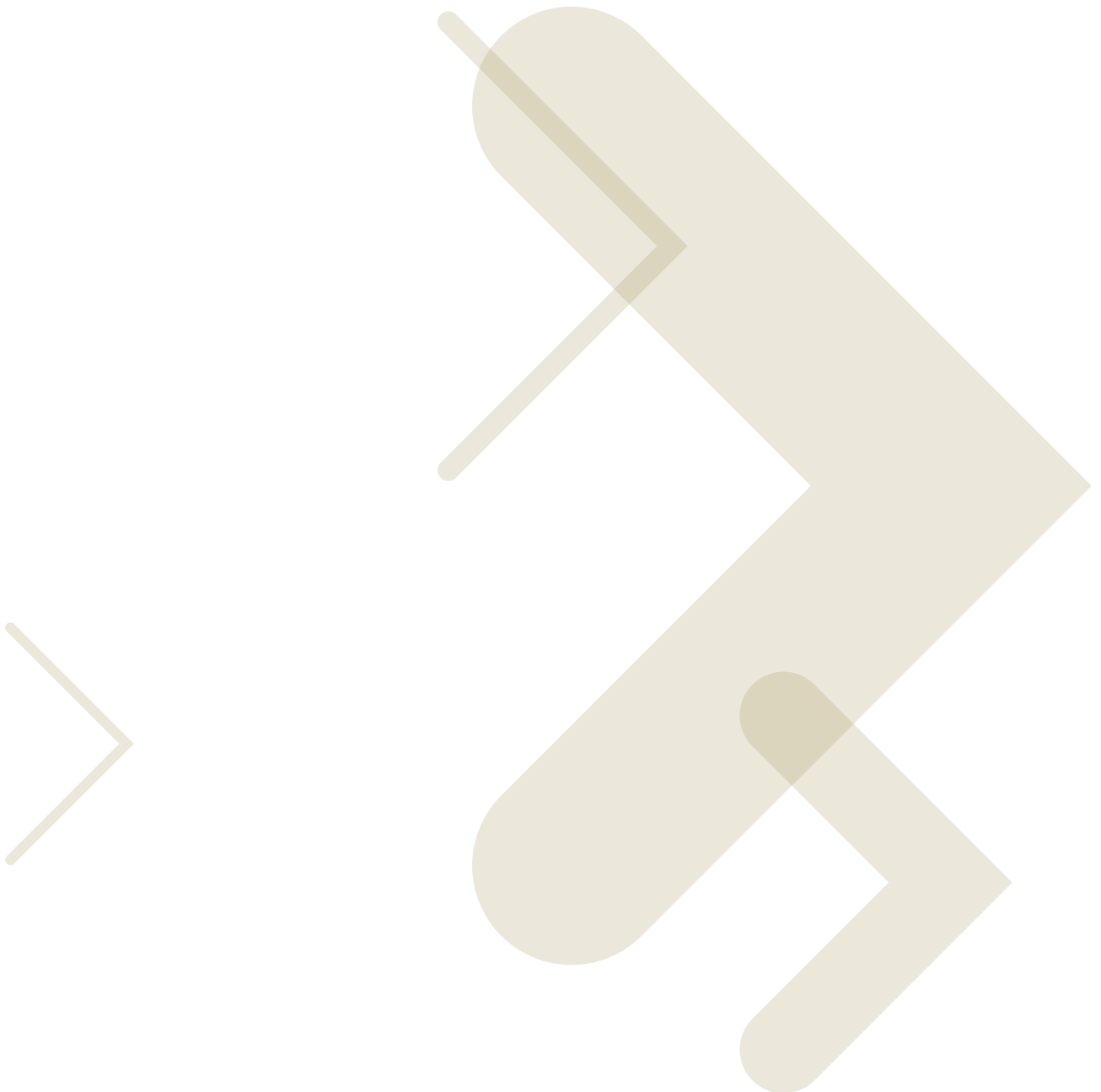




Building a Unified Enterprise Mobility Strategy

For Government Agencies



This paper discusses the challenges of managing multiple networks to access mobile data. The following pages outline a step-by-step approach to developing a unified enterprise mobility strategy that will enable a more cost-effective and efficient delivery of network connectivity to a larger mobile government workforce.

Executive summary

In today's federal, state and local government agencies, it is no longer economically feasible for IT organizations to separately manage multiple networks to access mobile data. Exponentially scalable infrastructure, such as sprawling access points and arrays of RFID readers, is prohibitively expensive in terms of manpower and operations costs for most organizations. Also, maintaining disparate pools of data results in a missed opportunity for government agencies to enable a wide range of workers to act as efficiently as possible — as well as access the most up-to-date data to support better decision-making and better outcomes.

Instead, government agencies must develop a unified enterprise mobility strategy that brings the management of multiple RF technologies into a single interface, optimizes the performance of agency applications in the mobile environment and allows for seamless bridging of data between wired and wireless networks. This strategic next-generation approach ensures that advanced mobile applications can be rolled out across cellular, RFID, Wi-Fi or broadband without complex management headaches. Having a unified strategy sets the stage for IT to take advantage of exciting new technologies such as WiMAX and Fixed Mobile Convergence (FMC) that will enable more cost-effective and efficient delivery of network connectivity to a larger mobile workforce.

With a converged approach, IT can streamline infrastructure costs and improve overall network and application performance. A single point of management allows IT groups to optimize wired and wireless voice, video and data traffic, further lowering the total cost of ownership.

By implementing a unified enterprise mobility strategy, organizations will be able to create an environment that allows for secure anytime, anywhere access to mission-critical data.

IT organizations are under pressure to carry out two goals: reduce costs and increase operational efficiencies. In most areas, they've been able to accomplish this through centralization, consolidation and streamlining of resources. However, one area that still has IT groups spending time and money is deploying and managing mobility solutions in the enterprise.

Mobility, which today is based on an array of wireless technologies, poses significant challenges for IT. The myriad RF signaling technologies, such as cellular, RFID, Wi-Fi and WiMAX, are kept separate, leading to islands of information and management systems within an agency.

The high cost associated with the lack of end-to-end visibility into all the data gathered in the organization is unacceptable. Take for example ERP networks. If an agency cannot access ERP data over a mobile system, then they've wasted a great part of their investment. Also, it's no longer tenable to have various entities deploying and managing RF data pools away from the core IT network. Doing so is a lost opportunity for IT to accomplish the mission of reducing costs and ensuring information security.

In the same way that servers and storage are moving toward centralization and consolidation, all wireless networking must be unified under the umbrella of IT. This allows for tighter security, easier and more cohesive management, and overall cost savings of human and monetary resources. Agencies will also be able to take advantage of cutting-edge applications across a host of RF networks and gain invaluable insight into data that was once stranded in isolated pools.

Understanding the challenge of wireless in the enterprise

To say mobility in the enterprise is on the rise is a severe understatement. According to recent studies, there are an estimated 639 million mobile workers worldwide. These users expect mobility and flexibility no matter where they choose to work. Regardless of device or location, they want LAN-like access to mission-critical applications. And with so many workers in the field away from headquarters, directors are demanding that IT deliver this in a secure and cost-effective manner.

However, challenges abound in carrying out this mission. Not the least of which is the difficulty in bringing together the vast array of wireless islands that exist throughout an organization. Over the past years, departments, small offices, remote offices and telecommuters have all implemented RF signaling technologies on their own, bypassing IT's influence. From 802.11 networks to voice over IP phones to smartphones and handhelds, users have rolled out wireless piecemeal, leaving IT to play catchup. Chances are Wi-Fi, wireless broadband technologies such as EVDO, and RFID all exist in the enterprise, but to the detriment of the organization they have not been put to the same standards of security, quality, management, and performance oversight as other critical network elements.

There is no clear path of ownership for these networks, leading to poor upgrade paths, severe performance hits and immense security vulnerabilities. More noticeably, ad-hoc wireless networks leave data disconnected from other information in the enterprise. Organizations are unable to gain intelligence from user-entered data, information gathered from RFID tags, and other important resources.

Ad-hoc wireless networks also significantly impede IT's ability to adopt new applications, services and hardware. Without unified oversight and management, IT often misses the chance to roll out enhanced networks that would boost productivity and allow anywhere, anytime access to critical data.

Security presents an obstacle for IT groups, especially shoring up wireless networks across the organization. In most cases, IT is unaware

of all the RF networks that exist in the enterprise, leaving holes for hackers and others to access corporate assets. For those outside of IT to implement security is difficult as the standards can be confusing. Determining if Wi-Fi Protected Access (WPA) or WPA2 protocol is the best and whether to implement 802.1x, access control lists or virtual private networking (VPN) are complicated decisions that can be ill-served if not part of an enterprise-wide deployment strategy.

Finally, ad-hoc networks put IT at a disadvantage in terms of network performance management and the overall end-user experience. Without a centralized view, IT cannot monitor and optimize the network to improve response times, leaving users frustrated because of poor application access. With typically thousands of access points to upgrade with each change in the network, ad-hoc networks severely drain IT's human and monetary resources.

Feeding the need for mobile access

At its most basic, the true value in all types of RF signaling is to allow critical real-time access to information for users. It should not matter if users are accessing the network from cell phones, laptops, handhelds, voice over IP phones, or any other device. The wireless network should be able to accommodate true anytime, anywhere access without jeopardizing the security of the overall network.

On the back end, IT requires a unified or common view of all mobile elements of the network. There cannot be a separate console for managing Wi-Fi networks and another for RFID and another for cellular. Instead, deployment and management decisions should be able to be based on a single view of the enterprise-wide wireless network.

Wireless management must be complimentary to wired management in a manner that is familiar to IT. IT cannot have a "wireless" staff and a "wired" staff to handle LAN issues. This would be counter to the goal of reducing costs. Wireless management should be heavily focused on the optimization of network performance needed to support mobility. This increases efficiency, further reducing the total cost of ownership of the wireless network.

Building a case for a unified strategy

A unified enterprise mobility strategy achieves all of these goals. It makes wireless access methods transparent to the user. Terms such as Wi-Fi, EVDO, mesh and RFID become unimportant to those accessing the network. Instead, they can focus on the intelligence they are trying to glean from access to the data.

Once this transparency is achieved, exciting new technologies such as WiMAX, which enables wireless networks over long distances; ZigBee, which addresses low-power wireless networking; Fixed Mobile Convergence (FMC), which allows for the melding of cellular and Wi-Fi networks; and future versions of 802.11 can all be easily deployed throughout the enterprise without disruption to users or a significant incremental investment in infrastructure management.

Bringing together all enterprise wireless resources, no matter how far flung they are, enables IT to develop a top-notch device and RF management strategy. In most organizations, users support their own devices or work with service providers in a piecemeal fashion, significantly increasing expenses. Also, because of poor RF planning, wireless networks can suffer poor performance that goes largely unattended.

With a unified enterprise mobility strategy, IT can streamline device management, ensuring that users are equipped with appropriate hardware, the latest software versions and necessary security patches. IT can also take advantage of emerging standards, such as FMC, to reduce costs by enabling the merging of voice over Wi-Fi and cell calls. Users no longer will be forced to be on the cell network, wasting minutes, if they are in range of a Wi-Fi network.

These improvements allow IT to be proactive, which in turn, dramatically reduces the administration burden seen today. For instance, if devices are upgraded and serviced on a scheduled basis, users will be less likely to call the help desk to report handheld access problems. If coverage issues such as interference for Wi-Fi, cellular and RFID signals are considered before hardware and service programs are purchased, networks are better able to perform at optimal levels - enabling IT to focus on delivering applications rather than the infrastructure.

A unified enterprise mobility strategy leads to heightened quality of service, whether the traffic crossing the network is voice, video or data. IT, with a single view of all network elements, can easily adjust the network to account for jitter and latency or heavy traffic patterns. Access controls, prioritization and other traditional network optimization tools can be used across the unified network to ensure that information is delivered in the proper fashion.

With a unified strategy, mobile applications are able to leverage a cross-section of RF technologies. For example locationing or asset tracking can use a combination of Wi-Fi, RFID and other technologies such as ZigBee to deliver much more accurate results and more value to the agency. This is a great benefit of the unified architecture.

Users also gain something they've been missing — persistent network connectivity. By melding all RF signaling tools into a single managed network, IT can support persistent connectivity across multiple wireless networks based on the same user credentials. Users no longer have to reconnect for each network they encounter and can stay on their calls or maintain their Internet sessions without suffering dropped connections. This is invaluable for users that move around campuses, work in various buildings or are constantly on the go.

Finally, unified enterprise mobility affords superior wireless security for organizations. Agencies don't have to rely on ad-hoc managers to flip the switch on WPA or other security tools. Instead, advanced security — including role-based wired and wireless firewalls, wireless intrusion protection system (IPS), virtual private networks, WPA2 and 802.11x — can be layered in a sophisticated manner that ensures the protection of voice, video and data traffic at the same level achieved on wired LANs. An overlay security monitoring and intrusion protection mechanism can be implemented without impacting the infrastructure performance. Patches and upgrades can be applied in a timely and efficient manner, ensuring that there are no holes in the network at any time.

A unified enterprise mobility strategy is a powerful tool for organizations large and small. It saves IT organizations from wasting valuable resources on being reactive and allows them to think of unique ways to offer real-time access to applications that add to the bottom line.

Creating your own unified strategy

Developing a unified enterprise mobility strategy is a simple task that every organization should undertake. The benefits are innumerable and immediately IT will be seen as a strategic part of the organization, focused on cost-cutting and enhanced productivity.

The first step is to determine where all your ad-hoc wireless networks exist. You should use detection devices throughout the network to pick up RF signaling frequencies and create an inventory of the Wi-Fi, mesh and RFID networks you find. Make sure these match up to departments and are viable networks, not rogue access points.

For cellular access, work with your agency's finance team, unit leaders and service providers to inventory all handhelds, smartphones and other service-based devices in use throughout the enterprise. Make sure that all devices are mapped to current users and have not been orphaned by past employees.

Next, consider the hardware and software that is being used in cellular, RFID, mesh and Wi-Fi deployments. Do they match the requirements of the users? Are they up to date on software versions and patching? Are the service contracts in line with your carrier contracts?

Check your access points. Are they mapped correctly? Are they suffering interference or poor performance due to positioning? Make sure to carry out automated site survey and access point analysis to guarantee accurate placement and optimal configurations.

As you begin to bring wireless networks under the umbrella of IT, make sure you understand what the goal is for access. For instance, how heavy are the applications that users want to access? Are they just doing e-mail or do they use the network for voice and video? Also are they just serving up Web pages or are they tapping into large file servers such as CAD/CAM design stores or medical imagery? These considerations will help you create a well-designed wireless network.

You should also factor in your users. Do they roam within the building, among buildings, across town or around the world? This will determine what types of network architecture to roll out. For instance, if your users are mostly within a building, then you can concentrate your efforts on Wi-Fi deployments. However, if they roam even just building to building, you'll want to consider how to bridge Wi-Fi traffic in a "mesh" network and enable Layer 3 mobility to make that roaming seamless. If the users require network access while on the road, consider technologies such as FMC that supports seamless handoffs between cellular and Wi-Fi networks and promises to minimize costs.

When looking at the myriad architectures, remember to be flexible. Your wireless network should be able to be integrated in both Layer 2 or Layer 3 designs, and enable seamless mobility across network boundaries without additional hardware or client software burden. In addition, the infrastructure needs to support wireless bridging (or mesh capabilities) to extend Wi-Fi support beyond the four walls and at the same time ensuring maximum security and Quality of Service (QoS). This becomes important, for instance, when bridging traffic across buildings or for easily deploying networks across a large campus.

Add RF management for all your signaling methods. You'll want to manage Wi-Fi, RFID, mesh and cellular traffic across the board, and be able to tweak traffic on the fly. For instance, if you notice interference within an RFID network, you need the ability to adjust how the sensors and tags are interacting without reconfiguring the entire network.

As you move away from the core of the network, out to the users, develop a strategy for managing and monitoring devices. Many users are accessing and storing mission-critical data over these devices. This puts an organization at risk when the employee leaves or the device is broken or lost. Make sure you roll out tools that allow you to remotely block or erase the device as soon as a problem is reported.

Also, with compliance creating such a heavy burden for IT, you'll need a way to routinely extract data from devices and store them centrally. Configure your management tools to regularly scan remote devices and ensure your storage pools are kept up-to-date. A final piece to device management is implementing automated tools that manage password protection, and push security patches and updated software out to devices.

Security is mission-critical for government networks. With a comprehensive suite of best-in-class tools, wireless networks can provide a level of security that surpasses that of the wired network counterparts. Wireless infrastructure that is FIPS 140-2 and CC EAL4 certified meets all the security requirements of cryptographic modules. Dedicated wireless intrusion protection systems enable around the clock instant detection and elimination of any wired or wireless threats. A role-based combination wired and wireless firewall completely secures the network against attacks and unauthorized access on either the wired or wireless networks, protecting, wired-to-wireless, wireless-to-wired and wireless-to-wireless traffic — while the ability to define access rights by user and location provides granular control over network access. Add in the availability of robust 802.1x authentication and WPA2 (AES encryption) and you have all the tools you need to create a multi-layered approach to security that is capable of meeting stringent government network security requirements.

As you build your enterprise mobility strategy, consider not just today's wireless technologies, but also those that are rapidly following on their heels. For instance, you can plan today for FMC so that cellular and Wi-Fi calls are interchanged seamlessly. You can also map out your WiMAX plans and develop a foundation for future versions of 802.11.

It's imperative to look beyond the physical layout of the infrastructure to how that infrastructure will support next-generation applications. Voice, video and data will all be merged in the future on your network and you need to have a method to optimize and prioritize traffic. Users will expect a high quality of service for all traffic types and a unified enterprise mobility strategy offers you the capabilities to deliver.

Unified enterprise mobility in action

For pioneers in this area, building a unified enterprise mobility strategy has significantly paid off. They have gained ubiquitous and transparent wireless coverage for users so that real-time access to mission-critical applications is seamless and at optimal performance levels.

Take, for instance, a health care organization in Canada. The organization is on the cutting edge of all things wireless, having already put to good use within the past decade voice over wireless LAN technology, RFID tagging, and 802.11 a/b/g.

Over the years, they've rolled out numerous pocketed areas of wireless access, including voice over wireless LAN for certain nursing wards, real-time location services featuring RFID tags for patients with dementia, and Wi-Fi for doctors teaching at the multiple downtown campuses.

Until recently, the IT group had kept each application apart, managing security and access separately. For an organization with limited IT resources - two network managers for thousands of nodes - this posed a significant burden. Though they wanted to pull together their wireless resources to save money and reduce the strain on IT, there were serious considerations, not the least of which was security.

What they found was that by bringing all wireless resources under a single umbrella via a unified enterprise mobility strategy, they have been able to achieve stronger security than before while allowing greater access to appropriate users.

They have implemented strict encryption that is based on 802.1x at the port-level and other advanced security standards. Using sophisticated security, they can offer physicians secure access to patient data and allow teachers to roam across logical subnets with a single log-on.

The group uses Windows Active Directory for authentication to avoid the headache of doing client-side certifications. By integrating the management and security of these disparate systems, they've achieved wired LAN-like access for their wireless network.

As they continue to reap the benefits of the unified enterprise mobility strategy, they have begun to lay the groundwork for future rollouts. For instance, the IT team would like to link their multiple campuses, which are separated by about six miles. Today, their only option is to hook onto a metropolitan area network and absorb the high cost of fiber connections. In the near term, the team says they are looking forward to deploying WiMAX, which will allow them all the benefits of a Metropolitan Area Network (MAN) without all the costs. They say that their unified enterprise mobility strategy positions them to quickly take advantage of this technology when it becomes available.

Conclusion

A unified enterprise mobility strategy is key for all organizations to operate in today's fast-paced world of mobile applications. Government agencies can take advantage of next-generation cellular, RFID, Wi-Fi, mesh and broadband technologies as they emerge, providing mission critical workers with the most up-to-date information available to improve decision-making, outcomes and accountability. Most importantly, a unified strategy allows IT to create a single point of management, which reduces infrastructure and personnel costs and streamlines operations.

Creating a unified enterprise mobility strategy is a simple task that will have significant benefits for every IT organization, including superior reliability, a reduced cost of ownership for your wireless infrastructure and the ability to draw all mobile resources into your intelligence network.

With a unified wireless architecture, mobile users are empowered to make critical decisions at any time and IT is seen as a strategic partner in keeping organizations on the cutting edge.

For more information on how Motorola can help your organization benefit from enterprise mobility, please contact us at 1.800.722.6234 or +1.631.738.2400, or visit us on the web at: www.motorola.com/enterpriseWLAN





MOTOROLA

motorola.com

Part number WP-GOVUEMS. Printed in USA 04/09. MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners. ©Motorola, Inc. 2009. All rights reserved. For system, product or services availability and specific information within your country, please contact your local Motorola office or Business Partner. Specifications are subject to change without notice.