



WHITE PAPER

## DEPLOYING NETLINK WIRELESS TELEPHONES: BEST PRACTICES

W I R E L E S S   A T   W O R K

Version 1.3  
May 2006

# Table of Contents

1.0	Introduction .....	4
2.0	Wireless LAN Layout Considerations .....	5
2.1	Coverage .....	5
2.1.1	Overlapping Coverage .....	5
2.1.2	Signal Strength.....	6
2.2	Wireless Bridges.....	6
2.3	Access Point Configuration Considerations .....	6
2.3.1	Channel Selection .....	7
2.3.2	Transmission Power.....	8
2.3.3	Data Rates.....	8
2.3.4	Interference .....	8
2.3.5	Multipath and Signal Distortion.....	8
2.3.6	Site Surveys.....	10
2.4	Capacity .....	11
2.4.1	Access Point Bandwidth Considerations .....	11
2.4.2	Push-to-Talk Multicasting Considerations .....	13
2.4.3	Telephone Usage.....	13
2.4.4	Telephony Gateway Capacity .....	14
3.0	Network Infrastructure Considerations.....	15
3.1	Physical Connections .....	15
3.2	Assigning IP Addresses.....	15
3.3	Software Updates Using TFTP .....	16
4.0	Quality of Service .....	17
4.1	SpectraLink Voice Priority (SVP).....	17
4.1.1	SVP Infrastructure.....	17
4.1.2	SVP Server Capacity .....	18

4.1.3 Multiple SVP Servers .....18

4.2 Access Point QoS.....18

4.3 VIEW Certification.....19

5.0 Security .....20

5.1 Security Concerns.....20

5.1.1 Wired Equivalent Privacy (WEP).....20

5.1.2 Wi-Fi Protected Access (WPA/WPA2) .....20

5.1.3 Cisco Fast Secure Roaming (FSR).....21

5.2 Using Virtual LANs .....21

5.3 MAC Filtering and Authentication .....21

5.4 Firewalls and Traffic Filtering .....22

5.5 Virtual Private Networks (VPNs).....22

6.0 NetLink Wireless Telephones and Subnets .....24

6.1 Subnets and NetLink Telephony Gateway Interfaces.....25

6.2 Subnets and IP Telephony Server Interfaces .....25

6.3 Network Performance Requirements.....25

7.0 Conclusion.....27

## 1.0 INTRODUCTION

Wi-Fi telephony enables the convergence of wireless voice and data applications using a common wireless local area network (LAN). Wi-Fi telephony bridges traditional telecommunications, data communications and mobile technologies. A Wi-Fi-enabled telephone is a wireless LAN client device, using the same network technology as wireless laptops and PDAs, and sharing the same medium. A Wi-Fi-enabled telephone is also functionally equivalent to a wired telephone, and allows for configuration and management from the local enterprise telephone system. These benefits can result in substantial cost savings over other similar wireless technologies by leveraging the Wi-Fi infrastructure and by eliminating recurring charges. However, a Wi-Fi telephone does impose different requirements on the network that result in deployment considerations that may vary from networks optimized for data.

Voice and data applications have different attributes and network requirements. A Wi-Fi telephone is a mobile communication device that requires special considerations for continuous high-quality connections as a user moves throughout the coverage area. Another significant difference is the tolerance for network errors and delays. Whereas data applications are designed to accept frequent packet delays and retransmissions, voice quality will suffer with just a few hundred milliseconds of delay or a very small percentage of lost packets. In addition, data applications are typically bursty in terms of bandwidth utilization, while a telephone conversation utilizes a consistent and relatively small amount of network bandwidth.

Using a wireless LAN for voice is not complex, but there are some aspects that must be considered, particularly for enterprise applications. A critical objective in deploying enterprise Wi-Fi telephony is to maintain similar voice quality, reliability and functionality as is expected in a wired telephone environment. The key issues in deploying Wi-Fi telephony are coverage, capacity, quality of service (QoS), telephone switch integration and wireless security.

SpectraLink pioneered the use of Wi-Fi enabled telephones in a wide variety of applications and environments, making SpectraLink's NetLink Wireless Telephones the market leader in this space. This document identifies issues and solutions based on SpectraLink's extensive experience in enterprise-class Wi-Fi telephony and provides recommendations for ensuring that a network environment is adequately optimized for use with NetLink Wireless Telephones.

## 2.0 WIRELESS LAN LAYOUT CONSIDERATIONS

NetLink Wireless Telephones utilize a Wi-Fi network consisting of wireless LAN access points (APs) distributed throughout an enterprise environment. The required number of APs is driven by several factors, including intended coverage area, system capacity, access point type and power output, and physical environment.

### 2.1 Coverage

One of the most critical considerations in deploying NetLink Wireless Telephones is to ensure there is sufficient wireless coverage. Enterprise Wi-Fi networks are often originally laid out for data applications and may not provide adequate coverage for Wireless Telephone users. Such networks may be designed to only cover areas where data terminals are 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.

The overall quality of coverage is also more important with telephony applications. Coverage that is suitable for data applications may not be seamless enough to support the requirements of Wi-Fi telephony. 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; lost or corrupted packets must be discarded. In areas of poor coverage, data application performance may be acceptable due to retransmission protocols, but real-time voice quality will not be acceptable.

Another factor to consider when determining the coverage area is the device usage. Wireless Telephone devices are used differently than wireless data terminals. Telephone 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 simply portability. NetLink Wireless Telephones are usually held very close to the user's body, introducing additional radio signal attenuation. Data terminals are usually set on a surface or held out at arms length so the user's body has little affect. This factor means that a Wireless Telephone may have less range than a data terminal and the wireless LAN layout should account for some reduction in radio signal propagation.

#### 2.1.1 Overlapping Coverage

To provide comprehensive coverage for Wi-Fi telephony applications, APs must be positioned with sufficient overlapping coverage to ensure there are no coverage gaps, or dead spots, between them. As NetLink Wireless Telephones move about the workplace, they seek out other APs to handoff to, or re-associate with, in order to maintain the most reliable network connection. A properly designed Wi-Fi network will provide seamless handoffs between APs, ensuring excellent voice quality throughout the facility.

The wireless LAN layout must factor in the transmission settings that are configured within the APs. The transmission of voice requires relatively low data rates and a small amount of bandwidth compared to other applications. The IEEE

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 (coverage) when operating at reduced transmission rates. If wireless voice is an application on the wireless LAN, APs should not be configured to limit the transmission to only the higher rates because the coverage area of the AP will be greatly reduced. If a site requires configuring the APs to only negotiate at the higher rates, the layout of the wireless LAN must account for the reduced coverage and additional APs will be required to ensure seamless overlapping voice coverage at the higher rates.

### 2.1.2 Signal Strength

To provide reliable service, wireless networks should be engineered to provide signal strength of -70dBm or stronger in all areas where NetLink Wireless telephones will be used. Although NetLink handsets may operate at signal strengths weaker than -70dBm, real world deployments involve many RF propagation challenges such as physical obstructions, interference and multipath effects that impact both signal strength and quality. Engineering radio frequency (RF) coverage to -70dBm or stronger provides an adequate buffer for these propagation challenges.

## 2.2 Wireless Bridges

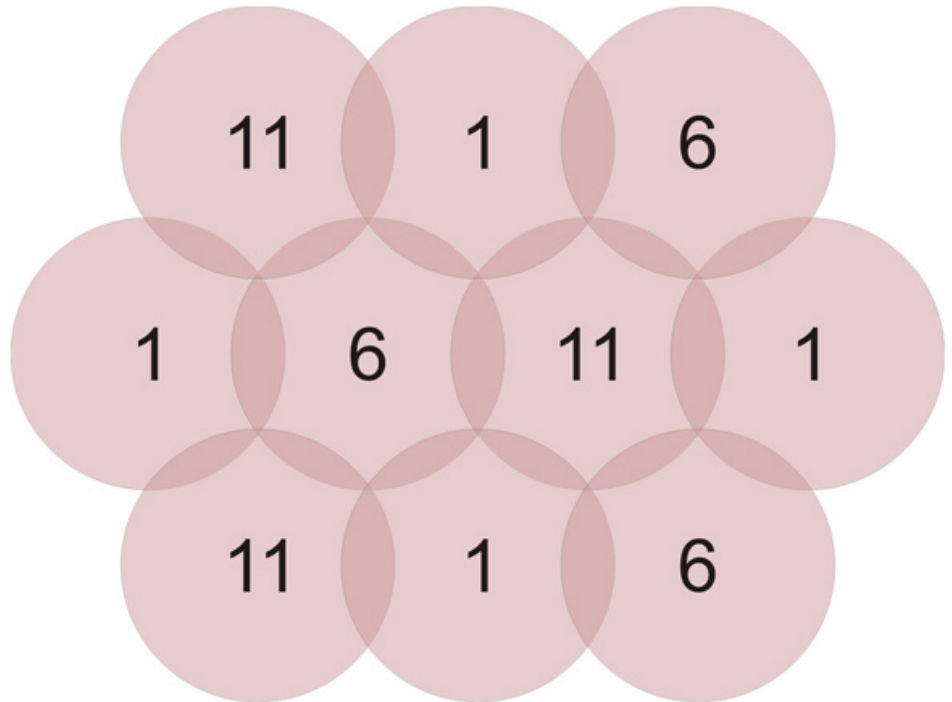
Wireless bridges are sometimes used to interconnect geographically disbursed Ethernet LANs or to extend the range of existing wireless LANs. Such devices create bottlenecks for network capacity and add delay to the overall network, which are generally not tolerable for real-time voice connections. SpectraLink does not support a configuration that includes wireless bridges and does not recommend using wireless bridges within any wireless voice network.

## 2.3 Access Point Configuration Considerations

There are several fundamental access point configuration options that must be considered prior to performing a site survey and completing a successful wireless LAN deployment for voice. This section does not cover all issues or considerations and it is strongly recommended that SpectraLink or another professional services organization qualified in Wi-Fi telephony be engaged to answer remaining questions about configurations that may affect voice quality or Wireless Telephone performance.

### 2.3.1 Channel Selection

Adjacent APs need to use different radio channels to prevent interference between them. The 802.11b standard utilized by NetLink Wireless Telephones provides three non-interfering channels - channels one, six and 11 for 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, as illustrated in the diagram below:



*802.11b Non-interfering Channels with Overlapping Cell Coverage*

If adjacent access points are set to the same channel or utilize channels with overlapping frequency bands, the resulting interference will cause a significant reduction in the network throughput and will degrade the voice quality.

### 2.3.2 Transmission Power

The transmission power of APs can be increased or decreased to provide more or less AP coverage area. The transmission power setting must be the same for all APs in a facility. This minimizes the chance of higher-power devices interfering with nearby lower-power devices and provides consistent coverage.

NetLink Wireless Telephones supports a statically configurable transmission power setting from 5 to 100 mW with a default setting of 100 mW. Lower power settings on the APs and handsets can be used to provide added overall capacity by increasing the density of access points in the network. In such deployments, special attention must be given to AP placement to ensure there are no frequency reuse issues. No matter what power level is used, the settings in all APs and handsets must be the same to avoid channel conflicts and interference. For access points that support automatic transmission power adjustments, SpectraLink recommends using only static power settings to ensure optimal performance of the NetLink Wireless Telephones.

### 2.3.3 Data Rates

All APs used for voice applications must be set to the same supported data rates. For 802.11b networks, all access points should be set to have 1, 2, 5.5 and 11Mb/s supported for optimal performance. NetLink phones will not associate to any AP that does not support full data rates if other APs in the network do support higher data rates. As these APs will not be used by the phones, this will effectively lead to coverage gaps.

### 2.3.4 Interference

Interference on 802.11b networks can come from many sources such as microwave ovens or other 2.4 GHz equipment including Bluetooth devices, cordless phones, and rogue APs.

Spectrum Analyzers can be used to help identify the sources of 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 the channel of the surrounding APs may be able to be changed to avoid as much frequency overlap with the interfering device as possible.

### 2.3.5 Multipath and Signal Distortion

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 signal wave fronts to be heard at 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 signal.

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

Diversity antennas should be used to help improve performance in a multipath environment. A diversity solution uses two antennas for each radio, and will send and receive signals on the antenna which is receiving the best signal. This greatly increases the probability that both the AP and the client will receive a better signal quality in multipath environments. Most access points support receive diversity in that they receive on the antenna that is getting the best signal, but some also support transmit diversity where the transmission is made on the same antenna that was last used to receive a signal from that specific client. SpectraLink recommends the use of APs supporting both receive and full transmit diversity where multipath is an issue in order to provide optimal voice quality.

Access point antennas should not be placed near a metal roof, wall, beam or other metal obstruction in a multipath environment, as this will amplify the reflection effects. Additionally, antennas should be positioned so that they have a line of site 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 diversity operation.

### 2.3.6 Site Surveys

A wireless site survey is highly recommended for any wireless network deployment, however it is especially critical when voice is an application on the network and is essential for large or complex facilities. Site surveys ensure that the wireless networks is optimally designed and configured to support voice by confirming RF coverage, cell overlap, channel allocation and reuse, packet transmission quality, and other wireless LAN infrastructure configurations. While many tools exist that allow customers to perform their own assessment, SpectraLink recommends a professional site survey to ensure optimum coverage and minimize interference. SpectraLink offers a full suite of site-survey services that will ensure a wireless LAN is properly configured to support wireless voice over IP (VoIP).

To verify coverage of an installed Wi-Fi network, NetLink Wireless Telephones offer a site-survey mode that can be used to ensure the AP locations and configurations are correct and adequate. This mode detects the strongest AP signals and displays the signal strength and the AP channel assignments. The site survey mode can also be used to detect areas with poor coverage or interfering channels, check for rogue APs, confirm the Extended Service Set Identification (ESSID) and data rates of each AP, and detect other common AP configuration problems. With NetLink Wireless Telephones, the entire coverage area must be checked to ensure that at least one access point's reading is stronger than  $-70$  dBm in all areas where the phone is to be used. Signal strength of  $-60$  dBm or better is required to ensure connections at 11 Mb/s, so if all APs are configured to accept only 11 Mb/s connections the entire coverage area should meet the stronger requirement. Also, if the site-survey mode indicates two APs using the same channel, then at least one other AP must be indicated at 10 dBm stronger than those APs to avoid channel conflicts.

After a site survey is complete, coverage issues can be resolved by adding and/or relocating APs. Overlap issues may be resolved by reassigning channels or by relocating some access points. Any time adjustments are made to the configuration an additional site survey should be performed to ensure that the changes are satisfactory and have not impacted other areas.

## 2.4 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 usually acceptable because data applications can tolerate network congestion with reduced throughput and slower response times. Voice traffic cannot tolerate unpredictable delays, but 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 several additional considerations that need to be addressed for Wi-Fi telephony with NetLink Wireless Telephones.

### 2.4.1 Access Point Bandwidth Considerations

There are several factors that 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. The payload information generally makes up a little more than half 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 rather than actual data throughput.

The percentage of bandwidth used increases for lower data rates, but it is not a linear function because of the bandwidth consumed by the timing gaps and overhead. For example, a call using standard 64 kb/s voice encoding (G.711) utilizes about 4.5 percent of the AP bandwidth at 11 Mb/s, and about 12 percent at 2 Mb/s. In this example, four simultaneous calls on an AP would consume about 18 percent of the available bandwidth at 11 Mb/s or about 48 percent at 2 Mb/s.

The following table lists the theoretical percentage of available bandwidth used per telephone call for each 802.11b data rate:

	1 Mb/s	2 Mb/s	5.5 Mb/s	11 Mb/s
<b>Recommended Total Utilized Bandwidth</b>	<b>80%</b>	<b>70%</b>	<b>65%</b>	<b>65%</b>
<b>NetLink Telephony Gateway (24 kb/s), 20 ms sample rate</b>	<b>15.7%</b>	<b>10.0%</b>	<b>6.4%</b>	<b>5.4%</b>
<b>G.711 (64 kb/s), 30 ms sample rate</b>	<b>20.5%</b>	<b>11.7%</b>	<b>6.1%</b>	<b>4.5%</b>
<b>G.729 (8 kb/s), 30 ms sample rate</b>	<b>9.3%</b>	<b>6.1%</b>	<b>4.1%</b>	<b>3.5%</b>
<b>Push-to-talk transmit</b>	<b>15.3%</b>	<b>9.0%</b>	<b>5.0%</b>	<b>3.9%</b>
<b>Push-to-talk receive</b>	<b>5.7%</b>	<b>3.3%</b>	<b>1.7%</b>	<b>1.3%</b>

Theoretical Call Bandwidth Utilization of 802.11b Access Points

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 40 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, as shown in the table. For example if all calls on an AP are using a theoretical 5.4 percent of the bandwidth at 11 Mb/s, 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). The actual number of calls expected at 2 Mb/s using the NetLink Telephony Gateway and a 20 milliseconds sample rate is about seven (70 percent of bandwidth available / 10 percent theoretical bandwidth utilized per call). Lower overall bandwidth is available when there are a greater number of devices associated with an AP.

Even with all of the known variables, there are many other vendor-specific characteristics associated with individual APs that make it difficult to exactly quantify the number of concurrent calls per AP without thoroughly testing specific configurations. As a general rule, and based on lab tests and experience, wireless LAN designs for NetLink Wireless Telephones should consider no more than 12 simultaneous calls at 11 Mb/s or no more than seven calls at 2 Mb/s using either G.711 or NetLink Telephony Gateways. Using the G.729 codec will typically yield roughly 50 percent more calls at these mentioned data rates. SpectraLink publishes access point configuration notes that identify the maximum number of calls per AP for specific models that have been tested to be compatible with the NetLink Wireless Telephones.

To allow for bandwidth to be available for data traffic, SpectraLink provides the ability to limit the number of calls per AP within the NetLink Telephony Gateway and the SpectraLink Voice Priority (SVP) Server. The “Calls per Access Point” setting limits the number of active NetLink Wireless Telephone calls on each AP. Wireless Telephones are free to associate with other APs within range that have not reached the set maximum number of calls. SpectraLink requires this setting to be equal to or below the maximum number of calls discussed in the previous paragraph.

### 2.4.2 Push-to-Talk Multicasting Considerations

The push-to-talk (PTT) mode of the NetLink i640 Wireless Telephone uses SpectraLink's proprietary SpectraLink Radio Protocol (SRP) ADPCM encoding. If a PTT broadcast is active (i.e. a user presses the PTT button), the feature will use the bandwidth as indicated in the table above for "Push-to-Talk transmit" for the AP with the transmitting NetLink i640 handset. All other APs in the system will use the bandwidth in the table for "Push-to-Talk receive" regardless of the number of Wireless Telephones using the AP. The data rate used for PTT depends on the AP's settings for multicast traffic.

Because the PTT mode uses IP multicasting, all APs on the subnet will transmit a PTT broadcast. 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.

### 2.4.3 Telephone Usage

Because data rate and packet rates are constant with voice applications, Wi-Fi telephony calls may be modeled in a manner very similar to circuit-switched calls. Telephone users (whether wired or wireless) generally tend to make calls at random times and of random durations. Because of this, mathematical models can be applied to calculate the probability of calls being blocked based on the number of call resources available.

Telephone usage is measured in units of Erlangs. One Erlang is equivalent to the traffic generated by a single telephone call that is in continuous use. A typical office telephone user will generate 0.10 to 0.15 Erlangs of usage during normal work hours, which equates to six to nine minutes on the telephone during an average one-hour period. Heavy telephone users may generate 0.20 to 0.30 Erlangs, or an average of 12 to 18 minutes of phone usage in an hour. Note that traffic analysis is based on the aggregate traffic for all users, so users with higher or lower usage are included in these averages.

The traffic engineering decision is a tradeoff between additional call resources and an increased probability of call blocking. Call blocking is the failure of calls due to an insufficient number of call resources being available. Typical systems are designed to a blocking level (or grade of service) of 0.5 percent to two percent at the busiest times. Traffic model equations use the aggregate traffic load, number of users and number of call resources to determine the blocking probability. The blocking probability can also be used along with the aggregate traffic load to determine the number of call resources required. Traffic model equations and calculators are available at [www.erlang.com](http://www.erlang.com).

Consider a system with APs that can support six active telephone calls. If a blocking probability of one percent or less is desired, each AP can support approximately 13 moderate Wireless Telephone users. If the AP coverage supports 12 simultaneous calls per AP, each AP can then support approximately 39 moderate users.

The following table shows maximum users per AP based on the AP's ability to handle simultaneous calls:

User Calling Intensity Erlangs per User	Light 0.10	Moderate 0.15	Heavy 0.20
<b>Max Active Calls per AP</b>	<b>Users Supported per AP (1% Blocking Probability)</b>		
1	1	1	1
2	2	2	2
3	4	3	3
4	8	6	4
5	13	9	7
6	19	13	10
7	25	17	13
8	31	21	16
9	37	25	19
10	44	30	22
11	51	34	26
12	58	39	29

**Users Supported per Access Point**

Areas where heavier Wireless Telephone usage is expected, such as cafeterias and auditoriums, can obtain higher call capacity and handle more users by installing additional APs. For most enterprise applications however, the table above should be sufficient in demonstrating the number of wireless handsets supported within each AP's coverage area.

#### 2.4.4 Telephony Gateway

Phone system administrators need to consider the user distribution on NetLink Telephony Gateways much in the same way as they do PBX line cards. NetLink Telephony Gateways incorporate a physical connection to a PBX line card. The phone system administrator should spread departments or functional areas across multiple PBX line cards and multiple NetLink Telephony Gateways so that a failure of either component does not cause a complete wireless handset outage in one department or area. In addition, system administrators must consider that one NetLink Telephony Gateway support a maximum of eight handsets in an active call state. Therefore, heavy users should be spread across Telephony Gateways to reduce the chance of call blocking.

## 3.0 NETWORK INFRASTRUCTURE CONSIDERATIONS

### 3.1 Physical Connections

NetLink Wireless Telephone infrastructure components must connect to a facility's local area network (LAN) using Ethernet switches rather than Ethernet hubs in order to provide adequate bandwidth and limit traffic collisions and bottlenecks.

Ethernet switches should be configured to negotiate the connection requirements automatically. NetLink Telephony Gateways require 10Base-T, half-duplex transmission and the NetLink SVP Server uses 10 or 100Base-T, half or full-duplex transmissions and can be set to automatically negotiate or be configured to a specific transmission configuration.

Network wiring is an important component of any Ethernet-based system and is subject to local and state building code specifications. Cat 5 or better, 4-pair 10/100 Base-T Ethernet cabling should be used for NetLink Wireless Telephone infrastructure equipment.

### 3.2 Assigning IP Addresses

NetLink Wireless Telephones operate as LAN client devices and therefore require IP addresses to work with the network. IP addresses can be assigned statically through the configuration menus on the handsets or dynamically using standard DHCP protocol. The NetLink Configuration Cradle can be used to quickly load and change administration options in the NetLink Wireless Telephones including static IP addresses. For dynamic IP addressing, a DHCP server is required.

NetLink Telephony Gateways and NetLink SVP Servers also require IP addresses and support either static or DHCP address assignment. When using one or more NetLink SVP Server(s), the master NetLink SVP Server must be assigned a static IP address.

When operating with an IP telephony server, the NetLink SVP Server also requires a range of IP addresses that cover the total number of Wireless Telephones supported by that NetLink SVP server.

When a NetLink Wireless Telephone registers with the telephony server, one of the IP address within this range is used to communicate between the NetLink SVP Server and the telephony server. This IP address is used by the IP telephony server as an alias for the NetLink Wireless Telephone but will not be equivalent to the handset's IP address that was either statically assigned or obtained from the DHCP server. The range of alias IP addresses must not be used within any DHCP range or cover the IP address used by any other device. In the case where multiple NetLink SVP Servers are used for added capacity, an exclusive range of IP addresses equivalent to the number of total users each NetLink SVP Server supports is required per NetLink SVP Server.

### 3.3 Software Updates Using TFTP

All NetLink components are field-upgradeable in terms of new software features or capabilities and bug fixes. NetLink Wireless Telephones utilize a TFTP client to automatically download new code when available. NetLink Telephony Gateways have an integrated TFTP server to support NetLink Wireless Telephone and OAI Gateway software upgrades. A network TFTP server will simultaneously update the handsets, while the NetLink Telephony Gateway updates handsets one at a time. Therefore, in a larger system, it is best to use a separate TFTP server rather than using the NetLink Telephony Gateway.

For installations that do not use NetLink Telephony Gateways, a separate TFTP server must be provided. Also, the NetLink SVP Server requires a separate TFTP server for software updates. The NetLink Telephony Gateway cannot be used as a TFTP server for the NetLink SVP Server code. NetLink Telephony Gateways receive software updates only through FTP updates. Software updates are available at [www.spectralink.com](http://www.spectralink.com).

## 4.0 QUALITY OF SERVICE

### 4.1 SpectraLink Voice Priority (SVP)

QoS is a means of providing a level of service that will result in a network connection of adequate quality. Typically this results in providing different levels of service for different applications, depending on their requirements. When data and voice are competing for bandwidth, it is necessary to have a prioritization method that provides a controlled preference to voice packets. The initial 802.11 standards did not provide a practical QoS mechanism, so SpectraLink developed SVP to allow delay-sensitive voice and asynchronous data applications to coexist on a Wi-Fi network without compromising voice quality.

Good voice quality is ensured on a shared network with SVP, which is fully compatible with Wi-Fi networks. Adopted by the leading AP vendors as a de facto standard for voice QoS, SVP guarantees audio quality in a shared voice and data network. Access points generally use random back-off intervals and require all types of traffic to contend for access to the wireless medium with equal rights. However, treating all traffic equally can cause significant delays to voice traffic. Modifying the AP behavior to recognize and prioritize voice packets increases the probability of better performance while continuing to treat asynchronous data packets normally. The two operations that comprise SVP in the AP, minimizing random back-off and priority queuing, require a packet-filtering mechanism. Packet filtering requires recognizing the packet's type, which for SpectraLink packets is registered protocol ID 119 for the SpectraLink Radio Protocol (SRP) at layer 4. The NetLink SVP Server also performs packet delivery timing in the link to the Wireless Telephones, which is critical for ensuring seamless handoffs among APs and for enhanced battery management processes. The following section offers a more detailed explanation of timed delivery.

#### 4.1.1 SVP Infrastructure

To trigger SVP in the APs from the wired side of the network, a NetLink Telephony Gateway and/or NetLink SVP Server is required. NetLink Telephony Gateways can provide SVP support for small installations with four or fewer Gateways. A NetLink SVP Server is required for applications using an IP telephony server or using more than four NetLink Telephony Gateways.

### 4.1.2 SVP Server Capacity

A single NetLink SVP Server supports 120 simultaneous calls when used with NetLink Telephony Gateways or 80 simultaneous calls with an IP telephony server. Multiple NetLink SVP Servers can be used to increase capacity to support up to 850 total calls (which can support approximately 8,000 Wireless Telephones) for IP telephony server interfaces. When used with NetLink Telephony Gateways, the total number of users is limited to 640 (40 NetLink Telephony Gateways). For smaller IP telephony interface deployments, 10 and 20-user SVP Servers are also available. Refer to the “NetLink SVP Server Installation, Setup, and Administration” guide for additional information regarding the maximum number of simultaneous calls and Wireless Telephones supported by multiple NetLink SVP Servers.

### 4.1.3 Multiple SVP Servers

For installations with multiple NetLink SVP Servers, call resources are automatically allocated between the APs and the NetLink Wireless Telephones by those devices’ Media Access Control (MAC) addresses. In most instances, because of the large number of Wireless Telephones and APs expected in such an application, the distribution of call processing will be relatively even across all NetLink SVP Servers.

If a NetLink SVP Server other than the SVP Server assigned as the “master” fails and can no longer be detected, the call processing will be automatically redistributed among the remaining servers. Some active calls may be lost during this process, but the process does not require any manual reconfiguration. To minimize downtime related to a failed master NetLink SVP Server or a single server, a spare NetLink SVP Server can reside on the network, and in the case of a failure, the network administrator can assign the IP address of the failed unit to the replacement SVP Server.

## 4.2 Access Point QoS

Wi-Fi Multimedia (WMM) is a testing and certification program created by the Wi-Fi Alliance and based upon the Enhanced Distributed Channel Access (EDCA) mechanism defined in the 802.11e draft. SpectraLink supports both SVP and the Wi-Fi Multimedia (WMM) QoS methods and either SVP or WMM-enabled APs are required for all NetLink Wireless Telephone installations, even if the wireless LAN is being used only for voice. Without a method of prioritization for voice packets, the lack of a controlled delivery method will result in poor audio quality, reduced capacity, poor handoffs and/or poor battery life even with only voice devices on the network.

Basic WMM implementation in access points generally does not include Unscheduled-Automatic Power Save Delivery (U-APSD) and Call Admission Control (CAC) defined as optional components in the 802.11e standard. Therefore, the SVP Server is still required to ensure the timing and delivery of SpectraLink voice packets, which is especially critical as the user hands off between APs and for improved battery life. The SVP Server also provides call admission control and allows the number of calls per AP to be configured.

### 4.3 VIEW Certification

SpectraLink's Voice Interoperability for Enterprise Wireless (VIEW) Certification Program certifies Wi-Fi network infrastructure products to be interoperable with NetLink Wireless Telephones. The objective of the program is to promote enterprise Wi-Fi telephony interoperability and performance.

VIEW Certification provides customers:

- ▶ Confidence in interoperability and enterprise-grade performance
- ▶ Confidence in integration and partnership between vendors
- ▶ Assurance of excellent voice quality, seamless roaming, maximum capacity and robust network security
- ▶ Demonstration of commitment to industry standards
- ▶ Detailed Configuration and Deployment Guides

Information regarding VIEW Certified wireless LANs and APs that are compliant with SVP can be found on SpectraLink's website. Configuration notes for specific AP models are also available on the SpectraLink website and should be closely followed to ensure a proper deployment for voice.

## 5.0 SECURITY

### 5.1 Security Concerns

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 a facility. The extent of security measures used is typically proportional to the value of the information accessible on the network. The security risk for Wi-Fi telephony 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 solutions can be implemented with NetLink 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.

#### 5.1.1 Wired Equivalent Privacy (WEP)

NetLink Wireless Telephones support Wired Equivalent Privacy (WEP) encryption as defined by the 802.11 standard. The handsets can use either 40-bit or 128-bit key lengths. WEP is intended to provide the same level of security over a wireless LAN as on a wired Ethernet LAN. Although security flaws have been identified, WEP still provides strong encryption that requires an experienced and dedicated hacker to break.

#### 5.1.2 Wi-Fi Protected Access (WPA/WPA2)

Recognizing the need for stronger security standards beyond WEP, the IEEE developed and ratified the 802.11i standard, which includes stronger encryption, key management, and authentication mechanisms. Wi-Fi Protected Access (WPA) is based on draft 3.0 of the 802.11i specification while Wi-Fi protected Access 2 (WPA2) is the Wi-Fi Alliance's certification and test program based on the fully ratified 802.11i standard. The major enhancement of WPA2 over WPA is the inclusion of the Advanced Encryption Standard (AES) for all traffic. AES is widely accepted as one of the most powerful forms of encryption available. SpectraLink's NetLink e340, h340 and i640 Wireless Telephones running on NetLink v2.0 or greater are fully compatible with WPA and WPA2-certified wireless infrastructure equipment.

Due to serious call quality concerns with 802.1x EAP-based authentication, SpectraLink supports WPA and WPA2 only using the Pre-shared Key (PSK) authentication method. 802.1x authentication employs a RADIUS authentication server and an EAP-based key exchange sequence. The time intensive key exchange sequence and roundtrip network latency results in an interruption in service when a client roams from one access point to another. It is unlikely that this interruption will disrupt data clients but real-time services such as voice and video will experience a degradation of service.

### 5.1.3 Cisco Fast Secure Roaming (FSR)

Certificate-based authentication protocols such as EAP-TLS and Cisco's LEAP were developed to provide a higher level of security for wireless networks. These advanced methods require a back-end authentication server to authenticate users and generate new keys. This authentication and re-keying process can take up to several seconds and is required each time a user hands off from one AP to the next in the same subnet. While this is taking place, the client device is not authenticated to an AP. There is an interruption in the data stream, and therefore in the voice conversation. This type of interruption is unacceptable for voice communication in most enterprise applications.

To address the voice quality issues with most security mechanisms, SpectraLink and Cisco have worked together to deliver a Fast Secure Roaming (FSR) mechanism. FSR allows the authentication process to be done in a way that minimizes the number of messages required between the NetLink Wireless Telephones and the Cisco wireless LAN infrastructure. It is designed to be compatible with wireless standards and allow backward compatibility with devices utilizing previous security mechanisms such as Cisco's LEAP.

Implementation of FSR for Cisco APs uses a combination of standards-based and proprietary security components including Cisco Client Key Management (CCKM), LEAP authentication, Michael message integrity check (MIC) and Temporal Key Integrity Protocol (TKIP). FSR not only addresses the roaming issue, but also provides strong security measures for authentication, privacy and data integrity.

## 5.2 Using Virtual LANs

Virtual LANs (VLANs) can be used to segregate traffic into different security classes. By using separate VLANs, data traffic can utilize the most robust but processing-intensive security methods.

The 802.1Q standard establishes a method for inserting VLAN membership information into Ethernet frames via header-information tags. NetLink infrastructure equipment and SVP do not generate or forward these tags, but are otherwise compatible with 802.1Q tags up to the Ethernet switch ports used for the NetLink equipment.

## 5.3 MAC Filtering and Authentication

Most access points can be configured to allow or deny association of wireless clients based on their unique MAC addresses, which can be used as a method of securing the wireless LAN. This process generally works, but can cause some performance issues on some APs.

A more robust method of using MAC addresses to secure the network includes authentication back to a RADIUS server. In general, the delays caused by this type of authentication are not acceptable for voice traffic. Such delays are most noticeable when the Wireless Telephone roams between access points because a re-authentication is often required with each handoff. Having the RADIUS server on the local network will help reduce delays, but the response time of the server may still be an issue. Adding any network delays will compound the issue. Network administrators should evaluate whether such delays are not great enough to affect the voice quality of NetLink Wireless Telephones.

## 5.4 Firewalls and Traffic Filtering

The traffic filtering capabilities of firewalls, Ethernet switches and wireless switches can also be used as an additional security layer if set up 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 NetLink Wireless Telephones.

When using NetLink Telephony Gateways to interface to a traditional PBX, the NetLink Wireless Telephones use the SpectraLink Radio Protocol (ID 119). This protocol is on a peer level with TCP and UDP and does not use ports like TCP and UDP.

For an IP telephony server interface, the ports used depend on the IP telephony protocol of the telephony switch interface. The telephony switch vendor should supply the port numbers used by the protocol.

The NetLink Wireless Telephones, NetLink Telephony Gateways and NetLink SVP Server use TCP and UDP and other common IP protocols from time-to-time. These include DHCP, DNS, WINS, TFTP, FTP, Telnet, ARP and ICMP. SpectraLink uses proprietary UDP channels between the infrastructure components that use UDP ports 5454 - 5458. The PTT mode of the NetLink i640 Wireless Telephone uses the multicast IP address 224.0.1.116, which NetLink Wireless Telephones and infrastructure components also use to locate and maintain each other.

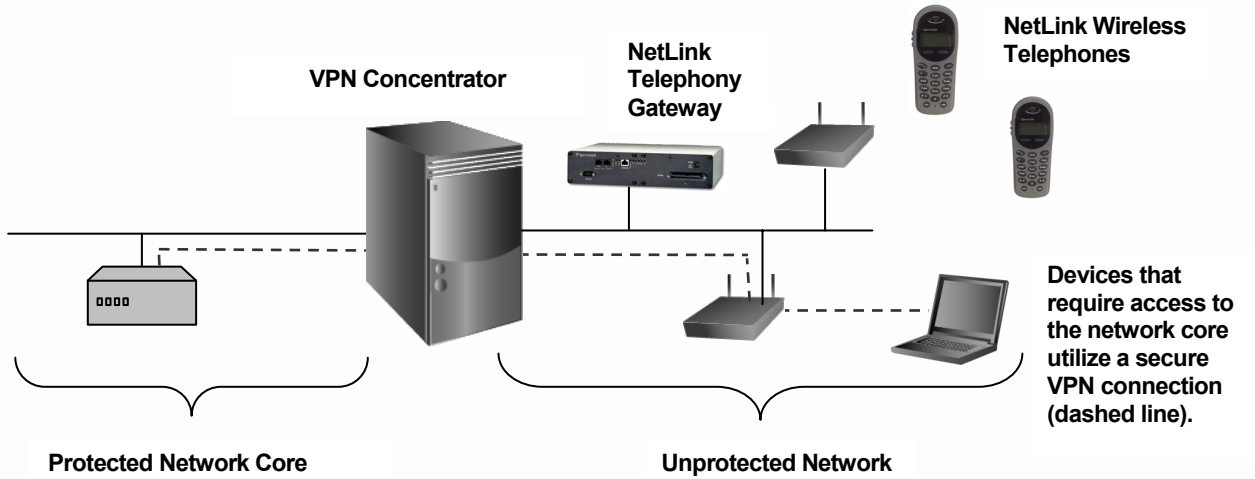
## 5.5 Virtual Private Networks (VPNs)

Virtual Private Networks (VPNs) are secure, private network connections. VPNs typically employ some combination of strong encryption, digital certificates, strong user authentication and access control to provide maximum security to the traffic they carry. They usually provide connectivity to many devices behind a VPN concentrator. The network can be broken into two portions - protected and unprotected:

1. The area behind the VPN server is referred to as the “protected” portion of the network. Sensitive, private network equipment such as file servers, e-mail servers and databases reside in this portion.
2. The area in front of the VPN server is referred to as the “unprotected” network, where the wireless APs and less sensitive network equipment often reside.

VPNs offer an extremely effective method for securing a wireless network. Many network administrators implement VPNs to maintain the integrity of their wireless LANs by requiring wireless users who need access to the protected portion of the network to connect through a VPN Server.

Most voice devices, such as the NetLink Wireless Telephones, do not require access to the protected portion of the network. Placing the NetLink Wireless Telephones, NetLink SVP Server(s) and NetLink Telephony Gateways on the unprotected network and requiring data users to connect to the VPN ensures that the network is protected against hackers seeking to access sensitive information within the network core.



*Deploying NetLink Wireless Telephones with a VPN*

## 6.0 NETLINK WIRELESS TELEPHONES AND SUBNETS

---

Subnets are used to create a boundary between network segments. Although these boundaries are logical, they become somewhat of 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 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. In the case of the NetLink Wireless Telephones, the handsets should be power cycled to obtain a new DHCP address. The handsets can automatically recover in the new subnet from a lost network connection with the original subnet, but the 40-second failure and recovery time generally warrants cycling the power.

Some APs, 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.

SVP can be controlled from a NetLink Telephony Gateway, a NetLink SVP Server or a combination of the two. Because the NetLink SVP Server can only operate in a single-PBX interface mode, Wireless Telephones cannot operate with a NetLink Telephony Gateway and in a native-IP interface to an IP telephony server on the same NetLink SVP server. All SVP Servers must operate in the same PBX interface mode (either native-IP or through NetLink Telephony Gateways).

Since the push-to-talk feature of the NetLink i640 Wireless Telephone uses multicast IP packets, a PTT call will generally be isolated to a single subnet.

There are additional subnet requirements for NetLink Wireless Telephones based on the infrastructure components that are used.

## 6.1 Subnets and NetLink Telephony Gateway Interfaces

NetLink Wireless Telephones, NetLink Telephony Gateways, NetLink SVP Server(s) and the wireless APs generally must reside on the same subnet. This is because NetLink Wireless Telephones use IP multicast messages to initialize the Wireless Telephone registration on the NetLink Telephony Gateways. In addition, The Telephony Gateways and SVP Server(s) use multicast to stay synchronized. Most routers deployed in multi-subnet Ethernet environments are configured to filter out multicast and broadcast messages. If a NetLink Wireless Telephone is powered up on a different subnet than the NetLink Telephony Gateway to which it is registered, the multicast message will not reach the NetLink Telephony Gateway.

## 6.2 Subnets and IP Telephony Server Interfaces

With an IP telephony interface, the SVP Server can be placed on a separate subnet from either the APs or IP telephony server. The NetLink Wireless Telephones will find the SVP Server and IP telephony server on another subnet through the default gateway (router) configured in the handset or DHCP server.

NetLink Wireless Telephones can be deployed across multiple subnets when used with an IP telephony server interface if the performance requirements outlined below are met. One of two deployment scenarios described below can be used, depending on needs and infrastructure capabilities, keeping in mind that the SpectraLink Wireless Telephones will never actively roam across a subnet boundary without power-cycling the handsets unless a VIEW certified layer-3 roaming infrastructure is used in accordance with the VIEW deployment guidelines.

In one deployment scenario for accommodating multiple subnets, each subnet is treated independently with respect to the SVP Servers and wireless network, but each subnet can still provide service to a single IP telephony server. One or more SVP Server(s) can be deployed on each subnet just as with a single subnet system, including identifying each master SVP Server via DHCP or static configuration. In the second scenario, a single SVP Server (or set of SVP Servers with one master) is deployed, generally on the same subnet as the IP telephony server. The single (or master) SVP Server is identified to all phones via DHCP or static configuration, regardless of what subnet the phone is operating in. This scenario requires less SVP Servers to be installed, but requires higher performance from the router (see performance requirements below).

The ability to cross a subnet boundary exists in either scenario, but the NetLink handsets will need to be power cycled to obtain new IP address within the new subnet. In addition, other configuration considerations must be addressed. Because users will not want to re-administer the Wireless Telephones to a separate subnet, Extended Service Set Identifications (ESSIDs) should be the same or the handsets should be set to the “Learn Always” mode, the security mode and associated key should be the same or turned off, and DHCP should be used.

## 6.3 Network Performance Requirements

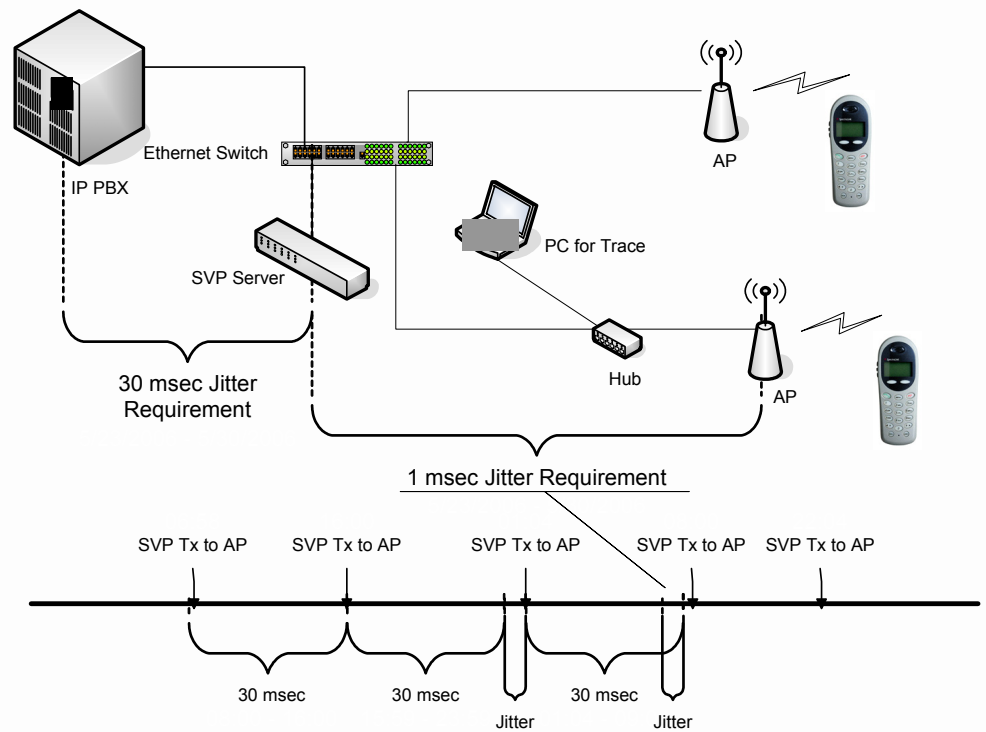
Ethernet packets containing voice as their payload have short, useful lifetimes, making the timely delivery of voice packets essential. Routers can introduce latency and delay between the NetLink SVP Server and the APs, resulting in poor voice quality.

Ethernet connectivity from the IP telephony server or other voice endpoint to the NetLink SVP Server should never exceed 100 milliseconds of network delay (one

way), 30 milliseconds of network jitter, and 2 percent packet loss end to end regardless of the physical properties of the link. The link from the SVP Server to the APs should be under 100 milliseconds of network delay, 1 millisecond of jitter and under 2 percent packet loss. In both cases, the jitter requirements are for wired network jitter and do not include the RF link.

One feature of the SVP Server is to control the timing of packets through the AP. The delay between the SVP Server and the AP does not need to be strictly controlled as long as it is consistent. The jitter requirement between the IP telephony server and the SVP Server is a function of how the audio is packetized for encapsulation in the SpectraLink Radio Protocol (SRP) tunnel and the packet queuing in the SVP Server.

Jitter between the SVP Server and the AP should be measured at the wired Ethernet connection to the AP. If the AP is an AP switch attached to lightweight APs and SpectraLink has VIEW Certified the system, jitter can be measured at the entry to the AP switch. For this measurement, assume the SVP Server is delivering packets at 30millisecond intervals with no jitter. The time is measured from the arrival of one packet from the SVP Server directed to a single Wireless Telephone to the next packet from the SVP Server to the same Wireless Telephone. The jitter measurement is the time difference from the ideal 30 millisecond arrival of packets at the AP.



*Measuring Network Jitter*

In a multiple SVP Server configuration, jitter is measured from the SVP Server that is responsible for the traffic to a given AP. This may be different than the SVP Server that is acting as a proxy for the Wireless Telephone to the IP PBX.

NetLink handsets have a diagnostic option that includes jitter measurement. The calculated jitter shown in this mode is not the jitter described above because it includes delays in the AP, radio link and queue times inside the Wireless Telephone. Jitter information from the handset diagnostic mode should only be used as a guideline for diagnosing major network or radio link problems.

## 7.0 CONCLUSION

---

Telephony over a wireless LAN represents the convergence of voice and data technology in the wireless environment. There are certain network design criteria that must be met for the network to successfully accommodate the demanding requirements of both voice and data.

By applying the guidelines described in this document, networking and telephony professionals can come together to confidently design and deploy a SpectraLink Wi-Fi telephony solution. Some of the major considerations include:

- Voice and data applications have different attributes and network requirements. Several aspects of the wireless LAN 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.
- Several network design attributes need to be considered before deploying a SpectraLink solution, including the use of subnets and complex network topologies that may not be conducive to the performance requirements of NetLink Wireless Telephones.

SpectraLink's dedication and expertise in wireless VoIP can help ensure proper deployment for voice over wireless LAN. SpectraLink's Voice Interoperability for Enterprise Wireless (VIEW) Certification Program certifies Wi-Fi network infrastructure products to be interoperable with and meet the performance requirements of NetLink Wireless Telephones. In addition, SpectraLink offers professional services including site surveys and deployment assistance.