

How to get your 8821/792x wireless phones performing reliably

Contents

[Introduction](#)

[Voice over WLAN - a challenging technology](#)

[Seven basic guidelines to making VoWLAN work well](#)

[1. Have solid coverage in 5GHz - and lock your phones to 802.11a](#)

[2. Run current phone firmware](#)

[3. If using FlexConnect local switching, enable ARP caching](#)

[4. Use WPA2/AES EAP with Fast Secure Roaming - beware TKIP](#)

[5. Optimize channels, power, and data rates](#)

[6. Enable continuous scan mode \(in CUCM\)](#)

[7. Configure all QoS, and everything else, exactly as documented in the Deployment Guides](#)

[Conclusion](#)

[Related Information](#)

Introduction

This document explains how to get Cisco 8821 and 792x wireless phones (7921G, 7925G, 7926G) to work well in a Cisco Unified Wireless Network.

Voice over WLAN - a challenging technology

Voice over WLAN (VoWLAN) is one of the most challenging technologies that Cisco provides. For VoWLAN to work satisfactorily - especially in the high-stress environments in which it is deployed, such as healthcare - the network, and the phone, must be able consistently to transport a real-time, bidirectional, securely encrypted audio stream, with almost no dropouts, while the endpoint moves across four dimensions (space and frequency).

Seven basic guidelines to making VoWLAN work well

Though delivering a reliable VoWLAN service is difficult, it **is** possible, provided that the network provider adheres to the following basic design guidelines.

1. Have solid coverage in 5GHz - and lock your phones to 802.11a

Your network's ability to perform is fundamentally dependent on a solid physical layer. VoWLAN uses both the 2.4GHz and 5GHz bands. Of these, the 2.4GHz band's lower frequency signals carry further - however, the constrained bandwidth (only three non-overlapping channels) and ever increasing interference, render 2.4GHz, in most cases, unsuitable for reliable voice. Network providers who want to deliver a reliable VoWLAN service will ensure that their design adheres to the following standard:

Every spot in the coverage area is serviced by at least **two viable 5GHz access points, at - 67dBm or stronger.**

You can easily validate the necessary coverage by setting your phone into site survey mode, and walking throughout your coverage area.

Additionally, AP placement, antenna selection, building construction, etc. must be such that **multipath distortion is kept to a minimum**. To ensure gap-free roaming, **a moving phone must be able to hear each roamed-to AP at least 5 seconds before it needs to roam to it** - so place all APs in the middle of halls, at corridor junctions, etc., rather than in blind spots.

2. Run current phone firmware

On the 792x: run 1.4.7 - nothing earlier

1.4.7 firmware or above is strongly recommended, due to the [CSCut25250 \(Phones stops sending SCCP messages\)](#) fix.

On the 8821: run the latest firmware

If you encounter problems with the latest firmware, contact TAC.

3. If using FlexConnect local switching, enable ARP caching

If using FlexConnect local switching, **make sure to enable ARP caching** (i.e. the AP ARPing on behalf of the wireless client), for the sake of reliability and phone battery lifetime. ARP caching is supported with FlexConnect local switching starting in 8.0.120.0 (see [CSCut14210](#)).

Other key concerns for FlexConnect for 792x phones:

- Fast Secure Roaming via CCKM is supported only among APs within the same FlexConnect group. As the number of APs within a Flex group is limited (for example, on the 5508 WLC, to 25 APs), FlexConnect is not suited to large deployments.
- Inter-AP roaming does not work between FlexConnect APs in standalone mode ([CSCuj22730](#))
- [CSCuw31813](#) Flex local auth, client roaming in-out-in during dot1x (fixed in 8.2, 8.0.120.10)

If your WAN link between the APs and the WLC is high latency, unreliable, or low bandwidth, then consider installing a WLC at the site where the phones are.

4. Use WPA2/AES EAP with Fast Secure Roaming - beware TKIP

For 8821: use WPA2/AES Enterprise with 802.11r (FT over the air)

The recommended security scheme for 8821 phones is **WPA2/AES Enterprise with 802.11r (FT over the air.)**

For 792x: use WPA2/AES Enterprise with CCKM.

WPA2/AES Enterprise with CCKM Fast Secure Roaming is the recommended security scheme

for 792x phones - it is the most secure method, and provides for the fastest roaming times.

(When using CCKM, use the WLC command "config wlan security wpa akm cckm timestamp-tolerance 5000" to increase the likelihood of performing a fast roam.)

- Special considerations for using CCKM:
 - See the [CCKM Client Disconnect Bugs in 7.0/7.2](#) tip
 - If using CCKM with AP1131/1242 in 8.0, beware [CSCuu49291](#) (7925 decrypt errors with AP1131 running 8.0 code), fixed in 8.0.132.0.

You may use Local Authentication on the WLC, if you do not want to use an external RADIUS server. (Note: Local Authentication with EAP-FAST does not work with the 792x in 8.0.140.0 or 8.3 - track [CSCvb44979](#) [WLC Local EAP with 7925 Handshake Failure] for the fix.

Avoid TKIP which is less secure, and is susceptible to MIC error triggered service interruptions. TKIP unicast ciphers are not supported with the 8821.

PSK: Although WPA2/AES Enterprise is the preferred security method, in some cases WPA2/AES-Preshared Key (PSK) will be used. For example, if FlexConnect APs have only a high latency, unreliable WAN path to a RADIUS server, then PSK with FlexConnect Local Authentication may be the best choice.

Note: For VoWLAN deployments operating both 792x and 8821 phones,

- Enable both CCKM and 802.11r (FT over the air) on the WLAN. In this scenario, 792x would use CCKM and 8821 would use 802.11r.
- Enabling FT PSK option will make 8821 phones use 802.11r Fast secure roaming and 792x phones to resort to PSK.

If using PSK with 7925G phones, do be aware of:

[CSCtt38270](#) 7925 sometimes takes 1+ second to respond to WPA M1 key message

This bug does not affect 7921G or 7926G phones. The problem can be mitigated to some extent with: **config advanced eap eapol-key-timeout 250** on the WLC, and by disabling Java on the phone (if using 1.4.6.3 firmware or above)

5. Optimize channels, power, and data rates

- **channels:** use at least 8 channels (if available in your regulatory domain) use channels from UNII-1 (36-48), UNII-2 (52-64), UNII-2 Extended (100-140), and/or UNII-3 (149-161 but **not** 165) if coverage is weak, avoid channels with lower power limits if radar detection is frequent, avoid the DFS channels (UNII-2, UNII-2 extended)
- **power:** in 5GHz, use a minimum power level of at least 11dBm in all 5GHz deployments but the very densest ones, you can simply set a power level of 1 (maximum)
- **data rates:** the Deployment Guide (see below) recommends a minimum data rate of 12Mbps if there is significant multipath in the environment, or if the 5GHz coverage is marginal, set 6Mbps as the lowest mandatory rate, and be sure that 12 and 24Mbps are enabled

Note:

1. Remember to make any changes on **all** WLCs in the RF group

2. For 8821 phones, beware of [CSCvd06463](#) IOS AP doing AMSDU aggregation for voice traffic in queue 0 despite BA req declined by 8821. Workaround is to disable AMSDU from all queues.

WLC CLI command:

config 802.11a disable network
config 802.11a 11nSupport a-msdu tx priority all disable
config 802.11a enable network

6. Enable continuous scan mode (in CUCM)

For 792x: continuous scan mode should be enabled; however idle battery life can be reduced to some extent. (A fresh battery should still last an 8-hour shift.) Without continuous scan mode, the AP may be intermittently associated to an AP with a weak signal, which may have an rare impact on incoming calls and pages

For 8821: continuous scan mode is enabled by default. Do not change this setting

7. Configure all QoS, and everything else, exactly as documented in the Deployment Guides

Go through the entire [7925G Deployment Guide](#), and/or [8821 Deployment Guide](#), and configure the phones and the wireless network as per its recommendations. In particular, make sure that all QoS configurations are set as per best practice, throughout your wireless and wired network.

Conclusion

With strict adherence to every single one of the above guidelines, there is a high probability that your VoWLAN service will meet your clients' performance expectations.

Related Information

- [Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Deployment Guide](#)
- [8821 Deployment Guide](#)
- [792x discussion in Cisco Support Community](#)
- [TAC Recommended AireOS](#)