NetMotion Wireless
1100 Dexter Avenue N
Seattle, WA 98109
206.6915555
www.netmotionwireless.com

Wireless LANs: The Essentials for Saving Your Sanity

WHITE PAPER

Wireless LANs:
The Essentials for Saving Your Sanity

State-of-the-art wireless LAN (WLAN) deployments are undergoing rapid transformation on a number of fronts. The increased standardization of operating systems and protocols, together with declining hardware prices, make previously marginal business cases for WLAN deployment economically viable and attractive. There seems to be little doubt that wireless networks have arrived. Wireless LANs, wireless wide area networks, Bluetooth… they are all over the media and on the "to do" lists of many IT professionals. But you need to know the things your consultants and system integrators may not be telling you. Read about these essentials and you'll be better prepared:

Security

1. Even if you turn on WEP security, your network is not secure
2. Not all VPNs are created equal, or created with wireless in mind
3. You don't want to support multiple security solutions for multiple platforms

Roaming

4. Users who roam out of range create unique security problems
5. Moving between subnets or networks wreaks havoc with applications
6. VLANs and hardware solutions do not solve all your roaming problems
7. Mobile IP does not solve all your subnet roaming problems, either

Application session persistence

8. Battery life is an issue
9. No matter how good your site survey is, you can still have coverage holes
10. You don't want to support custom applications for just your mobile users
11. "Session persistence" means more than forwarding packets to a user's new location
12. Once your field force has a wireless LAN, they will want wireless WAN and hotspot access

The NetMotion Mobility solution

13. NetMotion Mobility makes your wireless network secure and reliable

The wired and the wireless computing worlds operate under very different paradigms. The wired

world assumes a fixed address and a constant connection with high bandwidth. A wireless environment uses intermittent connections and has higher error rates over what is usually a narrower bandwidth. As a result, applications and messaging protocols designed for the wired world operate poorly in a wireless environment. The wireless expectations of end users and IT managers are set by the performance and behaviors of their wired networks. A number of workarounds have been deployed with some measure of success in specific environments, but they don't overcome existing limitations and, as a consequence, the demand for wireless data remains unmet. Below are the issues you need to be familiar with.

Security

1. Even if you turn on WEP security, your network is not secure

The security flaws in WEP have been widely reported, but that doesn't keep others in your organization from thinking that using WEP is good enough. And then there is the problem of rogue access points, which are common enough that all advanced wireless network administration tools include a means of detecting them. Rogue APs can be installed by an employee who wants to extend wireless coverage, but instead ends up making the whole network vulnerable to outside attack. However, if you install a security solution that works independent of your access points, you can avoid these problems completely. What you need to look for is security that starts at the mobile device and ensures both user authentication and, if you need it, data encryption.

Many hardware vendors will tell you that they have solutions for Wi-Fi security. They will also tell you that the solutions entail using their products exclusively, locking you into a single-vendor solution that is not based on industry standards. On top of that, the solutions address only the Wi-Fi networks that are under your control—what do you do about users who need access to a Wi-Fi network in a hotspot or a wide-area wireless solution like CDPD or GPRS? A vendor might also recommend that you use a VPN—which leads us to…

2. Not all VPNs are created equal, or created with wireless in mind

Virtual private networks are common these days on both wired and wireless networks: they connect network components and resources through a secure protocol tunnel so that devices connected to separate networks appear to share a common, private backbone. But not all VPNs will let wireless users roam between subnets or networks without "breaking" the secure tunnel, and not all VPNs will permit transport and application connections to remain established during roaming. Another stumbling block is the operating system—what operating system or systems do the mobile clients have to be running in order to get the protection of a wireless VPN?

3. You don't want to support multiple security solutions for multiple platforms

Another thing to watch out for is relying on OS-based security measures. If your organization is typical, you have more than one operating system on your network, and you can't rely on having the same security features for all of them. For example, IPSec is often cited as the key to a security solution—but for mainstream devices running anything other than Windows 2000 or Windows XP, IPSec is not currently built into the OS, and may be available only from a third party. If you have Windows 2000 and Windows 98 devices, not to mention Windows CE and Pocket PC, you may have to purchase a different software package. This could be a management nightmare—you need a security solution that works for all your devices, not just a few of them.

Roaming

4. Users who roam out of range create unique security problems

Wireless security has many faces—man-in-the-middle attacks, eavesdropping, "free rides," and wide area network security—and you have to think about all of them. One way to ensure the ongoing security of your network when users are mobile is to ensure that users are re-authenticated every time their IP address or network attachment point changes.

5. Moving between subnets or networks wreaks havoc with applications

Today's core networking protocols were not designed with mobility in mind. TCP/IP, for example, assumes that once a connection is established, the device in question will remain at the same network address for the life of that connection. However, if a mobile device is attached to a network that is segmented, and the device moves from one area into another that is serviced by a different subnet, the device needs to acquire a new IP address to function properly on the new network segment. Transport and application end points are then lost and users may be forced to log in again, re-authenticate, restart their applications, and recreate lost data—a true loss in productivity at a cost to the enterprise. There are a few solutions for this problem:

- Deploy a software solution that manages network-addressing issues.
- Attach all WLAN access points to specialized hardware. While this solution makes it possible to forward packets as users move from one subnet to another, application and transport sessions can still crash, forcing users to restart applications and recreate lost data. This occurs because packet-forwarding solutions using specialize hardware do not solve transport layer issues if the user is out of range of an access point, if there is radio interference, or if the device is suspended to conserve battery life. In many cases, the application crashes and the device has to be rebooted anyway.
- Deploy all access points on a single subnet so that there is no change of address (physically or using a VLAN).

But…

6. VLANs and hardware solutions do not solve all your roaming problems

Another constraint of existing technology is that networks are often segmented for manageability. Large enterprise networks are implemented with separate subnets or VLANs for each building, floor, or organizational unit to ensure sufficient bandwidth as traffic increases, to contain data-storms, and to configure different levels of security and data access.

Without true subnet-roaming capabilities, wireless LAN access points must all be connected to a single subnet or VLAN to allow a mobile device to maintain network layer addressability. This is the solution proposed by many popular WLAN hardware vendors and only works for networks segments under your control. This workaround can be used, though it entails a loss of network management flexibility and might come at a significant cost. Some organizations may be willing to incur this forklift upgrade of their network if mobility is important enough to them. Many network environments, however (e.g., multi-building campuses, multi-floored high rises, or older or historical buildings) cannot embrace a "flat" network solution as a practical option. Even with these hardware solutions logically connecting all access points on a single subnet, mobile users still encounter coverage problems. The solution also may not address security issues, thus requiring additional software anyway.

7. Mobile IP does not solve all your subnet roaming problems, either

Mobile IP continues to draw attention as a candidate for use in mobile and wireless environments where IP address management is an issue. IP address management is a necessity when it is impractical or too expensive to deploy all network access points on a "flat" network (where all network points of attachment share the same IP subnet). As a modification to IP version 4 (IPv4), Mobile IP functions at the network layer to manage changes in IP addressing.

But Mobile IP does not address enough of the issues of mobility management to constitute a complete solution and suffers all of the deficiencies of other packet-forwarding approaches (like the hardware solutions mentioned above). Mobile IP does not allow mobile devices and the mobility agents on the network to share state information about each session that a mobile device has established. This means that applications can't persist during periods when the mobile device cannot be reached. When the mobile device reattaches to the network, there may be a need to clean up broken applications sessions, log in again, re-authenticate, restart applications, and re-enter lost data (again a productivity loss, not to mention a usability failure). Furthermore, if a mobile device moves out of coverage, moves into a coverage hole, or suspends to save battery life, Mobile IP, which operates at the network layer, cannot be of service. It does not support persistent connections—continuous, reliable, secure computing in a mobile environment. In addition, Mobile IP is not widely supported on many platforms and does not address security.

Application session persistence

8. Battery life is an issue

No doubt about it, WLAN NICs have an impact on the battery life of a mobile device. To conserve battery life, users should be able to suspend their mobile devices when they are not using them or when they are in transit. Unfortunately, this has the same effect as roaming out of coverage—the application sessions are dropped, causing a loss in user productivity and increased dissatisfaction with the wireless solution.

9. No matter how good your site survey is, you can still have coverage holes

A mobile device's range of mobility is limited by coverage. The positioning and distribution of access points defines coverage within a physical environment. The best way to avoid coverage holes or a situation in which devices are out of range is to create overlapping coverage by blanketing an area with access points. This can work in well-defined spaces, but it adds cost to a customer solution and still does not address situations in which coverage is unreliable due to building construction. Throwing more access points at a problem like this can be expensive and impractical. And when too many access points are deployed in an overlapping area, the interference from adjoining cells reduces system throughput and can have the same effect as coverage holes.

10. You don't want to support custom applications for just your mobile users

Software developers often create custom mobile applications or use mobile libraries to get applications to work in a mobile environment. Customization drives up the cost of implementing wireless solutions, increases the time required to deploy a solution, creates software support requirements, and limits the use of wireless to those applications that can be specialized for mobility. It also means that users must be trained in the use of these custom applications, further driving up cost and time to deployment.

11. “Session persistence” means more than forwarding packets to a user’s new location

“Persistence” is being used in many ways—what should it really mean? Just having packets forwarded as users roam between subnets, coverage areas, and network types (wired LANs, wireless LANs, and wireless WANs) isn’t enough. Many vendors today use the term “persistence” for these packet-forwarding solutions and some people have started to call this “network layer persistence”. But if you don’t have transport and application session persistence, the solution breaks down. Why? Because when a transport protocol cannot communicate to its peer, the underlying protocols, like TCP/IP, assume that the disruption of service is due to network congestion. When this occurs these protocols back off, reducing performance and eventually terminating the connection. The only way to solve this problem is to have mobile nodes deployed with a software solution that acts on behalf of the mobile device when it is unreachable. As Richard Paine, advanced computing technologist at The Boeing Company, puts it, “Our mobility plans require more than just having packets forwarded—without application session persistence, I can’t recommend the solution.”

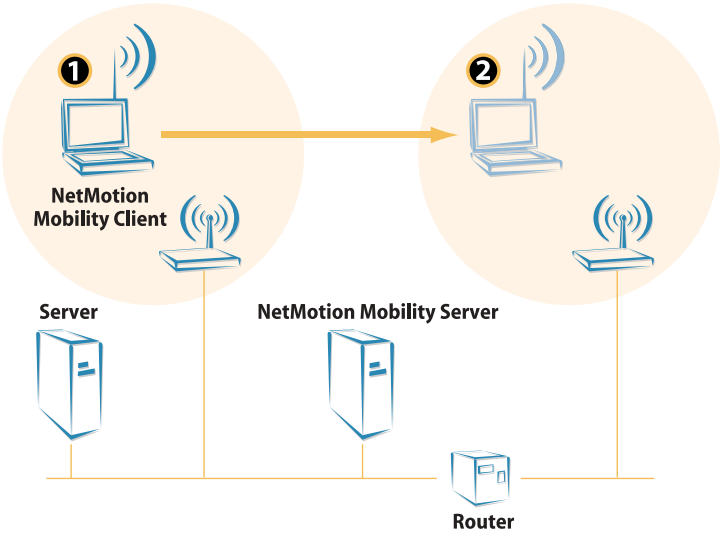
12. Once your field force has a wireless LAN, they will want wireless WAN and hot spot access

Once users have mobility within the company, they will want to have it outside the company—on the road, on sales calls, from conferences. This means you have to begin to consider wireless wide area network (WWAN) solutions. And your users will want to roam between your WLAN and the WWAN without having to think about it. Be prepared to add WWAN access to avoid costly re-fitting later. Wireless LAN hot spot deployments in hotels, airports, conference centers, and other public areas will also create a unique requirement for a wide area solution.

The NetMotion Mobility solution

13. NetMotion Mobility makes your wireless network secure and reliable

One way to deal with all of these challenges is to implement NetMotion Mobility products as part of your wireless infrastructure. A server operates as a proxy for mobile devices as they roam, so users have an essentially continuous connection to application servers on the network.



NetMotion Mobility on a subnetted WLAN network

Network-dependent applications fail when a wireless connection breaks, whether a device suspends to save battery life or moves out of coverage, as pictured above. This is true for both wide area and local area wireless data networks, and cannot be solved by hardware-based solutions that do not include the mobile device in the solution. The network in this figure has an added complication: it is a subnetted WLAN network. But with NetMotion Mobility added, the mobile device 1) can move out of and then back into coverage and 2) acquire a new IP address, while the Mobility server continues to properly route packets to the device, maintaining all active sessions.

NetMotion Mobility Server takes on the responsibility of managing IP addresses and facilitates communication of data and commands between the client and the rest of the network. This ensures transport and application session persistence even as the mobile device roams across subnets, moves in and out of coverage, or is suspended to conserve battery life. In addition, NetMotion Mobility works within existing network security so that the network is not compromised.

- The server maintains the state of each mobile device and handles the session management required to maintain continuous connections to network applications. When a mobile device becomes unreachable because it suspends, moves out of coverage, or changes its "point of presence" address, the server maintains the connection to the network host by acknowledging receipt of data and queuing requests.
- NetMotion Mobility Server also manages network addresses for the mobile devices. Each device running NetMotion Mobility Client has a virtual address on the wired network and a point of presence address. A standard protocol (DHCP) or static assignment determines the virtual address. While the point of presence address of a mobile device will change when the device moves from one subnet to another, the virtual address stays constant while connections are active.
- NetMotion Mobility works with Microsoft's standard TCP/IP protocol. Intelligence on both the mobile device and server assures that an application running on the client remains in synch with its server.
- NetMotion Mobility Server provides centralized system management through console applications and exhaustive metrics. A system administrator can use these tools to configure and manage remote connections, troubleshoot problems, and conduct traffic studies, from either a local desktop or a secure web browser connection.
- The server also manages the security of data that passes between it and the Mobility clients on the public airways or on a wireline network. NetMotion Mobility provides a basic firewall function by giving only authenticated devices access to the network. It can also certify and optionally encrypt all communications between the server and client. NetMotion Mobility fully supports RADIUS and Microsoft's Kerberos, PKI, and IPSec. Tight integration with active directory provides centralized user policy management for security.

The computing environment and the applications do not change—the mobility is there but its use is transparent to the user. Since nearly all applications run unmodified, neither re-development nor user training is required.

The expectations of wireless network users have been set by their desktop experience. They will expect to be able to roam to different IP subnets and different access point coverage areas—only the IT staff is likely to even know where those boundaries are—without losing their application sessions. They will expect to run any application wirelessly that they use on their desktops. And they will expect their wireless communications to remain completely secure. If user expectations aren't met, the wireless LAN that was a critical objective will fall into disuse. As a health care customer put it, NetMotion Mobility "… runs on everything, is inexpensive, and really does exactly what it promises." It's that simple.