



# Cisco Unified Wireless IP Phone 7921G Deployment Guide



The Cisco Unified Wireless IP Phone 7921G is adaptable for all mobile professionals, from users on the move within an office environment to nurses and doctors in a healthcare environment to associates working in the warehouse, on the sales floor, or in a call center. Staff, nurses, doctors, educators, and IT personnel can be easily reached when mobile.

This guide provides information and guidance to help the network administrator deploy these phones in a wireless LAN environment.

## Revision History

Date	Comments
02/28/2007	Initial Version
3/16/2008	1.0(5) Update
10/13/2008	1.1(1) and 1.2(1) Updates

# Table of Contents

<b>Requirements for the Cisco Unified Wireless IP Phone 7921G .....</b>	<b>5</b>
<i>Site Survey .....</i>	<i>5</i>
<i>Call Control.....</i>	<i>5</i>
<i>Supported Protocols .....</i>	<i>5</i>
<i>Supported Access Points.....</i>	<i>6</i>
<b>Phone Models and Localization .....</b>	<b>7</b>
<i>Phone Models .....</i>	<i>7</i>
World Mode (802.11d) .....	8
<i>Supported Countries .....</i>	<i>8</i>
<i>Language Support.....</i>	<i>9</i>
<b>Radio Characteristics .....</b>	<b>9</b>
<b>Wireless Security.....</b>	<b>10</b>
<i>Cisco Centralized Key Management (CCKM).....</i>	<i>10</i>
<i>Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling (EAP-FAST).....</i>	<i>10</i>
<i>Extensible Authentication Protocol – Transport Layer Security (EAP-TLS).....</i>	<i>11</i>
<i>Protected Extensible Authentication Protocol (PEAP).....</i>	<i>13</i>
<b>Voice Security.....</b>	<b>14</b>
<b>Power Management .....</b>	<b>15</b>
<i>Protocols.....</i>	<i>15</i>
Unscheduled Auto Power Save Delivery (U-APSD).....	15
Power Save Poll (PS-POLL).....	16
Active Mode .....	16
<i>Delivery Traffic Indicator Message (DTIM).....</i>	<i>16</i>
<i>Scan Modes.....</i>	<i>16</i>
<b>Quality of Service (QoS) .....</b>	<b>17</b>
<i>Configuring QoS in Cisco Unified Communications Manager.....</i>	<i>17</i>
<i>Configuring QoS Policies for the Network .....</i>	<i>17</i>
Configuring Cisco IOS Access Points .....	17
Configuring Cisco Switch Ports .....	18
Configuring Switch Ports for Wired IP Phones .....	18
Sample Voice Packet Capture.....	19
<i>Call Admission Control .....</i>	<i>19</i>
Pre-Call Admission Control.....	20
Roaming Admission Control .....	20
<i>Traffic Classification (TCLAS).....</i>	<i>21</i>
<b>Multicast .....</b>	<b>22</b>
<b>Designing the Wireless LAN for Voice.....</b>	<b>22</b>
<i>Configuring Data Rates.....</i>	<i>23</i>

Call Capacity .....	23
Dynamic Transmit Power Control (DTPC).....	24
Planning Channel Usage.....	24
5 GHz (802.11a) .....	24
Using Dynamic Frequency Selection (DFS) on Access Points .....	25
2.4 GHz (802.11b/g).....	26
Signal Strength and Coverage.....	27
Multipath.....	29
Verification with Site Survey Tools.....	30
Cisco 7921G Neighbor List.....	30
Cisco 7921G Site Survey.....	30
<b>Configuring Cisco Unified Communications Manager.....</b>	<b>32</b>
Phone Button Templates .....	32
Softkey Templates .....	32
Security Profiles.....	32
G.722 Advertisement.....	33
Product Specific Configuration Options.....	33
<b>Configuring the Cisco Unified Wireless LAN Controller and Access Points.....</b>	<b>37</b>
SSID / WLAN Settings.....	37
Controller Settings.....	39
802.11 Network Settings .....	41
Auto RF .....	41
DFS (802.11h) .....	43
Call Admission Control Settings.....	44
Configuring QoS Basic Service Set (QBSS).....	46
Setting the Controller 802.1x Timeout.....	47
Configuring Proxy ARP.....	48
Configuring TKIP Countermeasure Holdoff Time.....	48
VLANs and Autonomous Access Points .....	49
<b>Configuring the Cisco Unified Wireless IP Phone 7921G .....</b>	<b>49</b>
Configuring the Network Profile Parameters.....	50
Installing Certificates .....	55
Using Templates to Configure Phones.....	60
Upgrading Phone Firmware.....	60
Wavelink Avalanche.....	61
Using the 7921 Configuration Utility for Quick Deployment .....	68
Configuring the Local Phone Book and Speed Dials.....	69
<b>Troubleshooting .....</b>	<b>71</b>
Stream Statistics.....	71
Network Statistics .....	73
Wireless LAN Statistics.....	74

<i>Traffic Stream Metrics (TSM)</i> .....	74
<i>Phone Logs</i> .....	75
Trace Modules .....	76
Trace Levels .....	77
<i>Restoring Factory Defaults</i> .....	77
<b>Healthcare Environments</b> .....	<b>77</b>
<b>Cleaning the Phone</b> .....	<b>77</b>
<b>Phone Accessories</b> .....	<b>77</b>
<b>Additional Documentation</b> .....	<b>79</b>

# Requirements for the Cisco Unified Wireless IP Phone 7921G

The Cisco Unified Wireless IP Phone 7921G is an IEEE 802.11a/b/g wireless IP phone that provides voice communications in conjunction with these components. Check that your wireless LAN meets the requirements to support the specifications for these phones:

## Site Survey

Before deploying the Cisco Unified Wireless IP Phone 7925G into a production environment, a site survey must be completed by a Cisco certified partner with the advanced wireless LAN specialization. During the site survey the RF spectrum can be analyzed to determine which channels are usable in the desired band (2.4 GHz or 5 GHz). Typically there is less interference in the 5 GHz band as well as more non-overlapping channels, so 5 GHz is the preferred band for operation. The site survey will include heatmaps showing the intended coverage plan for the location. The site survey will also determine which access point platform type, antenna type, access point configuration (channel and transmit power) to use at the location. See the “[Designing the Wireless LAN for Voice](#)” section for more information.

## Call Control

For call control, the Cisco Unified Wireless IP Phone 7921G supports only Skinny Client Control Protocol (SCCP) on the following applications:

- Cisco Unified Communications Manager 4.1, 4.2, 4.3, 5.0, 5.1, 6.0, 6.1, 7.0 and later
- Cisco Unified Communications Manager Express 4.1, 4.2, 4.3 and later (Minimum of 12.4(15)T7)
- SRST 4.1, 4.2, 4.3 and later (Minimum of 12.4(15)T7)

## Device Support in Cisco Unified Communications Manager

Cisco Unified Communications Manager requires that you install a device package or service release update in order to enable Cisco Unified Wireless IP Phone 7921G device support.

Cisco Unified Communications Manager 5.0(4) or higher requires signed COP files.

Device packages for Cisco Unified Communications Manager are available at <http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml>.

## Supported Protocols

Supported voice and wireless LAN protocols include these:

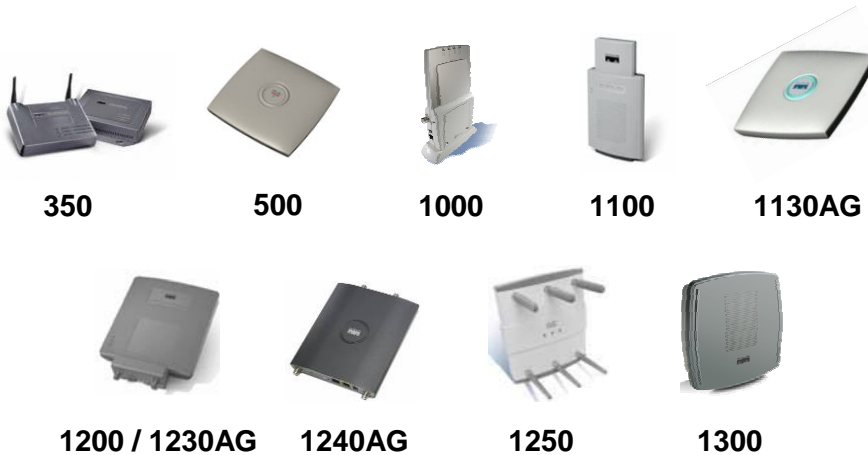
- Real Time Protocol (RTP)
- G.711u-law, G.711a-law, G.729a, G.729ab, G.722, iLBC
- Real Time Control Protocol (RTCP)
- Cisco Discovery Protocol (CDP)
- Syslog
- CCX v4
- Wi-Fi MultiMedia (WMM) and Traffic Specification (TSPEC)
- Unscheduled Auto Power Save Delivery (U-APSD) and Power Save Poll (PS-POLL)

## Supported Access Points

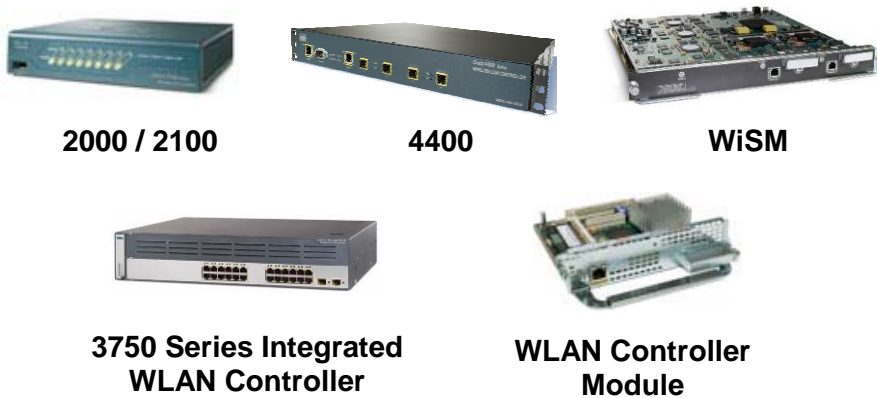
The Cisco Unified Wireless IP Phone 7921G is supported on both the Cisco autonomous and unified solutions.

- Cisco Unified Wireless LAN Controller  
Minimum = 4.0.217.0 or later  
Recommended = 5.1.151.0 or later
- Cisco IOS Access Points (Autonomous)  
Minimum = 12.3(8)JEA or later  
Recommended = 12.4(3g)JA1 or later (does not apply to 350, 1100, 1200, 1230)

### Cisco Access Points



### Wireless LAN Controllers



**Note:** VoWLAN is not currently supported in conjunction with MESH technology (1500).

The table below lists the modes that are supported by each Cisco access point.

Cisco Series	802.11b	802.11g	802.11a	Autonomous	Unified
350	Yes	No	No	Yes	No
500	Yes	Yes	No	Yes	Yes

<b>1000</b>	Yes	Yes	Yes	No	Yes
<b>1100</b>	Yes	Yes	No	Yes	Yes
<b>1130AG</b>	Yes	Yes	Yes	Yes	Yes
<b>1200</b>	Yes	Yes	Optional	Yes	Yes
<b>1230AG</b>	Yes	Yes	Yes	Yes	Yes
<b>1240AG</b>	Yes	Yes	Yes	Yes	Yes
<b>1250</b>	Yes	Yes	Yes	Yes	Yes
<b>1300</b>	Yes	Yes	No	Yes	Yes

## Phone Models and Localization

### Phone Models

Cisco manufactures four Cisco Unified Wireless IP Phone 7921G models that support the following domains. On the phone, you can identify its domain by pressing **Settings > Model Information > WLAN Regulatory Domain** and referencing the Regulatory Domain number in this list:

Use this table to identify specific phone versions that support these regulatory domains for use around the world:

<b>Regulatory Domain</b>	<b>Part Number</b>	<b>Regulatory Domain Number</b>	<b>Band Range</b>	<b>Available Channels</b>	<b>5 GHz Channel Set</b>
FCC (Americas)	CP-7921G-A-K9	1050	2.412–2.462 GHz 5.15–5.25 GHz 5.25–5.35 GHz 5.47–5.725 GHz 5.725–5.825 GHz	11 4 4 8 4	UNII-1 UNII-2 UNII-2 Extended UNII-3
ETSI (Europe)	CP-7921G-E-K9	3051	2.412–2.472 GHz 5.15–5.725 GHz	13 19	
Japan	CP-7921G-J-K9	4157	2.412–2.472 GHz 2.412–2.484 GHz 5.15–5.35 GHz	13 (OFDM) 14 (CCK) 8	
Rest of World	CP-7921G-W-K9	5252	Uses 802.11d to identify available channels and transmit powers		

## World Mode (802.11d)

If using the Cisco Unified Wireless IP Phone 7921G World (-W) model, then you must enable 802.11d. The Cisco Unified Wireless IP Phone 7921G gives precedence to 802.11d to determine the channels and transmit powers to use and inherits its client configuration from the associated access point.

Enable World Mode (802.11d) for the corresponding country where the access point is located.

If 802.11d information is not available from the access point, then the phone uses the locally configured regulatory domain. If the Cisco Unified Wireless IP Phone 7921G -A, -E or -P model is taken to another country, where the access point uses a different regulatory domain, then 802.11d will be required for the Cisco Unified Wireless IP Phone 7921G to operate successfully.

When using 802.11a, you can enable 802.11d to discover which channels are used in the network. Specifically, for 802.11h support, the phone passively scans some of the 5 GHz channels (DFS) first before actively scanning any network channels.

The supported countries where the Cisco Unified Wireless IP Phone 7921G is allowed to operate are listed below:

**Note:** World Mode is enabled automatically for the Cisco Unified Wireless LAN Controller.

World Mode must be enabled manually for Cisco Autonomous Access Points using the following commands:

```
Interface dot11radio X
world-mode dot11d country US both
```

## Supported Countries

Below are the countries and their 802.11d codes that are supported by the Cisco Unified Wireless IP Phone 7921G.

Argentina (AR)	Iceland (IS)	Phillipines (PH)
Australia (AU)	India (IN)	Poland (PL)
Austria (AT)	Indonesia (ID)	Portugal (PT)
Belgium (BE)	Ireland (IE)	Puerto Rico (PR)
Brazil (BR)	Israel (IL)	Romania (RO)
Bulgaria (BG)	Italy (IT)	Russian Federation (RU)
Canada (CA)	Japan (JP)	Saudi Arabia (SA)
Chile (CL)	Korea (KR / KP)	Singapore (SG)
Colombia (CO)	Latvia (LV)	Slovakia (SK)
Costa Rica (CR)	Liechtenstein (LI)	Slovenia (SI)
Cyprus (CY)	Lithuania (LT)	South Africa (ZA)
Czech Republic (CZ)	Luxembourg (LU)	Spain (ES)
Denmark (DK)	Malaysia (MY)	Sweden (SE)
Estonia (EE)	Malta (MT)	Switzerland (CH)
Finland (FI)	Mexico (MX)	Taiwan (TW)
France (FR)	Monaco (MC)	Thailand (TH)
Germany (DE)	Netherlands (NL)	Turkey (TR)
Gibraltar (GI)	New Zealand (NZ)	Ukraine (UA)
Greece (GR)	Norway (NO)	United Kingdom (GB)
Hong Kong (HK)	Panama (PA)	United States (US)
Hungary (HU)	Peru (PE)	Venezuela (VE)



**Note:** Compliance information is available on the Cisco Product Approval Status web site at the following URL:  
[http://tools.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL\\_SEARCH](http://tools.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH)

## Language Support

The Cisco Unified Wireless IP Phone 7921G currently supports the following languages.

Bulgarian	English	Japanese	Serbian
Catalan	Finnish	Korean	Slovak
Chinese	French	Norwegian	Slovenian
Croatian	German	Polish	Spanish
Czech	Greek	Portuguese	Swedish
Danish	Hungarian	Romanian	
Dutch	Italian	Russian	

The corresponding locale package must be installed to enable support for that language. English is the default language on the phone.

Download the locale packages from the Localization page at the following URL:

<http://www.cisco.com/kobayashi/sw-center/telephony/callmgr/locale-installer.shtml>

## Radio Characteristics

Use this table to see the data rates, ranges, and receiver sensitivities for Cisco Unified Wireless IP Phone 7921G depending on the Wi-Fi standard in use.

<b>802.11a</b>	<b>Data Rate</b>	<b>Range</b>	<b>Receiver Sensitivity</b>
Max Tx Power is 16 dBm	6 Mbps	610 ft (186 m)	-89 dBm
	9 Mbps	610 ft (186 m)	-88 dBm
	12 Mbps	558 ft (170 m)	-86 dBm
	18 Mbps	541 ft (165 m)	-85 dBm
	24 Mbps	508 ft (155 m)	-82 dBm
	36 Mbps	426 ft (130 m)	-80 dBm
	48 Mbps	328 ft (100 m)	-76 dBm
	54 Mbps	295 ft (90 m)	-74 dBm
<b>802.11g</b>	<b>Data Rate</b>	<b>Range</b>	<b>Receiver Sensitivity</b>
Max Tx Power is 16 dBm	6 Mbps	722 ft (220 m)	-90 dBm
	9 Mbps	656 ft (200 m)	-89 dBm
	12 Mbps	623 ft (190 m)	-87 dBm
	18 Mbps	623 ft (190 m)	-85 dBm
	24 Mbps	623 ft (190 m)	-82 dBm
	36 Mbps	492 ft (150 m)	-78 dBm
	48 Mbps	410 ft (125 m)	-74 dBm
	54 Mbps	394 ft (120 m)	-73 dBm

802.11b	Data Rate	Range	Receiver Sensitivity
Max Tx Power is 17 dBm	1 Mbps	1,027 ft (313 m)	-95 dBm
	2 Mbps	951 ft (290 m)	-89 dBm
	5.5 Mbps	853 ft (260 m)	-89 dBm
	11 Mbps	787 ft (240 m)	-85 dBm

**Note:** Receiver sensitivity is the minimum signal needed to decode a packet at a certain data rate.

See the “[Designing the Wireless LAN for Voice](#)” section for more information on signal requirements.

## Wireless Security

When deploying a wireless LAN, you must provide security. The Cisco Unified Wireless IP Phone 7921G supports the following wireless security features.

### Authentication

- Cisco Centralized Key Management (CCKM)
- 802.11i (802.1x authentication + TKIP encryption)
- 802.11i (802.1x authentication + AES encryption)
- 802.11i (Pre-Shared key + TKIP encryption)
- 802.11i (Pre-Shared key + AES encryption)
- Extensible Authentication Protocol – Flexible Authentication via Secure Tunneling (EAP-FAST)
- Extensible Authentication Protocol – Transport Layer Security (EAP-TLS)
- Protected Extensible Authentication Protocol (PEAP)
- Lightweight Extensible Authentication Protocol (LEAP)
- Open and Shared Key

### Encryption

- Advanced Encryption Scheme (AES)
- Temporal Key Integrity Protocol (TKIP) / Message Integrity Check (MIC)
- 40-bit and 128-bit Wired Equivalent Protocol (WEP)

## Cisco Centralized Key Management (CCKM)

When using 802.1x type authentication, you should implement CCKM for authentication. 802.1x can introduce delay during roaming due to its requirement for full re-authentication. CCKM centralizes the key management and reduces the number of key exchanges. Also, WPA introduces additional transient keys and can lengthen roaming time.

TKIP encryption is recommended when using CCKM for fast roaming as CCKM does not support AES currently.

## Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling (EAP-FAST)

This client server security architecture encrypts EAP transactions within a Transport Level Security (TLS) tunnel between the access point and the Remote Authentication Dial-in User Service (RADIUS) server such as the Cisco Access Control Server (ACS).

The TLS tunnel uses Protected Access Credentials (PACs) for authentication between the client (phone) and the RADIUS server. The server sends an Authority ID (AID) to the client (phone), which in turn selects the appropriate PAC. The client (phone) returns a PAC-Opaque to the RADIUS server. The server decrypts the PAC with its master-key. Both end points now have the PAC key and a TLS tunnel is created. EAP-FAST supports automatic PAC provisioning, but you must enable it on the RADIUS

To enable EAP-FAST, you must install a certificate.

The Cisco Unified Wireless IP Phone 7921G currently supports only automatic provisioning of the PAC, so enable “Anonymous In-Band PAC Provisioning” on the RADIUS server as shown below.

EAP-FAST requires that a user account be created on the authentication server.

The screenshot shows the Cisco System Configuration interface for EAP-FAST. The left sidebar contains navigation options like User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled 'EAP-FAST Configuration' and includes an 'Edit' button. The 'EAP-FAST Settings' window is open, showing various configuration options. Two red boxes highlight specific sections: the first box encloses the 'Allow anonymous in-band PAC provisioning' section, and the second box encloses the 'Allowed inner methods' section.

**EAP-FAST Configuration**

**EAP-FAST Settings**

**EAP-FAST**

- Allow EAP-FAST
- Active master key TTL: 1 months
- Retired master key TTL: 3 months
- Tunnel PAC TTL: 1 weeks
- Client initial message: [ ]
- Authority ID Info: sic21-21a-acs

**Provisioning Options (highlighted in red box):**

- Allow anonymous in-band PAC provisioning
- Allow authenticated in-band PAC provisioning
- Accept client on authenticated provisioning
- Require client certificate for provisioning
- Allow Machine Authentication

Machine PAC TTL: 1 weeks

Allow Stateless session resume

Authorization PAC TTL: 1 hours

**Allowed inner methods (highlighted in red box):**

- EAP-GTC
- EAP-MSCHAPv2
- EAP-TLS

Select one or more of the following EAP-TLS comparison methods:

- Certificate SAN comparison
- Certificate CN comparison
- Certificate Binary comparison

EAP-TLS session timeout (minutes): 120

EAP-FAST master server

Actual EAP-FAST server status: **Master**

## Extensible Authentication Protocol – Transport Layer Security (EAP-TLS)

Extensible Authentication Protocol Transport Layer Security (EAP-TLS) is using the TLS protocol with PKI to secure communications to the authentication server.

TLS provides a way to use certificates for both user and server authentication and for dynamic session key generation.

Either the internal Manufacturing Installed Certificate (MIC) or a user installed certificate can be used for authentication.

EAP-TLS provides excellent security, but requires client certificate management.

Ensure that “Certificate CN Comparison” is selected when enabling EAP-TLS.



## System Configuration

Edit

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

### Global Authentication Setup

#### EAP Configuration

##### PEAP

- Allow EAP-MSCHAPv2
- Allow EAP-GTC
- Allow Posture Validation

- Allow EAP-TLS

Select one or more of the following options:

- Certificate SAN comparison
- Certificate CN comparison
- Certificate Binary comparison

EAP-TLS session timeout (minutes):

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

##### EAP-FAST

[EAP-FAST Configuration](#)

##### EAP-TLS

- Allow EAP-TLS


Select one or more of the following options:

- Certificate SAN comparison
- Certificate CN comparison
- Certificate Binary comparison

EAP-TLS session timeout (minutes):

EAP-TLS also requires that a user account be created on the authentication server matching the common name of the certificate imported into the Cisco Unified Wireless IP Phone 7921G.

It is recommended to use a complex password for this user account.



# User Setup

Edt

**User: CP-7921G-0018BA78C222**

Account Disabled

**Supplementary User Info** ?

Real Name: Gillespie, Michael

Description:

**User Setup** ?

Password Authentication:

ACS Internal Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password: .....

Confirm Password: .....

Separate (CHAP/MS-CHAP/ARAP)

Password: .....

Confirm Password: .....

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

Default Group

Submit Delete Cancel

See the “[Installing Certificates](#)” section for more information.

## Protected Extensible Authentication Protocol (PEAP)

Protected Extensible Authentication Protocol (PEAP) uses server-side public key certificates to authenticate clients by creating an encrypted SSL/TLS tunnel between the client and the authentication server.

The ensuing exchange of authentication information is then encrypted and user credentials are safe from eavesdropping.

MS-CHAP v2 is the current supported inner authentication protocol (GTC is not supported).

**System Configuration**

**Global Authentication Setup**

**EAP Configuration**

**PEAP**

Allow EAP-MSCHAPv2

Allow EAP-GTC

Allow Posture Validation

---

Allow EAP-TLS

Select one or more of the following options:

Certificate SAN comparison

Certificate CN comparison

Certificate Binary comparison

EAP-TLS session timeout (minutes):

---

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

**EAP-FAST**

[EAP-FAST Configuration](#)

---

**EAP-TLS**

Allow EAP-TLS

Select one or more of the following options:

Certificate SAN comparison

Certificate CN comparison

Certificate Binary comparison

EAP-TLS session timeout (minutes):

PEAP (MS-CHAPv2) requires that a user account be created on the authentication server.

In release 1.2(1), the authentication server can be validated via importing a certificate into the Cisco Unified Wireless IP Phone 7921G.

See the “[Installing Certificates](#)” section for more information.

## Voice Security

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)
- Signaling encryption (TLS)
- Certificate authority proxy function (CAPF)

- Secure profiles
- Encrypted configuration files
- Settings Access (can limit user access to configuration menus)
- Locked network profiles
- Administrator password

## Power Management

The Cisco Unified Wireless IP Phone 7921G has an option for a standard or extended battery.

The standard battery can provide up to 150 hours standby time or up to 11.5 hours talk time.

The extended battery can provide up to 200 hours standby time or up to 15.5 hours talk time.

With firmware version 1.0(4) or later and when the access point supports the Cisco Client Extensions (CCX) proxy ARP information element, the idle battery life will be optimized.

When on call U-APSD, PS-POLL, or active mode can be utilized depending on the Cisco Unified Wireless IP Phone 7921G and Access Point configuration.

To extend on call battery life, the Cisco Unified Wireless IP Phone 7921G can use U-APSD or PS-POLL power save methods.

The Cisco Unified Wireless IP Phone 7921G will use either U-APSD or PS-POLL when in idle (no active phone call).

The table below lists the maximum on call and idle times for each 802.11 mode and battery type.

802.11 Mode	Call State	Standard Battery	Extended Battery
<u>2.4 GHz</u>	On Call	11.5	15.5
	Idle	150	200
<u>5 GHz</u>	On Call	11.5	15.5
	Idle	150	200

If the access point does not support CCX or proxy ARP is not enabled, then the idle battery life will be up to fifty percent less. See the "[Configuring Proxy ARP](#)" section for more information.

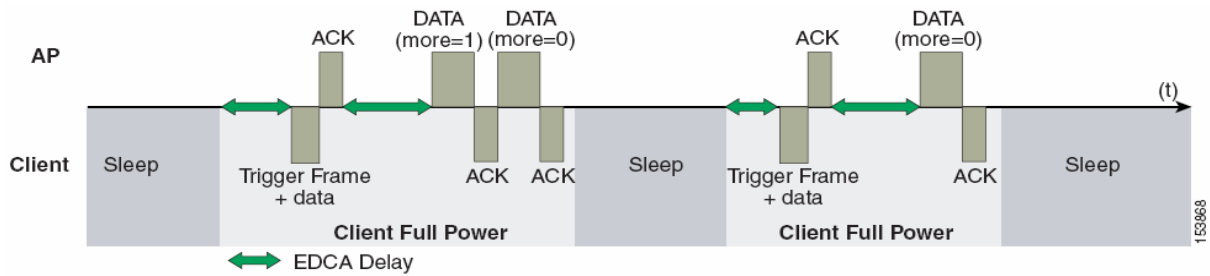
## Protocols

### Unscheduled Auto Power Save Delivery (U-APSD)

The Cisco Unified Wireless IP Phone 7921G will use U-APSD (Unscheduled Auto Power Save Delivery) for power save when in idle mode or when a phone call is active if WMM is enabled, where U-APSD is supported.

U-APSD helps optimize battery life.

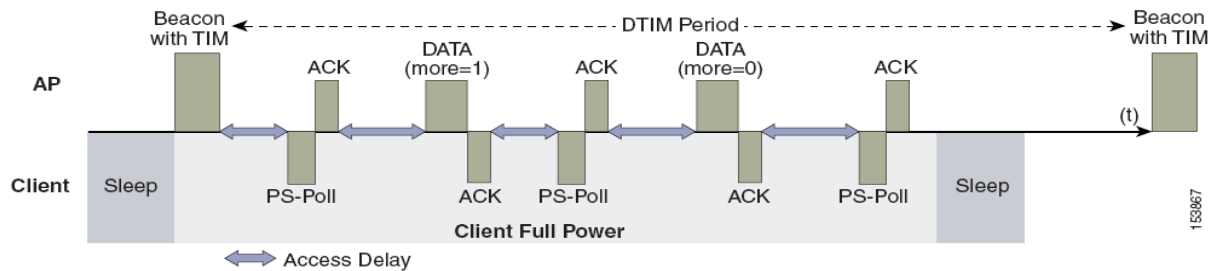
Below is a sample packet sequence when using U-APSD.



## Power Save Poll (PS-POLL)

If Wi-Fi MultiMedia (WMM) is disabled, which will disable U-APSD support, or U-APSD support is not available on the access point, then the Cisco Unified Wireless IP Phone 7921G will use PS-POLL for power save when in idle mode and when a phone call is active.

Below is a sample packet sequence when using PS-POLL.



## Active Mode

If the “Call Power Save Mode” is set to “None”, then the phone will use active mode and no power save will be used, which will reduce the battery life.

## Delivery Traffic Indicator Message (DTIM)

Increasing the DTIM period can also increase the battery life. The Cisco Unified Wireless IP Phone 7921G can use the DTIM period to schedule wakeup periods to check for broadcast and multicast packets as well as any unicast packets.

For optimal battery life and performance, we recommend setting the DTIM period to “2” with a beacon period of **100ms**.

The DTIM period is a tradeoff between battery life and multicast performance.

Broadcast and multicast traffic will be queued until the DTIM period when there are power save enabled clients associated to the access point, so DTIM will determine how quickly these packets can be delivered to the client. If using multicast applications, a shorter DTIM period can be used.

## Scan Modes

When using only one access point, select Single Access Point Mode on the phone to reduce scanning and optimize battery life for phones that do not roam.

When using multiple access points where roaming is required, “Single AP Mode” should not be enabled. Instead use the auto (default) or continuous scan mode, which will allow for seamless roaming.

Continuous scan mode can be optionally enabled to allow for better location tracking.



## Quality of Service (QoS)

Quality of Service enables queuing to ensure high priority for voice traffic. To implement appropriate queuing for voice traffic, use the following suggestions:

- Ensure that WMM is enabled on the access point.
- Create a QoS policy on the access point giving priority to voice (RTP) traffic and apply that profile to the desired interfaces.
  - RTP (DSCP = EF) to COS = 6
  - SCCP (DSCP = CS3) to COS = 4
- Be sure that RTP packets have the proper QoS markings and other protocols are not using the same QoS markings.
- Select the “Platinum” QoS profile for the voice wireless LAN when using Cisco Unified Wireless LAN Controller technology and set the 802.1p tag to “6”.
- Enable Differentiated Services Code Point (DSCP) preservation on the Cisco IOS switch and/or use a QoS policy to set DSCP to EF for RTP traffic (UDP port range 16384-32767) on the Cisco IOS router.

## Configuring QoS in Cisco Unified Communications Manager

The SCCP DSCP values are configured in the Cisco Unified Communications Manager enterprise parameters. Cisco Unified Communications Manager uses the default value of CS3 to have devices set the DSCP marking for SCCP packets as shown in the Enterprise Parameters Configuration page.

Parameter Name	Parameter Value	Suggested Value
<a href="#">Synchronization Between Auto Device Profile and Phone Configuration</a> *	True	True
<a href="#">Max Number of Device Level Trace</a> *	12	12
<a href="#">DSCP for Phone-based Services</a> *	default DSCP (000000)	default DSCP (000000)
<a href="#">DSCP for Phone Configuration</a> *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
<a href="#">DSCP for Cisco CallManager to Device Interface</a> *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
<a href="#">Connection Monitor Duration</a> *	120	120
<a href="#">Auto Registration Phone Protocol</a> *	SCCP	SCCP
<a href="#">BLF For Call Lists</a> *	Disabled	Disabled
<a href="#">Advertise G.722 Codec</a> *	Enabled	Enabled
<a href="#">Phone Personalization</a> *	0	0

## Configuring QoS Policies for the Network

Set up QoS policies and settings for the following network devices.

### Configuring Cisco IOS Access Points

You can use this QoS policy on the Cisco IOS access point (AP) to enable DSCP to COS mapping. This allows RTP packets to be placed into the voice queue, if those packets are marked correctly, when received at the access point level.

```
class-map match-all RTP
match ip dscp ef
class-map match-all SCCP
match ip dscp cs3
!
policy-map Voice
```

```
class RTP
  set cos 6
class SCCP
  set cos 4
!
interface X
  service-policy input Voice
  service-policy output Voice
```

## Configuring Cisco Switch Ports

Configure the Cisco access point switch ports and uplink switch ports for DSCP trust.

```
mls qos
!
interface X
  mls qos trust dscp
```

**Note:** When using the Cisco Unified Wireless LAN Controller utilizing LWAPP technology, DSCP trust must be implemented or trust the LWAPP UDP data ports (12222) on all interfaces where LWAPP packets will traverse to ensure QoS markings are correctly set.

## Configuring Switch Ports for Wired IP Phones

Enable the Cisco wired IP phone switch ports for Cisco phone trust

```
mls qos
!
Interface X
  mls qos trust device cisco-phone
  mls qos trust dscp
```

If DSCP markings are not preserved, then the below configuration can be used to set the DSCP based on the TCP or UDP port to map RTP and SCCP correctly.

Ensure the following QoS policy is not applied to an interface where LWAPP traffic traverses.

```
ip access-list extended SCCP
  permit tcp any eq 2000 any
  permit tcp any any eq 2000
!
ip access-list extended RTP
  permit udp any range 16384 32767 any
  permit udp any any range 16384 32767
!
class-map match-all SCCP
  match access-group name SCCP
class-map match-all RTP
  match access-group name RTP
```

```

!
policy-map Voice
class RTP
set dscp ef
!
class SCCP
set dscp cs3
!
interface X
service-policy input Voice
service-policy output Voice

```

## Sample Voice Packet Capture

This packet capture below shows that packets bound for the Cisco Unified Wireless IP Phone 7921G over the air are marked with DSCP = EF and COS = 6 for RTP packets.

The image shows a Wireshark packet capture analysis for a packet bound for a Cisco Unified Wireless IP Phone 7921G. The packet is identified as an 802.11 MAC Header. The QoS Control Field is highlighted with a red box, showing the following details:

- Version: 0
- Type: %10 Data
- Subtype: %1000 QoS Data
- Frame Control Flags: %00000010
  - 0... Non-strict order
  - .0... Non-Protected Frame
  - .0... No More Data
  - ...0... Power Management - active mode
  - ...0... This is not a Re-Transmission
  - ...0... Last or Unfragmented Frame
  - ...1... Exit from the Distribution System
  - ...0... Not to the Distribution System
- Duration: 44 Microseconds
- Destination: 00:18:BA:78:C2:22 7921G
- BSSID: 00:13:5F:FA:25:1F AP
- Source: 00:1D:A2:1A:24:D7
- Seq Number: 3744
- Frag Number: 0
- QoS Control Field: %0000000000010110
  - ..... AP PS Buffer State: 0
  - ..... A-MSDU: Not Present
  - .....00... Ack: Normal Acknowledge
  - .....1.... EOSP: End of Triggered Service Period
  - .....X... Reserved
  - .....110 UP: 6 - Voice

The IP Header - Internet Protocol Datagram is also shown, with the Differentiated Services field highlighted by a red box:

- Version: 4
- Header Length: 5 (20 bytes)
- Differentiated Services: %10111000
  - 1011 10.. Expedited Forwarding
  - .....00 Not-ECT
- Total Length: 200
- Identifier: 37214
- Fragmentation Flags: %0000
- Fragment Offset: 0 (0 bytes)
- Time To Live: 64
- Protocol: 17 UDP
- Header Checksum: 0xD2A9
- Source IP Address: 10.2.0.250
- Dest. IP Address: 10.2.0.104
- UDP: Src=19920 Dst=24096
- RTP: Version=2 Extension=0 CSRC Count=0 Marker=0 Payload Type=9 G.722 Sequence=32662 Time Stamp=2124782394 Sync Src ID=2023474068
- App Layer: Data Area=(160 bytes)
- FCS: FCS=0x4C20007B

## Call Admission Control

You have the option to configure inbound and outbound call admission control on the access point:

- Enable Call Admission Control / Wi-Fi MultiMedia Traffic Specifications (TSPEC)
- Set the desired maximum RF bandwidth that is allocated for voice traffic
- Set the bandwidth that is reserved for roaming clients.

You can modify the PHY rate for the phone to use when Call Admission Control (CAC) is enabled.

Enable a rate that is greater than or equal to 12 Mbps. (Default setting is 12 Mbps)

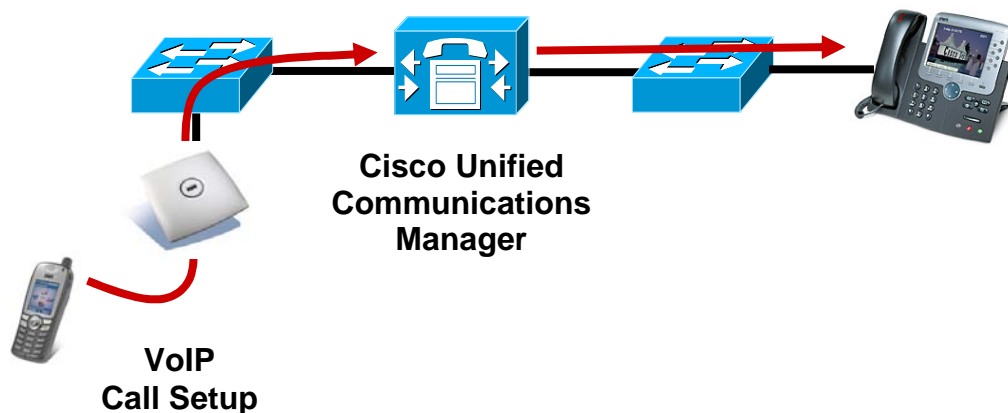
Cisco Access Points will only accept a PHY rate of 6, 11, 12 or 24 Mbps.

If you are using an 802.11b access point, then you must modify the PHY rate on each Cisco Unified Wireless IP Phone 7921G phone to a supported data rate for 802.11b.

TSPEC has precedence over QoS Basic Service Set (QBSS). QBSS is primarily used for roaming decisions if the channel gets busy.

## Pre-Call Admission Control

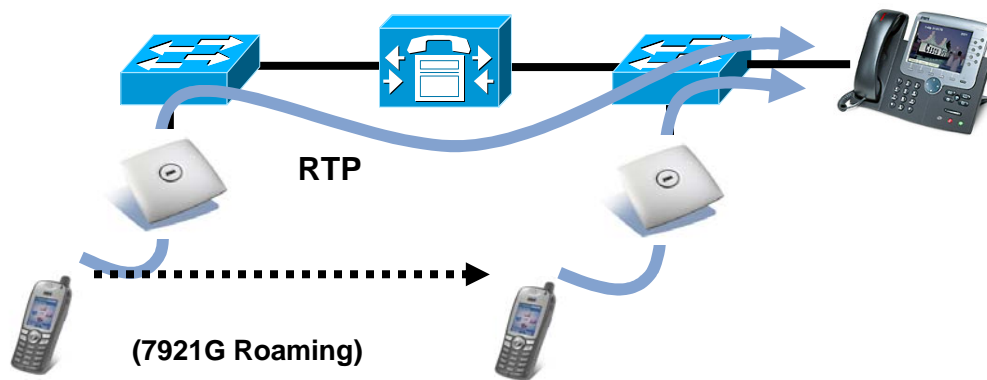
If Call Admission Control (TSPEC) is enabled on the access point, the Cisco Unified Wireless IP Phone 7921G 1 sends an Add Traffic Stream (ADDTS) to the access point to request bandwidth in order to place or receive a call. If the AP sends an ADDTS successful message then the Cisco Unified Wireless IP Phone 7921G establishes the call. If the call is rejected by the access point and the wireless IP phone has no other access point to roam to, then phone displays “Network Busy”.



## Roaming Admission Control

During a call, the Cisco Unified Wireless IP Phone 7921G measures Received Signal Strength Indicator (RSSI), QoS Basic Service Set (QBSS), and Packet Error Rate (PER) values for the current and all available access points to make roaming decisions.

If the original access point where the call was established had Call Admission Control (TSPEC) enabled, then the wireless IP phone will send an ADDTS request during the roam to the new access point.



For more information about Call Admission Control and QoS, refer to the “Cisco Unified Wireless Quality of Service” chapter in the *Enterprise Mobility Design Guide* at this URL:  
[http://www.cisco.com/application/pdf/en/us/guest/netso1/ns279/c649/cemigration\\_09186a00808d9330.pdf](http://www.cisco.com/application/pdf/en/us/guest/netso1/ns279/c649/cemigration_09186a00808d9330.pdf)

## Traffic Classification (TCLAS)

Traffic Classification (TCLAS) is required to ensure that the access point properly classifies voice packet streams.

Without proper classification, voice packets will be treated as best effort which will defeat the purpose of TSPEC and QoS in general.

TCP and UDP port information will be used to set the UP (User Priority) value

The previous method of classification depends upon preservation of DSCP value throughout the network, where the DSCP value maps to a particular queue (BE, BK, VI, VO).

However, the DSCP values are not always preserved as this can be viewed as a security risk.

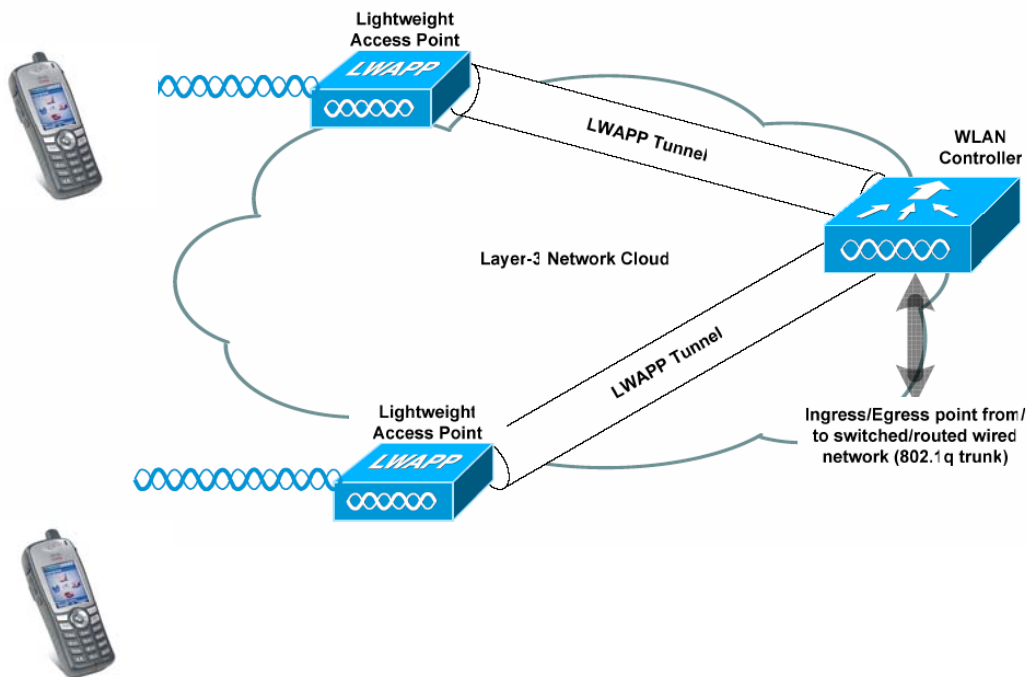
TCLAS is supported in the Cisco Unified Wireless LAN Controller release 5.1.151.0.

Using port based QoS policies is inadequate as all LWAPP data packets use the same UDP port 12222 and the access point uses the outside QoS marking to determine which queue the packets should be placed in.

Call Admission Control (TSPEC) must be enabled on the access point in order to enable TCLAS

TCLAS will be negotiated within the ADDTS packets, which are used to request bandwidth in order to place or receive a call.

## LWAPP Layer-3 Mode



## Multicast

When enabling multicast in the wireless network, impacts on battery life, performance, and capacity must be considered.

The Cisco Unified Wireless IP Phone 7921G uses the DTIM period to receive the queued broadcast and multicast packets.

If there are many packets queued up, then they client may have to stay awake longer thus potentially reducing battery life.

With multicast, there is no reliability that the packet will be received the by the client.

The multicast traffic will be sent at the highest basic data rate enabled on the access point, so will want to ensure that only the lowest enabled rate is configured as the only basic rate.

The client will send the IGMP join request to receive that multicast stream. The client will send the IGMP leave when the session is to be ended.

The Cisco Unified Wireless IP Phone 7921G supports the IGMP query feature, which can be used to reduce the amount of multicast traffic on the wireless LAN when not necessary.

Ensure that IGMP snooping is also enabled on all switches.

## Designing the Wireless LAN for Voice

You must consider these network design areas to insure adequate call capacity, signal strength and coverage for mobile wireless phones.

For more information about these topics, refer to the “VoWLAN Design Recommendations” chapter in the *Enterprise Mobility Design Guide* at this URL:

[http://www.cisco.com/application/pdf/en/us/guest/netsol/ns279/c649/cmigration\\_09186a00808d9330.pdf](http://www.cisco.com/application/pdf/en/us/guest/netsol/ns279/c649/cmigration_09186a00808d9330.pdf)

## Configuring Data Rates

It is recommended to disable rates below 12 Mbps for 802.11a and below 12 Mbps for 802.11b/g deployments where capacity and range are factored in for best results.

If 802.11b clients are not allowed in the wireless LAN, then it is recommended to disable the 1, 2, 5.5, 11 Mbps data rates.

When 802.11b clients exist in the wireless network, then an 802.11b rate must be enabled and only an 802.11b rate can be configured as a basic rate. In this case, it is suggested to enable the data rates 11 Mbps and higher.

The recommended data rate configuration is the following:

802.11 Mode	Basic (Mandatory) Data Rates	Supported (Optional) Data Rates	Disabled Data Rates
802.11a	12 Mbps	18 - 54 Mbps	6, 9 Mbps
802.11b	11 Mbps	None	1, 2, 5.5 Mbps
802.11g	12 Mbps	18 - 54 Mbps	6, 9 Mbps
802.11b/g	11 Mbps	12 -54 Mbps	1, 2, 5.5 Mbps

**Note:** Some environments may require that you enable a lower rate due to use of legacy clients, environmental factors or maximum range is required.

Set only the lowest data rate enabled as the single basic rate. Multicast packets will be sent at the highest basic data rate enabled.

Note that capacity and throughput are reduced when lower rates are enabled.

If Call Admission Control (TSPEC) is enabled then the Traffic Stream Rate Set (TSRS) feature will also be enabled, which will allow lower rates to be enabled for legacy devices, but prevent the Cisco Unified Wireless IP Phone 7921G to transmit at rates below 12 Mbps for 802.11a and 11 Mbps for 802.11b/g. See the [“Product Specific Configuration Options”](#) section for information on how to configure the Restricted Data Rates options on the Cisco Unified Wireless IP Phone 7921G in order to utilize the TSRS feature.

## Call Capacity

Design the network to accommodate the desired call capacity.

The Cisco Access Point can support up to 27 bi-directional RTP streams for both 802.11a and 802.11g at a data rate of 24 Mbps or greater. To achieve this capacity, you must use U-APSD and have minimal wireless LAN background traffic and radio frequency (RF) utilization.

The number of calls may vary depending on the data rate, initial channel utilization, and the environment.

At 6 Mbps, the Cisco Access Point can support up to 13 bi-directional RTP streams.

Using U-APSD instead of PS-POLL provides higher call capacity because U-APSD is more efficient and has limited management overhead.



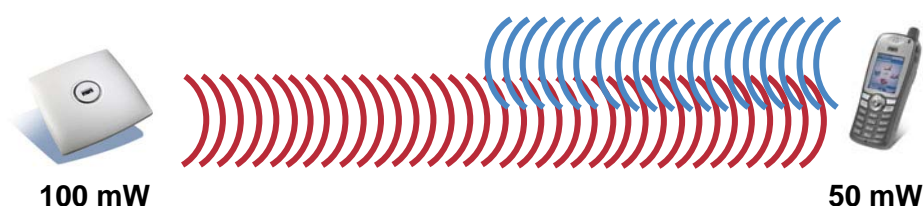
## Dynamic Transmit Power Control (DTPC)

To successfully exchange packets between the wireless IP phone and the access point, you need to configure Dynamic Transmit Power Control (DTPC).

When using an access point that supports DTPC, set the client power to match the local access point power.

Do not use default setting of Max power for client power as that will not advertise DTPC to the client.

If the access point does not support DTPC, then manually set the transmit power on the phone to match the highest transmit power of an access point in the wireless LAN. This setting prevents one-way audio when RF traffic is heard in one direction only. By default the Cisco Unified Wireless IP Phone 7921G will use the highest available transmit power by default (i.e. 17 dBm / 50 mW for 2.4 GHz and 16 dBm / 40 mW for 5 GHz).



## Planning Channel Usage

Use these guidelines to plan channel usage for these wireless environments.

### 5 GHz (802.11a)

The Cisco Unified Wireless IP Phone 7921G supports Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) from 802.11h, which are required when using channels operating at 5.25–5.725 GHz, which is 15 of the 23 possible channels.

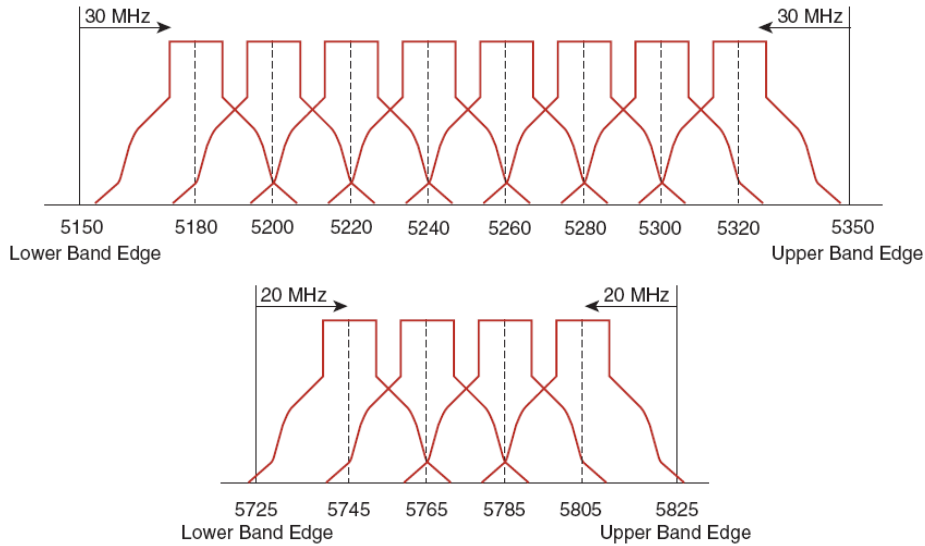
DFS dynamically instructs a transmitter to switch to another channel whenever radar signal is detected. If the access point detects radar, the radio on the access point goes on hold for at least 60 seconds while the access point passively scans for another usable channel.

TPC allows the client and access point to exchange information, so that the client can dynamically adjust the transmit power. The client uses only enough energy to maintain association to the access point at a given data rate. As a result, the client contributes less to adjacent cell interference, which allows for more densely deployed, high-performance wireless LANs.

Lower power on the client provides longer battery life because less power is used by the radio.

5 GHz channels overlap their adjacent channel, so there should be at least 1 channel of separation for adjacent access points.





<b>Channel ID</b>	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	149	153	157	161		
<b>Center Freq. MHz</b>	5180	5200	5220	5240	5260	5280	5300	5320	5500	5520	5540	5560	5580	5600	5620	5640	5660	5680	5700	5745	5765	5785	5805		
<b>Band</b>	UNII-1				UNII-2																		UNNI-3		

## Using Dynamic Frequency Selection (DFS) on Access Points

For autonomous solution access points, select Dynamic Frequency Selection (DFS) to use auto channel selection.

When DFS is enabled, enable at least one band (bands 1-4).

For unified access points, enable Auto RF unless there is an intermittent interferer in an area which select access points can have the channel statically assigned.

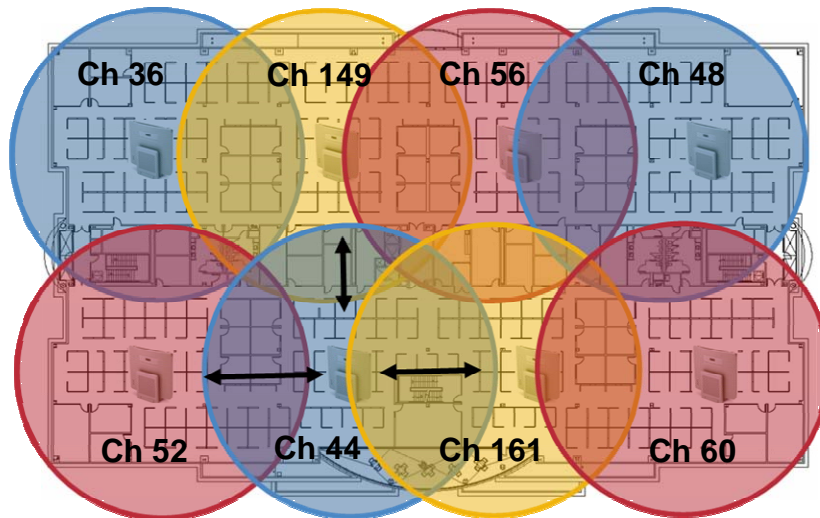
In case of radar activity, have at least one access point per area that uses a non-DFS channel (UNII-1). This ensures that a channel is available when an access point's radio is in its hold-off period while scanning for a new usable channel.

For autonomous access points, enable band 1 only which allows the access point to use only a UNII-1 channel.

For unified access points, can manually select a UNII-1 channel (channels 36, 40, 44, 48) for the desired access points.

A UNII-3 channel (5.725 – 5.825 GHz) can optionally be used if available.

In this diagram, 5 GHz cells use a non-DFS channel while other nearby cells use DFS channels to permit maximum call capacity under all conditions.



**Minimum 20% Overlap**

For 5 GHz, 20 channels are available in the Americas and 19 channels in Europe and Japan.

Where UNII-3 is available, it is recommended to use UNII-1, UNII-2 and UNII-3, to utilize a 12 channel set.

If planning to use UNII-2 extended channels (channels 100-140), it is recommended to disable UNII-2 (channels 52-64) on the access point.

Having many 5 GHz channels enabled in the wireless LAN can delay discovery of new access points.

**Default Radio Channel:**

Dynamic Frequency Selection (DFS) Channel 48 5240 MHz

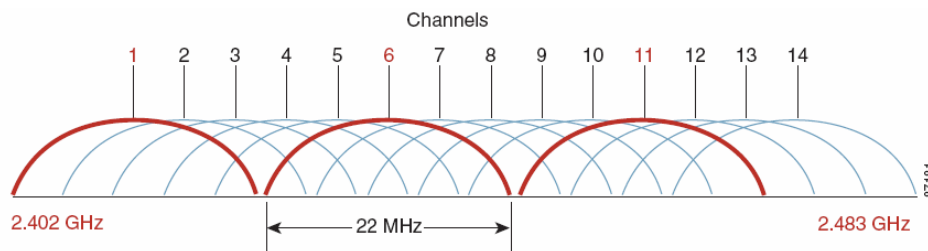
**Dynamic Frequency Selection Bands:**

- Band 1 - 5.150 to 5.250 GHz
- Band 2 - 5.250 to 5.350 GHz
- Band 3 - 5.470 to 5.725 GHz
- Band 4 - 5.725 to 5.825 GHz

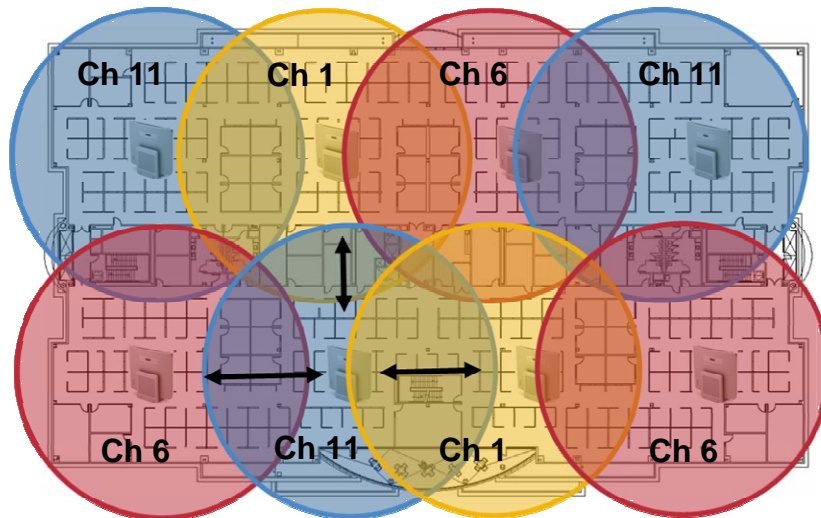
## 2.4 GHz (802.11b/g)

In the 2.4 GHz (802.11b/g) environment, you must use non-overlapping channels when deploying VoWLAN. Non-overlapping channels have 22 MHz of separation and are at least 5 channels apart.

There are only 3 non-overlapping channels in the 2.4 GHz frequency range (channels 1, 6, 11). In Japan, you can use Channel 14 as a fourth non-overlapping channel when using 802.11b access points.



You must use non-overlapping channels and allow at least 20 percent overlap with adjacent channels when deploying phones in the 802.11b/g environment.



**Minimum 20% Overlap**

### Signal Strength and Coverage

To ensure acceptable voice quality, the Cisco Unified Wireless IP Phone 7921G should always have a signal of -67 dBm or higher when using 2.4 or 5 GHz and ensure the Packet Error Rate (PER) is no higher than 1%.

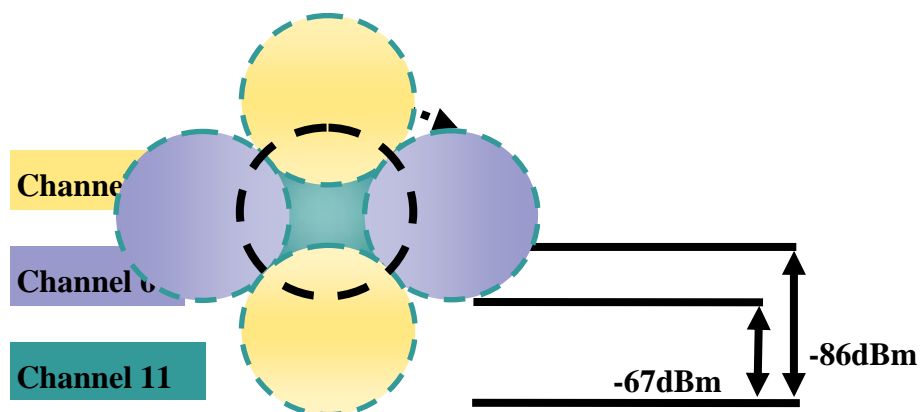
A minimum Signal to Noise Ratio (SNR) of 25dB = -92dBm noise level with -67 dBm signal should be maintained.

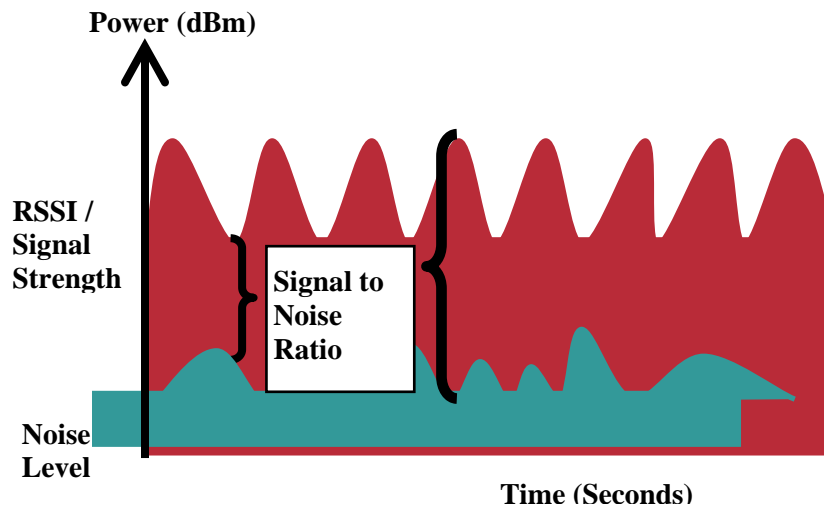
To achieve maximum capacity and throughput, the wireless LAN should be designed to 24 Mbps. Higher data rates (36-54 Mbps) can optionally be enabled.

Recommended to set the minimum data rate to 11 Mbps or 12 Mbps for 2.4 GHz (dependent upon 802.11b client support policy) and 12 Mbps for 5 GHz, which should also be the only rate configured as a basic rate.

For more information about signal strength and cell edge design, refer to the “VoWLAN Design Recommendations” chapter in the *Enterprise Mobility Design Guide* at this URL:

[http://www.cisco.com/application/pdf/en/us/guest/netso/ns279/c649/ccmigration\\_09186a00808d9330.pdf](http://www.cisco.com/application/pdf/en/us/guest/netso/ns279/c649/ccmigration_09186a00808d9330.pdf)





### Coverage

When designing the placement of access points, be sure that all key areas have sufficient coverage (signal).

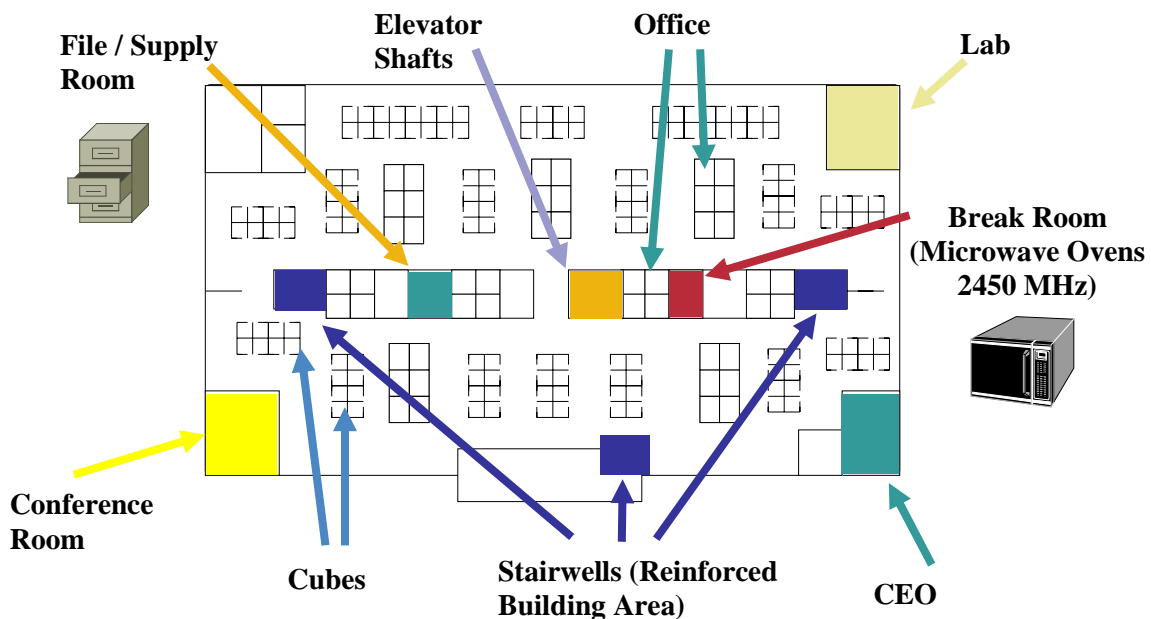
Typical wireless LAN deployments for data only applications do not provide coverage for some areas where VoWLAN service is necessary such as elevators, stairways, and outside corridors.

wireless LAN interference is generated by microwave ovens, 2.4 GHz cordless phones, Bluetooth devices, or other electronic equipment operating in the 2.4 GHz band.

Microwave ovens operate on 2450 MHz, which is between channels 8 and 9 of 802.11b/g. Some microwaves are shielded more than others and that shielding reduces the spread of the energy. Microwave energy can impact channel 11, and some microwaves can affect the entire frequency range (channels 1 through 11). To avoid microwave interference, select channel 1 for use with access points that are located near microwaves.

Most microwave ovens, Bluetooth, and frequency hopping devices do not have the same effect on the 5 GHz frequency. The 802.11a technology provides more non-overlapping channels and typically lower initial RF utilization. For voice deployments, it is suggested that you use 802.11a for voice and use 802.11b/g for data.

However there are products that also utilize the non-licensed 5 GHz frequency (i.e. 5.8 GHz cordless phones, which can impact UNII-3 channels).



## Multipath

Multipath occurs when RF signals take multiple paths from a source to a destination.

A part of the signal goes to the destination while another part bounces off an obstruction, then goes on to the destination. As a result, part of the signal encounters delay and travels a longer path to the destination which creates signal energy loss.

When the different waveforms combine, they cause distortion and effect the decoding capability of the receiver as the signal quality is poor.

Multipath can exist in environments where there are reflective surfaces (i.e. metal, glass, etc.). Avoid mounting access points on these surfaces.

Below is a list of multipath effects:

### Data Corruption

Occurs when multipath is so severe that the receiver is unable to detect the transmitted information.

### Signal Nulling

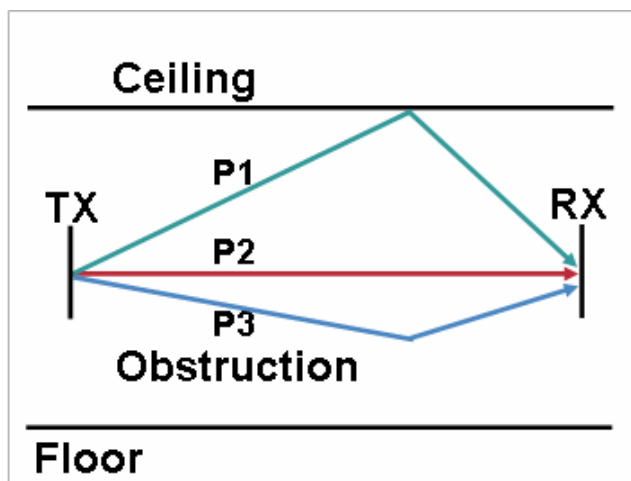
Occurs when the reflected waves arrive exactly out of phase with the main signal and cancel the main signal completely.

### Increased Signal Amplitude

Occurs when the reflected waves arrive in phase with the main signal and add on to the main signal thereby increasing the signal strength.

### Decreased Signal Amplitude

Occurs when the reflected waves arrive out of phase to some extent with the main signal thereby reducing the signal amplitude.



Use of Orthogonal Frequency Division Multiplexing (OFDM), which is used by 802.11a and 802.11g, can help to reduce issues seen in high multipath environments.

If using 802.11b in a high multipath environment, lower data rates should be used in those areas (i.e. 1 and 2 Mbps).

Use of antenna diversity can also help in such environments.

## Verification with Site Survey Tools

These are many tools and applications that can be utilized to verify coverage, quality and configuration.

- [Cisco Wireless Control System \(WCS\) for Unified Wireless LAN management](#)
- [Cisco Wireless LAN Solution Engine \(WLSE\) for Autonomous Wireless LAN management](#)
- [Cisco Spectrum Expert](#)
- [AirMagnet](#) (Survey, Laptop Analyzer, VoFi Analyzer)
- [Cisco Unified Wireless IP Phone 7921G](#)

### Cisco 7921G Neighbor List

The Cisco Unified Wireless IP Phone 7921G can be utilized to verify coverage by using the Neighbor List menu.

The Cisco Unified Wireless IP Phone 7921G only scans other non-associated channels when the current signal lowers to a certain threshold, so you may see only one access point in the list if configured for auto scan mode.

To see all access points in the neighbor list menu, 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 in auto scan mode. Otherwise configure continuous scan mode.

Access the neighbor list menu on the phone by pressing **Settings > Status > Neighbor List**



### Cisco 7921G Site Survey

The Cisco Unified Wireless IP Phone 7921G also has a Site Survey application as of release 1.1(1), which is an offline mode that gathers information about the access points for the configured network profile and generates an HTML report after exiting the application.

This information can be utilized to confirm access point configuration as well as coverage.

The neighbor table shows which access points (along the column) are neighbors of the access points with the strongest signal listed in the row. The percentage of time that the access point had the highest RSSI is displayed as well as the RSSI range for that access point when it was observed. The access point name is hyperlinked to the access point detail listed below.

Neighbor Table	sjc21-21a-air12	sjc21-21a-air13	sjc21-21a-air24	sjc21-21a-air8	sjc
sjc21-21a-air12	64% -60/-43	78% -69/-52	19% -70/-59	*	
sjc21-21a-air13	86% -56/-52	7% -55/-49	13% -57/-56	*	
sjc21-21a-air24	59% -73/-58	39% -72/-56	27% -61/-39	*	
sjc21-21a-air8	*	*	*	*	
sjc21-21a-air21	*	*	*	*	

<b>AP:</b> sjc21-21a-air12			
<b>MAC:</b> 00:19:07:8D:5A:DE			
<b>Observation Count:</b> 463			
<b>Channel - Frequency:</b> 64 - 5320000hz			
<b>Country:</b> US			
<b>Beacon Interval:</b> 100			
<b>DTIM Period:</b> 2			
<b>RSSI Range [Lo Hi]:</b> [-73 -43]			
<b>BSS Lost Count:</b> 0			
<b>Channel Utilization:</b> 2			
<b>Station Count:</b> 1			
<b>Available Admission Capacity:</b> 23437			
<b>Warning Flags:</b> 100000			
<b>Basic Rates:</b> 6			
<b>Optional Rates:</b> 9 12 18 24 36 48 54			
<b>Multicast Cipher:</b> TKIP			
<b>Unicast Ciphers:</b> TKIP			
<b>AKM:</b> WPA1_1X WPA1_CCKM			
<b>Proxy ARP supported:</b> Yes			
<b>WMM Supported:</b> Yes			
<b>CCX Version Number:</b> 5			
<b>U-APSD Supported:</b> Yes			
<b>Background AC(1)</b>			
<b>Admission Control Required:</b> No			
<b>AIFSN</b>	<b>ECWMin</b>	<b>ECWMax</b>	<b>TXOpLimit</b>
7	4	10	0
<b>Best Effort AC(0)</b>			
<b>Admission Control Required:</b> No			
<b>AIFSN</b>	<b>ECWMin</b>	<b>ECWMax</b>	<b>TXOpLimit</b>
3	4	10	0
<b>Video AC(2)</b>			
<b>Admission Control Required:</b> No			
<b>AIFSN</b>	<b>ECWMin</b>	<b>ECWMax</b>	<b>TXOpLimit</b>
2	3	4	94
<b>Voice AC(3)</b>			
<b>Admission Control Required:</b> Yes			
<b>AIFSN</b>	<b>ECWMin</b>	<b>ECWMax</b>	<b>TXOpLimit</b>
2	2	3	47
<b>Channels</b>	36 40 44 48 52 56 60 64 100 104 108 112 116 132 136 140 149 153 157 161		
<b>Power</b>	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20		
Data rates less than 11mb/s are not recommended.			



# Configuring Cisco Unified Communications Manager

Cisco Unified Communications Manager provides many different phone, calling and security features.

## Phone Button Templates

The Cisco Unified Wireless IP Phone 7921G supports 6 lines. The default phone button template includes support for 2 lines and 4 speed dials.

Custom phone button templates can be created with the option for many different features, which can then be applied on a phone by phone basis.

**Phone Button Template Information**

Button Template Name \* Cisco 7921G

**Button Information**

Button	Feature
1	Line **
2	Line
3	Speed Dial
4	Privacy
5	Service URL
6	Speed Dial BLF
	Call Park BLF
	Intercom
	Mobility
	Do Not Disturb
	None

Save Delete Copy Reset Add New

## Softkey Templates

Custom softkey templates can be created with the option of giving additional feature access or limiting feature access.

Softkeys are assigned based on the state of the phone (on hook, connected, on hold, ring in, off hook, connected transfer, digits after first, connected conference, ring out, off hook with feature, remote in use, connected no feature).

The order of the softkeys can also be arranged when creating a custom softkey template.

The Cisco Unified Wireless IP Phone 7921G has 2 softkeys available. The feature listed first in the softkey template will be displayed on the left softkey if on a call, where the other features will be listed under the options menu on the right softkey.

## Security Profiles

Security profiles can be utilized to enable authenticated mode or encrypted mode, where signaling, media and phone configuration file encryption.

The Certificate Authority Proxy Function (CAPF) to be operational.

Each Cisco Unified Wireless IP Phone 7921G has a Manufactured Installed Certificate (MIC).



**Protocol Specific Information**

Packet Capture Mode\*

Packet Capture Duration

Presence Group\*

Device Security Profile\*

SUBSCRIBE Calling Search Space

Unattended Port

---

**Certification Authority Proxy Function (CAPF) Information**

Certificate Operation\*

Authentication Mode\*

Authentication String

Key Size (Bits)\*

Operation Completes By     (YYYY:MM:DD:HH)

Certificate Operation Status: None

Note: Security Profile Contains Addition CAPF Settings.

## G.722 Advertisement

Cisco Unified Communications Manager versions 5.0 and later support the ability to configure whether G.722 is to be a supported codec system wide or not.

Earlier versions of Cisco Communications Manager do not have this capability, where a Cisco Unified Wireless IP Phone 7921G with release 1.1(1) or later will attempt to use G.722 assuming the other endpoint also advertises G.722 capabilities.

**Enterprise Parameters Configuration**

Parameter Name	Parameter Value	Suggested Value
<a href="#">Synchronization Between Auto Device Profile and Phone Configuration</a> *	<input type="text" value="True"/>	True
<a href="#">Max Number of Device Level Trace</a> *	<input type="text" value="12"/>	12
<a href="#">DSCP for Phone-based Services</a> *	<input type="text" value="default DSCP (000000)"/>	default DSCP (000000)
<a href="#">DSCP for Phone Configuration</a> *	<input type="text" value="CS3(precedence 3) DSCP (011000)"/>	CS3(precedence 3) DSCP (011000)
<a href="#">DSCP for Cisco CallManager to Device Interface</a> *	<input type="text" value="CS3(precedence 3) DSCP (011000)"/>	CS3(precedence 3) DSCP (011000)
<a href="#">Connection Monitor Duration</a> *	<input type="text" value="120"/>	120
<a href="#">Auto Registration Phone Protocol</a> *	<input type="text" value="SCCP"/>	SCCP
<a href="#">BLF For Call Lists</a> *	<input type="text" value="Disabled"/>	Disabled
<a href="#">Advertise G.722 Codec</a> *	<input type="text" value="Enabled"/>	Enabled
<a href="#">Phone Personalization</a> *	<input type="text" value="0"/>	0

For more information, refer to the Cisco Unified Communications Manager documentation.

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html)

## Product Specific Configuration Options

On the IP Phone Configuration page in Cisco Unified Communications Manager Administration, these Cisco Unified Wireless IP Phone 7921G configuration options are available. For explanations of these options, click the "?" on the configuration page.

Below are the default settings when adding a phone.

**Product Specific Configuration Layout** 

Disable Speakerphone

Gratuitous ARP\*

Settings Access\*

Web Access\*

Profile 1\*

Profile 2\*

Profile 3\*

Profile 4\*

Load Server

Admin Password

Special Numbers

Application URL

"Send" Key Action\*

Days Display Not Active

Display On Time

Display On Duration

Display Idle Timeout

Phone Book Web Access\*

Unlock-Settings Sequence (\*\*#)\*

Application Button Activation Timer\*

Application Button Priority\*

Out-of-Range Alert\*

Scan Mode\*

Restrict Data Rates\*

Power Off When Charging\*

Cisco Discovery Protocol (CDP)\*

Advertise G.722 Codec\*

Home Screen\*

### **Disable Speakerphone**

Speakerphone capabilities can optionally be disabled.

### **Gratuitous ARP**

Determines whether Gratuitous ARP is enabled or not.

### **Settings Access**

Settings Access can be used to limit user access to certain menus (i.e. Network Profiles).

### **Web Access**

Web Access can be set to Full, where configuration changes can be made remotely or Read Only to provide information but not allowing changes to be made.

### **Locked Profiles**

Individual profiles can also be locked, which does not allow the user to modify those settings.

### **Load Server**

A load server can be specified in IP format (x.x.x.x) if wanting to use an alternate TFTP server for phone firmware downloads.

### **Admin Password**

The admin password is used for web access. With Cisco Unified Communications Manager 5.0 or later the admin password must be managed in Communications Manager Administrator page, where previous versions allow local management.

### **Special Numbers**

Special numbers can be programmed to dial out regardless of keypad lock state (i.e. 911).

### **Application URL**

An application URL can be configured, which will convert the application button to a service URL button.

### **“Send” Key Action**

“Send” key action determines whether the green dial button is to use onhook dialing and serve as last number redial, where a list of previously dialed numbers will be listed, or to use offhook dialing, which will play dial tone.

### **Display Settings**

Display on time can also be configured, where the days to be active, display on time and display duration can be adjusted.

### **Phone Book Web Access**

Phone book web access must be set to “Allow Admin” in order to access the phone book via the web page.

### **Unlock-Settings Sequence**

By default, \*\*# must be entered to unlock a menu that contains configurable items, which can optionally be disabled.

### **Application Button Activation Timer**

The activation timer and priority of the application button can also be specified. This determines how long the button must be pressed and held to activate.

### **Application Button Priority**

If the priority is low, then will only function when the keypad is unlocked and on the home screen. Medium priority will allow the application button to function when in any menu or XML screen and high priority will allow the application button to function when in any state including keypad lock.

### **Out of Range Alert**

An out of range alert can be configured to beep once or periodically to audibly notify the user that they have traveled out of the coverage area.

### **Scan Mode**

Scan mode allows for auto, continuous, and single AP options, where auto primarily scans only when on call and single AP only at power on.

### **Restricted Data Rates**

The restricted data rates feature utilizes the Traffic Stream Rate Set (TSRS) information element from CCX v4, which can define a data range for the client to use. This can be beneficial for environments that have legacy clients requiring lower data rates to be enabled on the access point, but also preventing other clients from downshifting to lower rates, which lowers overall throughput and capacity. When enabled the Cisco Unified Wireless IP Phone 7921G will not transmit below 12 Mbps for 802.11a and 11 Mbps for 802.11b/g.

### **Power Off When Charging**

Power off when charging feature will power off the phone when placed on AC power.

### **Cisco Discover Protocol (CDP)**

Enabled or disabled CDP.

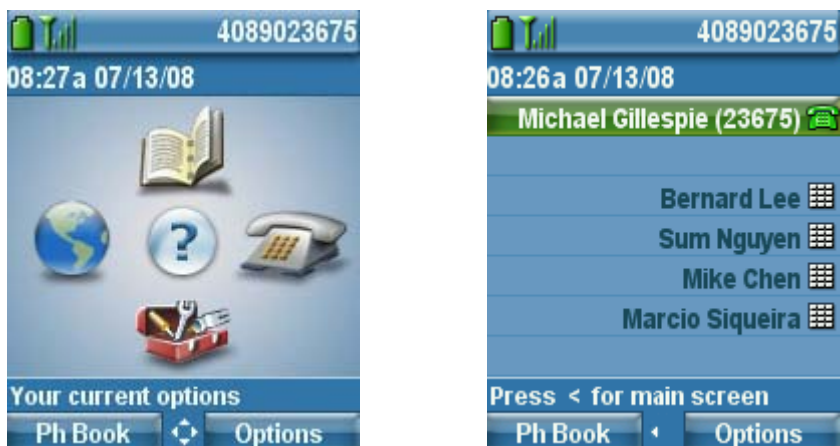
### **Advertise G.722 Codec**

With release 1.2(1), G.722 capabilities can be configured on a phone by phone basis and optionally override the system default.

### **Home Screen**

By default the Cisco Unified Wireless IP Phone 7921G will show the traditional screen with the four icons for directory, services, settings and line access. In release 1.2(1), line view can be set as the default home screen vs. main phone screen.

Below shows the main phone screen (left) and line view (right) display options for the home screen.



**Note:** If configuring the “Admin Password” in Cisco Unified Communications Manager versions 5.0, 5.1, 6.0, 6.1, 7.0 or later and web access is set to “Full”, then it is recommended to enable TFTP encryption via the device security profile.

To configure product specific configuration options for the Cisco Unified Wireless IP Phone 7921G with Cisco Unified Communications Manager Express, create an ephone template with the necessary options.

"service phone <module> <value>"

<u>Module</u>	<u>Value</u>
disableSpeaker	false = Enabled; true = Disabled
garp	0 = Enabled; 1 = Disabled
settingsAccess	0 = Disabled; 1 = Enabled; 2 = Restricted
webAccess	0 = Full; 1 = Disabled; 2 = ReadOnly
WLANProfile<1-4>	0 = Unlocked; 1 = Locked, 2 = Restricted
loadServer	x.x.x.x
specialNumbers	(i.e. 411,911)
PushToTalkURL	http://x.x.x.x
sendKeyAction	0 = Onhook Dialing; 1 = Offhook Dialing
daysDisplayNotActive	<1-7> = <Sunday, Monday Tuesday, Wednesday, Thursday, Friday, Saturday>
displayOnTime	(([0-1][0-9]) (2[0-3])):[0-5][0-9] (i.e. 07:30)
displayOnDuration	(([0-1][0-9]) (2[0-3])):[0-5][0-9] (i.e. 10:30)
displayIdleTimeout	(([0-1][0-9]) (2[0-3])):[0-5][0-9] (i.e. 01:00)
phoneBookWebAccess	0 = Deny All; 1 = Allow Admin
unlockSettingsSequence	0 = Disabled; 1 = Enabled
appButtonTimer	0 = Disabled; <1-5> = <1-5> seconds
appButtonPriority	0 = Low; 1 = Medium; 2 = High
outOfRangeAlert	0 = Disabled; 1 = Beep Once; <2-4> = Beep every <10,30,60> seconds
scanningMode	0 = Auto; 1 = Single AP; 2 = Continuous

restrictDataRates	0 = Disabled; 1 = Enabled
powerOffWhenCharging	0 = Disabled; 1 = Enabled
cdpEnable	0 = Disabled; 1 = Enabled
g722CodecSupport	0 = Use System Default; 1 = Disabled; 2 = Enabled
homeScreen	0 = Main Phone Screen; 1 = Line View
thumbButton1	PTTH<1-6>

For more information on these features, see the *Cisco Unified Wireless IP Phone 7921G Administration Guide* or the Cisco Unified Wireless IP Phone 7921G Release Notes.

[http://www.cisco.com/en/US/products/hw/phones/ps379/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/phones/ps379/prod_maintenance_guides_list.html)

[http://www.cisco.com/en/US/products/hw/phones/ps379/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/hw/phones/ps379/prod_release_notes_list.html)

Enable individual phone configuration files with the following commands.

```
telephony-service
cnf-file perphone
create cnf-files
```

## Configuring the Cisco Unified Wireless LAN Controller and Access Points

When configuring your access points, use these guidelines:

- Set the QoS policy to “Platinum”.
- Enable WMM to enable QoS and the ability to use U-APSD.
- Disable “DHCP address assignment”.
- Ensure “Aggressive Load Balancing” is disabled
- Ensure ARPUnicast is disabled
- Disable Peer to Peer Blocking / Public Secure Packet Forwarding (PSPF)
- Ensure Client Management Frame Protection (MFP) is set to disabled or optional
- Enable “Symmetric Tunneling” if Layer 3 mobility is enabled
- Enable short preamble if using 2.4 GHz

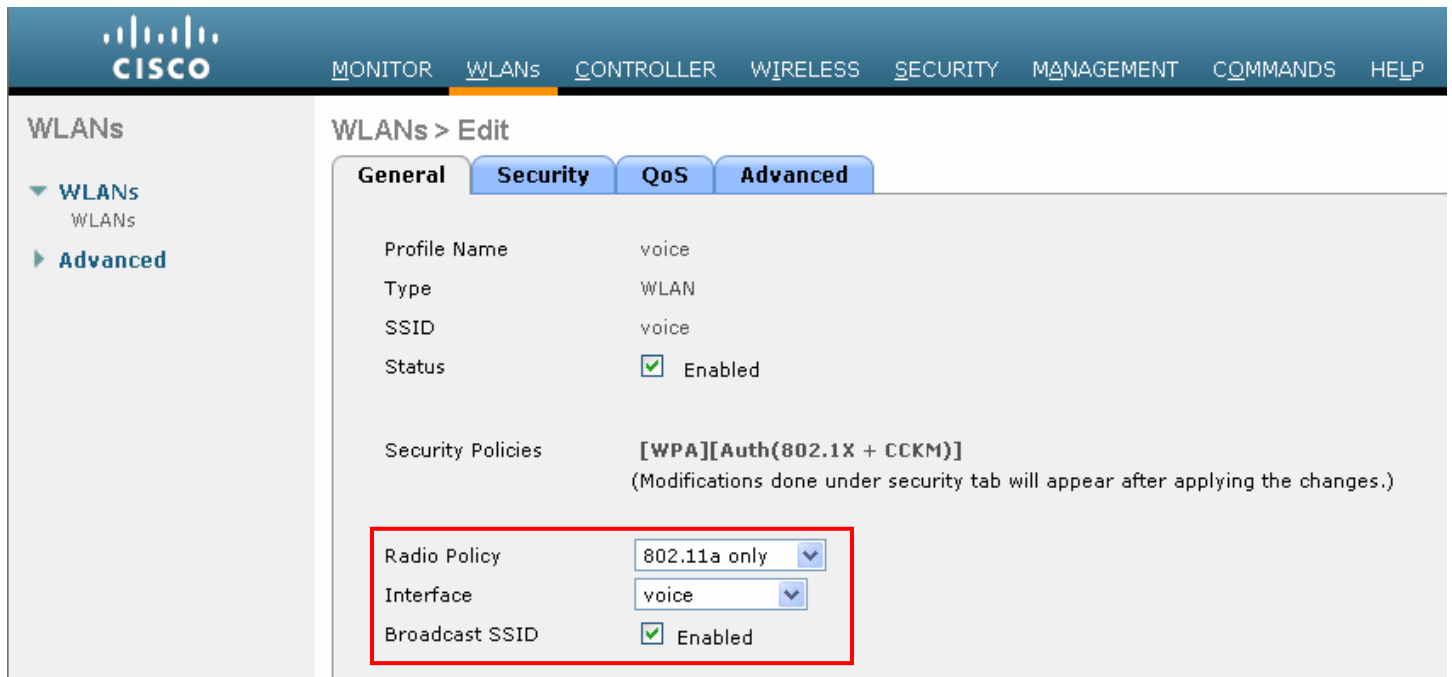
When using 802.1x authentication, it is recommended to implement CCKM.

**Note:** If you have clients from other regions that will attempt to associate with the wireless LAN, then ensure that World Mode (802.11d) is enabled.

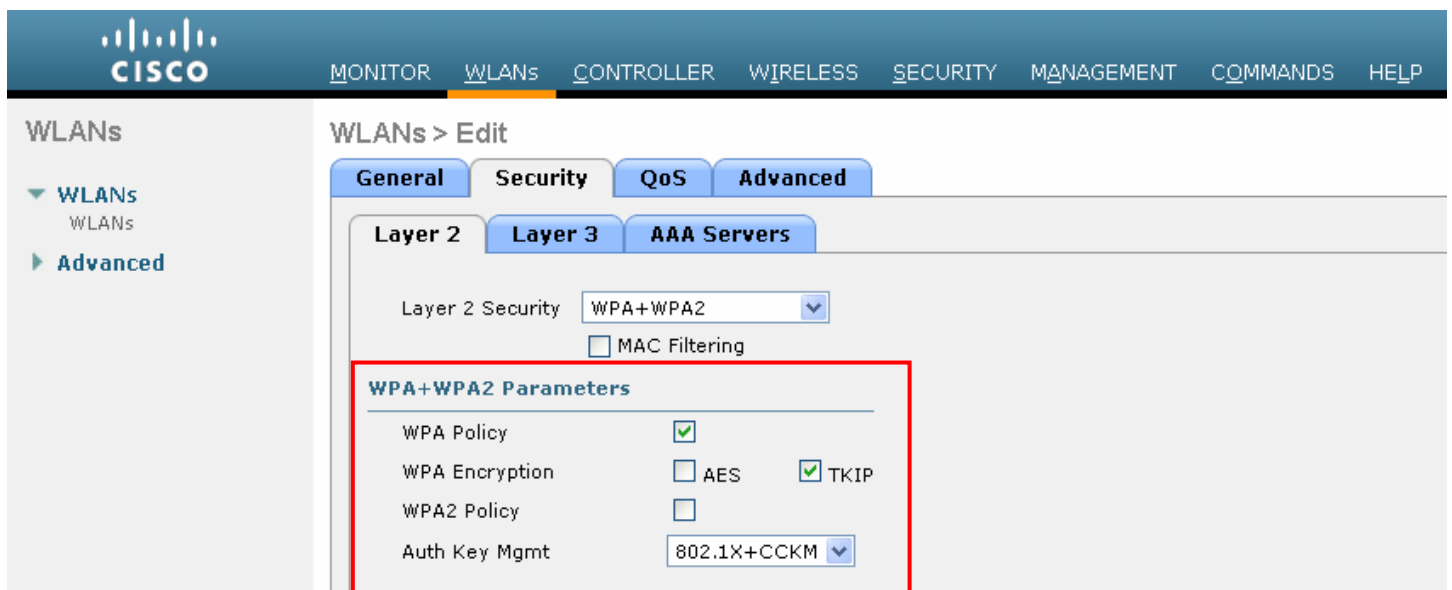
### SSID / WLAN Settings

The SSID to be used by voice clients can be configured to only apply to a certain 802.11 radio type.

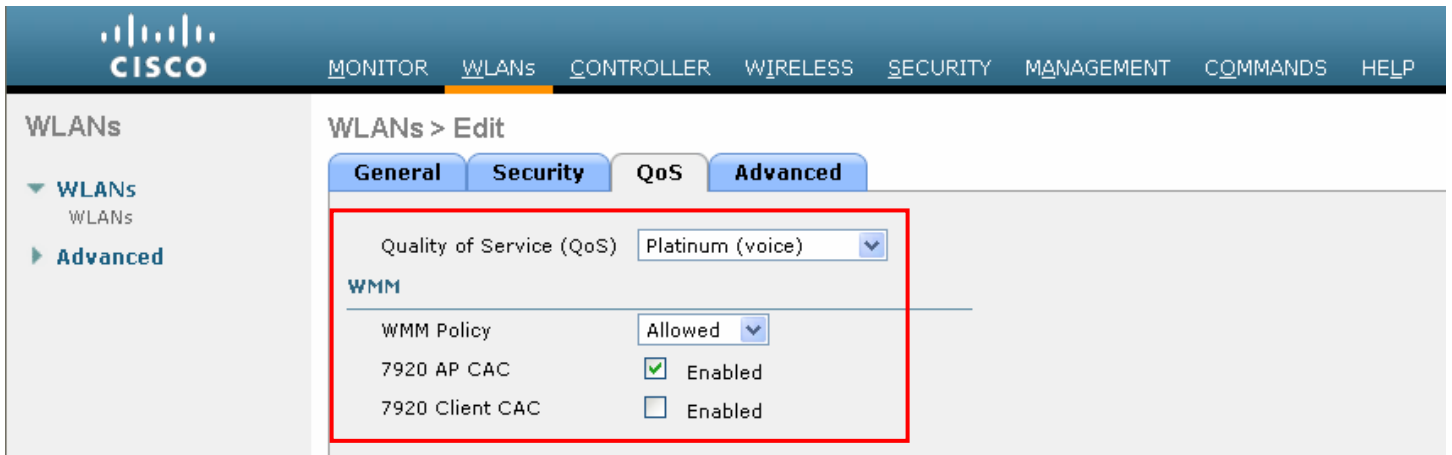
Use the short preamble setting in the 2.4 GHz radio configuration setting on the access point when no legacy clients that require a long preamble are present in the wireless LAN. By using the short preamble instead of long preamble, the wireless network performance is improved.



Enable WPA policy with TKIP in order to use CCKM, when 802.1x authentication is used.



The WMM policy can be set to “Mandatory” if only the Cisco Unified Wireless IP Phone 7921G will be using this SSID. If 7920 or other non-WMM clients will associate using this SSID, then ensure the WMM policy is set to “Allowed”. Enable “7920 AP CAC” to advertise Qos Basic Service Set (QBSS) to the client.



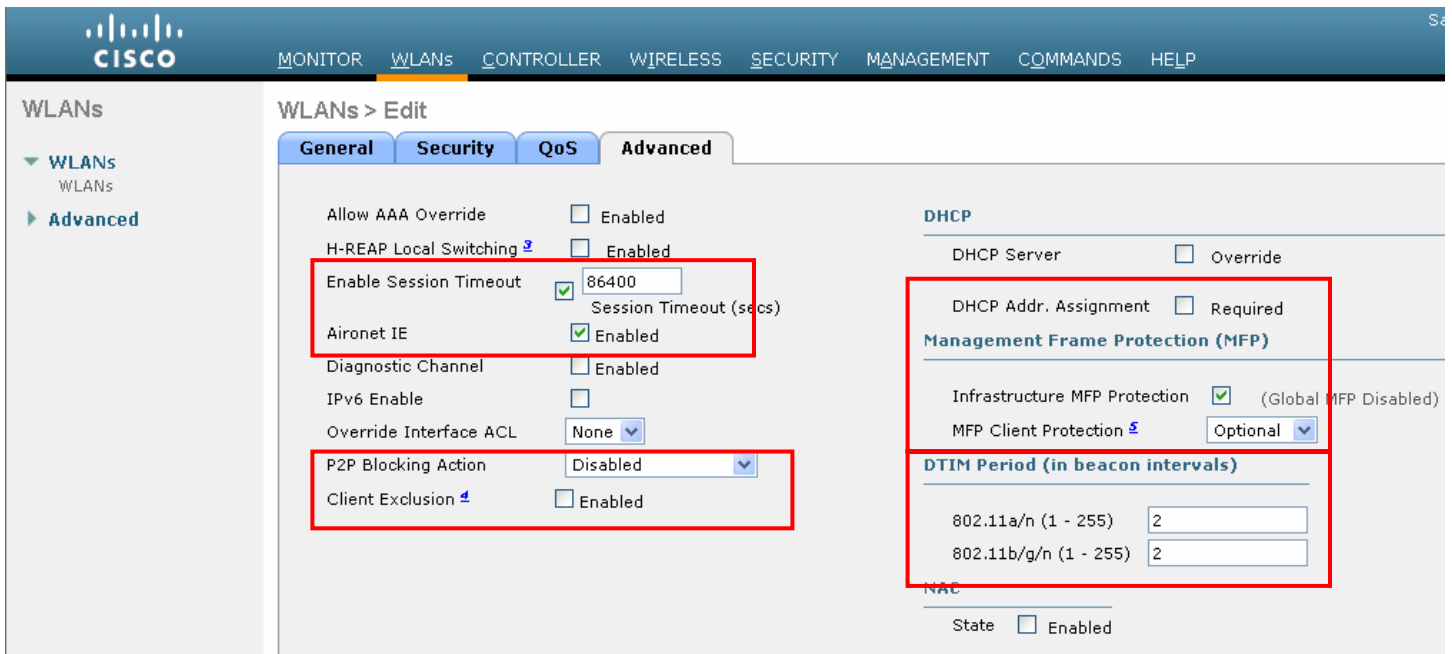
Configure session timeout as necessary. It is recommended to extend the timeout to avoid possible interruptions during re-authentication.

Enable Aironet Extensions (Aironet IE).

Disable client exclusion for the voice network.

DHCP Address Assignment should be disabled.

MFP client protection should be disabled or only set to optional.



## Controller Settings

Ensure that aggressive load balancing is disabled.

The screenshot shows the Cisco Unified Wireless LAN Controller configuration page, specifically the General tab. The left sidebar contains a navigation menu with options like General, Inventory, Interfaces, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, and Advanced. The main content area is titled 'General' and lists various configuration parameters. A red box highlights the 'Aggressive Load Balancing' setting, which is currently set to 'Disabled'. Other settings include Name (WISM-1), 802.3x Flow Control Mode (Disabled), LAG Mode on next reboot (Enabled), Ethernet Multicast Mode (Unicast), Broadcast Forwarding (Disabled), Over The Air Provisioning of AP (Disabled), AP Fallback (Enabled), Apple Talk Bridging (Disabled), Fast SSID change (Disabled), Default Mobility Domain Name (VTG), RF Group Name (VTG), User Idle Timeout (seconds) (300), ARP Timeout (seconds) (300), Web Radius Authentication (PAP), 802.3 Bridging (Disabled), Operating Environment (Commercial (0 to 40 C)), and Internal Temp Alarm Limits (0 to 65 C). A note indicates that LAG Mode is currently enabled.

Parameter	Value
Name	WISM-1
802.3x Flow Control Mode	Disabled
LAG Mode on next reboot	Enabled (LAG Mode is currently enabled)
Ethernet Multicast Mode	Unicast
Broadcast Forwarding	Disabled
Aggressive Load Balancing	Disabled
Over The Air Provisioning of AP	Disabled
AP Fallback	Enabled
Apple Talk Bridging	Disabled
Fast SSID change	Disabled
Default Mobility Domain Name	VTG
RF Group Name	VTG
User Idle Timeout (seconds)	300
ARP Timeout (seconds)	300
Web Radius Authentication	PAP
802.3 Bridging	Disabled
Operating Environment	Commercial (0 to 40 C)
Internal Temp Alarm Limits	0 to 65 C

If using layer 3 mobility, then symmetric tunneling should be enabled and that the mobility group has been configured containing each Cisco Unified Wireless LAN Controller's IP and MAC address.

The screenshot shows the Cisco Unified Wireless LAN Controller configuration page, specifically the Mobility Anchor Config tab. The left sidebar contains a navigation menu with options like General, Inventory, Interfaces, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, and Advanced. The main content area is titled 'Mobility Anchor Config' and lists various configuration parameters. A red box highlights the 'Symmetric Mobility Tunneling mode' setting, which is currently checked and enabled. Other settings include Keep Alive Count (3) and Keep Alive Interval (10). A note indicates that Symmetric mobility tunneling mode should be the same across all members of the controller's mobility group.

Parameter	Value
Keep Alive Count	3
Keep Alive Interval	10
Symmetric Mobility Tunneling mode *	Enabled (currently enabled)

\* Symmetric mobility tunneling mode should be same across all members of the controller's mobility group.



## 802.11 Network Settings

For optimal battery performance and quality, use DTIM of 2 with a beacon period of **100ms**.

The screenshot shows the Cisco Unified Wireless LAN Controller configuration interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar shows the configuration tree with '802.11a/n' selected. The main content area is titled '802.11a Global Parameters' and is divided into three sections:

- General** (highlighted with a red box):
  - 802.11a Network Status:  Enabled
  - Beacon Period (milliseconds):
  - Fragmentation Threshold (bytes):
  - DTPC Support:  Enabled
- 802.11a Band Status**:
  - Low Band: Enabled
  - Mid Band: Enabled
  - High Band: Enabled
- Data Rates\*\*** (highlighted with a red box):
  - 6 Mbps: Disabled
  - 9 Mbps: Disabled
  - 12 Mbps: Mandatory
  - 18 Mbps: Supported
  - 24 Mbps: Supported
  - 36 Mbps: Supported
  - 48 Mbps: Supported
  - 54 Mbps: Supported

Below the Data Rates section is the **CCX Location Measurement** section:

- Mode:  Enabled
- Interval (seconds):

A note at the bottom states: **\*\* Data Rate 'Mandatory' implies that clients who do not support that specific rate will not be able to associate. Data Rate 'Supported' implies that any associated client that also supports that same rate may communicate with the AP using that rate. But it is not required that a client be able to use the rates marked supported in order to associate**

## Auto RF

When using the Cisco Unified Wireless LAN Controller it is recommended to enable Auto RF to manage the channel and transmit power settings. If electing to utilize the Auto-RF feature on the Cisco Unified Wireless LAN Controller, it is recommended to use version 4.1.185.0 or later.

**CISCO** MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Wireless 802.11a > RRM > Tx Power Control(TPC)

**Tx Power Level Assignment Algorithm**

Power Level Assignment Method  Automatic  On Demand  Fixed Every 600 sec

[Invoke Power Update now](#)

1

Power Threshold -65 dBm

Power Neighbor Count 3

Power Assignment Leader 00:1f:ca:be:c4:e0

Last TPC Iteration 192 secs ago

**CISCO** MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Wireless 802.11a > RRM > Dynamic Channel Assignment (DCA)

**Dynamic Channel Assignment Algorithm**

Channel Assignment Method  Automatic  Freeze  OFF Interval: 10 minutes AnchorTime: 0

[Invoke Channel Update Once](#)

Avoid Foreign AP interference  Enabled

Avoid Cisco AP load  Enabled

Avoid non-802.11a noise  Enabled

Channel Assignment Leader 00:1f:ca:be:c4:e0

Last DCA Iteration 319 secs ago

DCA Channel Sensitivity Medium (20 dB)

Channel Width  20 MHz  40 MHz

**DCA Channel List**

DCA Channels 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161

Select	Channel
<input checked="" type="checkbox"/>	36
<input checked="" type="checkbox"/>	40
<input checked="" type="checkbox"/>	44
<input checked="" type="checkbox"/>	48
<input checked="" type="checkbox"/>	52

Individual access points can be configured to override the global setting to use dynamic channel and transmit power assignment.

Other access points enabled can be enabled for Auto RF and workaround the access points that are statically configured. This may be necessary if there is an intermittent interferer present in an area.

The screenshot shows the Cisco configuration interface for a radio. The left sidebar contains a navigation menu with options like 'Access Points', 'Mesh', 'HREAP Groups', '802.11a/n', '802.11b/g/n', 'Country', 'Timers', and 'QoS'. The main content area is titled '802.11a/n Cisco APs > Configure'. It is divided into several sections: 'General' (AP Name: sjc21-21a-air13, Admin Status: Enable, Operational Status: UP), '11n Parameters' (11n Supported: No), 'Antenna Parameters' (Antenna Type: Internal, Diversity: Enabled), and 'WLAN Override' (WLAN Override: disable). On the right side, there are three sections: 'RF Channel Assignment' (Current Channel: 36, Assignment Method: Global), 'Tx Power Level Assignment' (Current Tx Power Level: 1, Assignment Method: Global), and 'Performance Profile' (View and edit Performance Profile for this AP, with a 'Performance Profile' button). A note at the bottom right states: 'Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.'

## DFS (802.11h)

Channel announcement and quiet mode should be enabled.

In versions prior to 5.0, power constraint (TPC) was a configurable option. Power constraint should be left un-configured as DTPC will be used by the Cisco Unified Wireless IP Phone 7921G to control the transmission power.

The screenshot displays the Cisco WLC configuration interface. The top navigation bar includes links for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar shows the configuration tree under 'Wireless', with '802.11a/n' expanded to show 'RRM' and 'DFS (802.11h)'. The main content area is titled '802.11h Global Parameters' and contains a section for 'Channel Switch Announcement' with two checked checkboxes: 'Channel Announcement' and 'Channel Quiet Mode'.

## Call Admission Control Settings

To enable Call Admission Control (TSPEC), you must configure maximum bandwidth and roaming bandwidth percentages for voice.

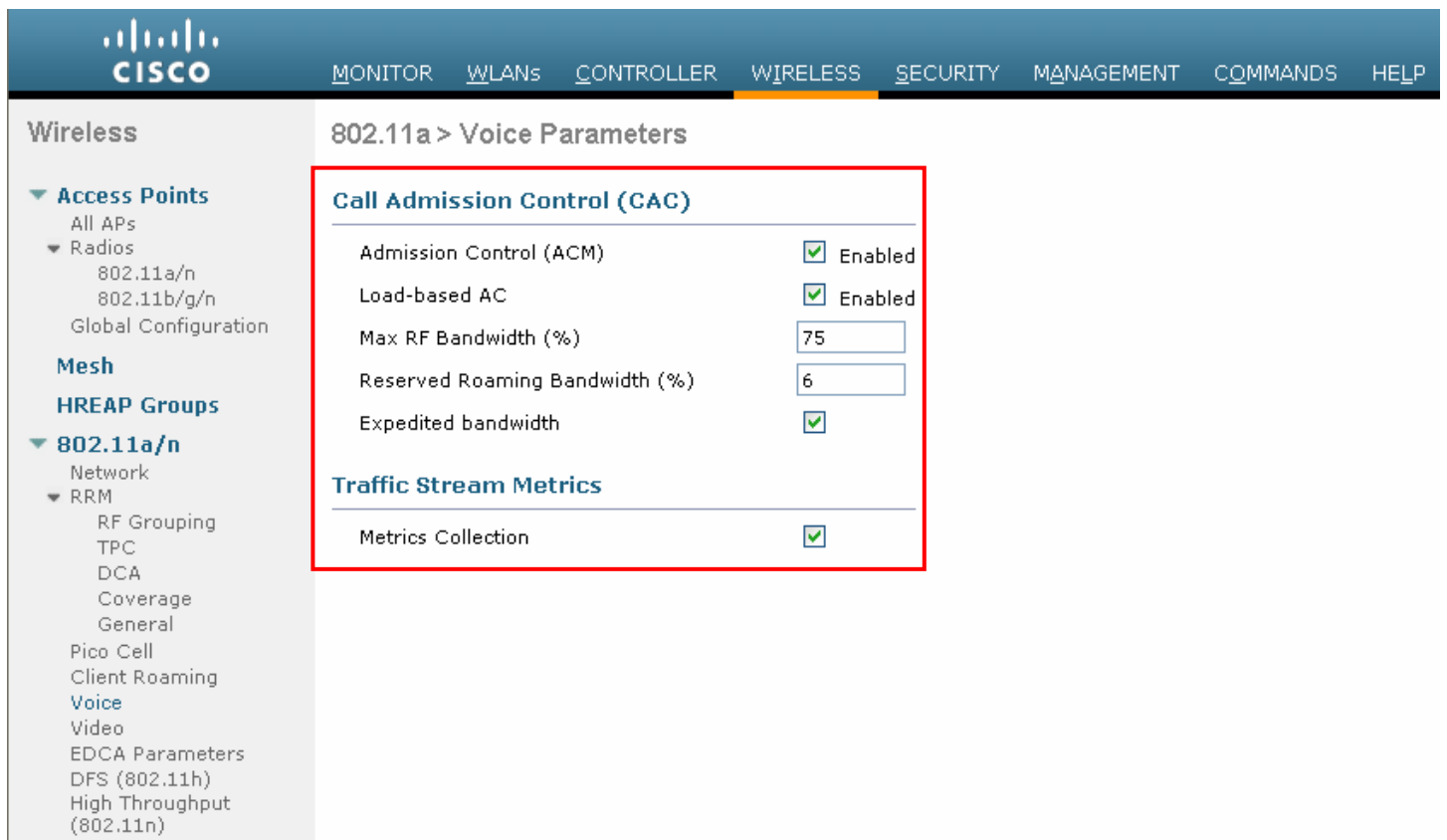
Maximum bandwidth default setting for voice is **75%**, and **6%** of that bandwidth is reserved for roaming clients.

Roaming clients are not limited to using the reserved roaming bandwidth, but is to reserve some bandwidth in case all other bandwidth is utilized.

Will want to ensure load-based CAC is enabled, which is available in the 4.1 release for the Cisco Unified Wireless LAN Controller, but not currently available on the autonomous access point platform.

Load-based CAC will account for non-TSPEC clients as well as other energy on the channel.

The AP1000 does not support load-based CAC as of release 4.1.185.0.



After enabling Call Admission Control, the following configuration should be enabled, which can be displayed in the “show run-config”.

```

Call Admission Control (CAC) configuration
Voice AC - Admission control (ACM)..... Enabled
Voice max RF bandwidth..... 75
Voice reserved roaming bandwidth..... 6
Voice load-based CAC mode..... Enabled
Voice tspec inactivity timeout..... Disabled
Video AC - Admission control (ACM)..... Disabled
Voice Stream-Size..... 84000
Voice Max-Streams..... 2
Video max RF bandwidth..... 25
Video reserved roaming bandwidth..... 6

```

The voice stream-size and voice max-streams values can be adjusted as necessary by using the following command.

```
config 802.11a cac voice stream-size 84000 max-streams 2
```

Ensure QoS is setup correctly under the WLAN / SSID configuration, which can be displayed via “show wlan <WLAN id>”.

```

Quality of Service..... Platinum (voice)
WMM..... Allowed

```

```
Dot11-Phone Mode (7920)..... ap-cac-limit
Wired Protocol..... 802.1P (Tag=6)
```

When enabling Call Admission Control on the autonomous access point, the admission must be unblocked on the SSID as well.

```
dot11 ssid voice
vlan 21
authentication open eap eap_methods
authentication network-eap eap_methods
authentication key-management wpa cckm
admit-traffic
```

Also ensure that the PHY rate configured on the Cisco Unified Wireless IP Phone 7921G is enabled as a nominal rate in the STREAM configuration of the autonomous access point.

Recommend to use the defaults, where 5.5, 6.0, 11.0, 12.0 and 24.0 Mbps are enabled as nominal rates for 802.11b/g and 6.0, 12.0 and 24.0 Mbps enabled for 802.11a.

If enabling the STREAM feature either directly or via selecting “Optimized Voice” for the radio access category in the QoS configuration section, ensure that only voice packets (RTP) are being put into the voice queue. Signaling packets (SCCP) should be put into a separate queue. This can be ensured by setting up a QoS policy mapping the DSCP to the correct queue.

For more information about Call Admission Control and QoS, refer to the “Configuring QoS” chapter in the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* at this URL:

[http://www.cisco.com/en/US/docs/wireless/access\\_point/12.3\\_8\\_JA/configuration/guide/s38qos.html](http://www.cisco.com/en/US/docs/wireless/access_point/12.3_8_JA/configuration/guide/s38qos.html)

## Configuring QoS Basic Service Set (QBSS)

There are three different versions of QoS Basic Service Set (QBSS) that the Cisco Unified Wireless IP Phone 7921G supports.

The first version from Cisco was on a 0-100 scale and was not based on clear channel assessment (CCA), so it does not account for channel utilization, but only the 802.11 traffic traversing that individual access point’s radio. So it does not account for other 802.11 energy or interferers using the same frequencies. The max threshold is defined on the client side, which is set to 45. This would allow for up to 7 calls at 11 Mbps plus some background traffic.

QBSS is also a part of 802.11e, which is on a 0-255 scale and is CCA based. So this gives a true representation on how busy the channel is. The max threshold is also defined on the client side, which is set to 105.

The second version from Cisco is based on the 802.11e version, but allows the default max threshold of 105 to be optionally configured.

Each version of QBSS can be optionally be configured on the access point.

For the Cisco Unified Wireless LAN Controller, enabling WMM will enable the 802.11e version of QBSS. There are also the “7920 Client CAC” and “7920 AP CAC” options, where “7920 Client CAC” will enable Cisco version 1 and “7920 AP CAC” enables Cisco version 2. See the “[SSID / WLAN QoS Settings](#)” section for more info.

For the Cisco Autonomous Access Point, “dot11 phone” or “dot11 phone dot11e” will enable QBSS.

“Dot11 phone” will enable the 2 Cisco versions, where “dot11 phone dot11e” will enable both CCA versions (802.11e and Cisco version 2). It is recommended to enable “dot11 phone dot11e”.

The screenshot shows the configuration interface for a Cisco Aironet 1200 Series Access Point. The 'ADVANCED' tab is selected, and the 'QoS POLICIES' section is active. The hostname is 'sjc21-12a-ap5'. Under 'Services: QoS Policies - Advanced', the 'IP Phone' section is expanded, and 'QoS Element for Wireless Phones' is highlighted with a red box. It shows 'Enable' selected with a radio button, and 'Dot11e' checked with a checkbox. Below this, 'IGMP Snooping' is shown with 'Snooping Helper' set to 'Enable'. 'AVVID Priority Mapping' is shown with 'Map Ethernet Packets with CoS 5 to CoS 6' set to 'No'. 'WiFi MultiMedia (WMM)' is shown with 'Enable on Radio Interfaces' checked for both 'Radio0-802.11G' and 'Radio1-802.11A'.

Below are the commands to change the QBSS max threshold for each platform type.

Cisco Unified Wireless LAN Controller = config advanced 802.11b 7920VSIEConfig call-admission-limit <value>

Cisco Autonomous Access Point = dot11 phone cac-thresh <value>

## Setting the Controller 802.1x Timeout

If using EAP, the 802.1x timeout on the controller (default = 2 seconds) should be increased.

The default timeout on the Cisco ACS server is 20 seconds, which is the recommended value

To change the 802.1x timeout on the Cisco Unified Wireless LAN Controller, 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
```

## Configuring Proxy ARP

To advertise the proxy ARP information element, ensure that Aironet extensions are enabled.

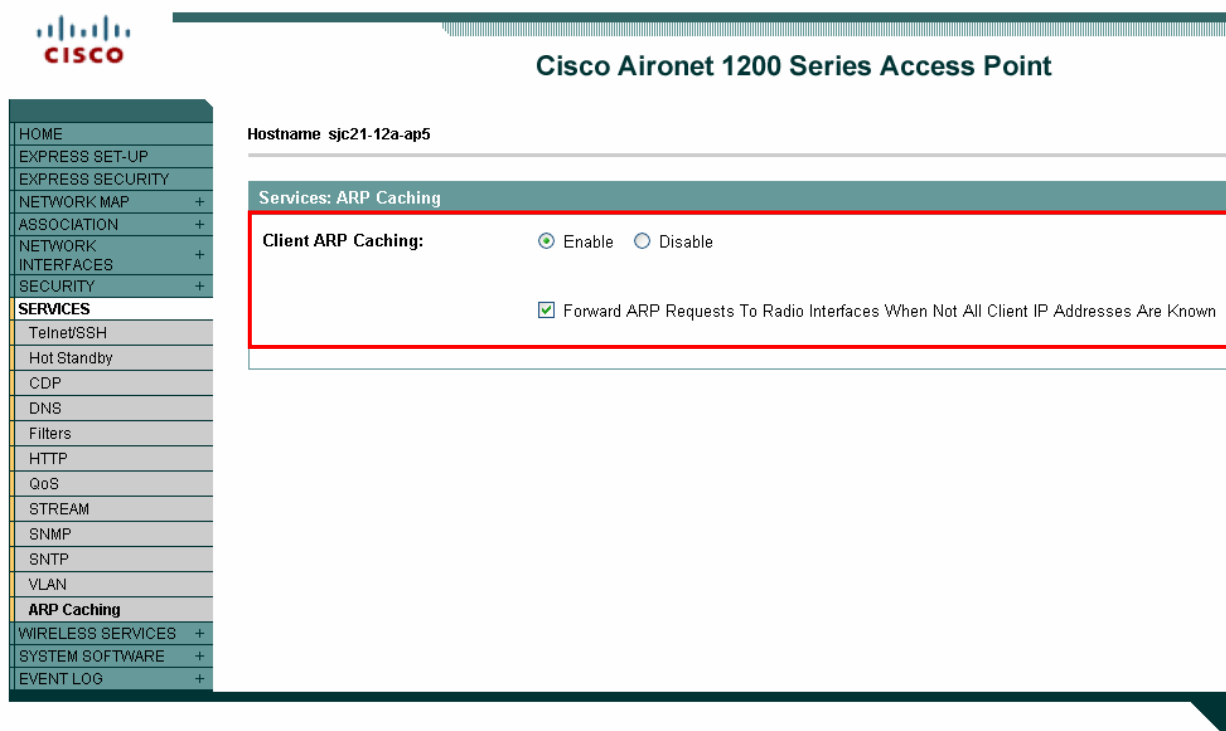
Ensure proxy ARP is enabled, where ARP Unicast Mode will be displayed as disabled on the Cisco Unified Wireless LAN Controller.

Telnet or SSH to the controller and enter “**show network**” or “**show network summary**” depending on the Cisco Unified Wireless LAN Controller version.

If ARP Unicast Mode is enabled, enter “**config network arpunicast disable**”.

In the 5.1.151.0 release, proxy ARP is always enabled and can not be disabled.

For autonomous access points, enter “**dot11 arp-cache optional**”.



The screenshot shows the configuration page for a Cisco Aironet 1200 Series Access Point. The page title is "Cisco Aironet 1200 Series Access Point" and the hostname is "sjc21-12a-ap5". The left sidebar contains a navigation menu with options like HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, Telnet/SSH, Hot Standby, CDP, DNS, Filters, HTTP, QoS, STREAM, SNMP, SNTP, VLAN, ARP Caching, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area is titled "Services: ARP Caching" and contains the following settings:

- Client ARP Caching:  Enable  Disable
- Forward ARP Requests To Radio Interfaces When Not All Client IP Addresses Are Known

## Configuring TKIP Countermeasure Holdoff Time

TKIP countermeasure mode can occur if the Access Point receives two message integrity check (MIC) errors within a 60 second period. When this occurs, the Access Point will de-authenticate all TKIP clients associated to that 802.11 radio and holdoff any clients for the countermeasure holdoff time (default = 60 seconds).

To change the TKIP countermeasure holdoff time on the Cisco Unified Wireless LAN Controller, telnet or SSH to the controller and enter the following command:

```
(Cisco Controller) >config wlan security tkip hold-down <nseconds> <wlan-id>
```

For the autonomous Access Point, enter the time in seconds to holdoff clients if a TKIP countermeasure event occurs.



```
Interface dot11radio X
  countermeasure tkip hold-time <nseconds>
```

For more information about these topics, refer to the *Enterprise Mobility Design Guide* at this URL:  
[http://www.cisco.com/application/pdf/en/us/guest/netso/ns279/c649/cemigration\\_09186a00808d9330.pdf](http://www.cisco.com/application/pdf/en/us/guest/netso/ns279/c649/cemigration_09186a00808d9330.pdf)

## VLANs and Autonomous Access Points

Segment wireless voice and data into separate VLANs.

When you have autonomous access points, use a dedicated native VLAN. Autonomous access points use Inter-Access Point Protocol (IAPP), which is a multicast protocol.

For the native VLAN, we recommend that you do not use VLAN1 to ensure that IAPP packets are exchanged successfully.

Ensure that Public Secure Packet Forwarding (PSPF) is not enabled for the voice VLAN as this will prevent clients from communicating directly when associated to the same access point. If PSPF is enabled, then the result will be no way audio.

The network ID in the SSID configuration, should only be disabled if Layer 3 mobility is enabled where the Wireless LAN Services Module (WLSM) is deployed.

## Configuring the Cisco Unified Wireless IP Phone 7921G

There are two methods for configuring network settings on the Cisco Unified Wireless IP Phone 7921G:

### Configuring Phones with the Keypad

You can use the menus and keypad on the phone by pressing **Settings > Network Profiles**. You need to unlock the screen by pressing **\*\*#**.

For more information, refer to the “Configuring Settings on the Cisco Unified Wireless IP Phone 7921G” in the *Cisco Unified Wireless IP Phone 7921G Administration Guide* at this URL:

[http://www.cisco.com/en/US/products/hw/phones/ps379/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/phones/ps379/prod_maintenance_guides_list.html)

### Configuring Phones with the Web Interface

The Cisco Unified Wireless IP Phone 7921G has an HTTPS enabled web interface that you can access via the 802.11a/b/g radio or USB.

If you are using the USB cable connection to a PC, you must manually set a static IP on the computer side, for example, 192.168.1.X /24. By default, the Cisco Unified Wireless IP Phone 7921G USB is statically set to 192.168.1.100 /24.

You must log in to the administration web pages by using these defaults:  
username is “**admin**” and the password is “**Cisco**”.

### Configuring Phones with Wavelink Avalanche

[Wavelink Avalanche](#) is a comprehensive management solution for the Wireless LAN enterprise providing complete visibility and control of Wireless LAN infrastructure and mobile client devices from a central console.

Wavelink Avalanche eases the configuration, deployment and management of Wireless LAN networks while offering extensive flexibility through the support of a wide range of mobile devices and infrastructure.

Refer to the [Wavelink](#) section below for more info.

For more information, refer to the “Using the Cisco Unified Wireless IP Phone 7921G Web Pages” in the *Cisco Unified Wireless IP Phone 7921G Administration Guide* at this URL:

[http://www.cisco.com/en/US/products/hw/phones/ps379/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/phones/ps379/prod_maintenance_guides_list.html)

## Configuring the Network Profile Parameters

Use these guidelines to configure network profiles.

- The Cisco Unified Wireless IP Phone 7921G supports multiple network profiles that allow one SSID per network profile.
- To extend battery life, use U-APSD mode for power save mode during active calls.  
Active mode “None” may need to be used instead of U-APSD/PS-POLL if the access point does not support power save enabled clients.
- 5 different 802.11 modes are available.
  - Auto-RSSI
  - 802.11a
  - 802.11bg
  - Auto-a
  - Auto-bg

Auto-RSSI mode will scan both 2.4 and 5 GHz channels and attempt to associate to the access point with the strongest signal if the configured network is available.

802.11a mode will only scan 5 GHz channels and 802.11bg mode will only scan 2.4 GHz channels, then will attempt to associate to an access point if the configured network is available.

For Auto-a and Auto-bg modes, this is giving preference to one band over another. At power on, will scan all 2.4 and 5 GHz channels then attempt to associate to an access point for the configured network using the preferred band if available. If the preferred band is not available, then the Cisco Unified Wireless Phone 7921G will try to use the less preferred band if available. If the phone roams out of coverage of the preferred band, where the less preferred band signal is available, then the phone will attempt to associate to that less preferred band. Once associated to the less preferred band, there is no mechanism to check if the preferred band is available again. For the phone to roam back to the preferred band, the less preferred band signal will have to be exhausted.

Some deployments may use one band for indoor (i.e. 5 GHz) and the other for outdoor coverage (i.e. 2.4 GHz). In this case, set the phone to either Auto-a or Auto-bg mode, depending on the preferred band. Then to ensure the phone is always associated to the preferred band, will need to ensure the less preferred band signal is not available, where the phone can then re-scan the preferred band and attempt to associate if the preferred band signal is available.

- Below are the available authentication and encryption configuration methods.

<b><u>Authentication</u></b>	<b><u>Encryption</u></b>
Open	N/A
Open+WEP	WEP (40 or 128 bit)
Shared Key	WEP (40 or 128 bit)
LEAP	WEP (40 or 128 bit), TKIP, AES
EAP-FAST	WEP (40 or 128 bit), TKIP, AES
EAP-TLS	WEP (40 or 128 bit), TKIP, AES
PEAP	WEP (40 or 128 bit), TKIP, AES
AKM	WEP (40 or 128 bit), TKIP, AES

**Note:** CCKM will be negotiated if enabled on the Access Point when using 802.1x authentication with LEAP, EAP-FAST, EAP-TLS, PEAP or AKM modes.

- If using 802.1x authentication via LEAP, EAP-FAST, PEAP or AKM (authenticated key-management) authentication modes, then you must configure a username and password. AKM mode will use LEAP as the 802.1x method.
- AKM mode requires a key management type to be enabled on the Access Point.
  - For 802.1x authentication methods, WPA, WPA2 or CCKM is required.
  - For non-802.1x authentication, WPA-PSK or WPA2-PSK is required.
- If using 802.11i (Pre-Shared key), enter the ASCII or hexadecimal formatted key.
- If using open authentication plus WEP encryption or shared key authentication, enter the static WEP key information that matches the access point configuration.
- Select whether to use Dynamic Host Configuration Protocol (DHCP) or configure static IP information.
- If option 150 or 66 is not configured to provide the TFTP server IP address via the network's DHCP scope, then enter the TFTP server IP address info.
- To enable PEAP with server validation, select "Validate Server Certificate" after importing the authentication server certificate.
- When using EAP-TLS, select either "Manufacturing Issued" or "User Installed" for the "Client EAP-TLS Certificate" option after selecting EAP-TLS.

**Note:** WEP128 is listed as WEP104 on the Cisco Unified Wireless LAN Controllers.



## Cisco Unified Wireless IP Phone 7921G

SEP0018BA78C222

Phone DN 23675

HOME
SETUP
<b>NETWORK PROFILES</b>
<b>Profile 1</b>
Profile 2
Profile 3
Profile 4
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

**Network Profile 1 Settings** [Advanced Profile 1](#)

**Wireless**

Profile Name:

SSID:

Call Power Save Mode:

802.11 Mode:

Scan Mode: **Auto**

Restricted Data Rates: **False**

**WLAN Security**

Security Mode:

Export Security Credentials:  True  False

**Wireless Security Credentials**

Username:

Password:

**WPA Pre-shared Key Credentials**

Pre-shared Key Type:  ASCII  Hex

Pre-shared Key:

**Wireless Encryption**

Key Type:  Hex  ASCII

	Transmit Key	Encryption Key	Key Size
Encryption Key 1	<input checked="" type="radio"/>	<input type="text"/>	<input checked="" type="radio"/> 40 <input type="radio"/> 128
Encryption Key 2	<input type="radio"/>	<input type="text"/>	<input checked="" type="radio"/> 40 <input type="radio"/> 128
Encryption Key 3	<input type="radio"/>	<input type="text"/>	<input checked="" type="radio"/> 40 <input type="radio"/> 128
Encryption Key 4	<input type="radio"/>	<input type="text"/>	<input checked="" type="radio"/> 40 <input type="radio"/> 128

Certificate Options	
Client EAP-TLS Certificate	Manufacturing Issued
Validate Server Certificate	<input type="radio"/> True <input checked="" type="radio"/> False
IP Network Configuration	
<input checked="" type="radio"/> Obtain IP address and DNS servers automatically	
<input type="radio"/> Use the following IP address and DNS servers	
IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Default Router	<input type="text"/>
Primary DNS Server	<input type="text"/>
Secondary DNS Server	<input type="text"/>
Domain Name	<input type="text"/>
TFTP	
<input checked="" type="radio"/> Obtain TFTP servers automatically	
<input type="radio"/> Use the following TFTP servers	
TFTP Server 1	<input type="text"/>
TFTP Server 2	<input type="text"/>

Copyright (c) 2006-2008 by Cisco Systems, Inc.

**Note:** If the TFTP IP is changed which is not included in the current Certificate Trust List (CTL) file, then TFTP will fail and may prevent the phone from registering successfully to the Cisco Unified Communications Manager. The CTL file will need to be erased manually in the Security Configuration menu from the Cisco Unified Wireless IP Phone 7921G.

## Configuring Advanced Network Profile Settings

In the Advanced Network Profile settings, you can adjust the PHY rate. If less than 12 Mbps is enabled in the wireless LAN, then you must configure this parameter.

By limiting number of channels to be scanned, this can help reduce the time for access point discovery while passively scanning DFS channels in 802.11a mode. This can also help preserve battery life.

If using this feature, then only disable those channels that are not used in the wireless LAN. If you disable a channel that is currently used by an access point, then the Cisco Unified Wireless IP Phone 7921G might not associate to the wireless LAN successfully.

If all channels that are used in the wireless LAN are disabled on the phone, then use one of these methods to browse to the Cisco Unified Wireless IP Phone 7921G webpage:

- USB cable connected to the PC where full web access was previously enabled
- Re-enable all channels by using the factory default



# Cisco Unified Wireless IP Phone 7921G

SEP0018BA78C222

Phone DN 23675

HOME
SETUP
<b>NETWORK PROFILES</b>
Profile 1
Profile 2
Profile 3
Profile 4
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

Network Profile 1 Advanced Settings [Basic Profile 1](#)

**TSPEC Settings**

Minimum PHY Rate: 12 Mbps

Surplus Bandwidth: 1.300000

**Antenna Settings**

Antenna Selection for 802.11A: Diversity

Antenna Selection for 802.11G: Vertical

**802.11 G Power Settings**

Channel	Enabled	Max Tx Power	Channel	Enabled	Max Tx Power
1	<input checked="" type="checkbox"/>	17 dBm	2	<input checked="" type="checkbox"/>	17 dBm
3	<input checked="" type="checkbox"/>	17 dBm	4	<input checked="" type="checkbox"/>	17 dBm
5	<input checked="" type="checkbox"/>	17 dBm	6	<input checked="" type="checkbox"/>	17 dBm
7	<input checked="" type="checkbox"/>	17 dBm	8	<input checked="" type="checkbox"/>	17 dBm
9	<input checked="" type="checkbox"/>	17 dBm	10	<input checked="" type="checkbox"/>	17 dBm
11	<input checked="" type="checkbox"/>	17 dBm	12	<input checked="" type="checkbox"/>	17 dBm
13	<input checked="" type="checkbox"/>	17 dBm	14	<input checked="" type="checkbox"/>	17 dBm

**802.11 A Power Settings**

Channel	Enabled	Max Tx Power	Channel	Enabled	Max Tx Power
36	<input checked="" type="checkbox"/>	17 dBm	40	<input checked="" type="checkbox"/>	17 dBm
44	<input checked="" type="checkbox"/>	17 dBm	48	<input checked="" type="checkbox"/>	17 dBm
52	<input checked="" type="checkbox"/>	17 dBm	56	<input checked="" type="checkbox"/>	17 dBm
60	<input checked="" type="checkbox"/>	17 dBm	64	<input checked="" type="checkbox"/>	17 dBm
100	<input checked="" type="checkbox"/>	17 dBm	104	<input checked="" type="checkbox"/>	17 dBm
108	<input checked="" type="checkbox"/>	17 dBm	112	<input checked="" type="checkbox"/>	17 dBm
116	<input checked="" type="checkbox"/>	17 dBm	120	<input checked="" type="checkbox"/>	17 dBm
124	<input checked="" type="checkbox"/>	17 dBm	128	<input checked="" type="checkbox"/>	17 dBm
132	<input checked="" type="checkbox"/>	17 dBm	136	<input checked="" type="checkbox"/>	17 dBm
140	<input checked="" type="checkbox"/>	17 dBm	149	<input checked="" type="checkbox"/>	17 dBm
153	<input checked="" type="checkbox"/>	17 dBm	157	<input checked="" type="checkbox"/>	17 dBm
161	<input checked="" type="checkbox"/>	17 dBm			

Save

Copyright (c) 2006-2008 by Cisco Systems, Inc.

## Installing Certificates

Extensible Authentication Protocol Transport Layer Security (EAP-TLS) is using the TLS protocol with PKI to secure communications to the authentication server.

TLS provides a way to use certificates for both user and server authentication and for dynamic session key generation.

EAP-TLS provides excellent security, but requires client certificate management.

Can utilize either the internal MIC (Manufacturing Installed Certificate) or install an alternate certificate to be used for authentication.

To use the MIC in the Cisco Unified Wireless IP Phone 7921G, the Manufacturing Root and Manufacturing CA certificates must be exported and installed onto the RADIUS server.

**Cisco Unified Wireless IP Phone 7921G**  
SEP0018BA78C222

Phone DN 23675

Certificates					
Type	Common Name	Issuer Name	Valid From	Valid To	
User Installed	<not installed>	<not installed>			Install
Manufacturing Issued	/O=Cisco Systems Inc./OU=EVVBU/CN=CP-7921G-SEP0018BA78C222	/O=Cisco Systems/CN=Cisco Manufacturing CA	02/10/2007 01:50:05	02/10/2017 02:00:05	
Authentication Server Root	/CN=ACS40	/CN=ACS40	10/01/2007 07:16:00	09/30/2008 07:16:00	Install Delete
Manufacturing Root	/O=Cisco Systems/CN=Cisco Root CA 2048	/O=Cisco Systems/CN=Cisco Root CA 2048	05/14/2004 20:17:12	05/14/2029 20:25:42	Export
Manufacturing CA	/O=Cisco Systems/CN=Cisco Manufacturing CA	/O=Cisco Systems/CN=Cisco Root CA 2048	06/10/2005 22:16:01	05/14/2029 20:25:42	Export

Copyright (c) 2006 by Cisco Systems, Inc.

After selecting “Export”, import the certificates into the RADIUS server and enable them in the certificate trust list.

For the user installed certificate method, select “Install” on the main certificates page, which will launch the installation wizard.

To generate the certificate signing request, enter the certificate information and import the certificate from the Certificate Authority server that is signing the certificate.

The Common Name defaults to “CP-7921G-SEP<MAC\_Address>”, but can be customized.

Browse to the Certificate Authority certificate and select “Submit”.



# Cisco Unified Wireless IP Phone 7921G

SEP0018BA78C222

Phone DN 23675

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
<b>CERTIFICATES</b>
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

### User Certificate Installation

**Step 1 of 4: Enter Identification Information**

**Common Name**

**Organization**

**Organization Unit**

**City**

**State**

**Country**

**Key Size**

---

**Step 2 of 4: Import Certificate Authority File**

**Certificate Authority File**

Click the "Submit" button to submit all the above information and start generating a Certificate Signing Request data. This process may take a while to complete.

Copyright (c) 2006-2008 by Cisco Systems, Inc.

After "Submit" is selected, the certificate will then be generated.

The certificate will then be displayed and is now ready to be signed.

Select all of the certificate data in order to copy it to the Certificate Authority server to be signed.



# Cisco Unified Wireless IP Phone 7921G

SEP0018BA78C222

Phone DN 23675

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
<b>CERTIFICATES</b>
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

### User Certificate Installation

**Step 3 of 4: Signing the Certificate**

Please copy the generated Certificate Signing Request below and submit it to your Certificate Authority Server.  
Please create the Signed Certificate in DER encoded format for this phone.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDNzCCAhsCAQAwDQELMAkGA1UEBhMCVVMxGzAxBgNVBAGTAkNBHREwDwYDVQOH
EvhNaUxwaXRhezEOMAwGA1UEChMFQ2IzY28xMjY1MBgNVBAsTBTU1Q00JVHSEwHwYD
VQDDExhdUC03OTIzRy1TRVAvMDE4QkE3OEYyMjIwggE1MA0GCSqGSIb3DQEBBQUA
A4IBDwAwggEKAoIBAQcduAVYAUjd/Q7L3gjSE7wYBN9126hNtdnrEbbk1qI51dp
YETE4Hx1+oqC995j2zxdG4WCQZBYN+/26xcRuYs0Wk3/1zD2VifsbMYLR01So8rx
lkrmuLL27znfFYkplGBup2e9PaKC30sqIcMhcIwJ7Cj7wD21181K26VDjzezv+Cc
FVAG4esAQXL+VmdJr6DIcM6LMPuFQZHjZwrbvNt1cypqU2I2pM6KytZ1TUQ2psIp
1Irgj/cJvhJe8T14UCpNKKXjgMrxfTOMGz6e3FRBzIGfCnQj3v6gMfkQj2kca01u
Vg1frBt3h20Q9qRnjGdW96exLJXBNFfKvrXAb3bnAgMBAAGggYewfwYJKoZIhvcN
AQkOMXlwcDAMBgNVHRMBAf8EAjAAACQGA1UdEQQdMBuGGUNQLTcSMjFHLVNFUDAw
MThQTC4QzIyMgAwDgYDVPROAQH/BAQDAgP4MCoGA1UdJQEB/wQgMB4GCCsGAQUF
BwMBBggrBgEFBQcDAgYIKwYBBQUHAWUwDQYJKoZIhvcNAQEFBQADggEBAAG4m/Y3
vMtwLcyYIA6Z1vO/RkdqPXFrlxUrATZ9n0cYVtu15DeA39kc6sgpcwu++MzvvEH
FjYlLmAmBj5QU6nhExl6j8+vtxwU8tZp/jNvjbaqdgQ1Ca++QP45Or6dxA65SR7+g
```

\* If you need more time to complete the above step of creating Signed Certificate, you may select the "Postpone" button and attempt the Import step at later time. [Note: Select the "Install" option again in the main Certificates page to resume the installation step after you had postponed it.]

\* If you ready have the Signed Certificate for this phone, you may select the "Import Step" button to continue with the installation steps.

Copyright (c) 2006 by Cisco Systems, Inc.



Select the method to submit a certificate request by using a base-64-encoded PKCS file.

Paste the certificate data from the Cisco Unified Wireless IP Phone 7921G to the Certificate Authority signing server and submit for signing

### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

#### Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

[Browse for a file to insert.](#)

#### Additional Attributes:

Attributes:

Submit >

When the certificate has been signed, download the CA certificate in DER encoded format (base 64 encoded not supported).

Ensure Client Authentication is listed in the Enhanced Key Usage section of the certificate details.

After selecting "Import Step", browse to the signed user certificate and select "Import" to complete the process.



## Cisco Unified Wireless IP Phone 7921G

SEP0018BA78C222

Phone DN 23675

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
<b>CERTIFICATES</b>
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

### User Certificate Installation

#### Final Step: Import Signed Phone Certificate (DER encoded format)

Certificate File To Install

Please click the "Import" button below to install the Signed Certificate into the phone.

Copyright (c) 2006 by Cisco Systems, Inc.

Once the certificate is installed successfully, a confirmation page will be displayed.

The CA chain should already be enabled in the authentication server's certificate trust list.

The authentication server certificate must also be imported into the Cisco Unified Wireless IP Phone 7921G for both methods. If the authentication server certificate was signed by a Certificate Authority (CA) server, then that DER encoded root certificate will need to be imported into the Cisco Unified Wireless IP Phone 7921G.

If the Cisco Unified Wireless IP Phone 7921G has not registered to a Cisco Unified Communications Manager yet, then the date and time must be configured manually for the first time.



## Cisco Unified Wireless IP Phone 7921G

SEP0018BA78C222

Phone DN 23675

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
<b>DATE &amp; TIME</b>
PHONE RESTART

### Date & Time Settings

#### Current Phone Date & Time

October 31, 2007 20:30:30

**Note: Phone Date & Time may change when phone registered with Cisco Unified Communications Manager**

#### Local Date & Time

October 31, 2007 20:29:06

#### Specify Date & Time

Date:

Time:  hours(24 hrs)  minutes  seconds

**NOTE:** After changing the Date & Time, you must execute **"SYSTEM / PHONE RESTART"** before the new time can be used to validate Certificates.

Copyright (c) 2006 by Cisco Systems, Inc.

The Cisco Unified Wireless IP Phone 7921G must be restarted after installing the certificate. Click on the hyperlink to navigate to the "Phone Restart" page.



## Cisco Unified Wireless IP Phone 7921G

SEP0018BA78C222

Phone DN 23675

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
<b>PHONE RESTART</b>

### Authentication Server Root Certificate

**Authentication Root certificate installed successfully.**  
Phone will use this new certificate after reboot. You can restart the phone with:  
**"SYSTEM / PHONE RESTART"**

Copyright (c) 2006 by Cisco Systems, Inc.

Click the "Restart" button to power cycle the phone.

## Using Templates to Configure Phones

Phone configuration templates can be exported and imported to other phones for quick configuration. The phone configuration template will be encrypted using the specified encryption key (8-20 characters).

For security reasons, the Wireless LAN security information (Username/Password, WPA Pre-shared key information, and WEP key information) is not exported by default. In order to export this Wireless LAN security information, the network profile must be configured to allow this capability. For each network profile where the Wireless LAN security information is to be exported, configure the [“Export Security Credentials”](#) option to **“True”**. After selecting **“True”**, you will need to enter the Wireless LAN security information again. This will then allow that information to be exported and then imported to other Cisco Unified Wireless IP Phone 7921G phones.

The screenshot displays the configuration page for a Cisco Unified Wireless IP Phone 7921G. The page title is "Cisco Unified Wireless IP Phone 7921G" with the phone ID "SEP0018BA78C222" and "Phone DN 23675". A left-hand navigation menu lists various settings categories, with "BACKUP SETTINGS" highlighted. The main content area is divided into two sections: "Import Configuration" and "Export Configuration". Both sections feature an "Encryption Key" input field and an "Import File" field with a "Browse..." button. The "Import Configuration" section includes an "Import" button, while the "Export Configuration" section includes an "Export" button. At the bottom of the page, a copyright notice reads: "Copyright (c) 2006-2008 by Cisco Systems, Inc."

## Upgrading Phone Firmware

To install the phone firmware, run the executable for Cisco Unified Communications Manager version 4.1, 4.2 and 4.3 or install the COP file for versions 5.0, 5.1, 6.0, 6.1, 7.0 and later.

There are two methods for upgrading Cisco Unified Wireless IP Phone 7921G firmware.

### Wireless TFTP

During TFTP server download, the phone configuration file is parsed and the device load is identified. The phone downloads the firmware files to flash if it is not running the specified image already.

Cisco Unified Communications Manager device load takes precedence over the TFTP firmware version.

You can specify the Load Server as an alternate TFTP server to retrieve firmware files in the Cisco Unified Wireless IP Phone 7921G product specific configuration in Cisco Unified Communications Manager Administration.

### Web Interface

You can upload the firmware to the phone by using the web interface option, Phone Upgrade and browsing to the firmware TAR file.

**Note:** If the Cisco Unified Wireless IP Phone 7921G registers to Cisco Unified Communications Manager, web access to the Cisco Unified Wireless IP Phone 7921G gets set to read-only mode. In this mode, you are not allowed access to upgrade firmware.

To install the firmware on Cisco Unified Communications Manager Express, extract the contents of the TAR file and upload into the router's flash. Each file will need to be enabled for TFTP download. Configure the phone load and reset the phones to upgrade the firmware.

Example below:

```
tftp-server flash: Cp7921g-1.2.1.LOADS
tftp-server flash:Apps-1.2.1.SBN
tftp-server flash:Gui-1.2.1.SBN
tftp-server flash:Sys-1.2.1.SBN
tftp-server flash:Tnux-1.2.1.SBN
tftp-server flash:Tnuxr-1.2.1.SBN
tftp-server flash:Wlan-1.2.1.SBN
!
telephony-service
load 7921 Cp7921g-1.2.1.LOADS
```

## Wavelink Avalanche

The Wavelink Avalanche server IP address can be set either via DHCP option 149 or statically.

To provide the server IP address automatically, configure option 149 on the DHCP server.

```
ip dhcp pool 10.10.11.0
network 10.10.11.0 255.255.255.0
default-router 10.10.11.1
dns-server 10.10.10.20
domain-name cisco.com
option 150 ip 10.10.10.22
option 149 ip 10.10.11.128
```

Custom parameters can also be set via the Cisco Unified Wireless IP Phone 7921G web page in order to help group clients for better management.



### Cisco Unified Wireless IP Phone 7921G

SEP0018BA78C222

Phone DN 23675

- HOME
- SETUP
- NETWORK PROFILES +
- USB SETTINGS
- TRACE SETTINGS
- WAVELINK SETTINGS**
- CERTIFICATES
- CONFIGURATIONS
- PHONE BOOK +
- INFORMATION
- NETWORK
- WIRELESS LAN
- DEVICE
- STATISTICS
- WIRELESS LAN
- NETWORK
- STREAM STATISTICS
- STREAM 1
- STREAM 2
- SYSTEM
- TRACE LOGS
- BACKUP SETTINGS
- PHONE UPGRADE
- CHANGE PASSWORD
- SITE SURVEY
- DATE & TIME
- PHONE RESTART

#### Wavelink Settings

Server Enabled  True  False

Enabler Version 3.11-01

Obtain Server address automatically

Use the following Server

IP Address

#### Wavelink Custom Parameters

Parameter 1

Name

Value

Parameter 2

Name

Value

Parameter 3

Name

Value

Parameter 4

Name

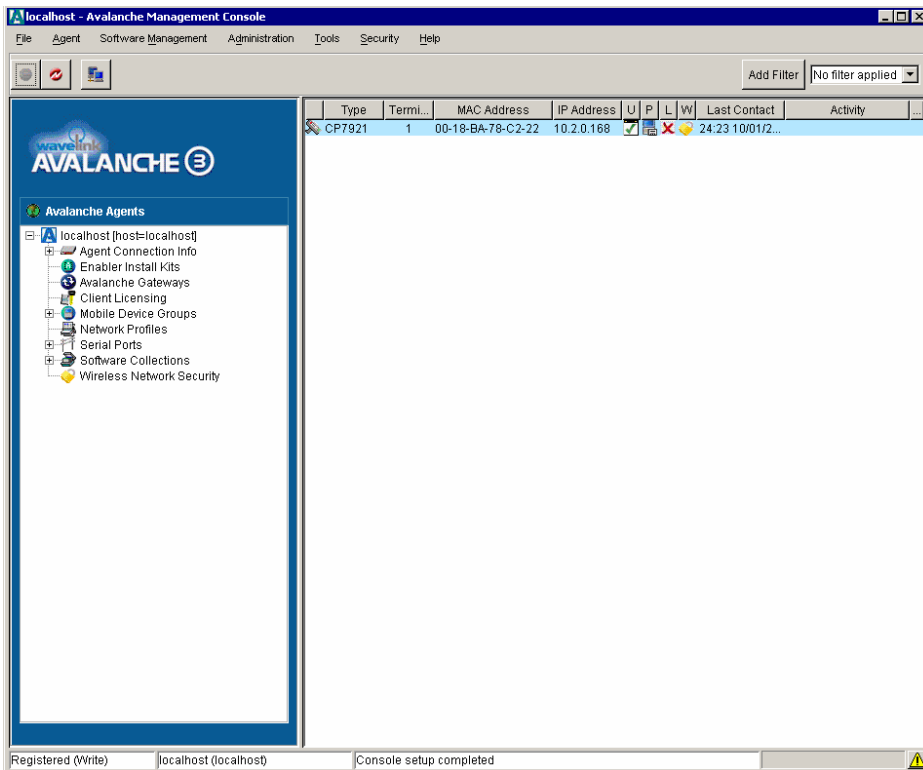
Value

Save

Copyright (c) 2006 by Cisco Systems, Inc.

When clients register with the Wavelink server, they will appear in the console.

To set client properties right click on the client and select "Client Settings".

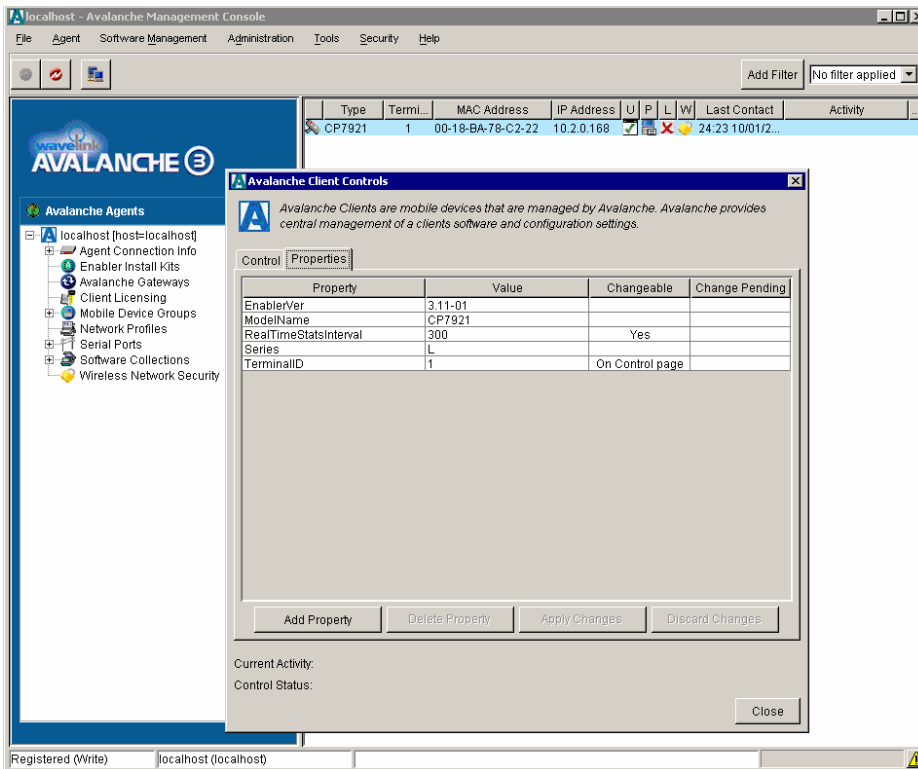


The Cisco Unified Wireless IP Phone 7921G will have parameters enabled by default.

EnablerVer = 3.11-01

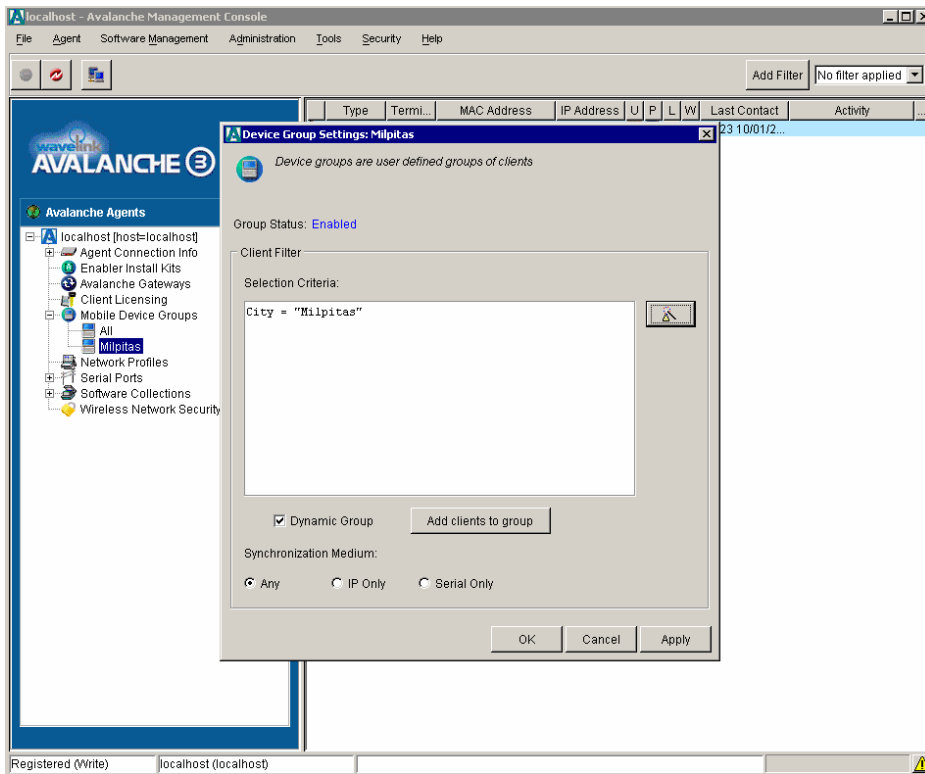
ModelName = CP7921G

Additional properties can be added as necessary for better client management.



Mobile Device Groups can be created to group clients based on client properties.

Enter the selection criteria either manually or using the wizard after right clicking on the mobile device group and selecting "Settings".



To install the 7921G Configuration Utility for Wavelink Avalanche, select “Install Software Package” under the Software Management menu.

Browse to the 7921G Configuration Utility package file (i.e. 7921CU-1.2.1.AVA).

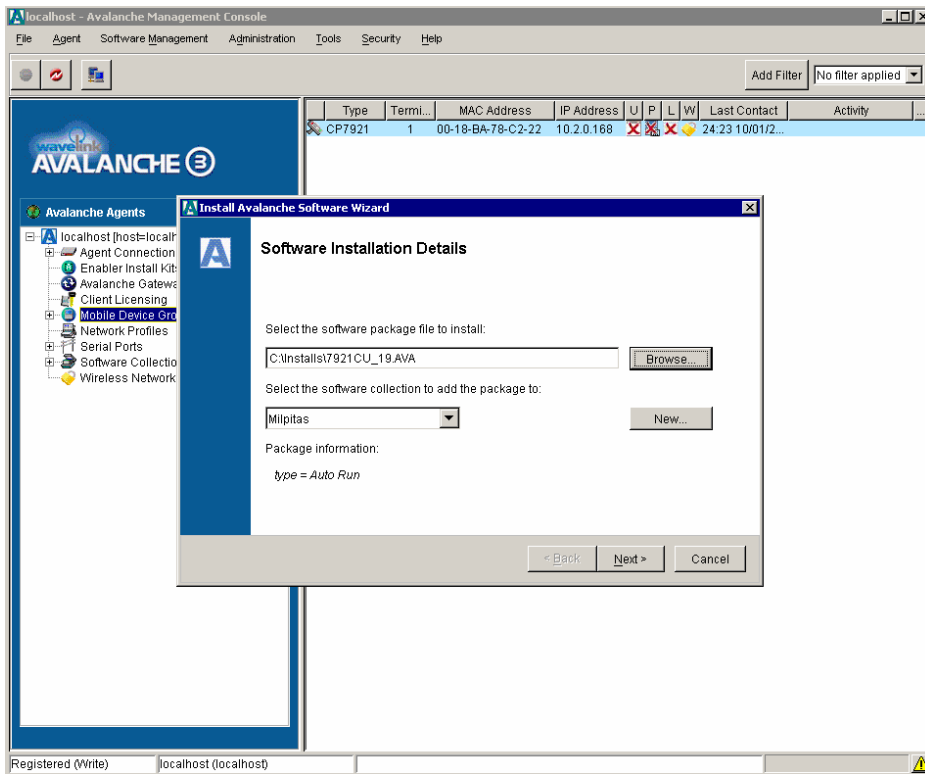
Create a software collection to add the package to.

The license agreement will be displayed, after selecting “Next”,

Click on “Finish” when the installation is complete.

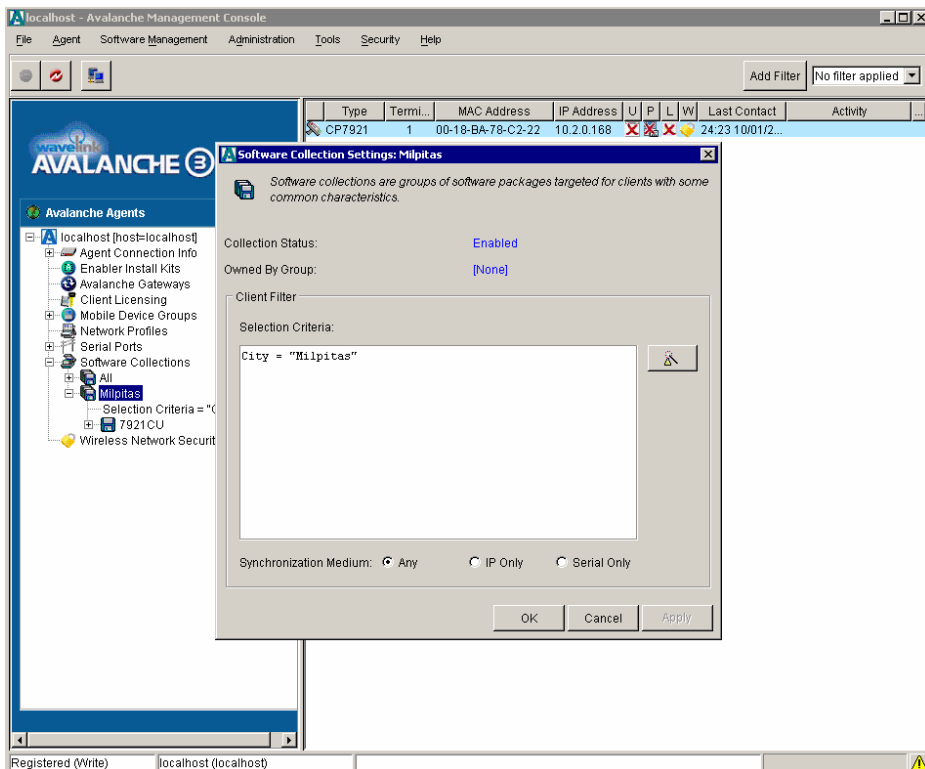
**Note:** The 7921CU must be installed locally on the Wavelink Avalanche server.



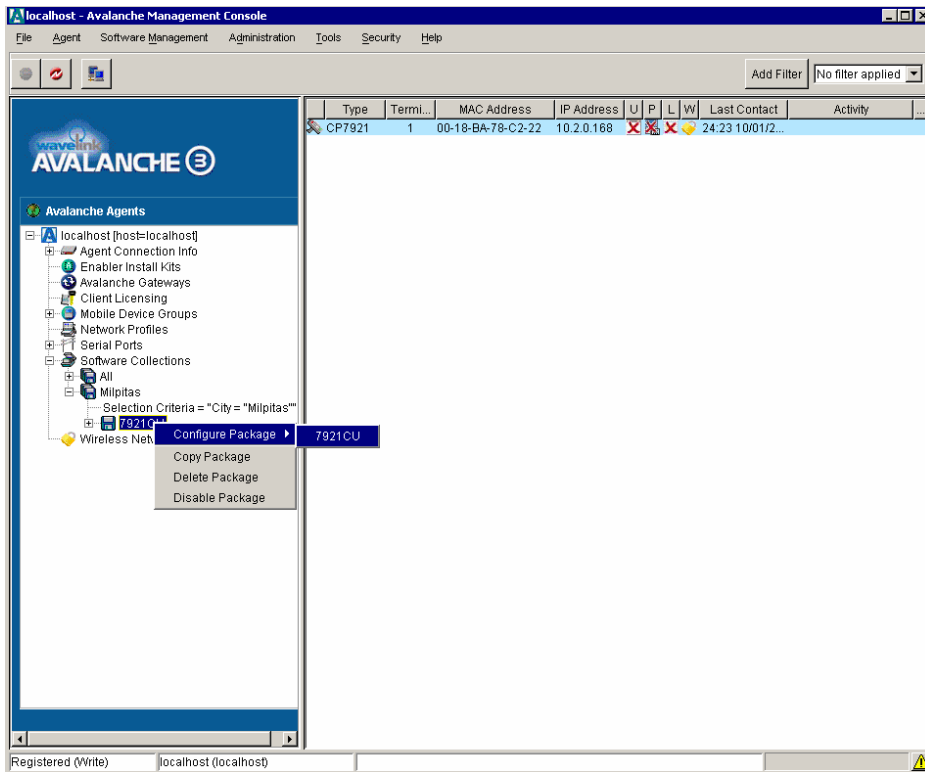


The software package must then be enabled by right clicking on the package and selecting “Enable Package”.

Selection collections can also be created with their own selection criteria to determine which clients should receive the software package.

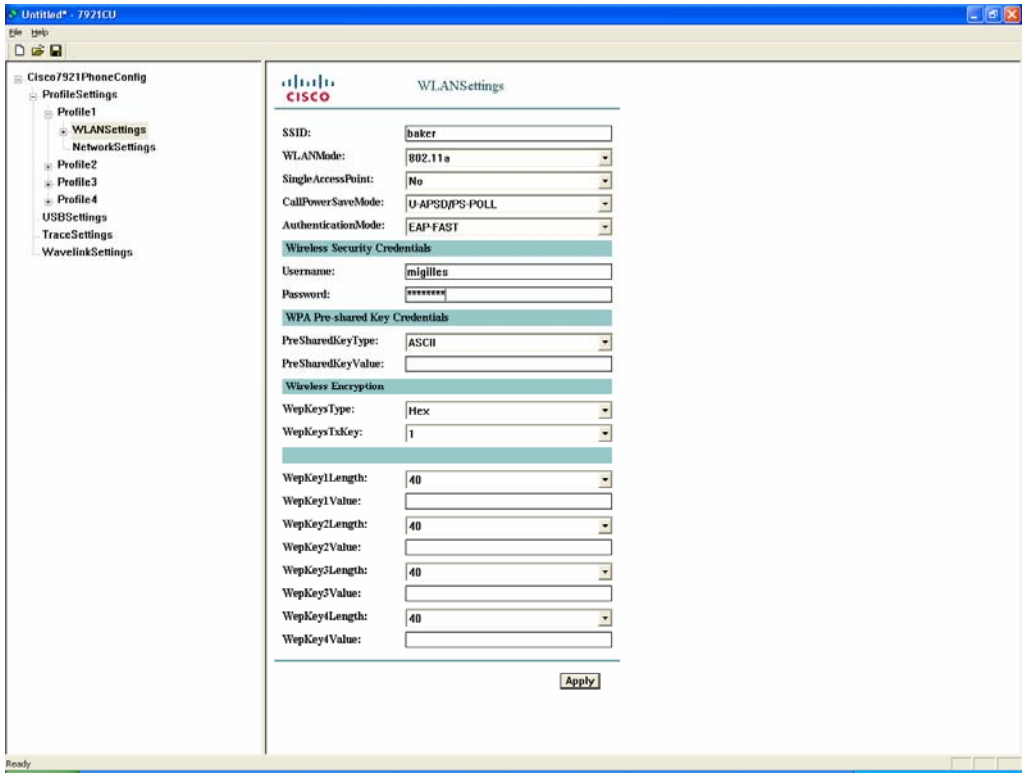


To configure the software package, right click on the package and select “7921CU”. The 7921G Configuration Utility will then be launched.

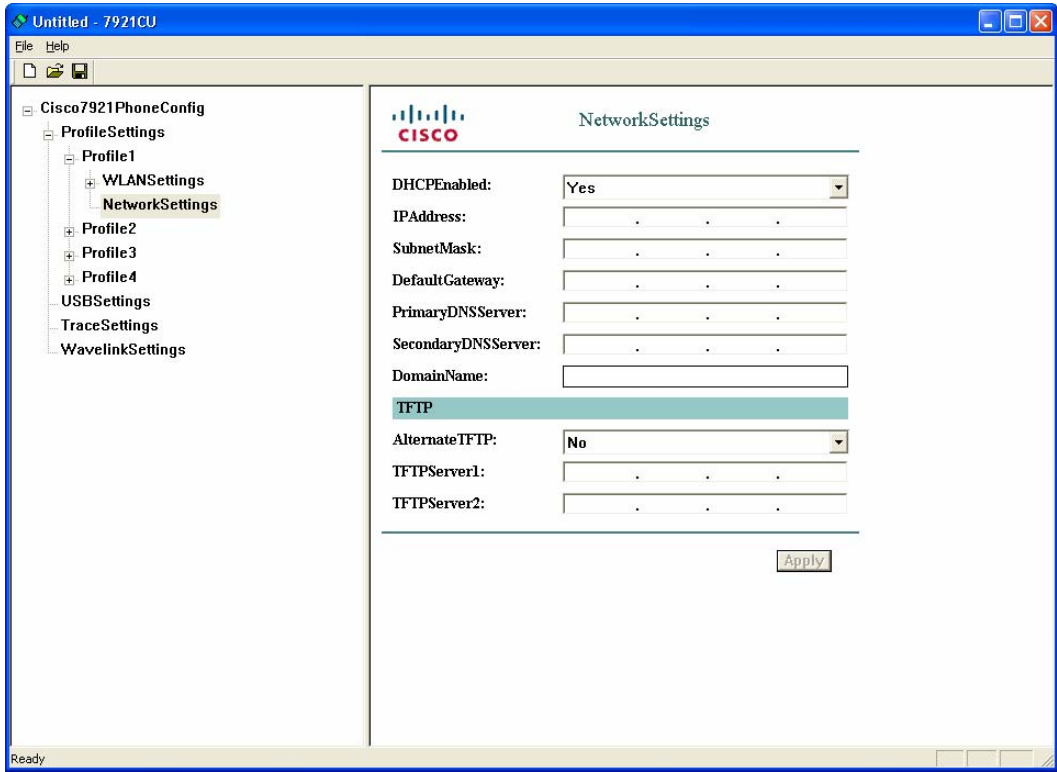


Enter the profile name and enable the profile.

Configure the network profiles by specifying the Wireless LAN credentials.



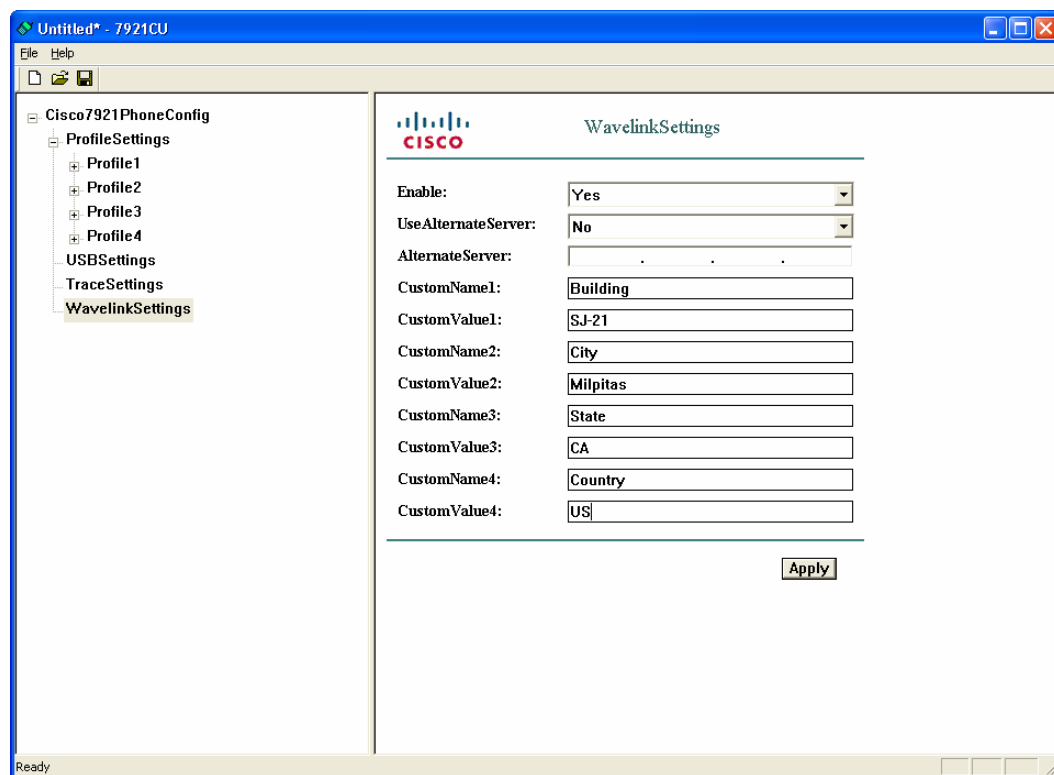
Configure the network settings for the network profile.



Ensure that Wavelink server enable is set to “Yes”.

Configure whether the client will get the Wavelink IP info from DHCP or configured statically.

Optionally set additional client parameters as necessary.



When the template has been completely configured, then select “Export to Wavelink” under the File menu.

A confirmation will then be displayed after the template has been exported successfully.

After the template has become available, will then need to push the package to the necessary clients.

This can be done on a device group or client level.

To update a single client, right click on it and select “Update Now”.

Can also optionally set “Force package sync during Update Now” in the client properties.

## Using the 7921 Configuration Utility for Quick Deployment

The 7921 Configuration Utility can also be utilized to push out a default WLAN template to multiple Cisco Unified Wireless IP Phone 7921Gs.

Download the [7921 Configuration Utility](#) from CCO.

Rename 7921CU-1.2.1.AVA to 7921CU-1.2.1.zip and extract the contents.

Launch the 7921 Configuration Utility (..\TempInstall.PRF\TempInstall.GRP\7921CU.PKG\APPS\7921CU\7921CU.exe). A template can then be configured with the necessary wireless LAN and network settings. Once the template is complete, it will then need to be exported into Wavelink format. Select “Export to Wavelink” under the file menu, which will create an encrypted template file named “7921Wlan.cfg.enc” file in the folder. The 7921 currently does a TFTP get for WLANDefault.xml and WLAN<MAC\_ADDRESS>.xml. Rename the “7921Wlan.cfg.enc” file to “WLANDefault.xml” and copy it to a TFTP server, where all phones directed to that TFTP server will download and apply that template.

The Cisco Unified Wireless IP Phone 7921G defaults with network profile 1 configured with an ssid “cisco” and open authentication. DHCP option 150 can be configured for that network to point to an alternate TFTP server containing the WLAN template file.

If using 802.1x authentication (EAP-FAST or LEAP) where unique user accounts are utilized, then can either push out a temporary username and password, which can be disabled after the grace period, and the users must update their username and password information or push out a template where the username and password is blank.

PEAP and EAP-TLS are not supported with the 7921 Configuration Utility at this time.

After pushing out the default WLAN template, remove the template from the TFTP server afterwards if the production voice network is using the same TFTP server to avoid from overwriting the current wireless LAN and network settings. If using a different TFTP server, may still want to remove the file to ensure that not just any Cisco Unified Wireless IP Phone 7921G can get on the wireless network.

## **Configuring the Local Phone Book and Speed Dials**

Release 1.1(1) and later contain local phone book and speed dials support.

Up to 100 contacts and 99 speed dials can be added. Key #1 is reserved for voicemail.

The left softkey on the home screen can be programmed for “Message” to access voice mail or to “PhBook” to access the local phone book.

The local phone book and speed dials can be configured via the local keypad or via the Cisco Unified Wireless IP Phone 7921G web interface. Since the web password is not managed by the user the web interface is primarily intended for use by the system administrator, where they can upload information into the phone book for the user. This requires that the “Phone Book Web Access” product specific configuration item be set to “Allow Admin”.



## Cisco Unified Wireless IP Phone 7921G

SEP0018BA78C222

Phone DN 23675

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
<b>PHONE BOOK</b>
Import/Export
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

### Phone Book (New Contact)

Name Information

First Name	<input type="text"/>
Last Name	<input type="text"/>
Nickname	<input type="text"/>
Company Name	<input type="text"/>

Phone Information

Primary#

Speed Dial#

	Primary#	Speed Dial#
Work Number	<input type="radio"/>	<input type="text"/>
Home Number	<input type="radio"/>	<input type="text"/>
Mobile Number	<input type="radio"/>	<input type="text"/>
Other Number	<input type="radio"/>	<input type="text"/>

Contact Information

Email Address	<input type="text"/>
IM Address	<input type="text"/>

Mailing Address

Street Number	<input type="text"/>
City	<input type="text"/>
State/Province	<input type="text"/>
ZIP/Postal Code	<input type="text"/>
Country	<input type="text"/>

Reset Save Cancel

Copyright (c) 2006-2008 by Cisco Systems, Inc.

The phone book data can be exported which can be imported onto other phones.

Release 1.2(1) supports XML and CSV format as well as the CSV format used by the Cisco Unified Wireless IP Phone 7920.



## Cisco Unified Wireless IP Phone 7921G

SEP0018BA78C222

Phone DN 23675

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
<b>PHONE BOOK</b>
<b>Import/Export</b>
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

### Phone Book (Import & Export)

Import Contact Info to Phone

Import from File:

DELETE ALL current Contacts before Importing

DELETE ONLY the current Contact if matched

MERGE current Contact info with Importing data

Matching Contacts:

Using Unique Identifier (UID) value

Using Name fields

**To import using CSV format, please specify a filename with 32 characters or less, and with the file-extension of ".csv".**

Export Contact Info to File

Create File of Type:

XML Phone Book format

Comma Separated Values (CSV) format

Copyright (c) 2006-2008 by Cisco Systems, Inc.

## Troubleshooting

### Stream Statistics

The Cisco Unified Wireless IP Phone 7921G provides call statistic information, where MOS, jitter and packet counters are displayed. DSCP for transmit and receive paths are also displayed, which can help to ensure that packets are being placed into the correct queues upstream and downstream.

Log onto the web interface and select “Stream Statistics” to view this information.

This information is also available locally on the phone under **Settings > Status > Call Statistics** or if on a phone call press the center button twice.



## Cisco Unified Wireless IP Phone 7921G

SEP0018BA78C222

Phone DN 23675

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
<b>STREAM 1</b>
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

### Stream Statistics

#### RTP Statistics

Domain Name	snmpUDPDomain	Remote Address	10.2.0.250
Remote Port	20350	Local Address	10.8.0.153
Local Port	28048	Sender Joins	1
Receiver Joins	1	Byes	0
Start Time	17:33:47	Row Status	Active
Host Name	SEP0018BA78C222	Sender DSCP	EF
Sender Packets	1064	Sender Octets	183008
Sender Tool	G.722	Sender Reports	3
Sender Report Time	17:34:04	Sender Start Time	17:33:47
Receiver DSCP (Previous, Current)	EF, EF	Receiver Packets	1104
Receiver Octets	176640	Receiver Tool	G.722
Receiver Lost Packets	0	Receiver Jitter	0
Receiver Reports	0	Receiver Start Time	17:33:47

#### Voice Quality Metrics

MOS LQK	4.5000	Avg MOS LQK	4.3847
Min MOS LQK	4.1855	Max MOS LQK	4.5000
MOS LQK Version	0.95	Cumulative Conceal Ratio	0.0035
Interval Conceal Ratio	0.0000	Max Conceal Ratio	0.0200
Conceal Seconds	2	Severly Conceal Seconds	1

Refresh

Stop

Copyright (c) 2006-2008 by Cisco Systems, Inc.

For more information, see the “Troubleshooting the Cisco Unified Wireless IP Phone 7921G” chapter in the *Cisco Unified Wireless IP Phone 7921G Administration Guide* at this URL:

[http://www.cisco.com/en/US/products/hw/phones/ps379/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/phones/ps379/prod_maintenance_guides_list.html)



# Network Statistics



## Cisco Unified Wireless IP Phone 7921G

SEP0018BA78C222

Phone DN 23675

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
<b>NETWORK</b>
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

Network Statistics			
IP Statistics			
IpInReceives	38847	IpInHdrErrors	0
IpInAddrErrors	0	IpForwDatagrams	0
IpInUnknownProtos	0	IpInDiscards	0
IpInDelivers	38796	IpOutRequests	40317
IpOutDiscards	0	IpOutNoRoutes	0
IpReasmTimeout	0	IpReasmReqds	0
IpReasmOKs	0	IpReasmFails	0
IpFragOKs	0	IpFragFails	0
IpFragCreates	0		
TCP Statistics			
TcpRtoAlgorithm	0	TcpRtoMin	0
TcpRtoMax	0	TcpMaxConn	0
TcpActiveOpens	16	TcpPassiveOpens	50
TcpAttemptFails	0	TcpEstabResets	0
TcpCurrEstab	3	TcpInSegs	2524
TcpOutSegs	3992	TcpRetransSegs	51
TcpInErrs	0	TcpOutRsts	5
UDP Statistics			
UdpInDatagrams	36311	UdpNoPorts	0
UdpInErrors	0	UdpOutDatagrams	36325

Copyright (c) 2006-2008 by Cisco Systems, Inc.

Queue statistics can also be displayed by navigating to Settings > Status > Network Statistics.

If on a phone call, should see the “DataRcvVO” counter increasing assuming QoS has been deployed correctly.



# Wireless LAN Statistics



## Cisco Unified Wireless IP Phone 7921G

SEP0018BA78C222

Phone DN 23675

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
<b>WIRELESS LAN</b>
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

### Wireless LAN Statistics

#### Rx Statistics

Rx OK Frames	3414	Rx error frames	0
Rx unicast frames	3414	Rx multicast frames	0
Rx broadcast frames	0	Rx FCS frames	0
Rx beacons	37262	Association Rejects	0
Association Timeouts	0	Authentication Rejects	0
Authentication Timeouts	0		

#### Tx Statistics (Best Effort)

Tx OK Frames	5468	Tx error frames	2
Tx unicast frames	5135	Tx multicast frames	311
Tx broadcast frames	24	RTS fail counter	0
ACK fail counter	108	Retries counter	38
Multiple retries counter	10	Failed retries counter	2
Tx timeout counter	0	Other fail counter	0
Success counter	5468	Max retry limit counter	1

#### Tx Statistics (Voice)

Tx OK Frames	35964	Tx error frames	0
Tx unicast frames	35964	Tx multicast frames	0
Tx broadcast frames	0	RTS fail counter	0
ACK fail counter	33	Retries counter	33
Multiple retries counter	0	Failed retries counter	0
Tx timeout counter	0	Other fail counter	0
Success counter	35964	Max retry limit counter	0

Copyright (c) 2006-2008 by Cisco Systems, Inc.

## Traffic Stream Metrics (TSM)

The Traffic Stream Metrics feature requires the client to report voice traffic related measurements to the AP.

The parameters (queue delay, media delay, packet loss, packet count, roaming delay, roaming count) will be gathered by the AP and escalated to the WLAN management system, which will help maintain a database that can be used for the benefit of the stations by ensuring low packet latency and loss.

Check the box “Metrics Collection” in the global 802.11 Voice Parameters to enable Traffic Stream Metrics.

See the “[Call Admission Control Settings](#)” section for further information on how to enable TSM.

To view Traffic Stream Metrics data for a client, select TSM from the drop down menu for which band the Cisco Unified Wireless IP Phone 7921G is using.

The Traffic Stream Metrics data entries will then be displayed.

Select one of the entries to display the uplink and downlink statistics.

The screenshot shows the Cisco Unified Wireless IP Phone 7921G web interface. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The left sidebar shows 'Monitor' with sub-items: Summary, Access Points, Statistics, CDP, Rogues, Clients, and Multicast. The main content area is titled 'Clients > AP > Traffic Stream Metrics' and displays the following client details:

- Client Mac Address: 00:18:ba:78:c2:22
- Radio Type: 802.11a
- AP Interface Mac: 00:13:5f:fa:25:10
- Measurement Duration: 90 sec

Below the client details are two tables: 'Uplink Statistics' and 'Downlink Statistics'. Both tables show 'Packets that experienced Delay' categorized by delay range (< 10ms, 10ms-20ms, 20ms-40ms, > 40ms) and 'Packets' and 'Lost Packets' (Total, Maximum, Average).

Timestamp	Packets that experienced Delay					Packets		Lost Packets	
	Average	< 10ms	10ms-20ms	20ms-40ms	> 40ms	Total	Total	Maximum	Average
Tue Sep 16 20:33:00 2008	0	0	0	0	0	0	0	0	0
Tue Sep 16 20:34:32 2008	0	0	0	0	0	0	0	0	0
Tue Sep 16 20:36:04 2008	0	0	0	0	0	0	0	0	0
Tue Sep 16 20:37:36 2008	0	0	0	0	0	0	0	0	0
Tue Sep 16 20:39:07 2008	0	0	0	0	0	0	0	0	0
Tue Sep 16 20:40:39 2008	5	2619	136	0	0	2755	0	0	0
Tue Sep 16 20:42:11 2008	5	4299	209	1	0	4509	0	0	0

Timestamp	Packets that experienced Delay					Packets		Lost Packets	
	Average	< 10ms	10ms-20ms	20ms-40ms	> 40ms	Total	Total	Maximum	Average
Tue Sep 16 20:33:00 2008	0	0	0	0	0	0	0	0	0
Tue Sep 16 20:34:32 2008	0	0	0	0	0	0	0	0	0
Tue Sep 16 20:36:04 2008	0	0	0	0	0	0	0	0	0
Tue Sep 16 20:37:36 2008	0	0	0	0	0	0	0	0	0
Tue Sep 16 20:39:07 2008	0	0	0	0	0	0	0	0	0
Tue Sep 16 20:40:39 2008	12	602	2151	64	0	2817	0	0	0
Tue Sep 16 20:42:11 2008	10	2365	2349	1012	0	5726	0	0	0

## Phone Logs

Phone logs for troubleshooting purposes can be obtained from the Cisco Unified Wireless IP Phone 7921G web interface..

The phone logs are stored in memory only by default, but can optionally enable “Preserve Logs” where the logs will be stored in flash.

Syslog can also be enabled to capture logging real-time via the wireless LAN or USB interface.



## Cisco Unified Wireless IP Phone 7921G

SEP0018BA78C222

Phone DN 23675

HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
<b>TRACE SETTINGS</b>
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

Trace Settings	
<b>General</b>	
Number of Files	2
File Size	50 Kilo Bytes
<b>Remote Syslog Server</b>	
<input type="checkbox"/> Enable Remote Syslog	
IP Address	0.0.0.0
Port (Valid range is 514, 1024-65535)	514
<b>Module Trace Level</b>	
Kernel	Error
Configuration	Error
Call Control	Error
Network Services	Error
Security Subsystem	Error
User Interface	Error
Wireless LAN Driver	Error
Wireless LAN Manager	Error
Audio System	Error
System	Error
<b>Advanced Trace Settings</b>	
Preserve Logs	<input type="radio"/> True <input checked="" type="radio"/> False
Reset Trace Settings upon Reboot	<input checked="" type="radio"/> Yes <input type="radio"/> No

Save

Copyright (c) 2006-2008 by Cisco Systems, Inc.

### Trace Modules

Kernel	Operating System
Wireless LAN Driver	Channel scanning, roaming, authentication
Wireless LAN Manager	WLAN Management, QoS
Configuration	Phone configuration, firmware upgrade
Call Control	Cisco Unified Communications Manager messaging (SCCP)
Network Services	DHCP, TFTP, CDP, WWW, Syslog
Security Subsystem	Application level security
User Interface	Keypad, softkeys, MMI
Audio System	RTP, SRTP, RTCP, DSP

## Trace Levels

Various levels of tracing are available which provide different levels of messaging.

Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug

**Note:** All trace modules are set to Error level by default.

Voice quality can potentially be impacted if higher trace levels are configured.

In firmware 1.1(1) and later, the trace level will reset to “Error” level by default unless configured to preserve the trace levels.

## Restoring Factory Defaults

You can clear configuration options that are stored in the phone by using the factory default menu option on the phone.

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:

1. Choose Settings > Phone Settings.
2. Press “\*\*2” on the keypad.  
The phone briefly displays “Restore to Default?”
3. Press the “Yes” softkey to confirm or “No” to cancel.  
The phone resets after selecting “Yes”.

## Healthcare Environments

This product is not a medical device and uses an unlicensed frequency band that is susceptible to interference from other devices or equipment.

## Cleaning the Phone

Gently wipe the Cisco Unified Wireless IP Phone 7921G screen and housing with a soft, dry cloth.

Do not use any liquids or powders to clean the phone. Using anything other than a soft, dry cloth can damage the phone and cause failures.

Carry cases can potentially help protect the phone from moisture, dust, and dirt, and provide drop protection.

## Phone Accessories

You can order these accessories for the Cisco Unified Wireless IP Phone 7921G.

For more information, refer to the *Cisco Unified Wireless IP Phone 7921G Accessories Guide* at this URL:

[http://www.cisco.com/en/US/products/hw/phones/ps379/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/hw/phones/ps379/products_user_guide_list.html)

- Batteries Standard and Extended
- Carry Cases Holster and Leather
- Desktop Charger
- Multi-Charger
- Lock Set
- Shoulder Strap (for leather carry case)
- USB Cable

### **3<sup>rd</sup> Party Accessories**

- Carry Cases [www.zcover.com](http://www.zcover.com), [www.systemwear.com](http://www.systemwear.com)
- Headsets [www.plantronics.com](http://www.plantronics.com)

**Note:** Cisco Unified Wireless IP Phone 7921G and 7920 accessories are not interchangeable.

## Additional Documentation

Cisco Unified Wireless IP Phone 7921G Data Sheet

[http://www.cisco.com/en/US/products/hw/phones/ps379/products\\_data\\_sheet0900aecd8059fcab.html](http://www.cisco.com/en/US/products/hw/phones/ps379/products_data_sheet0900aecd8059fcab.html)

Cisco Unified Wireless IP Phone 7921G Administration Guide

[http://www.cisco.com/en/US/products/hw/phones/ps379/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/phones/ps379/prod_maintenance_guides_list.html)

Cisco Unified Wireless IP Phone 7921G Phone Guide and Quick Reference

[http://www.cisco.com/en/US/products/hw/phones/ps379/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/hw/phones/ps379/products_user_guide_list.html)

Cisco Unified Wireless IP Phone 7921G Firmware

<http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser-crypto>

Cisco Voice Software

<http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml>

Cisco Localization

<http://www.cisco.com/kobayashi/sw-center/telephony/callmgr/locale-installer.shtml>

Cisco Unified IP Phone Services Application Development Notes

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cuipph/all\\_models/xsi/6\\_0/english/programming/guide/XSIbook.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/all_models/xsi/6_0/english/programming/guide/XSIbook.html)

Cisco Unified Communications SRND

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cucm/srnd/7x/uc7\\_0.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/uc7_0.html)

Mobility SRND

[http://www.cisco.com/application/pdf/en/us/guest/netsol/ns279/c649/cmigration\\_09186a00808d9330.pdf](http://www.cisco.com/application/pdf/en/us/guest/netsol/ns279/c649/cmigration_09186a00808d9330.pdf)

Cisco Unified Wireless LAN Controller Documentation

[http://www.cisco.com/en/US/products/ps6366/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6366/products_installation_and_configuration_guides_list.html)

Autonomous Access Point Documentation

[http://www.cisco.com/en/US/products/ps6521/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6521/products_installation_and_configuration_guides_list.html)

Open Source License Notices for the Cisco Unified IP Phones 7900 Series

[http://www.cisco.com/en/US/products/hw/phones/ps379/products\\_licensing\\_information\\_listing.html](http://www.cisco.com/en/US/products/hw/phones/ps379/products_licensing_information_listing.html)

---

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

© 2008 Cisco Systems, All rights reserved.