
WIRELESS IN THE WORKPLACE

A Guide for Government Enterprises

April 2004, Version 1.0



National Association of State
Chief Information Officers



NASCIO represents the state chief information officers from the 50 states, six U.S. territories and the District of Columbia. Members include cabinet and senior level state officials responsible for information resource management. Other IT officials participate as associate members and private sector representatives may become corporate members.

AMR provides NASCIO's executive staff.

© Copyright National Association of State Chief Information Officers (NASCIO), April 2004. All rights reserved. This work cannot be published or otherwise distributed without the express written permission of NASCIO.

Table of Contents

Acknowledgments..... iii

Executive Summary..... 1

- Wireless in the Workplace
- The Wireless World - Business, Public and Private Spheres
- Advantages of Wireless
- Issues for Consideration

Wireless Technology Options..... 3

- Pervasive and Autonomous Computing
- Wireless Local Area Networks (WLAN)
- Wireless Wide Area Networks (WWAN)
- Public Wireless Local Area Networks (PWLAN)
- Voice over Internet Protocol (VoIP)
- Radio Frequency Identification (RFID)
- Ad Hoc Networks
- Emerging Technologies

Wireless Security..... 15

- Evolution of Wireless Security
- Authentication 802.11 (WEP)
- Dealing with 802.11b Security Issues
- Wi-Fi Protected Access (WPA)
- Wireless LAN Security Risks
- Wireless Network Security Recommendations

Wireless Network Management & Performance..... 23

- Integration with Legacy Applications
- Radio Frequency Coverage
- Access Points
- E911
- Quality of Service (QoS)
- Data Integrity & Interference
- Application Management
- Authentication & Encryption

Wireless Installation & Maintenance..... 35

- Installation Issues
- Maintenance Issues
- Supporting the Mobile Workforce
- Flexible Workplace Options
- Remote Access To Data/Applications/Co-Workers

.....

Wireless Applications & Uses	40
• On-Line vs. Off-Line Wireless Applications	
• Cross-Functional Wireless Applications	
• Vertical Applications in the Public Sector	
Appendix A - Wireless Standards	43
• 802.11 (WLAN/Wi-Fi)	
• 802.15 (WPAN)	
• 802.16 (WiMax)	
• 802.20 (WiMAN)	
• Voice over Internet Protocol (VoIP)	
• Radio Frequency Identification (RFID)	
• 3rd Generation (3G)	
• Wireless Application Protocol (WAP)	

Acknowledgments

Wireless in the Workplace: A Guide for Government Enterprises was produced in cooperation with the NASCIO Strategic Business & Services' Infrastructure Subcommittee.

NASCIO would like to express its appreciation to the Infrastructure Subcommittee chair, John Gillispie, Chief Operating Officer, Information Technology Services, State of Iowa, whose leadership and guidance made this publication possible. The following subcommittee members also contributed a great deal of their time and expertise to this publication:

Steve Dawson, State of New Jersey
Marty Dunning, Sun Microsystems
Gary Falis, Microsoft
Larry Johnson, State of South Carolina
John Rowland, IBM
Gail Ulan, State of Arizona

In addition, NASCIO would like to extend its appreciation to Dave Blackwell, State of New Jersey, Tom Sheperd, State of Iowa, and Lisa Somner-Sams, IBM, for their technical contributions and assistance in providing many of the graphics and charts included in the publication.

Finally, NASCIO would like to thank Jack Gallt, NASCIO Issues Coordinator, for his work on editing the publication, along with Elizabeth VanMeter, NASCIO Executive Director; Matthew Trail, NASCIO Assistant Director; Chris Walls, AMR Senior Publications and Website Coordinator; Kim Byars, AMR Records Coordinator; and Barbara Denton, AMR Administrative Assistant, for their guidance and assistance in producing and distributing this publication.

Please direct any questions or comments about *Wireless in the Workplace: A Guide for Government Enterprises* to Jack Gallt at jgallt@amrinc.net or (859) 514-9187.

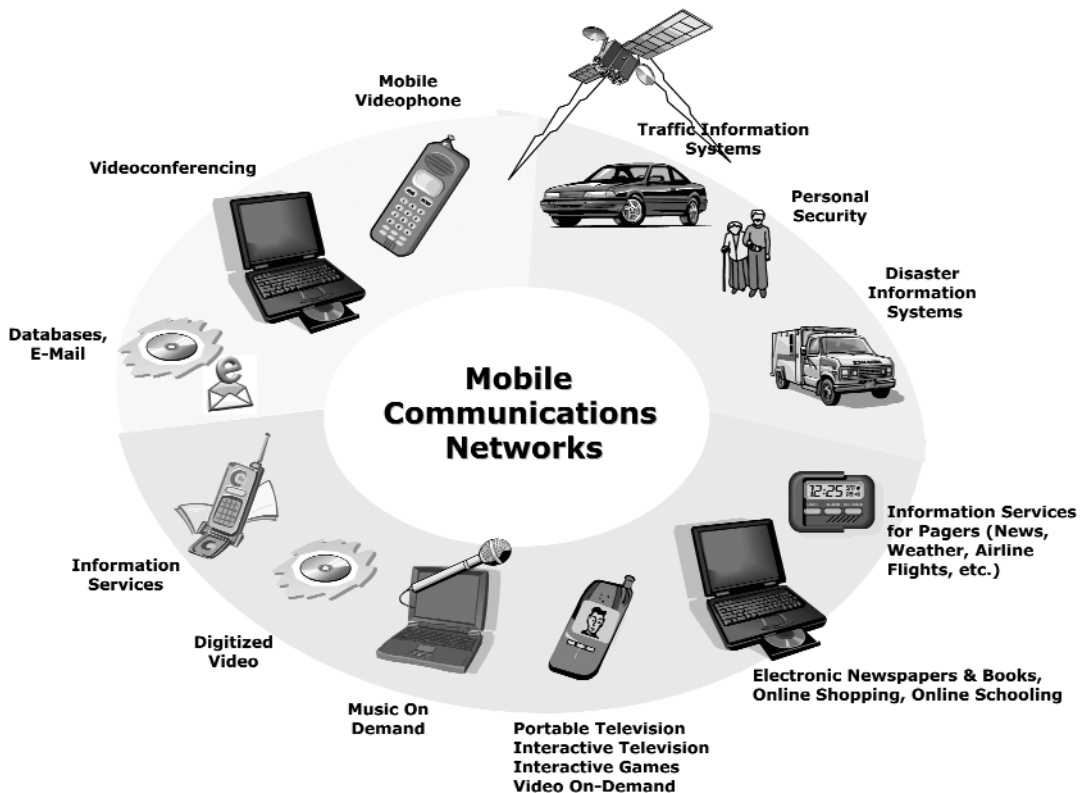
Executive Summary

Wireless in the Workplace

The use of wireless technology in the workplace, especially in the public sector, has been increasing at a rapid pace. There are many reasons behind this boom. Wireless can take an organization where no wired technology has taken them before. However, even with all the advantages of wireless solutions, there are some risks in exposing systems to this inherently open technology.

This publication is designed to guide you through the options available when working in the wireless world including background information on the standards, security options, and potential applications of wireless in the workplace. The intent is to help government enterprises make informed decisions about where they want to take wireless technology, and where the technology can take them.

The Wireless World - Business, Public and Private Spheres



Advantages of Wireless

The advantages of using wireless in the workplace are many fold:

- **Mobility** - The freedom to move anywhere, anytime within a building or multi-building campus and remain connected to real-time information. Laptop or PDA users can access broadband Internet services, email and the network wherever they choose to be on-site.
- **Flexibility** - Public areas, meeting rooms and the whole office space become more flexible. Fully functional work areas are created wherever you place your laptop. The wireless network provides extra capacity instantly, wherever you need it in your office space. Project teams, ad hoc groups and others needing temporary networks can be accommodated instantly.
- **Productivity** - All users can access the resources they need, when they need them. Remote workers and field workers can connect as soon as they arrive at your office. Since employees and business partners stay connected to the network, they can enter data while on the move.
- **Reduced Cost** - Installing or expanding a wireless network is fast and it avoids the time, cost, complexity and disruption of pulling cables through walls and ceilings. Adds, moves and changes within organizations become less time consuming and costly. Less is spent when offices are reconfigured or as organizations grow.

Issues for Consideration

The freedom and flexibility of a wireless solution does not come without its challenges. Whenever you hear about wireless solutions a discussion about security is not far behind. There are ways to secure wireless enterprises, but it is not always intuitive. You need to weigh the benefits of your solution and the costs of implementation, on-going security and support.

There are impacts on existing business processes when wireless solutions are introduced. Security concerns include exposing your locked down, wired environment to a more open, easily accessed (or compromised) solution. As with every technology decision, there are costs and benefits that must be outlined and weighed.

Dollar considerations may also be part of the impact to your existing infrastructure. Both wired and wireless solutions are coming out of the same pot of money. If the focus on wireless is made, you must ensure that your existing infrastructure is not forgotten.

One of the biggest hurdles to the proper funding for implementation of a wireless solution is caused by mass media. The focus on wireless technology for the "non-techie" user makes it seem like an effective solution is only a click away. Most consumer implementations of wireless solutions are not secure, and ignorance seems bliss. Rarely do those communications emphasize the wireless implementation, management costs and security concerns. Most people see the wireless movement as just another plug-and-play device. Unfortunately, battling that myth in the workplace, while educating executive management on the true costs of a wireless implementation, can be challenging.

Wireless Technology Options

Pervasive and Autonomous Computing

The computer-based Internet era in which we operate is very dynamic and has changed quite rapidly over the past few years. Many view the second wave of interconnectivity as one of pervasive computing—anyone connected any time, anywhere, using any device, communicating anything, in any format.

Because computing is becoming pervasive, it must also become autonomous. To understand autonomous computing, think of pervasive computing, defined above, with 'no one' substituted for 'anyone'. Computing should work more like our autonomic nervous system, which regulates basic functions without our awareness of it. Given the size and complexity of today's networks, this is a requirement.

Advances in mobile and wearable devices and network connectivity will allow for an implementation that is based on location-specific business needs instead of more generic functional needs. What is required is an extremely flexible solution that is precisely targeted to the objectives of the enterprise and meets the specific needs of a wide range of users.

Wired solutions generally use dial up modems or LAN connections. Wireless communication channels include:

Communication Channel	Range	Transmission Speed	Technology	Application
Infrared Data Communication	1 m	576 and 1152 Kbps	IrDa	Mobile device to PC / Mobile Device to printer
Wireless Personal Area Network (WPAN)	10 m	800 Kbps	Bluetooth	Cable replacement between nearby devices
Wireless Local Area Network (WLAN)	100 m (to an access point)	11 Mbps	IEEE 802.11 family	Accessing an existing Ethernet network
Wireless Wide Area Network (WWAN)	2-3 km (to a base station)	14.5 - 56 Kbps	GSM, CDMA, GORSm, CDPDm, TDMA	Voice and data communication
Wireless Metropolitan Area Network (WMAN)	30 km	1.5 Mbps	IEEE 802.16	Replace ISDN DSL, cable modems

The Technology of Wireless Generations

A brief history of wireless technology "generations" follows in an effort to better understand the current wireless environment.

1G - Also known as analog cellular, this is the first generation of wireless that introduced analog systems transmitting over radio frequencies. This wireless technology, used primarily for voice, represented a quantum leap in mobile communication (especially in capacity and mobility). This gave us the first cell phones in the early 1980s.

2G - The second generation of wireless introduced digital encoding and text messaging, and was also used primarily for voice. The development of 2G cellular systems was driven by the need to improve transmission quality, system capacity, and coverage in the mid-1990s.

2.5G - This describes the state of wireless technology and capabilities associated with General Packet Radio Services (GPRS)—that is, between the second and third generations of wireless technology. GPRS is a packet-based wireless communication service with data rates up to 114 Kbps and continuous connection to the Internet and is particularly suited for sending and receiving small bursts of data, such as e-mail and Web browsing. GPRS packet-based service makes better use of wireless bandwidth than circuit-switched services since communication channels are used on a shared, as-packets-are-needed basis rather than dedicated to one user at a time.

3G - This is short for third generation wireless, and refers to current and future developments in personal and business wireless technology, especially mobile communications. This phase is expected to reach maturity by the fourth quarter of 2005. Ultimately, 3G is expected to include capabilities and features such as:

- Enhanced multimedia (voice, data, video, and remote control)
- Usability on all popular modes (cellular telephone, e-mail, paging, fax, videoconferencing, and Web browsing)
- Broad bandwidth and high speed (upwards of 2 Mbps)
- Routing flexibility (repeater, satellite, LAN)
- Operation at approximately 2 GHz transmit and receive frequencies
- Roaming capability throughout Europe, Japan, and North America

In addition to mobile wireless, 3G is also relevant to fixed wireless and portable wireless. UMTS (Universal Mobile Telecommunications Service) is the third-generation (3G) broadband, packet-based standard supporting the transmission of text, digitized voice, video, and multimedia and promises to offer a consistent set of services to mobile computer and phone users no matter where they are located in the world. Once UMTS is fully available geographically, computer and phone users can be constantly attached to the Internet as they travel and, as they roam, they can have the same set of capabilities no matter where they travel.

Wireless Application Protocol (WAP) - An application environment and set of communication protocols for wireless devices that enables manufacturer, vendor and technology-independent access to the Internet and advanced telephony services.

Bluetooth - A specification for short-range radio links between mobile computers, mobile phones, and other portable devices. Bluetooth is used to create PANs (Personal Area Networks) among devices, and network with other nearby devices.

With WAP and Bluetooth providing stepping stones to 3G mobility and higher bandwidth services, the next step will be the network living where the customer requires ubiquitous access to high-speed pipes. In this scenario, the wireless local area network (WLAN) will give customers secure and cost-effective access to the Internet and web applications while simultaneously giving controlled connectivity to the home network. The development of the WLAN therefore goes hand in glove with broad band connectivity between the campus and the core network.

Wireless communications technology has increased the mobility of the workforce. The mobile phones and local connectivity enabled by radio frequency technologies such as wireless LAN and Bluetooth give the ability to transmit voice and data signals over wireless links. Increasingly, enterprises are starting to take advantage of mobility provided by the wireless technology. Wireless LANs combine data connectivity with user mobility, thus providing productivity, convenience, and cost advantages over traditional wired networks.

Almost any application that works over a wired Ethernet LAN should work over a wireless LAN. The only thing to consider is the speed of the network. Rather than 10 or in some cases 100 Mbps speeds, the wireless LAN operates at 11 Mbps in close proximity of the access point and shifts down to 5, 2 and 1 Mbps as the distance is increased. While this is acceptable to the workstations, the servers should typically be connected to the wired LAN to provide maximum performance.

Wireless Local Area Networks (WLAN)

Emergence of the 802.11b standard-based products in 2000, from a number of recognized and trusted network equipment manufacturers, has moved the wireless LAN market forward into the wider acceptance that has eluded it for years.

The first WLAN standard, IEEE 802.11, emerged in 1997 (see Appendix A for a complete listing of IEEE wireless standards). This standard defined three different technologies and led to frustration for both vendors and customers as they were looking for true interoperability. The ratification of the next generation 802.11b standard created momentum from traditional WLAN vendors as well as new entrants.

Emerging Wireless Standards

Nickname	3G	Wi – Fi	Wider - Fi	Mobile - Fi
Official name	WCDMA, CDMA 2000	802.11	802.16	802.20
Max. speed (megabits/second)*	2	54	10 to 100	16
Coverage area	Several miles	About 300 feet	Several miles	Several miles
Who runs the network	Cell phone companies	Individuals, IT Departments	Individuals or WISPs2	WISPs2
Type of airwave required	Licensed	Unlicensed	Either	Licensed
Advantages	Range, mobility	Great speed, ultra-cheap	Versatile, fast, long range	Fast, mobile
Disadvantages	Relatively slow, expensive	Short range	Interference issues?	More expensive?

Source: Forbes 04/03

Standards are now in place for the wireless LAN industry. They should allow users to be more amenable to adopting the technology. The 802.11b standard is now a de-facto standard. The Wireless Ethernet Alliance that supports and promotes the proposed 802.11b standard will test all products wanting 802.11b certification. This means that the products are interoperable with one another and will work at speeds up to 11 Mbps. Products that pass the test will be Wi-Fi (wireless fidelity) certified, and will bear a label with the Wi-Fi certification. This will certainly help quell uncertainty about interoperability. With standards now in place, vendors both large and small are entering the market, hoping to meet the users' expectations. The ratification of 802.11b also assisted in significantly driving costs down.

Enterprise Wireless LANs

Enterprises primarily introduce wireless LANs to enable mobility and to make additions, moves and changes easier. Wireless LANs allow mobile workers the flexibility that they require to use a complete suite of productivity tools while away from their desks.

Wireless LANs connect PCs and other peripherals within a building, and wireless bridges connect products between buildings. Wireless LAN access points create a cell of roaming coverage for mobile users. By plugging in and configuring an access point to attach to the wired backbone network, wireless LANs give wireless PC card-equipped computers access to the enterprise network. Overlapping cells of coverage form when multiple access points exist around the floor or building. These systems are helpful in environments where computers are mobile, where station relocation occurs frequently or where it is difficult to lay cables.

The enterprise wireless LAN market is estimated to grow rapidly as IT managers finally find the higher speeds, interoperability and lower prices that previously had been missing from this once niche market.

Public Access Wireless LANs

As the world accelerates into a broadband mobile environment, wireless LANs, designed to facilitate Internet access in localized communications hot spots, are expected to grow at a phenomenal rate. Wherever a concentration of users rely on mobile devices or laptops for communication, the public access wireless LAN introduces a flexible way to access the Internet—and with correct security software—an enterprise's Intranet.

According to the Dell'Oro Group, a market research firm that specializes in strategic competitive analysis in the networking and telecommunications industries, the overall WLAN market grew 10% in the fourth quarter of 2003 (to \$509 million) and posted full-year revenues of \$1.8 billion, a 16% increase over 2002.

Wireless Wide Area Networks (WWAN)

The wireless telecommunications industry worldwide is in the midst of transition from rapidly growing, profitable (to wireless operators), voice-centric services to a set of services that include data-oriented, wireless Internet services requiring broadband wireless infrastructures. To complicate matters, the industry is also caught in a slowdown. Wireless voice technology has matured and penetrated the population so that the battle for holding and acquiring subscribers is intense. Prices are falling, traditional voice services are approaching commodity status, and average revenues per user (ARPU) are decreasing as a result.

This telecommunications slowdown, coupled with the current worldwide economic downturn, is causing wireless carriers to scramble in search of differentiated services and new opportunities that will maintain ARPUs at acceptable levels and increase them to offset stagnant subscriber growth. This is especially true in more highly penetrated, developed markets.

At the other end of the spectrum, enterprises worldwide are acknowledging that delivery of key business information to a mobile workforce is a high priority. Demand for wireless data is steadily increasing.

In the midst of these challenges and the turmoil of a dynamic wireless data network evolution, clients and customers are in need of guidance to sort hype from reality in understanding and developing their wireless requirements and formulating strategies to take advantage of wireless e-business and the advantages that it offers.

In mobile telephony, 2.5G extends 2G systems, which support circuit-switched data transmission, using the same 2G-licensed radio spectrum to provide additional features like packet-switched data and enhanced data rates. A simplified way of thinking of 2.5G is as the result of gluing 3G concepts like increased data rates and "always on" data access onto 2G systems. 3G supports much higher data rates and is targeted as the wireless transmission basis for services other than voice, such as bandwidth-hungry applications like full-motion video, video-conferencing and full Internet access. The definition for 3G frequently implies that new radio spectrum must be licensed and all new wireless infrastructures must be procured and installed for 3G network implementation. As will be noted later in this section, it may be possible to achieve 3G by upgrading existing 2.5G networks using existing radio spectrum.

2.5G is also seen as an intermediate step to 3G networks and services, giving subscribers a first taste of always on, high-speed wireless access, without requiring that service providers undergo the spectrum licensing and system-wide upgrades associated with 3G. Presently, this intermediate step is also serving as a breather for an industry exhausted from outrageous spectrum bidding wars (notably in Europe) and a flagging economy. 2.5G is also viewed as a way for the financially strapped wireless operators to recoup some of their 3G-related expenses (spectrum licensing) and prepare for the capital-intensive 3G build-outs that are on the horizon. Some in the industry have suggested that 2.5G may meet most of the needs of subscribers as a legitimate alternative to 3G, and in a more extreme view that 3G may not be required at all.

New spectrum licensing deserves a word here. Spectrum designated as unlicensed is open to the public and available for use at no charge. An example of unlicensed spectrum is that designated for use with Bluetooth and WLANs. Controls on unlicensed spectrum do not exist to protect one user from interference or intrusion by another user. Alternatively, 1G, 2G, 3G, and future generations of wireless wide area network implementations by commercial operators require radio spectrum to be licensed for development and use in countries worldwide.

Most in the industry believe that 3G should not be completely abandoned. At its core are features all wireless users will welcome eventually—faster access speeds and always-on availability. The main characteristics of 3G systems, known collectively as IMT-2000, are a single family of compatible standards that have the following characteristics:

- Used worldwide
- Used for all mobile applications
- Support both packet-switched and circuit-switched data transmission
- Offer high data rates up to 2 Mbps (depending on range of mobility and velocity of motion)
- Offer high spectrum efficiency

IMT-2000 is a set of requirements defined by the International Telecommunications Union (ITU), an organization within the United Nations, and is the official ITU name for 3G. IMT stands for International Mobile Telecommunications, and, when originally conceived, "2000" optimistically represented both the scheduled year for initial trial systems and the frequency range of 2000 MHz for 3G implementation. IMT-2000 began as a project in the early 1990s to unite the world under a single mobile communications standard, given the disparate 2G mobile communications standards (like GSM, TDMA, and CDMA) in place at the time.

The ITU has established minimum requirements for the data speeds that the IMT-2000 standards must support, as summarized below. These requirements are defined according to the degree of mobility involved when a 3G call is being made. As such, the data rate that will be available over 3G will depend upon the environment in which the call is being made.

- **High Mobility** - 144 Kbps for rural, outdoor mobile use. This data rate is available for environments in which the 3G users are traveling more than 120 kilometers per hour (75 miles per hour) in outdoor environments.
- **Full Mobility** - 384 Kbps for pedestrian users traveling less than 120 kilometers per hour (75 miles per hour) in urban outdoor environments.
- **Limited Mobility** - At least 2 Mbps with low mobility (less than 10 kilometers per hour (6 miles per hour) in stationary indoor and short range outdoor environments.

Public Wireless Local Area Networks (PWLAN) - Community/City-Wide Broadband

We are just beginning to understand the potential impact of the radical changes taking place in personal, business and public communications due to mobile and wireless networks. As the world becomes more reliant on information-based services wherever they are, wireless is becoming the key factor to enabling these services. The sheer number of wireless devices, expected to reach the billions in the near future, is already beginning to drive trends such as self-forming, autonomic wireless networks.

This dramatic growth in wireless networks and users has resulted in several important trends impacting government:

- Government entities are now building and/or operating their own wireless networks and buying application solutions to address constituent requirements and to enable increased commerce
- New wireless ecosystems are emerging with ever-increasing capacity and broader uses, driving new partnerships, networks, devices and software
- The build-out of Wi-Fi and ad hoc networks has enabled a new paradigm of peer-oriented services including sensing, monitoring, data sharing, voice, video, nearest neighbor and context

The new wireless paradigm for government is a model where governments own and deploy the communications infrastructure much like they do with highway systems and utilities. A municipality can build the infrastructure for its own use, then optionally sell or give away extra bandwidth, providing both direct and indirect benefits to the community. In many cases, the wireless spectrum utilized is either set aside for government use or is part of a non-regulated set of frequencies.

Wireless Network Value for Governments

As noted, municipalities have already begun to build wireless networks and to invest in wireless and mobile applications to increase community services or to enable commerce. As these networks and the technology continue to evolve, a few specific areas in which wireless technology will add enormous future value in providing community services are apparent.

Voice and data services for rural and emerging communities - Governments are expected in the future to be the vehicle for providing basic voice and data services to emerging and rural marketplaces. The role of governments may be direct—building and managing new networks—or indirect—partially or completely financing these services. Governments may choose to utilize existing second-generation technologies obtained from traditional sources at very low costs; or they may bypass traditional networks and jump right to highly efficient data-based third- or fourth-generation networks. In other cases, government may choose to deploy nontraditional wireless-based networks or utilize voice over Internet (VoIP) technologies.

Mobile e-government: the key to value-added services - A huge amount of value will be derived from the concept of mobile e-government. With wireless technologies, the ability to support the population as well as government agencies with directories to find the right resources will take a major leap ahead. These services will be highly context-based—for example, knowing where a constituent is, what types of services they require, the time of day and the urgency of the request will enable a highly appropriate and timely government response. As society becomes increasingly more mobile, in both the government workforce as well as the general population, these types of communications will become increasingly challenging.

Contextual wireless technologies can support a wide variety of services. For constituents and visitors, it will be possible to dispense appropriate information such as electronic guidebooks at parks and museums. For emergency response units, this technology will make possible a highly coordinated response to a particular event, even locating and enlisting necessary resources within response range.

Safety and security - Governments are starting already to be early adopters of sensor-based networks designed to provide security and safety services as well as improved asset protection and utilization. For example, a port may want to monitor the movement of vehicles on their roadways during off-hours. An airport may want to monitor numerous digital surveillance cameras positioned around the facility. A community may want to monitor the health and welfare of their isolated elderly.

The key to successful deployment of this technology is how the data is utilized. In the near term, it will be, to a great extent, logistically impossible to centralize collection and analysis of the huge number of sensors that will be deployed, so it will be critical for the sensors, and the networks supporting them, to function autonomously. Therefore, coordination of data will largely be a function of the sensors themselves. Sensors will collect, disseminate, and analyze their target environment, transmitting information to the appropriate recipients. With this approach, it will be possible to expand these systems to control and monitor a virtually unlimited amount of assets.

Wireless sensor networks for governments will leverage highly specialized technologies such as smart dust sensors which can gather field biological data, including temperature change and detection of foreign chemical agents, then transmit information through a wireless network connection. Wireless ease of deployment and real-time adaptive rerouting will provide the network the reliability and resiliency it needs to be effective.

Summary

Governments, and the organizations which support them, will be the largest implementers of advanced wireless and mobile networks of the future due to the enormous potential these networks have to efficiently and effectively leverage available resources. In some areas, complete citywide network grids are already being planned using Wi-Fi, ad hoc and beam-forming technologies to provide uninterrupted wireless connectivity across entire cityscapes.

Comprehensive capabilities of wireless applications such as incident command and control, resource tracking, alarming and video, in addition to ubiquitous connectivity to people and networks, will help citizens and government to stay in touch with one another and government agencies to stay in constant communication with a vast array of resources and personnel.

Voice over Internet Protocol (VoIP)

The concept of the convergence of voice and data infrastructure systems has been a topic of discussion for some time. Until recently, however, there have not been many large-scale deployments of unified networks for voice and data in the wired world. While there are numerous reasons why this convergence has not taken off in the wired world as predicted, including technology, quality and reliability issues, the scenario in the wireless domain is very different. Most infrastructure for wired telephone systems already existed when the LAN was deployed. Furthermore, the technology was not in existence to deploy real time voice systems on the local area network nor was there enough bandwidth to support the throughput requirements.

Enterprises are deploying WLANs in large numbers providing mobility to their data network users. While enabling data mobility in the workplace creates greater efficiencies, enterprises want total communications mobility including voice. As customers feel increased pressure to cut costs and improve efficiencies on their networks, the idea of deploying and managing

multiple wireless infrastructures supporting total mobility is prohibitive. Using a single wireless infrastructure supporting both data and real time voice communication is most appealing to enterprises.

One of the most important aspects in designing WLAN systems that employ VoIP telephony lies in understanding the different usage models that exist between data and voice. In the context of data, to a large extent usage is discontinuous or asynchronous. For example, users will request data from a server on an intermittent basis, requiring "burst" transmissions. With voice, on the other hand, a continuous (isochronous) stream of data or voice packets must be received and transmitted in order to achieve an acceptable level of Quality of Service (QoS). It is this usage model difference that drives more stringent network design and implementation requirements.

Also important is that this architecture stresses industry standard solutions. Despite the expected maturing process, the fundamentals for this environment are well established in the standards bodies and are not expected to change. When transformation issues arise that are not addressed by the standards and development is needed, this development should focus on the emerging standards rather than the legacy standards.

Voice strategies should focus on the following elements which provide basic requirements and expectations for the development of on-demand IP communications infrastructure:

- This is a long-term strategy that focuses on the tools that employees need to do their jobs today and into the future as well as the need to communicate with customers and partners worldwide.
- The strategy is designed to enable the creation of communication services and applications using on-demand computing principles as a foundation.
- The strategy is based on recognized, industry standards to support a fully interoperable and multi-vendor environment.
- The infrastructure focus is IP networks and public cellular networks. In addition, the strategy looks toward a reduced fixed infrastructure with servers appropriately consolidated, most likely in Service Delivery Centers (SDC).

Radio Frequency Identification (RFID)

RFID tag technology is growing fast. The advantages of this technology are the simultaneous reading of many RFID tags without the need to actually be in the line of sight of each tag. The disadvantages are the cost of the tags in comparison to printed bar code labels. The cost of RFID tags will go down from year to year and already technology is available to print a low cost passive RFID tag.

Much of the recent research involving RFID technology has shown that, in general, the technology remains expensive for most types of applications, especially at the item level. This is especially true for two reasons:

- **High Cost of Tags** - The cost of the RFID tags, at around \$0.20 cents per tag, still does not represent an economical solution for tracking individual high volume, low value pieces. In fact, even when the cost drops to \$0.05 a piece (as is predicted within the next four years), the difficulty of programming and affixing the tags to certain items will still make it difficult to justify the cost of tracking these items with RFID tags.

- ***Huge Amount of Readers Needed*** - The read ranges on the least expensive types of tags (i.e., the tags that would most likely meet item level application needs) do not exceed more than a few feet. This means that the enterprise would need to buy a very large number of tag readers. At several hundred dollars a piece, combined with the cost of RFID tags, using RFID technology for tracking individual pieces becomes very expensive.

However, using RFID technology to track the departure and arrival of trucks (truck and pallet level) would not likely be cost prohibitive. Combined with a nesting methodology that linked unit loads to containers and containers to trucks using ring scanners or handheld scanners, RFID technology could be used to provide complete visibility into the transportation of assets throughout the supply chain.

Fortunately, passive and durable tags have become relatively commoditized in recent years and will not be extremely costly. In fact, there are many types of tags that most enterprises could use to meet their needs.

Ad Hoc Networks

Ad hoc peer-to-peer networking technology enables direct device-to-device communications and high-speed access to corporate LANs or public networks such as the Internet or PSTN. Ad hoc peer-to-peer mobile architecture offers several unique value propositions to both users and operators of the network. All nodes in the network act as routers and repeaters for other subscribers in the network. This capability enables users to "hop" between any number of devices in the network to achieve the desired connection. As a result, the network offers several unique capabilities:

- Easy for two people to directly share files, email, music, video or voice calls. Network infrastructure is not needed. This is true ad hoc peer-to-peer communications. Users can form high-speed voice and data networks anywhere, anytime.
- Groups can also form ad hoc peer-to-peer networks anytime, anywhere. Again, no network infrastructure is required.
- Members of a peer-to-peer group can also access the Internet or telephone network when infrastructure is available.
- Users can create long-range peer-to-peer communications links by hopping through network infrastructure elements called wireless routers.
- Users can hop through multiple wireless routers to reach the network or directly reach each other. This simplifies network deployment, reduces costs and increases network efficiency.
- User devices can also act as wireless routers. That is, they act as routers and repeaters for other users. This increases network robustness, while reducing infrastructure deployment complexity and costs.

These capabilities lead to some very profound paradigm shifts. The technology creates a network where users co-operate, rather than compete, for network resources. Thus, as the service gains popularity, and the number of users increase, service likewise improves for all users. Obviously, this is not the case with today's cellular-based systems. But what may not be obvious is that when user devices act as routers and repeaters, these devices are actually part of the network infrastructure. So, instead of wireless operators subsidizing the cost of user devices (i.e. handsets), as is today's custom, users actually subsidize and help deploy the network for the

operator! This has major implications to the operator's capital network expenditures, subscriber acquisition cost (which may be less than zero) and overall profitability.

Emerging Technologies



Wireless to the Max – WiMAX

- **802.16a - non-line-of-site, point to multi-point, last mile wireless broadband solution**
- **Supports 2 to 11 Ghz range up to 40 Kilometers**
- **Supports 1,000's of users at an aggregated throughput of up to 70Mbps**
- **Primarily designed for licensed spectrum (QoS) – supports carrier grade voice and video**
- **802.16a will co-exist with 802.11 supplying the backhaul**
- **As 802.16a client devices scale down competition increases with 802.11**
- **802.16e will add mobility - moving people not to compete with Cellular**

	802.11	802.16
Bandwidth	54Mbps (11a)	70Mbps
Range	100m	40Km
QoS	None	Centrally enforced
Coverage	Optimized for indoor non-line-of-sight (NLOS)	Optimized for outdoor NLOS
Security	802.11i	Triple-DES, RSA
Service levels	None	Multiple levels support differentiated bandwidth requirements
Users	Hundreds	Thousands



802.16/WiMax

This is a new emerging technology from the IEEE committee. 802.16 products will be used in both licensed and license-exempt bands. For the U.S., the licensed band targeted is the 2.5 GHz also known as the MMDS bands. Licensees in this band include Nextel, Sprint, BellSouth and recently Flux (a new company formed by McCaw). The owners of a license will determine which technology they will use for the spectrum.

802.16a

This standard addresses a Physical Layer/Media Access Control (PHY/MAC) that will work over the range of frequencies mentioned above. The 802.16a MAC is different from the 802.11 MAC, and it is based on request-grant model. The end devices request resources (bandwidth, timeslot) from a central base station, and the central base station then provides resources based on service level agreements and availability of resources. The user data rate will be a fraction of overall data rate for each packet sent. This is in contrast to 802.11 basic access scheme, for which each station has equal probability of accessing the medium, and if the medium is accessed, the full bandwidth is available to the station for the period of transmission.

For this reason, it is not a straightforward answer to determine the bandwidth per user for 802.16-based system. 802.16a however has PHY defined to support higher data rates (up to 63 Mbps); so this will be shared by x number of users to be determined by the service provider.

802.16a will be used for the following applications:

- Last mile access
- Backhaul for 802.11 networks
- Point to point links (between sites)

802.16e

This will modify 802.16 MAC to support stations in motion. The stated goal is pedestrian speeds, but it is anticipated that actual products will exceed pedestrian speeds.

802.20

This is a new standard targeted to the mobile application in the licensed band. It will take a few years before the details of the standard are finalized. It is mentioned for completeness.

Wireless Security

Wireless LANs (WLANs) deliver great flexibility and efficiencies within organizations based on their inherent mobility. The security procedures that apply to wired networks also apply to a WLANs overall security. A WLAN is just another media type (physical layer), however this wireless media type does introduce new security and integration challenges in terms of authentication/authorization, encryption, privacy, infrastructure, devices and location. Along with the new challenges, wireless introduces variations to existing security methodologies that may also have to be taken into consideration.

Evolution of Wireless Security

In 1999, the IEEE approved the 802.11b standard and WLANs were born (see Appendix A for a complete listing of IEEE wireless standards). The 802.11b standard specifies that the radios in the wireless equipment operate on the unlicensed 2.4GHz band on one of 15 specific channels (the U.S. is limited to using only the first 11 channels). There are two modes specified in the standard, *ad hoc* (peer-to-peer) and *infrastructure* which uses a central site, an access point (AP), that several clients talk to. Each AP is limited to 11Mb of shared (divided amongst the connected users) bandwidth which requires adding another AP with a different network name and radio channel to deal with bandwidth issues. This results in a separate network from the original (up to a maximum of three). APs have approximately a 300 foot range.

In an *infrastructure mode* WLAN, an AP beacons a SSID (Service Set Identifier) and also broadcasts DHCP addresses, ARP requests, etc. Client wireless network cards scan the channels looking for wireless networks and connect to the network as long as their security settings match. [Note: Some Operating Systems allow a client card to be set to a configuration that allows connecting in either an *ad hoc* or *infrastructure* mode. This can be locked down to prevent either *ad hoc* or *infrastructure* connections.]

Basic Security: SSID

The SSID is essentially the name of the wireless network and the "access point" for devices to connect to it. If a client wireless card is configured with the SSID name or can scan and capture it, then it can identify the network to connect to for authentication. The original purpose of the SSID was to differentiate networks from each other.

The manufacturers of wireless AP devices normally ship them with a default SSID, for instance, Cisco's SSID is "tsunami" and the Linksys is set to "linksys." These default SSIDs are very well known so leaving them in place opens a network to discovery. Another concern is naming a SSID related to a location or the department it is located in. It is recommended that SSIDs be generated with the same recommendations around strong network passwords. Even with a "strong" SSID, the fact that an AP broadcasts the SSID every few seconds in beacon frames in order to make it easier for authorized users to find the network also allows unauthorized users to find it. This beaconing is what allows wireless network detection software to find networks without having the SSID upfront.

The SSID can be seen as the first line of defense although it is difficult to control who gets access to your network. Configuring with strong password type SSID will make it difficult for intruders to know what they are looking at.

Authentication 802.11 (WEP)

Once a network is discovered (SSID), 802.11 specifies that a dialog must begin, called "associating," before any other communications can take place. This can be set to either a *shared key authentication* or an *open authentication* mode. *Open Authentication* allows any wireless device to "associate" with the AP and provides no access security. *Shared Key Authentication* provides for a basic challenge/response communication. When the client sends an association request the AP responds with a string of challenge text (unencrypted) which the client encrypts using the WEP (Wired Equivalent Privacy) key. If the returned encrypted text is correct then the client is allowed to communicate with the AP and move onto the next layer of security.

WEP was intended to give a wireless security equivalent to a wired network. WEP is designed in such a way that it takes the packet's data payload and encrypts it using a secret 40 bit number and then passing it through a RC4 cipher. The receiving station uses the same 40 bit number and passes it through the RC4 cipher backwards which results in the host receiving good usable data.

Issues: WEP

The main problem with WEP is that the RC4 stream cipher has proven to be insecure. WEP uses the 40 bit WEP key and a 24 bit random number known as an Initialization Vector (IV) to encrypt data. An attacker can capture packets and discover what the WEP key is mathematically by monitoring the IV which will eventually repeat itself. Additionally, numbers in the 0 to 16777215 range are considered "weak IVs" that can be exploited to reveal the WEP key.

Managing WEP keys is also very difficult, especially in a large environment; you have to visit each device and enter the WEP key. This can be done initially on a new client rollout without too much difficulty, however if your key becomes compromised or discovered you have no security unless you visit each machine and enter a new key. This could be quite a logistical challenge in a large environment.

Dealing with 802.11b Security Issues

SSID

In order to deal with the SSID issue mentioned above (beaconed SSID by APs), Lucent developed what they called the "closed network" which essentially turns off the "beaconing" function of the AP which makes discovering the SSID much more difficult. In this scenario, the end user has to enter the SSID manually to connect to the network. This requires no special software, but from a management perspective your SSID should never change. Many vendors picked up on this strategy. Although this will not protect your network from a planned attack, it does defend against the so-called "war driver," preventing attacks before they start. "War drivers" are individuals who look for existing wireless networks that they can attach to and use. [Note: Even if a "war driver" cannot authenticate into your network they can still attach to your wireless network and use it for peer to peer communications with others; depending on your security setup they could go out to the Internet over your network or could flood your AP with traffic thus effectively shutting down your network.] Another issue with the "closed network" is that the SSID is sometimes contained in management messages that are broadcast in clear text so there is the possibility of "sniffing" and discovering the network name.

128 bit WEP

Lucent also introduced 128 bit WEP keys which extend the WEP key from 40 bits to 104 bits. Although this significantly increases the time to do a brute force crack of a WEP key, the real weakness of WEP, the 24 bit IV, is still there. The 128 bit WEP key in combination with other security measures is still a good idea. The 128 bit WEP key is outside of the 802.11 standard although for the most part you are given the option of no encryption, 40 bit encryption or 128 bit encryption when configuring WEP.

Broadcast Key Rotation

In the 802.11b specification there are two WEP keys, one for data encryption and one for broadcast encryption (DHCP; ARP). The broadcast key is usually the same as the data key. Cisco introduced the idea of dynamic and short lived broadcast WEP keys which has been adopted by the other AP vendors. The strategy is to change the broadcast key within a certain time interval encrypting it with the old key in order to not allow enough time to collect enough packets to crack the key. This is effective, but only secures the broadcast communications.

MAC Address Filtering

In this scenario, the unique 12 digit hex number of a network card, its MAC address, is used to allow access to the AP. Authorized MAC addresses are stored at the AP or on a RADIUS (Remote Authentication Dial In User Service) server. Unfortunately there are also issues with this approach. First, managing a database of MAC addresses is a very difficult task and in larger environments it becomes very impractical with additions and deletions of devices not to mention servicing of the devices in the case of a NIC failure. Of more concern is the fact that with the right equipment a MAC address can be sniffed and since these addresses can be changed on some network cards, the captured MAC address can be cloned thus allowing access to the network.

Virtual Private Networks (VPN)

In order to deal with security issues mentioned above around wireless, the use of a VPN became popular. As with leveraging a VPN over the public Internet, wireless networks were segmented behind firewalls and wireless clients were configured for VPN. The clients tunneled over the wireless network and connected to the "wired" network with a safe encrypted standard VPN connection. This leverages the proven technology that prevents access to your wired/enterprise private network.

Unfortunately the nature of the VPN can cause issues. Since the wireless net is supplying IP addresses via DHCP, there is nothing preventing an unauthorized user from gaining a legitimate IP address on the wireless network. Once this is done, depending on the configuration of the clients, it is possible for this rogue client to communicate with authorized clients and attack their machines. Even if an authorized client is configured to only talk to the AP point, rogue clients can still piggyback on your network and communicate with each other and even kick off a "jamming" attack that could shut down your network. VPNs are a proven way to protect your "wired/enterprise private" network, however the issues mentioned above need to be taken into consideration when thinking of employing this strategy.

802.1X

The IEEE ratified the 802.1X standard in April 2001. This standard originally developed for wired networks is very applicable to wireless networks. It is a Layer 2 (MAC address) security protocol that exists at the authentication stage of the security process. Under 802.1X, an AP demands a set of credentials from a client trying to access it and passes them to a RADIUS

server for authentication and authorization. The 802.1X standard EAP (Extensible Authentication Protocol) defines the method for supplying credentials. EAP is the main security measure in 802.1X and it allows developers to create their own methods for passing credentials. The four EAP methods in use today are EAP-MD5; EAP Cisco (LEAP); EAP-TLS and EAP-TTLS.

- **EAP-MD5** - Uses static WEP keys and leverages a MD5 hash of a username and password to pass credentials to the RADIUS server. EAP-MD5 is considered the least secure of the common EAP standards.

Concerns:

- ⇒ Offers no key management or dynamic key generation.
- ⇒ Prevents unauthorized users from accessing the network, but provides nothing to address the insecure WEP encryption screen.
- ⇒ Subject to "sniffing" that allows the WEP key to be decrypted which allows all of the data on the wireless network to be viewed.
- ⇒ Offers no protection against rogue APs.

- **EAP Cisco Wireless (LEAP)** - LEAP developed by Cisco also passes encrypted user names and passwords to a RADIUS server. What sets LEAP apart is that it generates a unique WEP key at each authentication. For greater security you can set the RADIUS server to force a re-login of the client (behind the scenes) at a specified time in order to nullify attempts to "crack" the WEP key since it is changed with each re-login. LEAP also forces a mutual client to AP authentication thus eliminating "rogue" AP attacks.

Concerns:

- ⇒ Uses MS-CHAPv1 for AP and Client authentication. MS-CHAPv1 has known vulnerabilities.
- ⇒ Originally only worked on end to end Cisco networks. Hardware and client software has to be checked to verify compatibility.

- **EAP-TLS** - Developed by Microsoft (RFC-2716) uses X.509 certificates for authentication. EAP-TLS relies on Transport Layer Security (IETF's standardization of SSL) to pass PKI information via EAP. EAP-TLS has dynamic one time key generation and authenticates the AP and Client.

Concerns:

- ⇒ PKI infrastructures are complex.
- ⇒ Dependence on Microsoft Active Directory (any client will work however if EAP-TLS client software has been written for it).

- **EAP-TTLS** - Developed by Funk Software as an alternative to EAP-TLS. The AP identifies itself with a Server Certificate but the user/password credentials are sent to the RADIUS server. EAP-TTLS as specified by the administrator can use any of the following challenge-response methods: PAP; CHAP; MS-CHAPv1; MS-CHAPv2; PAP/Token Card or EAP.

Concern:

- ⇒ Less secure than the EAP-TLS 2 certificate mechanism.

- **PEAP** - PEAP (Protected EAP) is an EAP type that addresses the security issue of EAP conversations that may be sent as clear text (unencrypted). PEAP creates a secure channel this is encrypted and integrity protected with Transport Level Security (TLS). Once the secure channel is established another EAP type authenticates the network access/authentication of the client. MS-Chap v2 is a scheme that has been used with PEAP. MS-Chap v2 is a password based, challenge-response, mutual authentication protocol that uses MD4 and DES algorithms to encrypt responses.

Wi-Fi Protected Access (WPA)

Recognizing the increased concern over WEP security issues, the Wi-Fi Alliance in conjunction with the IEEE has driven an effort to bring strongly enhanced, interoperable Wi-Fi security to the market which resulted in Wi-Fi Protected Access (WPA). WPA is derived from and will be forward-compatible with IEEE 802.11i although it is designed to run on existing hardware. The design goals of WPA were to be a strong, interoperable security replacement for WEP; be software upgradeable to existing Wi-Fi certified products; be applicable for both home and large enterprise users and be available immediately.

In order to accomplish this, WPA had to improve data encryption and provide a mechanism for enterprise level user authentication. To provide enhanced data encryption, WPA utilizes TKIP (Temporal Key Integrity Protocol) which addresses WEP vulnerabilities with:

- A per-packet key mixing function
- A message integrity check (MIC)
- An extended initialization vector (IV) with sequencing rules
- A re-keying mechanism

WPA implements 802.1X and EAP in order to provide for enterprise-level user authentication.

WPA and Home/SOHO applications

WPA provides a special "home" mode for homes or small businesses that do not have central authentication servers. WPA uses "pre-shared keys" and passwords that are easy to setup. WPA will only allow devices with the "key and password" on the network. Once the password is authenticated, WPA kicks off the TKIP process to add data encryption protection.

802.11i

This is a standard that is currently under development to address the security concerns around the current wireless standards based on WEP. As mentioned above, WPA and other methods such as PEAP employ some of the upcoming methodologies that will be included in the 802.11i standard.

802.11a and 802.11g

These standards address performance enhancements to the wireless standard allowing more bandwidth and faster speeds for wireless communications. There is no change to the basic security "design" of the 802.11 standard included in these later versions. The only exception is that 802.11g runs at a different frequency than 802.11a and 802.11b thus eliminating the shared frequency issues that plague 802.11a and 802.11b. These standards share the same frequency range as Bluetooth devices, baby monitors and certain cordless phones.

Ad Hoc Wireless

As mentioned previously, IEEE 802.11 support for wireless LANs (WLANs) provides for two different implementation modes that can be deployed, *infrastructure* and *ad hoc*. The *infrastructure* mode which depends on a central station (access point) to connect the clients is the most widely deployed mode. In an *ad hoc* environment, any security that could be accomplished at an AP has to be pushed down to the peer-to-peer clients. However, in this mode WEP, WPA and encryption can be leveraged to achieve a level of security. More advanced security such as leveraging a RADIUS server as described earlier in this section is not available. *Ad Hoc* mode would also require the manual entry of WEP keys on each client, thus making this mode more applicable to a small business/agency or home application.

Wireless LAN Security Risks

Risk	Description
Insertion Attacks	<p>Unauthorized Clients: A client scans and connects to access points (APs) that are either insecure or the password/keys are cracked. These clients are referred to as "war drivers."</p> <p>Renegade Access Points: Someone can hook an AP to the enterprise network and thus create a new unmanaged wireless network.</p>
Interception and Unauthorized Monitoring of Traffic	<p>Wireless Packet Analysis: Wireless network traffic can be captured using techniques similar to wired networks. Typically, intercepting username and password to masquerade as a legitimate user.</p> <p>Broadcast Monitoring: A result of connecting an AP to a hub instead of a switch will cause all traffic across the hub to be potentially broadcast over the wireless network even if it was not intended to be.</p> <p>Access Point Clone: A stronger signal unauthorized AP is put in proximity to wireless clients where the clients then try and log into substitute servers unknowingly revealing user names and passwords.</p>
Jamming	<p>Jamming: denial of service attack that can be accomplished in many ways leveraging various tools to overwhelm the 2.4GHz frequency. [Note: This can also be caused by other 802.11b devices installed in the environment or even by cordless phones or Bluetooth devices.]</p>
Client to Client Attacks	<p>File Sharing/TCP/IP Service Attacks: Wireless clients running file sharing or web servers are susceptible to the same attacks as wired clients.</p> <p>DOS (Denial of Service): Wireless networks operate on a limited bandwidth (11Mbps shared) so a device can flood the network. Also duplicate MAC or IP addresses can cause a DOS issue.</p>

Risk	Description
Access Point Password Attacks	Brute force dictionary attacks against passwords or keys can cause network compromise.
Encryption Attacks	WEP weakness exploits.
Misconfigurations	<p>Failing to secure AP points that ship in an un-secure fashion.</p> <p>SSIDs: APs ship with standard known names specific to the vendor.</p> <p>WEP: Encryption settings, none, 40 bit; 128 bit.</p> <p>SNMP: APs ship with SNMP agents which can provide access to the network if not properly configured.</p> <p>Configuration Interfaces: APs have certain interfaces that might be compromised: SNMP, serial, Web, Telnet.</p> <p>Client Side Security Risk: Data such as the SSID and WEP key in some instances can be stored on the client such as the Windows registry.</p> <p>Installation: Default installation of APs favors ease and speed of network creation over security.</p>

Wireless Network Security Recommendations

Wireless network security as with any other asset should be protected with a combination of process and technology. Below are some recommendations that are not inclusive, but should provide some guidance when planning a wireless network. It is important to point out that any emerging technology is still not a substitute for proper policy and process.

Security Policy/Architectural Design - Wireless in the overall enterprise policy, standards and security management.

Access Point Policy - APs should be evaluated on a regular basis to ensure that they have not slipped into an untrustworthy state needing to be quarantined. The appropriate placement of firewalls, VPNs, intrusion detection systems and authentication between access point and intra/internet has to be ensured.

Access Point Configuration Policy - Security and configuration policy concerning SSID, WEP keys, Encryption and SNMP community words needs to be established and enforced.

Wireless Client Protection - Wireless clients need to be reviewed for proper security. Considerations such as personal firewalls, VPNs, virus protection, and intrusion detection should be reviewed.

Managed Security Services - Providers or in-house experts should be employed to monitor security 7X24 and provide emergency response services. Some examples would be: deploying firewalls to separate the wireless network from the internal network or internet; establishing and monitoring VPN gateways and monitoring VPN clients and maintaining an intrusion detection system.

Leverage Security Software Products - There are various software-based security products available to assist in securing wireless and wired networks that do such functions as vulnerability detection, configuration assessment, network intrusion monitoring, etc.

Leverage Security/Network Devices - There are a variety of dedicated devices that provide intrusion detection, network sniffing, network "health", etc. that can be used for wireless networks.

IPSec/X.509 Certificate Configurations - Recommendations to leverage IPSec over L2TP (Layer Two Tunneling Protocol) in conjunction with X.509 certificate services over 802.1X have shown to be very flexible and secure. The inclusion of smart cards or similar security devices has been used to enhance the security of these implementations.

Physical Security Concerns - Care should be taken to ensure that APs are placed in a secure location and locked away from non-authorized personnel access.

Wireless networks are an exciting and evolving technology that promises to provide greater productivity and ease of networked computing to large and small computing environments. As evidenced in this section there are a number of security concerns that the Industry are working to deal with actively. Currently, by leveraging technologies available and implementing good policies and processes, wireless networks can be secured as evidenced by the number of successful deployments throughout the world. As the industry as a whole is quite aware of the security issues surrounding wireless networks, there is a lot of work in place to address it in the future. The Wi-Fi Alliance, vendors and the IEEE under the working 802.11i standard are actively working to put in place even greater security than we have today.

Wireless Network Management & Performance

Integration with Legacy Applications

The need to leverage existing information technology assets, the desire to attain expertise in new technologies, and the necessity to create solutions with long-term benefits are important considerations for any large organization. Selecting a middleware architect should provide an architecture that can minimize risks and provide the IT technology necessary to mobilize the enterprise. The use of middleware tools can help build extensions to existing and new applications.

Leading enterprises are now moving beyond mobile e-mail and calendar to critical business applications that improve data capture and field-level effectiveness. Platforms for today's mobile workforce should feature the robust architecture that enterprises need to expand mobile capabilities and make a quantum leap in productivity.

A core platform for mobility should allow for the delivery of advanced services to mobile devices for push-based e-mail, personal information management (PIM), notification, location services, embedded databases, Web content and instant messaging. This platform should also provide a rich set of tools for developing mobile applications and accessing core order entry, field service, repair, inventory, insurance claims processing and supply chain systems.

Consideration should be given to a middleware platform from an architectural, feature and integration perspective, which covers:

- New advanced capabilities in location-aware services, intelligent notification, device management, e-mail push and instant messaging
- Enhanced integration with portal applications for remote portlet access
- Database synchronization and offline forms
- A development toolkit to create, emulate, test and debug applications
- Support for cell phones, smart phones, and Palm, Pocket PC, embedded Linux and Symbian operating systems.

Extending the Enterprise

Deploying a wireless solution on a short-term basis can be a costly approach. The selection of a platform that employs an extensible uniform architecture as opposed to a single function approach should be considered. The solution selected must encompass an industrial-strength infrastructure, software, development tools and professional services for tight integration to core systems.

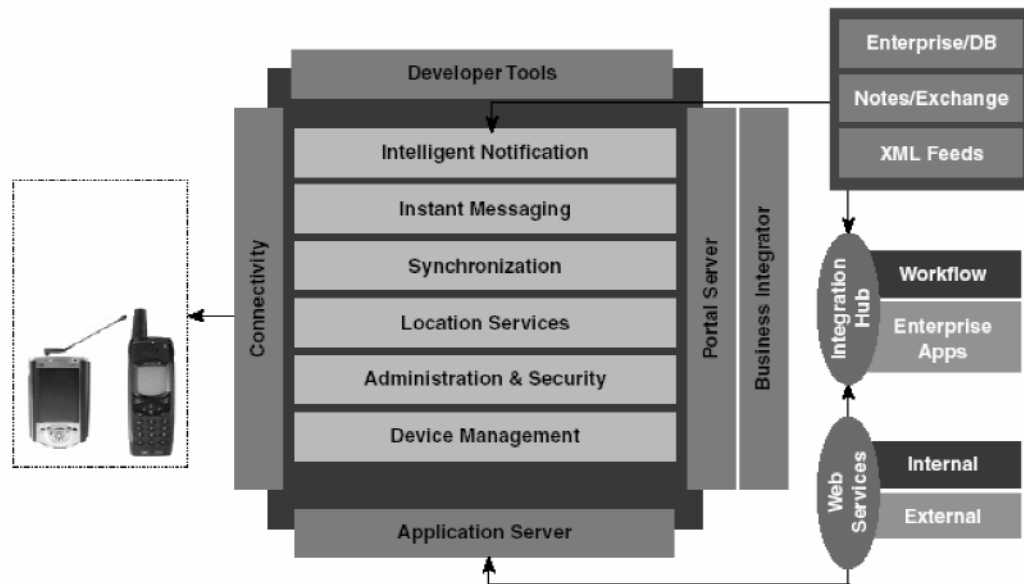
Location-aware services - Location-aware services enable enterprises to dynamically integrate mapping, routing and information directories within their applications for driving directions and proximity searching. With the latitude/longitude of the device provided by an onboard Global Positioning System (GPS), customers can now re-route crews for emergency response, or reschedule field service and deliveries.

Mobile instant messaging - With the advent of always-on wireless networks, mobile instant messaging is rapidly becoming one of the most powerful forms of instant communication. The

implications for instant messaging are compelling: enterprises can instantly message field service agents about work assignments, quickly answer questions and expedite decisions.

Mobility architecture - The considered architecture should specifically be able to bridge complex wireless environments with a single, scalable architecture and from a technical perspective be built to include an advanced set of data aggregation, programming tools, business workflow and application interfaces. In essence, it is desired to deliver a single access point to mobile devices for a wide range of services that extend business applications:

- A diverse set of connected and intermittently connected wireless devices
- Seamless integration with portals, and Java 2 Enterprise Edition (J2EE)
- Strong security and authentication capabilities



A core software platform provides both a mobile platform and a powerful entry point into back-end applications. By linking through portal and application servers to a business integration hub, field transactions can flow directly to core systems with speed and accuracy. Placing new orders, receiving alerts on inventory levels and requesting service parts on-site also allow enterprises to better manage their customer relationships. The net impact means a new generation of fast, agile workers who are tightly linked with line-of-business workflows.

Developing mobile applications - Wireless developers need a standards-based, functionally rich set of development tools to streamline the launch cycle for applications. To meet that demand, a comprehensive middleware framework that supports the development of mobile applications is desired. Some of the features to look for are: wizards for content development and adaptation to permit developers to code, emulate, test and debug applications without extensive experience or the actual device.

As the number of devices continues to rise, developers are facing an increasingly complex series of functions in each application. With certain applications, Web and portlet applications can now be written once and deployed to multiple devices with different characteristics, a big step toward rapid application development.

Recommendations

Although the market for wireless deployments is still emerging, many organizations have already started pilots and are now looking beyond basic office mobility features. The anticipation is that integrating the handheld device with front-end portals and core applications will yield strong returns in productivity, responsiveness and operational effectiveness. In order to take advantage of the deeper potential in wireless deployments, organizations should consider a five-point plan to efficiently extend, create, deploy and manage a new generation of applications:

- Analyze operational constraints and potential improvements, and build a detailed business case
- Evaluate wireless solutions using an e-business infrastructure that links the device to core business applications, databases and portals
- Quantify returns from both office (e-mail and PIM) and enterprise-class mobility, particularly in the areas of supply chain management, sales and field service
- Partner with a leading vendor on the basis of product capabilities, partnerships, future roadmap and financial stability and services expertise
- Design and build an infrastructure that is standards based, functionally rich, highly extensible and user friendly

As mobility goes mainstream, organizations may start folding mobile deployments into an enterprise-wide architecture, with options for utility-based computing and flexible financing. That approach could have major implications in terms of improving efficiency, building greater resilience and creating links between enterprises.

Radio Frequency Coverage

Successful wireless networks happen by design, not by luck. Designing a successful wireless network requires every bit as much careful planning as designing the wired network it extends. Planning begins by understanding the objective of the customer's wireless network and the environment in which it will need to operate. The RF site survey is the tool by which the designer gains an understanding of the environment.

The ultimate goal of a Radio Frequency (RF) site survey is to acquire enough information to determine the optimum number and placement of wireless infrastructure devices (quite often, but not exclusively, wireless access points) that provides adequate coverage throughout the required coverage area. In most implementations, "adequate coverage" means support of some minimum data rate as determined by the needs of the applications which will utilize the wireless network. These applications may have small data transport requirements (looking up part numbers in a repair shop, for instance) or much more intense requirements (downloads of large graphical files, perhaps). Except for the very simplest of environments (for example, a small three-room office) where one centrally located access point provides all the coverage necessary, site surveys are necessary to methodically consider the numerous environmental influences that can reflect, refract, absorb, and otherwise diminish or interfere with the propagation of radio waves sufficient to meet the data carrying objectives of the installation.

The 2.4 GHz radio band, where 802.11b and 802.11g devices operate, is a crowded space populated by microwave ovens, wireless telephones, baby monitors, arc welders, security cameras, Bluetooth devices, other establishment's access points, and many other unlicensed devices. The

5 GHz band (where 802.11a resides) is somewhat less crowded at the moment but the same considerations that might advocate for one customer's deployment of an 802.11a network advocate just as strongly for another customer's similar choice of frequency. In other words, the 5 GHz band is getting more crowded all the time. Any devices operating in one frequency within the operational domain of other devices operating in the same frequency are likely to interfere with or be interfered with by those other devices. It is the purpose of the site survey to discover those potential sources of interference so the wireless network designer can take steps to avoid them or limit their impact.

The site survey will also provide information necessary to help the wireless network designer determine antenna types and placement, access point radio power requirements, RF frequency reuse capabilities, wired infrastructure attachment points, provide redundancy, provide for seamless roaming between access points, minimize (or take advantage of) RF multi-pathing (a kind of self-interference which happens when radio waves, because of reflection off certain materials, do not all get to the receiving device at the same time). The objective of all of it being to get the deployment done correctly the first time. Without a good site survey there will inevitably be 'dead spots' in the RF coverage provided by the deployed wireless network, and these dead spots can be expensive to try to cover at a later date as, besides having to add new devices, it could mean having to move and/or reconfigure already installed devices.

Access Points (APs)

802.11 access points (APs) are the radio transmitters/receivers that are the basic building blocks of a wireless LAN network. These small devices are connected to a wired Ethernet, cable, or DSL connection to offer access to the Internet or an enterprise network. They search, detect, and connect to WLAN-enabled laptops, handheld computers, or other wireless client devices in a radius of a few hundred feet (the maximum range offered over standard 802.11b systems is 300 feet).

As vendors have started to sell WLAN gear to enterprise customers, rather than home networking types, so they have started to add features to their access points designed to address the technical requirements and security and management needs of the corporate crowd.

Here's a checklist of features that tend to differentiate corporate-class APs from their consumer cousins:

- Management information bases (MIBs) installed on the AP so an access point can be configured using Simple Network Management Protocol (SNMP)
- Implementations of the newest security specifications agreed on by the industry, such as Wi-Fi Protected Access (WPA), as well as Cisco and Microsoft specifications (LEAP and PEAP, respectively)
- Support for multiple wireless LAN radio standards—namely, 802.11b (11-Mbps over 2.4GHz), 802.11a (54-Mbps over 5GHz), and, more recently, 802.11g (54-Mbps over 2.4 GHz)
- Compliance with plenum ratings from the UL, which means they can be safely installed in the crawlspace in the ceiling of an office building
- Support for the Power-Over-Ethernet (POE) standard, which means that network managers only need to run one cable from the wired network to the access point.

E911

The wireless Enhanced 911 (E911) rules seek to improve the effectiveness and reliability of wireless 911 service by providing 911 dispatchers with additional information on wireless 911 calls. The wireless E911 program is divided into two parts—Phase I and Phase II. Phase I requires carriers, upon appropriate request by a local Public Safety Answering Point (PSAP), to report the telephone number of a wireless 911 caller and the location of the antenna that received the call. Phase II requires wireless carriers to provide far more precise location information, within 50 to 100 meters in most cases.

The deployment of E911 requires the development of new technologies and upgrades to local 911 PSAPs, as well as coordination among public safety agencies, wireless carriers, technology vendors, equipment manufacturers, and local wireline carriers. The FCC established a four-year rollout schedule for Phase II, beginning October 1, 2001 and to be completed by December 31, 2005.

Localities will fall far short of the FCC's goals for location-specific wireless E911 capabilities, according to a recent study issued by the National Emergency Number Association (NENA), a leading nonprofit 911 organization. Only about half of the public safety answering points in the nation will be E911 Phase II capable by the end of 2005, according to a study. More alarmingly, only 80 percent of the nation will have access to E911 Phase II capable public safety answering points (PSAPs) by the end of 2007, a date well beyond the FCC's initial goal of 2001.

The alarmingly slow installation rate is a sign that more work needs to be done on a local level to get the systems up and running. States should bear an increasing responsibility in stewarding E911 implementation among PSAPs, noting that PSAPs, particularly the small ones with less than five people that make up the bulk of the PSAPs in the country, lag behind in their ability to deploy E911 systems.

The problem is not only immediate resources, according to the NENA study. There is currently almost a \$1 billion shortfall in funding for the efforts to get E911 systems installed. Almost \$1.5 billion is needed to fund the effort every year.

The study incorporates guidelines on how to set up an E911 system technically, politically and financially for PSAPs and other interested parties. It does not provide a 'one size fits all' template, however, as each locality has to determine those needs by itself. There are still outstanding issues that weren't resolved and some dissent among participants over the details of some of the recommendations.

For instance, Cingular Wireless took exception to the study's call for \$3 billion in Congressional funding over the next five years for E911 implementation and called for a halt to state 'raids' on E911 money. It also opposed delay in the FCC's handset requirements, saying a delay in the commission's requirement that 95 percent of carrier customers have an E911 capable handset by 2005 'would run counter to' SWAT's implementation objectives.

Certain telematics services, as well as mobile satellite services, resold cellular services and broadband PCS mobile wireless services, including mobile prepaid calling card services, should all be subject to E911 requirements, commissioners said. The requirements vary from

service to service. For instance, MSS carriers that provide interconnected voice service calls are required to establish call centers for answering E911 calls and forwarding those calls to public safety answering points.

Quality of Service (QoS)

QoS and Network Characteristics for Quality

A quality telephone conversation and video sessions have dependencies on three common data network quality characteristics—latency, jitter & packet loss. It is expected that an internal network (LAN, MAN, WAN, WLAN, etc.) will provide leading edge industry standard latency, jitter and packet loss characteristics. This architecture expects each section of the data network to target the best possible performance levels. The current end-to-end design goals for quality voice for these characteristics are summarized in the following table:

	Campus	WAN	Voice equip. (including packetization, etc.)	Total
Delay	< 5 ms	< 55 ms	< 40 ms	< 100 ms
Packet loss	< 1%	< 1%	0	< 2%
Jitter	< 1 ms	< 15 ms	< 4 ms	< 20 ms

In a congested network, techniques are needed to control the proper balance of traffic from various applications in a manner to provide the appropriate levels of service needed by each. QoS is a technique for achieving consistent end-to-end delivery of the above characteristics. While congestion is most likely expected at the access leg, lack of QoS support at any congestion point along the path of a VoIP call may result in undesirable quality.

QoS is achieved by tagging data packets (coloring) so that network infrastructure can queue preferred packets preferentially. Since VoIP technology is relatively new, most VoIP devices have the ability to self-color their packets. VoIP data packets should be tagged with the DHCP value of "101 110" which is the industry standard for Real Time Services - Expedited forwarding PHB (EF).

Other Quality Considerations

Several other architectural and design characteristics can contribute to the quality of a voice call. These characteristics are listed here to be used as an overall checklist for designers to ensure proper consideration of all factors. They are:

- Codec selection
- Minimizing transcoding along a call path
- UA selection (hardphone, softphone) from approved and lab tested standards list; appropriate for the specific application

Reliability

The reliability of the service is typically measured in terms of its availability, with specific targets established in our standards and measured via our SLAs and end-to-end management tools. Reliability can be achieved via two means:

- **Use of Resiliency Techniques** - This architecture provides for the provision of resilient elements at critical points in the infrastructure. The designer has been offered architectural choices for providing this resiliency consistent with a variety of principles including risk (appropriate for the project), cost, etc.
- **Security** - Availability can also be impacted by malicious attacks. Designers are required to incorporate these techniques in their design.

Data Integrity & Interference

Data and information management involves managing the storage and retrieval of data, insuring the integrity of data during these operations, and protecting the quality of data from sources of interference.

In wireless and mobile environments, these tasks become much more difficult. As enterprise data moves to wireless and mobile environments, the risk of data being corrupted during transfer to enterprise information management systems is exponentially higher. Through radio or transmission fault, perfectly composed data can become corrupted or garbled. If this data is transferred into the enterprise information management system it threatens the quality and integrity of other data in the system. The key to defending against radio or transmission failure is advanced error-correcting messaging systems. Advanced messaging systems for mobile topologies provide guaranteed message delivery and integrity.

Any enterprise wireless system should use an advanced messaging system. Common messaging scenarios are information synchronization, notification services, and instant messaging. Advanced messaging systems guarantee the integrity of information synchronized from business data such as calendars and contact information or database data such as service inventories or customer information. Notification services used with advanced messaging provide guaranteed delivery of a wireless notification, removing any doubt about whether or not a message has been received.

In addition to message delivery and integrity, the security of the communication is critical. Secure communications products can provide Virtual Private Network (VPN) capabilities to mobile users. In addition, secure communications products for wireless use should also provide other advanced technology such as data compression and roaming across multiple networks and connection types. A secure, compressed, roaming wireless connection supporting applications using advanced messaging systems provides a safe operating environment for protecting data integrity.

The remaining critical component is information management at the wireless device. Traditional enterprise information management systems use transactions and structured query languages to provide atomicity, consistency, integrity, and durability for enterprise data. Wireless systems connected to enterprise information management systems should provide similar capabilities. Wireless or mobile databases can provide transactional capability and structured query language support. Critical properties of wireless and mobile databases and

information management systems are footprint, performance, and application development support. Wireless devices demand an operating footprint and offer unique challenges for achieving acceptable user performance. Wireless or mobile databases optimized for this environment often provide less functionality than a traditional enterprise information management system to achieve a smaller footprint.

When selecting wireless and mobile data management systems, always consider the skills and productivity of the application development team and how any proposed systems supports those skills through programming languages and application development tools.

Application Management

Application portfolio management involves continuous assessment of the application portfolio in terms of business value, enhancement potential, cost and technology concerns. Such comprehensive evaluations help facilitate strategic application development, maintenance, transformation and retirement, which, in turn, can help enterprises:

- Reduce costs and optimize value
- Align the application portfolio with business strategies
- Standardize business practices
- Implement shared services
- Increase speed-to-deployment

Specific Strategies for Cost Savings

When properly deployed, application portfolio management can facilitate application support, deliver marked cost savings and promote a more useful application portfolio overall. Application portfolio management drives transformation initiatives that are designed to enable organizations to:

- ***Prioritize maintenance activities and approval requirements*** - Maintenance actions should be segregated according to the importance of each application. This can help reduce maintenance spending and determine that maintenance funds contribute real value to the organization.
- ***Rationalize complex and/or undocumented code in critical applications*** - To reduce maintenance problems associated with legacy applications, organizations must first identify application architectures with complex code. Steps can then be taken (via software tools) to rectify the problem, which can decrease application downtime and help determine the extendibility of specific applications.
- ***Retiring redundant, outdated or low-value applications*** - Applications with similar or overlapping functions should be consolidated. Alternatives include extending existing applications to a broader group of users, or developing new, standardized solutions that are designed to eliminate redundant applications.

Application portfolio management is not a static, one-time exercise; rather, it is a continual and evolutionary process involving the assessment, rationalization, categorization and disposition of applications to achieve better strategic alignment with the business, higher usability and lower costs. Ultimately, these activities can increase the asset value of the application portfolio and minimize business constraints.

In almost every organization, the application portfolio is fundamental to day-to-day operations, and to supporting the future aims of the enterprise. Enterprises can transform their application portfolios—by activities such as upgrading, growing, retiring or consolidating those systems—with a focus on fulfilling strategic transformation initiatives. This process requires two distinct but equally critical phases of activity:

- **Portfolio assessment** - Collecting relevant application portfolio information, analyzing the information in the context of business and technical objectives, and identifying transformation opportunities.
- **Portfolio transformation management** - Identifying key business drivers and monitoring their effect on the application portfolio, providing governance and sequencing over transformation projects and activities, and measuring the business value of transformation projects against identified objectives.

Assessing the Application Portfolio: Identifying Gaps, Risks and Redundancies

The resulting data, along with information regarding the organization's business objectives, can then be used to align the application portfolio in a manner that is designed to provide direct business value. In this way, a vendor can strategically help an organization:

- Gain greater control over—and reduce the costs associated with—the maintenance and management of the application portfolio
- Focus application spending on supporting overall business strategies
- Create a customized application portfolio strategy designed to drive business value
- Access industry best practices, leading-edge technologies and expertise beyond what is available in-house.

In light of the current economic climate, organizations must prioritize and optimize spending effectiveness, achieve rapid and reliable ROI and otherwise streamline the enterprise. Toward these ends, application portfolio management involves a comprehensive assessment of—and transformation framework for—an organization's application portfolio systems, taking into account business, industry and technology priorities. The result? An application portfolio that can help reduce management costs and overall spending, meet the strategic needs of an ever-changing business environment, deliver process efficiencies enterprise-wide, and contribute directly to business objectives—all with limited risk.

Authentication & Encryption

The incorporation of a software platform that is capable of allowing enterprises to efficiently extend existing applications to mobile workers over many different wireless and wireline networks is one possible approach. Furthermore, it allows users with different application needs (based on transmission costs, coverage, or devices) to select the wireless network that is best for their specific situation.

This approach is based on a distributed, scalable, multipurpose communications platform designed to optimize bandwidth, help reduce costs, and help ensure security. It creates a mobile Virtual Private Network (VPN) that encrypts data over vulnerable wireless LAN and wireless WAN connections. It integrates an exhaustive list of standard Internet Protocols (IP) and non-IP wireless bearer networks, server hardware, device operating systems and mobile security protocols.

Functional Considerations

- Wireless network data optimization via improved data communication efficiencies for a Virtual Private Network (VPN)
- High level of security with AES, DES, 3DES, RC5, SSL, WTLS, and FIPS 140-2 certification
- Seamless cross-network roaming and session stability
- Network intelligence that senses, selects, and prioritizes network connections
- High reliability and scalability by supporting gateway clustering, distribution across multiple sites, and High Availability Cluster Processing (HACMP)
- Clientless connection to allow Web browser access to information behind the firewall
- Thin client access options
- Server integration with existing AAA via Remote Authentication Dial-In User Service (RADIUS) support, and directory via LDAP and ODBC databases
- Two-way messaging for WAP, SMS, packet radio, and paging networks

A communications platform for compression, security, and persistence to drive higher wireless data throughput and lower costs is critical. The platform needs to support highly encrypted access over a wide range of wireless and wireline networks.

The platform should also provide a standard TCP/IP communications interface to a variety of wireless, dial-up, and LANs with data optimization and security. The components that make up this platform should be designed to run on multi-vendor hardware and operating system platforms.

The ability to support a comprehensive spectrum of communication protocols for both IP and non-IP networks should be a consideration. Some offerings will allow for flexible connections to be created by configuring multiple Mobile Network Connections (MNC) for many combinations of public or private physical networks. Each MNC can be tuned for optimal performance, compensating for latency, link speed, and other characteristics that vary across different communications technologies.

Mobile Network Interfaces (MNI) and IP Addressing

MNI is implemented to allow the operating system IP layer to communicate with all supported wireless, dial, or wireline networks. The platform controls one or more IP subnets of users whose traffic is routed through the appropriate MNI. In order to help reduce and control data traffic, each MNI can be customized with packet filtering or packet mapping.

For mobile devices with an SSL-capable browser, connectivity for both unsecured HTTP and authenticated Hypertext Transfer Protocol over SSL (HTTPS) is supported. Light Weight Third Party Authentication (LTPA) token support enables single sign-on through Web servers or portals.

Mobile Access Services

An encrypted tunnel will help to secure wireless connections between the selected software and the mobility client, which work in conjunction to help offer enhanced functionality, improved performance, and a high level of security.

Applications are supported by using industry standard socket programming interfaces provided by the operating system. This helps reduce the need for developers to learn special programming interfaces or proprietary tools and protocols.

Cluster Support

Clustering helps enable a highly scalable architecture and distributes the load geographically across multiple sites to help adapt to the mobile needs of the customer. Support for HACMP helps obtain high reliability.

Security

Multiple levels of authentication and encryption are provided to help assure the identity of the mobile user, prevent unauthorized access, and protect data privacy. In addition to the mobile VPN option, SSL, WTLS, and PPP protocols are incorporated. Certification for FIPS 140-2, 197, 46-3, 186-2, and 180-1 Standards are critical for enhanced security within the public sector.

A symmetric encryption key encodes or decodes data with varying key lengths, the strongest being the 256-bit (AES). Customers can choose from DES, Triple DES, RC5, AES, and other algorithms.

A feature that will validate users against corporate Lightweight Directory Access Protocol (LDAP) directory servers and RADIUS-compliant authentication servers should be a consideration to enhance security.

Data Optimization

Certain connection management and client mobility applications can work in tandem to help reduce data transmission costs over wireless networks by utilizing advanced data compression, byte reduction, and minimization of Transmission Control Protocol (TCP) retransmissions. This helps reduce data loads, increase effective bandwidth, and can lower reconnection fees.

Messaging Services

Messaging services support several types of messaging modes, including SMS, e-mail using SMTP, unconfirmed WAP push, message delivery over proprietary networks such as Mobitex or Motien, and Simple Network Paging Protocol (SNPP). The Wireless Communication Transfer Protocol (WCTP) has been added to enable delivery of wireless messages to appropriate receiving devices.

Wireless Application Protocol (WAP)

With certain connection management tools, the management can be configured as a WAP proxy to provide connectivity for multi-vendor WAP V1.1 and WAP V1.2 client services. This could support the WAP WSP which links the microbrowser with cellular phones and PDAs.

Authentication and encryption offerings might also provide the ability to act as a WAP Push Proxy Gateway allowing external applications to push various content down to WAP devices. Wireless Transport Layer Security (WTLS) helps secure the connection to the WAP client, and SSL is used to establish a highly encrypted connection to the back-end Web servers.

Summary

Governments, and the organizations which support them, will be the largest implementers of advanced wireless and mobile networks of the future due to the enormous potential these networks have to efficiently and effectively leverage available resources for the community. In some areas, complete citywide network grids are already being planned using Wi-Fi, ad hoc and beam-forming technologies to provide uninterrupted wireless connectivity across entire cityscapes.

Comprehensive capabilities of wireless applications such as incident command and control, resource tracking, alarming and video, in addition to ubiquitous connectivity to people and networks will allow citizens and government to stay in touch with one another and government agencies to stay in constant communication with a vast array of resources and personnel.

In support of this new paradigm, the evolving wireless landscape will continue to benefit from lower costs, improved connectivity and bandwidth, new computing models and the results of entire new groups of highly motivated alternative network providers and their break-through technologies. This creates a new and dramatic opportunity and challenge for governments, not unlike the early stages of the Internet just ten years ago. For government, as the paramount user and beneficiary of wireless and mobile networks along with their associated devices and applications, there will be a new era of policy and decision-making required to manage these amazing new tools and to leverage them to provide maximum value in supporting and improving communities across the world.

Wireless Installation & Maintenance

Installation Issues

Design Considerations

An organization must be aware that the wireless local area networks (WLANs) will never behave or perform precisely like the wired network. Access points (APs) behave like a shared Ethernet hub. Prior to installation, the proper extension of technologies and policies to the wireless clients must be examined (security, etc.). With wireless, roaming capabilities (standards, features and capacity) must be examined.

Interoperability

Wireless cards from various vendors can provide very different range limits. It is important to understand that enterprise security and load-balancing features will typically not work with certain mixes of client radios. This is why you must differentiate between the specifications of the 802.11 standard and vendor proprietary features when making decisions about the equipment to be used. Beware of creating a "closed system" which will lock the wireless LAN into a vendor specific solution—especially if you will be supporting public areas where various cards will be used. Products that have obtained Wi-Fi (Wireless Fidelity) certification will, at a minimum, guarantee a basic level of interoperability.

Installation Issues For Wi-Fi

Access points typically support 20-25 users. A site survey is critical to optimize access point location and density. Hardware antenna selection can alter how the radio signal propagates. PoE (Power over Ethernet) allows for both data and power to be delivered via Cat5 cabling. Use of PoE eliminates the expense of delivering AC power to wireless access points and can reduce your installation costs.

Wireless LAN System Components

Wireless Client Receiver - Wireless LAN client receivers are needed to connect a computing device (e.g. laptop, PDA, desktops, etc.) to the wired network via an access point. The receiver takes care of data processing in the physical and MAC layer of the OSI framework. Depending on the interfaces of the computing devices, there are different forms of receivers, however most of them come in PCMCIA and Compact Flash cards, PCI/ISA adapters, or USB adapters.

Access Point - Access points are needed only in the Infrastructure Mode of WLANs. They provide the wireless clients with a point of access into a network, as its name already suggests. They are comparable to a sophisticated Ethernet switch and operate in half-duplex mode, i.e. they either receive or transmit at a given time. APs can be used in different constellations, and therefore support three modes of operation known as Root Mode, Bridge Mode, and Repeater Mode:

- In the Root Mode, the AP is connected to a wired network and the wireless client directly accesses this network via the AP. Also, several clients can talk to each other by means of using APs that are connected to the same backbone network. Root Mode is the default configuration of most APs.

- The Bridge Mode of APs makes it possible to wirelessly connect two separate wired network segments with each other. No clients use the AP to enter a network. The bridging functionality of APs is only found in a few commercially available APs, which are significantly more expensive than their non-bridging counterparts.
- An AP in Repeater Mode provides a wireless upstream link into a network instead of being hard-wired to the network and using its Ethernet port. It functions as intermediary between the clients and an AP in root mode for entry into the network, and is thought to either extend the perceived range of a WLAN or to make WLAN deployment possible in difficult environments. Since an AP in repeater mode connects to another AP (root mode) and the wireless clients, its throughput is reduced dramatically. The repeater mode should only be used if absolutely necessary.

WLAN Antennas - The wireless transmission of data and voice necessarily needs antennas—at sender and receiver—for proper operation. The selection of appropriate antennas can impact the functionality of a system dramatically. However, none of the WLAN standards regulates the use of antennas and one is free to choose. It should be noted that adding an antenna does not increase the power you originally started with, but focuses it in a particular direction as to increase reception, and also limits the beam radius. Proper installation of the antenna is crucial. There is a wide range of antennas available and the following description of antennas and parameters may help in selecting the correct one for a given application:

- **Omnidirectional Antennas** - radiate the signal outward equally in all directions. They are shaped like a tall pole and have their highest sensitivity in horizontal direction. They are used to cover large areas where the exact location of the receiver is unknown. One disadvantage is that an omnidirectional antenna picks up a lot of noise surrounding it and distributes the transmit power over all directions making for a weaker signal.
- **Sectorized Antennas** - have a similar shape of omnidirectional, but have reflectors behind the pole that direct the transmitted energy in a certain direction. Mostly these sectors are 60° to 120° and form the radiation pattern as needed. This kind of antenna is used when multiple clients need to access an AP from the same direction. They increase range and decrease interference.
- **Yagi Antennas** - consist of multiple elements that are all aligned to guide incoming radio waves from a particular direction to the receiving dipole of the antenna. They are similar to old TV aerial, but smaller in size. They are very directional and the radiation pattern has an opening angle of anywhere from 15° to 60°. Adding more elements means more gain, a longer antenna, but also more cost. These antennas are used for point-to-point or point-to-multipoint application where long distances need to be spanned.
- **Parabolic (dish) Antennas** - are the most directional antennas and deliver the highest gains. They are tightly focused on a distinct direction, which makes them ideal for point-to-point operations. The dish can either be a meshed wire grid or solid metal. The diameter ranges from several inches to a few feet. A correctly aligned pair of parabolic antennas can extend the range of wireless networks up to 20 miles.

Polarization plays an important role in antennas. This parameter refers to the direction the electro-magnetic waves travel through the air. This can be horizontal or vertical, but also—in very rare cases—a circular polarization is used. The transmitter and receiver must be used in the same polarization or no communication is possible. Omni-directional and sectorized antennas are vertically polarized, whereas Yagi and parabolic antennas can be either horizontally or vertically polarized, depending on environment and application.

Maintenance Issues

Access points have grown highly reliable when supported with clean power, and hardware is more durable than ever. But WLANs do require maintenance. Security, for example, must remain top of mind. At minimum, Value Added Resellers (VARs) or users need to periodically change WEP codes and SSIDs and reassess needs as applications and relationships change. Software network management tools and debugging tools are available to help the VAR's or customer's centralized network management departments identify and solve problems before system failures occur. It is essential to have these tools available and support staff trained to use them.

Since WLAN technology is continually advancing, both hardware and software manufacturers update their software and firmware for access points and mobile computing client devices multiple times per year. Support personnel must be aware of these changes and determine if a software upgrade is beneficial to the network or application. Some of these issues can be managed centrally with the latest software utilities and version control server software. Annual site re-surveys guarantee the level of system performance and RF coverage and mitigate possible radio frequency interference issues. Many facilities and inventory layouts change over time, so performing periodic site surveys is valuable.

Supporting the Mobile Workforce

Supporting the mobile workforce requires recognition of, and strategies for the implementation of, new technology and support models such as:

- Focus on self-enabling technologies
- Easy access anywhere, anytime
- Migration to Internet based technology models
- Shift investments in technology toward client based work

Mobile working is a reality and, as a result, mobile devices are almost certainly being used in your organization, whether you know it or not. Studies show that most PDAs are being purchased by individuals, rather than organizations, but are used for essential business matters, such as managing activities, accessing emails and keeping contacts in order. There are elements to implementing and supporting mobile devices that are unique, but this is not reason enough to treat them separately from your overall IT infrastructure. Doing so will lead to long-term problems integrating mobile working into your existing enterprise IT strategy.

Support for mobile workers should be considered as part of the overall IT infrastructure and not an added extra. Therefore, when deciding on what devices are used and support needed, this should be done in exactly the same method as systems for office based workers. A mobile worker needs to be provided with the same degree of support as a desk-based worker, even if sometimes this requires a little more thought on how it will be delivered. Essential services must include access to help desks, asset management, procurement and hardware support. It is easy for mobile workers to feel alienated from the office based 'mainstream' and IT strategies should not reinforce this.

Until ubiquitous connectivity is a reality, travelers will continue to utilize slow, unpredictable network connections to conduct their business. These systems need to remain managed in order to ensure access to critical business applications, as well as maintain up-to-date security

configurations, while also providing IT with visibility into application configuration, presence, and usage.

Flexible Workplace Options

Organizations increasingly find themselves faced with supporting high performance workspaces having the following requirements. They must:

- Facilitate interaction and knowledge exchange
- Foster and support community within the organization
- Provide for employee comfort and safety
- Respect local culture
- Respect work/life balance through remote work opportunities

As enterprises become increasingly mobile, more business is conducted by roaming and infrequently connected users who need the same access to critical business applications and security patches available to the desk worker. Users frequently traveling between multiple sites require the same level of cost effective management as is provided for users in a fixed location. One of the problems when implementing a mobile strategy is the temptation to oversimplify. With the proliferation of different devices it is inevitable that what works for some users will not meet the needs of others.

One of the first problems facing any organization is how to budget for mobile support. Support can vary massively in cost, and what might be expensive but essential for one organization may be needlessly costly for another. Take a hard and honest look at what you require and ensure you know what it costs and why. Gartner predicts that by 2005, PDAs and mobile appliances will raise enterprise total cost of ownership for user devices by 10%.

When rolling out a mobile IT strategy, ensure that you understand the benefits and communicate them properly. It is a frequent mistake to assume that all people are excited by new technologies when many are, in fact, resistant. Thirty per cent of managers in a recent Fujitsu Services survey said they would not currently feel comfortable using a PDA because they did not understand the benefits that their use could bring.

To make any support strategy work, training must have a major role. Initial research suggests that typically, only 10 per cent of software application functionality is properly used. An educated workforce is an effective workforce, able to maximize the investment made in mobile devices and their support, as well as less likely to drain support service. A dollar spent on training in IT can often save countless more.

Whether you are choosing a company to supply your mobile devices, implement your mobile strategy or provide the ongoing support, choose wisely. Implementing a proper support strategy for mobile workers is undeniably complex, due to the number of variants involved. Times are tough, budgets are shrinking and it is vital that you get expertise for your money.

Remote Access To Data/Applications/Co-Workers

One of the exposures of mobile computing is that it is easy to work outside the normal jurisdiction and rules of in-house IT support. Data is vulnerable and security must be a priority. People lose these devices and they can be stolen. What happens to the data on these devices when they get stolen? What happens if somebody then takes that device and accesses your network? These implications need to be looked at. Keep it simple, keep it effective and ensure data is regularly backed up by the right technologies and the risk of virus attacks is minimized. This need not be costly and time-intensive, but can often be an automated process. Issue guidelines to mobile workers to ensure that they understand how to protect themselves and the organization from security breaches and hackers.



Wireless Applications & Uses

Wireless technology provides the ability to replace traditional wired applications and give users the freedom to roam. No longer must you be tied to a desk, or limited by your length of cables. The potential applications for wireless technology are far-reaching and cover every area of government. While the following list is far from exhaustive, it is meant to give an overview of some of the potential applications in a government setting.

When talking about the applications and uses of wireless technology, the first area that needs to be addressed is the multitude of devices that are available to take advantage of the wireless wave. From handhelds to laptops, pagers to smart phones, the devices that help facilitate wireless applications are as plentiful as the range of applications. Each device has positives and negatives—size vs. battery life, readability vs. portability, etc. Different devices are better suited for certain applications.

On-line vs. Off-line Wireless Applications

There are different levels of wireless access, and some devices are better suited to specific applications. On-line wireless applications access stored information on a remote server and require constant connectivity. No data is stored on the portable device so if the connection is unavailable the application cannot be used. An example of this type of application would be a browser application running on a wireless device that simply displays data from a back-end system.

Off-line applications work with devices that can store data locally. A copy of a table or database is stored on the portable device so work can be accomplished and information accessed even if the wireless connectivity is temporarily unavailable. When the connectivity is restored the device either uploads all the data from the portable device, or the information is synchronized to a back-end data store. An example of an off-line wireless application may be an order system. The user can create an order, pull item details from a table stored on the wireless device, but the order is not processed through the back-end system until connectivity is reestablished.

Cross-Functional Wireless Applications

There are quite a few generic applications of wireless technology that cross all division and department boundaries within the public sector. Independent of the critical business function of different agencies, there are several basic IT or tracking applications that have been transitioned to wireless solutions.

LAN/WAN Connectivity

While this seems very basic, the ability to connect to a LAN without being constrained by hard-wired connections is probably the most widespread use of wireless technology today. Allowing users to take their laptop and work from a variety of locations in the building, or other office locations. To authenticate to a network, have file access, and a roaming Internet connection.

Remote Data Access

Regardless of the type or makeup of the data, having wireless connectivity to securely access information from remote data stores opens doors in a wide variety of areas.

Asset Tracking

With and without the use of barcode technology (or RFID), having the ability to remotely track physical assets for an organization eliminates the duplication of documenting in the field and then having to re-enter or transfer that asset information into the actual database. Asset tracking implementations are again, some of the most prevalent uses for wireless technology.

IP Phone Service

Both fixed LANs and now wireless LANs can carry VoIP traffic effectively. These wireless VoIP systems are ideal for hospitals, retail stores and other corporations that want to keep their employees connected. As long as users are within range of a wireless access point, they can make and receive calls and even use the handheld device's functions at the same time. With a combination of a wireless infrastructure and an IP-based phone system, wireless VoIP becomes an integral part of the mix.

Vertical Applications in the Public Sector

Homeland Security

When most people think of the applications of wireless technology in a homeland security environment, they think first responder access. Gaining access to other agencies, personnel, or data in the event of an incident or disaster can be the difference between life and death. Wireless can provide this communication bridge in times of crisis.

Other homeland security applications might include the ability to track or disable equipment remotely. Tracking biological tools/weapons to a central location, allowing sensor devices to be placed in remote locations and report back to a specific program or office.

Public Safety & Criminal Justice

Public safety applications include portable devices which allow instant reporting to criminal databases and retrieval of information during incidents, rather than after the fact. Access to remote data can make the difference between a routine stop and apprehending an individual with a history of criminal activity.

Probation officers and case workers can have a traveling office. With the appropriate middleware, databases can be accessed over the Internet with instant update capability, eliminating the duplication of processes and making workers more productive in the field. Lowering dispatch times for related groups/agencies to respond with the next level solution.

Education

All levels of education can benefit from the introduction of secure wireless technology. Internet access is just the beginning. Access to student records, class enrollment, on-line course materials, e-mail, file sharing, and attendance tracking are just a few of the many potential wireless applications.

The use of wireless connectivity in schools has increased, particularly in rural districts, where there's a lack of traditional communications companies willing to support educational bandwidth needs at affordable prices.

Health Care

The health care industry was an early adopter of wireless technology. Most applications have been set up in a controlled environment, using a limited number of devices, with heavy security consideration. Giving doctors the ability to see all lab reports and patient files on roving laptops that can be wheeled into patient rooms, leaves less room for error in the transmission of orders.

Emergency room admissions and triage can be handled through wireless sensors and portable devices. Even RFID has a potential use in health care, tracking the patient from admittance through release, having tests and patient records available immediately, in patient rooms, rather than at specific workstations.

Transportation

Although traffic monitoring, road condition tracking, and remote camera/monitoring equipment all have been implemented as wireless applications, the most common transportation use is tracking of trucks and cargo.

Wireless systems can provide for real time, automated two-way communication between delivery drivers and customer service personnel in order to:

- Locate drivers
- Dispatch drivers for new customer orders
- Confirm order status
- Communicate driver delays / problems / cancellations
- Capture delivery confirmations and signatures for immediate access by customer service representatives and/or the customer

Appendix A - Wireless Standards

The Institute of Electrical and Electronics Engineers, Inc., (IEEE) has established the following standards categories for 802 Wireless. Within these categories, IEEE has either approved or is proceeding to approve specifications.

802.11 (WLAN/Wi-Fi)

802.11 - IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Media Access Control (MAC) and Physical Layer (PHY) specifications: High Speed Physical Layer in 2.4 GHz band

Common Name - Wi-Fi, LAN

Status - Approved 1999, Reaffirmed 2003

Scope - Base standard in the 802.11 family of IEEE standards. Applies to Wireless LANs and provides 1 or 2 Mbps in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spectrum (DSSS) between a wireless client and base station or between two wireless clients.

802.11a - High Speed Physical Layer in the 5 GHz band

Status - Approved February 11, 2000, Reaffirmed 2003

Scope - Extension to 802.11. Provides a Higher Speed PHY and used in conjunction with the 802.11 MAC in fixed, moving or portable Wireless Local Area Networks. Supports data, voice and image information services. Provides up to 54 Mbps in the 5 GHz band and employs orthogonal frequency division multiplexing as an encoded system.

802.11b - 1999 - High Speed Physical Layer in 2.4 GHz band

Common Name - 802.11 High Rate, Wi-Fi, WLAN

Status - Approved February 11, 2000, Reaffirmed 2003

Scope - Extension to 802.11. Applies to Wireless LANs and provides 11 Mbps (with fallback to 5.5, 2 and 1 Mps) in the 2.4 GHz band. Provides Ethernet like functionality and uses only the direct sequence spread (DSSS) approach for data, voice and image information access, Range limits at 1 Mps - outdoors 500 meters and indoors 150 meters. Signal quality is consistent within range. Upward compatible with 802.11g.

802.11g - 2003 - Further Higher Data Rate Extension in the 2.4 GHz band

Status - Approved October 20, 2003

Scope - Extension to 802.11b. Increases the data rate achievable by 802.11b devices with a new

PHY extension. Improves access to fixed network LAN and inter-network infrastructure (including access to other Wireless LANs) via a network of access points and the creation of higher performance ad hoc networks. Backward compatible with 802.11b devices but communication speeds will be that of the lowest speed 802.11b device connected. Provides 20+ Mbps in the 2.4 GHz band.

802.11n - Enhancements for Higher Throughput

Status - Under Development; Project Initiated September 11, 2003

Scope - Extension to the PHY and MAC layers of 802.11 so that modes of operation can be enabled with much higher throughput to a maximum of at least 100 Mbps as measured at the MAC data services access point. The effort is often referred to as "turbocharged 802.11g."

802.1X - IEEE Standard for Local and Metropolitan Area Networks - Port-Based Access Control

Status - Approved October 25, 2001

Scope - Basic specification of mechanisms to allow network access decisions, using higher layer authentication and authorization protocols, to be enforced at individual ports of a networked system.

802.1AE - IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security

Status - Under Development - New project Initiated September 11, 2003

Scope - Provides the specifications for connectionless user data confidentiality, frame data integrity, and data origin authenticity by media access independent protocols and entities that operate transparently to MAC clients. Facilitates secure communications over publicly accessible LAN/WAN media and expands use of 802.1X to additional applications.

802.11i - IEEE Standard for Local and Metropolitan Area Networks: Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Method (MAC) Security Enhancements.

Common Name - Wireless Protected Access (WPA)

Status - Under Development, Amendment Initiated May 30, 2001

Scope - Enhances the Medium Access Control (MAC) to provide improvements in security and authentication mechanisms.

802.15 (WPAN)

802.15.1 - 2002 - IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN - Specific Requirements - Part 15: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)

Common Name - WPAN, PAN, Bluetooth

Status - Approved July 26, 2002

Scope - Provides PHY and MAC specifications for wireless connectivity with fixed, portable and moving devices within or entering a Personal Operating Space (POS) that extends up to 10 meters in all directions and envelopes the person whether stationary or moving. Coexistence with all 802.11 networks is provided with a low complexity, low power consumption for devices worn, carried or located near the body.

802.15.2 - 2003 - IEEE Recommended Practice for Information Technology - Telecommunications and Information Exchange Between Systems - LAN/MAN - Specific Requirements - Part 15.2, Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Bands.

Status - Approved October 15, 2003

Scope - Provides specifications for a Wireless Personal Area Network (WPAN) 802.15.1 devices to coexist with other selected wireless devices that operate in the unlicensed frequency bands.

802.15.3 - 2003 - IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN - Specific Requirements - Part 15.3, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Personal Area Networks (WPAN)

Common Name - WPAN-HR

Status - Approved October 20, 2003

Scope - Defines MAC and PHY specifications for high data rate wireless connectivity with fixed, portable or moving devices within or entering a Personal Operating Space (POS). Provides low complexity, low cost, low power consumption solution at a data rate of 20 Mbps to support multimedia needs and data types.

802.15.3a - Amendment to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN - Specific Requirements - Part 15.3, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher Speed Physical Layer Extension for the High Rate Wireless Personal Area Networks (WPAN)

Status - Amendment Under Development; Project Initiated December 11, 2002

Scope - Provide an alternative PHY for 802.15.3 comparable to the features of 802.11.3 but with a data rate of 110 Mbps or higher for more advanced multimedia data types in multiple co-located systems.

802.15.4 - 2003 - IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN - Specific Requirements - Part 15: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Personal Area Networks (WPAN)

Status - Approved May 12, 2003

Scope - Defines the MAC and PHY specifications for low data rate wireless connectivity with fixed, portable and moving devices with no battery or very limited battery consumption operating in a Personal Operating Space (POS). Raw data rate ranges from a maximum of 200 Kbps to satisfy a simple need for interactive capability and scalable down to sensor or automation needs at 10 Kbps or less.

802.16 (WiMax)

802.16 - 2001 - IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN /MAN Specific Requirements - Part 16: Air Interface for Fixed Broadband Wireless Access Systems

Common Name - WiMax, MAN, 3G

Status - Approved May 24, 2002

Scope - Defines the basic Medium Access Control (MAC) and Physical Layer (PHY) of the air interface for interoperable fixed point to multipoint broadband wireless access systems. Transport of data, video and voice services are supported in the vicinity of 30 GHz but generally applicable to systems operating between 10 to 66 GHz. An alternative to wireline broadband access.

802.16.a - 2003 - Amendment to IEEE Standard for Local and Metropolitan Networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems - Media Access Control (MAC) Modifications and Additional Physical Layer (PHY) for 2-11 GHz.

Status - Approved May 27, 2003

Scope - Expands 802.16 to include 2 to 11 GHz for use in residences, Small Office/Home Office, telecommuters and Small and Medium Enterprises. PHY is specified for both licensed and unlicensed (mesh topology) supporting data rates of DS1/E1 or greater.

802.16e - Amendment to IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems - Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed bands

Common Name - 3G, Universal Mobile Telecommunications Systems (UMTS)

Status - Amendment Under Development; Project Initiated December 11, 2002

Scope - The specification will provide enhancements to 802.16 and 802.16a to support subscriber stations moving at vehicular speeds up to 120 Km/h. The specification defines the system for combined fixed and mobile wireless access with the higher level hand-offs between base stations and sectors detailed. Operations is limited to licensed bands between 2 and 6 GHz and meets the needs between very high rate Wireless LANs and very high mobility cellular systems.

802.20 (WiMAN)

802.20 - Local and Metropolitan Area Networks - Standard Air Interface for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility - Physical and Media Access Control Layer Specification

Common Name - WiMan, MobileFi, WAN and 4G

Status - Standard Under Development; Project Initiated December 11, 2002

Scope - Specification defines the PHY and MAC layers of the air interface for interoperable mobile broadband wireless access systems, operating in licensed bands below 3.5GHz, optimized for IP-data transport, with peak data rates per user in excess of 100 Mbps. The standard will support various mobility classes up to 250 Km/h in a MAN environment and targets spectrum efficiencies, sustained user data rates and user populations higher than that achieved with 802.16. Addresses access to Internet, intranet, enterprise applications and commercial infotainment services. The specification will support FDD (Frequency Division Duplexing) and TDD (Time Division Duplexing) frequency arrangements which are orthogonal frequency division multiplexing techniques.

Voice over Internet Protocol (VoIP)

The Voice over IP (VoIP) standard that has been most widely adopted is H.323 that has been sponsored by the International Telecommunications Union (ITU-T). H.323 defines standards for Terminals, Gateways, Gatekeepers and Multiple Control Units (MCU). In reality H.323 is one component of a family of standards (H.324, H.320, H.321, H.310 and H.322) that define communication over other networks.

Radio Frequency Identification (RFID)

The Radio Frequency Identification (RFID) standard has two major definitions at this time. U.S. commercial enterprises (most notably Wal-Mart) and the U.S. Department of Defense have each selected different alternatives to be placed in effect in January 2005.

DOD supports the upcoming ISO/IEC1800 specification as DOD always adopts International Standards Organization (ISO) standards. The alternative standard is EPCglobal sponsored by the Uniform Code Council and EAN International. Some of the essential differences center around the special higher frequency ranges (135 kHz below, 13.56 MHz, 2.45 GHz, 5.8 GHz and UHF) needed by DOD whereas the EPCglobal standard is far more narrow. ISO1800 operates in coordination with ISO15962 (Data Syntax), ISO15961 (Tag Commands), ISO15963 (Tag Identification & Registration), ISO15418 (Application Identifiers), ISO15434 (Transfer Syntax) and ISO15459 (Transport Unit) which detail many of the specifics for the ISO solution. Both alternatives are under rapid development with convergence expected in the future.

3rd Generation (3G)

The 3G effort is supported by the International Telecommunications Union for broadband, packet-based transmission of text, digitized voice, video and multimedia at data rates up to and possibly higher than 2 Mbps with the objective of consistent services to mobile computer and

phone users worldwide. 3G has proven to deliver a data transfer rate of only 384 Kbps, suffering from incompatible hybrid versions and very high capital investment implementation costs that produce an unattractive ROI. 3G is digital packet switched technology.

Wireless Application Protocol (WAP)

WAP is an industry sponsored defacto application standard for mobile users with wireless devices. The industry group (WAP Forum) is composed of some 450 wireless solution providers and Internet companies that include handset manufacturers, carriers, infrastructure providers and other solution providers to the wireless community. The current release (v.2) embraces architecture, client identification, client provisioning, external interfaces, general formats, messaging services, persistence, pictograms, push, synchronization and agent profiles.