

When we discuss wireless you might have a feeling of deja-vu that harkens back to the early days of the public Internet when the importance of the online revolution was acknowledged but its implications not clearly understood. Similarly, many wireless discussions center on notions of a fundamental change in the connected lifestyle, or are unduly focused on a barrage of products, protocols and standards that may only be related by the common goal of working without wires.

By keeping prediction and technology detail to a minimum this brief examines the foundation of the wireless world: the personal, local and wide area wireless networks. Through consideration of these types of network's standards, application potential, and cautions, this analysis provides an introduction to working wireless.

### **What Kind of Wireless**

For the purpose of this brief, we will break the wireless discussion into three segments:

**The Wireless Personal Area Network (WPAN)... Wireless desktop.**

**The Wireless Local Area Network (WLAN)... Wireless building.**

**The Wireless Wide Area Network (WWAN)... Wireless on the road.**

Each type of network is applicable to different types of use and carries its own standard sets, operability focus and security concerns. Here is a quick look at these three networks:

#### **Wireless Personal Area Networks/WPAN: The wireless desktop.**

The WPAN is a network designed for a small group or individual person. The WPAN has limited range and is used to transfer data between a mobile/unconnected device and receiver such as a PC. Examples of use for WPAN can be found in the wireless device (PDA, Input device, Cell, etc.) that can wirelessly transmit data across the office to PC. WPAN has a close range of approximately 20 feet without an additional booster.

Premier network enabling standards for WPANs come in two base types:

- Point to Point, which eliminates the wires, but doesn't offer interoperability, and;
- Multipoint, which promise wireless interoperability between different devices.

There are numerous proprietary point to point standards (requiring individual transmitters and receivers), but multipoint wireless personal networks are primarily enabled by Bluetooth and 802.15, based on Bluetooth. The goal of a multipoint WPAN is to enable a variety of devices to connect to many other independent devices as opposed to necessitating a receiver and transmitter for each device. For example, keyboard manufacturer NMB Technologies Corporation produces a 2.4GHz Bluetooth-HID keyboard that can interact with any other Bluetooth-HID system such as a computer, PDA or Set-Top Box.

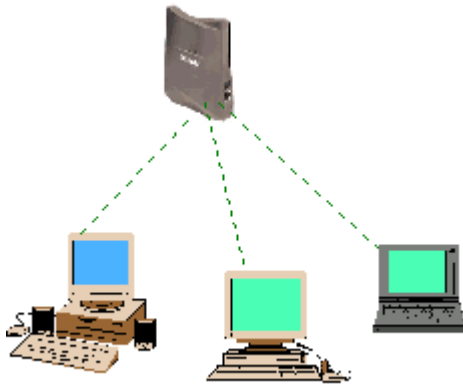
However, to achieve the promise of multi-point communication across a Bluetooth wireless network there is still more work to be done to integrate these devices and establish one Bluetooth implementation standard. Proof of the operability obstacle is found by review of top PC's which utilize completely different Bluetooth user interfaces. The result for even a skilled user is frequently failure to connect different Bluetooth enabled devices. For this reason, the Bluetooth SIG will be publishing implementation guides for each of the Bluetooth profiles (computer, PDA, input device, phone, file exchange, headset, et al) which can be used by device manufacturers

and vendors that want to ensure a more consistent near-field-communication outcome for their customers.<sup>1</sup>

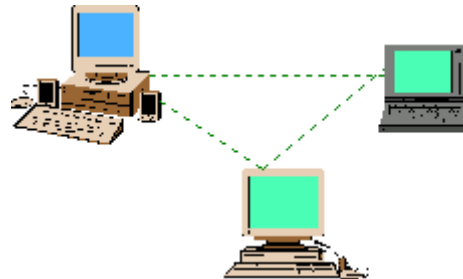
### **Wireless Local Area Networks (WLAN)... The wireless building.**

Like the name suggests, WLANs offer network access without the wires. A WLAN solution offers advantages not only in convenience of use for mobile users, but is a data enabler for those in situations or locations where a hardwire network connection is not an option. Beyond the office-worker who would benefit by taking the laptop to a meeting is the worker on the move who cannot hard-wire a connection for their data needs at every stop. Examples in this area can be found in the medical space where doctors and medical personnel move from area to area still relying on paper-based data to treat their patients. Workers in these situations will be able to improve efficiency by being connected and increasingly paperless even when on the move.

A wireless LAN does not require lining up devices for line of sight transmission like IrDA. Wireless access points (base stations) are connected to an Ethernet hub or server and transmit a radio frequency over an area of several hundred to a thousand feet which can penetrate walls and other non-metal barriers. Roaming users can be handed off from one access point to another like a cellular phone system. Laptops use wireless modems that plug into an existing Ethernet port or that are self contained on PC cards, while stand-alone desktops and servers use plug-in cards (ISA, PCI, etc.).



**Figure 1: 802.11b Wireless Ethernet, Infrastructure Mode: a communication method that requires a wireless access point.**



**Figure 2: 802.11b Wireless Ethernet without an access point: Two or more wireless Ethernet computers (802.11b) may communicate with each other without a wireless access point.**

A family of standards for wireless LANs was first introduced in 1997. The first standard was 802.11b, which specifies from 1 to 11 Mbps in the unlicensed 2.4GHz band. Also working from the 802.11 standard, but offering a significant improvement in data-rates over 802.11b is 802.11g which was approved June 2003 by the IEEE (Institute of Electrical and Electronics Engineers). The 802.11g standard for wireless local area networks extends the data rate of 802.11b to 54 Mbps from its current level of 11 Mbps.

<sup>1</sup> The Bluetooth Truth Hurts, David Berlind, ZDNet, May 2003

### **The Wireless Wide Area Network (WWAN)... Wireless on the road.**

You have undoubtedly heard the hype: 3G, the last mile, expanded local loop, ubiquitous networking, the holy grail of mobile computing... so what is it?

Wireless Wide Area Networks cover a wide geographic area, such as a county, state or country. WWANs offer an alternative to traditional copper wire or coaxial cable which was previously the carrier of the connection between the customer and the cable or telephone company. The elimination of the need for wire over a wide area enables greater rural connectivity, empowers connection during travel, and promises obvious process and direct cost improvements.<sup>2</sup> Though the promise of the WWAN is great, the current model presents some challenges which need to be met before the 'ubiquitous, 3G, last mile network' is realized.

CDMA network (Code Division Multiple Access) providers such as AT&T and Sprint have achieved a degree of wide area wireless with coverage mirroring cellular networks and speed claims of up to 130KB. Current CDMA services offer better speed than dial-up but it is still not enough for complex applications and with the monthly price between \$70-100/month the cost is prohibitive.

While providers of CDMA services predict a rough doubling of speed and a significant lowering of cost over the next sixteen months, other options such as 802.16 offer much greater speed (70Mbps at a range of up to 35 miles)<sup>3</sup>, but do not currently have the coverage of existing CDMA networks. However, groups such as The WiMAX Forum, ([www.wimaxforum.org](http://www.wimaxforum.org)) are actively working to promote development of 802.16 broadband wireless networks and certify the interoperability of products and technologies supporting this protocol.

### **Wireless Warning**

Having reviewed the some of the fundamental specifications for personal through wide area wireless networks, the discussion will turn to one of the most formidable obstacles to wireless implementation... security.

Because wireless is a shared medium, everything that is transmitted or received over a wireless network can be intercepted. Encryption and authentication should always be considered when developing a wireless networking system; however analysts estimate that more than 50% of wireless networks are completely unprotected<sup>4</sup>; of protected wireless networks, security protocols are often not appropriately applied and their weaknesses not understood. At issue is the relative ease for any individual with a wireless LAN adapter and a portable computer to access an un-secure network.

---

<sup>2</sup> WWAN process and cost benefit is the focus of much analytical attention from both industry and research groups... or a combination of both such as this IDC paper sponsored by Intel: [Untethered Computing: Feasible, Economic, and Desirable.](#)

<sup>3</sup> 802.16 offers true broadband speed and can hand off between 802.11 networks with adaptation; however the integration between and mobility across this network is not intuitive and would require cooperation is a close proximity such as large city. The lack of current infrastructure for 802.16 is a cornerstone of the CDMA argument.

<sup>4</sup> Wireless Security End to End, Carter and Shumway, CISSP

Any network adapter coming within range of another 802.11b network adapter or access point can instantly connect and join the network unless the network transmissions are secure. To complicate matters, each wireless network has specific concerns that need be addressed by different types and combinations of security systems. Dependent on IT policy and user patterns, wireless network administrators may not only need be concerned about protecting the network from unauthorized access, but also about protecting WLAN enabled mobile devices from undesired intrusion at another network's hotspot.

To mitigate the risks of wirelessly transmitting data, 802.11 compliant products offer some options for providing for authentications and privacy. The Wired Equivalent Privacy (WEP) standard provides a mechanism from protecting data with 40- or 128-bit RC4-based encryption. However some serious flaws have been discovered in the WEP mechanism that could render it ineffective against a deliberate intrusion by a moderately skilled attacker... the tools to discover wireless networks and break light-security are public.

### **So then, what is the status and future of wireless technology?**

Wireless access is real, can be secure, and offers hard and soft benefits which may be had immediately. However, there is a great deal of space between the wireless networks which are readily available in 2003 and the degree of interoperability and wireless improvement we will see in 2004-05. While a carefully planned wireless network and device management plan may currently offer freedom from the necessity of hardwire, there are legitimate obstacles to taking one's devices, data and applications from the 'home' or 'base' network and using them at another wireless network hotspot. For the future, the current intense IT industry review of wireless network security and interoperability will afford tremendous improvement of secure wireless connections in the next 18 months... but what of the devices?

Beyond the ability to use a wireless network securely is the question of what types of devices will be enabled and authorized to connect to said networks. Will we be able to walk up to a wireless printer at an Airport or other hotspot, and using any sort of personal data device (phone, pda, pc, etc), be able to easily print our data in the correct format regardless of the operating system or application being used? The answer: It depends. It depends on the adoption of device management standards and use of non-proprietary access protocol. That said, the benefits of true wireless device connection and interoperability not only offer obvious benefit to the end-user, but promise profit to the manufacturer and reseller... look for more on implementation standards from groups like Bluetooth SIG over the next year and a half.

### **The Bottom Line**

Though there is room for, and will certainly be improvements, wireless networks currently offer convenience, mobile productivity, and direct network cost reductions. The benefits offered by wireless networks provide many reasons to consider their use. However, managing wireless risk is difficult and requires careful planning, dedicated administration and a regular schedule of review. Only with a commitment to complete consideration of wireless implications, both benefits and risks, should the informed organization move forward with a wireless device or network implementation.

## **Resources For This Brief**

Wireless Security End to End, Carter and Shumway, CISSP

Paving the Way for Personal Area Network Standards: An Overview of the IEEE

<http://www.comsoc.org/pci/private/2000/feb/Gifford.html>

P802.15 Working Group for Wireless Personal Area Networks

Siep, Gifford, Braley, Heile

The wireless glossary

<http://www.devx.com/wireless/>

Techweb Definitions

<http://www.techweb.com>

Newsweek

Wi-Fi Goes Wild

Jason McLlure and Jamie Reno

The Computer Desktop Encyclopedia

2002 Intersil Corporation