DEPLOYING VOWLAN OVER WiNG5 NETWORKS

BEST PRACTICES GUIDE

DEPLOYING VOWLAN OVER WING5 NETWORKS BEST PRACTICES GUIDE

MN001150A02

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

ABOUT THIS GUIDE

Introduction

This guide provides best practices when deploying VoWLAN over a WiNG5 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 WiNG5 wireless network.
- *Chapter 2, Quality of Service* provides information for setting up QoS policies.
- *Chapter 3, Smart RF* provides information for setting up Smart RF policies.
- *Chapter 4, WLAN* provides information for setting up WLAN settings.

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 MN001147A01*
- Cisco CME Technical Guide, p/n MN001148A01

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

CHAPTER 2 QUALITY OF SERVICE

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.

Radio-QoS Policy

Radio QoS Policies are applied to individual radios within an Access Point. They are applied through Group Device Profiles.

Radio QoS parameters enforce WMM and police the different traffic types at the radio level. The most important of these is Admission Control.

NOTE Enter the CLI configuration mode by issuing the **`config t`** command from a SSH or Console session in enhanced mode.

Remember to Commit and Save from the GUI, or issue the **`commit write`** command from the CLI.

From the GUI, select **Configuration** > **Wireless** > **Radio QoS Policy** > **Add**.

Provide a name for the policy.

Table 2-1 *Radio-QoS Policy*

Option	Description	CLI Command
Customer-Radio-QoS	Name of Radio QoS Policy	Radio-QoS-Policy Customer-Radio-QoS

WMM Tab - Voice Access

Currently set to defaults, which should work well for the Workforce Connect Voice Client on the MC40. Adjust as necessary.

Table 2-2 *WMM Tab - Voice Access*

Option	Description	CLI Command
Transmit Ops	amount of time client is allowed to transmit after obtaining a transmit opportunity. <0 to 65535>	wmm voice txop-limit 47
AIFSN	wait period between frames based on Access Category. <1 to 15> (Higher priority categories should have lower AIFSNs.)	wmm voice aifsn 1
ECW-Min	minimum contention window. <0 to 15> (Higher priority traffic should have lower values.)	wmm voice cw-min 2
ECW-Max	maximum contention window. <0 to 15> (Higher priority traffic should have lower values.)	wmm voice cw-max 3

Admission Control Tab - Voice Access

Currently set to defaults, which should work well for the Workforce Connect Voice Client on the MC40. Adjust as necessary.

Table 2-3 *Admission Control Tab - Voice Access*

Option	Description	CLI Command
Enable Voice	Enable Admission Control for voice traffic.	
Maximum Airtime	Up to 150% to accommodate over-subscription. <0 to 150> (Voice traffic requires longer Radio Airtime to process.)	admission-control voice max-airtime-percent 75

Table 2-3 *Admission Control Tab - Voice Access (Continued)*

Option	Description	CLI Command
Maximum Wireless Clients	Maximum clients allowed on radio, used to mitigate over-subscription. <0 to 256> (Voice clients use a greater proportion of resources.)	admission-control voice max-clients 100
Maximum Roamed Wireless Clients	Limit for voice supported clients allowed to roam to a different radio. <0 to 256>	admission-control voice max-roamed-clients 10
Reserved for Roam	Percentage of radio bandwidth allotted to clients who have roamed to a different radio. <0 to 150>	admission-control voice reserved-for-roam-percent 10

Multimedia Optimizations Tab - Accelerated Multicast

Currently set to defaults, which should work well for the WFC Voice Client on the MC40. Adjust as necessary.

Table 2-4 *Multimedia Optimizations Tab - Accelerated Multicast*

Option	Description	CLI Command
Max number of wireless clients allowed	Maximum number of accelerated multicast or mcast to unicast clients. <1 to 4>	accelerated-multicast max-client-streams 2
When wireless client count exceeds limit	Over-limit client handling. <reject or revert>	accelerated-multicast overflow-policy reject
Maximum multicast streaming per client	Maximum number of multicast streams subscribed to one client. <0 to 256>	accelerated-multicast max-streams 25
Pkts/sec for mcast flow to be accelerated	Threshold at which multicast will be accelerated. <1 to 500>	accelerated-multicast stream-threshold 25
Timeout for wireless clients	Timeout for all clients (in second). <5 to 6000>	accelerated-multicast client-timeout 60

WLAN QoS Policy

WLAN QoS Policy definitions are used in the WLAN definition.

By defining Guest, Normal, and Voice policies and using them appropriately, Voice traffic can be prioritized.

NOTE Enter the CLI configuration mode by issuing the **`config t`** command from a SSH or Console session in enhanced mode.

Remember to Commit and Save from the GUI, or issue the **`commit write`** command from the CLI.

From the GUI, select **Configuration** > **Wireless** > **WLAN QoS Policy** > **Add**.

Provide a name for the policy.

Table 2-5 *WLAN QoS Policy*

Option	Description	CLI Command
Customer-Voice-WLAN-QoS	Name of WLAN Voice QoS Policy	WLAN-QoS-Policy Customer-Voice-WLAN-QoS

WMM Tab - Settings Section

These settings should work well for the Workforce Connect Voice Client on the MC40. Adjust as necessary.

Table 2-6 *WMM Tab - Settings Section*

Option	Description	CLI Command
Wireless Client Classification	Select how traffic on this WLAN must be classified. <wmm, voice, video, normal, low, non-wmm, or non-unicast> (WMM implies WMM QoS extensions are enabled on this radio.)	classification wmm
Non-Unicast Classification	Select how bcast and mcast traffic is classified. <voice, video, normal, low, or default>	classification non-unicast default
Enable Voice Prioritization	Enable / disable support for legacy Symbol VOIP phones.	no voice-prioritization
Enable SVP Prioritization	Enable / disable support for legacy SpectraLink / Polycom VOIP phones.	no svp-prioritization

Table 2-6 *WMM Tab - Settings Section (Continued)*

Option	Description	CLI Command
Enable WMM Power Save	Enable / disable unscheduled automatic power save delivery mechanism.	wmm power-save
Enable QBSS Load Element	Enable / disable Load IE within QoS BSS frames to inform clients of load.	wmm qbss-load-element
Configure Non-WMM Client Traffic	How to treat traffic not marked as one of the WMM access category types. <voice, video, normal or low>	classification non-wmm normal

WMM Tab - Voice Access Section

These settings should work well for the Workforce Connect Voice Client on the MC40. Adjust as necessary.

Table 2-7 *WMM Tab - Voice Access Section*

Option	Description	CLI Command
Transmit Ops	Amount of time client is allowed to transmit after obtaining a transmit opportunity. <0 to 65535>	wmm voice txop-limit 47
AIFSN	Wait period between frames based on Access Category. <1 to 15> (Higher priority categories should have lower AIFSNs.)	wmm voice aifsn 2
ECW-Min	Minimum contention window. <0 to 15> (Higher priority traffic should have lower values.)	wmm voice cw-min 2
ECW-Max	Maximum contention window. <0 to 15> (Higher priority traffic should have lower values.)	wmm voice cw-max 3

CHAPTER 3 SMART RF

Self-Monitoring At Run Time RF Management is designed to simply RF configurations and optimize radio performance over time.

Smart-RF:

- Centralizes the decision process and makes intelligent RF configuration decisions using data obtained from the RF environment.
- Intelligently applies various algorithms to arrive at the optimal channel and power selection for all access points in the network.
- Monitors the network for external Wi-Fi interference, neighbor Wi-Fi interference, non-Wi-Fi interference and client connectivity.
- Provides automatic mitigation from problematic events such as interference, noise, coverage holes and radio failures.
- Reacts to changes in the RF environment, self-healing if necessary.

Basic Settings

Use Sensitivity = Custom to allow for changes in individual off-channel scanning settings.

From the GUI, select **Configuration** > **Wireless** > **SMART-RF Policy** > **Add**.

Provide a name for the policy.

Table 3-1 *Smart-RF Policy*

Option	Description	CLI Command
Customer-smart-rf-policy	Customer-Smart-RF	smart-rf-policy Customer-Smart-RF

Table 3-2 *Basic Settings*

Option	Description	CLI Command
Sensitivity	Configure Smart-RF sensitivity. <high, medium, low, custom> (Custom allows adjustment of parameters and thresholds.)	sensitivity custom
SMART RF Policy Enable	Enable / disable SMART-RF Policy.	enable
Interference Recovery	Enable / disable Interference Recovery.	interference-recovery
Coverage Hole Recovery	Enable / disableCoverage Hole Recovery.	coverage-hole-recovery
Neighbor Recovery	Enable / disable Neighbor Recovery.	neighbor-recovery

Power Settings

Power settings should be adjusted to the TX power of the client and AP density.

Min 8dB and Max 14dB is a good starting point. The MC-40 is capable of 20dB TX Power.t

Table 3-3 *Power Settings*

Option	Description	CLI Command
5GHz Minimum Power	Minimum power threshold for 5GHz. <1 to 20>	assignable-power 5GHz min 8
5GHz Maximum Power	Maximum power threshold for 5GHz. <1 to 20>	assignable-power 5GHz max 14
2.4GHz Minimum Power	Minimum power threshold for 2.4GHz. <1 to 20>	assignable-power 2.4GHz min 8
2.4GHz Maximum Power	Maximum power threshold for 2.4GHz. <1 to 20>	assignable-power 2.4GHz max 14

Channel Settings

Avoid using UNI-2 and UNI-2 Extended Channels as they are subject to 802.11h and may become unavailable in mid-call.

20MHz wide channels are recommended for Voice over Wireless.

Table 3-4 *Channel Settings*

Option	Description	CLI Command
5GHz Channels	Channel-list 5GHz. <36,40,44,48,52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149,153,157,161>	channel-list 5GHz 36,40,44,48,149,153,157,161
5GHz Channel Width	Channel-width 5GHz. <20MHz, 40MHz, 80MHz or Automatic>	channel-width 5GHz 20MHz
2.4GHz Channels	Channel-list 2.4GHz. <1, 6, 11>	channel-list 2.4GHz 1,6,11
2.4GHz Channel Width	Channel-width 2.4GHz. <20MHz, 40MHz, or Automatic>	channel-width 20MHz

Scanning Configuration

Enable off-channel scanning.

Table 3-5 *Scanning Configuration*

Option	Description	CLI Command
Smart Monitoring Enable	Enable / disable off-channel scanning.	smart-ocs-monitoring

Scanning Configuration for 5 GHz

The specified settings are the defaults for Sensitivity = Medium.

These settings should work fine for Voice over Wireless, but can be individually adjusted as necessary.

Table 3-6 *Scanning Configuration for 5 GHz*

Option	Description	CLI Command
Duration	Duration to spend off-channel scanning. <20 to 150>	smart-ocs-monitoring off-channel-duration 5GHz 50
Frequency	Frequency at which neighbor off-channel scanning is to be performed. <1- to 20>	smart-ocs-monitoring frequency 5GHz 6
Extended Scan Frequency	Frequency at which extended off-channel scanning is to be performed. <0 to 50>	smart-ocs-monitoring extended-scan-frequency 5GHz 5

Table 3-6 *Scanning Configuration for 5 GHz*

Option	Description	CLI Command
Sample Count	Number of samples to take during off-channel scanning. <1 to 15>	smart-ocs-monitoring sample-count 5GHz 5
Client Aware Scanning	Client-aware client count used during off-channel scanning. <1 to 255>	no smart-ocs-monitoring client-aware 5GHz
Power Save Aware Scanning	Power save aware settings used during off-channel scanning. <dynamic, strict, disable>	smart-ocs-monitoring power-save-aware 5GHz strict
Voice Aware Scanning	Voice aware settings used during off-channel scanning. <dynamic, strict, disable>	smart-ocs-monitoring voice-aware 5GHz strict

Scanning Configuration for 2.4 GHz

The specified settings are the defaults for Sensitivity=Medium.

These settings should work fine for Voice over Wireless, but can be individually adjusted as necessary.

Table 3-7 *Scanning Configuration for 2.4 GHz*

Option	Description	CLI Command
Duration	Duration to spend off-channel scanning. <20 to 150>	smart-ocs-monitoring off-channel-duration 2.4GHz 50
Frequency	Frequency at which neighbor off-channel scanning is to be performed. <1- to 20>	smart-ocs-monitoring frequency 2.4GHz 6
Extended Scan Frequency	Frequency at which extended off-channel scanning is to be performed. <0 to 50>	smart-ocs-monitoring extended-scan-frequency 2.4GHz 5
Sample Count	Number of samples to take during off-channel scanning. <1 to 15>	smart-ocs-monitoring sample-count 2.4GHz 5

Table 3-7 *Scanning Configuration for 2.4 GHz (Continued)*

Option	Description	CLI Command
Client Aware Scanning	Client-aware client count used during off-channel scanning. <1 to 255>	no smart-ocs-monitoring client-aware 2.4GHz
Power Save Aware Scanning	Power save aware settings used during off-channel scanning. <dynamic, strict, disable>	smart-ocs-monitoring power-save-aware 2.4GHz strict
Voice Aware Scanning	Voice aware settings used during off-channel scanning. <dynamic, strict, disable>	smart-ocs-monitoring voice-aware 2.4GHz strict

CHAPTER 4 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 32 AP WLANs can be configured on 4xxx and 6xxx controller platforms, up to 256 WLANs on 7xxx platforms, and up to 1000 WLANs on the 9xxx platforms. WLANs are mapped to VLANs or VLAN Pools. VLANs are mapped to physical interfaces. Verify or apply the following settings for each WLAN intended to deliver VoIP over wireless.

WLAN Policy

WLANs associate a service set identifier (SSID) to a VLAN interface.

NOTE Enter the CLI configuration mode by issuing the **`config t`** command from a SSH or Console session in enhanced mode.

Remember to Commit and Save from the GUI, or issue the **`commit write`** command from the CLI.

Basic Configuration

From the GUI, select **Configuration** > **Wireless** > **Wireless LAN Policy** > **Add**.

Table 4-1 *Basic Configuration*

Option	Description	CLI Command
WLAN	Name of Customer-WLAN (32 characters)	wlan *Customer-WLAN*
SSID	Service Set Identifier (32 characters)	description *Customer-WLAN*
Description	Textural description of WLAN (64 characters)	ssid *Customer-WLAN*
WLAN Status	enable to make WLAN Active and available for use on radios where it is mapped	shutdown / no shutdown

Table 4-1 *Basic Configuration (Continued)*

Option	Description	CLI Command
QOS Policy	assign existing WLAN QOS Policy	use wlan-qos-policy *Customer-Voice-Policy*
Bridging Policy	Specify Bridging Policy for this WLAN <Local, Tunnel, Split-Tunnel>	bridging-mode local
Broadcast SSID	Broadcast SSIDs within beacons	braodcast ssid
Answer Broadcast Probes	Associate client with a blank SSID	no answer-broadcast-probes
Single VLAN	Select to assign a single VLAN to this WLAN. Enter the VLAN Number (1 to 4094) within the VLAN Parameter Field.	vlan 1
VLAN Pool	Select to assign a pool of VLANs with corresponding Client Counts/VLAN.	vlan-pool-member

Configuring Security

Select Authentication

A client must authenticate to an Access Point to receive resources from the network.

Table 4-2 *Select Authentication*

Option	Description	CLI Command
Authentication	<EAP, EAP/PSK, EAP/MAC, MAC, PSK/None>	authentication-type none

Select Encryption

WPA2 is the 802.11i standard that provides stronger wireless security than WPA or WEP.

CCMP is the security standard used by the Advanced Encryption Standard (AES).

Table 4-3 *Select Encryption*

Option	Description	CLI Command
Encryption	<WPA/WPA2-TKIP,WPA2-CCMP,WEP128,WEP64,Keyguard,Open>	encryption-type ccmp
Pre-Shared Key	Alphanumeric string of 8 to 63ASCII or 64 HEX characters as the primary string both TX and RX authenticators must share.	wpa-wpa2 psk 0 W0rkf0rc3#

Configuring Firewall Support

IP Firewall Rules

Use the IP Firewall Rules to allow or deny traffic based on IP network Addresses and Protocols.

Table 4-4 *IP Firewall Rules*

Option	Description	CLI Command
Inbound IP Firewall Rules	with respect to Inbound traffic	use ip-access-list out BROADCAST-MULTICAST-CONTROL
Outbound IP Firewall Rules	with respect to Outbound traffic	none

MAC Firewall Rules

Use the MAC Firewall Rules to allow or deny traffic based on MAC network Addresses and Protocols.

Table 4-5 *MAC Firewall Rules*

Option	Description	CLI Command
Inbound MAC Firewall Rules	with respect to Inbound traffic	use mac-access-list out PERMIT-ARP-AND-IPv4
Outbound MAC Firewall Rules	with respect to Outbound traffic	none

Configuring Client Settings

Each WLAN can maintain its own client setting configuration.

Table 4-6 *Configuring Client Settings*

Option	Description	CLI Command
Enable Client-to-Client Communication	Enable / Disable client to client communication. Enabled, clients are allowed to exchange packets with other clients.	client-client-communication
Wireless Client Power	Maximum Client TX Power. <0 to 20> dB	wireless-client tx-power 20
Wireless Client Idle Time	Maximum amount of time Client is allowed to be idle. <60 to 86400> seconds	wireless-client inactivity-timeout 43200

Table 4-6 *Configuring Client Settings (Continued)*

Option	Description	CLI Command
Max Clients allowed per Radio	Maximum number of Clients allowed to associate with a radio. <0 to 256>	wireless-client count-per-radio 128
Radio Resource Measurement	Enable / Disable radio resource measurement capabilities (802.11k).	radio-resource-measurement
Radio Resource Meas Channel Report	Enable / Disable radio resource measurement channel reporting (802.11k).	radio-resource-measurement channel-report
Radio Resource Meas Neighbor Report	Enable / Disable radio resource measurement neighbor reporting (802.11k).	radio-resource-measurement neighbor-report
Enforce Client Load Balancing	Enable / Disable Load balancing. Loads are balanced by ignoring association and probe requests. Probe and association requests are not responded to, forcing a client to associate with another Access Point radio. ***This is not recommended for a Voice WLAN.***	no client-load-balancing
Enforce DHCP Client Only	Enforce that the firewall only allows packets from clients if they used DHCP, disallowing static IP addresses.	enforce-dhcp
Proxy ARP Mode	Proxy ARP is the technique used by the Access Point to answer ARP requests intended for another system.	proxy-arp-mode dynamic
Enforce DHCP-Offer Validation	Enable / Disable DHCP Offer Validation.	broadcast-dhcp validate-offer
Smart Scan	Refine a Motorola client's channel scans to listed channels as opposed to all available channels.	motorola-extensions smart-scan
Rate Settings - 2.4GHz	Select Data Rates to be advertised and used for 2.4 GHz.	data-rates 2.4GHz custom basic-11 basic-12 18 24 36 48 54 mcs0-7 mcs8-15
Rate Settings - 5GHz	Select Data Rates to be advertised and used for 5 GHz.	data-rates 5GHz custom basic-12 18 24 36 48 54 mcs0-7 mcs8-15

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

MN001150A02 Revision A - May 2015