# Sound Solutions for Wireless Woes

By Wayne Caswell
CAZITech Consulting
www.cazitech.com

*Several new technologies will improve the range and speed of wireless networks, with a combined effect of 10,000 times the capacity of dialup 56 Kbps modems. With such advancements, networks that use radio signals for communication could replace most of the network cabling we now use. How real is this promise? When will we see it? And what will it mean for equipment manufacturers, service providers, homebuilders, and homeowners?*

January is a good time to reflect back on the past year, ponder the future, and explore the answers to those questions. I just returned from the annual International Consumer Electronics Show where many of the newest devices and technologies are shown. A similar article, *"Wireless in 2003: CES Shows Consumers the Way,"* (www.hometoys.com/mentors/caswell) provided a starting point for listing important events of the year and for considering the wireless potential and challenges still ahead.

This report examines wireless developments during 2003 and those on the near horizon, along with their implications for three categories of wireless products and services:

1. Wireless LAN (WLAN) for devices in local networks,
2. Cellular & PCS service for highly mobile devices in wide coverage areas, and
3. Fixed broadband wireless for buildings and stationary devices.

The report concludes with implications for homeowners and builders.

**IEEE 802.11 Standards (Wireless LAN)**

Wireless Fidelity (Wi-Fi) is the consumer name covering a mix of IEEE 802.11 standards, including 802.11b, 802.11g, and 802.11a. It has become the worldwide standard for wireless LANs, beating out competitors like HomeRF. Wi-Fi is "wireless Ethernet," and compared to other wireless technologies like GSM, PCS and CDMA, it has a wider global presence.

Sales of Wi-Fi products helped lead the technology industry into recovery last year. Market research firm In-Stat/MDR says over 22 million Wi-Fi products shipped in 2003, an increase of more than 200% over 2002, when the industry sold about 7.2 million units. But even with this success, it's clear that there still is a lot of work to do in the area of standards.

Security remains a critical issue that has tempered enterprise deployment and caused most of the growth to occur in homes where security is less of a concern. Quality-of-service (QoS) is another concern because of new wireless applications for home users that include voice services and streaming audio and video.

*802.11g (2.4 GHz)*

802.11g gained momentum in 2003 as a faster follow-on to 802.11b. Its rated speed of 54 Mbps (about 22 Mbps throughput at close range) compares well against 802.11b (11 Mbps with 4-5 Mbps throughput). The added speed means that newer .11g products should outsell .11b products in 2004, even as prices of the older products fall; and this trend parallels what happened with Ethernet. Older 10 Mbps Ethernet adapters gave way to new ones that were 10 times faster, were backward compatible, and only carried a small price premium.

The two 802.11 standards are compatible since they both use the license-free 2.4 GHz frequency band. That band is especially crowded, however, since cordless phones, microwave ovens, and numerous other devices that cause interference also use it. Because it's becoming more difficult to avoid interference problems at 2.4 GHz, I recommend looking at 802.11a instead, and I'm especially excited about products that automatically support both 2.4 GHz and 5 GHz frequencies.

### *802.11a (5 GHz)*

A key advantage of 802.11a is that it's less susceptible to radio interference. The 5 GHz band is less noisy than the crowded 2.4 GHz band, and with more spectrum available there's more non-overlapping channels and more overall performance. 802.11a has 19 channels in most of the world, and the FCC just increased that to 24 in the United States. Avoiding interference will become a critical factor as wireless networks gain popularity and more people have them. In contrast, 802.11b and .11g each have only three non-overlapping channels, so it's harder to avoid interference from neighboring networks.

Everyone is not a fan of 802.11a, and companies that only sell 802.11g products often say the .11a standard has a limited market. I don't agree, however, and think this rhetoric is simply designed to protect their turf.

Because 802.11a uses a different frequency band (5 GHz), a common complaint is that it is not compatible with the large installed base of .11b products, but several companies already offer multi-mode products that support either standard. The NetGear equipment I use, for example, recognizes both .11b and .11a networks and automatically picks the band with the best performance. My notebook PC uses 802.11a at home and downshifts to .11b when I'm at a public hotspot.

A second argument is the theory that 802.11a has a limited range because there's more signal loss over distance with higher frequencies, thus impacting performance. That's not necessarily the case and not supported by my own experience. I placed a single access point in my home office, and it provides an average throughput of about 70 Mbps anywhere in the house, using Netgear's proprietary "turbo" mode. That's much faster than native .11g products deliver, with just 22 Mbps of throughput. And even though NetGear now offers an upgrade to add .11g support, I feel no need to install it.

Contrary to some claims, 802.11a doesn't necessarily cost more since retail prices depend more on the manufacturer, the store, and marketing promotions. Several months ago I paid $29.95 for my multimode PC card adapters and $49.95 for my access point, after receiving $50 rebates on each, and I still haven't seen 802.11g products advertised with a lower price.

A final concern with 802.11a was recently settled at a conference sponsored by the International Telecommunications Union in Geneva, Switzerland. Negotiators from 180 nations agreed to allocate more bandwidth for 802.11a products in the 5 GHz band and eliminated differences in how countries allocate spectrum in that band. As a result, vendors can more easily make products for use anywhere in the world.

### *802.11e (Quality of Service)*

Applications for home users are expanding beyond simple data networking and now include voice services and audio and video streaming. These apps add specific requirements for bandwidth, latency, and jitter that current 802.11 standards don't satisfy. So the standards community has put a high priority on adding quality-of-service (QoS) guarantees. Most of this work is in the 802.11e task group.

I see little chance of 802.11e actually solving the QoS problem, however, because every device in the network must play by the same rules that give some information packets priority over others. For QoS to work, each device in a network must be replaced or upgraded, since any one device that ignores the rules or cheats can destroy QoS for all others.

The QoS problem goes beyond simple priorities and also includes the issue of RF interference since 802.11 is contention-based and uses CSMA-CA protocols. “Carrier Sense Multiple Access – Collision Avoidance” is the protocol that causes devices to first listen before transmitting. If they hear other transmissions (or noise), they must wait a random amount of time before retrying. These minor delays are not noticed in data apps, and video apps can compensate by buffering content, but voice apps have very tight timing requirements, and any interference can be deadly. In the worse cases, 802.11b and .11g networks can be shut down entirely by certain types of interference from cordless phones that hold up their transmit energy for the entire duration of a phone call.

The interference problem is easier to solve in the 5 GHz band where the additional capacity gives enough “headroom” to help avoid packet collisions and where it’s easier to pick a clean channel. That’s why I think apps that need QoS will migrate to 802.11a until Wi-Fi is replaced by something better.

### *802.11i (Security)*

Privacy is about perception; security is about trust; and technology either makes us feel better or causes more concern. I find it interesting that personal modesty goes out the door when we are seriously injured and need medical attention, but hidden cameras in restrooms or airports outrage us. And even though many of us grew up in neighborhoods where we never locked the doors, but we wouldn’t think of doing that today. Wireless brings similar conflicts, with both great benefits and serious concerns.

Security remains a concern for wireless enterprise and consumer apps since radio signals penetrate walls and can be monitored by someone miles away with a directional antenna. Wi-Fi products include an encryption mechanism called Wire Equivalent Protection, and while enabling WEP can add complexity and reduce performance, not having it is like having no lock on your door.

WEP is like a flimsy lock. It won’t keep out determined criminals, but it does an effective job against casual burglars. Please follow the advice of experts and turn on WEP. Here’s what can happen if you don’t:

1. Personal Records – A young reporter doing work on a story at Palo Alto High School made a discovery that evolved into a much bigger story on security that was picked up by TechTV and other national media. It was a huge embarrassment for the school district and could have been far worse. The reporter opened her notebook PC to take notes, and up popped a Windows XP invitation to log into the school’s wireless network. OK, why not? Once connected, she discovered that personal student files weren’t even password protected. They included a psychological profile of each student, grades, home addresses, phone numbers, and color photographs. OUCH!

2. Credit Card Numbers – A network administrator who went to BestBuy with his wife stayed in the car working on a project while she went inside. While typing on his notebook PC, he noticed that there was unprotected network nearby, so he curiously checked it out. The guy didn’t want to hack into the network itself but just wondered what kind of information was being sent, so he started a trace program. Concerned by what he saw, he left the PC running and went inside to buy something. He returned and found his credit card number in the trace log, so he took the PC in to show the store manager. They closed the store immediately and didn’t open again until the problem was fixed. It

seems that BestBuy used Wi-Fi to connect cash registers to the back office systems for credit verification, but they never turned on WEP. OOPS!

3. National Security – A grandfather with no experience downloading digital music was surprised to be the subject of a lawsuit by the RIAA. He had an unprotected wireless network, and it seems that a neighbor (or even someone high on a hill a mile away with a directional antenna) must have tapped into his network for free Internet access. This brings up a national security concern, because an Internet trace only goes as far as the IP address. In this case it was the grandfather's Internet account, but it could be your PC; and instead of a neighbor looking for music, it could be an international terrorist. SCARED YET?

The standards guys know they should have made WEP mandatory, so the 802.11i task group is working on security improvements for 2004. Some of them are available to vendors today. Even before official 802.11i security standards are ratified, the Wi-Fi Alliance endorsed a specification called WPA (Wi-Fi Protected Access). WPA includes much stronger encryption, user authentication, and dynamic encryption-key distribution, and since most homes and small offices don't have network administrators or authentication servers, a simplified mechanism is included as well.

Security will remain an issue throughout the year because Wi-Fi can't be made bulletproof. A lot of work has been done on products that find the rogue access points that compromise network security (usually installed by office workers or others), but none of those products are able to find a lurker. A lurker is someone that simply monitors network traffic, decrypting it if need be, but never actually transmits or attempts to break in. The lurker can collect personal records and credit card numbers and become a national threat without detection.

### *802.11n (faster still)*

Even with planned QoS enhancements, Wi-Fi won't easily send high-definition TV programs from your PVR to HDTV sets, at least not this year. There's not enough wireless capacity, but that will change in the future.

One initiative for the 2005-2006 timeframe is IEEE 802.11n. Developers have defined a requirement for at least 100 Mbps of real throughput, not just the rated radio speed. That's enough for several HDTV streams.

802.11n will operate in the 5 GHz bands and include built-in QoS and security. You may not need its performance now, but you'll want it when falling prices entice you to mount flat-panel HDTV sets on walls. You won't want to see the wires, and you'll want to watch content that's stored in your media center.

## **IEEE 802.15 Standards (Wireless PAN)**

The 802.15 Working Group develops low-power standards for personal area networks (PANs) with long battery life and low cost requirements. Some of the interesting sub-groups include:

- 802.15.1 – derivative of Bluetooth
- 802.15.3 – 20+ Mbps WPAN for digital imaging and multimedia
- 802.15.3a – 110+ Mbps follow-on to 802.15.3
- 802.15.4 – 200 Kbps max for interactive toys, sensor, actuators and automation

### *802.15.3 and .15.3a (Ultra-wideband)*

802.15.3 is a recently approved standard for high-speed PANs. It operates in the same 2.4 GHz band as 802.11g but uses much less power, so it has a shorter range of about 30 feet like Bluetooth instead of up to 300 feet for .11g. It includes QoS for voice and video apps and should have enough capacity to carry one HDTV signal from a set-top box to a TV.

Developer are also working on a follow-on standard that uses the same media access control (MAC) layer on top of ultra-wideband (UWB) radio technology for much higher performance that should exceed 100 Mbps. While 802.15.3 is being positioned as a high-speed wireless PAN, some advocates expect it to compete with 802.11n and offer whole-house coverage, but they've not said how they'll extend the range.

Proponents say ultra-wideband could blow Wi-Fi away in a few years with performance that could exceed 1 Gbps. UWB spreads itself across more spectrum than Wi-Fi and does it in a way that both avoids interference and causes less of it. It also uses far less power than even Bluetooth, so some say UWB could eventually replace both Bluetooth and Wi-Fi, but that's still years away.

UWB became an important technology last year when the FCC approved its use in commercial applications. Current rules governing UWB limit the transmit power, but the FCC has hinted that it may relax those rules and allow more power and more spectrum. (That may be how UWB gets more range.)

Political infighting in the 802.15.3a group is currently divided over two competing technologies – Multiband OFDM and Direct Sequence CDMA. Consumers won't really care which one wins, but it will be interesting to watch how the battle plays out since each side has its own set of advantages and strong allies. Motorola has an early start in the UWB battle by providing chipsets from its recent acquisition of XtremeSpectrum, and early adopters of its technology include companies like Samsung. On the other side, a group led by Texas Instruments has gained press coverage of Multiband OFDM, describing it as a new technology for sending cable television signals from wall outlets to nearby TV sets. I won't bet on a winner since history has shown that it may not be the better technology.

### *802.15.4 (ZigBee)*

ZigBee is for applications that need the ultimate in low cost and low power-consumption – things like smoke alarms, security sensors, and tire pressure sensors that must function for the 50,000 mile life of the tire tread.

ZigBee is not fast by data networking standards, but it's good enough for wireless keyboards, mice, toys, and control systems. ZigBee supports speeds of 20 Kbps in the 858 MHz band (in Europe), 40 Kbps in the 902-928 KHz band (in the U.S.), and 250 Kbps in the 2.4 GHz band. When ZigBee apps need a range past 30 feet, devices can create mesh topologies with multi-hop and self-configuring capabilities.

We should see early ZigBee products emerge in 2004, and I can imagine homes with hundreds of ZigBee devices, so there's lots of market potential. And recently there has been talk about ZigBee converging with RFID, the wireless tracking technology that Wal-Mart uses. By combining the two and making them work together in tandum, vendors could offer wireless tracking, sensing, and control in one system.

## IEEE 802.16 and 802.20 Standards (Wireless WAN)

Emerging 802.16 and .20 standards for municipal and wide area networks will be serious challengers for both fixed wireless networks (MMDS/LMDS) and mobile networks (2.5/3G). And with these new technologies, wireless could also compete with cable and DSL services for voice, data, and entertainment apps. Let's look at how these different technologies stack up.

### *MMDS (point-to-multipoint)*

Multichannel multipoint distribution service (MMDS) uses licensed spectrum in the 2.1 to 2.7 GHz range and is designed for line-of-sight communication, meaning there must be a clear path between each antenna. This restriction and the high cost of licensing spectrum has limited MMDS to specialized commercial applications, even though it supports speeds up to 10 Mbps over distances of up to 30 miles. In my opinion, the line-of-sight requirement makes MMDS a poor choice for offering broadband services to consumers.

### *LMDS (point-to-point)*

LMDS also is unsuitable for residential broadband services since it is point-to-point and requires a directional antenna. That's because LMDS operates at much higher frequencies (24 GHz, 28 GHz, and 39 GHz) to deliver speeds ranging between 150 Mbps and 620 Mbps. LMDS is primarily used between cell phone towers and central offices.

### *802.16 (WiMAX)*

802.16 is an emerging standard that should be completed sometime this year and has real potential for last-mile access and consumer broadband services. Compared with LMDS, it operates over greater distances, supports a variety of deployment architectures, and takes advantage of a broader range of frequencies that spans from 2 GHz to 66 GHz and includes both licensed and unlicensed bands.

At lower frequencies, 802.16 doesn't need a line-of-sight path to work, and that's a big advantage. The roof of your home may be too low for line-of-sight service, but 802.16 lets carriers offer wireless broadband anyway. 802.16 will be especially beneficial to consumers and communities that can't get broadband today. It can support a bundle of voice, data, and entertainment services and adds new competitive choices for consumers with cable or DSL service.

WiMAX, the consumer name for 802.16, can cover 30 miles and support multiple channels of tens of megabits each, compared to Wi-Fi networks that only extend up to 300 feet. Subscribers that share a single 70 Mbps channel will likely see that subdivided into symmetrical bandwidth matching T-1 speeds (1.5 Mbps). The symmetry means upstream transmissions can be as fast as downstream ones, a distinct advantage over cable and DSL.

An extension of the WiMAX spec, called 802.16a, will be ratified in 2004 and add mobility with the ability to roam between access points.

### *802.20 (mobile broadband)*

Think of 802.20 as mobile broadband wireless access (MBWA), with the potential of replacing 3G cellular networks that were designed and optimized for voice apps with more capacity for more subscribers.

802.20 will bring global mobility and roaming capabilities to data applications, including voice-over-IP (VoIP) with its low-latency requirements. Just as with cellular networks, 802.20 connections are handed off from one access point to another as you drive, but this standard offers much greater performance and less cost due to its ability to use unlicensed spectrum.

In an extreme test of rapid handoff, data rates of 1 Mbps were sustained while driving at highway speeds of up to 150 miles per hour.

### *2.5G, 3G, and 4G Cellular*

First generation (1G) cellular used analog circuit-switched networks. 2G added digital voice encoding and data capabilities at 9.6 Kbps or 14.4 Kbps. A problem with 2G in the United States was competition between three incompatible standards: CDMA (Code Division Multiple Access), TDMA (Time Division Multiple Access), and GSM (Global System for Mobile Communication). This contention put our nation several years behind the Asians and Europeans who more easily adopted 3G technologies. A roadmap to 3G now exists for each of the American standards, and the half step toward getting there is often called 2.5G.

Packet-switched 3G networks can use a range of frequencies and support simple data apps at speeds up to 2 Mbps when stationary, 384 Kbps when moving slowly (walking), or 144 Kbps when driving in a car.

4G is a conceptual term that describes a future convergence of cellular networks and WLAN, supporting a rich mix of data, voice and video over Internet Protocol version 6 (IPv6). 4G will likely rely on smarter antennas and software and multiband radios for speeds between 20 Mbps and 100 Mbps while moving.

### Agile, Multimode Radios offer Flexibility

With such rapid change in the wireless market, you should look for products that can be upgraded and support multiple standards. That way, future QoS, security, and performance enhancements can be added as firmware upgrades instead of product replacements.

Multimode 802.11a/b/g products automatically associate with the strongest signal and the fastest speed available, making it easy for you to move between an office network using 802.11a at 5 GHz, a home network with 802.11g at 2.4 GHz, and 802.11b in a public hotspot, all without swapping out network adapters or changing configuration settings. Multimode also lets newer devices work with older ones, albeit with compromises in speed and features.

The next trend in agile radios is to differentiate between 2.4 GHz and 5 GHz networks and also support 1.9 GHz mobile phone networks with the ability to keep a connection active while moving from one network to another. That will give you Internet access even while you're away from your enterprise or home office and away from public hotspot – like at your customer, at a bus stop, or anywhere you get cellular coverage.

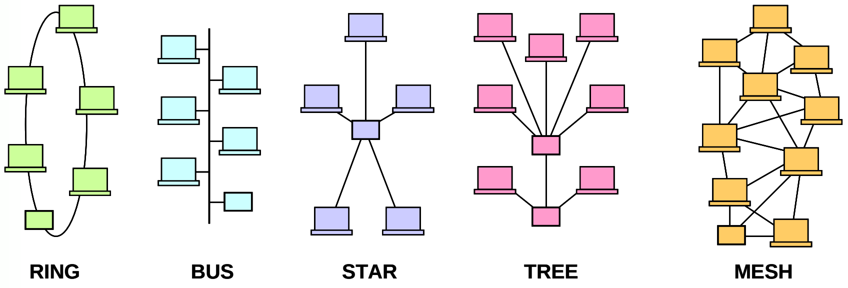
Multimode wireless is becoming a standard feature of all notebooks, and the trends will carry into desktop PCs and consumer electronics products this year. Intel, which holds about 80% market share in PC microprocessors, has had a big impact on notebook configurations with its low-power Pentium M and its Centrino chipset, but Centrino only supports 802.11b today.

Intel will add multimode (802.11a/b/g) support and introduce a similar chipset for the 120 million desktop PCs produced each year. Intel's new desktop chipset, codenamed Grantsdale, will feature Mesh topology that turns each PC into a wireless access point. These significant moves will help make Wi-Fi as ubiquitous as Ethernet and will help Intel dominate the Wi-Fi chip market.

### Mesh Topologies extend Range and improve Performance & Security

Mesh Routing is a new, self-adjusting and self-healing topology that extends range, reduces interference, improves security and performance, and lowers costs by requiring fewer access points. Each device only transmits enough power to reach adjacent devices instead ones far away. Performance is improved because there's less attenuation over distance, and security is improved since signals don't transmit as far.

NETWORK TOPOLOGIES



Mesh is not yet popular in notebook PCs since precious battery power must be used to retransmit signals for others. Users also worry about security when someone else's network traffic goes through their PC, especially when it's a stranger in the same public hotspot. These concerns vanish, however, in enterprise offices where people know each other and use desktop PCs.

Mesh also has promise in deploying wide area wireless networks. An electric utility can install access points on light poles and have them share one broadband connection, with the poles providing height and electric power. The access points could even be solar powered, so no wired infrastructure is needed beyond the first broadband connection – a great solution for developing countries.

### *Powerline & Coax Signal Repeaters also extend range*

Just as Mesh networks let adjacent PCs extend the range and function as wireless signal repeaters; repeaters can also work on wired networks.

A Panasonic demo at CES showed three HDTV video streams being sent simultaneously between A/C outlets in a home. They were using a prototype version of HomePlug-AV, an emerging standard for high-speed audio/video applications over the 110v powerline with speeds up to 170 Mbps and with full QoS support. These characteristics are especially impressive when you consider the "noise" injected by electric motors, fluorescent lights, and air conditioners. Even if the available bandwidth varies at different outlets or fluctuates over time, powerline still makes a good backbone for extending the range of wireless networks.

Coax can also be a backbone for extending range. The Multimedia over Coax Alliance (MoCA) presented new work at CES designed to let TV programs, data, and voice applications share the same coax cabling.

## More Spectrum leads to more Capacity

The FCC is happy to see that unlicensed spectrum has caused so much innovation, and it is opening up more spectrum space for general use. Much of this is tied to HDTV and FCC plans to reclaim spectrum used for analog TV broadcasts. That won't happen until sometime after 2006 when 85% of homes can receive digital TV signals over the air.

Other countries are already freeing up spectrum. Germany recently took back spectrum in Berlin by subsidizing the cost of converter boxes for low-income families, and South Korea is another particularly interesting example.

The Korean government plans to allocate more than 100 MHz of spectrum for their "Portable Internet" project, but that's just part of a very deliberate "Broadband IT Powerhouse Vision" that calls for ubiquitous broadband access of 155 Mbps to 5 Gbps by 2005.

## Better Digital Compression lets us send More Exciting Content

Digital networks that carry a mix of signals – beyond just voice, music, or television – help eliminate redundancy and dead space – redundant networks, TV channels that no one is watching, and the idle time when no one is talking on the phone or the space between words. Once content is in digital form, it's easier to compress and decompress (codec), eliminating further redundancy and improving the ability to send more information across a given network.

Compression can either be "lossless," as required for most data applications, or "lossy," which is OK for pictures, music, and video where users may not even notice a difference. Increasingly powerful processors, driven by Moore's Law, help improve the compression algorithms, and that in turn helps wireless networks carry more interesting content.

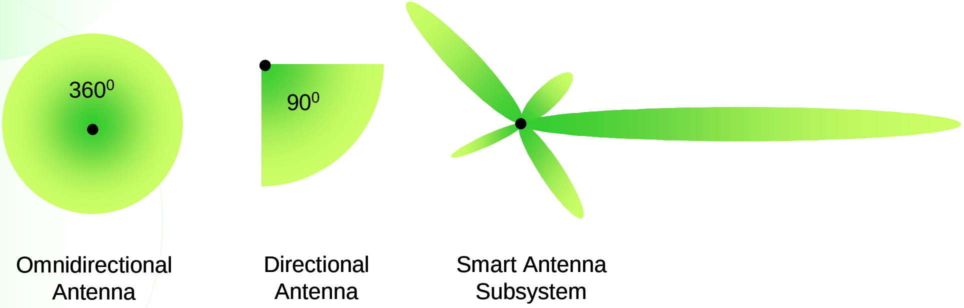
To see the impact of video compression, just look at MPEG-4, a relatively new codec for video. It needs far less storage and bandwidth than the older MPEG-2 format. Rather than demanding 3

Mbps for DVD-quality video, MPEG-4 gets nearly the same quality at just 750 Kbps – a huge savings. And rather than 20 Mbps for HDTV, MPEG-4 needs only 2-3 Mbps.

### Smarter Antennas extend Range, conserve Power, and improve Security

Where omnidirectional antennas radiate energy in a $360^0$ pattern like ripples in a pond when you throw in a stone, directional antennas focus that energy more narrowly like a cheerleader's megaphone that focuses her voice and helps it reach longer distances. Directional $180^0$ antennas are useful on the outside walls of buildings when aimed inward, and $90^0$ antennas are good for corners. Even more narrowly focused models are good between two buildings: point-to-point.

COVERAGE PATTERNS



Smart antennas are derivatives of the directional antenna conept. With technically called MIMO (for multiple input, multiple output), smart antennas greatly improve range and bandwidth capacity, sometimes extending more than 100 times farther than omnidirectional antennas. They use digital signal processing and an array of two or more antennas to adjust the focus and shape of transmissions.

Think of smart antennas as narrowly focused directional antennas that can "spin" around electronically and aim at each user in turn. Some of them can also adjust transmit power as they spin. It's like talking to someone close by for one millisecond and someone far away the next. There's no need to yell when they're close and you can whisper instead and make it hard for others to hear. Smart antenna systems also conserve power and improve security.

### Number Portability increases Competition and talks of Consolidation

Local phone companies have noticed that consumers are starting to replace their local service with mobile phone service, and recently the FCC ruled that consumers must be allowed keep their phone number when changing services. Now both local and wireless carriers are running scared, improving their networks and customer support, extending service plans, and stepping up their marketing.

The latest Number Portability ruling is an extension of similar requirements imposed on local phone companies as part of the Telecommunications Act of 1996, and it includes the ability to keep the same number when switching between local services and mobile services, not just between two local services or two different mobile services. Since Congress and the FCC are still studying VoIP and whether to apply any rules from traditional phone service, don't be surprised if they extend number portability to cable companies and VoIP as well.

#### *Wireless Carriers are Prime for Consolidation*

Industry analysts predict that the six big national carriers – Cingular Wireless, AT&T Wireless, Nextel, Sprint PCS, Verizon and VoiceStream – will consolidate into to four or five bigger players. I also expect mergers between wireless and DSL or cable companies. Any one of several factors could be the catalyst that causes a consolidation firestorm.

- Stock prices of wireless carriers have fallen along with the rest of the telecom sector, helping to spur talks of consolidation among carriers.

- Wireless subscribers are growing slowly as carriers face new competition and are forced to react to new FCC rules regarding Number Portability, and that has caused price wars that make it harder to turn profits.

- VoIP creates new service opportunities and opens new markets, but it lets in new competitors and obsoletes old networks.

- Carriers face the costly task of enhancing their networks to support next-generation services and hope new revenues justify this investment. They are looking for ways to hold down those costs.

- Standards-based technologies that use Internet protocols and license-free spectrum are less expensive to deploy, reducing the cost of entry and offering more capacity.

- Nextel has been acquiring spectrum licenses at bargain basement prices and was the highest bidder for WorldCom's spectrum. At the same time, the FCC plans to open up more spectrum, much of it license-free.

- The latest rumor is that Cingular Wireless is in talks to acquire AT&T Wireless, and more bidders are emerging, including NTT DoCoMo from Japan.

- Since Cingular is partly owned by BellSouth and SBC Communications, a merger with AT&T could also prompt consolidation among RBOCs, long-distance carriers, and even cable MSOs.

- Local phone companies are squeezed by cable telephony on one hand and cellular competition on the other. Over 10 million U.S. consumers have already replaced their local phone service with wireless, and in markets where cable companies offer voice services, they've grabbed up to 25% from the Baby Bells.

- Phone companies bet heavily on the ability to squeeze more bandwidth out of old copper wires, but DSL is hampered by limited range. Telcos also face a downward spiral of high per-user costs, few customers, and little new revenue opportunity.

- Replacing copper phone wires with fiber is expensive and hard to justify, so companies like Verizon are testing wireless in the last mile with an eye on mobility too, and with their fiber interests focused on new neighborhoods where there's no infrastructure yet.

- Telecom lobbyists are busy with politicians, but they may become less influential as these policy makers begin to worry that our nation is losing its technological leadership to countries with more aggressive broadband policies.

- The Wi-Fi hotspots built by community groups in Austin, New York, San Francisco, and other large cities or small municipalities are largely for free use by the general public. How do you compete against "free?" Carriers want ways to minimize or share their risks as they experiment with new business models.

### Wireless Future-proofs Homes

As I started this paper and pondered the implication of new wireless technologies, I reflected upon my first HomeToys article, *"Future-Proofing Your Home: Is it Possible?"* and I found that many of my original observations remain true today.

4. Lifestyles will change. As kids grow older or go off to college, you may want to reclaim a bedroom as your home office, but that may mean you need more power outlets and a broadband connection.

5. New device types and applications will appear. Multi-handset cordless phone systems let you put handsets anywhere there's a power plug. Wireless will soon let you hang the flat TV screen on the wall without wires showing.

6. Ordinary devices will get smart and networked. Smart doorknobs with fingerprint recognition that eliminates the need for keys (they showed one at CES). Networked appliances and wireless sensors, actuators, and interactive toys based on ZigBee. Don't forget the smart toilet? Panasonic sells one in Japan that includes a heater, bidet, exhaust fan, and dryer. It also recognizes you by your weight and body fat, chemically analyzes your output, and sends the results to a health monitoring service.

7. Residential Gateways will enable convergence. By bridging between different media, gateways allow an easier migration from legacy analog services and devices to digital so you don't have to replace everything at once.

8. Technology will come to the rescue. It's often impossible to imagine the impact of scientific and technical innovation, government regulation, or changes in economic conditions, fashion and social interaction. But engineers love a challenge. That's why I'm convinced that technology will evolve to address any market need. In the context of this paper, that means "wireless" technology.

***Wayne Caswell is a home systems visionary, pioneer, and change agent with over 30 years of experience applying computer systems, marketing and strategy to solving business problems and building new markets. He is also founder of CAZITech Consulting, an Austin, TX firm serving broadband, wireless and home network markets with marketing related services. Contact him at wcaswell@cazitech.com or 512-335-6073.***