Cisco IP Phone Multiplatform Phones Firmware - Wireless LAN Deployment Guide

The Cisco IP Phones with the Multiplatform Phone Firmware and a Wi-Fi capability are adaptable for scenarios where wired Ethernet networks are not available nor desirable. It is easier to move Wi-Fi enabled desk phones from once location to another. The Wireless LAN capability enables communications in a WLAN-deployed working place or home.

This document describes how to deploy the phone in a wireless LAN environment

Revision History

Issue Date	Comments
9/10/2020	Initial Version

Contents

Intended Audience

Network administrators and any other users who plan, design, and install a Cisco IP Phone with Multiplatform Phones Firmware in a Wireless Environment.

Introduction to Setup and Installation

This section is a quick step guide with few technical details. This section requires you to be familiar with Wi-Fi as a technology and, more specifically, with Wi-Fi access point configurations. If you are not familiar with Wi-Fi, the following sections of this document go into the lower level details.

Prerequisites for the installation

- Installed and configured Wi-Fi Access Points.
- One or more repeaters, also known as extenders.
- Wi-Fi capable desktop phones.

Following MPP phones support Wi-Fi:

- Cisco IP Phone 6861
- Cisco IP Phone 8861
- Cisco IP Video Phone 8865

Ensure there is adequate Wi-Fi coverage where the phone is being installed. As a quick test, you can see how strong your Wi-Fi signal is on your laptop or smart phone. If you are in a small office with a few devices, such as a laptop, smart phone and a printer, and there is a clear line of sight between the access point and the desk phone, getting a good signal on your phone is not going to be a problem.

If the access point is in your garage and there is a washroom or laundry room between the garage and the room where the phone is installed, the plumbing may be interfering with the Wi-Fi signal. Move the access point closer or buy a repeater and install the repeater in the same room as the phone. It is a best practice to use a repeater or extender made by the same vendor as your access point.

If the office is on the top floor of a house and the access point is in the basement, expect interference from plumbing and other obstacles in between. Move the access point closer or add a repeater or two to the system.

For an office with 5-50 people or more, with many walls and plumbing, run a proper site survey to ensure a successful deployment with good signal strength and reliability. Hire a trained professional to run the survey for you. Unlike a simple home office, in a larger, professional office, repeaters may not provide the required signal strength, if you require coverage over a large area with many phones and other Wi-Fi devices, install more access points.

Phone Power Information

The Cisco IP Phone 6861

The phone supports using a physical Ethernet cable as a backup when Wi-Fi is not available. The phone must be wall powered. It does not support Power over Ethernet and does not have a physical Ethernet switch port for connecting a PC.

The Cisco IP Phones 8861 and 8865

The phones support a wired Ethernet connection and have a physical Ethernet switch port for a PC. They can run on Power over Ethernet if they are using an Ethernet cable for their network connection. When the phone is in Wi-Fi mode, it disables Power over Ethernet and the PC port. When the phone is in Wi-Fi mode, the PC must connect to the Internet service separately. This is not inconvenient and is how most people connect their PC's to the Internet today.

Power Supply Ordering

With all three Wi-Fi enabled phone models, you must order a power supply when you order the phone. The actual power supplies are international. The difference is the kind of power cord or adapter connectors used to plug the supply into the wall. See the Appendix for a list of SKUs.

Some power cords and adapter clips can be used in other regions of the world. The North America power cord or adapter clip is valid for Japan and Mexico. Many emerging countries use the Continental Europe or United Kingdom power cord or adapter clip.

For the 6861, the power supply and regional adapter clip ships in the same box as the phone for all four available types.

For the 8861 and 8865,

The North America and Australia power supply and regional cord may be ordered to ship in the same box as the phones.

The Europe and the UK power supply and regional cord must be ordered separately.

Connect to a Wi-Fi

Power on the phone and do the following:

Do a Wi-Fi Scan on the Phone.

- The available access points appear on the screen. If there is more than one access point listed, use the Navigation key to scroll down and select the one with the most signal strength.
- If there is only one listed, press Select.

Select the Network Name:

Look at the number of bars for the Network Name in the location.

- It is best to have all 4 bars for the Network Name highlighted.
- If you do not see all 4 bars, adjust the phone's orientation so that top of the phone points towards the access point's antenna. Put the phone in a direct line of sight to the access point increases the signal strength. After making these adjustments, redo the scan.
- Put the phone in a separate network to guarantee voice traffic on the phone. Sharing the same network name with other phones may impact phone calls on the phone when the other phones are using heavy network traffic.
- For voice deployments, use 802.11a/n for voice and 802.11b/g/n for data.

Connect to a Network:

After you select the preferred Network Name, enter the details that is required to connect to the network.

- Select the **Security mode** that is configured for your Network Name
- The **Network Name** is auto-filled. If it isn't, redo the Wi-Fi Scan.
- **Passphrase** is the password or PIN for the network. If you are not sure about passphrase or if the phone asks for something else, go to Security in this document.
- **Frequency band** can remain as **Auto**. Your best option when the phone is close to the access point is 5 GHz. 5 GHz is the preferred band for operation and mandatory for use when the phone is mission critical.

- Press the **Connect** soft key.

When the connection is established, the phone will download its configuration by following the steps in Provisioning of the Phone below and then register.

- During this step, the phone may ask you to enter an Activation Code, it may also ask for a user name and password. Contact your service provider or system administrator for that information.
- Place the phone at the user's workspace.

Provisioning of the Phone

Once the phone receives its IP address via Wi-Fi or wired Ethernet, it will attempt to receive its provisioning by following the procedure set up by your service provider. Refer to the service provider's instructions for the details.

At a high level, the phone will follow these steps to complete the process:

- The phone attempts DHCP Options.
  If successful, it receives its provisioning. Process completed.
  If not, it attempts to contact the Cisco EDOS/CDA service over the public Internet.
- If EDOS/CDA returns a configuration, the phone is provisioned. Process completed.
  If EDOS/CDA returns no configuration, the phone will ask you for an "Activation Code," which is provided by your service provider or IT administrator.
- After entering the Activation Code, the phone is provisioned. Process completed.
- Phone might ask to enter username and password

For more information the following guides:

- *Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide*.
- *Cisco IP Phone 6800 Series Multiplatform Phones Administration Guide*

Supported Spectrum

The wireless enabled Cisco IP Phones extends collaboration with an 802.11 (Wi-Fi) capability. You can use the phones with either a wired or wireless Ethernet connection.

Wi-Fi uses an unlicensed spectrum. It may experience interference from other devices that use the same spectrum. The proliferation of devices in the 2.4 GHz spectrum, such as Bluetooth headsets, Microwave ovens, and cordless consumer phones, means that the 2.4 GHz spectrum may contain more congestion than other spectrums.

The 5 GHz spectrum is normally less congested and is the preferred spectrum for the phone so that it may take advantage of the available 802.11a/n/ac data rates.

Range comparison – 2.4 GHz vs. 5 GHz

Standard	Frequency	Theoretical Distance	Real World Distance
802.11a	5Ghz	390 ft	195 ft
802.11b	2.4Ghz	460 ft	230 ft
802.11g	2.4Ghz	125 ft	62 ft
802.11n	2.4Ghz	820 ft	410 ft
802.11n	5Ghz	460 ft	230 ft
802.11ac	5Ghz	up to 820 ft (amplified)	up to 410 ft (amplified)

Speed comparison – 2.4 GHz vs. 5 GHz

Standard	Frequency	Theoretical Speed	Real-World Speed
802.11a	5Ghz	6-54 Mbps	3 - 32 Mbps
802.11b	2.4Ghz	11 Mbps	2-3 Mbps
802.11g	2.4Ghz	54 Mbps	10 -29 Mbps
802.11n	2.4Ghz	300 Mpbs	150 Mbps
802.11n	5Ghz	900 Mbps	450Mbps
802.11ac	5Ghz	433 Mbps - 1.7 Gbps	210 Mbps - 1 G

Site Survey

The site survey, determines the best frequency and access point locations for the most reliable coverage. If you have 5 or more Wi-Fi phones, hire a professional to do your site survey for you.

The survey will tell you the best places to mount your access points and advise you about:

- Platform type
- Antenna type
- Configurations for channel and transmit power

From the survey, you will also learn if there are other Wi-Fi devices or obstacles preventing good signal strength being available to the phone. A common mistake made by end users is assuming that because their present signal strength provides good coverage for email; streaming audio and video; and browsing; that calling should not be a problem. In fact, the demands of sustaining good quality audio or video calls are different than they are for other commonly used web or Internet applications. A good site survey will reveal any potential problems that may be mitigated by moving the access points to new locations or adding more access points to your network or using a more appropriate type of access point for your worksite.

Recommendations for Wi-Fi Characteristics:

Signal

The signal coverage for the phone must be no lower than -67 dBm to ensure that the phone always has an adequate signal.

Channel Utilization

Channel Utilization levels must be kept under 40%.

The phone converts the 0-255 scale value to a percentage: 105 is equivalent to 40% on the phone.

Noise

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

Make sure the upstream signal from the phone meets the access point's SNR for the transmitted data rate.

Packet Loss / Delay

Per voice guidelines, packet loss must not exceed 1%. Otherwise, the voice quality can be degraded significantly. Jitter must be kept at the minimal (< 100 ms).

Retries

802.11 retransmission must be less than 20%.

Multipath

Multipath must be avoided or kept to the minimal to create nulls and reduce signal levels.

Number of allowed devices

AP's support a maximum quantity of 10 connected devices.

Protocols

The Wi-Fi phones all support these wireless LAN protocols:

- 802.11a: best for voice
- 802.11b: best for data
- 802.11d
- 802.11e
- 802.11g: best for data
- 802.11h
- 802.11i
- 802.11n: best for voice or data

The 8861, 8865 also support

- 802.11r
- 802.11ac: best for voice

The Phones can support these features in wireless LAN protocols:

- Wi-Fi Multimedia (WMM)
- Traffic Specification (TSPEC)
- Traffic Classification (TCLAS)

Interference Sources

The ideal situation is to always have the access point and the phone in a line of sight to each other. Line of sight is a straight physical path between the access point and the phone without obstruction. Any interference or RF attenuation materials in the line of sight reduces the coverage distance.

This section identifies common interference sources for 802.11.

Attenuation Sources

Every type of RF attenuation material may have unique characteristics.

The table provides the attenuation level for each type of material. The thickness of the material also plays a significant role in the attenuation. The thicker the material, the higher the attenuation.

- If the wood material is thick, the attenuation level may change from low to medium. Example: a solid core door.
- If the glass door is very thick, the attenuation level may change from medium to high. Example: a double set of glass doors enclosing a vestibule.
- If there are tiles on both sides of the walls, attenuation is almost doubled through the wall

Material	Level of Attenuation	Comments
Wood	Low	Doors, floors, and so on
Plastics	Low	Room partitions
Tinted Glass	Medium	Wall hangings, glass door, and window

Material	Level of Attenuation	Comments
Living Objects	Medium	Crowds, and Plants
Bricks	Medium	Walls
Ceramic	High	Tiles
Concrete	High	Walls, pillars, floors, and stairs
Metal	Very High	Elevator, and cabinet

Microwave Ovens

Microwave ovens operate on 2.450 GHz, which is between channels 8 and 9 of 802.11b/g/n. Microwaves impact channel 11, and poorly shielded microwave ovens can affect the entire frequency range (channels 1 through 11). To avoid interference, select channel 1 for use with access points that are located near microwave ovens.

Most microwave ovens do not affect the 5 GHz frequency.

Cordless Phones

Some sites have 5.8 GHz cordless phones, which can impact UNII-3 channels.

Bluetooth

Bluetooth is another potential source of interference on the 2.4 GHz spectrum. The Cisco IP Phone 8861 and 8865 support Bluetooth headsets. If the phone is connected to the WLAN and the end user has a Bluetooth headset, use 5 GHz for the WLAN. If there are other Bluetooth devices being used at the worksite that are not interacting with the phone, keep those devices at least 10 feet away from the phone so that they will not interfere with the Bluetooth headset.

For optimum performance from a Bluetooth headset, follow the same best practices as you would for Wi-Fi. A 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 signal quality.

Bluetooth was designed for use with a single connected nearby host in a remote environment like a home office, a car, or while the user is walking around with their headset connected to the cell phone in their pocket or purse. Bluetooth was not designed for use in an office full of other Bluetooth users as it does not perform well when other nearby devices, that are within 10 feet, are using the same frequency range. For users in a busy office, use a corded or DECT headset with the phone.

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

Coexistence

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

Capacity

When using coexistence, call capacity is reduced due to the utilization of CTS to protect the Wi-Fi and Bluetooth transmissions.

Voice Quality

Depending on the current data rate configuration, CTS may be sent to protect the Bluetooth transmissions when using Coexistence.

In some environments, real-world should be 6 Mbps or above. For more information see Supported Spectrum.

It is recommended to use 5GHz. If only 2.4 GHz can be used, it is recommended to use 802.11a/n/ac.

Recommended Practices

- Use 5 GHz for the Wi-Fi phones.
- Use automatic channel selection instead of manually assigning channels to access points.
- If there is an intermittent interreference, then the access point or access points serving that area may need to have a channel statically assigned. Otherwise, use dynamic channel assignments.
- Use a signal of -67 dBm or higher when using 5 GHz or 2.4 GHz
- Make sure the Packet Error Rate (PER) is no higher than 1%.
- Maintain a minimum Signal to Noise Ratio (SNR) of 25 dB = -92 dBm noise level with -67 dBm signal.
- If there are two access points at the phone installation site, use non-overlapping channels with at least -67 dBm signal with the 25 dB SNR to provide redundancy.
- To achieve maximum capacity and throughput, use a 24 Mbps design.
- 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, configured as a mandatory / basic rate.

Data Rates

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.

Wireless enabled Cisco IP Phone have a single antenna therefore it supports up to 150 Mbps for 802.11n and up to 433 Mbps for 802.11ac.

If 802.11b clients are not allowed in the wireless network, then disable the data rates below 12 Mbps. This will eliminate the need to send CTS frames for 802.11g and 802.11n protection as 802.11b clients cannot 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 or basic rate.

For a voice only application, data rates higher than 24 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.

For a video application, enabling higher data rates is recommended. To preserve high capacity and throughput, enable data rates of 24 Mbps and higher.

If deploying in an environment where excessive retries may be a concern, then a limited set of the data rates can be used, where the lowest enabled rate is the mandatory or basic rate.

For rugged environments or deployments requiring maximum range, enable 6 Mbps as a mandatory or basic rate.

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 or basic rate. Multicast packets will be sent at the highest mandatory or basic data rate enabled.

Note:Capacity and throughput are reduced when lower rates are enabled.

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.

Following is the 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

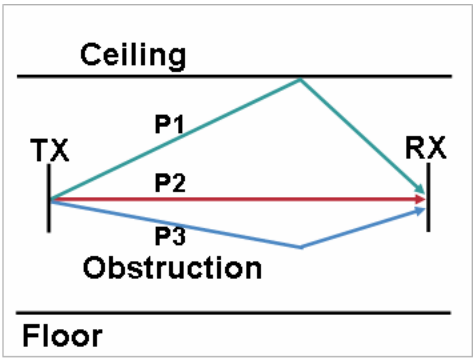
Occurs when the reflected waves arrive out of phase to some extent with the main signal thereby reducing the signal amplitude

Use of Orthogonal Frequency Division Multiplexing (OFDM), which is used by 802.11a, 802.11g, 802.11n, 802.11ac, 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.

The following diagram shows the multipath effects.



Security Modes

When deploying a wireless LAN, security is essential. The phone supports the following wireless security modes.

Wi-Fi Security mode

Wireless enabled Cisco IP Phone with Multiplatform Phone firmware supports the following Wi-Fi Security modes:

- Auto
- EAP-FAST
- PEAP-GTC
- PEAP-MSCHAPV2
- PSK
- WEP
- None

Auto

Auto mode is used only when accessing free Wi-Fi. This may be useful if these phones are used when the authentication to login to Wi-Fi keeps changing based on the user.

In general, it is rare to use "Auto" mode for Wi-Fi access on the desk phones. This is very similar to the password that is given to access a hotel's Wi-Fi service.

Auto mode will require you to enter "User ID" and "Password".

Required Configuration:

Setup User ID and password for login access in the backend for auto login. This User ID and Password are entered on the phone.

EAP-FAST

EAP-FAST stands for Extensible Authentication Protocol – Flexible Authentication via Secure Tunneling.

The username and password must be setup by the access point administrator before it can be entered on the phone.

Required Configuration

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) or Cisco Identity Services Engine (ISE).

EAP-FAST supports automatic Protected Access Credentials (PAC) provisioning, but it must be enabled on the RADIUS server. To enable EAP-FAST, install a certificate onto the RADIUS server.

The Wi-Fi phones support automatic provisioning of the PAC only. Enable Allow anonymous in-band PAC provisioning on the RADIUS server as shown below. Enable both EAP-GTC and EAP-MSCHAPv2 when enabling Allow anonymous in-band PAC provisioning.

Create a user account with a password on the authentication server for EAP-FAST. Enter this username and password on the phone.

PEAP-GTC

PEAP-GTC stands for Protected Extensible Authentication Protocol - Generic Token Card.

The username and password must be set by the access point administrator before it can be entered in the phone.

Required Configuration

Protected Extensible Authentication Protocol (PEAP) uses server-side public key certificates to authenticate clients by creating an encrypted SSL/TLS tunnel between the client and the authentication server. The ensuing exchange of authentication information is then encrypted, and user credentials are securely protected from eavesdropping.

PEAP requires that a user account be created on the authentication server. The authentication server can be validated via importing a certificate into the Cisco IP Phone.

PEAP-MSCHAPV2

PEAP-MSCHAPV2 stands for Protected Extensible Authentication Protocol - Microsoft Challenge Handshake Authentication Protocol Version 2. The username and password must be set by the access point admin to enter in the phone.

Required Configuration

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

The ensuing exchange of authentication information is then encrypted and user credentials are safe from eavesdropping. PEAP requires that a user account be created on the authentication server. The authentication server can be validated by importing a certificate into the Cisco IP Phone.

PSK

PSK stands for Pre-Shared Key.

Passphrase is required for PSK.

Required Configuration

In the Wireless access point, it may be configured as one of WPA variants as listed below:

WPA2-PSK (AES):

Wireless Protected Access 2 with Pre-Shared key. This uses AES (Advanced Encryption Standard) for encryption. It is recommended to use WPA2-PSK for small and home office environments where RADIUS server is not available.

WPA-PSK (TKIP):

Wireless Protected Access with Pre-Shared key. This uses TKIP (Temporal Key Integrity Protocol) for encryption. This method allows a better security than WEP or no security.

WPA or WPA2:

Wireless Protected Access 2 with 802.1x authentication. This requires RADIUS (Remote Authentication Dial-in User Service) authentication Server to provide authentication services. Admin of the RADIUS server should be able to provide the authentication details needed.

All of the above requires a passphrase that should be configured on the access point. The same passphrase must be entered on the Cisco IP Phone as well.

WEP

WEP stands for Wired Equivalent Protocol. The Wi-Fi phone needs a WEP Key to authenticate with the service.

WARNING: This method of authentication is sub-optimal as it has been proven to be vulnerable to hacking. This method has been superseded by the PSK mechanisms that are discussed above. Most commercially available Wi-Fi access points supports at least one of the modes of the PSK listed above. It is recommended to use PSK at the least.

Required Configuration:

This requires WEP Key to be configured on the access point. Same WEP Key should be entered on the phone.

None

If you chose None, there is no security at all.

The phone will be able to connect to the access point just with SSID, if access point allows None.

WARNING: It is not recommended to use No Security for wireless communications as eavesdropping is very easy.

Recommended Security Mode

Most commercially available Wi-Fi Access Points supports WPA/PSK method. Advanced Access points will support PEAP-GTC, PEAP-MSCHAPV2 and EAP-FAST.

If any one of the PEAP-GTC, PEAP-MSCHAPV2 or EAP-FAST is available, it is recommended to use these mechanism as they provide better security at the wireless layer.

If those mechanisms are not available, it is recommended to use one to WPA/PSK method. Among WPA/PSK methods, WPA2-PSK is recommended.

It is NOT advisable to use WEP or None as Security Mode due to Security Concerns that these mechanisms provide.

Wi-Fi Profile Management

Cisco IP Phones with Multiplatform Phone firmware allows Wi-Fi profiles to be managed remotely through configuration. This capability enables Service Providers who manage the Wi-Fi access points and the Cisco IP Phones with Multiplatform Phone firmware on the install premise.

Remote Provisioning of Wi-Fi Profile

Steps involved in the remote configuration of Wi-Fi Profile is as follows:

1. Connect the phone to the Ethernet network and obtain an IP address
2. The phone connects to the Service Provider provisioning server
3. The provisioning file containing the Wi-Fi Profile is sent to the phone
4. Remove the ethernet and power from the phone
5. The phone reboots and connects with Wi-Fi profile given in the provisioning file

By pushing a new configuration file via Re-sync, Wi-Fi profile can be managed.

Service provider need to design and plan Remote Provisioning by referring to "Cisco IP Phone Multiplatform Phone Administration Guide"

Wi-Fi Profile Setup

The Wi-Fi phones can accept up to 4 Wi-Fi Profiles that can be configured with an assigned priority order. For Security purposes, you can turn off the Wi-Fi radio, and always use the wired connection.

Refer to *Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide* and *Cisco IP Phone 6800 Series Multiplatform Phones Administration Guide* for more information. For quick reference, the Wi-Fi profile parameters are given here.

```
<!-- Wi-Fi Settings -->
<Phone-wifi-on ua="rw">Yes</Phone-wifi-on>
<!-- Wi-Fi Profile 1 -->
<Network_Name_1_ ua="rw">SSID </Network_Name_1_>
<!-- available options: Auto|EAP-FAST|PEAP-GTC|PEAP-
   MSCHAPV2|PSK|WEP|None -->
<Security_Mode_1_ ua="rw">Auto</Security_Mode_1_>
<Wi-Fi_User_ID_1_ ua="rw"/>
<!-- <Wi-Fi_Password_1_ ua="rw"/> -->
<!-- <WEP_Key_1_ ua="rw"/> -->
<!-- <PSK_Passphrase_1_ ua="rw"/> -->
<!-- available options: Auto|2.4 GHz|5 GHz -->
<Frequency_Band_1_ ua="rw">Auto</Frequency_Band_1_>
<!-- available options: 1|2|3|4 -->
<Wi-Fi_Profile_Order_1_ ua="rw">1</Wi-
   Fi_Profile_Order_1_>
```

Trouble Shooting Tips

Not able to see SSID on the phone

Check whether the Access point is powered on. And redo "Scan" on the phone.

On the phone, navigate to Settings -> Network Configuration -> Wi-Fi Configuration -> Wi-Fi Profile. In the screen, the phone may list the known and/or configured SSID. Press the softkey "Scan". This will refresh the list of SSID that are seen now.

Wi-Fi Scan does not result in any result

Check whether the Access point is powered on. Check there are no high attenuation objects in the line-of-sight between the phone and the access point. Refer to "Interference Sources" section.

Error "Wi-Fi must be enabled"

If you see this error on the phone screen, Wi-Fi is disabled by configuration. Press OK to dismiss the error. Go to Settings -> Network Configuration -> Wi-Fi Configuration. Turn "On" Wi-Fi by pressing the right or left key on the navigation cluster and press "Set"

Error "Ethernet must be disconnected to use Wi-Fi"

If you see this error on the phone screen, the phone has Ethernet connected to a switch. The phone will automatically choose ethernet if it is connected. The Ethernet must be disconnected. As Ethernet cannot be used, PoE and Wi-Fi cannot be used together. Use wall power for the phone.

How to check that the Wireless is connected?

On the phone, go to Settings -> Status -> Network Status. Check "Network type" is "Wireless" and "Network Status" is "Connected"

Go into, "IPv4 Status" or "IPv6 Status" to get the IP address of the phone.

Which Wi-Fi Network (i.e. SSID) is the phone is connected to?

To find which SSID phone is connected to, Go to Settings -> Network Configuration and check the value against "Wi-Fi Configuration". This is the Wi-Fi Network that the phone is connected to.

Note, the phone will order in the Wi-Fi Profile list to attempt to connect. If you see that, the phone is connected to wrong SSID, it may be because the Wi-Fi profile order OR the configuration of the SSID profile.

Further if you select "Wi-Fi Configuration" -> Wi-Fi Profile, the phone will show a green tick against the Wi-Fi network name to show that SSID is connected. Here the phone will show the wireless strength as well – highlight strength as number of bars out of 4 bars. (This is typical Wi-Fi icon to show the strength seen)

Error "You need to configure the network to enable the call features"

The phone will give two options "Wi-Fi Scan" and "Cancel". If the phone is in new Wi-Fi network, press "Wi-Fi Scan" to see the new Wi-Fi network and configure it. If the phone has the Wi-Fi network already configured, probably some of the settings including username, password OR SSID name has changed. In that case, press "Cancel", go to Settings -> Network Configuration -> Wi-Fi Configuration -> Wi-Fi Profile.

In this screen select the Wi-Fi network to connect to and check the configuration and/or re-enter the authentication details.

Number of bars in the Wi-Fi icon

The phone will always show 4 bars. But the actual strength is displayed with dark color (either blue or dark grey depending on the phone being used) to show out of 4 bars, how much is seen.

Network configuration is correct, but still, the phone does not get IP address

There are some corner configurations that cause this trouble. On the phone, go to Settings -> Network Configuration and check the value of "IP mode". Make sure it is the desired value. Possible values are "Dual mode", "IPv4 Only" and "IPv6 Only". Recommended is "Dual mode". Refer to "Cisco IP Phone Multiplatform Phone Administration Guide"

OR May be DHCP is providing the correct IP address. In that case, check "IPv4 address settings" and "IPv6 address settings" per your network

Appendix:

Abbreviations

For the purpose of this document, the following abbreviations are used:

- AP Access Point
- DHCP Dynamic Host Configuration Protocol
- EDOS/CDA Cisco Device Activation Service
- CTS Clear to Send
- LAN Local Area Network
- PoE Power over Ethernet
- RF Radio Frequency
- RTS Ready to Send
- SSID Service Set Identifier. Also known as Network Name
- SKU Stock Keeping Unit
- WLAN Wireless LAN

SKUs

Refer to the data sheet for more and latest information.

CP-8861-3PW-AU-K9=	Cisco IP Phone 8861 shipped with multiplatform phone firmware, and with a power cube and a power cord for Australia and New Zealand
CP-8861-3PW-NA-K9=	Cisco IP Phone 8861 shipped with multiplatform phone firmware, and with a power cube and a power cord for North America
CP-8861-3PCC-K9= CP-PWR-CUBE-4 CP-PWR-CORD-CE=	Cisco IP Phone 8861 shipped with multiplatform phone firmware Power cube and a power cord for Europe are ordered separately
CP-8861-3PCC-K9= CP-PWR-CUBE-4 CP-PWR-CORD-UK=	Cisco IP Phone 8861 shipped with multiplatform phone firmware Power cube and a power cord for United Kingdom are ordered separately
CP-8865-3PW-NA-K9=	Cisco IP Video Phone 8865 shipped with multiplatform phone firmware, and a power cube and a power cord for North America
CP-8865-3PCC-K9= CP-PWR-CUBE-4 CP-PWR-CORD-CE=	Cisco IP Phone 8865 shipped with multiplatform phone firmware Power cube and a power cord for Europe are ordered separately
CP-8865-3PCC-K9= CP-PWR-CUBE-4	Cisco IP Phone 8865 shipped with multiplatform phone firmware Power cube and a power cord for United Kingdom are ordered separately

CP-PWR-CORD-UK=	
CP-8865-3PCC-K9= CP-PWR-CUBE-4 CP-PWR-CORD-AU=	Cisco IP Phone 8865 shipped with multiplatform phone firmware Power cube and a power cord for Australia and New Zealand are ordered separately
CP-6861-3PW-NA-K9=	Cisco IP Phone 6861 with power adapter for North America
CP-6861-3PW-CE-K9=	Cisco IP Phone 6861 with power adapter for Europe
CP-6861-3PW-UK-K9=	Cisco IP Phone 6861 with power adapter for the United Kingdom
CP-6861-3PW-AU-K9=	Cisco IP Phone 6861 with power adapter for Australia/New Zealand

Supported Frequencies and Channels

The following table lists the frequencies and channels that Cisco IP Phone Multiplatform Phones support.

Part Number	Description	Peak Antenna Gain	Frequency Ranges	Avail. Chan.'s	Channel Set
CP-6861-3PW-CE-K9= CP-6861-3PW-AU-K9= CP-6861-3PW-CE-K9= CP-6861-3PW-NA-K9= CP-6861-3PW-UK-K9=	Cisco MPP Phone 6861	2.412-2.472GHz: 2.44 dBi 5.150-5.350GHz: 0.53 dBi 5.470-5.725GHz: 0.7 dBi	2.412 - 2.472 GHz 5.180 - 5.240 GHz 5.260 - 5.320 GHz 5.500 - 5.700 GHz 5.745 - 5.825 GHz	13 4 4 11 5	1-13 36, 40, 44, 48 52, 56, 60, 64 100-144 149, 153, 157, 161, 165
CP-8861-3PCC-K9= CP-8861-3PW-AU-K9= CP-8861-3PW-NA-K9=	Cisco MPP Phone 8861	2.4 GHz = 3.2 dBi 5 GHz = 2.4 dBi	2.412 - 2.472 GHz 5.180 - 5.240 GHz 5.260 - 5.320 GHz 5.500 - 5.720 GHz 5.745 - 5.825 GHz	13 4 4 12 5	1-13 36, 40, 44, 48 52, 56, 60, 64 100-144 149, 153, 157, 161, 165
CP-8865-3PCC-K9= CP-8865-3PW-AU-K9= CP-8865-3PW-NA-K9=	Cisco MPP Phone 8865	2.4 GHz = 2.1 dBi 5 GHz = 1.9 dBi	2.412 - 2.472 GHz 5.180 - 5.240 GHz 5.260 - 5.320 GHz 5.500 - 5.720 GHz 5.745 - 5.825 GHz	13 4 4 12 5	1-13 36, 40, 44, 48 52, 56, 60, 64 100-144 149, 153, 157, 161, 165

Notes:

- 802.11j (Channels 34, 38, 42, 46) are not supported
- Channel 14 for Japan is not supported
- 6861 comes with Power cube
- 8861 & 8865 requires Power-cube to operate in wireless mode

Regulatory

World Mode (802.11d) allows a client to be used in different regions, where the client can adapt to use the channels and transmit powers advertised by the access point in the local environment.

The phone operates best when the access point is 802.11d-enabled. The AP can determine the channels and transmit powers per the local region.

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 to be 802.11h-compliant to utilize those radar frequencies (DFS channels). 802.11h requires 802.11d to be enabled.

The Cisco IP Phone with Multiplatform Phone firmware will passively scan DFS channels first before engaging in active scans of those channels.

If 802.11d is not enabled, then the phone can attempt to connect to the access point using reduced transmit power.

Below are the countries and their 802.11d codes that the phone supports.

Argentina (AR)
Australia (AU)
Austria (AT)
Bahrain (BH)
Belgium (BE)
Brazil (BR)
Bulgaria (BG)
Canada (CA)
Chile (CL)
Colombia (CO)
Costa Rica (CR)
Croatia (HR)
Cyprus (CY)
Czech Republic (CZ)
Denmark (DK)
Dominican Republic (DO)
Ecuador (EC)
Egypt (EG)
Estonia (EE)
Finland (FI)
France (FR)
Iceland (IS)
India (IN)
Ireland (IE)
Israel (IL)
Italy (IT)
Japan (JP)
Korea (KR)
Latvia (LV)
Liechtenstein (LI)
Lithuania (LT)
Luxembourg (LU)
Macau (MO)
Macedonia (MK)
Malaysia (MY)
Malta (MT)
Mexico (MX)
Monaco (MC)
Montenegro (ME)
Netherlands (NL)
New Zealand (NZ)
Nigeria (NG)
Philippines (PH)
Poland (PL)
Portugal (PT)
Puerto Rico (PR)
Romania (RO)
Russian Federation (RU)
Saudi Arabia (SA)
Serbia (RS)
Singapore (SG)
Slovakia (SK)
Slovenia (SI)
South Africa (ZA)
Spain (ES)
Sweden (SE)
Switzerland (CH)
Taiwan (TW)
Thailand (TH)
Turkey (TR)
Ukraine (UA)
United Arab Emirates (AE)
United Kingdom (GB)

Germany (DE)
Gibraltar (GI)
Greece (GR)
Hong Kong (HK)
Hungary (HU)
Norway (NO)
Oman (OM)
Panama (PA)
Paraguay (PY)
Peru (PE)
United States (US)
Uruguay (UY)
Venezuela (VE)
Vietnam (VN)