Spectralink VIEW Certified Configuration Guide

Cisco Systems Inc.

104x, 114x, 126x, 160x, 260x, 350x, and 360x Autonomous APs

1725-86193-000 Rev: E
September 2013

Copyright Notice

Notice

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

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

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

Contact Information

US Location
800-775-5330

Spectralink Corporation
2560 55th Street
Boulder, CO 80301

info@spectralink.com

Denmark Location
+45 7560 2850

Spectralink Europe ApS
Langmarksvej 34
8700 Horsens

infodk@spectralink.com

Contents

Introduction

Spectralink's Voice Interoperability for Enterprise Wireless (VIEW) Certification Program is designed to ensure interoperability and high performance between Spectralink 84-Series and 80-Series handsets and WLAN infrastructure products.

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

Certified Product Summary

Manufacturer:	Cisco Systems Inc. www.cisco.com
Approved models:	104x, 114x, 126x, 160x, 260x, 350x, and 360x
AP Radio(s):	2.4 GHz (802.11b/g/n), 5 GHz (802.11a/n)
Security :	WPA-PSK, WPA2-PSK, WPA2-Enterprise** (EAP-FAST and PEAPv0/MSCHAPv2), Cisco FSR (LEAP)
QoS:	Wi-Fi Standard**, CCX**
AP firmware version(s) tested:	15.2.4-JA1
Network topology:	Switched Ethernet (recommended)

Handset models tested:*	*Spectralink 8440/8441/8450/8452/8453 Handsets*			
Handset radio mode:	802.11b	802.11b/g	802.11bgn	802.11a & 802.11an
Meets VIEW minimum call capacity per AP:	8 calls	8 calls	8 calls	10 calls

Handset models tested:	*Spectralink 8020/8030 Handsets*	
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 (Wi-Fi Standard QoS) **

*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, 8441 (8440 with personal alarm hardware), 8450 (with 1D bar code reader), 8452 (with 1D and 2D bar code reader), and

8453 (8452 with personal alarm hardware) handsets will be referred to collectively as the 84-Series handsets.

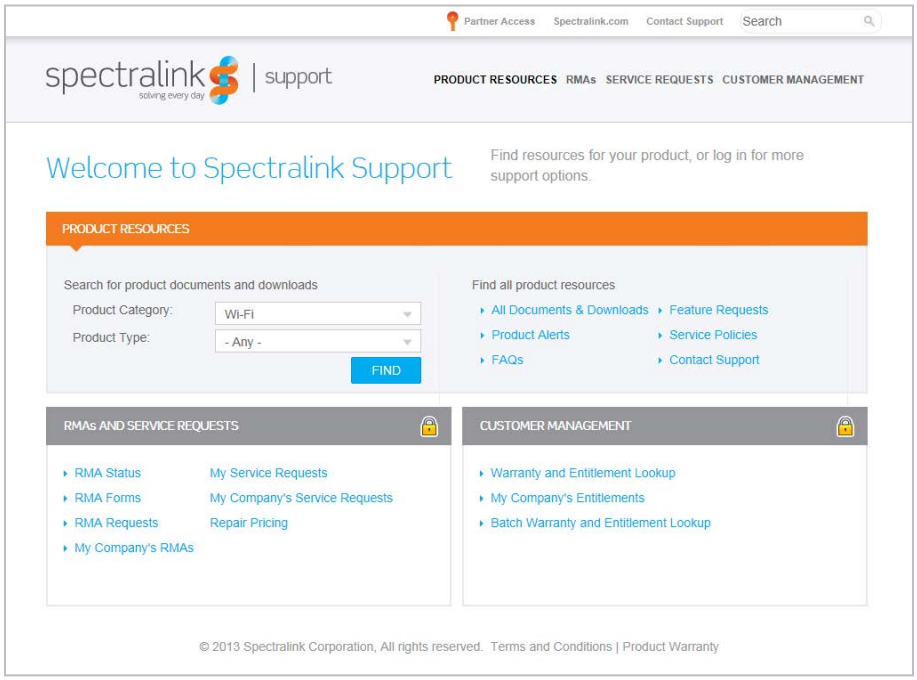
** Only Release 3.0 capable Spectralink 8020/8030 handsets support WPA2-Enterprise, Wi-Fi Standard QoS, and CCXv4 (Cisco Compatible Extensions). Release 3.0 capable handset types connect to PBX's that support IP telephony. Release 3.0 capabilities are not available for Spectralink 8020/8030 handsets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

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.
- The 350x and 126x AP's will not work in 11n mode with the 84-Series handsets. The other models certified only work in 11n mode with the 84-Series handsets if the a-msdu aggregation feature is disabled.
- The SVP mode cannot be configured in the 15.2.4-JA1 software release. This feature is scheduled for inclusion in a future autonomous software release.
- The 160x AP models do not provide the OKC fast roaming method.

Spectralink References

All Spectralink documents are available at http://support.spectralink.com.



To go to a specific product page:

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

Specific Documents

For the Spectralink 8020/8030 Wireless Telephones, please refer to *Best Practices Guide for Deploying Spectralink 8020/8030 Wireless Telephones.* This white paper covers the security, coverage, capacity and QoS considerations necessary for ensuring excellent voice quality with enterprise Wi-Fi networks.

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

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

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

The *Spectralink 84-Series Deployment Guide* is your essential reference for provisioning and deploying Spectralink 84-Series handsets in any environment.

The *Web Configuration Utility User Guide* explains how to use a web browser to configure the Spectralink 84-Series handsets on a per handset basis.

The *Spectralink 8020/8030 Wireless Telephone Handset Administration Tool* document explains how to use a software interface to configure the handsets.

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 use the instructions available at http://www.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwapnote.html

Once the APs are converted, this document can be used to provision APs.

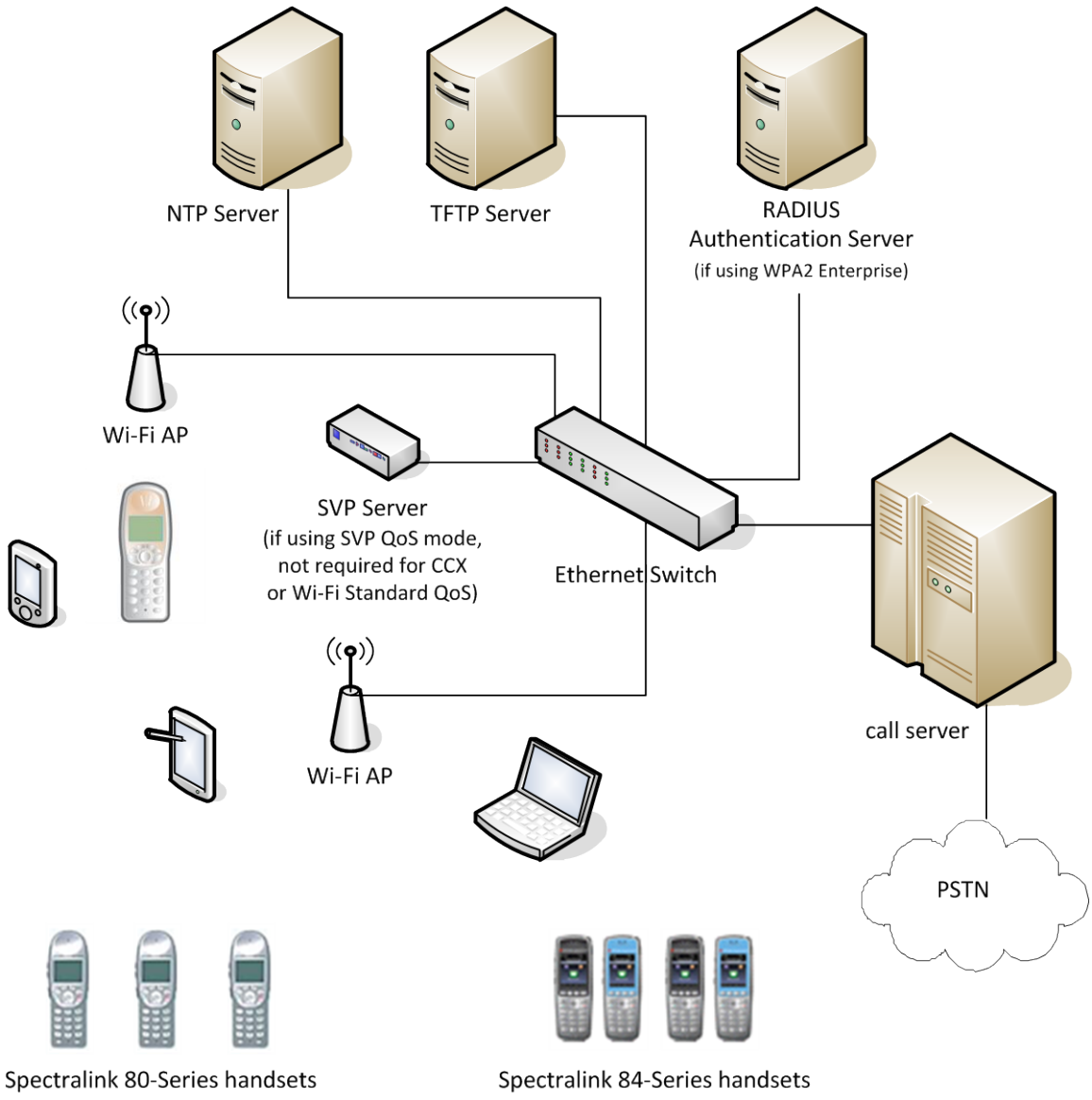
Note: RADIUS server configuration

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/lwapnote.html
- For other assistance, contact either Cisco's customer service at: www.cisco.com or Spectralink's customer service at http://support.spectralink.com.

Network Topology

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



Chapter 1: 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> Downloads**.
3. Select **Wireless> Access Points>{Series}>{Model Number}>Autonomous AP 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 Certified Product Summary.

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 console connection on the AP via a 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.

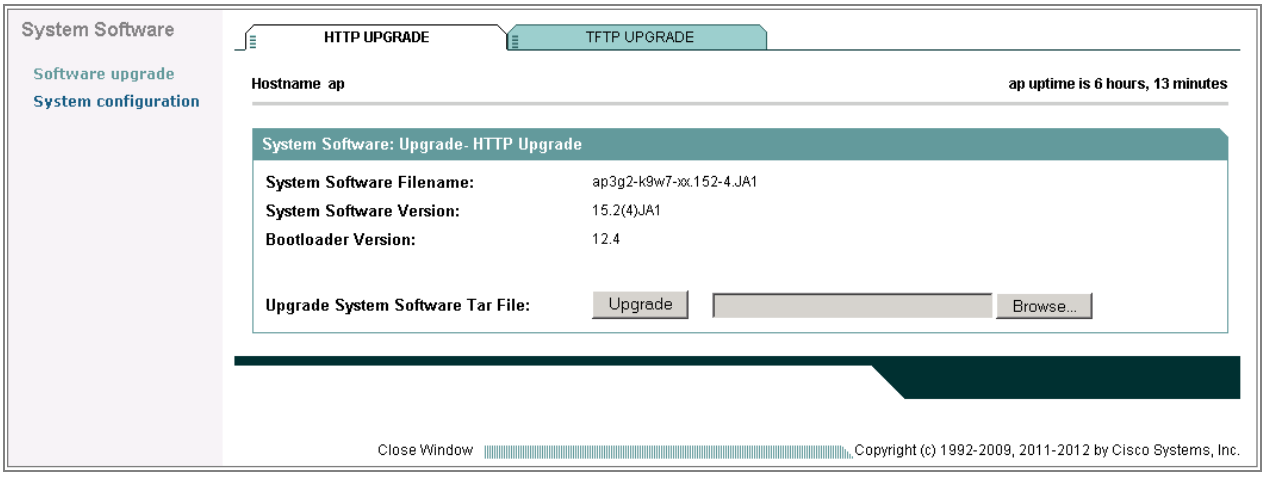
Log into the AP via a Web browser, using the IP address assigned in the above step.

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** Web site.
2. Connect to the AP via a browser, preferably Internet Explorer. Turn off pop-up blocking (See the **Tools** menu in IE).
3. In the navigation pane, click **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.
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.

Chapter 2: 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 on the desired QoS mode.

Note: No SVP

The version of the autonomous software covered by this document does not contain a working SVP configuration method.

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:

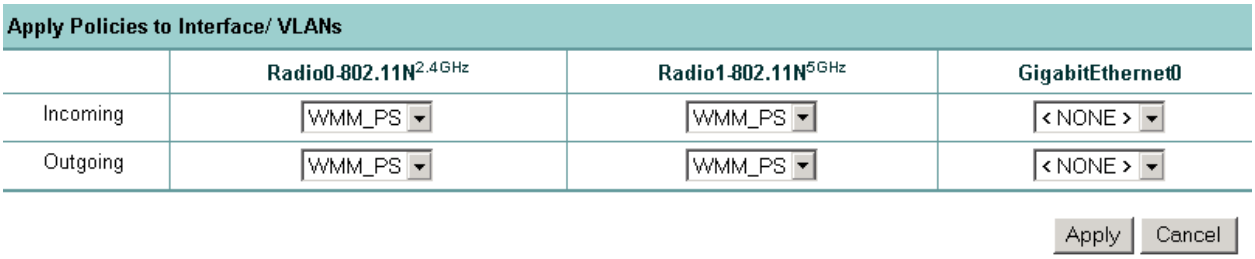
Assume that a DSCP value of 46 is used for voice packets and 40 for PBX control packets.

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.

Associate the QoS policy created in the previous step:

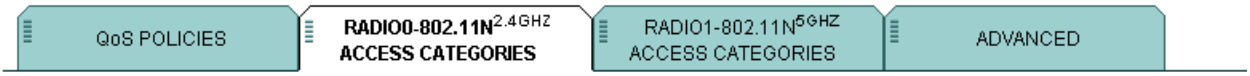
Assuming both radios are being used, perform the following steps under **Apply Policies to Interface/VLANS**:

1. Select **WMM-PS** for the following network interfaces:
   a. **Incoming** for the **GigabitEthernet0**
   b. **Incoming** and **Outgoing** for the **Radio0-802.11G**
   c. **Incoming** and **Outgoing** for the **Radio1-802.11A**
2. Click the **Apply** button to save the QoS policies.

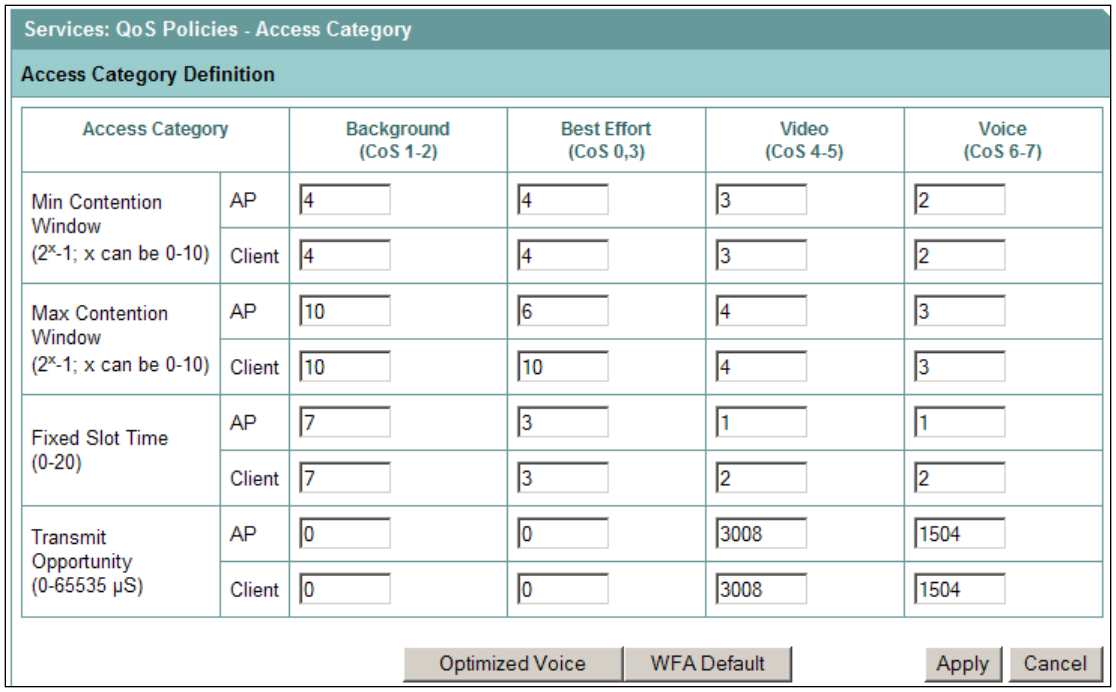


Use WFA Defaults for Access Categories

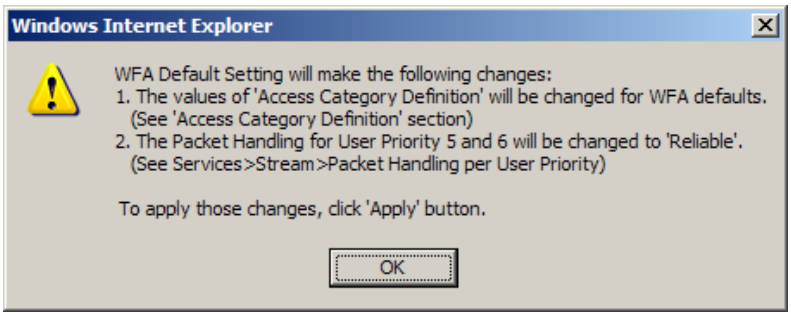
1. For each radio used by the handsets, go to the **Access Categories** tab in the **QoS Services** menu.



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



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

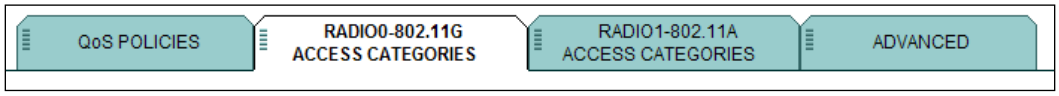


4 Click the **Apply** button in the **Services: QoS Policies – Access Category** section to save the WFA default settings.

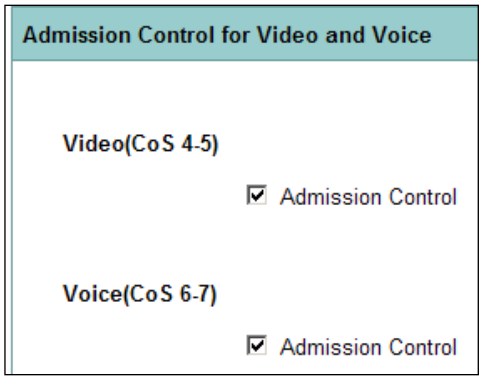
Enable Admission Control

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

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



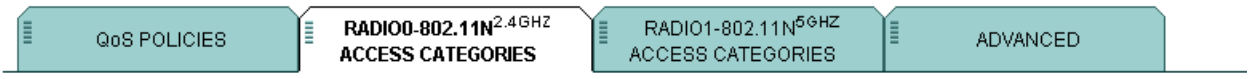
2 Enable both **Video** and **Voice** admission control.



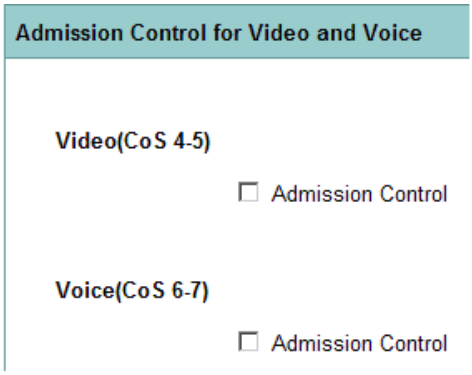
3 Click the **Apply** button to save selections.

Disable Admission Control

1 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.



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

Enable WMM

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

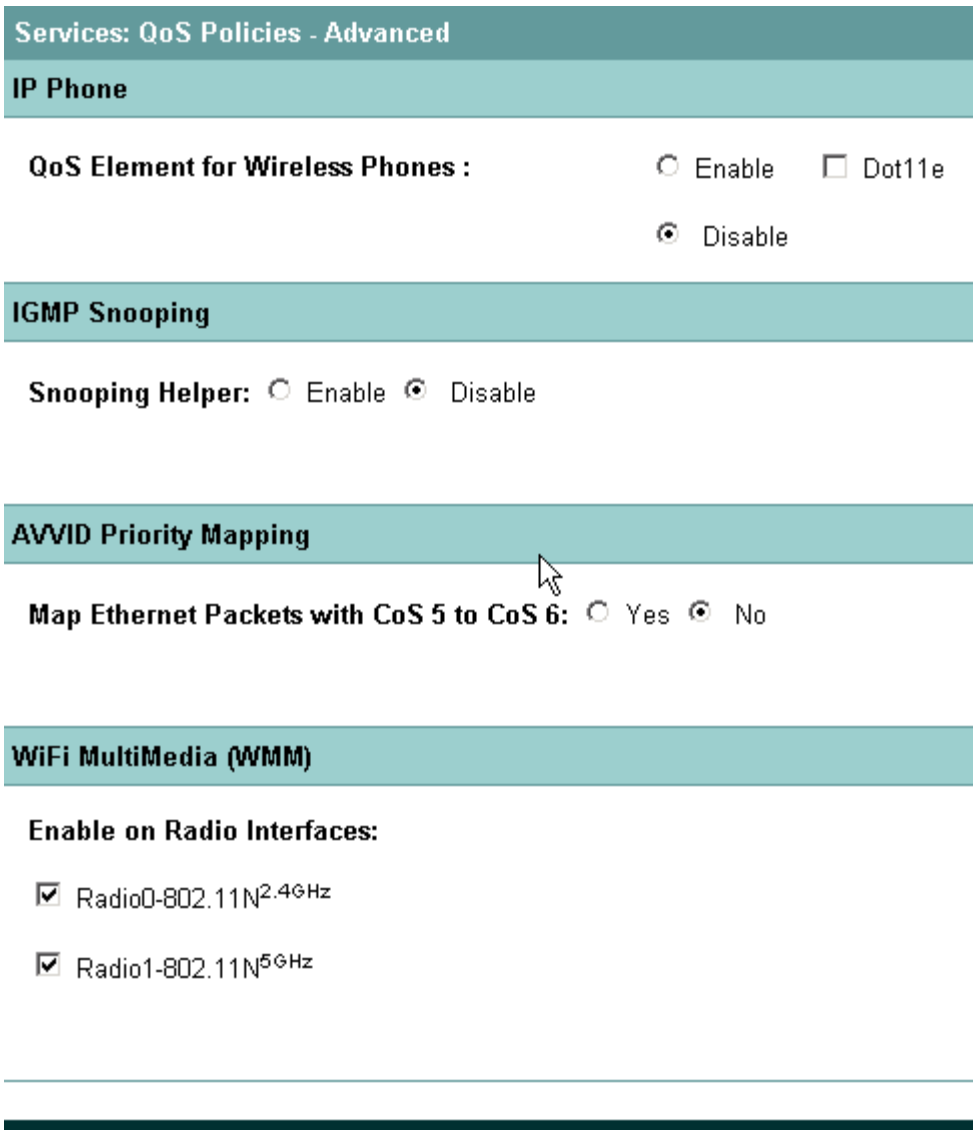
2 Enable **WMM** for all radios used by handsets.

3 Disable **QoS Element for Wireless Phones.**

4 Disable **IGMP Snooping.**

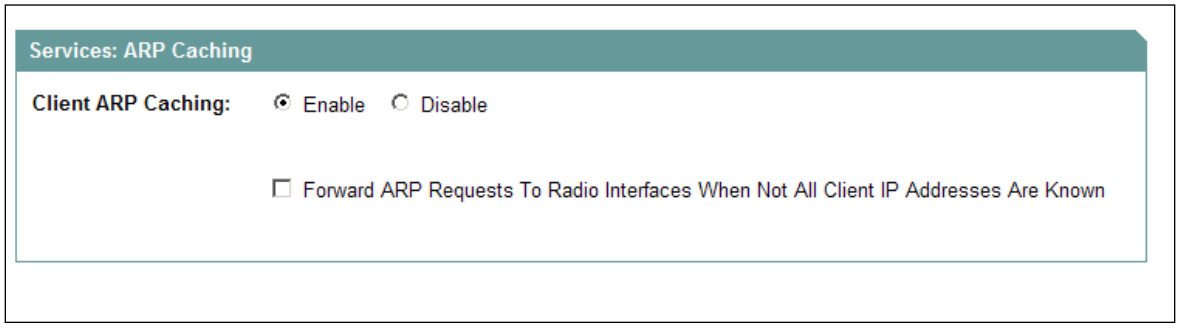
5 Select **No** for **AVVID Priority Mapping.**

6 Click **Apply** to save **ADVANCED** settings.


Services: QoS Policies - Advanced
IP Phone
QoS Element for Wireless Phones :
Enable
Dot11e
Disable
IGMP Snooping
Snooping Helper:
Enable
Disable
AVVID Priority Mapping
Map Ethernet Packets with CoS 5 to CoS 6:
Yes
No
WiFi MultiMedia (WMM)
Enable on Radio Interfaces:
Radio0-802.11N2.4GHz
Radio1-802.11N5GHz

Enable ARP Caching/Proxy ARP

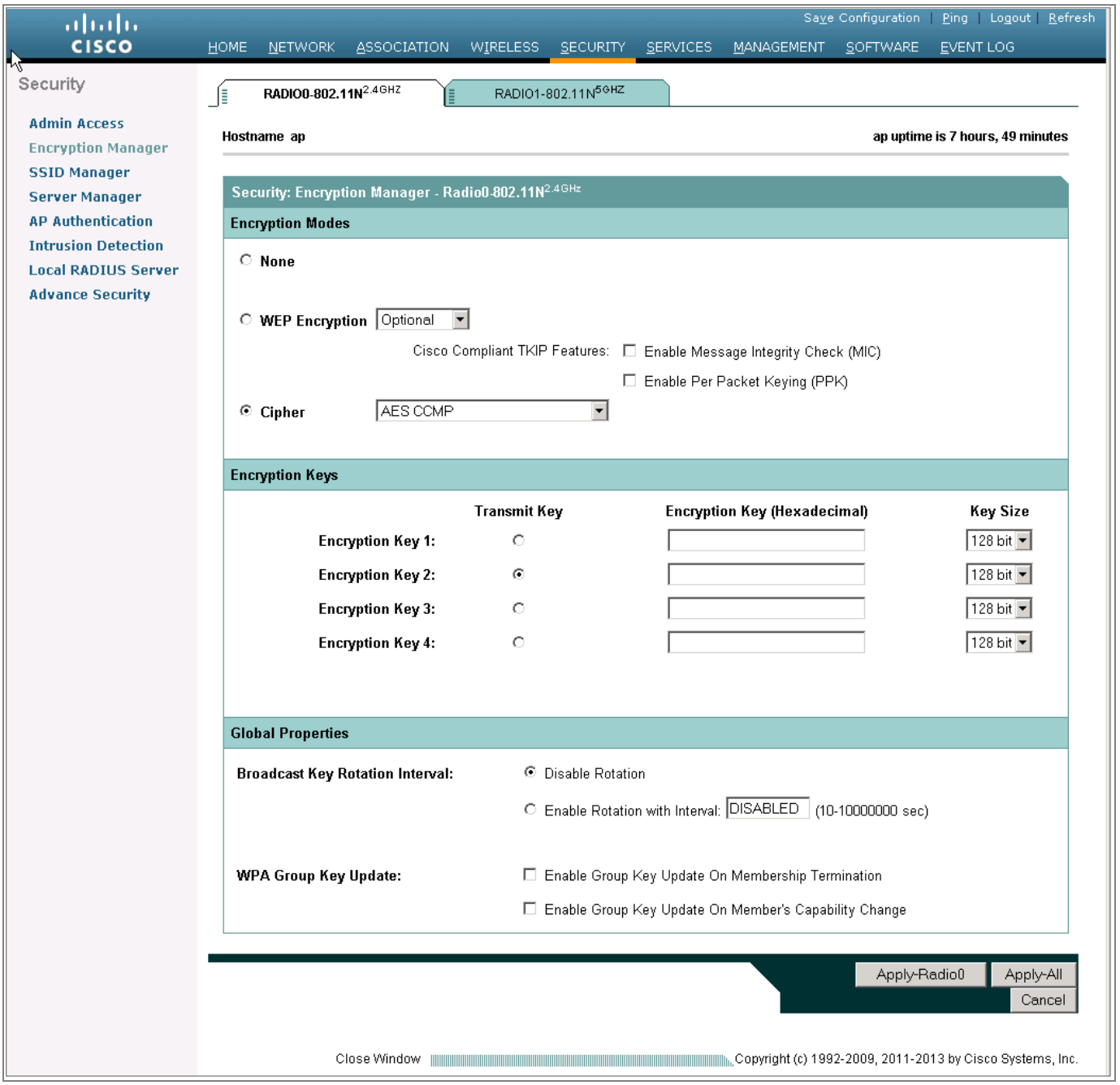
1. Under **SERVICES**, go to **ARP Caching**.
2. Enable **Client ARP Caching**.
3. Click the **Apply** button to save settings.



Chapter 3: 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.


Save Configuration | Ping | Logout | Refresh
HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG
Security
Admin Access
Encryption Manager
SSID Manager
Server Manager
AP Authentication
Intrusion Detection
Local RADIUS Server
Advance Security
RADIO0-802.11N2.4GHZ
RADIO1-802.11N5GHZ
Hostname ap
ap uptime is 7 hours, 49 minutes
Security: Encryption Manager - Radio0-802.11N2.4GHz
Encryption Modes
None
WEP Encryption Optional
Cisco Compliant TKIP Features: Enable Message Integrity Check (MIC)
Enable Per Packet Keying (PPK)
Cipher AES CCMP
Encryption Keys
Transmit Key
Encryption Key (Hexadecimal)
Key Size
Encryption Key 1: 128 bit
Encryption Key 2: 128 bit
Encryption Key 3: 128 bit
Encryption Key 4: 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
Apply-Radio0
Apply-All
Cancel
Close Window
Copyright (c) 1992-2009, 2011-2013 by Cisco Systems, Inc.

Time Server

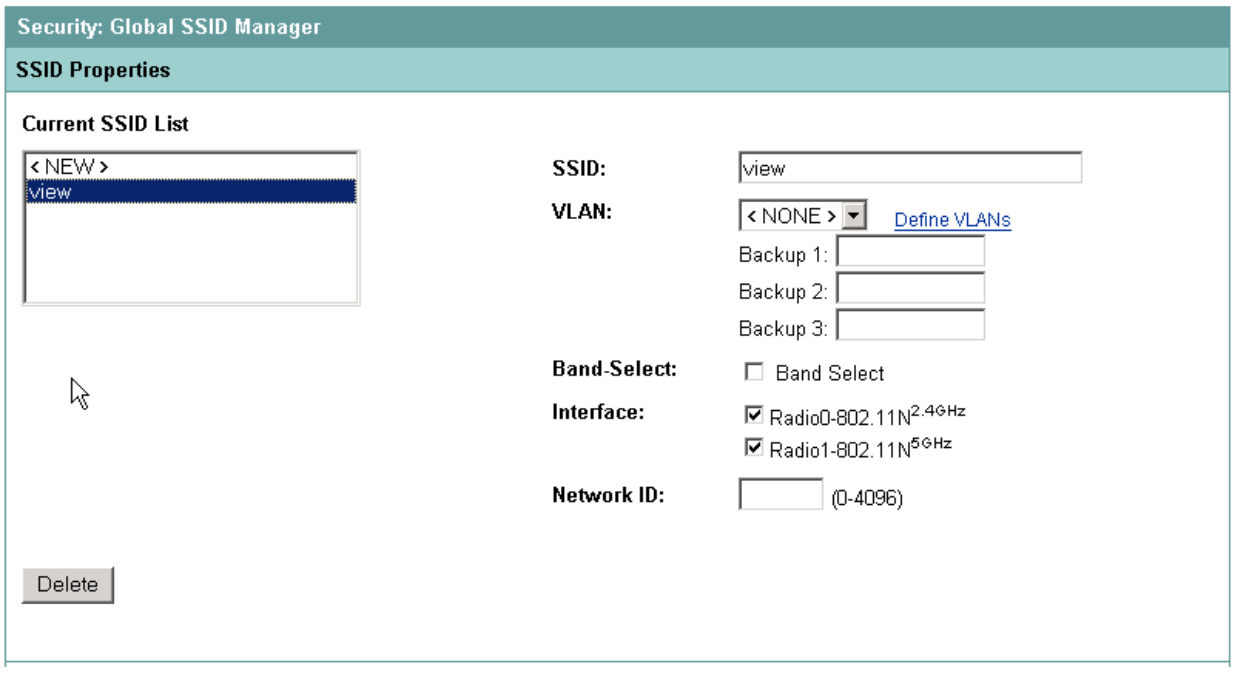
1. In the navigation pane, click **SERVICES**.
2. Select **SNTP** from the sub-menu.
3. Set the **Simple Network Time Protocol (SNTP)** to **Enable**.
4. Enter the **GMT Offset** and **Use Daylight Savings Time (United States only)** if desired.
5. Or, manually set the time if desired.

Note: Time Needed for Enterprise Security

It is important for proper certificate processing that the AP have a time setting.

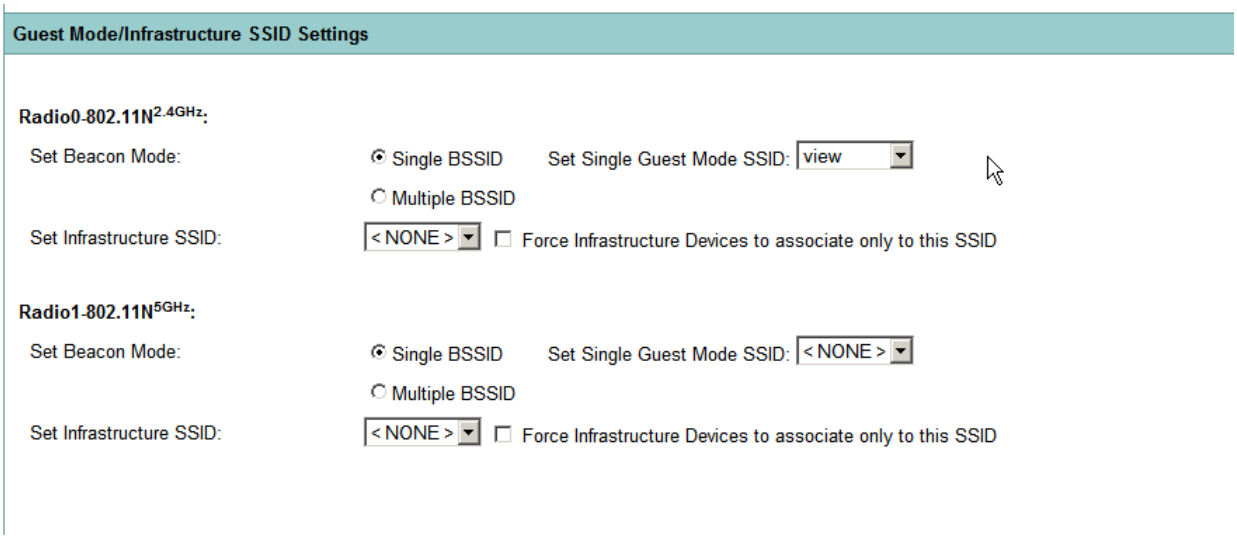
SSID Manager

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, **Radio0-802.11N$^{2.4GHz}$** or **Radio1-802.11AN^{5GHz}**.



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

5 To advertise the SSID name in the beacon, type the ssid name into the guest mode setting and click **Apply** as shown below:

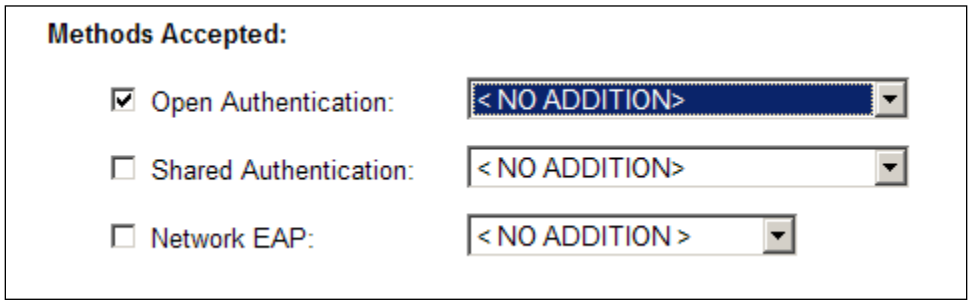


Configure Open Authentication

1 For WPA-PSK or WPA2-PSK:

a Select the **Open Authentication** check box.

b Select **<No Addition>** from the drop-down list.

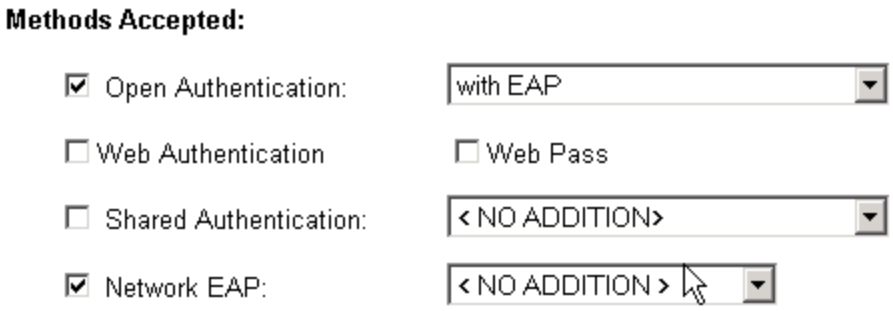


2 For WPA2-Enterprise:

a Select the **Open Authentication** check box.

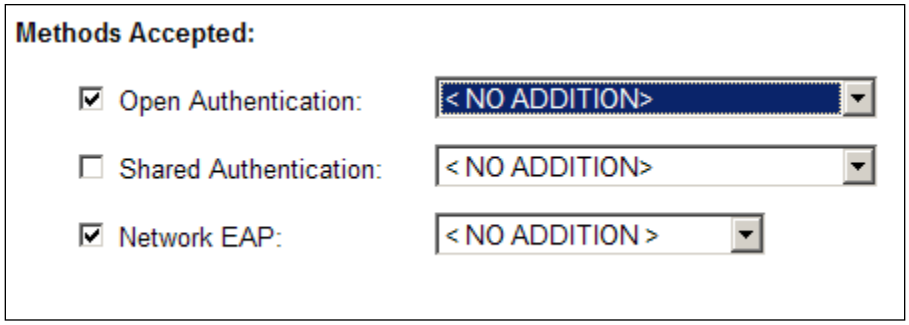
b Select **with EAP** from the drop-down list.

c Select the **Network EAP** check box.



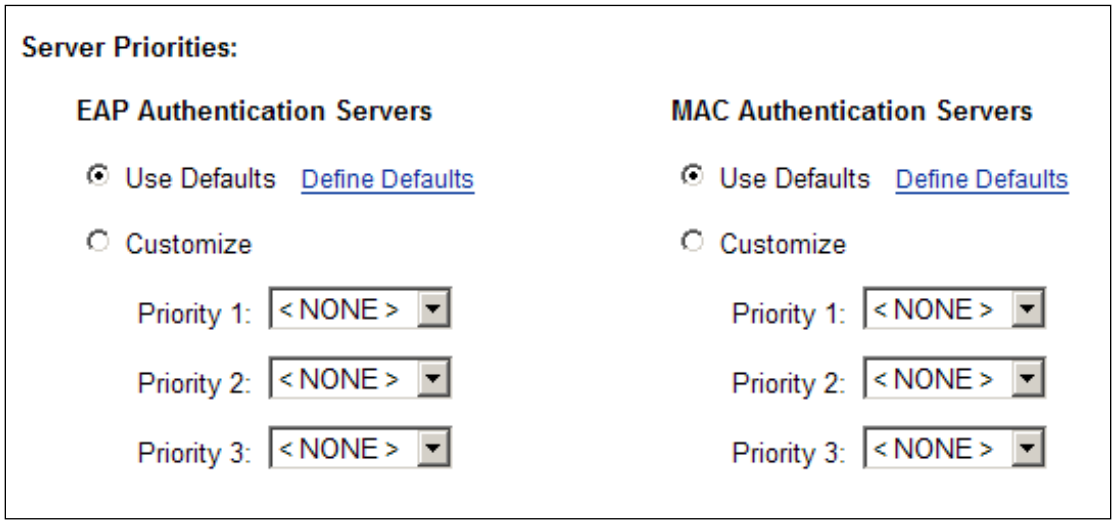
3 For Cisco FSR:

- **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.



Configure EAP Authentication Servers

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



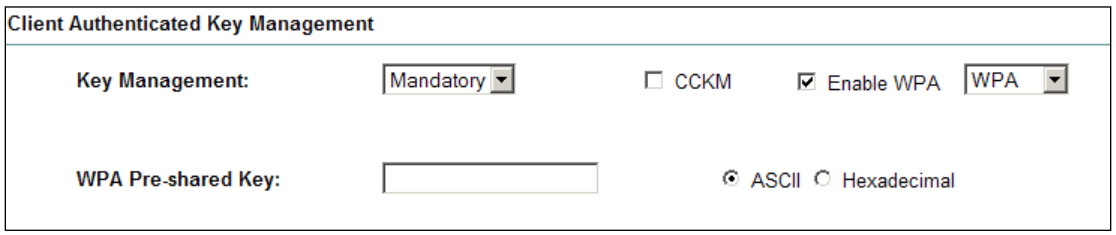
Configure Client Authenticated Key Management:

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.

Note: Check other client compatibility with CCKM

Many wireless adapters are not compatible with a network advertising CCKM.

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.



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.

6 Click the **Apply** button.

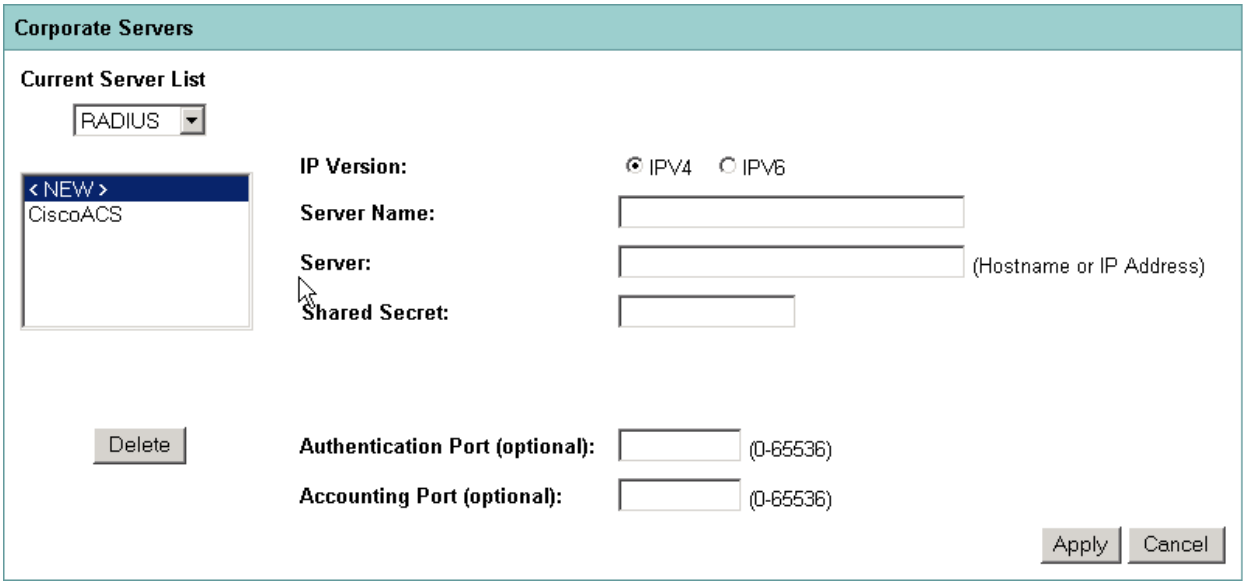
Note: Enter WDS Host in Radius Server

The WDS Host AP must be entered as an approved AP (authenticator) on the Radius server.

Server Manager

(WPA2-Enterprise and Cisco FSR (LEAP) 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.



4. Click the **Apply** button.

Wireless Services

(WPA2-Enterprise and Cisco FSR (LEAP) only)

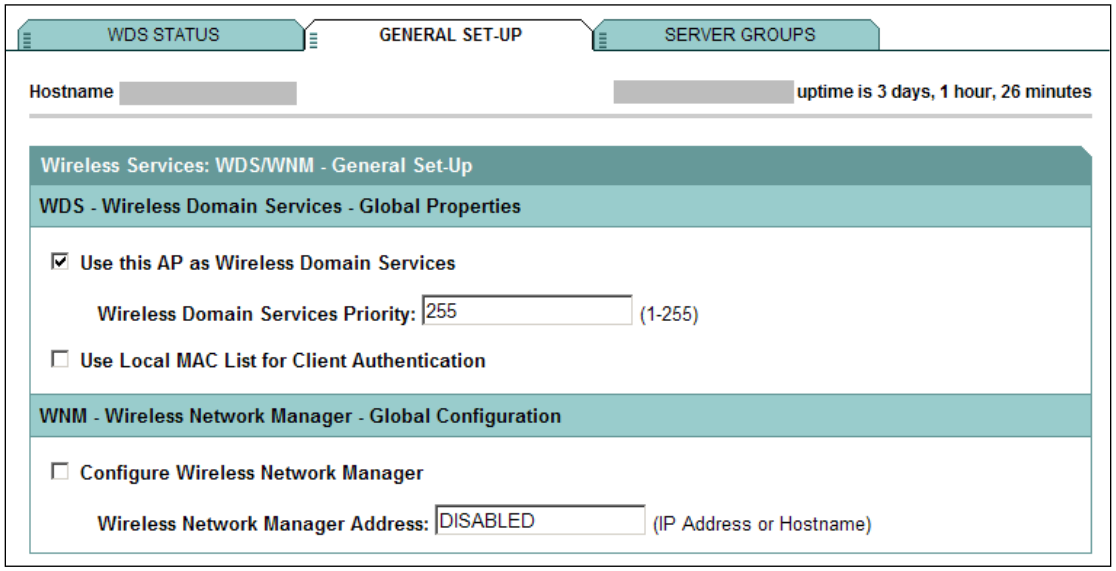
Configure WDS Host

On another AP that is designated as the WDS Host and provides no wireless service:

1. : In the navigation pane, click **WIRELESS** and select **WDS**.
2. Configure options in **GENERAL SET-UP** tab:

a Select **Use this AP as Wireless Domain Services**

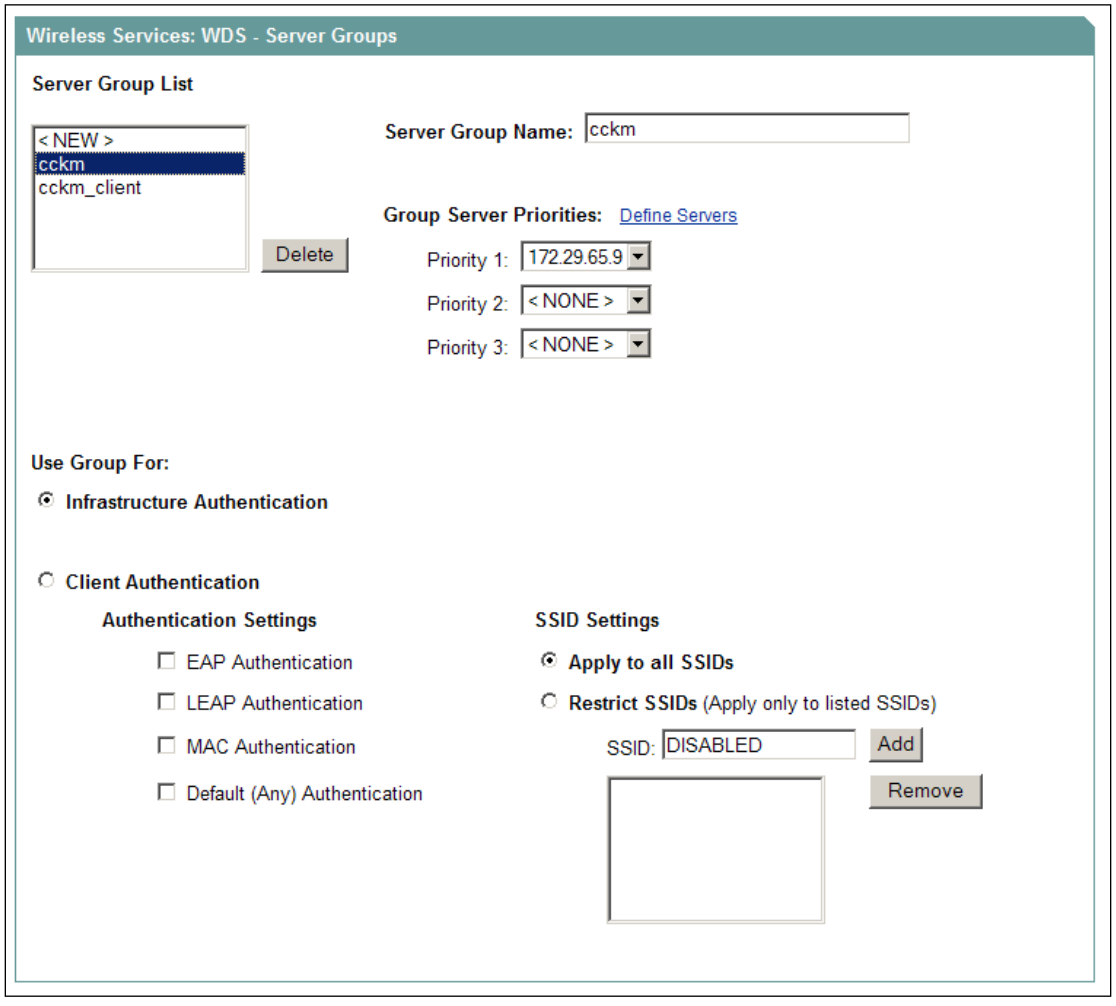
b Enter **255** in the **Wireless Domain Services Priority** field.



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.

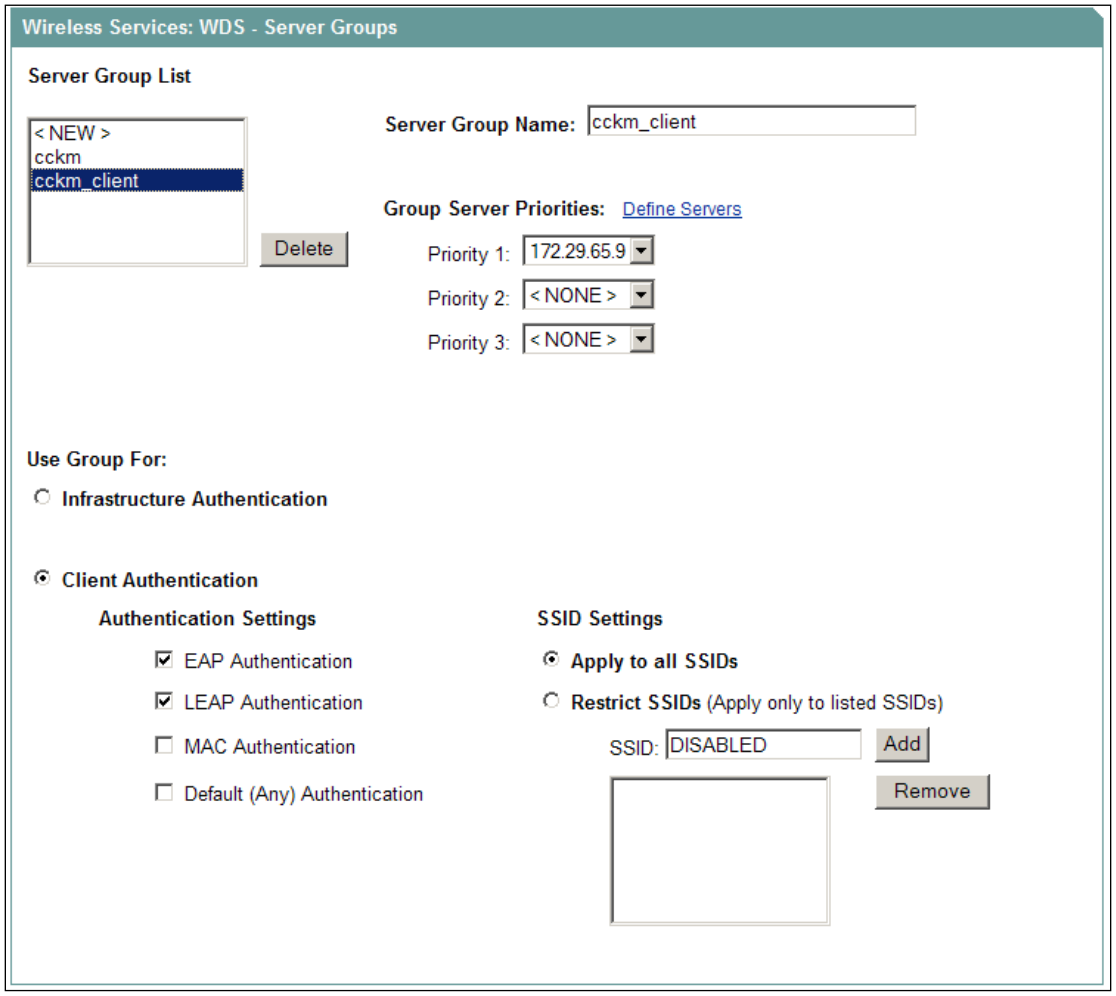
4 Click the **Apply** button.



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.

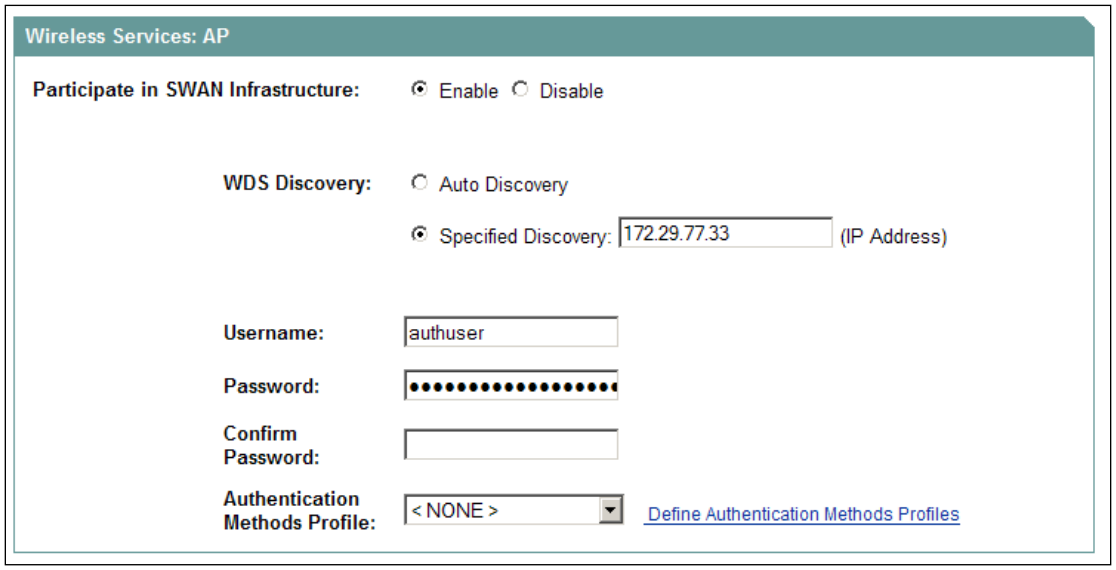
6 Click the **Apply** button.



Configure WDS Client

Back on the AP that provides wireless connections:

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



Chapter 4: Radio Settings

Network interfaces – radio 802.11n 2GHz

1. In the navigation pane, click **NETWORK** and select **NETWORK INTERFACE>Radio0-802.11n 2GHz** from the sub-menu.
2. Click the **SETTINGS** tab and set **Enable Radio** to **Enable**.
3. For the **11r Configuration**, if using CCKM fast roaming (see the ***Security*** section), select the radio button **disable**. If using CCKM fast roaming, for compatibility with the greatest number of other clients, select **enable** and **over-air** and enter a **Reassociation-time** of **200** ms as shown in the screen shot below.
4. 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	-75 dBm	1 Mb/s
	-60 dBm	11 Mb/s
802.11g	-67 dBm	6 Mb/s
	-47 dBm	54 Mb/s
802.11a	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s

Note

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*.

5. For 802.11n operation, check the Enabled radio boxes for the MCS rates. For legacy operation, uncheck all of the Enabled radio boxes for the MCS rates. The a-msdu aggregation feature of 11n must be disabled in the AP's from the cli as follows:

a Connect the PC's serial port to the console connection on the AP via a CLI cable. Open a terminal program, such as HyperTerminal. Configure the settings to 9600 baud, 8 data bits, no parity.

b At the prompt, type **enable**.

c Type in the password; default password is **Cisco**.

d Type in the command **configure terminal**.

e Type in the command **interface do11Radio0**.

f Type **no amsdu transmit priority 0**

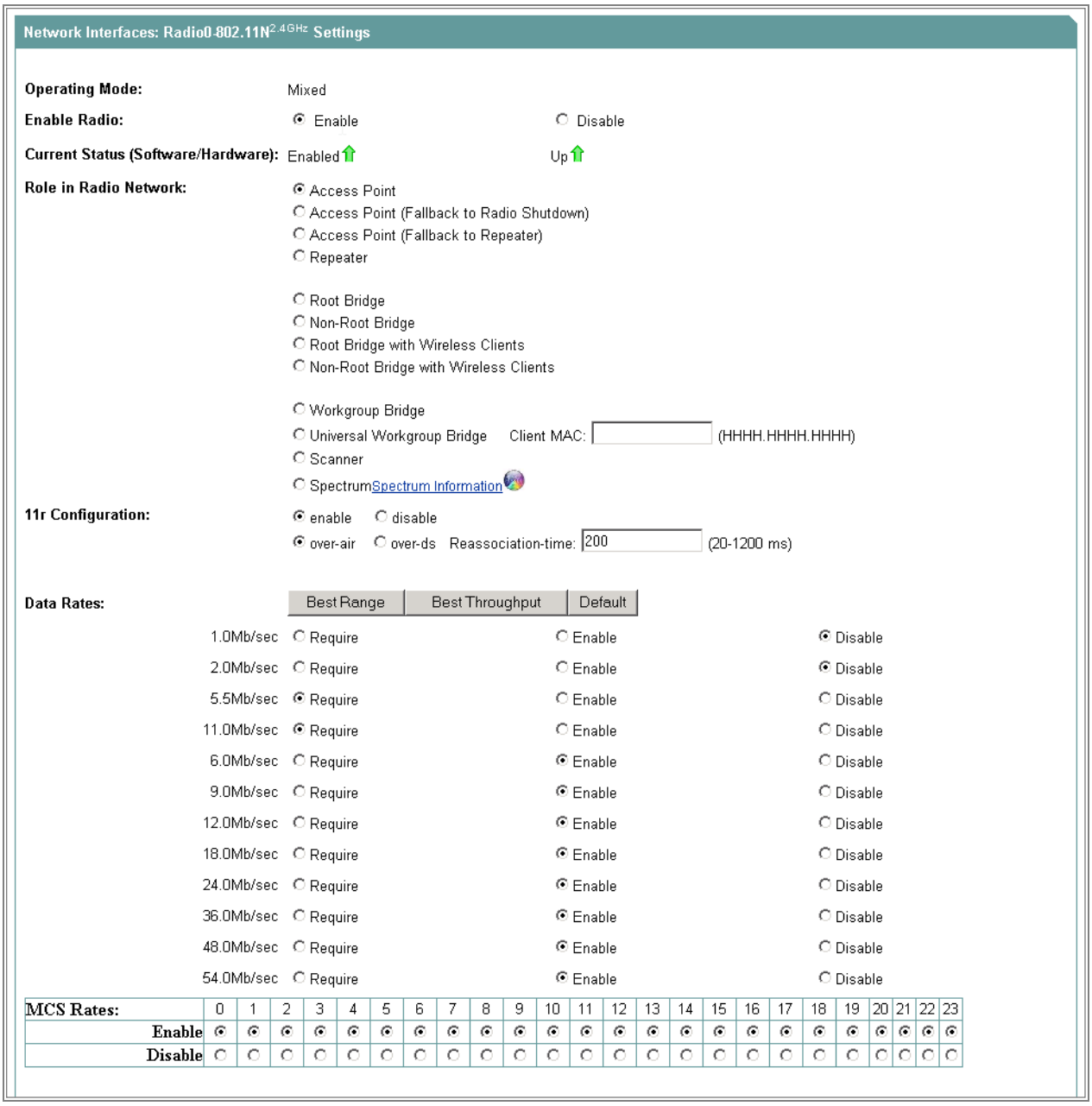
g Type **no amsdu transmit priority 1.**

h Type **no amsdu transmit priority 7.**

i Type **end** and then **write mem** to save configuration.

Note

For AP models 1260 and 3500, 802.11n operation is not compatible with the 84-Series handsets and the 15.2.4-JA1 version.



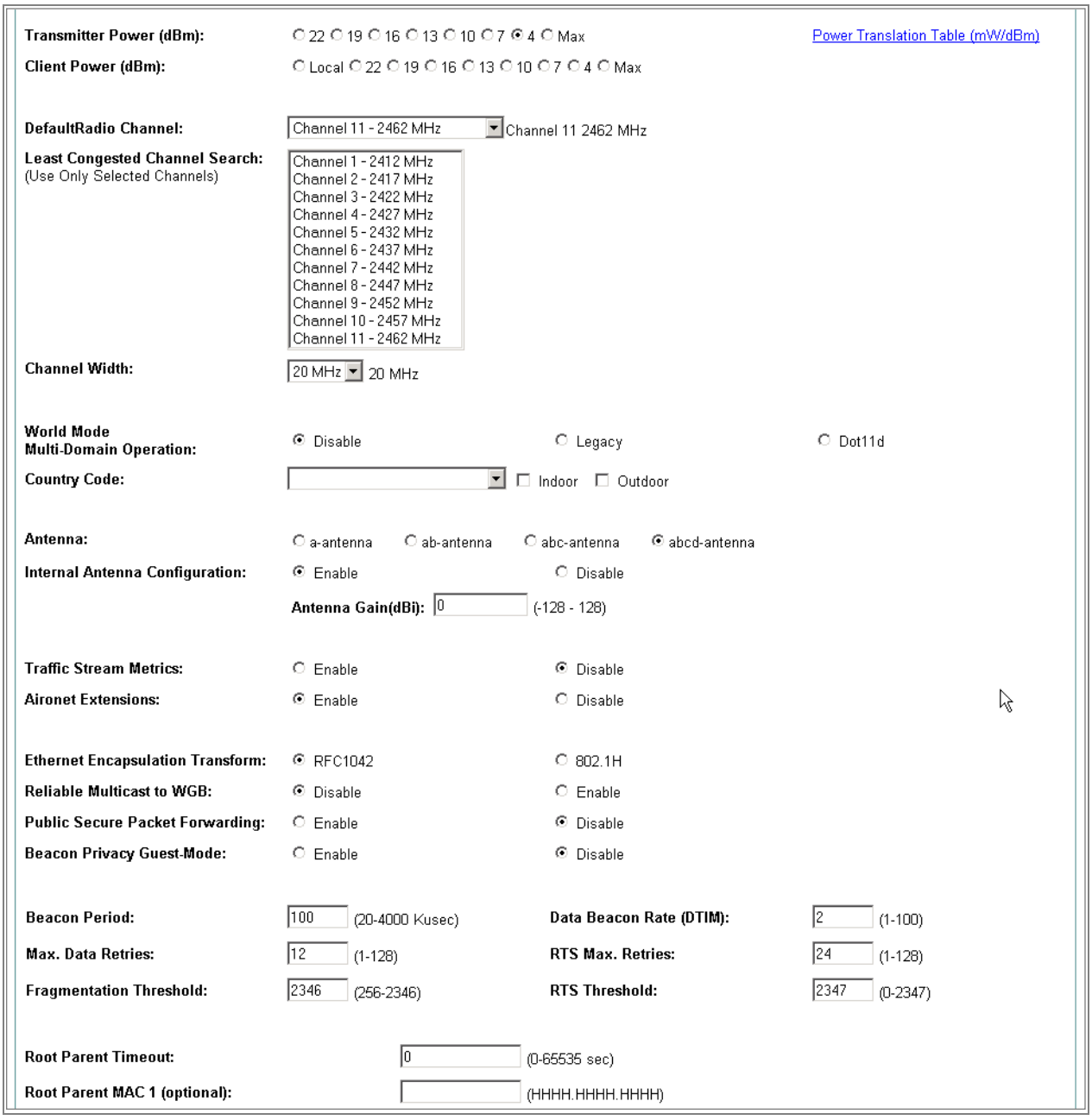
6 Power level selection should be determined from your facility's RF site survey. Setting the **Client Power** to **Local** sets the handset power level as follows:

a The 8020/8030 handsets will set the handset power level to the value advertised by the AP.

b The 84-Series handsets, if the power settings for a given radio band are set to **Auto**, will set the handset power level to the value advertised by the AP.

c The 840-Series handsets, if the power settings for a given radio band are set to something other than **Auto**, will set handset power to the level configured in the handset or the value advertised by the AP, whichever is lower.

7 **Channel** selection should be determined from your facility's RF site survey using only channels **1**, **6**, and **11** (non-overlapping channels). In countries which support channel 13, channels **1, 5, 9,** and **13** are a good choice.



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.

Network interfaces – radio 802.11a

1. In the navigation pane, click **NETWORK** and select **NETWORK INTERFACES>Radio1-802.11n-5GHz** from the sub-menu.
2. Click the **SETTINGS** tab and set **Enable Radio** to **Enable**.
3. For the **11r Configuration**, if using CCKM fast roaming (see the Security section), select the radio button **disable**. If using CCKM fast roaming, for compatibility with the greatest number of other clients, select **enable** and **over-air** and enter a **Reassociation-time** of **200** ms as shown in the screen shot below.
4. 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	-75 dBm	1 Mb/s
	-60 dBm	11 Mb/s
802.11g	-67 dBm	6 Mb/s
	-47 dBm	54 Mb/s
802.11a	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s

Note

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*.

5. For 802.11n operation, check the Enabled radio boxes for the MCS rates. For legacy operation, uncheck all of the Enabled radio boxes for the MCS rates. The a-msdu aggregation feature of 11n must be disabled in the AP's from the cli as follows:
   a. Connect the PC's serial port to the console connection on the AP via a CLI cable. Open a terminal program, such as HyperTerminal. Configure the settings to 9600 baud, 8 data bits, no parity.
   b. At the prompt, type **enable**.

c Type in the password; default password is **Cisco**.

d Type in the command **configure terminal**.

e Type in the command **interface do11Radio1**.

f Type **no amsdu transmit priority 0**

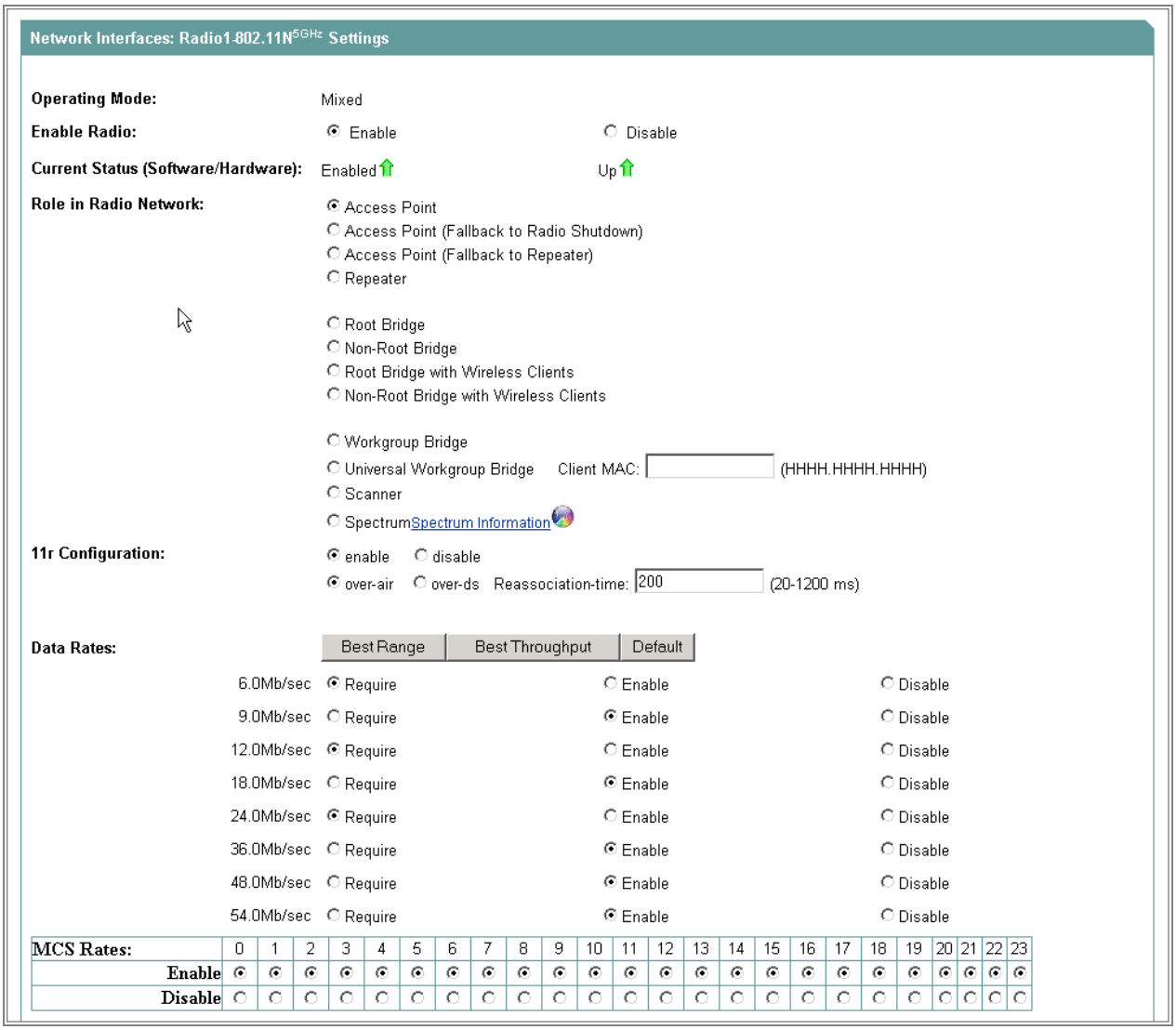
g Type **no amsdu transmit priority 1.**

h Type **no amsdu transmit priority 7.**

i Type **end** and then **write mem** to save configuration.

Note

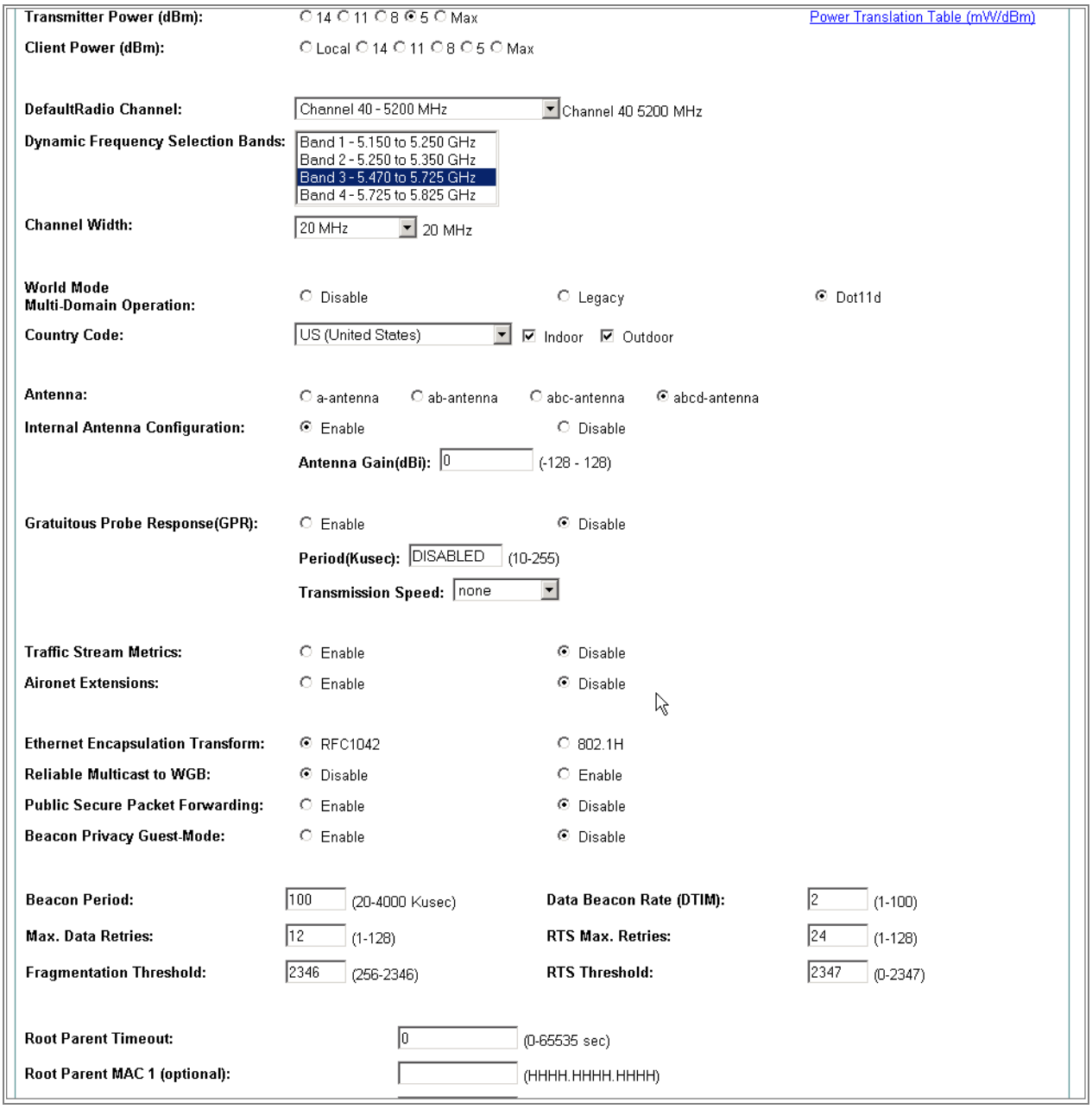
For AP models 1260 and 3500, 802.11n operation is not compatible with the 84-Series handsets and the 15.2.4-JA1 version.



6 Power level selection should be determined from your facility's RF site survey. Setting the **Client Power** to **Local** sets the handset power level as follows:

- **a** The 8020/8030 handsets will set the handset power level to the value advertised by the AP.
- **b** The 84-Series handsets, if the power settings for a given radio band are set to **Auto**, will set the handset power level to the value advertised by the AP.
- **c** The 84-Series handsets, if the power settings for a given radio band are set to something other than **Auto**, will set handset power to the level configured in the handset or the value advertised by the AP, whichever is lower.

7 **Channel** selection should be determined from your facility's RF site survey.



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.