



**Best Practices for Deploying
Polycom[®] SpectraLink[®] 8400
Series Handsets**
White Paper

August 2011 | 1725-36727-001 Rev A

Patent Information

The accompanying product is protected by one or more US and foreign patents and/or pending patent applications held by Polycom, Inc.

Copyright Notice

© 2011, Polycom, Inc. All rights reserved. POLYCOM®, the Polycom "Triangles" logo and the names and marks associated with Polycom's products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

All rights reserved under the International and pan-American copyright Conventions.

No part of this manual, or the software described herein, may be reproduced or transmitted in any form or by any means, or translated into another language or format, in whole or in part, without the express written permission of Polycom, Inc.

Do not remove (or allow any third party to remove) any product identification, copyright or other notices.

Every effort has been made to ensure that the information in this document is accurate. Polycom, Inc. is not responsible for printing or clerical errors. Information in this document is subject to change without notice and does not represent a commitment on the part of Polycom, Inc.

Notice

Polycom, Inc. has prepared this document for use by Polycom personnel and customers. The drawings and specifications contained herein are the property of Polycom and shall be neither reproduced in whole or in part without the prior written approval of Polycom, nor be implied to grant any license to make, use, or sell equipment manufactured in accordance herewith.

Polycom reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult Polycom to determine whether any such changes have been made.

NO REPRESENTATION OR OTHER AFFIRMATION OF FACT CONTAINED IN THIS DOCUMENT INCLUDING BUT NOT LIMITED TO STATEMENTS REGARDING CAPACITY, RESPONSE-TIME PERFORMANCE, SUITABILITY FOR USE, OR PERFORMANCE OF PRODUCTS DESCRIBED HEREIN SHALL BE DEEMED TO BE A WARRANTY BY POLYCOM FOR ANY PURPOSE, OR GIVE RISE TO ANY LIABILITY OF POLYCOM WHATSOEVER.

Contact Information

Please contact your Polycom Authorized Reseller for assistance.

Polycom, Inc.

4750 Willow Road,

Pleasanton, CA 94588

<http://www.polycom.com>

Model Numbers and Product Compatibility

The information in this document pertains only to SpectraLink 8400 Wireless Handsets, Battery Packs, and chargers. All 8400 Series products are compatible with each other. Use only 8400 Series products with other 8400 Series products as identified by the model number located on the label of the product. If you have any questions about product compatibility, contact your system administrator.

Product	Model Number
SpectraLink 8440 Wireless Handset	8440
SpectraLink 8450 Wireless Handset	8450
USB Charger	SA106B-05
Dual Charger	DCA39
Quad Charger	DCA40
Standard Capacity Battery Pack	RS657
Extended Capacity Battery Pack	RS658

Contents

- Introduction 5**
- Wireless LAN Considerations 7**
 - Coverage..... 7
 - Roaming Coverage*..... 7
 - Signal Strength*..... 11
 - Access Point Diversity*..... 13
 - Deployment Considerations 13
 - 2.4 GHz*..... 13
 - 5 GHz*..... 13
 - 802.11n* 14
 - Access Point Configuration* 15
 - Channel Selection*..... 15
 - AP Transmission Power and Capacity* 18
 - Interference*..... 18
 - Multipath and Signal Distortion*..... 19
 - Site Surveys* 20
 - Wireless Telephone Call Capacity..... 20
 - Access Point Bandwidth* 21
 - Push-to-Talk Multicasting* 21
- Quality of Service (QoS) 23**
 - WMM*..... 23
 - WMM Power Save* 24
 - WMM Admission Control*..... 25
 - DSCP for Wi-Fi Standard QoS Deployments* 27
- Security 28**
 - VoWLAN Security..... 28
 - Wired Equivalent Privacy (WEP)..... 28
 - Wi-Fi Protected Access (WPA) and WPA2 29
 - WPA Personal, WPA2 Personal* 29

WPA2 Enterprise 29

Using Virtual LANs 32

MAC Filtering and Authentication 32

Firewalls and Traffic Filtering 32

Diagnostic Tools..... 33

Subnets, Network Performance and DHCP **35**

 Subnets and IP Telephony Server Interfaces..... 35

 DHCP Requirements 35

Conclusion..... **38**

Introduction

Voice over Wireless LAN (VoWLAN), also known as “Voice over Wi-Fi” (VoWiFi), delivers the capabilities and functionality of an enterprise telephone system in a Wi-Fi handset. The handset is a WLAN client device, sharing the same wireless network as laptops and other handheld devices. For enterprise use, the handset is functionally equivalent to a wired desk phone, giving end-users all the features they are used to having in a wired office telephone. The benefits of VoWLAN can result in substantial cost savings over other wireless technologies by leveraging the Wi-Fi infrastructure and by eliminating recurring charges associated with the use of public cellular networks. For end users, VoWLAN can significantly improve employee mobility, resulting in increased responsiveness and productivity.

Delivering enterprise-grade VoWLAN means that wireless networks must be designed to provide the highest audio quality throughout the facility. Because voice and data applications have different attributes and performance requirements, thoughtful WLAN deployment planning is necessary. A Wi-Fi handset requires a continuous, reliable connection as a user moves throughout the coverage area. In addition, voice applications have a low tolerance for network errors and delays. Whereas data applications are able to accept frequent packet delays and retransmissions, voice quality will deteriorate with just a few hundred milliseconds of delay or a very small percentage of lost packets. Additionally, data applications are typically bursty in terms of bandwidth utilization; whereas voice conversations use a consistent and a relatively small amount of network bandwidth throughout the length of a conversation.

Using a Wi-Fi network for voice can be complex, but there are ways to mitigate complexity with some basic considerations. A critical objective in deploying enterprise-grade VoWLAN is to maintain equivalent voice quality, reliability and functionality as is expected from a wired telephone. Some key issues in deploying Wi-Fi telephony include WLAN coverage, capacity, quality of service (QoS) and security.

Polycom’s [VoWLAN certification program](#) is designed to ensure interoperability and maximum performance for enterprise-grade Wi-Fi infrastructure products that support SpectraLink handsets. The program is open to manufacturers of Wi-Fi infrastructure products that incorporate the requirements of the VoWLAN Technical Specification and pass certification testing. VoWLAN certification requirements focus on implementing industry standards for Wi-Fi networks along with meeting the specific quality of service (QoS) and performance characteristics that are necessary for supporting SpectraLink handsets.

Full Access Point diversity is critical for improved communication between the wireless handset and AP. This configuration, using both AP antennas, helps provide low retry rates and improves voice quality.

For each certified product, Polycom provides a [VoWLAN Configuration Guide](#) that details the tested hardware models and software versions; radio modes and expected calls per AP; and specific AP configuration steps. [VoWLAN Configuration Guides](#) are available on the Polycom website and should be followed closely to ensure a successful deployment.

Polycom pioneered the use of VoWLAN in a wide variety of applications and environments, making the SpectraLink Wireless Telephone the market leader in this category. Based on our experience with

enterprise-grade deployments, this guide provides recommendations for ensuring that a network environment is optimized for use with Polycom SpectraLink 8400 Series Wireless Telephones, the latest generation of our industry-leading platform.

Wireless LAN Considerations

SpectraLink 8400 Series handsets utilize a Wi-Fi network consisting of access points (APs) distributed throughout a building or campus. The required number and placement of APs in a given environment is driven by multiple factors, including intended coverage area, system capacity, power output, physical environment, and radio types.

Coverage

One of the most critical considerations in deployment of SpectraLink handsets is to ensure sufficient wireless signaling coverage. Enterprise Wi-Fi networks are often initially laid out for data applications and may not provide adequate coverage for voice users. Such networks may be designed to only cover areas where data devices are commonly used, and may not include coverage in other areas such as stairwells, break rooms or building entrances – all places where telephone conversations are likely to occur. It is important to consider coverage requirements in areas where a voice conversation may not be as common, such as restrooms and stairways, stairwells & parking areas, for the purpose of emergency planning. The overall quality of coverage is more important for telephony applications. Coverage that may be suitable for data applications may not be seamless enough to support the requirements of VoWLAN. Most data communication protocols provide a mechanism for retransmission of lost or corrupted packets. Delays caused by retransmissions are not harmful, or even discernable, for most data applications. However, the real-time nature of a full-duplex telephone conversation requires that voice packets be received correctly within tens of milliseconds of their transmission. There is little time for retransmission, and lost or corrupted packets must be discarded after limited retries. In areas of poor wireless coverage, the performance of data applications may be acceptable due to retransmission of data packets, but for real-time voice, the audio quality will suffer.

Another factor to consider when determining the coverage area is the device usage. Wireless telephones are used differently than wireless data devices. Handset users tend to walk as they talk, while data users are usually stationary or periodically nomadic. Wireless voice requires full mobility while data generally requires simple portability. Wireless handsets are typically held close to the user's body, introducing additional radio signal attenuation. Data devices are usually set on a surface or held away from the body. The usage factor may result in reduced range for a wireless telephone as compared with a data device. Therefore, the WLAN layout should account for some reduction of radio signal propagation.

Roaming Coverage

Appropriate cell coverage overlap is key to having a successful VoWLAN deployment. But the typical, minimal cell overlap between APs people think about is not sufficient when considering the unique ability of the SpectraLink 8400 Series to also seamlessly roam between the 2.4 GHz and 5 GHz bands. For

this reason, coverage design for roaming between Access Points has to expand beyond typical cell overlap. This section will first cover single band cell coverage and then cover band overlap coverage.

In a single band design, handsets make a determination to roam in less than half the overlapping coverage area from a neighboring AP. Therefore, the coverage area must be adequate so that when a voice user is moving, the handset has time to discover, associate with and connect to the next AP before the signal on the currently connected AP becomes too weak. You will need to understand what impacts RF coverage and cell size and how much cell overlap is required to properly design and configure your VoWLAN.

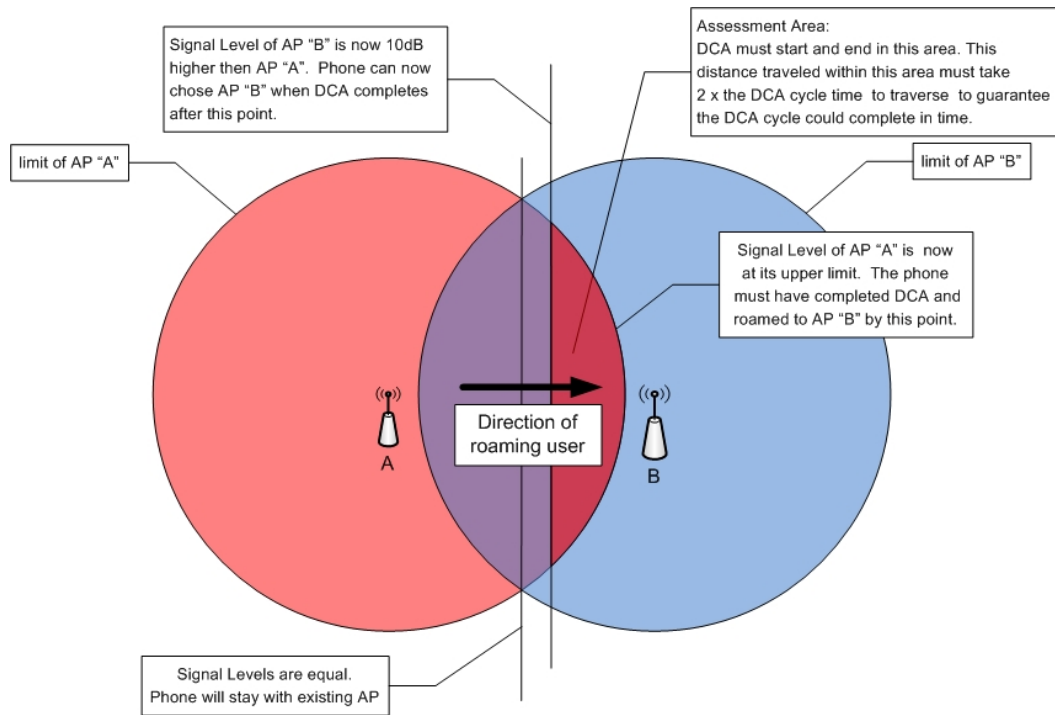
The usable cell size of an AP is dictated by the frequency, signal power level, minimum data rate, and objects that attenuate the signal. A properly designed Wi-Fi network will position APs with sufficient overlapping coverage to ensure there are no coverage gaps, or “dead spots” between them. The result is seamless handoff between APs and excellent voice quality throughout the facility. Sufficient overlapping coverage is usually considered 15% to 20% signal overlap between AP cells in a deployment utilizing maximum transmit power for both handsets and APs. The WLAN layout must factor in the transmission settings that are configured within the APs. The transmission of voice requires relatively low data rates (in low RF signal strength areas) and a small amount of bandwidth compared to other applications. The 802.11 standard includes automatic rate switching capabilities so that as a user moves away from the AP, the radio adapts and uses a less complex and slower transmission scheme to send the data. The result is increased range when operating at reduced transmission data rates.

When voice is an application on the WLAN, APs should be configured to allow lower transmission rates in order to maximize coverage area. If a site requires configuring the APs to negotiate only at the higher rates, the layout of the WLAN must account for the reduced coverage and additional APs will be required to ensure seamless overlapping coverage.

The 15% to 20% of signal overlap between AP cells generally works well with a typical walking speed of the user (the average walking speed of an individual is 3 mph). If the speed of the moving user is greater (such as a golf cart, fork lift or running/jogging) or the cell size is smaller than a different overlap strategy may be necessary for successful handoff between APs. The amount of time needed to find a new AP is a fixed constant. Smaller cells or faster roaming speeds will need larger overlap percentages due to the need to maintain an overlap area that still allows time to find the next access point.

SpectralLink handsets perform Dynamic Channel Assessment (DCA) in between the transmission of voice and control packets to learn about neighboring APs. It takes a little over one second for a DCA cycle to complete. In order to ensure a DCA cycle can complete within the assessment area (see Figure 1), a person moving through the assessment area must be within the area for at least 2-3 seconds to make sure the DCA starts and ends within the assessment area. Failure to complete the DCA cycle within the assessment area can lead to lost network connectivity resulting in a hard handoff, lost audio, choppy audio or potentially a dropped call.

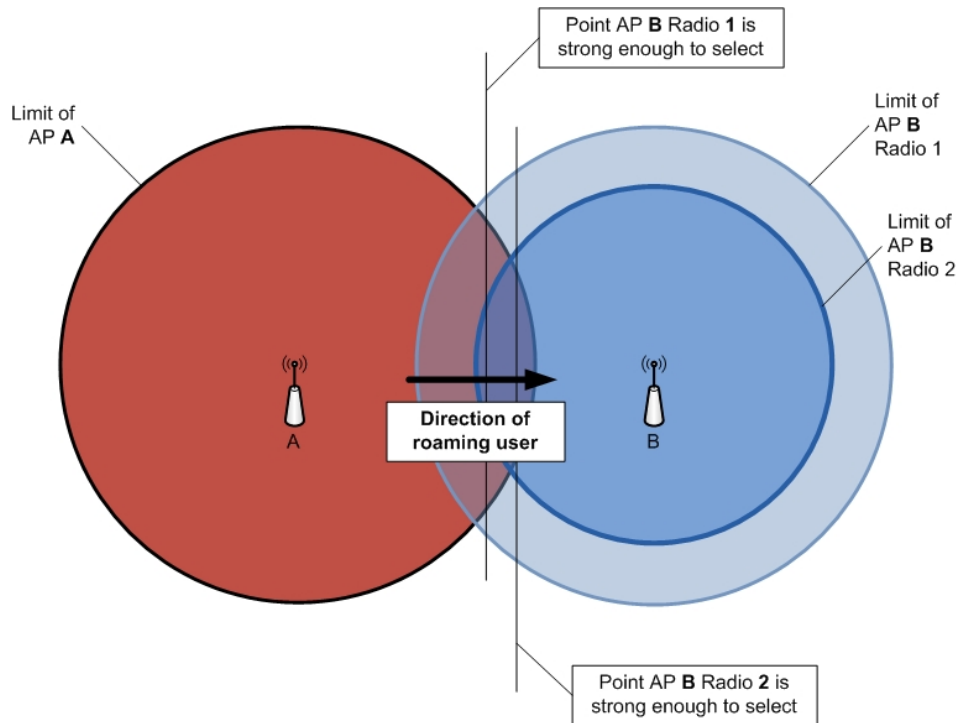
Figure 1 – Dynamic Channel Assessment (DCA)



The handset compares the signal strength of neighboring APs to determine whether to roam from the current AP. In order to roam, the handset has to determine whether another AP should be roamed to, it must be 10 (ten) decibels stronger than the current AP’s signal. Corners and doorways pose a particular design issue. The shadowing of corners can cause steep drop-offs in signal coverage. This is particularly true of the 5 GHz band. Make sure to have adequate cell overlap at and around corners so that the audio stream is not impacted by a user going around corners. This may require placement of an AP at corner locations to ensure appropriate coverage to prevent RF shadows.

In a dual band deployment, cell overlap is considered from both different APs and between different radios on the same AP. To the phone, different radios on the same AP are really just two different APs. The stronger signal will be given the higher priority. In the follow diagram this is easy to see why.

Figure 2 – DCA with Dual Band Deployment



In the case of an AP with both bands enabled and the phone enabled for band roaming, the stronger band will usually be selected. Such things as attenuation caused by the phone being close to the caller's head will influence 5 GHz more than 2.4 GHz so if 2.4 GHz is the weaker signal, there are times it may be selected since 2.4 GHz has better penetration.

Currently there is no way to give a preference to either band. The phone will pick the strongest signal it sees. Therefore, the case for enabling band roaming can be made.

Added capacity, areas of difficult access to provide coverage, such as stairways and elevators, and mixed infrastructure with older equipment, that does not provide the 5 GHz band, are more reasons to enable band roaming.

In the case of capacity, if a radio becomes saturated with calls the AP will tell a phone trying to request access for a call to use another AP. That other AP may be another physical AP or it can be a second radio on the same AP.

When deploying voice on 5GHz, there are times that getting adequate coverage in stairways and elevators becomes a challenge. Either APs are not allowed in those spaces or the structure is such that the signal is too attenuated in portions of the space no matter where they are placed to provide complete coverage. Using 2.4 GHz to cover these areas may be a solution. The APs can be placed outside these spaces and antenna selection and placement can be used to penetrate better than 5 GHz can achieve.

Signal Strength

To provide reliable service, wireless networks should be engineered to deliver adequate signal strength in all areas where the wireless telephones will be used. The required minimum signal strength for all SpectralLink handsets depends on the 802.11 frequency band it is operating in, modulation used, data rates enabled on the AP, and data rate used by the handset at any particular time.

Recommended signal strength characteristics are summarized in Table 1, 2 and 3. Use these values to determine RF signal strength at the 'limit of AP A' or 'limit of AP B', illustrated in Figure 1. The handset should be in the assessment area for 2–3 seconds to allow for smooth roaming handoffs.

Table 1 – 2.4GHz

	2.4GHz 802.11b/802.11g (CCK)				2.4GHz 802.11g (OFDM)							
Rate (Mb/s)	1	2	5.5	11	6	9	12	18	24	36	48	54
Best Practices (dBm)	-75	-70	-69	-65	-67	-66	-64	-62	-60	-56	-52	-47

Table 2 – 5GHz

	5GHz 802.11a (OFDM)								5GHz 802.11n (OFDM)							
Rate (Mb/s)	6	9	12	18	24	36	48	54	6.5	13	19.5	26	39	52	58.5	65
Best Practices (dBm)	67	5	-63	-61	-58	-54	-52	-50	-67	-65	-63	-61	-58	-54	-52	-50

Table 3 – 5GHz

	5GHz 802.11a (OFDM)							
Rate (Mb/s)	6	9	12	18	24	36	48	54
Best Practices (dBm)	-60	-59	-58	-56	-53	-49	-47	-45

The critical factor is the lowest data rate set to “Required” or “Mandatory”¹. Other data rates can be set to “Supported”. The highest AP data rate set Mandatory determines the RF power required by the wireless telephone for proper operation. Broadcast frames (beacons) utilize the lowest “Basic”² data rate and multicast frames (used for the push-to-talk feature) also use the lowest data rate set Mandatory. Unicast frames (data) utilize the ‘best or highest’ data rate which supports low frame errors and low retry rates but will rate scale up or down to use the ‘best’ rate of all available rates.

Referencing Table 1, 2 and 3 the lowest rate set Mandatory (Required) determines the signaling requirements for the wireless telephone in all areas (limit of AP) where they are used.

- For example, if an 802.11b/g access point has 1Mbps, 2Mbps, 5.5Mbps and 11Mbps all set Mandatory, the handset requires -75dBm in all areas.
- For example, if an 802.11b/g access point has 1Mbps Mandatory and other rates set Supported (or “Enabled”) the handset requires -75dBm in all areas.
- For example, if an 802.11a access point has 6Mbps, 12Mbps & 24Mbps set Mandatory and all other data rates set to Supported the handset requires -58dBm to -60dBm in all areas.
- Some AP vendors use a parameter to set the data rate used by broadcast (beacons) and multicast packets. The data rate used by broadcast & multicast packets determine the signal strength required by the wireless handset from Table 1, 2 and 3 above.
- Other AP vendors pick a data rate set Basic for transmission of broadcast & multicast packets. The data rate used by broadcast & multicast packets determine the signal strength required by the wireless handset from Table 1, 2 and 3 above.

SpectraLink handsets have a Site Survey mode that can be used to validate the signal strength it is receiving from the AP. The handset also has a Diagnostics mode which can show AP signal strength, as well as other details, as received during a call. See the [SpectraLink 8400 Wireless Telephone Deployment Administration Guide](#) for details on using the Run Site Survey and Wi-Fi Diagnostics mode features, Section 4 Troubleshooting SpectraLink 8400 Series Handsets.

Although it is possible that SpectraLink handsets may operate at signal strengths which are weaker than those provided in Table 1, 2 and 3; real world deployments involve many RF propagation challenges such as physical obstructions, interference, and multipath effects that impact both signal strength and quality. Designing RF coverage to the required levels will provide an adequate buffer for these propagation challenges, enabling a more reliable and consistent level of performance with low retry rates.

¹ Access Point (AP) vendors refer to this configuration setting differently but the value indicates a data rate that clients must be capable of utilizing in order to associate with the access point. These data rates are also used for different data traffic types by clients and APs which should be considered when designing for coverage requirements.

² The 802.11-2007 Standard defines any data rate set as required to be basic rates. See 802.11-2007 for additional details. (<http://www.ieee.org>)

Access Point Diversity

Full, bi-directional, access point diversity, using both antennas, is critical for improved communications between the AP and wireless handset to keep retry rates low, to improve voice quality and to provide a different & unique path between the AP and handset on any packet retries.

Deployment Considerations

2.4 GHz

The 802.11b, 802.11g and 802.11n standards utilize the 2.4 GHz frequency spectrum. 802.11g 802.11n networks that support 802.11b-only clients must run in protected mode to enable backward compatibility. Protected mode adds considerable overhead to each transmission which ultimately translates into significantly reduced overall throughput. SpectraLink 8400 Series Wireless Telephones, support running in a mixed mode. The overhead associated with performing protected mode transmissions largely negates any benefits of transmitting relatively small voice packets at higher 802.11g data rates. For this reason, when SpectraLink handsets are installed on a mixed 802.11b/g network which is already running in protected mode, the handset must be configured for 802.11b & b/g mixed mode. In an 802.11b/g mixed environment a handset that is configured for the 802.11b and b/g mixed mode will only utilize 802.11b data rates and has no 802.11g functionality while this mode is enabled.

The handset operating in 802.11g-only mode must use a WLAN with data rates set so only 802.11g clients can associate. There must be no 802.11b client connected to and using the WLAN. The way to ensure only 802.11g clients use the WLAN is to set to disable all 802.11b data rates (1, 2, 5.5, and 11Mbps). It is important to include these settings for all SSIDs in the handset coverage area and not just the voice SSID, since this affects the spectrum for the entire area.

5 GHz

The 802.11a standard utilizes the 5.1 GHz to 5.350 and the 5.725 to 5.825 GHz Unlicensed National Information Infrastructure (UNII) Spectrum. Although having the same maximum throughput as 802.11g (54 Mb/s), the increased frequency spectrum at 5 GHz offers up to 23 channels, providing the potential for higher AP density and increased aggregate throughput. There is significant variation in channel availability and use between countries, however, which must be considered for any particular 802.11a deployment.

As compared with the 2.4 GHz frequency of 802.11b/g radio deployments, higher frequency RF signals utilized by the 802.11a/n 5GHz band do not propagate as well through air or obstacles. This typically means that an 802.11a network will require more APs than an 802.11b/g network to provide the same level of coverage. This should be taken as a guideline however, as signal propagation may also be impacted by the output power settings of the AP and the antenna type. A comprehensive wireless site survey focusing on VoWLAN deployments should be conducted to identify the specific needs for each environment.

802.11n

The SpectraLink 8400 Series handsets support the 802.11n standard. However, currently only 20 MHz channels are supported, not 40 MHz channels (bonded channels). The 802.11n standard most typically is used in the 5 GHz band.

Like the issue of 802.11g clients used alongside 802.11b clients, 802.11n clients must operate in a protected mode when 802.11a clients are co-existing. The same issues apply with the protected mode operation and small packet sizes and as such when sending voice packets the phone will only send using 802.11a. It can receive 802.11n packets from the AP though.

The SpectraLink 8400 Series handset will use many 802.11n features and enhancements when enabled. The configuration file parameters to enable 802.11n features are:

```
<device.wifi.dot11n device.wifi.dot11n.enabled="1"> <device.wifi.dot11n.enabled
device.wifi.dot11n.enabled.set="1"> </device.wifi.dot11n.enabled> </device.wifi.dot11n>
```

Set the parameter to zero as follows: <device.wifi.dot11n device.wifi.dot11n.enabled="0"> to disable 802.11n features.

The Polycom SpectraLink 8400 Series wireless handset 802.11n features include:

- Number of antennas: 1
- Data Rates: MCS0 – MCS7 (20MHz channels only)
 - TX: 6.5Mbps to 65Mbps (w 800ns Guard Band interval)
 - RX: 7.2Mbps to 72.2Mbps (w 400ns Short Guard Band interval)
- Short Guard Band Interval (400ns GI): RX Only
- Frame Aggregation
 - A-MSDU: RX only (check)
 - A-MPDU: Disabled (phone can't receive, but can coexist in the same network with other devices that do)
- Protection (Backward Compatibility)
 - Mixed Mode: Yes
 - 40MHz Frames: No Support
 - RTS/CTS or CTS to Self: Yes (for 802.11b STAs)
- Greenfield Support: Yes
- MIMO (multiple spatial streams): No (one antenna has no MIMO)
- Space-Time Block Coding: RX only

Access Point Configuration

Several fundamental access point configuration options must be considered prior to performing a site survey and deploying a voice-capable WLAN infrastructure. The SpectraLink 8400 Series handset provides support for IEEE 802.11b, 802.11g, 802.11a and 802.11n radio types. The selection of radio type has significant impact on the overall configuration and layout of the WLAN infrastructure. This fundamental selection determines most other configuration considerations. In general, however adjacent APs in three dimensions (above, below and beside) must use different, non-overlapping, radio channels to prevent interference between them regardless of 802.11 radio type.

This document does not cover all issues or considerations for WLAN deployment. It is strongly recommended that Polycom Professional Services be engaged to answer additional questions about configurations that may affect voice quality or wireless telephone performance. In addition, configuration guides for WLAN infrastructure, which are available from the Polycom web site, should be followed closely.

Channel Selection

The 802.11b/g standard provides for three non-interfering, non-overlapping channels - channels one, six and eleven in North America. Access points within range of each other should always be set to non-interfering channels to maximize the capacity and performance of the wireless infrastructure. Figure 4 - 802.11b/g Channels illustrates the correct deployment methodology for 802.11b/g deployments.

If adjacent access points in three dimensions (above, below or beside) are set to the same channel, or utilize channels with overlapping frequency bands, the resulting interference will cause a significant reduction in the network performance and throughput, and will degrade overall voice quality. A channel space of twenty five MHz, five channels or greater should be used to configure neighbor APs for non-interfering channels. Figure 5 - 802.11a Non-interfering Channels with Overlapping Cell Coverage represents the 2.4 GHz frequency range, indicating the overlap in channel frequencies.

Figure 3 - 802.11b/g Non-interfering Channels with Overlapping Cell Coverage

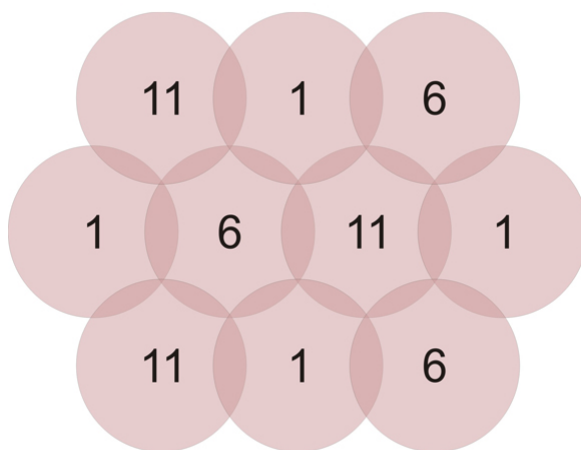
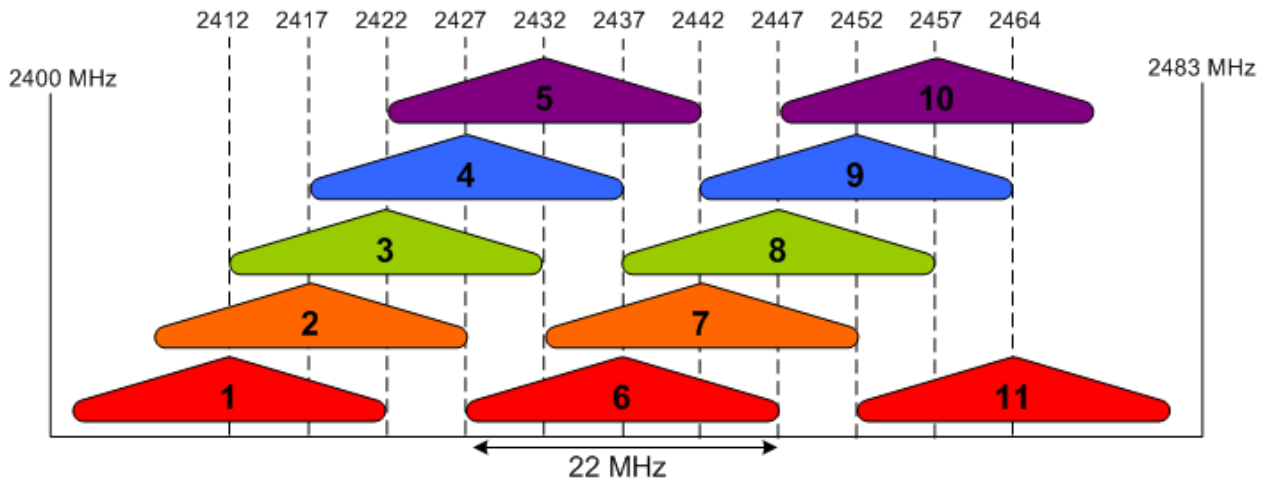
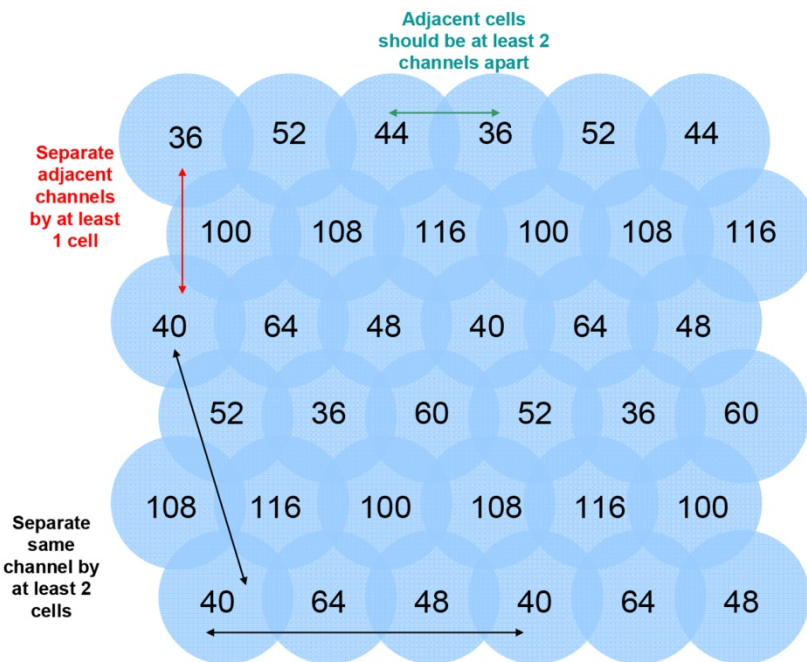


Figure 4 - 802.11b/g Channels



With more available channel options, the 802.11a standard has improved the flexibility of WLAN layouts, and enabled the possibility for greater density of APs. In an 802.11a deployment, all 23 channels are considered non-overlapping, since there is 20 MHz of separation between the center frequencies of each channel. However, because there is some frequency overlap on adjacent 802.11a channel sidebands, there should always be at least one cell separating adjacent channels and two cells separating the same channel. This methodology is depicted in Figure 5.

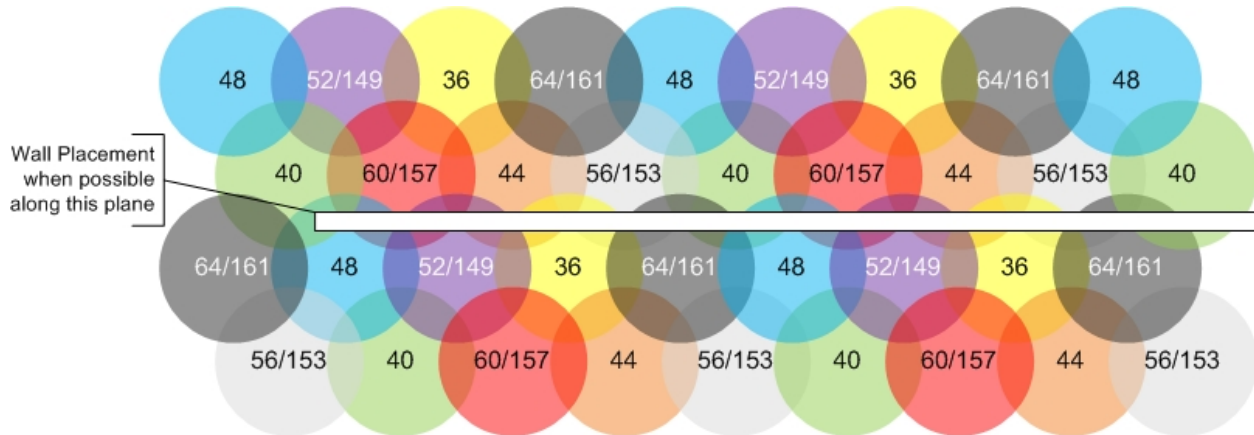
Figure 5 - 802.11a Non-interfering Channels with Overlapping Cell Coverage



Some deployment scenarios require limiting the number of 802.11a channels. A key reason is to improve roaming performance. With 802.11a there are four channel bands available to choose from.

These channel bands comprise a number of individual channels over a specific range of frequencies in the 5GHz range. These bands include UNII-1 (5.15 – 5.25GHz), UNII-2 (5.25 – 5.35GHz), UNII-2 Extended (5.47 – 5.725GHz) and UNII-3 (5.725 – 5.825GHz). The two UNII-2 bands are DFS (Dynamic Frequency Selection) bands. The 802.11a specification identifies DFS bands as overlapping with the frequencies utilized globally by radar systems. Because of this shared use for these two frequency ranges the 802.11a standard calls for a zero contention behavior from wireless devices on the channels in these bands. This means that a DFS channel can possibly become unavailable due to the detection of radar signals by an access point on one of the DFS channels as required by the standard. In addition, the full set of channels available in the U.S. may not be available outside the U.S. Refer to your local RF governing body for specific channel availability. It is important to note that the SpectraLink 8400 Series handset requires that access points configured to utilize DFS channels must advertise support for Channel Announcement as defined in the IEEE 802.11h³ specification. Handsets will not be able to associate to access points that do not advertise Channel Announcement. In some cases, where use of DFS channels is either not allowed due to legal restrictions or use of DFS channels is not desired, an eight-channel plan is recommended as depicted in Figure 6. As illustrated, there is still separation of adjacent channels by at least one cell. Same channel separation can now be a minimum of one cell in a single plane, rather than in three dimensions, because only eight channels are being utilized instead of all 23. Many sites use this pattern with no reported issues.

Figure 6 - Eight 802.11a Non-interfering Channels with Overlapping Cell Coverage (52/149, 64/161, etc. shows 1st DFS range channel or upper non-DFS range)



To deploy an eight-channel plan for North America, 802.11a networks use channels 36, 40, 44, 48, 149, 153, 157 and 161, which are part of the UNII-1 and UNII-3 bands, or channel 165 ISM Band. This will avoid the DFS channels. In Europe 149, 153, 157, 161 and 165 are not available so the DFS channels 52, 56, 60, and 64 should be used instead. Try to design your AP cell layout so that walls can help divide the cell plane where single cell spacing is used in a single plane to help attenuate the signal, which will help

³ IEEE 802.11h – Channel Announcement support is identified in the beacon of access points where the Spectrum Management bit is set, 1 for enabled or 0 for disabled.

to prevent co-channel interference. Doing so will provide optimal cell co-channel separation, as illustrated in Figure 6.

AP Transmission Power and Capacity

The AP transmit power should be set so that the handsets receive the required minimum signal strength, as defined in Section 0 of this document. For deployments with higher AP density, lower transmit power settings are typically required to prevent channel interference. Maximum AP power settings vary by band and by channel, and can vary between countries. Local regulations should always be checked for regulatory compliance considerations. In addition, maximum power output levels may vary by AP manufacturer. Where possible, all APs should be set to the same transmit power level within a given radio type. For example, set all 802.11a radios to 50mW and set all 802.11b and 802.11g radios to 30mW.

It is crucial to then set the transmit power of the handset to match the transmit power of the APs for that band. This will ensure a symmetrical communication link. Mismatched transmit power outputs will result in reduced range, poor handoff, one-way audio and other quality of service or packet delivery issues. SpectraLink Wireless Telephones support transmission power settings in the range from 5mW to 100mW (in the United States).

In mixed 802.11b/g environments, Polycom recommends configuring the transmit power of the 802.11b and 802.11g radios to the same setting, if they are separately configurable. For example, set both radios to 30mW to ensure identical coverage on both radios. For mixed 802.11a/b/g environments, where the AP utilizes all three radio types, AP placement should first be determined by modeling for the characteristics of 802.11a, since this environment will typically have the shortest range. Then, the transmit power of the 802.11b and 802.11g radios should be adjusted to provide the required coverage levels and cell overlap for those networks, within the already established AP locations.

Interference

Interference on a wireless network may originate from many sources. Microwave ovens, Bluetooth devices, cordless phones, wireless video cameras, wireless motion detectors, and rogue APs are among the many potential interfering RF (radio frequency) sources. In general, devices that employ or emit radio frequency signals within a given radio coverage area will have the potential to cause unwanted signal interference.

Radio frequency spectrum analyzers can be used to help identify the sources of such interference. Once identified, interference is best mitigated by removing the interfering device(s) from the network area. Otherwise, it may be possible to change the channel setting of the interfering device to avoid conflict with the surrounding APs. If this is also not possible, then it may be possible to change the channel of the surrounding APs to avoid as much radio frequency overlap with the interfering device.

A documented facility-wide radio frequency usage policy will help control sources of RF energy. Ideally, any RF generating device should have prior approval before introduction onto the property or installation in any building or structures.

Only Bluetooth headsets that support EDR and eSCO protocols are recommended for the SpectraLink 8400 Series handsets.

Bluetooth headset use is not recommended with phones and other peripheral devices that have the 2.4 GHz Wi-Fi band enabled.

Multipath and Signal Distortion

For 802.11a/b/g environments, multipath distortion is a form of RF interference that occurs when a radio signal has more than one path between the transmitter and the receiver causing multiple signals to be detected by the receiver. This is typically caused by the radio signal reflecting off physical barriers such as metal walls, ceilings and other structures and is a very common problem in factories and storage environments. Multiple converging wave fronts may be received as either an attenuated or an amplified signal by the receiver. In some instances, if the signals arrive exactly out of phase, the result is a complete cancellation of any RF signal. In 802.11n networks multipath is an exploited feature, rather than a potential interference problem. The multiple radios used for 802.11n (up to three in an AP) provide increased throughput. The resulting multipath effects of the multiple radios are used to obtain increased range and overall throughput. The remainder of this section focuses on 802.11a/b/g deployments in which it is favorable to mitigate multipath.

Multipath can cause severe network throughput degradation because of high error rates and packet retries. This in turn can lead to severe voice quality impairment with SpectraLink Wireless Telephones. Correctly locating antennas and choosing the right type of antenna can help reduce the effects of multipath interference.

AP diversity antennas should always be used to help improve performance in a multipath environment. A diversity solution uses two antennas for each AP radio, and will send and receive signals on the antenna which is receiving the best signal from the wireless client. Diversity in an AP with two antennas, which provide signaling to the same geographic area, provides a unique signal path from each antenna to the handset. This greatly increases the probability that both the AP and the handset will receive better signal quality in multipath environments. Most Access Points support receive-diversity in that they accept the received transmission on the antenna that is getting the best signal. Some also support full transmit diversity where the transmission is made on the same antenna that was last used to receive a signal from that specific client. In order to provide optimal voice quality, Polycom recommends the use of APs supporting both receive and full transmit diversity in environments where multipath is an issue. This will help optimize the WLAN for all wireless clients. External antennas provide additional flexibility in type (omnidirectional or directional), mounting options and gain. External antennas can be separated from 4.5 inches to 5 feet at each AP radio. Full AP antenna diversity allows the other antenna to be used whenever a packet is retried and is recommended.

Access point antennas should not be placed near a metal roof, wall, beam or other metal obstruction in any environment, as this will amplify the reflection effects. Additionally, antennas should be positioned so that they have line of sight (LoS) to most of the clients that they service. Additional instructions from the wireless network infrastructure vendor should be followed with regard to antenna selection and placement to provide correct AP diversity operation.

Site Surveys

A wireless RF site survey is highly recommended for any wireless network deployment. However, it is especially critical for VoWLAN and is essential for large or complex facilities. An RF site survey can ensure that the wireless network is optimally designed and configured to support voice by confirming RF signal levels, cell overlap, channel allocation/reuse, co-channel & adjacent interference, packet transmission quality, packet retry rates, antenna type, gain & placement and other deployment considerations. While many tools exist that allow customers to perform their own assessment, Polycom recommends a professional site survey to ensure optimum coverage and minimum interference. Polycom offers a full suite of site-survey services, which take advantage of the extensive experience from years of successful deployments that will ensure a WLAN is properly configured and optimized to support wireless voice.

To verify coverage of an installed Wi-Fi network, Polycom handsets offer a site-survey mode that can be used to validate the AP locations and configurations are both correct and adequate. This mode detects the four strongest AP signals and displays the signal strength along with the AP channel assignments. The site survey mode may be used to detect areas with poor coverage or interfering channels; check for rogue APs; confirm the Service Set Identification (SSID) and data rates of each AP and include the security and QoS mechanisms supported by the AP; and detect some AP configuration problems. With SpectraLink handsets, the entire coverage area must be checked to ensure that at least one access point's output meets the signal strength requirements summarized in Section 0 of this document. If the site-survey mode indicates that two APs are using the same channel within range of the handset, it is important to adjust the channelization to avoid channel conflicts.

After a site survey is complete, coverage issues can be resolved by adding and/or relocating APs if necessary. Overlap issues may be resolved by reassigning channels or by relocating some access points. When adjustments are made to the WLAN configuration an additional site survey or site verification should be performed to ensure that the changes are satisfactory and have not had an adverse impact in other areas of coverage.

Wireless Telephone Call Capacity

Network capacity requirements factor into the number of APs required, although in most cases the coverage area is the primary factor. Data traffic is often very "bursty" and sporadic. This is typically acceptable because data applications can tolerate network congestion with reduced throughput and slower response times. Voice traffic cannot tolerate unpredictable delays, where the bandwidth requirements are much more constant and consistent. Voice traffic can also be predicted using probabilistic usage models, allowing a network to be designed with high confidence in meeting anticipated voice capacity requirements. Beyond the standard IP telephony design guidelines, some considerations should be addressed for VoWiFi with SpectraLink handsets.

Access Point Bandwidth

Several factors determine AP bandwidth utilization during a telephone call. The first is the VoIP protocol used and its characteristics. The type of codec utilized combined with the packet rate will determine the size of the voice packets along with any additional overhead information required for the protocol. Payload data will generally account for 30-50% of a typical voice packet, with 802.11 and IP protocol overhead filling the rest. The 802.11 protocols include timing gaps for collision avoidance, which means bandwidth utilization is more accurately quantified as a percentage of available throughput rather than actual data throughput.

The percentage of bandwidth required is greater for lower 802.11a/b/g data rates; however it is not a linear function because of the bandwidth consumed by the timing gaps and overhead. For example, a call using standard 64 Kbps voice encoding (G.711ulaw) utilizes about 4.5 percent of the AP bandwidth at 11 Mbps, and about 12 percent at 2 Mbps. In this example, four simultaneous calls on an AP would consume about 18 percent of the available bandwidth at 11 Mbps or about 48 percent at 2 Mbps or about 90 percent at 1Mbps.

The maximum number of simultaneous telephone calls an AP can support is determined by dividing the maximum recommended bandwidth usage by the percentage of bandwidth used for each individual call. Note that approximately 20 to 35 percent of the AP bandwidth must be reserved for channel negotiation and association algorithms, occasional retries, and the possibility of occasional transmission rate reductions caused by interference or other factors. Therefore, 65 to 80 percent of the total available bandwidth should be used for calculating the maximum call capacity per AP. For example, if all calls on an AP are using a theoretical 5.4 percent of the bandwidth at 11 Mbps, the actual number of calls expected at that rate would be about 12 (65 percent of bandwidth available / 5.4 percent theoretical bandwidth utilized per call). Lower overall bandwidth is available when there are a greater number of devices associated with an AP or when lower data rates are used for the telephone call or calls.

Even with all of the known variables, there are many other vendor-specific characteristics associated with individual APs that make it difficult to quantify the precise number of concurrent calls per AP, without thorough testing of specific configurations. Polycom WLAN configuration guides identify the maximum number of calls per AP for specific models and specific QoS mechanisms that have been tested to be compatible with the SpectraLink handset.

Push-to-Talk Multicasting

SpectraLink 8400 Series handsets provide push-to-talk (PTT) functionality using the Polycom-proprietary SpectraLink Radio Protocol (SRP) ADPCM encoding. Because the PTT mode uses IP multicasting, all APs on the subnet will re-transmit a PTT multicast packet. This can be limited to only the APs that are handling one or more PTT-enabled handsets by enabling the Internet Group Management Protocol (IGMP) on the wired infrastructure network.

When SpectraLink 8400 Series handsets are deployed on a network with previous versions of SpectraLink handsets, some interoperability considerations must be observed. The SpectraLink 8400

Series handsets have 24 PTT channels plus one priority channel and one emergency channel available. Earlier models enabled only eight PTT channels with no priority channel. When PTT is activated on a network using a mix of handset versions, only the eight common channels will be available for inter-communication with older handsets.

Quality of Service (QoS)

The SpectraLink 8400 Series handset uses Wi-Fi Multimedia (WMM), WMM Power Save and WMM Admission Control mechanisms to deliver enterprise-grade QoS. The handset is compatible with AP implementations of the three WMM features and all three are required to provide the best user experience. Therefore, use of all three WMM specifications is highly recommended by Polycom and is the default operating mode of the handset. However, Polycom does offer the flexibility to disable the use of WMM Admission Control. See Section 4.2.3 for additional detail and possible negative effects. The use of WMM and WMM Power Save are required.

The WMM specifications are each based on a component of the 802.11e standard, which was ratified in 2005 by the IEEE. 802.11e is a 'toolbox' full of features and the appropriate tool can be used by applications for QoS on the WLAN as long as both the client device and the AP support them.

To use Wi-Fi Standard QoS, the AP needs to support and be configured to enable the corresponding features. In addition, Proxy ARP is an AP feature that optimizes bandwidth utilization by limiting the amount of broadcast and multicast traffic that is sent over the WLAN. Enabling Proxy ARP allows a given access point to forward traffic to a handset in standby or in-call; thereby, decreasing delays in the delivery of voice packets to the handset. When Wi-Fi Standard QoS is used, the APs are required to have Proxy ARP enabled. Consult the appropriate Polycom [VIEW Configuration Guide](#) for enabling these features and the proper configuration in your WLAN product.

WMM

WMM is based on IEEE 802.11e Enhanced Distributed Coordination Access (EDCA). Wi-Fi networks that implement WMM optimize the allocation of shared network resources among competing applications by prioritizing media access depending on the traffic type. This approach brings flexibility in networks that have concurrent applications with different latency and bandwidth requirements.

WMM defines four access categories derived from 802.1d, which correspond to priority levels, as shown in Table 4. Although the four access categories were designed with specific types of traffic and associated priorities in mind, WMM relies on the application to assign the appropriate access category for the traffic they generate. Once the application assigns each packet to an access category, packets are then added to one of four independent transmit queues in the AP and client. Once transmitted onto the wireless network applications may compete for available bandwidth, resulting in packet collisions. When this happens the access category used will determine the retransmission timing. The higher the priority level, the lower the required wait time and random "back-off" window. High-priority packets transmitted by the client device that are assigned to AC_VO wait for two slot times with a random back-off of 0-3 slots. Whereas low-priority packets assigned to AC_BK wait for seven slot times with a random back-off of 0-15 slots.

Table 4 - WMM Access Categories

WMM Access Category	Priority level	802.1d tags	Client wait time + random backoff window (slots)	SIP traffic type
Voice (AC_VO)	highest	7, 6	2 + 0 to 3	Voice
Video (AC_VI)		5, 4	2 + 0 to 7	Call control
Best Effort (AC_BE)		0, 3	3 + 0 to 15	Other (PTT, OAI, RTLS)
Background (AC_BK)	lowest	2, 1	7 + 0 to 15	Not used

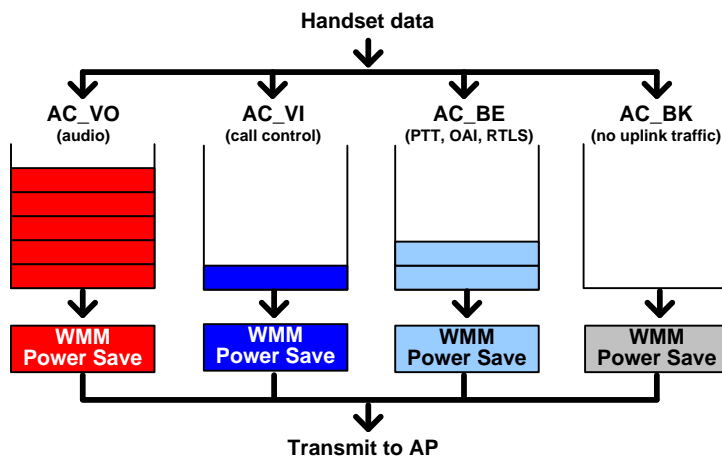
WMM Power Save

The second component of WMM, WMM Power Save, is based on the IEEE 802.11e Unscheduled-Automatic Power Save Delivery (U-APSD) mechanism and is an enhancement over the legacy 802.11 power save mechanism. The application-based approach used in WMM Power Save enables individual applications to decide how often the client needs to communicate with the access point and how long it can remain in a 'restful' state. In addition, WMM Power Save increases transmission efficiency because the same amount of data can be transmitted in a shorter time and using fewer frames.

Two benefits of WMM Power Save for the SpectraLink 8400 Series handset are to conserve battery life and to make AP handoff decisions without the risk of missing packets.

Power save behavior is negotiated during the association of a handset with an AP. WMM Power Save or legacy power save is set for each WMM access category transmit queue separately, as shown in Figure 7. For each access category queue, the AP will transmit all the data using either WMM Power Save or legacy power save, using the assigned WMM QoS mechanism.

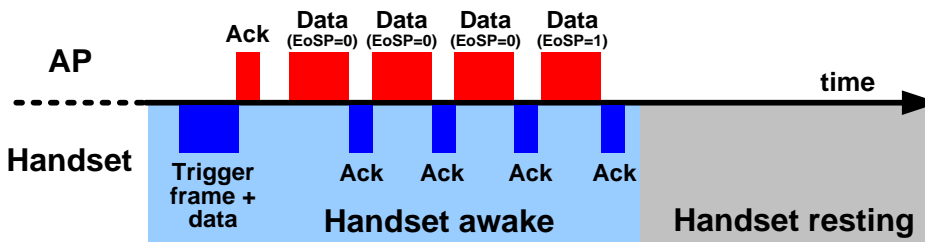
Figure 7 – WMM Queues Using WMM Power Save



Applications that do not initiate power save can still coexist with WMM Power Save enabled applications on the same device. In this case, data from the other applications will be delivered with legacy power save.

The transmission process begins with the handset sending a trigger frame on any of the WMM access categories using WMM Power Save to indicate that it is awake and ready to download any data frame that the AP may have buffered (Figure 8). After the AP receives the trigger frame, it sends an acknowledgement frame (ACK) to indicate it is ready to send the data. Each frame transmitted by the AP indicates whether more data for the handset is buffered (more data = 1). When the AP is ready to stop sending downlink data it sends an EOSP (End of Service Period) message to the handset. If the handset has uplink data to send, it will need to send a new trigger frame to the AP. Otherwise the EOSP is the handset's indication to resume low power mode.

Figure 8 – WMM Power Save Timing



WMM Admission Control

The third component of WMM, WMM Admission Control, allows the AP to manage its available 'air time' based on traffic requirements submitted by associated clients and rejects requests if insufficient resources are available. Use of WMM Admission Control avoids over-subscription of the AP, therefore preserving and protecting QoS for all associated devices. For this reason, enabling WMM Admission Control (not enabled by default) is the recommended best practice.

However, Polycom does also offer the flexibility to disable the use of WMM Admission Control in the handset in order for it to participate in WLANs where WMM Admission Control is not used or not supported. Additional details and possible negative results on this setting are provided at the end of this section.

WMM Admission Control uses another optional feature from 802.11e, which is critical to delivering enterprise-grade VoWLAN. The Admission Control facility adds the capability to manage how the total medium time is reserved and used by various devices and QoS priorities. The AP controls the medium time by allocating a percentage of the total time, measured on a per second basis, in response to requests from each participating client. Any client that does not participate in the admission control allocations must send only low-priority traffic (typically assigned AC_BE and AC_BK). For this reason, all wireless devices using AC_VO or AC_VI will also need to use admission control to maintain their QoS settings.

Participating WLAN clients gain an allocation of medium time by sending an explicit request to the AP, called an ADDTS (add traffic stream) Request, describing the nature of the traffic flow the client anticipates it will use. This includes factors such as total bandwidth in bits per second, average packet size, expected PHY data rate, etc. From this the AP can determine how much medium time the client is likely to use as well as gain some understanding of the expected traffic flow – whether it is a flow with few, large packets or many, small packets, for example, or whether the traffic is “bursty” or fairly regular. The SpectraLink handset will indicate its traffic as small, frequent packets at a consistent flow. From the client’s ADDTS Request, the AP can enforce a number of policy decisions in determining whether the traffic flow requested will fit well into the existing traffic streams. Usually, there is spare bandwidth available, and the AP will admit the traffic and the client proceeds normally using WMM and WMM Power Save techniques to do the packet transfers.

Occasionally, the AP may determine that the traffic load already in place on the AP is incompatible with the requested traffic stream. In this case, the AP refuses the ADDTS Request, letting the client know that if it starts to exchange packets at the described rate it will affect its own or other clients’ traffic. The client is then free to try another nearby AP instead, thus ensuring that all clients’ traffic will maintain a high level of QoS.

Typically, admission control is enabled only for high-priority traffic, usually AC_VO and AC_VI. The lower-priority traffic will not significantly affect the QoS of the higher-priority traffic in the case where the medium time is over-used, so this is acceptable and it leaves an option for client devices that do not support admission control to use AC_BE and AC_BK.

In most respects, WMM Power Save and WMM Admission Control are separate facilities and operate independently. However, the same mechanism that supports WMM Admission Control, the ADDTS Request, can also be used to more finely tune control over WMM Power Save. This allows a client to go beyond simply setting the power save mode for each access category transmit queue. With an ADDTS Request, a client can separately control the uplink and downlink directions of each access category. This allows the client more flexibility over which types of traffic will be buffered and how they will be delivered by trigger frames, thus allowing it to optimize the ‘restful’ state times and durations.

The benefits of using WMM Admission Control for VoWLAN are clear; handset audio quality is preserved and protected by avoiding over-allocation of AP resources. Therefore, its use is highly recommended.

However, there may be circumstances in which the use of WMM Admission Control may not be feasible or practical. If this is the case, WMM Admission Control should be set to optional in the SpectraLink 8400 Series handset and the ACM (Admission Control Mandatory) setting in the APs should be cleared for AC_VO and AC_VI. This configuration can be used to share the network with any other devices that use AC_VO and AC_VI but do not have support for admission control. The result of this configuration is the SpectraLink 8400 Series handset operates using WMM and WMM Power Save, but there is no admission control on the WLAN. In heavily loaded networks the result can be poor handset audio quality. Therefore, careful planning to ensure adequate AP bandwidth is necessary.

DSCP for Wi-Fi Standard QoS Deployments

Differentiated Services Code Point (DSCP) is a field in the header of IP packets for packet classification purposes. DSCP is used to indicate an assigned priority level to individual packets that will be used through the network. For traffic going from the handset to the call server, WMM access categories address WLAN prioritization, and DSCP addresses prioritization on the wired network.

The defaults values are:

- Voice: 46
- Control (call control): 44
- Other (PTT, OAI and RTLS): 0

Default DSCP values can be accepted or replaced. Note that this is not configurable from the keypad. Regardless of the DSCP values selected, the WMM access categories will be used for sending the various traffic types through the WLAN as indicated in Table 4.

For traffic from the call server to the handset, call server DSCP determines priority on the wired network, but is also used by most WMM-capable access points to determine which WMM access category to use when placing the packet over the air. Please refer to your WLAN vendor's documentation for detailed instructions on how to map DSCP values to WMM access categories. Refer to your call server vendor's documentation for setting DSCP values for traffic from the call platform.

It is highly recommended that the DSCP values for the different types of traffic out of the call server (voice or control) match the settings entered in the phone configuration files.

Security

Proper security provisions are critical for any enterprise Wi-Fi network. Wireless technology does not provide any physical barrier from malicious attackers since radio waves penetrate walls and can be monitored and accessed from outside the facility. The extent of security measures used is typically proportional to the value of the information accessible on the network. The security risk for VoWLAN is not limited to the typical wired telephony concerns of eavesdropping on telephone calls or making unauthorized toll calls, but is equivalent to the security risk of the data network that connects to the APs. Several different security options are supported on SpectraLink Wireless Telephones. Determining the proper level of security should be based on identified risks, corporate policy and an understanding of the pros and cons of the available security methods.

VoWLAN Security

VoWLAN has specific characteristics that influence the supported security mechanisms. For instance, a Wi-Fi handset generally has a simple user interface, limited computing resources and is battery-operated. The packet delay tolerance is very low compared to a device primarily used for data applications. In addition, a voice handset is highly mobile within the coverage area, requiring frequent handoffs between APs as the user roams throughout the facility.

When the handset roams between APs and maintains WLAN connectivity it is referred to as a 'soft' handoff. During soft handoffs the voice stream is maintained and there should be no perceptible changes in audio quality while the user is in-call. A 'hard' handoff occurs when the handset loses AP connectivity and must re-acquire the WLAN. In this case, audio impairments are possible. The degree of the audio degradation is influenced by the security method used; the more complex the mechanism, the greater the duration of time in the security exchange.

Selection of a WLAN security method is a trade-off between the degree of security, the end-user experience and the complexity of management. Generally, the most secure methods require the greatest degree of management and have the greatest potential negative impact on the end-user experience. Polycom offers several security options that span the range from basic protection with minimal effort to robust protection with involved IT management.

Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) encryption was defined in the original 802.11 standard and has since been replaced by much stronger WLAN security methods. Because some customers chose this method for its ease of administration, the SpectraLink 8400 Series handset supports it. The handsets can use either 40-bit or 128-bit key lengths.

Wi-Fi Protected Access (WPA) and WPA2

Wi-Fi Protected Access (WPA) is based on draft 3.0 of the 802.11i specification and uses TKIP (Temporal Key Integrity Protocol) encryption. WPA2 is based on the ratified 802.11i standard. The major enhancement of WPA2 over WPA is the inclusion of the Advanced Encryption Standard (AES), which is widely accepted as one of the most secure encryption algorithms available.

WPA2 has two different authentication modes, Personal and Enterprise, both of which are supported on the SpectraLink 8400 Series. Authentication is the process that occurs after WLAN association in which the handset and authentication server verify each other's credentials, then allow the handset access to the network.

WPA Personal, WPA2 Personal

Personal mode uses a password-based authentication method called Pre-Shared Key (PSK). Personal mode is good for time-sensitive applications such as voice, because the key exchange sequence is limited and does not adversely affect roaming between APs. The PSK can be entered in hexadecimal or as an ASCII passphrase from the handset's administration menu or via configuration files. The handset supports both WPA Personal and WPA2 Personal modes.

WPA2 Enterprise

WPA2 Enterprise security mode requires a WLAN device to mutually validate credentials via 802.1X with a RADIUS server on the network every time the device roams to a new AP. With each roam, authentication delays may cause dropped packets resulting in long delays between APs and audio dropouts. The size of the credentials used and the location of the RADIUS authentication server can significantly affect the duration of the delay. Larger credentials are more secure, but take more time to process. RADIUS servers that are local and reside on high-speed Ethernet switches are faster to respond to authentication requests than those in remote locations.

Because the use of WPA2 Enterprise requires 802.1X authentication by the device and that each exchange can cause delays during the AP handoff, Polycom requires the use of a fast AP handoff mechanism. Fast AP handoff techniques allow for the part of the key derived from the authentication server to be cached in the wireless network, thereby shortening the time to renegotiate a secure handoff. The SpectraLink 8400 Series handset offers two 802.1X authentication types (PEAPv0 with MSCHAPv2 and EAP-FAST) and two fast AP handoff mechanisms (OKC and CCKM). The combination of the selected 802.1X authentication type and fast AP handoff mechanism is expected to result in soft handoffs as the handset user roams the facility.

It is important to note that the placement of the RADIUS authentication server on the network can have a direct effect on the overall performance of the wireless handset when acquiring WLAN connectivity and during AP handoff. If the authentication server is accessible only across a WAN (Wide Area Network) link then there is the risk that additional latency will be introduced. In situations where a wireless telephone experiences a loss of coverage and must reacquire the network while in-call there is a high risk of long audio gaps. The required use of the fast AP handoff methods does not mitigate the risk of

'hard handoff' situations where full 802.1X key exchanges must re-occur. It is always recommended that the authentication server be located within the same geographic location, on a local network segment, as the network to which it will be providing authentication services. For more information on the fast AP handoff options see Section 0.

PEAPv0/MSCHAPv2

PEAP (Protected Extensible Authentication Protocol) was developed by Microsoft, Cisco and RSA Security for 802.1X authentication on WLANs. PEAPv0 with MSCHAPv2 is one of the most-commonly used PEAP subtypes hence its use on the SpectraLink 8400 Series handset. PEAP makes use of a server-side public key certificate to authenticate the server and creates an encrypted tunnel to exchange information between the server and the client. Larger certificate key sizes provide stronger encryption, but are more computationally intensive and therefore take more time to process. This longer processing time to perform the 802.1X key validation means that the handset cannot communicate with the rest of the network for a longer time, and cannot receive or transmit audio packets, resulting in missing audio when in call. While the handset supports key sizes of 512, 1024, 2048 and 4096 bits, a key size of 512 or 1024 bits is recommended, as these sizes balance the degree of security with the need to maintain audio during WLAN acquisition and re-acquisition during roaming.

PEAP root certificates must be loaded using the provisioning server, during initial handset configuration. Each handset can support multiple root certificates loaded into non-volatile memory. Certificates must be in PEM (base-64) format to be loaded onto handsets. The ASCII characters of the PEM format certificate will be pasted directly into the handset configuration file placing the certificate in the appropriate certificate store location. Other certificate formats exist, and can be translated to PEM format by third party tools before being loaded to the handset.

A username (relates to the device name, not necessarily an end-user) and password are entered via the initial handset configuration files.

Certificates carry a validation period (start and end date of validity). When using a certificate, the handset will attempt to check its validity by using time information available from a Simple Network Time Protocol (SNTP) server. If no time information is available, the certificate is assumed to be valid, making the use of a time source optional but still important. If the certificate is deemed expired (or not yet valid) the handset will stop operating and display an error message. SNTPSSNTPS

EAP-FAST

EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling) was created by Cisco as a replacement for LEAP (Lightweight Extensible Authentication Protocol). EAP-FAST has since gained adoption by WLAN vendors besides Cisco and is growing in popularity.

Rather than relying on certificates, EAP-FAST use a Protected Access Credential (PAC) to establish a tunnel in which client credentials are verified. PAC files may be provisioned either over-the-air (called server unauthenticated or Phase 0) or manually via initial provisioning of handset configuration files. Server unauthenticated provisioning is easy to manage, but offers a lesser degree of security than

provisioning with a USB cable. The administrator must choose between the two methods by weighing the desired level of security with ease of management.

Much like certificates, PAC files can be loaded into the SpectraLink 8400 Series handset by first converting the PAC file into a base-64 format and then pasting the ASCII string that results into the handset's configuration file.

OKC

Opportunistic Key Caching (OKC), sometimes called PMK (Pairwise Master Key) caching, is a fast AP handoff technique specified in the 802.11i standard. OKC has growing support among enterprise WLAN vendors and is the only standards-based fast AP handoff method supported today. Check Polycom's WLAN Certified Products Guide to find a list of WLAN products tested for OKC support.

The combination of either PEAP or EAP-FAST and OKC is expected to result in soft handoffs, once the initial 802.1X exchange has occurred establishing network connectivity for the handset. The soft handoffs occur as the user roams within the coverage area and the WLAN infrastructure retains authentication key information for the associated clients. Therefore, the RADIUS server does not need to be reached at every AP handoff and the duration of the authentication exchange is fast enough to maintain audio quality. Hard handoffs occur when the handset loses AP connectivity and subsequently the handset must re-acquire its connection to the WLAN. When WPA2 Enterprise is the selected security method and connectivity is lost, a full 802.1X authentication with the RADIUS server is required during the re-acquisition. Once the handset has re-acquired the network after a hard handoff, soft handoffs will resume as long as OKC is used and WLAN connectivity is maintained. OKC must be supported and properly configured on the WLAN. Consult the [WLAN Configuration Guide](#) for your WLAN product to ensure proper operation and proper WLAN interoperability.

CCKM

Cisco Centralized Key Management (CCKM) is a Cisco-proprietary fast AP handoff method and therefore only supported on Cisco APs. The combination of either PEAP or EAP-FAST and CCKM is expected to result in soft handoffs, once the initial 802.1X exchange has occurred establishing network connectivity for the handset. The soft handoffs occur as the user roams within the coverage area and the WLAN infrastructure retains authentication key information for the associated clients. Therefore, the RADIUS server does not need to be reached at every handoff and the duration of the authentication exchange is fast enough to maintain audio quality. Hard handoffs occur when the handset loses AP connectivity and subsequently the handset must re-acquire its connection to the WLAN. When WPA2 Enterprise is the selected security method and connectivity is lost, a full 802.1X authentication with the RADIUS server is required during the re-acquisition. Once the handset has re-acquired the network after a hard handoff, soft handoffs will resume as long as CCKM is used and WLAN connectivity is maintained. CCKM must be properly configured on the Cisco APs. Consult the [WLAN Configuration Guide](#) for your Cisco products to ensure proper operation and WLAN interoperability.

Using Virtual LANs

Virtual LANs (VLANs) should be used to segregate traffic into different security classes and purposes. By using separate VLANs, data traffic can utilize the most robust but processing-intensive security methods. In order for voice to operate efficiently in a WLAN, it is critical that it be separated from the data traffic by using VLANs, mapped to WLAN SSIDs. The 802.1Q standard establishes a method for inserting VLAN membership information into Ethernet frames via header-information tags.

MAC Filtering and Authentication

Most access points can be configured to allow or deny association of wireless clients based on their unique MAC address, which can be used as a method of securing the WLAN. This process generally works well, but can cause some performance issues on some APs and is never recommended when using voice on a WLAN. MAC filtering is ineffective as a security method since MAC spoofing can occur.

Firewalls and Traffic Filtering

The traffic filtering capabilities of firewalls, Ethernet switches and wireless controllers can also be used as an additional security layer if configured to allow only certain types of traffic to pass onto specific areas of the LAN. To properly provide access control, it is necessary to understand the type of IP traffic used by the SpectraLink handsets.

While the SpectraLink handset will generally work through a firewall if the appropriate ports are made available, this is never recommended. Firewalls create a great deal of jitter (packet delay) in the network which can severely limit the successful, on-time delivery of audio packets to the wireless telephone. Additionally, the use of ICMP redirects is not supported because of the extreme delay that can result when the gateway of the handsets is changed dynamically. SpectraLink handset requires less than one millisecond of jitter from the SIP Call Server to handset. This will be difficult to achieve if there are multiple 'hops' between the SIP Call Server and handset.

The SpectraLink Wireless Telephones use TCP and UDP and other common IP protocols. These include DHCP, DNS, HTTP, HTTPS, TFTP, FTP, SNMP, SIP, Telnet, ARP and ICMP which are all common ports. Polycom uses proprietary UDP channels between the OAI Gateway utilizing UDP ports 5454 - 5458. The push-to-talk (PTT) mode of the SpectraLink 8400 Series Wireless Telephone uses the multicast IP address 224.0.1.116, which other model handsets also employ. Note that the SpectraLink 8400 Series handset can be configured to utilize different multicast group addresses, if necessary. The Real Time Location Service (RTLS) uses UDP port 8552 by default (configurable in the Administration menu or handset configuration files). In addition to the above, the SpectraLink 8400 Series Wireless Telephone can be ordered equipped with a bar code scanner. In order to use the bar code capabilities you will need the QBC (Quick Bar Code) application and ensure that port 14394 is available. Table 5 below outlines the common port numbers used by the SpectraLink 8400 Series wireless telephone.

Table 5- Ports used by SpectraLink 8400 Series

Port Number	Protocol	Outgoing	Incoming	UDP or TCP
21	FTP	Provisioning, Logs		TCP
22	SSH	Admin	Admin	TCP
23	Telnet	Admin		TCP
53	DNS			UDP
67	DHCP	Server		UDP
68	DHCP	Client		UDP
69	TFTP	Provisioning, Logs		UDP
80	HTTP	Provisioning, Logs, Pull Web Interface, Poll		TCP
123	NTP	Time Server		UDP
389	LDAP			
443	HTTPS	Provisioning, Logs		TCP
514	Syslog	Logs		
636	LDAP			
2222	RTP	Media Packets	Media Packets	
2223	RTCP	Media Packets Statistics	Media Packets Statistics	
5060	SIP	SIP Signaling	SIP Signaling	
5061	SIP over TLS	Secure Signaling	Secure Signaling	
7778	OCS			

Diagnostic Tools

The SpectraLink 8400 Series handset provides three comprehensive diagnostic tools to assist the administrator in evaluating the functionality of the handsets and its support by the surrounding wireless infrastructure. These tools are Run Site Survey, Diagnostics Enabled, and Syslog Mode.

Site Survey can be used to evaluate the radio coverage within the facility where the handsets are deployed by testing the signal strength, or to gather information about access points regardless of the SSID.

Diagnostics – (WiFi Stats) is used to evaluate and report the overall quality of the link between the handset, access point, and other infrastructure equipment such as IP PBX and gateways. The handset's diagnostics are enabled through the handset settings menu.

Syslog Mode allows the handset to send various Syslog messages such as Successful and Failed handoffs along with reason codes indicating why the handset chose to handoff to a particular AP; Call Starts and Ends; AP RSSI, audio statistics & retry rates; security errors and other information. Refer to the

Diagnostic Tools section of the Polycom UC Software Administrator's Guide for a detail explanation of information provided by each of the Diagnostic tools.

App/Boot Logs are automatically uploaded by the SpectraLink 8400 Series handset to the provisioning server at regular intervals. These logs are supplemental to syslog output and will often contain important information about the status of the handset. Because syslog requires that a usable network connection be available, it is possible that some log information will not be available. However, with the App and Boot logs from the SpectraLink 8400 Series handset, the handset will store the log information in flash until a network connection is available. This ensures that critical information about handset performance is retained for troubleshooting purposes.

App logs contain details regarding all aspects of the SpectraLink 8400 Series handset's operation and can include information on network operation, user interface, memory and CPU statistics, and much more. The amount of information generated is dependent on configurable logging levels. Higher logging levels will generate detailed information on handset operation but will have an impact on CPU performance. High logging levels are only recommended when troubleshooting issues and not during normal operational periods.

Boot logs are specific to the boot of process of the handset. Since the handset will contact the provisioning server during boot up, information about what the handset requests and what it receives will be available in this log. The boot log can also be helpful for investigating reboot problems. The boot log, just as the app log, will be stored on the provisioning server when network connection is available. Since during the boot up process there are no mechanisms for delivery of syslog messages to a syslog server, the boot log is the pivotal source of information on a wide variety of problems. Logging levels can be modified for the boot log as well using the handset configuration files.

Core Dumps (Tech Support Information Dump) occur when a handset experiences an unexpected interruption in operation. This can happen when a software exception, hardware failure or other unknown problem occurs. The SpectraLink 8400 Series handset will automatically upload a dump file to the provisioning server when it is able to access the network successfully. Dump files will be in an archived format allowing for a great deal of information to be included that can be easily delivered to Polycom Support for further investigation.

Self-Test Mode is available via the handset Settings menu and allows the handset's hardware components to be tested for proper operation. Tests include display sequences to verify the operation of the color LCD screen, key press tests to verify the keypad and audio tests for the speakers and microphone. The self-test mode should always be used to verify proper handset operation prior to requesting an RMA. In many cases a perceived failure in hardware can be the result of configuration issues on both the handset and/or the SIP call server.

Subnets, Network Performance and DHCP

Subnets are used to create a boundary between network segments. Although these boundaries are logical, they become like a physical boundary for mobile network devices moving throughout the enterprise. When a device with an established IP data stream (such as with an active phone call) attempts to roam across a subnet boundary, it must obtain a new valid IP address within the new subnet. During this process, the data stream cannot be re-established automatically and the connection (voice call) is dropped. The handsets can automatically recover in the new subnet from a lost network connection but will automatically reboot to apply the new IP address. Please note that in order for the phone to continue functioning in the new subnet the DHCP scope must contain the appropriate DHCP options to allow the phone to regain connectivity with the voice infrastructure, provisioning server and SIP Server.

Some WLAN controllers, Ethernet switches and third-party devices have implemented methods to facilitate subnet roaming. While these methods are transparent to the client device and are fundamentally a good approach to accommodating multiple subnets, they often cause enough delay and jitter to manifest poor voice quality and the tradeoffs might make such solutions unattractive for voice applications.

Since the push-to-talk feature of the SpectraLink 8400 Series Wireless Telephones use multicast IP packets, a PTT transmission will generally be isolated to a single IP subnet. With the deployment of IP multicast routing it is possible for the multicast traffic that is normally pruned at the network boundary to be passed into one or more other subnets. Please review your network manufacturer's documentation for information on how to properly configure network multicast routing.

There are additional subnet requirements for Wireless Telephones based on the infrastructure components that are used, as described in the following sections.

Subnets and IP Telephony Server Interfaces

SpectraLink Wireless Telephones can be deployed across multiple subnets if the performance requirements outlined below are met. Keep in mind that the handset will never actively roam across a subnet boundary without power-cycling the handset. Because users will not want to re-administer the wireless telephones to a separate subnet, Extended Service Set Identifier (ESSIDs) should be the same, the security mode and associated key must be the same, and DHCP must be used.

DHCP Requirements

The SpectraLink 8400 Series wireless telephones network settings can be configured via DHCP, manually entered using the handset's user interface, or from configuration files. DHCP is recommended as it reduces manual entry of common networking parameters.

Table 6 displays several DHCP options that are universally required for the normal operation of the handset. These DHCP options should be provided by the system administrator to ensure that the appropriate information and values required for those options are correct for the deployment of the handsets.

Table 6 – DHCP Options

DHCP Option	Value Expected	Purpose
1	IP Address (i.e. 255.255.255.0)	Subnet Mask
3	IP Address (i.e. 192.168.1.1)	Default Gateway
6	IP Address (i.e. 192.168.1.10)	DNS Server IP Address
7	IP Address (i.e. 192.168.1.20)	Syslog Server
15	String (i.e. mycompany.com)	DNS Domain Name
42	IP Address (i.e. 192.168.1.30)	SNTP Server Address (Network Time Protocol)
66	IP Address (i.e. 192.168.1.40)	Boot Server (Provisioning Server)
151	IP Address (i.e. 192.168.1.45)	SIP Server Address
152	IP Address (i.e. 192.168.1.60)	OAI Gateway

While the wireless telephone does support using a DNS server, it is not recommended to do so. Using DNS creates a dependency on a service that may not be reliable when the services a phone provides can be critical. By using DNS, there is also the addition of latency in transactions that the handset must complete with the DNS server which could lead to undesirable behavior from the wireless telephone. Please note if DNS is necessary then DHCP option 15 is also required. Moreover, DHCP options 6 and 15 must be present or the wireless telephone will not complete DNS queries.

A common enterprise deployment scenario includes the use of redundant DHCP servers. Redundant DHCP servers are intended to ensure availability of IP addressing services for all network clients including times when normal operation of primary DHCP services are unavailable. When utilizing redundant DHCP servers it is important to consider the deployment model and the expected behavior of the DHCP servers. In particular, how IP address pools are shared between redundant servers can have a significant impact on how the SpectraLink 8400 Series handset interacts with the WLAN environment.

One design method for redundant DHCP servers provides each server with a separate range of IP addresses for the same IP address pool. This particular model can be implemented differently depending on the DHCP server type being used. In one model each DHCP server is unaware of the IP addresses that have been leased by clients on the network which means that should one of the DHCP servers fail the clients the had received leases from this server will need to re-IP at lease renewal. With the SpectraLink 8400 Series handset, this creates a situation where the handset will need to restart the SIP application in

order to begin using the new IP address. When the handset is in standby this poses no real risk but if it were to happen while in call the handset would be unable to continue with its current call. An alternative DHCP redundancy setup, and the more reliable setup, would be one where both DHCP servers keep state with each other to ensure addressing requests can be handled by either server. This would eliminate the risk of the SpectraLink 8400 Series handset restarting as it would always receive the same IP address from the DHCP servers regardless of which server responds.

Unfortunately, not all DHCP servers may be able to support the “stateful” functionality. DHCP servers that aren’t able to share lease status information with other active DHCP servers may need to be disabled to prevent unintentional restarts should a handset be out of coverage for greater than 20 seconds at a time. In these cases it may be more appropriate to configure each DHCP server independently to service different IP ranges and to even configure back up IP scopes on each server that can be deactivated under normal operation but could be activated should the need arise. This is not an ideal situation as it does require manual intervention but would provide some measure of redundancy.

Pay special attention to your DHCP server setup and check with your DHCP server vendor to ensure it supports “stateful” operation should you require redundant DHCP functionality. All DHCP server configurations, or other network configuration, should fit within your corporate security policy, meet existing business needs, and meet disaster recovery requirements.

Conclusion

The SpectraLink 8400 Series Wireless Telephone uses Wi-Fi technology to deliver a full-featured mobile extension to a SIP Call Server. The purpose of this document is to outline the network design criteria for a successful VoWLAN deployment. By applying the guidelines described in this document, networking and telephony professionals can confidently design and deploy a Polycom Wi-Fi telephony solution.

Some of the key takeaways include:

- Voice and data applications have different attributes, characteristics and network requirements. Several aspects of the WLAN infrastructure, including coverage and capacity planning, require special considerations for voice traffic.
- Reliable QoS is a requirement for any enterprise voice application. Wireless VoIP is especially vulnerable to many WLAN processes that can affect voice quality, including wireless traffic contention and security authentication delays.
- Selection of a security method for the SpectraLink 8400 Series handsets is a balance between the degree of security required, the complexity of management and acceptable roam time performance. Polycom offers a wide breadth of options along the WLAN security spectrum.
- Several network design attributes need to be considered before deploying a VoWLAN solution, including the use of subnets and complex network topologies that may affect the performance of SpectraLink handsets.
- Polycom's dedication, expertise and experience help ensure proper deployment for VoWLAN.