NetMotion™ Wireless

1100 Dexter Avenue N
Seattle, WA 98109
206.691.5555
www.netmotionwireless.com

Networking Standards and Wireless Networks

Developed for NetMotion Wireless
by
Peter Rysavy
www.rysavy.com

RYSAVY RESEARCH

Networking Standards and Wireless Networks

Introduction

Networking standards have played a crucial role in the widespread adoption of computer networks. Through broad acceptance of standards such as the TCP/IP protocol suite, the Internet has allowed a huge number of systems worldwide to interconnect. However, standards must fulfill a true need and be broadly accepted to play such a role. Where standards do not exist, are deficient, or do not enjoy broad acceptance, the networking industry has a long history of using alternative approaches in order to provide users with the functionality they need. In the end, these approaches often have the effect of augmenting standards.

This paper analyzes the growth in wireless networking, what makes wireless networking different from other forms of networking, the various approaches available to address wireless needs, the role of networking standards, and how NetMotion Mobility provides a practical and effective solution today to the most pressing problems of wireless networking.

Wireless market and technology overview

The adoption of wireless networks is surging. Wireless local area networks (WLANs) in particular are proving extremely popular, with rapid growth in industry, businesses, universities, homes, and most recently in public areas like restaurants and airports. IDC predicts that revenue for WLAN equipment worldwide will increase from $1.45 billion in 2001 to $3.72 billion by 2006. With rapidly declining costs, this translates to a huge increase in unit sales. Cellular data is also on the verge of widespread adoption with global deployment of next-generation cellular technologies that include General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS) and Code Division Multiple Access (CDMA) 2000. Especially exciting for users is the emerging integration of WLAN networks with cellular networks, giving users seamless wireless coverage: broadband access in hot-spot areas and lower rate but ubiquitous coverage everywhere else.

As customers gain experience with these wireless technologies, they are finding that wireless is similar to wireline in many respects, but that there are significant differences. Successful use of wireless technologies requires that customers pay special attention to mobility, security, and connection-oriented issues.

IP mobility is an especially troublesome area for wireless networks. Currently, an IP address designates an attachment to a particular network subnet. If WLAN access points bridge traffic directly into a segmented network infrastructure, a mobile user can easily and inadvertently roam across router boundaries into another subnet where the current IP address is no longer valid. If the user is in the midst of a transaction, such as a file download, the effect of acquiring a new IP address is highly disruptive. Beyond this is the even more difficult problem of seamlessly roaming from one type of network (e.g., WLAN) to another type of network (e.g., cellular, LAN, etc.)

Wireless security has received a huge amount of attention recently as researchers have uncovered significant deficiencies with the security mechanisms built into current WLAN standards. Ironically, the majority of customers who have deployed WLANs have not even enabled the flawed security mechanisms available in their hardware today due to the awkwardness of managing the current mechanisms. New security standards such as IEEE 802.1x and IEEE 802.11i will address some of the current shortcomings, but will not be available for some time. Cellular data connections are also vulnerable, as only some cellular networks encrypt data communications.

Finally there are connection issues. Radio waves simply do not offer the same level of reliability as wired connections. Even with the most careful deployments, users will experience temporary connection loss due to interference and gaps in coverage. Losing a connection in the midst of an operation can have a wide range of adverse effects, including operating system lockups, application failure, corrupted transactions, or operations such as file transfers having to be restarted. And what if users want to suspend a device to conserve power? They are likely to run into similar difficulties as servers time out applications and sessions. Beyond their intermittent nature, wireless connections are slower, have higher delays, and cost more than wireline connections.

There are a number of approaches available to customers to address the problems just discussed and to make the applications they run over wireless networks more reliable. These include using new Internet standards (such as Mobile IP), using virtual private network (VPN) technologies, and using products designed specifically to solve these wireless challenges.

In actuality, most customers begin by ignoring the problems, especially because many vendors promote wireless as a wireline replacement. For small office, home, or trial deployments, this is initially all right—but before long, the limitations discussed above become painfully obvious.

Recognizing the limitations of current IP protocols in mobile networks, the Internet Engineering Taskforce (IETF) has spent more than ten years developing a set of protocols called Mobile IP for use with IP version 4 networks (Mobile IPv4). The IETF has also designed similar mobility mechanisms into IP version 6 (Mobile IPv6). These standards solve some of the inherent IP mobility problems, but as we examine in the next section, there are some serious limitations in basing solutions on these standards.

One approach to the security issue is to use traditional VPN technologies. One advantage to a VPN approach is that many customers already use VPNs for their remote workers, and they can use these same VPNs for wireless connectivity. VPNs address security requirements nicely, but are deficient in many other areas.

Given the limitations of these approaches, integrating them into a single mobility solution can be a complex and frustrating undertaking. However, there are solutions engineered to address exactly the requirements imposed by wireless technologies. This is the approach of NetMotion Wireless: its products use the standards that make sense today, and enhancements are used where standards are not sufficient. To understand how NetMotion Wireless augments standards, we need to first understand what constitutes a successful standard and then how well today's standards address mobility requirements.

The role of networking standards

What makes a true standard? Two things: first is an agreement by an accredited standards organization on how something should be done; second is its widespread acceptance and adoption. Formal acceptance of a standard alone in no way guarantees that industry or the marketplace will actually accept or use the standard. For example, the International Organization for Standardization (ISO) spent many years developing a comprehensive family of networking standards called Open Systems Interconnection (OSI), intending to provide a common networking fabric worldwide. Instead, the TCP/IP protocol suite gained immense popularity, and has today become the *de facto* standard for the Internet.

It is important to understand why standards are needed, and the role they play in the adoption and use of technology. The most important reason is for interoperability, enabling multiple vendors to supply equipment that can be integrated into complete systems, ranging from phones plugging into RJ-11 connectors, VCRs connecting to televisions, and in the case of wireless, mobile telephones and wireless modems communicating with wireless networks.

One of the benefits to customers is that an accepted standard reduces technology risk because there are multiple vendors available to choose from. Customers can change vendors if another vendor offers better prices or features or if a vendor stops supplying equipment. Consequently, networking standards can play a crucial role both in legitimizing and providing a foundation for broad use of networking technologies. For example, IEEE 802.11b has ignited the WLAN industry.

To be successful, there are three questions a standard must address: 1) is it useful, 2) is it complete, and 3) is it practical. In the case of the IEEE 802.11 standard, the first version of the standard offered only 2 Mbps of throughput and two types of radio interfaces; it experienced a lukewarm reception. Many vendors continued to supply products based on proprietary approaches. Only after IEEE 802.11b became available did customers and vendors consider the standard truly useful.

As for completeness, standards often only solve a portion of the overall problem, and as a result, vendors extend their implementations with proprietary features to further lock customers in. For example, Cisco is the market leader for WLAN equipment, and complies with IEEE 802.11 standards. Yet to use Cisco's augmented security capabilities, customers need to purchase both network interface cards and access points from Cisco. Mobile IP is another example of a standard that is not complete. It addresses the question of forwarding packets regardless of a mobile station's location, but it does nothing to address transport, session, and application layer optimizations for mobility, nor does it fully address security concerns. Meanwhile, IPSec provides sound security mechanisms, but its tunnels are static and need additional mechanisms to function in a mobile environment.

And even if standards are useful and complete, they may not be immediately practical due to the expense of deployment and use. IP version 6, which addresses the most serious deficiencies of today's IPv4, namely address space and security, is a case in point. IPv6 is commonly accepted as inevitable, yet the transition could take the rest of the decade, and some argue that it may never be fully adopted as vendors invent ever more elaborate workarounds to the limitations of IPv4. Whether or not IPv6 is adopted in the future, it is not practical to build solutions based on it today.

Figure 1 suggests how to evaluate a standard.

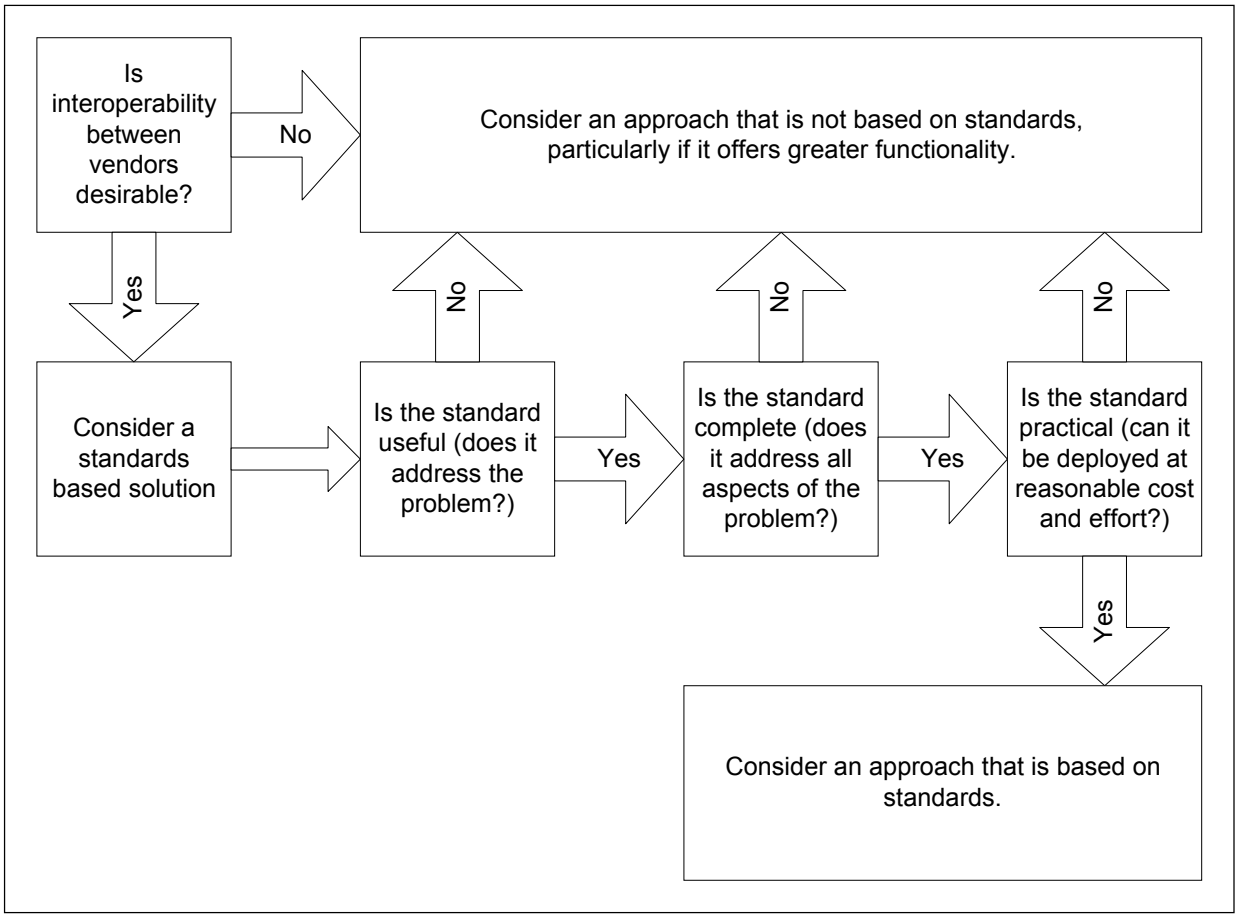

Figure 1: Decision process for standards-based solutions.

When standards do not properly address needs, the marketplace resists adoption. Because Mobile IP does not fully address all of the issues surrounding mobility, key vendors like Microsoft are not supporting the standard. This further erodes motivation for other vendors to support it, and the standard simply has not been able to achieve critical mass.

Table 1 summarizes the strengths and weaknesses of particular networking standards in a mobile environment.

	Strengths	Weaknesses
TCP/IP Protocol Suite	Universally accepted. Excellent interoperability.	Not optimized for wireless connections. No mobility support.
Mobile IP	Provides a mechanism for forwarding packets to a host operating in another network.	Does not address other mobility aspects such as loss of connections or link optimization. Not widely accepted.
IPv6	Increased address space. Mobility support. Security mechanisms.	No deployment today. Huge logistics issues for widespread deployment.
IPSec	Security mechanisms.	No built-in mobility support.

Table 1: Merits of different standards

A final example of a standard that has not fully addressed market needs is the wireless application protocol (WAP). Despite acceptance by hundreds of companies in the wireless industry, this "consortium standard" has experienced limited market penetration due to poor customer utility, interoperability issues, difficulties in developing applications and security weaknesses.

It is not that standards should be avoided—quite the opposite. Standards are absolutely essential to the success of any industry. The author himself chairs a standards committee and has promulgated standards for over a decade. But as discussed, only some formal standards prevail. Meanwhile, other approaches that either substitute for, or augment standards can prove effective in solving specific industry problems. For many years, Novell's proprietary IPX/SPX, Microsoft's NetBEUI, and IBM's SNA protocols were the most common networking protocols in use. Motorola's proprietary ReFLEX paging protocols account for over eighty percent of the paging industry. The Cellular Digital Packet Data (CDPD) specification was developed outside of a formal standards process. Larger companies have prevailed using ingenious communications approaches, and so have some smaller ones, such as Symantec and its pcAnywhere product. Customer demand drove ultimate acceptance, not a formal standards process.

In many cases, there is simply no way for products to be built solely on formal standards: either there aren't any relevant standards that address the entire problem, or the problem does not warrant a standards-based solution in the first place. Perhaps the best approach is to choose a solution that employs accepted standards such as the TCP/IP protocol suite to solve as much of the problem as possible, and then provide complementary and compatible technology to finish the job. With this approach, the standards are enhanced by adding functionality while maintaining compatibility with existing standards, infrastructure, and applications. This is the approach that NetMotion Wireless had taken with their technology.

Advantages of NetMotion Mobility

NetMotion Mobility addresses mobility requirements by using an architecture that consists of software that resides on the mobile device and a mobility management server that acts on its behalf. All communication between these two entities uses a highly efficient, wireless-aware communications protocol over standard TCP/IP protocols. Once a link is established, all application communication requests from the mobile device are executed through the mobility server. Since the server is highly available, it can even represent the mobile device when it is out of range or suspended to save battery life. However, unlike other products that are available in the marketplace where applications must be reconfigured or (re)written to a proprietary application programming interfaces (API), NetMotion allows any IP-based application to operate with no change to the application or infrastructure. One can consider this a transparent deployment.

Furthermore, like Mobile IP, NetMotion Mobility handles all the problems of mobile devices moving across subnets. But unlike Mobile IP it does this without requiring yet another component, known as a "foreign agent," thus making it compatible with today's network infrastructures. In addition, NetMotion Mobility provides a number of significant advantages, including application persistence, central management and control, security, and bandwidth optimization.

Application persistence refers to the ability of NetMotion Mobility to maintain application sessions even if the mobile device moves out of coverage or is suspended. When the mobile device reconnects with a network, applications can resume where they left off.

NetMotion Mobility provides centralized administration with the ability to track mobile devices, perform traffic studies, assist in troubleshooting, and provide information about devices, like connection status and battery level. Managers can enforce access policies that define which network resources are available to each mobile device, and reporting mechanisms show which mobile devices have active connections to the NetMotion Mobility Server. Support for SNMP extends this management information to other network management consoles.

Whereas Mobile IP provides minimal security mechanisms, NetMotion Mobility offers comprehensive security that re-authenticates the mobile device every time it roams to a new subnet, prevents unauthorized users from accessing the system, prevents eavesdropping through optional use of AES encryption, and prevents replay attacks. NetMotion Mobility security is currently integrated with the security features in Windows NT and Windows 2000, including the Windows 2000 Active Directory service. NetMotion Mobility also simplifies deployment in existing networking infrastructure: unlike Mobile IP and IPSec, NetMotion Mobility protocols can readily traverse routers, firewalls, and nodes that perform network address translation.

Finally, no totally standards-based solution today offers bandwidth optimization, a feature that is particularly helpful, if not outright necessary, for cellular data networks where throughputs are low and usage is expensive. Not only do the NetMotion Mobility protocols minimize the amount of traffic communicated, but their resiliency allows recovery from momentary loss of connectivity, a common wireless occurrence that can terminate or hang applications and sessions.

What about conventional VPNs? By conventional, we mean VPNs used in the Internet at large. NetMotion Mobility might be considered a wireless VPN. Many companies are considering these for securing their WLAN connections. While virtual private networks do offer an effective security solution, they do nothing to optimize bandwidth usage, and in fact throttle throughput due to protocol overhead. They also do not address roaming issues, or session persistence. But for companies that need to use VPNs, they can augment these with NetMotion Mobility, which is compatible with them. This combined approach allows customers to maintain their existing corporate policy and to add full mobility support.

Table 2 summarizes the features of NetMotion Mobility compared to a VPN or Mobile IP approach.

	Mobile IP	IPSec	Conventional VPNs	NetMotion Mobility
IP Subnet Roaming	Yes	No	No	Yes
Application Persistence	No	No	No	Yes
Central Management and Control	No	No	Yes	Yes
Security	Partial	Yes	Yes	Yes
Bandwidth Optimization	No	No	Bandwidth Degradation	Yes
Transparent Deployment	No	Yes (assuming support in all appropriate nodes)	Yes	Yes

Table 2: NetMotion Mobility versus Mobile IP, IPSec and VPN approaches

It should be noted that while NetMotion Mobility does not provide mobility standards such as Mobile IP, it complies with and/or is complementary to all standards (formal or *de facto*) that are relevant today, including Mobile IP, TCP/IP protocols, IPSec, IEEE 802.11, and AES encryption. In addition, NetMotion Mobility operates on every important Microsoft Windows platform, including: Pocket PC; Pocket PC 2002; Windows CE 2.1, 3.0; Windows 2000; Windows XP Professional; Windows 95/98/ME; as well as Windows 2000 Server and Windows NT Server.

Most products that use standardized mobility protocols, including NetMotion Mobility, also provide components and capabilities that are not standardized. But the primary benefit of Mobility is that is offers interoperability: one vendor's WLAN card or access point, for example, can be substituted for that of another.

Eventually, standards such as Mobile IP and IPv6 are likely to become broadly available, but this will happen over five to ten years. Because applications must be written to explicitly support IPv6, there will be mixed IPv4 and IPv6 network environments for quite some time and the standards do not adequately address these mixed environments. NetMotion Mobility will continue to play an important role because it allows these mixed environments to easily coexist – and enterprises that use NetMotion Mobility will find that, when the time comes, the transition between evolving technologies will be smoother.

Conclusion

NetMotion Mobility provides significant advantages over what can be accomplished using today's networking standards, at essentially no greater risk. This translates to a competitive advantage today for customers who will obtain greater productivity and lower operational costs from their wireless network. In addition, NetMotion Mobility provides a transition path to tomorrow's IPv6 networking environment.