AVAYA

IP Telephony

Contact Centers

Mobility

Services

WHITE PAPER

Preparing the WLAN for Voice

May 2005

Table of Contents

Executive Summary

Companies have deployed IEEE 802.11 Wireless Local Area Network (WLAN) technology to provide employees with un-tethered access to network resources and increase productivity and mobility. These wireless networks are often dedicated for data applications such as web browsing and E-mail. Enterprises are increasingly integrating IP telephony and 802.11 wireless networking to enable Voice over WLAN (VoWLAN) as the technology matures and standards evolve.

Combining voice with wireless data networking introduces some challenges due to the network requirements imposed by voice communications. Voice is a real-time application that requires low latency and reliable delivery as it travels through the network. In converged voice and data networks, Quality of Service (QoS) mechanisms are imperative to achieving quality voice communication. This white paper reviews both proprietary and standard QoS protocols. Related to QoS is battery life, which also plays a role in the quality of voice communications. Stronger, bigger batteries provide increased radio range and longer talk time.

Wireless devices should support appropriate security features to protect interior networks from outsiders. The rapid proliferation of 802.11 has made the wireless LAN an attractive and often easy target for hackers. The possibility that an unauthorized network user is able to gain access to the enterprise network resources and data should not be underestimated. This white paper covers the weaknesses and strengths of various 802.11 security mechanisms available.

Maximizing end-user mobility is a desired characteristic for VoWLAN solutions. In order to achieve it, end users must be able to roam around a building without losing network connectivity. Wireless networks can accommodate this by allowing end-user wireless devices to roam seamlessly between access points using IEEE 802.11 standards. Tightly coupled to the degree of mobility provided to users is the amount of wireless coverage available within a building. Coverage and capacity for wireless mobility are discussed as it relates to 802.11 radio standards and secure fast roaming.

Finally, this technical white paper discusses important VoWLAN design considerations, including all the issues outlined above, and gives recommendations for features, which support wireless voice communications. This white paper is intended for IT professionals considering a VoWLAN solution who require a better understanding of the key features necessary to achieve quality voice communications using the 802.11 standards.

Introduction

Companies that have adopted both IP telephony and 802.11 wireless networking are now taking the next logical step – providing IP telephony over 802.11 wireless networks.

Voice over WLAN (VoWLAN) services are provided through the use of handheld wireless-fidelity (Wi-Fi) telephones and devices in a converged network. The term *converged* indicates that a single network is providing connectivity for both voice and data applications concurrently. Each end-user device, whether it is a PDA, laptop computer, or Wi-Fi telephone communicates over the air with an access point device using the 802.11a, b or g radio standard as shown in **Figure 1**. The basic attributes of each radio type, including operating frequency, available bandwidth and the number of supported non-overlapping channels per access point, are listed in **Table 1**. The access point provides connectivity back to the existing wired network using an Ethernet connection. This connection serves as a demarcation point between wireless and wired networks, and allows internetworking between access points.

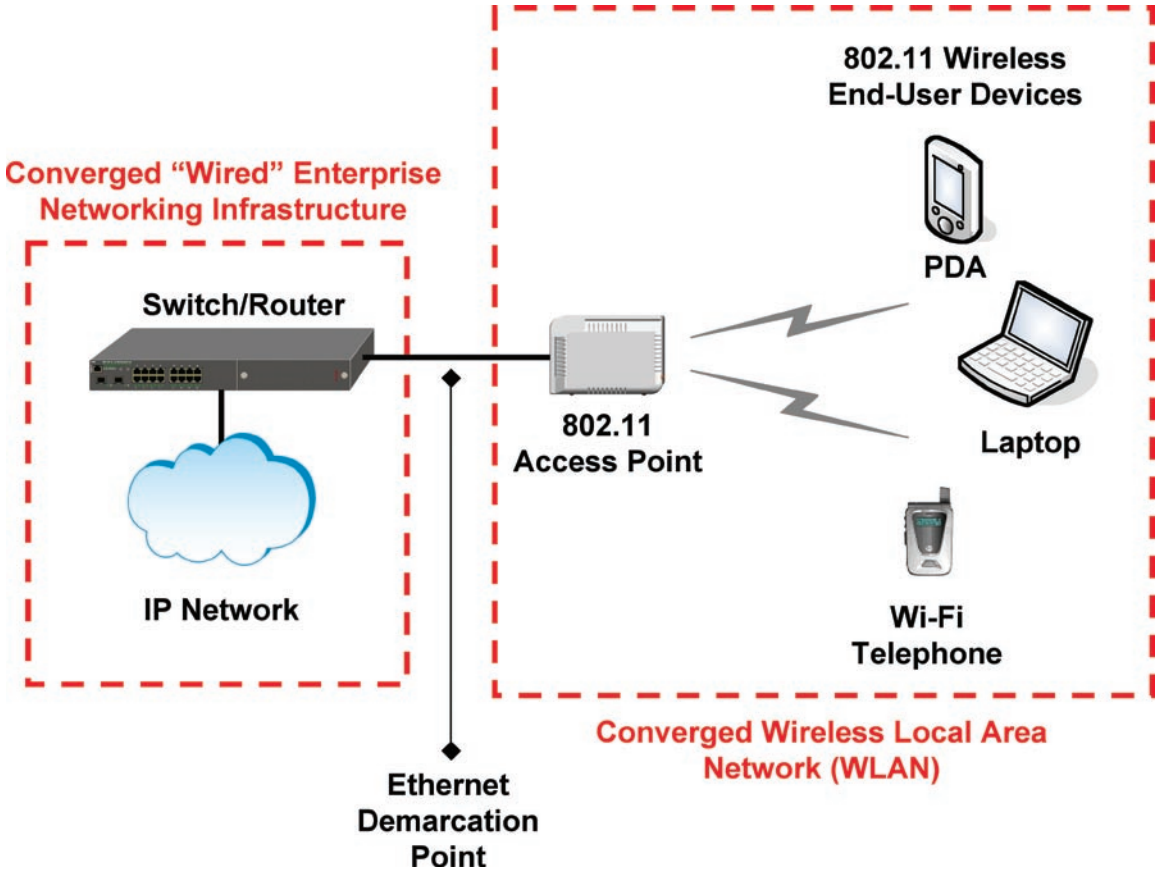

Figure 1. Converged Wireless Local Area Network (WLAN) Components

Table 1. Basic 802.11 Physical Layer Parameters

	IEEE Standards		
	802.11a	802.11b	802.11g
Radio Spectrum	5 GHz	2.4 GHz	2.4 GHZ
Throughput	54 Mbps	11 Mbps	54 Mbps
Non-Overlapping Channels	8-12	3	3

Providing wireless connectivity for data applications is relatively straightforward and proven, while wireless connectivity for voice applications is more complex and requires additional planning and consideration. Bandwidth contention, security and wireless mobility are the primary factors to consider when implementing VoWLAN. These issues are described below:

Bandwidth Contention – The original IEEE 802.11 media access standard relies on Distributed Coordination Function (DCF) to transmit packets over the air between the end-user devices and the access points. The standard uses a technique known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) in order to "listen before sending" information over the air. As the number of end-user devices within communication range of one another increases so does contention for the bandwidth. When two or more end-users attempt to transmit at the same time a collision occurs. In order to avoid collisions, each

end-user device must wait a period of random duration, known as the random backoff interval. The backoff is a timer that is reduced only while the medium is idle. The end-user devices must then listen to see if the medium ("air") is idle before attempting to transmit again. If a collision occurs the backoff time is increased on the endpoints. As a result, excessive collisions can introduce delay and packet loss in networks supporting many applications and users, which can impair audio quality and drop calls. This is further exacerbated in converged networks where voice and data applications contend for the same bandwidth, because CSMA/CA treats all applications with equal priority.

Security – Wireless networks have become an easy target for hackers. Access point coverage areas often exceed the physical perimeters of buildings, which make the network inside vulnerable to attacks from the outside. Hackers have adopted a popular cracking technique known as "war driving" to survey, map and later exploit exposed networks. The hacker simply drives around with a wireless-enabled notebook computer running a snooping utility like AirSnort to probe homes and businesses for potential targets. Unauthorized network access may introduce risks such as Denial of Service (DoS) attacks, eavesdropping, and theft of data or telephony resources. To protect against such security threats, WLANs need to authenticate users before providing network access and use encryption to protect data.

Wireless Mobility – Voice over WLAN (VoWLAN) users need to be able to reliably roam throughout a building while on an active call. As the user roams, the access point must be able to seamlessly hand off the end-user device to another access point without degrading voice quality or dropping the call. Sufficient wireless coverage is also required in order to maximize wireless mobility.

Avaya wireless solutions provide QoS, security, and roaming features that address these VoWLAN issues. These features are discussed in more detail throughout this technical white paper.

Quality of Service

Voice and data traffic flows have different network requirements. Most data applications can withstand some network packet loss because the Transmission Control Protocol (TCP) can retransmit "lost packets" to ensure reliable delivery. Retransmissions introduce delay, which is perceptible in real time communications such as voice, breaking the flow of a voice conversation and making it difficult for people to understand what is being said. Therefore, voice communications over Internet Protocol (IP) must be forwarded with minimal delay, minimal packet loss and minimal "jitter" (i.e., variation in delay). Quality of Service (QoS) mechanisms and features are necessary to achieve these service levels in 802.11 environments.

Proprietary Implementations

Prior to standards, equipment providers implemented proprietary QoS mechanisms for supporting VoWLAN. A popular proprietary QoS mechanism is Spectralink Voice Priority (SVP), which is supported by Avaya and other vendors. SVP minimizes (eliminates) the collision backoff interval for voice packets so that they are always transmitted first, while data packets must back off during periods of congestion. Such proprietary features can limit product selection and inhibit multi-vendor wireless environments.

Standard Implementations

The Institute for Electrical and Electronic Engineers (IEEE) is currently ratifying a QoS standard known as 802.11e to promote multi-vendor interoperability, allowing companies to select "best of breed" products from different vendors. Wi-Fi Multimedia (WMM) will eventually support two modes of operation known as

Enhanced Distributed Coordination Function (EDCF), commonly referred to as WMM, and Hybrid Coordination Function (HCF), commonly referred to as WMM Scheduled Access.

WMM

The WMM portion of the standard is currently available and being supported by wireless equipment manufacturers including Avaya. WMM is based on a subset of the IEEE 802.11e draft standard. It allows 802.11 access points and clients to distinguish amongst different applications, contending for the same bandwidth, and treat the delivery of each application uniquely, based on certain traffic characteristics. Some manufacturers have already begun to adopt capabilities from the upcoming WMM 802.11e standard so that their products will be compatible with the standard once it is ratified.

WMM defines four access categories: voice, video, best effort and background. These access categories are described in **Table 2** below. An advantage of WMM is its backward compatibility with 802.1D, predominantly used by QoS aware Layer 2 switches. The two standards, WMM and 802.1D priority levels, map together forming a seamless QoS policy transition when going between wired Ethernet and 802.11 wireless networks.

Table 2. Wi-Fi Multimedia (WMM) Access Categories

Designation	Access Category	Description	802.1D Tag	802.1D Designation
Voice	AC_VO	Highest priority category designed to allow multiple concurrent VoIP calls. Provides voice packets with low latency forwarding in order to achieve toll quality communications.	7	NC
			6	VO
Video	AC_VI	Allows video to be transported with priority above data applications, but slightly below voice communications.	5	VI
			4	CL
			3	EE
Best Effort	AC_BE	Designed for transporting traffic from applications that lack QoS capabilities. Average enterprise user traffic, such as web browsing would fall under this category, because it is less sensitive to latency, but long delays could become unacceptable.	0	BE
Background	AC_BK	Lowest priority category, designed to deliver traffic that is not sensitive to delay or throughput. Examples would include file downloads and print jobs.	2	-
			1	BK

As application traffic destined for the air arrives at a WMM enabled end-user device or access point, it is first classified into one of the four access categories and moved into the appropriate forwarding queue. If an end-user device is supporting several applications, which all attempt to transmit at the same time an internal collision occurs amongst them. When this happens the device queuing logic must resolve the collision internally. WMM internal queuing logic is illustrated in **Figure 2**.

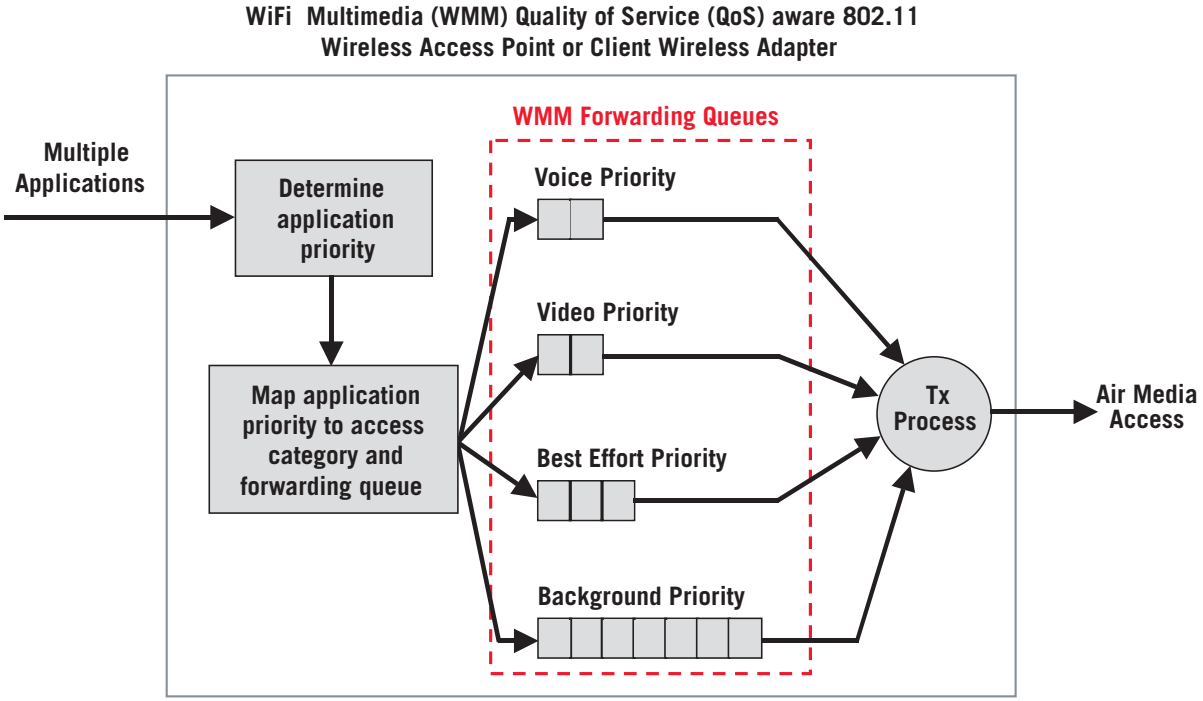

Figure 2. Queue Logic for WMM Access Categories

Once an end-user device or access point has a transmit opportunity, data is selectively transmitted using a set of unique media access parameters, according to the applications access category. Different levels of service are provided by differentiating the arbitration inter-frame space (AIFS), contention window (CW) size and transmit opportunity (TXOP) limits of the traffic flows from each access category.

Arbitration Inter-frame Space (AIFS) – The AIFS interval specifies the time interval between medium-idle and the start of media access negotiations. Each access category is assigned a different AIFS value. Higher priority access category traffic receives a shorter AIFS value. Lower priority access category traffic receives a longer AIFS value. The result is a favorable TXOP for higher priority traffic.

Contention Window (CW) Size – The dynamic backoff intervals for legacy DCF implementations are fixed for all end-user devices and applications. In contrast, the CW backoff interval for EDCF (WMM) is a function of the access category. Higher priority access categories are given a shorter/smaller CW range to select from. This corresponds to fewer backoff slots being traversed per transmission, on average.

Transmit Opportunity (TXOP) Limit – The TXOP limit specifies the duration that an end-user device can transmit for a given access category. The TXOP limit can be used to give higher priority traffic longer access to the medium and lower priority traffic is given shorter access.

WMM is designed to deal with mixed traffic environments. In certain instances, where there is only voice traffic being transported over the wireless LAN, legacy/proprietary standards may be more appropriate.

WMM Scheduled Access

WMM Scheduled access is a bandwidth reservation QoS mechanism designed to ensure that subscribing applications are provided a pre-negotiated percentage of bandwidth for a given communication flow. Its mode of operation differs from pure WMM, which is contention based. Instead, scheduled access uses a poll-based mechanism, whereby clients are polled by the access points and given an opportunity to request a predefined amount of bandwidth. A centralized bandwidth reservation process can either accept or refuse the connection based on available bandwidth. Scheduled access is a desirable and optimal feature for constant bit rate applications, like Voice over IP (VoIP) because of its predictability and scalability in high capacity environments. Today, WMM with scheduled access lacks Operating System (OS) and application support. As the technology supporting scheduled access matures, more VoWLAN solutions will support this capability for providing network level admission control.

Call Admission Control (CAC)

There are other issues that can adversely affect voice quality – chief among these is when too many equal priority users contend for the same access point bandwidth. This condition is referred to as oversubscription. Bandwidth *oversubscription* occurs whenever N+1 users are attempting to transmit voice, data or both, but there is only enough bandwidth to support N users. An example of bandwidth oversubscription occurring with VoWLAN users is illustrated in **Figure 3**. When oversubscription occurs it introduces excessive collisions and packet loss, which can degrade audio quality for all voice transmissions associated with the overloaded access point. Radio load balancing can mitigate this, but it cannot completely eliminate the problem if there is no other access point within load sharing proximity.

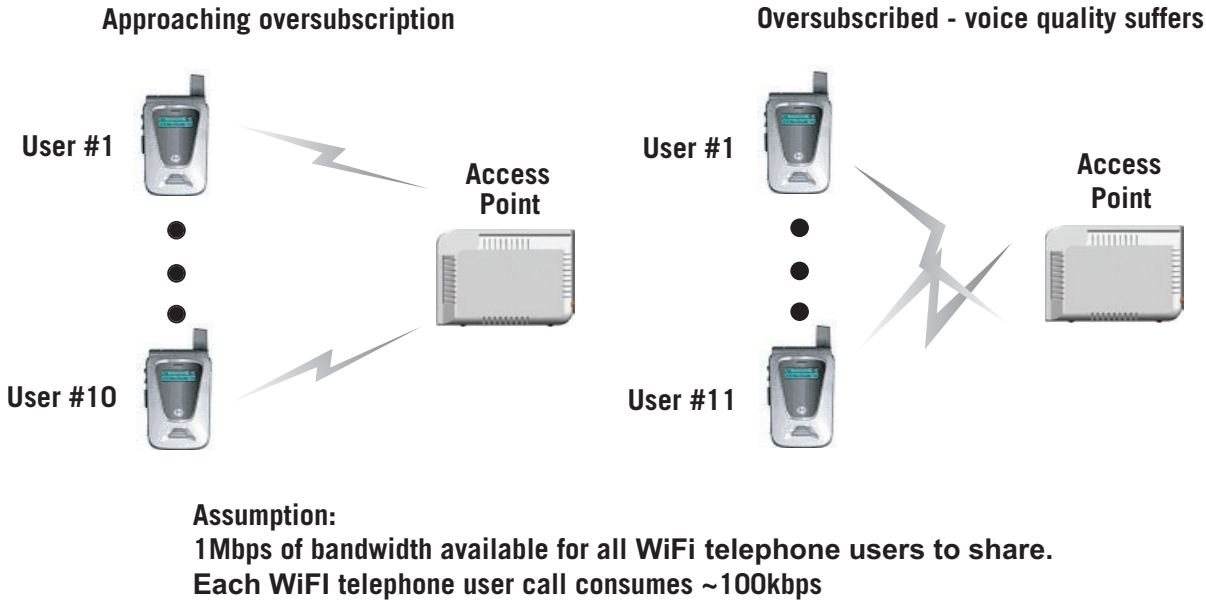

Figure 3. VoIP Bandwidth Oversubscription "The N+1 Problem"

Over the Air Call Admission Control can be used to restrict new telephone calls once a user threshold or bandwidth capacity has been reached. In converged networks, this would require that all devices, including laptops, Wi-Fi telephones and handheld PCs share a common QoS mechanism that can schedule and deny voice or data users according to predefined policies. WMM scheduled access provides this capability at the network level through the use of admission control, based on Traffic Specifications (TSPECs).

WMM would have to be augmented with a separate Admission Control certification to achieve the same capability. Then, if a Wi-Fi telephone device attempts to place a call with an access point and it fails because network resources are not available, the telephone can block the call locally and give the user the appropriate denial notification. Admission control and associated policies can also be used to prevent high priority applications from monopolizing the network and starving other data applications of bandwidth.

Battery Life

One of the more important characteristics to consider for any VoWLAN solution is talk time and standby time. Talk time is the amount of time that an end-user can carry on a conversation before battery power runs out. Standby time is the amount of time that an end-user device can remain idle before battery power runs out. Since distances between end-user devices and access point radios vary constantly, power management needs to be able to compensate and reserve the necessary energy to satisfy power output requirements. Avaya wireless solutions take a holistic approach to battery life, both by supporting network-based industry standard methods of power management and by providing the necessary battery capacity to meet customer needs.

The newer mechanisms used to extend the battery life of 802.11 wireless end-user devices fall under the QoS standard umbrella. Automatic Power-Save Delivery (APSD) is a new 802.11e enhancement, which allows battery life to be extended by turning off end-user device radios when they are not actively communicating with other devices. There is a scheduled and unscheduled flavor of APSD. The unscheduled form of APSD will become available first and the scheduled form of APSD second. Similar to WMM with scheduled access, the scheduled form of APSD is desirable for constant bit rate applications, like VoIP, because of its predictable nature.

Avaya has introduced more efficient ways to do APSD into the 802.11e standard. It enables unscheduled APSD to be used by multimedia devices receiving different types of traffic streams, both constant and variable bit rate. Avaya's scheduled APSD approach employs time offsets, which are optimally determined by the access point. During sleep time the end-user device radio is disabled and the access point buffers any frames that are destined for the device.

Dedicated voice application devices, like Wi-Fi telephones, should be designed with components that take power saving into account. Each component must work individually and collectively to minimize power consumption at all times. For example, both the voice processing and radio components can be put into sleep mode while a Wi-Fi telephone is on-hook. When a user goes off-hook to place a call, the voice-processing component can remain asleep, while the radio is energized, until it is needed for voice processing. Once on the call, the voice processing and radio components are active. In the meantime, other components in the telephone, such as the LCD display, can be separately powered down after a period of inactivity to further conserve power. Similar operations should also be performed in the call receive direction.

Access points can also make use of wired networking mechanisms, like proxy ARP to extend battery life, in addition to the 802.11 standards. Instead of having the end-user devices respond to Layer 2 broadcast messages periodically over the air, a proxy built into the access point or external controller can respond in place of the end-user device. This offloads the end-user device from continuously and perhaps excessively transmitting in response to broadcast messages, like ARP requests.

Security

Wireless security must be implemented as part of a company's overall security policy. A layered security design approach consisting of both authentication and privacy phases is recommended for protecting voice and data communication over the air.

Authentication – Provides LAN access control through the use of an authentication mechanism. This allows the network to distinguish authorized user-devices from unauthorized user-devices.

Privacy – Provides data privacy by using encryption algorithms to make traffic appear pseudo-random in nature. This mitigates the probability of successful eavesdropping and interception of voice and data communication from the air.

VoWLAN solutions must balance voice quality and security. Authentication and privacy measures must satisfy network security requirements with minimal processing delay and fast roaming support. Recall that roaming is the ability of the network to seamlessly hand off a user-device from one access point to another. If the solution relies on an authentication process that takes a long time to authenticate and re-authenticate users, it will prove to be unsuitable for voice. Also, solutions based on encryption standards without properly optimized hardware can introduce delay, adversely impacting audio quality.

MAC Based Authentication

Media Access Control (MAC) address based authentication allows a list of permitted MAC addresses to be defined in an access point. End-user devices with unknown MAC addresses are denied and known MAC addresses are granted network access. The unidirectional nature of MAC based authentication, address spoofing and the possibility of physical device theft render this technique ineffective. Avaya wireless infrastructure solutions continue to evolve with and support new security standards as they become available. MAC based authentication continues to be supported, but it should only be used for providing security to legacy devices if and when necessary.

IEEE 802.1X Authentication

802.1X provides access control at the point where a user joins the network. In 802.11, this occurs over the wireless link between the end-user device and the access point. The 802.1X standard offers significant improvements over MAC based authentication. It uses the Extensible Authentication Protocol (EAP) transport mechanism, which allows 802.1X to support several different authentication methods and credentials. 802.1X authentication allows the possibility for both client-to-access point and access point-to-client authentication, minimizing rogue access point threats. It also allows dynamic key generation and depending on the EAP method, can support fast reconnections allowing for faster roaming. Some of the key differences between the more common 802.1X EAP methods are defined in **Table 3**.

Table 3. Popular 802.1X EAP Authentication Methods

EAP Methods	Certificate Usage	Authentication Direction	Dynamic Key Support	Fast Reconnect Support	Strength Comparison
TLS	Client/Server	Two way	Yes	Yes	Strongest
TTLS	Server only	Two way	Yes	Yes	Strong
PEAP	Server only	Two way	Yes	Yes	Strong

Transport Layer Security (EAP-TLS) requires certificates on both the RADIUS server and the end-user device; making it very secure, but complex at the same time. Tunneled Transport Layer Security (EAP-TTLS) allows passwords to be used on the client instead of relying on a certificate. The only downside is a lack of free client support. EAP-TTLS users must pay for a matching client from the RADIUS or Authentication server vendor (e.g. Funk Odyssey client). Protected Extensible Authentication Protocol (EAP-PEAP) does not require client certificates, making it simpler to deploy, and the client package is available for free from Microsoft.

There are other EAP methods available that are not covered in **Table 3** because they are not widely deployed. Avaya recommends and supports only the most common EAP methods for securing voice and data communications. This allows Avaya products to work with other third party products that comply with the standards, giving enterprise customers maximum flexibility for selecting interoperable components from different vendors that best meet their communications needs.

TKIP and AES Encryption

Once static Wired Equivalent Privacy (WEP) vulnerabilities were exposed, 802.11 users needed an alternative solution to improve security strength. The Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) standards were designed to replace WEP. Both offer significant improvements over static and dynamic WEP solutions.

TKIP encryption was introduced with the release of Wi-Fi Protected Access Version 1.0, known simply as WPA. It uses the same RC4 encryption method as WEP, but it has been improved through the use of a longer initialization vector, making the number of combinations larger and more difficult to crack. It also uses per-packet key rotation, meaning that keys are rotated more often, which minimizes the algorithms susceptibility to key replay attacks. Finally, TKIP uses a Message Integrity Check (MIC), which ensures that the data has not been modified during transport. TKIP has a major advantage because of its RC4 algorithm foundation. Older access points and end-user devices were optimized to support RC4 for WEP. Since TKIP is based on the same encryption algorithm, it is possible to TKIP-enable older devices through firmware updates. This gives enterprises an attractive, strong security migration strategy between WEP and AES.

AES encryption was originally developed as a Federal Information Processing Standard (FIPS) specifying a cryptographic algorithm, which may be used by the U.S. Government to protect sensitive, unclassified information. It is the strongest, commercially available encryption standard for securing IP traffic and it is a key component for WPAv2. The standard uses a symmetrical block cipher that can process data blocks of 128 bits in length using any one of the three available key lengths or “flavors”: AES-128, AES-192 and AES-256. Historically, the AES algorithm was designed to replace the more vulnerable Data Encryption Standard (DES) algorithm, common in Virtual Private Network (VPN) implementations. The only downside of supporting AES encryption is device support. Many legacy end-user devices will require a forklift upgrade/replacement to support AES. IT managers considering various wireless solutions should look for equipment that either currently supports AES or has the processing “horse power” to handle AES through a future firmware update. A comparison of dynamic 802.11 wireless encryption variants is listed in **Table 4**. Avaya recommends the use of dynamic keys for protecting all mission critical enterprise voice and data applications.

Table 4. Comparison of Dynamic 802.11 Wireless Encryption Variants

Encryption Variants	Encryption Method	Key Size	Improvements	Strength Comparison**
WEP	RC4	40, 128-bit	Different keys per user Key material rotation	Weakest
TKIP	RC4	128-bit	Per packet key rotation Longer initialization vector Message Integrity Check (MIC)	Strong
AES-CCMP	AES	128, 192, 256-bit	Highest strength encryption Largest key sizes	Strongest*

* Requires optimized hardware

** Relative to the other variants in this table

Virtual Private Networks

VPN technology is used primarily to provide employees access to enterprise network resources from remote locations. It can also be used to provide supplemental security for 802.11 wireless deployments. This is typically done in scenarios where a weaker encryption mechanism, like WEP, is being used to secure wireless transmissions over the air. A security gateway is placed in between the access point and the wired network infrastructure. Laptop and pocket PC users must first establish a wireless connection using 802.11 security. Once a wireless connection is successfully established, the laptop and pocket PC users must use a VPN client to establish a tunnel with the security gateway in order to access the corporate LAN. This provides protection for data and IP Softphone applications at the network and application layers. VPN tunneling provides a strong authentication and encryption option and it can be made scalable through the use of RADIUS authentication services. For enterprises familiar with VPNs, how they work and how they scale, this may be a desirable capability to extend over WLAN.

Wireless Mobility

WLAN radio coverage requirements for voice and data applications are different. Data centric designs traditionally focus on areas where users tend to congregate such as lobbies, offices and conference rooms. Voice network designs need to cover these same areas, but they must also provide coverage where employees tend to roam like hallways, stairways, and elevators. The range of mobility that a wireless IP telephony end-user exerts, and the required network coverage area, depends greatly on the end-user device type. For example, a laptop computer user equipped with IP Softphone is free to move about, but tends to remain stationary because of the size, shape and weight of the device. The opposite is true for Wi-Fi handheld phone and Pocket PC users because these devices are smaller and lighter, making it far less restrictive to movement. Data centric designs have been able to provide adequate coverage for PC-based IP Softphone solutions, but Wi-Fi handheld users will likely require additional access points for coverage and capacity as well as fast roaming support to handle their rapid movement between access points.

Fast Roaming

As end-users move between access points the 802.11 end-user device must be handed off from one radio to the next. This can be problematic for voice communications, because the act of disassociating with one access point and re-associating with another access point takes time. During this handoff interval, no communications between the end-user device and the network are possible, which can impact delay sensitive voice conversations.

Fast Roaming – The ability of the end-user device to roam between two access points without the end-user or application noticing that a change has occurred.

Fast roaming is imperative for accommodating voice calls over 802.11 wireless networks. The 802.11r task group is chartered with standardizing a mechanism to provide fast roaming support over wireless LANs. There are many challenges facing the fast roaming standard. For one, security needs to be provided to fast roaming end-user devices, but it cannot impact the handoff interval. This is a problem for many authentication and encryption mechanisms, because they rely on keying material that must be established with each new peer. This key negotiation process takes time, which can introduce delay as the end-user moves. A fast secure roaming mechanism needs to be developed, which can minimize the effect of security negotiations for delay sensitive applications like voice.

Avaya wireless solutions, such as the dual-networked 802.11/cellular Seamless Communications Solutions use a proprietary form of fast roaming today, because there is no standard. Avaya plans to implement 802.11r, giving customers maximum design flexibility, once the standard has been ratified.

802.11 Radio Standards

The type of 802.11 standard radio that a wireless IP telephony solution uses must be considered before deployment, because it directly impacts coverage area, call capacity, growth opportunity and Quality of Service (QoS).

The 802.11b and 802.11g standards both operate in the crowded 2.4 GHz spectrum, which overlaps with many common household devices including microwave ovens and cordless telephones. The two standards are limited to three non-overlapping channels, increasing the probability of co-channel interference in dense deployments. 802.11b/g channel reuse is depicted in **Figure 4**. 802.11b has a maximum throughput of 11Mbps and 802.11g has a maximum throughput of 54Mbps. The 802.11b radio standard has proven itself to be fairly reliable for small, low density, low cost configurations and it supports approximately eight concurrent G.711mu-law calls per access point. The 802.11g standard is backward compatible with 802.11b devices. An 802.11g access point can accept connections from an 802.11b client cards, but all other 802.11g devices must be downgraded to a slower throughput rate in order to support this. In theory, this means that all clients would be downgraded to 11Mbps, but in reality this number can often be as low as 7Mbps for certain configurations. The mixing of b/g radios makes throughput performance for g-based clients unpredictable, therefore, 802.11g is primarily reserved for data applications only.

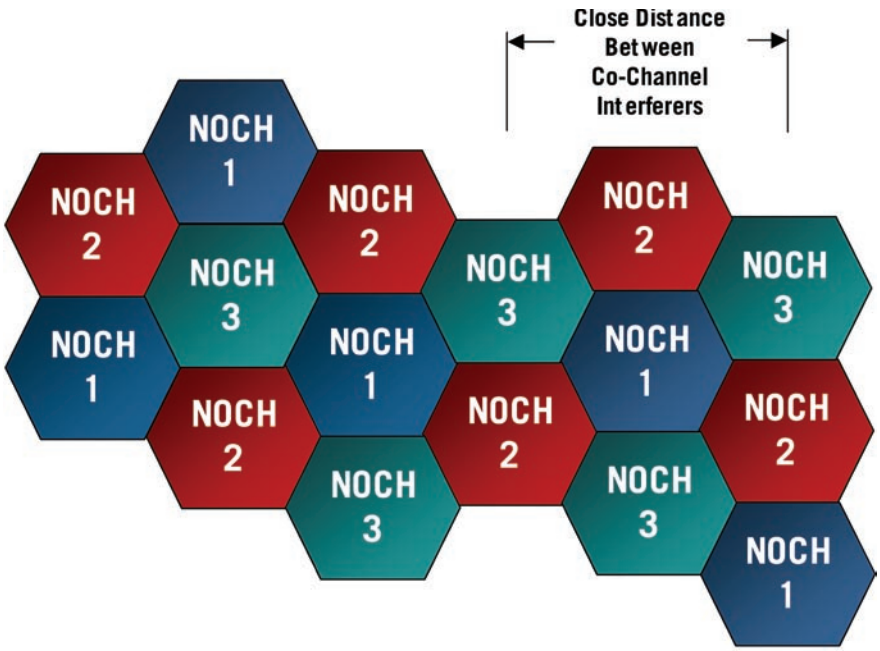

Figure 4. Sample 802.11b/g Non-overlapping Channel Reuse

The 802.11a radio standard is best suited for Voice over WLAN solutions. It operates in the far less crowded 5 GHz spectrum, it also provides a higher 54Mbps throughput, and supports up to twelve non-overlapping channels. The advantage of this is depicted using eight of the non-overlapping channels in **Figure 5**. This gives solutions based on 802.11a radios an advantage for voice because they can support approximately 20 G.711mu-law calls per access point and the access points can be placed closer together, allowing for greater call densities.

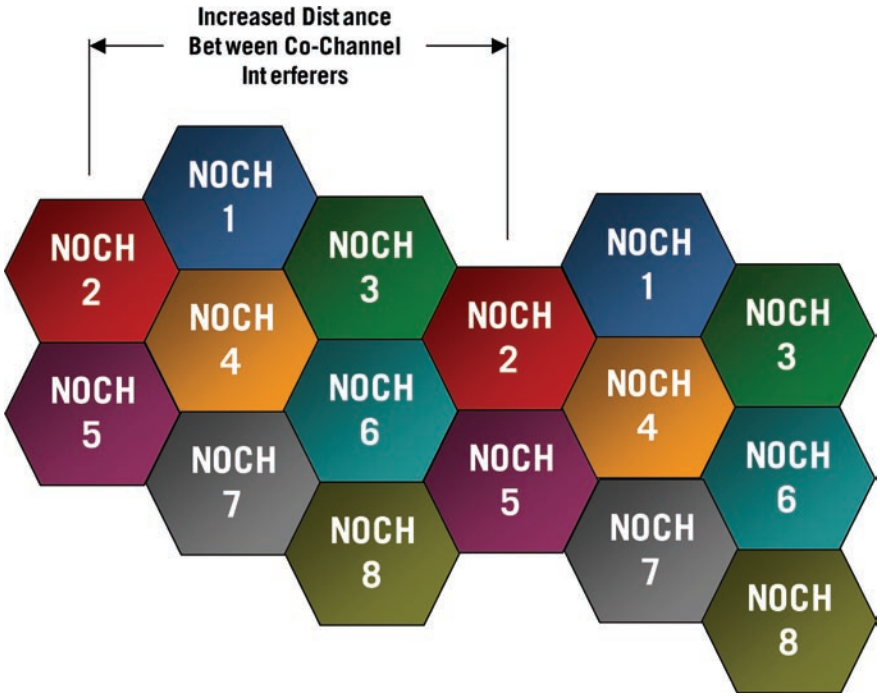

Figure 5. Sample 802.11a Non-overlapping Channel Reuse (only 8 channels)

Higher frequency radios cannot achieve the same range as lower frequency radios at the same output power. Therefore, a larger number of 802.11a radios are needed to provide adequate coverage for the same area compared to their 802.11b/g counterparts. Requiring more access points is a tolerable drawback. The price per access point continues to fall and the ability to support more concurrent calls per access point counters the increased cost in high use configurations where capacity is desperately needed.

Some manufacturers, including Avaya, offer dual-radio access point solutions, allowing the access point to support both 802.11a and b and/or g connectivity simultaneously. This gives the enterprise flexibility to dedicate optimal radios for certain applications (e.g. 802.11a for voice and 802.11g for data). The pros and cons of the three 802.11 radio standard options for wireless IP telephony are listed in **Table 5**.

Table 5. Voice Support Comparison of IEEE 802.11 Radio Standards

IEEE Standard	Pros	Cons	Voice Support Comparison
802.11a	Reduced RF interference Many non-overlapping channels Higher user/call capacity Higher throughput	Higher cost Smaller signal range Dealing with obstructions	Best
802.11b	Reduced cost Larger signal range Deals with obstructions More predicable call capacity	Increased RF interference Fewer non-overlapping channel Lowest user/call capacity Throughput	Good
802.11g	Reduced cost Larger signal range Higher user/call capacity Higher throughput Deals with obstructions	Increased RF interference Few non-overlapping channels Less predictable call capacity	Good

Summary

Voice is not just another data application. Features that address bandwidth contention, security and wireless mobility are necessary for delivering quality voice communications over 802.11 networks. Avaya delivers solutions for wireless telephony and IP telephony infrastructure that enable customers to reliably and securely implement Voice over WLAN services today.

Best of breed solutions from Avaya include access points supporting standard QoS, security and roaming features required by voice applications. Standard features provide customers with maximum design flexibility for deploying multi-vendor solutions. Proprietary solutions inhibit interoperability and limit device selection, but are sometimes necessary for supporting legacy systems. Avaya wireless infrastructure components support both popular proprietary features, like SVP, and industry standard features, like WMM, necessary for delivering quality wireless voice communications. This allows the same infrastructure to support legacy and next generation VoWLAN systems and solutions.

There are many potential pitfalls in designing and deploying an effective VoWLAN solution. The task is nontrivial and may require significant resources and expertise, which the typical enterprise may not have. In those cases, Avaya CSI can supplement the customer's IT resources or even take on the entire project for the customer with design, security assessment, and maintenance services.

For more information on how Avaya can take your enterprise from where it is to where it needs to be, contact your Avaya Client Executive or Authorized Avaya BusinessPartner, or visit us at www.avaya.com

About Avaya

Avaya enables businesses to achieve superior results by designing, building and managing their communications infrastructure and solutions. For over one million businesses worldwide, including more than 90 percent of the FORTUNE 500®, Avaya's embedded solutions help businesses enhance value, improve productivity and create competitive advantage by allowing people to be more productive and create more intelligent processes that satisfy customers.

For businesses large and small, Avaya is a world leader in secure, reliable IP telephony systems, communications applications and full life-cycle services. Driving the convergence of embedded voice and data communications with business applications, Avaya is distinguished by its combination of comprehensive, world-class products and services. Avaya helps customers across the globe leverage existing and new networks to achieve superior business results.

AVAYA

COMMUNICATIONS
AT THE HEART OF BUSINESS

avaya.com

Printed in the U.S.A.
05/05 • EF-LB2731