February | 09

Five Steps to Effective Mobile Management

Michael F. Finneran

dBrn Associates, Inc. 189 Curtis Road, Woodmere, NY 11598 516.569.4557

It is no secret that enterprise initiatives for fixed mobile convergence (FMC) and mobile unified communications (UC) are not being deployed at a rate commensurate with the hype. Embarrassingly, few users get beyond the most rudimentary mobility solutions: cell phones, push email, and a wireless LAN for mobile data access. It appears that mobility remains the strategic development that is least likely to be used strategically. While some of the blame can be attributed to product deficiencies, the main reason these initiatives are not moving forward is that enterprises are simply not organized to capitalize on the potential.

The biggest obstacle to enterprises attempting to deploy mobile applications is that they have different groups responsible for the different forms of mobility and no incentive for them to coordinate their activities. Enterprises have organized around technologies, and the two major components of that are cellular and Wi-Fi. In such an environment it is highly unlikely that anyone is going to propose the idea of eliminating Sprint Nextel walkie-talkie phones with a push-to-talk system that operates over the wireless LAN.

Therein lies the biggest problem with moving forward on a meaningful mobility initiative. We have people responsible for cellular and people responsible for wireless LAN, but we don't have anyone responsible for "mobility". In this paper we will lay out the five primary steps an enterprise should take to establish meaningful mobility plan. They are:

1. Organize Around Mobility
2. Quantify Networks, Users, and Expenditures
3. Take Control: Define the Policy
4. Initiate Near-Term Improvements
5. Start Thinking Strategically

Different organizations will be at different stages with regard to each of these, and those who have already addressed some of the preliminary issues will be able to move ahead more quickly. However, the key will be to organize around "mobility" not mobile technologies.

1. Organize Around Mobility

The first step in becoming proactive about mobility and mobile UC is to put someone in charge of it and define what they are in charge of. When we're dealing with wireless networking, the emphasis should be on networking and the function should be located in the IT or networking department reporting up through the CIO or CTO. Of course, mobility will cut across several existing organizational boundaries so it will be important to correctly define those inter-group relationships. Wired voice systems will have an impact on fixed mobile convergence. Email and data access systems may have to be

modified to support mobile devices. Wireless introduces a number of potential security vulnerabilities so a strong link to the security group will be essential.

The two core groups to be included under mobility are cellular and wireless LAN. Cellular services are typically managed by a purchasing group whose primary function is to select the best mix of carriers and service plans to provide cost-effective cellular voice and data services. Their focus is cost management, not applications or network design. The group responsible for implementing and maintaining the wireless LAN is already part of the lT or networking department, however they are not involved with cellular services, voice is largely out of their purview, and they focus primarily on local wireless data. Health care may be the exception to that where there are significant deployments of voice over WLAN systems.

For many organizations, mobility extends beyond WLANs and cellular, and you should consider all of the applications of wireless technology to determine how they should be addressed. Along with push-to-talk services, traditional walkie-talkie or trunk radio systems if they are used should certainly be part of the plan. In medical and manufacturing environments, there may be a number of devices that use various forms of radio transmission, and even though those devices fall under the control of other departments, the potential for interference requires that there be some interface with the mobility group.

Short-range radio devices like Bluetooth, radio frequency identification (RFID), and even wireless keyboards and speakerphones should also be addressed. Many would say that these are not “communication” technologies, but as they use radio frequency transmission they are also possible sources for interference. Further, many of these now pose potential security threats, and so they should not be overlooked.

Organizations like electric utilities and railroads often build private transmission networks using point-to-point microwave or satellite communications. As they support non-mobile applications, these systems are typically grouped with the wired networks. However, the people who manage them often have the most extensive technical background in radio. While they may have little or no experience with cellular or wireless LAN technologies, those deficiencies can be addressed with additional training. With the organization’s best understanding of the general principles of radio transmission, antenna systems and other RF issues those in-house experts can be invaluable in assisting on other mobility initiatives.

Correctly implemented, virtually any wireless technology is going to allow the user to be mobile. However, unless we organize around the concept of “mobility”, we will have people shopping for products, not for solutions. The old saw holds true: to a hammer, every problem looks like a nail. We need to be thinking about the job of joining boards together, not assuming hammers and nails are always the best option.

2. Quantify Networks, Users, and Expenditures

Once the mobility group is established, it's time to determine what they are actually in charge of. That calls for a systematic review the existing wireless networks, users, and expenditures with a view toward capturing the organization's overall capabilities and expenditures in the mobility area.

In most organizations, cellular services will represent the biggest part of mobility spending; some estimates put cellular at 25% of the total network budget. Many large organizations have already taken steps to get their cellular costs under control. For those who have not, this can easily be a yearlong effort. That will most certainly be the case if they are still allowing users to purchase their own cellular plans and reimbursing them through expense vouchers. A few years back that was the standard operating procedure, but it virtually eliminated the possibility of volume discounts, special service terms, corporate standards, enforceable security policies, or anything else that smacks of management. Any organization that is still operating in that mode is two-steps behind in getting their mobility under control.

Organizations that have gotten their cellular spend in a manageable form will typically have contracts with a selected number of carriers and implemented review procedures to ensure that those services continue to be provided in a cost-effective fashion. Those review procedures should also ensure policy compliance and eliminate unnecessary waste (e.g. excessive after-hours texting, directory assistance calls, identifying cell phones with zero use, etc). However, all of that deals with cost control, not networking or integration.

While cellular will most likely be the biggest element in the mobility budget, it is important not to ignore the rest. The wireless inventory should include WLANs (headquarters and remote), walkie-talkie systems, point-to-point microwave, and any other device that depends RF transmission.

Again, we should not have people responsible for managing "cellular" or "Wi-Fi", but for managing "mobility". In evaluating mobility solutions we will be doing a disservice to the organization if we constrain our search space to one set of options that one set of suppliers has to offer. We have to begin to look at mobility requirements in terms of applications (voice, PTT, email, data access), range and frequency of mobility (in-building/campus, nationwide, worldwide), performance and reliability requirements, and then look for the best and most cost effective way of providing those capabilities.

3. Take Control: Define the Policy

The first step in becoming proactive with regard to mobility is the development of a policy that describes your organizational objectives, acceptable use practices, and required security measures. The policy should also spell out the type of wireless devices and services will be provided for each job function and how numbers will be assigned/ported. Most users do not require "the latest and greatest" when it comes to mobile devices, and devices that cannot be secured or managed should not be considered.

That mobile acceptable use policy should address the full range of mobile devices including:

- Laptops and Ultra-Mobile PCs
- Cell phones/smartphones/mobile PDAs
- Home PCs used for corporate network access
- Any thumb drive, MP3 player, or other device capable of storing and transporting corporate data

The definition of user responsibilities regarding acceptable use, security and safety are also key. Any user provided with a corporate mobile device should have to attend a training session where the requirements are reviewed, and sign a statement acknowledging their responsibilities under the policy.

A meaningful policy also includes penalties for non-compliance so a full buy-in from human resources and executive management is essential. Some requirements should be unambiguous like an outright prohibition against storing any corporate data on a personally owned device. Security compliance is critically important, but company liability is a growing concern. If an employee is involved in a car accident while talking on a company phone on company business, the liability will certainly be tied back to the business. There must be a no-exceptions ban on cellular voice or text use while operating a vehicle.

Beyond the cost control and policy establishment, there are a number of essential management systems that should be in place.

• Ordering/Delivery: While there will be a central mobility group, you will also require trained local administrators to deal directly with end users. Those administrators may be assigned on a location or a department basis, and all ordering and provisioning should be routed through them. Do not overlook security issues in the ordering procedures, as there have been cases of wireless administrators ordering corporate cell phones, selling them as a sideline business, and then approving the expenditures!

- Security: For every type of mobile device and service there should be a specification for the security measures that must be in place and a procedure for ensuring compliance. The watchword in security is: “Trust is nice, but automated monitoring works better”. It is critically important that those procedures address all mobile devices including smartphones and PDAs. Those devices have operating systems and software and so are vulnerable to viruses, worms, and malware. They also have considerable data storage so onboard encryption and power-on passwords are mandatory. Given the sensitive nature of the information, remote lock and wipe should be available, and employees must understand that they need to contact IT immediately if they think the device is lost. Organizations will typically have provisioning, lock-down, and upgrade cycles for laptops, but the same type of systems must be developed for all mobile devices.

- Help Desk and Troubleshooting: The help desk personnel will need to be trained to field trouble calls from mobile users, and they will have to be retrained when new devices are added to the supported equipment list.

- Equipment Insurance and Upgrades: Cellular contracts generally call for equipment upgrades on a 24-month cycle, and you will need a system to track the devices that are eligible for upgrades. Equipment insurance is also important, but be aware that many users “lose” their devices when they get tired of them. You should consider a corporate policy that limits users to one “lost” or “broken” unit per 24-month period and specifies that any additional replacements will be the user’s responsibility.

- Repair and Back-up Devices: If a device needs to be repaired, there should be a mechanism to deliver a replacement device within one business day. Those requests might be routed through the department’s mobility administrator, but there should also be an emergency 24X7 replacement procedure for traveling users. The importance of backing-up files regularly can be come painfully evident when the user has to switch to that back-up device.

- Employee Termination Procedures: If an employee is terminated, their mobile device(s) should be collected along with their ID card and corporate credit card. Many organizations still have rather haphazard termination procedures that fail to cancel user passwords when an employee is terminated.

4. Initiate Near-Term Improvements

With a mobility policy in place, procedures to handle day-to-day tasks and a cellular contract that is monitored routinely, you are now ready to start taking control of your mobility. To get the ball rolling you should begin a systematic review of mobile applications to determine if there are better mechanisms to meet those requirements. Many of those ideas will likely crop up as you go through the exercise of inventorying your mobile assets.

Typically the biggest savings will come from moving applications from cellular to wired or WLAN services. International cellular calling is outrageously expensive, so that is typically a prime target. IP soft phones for international travelers used over either wired or WLAN Internet connections are a far cheaper option, but you must pay attention to security if WLAN access is used. However, there are clients that can provide secure access in virtually any wireless environment. Remember, we should also be looking at reducing cellular costs for our employees visiting from overseas offices.

Generally what you will find is that when you put everyone who is involved with mobility under the same umbrella, they will start coming up with ideas for how to do things better. It is important to reinforce the message that they are now responsible for mobility, not for “cell phones”.

5. Start Thinking Strategically

Once you have worked through the “quick kills”, it’s time to get serious about using mobility to your advantage. Forward thinking organizations are looking at how they can make the best use of mobility to foster their overall business objectives. In the move to unified communications and communications enabled business processes, mobility will be a key component. Virtually all IP PBXs and UC platforms support some form of mobility, though it is generally the user’s responsibility to determine which capabilities are the best fit for each application.

Marty Parker of UniComm Consulting defines unified communications as “Communications integrated to optimize business processes.” It is most useful to divide mobile UC applications into two groups:

1. User Solutions: This refers to generic productivity benefits that can be applied to a wide population of users. Those solutions can be categorized as UC- User benefits or UC-U.
2. Mobile Communications Enabled Business Processes (mCEBP): Mobility can also be added to any variety of communications intensive business processes. Those solutions can be categorized as UC- Business benefits or UC-B.

With regard to UC-U, integrating the desk phone with the right mobile device can produce significant benefits.

- Improved Accessibility: Mobility leads to faster decision making, as critical people can be accessible continuously via one number and one voicemail.
- Increased User Productivity: Greater productivity for mobile users by extending presence, collaboration, visual voicemail and other UC features to the mobile device.
- Business Control of Telephone Numbers: In most business situations, customers and other business contacts should be calling a business number, not a user's personal cellular number. That is particularly true of calls to customer-facing personnel like salespeople who might leave and go to work for a competitor. In designing a mobility solution you must pay attention to the value of business contacts and to how numbers are assigned, ported, and controlled.
- Better Indoor Coverage: Indoor coverage can be addressed with a voice-capable wireless LAN or a cellular distributed antenna system (DAS), but it is important to remember that there are no airtime charges for WLAN calls.
- Cost Savings: It is important to look for solutions that support the widest range of mobile network options. If the user is in the building, you should be able to reach them over the wireless LAN for either a traditional voice call or a push-to-talk capability without having to use cellular plan minutes.

UC-B applications have an even greater potential to deliver quantifiable improvements in ROI. Companies like Federal Express and UPS have demonstrated how the incorporation of mobile data collection has revolutionized the package delivery business. Similar opportunities exist for countless businesses that have employees who work out of the office or simply perform their tasks while away from their desks. Determining how to incorporate mobile communications into those processes should be a major imperative for the organization.

When the mobility team is assembled, they should meet with business managers to discuss how mobility can improve their operations. That should not be limited to managers with personnel operating outside of the building, as in-building mobile access can be equally important. In moving into these areas your philosophy should be to start small, ensure your management systems are sound, learn by doing, and then move on to bigger and more important projects.

Conclusion

CIOs have come to realize that mobility is one of the cornerstones of unified communications. The networks of the future will have to extend that same form of rich communications from the desktop to the mobile user and integrate them into the overall business process. The fundamental disconnect is that we haven't trained anyone in how to do that, and more importantly, we haven't identified anyone who would actually be responsible for bringing it about. Mobility initiatives like fixed mobile convergence and mobile UC are stalled because there's nobody equipped and responsible for defining the requirements, evaluating the full range of options, and managing a mobile network implementation.

Cellular carriers will continue to sell cellular services and WLAN companies will continue to sell WLANs. If organizations hope to capitalize on the new wave of mobility and start to use mobile solutions strategically to improve business performance, they're going to have to get themselves organized and take mobility matters into their own hands. While everyone gives lip service to the importance of mobility, that initiative is currently organized in the way that is least likely to yield an integrated mobility solution. Getting cellular expenditures under control is the first step, but the process must be followed through to address the whole spectrum of mobility services.

Consumers are already seeing the benefits of adding mobility to their daily lives, and those people are expecting that same level of convenience in their business lives. Enterprises will have to step up to ensure that those same mobile capabilities can be delivered in the secure, manageable fashion required for business.

dBrn Associates, Inc. is an independent consulting/analyst firm specializing in wireless networks and technologies.

Michael Finneran can be reached at mfinneran@dbrnassociates.com, and his training programs in wireless and mobility are offered through Telecom+UC Training.