Vocera Infrastructure Planning Guide

B3000n Compatible

Notice

Vocera Communications, Inc.
www.vocera.com
tel :: +1 408 882 5100
fax :: +1 408 882 5101
2015-04-18 12:05:50

Contents

Infrastructure Planning

Learn how to set up your infrastructure to support Vocera and how to configure the Vocera badge to recognize certain features of your infrastructure.

Introduction

The Vocera Communications System enables people to communicate instantly over a wireless 802.11a/b/g/n network. Vocera users speak into a small, lightweight wireless device, the Vocera badge, to connect and communicate with each other. For an end user, communication is as easy as pushing a button on the badge and saying, “Call Jodie Lee.”

Behind the scenes, however, Vocera is an enterprise application that resides in a complex network infrastructure. Deploying Vocera requires an understanding of how a real-time voice application interacts with your wired and wireless network.

Important: The design guidelines provided in this guide are based on ongoing product testing, research, field experience, and customer feedback. These guidelines represent the best information that we have at any time, and they are refined continually. Make sure you download the latest copy of this guide from **http://www.vocera.com/resource/vocera-infrastructure-planning-guide**.

About this Guide

This guide shows you how to configure your wired and wireless network infrastructure to support the Vocera Communications System. It also describes the badge properties you need to set to make Vocera work efficiently and correctly within your specific network environment. Many of the network topics discussed in this guide are complex and require lengthy explanations that are outside the scope of this document.

This document focuses primarily on network infrastructure topics that affect the Vocera system and discusses larger network infrastructure topics in a summary manner only to provide context. Consequently, this guide assumes that readers have an appropriate background in enterprise networking.

Because complex network infrastructure topics are often interrelated, some points are repeated multiple times in this guide. Cross-references allow you to jump quickly to related topics.

See **WLAN Requirements and Best Practices** on page 95 for a summary of required WLAN settings and best practices for Vocera system implementations.

About the Vocera Badge

The Vocera B3000n badge is the newest badge model and provides several distinct features, including a radio with 802.11 a/b/g/n support, support for both 2.4GHz and 5GHz frequency bands, a call button halo, and an orientation sensor. The information in this guide applies to both the B3000 badge and the more recent B3000n badge.

The badge is a wireless network client that requires configuration before it can communicate on your network, as any IP device does. For example, when you configure a badge, you must specify that a DHCP (Dynamic Host Configuration Protocol) server will assign an IP address dynamically. This IP address is a badge *property*. Similarly, you must specify other properties for your badge, such as the SSID (Service Set Identifier) your wireless network uses, and any security settings your network may require.

Because the badge does not have a keyboard, you must download property settings to it from utilities that run on a configuration computer. The badges are most easily configured and administered as a group. You use the utilities to create a single properties file that describes settings for all Vocera badges, and then use the radio in the badge to download the settings in the properties file.

A badge *profile* is the set of properties that specifies how that badge connects to your network and behaves in your wireless environment. If you are supporting B3000n and B3000 badges, you can configure them to use different profiles. That is, you can place them on WLANs with different security settings, tune them independently to optimize their performance, or give them any combination of different property settings for specific purposes.

While this document discusses the badge properties you need to set to support your network environment, it does not provide detail on using the utilities, setting up the configuration computer, or downloading the properties. See the *Vocera Badge Configuration Guide* for a complete description of these topics.

About the Vocera Collaboration Suite

The Vocera Collaboration Suite (VCS) includes a powerful application enabled by the Apple IOS and Android operating systems. The VCS app provides access to all the voice communication features of a Vocera badge as well as offering secure messaging, alert, alarm, and chat capabilities.

You can download the VCS app from the iTunes and Google stores and install it in recommended devices. See the *Vocera Messaging Platform iPhone User Guide* and *Vocera Messaging Platform Android User Guide* for more details.

The Vocera Client Gateway provides a signaling and multimedia gateway from the VCS app to the Vocera Server for all calls. All voice communication between the Vocera Server and the Vocera app is done through the Vocera Client Gateway.

Important: When you are designing your wireless network, make sure that you configure your access points to provide the VCS app and badges with the minimum signal strength of -65 dBm recommended by Vocera for the area where the devices are used. If you are using both badges and the Vocera Collaboration Suite, the transmit power of the access points should be set to a level comparable to the Vocera badge, which has a smaller radio and battery than the smartphone due to its lightweight, wearable design.

About the Vocera Smartphone

The Vocera smartphone provides the one-touch, instant communication capability of a Vocera client in a familiar phone form factor. The Vocera smartphone provides a powerful application platform enabled by the Microsoft Windows Mobile operating system.

The Vocera smartphone is a wireless phone that supports 802.11 a/b/g frequency bands. You can also pair your smartphone with a Bluetooth headset to perform hands-free calls and play audio.

The Vocera Client Gateway provides a signaling and multimedia gateway from the smartphones to the Vocera Server for all calls. All communication between the Vocera Server and the Vocera smartphone is done through the Vocera Client Gateway.

Smartphones are configured separately from Vocera badges. For details on how to configure smartphones for your network, see the separate *Vocera Smartphone Configuration Guide*.

Important: When you are designing your wireless network, make sure that you configure your access points to provide smartphones and badges with the minimum signal strength of -65 dBm recommended by Vocera for the area where the devices are used. If you are using both badges and smartphones, the transmit power of the access points should be set to a level comparable to the Vocera badge, which has a smaller radio and battery than the smartphone due to its lightweight, wearable design.

Voice and Data Applications

Wireless networks are often designed to support the needs of mobile computers accessing data, not the requirements of applications that perform real-time processing, like Vocera. Although wireless networks can support both types of traffic, voice applications have delivery requirements that data traffic does not have.

Specifically, voice applications have a very low tolerance for packet delays, latency, or jitter that affect data in only superficial ways. For example, depending upon the sensitivity of the listener, a delay of 150 milliseconds may cause an unacceptable and distinct interruption in a stream of spoken words, but it is essentially imperceptible to a user opening or copying a file.

Wireless LAN Configuration

Deploying Vocera into a wireless network requires you to configure settings on your network devices and also properties on the Vocera badge. In addition, you need to consider certain configuration options that—while not actual requirements—may improve the performance of the Vocera system.

This chapter discusses the requirements and recommendations for deploying Vocera into your wireless infrastructure.

802.11b/g/n and 802.11a/n Support

Both the B3000n and B3000 automatically use the 802.11b and 802.11g data rates that have been enabled on the access points. For optimal coverage, Vocera recommends that you enable all 802.11b, 802.11g, and 802.11a data rates on the access points.

802.11a Support

The B3000n badge, the Vocera Smartphone, and many iOS and Android devices running the Vocera Collaboration Suite application support 802.11 a/b/g/n. The B3000 badge supports 802.11b/g only.

802.11a supports bandwidth up to 54 Mbps, and uses the higher, regulated frequency spectrum above 5 GHz. Channels are 20 and 40 MHz and are non-overlapping. However, due to the higher frequency, 802.11a has a shorter range signal than 802.11b/g.

The B3000n and Vocera smartphones can be configured to use 802.11a/n only, 802.11a/b/g/n, or 802.11b/g/n. Vocera recommends avoiding a deployment that requires inter-band roaming. Configure the B3000n badges to use only one band: either 2.4Ghz or 5Ghz, but not both at the same time.

Important: If you decide to deploy any Vocera devices on 802.11a, you must perform a voice quality site survey prior to deployment to ensure proper coverage.

Access Point Settings

Vocera requires specific settings for the following access point features:

Table 1: Required AP settings for Vocera

AP Feature	Setting
Beacon Interval	**100 milliseconds** (typically the default). See Beacon and DTIM Intervals on page 14.
DTIM Interval	**1**. See Beacon and DTIM Intervals on page 14.

AP Feature	Setting
Data Rates	Enable all 802.11a/b/g/n data rates, and set one or more to Basic. See **Data Rates** on page 15.
SSID	The same for all access points on a VLAN. You can configure badge profiles to use different SSIDs for different badge types. See **SSID and Security** on page 15.
Security Settings	The same for all access points on a VLAN. You can configure badge profiles to use different security settings for different badge types. See **SSID and Security** on page 15.
Peer-To-Peer Communication	**Enabled** on the access point or on the WLAN controller (if using CAPWAP access points). See **Peer-To-Peer Communication** on page 15.
Encryption	**AES** (If 802.11 rates are used).
Radio Channel Utilization	Consistently less than 30%.
Channel Width	**20 Mhz** (for 2.4GHz). **20Mhz or 40Mhz** (for 5 Ghz).
Guard Interval	**Long** (for both 2.4Ghz and 5 Ghz).

Autonomous Versus CAPWAP Access Points

Vocera supports both autonomous and CAPWAP (Control and Provisioning of Wireless Access Points) access points. Autonomous access points are useful in smaller deployments but typically lack the centralized configuration management needed for a large-scale enterprise WLAN deployment. CAPWAP access points are centrally configured and controlled by a WLAN controller.

Ruckus Wireless, howerver, offers wireless solutions with Autonomous access points. See **Vocera Recommendations for Ruckus Networks** on page 97.

Cisco Unified Wireless Network

Cisco Systems offers several models of CAPWAP access points with WLAN controllers, which are part of Cisco's Unified Wireless Network architecture. For tips on Cisco Unified Wireless Network deployments, see **Best Practices for Cisco Unified Wireless Networks (CAPWAP)** on page 75.

Beacon and DTIM Intervals

An access point broadcasts a special management frame called a beacon at a fixed interval, providing wireless clients such as the Vocera badge with information about the wireless network.

Note: When using DFS channels, a best practice is to broadcast the Vocera SSID in beacons for the B3000n badge.

One information element in the beacon specifies the access point's DTIM (Delivery Traffic Indication Map) interval. The product of the DTIM and beacon intervals determines the total length of time an access point will wait before sending multicast or broadcast traffic to a client. For example, if the DTIM interval is 1 and the beacon is set to 100 milliseconds, the total interval is 100 milliseconds; similarly, if the DTIM interval is 2 and the beacon is set to 100 milliseconds, the total interval is 200 milliseconds.

Vocera employs a 108-millisecond jitter buffer to help ensure uninterrupted audio on the badge. If a packet arrives out of sequence or is transmitted with a slight delay, the buffer allows for continuous audio if the delay does not exceed the buffer's size.

Consequently, you must set the DTIM interval to 1 and the beacon interval close to 100 milliseconds to ensure that the badge receives multicast traffic properly and plays audio that does not sound choppy. Vocera recommends setting the beacon to 100 milliseconds, although values between 95 and 105 milliseconds have worked successfully.

Important: The product of the DTIM interval and the beacon interval should not exceed 108 milliseconds. Otherwise, multicast audio will sound choppy.

Data Rates

When designing a network to support VoWLAN devices, industry best practices encourage enabling higher 802.11 basic data rates (11Mbps optimal) and removing support for lower rates (1, 2, 5.5 Mbps). If you absolutely need to enable lower data rates, configure your 802.11 beacons for 11Mbps anyway, when your AP/controller solution allows it. This configuration allows beacons and other 802.11 management traffic to be on and off the wireless medium faster, improving low channel utilization and optimizing capacity.

Low-speed frames (e.g. 1 and 2Mbps) decrease the overall throughput of your wireless network. As you add APs and devices to your wireless network, make sure you re-check channel utilization to ensure that they stay within acceptable levels (anything below 10% average is optimal).

Important: Your RF site survey must reflect the lowest 802.11 basic rate you have configured. Be careful if you increase the 802.11 basic or "beacon" rate without a site survey, as this can create coverage holes in your deployment.

See **Data Rates and Overlapping Cells** on page 21 and **Configuring AP Radio Data Rates** on page 79 for additional information.

SSID and Security

The badges are centrally maintained by the Vocera server from a single configuration file. Because the badge does not have a keyboard, this centralized management is practical and minimizes maintenance that would otherwise be time-consuming and error-prone.

You can use the Badge Properties Editor to specify properties for all Vocera badges. In addition, you can specify different network profiles for different badge types, allowing them to reside on different VLANs.

See the *Vocera Badge Configuration Guide* for additional information about configuring badge security.

See **Security** on page 30 for additional information about configuring badge security.

Peer-To-Peer Communication

For a wireless network, peer-to-peer communication is the capability of a client to communicate with another client that is connected to the same access point. Some vendors implement features that optionally allow you to prevent this capability. For example, Cisco optionally lets you use the "P2P Blocking Action" feature to prevent peer-to-peer communication.

You must enable peer-to-peer communication on each autonomous access point or on the WLAN controller (if using CAPWAP access points) to allow badges to communicate with each other when they are connected to the same access point.

Automatic Wireless Configuration

Some WLAN controllers offer automatic configuration features that allow you to dynamically adjust transmit power levels and wireless channels used by the access points. If you use these automatic configuration features, they must be tuned properly for your Vocera system.

- **Dynamic Transmit Power Adjustment**—If an access point goes off line, its neighboring access points will increase their power to compensate for the coverage hole. If not tuned

properly for Vocera, the Dynamic Transmit Power Adjustment feature can cause neighboring APs to increase their power, resulting in transmit power asymmetry in some coverage areas, which in turn may cause choppy audio or one-way audio on badge calls.

Vocera suggests limiting the Dynamic Transmit Power adjustment according to the device and frequency, as follows:

Table 2: Dynamic Transmit Power adjustment limits

Device and Frequency	Maximum Adjustment
B3000n Transmit Power 5GHz	Max 16dBm (40mW) - Min 13dBm (20mW)
B3000n Transmit Power 2.4 GHz	Max 17dBm (50mW) - Min 12dBm (16mW)
B3000 Transmit Power only in 2.4 GHz	Max 15dBm (30mW) - Min 11dBm (12.5mW)

- **Dynamic Channel Assignment**—If the adaptive wireless network detects an interference that conflicts with the access point's channel, it may change the channel of some or all of the access points on the network. There is no mechanism for the access point to inform the badge that it is changing its channel. When the access point changes its channel, the badge may take several seconds to discover that the access point it is associated with is no longer on that channel and it will begin its roaming process to find a suitable access point.

For tips on tuning Radio Resource Management (RRM) algorithms for Cisco CAPWAP deployments, see **Best Practices for Cisco Unified Wireless Networks (CAPWAP)** on page 75.

If you decide to use automatic AP configuration features, it's important that you perform a complete **voice quality** site survey after the configuration has been done. You may need to tune the settings. Resurvey the system to verify proper coverage and power levels.

Coverage

You must perform a voice quality site survey to ensure adequate network coverage prior to installing Vocera. If your site survey was not performed to meet the specific needs of Vocera, you will probably need to extend your coverage because:

- The badge is used in physical locations that are frequently ignored by a site survey because they are irrelevant to traditional notebook computer use. Such locations include stairwells, elevators, break rooms, closets, and outside the front door.
- Vocera has different tolerance for errors and delays than data.

  See **Voice and Data Applications** on page 11 for additional information.
- The antenna in the badge behaves differently than the antennas typically used to perform site surveys.

  See **Minimum Signal Strength** on page 17.

You should perform a site survey as an initial step in determining appropriate network coverage. However, you must perform the additional tasks described in this section to make sure your network coverage is adequate for Vocera.

Use the following steps to confirm site survey coverage for Vocera:

1. Set AP power levels comparable to the transmit power of the Vocera badge (See**Power** on page 22).
2. Make sure you have adequate signal strength for the Vocera badge throughout your facility (See **Minimum Signal Strength** on page 17.
3. Make sure the signal-to-noise ratio (SNR) is greater than 25 dB.
4. Use the Vocera badge in survey mode to confirm proper coverage and ensure voice quality throughout your facility (See **Acceptable Voice Quality** on page 17).

5. Use the appropriate subset of channels, based on the frequency band:
   - For 5GHz, do not use either the Dynamic Frequency Selection channels (52,56,60,64,100,104,108,112,116,120,124,128,132,136,140,144) or channel 165. Use all other available channels.
   - For 2.4GHz, use only channels 1, 6, and 11 to maintain adequate channel separation (See **Channel Separation** on page 19).

   Make sure the channels you enable in the wireless controller match the channels you specify in the `B3N.ChannelsToScan5G`, `B3N.ChannelsToScan`, and `B3.ChannelsToScan` properties in the `badge.properties` file. See the *Vocera Badge Configuration Guide*
6. Make sure the coverage cells for all access points overlap sufficiently while maintaining separation between access points on the same channel. (See **Overlapping Cells** on page 21).
7. Minimize co-channel interference (See **Co-Channel Interference** on page 20).

Minimum Signal Strength

Check the entire badge usage area to ensure adequate signal strength as follows:

1. Perform measurements in at least two directions, but ideally four.
2. Make sure the signal strength is always greater than -65 dBm.
3. Make sure AP transmit power is set to a level comparable to the typical transmit power of the Vocera badge, 14.5 dBm (28 mW). See **Power** on page 22.

Note: Testing in four directions offset by 90 degrees provides a margin of error and an additional check of your work.

The notebook computers typically used to perform site surveys contain omnidirectional antennas; however, the badge antenna is less perfectly omnidirectional and the signal strenght is additionally affected by the body of the person wearing the badge.

The antenna in the Vocera badge is directional when the badge is worn properly. That is, attenuation resulting from the human body causes badge coverage at the back of the body to drop considerably.

Consequently, if you are performing measurements with equipment that uses an omnidirectional antenna, *you must ensure a minimum of -65 dBm signal strength in all areas where the badge is used* to accommodate situations where the body of the person wearing the badge is directly between the badge and the access point with which it is associated.

See **B3000n Antenna Patterns** on page 83 for plots of the B3000n antenna patterns.

Acceptable Voice Quality

Each type of Vocera badge provides a different utility for evaluating the communication quality of the signal you are receiving from an access point.

The Vocera badge measures communication quality in *SNR* (for Signal-to-Noise Ratio). The SNR values are not equivalent to traditional SNR values, which are normally measured in decibels. Instead, SNR values are based on a logarithmic scale ranging from 0 to 92, where 0 represents no signal and 92 is the strongest possible signal with essentially no background noise.

Use the Vocera badge survey tools to confirm that your access point coverage is sufficient to support the badge in all areas where it will be used. The Vocera system can maintain good voice quality in all places where the SNR value is greater than or equal to 18.

The Vocera utilities for evaluating communication quality are Layer 2 applications that do not require the badge to connect to the Vocera server or to acquire an IP address. Consequently, you can use it to confirm network coverage early in the implementation process, before the Vocera system is physically deployed.

Use the following steps to confirm communication quality levels throughout a site:

1. Press the Select button and scroll to display the Info icon.
2. Press the Select button to display the Info menu.
3. Press the Down button until RADIO appears.
   The badge displays information similar to the following:

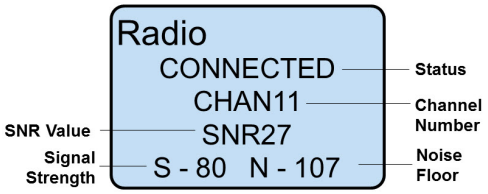


Figure 1: Radio Info screen

4. The badge begins beeping at the following rate to indicate the SNR value:

   Table 3: B3000 badge beep rates in survey mode

Roaming Policy	SNR Value	Beep Rate
0	SNR > 16 16 >= SNR >= 12 12 >= SNR >= 0	1 beep / 5 seconds 1 beep / second 2 beeps / second
1	SNR > 18 18 >= SNR >= 12 12 > SNR >= 0	1 beep / 5 seconds 1 beep / second 2 beeps / second
2	SNR > 20 20 >= SNR >= 12 12 > SNR >= 0	1 beep / 5 seconds 1 beep / second 2 beeps / second
3	SNR > 22 22 >= SNR >= 12 12 > SNR >= 0	1 beep / 5 seconds 1 beep / second 2 beeps / second

5. Wear the badge normally.

   Use a lanyard or one of the other badge attachments to wear the badge properly. Do not handle the badge or read the display as you perform the test, or it will not measure access point signal strength correctly.

   Note: You may want to perform a survey with two badges, both in survey mode. Wear the first badge normally and listen for beeping tones that indicate the general SNR range. Hold the second badge to display the SNR value, but turn down the badge volume so the tones do not distract other people.

6. Connect a headset to the badge.

   The badge emits a tone during the test to indicate the communication quality. In certain environments, such as hospitals, this tone can be mistaken for the emergency sound made by life-support equipment.

7. Walk slowly through the entire coverage area and listen to the tones made by the site survey tool. You must perform the test in two directions offset by 180 degrees (while facing one direction, and then while facing the direction 180 degrees opposite).

   Don't forget to include stairways, elevators, kitchens, bathrooms, and other areas where Vocera usage exposes gaps in conventional site surveys.

8. To exit from the Radio Info screen, press the badge Select button.

9. Note any area where the tone from the Radio Info tool indicates that the coverage is less than or equal to the acceptable level for the current roaming policy, somewhere between 18 and 22.

   You must improve the coverage in these areas in order to have a successful deployment.

Playing a Test Tone

Vocera badges provide two voice commands that allow you to play a continuous test tone, which can help identify areas with choppy audio or inadequate wireless coverage:

- Play Test Tone—plays a continuous test tone
- Broadcast Test Tone—plays a multicast test tone (a broadcast sent from the server to you only).

Both commands require that you are logged in as a user with administrator privileges.

If Vocera users complain of poor coverage or choppy audio, you can use the Play Test Tone and Broadcast Test Tone commands to test the badge's operation in that location.

Attention: DO NOT play the test tone for longer than a couple minutes at a time. Repeatedly playing a test tone on a badge continuously for ten minutes or more could cause speaker performance to degrade over time.

Use the following steps to play a test tone in a particular location:

1. Bring two Vocera badges to a location where choppy audio was reported.
2. Approach the nearest wireless access point.
3. On one badge, press the Call button and say “Play Test Tone.”
4. On the other badge, select the Info > Radio command to see the Vocera SNR value for that location.
5. With both badges, walk away from the access point.

   Note the quality of the test tone and the SNR value as you are walking.
6. Continue walking until the badge indicates that the SNR value has dropped to 18. This is the fringe of the signal for acceptable voice quality. Stop the test.
7. Walk back to the original point and repeat the test, but this time say the voice command “Broadcast Test Tone.”

Channel Separation

Under the 802.11b/g standard, a transmission on one channel can interfere with transmissions as far as four channels away. That is, an 802.11b/g signal on channel 1 can cause interference with a transmission on channels 2, 3, 4, or 5.

To prevent adjacent channel interference, the radio channels in nearby access points should be separated from each other by five channels. In the United States, you must use channels 1, 6, and 11 to avoid adjacent channel interference (there is a bit more flexibility for channel selection in an 802.11b/g network in Europe, where channels 1 through 13 are available). You should assign specific non-interfering channels to your access points, rather than relying on settings such as "Least congested channel" that allow access points to select a channel dynamically.

Note: The Vocera system locale determines which wireless channels are supported on Vocera badges. When you install the software, you specify the locale in the Country field. For more information, see the "Working with Locales" appendix in the *Vocera Installation Guide*.

If your network uses channels 1, 6, and 11 only, you can further improve the performance of Vocera badges by configuring them to scan only those three channels, which minimizes reconnect time while roaming.

To specify the default 2.4GHz channels to scan:

- Use the Wireless Properties section of the Badge Properties Editor to specify the 2.4 GHz channels for all badges. In the `badge.properties` file, make sure you have set values for both `B3.ChannelsToScan` and `B3N.ChannelsToScan`. For more information, see the *Vocera Badge Configuration Guide*.

Following is a simplified illustration of access points in a network using channels 1, 6, and 11 only:

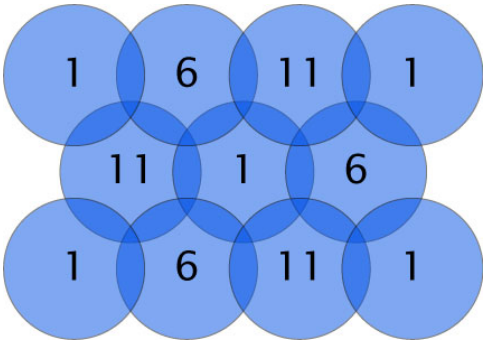


Figure 2: Access points using channels 1, 6, and 11

The above illustration is a simplified representation of an access point map, because the coverage cell of each access point is actually irregular, rather than a constant radius, due to environmental factors. In addition, the boundary of the coverage cell changes dynamically, as people and objects move around in the network environment.

To specify the default 5GHz channels to scan:

- Use the Wireless Properties section of the Badge Properties Editor to specify the 5GHz channels. In the `badge.properties` file, make sure you have set the proper value for `B3N.ChannelsToScan5G`. For more information, see the *Vocera Badge Configuration Guide*.

Note: For further recommendations on specifying 5GHz channels, see **Enterprise Mobility 4.1 Design Guide VoWLAN Design Recommendations**.

Co-Channel Interference

Co-channel interference occurs when access points on the same channel are located too close to each other. When this situation occurs, multiple access points can transmit at the same time on the same channel, corrupting packets on both channels, and causing transmission delays.

In order for a network to provide continuous coverage over a large area, access points must be placed fairly close together. Considering that only three non-interfering channels are available for use in an 802.11b/g network, it is quite possible that the location of some access points will cause co-channel interference.

Make a note of the areas where co-channel interference occurs instead of creating coverage gaps to avoid it. Test these areas thoroughly and keep track of user complaints. Badge usage patterns can determine whether it is sufficient to manage these areas or if you need to change them.

You can mitigate some co-channel interference problems by using directional antennas. In some situations, these antennas provide better performance than omnidirectional antennas because you can use them to fine-tune coverage areas.

Overlapping Cells

Successful and smooth hand-offs can occur only if the coverage cells of adjacent access points overlap. For example, a person who is roaming while wearing a badge must be able to stay connected to the current access point while moving into the coverage area of an adjacent access point, so the hand-off can occur without dropping packets. A properly designed wireless network must provide cells with overlapping coverage on non-interfering channels, while simultaneously maintaining proper cell separation among access points using the same channel.

Vocera recommends that you design for 10% to 20% overlap of coverage cells. This ensures that when someone moves from one cell to another adjacent cell while on a Vocera call, a smooth hand-off can occur without any lost packets.

As mentioned previously, the boundaries of access point coverage cells can change in real-time, as people and objects move around in the network environment. Some access points attempt to accommodate this situation by adjusting their power output dynamically.

Data Rates and Overlapping Cells

The 802.11b/g standard provides the following data rates: 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, and 1 Mbps. For optimal performance, Vocera recommends that you enable all 802.11b/g data rates. This will allow a client to maintain a connection by switching among data rates, if necessary, rather than losing the connection and dropping packets. Although 11 Mbps-only networks are growing in popularity, they require access points to be more densely packed, increasing the likelihood of access points on the same channel having overlapping cells, causing interference and dropped packets.

When all 802.11b/g data rates are enabled, the badge can move farther away from the current access point but stay connected at a lower data rate, allowing a hand-off to occur while minimizing the likelihood of lost packets. The following graphic, although simplified, illustrates the overlap between cells when multiple data rates are enabled.

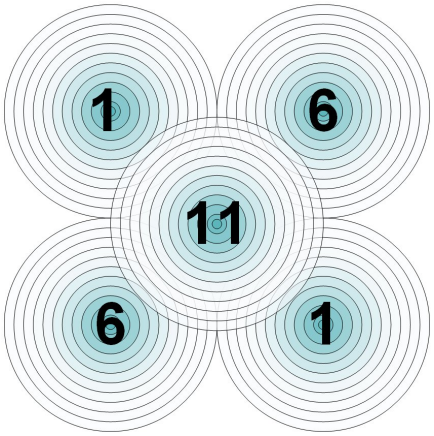


Figure 3: Overlapping cells with multiple data rates

The following illustration shows access points on which only the 11 Mbps data rate has been enabled. This densely packed wireless network results in access points on the same channel having overlapping cells.

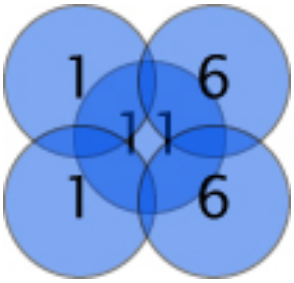


Figure 4: Access points on the same channel with overlapping cells

These overlapping cells on the same channel result in

- interference and dropped packets
- shared network bandwidth
- increase in noise flow
- decrease in signal-to-noise ratio (SNR)

As discussed in **Voice and Data Applications** on page 11, data networks have more tolerance for dropped packets than voice networks, where lost packets show up as dropouts or choppy audio. Consequently, Vocera and other voice applications have best performance when all data rates are enabled.

Many AP vendors now offer location-based services that require very densely deployed APs. Such services allow you to track many types of Wi-Fi devices, including Wi-Fi clients, RFID tags, rogue access points, and rogue devices. In such a WLAN environment, you may need to change the Basic data rates to higher rates.

Power

Make sure that you configure your access points with the minimum signal strength recommended by Vocera for the area where the devices are used. The power of the access points should be set to a level comparable to the Vocera badge. If an access point is set to its default power level (usually 100 mW), there will be a power asymmetry problem. The badge can receive data from the AP, but the AP cannot receive a signal from the badge. This power asymmetry results in choppy audio and one-way audio. See **Automatic Wireless Configuration** on page 15 for suggested limits on automatic power adjustments.

The following tables show the typical transmit power and receiver sensitivity for the B3000n, B3000, and Vocera Smartphone.

Table 4: Radio transmit power and receiver sensitivity for B3000n (2.4GHz)

Mode	Data Rate	Typical Transmit Power	Receiver Sensitivity
802.11b	11 Mbps	+17 dBm	-87 dBm
	1 Mbps	+17 dBm	-90 dBm
802.11g	54 Mbps	+16 dBm	-73 dBm
	6 Mbps	+17 dBm	-91 dBm
802.11n (HT20)	MCS7	+16 dBm	-70 dBm
	MCS50	+17 dBm	-90 dBm

Table 5: Radio transmit power and receiver sensitivity for B3000n (5GHz)

Mode	Data Rate	Typical Transmit Power	Receiver Sensitivity
802.11a	54 Mbps	+14 dBm	-73 dBm
	6 Mbps	+16 dBm	-92 dBm

Mode	Data Rate	Typical Transmit Power	Receiver Sensitivity
802.11n (HT20)	MCS7	+14 dBm	-70 dBm
	MCS0	+16 dBm	-91 dBm
802.11N (HT20, 5GHz only)	MCS7	+14 dBm	-68 dBm

Table 6: Radio transmit power and receiver sensitivity for B3000

Mode	Data Rate	Typical Transmit Power	Receiver Sensitivity
802.11g	54 Mbps	+15.8 dBm	-65 dBm

Table 7: Radio transmit power and receiver sensitivity for Vocera smartphone

Mode	Data Rate	Typical Transmit Power	Receiver Sensitivity
802.11a	54 Mbps	+12 dBm	-74 dBm
	6 Mbps	+17.5 dBm	-90 dBm
802.11g	54 Mbps	+12.5 dBm	-74 dBm
	6 Mbps	+17.5 dBm	-91 dBm
802.11b	11 Mbps	+18 dBm	-87 dBm
	1 Mbps	+18 dBm	-94 dBm

For more details about radio receiver sensitivity, see **Radio Receiver Sensitivity** on page 81.

Interference

802.11 interference occurs when an intruding radio signal interrupts normal system operations. In some cases, an intruding signal can originate in another 802.11 network; in other cases, non-802.11 radio energy can disrupt 802.11 communications. Common sources of non-802.11 interference include microwave ovens, wireless phones, and Bluetooth devices.

Interference can affect any 802.11 transmissions and is not specific to the Vocera system. However, because Vocera is a voice application, interference will be noticed more on Vocera than a data application. Vocera recommends the use of a spectrum analyzer or similar third-party tool to identify and eliminate sources of possible RF interference.

Capacity and Call Load

Capacity refers to the maximum number of badge-to-badge calls a specific access point can support simultaneously, and it varies according to the manufacturer, model, and firmware level of an access point.

Capacity planning is an important aspect of a Vocera deployment. An access point is *flooded* when the number of calls it is processing exceeds its capacity. To prevent flooding, high traffic areas may require more access points than low traffic areas.

For example, you may need to provide additional access points in places such as break rooms or nursing stations, if badge users tend to congregate there. Make sure you pay attention to user traffic patterns when you update your site survey to accommodate the Vocera system.

Keep in mind that the Vocera usage pattern is not similar to that of a conventional telephone. People often use telephones for sustained conversations. However, Vocera calls are typically brief. Because Vocera calls are so short, there is less likelihood of many users being involved in simultaneous calls and exceeding an access point's capacity.

Be careful when introducing additional access points to a network, and make sure you don't inadvertently create new problems, such as choppy audio due to interference with existing access points.

The following table shows the packet characteristics per Vocera device. As you can see, the Vocera smartphone sends more packets per second than Vocera badges, which means it requires more overhead to transmit the sound. Keep this in mind when doing capacity planning for high traffic areas.

Table 8: Packet characteristics per Vocera device

Vocera Version	Device	Codec	Bandwidth Used for Sound	Packet Interval	Packets Per Second
VS 4.4.x	B3000n/B3000	G.711	64 Kbps	36 ms	27.8
	Smartphone	G.711	64 Kbps	20 ms	50
VS 5.x	B3000n/B3000	G.711	64 Kbps	20 ms	50
	Smartphone	G.711	64 Kbps	20 ms	50

The following table shows the recommended maximum number of badge and smartphone calls *with acceptable voice quality* supported on a test wireless network. Results may vary on your wireless network and on other AP models.

Important: It is possible to achieve more calls per AP than shown in the table, but the voice quality will degrade, resulting in choppy audio.

Table 9: Recommended maximum number of calls per AP

Wireless Band	Device	Max Calls Per AP	Max Devices on Calls Per AP
2.4GHz	B3000n/B3000/ Smartphone	8	14
5GHz	B3000n/B3000/ Smartphone	18	30

How MaxClients Can Affect Capacity

Some access point models have a MaxClients setting that limits the number of clients that can be connected to the access point. When the maximum number of clients is reached, additional badges or other clients cannot connect to the access point and will be forced to connect to a less populated but more distant access point, which may affect signal strength and cause choppy audio. If your access point model has a MaxClients setting, you may not need to change its default value, but you should be aware of the setting and how it can affect capacity.

Vocera recommends keeping the AP radio channel utilization at a maximum of 30% consistently.

Note: When WMM is enabled in the Wireless Controller the QBSS (Quality of Service Basic Service Set) is advertised in the beacons. You can use this value as a reference to measure radio utilization. Refer to Vocera Technical Support KB article 2340 Quality of Service (QoS) Basic Service Set (QBSS) for more details.

Roaming

When a user first boots a Vocera badge, it associates with the access point that has the strongest signal. As the user moves around, the signal-to-noise (SNR) ratio of the transmission from an access point may deteriorate. When the SNR reaches the threshold set by the Roaming Policy, the badge starts to probe the network for other access points.

The badge first scans the channels on which other access points were found when the badge was booted. If the badge is unable to find an access point with an acceptable signal, it waits two seconds and then scans three new channels. If an acceptable access point is not found on those channels, it waits two more seconds before scanning three more channels. When the badge identifies an access point with an acceptable signal, it begins a hand-off procedure and associates with that access point. This process is called *roaming*.

Try to plan transition areas between access points as much as possible, so users don't roam in unexpected places. For example, you may want to avoid having an access point cell boundary fall within a conference room, causing users to roam simply by moving about within the room. In most cases, the Vocera badge roams seamlessly, and users do not notice the transition. If necessary, however, you can create a map of transition areas to help manage user expectations.

If WMM and QBSS are enabled, the B3000n badge uses the QBBS information included in beacons (e.g. channel utilization and the number of stations associated with the access point) to find less congested access points with better SNR. The badge then uses these access points as the first roaming candidates.

If you have only B3000 badges, test your cell transition zones carefully, making sure that one access point is a "clear winner" and has a distinctly stronger signal than all others. If all access points have weak signals in a transition zone, a badge user may constantly roam back and forth among them just by turning around or making small movements.

The hand-off between access points that occurs during roaming can potentially affect the performance of Vocera. Roaming performance is discussed in the following sections:

- **The Roaming Policy Property** on page 25
- **Layer 2 Roaming** on page 26
- **Layer 3 Roaming** on page 26

The Roaming Policy Property

The **Roaming Policy** property determines how aggressively the badge attempts to roam as the signal-to-noise (SNR) ratio of the transmission from an access point deteriorates. The badge assesses the SNR in terms of the SNR metric, as discussed in **Acceptable Voice Quality** on page 17. The badge begins to look for another access point when the SNR value drops to a level specified by the **Roaming Policy** value.

The **Roaming Policy** value is an integer from 1 to 3, where 1 specifies the least aggressive roaming and 3 is most aggressive. By default, **Roaming Policy** is set to 2. The following table shows the relationship between badge SNR values and **Roaming Policy**:

Table 10: Roaming policy and badge SNR values

Roaming Policy Value	Typical B3000n/ B3000 SNR when Roaming	Comments
1	18	The lowest value used, since voice quality is maintained when roaming is initiated.
2	20	The default value, initiates roaming while voice quality is good on most networks.
3	22	Initiates roaming while voice quality is high. This value usually causes roaming that is too aggressive, but it may help roaming on a network with densely deployed APs. See **Data Rates and Overlapping Cells** on page 21 for information about data rates.

The previous table shows the typical SNR values at which the badge initiates roaming. The actual SNR values may vary somewhat, due to environmental factors and dynamic changes in coverage.

If you are not satisfied with the roaming behavior of the badge, you can experiment by adjusting the Roaming Policy property. Make sure you test any changes thoroughly before implementing them on all badges in a production system.

To specify the Roaming Policy property:

- Use the Badge Properties Editor to set the **Roaming Policy** property to the appropriate value on all badges. See the *Vocera Badge Configuration Guide*.

Layer 2 Roaming

Vocera supports Layer 2 roaming—Vocera can maintain calls, broadcasts, and other types of badge activity without interruption while the badge associates with a new access point. However, the type of security implemented on your VLAN can potentially affect the performance of Vocera during roaming.

For example, if your VLAN requires 802.1X authentication protocols, the badge must re-authenticate when it roams among access points. Because this authentication adds time to the hand-off, it can potentially result in dropped packets which are noticeable as audio glitches or choppy speech. See Security on page 30 for complete information.

You do not need to configure the badge, the server, or your network in any special way to enable Vocera for Layer 2 roaming; however, you can optionally use the **Roaming Policy** property to change the threshold at which the badge roams.

Layer 3 Roaming

Layer 3 roaming or *Subnet roaming* occurs when the badge is associated with an access point on one subnet and then roams to an access point on a different subnet. Vocera badges support Layer 3 roaming with call preservation.

If IP Mobility is not enabled on the network, the badge will be forced to do a DHCP request and acquire a new IP address in order to roam. This IP acquisition will cause a hand-off delay that can result in lost packets and noticeable audio glitches or choppy speech during a call. The extent of the symptoms you notice are dependent upon the speed of your infrastructure and the length of time it takes the DHCP server to complete the DHCP transaction. See Security on page 30.

Use the following steps to enable Vocera for Layer 3 roaming:

1. Set up each Vocera subnet as described in Multiple Vocera Subnets on page 49.
2. Make sure the **Subnet Roaming** property is set to FALSE on all badges. See the *Vocera Badge Configuration Guide*.

Smartphones and Subnet Roaming

Unlike the Vocera badge, the Vocera smartphone cannot change its IP address mid-stream when moving from one AP to another on different subnets. Consequently, if you deploy Vocera smartphones you must either have a single subnet where the phones are used or you must enable IP Mobility on the WLAN controllers. When IP Mobility is enabled, the Vocera smartphone can roam across subnet boundaries while maintaining its original IP address. See IP Mobility on page 26 .

IP Mobility

IP mobility is the capability of a network to allow a wireless client to roam across subnet boundaries while maintaining its original IP address. For example, the Cisco Wireless LAN Services Module (WLSM) can implement IP mobility on your network. Some vendors refer to IP mobility as *mobile IP*, *Layer 3 mobility*, or *subnet mobility*.

If IP mobility is enabled in your infrastructure, make sure the **Subnet Roaming** property is set to FALSE on all badges. See the *Vocera Badge Configuration Guide*.

Quality of Service

Quality of Service (QoS) refers to techniques for ensuring a certain level of quality for specific applications by allowing a network to treat various types of data differently. For example, a network may prioritize the treatment of packets for real-time applications, such as voice or video communications, while assigning a lower priority to packets for data and other applications that are less affected by latency.

To implement an end-to-end QoS solution for your Vocera system, the following configuration tasks must be performed:

- The QoS Packet Scheduler network service must be installed and enabled on a network connection. When you install QoS Packet Scheduler on any network connection, it is installed on every local network connection. See **Installing the Vocera QoS Manager Service** on page 28.
- Access points must be configured to map IP level DSCP EF to WMM/802.11e level voice priority. The access points pass the DSCP markings through to the network.
- On the network side, switches and routers must be configured to honor DSCP markings.

Vocera B3000n and B3000 badges mark Vocera application packets for both signaling and audio with DSCP value 46 (Express Forwarding) at all times (that is, with or without WMM enabled). The Vocera Collaboration Suite does not mark any packets.

If you skip any of these QoS configuration tasks, performance problems can result. For example, do not enable the Vocera QoS Manager service on the Vocera Server, then packets coming from the Vocera Server will have much less priority on the air than those originating from badges. If there are many active calls under a given AP, then users may experience problems during voice communication with the Vocera Server.

Enabling 802.11e QoS on Badges, Smartphones, and Access Points

802.11e provides standards-based QoS to prioritize voice over data traffic and ensure high level voice quality. Vocera B3000n and B3000 badges as well as the iOS and Android smartphones that host the Vocera Collaboration Suite allow you to use 802.11e to prioritize packets. This prioritization happens at layer 2 (WLAN), unlike the layer 3 tagging described in **Installing the Vocera QoS Manager Service** on page 28. In order to take advantage of this standard, your access points must also support it. When the WMM and EnableAPSD badge properties are set to TRUE and WMM/802.11e is configured properly on the access points, Voice Prioritization is carried out on the WLAN. This allows voice packets originating from badges and smartphones to enjoy higher priority in the air.

When 802.11e is enabled, the Vocera QoS Manager should also be installed and running on the Vocera Server, Vocera SIP Telephony Gateway, and Vocera Client Gateway to ensure that voice packets originating from the server are tagged with DSCP Expedited Forwarding (EF). The access points can be configured to map IP level DSCP EF to 802.11e level voice priority. The access points pass the DSCP markings through to the network.

Vocera smartphones support 802.11e QoS by default. When WMM/802.11e is enabled on the access points, voice packets from smartphones are prioritized for high level voice quality.

Use the following steps to enable 802.11e QoS for Cisco CAPWAP access points:

1. In the Cisco WLC Web User Interface, click WLANS, and then click a WLAN profile name.
2. Click the QoS tab.

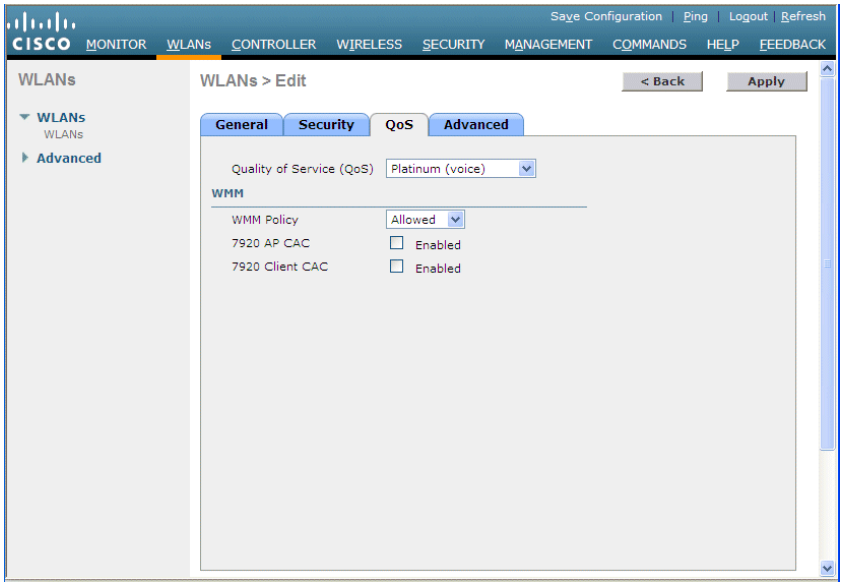


Figure 5: Cisco WLC QoS settings

3. In the Quality of Service list, select `Platinum (Voice)`.
4. In the WMM Policy list, select `Allowed`.
5. Click Apply.

Installing the Vocera QoS Manager Service

The Vocera QoS Manager service is automatically installed with the Vocera Voice Server, Vocera SIP Telephony Gateway, and Vocera Client Gateway. However, the service requires some configuration after installation to make sure it is started. The Vocera QoS Manager service configures the QoS Packet Scheduler network service with QoS parameters required by Vocera, thereby prioritizing the treatment of Vocera voice packets originating from the server.

When the Vocera QoS Manager service is running, each Vocera voice packet originating from the server is tagged with DSCP Expedited Forwarding (EF). On the network side, switches and routers must be configured to honor DSCP markings. See the *Vocera Infrastructure Planning Guide*.

Important: To take full advantage of the benefits of Vocera QoS Manager, the QoS Packet Scheduler network service must be installed and enabled on a network connection. The Vocera installer does not install QoS Packet Scheduler for you. You must do that separately. During installation of QoS Packet Scheduler, you will lose your network connection for a moment, and after installation of the QoS Packet Scheduler you will need to restart the computer to make sure all Vocera services are restarted. In a clustered environment, perform these steps on a standby node first.

To install the Vocera QoS Manager service:

1. Install the Vocera Voice Server, Vocera SIP Telephony Gateway, and Vocera Client Gateway as needed. The Vocera QoS Manager service is installed automatically with these products.
2. Install the QoS Packet Scheduler network service on a network connection. Perform these steps on one computer only, either the Vocera Voice Server, Vocera SIP Telephony Gateway, or Vocera Client Gateway. In a clustered Vocera Voice Server environment, perform the installation on a standby node.
   a) Log in to the Vocera Voice Server computer with administrator privileges.
   b) Choose Start > Control Panel > Network Connections.
   c) Right-click a connection, and choose Properties.

d) Click Install, click Service, and then click Add.

e) Click QoS Packet Scheduler, and then click OK.

Note: When you install QoS Packet Scheduler on any network connection, it is installed on *every* local network connection.

3. Restart the computer.
4. Start the Vocera QoS Manager service, and make sure the startup type of the service is Automatic. Perform these steps on each Vocera Voice Server, Vocera SIP Telephony Gateway, and Vocera Client Gateway.

   a) Choose Start > Control Panel > Administrative Tools > Services.
   The Services dialog box appears, displaying the list of installed Windows services.

   b) Right-click the Vocera QoS Manager service and select Properties. The Vocera QoS Manager Properties dialog box appears.

   c) In the Startup type field, select Automatic.

   d) Click Start to start the service.

   e) Click OK to save the settings and close the Vocera QoS Manager Properties dialog box.

Layer 3 QoS Tagging

Access points provide various mechanisms for prioritizing traffic. For example, you may be able to assign different priorities to traffic based upon any of the following criteria:

- VLAN
- MAC address
- Packet type
- Type of Service (ToS) header

If you set up specific VLANs for real-time applications, you can configure access points to transmit the packets on those VLANs immediately, buffering traffic on other VLANs if necessary. For example, you can effectively prioritize Vocera traffic by setting up a VLAN that is dedicated to voice, and then assigning that VLAN the highest priority.

Similarly, if your access points allow you to prioritize traffic by MAC address, you can configure them with the MAC address of each Vocera badge. This system has the disadvantage of being error-prone and difficult to maintain as new badges are added. In general, prioritizing by VLAN is more effective. However, many customers record the MAC address of each Vocera badge in a spreadsheet or database for tracking purposes, and you may be able to leverage that data when configuring your access points.

QoS focuses on prioritization of downstream flows from the access point. If the Vocera QoS Manager service is installed on the Vocera Server, you can also prioritize upstream flows of traffic. See **Installing the Vocera QoS Manager Service** on page 28 .

Many access points allow you to flag specific types of packets as high priority traffic. Some access points can properly identify Vocera traffic.

All voice traffic originating from the badge is tagged with ToS bits in order to be identified and prioritized by network equipment that is sensitive to QoS tagging. When Vocera QoS Manager is running, all voice traffic originating from the Vocera Server is similarly tagged. All voice traffic originating from Vocera SIP Telephony Gateway and Vocera Client Gateway is also QoS-tagged without requiring Vocera QoS manager.

The system uses the IP header's ToS field and sets it to 0xB8 (10111000). This provides some flexibility for QoS-aware equipment to handle Vocera packets for low-latency, jitter-free communications.

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)

Note: This is layer 3 tagging only, and does not reflect Class of Service (CoS) marking in the data frames. All voice packets originating from the badge are tagged with the respective ToS bits. Classification and prioritization can be done at Ethernet egress and ingress of the AP and switched network. This is only applicable if the AP has the capability to support and examine ToS markings.

See your vendor documentation for information about how to identify Vocera packets to your access point.

Security

Security is a critical concern for any enterprise application. In particular, the data transmitted on a wireless network is often considered to be at risk because radio waves can be monitored without physical access to the network.

Vocera supports well-known industry standards for wireless security. The following topics describe security support provided by Vocera and discusses the network overhead introduced by various security methodologies.

Note: In order to support 802.11n data rates, you must configure the B3000n to use AES-CCMP. See the *Vocera Badge Configuration Guide* for additional information.

Security Support

Vocera supports industry standard security systems as well as popular proprietary security methods such as Cisco LEAP. The following table summarizes the security support in Vocera:

Table 11: Vocera security support

Authentication	Encryption	B3000n Support	B3000 Support	Smartphone Support
Open	None	✓	✓	✓
	WEP64	✓	✓	✓
	WEP128	✓	✓	✓
WPA-PEAP	TKIP-WPA	✓	✓	✓
WPA-PSK	TKIP-WPA	✓	✓	✓
EAP-FAST	TKIP-WPA	✓	✓	
EAP-TLS	TKIP-WPA	✓	✓	
WPA-PEAP	AES-CCMP	✓	✓	✓
WPA-PSK	AES-CCMP	✓	✓	✓
EAP-FAST	AES-CCMP	✓	✓	
EAP-TLS	AES-CCMP	✓	✓	
LEAP	WEP64	✓	✓	
	WEP128	✓	✓	
	TKIP-WPA	✓	✓	
	AES-CCMP	✓	✓	

Note: In order to support 802.11n data rates, you must configure the B3000n to use AES-CCMP. See the *Vocera Badge Configuration Guide* for additional information.

The LEAP, WPA-PEAP, EAP-FAST, and EAP-TLS protocols typically require each user in a network environment to be authenticated with a unique set of credentials. However, each badge in a profile must have the same security properties so the Vocera server can automatically update all badges when necessary. Consequently, Vocera supports device authentication for WPA-PEAP, LEAP, EAP-FAST, and EAP-TLS, not user authentication. All badges must present the same set of credentials for network authentication.

The WiFi Alliance (WFA) has deprecated support for WEP, and newer versions of wireless controllers may not have configuration options for TKIP. Even though the B3000n and B3000 badges support WEP or TKIP, Vocera recommends not using them.

Vocera has tested the following authentication servers:

Table 12: Authentication servers

Model	Manufacturer	Supported Authentication
ACS (Access Control Server)	Cisco	EAP-TLS, EAP-FAST, LEAP, WPA-PEAP, and mixed LEAP/WPA-PEAP client environments
IAS (Internet Authentication Service)	Microsoft	EAP-TLS, WPA-PEAP (badge only)
Steel-Belted Radius	Juniper Networks	LEAP

Security and Roaming Delays

In general, increasing levels of security increase the amount of time required for a client to associate with the network. The overhead introduced by security can cause performance problems with Vocera. This overhead is not noticeable the first time a badge associates with an access point, but it may cause a noticeable interruption in speech if a badge roams and re-associates while a call is active.

While encryption techniques such as WPA-PSK introduce a certain amount of overhead to each packet, the required processing is minimal and does not affect Vocera. The overhead introduced by authentication techniques, however, can be significant and may affect the performance of the badge as it roams.

The delay in re-associating when roaming depends upon the specific configuration of your network and the type of security you implement. You may need to experiment to find the best balance between an appropriate level of security and acceptable performance.

Authentication Delays

The following table provides general guidelines for the amount of additional overhead different methods of security introduce when roaming. The specific performance you see may vary depending upon the access point you are using and your network configuration.

Table 13: Average additional association delays caused by authentication

Authentication Type	Association Delay	Comments
WPA-PSK	< 100 ms	WPA-PSK often provides the optimal trade-off between security and performance.
EAP-FAST	200 ms	Frequent session timeouts can result in additional delays. See **Optimizing WPA-PEAP, LEAP, EAP-FAST, and EAP-TLS** on page 32.
LEAP		
WPA-PEAP	Varies	The association delay caused by authentication varies based on the cipher strength (1024 bit or 2048 bit) and the depth of certificate chains.
EAP-TLS		

All forms of authentication introduce considerable overhead. In particular, WPA-PEAP and EAP-TLS add the most overhead due to the time required for connecting to an authentication server. WPA-PSK provides a considerable level of security while introducing only minimal overhead.

B3000n and B3000 badges support Opportunistic Key Caching (OKC), which is available for authentication between multiple APs with cached credentials. The B3000n and B3000 also support Cisco CCKM. See **Enabling CCKM for Fast Roaming** on page 33 for additional information.

Optimizing WPA-PEAP, LEAP, EAP-FAST, and EAP-TLS

The WPA-PEAP, LEAP, EAP-FAST, and EAP-TLS protocols require back-end authentication servers to authenticate client credentials the first time a client connects to the network, each time the client roams, and at periodic intervals. Various properties control how often the authentication occurs, and in the case of WPA-PEAP and EAP-FAST, whether a full authentication or a fast authentication occurs.

The authentication that occurs the first time a client connects to the network is not noticeable to a badge user because it appears to be part of the general boot and connection procedure. However, the authentication that occurs during roaming or at a timeout interval can interrupt a conversation, due to packets that are lost while the authentication server processes credentials and re-authenticates the badge. You can optimize badge performance by allowing fast reconnects and setting a lengthy timeout interval, as described in the following sections.

Timeout Intervals

On authentication servers, a Session Timeout value specifies the duration of time that elapses before a client such as the badge is required to re-authenticate, regardless of whether it has roamed. Some vendors may refer to this timeout value as a group session timeout or a user session timeout.

Because a session timeout always triggers re-authentication, you can optimize performance by making sure that the timeout interval does not expire too frequently. For example, if your employees typically work eight-hour shifts, you could set the session timeout value to eight hours, ensuring that an authentication timeout does not occur during a shift.

Note: Do not confuse this session timeout, with the WPA-PEAP session timeout described in **PEAP Session Timeouts** on page 32.

Fast Reconnects

WPA-PEAP and EAP-FAST require a full authentication the first time a client connects to the network, but optionally allow a fast reconnect any other time an authentication occurs, up until the expiration of the PEAP session timeout interval for WPA-PEAP or the expiration of the authorization PAC time to live (TTL) for EAP-FAST. See **PEAP Session Timeouts** on page 32 and **EAP-FAST Stateless Session Resume** on page 33.

Because a fast reconnect reduces the time required for re-authentication by several seconds, you can optimize WPA-PEAP and EAP-FAST performance by enabling fast reconnects. For example, if a user roams during a conversation, the authentication that occurs causes the minimum possible interruption when fast reconnects are enabled.

PEAP Session Timeouts

When you are using WPA-PEAP authentication, an additional value called the PEAP Session Timeout interacts with fast reconnects. When the PEAP session timeout interval expires, a client is required to perform a full authentication, regardless whether fast reconnects are enabled, the next time any authentication occurs. Do not confuse the PEAP session timeout with the session timeout described in **Timeout Intervals** on page 32.

You can optimize performance by making sure that the PEAP session timeout interval does not expire too frequently, as you do with the regular session timeout. For example, if your employees typically work eight-hour shifts, you could set the PEAP session timeout value to eight hours, ensuring that a full authentication does not occur during a shift.

EAP-FAST Stateless Session Resume

When you are using EAP-FAST authentication, an additional option called Allow Stateless Session Resume interacts with fast reconnects. This setting is similar to the PEAP Session Timeout setting. Make sure this option is selected, and specify a value for the Authorization PAC Time to Live (TTL) property. The Authorization PAC TTL value (in minutes or hours) sets the time after which the user authorization PAC expires. When ACS receives an expired authorization PAC, the stateless session cannot resume and phase two EAP-FAST authentication is performed. Therefore, you should set the Authorization PAC TTL property to a value that does not trigger a full authentication over the duration of a typical shift.

Enabling CCKM for Fast Roaming

Cisco Centralized Key Management (CCKM) is a form of fast roaming supported on Cisco access points and on various routers. Using CCKM, Vocera B300n and B3000 badges can roam from one access point to another without any noticeable delay during reassociation. After a Vocera device is initially authenticated by the RADIUS authentication server, each access point on your network acts as a wireless domain service (WDS) and caches security credentials for CCKM-enabled client devices. When a Vocera device roams to a new access point, the WDS cache reduces the time it needs to reassociate.

To take advantage of CCKM for B300n and B3000 badges, your access points and badges must be configured to enable CCKM. You also must use either LEAP, WPA-PEAP, EAP-FAST, or EAP-TLS authentication. For details on how to configure badges for CCKM, see the *Vocera Badge Configuration Guide*.

Follow these steps to enable CCKM for Cisco CAPWAP access points:

1. In the Cisco WLC Web User Interface, click WLANS, and then click a WLAN profile name.
2. Click the Security tab.
3. For Layer 2 Security, select "WPA+WPA2".
4. For Auth Key Mgmt, select "CCKM" or "802.1X+CCKM". The "802.1X+CCKM" setting should be selected only if you have clients that are not CCKM-enabled.

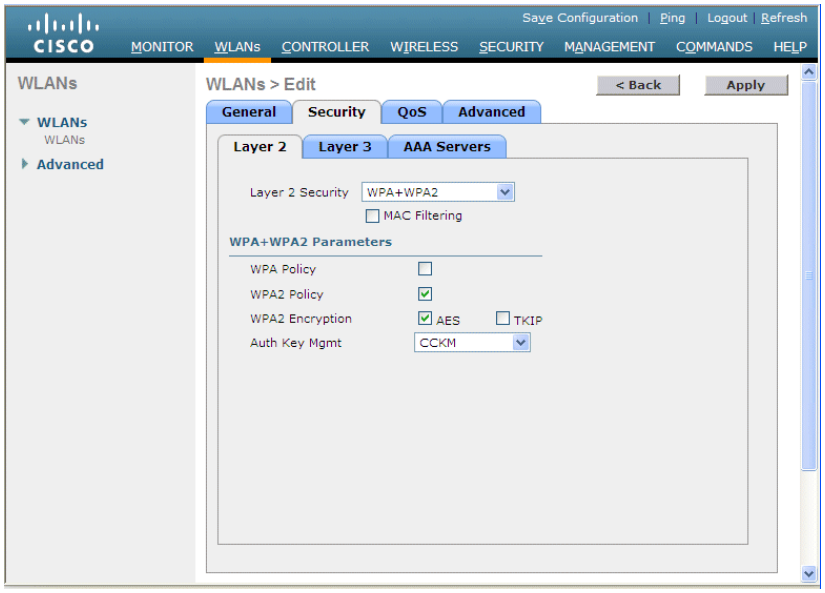


Figure 6: Cisco WLC Security settings for CCKM

5. Under Security, click the AAA Servers tab.
6. Specify which RADIUS authentication server to use with this WLAN profile.
7. Click Apply.

8. See the following Cisco document for instructions on how to enable CCKM for autonomous APs:

   Configuring WDS, Fast Secure Roaming, Radio Management, and Wireless Intrusion Detection Services [1]

Configuring EAP-TLS Authentication

B3000n and B3000 badges support EAP-Transport Layer Security or EAP-TLS, which provides excellent security, relying on client-side and server-side certificates. EAP-TLS is an IETF open standard, and is universally supported by WLAN vendors. It provides strong security by requiring both the badge and an authentication server to prove their identities via public key cryptography, or digital certificates. The EAP-TLS exchange is encrypted in a TLS tunnel, making it resistant to dictionary attacks.

For background on EAP-TLS authentication and public key cryptography, see the following article:

EAP-TLS Deployment Guide for Wireless LAN Networks[2]

Authentication Server

If you are implementing EAP-TLS, you will need an authentication server (Microsoft Internet Authentication Services or Cisco Access Control Server). For information about EAP-TLS, see the following articles:

Server	Article
Microsoft IAS	**EAP**[3]
Cisco ACS	**EAP-TLS Version 1.01 Configuration Guide**[4]

EAP-TLS Session Timeouts

For EAP-TLS, Vocera highly recommends the related Session Timeout interval be set to the duration of one shift (for example, 8 hours). Otherwise, voice quality of calls while roaming will be sub-optimal.

Supported Certificate Formats

On the client (badge) side, Vocera supports only the PEM certificate file format. Other certificate formats, such as DER, PFX, and P12, are not supported in this release for the client (badge) side. To convert certificates to PEM format from another format, you can use tools like openssl (http://www.openssl.org/). On the authentication server, you can use whatever certificate format your server supports.

Certificate Revocation

Vocera badges do not check the revocation status of certificates, and therefore do not support Certificate Revocation Lists (CRLs) maintained on the authentication server.

---

1 http://www.cisco.com/en/US/docs/wireless/access_point/12.4_3g_JA/configuration/guide/s43roamg.html
2 http://www.cisco.com/en/US/tech/tk722/tk809/technologies_white_paper09186a008009256b.shtml
3 http://technet.microsoft.com/en-us/library/cc782851(WS.10).aspx
4 http://72.163.4.161/en/US/products/sw/secursw/ps2086/products_configuration_example09186a008068d45a.shtml

Using Vocera Manufacturer Certificates

If you do not want to manage EAP-TLS certificates for Vocera B3000n and B3000 badges, you can choose to use the Vocera Manufacturer Certificates, client- and server-side certificates supplied by Vocera. Vocera Manufacturer Certificates use 2048-bit RSA keys, which provide excellent security for today's enterprise and conform to industry standards and NIST recommendations.

B3000n and B3000 badges are preconfigured with EAP-TLS client certificates that are automatically downloaded from the Vocera Server or the configuration computer. However, you need to install Vocera server-side certificates on your authentication server.

Note: Vocera Manufacturer Certificates are not pre-installed on Vocera smartphones. If you want to use EAP-TLS authentication for Vocera smartphones, you need to either obtain certificates from a trusted CA, or generate your own certificates.

Use the following steps to configure your authentication server for EAP-TLS using Vocera Manufacturer Certificates:

1. Locate the following server-side certificates in the `\VS\certificates\EAP-TLS` folder on the Vocera DVD:

File	Description
vmc_rootca_cert.pem	Root CA certificate
server_cert.pem	Server certificate
server_key.pem	Server private key

2. Install all the above certificates and configure the EAP-TLS part of your authentication server.
3. Add a username named `Vocera Manufacturer Certificate Client` to your authentication server database. The name must match exactly, otherwise authentication will fail. Choose any password for this user.
4. Run the Badge Properties Editor on the configuration computer, click the Security tab, and specify the following B3000n and B3000 badge properties:
   - Authentication – EAP-TLS
   - Use Custom EAP-TLS Certificates – unchecked
   - Encryption – TKIP-WPA or AES-CCMP

   Save the `badge.properties` file, and then copy it to your Vocera Server computers.
5. Stop and start the Vocera Server. B3000n and B3000 badges are automatically updated, and they are authenticated with the authentication server.

Using External Certificates

Rather than using the Vocera Manufacturer Certificates, you can manage the EAP-TLS certificates yourself, either generating your own self-signed certificates or obtaining certificates from a trusted Certificate Authority (CA) such as Microsoft Certificate Authority.

Use the followiong steps to configure your authentication server for EAP-TLS using external certificates:

1. Generate the new EAP-TLS certificates.

   Note: Note the password used to encrypt the client key. You will need to enter this password for the Client Key Password property (see below).
2. Download the server-side certificates to your authentication server.
3. Copy the Root CA certificate, the client certificate, and the client key to the following folder on the Vocera Server and the configuration computer:

   `%VOCERA_DRIVE%\vocera\config\gen2\badge\res\certificates\EAP-TLS`

   Note: The certificates for the client (badge) side must be in PEM format.

4. Rename the files with the following names:

File	Description
rootca_cert	Root CA certificate
client_cert	Client certificate
client_key	Client private key

5. Add a username to your authentication server database that the badges will use for authentication. Choose any password for this user.
6. Run the Badge Properties Editor on the configuration computer, click the Security tab, and specify the following B3000n and B3000 badge properties:
   - Authentication – EAP-TLS
   - Use Custom EAP-TLS Certificates – checked
   - User Name – Username created on the authentication server
   - Client Key Password – Password used to encrypt the client key
   - Encryption – TKIP-WPA or AES-CCMP

   Save the `badge.properties` file, and then copy it to your Vocera Server computers.
7. Stop and start the Vocera Server. B3000n and B3000 badges are automatically updated, and they are authenticated with the authentication server.

Configuring EAP-TLS for Cisco ACS

Follow these steps to configure EAP-TLS for Cisco ACS:

1. Install a New ACS Certificate.
2. Add a Certificate Authority to the List of Trusted Certificate Authorities.
3. Edit the Certificate Trust List.
4. Specify Global Authentication Settings.
5. Add a User for EAP-TLS Authentication.
6. Set Up Access Points on the ACS.
7. Restart ACS.

Installing a New Cisco ACS Certificate

1. In the ACS web interface, choose System Configuration > ACS Certificate Setup > Install ACS Certificate.

Figure 7: Install New Certificate page

2. Select whether to read the certificate from a file or use a specified certificate from storage.

   Note: The certificate file refers to the Server Certificate file. If you are using Vocera Manufacturer Certificates, the certificate file is `server_cert.pem`.

3. If you selected to read the certificate from a file, specify the full path of the certificate file in the Certificate File field.
4. If you selected to use a certificate from storage, type the Common Name (CN) of the certificate in the Certificate CN field.
5. To select a certificate from storage, check the Select Certificate from Storage box, and then select a certificate from the list.
6. In the Private Key File field, type the full path of the private key file.

   Note: The private key file refers to the Server Private Key file. If you are using Vocera Manufacturer Certificates, the private key file is `server_key.pem`.
7. In the Private Key Password field, type the private key password. If you are using Vocera Manufacturing Certificates, contact Vocera Technical Support to obtain the private key password.
8. Click Submit.

Adding a Certificate Authority to the List of Trusted Certificate Authorities

1. In the ACS web interface, choose System Configuration > ACS Certificate Setup > ACS Certification Authority Setup.
2. In the CA Certificate File field, type the full path and file name of a new certificate authority.

   Note: Type the path of a certificate that has a Root CA. If the certificate has a multiple layer Root CA hierarchy, submit each Root CA certificate in the hierarchy.
3. Click Submit.

Editing the Certificate Trust List

1. In the ACS web interface, choose System Configuration > ACS Certificate Setup > Edit Certificate Trust List.
2. Select the certificate (make sure it's checked) that you submitted, such as the Vocera Manufacturer Certificate CA. if you submitted multiple Root CA certificates, make sure all of them are checked.
3. Click Submit.

Specifying Global Authentication Settings

1. In the ACS web interface, choose System Configuration > Global Authentication Setup.
2. Under EAP-TLS settings, select the following options:

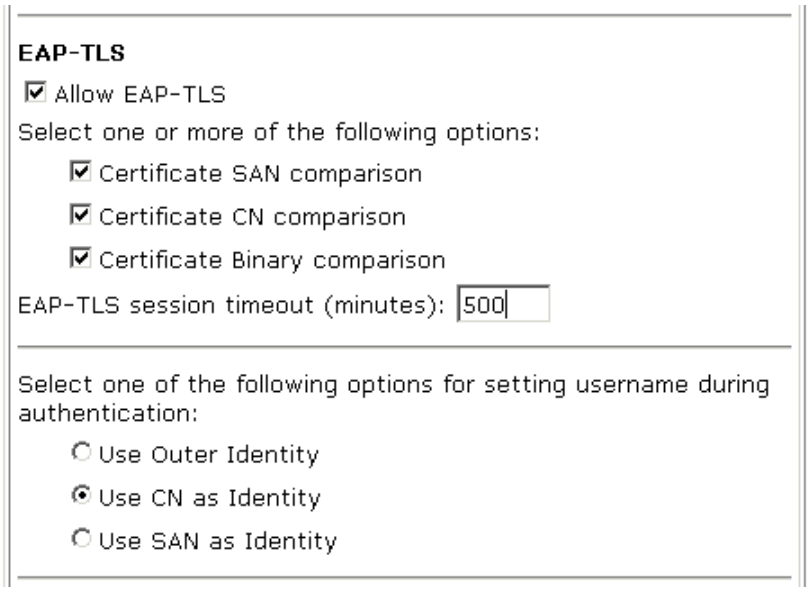


Figure 8: EAP-TLS settings

a) Make sure Allow EAP-TLS is checked.
b) Select at least one certificate comparison option.
c) In the EAP-TLS Session Timeout field, Vocera recommends specifying the duration of a full shift (in minutes). For example, if a shift is 8 hours long, enter 500 (which allows for a 20 minute overlap in shifts).
d) Select an option for setting user identify. Vocera recommends Use CN as Identity, which uses the Certificate Name as the username to search for in the database.
e) Click Submit.

Adding a User for EAP-TLS Authentication

Whatever option you selected for setting user identify (outer identify, CN, or SAN), that's the user name you need to add to the authentication server. If you are using Vocera Manufacturer Certificates, the CN value is Vocera Manufacturer Certificate Client. This is the user name you must add to the ACS database.

1. In the ACS web interface, choose User Setup.
2. Type a username in the User field, and then click Add/Edit.

Setting Up Access Points on the ACS

1. In the ACS web interface, choose System Configuration > Network Configuration.
2. Click Add Entry to add an AAA client.

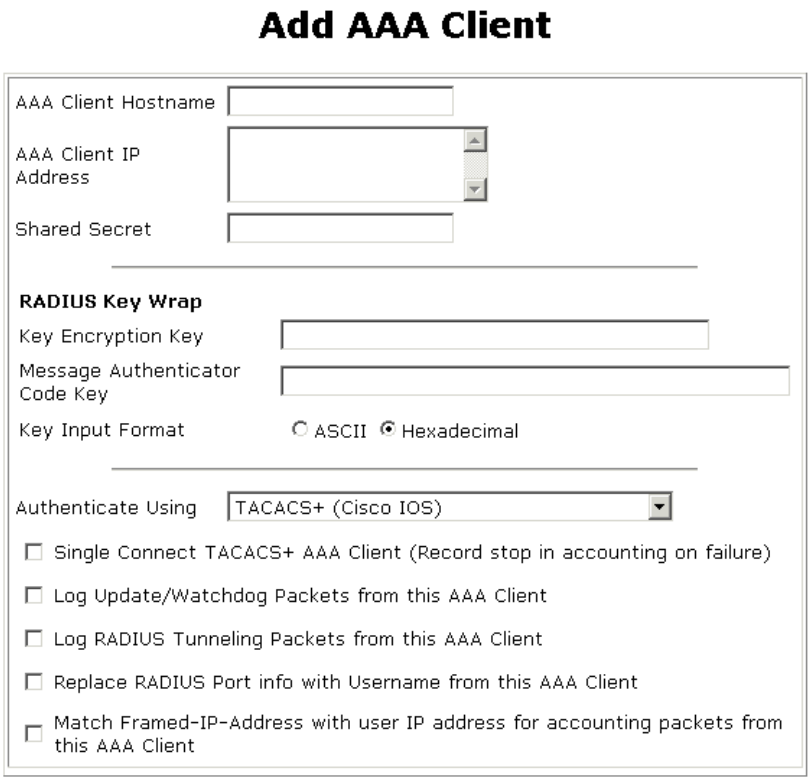


Figure 9: AAA Client settings

3. Specify the following values:
   - AAA Client IP Address: The IP address of your AP
   - Shared Secret: Enter the AP shared secret key
   - Authenticate Using: Select the type of security control protocol that's appropriate for your AP model
4. Click Submit.

Restarting Cisco ACS

1. In the ACS web interface, choose System Configuration > Service Control.
2. Click Restart.

Configuring EAP-FAST Authentication

The EAP-FAST protocol, supported by B3000n and B3000 badges, is a client-server security architecture that encrypts EAP transactions with a TLS tunnel. The tunnel is established based on shared secrets called Protected Access Credentials (PACs) instead of public key certificates.

To implement EAP-FAST, you can choose from two types of PAC provisioning:

- Automatic PAC provisioning – Badges automatically download a PAC from the Cisco ACS, and the ACS periodically refreshes the PAC to make sure it does not expire. To take advantage of automatic PAC provisioning, you must configure badges correctly by setting Auto-PAC properties. For details, see the *Vocera Badge Configuration Guide*. With automatic PAC provisioning, you do not need to copy a PAC to the Vocera Server and you do not need to worry about the PAC expiring.
- Manual PAC provisioning – Badges uses a PAC that is created on the Cisco ACS and then manually copied to the Vocera Server. Generally, the PAC should be set to expire a year or more later so that you do not need to frequently update it. The badge downloads this PAC from the Vocera Server and then exchanges it with an access point that is enabled to support EAP-FAST.

  Note: EAP-FAST has been tested with Cisco Secure ACS v4.0(1) Build 27.

Each badge must use the same user name and password for EAP-FAST authentication (this is also true for LEAP and WPA-PEAP authentication).

Use the following steps to implement EAP-FAST authentication:

1. On the Cisco Secure ACS, login and choose System Configuration > Global Authentication Setup.
2. Under PEAP settings, make sure the Enable Fast Reconnect option is checked.
3. Click EAP-FAST Configuration.
4. Make sure the Allow EAP-FAST option is checked.
5. Enter the following property values:
   - Active Master Key TTL – amount of time that a master key is used to generate new PACs.
   - Retired Master Key TTL – amount of time that PACs generated using a retired master key are acceptable for EAP-FAST authentication.
   - Tunnel PAC TTL – amount of time that a PAC is used before it expires and must be replaced.

     Note: If you are using manual PAC provisioning, set this property value to 5 years to ensure that the PAC file you create for Vocera will not expire soon.
6. Make sure the Allow Stateless Session Resume option is checked, and set Authorization PAC TTL to 8 hours, or the length of a typical shift. This ensures that a session will not trigger a full authentication over the duration of a typical shift.
7. Click Submit.
8. On the Cisco Secure ACS, create a single user that all Vocera badges will use.
9. If you are using manual PAC provisioning, follow these steps:
   a) On the computer running Cisco Secure ACS, open an MS DOS command prompt window and change to the directory containing the CSUtil file.
   b) Start CSUtil with following arguments: `CSUtil.exe -t -u username -passwd password -filepath C:\ClientPACs`

      Where username and password are the user account and password set up for Vocera.

c) Press Enter.
The CSUtil application creates a PAC called `username.pac` in the directory `C:\ClientPACs`.

d) Rename this file to `eapfast.pac`.

e) Copy `eapfast.pac` to the following locations on both the Vocera Server and the stand-alone configuration computer:

`\vocera\config\gen2\badge\res\certificates\EAP-Fast\ \vocera\config\gen3\badge\res\certificates\EAP-Fast\`

Note: The folder name is case-sensitive.

10. On the Vocera Server, start the Badge Properties Editor as described in Using the Badge Properties Editor in the Vocera Badge Configuration Guide.
11. In the Badge Type list, select "B3000N".
12. Click the Security tab, and supply the following property values:
    - Set **Authentication** to **EAP-FAST**.
    - Set **Encryption** to either **TKIP-WPA** or **AES-CCMP**.
    - Set **User Name** to *username*.

      Where *username* is an ACS user ID.
    - Set **Password** to *password*.

      Where *password* is the password of the ACS user.
13. Click Apply to save these values.
14. In the Badge Type list, select "B3000".
15. On the General tab and the Security tab, specify the same property settings for B3000 that you specified for B3000n.
16. Click OK to save these values and close the Badge Properties Editor.
17. Copy `badge.properties` to the following location on both the Vocera Server and the stand-alone configuration computer:

    `\vocera\config`
18. Do either of the following:
    - Stop the Vocera Server and restart it.

      This causes the server to reload `badge.properties` into memory. When the server restarts, it updates the badges with `badge.properties` and retrieves the PAC file, allowing the badge to be authenticated during boot-up and roaming.
    - Run the Badge Configuration Utility.

      When the badge connects, the Badge Configuration Utility updates it with `badge.properties` and the badge retrieves the PAC file, allowing the badge to be authenticated during boot-up and roaming.

Important: If you use manual PAC provisioning, the `eapfast.pac` file must be in place before the badges download the `badge.properties` file with EAP-FAST security enabled.

Increasing the EAP Request Timeout for Automatic PAC Provisioning

If you use automatic PAC provisioning, badges automatically download a PAC from the Cisco ACS, and the ACS periodically refreshes the PAC to make sure it does not expire. When the badge retrieves the PAC for the first time, the provisioning stage takes up to 10 seconds. This delay should occur only once in the lifetime of a regularly used badge.

Because of this initial delay in PAC provisioning, you MUST increase the EAP Request Timeout to 15 seconds on the wireless access points. For Cisco CAPWAP access points, use the following Cisco WLC Command Line Interface (CLI) commands to configure the EAP Request Timeout on Cisco controllers. (The setting is not available in the Cisco WCS or Cisco WLC Web User Interface.)

```
controller> configure advanced eap request-timeout 15
controller> save config
controller> show advanced eap
```

Important: If you do not set the EAP Request Timeout to 15 seconds on your access points, automatic PAC provisioning will not work. Either the ACS or the badge will send an error during PAC provisioning.

Generating a New PAC when User Credentials Change

A PAC file contains credentials directly tied to the username and password. If the username or password values change, the PAC file is no longer valid and a new one must be generated. With manual PAC provisioning, this means you must generate a new PAC file on the Cisco ACS and then copy it to the Vocera Server and the Vocera configuration computer. With automatic PAC provisioning, you must restore the factory settings on the badge and then reconfigure it; see Vocera Badge Configuration Guide. When the badge reconnects, it retrieves the new PAC file automatically from the ACS.

Replacing a PAC File Before it Expires

If you use manual PAC provisioning, you must avoid allowing the PAC file to expire. When you create a PAC file on the Cisco ACS, it has an expiration date determined by the Tunnel PAC TTL property. Best practice is to set the Tunnel PAC TTL property to 5 years or more so you do not have to replace the file frequently. If you choose to set Tunnel PAC TTL to a shorter duration (for example, 1 year), make sure you replace the PAC file on the Vocera Server *before* it expires.

Important: If badges are connected to the Vocera Server when a PAC file expires, they will not be able to authenticate and therefore cannot download an updated PAC file from the server. If that happens, you need to reconfigure any badges that were connected to the Vocera Server when the PAC file expired.

If you use automatic PAC provisioning, there is no need to replace a PAC file on the Vocera Server. The PAC is automatically provisioned by the ACS.

Configuring Microsoft IAS for WPA-PEAP

This section provides high-level instructions for how to configure Microsoft Internet Authentication Service (IAS) for WPA-PEAP authentication.

Configuration Overview

This section provides an overview of the steps needed to configure Microsoft IAS for WPA-PEAP.

1. Do a "Windows update" to ensure you have all the latest Windows service packs.
2. If you are configuring your wireless network for WPA-PEAP and plan to enable Federal Information Processing Standard (FIPS) 140-2 support for Vocera B2000 badges, you will need to download and install a Microsoft update for your IAS server. This update adds support for additional AES cipher suites in the `Schannel.dll` module.

   For details, see **http://support.microsoft.com/kb/948963**.
3. Promote the server to be a Domain Controller (using the DOS command `dcpromo`).
4. Install Microsoft Certificate Server. WPA-PEAP can only be used with certificates.

   Installing a New Cisco ACS Certificate on page 36.
5. Install a self-signed certificate (Optional).

Installing A Self-Signed Certificate (Optional) on page 42.

6. Install IAS on your Windows server.

Installing Microsoft IAS on your Windows server on page 43.

7. Create a “Wireless Users” security group in Active Directory.

Creating "Wireless Users" in Active Directory on page 43.

8. Create a “Wireless Access” policy in IAS.

Creating a Wireless Access Policy in IAS on page 43.

9. Add your Access Points as “RADIUS clients” in IAS.

Adding your Access Points as RADIUS Clients in IAS on page 44.

10. Configure your badge for WPA-PEAP.

Configuring Your Badge For WPA-PEAP on page 44.

11. Configuring a Cisco Wireless LAN Controller (WLC) for WPA-PEAP and IAS.

Configuring a Cisco Wireless LAN Controller (WLC) for WPA-PEAP and IAS on page 44.

Installing Microsoft Certificate Server

1. From the Control Panel, choose Add or Remove Programs.
2. Select Add/Remove Windows Components.
3. Make sure the "Certificate Services" component is checked, and click Next.
4. Select “Enterprise root CA,” and click Next.
5. Enter the name for your CA, and click Next.
6. For “Certificate Database Settings,” accept the defaults and click Next.
7. IIS is not required unless you intend to use Web Enrollment.
8. Click Finish and reboot the computer.

Installing A Self-Signed Certificate (Optional)

This section is optional and only applies if you have not purchased and installed a certificate from valid certification authority (CA) (for example, VeriSign). There are several types of self-signed certificates. See your network administrator for the type of certificate that is appropriate for your network and security requirements. This task describes how to install a self-signed “Computer” certificate.

1. Choose Start > All Programs > Administrative Tools > Certification Authority.
2. Under Certification Authority (Local), expand the name of your CA.
3. have been issued. If not, you can install a self-signed certificate by following the remaining steps. See your network administrator for the appropriate type of certificate to be installed.
4. To install a self-signed certificate, choose Start > All Programs > Administrative Tools > Certification Authority.
5. Right-click “Certificate Templates” and choose Manage.
6. Double-click the “Computer” template, and select the Security tab.
7. For “Permissions for Authenticated Users,” under “Allow” check the Enroll box.
8. Click OK to save and close “Certificate Templates”.
9. Choose Start > All Programs > Administrative Tools > Active Directory Users and Computers.
10. Right-click the appropriate domain name and choose Properties.
11. Select the Group Policy tab.
12. Select Default Domain Policy, and choose Edit.
13. Double-click Computer Configuration.

14. Double-click Windows Settings.
15. Double-click Security Settings.
16. Double-click Public Key Policies.
17. Right-click Automatic Certificate Request Settings, and choose New > Automatic Certificate Request.
18. Click Next.
19. Select Computer, click Next, and then click Finish.
20. Reboot the computer.
21. A self-signed certificate is now installed and you can verify by repeating steps 1 to 3.

Installing Microsoft IAS on your Windows server

1. From the Control Panel, choose Add or Remove Programs.
2. Click Add/Remove Windows Components.
3. Check the Networking Services box and click Details.
4. Check the Internet Authentication Service box, if it is not already checked.
5. Follow the wizard.
6. Choose Start > All Programs > Administrative Tools > Internet Authentication Service.
7. Right-click Internet Authentication Service (Local) and choose Register in Active Directory.

Creating "Wireless Users" in Active Directory

1. Choose Start > All Programs > Administrative Tools > Active Directory Users and Computers.
2. Expand your domain for the IAS and select the Users folder.
3. Right-click Users, and choose New > User.
4. Enter user details and the logon name, and click Next.
5. Enter the password.
6. Uncheck the User must change password at next logon box and check the Password Never Expires box.
7. Click Next, and then click Finish.
8. Right-click the new user, and choose Properties.
9. Click the Dial-in tab.
10. For Remote Access Permission, choose “Allow Access”.
11. Click OK.

Creating a Wireless Access Policy in IAS

1. Choose Start > All Programs > Administrative Tools > Internet Authentication Service.
2. Right-click Remote Access Policies, and choose New > Remote Access Policy.
3. Click Next.
4. Select Use the wizard to setup a typical policy for a common scenario.
5. Enter your policy name.
6. Click Next.
7. For Select the method of access for which you want to create a policy, select “Wireless” and click Next.
8. For Grant access based on the following, select "User", and then click Next.
9. For Select the EAP type for this policy, select “Protected EAP (PEAP)” and click Configure.
10. For Certificate issued, select the IAS computer and domain name.
11. Check Enable Fast Reconnect.
12. For EAP types, select “Secured password (EAP-MSCHAP v2)” and click Edit.

13. Set Number of authentication retries to “99” and click OK.
14. Click OK, click Next, and then click Finish.
15. Double-click the remote access policy you created. It should be the first in the list.
16. Click Edit Profile, and click the Advanced tab.
17. Add the following attributes:
    - Framed-MTU (Vendor RADIUS Standard) with value “1024”
    - Termination-Action (Vendor RADIUS Standard) with value “RADIUS-Request”
18. Click OK.
19. For If a connection request matches the specified conditions, choose “Grant remote access permission”.
20. Click OK.

    Note: All “Connection Request Processing” will be based on the default “Use Windows authentication for all users” policy. You can view this policy under Connection Request Processing > Connection Request Policies.

Adding your Access Points as RADIUS Clients in IAS

1. Choose Start > All Programs > Administrative Tools > Internet Authentication Service.
2. Right-click RADIUS Clients, and choose New RADIUS Client.
3. Type a name and the IP address of your access point, and click Next.
4. Select RADIUS Standard for most access points or set Client-Vendor as appropriate.
5. Type in a "Shared secret" (password) to be used between the RADIUS server and the access point. Note this down, because you will have to configure this on the access point as well.
6. Click Finish.

Configuring Your Badge For WPA-PEAP

Make sure your badge is logged in to the Vocera Server before changing the settings. Update the badge first with your existing settings then update the access point with WPA-PEAP settings.

1. Start the Badge Properties Editor.
2. For Badge Type, select "B3000n".
3. On the General tab, enter the SSID that will be used for WPA-PEAP.
4. Enter the Vocera Server IP Address.
5. Click the Security tab.
6. For Authentication, select “WPA-PEAP”.
7. Enter User Name and Password that you created in Active Directory. The user name should include the domain, for example, “mydomain\vocera”.
8. Click Apply.
9. For Badge Type, select "B3000".
10. On the General tab and the Security tab, specify the same property settings for B3000 that you specified for B3000n.
11. Click OK.
12. Stop and Start the Vocera Server for these properties to take affect.

Configuring a Cisco Wireless LAN Controller (WLC) for WPA-PEAP and IAS

Use the following steps to configure a Cisco WLC for WPA-PEAP and IAS.

1. Set up IAS security details:
   a) On the Cisco WLC home page, select Security.
   b) Under AAA, select “RADIUS Authentication”.

c) For RADIUS Authentication Servers, click New.
d) In the Server IP Address field, enter the IP Address of your IAS server.
e) For Shared Secret Format, select “ASCII”.
f) Enter your Shared Secret as an ASCII string. This shared secret must be the same as the one entered in the IAS RADIUS Clients when setting up Cisco WLC as a RADIUS Client in IAS.
g) For Port Number, accept the default of “1812”.
h) Set Server Status to “Enabled”.
i) Accept defaults for the remaining settings, and then click Apply.
j) To confirm that the Cisco WLC can reach the IAS server, under AAA select “RADIUS Authentication”. For the entry of your IAS server, click Ping.

2. Set up the SSID details:
   a) On the Cisco WLC home page, select WLANS.
   b) For WLANS, click New.
   c) For WLAN SSID, enter your SSID.
   d) Accept defaults for the remaining settings, and then click Apply.
   e) For the SSID you entered, click Edit.
   f) For Radio Policy, select "802.11 b/g only".
   g) For Admin Status, check Enabled.
   h) For Session Timeout (Secs), set the value to 0 (meaning no session timeout). Cisco WLC does not support RADIUS-set session timeouts.
   i) For Quality Of Service (QoS), select “Platinum (Voice)”.
   j) For Client Exclusion, uncheck Enabled.
   k) For DHCP Server, check Override and then enter the IP address of your DHCP server.
   l) For Layer 2 Security, select “WPA”.
   m) Accept defaults for the remaining settings, and click Apply.
3. Setting Cisco WLC general settings
   a) For Cisco WLC switch general settings, make sure the following settings have been made:
      - AP Multicast Mode Support is “Enabled”
      - Load Balancing is “Disabled”
      - Band Select is “Disabled”
      - P2P Blocking Action is “Disabled”
      - Over The Air Provisioning of AP is “Disabled”
      - Client Load Balancing is “Disabled”

Wired Infrastructure Configuration

Although Vocera runs on a wireless 802.11b/g network, the implementation of your wired infrastructure affects its performance. This chapter discusses the wired infrastructure topics you must consider when deploying the Vocera system.

Network Topology

A virtual local area network (VLAN) is an independent logical network within a physical network that is determined by software configuration rather than by physical connections between devices. It allows computers and other clients to behave as if they are connected to the same wire, regardless of where they are actually attached to the LAN.

Vocera does not require any specific network topology; you have the flexibility to deploy it in a variety of different ways to support your own requirements. You can isolate the system on its own VLAN or distribute different parts of the system across several VLAN segments.

Vocera is often deployed into network environments such as the following:

- A network with a wired VLAN and a wireless VLAN.
- A network with a wired VLAN, a wireless data VLAN, and a wireless voice VLAN.
- A network with a dedicated Vocera VLAN in combination with one or more other VLANs.

The actual network topology may be much more complex than this, with numerous segments for various reasons.

Vocera is often fully or partially isolated on its own VLAN. Some reasons for deploying Vocera onto a separate VLAN include:

- Security. The Vocera VLAN may have different security requirements than the data VLAN.
- Minimizing broadcast domains. A separate Vocera VLAN can prevent Vocera broadcasts from causing unnecessary traffic in other segments of the network.
- Ease of management. Isolated network traffic is easier to manage in general.

The following sections discuss several deployment topologies. These sections are intended only to give you ideas about different ways to deploy Vocera. Your specific network topology may be different than any of the ones presented here.

Dual-NIC Server

In the Dual-NIC server topology, the Vocera server contains two network interface cards (NICs): one card gives the server an address on an isolated Vocera VLAN, and the other card gives the server an address on the corporate LAN. This topology often provides the best of both worlds: for the purposes of security, the Vocera voice VLAN is isolated from the other corporate assets, but for the purposes of badge configuration, the Vocera server resides on the same VLAN as the badges.

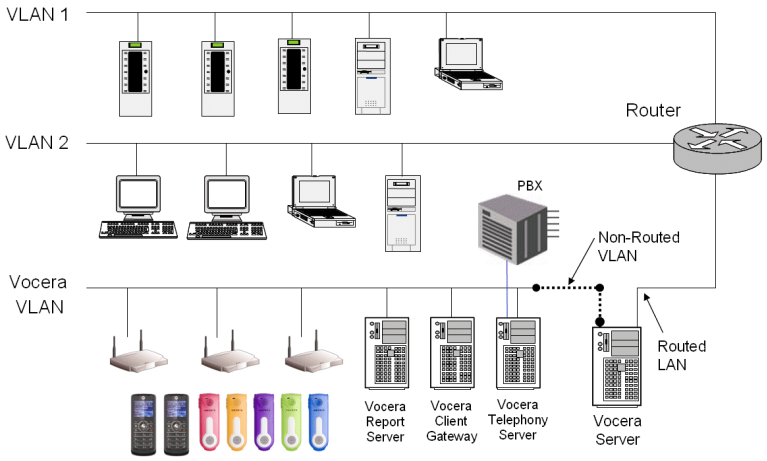


Figure 10: Dual-NIC server topology

Note: Dual-NICs are often used for load balancing, but in this topology they are used to provide different benefits. Do not confuse the topology described in this section with the load-balancing usage.

The major limitation of this topology is that you do not have access to all the features of the Administration Console through an HTTP connection from the corporate LAN. A few administrative tasks require the use of the Tomcat applet, which cannot bind to the NIC on the corporate network. You can work around this limitation in any of the following ways:

- Use Microsoft Terminal Services and the Remote Desktop Connection to gain full access to the Vocera server machine, instead of relying on HTTP access to the Administration Console.
- Perform Administration Console tasks locally on the Vocera server machine or through another machine on the Vocera VLAN.
- Do not perform any task that requires the Tomcat applet by remote HTTP access. These tasks include transferring site data and maintenance functions such as backup, restore, import, export, and so on.

Note: This limitation does not affect the User Console, which does not require the Tomcat applet for any task.

The following table summarizes the advantages and disadvantages of this topology:

Table 14: Dual-NIC server topology

Advantages	Disadvantages
• Common server configuration. • Allows isolation of voice VLAN from other network assets.	• Less convenient access to Vocera Administration Console.

Firewalled Vocera Server

In a firewalled Vocera server topology, the Vocera devices are set up on a voice VLAN, and the Vocera server is set up behind a firewall for security reasons. Alternatively, routers can be be configured to act as rudimentary firewalls by using Access Control Lists (ACLs) to control access to the servers.

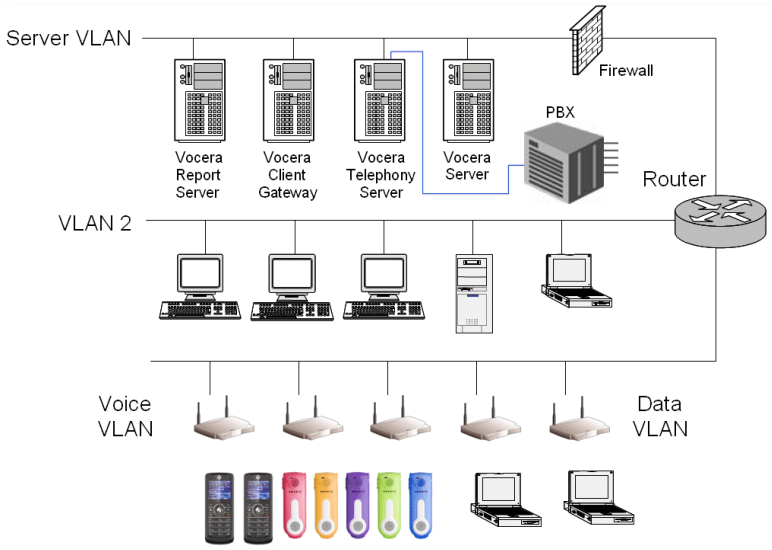


Figure 11: Firewalled Vocera server topology

You must open up ports in the firewall to allow access to the Administration and User Consoles. Otherwise, you can access them only from the Vocera server machine. Opening up ports in the firewall partially offsets the security benefits of this topology. For a list of Vocera IP ports, see **IP Port Usage** on page 87.

Another consideration is that the voice VLAN is accessible to the rest of the network. If your router supports some form of access control, you can restrict the number of users who have direct access to this VLAN.

The following table summarizes the advantages and disadvantages of this topology:

Table 15: Secure, routable Vocera server topology

Advantages	Disadvantages
• Provides security for Vocera servers and data.	• Requires you to open ports in the firewall for Administrator and User Consoles. • Voice VLAN accessible from everywhere unless you implement access control at the router.

Isolated Connection for PBX

To isolate the PBX from the Vocera Voice Server, make sure the VSTG machine has two Network Interface Cards (NICs). Configure the first card with an IP address on the Vocera Voice Server VLAN to allow communication between the Voice Server and the VSTG. Configure the second card with an IP address on the PBX VLAN to enable communication between the SIP trunk and the PBX.

Multiple Vocera Subnets

Vocera devices are often deployed on a single IP subnet. In some situations, however, you may want to enable Vocera devices to work on more than one subnet. For example, you may want to set up several Vocera subnets if your deployment spans more than one building in a campus environment or physically separate geographical sites.

If your Vocera system runs on multiple subnets, make sure you configure the following badge properties correctly:

Table 16: Badge properties for multiple subnets

Property	Recommendation
Broadcast Uses IGMP	Make sure the Broadcast Uses IGMP property is set to TRUE for all badges. This property ensures that multicast features (broadcasts and push-to-talk conferences) work across subnet boundaries. See **Layer 2 IGMP Snooping** on page 53.
Subnet Roaming	If badges need to request a new IP address when they roam to a new floor, building, or campus, make sure the Subnet Roaming property is set to TRUE for all badges. If IP mobility is enabled in your infrastructure and badges can maintain the same IP address while roaming across subnet boundaries, make sure the Subnet Roaming property is set to FALSE for all badges. For details about badge properties, see the *Vocera Badge Configuration Guide*.

Multicast Traffic

Multicasting is a method of sending messages or data to many clients at the same time using IP multicast group addresses. Multicasting is more efficient than unicasting. A device can send one multicast packet to many receivers instead of sending one copy of the unicast packet to each receiver. Vocera uses multicast transmissions to provide broadcasts and push-to-talk conferences. Vocera multicast features can be configured to cross subnet boundaries.

Vocera broadcast and instant conference (push-to-talk) features normally use multicast to forward IP datagrams to a multicast group within a single subnet. If your network uses Internet Group Management Protocol (IGMP) to manage multicast traffic between IP hosts across an IP subnet boundary, you may configure all badges to support IGMP broadcasts.

Important: Vocera devices support IGMPv2. Make sure you enable IGMPv2 on all intermediate routers or other Layer 3 network devices on each subnet used by Vocera devices.

Tip: Vocera recommends that you enable IGMP multicast routing on all intermediate routers or other Layer 3 network devices on each subnet used by Vocera devices. You should also make sure that IGMP snooping is enabled for switches and access points on those subnets. Many switches and access points come with IGMP snooping enabled by default. Finally, you should use the Badge Properties Editor to enable the Broadcast Uses IGMP property on all Vocera badges. For more information, see **Layer 3 IGMP** on page 53 and **Layer 2 IGMP Snooping** on page 53.

Multicast and Smartphones

The Vocera Collaboration Suite clients running in iOS and Android devices support multicast transmissions for broadcast and push-to-talk conferences. The Vocera Client Gateway uses IGMPv2 by default for multicast traffic. However, to enable multicast transmissions on the Vocera Client Gateway, you must set the VGWSupportMulticast property to TRUE. Otherwise, Vocera Client Gateway performs multicast to unicast translation for Vocera Collaboration Suite devices. For more information, see the *Vocera Telephony Configuration Guide*.

If you decide to *disable* multicast transmissions on the Vocera Client Gateway, follow these guidelines to ensure that multicast traffic is properly routed from badges and the Vocera Server to the Vocera Client Gateway:

- Enable multicast routing support on the Layer 3 switches that the Vocera Client Gateway subnet crosses. Check the IP multicast settings that you have enabled on the subnet that the badges are using.
- Set the Broadcast Uses IGMP property to TRUE on all badges.
- Make sure that IGMPv2 is enabled on all intermediate routers or other Layer 3 network devices on each subnet used by Vocera devices. See **Layer 3 IGMP** on page 53.

If multicast traffic is not properly routed, smartphone users will not receive audio packets from badge users during broadcasts or instant conferences (push-to-talk sessions).

Use the following steps to test broadcasts on a smartphone:

1. Log into the Administration Console as a Vocera system administrator.
2. Create two test users, `UserOne` and `UserTwo`.
3. Create an administrative group called `Broadcast` if one does not already exist.
4. Grant the Broadcast group the Initiate Broadcasts permission.
5. Create another group called `Test`.
6. Add UserOne and UserTwo to the Broadcast group.
7. Add UserOne and UserTwo to the Test group.
8. Log into a badge as UserOne.
9. Log into a Vocera smartphone as UserTwo.
10. On the badge, press the Call button and say, “Broadcast to Test.” Proceed to say a test broadcast, for example, “Testing 1, 2, 3, 4.”
11. On the receiving end of the broadcast, the smartphone should play a chime and then you should hear the broadcast.

    If you hear the chime but no audio from the broadcast, multicast packets are not being routed properly. Check the IP multicast settings on the Layer 3 switches that the Vocera Client Gateway subnet crosses.
12. Now test a broadcast from a smartphone to a badge.

    On the smartphone, press the Call button and say, “Broadcast to Test.” Proceed to say a test broadcast as you did earlier on the badge.
13. The badge should play a chime and then you should hear the broadcast.

    If you hear the chime but no audio from the broadcast, multicast packets are not being routed properly.

Multicast and Vocera Connect for Cisco

If a Vocera badge sends a broadcast to a group, the Vocera SIP Telephony Gateway will convert the multicast to unicast for any recipients who are using Vocera Connect on the Cisco Unified Wireless IP Phone 7921G, 7925G, and 7926G.

For multicast to be delivered to a Cisco wireless IP phones where the Vocera SIP Telephony Gateway is located on a different subnet from the Vocera badges, you MUST enable multicast routing support on the Layer 3 switches that the Vocera SIP Telephony Gateway subnet crosses. Check the IP multicast settings that you have enabled on the subnet that the badges are using. If multicast traffic is not properly routed, users of Cisco wireless IP phones will not receive audio packets from badge users during broadcasts.

Each unicast transmission sent to a Cisco wireless IP phone for a Vocera broadcast consumes an additional SIP line. The Vocera license does not limit SIP lines used for broadcasts to Cisco wireless IP phones, so you don't need to provision more SIP lines just to support broadcasts.

Note: If you send a broadcast to a group with more than 100 users of Cisco wireless IP phones, the broadcast may be delayed for some users of the Cisco phones.

Multicast and Vocera Messaging Interface Broadcasts

Vocera Messaging Interface (VMI) can be configured to use IP multicast to broadcast one-way, urgent VMI messages from the server to all recipient devices, thus using only one speech port for the broadcast. For details on how to enable VMI broadcasts, see the *Vocera Messaging Interface Guide*.

To support broadcast of one-way, urgent VMI messages, follow these guidelines to ensure that multicast traffic is properly routed from the Vocera Server to Vocera devices:

- Enable multicast routing support on the Layer 3 switches that the Vocera Server subnet crosses. Check the IP multicast settings that you have enabled on the subnet that Vocera devices are using.
- Set the Broadcast Uses IGMP property to TRUE on all Vocera badges.
- Make sure that IGMPv2 is enabled on all intermediate routers or other Layer 3 network devices on each subnet used by Vocera devices. With IGMP enabled, VMI broadcasts can cross subnet boundaries. See **Layer 3 IGMP** on page 53.

If multicast traffic is not properly routed, Vocera users will not receive audio packets during the broadcast of an urgent VMI message.

Use the following steps to test the broadcast of a one-way, urgent VMI message:

1. Enable broadcast of urgent VMI messages by modifying the `properties.txt` file on the Vocera Server. For details, see the *Vocera Messaging Interface Guide*.
2. Log into the Administration Console as a Vocera system administrator.
3. Create a group called `Test`.
4. Create two test users, `UserOne` and `UserTwo`.
5. Add UserOne and UserTwo to the Test group.
6. Log into one badge as UserOne and another badge as UserTwo.
7. Run the `vmitest.exe` sample application that is included with VMI. The application opens in a command prompt window.

   For more details on vmitest, see the *Vocera Messaging Interface Guide*.
8. In the vmitest application, type `o` to open a gateway. Enter the client ID and then the Vocera Server IP address. You should see "Accepted" when the connection is opened.
9. Type `m` to send a message. Enter the following parameter values:

Parameter	Value
Message ID	<any number>
Login ID	`Test`
Message Text	<any message long enough to test the broadcast, such as `Testing 1, 2, 3, 4` repeated several times>
Priority	`urgent`
Call-back Phone No	<Press Space to clear the value, then press Enter>
Response Choices	<Press Space to clear the value, then press Enter>
WAV File Root Names	<Press Space to clear the value, then press Enter>

10. On the receiving end of the broadcast, the badges should play the alert tone for urgent messages (by default, two klunks) and then you should hear the broadcast being played on both badges.

If you hear the alert tone but no audio from the broadcast, multicast packets are not being routed properly. Check the IP multicast settings on the Layer 3 switches that the Vocera Server subnet crosses.

Multicast Address Range

The Class D multicast address range for Vocera starts at 230.230.0.0 and has a range of 4096 addresses. You can configure the multicast address range by adding the following properties to the `\vocera\server\Properties.txt` file on each Vocera Server:

- IPBaseMulticastAddr – specifies the start of the range (the default is 230.230.0.0).
- IPMulticastRange – specifies the number of addresses in the range (the default is 4096).

Note: If you modify the Properties.txt file, you must stop and start the Vocera Server to load the properties into memory.

Layer 3 IGMP

IP networks use IGMP to manage multicast traffic across Layer 3 boundaries. When IGMP is enabled on your network, routers and other network devices use it to determine which hosts in their domain are interested in receiving multicast traffic. Hosts register their membership in multicast groups, routers maintain membership lists for these multicast groups, and then routers make sure that multicast traffic is passed on to the hosts that want to receive it. With IGMP enabled, the multicast features of Vocera—broadcasts and push-to-talk conferences—can cross subnet boundaries.

If IGMP is enabled on your network and you want to be able to broadcast across subnets, you must also set the **Broadcast Uses IGMP** property to TRUE on the badge. Enabling this property allows a badge to register its membership in the appropriate multicast group, so it can receive multicast traffic from other badges, even from another subnet.

For B3000n and B3000 badges, the **Broadcast Uses IGMP** property is enabled by default.

To enable badge multicasts when IGMP is enabled on the network:

- Set the **Broadcast Uses IGMP** property to TRUE on all badges.

  See the *Vocera Badge Configuration Guide* for complete information.

Note: If IGMP is not enabled on your network, Vocera multicasts will occur successfully within a single subnet. However, multicast traffic will not cross subnet boundaries.

Layer 2 IGMP Snooping

IGMP snooping is a method by which Layer 2 devices can listen in on IGMP conversations between hosts and routers and then intelligently forward multicast traffic only to those ports that have joined the multicast group. IGMP snooping can be configured on network switches and access points.

Use the following steps to enable multicast features across subnet boundaries:

1. Enable IGMP snooping for ALL devices (for example, switches and access points) on each subnet used by the badge.
2. Enable IGMP multicast routing on all intermediate routers or other Layer 3 network devices on the Vocera subnets.
3. Set the **Broadcast Uses IGMP** property to TRUE on all badges.

   See the *Vocera Badge Configuration Guide* for complete information.

IP Addressing

As described in **About the Vocera Badge** on page 9, the badges are most easily configured and administered as a group. Consequently, you should use a DHCP server to assign IP addresses to them dynamically.

Make sure you manually specify a default DHCP gateway in the **B3N.GatewayIPAddr** or **B3.GatewayIPAddr** property in the `badge.properties` file (this property is not currently exposed in the Badge Properties Editor. Vocera uses this property for multicast sessions even when badges and the Vocera Voice Server are in the same VLAN.

Avoid assigning static IP addresses because you must configure each badge manually, which is a slow and potentially error-prone process. You should use static IP addresses only in the following situations:

- You are setting up a small evaluation system.
- Static IP addresses are mandatory at your site.

Note: For more information see on page in the Vocera Badge Configuration Guide.

DHCP and Subnet Roaming

If your site is configured for multiple Vocera subnets and IP Mobility is not enabled on the network, a DHCP server must assign a new IP address whenever a badge user roams across subnet boundaries. As described in **Layer 3 Roaming** on page 26 , the latency introduced by acquiring a new IP address can result in dropped packets and audio loss.

If you allow subnet roaming, make sure you use the badge in a live call to test audio loss when crossing subnet boundaries. You may be able to optimize DHCP server settings to minimize latency, depending upon the specific DHCP server you are using at your site.

Large networks often use multiple DHCP servers to establish a redundant method of providing IP addresses in case a single server fails. If two or more DHCP servers are running on a network, they typically employ some form of conflict detection to determine if an IP address is already in use before offering it to a new client. This conflict detection introduces additional latency by increasing the time required for a client to receive an IP address.

If your network *does not* require multiple DHCP servers, make sure the conflict detection mechanism is turned off to minimize latency. For example, if you are using the Microsoft DHCP server, set the **Conflict Detection Attempts** property to 0.

If your network *does* use multiple DHCP servers, experiment with other techniques to minimize latency. For example, consider assigning each DHCP server a pool of addresses that does not overlap with the other servers, so conflict detection can be disabled.

Network Considerations

Your wired network must be able to satisfy the bandwidth and latency requirements of badge-to-badge and badge-to-server communication. If you are planning a centralized deployment across multiple sites, a centralized Vocera server and remote telephony servers, or a cluster with geographically distributed nodes, your WAN circuit must satisfy these requirements throughout your enterprise.

If you are planning to allow Vocera communication over a WAN, keep in mind that authentication can add considerable delays to network traffic.

The bandwidth requirement for your wired infrastructure increases linearly as the number of badges simultaneously transmitting increase. Vocera has calculated the *theoretical* maximum bandwidth requirement for simultaneous badge transmissions as follows. The actual requirement in any given deployment may differ.

Table 17: Maximum bandwidth requirements

Number of Simultaneous Calls or Genie Sessions (Full Duplex)	Maximum Bandwidth Required
50	8 Mbps
100	16 Mbps
150	24 Mbps
350	56 Mbps

In addition, the total one-way latency of the circuit, including all network propagation and serialization delays, must not exceed 150 ms.

Important: Network capacity planning must take into account the duration of Vocera calls, the total number of Vocera devices deployed, the statistical likelihood of simultaneous transmissions, and other usage issues, similar to Erlang calculations prepared for PBXs.

Most Vocera calls typically have a short duration (under 30 seconds). In a deployment with 500 total Vocera devices, the statistical likelihood of all of them being involved in simultaneous device-to-device calls (250 simultaneous transmissions) may be fairly small.

WAN QoS

In a large network, it is often not sufficient to enable QoS only at the access point level—Vocera traffic may pass through distribution switches, core routers, and other devices. You must enable end-to-end QoS so traffic that is prioritized at the access point does not lose its priority as it passes through these other devices.

Some devices, such as core routers, may provide enough bandwidth that traffic prioritization is unnecessary. However, you should enable QoS on any network leg whose throughput is 100 Mbps or less, if it carries Vocera traffic.

Vocera marks the ToS (Type of Service) header in its packets to support routers that use this technology to classify and prioritize traffic. Vocera sets the ToS byte in the following ways:

- With a DSCP (DiffServ Code Point) marking of EF (Expedited Forwarding).
- With an IP Precedence marking of 5.

If your Vocera traffic will traverse a WAN circuit, you should make sure the following QoS requirements are met:

- Enable QoS at all WAN ingress and egress points.
- Make sure the routers that provide WAN circuits give the highest priority to traffic with a DSCP marking of EF or an IP Precedence of 5.

See **Quality of Service** on page 27 for information about enabling QoS on your wireless network.

Hardware Infrastructure

The following topics summarize computer system requirements, deployment scenarios, and equipment preparation for the Vocera system.

System Requirements

For server configuration guidelines, whether you are installing on physical machines or on VMware virtual machines, see the **Vocera Voice Server Sizing Matrix**.

Vocera Server Infrastructure

Vocera Voice Server Requirements

Use a dedicated computer to run the Vocera Voice Server—it should not run any other applications. If the computer has previously run other applications, you should re-install the operating system and its appropriate service packs to ensure you install the Vocera software into a clean environment.

About Vocera Clusters

Some environments require redundancy to support critical applications in the event of hardware or software failure. In such environments, a critical application is installed on two or more computers. The computer controlling the application is called the *active* node, and the other computers are called the *standby* nodes. This redundant combination of active and standby nodes is called a *cluster*.

Vocera clustering provides high availability when any of the following events occur:

- The computer hardware fails.
- The Vocera Voice Server fails.
- The Nuance service fails.
- The MySQL service fails.

The cluster's active node controls the Vocera system, but a standby node can take over control of the application if the active node fails. The situation where a standby node takes control from the active node is called a *failover*.

The telephony integration option (Vocera SIP Telephony Gateway, if installed, should run on a server that is separate from the Vocera cluster so telephony support can continue if the Vocera server fails over. Failover for the telephony server itself is supported as part of the high availability architecture.

The following figure shows the way that the Vocera SIP Telephony Gateway, the Vocera Report Server, and badges connect to a Vocera cluster:

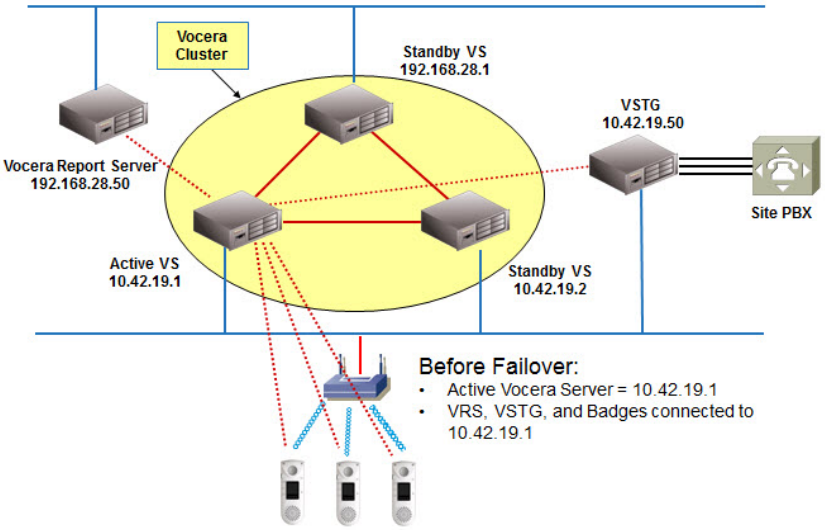


Figure 12: Vocera Cluster Before Failover

As shown in the above illustration, the nodes in a Vocera cluster do not share a single virtual IP address, as they would with the Microsoft Cluster Service. Instead, the badges, the Vocera SIP Telephony Gateway, and the Vocera Report Server are all associated with `10.42.19.1`, the IP address of the *active* Vocera Voice Server. Similarly, any Administration Console or User Console sessions would also point to the IP address of the active Vocera Voice Server.

Vocera supports a maximum of four cluster nodes (one active node and three standby nodes). Each cluster node maintains its own copy of the Vocera database, the Vocera Report Server log files, and the `badge.properties` file. The cluster synchronizes these files continually.

If a failover occurs, one of the standby nodes becomes active and takes control of the cluster. At that time, the badges, the Vocera SIP Telephony Gateway, and the Vocera Report Server automatically associate with the IP address of the newly active node, as shown in the following illustration:

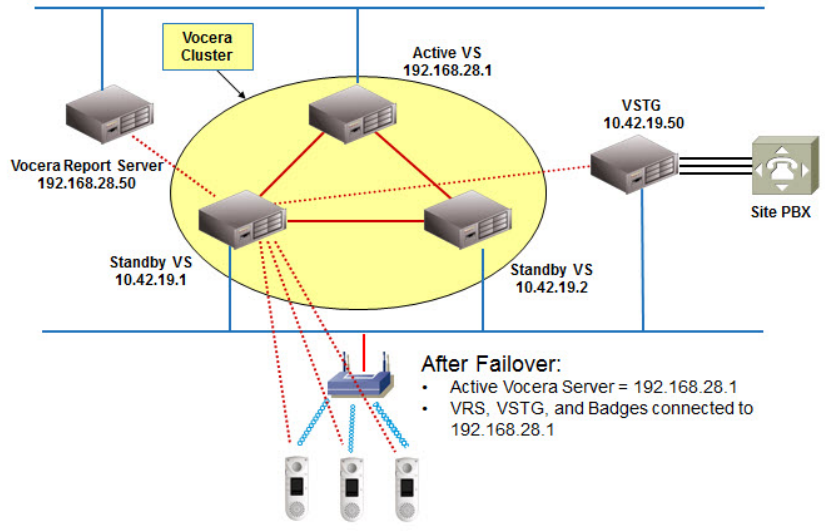


Figure 13: Vocera Cluster After Failover

As shown in the above illustration, Vocera Voice Server nodes, the Vocera SIP Telephony Gateway, and the Vocera Report Server can reside on different subnets. In a Vocera cluster, the Vocera Voice Server and all its related services are always running on any standby nodes so failover can occur quickly. If the active node fails, a standby node becomes active and takes control of the cluster almost immediately.

You can use the Administration Console or the Vocera Control Panel to determine which node of a cluster is active:

- The Vocera Control Panel displays a status message to indicate whether its server is in active or standby mode.

  See "Determining the Status of a Server" in the Vocera Installation Guide for complete information.
- The Address field of your web browser displays the IP address of the active Vocera Voice Server.

Because each node maintains an independent copy of the database, the Vocera cluster architecture allows disaster survival. The use of multiple nodes will also allow rolling upgrades with minimal down-time in the future.

Network Problems and Clustering

Vocera clustering provides a distributed architecture that allows you to locate nodes anywhere on your network, including on different subnets and in different geographic locations. This flexibility is intended in part to provide disaster recovery capabilities from catastrophic events such as an earthquake or a WAN failure.

The flexibility of this distributed cluster architecture requires you to have a stable network environment. In particular, either of the following network problems will cause unwanted cluster behavior:

- Network outages

  For Vocera purposes, any network event that blocks all routes between the active node and a standby node is an outage. For example, restarting a switch may cause an outage.
- Excessive latency

  The standby nodes each poll the active node periodically to draw down synchronization transactions. If the active node fails to service a poll from a standby node **within 10 seconds**, it fails over to one of the standby nodes.

Either of the network problems described above may result in the following cluster behavior:

- Multiple nodes become active as independent servers that are isolated from each other (a *split brain* state).
- Some badges may connect to one active server; other badges may connect to another active server.

For more information about how to troubleshoot network problems and Vocera clusters, see the *Vocera Administration Guide*.

Disk Defragmentation

Vocera recommends that you schedule the Microsoft Disk Defragmenter tool (or a similar tool) to run regularly on your Vocera Server and on all other Vocera servers to maintain disk performance and consolidate free disk space. For more information, see **Disk Defragmenter Technical Reference**.

Configuration Hardware Requirements

The *configuration hardware* is the computer and other equipment that configures Vocera devices. The configuration computer is the computer on which you run the Vocera Badge Configuration Utility (BCU), so it is referred to as the BCU computer.

Vocera requires the following configuration hardware for badges and phones:

Table 18: Configuration hardware requirements

Component	Requirement
Configuration Computer	See the **Vocera Voice Server Sizing Matrix**.
Access Point	An isolated access point that is not connected to the installation site's network.
Cable	An Ethernet crossover cable to connect the configuration computer and the access point.

Vocera SIP Telephony Gateway Infrastructure

Vocera SIP Telephony Gateway Architecture

Vocera SIP Telephony Gateway is a SIP telephony gateway between the Vocera Voice Server and an IP PBX or a VoIP gateway.

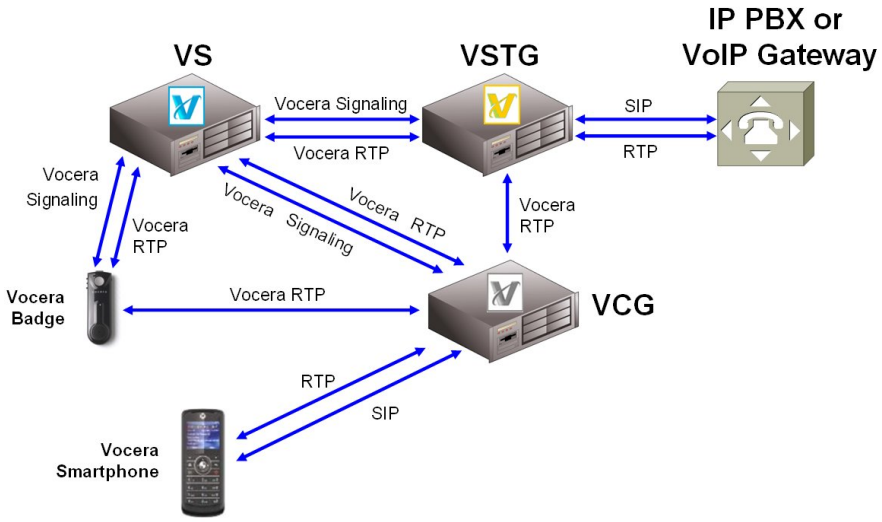


Figure 14: Vocera SIP Telephony Gateway architecture

Session Initiation Protocol Support

Vocera SIP Telephony Gateway is based on Internet Engineering Task Force (IETF) standards for Session Initiation Protocol (SIP) 2.0 and Real Time Transport Protocol (RTP). Vocera SIP Telephony Gateway communicates via a SIP trunk with a SIP-enabled PBX or a SIP Gateway. The Vocera SIP Telephony Gateway provides basic SIP telephony functionality, including placing and receiving calls, OPTIONS keep-alive messages, and obtaining ANI and DNIS information. The Vocera SIP Telephony Gateway is interoperable with SIP-enabled PBXs and SIP Gateways as long as they follow SIP 2.0 and RTP standards.

For audio transport, Vocera SIP Telephony Gateway uses Real-time Transport Protocol (RTP), an Internet protocol standard for delivering multimedia data over unicast or multicast network services (see RFC 35504[5] and RFC 35515[6]).

[5] http://tools.ietf.org/html/rfc3550

Vocera Server uses Vocera's proprietary signaling and transport protocols for all communication between the server and Vocera badges. Consequently, Vocera SIP Telephony Gateway converts from SIP/RTP protocols to Vocera's protocols, and vice versa, to enable communication between the Vocera Server and the IP PBX.

Using the SIP Testing Tool

Before installing Vocera SIP Telephony Gateway, Vocera recommends testing the SIP connection to your PBX using a SIP Testing Tool that it provides. The SIP Testing Tool allows you to test the following SIP functionality:

- Place a SIP test call to the PBX.
- Receive a SIP call from the PBX (requires a SIP handset or soft phone).
- Test whether OPTIONS keep-alive is working.

For more information about the SIP Testing Tool, see KB1086 in the Vocera Technical Support Knowledge Base.

You can download the SIP Testing Tool from the following location:

http://www.vocera.com/ts/VSTG_siptest/siptest.zip

Important: Make sure the Vocera SIP Telephony Gateway is not running on the computer on which you run the SIP Testing Tool.

Vocera SIP Telephony Gateway Requirements

Install the Vocera SIP Telephony Gateway on a dedicated computer. The Vocera SIP Telephony Gateway uses software that might cause conflicts, and it performs resource-intensive tasks that might affect performance of other applications.

The following figure shows a typical Vocera system consisting of Vocera Client Gateway, Vocera Voice Server, and Vocera SIP Telephony Gateway installed on separate computers. Optionally, Vocera Report Server can also be installed on a separate computer.

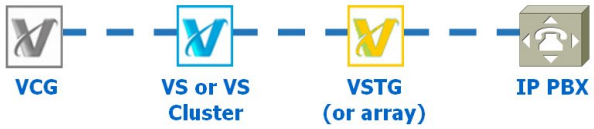


Figure 15: Vocera software installed on separate computers

If your PBX is not SIP-enabled or does not handle all SIP features such as RFC 2833 DTMF relay, you can use a VoIP media gateway (such as Dialogic Media Gateway) to connect to the PBX, as shown in the following figure.

Figure 16: VSTG connecting to PBX through Dialogic Media Gateway

If the computer on which you are installing Vocera SIP Telephony Gateway has previously run other applications, re-install the operating system and apply appropriate service packs to ensure you install the Vocera SIP Telephony Gateway into a clean environment.

[6] http://tools.ietf.org/html/rfc3551

Cisco Unified Communications Manager Support

Vocera has tested Vocera SIP Telephony Gateway with the following versions of Cisco Unified Communications Manager:

- Cisco Unified Communications Manager version 8.5
- Cisco Unified Communications Manager Express (CME) version 7.1

Dialogic Media Gateway Support

Vocera has tested Vocera SIP Telephony Gateway with the following Dialogic Media Gateways:

Table 19: Digital Dialog Media Gateway models

SKU	Digital Gateway Description	Ports
235-02030	Dialogic DMG2030DTIQ – single T1/E1	30

Table 20: Analog Dialog Media Gateway models

SKU	Analog Gateway Description	Ports
235-01004	Dialogic DMG1004LSW – 4 port analog	4
235-01008	Dialogic DMG1008LSW – 8 port analog	8

Telephony SIP Deployment Scenarios

With the high availability features provided for the Vocera SIP Telephony Gateway there are several telephony deployment scenarios to choose from based on whether your enterprise fully takes advantage of these features, and also based on the following factors:

- number of Vocera sites
- number of PBXs at those sites
- mission criticality of the Vocera system
- capital budget limits

Single Site Scenarios

The simplest single site deployment scenario has one Vocera Server connected to one telephony server using one PBX. This scenario does not take advantage of any high availability features, such as redundancy, scalability, and load balancing.

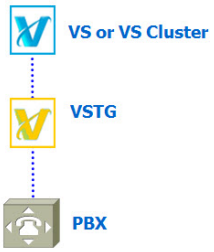


Figure 17: Single Site Scenario with 1 Telephony Server

Summary	
Sites:	1
Telephony Sharing:	No
PBX Failover:	No

Summary	
High Availability:	No

To add high availability to a single site Vocera system, an array of telephony servers can be installed, and two SIP trunks can be used to provide failover support. This scenario provides redundancy, scalability, and load balancing. The Vocera Server handles outbound load balancing by automatically allocating calls to the least busy telephony server. The PBX handles inbound load balancing.

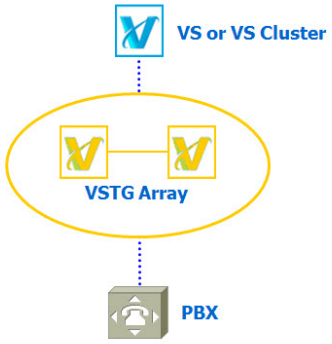


Figure 18: Single Site Scenario with a Telephony Server Array

Summary	
Sites:	1
Telephony Sharing:	No
PBX Failover:	Yes
High Availability:	Yes

Multiple Site Scenarios

With multiple sites, the complexity of telephony deployment scenarios increases due to the following factors:

- Option of installing redundant telephony gateways at each site for high availability
- Option of sharing telephony gateways between sites
- Potentially multiple PBXs

The following scenario shares telephony gateways between sites. In this example, the telephony gateway uses the PBX at site A. The telephony gateway is shared with site B, which may or may not have its own PBX. Because a single telephony gateway instead of an array of telephony gateways is installed at site A, high availability features are not supported.

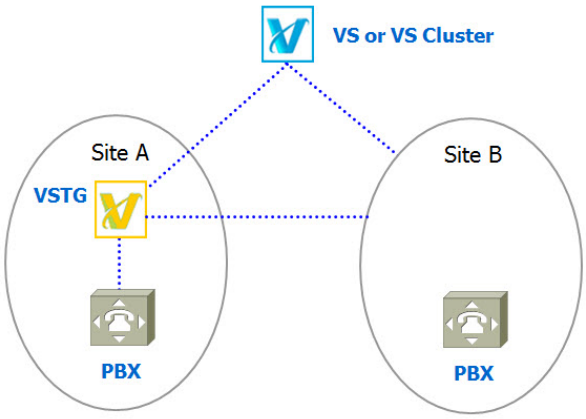


Figure 19: Multiple Site Scenario Using a Shared Telephony Gateway and 1 PBX Per Site

Summary	
Sites:	Multiple
Telephony Sharing:	Yes
PBX Failover:	No
High Availability:	No

The following scenario is a variation of the previous one. An array of telephony gateways has been added, which provides redundancy, scalability, and load balancing.

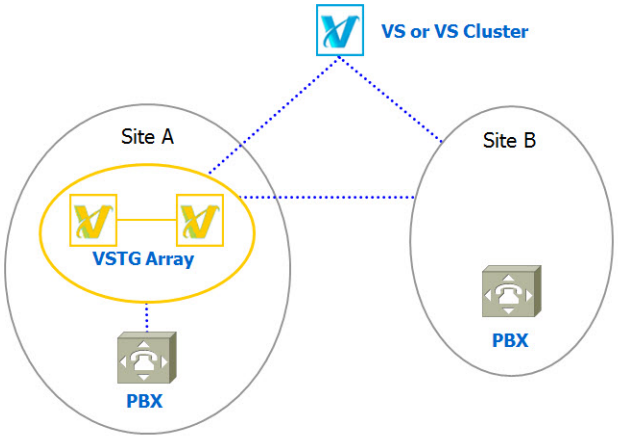


Figure 20: Multiple Site Scenario Using a Shared Telephony Gateway Array and 1 PBX Per Site

Summary	
Sites:	Multiple
Telephony Gateway Sharing:	Yes
PBX Failover:	No
High Availability:	Yes

The following scenario has a telephony gateway and PBX at each site. Using independent telephony gateways instead of sharing a telephony gateway between sites may be needed for performance and scalability. Because a single telephony gateway is installed at each site instead of an array of telephony gateways, high availability features are not supported.

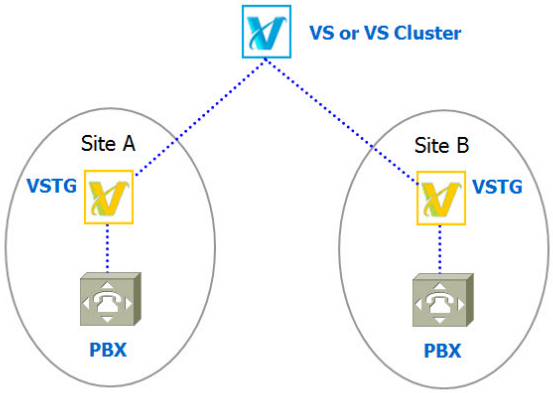


Figure 21: Multiple Site Scenario Using a telephony gateway and PBX at Each Site

Summary	
Sites:	Multiple
Telephony Gateway Sharing:	No
PBX Failover:	No
High Availability:	No

The following multiple site scenario represents the best practice for high availability support. It has an array of telephony gateways and redundant PBXs at each site.

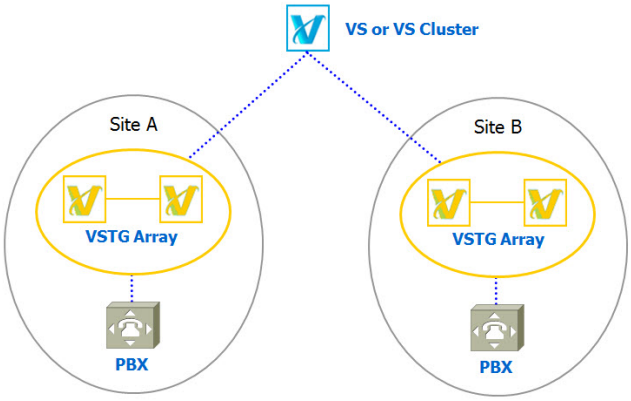


Figure 22: Multiple Site Scenario Using 2 Telephony Gateways and 2 PBXs at Each Site

Summary	
Sites:	Multiple
Telephony Gateway Sharing:	No
PBX Failover:	Yes
High Availability:	Yes

This next scenario is an option for multiple sites where one site uses Vocera as a mission critical application, and the other site does not (perhaps because it is a small test deployment). In this example, an array of telephony gateways and two PBXs are installed at site A but not at site B. Therefore, only site A has high availability features.

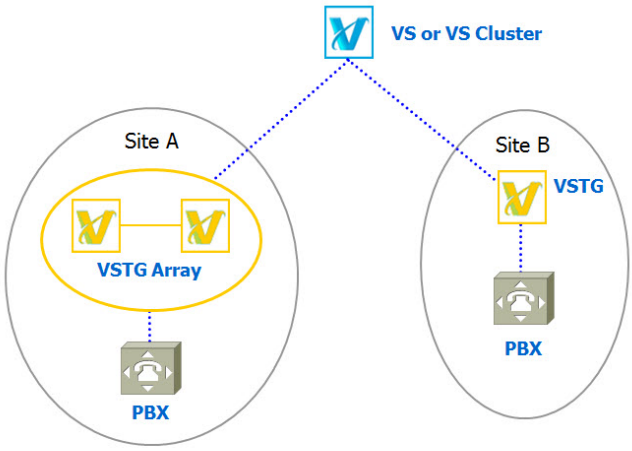


Figure 23: Multiple Site Scenario with a Mission Critical Vocera System at One Site, and a Test System at Another

Summary	
Sites:	Multiple
Telephony Gateway Sharing:	No
PBX Failover:	Yes at Site A, No at Site B
High Availability:	Yes at Site A, No at Site B

Vocera Client Gateway Infrastructure

Vocera Client Gateway Architecture

Vocera Client Gateway supports Vocera smartphones, providing a signaling and multimedia gateway from the phones to the Vocera Voice Server for all calls. Vocera Client Gateway also provides a tunnel for application data between the Vocera smartphone and the Vocera Voice Server. All communication between the Vocera Voice Server and the Vocera smartphone is done through the Vocera Client Gateway.

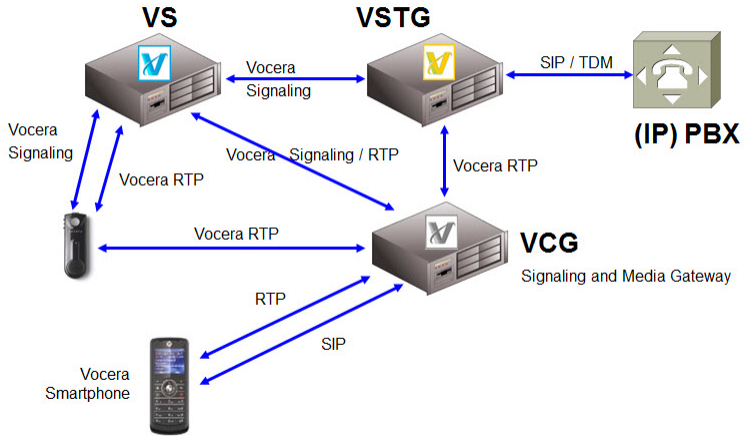


Figure 24: Vocera Client Gateway architecture

Vocera Client Gateway Requirements

Install the Vocera Client Gateway on a dedicated computer. The Vocera Client Gateway uses software that might cause conflicts, and it performs resource-intensive tasks that might affect performance of other applications.

The following figure shows a typical Vocera system consisting of Vocera Client Gateway, Vocera Voice Server, and Vocera SIP Telephony Gateway installed on separate computers. Optionally, Vocera Report Server can also be installed on a separate computer.

Figure 25: Vocera software installed on separate computers

The Vocera Client Gateway must be installed with the same version as the Vocera Voice Server and the Vocera Client Gateway cannot communicate with earlier versions of Vocera Voice Server.

If the computer on which you are installing Vocera Client Gateway has previously run other applications, re-install the operating system and apply appropriate service packs to ensure you install the Vocera Client Gateway into a clean environment.

Vocera Client Gateway Deployment Scenarios

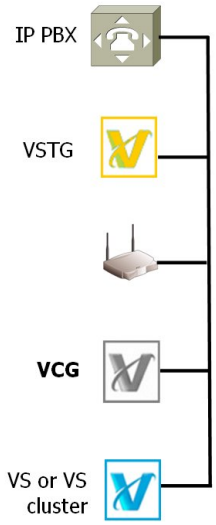
With the high availability features provided for Vocera Client Gateway, there are several deployment scenarios to choose from based on whether your enterprise fully takes advantage of these features, and also based on the following factors:

- number of Vocera sites
- capital budget limits

Single Site Scenarios

The simplest single site deployment scenario has one Vocera Voice Server connected to one VCG. This scenario does not take advantage of any high availability features, such as redundancy and scalability.

Single Site Scenario with 1 VCG



Summary	
Sites:	1
High Availability:	No

To add VCG high availability to a single site Vocera system, an array of VCG servers can be installed. This scenario provides redundancy and scalability.

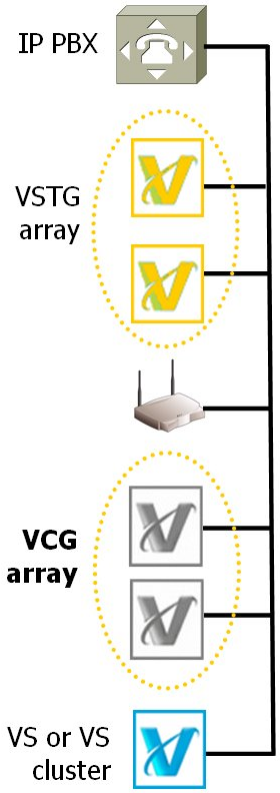


Figure 26: Single Site Scenario with a VCG Array

Summary	
Sites:	1
High Availability:	Yes

Multiple Site Scenarios

If your Vocera system has multiple sites, you can install a VCG at each site, or install multiple VCGs at each site for redundancy. As long as you have multiple VCGs deployed, you can take advantage of high availability features.

The following multiple site scenario shows only one VCG installed at each site. This scenario lacks VCG redundancy unless smartphones are configured to connect to the VCGs at both sites.

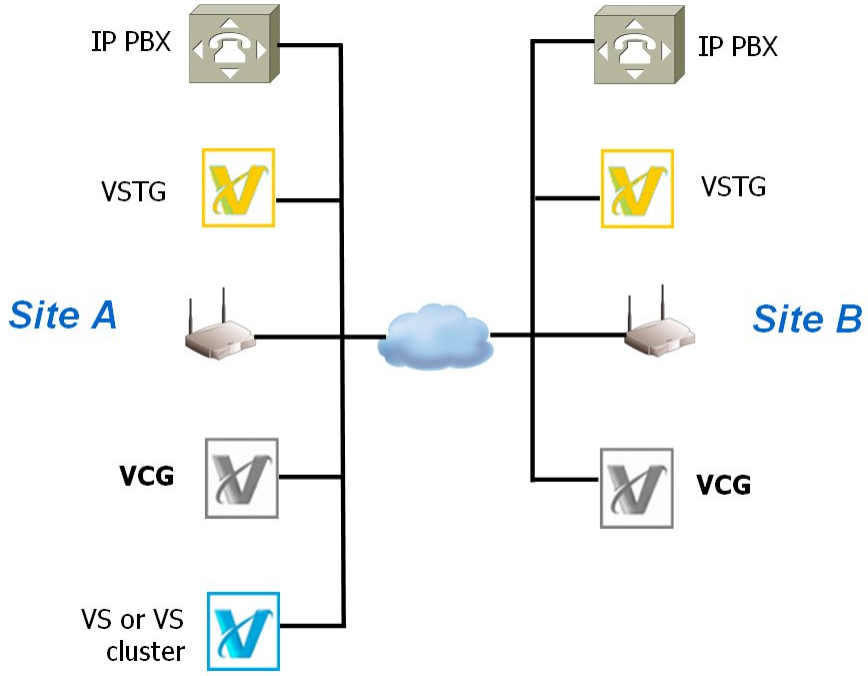


Figure 27: Multiple Site Scenario Using 1 VCG at Each Site

Summary	
Sites:	Multiple
High Availability:	No, unless smartphones are configured to connect to both VCGs across the WAN

The following multiple site scenario represents the best practice for high availability support. It has arrays of VCG servers installed at each site.

Important: You cannot require specific Vocera Collaboration Suite clients to use specific VCG servers. To limit traffic across the WAN, configure firewall rules or ACLs that allow WAN traffic from the Vocera Collaboration Suite clients to the VCG servers but prevent other traffic.

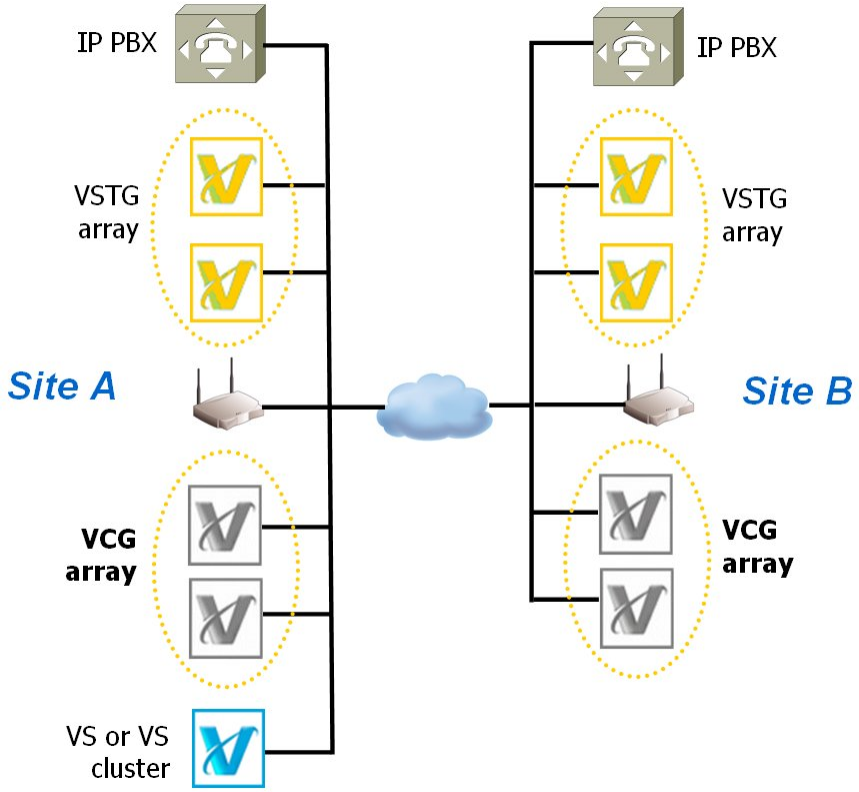


Figure 28: Multiple Site Scenario Using VCG Server Arrays

Summary	
Sites:	Multiple
High Availability:	Yes

Vocera Report Server Infrastructure

Vocera Report Server Limitations

Consider the following limitations when you install Vocera Report Server:

- Do not install more than one copy of the Vocera Report Server on your network.
- Do not install Vocera Report Server on a machine with dual network interface controllers (NICs). Only one NIC is supported.

The Vocera Report Server generates reports from logs and user data acquired from the Vocera Voice Server. The Vocera Report Server cannot communicate with earlier versions of the Vocera Voice Server.

Install the Vocera Report Server on a dedicated computer—it should not run any other applications. The Vocera Report Server uses software that might cause conflicts, and it performs resource-intensive tasks that might affect performance of other applications.

If the computer has previously run other applications, re-install the operating system and apply appropriate service packs to ensure you install the Vocera Report Server into a clean environment.

Appendixes

Find additional information about badge and network configuration.

Wireless Troubleshooting Tools

Learn about recommended WLAN tools that are useful for troubleshooting and diagnosing wireless problems.

Spectrum Analyzers

An RF spectrum analyzer lets you visualize spectrum utilization and find sources of RF interference that affect the Wi-Fi network.

- **Cisco Spectrum Expert**

  http://www.cisco.com/en/US/products/ps9393/index.html
- **Fluke Networks Airmagnet Spectrum XT**

  http://www.flukenetworks.com/enterprise-network/wireless-network/airmagnet-spectrum-xt
- **Wildpackets OmniPeek Network Analyzer**

  http://www.wildpackets.com/products/distributed_network_analysis/omnipeek_network_analyzer

WLAN Packet Capturing Tools

A WLAN packet capture tool, also called a wireless sniffer, can capture and analyze 802.11 traffic and decode TCP/IP and application protocols. These tools allow you to use filters to focus the capture. The captured traffic can usually be viewed in real-time, recorded to a capture buffer, or saved to a file.

- **Fluke Networks AirMagnet WiFi Analyzer**

  http://www.flukenetworks.com/enterprise-network/wireless-network/AirMagnet-WiFi-Analyzer
- **Wireshark**

  http://www.wireshark.org/
- **Riverbed AirPcap Adapter for Microsoft Windows**

  http://www.riverbed.com/products-solutions/products/network-performance-management/wireshark-enhancement-products/Wireless-Traffic-Packet-Capture.html
- **Wildpackets OmniWiFi WLAN Capture Adapter**

  http://www.wildpackets.com/products/omniwifi_adapter

WLAN Monitoring Tools

WLAN monitoring tools can help WLAN administrators detect security vulnerabilities and active attacks, monitor performance and pin-point potential problems, and evaluate network and application usage.

- **Fluke Networks AirMagnet Enterprise**

http://www.flukenetworks.com/enterprise-network/wireless-network/AirMagnet-Enterprise

- **Network Instruments Observer**

  http://www.networkinstruments.com/products/observer/index.php

- **WildPackets OmniPeek Network Analyzer**

  http://www.wildpackets.com/products/distributed_network_analysis/omnipeek_network_analyzer

VOIP Monitoring Tools

VOIP monitoring tools collect, monitor and analyze signaling, voice, and data traffic performance. They can decode calls, and provide VOIP metrics such as packet loss, latency, and voice quality.

- **Fluke Networks AirMagnet VoFi Analyzer**

  http://www.flukenetworks.com/enterprise-network/wireless-network/AirMagnet-VoFi-Analyzer

- **Network Instruments Observer**

  http://www.networkinstruments.com/products/observer/index.php

Site Survey Tools

Site survey tools help you plan wireless access point locations for adequate coverage and allow you to see how an AP will transmit its signals throughout a building.

- **Fluke Networks AirMagnet Survey**

  http://www.flukenetworks.com/enterprise-network/wireless-network/AirMagnet-Survey

- **Ekahau Site Survey**

  http://www.ekahau.com/wifidesign/ekahau-site-survey

- **VisiWave Site Survey**

  http://www.visiwave.com/index.php/ScrInfoProducts.html

Best Practices for Cisco Unified Wireless Networks (CAPWAP)

This appendix provides best practices for configuring Cisco Unified Wireless Networks for a Vocera VLAN. It only addresses configuration parameters that are particular to a Vocera deployment in a CAPWAP architecture. For complete information about the Cisco Wireless Control System (WCS), Cisco Prime, or the Cisco Wireless LAN Controller (WLC), refer to the Cisco Systems documentation.

Related Cisco Systems Documentation

On the Cisco Systems web site (http://www.cisco.com), the following documents provide information about configuring Cisco Unified Wireless Networks:

- **Vocera IP Phone Deployment in Cisco Unified Wireless Network Infrastructure**

  Describes how to configure Cisco CAPWAP access points for a Vocera architecture.
- **Radio Resource Management under Unified Wireless Networks**

  Describes the functionality and operation of Radio Resource Management (RRM) features.

Configuring Cisco CAPWAP Access Points

Cisco Wireless LAN Controllers provide advanced management capabilities for configuring and controlling CAPWAP access points. Among these features are Radio Resource Management (RRM) algorithms designed to automatically adjust APs' power and channel configurations to mitigate co-channel interference and signal coverage problems.

RRM allows access points to dynamically adjust their transmit power and wireless channels used by the access points to compensate for coverage holes and interference in the WLAN. If RRM is not configured correctly, transmit power asymmetry can result. Although the access point's signal can reach the badge, the badge's signal may not be able to reach the access point. This may cause choppy audio or one-way audio on Vocera badge calls.

Use the following steps to configure a Cisco Unified Wireless Network for the Vocera VLAN:

1. Design your wireless network taking into account the specifications of the Vocera badge. For more information, see **Power** on page 22.
2. Make sure your Cisco WLAN Controller software has been updated to AssureWave code or the most recent version available from Cisco. Check with Vocera Technical Support for the latest recommendations about Cisco WLAN Controller software versions.
3. If you are running Cisco Wireless Lan Controller release 7.6.120.0, you can use RRM by specifying maximum and minimum power level assignments. Here are the instructions for the Cisco WLC Web User Interface:
   a) Click **Wireless** to access the All APs page.
   b) Navigate to the 802.11b/g/n > RRM > Tx Power Control (TPC) or 802.11a/n > RRM > Tx Power Control (TPC) page. See the following figure.

Figure 29: 802.11a > RRM > Tx Power Control (TPC) page

c) Under Power Level Assignment Method, choose Fixed. In the drop-down box, select power level 3.

If your available power is 100 mW, a power level setting of 3 translates to 25 mW transmit power.

Note: Refer to the Cisco documentation for your access points for the maximum transmit power levels supported per regulatory domain and the number of power levels supported.

d) Click **Apply** to commit your changes.

e) Click **Save Configuration** to save your changes.

4. Configure all 802.11b/g data rates as supported. For maximum reliability, you should also select one or more **Basic** rates. In the Cisco WLC or Cisco WCS Web User Interface, "Basic" is referred to as "Mandatory" or "Required."

Here are instructions for configuring data rates using the Cisco WLC Web User Interface:

a) Click **Wireless** to access the All APs page.

b) Access the 802.11b/g Global Parameters page. See the following figure.

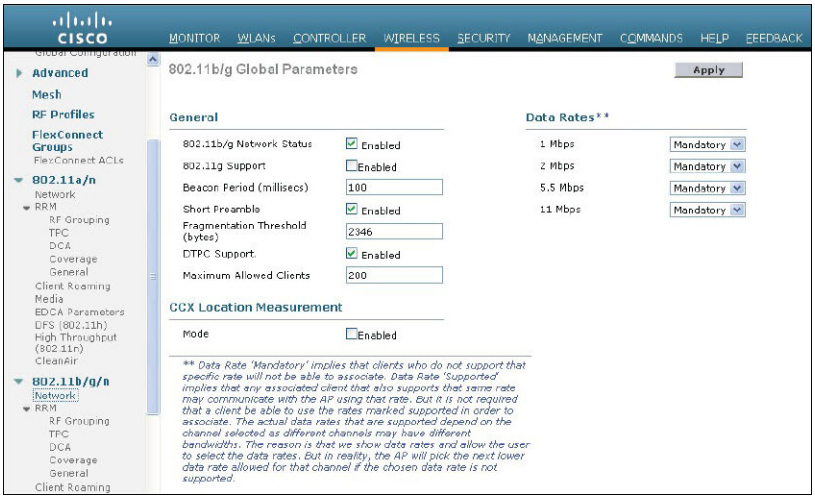


Figure 30: 802.11b/g Global Parameters page

c) Make sure none of the 802.11b/g data rates are disabled. To make a data rate supported, select Supported from the drop-down list.

d) Choose at least one mandatory data rate. To make a data rate mandatory, select Mandatory from the drop-down list.

Note: Depending on your wireless network, you may need to set multiple data rates as Mandatory. See **Configuring AP Radio Data Rates** on page 79 for more information.

e) Click **Apply** to commit your changes.

f) Click **Save Configuration** to save your changes.

5. Perform a **voice quality** site survey to ensure proper network coverage prior to installing Vocera.
6. Adjust the transmit power threshold setting of your APs using the Cisco WLC Command Line Interface (CLI). The transmit power threshold setting controls how strong each access point hears its third strongest neighbor. Start with a value of -70 dBm and then adjust it appropriately for your environment. Use this command:

```
config advanced 802.11b tx-power-control-threshold -70
```

7. Disable dynamic power level assignment in the APs using either the Cisco WCS Cisco Prime or the Cisco WLC Web User Interface. Here are the instructions for the Cisco WLC Web User Interface:
   a) Click **Wireless** to access the All APs page.
   b) Navigate to the 802.11b/g/n > RRM > Coverage or 802.11a/n > RRM > Coverage page. See the following figure.

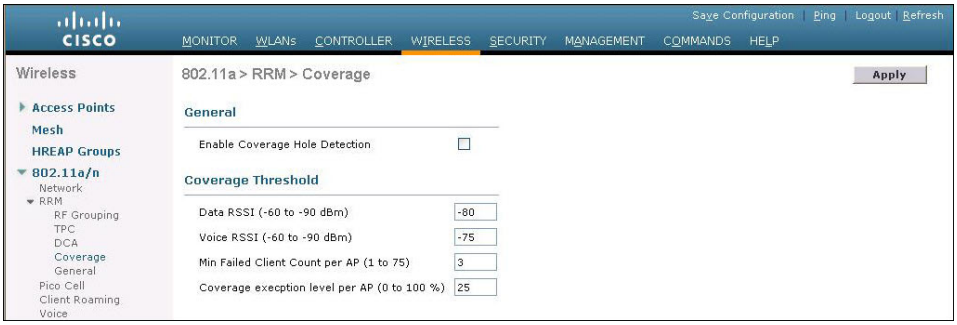


Figure 31: 802.11a > RRM > Coverage page

   c) Specify settings for Coverage Hole Algorithm.
      - Set Voice RSSI (-60 to -90 dBm) to -70.
      - Set Min Failed Client Count per AP to 12.
   d) Click **Apply** to commit your changes.
   e) Click **Save Configuration** to save your changes.
8. Wait at least 60 minutes after enabling dynamic power level assignment to allow the WLAN to stabilize.

   Each WLAN has its own unique characteristics, based on the structural features of the facility, density of APs, activity levels, and many other factors. Therefore, achieving optimal coverage is an iterative process. The goal of this iterative configuration process is to have the APs transmit power set to level 3 under normal conditions.
9. Verify AP transmit power levels and coverage.
10. After you verify coverage, you may need to adjust transmit power threshold setting (using the CLI), as well as the Coverage and Client Min Exception Level settings until you achieve proper coverage throughout the site.

Configuring AP Radio Data Rates

This appendix provides recommendations for how to configure data rates for AP radios to ensure proper range and throughput and to improve coverage and reliability of your Vocera system.

About Data Rates

You can configure an access point's data rate settings to choose which data rates it uses for transmission. The rates are expressed in megabits per second. For 802.11b, the data rates are 1, 2, 5.5, and 11 Mbps. For 802.11g, the data rates are 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

You can set each data rate to one of three states:

- **Basic** – Allows transmission at this rate for all packets, both unicast and multicast. In some Cisco user interfaces, Basic data rates are called Required or Mandatory data rates.

  Important: At least one of the access point's data rates must be set to Basic.

- **Enabled** – The access point transmits only unicast packets at this rate. Multicast packets are sent at one of the Basic data rates. In some Cisco user interfaces, Enabled data rates are called Supported data rates.
- **Disabled** – The access point does not transmit data at this rate.

The access point always attempts to transmit at the highest enabled data rate. If the access point cannot transmit at that rate due to interference or another reason, it tries to transmit using the next highest data rate that is enabled. On most access points, multicast and broadcast packets are transmitted at the lowest Basic rate. However, some access point models transmit multicast and broadcast packets at the highest enabled data rate; see **Multicast Transmissions** on page 80. Management packets, which can be transmitted only at Basic rates, are usually transmitted at the highest Basic rate.

Beacons and Basic Rates

An access point broadcasts a special management frame called a beacon at a fixed interval, providing wireless clients such as the Vocera badge with information about the wireless network. Access points send beacons at the beacon interval, which is usually set to 100 milliseconds. See **Beacon and DTIM Intervals** on page 14.

Beacons must be transmitted at a Basic data rate. Generally, access points send out beacons at the lowest common Basic data rate. For example, if the 1 Mbps data rate is set to Basic, access points will send out beacons at that rate, allowing wireless clients that are far away to hear the beacons.

Multicast Transmissions

Multicast packets must be transmitted at Basic data rates. Usually, access points send multicast packets at the lowest Basic rate. However, the following Cisco access point models send multicast packets at the highest Basic rate.

- **Cisco Aironet 1100 and 1200 series**

Consequently, if you have Cisco Aironet 1100 or 1200 series access points, you may need to set the highest Basic rate to a lower data rate, such as 2 Mbps, to prevent choppy audio on badge broadcasts and push-to-talk conferences, and make higher rates, such as 5.5 and 11, supported rates.

Ideally, you should set only one Basic rate (while keeping all other rates set to supported) to be the lowest data rate that a Vocera badge might use in a unicast call. Using a wireless packet capture program, also known as a wireless sniffer, you can capture a sniffer trace of a Vocera broadcast from a badge to determine the lowest data rate it shifts down to while roaming. If the Basic rate is set to a data rate higher than the lowest data rate used for a Vocera unicast call, the audio for broadcasts may sound choppy. If the Basic rate is set to a data rate lower than the lowest data rate used for Vocera broadcasts, WLAN congestion may result due to the increased propagation of management frames being broadcast, especially with a dense deployment of access points.

Data Rates and Roaming

Vocera best practice is to enable all data rates as "Supported" or greater. Enabling all rates allows a badge to shift to different rate for a more reliable transmission. Badges do not rely too much on data rates to roam, but on how well they can receive beacons, which is determined by power. Badges may depend on the lower rates, and they generally have better performance when they are able to shift down to the lower rates if necessary.

Data Rate Recommendations

Density of access point deployment is the biggest determining factor in whether lower data rates should be Basic or not.

Use the following strategy for configuring data rates:

1. Pick an access point power level appropriate for the Vocera badge and your RF cell size. For more information, see **Power** on page 22.
2. Design your WLAN for that power level.
3. Enable all 802.11b/g data rates, and set Basic rates based on access point density and power levels to ensure coverage and prevent choppy audio and roaming.
4. Set the Roaming Policy property on Vocera badges to a value that is appropriate for your RF cell size. For example, if access points are densely deployed, you may need to increase the Roaming Policy property to 3.

Radio Receiver Sensitivity

The following table shows the radio receiver sensitivity for Vocera devices at 802.11a/b/g data rates.

Table 21: Radio receiver sensitivity

Protocol	Data Rate	Receiver Sensitivity	
		Smartphone	B3000/B2000
802.11a	6 Mbps	-90 dBm	NA
	9 Mbps	-89 dBm	NA
	12 Mbps	-88 dBm	NA
	18 Mbps	-86 dBm	NA
	24 Mbps	-84 dBm	NA
	36 Mbps	-80 dBm	NA
	48 Mbps	-76 dBm	NA
	54 Mbps	-74 dBm	NA
802.11g	6 Mbps	-91 dBm	-79 dBm
	9 Mbps	-90 dBm	-79 dBm
	12 Mbps	-89 dBm	-78 dBm
	18 Mbps	-87 dBm	-77 dBm
802.11g	24 Mbps	-85 dBm	-76 dBm
	36 Mbps	-81 dBm	-70 dBm
	48 Mbps	-77 dBm	-67 dBm
	54 Mbps	-74 dBm	-65 dBm
802.11b	1 Mbps	-94 dBm	-85 dBm
	2 Mbps	-92 dBm	-85 dBm
	5.5 Mbps	-91 dBm	-84 dBm
	11 Mbps	-87 dBm	-82 dBm

B3000n Antenna Patterns

The illustrations in this section show antenna patterns of the B3000n badge in free space. The signal received by the badge, however, is affected by the body of the person wearing the badge.

Consequently, *you must follow the recommendations in* **Minimum Signal Strength** *on page 17* to ensure adequeate signal strength where the badge is actually in use.

B3000n Azimuth Pattern

The following illustration shows an azimuth antenna pattern of the B3000n badge:

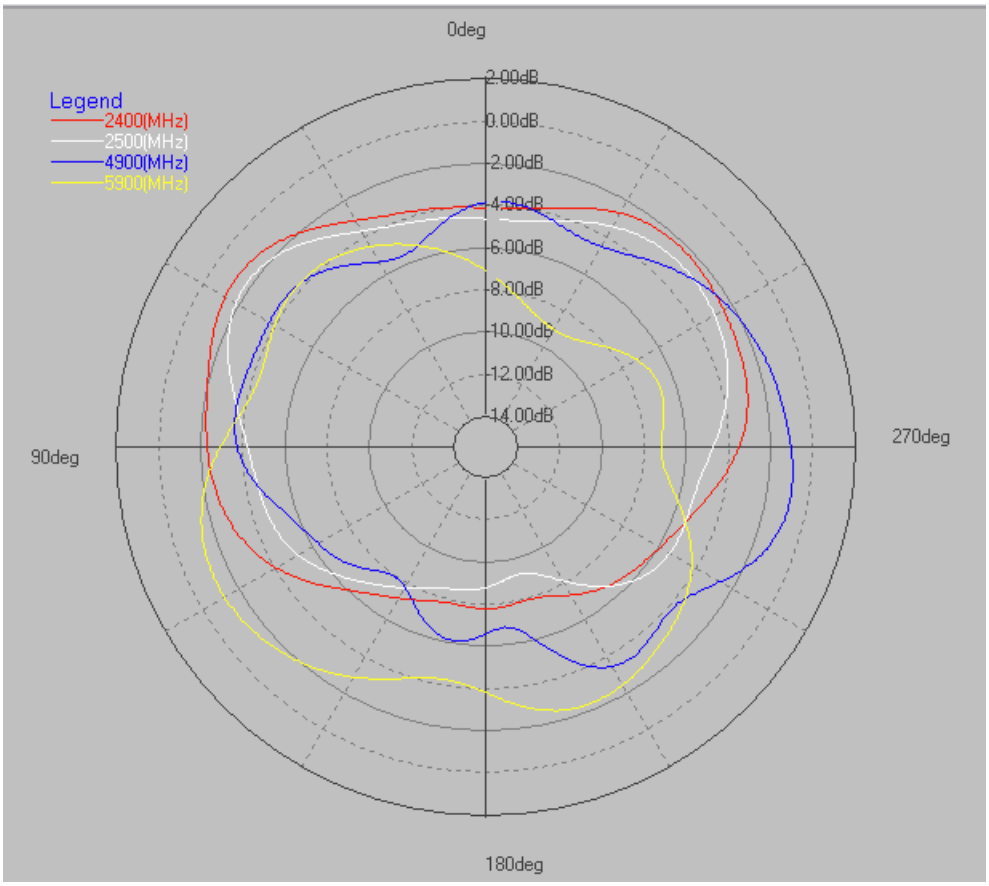


Figure 32: B3000n azimuth pattern

In the previous illustration of the azimuth antenna pattern, the badge is oriented in this position:

Figure 33: B3000n position: azimuth pattern

B3000n Elevation 1 Pattern

The following illustration shows an elevation antenna pattern of the B3000n badge:

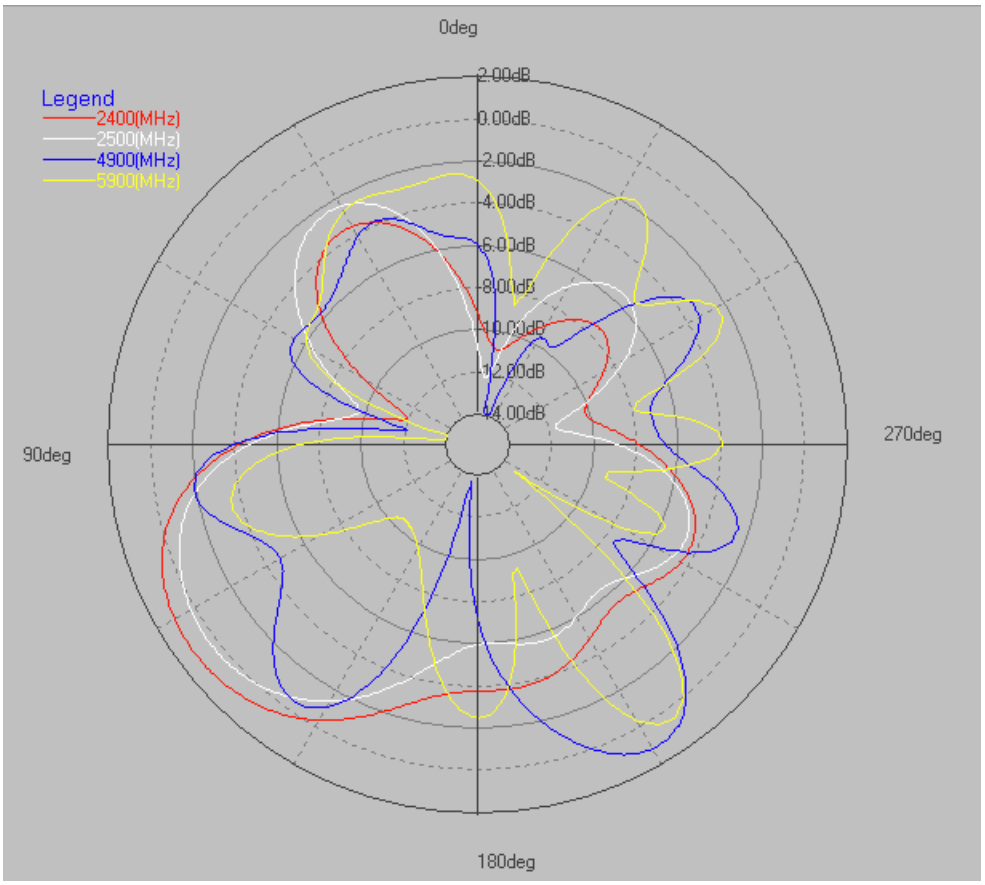


Figure 34: B3000n elevation 1 pattern

In the previous illustration of the elevation antenna pattern, the badge is oriented in this position:

Figure 35: B3000n position: elevation 1 pattern

B3000n Elevation 2 Pattern

The following illustration shows an another elevation antenna pattern of the B3000n badge:

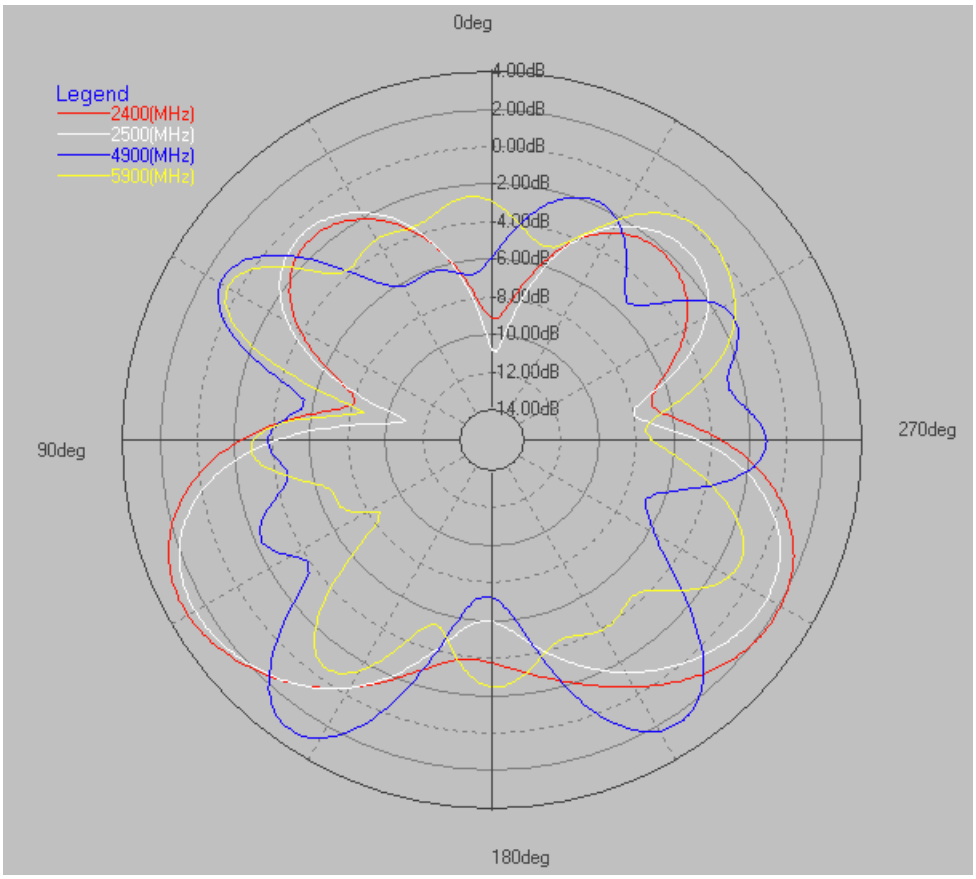


Figure 36: B3000n elevation 2 pattern

In the previous illustration of the elevation antenna pattern, the badge is oriented in this position:

Figure 37: B3000n position: elevation 2 pattern

IP Port Usage

The following tables indicates the ports used by Vocera system components for IP communication:

Table 22: Vocera Server IP port usage

Description	Protocol	Port No
Badge ↔ Server Signaling	UDP	5002
Vocera SIP Telephony Gateway -> Vocera Server Signaling	TCP	5001
Vocera Client Gateway -> Vocera Server Signaling	TCP	5006
Badge ↔ Updater Signaling	UDP	5400
Badge -> Vocera Server Audio	UDP	5100 - Max [7]
Badge -> Vocera Server Audio Recording	UDP	7200-7263
Vocera SIP Telephony Gateway -> Vocera Server Audio	UDP	5100 - 5149
Vocera Client Gateway -> Vocera Server Audio	UDP	5100 - 5355
Browser ↔ Apache Signaling	TCP	80 and 443 (for SSL)
Apache Tomcat Connector	TCP	8009
Tomcat HTTP Connector	TCP	8080
MySQL Signaling	TCP	3306
Vocera Server ↔ VMI Clients	TCP	5005
Vocera Server ↔ VMI Clients (TLS)	TCP	5007
Vocera Server ↔ VAI Clients	TCP	5251
Vocera Server ↔ Vocera Report Server Signaling	TCP	5251
Vocera Server Cluster Signaling	TCP	5251
Badge ↔ Vconfig (Vch) Signaling during Discovery	UDP	5555 and 5556
Badge ↔ Vconfig (Vch) Signaling during Connection	TCP	5555 and 5556
Nuance Watcher Telnet Client	TCP	7023
Nuance Watcher HTTP Client	TCP	7080
Nuance Watcher	UDP	7890
Nuance License Manager	TCP	27000
Nuance Speech Server (listens)	TCP	5060, 5062
Nuance Speech Server (allows UDP connections)	TCP	5060, 5062
Nuance Recognition Server (nuance-server.exe)	TCP	8200

[7] The port range used is based on the number of licensed speech ports.

Description	Protocol	Port No
Nuance RTP signaling	UDP	7500-8099
Administration Console ↔ Vocera Server	TCP	9091
Vocera Server ↔ CUCM JTAPI Signaling	TCP	2748

Table 23: Vocera SIP Telephony Gateway IP port usage

Description	Protocol	Port No
IP PBX ↔ Vocera SIP Telephony Gateway Signaling	UDP	5060
Vocera Server -> Vocera SIP Telephony Gateway Audio	UDP	5300 - 5555 [8]
IP PBX -> Vocera SIP Telephony Gateway Audio (RTP/RTCP)	UDP	8700 - 9467 [9]
Vocera Server -> Vocera SIP Telephony Gateway Signaling	TCP	any free port

Table 24: Vocera Client Gateway IP port usage

Description	Protocol	Port No
Smartphone ↔ Vocera Client Gateway Signaling	UDP	5060, 5888-5889
Badge -> Vocera Client Gateway Audio Vocera Server -> Vocera Client Gateway Audio Vocera SIP Telephony Gateway -> Vocera Client Gateway Audio	UDP	6300 - 6555 [10]
Smartphone -> Vocera Client Gateway Audio (RTP/RTCP)	UDP	7700 - 8467 [11]
Vocera Server -> Vocera Client Gateway Signaling	TCP	any free port

Table 25: MSP Server IP port usage

Description	Protocol	Port No
MSP Console (Browser) ↔ IIS Web Server	TCP	80 and 443 (for SSL)
FTP Server ↔ Smartphone **Note:** Different ports are required based on the FTP mode used (Active vs. Passive). See below.	TCP UDP	20 and 21 > 1023

Ports used when the FTP Server is in Passive Mode:

- FTP Server's port 21 from anywhere

  (Client initiates connection)
- FTP Server's port 21 to ports > 1023

  (Server responds to client's control port)

[8] The number of ports used is based on the number of lines configured. The maximum number of lines is 256 with one Vocera RTP port for each. The base port for this range is configurable.

[9] The number of ports used is based on the number of lines configured. The maximum number of lines is 256 with 2 ports (RTP and RTCP) for each, or 512 total. The server multiplies 512 by 1.5 to reserve additional ports in case some ports are already in use, resulting in 768 ports. The base port for this range is configurable.

[10] The number of ports used is based on the number of lines configured.

[11] The number of ports used is based on the number of lines configured.

- FTP Server's ports > 1023 from anywhere

  (Client initiates data connection to random port specified by server)
- FTP Server's ports > 1023 to remote ports > 1023

  (Server sends acknowledgments and data to client's data port)

Ports used when the FTP Server is in Active Mode:

- FTP Server's port 21 from anywhere

  (Client initiates connection)
- FTP Server's port 21 to ports > 1023

  (Server responds to client's control port)
- FTP Server's port 20 to ports > 1023

  (Server initiates data connection to client's data port)
- FTP Server's port 20 from ports > 1023

  (Client sends acknowledgements to server's data port)

Table 26: Vocera Report Server IP port usage

Description	Protocol	Port No
Vocera Server ↔ Vocera Report Server Signaling	TCP	5251
Report Console (Browser) ↔ Apache Tomcat	TCP	8080
Report Console↔ Report server	TCP	9090
Report results	TCP	80
MySQL port	TCP	3306

Table 27: Badge IP port usage

Description	Protocol	Port No
Badge ↔ Server Signaling	UDP	5002
Badge -> Vocera Server Audio Recording	UDP	7200-7263
Vocera Server -> Badge Audio Vocera SIP Telephony Gateway -> Badge Audio Badge -> Badge Audio	UDP	5200
Badge ↔ Updater Signaling	UDP	5400
Badge ↔ Vconfig (Vch) Signaling during Discovery	UDP	5555 and 5556
Badge ↔ Vconfig (Vch) Signaling during Connection	TCP	5555 and 5556

Table 28: Smartphone IP port usage

Description	Protocol	Port No
Smartphone ↔ Vocera Client Gateway Signaling	UDP	5060, 5888-5889
Vocera Client Gateway -> Smartphone Audio (RTP)	UDP	50000 - 50255
FTP Server ↔ Smartphone	UDP	> 1023

Table 29: Vocera Collaboration Suite IP port usage

Description	Protocol	Port No
Vocera Collaboration Suite Contacts	TCP	80 or 443 (for SSL)

Description	Protocol	Port No
iPhone and Android Smartphone ↔ Vocera Client Gateway Signaling	UDP	5060, 5888-5889
iPhone Audio	UDP	7700-8467
Android Audio	UDP	7700-8467 32768-65536

Opening Ports for Communication

If a firewall separates Vocera servers from the wireless network, make sure the following ports are open for communication:

Table 30: WLAN Ports Used by Vocera Clients

Client	Direction	Server / Client	Type	Protocol	Ports
Badge	Inbound/ Outbound	VS	Signaling	UDP	5002
Badge	Inbound	VS	Audio	UDP / TCP	5100-5199
Badge	Inbound/ Outbound	Badge/VS/VSTG	Audio	UDP	5200
Badge	Inbound	VSTG	Audio	UDP	5300-5555
Badge	Inbound/ Outbound	Updater	Signaling	UDP	5400
Badge	Inbound/ Outbound	VS	Discovery	UDP	5555 & 5556
Badge	Inbound/ Outbound	VS	Connection	TCP	5555 & 5556 [12]
Badge	Inbound	VCG	Audio	UDP	6300-6555 [13]
Badge	Inbound	VS	Audio	UDP	7200-7263
Smartphone	Inbound/ Outbound	VCG	Signaling	UDP	5060
Smartphone	Outbound	VCG	Audio	UDP	50000-50255
Smartphone	Inbound/ Outbound	FTP Server	MSP / FTP	TCP	20 & 21
Smartphone	Inbound/ Outbound	FTP Server	MSP / FTP	UDP	> 1023
Smartphone, Vocera Collaboration Suite for Android and iPhone	Inbound	VCG	Audio	UDP	7700-8467
Smartphone, Vocera Collaboration Suite for Android and iPhone	Inbound	VS	Signaling (Comet push)	TCP	80 or 443 (for SSL)
Vocera Collaboration Suite for Android and iPhone	Inbound	VMP	Signaling (Data)	TCP	80 or 443 (for SSL)

[12] Make sure you allow packets from TCP port 5556 to be received on any available port on the Vocera Voice Server.

[13] The base port for this range is configurable.

Client	Direction	Server / Client	Type	Protocol	Ports
Vocera Collaboration Suite for Android and iPhone	Inbound/ Outbound	VCG	Signaling	UDP	5060, 5888-5889
Vocera Collaboration Suite for Android	Inbound/ Outbound	Vocera Devices	Audio	UDP	32768-65536
VMIClients	Inbound/ Outbound	VS	Connection	TCP	5005
VAI Clients (includes Staff Assignment)	Inbound/ Outbound	VS	Connection	TCP	5251
VS (Vocera Connect for Cisco)	Outbound	Cisco UCM	Signaling	TCP	2748

Performance Tuning for Large Customers

This appendix provides performance tuning recommendations for large customers. A large Vocera system typically has more than 2,500 users at multiple sites and a spoken name count (which includes user names, group names, alternate spoken names, and department names) equal to or greater than 90,000.

Pre-Installation Recommendations

General Recommendations

- Set the cluster size for the Vocera drive to 64 KB.

  For more information, see the following articles:

  - **How to Locate and Correct Disk Space Problems on NTFS Volumes**
  - **Disk Configuration Best Practices & Common Pitfalls**
- Change from RAID 5 to RAID 10.

  Vocera is both read and write intensive. As a result, choose a RAID option that optimizes both read and write, such as RAID 1+0.

  For more information, see **Performance Tuning Guidelines for Windows Server 2003**.
- Make sure the %VOCERA_DRIVE% is located on a different physical disk than the system and pagefile drive.
- Configure your server to set processor scheduling and memory usage to Programs.

  For more information, see **Configuring Performance Options** on page 94
- If you are running antivirus software on the Vocera Server, set up folder exclusions for the `%VOCERA_DRIVE%\vocera` directory.

  For more information, see KB737 in the Vocera Technical Support Knowledge Base.
- Check server specifications against the **Vocera Server Sizing Matrix**.
- Improve performance by defragmenting your hard disks. Perform this task regularly to maintain disk performance.

  For more information, see **Disk Defragmenter Technical Reference**.

Windows 2003 Recommendations

- Align the Vocera data partition to the RAID stripe boundary to reduce storage I/O waste.

  For more information, see KB1095 in the Vocera Technical Support Knowledge Base.
- If 4 Gb or more RAM is installed on the server, make sure the /PAE boot parameter is used in the `boot.ini` file to enable Physical Address Extension (PAE), which will allow Windows to access all the RAM.

  For more information, see **Boot.ini Boot Parameter Reference: /PAE**.

Post-Installation Recommendations

- Increase the number of log files retained by the Vocera Server to 150 or 200 files.

  By default, the Vocera Server retains up to 100 log files. You can increase this number by modifying the LogMaxFiles property in the `\vocera\server\Properties.txt` file on the Vocera Server:

  ```
  LogMaxFiles     =     200
  ```

  Note: If you modify the `Properties.txt` file, you must stop and start the Vocera Server to load the properties into memory.

- Remove inactive Vocera users, groups, and address book entries.

  You can use the Vocera Report Server to generate reports of inactive Vocera users, groups, and address book entries. Once you identify inactive Vocera entities, you can delete them in the Vocera Administration Console.

Configuring Performance Options

Nuance Speech Recognition, Verifier, and Vocalizer software work best when the server is set to give the best performance to Programs rather than Background Services.

In Programs mode, Windows provides more frequent but smaller time slices during thread switching. In Background Services mode, Windows provides longer and less frequent time slices. If you run Windows with Background Services mode, Vocera badges may experience choppy audio.

Use the following steps to set Windows performance options for the Vocera Server:

1. Choose Start > Settings > Control Panel > System. The System Properties dialog box appears.
2. Click the Advanced tab.
3. In the Performance box, click Settings. The Performance Options dialog box appears.
4. Click the Advanced tab.
5. In the Processor Scheduling box, click Programs. This gives more processor resources to the Vocera Server instead of background services.
6. In the Memory Usage box, click Programs. This allocates more system memory to the Vocera Server instead of the system cache
7. Click OK.
8. A dialog box informs you that the changes will not take effect until you restart the computer. Click OK to close the dialog box.
9. In the Performance Options dialog box, click OK.
10. In the System Properties dialog box, click OK.
11. Restart the computer.

WLAN Requirements and Best Practices

This appendix provides a summary of required WLAN settings and best practices for Vocera system implementations.

WLAN Settings

Table 31: Required WLAN Settings

Setting	Required Value
Voice Grade Site Survey	Required
Max AP Transmit Power	15dBm (30mW)
Min AP Transmit Power	11dBm (12.5mW)
Minimum Power Coverage	-65dBm
Minimum SNR	25
Beacon Interval	100
DTIM	1
Public Secure Packet Forwarding	Disabled
ARP Cache	Enabled except for Autonomous APs
Priority Queue	Highest - Voice

Table 32: Recommended WLAN Settings

Setting	Recommended Value
Code Version	Use most recent version of AP code
Basic Data Rates	Needs to be determined for each site
Supported Data Rates	All Enabled
Channel Plan	1, 6, 11
Roam Threshold	2 - May adjust based on AP density or Meru Virtual Cell
Max Number of SSIDs	5
Client Exclusions	Disabled
Authentication Timeouts	Add session timeout of at least 1 full shift
EAP Retry Timeout	200 milliseconds or lower
Max Retries	4

Table 33: Multicast Recommendations

Setting	Recommended Value
IGMP on Badge	Enabled
IGMP V2 on Network	Enabled
Multicast Configuration	• PIM (Sparse Mode or Sparse Dense Mode) must be applied to all Vocera VLANs and the WLC management VLAN • Enable IGMP Snooping on APs and all L2 devices in the multicast audio path • Block all unnecessary multicast traffic • Use Band Steering for data SSIDs to steer them towards 802.11a to reduce airtime contention • Configure UDP Broadcast Port 5555 for Badge Discovery for Meru
Reverse Path Forwarding	Enabled

Vocera Recommendations for Cisco CAPWAP

Table 34: Cisco Settings

Setting	Recommended Value
RRM – Dynamic Channel Assignment	OK - Interval should be more than 8 hours (typical duration of one nursing shift)
RRM – Dynamic Transmit Power Control	Enabled if honoring the maximum and minimum transmit power levels
Transmit Power Threshold	Adjust to fit site
Coverage Hole	Disabled - If Coverage Hole Detection is necessary, enable it with the following settings: • Set Voice RSSI (-60 to -90 dBm) to -70 • Set Min Failed Client Count per AP to 12
Aggressive Load Balancing	Disabled
Multicast Mode	Multicast, Direct Disable Mobility Multicast Messaging if multicast is not properly enabled in network (causes one-way audio or no audio)
Multicast Tx Data Rate	Highest data rate Only have one Mandatory rate, fit to site.
Unicast-ARP	Disabled
WMM	B3000n: Enabled B3000: Disabled Smartphone clients: Enabled
U-APSD	B3000n: Enabled B3000: Disabled Smartphone clients: Enabled
DHCP Address Assignment	Disabled
Symmetric Mobility Tunneling	Enabled
Priority Queue	Platinum
Client Load Balancing	Disabled
Band Select	Disabled
CCKM	Enabled

Setting	Recommended Value
Frame Aggregation	Disabled on transmit or receive for Traffic ID 6 (voice) and 7 (network control)
Encryption	Avoid WEP and TKIP

Vocera Recommendations for Aruba Networks

Table 35: Aruba Settings

Setting	Recommended Value
Minimum Controller Code	6.1.3
Role	Voice
ARM	Enabled if honoring the maximum and minimum transmit power levels
Voice Aware Scanning	Enabled
Tx Data Rates	2.4 GHz: 6, 9, 11, 12, 18, 24 5 GHz: Enable 9Mbps and above; disable all lower rates
Probe Retry	Disabled
Max Tx Failure	25
Session ACL	vocera-acl
Mcast-rate-opt (needed for multicast to go at highest rate)	Enabled
Multicast Filters - Use the Aruba Policy Enforcement Firewall (PEF) to configure these multicast filters to block traffic.	netdestination HSRP Host 224.0.0.2 netdestination VRRP host 224.0.0.18 netdestination RIP host 224.0.0.9 netdestination OSPF host 224.0.0.5 host 224.0.0.6 netdestination PIM host 224.0.0.13 netdestination EIGRP host 224.0.0.10
OKC	Enabled

Vocera Recommendations for Ruckus Networks

Table 36: Aruba Settings

Setting	Recommended Value
Tunnel traffic	Disabled
Channel fly	Disabled
QOS	High

Setting	Recommended Value
Smart-Roam	Disabled
Vlan	Dedicated non-native Vlan
Authentication/Encryption	WPA2/AES (802.11i)
Wireless Client Isolation	Disabled
Wlan Background Scanning	Disabled
Power Level	1/8 (25mW)
Directed-Multicast	Turn off using SSH / console CLI
OKC	If applicable: Enabled

Vocera Recommendations for Meru Networks

Table 37: Meru Settings

Setting	Recommended Value
SSID	Separate for Vocera
IGMP Snooping	Enabled
QoS Rules	Enable QoS Rules 7 & 8 (Enabled by Default)
Virtual Port	Disabled
Virtual Cell [14]	Enabled
Badge Roaming Policy	1
Silent Client Polling	Enabled
Vocera Location Feature	Disable Virtual Cell or divide APs into zones
Multicast setting	Configure UDP Broadcast Port 5555 for Badge Discovery for Meru

[14] A Transmit Power Asymmetry problem may arise at the edges of Virtual Cell coverage if an AP's transmit power is higher than the Vocera device (~30mW). To avoid poor audio at the edges of the Virtual Cell, the RSSI of the Vocera device on the AP must be verified. The Vocera device should never drop below an RSSI of -75dBm on the AP.