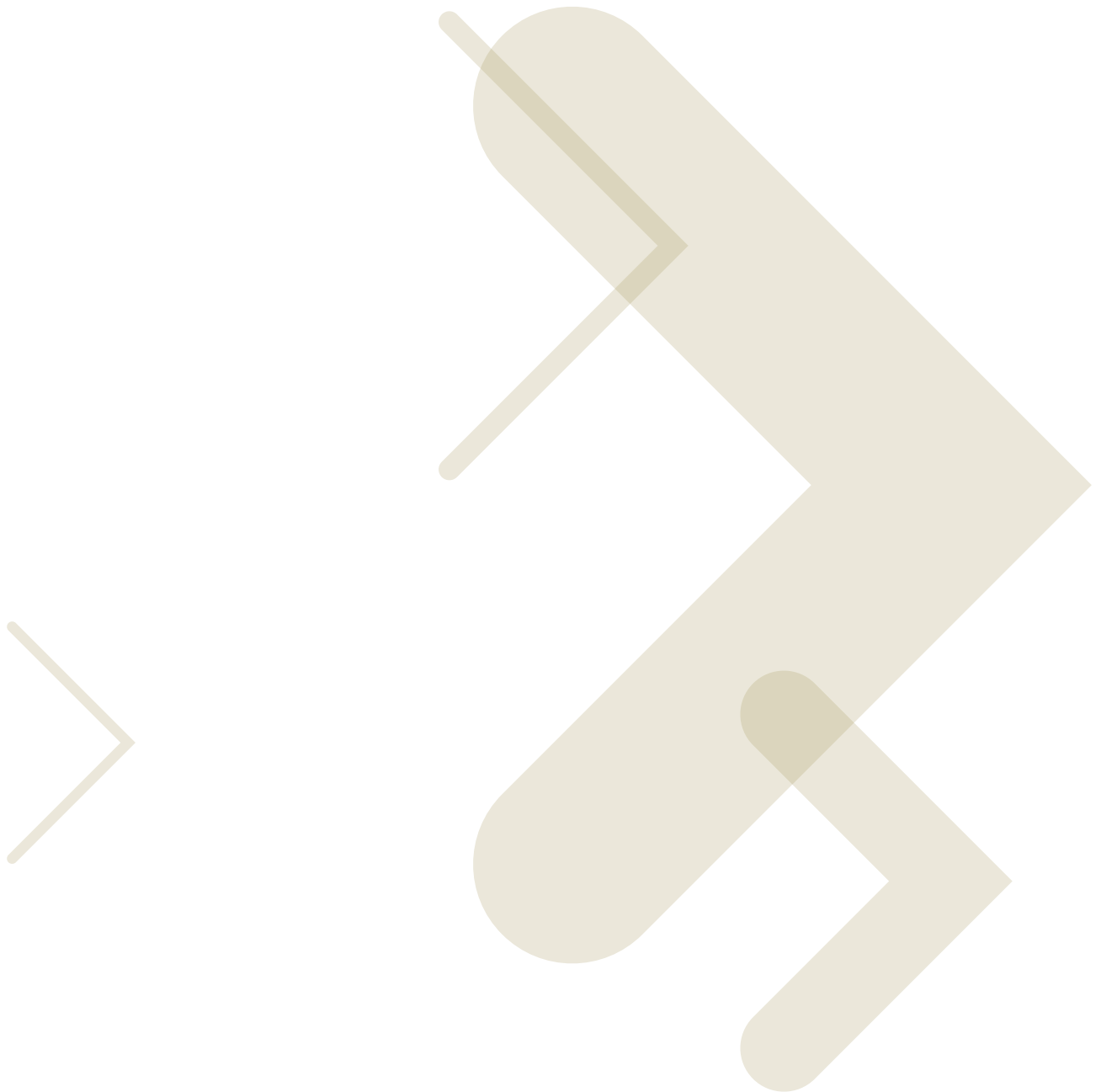




# Preparing your WLAN infrastructure for voice



## Introduction

Adding mobility to enterprise voice communications can be the key to unlocking business productivity and responsiveness. Whether addressing production problems, planning promotions or responding to customer requests, enterprises require that associates be able to move about freely and still be accessible at a moment's notice. Those communications links must extend from the office to the shop floor and out to the loading dock.

The *Webtentials 2008 State of the WLAN Report* indicates that 36% of enterprise wireless LANs support voice today, and an additional 33% plan to add it within the next 12 months. Organizations of all types are using their wireless LANs to support mobile workers with both connection-based and push-to-talk voice services in a wide range of applications. From healthcare to retail and warehouse management, users are discovering the benefits of cost-effective continuous access. However, that flexibility and responsiveness will depend on having a reliable mobile network that allows employees to remain productive while they move through their daily activities.

A sound and reliable wireless infrastructure is needed to ensure the quality and availability of a mobile voice service. At the outset, it is imperative that the networking group recognize the requirements of a WLAN voice network, assess the capabilities of their existing infrastructure and take the necessary steps to bring the network capacity and coverage up to the levels needed to support enterprise-quality voice services. Mobility will not lead to improved productivity if the network is unreliable or unable to provide good voice quality.

## Defining requirements for WLAN voice

The first step in a voice over WLAN (VoWLAN) project will be to develop a definition of service you look to provide, and that starts with an adequate definition of requirements. The first step is to specify the number of users to be served, the type of voice service you will provide (i.e., traditional voice calling or push-to-talk), the areas where the service will be available and the expected traffic volumes. Having a handle on traffic volumes and usage patterns will not only help in planning your infrastructure requirements, it will also be key in determining other parameters such as battery requirements.

In contrast to data users who typically operate from a stationary location, voice users are highly mobile, so it will be difficult to predict accurately where they will be when they need to make or receive calls. That means you will also require a sound network management system that allows you to identify capacity and coverage problems, and plan for expansion. Further, mobility is highly appealing, and as other employees see that the service is available, you can anticipate more requests, more mobile handsets and hence more WLAN voice traffic.

In defining your requirements it will also be important to categorize the various types of users to be supported (e.g., general office, tech support, security, production, etc.), the criticality of their communications (e.g., general business calls versus security or emergency services) and the types of handsets or other mobile voice-enabled devices they will be using. Classifying users can help to quantify the volume and location of calling and will also be useful in predicting the amount of traffic additional users of that type will likely generate. Finally, you should identify the types and models of the WLAN voice devices you will support, and the systems for maintaining them. New WLAN voice devices are introduced regularly, so you should define the procedure by which new devices are tested before they are added to that list.

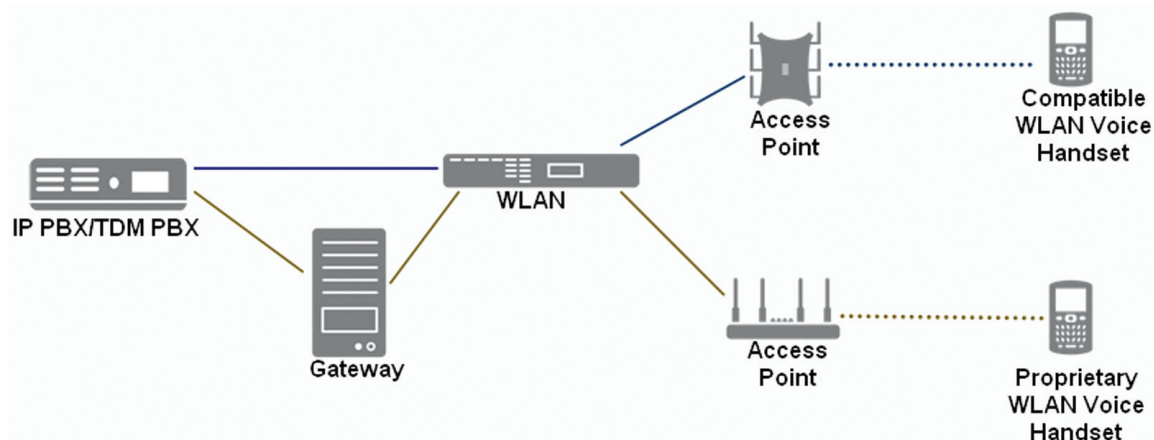
## Getting your wired network ready for WLAN voice

The backbone for your WLAN voice service will be the wired LAN. Whether your wired voice system is based on an IP PBX, a traditional TDM model or a hybrid configuration, you will have to interconnect calls between the wired and wireless systems. Further, if you will be supporting push-to-talk (PTT) devices, they should be able to interconnect to any other PTT systems or services you already have in place.

The requirements for the wired network interconnection will vary based on the nature of the wired telephone system and the signaling that is used on the wireless LAN voice devices. As shown in Figure 1, if the wireless LAN handsets use a signaling protocol that is compatible with the telephony server on the wired IP PBX, you should be able to pass calls directly through to the wired LAN. On the other hand, if you are using a TDM PBX or a WLAN handset that employs a proprietary signaling system, you will require a gateway between the wireless LAN devices and the wired PBX. In the longer term it is expected that all voice services will migrate to IP technology and the Session Initiation Protocol (SIP) will be adopted as the signaling standard, which should greatly ease the integration of wired and wireless users.

If you are using an IP PBX or a hybrid configuration that supports LAN-connected IP/Ethernet handsets, there are several features and configurations that are universally recommended for the wired LAN infrastructure. Those would include:

- A fully-switched LAN configuration (i.e., no hubs)
- Use of 802.1p QoS for prioritizing voice frames over the LAN
- Power over Ethernet (PoE) to power wired IP handsets and WLAN access points
- All voice devices should be configured on a separate virtual LAN (VLAN) for improved security capabilities



**Figure 1:** If the wireless LAN handsets use a signaling protocol that is compatible with the telephony server on the wired IP PBX, you should be able to pass calls directly through to the wired LAN. On the other hand, if you are using a TDM PBX or a WLAN handset that employs a proprietary signaling system, you will require a gateway between the wireless LAN devices and the wired PBX.

These features must be coordinated with the WLAN voice implementation. The WLAN is a shared media configuration, but the use of a fully-switched wired infrastructure will minimize the delay for delivery of voice frames over the wired network. The 802.1p QoS standard is important to minimize delay in forwarding voice frames, and that implementation will have to be coordinated with the WLAN's 802.11e QoS; those issues will be described later. To associate WLAN voice devices with the voice VLAN in the wired network, you will have to define separate wireless VLANs with different network names (i.e., SSID's) for the voice and data traffic. Those wireless voice and data users may be sharing the same WLAN channel, but each group can still be associated with the appropriate wired VLAN.

The WLAN access points will be connected over the wired infrastructure. For that, it is important that the LAN switches be capable of supporting the required number of IEEE 802.3af Power over Ethernet (PoE) ports. Both wireless LAN access points and wired IP voice handsets use PoE, so if you are using or planning to migrate to an IP PBX, you will want to ensure there is sufficient PoE capacity on your LAN switches or be prepared to invest in mid-span PoE devices. Further, you must ensure that the power supplied is sufficient for the access points you intend to use.

One major development in WLANs is the introduction of the new higher capacity 802.11n radio link. WLAN access points supporting the

54 Mbps 802.1a or g radio links require a 100 Mbps connection to the wired LAN. If you plan to upgrade to 802.11n, the access points will require 1 Gbps wired connections. WLAN voice handsets supporting 802.11n are not likely to appear for the next few years, but n-capable access points might still be used to provide higher capacity data services, so choosing a vendor with a strong 802.11n portfolio will be key.

Finally, the network management capabilities of the wired LAN network should be investigated with regard to their ability to provide information that will be useful in supporting voice applications.

## The WLAN infrastructure

The basic requirement for a WLAN infrastructure to support voice is dense, pervasive coverage. Density refers to the signal strength and pervasiveness refers to the coverage. Signal strength impacts the transmission rate users receive on the network and hence the number of simultaneous calls that can be supported on an access point. The generally accepted design parameter is a received signal strength floor of -67 dBm, though better designed handsets can often work down to -70 dBm. The goal is to provide signal strength that will result in the most efficient network utilization, the shortest transit delays and the maximum number of calls supported.

With regard to density, there are two important factors that characterize WLANs: shared media and adaptive modulation. Shared media means that

all devices associated with an access point take turns using one half duplex channel. As with any contention-based network, the greater the volume of traffic vying for access to the channel, the greater the delay that users will experience. Good signal coverage results in better network efficiency, and that in turn leads to lower transit delays, a key factor in providing high quality voice. For enterprise-grade voice service, the requirement is to provide one-way, end-to-end delay below 150 msec.

Better signal coverage also leads to higher transmission rates. WLAN devices use adaptive modulation, which means the WLAN device reduces its transmission rates as the signal strength decreases and the signal-to-noise ratio degrades; the range of data rates supported on WLANs is summarized in Table 1. Signal strength is primarily a factor of the distance to the access point and any material obstructions in the path. In a shared media network, adaptive modulation means that faster and slower transmitters will be sharing the same channel. It stands to reason that the channel will be used most efficiently if all stations transmit at their highest data rates. Further, devices with poor signal quality will not only transmit at lower rates, they will have to retransmit more frequently, increasing delay and degrading efficiency.

In selecting WLAN voice equipment it is important to locate devices that can operate in both the 2.4 GHz (i.e. 802.11b/g) and 5 GHz (i.e.802.11a) bands. Support for the 5 GHz 802.11a interface provides far greater flexibility in the network configuration. First, the 5 GHz band provides a

potential 23 non-interfering channels versus three in the 2.4 GHz band. Further, the 2.4 GHz channels might already be congested with data traffic, particularly if 802.11b and g devices are sharing the channel. The 5 GHz band provides an expansive frequency window for voice deployments with fewer interference issues and no impact on 2.4 GHz data users.

The key to providing high-quality voice service is a WLAN network design that delivers good signal strength throughout the desired coverage area; everything works better with a strong signal. Devices will transmit at the highest data rates, the channel will be used more efficiently and there will be fewer retransmissions all of which leads to higher call capacity. Good signal quality is a result of sound network design and a configuration with sufficient access points to support the expected volume of voice traffic. Maintaining that level of performance over time requires a network management system that monitors traffic volumes and identifies problem areas before they affect user performance.

With regard to coverage, most organizations have deployed WLANs with “spot coverage” in conference rooms, public areas and other defined areas (e.g., loading dock, warehouse, etc.) where they need to support mobile devices. *The Webtorials 2008 State of the WLAN Report* notes that only 55% of users report having WLAN coverage throughout the office areas. Voice users may wander anywhere within the facility, and the WLAN service will have to be available so they can make and receive calls.

IEEE 802.11 Radio Link Interfaces						
Standard	Max. Bit Rate	Fallback Rates	Channel Bandwidth	Transmission Band	Non-Interfering Channels	Radio Technique
02.11b	11 Mbps	5.5 M, 2 M, and 1 Mbps	22 MHz	2.4 GHz	3	DSSS
02.11g	54 Mbps	Same as 802.11a plus 11 M, 5.5 M, 2 M, 1 Mbps	20 MHz	2.4 GHz	3	OFDM
02.11a	54 Mbps	48 M, 36 M, 24 M, 18 M, 12 M, 9 M, and 6 Mbps	20 MHz	5 GHz	23	OFDM

Table 1

It is generally accepted that any large-scale, enterprise-grade wireless LAN should be built using a centrally controlled WLAN switch. As WLANs grew in size and importance, it became clear that networks built on autonomous standalone access points were too difficult to design and manage. In a centrally-controlled solution, a network of thin access points is coordinated by a central controller that can assign channels and adjust transmit levels automatically to ensure good coverage throughout the area.

The major decision regarding the infrastructure will be whether voice and data devices are supported on the same or on different wireless LANs. While the idea of building a separate WLAN for voice was originally viewed as wasteful extravagance, centrally-controlled WLAN switches are making this strategy more cost effective. A single WLAN controller can typically support both networks, and many commercial access points can be configured with two radios. As a result, much of the infrastructure can be shared. This type of deployment is called a dual overlay network, and it would typically use a 2.4 GHz 802.11b/g network for data devices and a 5 GHz 802.11a network for voice. It is important to note that signal loss is greater at 5 GHz than at 2.4 GHz, so a 5 GHz network will typically require more access points to effectively cover the same area.

## Network design tools

A sound network design is the starting point for any voice-capable WLAN infrastructure. The first generation of wireless LANs were built using an inexact and time-consuming process of trial and error. That process involved conducting a site survey, identifying potential locations for access points, assigning channels to each and then adjusting the transmit power to achieve adequate coverage with minimal interference between access points assigned to the same channel. With only three non-interfering channels in the 2.4 GHz band, minimizing interference could be highly problematic.

Once the preliminary installation was complete, the network designers could then spend a considerable amount of time tuning the network. Those adjustments would involve relocating access points to improve coverage, reassigning channels and adjusting transmit power to minimize interference. That process would have to be

repeated on a smaller scale each time a new access point was added to the network.

One of the important developments in wireless LANs has been the introduction of computerized network design tools. To use the design tool, the user first imports a CAD drawing of the facility. They then define the scale, building materials (e.g., sheet rock versus cinder block walls) and furnishings as they will affect the signal propagation. Finally they identify the number of users, capacity requirements and whether the network will be using 2.4 GHz or 5 GHz channels. The better systems also take into account the design of the handset, in particular the antenna. In that way it is possible to provide an accurate assessment for both inbound and outbound transmissions. Based on those inputs, the tool generates a design for the installation that identifies the number and placement of access points, the channels to be used in each area and the transmit power setting based on formulas that reflect signal loss based on frequency, distance and material obstructions.

The result is that you can have a highly accurate design that can cut weeks off the time it takes to tune the network. Rather than a set of circular coverage areas centering on each access point, you will typically find that the building materials and other features in the environment shape the coverage area. With a sound preliminary design, the RF management capabilities of a centrally controlled WLAN switching system will allow you to implement a network that is capable of supporting the stringent requirements of WLAN voice traffic.

## WLAN network features for voice

While a sound radio infrastructure will be essential for any WLAN voice deployment, there are several specific features that will also be important for voice support. In particular, these features will deal with quality of service (QoS), handoffs and battery life.

### **IEEE 802.11e/Wi-Fi Multi-Media (WMM) Quality of Service (QoS)**

To recognize the requirement for WLAN QoS, it is important to understand a little about the WLAN access protocol used on wireless LANs. WLANs use a protocol called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Wireless LAN stations transmit and receive on the same channel, so, when a device is transmitting, it cannot hear other transmitters; hence there is no way to

“detect” collisions as is done in a traditional wired Ethernet. To complete each transmission, the receiving station tests the frame for errors and returns an acknowledgement.

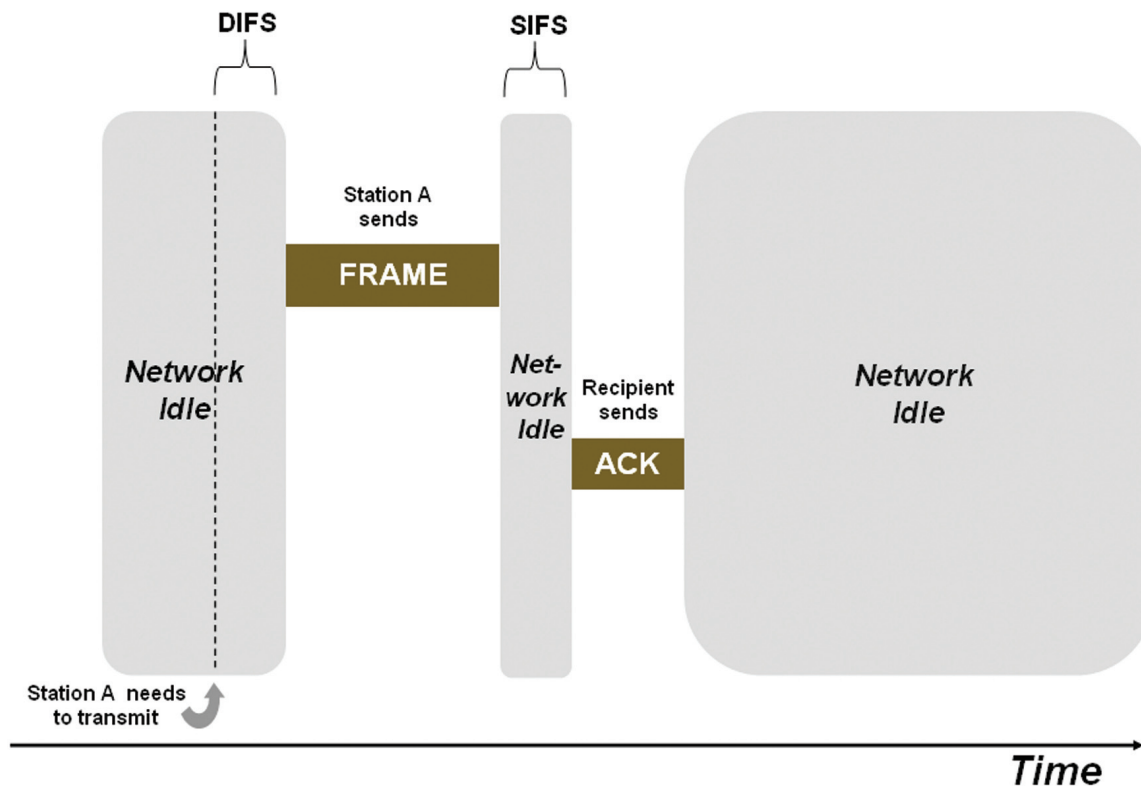
As collisions cannot be detected, the WLAN protocol takes steps to help avoid collisions. When a WLAN station senses that the channel is idle, it waits a defined interval called an Inter-Frame Spacing before it attempts to transmit. If a collision or other failure occurs (i.e., the sender does not receive an acknowledgement), the stations back off by a random interval before trying again; that back-off range is called a contention window (CW). The stations also back-off a random amount if they sense the channel is busy when they try to access it.

The original 802.11 CSMA/CA protocol defined two pre-transmission waiting intervals:

- **DCF Inter-Frame Spacing (DIFS):** The interval a station waits before sending a frame
- **Short Inter-Frame Spacing (SIFS):** The interval a station waits before sending an acknowledgement or ACK.

As the SIFS interval is shorter, if one station is waiting to send a frame and another is waiting to send an ACK, the ACK will always be sent first.

Recognizing the time-sensitive nature of voice transmissions, in 2005 the IEEE introduced a quality of service mechanism designated 802.11e; the Wi-Fi Alliance identifies products that are compatible with that standard as Wi-Fi Multi-Media (WMM) Certified.



**Figure 2:** To help avoid collisions, the WLAN access protocol uses a system of pre-transmission waiting intervals. Those waiting intervals are of varying duration, so they can serve as a mechanism for prioritizing transmissions (e.g., higher priority transmissions are assigned shorter intervals). If collisions occur, the intervals can be random to lessen the likelihood of subsequent collisions. The above diagram shows the process of transmitting a frame and the resulting acknowledgement. The acknowledgement is sent with the shortest waiting interval (i.e., SIFS), which means that the acknowledgement will be sent before any other traffic can be generated.

The 802.11e EDCA/WMM option defines an “enhanced” access mechanism with different pre-transmission waiting intervals called Arbitrated Inter-Frame Spacing (AIFS). To give time-sensitive voice and video transmissions higher priority access to the shared radio channel, they are assigned shorter pre-transmission waiting intervals. So if a voice user and a data user are both waiting to transmit a frame, the voice user will always go first. The standard also defines shorter back-off ranges (i.e. CWMIN and CWMAX) for the higher priority retransmissions.

The four priority levels or Access Categories (ACs) are designated:

AC 1: Voice

AC 2: Video

AC 3: Data: Uses the same pre-transmission interval and back-off range as legacy (i.e. pre-802.11e) WLAN devices

AC 4: Background Data

The AIFS and Contention Window ranges for each access category are summarized in Table 2.

IEEE 802.11e Default Parameters								
Parameter	DSSS PHY (802.11b)				OFDM PHY (802.11a/g)			
	Access Category				OFDM Access Category (802.11a/g)			
	1	2	3	4	1	2	3	4
IFS (SIFS + x Time Slots)	2	2	3	7	2	2	3	7
IFSTime (µsecs)	50	50	70	150	28	28	37	73
WMIN	7	15	31	31	3	7	15	15
WMAX	15	31	1023	1023	7	15	1023	1023

**Table 2**

Note: Time slot duration is 20 µsec for 802.11b and 9 µsec for 802.11a/g

Given the shared media design of a WLAN, 802.11e/WMM will be a critical element in ensuring enterprise-grade voice services over the wireless LAN. The priority setting in the WLAN must be coordinated in the access point configuration so that voice frames are marked with the corresponding 802.1p priority before they are forwarded over the wired LAN. That QoS mechanism must also be coordinated with the IP Differentiated Service (DiffServ) priority, as users may roam between different IP subnets.

### Handoffs

Along with QoS, a WLAN voice network must also be capable of handing off connections from access point to access point quickly and securely as a user moves through the coverage area. In a typical WLAN voice deployment, the radius of an access point's coverage area will be roughly fifty feet. At typical walking speeds, a user will cross the coverage area of a cell in 20 to 30 seconds, so a call may experience several hand offs if the user is walking. The initial laptop oriented Wi-Fi standards provided a handoff that might take 5 to 10 seconds. While that might be suitable for data applications, it certainly does not meet the performance requirements of a voice application.

The IEEE 802.11r committee has developed a standard for fast, secure hand-offs, with a performance objective of 50 msec for the handoff time. Even without this standard, existing WLAN switching systems can provide handoffs in time ranges that are almost as good. Current systems support handoff latency between 10 and 150 msec; typically the longest intervals are for handoffs that involve moving stations between IP subnets. However, even a 150 msec handoff interval will result in a barely perceptible click in the conversation path. As time goes on, it is anticipated that WLAN infrastructure vendors will all migrate to the 802.11r standard; however the ability to do fast, secure handoffs should not be a deterrent to deploying WLAN voice systems today.

The 802.11r standard will provide an improved handoff function. Using the IEEE 802.11k standard for Radio Resource Management, the Wi-Fi clients can collect information regarding nearby access points, a capability called neighbor reporting. Not only will that information be important to guide handoff decisions, it will also allow stations to do opportunistic key caching, where they can store encryption keys for those adjacent access points. The combination of 802.11r and 802.11k will allow a station to roam to another access point more quickly as it will not need to secure an encryption key as part of the handoff process.

### Battery life

One last though critical element in providing an enterprise-grade voice over WLAN solution has been battery life of the mobile device. Where cell phones routinely deliver several hours of talk time and dozens of hours of standby operation on a single charge, early Wi-Fi voice devices provided a fraction of that. The problem is that power conservation was not one of the primary goals in the original Wi-Fi standards that were geared for devices like laptops that could include large, bulky batteries.

The original Wi-Fi standards did include a Power Save feature, but it was not particularly effective and introduced considerable latency for voice transmissions. A far more effective power saving feature is included with the Wi-Fi Multimedia (WMM) QoS standard. Designated WMM-Automatic Power Save Delivery (APSD), this feature allows for far more efficient power conservation along with reduced latency for voice. For example, the Session Initiation Protocol (SIP), the emerging standard for VoIP signaling, involves considerable "chatter" between the end devices and the telephony server. By monitoring that traffic the access point can determine if it really needs to be forwarded over the radio link. As those advanced features are not yet defined in the standards, the handsets and infrastructure elements must come from the same vendor in order to implement them.

### Wi-Fi voice security

Security is always an issue with telephone calls, and it was certainly a concern with early WLAN voice networks given the security deficiencies of the Wireless Equivalent Privacy (WEP) security mechanisms. Fortunately those issues have now been addressed, and it is possible to provide security as sound as that typically found in public cellular networks.

There are two major areas to consider when addressing security: device authentication and privacy. If the authentication system is compromised, unauthorized devices could make and receive calls over the network. That could expose the network to toll fraud or theft of service (i.e., paying for a hacker's phone calls), call redirection and potentially registration hijacking where an attacker is able to impersonate a legitimate party. If the privacy mechanisms were compromised, unauthorized parties would have the ability to eavesdrop on WLAN phone calls.

Today Wi-Fi voice devices typically use authentication mechanisms based on the IEEE 802.1x Extensible Authentication Protocol (EAP). The most secure WLAN voice solutions utilize client certificates, making such an attack virtually impossible. With a client certificate that is bound to the device's MAC address, the Transport Layer Security (TLS) protocol can forward the device's unique credentials in a secure, tunneled connection all the way from the mobile device to the authentication server.

Eavesdropping on WLAN voice conversations is a potential concern, but only if the encryption is based on the early Wired Equivalent Privacy (WEP). Most Wi-Fi voice devices today support 802.11i, what the Wi-Fi Alliance terms Wi-Fi Protected Access-2 (WPA2) Certified. WPA2 uses encryption based on the Advanced Encryption standard, the new encryption standard for the US government under Federal Information Processing Standard 197 (FIPS 197). In enterprise environments with 802.1x authentication, the authentication process produces the encryption key and the solution has no known flaws.

If WPA2 is not an available option, the Wi-Fi Alliance's earlier WPA (Wi-Fi Protected Access) solution can be used. WPA uses the same encryption algorithm as WEP, but a longer key is used and the key is changed on every packet, effectively thwarting the type of brute force attacks that rendered WEP ineffective. When used with 802.1x for authentication and key generation, what the Wi-Fi Alliance calls WPA Enterprise, there are no known flaws.

While authentication and privacy are the major concerns regarding user devices, wireless security must also address the vulnerability of the network itself. Users could connect unauthorized or "rogue" access points, weakening the security perimeter,

and attackers may also use them as part of a strategy to learn valid user names and passwords they could use to access the network. Locating and disabling those access points in a timely fashion will be critical in maintaining the security of the network. The WLAN security system should include the ability to continuously monitor the RF environment to discover those security threats. When a rogue access point is located, the system should alert the network managers, disable the unauthorized device and provide location information so that it can be found and removed.

## WLAN voice network capacity

Probably the most difficult issue to quantify in a WLAN voice deployment is the number of simultaneous calls an access point will be able to support without degrading the voice quality or noticeably increasing the transit delay. There are a number of factors that contribute to the complexity of this problem, starting with the fact that the amount of capacity required per call can be reduced through use of voice compression. The ITU's G.729A compression algorithm for example can reduce the voice payload from 64 Kbps to 8 Kbps. It is important to note that even though the voice payload is reduced by a factor of eight, the overhead associated with WLAN voice will not accommodate an equivalent number of additional voice calls.

Another factor that makes it difficult to specify the maximum number of calls the WLAN can support is the fact that different users may be operating at different data rates. The lower rate users will take proportionally longer to send their voice frames, tying up the network for longer intervals and causing other users to defer their transmissions. Assuming a 50% maximum throughput on the network, the approximate maximum number of simultaneous calls for different voice coding systems and average transmission rates is listed in Table 3.

Approximate Maximum Calls Per WLAN (20 msec Voice Sampling, No Voice Activity Detection)								
	802.11b Network				802.11a or g Network			
Codec	11 Mbps	5.5 Mbps	2 Mbps	1 Mbps	54 Mbps	36 Mbps	18 Mbps	6 Mbps
<b>G.711 (64 Kbps)</b>	12	8	4	2	39	35	25	12
<b>.729A (8 Kbps)</b>	15	12	7	4	46	43	37	22
<b>.723.1 (5.3 Kbps)</b>	22	18	10	6	69	64	55	33

Table 3

A third element that could impact the voice call capacity is voice activity detection (VAD), the option of having voice packets sent only when the party is actually speaking. Given the difficulty of coordinating that function with a wired PBX, most WLAN voice systems do not use VAD today. The exception to that would be push-to-talk systems, where voice packets are generated only when the transmit key is depressed.

Push-to-talk presents a different set of capacity concerns. Used in a growing number of work environments, push-to-talk (PTT) over the wireless LAN can provide a more cost-effective alternative to traditional walkie-talkies. As a PTT system generates WLAN traffic only when the transmit key is depressed, it should be inherently more efficient than traditional voice services that generate frames continuously. However, in a poorly designed PTT solution, those PTT packets are broadcast through every access point, thereby creating unnecessary WLAN traffic throughout the entire network. An efficient PTT system should be able to track users within the network and transmit their frames only on the WLAN where they are actually located.

One last factor that comes into play if a shared voice/data network is deployed is the amount of capacity to reserve for voice users. This is particularly important when 802.11e/WMM QoS is implemented. As the QoS capability gives voice users preferred access to the channel, if too many voice calls are in progress, the data users could be squeezed out entirely. So in a shared voice/data WLAN, you must reduce the number of voice calls an access point will accept to help ensure there will be capacity available for data users.

Call admission control (CAC) is the parameter that defines the maximum number of simultaneous calls supported on each access point; that parameter must be set in the access point or the central network controller. Some systems now have the ability to override the setting in the event that a user who is involved in a call roams into the area. In that case, a user who is involved in a call might be allowed to roam in even though that would technically push the number of calls over the defined parameter, while a new call request in that area would be denied.

Given the dynamic nature of voice usage and the relatively limited number of channels an access point will be able to support, users will be well advised to pilot test their planned configurations before progressing to a full scale roll out. Further, a comprehensive network management system that will monitor voice usage, identify problem areas and help plan for growth and expansion will be critical to ensure that the network can continue to provide enterprise-grade service as the number of users and the traffic volume grows.

## Network planning, traffic monitoring and network management

Providing WLAN voice is not simply a matter of picking some handsets, ensuring that they adhere to a checklist of standards and passing them out. The primary responsibility of the IT department is to deploy a solution that will provide the basic service, support the required features and have the tools that are necessary to maintain and operate the network. Those functions will be critical issues in selecting the equipment needed to implement the solution.

Earlier we introduced the computerized tools available to help design a voice-capable wireless LAN. However, those tools can only help determine how to select and configure the equipment needed to provide the desired amount of wireless network capacity. The real design involves determining how many users you will have, how much capacity their calling volume will require and where they will be when they need to make or receive a call. Common sense can provide some of that planning information. For example, if you have 200 people with WLAN handsets in an auditorium, you can anticipate a torrent of voice calls as soon as the meeting adjourns.

Much of the necessary information for determining WLAN voice capacity requirements can only be gleaned from monitoring the actual network utilization. That is where network management systems become critical. Network management involves all of the systems required to help ensure delivery of a reliable and cost-effective service on an ongoing basis. The key element in that definition is "an ongoing basis."

The first step in providing good WLAN voice service will be the ability to confirm that users can get a usable signal to make and receive a call wherever they move within the facility. Once the signal is provided, it will be necessary to ensure that there is enough network capacity in that area to support the required volume of calls. That will require some amount of coverage overlap among adjacent access points. In short, some important assumptions will be made in the design of our coverage plan, and if guessed incorrectly, some users will be getting busy signals.

Unpredictability is a given in mobile network design, so network management systems that allow us to recognize and adjust to changing conditions are a necessity. Further procedures will be needed to deal with lost, stolen or broken handsets; terminated employees; handset software upgrades; equipment failures; areas with poor signal coverage and all of the day-to-day issues that go into providing a communication service.

In planning a voice over WLAN solution, you should be considering the network management and support systems concurrently with the network design. The biggest mistake that is made in network management is trying to add network management after the network has been installed. It is absolutely essential that network management be considered as a critical factor in the overall network design.

Here are some of the major areas that should be investigated:

**RF Mapping.** Once the network is installed, the network managers should conduct an RF survey that records the signal strength and maps the coverage area of each access point. That type of survey can confirm that the initial design is sound and is an invaluable tool in troubleshooting coverage problems that crop up later.

**Traffic Monitoring.** A mechanism will be needed to determine if there is sufficient network capacity to accommodate normal and peak usage in all areas. Key to that will be the ability to identify the average and maximum number of users per access point, the periods of heaviest activity and the number of call requests that are being denied. If voice and data are supported on the same network, it will also be necessary to gauge the impact of heavy voice traffic on data users.

**Call Quality.** The network might allow a user to make or receive a call but then does not have the ability to maintain the voice quality. VoIP quality assessment tools are become a standard addition to IP PBX systems, however, the use of a wireless LAN adds additional complexity to the problem. The contention-based nature of wireless LANs will typically increase transit delay and jitter, and can potentially cause packet loss if the delay exceeds the jitter buffer's ability to compensate. Further, those parameters can vary widely during the call, particularly if the call is handed off access point to access point. You will need a tool that tracks the performance throughout the call and is able to identify the access point being used during each portion of the call.

**Identifying/Rectifying Coverage Problems.**

Troubleshooting is inherently difficult in a wireless network, as you cannot "see" the radio signal. Anyone can spot a broken wire, but how do you determine why there is a good signal in one area but not another, particularly when they are both the same distance from the access point? Given the vagaries of indoor radio propagation, there can be vastly different signal readings at points just a few feet apart! Training the Help Desk personnel to get accurate location information from wireless users will be the first step, but many of these problems require dispatching a technician with a test device to the area in an attempt to replicate the problem. When all is said and done, it could just be that the user's handset is faulty!

**Security.** While WPA, WPA2 and 802.1x have addressed the privacy and authentication concerns in a wireless LAN, there are other security exposures that will need to be monitored. As noted earlier, users or contractors working in the facility may install unsecured rogue access points on wired network connections, creating unwanted security exposures. Attackers may attempt to set up access points in close proximity to the network in hopes of getting client devices to associate with them so they can steal valid user credentials (i.e., user names and passwords). Also radio jammers or leaky microwave ovens can cause directed or accidental denial of service attacks on the wireless infrastructure. The infrastructure must include mechanisms to detect, disable and locate these security vulnerabilities quickly.

**Record Keeping.** You will also have to modify your ordering and record keeping systems to track your new class of mobile devices and define whether they will be assigned to individual users or shared by several people within one department.

Good-quality voice service requires the ability to recognize problems before the user calls to complain. As these features are not defined in the standards, it is important to look at what capabilities are provided in the WLAN switch and the handsets to determine what additional tools and procedures will be needed to help ensure an adequate service level.

## Conclusion

Mobile voice communications over a WLAN can help organizations increase productivity, enhance collaboration and, ultimately, improve customer service by making workers instantly accessible wherever they are in the enterprise. Enabling these enterprise-quality mobile voice services requires a sound and reliable wireless infrastructure. That infrastructure is the result of good planning, quality tools and a set of systems that will allow the network manager to ensure that the network is maintained to the highest standards. Tools and expertise are available today that will provide a wireless LAN voice capability that delivers the quality and reliability business users expect. With the right tools and a good design plan, IT departments can deliver a functional and cost-effective mobile voice solution on their WLAN infrastructure.



Glossary of Acronyms			
<b>AC</b>	Access Category	<b>PRI</b>	Primary Rate Interface
<b>ACK</b>	Acknowledgement	<b>QoS</b>	Quality of Service
<b>AIFS</b>	Arbitrated Inter-Frame Spacing	<b>SIFS</b>	Short Inter-Frame Spacing
<b>CAC</b>	Call Admission Control	<b>SSID</b>	System Services Identifier
<b>CSMA/CA</b>	Carrier Sense Multiple Access with Collision Avoidance	<b>VLAN</b>	Virtual LAN
<b>CW</b>	Contention Window	<b>VoIP</b>	Voice over Internet Protocol/Voice over IP
<b>DCF</b>	Distributed Control Function	<b>VoWLAN</b>	Voice over Wireless LAN
<b>DIFS</b>	DCF Inter-Frame Spacing	<b>WEP</b>	Wired Equivalent Privacy
<b>DSSS</b>	Direct Sequence Spread Spectrum	<b>WLAN</b>	Wireless LAN
<b>EDCA</b>	Enhanced Distributed Control Access	<b>Wi-Fi</b>	Wireless Fidelity
<b>IT</b>	Information Technology	<b>WMM</b>	Wi-Fi Multi-Media
<b>HCCA</b>	Hybrid Controlled Channel Access	<b>WMM-APSD</b>	Wi-Fi Multi-Media-Automatic Power Save Delivery
<b>LAN</b>	Local Area Network	<b>WPA</b>	Wi-Fi Protected Access
<b>OFDM</b>	Orthogonal Frequency Division Multiplexing	<b>WPA2</b>	Wi-Fi Protected Access 2 (i.e. 802.11i Compliance)
<b>PoE</b>	Power over Ethernet	<b>WVLAN</b>	Wireless Virtual LAN





**MOTOROLA**

[motorola.com](http://motorola.com)

Part number WP-PYWLAN. Printed in USA 04/09. MOTOROLA and the Stylized M Logo and Symbol and the Symbol Logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners. ©Motorola, Inc. 2009. All rights reserved. For system, product or services availability and specific information within your country, please contact your local Motorola office or Business Partner. Specifications are subject to change without notice.