



SpectraLink and KIRK are now part of Polycom

Best Practices for Deploying Enterprise-Grade Wi-Fi Telephony

Security, coverage, capacity, and QoS considerations
for ensuring excellent voice quality with enterprise
Wi-Fi networks

October 2007

Best Practices for Deploying Enterprise-Grade Wi-Fi Telephony

October 2007

White Paper

Table of Contents

Introduction	3
Security	3
Coverage	4
Capacity	5
Quality of Service	6
Conclusion	7

Best Practices for Deploying Enterprise-Grade Wi-Fi Telephony

October 2007

White Paper

Introduction

Wi-Fi telephony enables the convergence of voice and data applications using a common wireless local area network (WLAN). It bridges traditional telecommunications, data networking, and mobile technologies to deliver highly functional products that are easy-to-use and provide cost savings for enterprise customers. A Wi-Fi-enabled handset is a WLAN client that uses the same network as wireless laptops, PDAs, and a host of other wirelessly-enabled devices. In addition, a Wi-Fi-enabled telephone may be functionally equivalent to a wired telephone, allowing 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 to eliminate recurring charges or redundant costs.

This paper addresses the network performance requirements and related deployment considerations for delivering high-quality voice over a Wi-Fi network. For example, as a mobile communication device, a Wi-Fi telephone requires special considerations for continuous high-quality connections as a user moves throughout the coverage area. Another important difference between voice and data applications is their 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. Data applications are typically bursty in terms of bandwidth utilization, while a telephone conversation creates a consistent and relatively small amount of traffic.

A critical objective in deploying enterprise-grade Wi-Fi telephony is to maintain similar voice quality, reliability and functionality as is expected in a wired telephone environment. Key issues in deploying Wi-Fi telephony are security, coverage, capacity, and quality of service (QoS), all of which are addressed in this paper.

SpectraLink, now a part of Polycom, pioneered the use of Wi-Fi-enabled telephones in a wide variety of applications and environments, making the SpectraLink 8000 Wireless Telephones the market-leading solution. Based on Polycom's extensive experience with enterprise-grade deployments, this white paper provides a high-level discussion of the unique deployment issues with Wi-Fi telephony along with solutions and recommendations.

Security

The first issue often raised with any wireless technology is security. 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 Wi-Fi network. Determining the proper level of security should be based on identified risks, corporate policy and, an understanding of the benefits and limitations of the available security methods.

In 2004, the IEEE developed and ratified the 802.11i standard, which includes strong encryption, key management and authentication mechanisms. Wi-Fi Protected Access 2 (WPA2) is the Wi-Fi Alliance's certification and test program based on the 802.11i standard. WPA2 includes

Best Practices for Deploying Enterprise-Grade Wi-Fi Telephony

October 2007

White Paper

Advanced Encryption Standard (AES), which is widely accepted as one of the most secure encryption algorithms available today.

WPA2 has two different authentication modes available: Enterprise mode and Personal mode. Enterprise mode uses 802.1x EAP-based authentication, while Personal mode uses a pre-shared key (PSK). Enterprise mode authentication requires an 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 device roams from one Wi-Fi access point (AP) to another. The interruption in the data stream during the authentication process has little effect on data applications, but causes noticeable drop-outs for real-time applications such as voice and video. For this reason Personal mode using a PSK is the preferred method to maintain excellent voice quality as users roam throughout an enterprise. PSK authentication is significantly more secure than legacy security methods because the PSK is used only for authentication and is never transmitted over the air.

In order to maintain the appropriate security level for different wireless applications, 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, while time-sensitive voice applications can use PSK. Separating all voice terminals and voice application servers or gateways onto a unique VLAN allows a more appropriate level of security to be implemented without compromising security for data applications and devices. Another option is to use WPA2 Personal mode but require VPN access for data applications, ensuring the highest level of data security without impacting voice quality for Wi-Fi telephony applications.

In addition, the IEEE 802.11r task group is developing a standard protocol for minimizing hand-off interruptions while supporting 802.1 x authentications. There are also proprietary security mechanisms that address the issue of hand-off authentication that are available from various Wi-Fi infrastructure vendors.

Key takeaway: *Voice-friendly, enterprise-grade Wi-Fi security mechanisms are available today. Segregating voice and data traffic provides flexibility in choosing the most appropriate security mode for the application.*

Coverage

One of the most critical considerations in deployment of Wi-Fi telephony is ensuring there is sufficient wireless coverage. Enterprise Wi-Fi networks are often initially planned for data applications and may not provide adequate coverage for a wireless telephony. 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 than with data applications. In areas of poor wireless coverage, the performance of data applications may be acceptable due to retransmission of packets, but for real-time voice, audio quality will likely suffer.

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. Wi-Fi telephones are typically held very close to the user's body, introducing additional radio signal attenuation, while data devices are usually set on a surface or held away from the body. This factor may result in

Best Practices for Deploying Enterprise-Grade Wi-Fi Telephony

October 2007

White Paper

reduced range for a Wi-Fi telephone as compared with a data device, therefore the Wi-Fi network layout should account for some reduction of radio signal propagation.

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 wireless telephones users move about the workplace, the devices seek out other APs to hand-off to, or re-associate with, in order to maintain the most reliable network connection. A properly designed Wi-Fi network will provide for a seamless hand-off 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. When Wi-Fi networks enable automatic rate switching capabilities, so that as the radio signal degrades as user moves away from the AP, the radio can adapt and uses a less complex and slower transmission scheme to send the data. The result is increased range but at reduced transmission rates, which lowers the total bandwidth available to all devices associated with an AP. It is important to take rate switching into account when laying out a Wi-Fi network, and either accept less bandwidth (and capacity) to increase coverage, or increase the number of APs required to maintain acceptable coverage at higher data rates.

The maximum signal strength of the APs can also be modified to allow denser deployment while minimizing co-channel interference from nearby APs. It is important to take this into account in Wi-Fi network design in order to maintain as much consistency as possible for wireless devices. A site survey is useful for determining the received signal level for wireless devices throughout the coverage area, and device vendors usually recommend specific minimum signal levels to maintain excellent voice quality. Although it is possible that Wi-Fi handsets operate at signal strengths below the recommended values, real-world deployments involve many radio signal propagation challenges such as physical obstructions, interference and multipath effects that impact both signal strength and quality. Planning AP coverage to the recommended signal levels will provide an adequate buffer for these propagation challenges and provide a reliable and consistent level of performance.

In general, Wi-Fi networks should be deployed using industry best practices for channel selection, power levels, and overlapping coverage. A wireless site survey is highly recommended for any Wi-Fi network deployment, however it is especially critical when voice is an application on the network and is essential for large or complex facilities. A site survey can ensure that the wireless network is optimally designed and configured to support voice by confirming coverage; cell overlap; channel allocation and reuse; packet transmission quality and other wireless LAN infrastructure deployment considerations.

Key takeaway: *Plan for comprehensive Wi-Fi coverage, since Wi-Fi telephone users are mobile throughout the facility. Utilize site survey and analysis services. Use tools to plan and deploy the APs in optimal locations with proper channel and power settings.*

Capacity

Network capacity requirements factor into the number of APs required, although in most cases, coverage area is the primary factor. Unlike voice traffic, data traffic is often bursty and sporadic. This is typically acceptable for WLANs because data applications can tolerate network congestion with reduced throughput and slower response times. Voice traffic, however, cannot tolerate unpredictable delays without negatively impacting voice quality. Voice traffic can be predicted

Best Practices for Deploying Enterprise-Grade Wi-Fi Telephony

October 2007

White Paper

using probabilistic usage models, allowing a network to be designed with high confidence in meeting anticipated voice capacity requirements.

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. 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). Lower overall bandwidth is available when there are a greater number of devices associated with an AP.

Several factors determine the AP bandwidth utilization during a telephone call. The first is the Voice over Internet Protocol (VoIP) protocol used and its characteristics. The codec being utilized 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 little more than half of a typical voice packet, with 802.11 protocol and IP overhead filling the rest. 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. Using 802.11b as an 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. More calls per AP can be achieved by using 802.11a, 802.11g and the emerging 802.11n standard with similar non-linear results.

The number of simultaneous calls supported by an AP can be a fraction of the number of actual users expected in the coverage area. In most enterprise applications the number and duration of telephone calls can be statistically predicted using telephone traffic analysis to meet anticipated caller density. Areas where heavier Wi-Fi telephone usage is expected, such as cafeterias and auditoriums can be covered with higher call capacity and handle more users by installing additional APs.

Key takeaway: *Wi-Fi networks offer sufficient call capacity for most enterprise voice applications, although special consideration may be required for areas where users congregate or for high call-traffic applications.*

Quality of Service

QoS is required for any network that supports multiple applications with different requirements for packet latency and jitter. When data and voice are competing for bandwidth, it is necessary to have a prioritization method that favors voice packets in order to maintain consistent voice quality. The initial 802.11 standards did not provide a practical QoS mechanism, so proprietary solutions such as SpectraLink Voice Priority (SVP) were developed to allow time-sensitive voice and asynchronous data applications to co-exist on a Wi-Fi network without compromising voice quality.

Best Practices for Deploying Enterprise-Grade Wi-Fi Telephony

October 2007

White Paper

Excellent voice quality is ensured on a shared Wi-Fi network with SVP, which is fully compatible with Wi-Fi standards. Adopted by the leading AP vendors as a de facto standard for voice QoS, SVP guarantees audio quality for SpectraLink handsets in a shared voice and data network. SVP provides prioritization of voice packets at the APs, along with minimizing back-off times to give voice packets favorable network access. SVP also improves network capacity and handset power utilization through timed delivery of packets. Controlling the timing of packet transmissions allows devices to use their radio resources more efficiently, improving battery life.

Today, standards-based QoS is becoming available using the Wi-Fi Alliance's Wi-Fi Multimedia (WMM), WMM Power Save and the forthcoming WMM Admission Control specifications, all based on the IEEE 802.11e standard. Basic WMM provides a prioritization mechanism with four levels assigned to different types of wireless applications: voice, video, best-effort data, and low-priority background data. WMM Power Save allows battery-operated devices to maximize power efficiencies by coordinating packet delivery with Wi-Fi APs. The forthcoming WMM Admission Control specification will add the final piece that is required for enterprise-grade QoS for voice devices – allocating available bandwidth for associated devices, based on their traffic requirements. WMM Admission Control will avoid oversubscription of AP resources, which is critical to maintaining voice quality.

Key takeaway: *QoS is critical for enterprise-grade Wi-Fi telephony to consistently ensure excellent voice quality. Proprietary and standards-based QoS mechanisms are required to improve device battery life and prevent AP oversubscription.*

Conclusion

Wi-Fi telephony represents the convergence of voice and data technology on a wireless LAN. There are certain design criteria that must be met for the network to successfully accommodate the demanding requirements of both voice and data. Although deploying Wi-Fi telephony requires special considerations for security, coverage, capacity, and quality of service, standards-based solutions are available to ensure enterprise-grade voice quality and system performance.

Deploying voice applications on a Wi-Fi network requires proper pre-installation planning. Site survey tools and network analysis services are highly recommended to identify potential network issues before deployment, along with ongoing network performance monitoring to maintain consistent quality and performance.

By applying the guidelines described in this document, networking and telephony professionals can confidently design and deploy a Wi-Fi telephony solution.

Polycom Headquarters: 4750 Willow Road, Pleasanton, CA 94588 (T) 1.800.POLYCOM (765.9266) for North America only.
For North America, Latin America and Caribbean (T) +1.925.924.6000, (F) +1.925.924.6100

Polycom Wireless

Voice Communications: 5755 Central Avenue, Boulder, CO 80301 (T) 1.800.676.5465 or +1.303.440.5330, (F) +1.303.440.5331