CHAPTER 2

General Troubleshooting Guidelines

Common VoWLAN Problems

- Choppy Audio / No Audio
- One-Way Audio
- Clipping, Echo
- Gaps in Audio / No Audio when Roaming

In many cases, all of the above symptoms may be the result of problems within the RF environment. This can either be due to poor signal, no signal, or asymmetric transmit where the client can hear the AP, but the AP cannot hear the client (one-way audio). In some instances we discover that it might be a misconfiguration or a problem with the physical network, such as QoS misconfiguration or a lack of trust as it relates to QoS Differentiated Service Code Point (DSCP) markings, or perhaps a gateway misconfiguration that causes an impedance mismatch resulting in echo when a Voice Over Wireless LAN (VoWLAN) user makes a call onto the PSTN. This document will place a great deal of emphasis on understanding RF propagation and stress the importance of performing a site survey as it relates to thorough RF planning.

As we mentioned in the first chapter, gathering facts about the problem is the most crucial and fundamental aspects of troubleshooting a VoWLAN problem. When a customer experiences a VoWLAN problem and is unable to isolate root cause on their own, they contact the Cisco Technical Assistance Center and open a Service Request (SR). Upon opening the SR, the Customer Support Engineer will usually review the problem description and ask for additional information based on the reported problem. In most VoWLAN cases, the TAC CSE will ask for a Network Topology Diagram, configurations for the Wireless LAN Controllers, and/or message logs and respective debugs from the equipment in question.

General Troubleshooting Questions

1. What version of code is installed on the Wireless LAN Controller?
2. What is the firmware version installed on the Cisco 792xG Series wireless IP phone?
3. What kind of AP is in use?
4. If the Access Point utilizes external antennas, what type of antenna is in use, what is the gain, is the gain configured correctly and is diversity enabled?
   - In some cases, it is ideal to get photographs of the antenna placement and direction where RF might be considered as the root cause of the problem.

5. Is the AP in local or HREAP mode?
6. Has the problem or symptom been experienced by users before?
   - Is the problem intermittent or reproducible?
7. Were there any recent changes made to the LAN or WLAN recently?
8. In the case of choppy or one-way audio, does the issue happen throughout the entire WLAN or in one particular area?
9. Is the client roaming when the problem is observed or stationary?
   - This is sometimes a tricky question to answer. In poorly deployed environments, a voice handset may actually roam several times even when stationary due to RF related problems and an RSSI differential.

     `Example`
     If we miss five back to back ACKs, the Cisco 792xG Series wireless IP phone will attempt to roam. We will discuss this in greater depth in the section on troubleshoot the 792xG Series wireless IP phone.
   - If the client is roaming, the systems engineer can run a Client Association Report in WCS to track which access points the clients roam between.
   - Power and Channel Change Report - Displays how frequently Radio Resource Management (RRM) adjusted the Transmit Power Control and Dynamic Channel Allocation modified the channel for each access point.
10. How many instances of Coverage Hole Alarms (CHA) were run when the problem was experienced?
11. Are calls made from a wired IP Phone to wireless, wireless to wireless, or wireless over the PSTN?
    - Understanding the call path is very important when troubleshooting VoWLAN cases.

Note If the configuration and RF analysis has been validated and meets the appropriate design and deployment best practices as outlined in Cisco documentation, perform the following steps to further analyze the problem.

Site Survey Questions

1. Did you perform a site survey?
   - If yes, please provide survey documentation.
2. If no in question 1., did you perform a post site survey after the wireless network was deployed?
   - If no, review heat maps in WCS.

Note WCS heat maps are predictive based on the configuration of antenna direction and gain in WCS. If WCS was not configured with those parameters, it will not provide even a predictive representation of RF propagation. WCS is should not be used as a pre- or post-site survey tool.

3. Review wired and wireless configurations. Use the configuration tool to isolate configuration criteria for the deployment when using the 792xG Series wireless IP phones. Discussed later in this chapter.
4. Use the Voice Audit tool in WCS to validate the voice configuration.

Note The audit results are based on the user configured criteria in the audit tool itself. If the criteria configured does not already adhere to Cisco documented VoWLAN best practices, you should configure the criteria in the audit tool to match accordingly. This will ensure the configuration adheres to the appropriate best practices. The Cisco Configuration Analyzer has VoWLAN checks for the 792xG Series wireless IP phones and is based on Cisco VoWLAN design and deployment best practices. This is the most ideal tool for analyzing configuration requirements.

5. Is QoS implemented end to end?
   - If yes, move on.
   - If no, remediate and ensure that packets are trusted appropriately.
6. Perform RF Analysis and ensure that uplink packets are queued correctly.
   - Ensure that the client has enough signal to communicate efficiently with the AP.
7. Is RRM enabled?
   - If yes, what code version is in use?
8. Did the customer implement transmit power throttling to define a Min and Max transmit power?
   - If transmit power throttling is not enabled, verify symmetric vs. symmetric transmit (Compare Client transmit to AP transmit).

The following is a checklist that is recommended when troubleshooting a VoWLAN. It also defines best practices and additional options that may need to be taken into consideration.

Table 2-1 VoWLAN checklist

Recommendation	Best Practice	May Consider	Done
Verify an AP can be seen from the phone at -67 dBm or better in all areas to be covered. You also need to verify that the AP sees the phone at -67 dBm or better in all areas as well.	X		
Ensure that the SNR is always 25 dB or higher in all areas to provide coverage.	X		
Verify that channel utilization is under 50%.	X		
Configure voice WLAN to use the 802.11a band.		X	
If using EAP authentication, ensure that fast roaming is supported such as CCKM.	X		
WMM should be allowed or required for the voice WLAN.	X		
Voice WLAN should be marked with Platinum QoS.	X		
Platinum QoS profile should have the 802.1p bits set to 6.	X		
Verify the switch ports used to connect to the controller are set to trust CoS and ports to APs and uplinks are set to trust DSCP.	X		
Verify that Call Admission Control is enabled globally for the radios.	X		

Table 2-1 VoWLAN checklist (continued)

Recommendation	Best Practice	May Consider	Done
Verify that Load-based CAC is enabled under Call Admission Control.	X		
Ensure that Load Based CAC (7920 AP CAC) under the WLAN is enabled for the voice WLAN if the network has a mix of 7920 and 792xG Series wireless IP phones.	X		
Ensure that Client Based CAC (7920 Client CAC) under the WLAN is disabled for the voice WLAN.	X		
Verify that the EDCA profile on the controller is set to Voice Optimized.	X		
Verify that Low Latency MAC is disabled.	X		
Verify that the 12 Mbps data rate is enabled (default PHY rate of the phone).	X		
If using 802.11b/g disable the 1, 2, 5.5, 6, and 9 Mbps data rates if possible.	X		
If using 802.11a disable the 6 and 9 Mbps data rates if possible.	X		
Verify coverage is designed for 24 Mbps to maximize throughput. Optionally disable 36-54 Mbps.		X	
Optionally disable 36-54Mbps			
Verify that Aggressive Load Balancing is disabled.		X	
Disabled ARP unicast if running a pre-4.2 image on the controller.	X		
Verify that DTPC is enabled so that the client and AP match tx power levels.	X		
Verify the Beacon interval is set to 100 ms.	X		
A DTIM of 2 is recommended.	X		
Ensure DHCP required is not enabled for the voice WLAN.		X	
Ensure that Aironet IE is enabled for the voice WLAN.	X		
Verify that Client MFP is set to Optional or Disabled.	X		
Session timeout for the WLAN should not be too short (300 seconds or more).	X		
Verify that peer-to-peer blocking is disabled.	X		
If using TKIP encryption, disable the hold down timer on the voice WLAN to prevent MIC errors from disrupting voice.	X		
Verify that the radio of the AP has multiple antennas and that diversity is enabled.	X		
Ensure controllers are configured for Symmetric Mobility if phones will be roaming between controllers.		X	

Table 2-1 VoWLAN checklist (continued)

Recommendation	Best Practice	May Consider	Done
Validate the virtual interface address is the same across all controllers in the same mobility group.	X		
Validate that the mobility status shows as UP between all controllers in the same mobility group.	X		
Enable Traffic Stream Metrics collection on the controller.	X		
DCA Channel Sensitivity set to Low to reduce chance of channel changes during business hours.	X		

Wireless LAN Configuration Tool

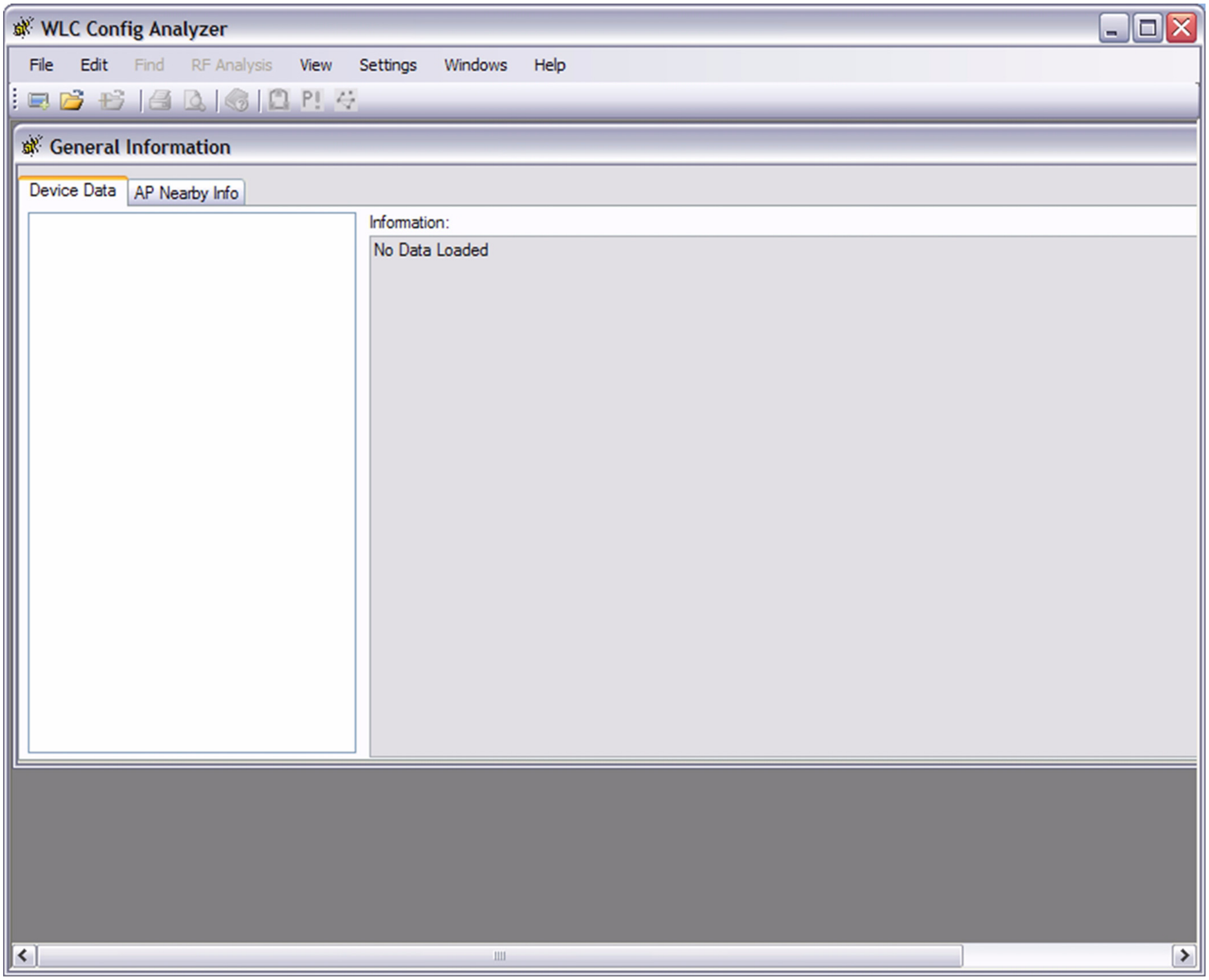
As an introduction to troubleshooting the VoWLAN, we are going to cover how TAC CSEs and Escalation Engineers at Cisco are able to isolate misconfigurations and problems within the Cisco Unified Wireless Network through the use of the Wireless LAN Controller Configuration Analyzer. The configuration analyzer is located on CCO under the download section for wireless software.

Step 1 Download and install the WLC Configuration Analyzer from the following URL:

https://supportforums.cisco.com/docs/DOC-1373

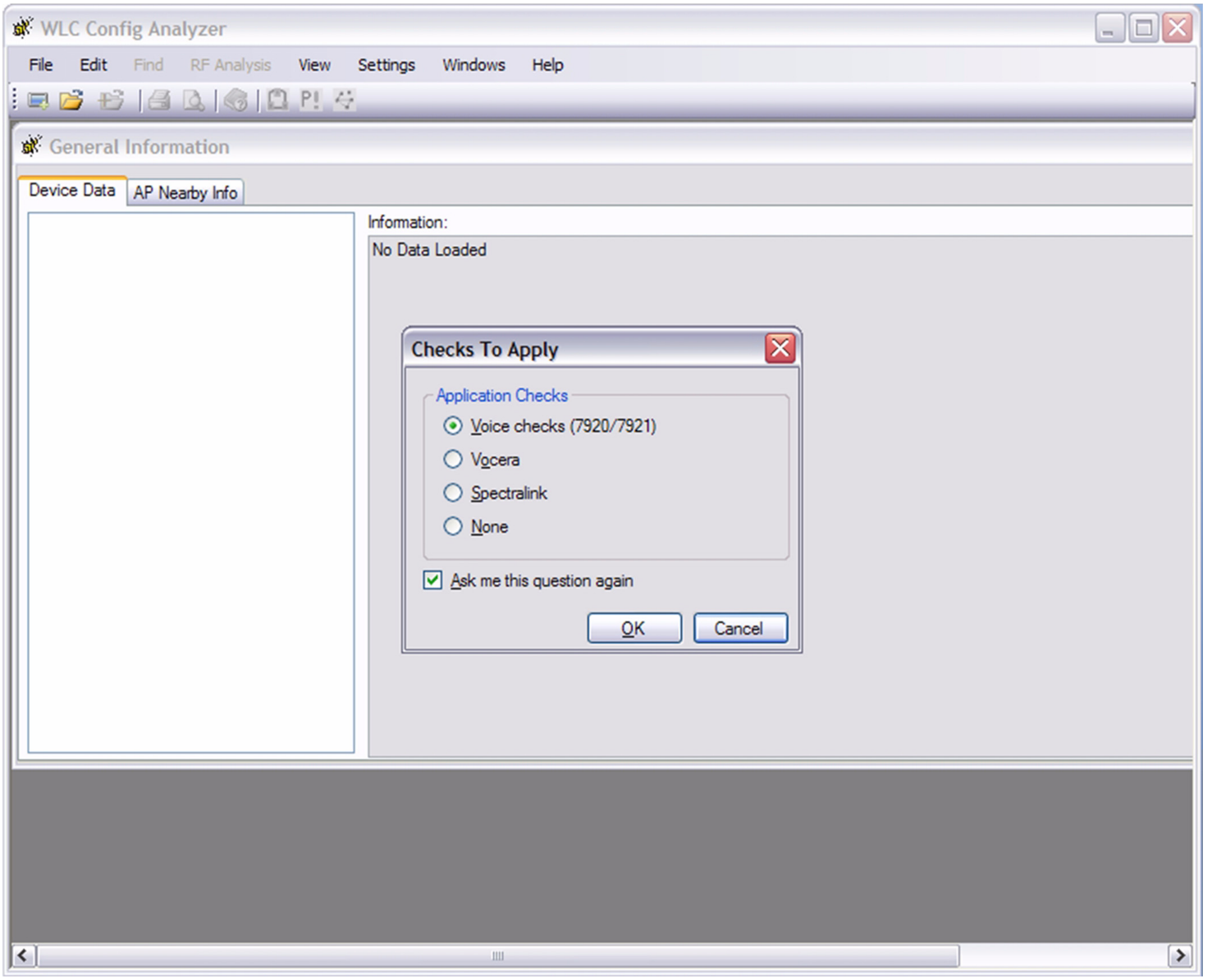
Step 2 To open the WLC Configuration Analyzer from the Windows Start menu, select **Start > Programs > WLC Config Analyzer > WLC Config Analyzer**.

Figure 2-1 WLC Configuration Analyzer



Step 3 Click **File > Open**

Figure 2-2 WLC Configuration Analyzer - Application Checks



Information:

No Data Loaded

Checks To Apply

Application Checks

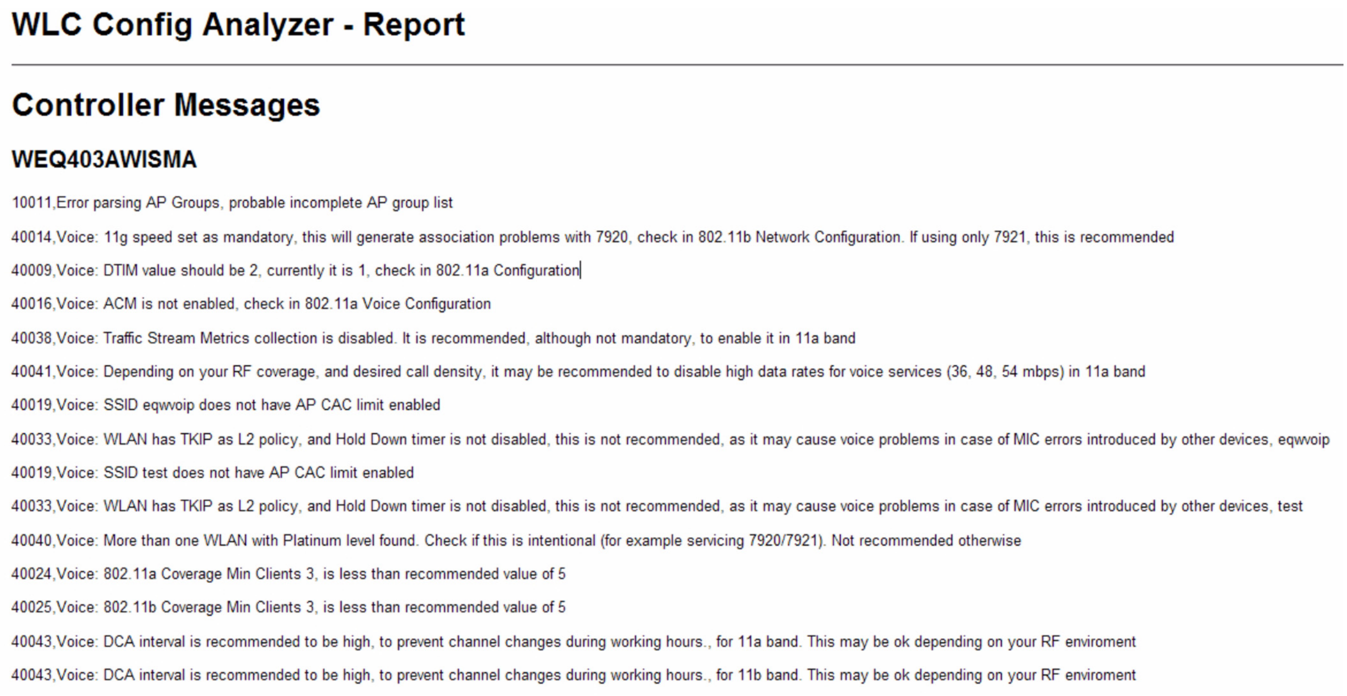
● Voice checks (7920/7921)
○ Vocera
○ Spectralink
○ None

☑ Ask me this question again

Step 4 Select **Voice Checks (7920/7921).**

Step 5 The tool will open a window that allows you to browse to a stored configuration file. Once you have selected the run-config file, click **OK** and the WLC Config Analyzer Report will be generated as seen in Figure 2-3.

Figure 2-3 WLC Config Analyzer Report



WLC Config Analyzer - Report

Controller Messages

WEQ403AWISMA

10011,Error parsing AP Groups, probable incomplete AP group list

40014,Voice: 11g speed set as mandatory, this will generate association problems with 7920, check in 802.11b Network Configuration. If using only 7921, this is recommended

40009,Voice: DTIM value should be 2, currently it is 1, check in 802.11a Configuration

40016,Voice: ACM is not enabled, check in 802.11a Voice Configuration

40038,Voice: Traffic Stream Metrics collection is disabled. It is recommended, although not mandatory, to enable it in 11a band

40041,Voice: Depending on your RF coverage, and desired call density, it may be recommended to disable high data rates for voice services (36, 48, 54 mbps) in 11a band

40019,Voice: SSID eqwvoip does not have AP CAC limit enabled

40033,Voice: WLAN has TKIP as L2 policy, and Hold Down timer is not disabled, this is not recommended, as it may cause voice problems in case of MIC errors introduced by other devices, eqwvoip

40019,Voice: SSID test does not have AP CAC limit enabled

40033,Voice: WLAN has TKIP as L2 policy, and Hold Down timer is not disabled, this is not recommended, as it may cause voice problems in case of MIC errors introduced by other devices, test

40040,Voice: More than one WLAN with Platinum level found. Check if this is intentional (for example servicing 7920/7921). Not recommended otherwise

40024,Voice: 802.11a Coverage Min Clients 3, is less than recommended value of 5

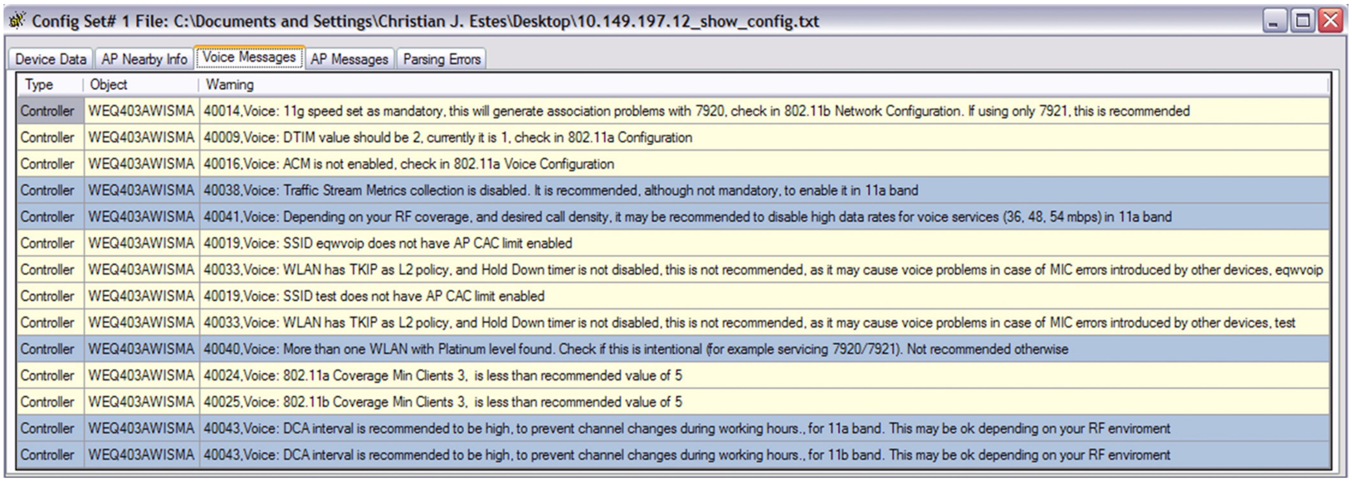
40025,Voice: 802.11b Coverage Min Clients 3, is less than recommended value of 5

40043,Voice: DCA interval is recommended to be high, to prevent channel changes during working hours., for 11a band. This may be ok depending on your RF enviroment

40043,Voice: DCA interval is recommended to be high, to prevent channel changes during working hours., for 11b band. This may be ok depending on your RF enviroment

Step 6 Another window will also open up in the WLC Config Analyzer and as seen in Figure 2-4 and will provide detailed information about Voice Messages. These are typically deviations for Cisco recommended Design and Deployment best practices as it pertains to the VoWLAN.

Figure 2-4 Voice Messages



Config Set# 1 File: C:\Documents and Settings\Christian J. Estes\Desktop\10.149.197.12_show_config.txt

Type	Object	Warning
Controller	WEQ403AWISMA	40014,Voice: 11g speed set as mandatory, this will generate association problems with 7920, check in 802.11b Network Configuration. If using only 7921, this is recommended
Controller	WEQ403AWISMA	40009,Voice: DTIM value should be 2, currently it is 1, check in 802.11a Configuration
Controller	WEQ403AWISMA	40016,Voice: ACM is not enabled, check in 802.11a Voice Configuration
Controller	WEQ403AWISMA	40038,Voice: Traffic Stream Metrics collection is disabled. It is recommended, although not mandatory, to enable it in 11a band
Controller	WEQ403AWISMA	40041,Voice: Depending on your RF coverage, and desired call density, it may be recommended to disable high data rates for voice services (36, 48, 54 mbps) in 11a band
Controller	WEQ403AWISMA	40019,Voice: SSID eqwvoip does not have AP CAC limit enabled
Controller	WEQ403AWISMA	40033,Voice: WLAN has TKIP as L2 policy, and Hold Down timer is not disabled, this is not recommended, as it may cause voice problems in case of MIC errors introduced by other devices, eqwvoip
Controller	WEQ403AWISMA	40019,Voice: SSID test does not have AP CAC limit enabled
Controller	WEQ403AWISMA	40033,Voice: WLAN has TKIP as L2 policy, and Hold Down timer is not disabled, this is not recommended, as it may cause voice problems in case of MIC errors introduced by other devices, test
Controller	WEQ403AWISMA	40040,Voice: More than one WLAN with Platinum level found. Check if this is intentional (for example servicing 7920/7921). Not recommended otherwise
Controller	WEQ403AWISMA	40024,Voice: 802.11a Coverage Min Clients 3, is less than recommended value of 5
Controller	WEQ403AWISMA	40025,Voice: 802.11b Coverage Min Clients 3, is less than recommended value of 5
Controller	WEQ403AWISMA	40043,Voice: DCA interval is recommended to be high, to prevent channel changes during working hours., for 11a band. This may be ok depending on your RF enviroment
Controller	WEQ403AWISMA	40043,Voice: DCA interval is recommended to be high, to prevent channel changes during working hours., for 11b band. This may be ok depending on your RF enviroment

If the problem still occurs after the configurations have been validated and/or remediated according to Cisco Design and Deployment best practices, it may be necessary to gather additional information including message logs, controller and /or AP debugs. In an effort to further isolate the problem and perform Root Cause Analysis, our Cisco TAC and Escalation Teams will often request a series of wired and wireless sniffer traces along with the respective debugs and message logs from the Cisco Wireless

LAN Controller. For the purposes of this troubleshooting guide, we will show what to look for in a sniffer trace or a wireless debug from the controller to isolate root cause for each problem or scenario provided.

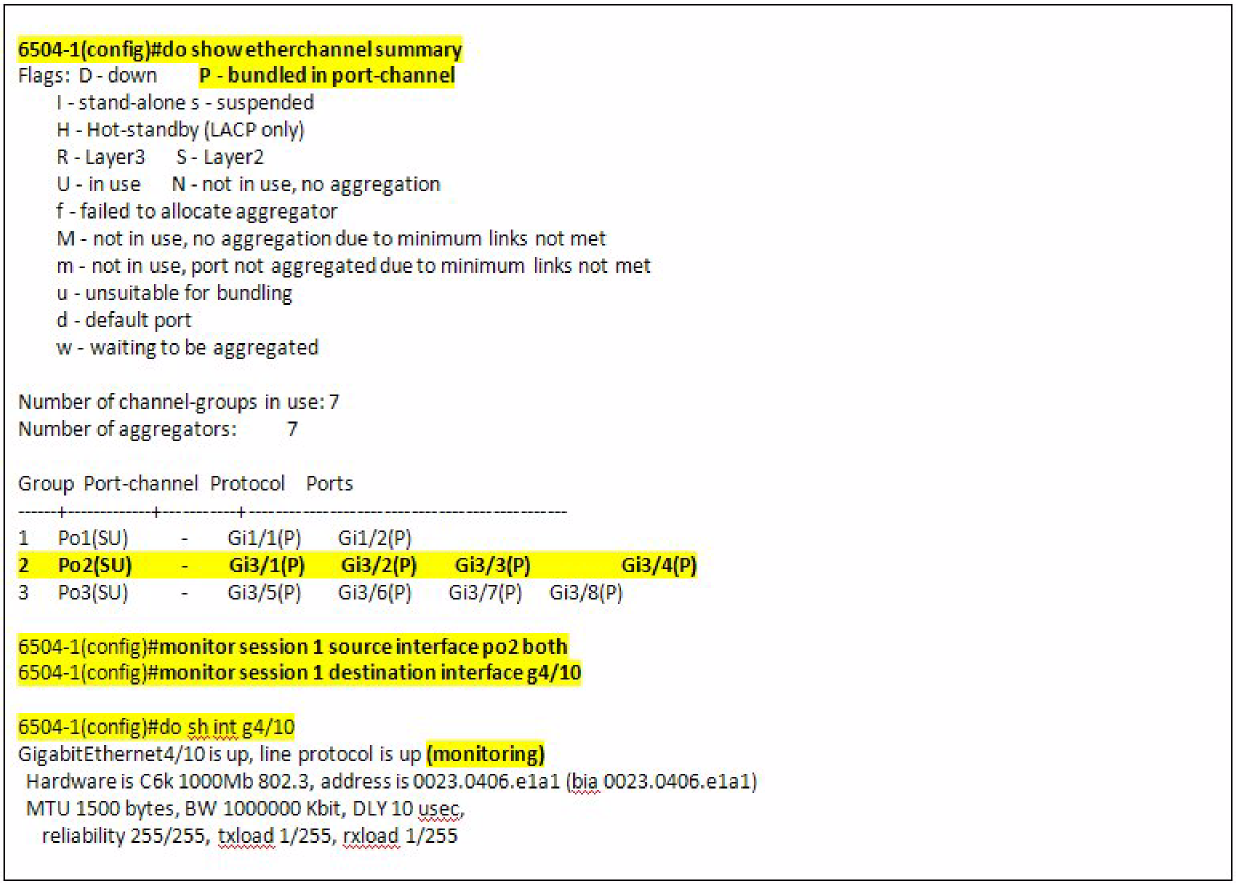
As a general suggestion, we often recommend that customers perform the following directions to gather additional data about the problem.

Step 1 Synchronize all laptops used for wired and wireless sniffer traces with the same NTP server that the Wireless LAN Controller is synchronized with. This will ensure that the time stamps listed in sniffer captures are consistent with controller debugs and logs gathered from the controller.

Step 2 Capture a wired sniffer trace on the trunk link or port channel between the distribution switch and the Wireless LAN Controller. This will display traffic in both directions between the Controller and AP, Controller and RADIUS, and Controller and DHCP Server.

This is an example of how to configure a SPAN port on the Port-Channel2 interface of a Cisco IOS switch to capture wired traffic in both directions between the controller and the switch. The output of traffic traversing the Port Channel will then be sent to a destination interface where a laptop running a protocol capture utility such as Wireshark will gather the protocol data for analysis.

Figure 2-5 Configuring an interface to monitor and capture wired traffic to a sniffer



```
6504-1(config)#do show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator
        M - not in use, no aggregation due to minimum links not met
        m - not in use, port not aggregated due to minimum  links not met
        u - unsuitable for bundling
        d - default port
        w - waiting to be aggregated

Number of channel-groups in use: 7
Number of aggregators:         7

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         -        Gi1/1(P)     Gi1/2(P)
2      Po2(SU)         -        Gi3/1(P)     Gi3/2(P)     Gi3/3(P)             Gi3/4(P)
3      Po3(SU)         -        Gi3/5(P)     Gi3/6(P)     Gi3/7(P)    Gi3/8(P)

6504-1(config)#monitor session 1 source interface po2 both
6504-1(config)#monitor session 1 destination interface g4/10

6504-1(config)#do sh int g4/10
GigabitEthernet4/10 is up, line protocol is up (monitoring)
 Hardware is C6k 1000Mb 802.3, address is 0023.0406.e1a1 (bia 0023.0406.e1a1)
 MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
   reliability 255/255, txload 1/255, rxload 1/255
```

Step 3 For troubleshooting wireless traffic on the 2.4 GHz frequency band, we recommend using an CACE AirPCAP adapter that acts as a multichannel aggregator. This adapter captures wireless traffic on all three non-overlapping channels (1, 6 and 11) and aggregates the data into a single file. This tool can be used with both Omnipeek and/or Wireshark to gather wireless data being sent between the Cisco Access

Point and the VoIP handset. For wireless troubleshooting on the 5 GHz frequency band, we suggest that you use one laptop per channel and use the tshark utility compiled in Wireshark or Omnipeek tools to combine both sniffer captures into a single file for review and analysis. For the purposes of this document, we will focus on troubleshooting as it pertains to deployments using the 792xG Series wireless IP phones.

Step 4 Once the laptops have been set up to capture both wired and wireless sniffer traces, you can gather the respective debugs and message logs from the controller(s). Depending upon the symptoms and potential problem experienced, the debugs that will need to be gathered will vary on a case by case basis. In most cases, it is prudent to gather the following debug for the client being tested, followed by any additional debugging needed.

```
(WiSM_4) >debug client ?

<MAC addr>     MAC address
```

For details with regard to client debugging on the Cisco Wireless LAN Controller, please refer to the following document for details.

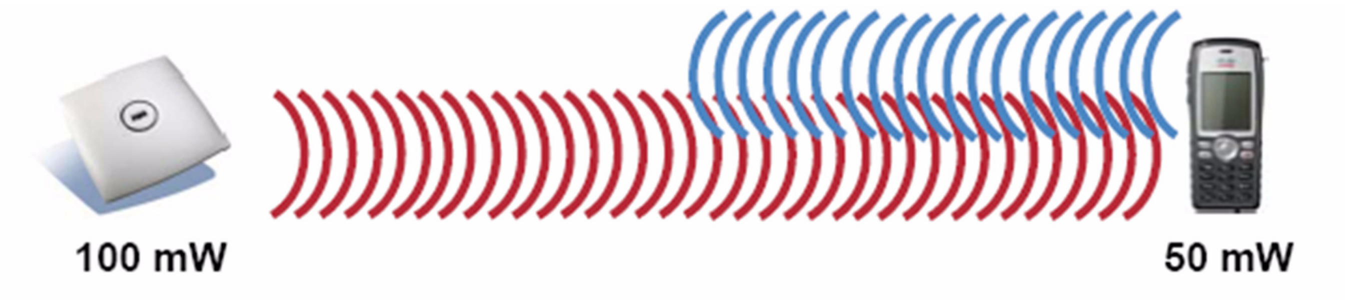
http://www.cisco.com/en/US/products/hw/wireless/ps430/products_tech_note09186a008091b08b.shtml

Troubleshooting One-Way Audio

It is important to understand that wireless communication occurs in a bi-directional manner. Uplink communication from the client to the AP is not always the same as downlink communication from the AP to the client. While an AP will send beacons downlink to the VoWLAN handset, most surveying tools will only display information as it pertains to downlink transmissions; therefore some problems are not easily detected using pre- or post-site survey tools. While a post site survey is vital after deploying the WLAN, a survey tool may not take into consideration the uplink signal being transmitted by the Cisco 792xG Series wireless IP phone in comparison to the downlink signal.

Most access points will often have a higher EIRP (Effective Isotropically Radiated Power), that is, the transmit power + the antenna gain. When comparing the EIRP to a VoWLAN handset, an AP on the 2.4 GHz band might be transmitting at its full power (100 mW), which is (20 dBm), and a Cisco 792xG Series wireless IP phone might be transmitting at only 40 or 50 mW. When this occurs, the IP phone will still hear the downlink frames sourced from the AP, but the AP will not hear the uplink frames from the wireless IP phone. This leads to Asymmetric Transmit as seen in Figure 2-6, and is typically the root cause of One-Way audio.

Figure 2-6 One-Way Audio Example



Note The regulatory requirements of 802.11g and 802.11a mean that clients do not have 100 mW transmit capabilities. Cisco highly recommends that the maximum configured transmit power on the access point be no higher than the maximum supported transmit rate on the IP phone. A phone with a slightly lower transmit power than the AP is better than the AP using less power than the phone, but having matching transmit powers lessens the likelihood of one-way audio.

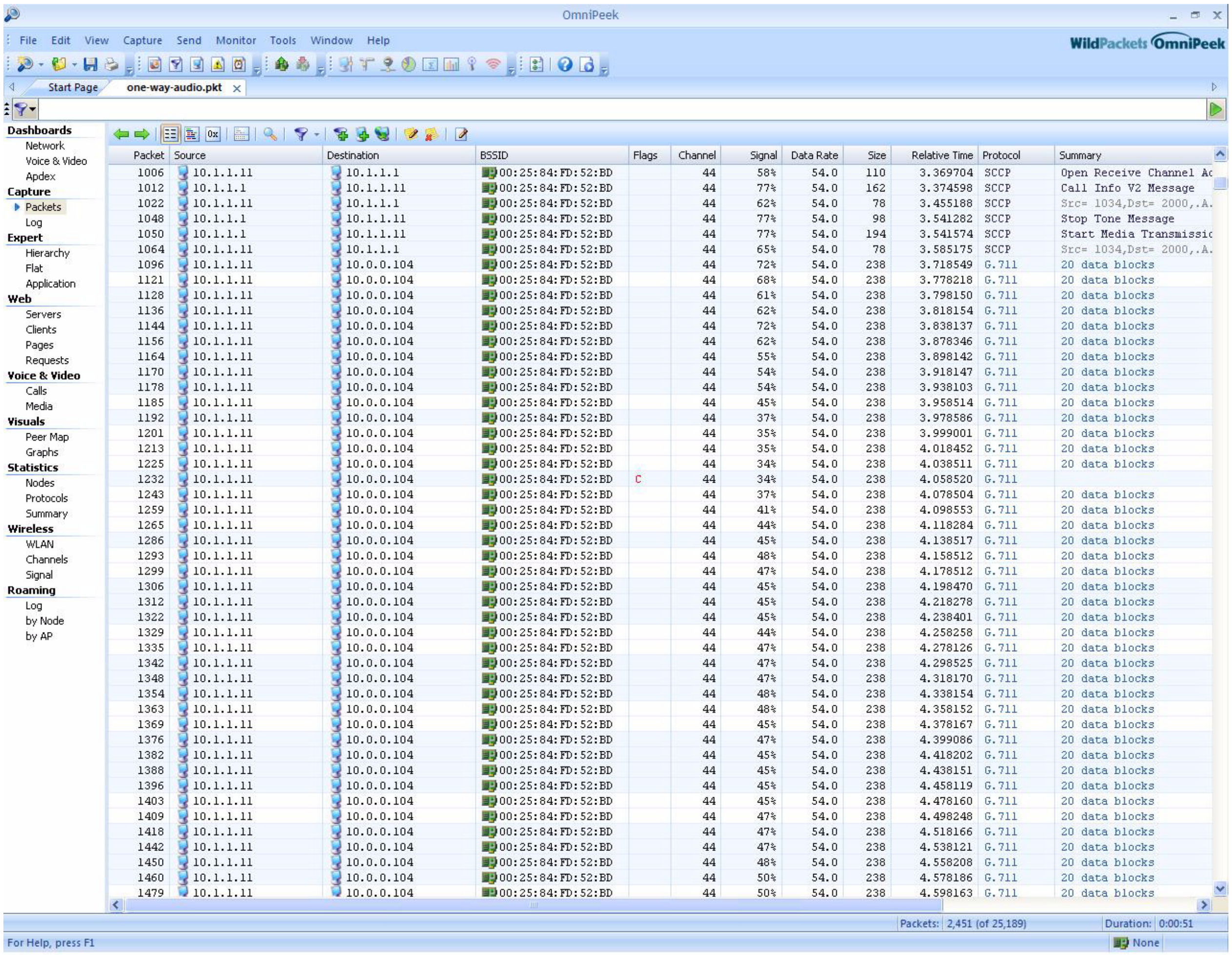
In an effort to mitigate One-Way Audio, Cisco recommends three possible solutions:

- Enabling Dynamic Transmit Power Control (DTPC)
- Manually configuring AP Transmit Power Control
- Transmit Power Throttling (available in WLC release 6.0.188.0 or later)

By default, DTPC is enabled on the Wireless LAN Controller so that Cisco access points will advertise the transmit power for clients to learn. CCX compatible clients will then learn the AP transmit power and adjust their transmit power to match, ensuring that one-way audio does not occur. In later versions of the Cisco Wireless LAN Controller code, there is also a feature referred to as Transmit Power throttling. This allows systems engineers to throttle the maximum transmit on the access point to ensure that mechanisms such as the Coverage Hole Algorithm do not run and increase the transmit power beyond that of the 792xG Series wireless IP phone’s capabilities, 40/50 mW, respectively.

Note Non-Cisco voice clients must support a minimum of Cisco Compatible Extension v2 to use DTPC.

Figure 2-7 Sniffer capture displaying One-Way Audio



Packet	Source	Destination	BSSID	Flags	Channel	Signal	Data Rate	Size	Relative Time	Protocol	Summary
1006	10.1.1.11	10.1.1.1	00:25:84:FD:52:BD		44	58%	54.0	110	3.369704	SCCP	Open Receive Channel Ac
1012	10.1.1.1	10.1.1.11	00:25:84:FD:52:BD		44	77%	54.0	162	3.374598	SCCP	Call Info V2 Message
1022	10.1.1.11	10.1.1.1	00:25:84:FD:52:BD		44	62%	54.0	78	3.455188	SCCP	Src= 1034,Dst= 2000,.A.
1048	10.1.1.1	10.1.1.11	00:25:84:FD:52:BD		44	77%	54.0	98	3.541282	SCCP	Stop Tone Message
1050	10.1.1.1	10.1.1.11	00:25:84:FD:52:BD		44	77%	54.0	194	3.541574	SCCP	Start Media Transmissic
1064	10.1.1.11	10.1.1.1	00:25:84:FD:52:BD		44	65%	54.0	78	3.585175	SCCP	Src= 1034,Dst= 2000,.A.
1096	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	72%	54.0	238	3.718549	G.711	20 data blocks
1121	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	68%	54.0	238	3.778218	G.711	20 data blocks
1128	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	61%	54.0	238	3.798150	G.711	20 data blocks
1136	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	62%	54.0	238	3.818154	G.711	20 data blocks
1144	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	72%	54.0	238	3.838137	G.711	20 data blocks
1156	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	62%	54.0	238	3.878346	G.711	20 data blocks
1164	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	55%	54.0	238	3.898142	G.711	20 data blocks
1170	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	54%	54.0	238	3.918147	G.711	20 data blocks
1178	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	54%	54.0	238	3.938103	G.711	20 data blocks
1185	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	45%	54.0	238	3.958514	G.711	20 data blocks
1192	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	37%	54.0	238	3.978586	G.711	20 data blocks
1201	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	35%	54.0	238	3.999001	G.711	20 data blocks
1213	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	35%	54.0	238	4.018452	G.711	20 data blocks
1225	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	34%	54.0	238	4.038511	G.711	20 data blocks
1232	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD	C	44	34%	54.0	238	4.058520	G.711	
1243	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	37%	54.0	238	4.078504	G.711	20 data blocks
1259	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	41%	54.0	238	4.098553	G.711	20 data blocks
1265	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	44%	54.0	238	4.118284	G.711	20 data blocks
1286	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	45%	54.0	238	4.138517	G.711	20 data blocks
1293	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	48%	54.0	238	4.158512	G.711	20 data blocks
1299	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	47%	54.0	238	4.178512	G.711	20 data blocks
1306	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	45%	54.0	238	4.198470	G.711	20 data blocks
1312	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	45%	54.0	238	4.218278	G.711	20 data blocks
1322	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	45%	54.0	238	4.238401	G.711	20 data blocks
1329	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	44%	54.0	238	4.258258	G.711	20 data blocks
1335	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	47%	54.0	238	4.278126	G.711	20 data blocks
1342	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	47%	54.0	238	4.298525	G.711	20 data blocks
1348	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	47%	54.0	238	4.318170	G.711	20 data blocks
1354	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	48%	54.0	238	4.338154	G.711	20 data blocks
1363	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	48%	54.0	238	4.358152	G.711	20 data blocks
1369	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	45%	54.0	238	4.378167	G.711	20 data blocks
1376	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	47%	54.0	238	4.399086	G.711	20 data blocks
1382	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	45%	54.0	238	4.418202	G.711	20 data blocks
1388	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	45%	54.0	238	4.438151	G.711	20 data blocks
1396	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	45%	54.0	238	4.458119	G.711	20 data blocks
1403	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	45%	54.0	238	4.478160	G.711	20 data blocks
1409	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	47%	54.0	238	4.498248	G.711	20 data blocks
1418	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	47%	54.0	238	4.518166	G.711	20 data blocks
1442	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	47%	54.0	238	4.538121	G.711	20 data blocks
1450	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	48%	54.0	238	4.558208	G.711	20 data blocks
1460	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	50%	54.0	238	4.578186	G.711	20 data blocks
1479	10.1.1.11	10.0.0.104	00:25:84:FD:52:BD		44	50%	54.0	238	4.598163	G.711	20 data blocks

Packets: 2,451 (of 25,189) Duration: 0:00:51

As you can see in the sniffer trace, the RTP stream occurs in only a single direction, causing the user to hear audio in the downlink RTP stream. Unfortunately, due to the limited transmit capability of the wireless IP Phone, the voice client has roamed out of range with regard to its transmit capabilities, therefore the user on the other end cannot hear the mobile user.

In addition to the solutions provided above, it is also recommended that systems engineers consider the following possibilities:

- Check that the access point is enabled for ARP caching. When the Cisco Unified Wireless IP 792xG Series Phone is in power save mode or scanning, the access point can respond to the wireless IP phone, but only when ARP caching is enabled.
- Check the phone hardware to be sure the speaker is functioning properly.
- Check the volume settings in the Phone Settings menu.

Troubleshooting No Audio

Q. Is the problem intermittent or does it occur consistently?

1. If so, try to use another phone to validate that the phone has signal.

2. If the issue is consistent across all phones, gather a wired and wireless sniffer trace and open a TAC case with Cisco Systems.

Scenario:

A 792xG Series wireless IP phone user places a call to another 792xG Series wireless IP phone user on the same wireless LAN across controller within the same mobility group. If the receiving phone rings and the audio is initially set up in both directions, this eliminates to need to look at the Cisco Unified Communication Manager as a potential point of failure. In a situation where no audio is reported, it is important to conclusively determine if both sides cannot hear to audio. Once the Systems Engineer has validated that no audio occurs, he or she should immediately take wired and wireless sniffer traces to isolate root cause. During analysis, it is important to validate using both wired and wireless sniffers that the RTP stream is getting sent and received in both directions between phones. From our experience, a loss of audio in both directions is often related to inadequate RF coverage or RF interference, and not QoS.

Troubleshooting Choppy Audio

Q. Does the choppy audio occur everywhere, in a particular area, or when roaming?

A. Everywhere / Particular Area / Intra-Controller Roaming

1. Ensure that WLAN QoS is set to Platinum.
2. Ensure that the Platinum queue is set to use 802.1p tagging and is configured to a value of 6.
3. Ensure that the **mls qos trust dscp** command is enabled on all switch ports between the AP switch port and the Wireless LAN Controller. If a marking is lost in one direction, and the traffic is classified as best effort when reviewing a wired or wireless traces, you must review the switch configuration of every switch between the AP and the Wireless LAN Controller where the RTP stream traverse.
4. Use a Spectrum Analysis tool to isolate potential sources of RF interference or inadequate coverage.

Improper Roaming and Voice Quality or Lost Connection

If users report that when engaged in an active phone call and walking from one location to another (roaming), the voice quality deteriorates or the connection is lost, you can use the following suggestions to identify the cause of the problem.

Voice Quality Deteriorates While Roaming

- Check the RSSI on the destination access point to see if the signal strength is adequate. The next access point should have an RSSI value of -67 dBm or greater.
- Check the site survey to determine if the channel overlap is adequate for the phone and the access point to hand off the call to the next access point before the signal is lost from the previous access point.
- Check to see if noise or interference in the coverage area is too great.
- Check that signal to noise ratio (SNR) levels are 25 dB or higher for acceptable voice quality.

Delays in Voice Conversation While Roaming

- Use the Site Survey Utility on the Cisco Unified Wireless IP Phone 792xG to see if there is another acceptable access point as a roaming option. The next access point should have an RSSI value of 35 or greater to roam successfully.
- Check the Cisco Catalyst 45xx switch to see if it has the correct version of Supervisor (SUP) blades. The blades must be versions SUP2+ or higher to prevent roaming delays.

Phone Loses Connection with Cisco Unified Communications Manager While Roaming

Check for the following configuration or connectivity issues between the phone and the access point:

- The RF signal strength might be weak. Use the Site Survey Tool and check the RSSI value for the next access point.
- The next access point might not have connectivity to Cisco Unified Communications Manager.
- There might be an authentication type mismatch between the phone and the next access point.
- The access point might be in a different subnet from the previous access point. The Cisco Unified Wireless IP Phone 792xG is capable of Layer 2 roaming only.

Inter-Controller Roaming

When roaming between controllers (Inter-Controller Roaming):

1. Validate whether the roam occurs at Layer 2 or Layer 3.

Note If running an older release than 5.2, make sure to configure symmetric tunneling using Step 2.

2. If the roam is at Layer 3, validate that the customer has implemented Symmetric Mobility on all Wireless LAN Controllers in the Mobility Group, utilizing the same tunneling type is outlined as a Mobility Group requirement.

   To validate and configure tunneling on the Wireless LAN Controller, utilize the following commands:

   ```
   (WiSM_4) >show mobility summary

   (WiSM_4) >config mobility symmetric-tunneling enable
   ```

3. If the problem still occurs, you will need to capture a wired and wireless sniffer trace along with the following debugs on the WLC:

   ```
   (WiSM_4) >debug client <MAC addr>

   (WiSM_4) >debug mobility handoff enable

   (WiSM_4) >debug cac packet enable
   ```

There is the possibility during an inter-controller roam that a phone could be roaming to another controller where the maximum available bandwidth has already been consumed. Please see the section on troubleshooting Call Admissions Control for isolating whether or not this is the issue.

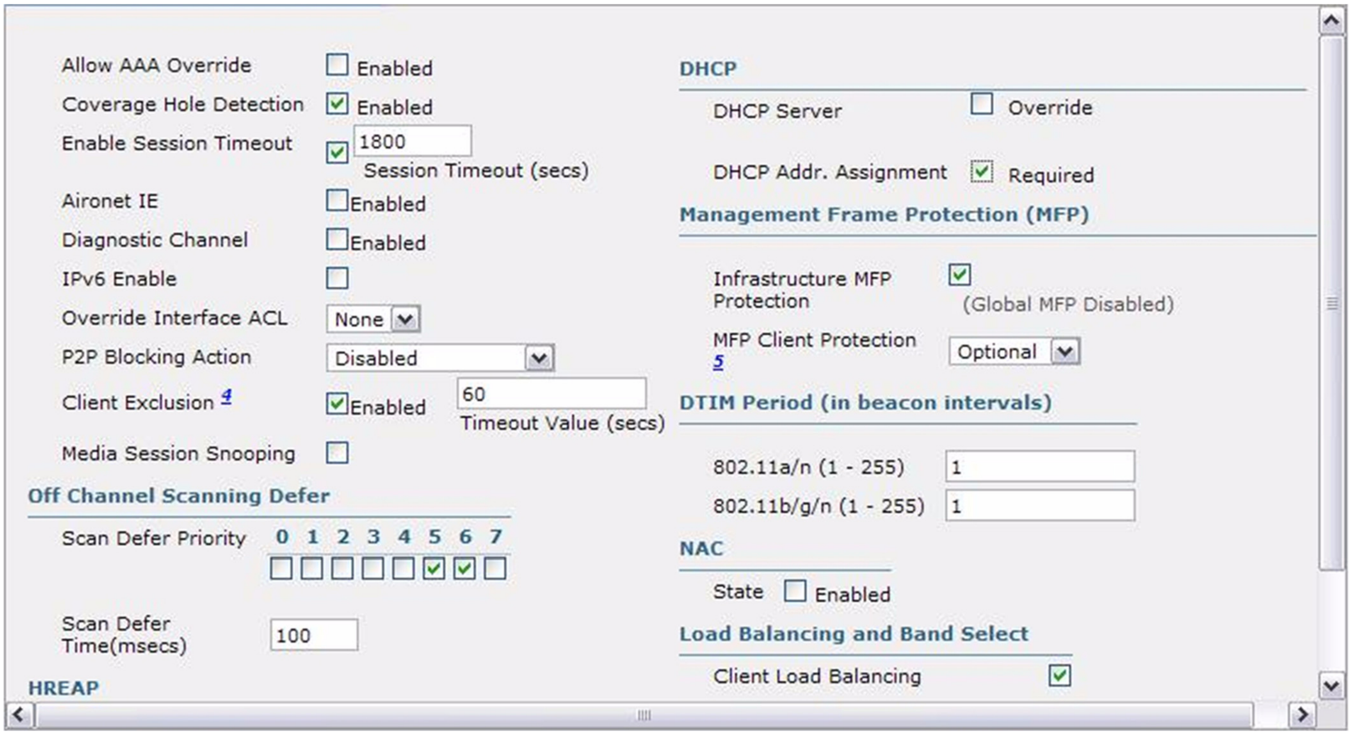
Note When a 792xG Series wireless IP phone makes an initial call and receives a "Status 202" error massager indicating that there is not enough available bandwidth, the phone will display "Network Busy". In the situation where the phone roams to a secondary controller and receives the same error, the 792xG Series wireless IP phone will then make an attempt to roam back to any AP with an acceptable RSSI as measured in Site Survey Mode on the 792xG Series wireless IP phone.

Dropped Calls

While dropped calls are not as common as Choppy or One-Way Audio, it is still something that the Cisco TAC deals with somewhat regularly. Most of the time, there is an RF problem within the customer's environment that causes severe packet loss, causing the call to be dropped. This is often due to the interference or an inadequate site survey.

Another common occurrence is when the 792xG Series wireless IP phone needs to perform a DHCP renewal when it roams from AP1, WLC1 to AP2, WLC2. This commonly occurs when DHCP Required is enabled on the Wireless LAN Controller where the phone roamed to. DHCP Required is security feature that is mostly used for Guest access and forces the client to obtain an IP address from a DHCP server but occasionally breaks VoWLAN calls when enabled in the WLAN Configuration as seen in Figure 2-8.

Figure 2-8 DHCP Required configured in the WLAN profile



Allow AAA Override □ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE □Enabled
Diagnostic Channel □Enabled
IPv6 Enable □
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion [4] ☑Enabled 60 Timeout Value (secs)
Media Session Snooping □

Off Channel Scanning Defer

Scan Defer Priority 0 □ 1 □ 2 □ 3 □ 4 □ 5 ☑ 6 ☑ 7 □
Scan Defer Time(msecs) 100

HREAP

DHCP

DHCP Server □ Override
DHCP Addr. Assignment ☑ Required

Management Frame Protection (MFP)

Infrastructure MFP Protection ☑ (Global MFP Disabled)
MFP Client Protection [5] Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC

State □ Enabled

Load Balancing and Band Select

Client Load Balancing ☑

While the following scenario should also be considered a possibility, it is not often the cause in environments where careful call capacity planning has been performed. Most of the time, the scenario outlined below has been discovered within the Healthcare vertical due to the need for an excessive number of wireless IP phones in use simultaneously in a single AP.

CAC Scenario:

792xG Series wireless IP phone is on AP1, Controller 1, and then roams to AP2 Controller 2. In a situation where there is not enough bandwidth available over the air on the Wireless LAN Controller where the phone is roaming to, a “Status code 202” error is sent to the phone resulting in a “Network Busy” message. The phone will then make an effort to roam to the AP with the strongest signal (usually the AP it was most recently connected to), but will perform a full Reauth. This scenario will also cause the call to be dropped.

Note As mentioned in the section on troubleshooting CAC, call capacity planning is essential and should be performed during an initial site survey and followed up by a post audit. The fundamental idea behind call capacity planning is to ensure that users do not saturate a single AP, causing CAC to deny access to network resources. The **debug cac all enable** command can be used to test and isolate if the scenario outlined above is the root cause of your problems. Please refer to the section on troubleshooting Call Admissions Control for details.