Vocera Communications® in a Cisco LWAPP Infrastructure

Design and Deployment Guide

Cisco Confidential

This document contains valuable trade secrets and confidential information belonging to Cisco Systems, Inc. and its suppliers. The aforementioned shall not be disclosed to any person, organization, or entity, unless such disclosure is subject to the provisions of a written non-disclosure and proprietary rights agreement, or intellectual property license agreement, approved by Cisco Systems, Inc. The distribution of this document does not grant any license or rights, in whole or in part, to its content, the product(s), the technology(ies), or intellectual property, described herein.

Disclaimer

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Table of Contents

Preface

This document provides design considerations and deployment guidelines for implementing the Vocera® Badge VoWLAN technology on Cisco's Unified Wireless Network infrastructure.

Note	Support for Vocera® products should be obtained directly from Vocera® support channels. Cisco TAC 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. All documents referenced here are available at www.cisco.com.
It must be noted that this document builds upon ideas and concepts presented in the *Cisco IP Telephony Solution Reference Network Design (SRND)* and the *Cisco Wireless LAN SRND*, both which are available online at: http://cisco.com/go/srnd
Readers are assumed to have familiarized themselves with the terms and concepts presented in the *Cisco IP Telephony SRND* and the *Cisco Wireless LAN SRND*.

Revision History

Revision Date	Comments
April 25, 2007	David Hunt, Update for BeMR2
December 19, 2006	David Hunt, Deployment Update
September 11, 2006	David Hunt, M-M Group Description
September 7, 2006	David Hunt, Updated for Multicast-Unicast Adding the reference to "AP Groups VLAN"
September 5, 2006	David Hunt, Clarifying AutoRF Support
August 30, 2006	David Hunt, Reformatting information
August 3, 2006	David Hunt, first cut
May 6, 2006	Larry Ross – Basis for VoWLAN deployment Recommendations

Executive Summary

The following table sumarized the four key functions and how they will behave within a Cisco Unified Wireless network.

	Single Controller	Controller-to-Controller L2-Roaming	Controller-to-Controller L3-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 Disable Vocera VLAN IGMP-Snooping or run 4.0.206.0 or later	4.0.206.0 or later
Badge Location	No special configuration	No special configuration	No special configuration

Vocera® Badge - Overview

The communication badges allow a wearer instant communication with any other badge wearer as well a PBX integration and badge location tracking. The utilization of an 802.11b/g wireless network requires the use of Multicast and UDP unicast packet delivery with limited requirements for QoS as of Vocera Server Software release 3.1 [Build 1081]. The encryption capabilities are 64/128 bit WEP, TKIP, MIC, and CKIP combined with the authentication capabilities of Open, WPA-PSK, WPA-PEAP and LEAP.

With the push of a button the Vocera server will respond with “Vocera ” which is a prompt for a user to issue commands such as “record”, “where (am I) /is...”, “Call ” ,”Play”, “Broadcast”, “Record”, “messages ..” etc. The Vocera server provides the necessary services and/or call setup to complete the request.

Vocera’s 802.11b capable Communication System makes use of proprietary voice compression and the use of a UDP port range. The Vocera System software runs on a Windows Server that manages call set up, call connection and User profiles. They have partnered with Nuance 8.5 Speech Recognition and voiceprint software to enable badge voice communications. Vocera recommends a separate Windows server to run the Vocera Telephony Solutions Software to enable POTS connectivity with the badges.

Vocera – Call Capacity Considerations

Please refer to the “Network Sizing” Page 20 for further details

Vocera Communications Server Capacity

For more details on Vocera Server sizing matrix please see this link…..
http://www.vocera.com/products/specifications.aspx

The Vocera Solution

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

Badge to Badge Comunctions – When one Vocera user calls another user, the Badge first contacts the Vocera Server who looks up the IP address of the callee's Badge and contacts the Badge user to ask the user if they can take a call. If the callee accepts the call, the Vocera Server will notify the calling Badge of the callee badge's IP address 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 a Vocera proprietary codec.

Badge Telephony Communication -– When Vocera Telephony Server is installed and setup with a connect to a PBX, a user is able to call internal extensions off of the PBX or outside telephone lines. Vocera allows users to make calls by either saying 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 (ex. Pharmacy, home, pizza.) the Vocera server will determine 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 Telephone Server which connects to the PBX and generates the appropriate telephony signaling (ex. DTMF). All communication between the Badge & Vocera Server and Vocera Server & Vocera Telephone 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 wears at the same time by using the Broadcast command. When a user Broadcasts to a group the users Badge send the command to the Vocera Server who 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.

Badge Location Function – The Vocera Server keeps track of the access point to which each active badge is associated as each badge will send a 30 second keep alive to the server with the associated BSSID. This 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 may not be associated to the AP to which it is closest.

Vocera's Infrastructure Planning

The Vocera whitepaper "Vocera Infrastructure Planning Guide", available at http://www.vocera.com/downloads/InfrastructureGuide.pdf describes the site survey minimum requirements showing that the badge should have a receive signal strength minimum of -65dBm, a signal-to-noise ratio greater than 25db and proper access point overlap and channel separation. Although the badges use a similar omni directional antenna as a notebook that would be used for a site survey, it does not mimic the behavior of the badge very well, given the wearers affects on signal strength. Given this unique requirement and this behavior of the transmitting device, making use of the Cisco Architecture and Radio Resource Management is ideal making sure there is a lack of unusual RF site characteristics.
The Vocera badge is a low powered device, worn next to the body with limited signal error correction capabilities. The Vocera requirements above may be easily achieved; it can become overwhelmed if there are too many SSID's for it to process and allow the badge to work effectively.

Architecture Overview

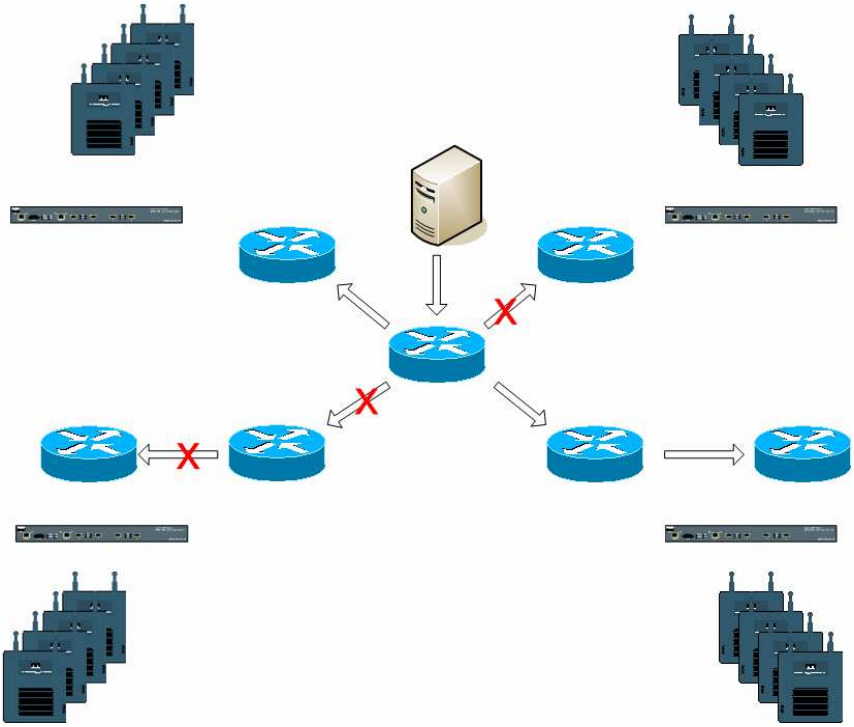


Figure 1 – General Multicast forward and Prune with LWAPP wireless

Multicast in an LWAPP deployment

Understanding multicast within an LWAPP deployment is necessary to deploy the Vocera broadcast function. Later in this document we will cover the essential steps of enabling Multicast within the controller based solution. There are currently two methods that the LWAPP controller will deliver multicast to the clients; Unicast-Multicast and Multicast-Multicast delivery methods.

Unicast-Multicast Delivery Method

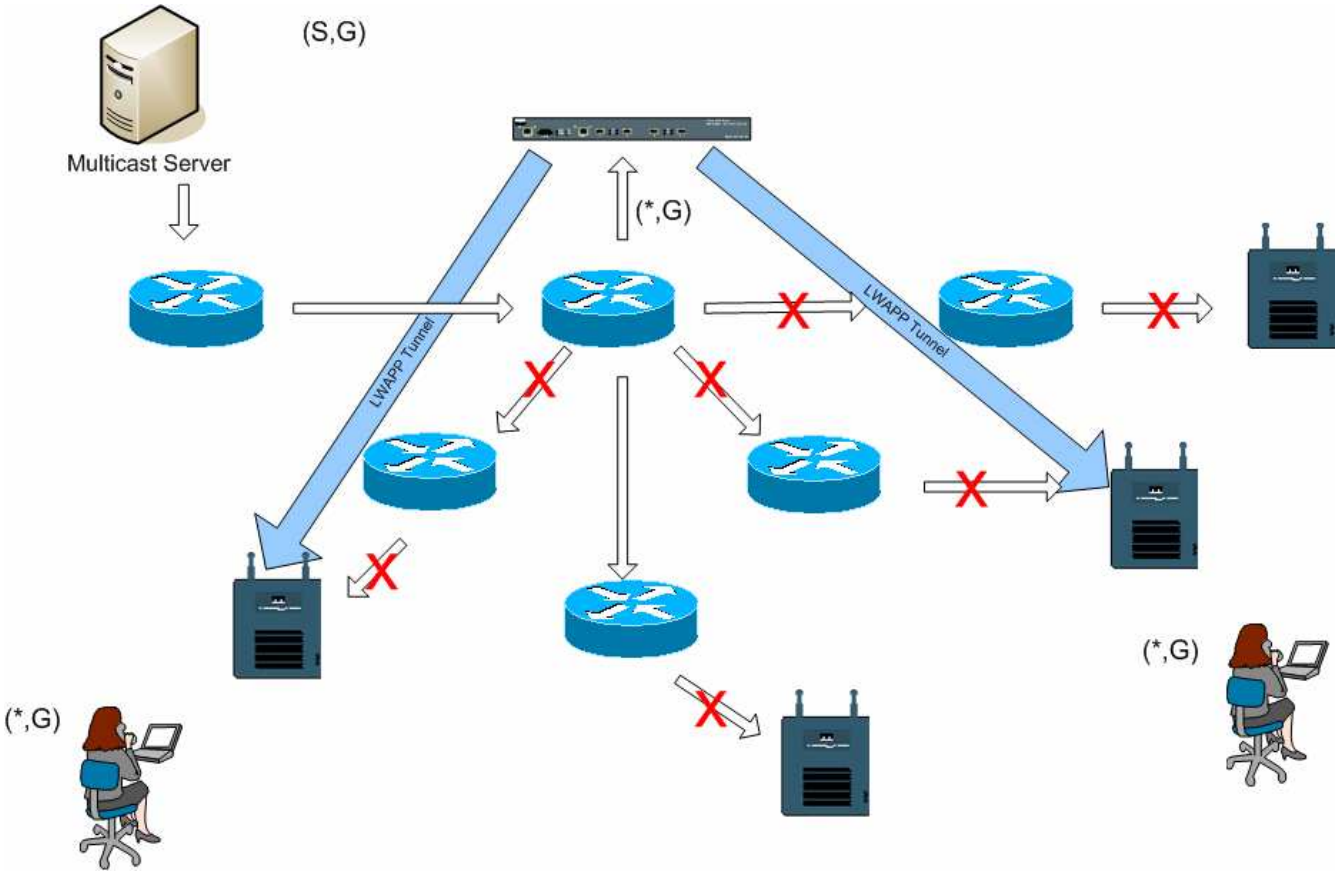


Figure 2 LWAPP Multicast-Unicast

Unicast-multicast delivery method will create a copy of every multicast packet and forward to every access-point . When a client sends a multicast join to the wireless LAN, the access-point forwards this join through the LWAPP tunnel to the controller. The controller will bridge this multicast join onto it's directly connected local area network connection that is the *default* [1]VLAN for the associated WLAN of the client. When an IP multicast packet arrives from the network to the controller, the controller will *replicate* this packet with an LWAPP header for each access-point that has a client within the wireless domain who has joined this specific group. When the source of the multicast is also a reciever within

[1] If, for example, AP Groups VLAN is configured, and an IGMP join is sent from a client through the controller it will be placed on the "default" VLAN of the WLAN the client is on. Therefore a client may not receive this multicast traffic unless he is a member of this "default" broadcast domain.

the wirless domain, this packet is also duplicated and forwarded back to the same client who sent this packet. For Vocera® badges this is not the prefered method of multicast delivery within the LWAPP contoller solution. The unicast delivery method will work with small deployments, however due to the considerable overhead on the wireless LAN controller, this is never the recommended multicast delivery method.

Multicast-Multicast Delivery Method

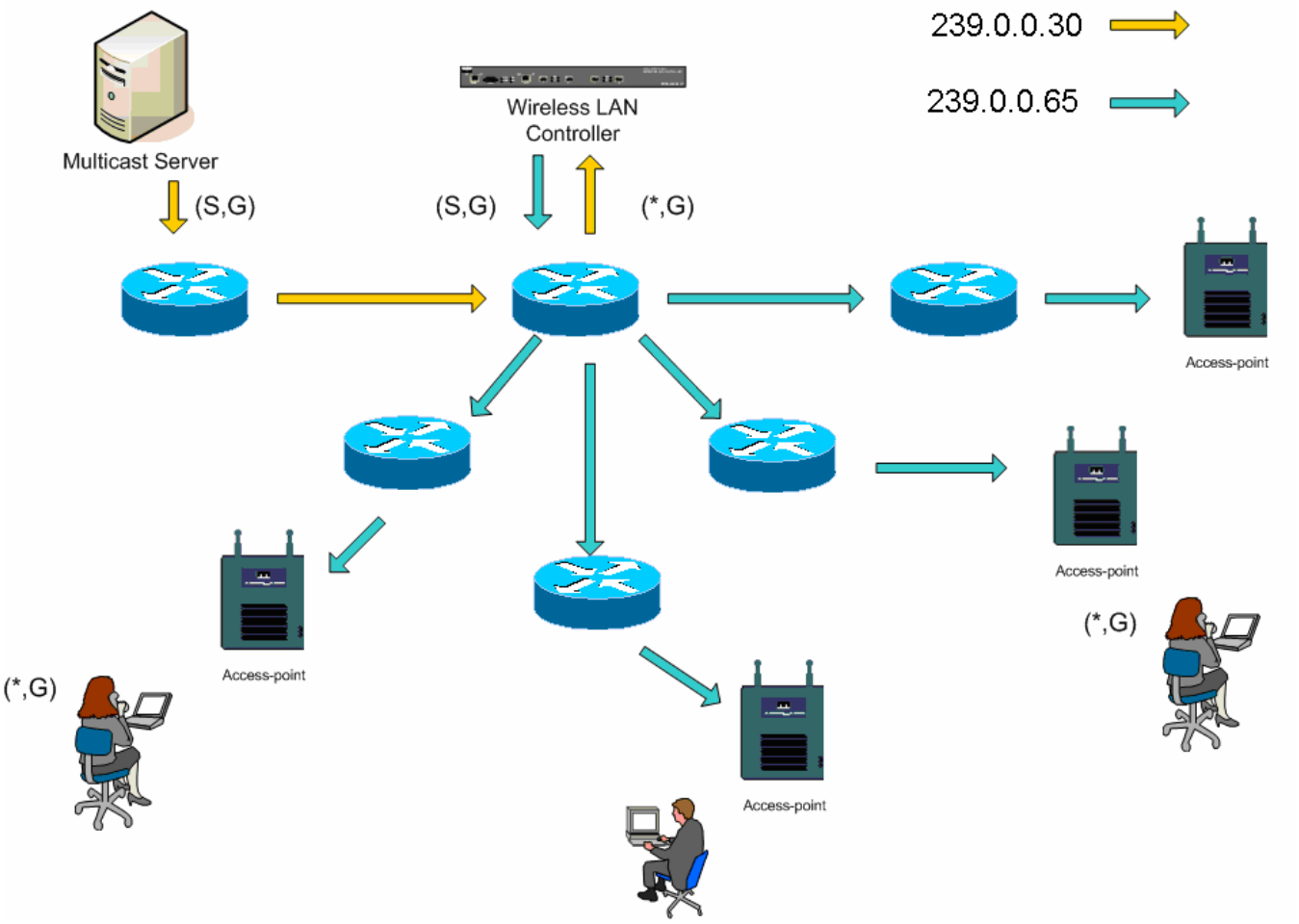


Figure 3- LWAPP Multicast-Multicast

Multicast-Multicast delivery method does not require the controller replicate each multicast packet recieved. The controller will be configured for an un-used multicast group address that each access-point will become a member of. With Figure 3 above the multicast group defined from the Wireless LAN Controller to the Access-points is 239.0.0.65. When a client sends a multicast join to the wireless LAN, the access-point forwards this join through the LWAPP tunnel to the controller. The controller will forward this link-layer protocol onto it's directly connected local area network connection that is the

default [2]VLAN for the associated WLAN of the client. The router that is local to the controller will then add this multicast group address to that interface for forwarding (**(*,G)**) entry. With Figure 3 above, the example multicast join was sent to the multicast group 239.0.0.30. When the network now forwards multicast traffic the multicast address of 239.0.0.30 it will be forwarded to the controller. The Controller will then encasulate the multicast packet into the an LWAPP multicast packet addressed the multicast group address (*example above* 239.0.0.65) that is configured on the controller and forwarded to the network. Each access point on the controller will receive this packet as a member of the controllers multicast group. The access point will then forward the clients/servers multicast packet (*example above* 239.0.0.30) as a broadcast to the WLAN/SSID identified within the LWAPP multicast packet.

NOTE: It should be noted that if you improperly configure your multicast network, you could end up receiving another controllers AP multicast packets. If the first controller has to fragment this multicast packet, the fragment will be forwarded to the network and each AP must spend time to drop this fragment. If you allow all traffic such as anything from the 224.0.0.x multicast range, this will also be encapsulated and subsequently forwarded by each AP.

Router and Switch Multicast Configuration

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca794.html

This will not be a network multicast configuration guide and the above link should be used for a complete implementation story. Here we will cover the basics to enable Multicast within your network environment.

Enabling IP Multicast Routing

This allows the Cisco IOS software to forward multicast packets. The following global configuration command is required to allow multicast to function in any multicast enabled network. This command should be enabled on all routers within your network between the Wireless LAN Controller(s) and their respective access-points.

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

Enabling PIM on an Interface

This enables the routing interface for IGMP operation. The PIM mode determines how the router will populate its multicast routing table. The example provided below 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 L3 interface directly connected to your controller should be PIM

[2] If, for example, AP Groups VLAN is configured, and an IGMP join is sent from a client through the controller it will be placed on the "default" VLAN of the WLAN the client is on. Therefore a client may not receive this multicast traffic unless he is a member of this "default" broadcast domain.

enabled for multicast to function. Again, all interfaces between your Wireless LAN Controller(s) and their respective access-points should be enabled.

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

Disabling Switch VLAN IGMP snooping

http://www.cisco.com/en/US/partner/products/hw/switches/ps708/products_configuration_guide_chapter09186a00804356ac.html

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, it can be undesirable to enable CGMP or IGMP snooping on the upstream switchport to the controller with software release older than 4.0.206.0. Multicast today; Roaming and multicast are not defined with a set of requirements to verify 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. At the same time, the LWAPP access point does not send a general multicast query to the roamed client to prompt for this IGMP join. With a layer 2 Vocera network design, disabling IGMP snooping allows traffic to be forwarded to all members of the Vocera network no matter where they roam and thereby making sure that the Vocera "broadcast" feature works irrespective of where the client roams. Disabling IGMP snooping globally is a very undesirable task and as such we are recomending that IGMP snooping only to be disabled on the Vocera VLAN that is directly connected to each Wireless LAN Controller.

Router(config)**# interface vlan 150**

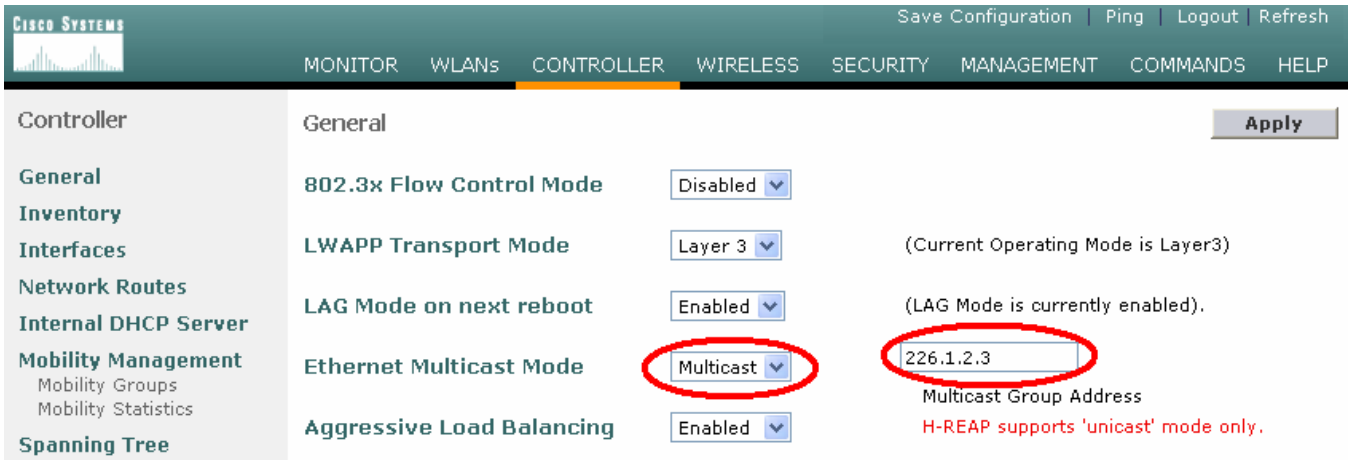
Router(config-if)**# no ip igmp snooping**

Multicast enhancements of 4.0.206.0 and later

With the release of 4.0.206.0, Cisco introduced an IGMP query to allow users to roam at layer 2 by sending a general IGMP query when this occurs. The client will then respond with the IGMP group that they are a member of and this is bridged to the wired network as described above. When a client roams to a controller that does not have layer 2 connectivity, or a layer 3 roam Synchronous routing was 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 will encapsulated this packet in the Ethernet over IP in IP (EoIP) tunnel to the "anchor" controller. The "anchor" controller will then forward that to the wireless clients locally associated as well as bridge this back to the wired network where it is routed using normal multicast routing methods.

Deployment Scenarios

The following three deployment scenarios will cover best practices and design parameters to help with a successful Vocera Badge Deployment. Understanding how the Vocera Badge features interact within an LWAPP split MAC environment is essential. With all deployment scenarios, multicast should be enabled and aggressive load balancing should be disabled. All badge WLAN's should be contained within the same broadcast domain across your entire network.



Single Controller Deployment

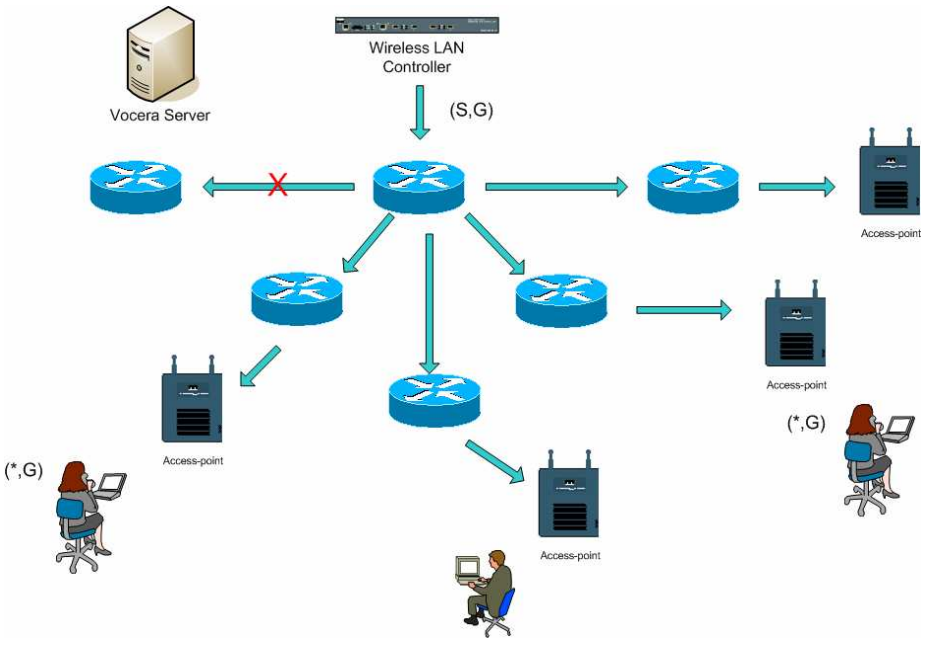


Figure 4 – Single Controller in Multicast-Multicast Mode

This is the most straight forward deployment scenario, allowing you to deploy the Vocera® Badge solution with little deployment concerns. Your network must be enabled for IP multicast routing only to allow the AP's to receive the LWAPP multicast packets. If required, you may limit network multicast complexity by configuring all routers and switches with the controllers multicast group.

With Multicast configured globally on the controller, the proper SSID, Security settings and all the access points registered the Vocera badge solution and all its functions will operate as expected. With the Vocera Broadcast function and a user roams the multicast traffic will follow as expected. There are no extra settings required to be configured to allow this solution to funtion properly.

When a Vocera badge sends a multicast message, as it will with the Vocera Broadcast, it will be forwarded to the controller. The controller in turn will encapsulate this multicast packet within an LWAPP multicast packet. The network infrastructure will forward this packet to every AP that is connected to this controller. When the AP recieves this packet, it will then look at the LWAPP multicast header to determine which WLAN/SSID it will then broadcast this packet to.

Multiple Controller Layer 2 Deployment

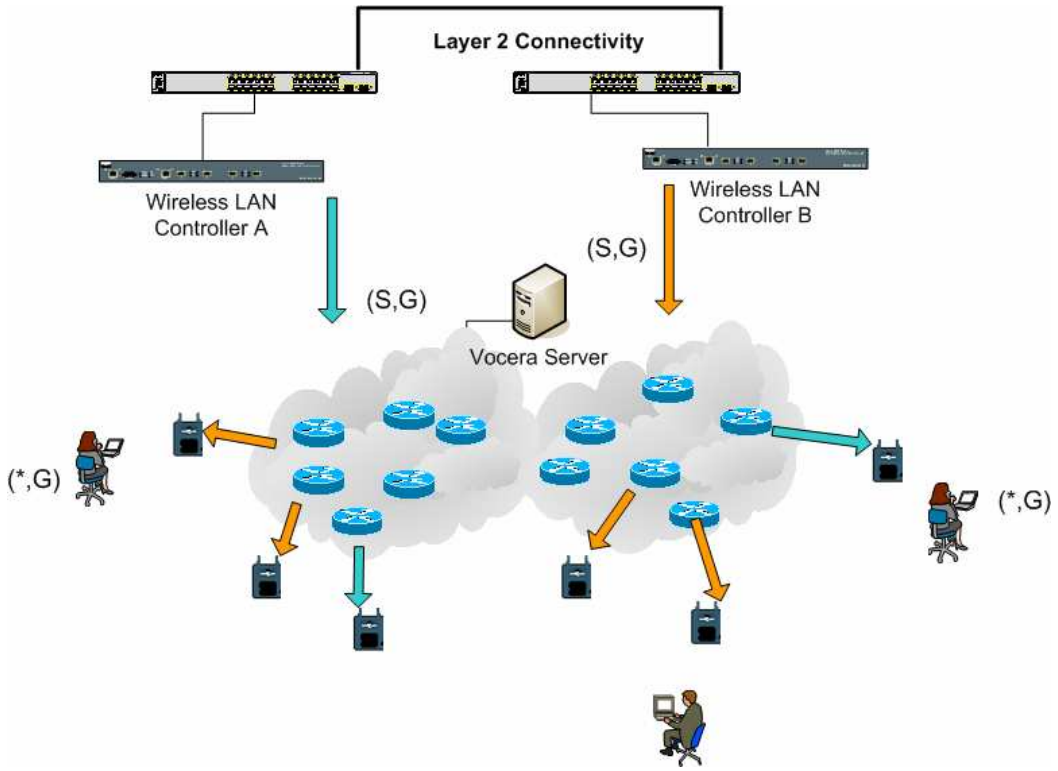


Figure 5 – Multiple Controller Layer 2 Deployment

Multiple controllers must all have connectivity to each other via the same layer 2 broadcast domain. Both controllers will be configured for multicast as shown above, using the identicle access point multicast group on each controller to limit fragmentation . 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 must be disabled for this single VLAN or be running 4.0.206.0 or later WLC sofware. With the Vocera Broadcast function and a user roam from an AP on one controller to an AP on a different controller, There is no mechanism for IGMP joins to be forwarded to the new layer 2 port for IGMP snooping to work. Without an IGMP packet reaching the upstream CGMP or IGMP capable switch, the specified multicast group will not be forwarded to the controller and therefore not to be received by the client. In some cases this may work, if a client that is part of the same Vocera Broadcast group has already sent this IGMP packet before the roaming client roams onto the new controller With the advantages of 4.0.206.0, a client who roams to another controller as a layer 2 roam will receive a general IGMP query immediately following authentication. The client should then respond with the interested groups and the new controller will then bridge this to the locally connected switch allowing the advantages of IGMP and CGMP on your upstream switches.

You can create additional badge SSID's and layer 2 domains for separate badge networks and they will so long as your network has been configured to pass multicast traffic appropriately. Also, each Vocera layer 2 broadcast domain created must exist everywhere a controller is connected to the network so as not to break multicast.

Multiple Controller Layer 3 Deployment

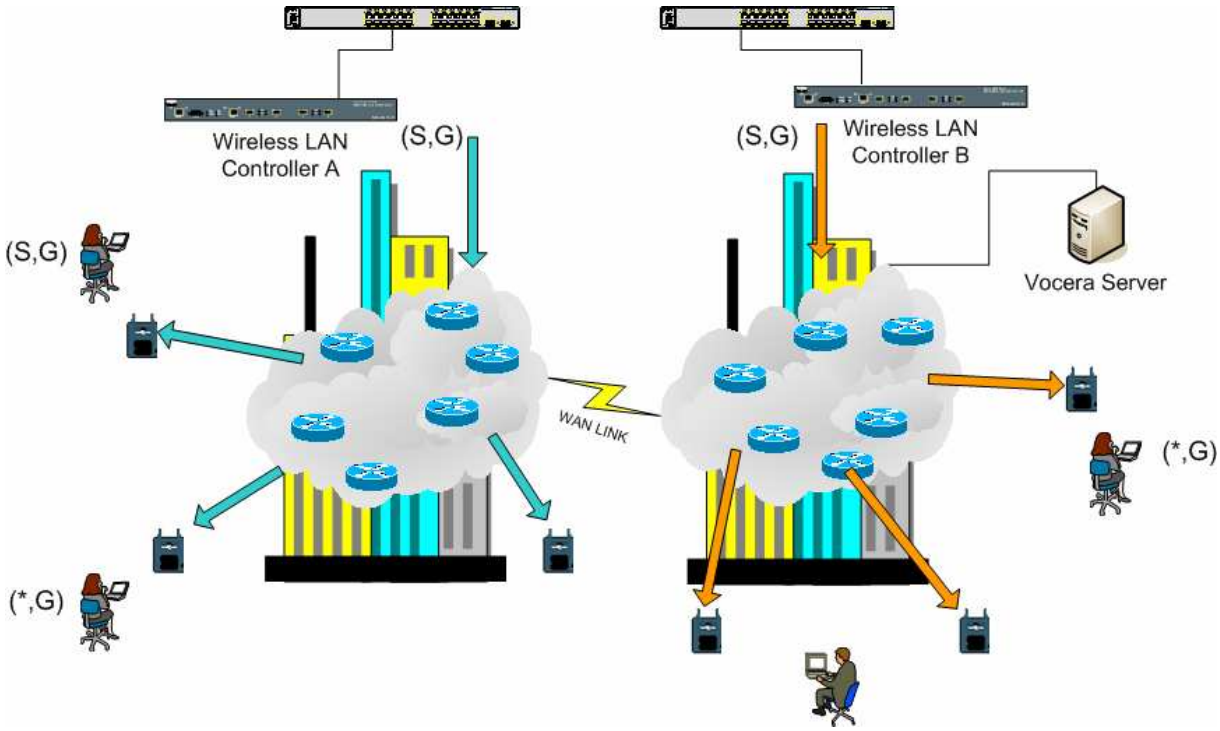


Figure 6 – Multiple Controller Layer 3 Deployment

The layer 3 roaming deployment strategy should only be used where Controller to Controller roaming with controller software release 4.0.206.0 or later. If a client that has been connected to the Vocera

"broadcast" group and is receiving the appropriate multicast stream and roams to another controller as a layer 3 roam with the LWAPP Layer 3 roaming configured, it will be queried for interested multicast groups. The client, when sourcing to the same Vocera "Broadcast" group will have these packets delivered to the "anchor" controller through the EoIP tunnel and have these packets routed through normal multicast routing methods.

VoWLAN Deployments: Cisco's Reccommendations

Wireless IP Telephony networks requires careful RF planning. A thorough voice site survey is often required to determine the proper levels of wireless coverage and to identify sources of interference. AP placement and antenna selection choices can be greatly eased with the help of the results of a valid voice site survey. Undoubtedly, the most important consideration is the transmit power of the wireless phone. Ideally the phone will learn the transmit power of the access point and adjust it's transmit power to that of the access point.

Although majority of the wireless networks today are deployed after an extensive RF site surveys but those 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 APs 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

Recommendations for Multi-Floor Buildings, Hospitals, and Warehouses

Consider the factors listed in this section when surveying 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 APs 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 are performing 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) will have 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 diversity 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 AP (antennas) helps minimize these conditions.

Multi-Floor Buildings

Keep in mind the following guidelines when conducting 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 2.4GHz 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 AP coverage because they are areas of high utilization

Extra precaution must be administered when surveying multi-floor facilities. APs on different floors can interfere with each other as easily as APs located on the same floor. It is possible to use this behavior to your advantage during a survey. Using higher-gain antennas, it might be possible to penetrate floors and ceilings and provide coverage to floors above as well as below the floor where the AP is mounted. Be careful not to overlap channels between APs on different floors or APs 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 the following 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. Of course, 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 may have several types of wireless networks installed, including 2.4 GHz non-802.11 equipment. This equipment may 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, often containing high storage racks. Many times these racks reach almost to the ceiling, where APs are typically placed. Such storage racks can limit the area that the AP can cover. In these cases, consider placing APs on other locations besides the ceiling, such as side walls and cement pillars. Also consider the following factors when surveying a warehouse:

- Inventory levels affect the number of APs needed. Test coverage with two or three APs in estimated placement locations
- Unexpected cell overlaps are likely because of multipath variations. The quality of the signal will vary more than the strength of that signal. Clients might associate and operate better with APs farther away than with nearby APs
- During a survey, APs and antennas usually do not have an antenna cable connecting them. But in a production environment, the AP and antenna might require antenna cables. All antenna cables introduce signal loss. The most accurate survey will include 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 warehousing, 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.

Security Mechanisms Supported

In addition to Static WEP and Cisco LEAP for authentication and data encryption, the Vocera® Badges also support WPA-PEAP (MS-CHAP v2)/WPA2-PSK.

LEAP Considerations

LEAP allows devices to be authenticated mutually (badge-to-AP and AP-to-badge) based on a user name and password. Upon authentication, a dynamic key is used between the phone and the AP to encrypt traffic. However, the ASLEAP dictionary attack should be considered when deciding to use LEAP as your security solution:

http://www.cisco.com/en/US/tech/tk722/tk809/technologies_security_notice09186a00801aa80f.html

If LEAP is used, a LEAP-compliant RADIUS server, such as the Cisco Access Control Server (ACS), is required to provide access to the user database. The Cisco ACS can either store the user name and password database locally, or it can access that information from an external Microsoft Windows NT directory. When using LEAP, 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.

Because all the badges use the same password and is stored within the badge, 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 (off-ACS) database to store the user names and passwords for the badges, Cisco does *not* recommend this practice. Because the ACS must be queried whenever the badge roams between APs, the unpredictable delay to access an off-ACS database could cause excessive delay and poor voice quality.

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 way of suggested deployment to ensure sufficient network bandwidth and ease of troubleshooting.

Voice, Data and Vocera® VLANs

VLAN's 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 AP 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, thus ensuring that appropriate QoS is provided for various classes of traffic and helping to resolve addressing issues such IP addressing, security, and network dimensioning. The Vocera® Badges use a broadcast feature that utilizes multicast to deliver; this common VLAN will ensure that when a badge roams between controllers that it remains part of the multicast group. This last process will be discussed in detail when multicast is addressed later in this paper.

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 the following 802.11b issues when sizing your Wireless IP Telephony network. The Vocera® badges are a specialized application that stretches the number of wired clients beyond our typical deployment recommendations:

Number of 802.11b Devices per AP

Cisco recommends that you have no more than 15 to 25 802.11b devices per AP.

Number of active calls per AP

Vocera® uses two different codecs depending if it is a badge-to-badge (proprietary low-bit rate codec) call or a Badge-to-Phone (G.711 codec) call. The following table that has been provided by Vocera® is showing a percentage of available bandwidth by data rates giving you a clearer picture of what can be the expected throughput:

Call Process	1 Mbps	2 Mbps	5.5 Mbps	11 Mbps
Badge-to-Phone (G.711)	20.7%	11.8%	6.3%	4.7%
Badge-to-Badge (Proprietary Low-bit rate codec)	9.4%	6.1%	4.2%	3.6%

Switch Recommendations

Note If you are using a Cisco Catalyst 4000 Series Switch as the main router in the network, ensure that it contains, at a minimum, either a Supervisor Engine 2+ (SUP2+) or Supervisor Engine 3 (SUP3) module. The SUP1 or SUP2 module can cause roaming delays, as can the Cisco Catalyst 2948G, 2980G, 2980G-A, 4912, and 2948G-GE-TX switches.

You can create a switch port template for use when configuring any switch port for connection to an AP. This template should add all the baseline security and resiliency features of the Standard Desktop template. In addition, when attaching the AP to a Cisco Catalyst 3750 switch, you can optimize the

performance of the AP 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 AP. A template should be designed in such a way that helps create a secure and resilient network connection with the following 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 AP.
- Disable Port Aggregation Protocol (PagP) — PagP is enabled by default but 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, thereby isolating traffic and ensuring greater control of traffic
- Enable Quality of Service (QoS); don't 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.

WS-C3750-48PS-S Inline Power Switches can be used to provide power to AP's that are capable of receiving inline power.

The Catalyst 6500, our premier switching and routing platform will allow you to forward packets at line rate with all the features described above as well as integrating a plethora of Service Modules. The Wireless Service Module (WiSM) allows you to have two controllers each with a capability of controlling 150 access-points each. With up to 5 WiSM's per chassis, allowing you to control over 1500 access-points supporting 50,000 clients within a single high performance switching architecture.

Deployments and Configuration

Badge Configuration

The Vocera Badge Configuration Utility (BCU) and the configuration of the badge can introduce roaming and latency into your environment if done incorrectly. Using the BCU and the Badge Properties Editor (BPE), Verify the following: (Please see Figure 7 Below of the BPE)

"Subnet Roaming" has been disabled

"Scan Default Channels (1,6,11)" has been checked

"Broadcast Uses IGMP" is enabled

"Roaming Policy" is set to 2 or greater

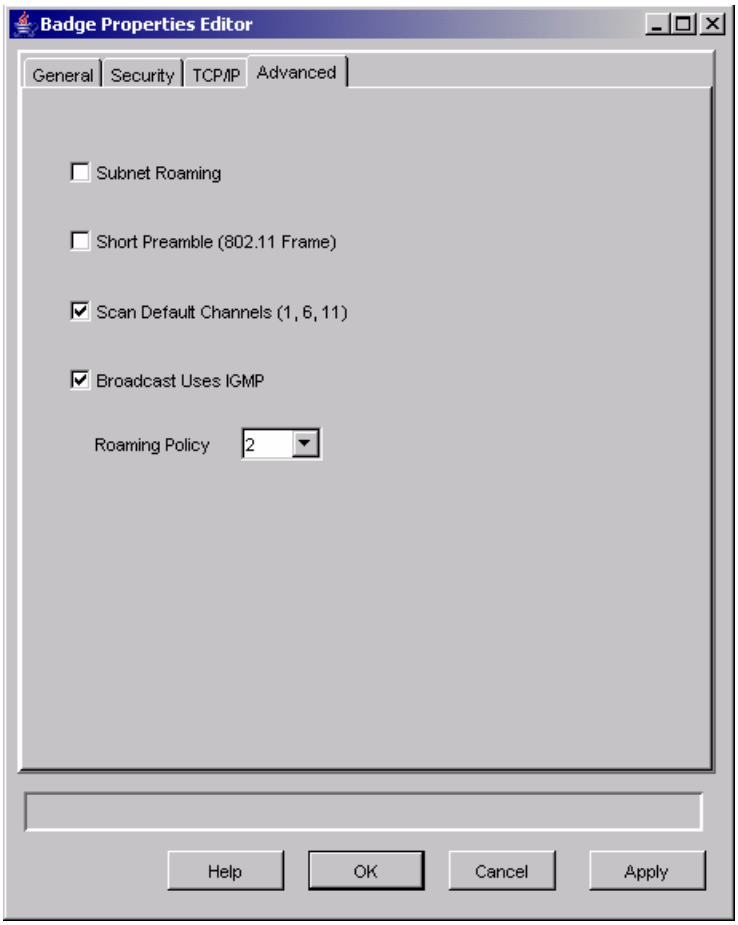


Figure 7 - Vocera BCU "Advanced" TAB

When "Subnet Roaming" is checked will instruct the badge to request a new IP address after each roam, in the LWAPP environment, the infrastructure helps maintain client connectivity at Layer 3. When a voice client must wait for the DHCP server to respond before being able to send or receive packets, delay and jitter are introducted. Without checking "Scan Default Channels (1,6,11)" the badge will scan all 802.11b channels when the badge looks to roam, preventing the forwarding of packets and seamless roaming.

Tuning AutoRF for your environment

As described above within the "Recommendations" section it is important to understand that each site has it's 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 adjusting AutoRF, please take a moment to reference Radio Resource Management under Unified Wireless Networks on CCO at:
http://www.cisco.com/warp/public/114/rrm.html

RRM allows you to adjust the transmit power of each AP, by adjusting how strong each AP will hear its THIRD strongest neighbor. This value can only be adjusted from the CLI using the "config advanced 802.11b tx-power-thresh" command as described the the Tx Power Level Assignment Settings section in the same document (http://www.cisco.com/warp/public/114/rrm.html#tx_power)

Before adjusting AutoRF, walk the deployment site, using the Vocera badge as worn by the end user and a site survey tool and to a strong understanding of how the badge roams and the power each AP is seen at, throughout. Once this is complete and it is determined that adjusting this value is required, begin with a value of –71dBm for the Transmit Power Control algorithm, using the following 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 observing any changes. Once the network has been given a sufficient amount of time, walk the site using the same survey tool and badges again, observing the same roaming characteristics and AP 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.

How do I know the tranmit power is too hot or too cold?
Determining whether you have your transmit power threshold too high or too low requires a good understanding of your environment. Having first 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.

Too Hot?
The Vocera badge will roam based solely on the signal strength rather than signal quality, if the Vocera badge does not roam after passing 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 of your network running too hot.

Too Cold?
The default transmit threshold should almost never provide you a deployment area where your network is running too cold. If the transmit power threshold was 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 may have been tuned too low. Again, 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 is "sticking" to an AP 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 be raising power?
- Look at the WLC log file and AP neighbor lists to help determine why such an anomaly could occur.

If you find that in one or more isolated areas, the badge is having "dead" or "spotty" coverage, it is again time to examine these areas separately.

- Is this area near an elevator shaft, radiology, or a break room?
- These areas may 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 may 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, etc. -

Wireless Network Infrastructure Configuration

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 the 'Apply' button is not pressed before moving on to the next step.

Under the "Controller" top-level menu:

- Change 'Ethernet Multicast Mode' to 'Multicast'
- Set the 'Multicast Group Address' to '239.0.0.255' (or some other unused multicast group address)[3]
- Set the 'Default Mobility Domain Name' and 'RF-Network Name' to your network design
- Disable Aggressive Load Balancing

[3] Avoid using Internet Assigned Numbers Authority (IANA) reserved addresses in the 224.0.0.0 - 224.0.0.255, 224.0.1.0 – 224.0.1.255 and 239.0.0.0 – 239.255.255.255 Please refer to http://www.iana.org/assignments/multicast-addresses for a complete list and understanding of such reserved IPv4 Multicast address.

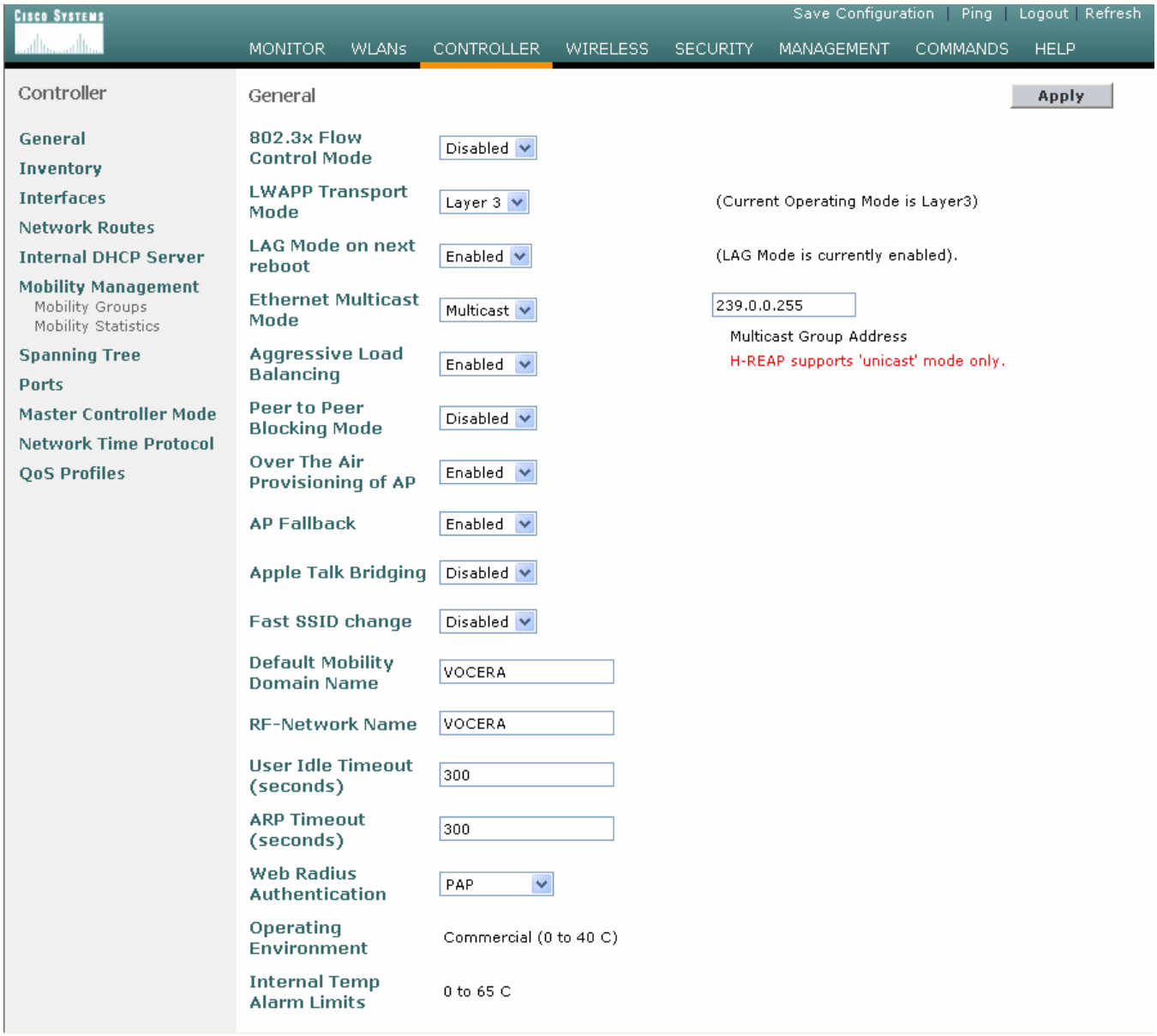


Figure 1. General WLC configuration

Creating Interfaces

Click on “Interfaces”, From the Controller top-level menu.

Note	Your VLAN and IP Address will vary. The screen shots below provide sample addressing which should not be directly followed..

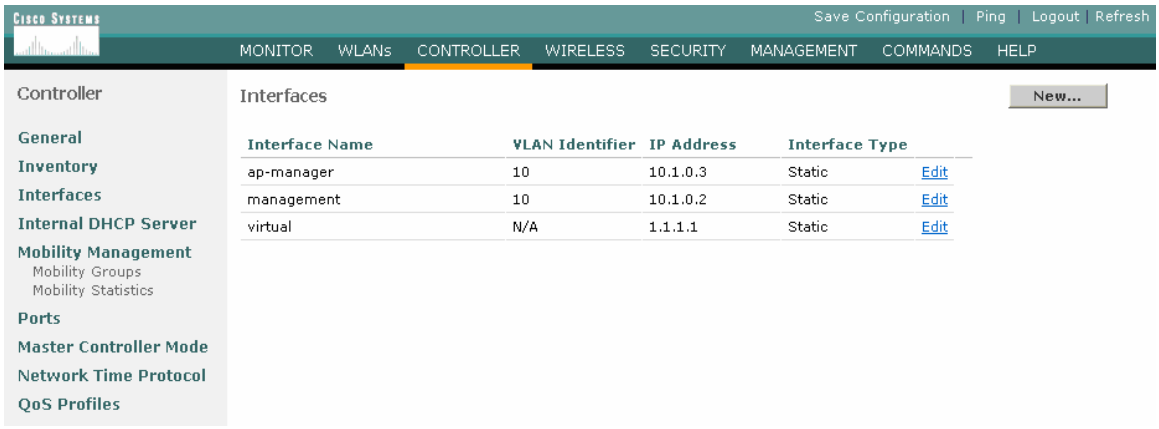


Figure 2. List of WLC Interfaces

Creating the Vocera® Voice interface:

- Select “New”
- Enter into the ‘Interface Name’ field a tag name representative of your Vocera® VoWLAN network
- Enter into the ‘VLAN ID’ field the VLAN number of that VoWLAN network
- Select “Apply” and go back to “Edit” the interface that is just created
- Enter the IP addressing for this interface that is in the range of the VLAN and other related information
- Select “Apply”

Wireless-specific Configuration

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

- The DTIM Period is 1
- Support for 802.11g has been disabled, only the 802.11b data rate of ‘11Mpbs’ is ‘Mandatory
- Short preamble is disabled
- DTPC is disabled

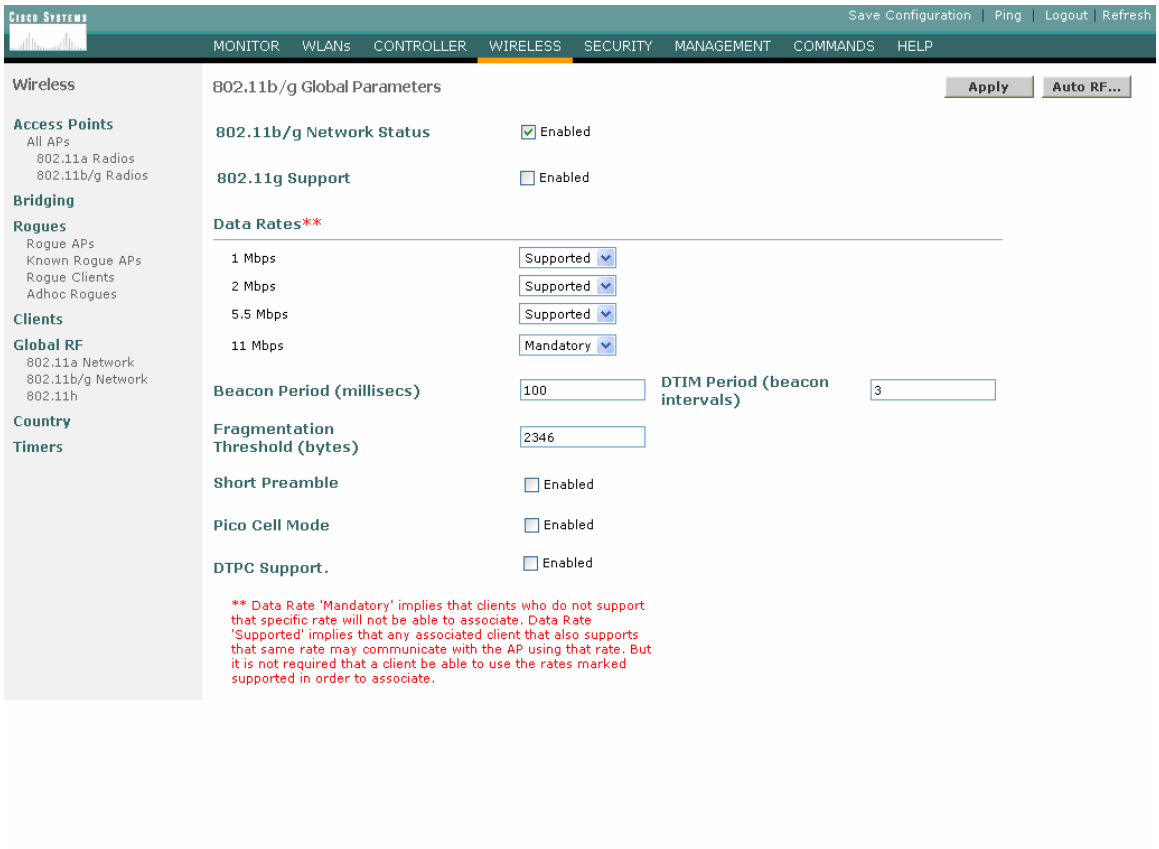


Figure 3. 802.11b/g configuration

WLAN Configuration

- Update the Radio Policy field to the value that best fits the needs.
- Change ‘Admin Status’ to ‘enabled’
- Set ‘Session Timeout’ to ‘1800’
- Set ‘Quality of Service’ to ‘Platinum’
- Set ‘Broadcast SSID’ to ‘enabled’
- Set the ‘Interface Name’ to the interface created for the Vocera® Communication Badges
- Set the security options up to match your corporate policies

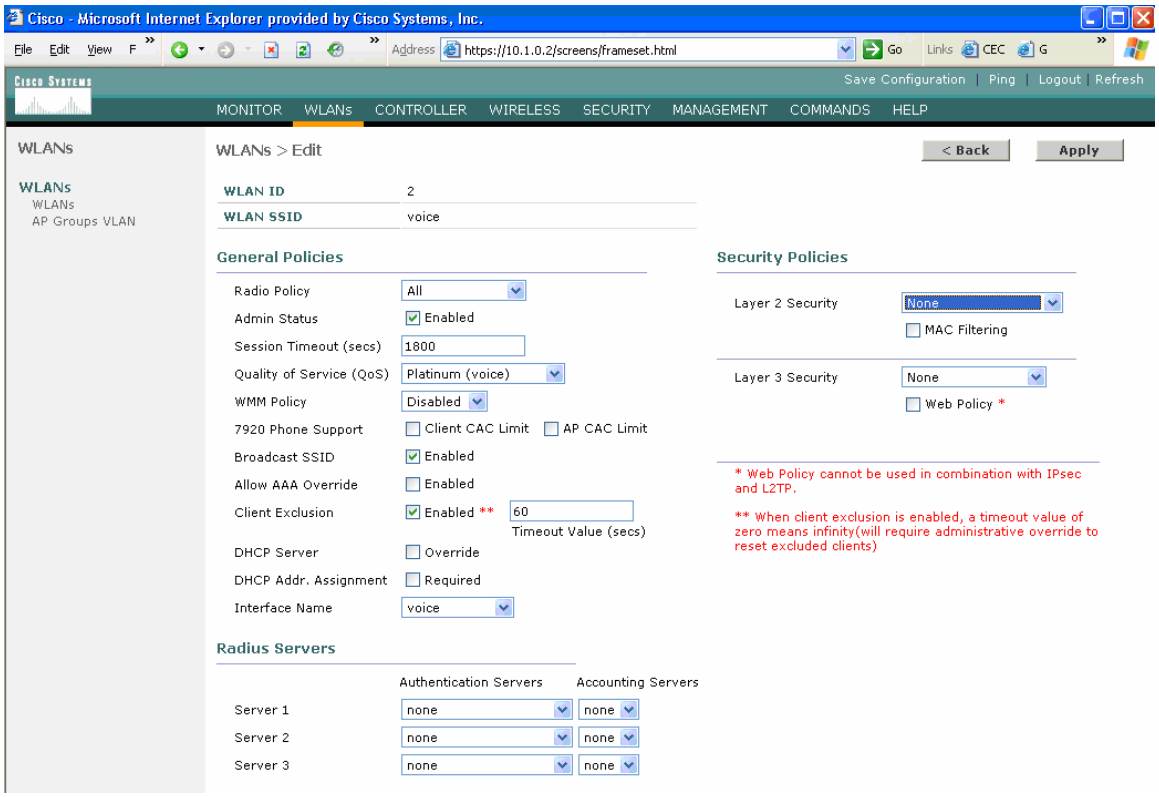


Figure 4. WLAN Configuration

Configuring AP Detail:

- Select “Detail”
- Configure the “AP Name”
- Ensure AP is configured for DHCP
- Ensure “Admin Status” is “Enable”
- “AP Mode” should be set to “local” for AP mode
- Enter the Location of the AP
- Enter the controller name the AP belongs to. The controller name can be found on the “Monitor” page
- Select “Apply”

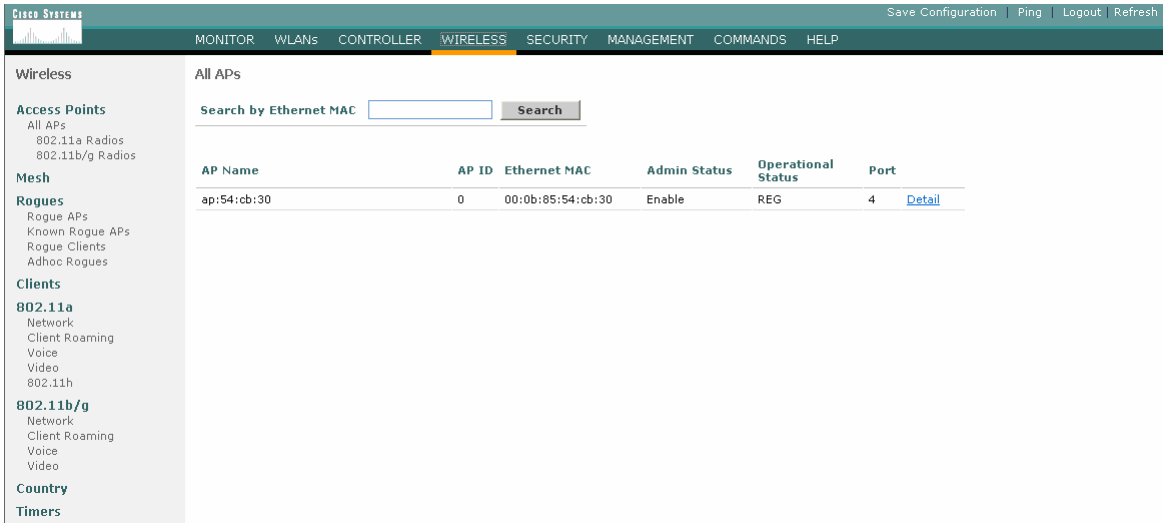
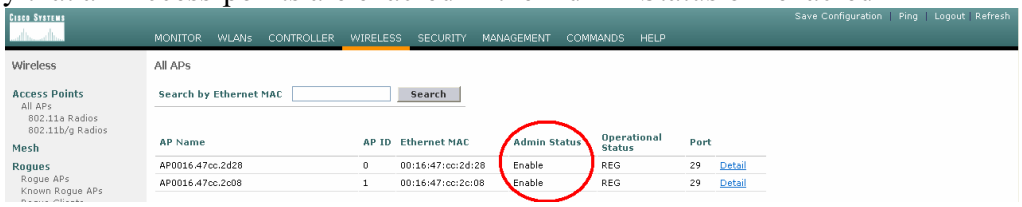


Figure 5. AP Detail

Configuring the 802.11b/g Radio:

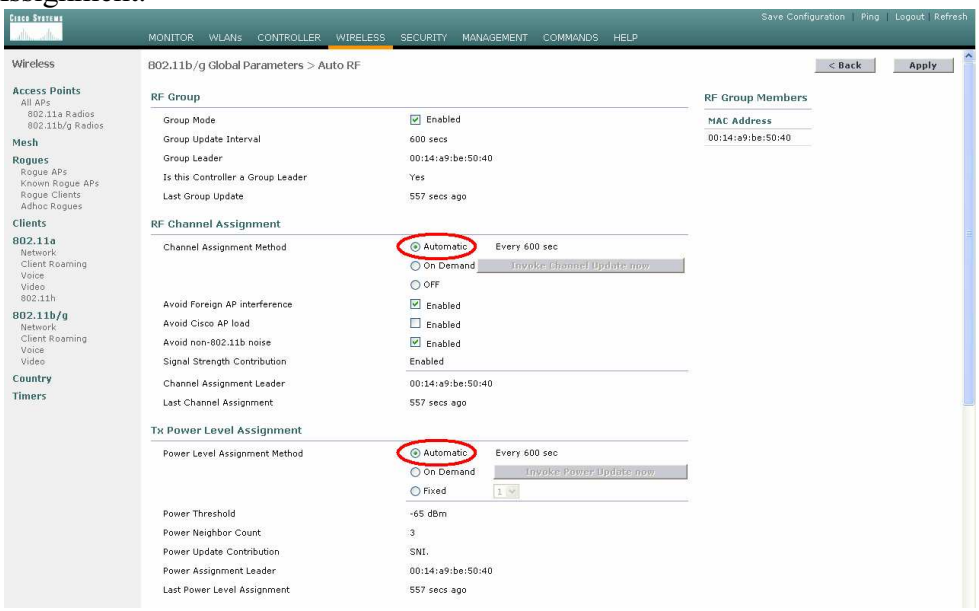
Select the “Wireless” link along the top of the WLC

- Verify that all Access-points are enabled in the Admin Status of “enabled”



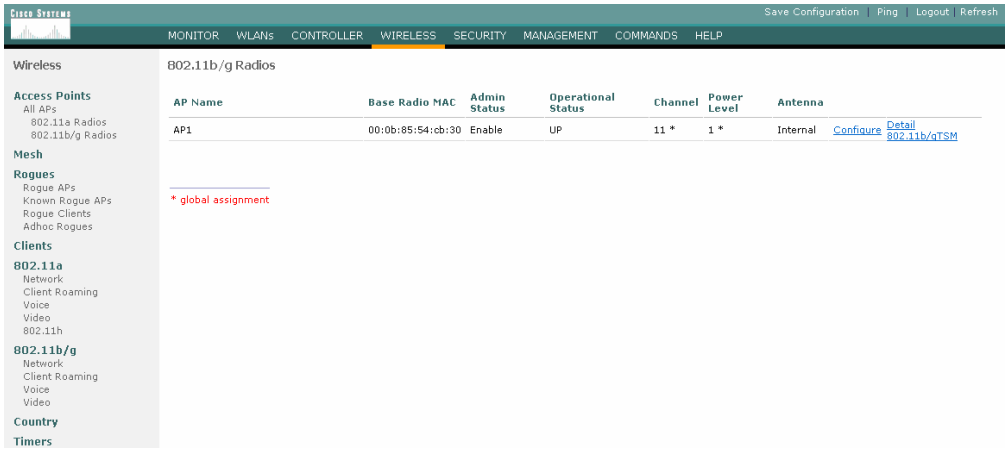
- On left side of WLC Select “Network” beneath “802.11b/g”
- Select “AutoRF” button

- Using AutoRF; create a complete coverage with non-overlapping RF channel and a transmit power by:
    - selecting “Automatic” for both RF Channel Assignment and Tx Power Level Assignment.



- Select “Apply”
- Select ‘Save Configuration’
- Note the section on “Tuning AutoRF for Your Environment” above

Select Wireless > Access Points > 802.11b/g Radios



Configuring Proxy ARP:

Proxy ARP enables the controller to send an 'arp reply' for associated clients that are in 'sleep mode' or are roaming. This feature is enabled by default.

From the WLC CLI, Proxy ARP can be enabled with the following command (The WLC must be rebooted after making this configuration change. Remember to save the configuration before any reboots)

config> network arpunicast enable

Wireless IP Telephony Verification

After conducting an RF site survey and configuring the APs 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 the following locations:

- The primary area of each AP cell (where the badges will most likely connect to that particular AP)
- 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 AP'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, of course, be the final tests.

Association, Authentication, and Registration

The following section explains how to verify that the badge is associating, authenticating, and registering properly.

- At multiple points throughout the environment, power-up the badges and verify association with the AP. If the badge does not associate with the AP, perform the following 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 AP successfully. If the client does not authenticate, check either the WEP key or the LEAP 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 Vocera® communication server. If the client does not register, perform the following checks:

  - Verify that the badge has the correct IP Address, Subnet Mask, Primary Gateway, Primary TFTP, Primary/Secondary and DNS.

- Stationary voice Calls:
  - At multiple points throughout the environment, while standing 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, perform the following: 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 is configured, at multiple points throughout the environment, while standing still, 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, perform the following: If you make a call using the wired phone, is the voice quality acceptable? If not, verify the wired network design against the guidelines.
- Use the site survey tools to verify that there is no more than one AP per RF channel from that location with signal strength (RSSI) greater than 35. If there are two APs 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 AP has an RSSI of 35, ideally the weaker AP should have an RSSI of less than 20. To achieve this goal, you might have to reduce one AP's transmit power or move the AP.
- Check the QoS settings on the AP to confirm proper recommended settings.
- Roaming badge Calls -
  - If the telephony server is not available initiate the Vocera Tutorial with the command "Begin Tutorial"

  OR
  - If the telephony Server is available, initiate a call with a stationary device to the badge
  - continually check voice quality while traversing the total wireless coverage area. If the voice quality is insufficient
  - 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 AP
  - Note the other available APs in the site survey to check coverage and interference.
- Make adjustments to AP placement and settings to fine-tune the WLAN, and perform the following checks to ensure voice quality:
  - Using the site survey tools, verify that there is no more than one AP per channel with an RSSI value greater than 35 in any given location. Ideally, all other APs 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 APs on the same channel should ideally be less than 20.
  - Use the site survey tools to verify that there are at least two APs (total, on separate channels) visible in all location with sufficient signal strength
  - Check that the APs in a given roaming area are all on a Layer 2 network.

Common Roaming Issues

The following roaming issues can occur:

- Badge does not roam when placed directly under AP
- 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 form the Wireless LAN controller.
- Badge is not receiving beacons or probe responses from AP.
- Badge roams too slowly

Badge loses connection to network or Voice service is lost when roaming

- Check authentication for a possible WEP mismatch.
- The badge does not send out IGMP joins or does the network send IGMP queries during a roam, so the Vocera® broadcast function will fail during an L2/L3 roam.
- The badge is capable of seamless Layer 2 roaming only (unless L3 mobility mechanism is configured), so ensure that the new Wireless LAN controller is not serving a different IP subnet
- Verify that the associated AP/controller has IP connectivity to Vocera® Communication server.
- Check RF signal strength and Badge CQ values.

Badge losses voice quality while roaming

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

Audio Problems

There are a few common configuration errors that can cause some easily resolved 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 AP, where a signal might be too weak on either the badge side or the AP side. Matching the power settings on the AP to the badge (20mW), when possible, can fix this problem. This problem is most common when the variation between the AP setting and the badge setting is large (for example, 100 mW on the AP 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. 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 using Layer 3 Mobility, your network could be blocking upstream traffic with Unicast Reverse Path Forwarding (uRPF) checks[4]
- One-way audio can occur if ARP caching is not configured on the Controller

Choppy or robotic audio

- A common reason for choppy or robotic audio is when a microwave is operating nearby. Microwaves start at channel 9 and can extend from channels 6 to 14.
- Check for 2.4Ghz wireless phones and other Nurse call wireless devices using tools like Cognio.

Registration and Authentication Problems

When encountering problems with authentication, perform the following checks:

- Check SSIDs to make sure they match on the badge and the AP (or network). Also be sure the network has a route to Vocera® server.
- Check the WEP keys 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 quite easy to make a typing error when entering a WEP key or password.

The following messages or symptoms can occur:

- Can Not Support All Requested Capabilities - The most likely an encryption mismatch between the AP and the client
- Authentication Failed / No AP found - Ensure authentication types match on AP and client.
- No Service – IP Config Failed - If using static WEP, ensure the keys are configured correctly. Ensure other clients can receive DHCP using the same SSID.
- De-authenticate all TKIP clients from AP - This problem will happen when the AP detects 2 MIC errors within 60 seconds. This countermeasure will keep all TKIP clients from re-authenticating for 60 seconds
- Re-authentication / Session timeout - If configured, a session timeout will trigger a re-authentication which will cause gaps in the voice stream (300ms + WAN delay for 802.1x authentication).

[4] For more information visit http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800ca7cf.html#wp1017386

Appendix A

AP and Antenna Placement

This section gives examples of both proper and improper placement of access points (APs) and antennas.
Improper AP and Antenna Placement
Figure 6 shows improper placement of an AP and antennas close to an I-beam, which creates distorted signal patterns. An RF null point is created by the crossing of signal waves, and multipath distortion is created when signal waves are reflected. This placement results in very little coverage behind the AP and reduced signal quality in front of the AP.

Figure 6. Improper Placement of Antennas Near an I-Beam

Figure 7 shows the signal propagation changes or distortions caused by an I-beam. The I-beam creates many reflections from both received packets and transmitted packets. The reflected signals result in very poor signal quality because of null points and multipath interference. However, the signal strength is high because the AP antennas are so close to the I-beam.

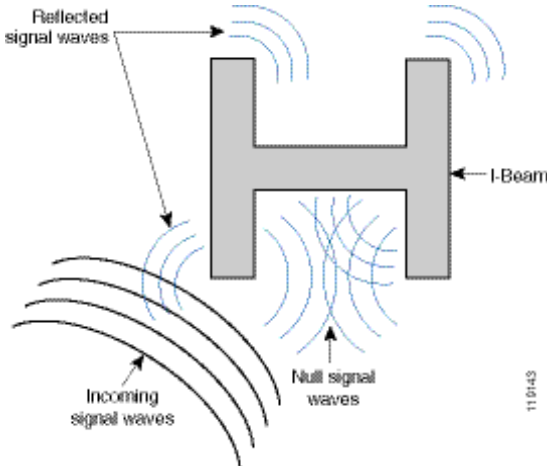


Figure 7. Signal Distortions Caused by Placing the Antennas Too Close to an I-Beam

The AP and antenna placement in Figure 8 is better because it is away from the I-beams and there are fewer reflected signals, fewer null points, and less multipath interference. This placement is still not

perfect because the Ethernet cable should not be coiled up so close to the antenna. Also, the access point could be turn with the 2.4GHz antennas pointed to the floor. This would provide better coverage directly below the access point. There are no users above the access point.

Figure 8. AP and Antennas Mounted on a Wall, Away from I-Beams

Figure 9 shows the signal propagation caused by the wall on which the AP is mounted.

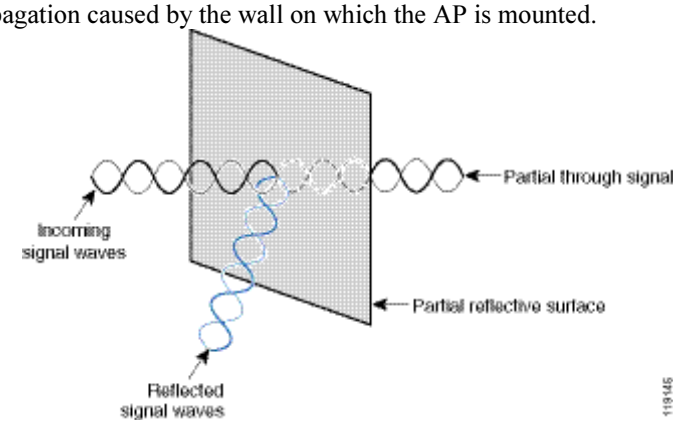


Figure 9. Signal Reflection Caused by a Wall

The preceding examples also apply when placing APs and antennas in or near the ceiling in a standard enterprise environment. If there are metal air ducts, elevator shafts, or other physical barriers that can cause signal reflection or multipath interference, Cisco highly recommends that you move the antennas away from those barriers. In the case of the elevator, moving the antenna a few feet away will help eliminate the signal reflection and distortion. The same is true with air ducts in the ceiling.

A survey conducted without sending and receiving packets is not sufficient. The I-beam example shows the creation of null points that can result from packets that have CRC errors. Voice packets with CRC errors will be missed packets that adversely affect voice quality. In this example, those packets could be above the noise floor measured by a survey tool. Therefore, it is very important that the site survey not only measures signal levels but also generates packets and then reports packet errors.

Figure 10 shows a Cisco AP1200 properly mounted to a ceiling T-bar, with the antennas in an omni-directional position.

Figure 10. Cisco AP1200 Mounted to a Ceiling

Figure 11 shows a Cisco Aironet 5959 omni-directional diversity antenna properly mounted to a ceiling T-bar. In this case, the Cisco AP1200 would be mounted above the ceiling tile.

Figure 11. Cisco Aironet 5959 Antenna Mounted to a Ceiling

Figure 12 shows a Cisco AP1200 properly mounted to a wall.

Figure 12. Figure 8Cisco AP1200 Mounted to a Wall

Figure 13 shows the Cisco Aironet 2012 diversity patch antenna mounted to a wall. In this case, the Cisco AP1200 would be mounted above the ceiling tile.

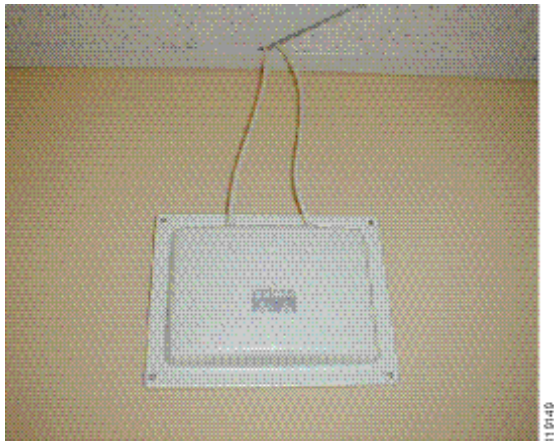


Figure 13. Figure 9Cisco Aironet 2012 Antenna Mounted to a Wall

For areas where user traffic is high (such as office spaces, schools, retail stores, and hospitals), Cisco recommends placing the AP out of sight and placing unobtrusive antennas below the ceiling. Separation for non-diversity antennas should not exceed 18 inches.

Interference and Multipath Distortion

The throughput performance of the WLAN network is affected by unusable signals. WLAN interference can be generated by microwave ovens, 2.4 GHz cordless phones, Bluetooth devices, or other electronic equipment operating in the 2.4 GHz band. Interference also typically comes from other APs and client devices that belong in the WLAN but that are far enough away so that their signal is weakened or has become corrupted. APs that are not part of the network infrastructure can also cause WLAN interference and are identified as rogue APs.

Interference and multipath distortion cause the transmitted signal to fluctuate. Interference decreases the signal-to-noise ratio (SNR) for a particular data rate. Packet retry counts go up in an area where interference and/or multipath distortion are high. Interference is also referred to as *noise level* or *noise floor.* The strength of the received signal from its associated AP must be high enough above the receiver's noise level to be decoded correctly. This level of strength is referred to as the signal-to-noise ratio, or SNR. The ideal SNR for the Vocera® badge is 25 dB. For example, if the noise floor is 95 decibels per milliwatt (dBm) and the received signal at the phone is 70 dBm, then the signal-to-noise ratio is 25 dB. (See Figure 14.)

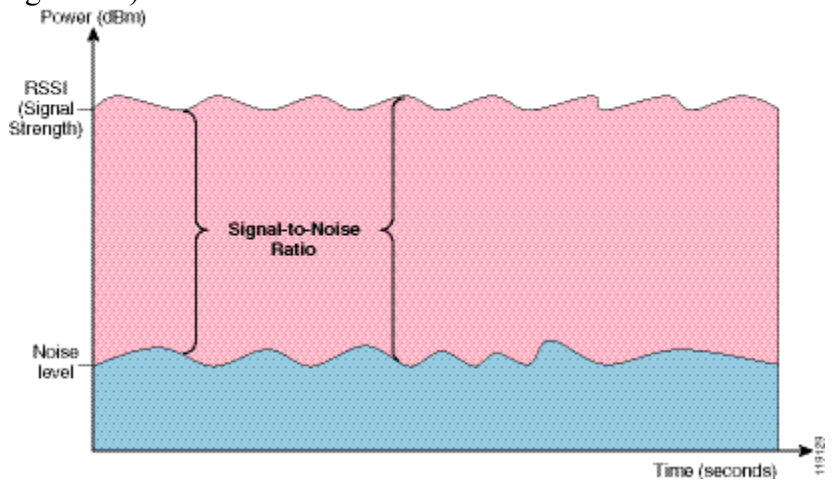


Figure 14. Signal-to-Noise Ratio (SNR)

Changing the type and location of the antenna can reduce multipath distortion and interference. Antenna gain adds to the system gain and can reduce interference if the interfering transmitter is not directly in the boresight of the directional antenna.

While directional antennas can be of great value for certain indoor applications, the vast majority of indoor installations use omni-directional antennas. Directionality should be strictly determined by a correct and proper site survey. Whether you use an omni-directional or patch antenna, indoor environments require diversity antennas to mitigate multipath distortion. The Cisco Aironet Series Access Point radios allow for diversity support.

Signal Attenuation

Signal attenuation or signal loss occurs even as the signal passes through air. The loss of signal strength is more pronounced as the signal passes through different objects. A transmit power of 20 mW is equivalent to 13 dBm. Therefore, if the transmitted power at the entry point of a plasterboard wall is at 13 dBm, the signal strength will be reduced to 10 dBm when exiting that wall. The table below shows the likely loss in signal strength caused by various types of objects.

Signal Attenuation Caused By Various Types of Objects

Object in Signal Path	Signal Attenuation through Object
Plasterboard wall	3 dB
Glass wall with metal frame	6 dB
Cinder block wall	4 dB
Office window	3 dB
Metal door	6 dB
Metal door in brick wall	12 dB
Human body	3 dB

Each site surveyed will have different levels of multipath distortion; signal loses, and signal noise. Hospitals are typically the most challenging environment to survey due to high multipath distortion, signal losses and signal noise. Hospitals take longer to survey, require a denser population of APs, and require higher performance standards. Manufacturing and shop floors are the next hardest to survey. These sites generally have metal siding and many metal objects on the floor, resulting in reflected signals that recreate multipath distortion. Office buildings and hospitality sites generally have high signal attenuation but a lesser degree of multipath distortion.