



VIEW Configuration Guide

Cisco

1131, 1232 and 1242 Autonomous APs

Patent Information

The accompanying product is protected by one or more US and foreign patents and/or pending patent applications held by Polycom, Inc.

Copyright Notice

© 2009, 2010, Polycom, Inc. All rights reserved. POLYCOM®, the Polycom "Triangles" logo and the names and marks associated with Polycom's 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.

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 Polycom, Inc.

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

Every effort has been made to ensure that the information in this document is accurate. Polycom, Inc. is not responsible for printing or clerical errors. Information in this document is subject to change without notice and does not represent a commitment on the part of Polycom, Inc.

Notice

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

Polycom 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 Polycom 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 POLYCOM FOR ANY PURPOSE, OR GIVE RISE TO ANY LIABILITY OF POLYCOM WHATSOEVER.

Contact Information

Please contact your Polycom Authorized Reseller for assistance.

Polycom, Inc.
4750 Willow Road,
Pleasanton, CA 94588
<http://www.polycom.com>

Contents

Overview.....	4
Product Summary	4
Known Limitations	5
Access Point Capacity and Positioning.....	5
Network Topology	6
AP Configuration Setup	7
Installing Software	8
Quality of Service	9
SVP QoS Configuration.....	9
Wi-Fi Standard and CCX QoS Configuration.....	13
Security	21
Radio Settings.....	31

Overview

Polycom’s Voice Interoperability for Enterprise Wireless (VIEW) Certification Program is designed to ensure interoperability and high performance between SpectraLink 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 the Cisco 1131, 1232 and 1242 Access Points (APs) with SpectraLink Wireless Telephones.

Product Summary

Manufacturer:	Cisco Systems: www.cisco.com	
Approved models:	AP 1131, 1232, 1242	
AP Radio(s):	2.4 GHz (802.11b/g), 5 GHz (802.11a)	
Security :	WPA-PSK, WPA2-PSK, WPA2-Enterprise** (EAP-FAST and PEAPv0/MSCHAPv2), Cisco FSR	
QoS:	SVP, Wi-Fi Standard**, CCX**	
AP firmware version(s) tested:	model 1131/1242: 12.4(10b)JDA model 1232: 12.3.8JEC2	
Handset models tested:	SpectraLink 8020/8030 Wireless Telephone*	
Handset software tested:	201.034	
Radio mode:	802.11b	802.11a
Meets VIEW minimum call capacity per AP:	8 calls (SVP) 6 (Wi-Fi Standard QoS)** 6 (CCX)**	12 calls (SVP) 8 (Wi-Fi Standard QoS)** 8 (CCX)**
Network topology:	Switched Ethernet (recommended)	

*SpectraLink handset models 8020/8030 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” or “handsets”.

** ONLY Release 3.0 capable handsets support WPA2-Enterprise, Wi-Fi Standard QoS, and CCXv4. Release 3.0 is not available for Polycom handsets connecting to traditional PBXs.

Known Limitations

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.



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

Access Point Capacity and Positioning

Please refer to the Polycom *Deploying Enterprise-Grade Wi-Fi Telephony* white paper. This document covers the security, coverage, capacity and QoS considerations necessary for ensuring excellent voice quality with enterprise Wi-Fi networks.

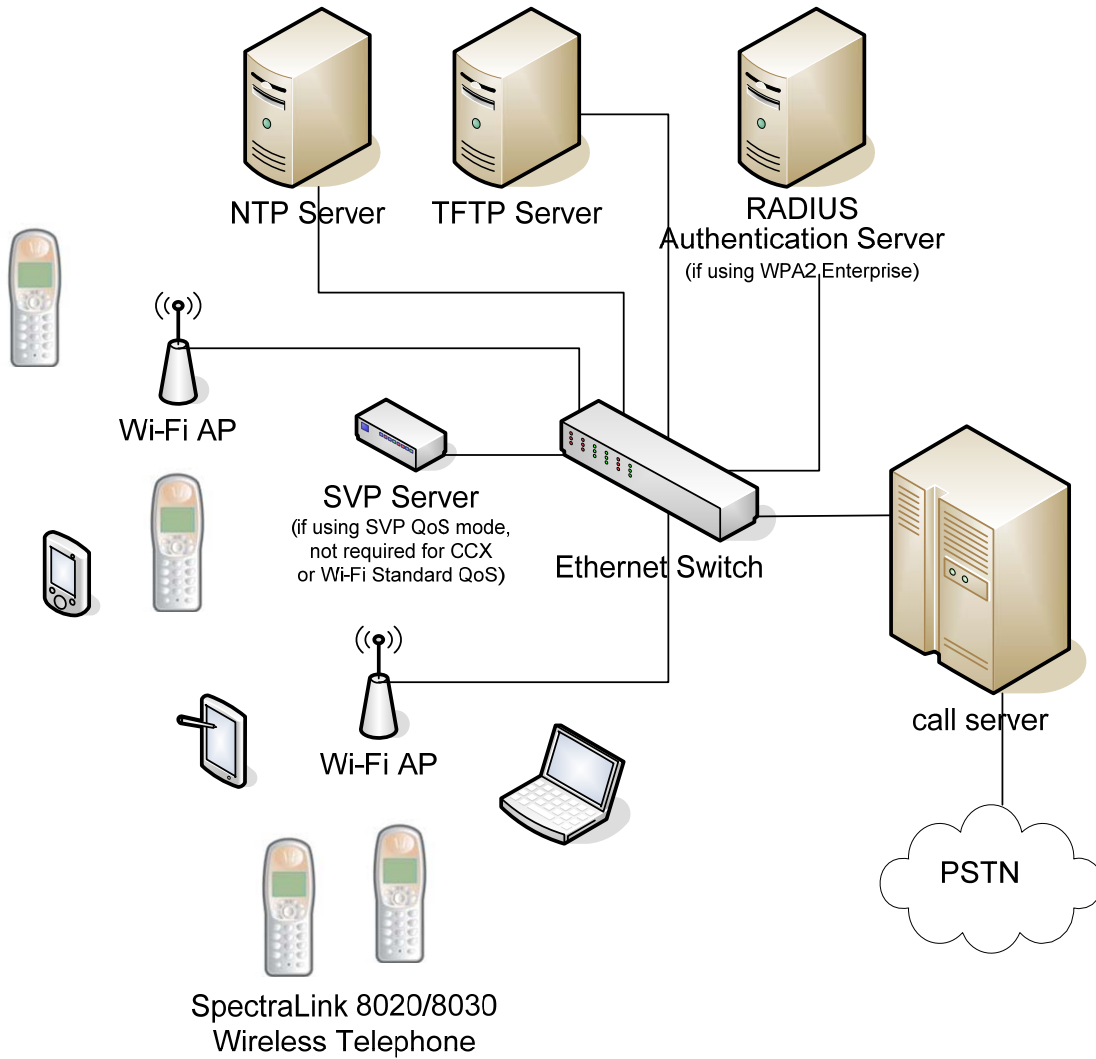
For more detailed information on wireless LAN layout, network infrastructure, QoS, security and subnets, please see the *Best Practices Guide for Deploying SpectraLink 8020/8030 Wireless Telephones*. This document identifies issues and solutions based on Polycom's extensive experience in enterprise-class Wi-Fi telephony, providing recommendations for ensuring that a network environment is adequately optimized for use with SpectraLink 8020/8030 Wireless Telephones.

These two white papers are available at:

http://www.polycom.com/products/voice/wireless_solutions/wifi_communications/handsets/spectralink_8020_wireless.html

Network Topology

The following topology was used during certification testing. It is important to note that this does not necessarily represent all possible configurations.



AP Configuration Setup

Initial setup

1. Go to the Cisco Web site at <http://www.cisco.com>
2. Navigate to the **Download Software** Web page by clicking **Support>Software Downloads**.
3. Select **Cisco IOS Software**.
4. Enter your **Username** and **Password** to gain access.
5. Download the correct code version for the access point model, listed in the table on page 3.

Assigning an IP address to a new AP

It is sometimes more convenient to assign an IP address to the access point using the command line interface (CLI). The steps are described below.

1. Connect the PC's serial port to the AP via the CLI cable. Open a terminal program, such as HyperTerminal. Configure the settings to 9600 baud, 8 data bits, no parity.
2. At the prompt, type **enable**.
3. Type in the password; default password is **Cisco**.
4. Type in the command **configure terminal**.
5. Type in the command **interface BVI 1**.
6. Type ip address <ip address> <net mask>.
7. Type **end** and then **write mem** to save configuration.

The rest of the configuration can easily be done through the browser interface.

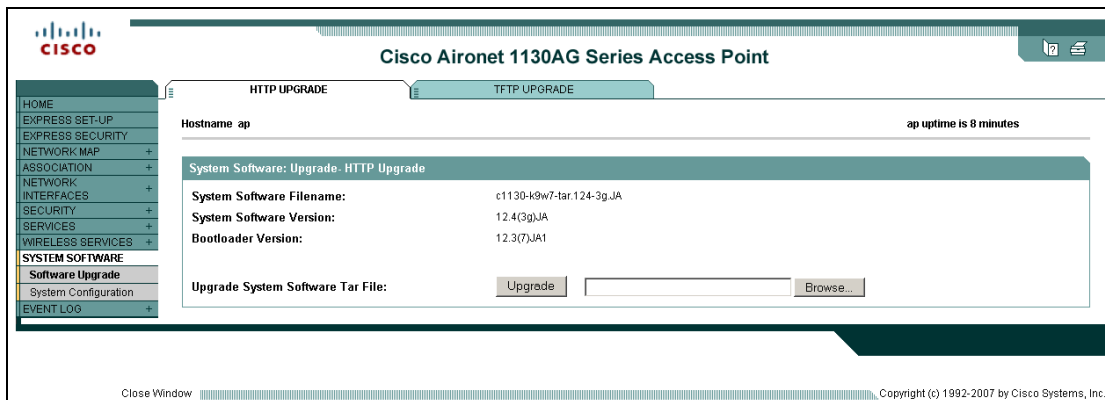
Log into the AP via a Web browser, using the IP address assigned in the above step.

Connecting to the AP

Connect to the AP via Netscape or Internet Explorer by entering the URL: http://<IP_Addr> (where <IP_Addr> is the IP address of the AP).

Installing Software

1. Download the appropriate firmware for your model AP from the **Cisco IOS Software Downloads** Web site.
2. Connect to the AP via a browser, preferably IE. Turn off pop-up blocking (See the **Tools** menu in IE).
3. In the navigation pane, click **SYSTEM SOFTWARE**.
4. Select **Software Upgrade** from the sub-menu.
5. Click the **HTTP UPGRADE** tab.
6. Use the **Browse** button to select the **tar** image.
7. Click the **Upgrade** button.



8. Allow at least five minutes for the upgrade to complete. The progress of the upgrade can be tracked via the AP's LEDs.
 - Center LED ON means image is being downloaded.
 - All LEDs ON means AP is decompressing the image, rebooting, etc.
 - Top LED GREEN, radio and status LEDs BLINKING, means Ethernet connectivity is OK, normal operation.
9. The Web browser opens a window indicating the amount of time since the upgrade started. After the upgrade is completed, this window may stay open. The user will need to close these window(s) and refresh browser's connection to the AP.

Quality of Service

The handset supports the following three Quality of Service (QoS) modes:

- SVP (Spectralink Voice Priority)
- Wi-Fi Standard (WMM-Power Save and WMM-Admission Control)
- CCX (Cisco Compatible Extensions)

Configuring the AP for QoS is distinctly different depending what the desired QoS mode is.

SVP QoS Configuration

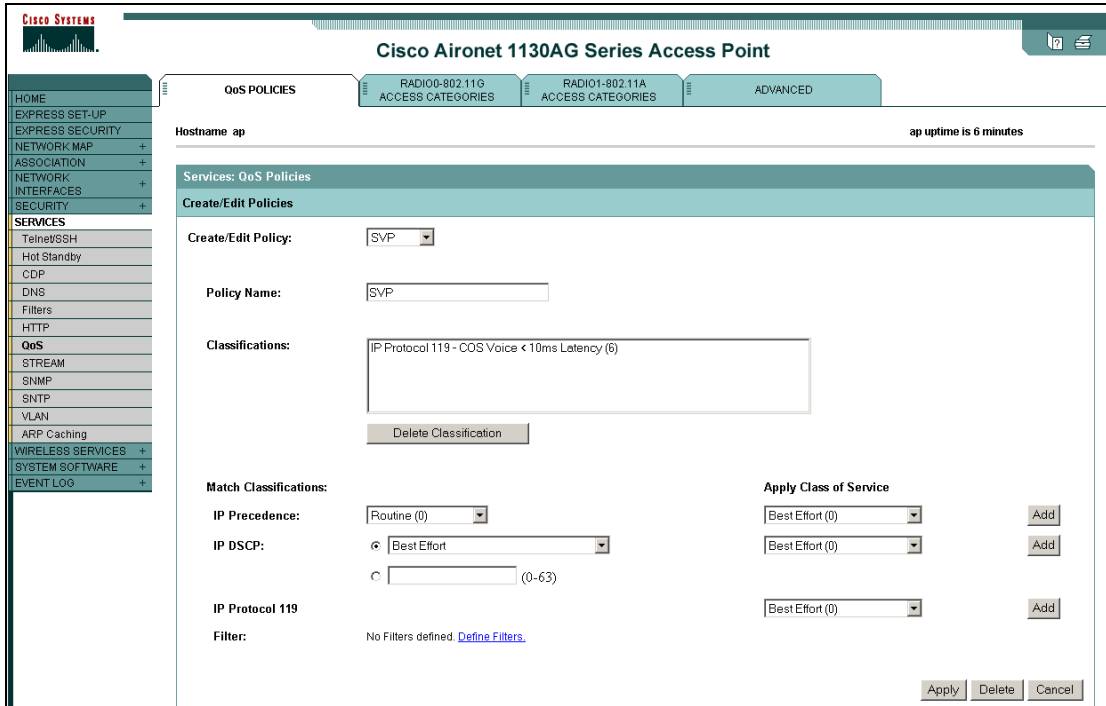
QoS Policy

1. In the navigation pane, click **SERVICES**.
2. Select **QoS** from the sub-menu.

The screenshot shows the configuration page for a Cisco Aironet 1130AG Series Access Point. The page title is "Cisco Aironet 1130AG Series Access Point". The hostname is "ap" and the uptime is 3 minutes. The left navigation pane is expanded to "SERVICES" and "QoS" is selected. The main content area displays a "Services Summary" table with the following data:

Services Summary	
Telnet/SSH : Enabled/Disabled	Hot Standby : Disabled
CDP : Enabled	DNS : Disabled
Filters : Disabled	HTTP : Enabled
QoS : Policy Defined	STREAM : Disabled
SNMP : Disabled	SNTP : Disabled
VLAN : Disabled	ARP Caching : Disabled

3. At **Create/Edit Policy**, create and name a new QoS policy.
4. From to the drop-down list under **Apply Class of Service** (to the far right of **IP Protocol 119**), select **Voice <10ms Latency (6)**.
5. Click **Add** to add this classification to your new QoS policy.
6. Click the **Apply** button.



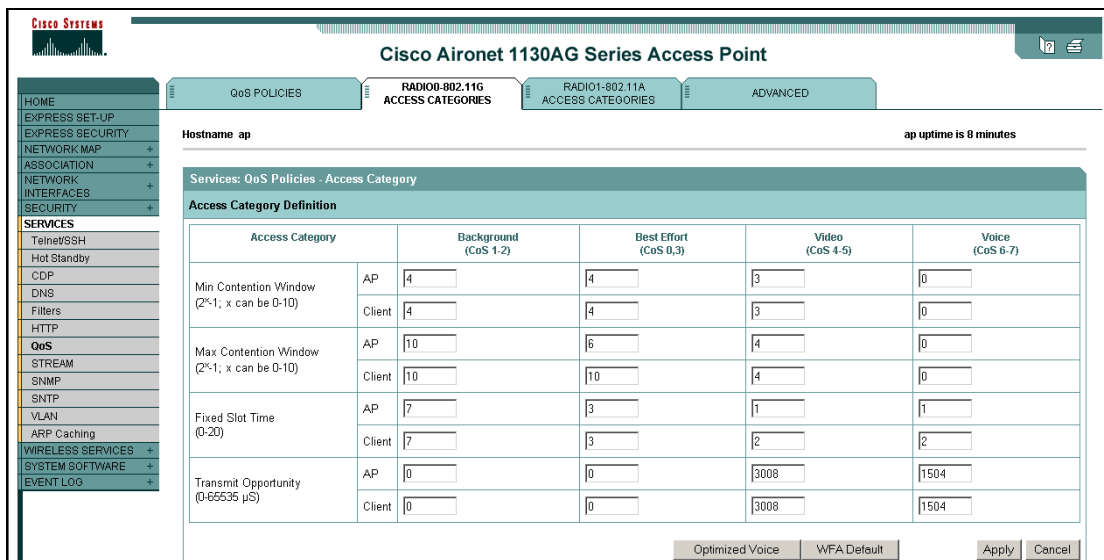
7. Under **Apply Policies to Interface/VLANs**, use the drop-down lists to apply the new QoS policy to:
 - a. **Incoming** for the **FastEthernet**
 - b. **Incoming** and **Outgoing** for the **Radio0-802.11G**
 - c. **Incoming** and **Outgoing** for the **Radio1-802.11A** for the appropriate interfaces of VLAN.
8. Click the **Apply** button.

Apply Policies to Interface/ VLANs			
	FastEthernet	Radio0-802.11G	Radio1-802.11A
Incoming	SLNK	SLNK	SLNK
Outgoing	< NONE >	SLNK	SLNK
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

Radio 802.11g access categories

(if SpectraLink Wireless Telephones are operating in 802.11 b and b/g mixed or 802.11g only mode and SVP QoS is being used)

1. Click the **RADIO0-802.11G ACCESS CATEGORIES** tab.
2. Under **Voice (CoS 6-7)**, set the **Min Contention Window** and **Max Contention Window** to **0**.
3. Leave the other settings at their default settings as shown.
4. Click the **Apply** button.



The screenshot shows the configuration page for a Cisco Aironet 1130AG Series Access Point. The page is titled "Cisco Aironet 1130AG Series Access Point" and has tabs for "QoS POLICIES", "RADIO0-802.11G ACCESS CATEGORIES", "RADIO1-802.11A ACCESS CATEGORIES", and "ADVANCED". The "RADIO0-802.11G ACCESS CATEGORIES" tab is selected. The page shows the "Access Category Definition" table with the following data:

Access Category		Background (CoS 1,2)	Best Effort (CoS 0,3)	Video (CoS 4-5)	Voice (CoS 6-7)
Min Contention Window (2^x-1; x can be 0-10)	AP	4	4	3	0
	Client	4	4	3	0
Max Contention Window (2^x-1; x can be 0-10)	AP	10	6	4	0
	Client	10	10	4	0
Fixed Slot Time (0-20)	AP	7	3	1	1
	Client	7	3	2	2
Transmit Opportunity (0-65535 μS)	AP	0	0	3008	1504
	Client	0	0	3008	1504

At the bottom of the table, there are buttons for "Optimized Voice", "WFA Default", "Apply", and "Cancel".



Do not click the **Optimized Voice** button. If this button is clicked, the SpectraLink Wireless Telephones will not ring.

Radio 802.11a access categories

(if SpectraLink Wireless Telephones are operating in 802.11a mode)

1. Click the **RADIO1-802.11A ACCESS CATEGORIES** tab.
2. Under **Voice (CoS 6-7)** set the **Min Contention Window** and **Max Contention Window** to **0**.
3. Leave the other settings at their default settings as shown.
4. Click the **Apply** button.

The screenshot shows the configuration page for a Cisco Aironet 1130AG Series Access Point. The 'RADIO1-802.11A ACCESS CATEGORIES' tab is selected. The page displays the 'Services: QoS Policies - Access Category' section, which includes an 'Access Category Definition' table. The table has columns for 'Access Category', 'Background (CoS 1-2)', 'Best Effort (CoS 0,3)', 'Video (CoS 4-5)', and 'Voice (CoS 6-7)'. The 'Voice' column settings are highlighted in the instructions. At the bottom of the table, there are buttons for 'Optimized Voice', 'WFA Default', 'Apply', and 'Cancel'.

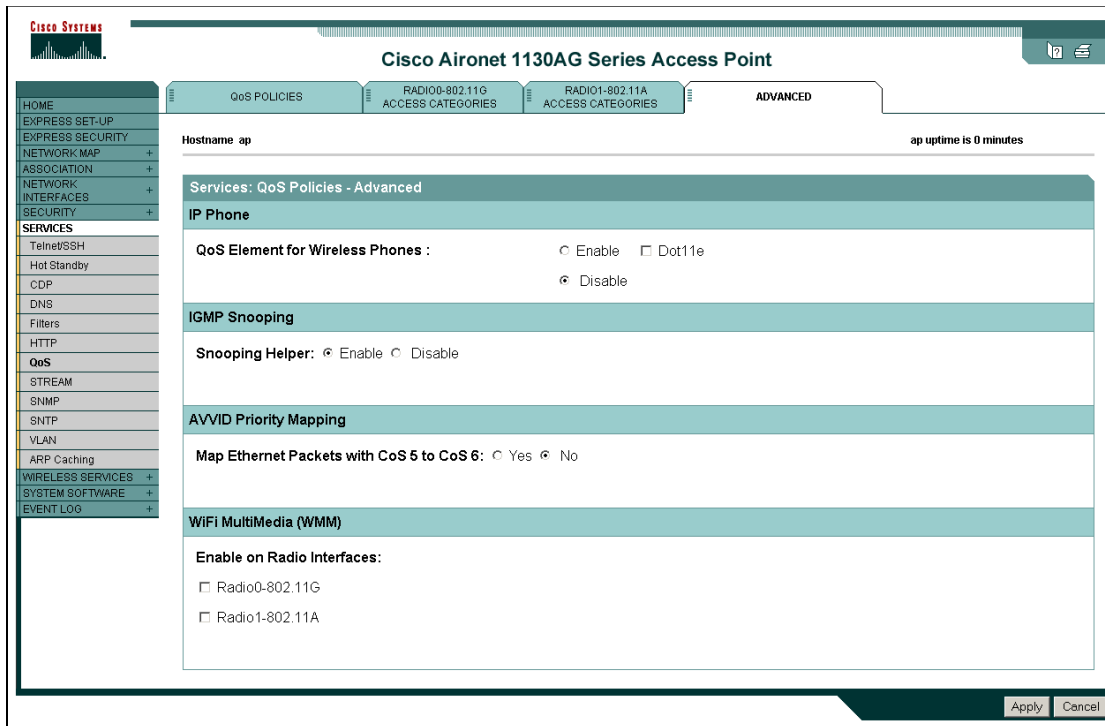
Access Category		Background (CoS 1-2)	Best Effort (CoS 0,3)	Video (CoS 4-5)	Voice (CoS 6-7)
Min Contention Window (2 ^x ; 1; x can be 0-10)	AP	5	5	4	0
	Client	5	5	4	0
Max Contention Window (2 ^x ; 1; x can be 0-10)	AP	10	6	5	0
	Client	10	10	5	0
Fixed Slot Time (0-20)	AP	7	3	1	1
	Client	7	3	2	2
Transmit Opportunity (0-65535 μS)	AP	0	0	3008	1504
	Client	0	0	3008	1504



Do not click the **Optimized Voice** button. If this button is clicked, the SpectraLink Wireless Telephones will not ring.

Advanced tab

1. Click the **ADVANCED** tab.
2. Under **QoS Element for Wireless Phones**, select the **Disable** option.
3. Disable **Wi-Fi MultiMedia (WMM)**, which is set by default.
4. Click the **Apply** button.



Wi-Fi Standard and CCX QoS Configuration

QoS policy

1. In the navigation pane, click **SERVICES**.
2. Select **QoS** from the sub-menu.

Create a policy to map DSCP values for voice and control packets.

Assume that a DSCP value of 46 is used for voice packets and 40 for PBX control packets.

1. Name the policy in the **Policy Name** field. For example **WMM-PS**.

2. To customize voice priorities, select the **IP DSCP** field, enter **46** in the text field, select **Voice < 10ms Latency (6)** as the class of service, and click the **Add** button.
3. Likewise, to configure control packet priorities select the **IP DSCP** field, enter **40** in the text field, select **Controlled Load (4)** as the class of service, and click the **Add** button. This results in two classifications.
4. Click the **Apply** button in the **Create/Edit Policies** section of the screen.

Create/Edit Policies

Create/Edit Policy: WMM-PS

Policy Name: WMM-PS

Classifications: DSCP Expedited Forwarding - COS Voice < 10ms Latency (6)
DSCP Class Selector 5 - COS Controlled Load (4)

Delete Classification

<p>Match Classifications:</p> <p>IP Precedence: Routine (0)</p> <p>IP DSCP: <input checked="" type="radio"/> Best Effort <input type="radio"/> (0-63)</p> <p>IP Protocol 119: Best Effort (0)</p> <p>Filter: No Filters defined. Define Filters.</p> <p>Rate Limiting:</p> <p>Bits per Sec.: (8000-2000000000) Burst Rate (Bytes): (1000-512000000)</p> <p>Conform Action: Transmit Exceed Action: Drop</p>	<p>Apply Class of Service</p> <p>Best Effort (0) Add</p> <p>Best Effort (0) Add</p> <p>Best Effort (0) Add</p>
---	---

Apply Delete Cancel

Associate the QoS policy created in the previous step

Assuming both radios are being used, perform the following steps under **Apply Policies to Interface/VLANS**:

1. Select **WMM-PS** for the following network interfaces:
 - a. **Incoming** for the **FastEthernet**
 - b. **Incoming** and **Outgoing** for the **Radio0-802.11G**
 - c. **Incoming** and **Outgoing** for the **Radio1-802.11A**

- Click the **Apply** button to save the QoS policies.

Apply Policies to Interface/ VLANs			
	FastEthernet	Radio0-802.11G	Radio1-802.11A
Incoming	WMM-PS ▾	WMM-PS ▾	WMM-PS ▾
Outgoing	< NONE > ▾	WMM-PS ▾	WMM-PS ▾
			<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

Use WFA Defaults for Access Categories

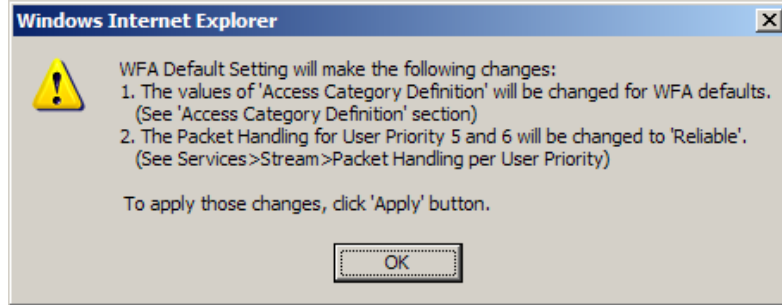
- For each radio used by the handsets, go to the **Access Categories** tab in the **QoS Services** menu.

<input type="button" value="QoS POLICIES"/>	<input checked="" type="button" value="RADIO0-802.11G ACCESS CATEGORIES"/>	<input type="button" value="RADIO1-802.11A ACCESS CATEGORIES"/>	<input type="button" value="ADVANCED"/>
---	--	---	---

- Click the **WFA Default** button to reset all access category settings to the WFA default.

Services: QoS Policies - Access Category					
Access Category Definition					
Access Category		Background (CoS 1-2)	Best Effort (CoS 0,3)	Video (CoS 4-5)	Voice (CoS 6-7)
Min Contention Window (2 ^x -1; x can be 0-10)	AP	<input type="text" value="4"/>	<input type="text" value="4"/>	<input type="text" value="3"/>	<input type="text" value="2"/>
	Client	<input type="text" value="4"/>	<input type="text" value="4"/>	<input type="text" value="3"/>	<input type="text" value="2"/>
Max Contention Window (2 ^x -1; x can be 0-10)	AP	<input type="text" value="10"/>	<input type="text" value="6"/>	<input type="text" value="4"/>	<input type="text" value="3"/>
	Client	<input type="text" value="10"/>	<input type="text" value="10"/>	<input type="text" value="4"/>	<input type="text" value="3"/>
Fixed Slot Time (0-20)	AP	<input type="text" value="7"/>	<input type="text" value="3"/>	<input type="text" value="1"/>	<input type="text" value="1"/>
	Client	<input type="text" value="7"/>	<input type="text" value="3"/>	<input type="text" value="2"/>	<input type="text" value="2"/>
Transmit Opportunity (0-65535 μS)	AP	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="3008"/>	<input type="text" value="1504"/>
	Client	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="3008"/>	<input type="text" value="1504"/>
			<input type="button" value="Optimized Voice"/> <input type="button" value="WFA Default"/>	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- Click **OK** to accept the notification message.

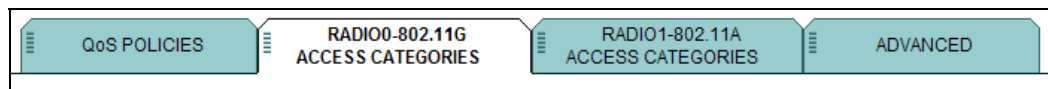


- Click the **Apply** button in the **Services: QoS Policies – Access Category** section to save the WFA default settings.

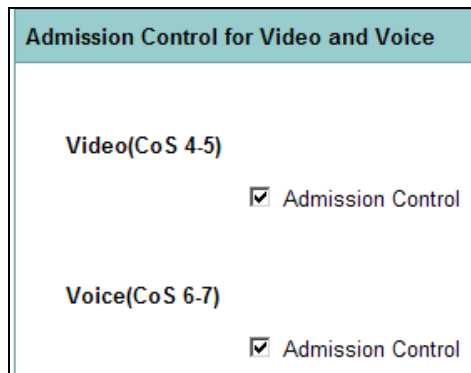
Enable Admission Control

(Highly recommended, all wireless clients must use Admission Control)

- For each radio used by the handsets, go to the **Access Categories** tab in the **QoS Services** menu.



- Enable both **Video** and **Voice** admission control.

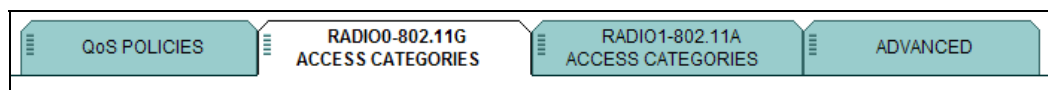


- Click the **Apply** button to save selections.

Disable Admission Control

(Only required if using a combination of SpectraLink 8002 and 8020/8030 handsets)

- For each radio used by the handsets, go to the **Access Categories** tab in the **QoS Services** menu.



2. Disable both **Video** and **Voice** admission control.

Admission Control for Video and Voice

Video(CoS 4-5)

Admission Control

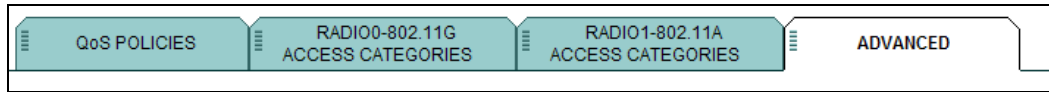
Voice(CoS 6-7)

Admission Control

3. Click the **Apply** button to save selections.

Enable WMM

1. Go to the **ADVANCED** tab in the **QoS Services** menu.

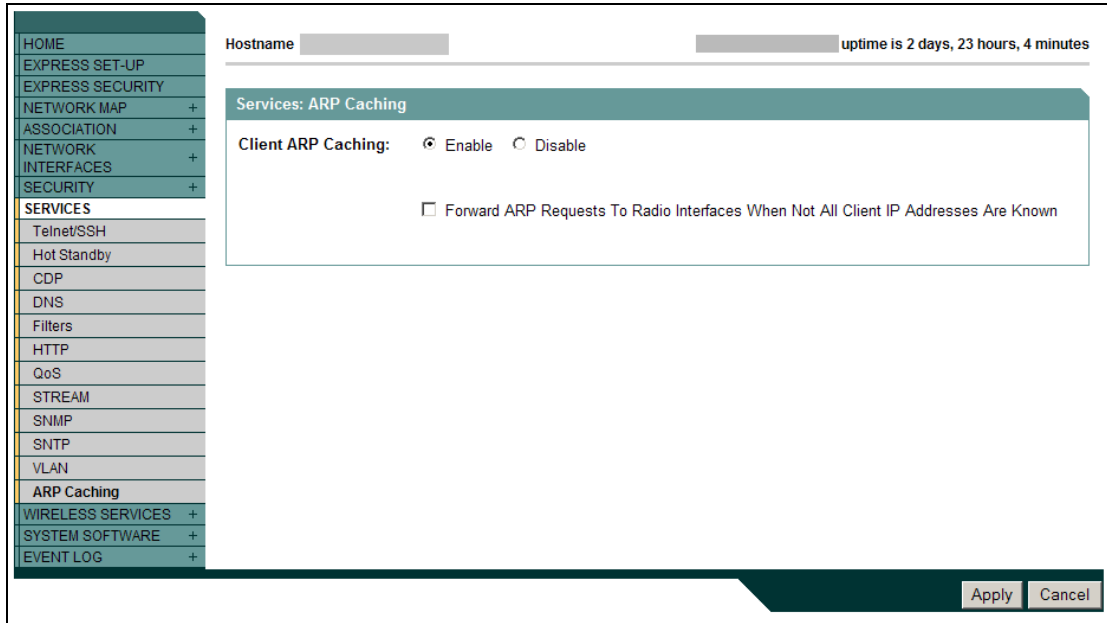


2. Enable **WMM** for all radios used by handsets.
3. Disable **QoS Element for Wireless Phones**.
4. Disable **IGMP Snooping**.
5. Select **No** for **AVVID Priority Mapping**.
6. Click **Apply** to save **ADVANCED** settings.

Services: QoS Policies - Advanced	
IP Phone	
QoS Element for Wireless Phones :	<input type="radio"/> Enable <input type="checkbox"/> Dot11e <input checked="" type="radio"/> Disable
IGMP Snooping	
Snooping Helper:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
AVVID Priority Mapping	
Map Ethernet Packets with CoS 5 to CoS 6:	<input type="radio"/> Yes <input checked="" type="radio"/> No
WiFi MultiMedia (WMM)	
Enable on Radio Interfaces:	
<input checked="" type="checkbox"/>	Radio0-802.11G
<input checked="" type="checkbox"/>	Radio1-802.11A

Enable ARP Caching/Proxy ARP

1. Under **SERVICES**, go to **ARP Caching**.
2. Enable **Client ARP Caching**.
3. Click the **Apply** button to save settings.



Security

Encryption manager

1. In the navigation pane, click **SECURITY**.
2. Select **Encryption Manager** from the sub-menu.
3. Under **Encryption Modes**, click the **Cipher** option.
4. For WPA-PSK, select **TKIP** from the **Cipher** drop-down list. For WPA2-PSK or WPA2-Enterprise, select **AES CCMP** from the drop-down list.
5. Under **Encryption Keys**, clear all **Encryption Key** fields.
6. Under **Global Properties**, select the **Disable Rotation** option.
7. Click the **Apply** button.

The screenshot displays the 'Security: Encryption Manager' configuration interface. On the left is a navigation pane with categories like EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area is titled 'Security: Encryption Manager' and contains the following sections:

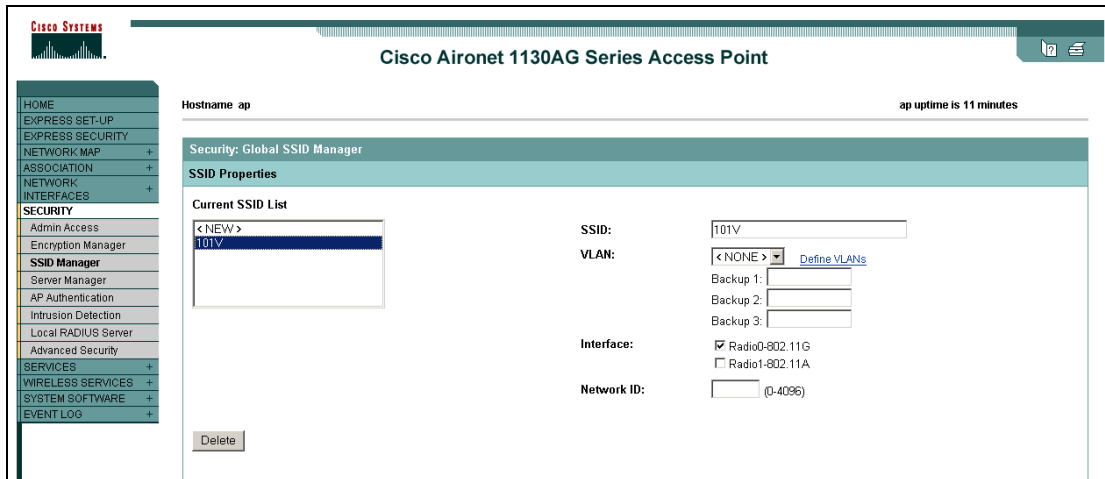
- Encryption Modes:**
 - None
 - WEP Encryption Optional
 - Cipher AES CCMP

Cisco Compliant TKIP Features: Enable Message Integrity Check (MIC) Enable Per Packet Keying (PPK)
- Encryption Keys:**

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 2:	<input checked="" type="radio"/>	<input type="text"/>	128 bit
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	128 bit
- Global Properties:**
 - Broadcast Key Rotation Interval:**
 - Disable Rotation
 - Enable Rotation with Interval: DISABLED (10-10000000 sec)
 - WPA Group Key Update:**
 - Enable Group Key Update On Membership Termination
 - Enable Group Key Update On Member's Capability Change

SSID manager

1. In the navigation pane, click **SECURITY**.
2. Select **SSID Manager** from the sub-menu.
3. Under **Current SSID List**, select the proper SSID from list box, or create a new one if necessary. Make sure the correct radio interface is selected, **Radio0-802.11G** or **Radio1-802.11A**.



4. Under **Authentication Settings**, select the **Open Authentication** check box.

Configure Open Authentication

1. For WPA-PSK or WPA2-PSK:
 - a. Select the **Open Authentication** check box.
 - b. Select **<No Addition>** from the drop-down list.



2. For WPA2-Enterprise:
 - a. Select the **Open Authentication** check box.
 - b. Select **with EAP** from the drop-down list.

Methods Accepted:

<input checked="" type="checkbox"/> Open Authentication:	with EAP
<input type="checkbox"/> Shared Authentication:	< NO ADDITION >
<input type="checkbox"/> Network EAP:	< NO ADDITION >

3. For Cisco FSR:
 - a. Select the **Open Authentication** check box.
 - b. Select **No Addition** from the drop-down list.
 - c. Select the **Network EAP** check box.
 - d. Select **No Addition** from the drop-down list.

Methods Accepted:

<input checked="" type="checkbox"/> Open Authentication:	< NO ADDITION >
<input type="checkbox"/> Shared Authentication:	< NO ADDITION >
<input checked="" type="checkbox"/> Network EAP:	< NO ADDITION >

Configure EAP Authentication Servers

Use the default settings for **Server Priorities**.



For WPA2-Enterprise security, the defaults will need to be defined.

Server Priorities:

<p>EAP Authentication Servers</p> <p><input checked="" type="radio"/> Use Defaults Define Defaults</p> <p><input type="radio"/> Customize</p> <p>Priority 1: <input type="text" value="< NONE >"/></p> <p>Priority 2: <input type="text" value="< NONE >"/></p> <p>Priority 3: <input type="text" value="< NONE >"/></p>	<p>MAC Authentication Servers</p> <p><input checked="" type="radio"/> Use Defaults Define Defaults</p> <p><input type="radio"/> Customize</p> <p>Priority 1: <input type="text" value="< NONE >"/></p> <p>Priority 2: <input type="text" value="< NONE >"/></p> <p>Priority 3: <input type="text" value="< NONE >"/></p>
---	---

Configure Client Authenticated Key Management:

1. Select **Mandatory** from the **Key Management** drop-down list.
2. Select the **Enable WPA** check box.
3. For CCX mode operation, Cisco FSR security or CCKM Fast Roaming when using WPA2-Enterprise security, select the **CCKM** check box.
4. For WPA-PSK or WPA2-PSK configure the **WPA Pre-shared Key** field. Type in the key code used in the handsets, and select the **ASCII** option. Characters are case-sensitive.

Client Authenticated Key Management

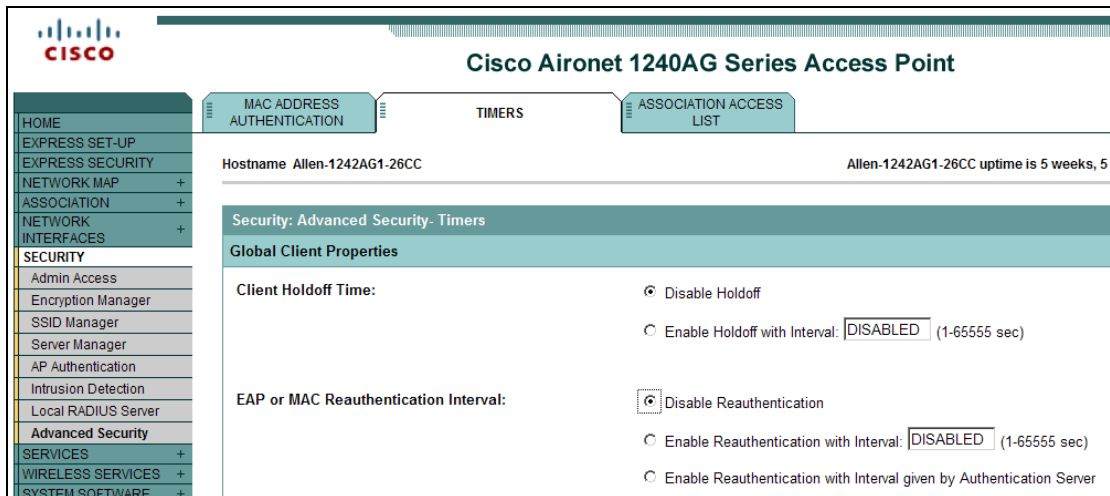
Key Management: CCKM Enable WPA

WPA Pre-shared Key: ASCII Hexadecimal

5. **IMPORTANT:** If Wi-Fi Standard QoS or CCX is being used, you must enable **Call Admission Control**. A handset configured for Wi-Fi Standard QoS or CCX will not associate with an AP that does not have this option enabled.

Call Admission Control: Enable Disable

6. Click the **Apply** button.
7. Disable session timeout:
 - a. In the navigation pane, select **Advanced Security**.
 - b. Click the **TIMERS** tab.
 - c. Select the **Disable Reauthentication** option.
8. Click the **Apply** button.



The screenshot shows the configuration page for a Cisco Aironet 1240AG Series Access Point. The navigation pane on the left includes sections for HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, and SYSTEM SOFTWARE. The main content area is titled "Cisco Aironet 1240AG Series Access Point" and has tabs for MAC ADDRESS AUTHENTICATION, TIMERS, and ASSOCIATION ACCESS LIST. The TIMERS tab is active, showing the Hostname as "Allen-1242AG1-26CC" and uptime as "Allen-1242AG1-26CC uptime is 5 weeks, 5". Under "Security: Advanced Security - Timers", the "Global Client Properties" section is visible. The "Client Holdoff Time" is set to "Disable Holdoff". The "EAP or MAC Reauthentication Interval" is set to "Disable Reauthentication".



This setting is a workaround for a known issue regarding Cisco Autonomous APs running 12.4(10b)JDA firmware. At session timeout the AP initiates an unencrypted EAPOL message instead of initiating full EAP Authentication in an encrypted tunnel where all the messages will be encrypted with existing session keys. This occurs only when the handset is associated using the fast roaming technique CCKM. If session timeouts are absolutely required, then the recommended minimum setting of 8 hours will minimize the impact of this issue.

Server manager (WPA2-Enterprise and Cisco FSR only)

1. In the navigation pane, click **SECURITY** and select **Server Manager**.
2. Configure a new Corporate Server:
 - a. Select **RADIUS** from the dropdown list.
 - b. Enter hostname or IP address in the **Server** field.
 - c. Enter shared secret in the **Shared Secret** field.
3. Click the **Apply** button.

Corporate Servers

Current Server List

RADIUS ▾

<div style="border: 1px solid gray; padding: 2px;"> <p>< NEW ></p> <p>172.29.65.9</p> </div> <p style="text-align: center; margin-top: 5px;">Delete</p>	<p>Server: <input style="width: 80%;" type="text"/> (Hostname or IP Address)</p> <p>Shared Secret: <input style="width: 80%;" type="text"/></p> <p>Authentication Port (optional): <input style="width: 50%;" type="text"/> (0-65536)</p> <p>Accounting Port (optional): <input style="width: 50%;" type="text"/> (0-65536)</p>	
---	---	--

4. Configure Default Server Priorities.
For **Priority 1** under **EAP Authentication**, select the corporate server created in step 2.
5. Click the **Apply** button.

Default Server Priorities

<p>EAP Authentication</p> <p>Priority 1: <input style="width: 80%;" type="text" value="172.29.65.9"/> ▾</p> <p>Priority 2: <input style="width: 80%;" type="text" value="< NONE >"/> ▾</p> <p>Priority 3: <input style="width: 80%;" type="text" value="< NONE >"/> ▾</p>	<p>MAC Authentication</p> <p>Priority 1: <input style="width: 80%;" type="text" value="< NONE >"/> ▾</p> <p>Priority 2: <input style="width: 80%;" type="text" value="< NONE >"/> ▾</p> <p>Priority 3: <input style="width: 80%;" type="text" value="< NONE >"/> ▾</p>	<p>Accounting</p> <p>Priority 1: <input style="width: 80%;" type="text" value="< NONE >"/> ▾</p> <p>Priority 2: <input style="width: 80%;" type="text" value="< NONE >"/> ▾</p> <p>Priority 3: <input style="width: 80%;" type="text" value="< NONE >"/> ▾</p>
<p>Admin Authentication (RADIUS)</p> <p>Priority 1: <input style="width: 80%;" type="text" value="< NONE >"/> ▾</p> <p>Priority 2: <input style="width: 80%;" type="text" value="< NONE >"/> ▾</p> <p>Priority 3: <input style="width: 80%;" type="text" value="< NONE >"/> ▾</p>	<p>Admin Authentication (TACACS+)</p> <p>Priority 1: <input style="width: 80%;" type="text" value="< NONE >"/> ▾</p> <p>Priority 2: <input style="width: 80%;" type="text" value="< NONE >"/> ▾</p> <p>Priority 3: <input style="width: 80%;" type="text" value="< NONE >"/> ▾</p>	

Wireless services (WPA2-Enterprise and Cisco FSR only)

Configure WDS Host

1. In the navigation pane, click **WIRELESS SERVICES** and select **WDS**.
2. Configure options in **GENERAL SET-UP** tab:
 - a. Select **Use this AP as Wireless Domain Services**
 - b. Enter **255** in the **Wireless Domain Services Priority** field.

The screenshot shows the configuration page for WDS (Wireless Domain Services) in the GENERAL SET-UP tab. The page is divided into three main sections: WDS STATUS, GENERAL SET-UP, and SERVER GROUPS. The GENERAL SET-UP section is active and contains the following configuration options:

- WDS - Wireless Domain Services - Global Properties**
 - Use this AP as Wireless Domain Services
 - Wireless Domain Services Priority: (1-255)
 - Use Local MAC List for Client Authentication
- WNM - Wireless Network Manager - Global Configuration**
 - Configure Wireless Network Manager
 - Wireless Network Manager Address: (IP Address or Hostname)

3. Configure **Infrastructure Authentication** in **SERVER GROUPS** tab:
 - a. Enter name for infrastructure authentication server group
 - b. Select the RADIUS server configured in **Server Manager** from the drop down list by **Priority 1**.
 - c. Under **Use Group For**: select the **Infrastructure Authentication** option.
 - d. Under **SSID Settings**, select the **Apply to all SSIDs** option.
4. Click the **Apply** button.

Wireless Services: WDS - Server Groups

Server Group List

< NEW >

cckm

cckm_client

Server Group Name:

Group Server Priorities: [Define Servers](#)

Priority 1:

Priority 2:

Priority 3:

Use Group For:

Infrastructure Authentication

Client Authentication

Authentication Settings

EAP Authentication

LEAP Authentication

MAC Authentication

Default (Any) Authentication

SSID Settings

Apply to all SSIDs

Restrict SSIDs (Apply only to listed SSIDs)

SSID:

5. Configure **Client Authentication** in **SERVER GROUPS** tab
 - a. In the **Server Group Name** field, enter a name for the client authentication server group.
 - b. Select RADIUS server configured in **Server Manager** from the drop down list by **Priority 1**.
 - c. Select the **Client Authentication** option.
 - d. Select the **EAP Authentication** check box for WPA2-Enterprise security.
 - e. Select the **LEAP Authentication** check box for Cisco FSR security.
 - f. Under **SSID Settings**, select the **Apply to all SSIDs** option.
6. Click the **Apply** button.

Wireless Services: WDS - Server Groups

Server Group List

< NEW >
 cckm
 cckm_client

Delete

Server Group Name: cckm_client

Group Server Priorities: [Define Servers](#)

Priority 1: 172.29.65.9

Priority 2: < NONE >

Priority 3: < NONE >

Use Group For:

Infrastructure Authentication

Client Authentication

Authentication Settings

EAP Authentication

LEAP Authentication

MAC Authentication

Default (Any) Authentication

SSID Settings

Apply to all SSIDs

Restrict SSIDs (Apply only to listed SSIDs)

SSID: DISABLED Add

Remove

Configure WDS Client

1. In the navigation pane, click **WIRELESS SERVICES** and select **AP**.
2. Specify the WDS host explicitly in the **Specified Discovery** field or allow **Auto Discovery** to find the host automatically.
3. Enable **Participate in SWAN Infrastructure**.
4. Enter the **Username** and **Password** configured on the RADIUS server.
5. Click the **Apply** button.

Wireless Services: AP

Participate in SWAN Infrastructure: Enable Disable

WDS Discovery: Auto Discovery
 Specified Discovery: (IP Address)

Username:

Password:

Confirm Password:

Authentication Methods Profile: [Define Authentication Methods Profiles](#)

Radio Settings

Network interfaces – radio 802.11g

1. In the navigation pane, click **NETWORK INTERFACES** and select **Radio0-802.11G** from the sub-menu.
2. Click the **SETTINGS** tab and set **Enable Radio** to **Enable**.
3. 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 **Required** data rate setting in the access point.

802.11 Radio Standard	Minimum Available Signal Strength (RSSI)	Maximum "Required" 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



For additional details on RF deployment please see the *Deploying Enterprise-Grade Wi-Fi Telephony* white paper and the *Best Practices Guide for Deploying SpectraLink 8020/8030 Wireless Telephones*.

Cisco Aironet 1130AG Series Access Point

Hostname **ap** ap uptime is 8 minutes

Network Interfaces: Radio0-802.11G Settings

Enable Radio: Enable Disable

Current Status (Software/Hardware): Enabled ↑ Up ↑

Role in Radio Network:

- Access Point
- Access Point (Fallback to Radio Shutdown)
- Access Point (Fallback to Repeater)
- Repeater
- Workgroup Bridge
- Scanner

Data Rates:

	Best Range	Best Throughput	Default
1.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
2.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
5.5Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
* 6.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
* 9.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
11.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
* 12.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
* 18.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
* 24.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
* 36.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
* 48.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
* 54.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable

* OFDM Rates

4. Power level selection should be determined from your facility's RF site survey. The **Limit Client Power** option is not supported by the SpectraLink Wireless Telephones. The handset power should be configured to match the highest transmit power of the APs.
5. **Channel** selection should be determined from your facility's RF site survey using only channels **1, 6, and 11**.
6. Set **Radio Preamble** to **Long**, unless the environment is an 802.11g only environment.

CCK Transmitter Power (dBm):	<input checked="" type="radio"/> -1 <input type="radio"/> 2 <input type="radio"/> 5 <input type="radio"/> 8 <input type="radio"/> 11 <input type="radio"/> 14 <input type="radio"/> 17 <input type="radio"/> 20 <input type="radio"/> Max	
OFDM Transmitter Power (dBm):	<input checked="" type="radio"/> -1 <input type="radio"/> 2 <input type="radio"/> 5 <input type="radio"/> 8 <input type="radio"/> 11 <input type="radio"/> 14 <input type="radio"/> 17 <input type="radio"/> Max	Power Translation Table (mW/dBm)
Client Power Local:	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Limit Client Power (dBm):	<input checked="" type="radio"/> 2 <input type="radio"/> 5 <input type="radio"/> 8 <input type="radio"/> 11 <input type="radio"/> 14 <input type="radio"/> 17 <input type="radio"/> 20 <input type="radio"/> Max	
Default Radio Channel:	Channel 1 - 2412 MHz	Channel 1 2412 MHz
Least Congested Channel Search: (Use Only Selected Channels)	<input type="radio"/> Channel 1 - 2412 MHz <input type="radio"/> Channel 2 - 2417 MHz <input type="radio"/> Channel 3 - 2422 MHz <input type="radio"/> Channel 4 - 2427 MHz <input type="radio"/> Channel 5 - 2432 MHz <input type="radio"/> Channel 6 - 2437 MHz <input type="radio"/> Channel 7 - 2442 MHz <input type="radio"/> Channel 8 - 2447 MHz <input type="radio"/> Channel 9 - 2452 MHz <input type="radio"/> Channel 10 - 2457 MHz <input type="radio"/> Channel 11 - 2462 MHz	
World Mode Multi-Domain Operation:	<input checked="" type="radio"/> Disable	<input type="radio"/> Legacy <input type="radio"/> Dot11d
Country Code:	<input type="text" value=""/>	<input type="checkbox"/> Indoor <input type="checkbox"/> Outdoor
Radio Preamble	<input type="radio"/> Short	<input checked="" type="radio"/> Long
Receive Antenna:	<input checked="" type="radio"/> Diversity	<input type="radio"/> Left (Secondary) <input type="radio"/> Right (Primary)
Transmit Antenna:	<input checked="" type="radio"/> Diversity	<input type="radio"/> Left (Secondary) <input type="radio"/> Right (Primary)
External Antenna Configuration:	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
	Antenna Gain(dB): <input type="text" value="DISABLED"/> (-128 - 128)	
Traffic Stream Metrics:	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Aironet Extensions:	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable

7. Set the **Data Beacon Rate (DTIM)** to **2**.
8. Set **Max. Data Retries** to **12** and **RTS Max. Retries** to **24**.
9. Click the **Apply** button.

Ethernet Encapsulation Transform:	<input checked="" type="radio"/> RFC1042	<input type="radio"/> 802.1H
Reliable Multicast to WGB:	<input checked="" type="radio"/> Disable	<input type="radio"/> Enable
Public Secure Packet Forwarding:	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Short Slot Time:	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Beacon Privacy Guest Mode:	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Beacon Period:	<input type="text" value="100"/> (20-4000 Kusec)	Data Beacon Rate (DTIM): <input type="text" value="2"/> (1-100)
Max. Data Retries:	<input type="text" value="12"/> (1-128)	RTS Max. Retries: <input type="text" value="24"/> (1-128)
Fragmentation Threshold:	<input type="text" value="2346"/> (256-2346)	RTS Threshold: <input type="text" value="2347"/> (0-2347)
Root Parent Timeout:	<input type="text" value="0"/> (0-65535 sec)	
Root Parent MAC 1 (optional):	<input type="text" value=""/>	
Root Parent MAC 2 (optional):	<input type="text" value=""/>	
Root Parent MAC 3 (optional):	<input type="text" value=""/>	
Root Parent MAC 4 (optional):	<input type="text" value=""/>	

Network interfaces – radio 802.11a

1. In the navigation pane, click **NETWORK INTERFACES**.
2. Select **Radio0-802.11A** from the sub-menu.
3. Click the **SETTINGS** tab.
4. Set **Enable Radio** to **Enable**.
5. 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 **Required** data rate setting in the access point.

802.11 Radio Standard	Minimum Available Signal Strength (RSSI)	Maximum "Required" 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



For additional details on RF deployment please see the *Deploying Enterprise-Grade Wi-Fi Telephony* white paper and the *Best Practices Guide for Deploying SpectraLink 8020/8030 Wireless Telephones*.

The screenshot shows the configuration page for Radio1-802.11A on a Cisco Aironet 1130AG Series Access Point. The page is titled "Network Interfaces: Radio1-802.11A Settings".

Enable Radio: Enable Disable

Current Status (Software/Hardware): Enabled Up

Role in Radio Network:

- Access Point
- Access Point (Fallback to Radio Shutdown)
- Access Point (Fallback to Repeater)
- Repeater
- Workgroup Bridge
- Scanner

Data Rates:

	Best Range	Best Throughput	Default
6.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
9.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
12.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
18.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
24.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
36.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
48.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
54.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable

6. Power level selection should be determined from your facility's RF site survey. The **Limit Client Power** option is not supported by the SpectraLink Wireless Telephones. The handset power should be configured to match the highest transmit power of the APs.
7. **Channel** selection should be determined from your facility's RF site survey.

Transmitter Power (dBm):	<input checked="" type="radio"/> -1 <input type="radio"/> 2 <input type="radio"/> 5 <input type="radio"/> 8 <input type="radio"/> 11 <input type="radio"/> 14 <input type="radio"/> 15 <input type="radio"/> Max	Power Translation Table (mW/dBm)
Client Power Local:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Limit Client Power (dBm):	<input checked="" type="radio"/> 2 <input type="radio"/> 5 <input type="radio"/> 8 <input type="radio"/> 11 <input type="radio"/> 14 <input type="radio"/> 15 <input type="radio"/> Max	
Default Radio Channel:	Channel 36 - 5180 MHz	Channel 36 5180 MHz
Least Congested Channel Search: (Use Only Selected Channels)	<input type="text" value="Channel 36 - 5180 MHz"/> <input type="text" value="Channel 40 - 5200 MHz"/> <input type="text" value="Channel 44 - 5220 MHz"/> <input type="text" value="Channel 48 - 5240 MHz"/> <input type="text" value="Channel 52 - 5260 MHz"/> <input type="text" value="Channel 56 - 5280 MHz"/> <input type="text" value="Channel 60 - 5300 MHz"/> <input type="text" value="Channel 64 - 5320 MHz"/> <input type="text" value="Channel 149 - 5745 MHz"/> <input type="text" value="Channel 153 - 5765 MHz"/> <input type="text" value="Channel 157 - 5785 MHz"/> <input type="text" value="Channel 161 - 5805 MHz"/>	
World Mode Multi-Domain Operation:	<input checked="" type="radio"/> Disable <input type="radio"/> Legacy <input type="radio"/> Dot11d	
Country Code:	<input type="text" value=""/> <input type="checkbox"/> Indoor <input type="checkbox"/> Outdoor	
Receive Antenna:	<input checked="" type="radio"/> Diversity <input type="radio"/> Left (Secondary) <input type="radio"/> Right (Primary)	
Transmit Antenna:	<input checked="" type="radio"/> Diversity <input type="radio"/> Left (Secondary) <input type="radio"/> Right (Primary)	
External Antenna Configuration:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
	Antenna Gain(dB): <input type="text" value="DISABLED"/> (-128 - 128)	
Gratuitous Probe Response(GPR):	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
	Period(Kusec): <input type="text" value="DISABLED"/> (10-255)	
	Transmission Speed: <input type="text" value="none"/>	
Traffic Stream Metrics:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Aironet Extensions:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	

8. Set the **Data Beacon Rate (DTIM)** to **2**.
9. Set **Max. Data Retries** to **12** and **RTS Max. Retries** to **24**.
10. Click the **Apply** button.

Ethernet Encapsulation Transform:	<input checked="" type="radio"/> RFC1042	<input type="radio"/> 802.1H	
Reliable Multicast to WGB:	<input checked="" type="radio"/> Disable	<input type="radio"/> Enable	
Public Secure Packet Forwarding:	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	
Beacon Privacy Guest Mode:	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	
Beacon Period:	<input type="text" value="100"/> (20-4000 Kusec)	Data Beacon Rate (DTIM):	<input type="text" value="2"/> (1-100)
Max. Data Retries:	<input type="text" value="12"/> (1-128)	RTS Max. Retries:	<input type="text" value="24"/> (1-128)
Fragmentation Threshold:	<input type="text" value="2346"/> (256-2346)	RTS Threshold:	<input type="text" value="2347"/> (0-2347)
Root Parent Timeout:	<input type="text" value="0"/> (0-65535 sec)		
Root Parent MAC 1 (optional):	<input type="text" value=""/>		
Root Parent MAC 2 (optional):	<input type="text" value=""/>		
Root Parent MAC 3 (optional):	<input type="text" value=""/>		
Root Parent MAC 4 (optional):	<input type="text" value=""/>		