



Converged Voice and Data on a Single Device - Extending the Enterprise Mobility Value Proposition

Introduction

Real-time voice communications among employees or associates, customers and partners is imperative with the velocity of today's business environment. And it has led to a proliferation of mobile devices for both voice and data communications. It is commonplace to see associates carrying multiple devices such as a mobile computer or data capture device, pager or walkie-talkie. Collectively, these devices support the direct associate-to-associate and customer-to-associate communication that is a requirement of so many jobs. Raising the bar for mission-critical mobile business applications includes designing voice features into a variety of mobile devices.

A wireless mobile computer that is also connected to the enterprise private branch exchange (PBX) and to the larger public switched telephone network (PSTN) supports calls to associates, customers and vendors, making it a powerful tool for improving associate productivity and enhancing customer service. The converged solution of voice and data places all the value and benefit of a traditional desktop telephone into the hands of mobile associates while leveraging the investment of the data capture capabilities. The result is a single device on a single network that is used for multiple purposes, which enables organizations to do more for less.

This white paper explores the benefits and challenges of consolidating the voice communication features of multiple devices onto a single wireless local area network (WLAN) and into a single mobile handheld device.

Overview

Adoption of the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards for wireless LANs and the maturing of voice-over-IP (VoIP) technology have set the stage for a new productivity tool - converged voice and data on mobile computers. Utilizing the installed 802.11 wireless infrastructure for both voice and data is the ideal approach to solving most employee communication requirements. This converged solution allows for leveraging wireless LAN investments to eliminate limitations found in other communication alternatives.

Today's Opportunity

There is a strong requirement for a durable, reliable, converged voice/data mobile computer that also provides key telephony functions. However, most consumer-grade PDAs are unable to meet the durability requirements for high-volume usage and at the same time provide high-quality voice capability. A durable mobile computer for the execution of business data applications combined with PBX and PSTN connectivity and toll quality voice fills an important market need.

Strategic Approach

The successful convergence of voice and data onto a mobile computer requires attention to three specific technology areas:

- ▶ **Hardware:** A fast CPU to handle the voice compression/decompression and a mechanical design that provides for microphone, speaker or speakerphone with the appropriate acoustical characteristics.
- ▶ **Software:** Addressing all the unique wireless VoIP challenges -- wireless quality of service (QoS), wireless latency and secure fast roaming.
- ▶ **Telephony integration:** Adopting wireless VoIP often requires integration into host PBX systems and emerging PBX and iPBX solutions.

Making the right hardware product decisions is only part of the solution for a robust converged voice/data implementation. Addressing both the software and integration challenges requires domain knowledge. This includes an in-depth understanding of the challenges in implementing VoIP on wireless in addition to knowing how to implement a best-in-class 802.11 wireless VoIP solution. The following sections detail some of the available technical challenges, solution options and implementation choices.

Challenges

A wireless mobile computer uses the same transport services that a desktop computer uses to support business applications. These applications are based on transmission control protocol/internet protocol (TCP/IP), which is configured with appropriate wireless security services. Support of converged voice and data is similar, because it is typically a TCP/IP-based application, but the challenges faced by a wireless voice application are unique. A robust wireless voice application also incorporates solutions to each of the following challenges.

Security

For chief information officers (CIOs), security is the biggest concern when considering the deployment of a wireless LAN. Fear of a hacker or spy stealing or corrupting valuable company data forces information technology (IT) managers and CIOs to take a conservative position. The security technologies applied to address these data security concerns often impact the ability to deliver good quality voice over a wireless LAN. The primary negative factor to voice quality is the additional burden of latency resulting from the implementation of the security policies. However, some security options have minimal impact on wireless voice quality.

There are a number of choices for wireless security schemes, mechanisms and standards. The basic 802.11 standard defines wireless equivalent privacy (WEP) which is supported by all 802.11 product manufacturers. However, WEP has inherent security flaws. To address that, 802.11i provides two fixes. The first is designed for the generations of equipment already in the field and changes the way WEP works, wrapping it in additional protection protocols. The second, for new generations of devices, replaces WEP with security based on the Advanced Encryption Standard (AES), the latest high-security global standard for encryption.

The Wi-Fi Alliance, a nonprofit international association formed in 1999 to certify interoperability of wireless LAN products based on the IEEE 802.11 specification, is helping to drive support of two modes: Wi-Fi Protected Access (WPA), versions 1 and 2. Neither WPA1 nor WPA2 enhances the mobility support of 802.11 networks to provide good voice quality when the devices are in motion. And, unlike laptop computers used on a desk, voice-enabled mobile devices are meant to be held, moved and carried around.

While WPA1 and WPA2 dramatically improve the security of 802.11 data networks, they are security standards first and foremost. These new security mechanisms provide stronger encryption services and add important authentication capabilities. However, they are also less than optimal in supporting real-time audio applications like VoIP because security mechanisms take time to operate and impose a latency penalty that degrades voice quality. In addition, all of the extra processing that is required is directly at odds with the kind of low-power operation needed in battery-operated devices. This leads to a requirement for hardware (ASIC) assist circuitry in order to get optimum voice quality when using mobile devices.

An alternative to 802.11i-based security is virtual private networks (VPNs). The use of VPN is viewed as a straightforward solution to wireless security problems, as it provides security control at the highest level with end-to-end encryption across a connection. VPNs meet authentication and data security requirements but impose a penalty on real-time applications like VoIP. In many cases, VPNs operate in a way that is contradictory to what is needed for good mobility. The most common and interoperable VPNs based on the IPSEC protocol assume a fixed connection link and are unsuited to mobile operations. By comparison, VPNs based on WTLS were developed as part of an advanced mobile cellular architecture and are optimized for secure operation across multiple bearers and unreliable networks.

Unfortunately, VPNs impose a significant computational burden on the networked device. Without an assist from a high-end processor or coprocessor, the resultant voice quality of a wireless PDA-class device is degraded. The tunneling of the packet flow through a VPN also adds to the overall latency within the system and further reduces the voice quality. It almost seems that VPNs and wireless VoIP are mutually exclusive. This is not quite true, but it means that care must be taken in implementing and deploying a wireless VPN solution. Consideration for the computing power of the mobile device, its battery capacity and the VPN design within the network fabric must all be assessed in an attempt to guarantee a secure, high-quality VoIP solution.

Another standard is Kerberos, which is a security architecture developed at MIT and implemented in most Unix products and in Microsoft® Windows Server 2003. Used as a standard security scheme for over 20 years, Kerberos provides a method of unit authentication and key management. It is implemented to support mutual authentication when every device within the network fabric, including access points, is authenticated. Once authenticated within a secured network, roaming from access point to access point is secure through the passing of pre-secured credentials, verified between parties. This architectural approach supports the concept of a fast, secured roam without requiring a complete re-authentication upon each roam. In addition, Kerberos goes beyond a simple authentication scheme to provide for dynamic key management for compliant devices.

Standards-Based Solutions

In the absence of a mobility-ready wireless security standard, manufacturers are moving forward with additional solutions that are good for secure mobility and build upon the 802.11i standard to make it mobility ready.

Both in standards bodies and collaborative associations, companies are working to enhance the wireless security options available and to ensure cross-vendor interoperability of products and mobility. The goal is to add value and mobility-enabling extensions that enable mobility. Good examples of these in-process works include:

- › Using the Wi-Fi WPA interoperability specifications to require some of the 802.11i options like pre-authentication
- › Extending 802.11i within Wi-Fi to add PMK (Pair-wise Master Key) caching
- › Opportunistic pre-authentication for improved roaming

Quality of Service (QoS)

Good voice quality demands the timely delivery of audio packets to the receiving device. Typically, a delay of more than 60 msec in delivering audio packets results in a deterioration of the overall voice quality. Management of this delivery problem requires enforcement of quality of service (QoS) that guarantees delivery of selected packet types within certain latency limits. For 802.3 networks, QoS is mandated by the IEEE 802.1p standard, a mechanism that tags each packet or frame with a priority label. As that frame traverses a network fabric, each switch and router enforces the indicated QoS in preference of lower QoS tagged frames.

The wireless segment of a network, by its nature, is the more fragile component with regard to reliability frame transmission/reception - where QoS is important. The IEEE committee has made a lot of headway in defining the 802.11e standard for QoS. However, this technology is in its first stages and hasn't met mass acceptance and customer adoption. Until then, today's product offerings meet this challenge using a proprietary QoS architecture.

Wireless Congestion

VoIP traffic places a unique demand on the wireless infrastructure, specifically the high packet/second rate. Most data applications are "bursty" and transmit large data frames. This kind of traffic is addressed through the data throughput capacities of the wireless infrastructure such as a wireless switch (in kilobits per second). Voice traffic is isochronous with small packets and places a different demand on the wireless infrastructure. Because much of a voice frame is header, there are a fixed number of frames per second that can be processed. In this case, it is possible that a large number of VoIP applications might reach the maximum capacity of a wireless LAN. This creates points of congestion within a wireless infrastructure, degrades voice quality (even with QoS) and causes data application failures resulting from the voice traffic congestion.

Addressing this potential congestion problem are general approaches that either:

- › Maximize the throughput (number of calls) through any single access point, or
- › Distribute the traffic demand more evenly across multiple network resources.

Maximizing throughput is best achieved through aggregation of the audio stream packets to minimize the packet per second through any one access point or access port. Implementing this technique has a demonstrable impact on being able to control congestion problems. Traditionally, distribution of traffic to minimize wireless infrastructure congestion has been approached in one of two ways:

- › Creating intelligent mobile client RF modules, or
- › Using a centralized server within the network.

Managing potential congestion via intelligence within the mobile device requires collaboration with the infrastructure to provide additional access point/access port loading information that permits making such intelligent roam decisions. This typically requires a modification of certain 802.11 signaling elements to carry this information. Fortunately, the 802.11 standard is written in such a way that this is possible.

Others attempt to manage the wireless infrastructure congestion issue with a server-based architecture where each mobile unit registers and derives roam information and roam permission from the server. However, this is an application-level architecture, a vendor/device specific solution that requires additional devices be added to the network.

Voice/Data Mobile Computer Design Considerations

Once the network and RF challenges are addressed, the feature set of the mobile device itself is considered. In order to provide the best user experience with wireless VoIP, the following items need to be addressed at the mobile unit level:

- › A fast CPU is needed to supply the necessary compression CODEC services. Support of CODECs like G.726 and G.729 requires that mobile computers have a very fast CPU clock (400Mhz or greater) for VoIP applications.
- › Acoustic design is important because the mechanical and electrical design of a VoIP-enabled mobile unit reflects clear design intent and support: microphone or speakerphone and/or headset. Also, assessing the basic ergonomics of the device and how a user holds the device while in a conversation is a critical consideration, because this is not usually a factor for PDA-class devices.

PBX Integration Considerations

Finally, it is vital to provide cost-effective, feature-rich solutions for integration into the customers' telephony systems (PBX or iPBX). Through these systems, a simple phone call to the vendor or customer is made. Two solutions are available to provide such integration:

- › Gateway/adjunct solutions
- › Direct integration solutions

Gateway solutions address the legacy market opportunities. Organizations with traditional PBXs connecting them to the PSTN are able to install a wireless VoIP solution by adding a gateway product, which also supports an analog or digital telephony interface. The gateway also provides a network interface and acts as an application bridge in support of VoIP-to-analog/digital translation of the signaling. This approach allows a business to retain their PBX investment while extending the services to include wireless VoIP.

Direct integration solutions are designed to complement the VoIP services being offered by the host PBX or iPBX. As VoIP technologies are deployed, more and more telephony vendors offer proprietary native VoIP support. Typically implemented to support an IP-desktop phone, these solutions also support wireless VoIP solutions that conform to the vendor's VoIP architecture and protocol. These solutions offer the tightest and most feature-rich solutions, but require the customer to already have made a VoIP decision with the internal telephony services.

The Solution

A robust wireless VoIP solution requires attention to supported components and functions across multiple technology disciplines. Attention to RF infrastructure design, Ethernet network configuration, security policies, acoustics, telephony and mechanical design converge across a multi-vendor landscape to result in a strong wireless VoIP solution.

- › Support with wireless infrastructure features (power save mode, QoS, security)
- › Collaboration with telephony customer premises equipment (CPE) providers
- › Acoustical and mechanical design requirements
- › Adherence to standards

Return on Investment- Demonstrating the Value

Having telephony support in a terminal requires a demonstration of real value -add to drive market demand. There are hard and soft ROI realizations with voice -enabled mobile computers. The hard ROI examples identify specific and calculable savings as a result of deploying such solutions, and the soft ROI considerations are valuable and real but often subjective in any attempts to quantify them. The detailed ROI analysis is different for each market segment based on cost structure and business dynamics in considering communication technologies.

All ROI analyses start from a customer's direct communication requirements. Whether this is between employees, employees and customers or employees and vendors, most organizations have a real business need for reliable, quick communications to keep their companies competitive and successful.

Hard ROI values are derived through the mitigation of current expenses. Whether it is the result of lowered material costs or elimination of ongoing operational expenses, these economic considerations are easily quantified. ROI metrics are derived from:

- ▶ **Elimination of duplicate infrastructures:** Some wireless VoIP solutions require deployment of a separate wireless network just for voice. Converged solutions (utilizing the 802.11 wireless LAN) provide a built-in reuse of the existing wireless LAN infrastructure, which also mitigates the cost and total cost of ownership (TCO) of the entire system. In addition, when consideration of a converged wireless LAN solution is made with new construction, significant savings are realized without the need to deploy a hardwired telephony infrastructure and rely solely on the wireless services for voice and data.
- ▶ **Elimination of duplicate devices:** Deploying mobile computers that provide both telephony services and in-building communications such as walkie-talkie features eliminates the need for additional devices. In addition to voice, support of text messaging or paging on the same wireless device eliminates the need for pagers. Again, the application of converged voice and data to use one device for many functions lowers overall expenditures.
- ▶ **Elimination of ongoing service charges:** Some companies deploy cell phones to provide for in-building communication. However, this option includes annual service contracts with the service providers. Also, some walkie-talkie products require a license to use the spectrum, which is eliminated when using a wireless LAN solution. Converged mobile computers are purchased as capital expenditures. Ongoing service charges and license fees for devices such as pagers and walkie-talkies are mitigated.
- ▶ **Elimination of unnecessary associate functions:** When deploying wireless communication devices, many companies restructure their personnel organization. This results in a streamlined operation that achieves business goals with fewer associates. The fact that associates are mobile and still reachable is an important factor in how a business allocates its people resources.

Soft ROI contributions are more difficult to quantify. These benefits often fall into the category of productivity improvements and associate response time enhancements. While challenging to measure, these considerations do contribute to an overall ROI. This simple example of productivity improvements for the management-level associate easily demonstrates the potential.

A manager saves 10 minutes each day by using a VoIP-enabled mobile computer. This time savings comes from the fact that the manager answers calls while on the floor and isn't trapped at a desk answering voice mail. If the manager makes \$80,000 per year, then each minute of his or her workday has a value of approximately 65 cents. Saving 10 minutes each day provides a \$6.50 per day productivity enhancement which, when extrapolated for the whole year, amounts to \$1,625. If the extra time afforded to the manager each day is economically productive in increased sales, then it is easy to justify the purchase of a wireless VoIP solution.

In addition, responding to customer and vendor calls immediately without having to interface with a voice mail system raises customer or vendor satisfaction levels. Responding to emergencies is also greatly enhanced through use of a converged VoIP and data mobile computer. Beyond the basic ROI considerations listed above, support for the VoIP services provides a platform for adding other high-value applications that are mission critical to certain vertical markets.

Markets	Applications	Users
Retail	Manager terminal Store reports Scheduling Clienteling Email and messaging Mobile point of sale Price management Replenishment Receiving	District and regional managers Store supervisors Store operations personnel
Sales Force Automation	Pharmaceutical Signature capture Compliance Medical devices/supplies CRM	Pharmaceutical and medical devices or supplies sales representatives Distribution center managers
Merchandising	Store visits Promotions Advertising	Account representatives

The MC50 with Converged Voice/Data from Symbol Technologies

The MC50 from Symbol Technologies is an enterprise digital assistant (EDA), the first in a class of mobile computers that delivers enterprise-class application support in an attractive, compact PDA-styled device. It goes beyond consumer-grade devices and into the realm of a business essential enterprise tool. The MC50 features integrated VoIP capabilities, data capture options, wireless support and management software. It performs seamless voice communications via push-to-talk (PTT), peer-to-peer (P2P), PBX connectivity, 1-to-1 or 1-to-many.

The following section offers more details on how the MC50 with converged voice and data addresses the challenges stated earlier. Some of these areas - QoS, wireless congestion - also encompass Symbol wireless LAN infrastructure solutions.

Security

The MC50 supports the WEP, TKIP, Cisco LEAP, 802.1x, PEAPv0, PEAPv1, EAP-TLS, EAP-TTLS, WPA1 and Kerberos security protocols. It also supports both IPSEC and WTLS VPNs. Finally, the MC50 integrates advanced mobility support with managed credentials handling and secure fast roaming to provide a secure, authenticated network connection along with very high voice quality.

In addition to standards-based 802.11i and VPN security, Symbol also offers security enhancements in areas from the RF domain all the way up to the network management system that provide answers to the heightened wireless security concerns.

Quality of Service (QoS)

In the popular Wireless Switch System product line, a proprietary QoS offers direct support of the VoIP standards. Unique from other proprietary QoS offerings, the Symbol implementation provides a mechanism where audio frames based on the Internet Engineering Task Force (IETF) real-time protocol (RTP) standard are treated with higher priority in transmission processing. An audio stream from/to a Symbol voice client is automatically given priority over data traffic to ensure the very best voice quality with minimal latency. Support for the 802.11e standard will be provided through firmware updates to support standards-based QoS.

Wireless Congestion Avoidance

Pre-emptive roaming and packet aggregation address real-time traffic and congestion at access points or access ports. Currently, Symbol offers the highest call capacity of any product

offering at 10+ calls per access point and port. Using load information from the access points/ports, MC50 enterprise digital assistants can be programmed to make intelligent decisions about roaming to a new access point or access port. Pre-emptive roaming results in load balancing within the network, and the Symbol MC50 supports collaborative decisions to load balance across multiple access points or access ports. Voice devices are driven in their roam decisions to ensure the best voice quality and will roam to a less congested access point or access port. This technology reduces wireless congestion and maximizes the voice quality and data throughput - a unique feature of Symbol mobile and wireless products.

Voice/Data Mobile Computer Design Considerations

To achieve a successful VoIP integration, the MC50 features a variety of features and capabilities.

- › Superior voice ergonomics
- › Dedicated buttons for voice (PTT, send, end, dial -pad)
- ›
 - › Supports multiple protocols and applications
 - › Echo canceller to improve voice quality
- › Standards based:
 - › G series CODECs, AEC, E.S. to increase call capacity
 - › UDP/IP voice stream
 - › Voiceband transducers
- › High-performance acoustics
- › Full duplex record and playback (stereo)
- › Security protocols: WEP, TKIP, Cisco LEAP, 802.1x, PEAPv0, PEAPv1, EAP-TLS, EAP-TTLS, WPA1 and WPA2
- › Handset, headset, PTT multi-cast, speakerphone modalities
- › Audio drivers for mission-critical communications
- › IEEE 802.11 wireless LAN connectivity
 - › Wake-on-LAN
 - › QoS
 - › Preemptive roaming
 - › Load balancing
- › Voice multi-cast

PBX Integration Considerations

Both gateway and direct integration solution approaches are provided. For customers who need to retain their host PBX investment, the MC50 supports a variety of gateway options that allow for straightforward deployment of wireless VoIP devices.

The Symbol MC50 EDA combines high performance to support enterprise-level applications with a compact, PDA-style form factor. Designed for busy managers and outside sales teams, the MC50 converges data capture, voice, wireless, smart battery, device management and security capabilities into one convenient device. On-the-go professionals are empowered to make rapid, informed decisions in real time. The MC50 adapts to a variety of enterprise applications including e-mail, phone, scheduling/calendar, signature capture, mobile customer relationship management (CRM) and sales force automation (SFA) applications. From retail to life sciences, the MC50 helps increase productivity, sales and customer satisfaction.

For more information, contact us at +1.800.722.6234 or +1.631.738.2400.

About the Symbol Wireless Switch System

A new and better WLAN infrastructure, the Wireless Switch System is the wireless LAN system with centralized intelligence — unifying network access, security, policy management and QoS at the switch level. This provides the highest level of wireless security to protect your network, data and devices (without compromising service). It offers easier definition of rules for QoS and security (for greater management efficiency) and provides media independence and scalability (from FH to 802.11b to 802.11a to emerging standards).

Glossary of Terms

AES: Advanced Encryption Standard - an advanced encryption scheme that is more secure than the traditional encryption algorithms such as DES, Triple DES or RC4

iPBX: IP Private Branch Exchange - Private Branch Exchange systems are designed to provide VoIP services in addition to or instead of the traditional time domain multiplex (TDM) services of the PSTN.

IETF SIP: Internet Engineering Task Force - Session Initiation Protocol. This standard emerged as a leading architecture for future VoIP solutions. Initially adopted for its simplified architecture, it has received worldwide industry focus.

ITU H.323: International Telecommunications Union standard H.323. This voice/video standard for packet networks is widely implemented for VoIP support.

Kerberos: This security architecture was developed by MIT and originally delivered as part of the Unix based technologies to support fast, secure roams within a fully authenticated domain.

LEAP: Light Extensible Authentication Protocol - Cisco Systems' proprietary wireless authentication protocol.

PBX: Private Branch Exchange - telephony systems hosted within businesses to provide extended features required by commercial concerns. A term that is synonymous with customer premise equipment (CPE).

PSTN: Public Switch Telephone Network is the traditional telephony hardwired international network.

RADIUS: Remote Access Dial-In User Service - this industry standard was initially implemented to support authentication requirements for Internet service providers (ISP). Many wireless LAN vendors adopted this architecture for the wireless LAN authentication because of its popularity.

TKIP: Temporal Key Integrity Protocol is an IEEE security standard that is part of the proposed 802.11i standard and the WiFi Alliance WPA. This scheme extends the encryption design of WEP and addresses the flaws of the former.

VoIP: Voice over IP is a packet-based technology that is being rapidly adopted worldwide for transmission of voice traffic. In addition to carrier level adoption of this technology, many PBX

telephony vendors now offer their own VoIP desktop service.

VOT: Voice on Terminal is a data terminal with a converged voice component that has value in the commercial space where daily job requirements necessitate use of both phone and data applications.

WiFi: Wireless Fidelity is a term generally applied to all commercial 802.11 products, but more specifically it refers to products that comply with the WiFi Alliance interoperability certification requirements.

WPA: WiFi Protected Access is a collectively supported "standard" for implementing enhanced wireless standards ahead of the ratification of the 802.11i. The WiFi Alliance has driven this initiative and is responsible for coordination of vendor conformance.

Specifications are subject to change without notice. Symbol ® and Spectrum24 ® are registered trademarks of Symbol Technologies, Inc. All other trademarks and service marks are proprietary to their respective owners.

For system, product or services availability and specific information within your country, please contact your local Symbol Technologies office or Business Partner.

Part No. MC50VOIP_WP © Copyright 2004 Symbol Technologies, Inc. All rights reserved. Symbol is an ISO 9001 and ISO 9002 UKAS, RVC, and RAB Registered company, as scope definitions apply.