



## Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Deployment Guide



The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G are 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, 7925G-EX, and 7926G are Bluetooth 2.0 + EDR (Enhanced Data Rate) compliant and supports both the headset and hands-free profiles. The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G are MIL-STD-810F, Method 516.5, Procedure I compliant. The Cisco Unified Wireless IP Phone 7925G and 7926G is IP54 rated protecting it from dust, liquid splashes and moisture, where the Cisco Unified Wireless IP Phone 7925G-EX is IP64 rated for complete dust protection and also certified for use in explosive and hazardous environments.

This guide provides information and guidance to help the network administrator deploy the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G successfully in a wireless LAN environment.

## Revision History

Date	Comments
10/13/08	1.3(1) Release
11/17/09	1.3(2) and 1.3(3) Release
05/03/10	1.3(4) Release
08/30/10	1.3(4)SR2 Release
12/15/10	1.4(1) Release
08/14/12	1.4(1)SR1 and 1.4(2) Release
08/21/12	1.4(3) Release

# Contents

<b>Cisco Unified Wireless IP Phone 7925G, 7925G-EX, 7926G Overview .....</b>	<b>7</b>
<b>Requirements for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G .....</b>	<b>7</b>
<i>Site Survey</i> .....	7
<i>RF Validation</i> .....	7
<i>Call Control</i> .....	9
<i>Protocols</i> .....	9
<i>Access Points</i> .....	10
<i>Antennas</i> .....	11
<b>Models .....</b>	<b>12</b>
<i>7925G-EX Certifications</i> .....	13
<i>7926G Barcode Scanner</i> .....	14
<i>World Mode (802.11d)</i> .....	15
Supported Countries .....	15
<i>Radio Characteristics</i> .....	16
<i>Language Support</i> .....	17
<b>Bluetooth .....</b>	<b>17</b>
<i>Bluetooth Profiles</i> .....	18
<i>Coexistence (802.11b/g + Bluetooth)</i> .....	18
<b>Security.....</b>	<b>19</b>
<i>Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling (EAP-FAST)</i> .....	20
<i>Extensible Authentication Protocol – Transport Layer Security (EAP-TLS)</i> .....	21
<i>Protected Extensible Authentication Protocol (PEAP)</i> .....	23
<i>Cisco Centralized Key Management (CCKM)</i> .....	25
<i>EAP and User Database Compatibility</i> .....	25
<b>Power Management.....</b>	<b>26</b>
<i>Protocols</i> .....	27
Unscheduled Auto Power Save Delivery (U-APSD) .....	27
Power Save Poll (PS-POLL).....	27
Active Mode .....	27
<i>Delivery Traffic Indicator Message (DTIM)</i> .....	28
<i>Scan Modes</i> .....	28
<b>Quality of Service (QoS) .....</b>	<b>28</b>
<i>Configuring QoS in Cisco Unified Communications Manager</i> .....	29
<i>Configuring QoS Policies for the Network</i> .....	29
Configuring Cisco Switch Ports .....	29
Configuring Cisco IOS Access Points.....	30
Configuring Switch Ports for Wired IP Phones.....	30
Sample Voice Packet Capture.....	31
<i>Call Admission Control</i> .....	31
Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Deployment Guide	3

Pre-Call Admission Control.....	32
Roaming Admission Control .....	33
<i>Traffic Classification (TCLAS)</i> .....	33
<b>Roaming .....</b>	<b>34</b>
<i>Interband Roaming</i> .....	34
<b>Multicast.....</b>	<b>35</b>
<b>Designing the Wireless LAN for Voice.....</b>	<b>35</b>
<i>Planning Channel Usage</i> .....	36
5 GHz (802.11a) .....	36
Using Dynamic Frequency Selection (DFS) on Access Points.....	36
2.4 GHz (802.11b/g) .....	38
Signal Strength and Coverage.....	38
<i>Configuring Data Rates</i> .....	41
<i>Call Capacity</i> .....	41
<i>Dynamic Transmit Power Control (DTPC)</i> .....	42
<i>Multipath</i> .....	42
<i>Verification with Site Survey Tools</i> .....	43
Cisco 792xG Neighbor List .....	44
Cisco 792xG Site Survey .....	45
<b>Configuring Cisco Unified Communications Manager .....</b>	<b>47</b>
<i>Phone Button Templates</i> .....	47
<i>Softkey Templates</i> .....	47
<i>Security Profiles</i> .....	48
<i>G.722 Advertisement</i> .....	48
<i>Common Settings</i> .....	49
<i>Audio Bit Rates</i> .....	49
<i>Product Specific Configuration Options</i> .....	50
<b>Configuring the Cisco Unified Wireless LAN Controller and Access Points .....</b>	<b>56</b>
<i>SSID / WLAN Settings</i> .....	57
<i>Controller Settings</i> .....	59
<i>802.11 Network Settings</i> .....	61
Auto RF (RRM) .....	63
Call Admission Control .....	67
EDCA Parameters.....	70
DFS (802.11h) .....	71
CleanAir.....	71
<i>Multicast Direct</i> .....	72
<i>QoS Profiles</i> .....	73
<i>QoS Basic Service Set (QBSS)</i> .....	75
<i>CCKM Timestamp Tolerance</i> .....	76
<i>Auto-Immune</i> .....	77
<i>WLAN Controller Advanced EAP Settings</i> .....	78

<i>Proxy ARP</i> .....	79
<i>TKIP Countermeasure Holdoff Time</i> .....	79
<i>VLANs and Cisco Autonomous Access Points</i> .....	80
<b>Configuring the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G</b> .....	<b>80</b>
<i>Wireless LAN Settings</i> .....	81
<i>Bluetooth Settings</i> .....	86
<i>Installing Certificates</i> .....	87
<i>Using Templates to Configure Phones</i> .....	93
<i>Wavelink Avalanche</i> .....	94
<i>Using the Bulk Deployment Utility</i> .....	101
Default Export.....	104
Bulk Export.....	104
Pushing Configuration Files to the Cisco 792xG .....	105
<i>Local Phone Book and Speed Dials</i> .....	105
<i>Increased Font</i> .....	107
<i>Using the Cisco Unified IP Phone 7925G Desktop Charger</i> .....	108
Bluetooth Pairing .....	108
Docking.....	109
<i>Using Phone Designer</i> .....	110
<i>Upgrading Firmware</i> .....	111
<b>IP Phone Services</b> .....	<b>113</b>
<i>Extensible Markup Language (XML)</i> .....	113
<i>Java Mobile Information Device Profile (MIDP)</i> .....	114
<b>Troubleshooting</b> .....	<b>114</b>
<i>Stream Statistics</i> .....	114
<i>Network Statistics</i> .....	116
<i>Wireless LAN Statistics</i> .....	117
<i>7926G Barcode Status Messages</i> .....	117
<i>Traffic Stream Metrics (TSM)</i> .....	118
<i>Phone Logs</i> .....	119
Trace Modules .....	120
Trace Levels.....	121
<i>Radio Status Indicator</i> .....	121
<i>Hardware Diagnostics</i> .....	121
<i>Firmware Recovery</i> .....	122
<i>Restoring Factory Defaults</i> .....	123
<i>Capturing a Screenshot of the Phone Display</i> .....	123
<b>Healthcare Environments</b> .....	<b>123</b>
<b>Cleaning the Phone</b> .....	<b>124</b>
<b>Accessories</b> .....	<b>124</b>

**Additional Documentation ..... 127**

# Cisco Unified Wireless IP Phone 7925G, 7925G-EX, 7926G Overview

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G provide mobile communication within enterprises. The levels of voice quality performance that have come to be expected from Cisco products are maintained in the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G with the inclusion of Cisco Compatible eXtensions (CCX).

Cisco's implementation of 802.11, employing CCX, permits time sensitive applications such as voice to operate efficiently across campus wide wireless LAN (WLAN) deployments. These extensions provide fast roaming capabilities and an almost seamless flow of voice traffic, whilst maintaining security as the end user roams between access points.

It should be understood that WLAN uses unlicensed spectrum, and as a result it may experience interference from other devices using the unlicensed spectrum. The proliferation of devices in the 2.4 GHz spectrum, such as Bluetooth headsets, Microwave ovens, cordless consumer phones, means that the 2.4 GHz spectrum may contain more congestion than other spectrums. The 5 GHz spectrum has far fewer devices operating in this spectrum and is the preferred spectrum to operate the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G in order to take advantage of the 802.11n data rates available. Despite the optimizations that Cisco have implemented in the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, the use of unlicensed spectrum means that uninterrupted communication can not be guaranteed, and there may be the possibility of voice or video gaps of up to several seconds during multimedia conversations. Adherence to the deployment guidelines will reduce the likelihood of these voice and video gaps being present, but there is always this possibility. Through the use of unlicensed spectrum, and the inability to guarantee the delivery of messages to a WLAN device, the Cisco is not intended as a medical device and should not be used to make clinical decisions.

## Requirements for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G are IEEE 802.11a/b/g wireless IP phones that provide voice communications.

The wireless LAN must be validated to ensure it meets the requirements to deploy the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

### Site Survey

Before deploying the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G into a production environment, a site survey must be completed by a Cisco certified partner with the advanced wireless LAN specialization. During the site survey the RF spectrum can be analyzed to determine which channels are usable in the desired frequency band (2.4 GHz or 5 GHz). Typically there is less interference in the 5 GHz band as well as more non-overlapping channels, so 5 GHz is the preferred frequency band for operation and even more highly recommended when the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G is to be used in a mission critical environment. The site survey will include heatmaps showing the intended coverage plan for the location. The site survey will also determine the access point platform type, antenna type, and access point configuration (channel and transmit power) to use at the location. See the [Designing the Wireless LAN for Voice](#) section for more information.

Refer to the Steps to Success website for additional information.

<http://www.cisco.com/go/stepstosuccess>

### RF Validation

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

## **Signal**

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

This ensures that the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G always has adequate signal and can hold a signal long enough in order to roam seamlessly where signal based triggers are utilized vs. packet loss triggers.

Also need to ensure that the upstream signal from the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G meets the access point's receiver sensitivity for the transmitted data rate. Rule of thumb is to ensure that the received signal at the access point is -67 dBm or higher.

It is recommended to design the cell size to ensure that the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G can hold a signal for at least 5 seconds.

## **Channel Utilization**

Channel Utilization levels should be kept under 50%.

If using the 7925G, 7925G-EX, and 7926G phone, this is provided via the QoS Basic Service Set (QBSS), which equates to around 105.

## **Noise**

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

Also need to ensure that the upstream signal from the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G can meet the access point's signal to noise ratio for the transmitted data rate.

## **Packet Loss / Delay**

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

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

## **Retries**

802.11 retransmissions should be less than 20%.

## **Multipath**

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

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

- Cisco Prime Network Control System (NCS) for Unified Wireless LAN Management  
[http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps11682/ps11686/ps11688/data\\_sheet\\_c78-650051.html](http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps11682/ps11686/ps11688/data_sheet_c78-650051.html)
- Cisco Wireless Control System (WCS) for Unified Wireless LAN Management  
[http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product\\_data\\_sheet0900aecd802570d0.html](http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd802570d0.html)
- Cisco Wireless LAN Solution Engine (WLSE) for Cisco Autonomous Wireless LAN Management  
[http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6380/ps6563/ps3915/ps6839/product\\_data\\_sheet0900aecd80410b92.html](http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6380/ps6563/ps3915/ps6839/product_data_sheet0900aecd80410b92.html)
- Cisco Spectrum Expert  
[http://www.cisco.com/en/US/prod/collateral/wireless/ps9391/ps9393/product\\_data\\_sheet0900aecd807033c3.html](http://www.cisco.com/en/US/prod/collateral/wireless/ps9391/ps9393/product_data_sheet0900aecd807033c3.html)
- Cisco Unified Operations Manager  
[http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6491/ps6705/ps6535/data\\_sheet\\_c78-636705.html](http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6491/ps6705/ps6535/data_sheet_c78-636705.html)



- AirMagnet (Survey, WiFi Analyzer, VoFi Analyzer, Spectrum Analyzer)  
<http://www.airmagnet.com>

## Call Control

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G utilize Skinny Client Control Protocol (SCCP) for call control with the following communications platforms.

### 7925G and 7925G-EX

- Cisco Unified Communications Manager 4.3, 5.1, 6.0, 6.1, 7.0, 7.1, 8.0, 8.5, 8.6, and later.
- Cisco Unified Communications Manager Express 4.3 and later (Minimum of 12.4(15)T7)
- Cisco Unified Survivable Remote Site Telephony (SRST) 4.3 and later (Minimum of 12.4(15)T7)

### 7926G

- Cisco Unified Communications Manager 7.1(5), 8.0, 8.5, 8.6, and later
- Cisco Unified Communications Manager Express 8.6 and later
- Cisco Unified Survivable Remote Site Telephony (SRST) 8.6 and later

## Device Support in Cisco Unified Communications Manager

Cisco Unified Communications Manager requires a device package to be installed or service release update in order to enable Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G device support.

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

Device packages for Cisco Unified Communications Manager are available at the following location.

<http://www.cisco.com/cisco/software/navigator.html?mdfid=278875240>

## Protocols

Supported voice and wireless LAN protocols include the following:

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

## Access Points

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G are supported on both the Cisco Unified and Cisco Autonomous solutions.

Below is the supported version information for each Cisco solution.

- Cisco Unified Wireless LAN Controller  
Minimum = 6.0.202.0  
Recommended = 7.0.235.0 or 7.2.110.0
- Cisco IOS Access Points (Autonomous)  
Minimum = 12.4(21a)JY  
Recommended = 12.4(25d)JA or later

The supported access point models are listed below.



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

Cisco AP Series	802.11a	802.11b	802.11g	802.11n	Unified	Autonomous
500	No	Yes	Yes	No	Yes	Yes
600	Yes	Yes	Yes	Yes	Yes	No

<b>1040</b>	Yes	Yes	Yes	Yes	Yes	Yes
<b>1100</b>	No	Yes	Optional	No	Yes	Yes
<b>1130 AG</b>	Yes	Yes	Yes	No	Yes	Yes
<b>1140</b>	Yes	Yes	Yes	Yes	Yes	Yes
<b>1200</b>	Optional	Yes	Optional	No	Yes	Yes
<b>1230 AG</b>	Yes	Yes	Yes	No	Yes	Yes
<b>1240 AG</b>	Yes	Yes	Yes	No	Yes	Yes
<b>1250</b>	Yes	Yes	Yes	Yes	Yes	Yes
<b>1260</b>	Yes	Yes	Yes	Yes	Yes	Yes
<b>3500</b>	Yes	Yes	Yes	Yes	Yes	Yes
<b>3600</b>	Yes	Yes	Yes	Yes	Yes	No
<b>860</b>	No	Yes	Yes	Yes	No	Yes
<b>870</b>	No	Yes	Yes	No	No	Yes
<b>880</b>	No	Yes	Yes	Yes	Yes	Yes
<b>890</b>	Yes	Yes	Yes	Yes	Yes	Yes
<b>UC500</b>	No	Yes	Yes	No	No	Yes

**Note:** VoWLAN is not currently supported in conjunction with outdoor MESH technology (1500 series). 3<sup>rd</sup> party access points have limited support, as there is no interoperability testing performed against 3<sup>rd</sup> party access points. However the user should have basic functionality when connected to a Wi-Fi compliant access point.

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G can take advantage of Cisco Client Extensions (CCX) enabled access points.

See the following links for more info on CCX.

[http://www.cisco.com/web/partners/pr46/pr147/partners\\_pgm\\_concept\\_home.html](http://www.cisco.com/web/partners/pr46/pr147/partners_pgm_concept_home.html)

[http://www.cisco.com/web/partners/pr46/pr147/program\\_additional\\_information\\_new\\_release\\_features.html](http://www.cisco.com/web/partners/pr46/pr147/program_additional_information_new_release_features.html)

## Antennas

Some of the Cisco Access Points require 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](http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/product_data_sheet09186a008008883b.html)

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

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

[http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6973/positioning\\_statement\\_c07-565470.html](http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6973/positioning_statement_c07-565470.html)

**Note:** The Cisco 1130, 1140 and 3502i series access points are to be mounted on the ceiling as they have omni-directional antennas.

## Models

Cisco currently offers four Cisco Unified Wireless IP Phone 7925G models, one Cisco Unified Wireless IP Phone 7925G-EX model and one Cisco Unified Wireless IP Phone 7926G model.

The Cisco Unified Wireless IP Phone 7925G and 7926 models are grey in color, where the Cisco Unified Wireless IP Phone 7925G-EX is yellow in color.

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

The Cisco Unified Wireless IP Phone 7925G-EX, and Cisco Unified Wireless IP Phone 7926G are configured like the Cisco Unified Wireless IP Phone 7925G –W model, which requires an 802.11d enabled access point.

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

### 7925G

Part Number	Regulatory Domain	Regulatory Domain Number	Frequency Range	Available Channels	Channel Set
CP-7925G-A-K9	FCC (Americas)	1050	2.412 – 2.462 GHz	11	1-11
			5.180 – 5.240 GHz	4	36,40,44,48
			5.260 – 5.320 GHz	4	52,56,60,64
			5.500 – 5.700 GHz	8	100-140
			5.745 – 5.805 GHz	4	149,153,157,161
CP-7925G-E-K9	ETSI (Europe)	3051	2.412 – 2.472 GHz	13	1-13
			5.180 – 5.700 GHz	16	36-48,52-64,100-140
CP-7925G-P-K9	Japan	4157	2.412 – 2.472 GHz	13 (802.11g)	1-13
			2.412 – 2.484 GHz	14 (802.11b)	1-14
			5.180 – 5.700 GHz	16	36-48,52-64,100-140
CP-7925G-W-K9	Rest of World	5252	Uses 802.11d to identify available channels and transmit powers. Channels operating at 2.412 GHz– 2.484 GHz and 5.180 GHz – 5.805 GHz are supported.		

### 7925G-EX

Part Number	Regulatory Domain Number	Frequency Range	Available Channels	Channel Set
-------------	--------------------------	-----------------	--------------------	-------------

CP-7925G-EX-K9	5252	2.412 – 2.484 GHz	14	1-14
		5.180 – 5.240 GHz	4	36,40,44,48
		5.260 – 5.320 GHz	4	52,56,60,64
		5.500 – 5.700 GHz	11	100-140
		5.745 – 5.805 GHz	4	149,153,157,161

## 7926G

Part Number	Regulatory Domain Number	Frequency Range	Available Channels	Channel Set
CP-7926G -K9	5252	2.412 – 2.484 GHz	14	1-14
		5.180 – 5.240 GHz	4	36,40,44,48
		5.260 – 5.320 GHz	4	52,56,60,64
		5.500 – 5.700 GHz	11	100-140
		5.745 – 5.805 GHz	4	149,153,157,161

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

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

Channel 14 for Japan is not supported on the newer Cisco access points.

## 7925G-EX Certifications

The Cisco Unified Wireless IP Phone 7925G-EX has both Atmospheres Explosibles (ATEX) Zone 2/Class 22 and Canadian Standards Association (CSA) Class1/Division II certifications in order to allow it to be used in hazardous and explosive environments.

### Atmospheres Explosibles (ATEX) Zone 2/Class 22 Certification

Organizations in the European Union must follow the ATEX directives to protect employees from explosion risk in areas with an explosive atmosphere.

- **ATEX 95 equipment directive 94/9/EC**

Equipment and protective systems intended for use in potentially explosive atmospheres.

- **ATEX 137 workplace directive 99/92/EC**

Minimum requirements for improving the safety and health protection of workers potentially at risk from explosive atmospheres.

Areas classified into zones (0, 1, 2 for gas-vapor-mist and 20, 21, 22 for dust) must be protected from effective sources of ignition. Equipment and protective systems intended to be used in zoned areas must meet the requirements of the directive. Zone 0 and 20 require Category 1 marked equipment, zone 1 and 21 required Category 2 marked equipment and zone 2 and 22 required Category 3 marked equipment. Zone 0 and 20 are the zones with the highest risk of an explosive atmosphere being present.

Certification ensures that the equipment is fit for its intended purpose and that adequate information is supplied with it to ensure that it can be used safely.

## Canadian Standards Association (CSA) Class I/Division II Certification

Laws and regulations in most municipalities, states, and provinces in North America require certain products to be tested to a specific standard or group of standards when they are to be deemed intrinsically safe when used in an explosive environment.

In North America, hazardous locations have traditionally been defined by the following combination of Class and Division:

- **Class I** - A location where a quantity of flammable gas or vapor, sufficient to produce an explosive or ignitable mixture, may be present in the air.
- **Class II** - A location made hazardous by the presence of combustible or electrically conductive dust, including Groups E (metal dust), F (coal dust) and G (grain dust).
- **Class III** - A location made hazardous by the presence of easily ignitable fibers in the air, but not likely in sufficient quantities to produce ignitable mixtures.
  
- **Division 1** - A location where a classified hazard is likely to exist.
- **Division 2** - A location where a classified hazard does not normally exist but is possible under abnormal conditions.

Internationally (and more recently in North America, for Class I hazardous locations), areas where explosive gas atmospheres are likely to be present are divided into three IEC-defined Zones:

- **Zone 0** - An area in which an explosive gas atmosphere is continuously present or present for long periods.
- **Zone 1** - An area in which an explosive gas atmosphere is likely to occur in normal operation.
- **Zone 2** - An area in which an explosive gas atmosphere does not normally exist.

## 7926G Barcode Scanner

The Cisco Unified Wireless IP Phone 7926G leverages the Cisco Unified Wireless IP Phone 7925G design, but with the addition of a 2D barcode scanner.

A Java MIDlet application is required to invoke the scanner.

Java MIDP support is included in the initial 1.4(1)SR1 release for the Cisco Unified Wireless IP Phone 7926G.

The Java MIDlet for the Cisco Unified Wireless IP Phone 7926G will be a custom built application for a customer, where lookups can be queried against their own databases.

The Cisco Unified Wireless IP Phone 7926G supports both the Basic and Extended barcode symbology groups.

- **Basic** - Basic, Code39, Code128, DataMatrix, EAN13, UCC/EAN128, UPC, PDF417
- **Extended** - Extended, Code39, Code128, DataMatrix, EAN13, UCC/EAN128, UPC, PDF417, Aztec, Codabar, Code11, Code93, EAN add on 2, Interleave 2 of 5, Matrix 2 of 5, Plessey, GS1 Databar, Standard 2 of 5, Telepen, QRCode, Maxicode, MicroPDF417

See the [Product Specific Configuration Options](#) section for information on how to configure barcode options.

For more info on creating Java MIDlet applications for the Cisco Unified Wireless IP Phone 7926G, refer to the following URL.

<http://developer.cisco.com/web/jmapi/home>



## World Mode (802.11d)

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

If using the Cisco Unified Wireless IP Phone 7925G World (-W) model, the Cisco Unified Wireless IP Phone 7925G-EX or Cisco Unified Wireless IP Phone 7926G model, then it is required to 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.

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

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will passively scan DFS channels first before engaging in active scans of those channels.

If 802.11d information is not available from the access point, then the Cisco Unified Wireless IP Phone 7925G (-A, -E, -P) model 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.

If using 2.4 GHz (802.11b/g) and 802.11d is not enabled, then the Cisco Unified IP Phone 7925G, 7925G-EX, and 7926G can attempt to use channels 1-11 and reduced transmit power.

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

World Mode must be enabled manually for Cisco Autonomous access points using the following commands:

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

## Supported Countries

Below are the countries and their 802.11d codes that are supported by the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

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)	Philippines (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](http://tools.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH)

## Radio Characteristics

The following table lists the data rates, ranges, and receiver sensitivity info for Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

<b>5 GHz - 802.11a</b>	<b>Data Rate</b>	<b>Range</b>	<b>Receiver Sensitivity</b>
Max Tx Power = 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
<b>2.4 GHz - 802.11g</b>	<b>Data Rate</b>	<b>Range</b>	<b>Receiver Sensitivity</b>
Max Tx Power = 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
<b>2.4 GHz - 802.11b</b>	<b>Data Rate</b>	<b>Range</b>	<b>Receiver Sensitivity</b>
Max Tx Power = 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. The above values are pure radio specifications and do not account for the integrated antenna gain. See the [Designing the Wireless LAN for Voice](#) section for more information on signal requirements.

## Language Support

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G support 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. Download the locale packages from the Localization page at the following URL:

<http://www.cisco.com/cisco/software/navigator.html?mdfid=278875240>

## Bluetooth

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G support Bluetooth 2.0 + EDR 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 Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

Up to five headsets can be connected, 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 (e.g. microwave ovens, cordless phones, etc.), so the Bluetooth quality can potentially be interfered with due to using this unlicensed frequency.

## Bluetooth Profiles

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G support the Bluetooth Headset and Hands-Free Profiles.

### **Headset Profile (HP)**

With Bluetooth Headset Profile (HSP) support, the following features can be available if supported by the Bluetooth headset.

- Ring
- Answer a call
- End a call
- Volume Control

### **Hands-Free Profile (HFP)**

With Bluetooth Hands-Free Profile (HFP) support, the following additional features can be available if supported by the Bluetooth headset.

- Last Number Redial
- Call Waiting
- Divert / Reject
- 3 way calling (Hold & Accept and Release & Accept)
- Speed Dialing

For more information, refer to the documentation from the Bluetooth headset manufacturer.

## 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 range.

### **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 (e.g. > 12 Mbps) to prevent from engaging in CTS for 802.11g protection when using Coexistence as voice quality can be impacted.

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

# Security

When deploying a wireless LAN, security is essential.

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G support the following wireless security features.

## **WLAN Authentication**

- WPA (802.1x authentication + TKIP or AES encryption)
- WPA2 (802.1x authentication + AES or TKIP encryption)
- WPA-PSK (Pre-Shared key + TKIP encryption)
- WPA2-PSK (Pre-Shared key + AES encryption)
- EAP-FAST (Extensible Authentication Protocol – Flexible Authentication via Secure Tunneling)
- EAP-TLS (Extensible Authentication Protocol – Transport Layer Security)
- PEAP (Protected Extensible Authentication Protocol) MS-CHAPv2
- LEAP (Lightweight Extensible Authentication Protocol)
- CCKM (Cisco Centralized Key Management)
- Open
- Shared Key

## **WLAN Encryption**

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

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G also support the following non-WLAN security features.

- X.509 Digital Certificates
- Image authentication
- Device authentication
- File authentication
- Signaling authentication
- Secure Cisco Unified SRST
- Media encryption (SRTP)
- Signaling encryption (TLS)
- Certificate authority proxy function (CAPF)
- Secure profiles
- Encrypted configuration files
- Settings Access (can limit user access to configuration menus)
- Locked network profiles
- Administrator password

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

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 (Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G), which in turn selects the appropriate PAC. The client (phone) returns a PAC-Opaque to the RADIUS server. The server decrypts the PAC with its master-key. Both endpoints now have the PAC key and a TLS tunnel is created. EAP-FAST supports automatic PAC provisioning, but it must be enabled on the RADIUS server.

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

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G currently support automatic provisioning of the PAC only, so enable **Allow anonymous in-band PAC provisioning** on the RADIUS server as shown below.

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

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

The screenshot displays the Cisco System Configuration interface for EAP-FAST. The left sidebar contains navigation options: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled "EAP-FAST Configuration" and includes an "Edit" button. The "EAP-FAST Settings" window is open, showing the following configuration options:

- Allow EAP-FAST
- Active master key TTL: 1 months
- Retired master key TTL: 3 months
- Tunnel PAC TTL: 1 weeks
- Client initial message: (empty text box)
- Authority ID Info: sjc21-21a-acs
- Allow anonymous in-band PAC provisioning
- Allow authenticated in-band PAC provisioning
  - Accept client on authenticated provisioning
  - Require client certificate for provisioning
- Allow Machine Authentication
  - Machine PAC TTL: 1 weeks
- Allow Stateless session resume
  - Authorization PAC TTL: 1 hours
- Allowed inner methods:
  - EAP-GTC
  - EAP-MSCHAPv2
  - EAP-TLS
- Select one or more of the following EAP-TLS comparison methods:
  - Certificate SAN comparison
  - Certificate CN comparison
  - Certificate Binary comparison
- EAP-TLS session timeout (minutes): 120
- EAP-FAST master server
- Actual EAP-FAST server status: Master

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, 7925G-EX, and 7926G.

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, 7925G-EX, and 7926G 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, 7925G-EX, and 7926G 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.



## System Configuration

Edit

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

### Global Authentication Setup

#### EAP Configuration

##### PEAP

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

- Allow EAP-TLS

Select one or more of the following options:

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

EAP-TLS session timeout (minutes):

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

##### EAP-FAST

[EAP-FAST Configuration](#)

##### EAP-TLS

- Allow EAP-TLS

Select one or more of the following options:

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

EAP-TLS session timeout (minutes):

EAP-TLS may also require a user account to be created on the authentication server matching the common name of the certificate imported into the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

It is recommended to use a complex password for this user account and that EAP-TLS is the only EAP type enabled on the RADIUS server.



## User Setup

Edit

**User: CP-7925G-SEP0013E0A0C587**

Account Disabled

### Supplementary User Info

Real Name   
Description

### User Setup

Password Authentication:

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

Password   
Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

Password   
Confirm Password

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

Group to which the user is assigned:

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-CHAPv2 is the current supported inner authentication protocol (GTC is not supported).



## System Configuration

Edit

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

### Global Authentication Setup

#### EAP Configuration

**PEAP**

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

---

- Allow EAP-TLS

Select one or more of the following options:

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

EAP-TLS session timeout (minutes):

---

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

---

**EAP-FAST**

[EAP-FAST Configuration](#)

---

**EAP-TLS**

- Allow EAP-TLS

Select one or more of the following options:

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

EAP-TLS session timeout (minutes):

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, 7925G-EX, and 7926G.

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

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

[http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps2086/ps7032/product\\_data\\_sheet09186a00800887d5.html](http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps2086/ps7032/product_data_sheet09186a00800887d5.html)

[http://www.cisco.com/en/US/prod/collateral/netmgts/ps5698/ps6767/ps9911/data\\_sheet\\_c78-614584.html](http://www.cisco.com/en/US/prod/collateral/netmgts/ps5698/ps6767/ps9911/data_sheet_c78-614584.html)

**Note:** If using a 3rd party RADIUS server, ensure that PEAP v0 (MS-CHAP v2) is enabled. PEAP v1 (GTC) is not supported.



## 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 and WPA2 introduce additional transient keys and can lengthen roaming time.

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

As of the 1.3(4) release, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G support CCKM with WPA2 (AES or TKIP), WPA (TKIP or AES) and 802.1x (WEP) authentication.

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

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

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

## EAP and User Database Compatibility

The following chart displays the EAP and database configurations supported by the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

Database Type	LEAP	EAP-FAST (Phase Zero)	EAP-TLS	PEAP (MS-CHAPv2)
Cisco ACS	Yes	Yes	Yes	Yes
Windows SAM	Yes	Yes	No	Yes
Windows AD	Yes	Yes	Yes	Yes
LDAP	No	No	Yes	No

ODBC (ACS for Windows Only)	Yes	Yes	Yes	Yes
LEAP Proxy RADIUS Server	Yes	Yes	No	Yes
All Token Servers	No	No	No	No

## Power Management

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G have 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. Proxy ARP allows the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G to remain in sleep mode longer versus waking up at each Delivery Traffic Indicator Message (DTIM) period to check for incoming broadcasts.

To optimize battery life, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will utilize either U-APSD or PS-POLL power save methods depending on whether Wi-Fi MultiMedia (WMM) is enabled in the Access Point configuration or not.

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

When on call U-APSD, PS-POLL, or active mode will be utilized depending on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G call power save mode configuration and the access point configuration.

When in idle (no active call), the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G depending on the Access Point configuration will utilize U-APSD or PS-POLL.

Battery life can be reduced 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
<u>2.4 GHz</u>	On Call	9.5	13
	On Call + Bluetooth	5.5	7
	Idle	180	240
<u>5 GHz</u>	Idle + Bluetooth Enabled	165	200
	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.

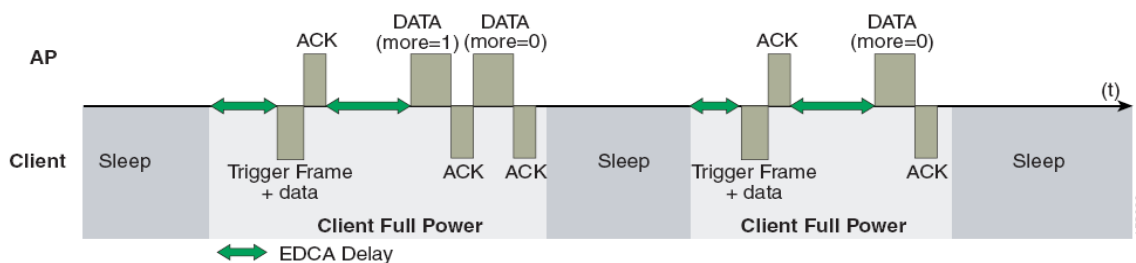
## Protocols

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

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will utilize U-APSD (Unscheduled Auto Power Save Delivery) for power management as long as Wi-Fi MultiMedia (WMM) is enabled in the access point configuration and the call power save mode on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G is set to U-APSD/PS-POLL.

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

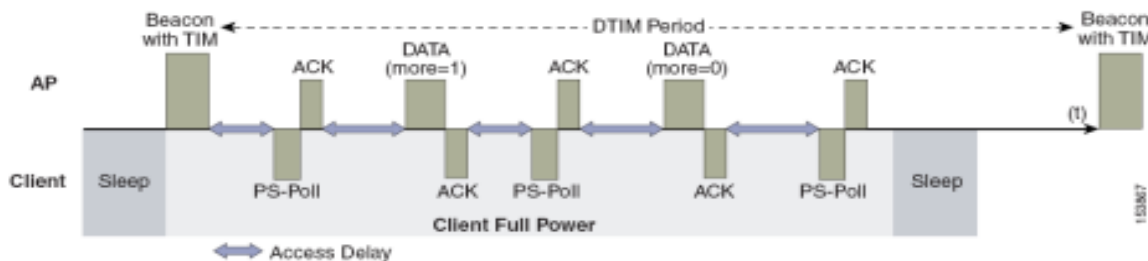
Below is a sample packet sequence when using U-APSD.



### Power Save Poll (PS-POLL)

If WMM is disabled (disabling U-APSD support) or U-APSD support is not available on the access point, then the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will utilize PS-POLL for power management when the call power save mode on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G is set to U-APSD/PS-POLL.

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)

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G can use the DTIM period to schedule wakeup periods to check for broadcast and multicast packets as well as any unicast packets.

If proxy ARP is enabled, then the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G do not have to wake up at DTIM.

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

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

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

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

## Scan Modes

There are three different scan modes (**Auto**, **Continuous**, **Single AP**), which can be configured for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G in the Cisco Unified Communications Manager.

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

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

When on an active call with **Auto** scan mode enabled, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will continuously be scanning. If in idle (not on an active call) and **Auto** scan mode is enabled, then the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will only start to scan once the scan threshold is met for the currently connected access point.

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

**Continuous** scan mode can also help with location tracking.

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

If using only one access point, select **Single AP** mode on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G to reduce scanning and optimize battery life.

## Quality of Service (QoS)

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

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

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

Traffic Type	DSCP	802.1p	WMM UP	Port Range
Voice	EF (46)	5	6	UDP 16384 - 32677
Call Control	CS3 (24)	3	4	TCP 2000

- Be sure that voice and call control packets have the proper QoS markings and other protocols are not using the same QoS markings.
- Select the **Platinum** QoS profile for the 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.

For more information about TCP and UDP ports used by the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G and the Cisco Unified Communications Manager, refer to the Cisco Unified Communications Manager TCP and UDP Port Usage document at this URL:

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cucm/port/8\\_6\\_1/portlist861.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/port/8_6_1/portlist861.html)

## Configuring QoS in Cisco Unified Communications Manager

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

Parameter Name	Parameter Value
<a href="#">Cluster ID</a> *	StandAloneCluster
<a href="#">Synchronization Between Auto Device Profile and Phone Configuration</a> *	True
<a href="#">Max Number of Device Level Trace</a> *	12
<a href="#">DSCP for Phone-based Services</a> *	default DSCP (000000)
<a href="#">DSCP for Phone Configuration</a> *	CS3(precedence 3) DSCP (011000)
<a href="#">DSCP for Cisco CallManager to Device Interface</a> *	CS3(precedence 3) DSCP (011000)
<a href="#">Connection Monitor Duration</a> *	120
<a href="#">Auto Registration Phone Protocol</a> *	SCCP
<a href="#">BLF For Call Lists</a> *	Disabled
<a href="#">Advertise G.722 Codec</a> *	Enabled
<a href="#">Phone Personalization</a> *	Disabled
<a href="#">Services Provisioning</a> *	Internal
<a href="#">Feature Control Policy</a>	< None >

## Configuring QoS Policies for the Network

Configure QoS policies and settings for the following network devices.

### Configuring Cisco Switch Ports

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

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

```
mls qos
```

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

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

Below is a sample switch configuration for an access point:

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

**Note:** When using the Cisco Unified Wireless LAN Controller, DSCP trust must be implemented or trust the UDP data ports used by the Cisco Unified Wireless LAN Controller (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 Cisco IOS Access Points

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

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

## Configuring Switch Ports for Wired IP Phones

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

Below is a sample switch configuration:

```
mls qos  
!
```

Interface X

```
mls qos trust device cisco-phone
```

```
mls qos trust dscp
```

## Sample Voice Packet Capture

The packet capture below displays a voice packet bound for the Cisco Unified IP Phone 7925G, 7925G-EX, or 7926G over the air being marked as DSCP = EF and UP = 6.

Packet Info | Packet Number=1 | Flags=0x00000000 | Status=0x00000000 | Packet Length=238 | Timestamp=14:13:12.968750000 09/25/2008 | Data Rate=108.54 .0 Mbps | Chan=52.5260 MHz

**802.11 MAC Header**

- Version: 0
- Type: 410 Data
- Subtype: 41000 QoS Data
- Frame Control Flags: 400001010
  - 0... Non-strict order
  - .0... Non-Protected Frame
  - ..0... No More Data
  - ...0... Power Management - active mode
  - ...1... This is a Re-Transmission
  - ...0... Last or Unfragmented Frame
  - ...1... Exit from the Distribution System
  - ...0... Not to the Distribution System
- Duration: 44 Microseconds
- Destination: 00:13:ED:A0:C5:87 7925G
- BSSID: 00:1B:53:FF:4F:EF AP
- Source: 00:16:9C:38:6C:40
- Seq Number: 203
- Fragment Number: 0
- QoS Control Field: 4000000000000110
  - ..... AP PS Buffer State: 0
  - ..... 0..... A-MSDU: Not Present
  - ..... 00..... Ack: Normal Acknowledge
  - ..... 0..... EOSF: Not End of Triggered Service Period
  - ..... 0..... Reserved
  - ..... 110 UP: 6 - Voice
- 802.2: D=0xAA SNAP S=0xAA SNAP C=0x03 Unnumbered Information

**IP Header - Internet Protocol Datagram**

- Version: 4
- Header Length: 5 (20 Bytes)
- Differentiated Services: 461011000
  - 1011 10.. Expedited Forwarding
  - ..... 00 Not-ECT
- Total Length: 200
- Identifier: 49262
- Fragmentation Flags=0000
- Fragment Offset: 0 (0 bytes)
- Time To Live: 63
- Protocol: 17 UDP
- Header Checksum: 0x569E
- Source IP Address: 150.1.1.11
- Dest. IP Address: 192.1.12.83

**UDP:** Src=19444 Dst=21424

**RTP:** Version=2 Extension=0 CSRC Count=0 Marker=0 Payload Type=0 PCMU Sequence=64052 Time Stamp=913006491 Sync Src ID=1700962776

**G.711 Payload (PCMA/PCMU) No. 01 Data Blocks=20 Audio Data Block#1: 0xEB75FD9787B6F6C Audio Data Block#2: 0x6CECDCDEE3F16F Audio Data Block#3: 0x7CF4F8FD7AEC3E4 Audio Data Block#4: 0x3178AD5F**

**FCS:** FCS=0x3178AD5F Calculated

## Call Admission Control

Inbound and outbound call admission control should be enabled on the access point.

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

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

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

As of the 1.3(3) release, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will auto-negotiate the minimum PHY rate to be used for TSPEC. By default it will try the locally configured minimum PHY rate (e.g. 12 Mbps) first, but if that data rate is not enabled on the access point, then it will try the next highest enabled data rate on the access point. If there is not a higher data rate enabled, then it will then try the next lowest data rate as the minimum PHY rate.

In releases prior to 1.3(3), the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G would use the static minimum PHY rate configured locally, which required that rate to be enabled on the access point.

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

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

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

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

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

## Pre-Call Admission Control

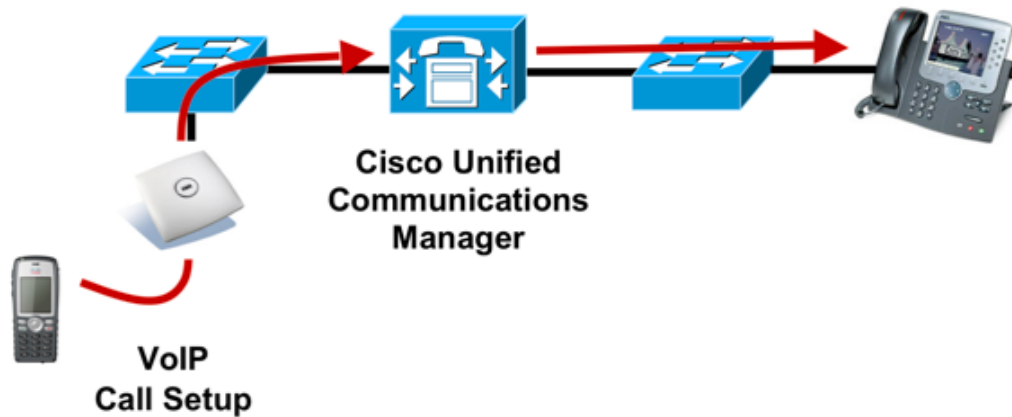
If Call Admission Control (TSPEC) is enabled on the access point, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will send an Add Traffic Stream (ADDTS) to the access point to request bandwidth in order to place or receive a call.

If the AP sends an ADDTS successful message then the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G establishes the call.

If the access point rejects the call and the wireless IP phone has no other access point to roam to, then the phone will display **Network Busy**.

If the admission is refused for an inbound call there is no messaging from the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G to inform the remote endpoint that there is insufficient bandwidth to establish the call, so the call can continue to ring out within the system until the remote user terminates the call.

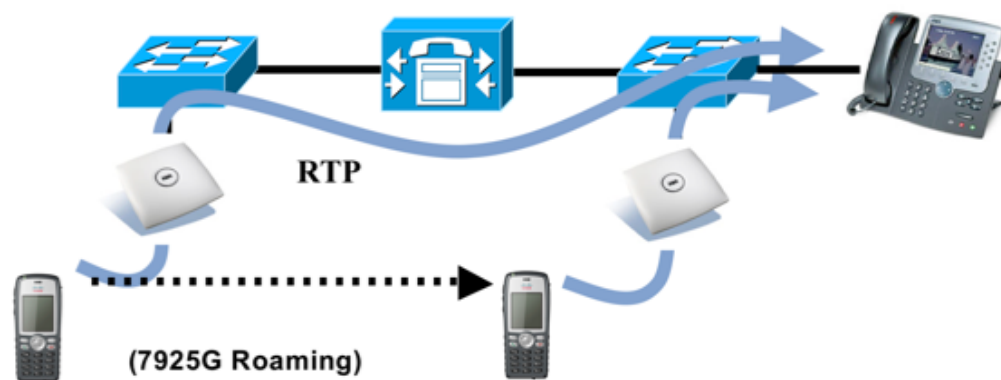




## Roaming Admission Control

During a call, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G measure Received Signal Strength Indicator (RSSI) and Packet Error Rate (PER) values for the current and all available access points to make roaming decisions.

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



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/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html>

## Traffic Classification (TCLAS)

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

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

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

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

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

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

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

With TCLAS, DSCP preservation is not a requirement.

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

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

## Roaming

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

For seamless roaming to occur, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G must be associated to an access point for at least 3 seconds, otherwise roams will occur based on packet loss (max tx retransmissions or missed beacons).

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

As of the 1.3(4) release, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G support CCKM with WPA2 (AES or TKIP), WPA (TKIP or AES), and 802.1x (WEP) authentication.

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

## Interband Roaming

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

For Auto-a and Auto-b/g modes, this is giving preference to one frequency band over another. At power on, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will scan all 2.4 and 5 GHz channels then attempt to associate to an access point for the configured network using the preferred frequency band if available. If the preferred frequency band is not available, then the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will try to use the less preferred frequency band if available. If the phone roams out of coverage of the preferred frequency band, where less preferred frequency band signal is available, then the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will attempt to associate to that less preferred frequency band.

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

In order for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G to roam from the preferred frequency band to the less preferred frequency band (e.g. roam to 2.4 GHz when configured for Auto-a mode), all access points in the preferred frequency band must have a signal lower than the preferred frequency band signal threshold as well as one access point in the less preferred frequency band meeting the RSSI differential threshold for roaming must be met. In order to roam back to the preferred frequency band, there must be at least one access point with sufficient signal matching the preferred frequency band signal threshold.

Prior to the 1.3(4) release, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G would have to roam out of range of the current band before it would attempt to roam to an access point on the other frequency band when configured for an Auto 802.11 mode (e.g. Auto-a, Auto-b/g, Auto-RSSI), where the user may experience choppy audio with the weak signal connection, followed up with a small second audio gap before associating to the new frequency band. Once the Cisco Unified Wireless IP Phone 7925G failed over to a less preferred frequency band (e.g. associated to 802.11b/g when the phone is configured for Auto-a), there was no mechanism to guarantee the Cisco Unified Wireless IP Phone 7925G would roam back to the preferred frequency band when available again or not as only the connected frequency band would be scanned.

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

## Multicast

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

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G uses the DTIM period to receive the queued broadcast and multicast packets.

If proxy ARP from CCX is enabled and the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G are not participating in a multicast session currently, then the access point is responsible to answer any ARP requests on behalf of the client and the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G can remain in sleep mode longer thus optimizing battery life.

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

With multicast, there is no 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, 7925G-EX, and 7926G support 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

The following network design guidelines must be followed in order to accommodate for adequate coverage, call capacity and seamless roaming for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

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/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html>

# Planning Channel Usage

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

## 5 GHz (802.11a)

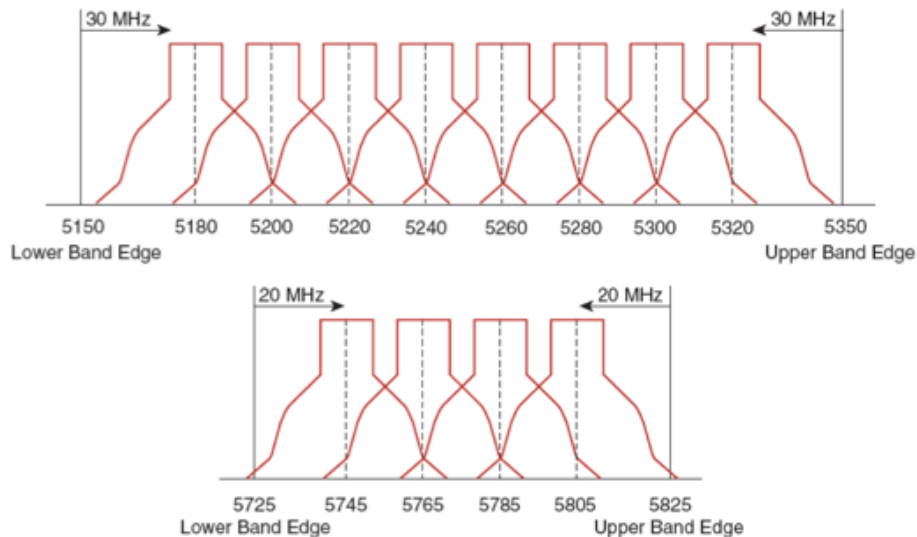
The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G support Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) from 802.11h, which are required when using channels operating at 5.260 - 5.700 GHz (12 of the 20 possible channels).

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

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

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

Need to ensure there is at least 20 percent overlap with adjacent channels when deploying the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G in the 802.11a environment, which allows for seamless roaming. For critical areas, it is recommended to increase the overlap (30% or more) to ensure that there can be at least 2 access points available with -67 dBm or better, while the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G also meet the access point's receiver sensitivity (required signal level for the current data rate).



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

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

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

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

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

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

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

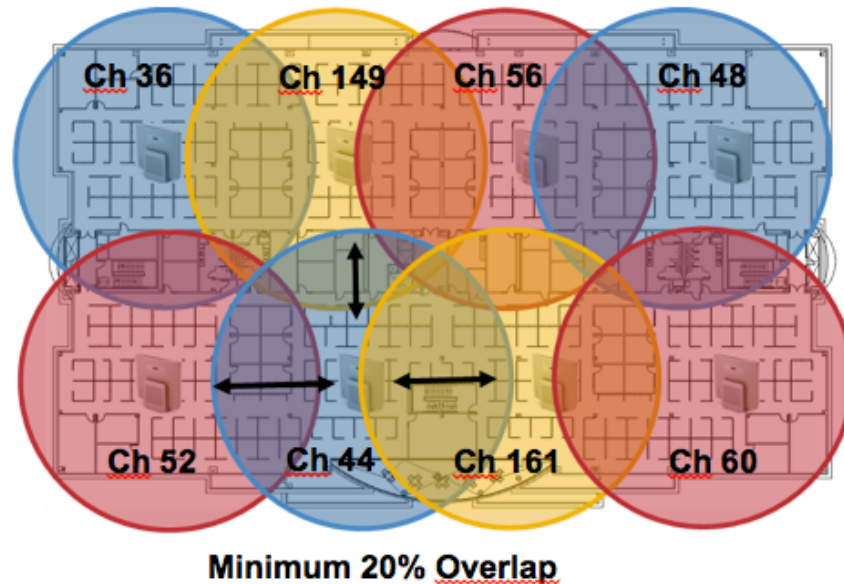
In case of radar activity, have at least one access point per area that uses a non-DFS channel (UNII-1). This ensures that a channel is available when an access point's radio is in its hold-off period while scanning for a new usable channel.

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

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

A UNII-3 channel (5.745 - 5.805 GHz) can optionally be used if available.

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



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

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

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

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

**Default Radio Channel:**

Dynamic Frequency Selection (DFS) Channel 48 5240 MHz

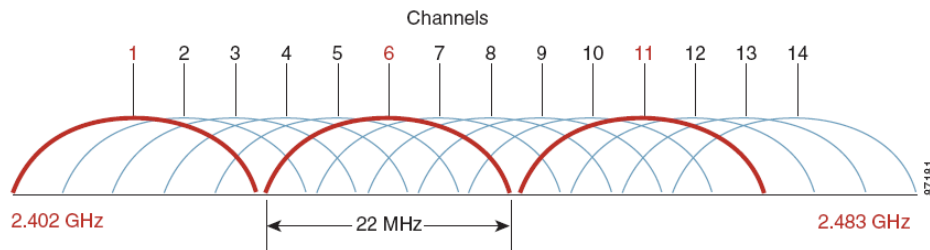
**Dynamic Frequency Selection Bands:**

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

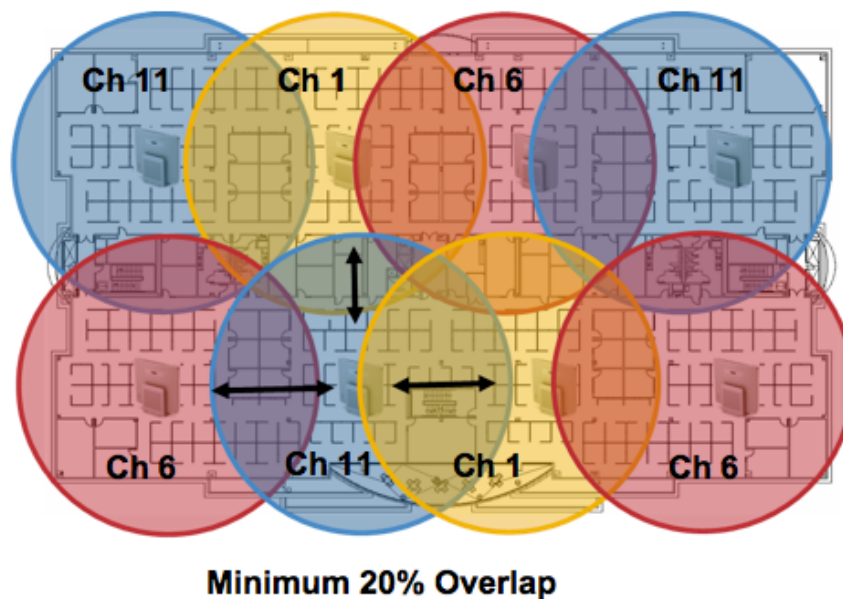
## 2.4 GHz (802.11b/g)

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

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



Non-overlapping channels must be used and allow at least 20 percent overlap with adjacent channels when deploying the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G in the 802.11b/g environment, which allows for seamless roaming.



## Signal Strength and Coverage

To ensure acceptable voice quality, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G should always have a signal of -67 dBm or higher when using 2.4 GHz or 5 GHz, while the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G also meet the access point's receiver sensitivity required signal level for the transmitted data rate.

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

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

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

To achieve maximum capacity and throughput, the wireless LAN should be designed to 24 Mbps. Higher data rates (36-54 Mbps) can optionally be enabled for other applications other than voice only that can take advantage of these higher data rates.

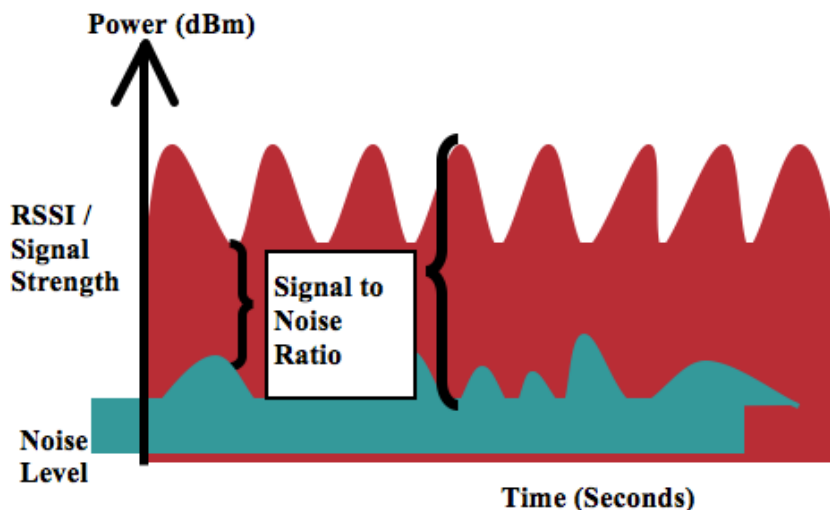
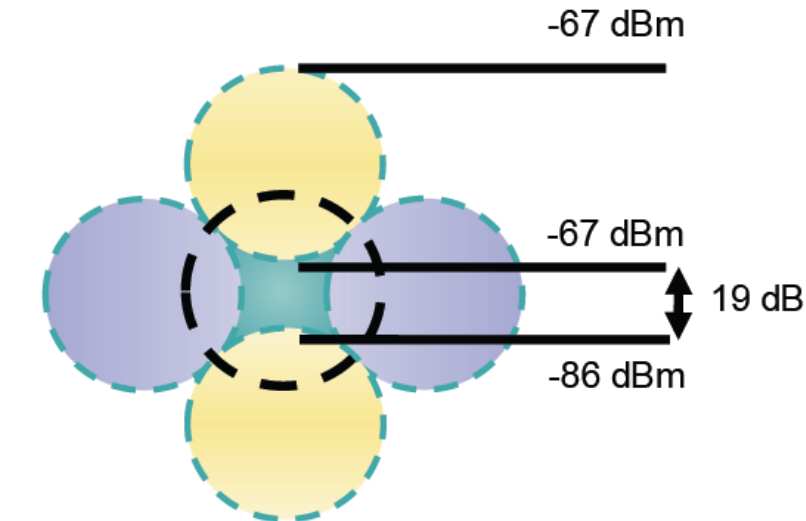
Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Deployment Guide

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.

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

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/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html>



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

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

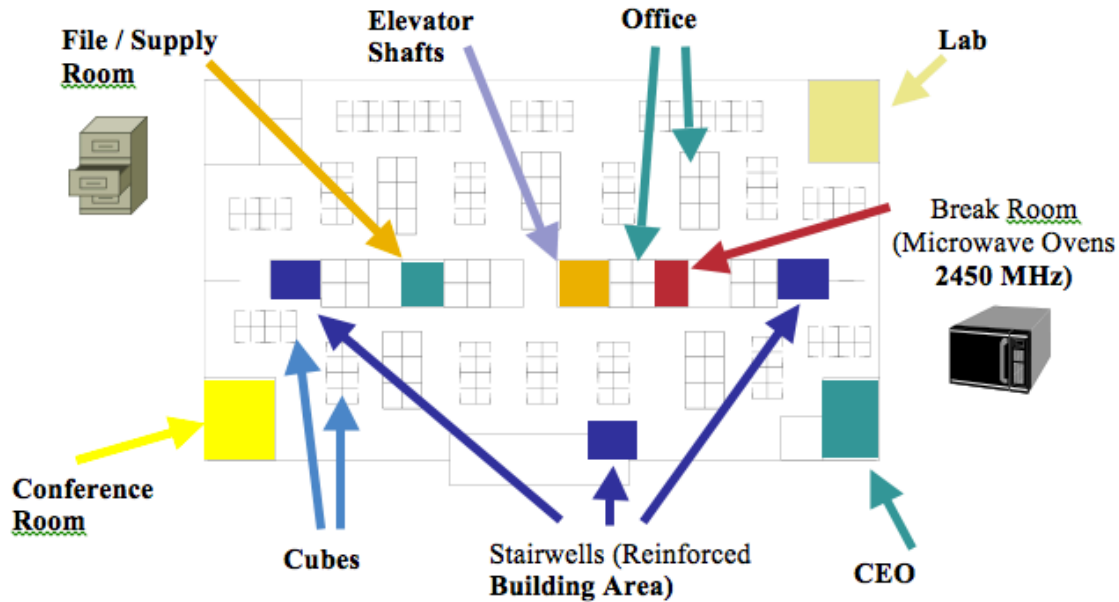
Wireless LAN interference is generated by microwave ovens, 2.4 GHz cordless phones, Bluetooth devices, or other electronic equipment operating in the 2.4 GHz band.

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

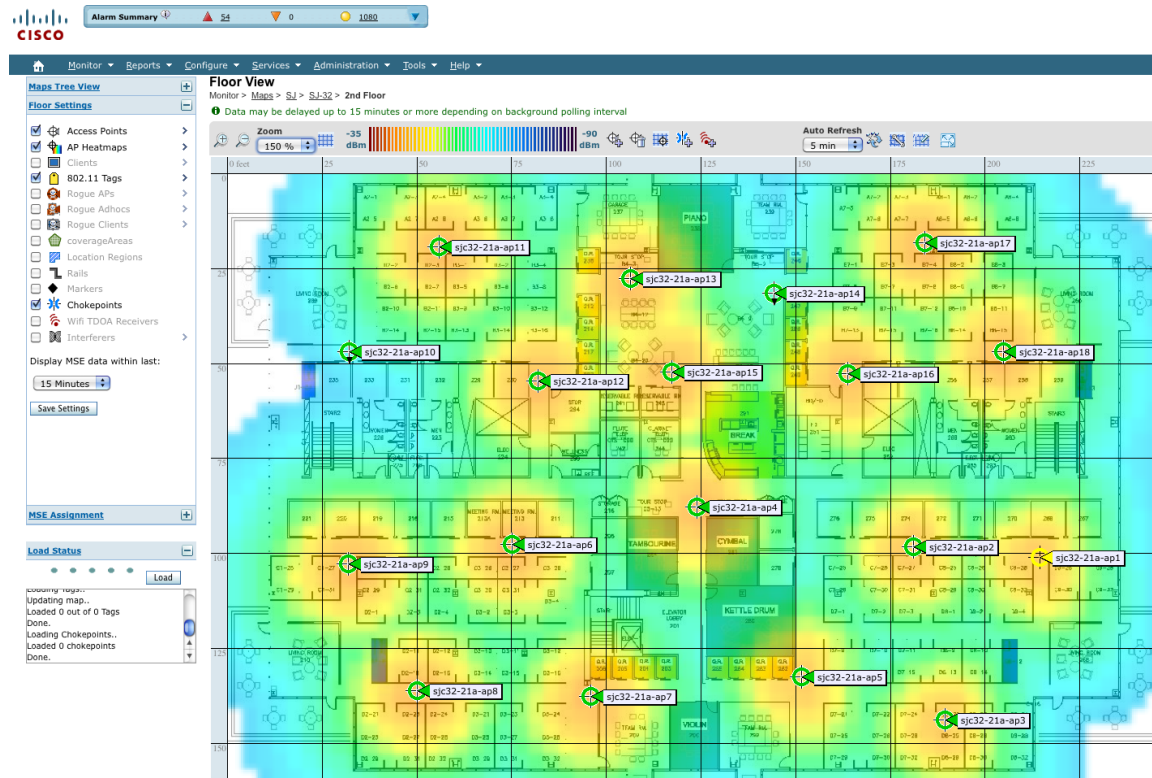


Most microwave ovens, Bluetooth, and frequency hopping devices do not have the same effect on the 5 GHz frequency. The 802.11a technology provides more non-overlapping channels and typically lower initial RF utilization. For voice deployments, it is suggested to use 802.11a for voice and use 802.11b/g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

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



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





## Configuring Data Rates

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

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

The recommended data rate configuration is the following:

<b>802.11 Mode</b>	<b>Basic (Mandatory) Data Rates</b>	<b>Supported (Optional) Data Rates</b>	<b>Disabled Data Rates</b>
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

For a voice only application, data rates higher than 24 Mbps (36, 48 and 54 Mbps) can optionally be enabled or disabled, but there is no advantage from a capacity or throughput perspective.

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

If using other clients that support applications like video or virtual desktop, then it is recommended to enable the higher data rates.

If deploying in an environment where excessive retries may be a concern, then a limited set of the data rates can be used (e.g. 12, 18, 24), where the lowest enabled rate is the basic / mandatory rate.

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

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

Set only the lowest data rate enabled as the single 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, 7925G-EX, and 7926G 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, 7925G-EX, and 7926G in order to utilize the TSRS feature.

## Call Capacity

Design the network to accommodate the desired call capacity.

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

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

Max # of Streams	802.11 Mode	Data Rate
13	802.11a 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.

## Dynamic Transmit Power Control (DTPC)

To ensure packets are exchanged successfully between the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G and the access point, Dynamic Transmit Power Control (DTPC) should be enabled.

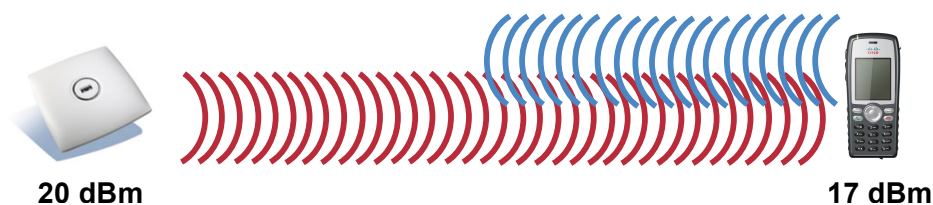
If the access point does not support DTPC, then the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will use the highest available transmit power depending on the current channel and data rate.

DTPC prevents one-way audio when RF traffic is heard in one direction only. Without DTPC, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will use the highest available transmit power.

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

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

The access point's radio transmit power should not have a transmit power greater than what the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G 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 affect the decoding capability of the receiver, as the signal quality is poor.

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

Below is a list of multipath effects:

**Data Corruption**

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

**Signal Nulling**

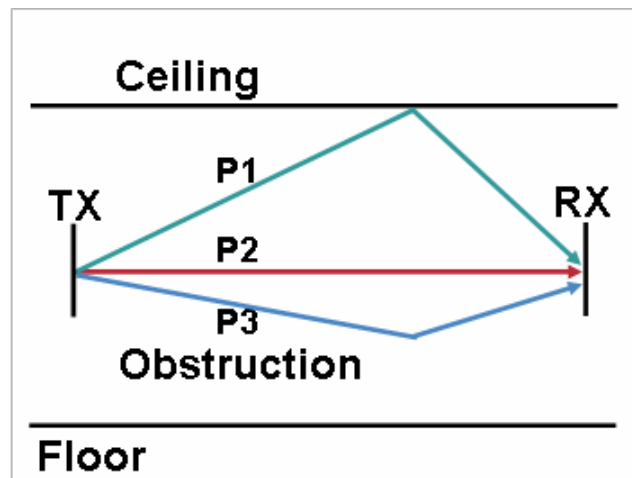
Occurs when the reflected waves arrive exactly out of phase with the main signal and cancel the main signal completely.

**Increased Signal Amplitude**

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

**Decreased Signal Amplitude**

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



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

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

Use of antenna diversity can also help in such environments.

## Verification with Site Survey Tools

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

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

[http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps11682/ps11686/ps11688/data\\_sheet\\_c78-650051.html](http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps11682/ps11686/ps11688/data_sheet_c78-650051.html)

- Cisco Wireless Control System (WCS) for Unified Wireless LAN Management  
[http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product\\_data\\_sheet0900aecd802570d0.html](http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd802570d0.html)
- Cisco Wireless LAN Solution Engine (WLSE) for Cisco Autonomous Wireless LAN Management  
[http://www.cisco.com/en/US/prod/collateral/netmgts/ps6380/ps6563/ps3915/ps6839/product\\_data\\_sheet0900aecd80410b92.html](http://www.cisco.com/en/US/prod/collateral/netmgts/ps6380/ps6563/ps3915/ps6839/product_data_sheet0900aecd80410b92.html)
- Cisco Spectrum Expert  
[http://www.cisco.com/en/US/prod/collateral/wireless/ps9391/ps9393/product\\_data\\_sheet0900aecd807033c3.html](http://www.cisco.com/en/US/prod/collateral/wireless/ps9391/ps9393/product_data_sheet0900aecd807033c3.html)
- Cisco Unified Operations Manager  
[http://www.cisco.com/en/US/prod/collateral/netmgts/ps6491/ps6705/ps6535/data\\_sheet\\_c78-636705.html](http://www.cisco.com/en/US/prod/collateral/netmgts/ps6491/ps6705/ps6535/data_sheet_c78-636705.html)
- AirMagnet (Survey, WiFi Analyzer, VoFi Analyzer, Spectrum Analyzer)  
<http://www.airmagnet.com>
- Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G  
[http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps9900/data\\_sheet\\_c78-504890.html](http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps9900/data_sheet_c78-504890.html)  
[http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps10649/data\\_sheet\\_c78-565676.html](http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps10649/data_sheet_c78-565676.html)  
[http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps11266/data\\_sheet\\_c78-649589.html](http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps11266/data_sheet_c78-649589.html)

## Cisco 792xG Neighbor List

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G can be utilized to verify coverage by using the Neighbor List menu.

To access the neighbor list menu on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, select **Settings > Status > Neighbor List**.

The connected access point will be highlighted in red.

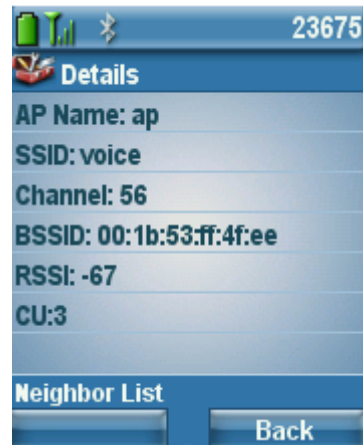
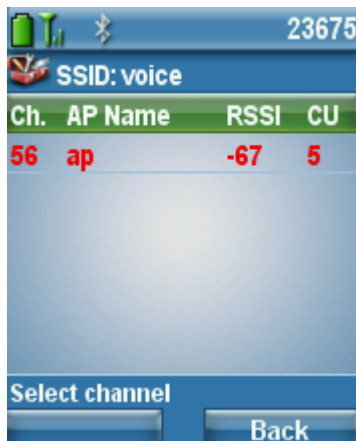
By default with the **Auto** scan mode enabled, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G in idle (not on call) only scans when the current signal lowers to the scan threshold, so only a single access point may be visible in the list.

To see all access points in the neighbor list menu with **Auto** scan mode, place a call from the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, where scanning occurs constantly while the phone call is active in **Auto** scan mode.

With **Continuous** scan mode, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will always be scanning regardless of call state (idle or on call) or current access point signal level (RSSI).

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

- Preferred Band Neighbors with  $\geq -67$  dBm RSSI
- Less Preferred Band Neighbors with  $\geq -67$  dBm RSSI
- Preferred Band Neighbors with  $< -67$  dBm RSSI
- Less Preferred Band Neighbors with  $< -67$  dBm RSSI



## Cisco 792xG Site Survey

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G has a Site Survey application, which is an offline mode that gathers information about the access points for the configured network profile and generates an HTML report after exiting the application.

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

To view the HTML report, select **System > Site Survey** from the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G webpage.

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

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



# CP7925G Site Survey Report SSID:baker

Neighbor Table	sjc32-11a-ap9	sjc32-11a-ap11	sjc32-11a-ap10	sjc32-11a-ap12	sjc32-11a-ap1
sjc32-11a-ap9	83% -53/-53	100% -66/-62	*	*	*

<b>AP:</b>		sjc32-11a-ap9																			
<b>MAC:</b>		C4:7D:4F:53:2C:DF																			
<b>Observation Count:</b>		6																			
<b>Channel - Frequency:</b>		157 - 5785000hz																			
<b>Country:</b>		US																			
<b>Beacon Interval:</b>		102																			
<b>DTIM Period:</b>		2																			
<b>RSSI Range [Lo Hi]:</b>		[-53 -53]																			
<b>BSS Lost Count:</b>		0																			
<b>Channel Utilization:</b>		7																			
<b>Station Count:</b>		17																			
<b>Available Admission Capacity:</b>		23437																			
<b>Basic Rates:</b>		12																			
<b>Optional Rates:</b>		18 24 36 48 54																			
<b>Multicast Cipher:</b>		CCMP																			
<b>Unicast Ciphers:</b>		WPA2_CCMP																			
<b>AKM:</b>		WPA2_1X WPA2_CCKM																			
<b>Proxy ARP supported:</b>		Yes																			
<b>WMM Supported:</b>		Yes																			
<b>CCX Version Number:</b>		5																			
<b>CCX Power Maximum in dBm:</b>		14																			
<b>U-APSD Supported:</b>		Yes																			
<b>Best Effort AC(0)</b>																					
<b>Admission Control Required:</b>		No																			
<b>AIFSN</b>	<b>ECWMin</b>				<b>ECWMax</b>				<b>TXOpLimit</b>												
12	6				10				0												
<b>Background AC(1)</b>																					
<b>Admission Control Required:</b>		No																			
<b>AIFSN</b>	<b>ECWMin</b>				<b>ECWMax</b>				<b>TXOpLimit</b>												
12	8				10				0												
<b>Video AC(2)</b>																					
<b>Admission Control Required:</b>		No																			
<b>AIFSN</b>	<b>ECWMin</b>				<b>ECWMax</b>				<b>TXOpLimit</b>												
5	3				5				0												
<b>Voice AC(3)</b>																					
<b>Admission Control Required:</b>		Yes																			
<b>AIFSN</b>	<b>ECWMin</b>				<b>ECWMax</b>				<b>TXOpLimit</b>												
2	2				4				0												
<b>Channels</b>	36	40	44	48	52	56	60	64	100	104	108	112	116	132	136	140	149	153	157	161	165
<b>Power</b>	17	17	17	17	24	24	24	24	24	24	24	24	24	24	24	24	30	30	30	30	30

# Configuring Cisco Unified Communications Manager

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

## Phone Button Templates

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G support 6 lines. The default phone button template includes support for 2 lines and 4 speed dials.

Custom phone button templates can be created with the option for many different features, which can then be applied on a device or group level.

The screenshot shows the configuration interface for a Phone Button Template. The top section, titled "Phone Button Template Information", contains a text field for "Button Template Name \*" with the value "Cisco 7925G". Below this is the "Button Information" section, which is a table with two columns: "Button" and "Feature".

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

At the bottom of the interface are several buttons: "Save", "Delete", "Copy", "Reset", and "Add New".

## Softkey Templates

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

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

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

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G have 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.

**Status**  
 Status: Ready

---

**Softkey Layout Configuration**  
 Softkey Template: Custom

Select a call state to configure: On Hook

Unselected Softkeys

- Call Back (CallBack)
- Conference List (ConfList)
- Direct Transfer (DirTrfr)
- Group Pick Up (GPickUp)
- HLog (HLog)
- Immediate Divert (iDivert)
- Join (Join)
- Meet Me (MeetMe)
- Mobility (Mobility)
- Other Pickup (oPickup)
- Pick Up (PickUp)
- Quality Report Tool (QRT)
- Remove Last Conference Party (RmLstC)
- Select (Select)
- Toggle Do Not Disturb (DND)
- Undefined (Undefined)

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

## 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.

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G have a Manufactured Installed Certificate (MIC).

**Protocol Specific Information**

Packet Capture Mode\* None

Packet Capture Duration 0

Presence Group\* Standard Presence group

**Device Security Profile\*** Cisco 7925 - Secure TFTP Encrypted

SUBSCRIBE Calling Search Space SJC DN Unlimited

Unattended Port

---

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

Certificate Operation\* No Pending Operation

Authentication Mode\* By Existing Certificate (precedence to MIC)

Authentication String

Generate String

Key Size (Bits)\* 1024

Operation Completes By 2008 10 5 12 (YYYY:MM:DD:HH)

Certificate Operation Status: None

Note: Security Profile Contains Addition CAPF Settings.

## G.722 Advertisement

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



Earlier versions of Cisco Unified Communications Manager do not have this capability, where a Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will attempt to use G.722 assuming the other endpoint also advertises G.722 capabilities. If using a version of Cisco Unified Communications Manager prior to 5.0 and want to disable G.722 capabilities, then the latest device package will need to be applied to the Cisco Unified Communications Manager to enable this product specific configuration option where **Advertise G.722 Codec** can be disabled for each Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

Parameter Name	Parameter Value
<a href="#">Cluster ID</a> *	StandAloneCluster
<a href="#">Synchronization Between Auto Device Profile and Phone Configuration</a> *	True
<a href="#">Max Number of Device Level Trace</a> *	12
<a href="#">DSCP for Phone-based Services</a> *	default DSCP (000000)
<a href="#">DSCP for Phone Configuration</a> *	CS3(precedence 3) DSCP (011000)
<a href="#">DSCP for Cisco CallManager to Device Interface</a> *	CS3(precedence 3) DSCP (011000)
<a href="#">Connection Monitor Duration</a> *	120
<a href="#">Auto Registration Phone Protocol</a> *	SCCP
<a href="#">BLF For Call Lists</a> *	Disabled
<a href="#">Advertise G.722 Codec</a> *	Enabled
<a href="#">Phone Personalization</a> *	Disabled
<a href="#">Services Provisioning</a> *	Internal
<a href="#">Feature Control Policy</a>	< None >

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

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

## Common Settings

Wireless LAN and Bluetooth can be configured on an enterprise phone, common phone profile or individual phone level. Override common settings can be enabled at either configuration level.

## Audio Bit Rates

The audio bit rate can be configured by creating or editing existing Regions in the Cisco Unified Communications Manager. It is recommended to select G.722 or G.711 for the audio codec.

Max Audio Bit Rate	Max Video Call Bit Rate (Includes Audio)
64 kbps (G.722, G.711)	<input type="radio"/> Keep Current Setting <input type="radio"/> Use System Default <input type="radio"/> None <input checked="" type="radio"/> 1064 kbps

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

Audio Codec	Audio Bit Rate
-------------	----------------

G.722 / G.711	64 Kbps
iLBC	16 Kbps
G.729	8 Kbps

## Product Specific Configuration Options

In Cisco Unified Communications Manager Administration, the following Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G configuration options are available.

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


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

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

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

## Common Configuration Options

**Product Specific Configuration Layout**

 **Param** **Override Common Settings**

Disable Speakerphone

Gratuitous ARP\*

Settings Access\*

Web Access\*

Profile 1\*

Profile 2\*

Profile 3\*

Profile 4\*

Load Server

Admin Password

Special Numbers

Application URL

"Send" Key Action\*

Phone Book Web Access\*

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

Application Button Activation Timer\*

Application Button Priority\*

Out-of-Range Alert\*

Scan Mode\*

Restrict Data Rates\*

Power Off When Charging\*

Cisco Discovery Protocol (CDP)\*

Advertise G.722 Codec\*

Home Screen\*

FIPS Mode\*

Auto Line Select\*

Bluetooth\*

File System Verification\*

Minimum Ring Volume\*

Field Name	Description
Disable Speakerphone	Speakerphone capabilities can optionally be disabled.
Gratuitous ARP	Determines whether the phone will learn MAC addresses from Gratuitous ARP responses or not.
Settings Access	Settings Access can be used to limit user access to certain menus (e.g. Network Profiles).
Web Access	This parameter indicates whether the phone will accept connections from a web browser or another HTTP client. Web Access can be set to Full, where configuration changes can be made remotely or Read Only to provide information but not allowing changes to be made.

Locked Profiles	Individual profiles can also be locked, which does not allow the user to modify those settings.
Load Server	A load server can be specified in IP format (x.x.x.x) if wanting to use an alternate TFTP server for phone firmware downloads.
Admin Password	The admin password is used for web access. With Cisco Unified Communications Manager 5.0 or later the admin password must be managed in Communications Manager Administrator page, where previous versions allow local management.
Special Numbers	Special numbers can be programmed to dial out regardless of keypad lock state (e.g. 911).
Application URL	<p>The application URL can be configured, which will convert the application button to a service URL button or as a speed dial.</p> <p>The application URL can be configured to link to a Push To Talk server for quick access.</p> <p>(e.g. PTT server =  <a href="http://x.x.x.x:8085/PushToTalk/displayPhoneGroupsMenu.do?sep=#DEVICENAME#">http://x.x.x.x:8085/PushToTalk/displayPhoneGroupsMenu.do?sep=#DEVICENAME#</a>)</p> <p>To configure the application button as a speed dial, enter in the format as <b>Dial:X</b> (e.g. Dial:23675).</p>
“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 <b>Allow Admin</b> in order to access the phone book via the web page.
Unlock-Settings Sequence	By default, <b>**#</b> 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 (e.g. 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, 7925G-EX, and 7926G will not transmit below 12 Mbps for 802.11a and 11 Mbps for 802.11b/g.

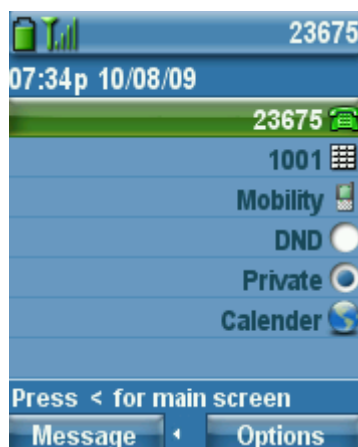
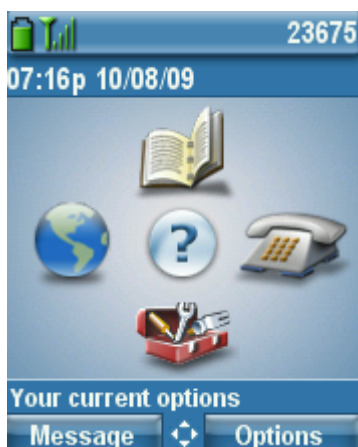
Power Off When Charging	Power off when charging feature will power off the phone when placed on AC power.
Cisco Discover Protocol (CDP)	Enables or disables CDP.
Advertise G.722 Codec	G.722 capabilities can be configured on a phone by phone basis and optionally override the system default.
Home Screen	By default the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G 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.
Bluetooth	Indicates whether the Bluetooth device on the phone is enabled or disabled.
File System Verification	This parameter indicates whether the phone will perform a file system integrity check as part of the firmware upgrade process. Enable this option to troubleshoot file system issues. This feature may impact phone performance if it is enabled.
Minimum Ring Volume	This parameter controls the minimum ring volume on the phone. This value is set by the administrator, and can not be changed by an end user. The end user can increase the ring volume, but may not decrease the ring volume below the level defined. The minimum ring volume range is from 0 to 7, with 0 (silent) being the default value.

### **7926G Specific Configuration Options**

Bar Code Symbology Group*	Basic
Scanner Commands	

<b><u>Field Name</u></b>	<b><u>Description</u></b>
Bar Code Symbology Group	This parameter specifies the symbology the scanner will use to scan bar codes. Select Basic or Extended symbology.
Scanner Commands	Use this field to customize the scanner features. Use comma to separate multiple commands. Please refer to the Midlet Developer Guide for additional information.

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

As of the 1.3(3) release, if settings access is set to **Disabled**, then the current ring volume will be locked in and will no longer be configurable.

To configure product specific configuration options for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G with Cisco Unified Communications Manager Express, create an ephone template with the necessary options.

**service phone <module> <value>**

<u>Field Name</u>	<u>Module</u>	<u>Value</u>
Disable Speakerphone	disableSpeaker	false = Enabled; true = Disabled
Gratuitous ARP	garp	0 = Enabled; 1 = Disabled
Settings Access	settingsAccess	0 = Disabled; 1 = Enabled; 2 = Restricted
Web Access	webAccess	0 = Full; 1 = Disabled; 2 = ReadOnly
Locked Profiles	WLANProfile<1-4>	0 = Unlocked; 1 = Locked, 2 = Restricted
Load Server	loadServer	x.x.x.x
Admin Password	adminPassword	(e.g. Cisco)
Special Numbers	specialNumbers	(e.g. 411,911)
Application URL	PushToTalkURL	http://x.x.x.x
“Send” Key Action	sendKeyAction	0 = Onhook Dialing; 1 = Offhook Dialing
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
Bluetooth	bluetooth	0 = Disabled; 1 = Enabled
File System Verification	fileSystemVerificationEnable	0 = Disabled; 1 = Enabled
Minimum Ring Volume	minimumRingVolume	0 = Silent; <1-7> = Different Volume Levels
Bar Code Symbology Group	barCodeSymbologyGroup	0 = Basic; 1 = Extended
Scanner Commands	scannerCommands	(e.g. 414b5a01) 414b5a01 enables UPC>EAN13 conversion 4170800005 will turn off the scanner after 5 seconds if no barcode is scanned
Application Button	thumbButton1	PTTH<1-6>

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

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

Enable individual phone configuration files with the following commands.

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

For more information on these features, see the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Administration Guide or the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Release Notes.

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

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

# Configuring the Cisco Unified Wireless LAN Controller and Access Points

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

- Ensure **CCKM** is **Enabled** if utilizing 802.1x authentication
- Set **Quality of Service (QoS)** to **Platinum**
- Set the **WMM Policy** to **Required**
- Ensure **Session Timeout** is enabled and configured correctly
- Ensure **Aironet IE** is **Enabled**
- Disable **P2P (Peer to Peer) Blocking Action / Public Secure Packet Forwarding (PSPF)**
- Ensure **Client Exclusion** is configured correctly
- Disable **DHCP Address Assignment Required**
- Set **MFP Client Protection** to **Optional** or **Disabled**
- Set the **DTIM Period** to **2**
- Set **Client Load Balancing** to **Disabled**
- Set **Client Band Select** to **Disabled**
- Set **IGMP Snooping** to **Enabled**
- Enable **Symmetric Mobile Tunneling Mode** if Layer 3 mobility is utilized
- Enable **Short Preamble** if using 2.4 GHz
- Set **DTPC Support** to **Enabled**
- Enable **ClientLink** if utilizing Cisco 802.11n capable access points
- Configure the **Data Rates** as necessary
- Enable **CCX Location Measurement**
- Configure **Auto RF** as necessary
- Set **Admission Control Mandatory** to **Enabled** for Voice
- Set **Load Based CAC** to **Enabled** for Voice
- Enable **Traffic Stream Metrics** for Voice
- Set **Admission Control Mandatory** to **Disabled** for Video
- Set **EDCA Profile** to **Voice Optimized** or **Voice and Video Optimized**
- Set **Enable Low Latency MAC** to **Disabled**
- Ensure that **Power Constraint** is **Disabled**
- Enable **Channel Announcement** and **Channel Quiet Mode**
- Enable **CleanAir** if utilizing Cisco access points with CleanAir technology
- Configure **Multicast Direct Feature** as necessary
- Set the **802.1p tag** to **6** for the **Platinum** QoS profile

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

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



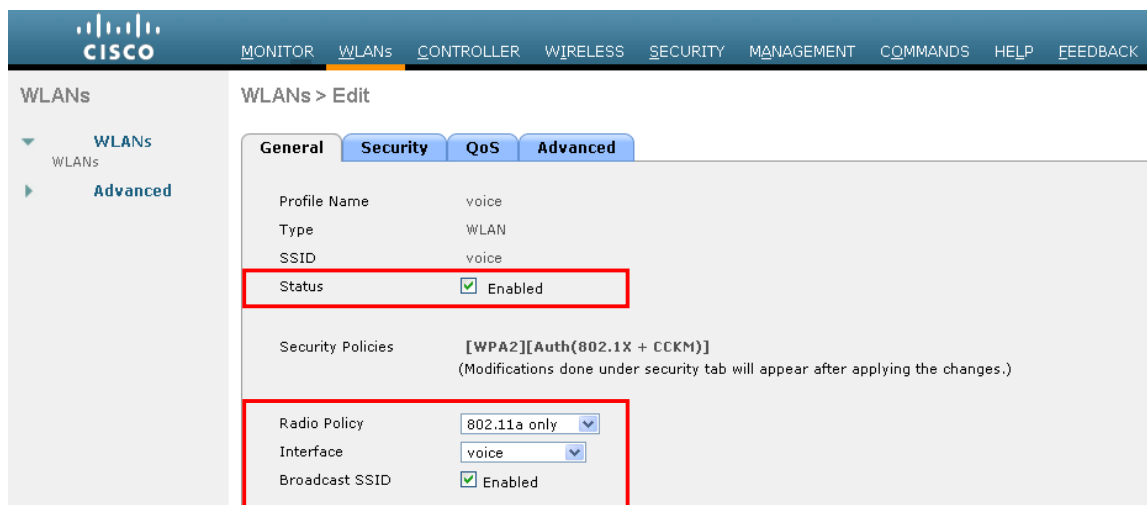
## SSID / WLAN Settings

It is recommended to have a separate SSID for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

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

The SSID to be used by the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G can be configured to only apply to a certain 802.11 radio type.

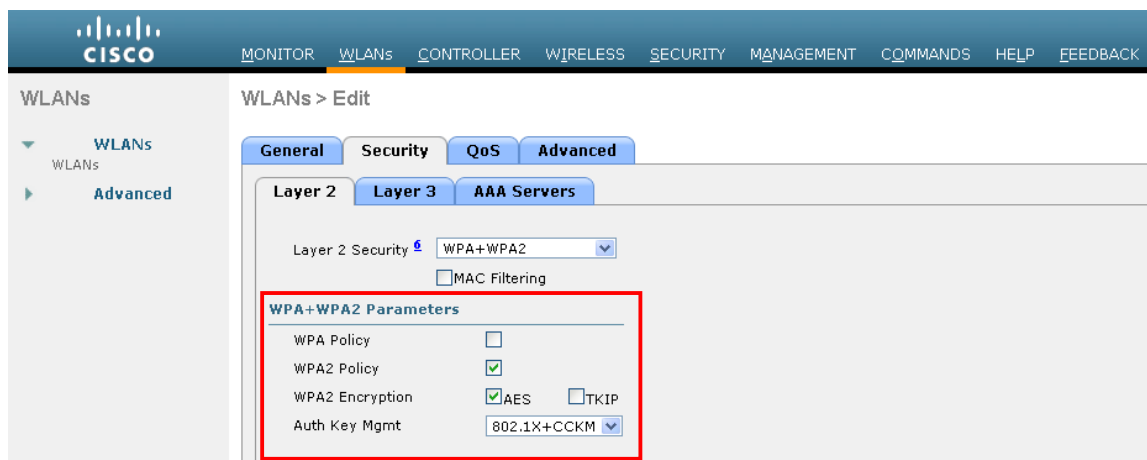
It is recommended to have the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G operate on the 5 GHz band due to have many channels available and not as many interferers as the 2.4 GHz band has.



The screenshot shows the Cisco WLAN configuration interface. The 'WLANs > Edit' page has tabs for General, Security, QoS, and Advanced. The 'General' tab is active, showing the following settings:

Profile Name	voice
Type	WLAN
SSID	voice
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X + CCKM)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	802.11a only
Interface	voice
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

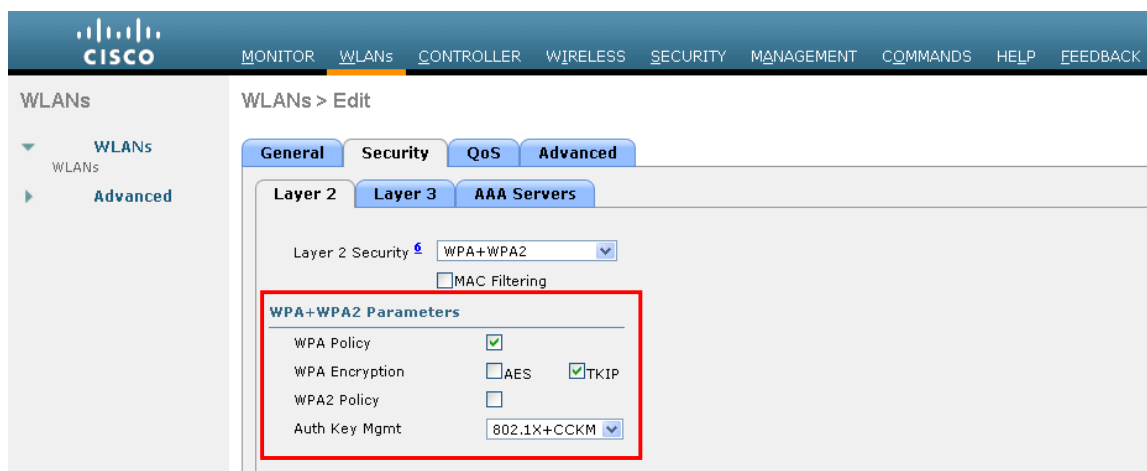
In order to utilize CCKM, enable WPA2 policy with AES encryption and 802.1x + CCKM for authenticated key management type when the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G are running firmware version 1.3(4) or later in order to enable fast secure roaming.



The screenshot shows the Cisco WLAN configuration interface, specifically the 'Layer 2' tab under the 'Security' section. The 'Layer 2 Security' is set to 'WPA+WPA2'. The 'WPA+WPA2 Parameters' section is expanded, showing the following settings:

WPA Policy	<input type="checkbox"/>
WPA2 Policy	<input checked="" type="checkbox"/>
WPA2 Encryption	<input checked="" type="checkbox"/> AES <input type="checkbox"/> TKIP
Auth Key Mgmt	802.1X+CCKM

If the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G are running firmware version 1.3(3) or earlier, then enable WPA policy with TKIP encryption and 802.1x + CCKM for authenticated key management type in order to enable fast secure roaming.



The WMM policy should be set to **Required** only if the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G or other WMM enabled phones will be using this SSID.

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

If non-other WMM clients must utilize the same SSID as the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, then ensure the WMM policy is set to **Allowed**.

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



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

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

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

Configure **Client Exclusion** as necessary.

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

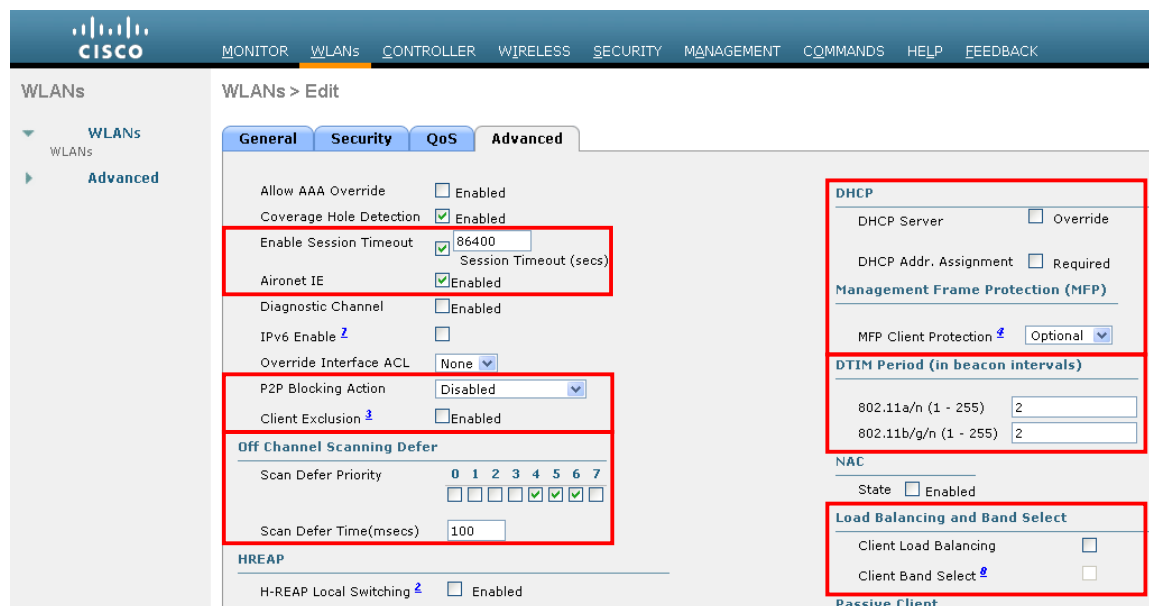
If using best effort applications frequently (e.g. IP Phone Services, VPN, etc.) or if DSCP values for priority applications (e.g. voice, video, call control) are not preserved to the access point, then is recommended to enable the lower priority queues to defer off channel scanning as well as potentially increasing the scan defer time.

**DHCP Address Assignment Required** should be disabled.

**MFP Client Protection** should be **Disabled** or set to **Optional**.

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

Ensure **Client Load Balancing** and **Client Band Select** are disabled for the voice SSID.



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

As of the 1.3(2) release, the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G utilizes open + eap when doing 802.1x authentication, but utilized network-eap in previous releases.

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

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

```
wlccp authentication-server infrastructure method_Infrastructure
wlccp authentication-server client mac method_Clients
wlccp authentication-server client eap method_Clients
wlccp authentication-server client leap method_Clients
wlccp wds priority 255 interface BV11
```

## Controller Settings

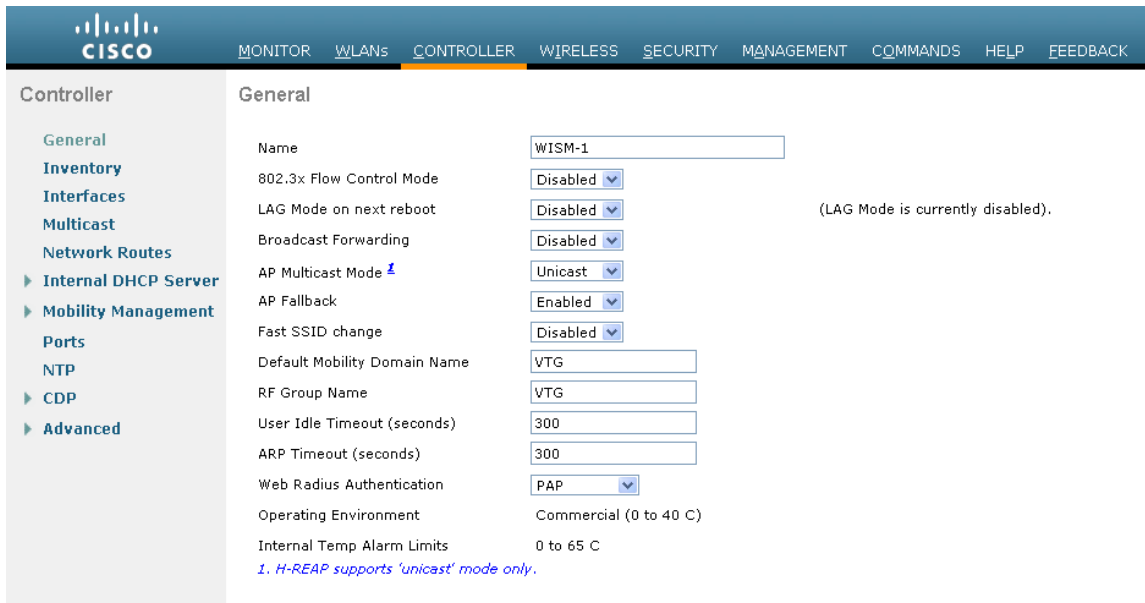
Ensure the Cisco Unified Wireless LAN Controller hostname is configured correctly.

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

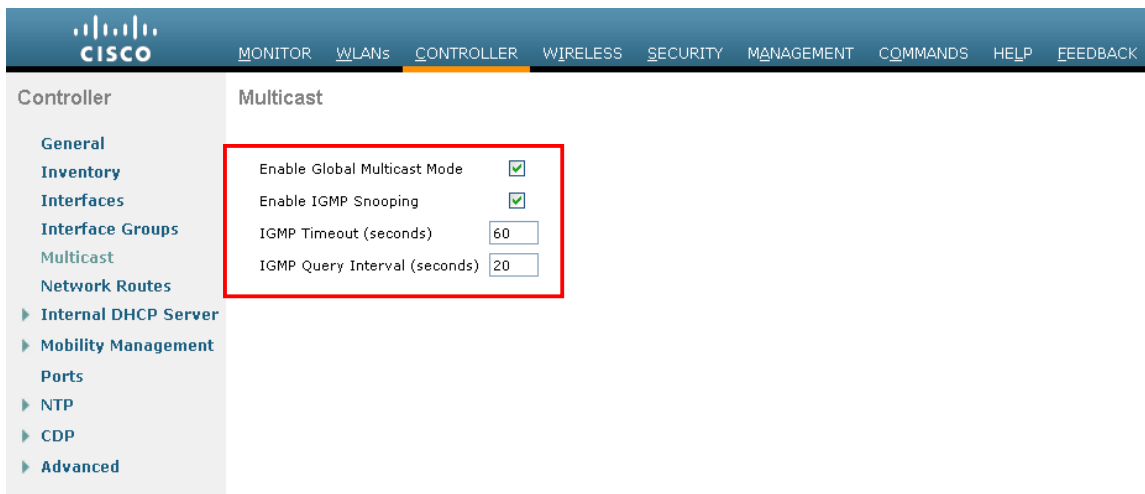
Configure the desired AP multicast mode.

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

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

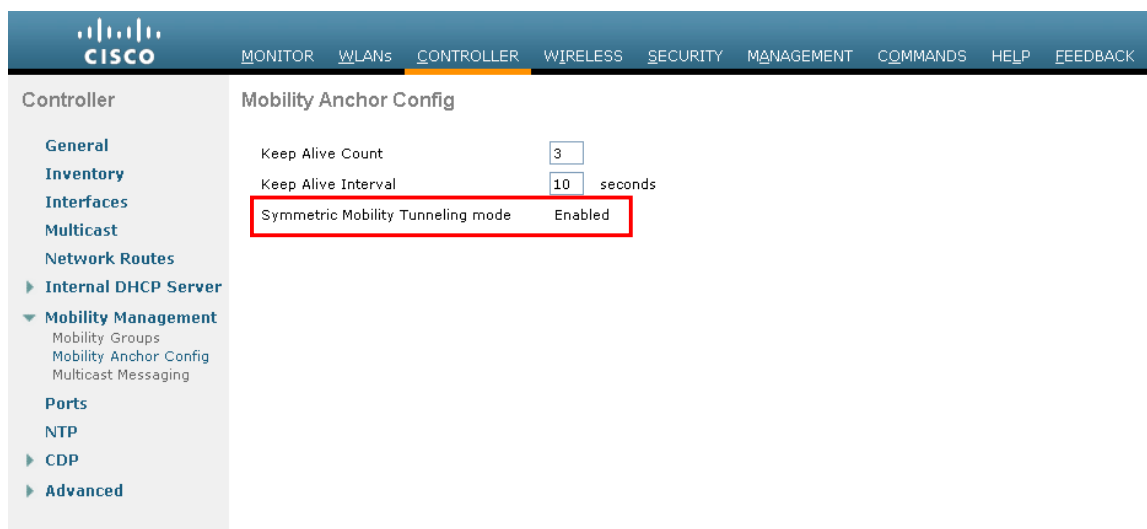


If utilizing multicast, then **Enable Global Multicast Mode** and **Enable IGMP Snooping** should be enabled.

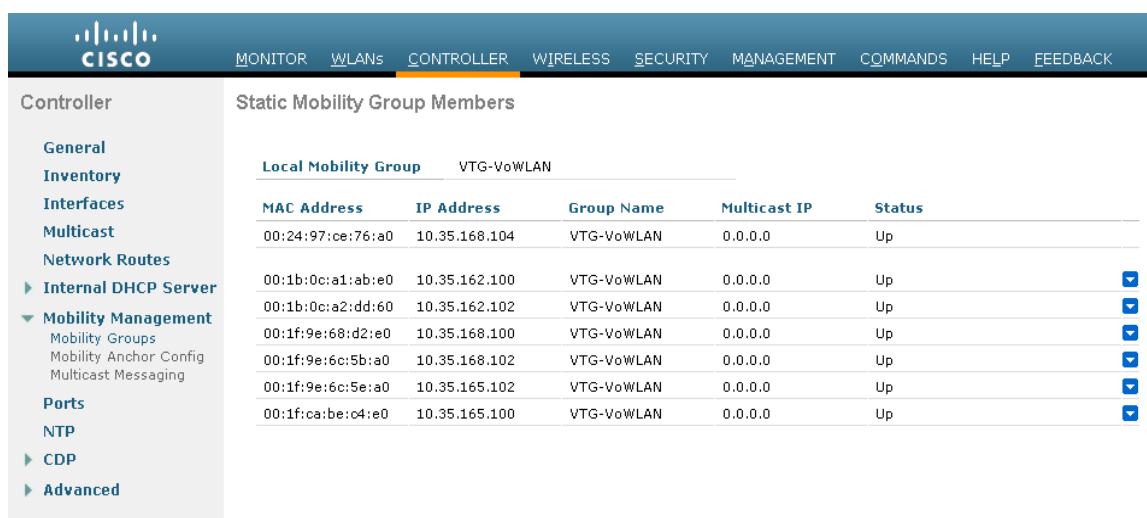


If utilizing layer 3 mobility, then **Symmetric Mobility Tunneling** should be **Enabled**.

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



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



## 802.11 Network Settings

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

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

Ensure **DTPC Support** is enabled.

If using 802.11n capable access points, ensure **ClientLink** is enabled.

Configure 12 Mbps as the mandatory (basic) rate and 18 – 24 or 54 Mbps as supported (optional) rates.

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

Enable **CCX Location Measurement**.

The screenshot shows the Cisco Wireless configuration interface for 802.11a Global Parameters. The left sidebar contains a navigation menu with options like Access Points, Radios, Advanced, Mesh, HREAP Groups, 802.11a/n, 802.11b/g/n, Media Stream, Country, Timers, and QoS. The main content area is titled '802.11a Global Parameters' and is divided into several sections:

- General:** 802.11a Network Status (Enabled), Beacon Period (100), Fragmentation Threshold (2346), DTPC Support (Enabled).
- 802.11a Band Status:** Low Band (Enabled), Mid Band (Enabled), High Band (Enabled).
- 11n Parameters:** ClientLink (Enabled).
- Data Rates:\*\*:** 6 Mbps (Disabled), 9 Mbps (Disabled), 12 Mbps (Mandatory), 18 Mbps (Supported), 24 Mbps (Supported), 36 Mbps (Supported), 48 Mbps (Supported), 54 Mbps (Supported).
- CCX Location Measurement:** Mode (Enabled), Interval (60 seconds).

Below the configuration sections, there is a note: *\*\* Data Rate 'Mandatory' implies that clients who do not support that specific rate will not be able to associate. Data Rate 'Supported' implies that any associated client that also supports that same rate may communicate with the AP using that rate. But it is not required that a client be able to use the rates marked supported in order to associate. The actual data rates that are supported depend on the channel selected as different channels may have different bandwidths. The reason is that we show data rates and allow the user to select the data rates. But in reality, the AP will pick the next lower data rate allowed for that channel if the chosen data rate is not supported.*

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

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

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

Ensure **DTPC Support** is enabled.

If using 802.11n capable access points, ensure **ClientLink** is enabled.

Configure 12 Mbps as the mandatory (basic) rate and 18 – 24 or 54 Mbps as supported (optional) rates assuming that there will not be any 802.11b only clients that will connect to the wireless LAN.

If 802.11b clients exist, then 11 Mbps should be set as the mandatory (basic) rate and 12-24 or 54 Mbps as supported (optional). 36-54 Mbps can optionally be disabled, if there are not any applications that can benefit from those rates (e.g. video).

Enable **CCX Location Measurement**.

**802.11b/g Global Parameters**

**General**

- 802.11b/g Network Status:  Enabled
- 802.11g Support:  Enabled
- Beacon Period (milliseconds): 100
- Short Preamble:  Enabled
- Fragmentation Threshold (bytes): 2346
- DTPC Support:  Enabled

**11n Parameters**

- ClientLink:  Enabled

**CCX Location Measurement**

- Mode:  Enabled
- Interval (seconds): 60

**Data Rates\*\***

- 1 Mbps: Disabled
- 2 Mbps: Disabled
- 5.5 Mbps: Disabled
- 6 Mbps: Disabled
- 9 Mbps: Disabled
- 11 Mbps: Disabled
- 12 Mbps: Mandatory
- 18 Mbps: Supported
- 24 Mbps: Supported
- 36 Mbps: Supported
- 48 Mbps: Supported
- 54 Mbps: Supported

\*\* Data Rate 'Mandatory' implies that clients who do not support that specific rate will not be able to associate. Data Rate 'Supported' implies that any associated client that also supports that same rate may communicate with the AP using that rate. But it is not required that a client be able to use the rates marked supported in order to associate. The actual data rates that are supported depend on the channel selected as different channels may have different bandwidths. The reason is that we show data rates and allow the user to select the data rates. But in reality, the AP will pick the next lower data rate allowed for that channel if the chosen data rate is not supported.

Enable **ClientLink** if using Cisco 802.11n capable access points.

**802.11a/n Cisco APs > Configure**

**General**

- AP Name: sjc32-11a-ap9
- Admin Status:
- Operational Status: UP
- Slot #: 1

**11n Parameters**

- 11n Supported: Yes
- ClientLink:

**CleanAir**

- CleanAir Capable: Yes
- CleanAir Admin Status:
- \* CleanAir enable will take effect only if it is enabled on this band.
- Number of Spectrum Expert connections: 0

**Antenna Parameters**

- Antenna Type:
- Antenna:
  - A:
  - B:
  - C:

**RF Channel Assignment**

- Current Channel: 36 (Extension : 40)
- Channel Width \*:
- \* Channel width can be configured only when channel configuration is in custom mode.
- Assignment Method:  Global  Custom

**Tx Power Level Assignment**

- Current Tx Power Level: 2
- Assignment Method:  Global  Custom

**Performance Profile**

View and edit Performance Profile for this AP

Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

## Auto RF (RRM)

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

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



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

The 5 GHz channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n capable access points.

Ensure that channel 165 is not enabled in the DCA list as the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G do not support this channel.



802.11a > RRM > Dynamic Channel Assignment (DCA)

### Dynamic Channel Assignment Algorithm

Channel Assignment Method:  Automatic Interval: 10 minutes AnchorTime: 0  
 Freeze **Invoke Channel Update Once**  
 OFF

Avoid Foreign AP interference:  Enabled  
 Avoid Cisco AP load:  Enabled  
 Avoid non-802.11a noise:  Enabled  
 Avoid Persistent Non-WiFi Interference:  Enabled  
 Channel Assignment Leader: SJC32-00A-TALWAR1 (10.35.168.104)  
 Last Auto Channel Assignment: 247 secs ago  
 DCA Channel Sensitivity: Medium (15 dB)  
 Channel Width:  20 MHz  40 MHz  
 Avoid check for non-DFS channel:  Enabled

### DCA Channel List

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

Select	Channel
<input checked="" type="checkbox"/>	36
<input checked="" type="checkbox"/>	40
<input checked="" type="checkbox"/>	44
<input checked="" type="checkbox"/>	48
<input checked="" type="checkbox"/>	52
<input type="checkbox"/>	56
<input type="checkbox"/>	60
<input type="checkbox"/>	64
<input type="checkbox"/>	149
<input type="checkbox"/>	153
<input type="checkbox"/>	157
<input type="checkbox"/>	161

Extended UNII-2 channels:  Enabled

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

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

The screenshot displays the Cisco Wireless configuration interface for Dynamic Channel Assignment (DCA). The left sidebar shows the navigation menu with '802.11b/g/n' selected. The main content area is titled '802.11b > RRM > Dynamic Channel Assignment (DCA)'. Under the 'Dynamic Channel Assignment Algorithm' section, the 'Channel Assignment Method' is set to 'Automatic', with an interval of '10 minutes' and an anchor time of '0'. A button labeled 'Invoke Channel Update Once' is visible. Below this, several options are checked: 'Avoid Foreign AP interference', 'Avoid non-802.11b noise', and 'Avoid Persistent Non-WiFi Interference'. The 'Channel Assignment Leader' is identified as 'SJC32-00A-TALWAR1 (10.35.168.104)', and the 'Last Auto Channel Assignment' occurred '549 secs ago'. The 'DCA Channel Sensitivity' is set to 'Medium (10 dB)'. A red box highlights the 'DCA Channel List' section, which contains a text box with '1, 6, 11' and a table with the following data:

Select	Channel
<input checked="" type="checkbox"/>	1
<input type="checkbox"/>	2
<input type="checkbox"/>	3
<input type="checkbox"/>	4
<input type="checkbox"/>	5
<input type="checkbox"/>	-

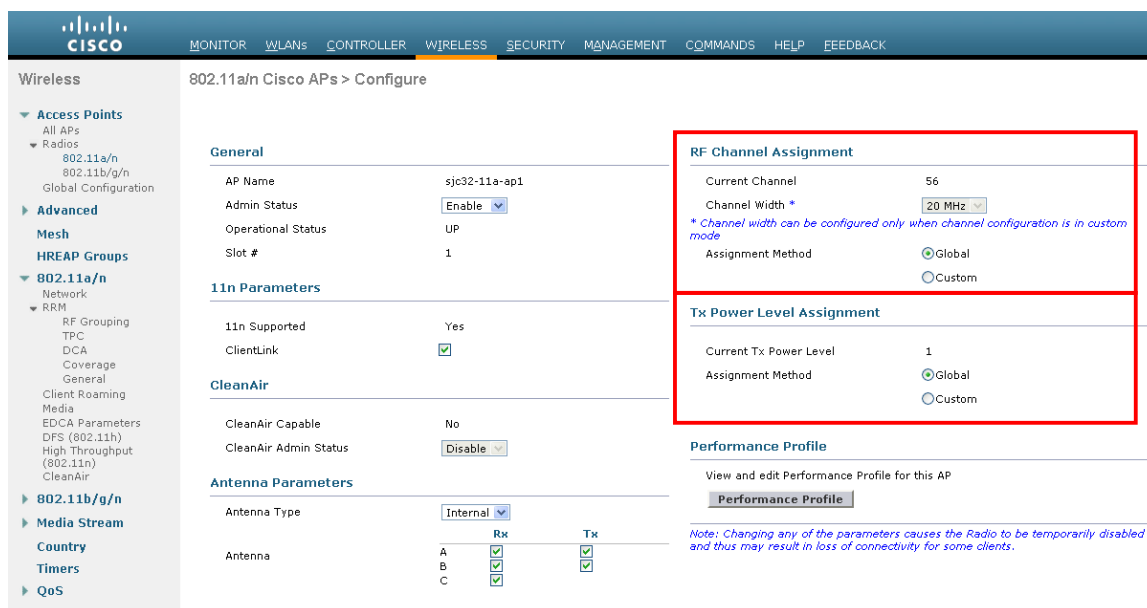
Individual access points can be configured to override the global setting to use dynamic channel and transmit power assignment for either 5 or 2.4 GHz depending on which frequency band is to be utilized.

Other access points enabled can be enabled for Auto RF and workaround the access points that are statically configured.

This may be necessary if there is an intermittent interferer present in an area.

The channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n capable access points.

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



## Call Admission Control

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G currently do not support TSPEC (Call Admission Control).

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

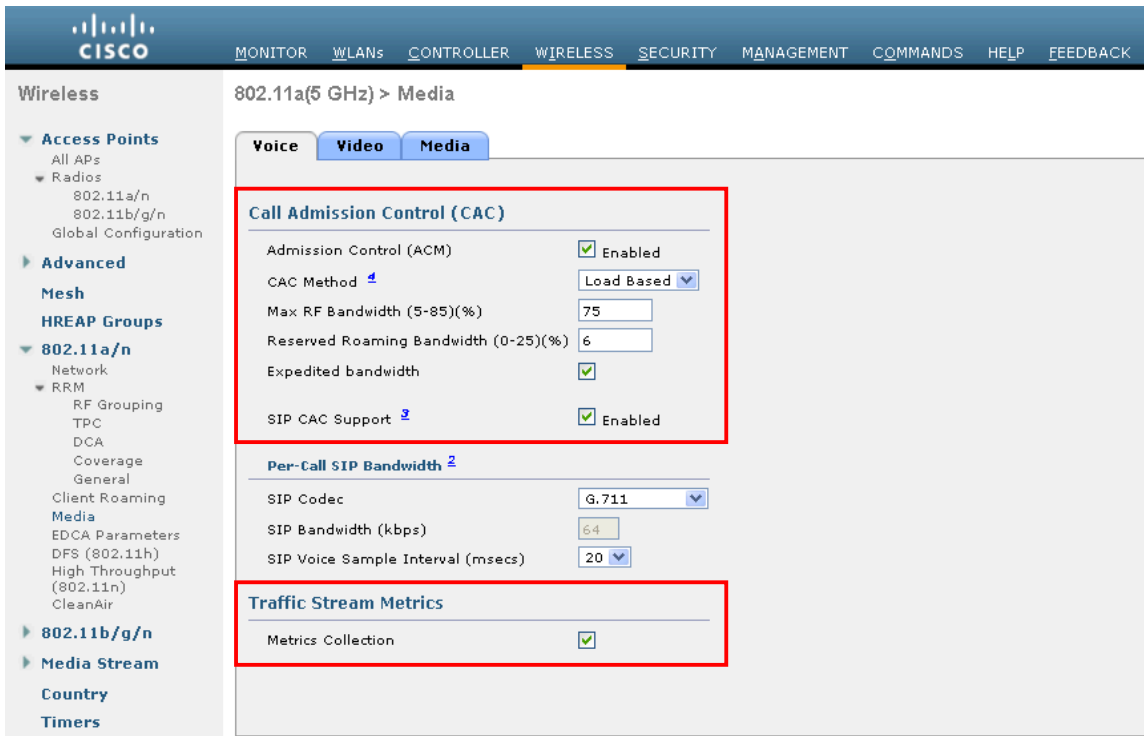
The maximum bandwidth default setting for voice is **75%** where **6%** of that bandwidth is reserved for roaming clients.

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

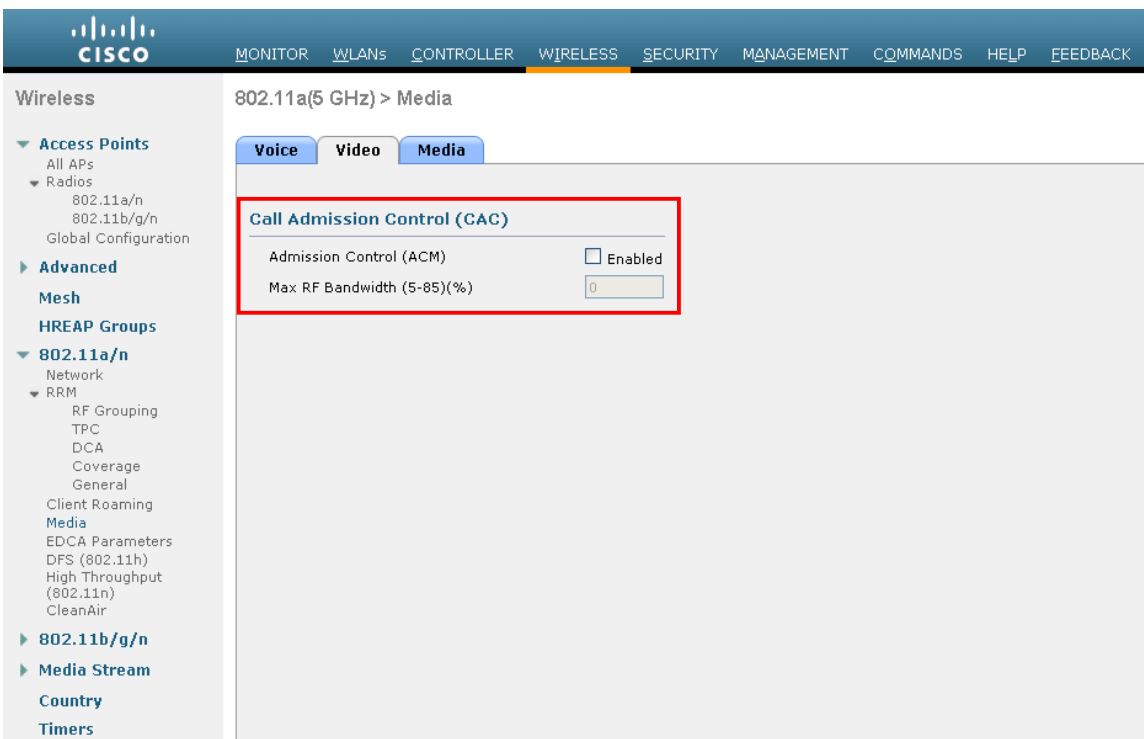
If CAC is to be enabled, will want to ensure **Load-based CAC** is enabled, which is available for the Cisco Unified Wireless LAN Controller, but not currently available on the Cisco Autonomous access point platform.

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

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



Admission Control Mandatory for Video should be disabled.



If Call Admission Control for voice is enabled, then the following configuration should be enabled, which can be displayed in the **show run-config**.

```

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

```

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

```
(Cisco Controller) >config 802.11a cac voice stream-size 84000 max-streams 2
```

Ensure QoS is setup correctly under the WLAN / SSID configuration, which can be displayed 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 Cisco Autonomous access point, the admission must be unblocked on the SSID as well.

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

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

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

```

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

```

Also ensure that the PHY rate configured on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G is enabled as a nominal rate in the STREAM configuration of the Cisco Autonomous access point.

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

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

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

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

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

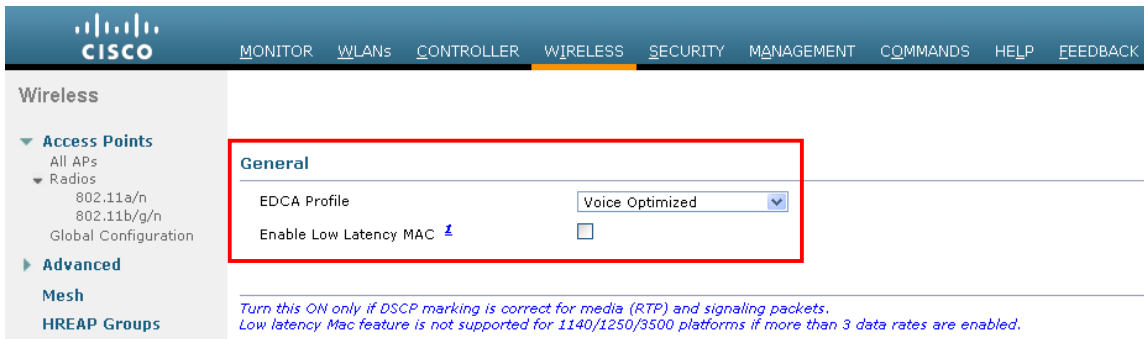
The screenshot displays the Cisco Wireless configuration page for the 802.11a(5 GHz) Media settings. The interface is divided into a sidebar on the left and a main content area on the right. The sidebar contains navigation options such as 'Access Points', 'Advanced', 'Mesh', 'HREAP Groups', '802.11a/n', '802.11b/g/n', 'Media Stream', 'Country', 'Timers', and 'QoS'. The main content area shows the '802.11a(5 GHz) > Media' configuration page. The 'Media' tab is selected, and the configuration is organized into several sections. Two sections are highlighted with red boxes: 'General' and 'Media Stream - Multicast Direct Parameters'. The 'General' section includes 'Unicast Video Redirect' (checked), 'Multicast Direct Admission Control' (checked), 'Maximum Media Bandwidth (0-85(%))' (85), 'Client Minimum Phy Rate' (6000), and 'Maximum Retry Percent (0-100%)' (80). The 'Media Stream - Multicast Direct Parameters' section includes 'Multicast Direct Enable' (checked), 'Max Streams per Radio' (No-limit), 'Max Streams per Client' (No-limit), and 'Best Effort QoS Admission' (unchecked). The interface also includes a footer with foot notes.

## EDCA Parameters

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

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

LLM is not supported on the Cisco 802.11n access points.



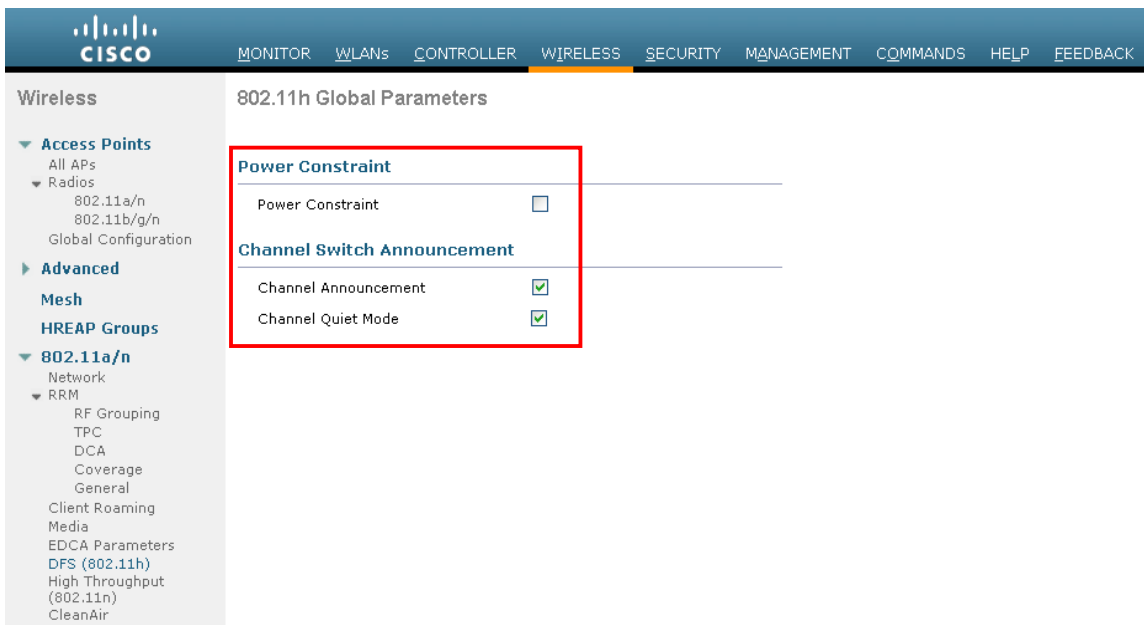
## DFS (802.11h)

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

**Power Constraint** should be left un-configured or set to 0 dBm as DTPC will be used by the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926 to control the transmission power.

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

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



## CleanAir

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

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

Wireless 802.11a > CleanAir

**CleanAir Parameters**

CleanAir  Enabled

Report Interferers  Enabled

**Interferences to Ignore**

- Canopy
- WiMax Fixed

**Interferences to Detect**

- TDD Transmitter
- Jammer
- Continuous Transmitter
- DECT-like Phone
- Video Camera

**Trap Configurations**

Enable AQI(Air Quality Index) Trap  Enabled

AQI Alarm Threshold (1 to 100)

Enable Interference For Security Alarm  Enabled

**Do not trap on these types**

- TDD Transmitter
- Continuous Transmitter
- DECT-like Phone
- Video Camera
- SuperAG

**Trap on these types**

- Jammer
- WiFi Inverted
- WiFi Invalid Channel

**Event Driven RRM (Change Settings)**

EDRRM Disabled

Sensitivity Threshold N/A

(1)Device Security alarms, Event Driven RRM and Persistence Device Avoidance algorithm will not work if Interferers reporting is disabled.  
(2)AQI value 100 is best and 1 is worst

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

Wireless 802.11a/n Cisco APs > Configure

**General**

AP Name sjc32-11a-ap9

Admin Status

Operational Status UP

Slot # 1

**11n Parameters**

11n Supported Yes

ClientLink

**CleanAir**

CleanAir Capable Yes

CleanAir Admin Status

\* CleanAir enable will take effect only if it is enabled on this band.

Number of Spectrum Expert connections 0

**Antenna Parameters**

Antenna Type

Antenna A

B

C

**RF Channel Assignment**

Current Channel 36 (Extension : 40)

Channel Width \*

\* Channel width can be configured only when channel configuration is in custom mode.

Assignment Method  Global  Custom

**Tx Power Level Assignment**

Current Tx Power Level 2

Assignment Method  Global  Custom

**Performance Profile**

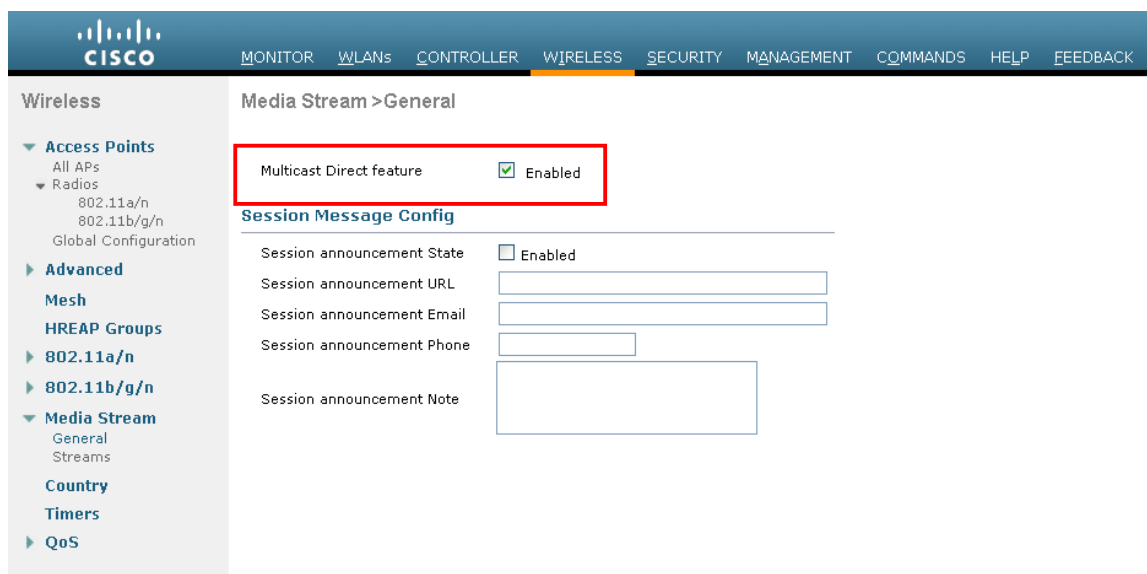
View and edit Performance Profile for this AP

Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

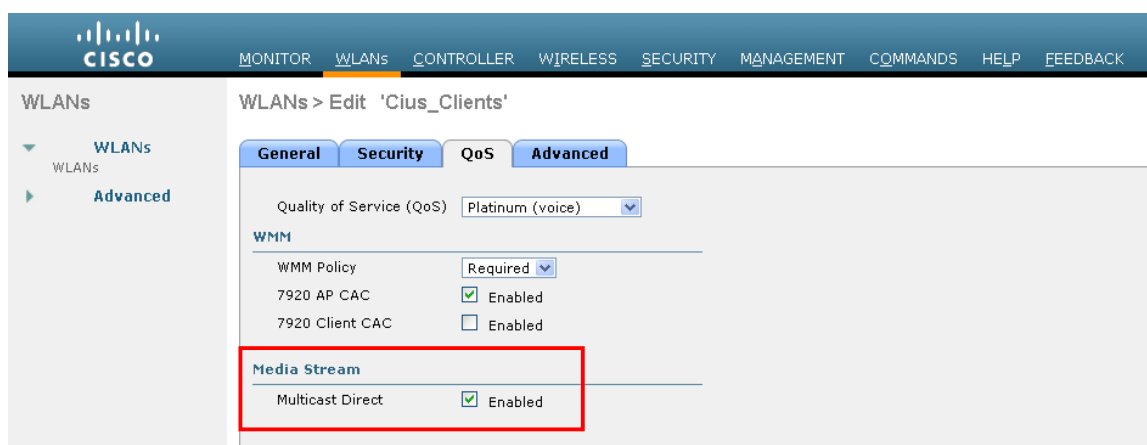
## Multicast Direct

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





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



## QoS Profiles

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

- Platinum =6
- Gold = 5
- Silver = 3
- Bronze = 1

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

Wireless

- Access Points
  - All APs
  - Radios
    - 802.11a/n
    - 802.11b/g/n
    - Global Configuration
- Advanced
  - Load Balancing
  - Band Select
- Mesh
- HREAP Groups
- 802.11a/n
- 802.11b/g/n
- Media Stream
- Country
- Timers
- QoS
  - Profiles
  - Roles

**Edit QoS Profile**

QoS Profile Name: platinum

Description: For Voice Applications

**Per-User Bandwidth Contracts (k) \***

Average Data Rate: 0  
 Burst Data Rate: 0  
 Average Real-Time Rate: 0  
 Burst Real-Time Rate: 0

**Wired QoS Protocol**

Protocol Type: 802.1p  
 802.1p Tag: 6

*\* The value zero (0) indicates the feature is disabled*

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

Wireless

- Access Points
  - All APs
  - Radios
    - 802.11a/n
    - 802.11b/g/n
    - Global Configuration
- Advanced
  - Load Balancing
  - Band Select
- Mesh
- HREAP Groups
- 802.11a/n
- 802.11b/g/n
- Media Stream
- Country
- Timers
- QoS
  - Profiles
  - Roles

**Edit QoS Profile**

QoS Profile Name: gold

Description: For Video Applications

**Per-User Bandwidth Contracts (k) \***

Average Data Rate: 0  
 Burst Data Rate: 0  
 Average Real-Time Rate: 0  
 Burst Real-Time Rate: 0

**Wired QoS Protocol**

Protocol Type: 802.1p  
 802.1p Tag: 5

*\* The value zero (0) indicates the feature is disabled*

The screenshot shows the Cisco Wireless configuration interface for editing a QoS profile named 'silver'. The profile description is 'For Best Effort'. Under 'Per-User Bandwidth Contracts (k)', all rates are set to 0. The 'Wired QoS Protocol' section is highlighted with a red box, showing 'Protocol Type' set to '802.1p' and '802.1p Tag' set to '3'. A note below states: '\* The value zero (0) indicates the feature is disabled'.

The screenshot shows the Cisco Wireless configuration interface for editing a QoS profile named 'bronze'. The profile description is 'For Background'. Under 'Per-User Bandwidth Contracts (k)', all rates are set to 0. The 'Wired QoS Protocol' section is highlighted with a red box, showing 'Protocol Type' set to '802.1p' and '802.1p Tag' set to '1'. A note below states: '\* The value zero (0) indicates the feature is disabled'.

## QoS Basic Service Set (QBSS)

There are three different versions of QoS Basic Service Set (QBSS) that the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G support.

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.

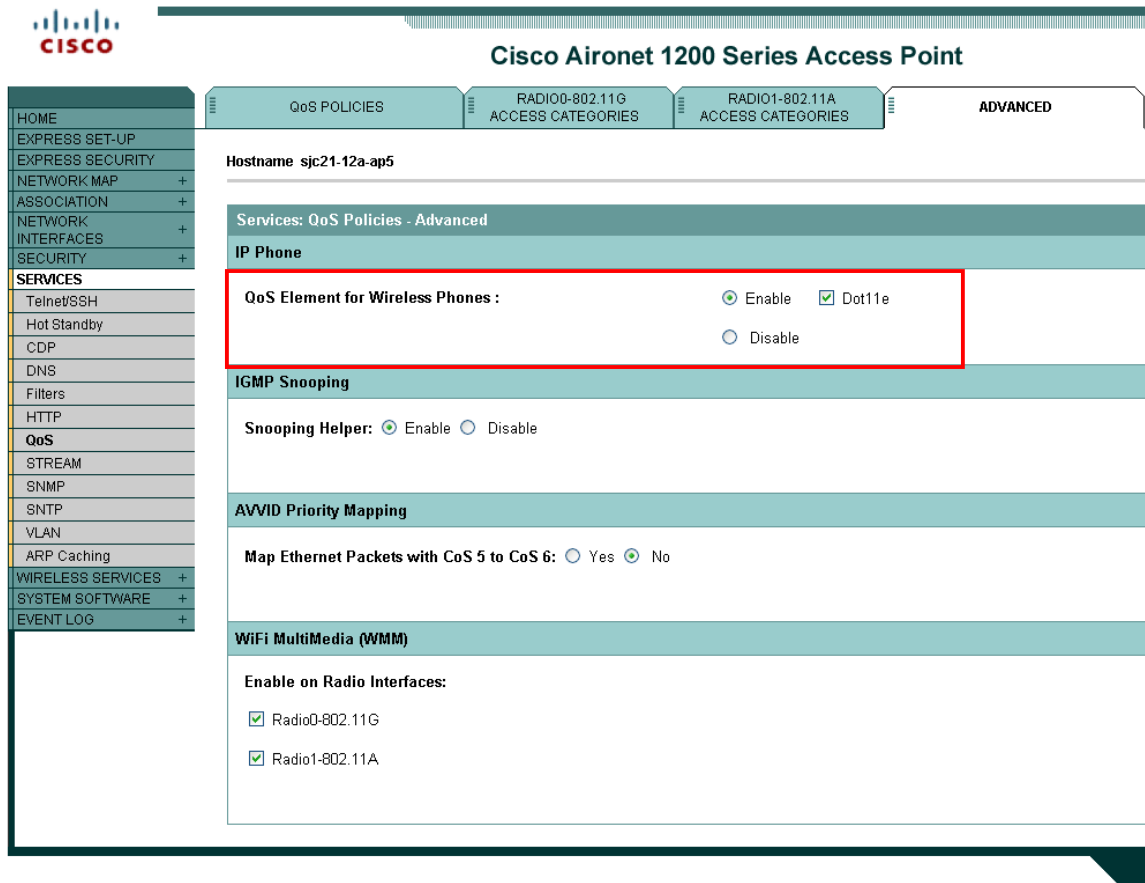
Each version of QBSS can be optionally be configured on the access point.

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Deployment Guide

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

For the Cisco Autonomous access point, **dot11 phone** or **dot11 phone dot11e** will enable QBSS.

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



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

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

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

## CCKM Timestamp Tolerance

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

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

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

It is recommended to adjust the CCKM timestamp tolerance to 5000 ms to optimize the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G roaming experience.

```
(Cisco Controller) >config wlan security wpa akm cckm timestamp-tolerance ?
<tolerance> Allow CCKM IE time-stamp tolerance <1000 to 5000> milliseconds; Default tolerance 1000 msec
```

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

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

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

```
CCKM tsf Tolerance..... 5000
```

## Auto-Immune

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

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

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

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

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

```
(Cisco Controller) >show wps summary
```

Auto-Immune

```
Auto-Immune..... Disabled
```

Client Exclusion Policy

```
Excessive 802.11-association failures..... Enabled
Excessive 802.11-authentication failures..... Enabled
Excessive 802.1x-authentication..... Enabled
IP-theft..... Enabled
Excessive Web authentication failure..... Enabled
```

Signature Policy

```
Signature Processing..... Enabled
```

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

(Cisco Controller) >config wps auto-immune disable

## WLAN Controller Advanced EAP Settings

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

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

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

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

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

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

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

```
(Cisco Controller) >config advanced eap request-timeout 30
```

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

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

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

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

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

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

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

## Proxy ARP

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

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

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

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

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

For Cisco Autonomous access points, enter **dot11 arp-cache optional**.

The screenshot shows the configuration page for a Cisco Aironet 1200 Series Access Point. The page title is "Cisco Aironet 1200 Series Access Point" and the hostname is "sjc21-12a-ap5". On the left side, there is a navigation menu with various configuration categories. The "Services: ARP Caching" section is highlighted with a red box. This section contains two configuration options: "Client ARP Caching" with radio buttons for "Enable" (selected) and "Disable", and a checked checkbox for "Forward ARP Requests To Radio Interfaces When Not All Client IP Addresses Are Known".

## TKIP Countermeasure Holdoff Time

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

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

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

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

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

For the Cisco Autonomous access point, enter the time in seconds to holdoff clients if a TKIP countermeasure event occurs.

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

For more information about these topics, refer to the Enterprise Mobility Design Guide at this URL:  
<http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html>

## VLANs and Cisco Autonomous Access Points

Segment wireless voice and data into separate VLANs.

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

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

For the native VLAN, it is recommended not to use VLAN 1 to ensure that IAPP packets are exchanged successfully.

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

Port security should be disabled on switchports that Cisco Autonomous access points are directly connected to.

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

## Configuring the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G

There are various methods for configuring network settings on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

### Configuring Phones with the Keypad

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

It may be required to unlock the screen by pressing **\*\*#**.

For more information, refer to the **Configuring Settings on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G** in the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Administration Guide at this URL:

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

### Configuring Phones with the Web Interface

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G have an HTTPS enabled web interface that can be accessed via the 802.11a/b/g radio or USB.



A PC running Windows 2000 or Windows XP is required to utilize the USB interface on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

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

By default, the USB interface USB of the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G is statically set to 192.168.1.100 /24.

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

Log into the administration web pages by using these defaults:

username = **admin** / password = **Cisco**

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

## Configuring Phones with Wavelink Avalanche

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

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

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

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

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

## Wireless LAN Settings

Use the following guidelines to configure network profiles.

- The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G support 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, 7925G-EX, and 7926G would default to Auto-RSSI mode, which would attempt to associate to the access point with the strongest signal.
- 802.11a mode will only scan 5 GHz channels and 802.11b/g mode will only scan 2.4 GHz channels, where it will then attempt to associate to an access point if the configured network is available.
- For Auto-a and Auto-b/g modes, this is giving preference to one frequency band over another. At power on, will scan all 2.4 and 5 GHz channels then attempt to associate to an access point for the configured network using the preferred frequency band if available. If the preferred frequency band is not available, then the Cisco Unified Wireless Phone 7925G will try to use the less preferred frequency band if available. If the phone roams out of coverage of the

preferred frequency band, where the less preferred frequency band signal is available, then the phone will attempt to associate to that less preferred frequency band.

- To 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 (**Call Power Save Mode** set to **None**) may need to be used instead of U-APSD/PS-POLL if the access point does not support power save enabled clients.
- As of the 1.3(3) release, the Prompt Mode feature can be optionally enabled. When enabled, the password will not be stored in flash, but only in memory after entering manually after each power on sequence for seamless roaming. However, the username can be stored after entering at the prompt, but can be overridden at the next login. If the prompt is dismissed, then there is a **Login** softkey presented in order to invoke the login process. The Prompt Mode feature is only supported with Network Profile 1. If multiple network profiles are enabled and Prompt Mode is enabled, then the user would have to dismiss the login in order to switch to other enabled network profiles.
- Below are the available security modes supported and the key management and encryption types can be used for each mode.

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

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

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

- The AKM security mode is an auto authentication mode that can use either LEAP for 802.1x authentication or WPA Pre-Shared Key.
- If using 802.11i (Pre-Shared key), enter the ASCII or hexadecimal formatted key.  
Pre-Shared Key requires that a passphrase be entered in ASCII or hexadecimal format.

Key Style	Characters
-----------	------------

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

- AKM mode requires a key management type to be enabled on the Access Point.  
For 802.1x authentication methods, WPA, WPA2 or CCKM is required.  
For non-802.1x authentication, WPA-PSK or WPA2-PSK is required.
- If using open authentication plus WEP encryption or shared key authentication, enter the static WEP key information that matches the access point configuration.

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

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

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

- Select whether to use Dynamic Host Configuration Protocol (DHCP) or configure static IP information.
- If option 150 or 66 is not configured to provide the TFTP server IP address via the network's DHCP scope, then enter the TFTP server IP address info.
- To enable PEAP with server validation, select **Validate Server Certificate** after importing the authentication server certificate.
- When using EAP-TLS, select either **Manufacturing Issued** or **User Installed** for the **Client EAP-TLS Certificate** option after selecting EAP-TLS.

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



## Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

Phone DN 89023675

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

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

**Wireless**

Profile Name:

SSID:

Call Power Save Mode:

802.11 Mode:

Scan Mode: **Auto**

Restricted Data Rates: **False**

**WLAN Security**

Security Mode:

Export Security Credentials:  True  False

**Wireless Security Credentials**

Username:

Password:

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

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

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

**Note:** If the TFTP IP is changed which is not included in the current Certificate Trust List (CTL) file, then TFTP will fail and may prevent the phone from registering successfully to the Cisco Unified Communications Manager. The CTL file will need to be erased manually in the Security Configuration menu from the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

## Configuring Advanced Network Profile Settings

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

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 a channel is disabled that is currently used by an access point, then the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G 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, 7925G-EX, and 7926G webpage:

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



## Cisco Unified Wireless IP Phone 7925G

SEP0013E0A0C587

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 Advanced Settings **Basic Profile 1**

**TSPEC Settings**

Minimum PHY Rate: 12 Mbps

Surplus Bandwidth: 1.300000

**802.11 G Power Settings**

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

check all clear all check non-overlap

**802.11 A Power Settings**

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

check all clear all check non-DFS

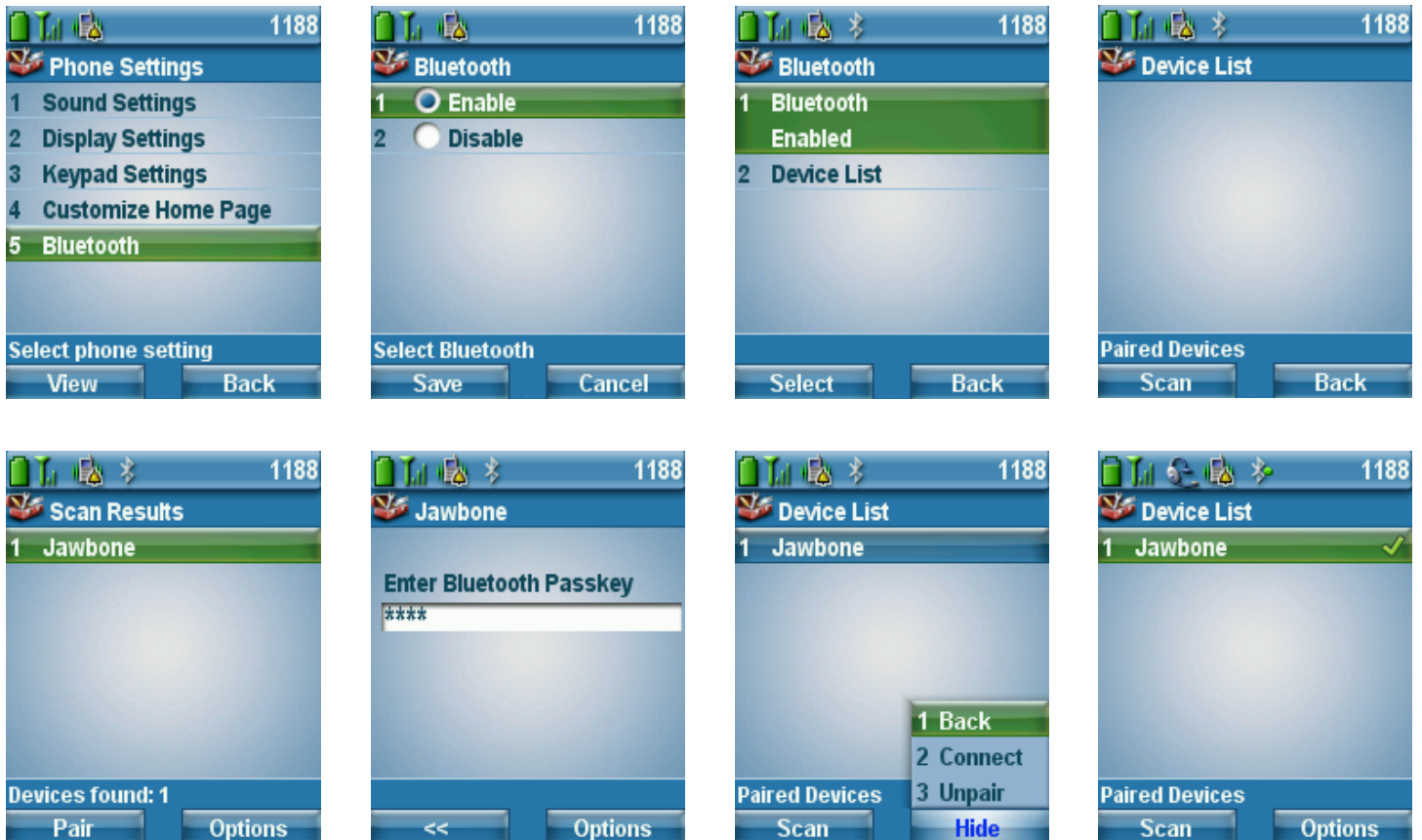
## Bluetooth Settings

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G have Bluetooth 2.0 + EDR support, which enables hands-free communications.

To pair a Bluetooth headset to the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, 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.



## Installing Certificates

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G support DER encoded binary X.509 certificates, which can be utilized with EAP-TLS or for authentication server validation when using PEAP (MS-CHAPv2).

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

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

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

Microsoft Certificate Authority (CA) servers are recommended as we have certified interoperability only with those CA types. Other CA server types may not be completely interoperable with the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G.

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

To use the MIC in the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, the Manufacturing Root and Manufacturing CA certificates must be exported and installed onto the RADIUS server.



## Cisco Unified Wireless IP Phone 7925G

SEP0013E0A0C587

Phone DN 89023675

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

Type	Common Name	Issuer Name	Valid From	Valid To	
User Installed	<not installed>	<not installed>			<input type="button" value="Install"/>
Manufacturing Issued	/O=Cisco Systems Inc./OU=EVVBU/CN=CP-7925G-SEP0013E0A0C587	/O=Cisco Systems/CN=Cisco Manufacturing CA	05/29/2008 08:37:13	05/29/2018 08:47:13	
Manufacturing Root CA	/O=Cisco Systems/CN=Cisco Root CA 2048	/O=Cisco Systems/CN=Cisco Root CA 2048	05/14/2004 20:17:12	05/14/2029 20:25:42	<input type="button" value="Export"/>
Manufacturing CA	/O=Cisco Systems/CN=Cisco Manufacturing CA	/O=Cisco Systems/CN=Cisco Root CA 2048	06/10/2005 22:16:01	05/14/2029 20:25:42	<input type="button" value="Export"/>
Authentication Server CA	/O=Digital Signature Trust Co./CN=DST Root CA X3	/O=Digital Signature Trust Co./CN=DST Root CA X3	09/30/2000 21:12:19	09/30/2021 14:01:15	<input type="button" value="Delete"/>
Authentication Server CA	<not installed>	<not installed>			<input type="button" value="Install"/>

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

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

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

To generate the certificate signing request, enter the certificate information and import the certificate from the Certificate Authority (CA) server that is signing the certificate. The signing CA root certificate is used for validation purposes to ensure that the user certificate was indeed signed by the correct CA.

The Common Name defaults to **CP-7925G-SEP<MAC\_Address>**, but can be customized, but must not be greater than 32 characters.

Browse to the Certificate Authority certificate that will be signing the client certificate and select **Submit**.

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

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

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

Certificates dated January 1 2038 and later are not supported.





## Cisco Unified Wireless IP Phone 7925G

SEP0013E0A0C587

Phone DN 89023675

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

### User Certificate Installation

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

Common Name	<input type="text" value="CP-7925G-SEP0013E0A0C587"/>
Organization	<input type="text" value="Cisco Systems"/>
Organization Unit	<input type="text" value="IPCBU"/>
City	<input type="text" value="Milpitas"/>
State	<input type="text" value="CA"/>
Country	<input type="text" value="US"/>
Key Size	<input type="text" value="1024"/>

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

Certificate Authority File	<input type="text" value="C:\CertAuthority.cer"/>	<input type="button" value="Browse..."/>
----------------------------	---	--

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

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

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

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

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



# Cisco Unified Wireless IP Phone 7925G

SEP0013E0A0C587

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

Phone DN 89023675

## User Certificate Installation

### Step 3 of 4: Signing the Certificate

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

```
-----BEGIN CERTIFICATE REQUEST-----
MIICQjCCAAmCAQAwDELMAkGA1UEBhMCVVMxMzA1BgNVBAGTAkNBMERwDwYD
VQOH
EwhNawXRhczEWMBOGA1UEChMNMjEzY2BzU3IzdGVtZzEOMAwGA1UECmMFSV
BD
Q1UwITAfBgNVBAMTGENQLTc5MjVhLVNFUDAwMTNFMEwQzU4NzCBnzANB
gkqhkiG
9wOBAQEFAAOBjQAwYkCgYEAx9wBOV71o2m2zsa1SPYBSFcTrmOzkI1Y9Rn
CrdO
WCqk7/5BEp/Pt3tPuYcm+ErQbSf5kvHwKzx+rYHbfmtmwoJu45TKBzccwQ2aVj+
EncD2dK16rOH2WrvQ7h/zFzLELXd5H9m1qFe/4YVpG+6k0JDbz21KT9JYs74dxPS
UJkCAwEAACBgTB/BgkqhkiG9wOBCQ4xcjBwMAwGA1UdEwEB/wQCAAAwJAYDVR
R
BB0wG4YZQ1AtNzkyNUctUOVQMDAxM0UwQTBNTG3ADA0BgNVHQ8BAf8EBAMCA/gw
KgYDVRO1AQH/BCAwHgYIKwYBBQUHAWEGCCeGAQUFBwMCBggrBgEFBQcDBTANBgkq
hkiG9wOBAQUFAAOBgQASTBwdYX8IPokfYotEANCuOHNEbJu2UIUpOPqjUBFAJpK
Uo/Q2h5rYYARTqU8vPTyptkuUR8Iha5VZsAr/HIaLmRV7ffNpxRT6T2Nwogkd1s
IhwqyFInncRceTlboH2YXSRnPV/E570WQAGkdtAz6b9yV7nxAcwNG112Czppg==
-----END CERTIFICATE REQUEST-----
```

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

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

Postpone Import Step

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

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

Paste the certificate data from the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G to the Certificate Authority signing server and submit for signing.

Microsoft Certificate Services -- peap-tls

Home

### Submit a Certificate Request or Renewal Request

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

#### Saved Request:

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

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

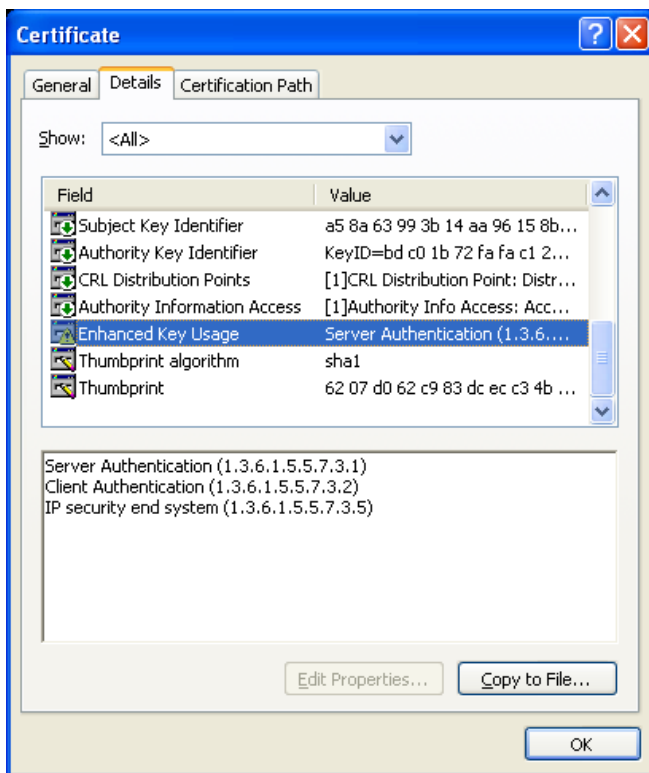
#### Additional Attributes:

Attributes:

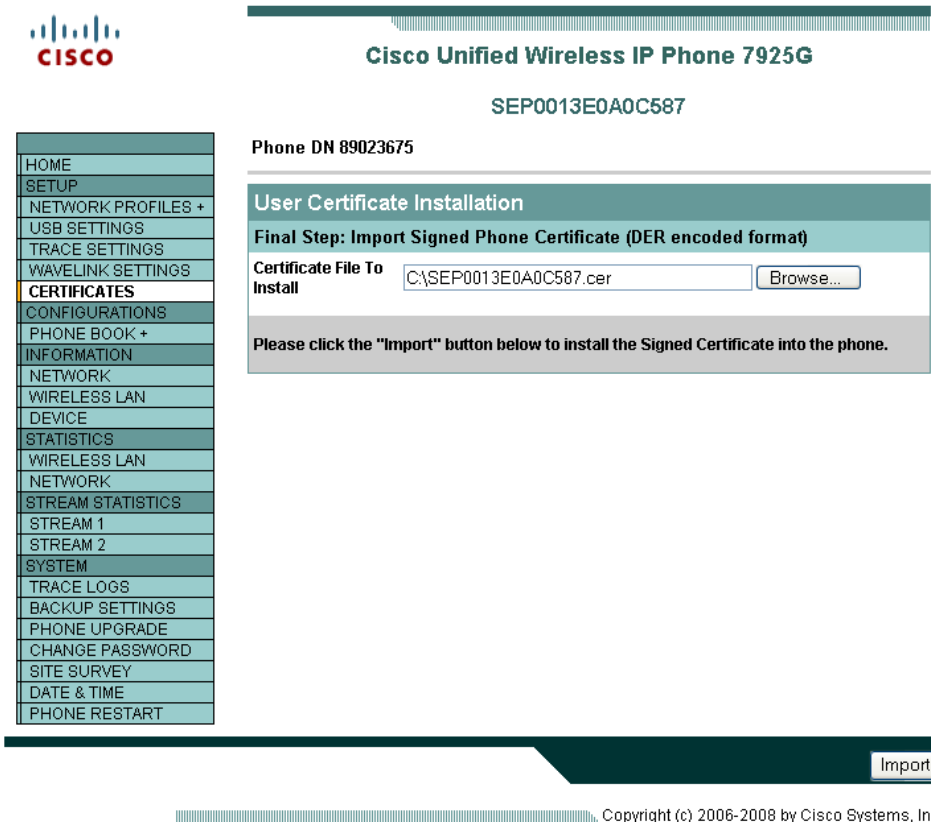
Submit >

When the certificate has been signed, download the CA certificate in DER encoded format (base 64 encoded certificates are 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.



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

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

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

The authentication server certificate must also be imported into the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G for both the MIC and User Installed methods. If the authentication server certificate was signed by a Certificate Authority (CA) server, then that DER encoded root certificate will need to be imported into the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

If the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G has not registered to a Cisco Unified Communications Manager yet, then the date and time must be configured manually for the first time.

The screenshot shows the configuration interface for a Cisco Unified Wireless IP Phone 7925G. On the left is a navigation menu with options like 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 (highlighted), and PHONE RESTART. The main content area is titled "Cisco Unified Wireless IP Phone 7925G" and "SEP0013E0A0C587". Below this, it shows "Phone DN 89023675". The "Date & Time Settings" section displays "Current Phone Date & Time" as "September 25, 2008 16:15:42". A red note states: "Note: Phone Date & Time may change when phone registered with Cisco Unified Communications Manager". The "Local Date & Time" section has a button "Set Phone to Local Date & Time". The "Specify Date & Time" section has dropdowns for "Date" (September 25 2008) and input fields for "Time" (16 hours, 15 minutes, 42 seconds), with a button "Set Phone to Specific Date & Time". A note at the bottom says: "NOTE: After changing the Date & Time, you must execute 'SYSTEM / PHONE RESTART' before the new time can be used to validate Certificates." The footer of the page reads "Copyright (c) 2006-2008 by Cisco Systems, Inc."

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G must be restarted after installing the certificate. Click on the hyperlink to navigate to the **Phone Restart** page.



## Cisco Unified Wireless IP Phone 7925G

SEP0013E0A0C587

Phone DN 89023675

### Authentication Server Root Certificate

Authentication Server CA certificate has been updated.  
Phone will use the new certificate after reboot. You can restart the phone with:  
**"SYSTEM / PHONE RESTART"**

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

OK

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

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

## Using Templates to Configure Phones

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

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

For security reasons, the Wireless LAN security information (Username/Password, WPA Pre-shared key information, and WEP key information) is not exported by default. In order to export this Wireless LAN security information, the network profile must be configured to allow this capability. For each network profile where the Wireless LAN security information is to be exported, configure the **Export Security Credentials** option to **True**. After selecting **True**, the Wireless LAN security information will need to be re-entered. This will then allow that information to be exported and then imported to other Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G phones.



## 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
<b>BACKUP SETTINGS</b>
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

### Backup Settings

#### Import Configuration

Encryption Key

Import File

#### Export Configuration

Encryption Key

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

## 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, 7925G-EX, and 7926G web page in order to help group clients for better management.



## 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

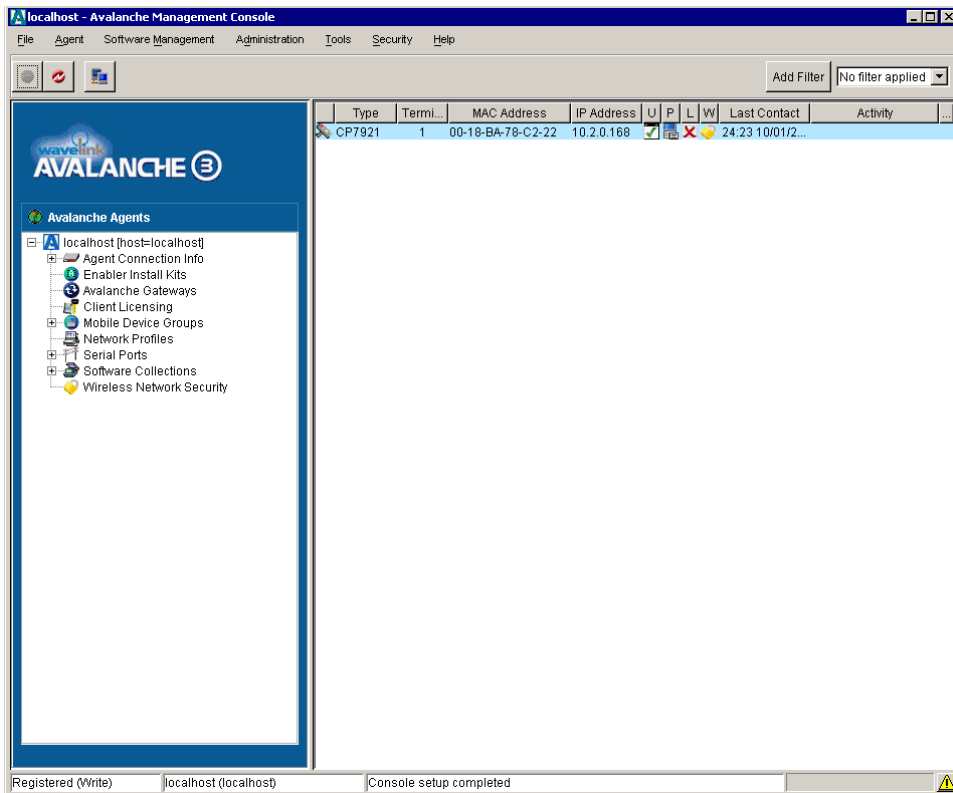
Wavelink Settings	
Server Enabled	<input checked="" type="radio"/> True <input type="radio"/> False
Enabler Version	3.11-01
<input checked="" type="radio"/> Obtain Server address automatically	
<input type="radio"/> Use the following Server	
IP Address	<input type="text" value="0.0.0.0"/>
Wavelink Custom Parameters	
<b>Parameter 1</b>	
Name	<input type="text" value="Building"/>
Value	<input type="text" value="SJ-21"/>
<b>Parameter 2</b>	
Name	<input type="text" value="City"/>
Value	<input type="text" value="Milpitas"/>
<b>Parameter 3</b>	
Name	<input type="text" value="State"/>
Value	<input type="text" value="CA"/>
<b>Parameter 4</b>	
Name	<input type="text" value="Country"/>
Value	<input type="text" value="US"/>

Save

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

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

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



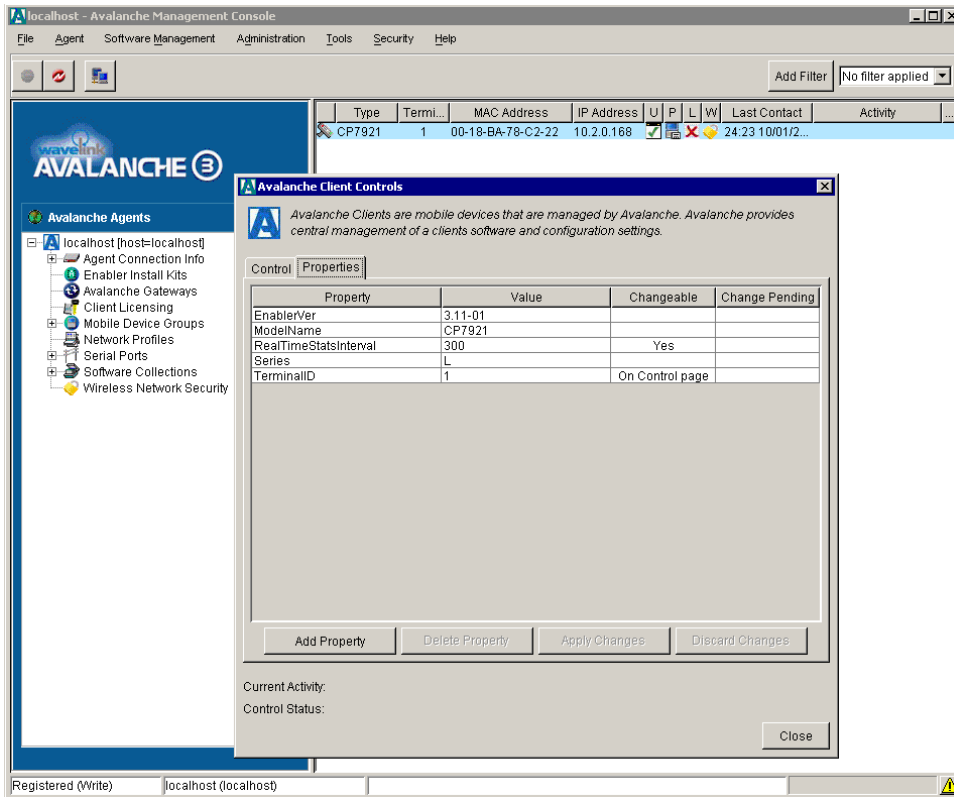
The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will have parameters enabled by default.

EnablerVer = 3.11-01

ModelName = CP7925G

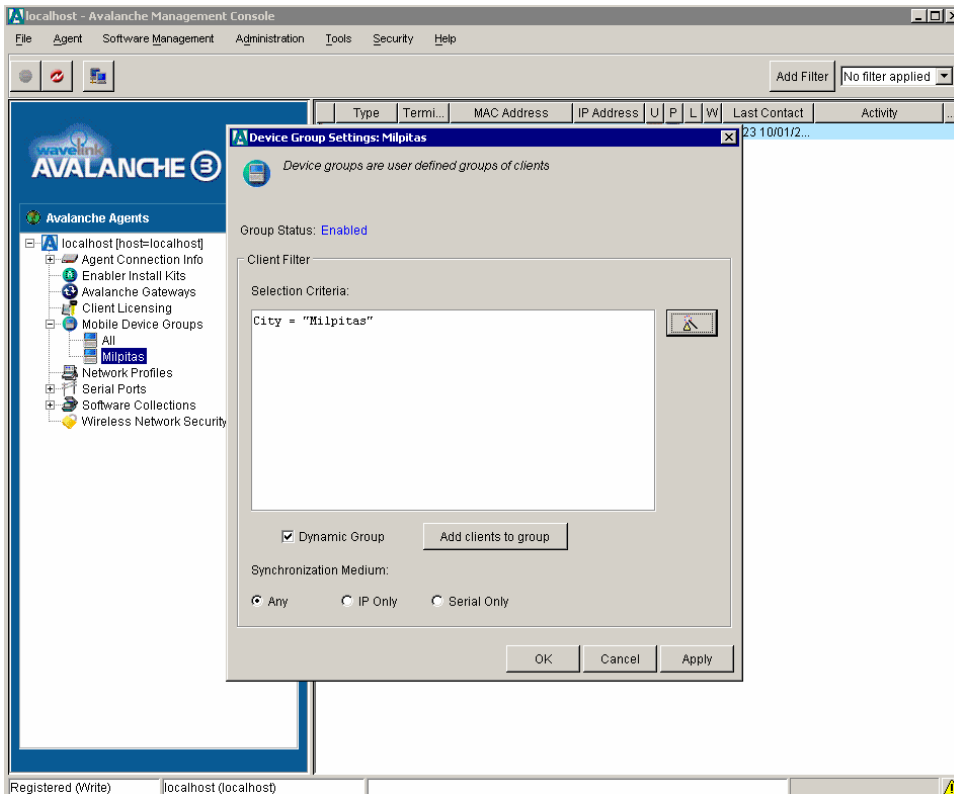
Additional properties can be added as necessary for better client management.





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.

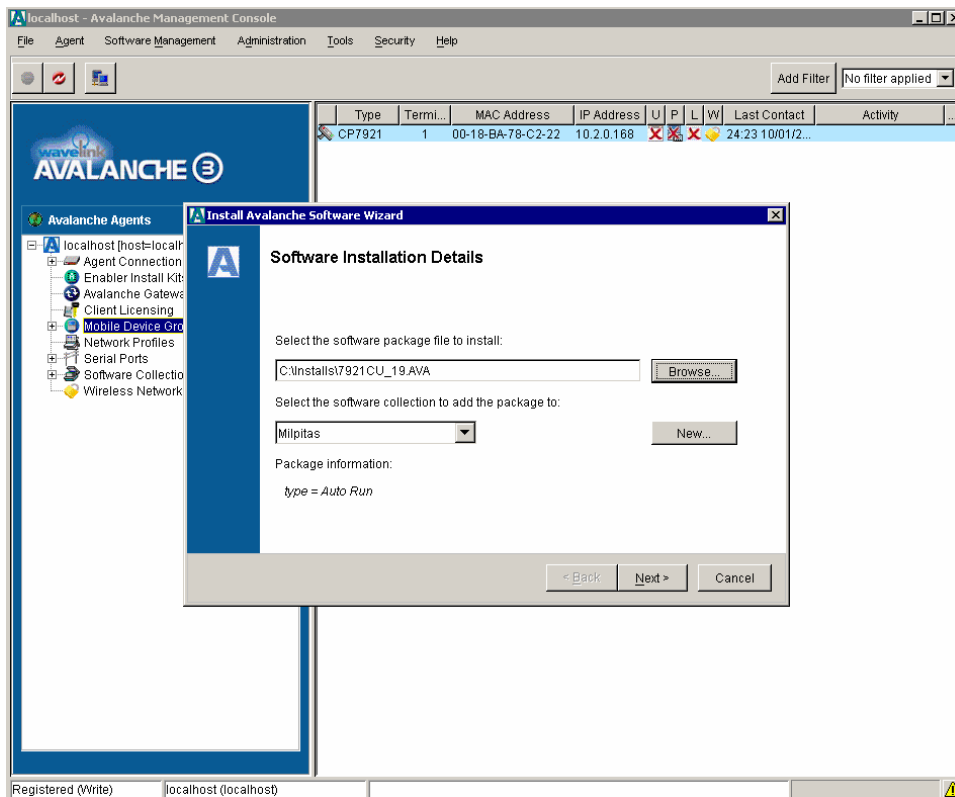
Browse to the 7925G Configuration Utility package file (e.g. 7925CU-1.3.1.AVA).

Create a software collection to add the package to.

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

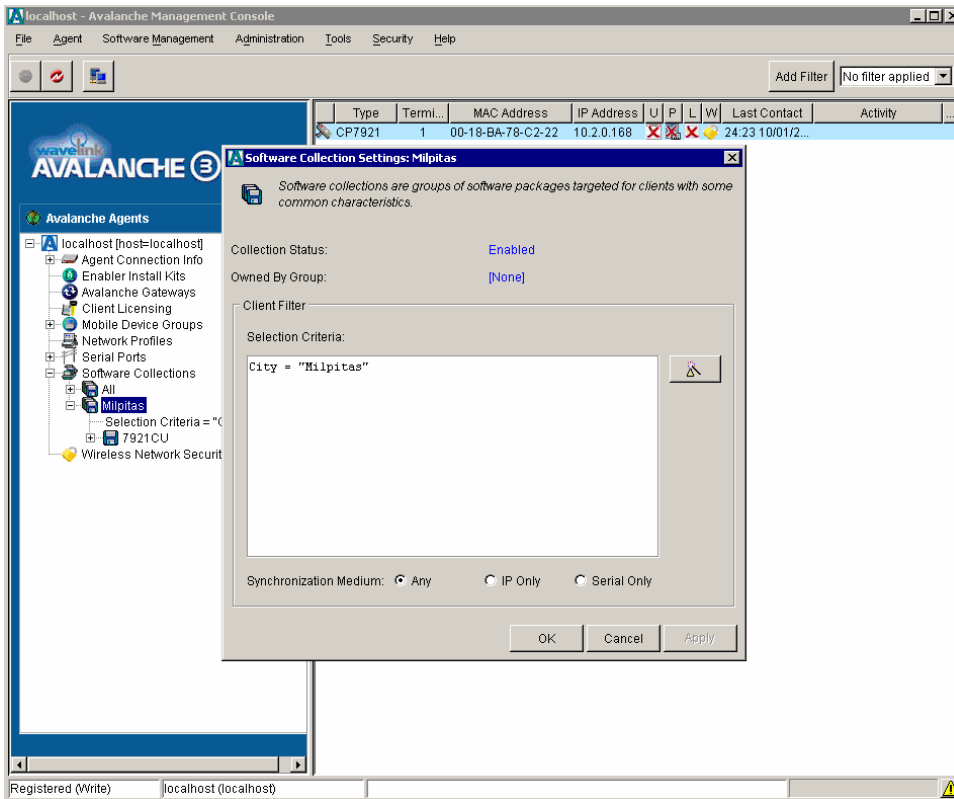
Click on **Finish** when the installation is complete.

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

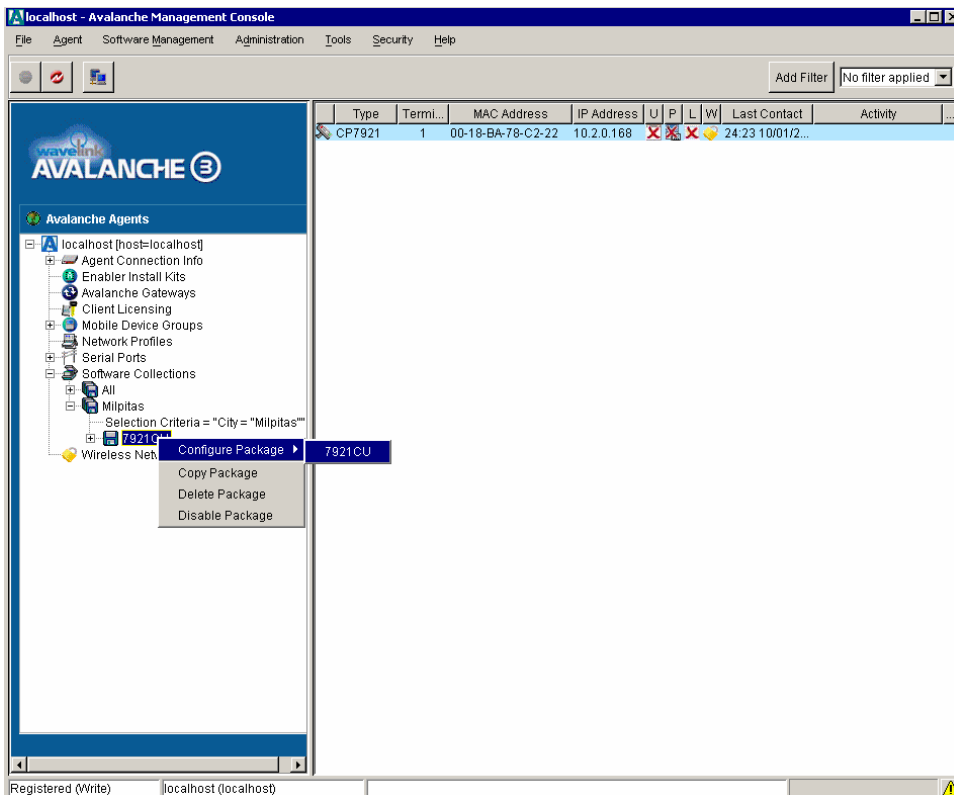


The software package must then be enabled by right clicking on the package and selecting **Enable Package**.

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



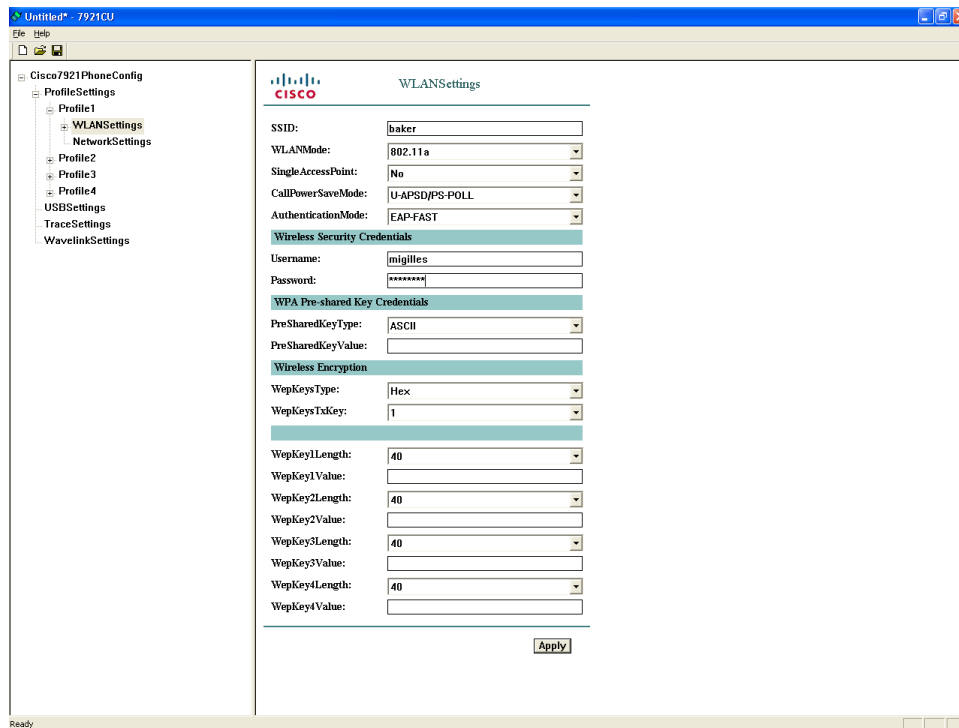
To configure the software package, right click on the package and select **7921CU**.  
The 7925G Configuration Utility will then be launched.



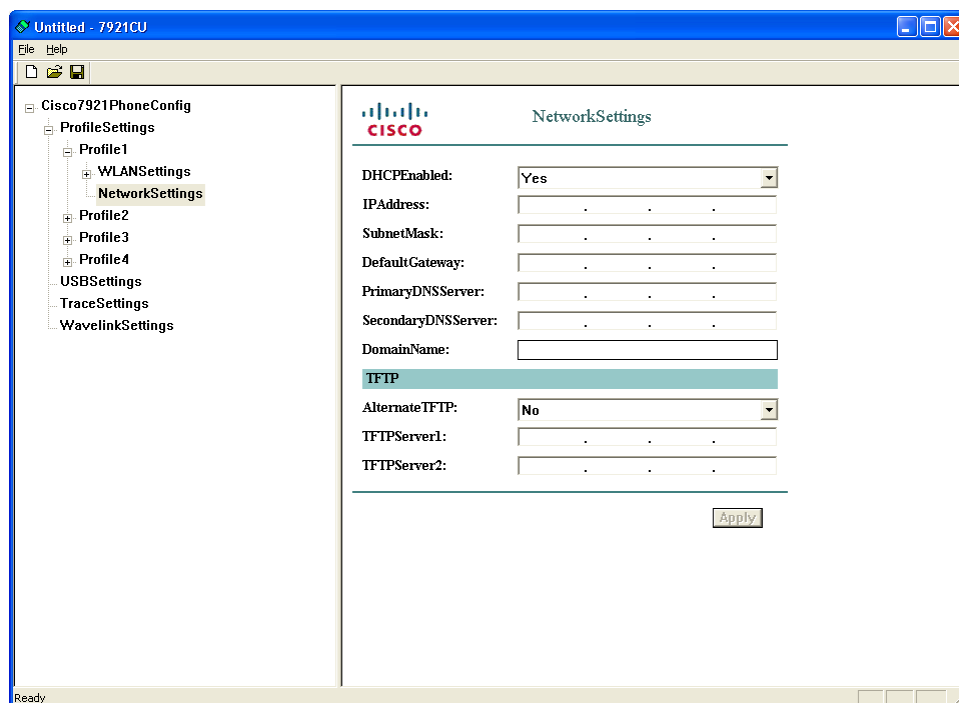
Enter the profile name and enable the profile.

Configure the network profiles by specifying the Wireless LAN credentials.

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

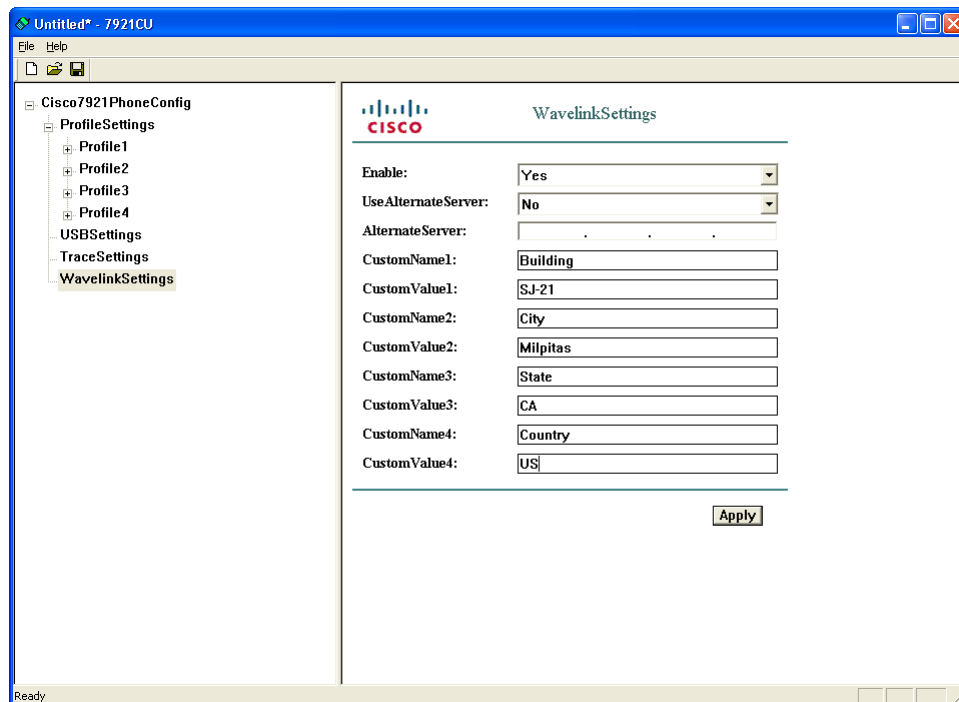


Configure the network settings for the network profile.



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 Bulk Deployment Utility

The Bulk Deployment Utility (BDU) for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G is intended to help quicken the provisioning and deployment process of many phones when unique 802.1x accounts are used with EAP-FAST, PEAP (MS-CHAPv2) or LEAP or if a common set of credentials are used by all phones (e.g. WPA2-PSK or a common 802.1x account).

The utility allows the creation configuration files, which can be exported then enabled for TFTP download by the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

The Bulk Deployment Utility requires firmware 1.3(4) or later on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

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

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

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

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

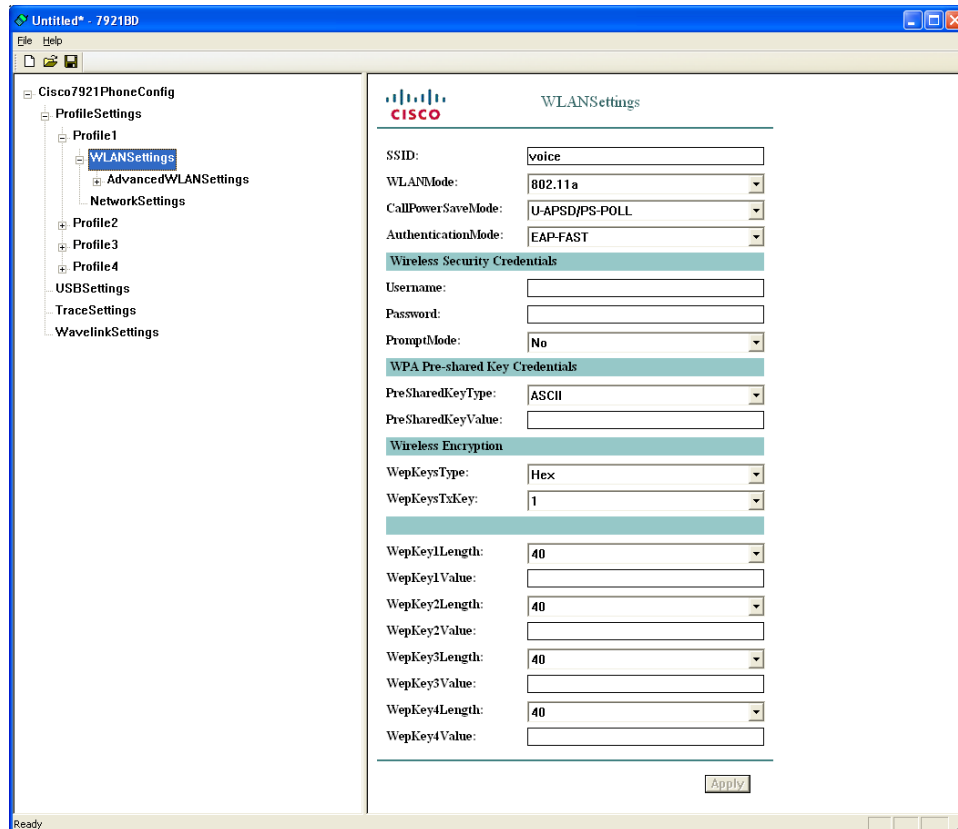
Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Deployment Guide

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

Configure the Profile Name as necessary.

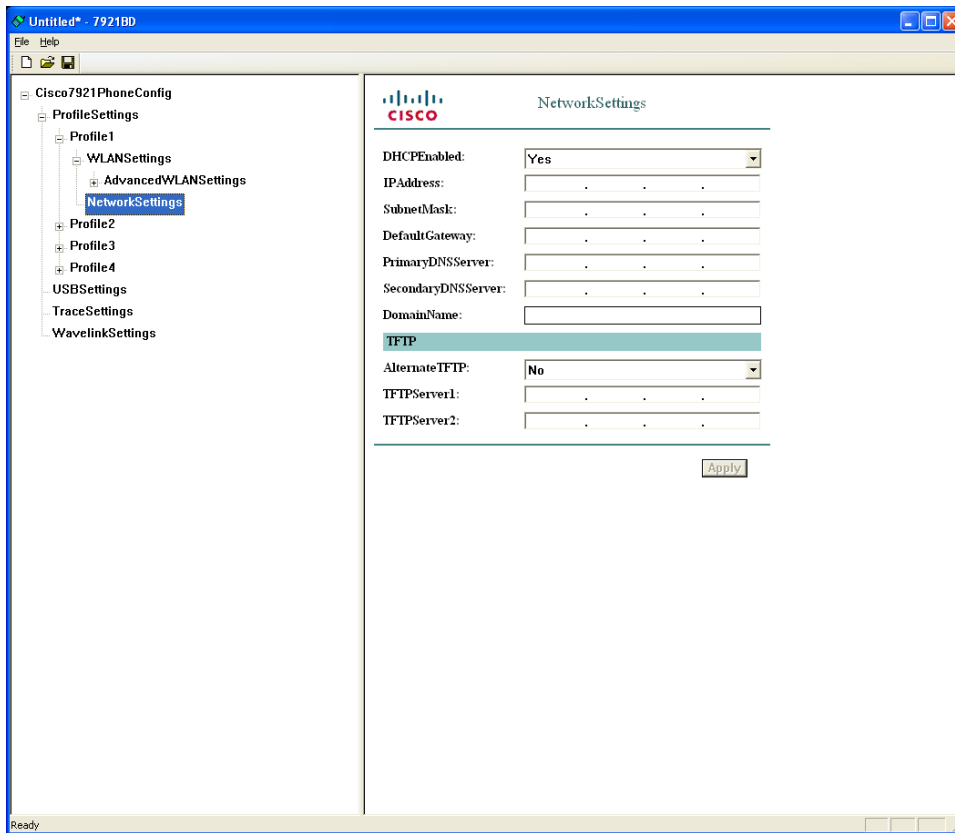
Configure the network profile WLAN settings (SSID, 802.11 mode, Security Mode, WLAN credentials) to match the WLAN that the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will utilize.

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



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

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



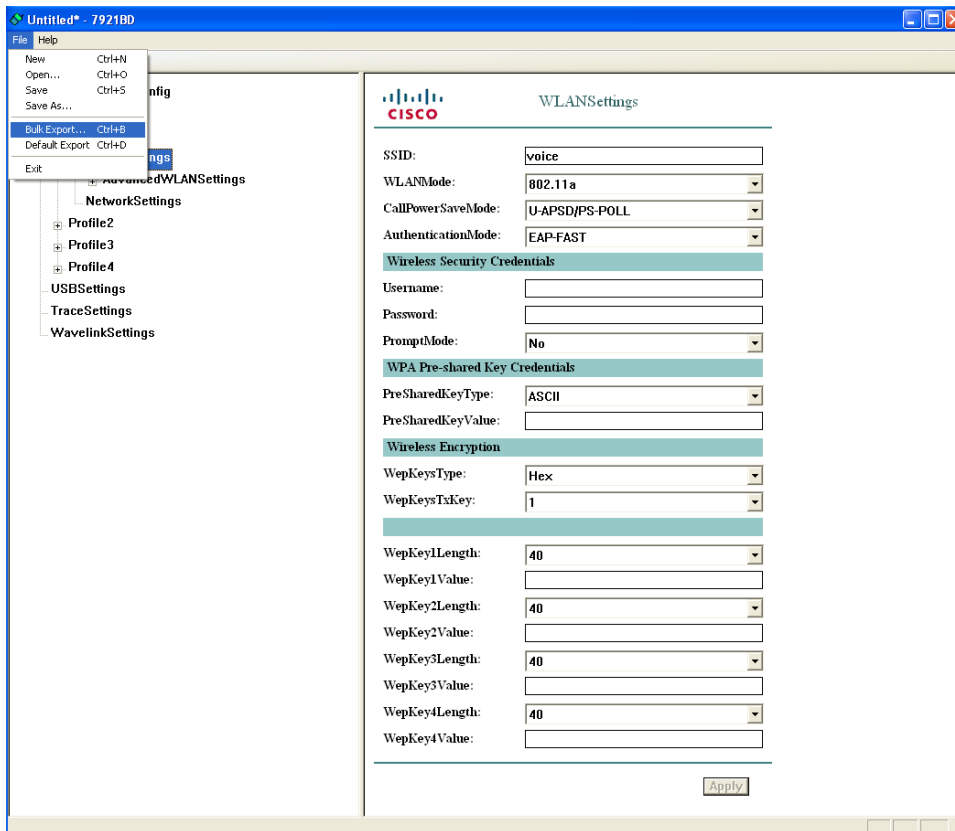
Templates can be created for later use, by selecting **File > Save As**.

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

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

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

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



## Default Export

If needing to deploy the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G with identical WLAN settings, then select the **Default Export** method.

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

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

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

## Bulk Export

If needing to deploy the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G with unique 802.1x accounts utilizing EAP-FAST, PEAP or LEAP, then select the **Bulk Export** method.

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

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

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

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

**MAC,Username,Password**



001e7abb19c8,admin,Cisco

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

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

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

## Pushing Configuration Files to the Cisco 792xG

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

For pre-deployment, it is recommended to install the TFTP server on the same system where the Bulk Deployment Utility is installed and have a staging environment setup with the default phone credentials in order for the phone to auto-download the configuration files by simply powering on the phones.

The staging environment setup, would need to have a single access point with the SSID **cisco** where the security mode is set to **Open** authentication, and option 150 of the DHCP scope for the staging network to be configured to point to the TFTP server hosting the phone configuration files.

If using the Cisco Unified Communications Manager's TFTP server, for security purposes it is recommended to the configuration files from the server and restart the TFTP service even though these files are encrypted.

Once the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G gets its configuration file, it will then re-provision with the new settings and attempt to join the intended WLAN based on the new credentials received.

The [Bulk Deployment Utility](http://www.cisco.com/cisco/software/navigator.html?mdfid=278875240) is available for download at the following URL.

<http://www.cisco.com/cisco/software/navigator.html?mdfid=278875240>

## Local Phone Book and Speed Dials

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G contains local phone book and speed dials support.

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

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

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

The local phone book and speed dials can be configured via the local keypad or via the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G web interface. Since the user does not manage the web password, the web interface is primarily intended for use by the system administrator, where they can upload information into the phone book for the user. This requires that the **Phone Book Web Access** product specific configuration item be set to **Allow Admin** as well as web access set to **Full**.



## Cisco Unified Wireless IP Phone 7925G

SEP0013E0A0C587

Phone DN 89023675

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

### Phone Book (New Contact)

Name Information

**First Name**

**Last Name**

**Nickname**

**Company Name**

Phone Information **Primary#** **Speed Dial#**

<b>Work Number</b>	<input type="text"/>	<input checked="" type="radio"/>	<input type="text"/>	
<b>Home Number</b>	<input type="text"/>	<input type="radio"/>	<input type="text"/>	
<b>Mobile Number</b>	<input type="text"/>	<input type="radio"/>	<input type="text"/>	
<b>Other Number</b>	<input type="text"/>	<input type="radio"/>	<input type="text"/>	

Contact Information

**Email Address**

**IM Address**

Mailing Address

**Street Number**

**City**

**State/Province**

**ZIP/Postal Code**

**Country**

Reset Save Cancel

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

Exported phone book data 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.



## Cisco Unified Wireless IP Phone 7925G

SEP0013E0A0C587

Phone DN 89023675

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

### Phone Book (Import & Export)

Import Contact Info to Phone

Import from File:

DELETE ALL current Contacts before Importing

DELETE ONLY the current Contact if matched

MERGE current Contact info with Importing data

Matching Contacts:

Using Unique Identifier (UID) value

Using Name fields

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

Export Contact Info to File

Create File of Type:

XML Phone Book format

Comma Separated Values (CSV) format

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

## Increased Font

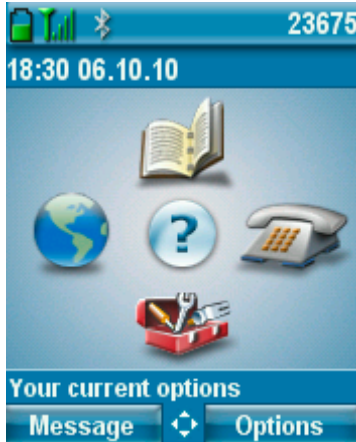
As of the 1.4(1) release, there are options for **Default** (original) font or **Increased** font.

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

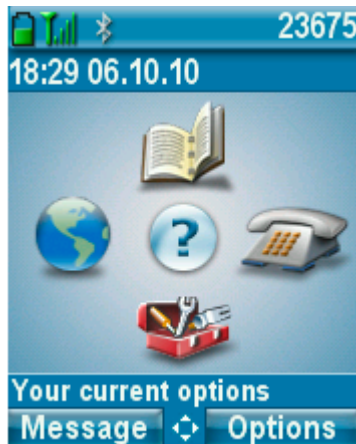
**Settings > Phone Settings > Display Settings > Font Size**



### Default Font



### Increased Font



## Using the Cisco Unified IP Phone 7925G Desktop Charger

The Cisco Unified IP Phone 7925G Desktop Charger is a single phone charger including a Bluetooth speakerphone and supports the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G running firmware version 1.4(1) or later.

When the Cisco Unified IP Phone 7925G, 7925G-EX, or 7926G is paired to the Cisco Unified IP Phone 7925G Desktop Charger, the audio path will automatically switch to the Bluetooth speakerphone once the phone is docked. And when removed from the desktop charger, the audio path will return to the previously used audio path (e.g. handset or speakerphone mode).

The audio volume is controlled from the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G by pressing the volume up or volume down button located on the left side of the phone. Mute can also be initiated by pressing the Mute button on the left side of the phone.

The audio path is controlled from the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G by pressing and holding the button located on the right side of the phone.

There is a battery slot in the rear of the Cisco Unified IP Phone 7925G Desktop Charger, which can be utilized for charging a spare battery or even powering the desktop charger.

### Bluetooth Pairing

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G can be paired to the Cisco Unified IP Phone 7925G Desktop Charger by performing the following steps.

1. Connect the power supply to the Cisco Unified Desktop Charger.
2. Insert the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G into the Cisco Unified Desktop Charger.
3. Power on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G.
4. Press and hold the **Control** button on the right side of the desktop charger for 5 seconds.  
The Power/Bluetooth status LED begins to flash, which indicates that the desktop charger is now in pairing mode.
5. From the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, choose **Settings > Phone Settings > Bluetooth**.
6. If Bluetooth is **Disabled**, press **Select**, select **Enable**, and then press **Save**.
7. Select **Device List**, then press **Scan**, which will then list the available devices. To rescan, press **Rescan**.
8. Select **Cisco Dock 7900** and press **Pair**.
9. If prompted, enter **0000** for the passkey and press **Select** or choose **Options > OK**, and the pairing will be completed.
10. Press the **End** button on the phone to return to the main screen.

If paired successfully, then the Power/Bluetooth status LED will turn to solid blue.



## Docking

After inserting the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G into the Cisco Unified IP Phone 7925G Desktop Charger, the Power/Bluetooth status LED will begin to flash blue to indicate a Bluetooth connection attempt is being made.

After the Bluetooth connection is established, the Power/Bluetooth status LED will turn to solid blue.

If currently on a call when the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G is docked, there will be a small delay to switch the audio path to the desktop charger's Bluetooth speakerphone while the Bluetooth connection completes. The call will continue using the Cisco Unified IP Phone 7925G Desktop Charger's Bluetooth speakerphone after the Bluetooth connection is made.

When the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G is undocked, the Bluetooth connection will be disconnected and the phone will return to the previously used audio path (e.g. handset or speakerphone mode).

See the following links for more information on the Cisco Unified IP Phone 7925G Desktop Charger.

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cuipph/7925g\\_7925gEX\\_7926/8\\_0\\_1/english/user\\_guide/P256\\_BK\\_EBE22\\_FA\\_00\\_wireless-ip-phones-user-guide\\_chapter\\_01001.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7925g_7925gEX_7926/8_0_1/english/user_guide/P256_BK_EBE22_FA_00_wireless-ip-phones-user-guide_chapter_01001.html)

## Using Phone Designer

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

The Cisco Unified Wireless IP Phone 7925G and 7925G-EX is supported in Phone Designer version 7.1(3) and later.

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

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

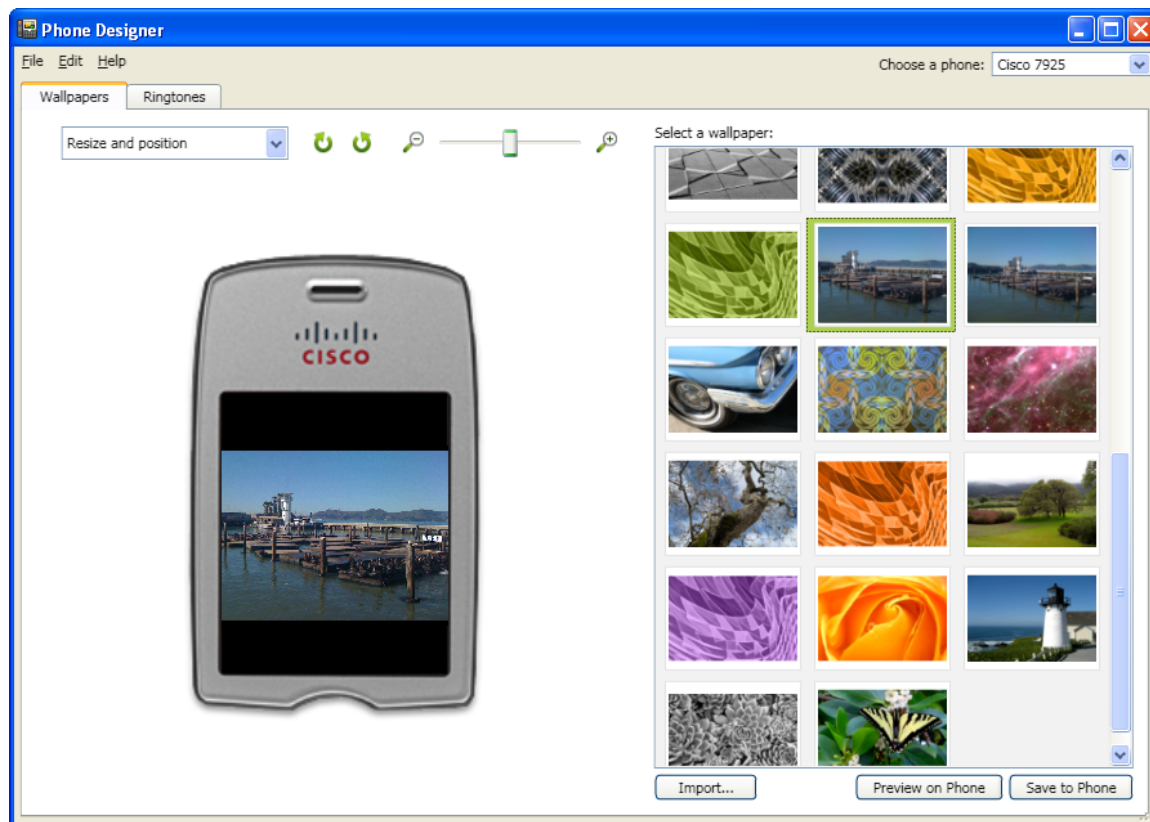
The user account must be created in the Cisco Unified Communications Manager and associated to the corresponding phone.

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

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

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

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

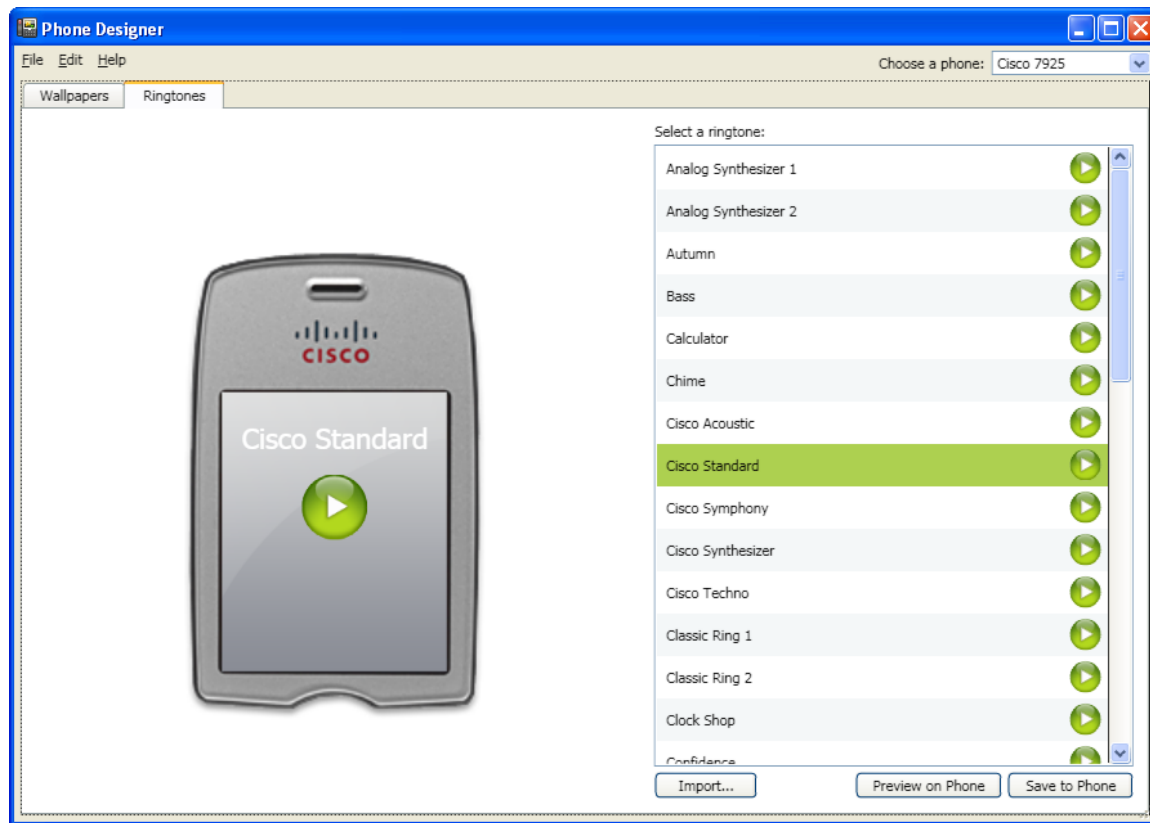


In order to configure the ringtone, either select a pre-defined ringtone or import a ringtone from the local computer by selecting **Import**.

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

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

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



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

<http://www.cisco.com/cisco/software/navigator.html?mdfid=278875240>

## Upgrading Firmware

There are two methods for upgrading the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G 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 4.3 or install the COP file for versions 5.1, 6.0, 6.1, 7.0, 7.1, 8.0, 8.5, 8.6, and later.

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

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Deployment Guide



[http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html)

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

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

The Load Server can be specified as an alternate TFTP server to retrieve firmware files in the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G 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.

#### **7925G Example:**

```
tftp-server flash: CP7925G-1.4.3.4.LOADS
tftp-server flash:APPSH-1.4.3.4.SBN
tftp-server flash:GUIH-1.4.3.4.SBN
tftp-server flash:JSYSH-1.4.3.4.SBN
tftp-server flash:JUIH-1.4.3.4.SBN
tftp-server flash:SYSH-1.4.3.4.SBN
tftp-server flash:TNUXH-1.4.3.4.SBN
tftp-server flash:TNUXRH-1.4.3.4.SBN
tftp-server flash:WLANH-1.4.3.4.SBN
!
telephony-service
load 7925 CP7925G-1.4.3.4.LOADS
```

#### **7926G Example:**

```
tftp-server flash: CP7926G-1.4.3.4.LOADS
tftp-server flash:APPSS-1.4.3.4.SBN
tftp-server flash:GUIS-1.4.3.4.SBN
tftp-server flash:JSYSS-1.4.3.4.SBN
tftp-server flash:JUIS-1.4.3.4.SBN
tftp-server flash:SYSS-1.4.3.4.SBN
tftp-server flash:TNUXS-1.4.3.4.SBN
tftp-server flash:TNUXRS-1.4.3.4.SBN
tftp-server flash:WLANS-1.4.3.4.SBN
tftp-server flash: EA15FW-BF3-220.SBN
!
telephony-service
load 7925 CP7926G-1.4.3.4.4.LOADS
```



## **Web Interface**

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

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

**Note:** If the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G registers to Cisco Unified Communications Manager, web access to the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G gets set to read-only mode by default. In this mode, firmware upgrades via the web interface are not allowed. Full web access must be enabled in Cisco Unified Communications Manager in order to make changes.

Ultimately the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G will use what is set as the phone load in the Cisco Unified Communications Manager.

## **IP Phone Services**

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G are capable of supporting Extensible Markup Language (XML) applications as well as Java Mobile Information Device Profile (MIDP) applications.

Java MIDP support is included in the 1.4(1) release for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

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

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cucm/admin/8\\_6\\_1/ccmcfg/b06phsrvr.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_6_1/ccmcfg/b06phsrvr.html)

## **Extensible Markup Language (XML)**

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

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/products\\_programming\\_reference\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html)

Below are features that are unique to the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

### **Vibrate URI**

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cuipph/all\\_models/xsi/8\\_5\\_1/supporteduris.html#wp1052264](http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/all_models/xsi/8_5_1/supporteduris.html#wp1052264)

### **Device URI**

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cuipph/all\\_models/xsi/8\\_5\\_1/supporteduris.html#wp1078268](http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/all_models/xsi/8_5_1/supporteduris.html#wp1078268)

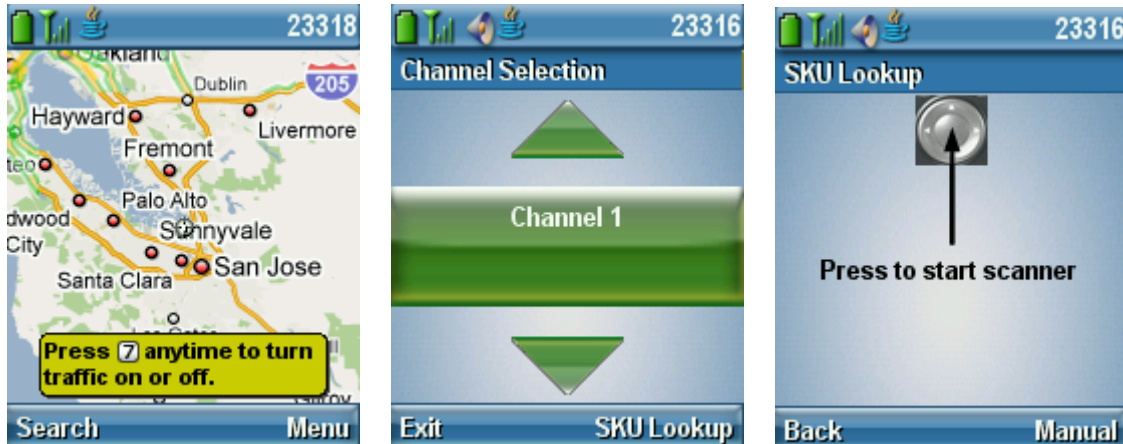
As of the 1.4(3) release, if a tone is pushed to the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G via XSI while on call, an alternate tone to the standard call waiting tone will be played so the user can distinguish the event type audibly.

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

## Java Mobile Information Device Profile (MIDP)

The following document provides the information needed for Java Mobile Information Device Profile (MIDP) programmers and system administrators to develop and deploy IP phone services.

<http://developer.cisco.com/web/jmapi/home>



## Troubleshooting

### Stream Statistics

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G provide 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.



## 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
<b>STREAM 1</b>
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

Stream Statistics			
RTP Statistics			
Domain Name	snmpUDPDomain	Remote Address	10.32.129.131
Remote Port	30162	Local Address	10.32.189.69
Local Port	18032	Sender Joins	1
Receiver Joins	1	Byes	0
Start Time	17:18:01	Row Status	Active
Host Name	SEP0013E0A0C587	Sender DSCP	EF
Sender Packets	1113	Sender Octets	191436
Sender Tool	G.711u	Sender Reports	5
Sender Report Time	17:18:23	Sender Start Time	17:18:01
Receiver DSCP (Previous, Current)	EF, EF	Receiver Packets	1087
Receiver Octets	173920	Receiver Tool	G.711u
Receiver Lost Packets	0	Receiver Jitter	2
Receiver Reports	0	Receiver Start Time	17:18:02
Voice Quality Metrics			
MOS LQK	4.5000	Avg MOS LQK	4.5000
Min MOS LQK	4.5000	Max MOS LQK	4.5000
MOS LQK Version	0.95	Cumulative Conceal Ratio	0.0000
Interval Conceal Ratio	0.0000	Max Conceal Ratio	0.0000
Conceal Seconds	0	Severly Conceal Seconds	0

Refresh Stop

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

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, 7925G-EX, and 7926G** chapter in the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Administration Guide at this URL:

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

# Network Statistics



## Cisco Unified Wireless IP Phone 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
<b>NETWORK</b>
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

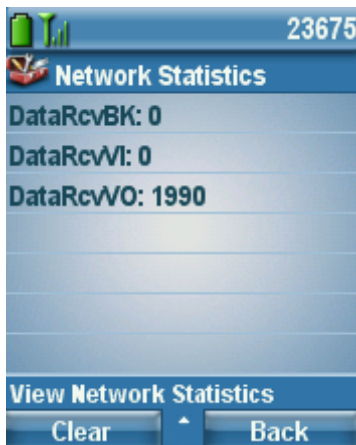
Network Statistics			
IP Statistics			
IpInReceives	4006	IpInHdrErrors	0
IpInAddrErrors	0	IpForwDatagrams	0
IpInUnknownProtos	0	IpInDiscards	0
IpInDelivers	3996	IpOutRequests	4408
IpOutDiscards	0	IpOutNoRoutes	0
IpReasmTimeout	0	IpReasmReqds	0
IpReasmOKs	0	IpReasmFails	0
IpFragOKs	0	IpFragFails	0
IpFragCreates	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			
UdplnDatagrams	3319	UdpNoPorts	0
UdplnErrors	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, 7925G-EX, and 7926G.



# 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
<b>WIRELESS LAN</b>
NETWORK
STREAM STATISTICS
STREAM 1
STREAM 2
SYSTEM
TRACE LOGS
BACKUP SETTINGS
PHONE UPGRADE
CHANGE PASSWORD
SITE SURVEY
DATE & TIME
PHONE RESTART

Wireless LAN Statistics			
<b>Rx Statistics</b>			
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		
<b>Tx Statistics (Best Effort)</b>			
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
<b>Tx Statistics (Voice)</b>			
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

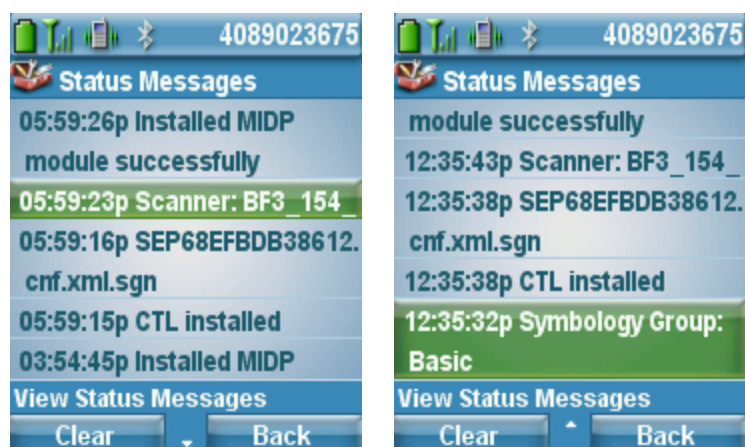
Copyright (c) 2006-2008 by Cisco Systems, Inc.

## 7926G Barcode Status Messages

Status messages on the Cisco Unified Wireless IP Phone 7926G provide information in regards to barcode scanner firmware installation, Java MIDP Add On Module (AOM) installation, and barcode scanner symbology group configuration events for the Cisco Unified Wireless Phone 7926G.

To view the status messages navigate to **Settings > Status > Status Messages**.

The barcode scanner firmware for the Cisco Unified Wireless IP Phone 7926G is included in the signed COP and ZIP files (scanner firmware is not included in the TAR file).



## Traffic Stream Metrics (TSM)

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

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

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

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

To view Traffic Stream Metrics data for a client, select TSM from the drop down menu for which frequency band the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G is using.

The Traffic Stream Metrics data entries will then be displayed.

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

Save Configuration

MONITOR | WLANS | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP

Monitor

- Summary
- ▶ Access Points
- ▶ Statistics
- ▶ CDP
- ▶ Rogues
- Clients
- Multicast

Clients > AP > Traffic Stream Metrics

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

**Uplink Statistics**

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

**Downlink Statistics**

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

## Phone Logs

Phone logs for troubleshooting purposes can be obtained from the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G web interface.

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

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



## Cisco Unified Wireless IP Phone 7925G

SEP002290EA9E64

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

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

Save

Copyright (c) 2006-2009 by Cisco Systems, Inc.

## Trace Modules

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



## Trace Levels

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

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

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

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

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

## Radio Status Indicator

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.



## Hardware Diagnostics

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

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

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

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

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

The scanner diagnostics will allow to scan a 2D barcode to ensure the scan engine is functional. A **Reset** option is available to reinitialize the barcode scanner.



## Firmware Recovery

If the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, or 7926G does not 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 simultaneously and keep it held until **Starting Recovery Mode** is displayed.
2. A firmware check will then be performed.
3. Insert the USB cable into the phone after USB initialization is complete.  
(Ensure that the USB driver has been installed prior and that an IP in the 192.168.1.0 /24 network has been configured for that network connection)
4. When **Web Access Available...** is displayed, then navigate to <http://192.168.1.100>.
5. Browse to the TAR file, then click on **Upload**.



## Cisco Unified Wireless IP Phone 7925G

Phone Recovery	
<b>Update Phone Software</b>	
Phone Software TAR File	<input type="text"/> <input type="button" value="Browse..."/>
	<input type="button" value="Upload"/>
<b>Device Information</b>	
System Load ID	CP7925G-1.3.3.LOADS *** Integrity Check Success ***
Version	V01
Serial Number	IAC1245A013
Model Number	CP-7925G
Hardware Revision	1.0
WLAN Regulatory Domain	0x1050
USB Vendor/Product ID	0x05A6 / 0x000A
USB RNDIS Device Address	002333309AF8
USB RNDIS Host Address	002333309AF9

## Restoring Factory Defaults

The configuration can be cleared by using the factory default menu option on the phone.

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

To erase the local configuration, follow these steps:

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

## Capturing a Screenshot of the Phone Display

The current display can be captured by browsing to <http://x.x.x.x/CGI/Screenshot>, where **x.x.x.x** is the IP address of the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G. At the prompt enter the username and password for the account for which the phone is associated to.

## Healthcare Environments

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

## Cleaning the Phone

The Cisco Unified Wireless IP Phone 7925G and 7926G are IP54 rated, which is designed to provide protection from dust, liquid splashes and moisture, where the Cisco Unified Wireless IP Phone 7925G-EX is IP64 rated for complete dust protection.

This allows the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G to be cleaned, sanitized without the possibility of damaging the unit.

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

## Accessories

The following accessories are available for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

For more information, refer to the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Accessories Guide at this URL:

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cuipph/7925g\\_7925gEX\\_7926/8\\_0\\_1/english/accessory\\_guide/P256\\_BK\\_W4FDAA91\\_00\\_wireless-ip-phone-accessories-guide.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7925g_7925gEX_7926/8_0_1/english/accessory_guide/P256_BK_W4FDAA91_00_wireless-ip-phone-accessories-guide.html)

- Cisco Unified IP Phone 7925G Desktop Charger
- Jawbone ICON for Cisco Bluetooth Headset
- Batteries (Standard and Extended)
- Carry Cases (Holster and Leather)
- Multi-Charger
- Lock Set
- USB Cable

For more information on the Cisco Unified IP Phone 7925G Desktop Charger, refer to the following URL:

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cuipph/7925g\\_7925gEX\\_7926/8\\_0/english/quick\\_start/7925Ch\\_qs.pdf](http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7925g_7925gEX_7926/8_0/english/quick_start/7925Ch_qs.pdf)

For more information on Jawbone ICON for Cisco Bluetooth Headset, refer to the following URL:

[http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps10655/ps11204/C78-615196-00\\_Jawbone\\_ICON\\_Cisco\\_Bluetooth\\_Headset\\_DS.pdf](http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps10655/ps11204/C78-615196-00_Jawbone_ICON_Cisco_Bluetooth_Headset_DS.pdf)



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

- Carry Cases [www.zcover.com](http://www.zcover.com)  
[www.systemwear.com](http://www.systemwear.com)
- Chargers [www.zcover.com](http://www.zcover.com)
- Headsets [www.plantronics.com](http://www.plantronics.com) (Quick Disconnect 2.5 mm Adapter – part # 65287-01)  
[www.jawbone.com](http://www.jawbone.com)  
[www.jabra.com](http://www.jabra.com)





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

The Cisco Unified Wireless IP Phone 7925G and 7925G-EX utilize the same accessories.

The batteries and chargers are the same for the 7925G, 7925G-EX, and 7926G, but have different cases.

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G has a 2.5 mm, 3 band / 4 conductor wired headset jack (Nokia compatible).

## Additional Documentation

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Data Sheets

[http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps9900/data\\_sheet\\_c78-504890.html](http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps9900/data_sheet_c78-504890.html)

[http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps10649/data\\_sheet\\_c78-565676.html](http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps10649/data_sheet_c78-565676.html)

[http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps11266/data\\_sheet\\_c78-649589.html](http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps11266/data_sheet_c78-649589.html)

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Administration Guide

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

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G User Guide and Quick Reference

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

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Accessory Guide

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cuipp/7925g\\_7925gEX\\_7926/8\\_0\\_1/english/accessory\\_guide/P256\\_BK\\_W4FDAA91\\_00\\_wireless-ip-phone-accessories-guide.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cuipp/7925g_7925gEX_7926/8_0_1/english/accessory_guide/P256_BK_W4FDAA91_00_wireless-ip-phone-accessories-guide.html)

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Release Notes

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

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Software

<http://www.cisco.com/cisco/software/type.html?mdfid=282359287>

<http://www.cisco.com/cisco/software/type.html?mdfid=283471435>

Cisco Unified Communications Manager

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

Cisco Unified Communications Manager Express

[http://www.cisco.com/en/US/partner/products/sw/voicesw/ps4625/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/partner/products/sw/voicesw/ps4625/tsd_products_support_series_home.html)

Cisco Voice Software

<http://www.cisco.com/cisco/software/navigator.html?mdfid=278875240>

Cisco Unified IP Phone Services Application Development Notes

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/products\\_programming\\_reference\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html)

Cisco Unified Communications SRND

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/products\\_implementation\\_design\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guides_list.html)

Mobility SRND

<http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html>

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Deployment Guide

Cisco Unified Wireless LAN Controller Documentation

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

Cisco Autonomous Access Point Documentation

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

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

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



---

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

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

© 2012 Cisco Systems, All rights reserved.



The Bluetooth word mark and logo are registered trademarks owned by Bluetooth SIG, Inc., and any use of such marks by Cisco Systems, Inc., is under license.