White Paper

Enabling a Successful Wireless Enterprise

Sumit Deshpande, Office of the CTO
January 2006

Enabling a Successful Wireless Enterprise

The demand for and adoption of mobile technologies and devices in the enterprise is increasing at a phenomenal rate. Simultaneously, the capabilities of mobile solutions, as well as the underlying mobile landscape, are changing rapidly. These changes create the need for solutions that facilitate the long-term growth and success of mobile enterprise initiatives. As a result, software vendors must provide comprehensive solutions to manage, secure and maintain the mobile infrastructure, while fostering development, integration and access to applications and information over wireless media. By leveraging initiatives, innovative technologies and a broad array of strategic business alliances, CA delivers comprehensive mobile enterprise solutions to promote customer success.

Understanding the Mobile Landscape

The use of mobile technologies is steadily rising for both business and personal applications. Mobile phones are a common sight, and many people use personal information management (PIM) devices, palmtop computers and personal digital assistants (PDA) to manage their schedules, contacts and other essential functions. Employees on the move appreciate the value of staying connected with the enterprise and other resources through mobile phones. In fact, most enterprises have corporate mobile phone plans that make it easier for mobile employees to stay in touch and increase productivity, regardless of their physical location.

With rapidly advancing technologies, most wireless carriers offer to transmit data and voice signals. For example, you can now receive email on your mobile phone in addition to regular calls. With the proliferation of wireless-enabled PDAs, Blackberry-type mobile email devices and notebook PCs, it is important to ensure that mobile employees are connected to and supported by the enterprise.

Although the terms "mobile" and "wireless" are similar in theory and often used interchangeably, they are in application very different:

- Mobile pertains to the ability of an entity to be on the move.
- Wireless pertains to the technology that allows transmission of voice, data and other content through radio waves without being restricted to cables or other physical media.
- Mobile devices are portable electronic hardware components that are used by mobile employees to do their work.

Wireless technology facilitates employee or enterprise mobility. Mobile devices depend on wireless technology to connect to the enterprise and transfer content to fulfill the users' business needs.

It is not surprising that an increasing number of employees are demanding mobile support from their enterprise to maximize performance. In fact, recent studies have shown that mobile employees connected to the enterprise are much more effective than if their enterprise did not support a mobile workplace. For employees whose work is mostly away from their desks, this is an important issue.

Mobile employees have a long list of enterprise capabilities needed to support their work. Here are some basic requirements:

- Mobile connection via laptops so that work can be done anywhere
- The ability to connect to enterprise assets wirelessly using laptops, PDAs, mobile phones and other devices for flexible access to business processes
- Advanced protection of information on wireless devices to ensure that confidential business information is not lost or stolen
- Real-time synchronization of information to ensure accuracy and consistency
- Appropriate alerts and messages to the mobile device to carry out required job functions with optimal efficiency

These expectations are quite typical, and the mobile infrastructure today can deliver them with significant success. Within the dynamics of the wireless industry, new demands and challenges related to a mobile work force are springing up constantly.

Most new technology goes through initial hype, education and experimentation before there is widespread implementation and the enterprise realizes the true usefulness of the technology. Wireless is no exception. Figure 1 depicts the perceived status of wireless technology adoption in the enterprise for 2004.

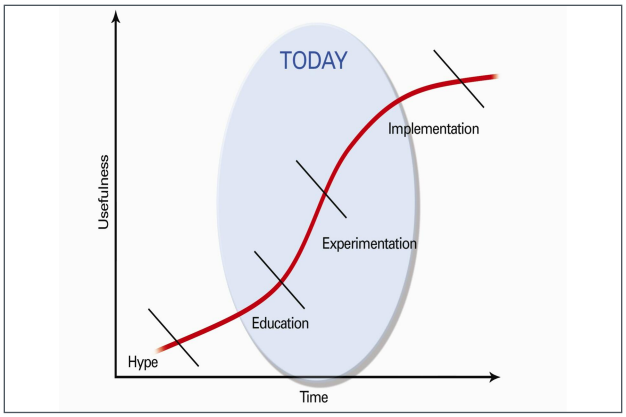

Figure 1: Increasing Awareness and Usefulness of Wireless Technology in the Enterprise

Note that the line between computing and telephony is slowly blurring. Several devices available today combine the features of mobile phones and PDAs. Eventually, it is likely that we will carry one device to handle our scheduling, email, Web surfing, videoconferencing, document management, and business and personal phone calls. With data storage capabilities and network bandwidth steadily improving, it won't be long before we have the capabilities of today's high-end desktop computer available in a device that fits into our pocket. One can only speculate about the ramifications this convergence of devices will have on the way we work and how enterprises function.

Wireless Industry Standards

No technology works in a vacuum. Many entities work at different levels to bring the technology to a more mature and usable state. Standards and specifications are conceived, developed and then implemented. Currently, most standards bodies for the mobile and wireless environment are focused on issues related to hardware or infrastructure. Listed below are some of the more important standards organizations related to the wireless industry:

- The Wi-Fi Alliance seeks to attest interoperability of products based on the 802.11b specification and certify them compatible with Wireless Fidelity (Wi-FI). It endorses Wi-Fi as the global wireless LAN (WLAN) standard across all market segments.
- The Institute of Electrical and Electronics Engineers (IEEE) does extensive research in technology spanning a broad spectrum. It created the 802.11 standard for wireless networks and is instrumental in creating security protocols such as Wired Equivalent Privacy (WEP). The IEEE does not provide certifications of any kind for its specifications.
- The Open Mobile Alliance (OMA) consolidated the efforts of the WAP Forum, SynchML and other mobile technology groups. Under a broader umbrella, the OMA is bringing together wireless device manufacturers, software solution providers, wireless operators and other related entities to facilitate an open environment for mobile applications and networks.

Many other organizations such as the W3C and Wireless DSL Consortium have standards that directly affect the wireless industry, although they are not specific to wireless communications. For example, XML and Web services standards are increasingly part of the development and deployment to server and desktop processing, but they are equally applicable to wireless application. Several new standards groups are forming to address specific issues regarding enterprise mobility.

Despite the prevalence of standards committees in the wireless industry, there is no single unifying standard. It is important for enterprises to consider all aspects involved in supporting a mobile work force. Some key criteria in choosing a wireless network specification include:

- The number of devices in the wireless network
- The range of transmission
- The average size of data transfers
- The speed of the network
- Security measures
- Quality of service

Depending on the above criteria, organizations can decide on what kind of wireless network to deploy.

802.11 Wireless LANs

Wireless LANs may operate in one of two modes, ad hoc or infrastructure:

- **Ad hoc mode (peer to peer) –** Each mobile device, also known as a mobile client, communicates with the other devices in the network, within a specified transmission range or cell. If a client has to communicate with a device outside the specified cell, a client within that cell must act as a gateway and perform the necessary routing. Advanced implementations of this technology are used in wireless mesh networks. Most enterprises discourage the use of ad hoc networks because of inherent security risks such as unauthorized devices connecting to a device in ad hoc mode and copying information.
- **Infrastructure mode (WLAN) –** Communications among multiple wireless clients are routed by a central station known as an access point. The access point acts as a bridge and forwards all communications to the appropriate client in the network, whether wireless or wired. Besides having routing mechanisms, the access point also has as a Dynamic Host Configuration Protocol (DHCP) server and other features that facilitate wireless communications in a small to large business environment. Access points geared towards home use do not have advanced management features such as Management Interface Base (MIB) interfaces and load balancing, which are required for corporate networks or high-traffic environments. A wireless client must first be authenticated and then associated with an access point before it can perform any communications. Figure 2 shows a typical WLAN environment.

The 802.11 specification, defined by the IEEE, is used as an extension of Ethernet-to-wireless communications and is quite flexible about the kinds of network traffic that pass over it. It is primarily used for TCP/IP but also supports AppleTalk and other PC file-sharing standards.

Figure 2: A Typical WLAN Environment

The 802.11 specification, defined by the IEEE, is used as an extension of Ethernet-to-wireless communications and is quite flexible about the kinds of network traffic that pass over it. It is primarily used for TCP/IP but also supports AppleTalk and other PC file-sharing standards. Disparate systems such as PCs and Macs can communicate over 802.11 by using PC or PCI cards, as can some of the newer hardware using Universal Serial Bus (USB) and other forms of 802.11-based wireless network cards. Adapters for PDAs such as Palm OS and PocketPC-based devices are also available.

802.11 in its various forms is the standard wireless network deployment platform for enterprises and public-area wireless networks such as those found at airports, hotels, conference centers, and coffee shops and restaurants. The coverage distance depends on line of sight and obstacles.

802.11b

This was the first protocol widely adopted by enterprises. It facilitates the wireless transmission of data at 11Mbps, at distances ranging from a few feet to several hundred feet over the standard 2.4-gigahertz (GHz) unlicensed band.

802.11a

This specification transmits at 54 Mbps over the 5-GHz band. This is ideal for large data file transfers and bandwidth-intensive applications over a limited area. While performance and throughput are significantly increased, the transmission range is notably reduced to about 50 to 100 feet at best.

802.11g

This specification transmits at 54 Mbps over 2.4 GHz. This specification is the next-generation wireless network platform for the enterprise, working twice as fast as 802.11b. Ratified in mid-2003, it has gained more and more traction in enterprises. Many network access points and interface cards support 802.11b and 802.11g, as well as 802.11a. Enterprises today choose to deploy 802.11g rather than 802.11b because of higher throughput.

802.11n

This specification is still in the works. It proposes using MIMO (Multiple Input Multiple Output) technology to accelerate the throughput to 100 Mbps and above, and is being touted as the successor to today's 802.11b/g/a networks. However, the IEEE working group has not yet come to an agreement on certain important aspects of the protocol such as frequency and channel bands.

802.11i

While this is an overlay specification, it is worth mentioning here. 802.11i has enhanced security and uses Extensible Authentication Protocol (EAP) to provide authentication services. It also supports the Advanced Encryption Standard (AES) that provides enhanced encryption facilities. It was released in mid-2004, but has yet to dominate the enterprise because of it requires hardware upgrades, and is complex to deploy. It is expected, however, that most enterprises will eventually adopt 802.11i as the standard security protocol for their 802.11 networks.

Other IEEE WLAN Specifications

The IEEE is working on other specifications, each with a specific goal, that are likely to be released in the near future. Some of them are:

- 802.11c — to improve interoperability between devices
- 802.11d — to improve roaming
- 802.11e — for improved quality of service
- 802.11f — to regulate inter-access point hand offs

As more wireless specifications are released and as the technology designs improve, it is quite possible that the enterprise will use multiple specifications..

The recommended deployment of Wi-Fi protocols for the enterprise today is a combination of 802.11g and 802.11a, although most organizations prefer to standardize on 802.11g because of its lower cost and backward compatibility with 802.11b.

Wireless MANs (WiMAX)

The IEEE has also finalized the draft of a specification for wireless metropolitan area networks (MANs) called 802.16, or WiMAX. This supports point-to-multipoint (PMP) architecture in the 10-66 GHz range, with an estimated throughput of up to 120 Mbps. Due to the particular frequency range used, line-of-sight is required for transmissions. Roofs of buildings might provide the best

mounting locations between WiMAX base stations and customer premise equipment (CPE).The base station connects to a wired backbone and can transmit wirelessly up to 30 miles to possibly hundreds of CPEs. Several hardware vendors are working on developing products that support WiMAX, but until a proper business model is established, this continues to be in a trial and a proof-of-concept stage.

Another protocol called 802.20 provides WiMAX capability to moving end-points so that wireless users in trains, buses, and other moving vehicles will have access to the metropolitan wireless network.

Wireless WANs

While the architectures discussed so far are specific to WLAN environments, employees outside the coverage area need to connect through wireless carriers that provide support for a wireless WAN (WWAN) environment. The latest generation of this technology is called 3G, and although many carriers claim to offer such services, most achieve only 2.5G ratings. And there is also talk of 4G networks that utilize advanced protocols for better quality of service. There are several WWAN protocols used around the world. Two of the most widely used are described below:

- **Code Division Multiple Access (CDMA) –** CDMA enables a large number of users to access wireless channels on demand. Used by many digital mobile phone companies, CDMA delivers performance that is almost eight to 10 times better than traditional analog cell phone systems. Wideband CDMA and CDMA 2000 are flavors of CDMA that claim to provide 3G services.
- **Global System for Mobile (GSM) –** This wireless platform provides full voice and data support, with worldwide roaming capabilities. Included in the GSM family is the General Packet Radio Service (GPRS) platform for delivering Internet content on mobile devices, and the forthcoming Enhanced Data Rates for GSM Evolution (EDGE) and third-generation GSM (3GSM) for delivering mobile multimedia. GPRS is the generally accepted WWAN standard in Europe and several Asian countries.

In addition, many carriers are investigating – and in some cases in Europe, implementing – the initial stages of the upgrade to Universal Mobile Telecommunications System (UMTS) to provide high-quality data and multimedia services.

Most wireless carriers base their offerings on the above-mentioned platforms, leveraging the strengths of the protocol they decide to use. For example, services offered by Sprint PCS and Verizon Wireless are based on CDMA, while Cingular Wireless and T-Mobile use GSM/GPRS.

Facilitators of a Wireless Environment

Facilitating a wireless environment requires several partners to participate, namely:

- Mobile device manufacturers
- Independent hardware vendors
- Wireless operators, or carriers
- Service providers
- Independent software vendors

Systems integrators with focused practices in mobile enterprise implementation connect all these participants to create a viable solution.

Wireless Hardware

Numerous devices are wireless-enabled to facilitate an efficient mobile work force. Some of the top companies that provide these devices include:

- **Nokia –** Nokia is a leading mobile phone manufacturer, with innovative products that combine mobile phones, PDAs and other features. It is currently working on next-generation business terminals that will support multiple wireless technologies.
- **Palm –** Palm uses Palm OS on its popular PDAs.
- **HP –** HP's iPAQ handheld computers are used in many enterprise settings because of their versatility and high performance. They use Microsoft's PocketPC platform as the operating system.
- **RIM –** Research In Motion makes the popular Blackberry wireless devices, which allow mobile users to send and receive email.
- **Kyocera –** This company specializes in mobile phones with PDA capabilities, using Palm OS.
- **Symbol Technologies –** Symbol is a leading manufacturer of wireless devices and scanners for retail, using the latest technology in bar-code scanning.

Wireless devices add value to the enterprise only when they connect to the IT infrastructure and are actively supported by IT administration. Access points, network cards and other components essential to deploying a WLAN infrastructure are available from several vendors, including 3Com, Cisco, D-Link, Fujitsu, HP, IBM and Siemens.

If you want to deploy a WWAN environment, you will need to choose the appropriate carrier to facilitate high-quality communications.

Wireless Operators

Wireless operators provide the hardware and communications infrastructure to make wireless transmission possible in a WWAN environment. Most provide basic wireless phone services, and many now offer services to transmit data in various forms. The top three wireless carriers worldwide

are Vodafone, China Mobile and NTT DoCoMo Inc. The top wireless carriers in the United States include Cingular Wireless, Sprint PCS, and Verizon Wireless.

Choose a partner that can provide the required regional or national coverage necessary for your enterprise. Many carriers also provide WLAN services, especially in public areas popularly known as hotspots.

Wireless Software

The wireless software industry is still maturing. Most vendors are niche solution providers, and few provide substantial and quantifiable value to enterprise deployments. However, wireless software vendors are engaged in several innovative research-and-development initiatives. Solutions range from low-footprint applications such as microbrowsers and PDA utilities to more sophisticated solutions such as inter-device communications and global positioning systems. Companies such as Microsoft, Sun and Palm are active in this area.

The two most popular handheld operating systems are Microsoft Mobile and Palm OS. Other operating platforms such as Symbian and even those based on variants of Java and Linux are gaining momentum.

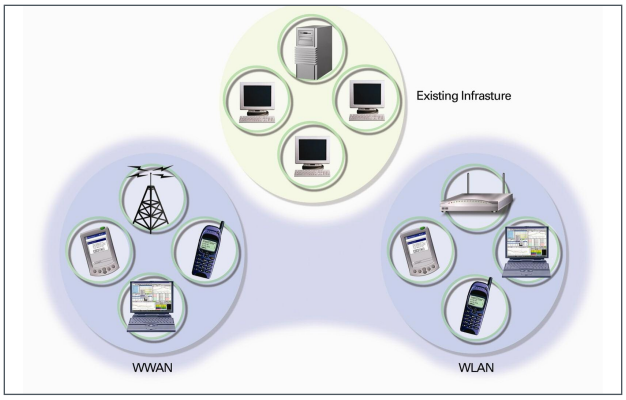

Figure 3: Enterprises are Extending to Wireless Environments

Wireless Users

The most important drivers of wireless technologies are the users. Employees typically choose one technology over another depending on their job functions and objectives. Users can be generally categorized as follows:

- **Desk warrior** This is someone who doesn't need to travel and primarily works from a fixed location. The user has a desktop or laptop and could have a PDA or mobile device (not necessarily wireless) connected to it.
- **Campus warrior** This is someone who is quite mobile, but only on the work premises. Examples include IT administrators, facilities staff, service technicians and specific line-of-business workers such as factory floor workers. Visitors and employees from other branch offices also fall into this category. These users normally use a laptop or wireless handheld device, primarily in a WLAN environment. Many enterprises now provision laptops with built-in support for WLANs so that employees can move among office rooms without network connectivity restrictions.
- **Road warrior** This is someone who is rarely in the office and does most of his or her daily tasks while on the move. The user might use a laptop or handheld device that has multiple network support (WLAN and WWAN).

Wireless benefits both knowledge workers and transactional workers, depending on their mobility needs. No matter who the user of wireless technology is, it is important that the enterprise address all security and management concerns.

When deploying a mobile enterprise strategy, you have to consider the right combination of wireless network architecture, platforms, infrastructure components, devices and applications to be successful. Figure 3 shows how enterprises are extending their existing infrastructure into a wireless environment.

Even in the absence of ubiquitous standards, the current wireless infrastructure is stable enough to support and deploy wireless applications developed for the mobile work force. As wireless technologies mature, the quality and availability of wireless software will grow. However, without an effective mechanism for managing and securing the wireless environment while providing trusted wireless access to enterprise assets, enterprises risk missing optimum return on investment (ROI) for this technology.

Concerns With Deploying Wireless

While it is one thing for organizations to keep up with the latest technologies, making them useful for everyday enterprise activities is a different story. Following are some key concerns of enterprises that are contemplating a mobile strategy:

- **Security** Wireless networks are easy to break into and difficult to monitor. Your enterprise assets must be protected.
- **Management** Effective management of the components that make up a mobile enterprise, from servers to mobile devices, is critical.
- **ROI** Wireless connections should perform as good as, if not better than, wired connections. They should add value to the enterprise and generate revenue. The benefits should be measurable in some way. ROI and business continuity from wireless deployments are important.

Security

The number one concern of wireless enterprises is security. Wireless networks are some of the easiest to hack into. Many security measures may not be adequate to prevent this intrusion, and few were designed with wireless in mind. There are several vulnerabilities in the WEP security features provided in the 802.11 standard. The goal of WEP is to provide data confidentiality in wireless networks at the same level as in one that is wired. However, despite having well-known encryption mechanisms, namely the RC4 cipher, WEP is vulnerable to attacks, both passive and active. This opens up the wireless network to malicious parties to eavesdrop and tamper with wireless transmissions. Static keys and weak authentication are serious problems with the WEP security feature for 802.11 networks.

Enterprises can use advanced encryption methods such as Advanced Encryption Standard (AES) or even Wi-Fi Protected Access (WPA), which has dynamic keys to correct this serious flaw in WEP. Many enterprises also use 802.1x, a specification in the wired network to authenticate users who are connecting from remote locations, for wireless user authentication. 802.11i is the IEEE ratified specification that combines the elements of AES encryption and 802.1x-based authentication. However, these measures do have overhead associated with them and may adversely affect transmission throughput. Moreover, managing the deployment of these security schemes is extremely cumbersome, and they do not typically scale.

Many enterprises are building their WLAN separate from the intranet and set up a firewall to protect wireless communications. Implementing a robust virtual private network (VPN) solution is also useful, and is considered by many to be the temporary quick fix for wireless security. The security features available with a VPN solution, along with additional authentication and access control features, secure users whether they are on a wired or wireless network. But VPNs have their own limitations, especially in terms of cost, performance, and maintaining connections when the user is roaming between access points.

Enterprises must also ensure that all devices are virus-free and do not act as carriers of malicious code. Access to the network from mobile devices must be authenticated, and only authorized users should be allowed access. Location-based access is an important consideration. Wireless coverage tends to go beyond the physical bounds of the enterprise campus. In order to enforce proper security, it is important that legitimate wireless uses get access to the network only if they are within a predefined perimeter.

Management

Wireless systems do not operate in a vacuum; they integrate with the IT infrastructure. Therefore, management of the wireless infrastructure must take place in the context of the overall enterprise infrastructure. Software point solutions for wireless networks are unable to effectively integrate wireless management information while monitoring the rest of the enterprise to promptly identify and resolve problems. Wireless management solutions must be integrated, comprehensive and reliable.

Wireless networks must be supported and managed no differently from the infrastructures supporting wired networks. In wireless networks, however, components that must be managed also include access points, mobile devices and wireless application servers.

Management of the network optimizes performance and allows the administration team to respond to issues quickly. If not configured properly, the access points will not function as desired. It is important to set up the appropriate channels on the access points to avoid any interference in the transmissions. Also, the load on each access point must be balanced to provide good throughput for all wireless users connected to the enterprise network. This is particularly important when dense traffic within a given area of the network needs to be optimized.

Besides providing a real-time view of the wireless network, the management solution must also provide a future view so that proactive measures can be taken to prevent problems before they occur.

Further, corporate assets need to be accounted for. Therefore, each mobile device should come under the eye of enterprise management. Automatic transfer of relevant information, applications and updates (such as the latest antivirus signatures) should be made possible. In addition, data on the mobile devices must be backed up without causing any impediment to normal processing and must be automatically moved to the server unobtrusively when back on a wired network.

Quality of service is another important issue. Wireless operators and application providers promise high performance, but it is critical to track and monitor service levels to ensure optimal work environments for your mobile employees.

Return on Investment

As the work force increasingly demands wireless support, enterprises need to act quickly and provide the necessary services to promote success. It is important for companies to make the right decisions to enable application longevity while remaining open to improved solutions. Defining a clear business objective and thoroughly researching the feasibility of wireless technology is crucial in achieving maximum ROI.

Other issues such as network and application performance, extensive coverage, hand-over (between WLANs and WWANs) and roaming are also important and must be part of the evaluation process when determining ROI.

Budgets are getting tighter, and though hardware prices are falling, the operational costs can be pretty high. In some cases they far exceed the purchase and set-up costs by 50% to 75%. It is very critical to build and maintain a secure and manageable environment to keep the operational costs and the total cost of ownership as low as possible.

Keys to a Successful Wireless Enterprise

Wireless technology is here to stay. It is important to learn more about the various aspects of wireless and how they might assist you in achieving your business objectives. This may involve substantial experimentation, trials and pilot projects. For enterprises that are contemplating a mobile strategy, the following best practices are worth considering:

1. **Develop your mobile strategy around a clearly defined business objective and keep an enterprise-wide focus.** All your wireless communications and other mobile activities are an integral part of your business, and therefore must not be treated as a separate island of technology. Remember that technology, including wireless, must solve a specific business objective. Choose an enterprise-wide solution that provides all the required measures for security, management and information access.
2. **Ensure that your wired enterprise infrastructure is in order first.** It is easier to integrate a wireless network into a well-managed wired environment on an enterprise-wide scale. One can only imagine the disastrous results of introducing a highly vulnerable wireless network into a wired environment that is improperly secured and managed.
3. **Choose the right partners. Establish partnerships with the vendors that can help you with your specific needs.** Work with systems integrators that have a focused wireless practice. It is extremely important to choose the right software vendor to deliver an integrated, comprehensive and reliable enterprise-wide solution for your organization.
4. **Anticipate change and be prepared to leverage new technologies.** The wireless industry is changing rapidly. Mobile devices are getting smaller, faster and more capable. Performance of wireless networks is steadily improving. Opportunities to leverage mobile technologies will continue to grow. Work with companies that will change with the times and yet be stable in what they do best.

To implement an enterprise-wide mobile strategy, it is imperative to work with a trusted business advisor that understands the enterprise environment as well as the technologies that enable success.

CA's Mobile and Wireless Enterprise Solutions: Delivering the Value of EITM

Enterprise IT Management (EITM) is CA's vision for how enterprises will be managed and secured, enabling companies to unlock value and realize the full potential of IT.

The vision of EITM is to unify and simplify the management of enterprise-wide IT. EITM enables companies to tie the IT infrastructure to business processes, including transactions and interactions, so as to understand the interdependencies between users, process, policy and technology and then orchestrate the IT processes in context to create a secure business service. EITM provides a contextual understanding of how IT operations continually relate to and affect the business process, while managing across the entire IT infrastructure to take action in support of business processes.

Adopting the EITM vision enables enterprises to manage risks, reduce costs, improve service, and better manage their investments.

Constantly innovating and evolving to address customer requirements, CA is a market leader in enterprise solutions worldwide. CA delivers value-added solutions for mobile enterprises, with the following key initiatives:

- **Innovative development –** With a broad array of skills and talented minds, CA's Research and Development team has developed innovative solutions for the wireless enterprise. Spanning all solution areas, CA is committed to ongoing research and development of solutions that add value to your enterprise and foster success.
- **Strategic partnerships –** CA is engaged in several strategic partnerships with successful companies, including:
  - Device and systems manufacturers such as Intel, Nokia, Microsoft, D-Link, Palm and Symbian
  - Wireless operators such as Cingular Wireless
  - Educational and research institutions such as Stony Brook University and UCLA
  - Systems integrators such as EDS and Fujitsu Services

These alliances enable CA to provide enterprises with complete and effective solutions. CA is also actively involved in several wireless research projects and standards committees, including:

- Stony Brook University's Center of Excellence for Wireless and Internet Technology, of which CA is a founding member and primary sponsor
- UCLA's Wireless Internet for Mobile Enterprises Consortium (WINMEC), of which CA is a founding member
- Open Mobile Alliance (OMA), of which CA is a full member and represented in the Device Management working group

As you extend the existing enterprise infrastructure to the wireless environment, you must secure and manage it. You must also deliver the appropriate information and services to mobile employees. CA's mobile enterprise solutions enable you to:

- **Protect, provision and monitor** mobile assets and information
- **Optimize reliability, availability and performance** by managing the wireless network, devices and services

The following sections highlight CA's solutions that facilitate secure and manageable wireless computing, based on the vision to deliver the benefits of EITM.

Wireless LAN Management and Security

CA Wireless Site Management enables you to manage and secure Wi-Fi network implementations. This includes the management and enforcement of security policies set up for wireless users. One of the greatest security concerns is the management of encryption keys provided by security schemes such as WEP and WPA. The primary reason for not deploying wireless encryption is the difficulty in managing the implementation. CA Wireless Site Management enables you to automatically rotate and synchronize the encryption keys between the access points and devices to ensure secure connections. A number of security schemes can be selected, as well as various authentication methods supported by 802.11i, depending on the desired level of security.

Location-based and time-based access is an important element. You can set up a virtual access perimeter to enable wireless access only if the user is within the access zone, as shown in Figure 4. If the user steps out of the access zone, the connection is dropped.

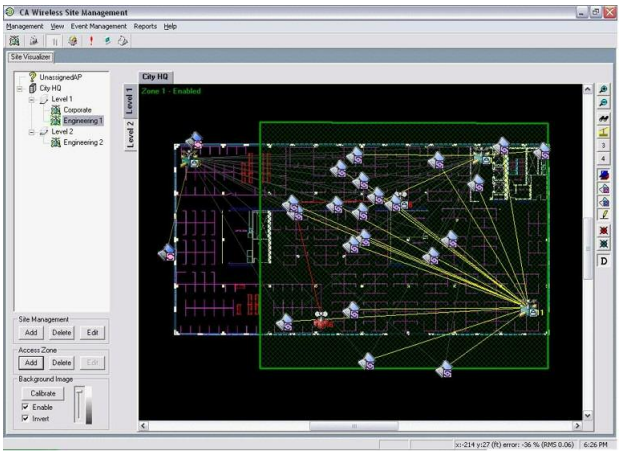

Figure 4: CA Wireless Site Management enables you to administer Wi-Fi security and monitor your wireless infrastructure.

Rogue access points are detected, and their location is indicated. The client software on legitimate wireless devices connected to the wireless network assists in the detection of rogue devices, and the appropriate alerts are generated. Events and alerts can be propagated to the Unicenter console, and several built-in security and management reports can be generated.

The performance and configuration settings are constantly monitored. Access-point channels are automatically allocated in an optimal way to minimize signal interference. The connection load between access points is also balanced to provide optimal throughput in dense network deployment.

From a central management perspective, you can monitor the condition of mobile devices from the Unicenter console and perform various event-driven procedures to ensure efficient performance. Based on the principles of EITM, you can run CA WSM as a stand-alone product, or integrate it with existing CA? Enterprise Systems Management and Security solutions.

Mobile Device Management and Security

With the steady proliferation of mobile devices in the enterprise, central management is imperative, especially for administering security features, loss control and other contingencies such as device shut-off and device BIOS flash.

Software assets on mobile devices need to be managed. Mobile employees must have access to all the latest corporate software and necessary updates, just as wired employees do. Unicenter Software Delivery ensures that the wireless devices are updated with all the necessary information every time mobile users synchronize their handhelds. Unicenter Asset Management ensures that only authorized software is installed on the mobile device, thereby protecting the user and the network from unsafe

applications. Software and hardware inventories are maintained and can be deployed to new devices at any time. In the event a device is lost or stolen, the data on the device can be remotely erased and the device locked. The data can then be rewritten if the device is recovered or a new one provisioned.

*e*Trust Antivirus protects your mobile device from malicious code, regularly updating the virus signatures.

VPN technology is widely accepted as a viable solution to augment the rudimentary security available with wireless networks. CA supports and recommends the use of VPNs to encrypt data transmissions and provide secure communications tunnels between remote wireless users and the enterprise network.

Smartphone Management and Security

Smartphones are the convergence of PDAs and cell phones and as a result have the management and security challenges of both wireless technology and cellular telephony. Enterprises will need to manage Smartphones of different platforms across a number of different cellular operators. Accordingly, all industry stakeholders are defining management standards for the wide variety of devices being introduced to the market.

The CA Smartphone Solution provides large organizations and cell phone operators with enterprise level device management tools for the most popular Smartphone platforms, such as Microsoft Mobile, Symbian and RIM. It provides over-the-air (OTA) management and security utilizing Open Mobile Alliance (OMA) Device Management (DM) standards components. The solution provides device-independent consolidated asset inventory, configuration management, policy compliance, and security management. Following CA EITM guidelines, it has a modular architecture, and operates as a comprehensive standalone management solution or synergistically integrates into CA's Enterprise Systems Management and Security suites.

Security Information Management

Using CA's advanced portal technology, the *e*Trust Security Command Center enables security administrators to have a uniform view of their enterprise-wide security systems – including those managed by CA Wireless Site Management and other related solutions.

Data Preservation

BrightStor ARCServe Backup for Laptops & Desktops takes incremental backups of your laptop data in a non-disruptive manner, without your having to connect to a backup server. Automatic synchronization is carried out with the backup server when you connect to the enterprise through a wired or wireless network. Since the backup transmissions are encrypted and compressed, it is extremely useful in a wireless environment.

Wireless Support and Quality of Service

The call center is an important aspect of an enterprise that delivers IT services to its employees and customers. Unicenter Service Desk is wireless-enabled so that mobile employees can use their handheld devices to look up information on their help desk tickets. For example, they can see how many issues are open, how many are pending, which ones are critical, and more. Unicenter Service Level Management enables you to track and manage service levels for your mobile environment so that you can take the necessary measures when service-level agreements (SLAs) are not met.

RFID Management and Security

There is a rapidly increasing deployment of RFID (Radio Frequency Identification) technology in several industry verticals, starting with the manufacturing and retail industries. As the scale and complexity of these deployments increase, the need to manage and secure the information and infrastructure becomes paramount. CA is teaming up with customers and partners to deliver a comprehensive solution to manage the deployment, security, and life-cycle of RFID environments.

As the market continues to be infiltrated with mobile devices of different kinds on various platforms, managing mobile devices is becoming a critical factor for organizations seeking to reap the benefits of wireless enablement. CA is committed to supporting your enterprise. In addition to our current offerings, extensive research is ongoing to build more solutions that allow you to effectively manage mobile devices in the context of your entire enterprise infrastructure.

Preparing for a Successful Wireless Enterprise

A global paradigm shift toward a mobile enterprise is well underway, and CA is poised to be a leading solutions provider for this market. Armed with strategic partnerships and innovative products that enhance the value chain, CA's mobile management solutions allow you to manage risk, improve service, manage costs and align IT investments with your business needs. Specifically, you benefit with:

- A secure wireless infrastructure that promotes safe communications and efficient mobile management
- The ability to efficiently manage your complete enterprise – including servers, access points, devices and other components of your wired and wireless environment – in an integrated manner
- Easy information access so that mobile users are equipped

with timely intelligence to make profitable business decisions without any restrictions
- A wireless infrastructure that you can leverage to provide quality service and reap significant ROI as you continue to grow your enterprise
- The ability to strategically manage your wireless technologies for greater competitive advantage and greater business results

As the wireless industry continues to evolve and mature, CA will continue to innovate, develop and deliver end-to-end, comprehensive and integrated solutions that foster customer success.

For more information, please visit ca.com.

Cited References and Notes

1 Wi-Fi Alliance, **wi-fi.org**

2 IEEE, **ieee.org**

3 Open Mobile Alliance, **openmobilealliance.org**

4 Extensible Authentication Protocol by the Internet Engineering Task Force. RFC is available at **ietf.org/rfc/rfc2284.txt**

5 N. Borisov, I. Goldberg, and D. Wagner. "Intercepting Mobile Communications: The Insecurity of 802.11" **isaac.cs.berkeley.edu/isaac/wep-faq.html**

6 Wagner, Jim. "A New AES Standard for Wireless" **wi-fiplanet.com/news/article.php/1449651**

7 Vaughn-Nicholls, Steven. "Protecting Your 802.11 Network With WPA" **wi-fiplanet.com/spring03/article.php/2210441**

8 Deshpande, Sumit. "Who's Watching Your Wireless Network?" © 2003 Computer Associates International, Inc.

About the Author

Mr. Deshpande is vice president of the Wireless Solutions group in the Office of the CTO. He is involved in defining and communicating CA's global strategy for wireless technology, as well as the development of new solutions. Sumit has a broad range of technical expertise and experience in varying aspects of information technology, including networking, application development, technology consulting, market analysis, and others. His articles and interviews on wireless and other topics have been published in several technical publications. Sumit is a much sought after speaker at several trade shows and advises clients, analysts, and other relevant parties on CA's strategy and solutions for the 21st century. He holds a bachelor's degree in Computer Science from Pune University, and master's degree in Computer Science and Information Systems from Marist.

MP294660106