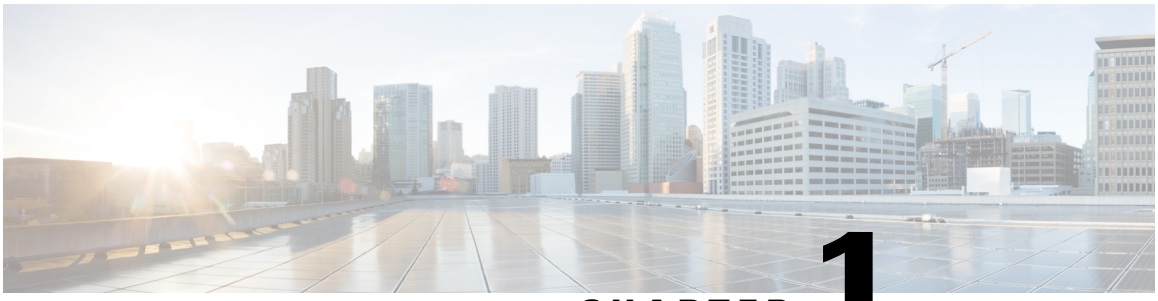
Vocera IP Phone Deployment in Cisco Unified Wireless Network Infrastructure, Release 7.4

Last Modified: April 05, 2014

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



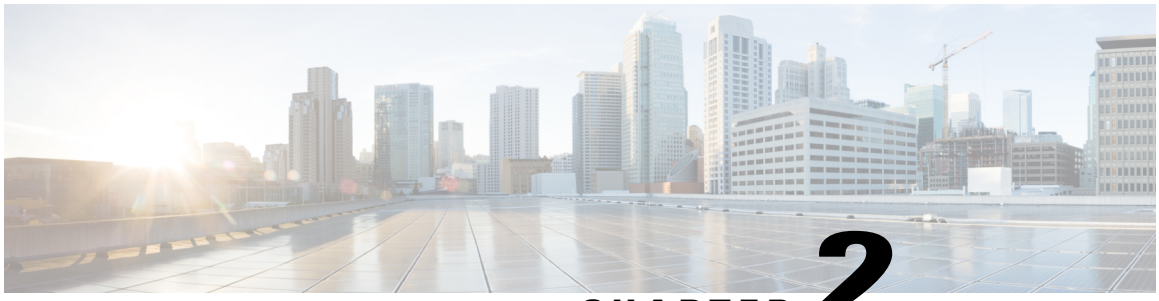
CHAPTER 1

Introduction

This document provides design considerations and deployment guidelines for the implementation of the Vocera® Badge Voice over WLAN (VoWLAN) technology on the Cisco Unified Wireless Network infrastructure.

Note Support for Vocera products should be obtained directly from Vocera support channels. Cisco Technical Support is not trained to support Vocera-related issues.

This guide is a supplement to the Cisco Wireless LAN Controller Deployment Guide and only addresses the configuration parameters that are particular to Vocera VoWLAN devices in a lightweight architecture. Refer to Cisco Wireless LAN Controller Configuration Guide for more information.



CHAPTER 2

Prerequisites

This chapter includes the following topics:

Requirements

We assume that you are familiar with the terms and concepts presented in the Cisco IP Telephony SRND and the Cisco Wireless LAN SRND.

Real-Time Traffic over Wireless LAN Solution Reference Network Design Guide: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/RToWLAN/CCVP_BK_R7805F20_00_rtowlan-srnd.html

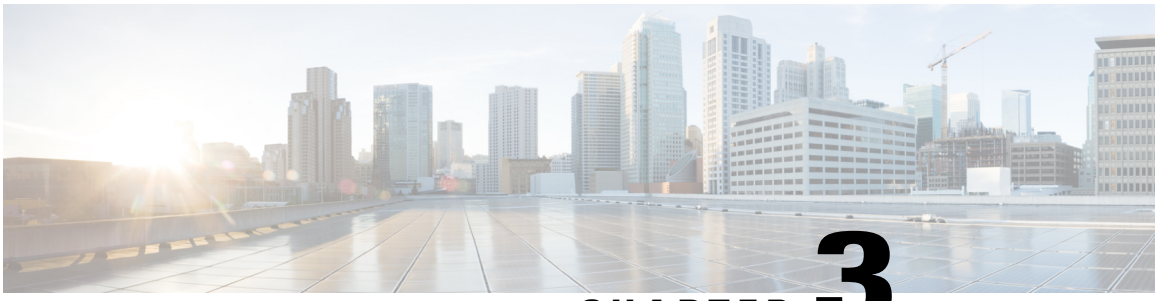
Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 7.x: http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns818/landing_uc_mgr.html

Components Used

This document is not restricted to specific software and hardware versions. However, it has been tested with Cisco Wireless LAN controller codes 7.0 and later.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

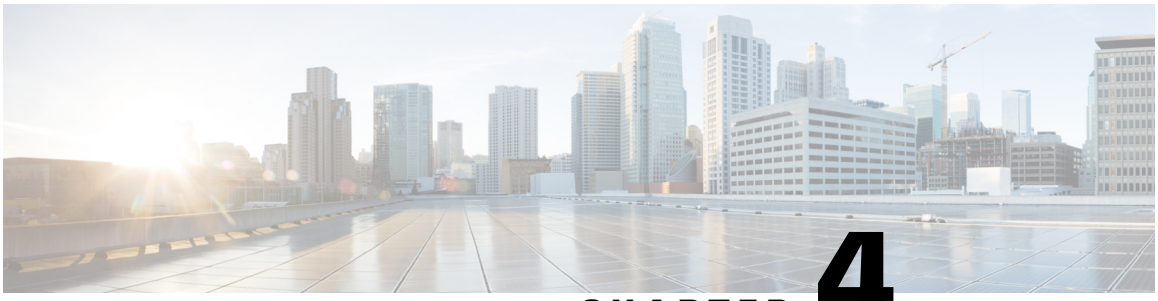


CHAPTER 3

Executive Summary

This table summarizes the four key functions and how they behave within a Cisco Unified Wireless network.

	Single Controller	Controller-to-Controller Layer 2 Roaming	Controller-to-Controller Layer 3 Roaming
Badge-to-Badge	No special configuration	No special configuration	No special configuration
Badge-to-Phone	No special configuration	No special configuration	No special configuration
Badge-to-Broadcast	Enable Controller Multicast	Enable Controller Multicast	Enable Controller Multicast
Badge Location	No special configuration	No special configuration	No special configuration



CHAPTER 4

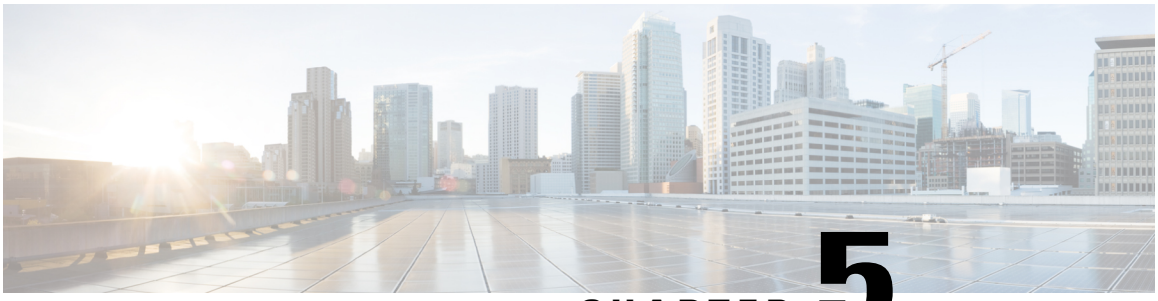
Vocera Badge Overview

The Vocera communication badges allow a wearer instant communication with any other badge wearer as well another phone through Private Branch Exchange (PBX) integration. Vocera offers two types of badges: B3000 and B2000. Vocera also has earlier B1000A badges. The information in this guide applies to B3000 and B2000 badges. Vocera also has a smartphone that supports 802.11a/b/g. B2000 and B3000 badges support 802.11b/g. Therefore, RF design is primarily targeted at the 2.4 GHz space.

The utilization of an 802.11b/g wireless network requires the use of multicast and UDP unicast packet delivery with limited requirements for Quality of Service (QoS) as of Vocera Server Software release 4.3 or later.

With the push of a button, the Vocera server responds with Vocera, which is a prompt to issue commands such as **record, where (am I) /is..., call, play, broadcast, messages**, and so forth. The Vocera server provides the necessary services and/or call setup to complete the request.

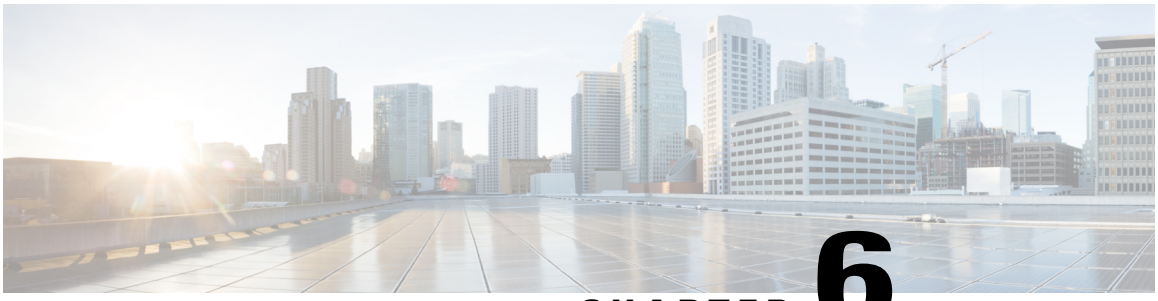
Vocera's 802.11b/g capable Communication System makes use of G711 codec and UDP port range to deliver signaling and audio communication. The Vocera System software runs on a Windows server that manages call set up, call connection, and user profiles. Vocera recommends a separate Windows server to connect calls to land lines or cell phones through PBX. The link can be created using a T1 connection with the Vocera Telephony Server (VTS) or a SIP trunk using the Vocera SIP Telephony Gateway VSTG.



CHAPTER 5

Vocera Call Capacity Considerations

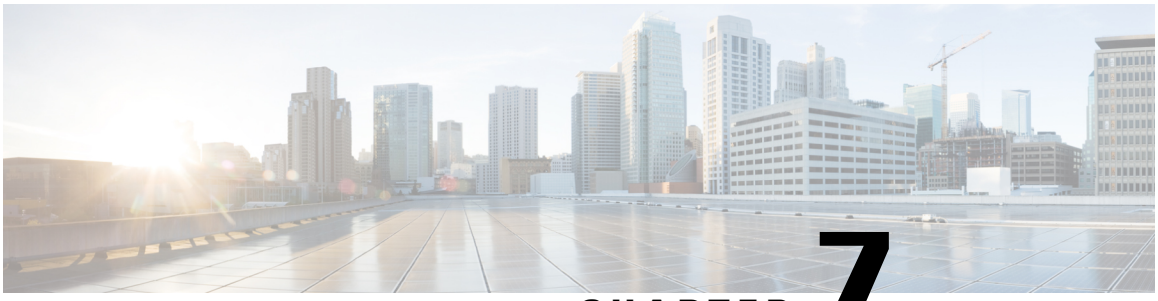
See the Network Sizing section of this document for further details.



CHAPTER 6

Vocera Communications Server Capacity

Refer to the Vocera Communications System Specifications for more information on Vocera Server sizing matrix.



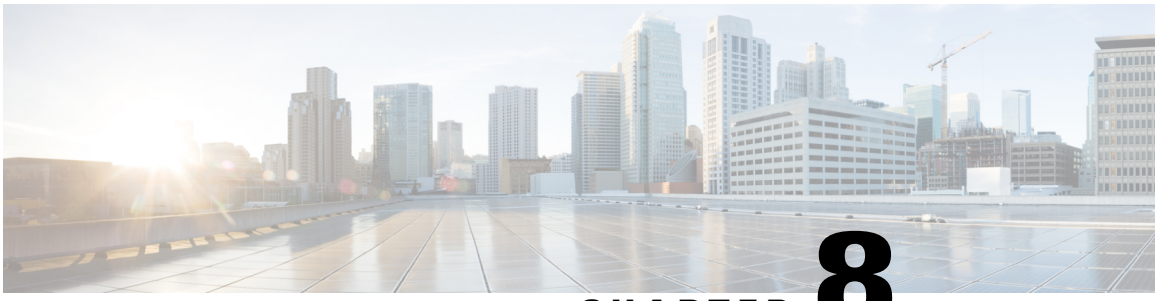
CHAPTER 7

The Vocera Solution

The Vocera Badge utilizes both unicast and multicast packet delivery to provide several key features that make up this complete solution. Here are four of the essential features that rely on proper packet delivery. Also provided is a basic understanding of how each feature uses the underlying network for delivery and functionality.

- Badge to Badge Communications—When one Vocera user calls another user, the badge first contacts the Vocera server, which looks up the IP address of the badge of the callee and contacts the badge user to ask the user if he/she can take a call. If the callee accepts the call, the Vocera server notifies the calling badge of the IP address of the callee badge to setup direct communication between the badges with no further server intervention. All communication with the Vocera server uses the G.711 codec and all badge-to-badge communication uses the G.711 codec and a Vocera proprietary signaling called Vocera RTP.
- Badge Telephony Communication—When a Vocera Telephony server is installed and setup with a connection to a PBX, a user is able to call internal extensions off of the PBX or outside telephone lines. When a Vocera SIP Telephony Gateway server is installed and setup with a connection to a VoIP infrastructure, a user is able to call IP phones using the SIP protocol. Vocera allows users to make calls by either calling out the numbers (five, six, three, two) or by creating an address book entry in the Vocera database for the person or function at that number (for example, pharmacy, home, pizza). The Vocera server determines the number that is being called, either by intercepting the numbers in the extension or by looking the name up in the database and selecting the number. The Vocera server then passes that information to the Vocera Telephony server which connects to the PBX and generates the appropriate telephony signaling (for example, DTMF), or the Vocera SIP Telephony Gateway server in case of a SIP call. All communication between the badge and Vocera server (and between the Vocera server and Vocera Telephony server) use the G.711 codec over unicast UDP.
- Vocera Broadcast—A Vocera Badge user can call and communicate to a group of Vocera badge wearers at the same time by using the Vocera broadcast command, a Push To Talk Session (PTT) or a Panic Call. When a user broadcasts to a group, the user's badge sends the command to the Vocera server which then looks up the members of a group, determines which members of the group are active, assigns a multicast address to use for this broadcast session, and sends a message to each active user's badge instructing it to join the multicast group with the assigned multicast address. After the call setup is done, the communication takes place between the badges, using multicast. The Vocera server is not involved in the multicast audio path. It is only involved in call set up and tear down using unicast signaling to each badge.
- Badge Location Function—The Vocera server keeps track of the access point to which each active badge is associated as each badge sends a keep alive message (Vocera Application Level Ping V_Ping)

every 30 seconds to the server, along with the associated BSSID. This action allows the Vocera system to roughly estimate the location of a badge user. This function has a relatively low degree of accuracy because a Badge might not be associated to the access point to which it is closest.

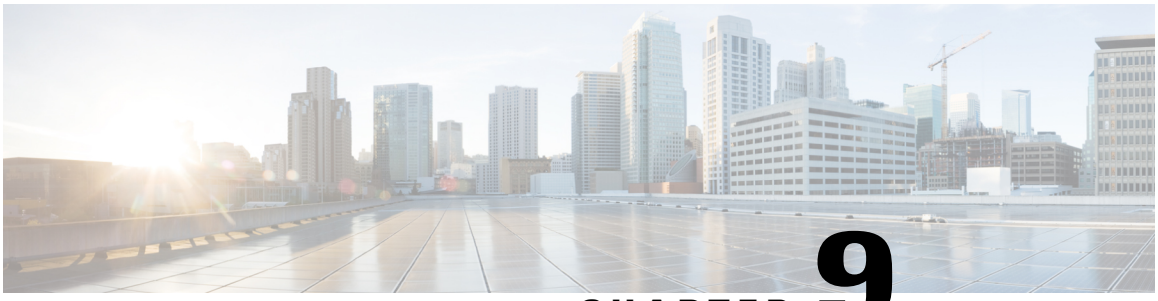


CHAPTER 8

Vocera's Infrastructure Planning

The Vocera Infrastructure Planning Guide, describes the site survey minimum requirements that show that the badge should have a minimum receive signal strength of -65 dBm, a signal-to-noise ratio greater than 25 dB, and proper access point overlap and channel separation. Although the badges use a similar omni directional antenna as a notebook that is used for a site survey, it does not mimic the behavior of the badge very well, given the wearers' effects on signal strength. Given this unique requirement and this behavior of the transmitting device, the use of the Cisco Architecture and Radio Resource Management is ideal in order to make sure that there is lack of unusual radio frequency (RF) site characteristics.

The Vocera badge is a low powered device, worn next to the body. The Vocera requirements in this document can be easily achieved. If the wireless network is designed properly, the badge should be able to work even in environments where many SSIDs are present. However, and just like any other 802.11 device running a voice time-sensitive application, problems like choppy audio may appear in case of poor network design and high RF resource utilization (wireless congestion).



CHAPTER 9

VoWLAN Deployments: Cisco's Recommendations

Wireless IP Telephony networks require careful RF planning. A thorough voice site survey is usually required to determine the appropriate level of wireless coverage and to identify sources of interference. Access point placement and antenna selection choices can be greatly eased with the help of the results of a valid voice site survey. The most important consideration is the transmit power of the wireless phone. Ideally, the phone detects the transmit power of the access point and adjusts its transmit power to that of the access point.

Although the majority of the wireless networks today are deployed after an extensive RF site survey, they are done with keeping data service in mind as well. VoWLAN phones are likely to have different roaming characteristics and different coverage requirements than those of a typical WLAN adapter for a mobile client such as a laptop. Therefore, an additional site survey for voice is often recommended to prepare for the performance requirements of multiple VoWLAN clients. This additional survey gives the opportunity to tune the access points to ensure that the VoWLAN phones have enough RF coverage and bandwidth to provide proper voice quality.

For additional information on RF design considerations, refer to the chapter on WLAN Radio Frequency (RF) Design Considerations in the Cisco Wireless LAN Design Guide, available at http://cisco.com/go/srnd.

This chapter includes the following topic:

Recommendations for Multi-Floor Buildings, Hospitals, and Warehouses

Consider the factors listed in this section when you survey multi-floor buildings, hospitals, and warehouses.

Construction Methods and Materials

Many aspects of the building construction are unknown or hidden from the site survey, so you might have to acquire that information from other sources (such as architectural drawings). Some examples of typical construction methods and materials that affect the range and coverage area of access points include metallic film on window glass, leaded glass, steel-studded walls, cement floors and walls with steel reinforcement, foil-backed insulation, stairwells and elevator shafts, plumbing pipes and fixtures, and many others.

Inventory

Various types of inventory can affect RF range, particularly those with high steel or water content. Some items to watch for include cardboard boxes, pet food, paint, petroleum products, engine parts, and so forth.

Levels of Inventory

Make sure you perform a site survey at peak inventory levels or at times of highest activity. A warehouse at a 50% stocking level has a very different RF footprint than the same warehouse at an inventory level of 100%.

Activity Levels

Similarly, an office area after hours (without people) has a different RF footprint than the same area full of people during the day. Although many parts of the site survey can be conducted without full occupation, it is essential to conduct the site survey verification and tweak key values during a time when the location is occupied. The higher the utilization requirements and the density of users, the more important it is to have a well-designed diversified solution. When more users are present, more signals are received on each user's device. Additional signals cause more contention, more null points, and more multipath distortion. Diversity on the access point (antennas) helps minimize these conditions.

Multi-Floor Buildings

Keep in mind these guidelines when you conduct a site survey for a typical office building:

- Elevator shafts block and reflect RF signals.
- Supply rooms with inventory absorb signals.
- Interior offices with hard walls absorb RF signals.
- Break rooms (kitchens) can produce 2.4 GHz interference through the use of microwave ovens.
- Test labs can produce 2.4 GHz or 5 GHz interference, creating multipath distortion and RF shadows.
- Cubicles tend to absorb and block signals.
- Conference rooms require high access point coverage because they are areas of high utilization.

Extra precaution must be administered when you survey multi-floor facilities. Access points on different floors can interfere with each other as easily as access points located on the same floor. Be careful not to overlap channels between access points on different floors or access points on the same floor. In multi-tenant buildings, there might be security concerns that require the use of lower transmission powers and lower gain antennas to keep signals out of neighboring offices.

Hospitals

The survey process for a hospital is much the same as that for an enterprise, but the layout of a hospital facility tends to differ in these ways:

- Hospital buildings tend to go through many reconstruction projects and additions. Each additional construction is likely to have different construction materials with different levels of attenuation.
- Signal penetration through walls and floors in the patient areas is typically minimal, which helps create micro-cells and multipath variations.
- The need for bandwidth increases with the increasing use of WLAN ultrasound equipment and other portable imaging applications. The need for bandwidth increases with the addition of wireless voice as well.

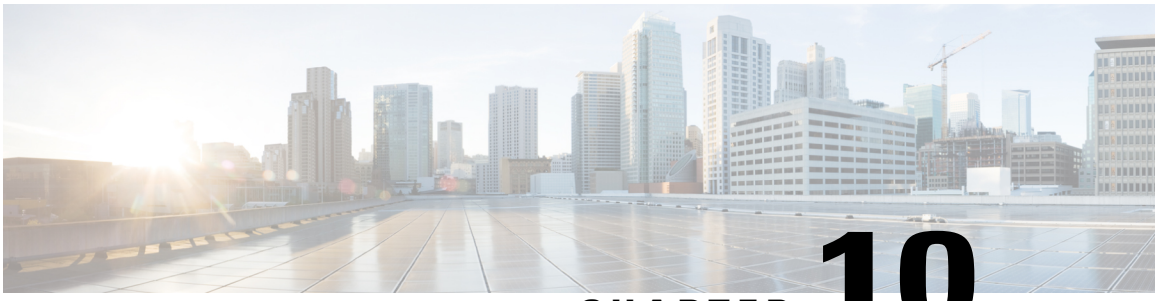
- Healthcare cells are small, and seamless roaming is essential, especially with voice applications.
- Cell overlap can be high, and so can channel reuse.
- Hospitals can have several types of wireless networks installed. This includes 2.4 GHz non-802.11 equipment. This equipment can cause contention with other 2.4 GHz networks.
- Wall-mounted diversity patch antennas and ceiling-mounted diversity omni-directional antennas are popular, but keep in mind that diversity is required.

Warehouses

Warehouses have large open areas that often contain high storage racks. Many times, these racks reach almost to the ceiling, where access points are typically placed. Such storage racks can limit the area that the access point can cover. In these cases, consider placing access points on other locations besides the ceiling, such as side walls and cement pillars. Also consider these factors when you survey a warehouse:

- Inventory levels affect the number of access points needed. Test coverage with two or three access points in estimated placement locations.
- Unexpected cell overlaps are likely because of multipath variations. The quality of the signal varies more than the strength of that signal. Clients might associate and operate better with access points farther away than with nearby access points.
- During a survey, access points and antennas usually do not have an antenna cable connecting them. But in a production environment, the access point and antenna might require antenna cables. All antenna cables introduce signal loss. The most accurate survey includes the type of antenna to be installed and the length of cable to be installed. A good tool to use to simulate the cable and its loss is an attenuator in a survey kit.

Surveying a manufacturing facility is similar to surveying a warehouse, except that there might be many more sources of RF interference in a manufacturing facility. In addition, the applications in a manufacturing facility usually require more bandwidth than those of a warehouse. These applications can include video imaging and wireless voice. Multipath distortion is likely to be the greatest performance problem in a manufacturing facility.



CHAPTER 10

Wireless Network Infrastructure

The wireless IP Telephony network, just like a wired IP Telephony network, requires careful planning for VLAN configuration, network sizing, multicast transport, and equipment choices. For both wired and wireless IP Telephony networks, separate voice and data VLANs is often the most effective and preferred deployment to ensure sufficient network bandwidth and ease of troubleshooting.

This chapter includes the following topics:

Voice, Data and Vocera VLANs

VLANs provide a mechanism for segmenting networks into one or more broadcast domains. VLANs are especially important for IP Telephony networks, where the typical recommendation is to separate voice and data traffic into different Layer 2 domains. Cisco recommends that you configure separate VLANs for the Vocera Badges from other voice and data traffic: a native VLAN for access point management traffic, data VLAN for data traffic, a voice or auxiliary VLAN for voice traffic, and a VLAN for the Vocera Badges. A separate voice VLAN enables the network to take advantage of Layer 2 marking and provides priority queuing at the Layer 2 access switch port. This ensures that appropriate QoS is provided for various classes of traffic and helps to resolve addressing issues such as IP addressing, security, and network dimensioning. The Vocera Badges use a broadcast feature that utilizes multicast to deliver. This common VLAN ensures that when a badge roams between controllers, it remains part of the multicast group. This last process is discussed in detail when multicast is addressed later in this document.

Network Sizing

IP Telephony network sizing is essential to ensure that adequate bandwidth and resources are available to meet the demands presented by the presence of voice traffic. In addition to the usual IP Telephony design guidelines for sizing components such as PSTN gateway ports, transcoders, WAN bandwidth, and so forth, also consider these 802.11b/g issues when you size your wireless IP Telephony network. The Vocera Badges are a specialized application that stretch the number of wired clients beyond our typical deployment recommendations.

Number of 802.11b/g Devices per Access Point

The default maximum number of devices accepted on a Cisco access point is 200. However, this number does not reflect the maximum number of calls that can be placed on a given access point. Each call consumes a share of the access point's available bandwidth. Devices far away from the AP communicate at a lower data rate, and therefore consume more airtime. These devices are also more commonly prone to retries due to losses or collisions. Vocera uses G.711 codec for badge-to-badge and badge-to-phone (G.711 codec) calls. The following table shows the amount of bandwidth consumed by each badge (traffic upstream and downstream), depending on the badge data rate:

Call Process	1 Mbps	2 Mbps	5.5 Mbps	11, 12 Mbps	24 Mbps	36 Mbps	54 Mbps
Badge Bandwidth Consumption (G.711)	9.6%	6.0%	4.3%	3.5%	2.7%	2.6%	2.6%

As data rate increases, the airtime consumed by each call decreases. However, beyond 24 Mbps, the relative gain reduces. This is because the overhead (acknowledgment, interframe spaces) are sent at relatively constant rates. A badge requires 160 kbps, but regardless of the rate, typically sends 27.8 frames per second. Therefore, higher data rates do not reduce the amount of time consumed by overhead. As voice frames are small, the gain from higher data rates represents a small percentage of the total airtime consumed by the call. This is the reason why enabling data rates higher than 24 Mbps does not present distinct performance advantages.

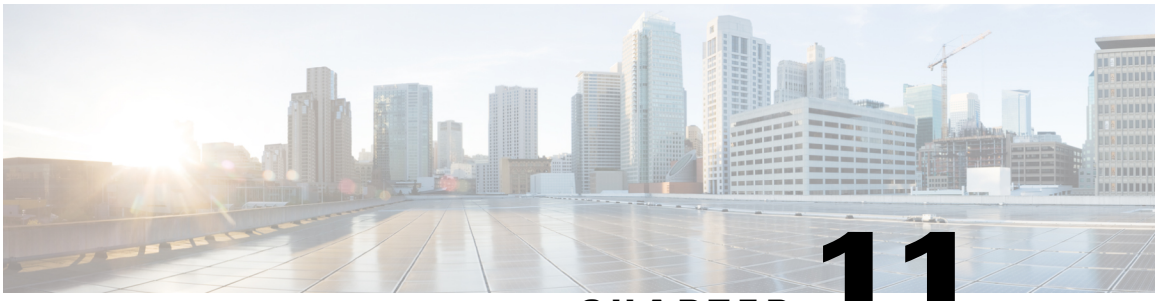
Low data rates consume significantly more airtime than higher data rates. A site survey should be performed to ensure that the badges would always get a signal of -65 dBm or higher, thus allowing data rates of 11 Mbps or higher. The Vocera B2000 or B3000 badge can process frames sent at 11 Mbps when the AP RSSI is -82 dBm or higher, and can support 54 Mbps when the AP RSSI is -65 dBm or better (with a 25 dB SNR or higher). In this configuration, lower data rates (9, 6, 5.5, 2 and 1 Mbps) can be disabled. Data rates higher than 24 Mbps can be left enabled or disabled. Disabling these higher data rates presents the advantage of avoiding scenarios where the phone has to rate-shift between data rates, delaying frame transmission for little or no gain in the transmission performances.

Once the proper rates are enabled, a Cisco 802.11n access point can support up to 20 concurrent calls in the 2.4 GHz band. This number represents a configuration where site survey was done properly, and no other interferers (including overlapping access points on the same channel) affects the local access point 2.4 GHz radio. You should reduce this number after testing in environments presenting different characteristics.

Also keep in mind that this is the maximum number of concurrent calls, not the maximum number of devices in the cell. As Vocera badge communications are usually short, you may have more than 20 badges in a given AP cell while not exceeding 20 concurrent calls.

Multicast messages are sent to the wireless cell at the highest mandatory rate supported by all clients currently associated with the AP. Allowing one mandatory rate allows you to determine the rate at which multicast packets will be sent. In networks where you expect a wide utilization of the “push-to-talk” or “Broadcast-to” function, you may want to set higher rates to mandatory, so as to allow multicast packets to be sent at higher rate. A common practice in this case it to set 24 Mbps as mandatory. Another common practice is to enable the Multicast Direct feature for the multicast address used by the badges (default 230.230.x.y). When this feature is enabled, the multicast flow is converted into a unicast flow at the AP level and sent to each Vocera badge client at optimal speed (which is commonly a high data rate, and often higher than the higher mandatory rate if the badge is within good range of the access point). This conversion also presents the advantage of

ensuring frame delivery to each badge, as each unicast frame is acknowledged by the client (and resent if no acknowledgment is received. This mechanism enhances the reliability of the frame delivery. As the frame may have to be distributed multiple times (one time per badge associated to a given AP, instead of one time for the entire cell with a multicast frame), this process may increase the delivery time of each packet, if several badges are in the call and far from the access point. This may be an issue in congested networks. However, the increased reliability typically outweighs the slight increase in airtime consumption.



CHAPTER 11

Switch Recommendations

You can create a switch port template for use when you configure any switch port for connection to an access point. This template should add all the baseline security and resiliency features of the standard desktop template. In addition, when you attach the access point to a Cisco Catalyst 3750 or 3850 Switch, you can optimize the performance of the access point by using Multilayer Switching (MLS) QoS commands to limit the port rate and to map Class of Service (CoS) to Differentiated Services Code Point (DSCP) settings.

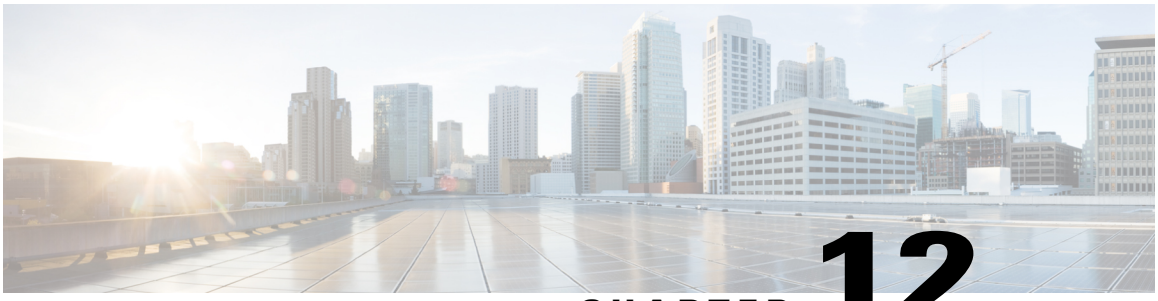
Any traffic that is not required by WLAN clients should not be sent to an access point. A template should be designed in such a way that it helps to create a secure and resilient network connection with these features:

- Return Port Configurations to default— Prevents configuration conflicts by clearing any pre-existing port configurations.
- Disable Dynamic Trunking Protocol (DTP)— Disables dynamic trunking, which is not needed for connection to an access point.
- Disable Port Aggregation Protocol (PagP)— PagP is not needed for user-facing ports.
- Enable Port Fast—Allows a switch to quickly resume forwarding traffic if a spanning tree link goes down.
- Configure Wireless VLAN—Creates a unique wireless VLAN that isolates wireless traffic from other data, voice, and management VLANs. This isolates traffic and ensures greater control of traffic on the wired infrastructure.
- Enable Quality of Service (QoS); do not trust port (mark down to 0)—Ensures appropriate treatment of high-priority traffic, including softphones, and prevents users from consuming excessive bandwidth by reconfiguring their PCs. Please refer to the mobility design guide for more details, at: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob73dg/ch5_QoS.html

Vocera badges use Voice marking. The following QoS information can be used to filter Vocera packets:

- IP Precedence (Class Selector) = 5 (101 binary)
- DSCP = Expedited Forwarding (EF) or 46 (101110 binary)
- IP ToS = 0xB8 (10111000)

Inline Power Switches can be used to provide power to access points that are capable of receiving inline power.



CHAPTER 12

Multicast in a Cisco CAPWAP Deployment

Understanding multicast within a CAPWAP deployment is necessary to deploy the Vocera "Broadcast to" command, Push to Talk session (PTT) and "Panic" functions. With Vocera broadcast function, a badge can inform the Vocera server that the badge needs to communicate to several devices. This communication to several badges will occur through the use of a multicast address. The Vocera server forwards the request to the target badges, requesting them to join the intended multicast address. The Vocera server does not play any further role in the communication. The source badge sends traffic to the intended multicast address. As the target recipients subscribed to the multicast flow, they receive the multicast traffic and the messages it contains. In this topology, the multicast packet is first receive by a controller (coming from the sending badge), and must be relayed to the wireless cells where the target recipients reside. This document later covers the essential steps to enable multicast within the controller-based solution. There are currently two delivery methods that the CAPWAP controller uses to deliver multicast to the clients:

- Unicast-Multicast Delivery Method
- Multicast-Multicast Delivery Method

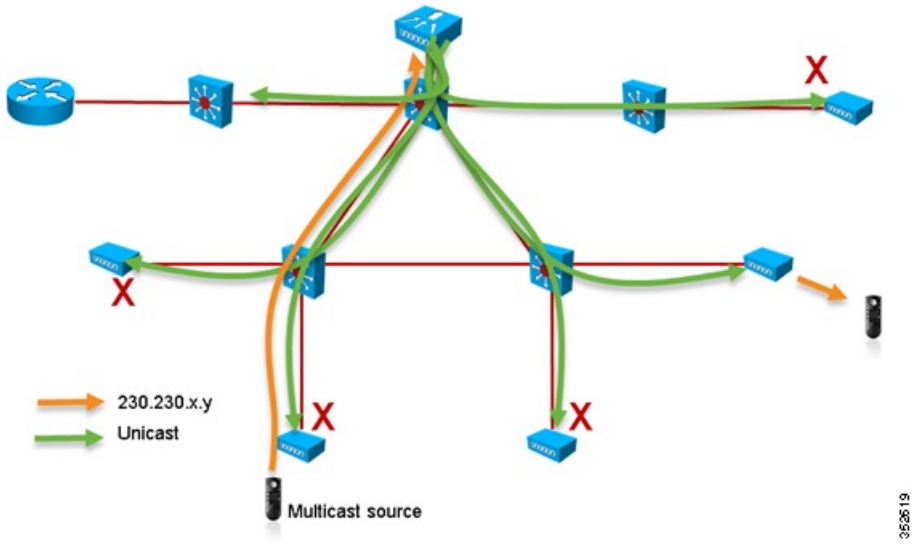
This chapter includes the following topics:

Unicast-Multicast Delivery Method

The unicast-multicast delivery is a legacy method, where the Wireless LAN Controller creates a copy of every multicast packet and forwards it to every access point. When a client sends a multicast join to the wireless LAN, the access point forwards this join through the CAPWAP tunnel to the controller. The controller bridges this multicast join onto its directly connected local area network connection that is the default VLAN for the associated WLAN of the client. When an IP multicast packet arrives from the network to the controller, the controller replicates this packet with a CAPWAP header for each access point. When the source of the multicast

is also a receiver within the wireless domain, this packet is also duplicated and forwarded back to the same client who sent this packet. This is not the preferred method of multicast delivery within the Cisco Wireless solution. The unicast delivery method works with small deployments. However, due to the considerable overhead on the Wireless LAN Controller (WLC), this is never the recommended multicast delivery method.

Figure 1: CAPWAP Multicast-Unicast



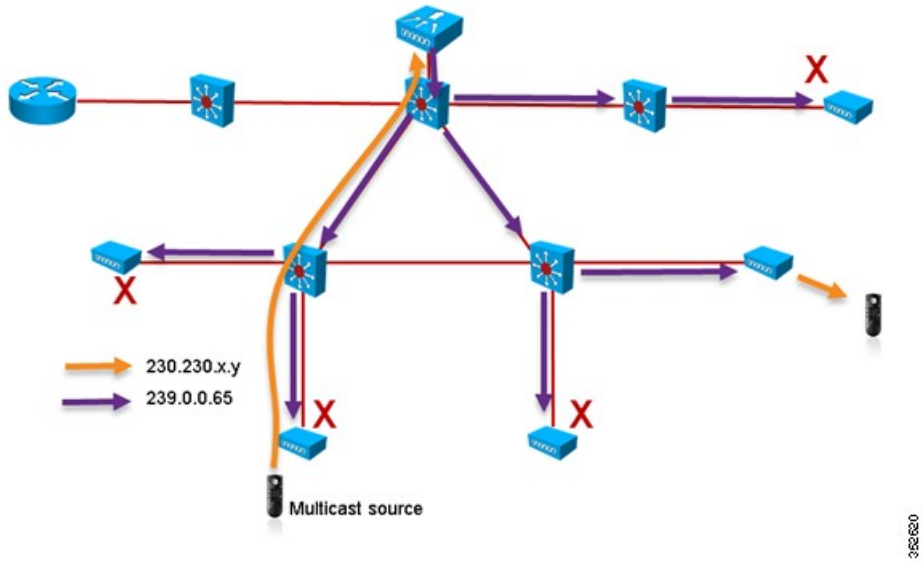
Note If AP Group VLANs are configured, and an IGMP join is sent from a client through the controller, it is placed on the default VLAN of the WLAN that the client is on. Therefore, the client might not receive this multicast traffic unless the client is a member of this default broadcast domain.

Multicast-Multicast Delivery Method

The multicast-multicast delivery method does not require the controller to replicate each multicast packet received. The controller is configured for an un-used multicast group address that each access point becomes a member of. With Figure 3, the multicast group defined from the WLC to the access point is 239.0.0.65. When a client sends a multicast join to the WLAN, the access point forwards this join through the CAPWAP tunnel to the controller. The controller can forward this link-layer protocol onto its directly connected local area network connection that is the VLAN for the associated WLAN of the client. The controller can transparently relay multicast client packets to the wired infrastructure (in which case the infrastructure sees the wireless client as the multicast client), or act as a proxy (in which case the infrastructure sees the controller as the multicast client). In both cases, the router that is local to the controller then adds this multicast group address to that interface for forwarding ((*,G)) entry. With Figure 3, the example multicast join was sent to the multicast group 230.230.x.y, which is the default multicast address used by Vocera badges. When the network forwards multicast traffic, the multicast address of 230.230.x.y is forwarded to the controller. The controller then encapsulates the multicast packet into a CAPWAP multicast packet addressed to the multicast group address (example here is 239.0.0.65) that is configured on the controller and forwards to the network. Each access point on the controller receives this packet as a member of the controller's multicast group. The access point then forwards the client's/server's multicast packet (example here is 230.230.x.y) to the

WLAN/SSID identified within the CAPWAP multicast packet, on each radio having a client for this multicast traffic. The access points that do not have clients for this multicast flow drop the multicast frame.

Figure 2: CAPWAP Multicast-Multicast



Router and Switch Multicast Configuration

This document is not a network multicast configuration guide. Refer to Configuring IP Multicast Routing for a complete implementation story. This document covers the basics to enable multicast within your network environment.

Enable IP Multicast Routing

IP multicast routing allows the Cisco IOS® software to forward multicast packets. The `ip multicast-routing` global configuration command is required to allow multicast to function in any multicast enabled network. The ip multicast-routing command should be enabled on all routers within your network between the WLC(s) and their respective access points.

```
Router(config)#ip multicast-routing
```

Enable PIM on an Interface

This enables the routing interface for Internet Group Management Protocol (IGMP) operation. The Protocol Independent Multicast (PIM) mode determines how the router populates its multicast routing table. The example provided here does not require the rendezvous point (RP) to be known for the multicast group and therefore sparse-dense-mode is the most desirable given the unknown nature of your multicast environment. This is not a multicast recommendation to be configured to work although the Layer 3 interface directly connected to your controller should be PIM enabled for multicast to function. All interfaces between your WLC(s) and their respective access points should be enabled.

```
Router(config-if)#ip pim sparse-dense-mode
```

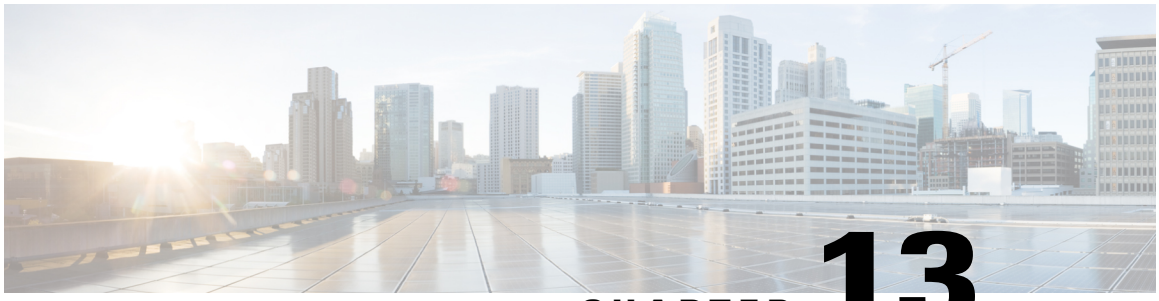
Switch VLAN IGMP Snooping

Roaming and multicast are not defined with a set of requirements to verify that multicast traffic can follow a subscribed user. Although the client badge is aware that it has roamed, it does not forward another IGMP join to make sure that the network infrastructure continues to deliver the multicast (Vocera broadcast) traffic to the badge. However, the controller is aware of the roaming event, and immediately sends a general IGMP query to any client that just roamed and requires multicast forwarding. The client then responds with the IGMP group that they are a member of and this is bridged to the wired network as described earlier in this document. When a client roams to a controller that does not have Layer 2 connectivity, or a Layer 3 roam, synchronous routing is added for multicast source packets. When a client, who has completed a Layer 3 roam sources a multicast packet from the wireless network, the foreign controller encapsulates this packet in the Ethernet over IP (EoIP) in IP tunnel to the anchor controller. The anchor controller then forwards that to the wireless clients locally associated as well as bridges this back to the wired network where it is routed using normal multicast routing methods.

IGMP snooping allows a switched network with multicast enabled to limit traffic to those switchports that have users who want multicast to be seen while pruning the multicast packets from switchports that do not wish to see the multicast stream. In a Vocera deployment, because the controller takes care of forwarding to the wired infrastructure all IGMP messages for all wireless clients needing multicast traffic, you can enable CGMP or IGMP snooping on the upstream switchport to the controller. This prevents multicast messages from flooding to the controller port when they are not needed. Vocera badges use IGMPv2 by default.

Refer to Configuring IGMP Snooping for more information.

```
Router(config)#interface vlan 150
Router(config-if)#ip igmp snooping
```



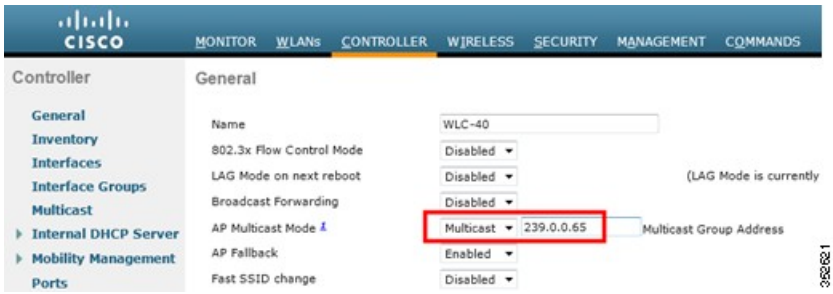
CHAPTER 13

Deployment Scenarios

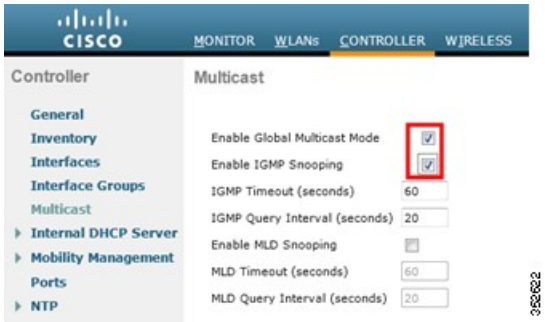
The following deployment scenarios cover best practices and design parameters to help with a successful Vocera Badge deployment:

- Single Controller Deployment
- Multiple Controller Layer 2 Deployment
- Multiple Controller Layer 3 Deployment

Understanding how the Vocera Badge features interact within a CAPWAP split MAC environment is essential. With all deployment scenarios, multicast should be enabled. The recommended mode is multicast-multicast.



When enabling multicast support, IGMP snooping allows the controller to act as a proxy for multicast messages, thus limiting the amount of IGMP messages originated from the wireless clients to be forwarded to the wired infrastructure. IGMP snooping is the recommended mode.



This chapter includes the following topics:

Single Controller Deployment

This is the most straight forward deployment scenario. It allows you to deploy the Vocera Badge solution with little deployment concerns. Your network must be enabled for IP multicast routing only to allow the access points to receive the CAPWAP multicast packets. If required, you can limit network multicast complexity by configuring all routers and switches with the controllers multicast group.

The Vocera badge solution and all its functions operate as expected when multicast is enabled globally on the controller, the proper SSID and security settings are configured, and all the access points are registered. With the Vocera Broadcast function, a user roams and the multicast traffic follows as expected. There are no extra settings required to be configured to allow this solution to function properly.

When a Vocera Badge sends a multicast message, as it does with the Vocera Broadcast, it is forwarded to the controller. The controller then encapsulates this multicast packet within a CAPWAP multicast packet. The network infrastructure forwards this packet to every access point that is connected to this controller. When the access point receives this packet, it then looks at the CAPWAP multicast header to determine the WLAN/SSID, and it then broadcasts this packet, if there is any multicast client (typically another Vocera badge) for this multicast packet

Multiple Controller Layer 2 Deployment

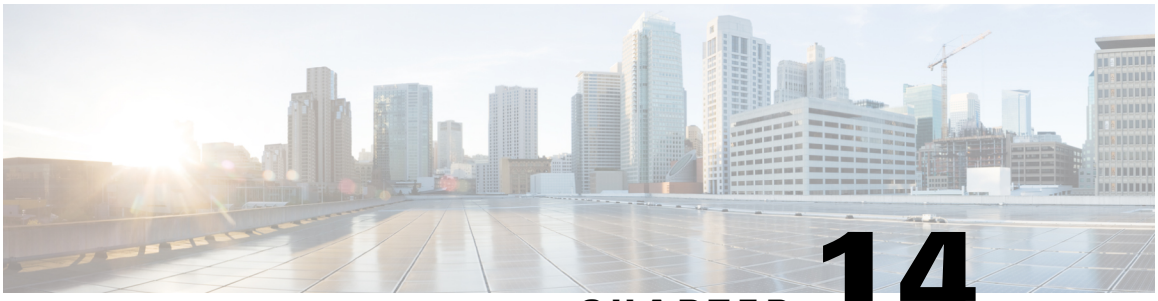
In a Layer 2 deployment, multiple controllers all have connectivity to each other via the same Layer 2 broadcast domain. Controllers are configured for multicast as shown, using a different access point multicast group on each controller. This configuration ensures that access points associated to controller 1 do not receive and process multicast messages destined for access points associated with controller 2[1]. With the assumption that this Layer 2 broadcast domain is connected via a common switch or a common set of switches, CGMP/IGMP snooping on these switches can be enabled for this single VLAN. With the Vocera Broadcast function and a user roam from an access point on one controller to an access point on a different controller, the badge automatically sends a new membership report upon roaming. At the same time, controllers processing the roaming event will send to the roaming client a general IGMP query immediately after authentication on the new controller, to ensure that it learns about all the multicast groups subscribed by the roaming device. The client should then respond with the interested groups and the new controller then makes sure that the IGMP message is forwarded to the upstream router via the locally connected switch. This allows the advantages of IGMP and CGMP snooping on your upstream switches, without interrupting the multicast flow.

You can create additional badge SSIDs and Layer 2 domains for separate badge networks as long as your network is configured to pass multicast traffic appropriately. However, common practice is to create one SSID for all badges. Also, each Vocera Layer 2 broadcast domain created must exist everywhere a controller is connected to the network so as not to break multicast.

1 Configuring different access point multicast groups is a recommended configuration. However, a controller and its APs automatically discard multicast packets sent to CAPWAP ports and a multicast address different from the access point multicast address configured on the controller, as these packets are necessarily exchanges between another controller and its APs.

Multiple Controller Layer 3 Deployment

The Layer 3 roaming deployment strategy can also be used with controller-to-controller roaming with WLC software release 4.0.206.0 or later. If a client that has been connected to the Vocera broadcast group receives the appropriate multicast stream roams to another controller as a Layer 3 roam with the CAPWAP Layer 3 roaming configured, it is queried for interested multicast groups. The client, when sourcing to the same Vocera broadcast group, has these packets delivered to the anchor controller through the EoIP tunnel and has these packets routed through normal multicast routing methods.



CHAPTER 14

Deployments and Configuration

This chapter includes the following topics:

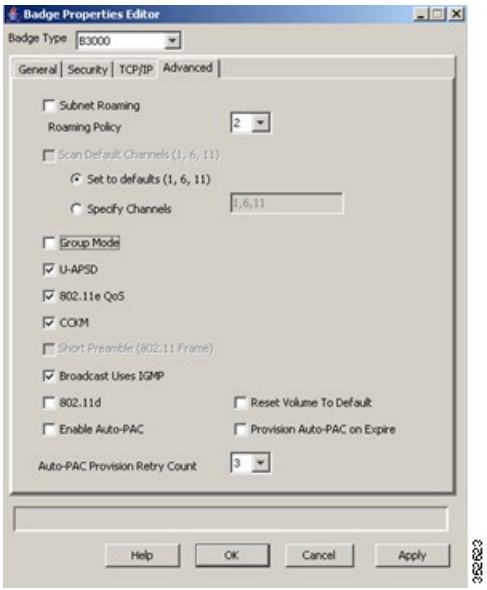
Badge Configuration

An incorrectly configured badge can introduce unnecessary roaming latency into your environment. Using the BCU and the Badge Properties Editor (BPE), verify these settings (see Figure below):

- Subnet Roaming is disabled. This function allows the badge to get a new IP address when roaming to another subnet. With Cisco L3 roaming, the badge is maintained in its subnet of origin, and the badge should not attempt to obtain a new IP address while roaming.
- Scan Default Channels (1,6,11) is selected and set to default. When this setting is not checked, the badge scans all 802.11b/g channels when the badge looks to roam. The badge scans segments of 3 channels at a time, then waits 2 seconds before moving to the next 3 channel segment. This prevents the forwarding of packets and seamless roaming.
- Broadcast Uses IGMP is enabled.
- Roaming Policy is set to 2 or higher. The roaming policy decides about the aggressiveness of the badge roaming behavior. Roaming policy set to 2 is the default, and initiates roaming when the AP SNR is 20 dB or less. Roaming policy set to 3 would initiate roaming when the AP SNR would be 22 dB or less, and is adapted to environments with small cells and where high voice quality is always needed. Roaming policy 1 and 0 would initiate roaming when the AP SNR would be less than 18 and 16 dB respectively, and are not recommended values.

- U-APSD and 802.11e QoS should be enabled. Notice that U-APSD and 802.11e-QoS are enabled together. In other words, on Vocera code 4.3 and later; enabling 802.11e QOS automatically enables U-APSD (and vice versa). Disabling 802.11e QOS automatically disables U-APSD (and vice-versa).

Figure 3: Vocera BPE Advanced Tab



Tune AutoRF for Your Environment

As described in the VoWLAN Deployments: Cisco's Recommendations section of this document, it is important to understand that each site has its own RF characteristics. AutoRF or Radio Resource Management (RRM) might need to be tuned, with the understanding that each site is different and AutoRF/RRM should be tuned for your environment.

Before you adjust AutoRF, refer to Radio Resource Management under Unified Wireless Networks for more information.

RRM allows you to adjust the transmit power of each access point, by adjusting how strong each access point hears its third strongest neighbor. This value can be adjusted from the CLI using the `config advanced 802.11b tx-power-thresh` command as described in Tx Power Level Assignment Settings or from the web interface, under **Wireless > 802.11b/g/n > RRM > TPC**.

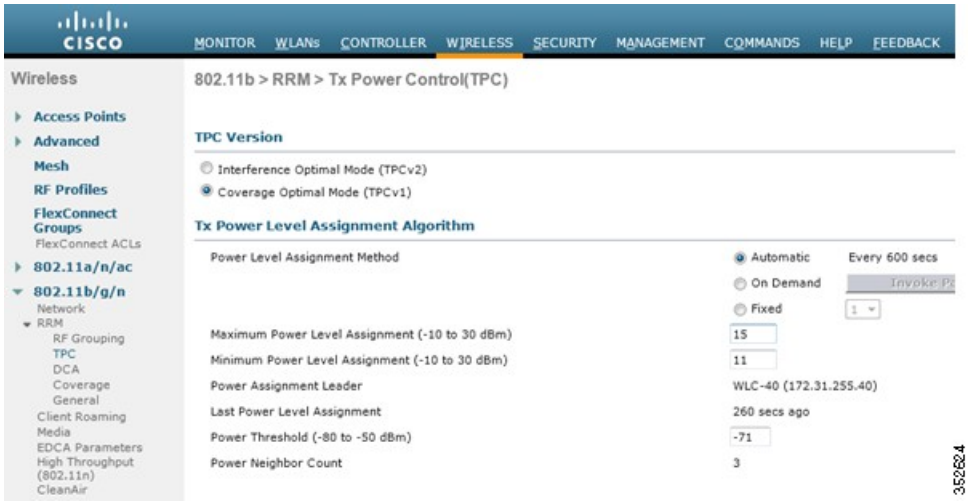
Before you adjust AutoRF, walk the deployment site using the Vocera badge as worn by the end user and use a site survey tool in order to gain a strong understanding of how the badge roams and at what power each access point is seen. Once this is complete and if it is determined that adjusting this value is required, begin with a value of –71 dBm for the Transmit Power Control algorithm. Use this CLI parameter:
`config advanced 802.11b tx-power-thresh -71`

Allow the network to work through this adjustment with a minimum of 30 minutes to an hour before you observe any changes. Once the network is given a sufficient amount of time, walk the site using the same survey tool and badges again. Observe the same roaming characteristics and access point power. The goal here is to attempt to have the badges roam at or before the next access point to get the best possible signal-to-noise ratio. At the edge of each cell, the AP RSSI should be -65 or better, and SNR 25 or higher.

The badge will attempt to roam solely based on the AP SNR, when the SNR level is less than 20 dB (with Roaming Policy of 2).

The AP power should not be too high, as a large mismatch between the AP and the badge power levels can result in one way audio issues. The B2000 and B3000 badge typical power is about 16 dBm (15.8 dBm, or 38 mW, for the B3000, and 14.5 dBm, or 28 mW, for the B2000). Therefore, it is recommended to set the AP max power value to 15 dBm or less. As coverage from another access point is expected when the badge gets close to the cell edge, the AP power level can be slightly less than the badge power level. Power should not be too low either. If there is a high difference between the badge power and the AP (low) power, the badge may not roam properly. To avoid such design issues forcing the AP to reduce its power level too much, set the AP minimum power assignment to 11 dBm. If the AP density forces RRM to reduce the AP power below 11 dBm, your badges will be likely to encounter coverage holes when roaming. When the AP power is high, each badge may suffer from interferences caused by detecting too many APs. You may need to adjust the AP density to avoid this behavior.

Figure 4: 802.11b/g/n Auto-RF configuration



How do I know if the AP transmit power is too high or too low?

Determining whether you have your transmit power threshold too high or too low requires a good understanding of your environment. If you have walked your entire deployment area (where you expect your Vocera badges to function), you should know where your access points are located as well as experience the roaming behavior of the badge.

What do I do if my transmit power is too high?

The Vocera Badge roams based solely on the signal quality (SNR) rather than pure signal strength (RSSI). If the Vocera Badge does not roam after it passes several access points while engaged in the welcome tutorial or the test tone, the badge is considered to be sticky. If this behavior is indicative of the entire campus deployment area, then your transmit power threshold is too hot and should be backed down. If only one or two isolated areas show this behavior and the rest of the deployment area shows more idealistic roaming characteristics this is not an indication that your network is running too hot.

What do I do if my transmit power is too low?

The default transmit threshold should almost never provide you a deployment area where your network runs too cold. If the transmit power threshold is adjusted down, and walking the halls with the Vocera Badge provides you with an environment where the badge roams well, but loses connectivity and/or dead/spotty coverage, then your network might have been tuned too low. If this is not characteristic of your entire network but isolated to one or two areas, then it is more indicative of a coverage hole rather than a network-wide problem.

Isolated Behavior

If you find that in one or two areas, the badge sticks to an access point rather than roaming in an idealistic manner, examine this area.

- How is this area different from the rest of the campus?
- If this/these areas are near building exits or areas under construction, could coverage hole detection be forcing these access points to raise the power?
- Look at the WLC log file and access point neighbor lists to help determine why such an anomaly could occur.

If you find that in one or more isolated areas, the badge experiences dead or spotty coverage, then you need to examine these areas separately.

- Is this area near an elevator shaft, radiology, or a break room?
- These areas might be better suited by the installation or better placement of an access point to allow for better voice coverage.

In both cases, it is always advisable to understand that you are working in an unlicensed radio spectrum and idealistic behavior might not ever be achievable. This could happen when you are situated next to a radio transmission tower or device, a television transmitter or possibly a non-802.11 2.4 GHz repair facility (wireless phones, and so forth).

Security Mechanisms Supported

In addition to static WEP and Cisco LEAP for authentication and data encryption, the Vocera Badges also support WPA (TKIP encryption) and WPA2 (AES-CCMP encryption), with PEAP (MS-CHAP v2), EAP-TLS, EAP-FAST, and PSK authentication. The encryption capabilities are as follows:

Security	Authentication	Encryption	B2000	B3000	Smartphone
Open	Open	None	Yes	Yes	Yes
		WEP 40	Yes	Yes	Yes
		WEP 128	Yes	Yes	Yes

Security	Authentication	Encryption	B2000	B3000	Smartphone
WPA	PSK	TKIP	Yes	Yes	Yes
	PEAP MSChapv2	TKIP	Yes	Yes	Yes
	EAP-TLS	TKIP	Yes	Yes	No
	EAP-FAST	TKIP	Yes	Yes	No
	LEAP	TKIP	Yes	Yes	No
WPA2	PSK	AES-CCMP	No	No	Yes
	PEAP MSChapv2	AES-CCMP	Yes	Yes	Yes
	EAP-TLS	AES-CCMP	Yes	Yes	No
	EAP-FAST	AES-CCMP	Yes	Yes	No
Dynamic WEP	LEAP	WEP 40	Yes	Yes	No
	LEAP	WEP 128	Yes	Yes	No
CKIP	LEAP	CKIP	Yes	Yes	No

When using an authentication method relying on individual user authentication, ensure that strong passwords are used on all wireless devices. Strong passwords are defined as being between 10 and 12 characters long and can include both uppercase and lowercase characters as well as the special characters. Cisco recommends that you use different user names and passwords on data clients and wireless voice clients. This practice helps with tracking and troubleshooting as well as security. Although it is a valid configuration option to use an external database to store the user names and passwords for the badges, Cisco does not recommend this practice. Because the RADIUS server must be queried whenever the badge roams between access points, the unpredictable delay to access a database external to the RADIUS server site could cause excessive delay and poor voice quality.

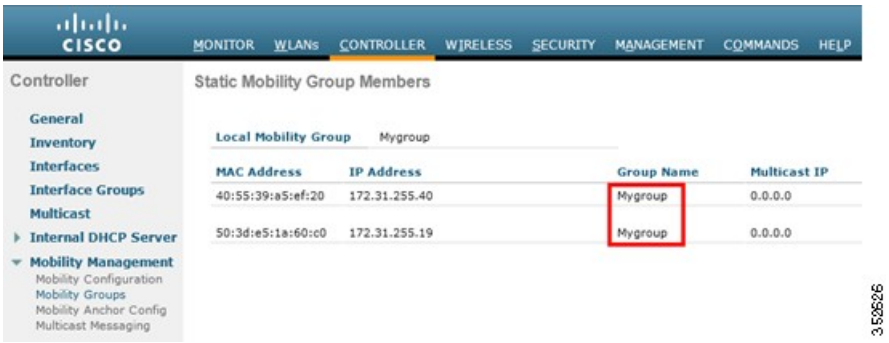
Also keep in mind that fast roaming is a key consideration in voice deployments. The Vocera badges support CCKM (Cisco Centralized Key Management). This mode ensures that roaming between access points and controllers do not need new connections to the RADIUS server, that would increase the roaming delay. Combined with AES-CCMP encryption, CCKM (as shown in figure 6) combines strong security and fast

roaming. WPA and WPA2 modes should not be mixed on the same WLAN. Cisco recommends using WPA2/AES.

Figure 5: CCKM configuration

Because CCKM only works optimally within a mobility group, make sure that all controllers share the same mobility group name, as shown in figure 7.

Figure 6: Mobility group configuration



CCKM is a key component of fast roaming configuration, because roaming can introduce important latency issues when authentication has to be performed after roaming occurs. When the WLAN security uses PSK (with WPA or WPA2), reauthentication typically consumes approximately 40 ms (without RF congestion issues). When 802.1x/EAP is used, communication to the RADIUS server can introduce a delay larger than 1 second for the authentication phase. The Vocera Infrastructure Guide (p51) lists common authentication delay and recommendations for the B2000 and B300m security setup.

As with most voice deployments, aggressive load-balancing should be disabled, as this feature delays roaming. When the deployment contains only B2000 and B3000 badges (that only support 802.11b/g), Cisco BandSelect is not needed, as the badge will not steer to the 5 GHz band. However, in mixed deployments where the same SSID is shared between Vocera badges (802.11b/g only) and other, 802.11a/b/g devices, Cisco BandSelect is recommended to encourage the 802.11a/b/g devices to be steered toward the 5 GHz band, and leave more space in the 2.4 GHz band for the badges. Cisco BandSelect is not recommended with Vocera smartphones deployments, as it can delay roaming of dual-band devices. The Vocera administrator can configure which band (2.4 Ghz or 5 GHz) the smartphone is required to use. You should use this configuration possibility to force the smartphone to a target band.

The Cisco Unified Wireless Network design and deployment guide should be followed for the overall configuration of your WLC(s). This section provides additional recommendations specific to Vocera® Communication Badges.

Note Changes are left unsaved if you do not press the **Apply** button before you move to the next step.

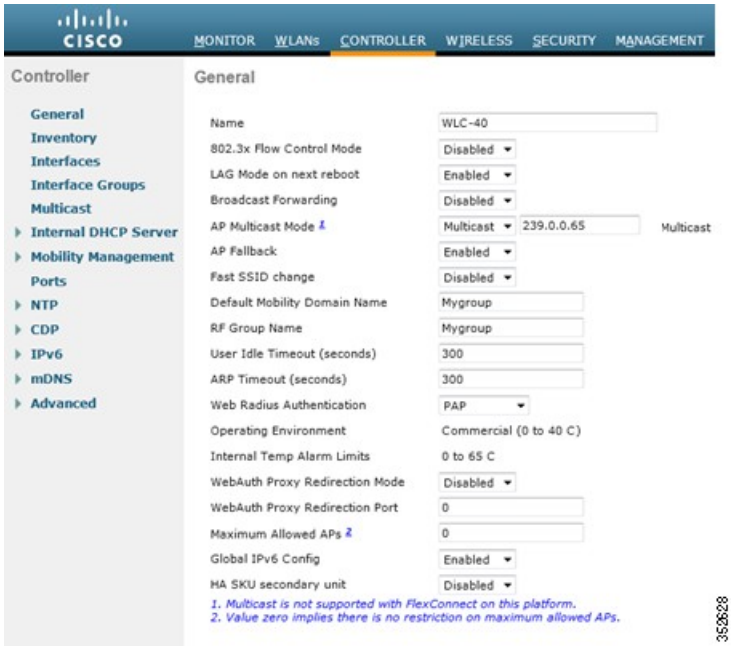
Complete these steps under the **Controller** top-level menu:

1. Make sure that the AP Multicast Mode is set to **Multicast**.
2. Set an AP Multicast Group Address, for example **239.0.0.65** (or another unused multicast group address). Cisco recommends using a different AP Multicast Group for each controller.

Note By default, Vocera push to talk function uses multicast and transmits Multicast using an IP range of 230.230.0.1 to 230.230.15.254 or a MAC prefix of 00:01:5E:66. Make sure NOT to use this address range for the AP multicast address. Cisco recommends using the Administrative range, 239.0.0.0 to 239.255.255.255.

3. Set the Default Mobility Domain Name and RF-Network Name to your network design.

Figure 7: General WLC Configuration



Create Interfaces

Click **Controller > Interfaces**.

Note Your VLAN and IP address varies. The screen shots here provide sample addressing which should not be directly followed.

Figure 8: List of WLC Interfaces

Create the Vocera Voice Interface

Complete these steps:

1. Click **New**.
2. Enter a tag name representative of your Vocera VoWLAN network in the Interface Name field.
3. Enter the VLAN number of that VoWLAN network in the VLAN ID field.
4. Click **Apply** and then click **Edit** in order to edit the interface that you just created.
5. Enter the IP addressing for this interface that is in the range of the VLAN and other related information.
6. Click **Apply**.

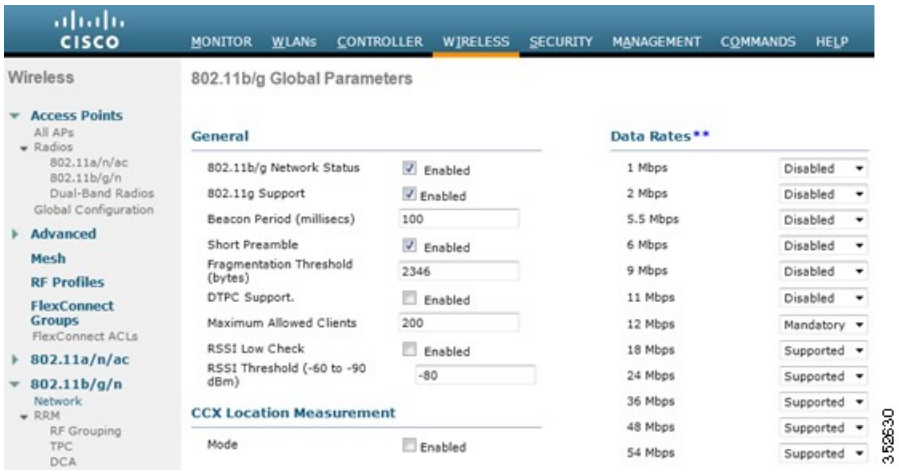
Wireless-Specific Configuration

For a WLAN that has only Vocera Badges, this configuration provides sample settings that best support the Vocera Broadcast application.

- Support for 802.11g is enabled. 802.11b is not needed for Vocera SSIDs, but is supported. If you enabled 802.11b, set 11 Mbps to Mandatory and disable all lower rates. If you enabled 802.11g only, a common practice is to set 12 Mbps to Mandatory, and disable all lower rates. In this example, rates higher than 24 Mbps are also disabled, but these rates can also be left enabled.
- Beacon interval is set to 100 (default). The badge needs this interval to confirm that the SSID is still available on the AP.
- Short preamble is enabled.

• DTPC is disabled (Vocera badges do not support DTPC).

Figure 9: 802.11b/g Configuration

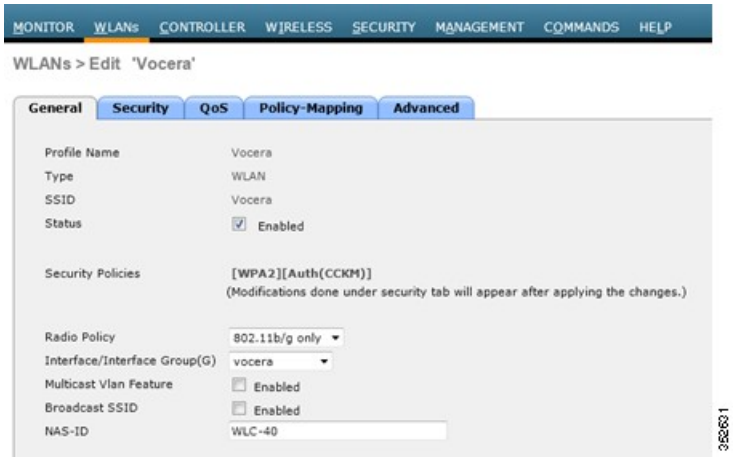


WLAN Configuration

Complete these steps:

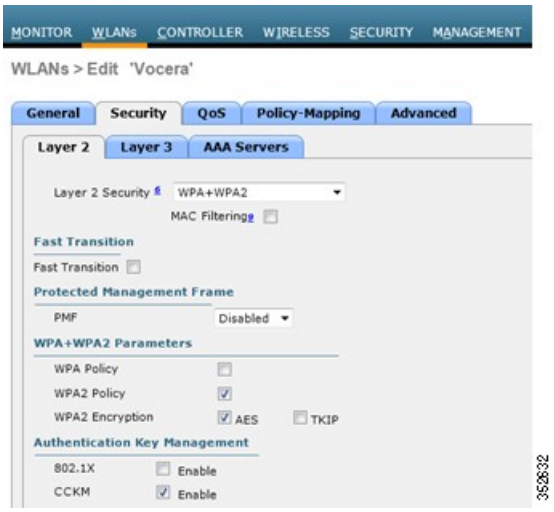
1. Update the Radio Policy field to 802.11b/g only for B2000 and B3000 badges.
2. Change Admin Status to **Enabled**.
3. Optionally, set Broadcast SSID to **Enabled**. Badges use active scanning, and will also detect the SSID with SSID Broadcasting disabled.
4. Set the Interface Name to the interface created for the Vocera Communication Badges.

Figure 10: WLAN Configuration



5 Set the security options to match your corporate policy. A 802.1x/EAP authentication method with AES-CCMP encryption provides the highest security. CCKM ensures fast roaming.

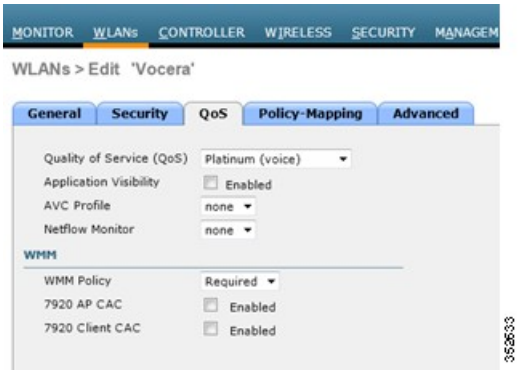
Figure 11: WLAN Security Configuration



6 Set Quality of Service to **Platinum**.

7 Set the WMM policy to **Allowed** or **Required**. Cisco recommends using **Required**.

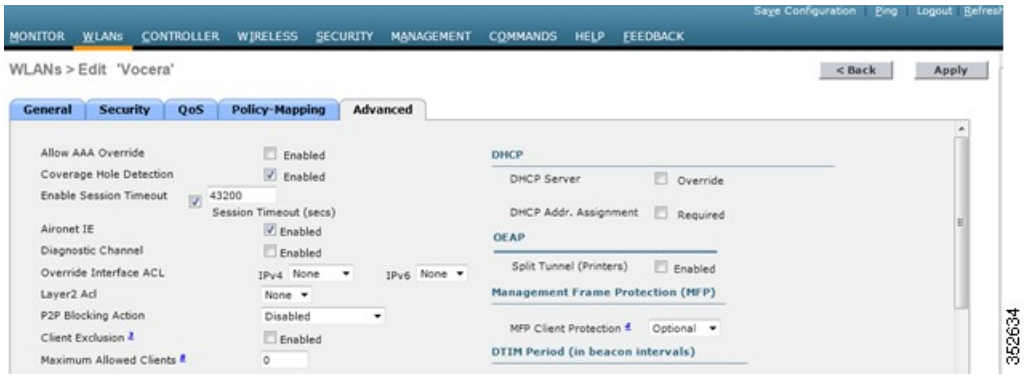
Figure 12: WLAN QoS Configuration



8 In the Advanced tab, set **DTIM** to 1.

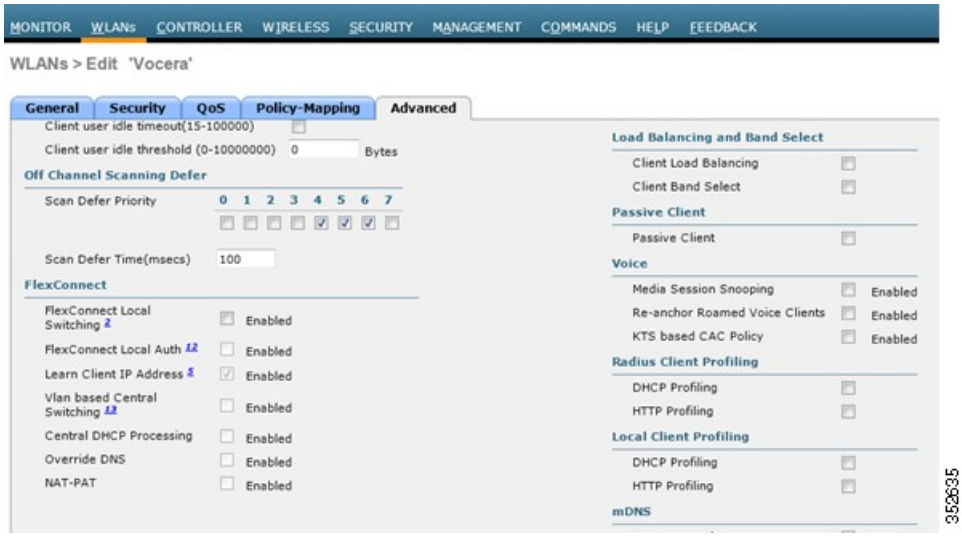
9 **Client Exclusion** is usually not needed. In some cases, delays and retries in the authentication process result in a badge being excluded. To avoid this issue, **Client Exclusion** can be left disabled.

10 In some cases, you may need to statically configure the badge IP address (especially when logs need to be collected and sent to a destination other than the FTP server). For this reason, you may want to uncheck the **DHCP Address Required** option.



11 Make sure that the **Off Channel Scanning Defer** feature is enabled for the voice queue (UP 6).
12 Uncheck **Client Band Select** for Badge only networks, check **Client Band Select** for deployments where badges and 802.11a/b/g devices share the same SSID.
13 **P2P Blocking** is set to Disabled to allow badge-to-badge communication.
14 **Client Load Balancing** is disabled.
15 **Session timeout** is typically set to 12 hours (43200 seconds).

Figure 13: WLAN Advanced Configuration



Coverage hole detection can be left enabled. However, this feature should not be needed if your design was conducted properly. Keeping the feature enabled aims at confirming that the controller does not report such events.

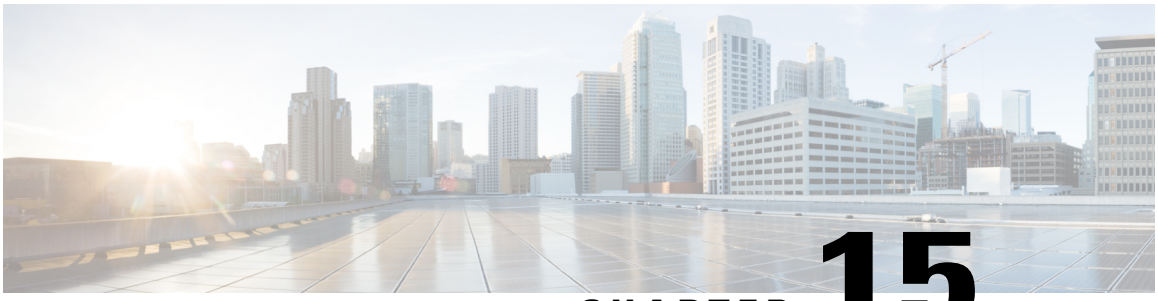
As Vocera badges are expected to roam when the AP SNR is 20 dB or lower, and as your design set the AP cell edge at -65 dBm RSSI and 25 dB SNR, badges are likely to roam when the AP signal falls below -70 to

-72 dBm. To confirm this behavior, you can tentatively set the Coverage hole algorithm to be triggered at a slightly lower value, for example -75 dBm.

Figure 14: 802.11b/g/n Coverage Hole Detection Configuration

However, keep in mind that the roaming trigger is not the AP RSSI, but the AP SNR. During testing, when seeing coverage hole events, verify the AP RSSI and SNR at the location of the event, and adjust the Coverage Threshold accordingly, to be set to the RSSI value that matches a 20 dB SNR.

Also make sure that your APs 2.4 GHz radio does not support too many SSIDs. Each SSID will create overhead for beacons and other administrative messages, thus reducing the amount of airtime effectively available on the AP radio for client communication. Cisco recommends limiting the number of SSIDs on a given AP radio to 5 or less when VoWLAN support is required.

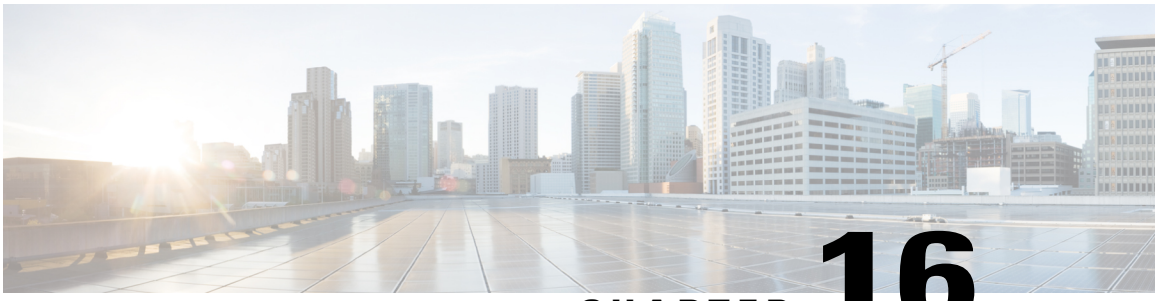


CHAPTER 15

Wireless IP Telephony Verification

After you conduct an RF site survey and configure the access points and the phones, it is crucial to conduct verification tests to ensure that everything works as desired. These tests should be performed at all of these locations:

- The primary area of each access point cell (where the badges are most likely to connect to that particular access point).
- Any location where there might be high call volume.
- Locations where usage might be infrequent but coverage still has to be certified (for example, stairwells, restrooms, and so forth).
- At the fringes of the access point's coverage area.
- These tests can be performed in parallel or series. If performed in parallel, ensure that phones are powered off between testing points to test full association, authentication, and registration at each location. Roaming and load tests must be the final tests.



CHAPTER 16

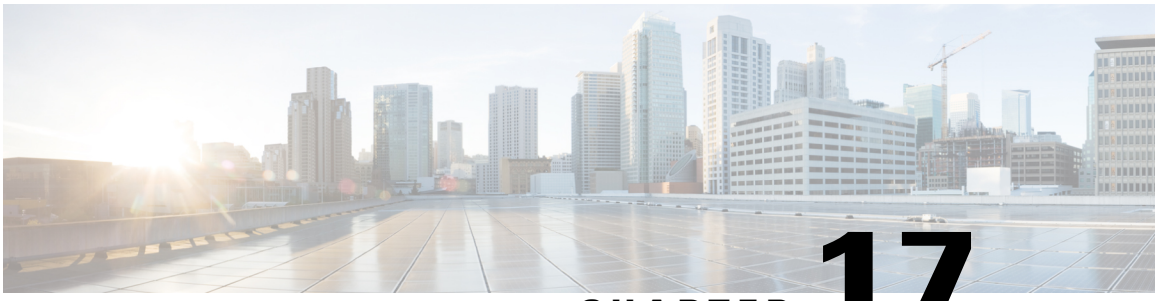
Association, Authentication, and Registration

This section explains how to verify that the badge associates, authenticates, and registers properly.

- At multiple points throughout the environment, power-up the badges and verify association with the access point. If the badge does not associate with the access point, perform these checks:
  - Check the badge configuration to ensure proper SSID, authentication type, and so forth.
  - Check the WLC configuration to ensure proper SSID, authentication type, radio channels, and so forth.
  - Check your site survey to ensure the location has adequate RF coverage.
- At multiple points throughout the environment, ensure that the phone authenticates through the access point successfully. If the client does not authenticate, check either the PSK or the 802.1/x/EAP username and password on the badges. Also, check the username and password on the AAA server by using a wireless laptop with identical credentials.
- At multiple points throughout the environment, ensure that the badges register with the Vocera Application Server. If the client does not register, perform these checks:
  - Verify that the badge has the correct IP address, subnet mask, and primary gateway.
- Stationary voice calls:
  - At multiple points throughout the environment, while you stand still, make a call to another badge and conduct 60 to 120-second voice tests to check voice quality. If the voice quality is unacceptable, move one badge to a better location and test again. Is the voice quality acceptable? If not, check your wireless coverage.
  - If the telephony server or a SIP gateway are configured, at multiple points throughout the environment, stand still and make a call to a wired phone and conduct 60 to 120-second voice tests to check voice quality. If the voice quality is unacceptable, ask if you can make a call using the wired phone. Is the voice quality acceptable? If not, verify the wired network design against the guidelines.
- Use a site survey tool to verify that there is no more than one access point per RF channel from that location with a signal strength (received signal strength indicator [RSSI]) greater than -65 dBm. If there are two access points present on the same channel, ensure that the signal-to-noise ratio (SNR) is as high as possible to minimize interference. For instance, if the stronger access point has an RSSI of -65

dBm, ideally the weaker access point should have an RSSI of less than -84 dBm (19 dB weaker). In order to achieve this goal, you might have to reduce one access point's transmit power or move the access point. Keep in mind that the badge roaming and association decisions are based on the AP SNR. Limiting the number of APs detected on the same channel helps maximizing the SNR.

- Check the QoS settings on the access point to confirm proper recommended settings.
- Roaming badge calls:
  - If the telephony server or the SIP gateway is not available, initiate the Vocera Tutorial with the command `Play Welcome Tutorial`, or,
  - If the telephony server is available, initiate a call with a stationary device to the badge.
  - Continually check voice quality while you traverse the total wireless coverage area. If the voice quality is insufficient, perform these tasks:
    - Listen for all unacceptable changes in voice quality and take note of the location and radio values on your laptop and CQ values from the badge.
    - Watch and listen for the badge to roam to the next access point.
    - Note the other available access points in the site survey to check coverage and interference.
- Make adjustments to access point placement and settings to fine-tune the WLAN, and perform these checks to ensure voice quality:
  - Use the site survey tools and verify that there is no more than one access point per channel with an RSSI value greater than 35 in any given location. Ideally, all other access points on the same channel should have RSSI values as low as possible (preferably less than 20). At the border of the coverage area where the RSSI is 35, the RSSI for all other access points on the same channel should ideally be less than 20.
  - Use the site survey tools to verify that there are at least two access points (total, on separate channels) visible at all locations with sufficient signal strength.
  - Check that the access points in a given roaming area are all on a Layer 2 network.



CHAPTER 17

Common Roaming Issues

These roaming issues can occur:

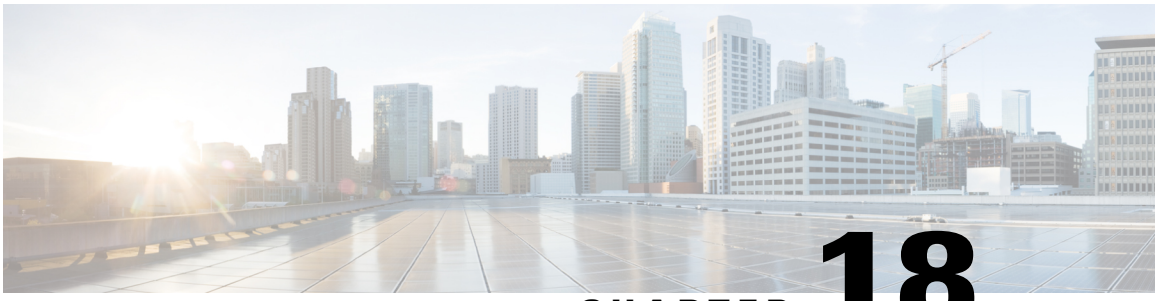
- The badge does not roam when placed directly under the access point.
- The badge is most likely not reaching the roaming differential thresholds for the received signal strength indicator (RSSI) and channel utilization (CU). Adjust the Transmit Power Threshold from the WLC.
- The badge does not receive beacons or probe responses from the access point.
- The badge roams too slowly.

The Badge Loses Connection to the Network or Voice Service is Lost when Roaming

- Check authentication for a possible authentication parameter mismatch between controllers.
- The badge does not send out IGMP joins or the network sends IGMP queries during a roam. Therefore, the Vocera broadcast function fails during a Layer 2/Layer 3 roam.
- Ensure that the new WLC is not serving a different IP subnet.
- Verify that the associated access point/controller has IP connectivity to the Vocera Communication Server.
- Check the RF signal strength and badge CQ values.

Badge Loses Voice Quality while Roaming

- Check for low RSSI on the destination access point.
- Channel overlap might be insufficient. The badge must have time to hand off the call smoothly before it loses its signal with the original access point.
- The signal from the original access point might be lost.



CHAPTER 18

Audio Problems

There are a few common configuration errors that can cause some easily resolvable audio issues. If possible, check audio problems against a stationary (reference) badge to help narrow the problem to a wireless issue. Common audio problems include:

One-sided Audio

- This problem can occur in the fringe areas of an access point, where a signal might be too weak on either the badge side or the access point side. Matching the power settings on the access point to the badge, when possible, can fix this problem. The badge max power is 16 dBm (30 mW), and the AP power should be set to the value closest to that max power. This problem is most common when the variation between the access point setting and the badge setting is large (for example, 100 mW on the access point and 28 mW on the badge).
- Check the gateway and IP routing for voice quality.
- Check to see if a firewall or NAT is in the path of the proprietary UDP packets. Typically Vocera calls are intra-site, but if there is a firewall or NAT on the path between Vocera devices, use the Vocera Infrastructure guide (p 156) to determine the list of ports that should be open between badges. By default, firewalls and NATs cause one-way audio or no audio. Cisco IOS® and PIX NATs and firewalls have the ability to modify those connections so that two-way audio can flow.
    - If you use Layer 3 mobility, your network could be blocking upstream traffic with Unicast Reverse Path Forwarding (uRPF) checks.
- One-way audio can occur if ARP caching is not configured on the WLC.

Choppy or Robotic Audio

- A common reason for choppy or robotic audio is when a microwave operates nearby. Microwaves start at channel 9 and can extend from channels 6 to 14.
- Another common source of choppy audio is when network utilization exceeds 40%.
- Check for 2.4 Ghz wireless phones and other nurse call wireless devices using tools like Cisco Spectrum Expert, or by using the CleanAir function and radio utilization reports of Cisco access points.

Registration and Authentication Problems

When you encounter problems with authentication, perform these checks:

- Check SSIDs to make sure they match on the badge and the access point (or network). Also be sure the network has a route to the Vocera server.
- Check the credentials to make sure they match. It is a good idea to re-enter them on the Badge Configuration Utility (BCU) and reprogram the badge, because it is easy to make a typing error when you enter a key or password.

These messages or symptoms can occur:

- Searching for Server (SFS): Every 30 seconds, each badge sends an application level ping (keep alive signal) to the Vocera Server and expects an acknowledgment (ACK) back from the Vocera Server. If it does not receive an ACK, the badge will resend the ping 10 more times, once every 600ms until it receives the ACK . If it still does not receive an ACK, the badge will display SFS and the LED will flash red. It will try to ping again 24.5 seconds later, when it reaches the scheduled time for its next ping.
- Searching for Access Point (SFAP): When not in a call, the Vocera Badge sleeps most of the time. The Badge wakes up every 500ms to listen to the Beacon from the Access Point it is associated with. If it sees the beacon and does not see its AID (Association ID) set in the TIM (Traffic Indication Map), it goes back to sleep. If it doesn't see a Beacon, it stays awake until the next Beacon interval. After 30 missed beacons (3 seconds) the Badge will display SFAP.
- Off Network: When the Badge boots up, it scans 3 times (in all configured channels), if no Access Point (for the configured SSID) is found, the badge will display Off Network. Every 12 seconds, the badge will then try to scan once (in all configured channels) to see if there is an Access Point present. If not, it will continue to be in off-campus mode (Off Network).
- Requesting IP address: When the badge is able to authenticate and associate to the network, it will try to obtain an IP address from the DHCP server. This message is displayed when the badge requests an IP address, but does not receive an address from a DHCP server.
- Authenticating: This message is displayed when the badge tries to authenticate. If the security parameters configured in the badge do not match the configuration of the Wireless LAN Controller WLAN, the authentication fails and this message stays displayed on the badge screen.