



The CIO's Guide to Wireless in the Enterprise

Over the past decade, wireless technology has made huge strides in security, reliability and throughput.

Companies that are moving forward with business mobility initiatives must plan for wireless security and mobile device management from the start. Learn about many of the notable trends and key issues associated with Business Mobility and where to find additional resources for consideration.



The CIO's Guide to Wireless in the Enterprise

Table of Contents

Executive Summary	2
Introduction	3
Wireless Technology Review	4
Notable Trends for Enterprise Mobility	6
Mobile Applications	6
Unified Communications and Fixed Mobile Convergence	6
Key Considerations for Enterprise Mobility	7
Wireless Security	7
Mobile Device Management	7
Conclusion	8

Executive Summary

Over the past decade, wireless technology has made huge strides in security, reliability and throughput. The wireless networks of today are almost as fast and reliable as wired networks and provide much more convenience and flexibility. As a result, there has been explosive growth in wireless networks of all types, from Personal Area Networks (PANs) to Wide Area Networks (WANs). This incredible growth and renewed consumer confidence has ushered in the era of Pervasive Wireless - the availability of reliable, high-speed wireless connectivity nearly wherever and whenever a user requires it. In return, pervasive wireless, together with more powerful mobile devices, has enabled a dramatic shift in employee work habits. More workers are spending more time away from their desks and on the road, and wherever they are and whatever the time of day, they require the tools they need to do their job.

When not properly managed, there is a potential risk to an increase in business mobility. More workers away from the safe and secure confines of their workspace increases a company's exposure to security breaches from lost or stolen mobile devices. Equally costly in the long term, the improper management of mobile devices can significantly increase their total cost of ownership (TCO).

Companies that are moving forward with business mobility initiatives must plan for wireless security and mobile device management from the start. The CIO's Guide to Wireless in the Enterprise is the first of several CIO Guides from Research In Motion. It introduces many of the notable trends and key issues associated with business mobility and directs the reader to additional resources for consideration.

Introduction

By any measure, wireless communications can be considered a colossal success. By the end of 2008, the International Telecommunications Union (ITU) estimated that there were over 4 billion cell phone users globally. Incredibly, this means that almost two out of every three people on the planet have a mobile phone. Much of this remarkable success has only recently happened, as the number of global subscribers was less than 1 billion at the end of 2002. During the same period of accelerated subscriber growth, wireless network coverage also grew dramatically. Wireless network operators were completing their 2G networks and were starting to build out their 3G networks and planning for even further down the road.

Equally as important, over the last few years, mobile devices have made huge strides. A new class of mobile device, the smartphone, features more powerful microprocessors, increased storage and larger, more colorful displays. A smartphone is capable of running many of the day-to-day applications that the consumer, prosumer and business user have come to depend on. Popular applications such as email, calendaring and messaging are standard on most smartphones, and these devices are making it possible to 'mobilize' high-ROI, industry-specific applications. Smartphones gained 14% of the handheld market in 2008 and, according to one industry study, are expected to comprise 31% of the market by 2013.

Not just smartphones, but most of today's mobile devices go beyond mobile voice and utilize wireless broadband networks to provide a full-featured mobile internet experience. In many locations, multiple connectivity options are available to the user, including:

- Short-range communications over a Personal Area Network (PAN),
- Medium-range connections over private or public Wi-Fi®, or
- Longer range connections using the public cellular network to provide a Wide Area Network (WAN).

This overlapping umbrella of wireless connectivity sets forth a new era of personal communications, the era of Pervasive Wireless - the general availability of reliable, high-speed wireless connectivity almost wherever and whenever the user requires it. This document will provide the reader with a high-level background on wireless communications technology and identify important issues and key trends for further reading and consideration.

Wireless Technology Review

The starting point for any introduction to wireless technology has to begin with an explanation of 'spectrum'. The electromagnetic spectrum is a simple way to represent and categorize the different types of radiation - everything from low frequency radio waves to high frequency gamma and cosmic rays. The portion of the spectrum most useful for communications is the radio spectrum, located from 3kHz to 300GHz. The portion of the spectrum that we are interested in for wireless communications is from 500MHz to 5GHz. This frequency range provides enough power for optimal signal propagation without compromising signal penetration. There are many different types of wireless technologies in this frequency range, from broadcast radio and television to satellite phones and police radar, making regulation and compliance vital to prevent interference. However, not all frequencies on the radio spectrum are regulated. Some are left unregulated to allow for low-power, short-range communications technology like cordless phones, FRS radio, RC toys and car alarms. In addition, an unlicensed frequency band has been set aside for the use of industrial, scientific and medical devices (ISM). Some of the devices that operate in the 2.4GHz range of ISM include Wi-Fi devices, cordless phones, microwave ovens and even some satellite phones.

Many different types of networks share the wireless spectrum. Each type of wireless network, such as Personal Area Networks (PANs), Wireless LANs and MANs, has different capabilities, distinctive strengths and weaknesses that make them more suitable in different situations.

Personal Area Network (PAN)

A Personal Area Network (PAN) is typically low-power and short-range (<10 meters) with slow data throughput. It is often used for a wireless point-to-point connection so that no physical cables are required to connect the two end points. Wireless keyboards and mice, game controllers, cell phone car kits and hands free headsets are examples of endpoints connecting over a PAN. Two examples of PAN technologies include the ZigBee® and Bluetooth® wireless standards.

Wireless Local Area Network (WLAN)

Wireless Local Area Networks (WLAN) differ from PANs in two major ways, transmission range and data throughput. 802.11 networks (Wi-Fi) have become the de facto standard for wireless networks in workplaces around the world. There are four different Wi-Fi standards available in the marketplace - 802.11 a, b, g and the recently ratified 802.11n. It is expected that with the release of 802.11n, together with some of the other significant standards ratified over the last few years (802.11e and 802.11i), that the WLAN will start to compete head-to-head with the legacy of wired LAN for enterprise networks.

Metropolitan Area Network (MAN)

A Metropolitan Area Network is an indoor/outdoor wireless network that can span a campus, several city blocks, or an entire metropolitan area. It is usually larger than a WLAN, but smaller than the WAN provided by mobile network operators. There are two types of wireless networks that can be classified as MANs. The first is the public Wi-Fi Hotspot network, which is usually a small hub-and-spoke 802.11 network. Service providers such as network operators, cable companies or other communications companies deploy hotspots in places like libraries, airports and train stations. The other type of MAN is larger in scope and is built upon a Wi-Fi mesh network that may blanket an entire metropolitan center.

Wide Area Network (WAN)

The last category of wireless network is the Wide Area Network (WAN). This type of network has various names around the world with the cell phone network and the public mobile network being two of the most common. WAN 'coverage' is often citywide, statewide or even countrywide and a result of many factors such as frequency ownership, network design and signal power. Underlying technology has evolved quickly - from the AMPS voice networks of the 1980s to today's rollouts of high-speed 4G networks.

It is common when writing about or discussing mobile telecommunications to refer to industry acronyms such as 2G, 3G or 4G. These 'G's refer to the 'generations' of mobile telecommunications technology. The first generation (1G) of wireless telecommunications began in the early 1980s with commercial deployment of Advanced Mobile Phone Service (AMPS) cellular networks. AMPS networks used circuit-switching technology to carry voice-only traffic. In the early 1990s, mobile operators introduced Cellular Digital Packet Data (CDPD) onto the existing AMPS infrastructure to allow data transfers up to 19.2Kbps.

The second generation (2G) of wireless telecommunications emerged in the mid 1990s. Multiple competing digital voice standards made 2G much more complicated than 1G. In North America, some mobile operators adopted the Code Division Multiple Access (CDMA) standard, while others deployed networks based on Time Division Multiple Access (TDMA). Outside of North America, the clear winner was Global System for Mobile (GSM) communications. Each of these wireless technologies also released interim (2.5G) standards such as EDGE and 1xRTT to improve network performance and user experience.

Unfortunately, 3G telecommunications are even more complicated than 2G. The high-level goal was for the 3G standard (IMT-2000) to create a digital, packet-switched network with increased bandwidth, a minimum speed of 2Mbps for stationary users and 384Kbps in a moving vehicle. Three competing 3G technologies were introduced as evolutions from 2G. Most GSM network operators settled on Universal Mobile Telecommunications System (UMTS), also known as Wideband CDMA (W-CDMA), to offer download speeds of up to 3.1Mbps. CDMA network operators deployed Code Division Multiple Access 2000 (CDMA2000) and the more commonly known 1xEV-DO (Evolution-Data Only). EV-DO offered an advantage over UMTS in that it was easily deployed in an overlay to the existing 2G infrastructure. UMTS, on the other hand, would require a significant investment in spectrum and telecom infrastructure by the mobile network operators. A third 3G standard, Time Division-Synchronous Code Division Multiple Access (TD-SCDMA), has been selected as the 3G standard for the People's Republic of China.

Going forward, the ITU has created the requirements for 4G wireless networks. The requirement states that a 4G network should be an all-IP, packet-switched network that is highly backwards compatible with existing wireless standards. The goal for 4G is to achieve mobile data rates of 100Mbps for mobile endpoints and speeds up to 1Gbps for stationary terminals. The technology contenders for 4G include Long Term Evolution (LTE) and World Interoperability for Microwave Access (WiMAX).

Most mobile network operators have moved beyond 2G and are well into their 3G and 3.5G deployments. Moreover, many large network operators are rolling out their 4G infrastructure and plan to have operational networks in early 2010. In January 2009, a market research company estimated that there were over 290 million WCDMA (3G) users worldwide. Another firm expects that the number of users of mobile broadband services (3G, 3G+ technologies) will grow to over 2 billion by 2014.

Notable Trends for Enterprise Mobility

All of these types of networks - PAN, WLAN, MAN and WAN - are becoming faster and more reliable, resulting in explosive growth and utilization. More mobile subscribers taking advantage of new flat-rate data plans has resulted in a huge increase in mobile data usage. One infrastructure manufacturer estimates that by 2011, mobile data will overtake voice traffic and will continue to grow exponentially until 2013. Since mobile network operators are deriving more and more of their average revenue per user (ARPU) from data services, as opposed to legacy voice, they are strongly motivated to add value to their data networks and manage costs. Mobile network operators are upgrading their 2G and 3G networks to increase concurrency and reduce costs, while mobile device users are happily using the extra bandwidth for more multimedia messaging, social networking, and entirely new classes of mobile applications for both the enterprise and the consumer.

Mobile Applications

Today's mobile devices are completely viable computing platforms - many boast the same processing power and physical storage as laptop computers a few years previously. These days, workers away from their desks are able to do much more than talk on the phone and check their email. However, 1st Generation mobile applications such as wireless email, calendaring and messaging are safe, logical and cost-effective first steps in an enterprise mobility strategy. They have a tremendous ROI and can rapidly pay for an enterprise mobility infrastructure that can then be leveraged for new mobile applications. When considering next-generation mobile applications beyond wireless email, businesses should identify the challenges and opportunities that exist, the expected returns and the associated costs. This analysis should form the business case to define the project's scope and justify necessary investments. Regardless of the wireless solutions businesses choose, they should be flexible, secure and scalable beyond their users' immediate needs.

For more information about mobile applications, visit www.blackberry.com/solutions or download the CIO's Guide to Mobile Applications.

Unified Communications and Fixed Mobile Convergence

Wireless communications are becoming so pervasive and affordable that there is a significant global trend toward Fixed Mobile Substitution (FMS) - where consumers and businesses are substituting mobile service for conventional landlines. According to a 2008 report, more than 17% of US households have a cell phone and no landline, and another 13% have a landline that they rarely use. These numbers are consistent in the EU, where more than 18% of households are 'mobile only' and Finland leads the pack, where a massive 47% of households use mobile as their only access method. One of the key enabling technologies for FMS is Mobile Unified Communications (UC) and Fixed Mobile Convergence (FMC).

UC is generally considered to mean the consolidation of multiple methods of communication, including voice, email, instant messaging, presence and collaboration into a single application, which is controlled by a user for both business and social purposes. For example, a UC user might have a common inbox for email, voice and instant messages. The UC client software makes the user experience similar, whether using it on a desktop or a mobile device. According to one study, more than half of SMB's and almost 75% of large enterprises are evaluating, installing or running UC solutions. UC reduces communications fragmentation and improves employee reachability and productivity.

An important component of Mobile UC is Fixed Mobile Convergence. Fixed Mobile Convergence (FMC) allows people to have one phone number and voice mail that can be used on both fixed (TDM or IP desk phones) and mobile (standard mobile phones or smartphones) devices. It should also provide seamless handover of calls between fixed and mobile networks. For example, the automatic ability to move an active call from desk phone to smartphone and vice versa.

For more information about FMC, visit www.blackberry.com/mvs or download the CIO's Guide to FMC.

Key Considerations for Enterprise Mobility

Bigger, faster networks enabling more and more mobile workers to take care of their jobs on the road and away from their desks seems like a great scenario. However, along with the promise of reduced operational costs and increased productivity, there are some significant issues to consider, such as avoiding potential regulatory issues, legal liability and/or new and unexpected costs, which each enterprise will need to evaluate with consideration to its particular circumstances.

Wireless Security

The growth in wireless network coverage and a new generation of faster, more capable mobile devices have given mobile workers a valuable tool to help do their work outside of the walls of the company office. However, there is a potential downside to this trend. More mobile workers doing their jobs outside of the secure boundaries of the office increases the risk of compromising data security and/or allowing malicious users access back to the corporate network. There is also a higher likelihood that a mobile device that contains sensitive corporate data will be lost or stolen. While losing data may be only an inconvenience or embarrassment for some organizations, significant financial loss and legal risks may result in many cases. Companies that are interested in securing their mobile workers' devices and preventing unauthorized access to important company resources need to implement an enterprise wireless security strategy. To be effective, an enterprise wireless security strategy needs to include means of securing the mobile device and its data, securing the communications to and from the mobile device to the corporate network, and optimizing the enterprise network to support business mobility. The most effective wireless security strategy is a proactive one, to develop, educate, enforce and maintain an enterprise-wide wireless security policy. For more information about wireless security, visit www.blackberry.com/security or download the CIO's Guide to Mobile Security.

Mobile Device Management

Another important consideration for companies that are dealing with rapidly growing ranks of mobile workers is Mobile Device Management (MDM). MDM solutions allow IT administrators to manage mobile devices similar to the way that they manage desktop and laptop computers. It includes a capability to distribute firmware upgrades, applications and configuration settings over the air (OTA) to mobile devices no matter where the device is located. An enterprise MDM solution ensures that mobile workers are up to date with the latest versions of applications and data, and that their device is secure. An effective MDM solution should include these important features:

Over the Air (OTA) - OTA facilitates the configuration of mobile devices, application updates and device locks when the mobile phone is lost or stolen.

Back-up and Restore - Back-up of a mobile device is an essential activity for dealing with hard-resets and lost or stolen devices. It can also be used for synchronizing files and folders between a desktop computer and a mobile device.

Asset and Configuration Management - Configuration management is designed to provide administrators the ability to view and categorize devices by user role, device type or any other criteria. The administrator can then selectively use the categorization to configure application profiles, mobile device settings and registry entries.

Mobile Security Management - Security management is designed to allow the administrator to enforce power-on passwords and VPN settings or wipe clean all corporate data stored on a lost or stolen device.

As the numbers of different mobile device models grows and the number of mobile users within a corporation reaches critical mass, an enterprise MDM solution becomes a necessity. One analyst report found that managed devices have significantly lower TCO (by 53% to 63%) than unmanaged devices. This applies to mobile devices running native applications and those using the onboard browser and web-based solutions. An enterprise MDM solution is designed to improve mobile security, reduce risk and make it easier for IT administrators to manage the growing number of mobile users.

Conclusion

The core issue is the incredible growth in popularity of wireless technology. More and more people around the globe are using Bluetooth appliances, Wi-Fi (private and public) and public mobile networks. Mobile devices are becoming more capable and high-end devices like smartphones are no longer exclusive to mobile business professionals.

This means that as many as four billion wireless subscribers around the globe are expected to ramp up their data usage as they start to browse the mobile web and download applications. This growth in mobility is both an opportunity and a challenge to many enterprises. The potential rewards for implementing business mobility are impressive, but conversely, if not done correctly, there is the potential for huge expenses and associated risk. Enterprises must be aware of all of the issues surrounding business mobility. Wireless security and device management should be planned for, implemented and monitored to prevent data breaches and high TCO.

Research In Motion (RIM) offers a number of different resources to learn more about wireless solutions in general and the BlackBerry® solution in particular. The web site www.blackberry.com is a good place to start. The site features a developer's forum at www.blackberry.com/developers/forum which is used by application developers around the world. RIM also offers BlackBerry solution reference documents on a variety of topics. The Technical Knowledge Center on the site at www.blackberry.com/support can help you find answers to particular questions.







This material, including all material incorporated by reference herein or made available by hyperlink, is provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation or warranty of any kind by Research In Motion Limited and its affiliated companies ("RIM") and RIM assumes no responsibility for any typographical, technical, or other inaccuracies, errors or omissions in this material and shall not be liable for any type of damages related to this material or its use, or performance, or non-performance of any software, hardware, service, or any references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party web sites.

The limitations and exclusions herein shall apply irrespective of the nature of the cause of action and in no event shall any director, employee, agent, distributor, supplier or independent contractor of RIM have any liability related to or use of the material.

©2010 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, SureType®, SurePress™ and related trademarks, names and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world. All other trademarks are the property of their respective owners.

MKT-31585-001