Spectralink Versity – Best Practices Guides

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 a must. 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 can 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.

Spectralink's VoWLAN VIEW 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 VIEW Technical Specification and pass certification testing. VIEW 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 was introduced as a critical component for improved communication between the wireless handset and AP. This configuration, using both AP antennas, provided low retry rates and improvement to voice quality.

The latest WLAN physical layer standards use MIMO technology to exploit multipath propagation. In any case using multiple antennas on the access point for diversity and MIMO technology is key to good performance. Complex RF environments like manufacturing or distribution are especially in need of proper antenna orientation and installation.

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 enough when considering the unique ability of the Spectralink Versity to also seamlessly roam between the 2.4 GHz and 5 GHz bands. For this reason, coverage design for roaming between Access Points must expand beyond typical cell overlap. This section will first cover single band cell coverage and then cover band overlap coverage.

For each certified WLAN product, Spectralink 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 Spectralink Support website and should be followed closely to ensure a successful deployment.

Spectralink 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 Spectralink Versity Wireless Telephones, the latest generation of our industry-leading platform.

Wireless LAN Considerations

Spectralink Versity 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, user density, system capacity, power output, physical environment, and radio types. It is vital to perform a professional RF site survey with WLAN design and validation for voice to provide optimized total wireless coverage.

Coverage

One of the most critical considerations in deployment of Spectralink handsets is to ensure enough 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 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 discernible, 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.

In a single band design, handsets decide 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 enough 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. Enough overlapping coverage is usually considered 15% to 20% signal overlap between AP cells. 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 to maximize coverage area. If a site requires configuring the APs to only negotiate 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% 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, forklift or running/jogging) or the cell size is smaller then, 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.

Spectralink 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. 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.

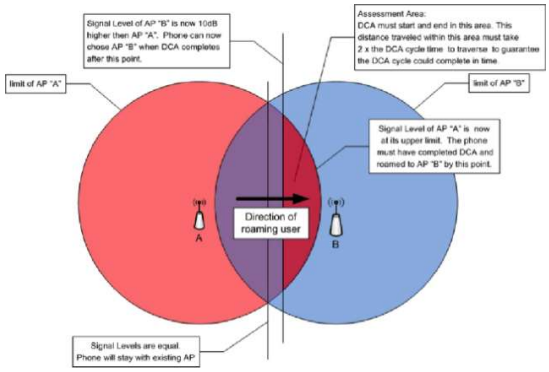

Figure 1

The handset compares the signal strength of neighboring APs to determine whether to roam from the current AP. To roam, the handset must determine whether another AP should be roamed to, it must be 5 (five) decibels stronger than the current AP's signal, or 10 (ten) decibels stronger if it is the previous AP.

Corners and doorways pose a design issue as do considerations for material construction such as cinderblock wall construction materials (absorb and attenuate RF signals), reinforced concrete (attenuate RF Signals), metallic surfaces, steel doors (reflect RF signals), wire reinforced glass windows (scatter RF signals), tinted windows (attenuate and/or reflect RF signals), etc. 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 just two different APs. The stronger signal will be given the higher priority. In the following diagram this is easy to see why.

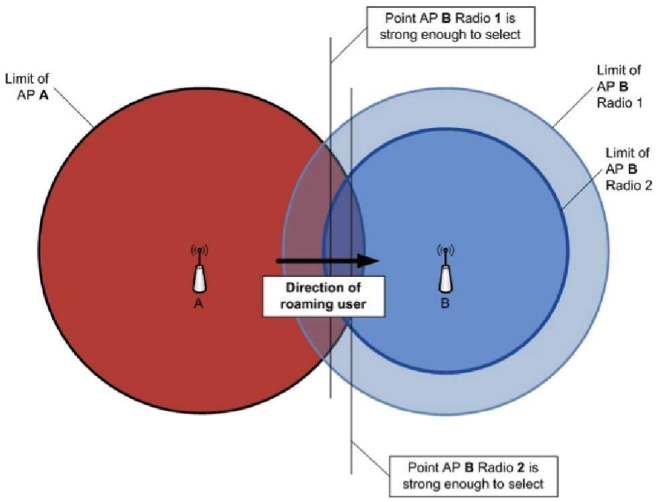

Figure 2

In the case of an AP with both bands enabled and the phone enabled for band roaming, the stronger band will almost always be selected. Such things as attenuation caused by the phone being close to the callers' head will impact 5

GHz more than 2.4 GHz. If 5 GHz is the weaker signal, then 2.4 GHz may be selected since it often has better RF signal penetration through building materials with a resultant stronger signal at the handset. The phone will pick the strongest signal it sees.

Added capacity, areas of difficult access to provide coverage, such as stairways and elevators, and mixed infrastructure with older equipment, which doesn't 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 the other radio on that 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 Spectralink 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 time.

Recommended signal strength characteristics are summarized in Table 1 and Table 2. 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 (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)								
Rate (Mb/s)	6	9	12	18	24	36	48	54
Best Practices (dBm)	-67	-65	-63	-61	-58	-54	-52	-50
5GHz 802.11n (OFDM)								
Rate (Mb/s)	6.5	13	20	26	39	52	59	65
Best Practices (dBm)	-67	-65	-63	-61	-58	-54	-52	-50

Table 3 – 5GHz 802.11ac

Spatial Streams	VHT MCS Index	Modulation	Coding Rate	20 MHz Data Rates (Mb/s)		Best Practices (dBm)	40 MHz Data Rates (Mb/s)		Best Practices (dBm)
				800ns GI	400ns GI		800ns GI	400ns GI	
1	0	BPSK	1/2	6.5	7.2	-67	13.5	15	-65
	1	QPSK	1/2	13	14.4	-65	27	30	-63
	2	QPSK	3/4	19.5	21.7	-63	40.5	45	-61
	3	16-QAM	1/2	26	28.9	-61	54	60	-58
	4	16-QAM	3/4	39	43.3	-58	81	90	-54
	5	64-QAM	2/3	52	57.8	-54	108	120	-52
	6	64-QAM	3/4	58.5	65	-52	121.5	135	-50
	7	64-QAM	5/6	65	72.2	-50	135	150	-48
	8	256-QAM	3/4	78	86.7	-48	162	180	-46
	9	256-QAM	5/6	n/a	n/a		180	200	-42

Spatial Streams	VHT MCS Index	Modulation	Coding Rate	80 MHz Data Rates (Mb/s)		Best Practices (dBm)	160 MHz / 80+80 MHz Data Rates (Mb/s)		Best Practices (dBm)
				800ns GI	400ns GI		800ns GI	400ns GI	
1	0	BPSK	1/2	29.3	32.5	-64	58.5	65	-61
	1	QPSK	1/2	58.5	65	-61	117	130	-58
	2	QPSK	3/4	87.8	97.5	-56	175.5	195	-56
	3	16-QAM	1/2	117	130	-54	234	260	-54
	4	16-QAM	3/4	175.5	195	-52	351	390	-50
	5	64-QAM	2/3	234	260	-50	468	520	-48
	6	64-QAM	3/4	263.3	292.5	-48	526.5	585	-46
	7	64-QAM	5/6	292.5	325	-46	585	650	-44
	8	256-QAM	3/4	351	390	-44	702	780	-42
	9	256-QAM	5/6	390	433.3	-41	780	866.7	-38

The critical factor is the lowest data rate set to “Required” or “Mandatory” on most WLAN’s. Other data rates can be set to “Supported” or “Enabled”. The AP data rate used to transmit beacon frames determines the RF power required by the wireless telephone for proper operation. Broadcast frames (beacons) utilize the lowest “Basic” 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, Table 2 and Table 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 -67dBm 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 & 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 determines the signal strength required by the wireless handset from Table 1, 2, & 3 above.
- There exist several free and pro apps on Google Play and the Amazon App Store that may be used for Site Survey and Diagnostics purposes.

Although it is possible that Spectralink handsets may operate at signal strengths which are weaker than those provided in Tables 1, 2 & 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.

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.

The latest APs since 802.11n was introduced do support MIMO technology. MIMO can multiply the capacity of the wireless links as well as exploit the multipath environment to enhance performance. The proper # of antennas to support MIMO on these APs should be installed correctly for voice performance.

Deployment Considerations

2.4 GHz

The 802.11b, 802.11g and 802.11n standards utilize the 2.4 GHz frequency spectrum. 802.11g and 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 Versity 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.

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 impacts the spectrum for the entire area.

5 GHz

The 802.11a/n/ac standard utilizes the 5.15 GHz to 5.350 and the 5.470 to 5.825 GHz Unlicensed National Information Infrastructure (UNII) Spectrum. In addition to having a higher maximum throughput, depending on the

configuration, the increased frequency spectrum at 5 GHz offers up to 25 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 802.11a/n/ac deployment.

As compared with the 2.4 GHz frequency of 802.11b/g/n radio deployments, higher frequency RF signals utilized by the 802.11a/n/ac 5GHz band do not propagate as well through air or obstacles. This typically means that an 802.11a/n/ac network will require more APs than an 802.11b/g/n 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.

It's important to note that the UNII-3 band of 802.11a is no longer available in Europe for WIFI deployments so alternative channel plans will need to be considered. Spectralink recommends always reviewing the current governing regulatory bodies' rules for Wi-Fi channel usage.

802.11n

The Spectralink Versity 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 Versity wireless handset 802.11n features include:

- Number of antennas: 2
- Data Rates: MCS0 – MCS7 (40MHz channels)
  - 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): Yes
- Frame Aggregation
  - A-MSDU: Yes
  - A-MPDU: Yes
- Protection (Backward Compatibility)
  - Mixed Mode: Yes
  - 40MHz Frames: Yes
  - RTS/CTS or CTS to Self: Yes
- Greenfield Support: Yes
- MIMO (multiple spatial streams): Yes
- Space-Time Block Coding: RX/TX

802.11ac

More recently is the availability of 802.11ac which is based on the 5GHz spectrum but takes advantage of different frequency modulation and channel bonding to significantly increase data rates and throughput potential. While 802.11ac uses up to 80MHz channels, it is still recommended to use 20 MHz channels for the vast majority of VoWLAN designs.

802.11k

802.11k is a standard that allows the client devices, in this case the phones, and the access points to exchange information about the available radio resources. Once enabled the devices can send each other neighbor reports, beacon reports, and information about the traffic stream. It is recommended to look at your own set of devices and find each vendor's guidelines on using 802.11k with their models and firmware versions to reach an overall design strategy.

802.11r

802.11r is a Wi-Fi security standard that is designed to facilitate reduced hand off delays while using more stringent security mechanisms. It was designed specifically for applications like VoWLAN which need seamless connectivity while maintaining robust security policies.

802.11v

802.11v is a standard that facilitates the exchange of information on network topology, and the RF environment. It is meant to provide more awareness of the surrounding area to the devices to improve overall network performance.

Access Point Configuration

There are several fundamental access point configuration options that must be considered prior to performing a site survey and deploying a voice-capable WLAN infrastructure. The Spectralink Versity handset provides support for IEEE 802.11b, 802.11g, 802.11a, 802.11n, and 802.11ac radio types. The selection of radio type has a 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 Spectralink 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 Spectralink support portal, 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 3 illustrates the correct deployment methodology for 802.11b/g deployments.

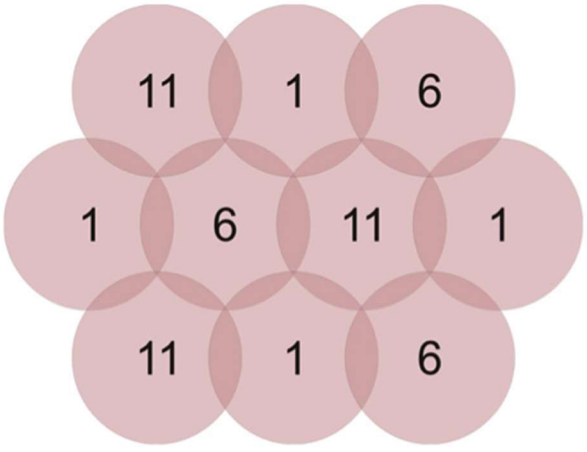

Figure 3 - 802.11b/g Non-interfering Channels with Overlapping Cell Coverage

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 4 represents the 2.4 GHz frequency range, indicating the overlap in channel frequencies.

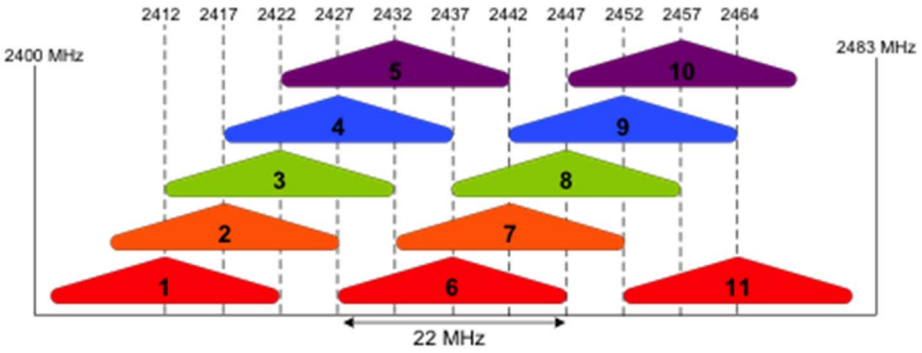

Figure 4 - 802.11b/g Channels

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/n/ac deployment, all 25 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/n/ac 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.

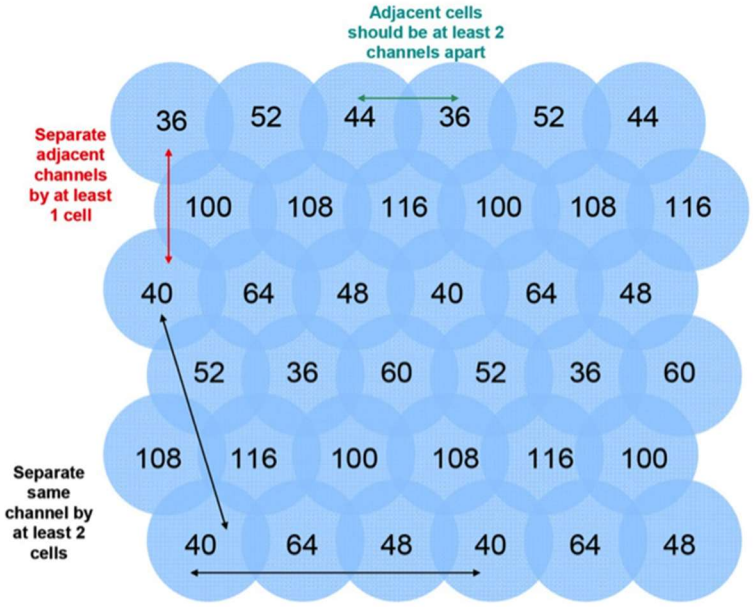

Figure 5 - 802.11a Non-interfering Channels with Overlapping Cell Coverage

There are some deployment scenarios that require limiting the number of 802.11a/n/ac channels. A key reason is to improve roaming performance. With 802.11a/n/ac there are four channel bands available to choose from. These channel bands comprise several 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)
- 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 frequencies 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. Also, 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 Versity handset requires that access points configured to utilize DFS channels must advertise support for Channel Announcement as defined in the IEEE 802.11h specification. It also is important to note that Channel 144 is only usable by 802.11ac capable devices. 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 5. As illustrated, there is still separation of adjacent channels by at least 1 cell. Same channel separation can now be a minimum of 1 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.

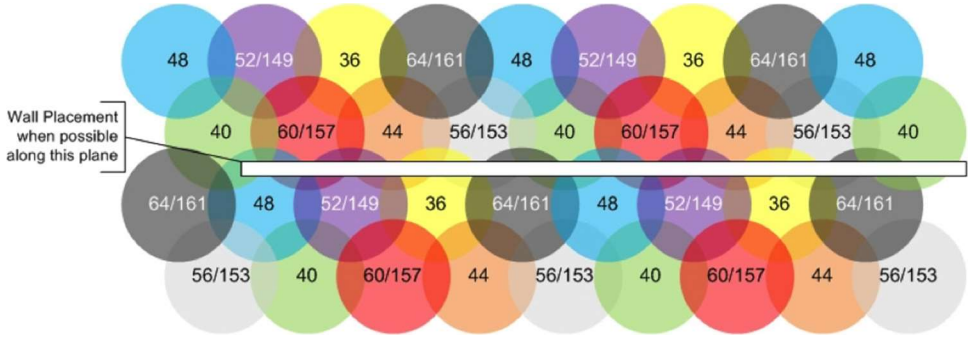

Figure 6 - Eight 802.11a Non-interfering Channels with Overlapping Cell Coverage (52/149, 64/161, etc. shows 1st DFS range channel or upper non-DFS range)

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

Channel 165 is available for use, in the United States, in the UNII3 band. This provides nine channels with UNII1 and UNII3 deployed in the handset and WLAN.

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 the Signal Strength section on page 5 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 leverage 802.11h TPC (Transmit Power Control) to learn the AP's transmit power and automatically match the current AP's transmit power. This helps make this process much easier. However, if your AP's do not support TPC then the handset will default to always using maximum transmit power.

In mixed 802.11b/g environments, Spectralink 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 overlapping 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 to be used with the Spectralink Versity 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 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. To provide optimal voice quality, Spectralink recommends the use of APs supporting both receive and full transmit diversity in all environments. 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.

For 802.11n/ac environments multiple antennas should be used to provide MIMO antenna technology. MIMO will use multiple antennas to take advantage of a multipath environment. When designing for MIMO it is important to make sure that the majority of AP’s are placed behind structure. Placing the APs behind structure will also serve to decrease co-channel interference, with the result being a mitigation of contention issues, and an increase in Wi-Fi performance.

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 regarding antenna selection and placement to provide correct AP diversity and MIMO operation.

Site Survey

A wireless RF design/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 channel 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, Spectralink recommends a professional site survey to ensure optimum coverage and minimum interference. Spectralink 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.

There is currently no integrated site survey tool in the Versity handset, however there are numerous Android applications available to perform site analysis from the handset. To verify coverage of an installed Wi-Fi network, Spectralink 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 Signal Strength Section on page 5 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 AP channel selection to avoid AP channel conflicts.

It is critical to understand that the facility should be designed to support the receive sensitivity of the VoWLAN device. For instance, a typical site survey adapter that is connected to a surveying laptop is significantly stronger than a VoWLAN telephony device. Let us remember that the VoWLAN telephony device is designed to work over an entire work shift and the power requirements of the radio in the phone must accommodate that. You could even see up to a 10-dB difference in receive sensitivity between a surveying laptop and VoWLAN telephony device. It is important to conduct your own testing on various client devices to ensure you are providing proper signaling for the device in the facility.

It is extremely important to also consider that WLANs are a contention based medium. Essentially, this means each client device in the WLAN environment will have to contend with the other clients (and APs) in order to access the medium and transmit. A quality WLAN design should seek to separate the channels using structure (walls), TX power, proper cell overlaps, in order to give each client device, the best chance to transmit. A poor WLAN design will result in inefficient use of the airtime which will result in poor performance for the client devices. For VoWLAN devices this is even more critical as real time applications are subject to poor performance with delayed and dropped frames and packets. Placing the majority of APs behind structure, reducing the # of SSIDs, eliminating Rogue APs, eliminating legacy client devices, are all ways you can increase airtime availability.

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.

RRM (Radio Resource Management)

Nearly all wireless LAN vendors provide some sort of radio management system that offers the ability to dynamically manage the channel and power of the access point radios. The entire point of a wireless LAN controller is to manage your access points after all. However, what we're talking about here is a little more specialized than the basic AP management functionality a controller provides. The RRM of the controller focuses on the access point's channel being used for each radio present in the AP and the transmit power of that radio. This system then works to build a map where the access points automatically create an appropriate level of overlap between access points while trying to avoid putting APs on the same channel, or adjacent channels, next to each other. It should seem obvious that this

software needs to be quite advanced and capable of handling a lot of different input sources to make decisions about the AP layout of your facility in three dimensions.

Not all AP manufacturers have chosen to implement this feature the same way which just means you will have widely varying experiences. There are few tools still that can beat a human mind at designing a wireless network and assigning the channel and transmit power plan to a three-dimensional space. There's just too much to consider that we can't tell the controllers about for them to be effective at doing these designs for us. That doesn't mean they can't do an okay job and manage to keep the system stable when running dynamically but there are some inherent risks you need to be aware of that aren't widely shared.

First, is the frequency that the controller performs its system scans to determine whether any changes need to be made to the AP's channel or power level. We'll pick Cisco for this example since they tend to be the most common. For the Cisco environment the default scan time is every 10 minutes; that's quite often. There are settings in the SSID that tell the controller when there are certain traffic types present to avoid performing a scan on that AP until the client with that traffic type roams away. That's great, except what happens if a client needs to roam to that AP when it starts to scan? The scans typically take very long and are mostly just AP listening, but it is still a period where AP is not servicing clients. Since these scans happen every 10 minutes there is a guarantee that they will happen during your peak network usage times too. Unless you know that your RF environment is constantly changing because of outside RF sources it really isn't necessary to scan so frequently. It would make far more sense to do it every 24 hours and choose for that scanning event to happen late at night when there are very few, if any, users present on the network. This might not account for spurious RF that only occurs during the day, but that is why you can trigger a scan anytime from the controller console.

Next, is the channel plan chosen by the RRM software. It is quite common for RRM software to deploy a channel plan to result in AP's that are either immediately next to each other or in proximity on the same channel. There is also a high likelihood of having co-channel APs in proximity. Either situation can lead to poor RF performance due to interference. The controller often seems to prefer to deal with the interference of adjacent AP's being on the same channel a lot of times rather than adjusting another APs to accommodate a more robust channel plan.

Lastly is the transmit power that is selected. It has been our experience that RRM will frequently choose to make some APs transmit power very low in comparison to other AP's. In many cases the original design called for all AP's to be at the same transmit power to ensure consistent cell overlap but over time RRM modifies the design and some APs are pushed to their maximum power to try and compensate for an AP that was turned down to its lowest transmit power by RRM instead of being set at a more reasonable level. This isn't going to be true for all wireless LAN vendors since they all do things differently, but it is certainly something that we at Spectralink have seen in the field on numerous occasions, so we feel it is important to make our customers aware.

You may be thinking that after all that we will tell you that you should never use RRM. And ultimately, you'd be right. We'd prefer our customers to use fixed channels and power plans based on the design and verification that was done. But we also realize that it is unreasonable of us to expect our customers to simply abide by this because we tell them they should. There are certainly some functions of RRM that add value to a network. Its ability to recover from access point failures, for example. So rather than tell you not to use RRM we would like to recommend that you become an informed user of RRM and not run it at its defaults. Configure a more reasonable scanning interval that won't put your clients at risk. Set up your channel plan well ahead of time so you can restrict RRM from using channels you don't want it to use and the behavior of how it makes the decision on which channel to pick. And for transmit power, just make sure you adjust your minimum transmit power to prevent RRM from setting your AP's so low that you end up with dead zones or overdriven AP's. It doesn't take much to have a robust and effective wireless LAN, so take the time to make it run well now to save yourself time later.

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, there are some considerations that should be addressed for VoWiFi with Spectralink handsets.

Access Point Bandwidth

There are several factors which determine the 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 phone 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 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. Spectralink 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 Versity handsets provide push-to-talk (PTT) functionality using the Spectralink- 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 Versity handsets are deployed on a network with previous versions of Spectralink handsets, some interoperability considerations must be observed. The Spectralink Versity 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 Versity handset uses Wi-Fi Multimedia (WMM), WMM Power Save mechanisms to deliver enterprise-grade QoS. WMM Admission Control is now supported. The handset is compatible with AP implementations using these WMM features and is required to provide the best user experience. You should always follow standard VoIP quality expectations as well with packet round-trip times not to exceed 150ms. Packet loss should be considered as well but must be viewed over a chosen period or even. For example, because of error correction mechanisms in codecs and automatic retries in Wi-Fi during a voice call, you can typically handle packet loss that averages up to 5 to 10% for the entire call. Ideally, you should never exceed packet loss greater than 1%. But realistically, because Wi-Fi is a shared and interference prone medium, it is far more likely that you will have higher packet loss over a given period.

Therefore, use of WMM is required by Spectralink and is the default operating mode of the handset. 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 if both the client device and the AP support them.

To use Wi-Fi Standard QoS, the AP needs to be supported 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 Spectralink 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 3. 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 3 - WMM Access Categories

WMM Access Category	Priority Level	802.1d tags	Client wait time + random back-off 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, RTLS, Apps)
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 Versity handset are to conserve battery life and to make AP handoff decisions without the risk of missing packets.

Power save behavior can be negotiated during the association of a handset with an AP. For Versity, WMM Power Save is not required by highly recommend. 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.

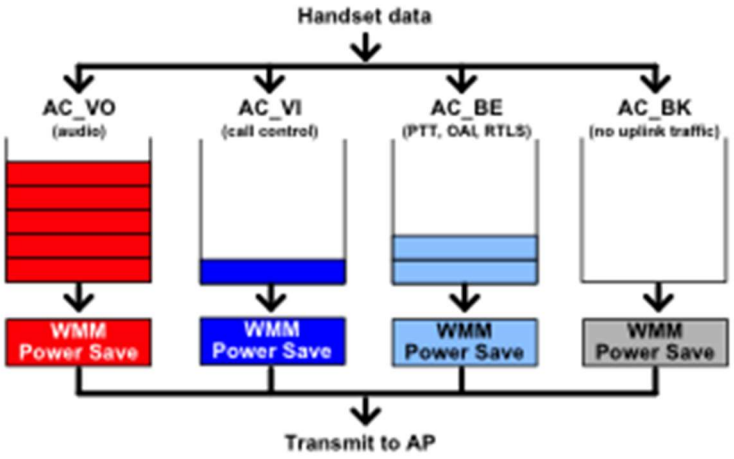

Figure 7 - WMM Queues Using WMM Power Save

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 acknowledgment 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.

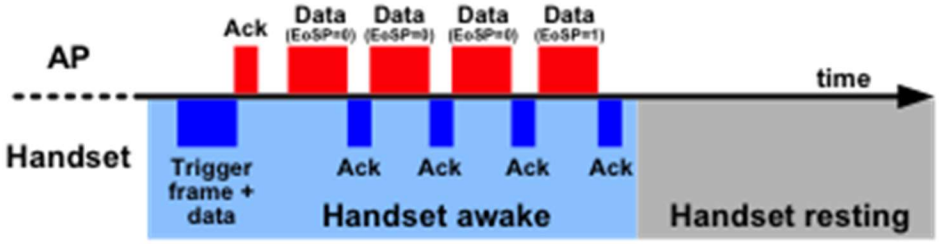

Figure 8 - WMM Power Save Timing

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): 26
- 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 3.

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 and supported by the network.

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. Spectralink 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 Versity 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 Versity. 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. 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 impact 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, Spectralink 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 Versity handset offers two 802.1X authentication types (PEAPv0 with MSCHAPv2 and EAP-TLS) 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.

PEAPv0/MSCHAPv2

PEAP (Protected Extensible Authentication Protocol) was developed by Microsoft, Cisco and RSA Security for 802.1X authentication on WLANs. PEAPv0 withMSCHAPv2 is one of the most-commonly used PEAP subtypes hence its use on the Spectralink Versity 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 during initial handset configuration. Each handset can support multiple root certificates loaded into non-volatile memory. A username (relates to the device name, not necessarily an end-user) and password are entered via the initial handset configuration.

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.

EAP-TLS

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) was defined by the IETF in RFC 5216. EAP-TLS is largely considered one of the most secure EAP standards available but also requires the use of client-side certificates for authentication.

Client certificates will need to be issued for each user or device by the root Certificate Authority. This implies that a certain amount of administrative knowledge is required to generate the required certificates for each client and to maintain the appropriate revocation services from user turnover and potential loss of theft. The rather ubiquitous

support of EAP-TLS by network manufacturers makes it a preferred security method for many enterprise environments.

Much like PEAP, a username and password can be used with EAP-TLS, but it is not required as the password is essentially just used to encrypt the client-side certificate for storage. You will need to load the CA certificate that issues the client certificate along with the client specific certificate onto the handset. You can choose to utilize the client's pre-loaded device certificate if desired.

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 Spectralink's WLAN Certified Products Guide to find a list of WLAN products tested for OKC support.

The combination of PEAP, EAP-TLS 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 if 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 PEAP or EAP-TLS 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 if 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. 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 filteringcapabilities 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, SNTP, SIP, Telnet, ARP and ICMP which are all common ports Spectralink uses proprietary UDP channels between the OAI Gateway utilizing UDP ports 5454 - 5458. The push-to-talk (PTT) mode of the Spectralink Versity Wireless Telephone uses the multicast IP address 224.0.1.116, which other model handsets also employ. Note that the Spectralink Versity 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). In addition to the above the Spectralink Versity Wireless Telephone can be ordered equipped with a bar code scanner. To use the bar code capabilities, you will need the QBC (Quick Bar Code) application and ensure that port 14394 is available. Table 4 below outlines the common port numbers used by the Spectralink Versity wireless telephone.

Table 4 - Ports Used by Spectralink Versity

Port Number	Protocol	Outgoing	Incoming	UDP or TCP
53	DNS			UDP
67	DHCP	Server		UDP
68	DHCP	Client		UDP
80	HTTP	Provisioning, Logs, Poll		TCP
123	NTP	Time Server		UDP
389	LDAP	Contact Directory		TCP
443	HTTPS	Provisioning, Logs		TCP
514	Syslog	Logs		
636	LDAP	Contact Directory		
2222	RTP	Media Packets	Media Packets	
2223	RTPC	Media Packets, Statistics	Media Packets, Statistics	
5060	SIP	SIP Signaling	SIP Signaling	UDP or TCP
5061	SIP over TLS	Secure Signaling	Secure Signaling	
5070	SIP	SIP Signaling	SIP Signaling	UDP or TCP
5071	SIP over TLS	Secure Signaling	Secure Signaling	

Diagnostic Tools

The Spectralink Versity handset provides access to comprehensive diagnostic tools to assist the administrator in evaluating the functionality of the handsets and its support by the surrounding wireless infrastructure. A multitude of different tools can also be downloaded from the App Store. For a detailed explanation of the Versity diagnostic tool set, please review the Technical Bulletin, CS-19-05 Spectralink Versity Advanced Debugging which is available on the Spectralink Technical Support Portal.

Subnets, Network Performance, Time 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 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 Versity 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.

Time – NTP and Why it Matters

Most customer environments have a time server or at least have systems that point to a global time server like the ones available from NIST (National Institute of Standards and Technology). Time servers are vital for ensuring that systems in a network operate consistently and for anyone who has ever tried to troubleshoot a problem without accurate time, you understand the pain of not having a valid time server. With Android devices it is important to realize that they are built out of the box to look for a time server on the Internet. Specifically, they will look for the Google time servers regardless of where you are in the world. If your Android device has Internet access, then it will be asking one of those servers for the correct time as it comes online.

Since not everyone is willing to give unfettered access to the Internet for their devices it may be necessary to provide an alternative method for your Android devices to get time. For that, you may need to set up an NTP server (Network Time Protocol). This is also known as SNTP (Simple Network Time Protocol). You are very likely already have an NTP server in your network and didn't even realize it. Most Microsoft Domain Controllers have an active NTP server automatically. Similarly, your core network router(s) will typically operate as an NTP server as well. But if you're unsure and would rather have a separate system to handle this function there are plenty of options available.

DHCP Recommendations

The Spectralink Versity wireless telephones network settings can be configured via DHCP or manually entered using the handset's user interface. DHCP is recommended as it reduces manual entry of common networking parameters.

Table 5 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.

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.

Table 5 - 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
15	String (i.e. mycompany.com)	DNS Domain Name
42	IP Address (i.e. 192.168.1.30)	SNTP Server Address

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 is unavailable. When utilizing redundant DHCP servers it is important to consider the deployment model and the expected behavior of the DHCP servers. How IP address pools are shared between redundant servers can have a significant impact on how the Spectralink Versity 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 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 Versity handset this creates a situation where the handset will need to restart the SIP application 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 Versity 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 can’t 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 and meet existing business needs and disaster recovery requirements.

Conclusion

The Spectralink Versity 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 Spectralink 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 Versity handsets is a balance between the degree of security required, the complexity of management, and acceptable roam time performance. Spectralink 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.
- Spectralink's dedication, expertise and experience help ensure proper deployment for VoWLAN.

Copyright Notice

Notice

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

Spectralink 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 Spectralink 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 SPECTRALINK FOR ANY PURPOSE, OR GIVE RISE TO ANY LIABILITY OF SPECTRALINK WHATSOEVER.

Warranty

The *Product Warranty and Software License and Warranty* and other support documents are available at http://support.spectralink.com.

Contact Information

US Location
+1 800-775-5330

Spectralink Corporation
2560 55th Street
Boulder, CO 80301
USA

info@spectralink.com

Denmark Location
+45 7560 2850

Spectralink Europe ApS
Bygholm Soepark 21 E Stuen
8700 Horsens
Denmark

infoemea@spectralink.com

UK Location
+44 (0) 20 3284 1536

Spectralink Europe UK
329 Bracknell, Doncastle Road
Bracknell, Berkshire, RG12 8PE
United Kingdom

infoemea@spectralink.com