WIRELESS MARKET CONFUSION

Kelly Kanellakis
General Manager
RoamAbout Wireless Business
Enterasys Networks

ENTERASYS
NETWORKS™

I am pretty tied up these days. I spend a lot of my time trying to keep ahead of all the competing technologies in the wireless field. Our engineers attend standards meetings and come back with the latest proposed ideas on which they brief me. Developing standards are at best a long and detailed process, and they are supposed to create a clear direction for the industry and customers to follow. Lately, however, in the field of wireless technologies the standards themselves have become quite confusing to an outside observer. The world was a much simpler place when we only had IEEE 802.11b wireless products to worry about.

So what is all the confusion about? For everyone who thought that there would be a smooth transition from 802.11b to something like 802.11a, this confusion will come as a bit of a surprise. Originally the plan was (for most vendors and customers) to move from an 802.11b technology to 802.11a technology. The new technology would give higher bandwidth (from 11 Mbps to 54 Mbps) and at the same time allow wireless data transmission to move to a less crowded area of the radio spectrum (from the 2.4 GHz band to the less crowded 5 GHz band). If this had happened smoothly, the wireless world would not be as confusing as it is now.

So what happened? Well a few things came up over the last couple of years which introduced a level of uncertainty into the plan. First, we discovered that WEP was not as secure as everyone thought. This was not an earth-shattering revelation to many people in the industry, but it did catch some people off guard. The reality is that WEP was designed only to provide the same expectation of privacy as a wired network. It can be argued whether or not WEP succeeded at even this level. A more valid concern may be how many organizations are turning on any sort of security? As part of the Wi-Fi standard (more on this later), wireless networks can advertise (literally broadcast) their network names to make them easy to find and join. This advertisement is called the SSID. The first step in providing some form of security would be to not broadcast this name. Then it would be smart to choose a name which cannot easily be guessed. Many organizations that set up wireless networks do not turn on any sort of security, and they allow the name of their network to be broadcast to anyone who wants to listen for it. The upshot of all this concern over security is that it has very quickly become a concern for enterprise clients who want to deploy a wireless solution.

To address this within the standards, the IEEE 802.11i sub-committee was formed. Their goal is to provide a standard, interoperable way to secure wireless data. In the meantime, there are a number of proprietary vendor solutions that are aiming to solve the same problem. While many of these solutions are better than nothing, they will not be as good as the standards-based solution.

The next bit of uncertainty centers on what the “next” technology should be. At last count there were ten(!) different options for wireless data transmission, outside of 802.11b. Why so many? Good question. It seems that every vendor and consortium has a different idea to solve the same basic problem—how to transport data via radio transmission, in a way that is both secure and efficient, at a high data rate. If there was only one answer, the world would be a simpler place. Unfortunately (or fortunately depending on your point of view), there are many valid ways to solve this problem. Let’s look at a few of these.

The first place to look is at the technology that is closest to 802.11b. Most people would think that this is 802.11a, but that’s not the case. A very contentious standard, 802.11g, is closer in technology to 802.11b than 802.11a is. IEEE 802.11g is based on doing a higher data rate (starting at 22 Mbps) in the same frequency spectrum (2.4 GHz) as 802.11b. If there were but one way to do 802.11g, that would make the question of this technology easier. As this point (late Nov 2001), there are three (!) incompatible ways for a vendor to provide an 802.11g solution. This means that you could potentially (some day in the future, because none are shipping right now) buy a solution to provide 802.11g from two different vendors. Both sets of equipment could conform to the 802.11g standard, but the two sets of equipment would not necessarily work together at any of the data rates past 11 Mbps. At 11 Mbps the solutions should be compatible with existing 802.11b Wi-Fi compliant solutions. This point was one of the few things that members of the standards body agreed to. Someday there will probably be a single market winner in the 802.11g race, but today it is far from certain which technology that will be.

The next set of technologies to examine are ones that, while they still exist and are being promoted, can really be considered fringe technologies at this point. They are fringe technologies from the point of view of serious consideration for the enterprise data network, because they lack many of the features that an enterprise data network requires. These technologies include the likes of HyperLAN 1 and 2, Bluetooth, Ultra-Wideband, Wide Band Frequency Hopping and HomeRF. While none of these technologies have any real presence within the mainstream, with the possible exception of Bluetooth (even that is a stretch), they are all trying to gain wireless market share. All these technologies have some technical merit, and may be a good solution in some cases. The problem is that because there are so many of them, they add to the confusion in the market. It is not expected that any of these will ever gain significant market share, although they will probably persist for a while yet.

Finally, there is the 802.11a (54 Mbps in the 5GHz spectrum) market space. This is an interesting technology because it is a standard, right? Well yes, it is a standard, but it is also a source of confusion right now. The problem is that in the time between when 802.11a became a standard in 1999 and the present, when we are actually beginning to see the technology emerge, the requirements for this technology have changed greatly. There is a greater need for security and interoperability now than ever before. When 802.11a was first accepted as a standard, none of the technology had been built or tested. Now we have discovered, based on our experience with 802.11b that we need to address some serious security concerns that are not covered by the existing standard. These concerns are being addressed by the 802.11i committee as mentioned above. While 802.11i can be used for any 802.11 wireless technologies, it is really seen as the security solution for 802.11a. The security specified in 802.11i will probably use some form of widely accepted encryption like AES or something just as strong. For 802.11a to be truly accepted as a technology to be used in the enterprise, it must include 802.11i to provide a standards-based and strong security capability. The IEEE should ratify 802.11i sometime in the summer timeframe. It will simply not be ready before this time. To implement 802.11i, technology changes must be made at the chip level. This means that any products shipped today do not and probably will never have the capability to support 802.11i.

The second major feature missing from any early 802.11a solutions is the guarantee of interoperability. Organizations really began to deploy 802.11b technology when there was an assurance given to them that what they bought was interoperable with other vendors' technologies. This is important to an organization because it means that even if they only buy from one vendor, they can always switch vendors whenever they choose to. This protects the investment they have made in the technology. The organization would not be held hostage to one company's proprietary technology. No matter how good that technology or vendor, proprietary technology is a significant business risk. In the 802.11a solution space interoperability will be promoted by the Wireless Ethernet Compatibility Alliance (WECA). This group was responsible for the Wi-Fi (Wireless Fidelity) specification for 802.11b and now has a specification for 802.11a called Wi-Fi5. The prerequisites for testing an interoperability standard, as far as WECA is concerned, is that there should be at least two chip manufacturers producing chips, and at least three vendor solutions based on these chips. The earliest these prerequisites are expected to be met is the late summer to early fall 2002. Before then, there is no assurance of compatibility, as there is only one chip vendor shipping a product today.

Another area of contention for 802.11a is in the output power and sub-bands which are used. In Europe, the HiperLAN specification has gained a level of acceptance that it does not have anywhere else in the world. One of the reasons for this is the ability for HiperLAN to throttle the amount of transmission (output) power sent by the antennae. This is important when there are other radios in the same frequency as your solution. Your solution (in this case 802.11a) needs to be able to detect these other radios and react by lowering its power output in order to keep them from interfering with each other. This has become a mandatory requirement in many European countries and in other countries around the world. Building an 802.11a solution which does not take this into account would severely limit the market it can address in the world. Many of us (vendors included) sitting in North America sometimes forget that there are different needs in other countries. From a technology point of view, it makes more sense for one solution to address as many situations as possible, rather than building a different solution for every country.

Given these limitations, the only 802.11a technology shipping now is aimed at the SOHO market where security and interoperability are not as great as a concern. In the enterprise, given the need for security and interoperability, anything that is deployed now will probably need to be replaced later on.

Finally, there is the follow-up to this early 802.11a technology. For lack of a better term, let's call this 802.11a+. This technology will include the capability to support 802.11i as well as being upgradeable to 802.11h. In addition to this, 802.11a+ will be Wi-Fi5 compliant simply by having enough variety of solutions to test against. This technology will address all of the concerns of the enterprise class organization—security, interoperability, reliability and management. This all means a longer wait for this technology, but some things are worth waiting for. It is predicted that this technology should be available in the fall of 2002.

So what should someone who is looking to deploy wireless technology today do? In times of risk and uncertainty, there is generally a "flight to safety." For this uncertain period of time in wireless development, the safe bet is standard and interoperable 802.11b technology. The best solution is one that would allow an organization to purchase an 802.11b solution today and easily upgrade it to any future wireless technology winners. Whether those winning technologies are based around 802.11a, 802.11g or some other specification, an upgradeable solution should be able to support them. By the way, by upgradeable I mean a solution where you can change a small component, and do not need to take out all the old technology to replace it entirely with new technology.

Enterasys Networks makes a product today that can provide just such an upgrade path. The RoamAbout R2 was designed to provide excellent investment protection for organizations that use it for their solutions. It has two slots built into it to accept current and future technologies. One of these slots is designed strictly for radio cards, while the other slot is a "mezzanine" card that can support not only a second radio card, but also other technologies. Other technologies for use in the mezzanine slot could be ones that would provide advanced security (VPN, firewall, IDS), advanced accounting, or something that has not even been thought of yet. These features, along with many others, make the RoamAbout R2 an excellent choice for organizations looking to deploy a wireless solution today. The RoamAbout R2 protects the investment of these organizations by allowing them to move into future wireless technologies once the dust settles.

On a closing note, remember the days when we went from 10 Mbps Ethernet to something faster? For a while, there was great confusion in the market—100VGAnylan, Full Duplex Switched Ethernet, 25 Mbps ATM, Fast Token Ring, FDDI, OC-3 ATM, and Fast Ethernet were all proposed as replacements for Ethernet. All of these technologies were standards. Eventually the market settled on one, Fast Ethernet, but not before a lot of incorrect technology decisions were made, and a lot of gear had to be discarded. Let's try to learn from history and let's not repeat the same mistakes.

Enterasys Networks

North America

35 Industrial Way
Rochester, NH 03867
U.S.A.
(603) 337-1600

50 Minuteman Road
Andover, MA 01810
U.S.A.
(978) 684-1000

Europe/Middle East/Africa

Network House
Newbury Business Park
London Road, Newbury
Berkshire, England RG13 2PZ
44-1635-580000

Asia Pacific

85 Science Park Drive
#03-01/04
The Cavendish
Singapore 118259
65-775-5355

Unit 10, 14A Rodborough Road
Beacon Business Park
Frenchs Forest NSW 2086
Sydney, Australia
61-29950-5900

Latin America

Periferico Sur No. 3642
Piso 6
Colonia Jardines del Pedregal
Deleg. Alvaro Obregon
Mexico City DF 01900
Mexico
525-490-3400

Av. Nacoes Unidas
12.551-18° floor
Brooklin
São Paulo-SP
04578-903 Brazil
55-11-5508-460

Lit. #9012921 12/01