

Wireless Networking: Not as Easy As It Looks

Security and technology issues, and their costs, must be faced before you build a muni WiFi net

By Tom Henderson ■ *ExtremeLabs*

Like wireless computing. Air is the ideal first mile. With wireless, I can do many crazy projects that I can't say 'no' to, wherever I am. So far this year, this means New York City, The Netherlands and Germany, San Jose, Tampa, Las Vegas (too many times), Chicago, Washington DC, and many airports in between.

Most airports have some kind of wireless offering. And every one of those offerings is like most others you'll see today – not only insecure, but also full of malware-infested client apps looking for new homes and unwitting victims.

My lab has wireless, and we get occasional drive-bys that try to crack it. So far, none has taken the juicy bait. Although I consider myself a wireless advocate, I prefer using a simple card from Verizon, an EV-DO card that fits into my Mac PowerBook.

Municipalities are also working toward wireless offerings – the “muni-wireless” phenomenon. Philadelphia is trying to do it. New Orleans did. San Francisco is on its way, as are other communities across the country. It's a nice idea: Increasing quality of life through mobility and convenience. RFPs now fly around the country, asking vendors for plans to do wireless networking. I applaud them in some ways, but I am very worried in others.

My advice to municipal officials: Don't over-promise. Successful wireless deployments are accomplished only when expectations are managed, because wireless connectivity is mercurial. Whether you are dealing with application support or network area coverage, and whether it's muni-wireless covering an area the size

My advice to municipal officials: Don't over-promise. Successful wireless deployments are accomplished only when expectations are managed, because wireless connectivity is mercurial.... It's all about implementation and application support – and the inevitable security questions.

of Philadelphia or San Francisco, or just the connections at the local Starbucks, it's all about implementation and application support – and the inevitable security questions.

WiFi networks, and data sent on them, are highly vulnerable to interception unless proper security measures are used – and managed. Services available to DSL and broadband users may not be usable over WiFi for now, or even the foreseeable future. Users don't really understand limitations, and so a few sentences on a WiFi greeting screen can mean the difference between happiness and seemingly eternal grouching.

Even the best WiFi municipal or community networks will not reach everyone, it's nearly impossible. Vendors are becoming very sensitive to coverage issues, and are using numerous methods to extend the reach of WiFi to their desired boundaries.

Wireless isn't a passing fancy, but asset life will be short lived compared to other broadband technologies as new generations of WiFi arrive on the scene. If these new technologies remain as affordable as WiFi is today, then we'll greet them with

glee for the enhanced expectations we can have in terms of performance and security. Otherwise, remaining skeptical can improve your quality of experience.

The Real Specs of 802.11

There are three viable “WiFi” wireless specs, derived from the IEEE's 802.11b/g, 802.11a, and 802.11n. Each is incompatible with the other, although 802.11n equipment is often backward-compatible with 802.11b/g. You can also buy equipment that combines all three. Beyond WiFi is WiMAX, the IEEE 802.16 standard, right now a far more difficult and expensive technology to deliver.

Both the 802.11b/g and 802.11n use the 2.4 GHz band. They're limited as to the amount of power they can transmit, and the power usage and antennas deployed define the operational radius of each access point. Each access point is, in turn, a central connecting device to an upstream network, usually the Internet. While this operational “cell” area is normally about 100-200 meters across (depending on many factors), using legal equipment, engineers at Defcon 13 were able to get a usable signal at over 120 miles.

Wireless isn't a passing fancy, but asset life will be short lived compared to other broadband technologies as new generations of WiFi arrive on the scene.

The 802.11a specification uses portions of the 5 GHz band, and was actually ratified before the other WiFi specs. Because of several factors, it hasn't been very popular – even though there are more non-overlapping channels available – eight or more. By contrast, the 802.11b/g and 802.11n (also known as MIMO) specifications are limited to three channels that don't overlap.

Interference Problems

The number of non-overlapping channels is extremely important. If they do overlap, or if one access point can "hear" the signals of another on the same channel or an overlapping one, they will interfere and have contention problems with each other. This means that 802.11b/g/n have to be somewhat controlled geographically speaking when laying out areas covered by cells, so that the cells' access points don't interfere with each other.

Some vendors of wireless products have ways to deal with this problem. They have software intelligence that closely monitors access points, adjusting both their power and even their available channels to prevent this so-called "co-channel interference" (or simply "CCI"). Some vendors and installers will use varying kinds of equipment to assess an area, choose an optimum layout, then "tweak" the layout after installation.

No matter what is done, CCI must be dealt with because it robs the access points of their ability to give speedy data to the (usually) portable computers that they must service. This results in slow speed, constant authentication problems for users, and poor overall satisfaction.

An additional effect is that the placement of 802.11b/g/n access points (and their antennas) still creates 'blind spots' where coverage can't be provided without a lot of work (entailing specialized antennas, monitoring, and perhaps special antennas for the users' client computers).

The same can be said for 802.11a, except that because there are so many non-interfering channels to choose from, placement isn't quite as critical a calculation step.

The Uplink

Each WiFi access point represents the first few hundred meters to a computer user's WiFi electronics. In turn, the access point has to uplink to the Internet. This is accomplished in one of two ways, either by a copper or fiber connection, or through a wireless uplink.

The access point is a local network control device, and has domain over devices connected to it – as though all the devices connected to each access point constitute a small LAN. When going through a wired uplink, the access point is controlled, and often throttled, by the speed of its uplink.

Wireless uplinks use one of two methods, either uplinking 802.11b/g/ (802.11n soon) via 802.11a, or via WiMAX. The new WiMAX standard provides point-to-multipoint connections (just as WiFi access points do) or point-to-point links at approximately 75 Mbps – in both directions. That's much faster than today's WiFi. In either case, several uplink hops from access point to access point can be accomplished wirelessly until the bandwidth consumed by the aggregation becomes throttled by the speed of 802.11a or a WiMAX alternative.

Either method, copper or fiber, or wireless uplinking, requires ever-faster uplink connections that also support things like automatic Quality of Service (QoS) or CoS (Class of Service) that can allow timing-sensitive applications to run without delays that affect quality – heard as conversational pauses or outages and seen as pixellation in video streams.

There are multiple methods for uplinking wireless access points, ranging from a simple indoor Ethernet connection to sophisticated broadband-over-power line

(BPL) backhaul using pole-mounted access points. Uplinking methods may include DSL and cable TV digital modems and fiber-to-copper conversion equipment. Each and every network is built differently, in terms of the first fifty meters, if not the first mile or kilometer. This has led to costly systems overlap in the US, where multiple providers deploy duplicate assets to try to capture the same customer – chasing the same dollar.

Your Data, In the Nude

Even if you, in your home or office or plant or campus or wherever, decides to do WiFi, there are several onerous problems. The first is security. Most places deploy publicly accessible WiFi with no security of any kind. If you connect in this way – through an unsecured hotspot, then unless you're using HTTPS, SSL, or another encryption method, all things you type can be seen by rudimentary capture programs that any 12-year-old (and even many adults) can find on the net in about five seconds.

That means your logons, your passwords, and everything you send can be seen as though you were handing it to someone on a platter. Essentially, your conversations are naked.

There are several grades of security that can be used in all WiFi products, and using just one (or demanding other encryption methods) will take away the network nudity. However, early encryption schemes used in WiFi products are simple to crack, taking just a few seconds to decrypt the keys that will expose all data going in and out of an access point. This encryption, known as WEP, comes in flavors from "weak" to "strong." Strong WEP takes about 22 minutes to crack.

Finally, there's a standard called WPA, which has variants, some of which are agreed (by experts who should know) as profoundly difficult to crack. These advanced forms of authenticating users and encrypting conversations requires only astute usernames and passwords.

WPA is safe enough for most uses, but computers connecting wirelessly must also have adequate firewalls and security software running to achieve what I, as a paranoid skeptic might call, wireless peace. Otherwise, someone may not be

Most places deploy publicly accessible WiFi with no security of any kind. If you connect in this way – through an unsecured hotspot, then unless you're using HTTPS, SSL, or another encryption method, all things you type can be seen by rudimentary capture programs that any 12-year-old (and even many adults) can find on the net in about five seconds.

able to read your message transmissions but may be able to read your hard drive.

Application Sensitivities

Four items have a direct bearing on applications, and many of them relate to speed in some way. First are the issues of what applications are able to take what priority within a network. This is called Quality of Service (QoS). Do isochronous applications like VoIP, video, and other

apps that live within their own time domain (and are sensitive to bandwidth, delays, routing events and competition for resources) get priority over Web surfing or email or Bit Torrent, or other downloads? No one wants to answer the question, so I'll try to do so: video downloads over commonly used protocols should be halted – as they're similar to dragging a bowling ball through a garden hose.

A second concern surrounds application

blocks. Some ISPs already block specific applications, ranging from Skype to RSS/Atom feeds. Your network may or may not have a no-blockage policy – but this doesn't mean that upstream, an ISP or carrier won't try to block what it believes to be “nuisance” applications from its infrastructure. A great wireless connection to Skype could be blocked for many different reasons, and many of those might be legal. The expectation that users have over what might or might not be supported is very important because blocked applications generate support/help desk calls needlessly.

The inherent limitations of the 802.11 “MAC” (ISO/OSI network Layer 1) design also means that there is a limitation to each access point regarding the number of users – and importantly available bandwidth among those users – that can be delivered. If all users are nearby (meaning that the access point hasn't fallen back automatically to a slower data rate because it can't hear the client sufficiently) and have applications that use available bandwidth resources conservatively, then it's a happy world and expectations of reasonable delivery times can be made.

The shared resource of an access point can be enhanced through the use of high-density access points, which are actually multiple access points built into special frames with specialized antennas – usually for conference rooms or other dense population uses.

It's possible, however, for a single user to dominate resources when downloading streams – whether governed by QoS protocol rules or not – to the detriment of all users of that access point. In fact, users can download software that mounts a denial-of-service attack on an access point. Will municipal officials roll a police car every time this happens?

The wave towards wireless is unstoppable, and each wave hits various rocks. It's important to give wireless network users realistic expectations about security, usable applications, blocked applications, and easily accessible help instructions. **BBP**

About the Author

Tom Henderson is Managing Director, ExtremeLabs, Inc. The company tests high-end networks and computer systems. He can be reached at 317-253-1169.

DON'T Miss It!

Broadband Properties
2006 Summit Irving, Texas

A Towns and Technologies Conference series, presents:
“Big Broadband for the First Mile”

September 11 – 13, 2006
 Marriott Las Colinas
 Irving, Texas

Space is filling up fast
 Call today to reserve your participation
 877-588-1649 or visit us on the web
 at www.bbpmag.com