**Wireless technology has come
a long way, but is it robust
enough for today's enterprise?**

We have been working in the wireless space in one form or another in excess of 10 years and have participated in every phase of its maturation process. We saw wireless progress from a toy technology before the dot-com boom, to something truly promising during the boom, only to be left wanting after the bubble when the technology was found to be *not* ready for prime time. Fortunately, it appears that we have finally reached the point where the technology and the enterprise's expectations have finally converged. Even with the current level of maturity in this space, creating and managing a cohesive wireless strategy within an enterprise is difficult. There are technological hurdles, cost/efficiency trade-offs to be considered, and obtaining buy-in/acceptance at all levels of the company. To identify and overcome these issues, we have developed a model called enterprise-grade wireless. This article is a discussion of the model itself, the context in which it exists, and a justification of its criticality to the enterprise.

WIRELESS IN THE ENTERPRISE DEFINED

It is important that we first define the context of this article. We have a specific view of what constitutes wireless in the enterprise; note that we are not espousing that this is the only view, just defining the perimeter of the space to improve the applicability of the various points we make in the discussion that follows.

Our general definition of enterprise wireless is quite broad: to extend enterprise applications to wireless devices used by employees and clients. More specifically, we see this as extending suitable applications to handheld devices over wide-area wireless networks. What this actually means is taking applications that lend themselves to a disconnected or partially connected model and extending them to PDA-type devices that access the network using WAN technology.

Clearly, this is a narrow view of modern-day wireless. We purposely exclude network technologies such as Wi-Fi and end-user devices

Enterprise-Grade WIRELESS

BRUCE ZENEL AND ANDREW TOY, MORGAN STANLEY

Enterprise-Grade WIRELESS

such as laptops with PCMCIA wireless cards. We do this for two reasons: to limit the context of the discussion to make our arguments more pertinent; and purely to limit the length of discussion.

THE DIFFICULTY OF PROVIDING WIRELESS TO THE ENTERPRISE

Generally speaking, nearly all of the issues outlined in this section—devices, networking, software, consumer-versus-enterprise devices, and support—have a historical component. Much of this is a result of the evolution of the technology from something with promise to modern technologies that when used together can create solutions that actually have merit and are beneficial. Enterprise wireless has finally come of age, but clearly that has not always been the case.

Devices. The improvements in device capabilities over time appear to be following Moore's law with no deceleration in sight. PDAs in the late 1990s were for the most part completely disconnected and used a cradle-based synchronization model to share data. By 2001 the first truly wireless PDAs were available, although capabilities were limited, especially with respect to network data rates. The devices have continued their evolution in a number of ways. Generally speaking, there is still no "killer" PDA—one that does all things for all people. Instead, the market is segmented into categories by application or feature, the most significant of which is consumer versus enterprise, which will be addressed below.

Networking. Similar to devices, WAN capabilities have improved dramatically over the past 10 years. In the mid- to late 1990s most wide area networking was accomplished by tunneling packet data over circuit-type connections (e.g., PPP over CMDA). In cellular technology parlance, this was 1G, providing bandwidth on the order of 8 Kbps. As wireless technology evolved to 2G and 2.5G, services such as GPRS (based on GSM technology) and 1xRTT (CDMA) became available, providing data rates of 30 Kbps and 60 Kbps, respectively. This jump in bandwidth suddenly allowed interactive applications such as browsing and instant messaging to be supported.

With round-trip latencies of approximately 1 second, they were at the far edge of usability, but possible. In the past few years we have seen the advent of 3G or near 3G wireless telephony. These technologies can provide data rates of 500 Kbps or more. The result is that applications are no longer limited by the network, shifting the limited resource equation toward CPU speed and battery life.

Software. Historically, IT organizations were made up of numerous different back-end systems. Very often the e-mail plant was separate from the calendar system, which was separate from the system that handled contact data, etc. This heterogeneity hindered the development of any type of unified wireless infrastructure since it would be required to interface with each type of back-end system. Eventually, this issue was resolved through the development of advanced middleware and the rise of monolithic systems. Various middleware companies appeared as early as 2001 providing software that was able to interface with numerous target applications, as long as those applications were standard in some way (e.g., the e-mail plant was based on IMAP, the contact system adhered to LDAP standards, etc.). These middleware systems took a protocol compatibility approach to the problem and were somewhat successful (only a few players remain in the field).

It was the rise of monolithic systems that really turned the tide with respect to the software conundrum. Large enterprises began to see the benefit of combining a number of their back-end systems into one larger system with relatively well-defined interfaces. This in turn led to simpler middleware design since a component would ideally need to interface with only a single target application. While the integration point is limited to one monolithic system, that system may provide many services, such as e-mail, calendar, contacts, etc.

Consumer versus enterprise devices. The market for PDAs is overwhelmingly directed toward the consumer. This is perfectly fine from a vendor business model point of view but creates particular problems when trying to fit a consumer-oriented device into an enterprise. Consumer-oriented devices have a tendency to be rich with

features such as cameras, memory expansion through the use of compact flash or secure digital cards, voice recording, and every possible network capability that can be fit into the form factor (with a focus on local area networking such as infrared, Bluetooth, and Wi-Fi). This is inversely proportional to the goal of security since the device is meant to be as open as possible by design. The converse of the above is that a device designed specifically for the enterprise will be readily integrated and gain acceptance quickly. These devices are for the most part single-purpose or at most directed toward extending specific enterprise applications.

The support nightmare. Until now, for the most part, this discussion has focused on issues of specific technology or lack thereof. One critical area that is often ignored has little to do with technology, and that is support. There are a number of support models used by an enterprise; support may be concentrated in one department, distributed such that each user group has a dedicated support organization, or it may be outsourced altogether to a different company. Regardless, the support methodology is orthogonal to an enterprise wireless solution.

In the overall wireless architecture, the network is by far the most opaque component. Server-side components can be examined in-house, devices can be manipulated by users, but issues within the network may be completely obscured from a user or support person. Given this, and a good understanding of the SLA expected by the user base, it may be vital to have visibility into the network. One way to do this is to design the wireless system to use specific technologies such as leased lines between the enterprise and wireless carrier. This would provide a level of visibility into the carrier network and is likely to provide an escalation path to resolve support issues. It is worthwhile to note that only enterprises of a certain size will be able to implement such a strategy. For small businesses the only solution is to rely on the Internet (which may suffice for many services).

Moving out to the device, the situation may be even less desirable. Organizations may choose to support numerous device types, making support difficult. Moreover, device-side applications may not have been designed with end-user support in mind. The latter can be improved by requiring that developers include debug and diagnostic information through the use of hidden or otherwise inconspicuous interfaces that can be enabled by support representatives during a remote support call. Unfortunately, there is no good solution to the device explosion other than thorough documentation and end-user education.

AN ENTERPRISE APPROACH

This space is complex, but the pieces required to put together an enterprise-grade wireless solution exist. Given the wireless products and technologies that are available on the market today, no single solution can provide the level of functionality required by a sophisticated enterprise. This is exacerbated by the fact that many vendors engaged in the wireless space, including network operators, handheld developers, and software companies, are heavily focused on wireless as a consumer, or at best a prosumer, offering. Enterprise-grade wireless is an approach to allow the enterprise to differentiate its requirements for wireless from those of the consumer market. By applying a different standard to existing wireless technology, enterprise-grade wireless aims to enable existing offerings to work synergistically for the company.

The first step in defining enterprise-grade wireless is to determine the areas of particular importance in differentiating the enterprise from the traditional consumer market. In general the fundamental individual user requirement for wireless is not much different whether the device is a PDA or an enterprise handheld: users want access to the information that is important to them. In the case of the enterprise users, however, the information they are accessing may be proprietary business data. It is therefore important for an enterprise to deliver the ability to its internal developers to quickly and reliably translate business applications to the wireless environment. It must also be able to protect this business information as it makes its way from the firm's systems, across public wireless networks, to the user's device (and vice versa). Finally, unlike with individual consumers, the enterprise must ensure that the wireless experience is delivered in an efficient manner that scales across thousands of users simultaneously.

Specifically, the enterprise needs to ensure that minimum standards are kept in the areas of security, uniformity, and manageability. Security allows the enterprise to provide its information and networks across wireless systems; uniformity provides the ability to leverage wireless to quickly deliver business functionality; and manageability provides the ability to scale the solution horizontally.

Security. A wireless handheld is simultaneously a repository of confidential corporate information, a proxy representative of a corporate user, and a potential launchpad for attacks against the corporate network. Given these attack vectors, security is the paramount concern in evaluating any solution. Enterprises must therefore ensure they have the expertise to internally evaluate the consequences of introducing any given wireless offering

Enterprise-Grade WIRELESS

on two fronts: technological security and information security. Each of these can be provided in a different manner; the goal, however, is to have a benchmark of security standards against which all offerings can be measured.

In assessing technological security, the assumption is that the device will contain corporate data and access corporate services. This means that the data on the device must be inherently secure from both the data repository and interface points of view. Ideally the data should be encrypted on the device, although if there is no capability for expansion through the use of compact flash or secure digital cards, this will suffice. The user interface on the device must provide a hardened screen lock. This will either meet the enterprise's requirements for data access or use a weaker level of protection in conjunction with an automated device destruction capability resulting from a relatively small number of failed access attempts. On the network interface side, the fewer the better.

If multiple interfaces are present, the capability must exist to render these devices unusable either by disabling the hardware or through the use of firewall software on the device. The transport using the network interface must also be secure since it is through this conduit that the enterprise is reached. There are many well-known methods for secure transport (e.g., SSL, VPN); any that fit the model of use can be employed.

Whereas technological security focuses on protecting the data on a handheld device and network, information security attempts to regulate what is appropriate to have on a handheld in the first place. As small-form-factor wireless handhelds are inherently more vulnerable to theft/misplacement than laptops or desktops, a valid approach to reducing their risk is to restrict the amount of functionality available on the platform. For example, a screen-lock-protected destroyable handheld may be sufficient for e-mail/contacts/calendar but may be too insecure to provide full trading functionality. Obviously an appropriate balance must be struck.

An area that is often not considered in the context of security is the usage model. An enterprise may develop and deploy an extremely secure PDA solution, but if it is

too difficult to use, then adoption will suffer. An example of this is the use of VPN connectivity in conjunction with two-factor authentication to provide a secure transport between the device and enterprise. The disconnected nature of wireless technology means that the VPN will have to be re-established every time the connection is broken, which for urban dwellers may be quite frequent (think elevators and subways). The fact that the user will have to provide a token (or other nontrivial information) for every connection will quickly render this solution impractical. The bottom line is that although security is critical, the enterprise must choose a solution that its users will be inclined to tolerate.

Uniformity. As various products, handhelds, and middleware systems are evaluated for introduction to the enterprise environment, there must be a conscious attempt to evaluate them all against a consistent standard. This standard may vary from company to company and may include factors such as whether push or sync technologies are favored, which input mechanisms are appropriate on handhelds, and which radio networks are considered best. Once these standards have been determined, the various products available can be examined and a minimum set of these chosen to fulfill the enterprise's need.

In addition to providing a standard set of requirements for evaluating offerings, uniformity must be maintained in the wireless development environment to allow business application functionality to be rapidly developed and deployed. While heterogeneity is valuable to a certain extent when selecting which handhelds and wireless technologies to deploy, a homogeneous development environment is required to be enterprise-grade. This is because there are several standard "hard" problems of wireless development that must be solved by almost all applications. Rather than forcing enterprise developers to individually and repeatedly solve these issues, it is more efficient to solve them once within a uniform development environment from which anyone can benefit.

One such uniformity requirement that merits special mention is the *partially offline* scenario. This occurs

simply because wireless coverage itself is nonuniform—network coverage can vary from full-strength to zero-strength in the space of a few meters. Users constantly travel through different levels of coverage as they move in and out of elevators, the subway, and other dead spots. An application tied directly to the network (such as one using a TCP-based technology) will unfortunately have a dependency on coverage to function. One of the most important roles of an enterprise-grade wireless platform is to insulate such applications as seamlessly as possible from network interruption by emulating an always-available guaranteed-delivery network when the reality is far different.

Manageability. As more wireless handhelds are introduced into the enterprise environment, manageability becomes an increasing concern. Many enterprises have ad-hoc approaches to managing their wireless devices, a carryover from the days when PDA handhelds were considered personal devices. Users may be expected to purchase, provision, and manage their device information on their own, or perhaps through simple policy adherence. For example, a user may purchase a popular handheld, install the included synchronization software, and begin syncing PIM (personal information manager) data to the device. This approach, however, simply does not provide the level of compliance guarantee that any company should demand of its infrastructure. Indeed, in this scenario, the company may have no idea that the handheld has been introduced to the network, let alone that it now contains confidential corporate information. To counteract this, the enterprise must endeavor to ensure that only managed devices are interacting with the corporate environment.

IMPLEMENTING ENTERPRISE-GRADE WIRELESS

An enterprise-grade approach to wireless must provide three essential services to clients of the system: products that allow quick development and deployment of enterprise-grade solutions; infrastructure that seamlessly provides uniform and secure wireless experiences; and expertise to provide design and auditing services to developers.

Products. Enterprise-grade products are software systems that allow users to access business application functionality from their wireless handheld devices. These may range from simple e-mail and PIM access to complicated custom applications that perform specific business tasks. A property of enterprise-grade products that separates them from consumer applications is their ability to solve general classes of business problems rather

than being focused on single “one-off” solutions. That is, rather than being designed to solve specific problems for specific users, it is best to provide applications that have appropriate interfaces that allow them to solve similar problems for different clients within the enterprise. More importantly, enterprise-grade wireless products should be implemented such that all wireless-specific aspects of the general problem are solved behind an abstraction wall. The role of the wireless abstraction is to provide developers with a single unified view of the inconsistent wireless environment. Thus, developers will not require any knowledge of the wireless space to solve their problems—only knowledge of the selected enterprise abstraction layer.

An example of this approach is the delivery of news and alert content to wireless devices. While many divisions and groups within the enterprise may have their own proprietary databases of information and alert feeds,

One of the most important roles of an enterprise-grade wireless platform is to **insulate applications** as seamlessly as possible from network interruption.

they all share a common problem: pushing news content to mobile devices in a readable, usable format that can be consumed either online or offline. A trivial solution to this problem is to have users consume such content in a browser on their handhelds. This solution has disadvantages, however, in that a browser does not provide asynchronous content delivery, nor does it provide an easy way to consume content offline. Instead, users must request content that they are interested in and wait for that content to be delivered via the wireless link. Browser applications also require developers to know all of the different browser types that exist in the enterprise so they can optimize the rendering of their content.

An enterprise-grade approach to this problem is to develop a thick client application for wireless handhelds that is able to provide an optimized wireless experience for the consumption of news—content can be pushed to the device and saved in local storage to be read later,

Enterprise-Grade WIRELESS

either offline or online. In addition, the experience provided by the thick client can be customized to the capabilities of the local device. A server-side component of the wireless product receives formatted content (such as RSS, a de facto standard for Internet publishing) from the internal network and delivers it to whatever mobile device is appropriate. All that developers have to do to deliver content is to host their data in the agreed-upon format.

An enterprise-grade wireless system provides uniformity that allows developers to ignore various wireless idiosyncrasies and instead focus on quickly delivering their business-specific content using their domain expertise. Having all similar content routed through the same application allows for a much more manageable and supportable solution. The example given above is simple, but the same technique can be applied to deliver products in the realm of CRM, supply chain, database querying, and other such general problems.

Infrastructure. Many of the requirements of enterprise-grade wireless can be fulfilled by creating specialized infrastructure designed to transparently enhance users' wireless experiences. By leveraging economies of scale, the enterprise has access to technology that is beyond the reach of regular consumers. For example, GSM mobile operators can arrange for a dedicated data APN (access point name), which serves only devices that are registered by the carrier for the enterprise. Since an APN is designed to route all data over secure leased lines between the mobile operator and the enterprise data center, devices connected to the APN receive a superior quality of service. In addition, enterprises can achieve increased levels of control over security and reliability through the implementation of monitoring and service-level agreements. In this way, traditional network infrastructure can be leveraged to simplify the problem of managing secure connections from mobile devices.

The enterprise must provide a uniform development environment to solve its wireless application needs. Several technologies exist in the wireless space today from which a uniform development model can be engineered. Past approaches include browsers and VPNs.

Traditionally, wireless platforms have attempted merely to translate the technologies that already existed for desktop computing and apply them to the wireless world. This resulted in technologies such as WAP, which attempted to solve wireless application delivery by delivering all content through a limited browser experience. This had the benefit of requiring little wireless experience to develop a wireless application, as most companies had the expertise and infrastructure in place to create WAP pages and applications. Unfortunately, WAP was a failure, as the traditional browsing experience is simply inappropriate for handheld devices where network bandwidth, screen real estate, and input capabilities are all extremely limited. In addition, browser technologies are inherently limited to online scenarios.

VPN technologies for handhelds enable direct access to the enterprise infrastructure from wireless devices. Although this simplifies many of the inherent network problems of wireless device access, the approach is a dangerous one. Without careful management of firewalls and networks permissions, a handheld device could receive far more network access than it requires, increasing its potential as an attack platform. Also, from a developer perspective, developing applications for a handheld VPN is not a direct analog to that of a broadband VPN. Applications for handhelds must be optimized for highly latent, lossy networks, as well as architected to provide support for offline and partially offline scenarios. Merely providing a VPN network connection to developers does nothing to help them build robust applications that operate well under these scenarios.

Current approaches to uniform development environments include J2ME (Java 2 Micro Edition) and .NET CF (.NET Compact Framework). Both of these environments provide enterprises with similar functionality: the ability to develop write-once, run-anywhere-there-is-a-VM applications. Both are also stripped-down versions of their desktop counterparts, Java and .NET, and any developer who is familiar with the more mature sibling should have no issue developing with the mobile edition. J2ME and .NET CF share a common weakness, however, in that

they do not assist developers with the “hard” problems of wireless development, such as solving the offline/partially offline issue, providing secure network transport, or integrating asynchronous push technology.

The same SOAP Web service technologies that are available for data exchange and RPC (remote procedure call) on mainstream desktops are also available on wireless development platforms such as J2ME and .NET CF. They are useful for allowing mobile applications to access the same back-end functionality as their desktop counterparts in a seamless fashion. They have a fundamental weakness, however, in that they require an authenticated secure transport component to deliver the HTTP transactions back to the enterprise. While HTTPS may be massaged into this role, it is not ideal in that Web servers must be exposed through Internet-facing firewalls to allow applications to use the services. In addition, Web service technology is inherently synchronous and client-initiated, which makes it a difficult technology to use in a push-based environment. Finally, other techniques must be used to wrap the SOAP Web service to solve the partially offline scenario; otherwise, application functionality will be unavailable in areas where wireless coverage is poor or nonexistent.

Database synchronization techniques are the oldest of the PDA data-retrieval technologies and are still in use today. They come in various forms—everything from text-based e-mail to SQL database synchronization. Although the synchronization process tends to be cumbersome, SQL databases offer an important benefit in that they provide a buffer that solves the partially offline scenario. A synchronization agent is used to keep the local data store as fresh as possible by synchronizing with the back end whenever the network is available. Applications access this local database instead of resources directly over the network; thus, they are never isolated from their core data by network outages. The downside to this approach is that realtime data transfer is not possible, excluding a number of application categories such as instant messaging and browsing.

A set of technologies has recently appeared that specifically provide mobile applications with a secure, reliable transport to the enterprise. There are varying approaches to this technique, ranging from a complete replacement of the TCP stack with one that is optimized for lossy, highly latent networks to an XML message bus technology that provides guaranteed delivery to any application using the transport. The main advantages are that they specifically address the requirements for enterprise-grade wireless and that they all generally provide uniform

interfaces for developers. Unfortunately, none of these transports has given birth to a new standard, so they tend to be proprietary and require a nontrivial amount of investment in resources (infrastructure, training, etc.).

Unfortunately, there is no silver bullet for deploying the ideal wireless development—each company must determine the technology or combination of technologies on which to standardize to meet its own needs.

Expertise. While one of the goals of enterprise-grade wireless is to remove the need for individual application developers and users to maintain wireless expertise, there occasionally will be problems that are exceptions. These could be true one-off problems that require special development or special technologies that do not currently exist in the environment. To allow for these cases, the enterprise-grade wireless system must provide a process for developers to inquire and determine the appropriate wireless technologies for their problems. By maintaining domain expertise over the wireless space within the firm, the enterprise-grade wireless group can provide shepherd-ing and consulting services to all applications destined for wireless devices. This is especially important for security, as many wireless technologies (e.g., WAP) have hidden security concerns that the average developer may not know about. By ensuring that all applications proceed through a formal approval process before launch, wireless solutions can be managed to ensure that they conform to the requirements set forth by enterprise-grade wireless.

CONCLUSIONS

Wireless in the enterprise is a difficult problem requiring more than a single solution or product. Tactical deployments may provide stopgap functionality, but the opportunity cost of dedicated, exclusive solutions may outweigh their benefits in the long run. Instead, it is our belief that a disciplined and well-thought-out enterprise-grade wireless strategy will provide the ability to deploy best-of-breed solutions as part of a cohesive architecture. This will optimally position the company to leverage the many fast-growing wireless technologies in order to maximize their value proposition to the enterprise at large. Q

LOVE IT, HATE IT? LET US KNOW

feedback@acmqueue.com or www.acmqueue.com/forums

BRUCE ZENEL is a vice president in Morgan Stanley’s Institutional Securities Information Technology department.

ANDREW TOY is an associate in Morgan Stanley’s Institutional Securities Information Technology department.

2005 ACM 1542-7730/05/0500 Copyright held by author/owner.