stryker

Vocera Infrastructure Planning Guide

Notice

Last modified: 2025-02-25 08:47

ED-Solution-VIG-Docs build 83

Contents

Introduction to the Vocera Infrastructure Planning Guide

The introduction section summarizes the product overview, the details covered in this document, the intended audience, the firmware releases applicable to the devices and the badge properties editor, and the related documentation you can refer for details on specific topics.

Overview of the Vocera Infrastructure Planning Guide

The Vocera Communications System enables you to connect and communicate instantly over a wireless network using a wireless device. The wireless devices use the latest IEEE standard and enable higher throughput and improved reliability and range.

Note: Any reference to a Vocera device in this document collectively refers to B3000n Badge, V5000 Smartbadge, and C1000 Minibadge.

The Vocera enterprise application is set up in a complex network infrastructure. Following are the Vocera clients related to this document:

- **Vocera C1000 Minibadge**—The Vocera C1000 Minibadge is a lightweight, hands-free device that you can operate using your voice. You can use the Minibadge as a standalone device or smartphone companion. Using the Minibadge, you can place and receive calls, listen and respond to messages and alarm notifications.
- **Vocera V5000 Smartbadge**—The Vocera Smartbadge is a small, lightweight, wearable communication device purpose-built for healthcare. The Smartbadge is powered by the Vocera Platform, enabling interoperability with most clinical and operational systems used in healthcare. The Smartbadge gives caregivers the agility to respond to the complex and unpredictable patient care environment. Some of the salient features of the Smartbadge are to enable real-time situational awareness, receive a prioritized alert and alarm notifications, make and answer calls hands-free, have a smooth, natural bi-directional conversation, and send messages securely. The Vocera Smartbadge provides several distinct features, dual-band 2.4 GHz and 5 GHz radio supporting 802.11 a/ac/b/g/n/r/k and an orientation sensor.
- **Vocera B3000n Badge**—The Vocera B3000n Badge is a small, lightweight wireless wearable device that enables clinical communication and workflow. You can initiate communication by pushing a button on the Badge and issuing a voice command. For example: “Call Jodie Lee.” The Badge provides several distinct features, dual-band 2.4 GHz and 5 GHz radio supporting 802.11 a/b/g/n and an orientation sensor.

  Devices are wireless network clients that require configuration before they can communicate on your network. For example, when you configure a device, 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 device, such as the SSID (Service Set Identifier), your wireless network uses, and any security settings that your network may require. You must download property settings to the device from the Badge Properties Editor (BPE) is a tool that allows you to set properties for the Badge and lets it connect to the wireless network. The Badge Properties Editor (BPE) is installed on both the configuration computer and the Vocera Voice Server computer. The devices are most easily configured and administered as a group. You use the utilities to create a single properties file that describes settings for all the devices and download the settings in the properties file.

- **Vocera Smartphone Applications**—The Vocera Smartphone Apps includes a powerful application enabled by the Apple IOS, Android operating systems. The Vocera Smartphone Apps provides access to all the voice communication features of a Vocera Badge and offers secure messaging, alert, alarm, and chat capabilities.

  You can download the VCS app from the iTunes and Google stores and install it on recommended devices. For more information, refer to 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 Voice Server for all calls. All voice communication between the Vocera Voice Server or the Vocera app is done through the Vocera Client Gateway.

  Vocera offers the MC40-HC as a platform for the VCS which includes Vocera voice, secure enterprise text messaging, clinical workflow, and alarm applications. For users who need a rugged, multi-functional smartphone, you can use the multi-functional Zebra TC51-HC that provides one-touch, instant communication capability of a Vocera client in a familiar phone form.

Important: When you are designing your wireless network, ensure that you configure your access points to provide the Vocera Voice Server app, Smartphones with VCS installed on it. Vocera recommends Badges with a minimum signal strength of -65dBm and a minimum SNR value of -25 dB based on a -90 dB noise floor for the area where the devices are used. If you are using both badges and other Vocera devices, set the transmit power of the access points to the level required by the Vocera Badge, which has a smaller radio and battery than the smartphone due to its lightweight, wearable design. For more information, refer to Signal Propagation on page 63.

About the Vocera Infrastructure Planning Guide

Vocera Infrastructure Planning Guide helps you understand the principles of voice over IP. It also provides information about how to configure your wired and wireless network infrastructure to support the Vocera Communications System.

You can refer to this document to understand the 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. The content focuses primarily on network infrastructure topics that affect the Vocera system and discusses larger network infrastructure topics as a summary only to provide context.

The specification required to set up your device to work in your network environment is covered in this document.

Important: The content provided in this document is based on ongoing product testing, research, field experience, and customer feedback. These guidelines represent the best information that we have at any time, and the document is updated continually.

Intended Audience for the Vocera Infrastructure Planning Guide

Vocera Infrastructure Planning Guide is intended for experienced network administrators and wireless engineers.

You must have a basic understanding of enterprise networking and how a real-time voice application interacts with your wired and wireless network to deploy Vocera.

Product Applicability of the Vocera Infrastructure Planning Guide

The product applicable and the supported firmware releases are listed in this section.

Vocera Firmware	Supported Vocera Software	Supported Devices
Firmware 4.0.1 or later Firmware 5.0.0 or later Firmware 5.1.0 or later Firmware 6.5.0 or later	Vocera Voice Server 5.2.1 or later. Vocera Platform 6.1.0 or later. Vocera Platform 6.5.0 or later	B3000n, V5000, and C1000

Related Documentation for the Vocera Infrastructure Planning Guide

The documents supporting the Vocera Infrastructure Planning Guide are listed here.

The following documents support the Vocera Infrastructure Planning Guide:

- Vocera B-Series Badge User Guide—Specifies how to use your Vocera Badge and the features. It also helps you understand how to use the voice commands using your Badge.
- Vocera V-Series Smartbadge User Guide—Specifies how to use your Vocera Smartbadge and the features. It also helps you understand how to use the voice commands using your Smartbadge.
- Vocera C-Series Minibadge User Guide—Specifies how to use your Vocera Minibadge and the features. It also helps you understand how to use the voice commands using your Minibadge.
- Vocera Voice Commands Reference Guide—Specifies the details of the voice commands that you can use on your Vocera Badges, Vocera Smartbadges, and smartphones to communicate.
- Vocera Device Configuration Guide—Specifies how to configure Vocera device using the Badge Properties Editor and the Badge Configuration Utility. It also provides details of the updates to the badge properties and firmware.
- Vocera Device Safety and Regulatory Guide—Specifies the safety details for electrical, magnetic, radio, wireless, chemical, chargers, along with your power supply safety.

Related Cisco documents

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.
- Cisco Wireless LAN Controller Configuration Best Practices —Describes the short configuration tips that cover standard best practices in a typical Wireless LAN Controller (WLC) infrastructure.

Note: Screenshots and instructions provided in the document are examples. Check vendor documentation for GUI and instruction updates.

VoIP Over Wired Networks

Wired network requires careful planning of network connectivity, Quality of Service (QoS), subnets, multicast traffic, and IP addressing.

Although Vocera runs on a wireless 802.11b/g network for B3000 badges, and 802.11 a/b/g/n for B3000n badges, the implementation of your wired infrastructure affects its performance.

Network Connectivity for Vocera Infrastructure Planning

Most contemporary wired networks comprise of packet switches which can support huge traffic.

Typically the wired network capacity is not an area of concern when deploying a VoIP solution. However, many large deployments are spread across geographically dispersed areas, and these utilize Wide Area Networks. When deploying a WAN, the bandwidth requirements for VoIP traffic and end to end latency become critical to the success of the deployment.

If you are planning to allow Vocera 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. The following table lists the number of simultaneous calls or Genie sessions and the corresponding 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

Also, 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, you must enable end-to-end QoS, so that the traffic prioritized at the access point does not lose its priority as it passes through other devices such as distribution switches, core routers, other devices, and so on.

Some devices, such as core routers, may provide enough bandwidth and the traffic prioritization is unnecessary. However, you should enable QoS on any network.

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:

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

If your Vocera traffic traverses a WAN circuit, you must ensure that the following QoS requirements are met:

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

Enabling Quality of Service

Enable QoS on the Vocera systems to improve the performance of your network. Excluding any of the QoS configuration tasks can result in performance problems.

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

- Enable QoS on your B3000n badges by setting `B3N.EnableWMM` and `B3.EnableWMM` to `TRUE`. For more information, refer to Vocera Device Configuration Guide.

  Note: The Vocera Collaboration Suite application automatically takes advantage of QoS in version 2.0.2 or later.

  On V5000 Smartbadge and C1000 Minibadge, QoS is enabled by default.
- Ensure that the Vocera QoS Manager service is installed and enabled on the Vocera Voice Server, Vocera Client Gateway, and Vocera SIP Telephony Gateway machines. For more information, refer to Confirming Vocera QoS Manager Installation on page 10.
- Ensure that the Windows QoS Packet Scheduler is installed and enabled on the network connection of your Vocera Voice Server, Vocera Client Gateway, and Vocera SIP Telephony Gateway machines. For more information, refer to Confirming Windows QoS Packet Scheduler Installation on page 11.
- Create a Local Group Policy to mark packets with DSCP 46 on each of your Vocera Voice Server, Vocera Client Gateway, and Vocera SIP Telephony Gateway machines. For more information, refer to Creating a Windows QoS Policy on page 13.
- Configure your access points to map IP level DSCP EF to WMM/802.11e level voice priority. The access points pass the DSCP markings through to the network. For more information, refer to Enabling 802.11e QoS on Cisco Access Points on page 16.
- Ensure that the switches and routers on your network are configured to accept 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 with or without WMM enabled. The Vocera Voice Server also marks packets with DSCP value 46. For the latest versions of the Vocera Voice Server refer to http://pubs.vocera.com/docportal/index.html#docportal/docportal/version/topics/vs.html.

For example, if you do not enable the Vocera QoS Manager service on the Vocera Voice Server, then packets that originate from the Vocera Voice Server has a lower priority than those that originate from badges. If there is excessive traffic on a given AP, you may experience problems during voice communication with the Vocera Voice Server.

Confirming Vocera QoS Manager Installation

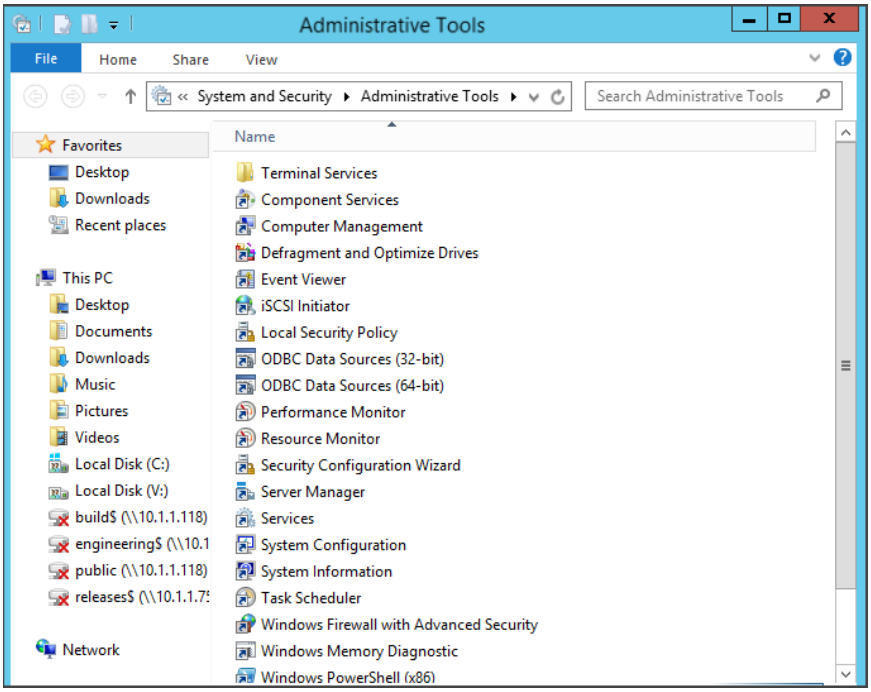
The Vocera QoS Manager installation program automatically installs and enables the Vocera QoS Manager service on the Vocera Voice Server, the Vocera SIP Telephony Gateway, and the Vocera Client Gateway during the application install.

Vocera Client Gateway

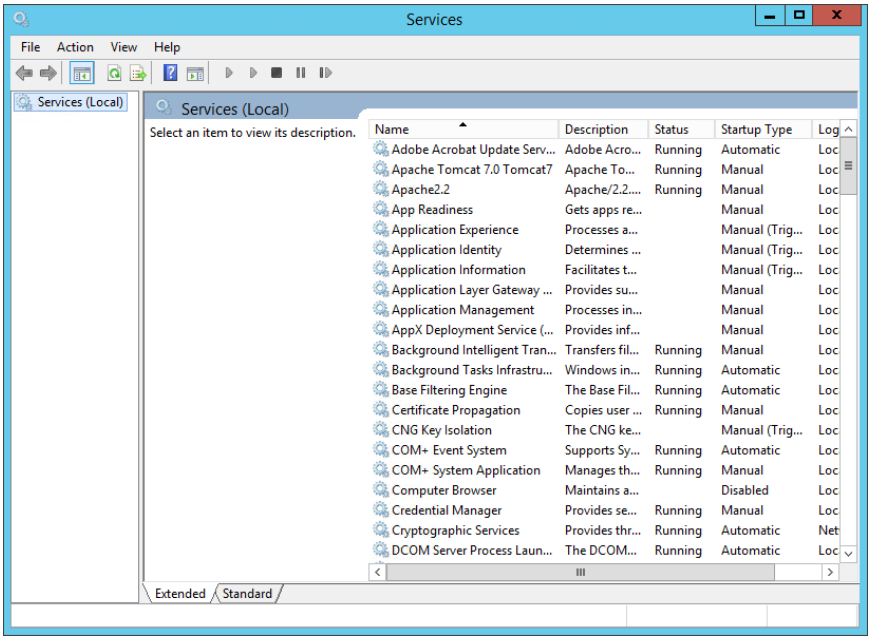
When the Vocera QoS Manager service is running, each Vocera voice packet that originate from the Vocera Server is tagged with DSCP Expedited Forwarding (EF). On the network side, switches and routers must be configured to accept DSCP markings.

To confirm that the Vocera QoS Manager is installed and enabled on a Windows Server 2012 machine:

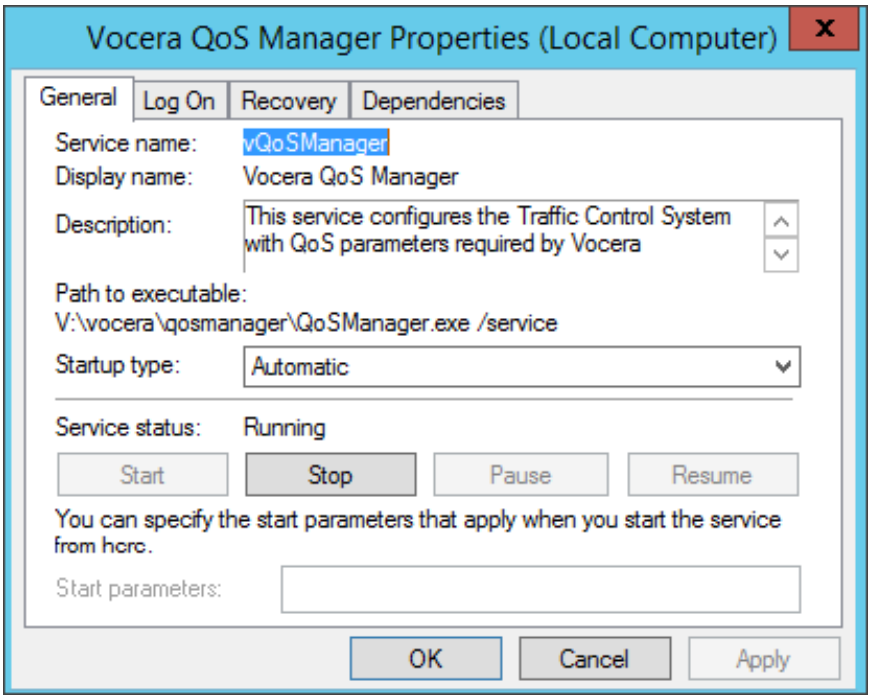
1. Select **Administrative Tools** from the Windows **Start** menu.
   The Administrative Tools window appears.



2. Double-click the **Services** shortcut.
   The Services window displays the list of installed Windows services.



3. Scroll to **Vocera QoS Manager**, right-click and choose **Properties**.
   The Vocera QoS Manager Properties (Local Computer) dialog box opens. By default, the General pane is visible.



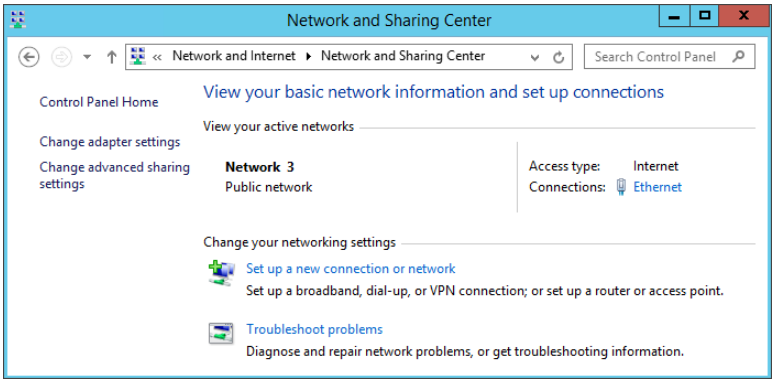
4. Ensure that the value of the **Startup Type** field is set to Automatic, or set it if necessary.
5. Click **OK**.
   The Vocera QoS Manager Properties (Local Computer) dialog box closes, saving your changes.

Confirming Windows QoS Packet Scheduler Installation

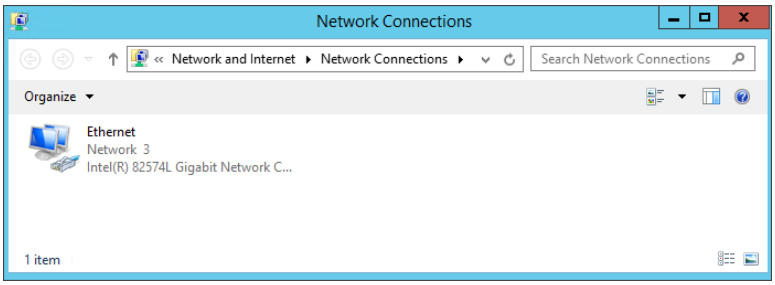
The Vocera QoS Packet Scheduler Installation is an important task to ensure good connectivity. Windows QoS Packet Scheduler helps in the management of network bandwidth. It monitors data packets and assigns higher or lower priority levels to traffic and protocols.

Vocera QoS Manager service configures the QoS Packet Scheduler network service with QoS parameters required by Vocera. The configuration prioritizes Vocera voice packets that originate from the server. To confirm that the Windows QoS Packet Scheduler is installed and enabled on a Windows Server 2012 machine, perform the following tasks:

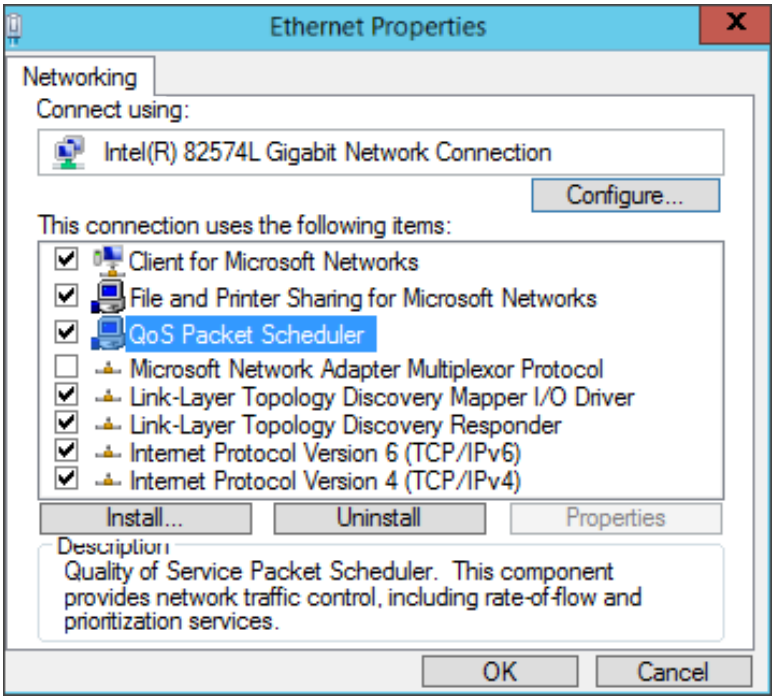
1. Select **Control Panel** from the Windows **Start** menu.
   The Control Panel window opens.
2. Select **Network and Sharing Centre**. The following figure displays the network and sharing window.



3. Select **Change adapter settings**.
   The Network Connections window opens.



4. Right-click **Ethernet** and select **Properties**.
   The Ethernet Properties dialog box appears.



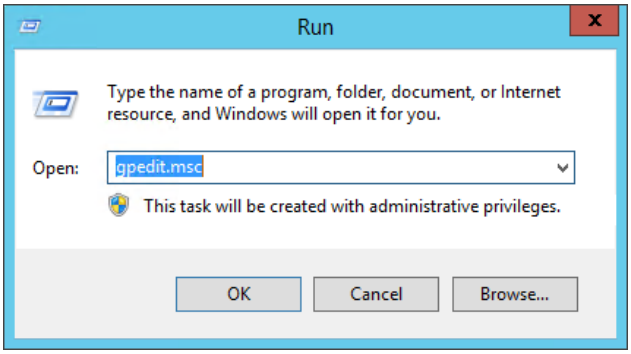
5. Ensure that the **QoS Packet Scheduler** property is enabled or enable as necessary.
6. Click **OK**.
   The Ethernet Properties dialog box closes, saving your changes.

Creating a Windows QoS Policy

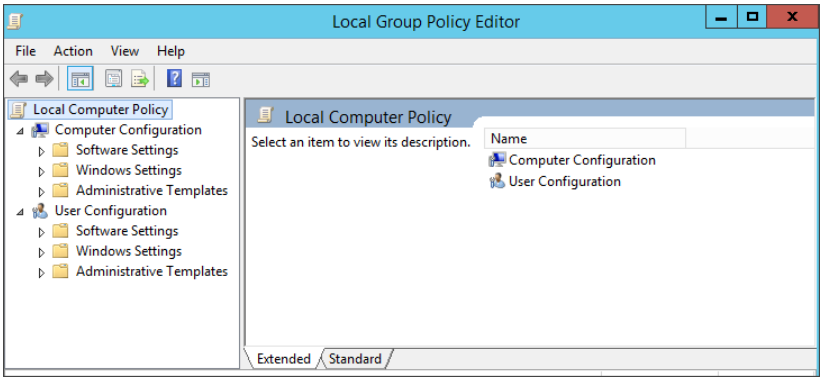
Windows allows you to specify a policy that tags and prioritizes Vocera packets, that helps you to provide an optimized voice experience.

To create a QoS policy on a Windows Server 2012 machine:

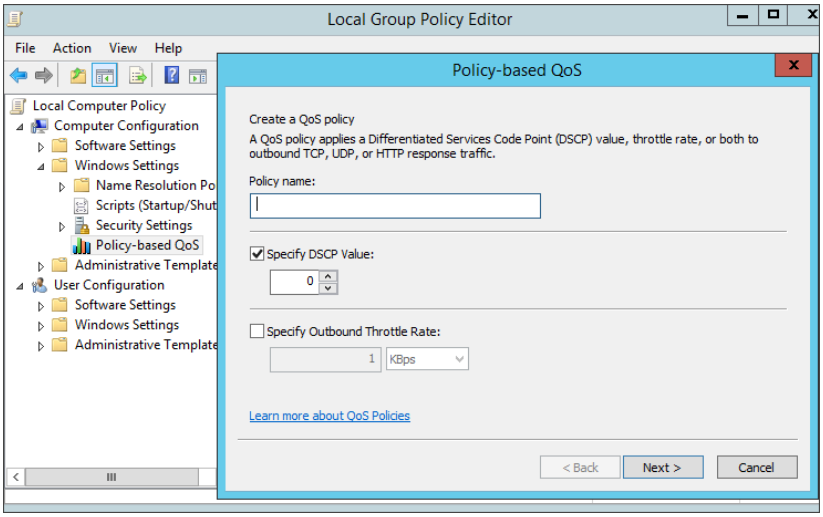
1. Right-click the **Windows Start** menu and select **Run**.
   The Windows Run dialog box opens.



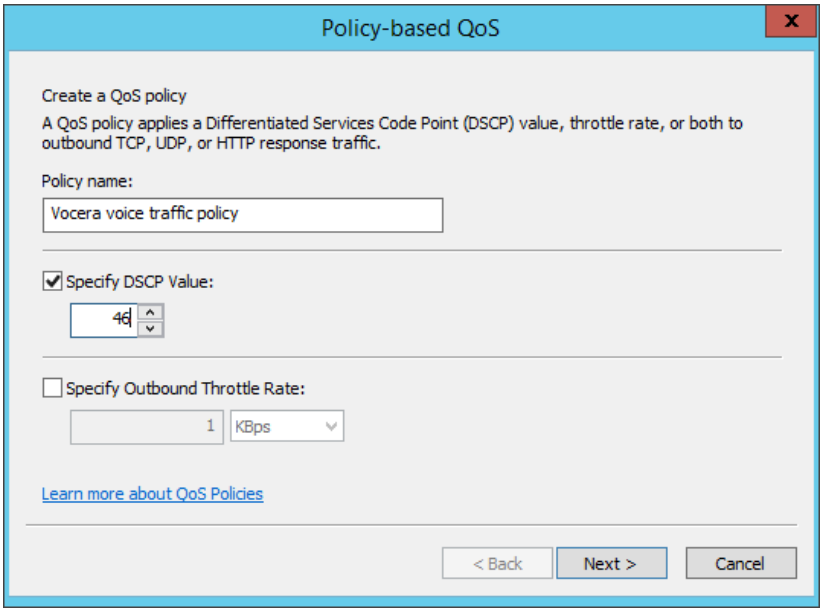
2. Enter `gpedit.msc` in the **Open** field, and click **OK**.
   The Local Group Policy Editor window opens.



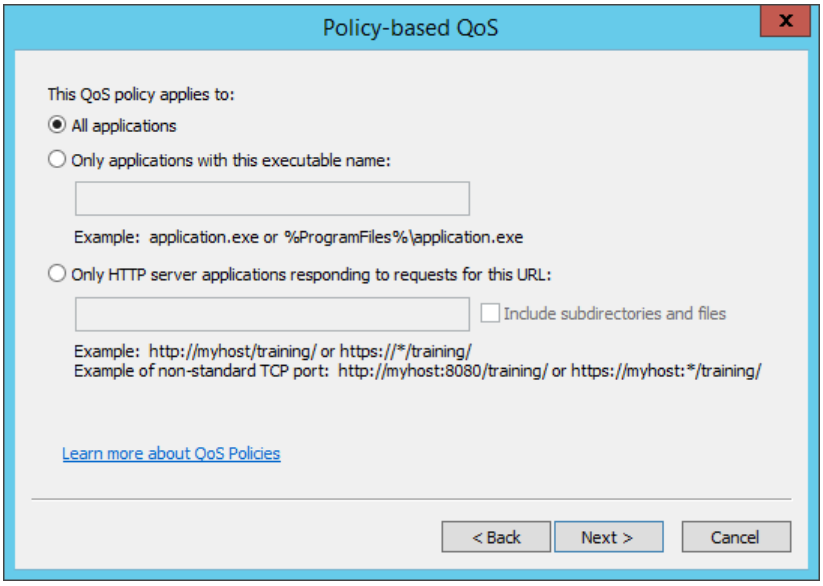
3. Expand **Local Computer Policy** >**Computer Configuration** >**Windows Settings**>**Policy-based QOS** and select **Create New Policy**.
   The Policy-bases QoS dialog box opens.



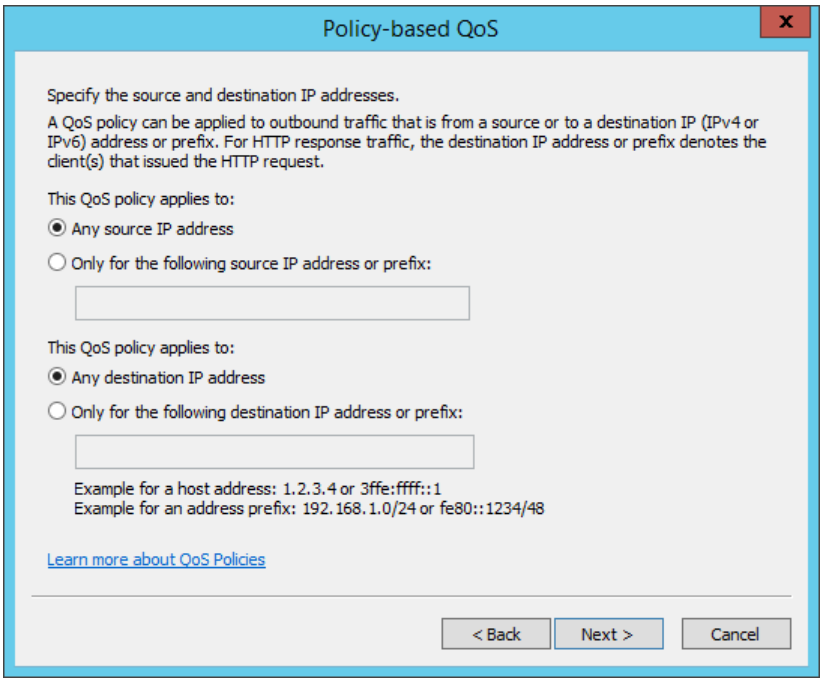
4. Specify a name such as `Vocera voice traffic policy` in the **Policy name** field.
5. Check **Specify DSCP Value** and set it to **46**.



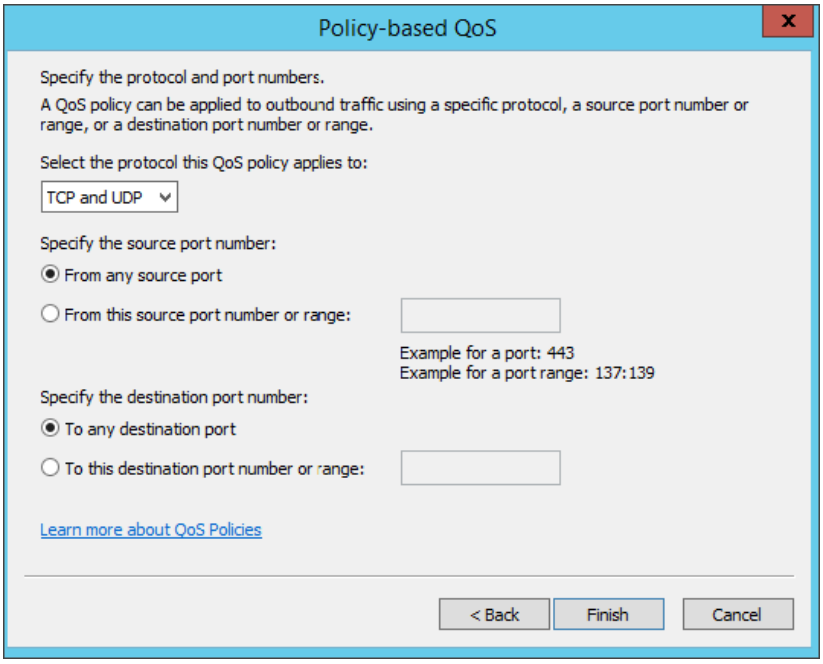
6. Click **Next** to display the second screen of the wizard.



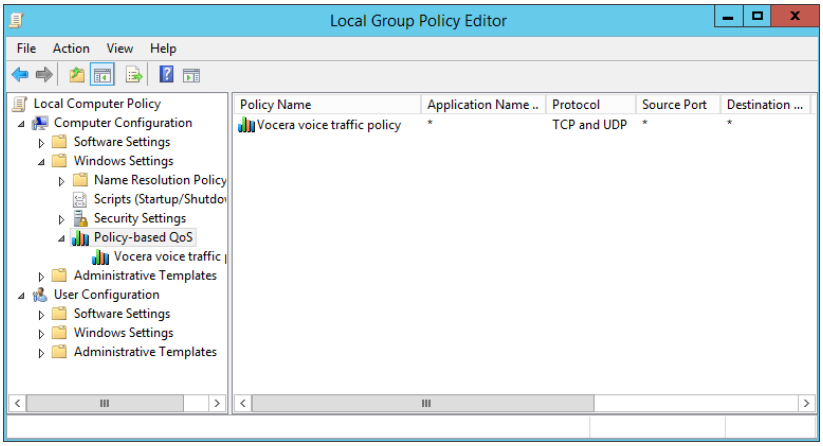
7. Check **All applications** and click **Next**.
   The third screen of the wizard appears.



8. Check **Any source IP address** and **Any destination IP address** and click **Next**.
   The fourth screen of the wizard appears.



9. Set **Select the protocol this policy applies to** to **TCP and UDP**.
10. Check **From any source port** and **To any destination port** and click **Finish**.
    The **Vocera voice traffic policy** appears in the **Local Group Policy Editor** window.

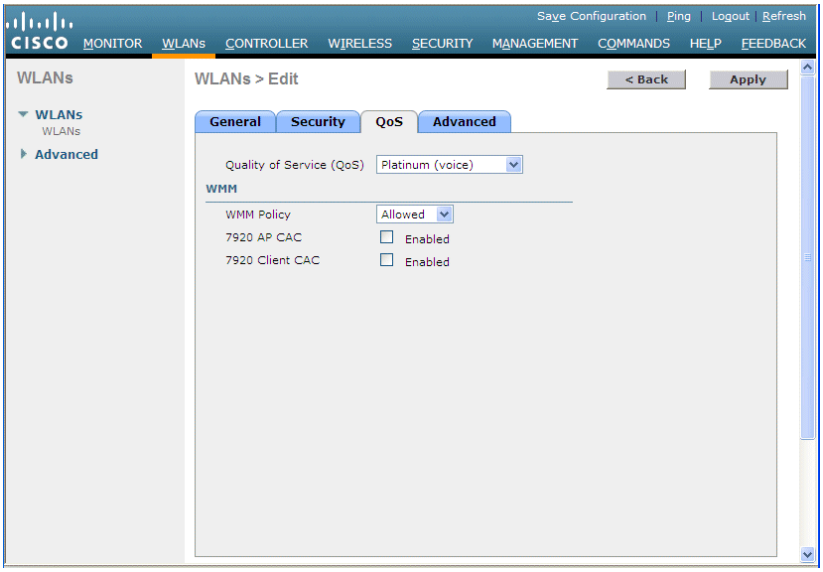


Enabling 802.11e QoS on Cisco Access Points

The Cisco Access Points is based on IEEE 802.11e and improves the bandwidth and provides faster wireless speed.

To enable 802.11e QoS for Cisco CAPWAP access points, perform the following steps:

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



3. Select **Platinum (Voice)** in the **Quality of Service** list.
4. Select **Allowed** in the **WMM Policy** list.

   Note: Vocera badges do not support CAC. Do not enable **7920 AP CAC** and **7920 Client CAC**.

5. Click **Apply**.

Multiple Vocera Subnets

Subnets is a logical division of a network. Several Vocera subnets are required when your deployment spans to more than one building in a campus environment or physically separate geographical sites.

Vocera devices are often deployed on a single IP subnet. If your Vocera system runs on multiple subnets, ensure that you configure the following badge properties:

Property	Recommendation
Broadcast Uses IGMP	The **Broadcast Uses IGMP** property is set to TRUE by default for all badges. This property ensures that multicast features such as broadcasts and push-to-talk conferences work across subnet boundaries. For more information, refer to Internet Group Management Protocol (IGMP) Snooping on page 21. For details, refer to 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 badge 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 (PTT) conferences. Vocera multicast features can be configured to cross subnet boundaries.

Vocera broadcast and instant conference push-to-talk feature use multicast to forward IP datagrams to a multicast group within a single subnet, for urgent broadcast command, VMI broadcast, and broadcast from a phone. 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.

By default, B3000n, V5000, and C1000 use IGMP version 2. Ensure that you enable IGMPv2 on all intermediate routers or other Layer 3 network devices on each subnet used by Vocera devices. For more information on IGMP, refer to Internet Group Management Protocol (IGMP) on page 20.

Tip: IGMP is typically enabled on switching infrastructure. Vocera recommends that you enable IP multicast routing and add PIM statements on all Layer 3 devices that traverses Vocera traffic.

Multicast Transmissions

Multicast transmission is a stream of packets that is transmitted at a specific data rate, to a group of hosts on a network.

Low data rates consume significantly more airtime than higher data rates. Hence, Vocera recommends that you enable higher 802.11 mandatory data rates (12 and 24 Mbps optimal) and remove support for lower rates (1, 2, 5.5,11 Mbps). This prevents choppy audio on badge broadcasts and push-to-talk conferences.

The Vocera B3000 badge can process frames sent at 11 Mbps. The lower data rates (9, 6, 5.5, 2 and 1 Mbps) can be disabled. Data rates higher than 24 Mbps can be left enabled or disabled. Disabling these higher data rates provides an advantage of avoiding issues when the phone rate-shifts between data rates, delaying frame transmission, compromising the performance of the transmission.

Ideally, you should set only one mandatory rate to be the lowest data rate that a Vocera badge might use in a unicast call. By using a wireless packet capture program, also known as a wireless sniffer, you can obtain a sniffer trace of a Vocera broadcast from a badge to determine the lowest data rate it shifts down to while roaming.

For more information on data rates, refer to: Data Rates on page 40.

Multicast for Vocera Collaboration Suite

Vocera Collaboration Suite clients that run on 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 Client Gateway devices.

Note:
Information provided in this topic does not apply for Vocera Vina.

To disable multicast transmissions on the Vocera Client Gateway, enable multicast routing support on 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 use.

This ensures that multicast traffic is routed properly from badges and the Vocera Voice Server to the Vocera Client Gateway.

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

To test broadcasts on a smartphone, perform the following steps:

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 smartphone with VCS 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. 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.

    The badge plays a chime, and then you hear the broadcast.

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

Multicast and Vocera Messaging Interface Broadcasts

Vocera Messaging Interface (VMI) can be configured to use IP multicast to broadcast one-way, urgent VMI messages without responses from the server to all recipient devices. VMI thus uses only one speech port for the broadcast.

To support broadcast of one-way, urgent VMI messages and to ensure that multicast traffic is routed correctly from the Vocera Voice Server to Vocera devices, use the following guidelines:

- Enable multicast routing support on the Layer 3 switches that the Vocera Voice Server subnet crosses.
- Check the IP multicast settings you enabled on the subnet that the Vocera devices use.
- Set the **Broadcast Uses IGMP** property to **TRUE** on all Vocera badges.
- Ensure 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. For more information, refer to Internet Group Management Protocol (IGMP) on page 20.

If multicast traffic is not routed properly, you will not receive audio packets during the broadcast of an urgent VMI message. For details on how to enable VMI broadcasts, refer to the Vocera Messaging Interface Guide.

To test the broadcast of a one-way urgent VMI message, perform the following steps:

1. Enable broadcast of urgent VMI messages by modifying the `properties.txt` file on the Vocera Voice Server. For more information, refer to 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 information on vmitest, refer to Vocera Messaging Interface Guide.

8. In the vmitest application, type **o** to open a gateway. Enter the client ID and then the Vocera Voice Server IP address.

   When the connection is opened **Accepted** message is displayed.
9. Type **m** to send a message. Enter the following parameter values:

Parameter	Value
Message ID	Specifies the message ID. A unique number.
Login ID	Specifies the login ID. For example: `Test`
Message Text	Specifies any message long enough to test the broadcast. For example: `Testing 1, 2, 3, 4`
Priority	Specifies the priority vales. For example: `urgent`
Call-back Phone No	Specifies the call-back phone number.
Response Choices	Specifies the response choice.
WAV File Root Names	Specifies the root name of the WAV file.

10. On the receiving end of the broadcast, the badges should play the alert tone for urgent messages. By default, two clunks are played.

    Broadcast being played on both badges.

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

Multicast Address Range

Vocera has a fixed address range to configure a multicast group. The Class D multicast address range for Vocera starts at 230.230.0.1 with 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 Vocera Voice Server and `\opt\vocera\server\Properties.txt` file on Vocera Platform 6:

- **IPMulticastRange**—Specifies the number of addresses in the range. The default address in the range is 4096.

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

Note: If you want to use the default range of 230.230.0.0 you do not have to update the server `Properties.txt` file.

Internet Group Management Protocol (IGMP)

IP networks use IGMP and PIM (Protocol Independent Multicast) to manage multicast traffic across Layer 3 boundaries. When IGMP is enabled on your network, routers and other network devices use it to determine the hosts in the domain that are interested in receiving multicast traffic.

The Vocera server assigns a multicast address to each broadcast session. The device registers to receive the stream and joins the group by sending an IGMP report to the upstream router. The router then adds that group to the list of multicast groups that should be forwarded onto the local subnet. IGMP allows the device to inform the router that it is interested in receiving a particular multicast stream. When a host no longer wants to receive multicast traffic, it sends the router an IGMP Leave message.

If IGMP is enabled on your network and you want to broadcast across subnets, you must also set the `B3.BroadcastUsesIGMP True` on the badge. Enabling this property allows a badge to register its membership in the appropriate multicast group to receive multicast traffic from other badges, also from another subnet. Vocera broadcast is implemented as IP Multicast. If broadcast commands must cross a subnet, IGMP must be supported in the switch, IP multicast routing on your router and PIM (Protocol Independent Multicast) on your VLANs.

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

When the badge property `V5.ForceIGMPVersion` is set, and if Vocera Smartbadge is configured to use IGMPv3, but your network only supports IGMPv2, the Smartbadge negotiates down to IGMPv2 and uses that with the network.

For more information, refer to Vocera Badge Configuration Guide.

Internet Group Management Protocol (IGMP) Snooping

IGMP snooping is a method wherein Switches, AP, and Controllers can listen in on IGMP messages between hosts and routers.

The Network Switches will 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.
To enable multicast features across subnet boundaries, perform the following steps:

1. Enable IGMP snooping for all Switches, AP, and Controllers . For example, switches and access points on each subnet used by the badge.
2. Enable IP multicast routing on all intermediate routers or other network devices on the Vocera subnets.
3. Enable PIM Sparse-Dense mode on all VLANs where the Voice traffic will traverse.

IP Addressing

Badges are most easily configured and administered as a group. Consequently, you should use a Dynamic Host Configuration Protocol (DHCP) server to assign IP addresses to the badges dynamically.

Ensure that you manually specify a default DHCP gateway in the **B3N.GatewayIPAddr** or **B3.GatewayIPAddr** property in the `badge.properties` file. Vocera uses this property for multicast sessions also when badges and the Vocera Voice Server are in the same VLAN.

Ensure that the DHCP uses the following values as part of the DHCP scope for Vocera that is configured in your corporate DHCP server:

- IP Address
- Subnet Mask
- Default Gateway

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

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

Note: For more information, refer to About Assigning Static IP Addresses in the Vocera Badge Configuration Guide.

Dynamic Host Configuration Protocol

Large networks often use multiple Dynamic Host Configuration Protocol (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, ensure that 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**.

An IPv4 DHCP client starts with device boots up and waits for instructions from the badge application.

On B3000n Badges, V5000 Smartbadges, and C1000 Minibadge DHCP time out value can be configured through badge property settings using the value `B3N.DhcpcTimeoutMS`, `V5.DhcpcTimeoutMS` and `C1.DhcpcTimeoutMS` respectively. The default DHCP retransmission timeout value is 200 ms.

This customization is made to achieve fast DHCP assignment when badge roams on call.

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 that conflict detection can be disabled.

VoIP over Wireless Network

Deploying Vocera into a wireless network requires you to configure settings on your network devices and properties on the Vocera badge. Also, you need to consider optional configuration options that may improve the performance, roaming, and security in the Vocera system.

This section provides details about the requirements and recommendations for deploying Vocera into your wireless infrastructure.

Wireless Connectivity Standards

Vocera uses the IEEE 802.11 to ensure seamless connectivity and reliable communication.

To understand 802.11, 802.11ac, 802.11b, 802.11d, 802.11g, 802.11h, 802.11n, 802.11k, 802.11r, and 802.11w, refer to https://standards.ieee.org/standard/802_11-2016.html.

Both the B3000n and B3000 automatically use the 802.11b and 802.11g data rates that are enabled on the access points. For optimal coverage, Vocera recommends that you enable 802.11g and 802.11a data rates per site. However, the implementation at each site varies based on the access point you use.

Note: B30000 does not support 802.11r and 802.11k.

To improve performance, roaming, and security, Vocera recommends that you also enable 802.11n, 802.11k, and 802.11r.

For more information, contact Vocera Customer Support.

Support for 802.11 Standards

The wireless protocols supported in the Vocera environment are listed in this topic.

The following table maps IEEE standard, frequency band to Vocera firmware, software, and supported devices:

IEEE standard	Frequency bands	Device and Vocera software
802.11a/n	5.0 GHz	B3000n, iOS, Android—Vocera Voice Server 4.4 and later V5000—Vocera Voice Server 5.0.0 and later
802.11b/g	2.4 GHz	B3000, B3000n, iOS, Android—Vocera Voice Server 4.1 and later V5000—Vocera Voice Server 5.0.0 and later
802.11k/r/w	2.4 and 5.0 GHz	B3000n—Vocera Voice Server 5.2.0 and later V5000—Vocera Voice Server 5.0.0 and later

Radio Resource Management: 802.11b/g/n and 802.11a/n

802.11b/g/n and 802.11a/n standards help in providing the best coverage in your Vocera wireless environment.

Cisco Wireless LAN Controllers provide advanced management capabilities for configuring and controlling Control And Provisioning of Wireless Access Points (CAPWAP). Among these features are Radio Resource Management (RRM) algorithms designed to automatically adjust power and channel configurations to mitigate adjacent and 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 with a minimum and maximum Transmit Power (Tx) power range, Tx power asymmetry can occur. Although the signal from access point can reach the badge, the signal from the badge may not be able to reach the access point. This may cause choppy audio or one-way audio on Vocera badge calls.

The B3000n badge, and iOS, 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 recommended Smartphones can be configured to use 802.11a/n only, 802.11a/b/g/n, or 802.11b/g/n. Vocera recommends that you avoid a deployment that requires inter-band roaming. Configure the B3000n badges to use either 2.4Ghz or 5Ghz. Vocera recommends that you do not use both the bands at the same time.

Note: Deploying any wireless voice requires a voice quality site survey to ensure proper performance.

To enable radio resource management, refer to Enabling 802.11 a/n/ac and 802.11 b/g/n on page 26.

Very High Throughput: 802.11ac

802.11ac is a wireless technology that represents the 5th generation of Wi-Fi technology and builds on the existing technology of 802.11n.

802.11ac provides high-throughput wireless local area networks (WLANs) on 5 GHz band. It is faster and delivers speeds ranging from 433 Mbps (megabits per second) up to several gigabits per second. Compared to 802.11n, 802.11ac offers better network performance and capability implemented through more advanced hardware and device firmware.

An essential feature of 802.11ac is the beamforming that is designed to increase the reliability of Wi-Fi connections in more crowded areas. Beamforming technology enables Wi-Fi radios to target signals in the specific direction of receiving antennas rather than spreading the signal across 180 or 360 degrees as traditional radios.

There are two versions of 802.11ac often refer to as Wave 1 and Wave 2. Wave 1 was introduced in 2013. It speeds up to 1.3 Gbps (Gigabits per second). Wave 2 was introduced in 2016 and speeds up to 2.34 Gbps with options of 160 MHz wide channel.

To enable assisted roaming, refer to Enabling 802.11ac on page 29.

Assisted Roaming: 802.11k

The 802.11k standards help in distributing traffic within a network. It provides radio resource measurements designed to allow a wireless client to request details of the neighboring access points.

Having a list of neighboring access points avoids active and passive scanning, and the device makes more informed roaming decisions, by discovering the best available access point.

For example, the 802.11k neighbor report provides measurements and information about nearby potential roaming points to the wireless client. An 802.11k client device can also determine whether an end-to-end link can carry a voice call reliably.

Note: Vocera highly recommends enabling 802.11k to advertise channels of both the band.

To enable assisted roaming, refer to Enabling 802.11k on page 30.

Fast Transition Roaming: 802.11r

The 802.11r standard is designed to permit continuous connectivity for devices in motion. 802.11r addresses the fast roaming and fast BSS transitions.

The key consideration is the roaming delay penalty imposed by the lengthy handshake between the supplicant, authenticator, and authentication server in WPA or WPA2 enterprise mode. 802.11r minimizes the loss of connectivity to the wireless distribution system during such BSS transitions, thus preventing degradation of voice quality.

To take advantage of 802.11r, your access points and B3000n badges must be configured to enable 802.11r. You can use a WPA2-Pre Shared Key passphrase, EAP-FAST, EAP-PEAP or EAP-TLS authentication. For more information on how to configure badges for 802.11r, refer to Vocera Badge User Guide.

Note: B3000n badges support 802.11r over-the-air or over-the-DS (Distribution System). Select the corresponding options on the AP and badge properties accordingly. V5000 Smartbadge does not support FT-Over DS roaming when using 802.11r roaming; it supports over-the-air roaming.

To enable fast transition roaming, refer to Enabling 802.11r on page 30.

Protected Management Frames: 802.11w

The 802.11w standard is a security feature that supports protected management frames.

With security breaches and other attacks designed to access sensitive data, it is necessary to protect management frames in a wireless environment. Management frames are normally not encrypted since they contain information about data and therefore must be heard and understood by all clients.

Note: It is difficult to troubleshoot security of encryption-related issues if the management frames are encrypted. Enable 802.11w security on the badge only if there is a client requirement.

The 802.11w security standard is designed to prevent things like denial-of-service, man-in-the-middle, and dictionary attacks.

802.11w management works with roaming. However, 802.11w must not be enabled with OKC.

To enable protected management frames, refer to Enabling 802.11w on page 32.

BSS Transition Management: 802.11v

802.11v is the Wireless Network Management standard for the IEEE 802.11 family of standards.

Vocera devices use idle period to ensure that they remain connected to access points. Therefore consume power when trying to search for Access Points in a wireless network. The 802.11v transition improves throughput, data rates and QoS for the voice clients in a network by transitioning the individual voice traffic loads.

Vendor Configurations Overview

For seamless connectivity and reliable communication, 802.11 standards are used. This section addresses only the configuration parameters that are particular to a Vocera deployment in a CAPWAP architecture.

Note: To configure 802.11 on Vocera, your network must have the corresponding configuration completed in the SSID where Vocera devices are used.

For more information on Cisco Wireless Control System (WCS), Cisco Prime, or the Cisco Wireless LAN Controller (WLC), refer to Cisco Systems documentation.

Enabling 802.11 a/n/ac and 802.11 b/g/n

802.11 a/n/ac and 802.11 b/g/n helps reduce the power of a radio transmitter to the minimum necessary to maintain the link with a certain quality.

This section provides the best practice To configure 802.11b/g Global Parameters, Tx Power Control (TPC), and Coverage on 802.11a/n/ac or 802.11b/g/n on a Cisco Unified Wireless Network for the Vocera VLAN. You must design your wireless network taking into account wireless clients with lower capabilities to ensure that all device types are accommodated. For more information on Tc Power, refer to Power on page 52.

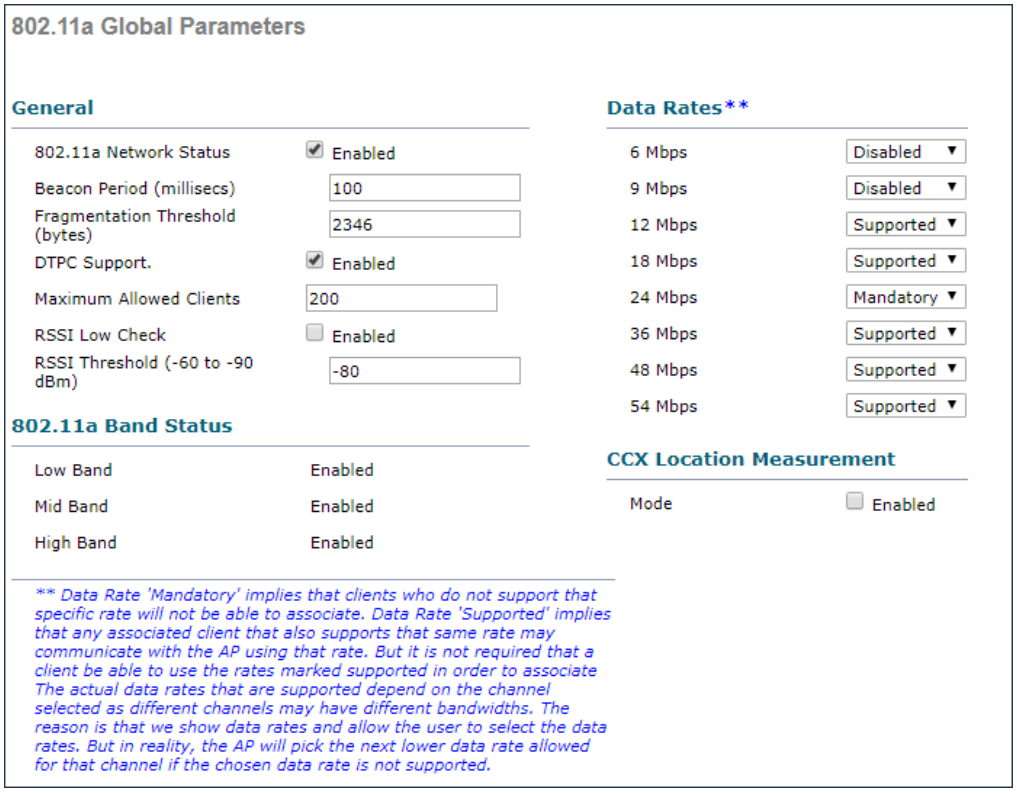
Note: Update the Cisco WLAN Controller software to the most recent version available. For more information on the latest recommendations on Cisco WLAN Controller software versions, contact Vocera Technical Support. If you are running the Cisco Wireless LAN Controller, you can use RRM by specifying maximum and minimum power level assignments.

Note: The steps to configure 802.11a/n/ac or 802.11b/g/n are the same. One of the options is used as an example in the screenshot

Global Parameters Settings

To configure global parameters for 802.11 a/n/ac or 802.11 b/g/n, perform the following task:

1. Click **Wireless** to access the All APs page.
2. Navigate to **802.11 a/n/ac** or **802.11 b/g/n** >**Network**.
   802.11a Global Parameters or 802.11b Global Parameters page appears.
3. Select data rates that are supported.
   The following screenshot provides the parameters that must be enabled.

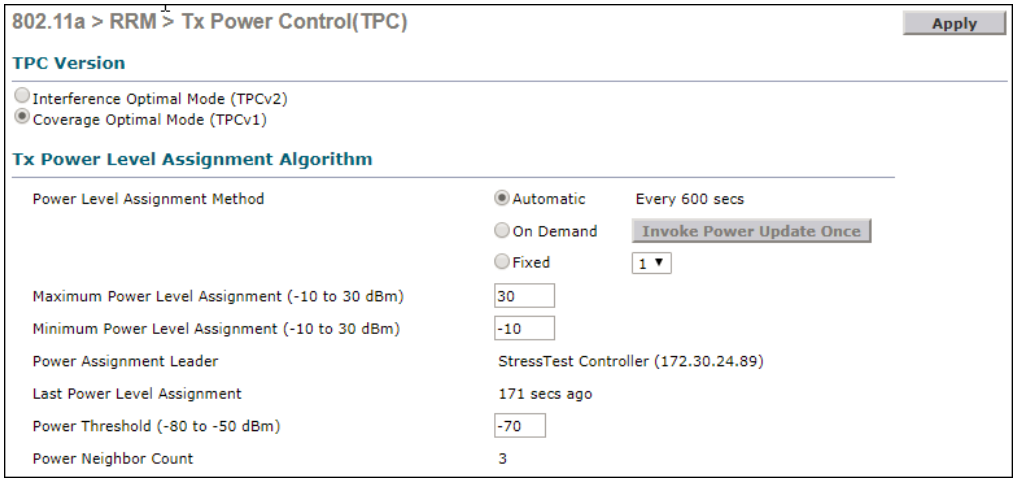


4. Disable lower data rates for maximum reliability. You must enable one Mandatory higher data rate. Data rates are selected based on sites.
5. Perform a **voice quality** site survey to ensure proper network coverage before installing Vocera.
6. Click **Apply**.
   Your changes are committed.

Tx Power Control Settings

To configure Tx Power control using 802.11 a/n/ac or 802.11 b/g/n, perform the following task:

1. Click **Wireless** to access the All APs page.
2. Navigate to **802.11 a/n/ac** or **802.11 b/g/n** >**RRM**>**TPC**.
3. Under **Tx Power Level Assignment Algorithm**, select the following options:



- **Power Level Assignment**—Automatic.

Note: Vocera does not recommend **Fixed** Power Level Assignment Method. However, if a static power is desired, a static power assessment is required, and power levels should be in the range recommended by Vocera. For more information, refer to the Cisco documentation for the maximum transmit power levels settings of your access points.

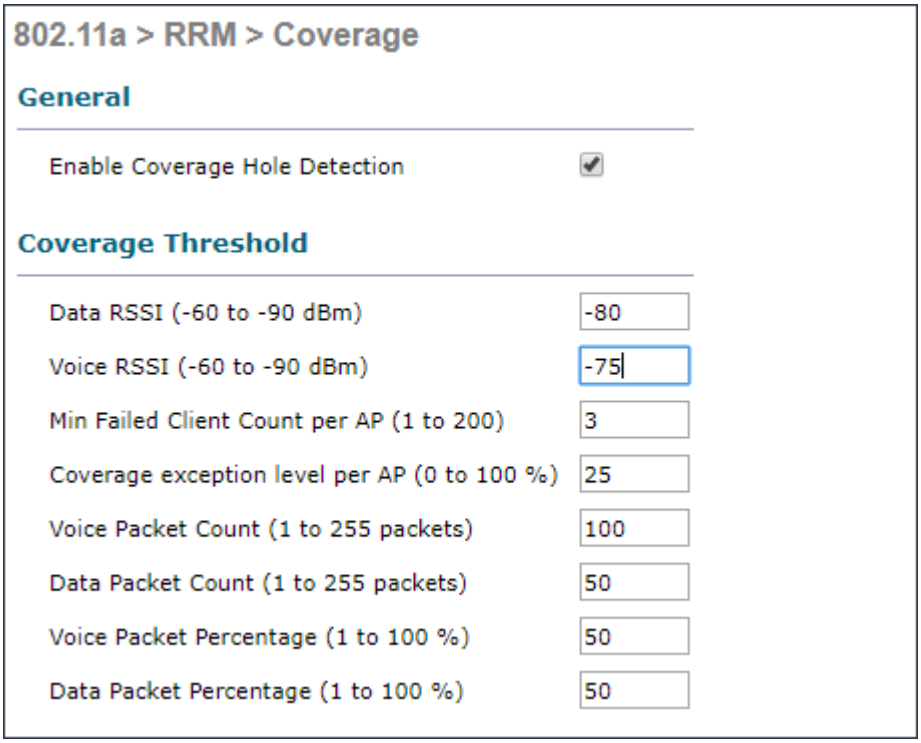
- **Power Threshold (-80 to -50 dBm)**— -70dB.
  Power changes are only made when an AP's third loudest neighbor is heard at a signal level higher than the default value of -70 dBm.

4. Click **Apply**.
   Your changes are committed.
5. Click **Save Configuration**.
   Your changes are saved.

Configuring Coverage

To configure coverage using 802.11 a/n/ac or 802.11 b/g/n, perform the following task:

1. Click **Wireless** to access the All APs page.
2. Navigate to **802.11 a/n/c**>**RRM** >**Coverage** or **802.11 b/g/n**>**RRM** >**Coverage** page as shown in the following screenshot.



3. Specify the following settings for the **Coverage Hole Algorithm**.
   - **Voice RSSI (-60 to -90 dBm)**—**-70**.
   - **Min Failed Client Count per AP**—**12**.
4. Click **Apply**
   Commits your changes.
5. Click **Save Configuration**
   Saves your changes.

Note: Wait for at least 60 minutes after enabling dynamic power level assignment to allow the WLAN to stabilize.

Each WLAN has its 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.

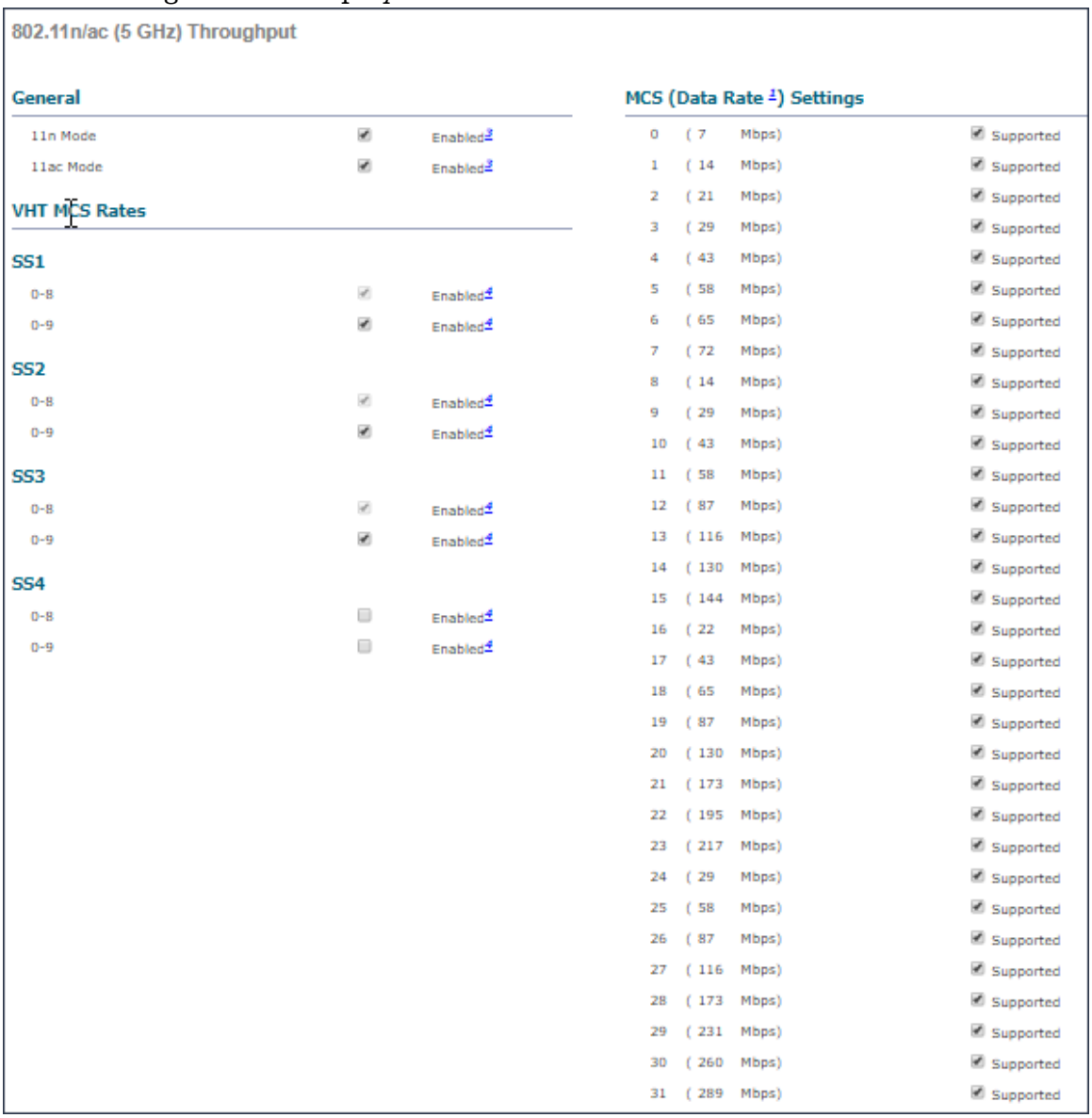
6. Verify AP transmit power levels and coverage.

Enabling 802.11ac

802.11ac on Cisco access points enable or disable support of the different modulation coding scheme (MCS) settings. The MCS settings determine the number of spatial streams, modulation, coding rate, and data rate values.

To enable 802.11ac for Cisco CAPWAP access points, perform the following steps:

1. Select **Wireless**>**802.11 a/n/ac**>**High Throughput (802.11n/ac)** on the Cisco WLC Web User Interface.
   The following screen is displayed.



2. Select **General**> **11ac Mode**.
   802.11 ac mode is enabled.

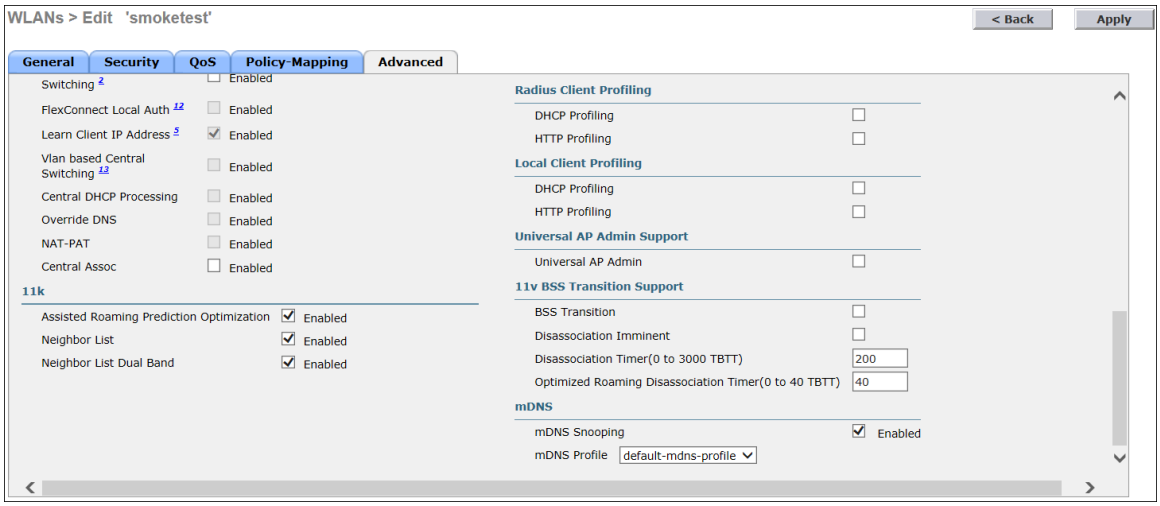
For more information, refer to Cisco Wireless LAN Controller (WLC) Configuration Best Practices .

Enabling 802.11k

802.11k on Cisco access points may help improve roaming on the Vocera Wireless environment.

To enable 802.11k, perform the following steps:

1. Click **Wireless** to access the All APs page.
2. Select one of the SSID.
   WLANs > **Edit SSID** page is displayed.
3. Click **Advanced**.
4. Under **11k** enable the following options.



- Assisted Roaming Prediction Optimization
- Neighbor List
- Neighbor List Dual Band

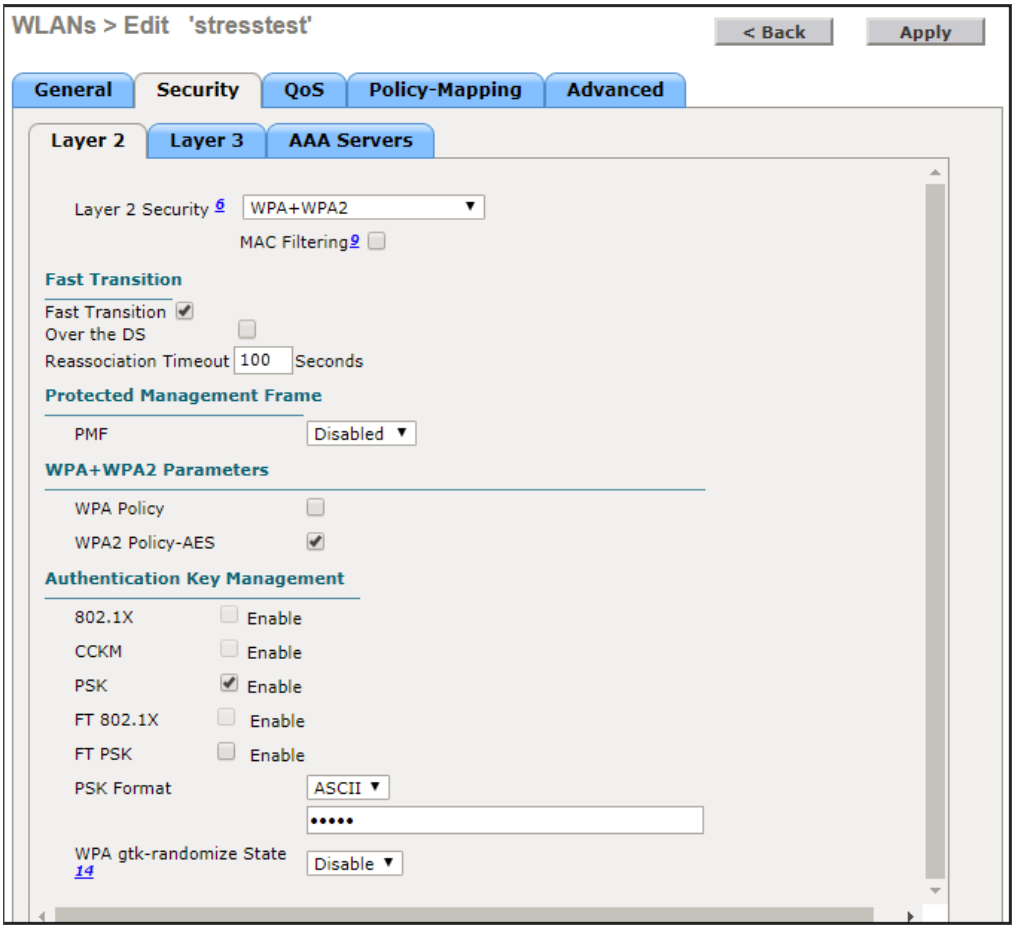
For more information, refer to Cisco Wireless LAN Controller (WLC) Configuration Best Practices .

Enabling 802.11r

802.11r on Cisco access points improves roaming for Cisco access points in the Vocera Wireless environment.

To enable 802.11r for Cisco CAPWAP access points, perform the following steps:

1. Select **WLANs>Security>Layer 2** on the Cisco WLC Web User Interface. The following screen is displayed.



2. Enter the following controls, for Layer 2 tab:
   - **Layer 2 Security**
     - Select **WPA+WPA2**
   - **Fast Transition**
     - **Fast Transition** —Enable
     - **Reassociation Timeout**—100 seconds.
   - **Protection Management Frame**
     - PMF—**Disabled**.

     Note: If you are enabling 802.11w on B3000n, this value should be set to **Optional** or **Required**.
   - **Authentication Key Management**
     - Enable **FT 802.1x** if you are using WPA-PEAP, EAP-FAST or EAP-TLS,
     - Select **FT PSK** if you using a pass-phrase key.
3. Select **WLANs>Security>AAA Servers**.
4. Select **Enabled** under **Authentication Server** and **Enabled** under **Accounting Servers** to be use with this WLAN profile.
5. Click **Apply**.

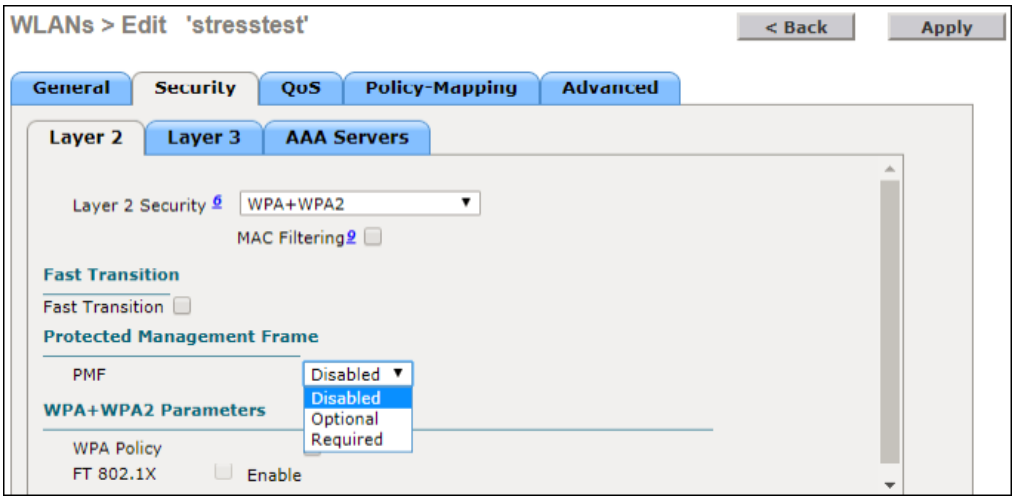
To enable CCKM for autonomous APs, refer to Cisco IOS Configuration Guide .

Enabling 802.11w

802.11w protected management frames improves roaming in the Vocera Wireless environment.

To enable 802.11w for Cisco CAPWAP access points:

1. Select **WLANs**>**Security** >**Layer 2** on the Cisco WLC Web User Interface.
2. On the Layer 2 tab, provide the following controls:
   - Select **Optional** or **Required** in Protected Management Frame.



Protected Management Frame is enabled.

Bluetooth and Wi-Fi Co-existence

Modern Wi-Fi operates in two sections of the radio spectrum, 2.4 GHz, and 5 GHz. Bluetooth also uses the 2.4 GHz spectrum, and this can add to the congestion encountered in the 2.4 GHz spectrum.

Because many communication products support both 2.4 GHz Wi-Fi and Bluetooth, using a single antenna to reduce overall size, a co-existence strategy is implemented by each product. The Bluetooth radio and the Wi-Fi radio access the antenna alternatively to transmit or receive Wi-Fi or Bluetooth signals, it is not possible for both the Bluetooth radio and the Wi-Fi radio to utilize the same antenna simultaneously.

Due to this co-existence, when a Bluetooth headset is used with a Wi-Fi device operating in the 2.4 GHz spectrum, there may be some disruption to audio quality as they can interfere with one another. When Bluetooth is enabled, deterioration of audio quality during badge to badge communication may not be noticeable when compared to the scenario where the badge is a multicast recipient. Audio quality is likely to minute interruptions as the WiFi, and Bluetooth radios alternate the use of the onboard antenna.

It is recommended that the Vocera badge is operated in the 5 GHz spectrum when you use Bluetooth headset to avoid the limitations of co-existence. The single antenna can simultaneously support Wi-Fi and Bluetooth operation if they are utilizing different radio frequencies.

Wi-Fi Connectivity Planning

This section describes all the parameters required for Wi-Fi connectivity.

Channel Utilization

Channel utilization is statics that represents the airtime utilization of a particular frequency or channel. The higher the channel utilization, more the traffic transmission. For the best performance of the device, it is recommended that the channel utilization is less than 30%.

802.11a offers at least 25 20 MHz non-overlapping channels on 5 GHz with the US-B domain.

Many products such as Bluetooth, wireless phones, and surveillance cameras use the 2.4 GHz frequencies. The 2.4 GHz band is hence overused and has channel allocation constraints. Vocera recommends that you must consider using the 5 GHz Wi-Fi band for new badge deployments.

Channel Separation

The IEEE 802.11b/g ISM band have 14 channels with a width of 22 MHz. The bands must have a channel separation that helps to transmit signals from the adjacent APs to use non-interfering channels.

For example channel 1, 6, and 11 with a separation of 25 MHz are non-overlapping. This channel separation governs the use and allocation of channels in a multi-AP environment. Adjacent APs are allocated non-overlapping channels.

Channel separation for 2.4 GHZ

You can improve the performance of the Vocera badges by configuring them to scan only channels 1, 6, and 11. Channels 1, 6, and 11 are the only WiFi channels that do not overlap with one another and hence minimizes reconnect time while roaming.

To specify the default channels to be scanned, use the **Wireless Properties** section of the Badge Properties Editor for all Badges. In the `badge.properties` file, ensure that you have set values for both `B3.ChannelsToScan` and `B3N.ChannelsToScan`. For more information, refer to the Vocera Device Configuration Guide.

Following is a simplified illustration of access points map in a network using channels 1, 6, and 11 only. The access point map do not have a constant radius, but have irregular coverage cell, due to environmental factors.

Channel separation for 5 GHZ

By default, the B3000n scans all 23 channels at 5GHz, which is time-consuming and inefficient. B3000n does not support US-B domain channels.

To specify the 5 GHz channels to be scanned, use the **Wireless Properties** section of the Badge Properties Editor for all badges. In the `badge.properties` file, ensure that you have set the value for `B3N.ChannelsToScan5G`. For more information, refer to the Vocera Badge Configuration Guide.

Following is a simplified illustration of access points in a network using 23 channels.

Note: For 2.4 GHz, if no channels are configured then badge uses default 1,6,11. For 5 GHZ, all DFS and non DFS channels for the relevant country code are used.

For further recommendations on specifying 5GHz channels, refer to Cisco Enterprise Mobility 8.1 Design Guide VoWLAN Design Recommendations.

Note: Device perform passive scan on all DFS channel. Vocera recommends that you use non-DFS channels.

Channel Scanning

802.11b/g/n radios scan in the 2.4-GHz spectrum and 802.11a/n radios scan in the 5.15 GHz spectrum.

Following are the types of scanning performed:

- Proactive scan—A periodic scan during active state to learn about the cache of nearby APs.
- Roam scan—A scan performed in response to a roam trigger (low RSSI, Tx Fa, beacon loss). The goal of this scan is to look for a better AP to roam. Roam scan is performed every 5 seconds when the badge RSSI is below roam threshold. This applies to both standby and voice.
- Off campus scan—A scan performed by a device in a disconnected state.
- Multiple profile scan—A scan that enables you to configure multiple profiles, such as SSIDs, encryption, and so on in the badges and enable auto-connect to different profiles.

Following are the states in which scanning is performed:

- Disconnected State—Roam scan is performed in the disconnected state. During the disconnected state, contiguous scanning is performed. The scan is performed on all the channels configured on the selected bands.
- Standby—During the standby state, scanning is performed when an event is triggered by the driver.
- In Call—Roam and Proactive are performed during in-call state. The actions taken are:
  - Periodic proactive scan for cached details when an event is triggered by the driver. Periodic proactive scan is performed every 10sec when RSSI value is above the roam threshold.
  - Interleaved scan as and when required.
  - Channel-by-channel scan for an active scan on non-DFS channels.
  - Passive scan on DFS channels based on the configuration.

Channel Interference

The performance of your network is affected by the 802.11 interference caused by intruding radio signal that 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. Access points that are not part of the network can also cause interference. Interference decreases the signal-to-noise ratio (SNR) for data rates. For more information on SNR, refer to Acceptable Voice Quality on page 64.

Interference can affect any 802.11 transmission 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.

Under the 802.11b/g standard, a transmission on one channel can interfere with transmissions as far as four channels away. 802.11b/g signal on channel 1 can cause channel with a transmission on channels 2, 3, 4, or 5. The channel interference concerning Vocera system are adjacent-channel interference and co-channel interference.

Adjacent-Channel Interference

Adjacent-channel interference is the interference caused by power from a signal in an adjacent channel. In this case, every client and access point on overlapping channels talk over each other. If the radio channels in nearby access points are not separated from each other by five channels, an adjacent channel interference occurs. You can mitigate this issue by separating the access point by five channels.

In the United States, you must use channels 1, 6, and 11. There is flexibility for channel selection in an 802.11b/g network in Europe, where channels 1 through 13 is 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 on working with locales, refer to the appendix in the Vocera Voice Server Installation Guide.

Co-Channel Interference

Co-channel interference is a crosstalk between two radio transmitters using the same frequency. Co-channel interference occurs when access points on the same channel competes for time to talk. 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.

Note the details 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 the access points.

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.

For a network to provide continuous coverage over a large area, access points must be placed fairly close. 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.

Vocera recommends moving to 5 GHz (if your network is designed for it) to mitigating CCI.

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 moving around 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 to ensure 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. Adequate cell overlap is required for smooth Basic Service Set (BSS) transitions.

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.

Overlapping cells on the same channel result in:

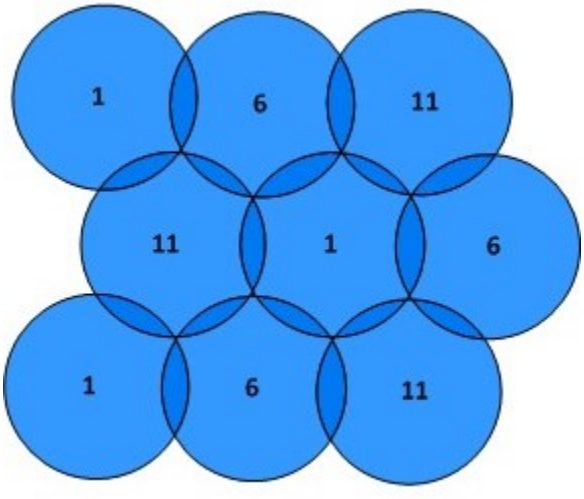
- Interference and dropped packets
- Shared network bandwidth
- Increase in noise flow
- Decrease in signal-to-noise ratio (SNR)

Overlapping Cells and Data Rates

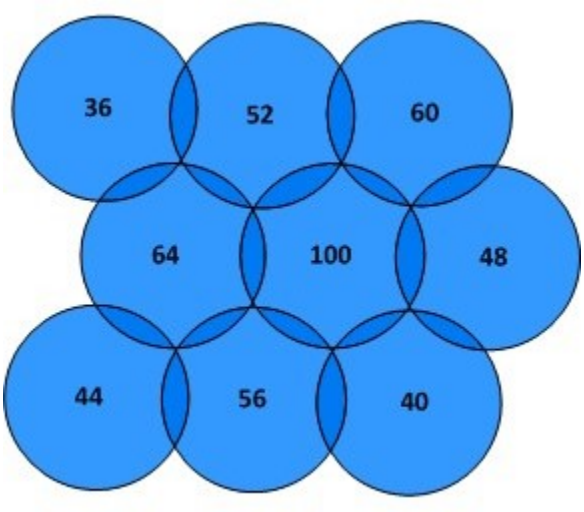
The 802.11b/g standard provides the data rates, 1, 2, 5.5, 11, 54, 48, 36, 24, 18, 12, and 6 Mbps.

Enabling all 802.11b/g data rates allow a client to maintain a connection by switching among data rates. The badge can move farther away from the current access point and stay connected at a lower data rate. It also minimizes the instances of losing the connection and dropping packets.

The following illustration shows the 2.4 GHz spectrum.



The following illustration shows 5 GHz band, with 20 MHz channels partially overlap. In addition, there are 25 channels with -B domain to use. This ensures that the same channels cells are not used.



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. You may need to change the basic data rates to higher rates in an environment with location-based services.

Data networks have more tolerance for dropped packets than voice networks. Lost packets show up as dropouts or choppy audio.

Capacity Planning

Capacity refers to the maximum number of device-to-device calls a specific access point can support simultaneously. The ability 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 processes exceeds its capacity. High traffic areas may require more access points than low traffic areas to prevent flooding.

For example, you may need to provide additional access points in places such as break rooms or nursing stations, if device users frequent these areas. Monitor user traffic patterns when you update your site survey to accommodate the Vocera system.

Vocera usage pattern is not similar to that of a conventional telephone. Vocera calls are typically brief because Vocera calls are short and there is less probability of many users being on calls simultaneously, exceeding the capacity of an access point.

Introducing additional access points to a network, create new problems, such as choppy audio due to interference with existing access points.

Smartphone with VCS enabled on it sends more packets per second than Vocera devices. While planning capacity for high traffic areas, note that it requires more overhead to transmit sound.

The following table displays the 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 and Platform 6.x	B3000n/B3000/ V5000/C1000	G.711	64 Kbps	20 ms	50
	Smartphone	G.711	64 Kbps	20 ms	50

The following table shows the recommended maximum number of device and smartphone calls with acceptable voice quality supported by a wireless test network. Results may vary based on your wireless network and 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.

Wireless Band	Device	Max Calls Per AP	Max Devices on Calls Per AP
2.4GHz	B3000n/B3000/Smartphone	8	14
5GHz	B3000n/B3000/V5000/ Smartphone	18	30

Capacity Setting

Some access point models have a capacity setting that limits the number of clients that can be connected to the access point. This setting is called MaxClients.

The maximum number of calls that an access point can handle is independent of the maximum number of devices accepted on an access point.

When the maximum number of clients is reached, additional badges or other clients cannot connect to the access point. They are forced to connect to a less populated and 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 Wi-Fi Multimedia (WMM) is enabled in the Wireless Controller, the Quality of Service enhanced Basic Service Set (QBSS) is advertised in the beacons. You can use this value as a reference to measure radio utilization.

Access Points

Vocera supports both Autonomous and Lightweight APs.

Autonomous access points are useful in smaller deployments but typically lack the centralized configuration management needed for a large-scale enterprise WLAN deployment. Lightweight access points are centrally configured and controlled by a WLAN controller. Ruckus Wireless offers wireless solutions with autonomous access points. For more information, refer to Ruckus Networks on page 61.

Cisco Systems offers several models of CAPWAP access points with WLAN controllers, that are part of Unified Wireless Network architecture. CAPWAP is based on LWAPP (Lightweight Access Point Protocol) which is a standard, interoperable protocol that enables a controller to manage a collection of wireless access points. For more information about the Cisco Wireless Control System (WCS), Cisco Prime, or the Cisco Wireless LAN Controller (WLC), refer to the Cisco Systems documentation.

Access Point Settings

Vocera requires specific access point settings and configuration recommendations to optimize wireless communication in your environment.

The following table displays the AP settings required for Vocera.

AP Feature	Setting
Beacon Interval	The typical default beacon interval is **100 milliseconds**. For more information, refer to Beacon and Delivery Traffic Indication Map Intervals on page 39.

AP Feature	Setting
DTIM Interval	The default DTIM interval is **1**. For more information, refer to Beacon and Delivery Traffic Indication Map Intervals on page 39.
Data Rates	Enable data rate as per the requirement of your site. For more information, refer to Data Rates on page 40.
SSID	Vocera recommends no more that 5 SSIDs. For more information, refer to SSID on page 40.
Security Settings	Vocera devices support many security types. For more information, refer to Security on page 43.
Peer-To-Peer Communication	For Vocera devices to work properly set the value to **enabled** on the access point or on the WLAN controller. For more information, refer to Peer-To-Peer Communication on page 41.
Encryption	Vocera supports many encryption types. For more information, refer to Authentication Overview on page 47 for the best performance.
Channel Utilization	Radio Channel Utilization should be consistently less than 30%. For more information, refer to Channel Utilization on page 32.
Channel Width	The channel width used are as follows: For B3000n badge • 2.4GHz—20 Mhz • 5 GHz—20Mhz or 40Mhz For V5000 Smartbadge • 5 GHz—20MHz, 40MHz, or 80MHz For C1000 Minibadge • 5 GHz—20MHz, 40MHz, or 80MHz Vocera recommends 20 MHz.

Beacon and Delivery Traffic Indication Map Intervals

Beacon is a special management frame broadcast by an AP at a fixed interval. The transmission is an announcement of the presence of a wireless network. Delivery Traffic Indication Map (DTIM) is the additional information added by your access point after a beacon broadcast.

The DTIM interval and beacon intervals determine 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.

Important: Broadcast the Vocera SSID in beacons for B3000n badge when you use Dynamic Frequency Selection (DFS) channels.

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

The speed at which data is transferred between devices in a network is called data rate. It is measured in megabits per second. You can configure the data rate settings of an access point to choose the data rate it uses for transmission.

Data rates selection is based on sites and Access Point density. You can set each data rate to one of three states:

- **Supported**—The access point transmits only unicast packets at this rate.
- **Mandatory**—The access point transmits at mandatory rate for management, broadcast frames and data frames. Multicast packets are sent at one of the mandatory data rates. Also, mandatory data rate is set per site.
- **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. For more information, refer to Multicast Transmissions on page 18. Management packets, which can be transmitted only at basic rate, are usually transmitted at the highest basic rate.

Data Rate Recommendations

Vocera recommends enabling lowest g rates as mandatory. Enabling rates allows a device to shift to different rate for a more reliable transmission. Devices rely on data rates to receive beacons.

When designing a network to support WLAN devices, industry best practices encourage enabling higher 802.11 basic data rates (12 and 24 Mbps optimal) and removing support for lower rates (1, 2, 5.5,11 Mbps). If you absolutely need to enable b data rates, configure your 802.11 beacons for 11 Mbps, when your AP or controller solution allows it.

Note: Having lower data rates enabled can have negative impact.

Low-speed frames, for example, 1 and 2Mbps decrease the overall throughput of your wireless network. As you add APs and devices to your wireless network, ensure that you recheck channel utilization so that it stays within acceptable level of 30%. For more information, refer to Overlapping Cells and Data Rates on page 36.

Important: Your RF site survey must reflect the lowest 802.11 basic rate you have configured. Remember that if you increase the 802.11 data rate to basic or beacon rate without a site survey, it can create coverage holes in your deployment.

Industry best practice: To support voice over WiFi enable data rates 11 Mbps and 12 Mbps depending on your site.

SSID

Service Set Identifier (SSID) is a unique 32-character ID used for naming a wireless network. Each packet sent on the network contains an SSID to ensures that data is sent to the appropriate destination. When multiple wireless networks overlap in a certain location, delivering packets to the correct destination is not possible without SSIDs.

You can use the Badge Properties Editor (BPE) to specify properties for all Vocera badges.

For more information on configuring badge security, refer to Vocera Device Configuration Guide.

Adding Badge Property for Profile Recovery

Vocera recommends enabling a recovery SSID in case production SSID fails or the authentication server has some issues like while using 802.1x authentication (EAP-FAST/PEAP/EAP-TLS). This recommendation is applicable only for B3000n and V5000 badges.

The prerequisites to adding a badge property for profile recovery are:

- VS 5.2.2 or higher
- BCU 5.2 or higher
- B3000n—Firmware 4.3.0.34 and higher

To enable recovery SSID, create a secondary SSID utilizing the multiple profile feature of Vocera Badges. The recovery SSID must be configured with WPA-PSK authentication for the Badge to connect when the primary SSID is down or not able to authenticate. The SSID profile is activated in the `Profiles.txt`, but the recovery SSID on the Controller need not be enabled until needed.

To create recovery SSID, perform the following tasks:

1. Locate and double-click the Vocera BPE Launcher icon on the desktop.
   The Badge Properties Editor UI appears.
2. Select **B3000n** or **V5000** under **Badges**.
   The B3000n/V5000 page appears.
3. Set the following badge property values for your badge:
   - **Profiles**—Select **Create New Profile** and enter a profile name.
   - **General Settings**—Enter **Server IP** and **SSID** for the Badge to connect.
     SSID is the recovery SSID. For example, `VCRA`.
   - **Security Settings**—Select **Authentication type** as **WPA-PSK**, encryption type as **AES-CCMP**, and enter **WPA Passphrase** to match SSID settings on WLC/AP.
   - **Wireless Settings**—Enter the wireless band settings to match the WLC WLAN settings.
4. Click **Submit**.
   The changes are saved.

Peer-To-Peer Communication

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 Vocera WLAN to allow badges to communicate with each other when they are connected to the same access point.

Roaming

Roaming refers seamless movement of a device from one access point to another.

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

If WiFi Multimedia (WMM) and QOS enhanced Basic Service Set (QBSS) are enabled, the B3000n Badge takes advantage of channel utilization and QBBS load information so that SNR (Signal Noise Ration) makes better informed roaming decisions.

If you have only B3000 Badges, test your cell transition zones carefully, and ensure that one access point 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.

For more information on assisted roaming and fast transition roaming, refer to Assisted Roaming: 802.11k on page 25 and Enabling 802.11r on page 30 respectively.

Optimum Roaming

For optimum roaming, 802.11k neighbor list feature must be enabled on the AP infrastructure. If you are using 802.1x profile, then 802.11r or OKC must be enabled on the AP infrastructure.

Radio has inbuilt algorithms to optimize the scan channel list to ensure scans are as efficient as possible.

Vocera also recommends using the `ChannelsToScan` badge property to limit the fulls cans performed by the Vocera device. ChannelsToScan is a combined list of 2.4 and 5ghz channels. By default, the Vocera device uses channels 1,6,11 if this property is not specified. All supported 5ghz channels, including DFS channels are scanned. For more information, refer to the Device Configuration Guide.

Roaming Policy Property

The roaming policy property determines how aggressively the device attempts to roam as the signal-to-noise (SNR) ratio of the transmission from an access point deteriorates.

The device assesses the SNR in terms of the SNR metric. For more information, refer to Acceptable Voice Quality on page 64. The device 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 5, where 1 specifies the least aggressive roaming and 3,4, and 5 are the most aggressive. By default, the roaming policy for B3000n is 2 and V5000 is 3 meaning the Vocera devices roam when the SNR falls below 20dB or RSSI falls below -70dB respectively.

The following table shows the relationship between device SNR values and roaming policy. It also provides the typical SNR values at which the device initiates roaming. Vocera recommends that you set the roaming policy property on Vocera devices to a value that is appropriate for your RF cell size.

Roaming Policy Value	Typical B3000n/B3000 SNR when Roaming	Typical V5000 RSSI when Roaming	Description
1	18	- 75 dB	The lowest value used since voice quality is maintained when roaming is initiated.
2	20	- 73 dB	The device initiates roaming while voice quality is good on most networks.
3	22	- 70 dB	The default value that 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. For information about data rates, refer to Overlapping Cells and Data Rates on page 36.
4	24	- 65 dB	This value initiates very aggressive roaming behavior and would not be used normally in a typical deployment.

Roaming Policy Value	Typical B3000n/B3000 SNR when Roaming	Typical V5000 RSSI when Roaming	Description
5	26	- 60 dB	This value represents the highest available policy value and should be used only in conjunction with guidance from Vocera Technical Support when investigating roaming performance.

Note: The actual SNR values may vary slightly, due to environmental factors and dynamic changes in coverage.

If you are not satisfied with the roaming behavior of the device and want to adjust the roaming policy property, contact Vocera Technical Support.

To specify the roaming policy property, use the Badge Properties Editor (BPE) to set the roaming policy property to the appropriate value on all badges. For more information on setting roaming policy, refer to Vocera Badge Configuration Guide.

Layer 2 Roaming

Layer 2 roaming is a process when a client roams between two APs registered to two different controllers, where each controller has an interface in the client subnet. Layer 2 roaming is also known as intercontroller roaming.

Vocera supports layer 2 roaming and 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. This authentication adds time to the hand-off, and can potentially result in dropped packets that are noticeable as audio glitches or choppy speech. For more information, refer to Security on page 43 for complete information.

Smartphones and Subnet Roaming

VCS runs on Smartphones such as Zebra MC40 or TC51 smartphone cannot change the IP address mid-stream when moving from one AP to another on different subnets.

If you deploy 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 Smartphone can roam across subnet boundaries while maintaining its original IP address.

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.

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.

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.

An 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 WPA2-AES-CCMP 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.

For Vocera devices to roam faster, use 802.11r, Opportunistic Key Caching (OKC), and Cisco Centralized Key Management (CCKM), which is available for authentication between multiple APs with cached credentials.

This section describes security support provided by Vocera and discusses the network overhead introduced by various security methodologies.

Security Terminologies

The wireless security terminologies that are covered in this section are listed in this topic.

The following table describes the abbreviations used in the security section.

Abbreviation	Expanded Form	Description
Authentication		
EAP	Extensible Authentication Protocol	An authentication framework used in wireless networks and point-to-point connections.
WPA	Wi-Fi Protected Access	A security standard used for computing devices with wireless internet connections.
WEP	Wired Equivalent Privacy	A security standard that encrypts transmitted data. It is used to provide data security. WEP has the following settings: • Off—Provides no security • 64-bit—Provides less security • 128-bit—Provides better security
PSK	Pre-Shared Key	A client authentication method used for WPA and WPA2 encryption. It uses a string or a passphrase to generate unique encryption keys for each wireless client.
PEAP	Protected Extensible Authentication Protocol	A WPA authentication type that transports secure authentication data including legacy password-based protocols. PEAP accomplishes this by tunneling between PEAP clients and an authentication server.
FAST	Flexible Authentication via Secure Tunneling	An EAP authentication type developed by Cisco. Mutual authentication is achieved by means of a PAC that can be managed dynamically by the authentication server.
TLS	Transport Layer Security	An EAP authentication type that provides certificate and mutual authentication between the client and the network to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.
Authentication Support		
CA	Certificate Authority	An entity that issues digital certificates. A digital certificate contains the public key of the owner.
NIST	National Institute of Standards and Technology	A measurement standards laboratory and a non-regulatory agency of the United States Department of Commerce.
PAC	Protected Access Credential	Strong shared secret key that enable the ACS and an EAP-FAST end-user client to authenticate each other and establish a TLS tunnel.
Encryption		
TKIP	Temporal Key Integrity Protocol	An encryption protocol used as part of the 802.11i to boost the encryption strength.
AES	Advanced Encryption Standard	A symmetric-key algorithm that uses the same key for encrypting and decrypting data.
CCMP	Cipher Block Chaining Message Authentication Code Protocol	An enhanced data cryptographic encapsulation mechanism for secure data.
Roaming		
CCKM	Cisco Centralized Key Management	A form of fast roaming supported on Cisco infrastructure and on wireless networks.

Abbreviation	Expanded Form	Description
WDS	Wireless Domain Service	A feature required for a network with many AP. It enables connection between APs in a network.
OKC	Opportunistic Key Caching	An authentication technique between multiple APs in a network where the APs are under common administrative control.
PMK	Pairwise Master Keys	An 802.1x authentication process that allows skipping the EAP exchange while roaming between APs.
FT	Fast transition	A form of roaming, also called fast roaming permits continuous connectivity aboard wireless devices in motion, with fast and secure handoffs from one base station to another managed in a seamless manner.

Security Support

Vocera supports industry standard security systems as well as popular proprietary security methods such as EAP-TLS and WPA-PEAP.

The following table summarizes the security support in Vocera.

Authentication	Encryption	C1000 Support	V5000 Support	B3000n Support
Open	None WEP64 WEP128 **Note:** Vocera recommends that you do not choose encryption TKIP and AES in the same WLAN.	Yes No No	Yes No No	Yes Yes Yes
WPA-PEAP WPA-PSK EAP-FAST EAP-TLS	TKIP-WPA TKIP-WPA TKIP-WPA TKIP-WPA	No No No No	No No No No	Yes Yes Yes Yes
WPA-PEAP WPA-PSK EAP-FAST EAP-TLS	AES-CCMP AES-CCMP AES-CCMP AES-CCMP	Yes Yes Yes Yes	Yes Yes Yes Yes	Yes Yes Yes Yes

Note: In order to support 802.11n data rates, you must configure the B3000n to use AES-CCMP. For additional information, refer to Vocera Device Configuration Guide.

The 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 that the Vocera Voice Server can automatically update all badges when necessary. Consequently, Vocera supports device authentication for WPA-PEAP, EAP-FAST, and EAP-TLS, not user authentication.

Vocera recommends that all badges use the same set of credentials for network authentication. However, device authentication also support unique certificates for each badge when EAP-TLS is used.

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.

The following table displays details of the models, manufacturers, and the supported authentication tests conducted by Vocera.

Model	Manufacturer	Supported Authentication
Access Control Server (ACS)	Cisco	EAP-TLS, EAP-FAST, WPA-PEAP
Internet Authentication Service (IAS)	Microsoft	EAP-TLS, WPA-PEAP (badge only)
Steel-Belted Radius	Juniper Networks	PEAP
Identity Service Engine (ISE)	Cisco	EAP-TLS, EAP-FAST, WPA-PEAP
HostAPD	Opensource	EAP-TLS, EAP-FAST, WPA-PEAP

Authentication Overview

Vocera devices support WPA2 (AES-CCMP encryption), with PEAP (MS-CHAP v2, GTC), EAP-TLS, EAP-FAST, and PSK authentication.

Wi-Fi Protected Access 2 (WPA2), a pre-shared key, is a secure and strong encryption protocol. It is a stronger algorithm for message integrity and confidentiality. It utilizes AES (Advanced Encryption Standard) in conjunction with counter mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP.)

These 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. This happens because to packets 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..

Authentication Delays

You can experience an authentication delay due to different methods of security introduced while roaming.

The following table provides general guidelines for additional overhead. The specific performance may vary depending upon the access point you use and your network configuration.

Authentication Type	Association Delay	Description
WPA-PSK	< 100 ms	WPA-PSK often provides the optimal trade-off between security and performance.
EAP-FAST	500 ms	Frequent session timeouts can result in additional delays. For more information, refer to Authentication Overview on page 47.
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 maximum overhead due to the time required for connecting to an authentication server. WPA2-PSK provides a considerable level of security while introducing minimum overhead.

Fast Transition

Fast Transition, also known as Fast Reconnect is a negotiation between the client and the AP that uses information exchanged in the initial authentication to expedite the reestablishment of a session.

Fast Reconnect allows wireless clients to move between APs on the same network without repeated authentication request. For example, if a user roams during a conversation, the authentication causes minimum possible interruption when fast reconnects are enabled. It also minimizes the impact on each client during a temporary network outage by enabling the client to reconnect to the server automatically and restart.

The different fast reconnect roaming methods used to optimize roaming time are TLS session, CCKM, OKC and 802.11r.

Opportunistic Key Caching for Fast Roaming

Opportunistic Key Caching (OKC) is an authentication technique between multiple APs in a network where those APs are under common administrative control.

OKC is applicable only when the key management is WPA2-Enterprise (WPA-2 and WPA). OKC is not a fast-secure roaming method defined by the 802.11 standards and is not supported by many devices. OKC is disabled by default.

When OKC is enabled, multiple APs shares Pairwise Master Keys (PMK). The client can roam to a new AP and reuse a PMK that was established with the current AP. OKC allows the station to roam quickly to an AP it has never authenticated to, without having to perform pre-authentication.

Enabling CCKM for Fast Roaming

Cisco Centralized Key Management (CCKM) is a form of fast roaming supported on Cisco infrastructure and on various routers.

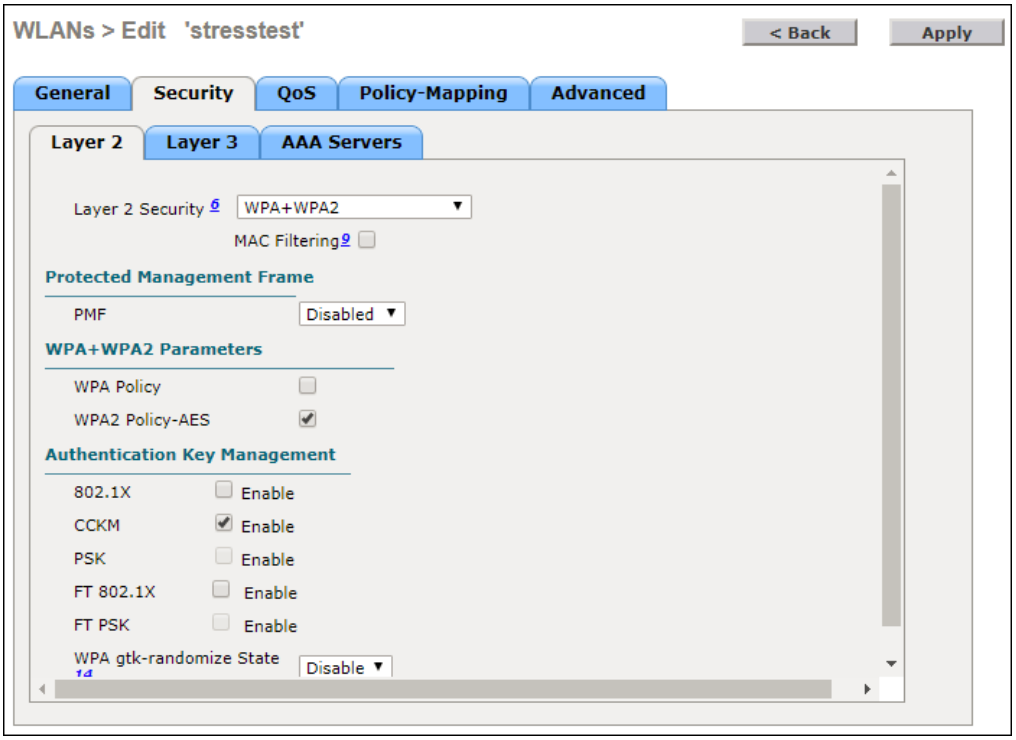
Using CCKM, Vocera B3000n and B3000 badges can roam from one access point to another without any noticeable delay during reassociation. After a Vocera device is initially authenticated by the RADIUS authentication server, each access point on your network acts as a wireless domain service (WDS) and caches security credentials for CCKM-enabled client devices. When a Vocera device roams to a new access point, the WDS cache reduces the time it takes to reassociate.

To take advantage of CCKM for B3000n and B3000 badges, your access points and badges must be configured to enable CCKM. You must also use either WPA-PEAP, EAP-FAST, or EAP-TLS authentication. For details on how to configure badges for CCKM, refer to Vocera Badge Configuration Guide.

To enable CCKM on autonomous APs, refer to Cisco IOS Software Configuration Guide.

To enable CCKM on Cisco CAPWAP access points, perform the following steps:

1. In the Cisco WLC Web User Interface, click **WLANS**>**WLAN profile name**.
2. Click **Security**>**Layer 2 Security**.
3. Select **WPA+WPA2**.
4. Select **CCKM** under **Authentication Key Management**.
   The following screenshot provides information on the CCKM settings.



5. Click **AAA Servers**.
6. Select **Enabled** under **Authentication Servers** and **Enabled** under **Accounting Server**.
7. Click **Apply**.
   CCKM for Cisco CAPWAP access points is enabled.

Fast Transition Roaming 802.11r

One of the fast reconnect roaming methods used is Fast Transition Roaming 802.11r. For more information on 802.11r, refer to Fast Transition Roaming: 802.11r on page 25 and Enabling 802.11r on page 30.

Authentication Support

This section describes the details of the supported authentications.

EAP Configuration Overview

EAP configuration overview provides the settings required for the controller, authentication server. It also provides the badge properties details required for EAP-TLS, PEAP, and EAP-FAST authentication framework.

Settings	EAP-TLS Configuration	PEAP Configuration	EAP-FAST Configuration
Controller Configuration			
Configure Encryption and Authentication 802.1x on the controller	Yes	Yes	Yes
Add Authentication Server IP	Yes	Yes	Yes
Select required "Authentication IP" for the profile	Yes	Yes	Yes
Authentication Server			
Install Certificates on the Authentication server	Yes	Yes	Yes

Settings	EAP-TLS Configuration	PEAP Configuration	EAP-FAST Configuration
Option to be enabled on the Authentication server	EAP-TLS	PEAP	EAP-Fast
Select Authentication policy "Internal Users Based"	No	Yes	Yes
Select Inner Authentication as MSCHAPv2 or GTC or both.	No	Yes	Yes
Select Anonymous PAC or Authentication PAC provisioning	No	No	Yes
Device Configuration – Badge Properties			
V5.AuthenticationType	WPA-EAP	WPA-EAP	WPA-EAP
V5.EAPMethod	TLS	PEAP	FAST
V5.UserName	<Provide Username>	<Provide Username>	<Provide Username>
V5.Password	–	<Provide password>	<Provide password>
V5.EnableHigherTLSVer	True	True	-
V5.EnableServerCertValidation	-	True/False If the parameter is set to true and you are using external certificate to validate the certificate, then place the certificates in `/gen5/badge/data/res/certificates/PEAP/` and set `V5.EAPTLSUseExtCert = true`, so that badge uses the certificate from correct path and validates the certificate. Note: To validate Server certificate rootca certificate is required.	False

Settings	EAP-TLS Configuration	PEAP Configuration	EAP-FAST Configuration
V5. EAPTLSUseExtCert	True/**False** • True— Enables the device to take the external certificates from a different path. Place the external certificates in `/gen5/badge/data/res/certificates/EAP-TLS/`. **Note**: EAP-TLS folders and certificates and will not be available. You must create it to place external certificates. • False—Enables the device to access the Vocera manufacturer internal certificate from `/gen5/badge/res/certificates/EAP-TLS/vi/`.	True/**False** • True—Enables the device to access the external certificates from a different path. Place the external certificates at `/gen5/badge/data/res/certificates/PEAP/` • False— Enables the device to access the Vocera manufacturer internal certificate from `/gen5/badge/res/certificates/PEAP/vi/`	True/**False** • True—Enables the device to access the external certificates from a different path. Place the external certificates at`/gen5/badge/data/res/certificates/EAP-Fast` • False— Enables the device to access the Vocera manufacturer internal certificate from `/gen5/badge/res/certificates/EAP-Fast/vi/`
V5.Provisioning	-	0 or 1 • 0—Uses MSCHAPv2 as the inner authentication method for authentication. • 0—Uses MSCHAPv2 as the inner authentication method for authentication. • 1—Uses GTC as the inner authentication method for authentication.	0/1/2/3 • 0— Allows manual PAC provisioning to create a manual PAC on the authentication server and the device at g5/badge/data/res/certificate/EAP-Fast/. • 1— Allows anonymous PAC provisioning for creating PAC and authentication. • 2— Allows authenticates PAC provisioning for creating PAC and authentication. • 3—Allows Authenticated and Unauthenticated PAC provisioning.

Datagram Transport Layer Security

Datagram Transport Layer Security (DTLS) protects data privacy and enables encryption of User Datagram Protocol (UDP) data packets at the transport layer.

It provides secure signaling between the Vocera Server and Vocera Smartbadge using the underlying TLS (Transport Layer Security) / SSL (Secure Sockets Layer) protocol for encrypting application data in transit. The highest TLS version supported by V5000 is version 1.2.

For V5000 Smartbadge, the transcribed speech is returned as text using the transcript flow Vocera Voice Server > Smartbadge > Vocera Messaging Server.

When a Vocera Smartbadge that is capable of supporting encrypted signaling attempts to connect to a server that wishes to use DTLS for the signaling encryption, the following behavior is exhibited:

- Both Vocera Smartbadge and server support the selected encryption mechanism, and the client connects seamlessly.
- The signal protocol version of the Smartbadge must be greater than 2.
- The Vocera Smartbadge indicates the following information under **Badge Settings** > **Security**.
  - Encryption is enabled
  - The type of encryption
- If the Vocera Smartbadge and server do not mutually support the encrypted connection, the client displays a message that the connection is unauthorized, and you need to contact your administrator.

For B3000n badges, the transcript is handled by the Vocera Server.

The DTLS handshake is performed on port 5500, and after that DTLS session is establishing successfully.

Power

Ensure that the TX power of your access points falls within the maximum and minimum power recommended by Vocera.

If an access point is set to its default power level (usually 100 mW), there will be a power asymmetry problem. If an access point is set to lower power level, the deployment is considered dense with many APs. The badge can receive data from the AP, but the AP cannot receive signals from the badge. This power asymmetry results in choppy audio and one-way audio.

The following table displays the radio transmit power for B3000n in 2.4 GHz spectrum.

Mode	Data Rate	Typical Transmit Power
802.11b	11 Mbps	+17 dBm
	1 Mbps	+17 dBm
802.11g	54 Mbps	+16 dBm
	6 Mbps	+17 dBm
802.11n (HT20)	MCS7	+16 dBm
	MCS50	+17 dBm

The following table displays the Radio transmit power for B3000n in 5 GHz spectrum.

Mode	Data Rate	Typical Transmit Power
802.11a	54 Mbps	+14 dBm
	6 Mbps	+16 dBm
802.11n (HT20)	MCS7	+14 dBm
	MCS0	+16 dBm
802.11N (HT40, 5GHz only)	MCS7	+14 dBm

For more information on radio receiver sensitivity, refer to Radio Receiver Sensitivity on page 54.

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.

To tune the configuration for your Vocera system consider the following:

- **Dynamic Transmit Power Adjustment**—If an access point goes offline, 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 shown in the following:

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 channel of the access point, 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 more information about the Cisco Wireless Control System (WCS), Cisco Prime, or the Cisco Wireless LAN Controller (WLC), refer to the Cisco Systems documentation.

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

Radio Receiver Sensitivity

Receiver sensitivity is the lowest power level at which the receiver can detect a Radio Frequency (RF) signal and produce a specified output signal. The ability of a device to pick up strong transmit signal and a high receiver sensitivity performs better in low WLAN coverage than a device with weaker signals.

The following table shows the radio receiver sensitivity for Vocera devices at 2.4 GHz data rates.

Protocol	Data Rate	Receiver Sensitivity for B3000n	Receiver Sensitivity for V5000	Receiver Sensitivity for C1000
802.11b	1 Mbps	-90 dBm	NA	NA
	2 Mbps	NA	NA	NA
	5.5 Mbps	NA	NA	NA
	11 Mbps	-87 dBm	–89 dBm	–85 dBm
802.11g	6 Mbps	-91 dBm	NA	NA
	9 Mbps	NA	NA	NA
	12 Mbps	NA	NA	NA
	18 Mbps	NA	NA	NA
	24 Mbps	NA	NA	NA
	36 Mbps	NA	NA	NA
	48 Mbps	NA	NA	NA
	54 Mbps	-73 dBm	–77 dBm	–75 dBm
802.11n (HT20)	MCS0	-90 dBm	NA	NA
	MSC7	-70 dBm T	–76 dBm	–73 dBm

The following table shows the radio receiver sensitivity for Vocera devices at 5 GHz data rates.

Protocol	Data Rate	Receiver Sensitivity for B3000n	Receiver Sensitivity for V5000	Receiver Sensitivity for C1000
802.11a	6 Mbps	-92 dBm	NA	NA
	9 Mbps	NA	NA	NA
	12 Mbps	NA	NA	NA
	18 Mbps	NA	NA	NA
	24 Mbps	NA	NA	NA
	36 Mbps	NA	NA	NA
	48 Mbps	NA	NA	NA
	54 Mbps	-73 dBm	-73 dBm	–75 dBm

Protocol	Data Rate	Receiver Sensitivity for B3000n	Receiver Sensitivity for V5000	Receiver Sensitivity for C1000
802.11n (HT20)	MCS0	-91 dBm	NA	NA
	MCS7	-70 dBm	–73 dBm	–73 dBm
HT40	MCS7	NA	–69 dBm	–70 dBm
VHT80	MCS7	NA	–62 dBm	–63 dBm

Wi-Fi LAN Vendor Settings

This section provides a summary of vendor specific settings and best practices for Vocera system implementations.

Note: The information covered in this section is not comprehensive and applies to the setting recommendations for Vocera only. For more information on specific access point settings, refer to the respective vendor documentation.

Common WLAN Settings

Universal WLAN settings and best practices that apply to all WLAN vendor equipment are listed in this topic.

The following table displays the required common WLAN settings.

Setting	Recommended Value
Authentication Timeouts	Add session timeout of at least 1 full shift
AP Transmit Power	• Max 17 dBm (50 mW) • Min 12 dBm (16 mW)
Band	5GHz
Band Steering	Disable
Basic Data Rate	Data Rates Determine the rate as needed for each site
Beacon Interval	100 (Required)
Channel Plan	2.4 GHz—1, 6, 11
	5 GHz—Any **Note**: • Vocera does not recommend using channels 120-128. • B3000n does not support channel 144. • If utilizing DFS channels, do not hide the SSID to speed up roaming.

Setting	Recommended Value
Channel Width	For optimal channel separation and to minimize co-channel interference Vocera recommends 20 MHz wide channels. B3000n Badge: • 2.4GHz—20 MHz • 5 GHz—20Mhz or 40MHz V5000 Smartbadge • 5 GHz—20MHz, 40MHz, or 80MHz C1000 Minibadge • 5 GHz—20MHz, 40MHz, or 80MHz
Client Exclusions	Disable
Coverage	-65dBm Minimum (Recommended: 2 Access Points with -65dBm) Vocera Badges require a sensitivity level of -65dBm, as measured from a mobile VoIP client. You should apply the recommended mobile VoIP offsets from a survey vendor of your choice. For instance, consider applying the RSSI offset from Ekahau. Stryker's internal testing has identified the following signal offsets when using the Ekahau Sidekick for data capture with Vocera devices. • -8 dB for 5 GHz • -5 dB for 2.4 GHz Stryker provides specific offsets for Stryker devices only. For device offsets for non-Stryker devices, refer to the respective device manufacturer's wireless specifications.
DTIM	1 (Required)
Load Balancing	Disable
Max Number of SSIDs	5
Minimum SNR	+ 25 dB
Neighbor Reports (802.11k)	Enable
Priority Queue	Highest—Voice (Required)
Roaming Policy	• B3000n—2 • V5000—3 • C1000—3
Voice Grade Site Survey	Recommended
WMM	Recommended

The following table displays the multicast recommendations.

Setting	Recommended Value
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.

The following table displays the association delays caused by authentication.

Authentication Type	Association Delay	Comments
EAP-FAST	200 ms	Frequent session timeouts can result in additional delays. **Note:** For EAP-FAST, use CCKM (only for B3000n), OKC, or 802.11r to cache credentials and optimize roaming times.
PEAP EAP-TLS	Varies	The association delay caused by authentication varies based on the cipher strength (1024 bit or 2048 bit) and the depth of certificate chains. **Note:** For EAP-TLS and PEAP, use CCKM (only for B3000n), OKC, or 802.11r to cache credentials and optimize roaming times.
PSK	< 100 ms	PSK often provides the optimal trade-off between security and performance.
Encryption	NA	AES-CCMP. Vocera badges do not support WEP, TKIP or SAE.

Cisco Networks

Vendor specific WLAN settings and best practices that apply to the Cisco networks equipment are listed in this topic.

Setting	Recommended Value
Admission Control (ACM)	Disable
AP Multicast Mode	Multicast (239.x.x.x)
Auto QoS (IOS-XE only)	None
Band Select	Disable
Coverage Hole	Disable 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
DHCP Address Assignment (required setting)	Disable
Flex Connect	Centralized Mode or Distributed mode. **Note:** For Vocera voice this option is not recommended. If you have a need to enable this option, contact Vocera Technical Support.
Load Balancing	Disable
Rogue Location Discovery Protocol (RLDP)	Disable
RRM—Dynamic Channel Assignment	Interval should be more than 8 hours. It is the typical duration of one nursing shift.
RRM—Dynamic Transmit Power Control	Enable if the maximum and minimum transmit power levels meets Vocera's recommended settings.

Setting	Recommended Value
Multicast Mode#Global	Enable Disable Mobility Multicast Messaging if multicast is not properly enable in network. It causes one-way audio or no audio.
Multicast Tx Data Rate	Highest data rate. 12Mbps and 24Mbps as mandatory data rates. **Note:** Vocera highly recommends to disable DSSS/11b rates (1,2,5.5, 11) on the AP.
Optimized Roaming	Disable
RSSI Low Check	Disable
Symmetric Mobility Tunneling	Enable
Transmit Power Threshold	Adjust to fit site
U-APSD	Enable
Unicast-ARP	Disable
WLAN QoS	Platinum
WMM	Optional

Cisco Networks with Apple Smart Devices

Vendor specific WLAN settings and best practices that apply to the Cisco Networks and Apple smart devices are listed in this topic.

Settings	Recommended Values
iPhone iOS version	10 or later
Band	5GHz
WLAN QoS	Platinum
Fastlane	Enable
Wireless Security	WPA2/AES - PSK
Fast Transition (802.11r)	• If using PSK - Set FT to Adaptive • If using 802.11X authentication - set FT to Enable • FT- OTA (over the air) must be used
Assisted Roaming (802.11k)	Enable (5GHz - single band)
BSS Transition Management (802.11v)	Enable
WMM	Optional
Band Select	Disable
Load Balancing	Disable
Voice CAC	Disable
EDCA Profile	Fastlane
RSSI Low Check	Disable
Optimized Roaming	Disable
Global Multicast Mode	Enable
AP Multicast	Multicast (239.x.x.x)

Settings	Recommended Values
IGMP Snooping	Enable
RLCP (Rogue Location Discovery Protocol)	Disable

Aruba Networks

Vendor specific WLAN settings and best practices that apply to the Aruba access points are listed in this topic.

Settings	Recommended Value
ARM	Enable if honoring maximum and minimum transmit power levels.
Dynamic Multicast Optimization	Enable
Dynamic Multicast Optimization Threshold	30
IGMP Proxy	Enable on Vocera VLAN(s)
Mcast-rate-opt (needed for multicast to go at highest rate)	Enable
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
Probe Retry	Disable
Role	Voice
Session ACL	vocera-acl
Tx Data Rates	2.4 GHz—6, 9, 11, 12, 18, 24 5 GHz—Data rates change depending on the site
Voice Aware Scanning	Enable

Extreme Networks

Vendor specific WLAN settings and best practices that apply to the Extreme Networks - Extreme Cloud Appliance are listed in this topic.

Setting	Recommended Value
Admission Control	Disabled (Default)
DTIM	1 To support multicast group calls
Radio Management (11k) support	Enable

Setting	Recommended Value
Radio Share Mode	Off
Multicast Bridging	Enable
Multicast Rule	VLAN Predefined Multicast Rule **Vocera Mcst** added to rule list.
Minimum Basic Rate (MBR)	Based on Site Survey MIN 12

Ruckus Networks

Vendor specific WLAN settings and best practices that apply to the Ruckus access points are listed in this topic.

Setting	Recommended Value
Authentication/Encryption	WPA2/AES (802.11i)
Band steering, load balancing	Disable
Controller Code	Latest from Ruckus
Directed-Multicast and Broadcast	Turn off conversion of broadcast and multicast to unicast on the WLAN interface using the following commands: • **ruckus(config-wlan) #** no qos directed-multicast • **ruckus(config-wlan) #** qos directed-threshold 0 **Note:** Both the commands are required. Issuing only the first command causes audio issues during Vocera Broadcasts.
DHCP	Enable
Hiding SSID in Beacons	Not recommended
Inactivity Timeout	720 (12 hrs)
Mesh	Disable
Minimum BSS Rate	Depends on AP density
Power Level	2.4 GHz—25 mW 5 GHz—50 mW
Proxy ARP and ARP Broadcast Filter	Enable
Smart-Roam	Disable
VLAN	Dedicated non-native VLAN
Wireless Client Isolation	Disable
WLAN Background Scanning	Disable

Meraki Networks

Vendor specific WLAN settings and best practices that apply to the Meraki Networks access points are listed in this topic.

Setting	Recommended Value
Wireless	
WPA encryption mode	WPA2

Setting	Recommended Value
802.11w	Disable
Splash page	None
Assign group policies by device type	Disable
VLAN tagging	Use VLAN tagging
Content filtering	Don't filter content
Bonjour forwarding	Disable Bonjour Forwarding
Mandatory DHCP	Disable
Band selection	Do not use Dual band operation with Band Steering
RF Profile	
Client balancing	Off
Switch	
Multicast routing	Enable IGMP snooping querier
Quality of service	DSCP 46

Fortinet/Meru Networks

Vendor specific WLAN settings and best practices that apply to the Meru Networks/Fortinet are listed in this topic.

Setting	Recommended Value
Badge Roaming Policy	1
IGMP Snooping	Enable
Multicast setting	Configure UDP Broadcast Port 5555 for Badge Discovery for Meru.
QoS Rules	Enable QoS Rules 7 and 8. It is enabled by default.Separate for Vocera
SSID	Separate for Vocera
Virtual Port	Disable **Note:** Vocera recommends that you do not use Virtual Port.
Virtual Cell [1]	Enable only if no native cell option
Vocera Location Feature	Disable Virtual Cell or divide APs into zone.

[1] A Transmit Power Asymmetry problem may arise at the edges of Virtual Cell coverage if the transmit power of an AP 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.

Site Survey

Vocera strongly recommends a voice grade site survey is conducted for voice to prepare for the performance requirements of the badges and the APs. The survey provides an opportunity to tune the WLAN for the roaming characteristics and different coverage requirements.

Vocera badges operate at a low power and require a Voice grade network, capable of transmitting human voice. All mobile battery clients operate at a lower power than the maximum TX power of an AP.

Note: Your data will be skewed if your TX power is at the recommended required TX power.

Signal Propagation

You must perform a voice quality site survey to ensure adequate network coverage prior to installing Vocera.

If your site was not surveyed to meet the specific needs of Vocera, you will probably need to extend your coverage due to the following reasons:

- 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.
- Voice has different tolerance for errors and delays than data.
- The antenna in the badge behaves differently than the antennas typically used to perform site surveys. For more information, refer to Minimum Signal Strength on page 64.

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

To confirm site survey coverage for Vocera, perform the following:

1. Set AP power levels comparable to the transmit power of the Vocera devices. For more information, refer to Power on page 52.
2. Ensure that you have adequate signal strength for the Vocera badge throughout your facility. For more information, refer to Minimum Signal Strength on page 64.
3. Ensure that the signal-to-noise ratio (SNR) is 25 dB and RSSI is -65 dBm or higher.
4. Use the Vocera badge in survey mode to confirm proper coverage and ensure voice quality throughout your facility. For more information, refer to Acceptable Voice Quality on page 64.
5. Use the appropriate subset of channels, based on the frequency band:
   - For 5 GHz, the industry practice is to use either the Dynamic Frequency Selection channels (52,56,60,64,100,104,108,112,116,120, 124, 128,132,136,140) or channel 165. Use all other available channels.

- For 2.4 GHz, use only channels 1, 6, and 11 to maintain adequate channel separation. For more information, refer to Channel Separation on page 33.

Ensure that the channels you enable in the wireless controller match the channels you specify in the Vocera the `badge.properties` file. For more information, refer to Vocera Device Configuration Guide

6. Ensure that the coverage cells for all access points overlap sufficiently. For more information refer to Overlapping Cells on page 36.
7. Minimize co-channel interference. For more information, refer to Channel Interference on page 35.

Minimum Signal Strength

Signal strength may be affected by objects, the distance between your devices, and the AP settings. It is important to measure and test for minimum signal strength.

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

1. Perform measurements in at least 2-4 corners of any room or both directions down a corridor. Testing in 2-4 directions offset by 90 degrees provides a margin of error and an additional check of your work.
2. Ensure that the signal strength is always greater than -65 dBm.
3. Ensure that the AP transmit power is set to a level comparable to the typical transmit power of the Vocera device. For more information, refer to Power on page 52.

   Industry Best Practice: Set the AP transmit power to match the global power in your environment.

The notebook computers typically used to perform site surveys contain omnidirectional antennas. However, the badge antenna is less perfectly omnidirectional and the signal strength 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. The attenuation resulting from the human body causes badge coverage at the back of the body to drop.

If you are performing measurements with equipment that uses an omnidirectional antenna, ensure a minimum of -65 dBm signal strength in all areas where the badge is used. Do this 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.

Acceptable Voice Quality

It is important to understand the parameters contributing to the quality of the calls. These parameters help in defining the acceptable voice quality.

Each type of Vocera badge provides a different utility to evaluate the communication quality of the signal you receive from an access point.

The Vocera badge measures communication quality in Signal-to-Noise Ratio (SNR). 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 25.

The Vocera utilities for evaluating communication quality are Layer 2 applications that do not require the badge to connect to the Vocera Voice 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.

To confirm communication quality levels throughout a site, perform the following:

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:

   The following table displays the roaming policy, SNR value, and the beep rate for the badge.

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

4. Measure signal strength.
   Wear the badge normally. Use a lanyard or one of the other badge attachments. Do not handle the badge or read the display as you perform the test. Else, the badge will not measure access point signal strength correctly.
5. 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.
6. Ensure to test for coverage using the site survey tool. You must perform the test in two directions offset by 180 degrees while facing one direction.
   You may want to perform the 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.

   Note: Do not forget to include stairways, elevators, kitchens, bathrooms, and other areas where Vocera usage exposes gaps in conventional site surveys.

7. Press the badge select button to exit from the radio info screen.

   Note: Make a note of areas 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. The accepted level is approximately between 18 and 22. You must improve the coverage in these areas in order to have a successful deployment.

Playing a Test Tone

To identify areas with choppy audio or inadequate wireless coverage, play a test tone.

Vocera devices 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. If Vocera users complain of poor coverage or choppy audio, you can use the following commands to test the operation of the Vocera device in that location.

- **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. For Vocera Voice Server Version 5, you must have **Perform System Administration** permission, and for Vocera Platform Version 6, you must have **Perform Voice Administration** permission.

The Vocera device plays a tone for 31.7 seconds and is then silent for 1.2 seconds before the next tone starts. If packets of information are being lost, you will hear the tone breaking up.

Important: Do not play the test tone for longer than a couple minutes at a time. Repeatedly playing a test tone on a Vocera device continuously for ten minutes or more could cause speaker performance to degrade over time.

To play a test tone in a particular location, perform the following:

1. Bring two Vocera badges to a location where choppy audio was reported.
2. Approach the nearest wireless access point.
3. Press the call button and say `Play Test Tone`, on one badge.
4. Select **Info**>**Radio** to see the Vocera SNR value for that location, on the other badge.
5. Take away both Vocera devices 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.
7. Repeat the test from step 1, using `Broadcast Test Tone` voice command.

Troubleshooting tools

This section provides recommended WLAN tools that can be used to survey site and troubleshoot WLAN issues.

These tools allow you to plan and design a wireless network, access point locations for adequate coverage, and APs locations to transmit its signals throughout a building.

AirMagnet Survey Pro

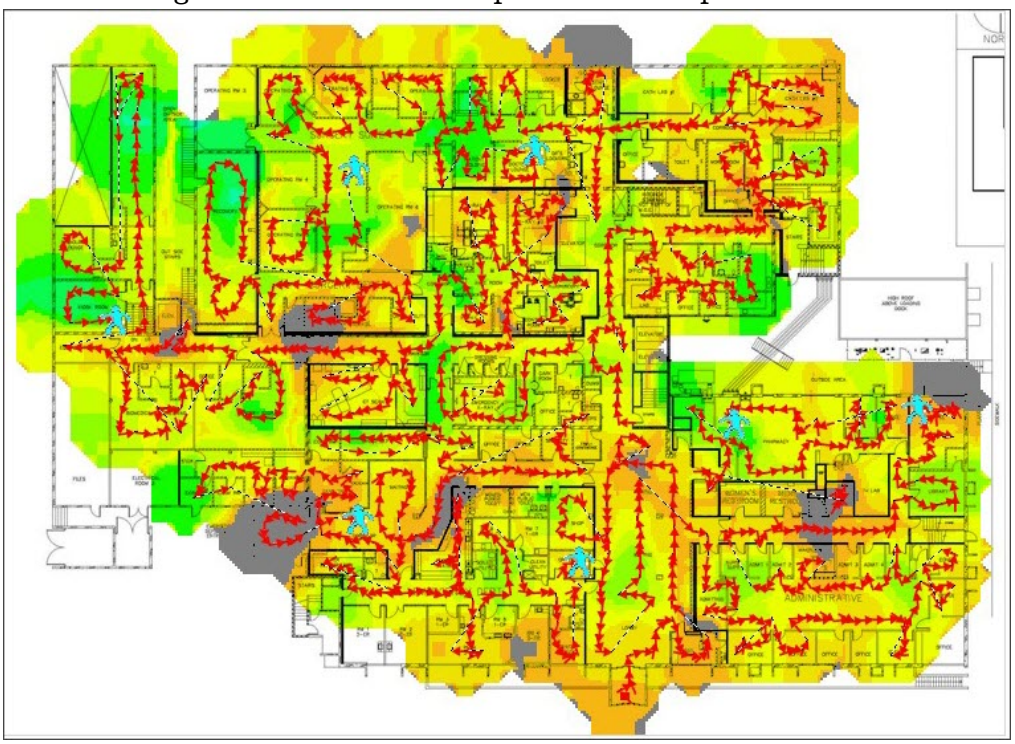
AirMagnet survey pro is a tool used to perform a heat map of the signal within the facility. All signals must be #65dBm/25 dB SNR or better.

It is an accurate wireless site survey software solution for mapping, planning and designing 802.11n/a/b/g/ac wireless LANs for optimal performance, security, and compliance. It identifies the areas of low coverage that may cause connectivity and transmission issues. The tool captures issues caused in both 2.4 GHz and 5 GHz spectrum.

The parameters depicted as a visual are:

- Signal strength heatmap
- SNR heatmap
- Channelization

The following screenshot is an example of a heatmap:



AirMagnet Spectrum XT

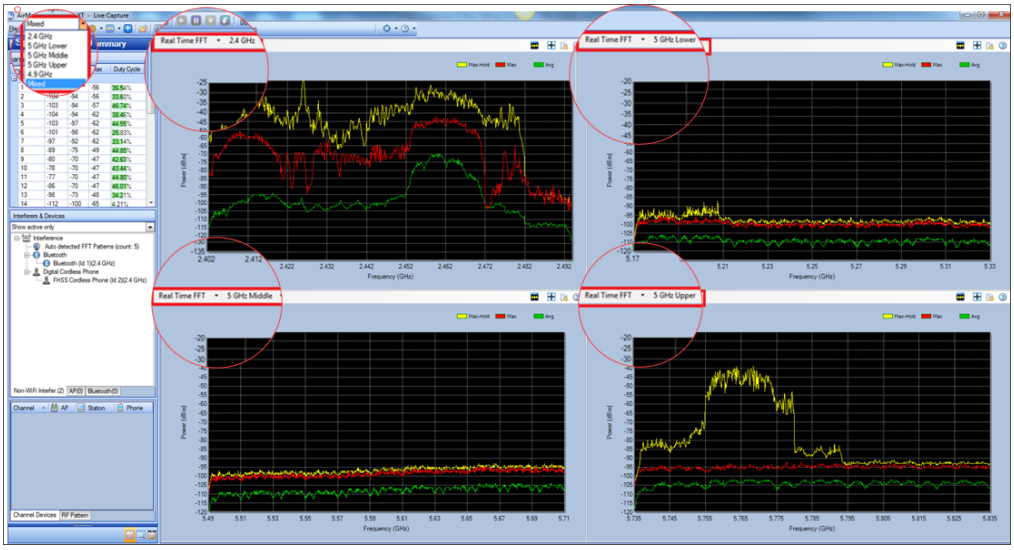
The AirMagnet Spectrum XT is a tool used to capture the real-time view and radio frequency (RF) bands for 2.4 GHz and 5 GHz.

It is an analyzer software tool that proactively identifies and locates any RF interference impacting WiFi network performance. It is also a WiFi troubleshooting and optimization tool that allows you to view the real performance of the wireless APs and channels.

To view the performance in both 2.4 GHz and 5 GHz, select **Mixed** mode. Select the desired view and frequencies.

Note: Recording the display view captures all the views and not just the views that are displayed.

The following screenshot displays the status of the RF.



The RF Summary pane displays the following information:

- Channel—All the channels available in the selected radio band.
- Current (dBm) —The average of current FFT readings.
- Avg(dBm)—The average historical FFT readings.
- Max(dBm)—The maximum FFT readings.
- Duty Cycle—The percentage of time the RF energy (both 802.11 and non#802.11) is present on the channel.

The following screenshot displays the details of the channel summary.

Channel Summary

C.	Cu...	Avg	Max	Duty Cycle
Band: 2.4GHz				
1	-80	-97	-58	32.40%
2	-83	-97	-58	36.48%
3	-88	-97	-55	39.02%
4	-95	-99	-52	50.25%
5	-100	-98	-49	12.90%
6	-96	-97	-49	25.27%
7	-96	-97	-49	63.27%
8	-90	-94	-49	36.78%

For more information on Fluke Networks AirMagnet Spectrum XT, refer to http://www.flukenetworks.com/enterprise-network/wireless-network/airmagnet-spectrum-xt.

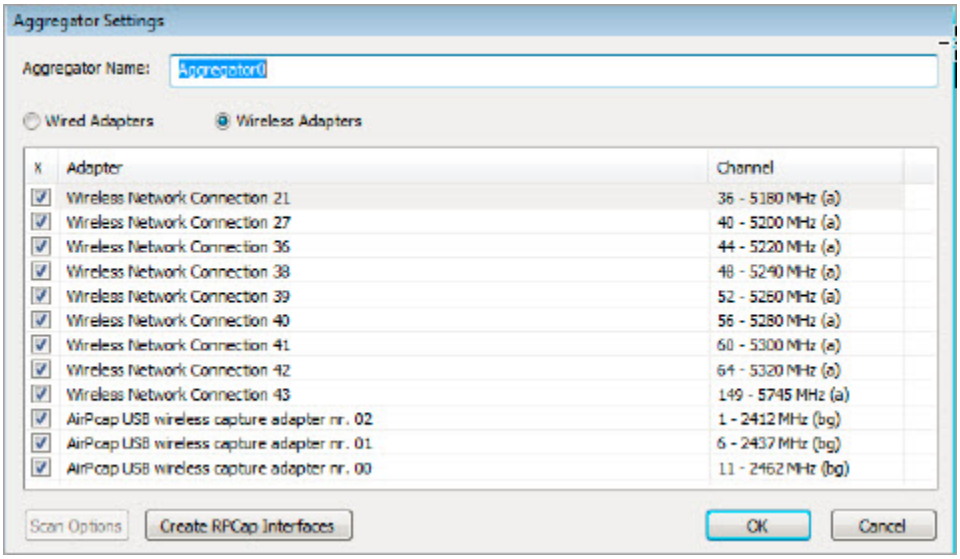
OmniPeek or Wireshark

Omnipeek and Wireshark are used to capture data packets that are transmitted and received by Vocera badges and access points.

It is a packet analyzer software tool that is used for network troubleshooting and protocol analysis. You can use one of the two tools to analyze your packets, test roams and data retries.

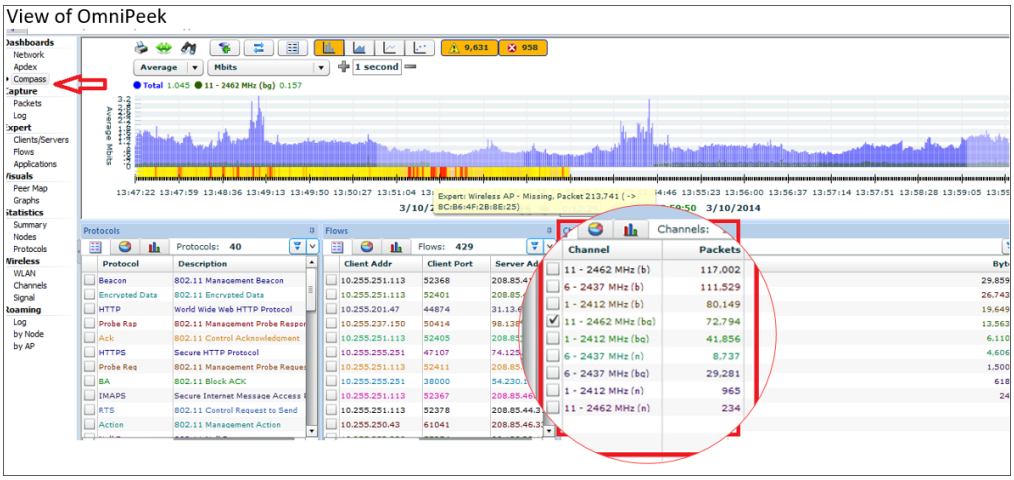
It exhibits the behavior of the badges and WLAN at the packet level. The packet analyzer is the most important among the three survey tests. This test is imperative to optimize badges and other WLAN devices. You must capture this test with a correlating Spectrum recording.

The following screenshot displays the details of the aggregator settings:



Before you begin the actual captures, configure your channels accordingly. If your channels are not configured correctly, your traces will be missing.

The following screenshot displays the details of the OmniPeek.



For more information on WildPackets OmniPeek Network Analyzer, refer to http://www.wildpackets.com/products/distributed_network_analysis/omnipeek_network_analyzer.

Multicast Hammer Tool

Multicast Hammer is a testing tool to test and validate multicast traffic on the network created by Nortel Networks. It is easy to use and can be downloaded for free on the Internet.

You can test with Nortel Multicast Hammer on the same SSID that the badges use. You can begin by testing the client and server on laptops in the following scenarios:

Wireless:

- Same AP
- Different APs on same controller

Wired:

- VS

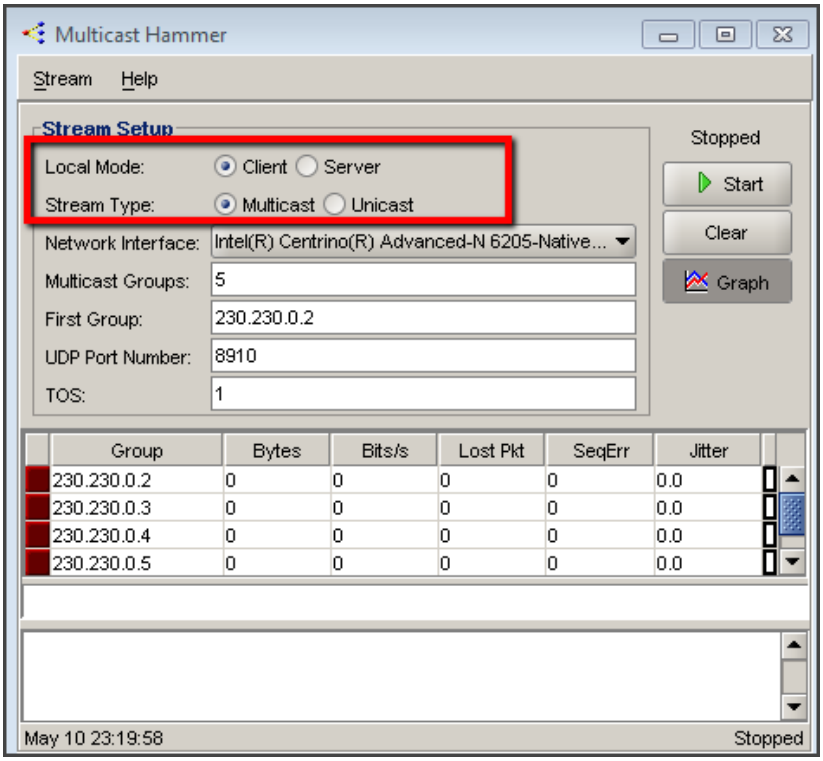
- VCG
- VSTG

Download the Multicast Hammer tool at http://multicast-hammer.software.informer.com/2.1/.

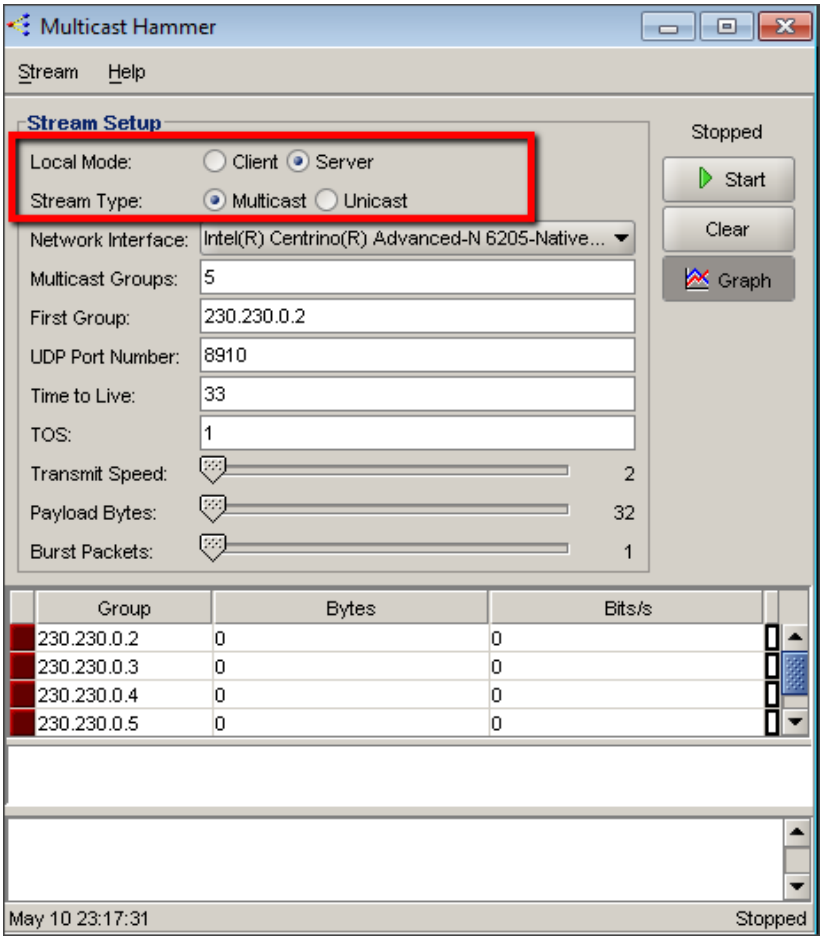
Setting up Multicast Hammer Tool

To set up Nortel Multicast Hammer Tool Server, perfom the following tasks:

1. Launch the Nortel Multicast Hammer Tool on both the client device and the server device. The following screenshots display the client device.

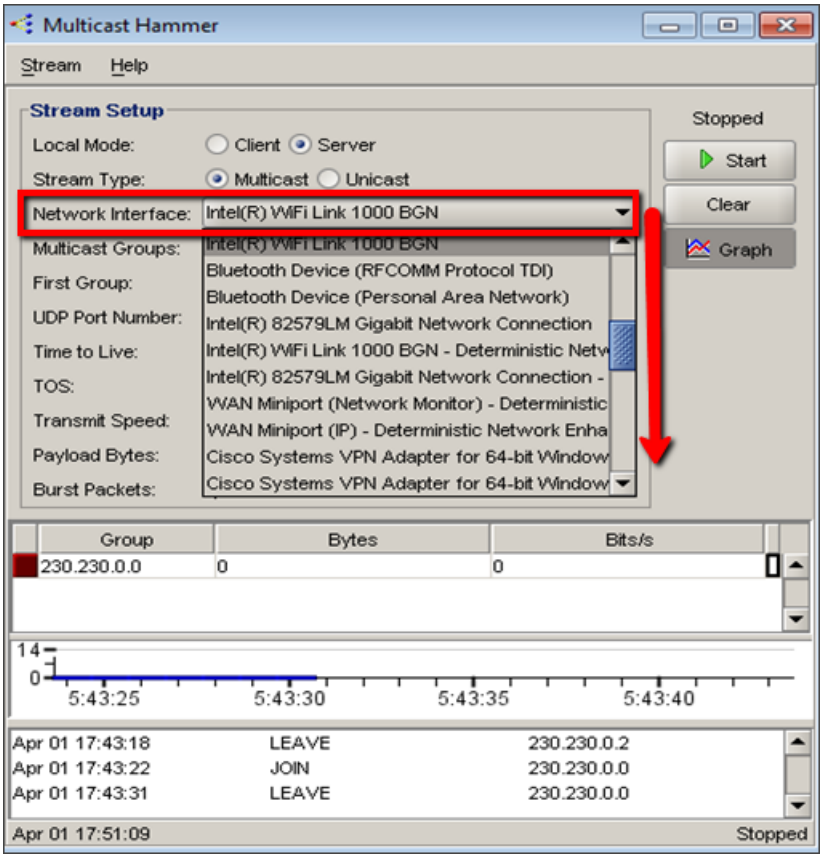


The following screenshots display the server device.

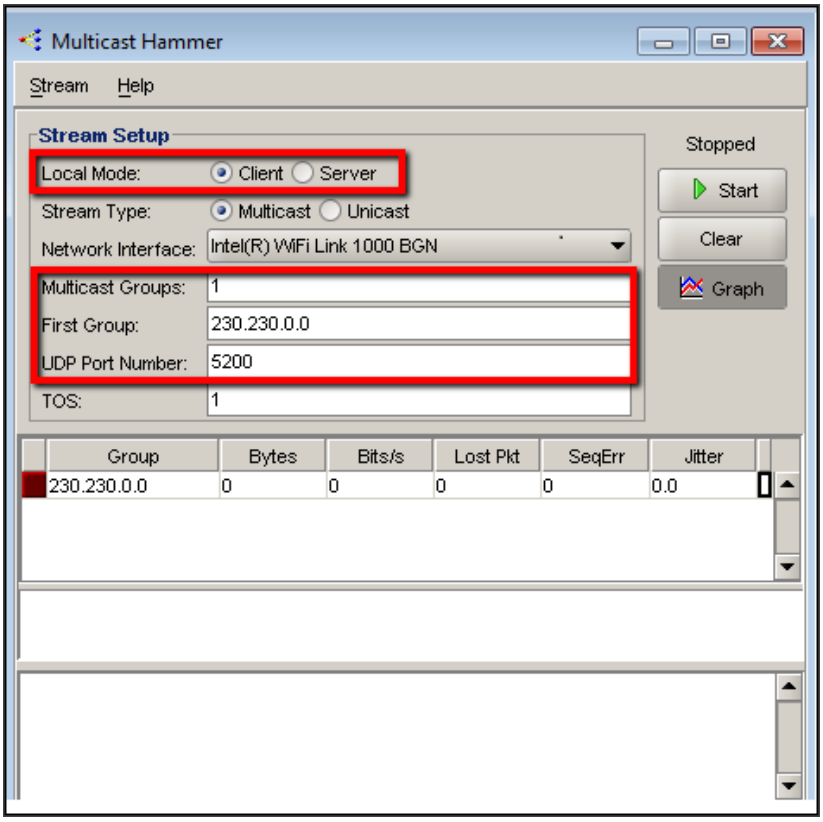


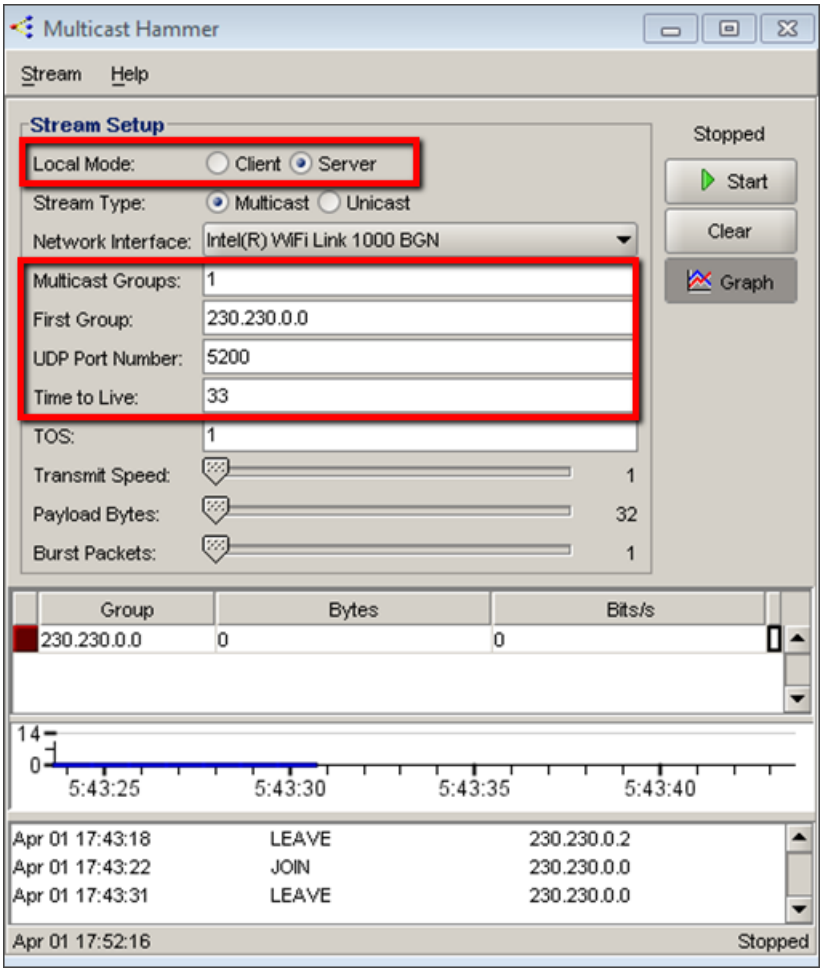
2. Identify and note the wireless adapter to be used for the multicast test from **Control Panel** > **Network and Internet** > **Network Connections**.

3. Select the desired network adapter from the Network Interface drop down menu.

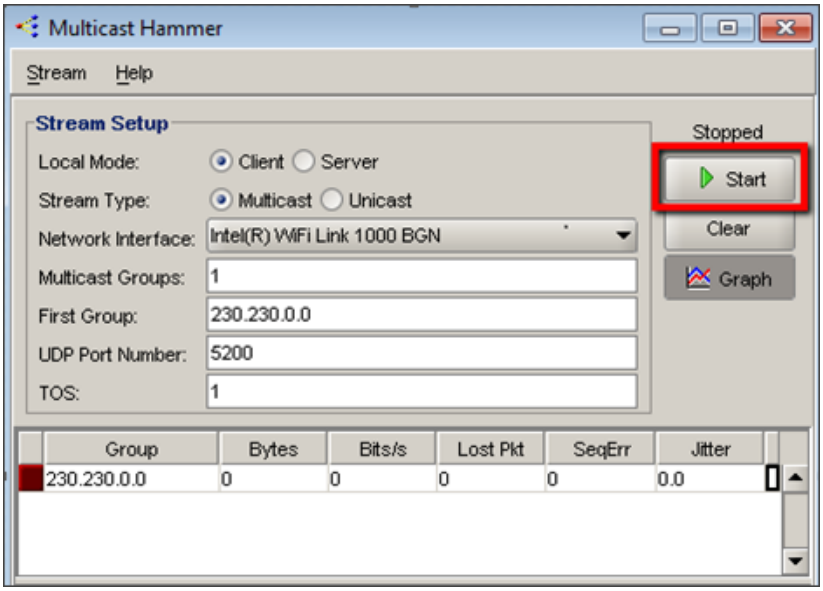


4. Input the same information on the server and the client device to set up multicast groups as shown in the following screenshots.

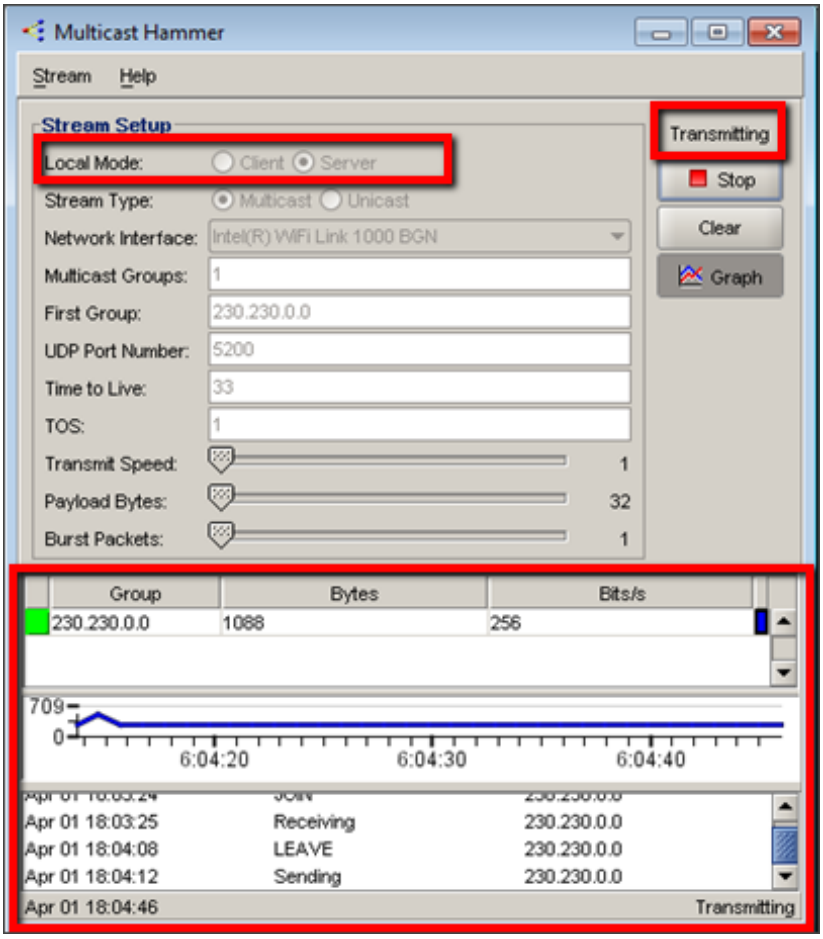


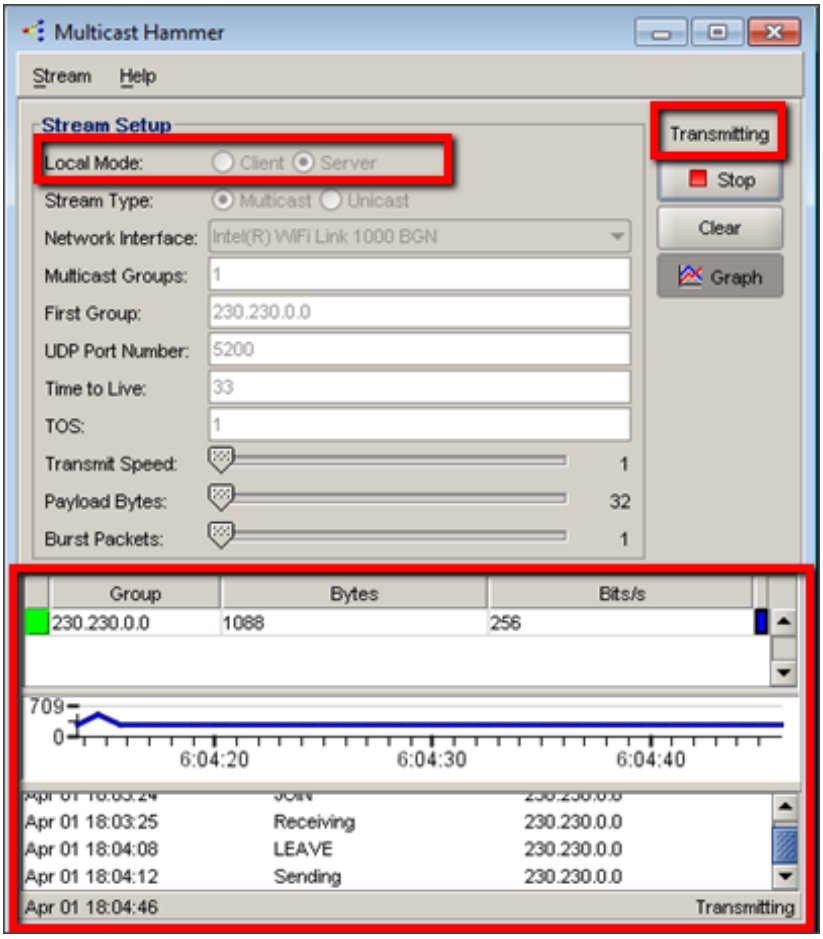


5. Select start on both the server device and the client device.



6. A successful test result are displayed as shows in the following screenshots.


Multicast Hammer
Stream
Help
Stream Setup
Local Mode:
Client
Server
Stream Type:
Multicast
Unicast
Network Interface:
Intel(R) WiFi Link 1000 BGN
Multicast Groups:
1
First Group:
230.230.0.0
UDP Port Number:
5200
Time to Live:
33
TOS:
1
Transmit Speed:
1
Payload Bytes:
32
Burst Packets:
1
Transmitting
Stop
Clear
Graph
Group
Bytes
Bits/s
230.230.0.0
1088
256
709
0
6:04:20
6:04:30
6:04:40
Apr 01 18:03:25
Receiving
230.230.0.0
Apr 01 18:04:08
LEAVE
230.230.0.0
Apr 01 18:04:12
Sending
230.230.0.0
Apr 01 18:04:46
Transmitting


Multicast Hammer
Stream
Help
Stream Setup
Local Mode:
Client
Server
Stream Type:
Multicast
Unicast
Network Interface:
Intel(R) WiFi Link 1000 BGN
Multicast Groups:
1
First Group:
230.230.0.0
UDP Port Number:
5200
Time to Live:
33
TOS:
1
Transmit Speed:
1
Payload Bytes:
32
Burst Packets:
1
Transmitting
Stop
Clear
Graph
Group
Bytes
Bits/s
230.230.0.0
1088
256
709
0
6:04:20
6:04:30
6:04:40
Apr 01 18:03:25
Receiving
230.230.0.0
Apr 01 18:04:08
LEAVE
230.230.0.0
Apr 01 18:04:12
Sending
230.230.0.0
Apr 01 18:04:46
Transmitting