

# Cisco Unified Wireless IP Phone 7921G Deployment Guide

February 28, 2007

EDCS-574256



The Cisco Unified Wireless IP Phone 7921G is adaptable for all mobile professionals, from managers on the move within an office environment to associates working in the warehouse, on the sales floor, or in the call center. Nurses, doctors, educators, and IT personnel can be easily reached as industries adopt wireless LANs.

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

# Table of Contents

<i>Revision History</i> .....	1
<b>Table of Contents</b> .....	<b>2</b>
<b>Requirements for Cisco Unified Wireless IP Phone 7921G</b> .....	<b>4</b>
<i>Call Control</i> .....	4
<i>Supported Protocols</i> .....	4
<i>Supported Access Points</i> .....	4
Cisco Access Point Models and Modes .....	5
<b>Phone Models and Regulatory Domains</b> .....	<b>5</b>
<i>World Mode (802.11d)</i> .....	6
<i>Supported Countries for the Cisco Unified Wireless IP Phone 7921G</i> .....	6
<b>Data Rates, Range and Receiver Sensitivity</b> .....	<b>7</b>
<i>Setting Data Rates</i> .....	8
<b>Wireless Security</b> .....	<b>8</b>
<i>Cisco Centralized Key Management (CCKM)</i> .....	8
<i>Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling (EAP-FAST)</i> .....	8
<b>Voice Security</b> .....	<b>9</b>
<i>Setting Voice Security in Cisco Unified CallManager</i> .....	10
<b>Phone Battery Life</b> .....	<b>11</b>
<i>Power Save Poll (PS-POLL)</i> .....	11
<i>Unscheduled Auto Power Save Delivery (U-APSD)</i> .....	11
<i>Delivery Traffic Indicator Message (DTIM)</i> .....	12
<i>Single Access Point Mode</i> .....	12
<b>Quality of Service (QoS)</b> .....	<b>12</b>
<i>Configuring QoS for Phones in Cisco Unified CallManager</i> .....	13
<i>Configuring QoS Policies for the Network</i> .....	13
Configuring Cisco IOS Access Points .....	13
Configuring Cisco Switch Ports.....	14
Configuring Switch Ports for Wired IP Phones .....	14
Configuring the Cisco IOS Router with the QoS Policy for Phones.....	14
Sample Packet Capture .....	15
<i>Configuring Call Admission Control</i> .....	15
Pre-Call Admission Control.....	15
Roaming Admission Control .....	16
<b>Designing the Wireless Network for Voice</b> .....	<b>16</b>
<i>Call Capacity</i> .....	16
<i>Dynamic Transmit Power Control (DTPC)</i> .....	17
Setting Preamble Type on the Access Point .....	17

<i>Planning Channel Usage</i> .....	18
5 GHz (802.11a) .....	18
Using Dynamic Frequency Selection (DFS) on Access Points .....	18
2.4 GHz (802.11b/g) .....	19
<i>Signal Strength and Coverage</i> .....	20
Coverage .....	21
<i>Verify Coverage with Site Survey Tools</i> .....	22
<b>Configuring Access Points</b> .....	<b>22</b>
<i>VLANs and Autonomous Access Points</i> .....	23
<i>Delivery Traffic Indicator Message (DTIM) Settings</i> .....	24
Call Admission Control (TSPEC) Settings .....	24
<i>Setting the Controller 802.1x Timeout</i> .....	25
<b>Voice Quality Metrics</b> .....	<b>25</b>
<b>Configuring the Cisco Unified Wireless IP Phone 7921G</b> .....	<b>26</b>
Configuring Phones with the Keypad .....	26
Configuring Phones with the Web Interface .....	26
<i>Configuring the Network Profile Parameters</i> .....	26
Configuring Advanced Network Profile Settings .....	28
<i>Using Templates to Configure Phones</i> .....	29
<i>Setting the Phone to Factory Default</i> .....	29
<i>Upgrading Firmware</i> .....	29
<b>Localization</b> .....	<b>30</b>
<b>Healthcare Environments</b> .....	<b>30</b>
<b>Cleaning the Phone</b> .....	<b>30</b>
<b>Available Phone Accessories</b> .....	<b>30</b>
<b>Additional Documentation</b> .....	<b>31</b>

## Requirements for 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:

### 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 CallManager 4.1, 4.2, 5.0, and later
- Cisco Unified CallManager Express 4.1 and later
- SRST 4.1 and later

### Device Support in Cisco Unified CallManager

Cisco Unified CallManager versions 4.1, 4.2 and 5.0 require that you install a device package or service release update in order to enable Cisco Unified Wireless IP Phone 7921G device support.

CM 5.0(4) or higher requires signed COP files.

Device packages for Cisco Unified CallManager 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
- Real Time Control Protocol (RTCP)
- Cisco Discovery Protocol (CDP)
- Syslog
- CCX v4 Support
- Unscheduled Auto Power Save Delivery (U-APSD) and TSPEC
- Power Save Poll (PS-POLL)

### Supported Access Points

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

These are the recommended software versions:

- Cisco Wireless LAN Controller (Lightweight) 4.0 or higher
- Cisco IOS Access Points (Autonomous) 12.3(8)JEA or higher

## Cisco Aironet Access Points



## Wireless LAN Controllers



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

## Cisco Access Point Models and Modes

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

Cisco Series	802.11b	802.11g	802.11a	Autonomous	Light Weight
<b>350</b>	Yes	No	No	Yes	No
<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>1240AG</b>	Yes	Yes	Yes	Yes	Yes
<b>1300</b>	Yes	Yes	No	Yes	Yes

## Phone Models and Regulatory Domains

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:

Regulatory Domain	Phone Device Number	Regulatory Domain Number	Band Range	Available Channels	5 GHz Channel Set
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 11 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	4153	2.412–2.472 GHz 2.412–2.484 GHz 5.15–5.35 GHz	13 (OFDM) 14 (CCK) 8	
World	CP-7921G-W-K9	5252	Uses 802.11d to identify band ranges and channels		

## World Mode (802.11d)

If using the Cisco Unified Wireless IP Phone 7921G World (-W) model, then you must enable 802.11d. The phone 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:

## Supported Countries for the Cisco Unified Wireless IP Phone 7921G

Australia (AU)	Hungary (HU)	Portugal (PT)
Austria (AT)	Iceland (IS)	Romania (RO)
Belgium (BE)	Ireland (IE)	Saudi Arabia (SA)
Bulgaria (BG)	Italy (IT)	Singapore (SG)
Canada (CA)	Japan (JP)	Slovakia (SK)
Cyprus (CY)	Latvia (LV)	Slovenia (SI)
Czech Republic (CZ)	Liechtenstein (LI)	South Africa (ZA)
Denmark (DK)	Lithuania (LT)	Spain (ES)
Estonia (EE)	Luxembourg (LU)	Sweden (SE)
Finland (FI)	Malta (MT)	Switzerland (CH)

France (FR)	Monaco (MC)	Turkey (TR)
Germany (DE)	Netherlands (NL)	Ukraine (UA)
Gibraltar (GI)	New Zealand (NZ)	United Kingdom (GB)
Greece (GR)	Norway (NO)	United States (US)
HongKong (HK)	Poland (PL)	

**Note:** To see if countries not included in this list are now supported, go to the Cisco Product Approval Status web site at this 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)

## Data Rates, Range and Receiver Sensitivity

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

<b>802.11a</b>	<b>Data Rate</b>	<b>Range</b>	<b>Receiver Sensitivity</b>
Max Tx Power is 40mW	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 40mW	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
<b>802.11b</b>	<b>Data Rate</b>	<b>Range</b>	<b>Receiver Sensitivity</b>
Max Tx Power is 50mW	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

## Setting Data Rates

When 802.11b clients exist in the wireless network, then you should set data rates as follows:

- 11 Mbps as the basic rate (mandatory)
- 18–54 Mbps as optional (supported)
- Disable the other lower data rates.

**Note:** Some environments may require that you enable the 5.5 Mbps rate as a basic rate.

Set the lowest data rate enabled as the basic rate.

If 802.11b clients are not allowed in the WLAN, then you can disable the 1, 2, 5.5, 11 Mbps data rates. Note that capacity and throughput are reduced when lower rates are enabled.

## Wireless Security

When deploying a WLAN, 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)

Lightweight Extensible Authentication Protocol (LEAP)

### 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 in ACS 4.0, you must install a certificate.

The Cisco Unified Wireless IP Phone 7921G currently supports only automatic provisioning of the PAC (Protected Access Credential), so enable “Anonymous In-Band PAC Provisioning” on the access point as shown.

The screenshot shows the Cisco ACS 4.0 System Configuration interface. The left sidebar contains navigation options: 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 window is titled 'System Configuration' and 'Edit'. The 'EAP-FAST Configuration' window is open, showing 'EAP-FAST Settings'. A red box highlights the following checked options: 'Allow anonymous in-band PAC provisioning', 'Allow authenticated in-band PAC provisioning', 'Accept client on authenticated provisioning', and 'Require client certificate for provisioning'. Other settings include: 'Allow EAP-FAST' (checked), 'Active master key TTL' (1 months), 'Retired master key TTL' (3 months), 'Tunnel PAC TTL' (1 weeks), 'Client initial message' (Welcome!), 'Authority ID Info' (sjc21-21a-ac), 'Allow Machine Authentication' (checked), 'Machine PAC TTL' (1 weeks), 'Allow Stateless session resume' (checked), 'Authorization PAC TTL' (1 hours), 'Allowed inner methods' (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), and 'EAP-FAST master server' (checked). The 'Actual EAP-FAST server status' is 'Master'. A 'Back to Help' button is at the bottom.

## 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

## Setting Voice Security in Cisco Unified CallManager

Cisco Unified CallManager provides these available voice security features. For more information, refer to the Cisco Unified CallManager documentation at

[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)

Protocol Specific Information	
Packet Capture Mode*	None
Packet Capture Duration	0
Presence Group*	Standard Presence group
Device Security Profile*	Cisco 7921 - Secure TFTP Encrypted
SUBSCRIBE Calling Search Space	SJ_Alpha_Calls
<input type="checkbox"/> Unattended Port	

Certification Authority Proxy Function (CAPF) Information	
Certificate Operation*	No Pending Operation
Authentication Mode*	By Existing Certificate (precedence to MIC)
Authentication String	
<input type="button" value="Generate String"/>	
Key Size (Bits)*	1024
Operation Completes By	2006 11 25 12 (YYYY:MM:DD:HH)
Certificate Operation Status: Upgrade Success	
Note: Security Profile Contains Addition CAPF Settings.	

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

**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

Push-to-Talk URL

## Phone Battery Life

The standard battery provides up to 80 hours standby time or up to 10 hours talk time.

The extended battery provides up to 100 hrs standby time or up to 12 hours talk time.

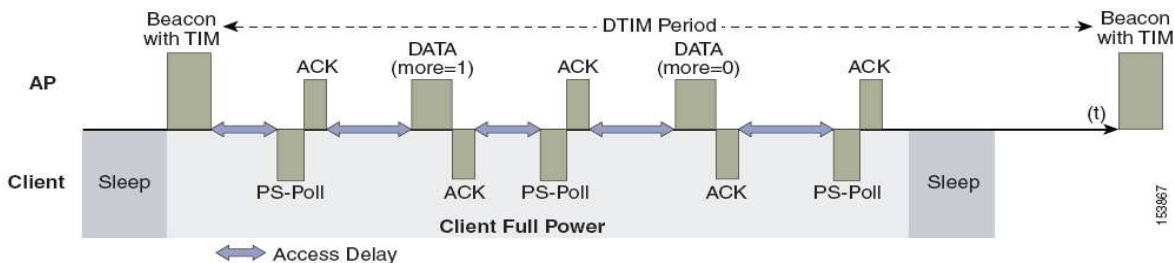
To extend battery life, Cisco Unified Wireless IP Phone 7921G can use PS-POLL or U-APSD power save methods.

### Power Save Poll (PS-POLL)

The Cisco Unified Wireless IP Phone 7921G uses PS-POLL when in idle mode.

If WiFi MultiMedia (WMM) is disabled on the access point, then the wireless IP phone uses PS-POLL for power save when a phone call is active.

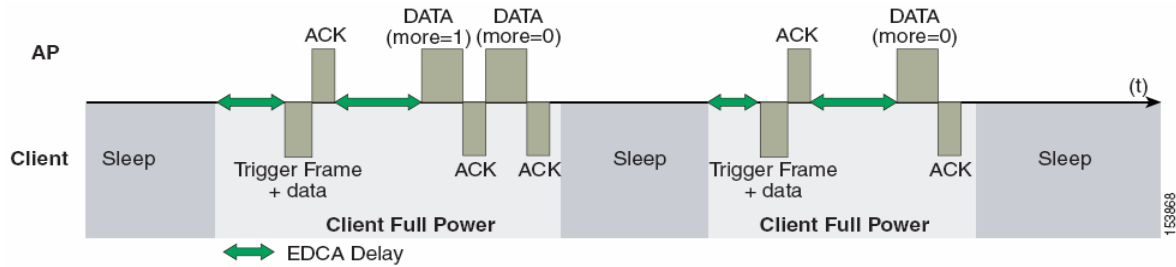
This is a sample packet sequence when using PS-POLL.



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

When the Cisco Unified Wireless IP Phone 7921G is in an active phone call, it uses U-APSD (Unscheduled Auto Power Save Delivery) instead of PS-POLL for power save when WMM is enabled. U-APSD helps optimize battery life.

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



## Delivery Traffic Indicator Message (DTIM)

Increasing the DTIM period can also increase the battery life. The Cisco Unified Wireless IP Phone 7921G uses the DTIM period to schedule wakeup periods to check for incoming packets.

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

## Single Access Point Mode

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 with roaming phones, disable “Single AP Mode”, which is the default setting. This will prevent voice quality issues for roaming phones.

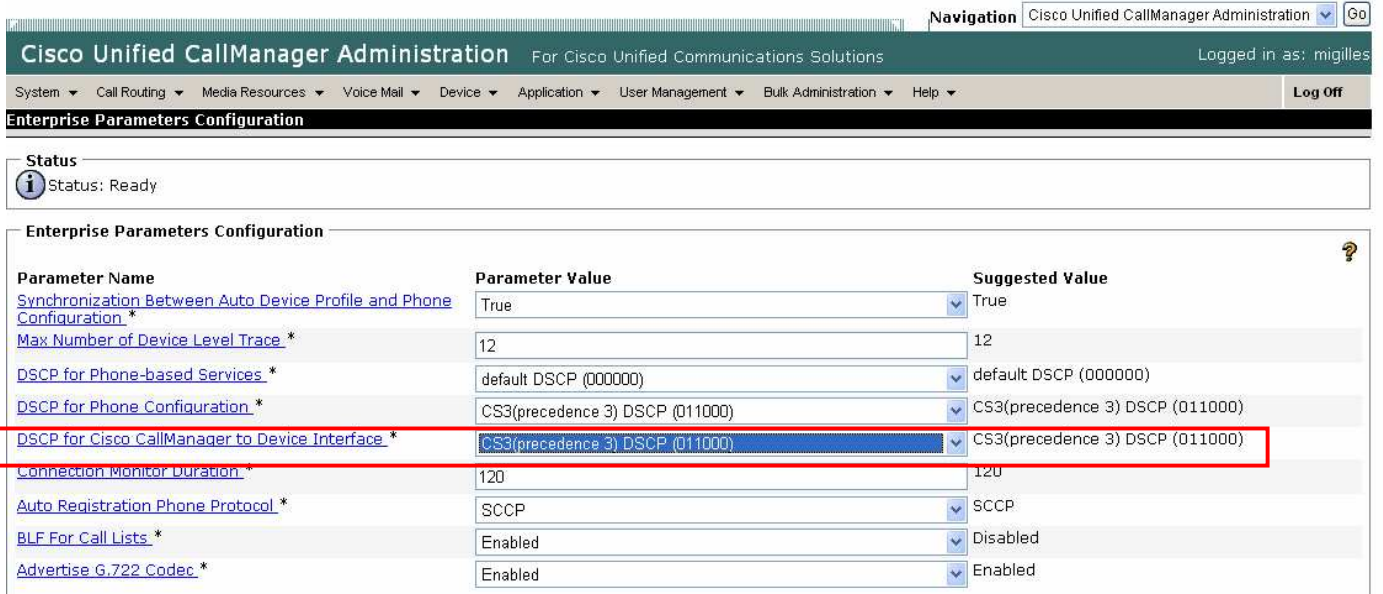
## Quality of Service (QoS)

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 = 3
- 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 WLAN when using Cisco 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 for Phones in Cisco Unified CallManager

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



The screenshot shows the Cisco Unified CallManager Administration web interface. The page title is "Cisco Unified CallManager Administration" and it is for "Cisco Unified Communications Solutions". The user is logged in as "migilles". The navigation menu includes "System", "Call Routing", "Media Resources", "Voice Mail", "Device", "Application", "User Management", "Bulk Administration", and "Help". The "Enterprise Parameters Configuration" page is displayed, showing a status of "Ready". The main content area is a table of Enterprise Parameters Configuration with the following data:

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>	Enabled	Disabled
<a href="#">Advertise G.722 Codec *</a>	Enabled	Enabled

## 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 3
!
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
```

## 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
```

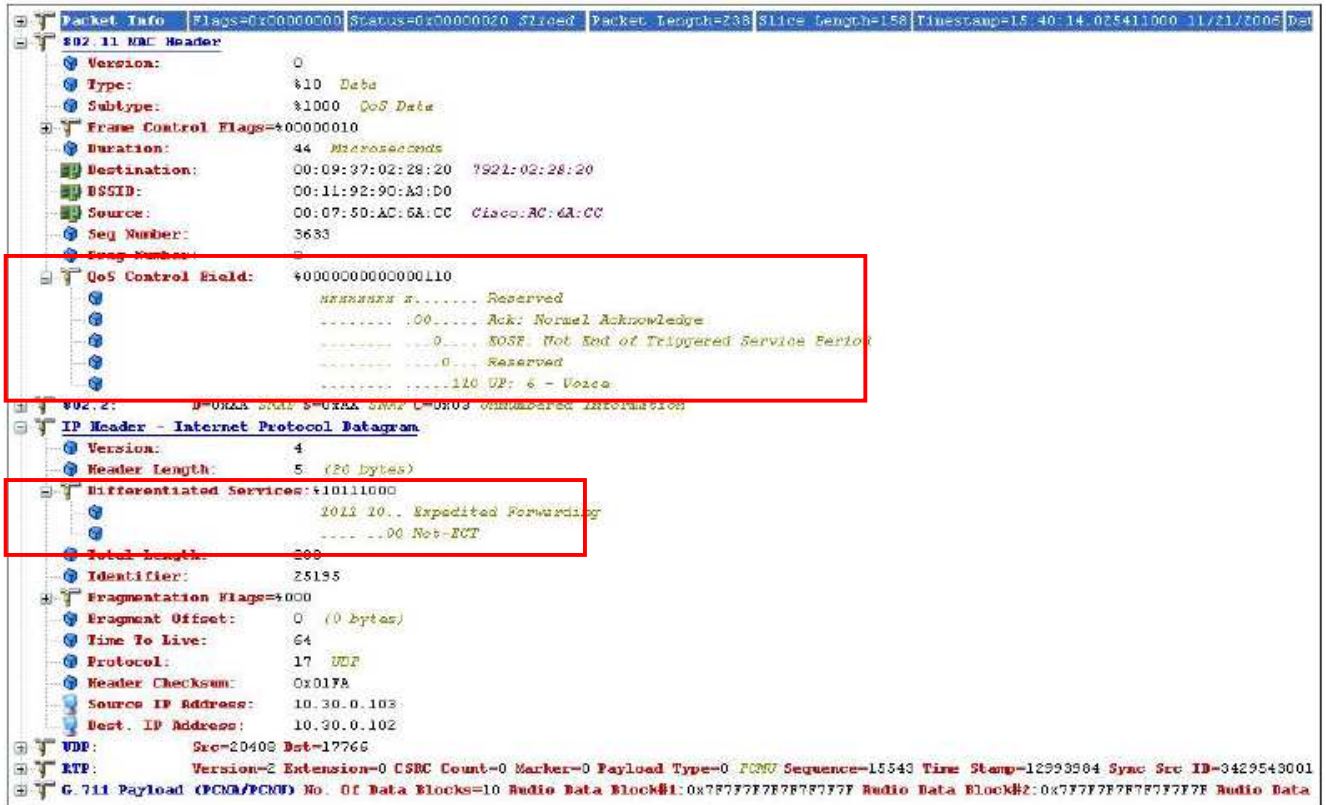
## Configuring the Cisco IOS Router with the QoS Policy for Phones

Use this QoS policy on IOS router interfaces to map RTP and SCCP correctly, and optionally, you can mark all other traffic as best effort.

```
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 Packet Capture

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



## Configuring Call Admission Control

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

- Enable Call Admission Control / WiFi 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)

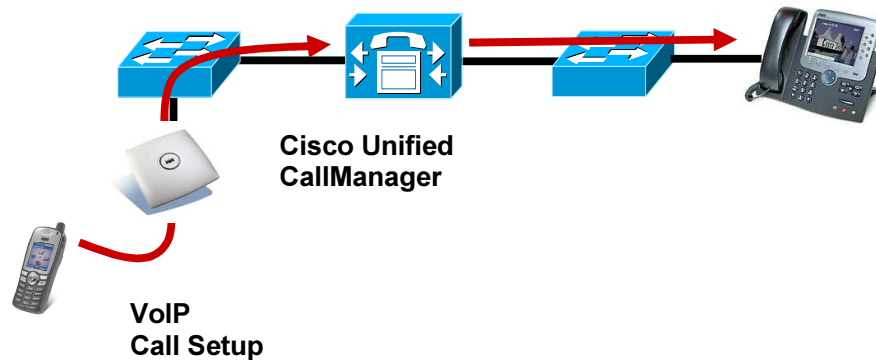
If you are using an 802.11b access point, then you must modify the PHY rate on each Cisco Unified Wireless IP Phone 7921G phone to a supported data rate for 802.11b.

TSPEC has precedence over QBSS (QoS Basic Service Set).

## Pre-Call Admission Control

If Call Admission Control (TSPEC) is enabled on the access point, the Cisco Unified Wireless IP Phone 7921G sends an ADDTS (Add Traffic Stream) 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”.

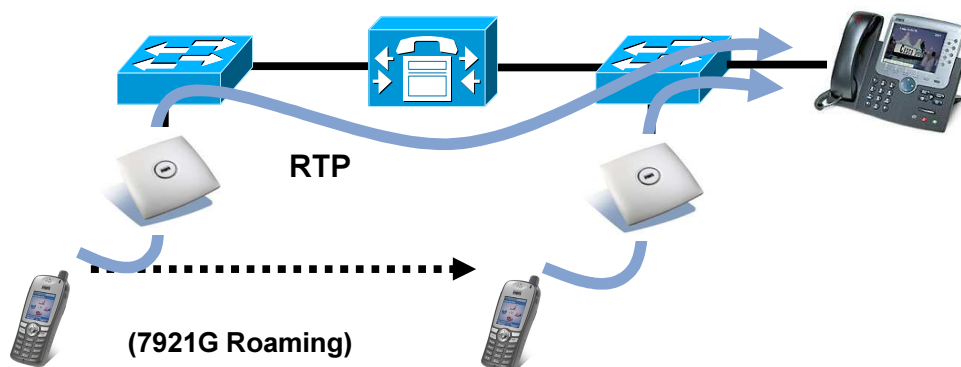
## Pre-Call Admission Control



## 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 chapter in the *Enterprise Design Mobility Guide* at this URL:

<http://www.cisco.com/univercd/cc/td/doc/solution/emblty30.pdf>

## Designing the Wireless Network 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 Design Mobility Guide* at this URL: <http://www.cisco.com/univercd/cc/td/doc/solution/emblty30.pdf>

## Call Capacity

Design the network to accommodate the desired call capacity. The Cisco Access Point can support up to 20 active RTP streams for both 802.11g and 802.11a at a data rate of 54 Mbps. To achieve this capacity, you must use U-APSD and have minimal WLAN background traffic and radio frequency (RF) utilization.

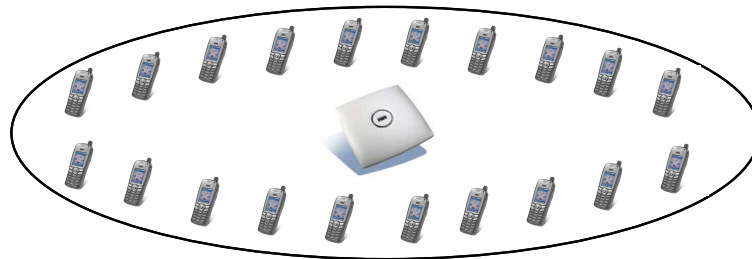


At 11 Mbps, the Cisco Access Point can support up to 10 active RTP streams when using U-APSD with the same WLAN traffic conditions.

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

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

Each RTP stream is a connection from a phone to the access point or from the access point to a phone.



## 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.

**Note:** Do not use default setting of Max power.

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 WLAN. This setting prevents one-way audio when RF traffic is heard in one direction only.



## Setting Preamble Type on the Access Point

Use the short preamble setting in the radio configuration setting on the access point when no legacy clients that require a long preamble are present in the WLAN.

By using the short preamble instead of the legacy long preamble, the wireless network performance is improved.

## Planning Channel Usage

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

### 5 GHz (802.11a)

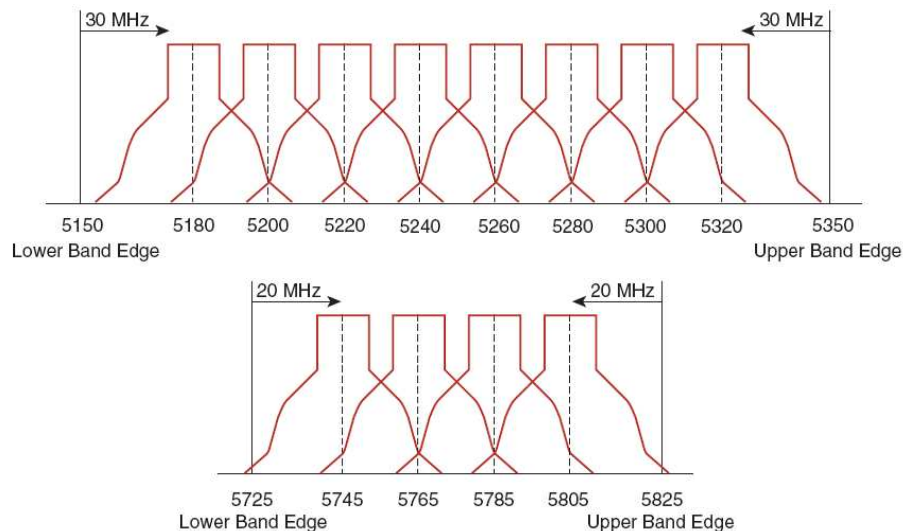
The Cisco Unified Wireless IP Phone 7921G supports Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) that are required for 802.11a (802.11h).

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 WLANs.

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.



### 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).

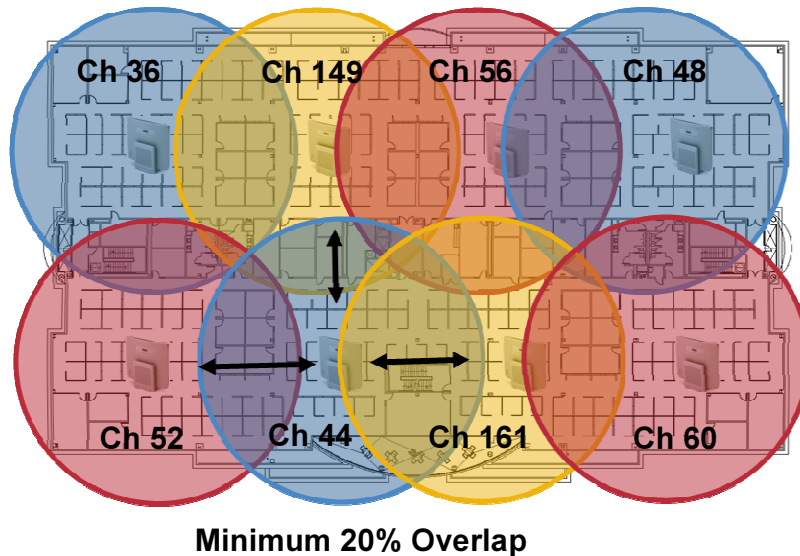
For lightweight solution access points, enable Auto RF.

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

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.



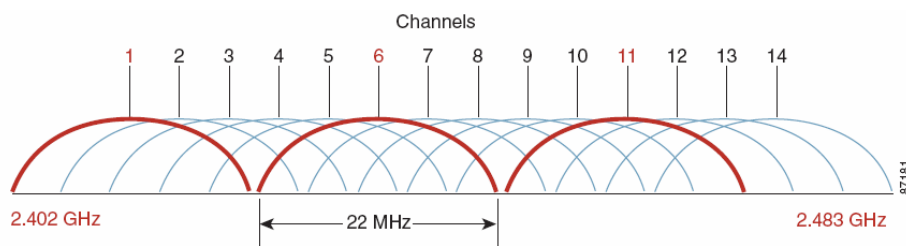
Currently the Cisco Unified Wireless IP Phone 7921G only supports up to 16 channels. For 5 GHz, 20 channels are available in the Americas and 19 channels in Europe. If the UNII-2 extended channels (channels 100-140) are available for use, we recommend that you disable UNII-2 (channels 52-64) on the access point.

<b>Default Radio Channel:</b>	Dynamic Frequency Selection (DFS) Channel 40 5200 MHz		
<b>Dynamic Frequency Selection Bands:</b>	<input type="checkbox"/> Band 1 - 5.150 to 5.250 GHz <input type="checkbox"/> Band 2 - 5.250 to 5.350 GHz <input type="checkbox"/> Band 3 - 5.470 to 5.725 GHz <input type="checkbox"/> Band 4 - 5.725 to 5.825 GHz		
<b>World Mode Multi-Domain Operation:</b>	<input type="radio"/> Disable <input type="radio"/> Legacy <input checked="" type="radio"/> Dot11d		
<b>Country Code:</b>	US (United States) <input checked="" type="checkbox"/> Indoor <input checked="" type="checkbox"/> Outdoor		
<b>Receive Antenna:</b>	<input checked="" type="radio"/> Diversity <input type="radio"/> Left (Secondary) <input type="radio"/> Right (Primary)		
<b>Transmit Antenna:</b>	<input checked="" type="radio"/> Diversity <input type="radio"/> Left (Secondary) <input type="radio"/> Right (Primary)		

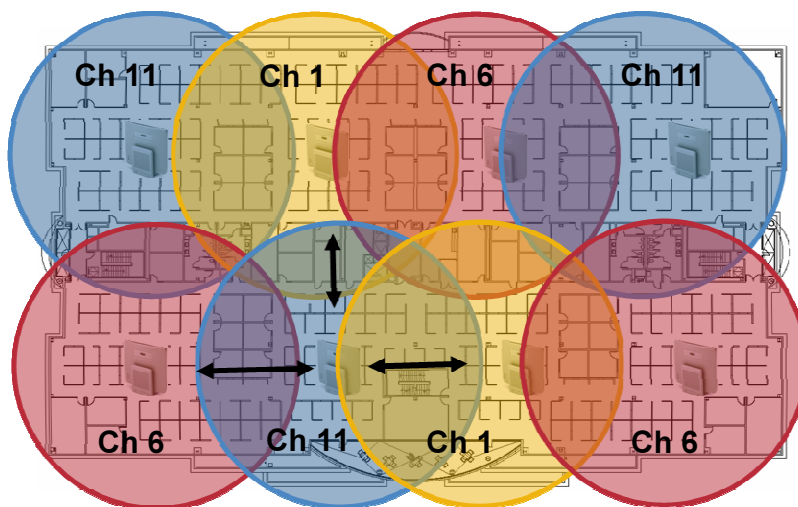
## 2.4 GHz (802.11b/g)

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

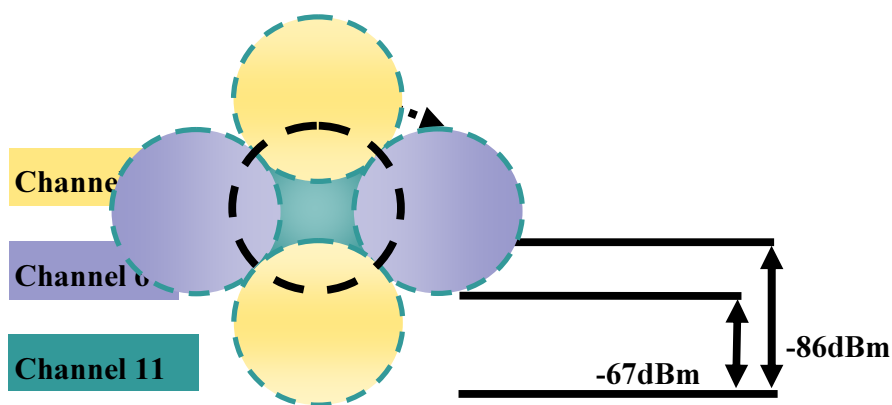
## Signal Strength and Coverage

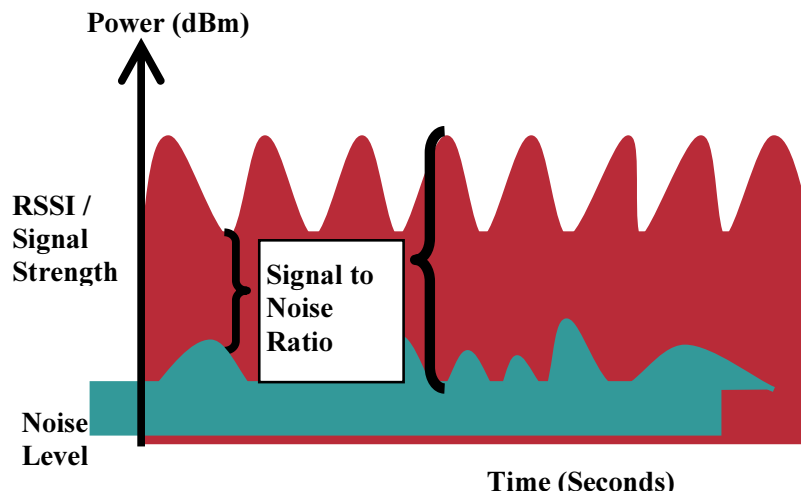
To ensure acceptable voice quality, the Cisco Unified Wireless IP Phone 7921G should always have a signal of -67 dBm or higher and ensure the Packet Error Rate (PER) is no higher than 1%.

Maintain a minimum SNR of 25dB = -92dBm noise level with -67 dBm signal.

The radius of the cell should be -67 dBm.

For more information about signal strength and cell edge design, refer to the “VoWLAN Design Recommendations” chapter in the *Enterprise Design Mobility Guide* at this URL: <http://www.cisco.com/univercd/cc/td/doc/solution/emblty30.pdf>





## Coverage

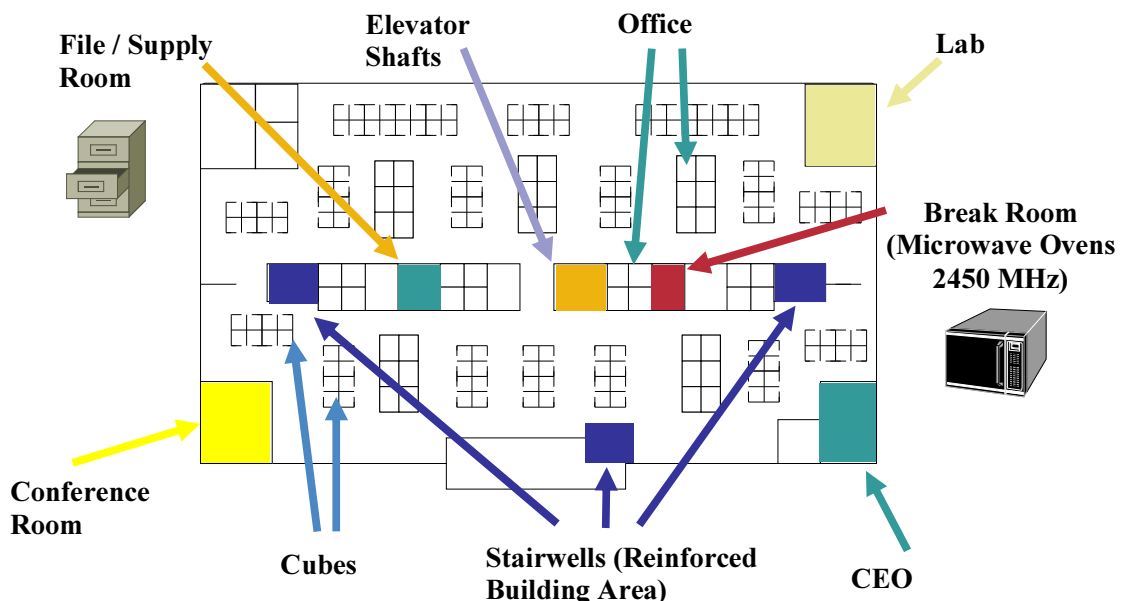
When designing the placement of access points, be sure that all key areas have sufficient coverage (signal).

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

WLAN 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, phones 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.



## Verify Coverage with Site Survey Tools

These are some of the tools and applications that you can use to verify coverage.

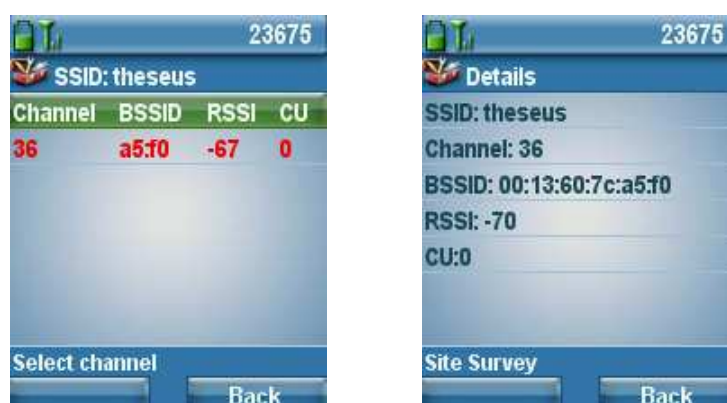
- Cisco Wireless Control System (WCS)
- Cisco Wireless LAN Solution Engine (WLSE)
- AirMagnet Survey ([www.airmagnet.com](http://www.airmagnet.com))

After the WLAN is deployed, you can also use the Cisco Unified Wireless IP Phone 7921G to verify coverage by using the Site Survey 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.

To see all access points, 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.

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



## Configuring 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 required.
- Ensure “Aggressive Load Balancing” is disabled

When using 802.1x authentication, we recommend that you use CCKM which is supported using either TKIP or WEP encryption.

**Note:** CCKM is not supported with AES encryption.

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

## VLANs and Autonomous Access Points

Segment wireless voice and data into two 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 packets are exchanged successfully.

## Delivery Traffic Indicator Message (DTIM) Settings

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

Wireless

Access Points  
All APs  
802.11a Radios  
802.11b/g Radios

Mesh

Rogues  
Rogue APs  
Known Rogue APs  
Rogue Clients  
Adhoc Rogues

Clients

802.11a  
Network  
Client Roaming  
Voice  
Video  
802.11h

802.11b/g  
Network  
Client Roaming  
Voice  
Video

Country

Timers

B02.11a Global Parameters

Apply Auto RF...

General

802.11a Network Status  Enabled

Beacon Period (milliseconds) 100

DTIM Period (beacon intervals) 2

Fragmentation Threshold (bytes) 2346

Pico Cell Mode  Enabled

DTPC Support  Enabled

802.11a Band Status

Low Band Enabled

Mid Band Enabled

High Band Enabled

Data Rates\*\*

6 Mbps Mandatory

9 Mbps Supported

12 Mbps Mandatory

18 Mbps Supported

24 Mbps Mandatory

36 Mbps Supported

48 Mbps Supported

54 Mbps Supported

CCX Location Measurement

Mode  Enabled

\*\* 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.

## Call Admission Control (TSPEC) 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.

Wireless

Access Points  
All APs  
802.11a Radios  
802.11b/g Radios

Mesh

Rogues  
Rogue APs  
Known Rogue APs  
Rogue Clients  
Adhoc Rogues

Clients

802.11a  
Network  
Client Roaming  
Voice  
Video  
802.11h

802.11b/g  
Network  
Client Roaming  
Voice  
Video

Country

Timers

B02.11a > Voice Parameters

Apply

Call Admission Control (CAC)

Admission Control (ACM)  Enabled

Max RF Bandwidth (%) 75

Reserved Roaming Bandwidth (%) 6

Traffic Stream Metrics

Metrics Collection



## Setting the Controller 802.1x Timeout

If using EAP-FAST or the 802.1x authentication is traversing the WAN, you need to increase the 802.1x timeout on the controller (default = 2 seconds) in order for the client to obtain the PAC via automatic provisioning.

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

To change the 802.1x timeout on the Cisco 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
```

For more information about these topics, refer to the *Enterprise Design Mobility Guide* at this URL:

<http://www.cisco.com/univercd/cc/td/doc/solution/embly30.pdf>

## Voice Quality Metrics

You can use the Cisco Unified Wireless IP Phone 7921G web interface to view call statistics information and troubleshoot possible problems with the network. Log onto the web interface and view Stream Statistics.

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/products\\_administration\\_guide\\_chapter09186a008079b52a.html](http://www.cisco.com/en/US/products/hw/phones/ps379/products_administration_guide_chapter09186a008079b52a.html)

The screenshot shows the Cisco Unified Wireless IP Phone 7921G web interface. The phone's MAC address is SEP00093702281D and the phone number is 23675. The interface is divided into a left sidebar with navigation options and a main content area displaying call statistics.

**Stream Statistics**

RTP Statistics			
Domain Name	snmpUDPDomain	Remote Address	0.0.0.0
Remote Port	0	Local Address	0.0.0.0
Local Port	0	Sender Joins	0
Receiver Joins	0	Byes	0
Start Time	12.00.00 AM	Row Status	Not Ready
Host Name	SEP00093702281D	Sender Packets	0
Sender Octets	0	Sender Tool	G.711u
Sender Reports	0	Sender Report Time	12.00.00 AM
Sender Start Time	12.00.00 AM	Receiver Packets	0
Receiver Octets	0	Receiver Tool	G.711u
Receiver Lost Packets	1	Receiver Jitter	0
Receiver Reports	0	Receiver Start Time	12.00.00 AM

**Voice Quality Metrics**

MOS LQK	0.0000	Avg MOS LQK	0.0000
Min MOS LQK	0.0000	Max MOS LQK	0.0000
MOS LQK Version	0.95	Cumulative Conceal Ratio	0.0000
Interval Conceal Ratio	0.0000	Max Conceal Ratio	0.0000
Conceal Seconds	0	Severly Conceal Seconds	0

At the bottom of the interface, there are 'Refresh' and 'Stop' buttons.

# 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/products\\_administration\\_guide\\_chapter09186a008079b4ce.html](http://www.cisco.com/en/US/products/hw/phones/ps379/products_administration_guide_chapter09186a008079b4ce.html)

## Configuring Phones with the Web Interface

The phone has an HTTPS enabled web interface that you can access via the 802.11 a/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**”.

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/products\\_administration\\_guide\\_chapter09186a008079b476.html](http://www.cisco.com/en/US/products/hw/phones/ps379/products_administration_guide_chapter09186a008079b476.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.
- If using 802.1x authentication via LEAP, EAP-FAST or AKM authentication modes, you must configure a username and password.
- If using WPA 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.

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



## Cisco Unified Wireless IP Phone 7921G

SEP00093702281D

Phone DN 23675

HOME
SETUP
<b>NETWORK PROFILES</b>
Profile 1
Profile 2
Profile 3
Profile 4
USB SETTINGS
TRACE SETTINGS
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD

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

**Wireless**

Profile Name:

SSID:

Single Access Point:  True  False

Call Power Save Mode:

802.11 Mode:

**WLAN Security**

Authentication Method:

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

**IP Network Configuration**

Obtain IP address and DNS servers automatically

Use the following IP address and DNS servers

IP Address:

Subnet Mask:

Default Router:

Primary DNS Server:

Secondary DNS Server:

Domain Name:

**TFTP**

Obtain TFTP servers automatically

Use the following TFTP servers

TFTP Server 1:

TFTP Server 2:

Reset Save

Copyright (c) 2006 by Cisco Systems, Inc.

## 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 WLAN, then you must configure this parameter.

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

Disable only those channels that are not used in the WLAN. 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 WLAN successfully.

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

- USB cable connected to the PC.
- Full web access enabled in the Cisco Unified CallManager
- Re-enable all channels by using the factory default

**Cisco Unified Wireless IP Phone 7921G**  
SEP00093702281D

Phone DN 23675

Network Profile 1 Advanced Settings **Basic Profile 1**

**TSPEC Settings**

Minimum PHY Rate: 12 Mbps

Surplus Bandwidth: 1.000000

**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"/>	16 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

check all clear all check non-overlap

**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			

check all clear all check non-DFS

Save

Copyright (c) 2006 by Cisco Systems, Inc.

## Using Templates to Configure Phones

You can import and export phone configuration templates to the phone for fast configuration. The web interface, under Backup Settings encrypts the configuration file. You must specify the encryption key before exporting the file.

To export WLAN security information, such as authentication, username/password, pre-shared key, WEP keys, to a template, you must set the network profile to allow this capability. In the network profile that you want to use as a template, set “**Export Security Credentials**” to “**True**”. Then you can import this information to other Cisco Unified Wireless IP Phone 7921G phones.

The screenshot shows the Cisco Unified Wireless IP Phone 7921G web interface. On the left is a navigation menu with items: HOME, SETUP, NETWORK PROFILES +, USB SETTINGS, TRACE SETTINGS, INFORMATION, NETWORK, WIRELESS LAN, DEVICE, STATISTICS, WIRELESS LAN, NETWORK, STREAM STATISTICS, STREAM 1, STREAM 2, SYSTEM, TRACE LOGS, **BACKUP SETTINGS**, PHONE UPGRADE, and CHANGE PASSWORD. The main content area is titled 'Cisco Unified Wireless IP Phone 7921G' and 'SEP00093702281D'. Below this, it shows 'Phone DN 23675'. The 'Backup Settings' section is active, showing 'Import Configuration' and 'Export Configuration'. The 'Import Configuration' section has an 'Encryption Key' input field, an 'Import File' field with a 'Browse...' button, and an 'Import' button. The 'Export Configuration' section has an 'Encryption Key' input field and an 'Export' button. At the bottom, there is a copyright notice: 'Copyright (c) 2006 by Cisco Systems, Inc.'

## Setting the Phone to Factory Default

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**”.

## Upgrading Firmware

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.

Cisco Unified CallManager 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 CallManager 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 CallManager, 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.

## Localization

The Cisco Unified Wireless IP Phone 7921G currently supports these languages. Other languages will be supported in the future.

- English
- French
- German
- Japanese

You must install the Locale packages to enable language support for these languages. English is the default language on the phone.

Download the locale packages from the Localization page at

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

## Healthcare Environments

This product is not intended for use with patient monitoring devices or other patient care devices, and should not be used as a primary communications tool in healthcare environments as it may use an unregulated frequency band 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.

Cover cases can protect the phone from moisture, dust, and dirt, and provide drop protection.

## Available Phone Accessories

You can order these accessories for the phone. 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\\_guide09186a008076b878.html](http://www.cisco.com/en/US/products/hw/phones/ps379/products_user_guide09186a008076b878.html)

- Carry Cases (also available at [www.zcover.com](http://www.zcover.com))
- Headsets ([www.plantronics.com/cisco](http://www.plantronics.com/cisco) and [www.jabra.com](http://www.jabra.com))
- Desktop Charger
- Multi-Charger (available mid year 2007)
- Lock Set

The Cisco Unified Wireless IP Phone 7921G Multi-charger works well for locations where users share a common charging area, such as shift rooms.

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

## Additional Documentation

Cisco Unified Wireless IP Phone 7921G Datasheet

[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 Documentation

[http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_ipphon/english/wip7921](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/wip7921)

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>

Mobility SRND

<http://www.cisco.com/univercd/cc/td/doc/solution/emblty30.pdf>

Access Points Using Lightweight Documentation

<http://www.cisco.com/univercd/cc/td/doc/product/wireless/control/index.htm>

Access Points Using Autonomous Solution Documentation

<http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1200/accsspts/b1238ja/1238jasc/index.htm>

---

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0612R)

© 2007 Cisco Systems, All rights reserved.