CHAPTER 10

Cisco Unified IP Phone 7921 Implementation for Voice over WLAN

This chapter describes how to deploy the Cisco Unified Wireless IP Phone 7921G in the context of a Voice over WLAN (VoWLAN) environment. This chapter provides a brief introduction to the Cisco Unified Wireless IP Phone 7921G in general which is followed by detailed implementation guidance about the following deployment topics:

Cisco Unified Wireless IP Phone 7921 Overview

The Cisco Unified Wireless IP Phone 7921G is an IEEE 802.11 dual-band wireless device that provides comprehensive voice communications in conjunction with Cisco Unified Communications Manager and Cisco Aironet IEEE 802.11a/b/g access points (AP) in a private business communications network. This phone model supports G.711a, G.711u, G.729a and G.729ab audio compression coder-decoders (CODEC). You must configure and manage a wireless IP phone like other IP phones and wireless devices on your network. The wireless IP phone supports multiple lines and most of the IP phone features of other Cisco Unified IP phones. Figure 10-1 shows the Cisco Unified Wireless IP Phone 7921G.

Figure 10-1 Cisco Unified Wireless IP Phone 7921G

Refer to the to the following URL for the complete list of Cisco Unified Wireless IP Phone 7921G features, specifications, and capabilities:

http://www.cisco.com/en/US/products/hw/phones/ps379/products_data_sheet0900aecd805e315d.html

Network Connectivity Test Configuration for Cisco Unified Wireless IP Phone 7921

This section provides the minimal configuration necessary to get the Cisco Unified Wireless IP Phone 7921 connected to the network and communicating with the Cisco Unified Communications Manager. The intent of this section is to make it as simple as possible to verify that the network infrastructure is correctly configured for 7921 connectivity. Subsequent sections provide guidance for the addition of the necessary security, RF, and QoS features. Specific topics addressed in this section include the following:

Warning **This network connectivity test configuration should not be left active in a production network, as it provides no security against unauthorized access.**

WLAN Controller Network Connectivity Test Configuration

This section provides implementation guidance for initial WLAN Controller configuration.

Creating a Voice WLAN

Creating a WLAN with the minimum necessary configuration needed to test Cisco Unified Wireless IP Phone 7921 connectivity can be done using the following steps on the controller GUI.

Step 1 Click the **WLANs** tab in the controller GUI.

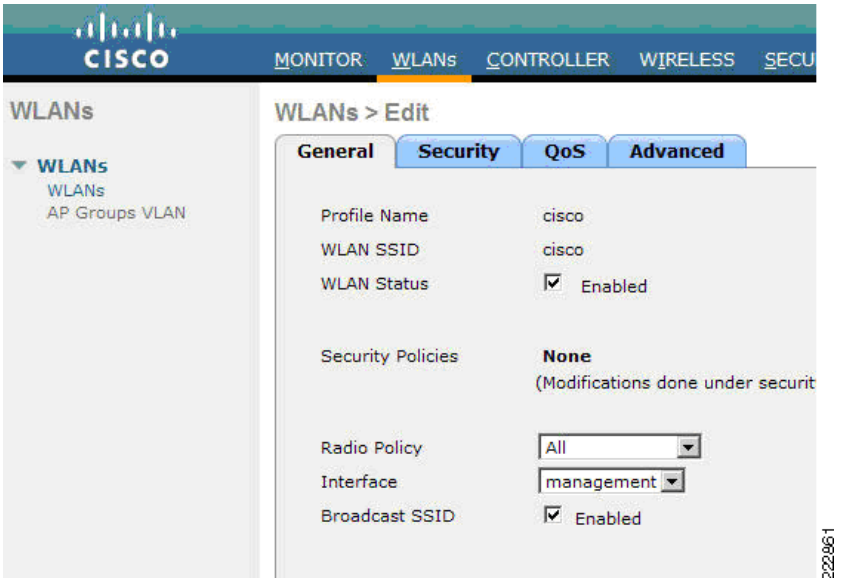
Step 2 Click the **New** button at the top-right corner of the page.

Step 3 For the new WLAN, define a profile name and use the Cisco Unified Wireless IP Phone 7921 default of **cisco** for the SSID.

Step 4 Click **Apply**.

Step 5 The *WLANs* > *Edit* page loads. See Figure 10-2.

Figure 10-2 WLANs > Edit Page



Step 6 Check **WLAN Status** box to signal that this new WLAN should be enabled.

Step 7 Change the *Interface* drop-down box to point to a user-defined dynamic interface (you must have predefined a dynamic interface; do not use the management interface)

Step 8 Click the **Security** tab.

Step 9 Change the *Layer-2 Security* drop-down box to **None**.

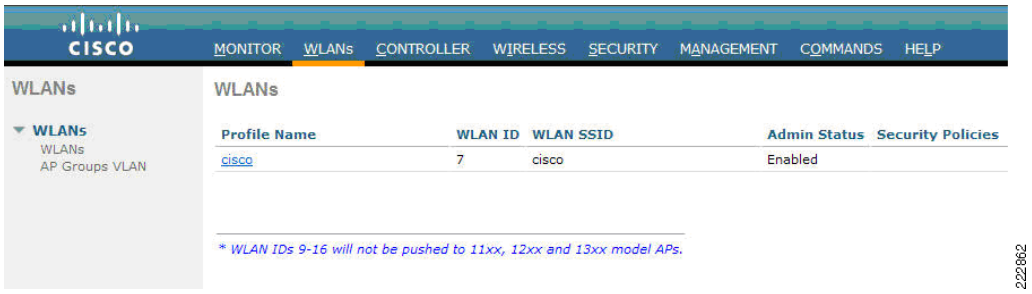
Step 10 Click the **QoS** tab.

Step 11 Change the *Quality of Service (QoS)* drop-down box to **Platinum (voice).**

Step 12 Click the **Apply** button at the top-right corner of the page

When the base controller WLAN configuration is complete, the WLAN window should look similar to Figure 10-3.

Figure 10-3 WLANs Page with Base Configuration



Network Infrastructure Base Configuration

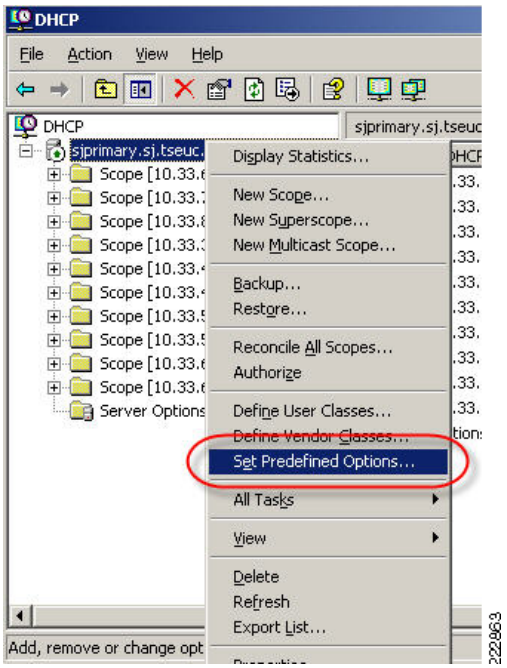
The network infrastructure used by the Cisco Unified Wireless IP Phone 7921 must provide DNS and DHCP services. These services are required for any Cisco IP phone, so they might be previously defined in many customer networks. If they are not defined, the following two sections provide details on how to define them.

Configuring the DHCP Server to Support Cisco Unified Communications Manager Option 150

To connect any Cisco IP phone, including the Cisco Unified Wireless IP Phone 7921, you must configure your DHCP server to provide option 150—the address of the TFTP server used by the phones to download the latest firmware version. Most networks use the default TFTP server provided with the Cisco Unified Communications Manager itself, so option 150 in the phones scope must point to the Cisco Unified Communications Manager IP address.

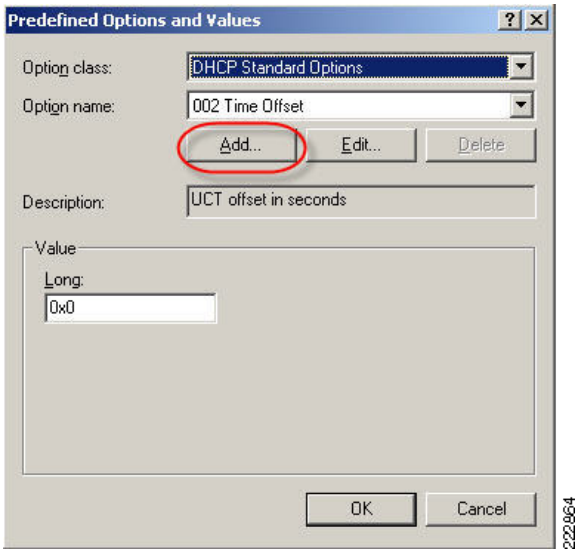
Step 1 Right-click appropriate DHCP Server and select **Set Predefined Options**. See Figure 10-4.

Figure 10-4 Setting Predefined Options



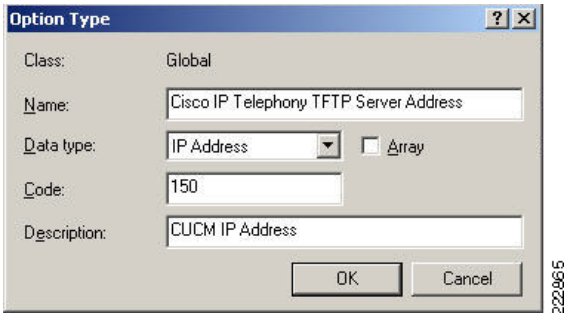
Step 2 Click **Add** in the *Predefined Options and Values* pop-up window. See Figure 10-5.

Figure 10-5 Selecting the Add Option



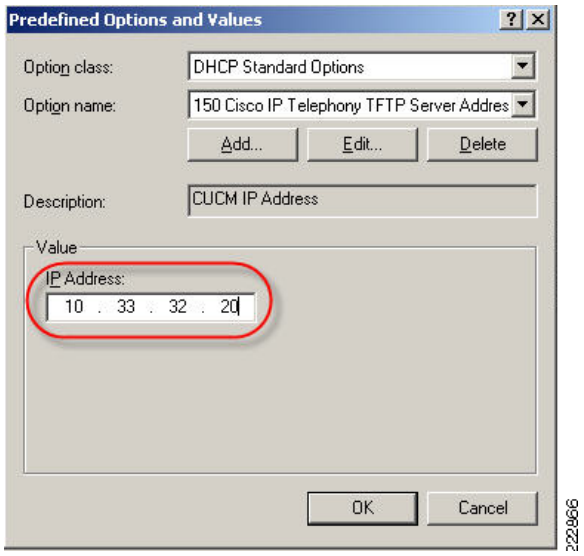
Step 3 Fill out the new option and click **OK**. See Figure 10-6.

Figure 10-6 Entering the Option Type Information



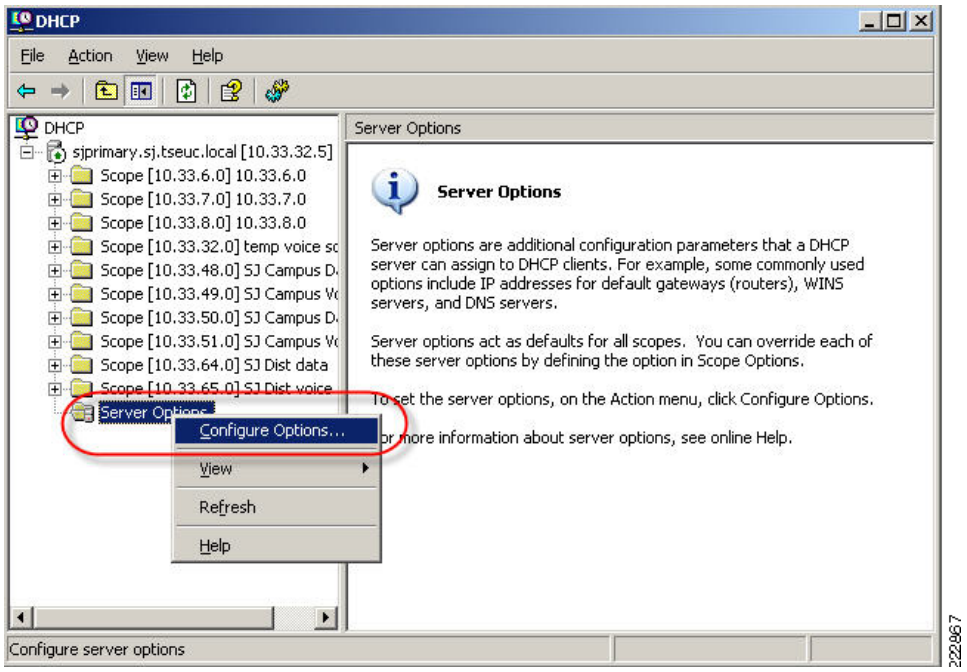
Step 4 Enter in the *IP address* of the Cisco Unified Communications Manager and click **OK.** See Figure 10-7.

Figure 10-7 Entering IP Address in Predefined Options and Values



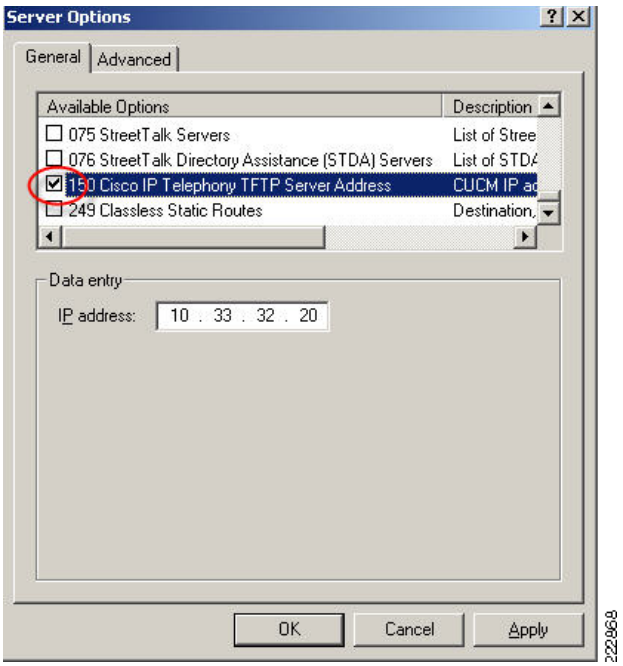
Step 5 Configure the DHCP server to pass the newly defined option 150 to all DHCP clients. Select **Server Options**, then click **Configure Options**. See Figure 10-8.

Figure 10-8 Choosing DHCP Server Configuration Options



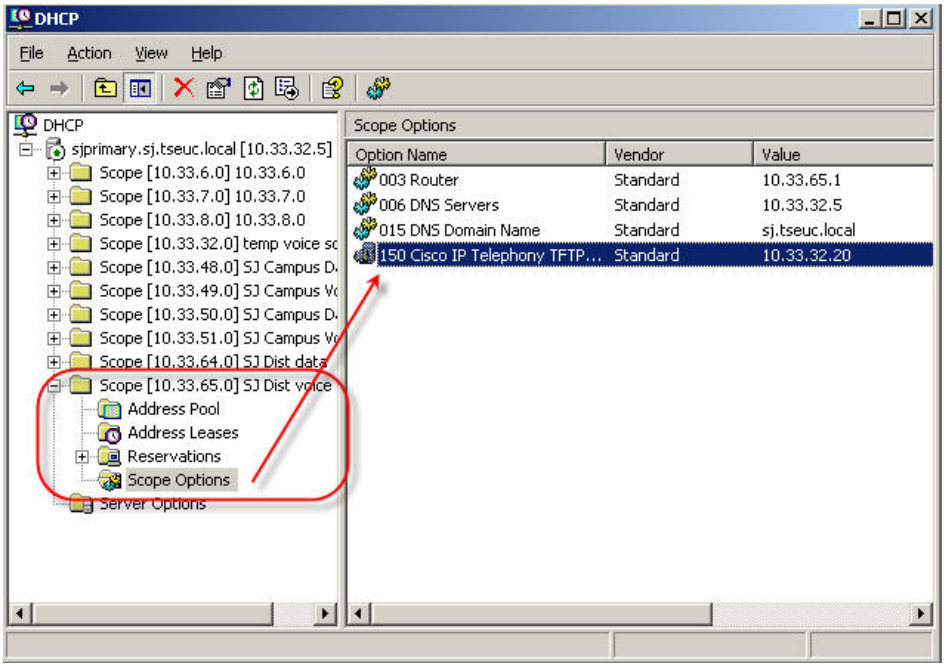
Step 6 Select your newly created class from the drop-down menu, check your newly created option 150, and click **OK**. See Figure 10-9.

Figure 10-9 Choosing Option 150 from Server Options



Step 7 Select a DHCP scope and verify that option 150 now shows up in the *Scope Options* window. See Figure 10-10.

Figure 10-10 DHCP Scope Options Window



Configuring the DNS with Cisco Unified Communications Manager Entries

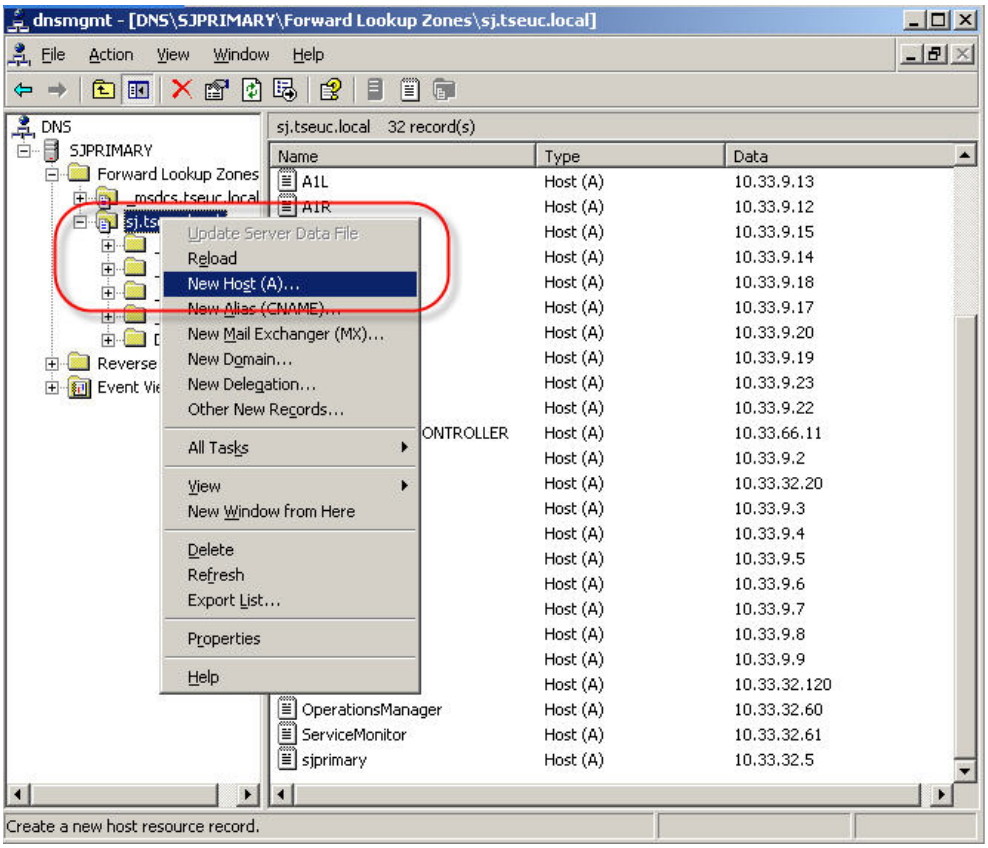
An Cisco IP phone (including the Cisco Unified Wireless IP Phone 7921) uses DHCP option 150 to learn the IP address of an associated TFTP server. An Cisco IP phone downloads its configuration file from the TFTP server. That configuration file contains the name of the Cisco Unified Communications Manager publisher and subscribers. The Cisco IP phone uses DNS to resolve a Cisco Unified Communications Manager name into an IP address that can be used with IP telephony registration messages.

If Cisco IP phones have already been deployed, the DNS configuration will already be complete, and this step can be skipped.

The following steps must be completed once for the Cisco Unified Communications Manager publisher, and once for each of the Cisco Unified Communications Manager subscribers.

Step 1 From the DNS server console, right-click the relevant forward lookup zone, and select **New Host (A)...** See Figure 10-11.

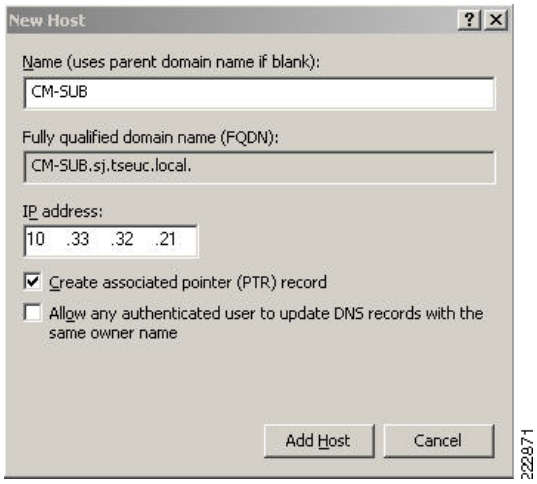
Figure 10-11 New Host (A)



Step 2 Fill out the *Name* and *IP address* of the Cisco Unified Communications Manager publisher server or subscriber server and click **Add Host**. See Figure 10-12.

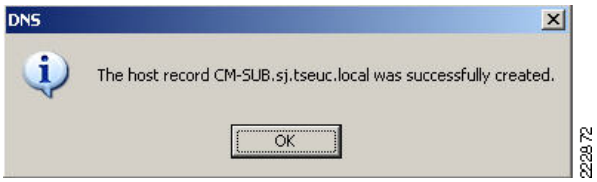
The "Cisco Unified Communications Manager Base Configuration" section on page 10-10 describes how to determine the Cisco Unified Communications Manager name from Cisco Unified Communications Manager administration.

Figure 10-12 Entering New Host Name



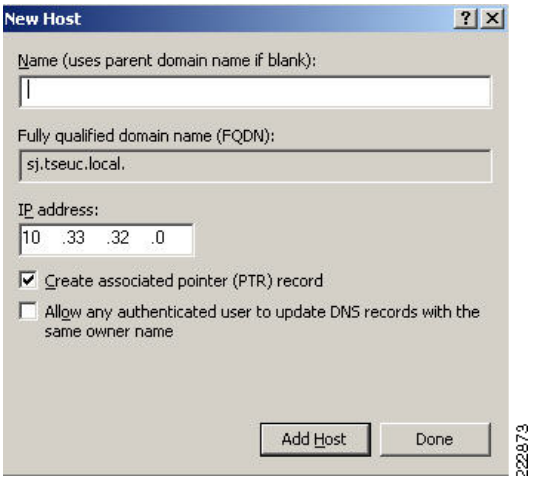
Step 3 Click **OK** to acknowledge the success message. See Figure 10-13.

Figure 10-13 Acknowledging Successful Host Record Creation



Step 4 Either, fill out the *Name* and *IP address* of the next Cisco Unified Communications Manager publisher server or subscriber server and click **Add Host**, or click **Done** to exit DNS configuration. See Figure 10-14.

Figure 10-14 Entering Cisco Unified Communications Manager Publisher Information



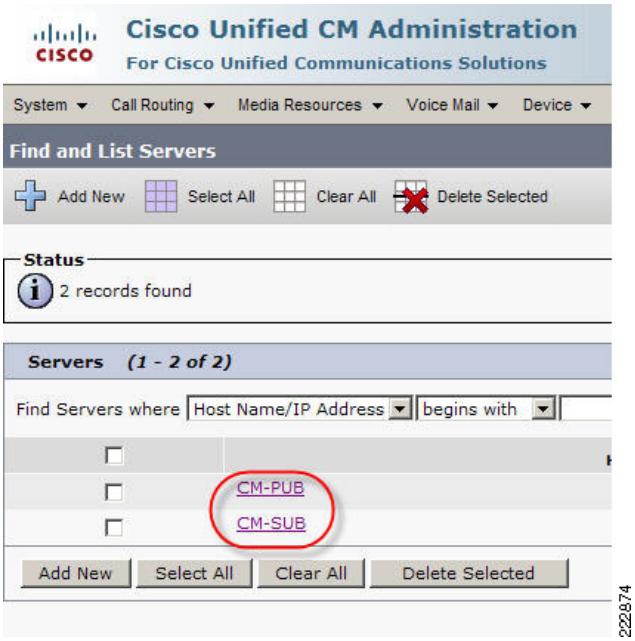
Cisco Unified Communications Manager Base Configuration

This section assumes a Cisco Unified Communications Manager installation pre-exists and provides procedures for verifying the necessary settings to enable a Cisco Unified Wireless IP Phone 7921 to successfully operate.

Verifying Cisco Unified Communications Manager Name

You must know the Cisco Unified Communications Manager server name in order to ensure that it is correctly configured in the DNS server as described in the "Configuring the DNS with Cisco Unified Communications Manager Entries" section on page 10-8. From Cisco Unified Communications Manager administration window, navigate to *System* > *Server* > *Find*. By leaving all the *Find* fields blank, the system will display all Cisco Unified Communications Manager names known to the system. See Figure 10-15.

Figure 10-15 Verifying Cisco Unified Communications Manager Server Names

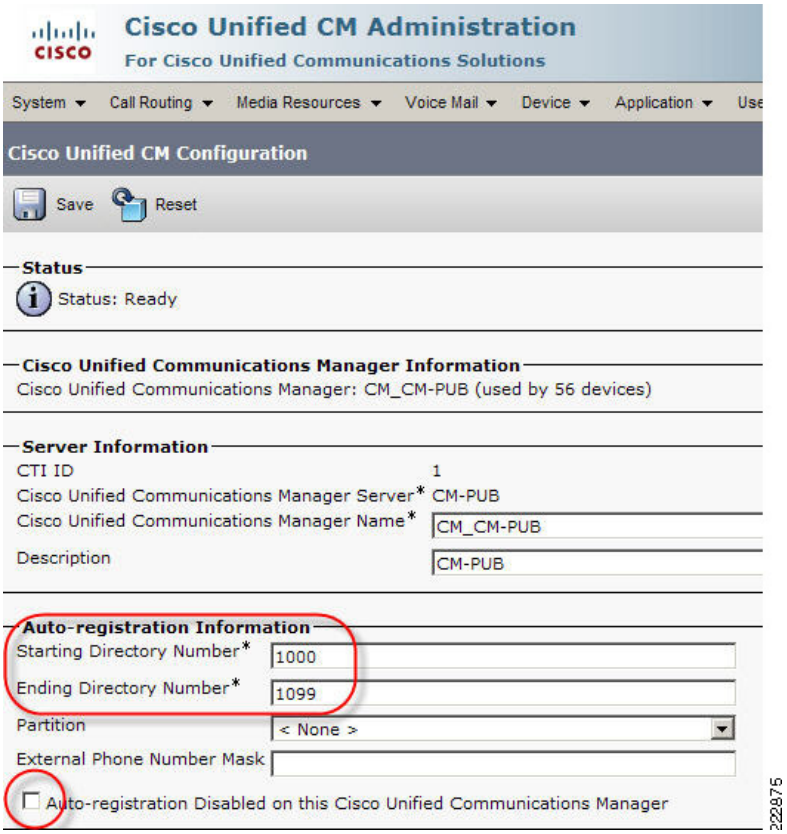


Verifying Auto-Registration Enabled

The simplest way to enable Cisco Unified Wireless IP Phone 7921 registration to a Cisco Unified Communications Manager is to enable auto-registration. To verify or enable auto-registration, navigate to *System* > *Cisco Unified CM* > *Find*. When the *Find* action completes, click the relevant Cisco Unified Communications Manager name and verify that auto-registration is enabled on that Cisco Unified Communications Manager. See Figure 10-16.

In production environments, auto-registration is often disabled and phones are added by explicitly defining each phone in Cisco Unified Communications Manager. Follow the procedures established at your site for adding phones.

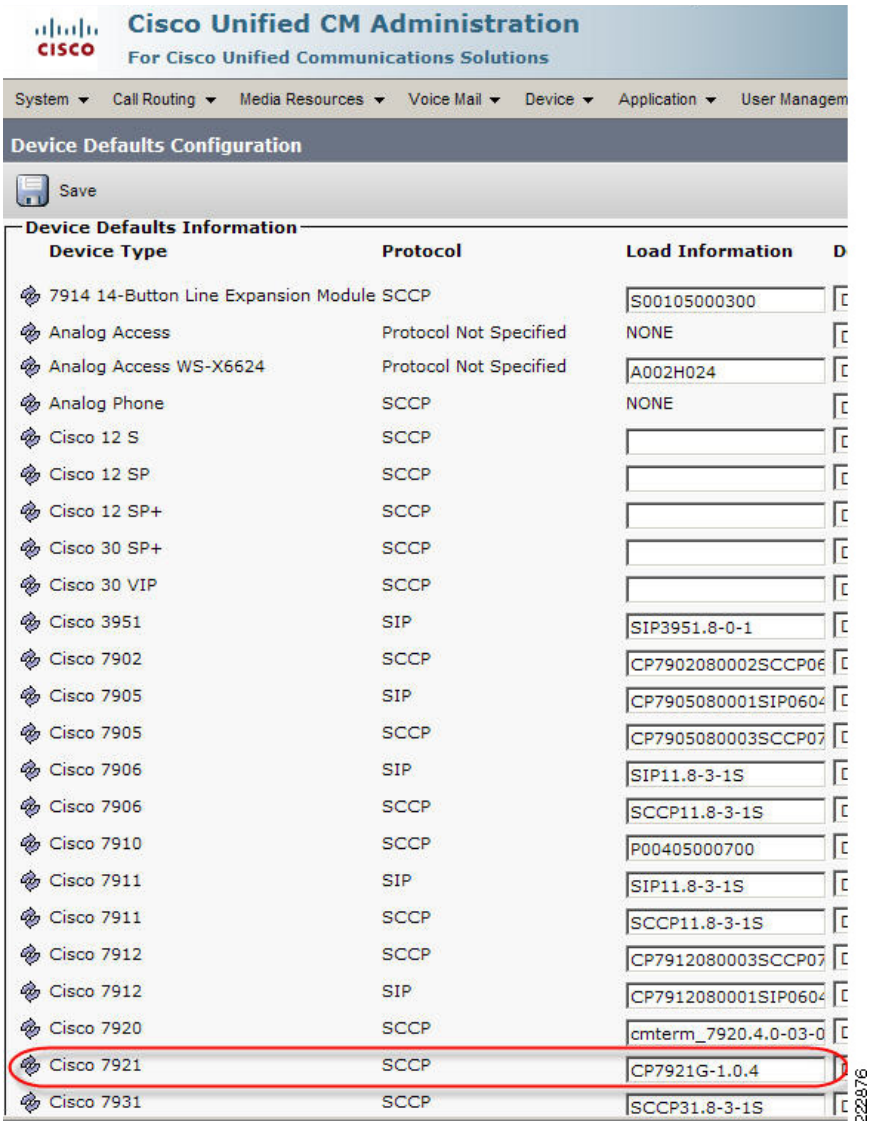
Figure 10-16 Cisco Unified Communications Manager Auto Registration:



Verifying Cisco Unified Wireless IP Phone 7921 Firmware

The Cisco Unified Wireless IP Phone 7921 updates its firmware from the Cisco Unified Communications Manager TFTP server. Customers are strongly encouraged to run the most recent release of Cisco Unified Wireless IP Phone 7921 firmware. The current release on Cisco.com can be determined by going to http://www.cisco.com, logging in, and navigating to *Support* > *Download Software* > *Voice Software* > *Cisco Unified Wireless IP Phone Firmware*. Make a note of the most recent version of firmware available on Cisco.com, and ensure the same version is loaded in the Cisco Unified Communications Manager by navigating on Cisco Unified Communications Manager to *Device* > *Device Settings* > *Device Defaults*. See Figure 10-17.

Figure 10-17 Cisco Unified Communications Manager Device Defaults



Cisco Unified Wireless IP Phone 7921 Base Configuration

Baseline configuration for the IP phone consist of two procedures:

- Resetting the IP Phone, page 10-13
- Configuring a WLAN Profile, page 10-14

Resetting the IP Phone

If necessary, reset the Cisco Unified Wireless IP Phone 7921 to factory defaults. The factory default option erases all user-defined entries in Network Profiles, Phone Settings, and Call History. To erase the local configuration, follow these steps:

Step 1 Press the **Navigation Button** downwards to enter *SETTINGS* mode

Step 2 Navigate to and select *Phone Settings*.

Step 3 Press ****2** on the keypad. The phone briefly displays this prompt: *Restore to Default?*

Step 4 Press the **Yes** softkey to confirm or **No** to cancel. The phone resets after selecting *Yes*

Configuring a WLAN Profile

The following procedure summarizes the process of configuring the WLAN profile:

Step 1 Press the **Navigation Button** downwards to enter *SETTINGS* mode

Step 2 Navigate to and select *Network Profiles* (pressing the number adjacent to a menu item is equivalent to selecting that item).

Step 3 Unlock the IP phone's configuration menu by pressing ****#.** The padlock icon on the top-right of the screen will change from closed to open.

Step 4 Navigate to the profile you want to change and press the **Change** softkey.

Step 5 Navigate to and select *Profile Name*.

Step 6 Use the IP phone's keypad to enter a profile name. Normally this name will match the corresponding WLAN profile name defined on the Cisco Wireless LAN Controller (Cisco WLC).

Step 7 Navigate to and select *WLAN Configuration*.

Step 8 Navigate to and select *SSID*.

Step 9 Use the IP phone's keypad to enter a SSID name (normally this name will match the corresponding WLAN SSID name defined on the Cisco WLC).

Step 10 Press the **Back** softkey until the **Exit** softkey appears.

Step 11 Press the **Exit** softkey.

Trace Analysis for a Base Configuration

This section presents annotated sections of a trace of a Cisco Unified Wireless IP Phone 7921 being connected to a network for the first time. Five distinct sections of this trace are examined—highlighting the different stages of the connection. See Figure 10-18. The first section shows the initial connection and the start of the TFTP download.

Because this is the first time the Cisco Unified Wireless IP Phone 7921 has connected, its firmware is out of date. One of the first files the phone downloads contains the name of the firmware image that the Cisco Unified Wireless IP Phone 7921 should be running. The Cisco Unified Wireless IP Phone 7921 will see this and will download the specified firmware image. Because of the need to download a new firmware image, the TFTP process takes longer than it would if the Cisco Unified Wireless IP Phone 7921 was already running the correct firmware.

Figure 10-18 Initial Cisco Unified Wireless IP Phone 7921 Connect Trace (Part 1)

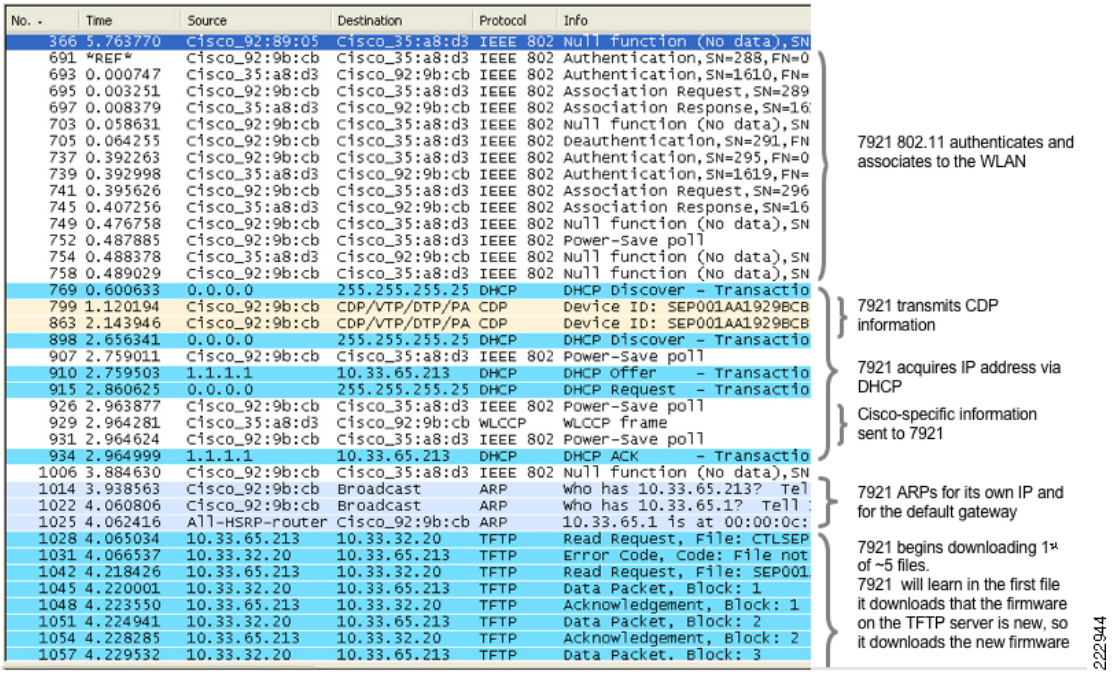


Figure 10-19 illustrates the end of the initial TFTP download sequence. At this point five TFTP files containing the Cisco Unified Wireless IP Phone 7921 configuration and firmware have been downloaded.

Figure 10-19 Initial Cisco Unified Wireless IP Phone 7921 Connect Trace (Part 2)

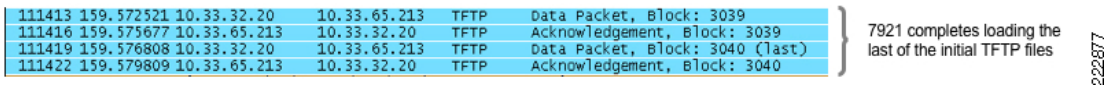


Figure 10-20 illustrates that the Cisco Unified Wireless IP Phone 7921 has downloaded and installed the new firmware, and then rebooted. The TFTP download in this case is much shorter and quicker.

Figure 10-20 Initial Cisco Unified Wireless IP Phone 7921 Connect Trace (Part 3)

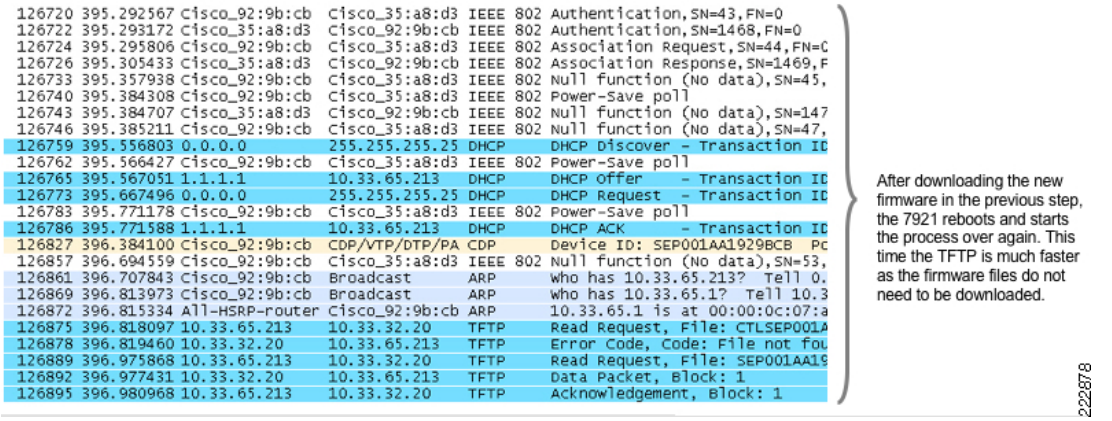
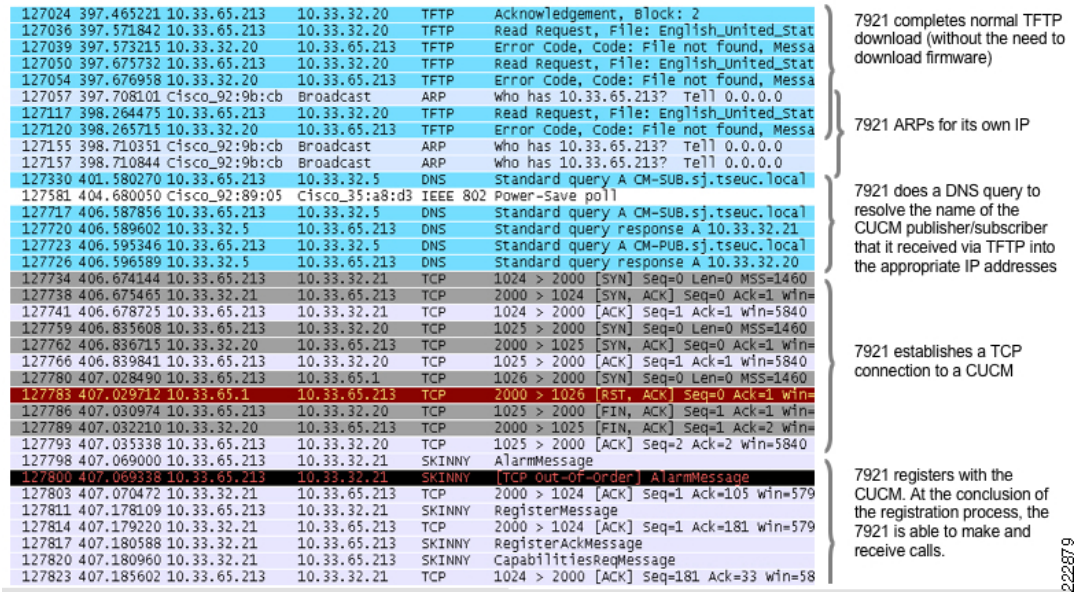


Figure 10-21 illustrates the conclusion of the normal TFTP sequence, the ARPs verifying that the IP address is unique, and a DNS lookup to resolve the name to IP address of the Cisco Unified Communications Manager publisher and subscriber that learned via the TFTP configuration file. The Cisco Unified Wireless IP Phone 7921 then starts a TCP connection to the subscriber Cisco Unified Communications Manager and begins the phone registration process (shown here as the *skinny* protocol).

Figure 10-21 Initial Cisco Unified Wireless IP Phone 7921 Connect Trace (Part 4)



Cisco Unified Wireless IP Phone 7921 Security

The Cisco Unified Wireless IP Phone 7921 supports the following WLAN security options:

- Security protocols
  - Wi-Fi Protected Access (WPA) Versions 1 and 2; Personal and Enterprise
- Authentication
  - Lightweight Extensible Authentication Protocol (LEAP) Authentication
  - Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)
  - WEP/WPA/WPA2 Shared Key
- Encryption
  - Wired Equivalent Privacy (WEP)
  - Temporal Key Integrity Protocol (TKIP)
  - Advanced Encryption Standard (AES)
- Fast roaming protocol
  - Cisco Centralized Key Management (CCKM)

The remainder of the Cisco Unified Wireless IP Phone 7921 security section provided in this chapter focuses on the items listed that comprise the current best practice recommendations for secure Cisco Unified Wireless IP Phone 7921 deployments. More information on other Cisco Unified Wireless IP Phone 7921 security options is available in the product documentation available at http://www.cisco.com.

Controller WLAN Security Configuration

The optimal configuration for the controller configuration for the WLAN supporting Cisco Unified Wireless IP Phone 7921s is for the WPA security protocol with TKIP encryption and IEEE 802.1X with CCKM key management.

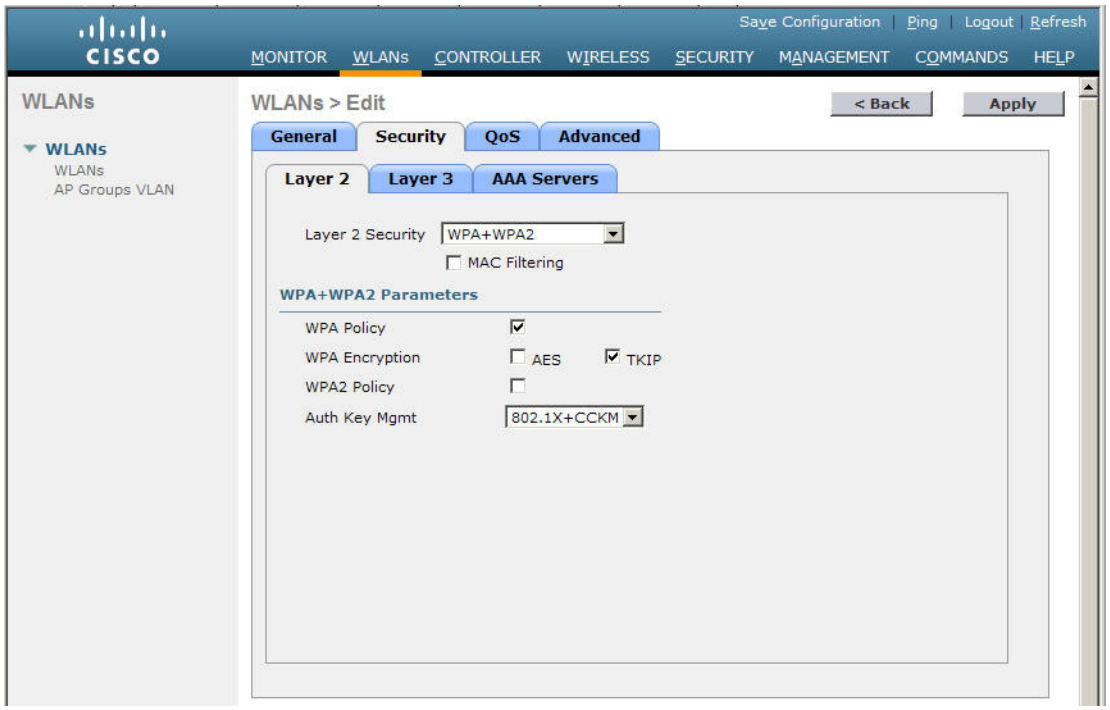
The combination of WPA, TKIP, IEEE 802.1X/CCKM provides the strongest supported authentication, encryption, and key management with CCKM for fast secure roaming between APs. Chapter 5, "Voice over WLAN Roaming," provides additional details addressing CCKM and describes why it is necessary to achieve voice handset roam times between APs in less than the ITU G.114 recommended maximum delay of 150 msec.

Note Cisco Unified Wireless IP Phone 7921s do not support WPA2 with TKIP encryption.

Note Cisco Unified Wireless IP Phone 7921s support WPA2 with AES encryption, but CCKM is not supported in this combination. Even though CCKM can be configured, and the Cisco Unified Wireless IP Phone 7921s appear to connect successfully, CCKM will not be used when roaming between APs in this combination.

The recommended configuration is shown Figure 10-22.

Figure 10-22 Cisco WLC Security Layer 2 Recommended Configuration

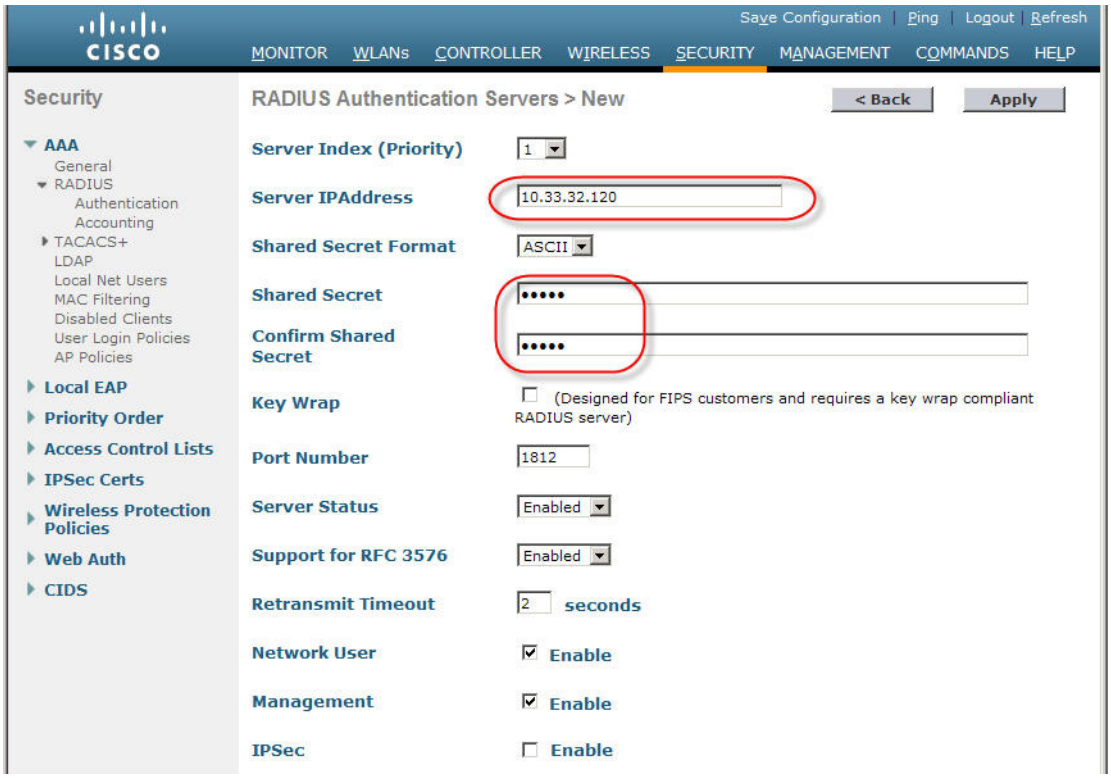


The recommended configuration uses IEEE 802.1X key management; that necessitates a RADIUS server for authentication. RADIUS server information is added to the controller by navigating *Security* > *RADIUS* > *Authentication*.

Cisco WLAN Controllers also support a mode known as *Local EAP*. When you enable Local EAP, the controller serves as the authentication server and the local user database, thereby removing dependence on an external authentication server. Local EAP is designed for use in remote offices that must maintain connectivity to wireless clients when the remote external authentication server is lost.

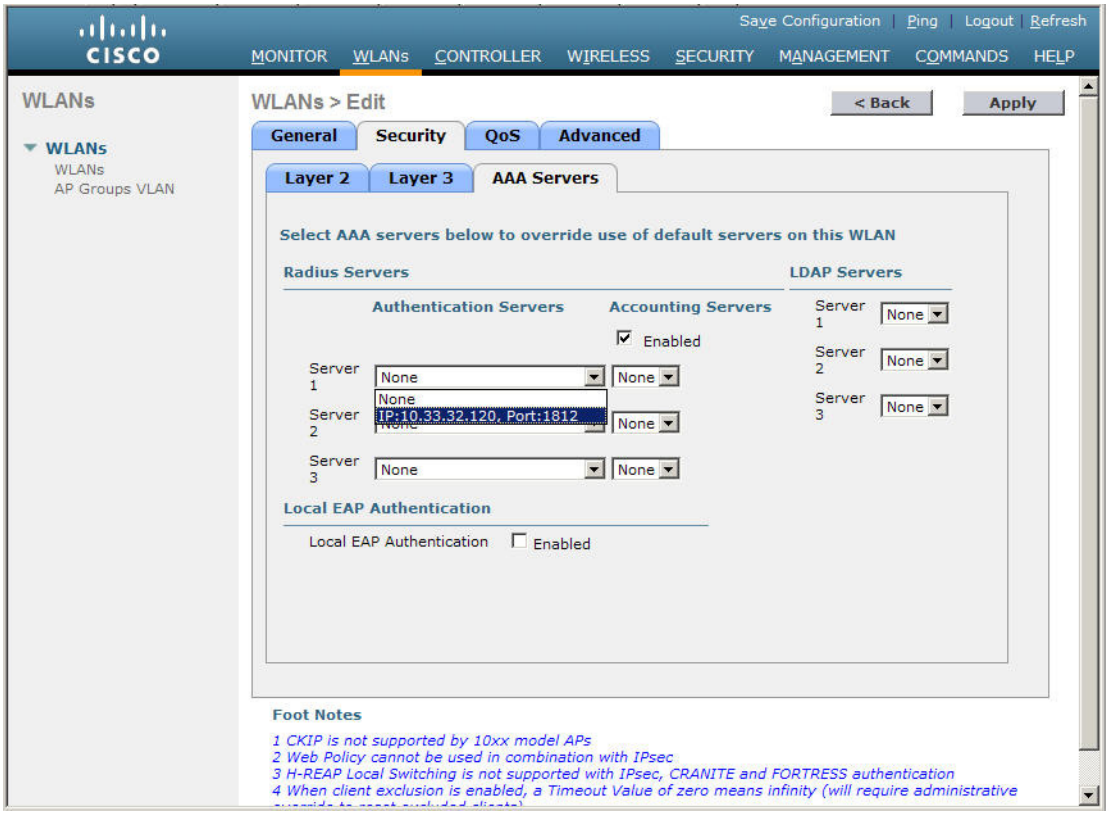
Figure 10-23 shows a RADIUS server definition being added to a controller. In Figure 10-23, the *Server IP Address* field is the IP address of the external RADIUS server. The shared secret is defined on both the controller and the RADIUS server; it is used to secure communications between the two. Chapter 4, "Voice over WLAN Security," provides details about configuring the Cisco ACS server to act as the external RADIUS server for wireless LAN EAP authentication.

Figure 10-23 Adding a RADIUS server to the Controller



Once the external RADIUS server definition has been added to the controller, the RADIUS server can be selected from the drop-down box for use by individual WLANs. Figure 10-24 shows a RADIUS server being selected from the *WLANs* > *Security* > *AAA Servers* tab.

Figure 10-24 Selecting Cisco WLC Security AAA Servers



Setting the WLAN Controller IEEE 802.1X Timeout for EAP-FAST

When using EAP-FAST, the IEEE 802.1X timeout on the controller must be increased (default = 2 seconds) in order for the client to obtain the PAC via automatic provisioning. The default timeout on the Cisco ACS server is 20 seconds, which is the recommended value. To change the IEEE 802.1X timeout on the Cisco Wireless LAN controller, connect using Telnet or SSH to the controller and enter the following command:

```
(Cisco Controller)> config advanced eap request-timeout 20

(Cisco Controller)> show advanced eap
 EAP-Identity-Request Timeout (seconds)..... 1
 EAP-Identity-Request Max Retries.............. 20
 EAP Key-Index for Dynamic WEP................. 0
 EAP-Request Timeout (seconds)................. 20
 EAP-Request Max Retries....................... 2
```

Cisco Unified Communications Manager Security Configuration

The Cisco Unified Wireless IP Phone 7921G supports the following voice security features:

- Certificates
- Image authentication
- Device authentication

- File authentication
- Signaling authentication
- Secure Cisco Unified SRST
- Media encryption (SRTP)

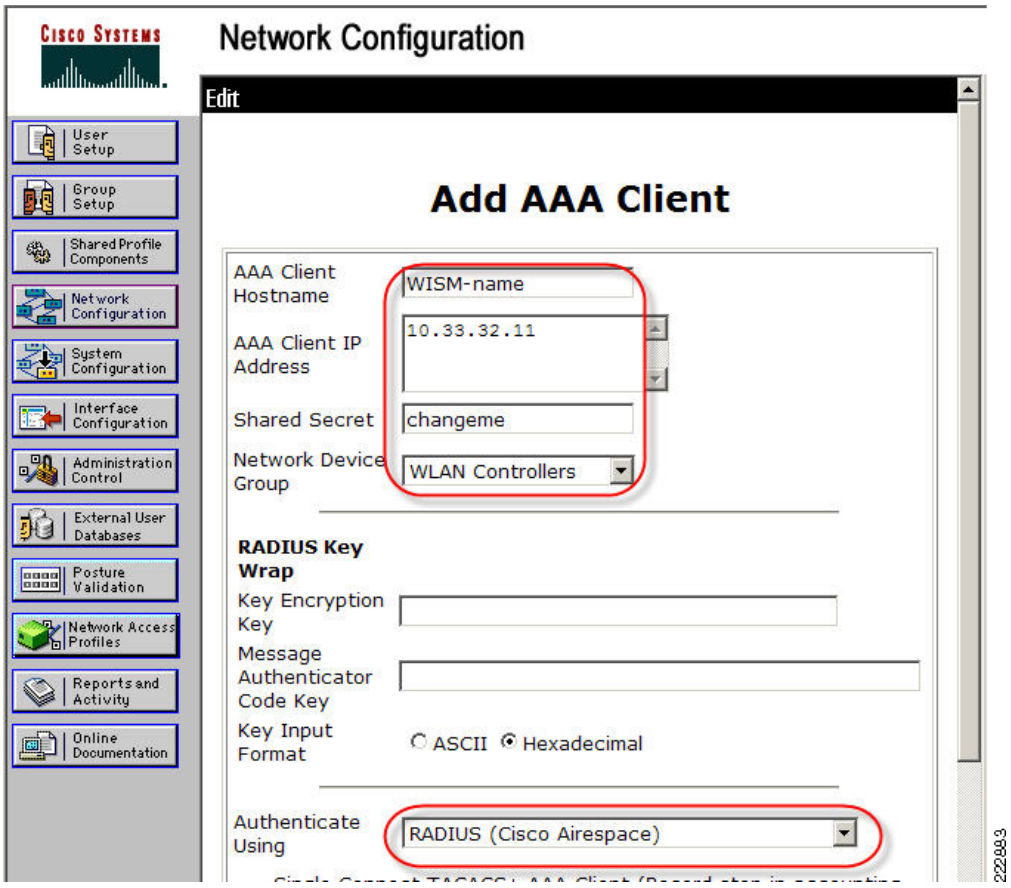
The Cisco Unified Communications Manager provides these available voice security features. For more information, refer to the Cisco Unified Communications Manager documentation at http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Network infrastructure Security Configuration

EAP-FAST authenticates to a RADIUS server. In this section, we configure the Cisco ACS server to support EAP-FAST authentication.

Every network device performing EAP authentication must be defined to the ACS as an *AAA Client*. On the ACS, we define the controller as an AAA Client by navigating *Network Configuration* > (select a group if device groups are being used) > *Add Entry*. Figure 10-25 shows an example of a controller being defined on the ACS.

Figure 10-25 Cisco ACS Configuration—Adding NAS



Every Cisco Unified Wireless IP Phone 7921 using EAP-FAST is configured with a *userid* and a *password*.

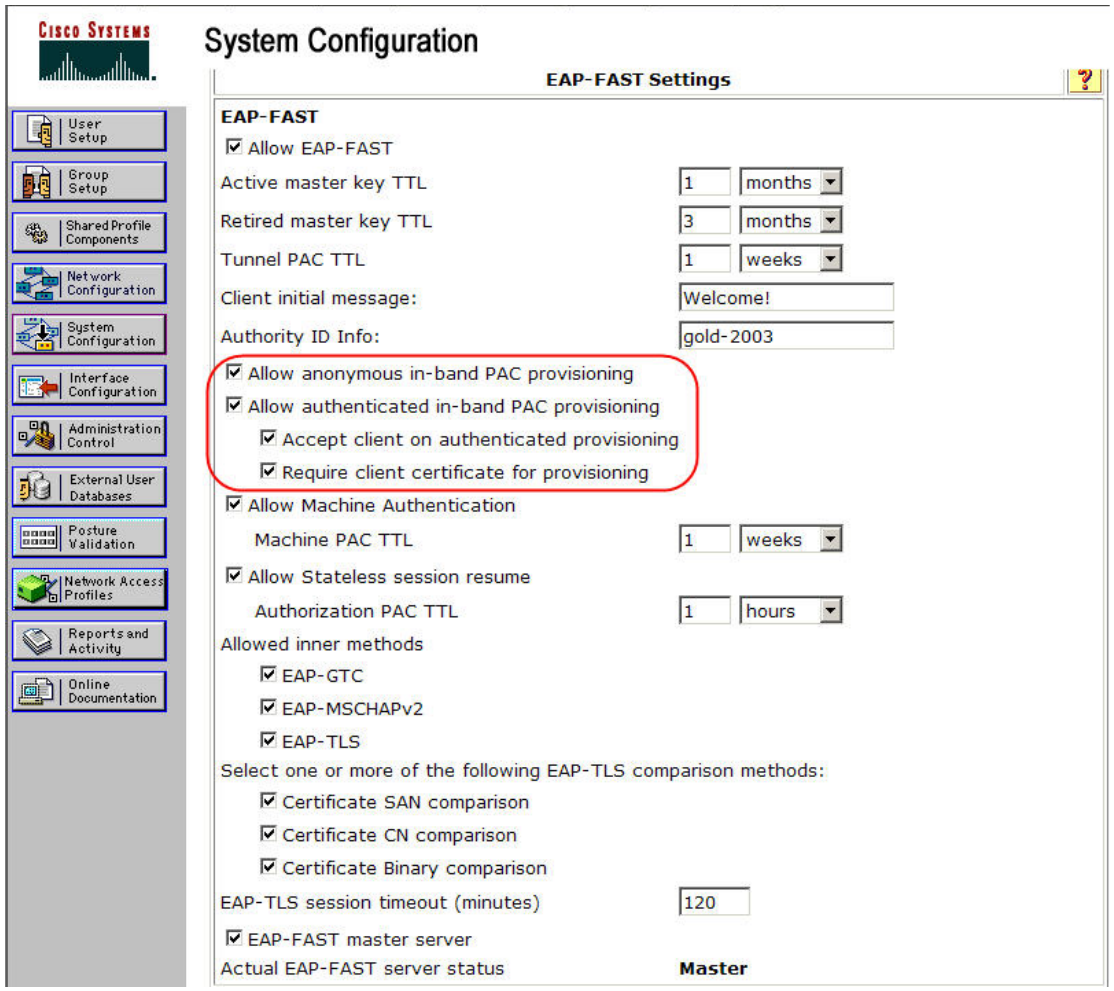
It is possible to configure multiple Cisco Unified Wireless IP Phone 7921s with the same userid and password. This is useful for small test deployments, but should be avoided in productions deployments where the loss of a single phone could require all deployed phones to be reconfigured.

Figure 10-26 shows a Cisco Unified Wireless IP Phone 7921s userid and password being configured on the ACS. This is done by navigating *User Setup* > (enter the name of the new user being added) > *Add/Edit*.

Figure 10-26 ACS Configuration—Adding a User

The ACS must also be configured to explicitly support EAP-FAST authentication. The Cisco Unified Wireless IP Phone 7921G currently supports only automatic provisioning of the Protected Access Credential (PAC), so *Anonymous In-Band PAC Provisioning* must be enabled. EAP-FAST is configured by navigating *System Configuration* > *Global Authentication Setup* > *EAP-FAST Configuration*. See Figure 10-27.

Figure 10-27 ACS Configuration—EAP-FAST Settings



Cisco Unified Wireless IP Phone 7921 Security Configuration

The "Cisco Unified Wireless IP Phone 7921 Base Configuration" section on page 10-13 covered resetting a Cisco Unified Wireless IP Phone 7921 to factory defaults (if necessary) and adding a new WLAN Profile. Follow the instructions in that section to create a new WLAN profile for a EAP-FAST WLAN. This section focuses on configuring EAP-FAST.

Configure a WLAN Profile to use EAP-FAST Authentication

Cisco Unified Wireless IP Phone 7921s can be configured to use EAP-FAST with a specific userid and password as described in the following procedure.

Step 1 Press the **Navigation Button** downwards to enter *SETTINGS* mode

Step 2 Navigate to and select **Network Profiles** (pressing the number adjacent to a menu item is equivalent to selecting that item).

Step 3 Unlock the phones configuration menu by pressing **#. The padlock icon on the top-right of the screen will change from closed to open.

Step 4 Navigate to the profile you want to change and press the **Change** softkey.

Step 5 Navigate to and select **WLAN Configuration**.

Step 6 Navigate to and select **Security Mode**.

Step 7 Navigate to and select **EAP-FAST**.

Step 8 Press the **Save** soft-key.

Step 9 Navigate to and select **UserName**.

Step 10 Use the IP phone's keypad to enter a *username* (press the **Select** button to enter).

Step 11 Navigate to and select **Password**.

Step 12 Use the IP phone's keypad to enter a *password* (press the select button to enter).

Step 13 Press the **Back** softkey until *Network Profiles* re-appears.

Step 14 Select the newly added profile for EAP-FAST and de-select the old profile.

Step 15 Press the **Back** softkey until the **Exit** softkey appears.

Step 16 Press the **Exit** softkey,

Cisco Unified Wireless IP Phone 7921 RF Considerations

A well-designed and effectively deployed RF environment is critical for a successful VoWLAN implementation. A wireless network that appears to function well for data traffic might provide unsatisfactory coverage for a voice deployment. This is because data applications can often tolerate packet delays or recover from packet loss that would be disruptive to a voice call.

Refer to the datasheet at the following URL for Cisco Unified Wireless IP Phone 7921 RF specifications:

http://www.cisco.com/en/US/products/hw/phones/ps379/products_data_sheet0900aecd805e315d.html

Chapter 3, "Voice over WLAN Radio Frequency Design," provides general RF deployment guidance as well as voice call capacity information. In particular, the following general VoWLAN guidelines, as stated in the RF design for voice, are applicable to the Cisco Unified Wireless IP Phone 7921:

- VoWLAN networks require overlaps of about 20 percent (for 2.4 GHz), and about 15 percent (for 5 GHz), where a WLAN data design might use an AP cell overlap of 5-to-10 percent.
- The recommended VoWLAN cell boundary recommendation is -67 dBm, while a WLAN data cell boundary might be acceptable at lower power levels.

Choosing Between IEEE 802.11b/g and IEEE 802.11a

It is a common customer requirement to deploy voice on the relatively interference-free IEEE 802.11a 5 GHz frequency band (see Chapter 3, "Voice over WLAN Radio Frequency Design," for more details). There are two ways in which voice can be restricted to just one frequency band (IEEE 802.11a or just IEEE 802.11b/g).

- By configuring the phone to use one frequency band

- By configuring the WLAN on the controller to support only one frequency band

Configuration guidance for these two option is provided in the sections that follow.

The recommended method used to limit the Cisco Unified Wireless IP Phone 7921 operation to a single frequency band is to leave the phones at their default setting and to configure the WLAN on the controller—or Cisco Wireless Control System (WCS)—to operate on the required frequency band.

Cisco Unified Wireless IP Phone 7921 RF Configuration

The Cisco Unified Wireless IP Phone 7921 is enabled for all IEEE 802.11 frequency bands (IEEE 802.11b/g and IEEE 802.11a) by default. The frequency band used can be changed with the following procedure:

Step 1 Press the **Navigation Button** downwards to enter *SETTINGS* mode.

Step 2 Navigate to and select **Network Profiles** (pressing the number adjacent to a menu item is equivalent to selecting that item).

Step 3 Unlock the phones configuration menu by pressing **#. The padlock icon on the top-right of the screen will change from closed to open.

Step 4 Navigate to the profile you want to change and press the **Change** softkey.

Step 5 Navigate to and select **WLAN Configuration**.

Step 6 Navigate to and select **802.11 Mode**.

Step 7 Navigate to and select the mode option you wish to use.

Step 8 Press the **Save** soft-key.

Step 9 Press the **Back** softkey until the **Exit** softkey appears.

Step 10 Press the **Exit** softkey.

The available options for IEEE 802.11 mode are shown in Table 10-1

Table 10-1 Available IEEE 802.11 Mode Options

IEEE 802.11 Mode	Description
IEEE 802.11b/g	Always use only IEEE 802.11b/g
IEEE 802.11a	Always use only IEEE 802.11a
Auto-b/g	Use IEEE 802.11b/g if available, fallback to IEEE 802.11a if not
Auto-a	Use IEEE 802.11a if available, fallback to IEEE 802.11b/g if not
Auto-RSSI	Use whatever frequency band has the strongest RSSI

Behavior in Presence of 2.4 GHz IEEE 802.11 b/g and 5 GHz

If the Cisco Unified Wireless IP Phone 7921 is enabled for both IEEE 802.11b/g and IEEE 802.11a, and receives beacons on both of these frequency bands for the voice SSID (assuming there is sufficient admission control capacity on each frequency band), the following notes apply.

On Cisco Unified Wireless IP Phone 7921 initial association:

- If the default Auto-RSSI is enabled, the phone will associate to the radio (and therefore frequency band) it acquires having the strongest Receive Signal Strength Indicator (RSSI).
- If Auto-b/g or Auto-a is enabled, the phone will associate to the frequency band specified and will fall back to the non-specified frequency band only if the specified frequency is unavailable
- If IEEE 802.11-b/g or IEEE 802.11-a is enabled, the phone will only associate to the frequency band specified.

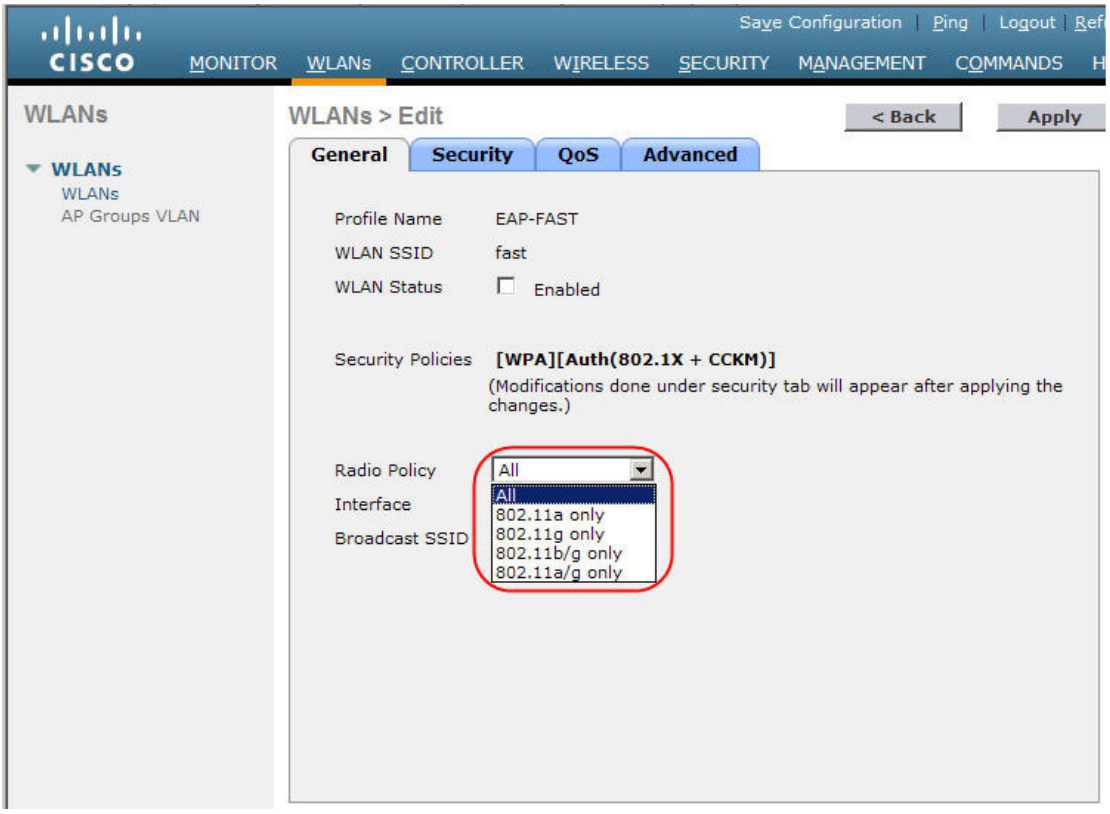
On Cisco Unified Wireless IP Phone 7921 roam:

- Once the phone has associated to an AP on a particular frequency band, it will only scan for and roam to APs on the same frequency band.
- If the Cisco Unified Wireless IP Phone 7921 has moved beyond the boundaries of the frequency band it initially associated with and cannot roam to another AP on that frequency band, then the Cisco Unified Wireless IP Phone 7921 will become disassociated and will begin the association process again (looking on both frequency bands).

WLAN RF—Controller Configuration

The recommended way to limit the Cisco Unified Wireless IP Phone 7921 operation to a single frequency band (such as IEEE 802.11a or IEEE 802.11b/g) is to leave the phone at its default setting and to configure the WLAN on the controller (or Cisco WCS) to operate on a single frequency band. Figure 10-28 shows the options available to restrict a voice VLAN to specific frequency ranges.

Figure 10-28 VLAN Radio Policy



Cisco Unified Wireless IP Phone 7921 QoS

A well-designed and effectively deployed QoS implementation is critical for a successful VoWLAN deployment. A wireless network that appears to function well for data traffic might well provide unsatisfactory performance for a voice deployment. This is because data applications can often tolerate packet delays or recover from packet loss that would be disruptive to a voice call.

Chapter 2, "WLAN Quality of Service," provides general QoS deployment guidance.

Cisco Unified Wireless IP Phone 7921 QoS Configuration

The Cisco Unified Wireless IP Phone 7921 supports the following QoS related protocols and standards;

- IEEE 802.11e/Wi-Fi Multimedia (WMM)
- Traffic Specification (TSPEC)
- Enhanced Distributed Channel Access (EDCA)
- QoS Basic Service Set (QBSS)
- Unscheduled automatic power-save delivery (U-APSD)
- Power-save mode

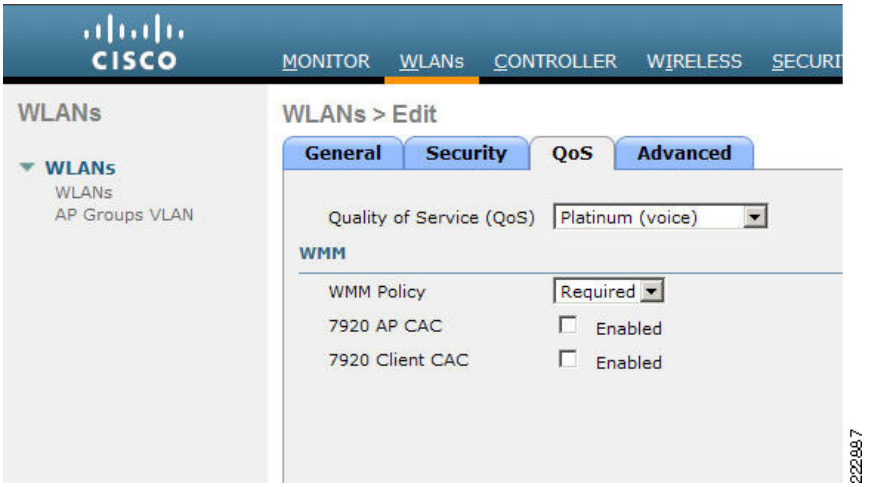
All of these features are enabled by default on the phone and will be used if enabled on the AP to which the phone associates. The QoS chapter provides more details about each of these.

Cisco WLC QoS configuration

A dedicated voice VLAN should be defined on the controller for all VoIP handsets including the Cisco Unified Wireless IP Phone 7921. The voice VLAN should be configured for the highest possible QoS by editing the VLAN and selecting the QoS tab.

As shown in Figure 10-29, in the *Quality of Service (QoS)* drop-down box *Platinum (voice)* should be selected. If only WMM-capable voice handsets, such as the Cisco Unified Wireless IP Phone 7921, are to be deployed, then the *WMM Policy* drop-down box should be set to *Required*. If there will be a mix of Cisco Unified Wireless IP Phone 7921 and nonWMM-capable devices, such as the Cisco Unified Wireless IP Phone 7920, then the WMM policy should be set to *Optional*.

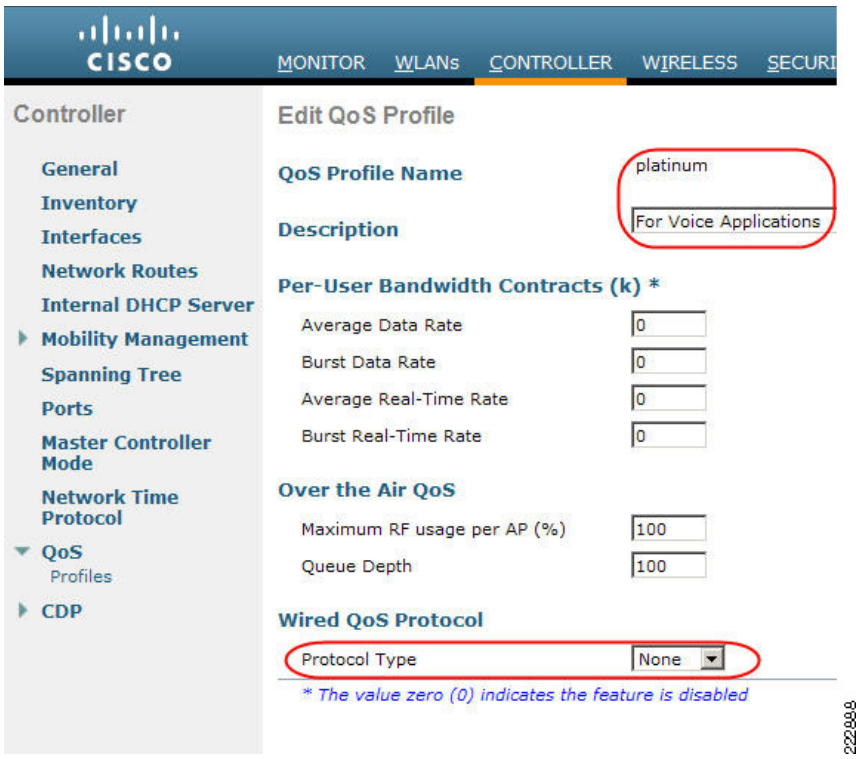
Figure 10-29 Cisco WLC WLAN QoS Policy Options



For each of the four QoS Profiles (*Bronze*, *Silver*, *Gold*, and *Platinum*) that can be selected for a given WLAN, there is a controller-wide option to change the characteristics of that profile.

Figure 10-30 shows an example of a *QoS Profile* edit screen. In most deployments, these settings should not be changed and the default configuration shown here should be used. More information on these options is available in the Chapter 2, "WLAN Quality of Service."

Figure 10-30 Cisco WLC Edit QoS Profile

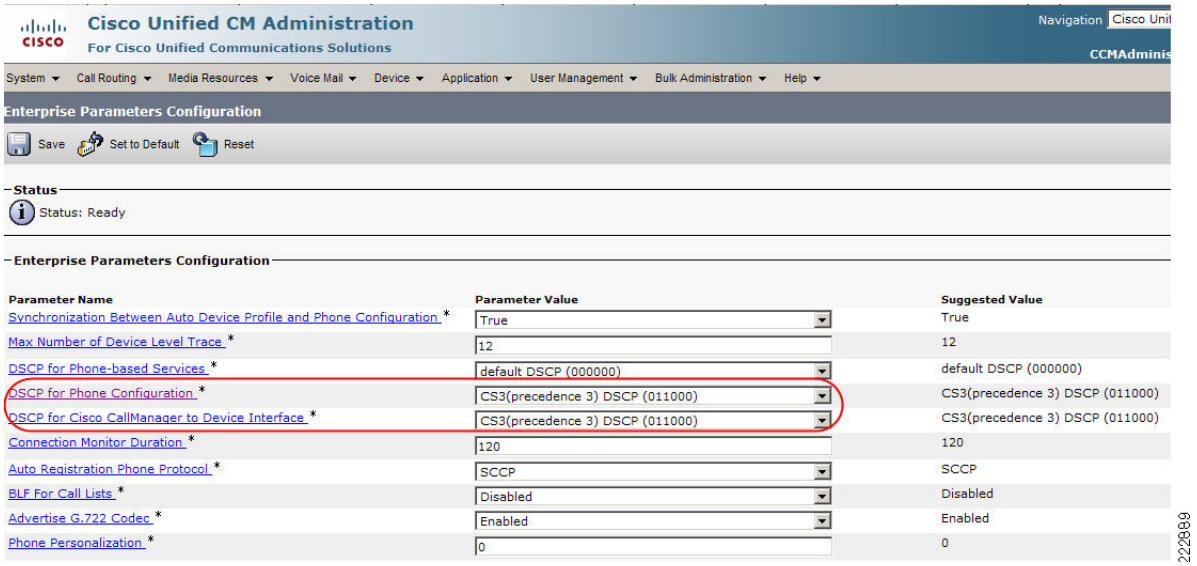


Cisco Unified Communications Manager QoS Configuration

The default Cisco Unified Communications Manager configuration contains the recommended values for Cisco Unified Communications Manager voice signaling QoS. The following relevant settings are shown in Figure 10-31 and are appropriate for most deployments:

- *DSCP for Phone Configuration*—This parameter specifies the Differentiated Service Code Point (DSCP) IP classification for any phone configuration, including any TFTP, DNS, or DHCP access necessary for phone configuration.
- *DSCP for Cisco Unified Communications Manager to Device Interface*—This parameter specifies the DSCP IP classification for protocol control interfaces used in Cisco Unified Communications Manager-to-device communications.

Figure 10-31 Cisco Unified Communications Manager QoS Parameters



Infrastructure QoS Configuration

This section shows sample QoS configurations for switch interfaces used in the campus network. More configuration details for all the switches and routers used in this design guide is available in the Appendix , "Voice over WLAN Campus Test Architecture," testing section of this guide.

Table 10-2 shows interface commands on a Cisco 3750G access-layer switch used to connect an IP Phone. The Auto-QoS configuration statement is shown in red and the statements generated by Auto-QoS follow it.

Table 10-2 Cisco 3750G—Wired IP Phone Port Configuration

Commands	Comments
`interface GigabitEthernet2/0/3` `description IP phone 7960`	Interface configuration mode and description.
`switchport access vlan 50` `switchport mode access`	Define access VLAN for data VLAN.

Table 10-2 Cisco 3750G—Wired IP Phone Port Configuration (continued)

Commands	Comments
`switchport voice vlan 51`	Define Voice VLAN.

`switchport port-security maximum 2`
`switchport port-security`
`switchport port-security aging time 2`
`switchport port-security violation restrict`
`switchport port-security aging type inactivity`
	Define Port Security features.

`spanning-tree portfast`	Spanning tree port configuration.
`auto qos voip cisco-phone`	Auto-QoS statement entered on all voice ports

`srr-queue bandwidth share 10 10 60 20`
`srr-queue bandwidth shape 10 0 0 0`
`queue-set 2`
`mls qos trust device cisco-phone`
`mls qos trust cos`
	Platform-specific QoS statements generated by the Auto-QoS statement that is in red in the preceding line.

Table 10-3 shows interface commands on a Cisco 4503 access-layer switch used to connect an AP. The Auto-QoS configuration statement is shown in red and the statements generated by Auto-QoS follow it.

Table 10-3 Cisco 4503—AP Port

Commands	Comments
`interface FastEthernet2/16` `description ports connected to APs in Isolation Boxes`	Interface configuration mode and description.
`switchport access vlan 48` `switchport mode access`	Define access VLAN for data VLAN all APs go on the access VLAN.
`auto qos voip trust`	Auto-QoS statement entered on all AP ports.
`qos trust dscp` **Note**—The **mls qos trust dscp** command is the equivalent command format for a 3750 switch.	The Auto-QoS statement above sets the switch port to trust Layer-2 CoS. For nonrouted ports, the CoS value of the incoming packet is trusted. For routed ports, the DSCP value of the incoming packet is trusted. This **qos trust dscp** command overrides that and sets the port to trust Layer-3 DSCP instead. The link between the AP and the switch port is not trunked and does not mark Layer-2 CoS.

`tx-queue 3`
`bandwidth percent 33`
`priority high`
`shape percent 33`
`service-policy output autoqos-voip-policy`
	Platform-specific QoS statements generated by the Auto-QoS statement shown in red in preceding line.

Table 10-4 shows interface commands on a Cisco 4503 access-layer switch used as an uplink port to a distribution-layer switch. The Auto-QoS configuration statement is shown in red and the statements generated by Auto QoS follow it.

Table 10-4 Cisco 4503 Uplink Port to Distribution Layer

Commands	Comments
`interface TenGigabitEthernet1/1` `description A4L to D3L`	Interface configuration mode and description.

`no switchport`
`ip address 10.33.3.10 255.255.255.252`
`ip hello-interval eigrp 100 1`
`ip hold-time eigrp 100 3`
`ip authentication mode eigrp 100 md5`
`ip authentication key-chain eigrp 100`
`eigrp-chain`
`ip pim sparse-mode`
`logging event link-status`
`load-interval 30`
`carrier-delay msec 0`
	Interface configuration unrelated to QoS.

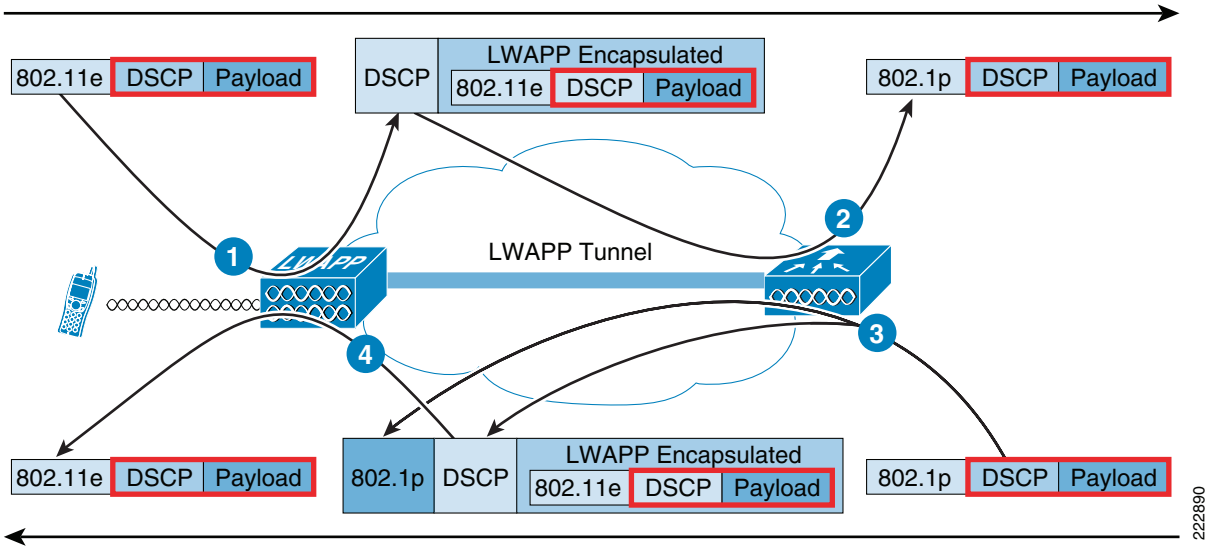
`auto qos voip trust`	

`qos trust dscp`
`tx-queue 3`
`bandwidth percent 33`
`priority high`
`shape percent 33`
`service-policy output autoqos-voip-policy`
	Platform-specific QoS statements generated by the Auto-QoS statement that is in red in the line above
	Note—Because this is a Layer-3 port, the **auto qos voip trust** command sets **qos trust dscp** not **qos trust cos** as it did in Table 10-3.

End-to-End QoS Mapping

In the centralized WLAN architecture, WLAN data is tunneled between the AP and the wireless LAN controller via LWAPP. In order to maintain the original QoS classification across this tunnel, the QoS settings of the encapsulated data packet must be appropriately mapped to the Layer 2 (IEEE 802.1p) and Layer 3 (IP DSCP) fields of the outer tunnel packet. See Figure 10-32.

Figure 10-32 End-to-end QoS Packet Marking Mappings



The original IP packet DSCP and user-data—sent by the WLAN client to the AP or received by the controller from the wired network infrastructure—are transmitted unaltered across the LWAPP tunnel between the AP and the controller. The Layer-2 and Layer-3 QoS markings are only changed on the headers that encapsulate the original IP packet. Table 10-5 provides additional marker mapping elaboration for the numbered labels in Figure 10-32.

Table 10-5 End-to-end QoS Packet Marking Mappings

Label Number[1]	From	To	Outbound UP (IEEE 802.1p/IEEE 802.11e) Mapping	Outbound IP DSCP Mapping
1	AP	Controller	N/A (APs do not support IEEE 802.1Q / IEEE 802.1p tags on the wired interface).	*WMM Client (such as Cisco Unified Wireless IP Phone 7921)*—Police the IEEE 802.11e UP value to ensure it does not exceed the maximum value allowed for the QoS policy assigned to that client; translate the value to the DSCP value. *Regular Client*—Use the IEEE 802.11e UP value for the QoS policy assigned to that client's WLAN; translate the value to the DSCP value.
2	Controller	Ethernet Switch	Translate the DSCP value of the incoming LWAPP packet to the IEEE 802.1p UP value. **Note**—The AP has policed the upstream DSCP (when it mapped from IEEE 802.1p UP to DSCP)	N/A (The original/encapsulated DSCP value is preserved) **Note**—The DSCP is un-policed; it is whatever was set by the WLAN client.
3	Controller	AP	Translate the DSCP value of the incoming packet to the Cisco Architecture for Voice, Video and Integrated Data (AVVID) IEEE 802.1p UP value. **Note**—The QoS profile is used to police the maximum IEEE 802.1p value that can be set	Copy the DSCP value from the incoming packet. **Note**—No policing is performed here; it is assumed that traffic was policed at ingress to the network.
4	AP	Wireless Client	*WMM Client (such as Cisco Unified Wireless IP Phone 7921)*—Translate the DSCP value of the incoming LWAPP packet to the IEEE 802.11e UP value. Police the value to ensure it does not exceed the maximum value allowed for the WLAN QoS policy assigned to the WLAN the client belongs to. Place packet in the IEEE 802.11 Tx queue appropriate for the UP value. *Regular Client*—Place packet in the default IEEE 802.11 Tx queue for the WLAN QoS policy assigned to that client.	N/A (original/encapsulated DSCP value is preserved).

1. Refer to Figure 10-32.

Table 10-6 provides the translations that occur between IEEE 802.11e/IEEE 802.1p UP values and IP DSCP values. Because Cisco AVVID defines the translation from IEEE 802.1 UP to IP DSCP, and the IEEE defines the translation from IP DSCP to IEEE 802.11e UP, two different sets of translations must be used.

Table 10-6 QoS Packet Marking Translations

Cisco AVVID IEEE 802.1p UP-Based Traffic Type	Cisco AVVID IP DSCP	Cisco AVVID IEEE 802.1p UP	IEEE 802.11e UP	Notes
Network Control	–	7	–	Reserved for network control only
Inter-Network Control	48	6	7 (AC_VO)	LWAPP control
Voice	46 (EF)	5	6 (AC_VO)	*Controller*—Platinum QoS profile
Video	34 (AF41)	4	5 (AC_VI)	*Controller*—Gold QoS profile
Voice Control	26 (AF31)	3	4 (AC_VI)	–
Best Effort	0 (BE)	0	3 (AC_BE) 0 (AC_BE)	*Controller*— Silver QoS profile –
Transaction Data	18 (AF21)	2	2 (AC_BK)	–
Bulk Data	10 (AF11)	1	1 (AC_BK)	*Controller*— Bronze QoS profile.

Cisco Unified Wireless IP Phone 7921 Troubleshooting

This section will focus on troubleshooting that is specific to the Cisco Unified Wireless IP Phone 7921G. For additional troubleshooting information, refer to Chapter 9, "Voice over WLAN Troubleshooting and Management Tools."

Configuration Checklist

When configuring your wireless LAN controller, use the following guidelines:

Step 1 Set the QoS policy to *Platinum*.

Step 2 Enable WMM to enable QoS and the ability to use U-APSD.

Step 3 Disable DHCP address assignment required.

Step 4 Ensure *Aggressive Load Balancing* is disabled.

Step 5 If you have clients from other regions that will attempt to associate with the WLAN, enable World Mode (IEEE 802.11d).

Verify Coverage with Cisco Unified Wireless IP Phone 7921G

Chapter 9, "Voice over WLAN Troubleshooting and Management Tools," covers the management of the RF deployment using the Cisco WCS, Cisco WLC, as well as using third-party site-survey and WLAN analysis tools. This section describes how the Cisco Unified Wireless IP Phone 7921G can be used to validate the RF design provided by those tools.

Wireless LAN performance varies from client device to client device. A client with a strong transmit signal and a high receiver sensitivity will perform better in marginal WLAN coverage than a client with weaker radio characteristics. For this reason, it is recommended that WLAN coverage is validated with the actual device you intend to use (in addition to using professional site survey tools such as *AirMagnet Survey* and *Cisco Cisco Spectrum Expert Analysis*).

After the initial deployment of wireless phones in the WLAN, it is a good practice to perform site surveys at regular intervals to verify that the APs are providing adequate coverage and that wireless phones can roam from one AP to another without audio problems. You should use the Cisco Unified Wireless IP Phone 7921G to verify that the signal range and transmission power provide adequate coverage for roaming phones.

Access the *Site Survey* menu on the phone by pressing **Settings** > **Status** > **Site Survey**

Note When not in a call, the Cisco Unified Wireless IP Phone 7921G only scans other non-associated channels when the current signal lowers to a certain threshold, so you might see the AP with which it is associated in the list. To see all APs, place a call from the Cisco Unified Wireless IP Phone 7921G to a wired IP phone where scanning occurs constantly while the phone call is active.

Figure 10-33 shows an example display output from a Cisco Unified Wireless IP Phone 7921.

Figure 10-33 Cisco Unified Wireless IP Phone 7921 Site Survey Screen Capture

Cisco Unified Wireless IP Phone 7921 coverage statistics can also be viewed by using Telnet to connect to the Cisco Unified Wireless IP Phone 7921.

Cisco Unified Wireless IP Phone 7921 Web Page Access

You can access the web page for any Cisco Unified Wireless IP Phone 7921G that is connected to the WLAN. Be sure the phone is powered on and connected. To access the web page for the Cisco Unified Wireless IP Phone 7921G follow these steps:

- Enabling or Disabling IP Phone Web Access from Cisco Unified Communications Manager, page 10-35
- Access the Cisco Unified Wireless IP Phone 7921s Web Pages, page 10-35

These procedure are summarized in the brief sections that follow.

Enabling or Disabling IP Phone Web Access from Cisco Unified Communications Manager

Web access for IP phones is enabled by default on Cisco Unified Communications Manager. The following steps are required to disable or re-enable web access.

Step 1 Navigate to the *Phone Configuration* web page in Cisco Unified Communications Manager Administration and set the *Web Access* field to *Read Only* or *Disabled*.

Step 2 Reset the phone from Cisco Unified Communications Manager to implement the change in web access policy.

Access the Cisco Unified Wireless IP Phone 7921s Web Pages

Step 1 Obtain the IP address of the Cisco Unified Wireless IP Phone 7921G using one of these methods:

a. Search for the phone in Cisco Unified Communications Manager by choosing *Devices* > *Phones*. Phones registered with Cisco Unified Communications Manager display the IP address on the *Find* and *List Phones* web page and at the top of the *Phone Configuration* web page.

b. On the Cisco Unified Wireless IP Phone 7921G, press **Settings** > **Device Information** > **Network Configuration** and then scroll to the *IP Address* option.

Step 2 Open a web browser and enter the following URL, where *IP_address* is the IP address of the Cisco Unified IP Phone: **https://***IP-address*

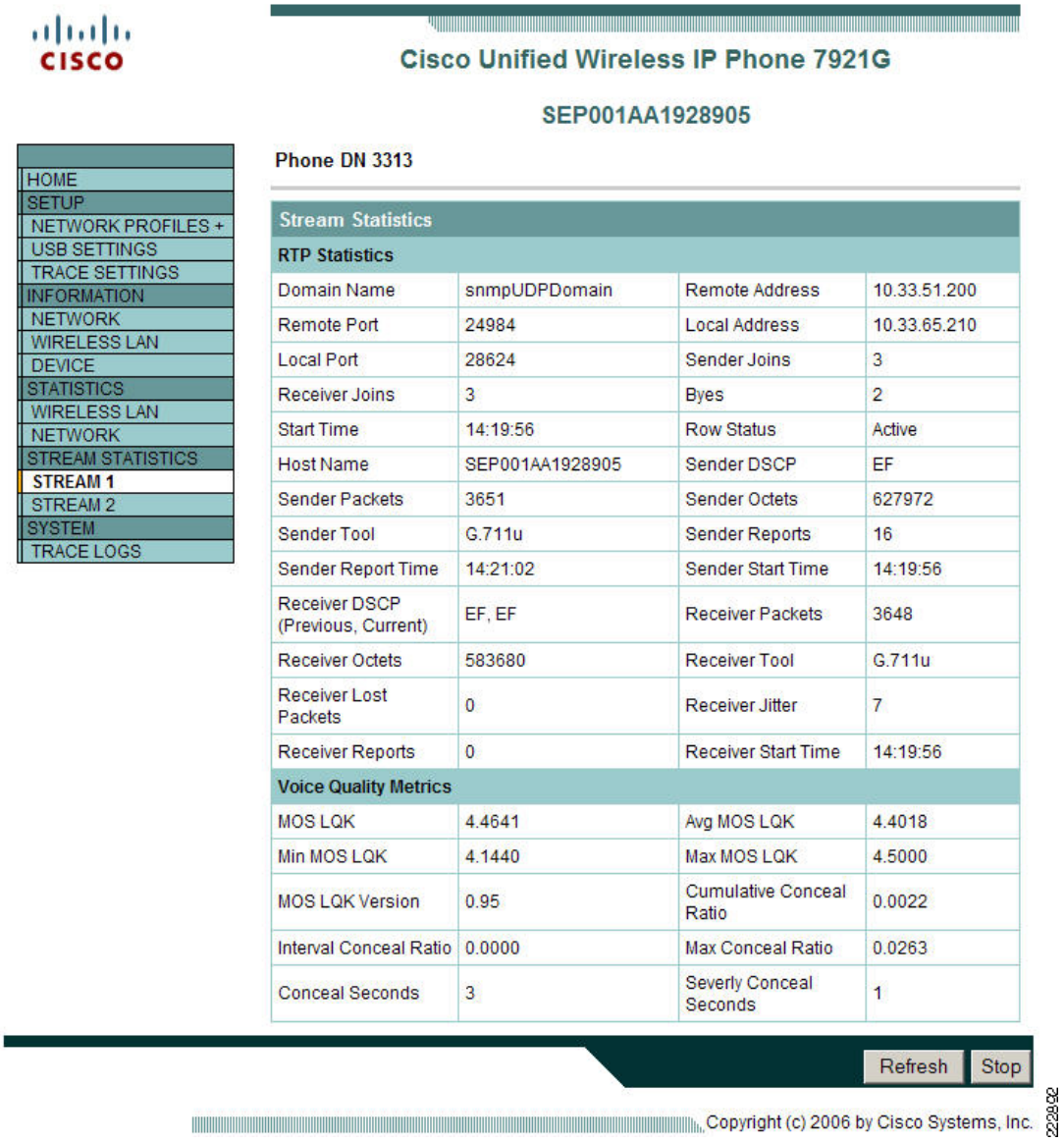
Note When the *Security Alert* dialog box displays a notice to accept the Trust Certificate, click **Yes** or **Always** to accept the application.

Step 3 Log in to the web pages with the username *admin* and enter the password *Cisco* for the phone web pages.

Step 4 View the informational pages and changes to configurable pages as needed.

Figure 10-34 provides an example display showing some of the information that is available from the Cisco Unified Wireless IP Phone 7921 web pages.

Figure 10-34 Cisco Unified Wireless IP Phone 7921 Stream Statistics



References

Please see the following publications for additional information:

- *Cisco Unified Wireless IP Phone 7921G Adminstration Guide*
  http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7921g/5_0_1/english/administration/guide/21adm501.html

- *Wireless LAN Controller Documentation*
  http://www.cisco.com/en/US/products/ps6366/products_installation_and_configuration_guides_list.html
- *Cisco Wireless Control System Configuration Guide*
  http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html