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
02/28/07	1.0(1) Release
03/16/08	1.0(5) Release
10/13/08	1.1(1) and 1.2(1) Release
11/17/09	1.3(2) and 1.3(3) Release
05/03/10	1.3(4) Release
12/15/10	1.4(1) Release
08/14/12	1.4(1)SR1 and 1.4(2) Release
08/21/12	1.4(3) Release
03/22/13	1.4(3)SR1
05/24/13	1.4(4) Release
08/20/13	1.4(5) Release
07/16/14	1.4(5)SR1 Release

Contents

Cisco Unified Wireless IP Phone 7921G Overview

The Cisco Unified Wireless IP Phone 7921G provides mobile communication within enterprises. The levels of voice quality performance that have come to be expected from Cisco products are maintained in the Cisco Unified Wireless IP Phone 7921G with the inclusion of Cisco Compatible eXtensions (CCX).
Cisco's implementation of 802.11, employing CCX, permits time sensitive applications such as voice to operate efficiently across campus wide wireless LAN (WLAN) deployments. These extensions provide fast roaming capabilities and an almost seamless flow of voice traffic, whilst maintaining security as the end user roams between access points.

It should be understood that WLAN uses unlicensed spectrum, and as a result it may experience interference from other devices using the unlicensed spectrum. The proliferation of devices in the 2.4 GHz spectrum, such as Bluetooth headsets, Microwave ovens, cordless consumer phones, means that the 2.4 GHz spectrum may contain more congestion than other spectrums. The 5 GHz spectrum has far fewer devices operating in this spectrum and is the preferred spectrum to operate the Cisco Unified Wireless IP Phone 7921G in order to take advantage of the 802.11a data rates available. Despite the optimizations that Cisco have implemented in the Cisco Unified Wireless IP Phone 7921G, the use of unlicensed spectrum means that uninterrupted communication can not be guaranteed, and there may be the possibility of voice gaps of up to several seconds during multimedia conversations. Adherence to the deployment guidelines will reduce the likelihood of these voice gaps being present, but there is always this possibility. Through the use of unlicensed spectrum, and the inability to guarantee the delivery of messages to a WLAN device, the Cisco Unified Wireless IP Phone 7921G is not intended as a medical device and should not be used to make clinical decisions.

Requirements

The Cisco Unified Wireless IP Phone 7921G is an IEEE 802.11a/b/g wireless IP phone that provides voice communications.

The wireless LAN must be validated to ensure it meets the requirements to deploy the Cisco Unified Wireless IP Phone 7921G.

Site Survey

Before deploying the Cisco Unified Wireless IP Phone 7921G 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 frequency 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 frequency band for operation and even more highly recommended when the Cisco Unified Wireless IP Phone 7921G is to be used in a mission critical environment. The site survey will include heatmaps showing the intended coverage plan for the location. The site survey will also determine the access point platform type, antenna type, and access point configuration (channel and transmit power) to use at the location. It is recommended to select an access point with integrated antennas for non-rugged environments (e.g. office, healthcare, education, hospitality) and an access point platform requiring external antennas for rugged environments (e.g. manufacturing, warehouse, retail).
See the Designing the Wireless LAN for Voice section for more information.

Refer to the Steps to Success website for additional information.
http://www.cisco.com/go/stepstosuccess

RF Validation

In order to determine if VoWLAN can be deployed, the environment must be evaluated to ensure the following items meet Cisco guidelines.

Signal

The cell edge should be designed to -67 dBm where there is a 20-30% overlap of adjacent access points at that signal level.

This ensures that the Cisco Unified Wireless IP Phone 7921G always has adequate signal and can hold a signal long enough in order to roam seamlessly where signal based triggers are utilized vs. packet loss triggers.

Also need to ensure that the upstream signal from the Cisco Unified Wireless IP Phone 7921G meets the access point's receiver sensitivity for the transmitted data rate. Rule of thumb is to ensure that the received signal at the access point is -67 dBm or higher.

It is recommended to design the cell size to ensure that the Cisco Unified Wireless IP Phone 7921G can hold a signal for at least 5 seconds.

Channel Utilization

Channel Utilization levels should be kept under 50%.

If using the 7921G phone, this is provided via the QoS Basic Service Set (QBSS), which equates to around 105.

Noise

Noise levels should not exceed -92 dBm, which allows for a Signal to Noise Ratio (SNR) of 25 dB where a -67 dBm signal should be maintained.

Also need to ensure that the upstream signal from the Cisco Unified Wireless IP Phone 7921G can meet the access point's signal to noise ratio for the transmitted data rate.

Packet Loss / Delay

Per voice guidelines, packet loss should not exceed 1% packet loss; otherwise voice quality can be degraded significantly.

Jitter should be kept at a minimal (< 100 ms).

Retries

802.11 retransmissions should be less than 20%.

Multipath

Multipath should be kept to a minimal as this can create nulls and reduce signal levels.

Many different tools and applications can be used to evaluate these items in order to certify the deployment.

- Cisco Prime Network Control System (NCS) for Unified Wireless LAN Management

  http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps11682/ps11686/ps11688/data_sheet_c78-650051.html
- Cisco Wireless Control System (WCS) for Unified Wireless LAN Management

  http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd802570d0.html
- Cisco Wireless LAN Solution Engine (WLSE) for Cisco Autonomous Wireless LAN Management

  http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6380/ps6563/ps3915/ps6839/product_data_sheet0900aecd80410b92.html
- Cisco Spectrum Expert

  http://www.cisco.com/en/US/prod/collateral/wireless/ps9391/ps9393/product_data_sheet0900aecd807033c3.html
- Cisco Unified Operations Manager

  http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6491/ps6705/ps6535/data_sheet_c78-636705.html
- AirMagnet (Survey, WiFi Analyzer, VoFi Analyzer, Spectrum Analyzer)

http://www.airmagnet.com

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 (CUCM)

  Minimum = 4.1
  Recommended = 8.6 and later

- Cisco Unified Communications Manager Express (CUCME)

  Minimum = 4.1

  Recommended = 8.6 and later

- Cisco Unified Survivable Remote Site Telephony (SRST)

  Minimum = 4.1

  Recommended = 8.6 and later

Note: 12.4(15)T7 is the minimum IOS Version for CUCME and SRST.

Device Support in Cisco Unified Communications Manager

Cisco Unified Communications Manager requires a device package to be installed 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 the following location.
http://software.cisco.com/download/navigator.html?mdfid=278875240

Protocols

Supported voice and wireless LAN protocols include the following:

- CCX v4
- Wi-Fi MultiMedia (WMM)
- Unscheduled Auto Power Save Delivery (U-APSD)
- Traffic Specification (TSPEC)
- Traffic Classification (TCLAS)
- Skinny Call Control Protocol (SCCP)
- Real Time Protocol (RTP)
- G.711, G.722, G.729, iLBC
- Real Time Control Protocol (RTCP)
- Cisco Discovery Protocol (CDP)

- Syslog

Access Points

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

Below is the supported version information for each Cisco solution.

- Cisco Unified Wireless LAN Controller
  Minimum = 6.0.202.0 (7.0.116.0 and 7.0.230 are not supported)
  Recommended = 7.0.250.0, 7.4.121.0, 7.6.120.0
- Cisco IOS Access Points (Autonomous)
  Minimum = 12.4(21a)JY
  Recommended = 12.4(25d)JA2, 15.2(4)JA1

The supported access point models are listed below.

Note: The Cisco Unified Wireless IP Phone 7921G is supported with the Cisco AP3600 when the internal 802.11abgn radio is utilized, however if the 802.11ac module (AIR-RM3000AC) for the Cisco AP3600 is installed, then Cisco Unified Wireless LAN Controller release 7.6.100.0 or later is required.

The table below lists the modes that are supported by each Cisco Access Point.

Cisco AP Series	802.11a	802.11b	802.11g	802.11n	802.11ac	Unified	Autonomous
500	No	Yes	Yes	No	No	Yes	Yes
600	Yes	Yes	Yes	Yes	No	Yes	No
700	Yes	Yes	Yes	Yes	No	Yes	No
1040	Yes	Yes	Yes	Yes	No	Yes	Yes
1100	No	Yes	Optional	No	No	Yes	Yes
1130 AG	Yes	Yes	Yes	No	No	Yes	Yes
1140	Yes	Yes	Yes	Yes	No	Yes	Yes
1200	Optional	Yes	Optional	No	No	Yes	Yes
1230 AG	Yes	Yes	Yes	No	No	Yes	Yes
1240 AG	Yes	Yes	Yes	No	No	Yes	Yes
1250	Yes	Yes	Yes	Yes	No	Yes	Yes
1260	Yes	Yes	Yes	Yes	No	Yes	Yes
1600	Yes	Yes	Yes	Yes	No	Yes	Yes
2600	Yes	Yes	Yes	Yes	No	Yes	Yes
3500	Yes	Yes	Yes	Yes	No	Yes	Yes
3600	Yes	Yes	Yes	Yes	Yes (with AIR-RM3000 AC module)	Yes	Yes
3700	Yes	Yes	Yes	Yes	Yes	Yes	Yes
860	No	Yes	Yes	Yes	No	No	Yes
870	No	Yes	Yes	No	No	No	Yes
880	No	Yes	Yes	Yes	No	Yes	Yes
890	Yes	Yes	Yes	Yes	No	Yes	Yes
UC500	No	Yes	Yes	No	No	No	Yes

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

Limited support is provided when using 3rd party access points as there are no interoperability tests performed for 3rd party access points.

However the user should have basic functionality when connected to a Wi-Fi compliant access point.

Some of the key features are the following:

- 5 GHz (802.11a/n)
- Wi-Fi Protected Access v2 (WPA2+AES)
- Wi-Fi Multimedia (WMM)
- Unscheduled Automatic Power Save Delivery (U-APSD)
- Traffic Specification (TSPEC)
- Traffic Classification (TCLAS)
- Differentiated Services Code Point (DSCP)
- Class of Service (CoS / 802.1p)
- QoS Basic Service Set (QBSS)

The Cisco Unified Wireless IP Phone 7921G can take advantage of Cisco Client Extensions (CCX) enabled access points.

Some of the key features are the following:

- Cisco Centralized Key Management (CCKM)
- Dynamic Transmit Power Control (DTPC)
- Proxy ARP

http://www.cisco.com/web/partners/pr46/pr147/partners_pgm_concept_home.html

http://www.cisco.com/web/partners/pr46/pr147/program_additional_information_new_release_features.html

Antennas

Some of the Cisco Access Points require or allow external antennas.

Please refer to the following URL for the list of supported antennas and how these external antennas should be mounted.

http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/product_data_sheet09186a008008883b.html

3rd party antennas are not supported, as there is no interoperability testing performed against 3rd party antennas including Distributed Antenna Systems (DAS) and Leaky Coaxial Systems.

Please refer to the following URL for more info on Cisco Wireless LAN over Distributed Antenna Systems.

http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6973/positioning_statement_c07-565470.html

Note: The Cisco 1040, 1130, 1140, 1602i, 2602i, 3502i, 3602i, and 3702i Series Access Points are to be mounted on the ceiling as they have omni-directional antennas and are not designed to be patches.

Models

There are four Cisco Unified Wireless IP Phone 7921G models.

All Cisco Unified Wireless IP Phone 7921G models support 802.11d therefore can adapt to local channels and transmit powers per region as necessary, where channels operating on frequencies 2.412 - 2.484 GHz and 5.180 GHz - 5.805 GHz can be utilized if available.

The regulatory domain can be identified by navigating to **Settings > Model Information > WLAN Regulatory Domain** and then referencing the Regulatory Domain number in the table below.

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

Part Number	Regulatory Domain	Regulatory Domain Number	Frequency Ranges	Available Channels	Channel Set
CP-7921G-A-K9	FCC (Americas)	1050	2.412 - 2.462 GHz 5.180 - 5.240 GHz 5.260 - 5.320 GHz 5.500 - 5.700 GHz 5.745 - 5.805 GHz	11 4 4 8 4	1-11 36,40,44,48 52,56,60,64 100-140 149,153,157,161
CP-7921G-E-K9	ETSI (Europe)	3051	2.412 - 2.472 GHz 5.180 - 5.700 GHz	13 16	1-13 36-48,52-64,100-140
CP-7921G-P-K9	Japan	4157	2.412 - 2.472 GHz 2.412 - 2.484 GHz 5.180 - 5.700 GHz	13 (802.11g) 14 (802.11b) 16	1-13 1-14 36-48,52-64,100-140
CP-7921G-W-K9	Rest of World	5252	Uses 802.11d to identify available channels and transmit powers. Channels operating at 2.412 GHz - 2.484 GHz and 5.180 GHz - 5.805 GHz are supported.		

Note: Channels 120, 124, 128 are not supported in the Americas, Europe, or Japan, but may be in other regions around the world.

802.11j (channels 34, 38, 42, 46) and channel 165 are not supported.

Channel 14 for Japan is not supported on the newer Cisco Access Points.

World Mode (802.11d)

World Mode allows a client to be used in different regions, where the client can adapt to using the channels and transmit powers advertised by the access point in the local environment.

If using the Cisco Unified Wireless IP Phone 7921G World (-W) model, then it is required to enable 802.11d.

All Cisco Unified Wireless IP Phone 7921G models give 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.

Some 5 GHz channels are also used by radar technology, which requires that the 802.11 client and access point be 802.11h compliant if utilizing those radar frequencies (DFS channels). 802.11h requires 802.11d to be enabled.

The Cisco Unified Wireless IP Phone 7921G will passively scan DFS channels first before engaging in active scans of those channels.

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, enable 802.11d to discover which channels can potentially be 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.

If using 2.4 GHz (802.11b/g) and 802.11d is not enabled, then the Cisco Unified Wireless IP Phone 7921G can attempt to use channels 1-11 and reduced transmit power.

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

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

Radio Characteristics

The following table lists the data rates, ranges, and receiver sensitivity info for Cisco Unified Wireless IP Phone 7921G.

802.11a	**Data Rate**	**Modulation**	**Range**	**Receiver Sensitivity**
Max Tx Power is 16 dBm	6 Mbps	OFDM - BPSK	610 ft (186 m)	-89 dBm
	9 Mbps	OFDM - BPSK	610 ft (186 m)	-88 dBm
	12 Mbps	OFDM - QPSK	558 ft (170 m)	-86 dBm
	18 Mbps	OFDM - QPSK	541 ft (165 m)	-85 dBm
	24 Mbps	OFDM - 16 QAM	508 ft (155 m)	-82 dBm
	36 Mbps	OFDM - 16 QAM	426 ft (130 m)	-80 dBm
	48 Mbps	OFDM - 64 QAM	328 ft (100 m)	-76 dBm
	54 Mbps	OFDM - 64 QAM	295 ft (90 m)	-74 dBm
802.11g	**Data Rate**	**Modulation**	**Range**	**Receiver Sensitivity**
Max Tx Power is 16 dBm	6 Mbps	OFDM - BPSK	722 ft (220 m)	-90 dBm
	9 Mbps	OFDM - BPSK	656 ft (200 m)	-89 dBm
	12 Mbps	OFDM - QPSK	623 ft (190 m)	-87 dBm
	18 Mbps	OFDM - QPSK	623 ft (190 m)	-85 dBm
	24 Mbps	OFDM - 16 QAM	623 ft (190 m)	-82 dBm
	36 Mbps	OFDM - 16 QAM	492 ft (150 m)	-78 dBm
	48 Mbps	OFDM - 64 QAM	410 ft (125 m)	-74 dBm
	54 Mbps	OFDM - 64 QAM	394 ft (120 m)	-73 dBm
802.11b	**Data Rate**	**Modulation**	**Range**	**Receiver Sensitivity**
Max Tx Power is 17 dBm	1 Mbps	DSSS - BPSK	1,027 ft (313 m)	-95 dBm
	2 Mbps	DSSS - QPSK	951 ft (290 m)	-89 dBm
	5.5 Mbps	DSSS - CCK	853 ft (260 m)	-89 dBm
	11 Mbps	DSSS - CCK	787 ft (240 m)	-85 dBm

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

The above values are pure radio specifications and do not account for the gain of the single integrated antenna.

See the Designing the Wireless LAN for Voice section for more information on signal requirements.

Language Support

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

Bulgarian	French	Portuguese
Catalan	German	Romanian
Chinese	Greek	Russian
Croatian	Hungarian	Serbian
Czech	Italian	Slovak
Danish	Japanese	Slovenian

Dutch	Korean	Spanish
English	Norwegian	Swedish
Finnish	Polish	

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

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

http://software.cisco.com/download/navigator.html?mdfid=278875240

Security

When deploying a wireless LAN, security is essential.

The Cisco Unified Wireless IP Phone 7921G supports the following wireless security features.

WLAN Authentication

- WPA (802.1x authentication + TKIP or AES encryption)
- WPA2 (802.1x authentication + AES or TKIP encryption)
- WPA-PSK (Pre-Shared key + TKIP encryption)
- WPA2-PSK (Pre-Shared key + AES encryption)
- EAP-FAST (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling)
- EAP-TLS (Extensible Authentication Protocol - Transport Layer Security)
- PEAP-MSCHAPv2 (Protected Extensible Authentication Protocol - Microsoft Challenge Handshake Authentication Protocol version 2)
- LEAP (Lightweight Extensible Authentication Protocol)
- CCKM (Cisco Centralized Key Management)
- Open
- Shared Key

WLAN Encryption

- AES (Advanced Encryption Scheme)
- TKIP / MIC (Temporal Key Integrity Protocol / Message Integrity Check)
- WEP (Wired Equivalent Protocol) 40/64 and 104/128 bit

The Cisco Unified Wireless IP Phone 7921G also supports the following additional security features.

- X.509 Digital 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

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

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

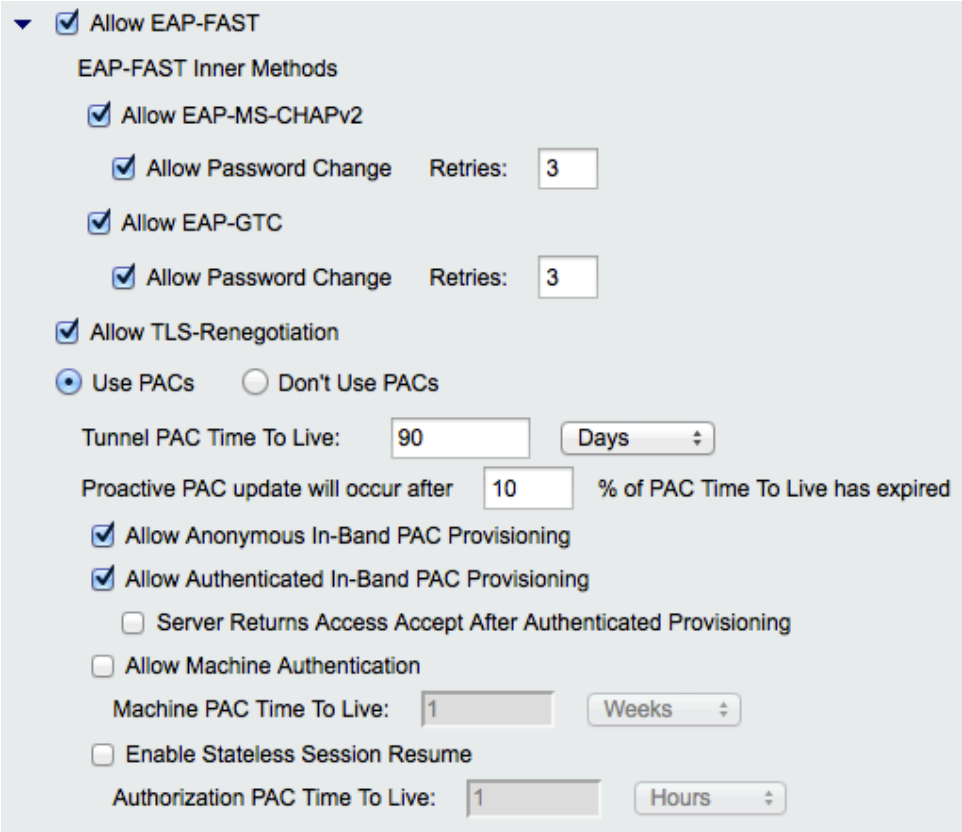
The TLS tunnel uses Protected Access Credentials (PACs) for authentication between the client (phone) and the RADIUS server. The server sends an Authority ID (AID) to the client (phone), which in turn selects the appropriate PAC. The client (phone) returns a PAC-Opaque to the RADIUS server. The server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

To enable EAP-FAST, a certificate must be installed on to the RADIUS server.

The Cisco Unified Wireless IP Phone 7921G currently support automatic provisioning of the PAC only, so enable **Allow anonymous in-band PAC provisioning** on the RADIUS server as shown below.

Both EAP-GTC and EAP-MSCHAPv2 must be enabled when **Allow anonymous in-band PAC provisioning** is enabled.

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



If anonymous PAC provisioning is not allowed in the production wireless LAN environment then a staging Cisco ACS can be setup for initial PAC provisioning of the Cisco Unified Wireless IP Phone 7921G.

This requires that the staging ACS server be setup as a slave EAP-FAST server and components are replicated from the product master EAP-FAST server, which include user and group database and EAP-FAST master key and policy info.

Ensure the production master EAP-FAST ACS server is setup to send the EAP-FAST master keys and policies to the staging slave EAP-FAST ACS server, which will then allow the Cisco Unified Wireless IP Phone 7921G to use the provisioned PAC in the production environment where **Allow anonymous in-band PAC provisioning** is disabled.

When it is time to renew the PAC, then authenticated in-band PAC provisioning will be used, so ensure that **Allow authenticated in-band PAC provisioning** is enabled.

Ensure that the Cisco Unified Wireless IP Phone 7921G has connected to the network during the grace period to ensure it can use its existing PAC created either using the active or retired master key in order to get issued a new PAC.

Is recommended to only have the staging wireless LAN pointed to the staging ACS server and to disable the staging access point radios when not being used.

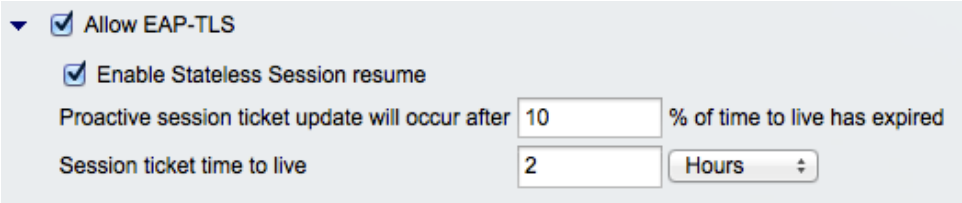
Extensible Authentication Protocol - Transport Layer Security (EAP-TLS)

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.

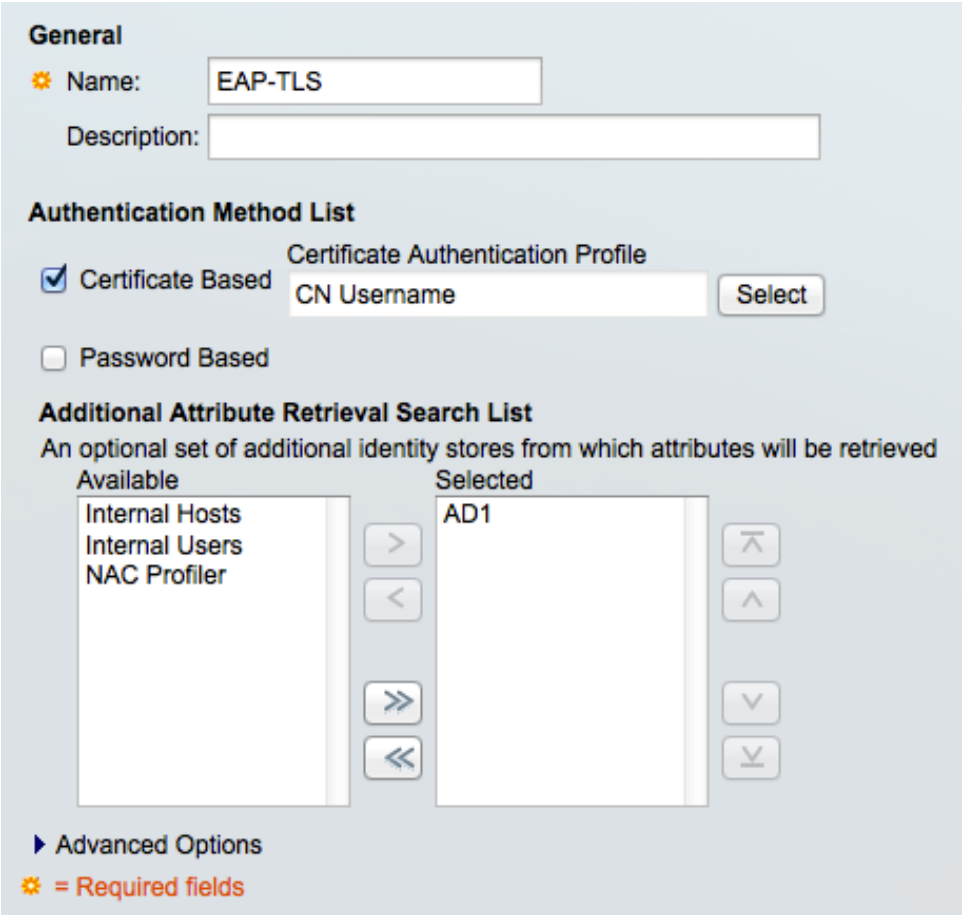
Either the internal Manufacturing Installed Certificate (MIC) or a user installed certificate can be used for authentication.

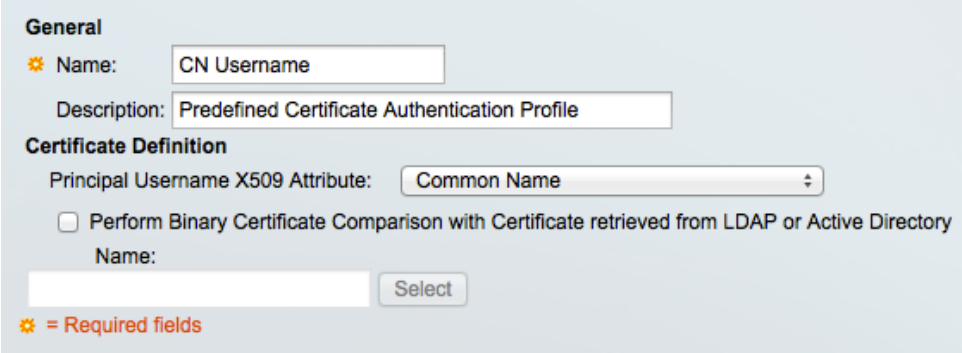
EAP-TLS provides excellent security, but requires client certificate management.



EAP-TLS may also require a user account to 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 and that EAP-TLS is the only EAP type enabled on the RADIUS server.





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.

PEAP-MSCHAPv2 is the current supported inner authentication protocol (GTC is not supported).

PEAP-MSCHAPv2 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.

For more information on Cisco Secure Access Control System (ACS), refer to the following links.

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps2086/ps7032/product_data_sheet09186a00800887d5.html

http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps5698/ps6767/ps9911/data_sheet_c78-614584.html

Note: If using a 3rd party RADIUS server, ensure that PEAP v0 (MSCHAPv2) is enabled. PEAP v1 (GTC) is not supported.

Fast Secure Roaming (FSR)

CCKM is the recommended deployment model for all environment types where frequent roaming occurs.

CCKM enables fast secure roaming and limits the off-network time to keep audio gaps at a minimum when on call.

802.1x authentication is required in order to utilize CCKM.

802.1x without CCKM can introduce delay during roaming due to its requirement for full re-authentication. WPA and WPA2 introduce additional transient keys and can lengthen roaming time.

CCKM centralizes the key management and reduces the number of key exchanges.

When CCKM is utilized, roaming times can be reduced from 400-500 ms to less than 100 ms, where that transition time from one access point to another will not be audible to the user.

As of the 1.3(4) release, the Cisco Unified Wireless IP Phone 7921G supports CCKM with WPA2 (AES or TKIP), WPA (TKIP or AES) and 802.1x (WEP) authentication, where WPA2 (AES) with CCKM is recommended.

EAP Type	Key Management	Encryption
EAP-FAST	802.1x, WPA, WPA2	AES, TKIP, WEP (40/64 or 104/128 bit)
EAP-TLS	802.1x, WPA, WPA2	AES, TKIP, WEP (40/64 or 104/128 bit)
PEAP	802.1x, WPA, WPA2	AES, TKIP, WEP (40/64 or 104/128 bit)
LEAP	802.1x, WPA, WPA2	AES, TKIP, WEP (40/64 or 104/128 bit)
AKM	802.1x, WPA, WPA2	AES, TKIP, WEP (40/64 or 104/128 bit)

CCKM was not supported with WPA2 in release 1.3(3) or earlier.

WPA Version	Cipher	Supported
WPA	TKIP	Yes
	AES	1.3(4) and later
WPA2	TKIP	1.3(4) and later
	AES	1.3(4) and later

EAP and User Database Compatibility

The following chart displays the EAP and database configurations supported by the Cisco Unified Wireless IP Phone 7921G.

Database Type	LEAP	EAP-FAST (Phase Zero)	EAP-TLS	PEAP-MSCHAPv2
Cisco ACS	Yes	Yes	Yes	Yes
Windows SAM	Yes	Yes	No	Yes
Windows AD	Yes	Yes	Yes	Yes
LDAP	No	No	Yes	No
ODBC (ACS for Windows Only)	Yes	Yes	Yes	Yes
LEAP Proxy RADIUS Server	Yes	Yes	No	Yes
All Token Servers	No	No	No	No

Power Management

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

The standard battery (1400 mAh) can provide up to 150 hours of standby time or up to 11.5 hours of talk time.

The extended battery (1860 mAh) can provide up to 200 hours of standby time or up to 15.5 hours of 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 the access point supports the Cisco Client Extensions (CCX) proxy ARP information element, the idle battery life will be optimized. Proxy ARP allows the Cisco Unified Wireless IP Phone 7921G to remain in sleep mode longer versus waking up at each Delivery Traffic Indicator Message (DTIM) period to check for incoming broadcasts.

To optimize battery life, the Cisco Unified Wireless IP Phone 7921G will utilize either U-APSD or PS-POLL power save methods depending on whether Wi-Fi MultiMedia (WMM) is enabled in the Access Point configuration or not.

U-APSD will be utilized when WMM is enabled on the Access Point.

When on call U-APSD, PS-POLL, or active mode will be utilized depending on the Cisco Unified Wireless IP Phone 7921G call power save mode configuration and the access point configuration.

When in idle (no active call), the Cisco Unified Wireless IP Phone 7921G depending on the Access Point configuration will utilize U-APSD or PS-POLL.

The current battery technology allows for around 300-500 full charging cycles (charging from empty to full) before it will lose around 20-30% of its capacity, therefore the battery should be replaced every 2-3 years.

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
2.4 GHz	On Call	11.5	15.5
	Idle	150	200
5 GHz	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.

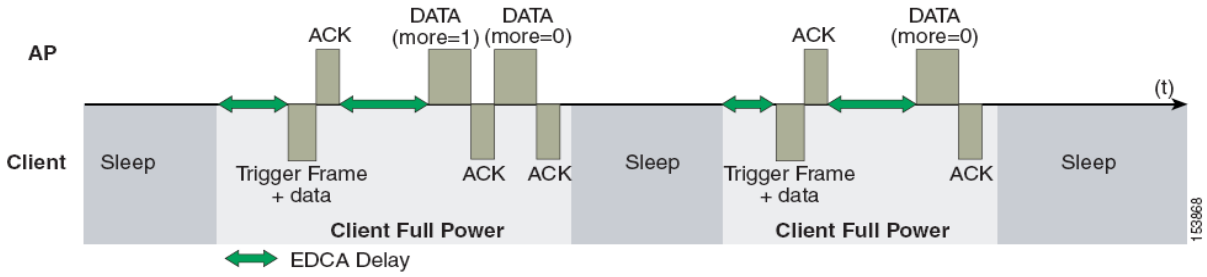
Protocols

Unscheduled Auto Power Save Delivery (U-APSD)

The Cisco Unified Wireless IP Phone 7921G will utilize U-APSD (Unscheduled Auto Power Save Delivery) for power management as long as Wi-Fi MultiMedia (WMM) is enabled in the access point configuration and the call power save mode on the Cisco Unified Wireless IP Phone 7921G is set to U-APSD/PS-POLL.

U-APSD helps optimize battery life and reduces management overhead.

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



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.

If proxy ARP is enabled, then the Cisco Unified Wireless IP Phone 7921G does not have to wake up at DTIM.

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

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.

If multiple multicast streams exist on the wireless LAN frequently, then it is recommended to set the DTIM period to **1**.

Scan Modes

There are three different scan modes (**Auto**, **Continuous**, **Single AP**), which can be configured for the Cisco Unified Wireless IP Phone 7921G in the Cisco Unified Communications Manager.

When using multiple access points where seamless roaming is required, **Auto** (default) or **Continuous** scan mode should be enabled (**Single AP** scan mode should not be used if multiple access points exist).

Auto scan mode is the default scan mode, which will optimize idle battery life as well as offer seamless roaming.

When on an active call with **Auto** scan mode enabled, the Cisco Unified Wireless IP Phone 7921G will continuously be scanning. If in idle (not on an active call) and **Auto** scan mode is enabled, then the Cisco Unified Wireless IP Phone 7921G will only start to scan once the scan threshold is met for the currently connected access point.

Continuous scan mode is recommended for environments where frequent roams occur or where smaller cells (pico cells) exist.

Continuous scan mode can also help with location tracking.

With **Continuous** scan mode, scans occur regardless of the current call state (idle or on call) or current access point signal level (RSSI). There will be a slight decrease in idle battery life when using **Continuous** scan mode in comparison to using **Auto** scan mode.

If using only one access point, select **Single AP** mode on the Cisco Unified Wireless IP Phone 7921G to reduce scanning and optimize battery life.

Quality of Service (QoS)

Quality of Service enables queuing to ensure high priority for voice traffic.

To enable proper queuing for voice and call control traffic use the following guidelines.

- Ensure that **WMM** is enabled on the access point.
- Create a QoS policy on the access point giving priority to voice and call control traffic.

Traffic Type	DSCP	802.1p	WMM UP	Port Range
Voice	EF (46)	5	6	UDP 16384 - 32767
Call Control	CS3 (24)	3	4	TCP 2000

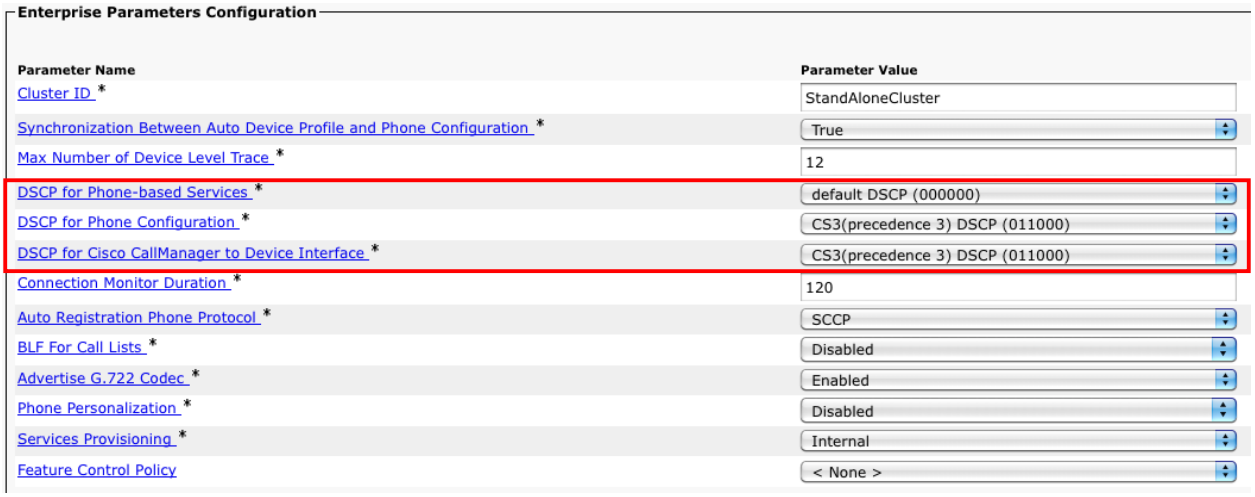
- Be sure that voice and call control packets have the proper QoS markings and other protocols are not using the same QoS markings.
- Select the **Platinum** QoS profile for the WLAN when using Cisco Unified Wireless LAN Controller technology and set the 802.1p tag to **5.**
- Enable Differentiated Services Code Point (DSCP) preservation on the Cisco IOS switch.

For more information about TCP and UDP ports used by the Cisco Unified Wireless IP Phone 7921G and the Cisco Unified Communications Manager, refer to the Cisco Unified Communications Manager TCP and UDP Port Usage document at this URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/port/8_6_1/portlist861.html

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.



Configuring QoS Policies for the Network

Configure QoS policies and settings for the following network devices.

Configuring Cisco Switch Ports

Configure the Cisco Unified Wireless LAN Controller and Cisco Access Point switch ports as well as any uplink switch ports.

Configure the Cisco Unified Wireless LAN Controller for trust COS.

Below is a sample switch configuration for the Cisco Unified Wireless LAN controller:

```
mls qos
!
interface X
 mls qos trust cos
```

Configure the Cisco Access Point switch ports as well as any uplink switch ports for trust DSCP.

Below is a sample switch configuration for an access point:

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

Note: When using the Cisco Unified Wireless LAN Controller, DSCP trust must be implemented or trust the UDP data ports used by the Cisco Unified Wireless LAN Controller (CAPWAP = 5246 and 5247) on all interfaces where wireless packets will traverse to ensure QoS markings are correctly set.

Configuring Cisco IOS Access Points

Use the following QoS policy on the Cisco IOS access point (AP) to enable DSCP to CoS (UP) mapping. This allows packets to be placed into the proper queue as long as those packets are marked correctly when received at the access point level.

```
class-map match-all Voice
 match ip dscp ef
class-map match-all CallControl
 match ip dscp cs3
!
policy-map 792x
 class Voice
  set cos 6
 class CallControl
  set cos 4
!
interface dot11radioX
```

service-policy input 792x
service-policy output 792x

Configuring Switch Ports for Wired IP Phones

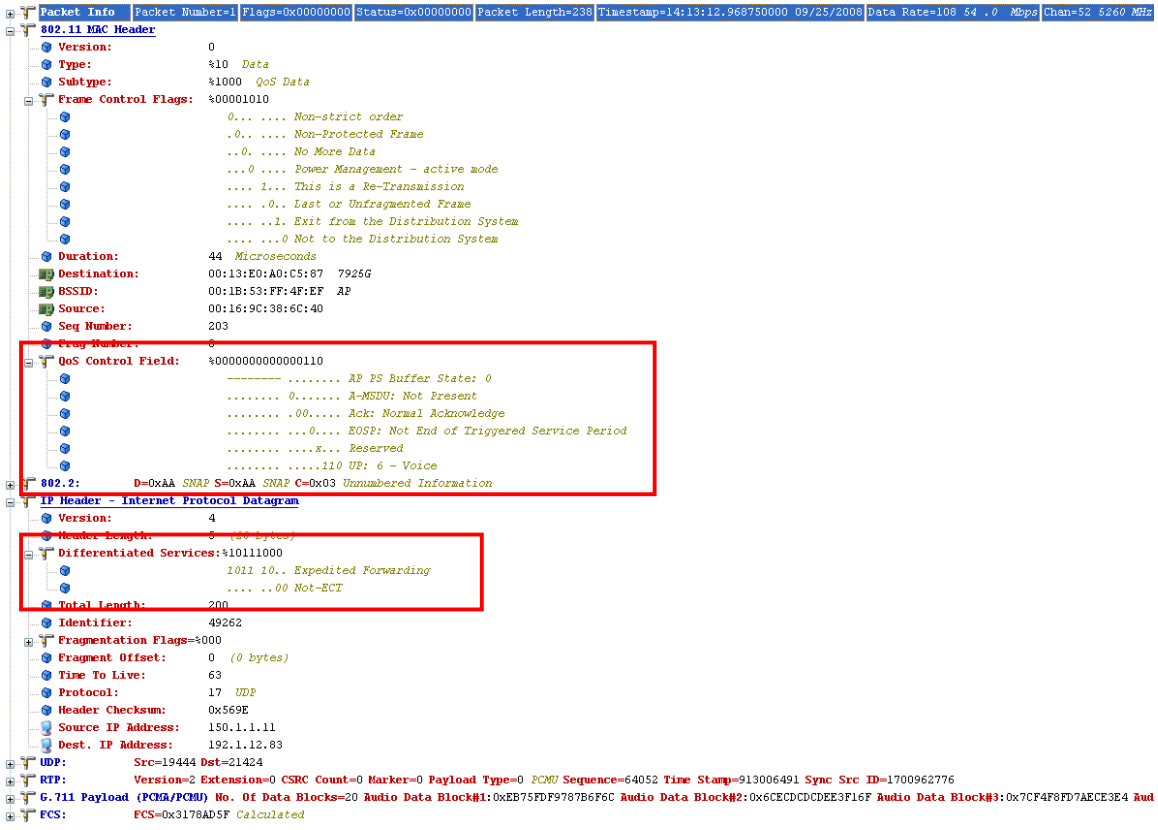
Enable the Cisco wired IP phone switch ports for Cisco phone trust

Below is a sample switch configuration:

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

Sample Voice Packet Capture

The packet capture below displays a voice packet bound for the Cisco Unified Wireless IP Phone 7921G over the air being marked as DSCP = EF and UP = 6.



Call Admission Control

Inbound and outbound call admission control should be enabled 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 (default = 75%)
- Set the bandwidth that is reserved for roaming clients (default = 6%)

The minimum PHY rate can be configured for which the phone is to use when Call Admission Control (CAC) is enabled.

- Enable a data rate that is enabled on the access point. (Default setting is 12 Mbps)
- Cisco Access Points will only accept a minimum PHY rate of 5.5, 6, 11, 12 or 24 Mbps, so ensure that at least one of these rates are enabled.

As of the 1.3(3) release, the Cisco Unified Wireless IP Phone 7921G will auto-negotiate the minimum PHY rate to be used for TSPEC. By default it will try the locally configured minimum PHY rate (e.g. 12 Mbps) first, but if that data rate is not enabled on the access point, then it will try the next highest enabled data rate on the access point. If there is not a higher data rate enabled, then it will then try the next lowest data rate as the minimum PHY rate.

In releases prior to 1.3(3), the Cisco Unified Wireless IP Phone 7921G would use the static minimum PHY rate configured locally, which required that rate to be enabled on the access point.

When using the 1.3(3) release or later and 12 Mbps is not enabled on the access point, then the next highest enabled data rate must be 24 Mbps. For example, if 12 Mbps is disabled but 18 Mbps is enabled, the phone will try the next highest rate of 18 Mbps and fail because that minimum PHY rate for CAC is not supported by the Cisco Access Point.

The dynamic minimum PHY rate is useful for deployments that require higher capacity where 24 Mbps and higher data rates are only enabled. For this high capacity deployment configuration and with release 1.3(3), the minimum PHY rate would be adjusted to 24 Mbps automatically even if the phone is configured statically for a minimum PHY rate of 12 Mbps. In releases prior to 1.3(3), the minimum PHY rate would have to be changed to 24 Mbps manually from the default of 12 Mbps in order for CAC to work correctly for this deployment configuration.

If an 802.11b AP is used, the highest available data rate would be 11 Mbps, so 12 Mbps can not be used as the minimum PHY rate. For this 802.11b (11 Mbps) deployment configuration and with release 1.3(3), the minimum PHY rate would be adjusted to 11 Mbps automatically even if the phone is configured statically for a minimum PHY rate of 12 Mbps. In releases prior to 1.3(3), the minimum PHY rate would have to be changed to 11 Mbps manually from the default of 12 Mbps in order for CAC to work correctly for this deployment configuration.

There is no support for load-based CAC or multiple streams on the Cisco Autonomous Access Points therefore it is not recommended to enable CAC on Cisco Autonomous Access Points.

If CAC is enabled on the Cisco Autonomous Access Point, then SRTP and barge calls will fail.

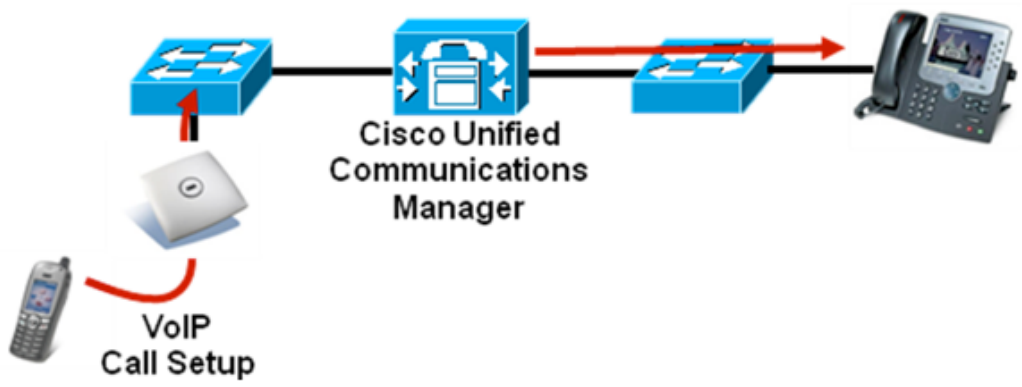
Pre-Call Admission Control

If Call Admission Control (TSPEC) is enabled on the access point, the Cisco Unified Wireless IP Phone 7921G will send 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 access point rejects the call and the Cisco Unified Wireless IP Phone 7921G has no other access point to roam to, then the phone will display **Network Busy**.

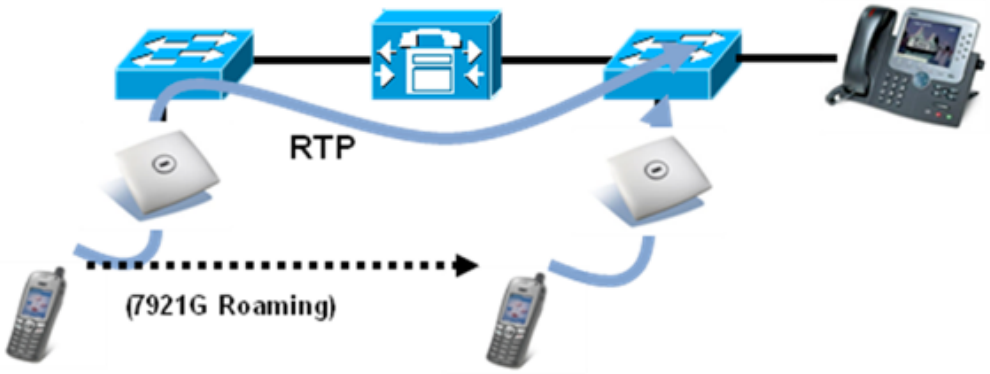
If the admission is refused for an inbound call there is no messaging from the Cisco Unified Wireless IP Phone 7921G to inform the remote endpoint that there is insufficient bandwidth to establish the call, so the call can continue to ring out within the system until the remote user terminates the call.



Roaming Admission Control

During a call, the Cisco Unified Wireless IP Phone 7921G measures Received Signal Strength Indicator (RSSI) 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 Cisco Unified Wireless IP Phone 7921G will send an ADDTS request during the roam to the new access point, which embedded in the reassociation request frame.



Traffic Classification (TCLAS)

Traffic Classification (TCLAS) helps to ensure that the access point properly classifies voice packets.

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 and later.

Using port based QoS policies is inadequate as all data packets use the same UDP port (LWAPP = 12222; or CAPWAP = 5246) and the access point uses the outside QoS marking to determine which queue the packets should be placed in.

With TCLAS, DSCP preservation is not a requirement.

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.

Roaming

CCKM is the recommended deployment model for all environment types where frequent roaming occurs.

802.1x authentication is required in order to utilize CCKM.

802.1x without CCKM can introduce delay during roaming due to its requirement for full re-authentication. WPA and WPA2 introduce additional transient keys and can lengthen roaming time.

When CCKM is utilized, roaming times can be reduced from 400-500 ms to less than 100 ms, where that transition time from one access point to another will not be audible to the user.

As of the 1.3(4) release, the Cisco Unified Wireless IP Phone 7921G supports CCKM with WPA2 (AES or TKIP), WPA (TKIP or AES), and 802.1x (WEP) authentication, where WPA2 (AES) with CCKM is recommended.

Authentication	Roaming Time
WPA/WPA2 Personal	150 ms
WPA/WPA2 Enterprise	300 ms
CCKM	< 100 ms

The scanning mechanism was enhanced in the 1.4(2) release to provide seamless interband roaming in the most challenging environments, including pico cell deployments.

The Cisco Unified Wireless IP Phone 7921G manages the scanning and roaming events; Client Roaming parameters in the Cisco Unified Wireless LAN Controller are not utilized.

Roaming can be triggered for either of the following reasons.

- RSSI Differential
- Max Tx Retransmissions (not receiving 802.11 acknowledgements from the access point)
- Missed Beacons
- Call Admission Control

The roaming trigger for the majority of roams should be due to meeting the required RSSI differential based on the current RSSI, which results in seamless roaming (no voice interruptions).

Unexpected roams are triggered either by missing contiguous 802.11 acknowledgements (Max Tx retransmissions) or missing beacons from the access point.

For seamless roaming to occur, the Cisco Unified Wireless IP Phone 7921G must be associated to an access point for at least 3 seconds, otherwise roams can occur based on packet loss (max tx retransmissions or missed beacons).

Roaming based on RSSI may not occur if the current signal has met the strong RSSI threshold.

Note: The Cisco Unified Wireless IP Phone 7921G does not utilize the RF parameters in the Client Roaming section of the Cisco Unified Wireless LAN Controller as scanning and roaming is managed independently by the phone itself.

Interband Roaming

Some deployments may use one frequency band for indoor (e.g. 5 GHz) and the other for outdoor coverage (e.g. 2.4 GHz). In this case, set the phone to either Auto-a or Auto-b/g mode, depending on the preferred frequency band.

For Auto-a and Auto-b/g modes, this is giving preference to one frequency band over another. At power on, the Cisco Unified Wireless IP Phone 7921G will scan all 2.4 GHz and 5 GHz channels then attempt to associate to an access point for the configured network using the preferred frequency band if available. If the preferred frequency band is not available, then the Cisco Unified Wireless IP Phone 7921G will try to use the less preferred frequency band if available. If the phone roams out of coverage of the preferred frequency band, where less preferred frequency band signal is available, then the Cisco Unified Wireless IP Phone 7921G will attempt to associate to that less preferred frequency band.

As of the 1.3(4) release, seamless interband roaming between 5 GHz and 2.4 GHz bands is supported as both frequency bands are now scanned simultaneously when on call or in idle if **Continuous** scan mode is enabled.

In order for the Cisco Unified Wireless IP Phone 7921G to roam from the preferred frequency band to the less preferred frequency band (e.g. roam to 2.4 GHz when configured for Auto-a mode), all access points in the preferred frequency band must have a signal lower than the preferred frequency band signal threshold as well as one access point in the less preferred frequency band meeting the RSSI differential threshold for roaming must be met. In order to roam back to the preferred frequency band, there must be at least one access point with sufficient signal matching the preferred frequency band signal threshold.

Prior to the 1.3(4) release, the Cisco Unified Wireless IP Phone 7921G would have to roam out of range of the current band before it would attempt to roam to an access point on the other frequency band when configured for an Auto 802.11 mode (e.g. Auto-a, Auto-b/g, Auto-RSSI), where the user may experience choppy audio with the weak signal connection, followed up with a small second audio gap before associating to the new frequency band. Once the Cisco Unified Wireless IP Phone 7921G failed over to a less preferred frequency band (e.g. associated to 802.11b/g when the phone is configured for Auto-a), there was no mechanism to guarantee the Cisco Unified Wireless IP Phone 7921G would roam back to the preferred frequency band when available again or not as only the connected frequency band would be scanned.

It is recommended to perform a spectrum analysis to ensure that the desired frequency ranges can be enabled in order to perform seamless interband roaming.

Multicast

When enabling multicast in the wireless LAN, 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 proxy ARP from CCX is enabled and the Cisco Unified Wireless IP Phone 7921G is not participating in a multicast session currently, then the access point is responsible to answer any ARP requests on behalf of the client and the Cisco Unified Wireless IP Phone 7921G can remain in sleep mode longer thus optimizing battery life.

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 guarantee that the packet will be received the by the client.

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

It is recommended to enable Multicast Direct in the Cisco Unified Wireless LAN Controller.

Designing the Wireless LAN

The following network design guidelines must be followed in order to accommodate for adequate coverage, call capacity and seamless roaming for the Cisco Unified Wireless IP Phone 7921G.

Planning Channel Usage

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

5 GHz (802.11a)

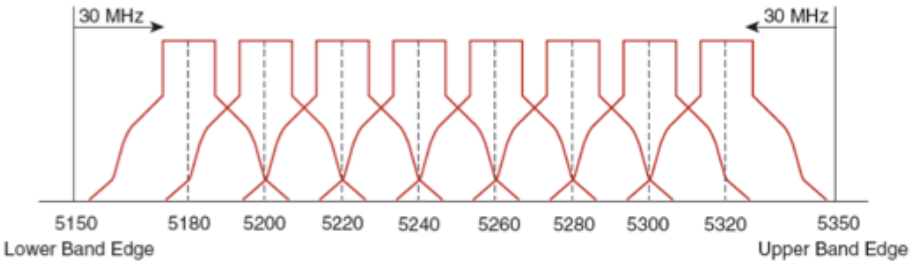
The Cisco Unified Wireless IP Phone 7921G supports Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) from 802.11h, which are required when using channels operating at 5.260 - 5.700 GHz (15 of the 23 possible channels).

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.

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

Need to ensure there is at least 20 percent overlap with adjacent channels when deploying the Cisco Unified Wireless IP Phone 7921G in the 802.11a environment, which allows for seamless roaming. For critical areas, it is recommended to increase the overlap (30% or more) to ensure that there can be at least 2 access points available with -67 dBm or better, while the Cisco Unified Wireless IP Phone 7921G also meet the access point's receiver sensitivity (required signal level for the current data rate).



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

Using Dynamic Frequency Selection (DFS) on Access Points

For Cisco Autonomous 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 Cisco 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.

If there are repeated radar events detected by the access point (just or falsely), determine if the radar signals are impacting a single channel (narrowband) or multiple channels (wideband), then potentially disable use of that channel or channels in the wireless LAN.

The presence of an AP on a non-DFS channel can help minimize voice interruptions.

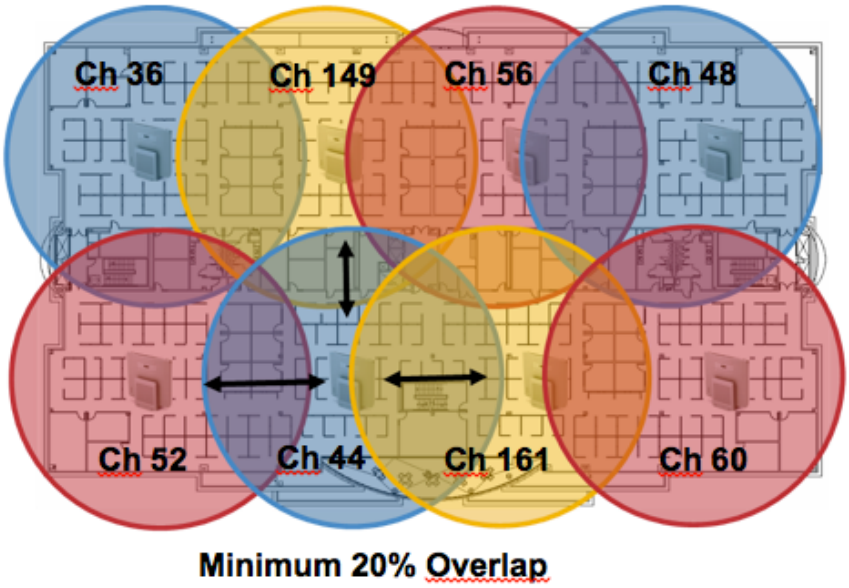
In case of radar activity, have at least one access point per area that uses a non-DFS channel (UNII-1). This ensures that a channel is available when an access point's radio is in its hold-off period while scanning for a new usable channel.

For Cisco Autonomous Access Points, enable band 1 only which allows the access point to use only a UNII-1 channel.

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

A UNII-3 channel (5.745 - 5.805 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.

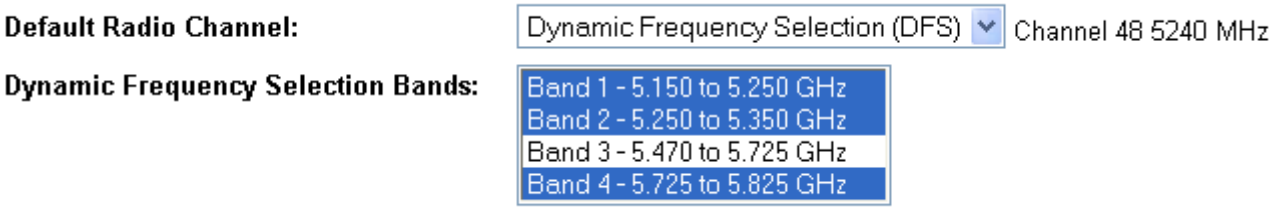


For 5 GHz, 20 channels are available in the Americas and 16 channels in Europe and Japan.

Where UNII-3 is available, it is recommended to use UNII-1, UNII-2, and UNII-3 only 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 to avoid having so many channels enabled.

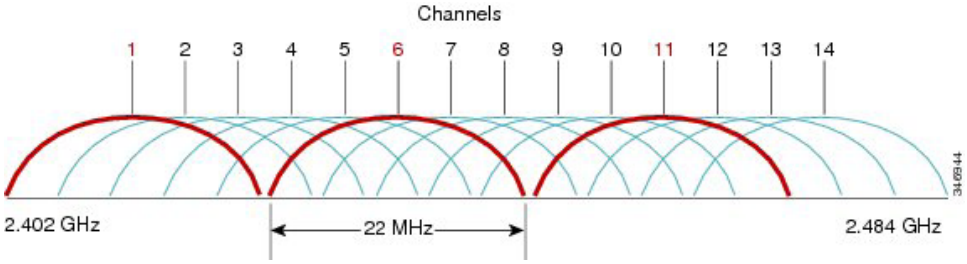
Having many 5 GHz channels enabled in the wireless LAN can delay discovery of new access points.



2.4 GHz (802.11b/g)

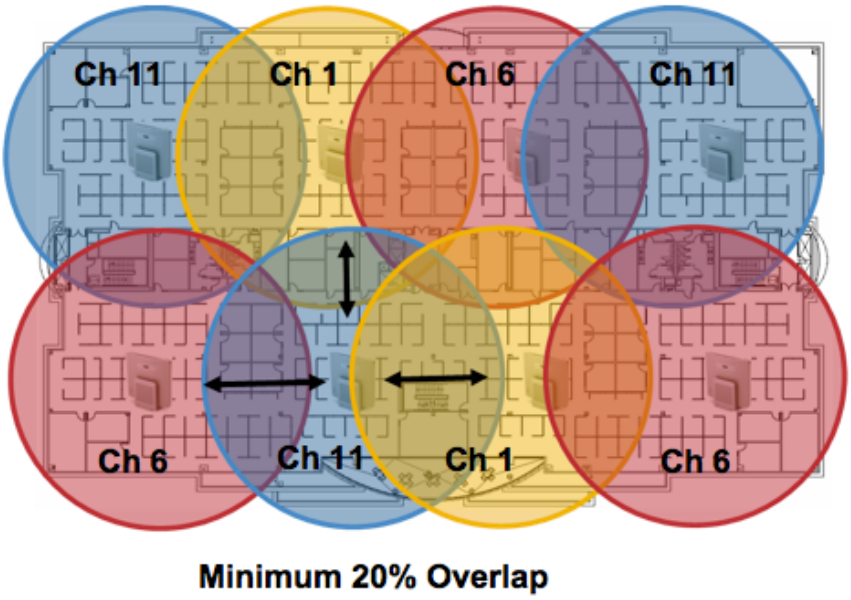
In the 2.4 GHz (802.11b/g environment, only non-overlapping channels must be utilized when deploying VoWLAN. Non-overlapping channels have 22 MHz of separation and are at least 5 channels apart.

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



Non-overlapping channels must be used and allow at least 20 percent overlap with adjacent channels when deploying the Cisco Unified Wireless IP Phone 7921G in the 802.11b/g/n environment, which allows for seamless roaming.

Using an overlapping channel set such as 1, 5, 9, 13 is not a supported configuration.



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 GHz or 5 GHz, while the Cisco Unified Wireless IP Phone 7921G also meet the access point's receiver sensitivity required signal level for the transmitted data rate.

Ensure the Packet Error Rate (PER) is no higher than 1%.

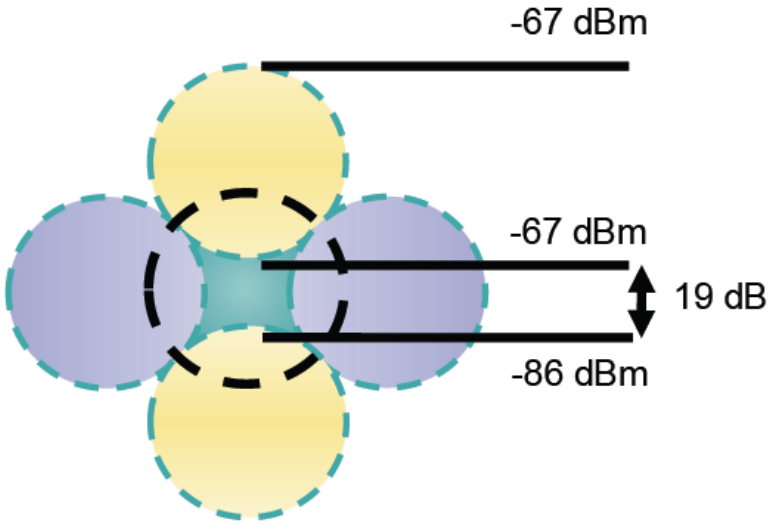
A minimum Signal to Noise Ratio (SNR) of 25 dB = -92 dBm noise level with -67 dBm signal should be maintained.

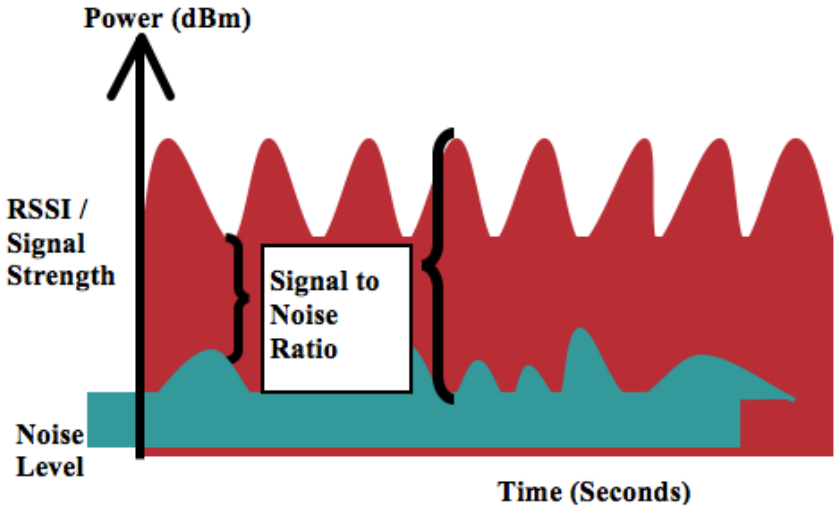
It is recommended to have at least two access points on non-overlapping channels with at least -67 dBm signal with the 25 dB SNR to provide redundancy.

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 for other applications other than voice only that can take advantage of these higher data rates.

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 mandatory / basic rate.
In some environments, 6 Mbps may need to be enabled as a mandatory / basic rate.

Due to the above requirements, a single channel plan should not be deployed.





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

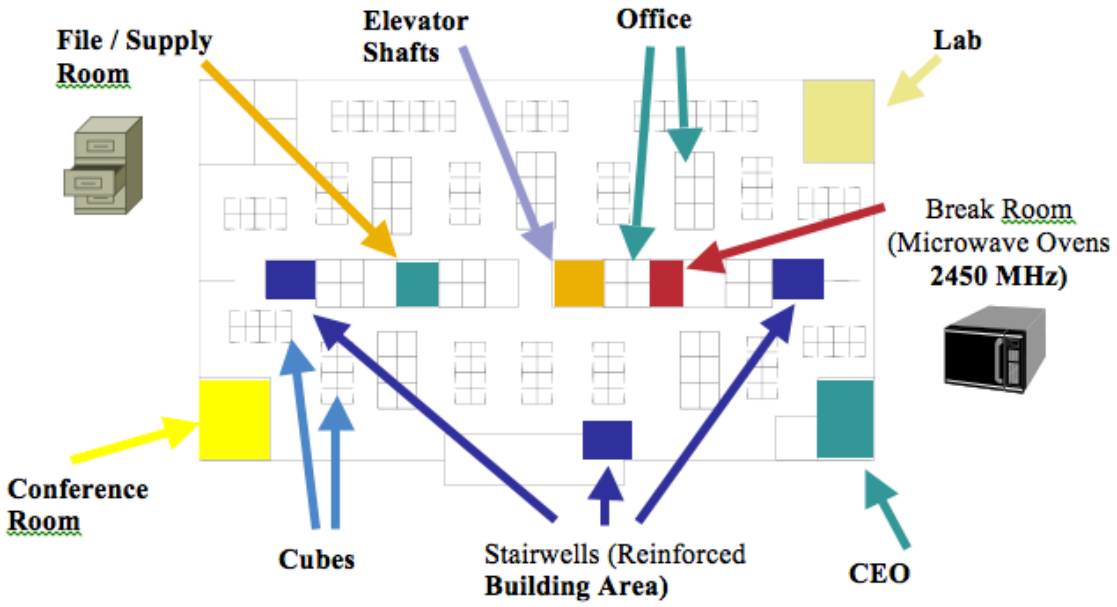
Typical wireless LAN deployments for data only applications do not provide coverage for some areas where VoWLAN service is necessary such as elevators, stairways, and outside corridors.

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.

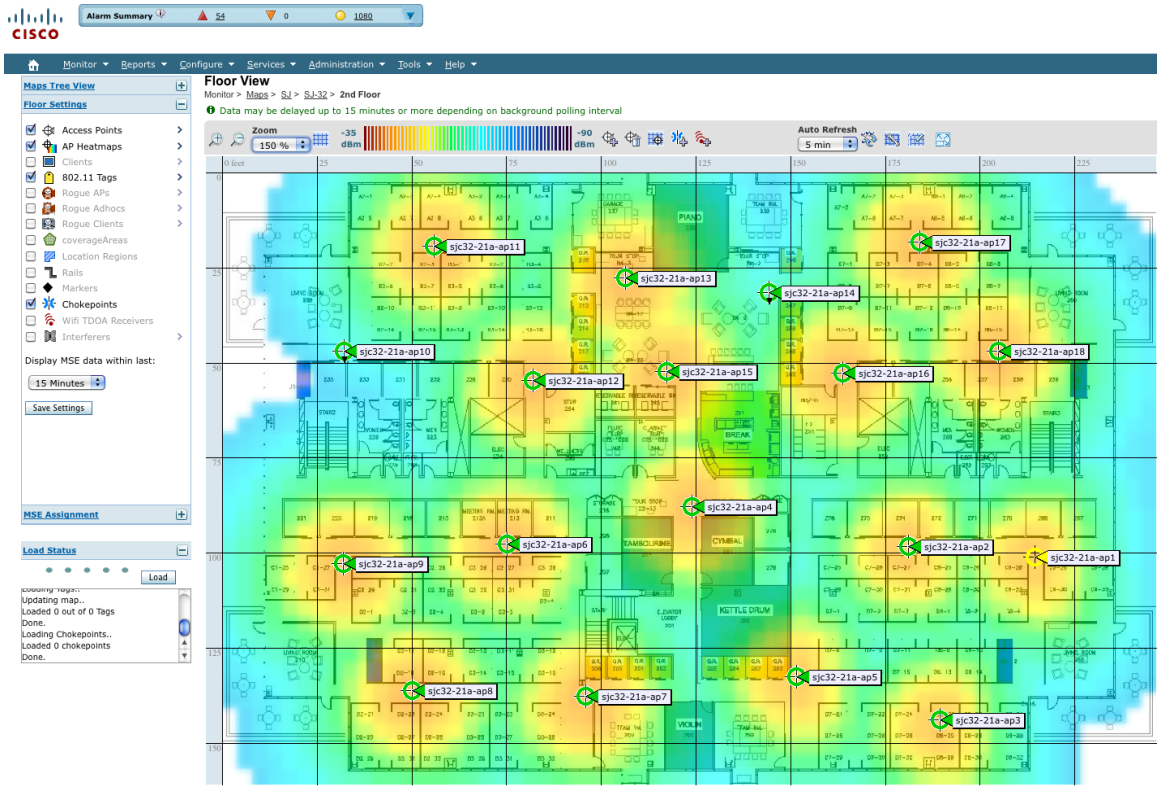
Microwave ovens operate on 2450 MHz, which is between channels 8 and 9 of 802.11b/g. Some microwaves are shielded more than others and that shielding reduces the spread of the energy. Microwave energy can impact channel 11, and some microwaves can affect the entire frequency range (channels 1 through 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 to 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 (e.g. 5.8 GHz cordless phones, which can impact UNII-3 channels).



The Cisco Unified WCS or NCS can be utilized to verify signal strength and coverage.



Configuring Data Rates

It is recommended to disable rates below 12 Mbps for 5 GHz deployments and below 12 Mbps for 2.4 GHz deployments where capacity and range are factored in for best results.

If 802.11b clients are not allowed in the wireless network, then it is strongly recommended to disable the data rates below 12 Mbps. This will eliminate the need to send CTS frames for 802.11g protection as 802.11b clients can not detect these OFDM frames.

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 mandatory / basic rate.

The recommended data rate configurations are the following:

802.11 Mode	Mandatory (Basic) Data Rates	Supported (Optional) Data Rates	Disabled Data Rates
802.11a	12 Mbps	18-24, <36-54> Mbps	6, 9, <36-54> Mbps
802.11b	11 Mbps	None	1, 2, 5.5 Mbps
802.11b/g	11 Mbps	12-24, <36-54> Mbps	1, 2, 5.5, 6, 9, <36-54> Mbps
802.11g	12 Mbps	18-24, <36-54> Mbps	1, 2, 5.5, 6, 9, 11, <36-54> Mbps

For a voice only application, data rates higher than 24 Mbps (36, 48 and 54 Mbps) can optionally be enabled or disabled, but there is no advantage from a capacity or throughput perspective and enabling these rates could potentially increase the number of retries for a data frame.

If deploying in an environment where excessive retries may be a concern, then a limited set of the data rates can be used (e.g. 12, 24, 54), where the lowest enabled rate is the mandatory / basic rate.

For rugged environments or deployments requiring maximum range, it is recommended to enable 6 Mbps as a mandatory / basic rate.

To preserve high capacity and throughput, data rates of 24 Mbps and higher only can be enabled (24-54 Mbps).

Other applications such as video may be able to benefit from having these higher data rates enabled.

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

Set only the lowest data rate enabled as the single mandatory / basic rate. Multicast packets will be sent at the highest mandatory / 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 can allow lower rates to be enabled for legacy devices, while preventing the Cisco Unified Wireless IP Phone 7921G from transmitting at rates below 12 Mbps for 802.11a and 11 Mbps for 802.11b/g as well as not above 24 Mbps if the Restricted Data Rates feature in Cisco Unified Communications Manager is enabled. Disallowing packets to be transmitted at lower rates preserves capacity. Sending voice frames at a more reliable rate (i.e. 24 Mbps) initially can potentially reduce the number of retries of a frame to ensure the packet transmission is successful on the first try.

See the Product Specific Configuration Options section for information on how to configure the Restrict 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 voice streams for both 802.11a and 802.11g at a data rate of 24 Mbps or higher. To achieve this capacity, there must be 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.

Max # of Streams	802.11 Mode	Data Rate
13	802.11a, 802.11g	6 Mbps
20	802.11a, 802.11g	12 Mbps
27	802.11a, 802.11g	24-54 Mbps

Dynamic Transmit Power Control (DTPC)

To ensure packets are exchanged successfully between the Cisco Unified Wireless IP Phone 7921G and the access point, Dynamic Transmit Power Control (DTPC) should be enabled.

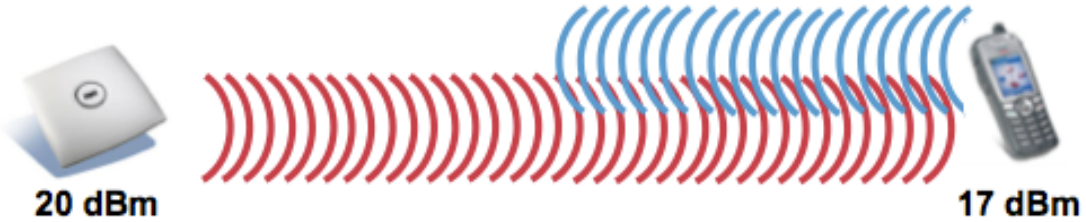
DTPC prevents one-way audio when RF traffic is heard in one direction only.

If the access point does not support DTPC, then the Cisco Unified Wireless IP Phone 7921G will use the highest available transmit power depending on the current channel and data rate.

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 on Cisco Autonomous Access Points as that will not advertise DTPC to the client.

The access point's radio transmit power should not have a transmit power greater than what the Cisco Unified Wireless IP Phone 7921G can support.



Rugged Environments

When deploying the Cisco Unified Wireless IP Phone 7921G in a rugged environment (e.g. manufacturing, warehouse, retail), additional tuning on top of the standard design recommendations may be necessary.

Below are the key items to focus on when deploying a wireless LAN in a rugged environment.

Access Point and Antenna Selection
For rugged environments, it is recommended to select an access point platform that requires external antennas (e.g. Cisco 1602e, 2602e, 3502e, 3602e, and 3702e Series Access Points). It is also important to ensure an antenna type is selected which can operate well in rugged environments.

Access Point Placement
It is crucial that line of sight to the access point's antennas is maximized by minimizing any obstructions between the Cisco Unified Wireless IP Phone 7921G and the access point. Ensure that the access point and/or antennas are not mounted behind any obstruction or on or near a metal or glass surface.
If access points with integrated antennas (e.g. Cisco 1040, 1130, 1140, 1602i, 2602i, 3502i, 3602i, and 3702i Series Access Points) are to be used in some areas, then it is recommended to mount those access points on the ceiling as they have omni-directional antennas and are not designed to be patches.

Frequency Band
As always, it is recommended to use 5 GHz. Use of 2.4 GHz, especially when 802.11b rates are enabled, may not work well.
If 2.4 GHz must be used in some areas, either due to decreased 5 GHz coverage in some areas or due to range requirements, then it is recommended to set the Cisco Unified Wireless IP Phone 7921G to Auto-a mode, which 5 GHz will be the preferred band, but can roam to 2.4 GHz as necessary.
For the 5 GHz channel set, it is recommended to use a 8 or 12 channel plan only; disable UNII-2 extended channels if possible.

Data Rates
The standard recommended data rate set of 12-54 Mbps may not work well if multipath is present at an elevated level. Therefore, it is recommended to enable lower data rates (e.g. 6 Mbps) to operate better in such an environment.
If 5 GHz is used for VoWLAN only, then it is also recommended to disable data rates above 24 Mbps (i.e. 36, 48, 54 Mbps) to increase first transmission success (e.g. 6 as mandatory, 12 and 24 as supported). If 5 GHz is also used for data, video or other applications, then is suggested to keep the higher data rates enabled (e.g. 6 as mandatory, 9, 12-54 as supported).

Transmit Power
Due to the potential of elevated multipath in rugged environments, the transmit power of the access point and Cisco Unified Wireless IP Phone 7921G should also be restricted. This is more important if planning to deploy 2.4 GHz in a rugged environment.

If using auto transmit power, the access point transmit power can be configured to use a specified range (maximum and minimum power levels) to prevent the access point from transmitting too hot as well as too weak (e.g. 5 GHz maximum of 16 dBm and minimum of 11 dBm).
The Cisco Unified Wireless IP Phone 7921G will utilize the access point's current transmit power setting to determine what transmit power it uses for transmitted frames when DTPC is enabled in the access point's configuration.

Fast Roaming
It is recommended to utilize CCKM for fast roaming. Enabling CCKM also reduces the number of frames in the handshake when roaming to only two frames. Reducing the number of frames during a roam, increases the chances of roam success. When using 802.1x authentication, it is important to use the recommended EAPOL key settings. See the **WLAN Controller Advanced EAP Settings** section in **Configuring the Cisco Unified Wireless LAN Controller and Access Points** for more information.

Quality of Service (QoS)
Need to ensure that DSCP values are preserved throughout the wired network, so that Cisco Unified Wireless LAN Controller and access points can set the WMM UP tag for voice and call control frames correctly.

Beamforming
If using Cisco 802.11n access points, then Beamforming (ClientLink) should be enabled, which can help with client reception.
See the **Beamforming (ClientLink)** section in **Configuring the Cisco Unified Wireless LAN Controller and Access Points** for more information.

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 affect the decoding capability of the receiver, as the signal quality is poor.

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

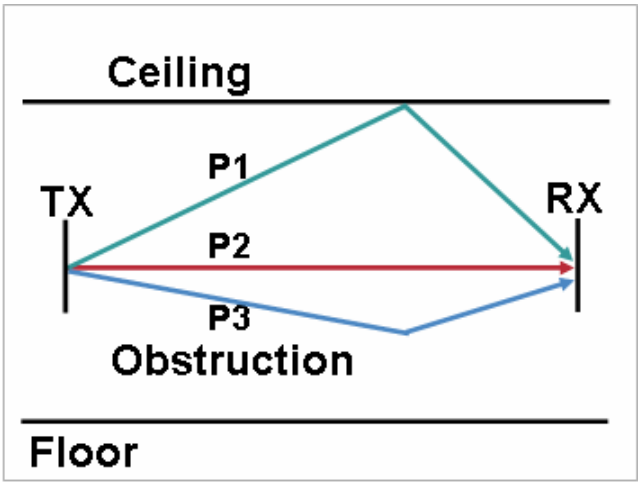
Below is a list of multipath effects:

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 (e.g. 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 Prime Network Control System (NCS) for Unified Wireless LAN Management
  http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps11682/ps11686/ps11688/data_sheet_c78-650051.html
- Cisco Wireless Control System (WCS) for Unified Wireless LAN Management
  http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd802570d0.html
- Cisco Wireless LAN Solution Engine (WLSE) for Cisco Autonomous Wireless LAN Management
  http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6380/ps6563/ps3915/ps6839/product_data_sheet0900aecd80410b92.html
- Cisco Spectrum Expert
  http://www.cisco.com/en/US/prod/collateral/wireless/ps9391/ps9393/product_data_sheet0900aecd807033c3.html
- Cisco Unified Operations Manager
  http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6491/ps6705/ps6535/data_sheet_c78-636705.html
- AirMagnet (Survey, WiFi Analyzer, VoFi Analyzer, Spectrum Analyzer)
  http://www.airmagnet.com
- Cisco Unified Wireless IP Phone 7921G
  http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/product_data_sheet0900aecd805e315d.html

Cisco 7921G Neighbor List

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

To access the neighbor list menu on the Cisco Unified Wireless IP Phone 7921G, select **Settings > Status > Neighbor List.**

The connected access point will be highlighted in red.

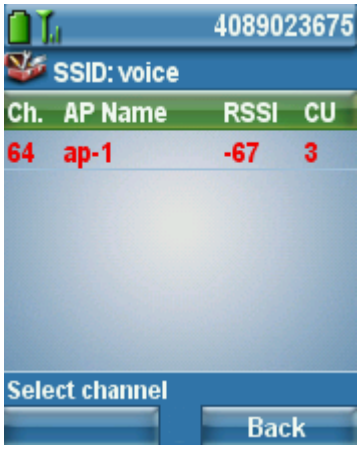
By default with the **Auto** scan mode enabled, the Cisco Unified Wireless IP Phone 7921G in idle (not on call) only scans when the current signal lowers to the scan threshold, so only a single access point may be visible in the list.

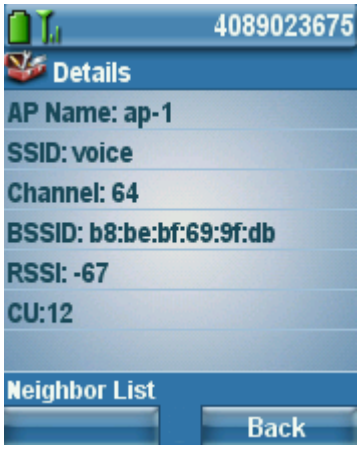
To see all access points in the neighbor list menu with **Auto** scan mode, place a call from the Cisco Unified Wireless IP Phone 7921G, where scanning occurs constantly while the phone call is active in **Auto** scan mode.

With **Continuous** scan mode, the Cisco Unified Wireless IP Phone 7921G will always be scanning regardless of call state (idle or on call) or current access point signal level (RSSI).

With the 1.4(2) release, neighbors will be listed in order from the strongest signal to the weakest signal when using Auto-RSSI, 802.11a or 802.11b/g mode. If using a Auto-a or Auto-b/g mode, then the neighbors will be displayed in the following order.

- Preferred Band Neighbors with >= -67 dBm RSSI
- Less Preferred Band Neighbors with >= -67 dBm RSSI
- Preferred Band Neighbors with < -67 dBm RSSI
- Less Preferred Band Neighbors with < -67 dBm RSSI





Cisco 7921G Site Survey

The Cisco Unified Wireless IP Phone 7921G 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 and HTML report after exiting the application.

To access the Site Survey application, navigate to **Settings > Status > Site Survey**.

To view the HTML report, select **System > Site Survey** from the Cisco Unified Wireless IP Phone 7921G webpage.

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

The neighbor table shows access points (along the column) that 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.

CP7921G Site Survey Report SSID:baker

Neighbor Table	sjc32-11a-ap9	sjc32-11a-ap11	sjc32-11a-ap10	sjc32-11a-ap12	sjc32-11a-ap1
sjc32-11a-ap9	85% -46/-45	100% -57/-57	*	*	*

AP:	sjc32-11a-ap9
MAC:	C4:7D:4F:53:2C:DF
Observation Count:	7
Channel - Frequency:	157 - 5785000hz
Country:	US
Beacon Interval:	102
DTIM Period:	2
RSSI Range [Lo Hi]:	[-46 -45]
BSS Lost Count:	0
Channel Utilization:	14
Station Count:	15
Available Admission Capacity:	22365
Basic Rates:	12
Optional Rates:	18 24 36 48 54
Multicast Cipher:	CCMP
Unicast Ciphers:	WPA2_CCMP
AKM:	WPA2_1X WPA2_CCKM
Proxy ARP supported:	Yes
WMM Supported:	Yes
CCX Version Number:	5
CCX Power Maximum in dBm:	14
U-APSD Supported:	Yes

Best Effort AC(0)			
Admission Control Required:	No		
AIFSN	**ECWMin**	**ECWMax**	**TXOpLimit**
12	6	10	0

Background AC(1)			
Admission Control Required:	No		
AIFSN	**ECWMin**	**ECWMax**	**TXOpLimit**
12	8	10	0

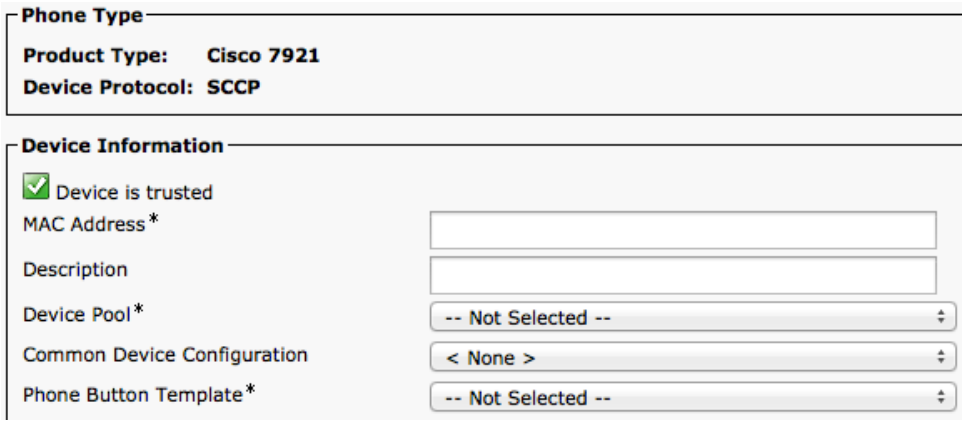
Video AC(2)			
Admission Control Required:	No		
AIFSN	**ECWMin**	**ECWMax**	**TXOpLimit**
5	3	5	0

Voice AC(3)			
Admission Control Required:	Yes		
AIFSN	**ECWMin**	**ECWMax**	**TXOpLimit**
2	2	4	0

Channels	36	40	44	48	52	56	60	64	100	104	108	112	116	132	136	140	149	153	157	161	165
Power	17	17	17	17	24	24	24	24	24	24	24	24	24	24	24	24	30	30	30	30	30

Configuring Cisco Unified Communications Manager

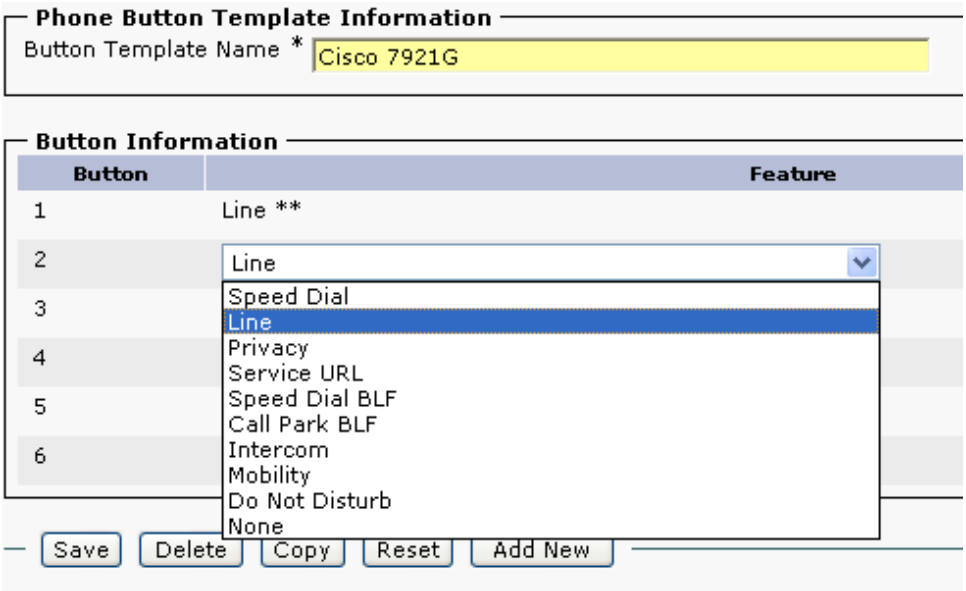
Cisco Unified Communications Manager offers many different product, call and security features.



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 device or group level.



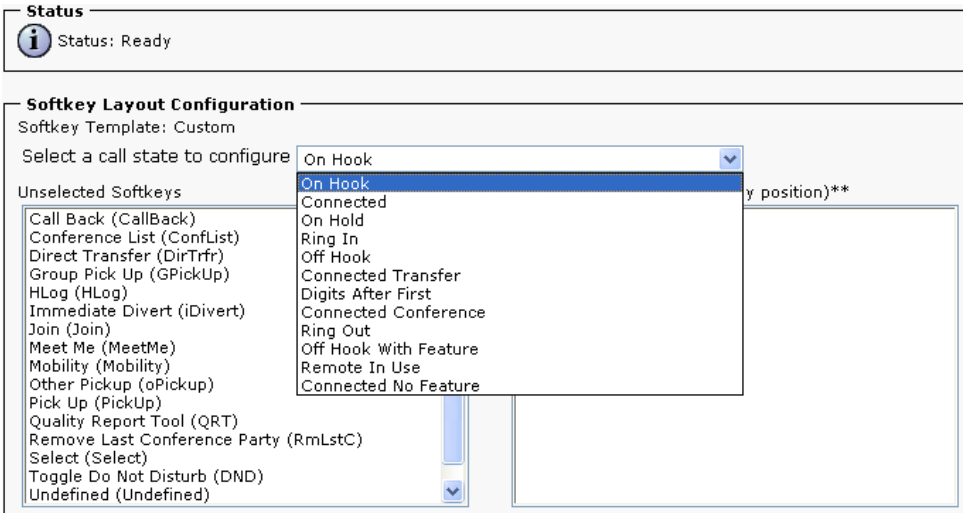
Softkey Templates

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.

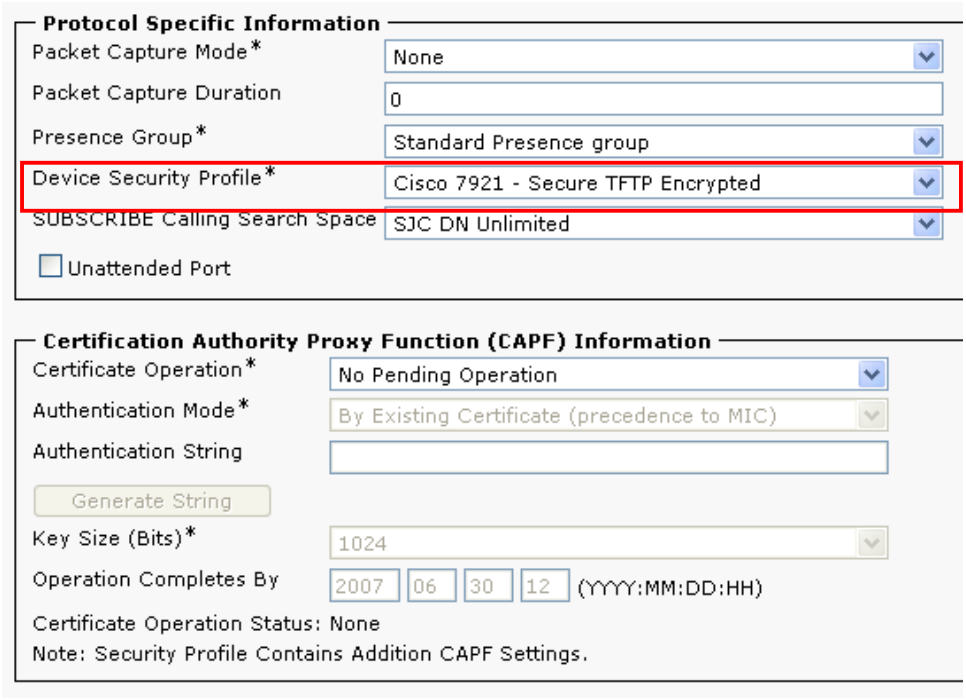


Security Profiles

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

The Certificate Authority Proxy Function (CAPF) must be operational in order to utilize a Locally Signed Certificate (LSC) with a security profile.

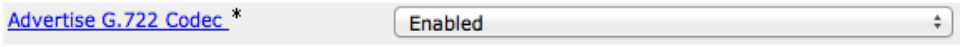
The Cisco Unified Wireless IP Phone 7921G has a Manufactured Installed Certificate (MIC), which can be utilized with a security profile as well.



G.722 Advertisement

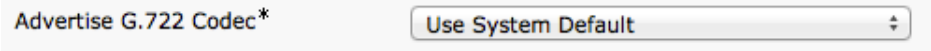
Cisco Unified Communications Manager versions 5.0 and later support the ability to configure whether G.722 is to be a supported codec system wide or not.

If using a recent version of Cisco Unified Communication Manager, G.722 can be disabled globally within **Enterprise Parameters** of Cisco Unified Communications Manager.



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.

If using a version of Cisco Unified Communications Manager prior to 5.0 and want to disable G.722 capabilities, then the latest device package will need to be applied to the Cisco Unified Communications Manager to enable this product specific configuration option where **Advertise G.722 Codec** can be disabled for each Cisco Unified Wireless IP Phone 7921G as necessary.



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

Note: The Cisco Unified Wireless IP Phone 7921G does not support the iSAC codec.

Common Settings

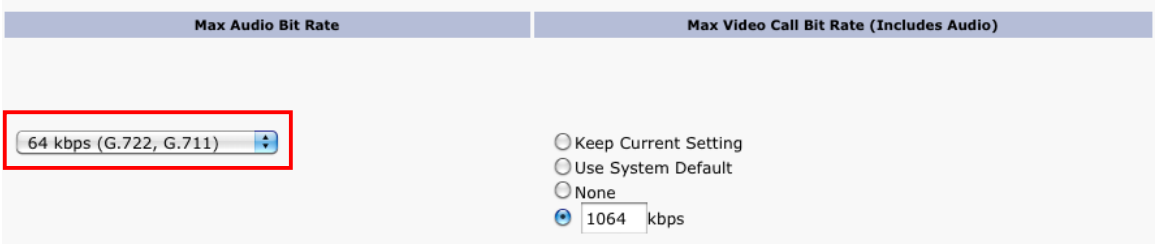
Some settings can be configured on an enterprise phone, common phone profile or individual phone level.

Override common settings can be enabled at either configuration level.

Audio Bit Rates

The audio bit rate can be configured by creating or editing existing Regions in the Cisco Unified Communications Manager.

It is recommended to select G.722 or G.711 for the audio codec.



Use the following information to configure the audio bit rate to be used for voice calls.

Audio Codec	Audio Bit Rate
G.722 / G.711	64 Kbps
iLBC	16 Kbps
G.729	8 Kbps

Product Specific Configuration Options

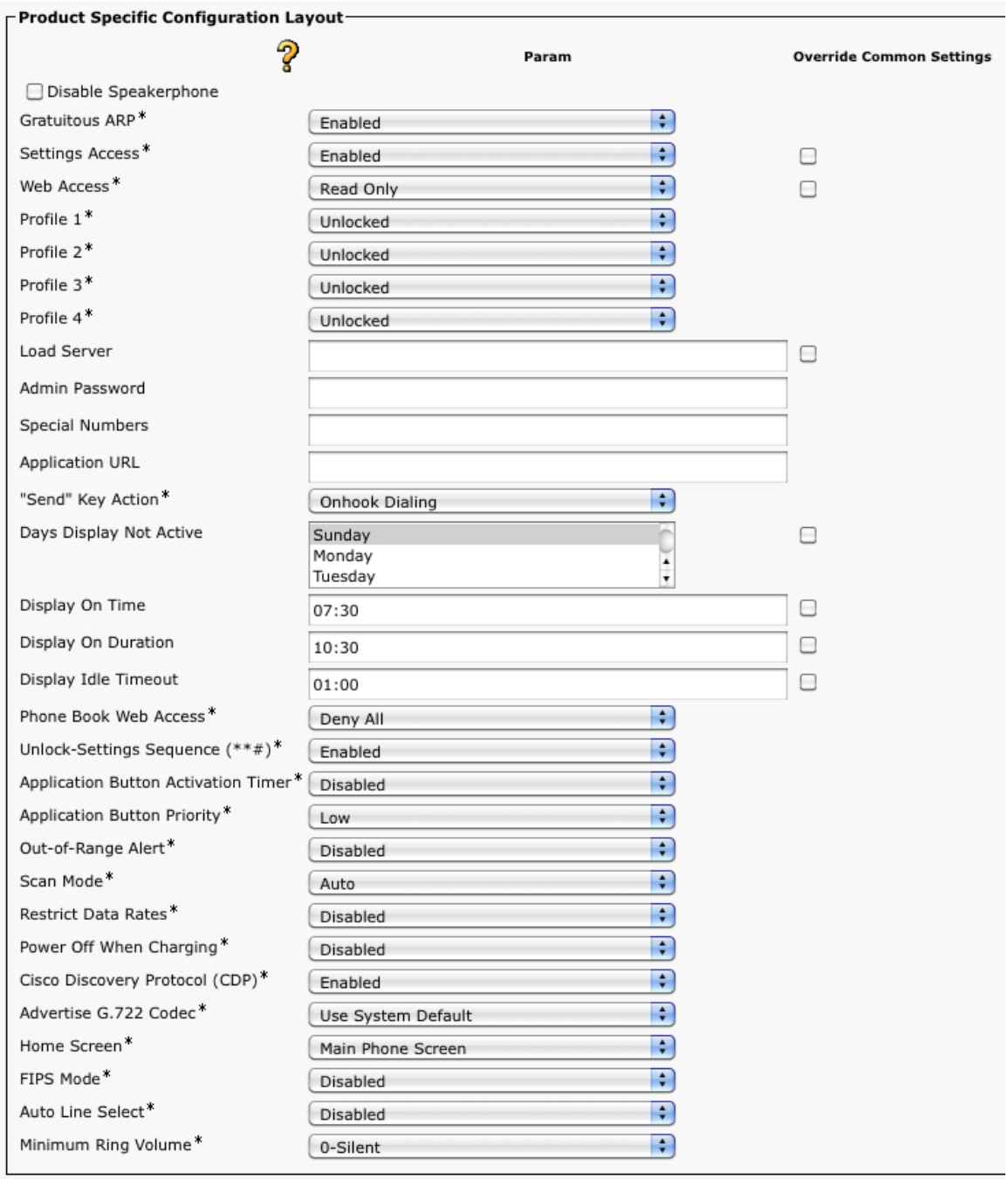
In Cisco Unified Communications Manager Administration, the following Cisco Unified Wireless IP Phone 7921G configuration options are available.

For an description of these options, click the **?** on the configuration page.

Product specific configuration options can be configured in bulk via the Bulk Admin Tool if using Cisco Unified Communications Manager 5.0 and later. If using a prior version, then must be configured separately.

As of the 1.4(1) release Multiple Level Vendor Configuration is allowed to override common settings.

Some of the product specific configuration options can be configured on an enterprise phone, common phone profile or individual phone configuration level.



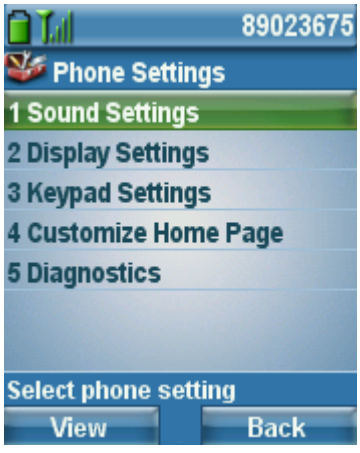
Field Name	**Description**
Disable Speakerphone	Speakerphone capabilities can optionally be disabled.
Gratuitous ARP	Determines whether the phone will learn MAC addresses from Gratuitous ARP responses or not.
Settings Access	Settings Access can be used to limit user access to certain menus (e.g. Network Profiles).
Web Access	This parameter indicates whether the phone will accept connections from a web browser or another HTTP client. 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 (e.g. 911).
Application URL	The application URL can be configured, which will convert the application button to a service URL button or as a speed dial. The application URL can be configured to link to a Push To Talk server for quick access. (e.g. PTT server = http://x.x.x.x:8085/PushToTalk/displayPhoneGroupsMenu.do?sep=#DEVICENAME#) To configure the application button as a speed dial, enter in the format as **Dial:X** (e.g. Dial:23675).
"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.
Days Display Not Active	This field allows the user to specify the days that the backlight is to remain off by default. To turn off the backlight for multiple days, hold down the control key while selecting the days. Saturday and Sunday is the default setting.
Display On Time	This field indicates the time of day the display is to automatically turn itself on if it is an active day. The value should be in a 24 hour format. The default setting is 07:30.
Display On Duration	This field indicates the amount of time the display is to be active for after the display on time. The default setting is 10:30 (hours:minutes), so the display would be turned off at 18:00 (6 pm).
Display Idle Timeout	This field indicates how long to wait before the display is turned off after the last user activity. This timer gets reset after each interaction. The default setting is 01:00 (hours:minutes).
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

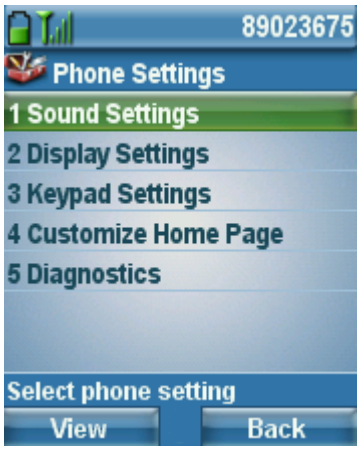
	the home screen. Medium priority will allow the application button to function when in any menu or XML screen and high priority will allow the application button to function when in any state including keypad lock.
Out of Range Alert	An out of range alert can be configured to beep once or periodically 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.
Restrict Data Rates	This parameter enables or disables the restriction of the upstream and downstream PHY rates according to CCX V4 Traffic Stream Rate Set IE (S54.2.6).
Power Off When Charging	Power off when charging feature will power off the phone when placed on AC power.
Cisco Discover Protocol (CDP)	Enables or disables CDP.
Advertise G.722 Codec	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.
FIPS Mode	The Federal Information Process Standards (FIPS) mode can optionally be enabled.
Auto Line Select	When enabled, indicates that the phone will shift the call focus to incoming calls on all lines. When disabled, the phone will only shift the focus to incoming calls on the currently used line.
Minimum Ring Volume	This parameter controls the minimum ring volume on the phone. This value is set by the administrator, and can not be changed by an end user. The end user can increase the ring volume, but may not decrease the ring volume below the level defined. The minimum ring volume range is from 0 to 7, with 0 (silent) being the default value.

Below shows the available menus when **Settings Access** is configured for either Enabled, Restricted, or Disabled.

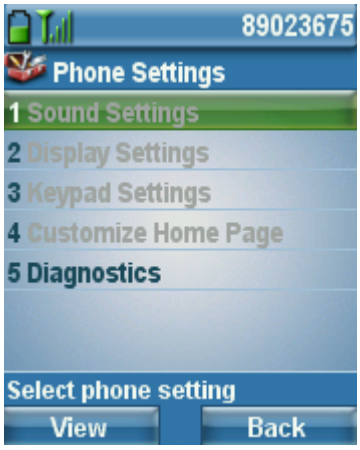
Settings Access = Enabled



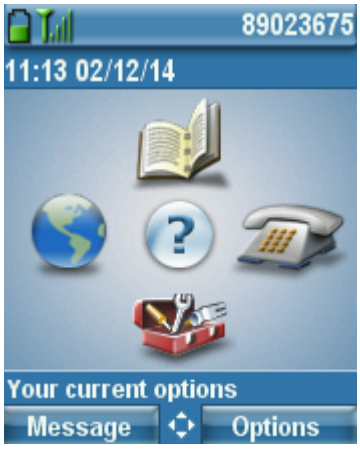
Settings Access = Restricted

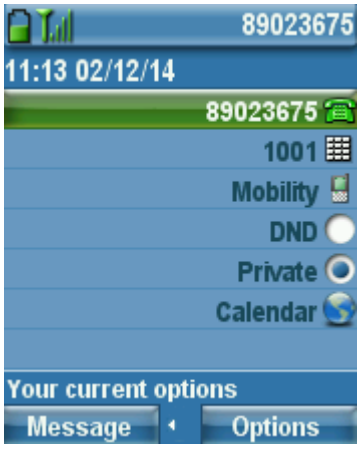


Settings Access = Disabled



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, 7.1, 8.0, 8.5, 8.6 or later and web access is set to **Full**, then it is recommended to enable TFTP encryption via the device security profile.

With the 1.3(3) and 1.3(4) releases, if settings access is set to **Disabled**, then the current ring volume will be locked in and will not be configurable.

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>

Field Name	Module	Value
Disable Speakerphone	disableSpeaker	false = Enabled; true = Disabled
Gratuitous ARP	garp	0 = Enabled; 1 = Disabled
Settings Access	settingsAccess	0 = Disabled; 1 = Enabled; 2 = Restricted
Web Access	webAccess	0 = Full; 1 = Disabled; 2 = ReadOnly
Locked Profiles	WlanProfile<1-4>	0 = Unlocked; 1 = Locked, 2 = Restricted
Load Server	loadServer	x.x.x.x
Admin Password	adminPassword	(e.g. Cisco)
Special Numbers	specialNumbers	(e.g. 411,911)
Application URL	PushToTalkURL	http://x.x.x.x
"Send" Key Action	sendKeyAction	0 = Onhook Dialing; 1 = Offhook Dialing
Days Display Not Active	daysDisplayNotActive	<1-7> = <Sunday, Monday Tuesday, Wednesday, Thursday, Friday, Saturday>
Display On Time	displayOnTime	00:00 - 23:59
Display On Duration	displayOnDuration	00:00 - 23:59
Display Idle Timeout	displayIdleTimeout	00:00 - 23:59
Phone Book Web Access	phoneBookWebAccess	0 = Deny All; 1 = Allow Admin
Unlock-Settings Sequence	unlockSettingsSequence	0 = Disabled; 1 = Enabled
Application Button Activation Timer	appButtonTimer	0 = Disabled; <1-5> = <1-5> seconds
Application Button Priority	appButtonPriority	0 = Low; 1 = Medium; 2 = High
Out of Range Alert	outOfRangeAlert	0 = Disabled; 1 = Beep Once; <2-4> = Beep every <10,30,60> seconds
Scan Mode	scanningMode	0 = Auto; 1 = Single AP; 2 = Continuous
Restrict Data Rates	restrictDataRates	0 = Disabled; 1 = Enabled
Power Off When Charging	powerOffWhenCharging	0 = Disabled; 1 = Enabled
Cisco Discover Protocol	cdpEnable	0 = Disabled; 1 = Enabled

(CDP)		
Advertise G.722 Codec	g722CodecSupport	0 = Use System Default; 1 = Disabled; 2 = Enabled
Home Screen	homeScreen	0 = Main Phone Screen; 1 = Line View
FIPS Mode	fipsMode	0 = Disabled; 1 = Enabled
Auto Line Select	autoSelectLineEnable	0 = Disabled; 1 = Enabled
Minimum Ring Volume	minimumRingVolume	0 = Silent; <1-7> = Different Volume Levels
Application Button	thumbButton1	PTTH<1-6>

With Cisco Unified Communications Manager Express, the **thumbButton1** command can tie the application button to a specific line.

For example, if line 2 is an intercom line tied to a multicast paging group, then this can be configured to achieve Push To Talk.

Enable individual phone configuration files with the following commands.

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

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_release_notes_list.html

Configuring the Cisco Unified Wireless LAN Controller and Access Points

When configuring the Cisco Unified Wireless LAN Controller and Access Points, use the following guidelines:

- Ensure **CCKM** is **Enabled** if utilizing 802.1x authentication
- Set **Quality of Service (QoS)** to **Platinum**
- Set the **WMM Policy** to **Required**
- Ensure **Session Timeout** is enabled and configured correctly
- Ensure **Aironet IE** is **Enabled**
- Set **DTPC Support** to **Enabled**
- Disable **P2P (Peer to Peer) Blocking Action** / **Public Secure Packet Forwarding (PSPF)**
- Ensure **Client Exclusion** is configured correctly
- Disable **DHCP Address Assignment Required**
- Set **MFP Client Protection** to **Optional** or **Disabled**
- Set the **DTIM Period** to **2**

- Set **Client Load Balancing** to **Disabled**
- Set **Client Band Select** to **Disabled**
- Set **IGMP Snooping** to **Enabled**
- Enable **Symmetric Mobile Tunneling Mode** if Layer 3 mobility is utilized
- Enable **Short Preamble** if using 2.4 GHz
- Enable **ClientLink** if utilizing Cisco 802.11n Access Points
- Configure the **Data Rates** as necessary
- Enable **CCX Location Measurement**
- Configure **Auto RF** as necessary
- Set **Admission Control Mandatory** to **Enabled** for **Voice**
- Set **Load Based CAC** to **Enabled** for **Voice**
- Enable **Traffic Stream Metrics** for **Voice**
- Set **Admission Control Mandatory** to **Disabled** for **Video**
- Set **EDCA Profile** to **Voice Optimized** or **Voice and Video Optimized**
- Set **Enable Low Latency MAC** to **Disabled**
- Ensure that **Power Constraint** is **Disabled**
- Enable **Channel Announcement** and **Channel Quiet Mode**
- Enable **CleanAir** if utilizing Cisco Access Points with CleanAir technology
- Configure **Multicast Direct Feature** as necessary
- Set the **802.1p tag** to **5** for the **Platinum** QoS profile

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

When using 802.1x authentication, it is recommended to implement CCKM to offer fast secure roaming.

SSID / WLAN Settings

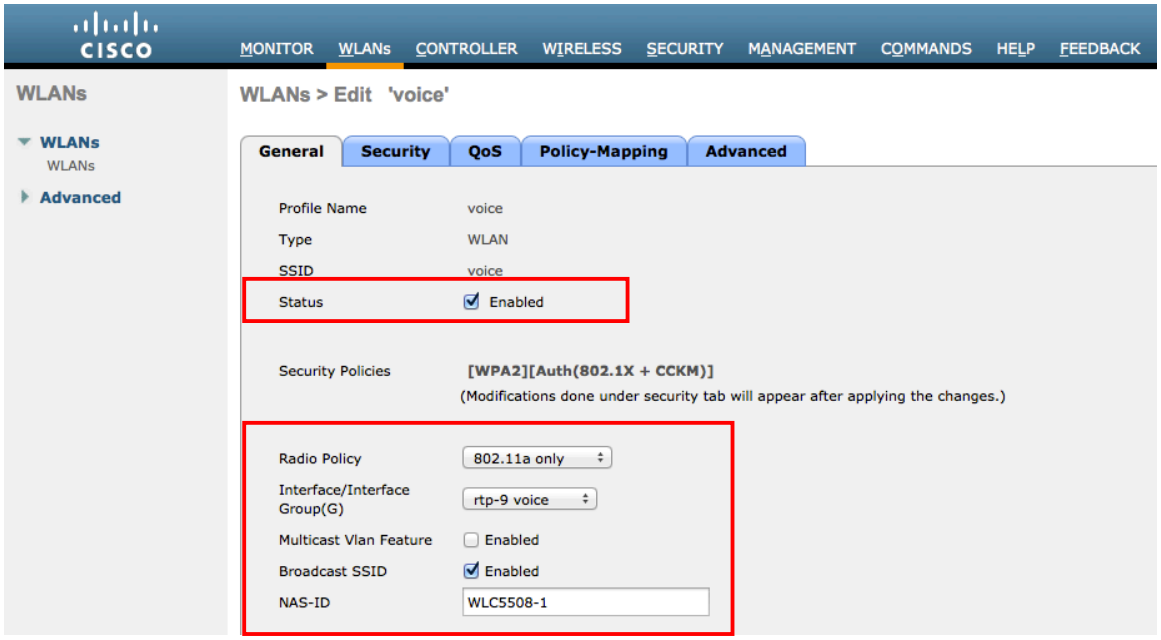
It is recommended to have a separate SSID for the Cisco Unified Wireless IP Phone 7921G.

However, if there is an existing SSID configured to support voice capable Cisco Wireless LAN endpoints already, then that WLAN can be utilized instead.

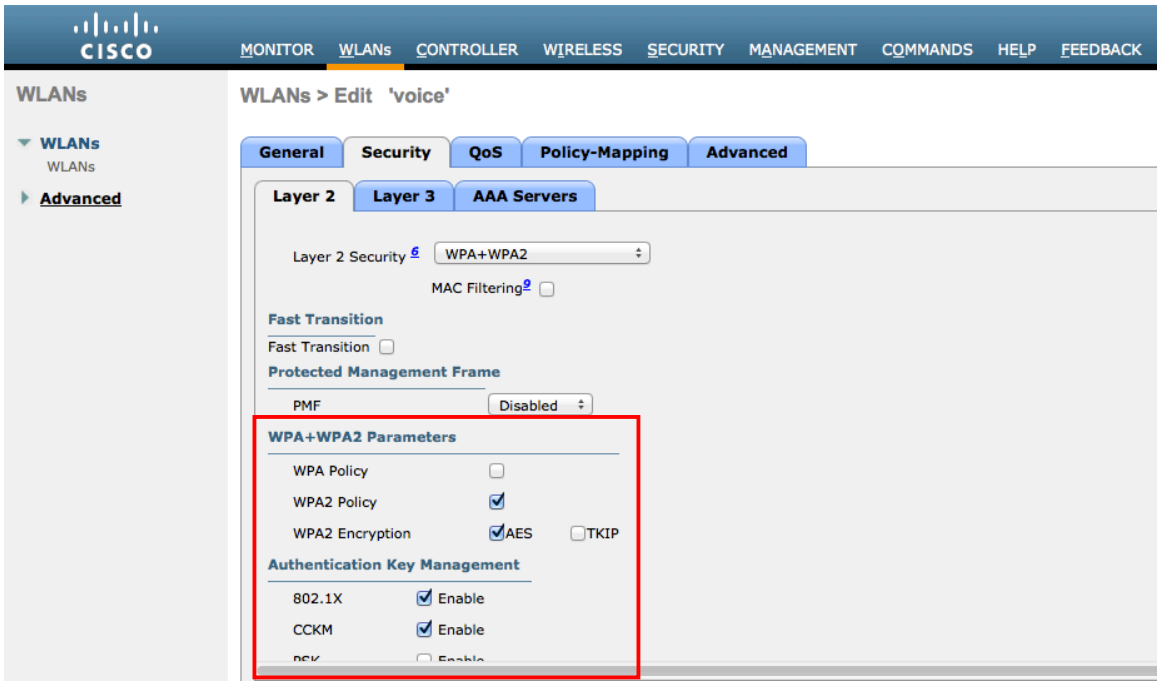
The SSID to be used by the Cisco Unified Wireless IP Phone 7921G can be configured to only apply to a certain 802.11 radio type.

It is recommended to have the Cisco Unified Wireless IP Phone 7921G operate on the 5 GHz band due to have many channels available and not as many interferers as the 2.4 GHz band has.

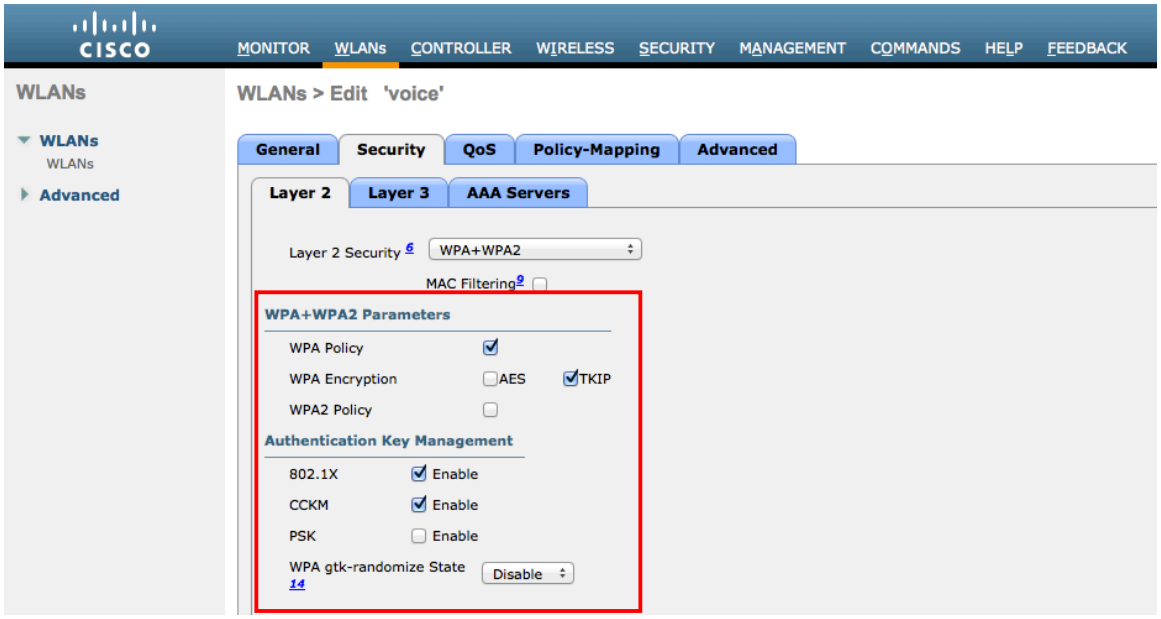
Ensure that the selected SSID is not utilized by any other wireless LANs as that could lead to failures when powering on or during roaming; especially if a different security type is utilized.



In order to utilize CCKM, enable WPA2 policy with AES encryption and 802.1x + CCKM for authenticated key management type when the Cisco Unified Wireless IP Phone 7921G is running firmware version 1.3(4) or later in order to enable fast secure roaming.



If the Cisco Unified Wireless IP Phone 7921G is running firmware version 1.3(3) or earlier, then enable WPA policy with TKIP encryption and 802.1x + CCKM for authenticated key management type in order to enable fast secure roaming.

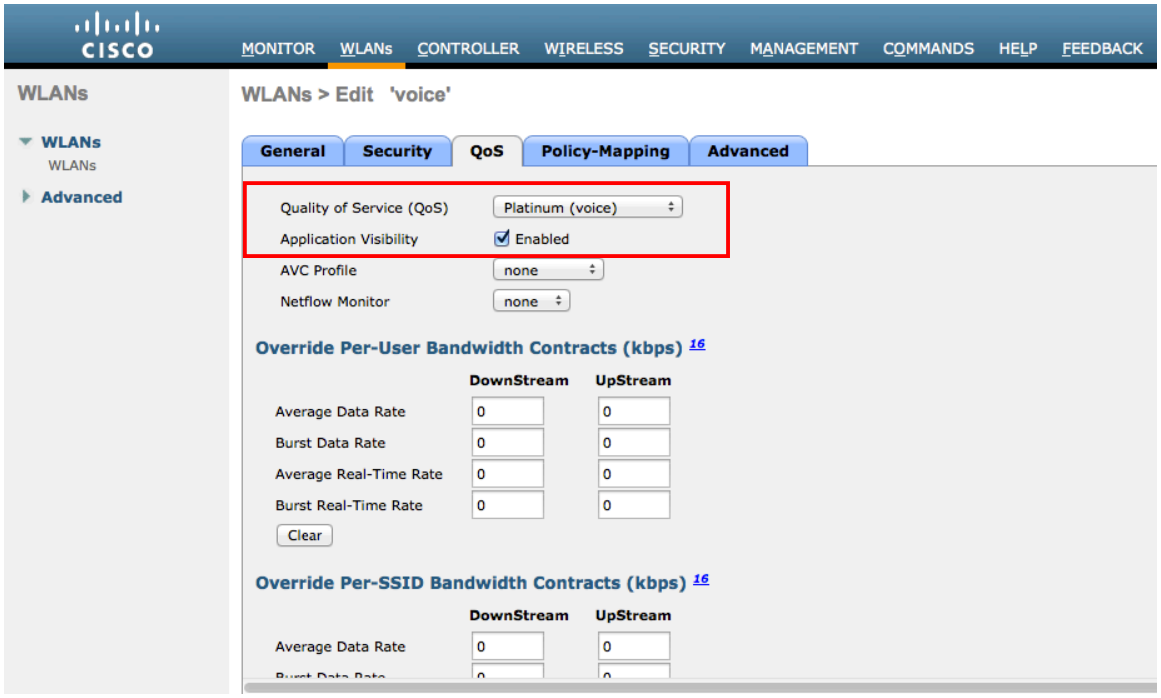


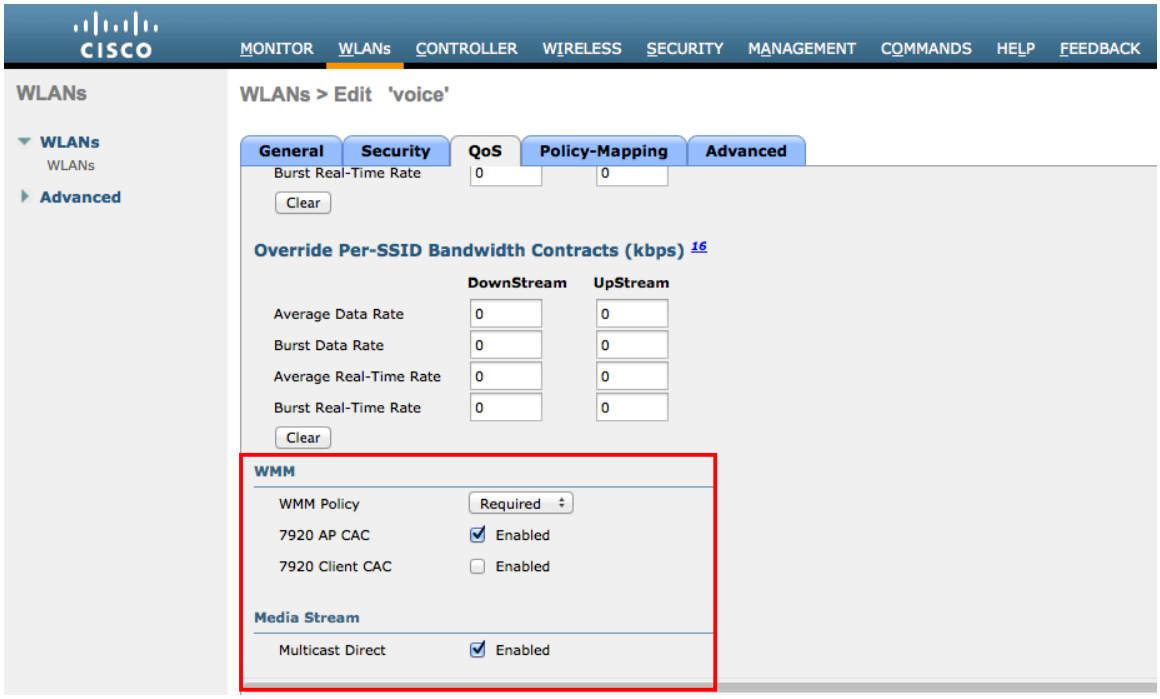
The WMM policy should be set to **Required** only if the Cisco Unified Wireless IP Phone 7921G or other WMM enabled phones will be using this SSID.

If there are non-WMM clients existing in the WLAN, it is recommended to put those clients on another SSID / WLAN.

If non-other WMM clients must utilize the same SSID as the Cisco Unified Wireless IP Phone 7921G, then ensure the WMM policy is set to **Allowed.**

Enable **7920 AP CAC** to advertise Qos Basic Service Set (QBSS) to the client.





Configure **Enable Session Timeout** as necessary per your requirements. It is recommended to either disable the session timeout or extend the timeout (e.g. 24 hours / 86400 seconds) to avoid possible interruptions during audio calls. If disabled it will avoid any potential interruptions altogether, but enabling session timeout can help to re-validate client credentials periodically to ensure that the client is using valid credentials.

Enable Aironet Extensions (**Aironet IE).**

Peer to Peer (P2P) Blocking Action should be disabled.

Configure **Client Exclusion** as necessary.

Off Channel Scanning Defer can be tuned to defer scanning for certain queues as well as the scan defer time.

The **Maximum Allowed Clients Per AP Radio** can be configured as necessary.

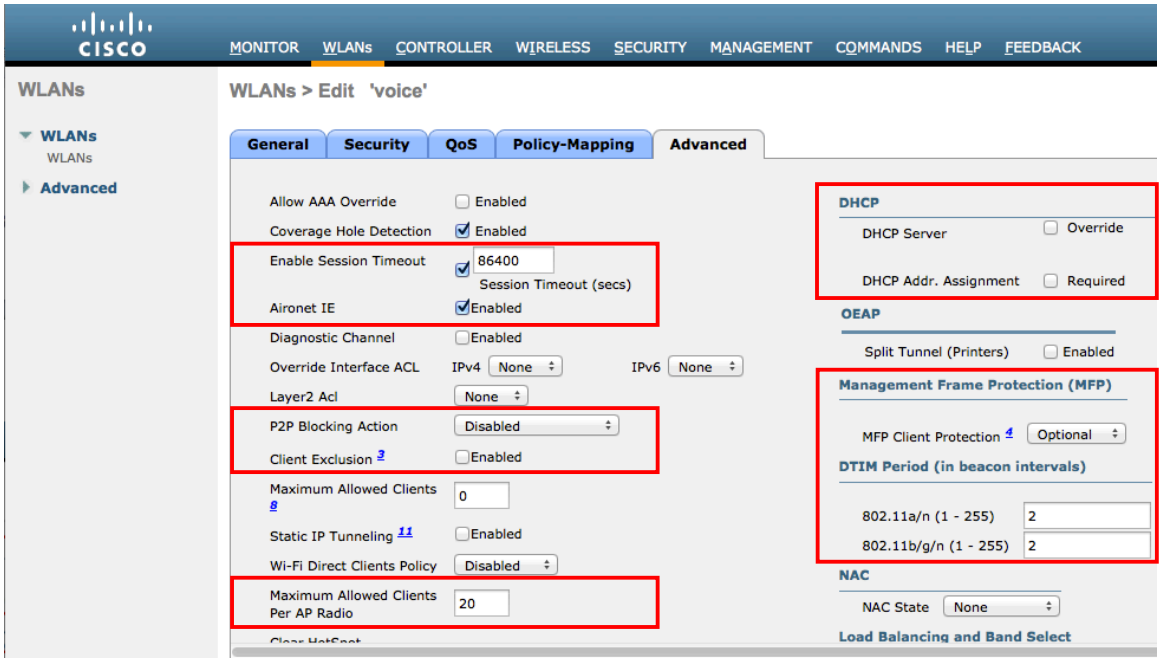
DHCP Address Assignment Required should be disabled.

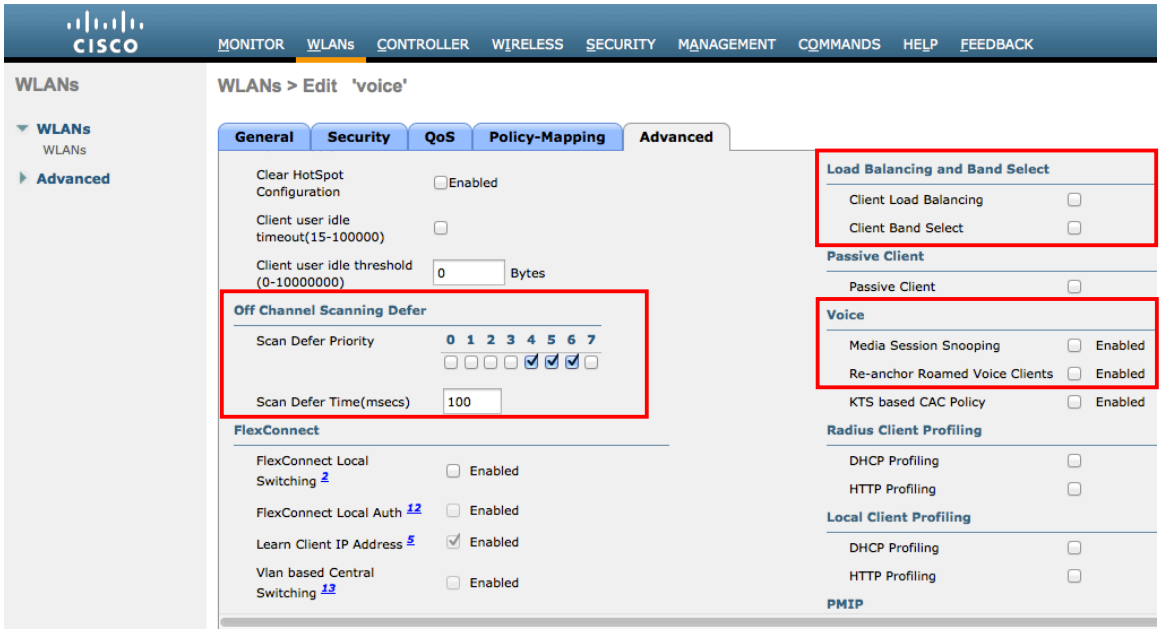
Management Frame Protection should be set to **Optional** or **Disabled.**

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

Ensure **Client Load Balancing** and **Client Band Select** are disabled.

It is recommended to set **Re-anchor Roamed Voice Clients** to disabled as this can cause brief interruptions with wireless LAN connectivity when a call is terminated after performing an inter-controller roaming.





For the Cisco Autonomous Access Point, ensure that the SSID is configured for open + eap as and network-eap when using 802.1x authentication.

As of the 1.3(2) release, the Cisco Unified Wireless IP Phone 7921G utilizes open + eap when doing 802.1x authentication, but utilized network-eap in previous releases.

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

If the Cisco Autonomous Access Point is registered to a WDS (Wireless Domain Services) server, ensure both leap and eap types of authentication are enabled in the WDS configuration.

wlccp authentication-server infrastructure method_Infrastructure

wlccp authentication-server client mac method_Clients

wlccp authentication-server client **eap** method_Clients

wlccp authentication-server client **leap** method_Clients

wlccp wds priority 255 interface BVI1

Controller Settings

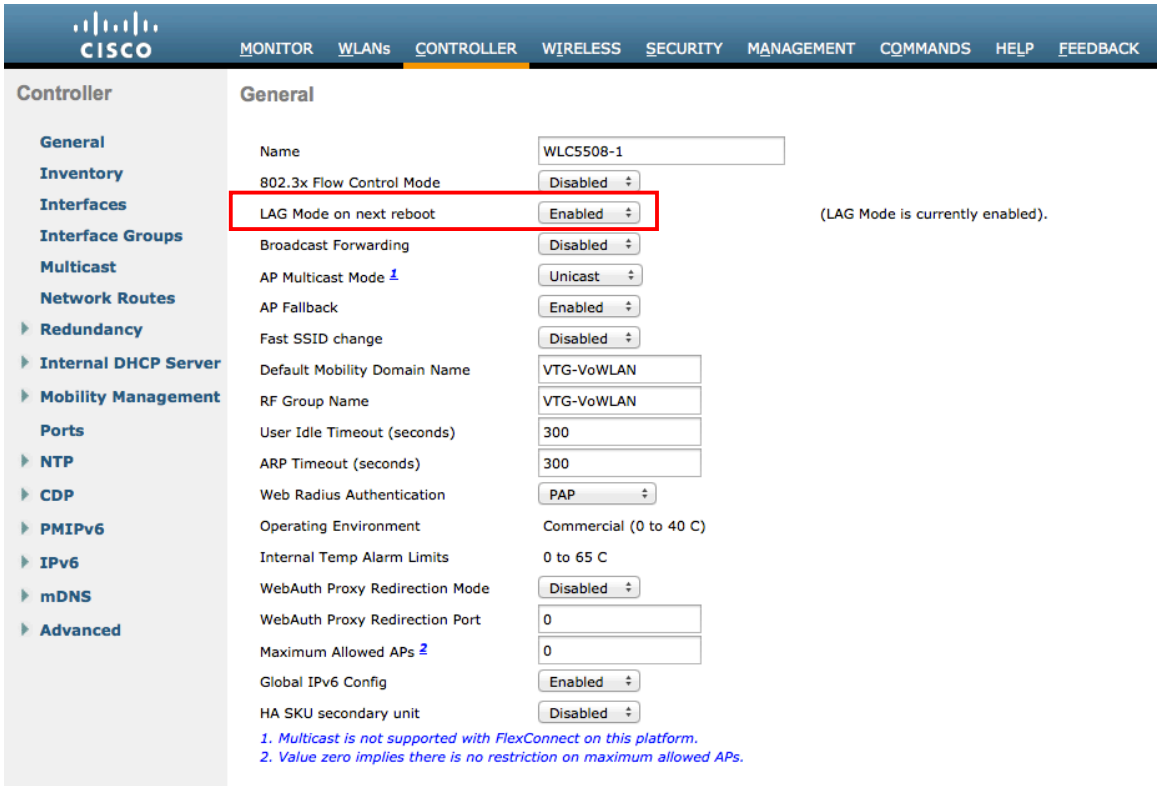
Ensure the Cisco Unified Wireless LAN Controller hostname is configured correctly.

Enable Link Aggregation (LAG) if utilizing multiple ports on the Cisco Unified Wireless LAN Controller.

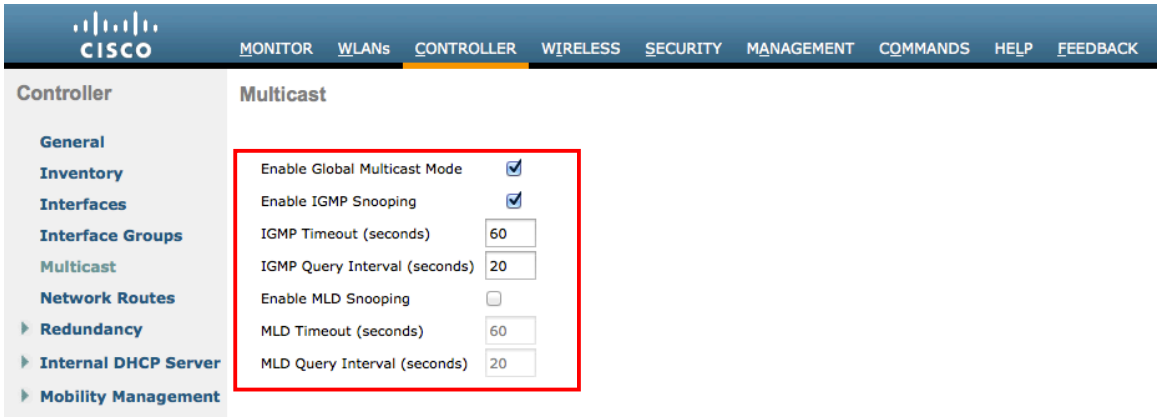
Configure the desired AP multicast mode.

In releases prior to 6.0, Aggressive Load Balancing was configured in the General Controller settings.

In 6.0 and later, this is referred to as Client Load Balancing and is configurable under the WLAN configuration (SSID settings).

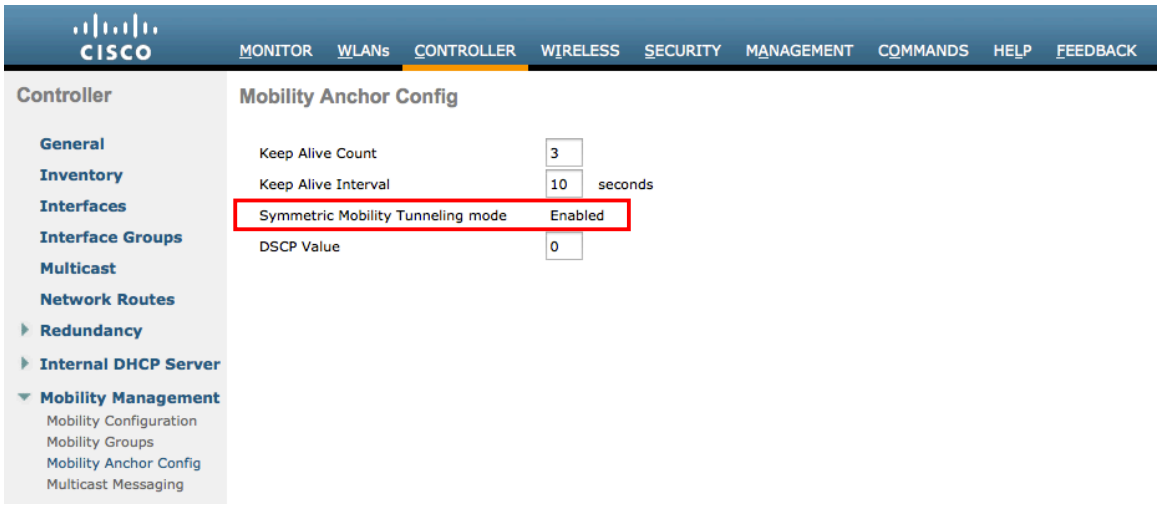


If utilizing multicast, then **Enable Global Multicast Mode** and **Enable IGMP Snooping** should be enabled.

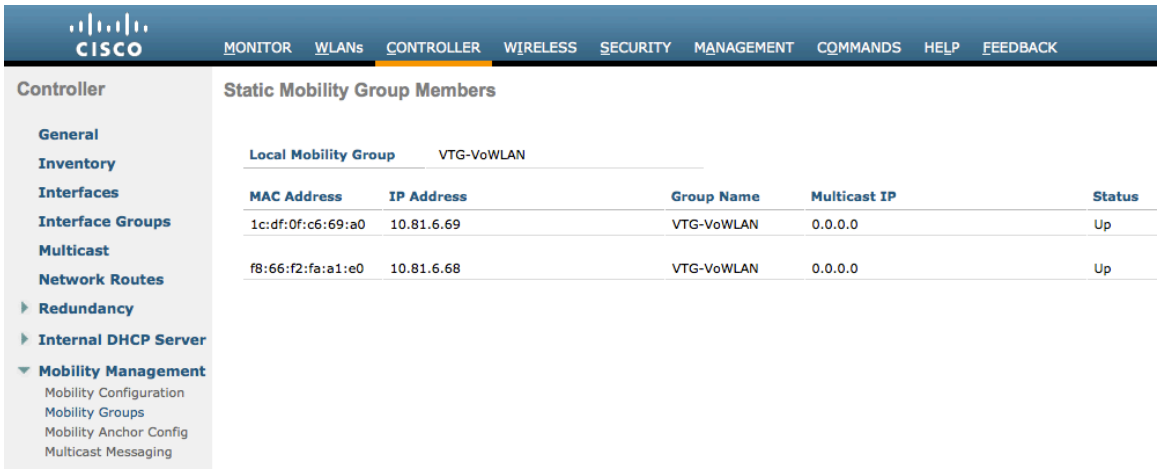


If utilizing layer 3 mobility, then **Symmetric Mobility Tunneling** should be **Enabled**.

In the recent versions, Symmetric Mobility Tunneling is enabled by default and non-configurable.



When multiple Cisco Unified Wireless LAN Controllers are to be in the same mobility group, then the IP address and MAC address of each Cisco Unified Wireless LAN Controller should be added to the Static Mobility Group Members configuration.



802.11 Network Settings

If using 5 GHz, ensure the 802.11a network status is **Enabled**.

Set the **Beacon Period** to **100 ms**.

Ensure **DTPC Support** is enabled.

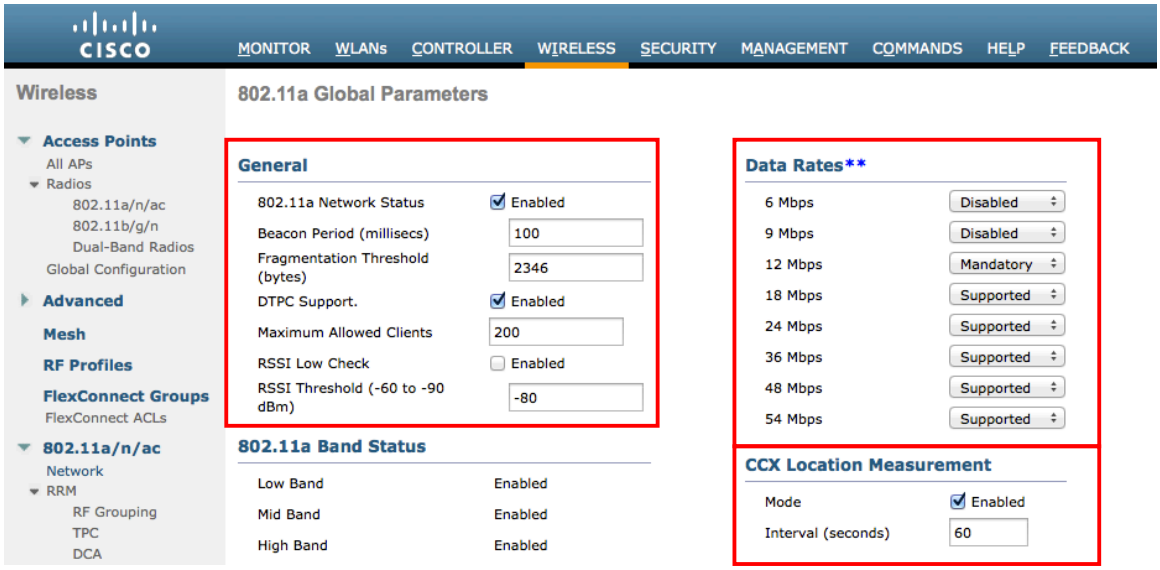
If using Cisco 802.11n Access Points, ensure **ClientLink** is enabled.

With the current releases, **Maximum Allowed Clients** can be configured.

Recommended to set 12 Mbps as the mandatory (basic) rate and 18-24 or 18-54 Mbps as supported (optional) rates; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.

36-54 Mbps can optionally be disabled, if there are not any applications that can benefit from those rates (e.g. video).

Enable **CCX Location Measurement**.



If using 2.4 GHz, ensure the 802.11b/g network status and 802.11g is enabled.

Set the **Beacon Period** to **100 ms**.

Short Preamble should be **Enabled** 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.

Ensure **DTPC Support** is enabled.

If using Cisco 802.11n Access Points, ensure **ClientLink** is enabled.

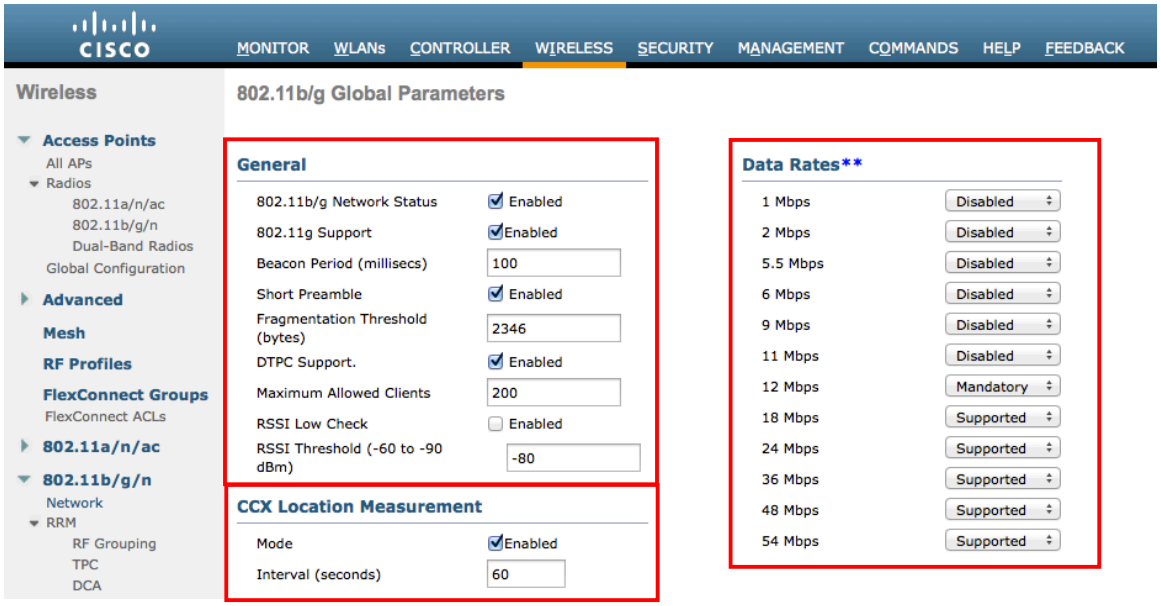
With the current releases, **Maximum Allowed Clients** can be configured.

Recommended to set 12 Mbps as the mandatory (basic) rate and 18-24 or 18-54 Mbps as supported (optional) rates assuming that there will not be any 802.11b only clients that will connect to the wireless LAN; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.

If 802.11b clients exist, then 11 Mbps should be set as the mandatory (basic) rate and 12-24 or 54 Mbps as supported (optional).

36-54 Mbps can optionally be disabled, if there are not any applications that can benefit from those rates (e.g. video).

Enable **CCX Location Measurement**.



Beamforming (ClientLink)

Enable **ClientLink** if using Cisco 802.11n Access Points.

Beamforming is not supported with data rates 1, 2, 5.5, and 11 Mbps.

For releases prior to 7.2.103.0, **ClientLink** can be enabled globally via the 802.11 Global Parameters section or on individual access points via the access point's 802.11 radio configuration page.

As of release 7.2.103.0, **ClientLink** is no longer configurable via the Cisco Unified Wireless LAN Controller's web interface and is only configurable via command line.

With releases 7.2.103.0 and later use the following commands to enable the beamforming feature globally for all access points or for individual access point radios.

(Cisco Controller) >config 802.11a beamforming global enable

(Cisco Controller) >config 802.11a beamforming ap <ap_name> enable

(Cisco Controller) >config 802.11b beamforming global enable

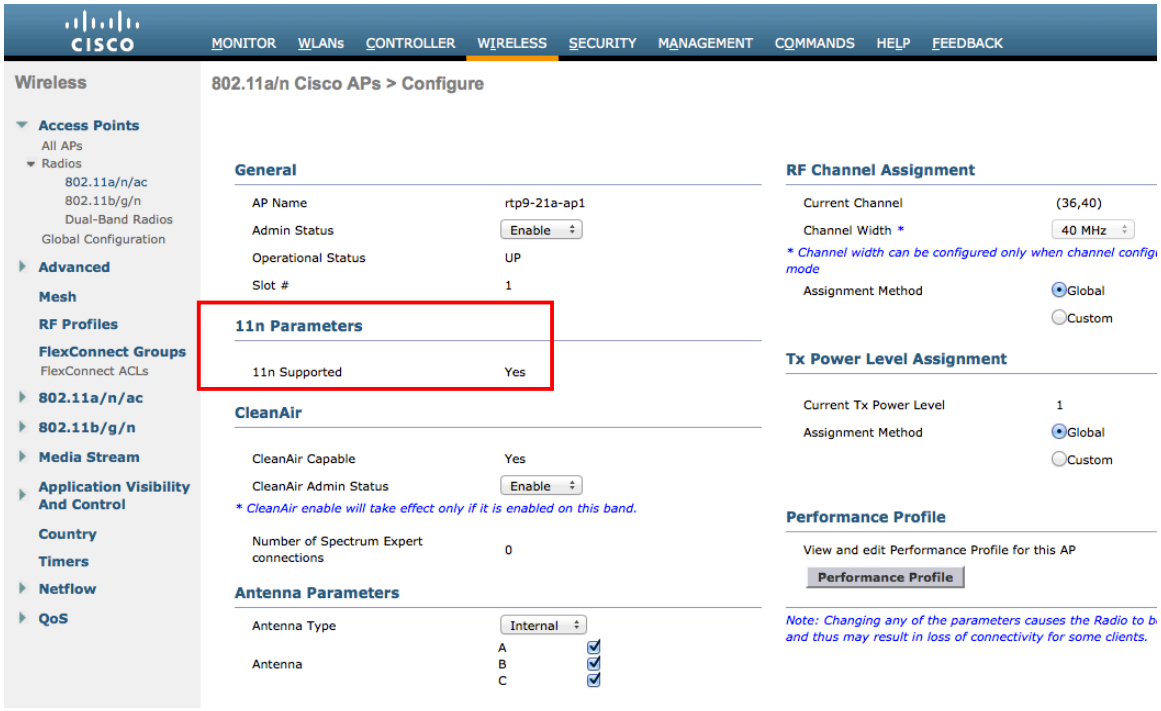
(Cisco Controller) >config 802.11b beamforming ap <ap_name> enable

The current status of the beamforming feature can be displayed by using the following command.

(Cisco Controller) >show 802.11a

(Cisco Controller) >show 802.11b

Legacy Tx Beamforming setting..... **Enabled**

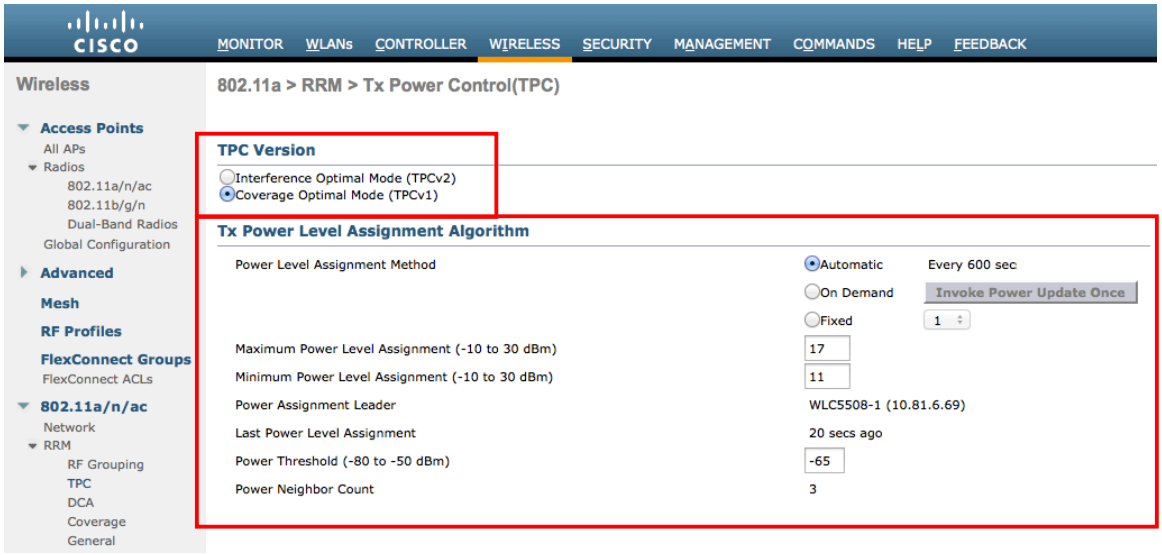


Auto RF (RRM)

When using the Cisco Unified Wireless LAN Controller it is recommended to enable Auto RF to manage the channel and transmit power settings.

Configure the access point transmit power level assignment method for either 5 or 2.4 GHz depending on which frequency band is to be utilized.

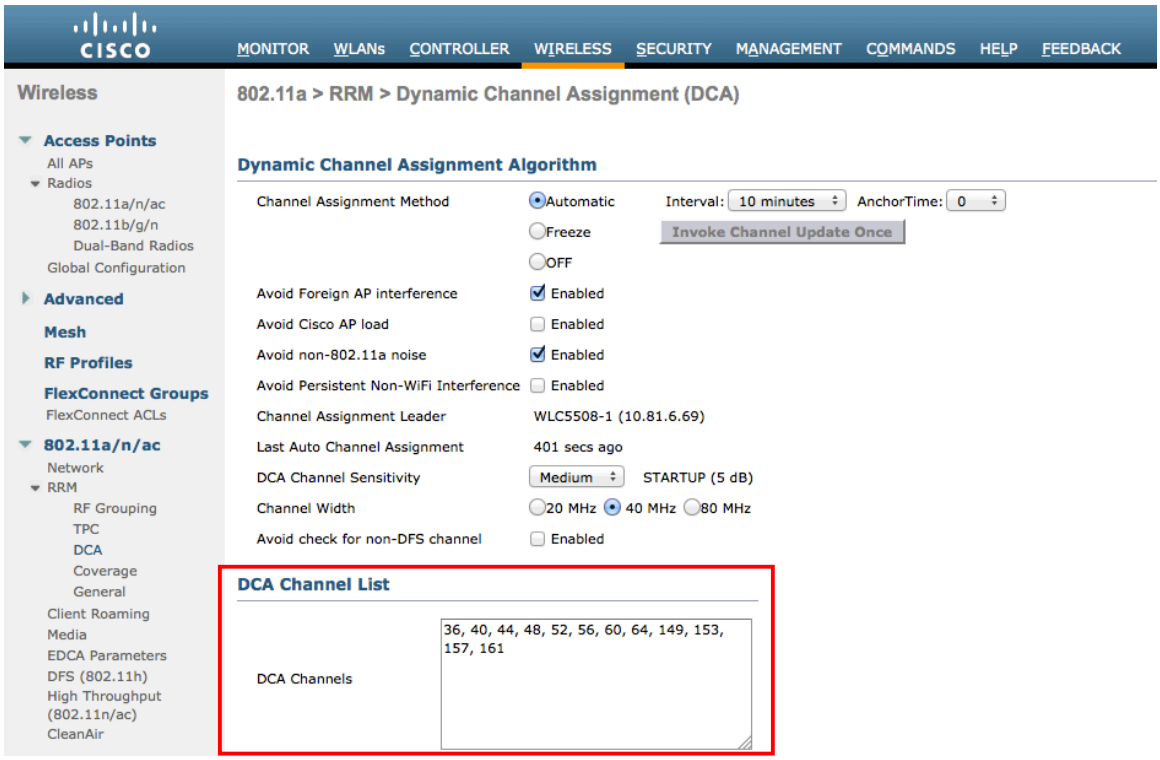
If using automatic power level assignment, a maximum and minimum power level can be specified.



If using 5 GHz, it is recommended to enable up to 12 channels only to avoid any potential delay of access point discovery due to having to scan many channels.

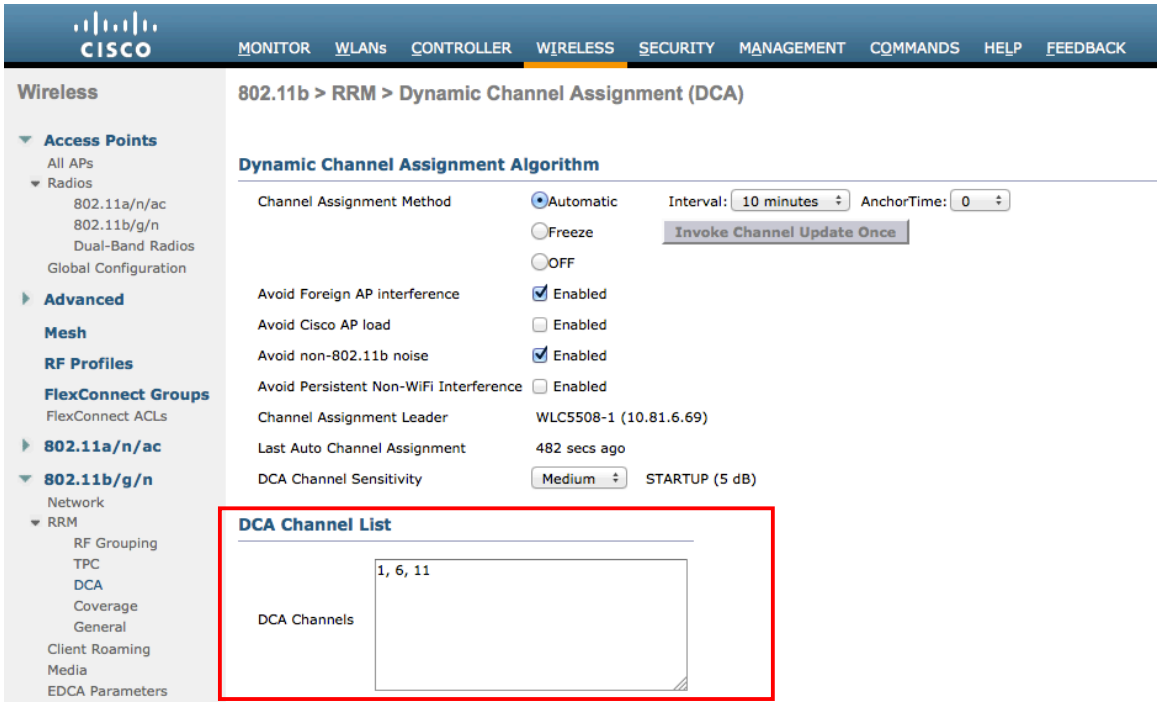
The 5 GHz channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n Access Points.

Ensure that channel 165 is not enabled in the DCA list as the Cisco Unified Wireless IP Phone 7921G does not support this channel.



If using 2.4 GHz, only channels 1, 6, and 11 should be enabled in the DCA list.

It is recommended to configure the 2.4 GHz channel for 20 MHz even if using Cisco 802.11n Access Points capable of 40 MHz due to the limited number of channels available in 2.4 GHz.



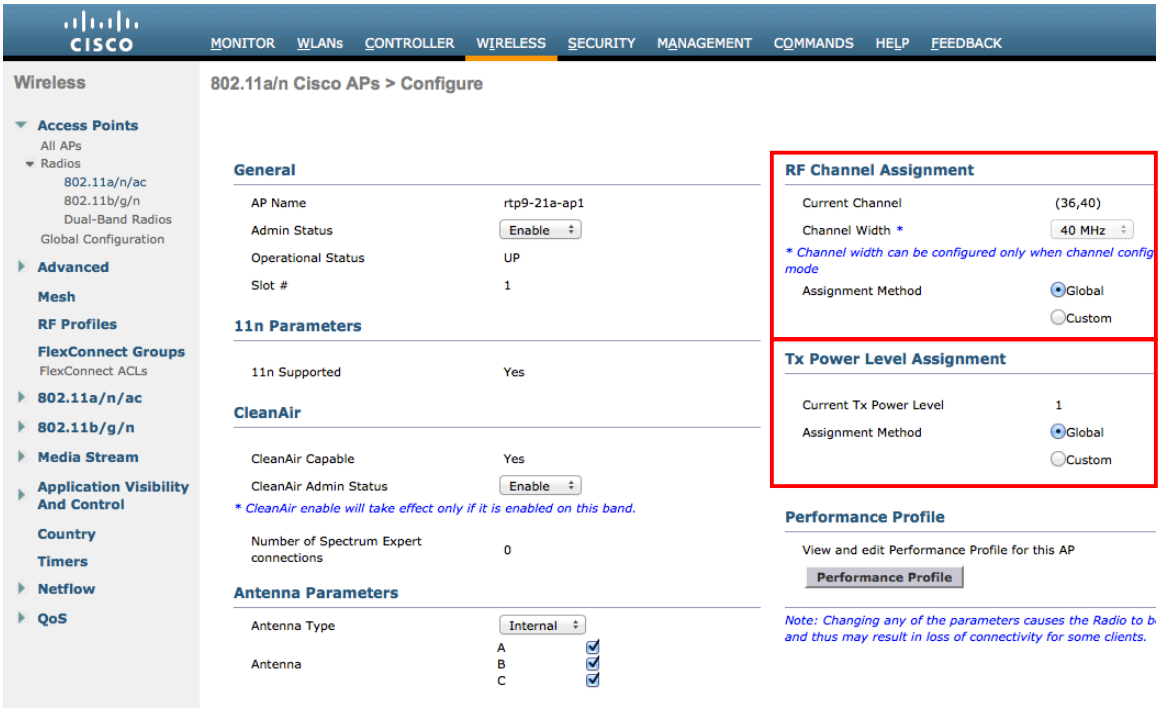
Individual access points can be configured to override the global setting to use dynamic channel and transmit power assignment for either 5 or 2.4 GHz depending on which frequency band is to be utilized.

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 channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n Access Points.

It is recommended to use 40 MHz channels only if using 5 GHz.



Client Roaming

The Cisco Unified Wireless IP Phone 7921G does not utilize the RF parameters in the Client Roaming section of the Cisco Unified Wireless LAN Controller as scanning and roaming is managed independently by the phone itself.

Call Admission Control

It is recommended to enable **Admission Control Mandatory** for **Voice** and configure the maximum bandwidth and reserved roaming bandwidth percentages for either 5 or 2.4 GHz depending on which frequency band is to be utilized.

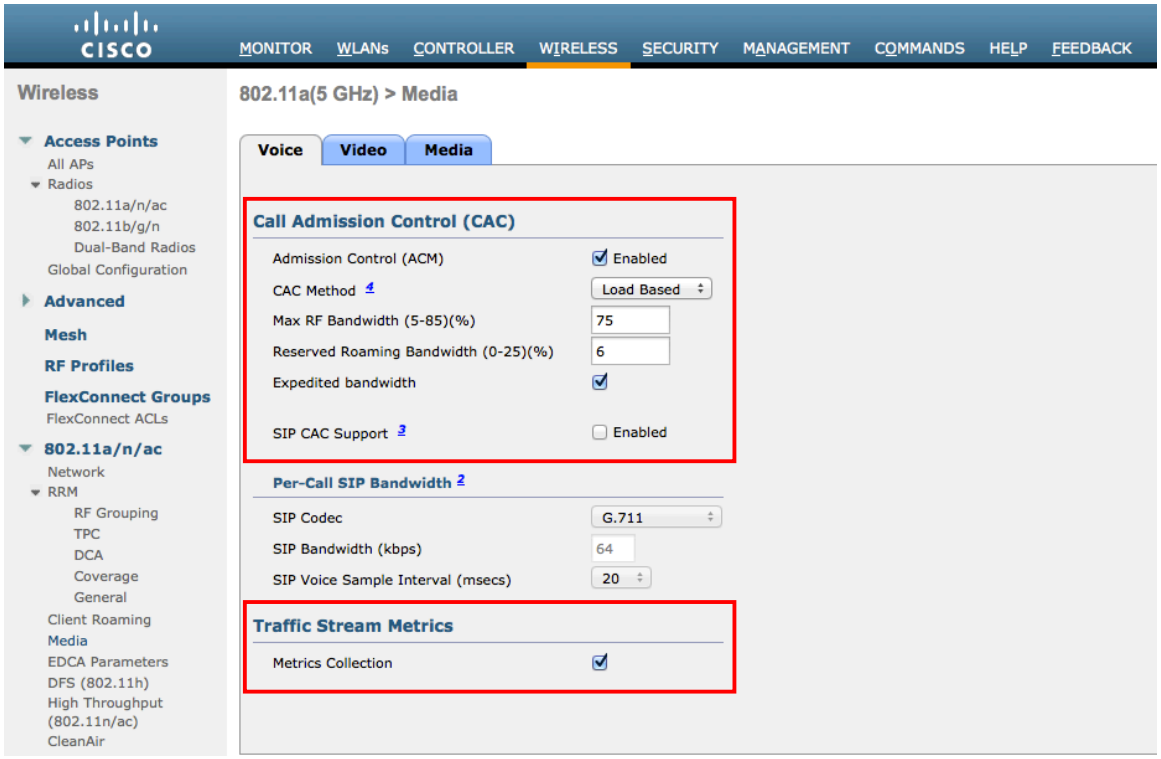
The maximum bandwidth default setting for voice is **75%** where **6%** of that bandwidth is reserved for roaming clients.

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

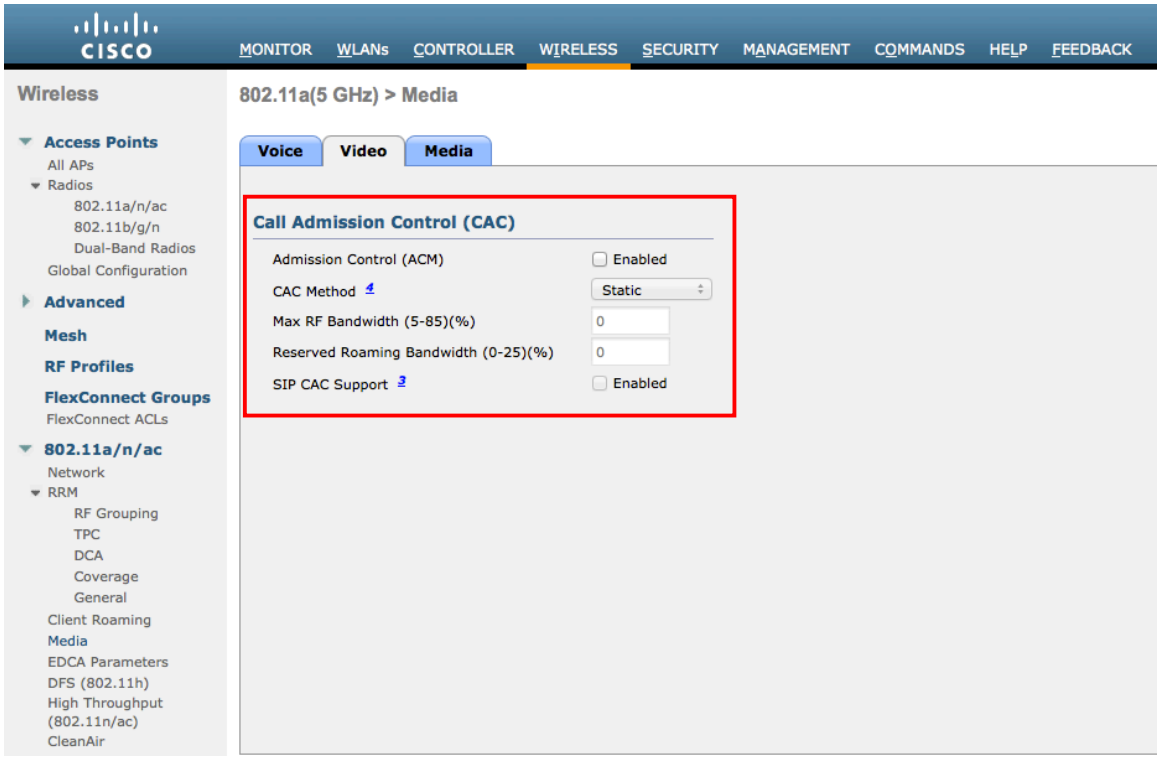
If CAC is to be enabled, will want to ensure **Load-based CAC** is enabled, which is available for the Cisco Unified Wireless LAN Controller, but not currently available on the Cisco Autonomous Access Point platform.

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

Enable **Traffic Stream Metrics (TSM)**.



Admission Control Mandatory for **Video** should be disabled.



If Call Admission Control for voice is enabled, then 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.

(Cisco Controller) >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 by using the following command.

(Cisco Controller) >show wlan <WLAN id>

Quality of Service..... Platinum (voice)
WMM..... Allowed
Dot11-Phone Mode (7920)..... ap-cac-limit
Wired Protocol..... 802.1P (Tag=5)

When enabling Call Admission Control on the Cisco Autonomous Access Point, the admission must be unblocked on the SSID as well.

It is required to enable Call Admission Control on the SSID configuration, regardless of Admission Control being enabled for Voice or Video.

Load-based CAC and support for multiple streams are not present on the Cisco Autonomous Access Points therefore it is not recommended to enable CAC on Cisco Autonomous Access Points.

The Cisco Autonomous Access Point only allows for 1 stream and the stream size is not customizable, therefore SRTP and barge will not work if CAC is enabled.

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 Cisco Autonomous Access Point.

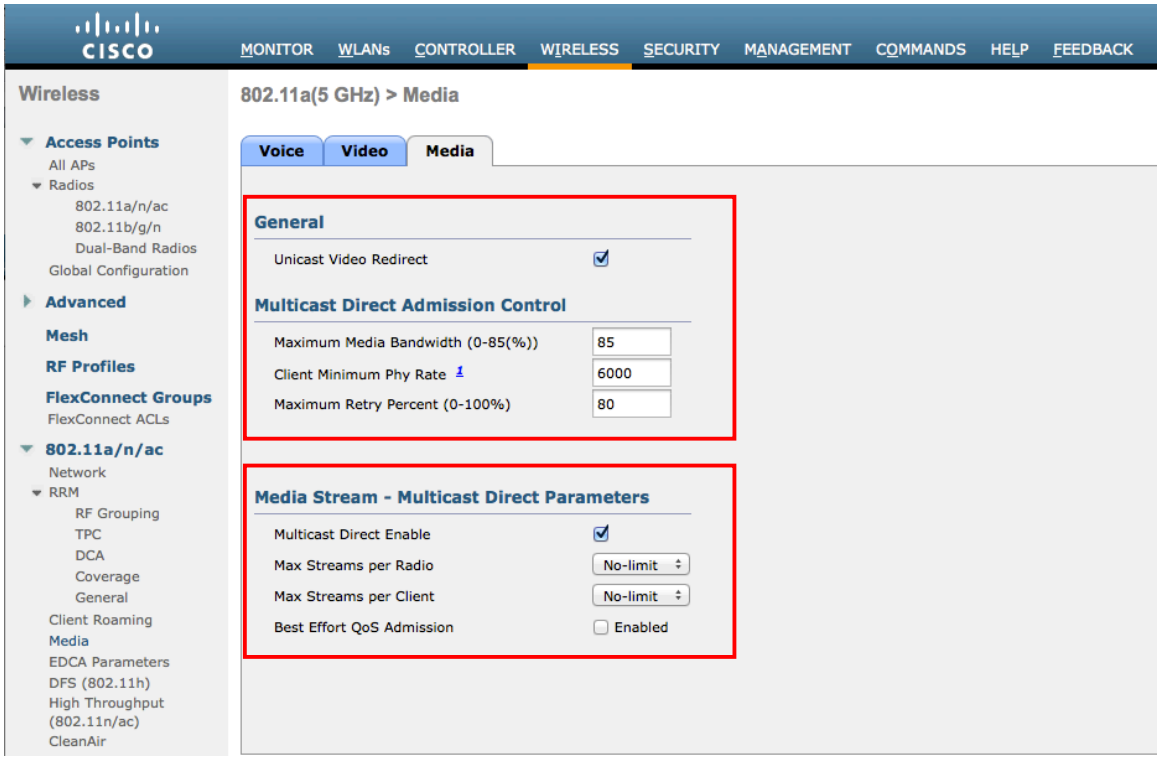
It is recommended to use the defaults, where 5.5, 6.0, 11.0, 12.0 and 24.0 Mbps are enabled as nominal rates for 802.11b/g and 6.0, 12.0 and 24.0 Mbps enabled for 802.11a.

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 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/partner/docs/wireless/access_point/12.4.25d.JA/Configuration/guide/scg12.4.25d.JA-chap15-qos.html

In the Media settings, **Unicast Video Redirect** and **Multicast Direct Enable** should be enabled.



EDCA Parameters

Set the EDCA profile for **Voice Optimized** and disable **Low Latency MAC** for either 5 or 2.4 GHz depending on which frequency band is to be utilized.

Low Latency MAC (LLM) reduces the number of retransmissions to 2-3 per packet depending on the access point platform, so it can cause issues if multiple data rates are enabled.

LLM is not supported on the Cisco 802.11n Access Points.

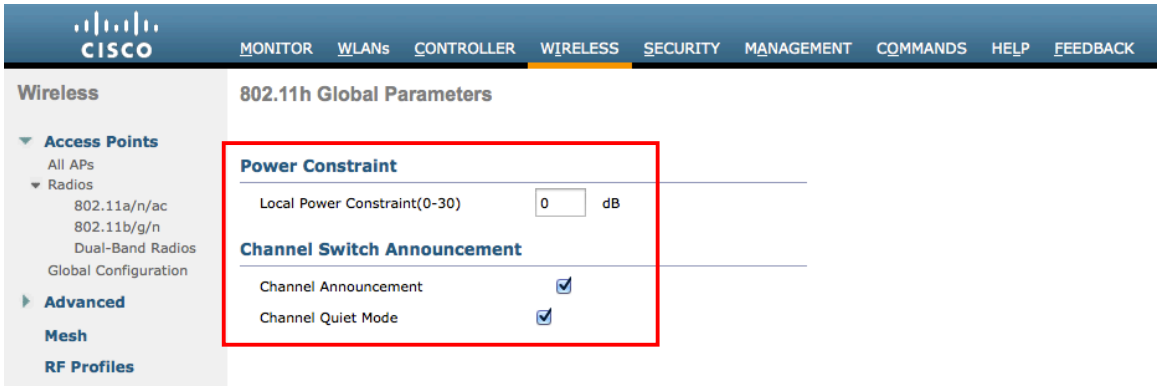
DFS (802.11h)

In the DFS (802.11h) configuration, channel announcement and quiet mode should be enabled.

Power Constraint should be left un-configured or set to 0 dB as DTPC will be used by the Cisco Unified Wireless IP Phone 7921G to control the transmission power.

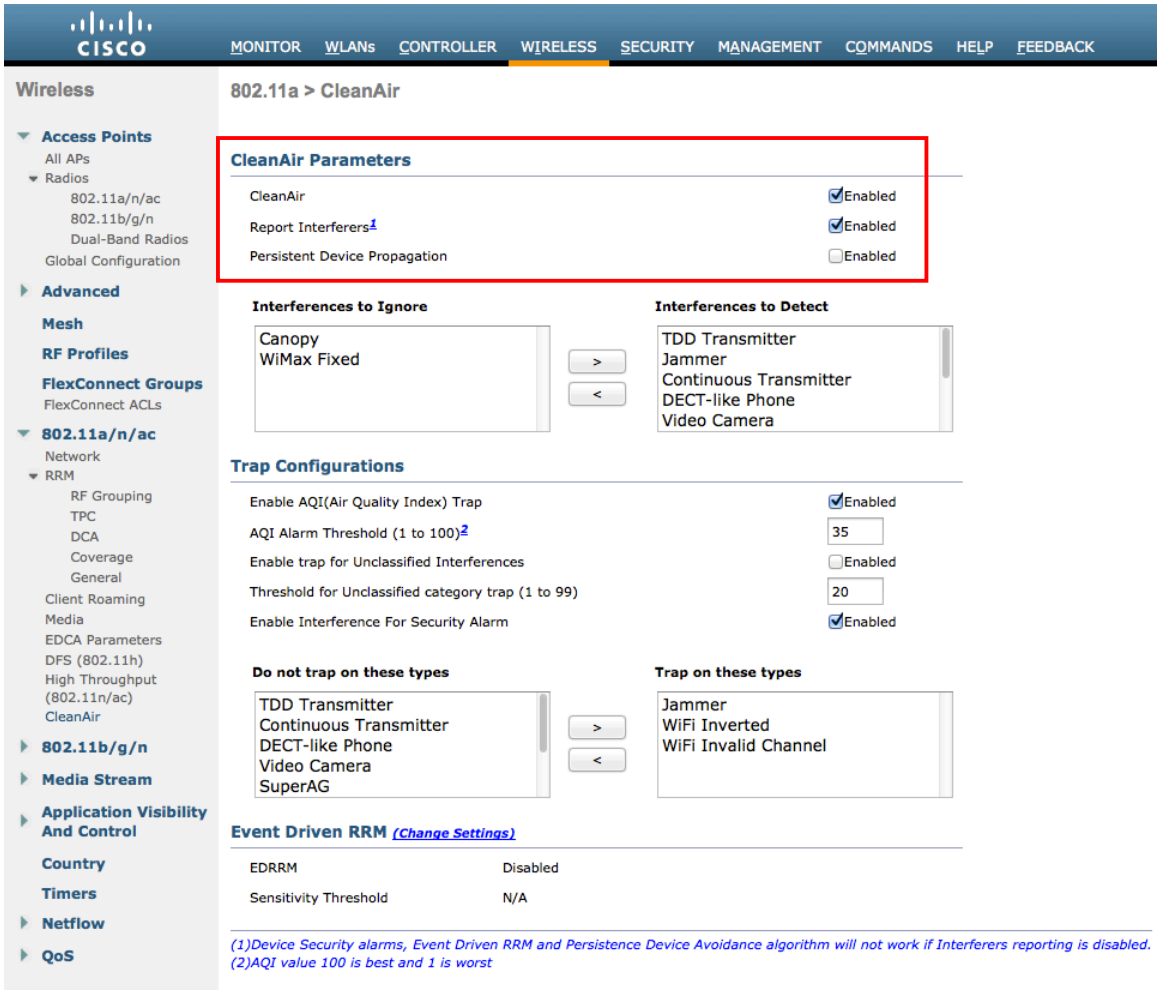
In later versions of the Cisco Unified Wireless LAN Controller it does not allow both TPC (Power Constraint) and DTPC (Dynamic Transmit Power Control) to be enabled simultaneously.

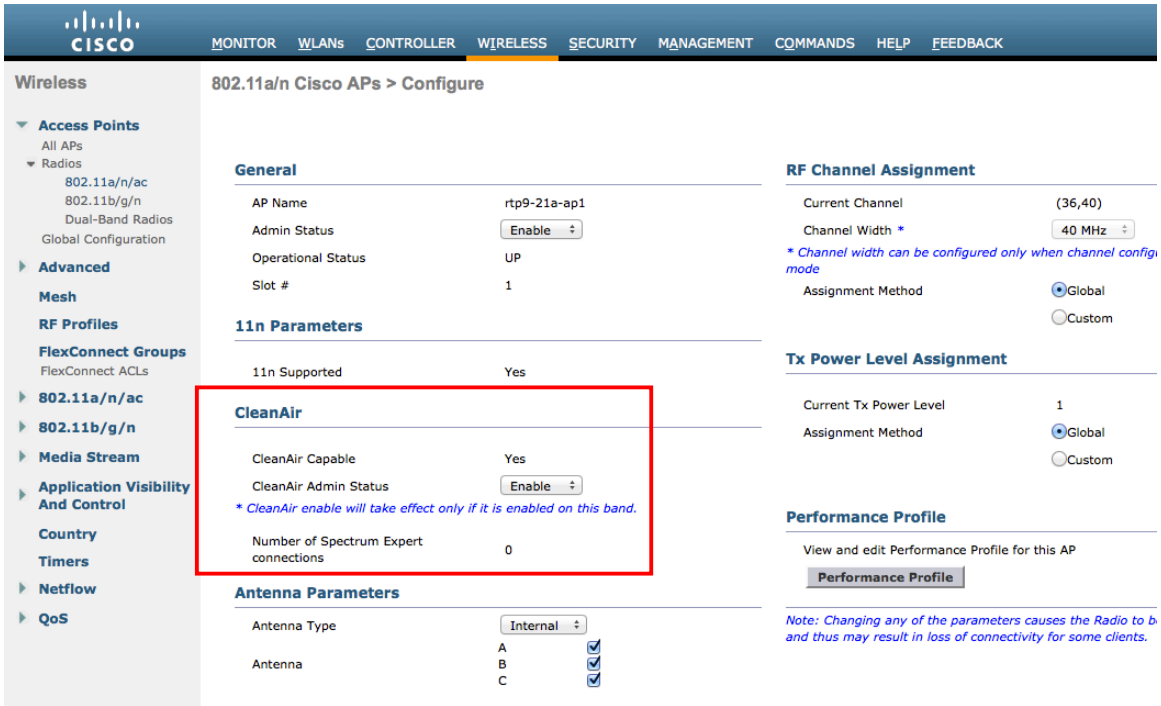
Channel Announcement and **Channel Quiet Mode** should be enabled.



CleanAir

CleanAir should be **Enabled** when utilizing Cisco Access Points with CleanAir technology in order to detect any existing interferers.

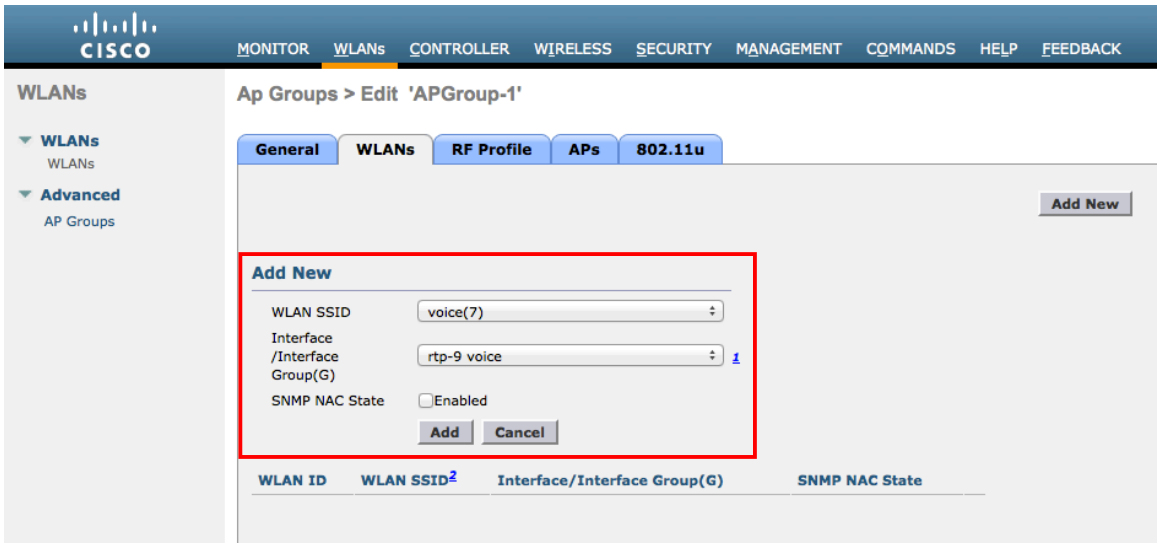

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless
802.11a > CleanAir
Access Points
All APs
Radios
802.11a/n/ac
802.11b/g/n
Dual-Band Radios
Global Configuration
Advanced
Mesh
RF Profiles
FlexConnect Groups
FlexConnect ACLs
802.11a/n/ac
Network
RRM
RF Grouping
TPC
DCA
Coverage
General
Client Roaming
Media
EDCA Parameters
DFS (802.11h)
High Throughput (802.11n/ac)
CleanAir
802.11b/g/n
Media Stream
Application Visibility And Control
Country
Timers
Netflow
QoS
CleanAir Parameters
CleanAir
Enabled
Report Interferers[1]
Enabled
Persistent Device Propagation
Enabled
Interferences to Ignore
Canopy
WiMax Fixed
Interferences to Detect
TDD Transmitter
Jammer
Continuous Transmitter
DECT-like Phone
Video Camera
Trap Configurations
Enable AQI(Air Quality Index) Trap
Enabled
AQI Alarm Threshold (1 to 100)[2]
35
Enable trap for Unclassified Interferences
Enabled
Threshold for Unclassified category trap (1 to 99)
20
Enable Interference For Security Alarm
Enabled
Do not trap on these types
TDD Transmitter
Continuous Transmitter
DECT-like Phone
Video Camera
SuperAG
Trap on these types
Jammer
WiFi Inverted
WiFi Invalid Channel
Event Driven RRM (Change Settings)
EDRRM
Disabled
Sensitivity Threshold
N/A
(1)Device Security alarms, Event Driven RRM and Persistence Device Avoidance algorithm will not work if Interferers reporting is disabled.
(2)AQI value 100 is best and 1 is worst


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless
802.11a/n Cisco APs > Configure
Access Points
All APs
Radios
802.11a/n/ac
802.11b/g/n
Dual-Band Radios
Global Configuration
Advanced
Mesh
RF Profiles
FlexConnect Groups
FlexConnect ACLs
802.11a/n/ac
802.11b/g/n
Media Stream
Application Visibility And Control
Country
Timers
Netflow
QoS
General
AP Name
rtp9-21a-ap1
Admin Status
Enable
Operational Status
UP
Slot #
1
11n Parameters
11n Supported
Yes
CleanAir
CleanAir Capable
Yes
CleanAir Admin Status
Enable
* CleanAir enable will take effect only if it is enabled on this band.
Number of Spectrum Expert connections
0
Antenna Parameters
Antenna Type
Internal
Antenna
A
B
C
RF Channel Assignment
Current Channel
(36,40)
Channel Width *
40 MHz
* Channel width can be configured only when channel config mode
Assignment Method
Global
Custom
Tx Power Level Assignment
Current Tx Power Level
1
Assignment Method
Global
Custom
Performance Profile
View and edit Performance Profile for this AP
Performance Profile
Note: Changing any of the parameters causes the Radio to b and thus may result in loss of connectivity for some clients.

AP Groups

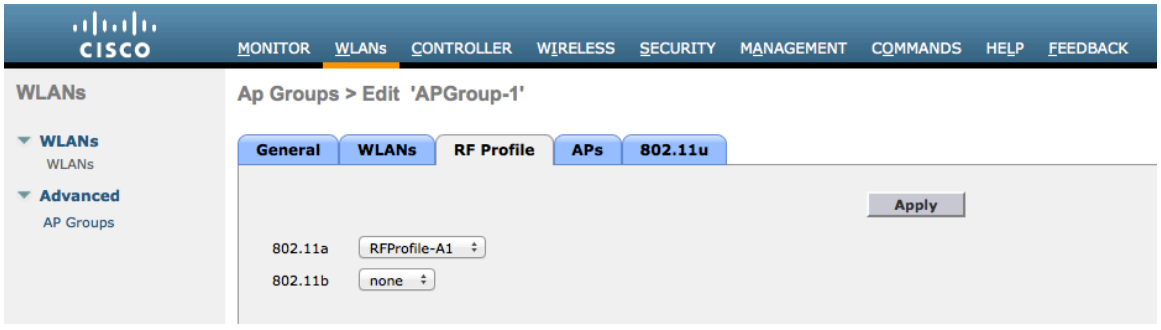
AP Groups can be created to specify which WLANs / SSIDs are to be enabled and which interface they should be mapped to as well as what RF Profile parameters should be used for the access points assigned to the AP Group.

On the **WLANs** tab, select the desired SSIDs and interfaces to map to then select **Add**.



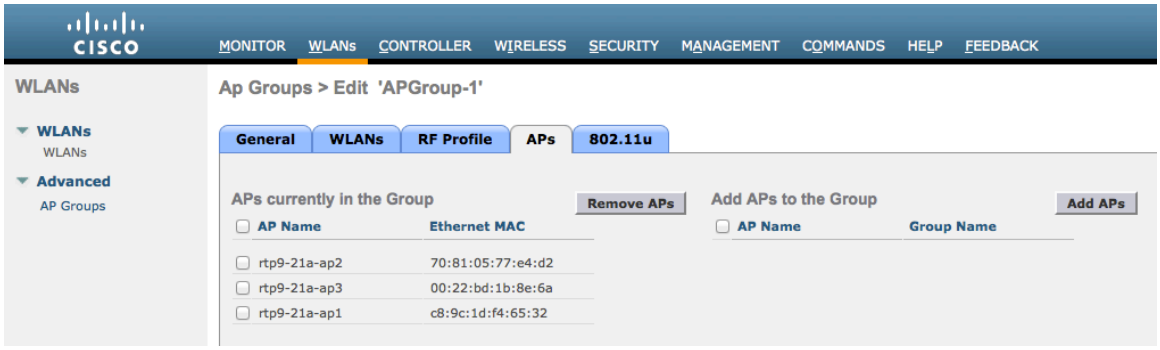
On the **RF Profile** tab, select the desired 802.11a or 802.11b RF Profile, then select **Apply**.

If changes are made after access points have joined the AP Group, then those access points will reboot once those changes are made.



On the **APs** tab, select the desired access points then select **Add APs**.

Those access points will then reboot.



RF Profiles

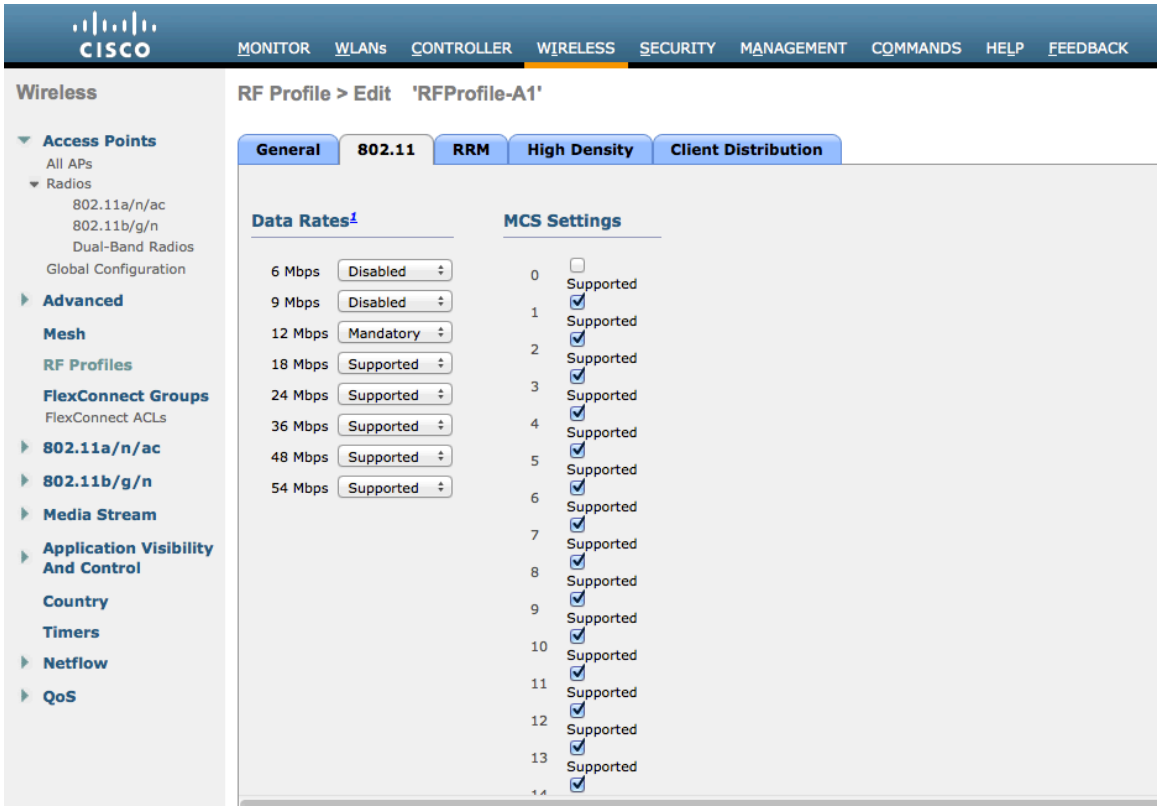
RF Profiles can be created to specify which frequency bands, data rates, RRM settings, etc. a group of access points should use. RF Profiles are applied to an AP group once created. See the AP Groups section for more info on AP Group configuration.

When creating an RF Profile, the **RF Profile Name** and **Radio Policy** must be defined.

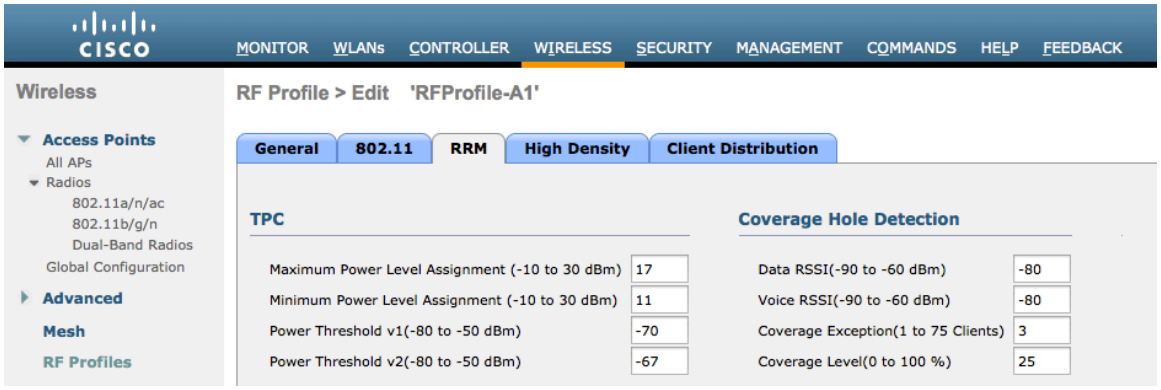
Select 802.11a or 802.11b/g for the **Radio Policy**.

On the **802.11** tab, configure the data rates as desired.

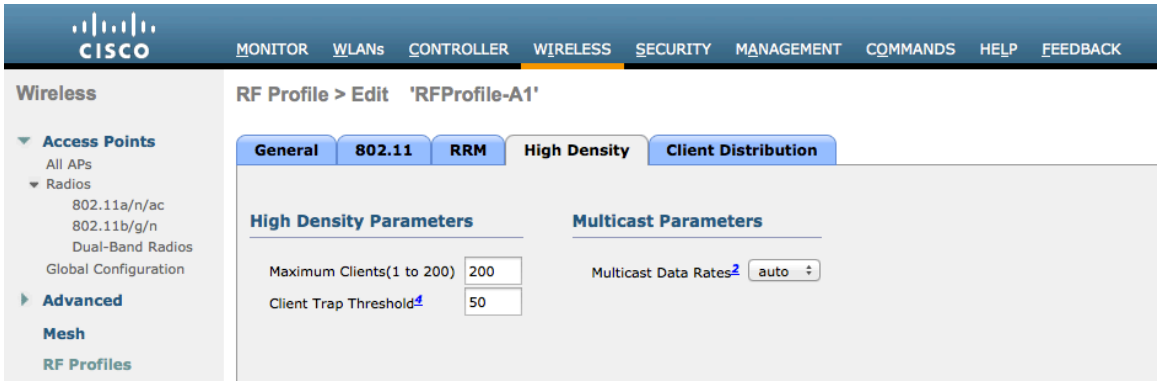
Is recommended to enable 12 Mbps as **Mandatory** and 18-54 Mbps as **Supported**; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.



On the RRM tab, the **Maximum Power Level Assignment** and **Minimum Power Level Assignment** settings as well as other **TPC** and **Coverage Hole Detection** settings can be configured.



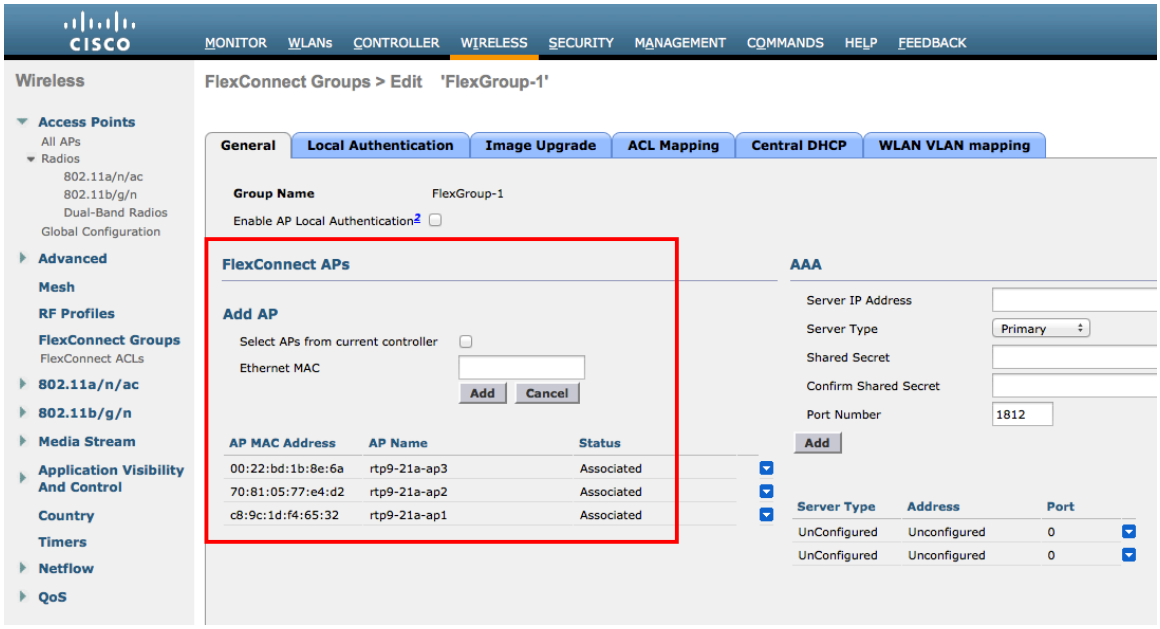
On the High Density tab, Maximum Clients and Multicast Data Rates can be configured.



FlexConnect Groups

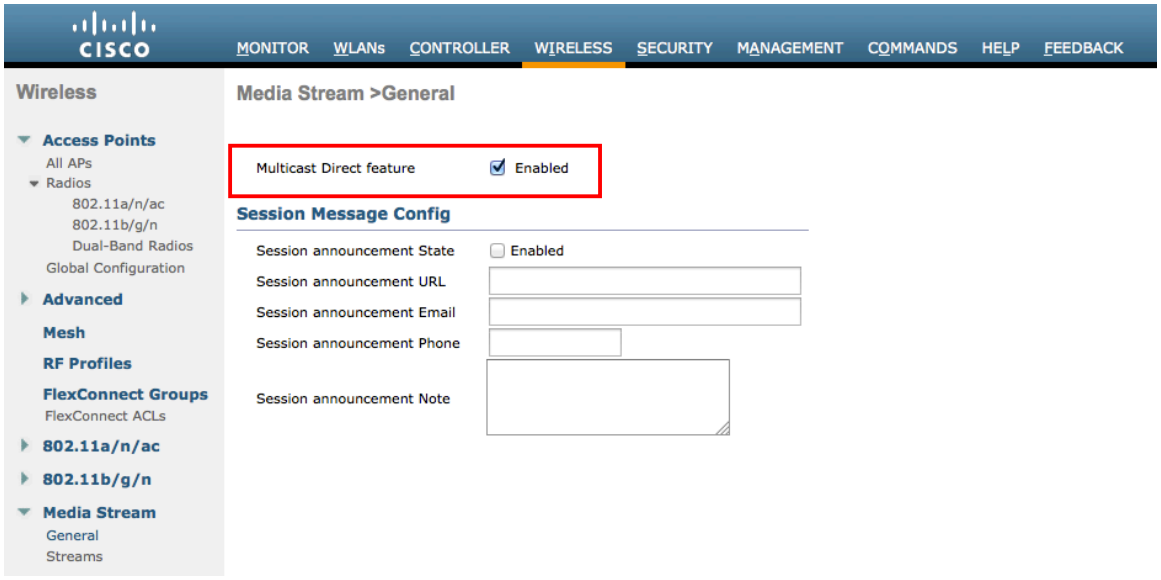
All access points configured for FlexConnect mode need to be added to a FlexConnect Group.

If utilizing CCKM, then seamless roams can only occur when roaming to access points within the same FlexConnect Group.

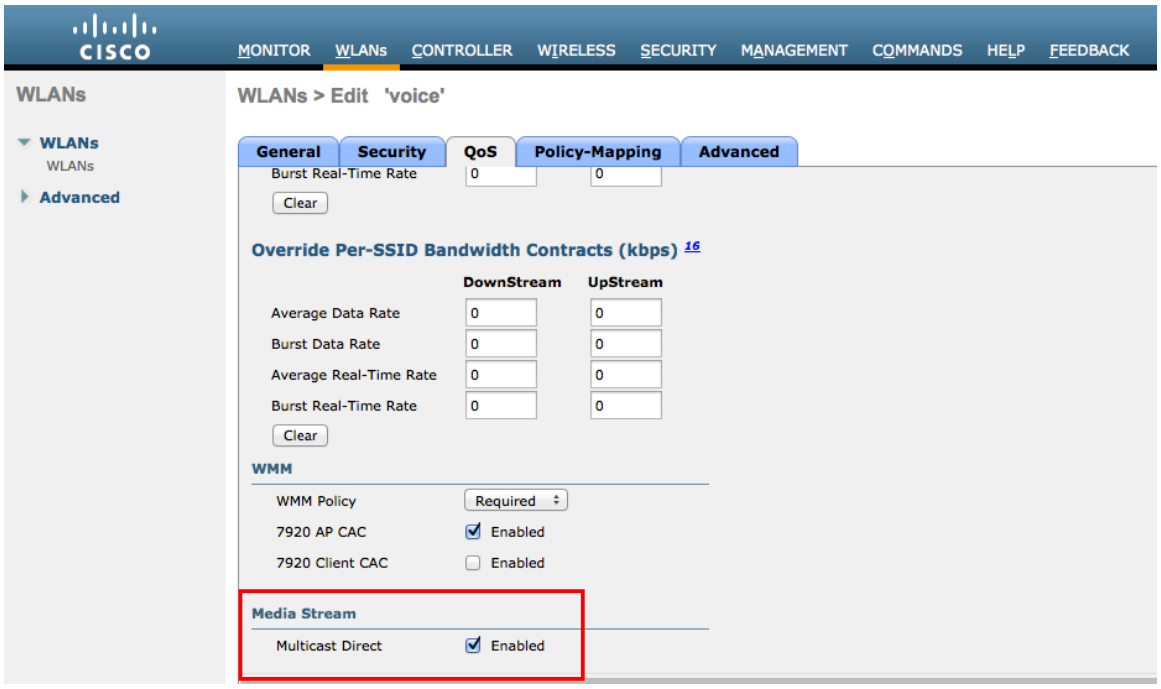


Multicast Direct

In the Media Stream settings, **Multicast Direct feature** should be enabled.



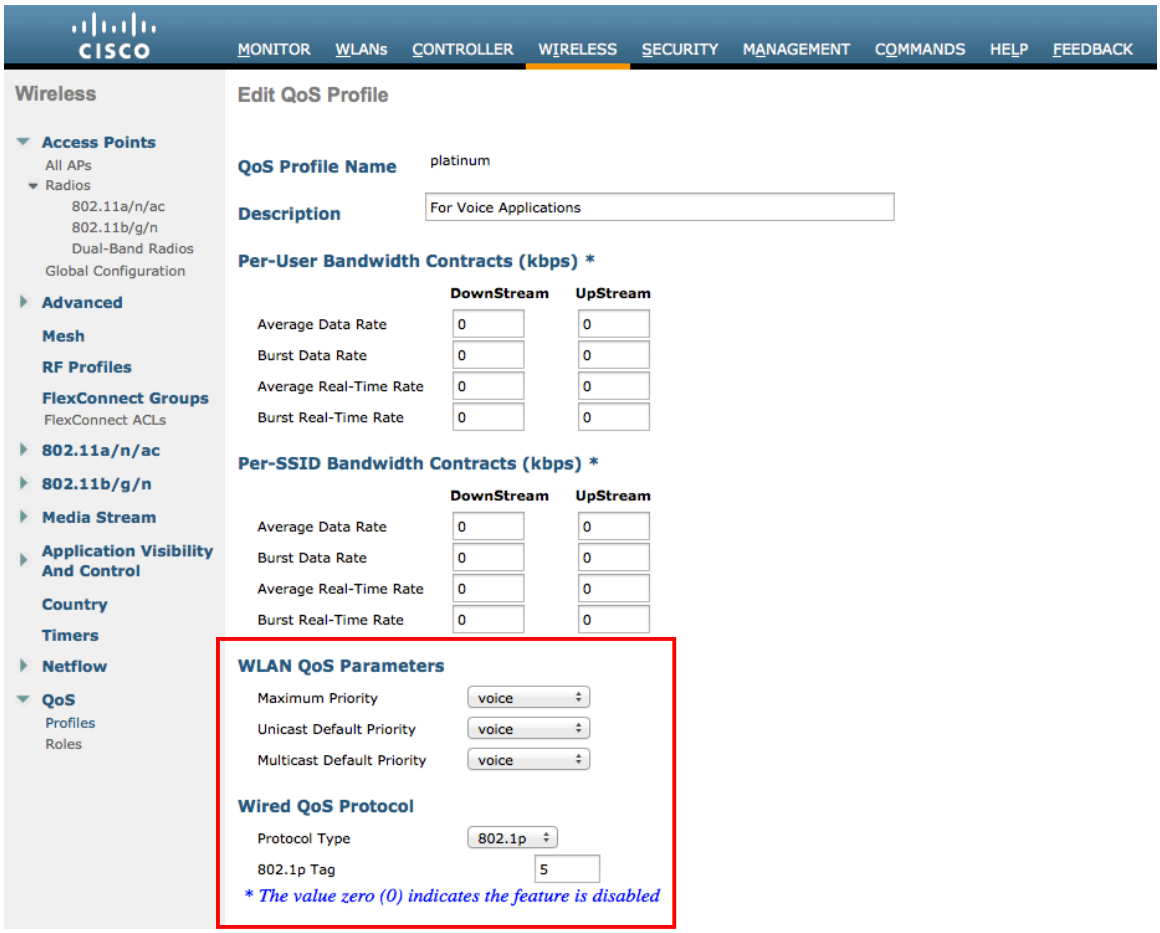
After **Multicast Direct feature** is enabled, then there will be an option to enable **Multicast Direct** in the QoS menu of the WLAN configuration.

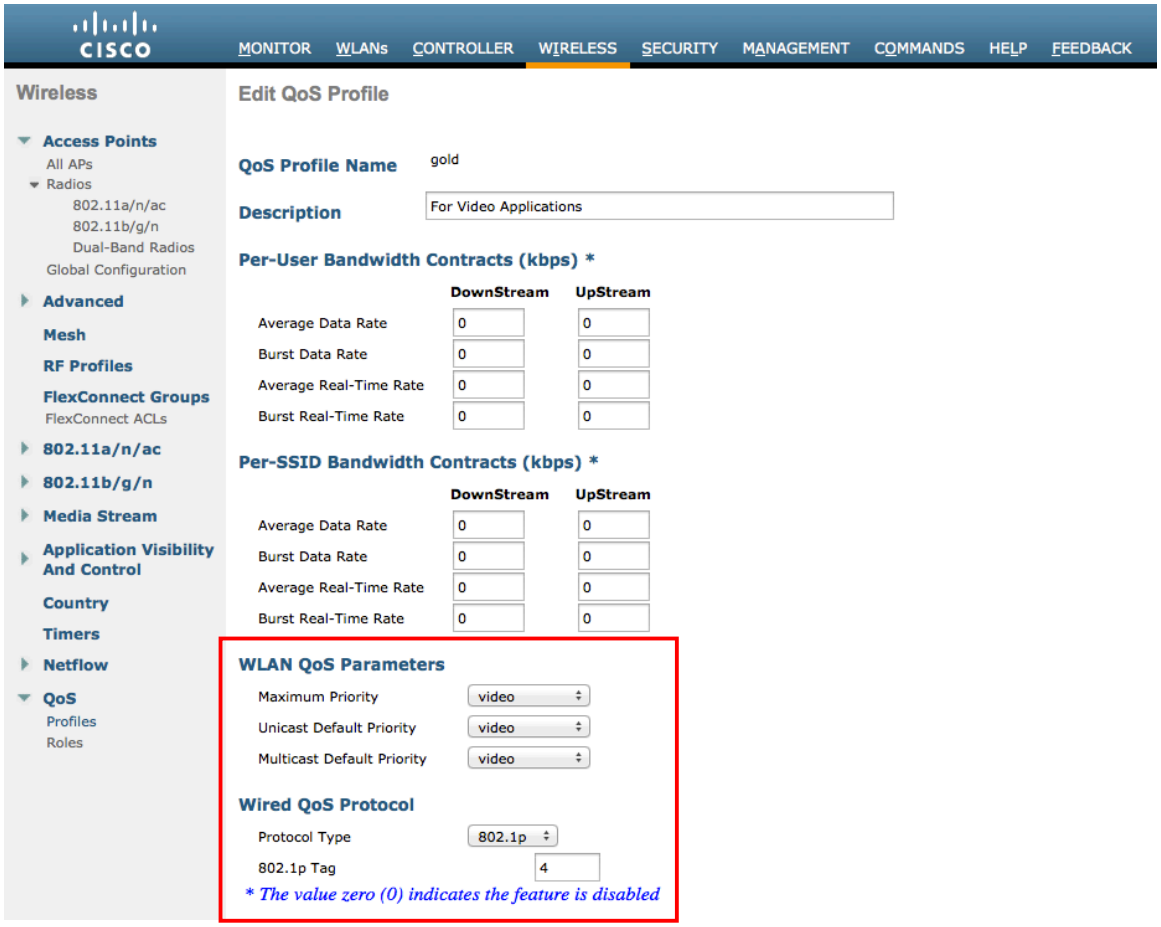


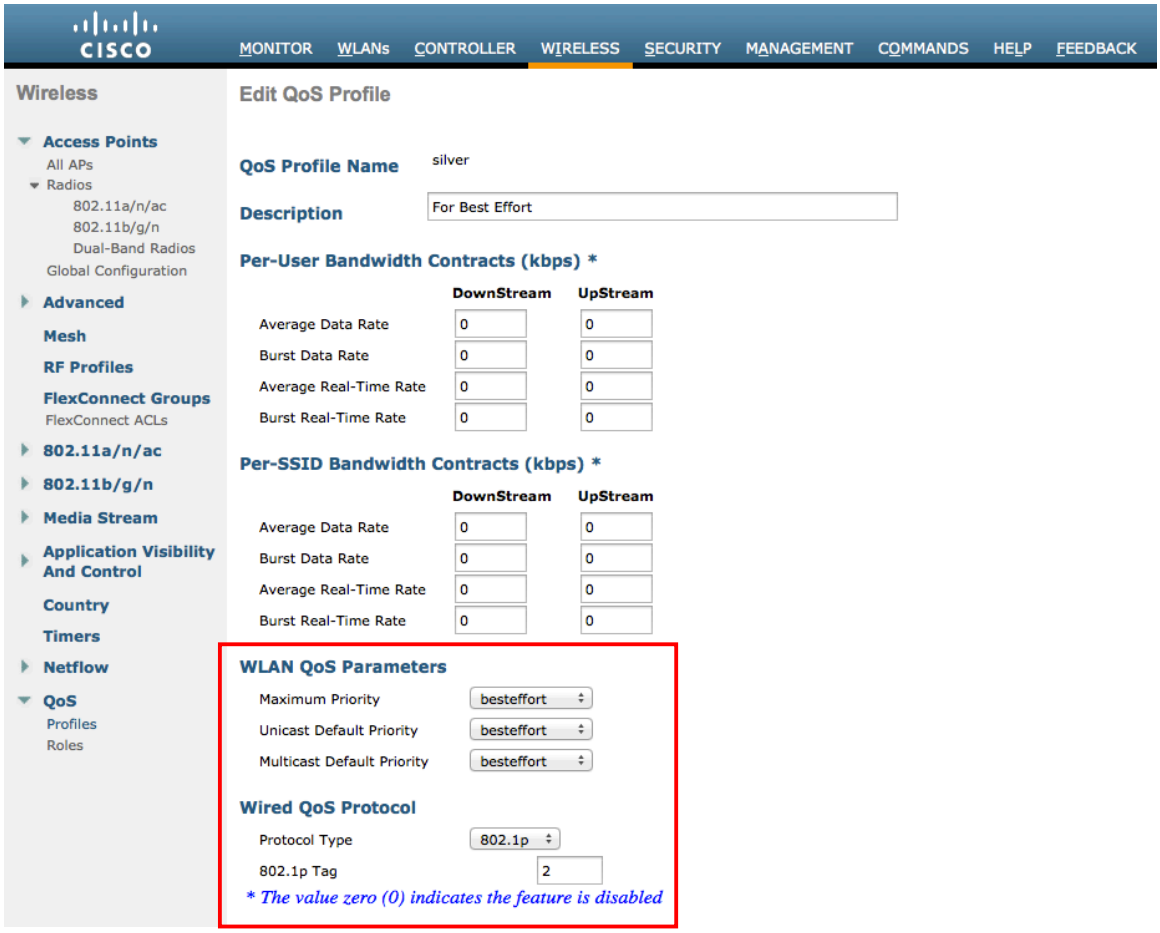
QoS Profiles

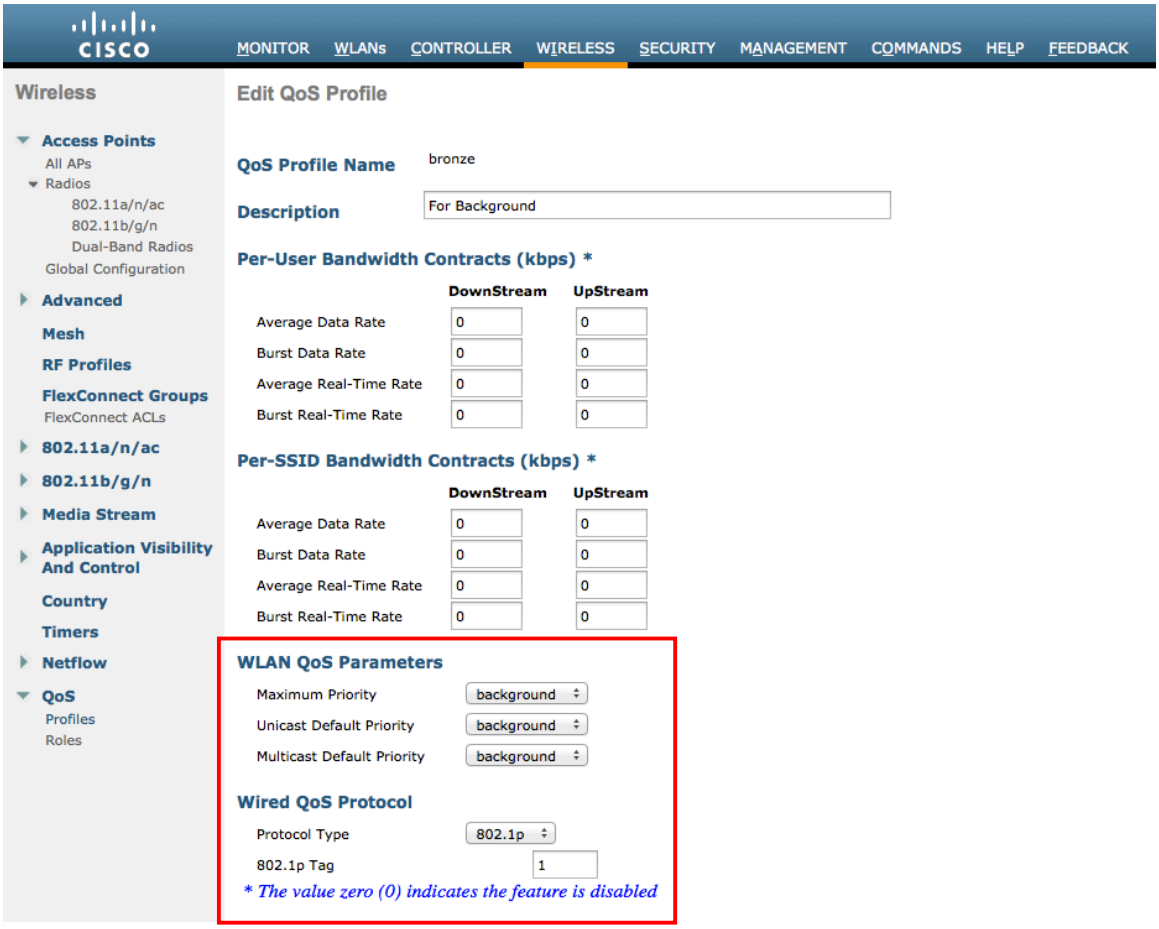
Configure the four QoS profiles (Platinum, Gold, Silver, Bronze), by selecting **802.1p** as the protocol type and set the **802.1p tag** for each profile.

- Platinum = 5
- Gold = 4
- Silver = 2
- Bronze = 1


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless
Access Points
All APs
Radios
802.11a/n/ac
802.11b/g/n
Dual-Band Radios
Global Configuration
Advanced
Mesh
RF Profiles
FlexConnect Groups
FlexConnect ACLs
802.11a/n/ac
802.11b/g/n
Media Stream
Application Visibility And Control
Country
Timers
Netflow
QoS
Profiles
Roles
Edit QoS Profile
QoS Profile Name
platinum
Description
For Voice Applications
Per-User Bandwidth Contracts (kbps) *
DownStream
UpStream
Average Data Rate
Burst Data Rate
Average Real-Time Rate
Burst Real-Time Rate
Per-SSID Bandwidth Contracts (kbps) *
WLAN QoS Parameters
Maximum Priority
Unicast Default Priority
Multicast Default Priority
voice
Wired QoS Protocol
Protocol Type
802.1p
802.1p Tag
5
* The value zero (0) indicates the feature is disabled


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless
Access Points
All APs
Radios
802.11a/n/ac
802.11b/g/n
Dual-Band Radios
Global Configuration
Advanced
Mesh
RF Profiles
FlexConnect Groups
FlexConnect ACLs
802.11a/n/ac
802.11b/g/n
Media Stream
Application Visibility And Control
Country
Timers
Netflow
QoS
Profiles
Roles
Edit QoS Profile
QoS Profile Name
gold
Description
For Video Applications
Per-User Bandwidth Contracts (kbps) *
DownStream
UpStream
Average Data Rate
Burst Data Rate
Average Real-Time Rate
Burst Real-Time Rate
Per-SSID Bandwidth Contracts (kbps) *
WLAN QoS Parameters
Maximum Priority
video
Unicast Default Priority
Multicast Default Priority
Wired QoS Protocol
Protocol Type
802.1p
802.1p Tag
4
* The value zero (0) indicates the feature is disabled


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless
Access Points
All APs
Radios
802.11a/n/ac
802.11b/g/n
Dual-Band Radios
Global Configuration
Advanced
Mesh
RF Profiles
FlexConnect Groups
FlexConnect ACLs
802.11a/n/ac
802.11b/g/n
Media Stream
Application Visibility And Control
Country
Timers
Netflow
QoS
Profiles
Roles
Edit QoS Profile
QoS Profile Name
silver
Description
For Best Effort
Per-User Bandwidth Contracts (kbps) *
DownStream
UpStream
Average Data Rate
Burst Data Rate
Average Real-Time Rate
Burst Real-Time Rate
Per-SSID Bandwidth Contracts (kbps) *
WLAN QoS Parameters
Maximum Priority
besteffort
Unicast Default Priority
Multicast Default Priority
Wired QoS Protocol
Protocol Type
802.1p
802.1p Tag
2
* The value zero (0) indicates the feature is disabled



Note: The 802.1p tag mappings were changed with the 7.5.102.0 release.

Prior to the 7.5.102.0 release, Platinum = 6, Gold = 5, Silver = 3, Bronze = 1.

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.

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.

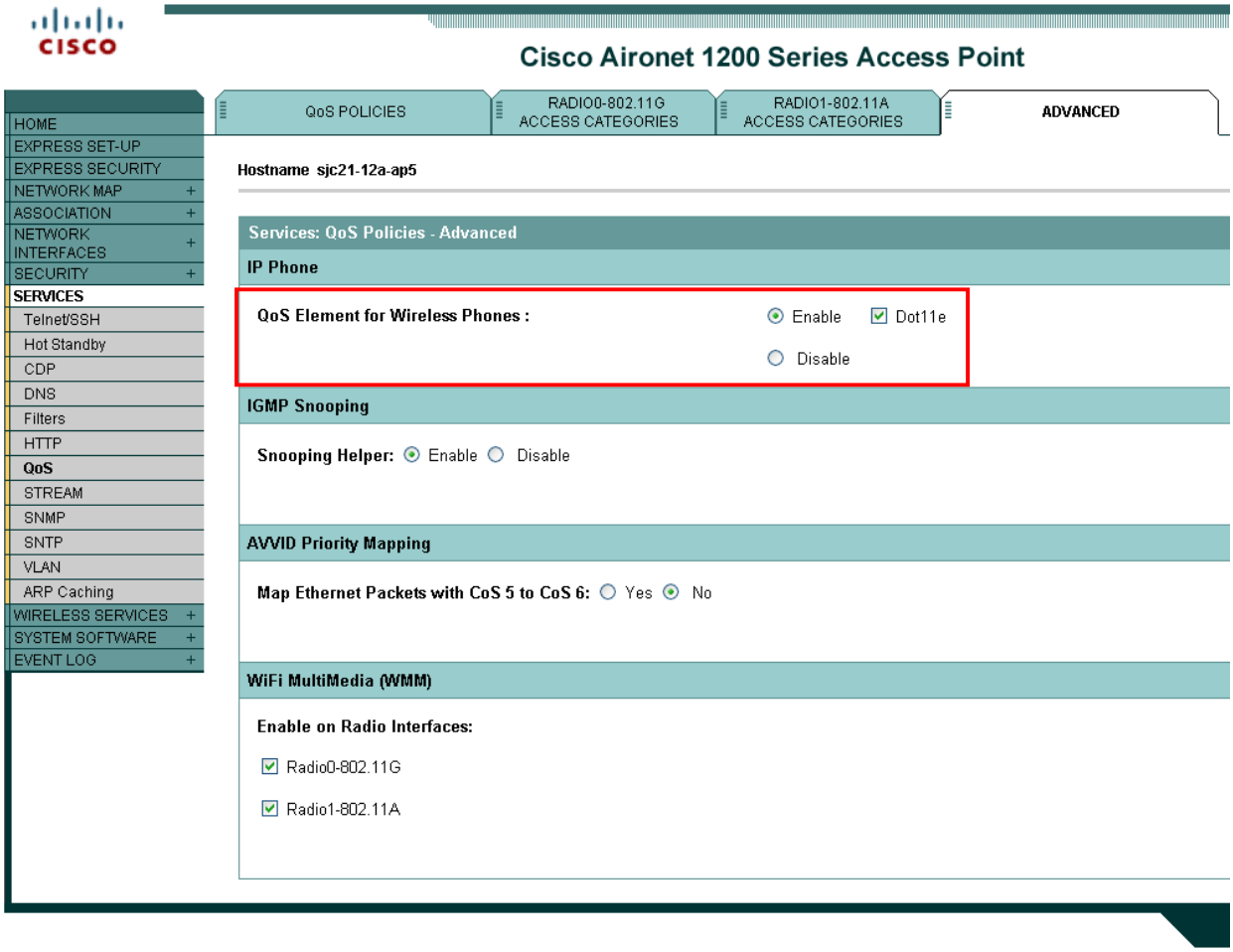
The second version from Cisco is based on the 802.11e version, but allows the default max threshold of 105 to be optionally configured.

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**.



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>**

CCKM Timestamp Tolerance

As of the 7.0.98.218 release, the CCKM timestamp tolerance is configurable.

In previous releases, the CCKM timestamp tolerance was set to 1000 ms and non-configurable.

The default CCKM timestamp tolerance is still set to 1000 ms in the later releases.

It is recommended to adjust the CCKM timestamp tolerance to 5000 ms to optimize the Cisco Unified Wireless IP Phone 7921G roaming experience.

(Cisco Controller) >config wlan security wpa akm cckm timestamp-tolerance ?

<tolerance> Allow CCKM IE time-stamp tolerance <1000 to 5000> milliseconds; Default tolerance 1000 msecs

Use the following command to configure the CCKM timestamp tolerance per Cisco recommendations.

(Cisco Controller) >config wlan security wpa akm cckm timestamp-tolerance 5000 <WLAN id >

To confirm the change, enter **show wlan <WLAN id>**, where the following will be displayed.

CCKM tsf Tolerance..... **5000**

Auto-Immune

The Auto-Immune feature can optionally be enabled for protection against denial of service (DoS) attacks.

Although when this feature is enabled there can be interruptions introduced with voice over wireless LAN, therefore it is recommended to disable the Auto-Immune feature on the Cisco Unified Wireless LAN Controller.

The Auto-Immune feature was introduced in the 4.2.176.0 release, which was enabled by default and non-configurable.

As of the 4.2.207.0, 5.2.193.0 and 6.0.182.0 releases this feature is disabled by default but can be enabled optionally.

To view the Auto-Immune configuration on the Cisco Unified Wireless LAN Controller, telnet or SSH to the controller and enter the following command.

(Cisco Controller) >show wps summary

Auto-Immune

Auto-Immune..... **Disabled**

Client Exclusion Policy

Excessive 802.11-association failures..... Enabled

Excessive 802.11-authentication failures..... Enabled

Excessive 802.1x-authentication..... Enabled

IP-theft..... Enabled

Excessive Web authentication failure..... Enabled

Signature Policy

Signature Processing..... Enabled

To disable the Auto-Immune feature on the Cisco Unified Wireless LAN Controller, telnet or SSH to the controller and enter the following command.

(Cisco Controller) >config wps auto-immune disable

WLAN Controller Advanced EAP Settings

Need to ensure that the advanced EAP settings in the Cisco Unified Wireless LAN Controller are configured per the information below.

To view the EAP configuration on the Cisco Unified Wireless LAN Controller, telnet or SSH to the controller and enter the following command.

```
(Cisco Controller) >show advanced eap
    EAP-Identity-Request Timeout (seconds)..... 30
    EAP-Identity-Request Max Retries..... 2
    EAP Key-Index for Dynamic WEP..... 0
    EAP Max-Login Ignore Identity Response..... enable
    EAP-Request Timeout (seconds)..... 30
    EAP-Request Max Retries..... 2
    EAPOL-Key Timeout (milliseconds)..... 400
    EAPOL-Key Max Retries..... 4
```

If using 802.1x or WPA/WPA2, the EAP-Request Timeout on the Cisco Unified Wireless LAN Controller should be set to at least 20 seconds.

In later versions of Cisco Unified Wireless LAN Controller software, the default EAP-Request Timeout was changed from 2 to 30 seconds.

The default timeout on the Cisco ACS server is 20 seconds.

To change the EAP-Request 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 30
```

If using WPA/WPA2 PSK then it is recommended to reduce the EAPOL-Key Timeout to 400 milliseconds from the default of 1000 milliseconds with EAPOL-Key Max Retries set to 4 from the default of 2.

If using WPA/WPA2, then using the default values where the EAPOL-Key Timeout is set to 1000 milliseconds and EAPOL-Key Max Retries are set to 2 should work fine, but is still recommended to set those values to 400 and 4 respectively.

The EAPOL-Key Timeout should not exceed 1 second (1000 milliseconds).

To change the EAPOL-Key Timeout on the Cisco Unified Wireless LAN Controller, telnet or SSH to the controller and enter the following command.

```
(Cisco Controller) >config advanced eap eapol-key-timeout 400
```

To change the EAPOL-Key Max Retries Timeout on the Cisco Unified Wireless LAN Controller, telnet or SSH to the controller and enter the following command.

```
(Cisco Controller) >config advanced eap eapol-key-retries 4
```

Proxy ARP

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

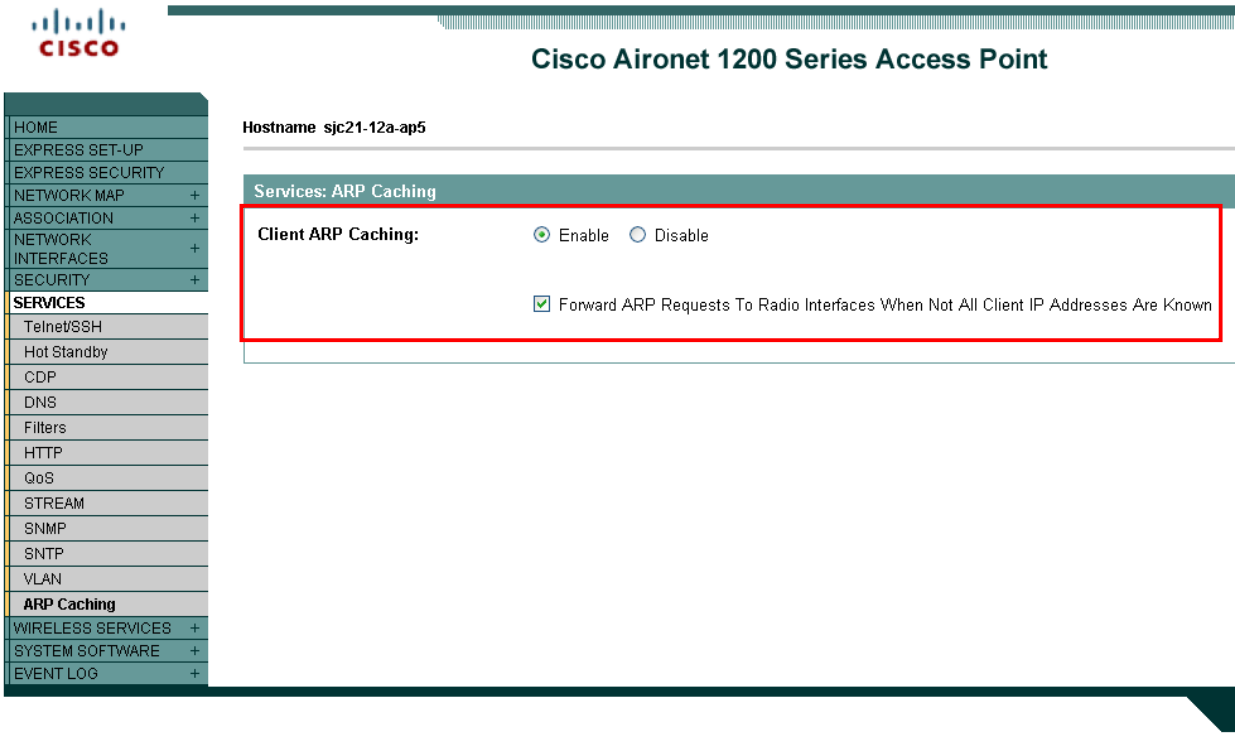
Ensure proxy ARP is enabled, where ARP Unicast Mode will be displayed as disabled on the Cisco Unified Wireless LAN Controller.

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**.

As of the 5.1.151.0 release, proxy ARP is always enabled and non-configurable.

For Cisco Autonomous Access Points, enter **dot11 arp-cache optional**.



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>

To confirm the change, enter **show wlan <WLAN id>**, where the following will be displayed.

Tkip MIC Countermeasure Hold-down Timer..... 60

For the Cisco 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>
```

VLANs and Cisco Autonomous Access Points

Segment wireless voice and data into separate VLANs.

A subnet for wireless clients should not exceed 1,000 hosts.

When using Cisco Autonomous Access Points, use a dedicated native VLAN. The Cisco Autonomous Access Points utilize Inter-Access Point Protocol (IAPP), which is a multicast protocol.

For the native VLAN, it is recommended not to use VLAN 1 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.

Port security should be disabled on switch ports that Cisco Autonomous Access Points are directly connected to.

The network ID in the SSID configuration the Cisco Autonomous Access Point 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 various methods for configuring network settings on the Cisco Unified Wireless IP Phone 7921G.

Configuring Phones with the Keypad

The network profiles can be configured by navigating to **Settings > Network Profiles**.

It may be required 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

Configuring Phones with the Web Interface

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

A PC running Microsoft Windows 7® 64 bit, Windows 7® 32 bit, Windows XP 32® bit or Windows 2000® 32 bit is required to utilize the USB interface on the Cisco Unified Wireless IP Phone 7921G.

If using USB, then set a static IP on the PC's USB network interface (e.g. 192.168.1.X /24).

In order to make configuration changes via the web interface, then web access must be set to **Full**, which will also enable a few additional menus.

Log into the administration web pages by using these defaults:
username = **admin** / password = **Cisco**

The USB driver installation packages for Microsoft Windows 7 64 bit, Windows 7 32 bit, Windows XP 32 bit, and Windows 2000 32 bit are available for download at the following URL.

http://software.cisco.com/download/navigator.html?mdfid=278875240

Note: It is not recommended to use the 192.168.1.0 /24 network for the wireless LAN interface as that network is used by the USB interface by default. If wanting to use the 192.168.1.0 /24 network for the wireless LAN, then either change the USB IP address on the phone or do not charge the phone via USB.

Configuring Phones with the Bulk Deployment Utility

The Bulk Deployment Utility (BDU) for the Cisco Unified Wireless IP Phone 7921G is intended to help quicken the provisioning and deployment process of many phones when unique 802.1x accounts are used with EAP-FAST, PEAP-MSCHAPv2 or LEAP or if a common set of credentials are used by all phones (e.g. WPA2-PSK or a common 802.1x account).

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 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

Wireless LAN Settings

Use the following guidelines to configure network profiles.

- The Cisco Unified Wireless IP Phone 7921G supports multiple network profiles that allow one SSID per network profile. 0 length SSIDs are not allowed.
- 5 different 802.11 modes are available.
    - Auto-RSSI
    - 802.11a
    - 802.11b/g
    - Auto-A
    - Auto-b/g
- As of the 1.3(3) release, Auto-a is the default 802.11 mode, so it will scan both channels and attempt to on the 5 GHz band if the configured network is available.
- In previous releases, the Cisco Unified Wireless IP Phone 7921G would default to Auto-RSSI mode, which would attempt to associate to the access point with the strongest signal.
- 802.11a mode will only scan 5 GHz channels and 802.11b/g mode will only scan 2.4 GHz channels, where it will then attempt to associate to an access point if the configured network is available.

- For Auto-a and Auto-b/g modes, this is giving preference to one frequency band over another. At power on, will scan all 2.4 GHz and 5 GHz channels then attempt to associate to an access point for the configured network using the preferred frequency band if available. If the preferred frequency band is not available, then the Cisco Unified Wireless Phone 7921G will try to use the less preferred frequency band if available. If the phone roams out of coverage of the preferred frequency band, where the less preferred frequency band signal is available, then the phone will attempt to associate to that less preferred frequency band.
- To optimize battery life, ensure the call power save mode is configured for U-APSD/PS-POLL mode to utilize power save mode during active calls.
- Active mode (**Call Power Save Mode** set to **None**) may need to be used instead of U-APSD/PS-POLL if the access point does not support power save enabled clients.
- As of the 1.3(3) release, the Prompt Mode feature can be optionally enabled. When enabled, the password will not be stored in flash, but only in memory after entering manually after each power on sequence for seamless roaming. However, the username can be stored after entering at the prompt, but can be overridden at the next login. If the prompt is dismissed, then there is a **"Login"** softkey presented in order to invoke the login process. The Prompt Mode feature is only supported with Network Profile 1. If multiple network profiles are enabled and Prompt Mode is enabled, then the user would have to dismiss the login in order to switch to other enabled network profiles.
- Below are the available security modes supported and the key management and encryption types can be used for each mode.

Security Mode	Key Management	Encryption
Open	N/A	N/A
Open+WEP	Static	WEP (40/64 or 104/128 bit)
Shared+WEP	Static	WEP (40/64 or 104/128 bit)
LEAP	802.1x, WPA, WPA2	TKIP, AES, WEP (40/64 or 104/128 bit)
EAP-FAST	802.1x, WPA, WPA2	TKIP, AES, WEP (40/64 or 104/128 bit)
EAP-TLS	802.1x, WPA, WPA2	TKIP, AES, WEP (40/64 or 104/128 bit)
PEAP	802.1x, WPA, WPA2	TKIP, AES, WEP (40/64 or 104/128 bit)
AKM	802.1x, WPA, WPA2, WPA-PSK, WPA2-PSK	TKIP, AES, WEP (40/64 or 104/128 bit)

- Open with WEP and Shared Key security modes require that the static WEP settings be entered.

Key Style	Key Size	Characters
ASCII	40/64	5
ASCII	104/128	13
HEX	40/64	10 (0-9, A-F)
HEX	104/128	26 (0-9, A-F)

- The AKM security mode is an auto authentication mode that can use either LEAP for 802.1x authentication or WPA Pre-Shared Key.

- If using 802.11i (Pre-Shared key), enter the ASCII or hexadecimal formatted key.

  Pre-Shared Key requires that a passphrase be entered in ASCII or hexadecimal format.

Key Style	Characters
ASCII	8-63
HEX	64 (0-9,A-F)

- 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 open authentication plus WEP encryption or shared key authentication, enter the static WEP key information that matches the access point configuration.

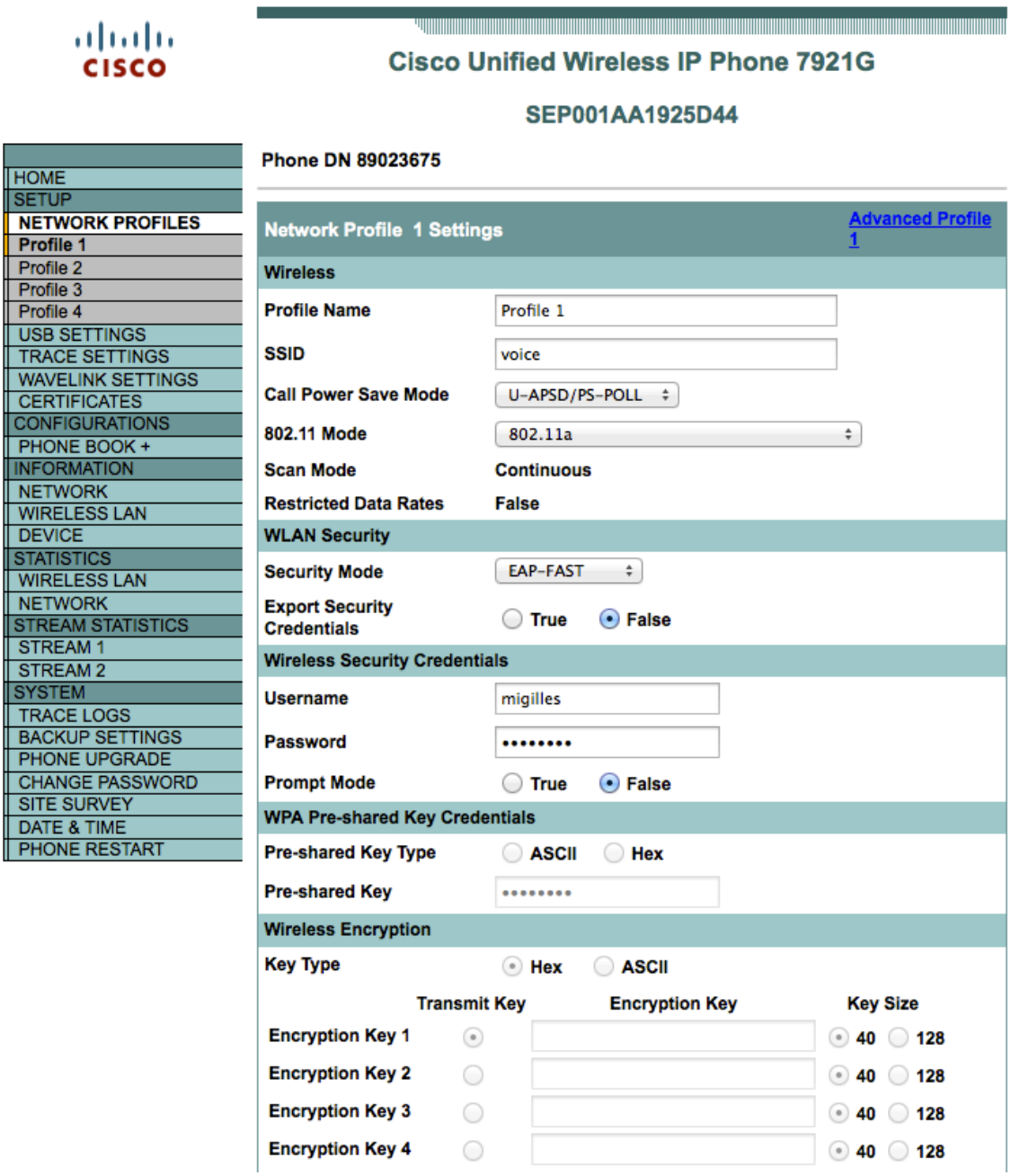
Note: CCKM will be negotiated if enabled on the access point when using 802.1x authentication with LEAP, EAP-FAST, EAP-TLS, PEAP or AKM modes.

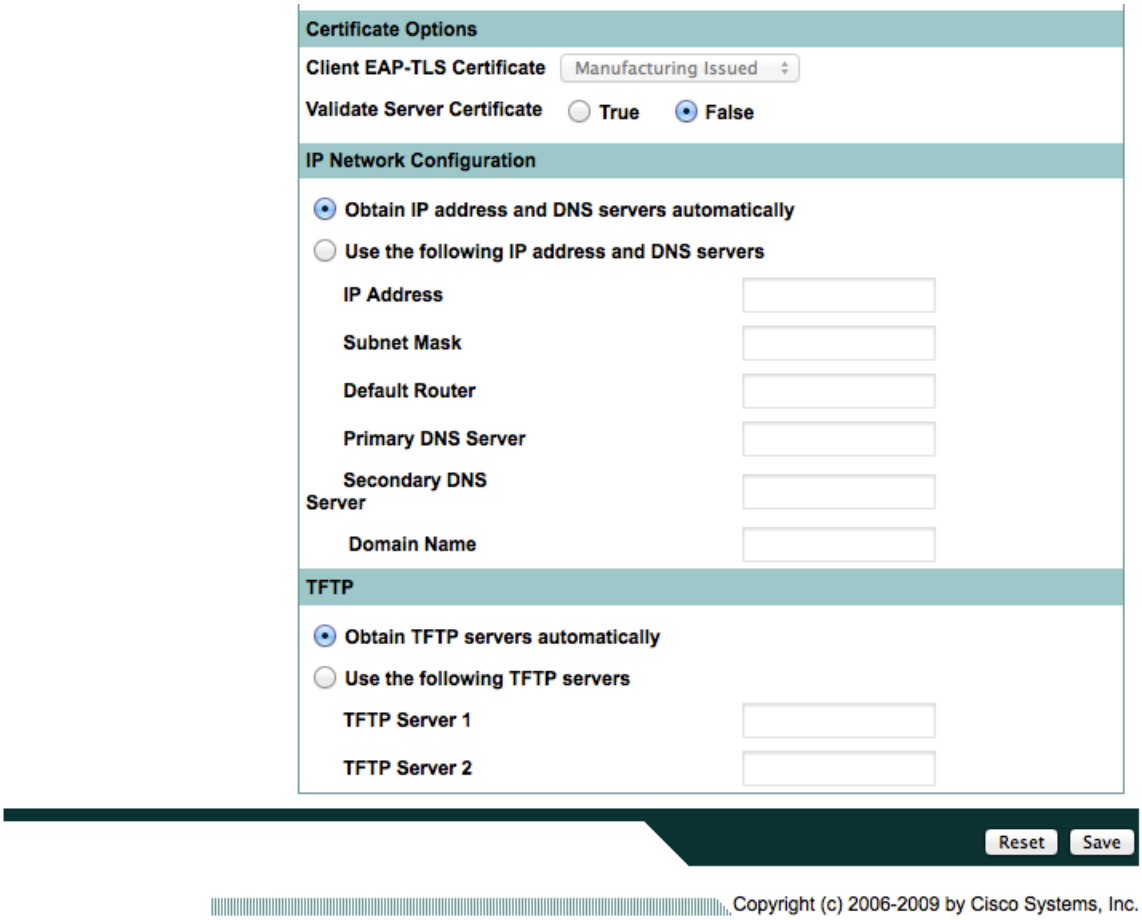
WEP with AKM is only applicable with 802.1x authentication (not WPA-PSK/WPA2-PSK).

If using 802.1x authentication via LEAP, EAP-FAST, PEAP or AKM (authenticated key-management) authentication modes, then a username and password must be configured. AKM mode will use LEAP as the 802.1x method.

- 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
SEP001AA1925D44
Phone DN 89023675
HOME
SETUP
NETWORK PROFILES
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 Settings
Advanced Profile 1
Wireless
Profile Name
Profile 1
SSID
voice
Call Power Save Mode
U-APSD/PS-POLL
802.11 Mode
802.11a
Scan Mode
Continuous
Restricted Data Rates
False
WLAN Security
Security Mode
EAP-FAST
Export Security Credentials
True
False
Wireless Security Credentials
Username
migilles
Password
Prompt Mode
True
False
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
40
128
Encryption Key 2
40
128
Encryption Key 3
40
128
Encryption Key 4
40
128



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, the minimum PHY rate can be adjusted. If 12 Mbps is not enabled in the wireless LAN, then this parameter may need to be configured or enable 12 Mbps on the access point.

Antenna diversity can be configured as necessary.

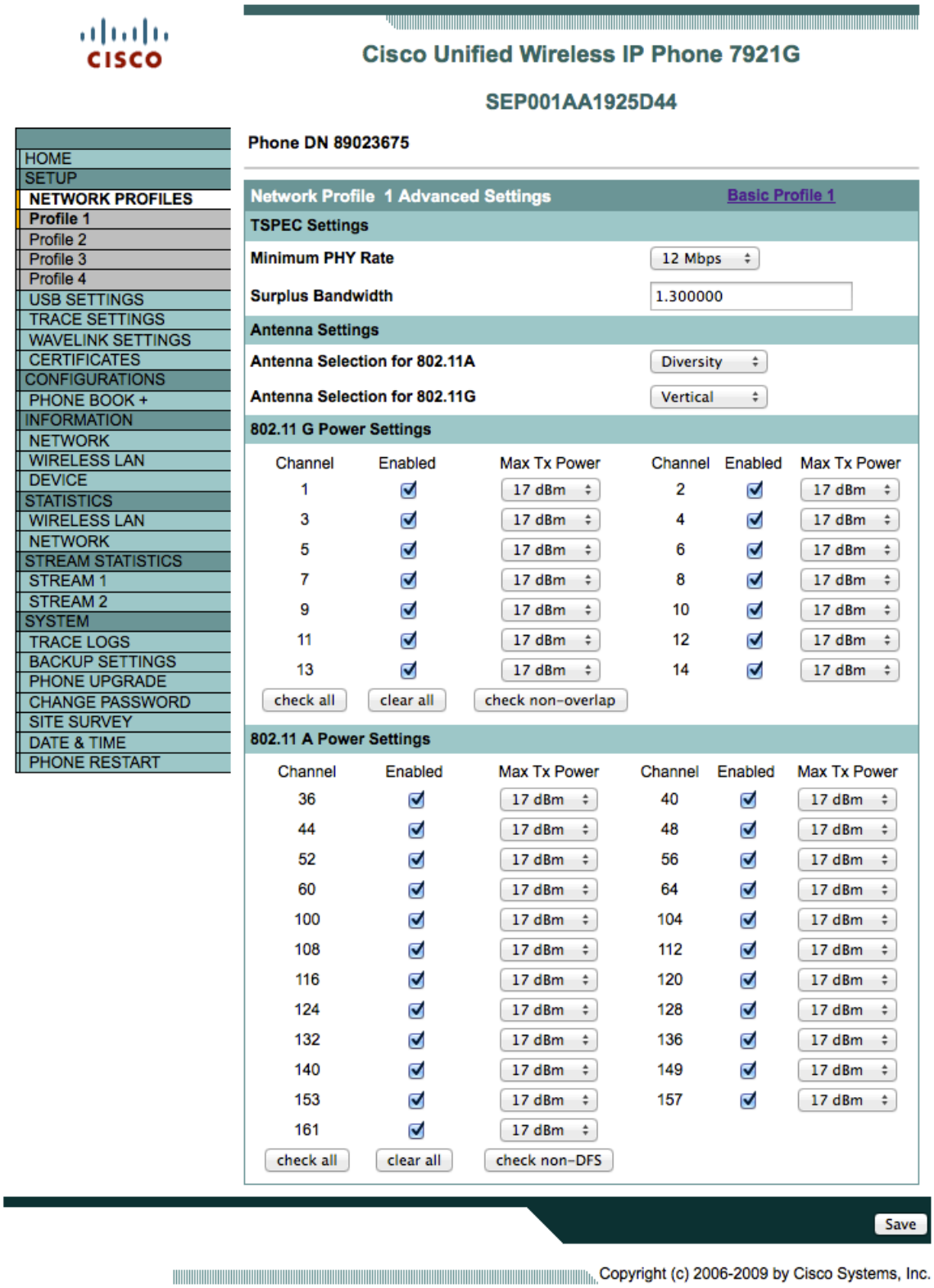
The channels enabled for scanning can also be managed in the Advanced Network Profile settings.

By limiting number of channels to be scanned, this can potentially reduce the time for access point discovery.

If planning to manage the enabled channels, then only disable those channels that are not used in the wireless LAN then restart the Cisco Unified Wireless IP Phone 7921G via the Phone Restart option on the webpage. If a channel is disabled that is currently used by an access point, then the Cisco Unified Wireless IP Phone 7921G might not be able to associate to the wireless LAN successfully.

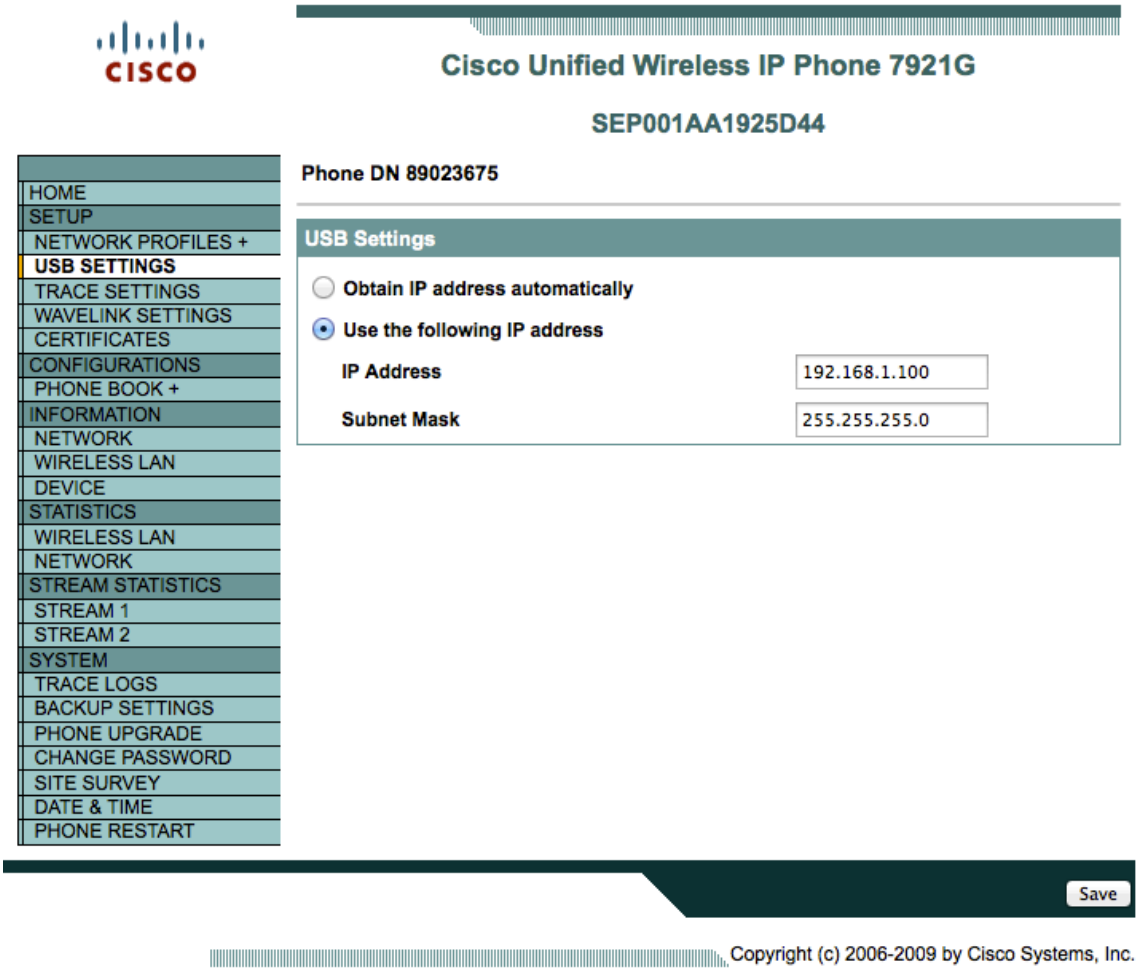
If all channels that are used in the wireless LAN are disabled on the phone, then use one of these methods to browse to the Cisco Unified Wireless IP Phone 7921G webpage and re-enable the necessary channels:

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



USB Settings

By default, the USB interface USB of the Cisco Unified Wireless IP Phone 7921G is statically set to 192.168.1.100 /24, but can be changed as necessary.



Installing Certificates

The Cisco Unified Wireless IP Phone 7921G supports DER encoded binary X.509 certificates, which can be utilized with EAP-TLS or for authentication server validation when using PEAP-MSCHAPv2.

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

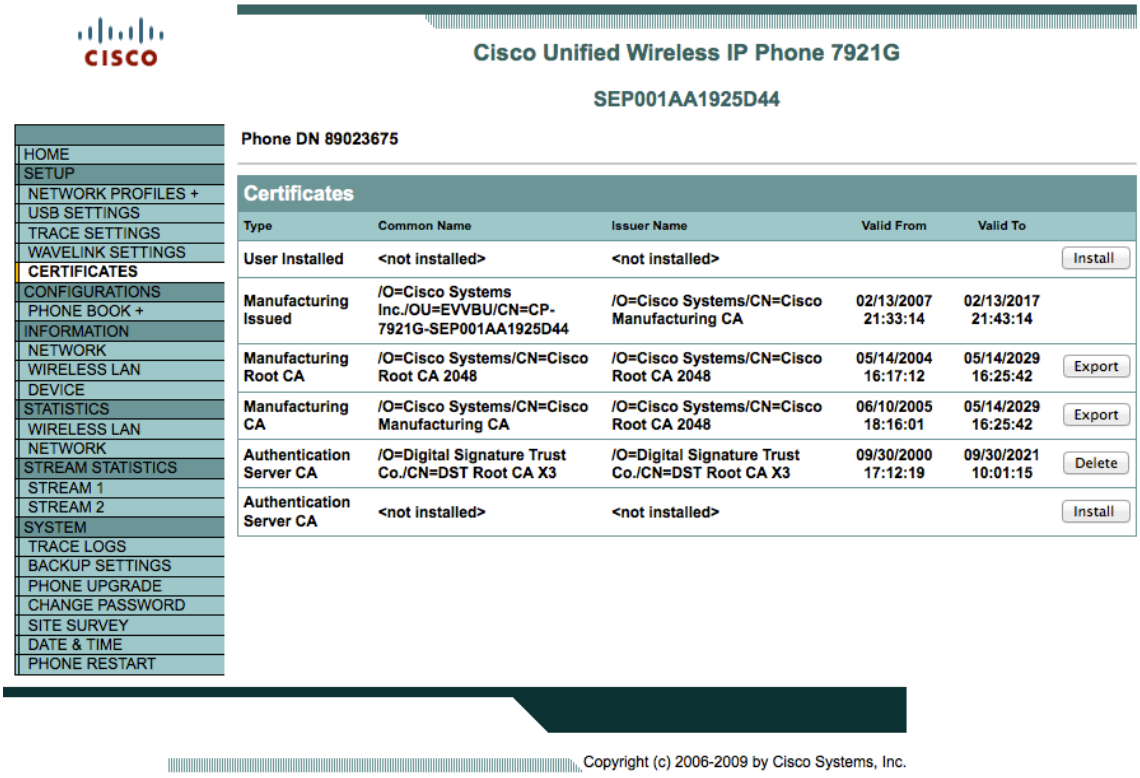
TLS provides a way to use certificates for both user and server authentication and for dynamic session key generation.

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

Microsoft® Certificate Authority (CA) servers are recommended as we have certified interoperability only with those CA types. Other CA server types may not be completely interoperable with the Cisco Unified Wireless IP Phone 7921G.

Can utilize either the internal MIC (Manufacturing Installed Certificate) or install a User Installed 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.



After selecting **Export**, import the certificates into the RADIUS server and enable them in the Certificate Trust List (CTL).

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 (CA) server that is signing the certificate. The signing CA root certificate is used for validation purposes to ensure that the user certificate was indeed signed by the correct CA.

The Common Name defaults to a string including the MAC address of the Cisco Unified Wireless IP Phone 7921G (**CP-7921G-SEP<MAC_Address>)**, however the Common Name can be customized to a string with up to 32 characters.

Some special characters (e.g. **! @ # $ % ^ & * _ [ ] { } \ | ; “ < > ` ~**) are not supported for the Common Name.

Organization, Organization Unit, City, and State fields can support up to 64 characters.

Browse to the Certificate Authority certificate that will be signing the user certificate then select **Submit**.

If using a CA configuration where one or more intermediate servers exist, ensure you upload the correct CA server certificate as this certificate will be used to validate whether the user certificate was signed by the intended CA or not.

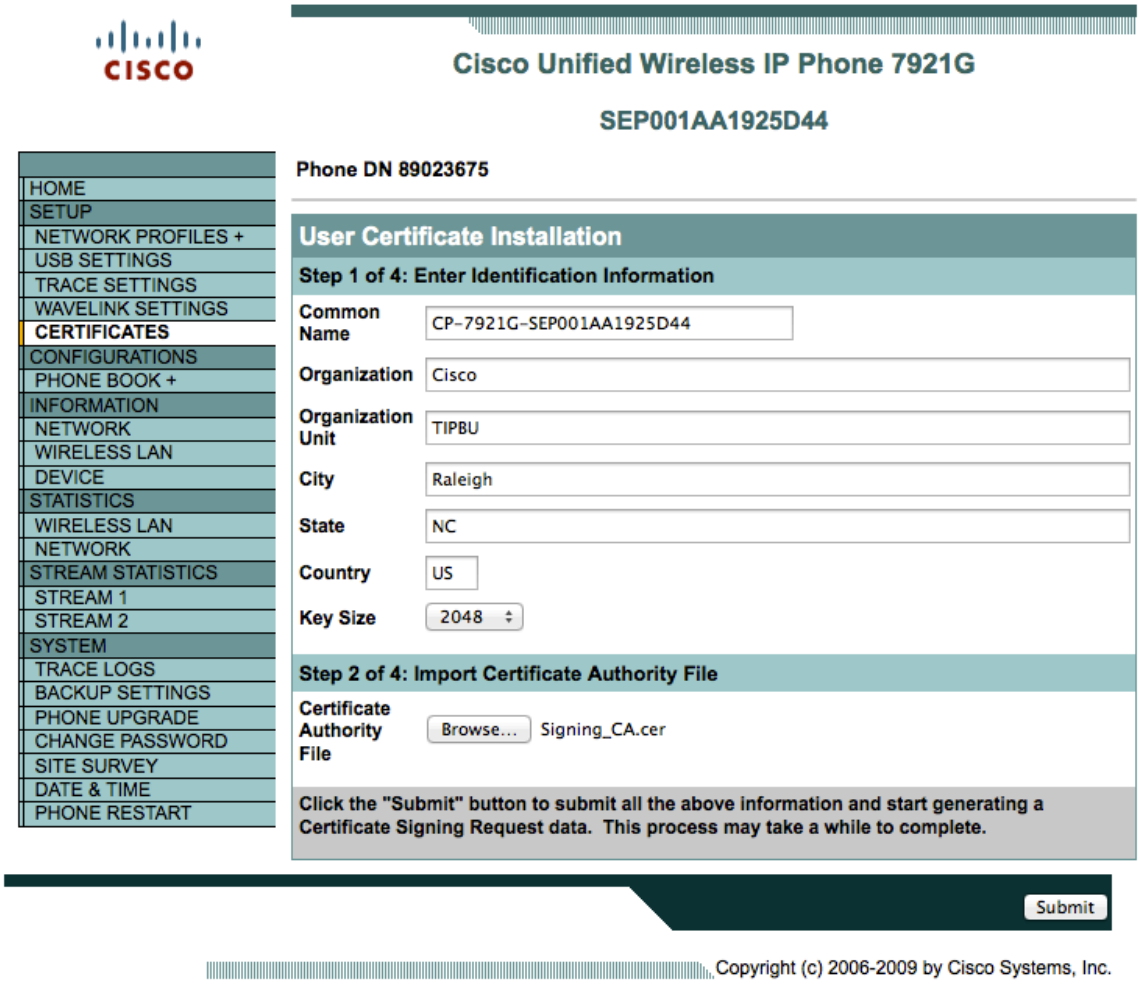
Ensure that the signing CA server certificate uploaded is in DER format.

Only certificates with a key size of 1024 or 2048 are supported.

Ensure the CA server certificate is signed using the SHA-1 algorithm as the SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512) and SHA-3 signature algorithms are not supported.

Certificates dated January 1 2038 and later are not supported.

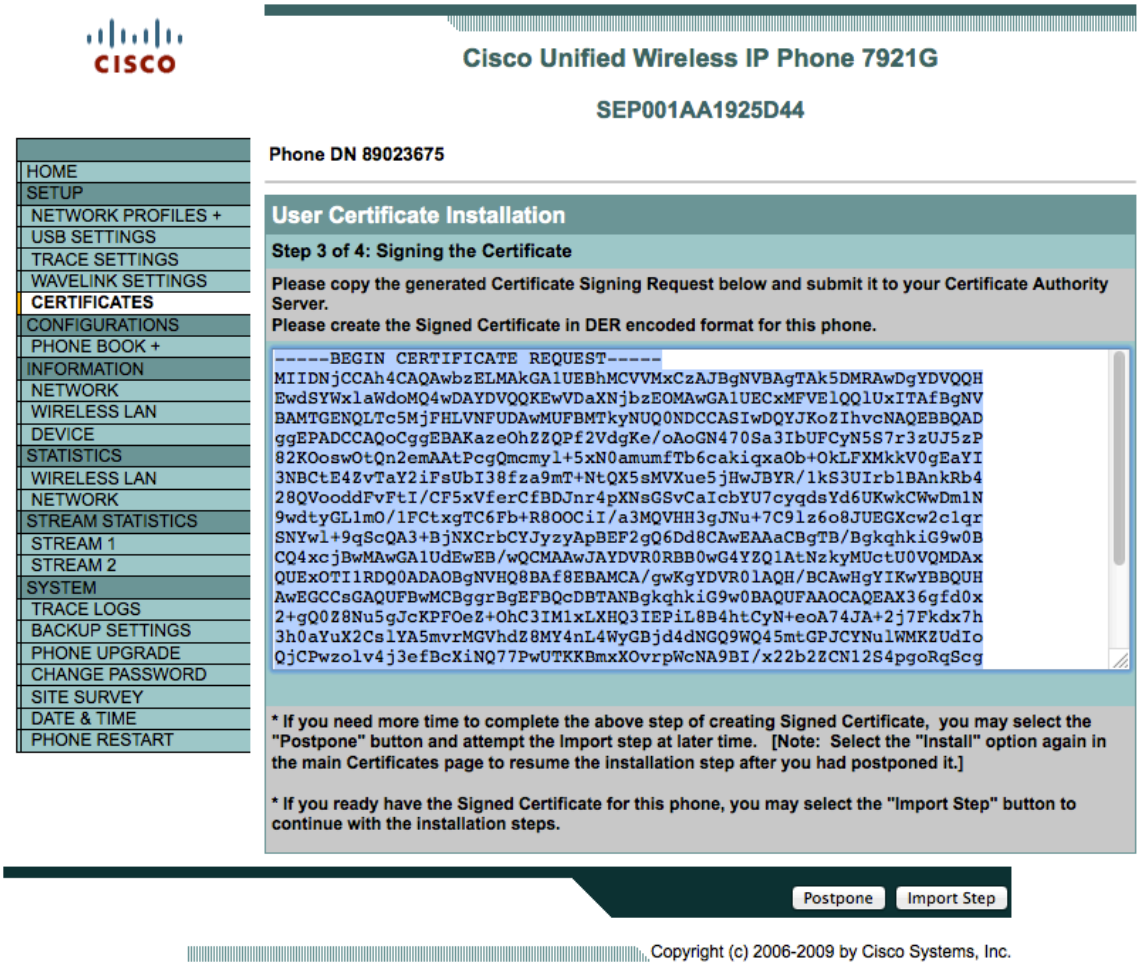
Additional extensions in the CA server certificate such as information for certificate renewal and Certificate Revocation List (CRL) are not supported and can lead to certificate installation failures.



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

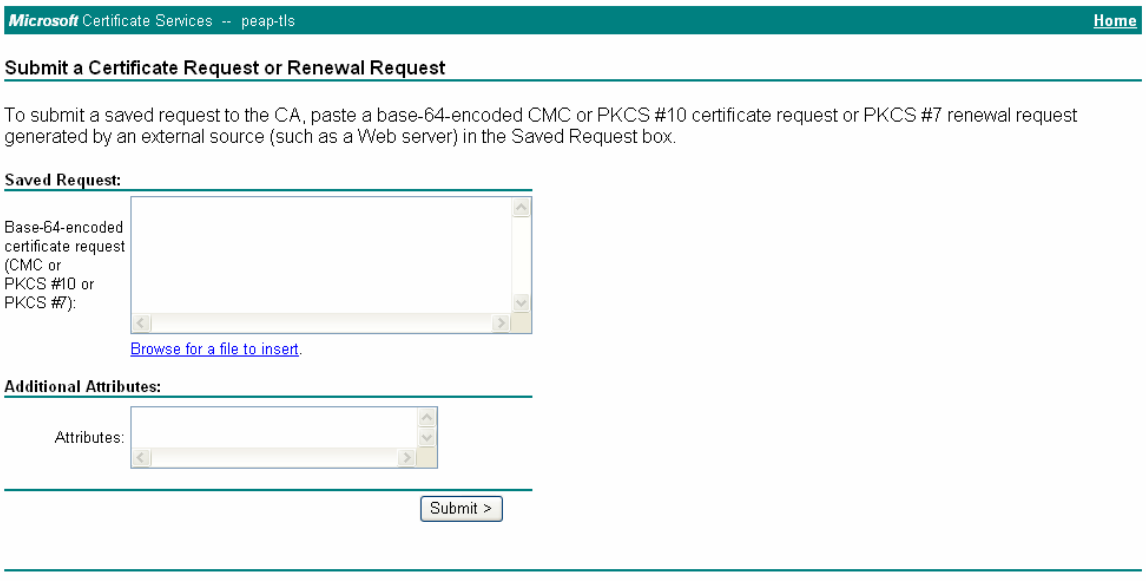
The user certificate will then be displayed and is now ready to be signed.

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



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

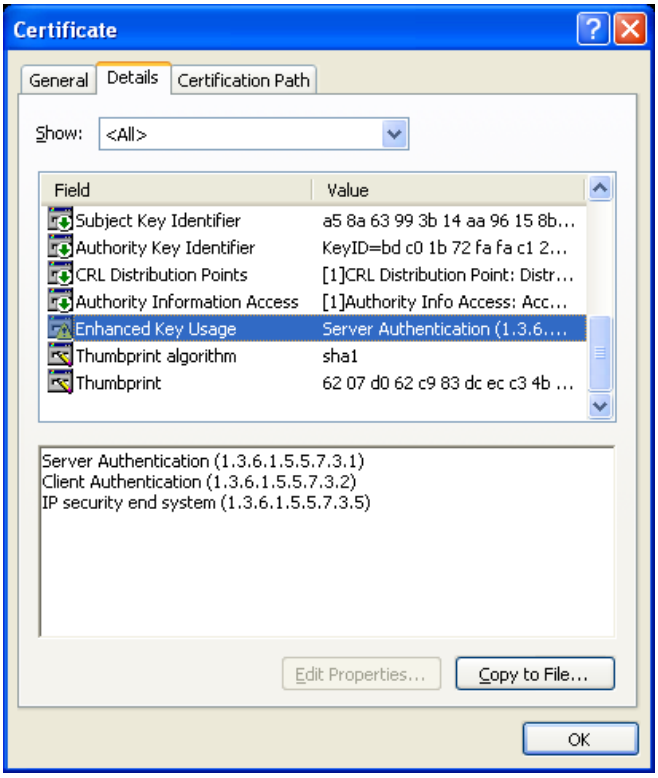
Paste the certificate data from the Cisco Unified Wireless IP Phone 7921G to the Certificate Authority signing server and submit for signing.



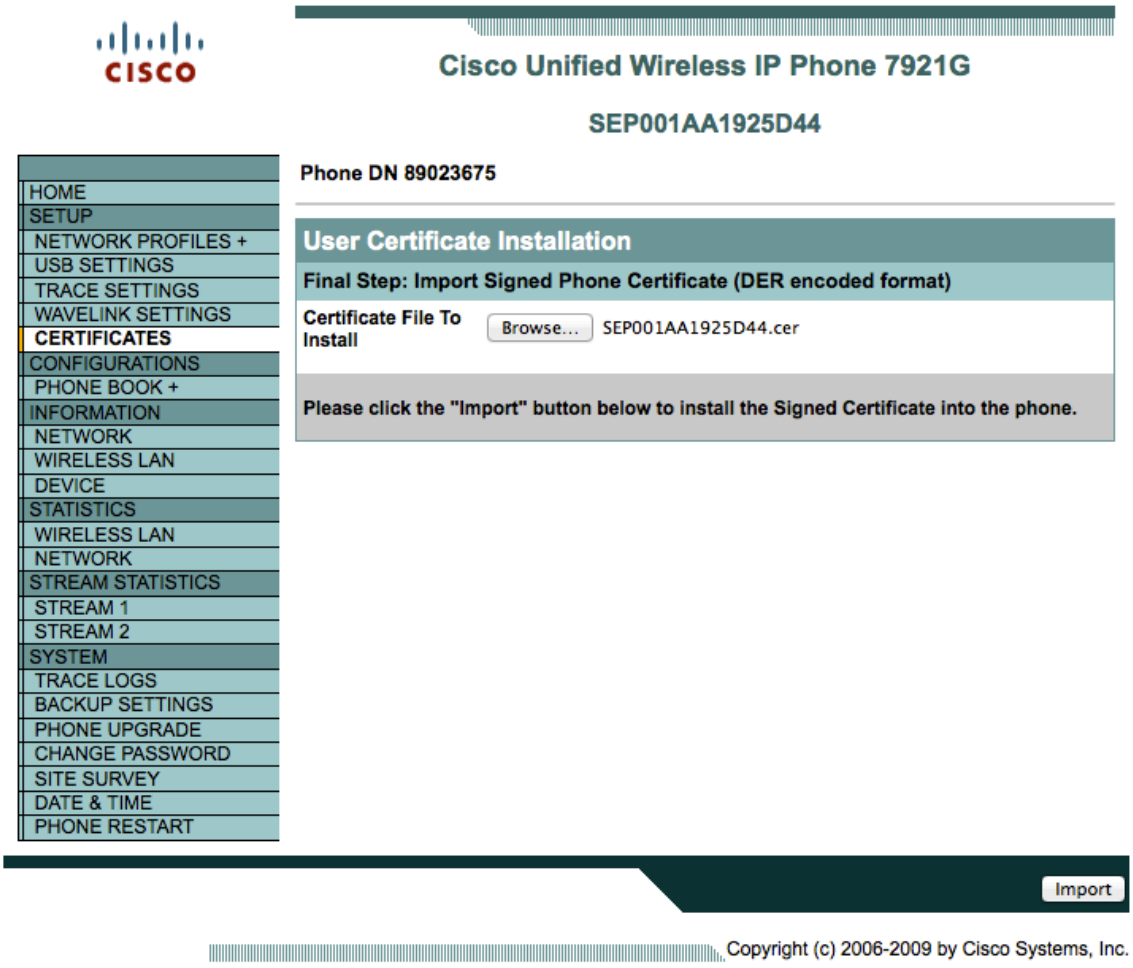
When the user certificate has been signed, download the CA certificate in DER encoded format (Base-64 encoded certificates are not supported).

Ensure the user certificate is signed using the SHA-1 algorithm as the SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512) and SHA-3 signature algorithms are not supported.

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



After selecting **Import Step**, browse to the signed user certificate then select **Import** to complete the process.



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

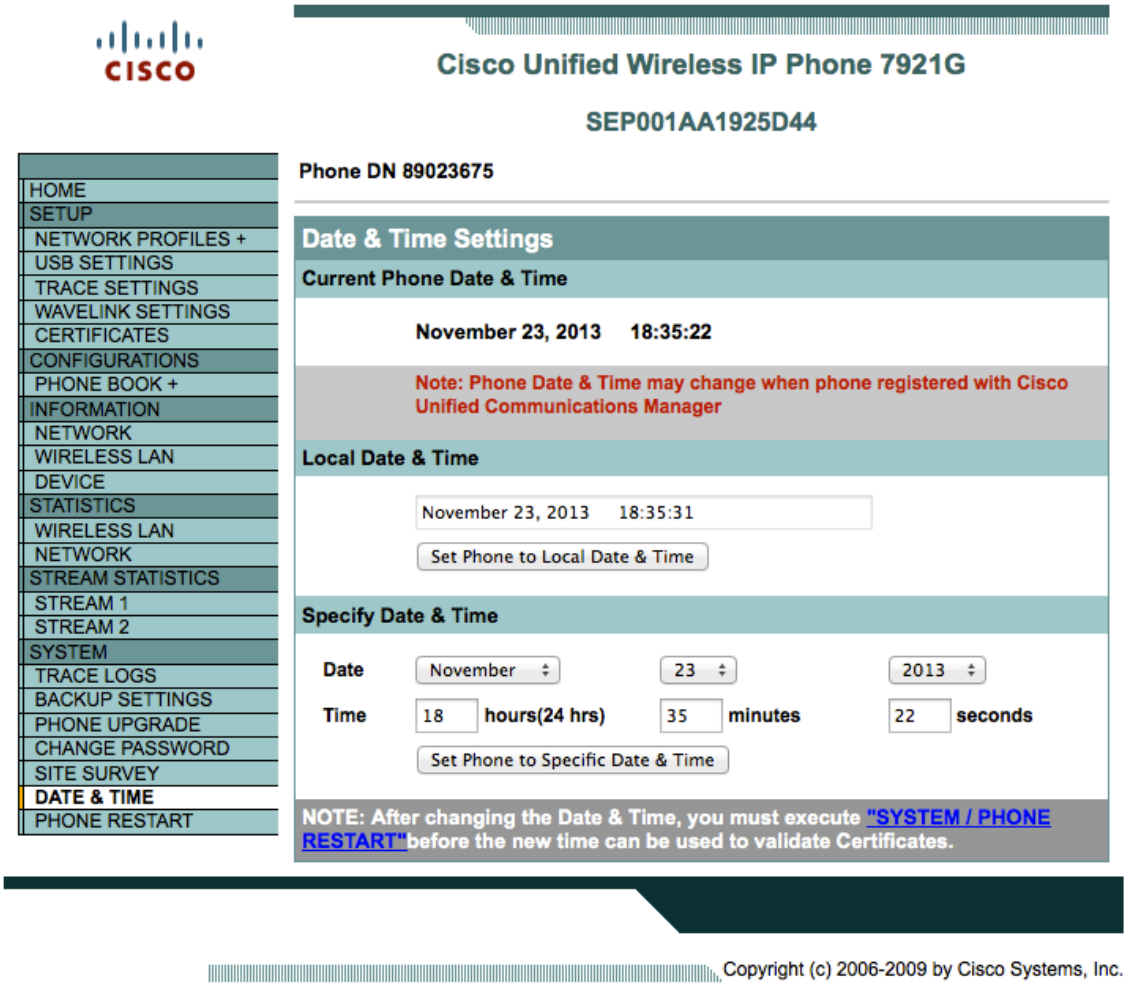
The CA chain should already be enabled in the authentication server's certificate trust list.

The authentication server certificate must also be imported into the Cisco Unified Wireless IP Phone 7921G for both the MIC and User Installed 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.

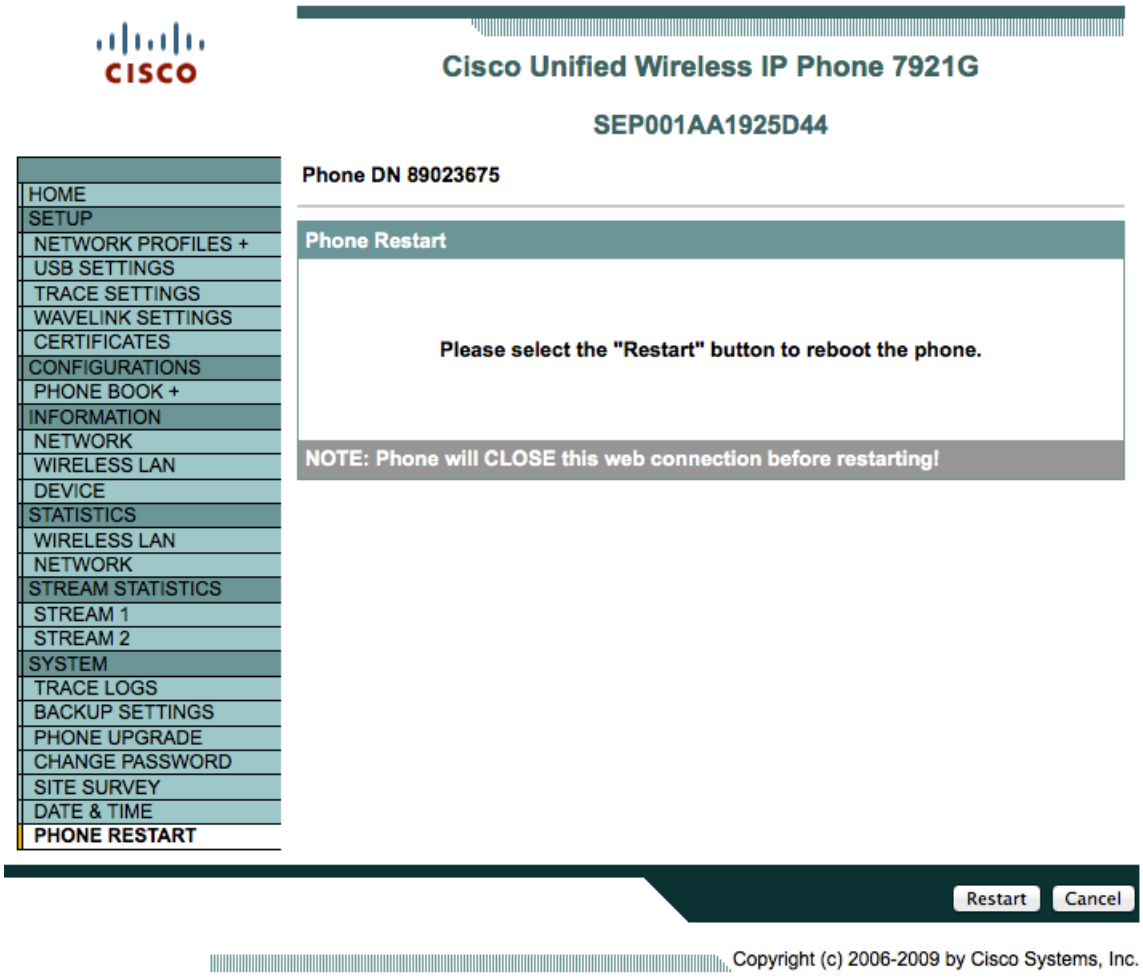
With 1.4(3)SR1 and earlier releases, the Cisco Unified Wireless IP Phone 7921G does not have timezone support, therefore a recently signed certificate may not be valid yet if the local time of the Cisco Unified Wireless IP Phone 7921G is west of Greenwich Mean Time (GMT).

As of the 1.4(4) release, timezone support has been added, which can allow newly issued certificates to be immediately used.



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.



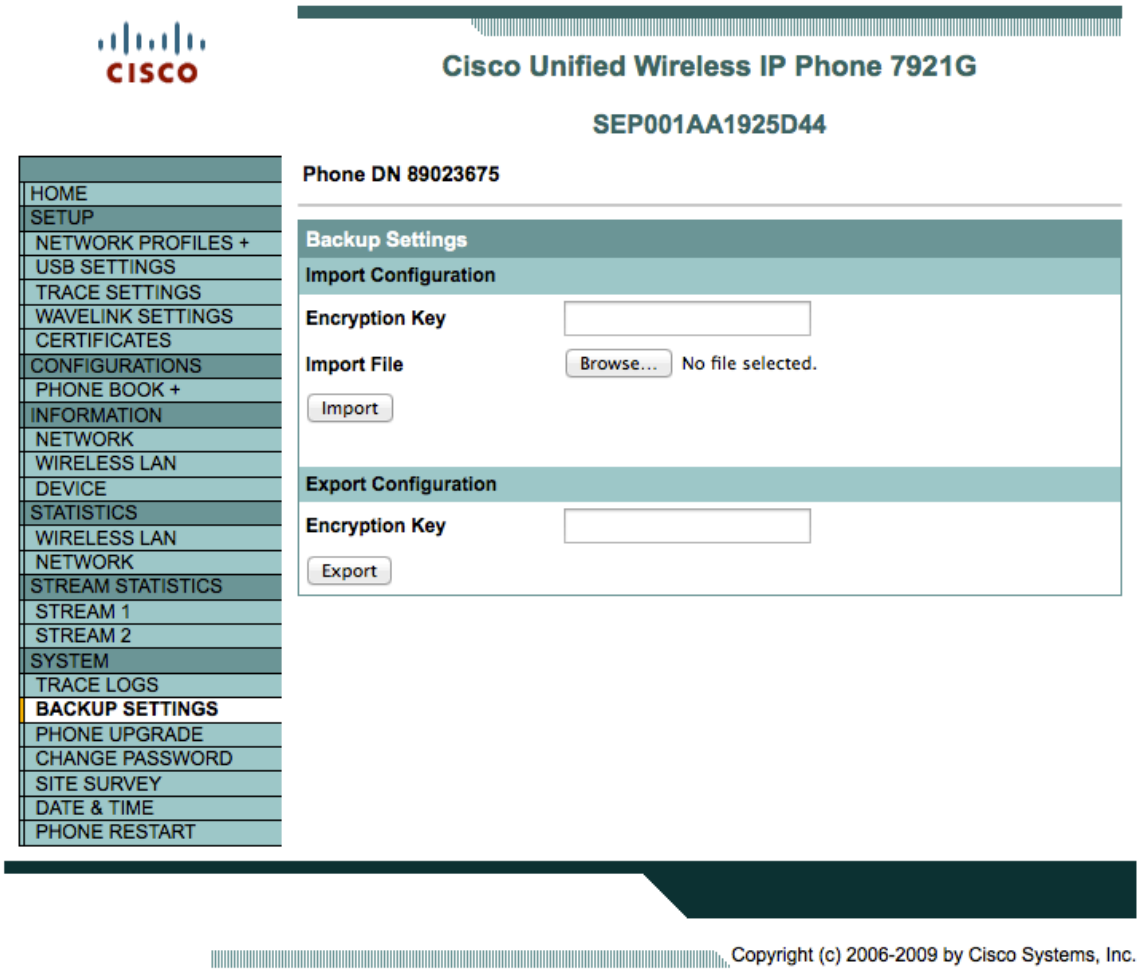
Click the **Restart** button to power cycle the phone.

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).

In order to access the Backup Settings menu, the web access must be set to **Full**.

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**, the Wireless LAN security information will need to be re-entered. This will then allow that information to be exported and then imported to other Cisco Unified Wireless IP Phone 7921G phones.



Using the Bulk Deployment Utility

The Bulk Deployment Utility (BDU) for the Cisco Unified Wireless IP Phone 7921G enables the creation of configuration files, which can be exported then enabled for TFTP download by the Cisco Unified Wireless IP Phone 7921G.

A personal computer running Microsoft Windows® is required.

The Bulk Deployment Utility requires firmware 1.3(4) or later on the Cisco Unified Wireless IP Phone 7921G.

This utility does not support certificate provisioning, which would be required in order to support server validation for PEAP or EAP-TLS.

The utility does allow PEAP to be configured, but without the server validation option.

The Bulk Deployment Utility supports up to **1000** entries per CSV for export. If more than 1000 phones are being deployed, then multiple CSV files will need to be created and imported.

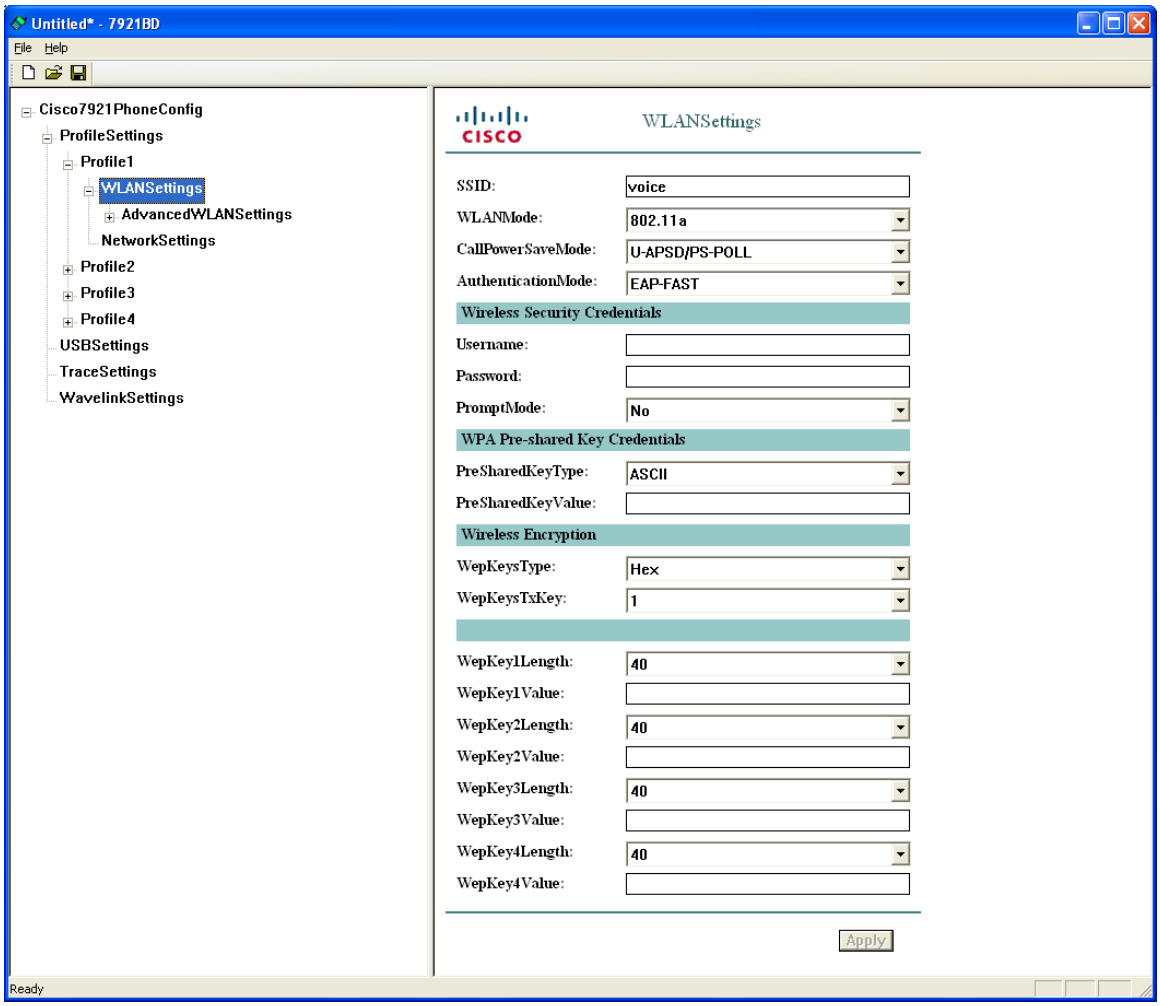
If doing a bulk export, the username and password is applied to network profile 1 only.

Before exporting the TFTP downloadable configuration files, a template must be created containing the Network Profile, USB, Trace, and Wavelink settings.

Configure the Profile Name as necessary.

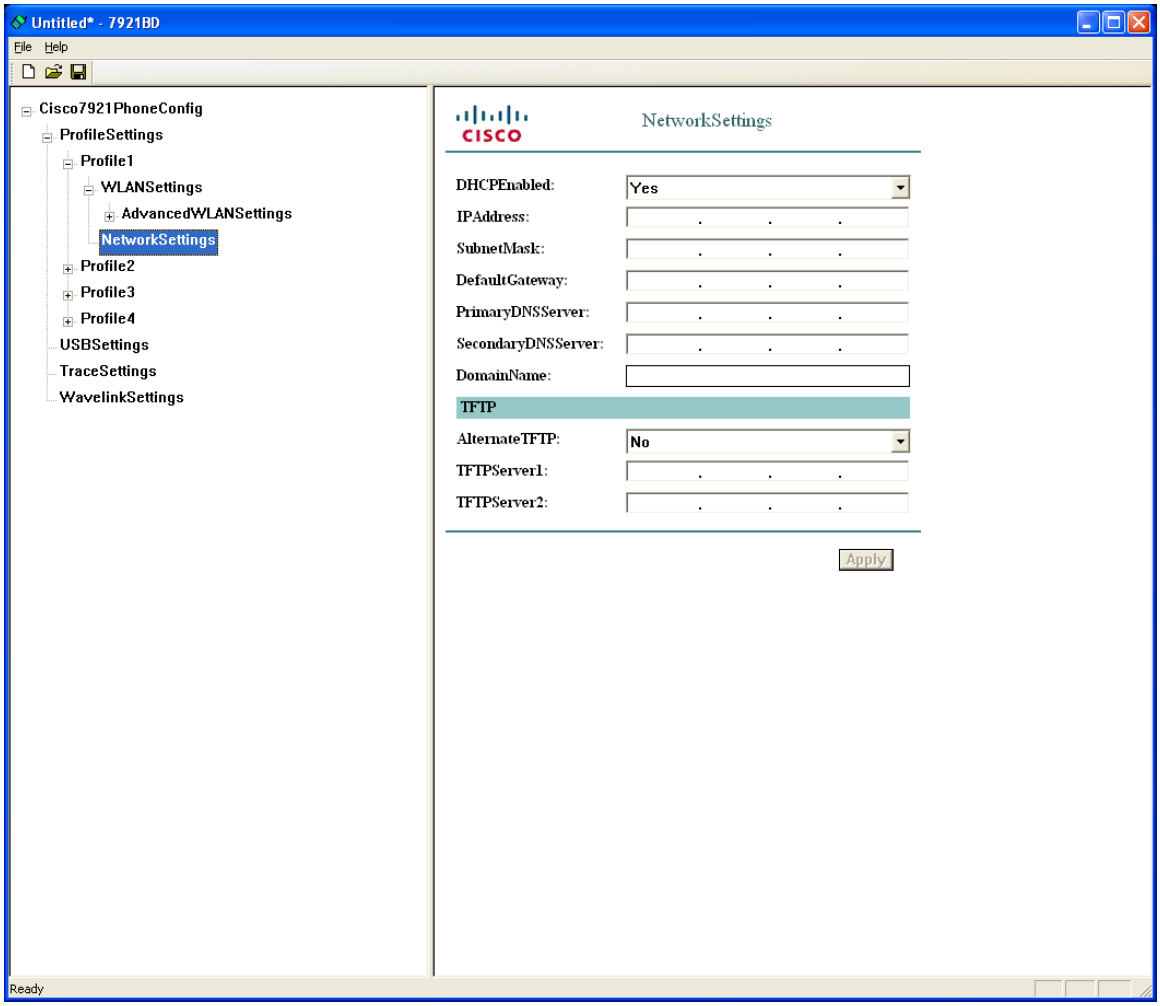
Configure the network profile WLAN settings (SSID, 802.11 mode, Security Mode, WLAN credentials) to match the WLAN that the Cisco Unified Wireless IP Phone 7921G will utilize.

If planning to use unique 802.1x accounts with the Bulk Export method, the username and password do not need to be configured, as that will be specified in the CSV file.



By default, DHCP is enabled and is the recommended method, otherwise would need a template per phone if planning to use static IP addressing.

An alternate TFTP server can be set if the Cisco Unified Communications Manager's TFTP server IP is not set in option 150 for the DHCP scope.



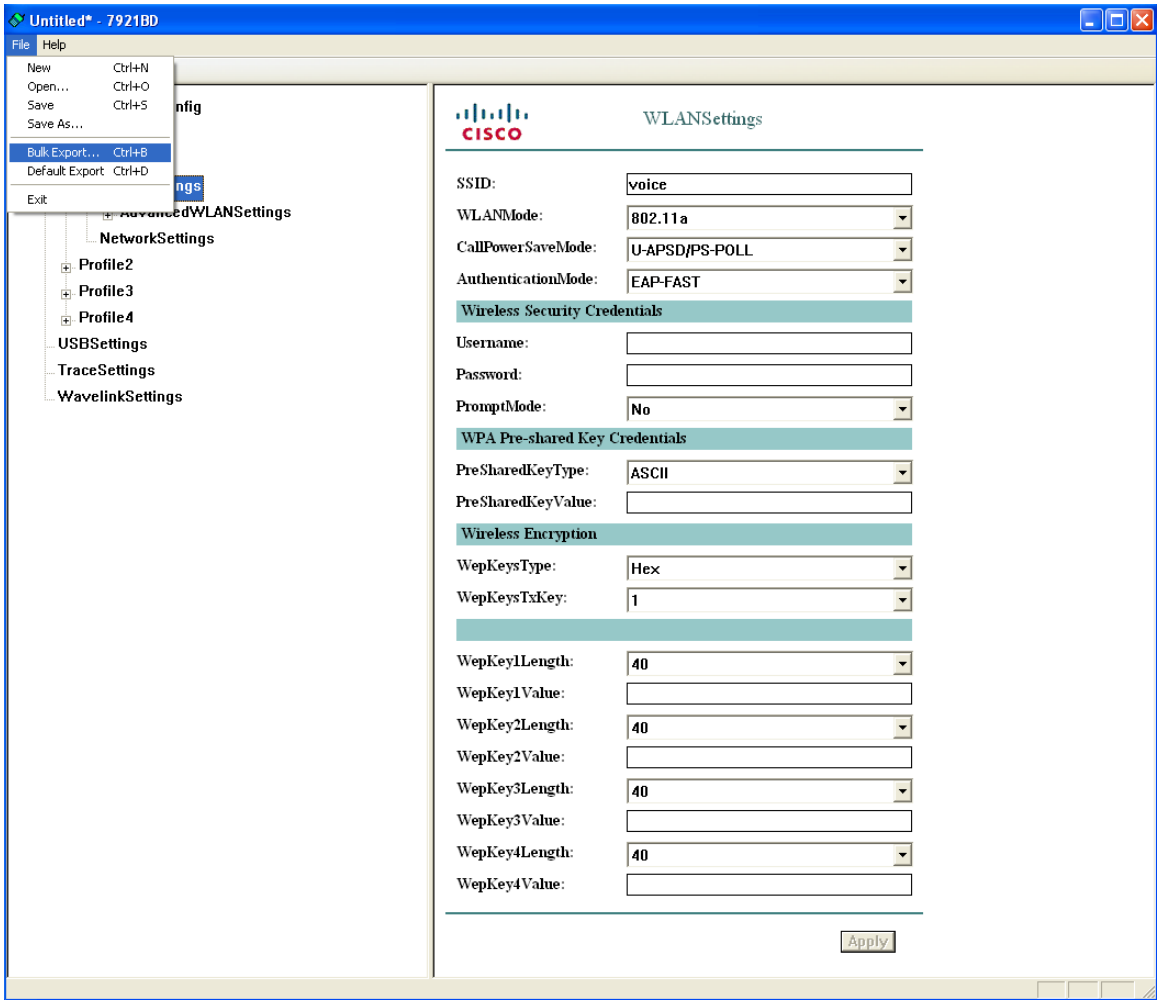
Templates can be created for later use, by selecting **File > Save As**.

Do not overwrite the **7921Cfg.xml** file, as that is the default template used when the utility opens.

Phone configuration files can be exported by either the **Default Export** method or the **Bulk Export** method.

If a common set of credentials is to be used by all phones (e.g. WPA2-PSK or a common 802.1x account), then use the Default Export method.

If unique 802.1x accounts are to be deployed, then use the Bulk Export method.



Bulk Export

If needing to deploy the Cisco Unified Wireless IP Phone 7921G with unique 802.1x accounts utilizing EAP-FAST, PEAP or LEAP, then select the **Bulk Export** method.

The common data entered plus a CSV containing the phone MAC address, username and password will be used to create the template.

After selecting **Bulk Export**, a prompt to display the CSV file will be presented.

Up to **1000** entries are supported per CSV file.

The **userinfo.csv** file in the install path can be used as a template.

MAC,Username,Password

001e7abb19c8,admin,Cisco

Once the CSV file is imported, the utility will create TFTP downloadable configuration files for each phone, which are exported to the application install path (C:\Program Files\Cisco Systems\7921BD).

A confirmation window will be displayed when the TFTP downloadable configuration files have been exported successfully.

The files will be in the format of **WLAN<MAC_Address>.xml**, which the phone does a TFTP get for when it powers on or re-provisions.

Default Export

If needing to deploy the Cisco Unified Wireless IP Phone 7921G with identical WLAN settings, then select the **Default Export** method.

After selecting **Default Export** the utility will create a TFTP downloadable configuration file based on the common data entered, which is exported to the application install path (C:\Program Files\Cisco Systems\7921BD).

A confirmation window will be displayed when the default TFTP downloadable configuration file has been exported successfully.

The default file will be in the format of **WLANDefault.xml**, which the phone does a TFTP get for when it powers on or during re-provisioning.

Pushing Configuration Files to the Cisco 7921G

The Bulk Deployment Utility can be utilized for initial deployment or after the Cisco Unified Wireless IP Phone 7921G has been deployed.

Install the Bulk Deployment Utility on a computer running Microsoft Windows.

The Bulk Deployment Utility does not have TFTP server capabilities, so an external TFTP server will be required, where the phone configuration files will need to be copied to and enabled for TFTP download.

For initial deployment, the recommendation is to set up a staging environment where the Cisco Unified Wireless IP Phone 7921G can connect to a wireless LAN using the default phone credentials, obtain an IP address via DHCP and TFTP download the phone configuration file. This setup will enable the phone to auto-download the configuration files by simply powering the Cisco Unified Wireless IP Phone 7921G on. The staging environment setup needs to consist of an access point with the SSID **cisco** configured and DHCP enabled either on the access point itself or another device in the local network, where DHCP option 150 is configured to point to the TFTP server's IP address that is hosting the phone configuration files.

For post-deployment where Cisco Unified Wireless IP Phone 7921G is already being utilized on the production wireless LAN, copy the phone configuration files to the TFTP server that the Cisco Unified Wireless IP Phone 7921G is pointed to, then reset the phones to reconnect to the production wireless LAN and TFTP download the phone configuration file. The TFTP service may need to be restarted prior to resetting the phones depending on which type of TFTP server is utilized.

After the phone received the configuration file, the Cisco Unified Wireless IP Phone 7921G will then re-provision with the new settings and attempt to join the intended wireless LAN.

For additional security, the recommendation is to remove any phone configuration files from the TFTP server when not needed.

The Bulk Deployment Utility is available for download at the following URL.

http://software.cisco.com/download/navigator.html?mdfid=278875240

Wavelink Avalanche

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

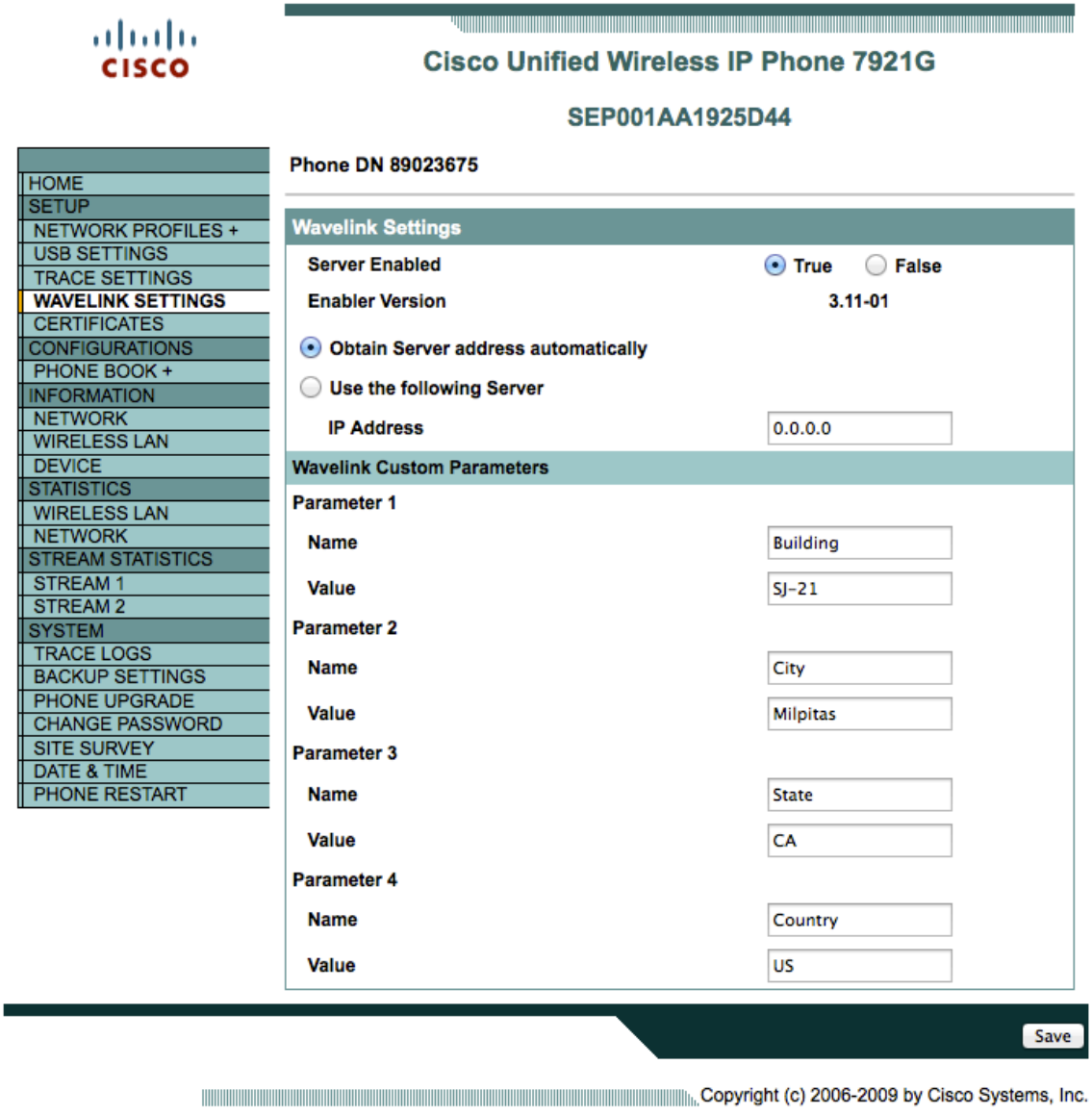
To provide the server IP address automatically, configure option 149 on the DHCP server.

```
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

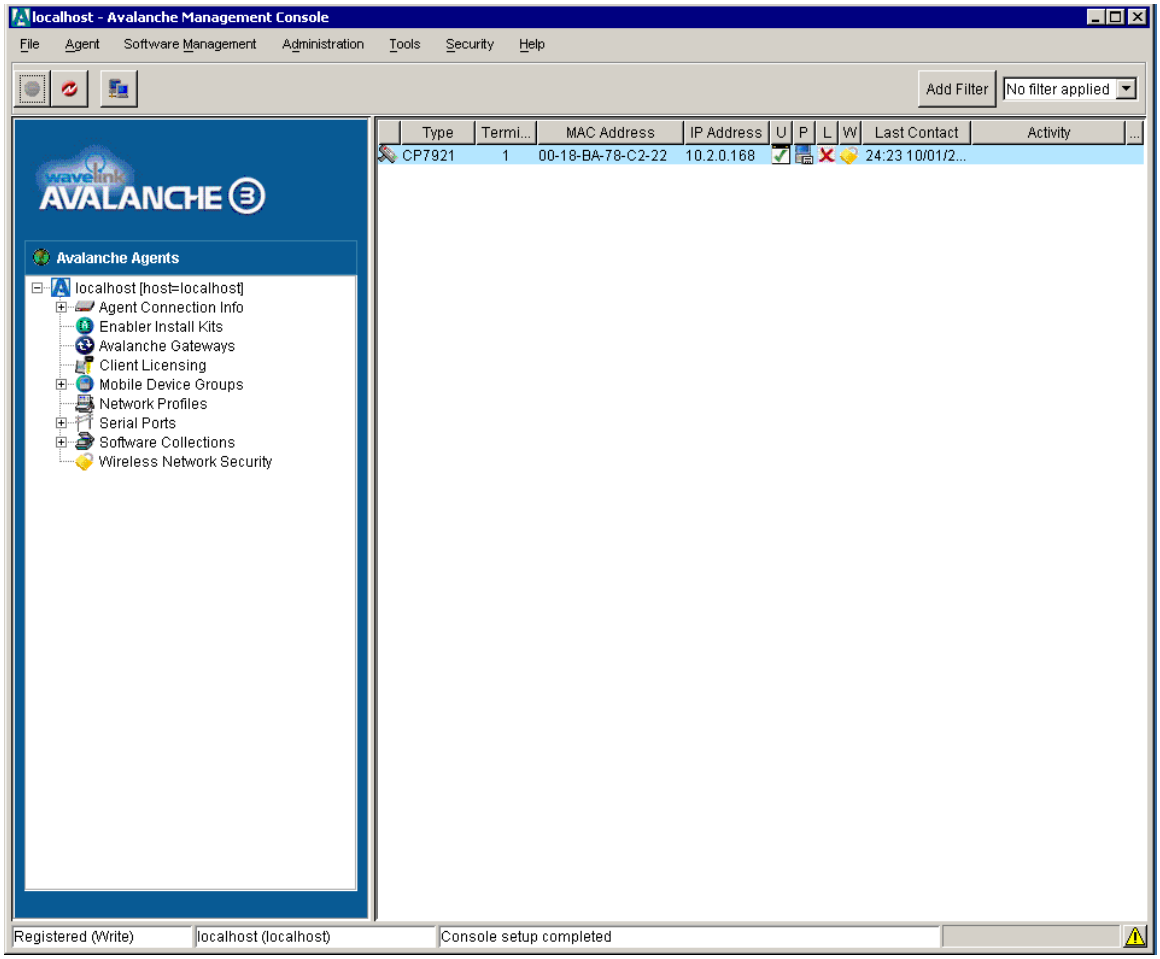
option 149 ip 10.10.11.128

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.



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

To set client properties, right click on the client then select **Client Settings.**

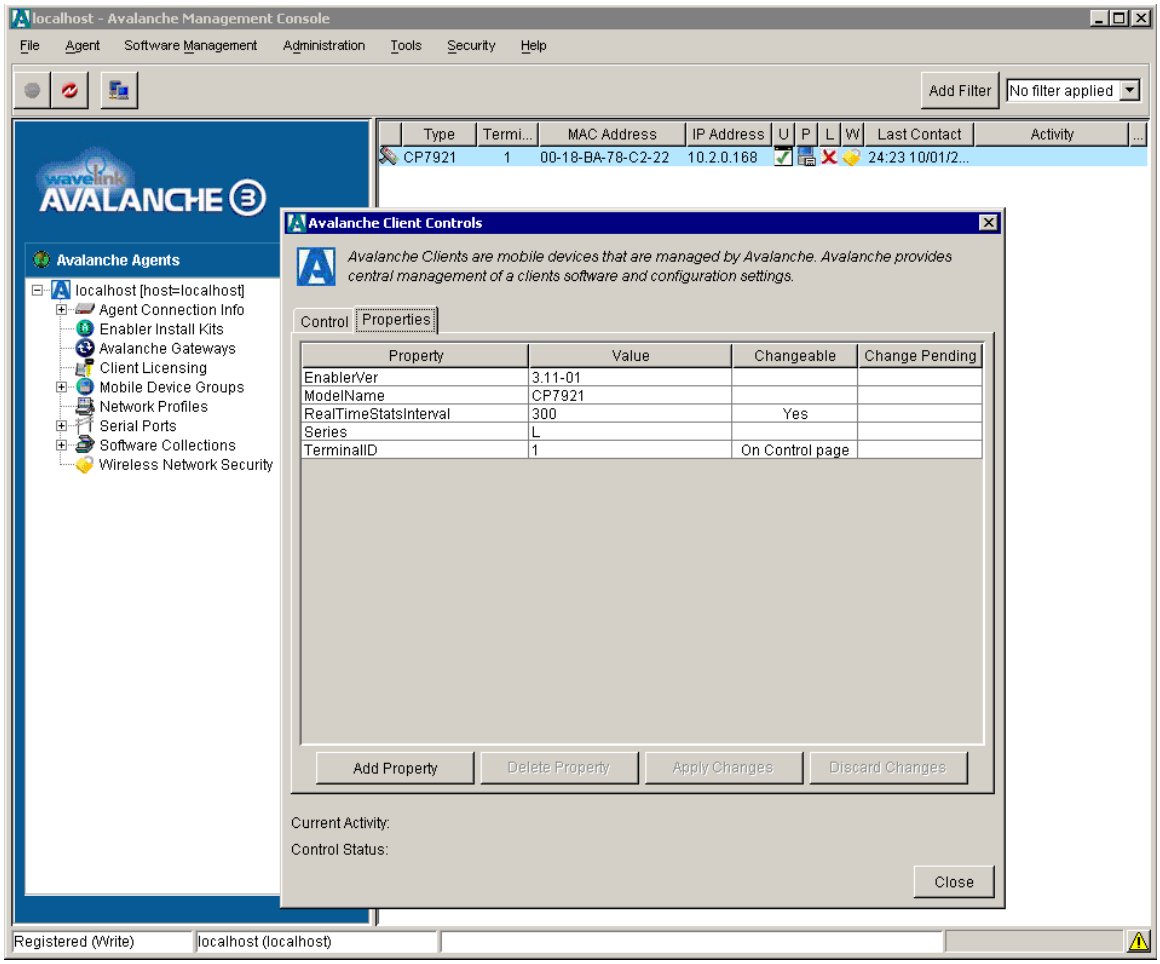


The Cisco Unified Wireless IP Phone 7921G will have parameters enabled by default.

EnablerVer = 3.11-01

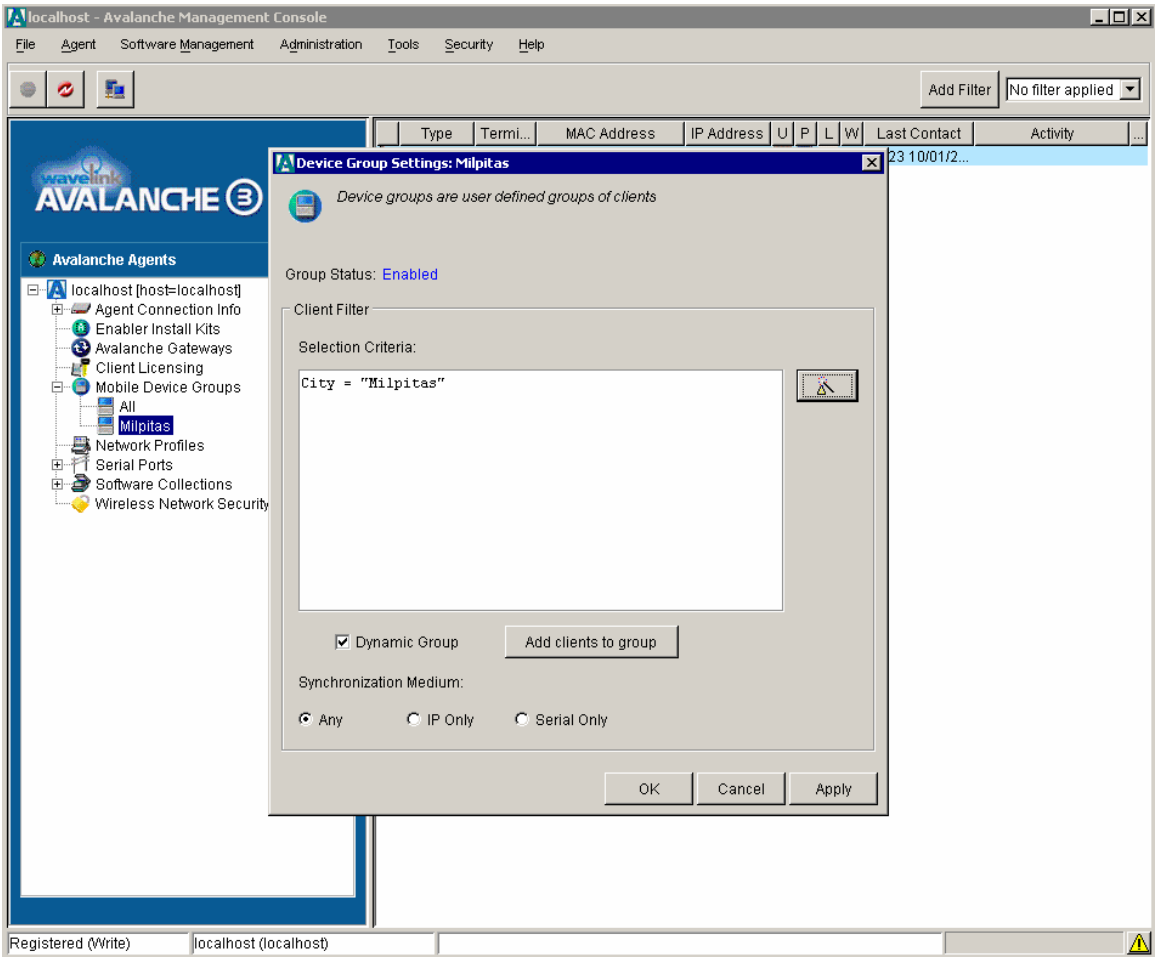
ModelName = CP7921G

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 then selecting **Settings**.



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

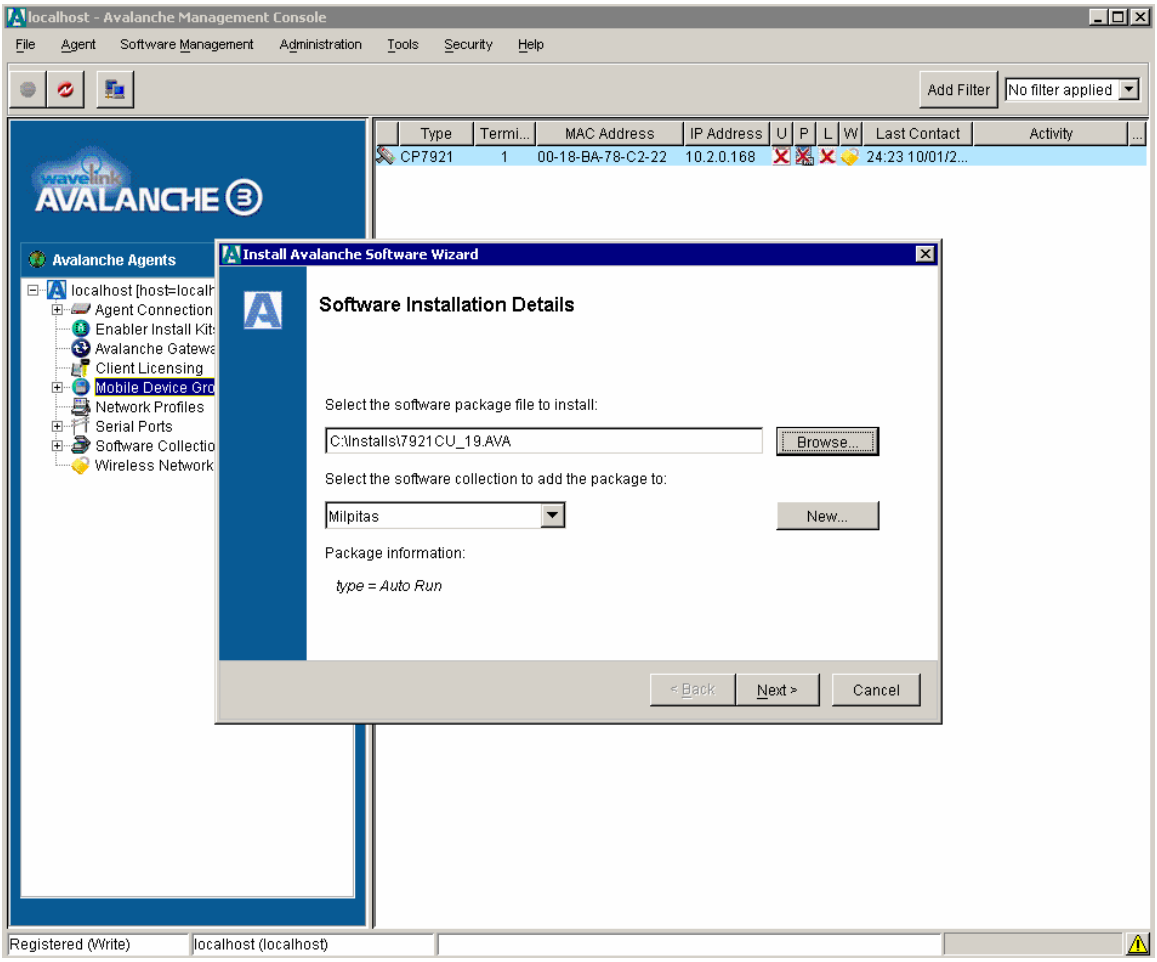
Browse to the 7921G Configuration Utility package file (e.g. 7921CU-1.2.1.AVA).

Create a software collection to add the package to.

The license agreement will be displayed, after selecting **Next,**

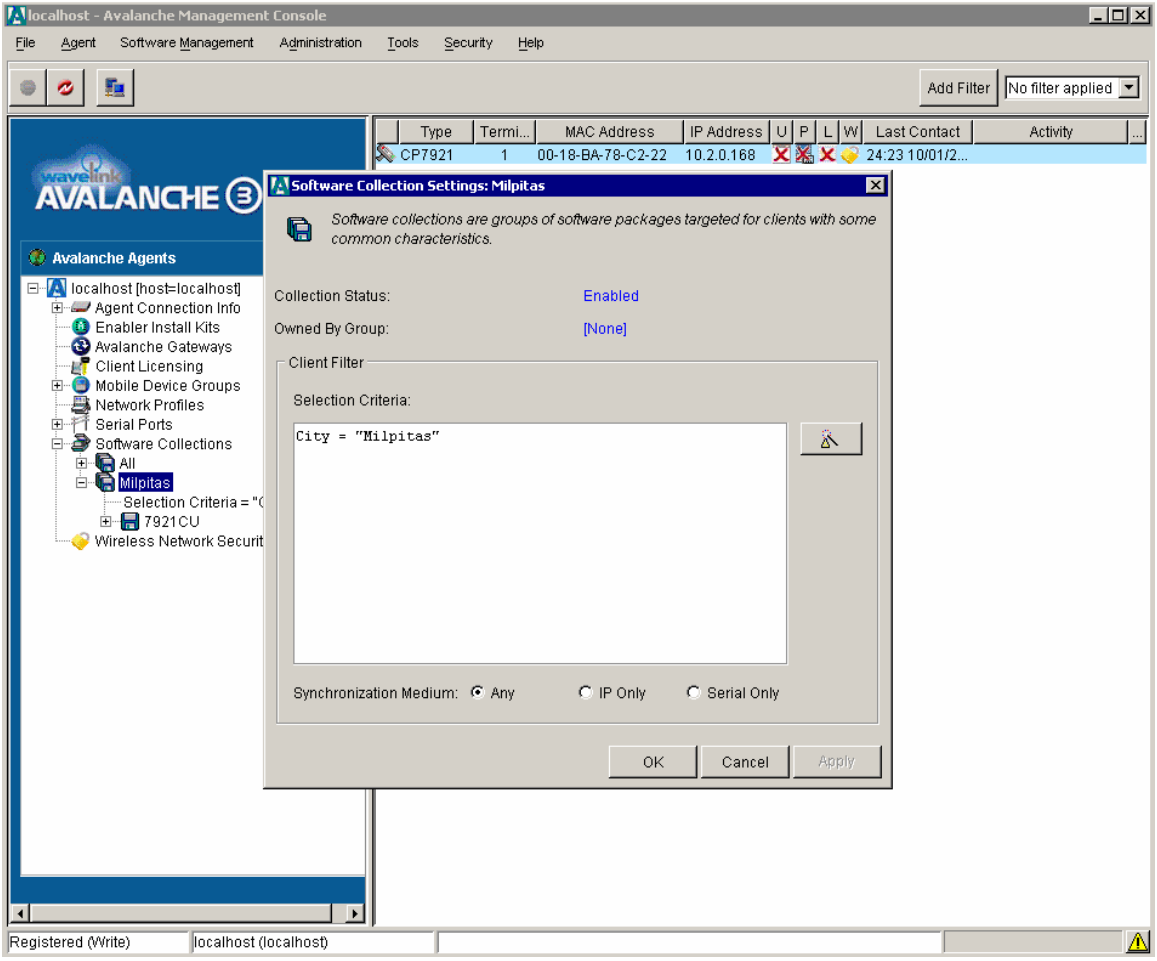
Click on **Finish** when the installation is complete.

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



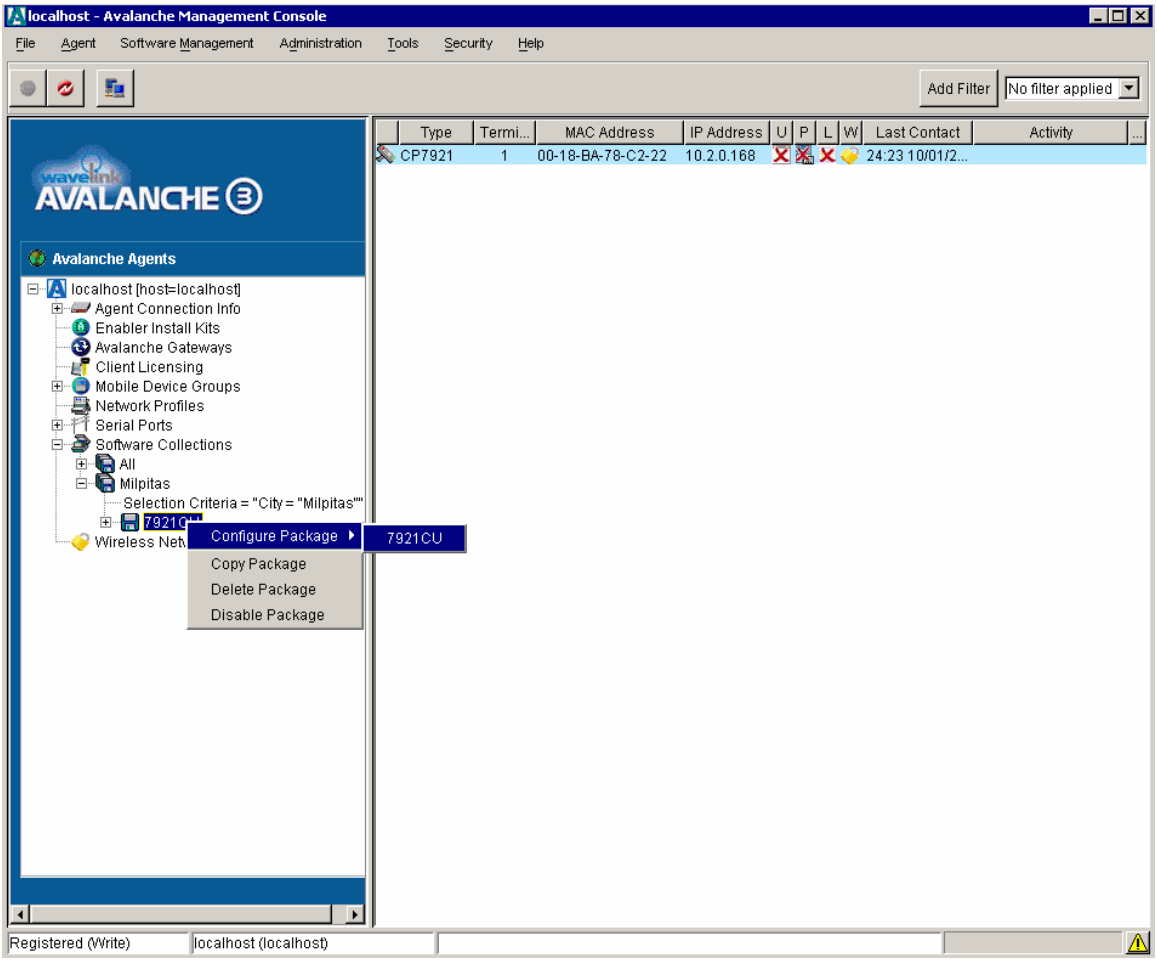
The software package must then be enabled by right clicking on the package then selecting **Enable Package**.

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 then select **7921CU**.

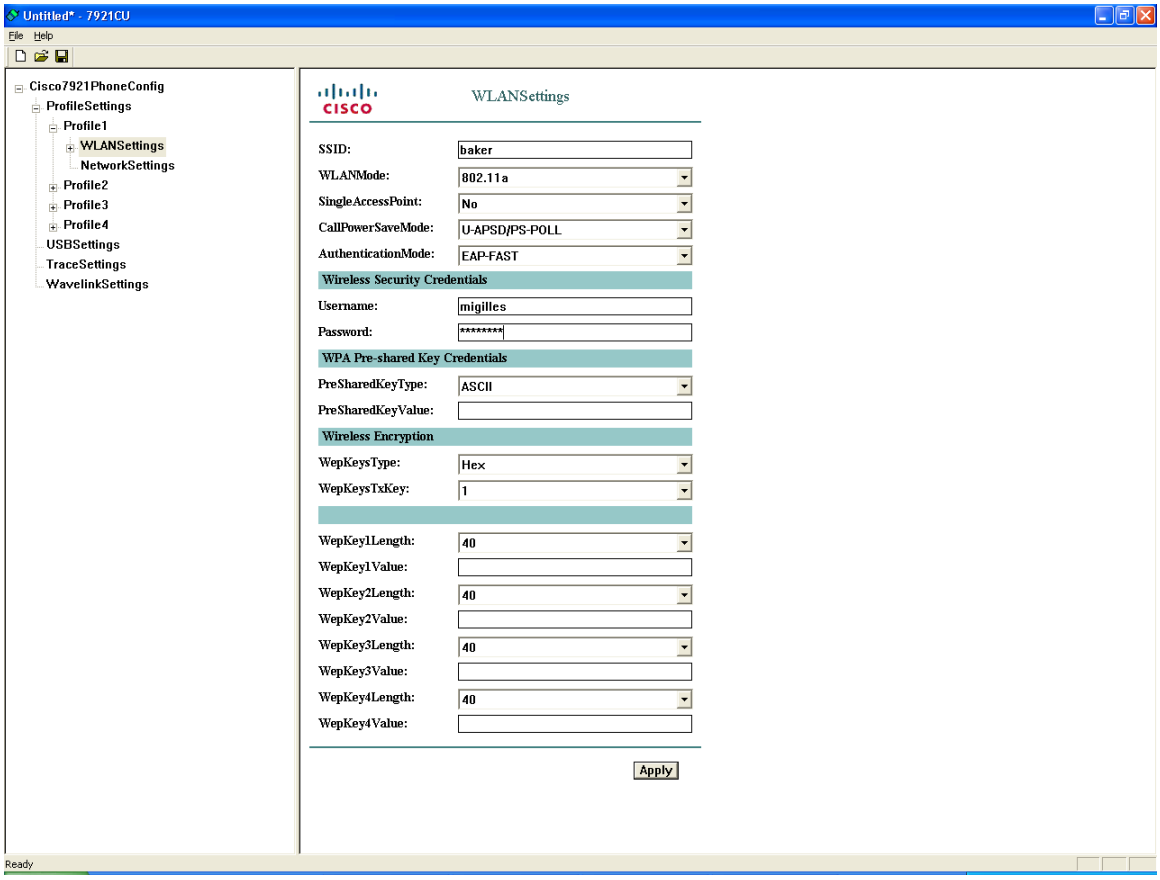
The 7921G Configuration Utility will then be launched.



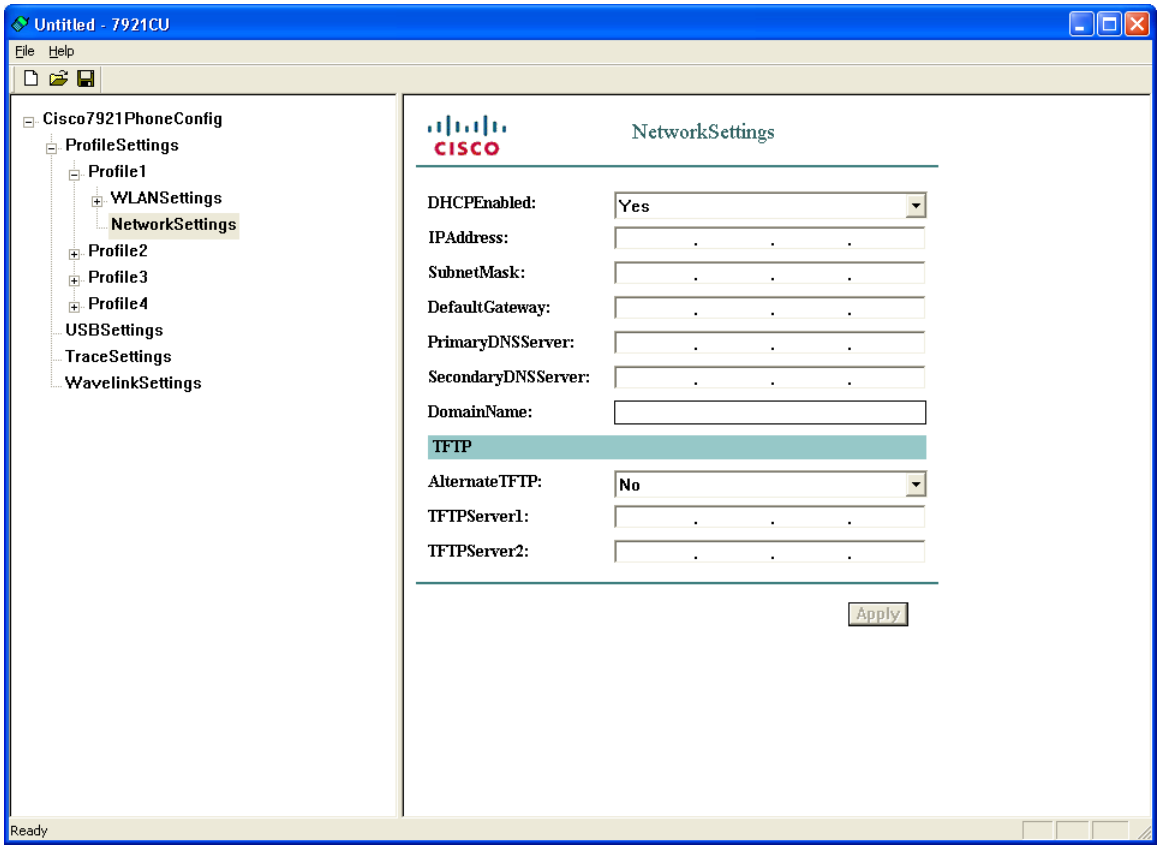
Enter the profile name and enable the profile.

Configure the network profiles by specifying the Wireless LAN credentials.

PEAP and EAP-TLS are not supported in the Configuration Utility for Wavelink.



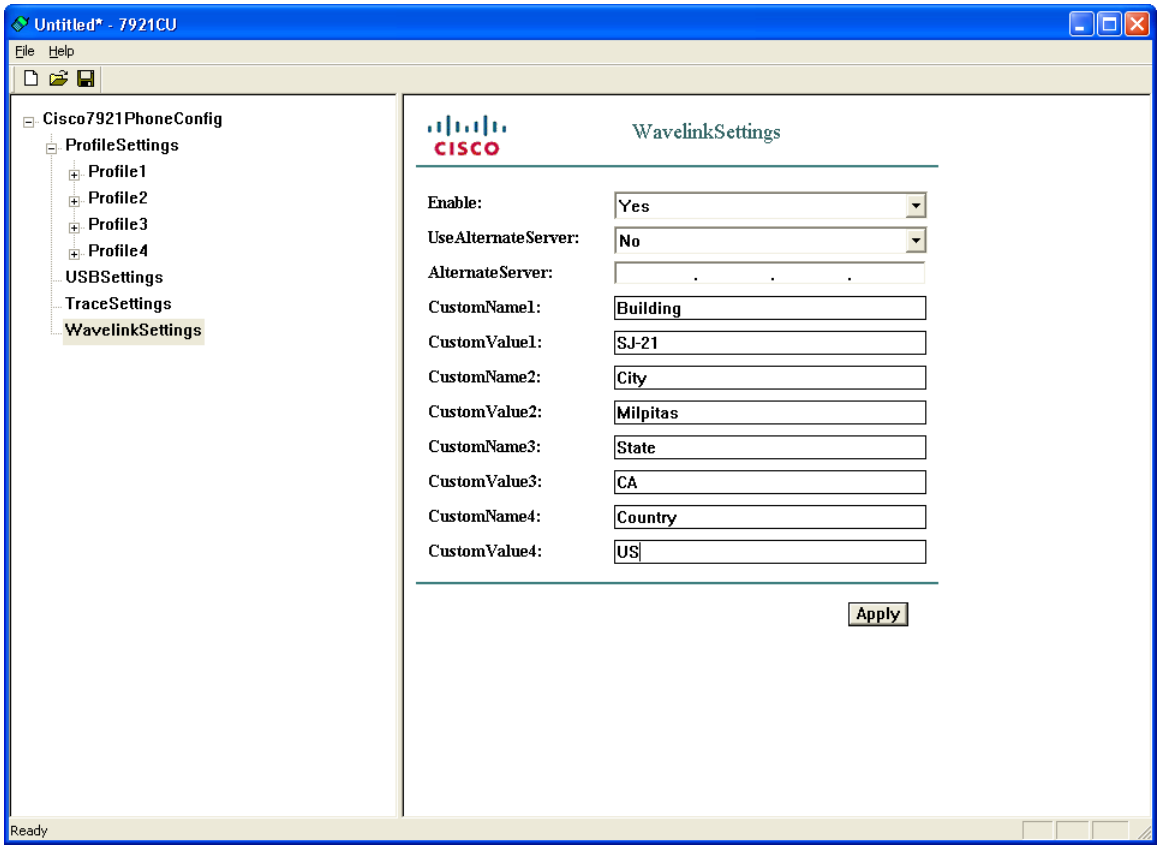
Configure the network settings for the network profile.



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 then select **Update Now**.

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

Local Phone Book and Speed Dials

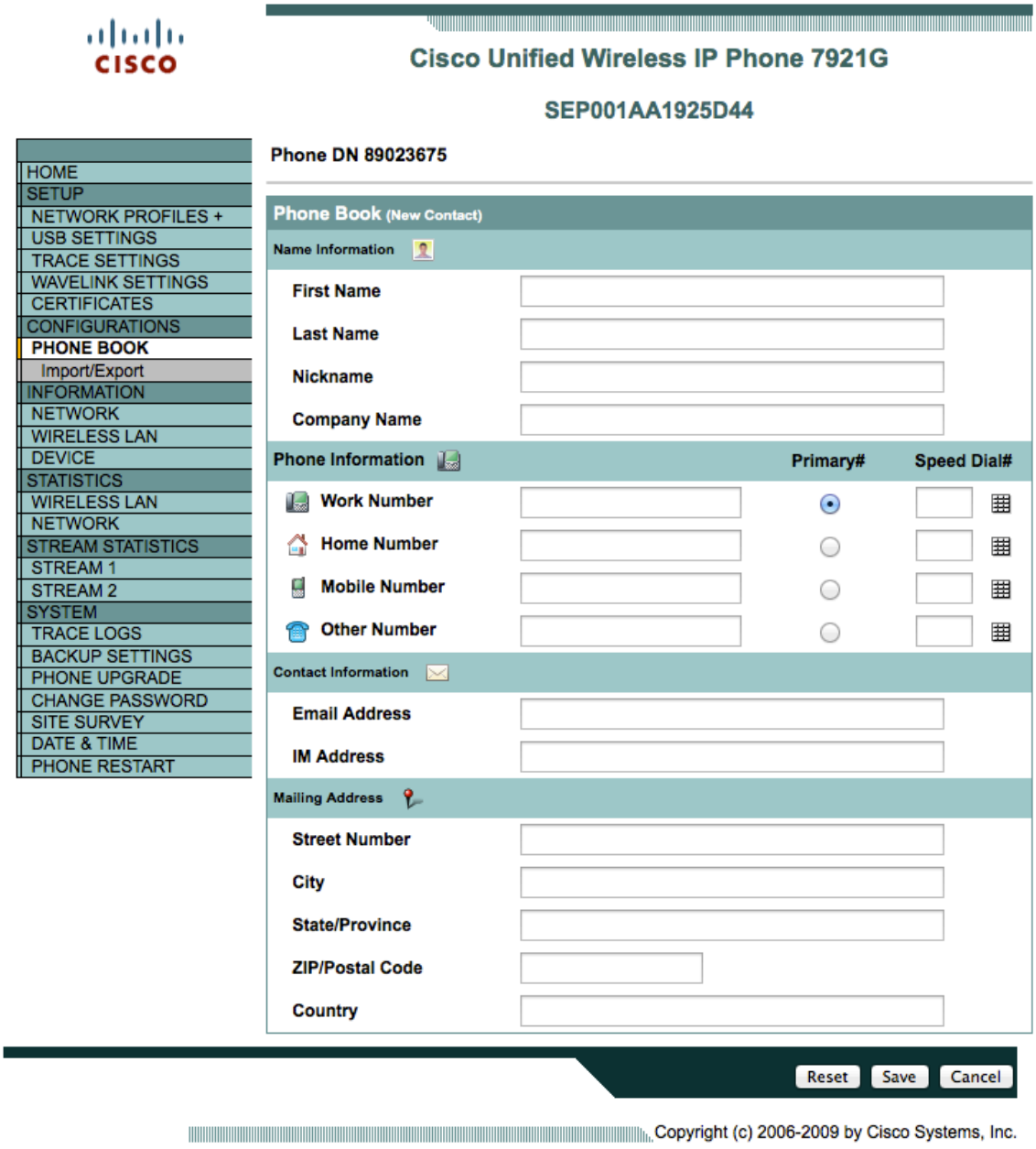
With release 1.1(1), the Cisco Unified Wireless IP Phone 7921G contains local phone book and speed dials support.

As of the 1.4(1) release up to 200 contacts (100 contacts in previous releases).

99 speed dials referenced from the local phone book can be added for quick dial access. Speed dial #1 is reserved for voicemail.

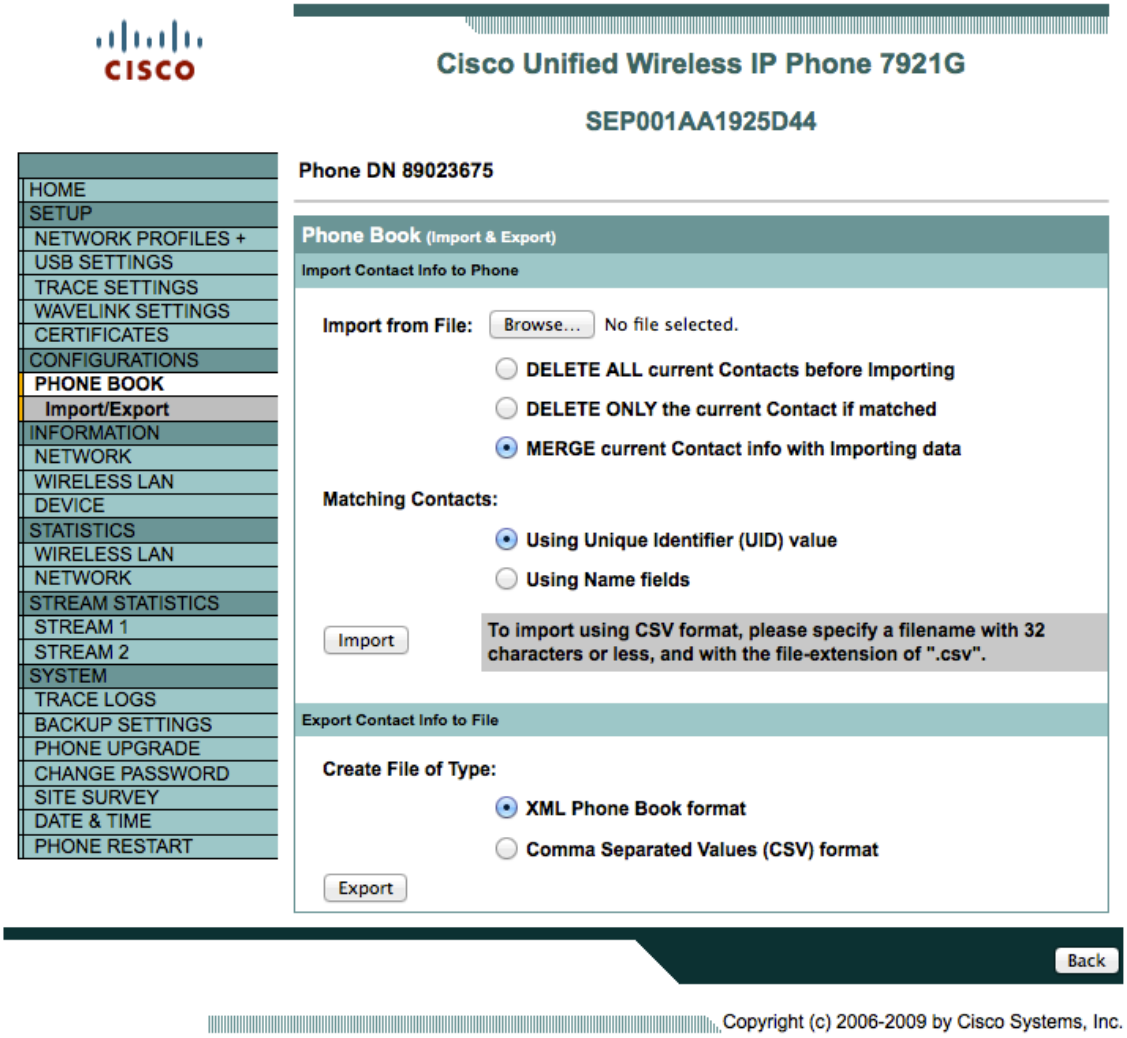
The left softkey on the home screen can be programmed for **Message** to access voice mail or to **PhBook** to access the local phone book.

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 user does not manage the web password, 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** as well as web access set to **Full**.



Exported phone book data 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.

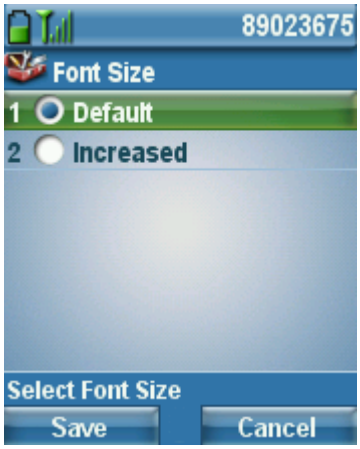


Increased Font

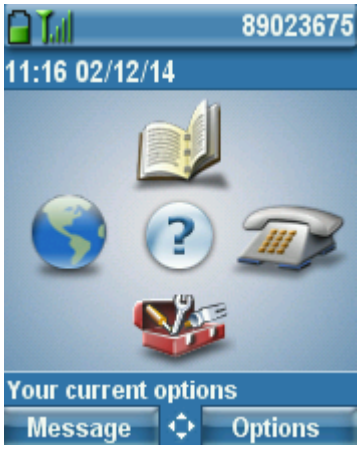
As of the 1.4(1) release, there are options for **Default** (original) font or **Increased** font.

The font size can optionally be configured locally on the phone.

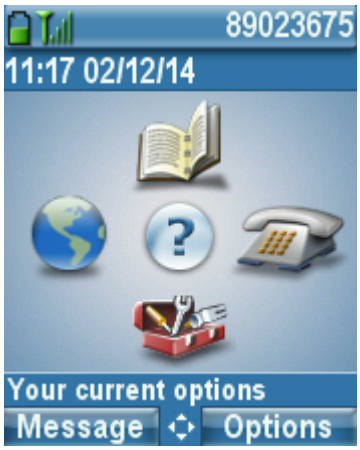
Settings > Phone Settings > Display Settings > Font Size



Default Font



Increased Font



Using Phone Designer

The Phone Designer application allows the ability to have a customer wallpaper and ringtone for each phone.

The Cisco Unified Wireless IP Phone 7921G is supported in Phone Designer version 7.1(3) and later.

Personalization must also be enabled in the Cisco Unified Communications Manager either in Enterprise Parameters, Common Phone Profile or on a per phone level.

After installing the phone designer, a username and password as well as the IP address of the Cisco Unified Communications Manager must be configured.

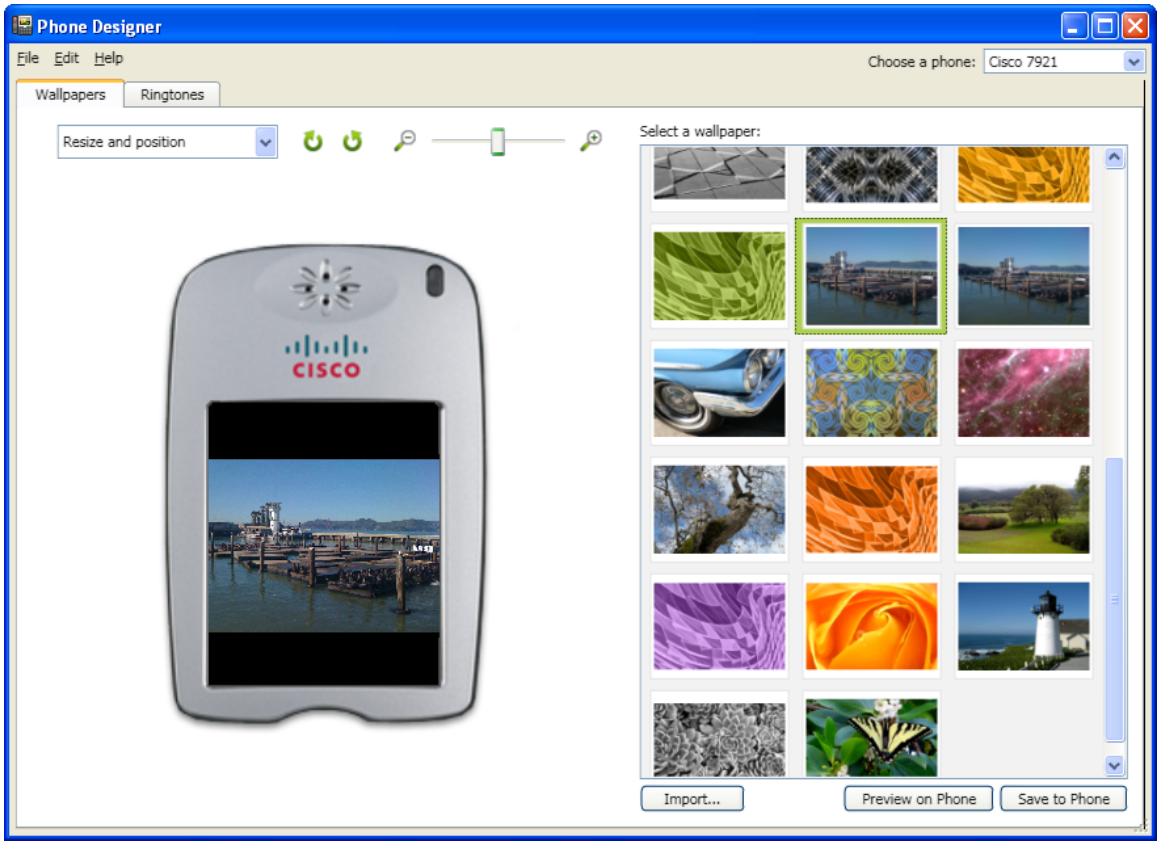
The user account must be created in the Cisco Unified Communications Manager and associated to the corresponding phone.

In order to configure the wallpaper, either select a pre-defined wallpaper or import a wallpaper from the local computer by selecting **Import**.

To display the wallpaper on the phone, select **Preview on Phone**.

To activate and save the wallpaper to the phone flash, select **Save to Phone**.

The default background image can be restored by navigating to **Settings > Phone Settings > Customize Home Page > Background Image.**

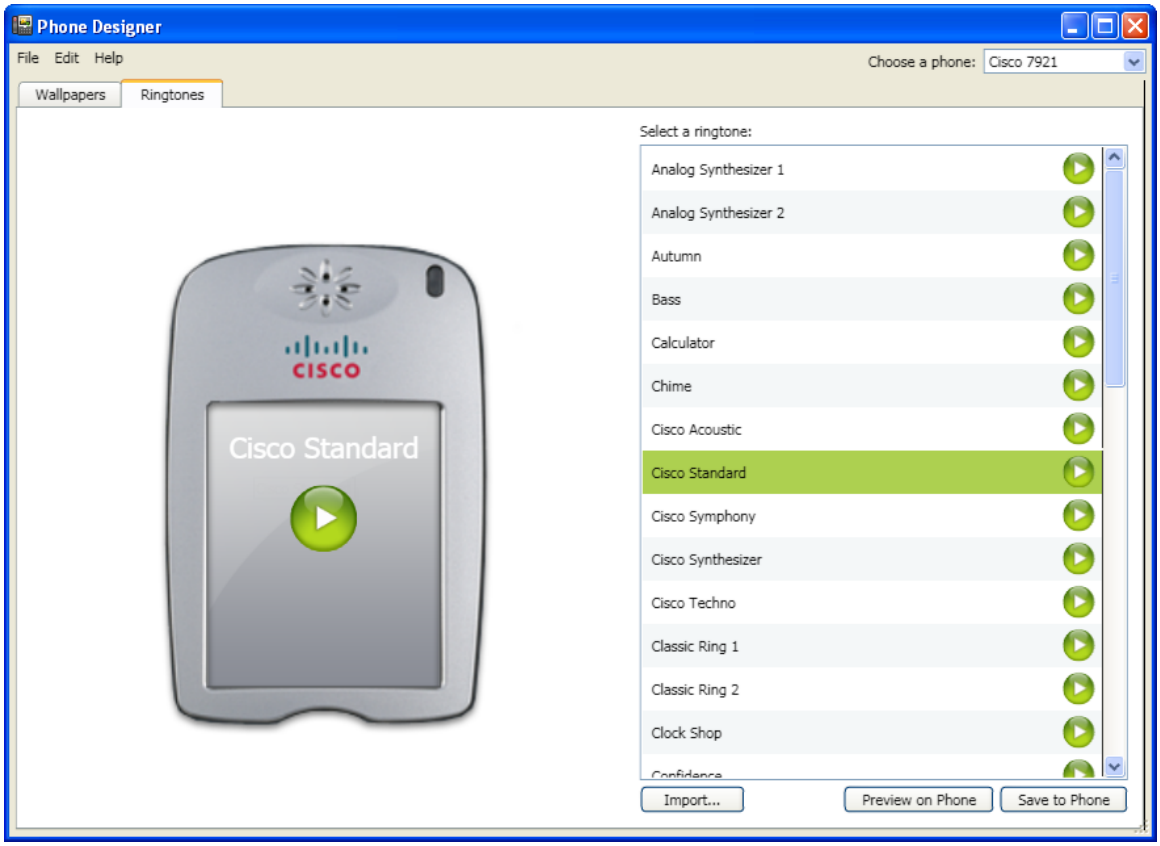


In order to configure the ringtone, either select a pre-defined ringtone or import a ringtone from the local computer by selecting **Import**.

To hear the ringtone on the phone, select **Preview on Phone**.

To activate and save the ringtone to the phone flash, select **Save to Phone**.

A pre-defined ringtone can be enabled by navigating to **Settings > Phone Settings > Sound Settings > Ring Tone.**



The Phone Designer application can be downloaded from the following location.

http://software.cisco.com/download/navigator.html?mdfid=278875240

Upgrading Phone Firmware

There are two methods for upgrading the Cisco Unified Wireless IP Phone 7921G firmware, which is either via wireless TFTP or the phone web interface.

Wireless TFTP

To upgrade 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, 7.1, 8.0, 8.5, 8.6, and later.

For information on how to install the COP file on CM versions 5.0 and later, refer to the Cisco Unified Communications Manager Operating System Administrator Guide at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

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.

The Load Server can be specified 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.

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.

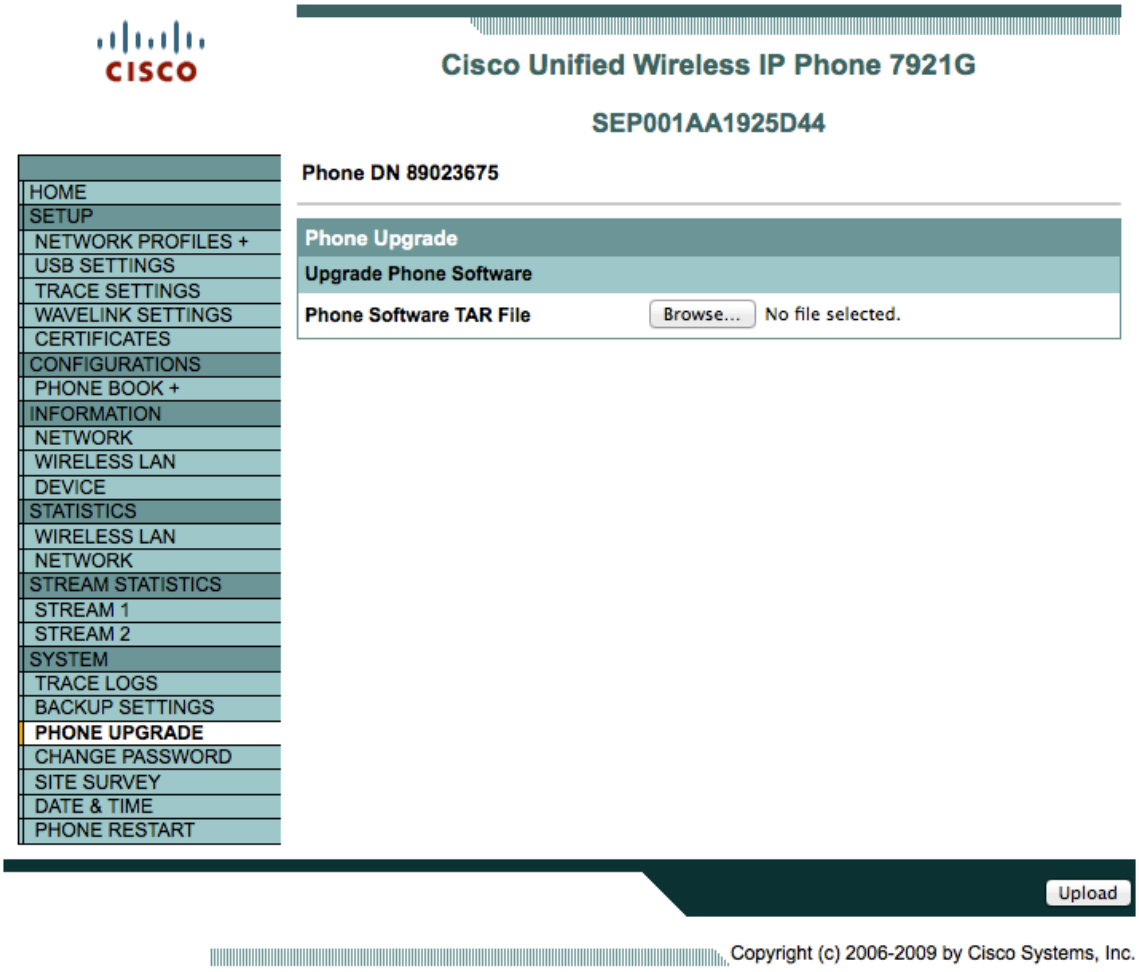
Example:

```
tftp-server flash: CP7921G-1.4.5SR1.3.LOADS
tftp-server flash:APPS-1.4.5SR1.3.SBN
tftp-server flash:GUI-1.4.5SR1.3.SBN
tftp-server flash:SYS-1.4.5SR1.3.SBN
tftp-server flash:TNUX-1.4.5SR1.3.SBN
tftp-server flash:TNUXR-1.4.5SR1.3.SBN
tftp-server flash:WLAN-1.4.5SR1.3.SBN
!
telephony-service
 load 7921 CP7921G-1.4.5SR1.3.LOADS
```

Web Interface

The phone firmware can be upgraded via the web interface by navigating to Phone Upgrade and browsing to the firmware TAR file.

In order to access the Phone Upgrade menu, the web access must be set to **Full**.



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 by default. In this mode, firmware upgrades via the web interface are not allowed. Full web access must be enabled in Cisco Unified Communications Manager in order to make changes.

Ultimately the Cisco Unified Wireless IP Phone 7921G will use what is set as the phone load in the Cisco Unified Communications Manager.

Hardware Compatibility

The following hardware and software compatibility matrix displays the minimum firmware version for each hardware revision of the Cisco Unified Wireless IP Phone 7921G.

To view the hardware revision information, select **Information > Device** from the Cisco Unified Wireless IP Phone 7921G webpage.

Model Type	Hardware Revision	Minimum Firmware Version
7921G	1.3	1.0(1)
	1.4, 1.5	1.0(3)

	2.5, 2.6	1.0(5)
	3.5, 3.6	1.3(4)
	4.5, 4.6	1.4(3)SR1

IP Phone Services

The Cisco Unified Wireless IP Phone 7921G is capable of supporting Extensible Markup Language (XML) applications.

Java MIDP support is not available on the Cisco Unified Wireless IP Phone 7921G.

For information on IP phone services configuration, refer to the following URL.

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_6_1/ccmcfg/b06phsrv.html

Extensible Markup Language (XML)

The following document provides the information needed for eXtensible Markup Language (XML) and X/Open System Interface (XSI) programmers and system administrators to develop and deploy IP phone services.

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html

Below are features that are unique to the Cisco Unified Wireless IP Phone 7921G.

Vibrate URI

http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/all_models/xsi/8_5_1/supporteduris.html#wp1052264

Device URI

http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/all_models/xsi/8_5_1/supporteduris.html#wp1078268

As of the 1.4(3) release, if a tone is pushed to the Cisco Unified Wireless IP Phone 7921G via XSI while on call, an alternate tone to the standard call waiting tone will be played so the user can distinguish the event type audibly.

Also in the 1.4(3) release, pressing the red button can silence a tone pushed via XSI.

XSI Audio Path Control

With the 1.4(4) release, the RTP URI has been extended to give an admin the option to specify whether audio received via XSI is played via the speakerphone or the handset speaker of the Cisco Unified Wireless IP Phone 7921G.

In releases prior to 1.4(4), the audio path is always set to speakerphone mode when an XSI "call" is received unless a headset is connected. The audio path could then be changed to the handset as necessary by the user.

The current RTP URI format is RTPRx:i:p:v or RTPMRx:i:p:v, where **i** equals IP address (x.x.x.x), p equals UDP port (20480-32768), and v equals volume (0-100). The volume value is a percentage of the maximum volume supported by the endpoint.

With the 1.4(4) release, there will be an additional parameter (speakerphone) supported (e.g. RTPRx:i:p:v:**s** or RTPMRx:i:p:v:**s**). The **s** parameter is to specify which audio path the Cisco Unified Wireless Phone 7921G should utilize.

If **s** is set to 0 then the speakerphone will be utilized; unless a headset is connected, where the audio will then be played to the headset.

If **s** is set to 1, then the handset or headset speaker will be utilized depending on whether a headset is currently connected or not.

If **s** is set to 2, then the current local mode will be utilized depending on whether speakerphone is enabled or not. If a headset is connected, audio will always be played to the headset.

If the **s** parameter is not specified, then the Cisco Unified Wireless Phone 7921G will set the audio path to speakerphone mode; unless a headset is connected, where the audio will then be played to the headset.

If currently on call and an XSI "call" comes in, then the current audio path will be used regardless of the **s** parameter value.

The audio path can be switched to the speakerphone or handset after a XSI "call" is received.

If wanting to utilize the **s** parameter for XSI "calls", the port and volume parameters are optional, but if not specified the colon must still be specified for that parameter (e.g. RTPRx:10.0.0.10:20500::1, RTPRx:10.0.0.10:::1, RTPMRx:10.0.0.10:20500::1, RTPMRx:10.0.0.10:::1).

If the port parameter is not specified, then the endpoint will select a UDP port and respond to the XSI push with that info.

If the volume parameter is not specified, then the endpoint will utilize its current volume setting.

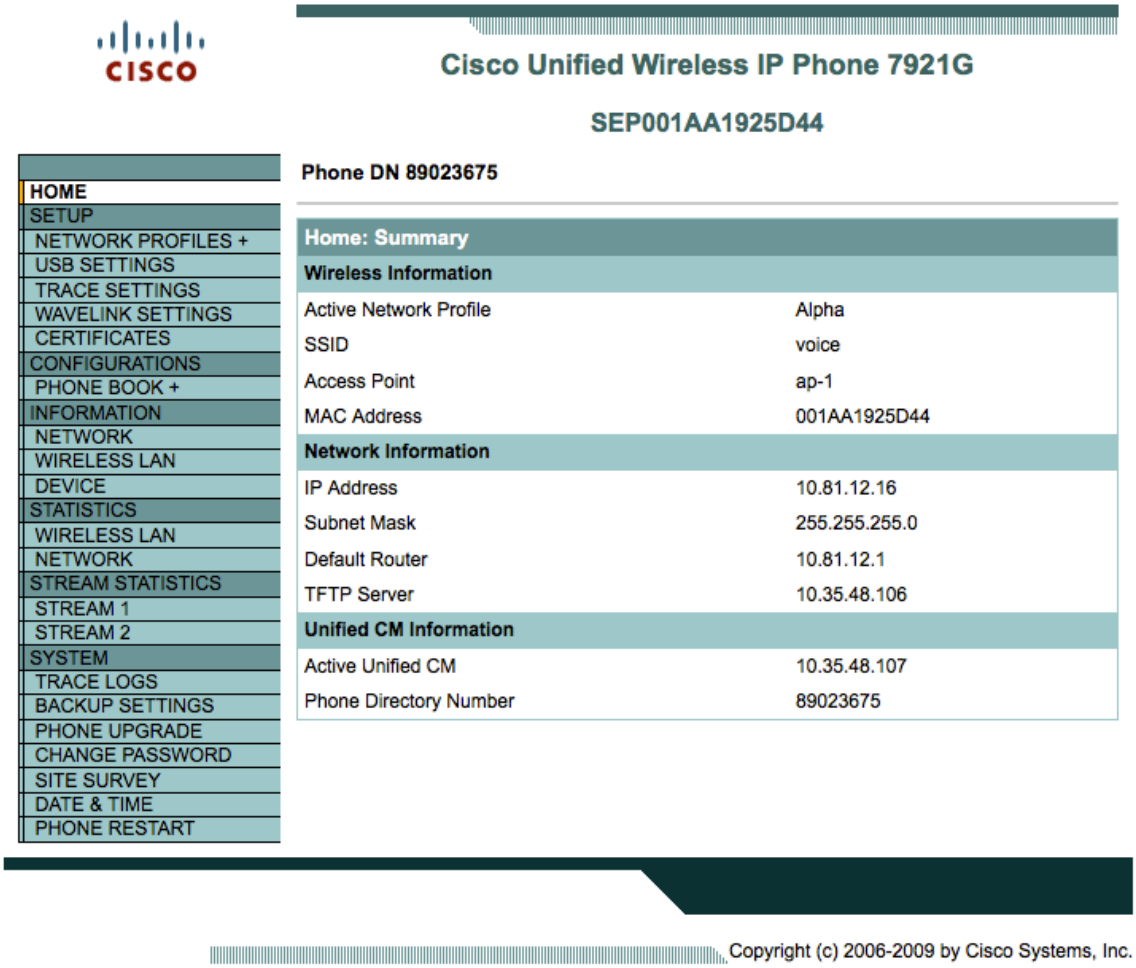
The chart below provides a few examples of the supported XSI audio path configurations per stream type.

XSI Audio Path	Stream Type	RTP URI Example
Speakerphone	Unicast	RTPRx:10.0.0.10:20500 RTPRx:10.0.0.10:20500::0 RTPRx:10.0.0.10:20500:100:0
Handset / Headset	Unicast	RTPRx:10.0.0.10:20500::1 RTPRx:10.0.0.10:20500:100:1
Speakerphone	Multicast	RTPMRx:10.0.0.10:20500 RTPMRx:10.0.0.10:20500::0 RTPMRx:10.0.0.10:20500:100:0
Handset / Headset	Multicast	RTPMRx:10.0.0.10:20500::1 RTPMRx:10.0.0.10:20500:100:1

Troubleshooting

Device Homepage

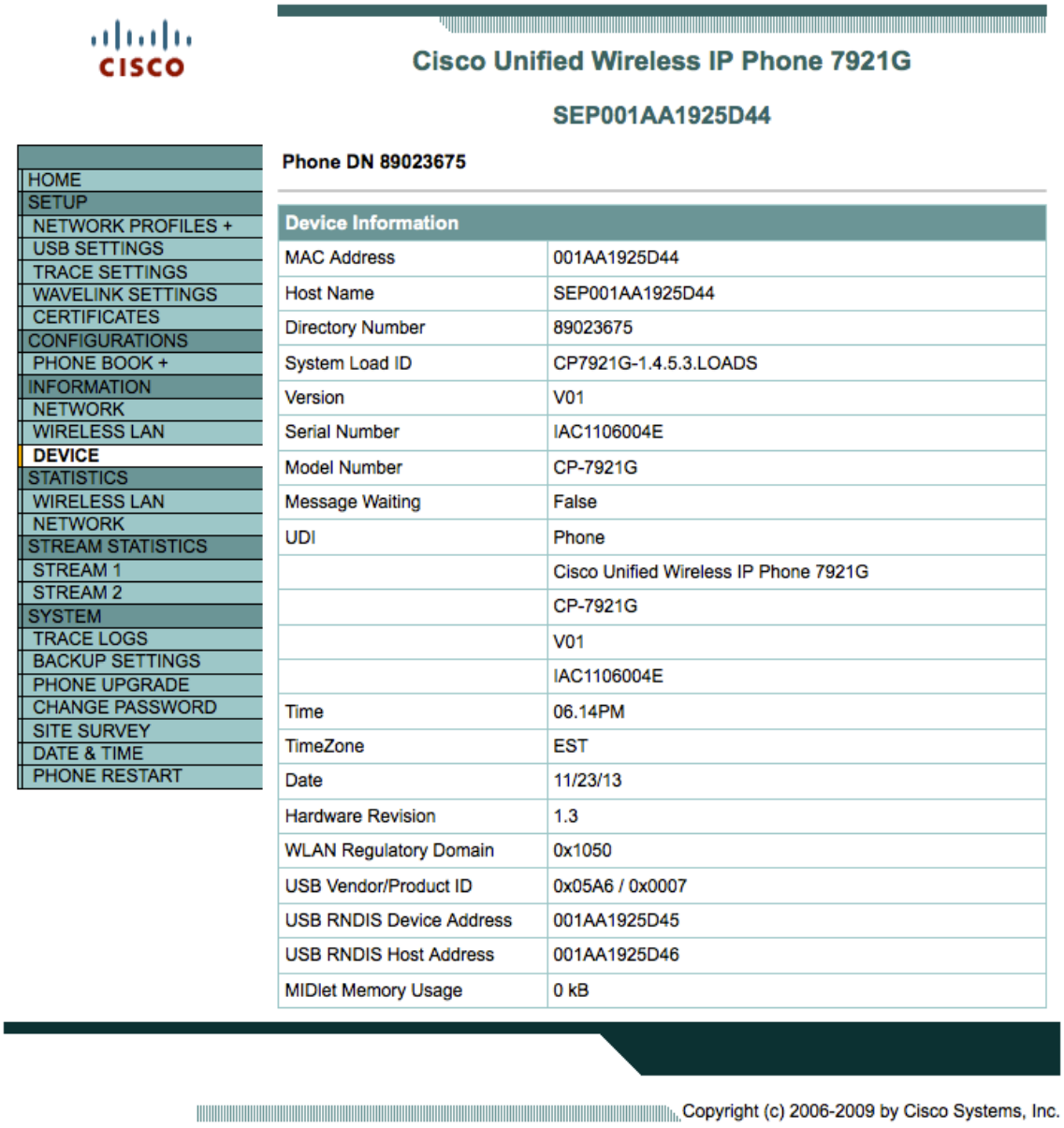
The Cisco Unified Wireless IP Phone 7921G webpage provides wireless, network, and Unified CM information.



Device Information

MAC address, hostname, directory number, and hardware and software version information is displayed in the Device Information section of the phone webpage.

Browse to the web interface (http://x.x.x.x) of the Cisco Unified Wireless IP Phone 7921G then select **Device** under the Information menu to view this information.

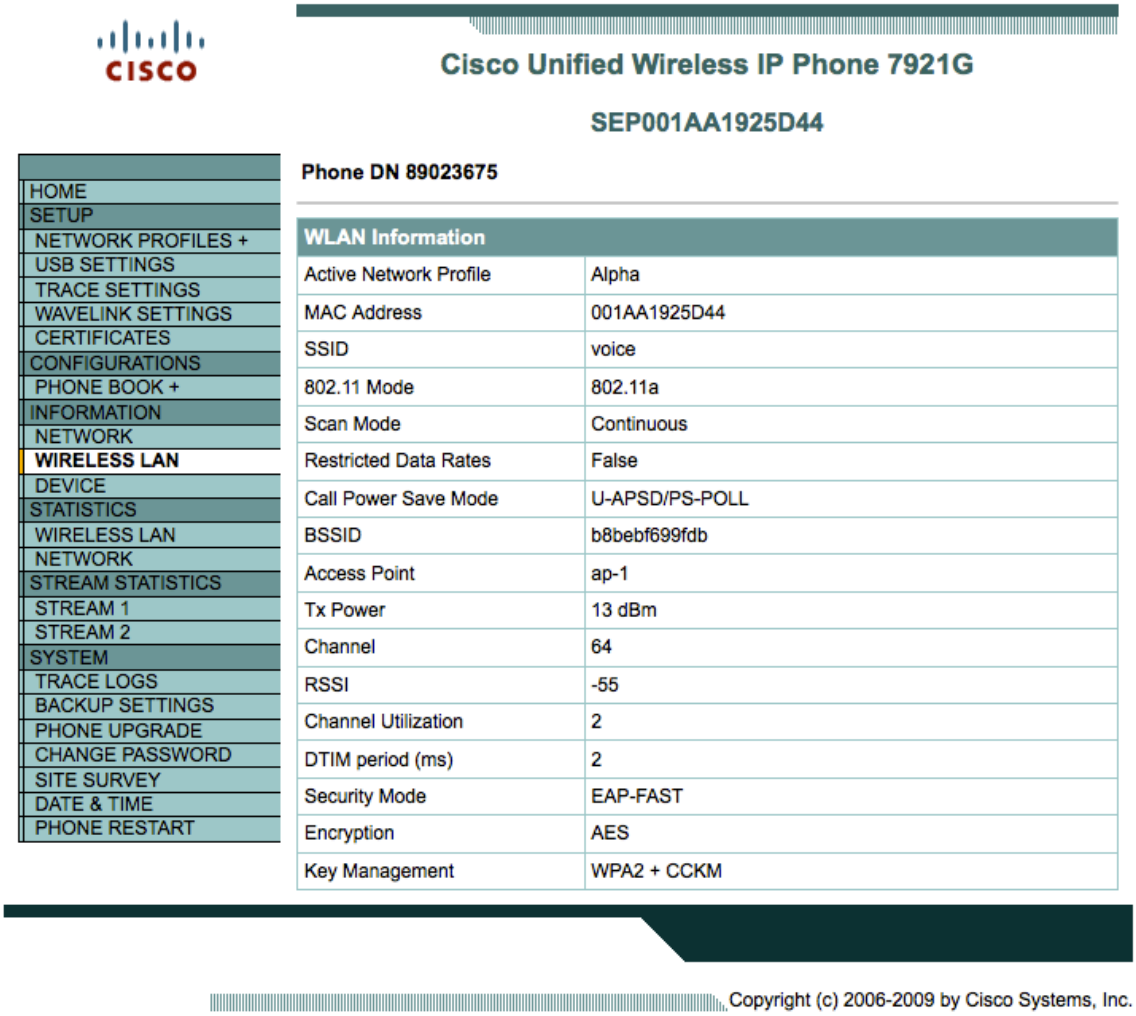


This information is also available locally on the phone under **Settings > Model Information**.

Wireless LAN Information

Detailed WLAN information is displayed in the Wireless LAN Information section of the phone webpage.

Browse to the web interface (http://x.x.x.x) of the Cisco Unified Wireless IP Phone 7921G then select **Wireless LAN** under the Information menu to view this information.

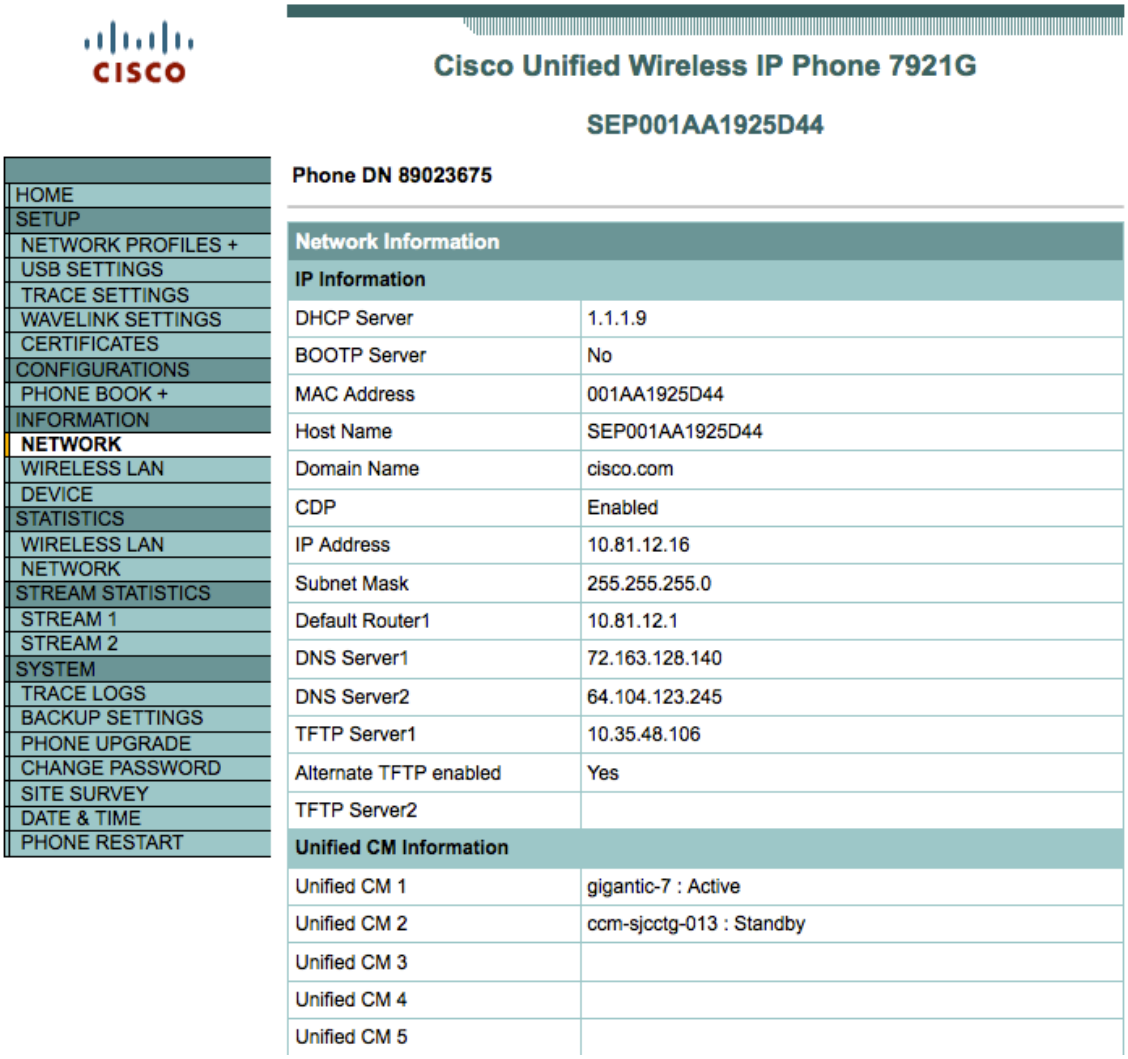


This information is also available locally on the phone under **Settings > Device Information > WLAN**.

Network Information

IP, Unified CM, SRST, MLPP, QoS, security, URL, and locale information is displayed in the Network Information section of the phone webpage.

Browse to the web interface (http://x.x.x.x) of the Cisco Unified Wireless IP Phone 7921G then select **Network** under the Information menu to view this information.



This information is also available locally on the phone under **Settings > Device Information**.

Stream Statistics

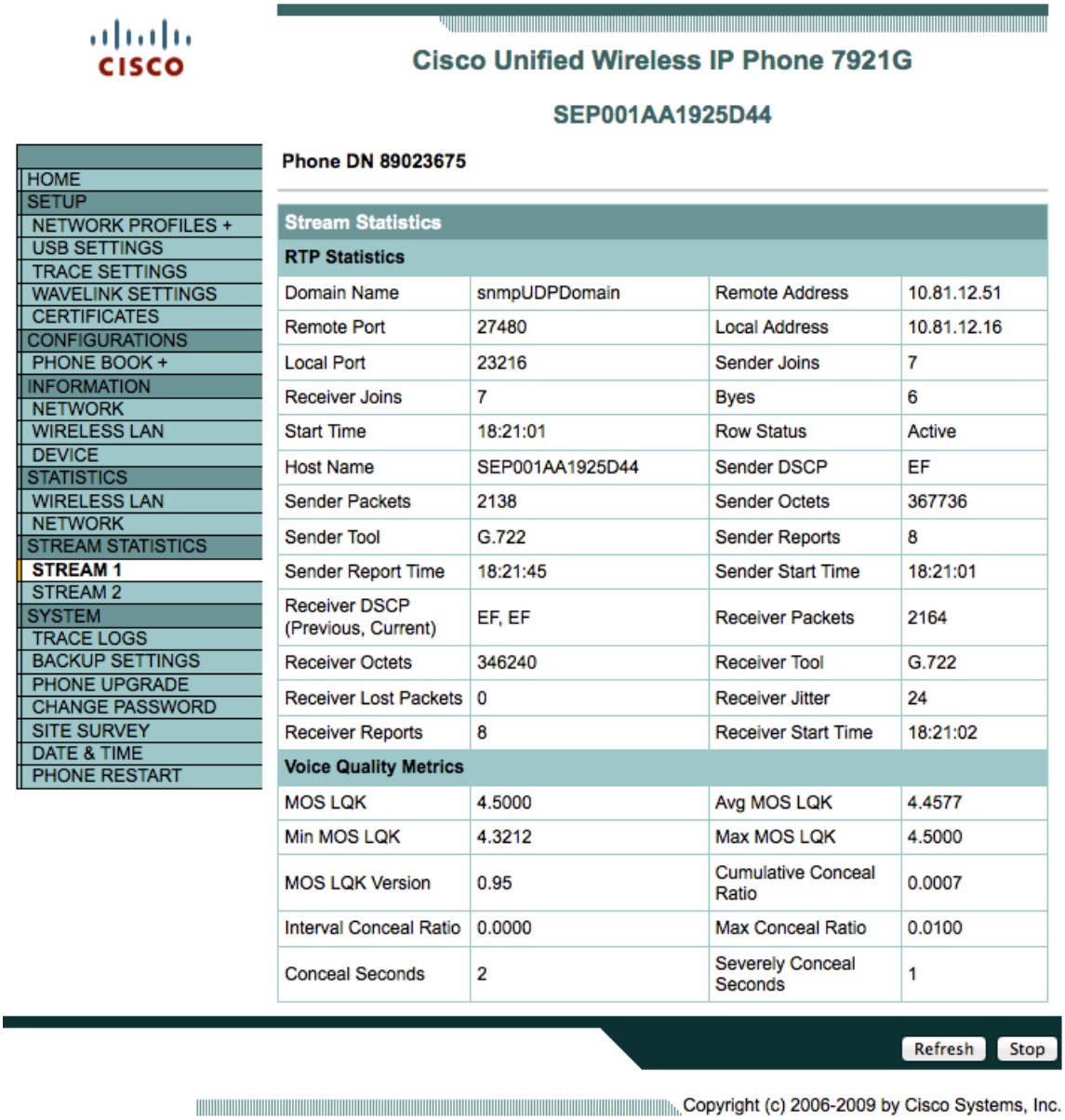
The Cisco Unified Wireless IP Phone 7921G provides call statistic information, where MOS, jitter and packet counters are displayed.

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.

The MOS value should be greater than or equal to 4.0 when using G.722 or G.711.

A MOS value of 3.8 is the highest possible value when using G.729.

Browse to the web interface (http://x.x.x.x) of the Cisco Unified Wireless IP Phone 7921G then select **Stream Statistics**.



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.

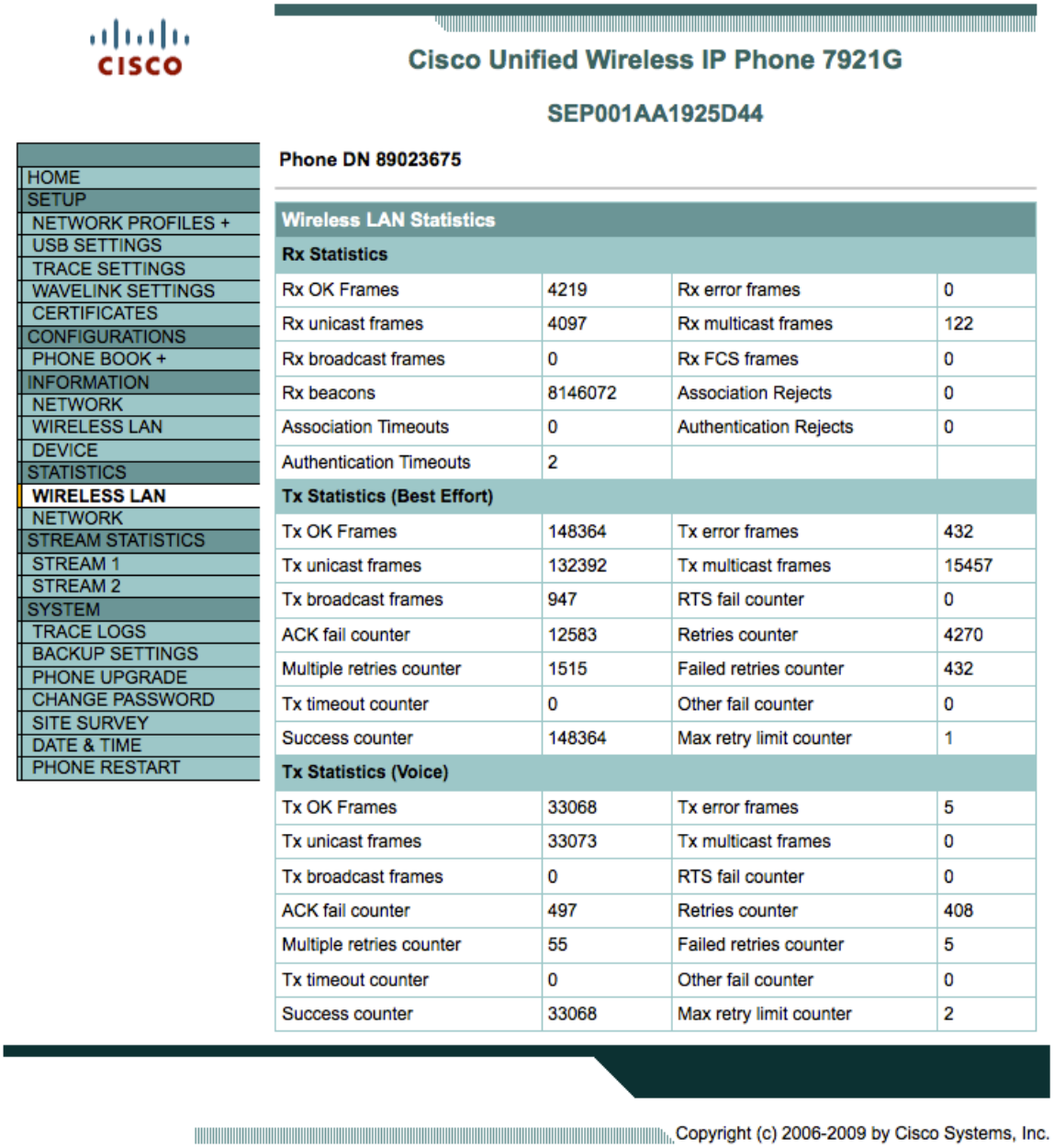
For more information, see the **Troubleshooting the Cisco Unified Wireless IP Phone 7921G** chapter in the Cisco Unified Wireless IP Phone 7921G Administration Guide at this URL:

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

Wireless LAN Statistics

Wireless LAN transmit and receive statistic information is displayed in the Wireless LAN Statistics section of the phone webpage.

Browse to the web interface (http://x.x.x.x) of the Cisco Unified Wireless IP Phone 7921G then select **Wireless LAN** under the Statistics menu to view this information.



Cisco Unified Wireless IP Phone 7921G

SEP001AA1925D44

Phone DN 89023675

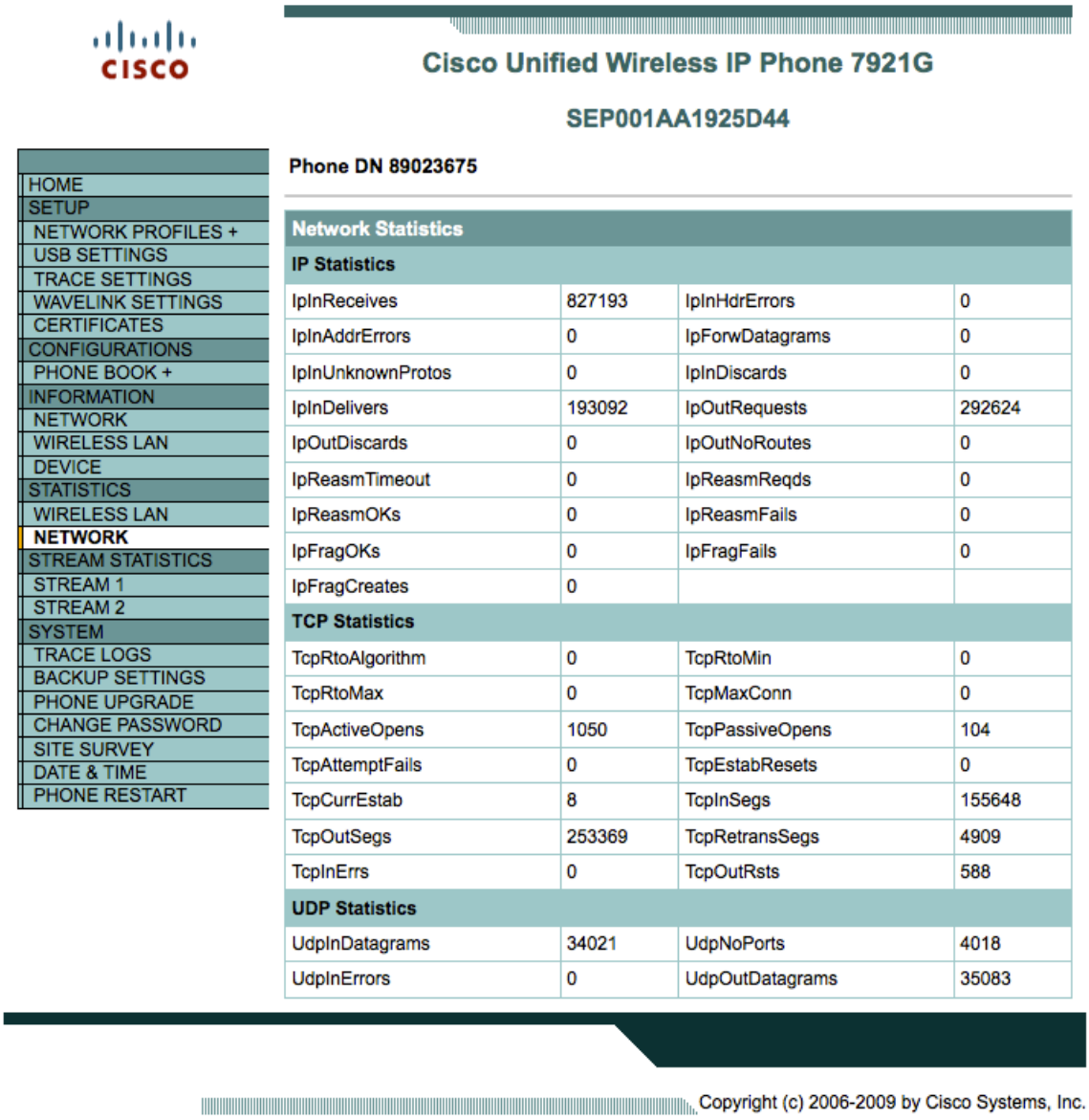
HOME
SETUP
NETWORK PROFILES +
USB SETTINGS
TRACE SETTINGS
WAVELINK SETTINGS
CERTIFICATES
CONFIGURATIONS
PHONE BOOK +
INFORMATION
NETWORK
WIRELESS LAN
DEVICE
STATISTICS
WIRELESS LAN
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY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

Wireless LAN Statistics			
Rx Statistics			
Rx OK Frames	4219	Rx error frames	0
Rx unicast frames	4097	Rx multicast frames	122
Rx broadcast frames	0	Rx FCS frames	0
Rx beacons	8146072	Association Rejects	0
Association Timeouts	0	Authentication Rejects	0
Authentication Timeouts	2		
Tx Statistics (Best Effort)			
Tx OK Frames	148364	Tx error frames	432
Tx unicast frames	132392	Tx multicast frames	15457
Tx broadcast frames	947	RTS fail counter	0
ACK fail counter	12583	Retries counter	4270
Multiple retries counter	1515	Failed retries counter	432
Tx timeout counter	0	Other fail counter	0
Success counter	148364	Max retry limit counter	1
Tx Statistics (Voice)			
Tx OK Frames	33068	Tx error frames	5
Tx unicast frames	33073	Tx multicast frames	0
Tx broadcast frames	0	RTS fail counter	0
ACK fail counter	497	Retries counter	408
Multiple retries counter	55	Failed retries counter	5
Tx timeout counter	0	Other fail counter	0
Success counter	33068	Max retry limit counter	2

Network Statistics

IP, TCP, and UDP statistic information is displayed in the Network Statistics section of the phone webpage.

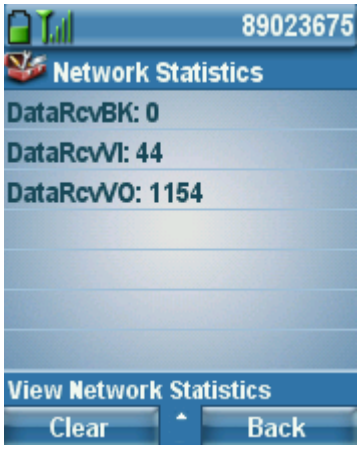
Browse to the web interface (http://x.x.x.x) of the Cisco Unified Wireless IP Phone 7921G then select **Network** under the Statistics menu to view this information.



Queue statistics can also be displayed locally on the phone by navigating to **Settings > Status > Network Statistics**.

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

This reflects that voice packets are being properly marked as UP6 (VO) downstream to the Cisco Unified Wireless IP Phone 7921G.



Phone Logs

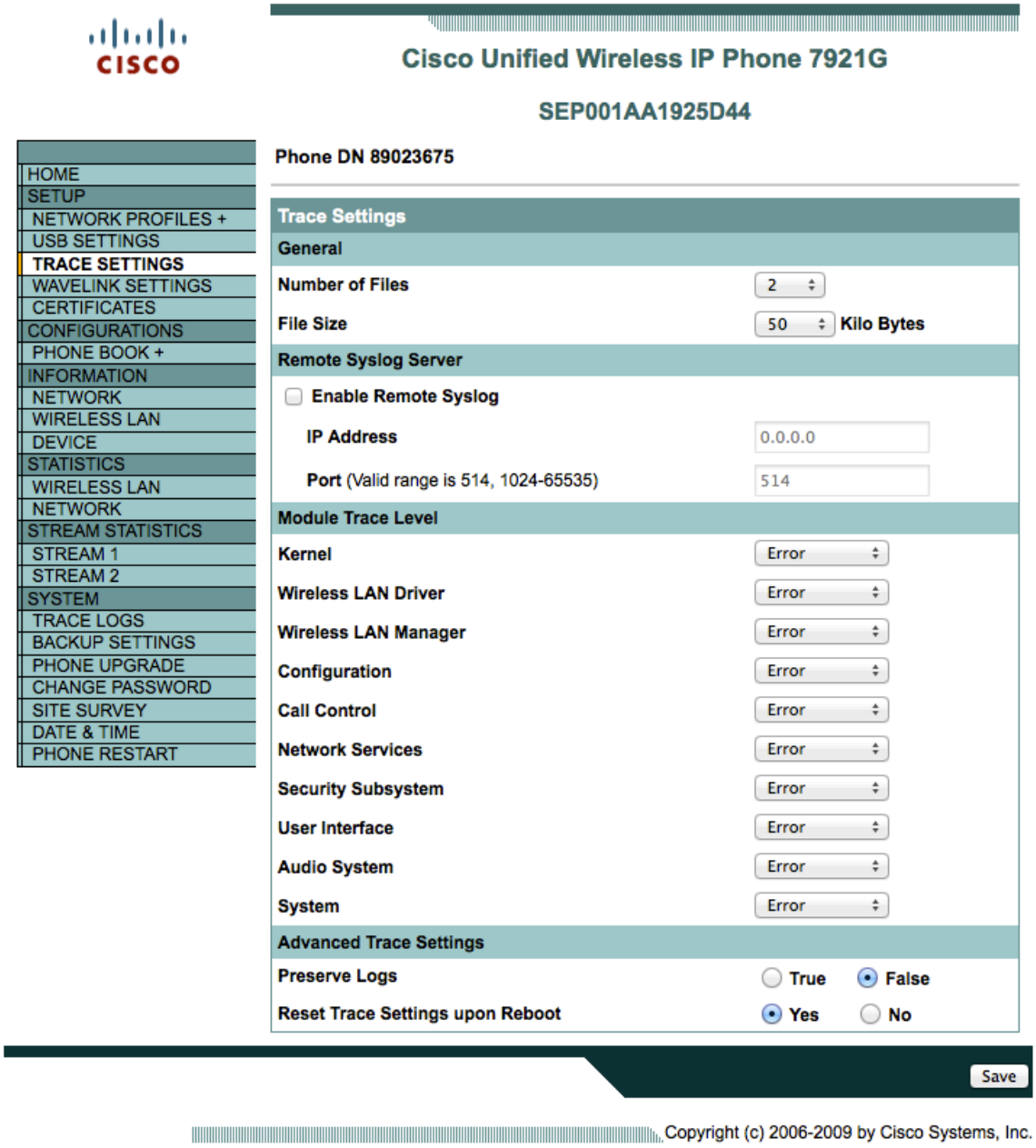
Phone logs for troubleshooting purposes can be obtained from the Cisco Unified Wireless IP Phone 7921G web interface.

Trace Settings

Browse to the web interface (http://x.x.x.x) of the Cisco Unified Wireless IP Phone 7921G then select **Trace Settings** to enable debugging.

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.



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

System	Event Manager

Trace Levels

Various levels of tracing are available, that can provide different levels of messaging.

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

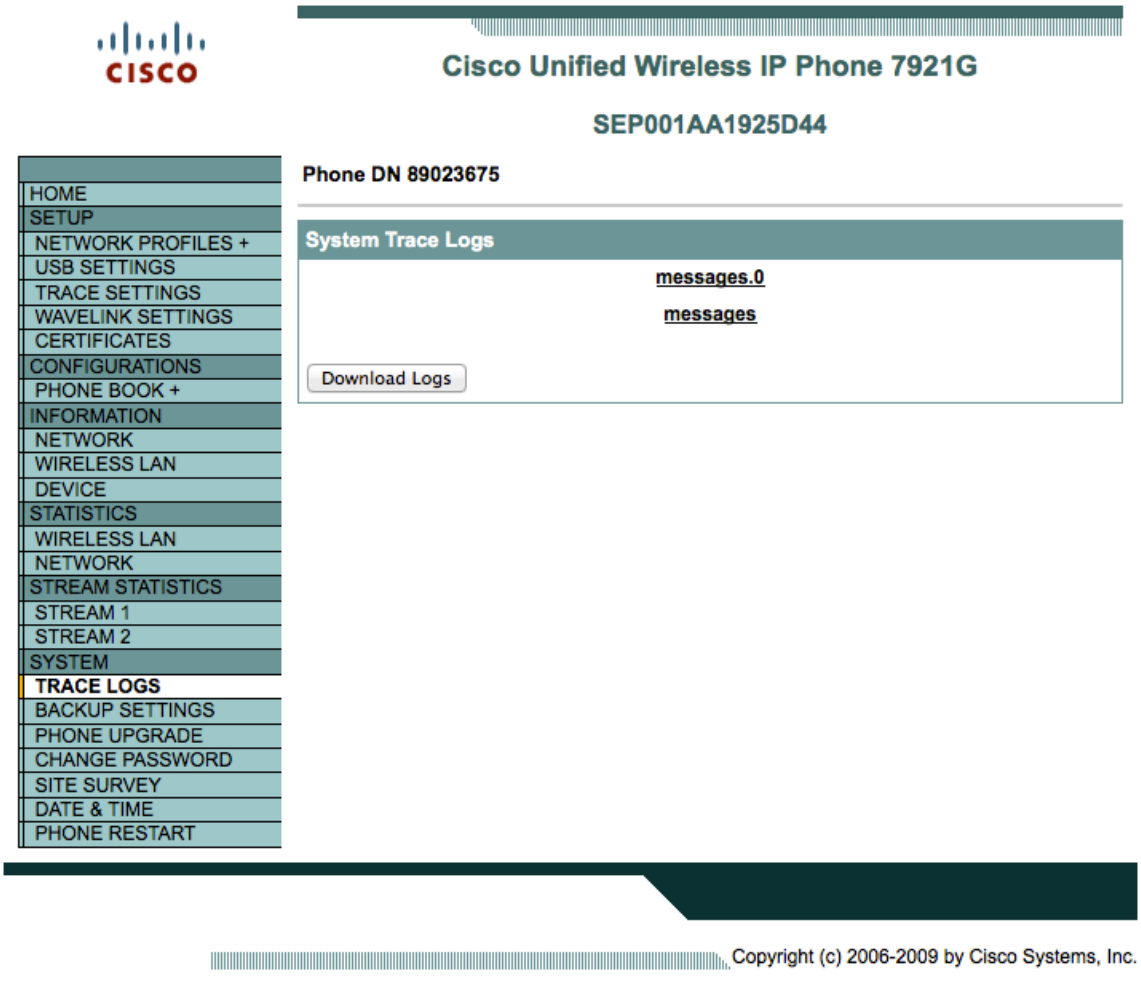
Note: All trace modules are set to Error level by default.

Voice quality can potentially be impacted if higher trace levels are configured or if **Preserve Logs** is enabled, which will write the logs to flash memory.

The trace level will reset to **Error** level by default unless configured to preserve the trace levels where **Reset Trace Settings upon Reboot** is set to **No**.

Trace Logs

To download the phone logs, browse to the web interface (http://x.x.x.x) of the Cisco Unified Wireless IP Phone 7921G then select **Trace Logs**.



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.

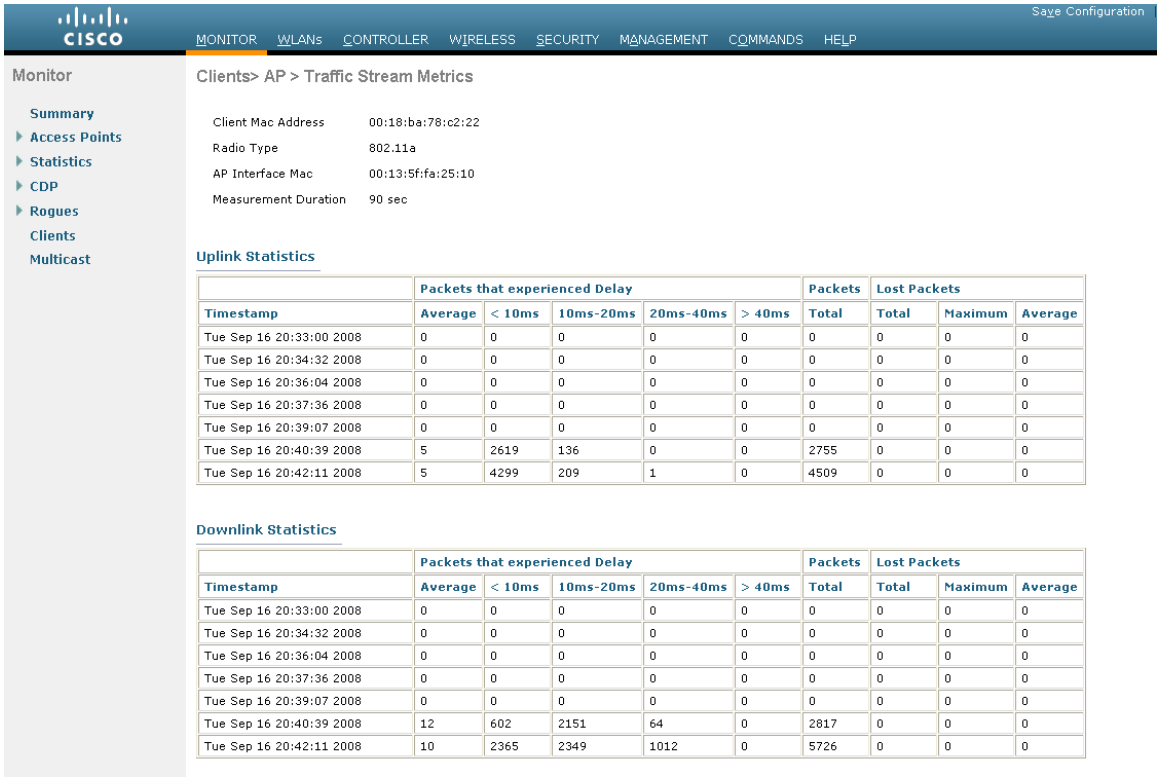
Check the box **Metrics Collection** in the global 802.11 Voice Parameters to enable Traffic Stream Metrics.

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 frequency 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.



	Packets that experienced Delay					Packets	Lost Packets		
Timestamp	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

	Packets that experienced Delay					Packets	Lost Packets		
Timestamp	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

Radio Status Indicator

As of the 1.3(3) release, the Cisco Unified Wireless IP Phone 7921G can help determine whether the radios is functional or not by displaying a number of bars for the signal indicator.

The number of bars equates to the signal received by the access point and will display those bars in either grey, yellow or green depending on the current status.

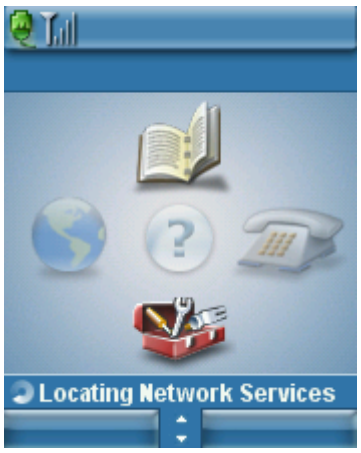
Below the correlation between the color and status are defined.

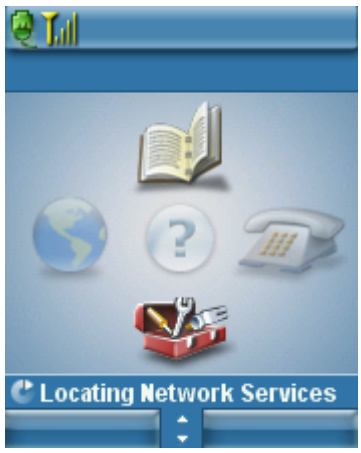
Grey - The phone is in range of some network, but it may not be in range of the configured network.

This could also be due to a SSID configuration issue.

Yellow - The phone has detected it is in range of the configured network and 802.11 band and is attempting to authenticate to the access point. If the indicator does not move to the green status, then there could be an issue with the authentication configuration.

Green - The phone is currently authenticated to the access point.





Hardware Diagnostics

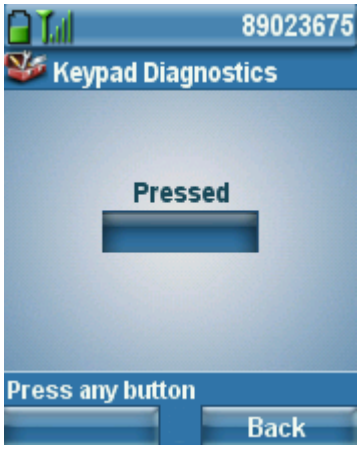
As of the 1.3(4) release, a self-diagnostics tool is now available that can help with hardware analysis.

The **Diagnostics** menu is located under the **Phone Settings** menu, where then the Keypad, Speaker, Microphone and Wireless LAN Radio and Antenna can be validated.

The keypad diagnostics allows for a button to be pressed and released to ensure they are functional.

The audio diagnostics performs an audio loopback, so the speaker and microphone can be validated.

The WLAN diagnostics menu is the standard Site Survey utility, which will use the current network profile information to perform passive and active scans for the configured SSID and 802.11 mode.



Firmware Recovery

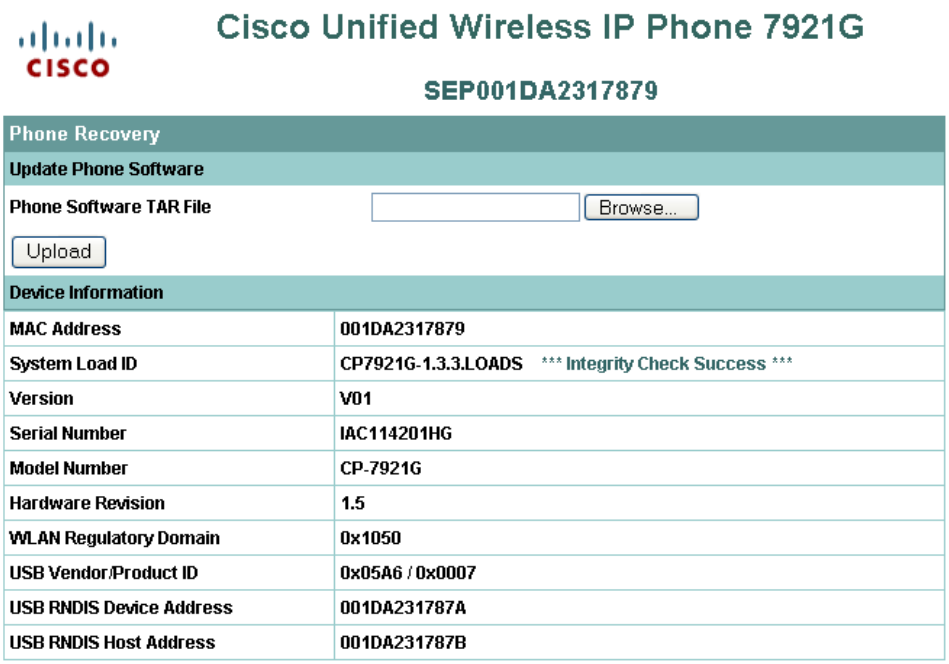
If the Cisco Unified Wireless IP Phone 7921G does no boot properly, then the firmware can be recovered via the USB connection.

Be aware that the current settings will be reset to factory defaults when performing the firmware recovery process.

Use the following steps to perform a firmware recovery.

1. Power on the phone while holding down the application button and the speakerphone button simultaneously and keep it held until **Starting Recovery Mode** is displayed.
2. A firmware check will then be performed.
3. Insert the USB cable into the phone after USB initialization is complete.

   (Ensure that the USB driver has been installed prior and that an IP in the 192.168.1.0 /24 network has been configured for that network connection)
4. When **Web Access Available...** is displayed, then navigate to http://192.168.1.100.
5. Browse to the TAR file and then click **Upload**.



Restoring Factory Defaults

The configuration can be cleared 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.**

Capturing a Screenshot of the Phone Display

The current display can be captured by browsing to http://x.x.x.x/CGI/Screenshot, where **x.x.x.x** is the IP address of the Cisco Unified Wireless IP Phone 7921G. At the prompt enter the username and password for the account for which the phone is associated to.

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.

Carry cases can additionally help protect the phone further and provide drop protection.

Accessories

The following accessories are available 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/docs/voice_ip_comm/cuipph/7921g/5_0/sccp/english/user/accessory/guide/7921Acc2.html

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

3rd Party Accessories

- Headsets www.plantronics.com (Quick Disconnect 2.5 mm Adapter - part # 65287-01)

Note: The Cisco Unified Wireless IP Phone 7921G is unable to utilize accessories from the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, as they are not compatible.

The Cisco Unified Wireless IP Phone 7921G has a 2.5 mm, 3 band / 4 conductor wired headset jack (Nokia compatible).

Additional Documentation

Cisco Unified Wireless IP Phone 7921G Data Sheet
http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/product_data_sheet0900aecd805e315d.html

Cisco Unified Wireless IP Phone 7921G Administration Guide
http://www.cisco.com/en/US/products/hw/phones/ps379/prod_maintenance_guides_list.html

Cisco Unified Wireless IP Phone 7921G User Guide and Quick Reference
http://www.cisco.com/en/US/products/hw/phones/ps379/products_user_guide_list.html

Cisco Unified Wireless IP Phone 7921G Accessory Guide
http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7921g/5_0/sccp/english/user/accessory/guide/7921Acc2.html

Cisco Unified Wireless IP Phone 7921G Release Notes
http://www.cisco.com/en/US/products/hw/phones/ps379/prod_release_notes_list.html

Cisco Unified Wireless IP Phone 7921G Software
http://software.cisco.com/download/type.html?mdfid=280808676

Cisco Unified Communications Manager
http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Cisco Unified Communications Manager Express
http://www.cisco.com/en/US/partner/products/sw/voicesw/ps4625/tsd_products_support_series_home.html

Cisco Voice Software
http://software.cisco.com/download/navigator.html?mdfid=278875240

Cisco Unified IP Phone Services Application Development Notes
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html

Real-Time Traffic over Wireless LAN SRND
http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/RToWLAN/CCVP_BK_R7805F20_00_rtowlan-srnd.html

Cisco Unified Communications SRND
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guides_list.html

Cisco Unified Wireless LAN Controller Documentation
http://www.cisco.com/en/US/partner/products/ps10315/products_installation_and_configuration_guides_list.html

Cisco Autonomous Access Point Documentation
http://www.cisco.com/en/US/partner/docs/wireless/access_point/12.4.25d.JA/Configuration/guide/cg_12_4_25d_JA.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