



## Mobility Is a Hot Topic

### Abstract

*Does mobility imply wireless? Does wireless ensure mobility? Is there a difference between portability and mobility? Should an organization have a mobility policy before it crafts a mobile solution? This white paper answers these questions and more.*

*The paper examines wireless from the PAN, LAN, MAN, and WAN perspective. For each coverage area, we look at the relevant technology and decide if it provides portability, mobility, or both. With this question resolved, we turn our attention to the issues related to introducing mobility into the enterprise. We address issues surrounding access, transport, security, devices, and applications. Finally, we introduce the components of the mobility policy.*

### Introduction

Every other article in the trade magazines focuses on mobility in the enterprise. Some discuss the advantages and others the disadvantages. All of them cite the inevitable movement of “everything” to mobile. But, very few of them look at the interrelationship of mobility and wireless. Sure, we all assume that to be mobile means wireless, but wireless itself does not ensure mobility. Therefore let’s begin our discussion with a look at contemporary wireless systems used in a personal area network (PAN), a local area network (LAN), a metropolitan area network (MAN), or a wide area network (WAN). As we shall see, all of these systems give us portability (i.e., connection is lost when you change locations) and some of them give us mobility (i.e., connection is maintained when you change locations).

### Wireless Personal Area Network (Bluetooth)

The big name in a wireless PAN is Bluetooth. The name comes from Harald “Bluetooth” Gormson, the King of Denmark near the end of the tenth century. His claim to fame was the unification of his people under the banner of Christianity. The name was chosen for the wireless PAN because it was going to be a universal connection for a variety of devices. Bluetooth provides a secure connection using a globally-available unlicensed radio band to connect mobile phones, PDAs, cameras, laptops, PCs, printers, and video games. Many of us now have a Bluetooth ear phone for use with our mobile telephone.

Bluetooth operates at very low power and has a coverage range of about 1 meter at its lowest power (1 mW) and 100 meters at its highest power (100 mW). It uses a spread spectrum technology. All Bluetooth devices advertise their capabilities making the creation of ad hoc networks a breeze. Bluetooth might or might not provide mobility. For example, if we use a Bluetooth ear piece for our mobile phone, as we move, both parts of the Bluetooth connection move with us. However, if we use Bluetooth for a wireless printer, as we move away from the printer we will lose the connection. In this case, Bluetooth offers portability, not mobility. Bluetooth is portable since we could reconnect with another printer in another location. To have mobility, a seamless handoff from one radio coverage area to another must occur.



## Wireless Local Area Network (IEEE 802.11)

Perhaps the biggest event in LAN evolution was the development of the wireless LAN that was defined by IEEE 802.11b. It gave the user portability and limited mobility at speeds of up to 11 Mbps. Because of its simplicity the price of an 802.11b wireless access point dropped to below \$100 in a matter of months.

The 802.11 standards define a set of wireless LAN systems that operate in the infrared and radio environments. Today we see very few infrared implementations. Most of the radio-based frequency hopping spread spectrum systems (FHSS) have been replaced by direct sequence spread spectrum (DSSS). Eventually, orthogonal frequency division multiplexing (OFDM) will replace them all.

802.11b was the first. It delivered up to 11 Mbps and operated in the 2.4 GHz unlicensed spectrum. 802.11a came next at up to 54 Mbps in the 5 GHz unlicensed spectrum. 802.11g upgraded 802.11b to the 54 Mbps level in the 2.4 GHz spectrum. Today we are rolling out 802.11n, which works in either 2.4 GHz or 5 GHz spectrum and delivers up to 200 Mbps. Only 802.11b was called wireless fidelity Wi-Fi but the name is now synonymous with any of the 802.11 systems.

Most people have a wireless LAN (WLAN) either at home or work. WLANs are found as freestanding LANs at conferences and on open manufacturing floors. They can be used to extend the wired LAN or to bridge between buildings. Depending on the antenna, wireless LANs can be extended to up to twenty-five miles. Needless to say, a wireless LAN is a savvy investment for any size business as long as the business addresses the security issues associated with wireless systems.

The wireless LAN does have some problems. Security in the form of wired equivalent privacy (WEP) is easily compromised. However, a simple upgrade to Wi-Fi protected access (WPA) can result in good network security. A full-blown security solution is also available as part of the IEEE 802.1x standard.

WLAN performance can be problematic because wireless communications requires significant overhead for timing and synchronization. At best we can expect throughput of about 50 percent of the raw network speed. Then we need to add TCP/IP overhead before we actually get to the data. Occasional lost connectivity can also lead to performance problems.

There are four flavors of 802.11, and the organization must consider how they all interact. 802.11a is all by itself, and 802.11b and 802.11g are fully compatible—but only at the point of lowest common denominator. That is, several 802.11g users will have their speed decreased when an 802.11b user joins the group. 802.11n is compatible with all flavors and does not suffer performance problems in mixed environments. However, since it does this via multiple radios, it does cost more.

Finally, the environment is a key consideration since interference can render the wireless LAN inoperable. Some interferers are microwave ovens and cordless phones. Also, the placement of the access points must be optimized to provide optimal coverage to the network.

So, back to the seminal question: is the WLAN portable or mobile? Clearly it is portable since a wireless laptop goes everywhere and connects to any available Wi-Fi hot spot. Mobility, on the other hand, is not achieved since there is currently no standardized way to hand off from one access



point to another. However, for some the disconnect and automatic connect of wireless systems may make the 802.11 family appear mobile for some applications.

### Wireless Metropolitan Area Network (WiMAX)

The wireless MAN is truly a unique system since its roots come from television and video. The multi-channel multipoint distribution system (MMDS) was a combination of educational spectrum and specialized TV distribution spectrum. MMDS was not successful for video and TV, as the cable TV industry and direct broadcast TV proved to be better solutions. MMDS moved to Internet access solutions and much of this spectrum was licensed to Sprint and MCI (now Verizon). The local multipoint distribution system (LMDS) offered cellular TV before it too became used for Internet access. BellSouth (now AT&T) has a successful TV offering in 11 markets using LMDS. Both of these systems were line of sight so there must be a clear path between the transmitter and receiver. MMDS and LMDS were eventually codified in the IEEE 802.16 standard.

The development of 802.16a moved the system from line of sight to near line of sight, thereby increasing the ease of deployment of the solution. It is called worldwide interoperability for microwave access (WiMAX). Fixed WiMAX is defined in 802.16-2004, and mobile WiMAX is defined in 802.16-2005. Both of these standards are enjoying significant deployment worldwide, and many are touting WiMAX as the 4G mobile telephony solution.

The 802.16 standards from the IEEE coupled with the conformance testing of the WiMAX forum are keys in promoting the success of WiMAX. It operates in licensed spectrum, which makes it ideal for carriers as a MAN or WAN alternative. It also works in unlicensed spectrum, which allows it to effectively compete in the LAN market. The biggest difference between licensed and unlicensed spectrum is the amount of and controllability of interference.

To compare WiMAX and Wi-Fi may be useful since they are both radio-based systems. However, they have different market perspectives (metropolitan vs. local) and different provider perspectives (carriers vs. users). Fixed WiMAX can cover up to a 30 mile diameter and could possibly compete with DSL and cable modem services. Mobile WiMAX has a smaller coverage area and it will compete with mobile telephone systems since it does have hand-off capabilities and thus is a truly mobile solution.

### Wireless Wide Area Networks (3G Cellular Telephony)

Third generation (3G) cellular telephone or mobile telephone systems offer a number of voice, data, and multimedia services. And, there is no doubt that mobile telephony provides the user with mobility. The ITU defines 3G coverage areas are defined by speed of movement or bandwidth provided to the user. For the vehicular user the minimum speed is 144 kbps, for the pedestrian user it is 384 kbps, and for the technically stationary user it is 2.048 Mbps.

The global system for mobile communication (GSM) is the number one system in the world commanding a whopping 90 percent share of the 3 billion-user mobile telephony market. In the U.S., GSM is offered by AT&T, T-Mobile USA, and several smaller carriers. GSM's first foray into 3G was the enhanced data rate for GSM/global evolution (EDGE). Now the service is called universal mobile telecommunications service (UMTS). UMTS uses wideband CDMA (WCDMA),



and the current service offerings are in the high-speed packet access arena for both downlink and uplink access.

The other 3G solution of note is cdma2000, a registered product of QUALCOMM and deployed in the U.S. by Verizon Wireless and Sprint. The current offering is the 1xEV-DO optimized (1xEV-DO); future offerings will be in the 3xRTT family.

Wideband CDMA and cdma2000 are generically the same, but they are implemented differently and thus incompatible. A simplistic view of the CDMA incompatibilities is outlined below.

- WCDMA is a European-developed standard and cdma2000 is a U.S.-developed standard.
- WCDMA has a 3.84 Mchips/second coding sequence and cdma2000 has a 3.75 Mchips/second sequence.
- WCDMA is not backward compatible with 2G systems; cdma2000 is backward compatible with cdmaOne and IS-95 since the 3xRTT rate is three times the 1xRTT rate.

Regardless of the incompatibilities, both of them are international standards along with a couple of Chinese standards. All of these systems will battle for subscribers over the next several years.

UMTS high-speed packet access (HSPA) is an IP-focused solution that was offered as part of the 3GPP/UTRAN-FDD Release 5 WCDMA. Voice will be implemented over IP in high-speed packet access (HSPA).

High-speed downlink packet access (HSDPA) has a theoretical rate of 14.4 Mbps and will be offered in 2–10 Mbps configurations depending on the size of the cell. The uplink rate will be 400–700 kbps. These speeds will improve to 5.8 Mbps in theory, or 2 to 3 Mbps in reality with high-speed uplink packet access (HSUPA). In comparison, cdma2000 is now being deployed in the 1xRTT EV-DO Rev A configuration that gets it close to 1 Mbps and introduces a voice over IP backbone concept. It will also see increased speeds as the technology evolves.

## **PANs, LANs, MANs, and WANs: Portable or Mobile?**

Using the ITU terms of technically stationary, pedestrian, and vehicular usage the distinctions between portable and mobile can be defined. For all practical purposes, wireless PANs and LANs fall into the technically stationary user camp and provide a level of portability. While there may be mobility within the coverage area, there is no easy way to roam from one coverage area to another.

Wireless MANs and WANs offer mobility to pedestrian and vehicular users since there are processes to roam from one coverage area to another. There are even ways to roam from one service provider to another as long as the network technologies are compatible. However, if users move into an area that has no coverage their mobility comes to a screeching halt. Service availability is the cornerstone of a viable mobility solution.



## Getting Started with Mobility

The first step in the execution of a mobile strategy is to understand the operational aspects of the users and their subsequent need for mobility. Consider the dedicated office worker that lives a static existence at the office. For this user mobility is not needed. A wired PC on the desktop is more than adequate. However, the campus worker might need a much more dynamic environment as he or she navigates through the various locations within the corporate campus. This level of mobility may require a mobile phone, a PDA, and a laptop. However, before jumping to any conclusions let us explore a couple other user profiles.

The traditional teleworker (now called a virtual workspace worker) works from home and could be classified as mobile except that the worker at home or some alternative location is basically static. He or she could work with a desktop or a laptop with communications being provided with either a fixed or mobile phone. The road warrior, on the other hand, works from his/her location at the moment. These users are dynamic and are often required to work while on the move. Mobility may be the answer for this group of users. The point is to understand the users' needs before rushing to a mobility solution—the more dynamic the user requirements, the more mobile the solution.

## Productivity and Mobility

The ultimate success of the mobile enterprise requires many factors to come together. First the user needs tools that will operate in the mobile environment (i.e., the user will need the appropriate device or set of devices to effectively use mobility). Moreover, there must be a set of applications that provides the content. For some this could be as simple as email and instant messaging, but others might need a sophisticated sales force automation application.

Regardless of the application or the tool, the user will need adequate bandwidth if mobility is to be viewed as valuable. The amount of bandwidth will be in direct proportion to the complexity and the applications and the amount of information that must be moved in a reasonable amount of time. An asynchronous email application can operate with lower bandwidth than a Web surfing application.

Finally, the mobile worker will need an environment conducive to working. Some workers might be able to use a hot spot at Starbucks while others will need a desk or workstation in a quiet area. We have no control over these environments, but they still must be considered in evaluating the effectiveness of the mobile enterprise.

## Mobility Parameters

Many parameters need to be considered when developing the mobile system. The network access method must be agreed upon and the available spectrum must be able to support the speed requirements. A cellular telephone solution can operate at up to 400 kbps, whereas an 802.11g solution can deliver up to 54 Mbps, albeit with less mobility. Coverage and availability become part of the solution since the user will want to have access in places that the user occupies, not just in places where mobile access is available.



To enable an enterprise-wide solution that includes suppliers and customers, users might have to use products and services that conform to a national or international standard. In addition, they will need to choose a service provider that gives them confidence in its ability to meet their needs now and in the future. This could be the most critical decision in the process because it might drive the technical aspects of the solution.

Security for both the fixed and mobile parts of the solution will need to be considered as will an appropriate set of applications. The applications will be the basis for the content delivery but they must be formatted for the mobile devices the users will use. The screen of a laptop is very different in display capability from that of a cellular telephone. Finally, there must be a seamless integration of the fixed and mobile environments. Network integration must look at how the legacy world will integrate with the mobile enterprise. Back office systems might be an even bigger challenge than the mobile system.

Contemporary wireless systems are usually based on radio technologies. While the concept of radio communication is over one hundred years old, many issues must be considered to ensure successful operation of the wireless system. These include spectrum, bandwidth, noise, antennas, and the environment in which the radio system operates. As a simple example, the coverage area of a radio transmitter is larger on sunny days than on rainy days. The rain absorbs energy in the radio waves, and as a result, they don't as far as those transmitted on sunny days.

While the details of radio are beyond the scope of this paper, there are a few realities of radio that need to be mentioned. First, radio channels cannot be engineered—they are what they are. In other words, the channel on a rainy day cannot be changed by a radio engineer. In addition, the channels cannot be cloned. Once all the available channels have been allocated, there are no more channels. It is not like using up a twenty-five pair cable and then stringing another one to get another twenty-five channels.

In addition, radio signals suffer significant destructive interference. In fact they can interfere with themselves. Adjacent channel interference occurs when a nearby channel in the spectrum bleeds into another channel. For example, interference from TV channel 2 on TV channel 3 is adjacent interference. When TV channel 2 interferes with another TV channel 2, the problem is called co-channel interference. Multipath propagation is a term applied when a radio signal interferes with itself, and the receiver gets time-delayed reflections of the original signal (often called a ghost). Finally Rayleigh fade is the signal lost to things like trees, walls, and people as the radio signals pass through these substances.

In the past much work has been done to eliminate these problems under the guise of reducing the noise in the signal. Claude Shannon developed the relationship between bandwidth, noise, and maximum data rate. He also suggested that we would eventually find information coding processes that would allow us to better live with the noise. Code division multiple access (either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS)) and orthogonal frequency division multiplexing (OFDM) are examples of these advanced coding schemes.

Mobility solutions are available in various forms and in coverage areas that can be described as LANs, MANs, or WANs. The IEEE 802.11 family defines a set of LAN solutions. IEEE 802.16, or



WiMAX, is a set of MAN solutions. Finally, there are several 3G mobile telephone systems defined in the WAN environment.

However, mobility is not just about access. There need to be mobile applications that can operate on IP-enabled mobile devices. There also needs to be a large and varied selection of mobile devices to meet the different needs of mobile users. Both the devices and the applications need to be equipped with sophisticated, yet easy to use, security and authentication capabilities. Finally, the social issues surrounding the mobile solution need to be addressed. This may be as simple as appropriate restaurant etiquette or as awkward as ensuring that someone is not viewing your screen over your shoulder.

## Putting It All Together—The Mobility Policy

A mobility policy will change from one business to another. It must meet a business's specific needs, cost the right amount of money, and add value to the mobile user's experience. The policy defines the who, what, where, and why of mobility, so it is not specific to the technologies that will be used to create the solution. The "how" should be left up to the IT organization, as it will have the knowledge to make the solution a success.

The mobility policy needs to define appropriate security measures as well as the acceptable devices and applications. In short, the mobility policy should guide the implementers and the users to do the right things.

## The Mobility Puzzle

Mobility can be described as a puzzle. It has five easy pieces, all of which must be chosen wisely to ensure that they fit together in a seamless mobility solution.

1. Mobile device
2. Access service
3. Transport service
4. Mobile-ready applications
5. Security

Mobile devices will continue to evolve; this evolution could lead to improvements in the mobility solution. This means that the mobility policy as it relates to acceptable mobile devices needs a periodic update.

Devices will continue to perform better and deliver a better quality of user experience. The device features will expand and things that appear somewhat innocuous at first (e.g., battery life) will improve. Remember that in the dynamic industry of wireless communications, old devices fall from grace and manufacturers discontinue support of these devices. The mobility policy must be a living document that receives regular consideration.

The most important and difficult to control aspect of the mobility policy is that users cannot introduce mobile devices that are not covered under the mobility policy. This can prove to be a



destructive influence on the infrastructure. Users always find a better solution that better meets their own needs. The better solution should be evaluated before including it in the policy. Currently, the IT world is trying to determine how the Apple iPhone will fit into the corporate infrastructure as an acceptable mobile device. Its place will most certainly be defined.

Wireless access will continue to be a challenge since data rates, coverage, availability, and quality are often driven by the technology of choice. Currently, cellular carriers have a variety of offerings under the technology headings of FDMA, TDMA, and CDMA. The 2G arena has offerings under the headings of GPRS, EDGE, and 1xRTT. The 3G arena has UMTS and cdma2000 as international standard offerings. Add to this the current state of Wi-Fi and WiMAX and there are numerous access options. Unfortunately there is no one correct choice that meets all the mobility needs.

Seamless mobility requires seamless roaming among all of the various access options; we are not there yet. Users find it irritating to lose a voice call because they moved out of range of their carrier, and there is no roaming partner. In data such problems can mean the ultimate demise of the mobility solution. Quite often, roaming problems are not due to technology problems but to geography and economics. The seminal question will always be, “Who will pay for this service?”

Transport options are evolving from the old circuit-switched model to a packet-switched model. In the packet-switched realm we see the dominance of IP transport networks. Unfortunately, native IP does not support the quality of service (QoS) that might be needed for the mobile solution. To enhance IP, carriers have added Multiprotocol Label Switching (MPLS) as a means of delivering QoS that meets the needs of the user application. MPLS-enabled IP infrastructures will continue to evolve and play a significant role in mobile communication solutions.

Mobile applications are available in many shapes and sizes from numerous vendors. The visual lists some mobile software vendors. Visit their websites to view what they have to offer. Be aware that the vendors can vary greatly in their philosophies related to mobility.

## Security—A Cornerstone of Mobility

There are three primary security concerns around mobility. First, a security hole in a wireless network can have a devastating effect on the wired network. Second, wireless is radio and radio waves traverse the wide open spaces. Anyone with a radio receiver and knowledge of the frequencies being used can intercept wireless communications. Third, technology can help with security but the user must be part of the solution. We are all guilty of discussing business at the airport within earshot of dozens of people. While nothing bad might happen based on overhearing a voice conversation, the repercussions of stolen data from a mobile device could disable a network and the business.

In addition, three big challenges come to the forefront when mobility is introduced. First is the proliferation of non-certified devices. Certification in these cases comes from the mobility policy. If it is not in the mobility policy, it should not be allowed. Any deviation from a strict policy could lead to a network overrun by rogue devices.

Second, users need to be educated about the policy, acceptable use of mobile devices, and how to efficient use of the mobile applications. Do not assume that every cell phone user knows how to



access the Internet via the cell phone. Assume that everyone needs to be educated and then be pleasantly surprised when you have a much smaller educational challenge.

Third, fixed mobile convergence means that these networks are no longer isolated from each other. They live and breathe together and thus adequately meet each other's needs. Remember that passwords on a PDA can compromise the entire enterprise network.

The wireless MAN/WAN environment contains many security threats. For example the transmission of unencrypted identification information over the air interface might make users visible to hackers. This was one of the major problems with early cell phones, which new authentication procedures fixed. Another problem arises if the mobile user device is subjected to a denial of service attack. Remember the mobile device is just like any other client so it could be attacked by a hacker. The denial of service attack could drain the battery (an inconvenience) or create over-billing situations (an expensive inconvenience).

Anyone impersonating someone else can abuse the other person's network privileges. The other individual would be blamed and perhaps lose network and application access. Along these same lines, someone impersonating another individual could access confidential information on corporate servers and compromise the business operations. Perhaps most annoying to the user and most problematic to the business is the simple loss or theft of wireless devices. Individuals often have business information on their cell phones, PDAs, or laptops, and most individuals do not lock these devices.

The wireless LAN has its own set of security threats. The most prevalent is the problem of radio frequency eavesdropping. Since the 802.11 family of protocols uses a small number of frequencies, it is easy to scan all of the frequencies. In fact, the wireless card in many laptops does this automatically when it powers up. The hacker term for RF spying is called war driving; all the hacker needs is a laptop with a wireless, high-gain antenna made from a Pringles potato chip can and a GPS device. After scanning a neighborhood, the hacker can create a map of places that have unsecured wireless LANs. In major cities, sometimes the hacker will mark the location with chalk, a process called war chalking. (The term is derived from the practice of hobos marking houses that were friendly to them with chalk.)

While the wireless LAN can be made secure, many times security and encryption are turned off or the default values are not changed. Everyone knows that the SSID for a Linksys router is linksys and password is admin. There are also rogue devices that provide for open access to a wireless LAN. This can lead to theft of services but can also open up a wireless device to a hacker. Individuals using an unsecured wireless LAN (that they do not own) can be prosecuted for "theft of services."

## Security Policy and Mobility Policy

We advocate a close relationship between the security policy and mobility policy. In fact, it may be best for the mobility policy to be a component of the security policy, which ensures that an integrated corporate policy is maintained. These policies must address not only the policy but also the people, process, and technology.

The overall security policy must define the issues below.



- The confidentiality needs of the business must be defined as well as the type of encryption that must be used to adequately secure the data and still make it available to authorized users.
- The authentication methods and procedures must be defined as well as the procedures to be followed when a user is denied access. Access can be denied if a hacker is randomly attempting to get in or a legitimate user has forgotten the password.
- The data protection strategies for all mobile users must be well-defined and related to when and how these strategies must be used.
- The security tools must be made available along with the appropriate documentation on their implementation and appropriate use.
- The enforcement policy must also be spelled out and any job-affecting parts of the policy should be memorialized in the corporate employee handbook.

To summarize the challenge of putting it all together, we offer the following tips.

- Focus on the business needs since mobility can be expensive and no business can afford to spend money on a solution in search of a problem.
- Planning, planning, and more planning wins the day. The planning process must involve all of the stakeholders; this means the users must have a say in the plan. Without their support, the project will most often fail.
- Develop the strategy first and then implement that strategy. This may seem obvious but all too often a run and gun approach is used without a strategy, or the strategy is ignored and ad hoc components are tossed in because they seemed like a good idea at the time.
- While wireless may be at the core of mobility, the whole solution is much more (e.g., applications, security, user interfaces and handheld devices).
- The selection of the right carrier(s) for access and transport is critical as is the choice of hardware, software, and middleware vendor(s).
- The issues surrounding return on investment (ROI) and total cost of ownership (TCO) need to be addressed. But, be reasonable and see how the solution costs play out over three years. Also attempt to quantify the intangibles like productivity, creativity, and convenience.
- Any solution must have a security policy and a mobility policy.

While these tips will not in and of themselves ensure a successful mobile solution, they will provide a road map for your trip to mobility.



### **About Paul Whalen**

*Paul Whalen has over 25 years' experience in telecommunications as an instructor and consultant. Over the past several years, he has used his expertise in wireless communications and business strategy to create and deliver courses that focus on the issues facing companies involved in the wireless communications marketplace. Business leaders rely on Paul's insights as they determine their business and technology strategies. His knowledge of convergence, both voice and data and wireline and wireless, has allowed him to create a variety of business strategies. As CEO of Hill Associates, he also brings a strong sense of business reality to the classroom. His in-depth knowledge of the telecommunications regulatory scene allows him to put a strategy into the correct regulatory perspective. Paul is also well versed in broadband communications and the IBM networking technologies.*

*A dynamic and energetic presenter with a broad perspective on technology and business, Paul is capable of dealing with technology issues and learning issues in the classroom. He has developed educational programs for technical and non-technical audiences that range from five days to over sixty days. He has been with Hill Associates since 1984. Before stepping into the role of CEO, Paul served as MTS, Senior MTS, CFO, the Director of Sales and Marketing, and the Director of Planning.*

*Prior to joining Hill Associates, he was the founder and CEO of Interactive Computing of Vermont and the Associate Director of Academic Computing as well as a lecturer in Computer Science at the University of Vermont. He holds a B.Sc. from Carnegie Mellon University, M.Sc. and Ph.D. in Mechanical Engineering from the University of Vermont.*

*Paul is a registered Professional Engineer in Vermont. He is a member of the American Society of Mechanical Engineers, the National Society of Professional Engineers, and the Vermont Society of Professional Engineers. His hobbies include hiking, canoeing, camping, antique collection and restoration, reading, and traveling.*

### **About Hill Associates, Inc.**

*Hill Associates is a premier training and marketing services firm specializing in the field of telecommunications. For over 20 years, we have demystified the complex world of data networking, network security, and telephony. Our clients leverage our expertise, content, and development capabilities to create customized solutions that bring benefit and deliver results. Today, in addition to knowledge-based technology courses, we offer solution selling, a variety of e-learning options, and hands-on workshops. Our Marketing Services bring industry and subject matter experts to your sales events, customer meetings, Webinars, and white papers.*

*At Hill Associates, our consultative approach addresses each client's unique needs and challenges. Whether it's executive consulting, training for field teams, network engineers or corporate IT, or marketing programs designed to bring knowledge to your prospects, Hill Associates delivers your solution. Come visit us at [www.hill.com](http://www.hill.com) and see what we can do for you.*



Copyright © by Hill Associates, Inc. All Rights Reserved.

No part of these materials may be reproduced, stored, presented or transmitted in any form or by any means, electronic, mechanical, photocopy, recording, or otherwise, without the written consent of Hill Associates, Inc. prior to use.

Request for permission to use any portion of these materials should be sent to:

Hill Associates, Inc.

Attn: Copyright Coordinator

106 Highpoint Center

Colchester, VT 05446

USA

Phone 802-655-0940

Fax 802-655-7974

E-mail [info@hill.com](mailto:info@hill.com)

Web Site [www.hill.com](http://www.hill.com)

Hill Associates, What Training Should Be, ExperTech Series, and FAQ Finder are either trademarks or registered marks of Hill Associates, Inc.

The company names, products, and services mentioned in our materials are or may be trademarks or registered trademarks, and are the property of their respective owners. Any names, products or services mentioned are for informational or educational purposes only and do not suggest or imply affiliation or sponsorship.

Although the mention, recommendation, or comparison of any name, product or service within this material is an expressed opinion by an industry expert, it should not be assumed as fact.