SCANNERS

SHORTWAVE

THE URBAN DX'ER

Vol.7 No.2
February - March, 2002
NYDXA@Hotmail.com

Established 1984

APOLOGIES and COMMENTS!

Many readers contacted me, fearful that their names were taken off the mailing list for this newsletter. Late January and early February had me running crazy at work. In my position, this time of year finds me evaluating various consumer electronics products you'll probably see next Christmas. This, coupled with the fact that I didn't receive too much input from listeners. The February issue would have been about 2 pages. Occasionally this scenario presents itself and we decide to combine two months into one issue.

So while I'm on the podium I'd also like to respond to some comments that were passed following one of our nets. The station initiating the comments suggested that our weekly net existed solely for one purpose... to collect and feed information to Warren Silverman and his publication "Scanner Master." What wasn't made very clear is that this person's primary agenda was to publish his own frequency directory.

To those of you who have been participating in our net for the past several years, it's certainly no secret that we exchange tons of information with Warren, as he also does with us. The sole purpose of the net and the newsletter is to SHARE scanner and radio related information with all those who share our enthusiasm for this great hobby. Any information which Charlie and I receive is shared equally, without any "favoritism". Political nonsense has no place in this group. We encourage any of you to share the newsletter and net discussions with your friends. Enough said?

WI-FI DX'ING

The wireless world is expanding faster than the media can report on all the new wireless toys that have been introduced. Scanning and the radio hobby in general have dozens of new ways to expand our wireless enjoyment. Over the past few weeks I've received a few E mails from readers, strangely all on the same subject. There's been a sudden explosion of growth and interest in wireless network devices in the Wi-Fi catagory. The NY Times recently ran two articles that I thought our readers might be interested in. How long will it take before we're DX'ing WI-FI networks?

NY TIMES
By JOHN MARKOFF

SAN FRANCISCO, March 3 - The informal Wi-Fi networks that inexpensively provide wireless Internet access are fine, as far as they go - which is generally a few hundred feet. But what happens when there are enough of them to weave together in a blanket of Internet coverage? What begins to appear is a high-speed wireless data network built from the bottom up, rather than the top-down wireless cellular data networks now being established by giant telecommunications companies. Many Silicon Valley engineers now believe that it will be possible to take the tens of thousands of inexpensive wireless network connections that are popping up in homes and coffee shops all over the country and lash them together into a single anarchic wireless network. Connections could theoretically be passed from one Wi- Fi node to another, similar to the way wireless phone signals pass from cell to cell, thereby significantly extending the wired Internet. Modeled closely on the original nature of the Internet, which grew by chaining together separate computer networks, the technology - known as wireless mesh routing - is being rapidly embraced in the United States as well as in the developing world, where it is viewed as a low-cost method for quickly building network infrastructure. If the engineers are right, the popular and inexpensive Wi-Fi wireless standard, also known as 802.11, could serve as the wedge for the next-generation Internet, enabling a new wave of wireless portable gadgets that ultimately blanket homes, schools and shopping malls with Internet access. Currently most 802.11 networks serve as individual beacons that provide wireless Internet connections to portable computers situated within 200 feet or so of an 802.11 transmitter. What wireless mesh routing offers is the promise of a vastly more powerful collaboration driven by the same forces that originally built the Internet. "The good news is that broadband wireless access will finally explode," said Nicholas Negroponte, the director of the M.I.T Media Laboratory. "The social contract is simple: you can

use mine when you are in the vicinity of Mount Vernon Street, Boston. But I want to be able to use yours when I am near you." The technology is being driven both by a gaggle of ambitious start-up companies in Silicon Valley and elsewhere and by a hobbyist movement that mimics the original Homebrew Club that led to the personal computer industry. Today, Tim Pozar and several of his friends are seizing the high ground, literally and figuratively, in a movement that could undercut the nation's cellular companies, which are investing tens of millions of dollars in top-down, heavily engineered, digital cellular networks. Mr. Pozar, a radio engineer, is a member of the Bay Area Wireless Users Group, an active band of hobbyists who have been building free networks in communities through the region. Mr. Pozar and some of his friends have quietly begun obtaining the rights to place $2,000 wireless network access stations on the mountains and hilltops that encircle San Francisco Bay. If he succeeds, the network will be a starting point for a wireless data network that could eventually spread all over the Bay Area. Significantly, what will set Mr. Pozar's planned Sunset Network and those like it apart from the commercial cellular networks now being constructed at great expense is that they will "self assemble" - expanding from one neighborhood to the next as individuals and businesses join by buying their own cheap antennas that either attach to the wired Internet or pass a signal on to another wireless node. Mr. Pozar has even come up with a new acronym to describe his plan. In addition to the existing terminology of LAN's and WAN's - local and wide area networks - he is proposing the idea of NAN's, or neighborhood area networks. The so-called Nanny Networks are rapidly becoming the hottest thing in Silicon Valley and internationally. There are now at least 19 companies developing proprietary wireless mesh routing technologies, all trying to replicate the original Internet in a wireless form. It is not an easy task because the companies are engineering for a new kind of design, with which they must route data packets over paths where network nodes constantly pop up and disappear. Moreover, wireless networks must overcome an array of environmental obstacles that do not plague wired networks, including hills, rain and trees. Such networks, however, do have the critical advantage of economy of scale. In contrast to the cellular data networks, in which every customer is an added cost, in some respects in wireless mesh networks the more users who join the better the network performs. In the jargon of Silicon Valley, wireless mesh routing is potentially a "disruptive technology," a new technology that is likely to upset the existing order by using the same powerful economics of cost and scale that initially drove the growth of the commercial Internet. Already, companies like Mesh Networks, based in Maitland, Fla., are selling systems of wireless routers, making it possible to create self- assembling and self-healing networks that would cover an urban area. There are also companies like Boingo Wireless and Sputnik, which focus on software and services that make it possible for wireless users to roam among networks. Similar technologies were crucial in the development of the original nationwide analog cellular voice networks. In Silicon Valley, companies like Skypilot Network, FHP Wireless, Ultradevices, CoWave Networks, SRI's Packet Hop and others are all developing networks that have the potential to weave together networks made up of wireless antennas. "We're going to start seeing more mom-and- pop Internet service providers buying access points that will support 802.11," Mr. Pozar said. "At first I thought it was going to just be geeks doing wireless, but now everyone has one of these things deployed."

NY TIMES
By AMY HARMON

When David Sarno moved to a new apartment on the Upper West Side of Manhattan recently, he learned he would have to wait several weeks for the phone company to install a fast Internet connection. But after opening his laptop, he discovered with a surge of delight that he was already able to check his e-mail and call up Web sites at lightning-fast speeds. Someone nearby had Wi-Fi, the technology behind the short-range, inexpensive and often unsecured wireless networks that are rapidly sprinkling the nation with sweet spots of airborne high-speed Internet access. "Thank God for my neighbor, whoever he may be," said Mr. Sarno, 29, who has taken advantage of similar serendipitous connections from a hotel room in Cambridge, Mass., and a street corner in downtown Manhattan. For Internet enthusiasts, Wi-Fi is manna from heaven. The technology - known in engineering parlance as 802.11 - has been around a few years. But with a recent proliferation of wireless data networks in homes, businesses and public spaces, growing numbers of people who have properly equipped laptops now find themselves able to tie into the Internet on the run, courtesy - knowingly or unknowingly - of someone else. From business travelers to a new breed of bandwidth hackers, people are surfing the Web and collecting e-mail at airport lounges, coffee shops, park benches and bed. "Wi-Fi sort of came out of nowhere," said Tim Bajarin, president of Creative Strategies, a technology industry consultant. "But it's growing like

wildfire." Wi-Fi, short for wireless fidelity, works a lot like a cordless phone. The D.S.L. or cable Internet line, instead of connecting directly to a computer, is plugged into a small radio transmitter. Any computer with a receiver in a radius of about 300 feet can potentially pick up the signal. Many of the free rides these days are the result of bandwidth bleeding from private networks that are intended to let their owners connect to the Internet without being tethered to a fixed spot in a home or office. Because the great majority of these wireless networks have not been secured, it is easy for neighbors and passers-by to use them undetected - although if enough freeloaders download large enough files, legitimate users will notice their own connections are been degraded. The popularity of 802.11 has also begun to inspire the construction of networks that are intended to be shared, either free or for a fee. "It's a fantastic thing," said Simon Skelly, who recently hooked up a Wi- Fi network to the high-speed Internet line in his apartment in the West Village in Manhattan so he - and anyone else - can work from the two cafes down the street. "It would be great if we could get the majority of Manhattan covered." Mr. Skelly is one of several hundred wireless enthusiasts across the country who have listed the locations of their Wi-Fi networks on a Web site called freenetworks.org. One of the site's supporters, a nonprofit group called nycwireless.org, recently persuaded the Bryant Park Restoration Corporation to jettison a plan to provide Internet cables in a small area of the park, in Midtown Manhattan. Instead, the restoration group will finance the installation of an 802.11 network designed to bathe the entire park in bandwidth this summer. "We thought it would make people want to stay in the park," said Daniel A. Biederman, executive director of the restoration group, a private organization that oversees the park. It may well do that. At the University of Akron, Internet use spiked to three times its previous level when the school installed Wi-Fi transmitters throughout the campus over the last year. In San Francisco, community- minded entrepreneurs have set up a wireless "cloud" over parts of the Presidio, which residents and visitors can use free. And Tallahassee, Fla., has perched 50 Wi-Fi transmitters on street lights and traffic signals in a five-block area around the State Capitol complex. For now, legislators and others in the area have free access, but the city plans to charge for the service eventually. The wireless buzz is being driven largely by the plummeting price of 802.11 equipment. Wireless network cards that slip into laptops now cost less than $90, and many new computers come with the technology built in. Wi-Fi transmitters cost less than $150, half the price Apple Computer (news/quote) initially charged for its AirPort model - one of the first to market - in late 1999. Antennas that can extend a network's average range by several miles can be bought for as little as $40. Moreover, because 802.11 networks send data over an unlicenced slice of the radio spectrum, there are no additional fees for the transmissions once the equipment and wired Internet connection have been paid for. That has led to some of the more ambitious plans to create extended access areas. The unwelcome competition is one reason the telecommunications industry, which has paid billions of dollars for spectrum licenses to provide various wireless services to consumers, has concerns about the popularity of Wi-Fi. Several of the major cable and phone companies that provide high speed wired connections to the Internet say customers are violating their service agreements - and perhaps breaking the law - by letting others outside a given household piggyback using 802.11. "Anyone who is using it that way would basically be stealing," a spokesman for Time Warner Cable said of those who patch into its Road Runner cable modem service. "It's the same thing as cable theft." Those who use cable theft as an analogy point to federal law, which prohibits anyone from receiving communications offered over a cable system unless authorized by the cable operator. But how the law will apply to the new technology has not yet been tested. Some legal experts say using stray Wi-Fi signals is like trespassing. Others say the burden of securing the network may lie with its owner, as it does with satellite broadcasters. It is not a crime to tune in to unscrambled satellite programs, but it is illegal to crack the encryption of scrambled broadcasts. For the practitioners of a new sport called "war driving" or "net stumbling," the finer legal points may be better left unexamined. With free software called NetStumbler and a small electronic global positioning device, war drivers seek to detect wireless networks and map their coordinates by walking or driving past them. Engineers at National Semiconductor (news/quote) used such a setup recently and found 800 Wi-Fi networks in a 14- mile stretch of Silicon Valley in California. More than 70 percent of them were unsecured, a number that matches those reported by less-professional surveyors in urban areas from San Diego to Salt Lake City. The nationwide map at Netstumbler.com lists more than 10,000 unsecured Wi-Fi networks, all supplied by the growing corps of security experts and "researchers" who use the software. "Whoa!" wrote one New York stumbler on the site's message boards. "Anyone see the network in the concourse in

Rockefeller Center right near the food public sit-down area?" (Yes, it works.) One student at the New Jersey Institute of Technology who declined to give his full name, said he regularly found oases of access while waiting for trains in Newark. Not at Pennsylvania Station in Manhattan, however: "The nearest connection is nearly four blocks away," he said. But for all the Wi-Fi networks that are plundered without permission, there is growing evidence that people are willing to pay for wireless Internet access. Marie Forleo, an executive coach who lives in the West Village, has memorized the hours and locations of all the Starbucks (news/quote) coffee shops in the neighborhood since she discovered last month that they provide Wi- Fi access. She has used up her 30- minute free trial and pays Starbucks $2.95 for 15 minutes when she needs to check her e-mail. "It's less than a grande Frappuccino," Ms. Forleo said. Wayport, a wireless provider that has connections in 450 hotels and several airports, including San Jose, Calif., and Dallas-Fort Worth, saw a 230 percent growth in use from the third quarter to the fourth last year. In recent months, several corporate customers have bought accounts for $19.95 a month for each user to provide employees with a way to be productive while logging longer airport hours. Sky Dayton, the founder of EarthLink (news/quote), one of the nation's largest Internet service providers, decided that there would be enough demand for Wi-Fi to start a new company called Boingo Wireless, which last month began selling a service that makes it easy for consumers to find wireless hot spots and connect to them. According to IDC, a technology market research firm, the market for Wi-Fi cards and equipment grew to $1.1 billion last year from $600 million in 1999. About 7 million > > wireless cards were sold last year, a number IDC expects to grow to 25 million by 2005. Mr. Sarno, for one, plans to set up his own unsecured Wi-Fi network as soon as he gets his Internet connection. "You share your Internet access, and I share mine," he said. "That's the whole idea."

SKING ANYONE?

Though our weather has not been too conducive to skiing many of you may do some skiing at Hidden Valley Ski area in Vernon, NJ Here's the lowdown on their communications as well as other active frequencies that may be active.

Vernon Valley Rec Assoc - **151.925**
Great Gorge Inc. (McAfee) - **154.515**
Great American Recreation Corp. (McAfee) - **151.685**
Great American Recreation Corp. (Vernon) - **151.715**
Great American Recreation Corp. (McAfee) - **463.450**
Great American Recreation Corp. (McAfee) - **464.975**
Hidden Valley (Ski Patrol) **155.220 (77.0)**
Hidden Valley (Mountain Operations) **154.540 (77.0)**
Hidden Valley (Ski Racing) **154.570 (77.0)**
Med-Alert Ambulance Service **453.125 (DPL025)**
Newton Hospital HEAR **155.340 (141.3)**
Mountain Creek (Ski Patrol) **153.635 (123.0)**
Mountain Creek (Other Usage) **153.440 (91.5)**

155.220 - National Ski Patrol System Inc. (Vernon)
155.235 - National Ski Patrol System Inc. (Vernon)
155.340 - National Ski Patrol System Inc. (Vernon)

The State of New Jersey OEM USAR Team (New Jersey Task Force One) does not use **155.325**.

We use the NJSP 800 MHz Radio System. For those of you that would like the information it is as follows.

If your trunk tracker is programmed for a Motorola Type II system, the groups below will be heard in the 400-12 group. If you program the trunking scanner for Motorola Type I these groups can be segrated into the individual talk groups listed below in ( ).

Talk group E39 (400-12) Statewide USAR Command (statewide patch)

(58288)	Rescue 1
(58320)	Rescue 2
(58352)	Tech. Search
(58384)	K-9 Search
(58416)	Medical
(58448)	Tech. Info.
(58480)	Logistics

We also use 2 Conventional 800 MHz Repeater channels if needed.

NJTF1-RP 1 **852.4625 DPL 023**
NJTF1-RP 2 **854.4525 DPL 023**
Other then the above listed frequencies we carry radio equipment for HAM Aircraft VHF/UHF, 800 MHz, Globlestar Satellite Telephone Systems, FEMA Radio Cache, JPS Communications Transportable Interconnect System TRP-1000
We are fully equipped to setup a full radio system anywhere we need to.

All NJSP USAR radios are programmed with NJ S/W MICU, EMRAD 28, & EMRAD SP, as well as NorthSTAR & SouthSTAR and the New Statewide Trauma Groups.

NJSP Division HQ activates us, via Alpha pager. REMCS is the designated communication center for the team and the back-up paging point.

Joe Burlew
NJ-TF1 Communication Specialist
UH-EMS Supervisor (REMCS)

The Urban DX'er would like to thank all those who contributed to this months issue!
Charlie - N2NOV, "R" from Bridgeport, CT, Joe Burlew,