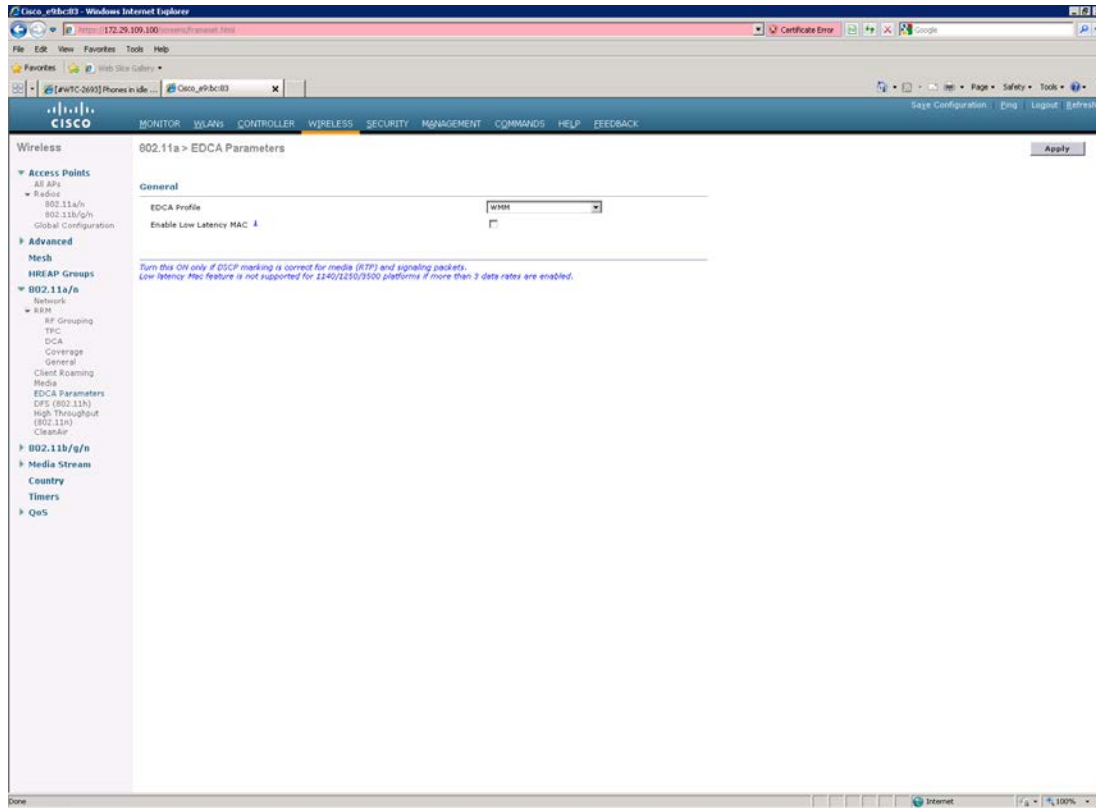


12 Click the **Apply** button to save all changes.

Setting up the EDCA parameters profile

The EDCA parameters must be set to the WMM setting after the WLAN network QoS has been set.

- 1 In the navigation pane under **802.11a/n**, select **EDCA Parameters**.
- 2 Ensure that **WMM** is selected from the drop-down list.
- 3 Click **Apply**.



Configuration for handsets running in 802.11b/g mode, 802.11b and b/g mixed mode, or 802.11 g only mode in 8020/8030 phones or 2.4 GHz in 8400 phones

- 1 In the navigation pane under **802.11b/g/n**, select **EDCA Parameters**.
- 2 Ensure that **WMM** is selected from the drop-down list.
- 3 Click **Apply**.

The screenshot shows the Cisco configuration interface for the '802.11b/g > EDCA Parameters' section. The top navigation bar includes 'MONITOR', 'WLAN', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WIRELESS' tab is active. The page title is '802.11b/g > EDCA Parameters' with an 'Apply' button on the right. The left sidebar shows a tree view of configuration options under 'Wireless', including 'Access Points', 'Radios', 'Advanced', 'Mesh', 'HREAP Groups', '802.11a/n', '802.11b/g/n', 'Media Stream', 'Country', 'Timers', and 'QoS'. The main content area is titled 'General' and contains the following configuration items:

- EDCA Profile:** A dropdown menu set to 'WMM'.
- Enable Low Latency MAC:** A checkbox that is currently unchecked.

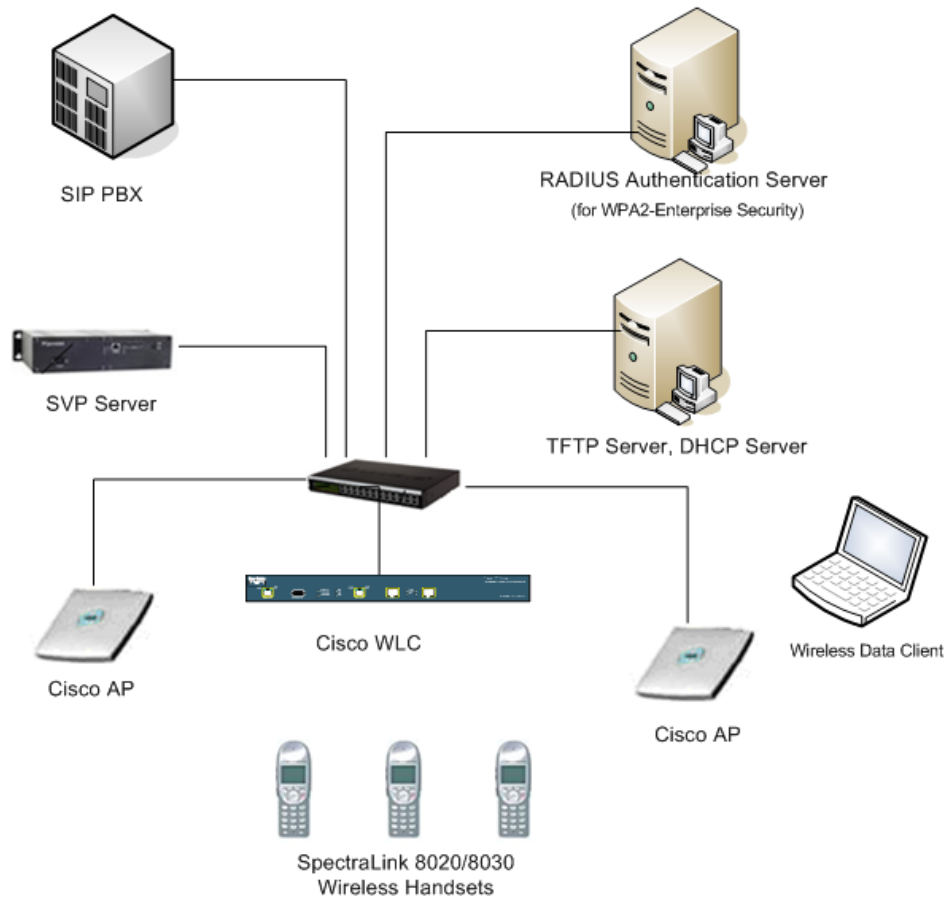
Below these items is a note: *Turn this ON only if DSCP marking is correct for media (RTP) and signaling packets. Low latency Mac feature is not supported for 1140/1230/3500 platforms if more than 3 data rates are enabled.*

Chapter 2: Configuration for SVP Operation

Introduction

SpectraLink 8020/8030 phones can be configured for SVP QoS from the WLAN Settings menu using the Custom selection. SpectraLink 8400 phones do not support SVP.

Network Topology



Note: Example only

This configuration is not applicable to all customer environments.

Configuring a New Controller Starting from Factory Defaults

Initial provisioning of the controller is done via the command line interface (CLI).

- 1 Connect a null modem serial cable between the console port of the controller and the serial port of a PC.
- 2 Open a terminal program, such as Hyper Terminal, and configure the port settings to 9600 baud, no parity, 8 data bits and 1 stop bit.
- 3 Power-on the controller. Status of the controller's boot process will appear as the controller is powering up. Once the controller is running, it will prompt you to run the Startup Wizard.
- 4 The Startup Wizard provides for an easy means to perform initial controller setup and provisioning. Refer to the *Installation and Startup Guide* for the Cisco 4400 Series WLC, or other appropriate controller, found at Cisco's website. This document contains a detailed explanation of using the Startup Wizard for the 4400:
<http://www.cisco.com/en/US/docs/wireless/controller/4400/quick/guide/ctrlv32.html#wp34023>
- 5 Once the controller has been configured via the Startup Wizard, the remaining configuration can be configured through the switch-web interface using a Web browser (Cisco recommends using MS IE 6.0+).
- 6 If necessary, the controller can be reset to factory defaults. To reset the WLC to factory default, you must reboot, then type **Recover-config** at the CLI. This only works before the first time a user logs in via the console.

Connecting to the Controller via a Browser

- 1 Connect to the WLC by pointing your internet browser to the URL: `https<IP_Addr>` (where `<IP_Addr>` is the IP address of the management interface of the WLC).
- 2 Click the **Login** prompt. The default **User Name** and **Password** is **admin**.
- 3 Once logged in properly, a page similar to the one below displays.

The screenshot shows the Cisco Wireless LAN Controller (WLC) web interface in Internet Explorer. The browser address bar shows `https://172.29.104.100/screens/frameset.html`. The page title is "Cisco WLC Monitor Summary". The interface includes a navigation menu on the left with options like Monitor, WLANs, Controller, Wireless, Security, Management, Commands, Help, and Feedback. The main content area is titled "Monitor Summary" and displays various system metrics and status indicators.

Controller Summary

Management IP Address	172.29.104.100
Service Port IP Address	0.0.0.0
Software Version	6.0.199.4
Emergency Image Version	N/A
System Name	Cisco_e9bc83
Up Time	2 days, 8 hours, 15 minutes
System Time	Wed Oct 20 22:43:29 2010
Internal Temperature	+46 C
802.11a Network State	Disabled
802.11b/g Network State	Enabled
Local Mobility Group	test
CPU Usage	0%
Memory Usage	32%

Access Point Summary

	Total	Up	Down	
802.11a/n Rados	1	0	1	Detail
802.11b/g/n Rados	1	1	0	Detail
All APs	1	1	0	Detail

Client Summary

Current Clients	3	Detail
Excluded Clients	0	Detail
Disabled Clients	0	Detail

Rogue Summary

Active Rogue APs	22	Detail
Active Rogue Clients	0	Detail
Adhoc Rogues	0	Detail
Rogues on Wired Network	0	Detail

Top WLANs

Profile Name	# of Clients	
SSA	1	Detail

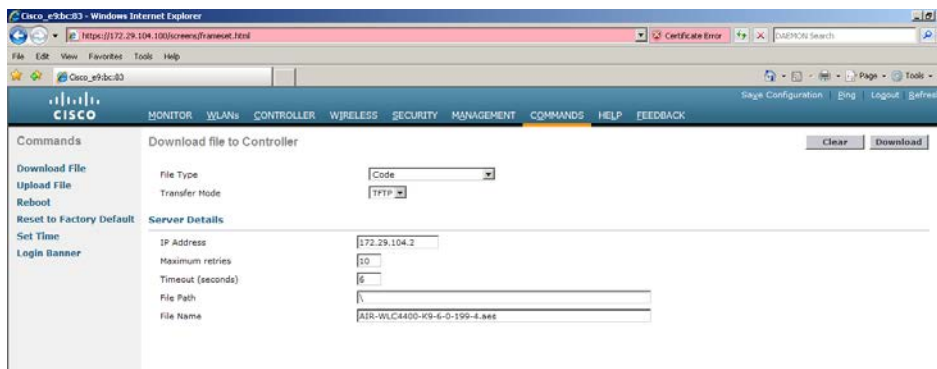
Most Recent Traps

Interference Profile Failed for Base Radio MAC: 00:25:45:a3:01:80 and slotId: 0
 Rogue AP : 00:23:eb:e4:fb:e4 detected on Base Radio MAC : 00:25:45:a3:01:80 Interface no:0(802.11b)
 Rogue AP : 00:23:eb:e4:fb:a9 detected on Base Radio MAC : 00:25:45:a3:01:80 Interface no:0(802.11b)
 Rogue AP : 00:23:eb:e4:fb:a8 detected on Base Radio MAC : 00:25:45:a3:01:80 Interface no:0(802.11b)
 Rogue AP : 00:23:eb:e4:fb:a4 detected on Base Radio MAC : 00:25:45:a3:01:80 Interface no:0(802.11b)
[View All](#)

This page refreshes every 30 seconds.

Installing Software

- 1 To check the installed version of software, listed in the **Product Summary**, click **Monitor** from the main menu.
- 2 In the navigation pane, click **Summary**. The heading labeled **Software Version** shows the current software version.
- 3 Download the appropriate software for your model of controller from the Cisco website.
- 4 Set up a Trivial File Transfer Protocol (TFTP) server running on a PC to download the file to the controller.
- 5 From the main menu, click **Commands**.
- 6 In the navigation pane, click **Download File**.
- 7 Fill in the download parameters:
 - a For **File Type**, select **Code**.
 - b For **TFTP Server**, type in the IP Address of the TFTP server.
 - c Add the **File Path** (this is the path in the TFTP server's root directory and not the system path where the TFTP server is located) and **File Name** of the firmware file to download. (Note the example simply uses the /designator for the root TFTP directory.) Point the TFTP server to the code.
- 8 Click **Download** and allow a few minutes for the download to complete.



- 9 Reboot the Controller.

Controller Setup

The initial setup of the controller is shown below.



Note: Example configuration

The setup instructions outlined in this document are for the configuration shown in the diagram only. Your configuration may differ, and the appropriate adjustments must be made.

- 1 From the main menu, click **Controller**.
- 2 Set the **AP Multicast Mode** to **Multicast** and enter a multicast IP address that is currently not being used on your network for the **Multicast Group Address**.
- 3 Click the **Apply** button.

The screenshot shows the Cisco Controller configuration page for the 'General' tab. The 'AP Multicast Mode' is set to 'Multicast' and the 'Multicast Group Address' is '224.0.1.100'. Other settings include Name: Cisco_e9:bc:03, 802.2k Flow Control Mode: Disabled, LAG Mode on next reboot: Disabled, Broadcast Forwarding: Disabled, AP Fallback: Enabled, Apple Talk Bridging: Disabled, Fast SSID change: Disabled, Default Mobility Domain Name: RF, RF Group Name: RF, User Idle Timeout (seconds): 300, ARP Timeout (seconds): 300, Web Radius Authentication: PAP, 802.3 Bridging: Disabled, Operating Environment: Commercial (0 to 40 C), and Internal Temp Alarm Limits: 0 to 65 C.

- 4 Click **Multicast** from the options on the left side of the screen.
- 5 Select **Enable Global Multicast Mode** checkbox.
- 6 Click the **Apply** button.

The screenshot shows the Cisco Controller configuration page for the 'Multicast' tab. The 'Enable Global Multicast Mode' checkbox is checked. Other settings include 'Enable IGMP Snooping' (unchecked) and 'IGMP Timeout (seconds)' set to 60.

- 7 Click **Save Configuration**.

Connecting APs

As the APs are connected to the network, they should automatically find the controller via the CAPWAP discovery algorithms. The Dynamic Host Configuration Protocol (DHCP) server will assign each AP an IP address.



Note: Add Title Here

You can configure a DHCP server to run on a remote PC for a small deployment. However, for large-scale deployments, an enterprise-grade DHCP server must be used.

The **ap-manager** and **management** interfaces' configuration should include the DHCP server you have configured. Alternately, you can configure the DHCP server internally on the controller to hand out leases to the connected clients. (Note: The WLC's DHCP server does not lease addresses to the AP.) The instructions for doing so are included at the end of this document.

- 1 From the main menu, click **Controller**.
- 2 In the navigation pane, click Interfaces. Verify that the proper IP addresses are assigned to the interfaces.
- 3 Under **Interface Name** click **management**. . Note: the screenshots are from a Cisco 4400. The 2100 does not contain a service-port interface. The 5500 does not contain an ap-manager interface. If the interface is not present on the model being configured, no values need to be entered.

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
ap-manager	untagged	172.29.105.101	Static	Enabled
management	untagged	172.29.105.100	Static	Not Supported
service-port	N/A	0.0.0.0	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported

- 4 Under **DHCP Information**, enter the IP address of the **Primary DHCP Server**.
- 5 Repeat this step for the **ap-manager** interface, if present on the model configured.
- 6 Click the **Apply** button and save the changes.

The screenshot shows the Cisco Controller configuration page for the 'management' interface. The page is titled 'Interfaces > Edit' and includes a navigation menu on the left with options like General, Inventory, Interfaces, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, and Advanced. The main configuration area is divided into several sections:

- General Information:** Interface Name: management, MAC Address: 00:0b:85:48:3c:40
- Configuration:** Quarantine: , Quarantine Vlan Id:
- Interface Address:** VLAN Identifier: , IP Address: , Netmask: , Gateway:
- Physical Information:** Port Number: , Backup Port: , Active Port: 1
- DHCP Information:** Primary DHCP Server: , Secondary DHCP Server:
- Access Control List:** ACL Name:

A note at the bottom states: "Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients."

- 7 Under **service-port**, (if present), enter a valid **IP Address** and **Netmask** in a different subnet than the **management** interface. Click the **Apply** button and save the changes.

The screenshot shows the Cisco Controller configuration page for the 'Interfaces' section. The page is titled 'Interfaces' and includes a navigation menu on the left with options like General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, and Advanced. The main configuration area displays a table of interfaces:

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
ap-manager	untagged	172.29.109.101	Static	Enabled
management	untagged	172.29.109.100	Static	Not Supported
service-port	N/A	172.29.107.107	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported

AP Configuration



Note: QoS setting

All handsets operating on a given AP radio must have the same QoS setting. All APs supporting the handsets must be configured to enable the corresponding features.

- 1 Power-on and connect the APs to the network. Wait a few minutes for the APs to find the controller.
- 2 Verify the APs are associated to the WLC.
- 3 From the main menu, click **Monitor**.

The screenshot shows the Cisco WLC Monitor interface. The main content area displays a 'Summary' section with a 'Controller Summary' table and an 'Access Point Summary' table. The 'Controller Summary' table includes fields like Management IP Address (172.29.105.100), Service Port IP Address (0.0.0.0), Software Version (6.0.188.0), System Name (Cisco_40:3c:43), System Time (0 days, 0 hours, 27 minutes), Internal Temperature (44.1 C), and various network states. The 'Access Point Summary' table shows the status of 802.11a/n Radios (1 up, 0 down), 802.11b/g/n Radios (1 up, 0 down), and All APs (1 up, 0 down). A 'Client Summary' table shows 3 Current Clients, 0 Excluded Clients, and 0 Disabled Clients. The 'Rogue Summary' table shows 67 Active Rogue APs, 2 Active Rogue Clients, 0 Adhoc Routers, and 0 Routers on Wired Network. The 'Top WLANs' table shows the DATA profile with 1 client. The 'Most Recent Traps' section lists several rogue AP detections.

Configuration for handsets running in 802.11b & b/g mixed and g only mode with 7.0 and 7.2 versions of controller software

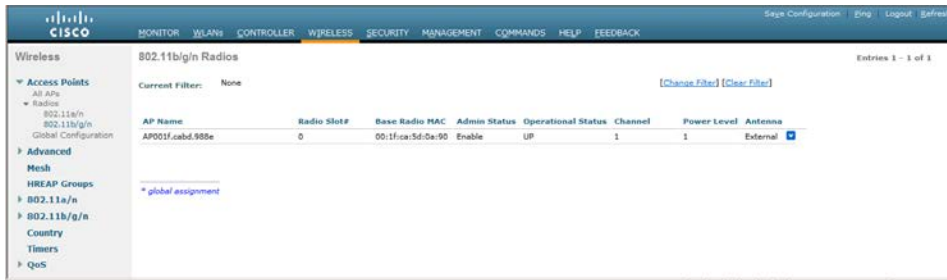


Note: g-only mode

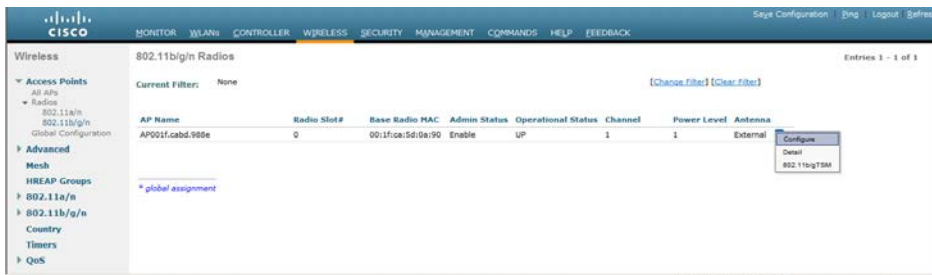
When 8020/8030 phones are set to g only mode, they support the higher g data rates. In g only mode, however, the handset will not detect 802.11b clients and will not provide protection. G only mode in these handsets should be used only if there is no possibility of an 802.11b client or the network will experience data corruption.

- 1 From the main menu, click **Wireless**.

- 2 In the navigation pane, under **Access Points** click **Radios**, then select **802.11b/g/n**. All the APs that are connected should be listed, showing their **Operational Status** as **UP**.



- 3 Select **Configure** from the drop-down list for the access point you wish to change. Set the parameters for that AP:

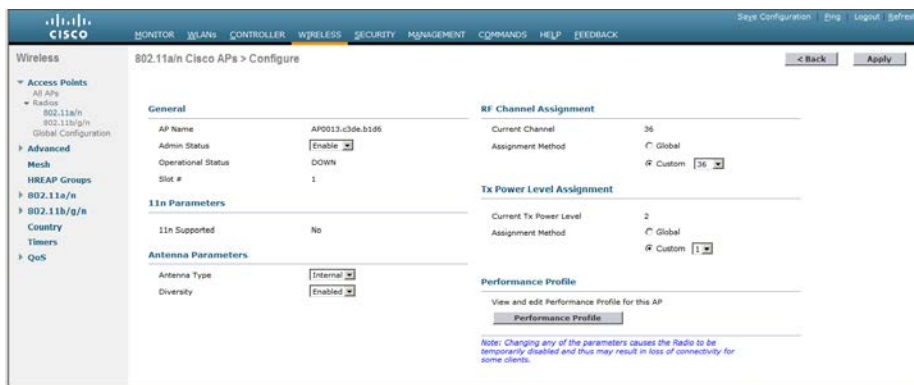


Note: Power and channel settings

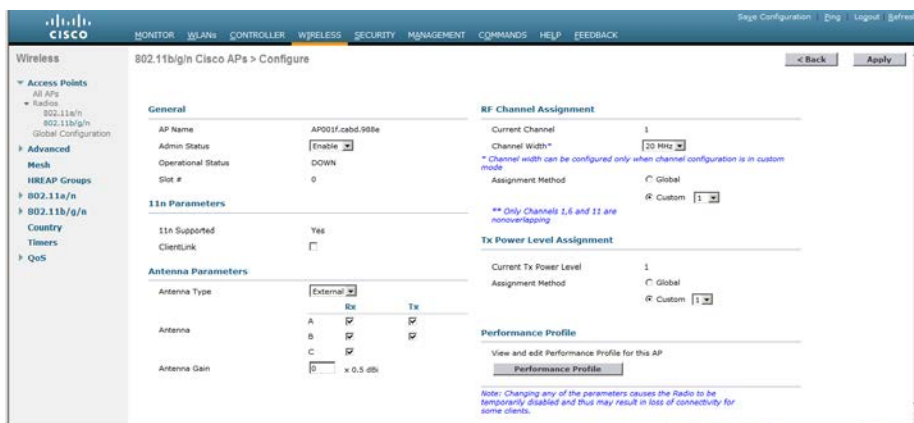
Global settings for **RF Channel Assignment** and **Tx Power Level Assignment** were not tested. For **Custom Tx Power** and **RF Channel** settings please consult your facility's RF site survey — optimized for wireless voice traffic — to determine correct power and channel settings for each AP using only channels **1**, **6** and **11**.

- a Set **Admin Status** to **Enable**.
- b Configure any other settings that might be relevant to your deployment as needed.
- c Click the **Apply** button to save all changes.

Screenshot for 113x, 120x, 123x and 124x series access points:



Screenshot for 104x, 114x, 125x, 126x, 350x, and 360x series access points (1040 has only 2 antennas):



- 4 In the navigation pane under 802.11b/g/n, click **Network**. Set network parameters as follows:
 - a Set 802.11b/g Network Status to Disable. The radio will be re-enabled after setting radio parameters.



Note: Data rates

For setting up the **Data Rates**, 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.

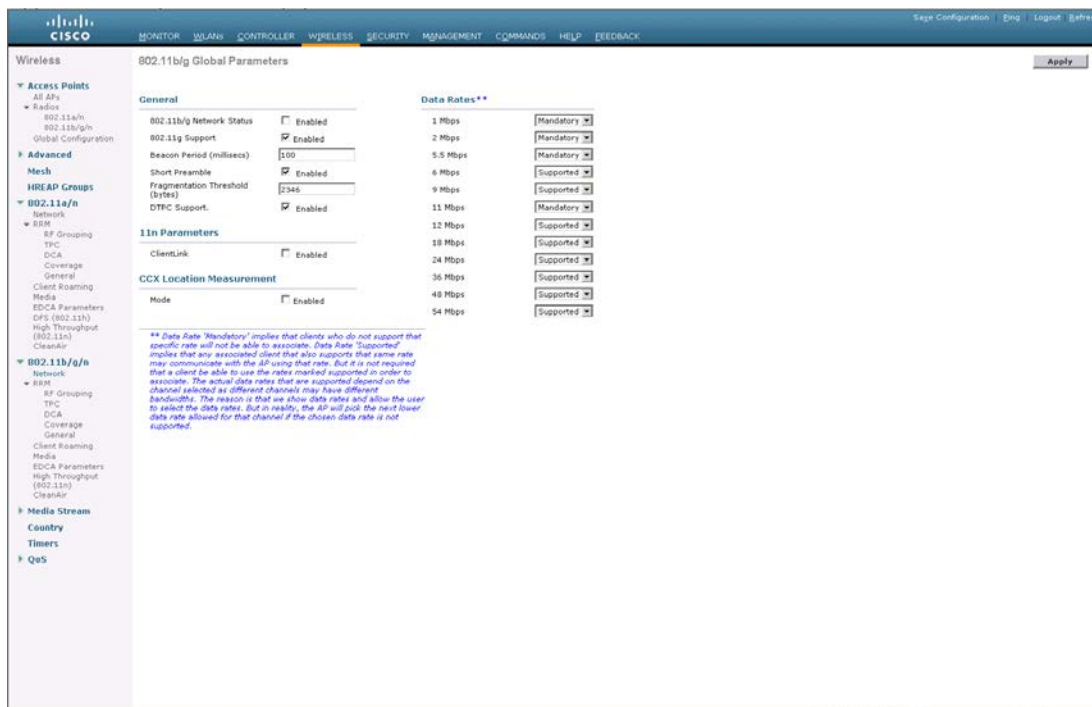
802.11 Radio Standard	Minimum Available Signal Strength (RSSI)	Maximum "Mandatory" Data Rate
802.11b	-70 dBm	1 Mb/s
	-60 dBm	11 Mb/s
802.11g	-63 dBm	6 Mb/s
	-47 dBm	54 Mb/s
802.11a	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s



Note: RF deployment reference

For additional details on RF deployment please see the Deploying Enterprise-Grade Wi-Fi Telephony white paper and the Best Practices Guide to Network Design Considerations for SpectraLink Wireless Telephones.

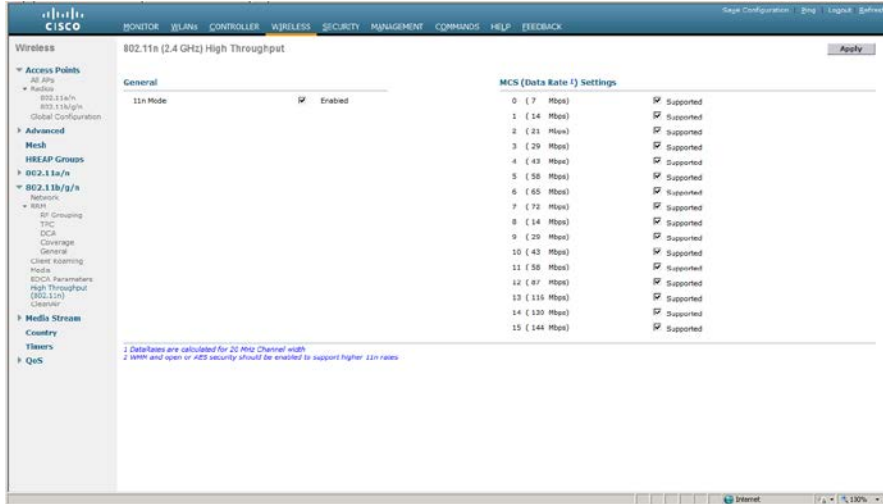
- b** Use the default **Fragmentation Threshold** (2346 bytes).
- c** Set the **Beacon Period** to 100.
- d** The handsets do not support dynamic power and will not utilize the information element that is set when DTPC Support is enabled. The handset power should be configured to match the highest transmit power of the APs.
- e** Click the **Apply** button to save the settings.



- 5 In the navigation pane under 802.11b/g/n, select **EDCA Parameters**.
- 6 Select **SpectraLink Voice Priority** from the drop-down list.
- 7 Click the **Apply** button to save the settings.



- 8 In the navigation pane under 802.11b/g/n, select **Network**.
- 9 Enable **802.11b/g Network Status** and **802.11g Support** if SpectraLink Wireless Telephones are configured for 802.11b & b/g mixed or g only modes.
- 10 Click the **Apply** button to save the settings.
- 11 If the network will be supporting 802.11n devices on a Cisco 7.0 release, in the navigation pane under 802.11 b/g/n, select **High Throughput (802.11n)**. Check the radio box to enable 11n mode and allow all data rates to be supported.

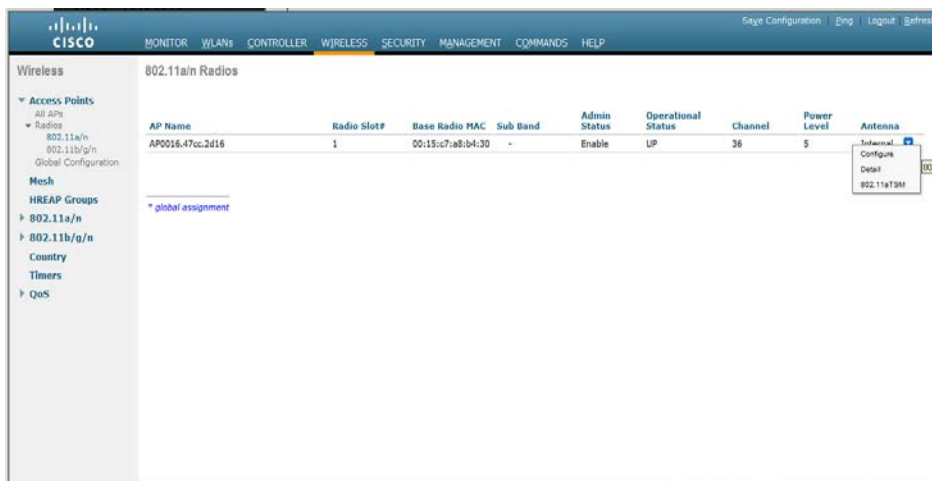


Note: SVP and 802.11n

When SpectraLink Voice Priority (SVP) is enabled under the EDCA parameters setting, the 802.11n capabilities will be disabled on that radio on Cisco 6.0 version releases. Polycom recommends deploying handsets using SVP on a different radio than 802.11n clients for Cisco 6.0 version releases.

Configuration for handsets running in 802.11a mode

- 1 From the main menu, click **Wireless**.
- 2 In the navigation pane, under **Access Points** click **Radios**, then select **802.11a /n**. All the APs that are connected should be listed, showing their **Operational Status** as **UP**.
- 3 Select **Configure** from the drop-down list for the access point you wish to change. Set the parameters for that AP:



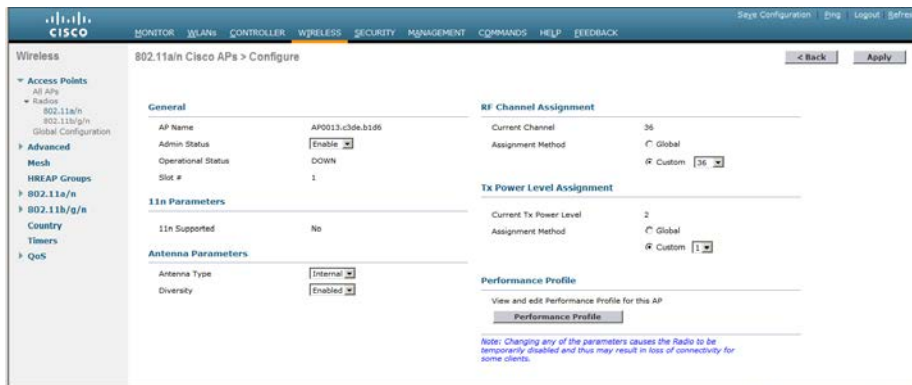


Note: Power and channel settings

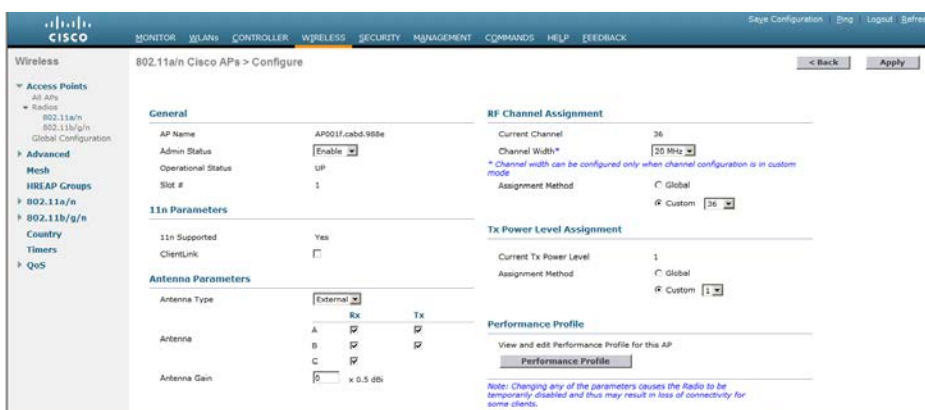
Global settings for **RF Channel Assignment** and **Tx Power Level Assignment** were not tested. For **Custom Tx Power** and **RF Channel** settings please consult your facility's RF site survey — optimized for wireless voice traffic — to determine correct power and channel settings for each AP using non-overlapping channels.

- a Set **Admin Status** to **Enable**.
- b Configure any other settings that might be relevant to your deployment as needed.
- c Click the **Apply** button to save all changes.

Screenshot for 113x, 120x, 123x and 124x series access points:



Screenshot for 104x, 114x, 125x, 126x, 350x, and 360x series access points (1040 has only 2 antennas):



- 4 In the navigation pane under **802.11a/n**, click **Network**. Set the network parameters as follows:
 - a Set **802.11a Network Status** to **Disable**; the radio will be re-enabled after setting radio parameters
 - b For setting up the **Data Rates**, please consult your facility's RF site survey, designed for voice traffic, to determine if you have sufficient coverage to support all data rates. The handset

requires the following minimum dBm reading to support the corresponding **Mandatory** data rate setting in the access point.

802.11 Radio Standard	Minimum Available Signal Strength (RSSI)	Maximum "Mandatory" Data Rate
802.11b	-70 dBm	1 Mb/s
	-60 dBm	11 Mb/s
802.11g	-63 dBm	6 Mb/s
	-47 dBm	54 Mb/s
802.11a	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s



Note: Add Title Here

For additional details on RF deployment please see the *Deploying Enterprise-Grade Wi-Fi Telephony* white paper and the *Best Practices Guide to Network Design Considerations for SpectraLink Wireless Telephone*.

- c Use the default **Fragmentation Threshold** (2346 bytes).
- d Set the **Beacon Period** to **100**.
- e SpectraLink Wireless Telephones do not support dynamic power and will not utilize the information element that is set when **DTPC support** is enabled. The handset power should be configured to match the highest transmit power of the APs.
- f Click the **Apply** button to save the settings.

The screenshot shows the Cisco Wireless Configuration Manager interface for configuring 802.11a Global Parameters. The interface includes a navigation menu on the left and a main configuration area on the right. The configuration area is divided into several sections:

- General:**
 - 802.11a Network Status: Enabled
 - Beacon Period (milliseconds): 100
 - Fragmentation Threshold (Bytes): 2346
 - DTPC Support: Enabled
- 802.11a Band Status:**
 - Low Band: Enabled
 - Mid Band: Enabled
 - High Band: Enabled
- Data Rates:****
 - 6 Mbps: Mandatory
 - 9 Mbps: Supported
 - 12 Mbps: Mandatory
 - 18 Mbps: Supported
 - 24 Mbps: Mandatory
 - 36 Mbps: Supported
 - 48 Mbps: Supported
 - 54 Mbps: Supported
- CCX Location Measurement:**
 - Mode: Enabled

At the bottom of the configuration area, there is a note: **** Data Rate "Mandatory" implies that clients who do not support that specific rate will not be able to associate. Data Rate "Supported" implies that any associated client that also supports that same rate may communicate with the AP using that rate. But it is not required that a client be able to use the rates marked supported in order to associate. The actual data rates that are supported depend on the channel selected as different channels may have different bandwidths. The reason is that we show data rates and allow the user to select the data rates. But in reality, the AP will pick the next lower data rate allowed for that channel if the chosen data rate is not supported.**

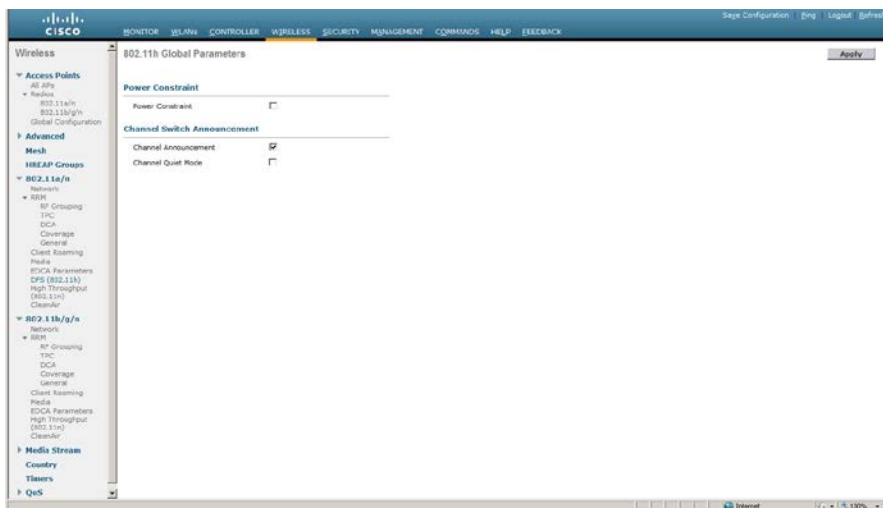
- 5 In the navigation pane under **802.11a/n**, select **EDCA Parameters**.
- 6 Select **SpectraLink Voice Priority** from the drop-down list.



Note: Add Title Here

When SpectraLink Voice Priority (SVP) is enabled under the EDCA parameters setting, the 802.11n capabilities will be disabled on that radio. It is therefore recommended to deploy handsets using SVP on a different radio than 802.11n clients.

- 7 Click the **Apply** button to save the settings.
- 8 In the navigation pane under **802.11a /n**, select **Network**.
- 9 For 802.11a Network Status, click the Enabled check box.
- 10 Click the **Apply** button to save the settings.



- 11 If DFS channels are used in the deployed network, in the navigation pane under 802.11a/n, select DFS (802.11h). Check the Channel Announcement radio box to cause the AP to advertise Spectrum Management.



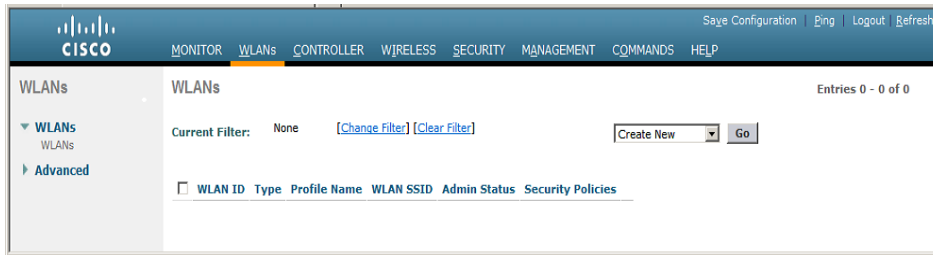
Note: Spectrum Management

If the AP does not advertise Spectrum Management, Polycom phones will not connect on DFS channels (bandwidth shared with radar facilities).

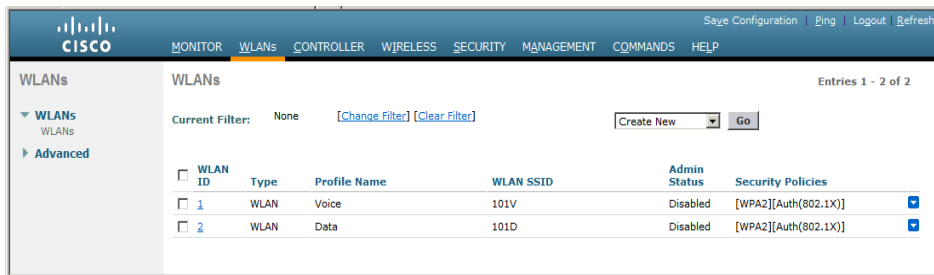
Setting up the SSID

Voice and data must be on separate SSIDs to prioritize voice traffic. The voice SSID must be set to **Platinum** for **Quality of Service** and the data SSID must be set to **Silver** for **Quality of Service**.

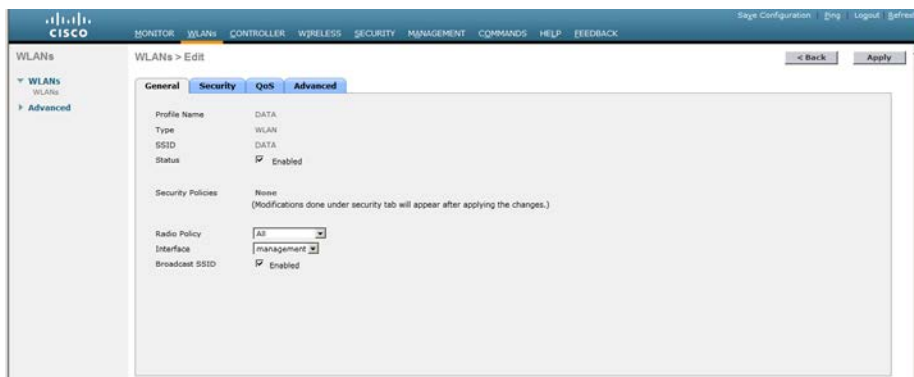
- 1 From the main menu, click **WLANs**.
- 2 In the **WLANs** screen, select Create New from the drop down list and click Go.



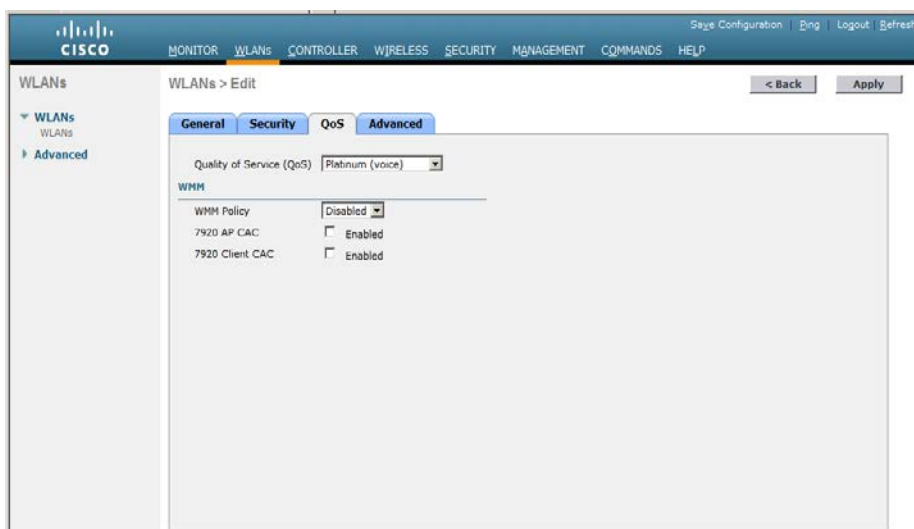
- 3 Enter the **Profile Name** and **SSID**.
- 4 Click the **Apply** button.



- 5 Select the **Profile Name** for the voice SSID.
- 6 Under the **General** tab, verify the **Radio Policy** corresponds to the SpectraLink Wireless Telephone configuration.
 - When **Radio Policy** is configured for **802.11b/g only**, the handsets should be configured for **802.11b & b/g mixed**.
 - When **Radio Policy** is configured for **802.11a only**, the handsets should be configured for **802.11a**.
 - When **Radio Policy** is configured for **802.11g only**, the handsets should be configured for **802.11g only**.
 - When **Radio Policy** is configured for **ALL**. The handsets may be configured for any of the settings without changing the **Radio Policy**.
- 7 For **Status**, select the **Enabled** check box.

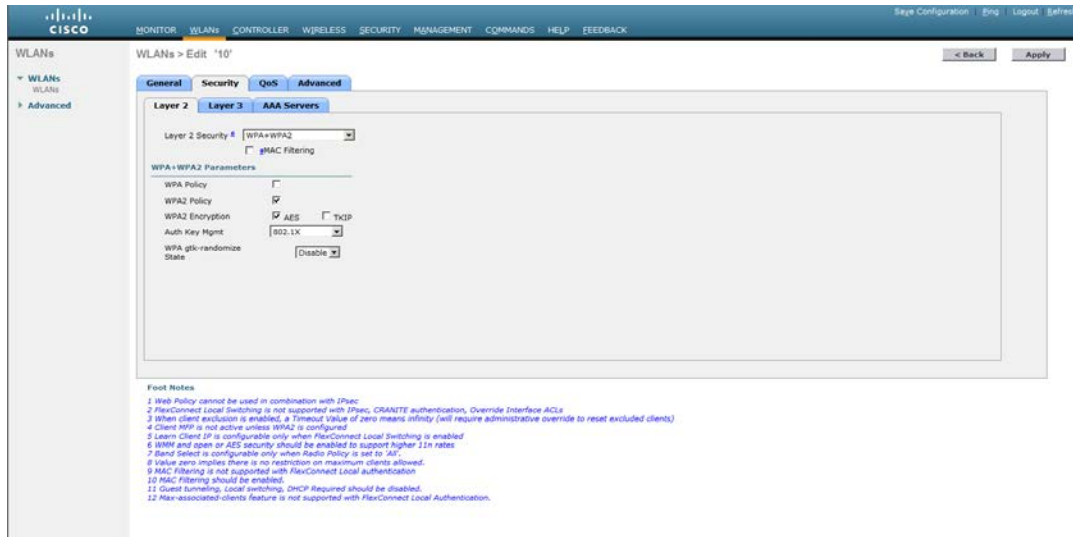


- 8 Under the **QoS** tab, set **Quality of Service** to **Platinum**. This is the required setting for voice traffic.
- 9 Set **WMM Policy** to **Disabled** (Note: This is required for usage with SpectraLink Wireless Telephones using SVP for QoS).



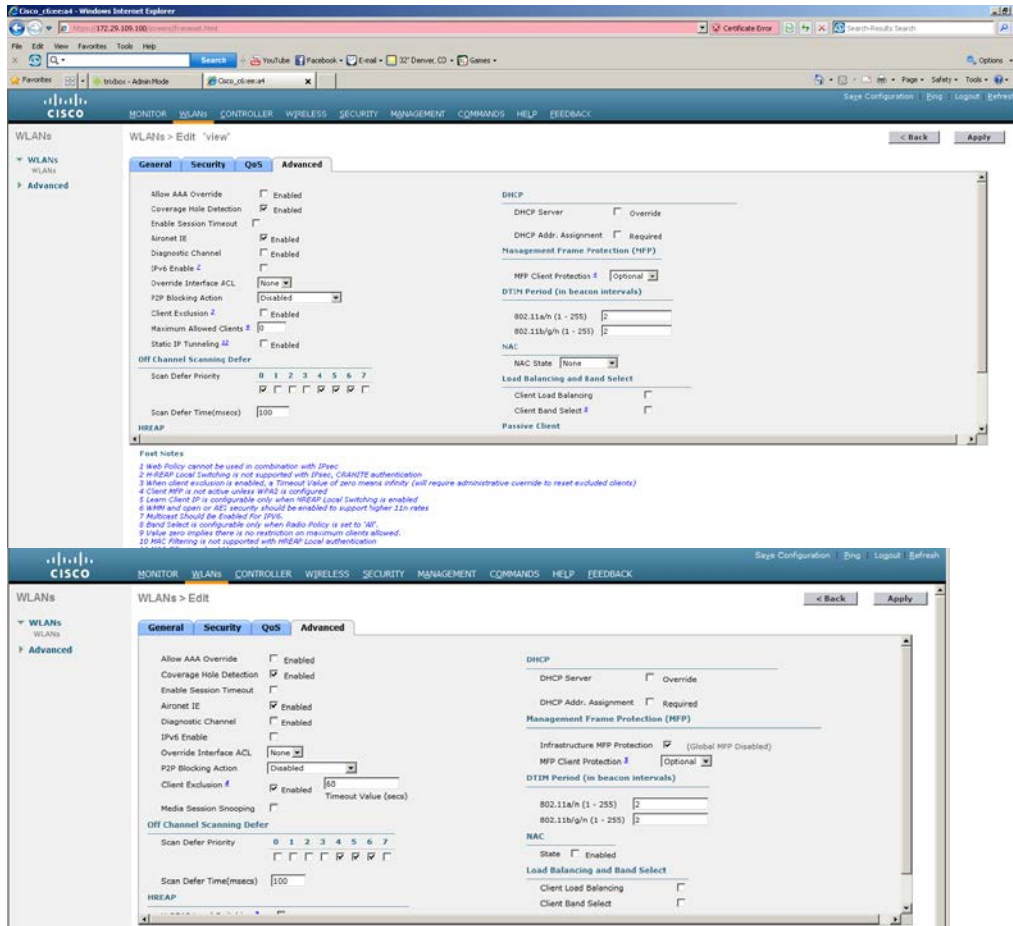
- 10 Under the **Advanced** tab, uncheck the **Client Load Balancing & Client Band Select** boxes.
- 11 Under the **Security** tab, at **Layer 2 Security** select the desired security policy from the drop-down list.
 - For **WPA2-PSK**, under **WPA+WPA2 Parameters**:
 1. Select the **WPA2-Policy** check box.
 2. Select the **AES** check box for **WPA2-Encryption**.
 3. At **Auth Key Mgmt** select **PSK** from the drop-down list.
 4. If present (version 7.2.103.0), ensure that **WPA gtk-randomize State** is set to **Disable**.
 - For **WPA-PSK**, under **WPA+WPA2 Parameters**:
 1. Select the **WPA-Policy** check box.
 2. Select the **TKIP** check box for **WPA Encryption**.

3. At **Auth Key Mgmt** select **PSK** from the drop-down list. The **PSK Format** may be selected as **ASCII** or **HEX** for both WPA-PSK and WPA2-PSK policies.
 4. If present (version 7.2.103.0), ensure that **WPA gtk-randomize State** is set to **Disable**.
- For WPA2-Enterprise (802.1X), select **WPA+WPA2 Parameters**:
 1. Select the **WPA2-Policy** check box.
 2. Select the **AES** check box for **WPA2 Encryption**.
 3. At **Auth Key Mgmt**, select **802.1X+CCKM** from the drop-down list.
 4. If present (version 7.2.103.0), ensure that **WPA gtk-randomize State** is set to **Disable**.



12 Under the **Advanced** tab

- a **Set the DTIM to 2** for the **radio** that corresponds to the SpectraLink Wireless Telephone configuration.
- b Ensure the **Enable Session Timeout** box is unchecked and that **Client Exclusion** is disabled.
- c Uncheck the **Client Load Balancing** and **Client Band Select** boxes.
- d Check off-channel scanning defer for the 0 priority class (prevents contention between off-channel scanning and PTT).



13 Click the **Apply** button to save all changes.

Appendix A

SpectralLink 8400 handsets must be configured with the 802.11n mode disabled when used with Cisco AP 114x and 125x with versions prior to 6.0.202.0. The use of 802.11n in the phones can only be disabled from a provisioning configuration file for the phone. It cannot be accessed from browser provisioning, USB provisioning, application menus, or updater (initial bootup) menus. See Polycom® SpectralLink® 8400 Series Wireless Telephone Deployment Guide, found at <http://support.polycom.com/PolycomService/support/us/support/voice/wi-fi/index.html> for instructions on provisioning an 8400 phone from a provisioning server.

Add the following lines to a .cfg file downloaded to the phone:

```
<device device.set = "1"  
  device.wifi.dot11n.enabled.set = "1"  
  device.wifi.dot11n.enabled = "0">  
</device>
```

To check that the disable was successful:

- 1 Select **Settings** from the menu by pressing the left or right navigation button until Settings is displayed.
- 2 Select **Status->Diagnostics->Wi-Fi Stats**.
- 3 Click on the **Prev** softkey.
- 4 The following picture should have a line stating that 802.11n is **Disabled**. If the line is not shown, 802.11n is not disabled: no line will be displayed under last EAP Err Code.

