DEPLOYING VOWLAN OVER CISCO WIRELESS NETWORKS

BEST PRACTICES GUIDE

DEPLOYING VOWLAN OVER CISCO WIRELESS NETWORKS
BEST PRACTICES GUIDE

MN001146A02

Rev. A

May 2015

Revision History

Changes to the original guide are listed below:

Change	Date	Description
-A01 Rev. A	12/2014	Initial release.
-A02 Rev. A	5/2015	Rebranding.

TABLE OF CONTENTS

Chapter 3: Cisco Lightweight Wireless – Global 5 GHz

Chapter 4: Cisco Lightweight Wireless – Global 2.4 GHz

Chapter 5: Cisco Lightweight Wireless – QoS

ABOUT THIS GUIDE

Introduction

This guide provides best practices when deploying VOWLAN over a Cisco® wireless network.

NOTE Screens and windows pictured in this guide are samples and can differ from actual screens.

Chapter Descriptions

Topics covered in this guide are as follows:

- *Chapter 1, Introduction* provides information for deploying VOWLAN over a Cisco wireless network.
- *Chapter 2, Cisco Lightweight Wireless – WLAN* provides information for setting up a Cisco Lightweight wireless WLAN.
- *Chapter 3, Cisco Lightweight Wireless – Global 5 GHz* provides information for setting up a Cisco Lightweight wireless 5 GHz WLAN.
- *Chapter 4, Cisco Lightweight Wireless – Global 2.4 GHz* provides information for setting up a Cisco Lightweight wireless 2.4 GHz WLAN.
- *Chapter 5, Cisco Lightweight Wireless – QoS* provides information for configuring Quality of Service.

Notational Conventions

The following conventions are used in this document:

- *Italics* are used to highlight the following:
  - Chapters and sections in this and related documents
  - Icons on a screen.

- **Bold** text is used to highlight the following:
  - Dialog box, window, and screen names
  - Drop-down list and list box names
  - Check box and radio button names
  - Key names on a keypad
  - Button names on a screen.
- Bullets (•) indicate:
  - Action items
  - Lists of alternatives
  - Lists of required steps that are not necessarily sequential
- Sequential lists (e.g., those that describe step-by-step procedures) appear as numbered lists.

Related Documents

- *Cisco CUCM Administrator Configuration Guide, p/n MN001147Axx*
- Cisco CME Technical Guide, p/n MN001148Axx

For the latest version of this guide and all guides, go to: http://www.zebra.com/support.

Service Information

If the user has a problem with the equipment, contact Global Customer Support in the region. Contact information is available at http://www.zebra.com/support.

When contacting support, please have the following information available:

- Serial number of the unit (found on manufacturing label)
- Model number or product name (found on manufacturing label)
- Software type and version number

We respond to calls by email or telephone within the time limits set forth in support agreements.

If the problem cannot be solved by the Global Customer Support, the user may need to return the equipment for servicing and will be given specific directions. We are not responsible for any damages incurred during shipment if the approved shipping container is not used. Shipping the units improperly can possibly void the warranty.

If the device was purchased from a business partner, contact that business partner for support.

CHAPTER 1 INTRODUCTION

Voice over Wireless LAN (VoWLAN) delivers the functionality of an enterprise telephone system in a wireless handset. The handset is a wireless client device, and it shares the wireless network with laptops and other hand-held devices. For enterprise use, the handset is functionally equivalent to a wired desk phone, giving end-users all the features they are used to in a wired office telephone. The benefits of VoWLAN can result in substantial cost savings, leveraging Wi-Fi infrastructure and eliminating recurring charges associated with the use of cell phones, while significantly improving employee mobility.

There are two types of mobility, being mobile and 100%-connected mobility. To help explain this, think of the marketing manager working on a presentation and saving it on a network share. He later wants to give that presentation in the boardroom. If he picks up his laptop, closes the lid, and walks to the boardroom, opens the laptop, connects to the wireless network, and gives his presentation - that is being mobile. His laptop may have disconnected from the wireless network in between his office and the boardroom, but he never noticed. The same manager starting a call on his VoWLAN handset while in his office, remaining on that call as he walked to the elevator, traveled up several floors, and then walked to the boardroom – that is true mobility. If his VoWLAN handset had disconnected during that call, he would have noticed.

True mobility and enterprise-grade VoWLAN requires wireless networks designed to provide the highest audio quality throughout the facility. VoWLAN handsets require continuous, reliable connections as a user moves throughout the coverage area. Voice applications have a low tolerance for network errors and delays, deteriorating with just a few hundred milliseconds of delay or 1% of packet loss.

Coverage

Most data communication protocols provide a mechanism for retransmission of lost or corrupted packets, thus delays caused by retransmissions are not discernable. The real-time nature of a telephone conversation requires that voice packets be received correctly within 100ms of transmission. Lost or corrupted packets are discarded after limited retries. In areas of inadequate wireless coverage, the audio quality of real-time voice will suffer.

Moving handsets make the determination to roam in less than half the overlapping coverage area from a neighboring access point. That Assessment Area must be large enough to allow the handset time to discover, associate with, and connect to the next access point before the signal on the currently connected access point becomes too weak. Understanding what impacts RF coverage, cell size, and overlap is essential to properly design and configure a wireless network for voice usage.

The usable cell size of an access point is dictated by the frequency, signal power level, minimum data rate, number of channels used, and objects that attenuate the signal. A properly designed wireless network

positions access points with sufficient overlapping coverage to ensure there are no coverage gaps between them. 20% overlapping coverage between access points will result in seamless hand-offs and excellent voice quality at the average walking speed of 3 mph. If the speed of the moving user is greater (golf cart, fork lift or running/jogging), a larger overlap percentage may be necessary.

Dynamic Channel Assessment (DCA) is generally performed between the transmission of voice and control packets to learn about neighboring access points. It takes approximately 250 ms to process each channel in the channel list. To determine the size of access point Cell Overlap, determine the number of feet covered per second for the average walking speed of 3mph:

- 5,280 feet per mile * 3mph = 15,840 feet per hour
- 15,840 feet per hour / 60 = 264 feet per minute
- 264 feet per minute / 60 = 4.4 feet per second

Then apply that distance to the duration of the DCA Cycle for each band/channel configuration. The Assessment Area is approximately ¾ of the Coverage Overlap Area. Overlap Percentage is based on access points located 60 feet apart.

The following table shows the results of those calculations for various channel configurations:

Band	Number Channels	Duration (ms)	DCA Cycle (seconds)	Assessment Area	Coverage Overlap	Overlap percentage
2.4 GHz	3.00	250.00	0.75	3.30	4.40	7%
5 GHz	8.00	250.00	2.00	8.80	11.70	20%
5 GHz	12.00	250.00	3.00	13.20	17.60	29%
5 GHz	23.00	250.00	5.75	25.30	33.70	56%

Failure to complete the DCA cycle within the assessment area can lead to loss of connectivity, choppy audio, or a dropped call. Give careful consideration to the number of channels deployed in 5 GHz for a VoWLAN environment to avoid this.

There are unique requirements for the various types of WLAN implementations. A data-only implementation does not require significant cell overlap as 802.11 clients typically step down their rate to accommodate the transition to another access point. Typical thresholds for a data-only implementation are a Signal Strength of -82 dBm and a Signal-to-Noise Ratio (SNR) of 10 dB.

The voice-data implementation generally requires a Signal Strength of -65 dBm, a Signal-to-Noise Ratio (SNR) of 25 dB or better, and a Cell Overlap of 20%. The Cell Overlap ensures that a VoWLAN handset can detect and connect to alternative access points before it reaches its current cell boundary. The Signal Strength target of -65 dBm at the cell edge results in more access points running at lower power levels. A same channel separation of 19 dB is necessary to diminish co-channel interference. In a voice-data implementation, a low noise background is as important as high energy density. Transient conditions will make themselves more evident in a voice-data implementation. The actual target minimum Signal Strength depends on the 802.11 frequency band it is operating in, modulation used, data rates enabled on the access point, and data rate used by the handset at any particular time.

2.4 GHz 802.11b/n (CCK)				
Rate (Mbps)	1	2	5.5	11
Minimum Signal Strength (dBm)	-75	-70	-68	-65

2.4 GHz 802.11g /n (OFDM)								
Rate (Mbps)	6	9	12	18	24	36	48	54
Minimum Signal Strength (dBm)	-67	-66	-64	-62	-60	-56	-52	-47

5 GHz 802.11a/n (OFDM)								
Rate (Mbps)	6	9	12	18	24	36	48	54
Minimum Signal Strength (dBm)	-67	-65	-63	-61	-58	-54	-52	-50

Dynamic Channel Assignment and Intelligent Transmit Power Control should be used in all VoWLAN deployments. Transmit Power Minimum and Maximum levels should be established based on the maximum transmit power of the client used. In the case of multiple clients, minimum and maximum levels should be set to accommodate the client with the weakest transmit power. It is essential to prevent the access point from transmitting at a higher power than the client.

QoS

WMM is based on IEEE 802.11e Enhanced Distributed Coordination Access (EDCA). The first component of WMM are the four Access Categories (derived from 802.1d).

WMM Access Category	Priority Level	802.1d tags	Client wait time + random backoff window (slots)	SIP Traffic Type
Voice (AC_VO)	highest	7,6	2 + 0 to 3	Voice
Video (AC_VI)		5,4	2 + 0 to 7	Call control
Best Effort		0,3	3 + 0 to 15	Other (PTT, OAI, RTLS)
Background (AC_BK)	lowest	2,1	7 + 0 to 15	Not used

WMM relies on the application to assign the appropriate access category for the traffic it generates. Once the application assigns each packet to an access category, packets are then added to one of four independent transmit queues in the access point and client. Once transmitted onto the wireless network applications

compete for available bandwidth, resulting in packet collisions. When this happens the access category used will determine the retransmission timing. The higher the priority level, the lower the required wait time and random “back-off” window.

WMM Power Save is the second component of WMM. Based on the IEEE 802.11e Unscheduled Automatic Power Save Delivery (U-APSD) mechanism, it is an enhancement of the legacy 802.11 power save mechanism. The application-based approach used in WMM Power Save enables individual applications to decide how often the client needs to communicate with the access point and how long it can remain in a “restful” state. In addition, WMM Power Save increases transmission efficiency by transmitting the same amount of data in a shorter time using fewer frames. Power save behavior is negotiated during the association of a handset with an access point

The third component of WMM, WMM Admission Control, allows the access point to manage its available “air time” based on traffic requirements submitted by associated clients. Requests are rejected if insufficient resources are available. Use of WMM Admission Control avoids over-subscribing the access point, preserving and protecting QoS for all associated devices.

Security

Authentication is the process that occurs after WLAN association, where the handset and authentication server verify each others credentials then allow the handset access to the network. WPA2 has two different authentication modes, Personal and Enterprise. Personal mode uses a password-based authentication method called Pre-Shared Key (PSK). Personal mode is good for time-sensitive applications such as voice, because the key exchange sequence is limited and does not adversely affect roaming between access points. The PSK can be entered in hexadecimal or as an ASCII passphrase from the handset’s administration menu or through configuration files.

WPA2 Enterprise security mode requires a WLAN device to mutually validate credentials through 802.1X with a RADIUS server on the network every time the device roams to a new access point. Authentication delays during roaming may cause dropped packets and result in longer delays and audio artifacts. The size of the credentials used and the location of the RADIUS authentication server can significantly affect the duration of that delay. Larger credentials are more secure, but they take more time to process.

Fast access point hand-off techniques allow for the part of the key derived from the authentication server to be cached in the wireless network, thereby shortening the time to renegotiate a secure hand-off. Client handsets generally offer two 802.1X authentication types (PEAPv0 with MSCHAPv2 or EAP-FAST), and two fast access point hand-off mechanisms (OKC or CCKM). The combination of the selected 802.1X authentication type and fast access point hand-off mechanisms results in faster roaming and fewer audio artifacts. Use of the fast access point hand-off methods does not eliminate situations where full 802.1X key exchanges must re-occur.

PEAP (Protected Extensible Authentication Protocol) was developed by Microsoft, Cisco and RSA Security for 802.1X authentication on WLANs. PEAPv0 with MSCHAPv2 is one of the most-commonly used PEAP subtypes. PEAP makes use of a server-side public key certificate to authenticate the server and creates an encrypted tunnel to exchange information between the server and the client. Larger certificate key sizes provide stronger encryption, but are more computationally intensive and therefore take more time to process. The longer processing time can result in audio artifacts.

EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling) was created by Cisco as a replacement for LEAP (Lightweight Extensible Authentication Protocol). EAP-FAST has since gained adoption by WLAN vendors besides Cisco and is growing in popularity. Rather than relying on certificates, EAP-FAST use a Protected Access Credential (PAC) to establish a tunnel in which client credentials are verified.

Cisco Centralized Key Management (CCKM) is a Cisco-proprietary fast access point hand-off method supported on Cisco access points. The combination of either PEAP/MSCHAPv2 or EAP-FAST with CCKM will result in faster hand-offs once the initial 802.1X exchange has occurred. The faster hand-offs occur as the user

roams within the coverage area and the WLAN infrastructure retains authentication key information for the associated clients. The RADIUS server does not need to be reached at every access point hand off and the duration of the authentication exchange is fast enough to maintain audio quality. When the handset loses access point connectivity and must re-acquire its connection to the WLAN, a full 802.1X authentication with the RADIUS server is required during the re-acquisition. During this period, audio artifacts may become apparent.

General Wireless Network Best Practices

In order for voice to operate efficiently in a wireless network, it is critical that it be separated from the data traffic by using 802.1q VLANs.

Most access points can be configured to allow or deny association of wireless clients based on their unique MAC address and is sometimes used as a method of securing the WLAN. This process is not recommended for a VoWLAN environment. MAC filtering is ineffective as a security method.

The traffic filtering capabilities of firewalls, Ethernet switches, and wireless controllers can also be used as an additional security layer when configured to allow only certain types of traffic to pass onto specific areas of the LAN. To properly provide access control, it is necessary to understand the type of IP traffic used. Following is a table of common port numbers:

Protocol	Type	Port
FTP	TCP	21
SSH	TCP	22
Telnet	TCP	23
DNS	UDP	53
DHCP	UDP	67
DHCP	UDP	68
TFTP	UDP	69
HTTP	TCP	80
NTP	UDP	123
LDAP	Both	389
HTTPS	TCP	443
Syslog	UDP	514
LDAP over TLS	Both	636
SIP	Both	5060
SIP over TLS	TCP	5061

While wireless handsets will generally work through a Firewall (if the appropriate ports are allowed) it is not recommended. Firewalls create jitter which can severely limit the successful and on-time delivery of audio packets.

General Recommendations

Setting	Value	Notes
Latency	<100 ms	end-to-end
Jitter	<30 ms	
Packet Loss	<1%	
Cell Overlap	20%	30% in critical environments
Band	5 GHz	
Channel Width	20 MHz	
SSIDs per access point	<6	5 access points detected per channel @ 9 Mbps on 5 GHz

Other Recommendations

- Verify that the switch ports used to connect to the controller are set to trust QoS and ports to access points and uplinks are set to trust DSCP.
- Validate that the Virtual Interface is the same across all WLCs in a Mobility Group and is not routable within the customer network.
- Disable Spanning Tree on WLCs.
- Ensure all WLCs are running the same code version.

CHAPTER 2 CISCO LIGHTWEIGHT WIRELESS – WLAN

A WLAN associates a service set identifier (SSID) to a VLAN interface. It is configured with security, quality of service (QoS), radio policies, and other wireless network parameters. Up to 512 AP WLANs can be configured per controller. WLANs are directly mapped to VLANs, which are mapped to physical interfaces. Verify or apply the following settings for each WLAN intended to deliver VoIP over wireless.

NOTE Prefix all commands by disabling the WLAN-ID:

config wlan disable <WLAN-ID>

Complete process by enabling the WLAN-ID:

config wlan enable <WLAN-ID>

Voice-specific setting.

WLAN ID

The WLAN ID is a number from 1 to16 that identifies the WLAN internally. The key is to keep the WLAN IDs consistent across all controllers in a Mobility Group. It is selectable by the Customer.

WLAN ID \ General

Setting	Value	Command Line
Profile Name	customer-specified	
SSID	customer-specified	
Status	Status	
Radio Policy	all	
Interface	customer-specified	
Broadcast SSID	customer-specified	

WLAN ID \ Security

Setting	Value	Command Line
Layer 2 Security	WPA+WPA2	
	WPA2 Policy	
	AES	
	802.1x	
	CCKM	
Layer 3 Security	none	

WLAN ID \ Security \ AAA Servers

Setting	Value	Command Line
Server1	select from pull-down	
Server2	select from pull-down	

WLAN ID \ QOS

Setting	Value	Command Line
V Quality of Service	Platinum	config wlan qos <WLAN-ID> platinum
V WMM	Allowed	config wlan wmm allow <WLAN-ID>
V 7920 AP CAC	disabled	config wlan 7920-support ap-cac-limit enable <WLAN-ID>
V 7920 Client CAC	disabled	config wlan 7920-support client-cac-limit enable <WLAN-ID>

WLAN ID \ Advanced

Setting	Value	Command Line
AAA Override	disabled	
Coverage Hole Detection	enabled	
(V) Session Timeout	customer-specified	config wlan session-timeout <WLAN-ID> <duration in seconds>
	This is the maximum time for a client session to remain active before requiring reauthorization.	
(V) Aironet IE	enabled	config wlan ccx aironetIeSupport enable <WLAN-ID>
	Access point sends Information Elements (IE) in Beacons, Probe Responses, and Reassociation Responses.These IEs contain specific information about the wireless network to aid in roaming.	
Diagnostic Channel	disabled	
IPv6	disabled	
Override Interface ACL	disabled	
(V) P2P Blocking Action	disabled	config wlan peer-blocking disable <WLAN-ID>
(V) Client Exclusion	enabled	config wlan exclusionlist <WLAN-ID> enabled
(V) Timeout Value (seconds)	60	config wlan exclusionlist <WLAN-ID> <duration in seconds>
	Clients who fail to authenticate three times when attempting to associate are automatically excluded from further association attempts for the duration of the Timeout Value.	

WLAN ID \ DHCP

Setting	Value	Command Line
DHCP Server Override	disabled	
(V) DHCP Addr Assign Required	disabled	config wlan dhcp_server <WLAN-ID> 0.0.0.0
	Prevent the use of static IP addresses for this WLAN.	

WLAN ID \ Management Frame Protection

Setting	Value	Command Line
V MFP Client Protection	disabled	config wlan mfp client disable <WLAN-ID>
	MFP provides security for otherwise unprotected and unencrypted 802.11 management messages sent between access points and clients. Client MFP is only supported with CCX V5 clients using WPA2/TKIP or AES-CCMP.	

WLAN ID \ DTIM Period (beacon intervals)

Setting	Value	Command Line
V 802.11a DTIM Period	2	config wlan dtim 802.11a 2 <WLAN-ID>
V 802.11b/g DTIM Period	2	config wlan dtim 802.11b 2 <WLAN-ID>
	DTIM allows power-saving clients to wake up to receive data. With a value of 2, the access point will transmit broadcast and multicast frames after every other beacon. Client devices can be set to listen less often thereby extending battery life.	

WLAN ID \ Load Balancing and Band Select

Setting	Value	Command Line
V Client Load Balancing	disabled	config wlan load-balance allow disable <WLAN-ID>
	Clients are load balanced between access points on the same controller. When a wireless client attempts to associate to a lightweight access point, the access point responds with an association response of “Success” if the Utilization Threshold is not met, and Code 17 (access point Busy) if it has been met or exceeded.	
V Client Band Select	disabled	config wlan band-select allow disable <WLAN-ID>
	Band selection works by regulating probe responses to clients. It makes 5-GHz channels more attractive to wireless clients by delaying probe responses to clients on 2.4-GHz channels.	

WLAN ID \ Off Channel Scanning Defer

Setting	Value	Command Line
V Scan Defer Priority	4, 5, 6	config wlan channel-scan defer-priority 4,5,6 enable <WLAN-ID>
V Scan Defer Timeout (ms	100	config wlan channel-scan defer-time <duration in msec> <WLAN-ID>

CHAPTER 3 CISCO LIGHTWEIGHT WIRELESS – GLOBAL 5 GHZ

The settings in this section apply to 5 GHz operation across all access points and WLANs managed by the Controller. In most cases, the 802.11a network will need to be disabled, the desired setting changed, then the network enabled before the setting will take effect. Verify or apply the following settings if the 5 GHz band is intended to deliver VoIP over wireless. Some settings related to 5 GHz operation are set on each WLAN.

✓ ***NOTE*** Prefix all commands by disabling the 802.11a Network Status using the command:

config 802.11a disable network

Complete process by enabling the 802.11a Network Status using the command:

config 802.11a enable network

V Voice-specific setting.

Network

Setting	Value	Command Line
Network Status	enabled	
V Beacon Period	100	config 802.11a beaconperiod 100
	A beacon period is converted internally by the controller to 802.11 Time Units (TUs) where one TU = 1.024msec. The 100msec value is rounded up to the nearest multiple of 17 TUs, resulting in an actual beacon period of 104msec.	
Fragmentation Threshold	2436	

Setting	Value	Command Line
V DTPC Support	enabled	config 802.11a dtpc enable
	DTPC is a beacon and probe information element that allows the access point to provide information about its transmit power. Client devices can use this information to adjust their transmit power to match that power level.	
V ClientLink	enabled	config 802.11a beamforming global enable
	Beamforming uses information derived from the signals received from a client device to transmit out an access point's multiple antennas at different times, attempting to have those signals arrive at the client more simultaneously. This will improve the client's SNR and enable it to use a more complex modulation technique resulting is higher data rates.	

Data Rates

Setting	Value	Command Line
V 6 Mbps	disabled	config 802.11a rate disabled 6
V 9 Mbps	disabled	config 802.11a rate disabled 9
V 12 Mbps	mandatory	config 802.11a rate mandatory 12
V 18 Mbps	supported	config 802.11a rate supported 18
V 24 Mbps	supported	config 802.11a rate supported 24
V 36 Mbps	supported	config 802.11a rate supported 36
V 48 Mbps	supported	config 802.11a rate supported 48
V 54 Mbps	supported	config 802.11a rate supported 54

CCX Location Measurement

Setting	Value	Command Line
V Mode	enabled	config advanced 802.11a ccx location-meas global enable
Interval	60 seconds	

RRM

Setting	Value	Command Line
RF Grouping	enabled	

TPC

Setting	Value	Command Line
Version	Coverage Optimal Mode	
Assignment Method	Automatic	
Maximum Power Level Assignment	17	
Minimum Power Level Assignment	11	
Power Threshold	-70 dBm	
Power Neighbor Count	3	

DCA

Setting	Value	Command Line
Channel Assignment Method	Automatic	
Interval	10 minutes	
Anchor Time	0	
Avoid Foreign AP Interference	enabled	
Avoid Cisco AP Load	disabled	
Avoid non-802.11a Noise	enabled	
(V) DCA Channel Sensitivity	High	config advanced 802.11a channel dca sensitivity high
	This option is used to specify how sensitive the DCA algorithm should be to environmental changes when deciding to change channels (Signal, Noise, Load, Interference). High =20dB Sensitivity Threshold for both 2.4GHz and 5GHz.	
Channel Width	20MHz	

Setting	Value	Command Line
Avoid Check for non-DFS Channel	disabled	
(V) DCA Channel List	36, 40, 44, 48,149, 153, 157, 161	config advanced 802.11a channel add 36,40,44,48,149,153,157,161
	Specify the channels that the controller can set the access points to use during Dynamic Channel Most of the time, an eight channel plan provides stable consistent coverage without a lot of co-channel interfernece.Assignment.	

Coverage

Setting	Value	Command Line
Coverage Hole Detection	enabled	
Data RSSI	-80 dBm	
Voice RSSI	-80 dBm	
Min Failed Client Count / AP	3	
Coverage Exception level / AP	0.25	

General \ Profile Threshold for Traps

Setting	Value	Command Line
Interference	0.1	
Clients	12	
Noise	-70 dBm	
Utilization	0.8	

General \ Noise / Interference / Rogue Monitoring Channels

Setting	Value	Command Line
Channels List	Country Channels	

General \ Monitor Intervals

Setting	Value	Command Line
Channel Scan Duration	180	
Neighbor Packet Frequency	60	

General \ Pico Cell

Setting	Value	Command Line
Mode	disabled	

General \ Client Roaming

Setting	Value	Command Line
Mode	default	
Minimum RSSI	-85 dBm	
Hysteresis	2 dB	
Scan Threshold	-72 dBm	
Transition Time	5 seconds	

General \ Voice

Setting	Value	Command Line
(V) Admission Control Mandatory	enabled	config 802.11a cac voice acm enable
(V) Load-based CAC	enabled	config 802.11a cac voice load-based enable
	CAC enables an access point to maintain controlled QoS when the WLAN experiences congestion. WMM is sufficient as long as the WLAN is not congested. Load-based CAC measures the utilization of the channel continuously, only admitting a new call if the channel has enough unused capacity to support that call. Load-based CAC prevents over-subscription of the channel and maintains QoS under all WLAN load and interference conditions.	
Max RF Bandwidth (%)	75	
Reserved Roaming Bandwidth (%)	6	

Setting	Value	Command Line
Expedited Bandwidth	enabled	
SIP CAC Support	enabled	
(V) Traffic Stream Metrics Collection	enabled	config 802.11a tsm enable
	TSM is used to monitor voice-related metrics on the connection between client and access point. It reports both latency and packet loss. It is a collection of uplink (client) and downlink (access point) statistics in clients supporting CCX V4. Measurements are collected every 5 seconds by the access point. The access point prepares and sends 90-second reports to the controller. The controller organizes these reports and maintains an hour's worth of historical data.	

General \ Video

Setting	Value	Command Line
(V) Admission Control	disabled	config 802.11a cac video acm disable
Max RF Bandwidth (%)	0	
Reserved Roaming Bandwidth (%)	0	

General \ EDCA Parameters

Setting	Value	Command Line
(V) EDCA Profile	Voice	config advanced 802.11a edca-parameters optimized-voice
	Enhanced Distributed Channel Access parameters are designed to provide preferential wireless channel access for voice and other QoS traffic. Voice-Optimized is used when voice services other than SpectraLink are deployed.	
(V) Low Latency MAC	disabled	config advanced 802.11a voice-mac-optimization disable
	This feature controls packet retransmits and ages out voice packets appropriately when employed with WMM enabled. It should not be used if Voice-Optimized or SpectraLink is enabled.	

General \ DFS (802.11h)

Setting	Value	Command Line
(V) Channel Announcement	enabled	config 802.11h channelswitch enable 1
	Access point should announce when it is switching to a new channel and provide the new channel number.	
(V) Channel Quiet Mode	enabled	config 802.11h channelswitch enable 1
	Access point should stop transmitting on the current channel.	

General \ High Throughput

Setting	Value	Command Line
11n Mode	enabled	
(V) MCS Settings - 0 - 7 Mbps	disabled	config 802.11a 11nSupport mcs tx 0 disable
1 - 14 Mbps	enabled	
2 - 21 Mbps	enabled	
3 - 29 Mbps	enabled	
4 - 43 Mbps	enabled	
5 - 58 Mbps	enabled	
6 - 65 Mbps	enabled	
7 - 72 Mbps	enabled	
8 - 14 Mbps	enabled	
9 - 29 Mbps	enabled	
10 - 43 Mbps	enabled	
11 - 58 Mbps	enabled	
12 - 87 Mbps	enabled	
13 - 116 Mbps	enabled	
14 - 130 Mbps	enabled	
15 - 144 Mbps	enabled	

CHAPTER 4 CISCO LIGHTWEIGHT WIRELESS – GLOBAL 2.4 GHZ

The settings in this section apply to 2.4 GHz operation across all access points and WLANs managed by the Controller. In most cases, the 802.11g and 802.11b networks will need to be disabled, the desired setting changed, then the networks enabled before the setting will take effect. Verify or apply the following settings if the 2.4 GHz band is intended to deliver VoIP over wireless. Some settings related to 2.4 GHz operation are set on each WLAN.

NOTE Prefix all commands by disabling the 802.11a Network Status, using the command:

config 802.11b disable network

Complete process by enabling the 802.11a Network Status, using the command:

config wlan enable <WLAN-ID>

V Voice-specific setting.

Network

Setting	Value	Command Line
802.11b/g Network Status	enabled	
802.11g Support	enabled	
V Beacon Period	100	config 802.11b beaconperiod 100
	A beacon period is converted internally by the controller to 802.11 Time Units (TUs) where one TU = 1.024msec. The 100msec value is rounded up to the nearest multiple of 17 TUs, resulting in an actual beacon period of 104msec.	
V Short Preamble	enabled	config 802.11b preamble short

Setting	Value	Command Line
Fragmentation Threshold	2436	
V DTPC Support	enabled	config 802.11b dtpc enable
	DTPC is a beacon and probe information element that allows the access point to provide information about its transmit power. Client devices can use this information to adjust their transmit power to match that power level.	
V ClientLink	enabled	config 802.11b beamforming global enable
	Beamforming uses information derived from the signals received from a client device to transmit out an access point's multiple antennas at different times, attempting to have those signals arrive at the client more simultaneously. This will improve the client's SNR and enable it to use a more complex modulation technique resulting is higher data rates.	

Data Rates

Setting	Value	Command Line
V 1 Mbps	disabled	config 802.11b rate disabled 1
V 2 Mbps	disabled	config 802.11b rate disabled 2
V 5.5 Mbps	disabled	config 802.11b rate disabled 5.5
V 6 Mbps	disabled	config 802.11b rate disabled 6
V 9 Mbps	disabled	config 802.11b rate disabled 9
V 11 Mbps	mandatory	config 802.11b rate mandatory 11
V 12 Mbps	supported	config 802.11b rate supported 12
V 18 Mbps	supported	config 802.11b rate supported 18
V 24 Mbps	supported	config 802.11b rate supported 24
V 36 Mbps	supported	config 802.11b rate supported 36
V 48 Mbps	supported	config 802.11b rate supported 48
V 54 Mbps	supported	config 802.11b rate supported 54

CCX Location Measurement

Setting	Value	Command Line
Mode	enabled	config advanced 802.11b ccx location-meas global enable
Interval	60 seconds	

RRM

Setting	Value	Command Line
RF Grouping	enabled	

TPC

Setting	Value	Command Line
Version	Coverage Optimal Mode	
Assignment Method	Automatic	
Maximum Power Level Assignment	17	
Minimun Power Level Assignment	11	
Power Threshold	-70 dBm	
Power Neighbor Count	3	

DCA

Setting	Value	Command Line
Channel Assignment Method	Automatic	
Interval	10 minutes	
Anchor Time	0	
Avoid Foreign AP Interference	enabled	
Avoid Cisco AP Load	disabled	

Setting	Value	Command Line
Avoid non-802.11b/g Noise	enabled	
(V) DCA Channel Sensitivity	medium	config advanced 802.11b channel dca sensitivity medium
	This option is used to specify how sensitive the DCA algorithm should be to environmental changes when deciding to change channels (Signal, Noise, Load, Interference). Medium =10dB Sensitivity Threshold for 2.4 GHz and 15 dB for 5 GHz	
DCA Channel List	1, 6, 11	

Coverage

Setting	Value	Command Line
Coverage Hole Detection	enabled	
Data RSSI	-80 dBm	
Voice RSSI	-80 dBm	
Min Failed Client Count / AP	3	
Coverage Exception level / AP	0.25	

General \ Profile Threshold for Traps

Setting	Value	Command Line
Interference	0.1	
Clients	12	
Noise	-70 dBm	
Utilization	0.8	

General \ Noise / Interference / Rogue Monitoring Channels

Setting	Value	Command Line
Channels List	Country Channels	

General \ Monitor Intervals

Setting	Value	Command Line
Channel Scan Duration	180	
Neighbor Packet Frequency	60	

General \ Pico Cell

Setting	Value	Command Line
Mode	disabled	

General \ Client Roaming

Setting	Value	Command Line
Mode	default	
Minimum RSSI	-85 dBm	
Hysteresis	2 dB	
Scan Threshold	-75 dBm	
Transition Time	5 seconds	

General \ Voice

Setting	Value	Command Line
V Admission Control	enabled	config 802.11b cac voice acm enable
V Load-based CAC	enabled	config 802.11b cac voice load-based enable
	CAC enables an access pont to maintain controlled QoS when the WLAN experiences congestion. WMM is sufficient as long as the WLAN is not congested. Load-based CAC measures the utilization of the channel continuously, only admitting a new call if the channel has enough unused capacity to support that call. Load-based CAC prevents over-subscription of the channel and maintains QoS under all WLAN load and interference conditions.	
Max RF Bandwidth (%)	75	
Reserved Roaming Bandwidth (%)	6	

Setting	Value	Command Line
Expedited Bandwidth	enabled	
(V) Metrics Collection	enabled	config 802.11b tsm enable
	TSM is used to monitor voice-related metrics on the connection between client and access point. It reports both latency and packet loss. It is a collection of uplink (client) and downlink (access point) statistics in clients supporting CCX V4. Measurements are collected every 5 seconds by the access point. The access point prepares and sends 90-second reports to the controller. The controller organizes these reports and maintains an hour's worth of historical data.	

General \ Video

Setting	Value	Command Line
(V) Admission Control	disabled	config 802.11b cac video acm disable
Max RF Bandwidth (%)	0	
Reserved Roaming Bandwidth (%)	0	

General \ EDCA Parameters

Setting	Value	Command Line
(V) EDCA Profile	Voice	config advanced 802.11b edca-parameters optimized-voice
	Enhanced Distributed Channel Access parameters are designed to provide preferential wireless channel access for voice and other QoS traffic. Voice-Optimized is used when voice services other than SpectraLink are deployed.	
(V) Low Latency MAC	disabled	config advanced 802.11b voice-mac-optimization disable
	This feature controls packet retransmits and ages out voice packets appropriately when employed with WMM enabled. It should not be used if Voice-Optimized or SpectraLink is enabled.	

General \ High Throughput

Setting	Value	Command Line
11n Mode	enabled	
V MCS Settings - 0 - 7 Mbps	disabled	config 802.11b 11nSupport mcs tx 0 disable
1 - 14 Mbps	enabled	
2 - 21 Mbps	enabled	
3 - 29 Mbps	enabled	
4 - 43 Mbps	enabled	
5 - 58 Mbps	enabled	
6 - 65 Mbps	enabled	
7 - 72 Mbps	enabled	
8 - 14 Mbps	enabled	
9 - 29 Mbps	enabled	
10 - 43 Mbps	enabled	
11 - 58 Mbps	enabled	
12 - 87 Mbps	enabled	
13 - 116 Mbps	enabled	
14 - 130 Mbps	enabled	
15 - 144 Mbps	enabled	

CHAPTER 5 CISCO LIGHTWEIGHT WIRELESS – QOS

Wireless networks transport a multitude of applications and data, including delay-sensitive data such as real-time voice. Bandwidth-intensive applications stretch network capabilities and resources, but also add value, and enhance business processes. Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required Quality of Service (QoS) by managing the delay, delay variation (jitter), bandwidth, and packet loss parameters on a network becomes the secret to a successful end-to-end business solution. Thus, QoS is the set of techniques to manage network resources. Verify or apply the following settings if the intent is to deliver VoIP over this wireless network.

(V) Voice-specific setting.

QOS Profiles

Setting	Value	Command Line
QOS Profiles	Platinum	

Per-User Bandwidth Contracts

Setting	Value	Command Line
Average Data Rate	0	
Burst Date Rate	0	
Average Real-Time Rate	0	
Burst Real-Time Rate	0	

Per-SSID Bandwidth Contracts

Setting	Value	Command Line
Average Data Rate	0	
Burst Date Rate	0	
Average Real-Time Rate	0	
Burst Real-Time Rate	0	

WLAN QOS Parameters

Setting	Value	Command Line
Maximum Priority	voice	
Unicast Default Priority	voice	
Multicast Default Priority	voice	

Wired QOS Protocol

Setting	Value	Command Line
Protocol Type	802.1p	config qos protocol-type platinum dot1p
802.1p Tag	6	config qos dot1p-tag platinum 6

Zebra Technologies Corporation
Lincolnshire IL, U.S.A.
http://www.zebra.com

MN001146A02 Revision A - May 2015