The Cisco Unified IP Phone 9971 is adaptable for professionals that require the ability to unplug the wired network connection and remain connected. The Wireless LAN and Bluetooth 2.1 + EDR capabilities enable mobility and cord-free communications. The Cisco Unified IP Phone 9971 supports both the headset and hands-free profiles.

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/17/09</td>
<td>9.0(1) Release</td>
</tr>
<tr>
<td>05/03/10</td>
<td>9.0(2) Release</td>
</tr>
<tr>
<td>12/15/10</td>
<td>9.1(1) Release</td>
</tr>
<tr>
<td>05/24/13</td>
<td>9.3(2) Release</td>
</tr>
<tr>
<td>08/20/13</td>
<td>9.3(4) Release</td>
</tr>
<tr>
<td>04/19/14</td>
<td>9.4(1) Release</td>
</tr>
<tr>
<td>07/16/14</td>
<td>9.4(1)SR1 Release</td>
</tr>
</tbody>
</table>
Contents

Cisco Unified IP Phone 9971 Overview ..................................................................................6

Requirements ..........................................................................................................................6
  Site Survey ..............................................................................................................................6
  RF Validation ..........................................................................................................................6
  Call Control ............................................................................................................................8
  Protocols ................................................................................................................................8
  Access Points ..........................................................................................................................9
  Antennas ................................................................................................................................11

Models ......................................................................................................................................11
  World Mode (802.11d) .........................................................................................................12
  Radio Characteristics ............................................................................................................13
  Language Support ................................................................................................................14

Bluetooth ..................................................................................................................................14
  Bluetooth Profiles .................................................................................................................15
  Coexistence (802.11b/g + Bluetooth) .................................................................................15

Video Calls ...............................................................................................................................16

Security ....................................................................................................................................17
  Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling (EAP-FAST) .............................................................................................................................17
  Fast Secure Roaming (FSR) ....................................................................................................19
  EAP and User Database Compatibility ................................................................................19

Power Management ................................................................................................................20
  Delivery Traffic Indicator Message (DTIM) ...........................................................................20

Quality of Service (QoS) .........................................................................................................20
  Configuring QoS in Cisco Unified Communications Manager ..............................................21
  Configuring QoS Policies for the Network ............................................................................21
    Configuring Cisco Switch Ports ............................................................................................21
    Configuring Cisco IOS Access Points ..................................................................................22
    Configuring Switch Ports for Wired IP Phones ....................................................................22
    Sample Voice Packet Capture ............................................................................................23
  Call Admission Control .......................................................................................................23
    Pre-Call Admission Control ...............................................................................................24
    Roaming Admission Control ..............................................................................................24
  Traffic Classification (TCLAS) ..............................................................................................24

Roaming ....................................................................................................................................25
  Interband Roaming ................................................................................................................26

Multicast ...................................................................................................................................26
Designing the Wireless LAN

Planning Channel Usage ........................................................................................................... 26
5 GHz (802.11a).......................................................................................................................... 26
Using Dynamic Frequency Selection (DFS) on Access Points................................................. 27
2.4 GHz (802.11b/g).................................................................................................................... 28
Signal Strength and Coverage ...................................................................................................... 29

Configuring Data Rates ............................................................................................................... 32
Call Capacity ............................................................................................................................... 33
Video Calls ................................................................................................................................ 33

Dynamic Transmit Power Control (DTPC) ................................................................................ 34
Rugged Environments ................................................................................................................. 34
Multipath .................................................................................................................................. 35

Verification with Site Survey Tools .......................................................................................... 36
Cisco 9971 Site Survey .............................................................................................................. 37

Configuring Cisco Unified Communications Manager ............................................................. 39

Phone Button Templates .......................................................................................................... 39

Security Profiles .......................................................................................................................... 40
G.722 and iSAC Advertisement .................................................................................................. 41

Common Settings ....................................................................................................................... 42
Audio and Video Bit Rates .......................................................................................................... 42

Configuring Video and Camera Capabilities .......................................................................... 43

Product Specific Configuration Options .................................................................................... 44

Configuring the Cisco Unified Wireless LAN Controller and Access Points .......................... 56

SSID / WLAN Settings .............................................................................................................. 57

Controller Settings .................................................................................................................... 62

802.11 Network Settings .......................................................................................................... 64
Beamforming (ClientLink) .......................................................................................................... 65
Auto RF (RRM) .......................................................................................................................... 66
Client Roaming ........................................................................................................................... 68
Call Admission Control ............................................................................................................ 68
EDCA Parameters ..................................................................................................................... 72
DFS (802.11h) ........................................................................................................................... 72
CleanAir ..................................................................................................................................... 73

AP Groups ................................................................................................................................ 74

RF Profiles ................................................................................................................................. 75

FlexConnect Groups .................................................................................................................. 77

Multicast Direct ........................................................................................................................ 77

QoS Profiles ............................................................................................................................... 78

QoS Basic Service Set (QBSS) .................................................................................................. 82

CCKM Timestamp Tolerance .................................................................................................... 83

Auto-Immune ............................................................................................................................ 84

WLAN Controller Advanced EAP Settings ............................................................................. 85

Proxy ARP ................................................................................................................................. 86

TKIP Countermeasure Holdoff Time ......................................................................................... 86
VLANs and Cisco Autonomous Access Points .................................................. 87

Configuring the Cisco Unified IP Phone 9971 .................................................. 87
  Wireless LAN Settings ..................................................................................... 87
  Bluetooth Settings ......................................................................................... 89
  Camera Settings for Video Calls ..................................................................... 91
  Upgrading Firmware ....................................................................................... 92

Troubleshooting ................................................................................................. 93
  Device Information .......................................................................................... 93
  Network Setup ................................................................................................. 94
  Current Access Point ....................................................................................... 95
  WLAN Statistics ............................................................................................. 97
  Streaming Statistics ....................................................................................... 97
  Device Logs ..................................................................................................... 98
  Traffic Stream Metrics (TSM) .......................................................................... 99
  WLAN Signal Indicator .................................................................................. 100
  WLAN Disconnect Display ............................................................................. 101
  Restoring Factory Defaults ........................................................................... 101
  Capturing a Screenshot of the Phone Display ................................................ 101

Healthcare Environments .................................................................................. 101

Accessories ....................................................................................................... 101

Additional Documentation ............................................................................... 103
Cisco Unified IP Phone 9971 Overview

The Cisco Unified IP Phone 9971 is the platform that provides communication within enterprises. The levels of voice quality performance that have come to be expected from Cisco products are maintained in the Cisco Unified IP Phone 9971 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 IP Phone 9971 in order to take advantage of the 802.11a data rates available. Despite the optimizations that Cisco have implemented in the Cisco Unified IP Phone 9971, 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 Unified IP Phone 9971 is not intended as a medical device and should not be used to make clinical decisions.

Requirements

The Cisco Unified IP Phone 9971 is an IEEE 802.11a/b/g device that provides voice and video communications. The wireless LAN must be validated to ensure it meets the requirements to deploy the Cisco Unified IP Phone 9971.

Site Survey

Before deploying the Cisco Unified IP Phone 9971 into a production environment, a site survey must be completed by a Cisco certified partner with the advanced wireless LAN specialization. During the site survey the RF spectrum can be analyzed to determine which channels are usable in the desired band (2.4 GHz or 5 GHz). Typically there is less interference in the 5 GHz band as well as more non-overlapping channels, so 5 GHz is the preferred band for operation and even more highly recommended when the Cisco Unified IP Phone 9971 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 which access point platform type, antenna type, access point configuration (channel and transmit power) to use at the location. It is recommended to select an access point with integrated antennas for non-rugged environments (e.g. office, healthcare, education, hospitality) and an access point platform requiring external antennas for rugged environments (e.g. manufacturing, warehouse, retail).

See the Designing the Wireless LAN for Voice section for more information.

Refer to the Steps to Success website for additional information.

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

RF Validation

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

Signal

The cell edge should be designed to -67 dBm where there is a 20-30% overlap of adjacent access points at that signal level.
This ensures that the Cisco Unified IP Phone 9971 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 IP Phone 9971 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 IP Phone 9971 can hold a signal for at least 5 seconds.

**Channel Utilization**

Channel Utilization levels should be kept under 50%.

If using the Cisco Unified IP Phone 9971, this is provided via the QoS Basic Service Set (QBSS), which equates to around 105.

The Cisco Unified IP Phone 9971 converts the 0-255 scale to a percentage, so 105 would equate to around 40% in the Cisco Unified IP Phone 9971 current access point menu.

**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 IP Phone 9971 meets 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  
- Cisco Wireless Control System (WCS) for Unified Wireless LAN Management  
- Cisco Wireless LAN Solution Engine (WLSE) for Cisco Autonomous Wireless LAN Management  
- Cisco Spectrum Expert  
- Cisco Unified Operations Manager  
• AirMagnet (Survey, WiFi Analyzer, VoFi Analyzer, Spectrum Analyzer)
  http://www.airmagnet.com

Call Control
The Cisco Unified IP Phone 9971 utilizes Session Initiation Protocol (SIP) for call control with the following applications.

• Cisco Unified Communications Manager (CUCM)
  Minimum = 7.1(3)
  Recommended = 8.6 and later
• Cisco Unified Communications Manager Express (CUCME)
  Minimum = 8.6
  Recommended = 8.6 and later
• Cisco Unified Survivable Remote Site Telephony (SRST)
  Minimum = 8.6
  Recommended = 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 IP Phone 9971 device support.
Device packages for Cisco Unified Communications Manager are available at the following location.

Protocols
Supported voice and wireless LAN protocols include the following:

• CCX v4
• Wi-Fi MultiMedia (WMM)
• Traffic Specification (TSPEC)
• Traffic Classification (TCLAS)
• Session Initiation Protocol (SIP)
• Real Time Protocol (RTP)
• G.722, G.711, iLBC, G.729
• Real Time Control Protocol (RTCP)
• Cisco Discovery Protocol (CDP)
Access Points

The Cisco Unified IP Phone 9971 is supported on both the Cisco Unified and Cisco Autonomous solutions.

Below is the supported version information for each Cisco solution.

- **Cisco Unified Wireless LAN Controller**
  
  Minimum = 6.0.202.0 (7.0.116.0 and 7.0.230 are not supported)
  
  Recommended = 7.0.250.0, 7.4.121.0, 7.6.120.0

- **Cisco IOS Access Points (Autonomous)**
  
  Minimum = 12.4(21a)JY
  
  Recommended = 12.4(25d)JA2, 15.2(4)JA1

The supported access point models are listed below.

![Access Points Image]

**Note:** The Cisco Unified IP Phone 9971 is supported with the Cisco AP3600 when the internal 802.11abgn radio is utilized, however if the 802.11ac module (AIR-RM3000AC) for the Cisco AP3600 is installed, then Cisco Unified Wireless LAN Controller release 7.6.100.0 or later is required.
The table below lists the modes that are supported by each Cisco Access Point.

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

**Note:** VoWLAN is not currently supported in conjunction with outdoor MESH technology (1500 series).
Limited support is provided when using 3rd party access points as there are no interoperability tests performed for 3rd party access points.
However the user should have basic functionality when connected to a Wi-Fi compliant access point.
Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide
Some of the key features are the following:

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

Cisco Unified IP Phone 9971 can take advantage of Cisco Client Extensions (CCX) enabled access points.

Some of the key features are the following:

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

Antennas

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

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

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

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

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


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

Models

There a few different Cisco Unified IP Phone 9971 models which the color (black or white) or handset type (standard and slimline) can vary.

All models require an 802.11d enabled access point if planning to utilize Wi-Fi.

The following Cisco Unified IP Phone 9971 models are available.

Below outlines the modes, frequency ranges and channels supported by each model.
A power cube (CP-PWR-CUBE-4=) is required when utilizing the Cisco Unified IP Phone 9971 in Wi-Fi mode.

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

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

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

### World Mode (802.11d)

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

If using the Cisco Unified IP Phone 9971, then it is required to enable 802.11d. The Cisco Unified IP Phone 9971 uses 802.11d to determine which 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 IP Phone 9971 will passively scan DFS channels first before engaging in active scans of those channels. If using 2.4 GHz (802.11b/g) and 802.11d is not enabled, then the Cisco Unified IP Phone 9971 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:

```bash
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 IP Phone 9971.

- Argentina (AR)
- India (IN)
- Poland (PL)
### Radio Characteristics

The following table lists the data rates, ranges, and receiver sensitivity info for Cisco Unified IP Phone 9971.

<table>
<thead>
<tr>
<th>5 GHz - 802.11a</th>
<th>Data Rate</th>
<th>Modulation</th>
<th>Range</th>
<th>Receiver Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Tx Power = 16 dBm</td>
<td>6 Mbps</td>
<td>OFDM - BPSK</td>
<td>604 ft (184 m)</td>
<td>-91 dBm</td>
</tr>
<tr>
<td></td>
<td>9 Mbps</td>
<td>OFDM - BPSK</td>
<td>604 ft (184 m)</td>
<td>-90 dBm</td>
</tr>
<tr>
<td></td>
<td>12 Mbps</td>
<td>OFDM - QPSK</td>
<td>551 ft (168 m)</td>
<td>-88 dBm</td>
</tr>
<tr>
<td></td>
<td>18 Mbps</td>
<td>OFDM - QPSK</td>
<td>545 ft (166 m)</td>
<td>-86 dBm</td>
</tr>
<tr>
<td></td>
<td>24 Mbps</td>
<td>OFDM - 16 QAM</td>
<td>512 ft (156 m)</td>
<td>-82 dBm</td>
</tr>
<tr>
<td></td>
<td>36 Mbps</td>
<td>OFDM - 16 QAM</td>
<td>420 ft (128 m)</td>
<td>-80 dBm</td>
</tr>
<tr>
<td></td>
<td>48 Mbps</td>
<td>OFDM - 64 QAM</td>
<td>322 ft (98 m)</td>
<td>-77 dBm</td>
</tr>
<tr>
<td></td>
<td>54 Mbps</td>
<td>OFDM - 64 QAM</td>
<td>289 ft (88 m)</td>
<td>-75 dBm</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.4 GHz - 802.11g</th>
<th>Data Rate</th>
<th>Modulation</th>
<th>Range</th>
<th>Receiver Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Tx Power = 16 dBm</td>
<td>6 Mbps</td>
<td>OFDM - BPSK</td>
<td>709 ft (216 m)</td>
<td>-91 dBm</td>
</tr>
<tr>
<td></td>
<td>9 Mbps</td>
<td>OFDM - BPSK</td>
<td>650 ft (198 m)</td>
<td>-90 dBm</td>
</tr>
<tr>
<td></td>
<td>12 Mbps</td>
<td>OFDM - QPSK</td>
<td>623 ft (190 m)</td>
<td>-87 dBm</td>
</tr>
<tr>
<td></td>
<td>18 Mbps</td>
<td>OFDM - QPSK</td>
<td>623 ft (190 m)</td>
<td>-86 dBm</td>
</tr>
</tbody>
</table>

**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)
24 Mbps | OFDM - 16 QAM | 623 ft (190 m) | -82 dBm
36 Mbps | OFDM - 16 QAM | 495 ft (151 m) | -80 dBm
48 Mbps | OFDM - 64 QAM | 413 ft (126 m) | -77 dBm
54 Mbps | OFDM - 64 QAM | 394 ft (120 m) | -76 dBm

**Note:** Receiver sensitivity is the minimum signal needed to decode a packet at a certain data rate.
The above values are pure radio specifications and do not account for the gain of the single integrated antenna.
See the [Designing the Wireless LAN for Voice](#) section for more information on signal requirements.

### Language Support

The Cisco Unified IP Phone 9971 currently supports the following languages.

<table>
<thead>
<tr>
<th>Arabic</th>
<th>French</th>
<th>Polish</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulgarian</td>
<td>German</td>
<td>Portuguese</td>
</tr>
<tr>
<td>Catalan</td>
<td>Greek</td>
<td>Romanian</td>
</tr>
<tr>
<td>Chinese</td>
<td>Hebrew</td>
<td>Russian</td>
</tr>
<tr>
<td>Croatian</td>
<td>Hungarian</td>
<td>Serbian</td>
</tr>
<tr>
<td>Czech</td>
<td>Italian</td>
<td>Slovak</td>
</tr>
<tr>
<td>Danish</td>
<td>Japanese</td>
<td>Slovenian</td>
</tr>
<tr>
<td>Dutch</td>
<td>Korean</td>
<td>Spanish</td>
</tr>
<tr>
<td>English</td>
<td>Latvian</td>
<td>Swedish</td>
</tr>
<tr>
<td>Estonian</td>
<td>Lithuanian</td>
<td>Thai</td>
</tr>
<tr>
<td>Finnish</td>
<td>Norwegian</td>
<td>Turkish</td>
</tr>
</tbody>
</table>

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

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

### Bluetooth

The Cisco Unified IP Phone 9971 supports Bluetooth 2.1 + 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 IP Phone 9971.
Up to ten headsets can be paired, where the previously connected headset is given priority. 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 IP Phone 9971 supports 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.

**Voice Quality**
Depending on the current data rate configuration, CTS may be sent to protect the Bluetooth transmissions when using Coexistence. In some environments, 6 Mbps may need to be enabled.

**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.

**Video Calls**

As of the 9.0(2) release, the Cisco Unified IP Phone 9971 supports video calling. The Cisco Unified IP Phone 9971 has a 5.6-inch 24 bit touchscreen color LCD.

In order to enable the video and camera capabilities, a device package or update for the Cisco Unified Communications Manager must be applied.

The USB camera that attaches to the back of the Cisco Unified IP Phone 9971 or 9951 is also required to transmit video. 360p is the recommended video format to utilize.

For remote users, 360p should be the maximum video resolution enabled in the Cisco Unified IP Phone 9971 endpoint configuration within Cisco Unified Communications Manager.

A Videoconferencing System with MCU running version 5.7 or later is required to provide videoconferencing capabilities. H.264 is the protocol used for the video stream, where up to 30 fps (frames per second) are supported.

There is a separate stream for the audio session that utilizes one of the support audio codecs. RTCP in the Cisco Unified IP Phone 9971 configuration within Cisco Unified Communications Manager should be enabled to help sync the audio and video streams.

The following frame formats are supported:

- QCIF (176 x 144)
- CIF (352 x 288)
- 360p (640 x 360)
- VGA (640 x 480)
Security

When deploying a wireless LAN, security is essential. The Cisco Unified IP Phone 9971 supports the following wireless security features.

**WLAN Authentication**
- WPA (802.1x authentication + TKIP or AES encryption)
- WPA2 (802.1x authentication + AES or TKIP encryption)
- WPA-PSK (Pre-Shared key + TKIP encryption)
- WPA2-PSK (Pre-Shared key + AES encryption)
- EAP-FAST (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling)
- 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 IP Phone 9971 also supports the following additional security features.
- 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)

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

Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling (EAP-FAST) encrypts EAP transactions within a Transport Level Security (TLS) tunnel between the access point and the Remote Authentication Dial-in User Service (RADIUS) server such as the Cisco Access Control Server (ACS).
The TLS tunnel uses Protected Access Credentials (PACs) for authentication between the client (phone) and the RADIUS server. The server sends an Authority ID (AID) to the client (Cisco Unified IP Phone 9971), which in turn selects the appropriate PAC. The client (phone) returns a PAC-Opaque to the RADIUS server. The server decrypts the PAC with its master-key. Both endpoints now have the PAC key and a TLS tunnel is created. EAP-FAST supports automatic PAC provisioning, but it must enabled on the RADIUS server.

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

The Cisco Unified IP Phone 9971 currently supports automatic provisioning of the PAC only, so enable **Allow anonymous in-band PAC provisioning** on the RADIUS server as shown below.

Both EAP-GTC and EAP-Mschapv2 must be enabled when **Allow anonymous in-band PAC provisioning** is enabled.

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

If anonymous PAC provisioning is not allowed in the production wireless LAN environment then a staging Cisco ACS can be setup for initial PAC provisioning of the Cisco Unified IP Phone 9971.

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 IP Phone 9971 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 IP Phone 9971 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.
Fast Secure Roaming (FSR)

CCKM is the recommended deployment model for all environment types where frequent roaming occurs. CCKM enables fast secure roaming and limits the off-network time to keep audio gaps at a minimum when on call. 802.1x authentication is required in order to utilize CCKM.

802.1x without CCKM can introduce delay during roaming due to its requirement for full re-authentication. WPA and WPA2 introduce additional transient keys and can lengthen roaming time. CCKM centralizes the key management and reduces the number of key exchanges.

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

As of the 9.1(1) release, the Cisco Unified IP Phone 9971 supports CCKM with WPA2 (AES or TKIP), WPA (TKIP or AES) and 802.1x (WEP) authentication, where WPA2 (AES) with CCKM is recommended.

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Key Management</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP-FAST</td>
<td>802.1x, WPA, WPA2</td>
<td>AES, TKIP, WEP (40/64 or 104/128 bit)</td>
</tr>
<tr>
<td>LEAP</td>
<td>802.1x, WPA, WPA2</td>
<td>AES, TKIP, WEP (40/64 or 104/128 bit)</td>
</tr>
<tr>
<td>AKM</td>
<td>802.1x, WPA, WPA2</td>
<td>AES, TKIP, WEP (40/64 or 104/128 bit)</td>
</tr>
</tbody>
</table>

CCKM was not supported with WPA2 in releases prior to 9.1(1).

<table>
<thead>
<tr>
<th>WPA Version</th>
<th>Cipher</th>
<th>Prior to 9.1(1)</th>
<th>9.1(1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPA</td>
<td>TKIP</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>AES</td>
<td>Not Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>WPA2</td>
<td>TKIP</td>
<td>Not Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>AES</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

EAP and User Database Compatibility

The following chart displays the EAP and database configurations supported by the Cisco Unified IP Phone 9971.

<table>
<thead>
<tr>
<th>Database Type</th>
<th>LEAP</th>
<th>EAP-FAST (Phase Zero)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ACS</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows SAM</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows AD</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>LDAP</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ODBC (ACS for Windows Only)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>LEAP Proxy RADIUS Server</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>All Token Servers</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Power Management**

The Cisco Unified IP Phone 9971 primarily is in active mode, so the radio will always be on. However, power save protocols such as U-APSD or PS-POLL can be utilized for off-channel scanning or when using Coexistence (802.11b/g + Bluetooth).

An AC adapter is required to use the 9971 in wireless LAN mode.

Wireless LAN is automatically disabled temporarily when Ethernet is connected, but will be automatically re-enabled once Ethernet is disconnected if Wireless LAN was enabled previously.

**Delivery Traffic Indicator Message (DTIM)**

It is recommended to set the DTIM period to 2 with a beacon period of 100 ms.

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.

**Quality of Service (QoS)**

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

To enable proper queuing for voice, interactive video, 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, interactive video, and call control traffic.

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>DSCP</th>
<th>802.1p</th>
<th>WMM UP</th>
<th>Port Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>EF (46)</td>
<td>5</td>
<td>6</td>
<td>UDP 16384 - 32767</td>
</tr>
<tr>
<td>Interactive Video &amp; Audio for Video Calls</td>
<td>AF41 (34)</td>
<td>4</td>
<td>5</td>
<td>UDP 16384 - 32767</td>
</tr>
<tr>
<td>Call Control</td>
<td>CS3 (24)</td>
<td>3</td>
<td>4</td>
<td>TCP 5060 - 5061</td>
</tr>
</tbody>
</table>

- Be sure that voice, interactive video, and call control packets have the proper QoS markings and other protocols are not using the same QoS markings.
• Select the **Platinum** QoS profile for the WLAN when using Cisco Unified Wireless LAN Controller technology and set the 802.1p tag to 5.

• Enable Differentiated Services Code Point (DSCP) preservation on the Cisco IOS switch.

**Note:** Voice and interactive video frames will be marked with DSCP AF41 and WMM UP 5 for video calls.

For more information about TCP and UDP ports used by the Cisco Unified IP Phone 9971 and the Cisco Unified Communications Manager, refer to the Cisco Unified Communications Manager TCP and UDP Port Usage document at this URL:


### Configuring QoS in Cisco Unified Communications Manager

The SIP 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 SIP packets as shown in the Enterprise Parameters Configuration page.

#### Enterprise Parameters Configuration

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster ID</td>
<td>StandAloneCluster</td>
</tr>
<tr>
<td>Synchronization Between Auto Device Profile and Phone Configuration</td>
<td>True</td>
</tr>
<tr>
<td>Max Number of Device Level Trace</td>
<td>12</td>
</tr>
<tr>
<td><strong>DSCP for Phone-based Services</strong></td>
<td>default DSCP (000000)</td>
</tr>
<tr>
<td>DSCP for Phone Configuration</td>
<td>CS3(precedence 3) DSCP (011000)</td>
</tr>
<tr>
<td>DSCP for Cisco CallManager to Device Interface</td>
<td>CS3(precedence 3) DSCP (011000)</td>
</tr>
<tr>
<td>Connection Monitor Duration</td>
<td>120</td>
</tr>
<tr>
<td>Auto Registration Phone Protocol</td>
<td>SCCP</td>
</tr>
<tr>
<td>BLF Call Lists</td>
<td>Disabled</td>
</tr>
<tr>
<td>Advertise G.722 Codec</td>
<td>Enabled</td>
</tr>
<tr>
<td>Phone Personalization</td>
<td>Disabled</td>
</tr>
<tr>
<td>Services Provisioning</td>
<td>Internal</td>
</tr>
<tr>
<td>Feature Control Policy</td>
<td>&lt; None &gt;</td>
</tr>
</tbody>
</table>

### Configuring QoS Policies for the Network

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

### Configuring Cisco Switch Ports

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

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

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

Configure the Cisco Access Point switch ports as well as any uplink switch ports for trust DSCP.
Below is a sample switch configuration for an access point:

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

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

### Configuring Cisco IOS Access Points

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

```
class-map match-all Voice
  match ip dscp ef
class-map match-all Video
  match ip dscp af41
class-map match-all CallControl
  match ip dscp cs3
!
policy-map 9971
  class Voice
    set cos 6
  class Video
    set cos 5
  class CallControl
    set cos 4
!
interface dot11radioX
  service-policy input 9971
  service-policy output 9971
```

### 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
```
Sample Voice Packet Capture

The packet capture below displays a voice packet bound for the Cisco Unified IP Phone 9971 over the air being marked as DSCP = EF and UP = 6.

Call Admission Control

Inbound and outbound call admission control can 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 Cisco Unified IP Phone 9971 will auto-negotiate the PHY rate to be used for TSPEC. By default it will try 12 Mbps, but if not enabled on the access point, then it will try the next highest enabled data rate on the access point.

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.

Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide
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 IP Phone 9971 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 IP Phone 9971 establishes the call.

If the access point rejects the call and the Cisco Unified IP Phone 9971 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 IP Phone 9971 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 IP Phone 9971 measures Received Signal Strength Indicator (RSSI) and Packet Error Rate (PER) values for the current and all available access points to make roaming decisions.

If the original access point where the call was established had Call Admission Control (TSPEC) enabled, then the Cisco Unified IP Phone 9971 will send an ADDTS request during the roam to the new access point, which embedded in the reassociation request frame.

**Note:** Call Admission Control for video is currently not supported.

**Traffic Classification (TCLAS)**

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

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

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

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

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

TCLAS is supported in the Cisco Unified Wireless LAN Controller release 5.1.151.0 and later.
Using port based QoS policies is inadequate as all data packets use the same UDP port (LWAPP = 12222; or CAPWAP = 5246) and the access point uses the outside QoS marking to determine which queue the packets should be placed in.

With TCLAS, DSCP preservation is not a requirement.

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

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

Roaming

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

802.1x authentication is required in order to utilize CCKM.

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

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

As of the 9.1(1) release, the Cisco Unified IP Phone 9971 supports CCKM with WPA2 (AES or TKIP), WPA (TKIP or AES) and 802.1x (WEP) authentication, where WPA2 (AES) with CCKM is recommended.

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Roaming Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPA/WPA2 Personal</td>
<td>150 ms</td>
</tr>
<tr>
<td>WPA/WPA2 Enterprise</td>
<td>300 ms</td>
</tr>
<tr>
<td>CCKM</td>
<td>&lt; 100 ms</td>
</tr>
</tbody>
</table>

The Cisco Unified IP Phone 9971 manages the scanning and roaming events; Client Roaming parameters in the Cisco Unified Wireless LAN Controller are not utilized.

Roaming can be triggered for either of the following reasons.

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

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

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

For seamless roaming to occur, the Cisco Unified IP Phone 9971 must be associated to an access point for at least 3 seconds, otherwise roams can occur based on packet loss (max tx retransmissions or missed beacons).

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

Note: The Cisco Unified IP Phone 9971 does not utilize the RF parameters in the Client Roaming section of the Cisco Unified Wireless LAN Controller as scanning and roaming is managed independently by the phone itself.
**Interband Roaming**

The Cisco Unified IP Phone 9971 defaults to Auto for the frequency band mode, which enables interband roaming and gives preference to 5 GHz over 2.4 GHz.

At power on, the Cisco Unified IP Phone 9971 will scan all 2.4 and 5 GHz channels when in Auto mode, then attempt to associate to an access point for the configured network if available.

If configured for 802.11a only (5 GHz) or 802.11b only (2.4 GHz) mode, then just those channels are scanned.

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

**Multicast**

When enabling multicast in the wireless LAN, performance and capacity must be considered.

The Cisco Unified IP Phone 9971 is a client that primarily utilizes active mode, but if there is an associated client that is in power save mode, then all multicast packets will be queued until the DTIM period.

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

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

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

The Cisco Unified IP Phone 9971 supports the IGMP query feature, which can be used to reduce the amount of multicast traffic on the wireless LAN when not necessary.

Ensure that IGMP snooping is also enabled on all switches.

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

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

**Designing the Wireless LAN**

The following network design guidelines must be followed in order to accommodate for adequate coverage, call capacity and seamless roaming for the Cisco Unified IP Phone 9971.

**Planning Channel Usage**

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

**5 GHz (802.11a)**

The Cisco Unified IP Phone 9971 supports Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) from 802.11h, which are required when using channels operating at 5.25 - 5.725 GHz, which are 15 of the 23 possible channels.

DFS dynamically instructs a transmitter to switch to another channel whenever radar signal is detected. If the access point detects radar, the radio on the access point goes on hold for at least 60 seconds while the access point passively scans for another usable channel.
TPC allows the client and access point to exchange information, so that the client can dynamically adjust the transmit power. The client uses only enough energy to maintain association to the access point at a given data rate. As a result, the client contributes less to adjacent cell interference, which allows for more densely deployed, high-performance wireless LANs.

5 GHz channels overlap their adjacent channel, so there should be at least 1 channel of separation for adjacent access points. Need to ensure there is at least 20 percent overlap with adjacent channels when deploying the Cisco Unified IP Phone 9971 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 IP Phone 9971 also meets the access point’s receiver sensitivity (required signal level for the current data rate).

### 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 IP Phone 9971 in the 802.11b/g environment, which allows for seamless roaming.

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

**Signal Strength and Coverage**

To ensure acceptable voice quality, the Cisco Unified IP Phone 9971 should always have a signal of -67 dBm or higher when using 2.4 GHz or 5 GHz, while the Cisco Unified IP Phone 9971 also meets the access point’s receiver sensitivity required signal level for the transmitted data rate.

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

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

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

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

Recommended to set the minimum data rate to 11 Mbps or 12 Mbps for 2.4 GHz (dependent upon 802.11b client support policy) and 12 Mbps for 5 GHz, which should also be the only rate configured as a mandatory / basic rate. In some environments, 6 Mbps may need to be enabled as a mandatory / basic rate.

Due to the above requirements, a single channel plan should not be deployed.
When designing the placement of access points, be sure that all key areas have sufficient coverage (signal).

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

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

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

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

However there are products that also utilize the non-licensed 5 GHz frequency (e.g. 5.8 GHz cordless phones, which can impact UNII-3 channels).
The Cisco Unified WCS or NCS can be utilized to verify signal strength and coverage.
Configuring Data Rates

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

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

When 802.11b clients exist in the wireless network, then an 802.11b rate must be enabled and only an 802.11b rate can be configured as a mandatory / basic rate.

The recommended data rate configurations are the following:

<table>
<thead>
<tr>
<th>802.11 Mode</th>
<th>Mandatory (Basic) Data Rates</th>
<th>Supported (Optional) Data Rates</th>
<th>Disabled Data Rates</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a</td>
<td>12 Mbps</td>
<td>18-24, &lt;36-54&gt; Mbps</td>
<td>6, 9, &lt;36-54&gt; Mbps</td>
</tr>
<tr>
<td>802.11b</td>
<td>11 Mbps</td>
<td>None</td>
<td>1, 2, 5.5 Mbps</td>
</tr>
<tr>
<td>802.11b/g</td>
<td>11 Mbps</td>
<td>12-24, &lt;36-54&gt; Mbps</td>
<td>1, 2, 5.5, 6, 9, &lt;36-54&gt; Mbps</td>
</tr>
<tr>
<td>802.11g</td>
<td>12 Mbps</td>
<td>18-24, &lt;36-54&gt; Mbps</td>
<td>1, 2, 5.5, 6, 9, 11, &lt;36-54&gt; Mbps</td>
</tr>
</tbody>
</table>

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

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

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

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

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

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

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

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

If Call Admission Control (TSPEC) is enabled then the Traffic Stream Rate Set (TSRS) feature will also be enabled, which can allow lower rates to be enabled for legacy devices, while preventing the Cisco Unified IP Phone 9971 from transmitting at rates below 12 Mbps for 802.11a and 11 Mbps for 802.11b/g as well as not above 24 Mbps if the Restricted Data Rates feature in Cisco Unified Communications Manager is enabled. Disallowing packets to be transmitted at lower rates preserves capacity. Sending voice frames at a more reliable rate (i.e. 24 Mbps) initially can potentially reduce the number of retries of a frame to ensure the packet transmission is successful on the first try.

See the Product Specific Configuration Options section for information on how to configure the Restrict Data Rates options on the Cisco Unified IP Phone 9971 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.

<table>
<thead>
<tr>
<th>Max # of Streams</th>
<th>802.11 Mode</th>
<th>Data Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>802.11a or 802.11g + Bluetooth Disabled</td>
<td>6 Mbps</td>
</tr>
<tr>
<td>20</td>
<td>802.11a or 802.11g + Bluetooth Disabled</td>
<td>12 Mbps</td>
</tr>
<tr>
<td>27</td>
<td>802.11a or 802.11g + Bluetooth Disabled</td>
<td>24-54 Mbps</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Max # of Streams</th>
<th>802.11 Mode</th>
<th>Data Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>802.11b/g + Bluetooth Enabled</td>
<td>11, &lt;12-54&gt; Mbps</td>
</tr>
<tr>
<td>7</td>
<td>802.11g + Bluetooth Enabled</td>
<td>12, &lt;18-54&gt; Mbps</td>
</tr>
</tbody>
</table>

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

Video Calls

Video calls over Wireless LAN will significantly reduce the potential call capacity.

Below lists the maximum number of video calls (single bi-directional voice and video stream) supported per access point / channel for each video bit rate.

If there are two Cisco Unified IP Phone 9971s communicating to each other, then that is two bi-directional voice and video streams.

<table>
<thead>
<tr>
<th>Max # of Video Calls</th>
<th>802.11 Mode</th>
<th>802.11 Data Rate</th>
<th>Audio Codec</th>
<th>Audio Bit Rate</th>
<th>Video Type</th>
<th>Video Resolution</th>
<th>Video Bit Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-10</td>
<td>802.11a or 802.11g + Bluetooth Disabled</td>
<td>12-54 Mbps</td>
<td>G.722 / G.711</td>
<td>64 Kbps</td>
<td>CIF</td>
<td>352 x 288</td>
<td>384 Kbps</td>
</tr>
<tr>
<td>3-7</td>
<td>802.11a or 802.11g + Bluetooth Disabled</td>
<td>12-54 Mbps</td>
<td>G.722 / G.711</td>
<td>64 Kbps</td>
<td>360p</td>
<td>640 x 360</td>
<td>512 Kbps</td>
</tr>
<tr>
<td>2-5</td>
<td>802.11a or 802.11g + Bluetooth Disabled</td>
<td>12-54 Mbps</td>
<td>G.722 / G.711</td>
<td>64 Kbps</td>
<td>VGA</td>
<td>640 x 480</td>
<td>1000 Kbps</td>
</tr>
</tbody>
</table>
Note: Currently no Call Admission Control support for video.

Dynamic Transmit Power Control (DTPC)

To ensure packets are exchanged successfully between the Cisco Unified IP Phone 9971 and the access point, Dynamic Transmit Power Control (DTPC) should be enabled.

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

If the access point does not support DTPC, then the Cisco Unified IP Phone 9971 will use the highest available transmit power depending on the current channel and data rate.

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

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

The access point’s radio transmit power should not have a transmit power greater than what the Cisco Unified IP Phone 9971 can support.

Rugged Environments

When deploying the Cisco Unified IP Phone 9971 in a rugged environment (e.g. manufacturing, warehouse, retail), additional tuning on top of the standard design recommendations may be necessary.

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

Access Point and Antenna Selection

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

Access Point Placement

It is crucial that line of sight to the access point’s antennas is maximized by minimizing any obstructions between the Cisco Unified IP Phone 9971 and the access point. Ensure that the access point and/or antennas are not mounted behind any obstruction or on or near a metal or glass surface.

If access points with integrated antennas (e.g. Cisco 1040, 1130, 1140, 1602i, 2602i, 3502i, 3602i, and 3702i Series Access Points) are to be used in some areas, then it is recommended to mount those access points on the ceiling as they have omni-directional antennas and are not designed to be patches.

Frequency Band

As always, it is recommended to use 5 GHz. Use of 2.4 GHz, especially when 802.11b rates are enabled, may not work well.

For the 5 GHz channel set, it is recommended to use a 8 or 12 channel plan only; disable UNII-2 extended channels if possible.

Data Rates

The standard recommended data rate set of 12-54 Mbps may not work well if multipath is present at an elevated level. Therefore, it is recommended to enable lower data rates (e.g. 6 Mbps) to operate better in such an environment.

If 5 GHz is used for VoWLAN only, then it is also recommended to disable data rates above 24 Mbps (i.e. 36, 48, 54 Mbps) to increase first transmission success (e.g. 6 as mandatory, 12 and 24 as supported). If 5 GHz is also used for data, video or other applications, then is suggested to keep the higher data rates enabled (e.g. 6 as mandatory, 9, 12-54 as supported).
Transmit Power
Due to the potential of elevated multipath in rugged environments, the transmit power of the access point and Cisco Unified IP Phone 9971 should also be restricted. This is more important if planning to deploy 2.4 GHz in a rugged environment. If using auto transmit power, the access point transmit power can be configured to use a specified range (maximum and minimum power levels) to prevent the access point from transmitting too hot as well as too weak (e.g. 5 GHz maximum of 16 dBm and minimum of 11 dBm).

The Cisco Unified IP Phone 9971 will utilize the access point’s current transmit power setting to determine what transmit power it uses for transmitted frames when DTPC is enabled in the access point’s configuration.

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

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

Beamforming
If using Cisco 802.11n access points, then Beamforming (ClientLink) should be enabled, which can help with client reception.

See the Beamforming (ClientLink) section in Configuring the Cisco Unified Wireless LAN Controller and Access Points for more information.

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

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

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

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

Below is a list of multipath effects:

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

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

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

Decreased Signal Amplitude
Occurs when the reflected waves arrive out of phase to some extent with the main signal thereby reducing the signal amplitude.
Use of Orthogonal Frequency Division Multiplexing (OFDM), which is used by 802.11a and 802.11g, can help to reduce issues seen in high multipath environments.

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

Use of antenna diversity can also help in such environments.

**Verification with Site Survey Tools**

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

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  
- Cisco Wireless Control System (WCS) for Unified Wireless LAN Management  
- Cisco Wireless LAN Solution Engine (WLSE) for Cisco Autonomous Wireless LAN Management  
- Cisco Spectrum Expert  
- Cisco Unified Operations Manager  
- AirMagnet (Survey, WiFi Analyzer, VoFi Analyzer, Spectrum Analyzer)  
  [http://www.aimagnet.com](http://www.aimagnet.com)
Cisco 9971 Site Survey

The Cisco Unified IP Phone 9971 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 Applications Button > Administrator Settings > Status > WLAN Site Survey.

To view the HTML report, select Device Logs > WLAN Site Survey from the Cisco Unified IP Phone 9971 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.
### Neighbor Table

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>sjc32-11a-ap9</th>
<th>sjc32-11a-ap11</th>
<th>sjc32-11a-ap10</th>
<th>sjc32-11a-ap12</th>
<th>sjc32-11a-ap1</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP:</td>
<td>sjc32-11a-ap9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC:</td>
<td>00:54:C4:D1:F5:38</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Observation Count:</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Channel - Frequency:</td>
<td>149 - 5745000hz</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Country:</td>
<td>US</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Beacon Interval:</td>
<td>102</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DTIM Period:</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSSI Range [dBm]:</td>
<td>[-55 -55]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BSSID Lost Count:</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Channel Utilization:</td>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Station Count:</td>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Available Admission Capacity:</td>
<td>23437</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Basic Rates:</td>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optional Rates:</td>
<td>18 24 36 48 54</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multicast Cipher:</td>
<td>CCMP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unicast Ciphers:</td>
<td>WPA2_CCMP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AKM:</td>
<td>WPA2_1X WPA2_CCKM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proxy ARP supported:</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WMM Supported:</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CCX Version Number:</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CCX Power Maximum in dBm:</td>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U-APSD Supported:</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Best Effort AC(0)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admission Control Required:</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIFS</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECWMin</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECWMax</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TXOpLimit</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Admission Control Required: No

### Background AC(1)

| AIFS | 12 | 8 | 10 | 0 |
| AIFS | 5 | 3 | 5 | 0 |

### Video AC(2)

### Voice AC(3)

| Channels | 36 | 40 | 44 | 48 | 52 | 56 | 60 | 64 | 68 | 72 | 76 | 80 | 84 | 88 | 92 | 96 | 100 | 104 | 108 | 112 | 116 | 120 | 124 | 128 | 132 | 136 | 140 | 144 | 148 | 152 | 156 | 160 | 164 |
|---------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|

*The beacon interval of 102 is not recommended, the recommended value is 100.*
Configuring Cisco Unified Communications Manager

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

When adding the Cisco Unified IP Phone 9971 to the Cisco Unified Communications Manager it must be provisioned using the Ethernet MAC address as the Wireless LAN MAC is used for Wi-Fi connectivity only.

The Ethernet MAC address can be found by navigating to Settings > Administration Settings > Network Setup > Ethernet Setup on the Cisco Unified IP Phone 9971.

Phone Button Templates

The Cisco Unified IP Phone 9971 supports 6 lines. The default phone button template includes support for 2 lines and 4 speed dials.

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

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

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

The Cisco Unified IP Phone 9971 has a Manufactured Installed Certificate (MIC), which can be utilized with a security profile as well.
G.722 and iSAC Advertisement

Cisco Unified Communications Manager supports the ability to configure whether G.722 is to be a supported codec system wide or not. G.722 can be disabled globally within Enterprise Parameters of Cisco Unified Communications Manager.

G.722 and iSAC codecs can be disabled at an individual phone level by setting Advertise G.722 and iSAC Codecs to Disabled.

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

Some settings such as Wireless LAN and Bluetooth can be configured on an enterprise phone, common phone profile or individual phone level.

Wireless LAN and Bluetooth are enabled by default.

Wireless LAN is automatically disabled temporarily when Ethernet is connected, but will be automatically re-enabled once Ethernet is disconnected if Wireless LAN was enabled previously.

Override common settings can be enabled at either configuration level.

Audio and Video Bit Rates

The audio and video 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.

By default the video call bit rate is set to 384 Kbps (CIF quality).

For typical deployments, it is recommended to utilize the 360p bit rate for the video stream.

For better video quality, set the video call bit rate to at least 480 Kbps to utilize VGA or 360p.

Use the following information to configure the audio bit rate to be used for audio or audio + video calls.

<table>
<thead>
<tr>
<th>Audio Codec</th>
<th>Audio Bit Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.722 / G.711</td>
<td>64 Kbps</td>
</tr>
<tr>
<td>iSAC</td>
<td>32 Kbps</td>
</tr>
<tr>
<td>iLBC</td>
<td>16 Kbps</td>
</tr>
<tr>
<td>G.729</td>
<td>8 Kbps</td>
</tr>
</tbody>
</table>

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

The value configured will determine the resolution of the transmitted video stream from the Cisco Unified IP Phone 9971.
The Cisco Unified IP Phone 9971 will be able to receive up to VGA video depending on the remote device’s capabilities, where the region settings configuration is factored in.

<table>
<thead>
<tr>
<th>Video Type</th>
<th>Video Resolution</th>
<th>Frames per Second (fps)</th>
<th>Video Bit Rate Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>QCIF</td>
<td>176 x 144</td>
<td>30</td>
<td>16-249 Kbps</td>
</tr>
<tr>
<td>CIF</td>
<td>352 x 288</td>
<td>30</td>
<td>250-399 Kbps</td>
</tr>
<tr>
<td>360p</td>
<td>640 x 360</td>
<td>30</td>
<td>400-999 Kbps</td>
</tr>
<tr>
<td>VGA</td>
<td>640 x 480</td>
<td>30</td>
<td>480-999 Kbps</td>
</tr>
</tbody>
</table>

**Configuring Video and Camera Capabilities**

In order for the Cisco Unified IP Phone 9951 or 9971 to send and receive video, that capability must be enabled in the Cisco Unified Communications Manager.

Set the **Video Capabilities** option to **Enabled** in the phone’s configuration within the Product Specific Configuration Layout section.

In order for the Cisco Unified IP Phone 9951 or 9971 to utilize the USB camera, it must be enabled in the Cisco Unified Communications Manager version 8.0.

Set the **Cisco Camera** option to **Enabled** in the phone’s configuration within the Product Specific Configuration Layout section.
Product Specific Configuration Options

In Cisco Unified Communications Manager Administration, the following configuration options are available for the Cisco Unified IP Phone 9971.

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

Product specific configuration options can be configured in bulk via the Bulk Admin Tool if using Cisco Unified Communications Manager.

Some of the product specific configuration options can be configured on an enterprise phone, common phone profile or individual phone configuration level.
<table>
<thead>
<tr>
<th>Param</th>
<th>Override Common Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC Port</td>
<td>Enabled</td>
</tr>
<tr>
<td>Back USB Port</td>
<td>Enabled</td>
</tr>
<tr>
<td>Side USB Port</td>
<td>Enabled</td>
</tr>
<tr>
<td>Cisco Camera</td>
<td>Disabled</td>
</tr>
<tr>
<td>Video Capabilities</td>
<td>Disabled</td>
</tr>
<tr>
<td>Enable/Disable USB Classes</td>
<td>Mass Storage Human Interface Device</td>
</tr>
<tr>
<td>SD/SDHC</td>
<td>Disabled</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>Enabled</td>
</tr>
<tr>
<td>Wii</td>
<td>Enabled</td>
</tr>
<tr>
<td>Bluetooth Profiles</td>
<td>Handset</td>
</tr>
<tr>
<td>Settings Access</td>
<td>Enabled</td>
</tr>
<tr>
<td>Gratuitous ARP</td>
<td>Disabled</td>
</tr>
<tr>
<td>PC Voice VLAN Access</td>
<td>Enabled</td>
</tr>
<tr>
<td>Web Access</td>
<td>Disabled</td>
</tr>
<tr>
<td>Show All Calls on Primary Line</td>
<td>Disabled</td>
</tr>
<tr>
<td>Days Display Not Active</td>
<td>Sunday Monday Tuesday</td>
</tr>
<tr>
<td>Display On Time</td>
<td>07:30</td>
</tr>
<tr>
<td>Display On Duration</td>
<td>13:30</td>
</tr>
<tr>
<td>Display Idle Timeout</td>
<td>01:30</td>
</tr>
<tr>
<td>HTTPS Server</td>
<td>http and https Enabled</td>
</tr>
<tr>
<td>Enable Power Save Plus</td>
<td>Sunday Monday Tuesday</td>
</tr>
<tr>
<td>Phone On Time</td>
<td>03:30</td>
</tr>
<tr>
<td>Phone Off Time</td>
<td>24:30</td>
</tr>
<tr>
<td>Phone Off Idle Timeout</td>
<td>60</td>
</tr>
<tr>
<td>Enable Audible Alert</td>
<td></td>
</tr>
<tr>
<td>EnergyWise Domain</td>
<td></td>
</tr>
<tr>
<td>EnergyWise Endpoint Security Secret</td>
<td></td>
</tr>
<tr>
<td>Allow EnergyWise Overrides</td>
<td></td>
</tr>
<tr>
<td>Span to PC Port</td>
<td>Disabled</td>
</tr>
<tr>
<td>Logging Display</td>
<td>Disabled</td>
</tr>
<tr>
<td>Load Server</td>
<td></td>
</tr>
<tr>
<td>Recording Tone</td>
<td>Disabled</td>
</tr>
<tr>
<td>Recording Tone Local Volume</td>
<td>130</td>
</tr>
<tr>
<td>Recording Tone Remote Volume</td>
<td>50</td>
</tr>
<tr>
<td>Recording Tone Duration</td>
<td></td>
</tr>
<tr>
<td>Display On When Incoming Call</td>
<td>Enabled</td>
</tr>
<tr>
<td>RTP</td>
<td>Disabled</td>
</tr>
<tr>
<td>Log Server</td>
<td></td>
</tr>
</tbody>
</table>
### Field Name | Description
--- | ---
Disable Speakerphone | Disable only the speakerphone functionality. Disabling speakerphone functionality will not affect the headset. You can use lines and speed dials with headset/handset.

Disable Speakerphone and Headset | Disable all speakerphone functions and headset microphone.

PC Port | Indicates whether the PC port on the phone is enabled or disabled. The port labeled "10/100 PC" on the back of the phone connects a PC or workstation to the phone so they can share a single network connection.

Back USB Port | Indicates whether the back USB port on the phone is enabled or disabled.

Side USB Port | Indicates whether the side USB port on the phone is enabled or disabled.

Cisco Camera | Indicates whether the Cisco Camera on the phone is enabled or disabled.

Video Capabilities | When enabled, indicates that the phone will participate in video calls.

Enable/Disable USB Classes | Indicates which USB Classes on the phone are enabled or disabled.

---

Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDIO</td>
<td>Indicates whether the SDIO device on the phone is enabled or disabled.</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>Indicates whether the Bluetooth device on the phone is enabled or disabled.</td>
</tr>
<tr>
<td>Wifi</td>
<td>Indicates whether the Wifi device on the phone is enabled or disabled.</td>
</tr>
<tr>
<td>Bluetooth Profiles</td>
<td>Indicates which Bluetooth profiles on the phone are enabled or disabled.</td>
</tr>
<tr>
<td>Settings Access</td>
<td>Indicates whether the Settings button on the phone is functional. When Settings Access is enabled, you can change the phone network configuration, ring type, and volume on the phone. When Settings Access is disabled, the Settings button is completely disabled; no options appear when you press the button. Also, you cannot adjust the ringer volume or save any volume settings. When Settings Access is restricted, you can only access User Preferences and volume settings. By default, Settings Access is enabled.</td>
</tr>
<tr>
<td>Gratuitous ARP</td>
<td>Indicates whether the phone will learn MAC addresses from Gratuitous ARP responses. Disabling the phones ability to accept Gratuitous ARP will prevent applications, which use this mechanism for monitoring and recording of voice streams from working. If monitoring capability is not desired, change this setting to Disabled.</td>
</tr>
<tr>
<td>PC Voice VLAN Access</td>
<td>Indicates whether the phone will allow a device attached to the PC port to access the Voice VLAN. Disabling Voice VLAN Access will prevent the attached PC from sending and receiving data on the Voice VLAN. It will also prevent the PC from receiving data sent and received by the phone. Set this setting to Enabled if an application is being run on the PC that requires monitoring of the phones traffic. These could include monitoring and recording applications and use of network monitoring software for analysis purposes.</td>
</tr>
<tr>
<td>Web Access</td>
<td>This parameter indicates whether the phone will accept connections from a web browser or other HTTP client. Disabling the web server functionality of the phone will block access to the phones internal web pages. These pages provide statistics and configuration information. Features, such as QRT (Quality Report Tool), will not function properly without access to the phones web pages. This setting will also affect any serviceability application such as CiscoWorks 2000 that relies on web access.</td>
</tr>
<tr>
<td>Show All Calls on Primary Line</td>
<td>When enabled, indicates that all calls presented to this device will be shown when the Primary line is selected.</td>
</tr>
<tr>
<td>Days Display Not Active</td>
<td>This field allows the user to specify the days that the backlight is to remain off by default. Typically this would be Saturday and Sunday for US corporate customers. Saturday and Sunday should be the default. The list contains all of the days of the week. To turn off backlight on Saturday and Sunday the User would hold down Control and select Saturday and Sunday.</td>
</tr>
<tr>
<td>Display On Time</td>
<td>This field indicates the time of day the display is to automatically turn itself on for days listed in the off schedule. The value should be in a 24 hour format. Where 0:00 is the beginning of the day and 23:59 is the end of the day. Leaving this field blank will activate the display at the default time of the day (e.g. - &quot;7:30&quot;). To set the display to turn on at 7:00AM the user would enter &quot;07:00&quot; without the quotes. If they wanted the display to turn on at 2:00PM they would enter &quot;14:00&quot; without the quotes.</td>
</tr>
<tr>
<td>Display On Duration</td>
<td>This field indicates the amount of time the display is to be active for when it is turned on by the programmed schedule. Leaving this field blank will make the phone use a pre-determined default value of &quot;10:30&quot;. Maximum value is 24 hours.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Display Idle Timeout</td>
<td>This field indicates how long to wait before the display is turned off when it was turned on by user activity. This inactivity timer will continually reset itself during user activity. Leaving this field blank will make the phone use a pre-determined default value of one hour. Maximum value is 24 hours. This value can be in free form hours and minutes. &quot;1:30&quot; would turn off the display after one hour and 30 minutes of inactivity.</td>
</tr>
<tr>
<td>HTTPS Server</td>
<td>Allows Administrator to permit http and https or https only connections if Web Access is enabled.</td>
</tr>
<tr>
<td>Enable Power Save Plus</td>
<td>To enable the Power Save Plus feature, select the day(s) that you want the phone to power off on schedule. You can select multiple days by pressing and holding the Control key while clicking on the days that you want Power Save Plus to operate. The default is disabled (no days selected). In Power Save Plus mode, enough power is maintained to illuminate one key. All other functions of the phone are turned off in Power Save Plus mode. Power Save Plus mode turns off the phone for the time period specified in the Phone On Time and Phone Off Time fields. This time period is usually outside of your organization's regular operating hours. The illuminated key allows a user to press it to restore full power to the phone. After pressing the illuminated key, the phone power-cycles and reregisters with Unified CM before it becomes fully operational. Power Save Plus is disabled by default. When you select day(s) in this field, the following notice displays to indicate e911 concerns. By enabling Power Save Plus, you are agreeing to the terms specified in this Notice. While Power Save Plus Mode (The &quot;Mode&quot;) is in effect, endpoints configured for the mode are disabled for emergency calling and from receiving inbound calls. By selecting this mode, you agree to the following: (I) You are taking full responsibility for providing alternate methods for emergency calling and receiving calls while the mode is in effect; (II) Cisco has no liability in connection with your selection of the mode and all liability in connection with enabling the mode is your responsibility; and (III) You will fully inform users of the effects of the mode on calls, calling and otherwise.</td>
</tr>
<tr>
<td>Phone On Time</td>
<td>This field determines the time that the phone turns on automatically on the days that are selected in the Enable Power Save Plus list box. Enter the time in 24 hour format, where 00:00 represents midnight. For example, to automatically turn the phone on at 7:00 a.m., (0700), enter 07:00. To turn the phone on at 2:00 p.m. (1400), enter 14:00. If this field is blank, the phone automatically turns on at 00:00.</td>
</tr>
<tr>
<td>Phone Off Time</td>
<td>This field determines the time of day that the phone will turn itself off on the days that are selected in the Enable Power Save Plus list box. Enter the time in the following format hours:minutes. If this field is blank, the phone automatically turns off at midnight (00:00). Note: If Phone On Time is blank (or 00:00) and Phone Off Time is blank (or 24:00), the phone will remain on continuously, effectively disabling the Power Save Plus feature unless you allow EnergyWise to send overrides.</td>
</tr>
<tr>
<td>Phone Off Idle Timeout</td>
<td>This field represents the number of minutes that the device must be idle before the device will request the power sourcing equipment (PSE) to power down the device. The value in this field takes effect: - When the device was in Power Save Plus mode as scheduled and was taken out of Power Save Plus mode because the phone user pressed the select key - When the phone is repowered by the attached switch - When the Phone Off Time is met but the phone is in use. The unit is hours. This value is in free form hours and minutes. &quot;1:30&quot; would activate the display for one hour and 30 minutes.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable Audible Alert</td>
<td>This checkbox, when enabled, instructs the phone to play an audible alert ten minutes prior to the time specified in the field, Phone Off Time. The select key on the phone will quickly flash to visually alert the user to the impending phone state change (powering off as a result of the Power Save Plus feature). To also audibly alert the user, enable this checkbox. The default is disabled. This checkbox only applies if the Enable Power Save Plus list box has one or more days selected.</td>
</tr>
<tr>
<td>EnergyWise Domain</td>
<td>This field defines the EnergyWise domain in which the phone is participating. An EnergyWise domain is required by the Power Save Plus feature. If you have chosen days in the Enable Power Save Plus feature, you must also provide an EnergyWise domain. The default is blank.</td>
</tr>
<tr>
<td>EnergyWise Endpoint Security Secret</td>
<td>This field defines the password (shared secret) used to communicate within the EnergyWise domain. An EnergyWise domain and secret is required by the Power Save Plus feature. If you have chosen days in the Enable Power Save Plus list box, you must also provide an EnergyWise domain and secret. The default is blank.</td>
</tr>
<tr>
<td>Allow EnergyWise Overrides</td>
<td>This checkbox determines whether you will allow the EnergyWise domain controller policy to send power level updates to the phones. A few conditions apply; first, one or more days must be selected in the Enable Power Save Plus field. If the Enable Power Save Plus list box does not have any days selected, the phone will ignore the EnergyWise directive to turn off the phone. Second, the settings in Unified CM Administration will take effect on schedule even if EnergyWise sends an override. For example, assume the Display Off Time is set to 22:00 (10 p.m.), the value in the Display On Time field is 06:00 (6 a.m.), and the Enable Power Save Plus has one or more days selected. If EnergyWise directs the phone to turn off at 20:00 (8 p.m.), that directive will remain in effect (assuming no phone user intervention occurs) until the configured Phone On Time at 6 a.m. At 6 a.m., the phone will turn on and resume receiving its power level changes from the settings in Unified CM Administration. To change the power level on the phone again, EnergyWise must reissue a new power level change command. Also, any user interaction will take effect so if a user presses the select softkey after EnergyWise has directed the phone to power off, the phone will power on as a result of the user action. The default is unchecked.</td>
</tr>
<tr>
<td>Span to PC Port</td>
<td>Indicates whether the phone will forward packets transmitted and received on the Phone Port to the PC Port. Select Enabled if an application is being run on the PC Port that requires monitoring of the IP Phone's traffic such as monitoring and recording applications (common in call center environments) or network packet capture tools used for diagnostic purposes. To use this feature PC Voice VLAN access must be enabled.</td>
</tr>
<tr>
<td>Logging Display</td>
<td>This option selects what type of console logging is allowed. This option does not control the generation of logs - just whether the logs display. Disabled indicates that logging does not display to the console, nor to the connected downstream port. PC Controlled indicates that the workstation attached to the PC port will control whether logging is enabled. Enabled indicates that logs are always sent both to the console and to downstream port. Use Enabled to force logs on so they can be captured with a packet sniffer.</td>
</tr>
<tr>
<td>Load Server</td>
<td>Indicates that the phone will use an alternative server to obtain firmware loads and upgrades, rather than the defined TFTP server. This option enables you to indicate a local server to be used for firmware upgrades, which can assist in reducing install times, particularly for upgrades over a WAN. Enter the hostname</td>
</tr>
</tbody>
</table>
or the IP address (using standard IP addressing format) of the server. The indicated server must be running TFTP services and have the load file in the TFTP path. If the load file is not found, the load will not install. The phone will not be redirected to the TFTP server. If this field is left blank, the phone will use the designated TFTP server to obtain its load files and upgrades.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recording Tone</td>
<td>This can be used to configure whether the recording tone is enabled or disabled on the phone. If enabled, the phone mixes the recording tone into both directions for every call.</td>
</tr>
<tr>
<td>Recording Tone Local Volume</td>
<td>This can be used to configure the loudness setting of the recording tone that the local party hears. This loudness setting applies regardless of the actual device used for hearing (handset, speakerphone, headset). The loudness setting should be in the range of 0% to 100%, with 0% being no tone and 100% being at the same level as the current volume setting. The default value is 100%.</td>
</tr>
<tr>
<td>Recording Tone Remote Volume</td>
<td>This can be used to configure the loudness setting of the recording tone that the remote party hears. The loudness setting should be in the range of 0% to 100%, with 0% being less than -66dBM and 100% being -4dBm. The default value is -10dBm or 50%.</td>
</tr>
<tr>
<td>Recording Tone Duration</td>
<td>Indicates the length of time in milliseconds for which the recording tone is inserted in the audio stream. The default for this parameter is set to the value in the Network locale file for this field. The valid range for this parameter is a value between 1 and 3000 milliseconds.</td>
</tr>
<tr>
<td>Display On When Incoming Call</td>
<td>When the phone is in Screen Save mode this will turn the display on when a call is ringing.</td>
</tr>
<tr>
<td>RTCP</td>
<td>Maintains statistic for audio.</td>
</tr>
<tr>
<td>Log Server</td>
<td>Specifies an IP address and port of a remote system where log messages are sent.</td>
</tr>
<tr>
<td>Advertise G.722 and iSAC Codecs</td>
<td>Indicates whether Cisco Unified IP Phones will advertise the G.722 codec to Cisco Unified CallManager. Codec negotiation involves two steps: first, the phone must advertise the supported codec(s) to Cisco Unified CallManager (not all endpoints support the same set of codecs). Second, when Cisco Unified CallManager gets the list of supported codecs from all phones involved in the call attempt, it chooses a commonly-supported codec based on various factors, including the region pair setting. Valid values specify Use System Default (this phone will defer to the setting specified in the enterprise parameter, Advertise G.722 Codec), Disabled (this phone will not advertise G.722 to Cisco Unified CallManager) or Enabled (this phone will advertise G.722 to Cisco Unified CallManager).</td>
</tr>
<tr>
<td>Wideband Headset UI Control</td>
<td>Allows users to enable or disable Wideband Headset option on phone UI.</td>
</tr>
<tr>
<td>Wideband Headset</td>
<td>Enable or disable the use of a Wideband Headset on the phone. Used in conjunction with User Control Wideband Headset.</td>
</tr>
<tr>
<td>Peer Firmware Sharing</td>
<td>PPID. Enables or disables Peer to Peer image distribution in order to allow a single phone in a subnet to retrieve an image firmware file then distribute it to its peers - thus reducing TFTP bandwidth and providing for a faster firmware upgrade time.</td>
</tr>
<tr>
<td>Cisco Discover Protocol (CDP):</td>
<td>Allows administrator to enable or disable Cisco Discovery Protocol (CDP) on the phone.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Switch Port</strong></td>
<td>switch port.</td>
</tr>
<tr>
<td><strong>Cisco Discover Protocol (CDP): PC Port</strong></td>
<td>Allows administrator to enable or disable Cisco Discovery Protocol (CDP) on the PC port.</td>
</tr>
<tr>
<td><strong>Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port</strong></td>
<td>Allows administrator to enable or disable Link Layer Discovery Protocol (LLDP-MED) on the switch port.</td>
</tr>
<tr>
<td><strong>Link Layer Discovery Protocol - (LLDP): PC Port</strong></td>
<td>Allows administrator to enable or disable Link Layer Discovery Protocol (LLDP) on the PC port.</td>
</tr>
<tr>
<td><strong>LLDP Asset ID</strong></td>
<td>Allows administrator to set Asset ID for Link Layer Discovery Protocol.</td>
</tr>
<tr>
<td><strong>LLDP Power Priority</strong></td>
<td>Allows administrator to set Power Priority for Link Layer Discovery Protocol.</td>
</tr>
<tr>
<td><strong>802.1x Authentication</strong></td>
<td>Specifies the 802.1x authentication feature status.</td>
</tr>
<tr>
<td><strong>Detect Unified CM Connection Failure</strong></td>
<td>This field determines the sensitivity that the phone has for detecting a connection failure to Cisco Unified Communications Manager (Unified CM), which is the first step before device failover to a backup Unified CM/SRST occurs. Valid values specify Normal (detection of a Unified CM connection failure occurs at the standard system rate) or Delayed (detection of a Unified CM connection failover occurs approximately four times slower than Normal). For faster recognition of a Unified CM connection failure, choose Normal. If you prefer failover to be delayed slightly to give the connection the opportunity to reestablish, choose Delayed. Note that the precise time difference between Normal and Delayed connection failure detection depends on many variables that are constantly changing. This only applies to the wired Ethernet connection. Default = Normal</td>
</tr>
<tr>
<td><strong>Switch Port Remote Configuration</strong></td>
<td>Allows remote configuration of the speed and duplex for the switch port of the phone, which overrides any manual configuration at the phone. Be aware that configuring this port may cause the phone to lose network connectivity.</td>
</tr>
<tr>
<td><strong>PC Port Remote Configuration</strong></td>
<td>Allows remote configuration of the speed and duplex for the PC port of the phone, which overrides any manual configuration at the phone.</td>
</tr>
<tr>
<td><strong>Automatic Port Synchronization</strong></td>
<td>Enables the phone to synchronize the PC and SW ports to the same speed and to duplex. Only ports configured for auto negotiate change speeds.</td>
</tr>
<tr>
<td><strong>Power Negotiation</strong></td>
<td>You should enable the Power Negotiation feature when connected to a switch that supports power negotiation. However, if a switch does not support power negotiation, then you should disable the Power Negotiation feature before you power up accessories over PoE. When the Power Negotiation feature is disabled, the phone can power up accessories up to 12.9W</td>
</tr>
<tr>
<td><strong>Restrict Data Rates</strong></td>
<td>This parameter enables or disables the restriction of the upstream and downstream PHY rates according to CCX V4 Traffic Stream Rate Set IE (S54.2.6).</td>
</tr>
<tr>
<td><strong>SSH Access</strong></td>
<td>This parameter indicates whether the phone will accept ssh connections. Disabling the ssh server functionality of the phone will block access to the phone.</td>
</tr>
<tr>
<td><strong>Incoming Call Toast Timer</strong></td>
<td>This parameter specifies the maximum time in seconds that the toast displays a new incoming call notification. The incoming call toast will be disabled if choose option 0.</td>
</tr>
<tr>
<td><strong>Provide Dial Tone from Release</strong></td>
<td>Indicates whether Dial Tone is provided when Release Button is pressed. If the</td>
</tr>
<tr>
<td>Button</td>
<td>value is true, then in &quot;Off Hook Dialing/RingingOut/Connected&quot; state, a new Call Windows will be brought out after Release Button is pressed. If &quot;Revert To All Calls&quot; feature was enabled, it should be active first before &quot;Dial Tone&quot; feature.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Hide Video By Default</td>
<td>This field provides an additional flexibility of hiding video window by default if &quot;Hide Video By Default&quot; is enabled.</td>
</tr>
<tr>
<td>Background Image</td>
<td>This parameter specifies the default wallpaper file. Only the administrator disables end user access to phone wallpaper list, could this parameter take effect.</td>
</tr>
<tr>
<td>Simplified New Call UI</td>
<td>This parameter specifies if use simplified call UI style when the phone is Off-hook. Those who like the New Call Window can continue to use that at the same time that those who prefer the Simplified New Call Session can use that method.</td>
</tr>
<tr>
<td>Enable VXC VPN for MAC</td>
<td>This field indicates whether the phone will establish the VXC VPN Tunnel for the specified MAC address used by the VXC device connecting to Phone's PC-Port. When this field is blank, the phone will not establish VXC VPN tunnel. When this field is one broadcast MAC address (i.e. FFFFFFFFFF), the phone will establish VXC VPN tunnel and allow any VXC device to access the tunnel. When this field is one non-broadcast MAC address, the phone will establish VXC VPN tunnel and only allow the specified VXC device's MAC address to access the tunnel. By default, this field is blank.</td>
</tr>
<tr>
<td>VXC VPN Option</td>
<td>This field indicates how VXC VPN is supported. If &quot;Dual Tunnel&quot; is selected, phone establishes two VPN tunnels, one for Phone and another for VXC device. If &quot;Single Tunnel&quot; is selected, phone establishes only one VPN tunnel for phone and VXC-device to share. Dual Tunnel: The default configuration will be the two tunnel mode of operation to ensure the highest quality of service for the 89/99xx voice and video services. Where uncompromised voice/video quality is required the dual VPN tunnel solution is recommended. Through the use of two VPN tunnels the host Cisco IP Phone is able to provide prioritization of its CPU and memory resources to the data associated with the Phones Voice/video functions over that of the data associated with the VXC VPN tunnel. This approach will require two manual login entries (dependent on security parameters), one for Phone's Voice/Video VPN and another for VXC VPN. The two tunnel approach also requires two VPN concentrator ports and two IP addresses adding potential costs. Single Tunnel: A single VPN tunnel option is implemented for those customers willing to trade off potential voice/video quality for a simplified operating model. The solution consists of operating over a single VPN tunnel by sharing the available 89/99xx processor and memory resources across the voice, video and VDI services. The IP Phone will be unable to prioritize data handing of one service over another. As a result, possible degradation of performance of the IP Phones voice/video media handling and/or Phone UI functions due to IP Phone CPU loading.</td>
</tr>
<tr>
<td>VXC Challenge</td>
<td>This field indicates whether or not to challenge VXC device. 1) If &quot;Challenge&quot; is selected, VXC device will be challenged. For &quot;Single Tunnel&quot; &quot;VXC VPN Option&quot;, Phone VPN tunnel will be torn down then pop-up &quot;Phone VPN Sign In&quot; window for user to input credentials and re-establish Phone VPN tunnel. For &quot;Dual Tunnel&quot; &quot;VXC VPN Option&quot;, &quot;VXC VPN Sign In&quot; window will pop up for user to input credentials and re-establish VXC VPN tunnel. 2) If &quot;No Challenge&quot; is selected, VXC challenge will be bypassed. For &quot;Single Tunnel&quot; &quot;VXC VPN Option&quot;, VXC traffic will silently be permitted to go over phone VPN without VXC challenge. For &quot;Dual Tunnel&quot; &quot;VXC VPN Option&quot;, credentials of Phone VPN tunnel will be reused to re-establish VXC VPN tunnel. By default, the &quot;Challenge&quot; will be used.</td>
</tr>
<tr>
<td>VXC-M Servers</td>
<td>VXC Management Server IP address list, separated with comma.</td>
</tr>
</tbody>
</table>
To configure product specific configuration options for the Cisco Unified IP Phone 9971 with Cisco Unified Communications Manager Express, create an ephone template with the necessary options.

```
  service phone <module> <value>
```

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Module</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable Speakerphone</td>
<td>disableSpeaker</td>
<td>false = Enabled; true = Disabled</td>
</tr>
<tr>
<td>Disable Speakerphone and Headset</td>
<td>disableSpeakerAndHeadset</td>
<td>false = Enabled; true = Disabled</td>
</tr>
<tr>
<td>PC Port</td>
<td>pcPort</td>
<td>0 = Enabled; 1 = Disabled</td>
</tr>
<tr>
<td>Back USB Port</td>
<td>usb1</td>
<td>1 = Enabled; 0 = Disabled</td>
</tr>
<tr>
<td>Side USB Port</td>
<td>usb2</td>
<td>1 = Enabled; 0 = Disabled</td>
</tr>
<tr>
<td>Cisco Camera</td>
<td>ciscoCamera</td>
<td>0 = Disabled; 1 = Enabled</td>
</tr>
<tr>
<td>Video Capabilities</td>
<td>videoCapability</td>
<td>0 = Disabled; 1 = Enabled</td>
</tr>
<tr>
<td>Enable/Disable USB Classes</td>
<td>usbClasses</td>
<td>0 = Mass Storage; 1 = Human Interface Device; 2 = Audio Class</td>
</tr>
<tr>
<td>SDIO</td>
<td>sdio</td>
<td>0 = Disabled; 1 = Enabled</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>bluetooth</td>
<td>1 = Enabled; 0 = Disabled</td>
</tr>
<tr>
<td>Setting</td>
<td>Environment</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Wifi</td>
<td>wifi</td>
<td>1 = Enabled; 0 = Disabled</td>
</tr>
<tr>
<td>Bluetooth Profiles</td>
<td>bluetoothProfile</td>
<td>0 = Headset; 1 = Human Interface Device</td>
</tr>
<tr>
<td>Settings Access</td>
<td>settingsAccess</td>
<td>1 = Enabled; 0 = Disabled; 2 = Restricted</td>
</tr>
<tr>
<td>Gratuitous ARP</td>
<td>garp</td>
<td>1 = Disabled; 0 = Enabled</td>
</tr>
<tr>
<td>PC Voice VLAN Access</td>
<td>voiceVlanAccess</td>
<td>0 = Enabled; 1 = Disabled</td>
</tr>
<tr>
<td>Web Access</td>
<td>webAccess</td>
<td>1 = Disabled; 0 = Enabled</td>
</tr>
<tr>
<td>Show All Calls on Primary Line</td>
<td>allCallsOnPrimary</td>
<td>0 = Disabled; 1 = Enabled</td>
</tr>
<tr>
<td>Days Display Not Active</td>
<td>daysDisplayNotActive</td>
<td>&lt;1-7&gt; = &lt;Sunday, Monday Tuesday, Wednesday, Thursday, Friday, Saturday&gt;</td>
</tr>
<tr>
<td>Display On Time</td>
<td>displayOnTime</td>
<td>00:00 - 23:59</td>
</tr>
<tr>
<td>Display On Duration</td>
<td>displayOnDuration</td>
<td>00:00 - 23:59</td>
</tr>
<tr>
<td>Display Idle Timeout</td>
<td>displayIdleTimeout</td>
<td>00:00 - 23:59</td>
</tr>
<tr>
<td>HTTPS Server</td>
<td>webProtocol</td>
<td>0 = HTTP and HTTPS; 1 = HTTPS Only</td>
</tr>
<tr>
<td>Enable Power Save Plus</td>
<td>enablePowerSavePlus</td>
<td>&lt;1-7&gt; = &lt;Sunday, Monday Tuesday, Wednesday, Thursday, Friday, Saturday&gt;</td>
</tr>
<tr>
<td>Phone On Time</td>
<td>phoneOnTime</td>
<td>00:00 - 24:00</td>
</tr>
<tr>
<td>Phone Off Time</td>
<td>phoneOffTime</td>
<td>00:00 - 24:00</td>
</tr>
<tr>
<td>Phone Off Idle Timeout</td>
<td>phoneOffIdleTimeout</td>
<td>20-1440</td>
</tr>
<tr>
<td>Enable Audible Alert</td>
<td>enableAudibleAlert</td>
<td>false = Disabled; true = Enabled</td>
</tr>
<tr>
<td>EnergyWise Domain</td>
<td>energyWiseDomain</td>
<td>&lt;domain_name&gt;</td>
</tr>
<tr>
<td>EnergyWise Endpoint Security Secret</td>
<td>energyWiseSecret</td>
<td>&lt;shared_secret&gt;</td>
</tr>
<tr>
<td>Allow EnergyWise Overrides</td>
<td>allowEnergyWiseOverrides</td>
<td>false = Disabled; true = Enabled</td>
</tr>
<tr>
<td>Span to PC Port</td>
<td>spanToPCPort</td>
<td>1 = Disabled; 0 = Enabled</td>
</tr>
<tr>
<td>Logging Display</td>
<td>loggingDisplay</td>
<td>0 = Disabled; 1 = PC Controller; 2 = Enabled</td>
</tr>
<tr>
<td>Load Server</td>
<td>loadServer</td>
<td>x.x.x.x</td>
</tr>
<tr>
<td>Recording Tone</td>
<td>recordingTone</td>
<td>0 = Disabled; 1 = Enabled</td>
</tr>
<tr>
<td>Recording Tone Local Volume</td>
<td>recordingToneLocalVolume</td>
<td>0-100</td>
</tr>
<tr>
<td>Recording Tone Remote Volume</td>
<td>recordingToneRemoteVolume</td>
<td>0-100</td>
</tr>
<tr>
<td>Recording Tone Duration</td>
<td>recordingToneDuration</td>
<td>0-3000</td>
</tr>
<tr>
<td>Feature</td>
<td>Property Name</td>
<td>Value Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Display On When Incoming Call</td>
<td>displayOnWhenIncomingCall</td>
<td>1 = Enabled; 0 = Disabled</td>
</tr>
<tr>
<td>RTCP</td>
<td>rtcp</td>
<td>0 = Disabled; 1 = Enabled</td>
</tr>
<tr>
<td>Log Server</td>
<td>logServer</td>
<td>x.x.x.x:y</td>
</tr>
<tr>
<td>Advertise G.722 and iSAC Codecs</td>
<td>g722CodecSupport</td>
<td>0 = Use System Default; 1 = Disabled; 2 = Enabled</td>
</tr>
<tr>
<td>Wideband Headset UI Control</td>
<td>headsetWidebandUIControl</td>
<td>0 = Enabled; 1 = Disabled</td>
</tr>
<tr>
<td>Wideband Headset</td>
<td>headsetWidebandEnable</td>
<td>0 = Enabled; 1 = Disabled</td>
</tr>
<tr>
<td>Peer Firmware Sharing</td>
<td>peerFirmwareSharing</td>
<td>1 = Enabled; 0 = Disabled</td>
</tr>
<tr>
<td>Cisco Discover Protocol (CDP):</td>
<td>enableCdpSwPort</td>
<td>1 = Enabled; 0 = Disabled</td>
</tr>
<tr>
<td>Switch Port</td>
<td>enableCdpPcPort</td>
<td>1 = Enabled; 0 = Disabled</td>
</tr>
<tr>
<td>Cisco Discover Protocol (CDP):</td>
<td>enableLldpSwPort</td>
<td>1 = Enabled; 0 = Disabled</td>
</tr>
<tr>
<td>PC Port</td>
<td>enableLldpPcPort</td>
<td>1 = Enabled; 0 = Disabled</td>
</tr>
<tr>
<td>Link Layer Discovery Protocol -</td>
<td>lldpAssetId</td>
<td>x</td>
</tr>
<tr>
<td>Media Endpoint Discover(LLDP-MED):</td>
<td>powerPriority</td>
<td>0 = Unknown; 1 = Low; 2 = High; 3 = Critical</td>
</tr>
<tr>
<td>Switch Port</td>
<td>detectCMConnectionFailure</td>
<td>0 = Normal; 1 = Delayed</td>
</tr>
<tr>
<td>PC Port</td>
<td>SWRemoteConfig</td>
<td>0 = Disabled; 1 = Auto Negotiate; 2 = 10 Half; 3 = 10 Full; 4 = 100 Half; 5 = 100 Full; 6 = 1000 Full</td>
</tr>
<tr>
<td>PC Port</td>
<td>PCRemoteConfig</td>
<td>0 = Disabled; 1 = Auto Negotiate; 2 = 10 Half; 3 = 10 Full; 4 = 100 Half; 5 = 100 Full; 6 = 1000 Full</td>
</tr>
<tr>
<td>Automatic Port Synchronization</td>
<td>PortAutoLinkSync</td>
<td>0 = Disabled; 1 = Enabled</td>
</tr>
<tr>
<td>Power Negotiation</td>
<td>powerNegotiation</td>
<td>1 = Enabled; 0 = Disabled</td>
</tr>
<tr>
<td>Restrict Data Rates</td>
<td>restrictDataRates</td>
<td>0 = Disabled; 1 = Enabled</td>
</tr>
<tr>
<td>SSH Access</td>
<td>sshAccess</td>
<td>1 = Disabled; 0 = Enabled</td>
</tr>
<tr>
<td>Incoming Call Toast Timer</td>
<td>incomingCallToastTimer</td>
<td>&lt;3,4,5,6,7,8,9,10,15,30,60&gt;</td>
</tr>
<tr>
<td>Provide Dial Tone from Release Button</td>
<td>dialToneFromReleaseKey</td>
<td>0 = Disabled; 1 = Enabled</td>
</tr>
<tr>
<td>Hide Video By Default</td>
<td>hideVideoByDefault</td>
<td>0 = Disabled; 1 = Enabled</td>
</tr>
<tr>
<td>Feature</td>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Background Image</td>
<td>defaultWallpaperFile</td>
<td>&lt;Wallpaper_file&gt;</td>
</tr>
<tr>
<td>Simplified New Call UI</td>
<td>simplifiedNewCall</td>
<td>0 = Disabled; 1 = Enabled</td>
</tr>
<tr>
<td>Enable VXC VPN for MAC</td>
<td>enableVXCVPNForMAC</td>
<td>&lt;MAC_Address&gt;</td>
</tr>
<tr>
<td>VXC VPN Option</td>
<td>vxcVpnOption</td>
<td>0 = Dual Tunnel; 1 = Single Tunnel</td>
</tr>
<tr>
<td>VXC Challenge</td>
<td>vxcChallenge</td>
<td>0 = Challenge; 1 = No Challenge</td>
</tr>
<tr>
<td>VXC-M Servers</td>
<td>vxcManagers</td>
<td>x.x.x.x</td>
</tr>
<tr>
<td>Revert to All Calls</td>
<td>revertToAllCalls</td>
<td>0 = Disabled; 1 = Enabled</td>
</tr>
<tr>
<td>80-bit SRTCP</td>
<td>SRTCP80bit</td>
<td>0 = Disabled; 1 = Enabled</td>
</tr>
<tr>
<td>RTCP for Video</td>
<td>VideoRTCP</td>
<td>1 = Enabled; 0 = Disabled</td>
</tr>
<tr>
<td>Record Call Log from Shared Line</td>
<td>logCallFromSharedLine</td>
<td>0 = Disabled; 1 = Enabled</td>
</tr>
<tr>
<td>Show Call History for Selected Line Only</td>
<td>showCallHistoryForSelectedLine</td>
<td>0 = Disabled; 1 = Enabled</td>
</tr>
<tr>
<td>Actionable Incoming Call Alert</td>
<td>actionableAlert</td>
<td>0 = Disabled; 1 = Show for all Incoming Call; 2= Show for Invisible Incoming Call</td>
</tr>
<tr>
<td>DF bit</td>
<td>dfBit</td>
<td>&lt;0,1&gt;</td>
</tr>
<tr>
<td>Default Line Filter</td>
<td>defaultLineFilter</td>
<td>&lt;Line_Numbers&gt;</td>
</tr>
</tbody>
</table>

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 IP Phone 9971 Administration Guide or the Cisco Unified IP Phone 9971 Release Notes.


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

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

- Ensure **CCKM** is **Enabled** if utilizing 802.1x authentication
- Set **Quality of Service (QoS)** to **Platinum**
• Set the WMM Policy to Required
• Ensure Session Timeout is enabled and configured correctly
• Ensure Aironet IE is Enabled
• Set DTPC Support to Enabled
• Disable P2P (Peer to Peer) Blocking Action / Public Secure Packet Forwarding (PSPF)
• Ensure Client Exclusion is configured correctly
• Disable DHCP Address Assignment Required
• Set MFP Client Protection to Optional or Disabled
• Set the DTIM Period to 2
• Set Client Load Balancing to Disabled
• Set Client Band Select to Disabled
• Set IGMP Snooping to Enabled
• Enable Symmetric Mobile Tunneling Mode if Layer 3 mobility is utilized
• Enable Short Preamble if using 2.4 GHz
• Enable ClientLink if utilizing Cisco 802.11n Access Points
• Configure the Data Rates as necessary
• Enable CCX Location Measurement
• Configure Auto RF as necessary
• Set Admission Control Mandatory to Enabled for Voice
• Set Load Based CAC to Enabled for Voice
• Enable Traffic Stream Metrics for Voice
• Set Admission Control Mandatory to Disabled for Video
• Set EDCA Profile to Voice Optimized or Voice and Video Optimized
• Set Enable Low Latency MAC to Disabled
• Ensure that Power Constraint is Disabled
• Enable Channel Announcement and Channel Quiet Mode
• Enable CleanAir if utilizing Cisco Access Points with CleanAir technology
• Configure Multicast Direct Feature as necessary
• Set the 802.1p tag to 5 for the Platinum QoS profile

Note: If clients from other regions are present and will attempt to associate with the wireless LAN, then ensure that World Mode (802.11d) is enabled.
When using 802.1x authentication, it is recommended to implement CCKM to offer fast secure roaming.

SSID / WLAN Settings

It is recommended to have a separate SSID for the Cisco Unified IP Phone 9971.
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 IP Phone 9971 can be configured to only apply to a certain 802.11 radio type. It is recommended to have the Cisco Unified IP Phone 9971 operate on the 5 GHz band due to have many channels available and not as many interferers as the 2.4 GHz band has.

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

In order to utilize CCKM, enable WPA2 policy with AES encryption and 802.1x + CCKM for authenticated key management type when the Cisco Unified IP Phone 9971 is running firmware version 9.1(1) or later in order to enable fast secure roaming.
If the Cisco Unified IP Phone 9971 is running firmware version prior to 9.1(1), 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 IP Phone 9971 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 IP Phone 9971, then ensure the WMM policy is set to **Allowed**.

Enable **7920 AP CAC** to advertise Qos Basic Service Set (QBSS) to the client.
Configure **Enable Session Timeout** as necessary per your requirements. It is recommended to either disable the session timeout or extend the timeout (e.g. 24 hours / 86400 seconds) to avoid possible interruptions during audio calls. If disabled it will avoid any potential interruptions altogether, but enabling session timeout can help to re-validate client credentials periodically to ensure that the client is using valid credentials.

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

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

Configure **Client Exclusion** as necessary.

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

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

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

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

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

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

**Media Session Snooping** can be enabled to utilize SIP CAC.

It is recommended to set **Re-anchor Roamed Voice Clients** to disabled as this can cause brief interruptions with wireless LAN connectivity when a call is terminated after performing an inter-controller roaming.
For the Cisco Autonomous Access Point, ensure that the SSID is configured for open + eap as and network-eap when using 802.1x authentication.

```
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.
Controller Settings

Ensure the Cisco Unified Wireless LAN Controller hostname is configured correctly.
Enable Link Aggregation (LAG) if utilizing multiple ports on the Cisco Unified Wireless LAN Controller.
Configure the desired AP multicast mode.

In releases prior to 6.0, Aggressive Load Balancing was configured in the General Controller settings.
In 6.0 and later, this is referred to as Client Load Balancing and is configurable under the WLAN configuration (SSID settings).

If utilizing multicast, then **Enable Global Multicast Mode** and **Enable IGMP Snooping** should be enabled.
If utilizing layer 3 mobility, then **Symmetric Mobility Tunneling** should be **Enabled**.

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

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

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

Set the Beacon Period to 100 ms.

Ensure DTPC Support is enabled.

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

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

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

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

Enable CCX Location Measurement.

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

Set the Beacon Period to 100 ms.

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

Ensure DTPC Support is enabled.

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

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

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

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

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).

Enable CCX Location Measurement.
Beamforming (ClientLink)

Enable ClientLink if using Cisco 802.11n Access Points.

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

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

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

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

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

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

(Cisco Controller) > show 802.11a
(Cisco Controller) > show 802.11b

Legacy Tx Beamforming setting.................... Enabled
Auto RF (RRM)

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

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

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

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

The 5 GHz channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n Access Points.
Ensure that channel 165 is not enabled in the DCA list as the Cisco Unified IP Phone 9971 does not support this channel.

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

It is recommended to configure the 2.4 GHz channel for 20 MHz even if using Cisco 802.11n Access Points capable of 40 MHz due to the limited number of channels available in 2.4 GHz.
Individual access points can be configured to override the global setting to use dynamic channel and transmit power assignment for either 5 or 2.4 GHz depending on which frequency band is to be utilized.

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

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

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

---

**Client Roaming**

The Cisco Unified IP Phone 9971 does not utilize the RF parameters in the Client Roaming section of the Cisco Unified Wireless LAN Controller as scanning and roaming is managed independently by the phone itself.

**Call Admission Control**

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

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

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

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

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

Enable Traffic Stream Metrics (TSM).

SIP CAC can help ensure that downstream voice frames are prioritized correctly when a client does not support TSPEC.
Load based CAC logic is utilized with SIP CAC, so all 802.11 traffic and energy on the channel is accounted for to determine available bandwidth.

The access point has different methods for call admission control when using SIP CAC depending on whether the client uses TCP or UDP for SIP communications.

If the client uses TCP for SIP, then the access point will snoop the SIP packets when media session snooping is enabled on the WLAN / SSID and will not forward the SIP frames upstream or downstream if there is not bandwidth available for the new voice stream. This could potentially result in loss of registration to the Cisco Unified Communications Manager.

If the client uses UDP for SIP, then the access point will snoop the SIP packets when media session snooping is enabled on the WLAN / SSID and will sent a 486 busy message to the client, which in turn can be interpreted as a Network Busy message and the client could either roam to another access point or simply terminate the call setup for that session.

The Cisco Unified IP Phone 9971 uses TCP for SIP communications, therefore if the channel is busy where another call can not be allowed, then the Cisco Unified IP Phone 9971 could potentially lose registration to the Cisco Unified Communications Manager.

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`.

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

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

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

Ensure QoS is setup correctly under the WLAN / SSID configuration, which can be displayed by using the following command.

```
(Cisco Controller) >show wlan <WLAN id>
```

```
Quality of Service......................... Platinum (voice)
WMM........................................... Allowed
```
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 IP Phone 9971 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:


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

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

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

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

DFS (802.11h)

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

**Power Constraint** should be left un-configured or set to 0 dB as DTPC will be used by the Cisco Unified IP Phone 9971 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.
AP Groups

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

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

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

If changes are made after access points have joined the AP Group, then those access points will reboot once those changes are made.
On the **APs** tab, select the desired access points then select **Add APs**.

Those access points will then reboot.

---

**RF Profiles**

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

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

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

---

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

Is recommended to enable 12 Mbps as **Mandatory** and 18-54 Mbps as **Supported**; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.
On the RRM tab, the **Maximum Power Level Assignment** and **Minimum Power Level Assignment** settings as well as other TPC and **Coverage Hole Detection** settings can be configured.

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

All access points configured for FlexConnect mode need to be added to a FlexConnect Group. If utilizing CCKM, then seamless roams can only occur when roaming to access points within the same FlexConnect Group.

Multicast Direct

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

**QoS Profiles**

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

- Platinum = 5
- Gold = 4
- Silver = 2
- Bronze = 1
Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide

Edit QoS Profile

<table>
<thead>
<tr>
<th>QoS Profile Name</th>
<th>platinum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>For Voice Applications</td>
</tr>
</tbody>
</table>

**Per-User Bandwidth Contracts (kbps)**

<table>
<thead>
<tr>
<th>DownStream</th>
<th>UpStream</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Data Rate</td>
<td>0</td>
</tr>
<tr>
<td>Burst Data Rate</td>
<td>0</td>
</tr>
<tr>
<td>Average Real-Time Rate</td>
<td>0</td>
</tr>
<tr>
<td>Burst Real-Time Rate</td>
<td>0</td>
</tr>
</tbody>
</table>

**Per-SSID Bandwidth Contracts (kbps)**

<table>
<thead>
<tr>
<th>DownStream</th>
<th>UpStream</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Data Rate</td>
<td>0</td>
</tr>
<tr>
<td>Burst Data Rate</td>
<td>0</td>
</tr>
<tr>
<td>Average Real-Time Rate</td>
<td>0</td>
</tr>
<tr>
<td>Burst Real-Time Rate</td>
<td>0</td>
</tr>
</tbody>
</table>

**WLAN QoS Parameters**

<table>
<thead>
<tr>
<th>Maximum Priority</th>
<th>voice 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uncast Default Priority</td>
<td>voice 1</td>
</tr>
<tr>
<td>Multicast Default Priority</td>
<td>voice 1</td>
</tr>
</tbody>
</table>

**Wired QoS Protocol**

<table>
<thead>
<tr>
<th>Protocol Type</th>
<th>802.1p 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1x Tag</td>
<td>5</td>
</tr>
</tbody>
</table>

*The value zero (0) indicates the feature is disabled*
Edit QoS Profile

QoS Profile Name: gold
Description: For Video Applications

Per-User Bandwidth Contracts (kbps) *

<table>
<thead>
<tr>
<th></th>
<th>DownStream</th>
<th>UpStream</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Burst Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Average Real-Time Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Burst Real-Time Rate</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Per-SSID Bandwidth Contracts (kbps) *

<table>
<thead>
<tr>
<th></th>
<th>DownStream</th>
<th>UpStream</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Burst Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Average Real-Time Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Burst Real-Time Rate</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

WLAN QoS Parameters

Maximum Priority: video
Unicast Default Priority: video
Multicast Default Priority: video

Wired QoS Protocol

Protocol Type: 802.1p
802.1p Tag: 4

* The value zero (0) indicates the feature is disabled
Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide

Edit QoS Profile

**QoS Profile Name**
silver

**Description**
For Best Effort

**Per-User Bandwidth Contracts (kbps)**

<table>
<thead>
<tr>
<th></th>
<th>DownStream</th>
<th>UpStream</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Burst Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Average Real-Time Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Burst Real-Time Rate</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Per-SSID Bandwidth Contracts (kbps)**

<table>
<thead>
<tr>
<th></th>
<th>DownStream</th>
<th>UpStream</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Burst Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Average Real-Time Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Burst Real-Time Rate</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**WLAN QoS Parameters**

- Maximum Priority: besteffort 1
- Unicast Default Priority: besteffort 1
- Multicast Default Priority: besteffort 1

**Wired QoS Protocol**

- Protocol Type: 802.1p
- 802.1p Tag: 2

*The value zero (0) indicates the feature is disabled*
Note: The 802.1p tag mappings were changed with the 7.5.102.0 release.
Prior to the 7.5.102.0 release, Platinum = 6, Gold = 5, Silver = 3, Bronze = 1.

QoS Basic Service Set (QBSS)

There are three different versions of QoS Basic Service Set (QBSS) that the Cisco Unified IP Phone 9971 supports.

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

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

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

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

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

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

Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide
**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 IP Phone 9971 roaming experience.

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

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

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

Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide
(Cisco Controller) >config wlan security wpa akm cckm timestamp-tolerance 5000 <WLAN id>

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

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

**Auto-Immune**

The Auto-Immune feature can optionally be enabled for protection against denial of service (DoS) attacks. Although when this feature is enabled there can be interruptions introduced with voice over wireless LAN, therefore it is recommended to disable the Auto-Immune feature on the Cisco Unified Wireless LAN Controller.

The Auto-Immune feature was introduced in the 4.2.176.0 release, which was enabled by default and non-configurable. As of the 4.2.207.0, 5.2.193.0 and 6.0.182.0 releases this feature is disabled by default but can be enabled optionally.

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

(Cisco Controller) >show wps summary

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

Client Exclusion Policy
Excessive 802.11-association failures........ Enabled
Excessive 802.11-authentication failures....... Enabled
Excessive 802.1x-authentication................ Enabled
IP-theft..................................... Enabled
Excessive Web authentication failure.......... Enabled

Signature Policy
Signature Processing......................... Enabled

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

(Cisco Controller) >config wps auto-immune disable
WLAN Controller Advanced EAP Settings

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

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

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

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

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

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

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

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

If using WPA/WPA2 PSK then it is recommended to reduce the EAPOL-Key Timeout to 400 milliseconds from the default of 1000 milliseconds with EAPOL-Key Max Retries set to 4 from the default of 2.
If using WPA/WPA2, then using the default values where the EAPOL-Key Timeout is set to 1000 milliseconds and EAPOL-Key Max Retries are set to 2 should work fine, but is still recommended to set those values to 400 and 4 respectively.
The EAPOL-Key Timeout should not exceed 1 second (1000 milliseconds).

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

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

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

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

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

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

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

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

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

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

TKIP Countermeasure Holdoff Time

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

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

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

To confirm the change, enter show wlan <WLAN id>, where the following will be displayed.
For the Cisco Autonomous Access Point, enter the time in seconds to hold off clients if a TKIP countermeasure event occurs.

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

**VLANs and Cisco Autonomous Access Points**

Segment wireless voice and data into separate VLANs.

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

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

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

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

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

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

**Configuring the Cisco Unified IP Phone 9971**

To configure the Wi-Fi settings on the Cisco Unified IP Phone 9971, use the keypad and touch screen to navigate to Applications Button > Administrator Settings > Network Setup > WLAN Setup.

**Wireless LAN Settings**

Use the following guidelines to configure the wireless LAN profile.

- Ensure that **Wireless** is set to **On**.
- **WLAN Sign in Access** can be set to **On** to give shortcut access in the Applications Menu in order to update the username or password.
- Enter the **SSID** for the voice wireless LAN, which is case sensitive.
- The Cisco Unified IP Phone 9971 supports a single wireless LAN profile that allows a single SSID.
- 3 different 802.11 modes are available.
  - Auto
  - 802.11a
  - 802.11b/g

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

**802.11a** mode will only scan 5 GHz channels and **802.11b/g** mode will only scan 2.4 GHz channels, then will attempt to associate to an access point if the configured network is available.
• Below lists the available security modes supported and the key management and encryption types that can be used for each mode.

<table>
<thead>
<tr>
<th>Security Mode</th>
<th>802.1x Type</th>
<th>Key Management</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>N/A</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Open with WEP</td>
<td>N/A</td>
<td>Static</td>
<td>WEP (40/64 or 104/128 bit)</td>
</tr>
<tr>
<td>Shared Key</td>
<td>N/A</td>
<td>Static</td>
<td>WEP (40/64 or 104/128 bit)</td>
</tr>
<tr>
<td>LEAP</td>
<td>LEAP</td>
<td>802.1x, WPA, WPA2</td>
<td>TKIP, AES, WEP (40/64 or 104/128 bit)</td>
</tr>
<tr>
<td>EAP-FAST</td>
<td>EAP-FAST</td>
<td>802.1x, WPA, WPA2</td>
<td>TKIP, AES, WEP (40/64 or 104/128 bit)</td>
</tr>
<tr>
<td>AKM</td>
<td>N/A, LEAP</td>
<td>802.1x, WPA, WPA2, WPA-PSK, WPA2-PSK</td>
<td>TKIP, AES, WEP (40/64 or 104/128 bit)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Key Style</th>
<th>Key Size</th>
<th>Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASCII</td>
<td>40/64 bit</td>
<td>5</td>
</tr>
<tr>
<td>ASCII</td>
<td>104/128 bit</td>
<td>13</td>
</tr>
<tr>
<td>HEX</td>
<td>40/64 bit</td>
<td>10 (0-9, A-F)</td>
</tr>
<tr>
<td>HEX</td>
<td>104/128 bit</td>
<td>26 (0-9, A-F)</td>
</tr>
</tbody>
</table>

• 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 Pre-Shared key, enter the ASCII or hexadecimal formatted key.

<table>
<thead>
<tr>
<th>Key Style</th>
<th>Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASCII</td>
<td>8-63</td>
</tr>
<tr>
<td>HEX</td>
<td>64 (0-9,A-F)</td>
</tr>
</tbody>
</table>

• **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 with WEP** or **Shared Key** for the security mode, enter the static WEP key information that matches the access point configuration.
• In the IPv4 Setup, 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’s IP address via the network’s DHCP scope, then set Alternate TFTP to Yes and enter the IP address for the TFTP Server.

**Note:** CCKM will be negotiated if enabled on the access point when using LEAP, EAP-FAST, or AKM.

If using 802.1x authentication via LEAP, EAP-FAST 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.

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

For more information, refer to the [Configuring Settings on the Cisco Unified IP Phone 9971](http://www.cisco.com/en/US/products/ps10453/prod_maintenance_guides_list.html) in the Cisco Unified IP Phone 9971 Administration Guide at this URL:

- Bluetooth Settings

  The Cisco Unified IP Phone 9971 has Bluetooth 2.1 support, which enables hands-free communications.
To pair a Bluetooth headset to the Cisco Unified IP Phone 9971, follow the instructions below.

1. Navigate to **Applications > Preferences**
2. Select **Bluetooth** then select the left softkey **On**
   (Ensure the system administrator has enabled Bluetooth)
3. Select the **Add Accessory** softkey in **Applications > Preferences** when Bluetooth is selected or **Add Bluetooth Accessory** in **Applications > Accessories**
   (ensure the Bluetooth headset is in pairing mode)
4. Select **Connect** after the Bluetooth headset is discovered
5. Enter the Bluetooth passkey if prompted (will attempt to use 0000)
Camera Settings for Video Calls

When the Cisco Unified Video Camera is connected, ensure that it appears in the Accessories menu list. Once discovered, then a few items can be configured (Auto Transmit Video, Brightness, View Area).

Auto Transmit Video determines if the phone is to start streaming video immediately at the beginning of the call or not assuming the far end device has video capabilities.

Configuring View Area determines if the video sent is to be zoomed in or out.

Brightness can also be configured to accommodate for the current working environment.
The video can be muted by pressing the video mute softkey.
If the call is muted via the mute hard key, then the video is also muted.
The camera also has a shutter that can be closed to prevent unnecessary video streaming.
When on a video call, it can be configured to display your own picture as well in either corner of the display.

**Upgrading Firmware**

To upgrade the firmware, install the signed COP file for Cisco Unified Communications Manager.
For information on how to install the COP file, refer to the Cisco Unified Communications Manager Operating System Administrator Guide at this URL:

During TFTP server download, the configuration file is parsed and the device load is identified. The Cisco Unified IP Phone 9971 then downloads the firmware files to flash if it is not running the specified image already.
The Load Server can be specified as an alternate TFTP server to retrieve firmware files, which is located in the product specific configuration section of Cisco Unified IP Phone 9971 within Cisco Unified Communications Manager Administration.
To install the firmware on Cisco Unified Communications Manager Express, extract the contents of the TAR file and upload into the router’s flash. Each file will need to be enabled for TFTP download. Configure the phone load and reset the phones to upgrade the firmware.

**Example:**

```shell
  tftp-server flash:sip9971.9-4-1SR1-2.loads
  tftp-server flash:kern9971.9-4-1SR1-2.sebn
  tftp-server flash:sboot9971.031610R1-9-4-1SR1-2.sebn
  tftp-server flash:skern9971.022809R2-9-4-1SR1-2.sebn
  tftp-server flash:dkern9971.100609R2-9-4-1SR1-2.sebn
  tftp-server flash:rootfs9971.9-4-1SR1-2.sebn

  !
  telephony-service
  load 9971 sip9971.9-4-1SR1-2.loads
```

**Troubleshooting**

**Device Information**

The Cisco Unified IP Phone 9971 provides device information, where network status, MAC address and version information is displayed.

Browse to the web interface (http://x.x.x.x) of the Cisco Unified IP Phone 9971 select **Device Information** to view this information.
Network Setup

The Cisco Unified IP Phone 9971 provides network setup information, where network and Cisco Unified Communications Manager information is displayed.

Browse to the web interface (http://x.x.x) of the Cisco Unified IP Phone 9971 then select **Network Setup** to view this information.
Current Access Point

The Cisco Unified IP Phone 9971 will only show the current access point (no neighbor list). To view go to the Applications Button > Administrator Settings > Status > Current Access Point.

The Cisco Unified IP Phone 9971 is constantly scanning regardless of current signal or call state to discover new access points.
As of the 9.0(2) release, the Current Access Point information can also be seen in the phone’s web interface.
WLAN Statistics

The Cisco Unified IP Phone 9971 provides WLAN statistic information, where packet and counters are displayed. Browse to the phone’s web interface (https://x.x.x.x) then select WLAN Statistics to view this information.

Streaming Statistics

The Cisco Unified IP Phone 9971 provides call statistic information, where MOS, jitter and packet counters are displayed. The MOS value should be greater than or equal to 4.0 when using G.722 or G.711. A MOS value of 3.8 is the highest possible value when using G.729. Browse to the phone’s web interface (https://x.x.x.x) then select Streaming Statistics to view this information.
This information is also available locally on the phone under the Applications Button > Administrator Settings > Status > Call Statistics.

For more information, see the Troubleshooting the Cisco Unified IP Phone 9971 chapter in the Cisco Unified IP Phone 9971 Administration Guide at this URL:

Device Logs

Console logs, core dumps, status messages for troubleshooting purposes can be obtained from the web interface of Cisco Unified IP Phone 9971.

Browse to the web interface (http://x.x.x.x) of Cisco Unified IP Phone 9971 then select the necessary menu item under Device Logs to view this information.
Traffic Stream Metrics (TSM)

The Traffic Stream Metrics feature requires the client to report voice traffic related measurements to the AP. The parameters (queue delay, media delay, packet loss, packet count, roaming delay, roaming count) will be gathered by the AP and escalated to the WLAN management system, which will help maintain a database that can be used for the benefit of the stations by ensuring low packet latency and loss.

Check the box Metrics Collection in the global 802.11 Voice Parameters to enable Traffic Stream Metrics. See the Call Admission Control Settings section for further information on how to enable TSM.

To view Traffic Stream Metrics data for a client, select TSM from the drop down menu for which band the Cisco Unified IP Phone 9971 is using. The Traffic Stream Metrics data entries will then be displayed. Select one of the entries to display the uplink and downlink statistics.
As of the 9.0(2) release, the WLAN status indicator will be visible in all menus within Administrator Settings. In the initial release, the WLAN signal indicator was only visible in the WLAN Setup menu.
WLAN Disconnect Display

As of the 9.0(2) release, a toast message will be displayed if the WLAN connection has been interrupted.

Restoring Factory Defaults

The configuration can be cleared by using the factory default menu option on the phone via the Applications Button > Administrator Settings > Reset Settings.

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 IP Phone 9971. At the prompt enter the username and password for the account that the Cisco Unified IP Phone is associated to in Cisco Unified Communications Manager.

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.

Accessories

The following accessories are available for the Cisco Unified IP Phone 9971. For more information, refer to the following URLs:


• Jawbone ICON for Cisco Bluetooth Headset
• Cisco Unified IP Color Key Expansion Module
• Cisco Unified Video Camera

For more information on Jawbone ICON for Cisco Bluetooth Headset, refer to the following URL:

3rd Party Accessories
• Bluetooth Headsets
  www.plantronics.com
  www.jabra.com
  www.jawbone.com
  www.vxicorp.com
  www.motorola.com
Additional Documentation

Cisco Unified IP Phone 9971 Data Sheet

Cisco Unified IP Phone 9971 Administration Guide

Cisco Unified IP Phone 9971 User Guide and Quick Reference

Cisco Unified IP Phone 9971 Release Notes

Cisco Unified IP Phone 9971 Software
http://software.cisco.com/download/type.html?mdfid=282749264

Cisco Unified Communications Manager

Cisco Unified Communications Manager Express

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

Cisco Unified IP Phone Services Application Development Notes

Real-Time Traffic over Wireless LAN SRND

Cisco Unified Communications SRND

Cisco Unified Wireless LAN Controller Documentation

Cisco Autonomous Access Point Documentation

Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide