Cisco Unified Wireless IP Phone 7925G Deployment Guide

The Cisco Unified Wireless IP Phone 7925G 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 utilizing a Bluetooth headset. The Cisco Unified Wireless IP Phone 7925G is Bluetooth 2.0 compatible and supports the headset and handsfree profiles. The Cisco Unified Wireless IP Phone 7925G is IP54 rated protecting it from dust, liquid splashes and moisture.

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

Revision History

Date	Comments
10/13/2008	Initial Version
11/17/2009	1.3(3) Release

Contents

Requirements for the Cisco Unified Wireless IP Phone 7925G

The Cisco Unified Wireless IP Phone 7925G is an IEEE 802.11a/b/g wireless IP phone that provides voice communications in conjunction with these components. Check that your wireless LAN meets the requirements to support the specifications for these phones:

Site Survey

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

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 the 7925G phone always has adequate signal and can roam seamlessly.

Channel Utilization

Channel Utilization levels should be kept under 50%.

If using the 7925G 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.

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 Spectrum Expert

AirMagnet (Survey , WiFi Analyzer, VoFi Analyzer, Spectrum Analyzer)

Cisco Wireless Control System (WCS) for Unified Wireless LAN management

Call Control

For call control, the Cisco Unified Wireless IP Phone 7925G supports only Skinny Client Control Protocol (SCCP) on the following applications:

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

Device Support in Cisco Unified Communications Manager

Cisco Unified Communications Manager requires that you install a device package or service release update in order to enable Cisco Unified Wireless IP Phone 7925G device support.

Cisco Unified Communications Manager 5.1 or higher requires signed COP files.

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

Supported Protocols

Supported voice and wireless LAN protocols include these:

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

Supported Access Points

The Cisco Unified Wireless IP Phone 7925G is supported on both the Cisco autonomous and unified solutions.

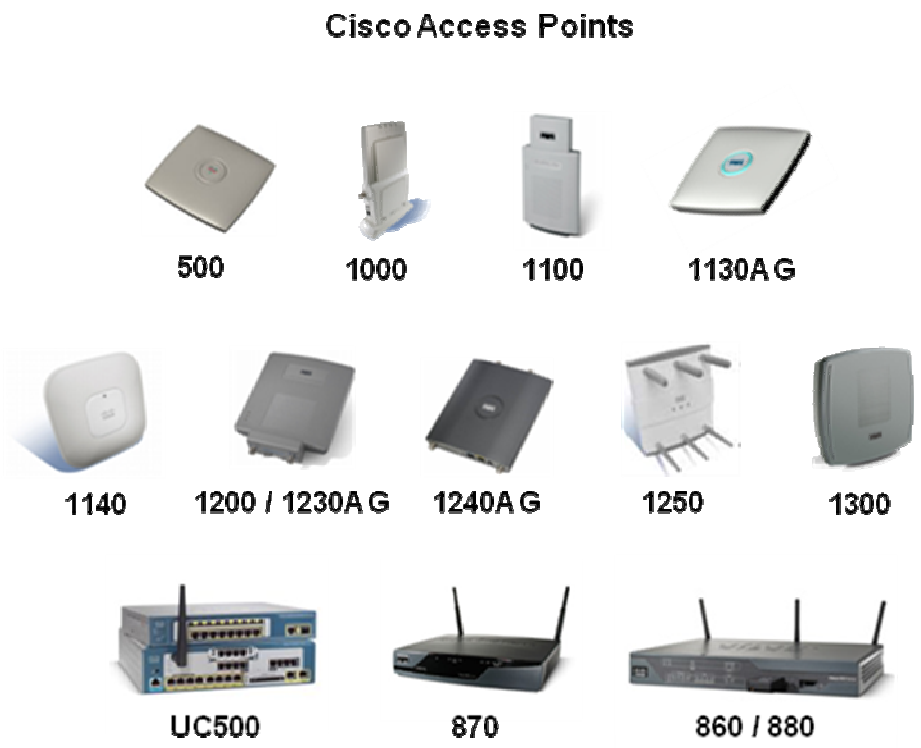
- Cisco Unified Wireless LAN Controller

  Minimum = 4.0.217.0 or later

  Recommended = 5.2.193.0 or later
- Cisco IOS Access Points (Autonomous)

  Minimum = 12.3(8)JEA2 or later

  Recommended = 12.4(10b)JA3 or later (does not apply to 1100, 1140, 1200, 1230)



Note: VoWLAN is not currently supported in conjunction with outdoor MESH technology (1500 series).
3rd party access points are not supported.

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

Cisco Series	802.11b	802.11g	802.11a	Autonomous	Unified
500	Yes	Yes	No	Yes	Yes
1000	Yes	Yes	Yes	No	Yes
1100	Yes	Yes	No	Yes	Yes
1130AG	Yes	Yes	Yes	Yes	Yes

1140	Yes	Yes	Yes	Yes	Yes
1200	Yes	Yes	Optional	Yes	Yes
1230AG	Yes	Yes	Yes	Yes	Yes
1240AG	Yes	Yes	Yes	Yes	Yes
1250	Yes	Yes	Yes	Yes	Yes
1300	Yes	Yes	No	Yes	Yes

Supported 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

Note: The Cisco 1130 and 1140 series access points are to be mounted on the ceiling as they have omni-directional antennas.

Phone Models and Localization

Phone Models

Cisco manufactures four Cisco Unified Wireless IP Phone 7925G models that support the following domains. On the phone, you can identify its domain by pressing **Settings > Model Information > WLAN Regulatory Domain** and referencing the Regulatory Domain number in this list:

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

Regulatory Domain	Part Number	Regulatory Domain Number	Band Range	Available Channels	5 GHz Channel Set
FCC (Americas)	CP-7925G-A-K9	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	 UNII-1 UNII-2 UNII-2 Extended UNII-3
ETSI (Europe)	CP-7925G-E-K9	3051	2.412 – 2.472 GHz 5.180 – 5.700 GHz	13 19	
Japan	CP-7925G-P-K9	4157	2.412 – 2.472 GHz 2.412 – 2.484 GHz 5.180 – 5.700 GHz	13 (OFDM) 14 (CCK) 19	

Rest of World	CP-7925G-W-K9	5252	Uses 802.11d to identify available channels and transmit powers

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

World Mode (802.11d)

If using the Cisco Unified Wireless IP Phone 7925G World (-W) model, then you must enable 802.11d. The Cisco Unified Wireless IP Phone 7925G gives precedence to 802.11d to determine the channels and transmit powers to use and inherits its client configuration from the associated access point.

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

If 802.11d information is not available from the access point, then the phone uses the locally configured regulatory domain. If the Cisco Unified Wireless IP Phone 7925G -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 7925G to operate successfully.

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

The supported countries where the Cisco Unified Wireless IP Phone 7925G is allowed to operate are listed below:

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

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

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

Supported Countries

Below are the countries and their 802.11d codes that are supported by the Cisco Unified Wireless IP Phone 7925G.

Argentina (AR)	India (IN)	Poland (PL)
Australia (AU)	Indonesia (ID)	Portugal (PT)
Austria (AT)	Ireland (IE)	Puerto Rico (PR)
Belgium (BE)	Israel (IL)	Romania (RO)
Brazil (BR)	Italy (IT)	Russian Federation (RU)
Bulgaria (BG)	Japan (JP)	Saudi Arabia (SA)
Canada (CA)	Korea (KR / KP)	Singapore (SG)
Chile (CL)	Latvia (LV)	Slovakia (SK)
Colombia (CO)	Liechtenstein (LI)	Slovenia (SI)
Costa Rica (CR)	Lithuania (LT)	South Africa (ZA)
Cyprus (CY)	Luxembourg (LU)	Spain (ES)
Czech Republic (CZ)	Malaysia (MY)	Sweden (SE)
Denmark (DK)	Malta (MT)	Switzerland (CH)
Estonia (EE)	Mexico (MX)	Taiwan (TW)
Finland (FI)	Monaco (MC)	Thailand (TH)

France (FR)	Netherlands (NL)	Turkey (TR)
Germany (DE)	New Zealand (NZ)	Ukraine (UA)
Gibraltar (GI)	Norway (NO)	United Arab Emirates (AE)
Greece (GR)	Oman (OM)	United Kingdom (GB)
Hong Kong (HK)	Panama (PA)	United States (US
Hungary (HU)	Peru (PE)	Venezuela (VE)
Iceland (IS)	Phillipines (PH)	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

Language Support

The Cisco Unified Wireless IP Phone 7925G currently supports the following languages.

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

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

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

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

Radio Characteristics

Use this table to see the data rates, ranges, and receiver sensitivities for Cisco Unified Wireless IP Phone 7925G depending on the Wi-Fi standard in use.

802.11a	**Data Rate**	**Range**	**Receiver Sensitivity**
Max Tx Power is 16 dBm	6 Mbps	604 ft (184 m)	-91 dBm
	9 Mbps	604 ft (184 m)	-90 dBm
	12 Mbps	551 ft (168 m)	-88 dBm
	18 Mbps	545 ft (166 m)	-86 dBm
	24 Mbps	512 ft (156 m)	-82 dBm
	36 Mbps	420 ft (128 m)	-80 dBm
	48 Mbps	322 ft (98 m)	-77 dBm
	54 Mbps	289 ft (88 m)	-75 dBm
802.11g	**Data Rate**	**Range**	**Receiver Sensitivity**
Max Tx Power is 16 dBm	6 Mbps	709 ft (216 m)	-91 dBm

	9 Mbps	650 ft (198 m)	-90 dBm
	12 Mbps	623 ft (190 m)	-87 dBm
	18 Mbps	623 ft (190 m)	-86 dBm
	24 Mbps	623 ft (190 m)	-82 dBm
	36 Mbps	495 ft (151 m)	-80 dBm
	48 Mbps	413 ft (126 m)	-77 dBm
	54 Mbps	394 ft (120 m)	-76 dBm
802.11b	**Data Rate**	**Range**	**Receiver Sensitivity**
Max Tx Power is 17 dBm	1 Mbps	1,010 ft (308 m)	-96 dBm
	2 Mbps	951 ft (290 m)	-85 dBm
	5.5 Mbps	919 ft (280 m)	-90 dBm
	11 Mbps	902 ft (275 m)	-87 dBm

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

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

Bluetooth

The Cisco Unified Wireless IP Phone 7925G supports Bluetooth Class 2 technology allowing for wireless headset communications. Bluetooth enables low bandwidth wireless connections within a range of 30 feet, however it is recommended to keep the Bluetooth device within 10 feet of the phone.

You can connect up to five headsets, but only the last one connected is used as the default.

The Bluetooth device does not need to be within direct line-of-sight of the phone, but barriers, such as walls, doors, etc. can potentially impact the quality.

Bluetooth utilizes the 2.4 GHz frequency just like 802.11b/g and many other devices (i.e. microwave ovens, cordless phones, etc.), so the Bluetooth quality can potentially be interfered with due to using this unlicensed frequency.

Coexistence (802.11b/g + Bluetooth)

If using Coexistence where 802.11b/g and Bluetooth are used simultaneously, then there are some limitations and deployment requirements to be considered as they both utilize the 2.4 GHz frequency.

Capacity

- When using Coexistence (802.11b/g + Bluetooth), call capacity is reduced due to the utilization of CTS to protect the 802.11g and Bluetooth transmissions.

Multicast Audio

- Multicast audio from Push To Talk (PTT), Music on Hold (MMOH) and other applications are not supported when using Coexistence.

Data Rate Configuration

- It is recommended to only enable 802.11g (OFDM) data rates (i.e. > 12 Mbps) to prevent from engaging in CTS for 802.11g protection when using Coexistence, which can impact voice quality.

Note: It is highly recommended to use 802.11a if using Bluetooth due to 802.11b/g and Bluetooth both utilizing the 2.4 GHz frequency, but also due to the above limitations.

Wireless Security

When deploying a wireless LAN, you must provide security. The Cisco Unified Wireless IP Phone 7925G supports the following wireless security features.

Authentication

- WPA (802.1x authentication + TKIP encryption)
- WPA2 (802.1x authentication + AES 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 (Protected Extensible Authentication Protocol)
- LEAP (Lightweight Extensible Authentication Protocol)
- CCKM (Cisco Centralized Key Management)
- Open and Shared Key

Encryption

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

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

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

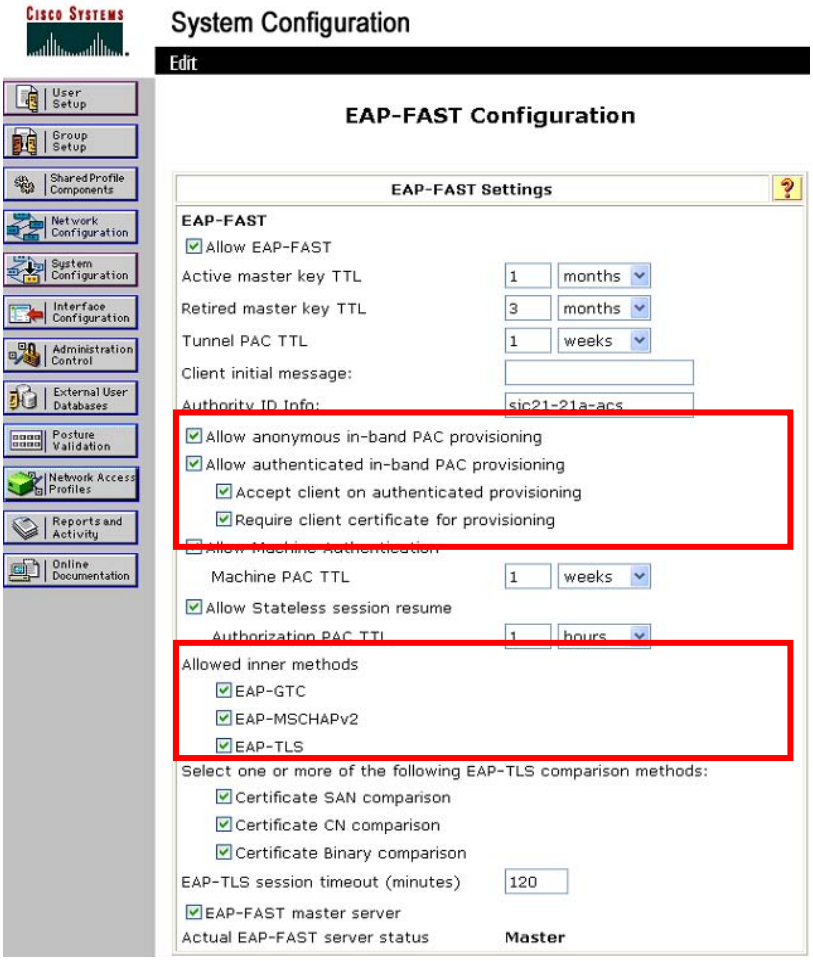
The TLS tunnel uses Protected Access Credentials (PACs) for authentication between the client (phone) and the RADIUS server. The server sends an Authority ID (AID) to the client (phone), which in turn selects the appropriate PAC. The client (phone) returns a PAC-Opaque to the RADIUS server. The server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

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

The Cisco Unified Wireless IP Phone 7925G currently supports only automatic provisioning of the PAC, 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 product wireless LAN environment then a staging Cisco ACS can be setup for initial PAC provisioning of the Cisco Unified Wireless IP Phone 7925G.

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 7925G 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 7925G 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)

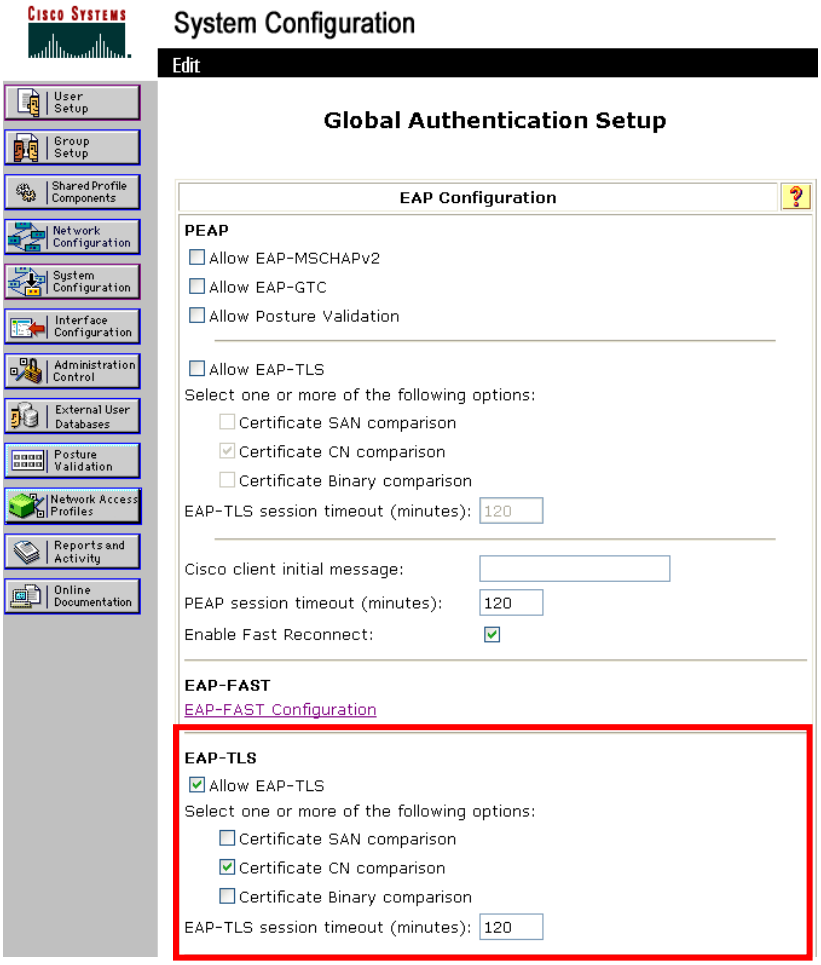
Extensible Authentication Protocol Transport Layer Security (EAP-TLS) is using the TLS protocol with PKI to secure communications to the authentication server.

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.

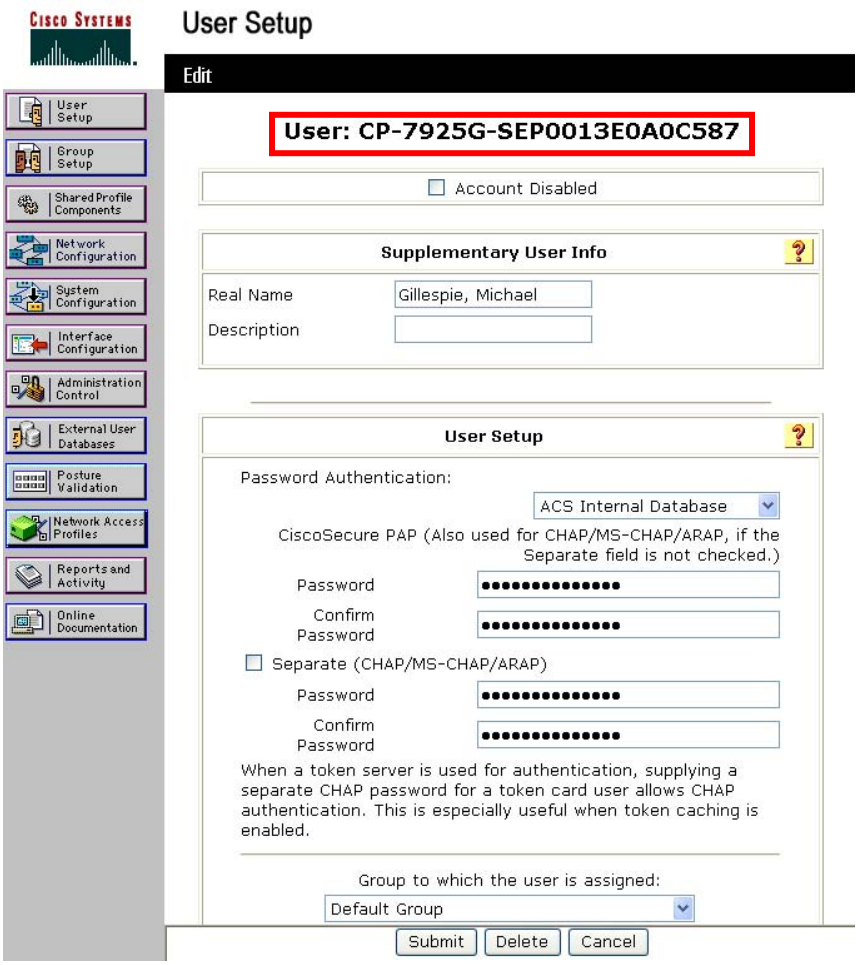
EAP-TLS provides excellent security, but requires client certificate management.

Ensure that **"Certificate CN Comparison"** is selected when enabling EAP-TLS.



EAP-TLS also requires that a user account be created on the authentication server matching the common name of the certificate imported into the Cisco Unified Wireless IP Phone 7925G.

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



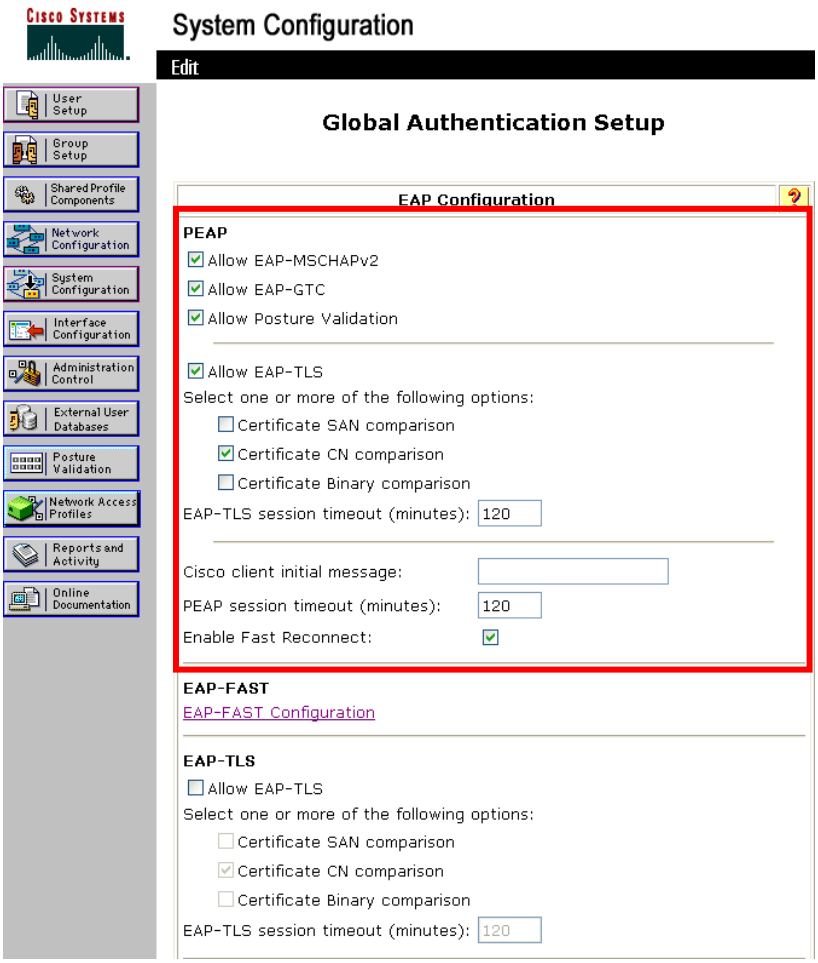
See the "Installing Certificates" section for more information.

Protected Extensible Authentication Protocol (PEAP)

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

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

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



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

The authentication server can be validated via importing a certificate into the Cisco Unified Wireless IP Phone 7925G.

See the "Installing Certificates" section for more information.

Cisco Centralized Key Management (CCKM)

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

The Cisco Unified Wireless IP Phone 7925G supports CCKM with WPA (TKIP) and 802.1x (WEP) authentication.

CCKM with WPA (AES) or WPA2 (TKIP/AES) are not supported at this time.

Authentication	Key Management	Encryption
LEAP	802.1x, WPA	TKIP, WEP (40 or 128 bit)
EAP-FAST	802.1x, WPA	TKIP, WEP (40 or 128 bit)
EAP-TLS	802.1x, WPA	TKIP, WEP (40 or 128 bit)

PEAP	802.1x, WPA	TKIP, WEP (40 or 128 bit)
AKM	802.1x, WPA	TKIP, WEP (40 or 128 bit)

EAP and User Database Compatibility

The following chart indicates which EAP and database configurations are supported by the Cisco Unified Wireless IP Phone 7925G.

Database	LEAP	EAP-TLS	PEAP (MS-CHAPv2)	EAP-FAST (Phase Zero)
ACS	Yes	Yes	Yes	Yes
Windows SAM	Yes	No	Yes	Yes
Windows AD	Yes	Yes	Yes	Yes
LDAP	No	Yes	No	No
ODBC (ACS for Windows only)	Yes	Yes	Yes	Yes
LEAP Proxy RADIUS Server	Yes	No	Yes	Yes
All Token Servers	No	No	No	No

Voice Security

The Cisco Unified Wireless IP Phone 7925G supports the following voice security features.

- Certificates
- Image authentication
- Device authentication
- File authentication
- Signaling authentication
- Secure Cisco Unified SRST
- Media encryption (SRTP)
- Signaling encryption (TLS)
- Certificate authority proxy function (CAPF)
- Secure profiles
- Encrypted configuration files
- Settings Access (can limit user access to configuration menus)
- Locked network profiles
- Administrator password

Power Management

The Cisco Unified Wireless IP Phone 7925G has an option for a standard or extended battery.

The standard battery can provide up to 180 hours standby time or up to 9.5 hours talk time.

The extended battery can provide up to 240 hours standby time or up to 13 hours talk time.

When the access point supports the Cisco Client Extensions (CCX) proxy ARP information element, the idle battery life will be optimized.

When on call U-APSD, PS-POLL, or active mode can be utilized depending on the Cisco Unified Wireless IP Phone 7925G and Access Point configuration.

To extend on call battery life, the Cisco Unified Wireless IP Phone 7925G can use U-APSD or PS-POLL power save methods.

The Cisco Unified Wireless IP Phone 7925G will use either U-APSD or PS-POLL when in idle (no active phone call).

There can be up to 40-50% reduction of battery life when on call and using Coexistence (802.11b/g + Bluetooth).

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	9.5	13
	On Call + Bluetooth	5.5	7
	Idle	180	240
	Idle + Bluetooth Enabled	165	200
5 GHz	On Call	9	11
	On Call + Bluetooth	7	10
	Idle	180	240
	Idle + Bluetooth Enabled	165	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.

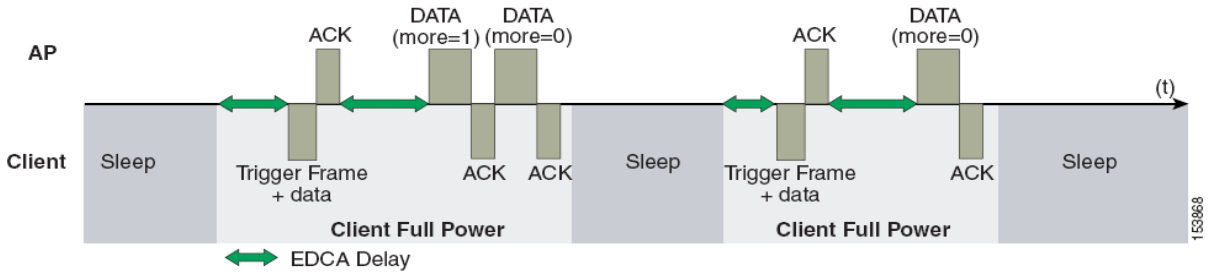
Protocols

Unscheduled Auto Power Save Delivery (U-APSD)

The Cisco Unified Wireless IP Phone 7925G will use U-APSD (Unscheduled Auto Power Save Delivery) for power save when in idle mode or when a phone call is active if WMM is enabled, where U-APSD is supported.

U-APSD helps optimize battery life.

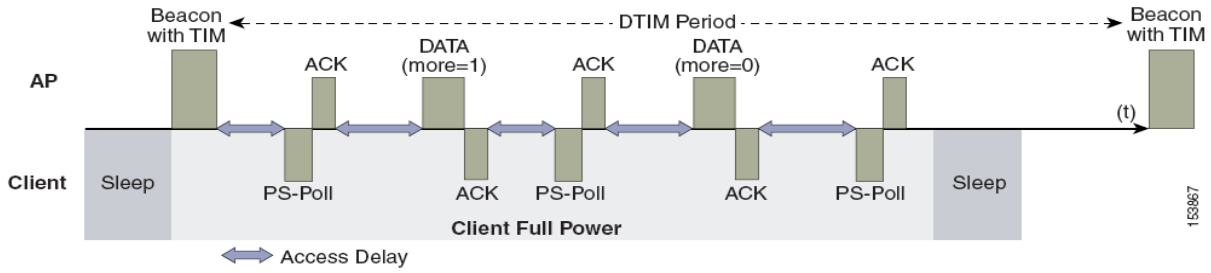
Below is a sample packet sequence when using U-APSD.



Power Save Poll (PS-POLL)

If Wi-Fi MultiMedia (WMM) is disabled, which will disable U-APSD support, or U-APSD support is not available on the access point, then the Cisco Unified Wireless IP Phone 7925G will use PS-POLL for power save when in idle mode and when a phone call is active.

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



Active Mode

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

Delivery Traffic Indicator Message (DTIM)

Increasing the DTIM period can also increase the battery life. The Cisco Unified Wireless IP Phone 7925G can use the DTIM period to schedule wakeup periods to check for broadcast and multicast packets as well as any unicast packets.

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

Scan Modes

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

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

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

Quality of Service (QoS)

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

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

For more information about TCP and UDP ports used by the Cisco Unified Wireless IP Phone 7925G 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/7_1_2/CCM_7.1.2PortList.pdf

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.

Enterprise Parameters Configuration

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

Configuring QoS Policies for the Network

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

Configuring Cisco IOS Access Points

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

```
class-map match-all RTP
 match ip dscp ef
class-map match-all SCCP
 match ip dscp cs3
!
policy-map Voice
 class RTP
  set cos 6
 class SCCP
  set cos 4
!
interface X
 service-policy input Voice
 service-policy output Voice
```

Configuring Cisco Switch Ports

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

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

Note: When using the Cisco Unified Wireless LAN Controller, DSCP trust must be implemented or trust the UDP data ports used by the Cisco Unified Wireless LAN Controller (LWAPP = 12222 and 12223; CAPWAP = 5246 and 5247) on all interfaces where wireless packets will traverse to ensure QoS markings are correctly set. Versions prior to 5.2 use LWAPP, where versions 5.2 and later use CAPWAP.

Configuring Switch Ports for Wired IP Phones

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

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

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

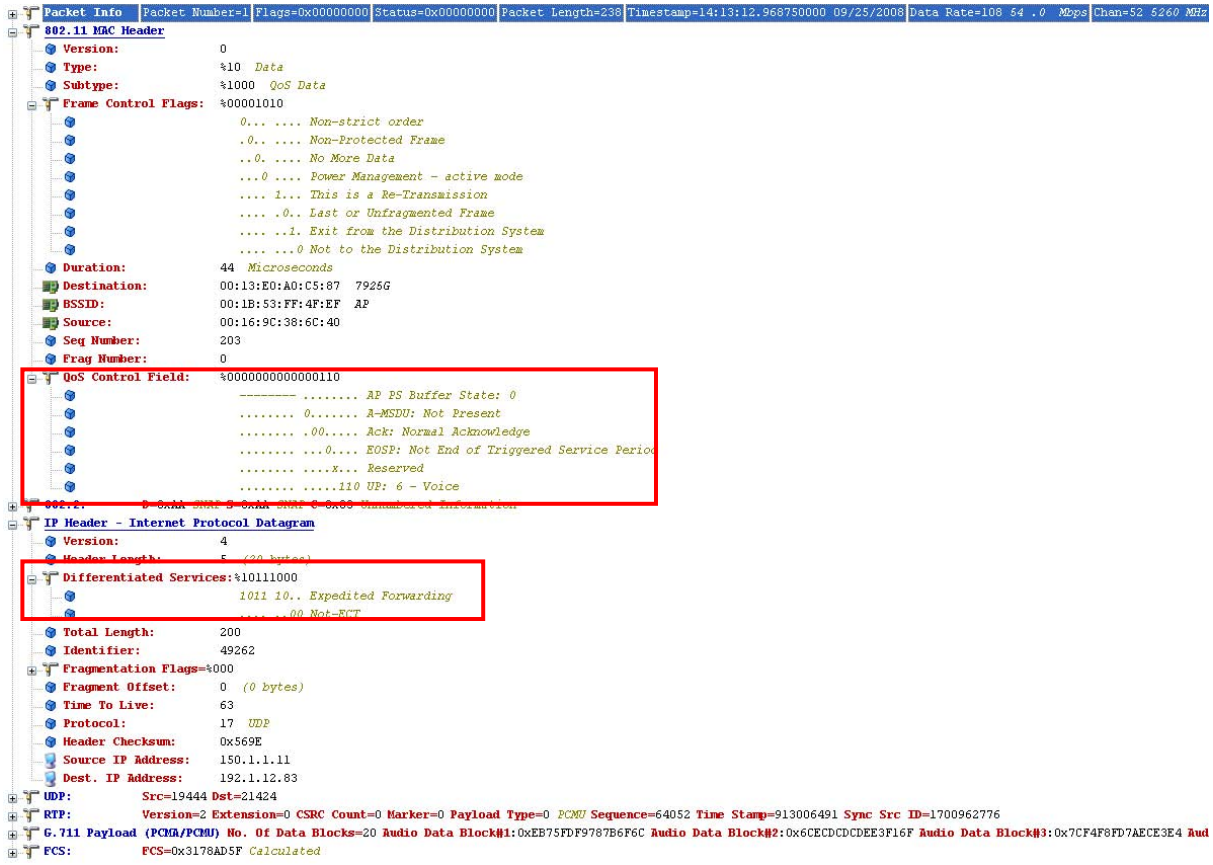
Ensure the following QoS policy is not applied to an interface where wireless traffic traverses.

If using non-secure SCCP, then TCP port 2000 is used. TCP port 2443 is used for secure SCCP.

```
ip access-list extended SCCP
 permit tcp any eq 2000 any
 permit tcp any any eq 2000
permit tcp any eq 2443 any
 permit tcp any any eq 2443
!
ip access-list extended RTP
 permit udp any range 16384 32767 any
 permit udp any any range 16384 32767
!
class-map match-all SCCP
 match access-group name SCCP
class-map match-all RTP
 match access-group name RTP
!
policy-map Voice
 class RTP
  set dscp ef
!
 class SCCP
  set dscp cs3
!
interface X
 service-policy input Voice
 service-policy output Voice
```

Sample Voice Packet Capture

This packet capture below shows that RTP packets bound for the Cisco Unified IP Phone 7925G over the air should be marked with DSCP = EF and COS = 6.



Call Admission Control

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

- Enable Call Admission Control / Wi-Fi MultiMedia Traffic Specifications (TSPEC)
- Set the desired maximum RF bandwidth that is allocated for voice traffic (default = 75%)
- Set the bandwidth that is reserved for roaming clients (default = 6%)

You can modify the minimum PHY rate for the phone 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 one of these rates are enabled.

As of the 1.3(3) release, the Cisco Unified Wireless IP Phone 7925G will auto-negotiate the minimum PHY rate to be used for TSPEC. By default it will try the locally configured minimum PHY rate (i.e. 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 7925G would use the static minimum PHY rate configured locally.

If 12 Mbps is not enabled on the access point, you must ensure that the next highest data rate is 24 Mbps (which is supported). 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.

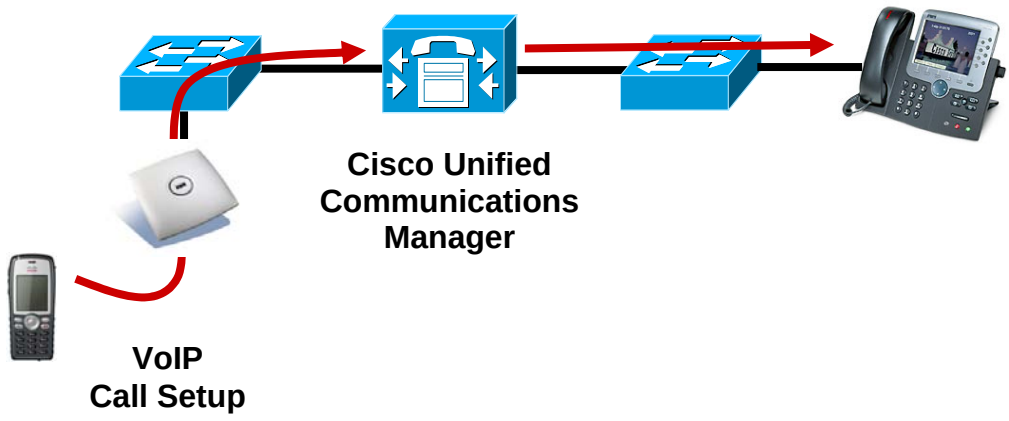
The dynamic minimum PHY rate is useful for deployments that require higher capacity where 24 Mbps and higher data rates are only enabled. For this high capacity deployment configuration and with release 1.3(3), the minimum PHY rate would be adjusted to 24 Mbps automatically even if the phone is configured 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 date 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.

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

Pre-Call Admission Control

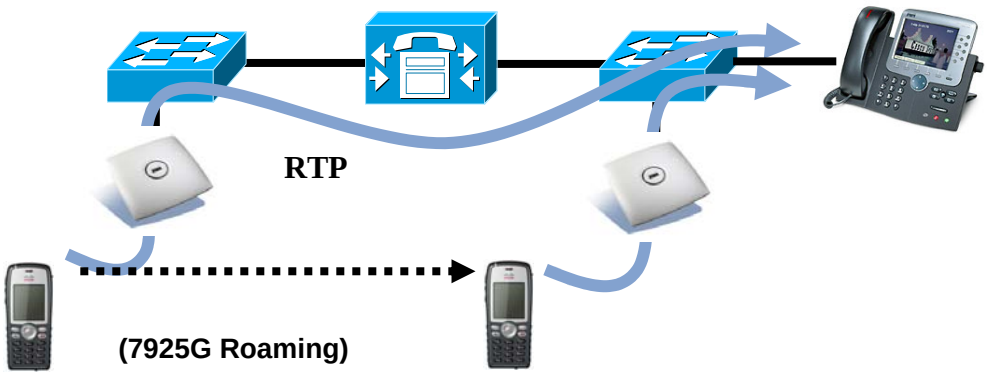
If Call Admission Control (TSPEC) is enabled on the access point, the Cisco Unified Wireless IP Phone 7925G sends an Add Traffic Stream (ADDTS) to the access point to request bandwidth in order to place or receive a call. If the AP sends an ADDTS successful message then the Cisco Unified Wireless IP Phone 7925G establishes the call. If the call is rejected by the access point and the wireless IP phone has no other access point to roam to, then phone displays **"Network Busy"**.



Roaming Admission Control

During a call, the Cisco Unified Wireless IP Phone 7925G measures Received Signal Strength Indicator (RSSI), QoS Basic Service Set (QBSS), and Packet Error Rate (PER) values for the current and all available access points to make roaming decisions.

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



For more information about Call Admission Control and QoS, refer to the “Cisco Unified Wireless Quality of Service” chapter in the *Enterprise Mobility Design Guide* at this URL:
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns279/c649/ccmigration_09186a00808d9330.pdf

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.

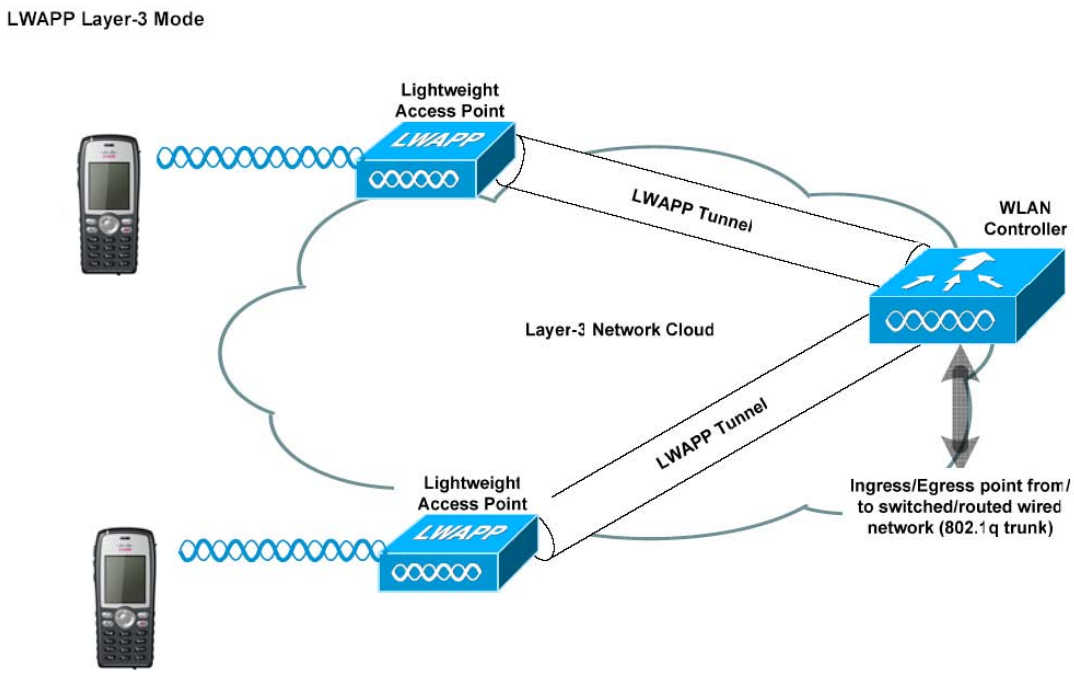
TCLAS is supported in the Cisco Unified Wireless LAN Controller release 5.1.151.0 and later.

Using port based QoS policies is inadequate as all data packets use the same UDP port (LWAPP = 12222; 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.



Multicast

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

The Cisco Unified Wireless IP Phone 7925G uses the DTIM period to receive the queued broadcast and multicast packets.

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

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

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

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

The Cisco Unified Wireless IP Phone 7925G 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.

Note: If using Coexistence where 802.11b/g and Bluetooth are being used simultaneously, then multicast voice is not supported.

Designing the Wireless LAN for Voice

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

For more information about these topics, refer to the "VoWLAN Design Recommendations" chapter in the *Enterprise Mobility Design Guide* at this URL:
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns279/c649/ccmigration_09186a00808d9330.pdf

Planning Channel Usage

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

5 GHz (802.11a)

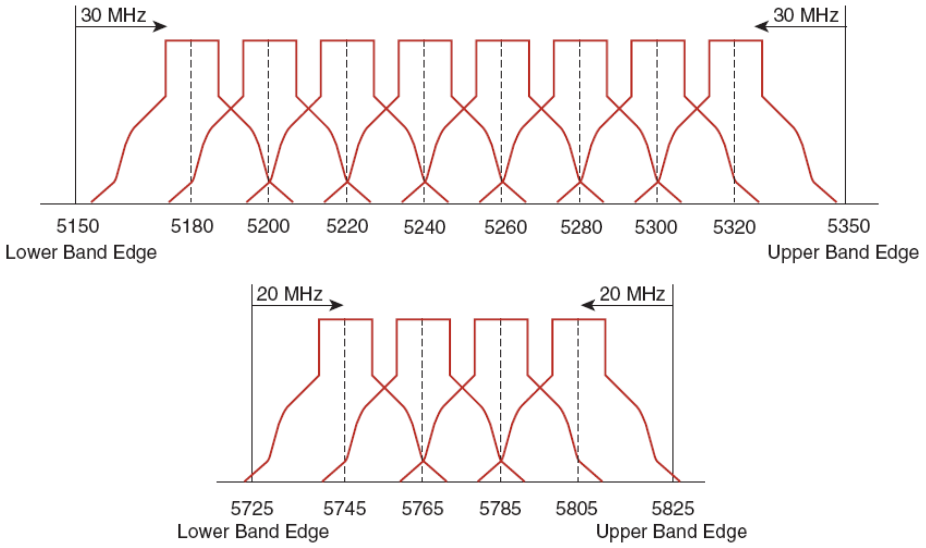
The Cisco Unified Wireless IP Phone 7925G supports Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) from 802.11h, which are required when using channels operating at 5.25 - 5.725 GHz, which is 15 of the 23 possible channels.

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

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

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

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



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

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

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

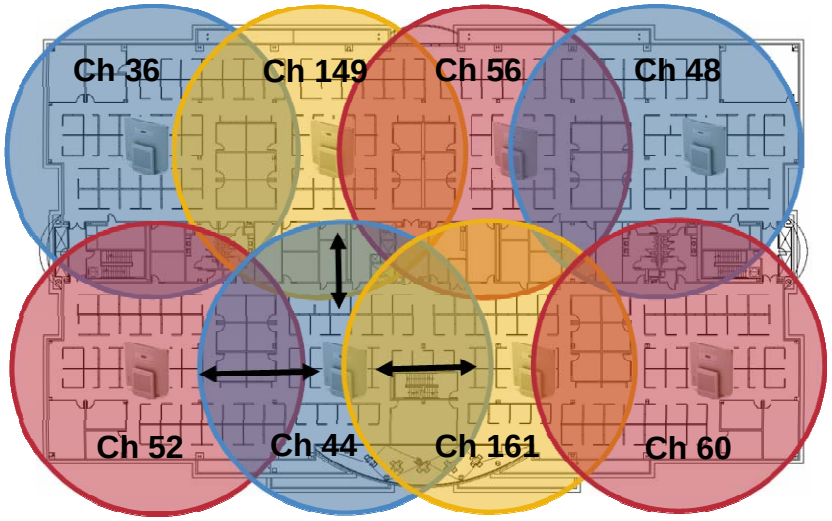
In case of radar activity, have at least one access point per area that uses a non-DFS channel (UNII-1). This ensures that a channel is available when an access point's radio is in its hold-off period while scanning for a new usable channel.

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

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

A UNII-3 channel (5.745 - 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.



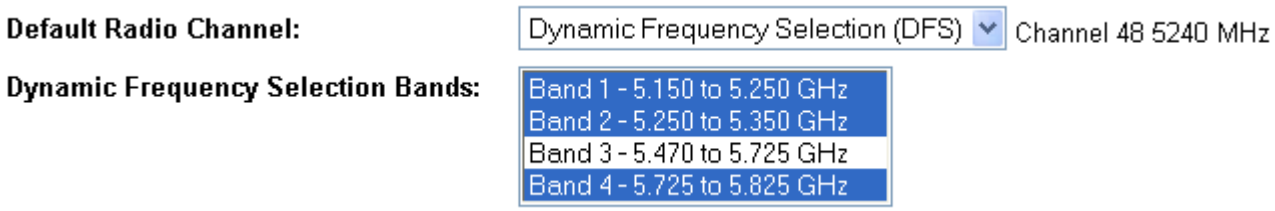
Minimum 20% Overlap

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

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

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

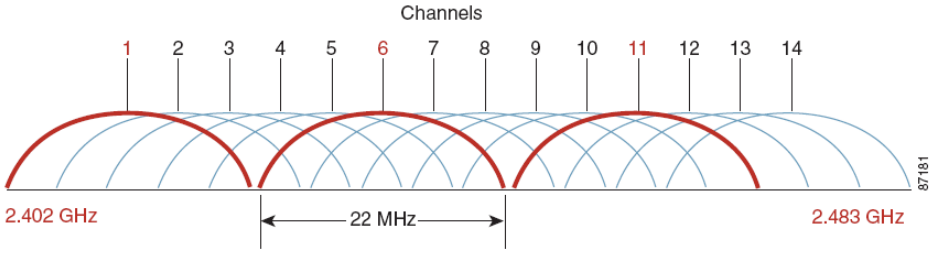
Having many 5 GHz channels enabled in the wireless LAN can delay discovery of new access points.



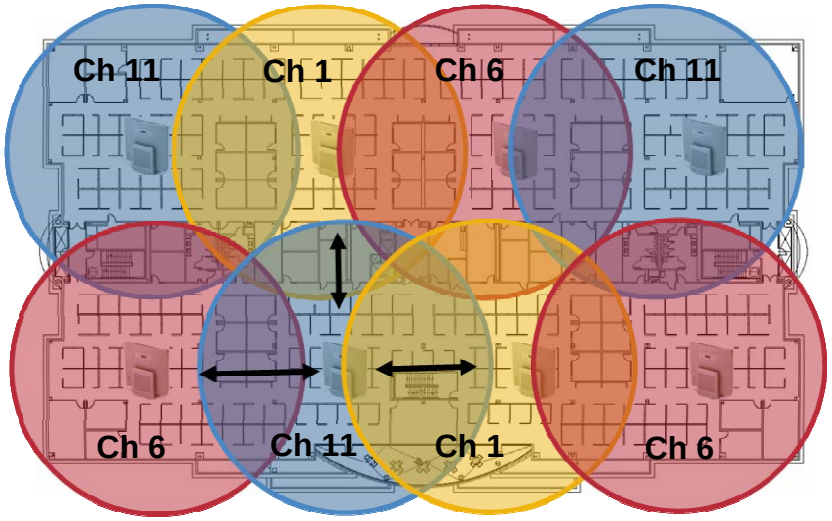
2.4 GHz (802.11b/g)

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

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



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



Minimum 20% Overlap

Signal Strength and Coverage

To ensure acceptable voice quality, the Cisco Unified Wireless IP Phone 7925G should always have a signal of -67 dBm or higher when using 2.4 or 5 GHz and ensure the Packet Error Rate (PER) is no higher than 1%.

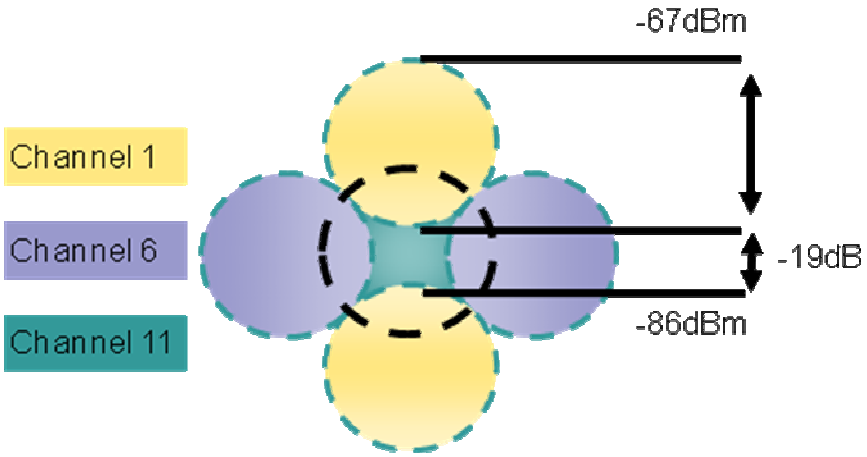
A minimum Signal to Noise Ratio (SNR) of 25dB = -92dBm noise level with -67 dBm signal should be maintained.

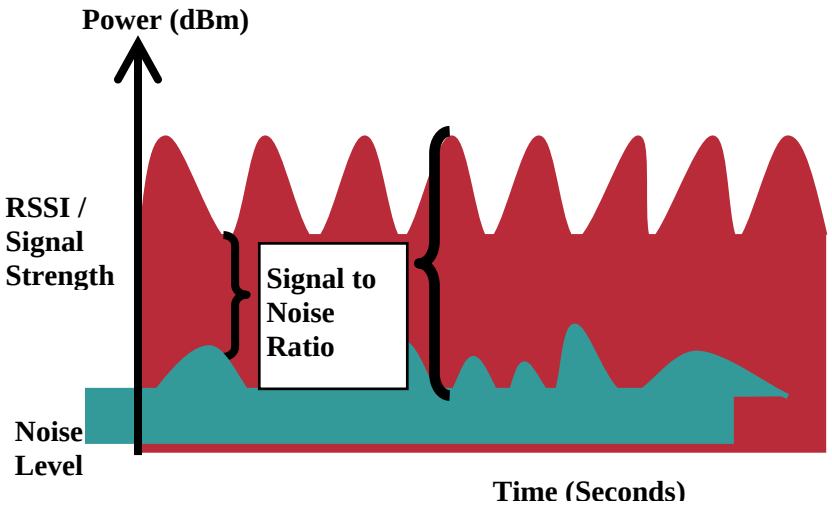
It is recommended to have at least two access points on non-overlapping channels with at least -67 dBm signal with the 25 dB SNR to provide redundancy.

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.

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

For more information about signal strength and cell edge design, refer to the "VoWLAN Design Recommendations" chapter in the *Enterprise Mobility Design Guide* at this URL:
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns279/c649/ccmigration_09186a00808d9330.pdf





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

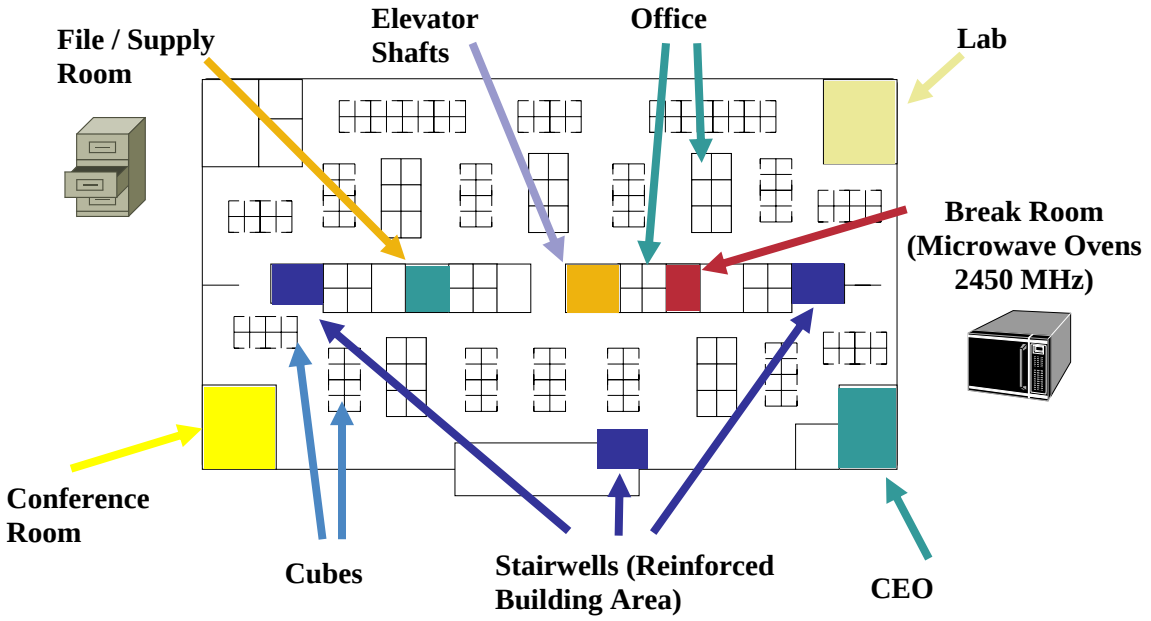
Typical wireless LAN deployments for data only applications do not provide coverage for some areas where VoWLAN service is necessary such as elevators, stairways, and outside corridors.

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

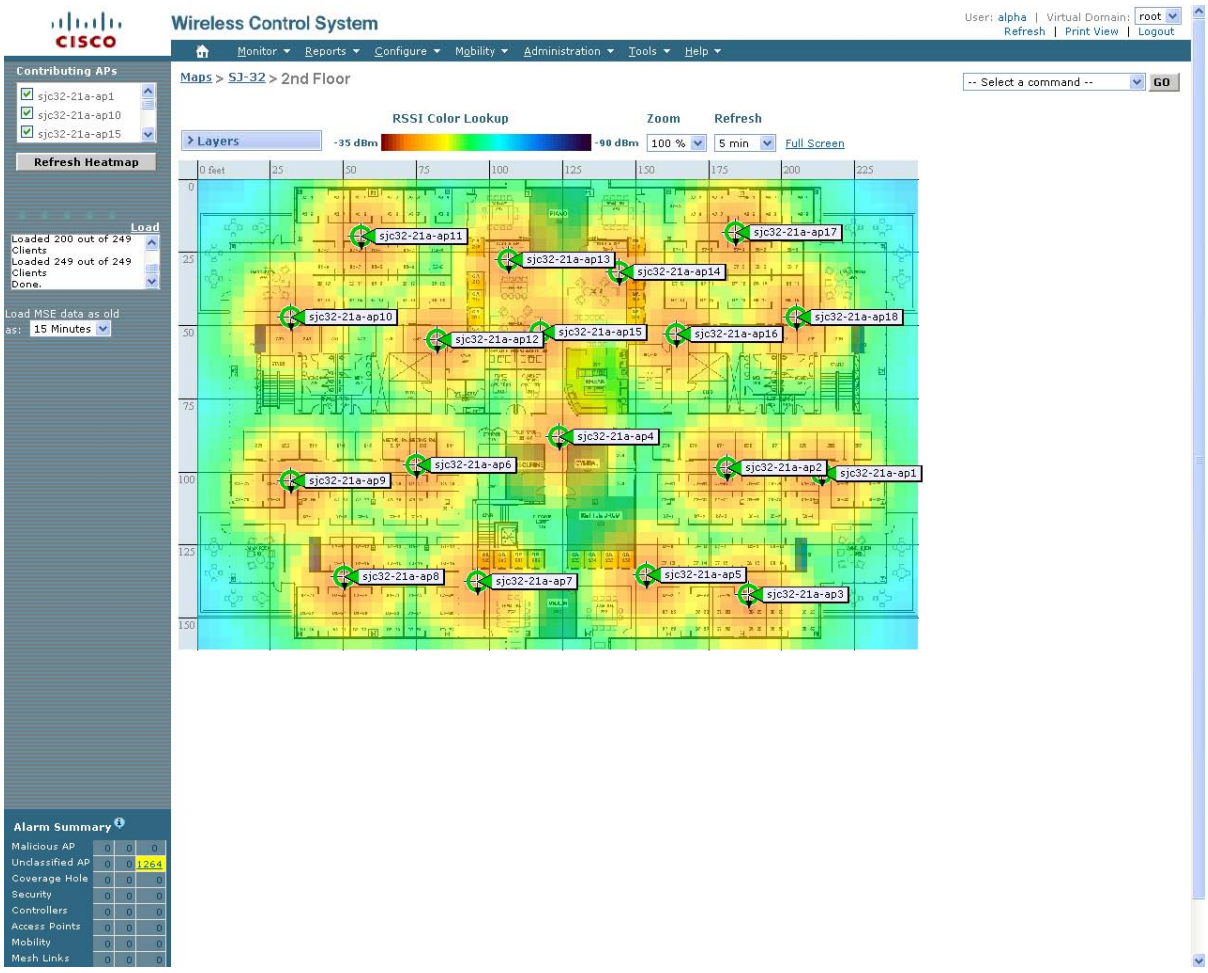
Microwave ovens operate on 2450 MHz, which is between channels 8 and 9 of 802.11b/g. Some microwaves are shielded more than others and that shielding reduces the spread of the energy. Microwave energy can impact channel 11, and some microwaves can affect the entire frequency range (channels 1 through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

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

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



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



Roaming

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

The Cisco Unified Wireless IP Phone 7925G supports CCKM with WPA (TKIP) and 802.1x (WEP) authentication.

CCKM with WPA (AES) or WPA2 (TKIP/AES) are not supported as of the 1.3(3) release.

Authentication	Roaming Time
Open	< 100 ms
802.1x	300 ms
WPA Personal	400 ms
WPA Enterprise	400 – 500 ms
CCKM	< 100 ms

Configuring Data Rates

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

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

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

If using Coexistence where 802.11b/g and Bluetooth are being used simultaneously, then the data rates below 11 Mbps should be disabled. 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.

The recommended data rate configuration is the following:

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

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 to enable these rates for a voice application.

Enabling these rates could potentially increase the number of retries for a data frame.

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

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

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

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

If Call Admission Control (TSPEC) is enabled then the Traffic Stream Rate Set (TSRS) feature will also be enabled, which will allow lower rates to be enabled for legacy devices, but prevent the Cisco Unified Wireless IP Phone 7925G to transmit at rates below 12 Mbps for 802.11a and 11 Mbps for 802.11b/g, while also allow set the ceiling data rate to a more reliable data rate (24 Mbps). Disallowing packets to be transmitted at lower rates preserves capacity. Sending voice frames at a more reliable rate initially can potentially reduce the number of retries of a data 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 Restricted Data Rates options on the Cisco Unified Wireless IP Phone 7925G in order to utilize the TSRS feature.

Call Capacity

Design the network to accommodate the desired call capacity.

The Cisco Access Point can support up to 27 bi-directional RTP streams for both 802.11a and 802.11g at a data rate of 24 Mbps or 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 or 802.11g + Bluetooth Disabled	6 Mbps
20	802.11a or 802.11g + Bluetooth Disabled	12 Mbps
27	802.11a or 802.11g + Bluetooth Disabled	24 – 54 Mbps

When using Coexistence (802.11b/g + Bluetooth), call capacity is reduced to the following:

Max # of Streams	802.11 Mode	Data Rate
4	802.11b/g + Bluetooth Enabled	11, <12-54> Mbps
7	802.11g + Bluetooth Enabled	12, <18-54> Mbps

Note: It is highly recommended to use 802.11a if using Bluetooth.

Prior to release 1.3(2), only 2 bi-directional RTP streams were supported when using Coexistence.

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

Dynamic Transmit Power Control (DTPC)

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

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

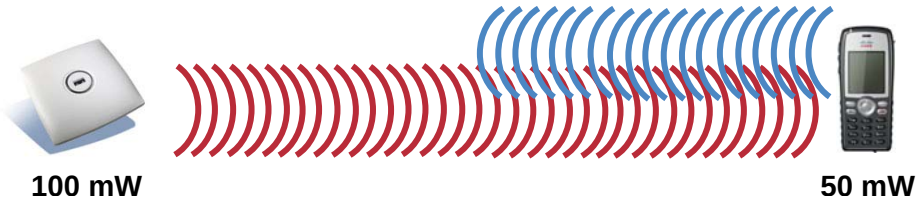
Do not use default setting of Max power for client power on Cisco autonomous access points as that will not advertise DTPC to the client.

If the access point does not support DTPC, then the Cisco Unified Wireless IP Phone 7925G will use the highest available transmit power depending on the current 802.11 mode and data rate.

The transmit power on the Cisco Unified Wireless IP Phone 7925G can also optionally be configured to match the highest transmit power of an access point in the wireless LAN. This setting prevents one-way audio when RF traffic is heard in one direction only.

By default the Cisco Unified Wireless IP Phone 7925G will use the highest available transmit power by default (i.e. 17 dBm / 50 mW for 2.4 GHz and 16 dBm / 40 mW for 5 GHz).

The access point's radio transmit power should not have a transmit power greater than what the Cisco Unified Wireless IP Phone 7925G can support.



Multipath

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

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

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

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

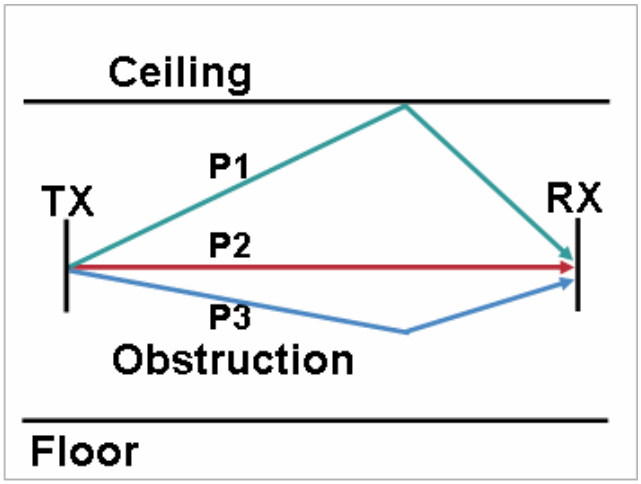
Below is a list of multipath effects:

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

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

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

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



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

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

Use of antenna diversity can also help in such environments.

Verification with Site Survey Tools

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

- Cisco Wireless Control System (WCS) for Unified Wireless LAN management
- Cisco Wireless LAN Solution Engine (WLSE) for Autonomous Wireless LAN management
- Cisco Spectrum Expert
- AirMagnet (Survey , WiFi Analyzer, VoFi Analyzer, Spectrum Analyzer)
- Cisco Unified Wireless IP Phone 7925G

Cisco 7925G Neighbor List

The Cisco Unified Wireless IP Phone 7925G can be utilized to verify coverage by using the Neighbor List menu.

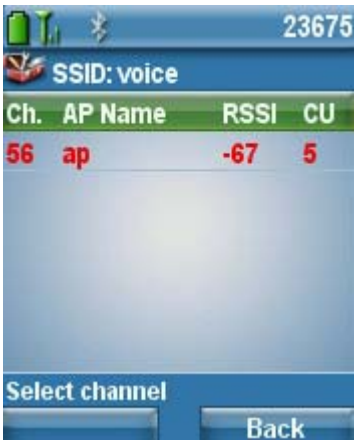
By Default, the Cisco Unified Wireless IP Phone 7925G only scans when the current signal lowers to a certain threshold, so you may see only one access point in the list if configured for auto scan mode.

To see all access points in the neighbor list menu, place a call from the Cisco Unified Wireless IP Phone 7925G to a wired IP phone, where scanning occurs constantly while the phone call is active in auto scan mode.

Otherwise configure continuous scan mode.

The connected access point will be highlighted in red.

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



Cisco 7925G Site Survey

The Cisco Unified Wireless IP Phone 7925G also has a Site Survey application, 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.

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

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

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

AP:	sjc21-21a-air12
MAC:	00:19:07:8D:5A:DE
Observation Count:	463
Channel - Frequency:	64 - 5320000hz
Country:	US
Beacon Interval:	100
DTIM Period:	2
RSSI Range [Lo Hi]:	[-73 -43]
BSS Lost Count:	0
Channel Utilization:	2
Station Count:	1
Available Admission Capacity:	23437
Warning Flags:	100000
Basic Rates:	6
Optional Rates:	9 12 18 24 36 48 54
Multicast Cipher:	TKIP
Unicast Ciphers:	TKIP
AKM:	WPA1_1X WPA1_CCKM
Proxy ARP supported:	Yes
WMM Supported:	Yes
CCX Version Number:	5
U-APSD Supported:	Yes

Background AC(1)			
Admission Control Required:	No		
AIFSN	ECWMin	ECWMax	TXOpLimit
7	4	10	0

Best Effort AC(0)			
Admission Control Required:	No		
AIFSN	ECWMin	ECWMax	TXOpLimit
3	4	10	0

Video AC(2)			
Admission Control Required:	No		
AIFSN	ECWMin	ECWMax	TXOpLimit
2	3	4	94

Voice AC(3)			
Admission Control Required:	Yes		
AIFSN	ECWMin	ECWMax	TXOpLimit
2	2	3	47

Channels	36	40	44	48	52	56	60	64	100	104	108	112	116	132	136	140	149	153	157	161
Power	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20

Data rates less then 11mb/s are not recommended.

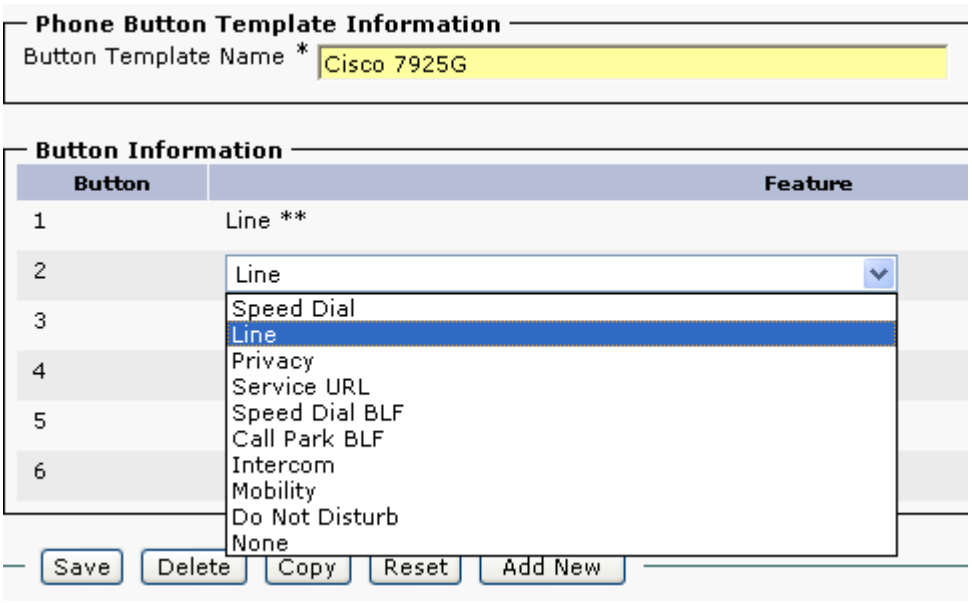
Configuring Cisco Unified Communications Manager

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

Phone Button Templates

The Cisco Unified Wireless IP Phone 7925G supports 6 lines. The default phone button template includes support for 2 lines and 4 speed dials.

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



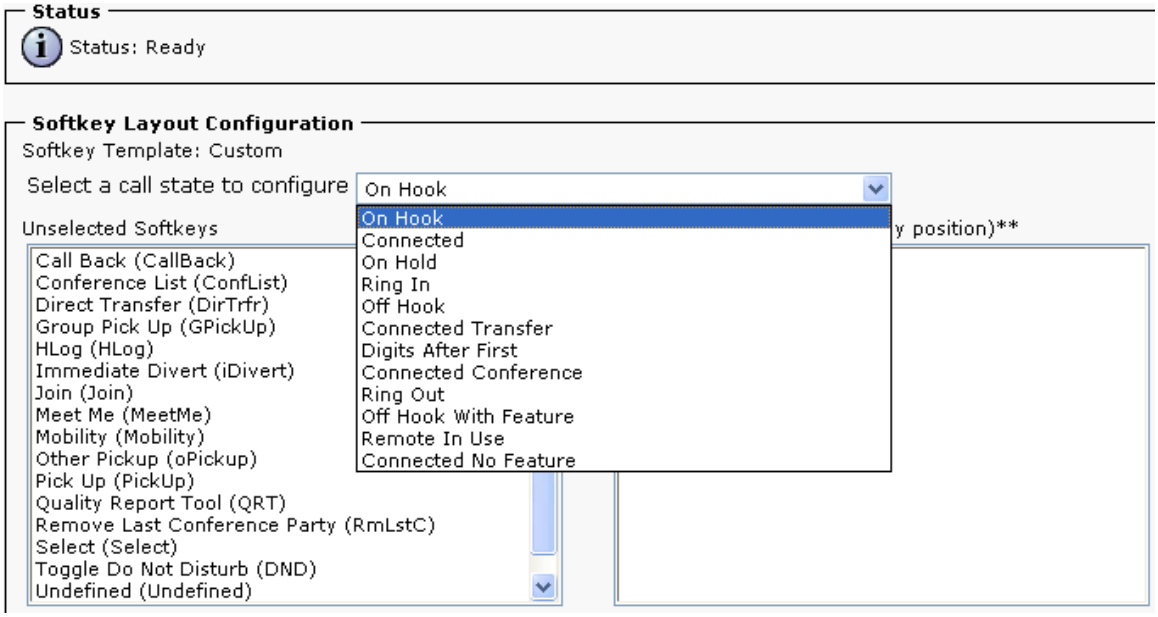
Softkey Templates

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 7925G has 2 softkeys available. The feature listed first in the softkey template will be displayed on the left softkey if on a call, where the other features will be listed under the options menu on the right softkey.

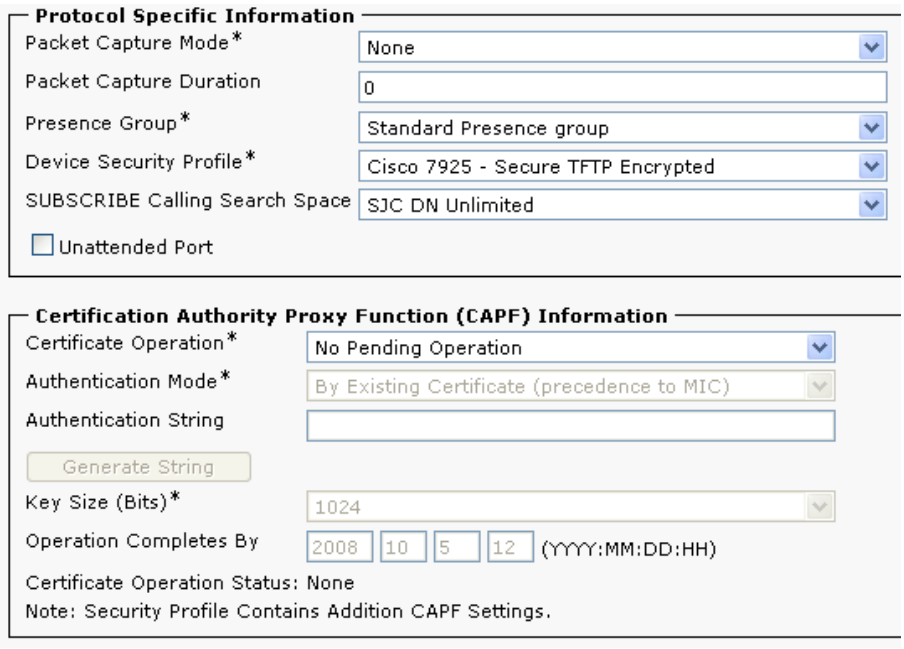


Security Profiles

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

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

Each Cisco Unified Wireless IP Phone 7925G has a Manufactured Installed Certificate (MIC).

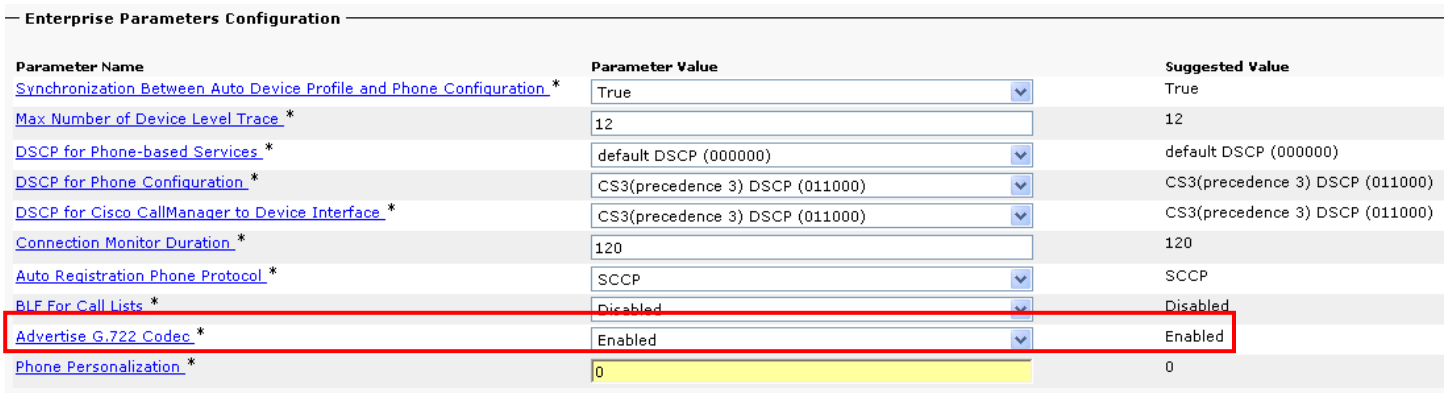


G.722 Advertisement

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

Earlier versions of Cisco Unified Communications Manager do not have this capability, where a Cisco Unified Wireless IP Phone 7925G 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 for each Cisco Unified Wireless IP Phone 7925G.



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

Product Specific Configuration Options

On the IP Phone Configuration page in Cisco Unified Communications Manager Administration, these Cisco Unified Wireless IP Phone 7925G configuration options are available.

For an explanation 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.

Below are the default settings when adding a phone.

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 (i.e. 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 (i.e. 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. (I.e. 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"** (i.e. 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.
Phone Book Web Access	Phone book web access must be set to **"Allow Admin"** in order to access the phone book via the web page.
Unlock-Settings Sequence	By default, **# must be entered to unlock a menu that contains configurable items, which can optionally be disabled.
Application Button Activation Timer	The activation timer and priority of the application button can also be specified. This determines how long the button must be pressed and held to activate.
Application Button Priority	If the priority is low, then will only function when the keypad is unlocked and on the home screen. Medium priority will allow the application button to function when in any menu or XML screen and high priority will allow the application button to function when in any state including keypad lock.
Out of Range Alert	An out of range alert can be configured to beep once or periodically to audibly notify the user that they have traveled out of the coverage area.

Scan Mode	Scan mode allows for auto, continuous, and single AP options, where auto primarily scans only when on call and single AP only at power on.
Restricted Data Rates	The restricted data rates feature utilizes the Traffic Stream Rate Set (TSRS) information element from CCX v4, which can define a data range (upper and lower) for the client to use (i.e. 12 - 24 Mbps). This can be beneficial for environments that have legacy clients requiring lower data rates to be enabled on the access point, but also preventing other clients from downshifting to lower rates, which lowers overall throughput and capacity. When enabled the Cisco Unified Wireless IP Phone 7925G will not transmit below 12 Mbps for 802.11a and 11 Mbps for 802.11b/g.
Power Off When Charging	Power off when charging feature will power off the phone when placed on AC power.
Cisco Discover Protocol (CDP)	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 7925G 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.

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 5.1, 6.0, 6.1, 7.0 or later and web access is set to **"Full"**, then it is recommended to enable TFTP encryption via the device security profile.

To configure product specific configuration options for the Cisco Unified Wireless IP Phone 7925G 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	(i.e. Cisco)
Special Numbers	specialNumbers	(i.e. 411,911)
Application URL	PushToTalkURL	http://x.x.x.x
"Send" Key Action	sendKeyAction	0 = Onhook Dialing; 1 = Offhook Dialing
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
Restricted Data Rates	restrictDataRates	0 = Disabled; 1 = Enabled
Power Off When Charging	powerOffWhenCharging	0 = Disabled; 1 = Enabled
Cisco Discover Protocol (CDP)	cdpEnable	0 = Disabled; 1 = Enabled
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
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.

For more information on these features, see the *Cisco Unified Wireless IP Phone 7925G Administration Guide* or the Cisco Unified Wireless IP Phone 7925G 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

Enable individual phone configuration files with the following commands.

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

Configuring the Cisco Unified Wireless LAN Controller and Access Points

When configuring your access points, use these guidelines:

- Set **"Quality of Service (QoS)"** to **"Platinum".**
- Ensure the **"WMM Policy"** is set to **"Allowed"** or **"Required"**
- Ensure **"Aironet IE"** is enabled
- Disable **"P2P (Peer to Peer) Blocking Action"** / **"Public Secure Packet Forwarding (PSPF)"**
- Disable **"DHCP Address Assignment"**
- Ensure **"MFP Client Protection"** is set to disabled or optional
- Ensure **"Admission Control Mandatory"** is **"Enabled"** for Voice
- Ensure **"Load Based CAC"** is **"Enabled"** for Voice
- Ensure **"Admission Control Mandatory"** is **"Disabled"** for Video
- Ensure the **"EDCA Profile"** is set to **"Voice Optimized"**
- Ensure **"Enable Low Latency MAC"** is disabled
- Ensure **"Aggressive Load Balancing"** is disabled
- Enable **"Symmetric Mobile Tunneling Mode"** if Layer 3 mobility is being used
- Ensure **"ARPUnicast"** is disabled, where proxy ARP will then be enabled
- Ensure that **"DTPC"** is **"Enabled"**
- Enable **"Short Preamble"** if using 2.4 GHz

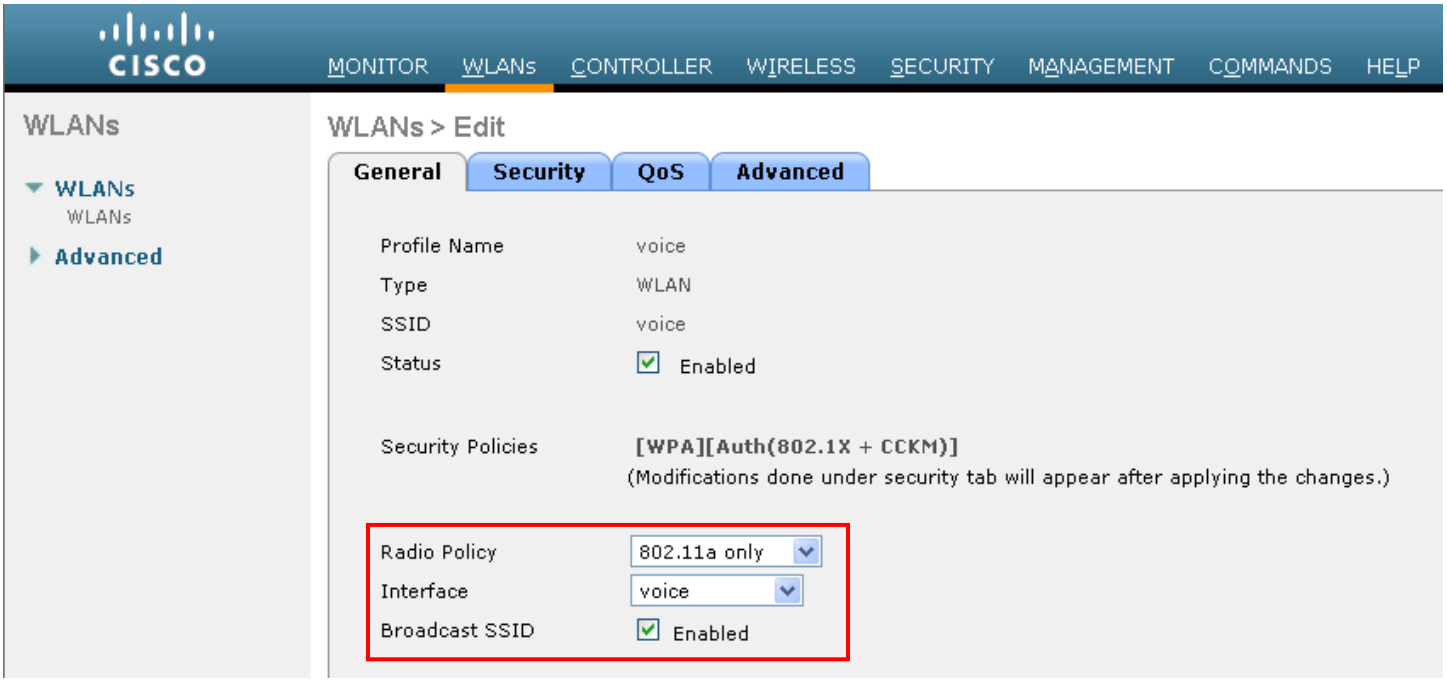
Note: If you have clients from other regions that will attempt to associate with the wireless LAN, then ensure that World Mode (802.11d) is enabled.

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

SSID / WLAN Settings

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

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

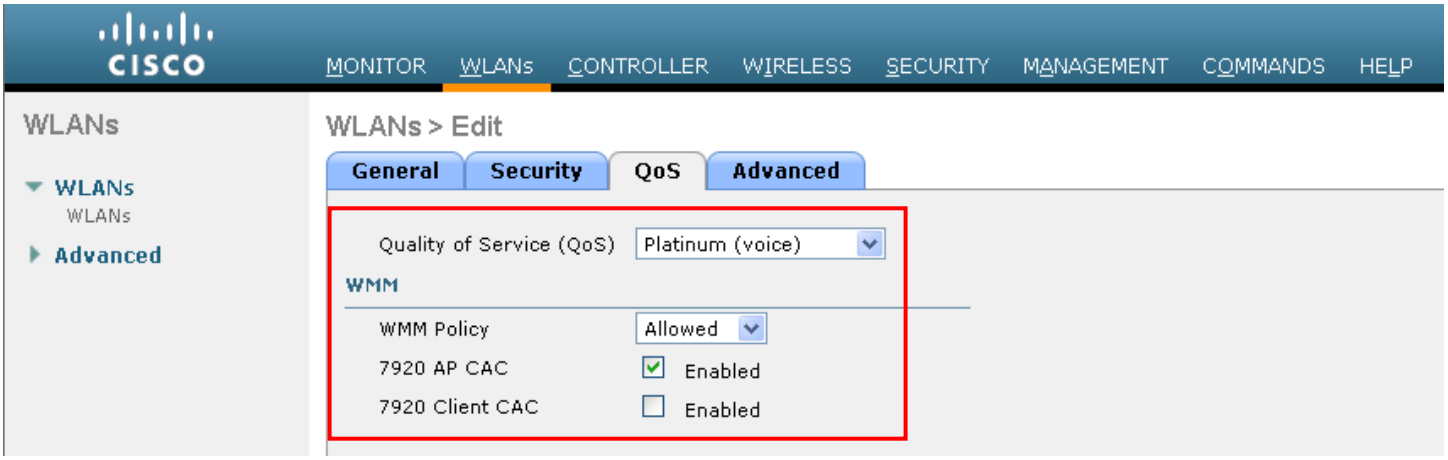


Enable WPA policy with TKIP in order to use CCKM, when 802.1x authentication is used.

The WMM policy can be set to **"Required"** if only the Cisco Unified Wireless IP Phone 7925G or other WMM enabled phones will be using this SSID.

If 7920 or other non-WMM clients will associate using this SSID, then ensure the WMM policy is set to **"Allowed".**

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



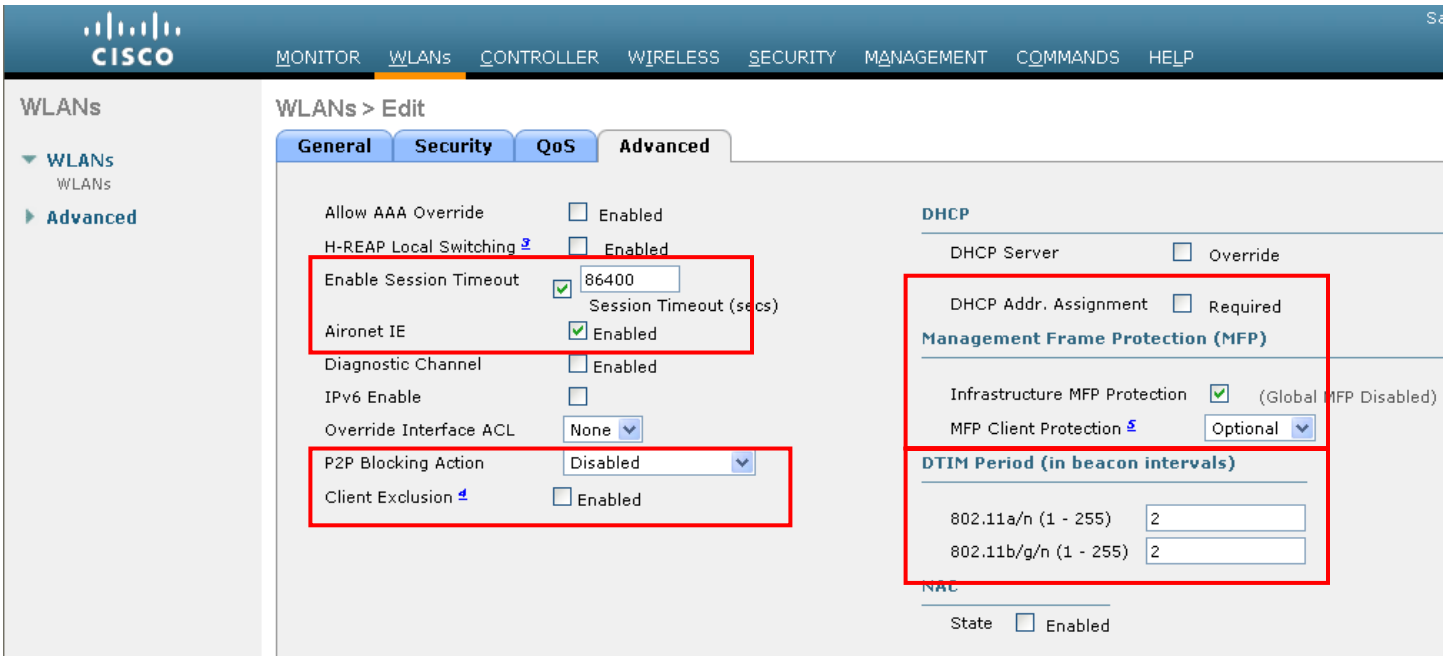
Configure session timeout as necessary. It is recommended to extend the timeout to avoid possible interruptions during re-authentication.

Enable Aironet Extensions (Aironet IE).

Disable client exclusion for the voice network.

DHCP Address Assignment should be disabled.

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



For the 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 7925G 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 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

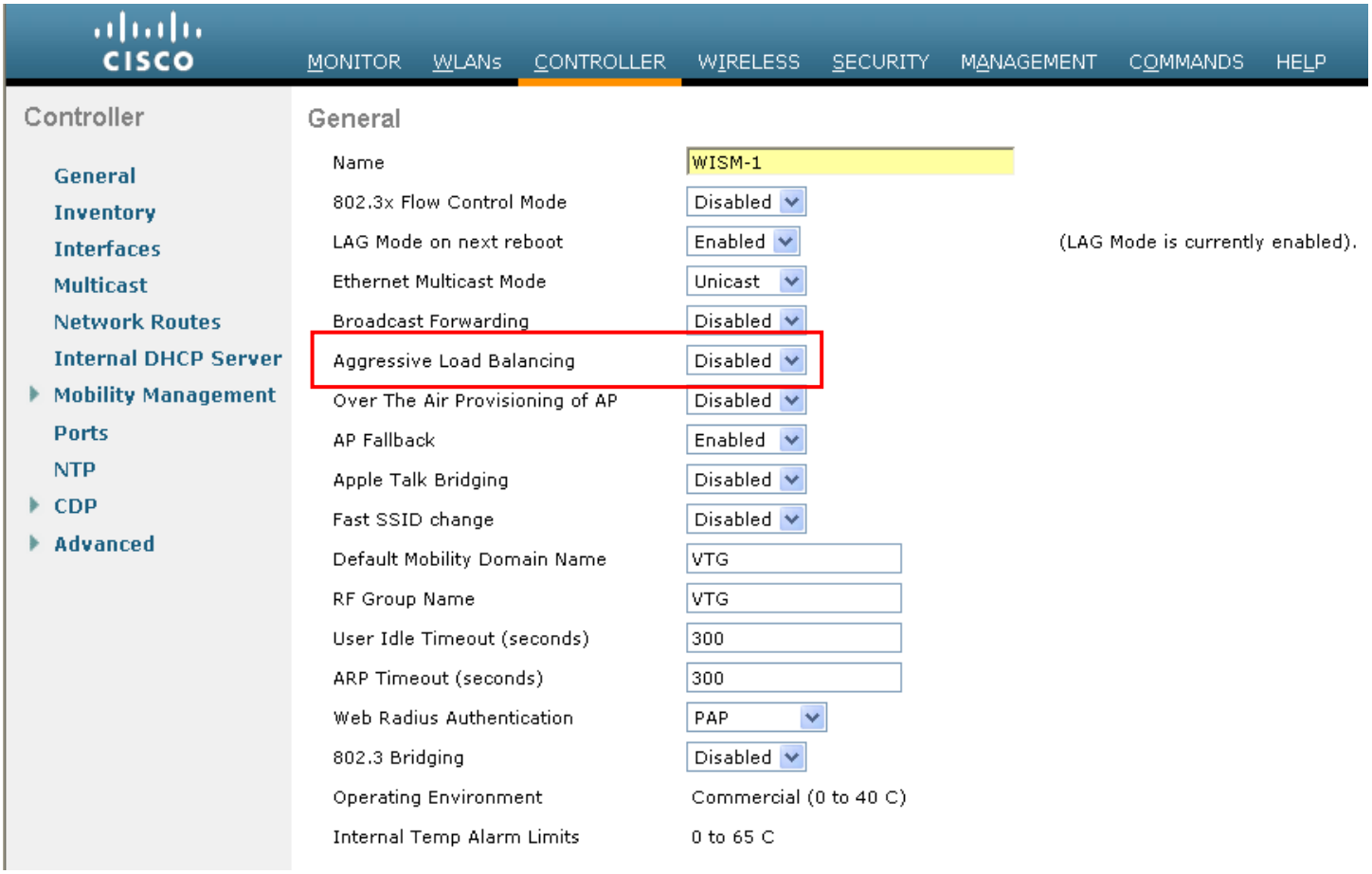
wlccp authentication-server client **eap** method_Clients

wlccp authentication-server client **leap** method_Clients

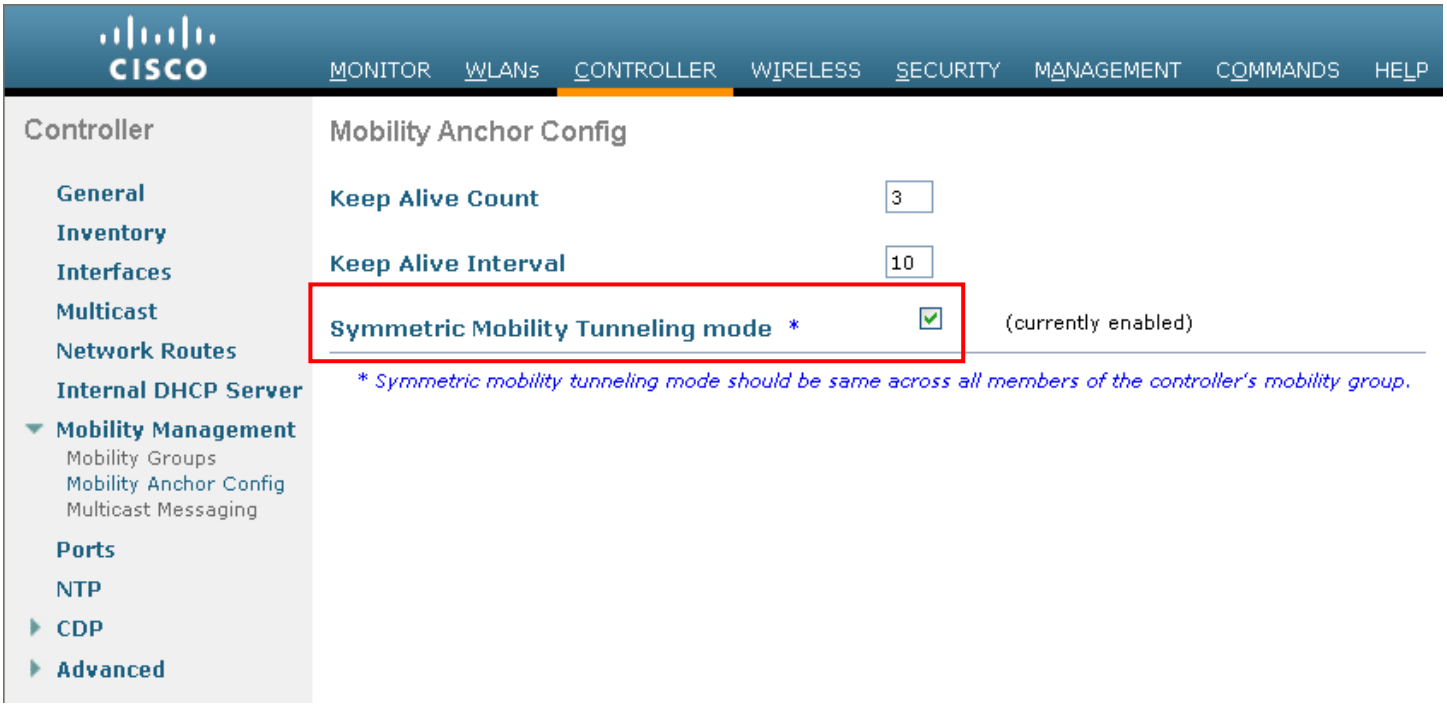
wlccp wds priority 255 interface BVI1

Controller Settings

Ensure that aggressive load balancing is disabled.

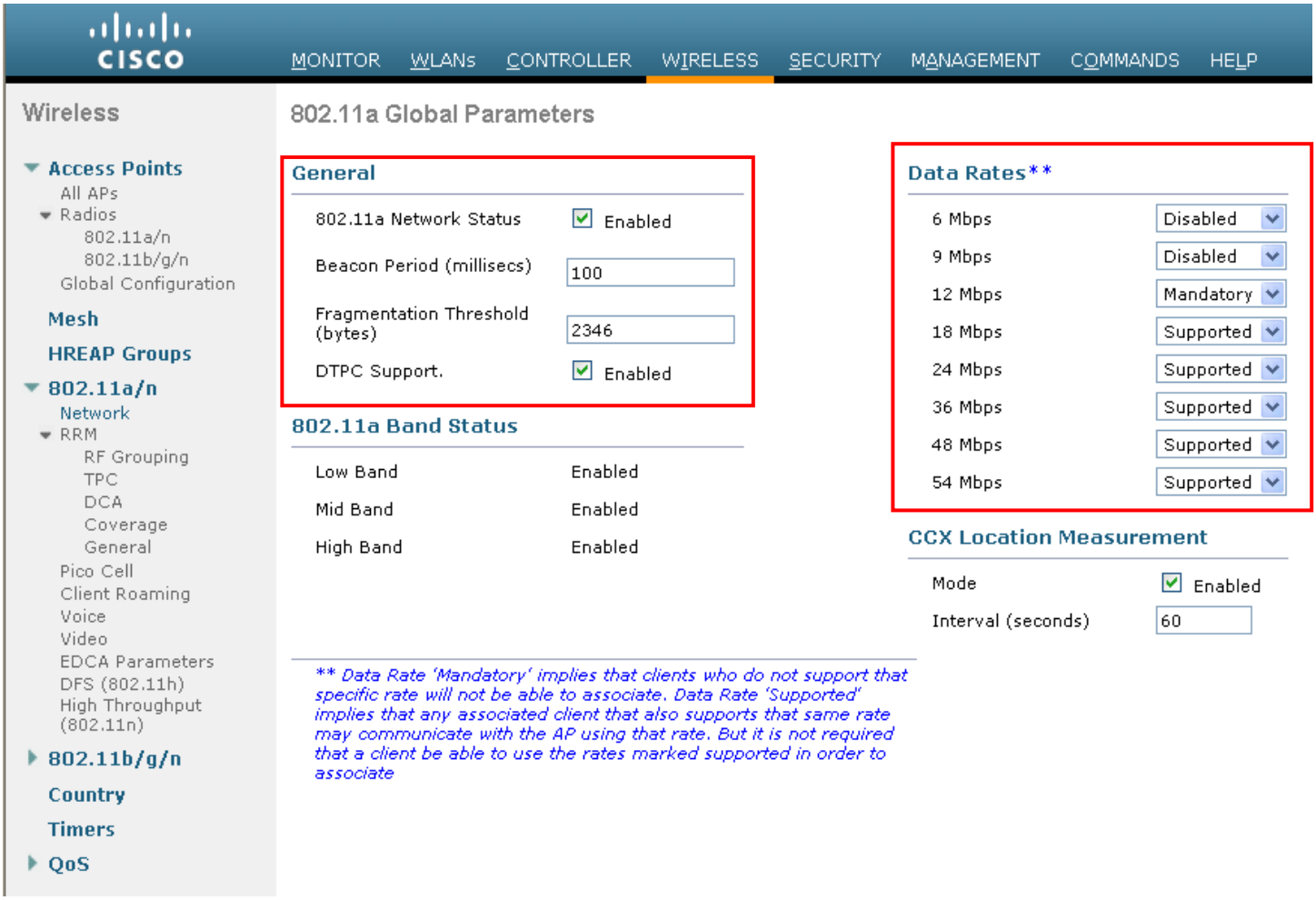


If using layer 3 mobility, then symmetric tunneling should be enabled and that the mobility group has been configured containing each Cisco Unified Wireless LAN Controller's IP and MAC address.



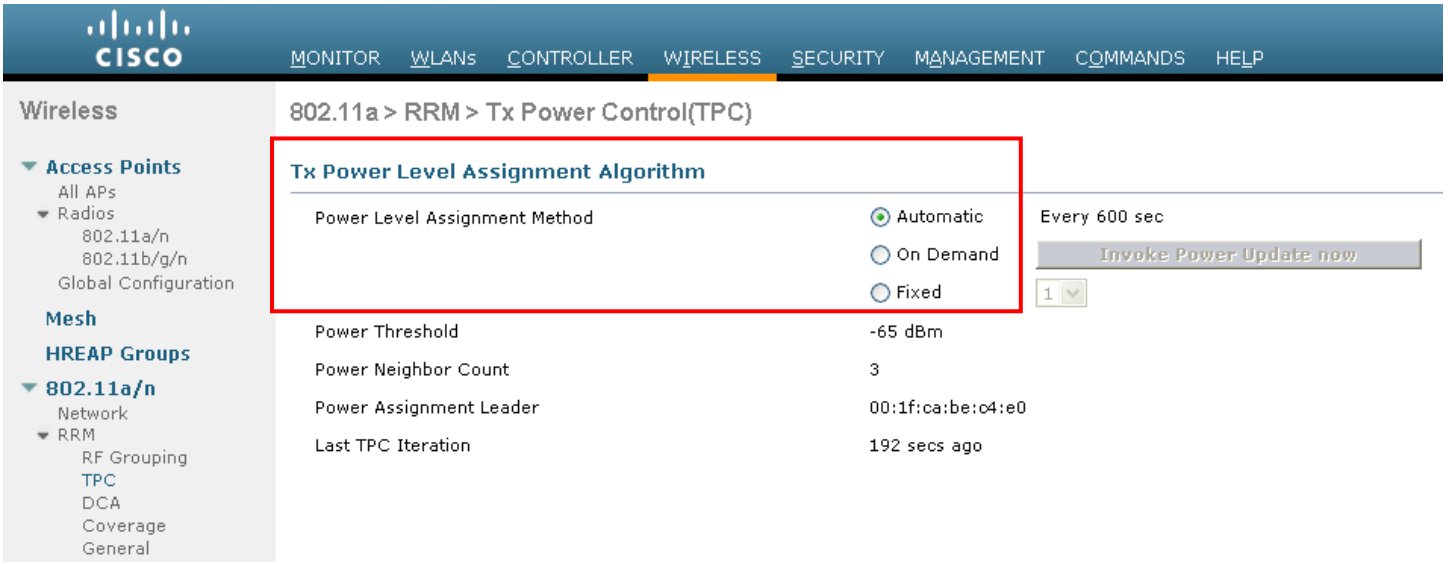
802.11 Network Settings

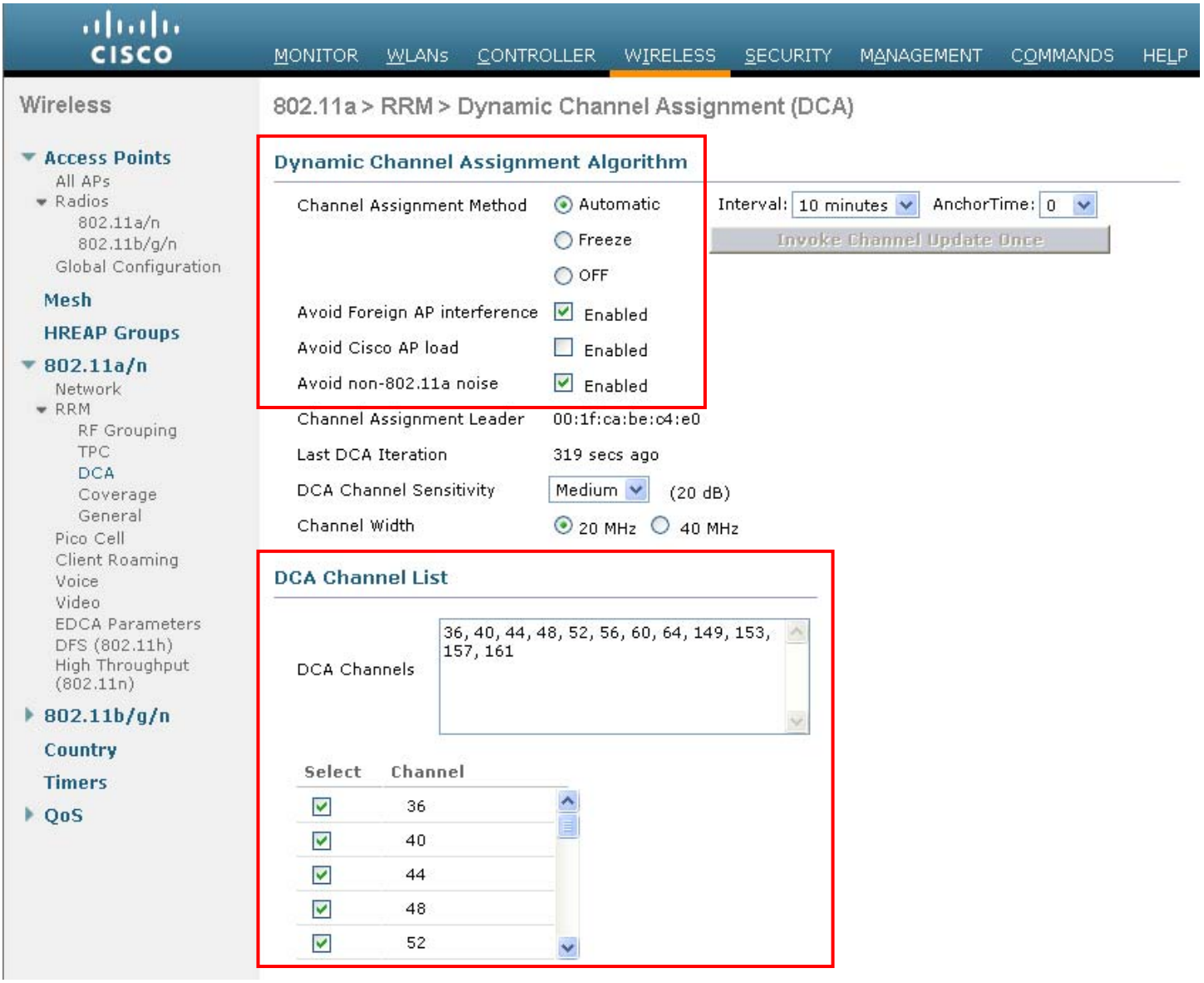
For optimal battery performance and quality, use DTIM of **2** with a beacon period of **100ms**.



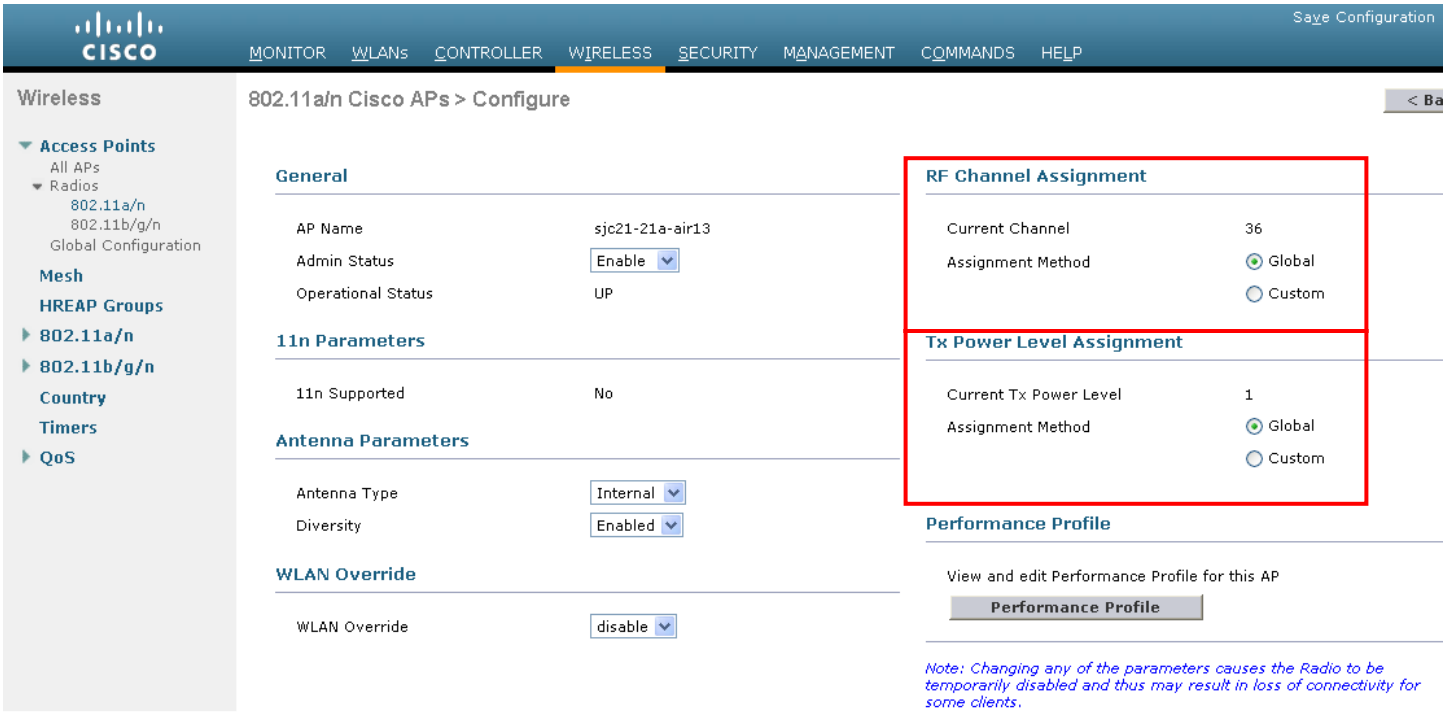
Auto RF

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





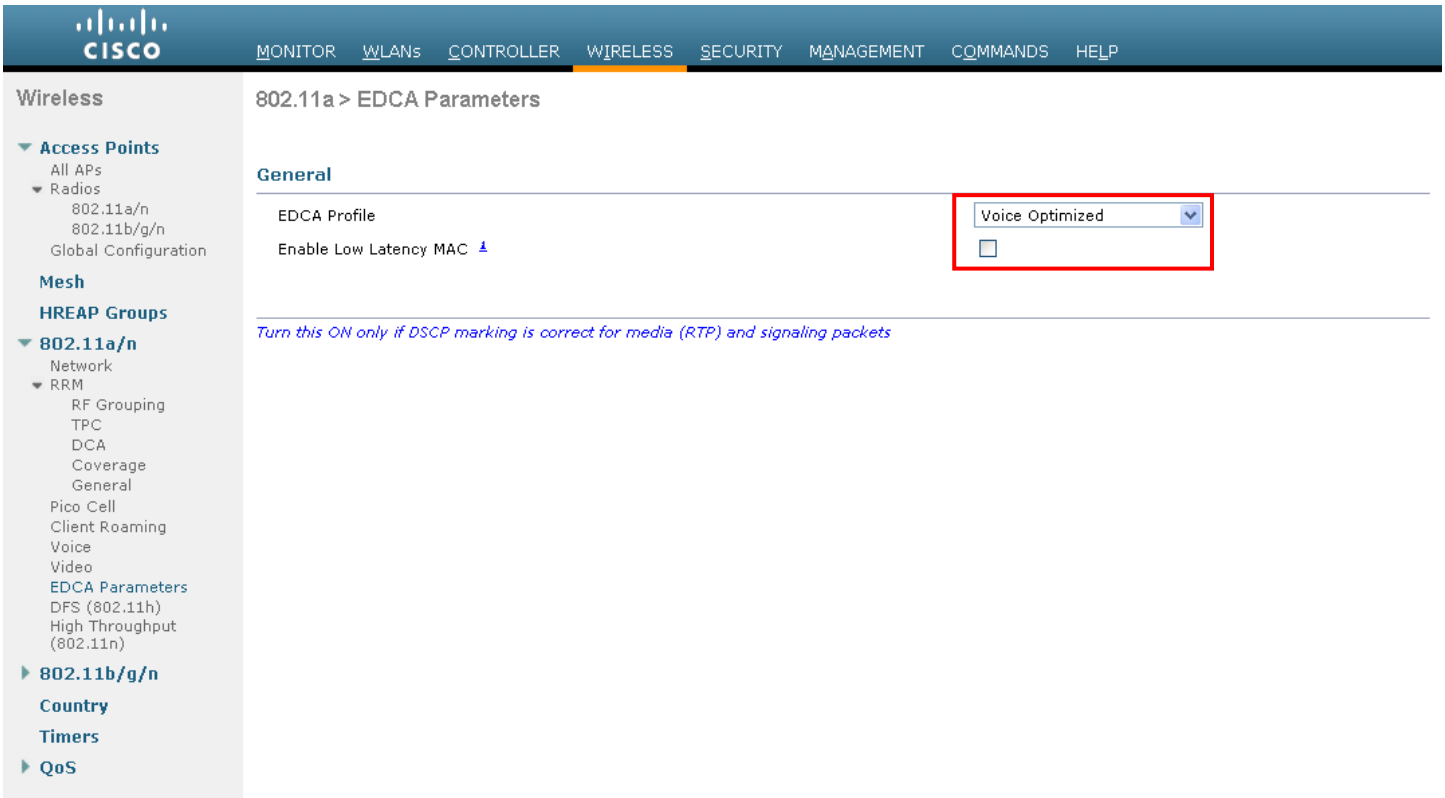
Individual access points can be configured to override the global setting to use dynamic channel and transmit power assignment. Other access points enabled can be enabled for Auto RF and workaround the access points that are statically configured. This may be necessary if there is an intermittent interferer present in an area.



EDCA Parameters

Set the EDCA profile for **"Voice Optimized"** and disable **"Low Latency MAC**".

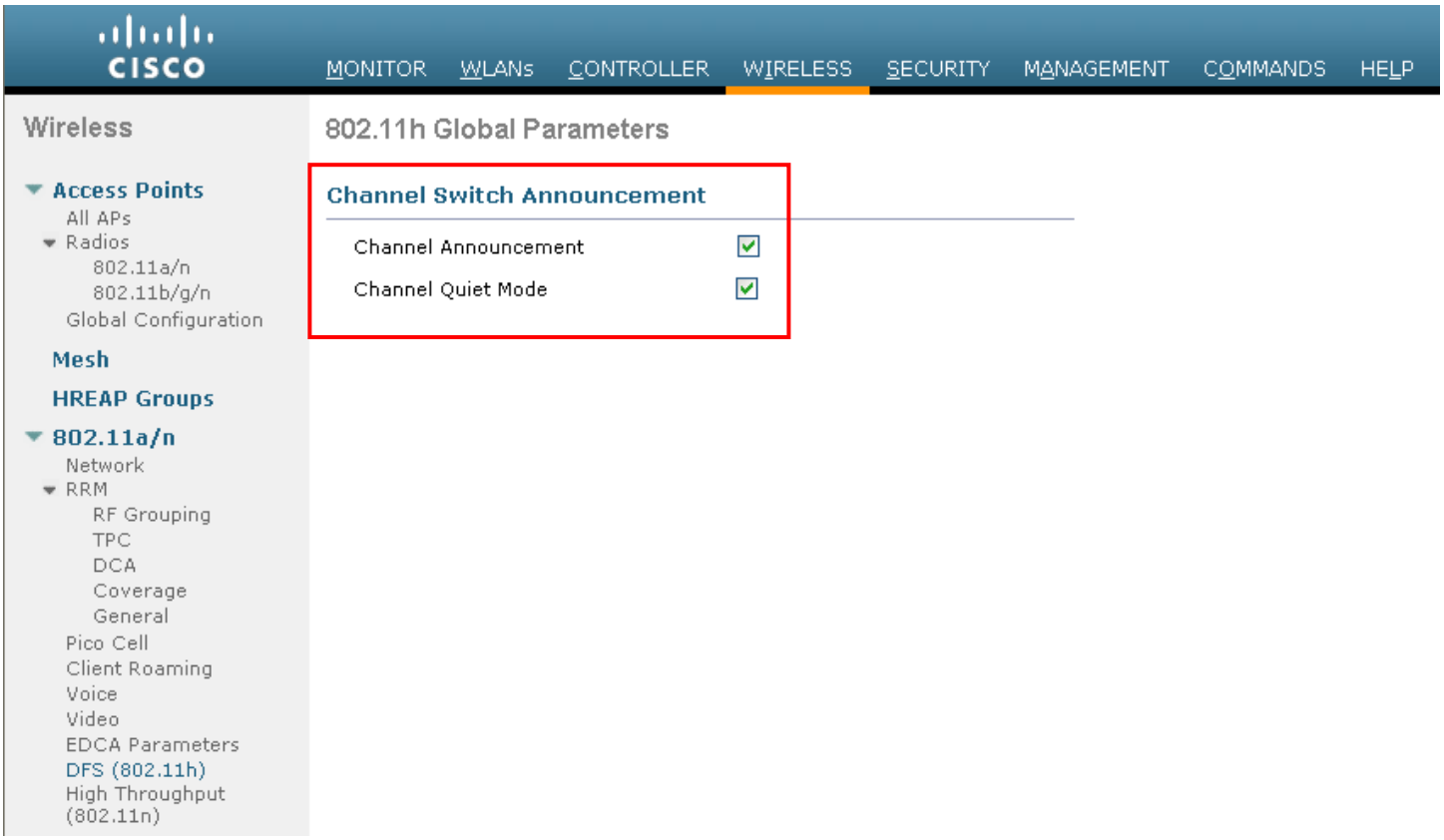
Low Latency MAC reduces the number of retransmissions to 2-3 per packet depending on the access point platform. This may cause issues if multiple data rates are enabled.



DFS (802.11h)

Channel announcement and quite mode should be enabled.

In versions prior to 5.0, power constraint (TPC) was a configurable option. Power constraint should be left un-configured as DTPC will be used by the Cisco Unified Wireless IP Phone 7925G to control the transmission power.



Call Admission Control Settings

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

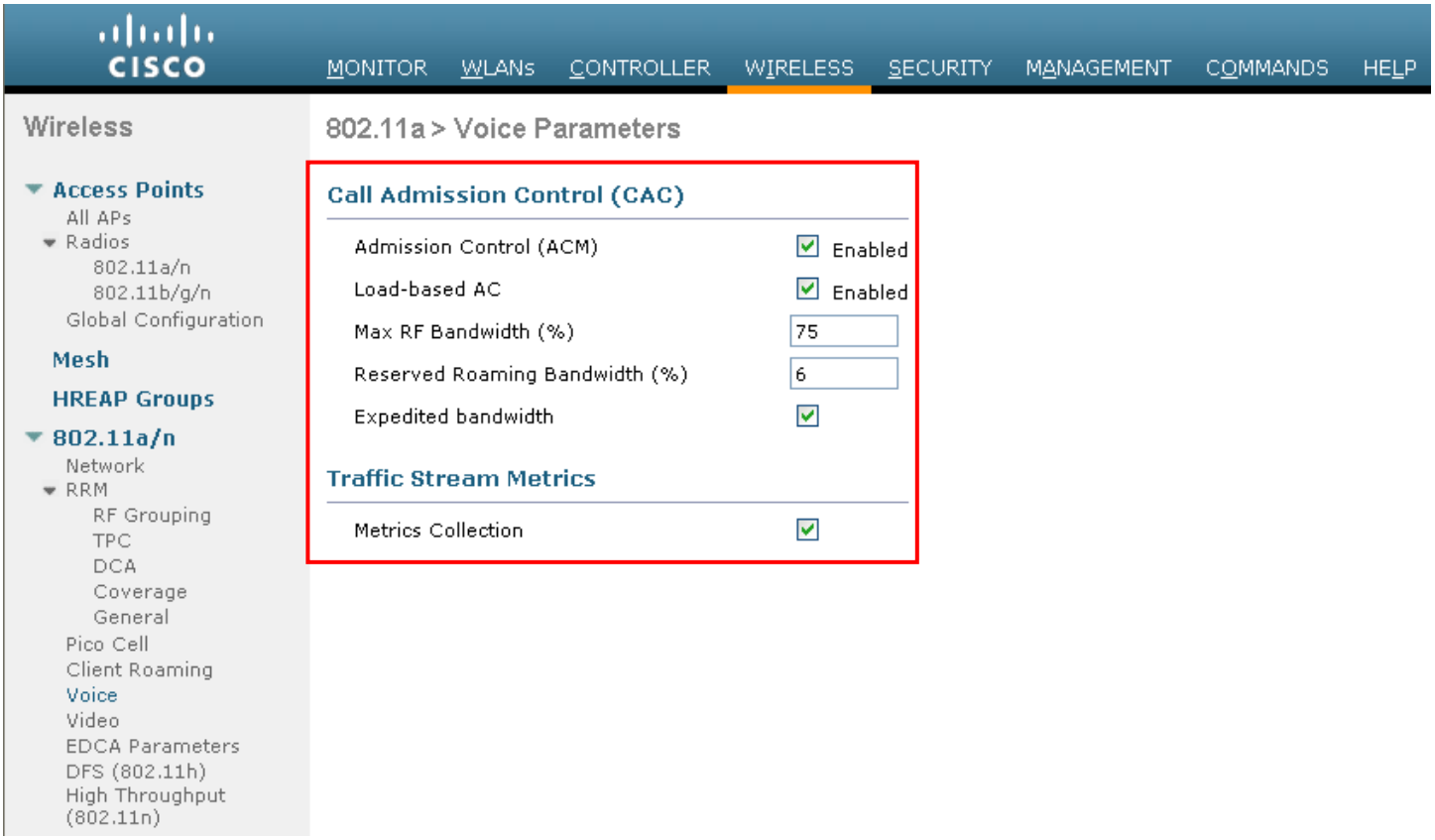
Maximum bandwidth default setting for voice is **75%**, and **6%** of that bandwidth is reserved for roaming clients.

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

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

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

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



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

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

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

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

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

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

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

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

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

```
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 7925G is enabled as a nominal rate in the STREAM configuration of the autonomous access point.

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

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

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

http://www.cisco.com/en/US/docs/wireless/access_point/12.3_8_JA/configuration/guide/s38qos.html

Configuring QoS Basic Service Set (QBSS)

There are three different versions of QoS Basic Service Set (QBSS) that the Cisco Unified Wireless IP Phone 7925G supports.

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

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

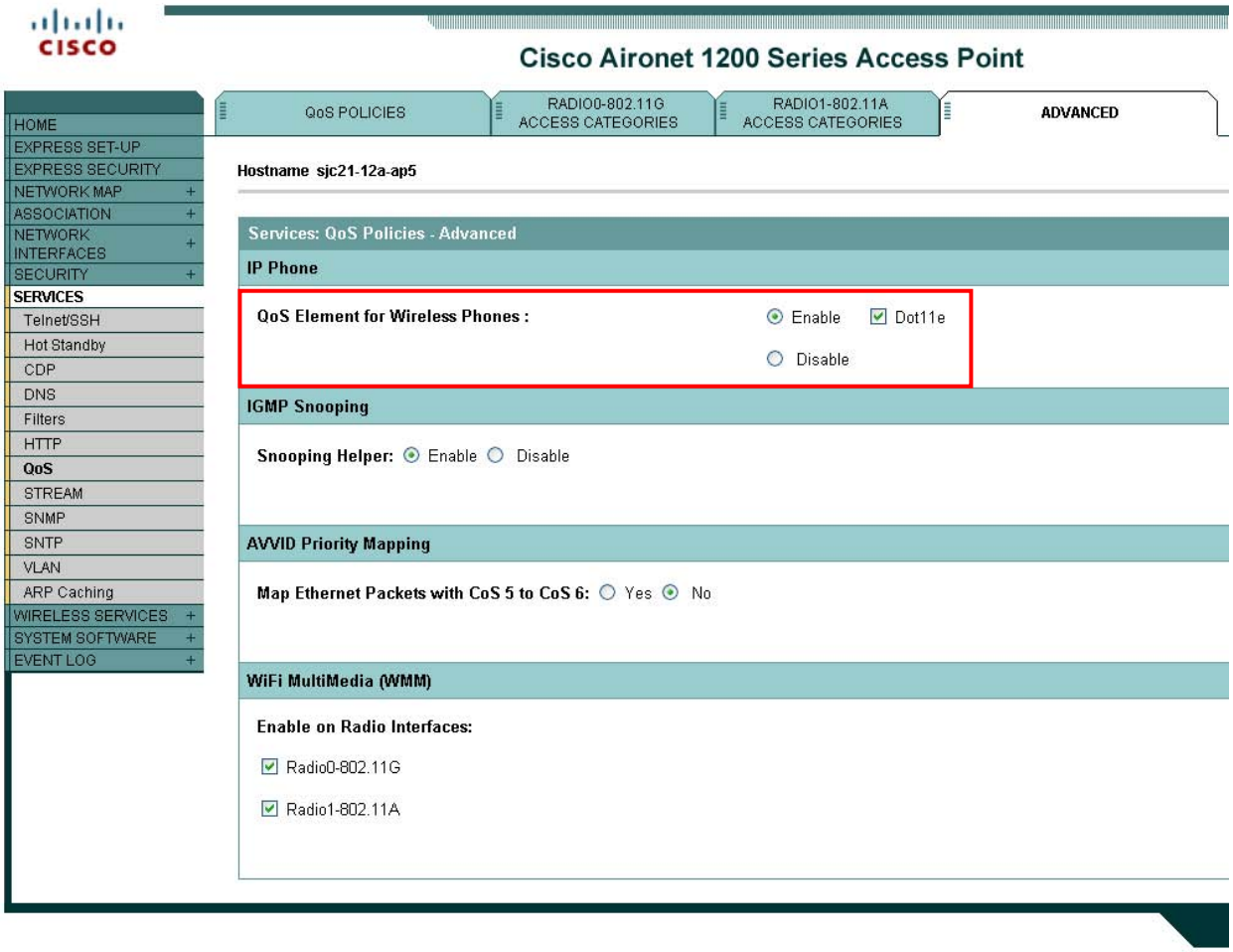
The second version from Cisco is based on the 802.11e version, but allows the default max threshold of 105 to be optionally configured.

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

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

For the Cisco Autonomous Access Point, **"dot11 phone"** or **"dot11 phone dot11e"** will enable QBSS.

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



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>”**

Configuring the WLAN Controller EAP-Request and EAPOL-Key Timeouts

If using EAP, the EAP-Request Timeout on the Cisco Unified Wireless LAN Controller should be set to at least 20 seconds.

In later versions, 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

(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..... 0
EAPOL-Key Timeout (seconds)..... **1**
EAPOL-Key Max Retries..... 2

Also ensure that the EAPOL-Key Timeout is left at the default of 1 second.

Configuring Proxy ARP

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

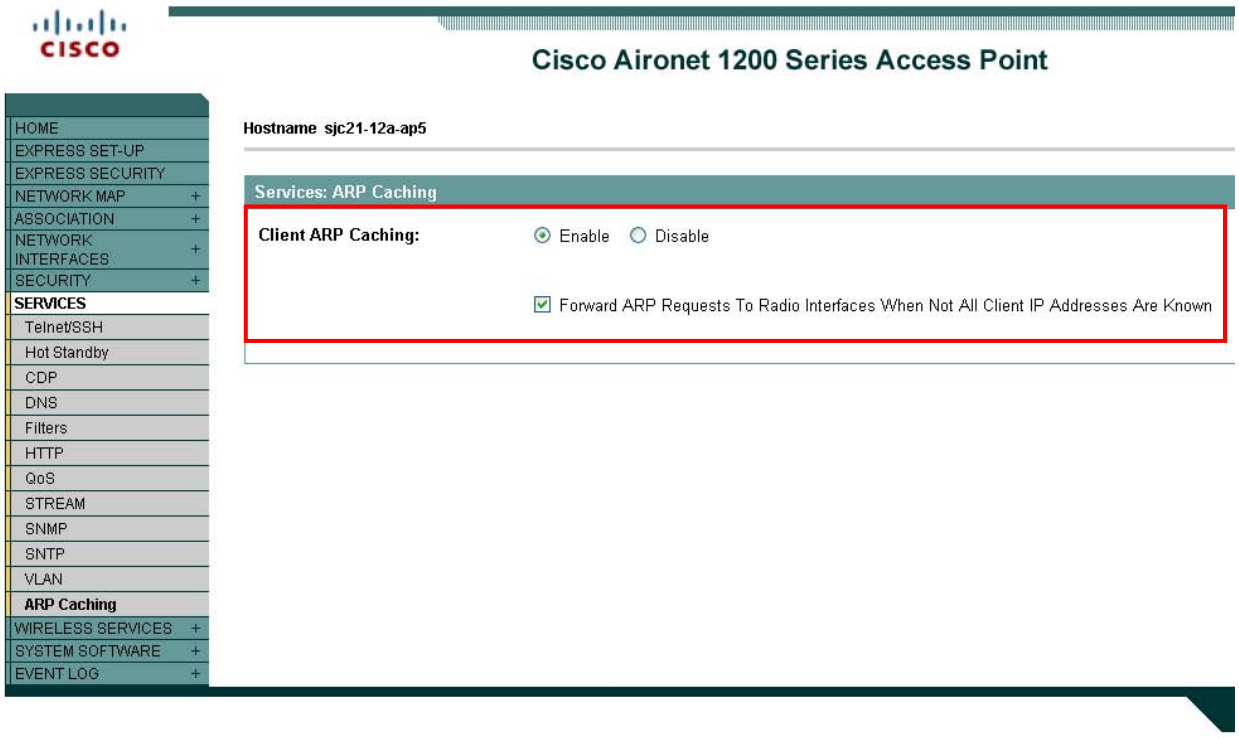
Ensure proxy ARP is enabled, where ARP Unicast Mode will be displayed as disabled on the Cisco Unified Wireless LAN Controller.

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

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

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

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



Configuring TKIP Countermeasure Holdoff Time

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

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

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

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

Interface dot11radio X
countermeasure tkip hold-time <nseconds>

For more information about these topics, refer to the *Enterprise Mobility Design Guide* at this URL:
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns279/c649/ccmigration_09186a00808d9330.pdf

VLANs and Autonomous Access Points

Segment wireless voice and data into separate VLANs.

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

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

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

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

Configuring the Cisco Unified Wireless IP Phone 7925G

There are three methods for configuring network settings on the Cisco Unified Wireless IP Phone 7925G:

Configuring Phones with the Keypad

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

For more information, refer to the "Configuring Settings on the Cisco Unified Wireless IP Phone 7925G" in the *Cisco Unified Wireless IP Phone 7925G 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 7925G has an HTTPS enabled web interface that you can access via the 802.11a/b/g radio or USB.

If you are using the USB cable connection to a PC, you must manually set a static IP on the computer side, for example, 192.168.1.X /24. By default, the Cisco Unified Wireless IP Phone 7925G USB is statically set to 192.168.1.100 /24.

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

Note: It is recommended not 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 Wavelink Avalanche

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

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

Refer to the Wavelink section below for more info.

For more information, refer to the "Using the Cisco Unified Wireless IP Phone 7925G Web Pages" in the *Cisco Unified Wireless IP Phone 7925G Administration Guide* at this URL:

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

Configuring the Network Profile Parameters

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 2.4 and 5 GHz channels and attempt to on the 5 GHz band if the configured network is available.

  In previous releases, the Cisco Unified Wireless IP Phone 7925G 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 band over another. At power on, will scan all 2.4 and 5 GHz channels then attempt to associate to an access point for the configured network using the preferred band if available. If the preferred band is not available, then the Cisco Unified Wireless Phone 7925G will try to use the less preferred band if available. If the phone roams out of coverage of the preferred band, where the less preferred band signal is available, then the phone will attempt to associate to that less preferred band. Once associated to the less preferred band, there is no mechanism to check if the preferred band is available again. For the phone to roam back to the preferred band, the less preferred band signal will have to be exhausted.

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

- To extend 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 **"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 which 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 or 128 bit)
Shared Key	Static	WEP (40 or 128 bit)
LEAP	802.1x, WPA, WPA2	TKIP, AES, WEP (40 or 128 bit)
EAP-FAST	802.1x, WPA, WPA2	TKIP, AES, WEP (40 or 128 bit)
EAP-TLS	802.1x, WPA, WPA2	TKIP, AES, WEP (40 or 128 bit)
PEAP	802.1x, WPA, WPA2	TKIP, AES, WEP (40 or 128 bit)
AKM	802.1x, WPA, WPA2, WPA-PSK, WPA2-PSK	TKIP, AES, WEP (40 or 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	5
ASCII	128	13
HEX	40	10 (0-9, A-F)
HEX	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.

  ASCII = 8-63 characters

  HEX = 64 characters (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.

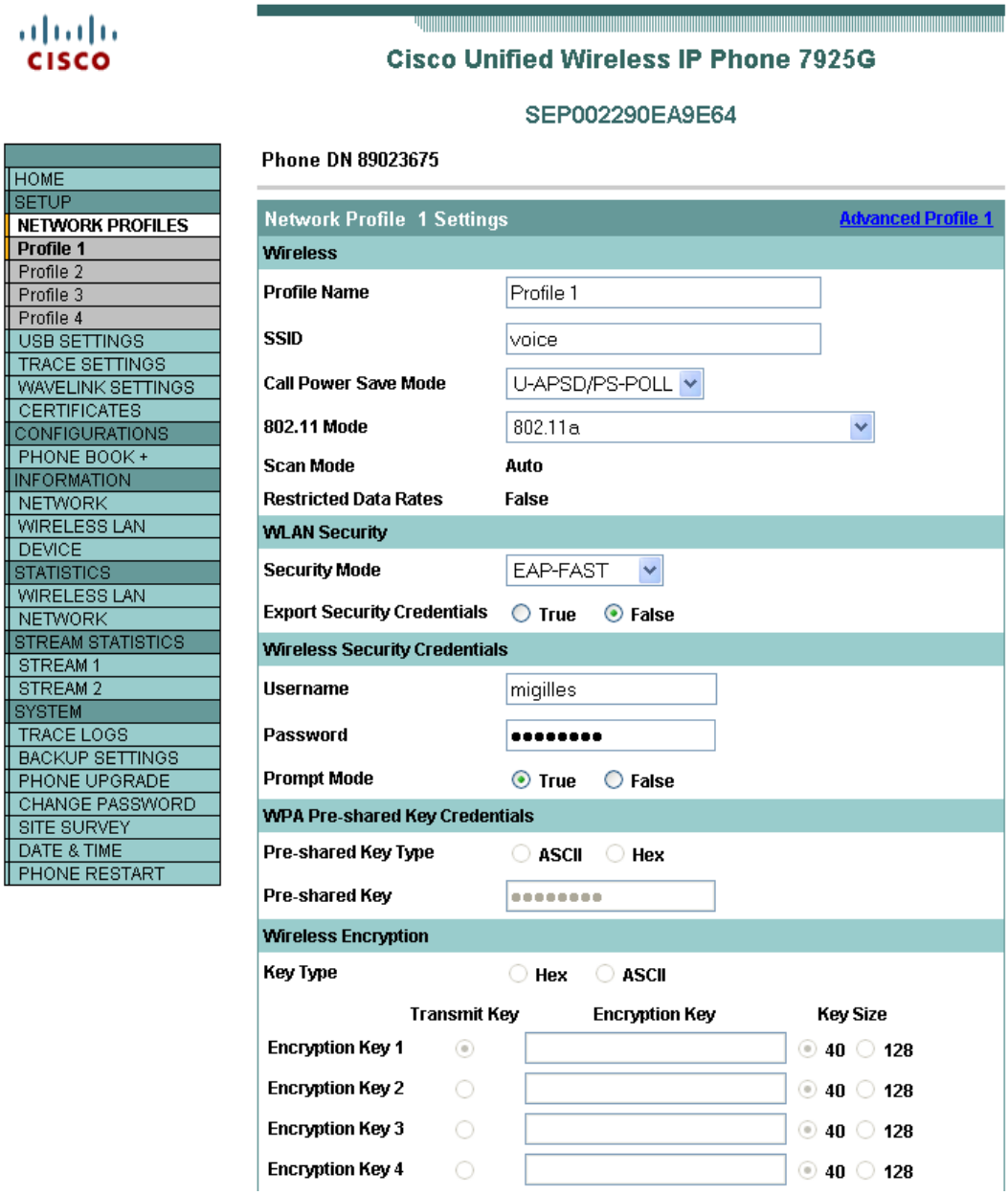
Note: CCKM will be negotiated if enabled on the Access Point when using 802.1x authentication with LEAP, EAP-FAST, EAP-TLS, PEAP or AKM modes.

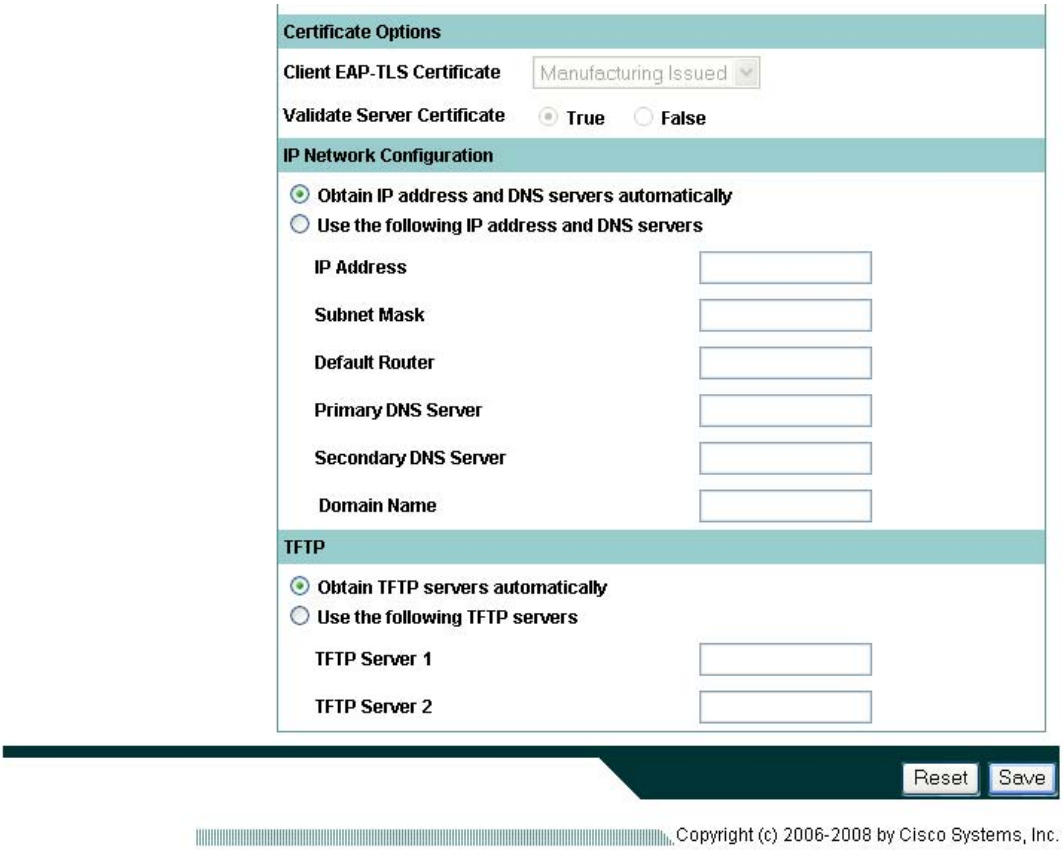
WEP with AKM is only applicable with 802.1x authentication (not WPA-PSK).

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

- 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 7925G
SEP002290EA9E64
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
Auto
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 7925G.

Configuring Advanced Network Profile Settings

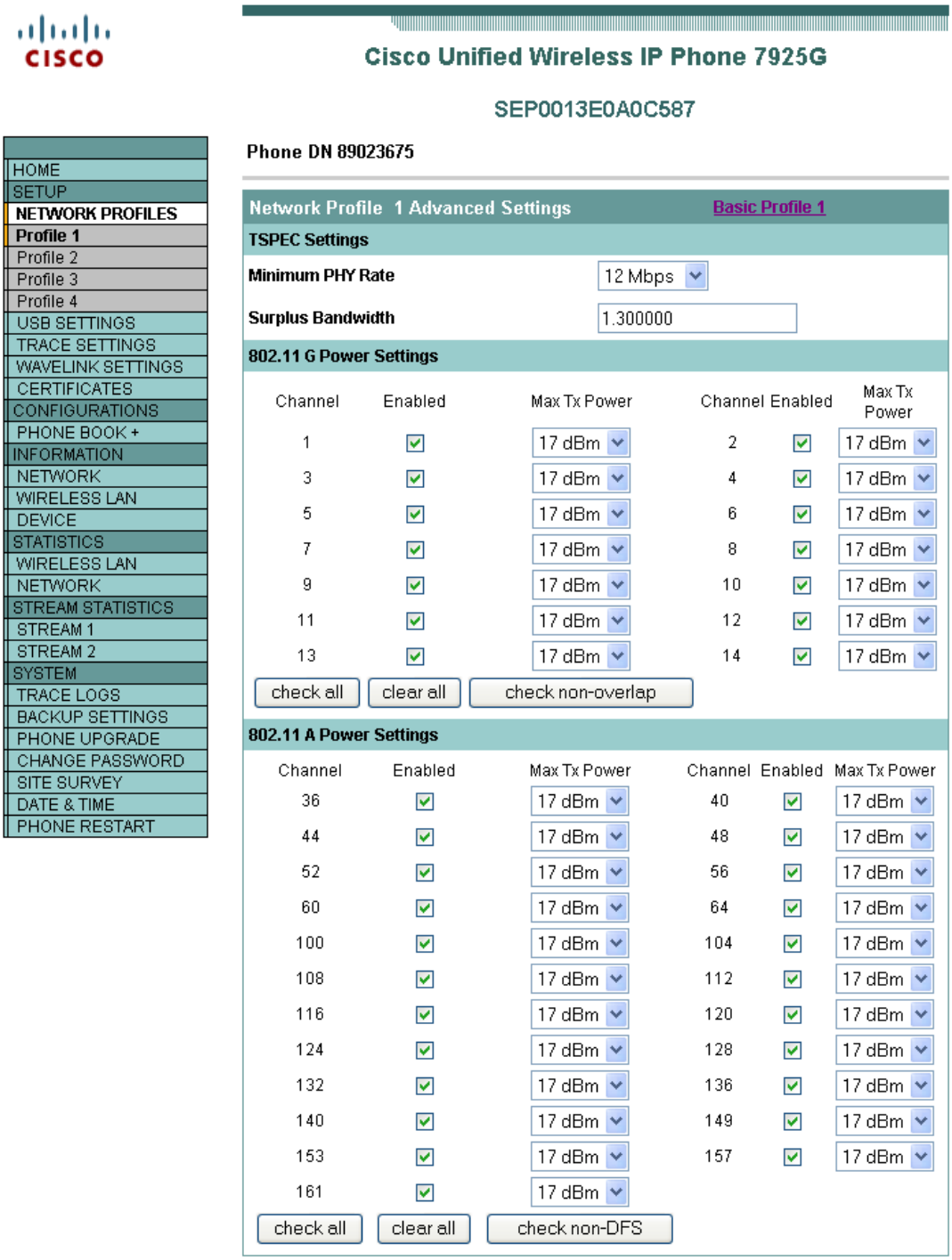
In the Advanced Network Profile settings, you can adjust the minimum PHY rate. If 12 Mbps is not enabled in the wireless LAN, then you may need to configure this parameter or enable 12 Mbps on the access point.

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

If using this feature, then only disable those channels that are not used in the wireless LAN. If you disable a channel that is currently used by an access point, then the Cisco Unified Wireless IP Phone 7925G might not associate to the wireless LAN successfully.

If all channels that are used in the wireless LAN are disabled on the phone, then use one of these methods to browse to the Cisco Unified Wireless IP Phone 7925G webpage:

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



Installing Certificates

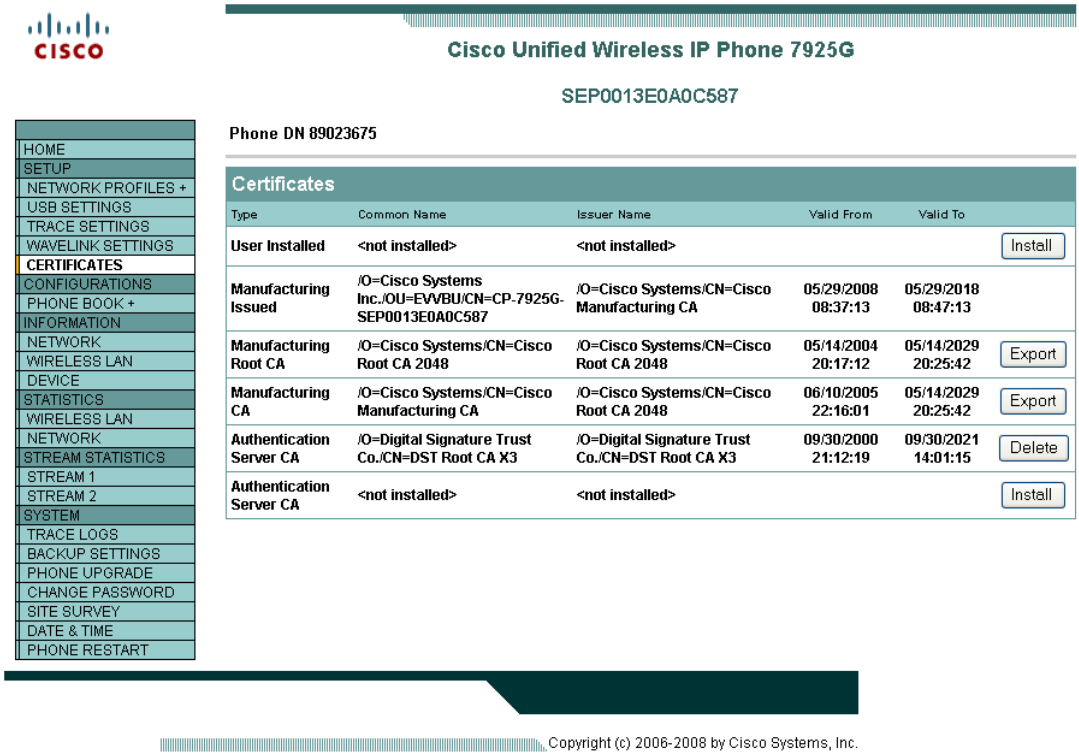
Extensible Authentication Protocol Transport Layer Security (EAP-TLS) is using the TLS protocol with PKI to secure communications to the authentication server.

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

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

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

To use the MIC in the Cisco Unified Wireless IP Phone 7925G, 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.

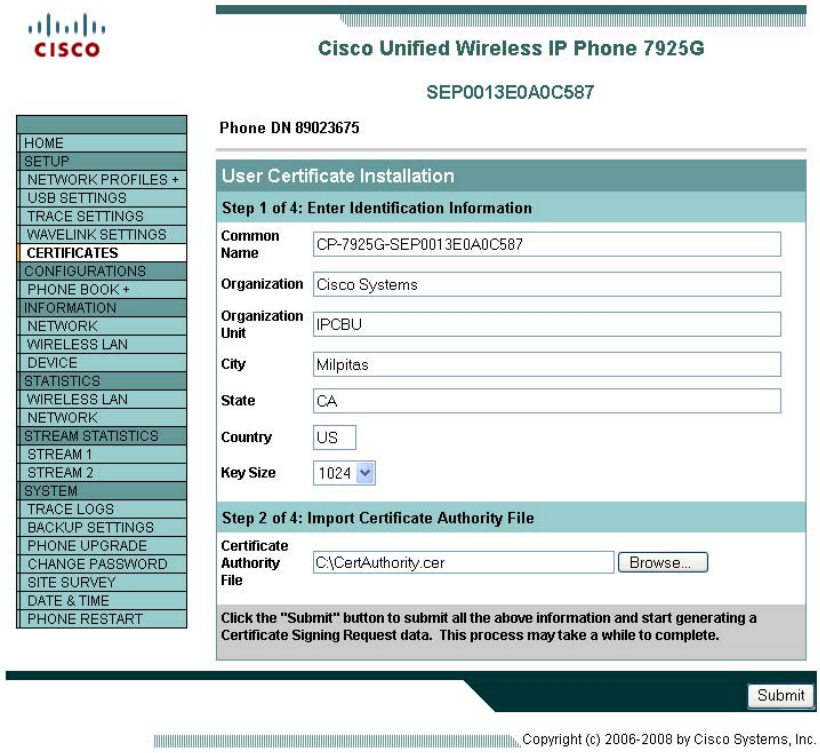
For the user installed certificate method, select "Install" on the main certificates page, which will launch the installation wizard.

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

The Common Name defaults to "**CP-7925G-SEP<MAC_Address>"**, but can be customized.

Browse to the Certificate Authority certificate and select **"Submit"**.

Certificates dated January 1 2038 and later are not supported.



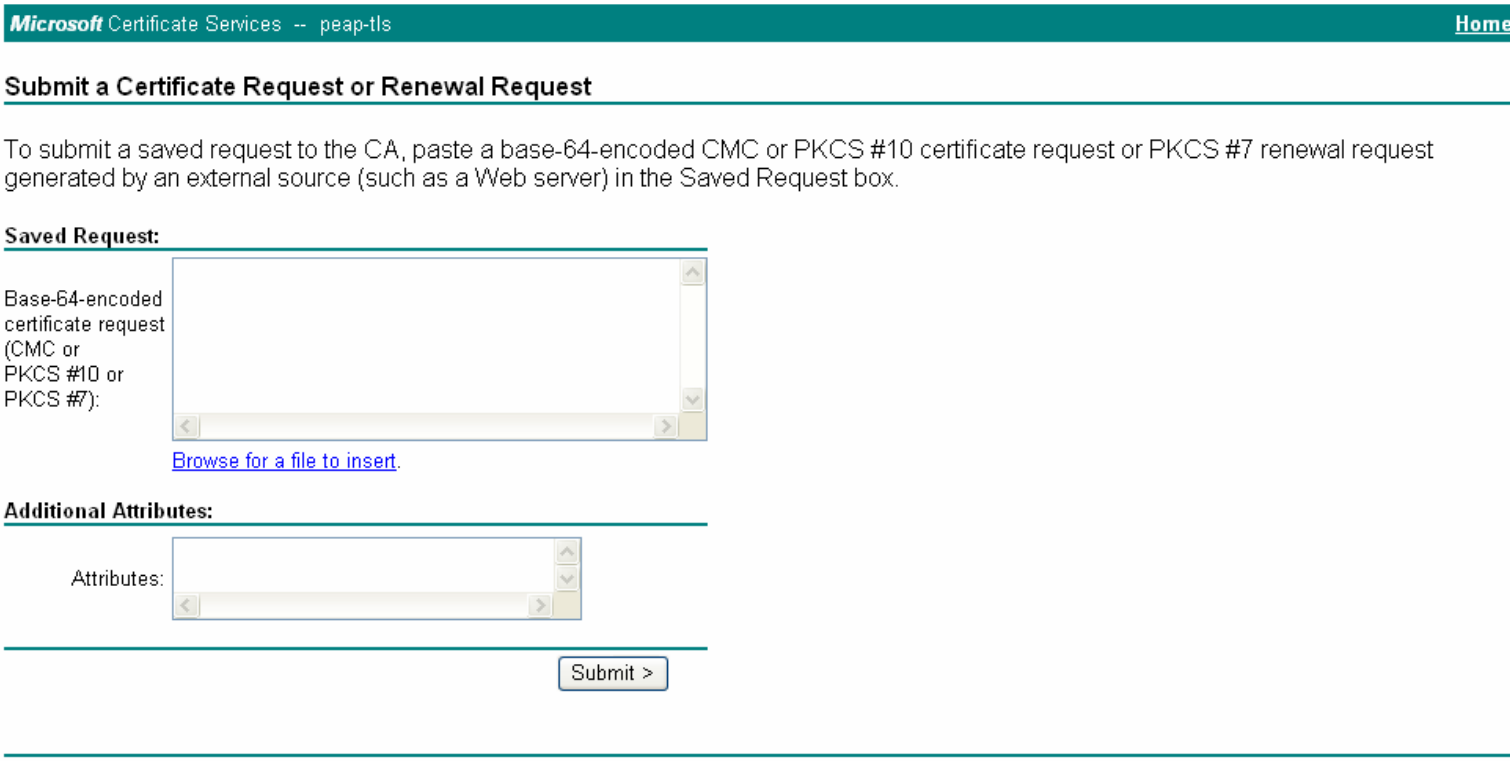
After **"Submit"** is selected, the certificate will then be generated.

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

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

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

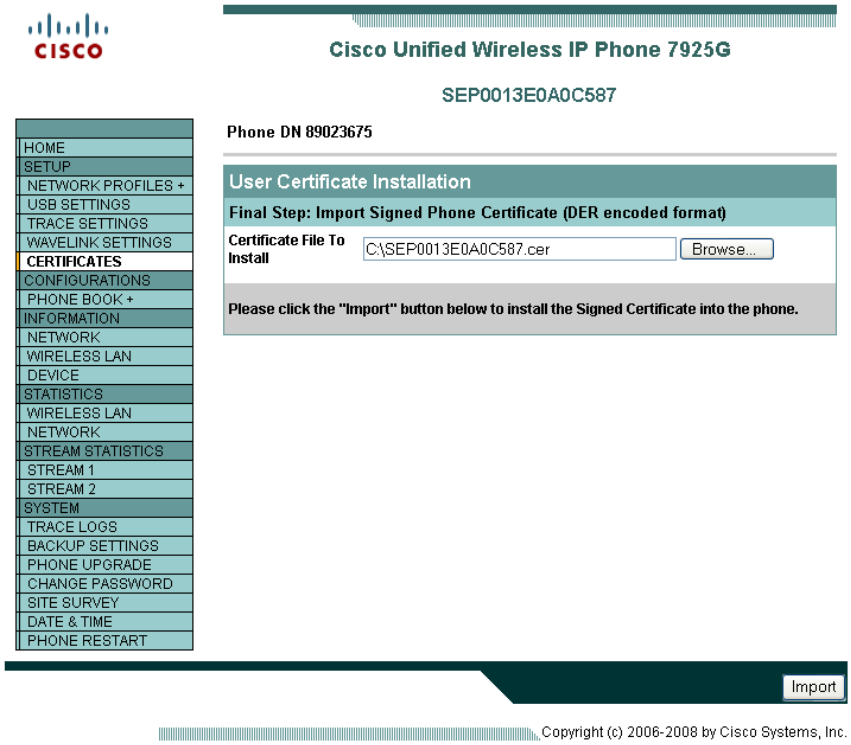
Paste the certificate data from the Cisco Unified Wireless IP Phone 7925G to the Certificate Authority signing server and submit for signing.



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

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

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

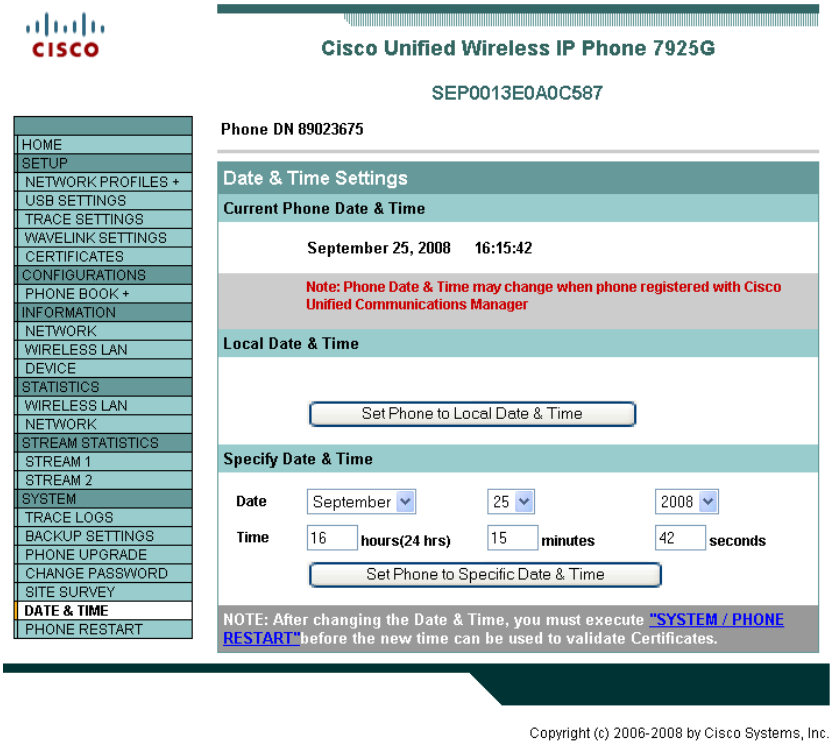


Once the certificate is installed successfully, a confirmation page will be displayed.

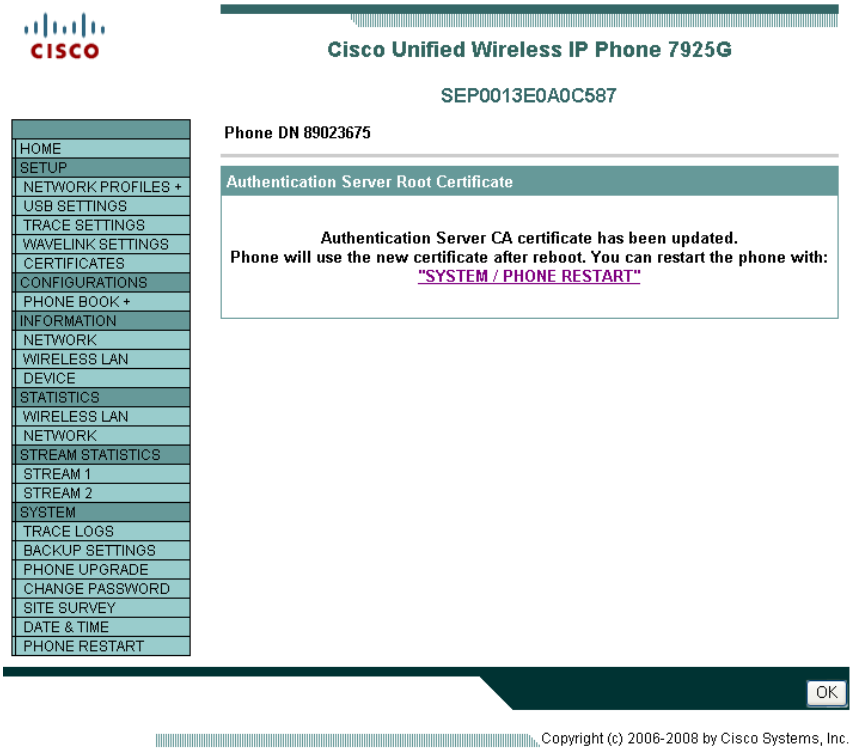
The CA chain should already be enabled in the authentication server's certificate trust list.

The authentication server certificate must also be imported into the Cisco Unified Wireless IP Phone 7925G for both methods. If the authentication server certificate was signed by a Certificate Authority (CA) server, then that DER encoded root certificate will need to be imported into the Cisco Unified Wireless IP Phone 7925G.

If the Cisco Unified Wireless IP Phone 7925G has not registered to a Cisco Unified Communications Manager yet, then the date and time must be configured manually for the first time.



The Cisco Unified Wireless IP Phone 7925G must be restarted after installing the certificate. Click on the hyperlink to navigate to the **"Phone Restart"** page.

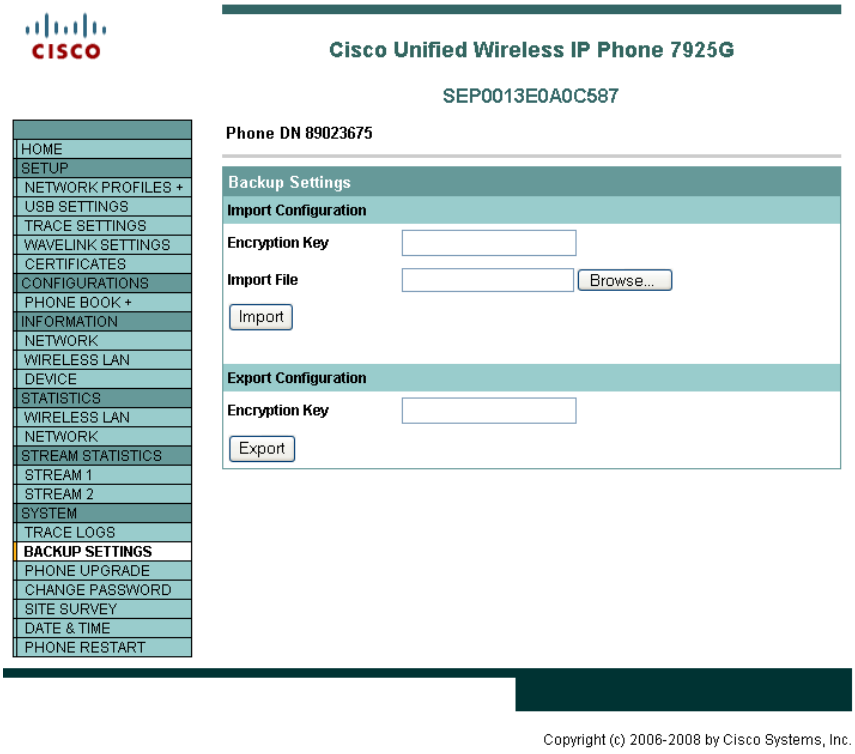


Click the **"Restart"** button to power cycle the phone.

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).

For security reasons, the Wireless LAN security information (Username/Password, WPA Pre-shared key information, and WEP key information) is not exported by default. In order to export this Wireless LAN security information, the network profile must be configured to allow this capability. For each network profile where the Wireless LAN security information is to be exported, configure the **"Export Security Credentials"** option to **"True".** After selecting **"True"**, you will need to enter the Wireless LAN security information again. This will then allow that information to be exported and then imported to other Cisco Unified Wireless IP Phone 7925G phones.



Bluetooth Configuration

The Cisco Unified Wireless IP Phone 7925G supports Bluetooth to allow wireless headset communications.

To pair a Bluetooth headset to the Cisco Unified Wireless IP Phone 7925G, follow the instructions below.

1. Choose Settings > Phone Settings > Bluetooth
2. Select **"Enable"** then select the left softkey **"Save"**
3. Select **"Device List"**
4. Select **"Scan"** (ensure the Bluetooth headset is in pairing mode)
5. Select **"Pair"** after the Bluetooth headset is discovered
6. Enter the Bluetooth passkey (will attempt to use 0000)
7. Select **"Connect"** after the Bluetooth headset is paired successfully

Upgrading Phone Firmware

There are two methods for upgrading the Cisco Unified Wireless IP Phone 7925G 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 5.1, 6.0, 6.1, 7.0 and later.

For information on how to install the COP file on CM versions 5.1 and later, refer to the *Cisco Unified Communications Manager Operating System Administrator Guide* at this URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/cucos/7_1_2/cucos/iptpch7.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.

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

You can specify the Load Server as an alternate TFTP server to retrieve firmware files in the Cisco Unified Wireless IP Phone 7925G 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 below:

```
tftp-server flash: Cp7925g-1.3.3.LOADS
tftp-server flash:Appsh-1.3.3.SBN
tftp-server flash:Guih-1.3.3.SBN
tftp-server flash:Sysh-1.3.3.SBN
tftp-server flash:Tnuxh-1.3.3.SBN
tftp-server flash:Tnuxrh-1.3.3.SBN
tftp-server flash:Wlanh-1.3.3.SBN
!
telephony-service
 load 7925 Cp7925g-1.3.3.LOADS
```

Web Interface

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

Note: If the Cisco Unified Wireless IP Phone 7925G registers to Cisco Unified Communications Manager, web access to the Cisco Unified Wireless IP Phone 7925G gets set to read-only mode. In this mode, you are not allowed access to upgrade firmware.

Ultimately the Cisco Unified Wireless IP Phone 7925G will use what is set as the phone load in the Cisco Unified Communications Manager.

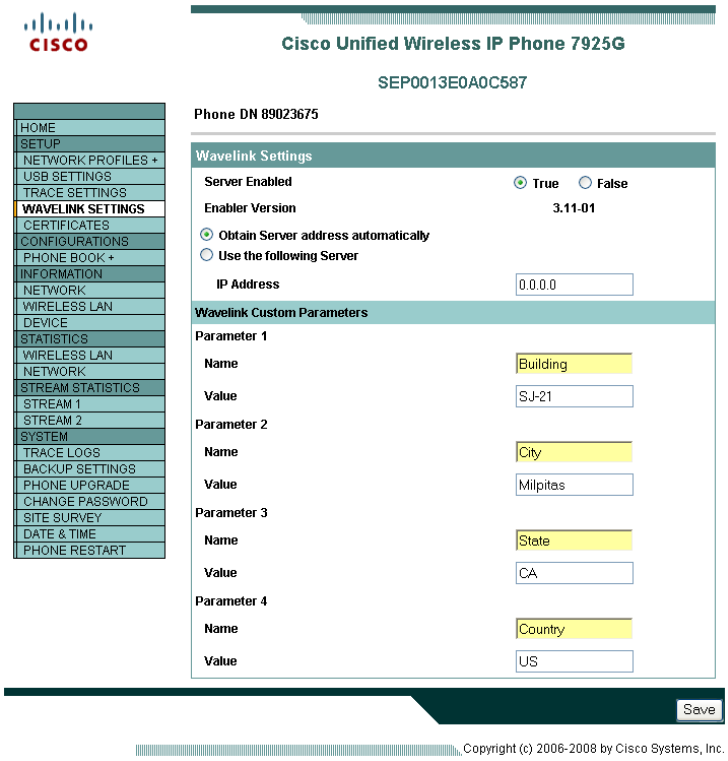
Wavelink Avalanche

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.

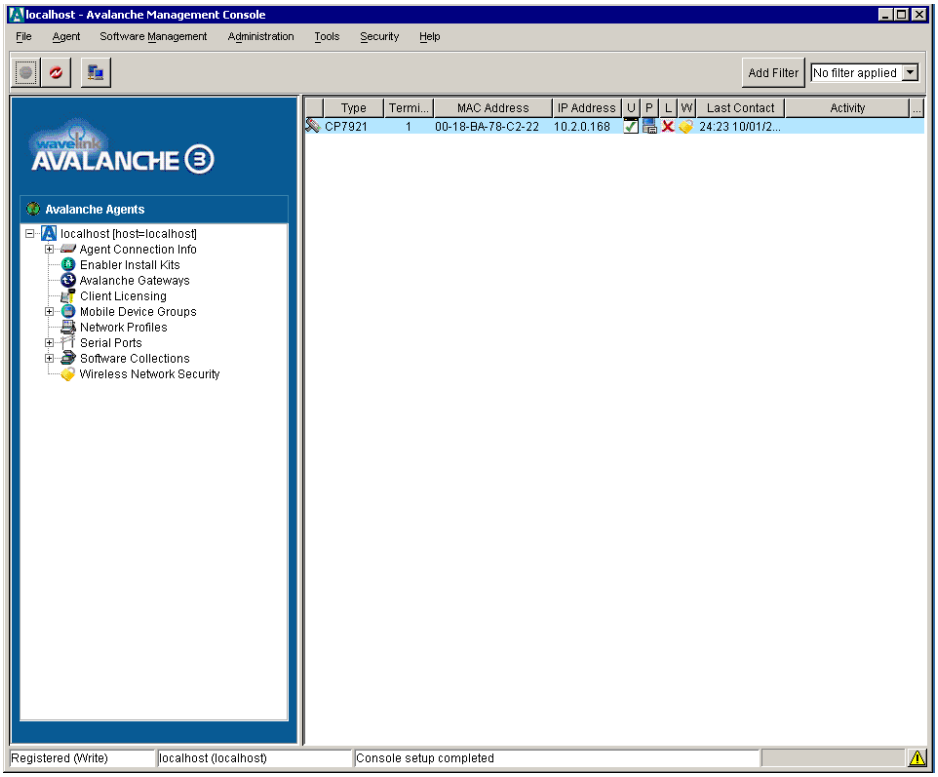
```
ip dhcp pool 10.10.11.0
  network 10.10.11.0 255.255.255.0
  default-router 10.10.11.1
  dns-server 10.10.10.20
  domain-name cisco.com
  option 150 ip 10.10.10.22
  option 149 ip 10.10.11.128
```

Custom parameters can also be set via the Cisco Unified Wireless IP Phone 7925G 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 and select **“Client Settings”.**

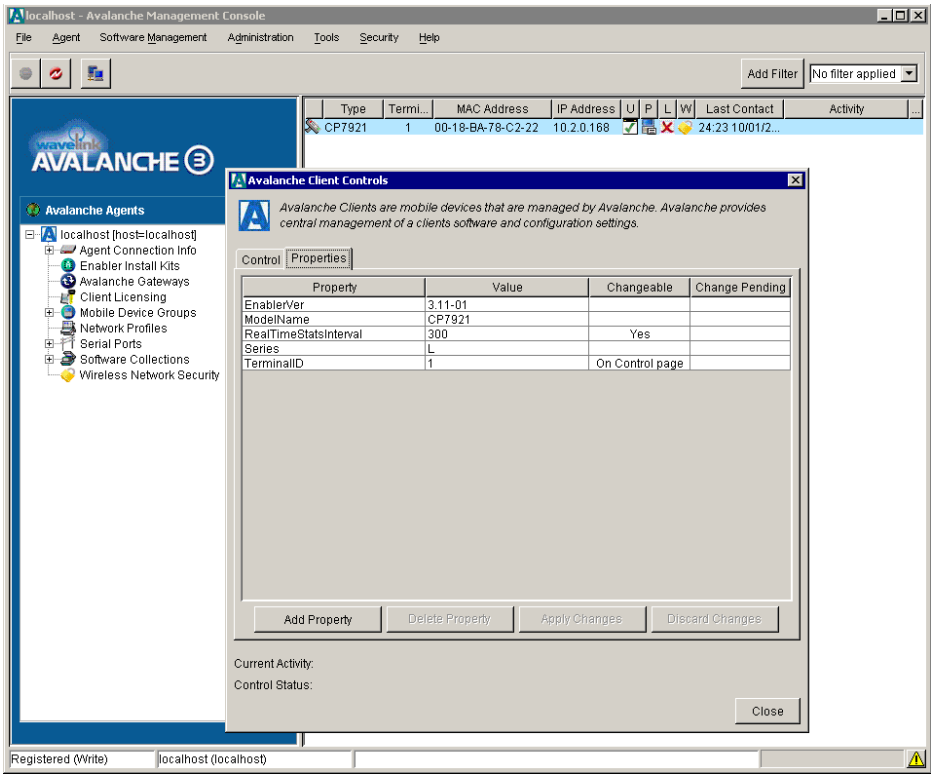


The Cisco Unified Wireless IP Phone 7925G will have parameters enabled by default.

EnablerVer = 3.11-01

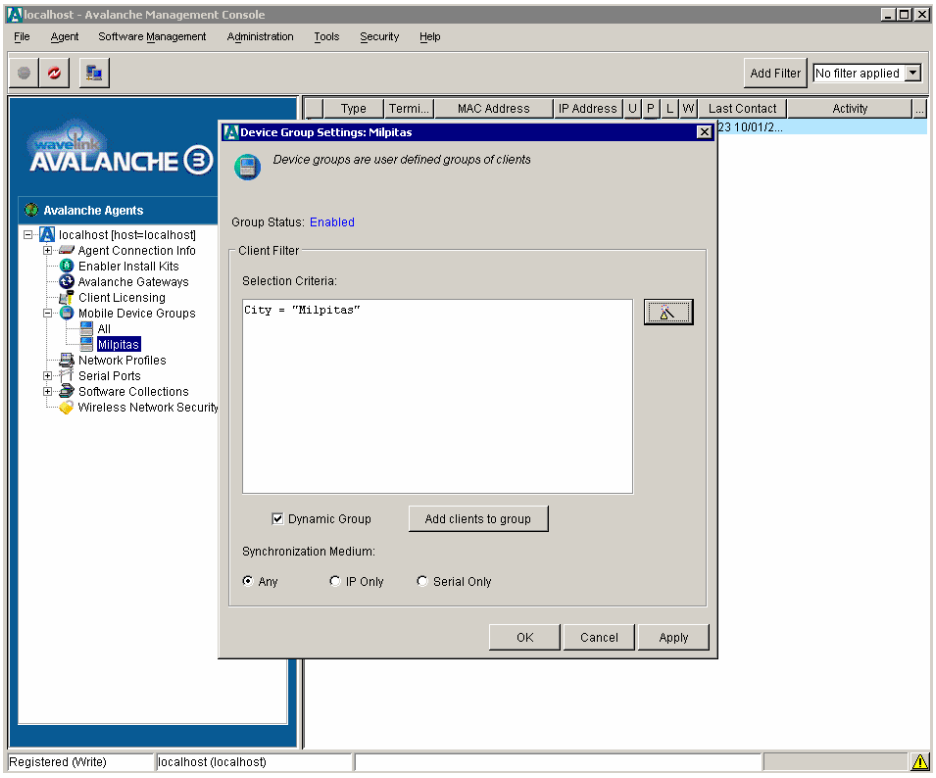
ModelName = CP7925G

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



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

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



To install the 7925G Configuration Utility for Wavelink Avalanche, select **"Install Software Package"** under the Software Management menu.

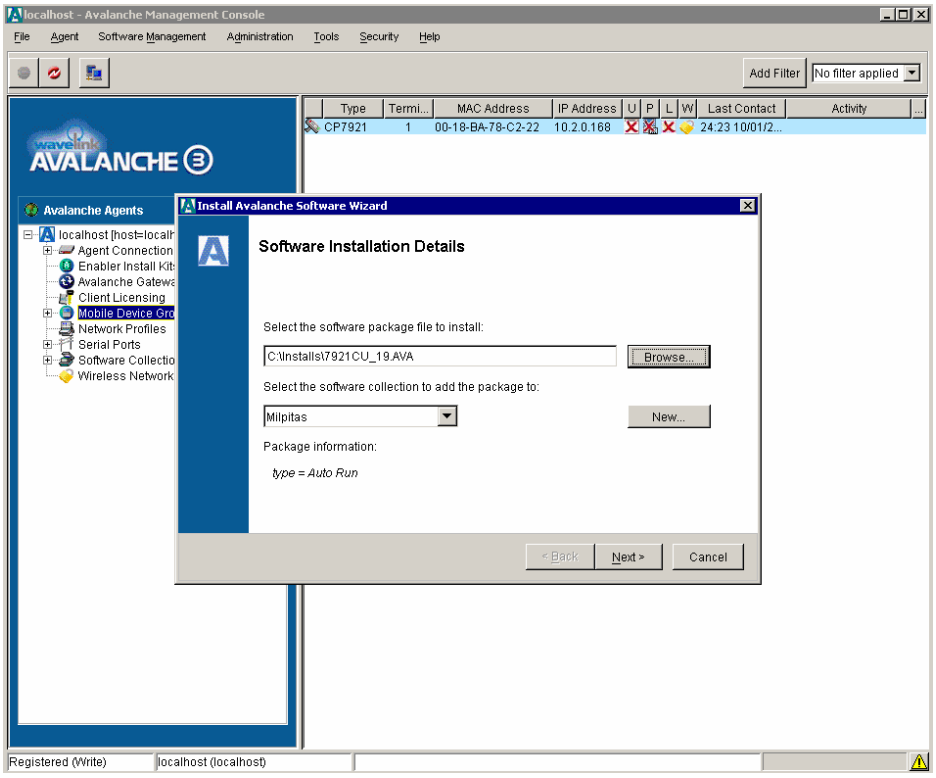
Browse to the 7925G Configuration Utility package file (i.e. 7925CU-1.3.1.AVA).

Create a software collection to add the package to.

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

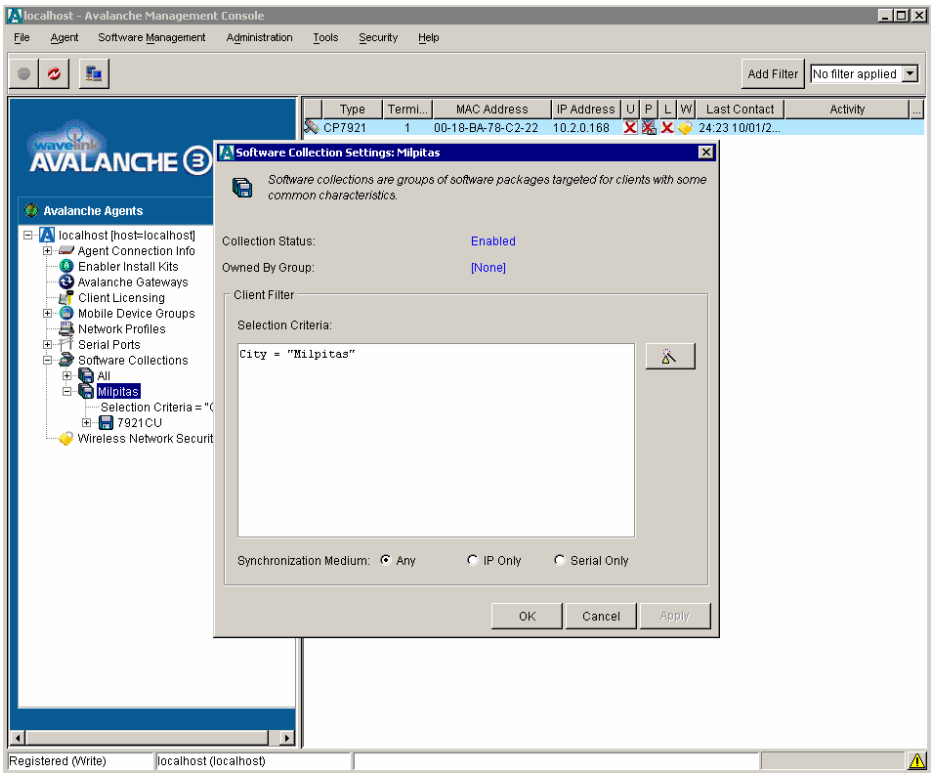
Click on **"Finish"** when the installation is complete.

Note: The 7925CU must be installed locally on the Wavelink Avalanche server.



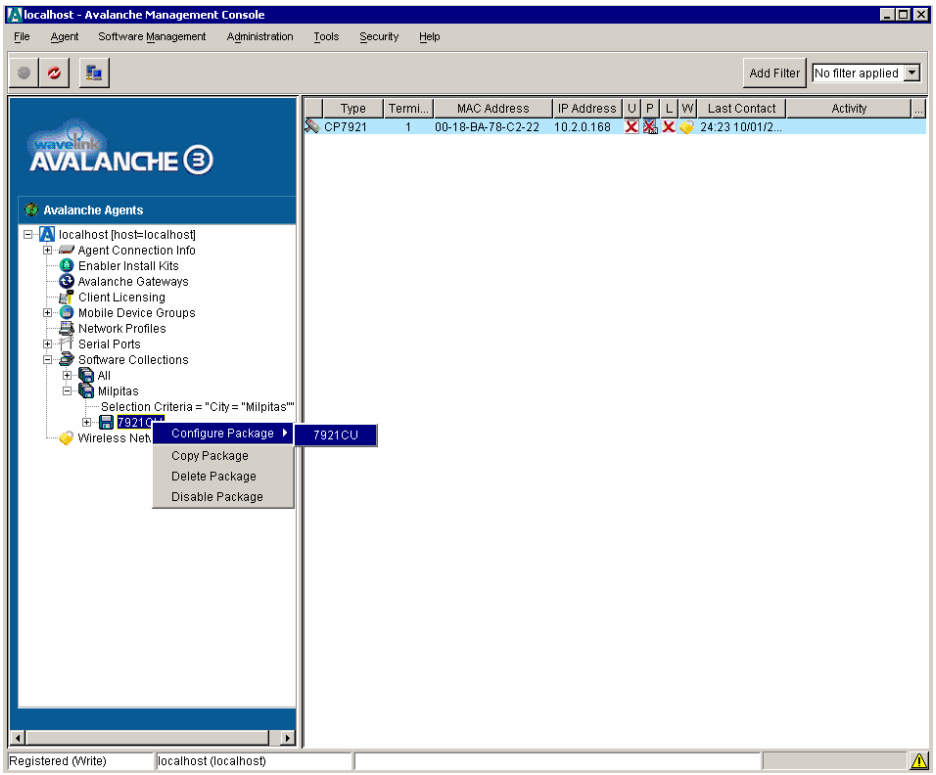
The software package must then be enabled by right clicking on the package and selecting **"Enable Package"**.

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



To configure the software package, right click on the package and select **“7921CU”**.

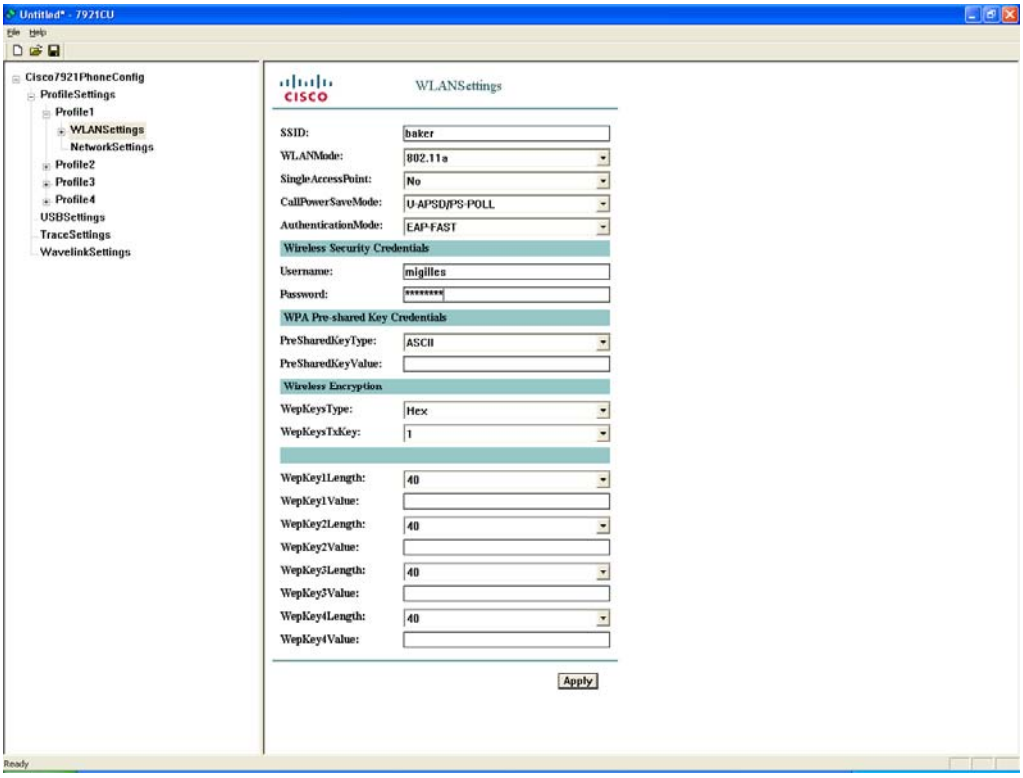
The 7925G Configuration Utility will then be launched.



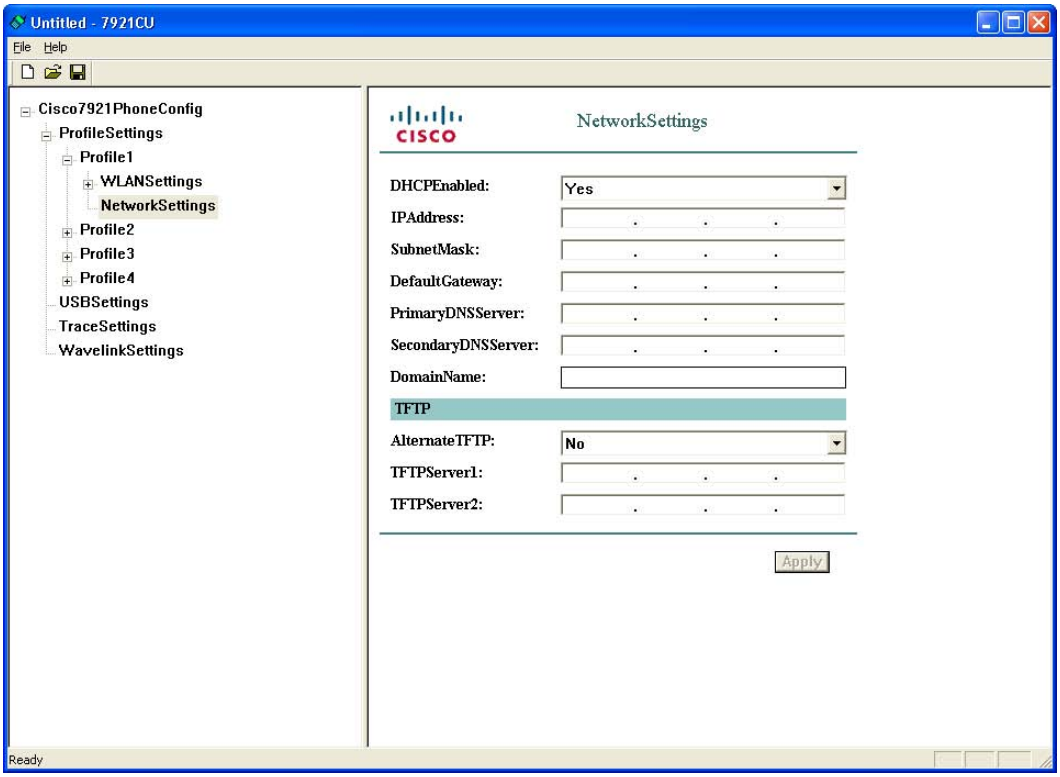
Enter the profile name and enable the profile.

Configure the network profiles by specifying the Wireless LAN credentials.

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



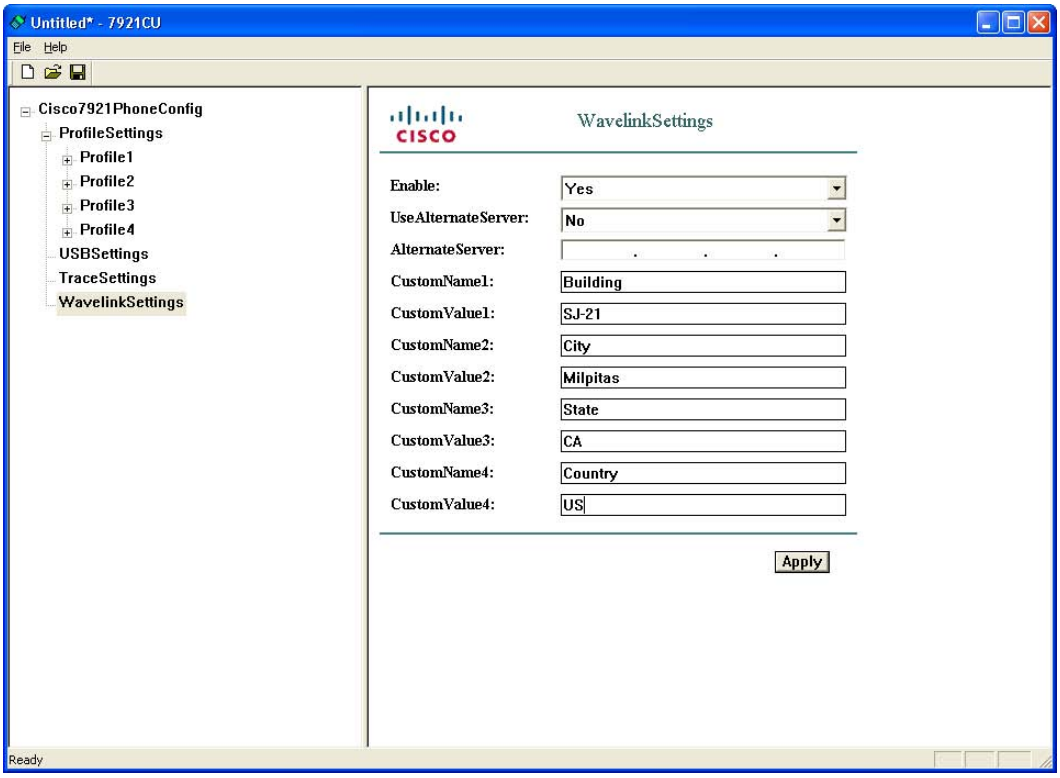
Configure the network settings for the network profile.



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 and select **"Update Now"**.

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

Using the 7925 Configuration Utility for Quick Deployment

The 7925 Configuration Utility can also be utilized to push out a default WLAN template to multiple Cisco Unified Wireless IP Phone 7925Gs.

Download the 7925 Configuration Utility from CCO.

Rename 7925CU-1.3.1.AVA to 7925CU-1.3.1.zip and extract the contents.

Launch the 7925 Configuration Utility (..\TempInstall.PRF\TempInstall.GRP\7921CU.PKG\APPS\7921CU\7921CU.exe). A template can then be configured with the necessary wireless LAN and network settings. Once the template is complete, it will then need to be exported into Wavelink format. Select **"Export to Wavelink"** under the file menu, which will create an encrypted template file named **"7921Wlan.cfg.enc"** file in the folder. The Cisco Unified Wireless IP Phone 7925G currently does a TFTP get for WLANDefault.xml and WLAN<MAC_ADDRES>.xml. Rename the **"7921Wlan.cfg.enc"** file to **"WLANDefault.xml"** and copy it to a TFTP server, where all phones directed to that TFTP server will download and apply that template.

The Cisco Unified Wireless IP Phone 7925G defaults with network profile 1 configured with an ssid **"cisco"** and open authentication. DHCP option 150 can be configured for that network to point to an alternate TFTP server containing the WLAN template file.

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

PEAP and EAP-TLS are not supported with the 7925 Configuration Utility at this time.

After pushing out the default WLAN template, remove the template from the TFTP server afterwards if the production voice network is using the same TFTP server to avoid from overwriting the current wireless LAN and network settings. If using a different TFTP server, may still want to remove the file to ensure that not just any Cisco Unified Wireless IP Phone 7925G can get on the wireless network.

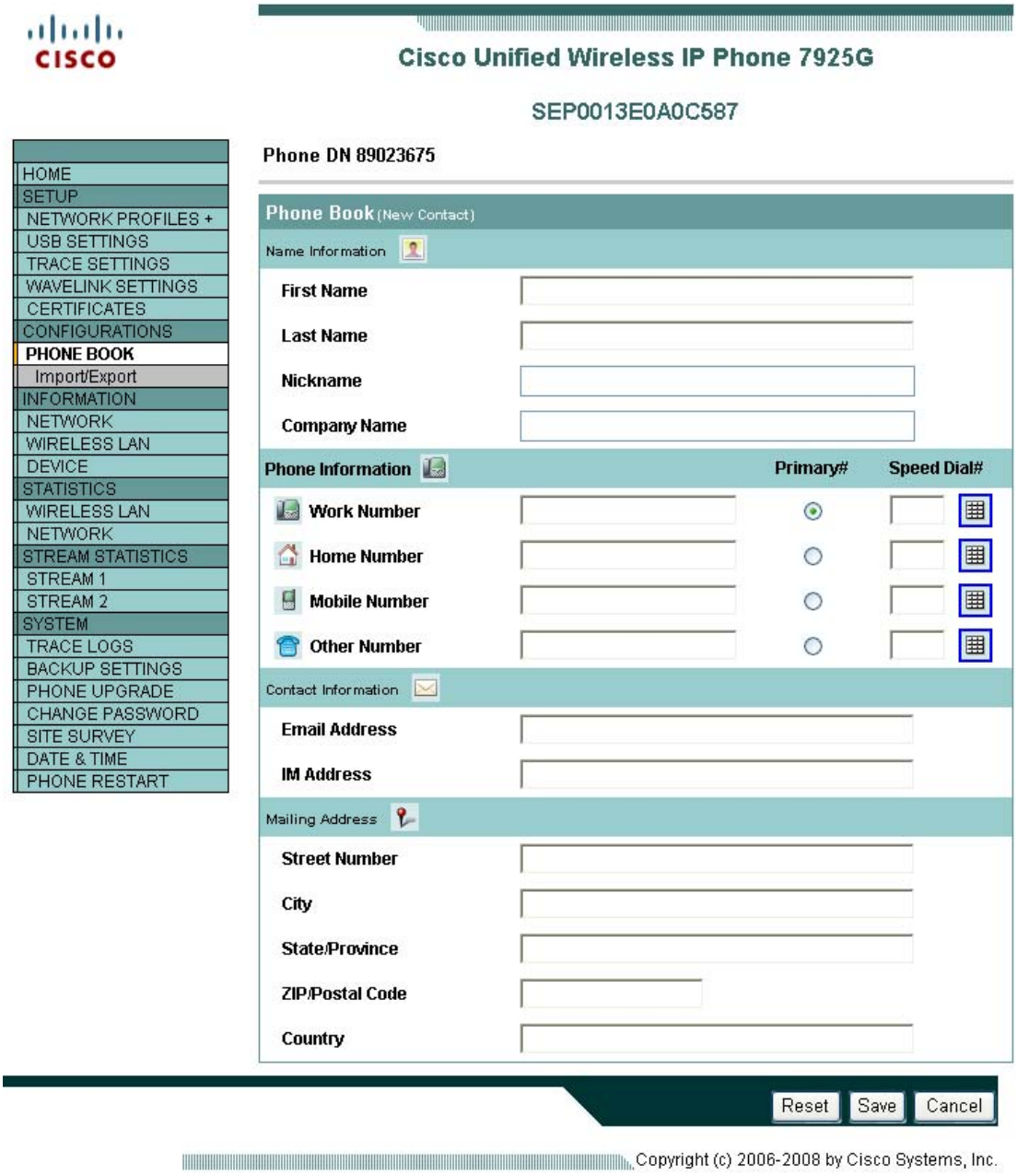
Configuring the Local Phone Book and Speed Dials

The Cisco Unified Wireless IP Phone 7925G contains local phone book and speed dials support.

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

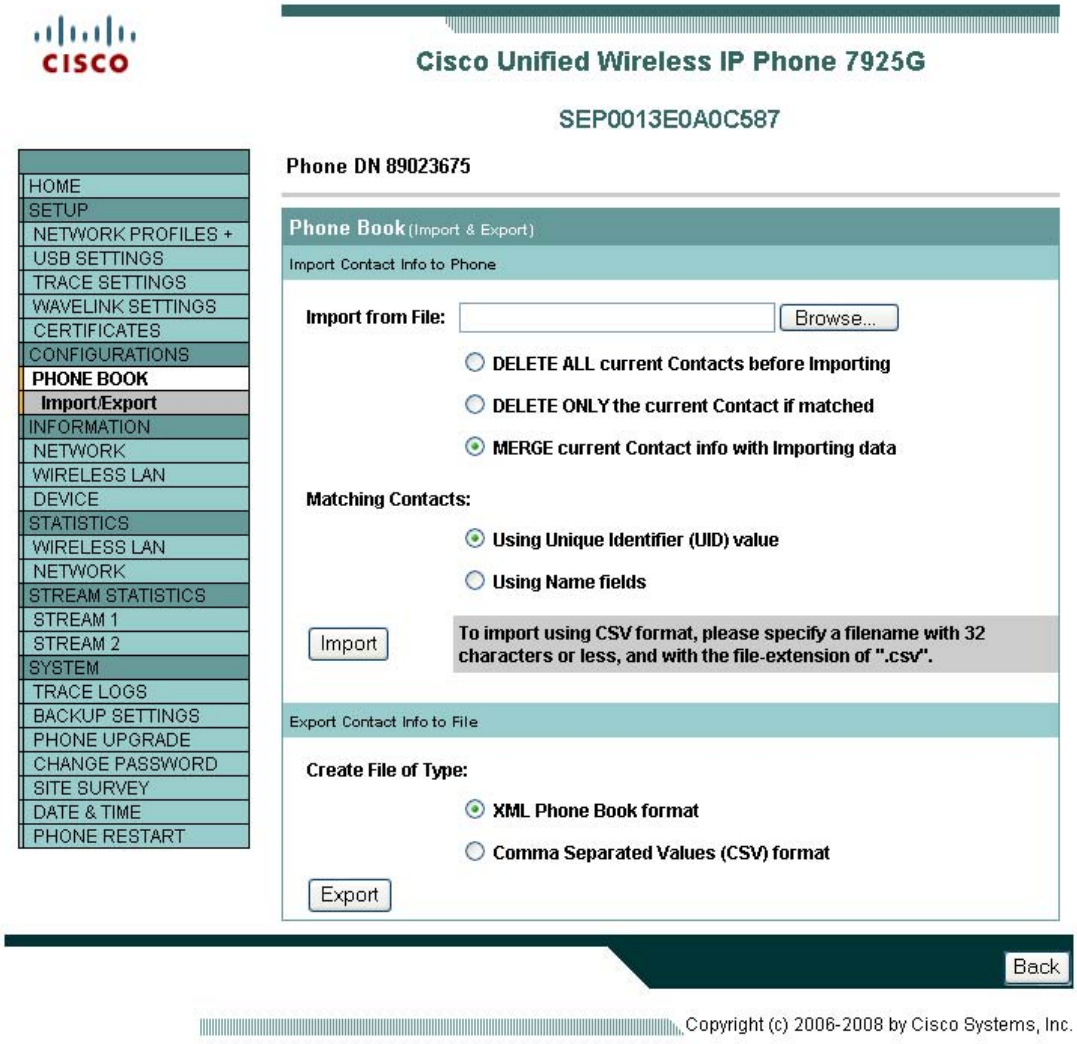
The left softkey on the home screen can be programmed for **"Message"** to access voice mail or to **"PhBook"** to access the local phone book.

The local phone book and speed dials can be configured via the local keypad or via the Cisco Unified Wireless IP Phone 7925G web interface. Since the web password is not managed by the user the web interface is primarily intended for use by the system administrator, where they can upload information into the phone book for the user. This requires that the **"Phone Book Web Access"** product specific configuration item be set to **"Allow Admin"**.



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

XML and CSV formats are supported as well as the CSV format used by the Cisco Unified Wireless IP Phone 7920.

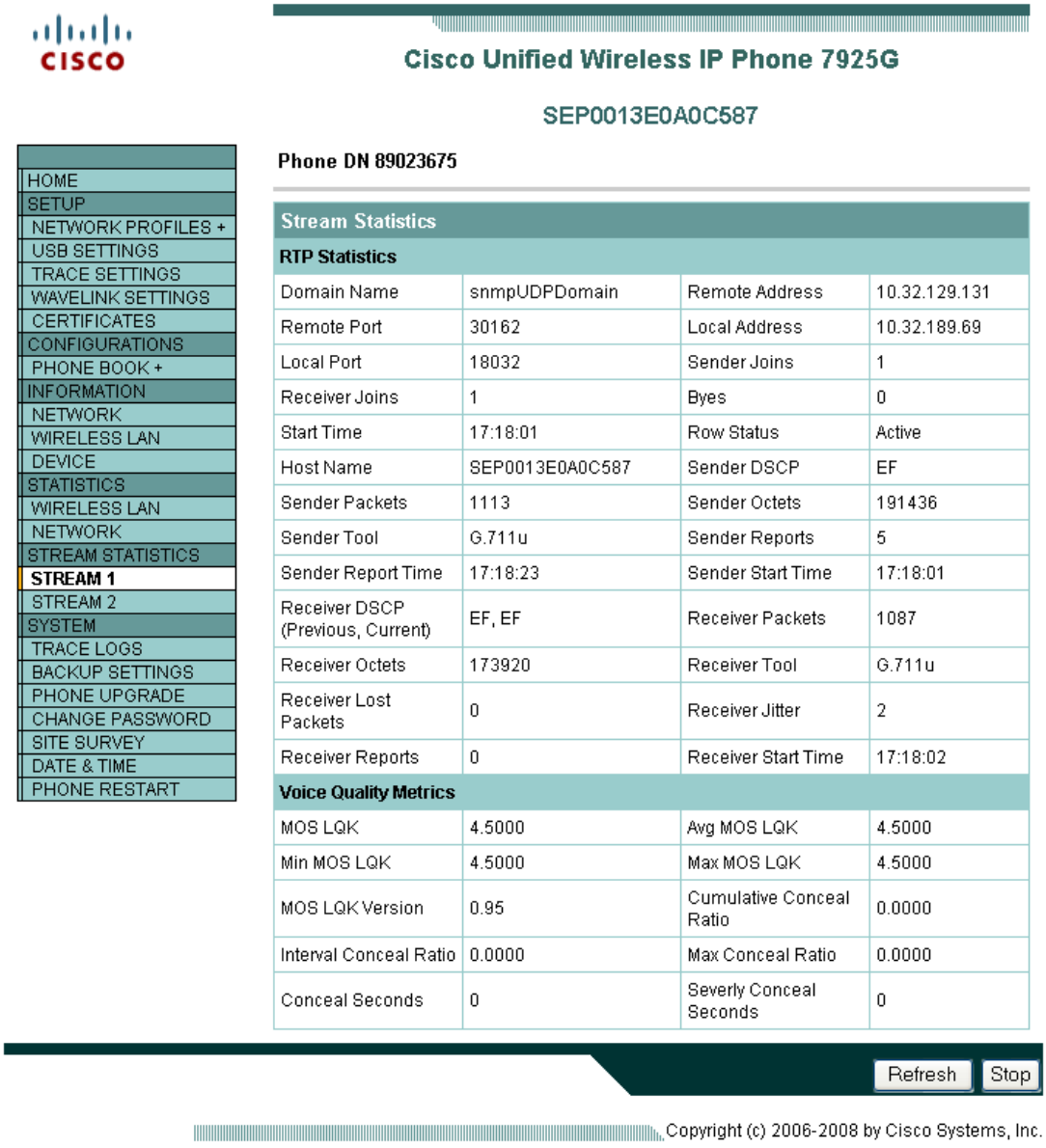


Troubleshooting

Stream Statistics

The Cisco Unified Wireless IP Phone 7925G 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.

Browse to the phone's web interface (https://x.x.x.x) and select **"Stream Statistics"** to view this information.

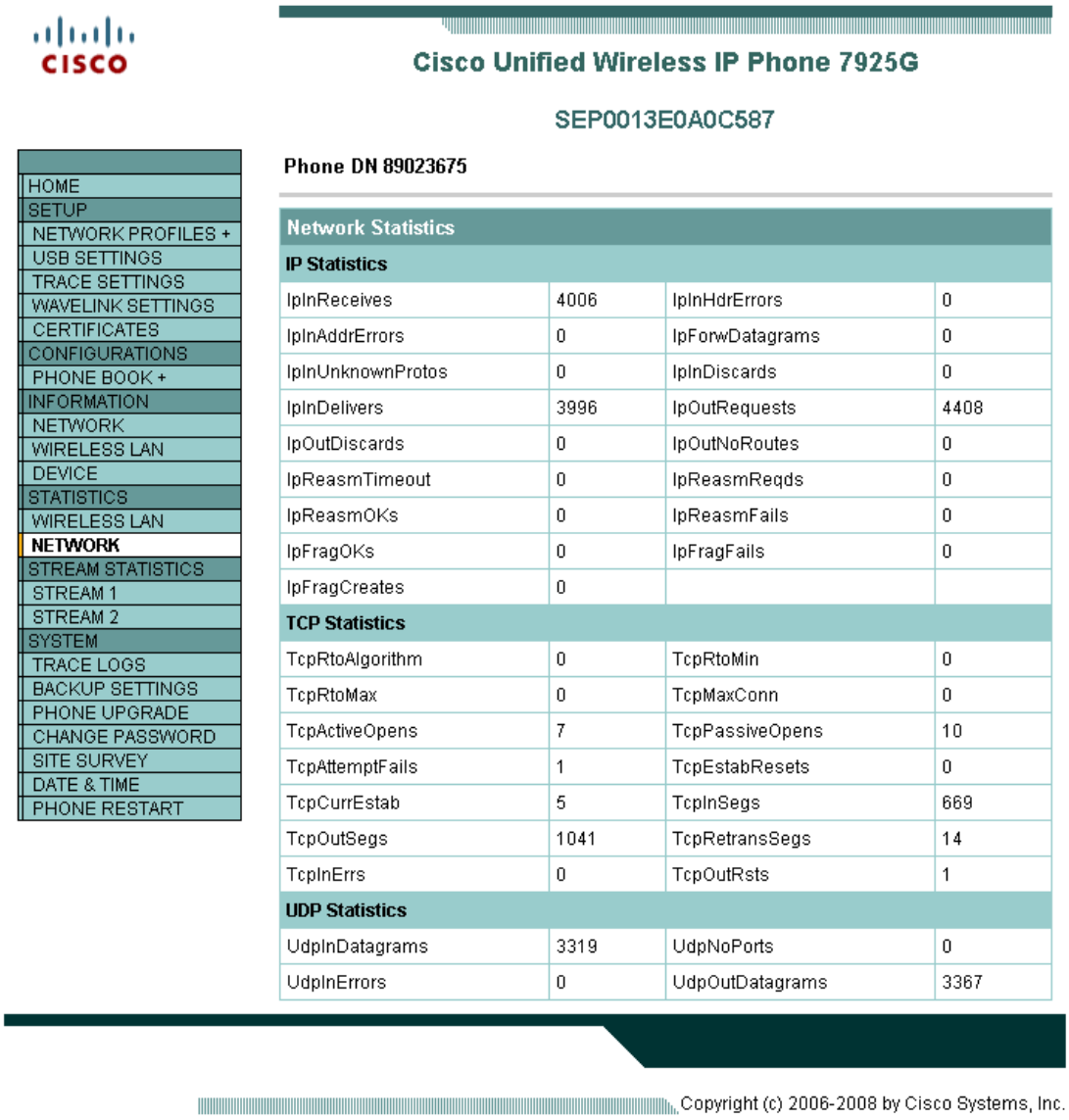


This information is also available locally on the phone under **Settings > Status > Call Statistics** or if on a phone call press the center button twice.

For more information, see the “Troubleshooting the Cisco Unified Wireless IP Phone 7925G” chapter in the *Cisco Unified Wireless IP Phone 7925G Administration Guide* at this URL:

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

Network Statistics



Cisco Unified Wireless IP Phone 7925G

SEP0013E0A0C587

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

Network Statistics			
IP Statistics			
IpInReceives	4006	IpInHdrErrors	0
IpInAddrErrors	0	IpForwDatagrams	0
IpInUnknownProtos	0	IpInDiscards	0
IpInDelivers	3996	IpOutRequests	4408
IpOutDiscards	0	IpOutNoRoutes	0
IpReasmTimeout	0	IpReasmReqds	0
IpReasmOKs	0	IpReasmFails	0
IpFragOKs	0	IpFragFails	0
IpFragCreates	0		
TCP Statistics			
TcpRtoAlgorithm	0	TcpRtoMin	0
TcpRtoMax	0	TcpMaxConn	0
TcpActiveOpens	7	TcpPassiveOpens	10
TcpAttemptFails	1	TcpEstabResets	0
TcpCurrEstab	5	TcpInSegs	669
TcpOutSegs	1041	TcpRetransSegs	14
TcpInErrs	0	TcpOutRsts	1
UDP Statistics			
UdpInDatagrams	3319	UdpNoPorts	0
UdpInErrors	0	UdpOutDatagrams	3367

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

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

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

This reflects that voice packets are being properly marked as UP6 (VO) downstream to the Cisco Unified Wireless IP Phone 7925G.

Wireless LAN Statistics

Cisco Unified Wireless IP Phone 7925G

SEP0013E0A0C587

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	4068	Rx error frames	0
Rx unicast frames	4068	Rx multicast frames	0
Rx broadcast frames	0	Rx FCS frames	0
Rx beacons	651	Association Rejects	0
Association Timeouts	0	Authentication Rejects	0
Authentication Timeouts	0		
Tx Statistics (Best Effort)			
Tx OK Frames	0	Tx error frames	0
Tx unicast frames	0	Tx multicast frames	0
Tx broadcast frames	0	RTS fail counter	0
ACK fail counter	0	Retries counter	0
Multiple retries counter	0	Failed retries counter	0
Tx timeout counter	0	Other fail counter	0
Success counter	0	Max retry limit counter	0
Tx Statistics (Voice)			
Tx OK Frames	3266	Tx error frames	1
Tx unicast frames	3266	Tx multicast frames	0
Tx broadcast frames	0	RTS fail counter	0
ACK fail counter	0	Retries counter	129
Multiple retries counter	16	Failed retries counter	1
Tx timeout counter	0	Other fail counter	0
Success counter	3266	Max retry limit counter	1

Traffic Stream Metrics (TSM)

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

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

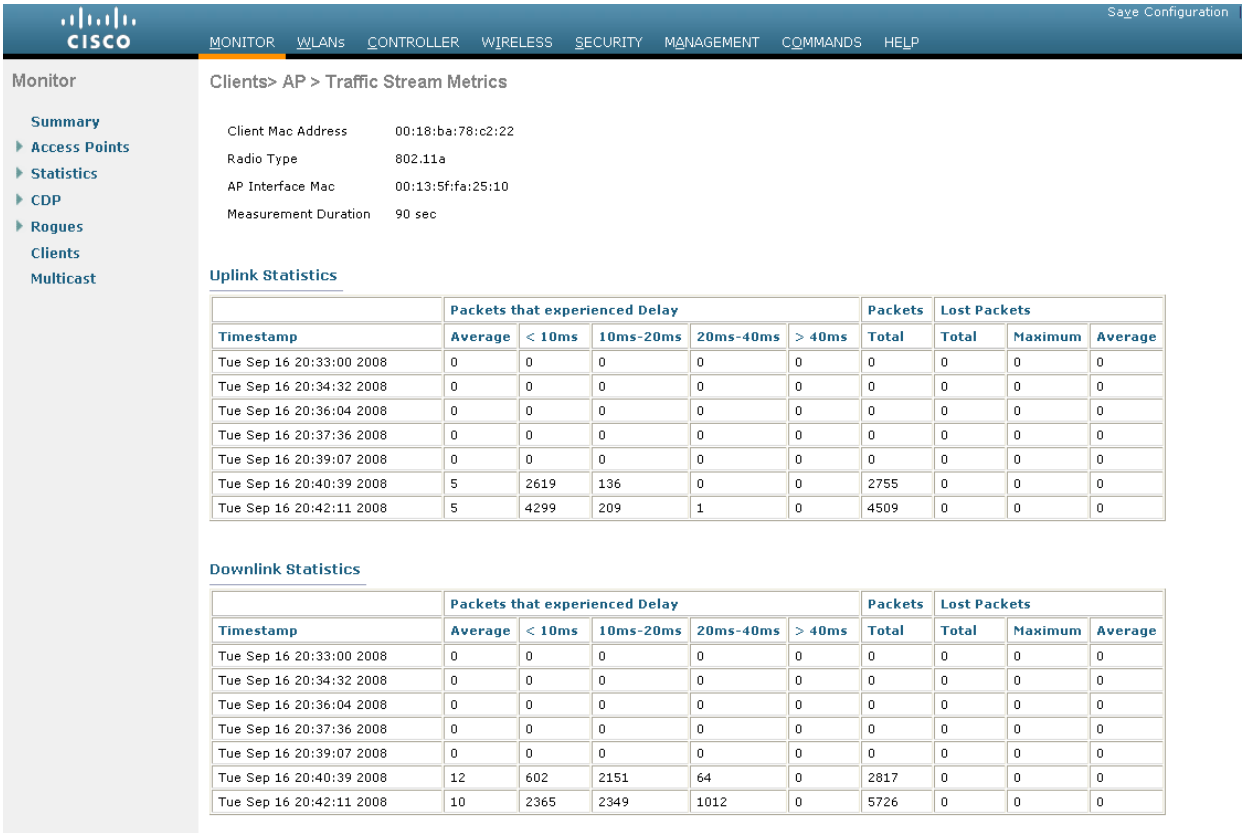
Check the box **"Metrics Collection"** in the global 802.11 Voice Parameters to enable Traffic Stream Metrics.

See the "Call Admission Control Settings" section for further information on how to enable TSM.

To view Traffic Stream Metrics data for a client, select TSM from the drop down menu for which band the Cisco Unified Wireless IP Phone 7925G 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

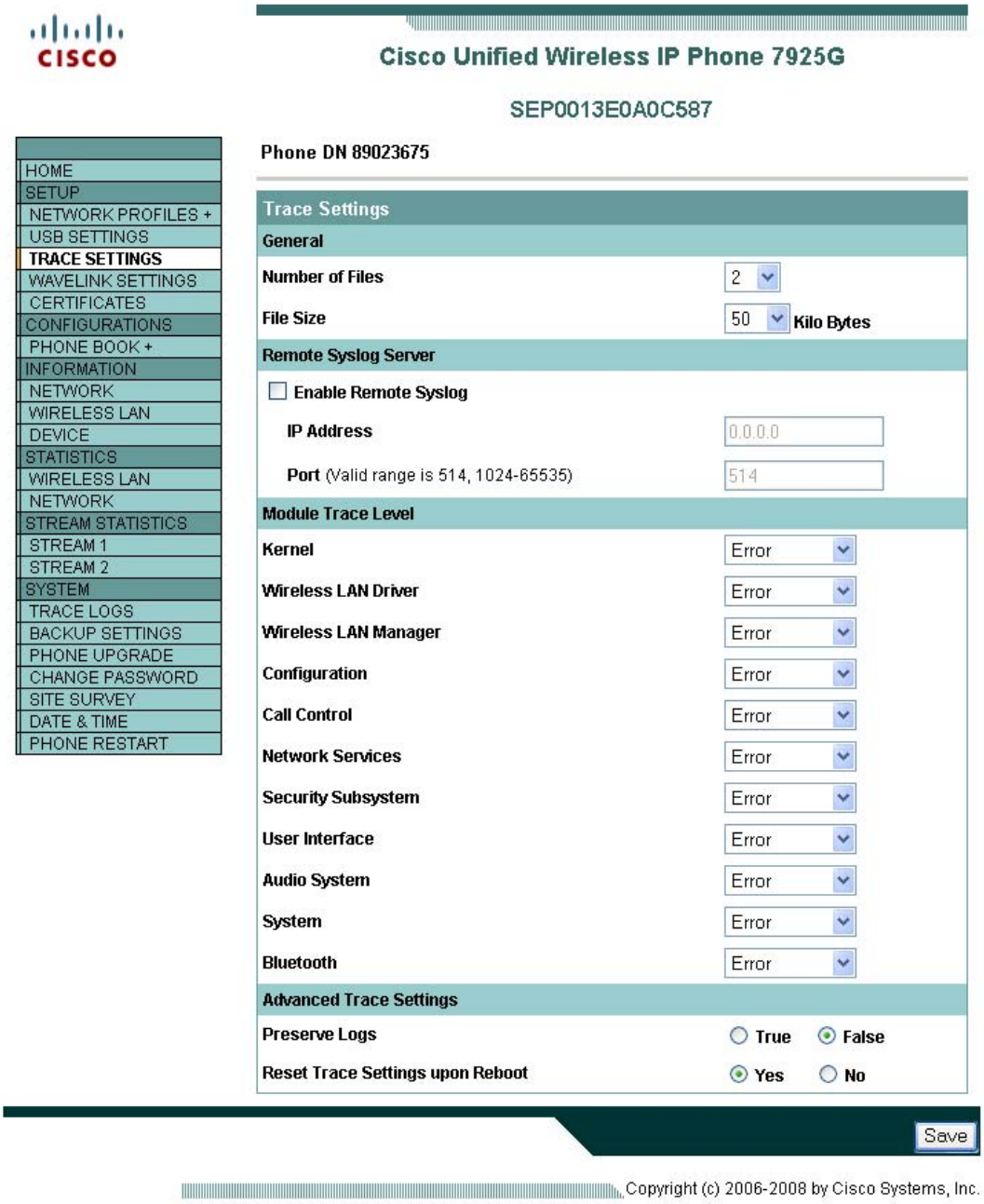
	Packets that experienced Delay					Packets	Lost Packets		
Timestamp	Average	< 10ms	10ms-20ms	20ms-40ms	> 40ms	Total	Total	Maximum	Average
Tue Sep 16 20:33:00 2008	0	0	0	0	0	0	0	0	0
Tue Sep 16 20:34:32 2008	0	0	0	0	0	0	0	0	0
Tue Sep 16 20:36:04 2008	0	0	0	0	0	0	0	0	0
Tue Sep 16 20:37:36 2008	0	0	0	0	0	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

Phone Logs

Phone logs for troubleshooting purposes can be obtained from the Cisco Unified Wireless IP Phone 7925G web interface.

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

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



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
Bluetooth	Bluetooth

Trace Levels

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

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

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

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

The trace level will reset to **"Error"** level by default unless configured to preserve the trace levels.

Radio Diagnostics

As of the 1.3(3) release, the Cisco Unified Wireless IP Phone 7925 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.

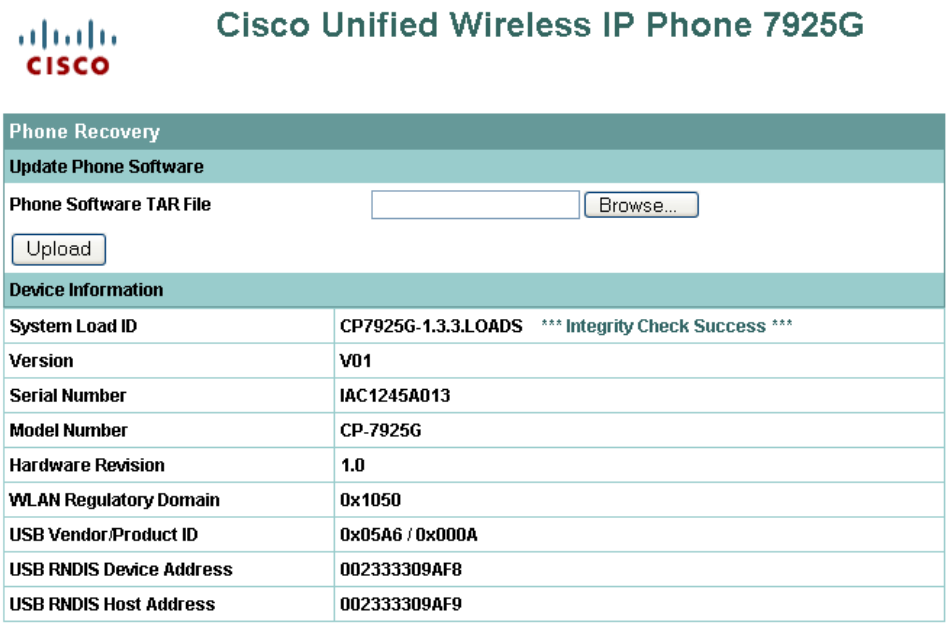
Green – The phone is currently authenticated to the access point.

Firmware Recovery

If the Cisco Unified Wireless IP Phone 7925G does no boot properly, then the firmware can be recovered via the USB connection.

1. Power on the phone while holding down the application button and the speakerphone button simultaneiously and keep it helf 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, then click on **"Upload"**.



Restoring Factory Defaults

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

The factory default option erases all user-defined entries in Network Profiles, Phone Settings, and Call History.

To erase the local configuration, follow these steps:

6. Choose Settings > Phone Settings.
7. Press **"**2"** on the keypad.

   The phone briefly displays **"Restore to Default?"**
8. Press the **"Yes"** softkey to confirm or **"No"** to cancel.

   The phone resets after selecting **"Yes".**

Healthcare Environments

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

Cleaning the Phone

The Cisco Unified Wireless IP Phone 7925G is IP54 rated, which is designed to provide protection from dust, liquid splashes and moisture. This allows the Cisco Unified Wireless IP Phone 7925G to be cleaned, sanitized without the possibility of damaging the unit.

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

Phone Accessories

You can order these accessories for the Cisco Unified Wireless IP Phone 7925G.

For more information, refer to the *Cisco Unified Wireless IP Phone 7925G Accessories Guide* at this URL:

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

- Batteries — Standard and Extended
- Carry Cases — Holster and Leather
- Multi-Charger
- Lock Set
- USB Cable

3rd Party Accessories

- Carry Cases — www.zcover.com, www.systemwear.com
- Chargers — www.zcover.com
- Headsets — www.plantronics.com (Quick Disconnect 2.5 mm Adapter – part # 65287-01), www.jawbone.com, www.jabra.com

Note: The Cisco Unified Wireless IP Phone 7925G, 7921G and 7920 accessories are not interchangeable (except the lock set for 7921G and 7925G).

Additional Documentation

Cisco Unified Wireless IP Phone 7925G Data Sheet
http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps9900/data_sheet_c78-504890.html

Cisco Unified Wireless IP Phone 7925G Administration Guide
http://www.cisco.com/en/US/products/hw/phones/ps379/prod_maintenance_guides_list.html

Cisco Unified Wireless IP Phone 7925G Phone Guide and Quick Reference
http://www.cisco.com/en/US/products/hw/phones/ps379/products_user_guide_list.html

Cisco Unified Wireless IP Phone 7925G Firmware
http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser-crypto

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/products/ps7273/tsd_products_support_series_home.html

Cisco Voice Software
http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml

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

Cisco Unified IP Phone Services Application Development Notes
http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/all_models/xsi/6_0/english/programming/guide/XSIbook.html

Cisco Unified Communications SRND
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/uc7_0.html

Mobility SRND
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns279/c649/ccmigration_09186a00808d9330.pdf

Cisco Unified Wireless LAN Controller Documentation
http://www.cisco.com/en/US/products/ps6366/products_installation_and_configuration_guides_list.html

Autonomous Access Point Documentation
http://www.cisco.com/en/US/products/ps6521/products_installation_and_configuration_guides_list.html

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