

Is Your WLAN Ready for Voice?

Critical Capabilities of the Cisco Unified Wireless Network Enabling Voice-over-Wireless-LAN service

Summary

Wireless LANs (WLANs) are rapidly becoming pervasive among enterprises. The increasing availability of wireless voice clients and the recent announcements of dual-mode (wireless and cellular) smartphones, coupled with the increased productivity realized by enabling a mobile workforce, are moving WLANs from a convenience to a critical element of the enterprise network infrastructure. When selecting a wireless LAN infrastructure that will support voice applications on the WLAN, IT managers should understand the deployment challenges and the capabilities necessary to solve them. This paper discusses the main requirements for voice support in both the WLAN infrastructure and the voice clients. It also describes the unique capabilities of the Cisco® Unified Wireless Networks that satisfy these requirements.

Challenge

Today's businesses are turning to wireless networking to give employees immediate access to the business applications and communications tools they need. By adding a voice-over-IP (VoIP) application to their wireless networks, businesses can further improve collaboration and responsiveness, and increase cost savings.

However, voice places unique requirements on the WLAN that are different from data applications on a WLAN. First, quality of service (QoS) for a VoIP call must be maintained, whether the call is being delivered to a wired or a wireless endpoint. It is critically important to minimize end-to-end delay and jitter for VoIP packets in order to provide optimal audio quality. (Jitter is variation in timing, or time of arrival, of the received signal.) To maintain QoS, it's critical to establish priority across the WLAN and translate the packet priority from the wireless to wired infrastructure during transit.

Because of the time sensitivity of VoIP, reauthentication must happen very quickly as a client roams across the campus, so that network security is maintained. A wireless LAN voice client must be able to maintain its security association from one access point to another, even across IP subnets, with as little latency as possible.

Furthermore, when you deploy any new technology or application on a network, you must consider the impact the application has on the management of the overall network. Voice, particularly when deployed over a WLAN, can cause increased support requirements due to its intolerance for delay and the expectations of end users that it will be as available and reliable as the handset at their desk. When problems occur, it cannot be immediately assumed that the problem is with the WLAN, so it is vital to ascertain if the voice quality issue is WLAN-related or part of another component of the VoIP system, and then immediately take the proper steps to resolve the issue.

WLAN systems that support VoIP also present operational challenges not faced by traditional wireless networks. The wireless medium is a shared resource. When coupled with the clients' ability to roam freely throughout the enterprise, reliable service must be maintained at the radio

frequency layer as well as the application layer. Another operational requirement that becomes much more important is availability: whereas users have a set of availability expectations for their data applications over WLAN, their expectations for voice services will be different. Just as VoIP on the wired network has driven new availability requirements, these requirements will be driven into the WLAN.

Clients for voice over WLAN (VoWLAN) are evolving, and new requirements must be accounted for. Although 802.11 has proven to be an efficient, cost-effective wireless standard, it was not originally designed for devices with limited battery capacity. Unlike the Global System for Mobile Communications (GSM) and Code Division Multiple Access (CDMA) cellular standards, the 802.11 standard was not focused on extended battery life of an endpoint. This impacts usability for wireless VoIP clients, as well as emerging dual-mode clients, because both have limited battery capacity. A technological evolution of the infrastructure is required to accommodate these clients.

Solution

Given the above challenges, enterprises deploying a WLAN that will support voice applications should aim to ensure that the following critical capabilities are present in the infrastructure and the clients:

- QoS priority maintained end-to-end throughout the network infrastructure, including over-the-air (from the access point to wireless client) and QoS Call Admission Control to ensure that there is sufficient capacity to provide the required QoS Priority.
- The ability to differentiate and optimize the flow of voice traffic to increase transmission reliability.
- Highly secure authentication and encryption that doesn't compromise voice quality.
- Seamless, low-latency mobility across Layer 2 and Layer 3 boundaries without compromising security.
- Proper WLAN instrumentation to proactively identify performance issues and isolate them during the diagnosis of VoIP problems.
- Centralized management of the RF environment to ensure pervasive coverage, network capacity and availability.
- Support for extending voice endpoint talk-time battery life.

The Cisco Unified Wireless Network is uniquely able to support these requirements through software capabilities in both the infrastructure and in Cisco Compatible Extensions program clients.

The Cisco Unified Wireless Network incorporates advanced technology that elevates WLANs from a means of efficient data connectivity to a reliable converged communication network for voice and data applications. The Cisco Unified Wireless Network is a comprehensive solution encompassing both clients and infrastructure that solves the limitations of traditional WLANs, while at the same time enabling management capabilities to efficiently deal with problems without overburdening corporate IT resources.

The Cisco Compatible Extensions program helps ensure the widespread availability of client devices that are interoperable with a Cisco WLAN infrastructure and that take advantage of Cisco innovations for enhanced security, mobility, quality of service, and network management. As part of the program, Cisco licenses a specification with the latest WLAN standards and Cisco

innovations to makers of WLAN client silicon which is incorporated into WLAN-enabled voice and data clients. More than 95 percent of the Wi-Fi devices are Cisco compatible. This strategy ensures voice clients have the critical features they need to securely and simply interoperate with the Cisco Unified Wireless Network.

The following sections provide technical details on the infrastructure and client capabilities and how they directly enable toll-quality VoWLAN service.

A Multifaceted Approach to End-to-End Quality of Service

QoS on a WLAN is much more than simply prioritizing one type of packet over another. Traffic on a WLAN is nondeterministic, and channel access is based on a binary back-off algorithm defined by the IEEE 802.11 Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) standard. The nature of CSMA/CA is to have clients back off for a random period of time to minimize contention for the channel. In an operational network, such as that of an enterprise WLAN, channel access times become more variable and on average longer. Indeed, the more clients are connected, the shorter their time window is to transmit, and the more they have to wait to avoid collision. This situation makes delivering reliable voice service on a WLAN exponentially more difficult as network utilization increases. The nature of mobility makes this challenge more difficult still as the number of active users in any one location changes dynamically and isn't predictable through the capacity management tools used in wired networks. The more organizations adopt collaboration, the more likely their workers are to be mobile within the network, and to cluster with other workers at different locations and different times during the day. Meeting the WLAN QoS needs of this critical demographic will determine the success or failure of the VoWLAN deployment.

IEEE 802.11e and WMM

To improve the reliability of voice transmissions in a nondeterministic environment, the Cisco Unified Wireless Network supports the industry standard IEEE 802.11e and is Wi-Fi Multimedia (WMM) certified. WMM enables differentiated services for voice, video, best effort data, and other traffic. However, in order for these differentiated services to provide sufficient QoS for voice packets, only a certain amount of voice bandwidth can be serviced or admitted on a channel at any one time. If the network can handle N voice calls with reserved bandwidth, when the amount of voice traffic is increased beyond this limit—that is, to the $N+1$ call—the quality of all calls will suffer.

Call Admission Control

To help address the QoS issues, the Cisco Unified Wireless Network infrastructure and Cisco Compatible Extensions clients deliver Call Admission Control (CAC) functionality to police the calls on a "per access point" basis. Cisco Unified Communications Manager provides additional CAC features for the wired network, ensuring an end-to-end CAC implementation. Utilizing Cisco Compatible Extension compliant clients with the infrastructure enables the use of the traffic specification (TSpec) for traffic flows in order to calculate call limits and proper WLAN load balancing. The TSpec of each voice flow allows the system to allocate bandwidth to voice devices on a first-come, first-served basis and maintains a small reserve so mobile phone clients can roam into a neighboring access point, even though the access point could otherwise be at "full capacity." Once the limit for voice bandwidth is reached, the next call will be load-balanced by the Cisco Unified Wireless Network to a neighboring access point, and the called completed without ever affecting the quality of the existing calls on the channel.

The difficulty of providing a good CAC function is exacerbated by overlapped coverage cells. In this situation, an RF channel can be shared amongst several access points. Cisco's technology allows for the resources to be globally managed across all the adjacent access points and thus each access point is not permitted to admit the same amount of voice traffic as it could if it were operating in isolation. Access points employ Media Access Control Layer (MAC) measurements from Cisco compatible clients and access points to aid in determining the amount of traffic on the RF channel and whether a new call should be admitted.

Fast Secure Roaming Across Layer 2 and Layer 3 Boundaries

In a typical WLAN deployment, a client roaming through the enterprise will experience multiple access point-to-access point handoffs. With each of these handoffs, the client must re-authenticate to help ensure that an outside security threat isn't able to take advantage of the inter-access point handoff as a way to gain access to the network. However, the re-authentication process must not cause high latencies that might degrade the quality of the voice call.

In addition, as clients roam, there has to be a mechanism for a persistent session—that is, wherever they go, their IP address, security context, and so on must follow. With these two issues to consider, the infrastructure must employ the most efficient methods for authenticating and protecting clients while minimizing the handoff delay; otherwise, the transit time of VoIP packets during roaming will become unacceptably long, and call quality and reliability will inevitably suffer. Cisco Unified Wireless Network provides a comprehensive solution for both seamless roaming and mobile IP clients throughout the wireless network.

Cisco Centralized Key Management for Fast, Secure Roaming

Most 802.11i EAP methods will induce too much latency when a voice client must re-authenticate after it has roamed to a new access points.

During roaming, the re-authentication back to the RADIUS server can alone take more than 500 ms. Real-time applications such as voice need delays of less than 150 ms end-to-end to maintain good voice quality. Cisco has introduced an innovative solution to achieve access-point-to-access point roaming latency of less than 100 ms with the Cisco Centralized Key Management (CKM) authentication method. Cisco CKM permits the negotiation of a session key from a cached master key and avoids the need to go back to the authentication, authorization, and accounting (AAA) server during a roam. When the client roams, it informs the infrastructure that it has roamed, and the infrastructure forwards the keying material to the new access point. The efficiency of EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) with CCKM is a requirement to help ensure maximum protection with minimum transaction time. CCKM is available with any client that is compliant with Cisco Compatible Extensions Version 3 or later.

Mobility Groups for Seamless Roaming

CCKM and EAP-FAST enable low-latency roaming, but do not ensure session persistence (if the client roams across IP subnets) or the availability of needed resources to maintain QoS. The Cisco Unified Wireless Network uses *mobility groups* to facilitate pooling of resources to help ensure that the desired client behavior is maintained across all access points. When a wireless client associates and authenticates to an access point, the access point's controller places an entry for that client in its client database. This entry includes the client's MAC and IP addresses, security context and associations, QoS contexts, the WLAN, and the associated access point. When the wireless client moves its association from one access point to another, the infrastructure simply updates the client database with the newly associated access point. This capability help to ensure

that time-sensitive applications, such as VoIP, can be fully mobile and secure with minimal roaming latency.

Inter-Controller Roaming

The Cisco access point and centralized controller architecture make it possible for a client to roam from an access point attached to one controller to an access point attached to a second controller. In this scenario, the Cisco Unified Wireless Network is still able to maintain session persistence. The network employs a Mobility Messaging Exchange that enables seamless roaming across physically separate controllers. When the client associates to the new access point and thus to a new controller, the new controller exchanges mobility messages with the original controller, and the client database entry is moved to the new controller. New security context and associations are established if necessary, and the client database entry is updated for the new access point. This process, as well as the inter-access-point handoff, is transparent to the user.

Layer 3 Roaming

A Layer 3 roaming occurs when the controllers' wireless LAN interfaces are on different IP subnets. Inter-controller roaming is similar to Layer 2 roaming in that the controllers exchange mobility messages on the client roam. However, instead of moving the client database entry to the new controller, the original controller marks the client with an "anchor" entry in its own client database. The database entry is copied to the new controller client database and marked with a "foreign" entry in the new controller. The roaming remains transparent to the wireless client, and the client maintains its original IP address.

Voice Packet Handling by the Access Points

Enterprise-quality voice communications are dependent on predictable low-latency packet delivery and not necessarily on the total bandwidth available on the network. Voice services consume bandwidth on the order of kilobits per second (Kbps) as opposed to megabits per second (Mbps), and therefore are not very bandwidth-intensive. However, voice is highly sensitive to delay, which can result from digital transmission errors. When voice is transmitted, a specific compression/decompression (codec) scheme is used to digitize and compress the traffic, which is reconstructed on the opposite end of the transmission by a matching codec. During transmissions, variable network delays and retransmissions can increase the jitter, and together with signal loss and packet loss, cause poor voice quality.

Voice packets require fundamentally different handling by the 802.11 MAC layer than best-effort data packets. If they are delivered too late to a receiver's playout buffer, which briefly stores packets before the voice decoder converts the packet to audio, the packet is considered lost. Because of this, if packets suffer too much jitter or delay while traversing the WLAN, they can significantly impact VoIP audio quality.

To facilitate delivery of voice packets over the WLAN with low latency, jitter, and packet loss, the following intelligence has been incorporated into the access points of the Cisco Unified Wireless Network:

- An innovative, low-latency, rate-shifting algorithm that minimizes retries for a faster delivery of relatively short voice packets, and thus results in fewer delays.
- A MAC algorithm that allows different number of retries for voice and data services. This means that transmission reliability to data clients is maintained and delay-sensitive packets destined for voice clients will not be overly retried. This results in a more efficient use of the wireless medium based on the nature of the traffic transported.

- Packet-discard algorithms capable of head-of-queue packet discard when voice packets have been in a queue too long. This avoids using the WLAN to transmit voice packets that are known to be delayed too long, improving efficiency in handling voice traffic.

With the efficiency of the access points' MAC optimized for real-time VoIP packets, quality problems caused by latency and jitter are greatly reduced, and service quality for end users improves.

Intelligent Radio Frequency (RF) Management

All Cisco WLAN controllers come equipped with embedded software for adaptive, real-time RF management. Cisco controllers use patent-pending radio resource management (RRM) software that detects and adapts to changes in the RF in real time. These adjustments create the optimal topology for wireless networking, in much the same way that routing protocols compute the best possible topology for IP networks.

Specific intelligent-RF capabilities managed by Cisco wireless LAN controllers include:

- **Dynamic channel assignment:** 802.11 channels are adjusted to optimize network coverage and performance based on changing RF conditions, such as the addition of new access points.
- **Interference detection and avoidance:** The system detects interference and recalibrates the network to avoid performance problems.
- **Load balancing:** The system provides automatic load balancing of users across multiple access points for optimum network performance, even under heavy loads.
- **Coverage hole detection and correction:** RRM software detects coverage holes and attempts to correct them by adjusting the power output of access points.
- **Dynamic power control:** The system dynamically adjusts the power output of individual access points to accommodate changing network conditions, helping to ensure predictable wireless performance and availability.

In order to support a great VoWLAN user experience, the radio coverage in a voice-ready WLAN must be pervasive—that is, it must provide continuous coverage everywhere a client may roam. This means that there is sufficient access point cell overlap that a client can roam from one access point to another while having sufficient signal strength for a low packet error rate.

To help ensure good radio coverage, coverage predictions made must be based on real usage measurements; otherwise, there will not be sufficient confidence to reliably predict coverage. Cisco compatible clients (Version 2 and later) allow the WLAN controller to obtain this information to finely tune the network.

In addition, the radio coverage analysis must also analyze access point overlap with its consequent impact on access point call capacity. To address this challenge, Cisco has enhanced its innovative RRM software to make it easier to deploy and support voice on a Cisco Unified Wireless Network.

Using data collected from access points and Cisco Compatible Extensions clients, the RRM software will predict call capacity on an access point basis to give the network administrator an estimate of overall network call capacity. This will enable the administrator to centrally manage the capacity of the network and make additional capacity available as necessary.

The RRM software will also receive aggregated WLAN instrumentation metrics (packet latency, packet jitter, packet loss, and roaming delay) and traffic-streaming metrics to create a centralized view for the network administrator on the operational state of the voice application on the WLAN. It will also provide network troubleshooting by reporting WLAN instrumentation for networks and access points, so that the network administrator can determine where the WLAN is experiencing excessive packet delay, packet loss, or roaming time.

Improved Handset Power Management

Before a WLAN device can communicate with other devices in a given WLAN, it must first locate access points. The IEEE 802.11 MAC Layer 2 protocol manages, coordinates, and maintains communications, traffic, and data distribution in wireless networks that have fixed access points or in ad hoc networks. The protocol defines beacon frames sent by an access point at regular intervals (for example, every 100 ms). These beacon frames, known as beacon intervals, allow WLAN devices to monitor for the presence of an access point. Both passive and active scanning techniques have been developed for WLAN devices to detect access points, although the 802.11 standard does not mandate particular methods for scanning.

Industry-standard Unscheduled Automatic Power Save Delivery (U-APSD) extends the talk-time battery life of mobile clients and reduces the latency of traffic flow over the wireless media. U-APSD operation begins with a client sending a trigger frame, which typically includes a voice packet. The access point responds by transmitting any buffered frames that it has. In addition to responding with one or more buffered voice packets, the access point can also send signaling packets or best-effort data packets if the client has requested this operation. Once the frame exchange sequence is over, the client can go back into power save mode until it has its next voice packet available to transmit as another trigger frame—typically 20 ms later. Thus, voice clients go through a wake/sleep process during a call, increasing talk time compared to previous operation without U-APSD, where clients were constantly awake during a call. This feature is supported in the Cisco Unified Wireless Network infrastructure and in Cisco Compatible Extensions.

The design of legacy power-save mode predated the requirement to transport VoIP over the WLAN and thus was not designed to provide low-latency service. In legacy power-save mode, a client wakes up from power-save state and transmits frames that are required to be sent using best-effort parameters, not voice parameters. This causes increased jitter. Moreover, a separate message must be transmitted by the client for every downlink frame from the access point. This means increased jitter and power consumption for the client. In summary, legacy power-save features are not sufficient to support enterprise voice applications.

Conclusion

WLANs have become a necessary part of the enterprise IT infrastructure. With Unified Communications growing exponentially and with enterprises and the WLAN being a natural extension of the wired LAN, it is critical to implement wireless technology that enables mobile workforce productivity without burdening the corporate IT staff. To accomplish this, the Cisco Unified Wireless Network employs advanced features that provide the enterprise with a voice-ready infrastructure. To deliver a WLAN that provides VoIP service with the quality and performance expected from a wired LAN, it is critical to address the limitations of a traditional WLAN and augment them with enhanced management capabilities that can proactively diagnose problems and provide the tools to quickly resolve them. The Cisco Unified Wireless Network lets businesses and other organizations bring the mobility and flexibility of wireless networking to their

voice communications systems. With robust QoS, fast secure roaming, diverse client support, and manageability, Cisco enables the enterprise to bring the immediate advantage of IP communications to a workforce on the move.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDF, CCVP, Cisco, Cisco StadiumField, the Cisco logo, CSE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play and Learn is a service mark; and Access Registrar, Altran, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSF, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS IPPhone, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuickStudy, IronPort, the IronPort logo, Lightspeed, Linksys, MediaTone, MeetingPlace, MIM, NetWorkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. ©2008 ITG