



Wireless LAN

Peter J. Welcher and Marty Adkins

Introduction

I'm writing this at the end of July, and the weather has been very hot (Pete). Something else that's been very hot is Wireless LANs!

Circumstances have combined to make this a good time for an article on Wireless LANs. Not the least of the circumstances is a substantial contribution of words and wisdom from a partner in Chesapeake NetCraftsmen, Marty Adkins. For a long time, Marty has been the best troubleshooter I know. He's made significant contributions to some federal networks, dealing with all of LAN and WAN and wireless design, troubleshooting, and security issues. For a long time, he's been an ace at teaching the Cisco CIT Troubleshooting course, which started many current CCIE's on the Road to the Test. The usual caveat applies: Pete is writing this, and any residual mistakes are Pete's.

This article also has more than the usual quota of links. I hope you find some interesting reading among them!

Wireless Networking

We have to be careful when we talk about wireless networking, since there are many kinds of wireless networks. (Scan the tables of contents of the books matching "wireless network" on Amazon, for example.) Wireless networking includes:

- Cell phones, if you're talking data or message, perhaps 2.5G or 3G cell phones.
- 802.11x standards, including Wi-Fi: IEEE 802.11a and 802.11b.
- Bluetooth, Wireless PAN, IEEE 802.15
- HomeRF (apparently Intel dropped chip plans)
- Fixed Broadband Wireless, IEEE 802.16
- Mobile Broadband (see Cisco, for example)
- Optical Point-to-Point Wireless (Laser)

Off the top of my head, I'd probably not have thought of the last one on the list. **Oh yeah, lasers don't use wires either!** The line-of-sight trade-off for low RF emission and low-detectability makes laser communications of great interest to military. Technology like this, one would expect to see quickly in the civilian world also, unless costly or subject to operational issues.

Having said all that, this article is going to focus mostly on Wireless LANs, aka 802.11x.

The following is a list of general wireless web sites. Most have sub-pages with 802.11x wireless LAN links too.

Wireless Web Sites

CIS-Ohio State: Wireless Networking and Mobile IP
References

Wireless LAN Column

BAWUG (Bay Area Wireless Users Group)

Pages of Links

http://www.cis.ohio-state.edu/~jain/refs/wir_refs.htm

<http://www.wireless-nets.com/column/index.htm>

<http://www.bawug.org/>

O'Reilly Network, Wireless Topics (see also the 802.11 and Bluetooth links to the left of the page) <http://www.oreillynet.com/topics/wireless/>

Some sites are more 802.11-ish than others. The following table list some interesting sites more focussed on 802.11x.

Wireless LAN (802.11x) Web Sites

Wireless LAN Association

Wireless Ethernet Compatibility Alliance (WECA)

Wireless Ethernet (Wi-Fi). **Resolves to WECA, above.**

Nova Wireless (Northern Virginia Wireless)

Wispair.net aironet web site

Pages of Links

<http://www.wlana.org/>

<http://www.wirelessethernet.org/>

<http://www.wi-fi.org/>

<http://www.novawireless.org/>

<http://aironet.wispair.net/aironet/>

And the following also were interesting. Practically Networked had articles you can find by poking around. And Marty and I are both amused by all the effort that's gone into using a Pringles can as an antenna. (Really!)

Interesting Wireless Articles

Practically Networked, Wireless Backgrounder http://www.practicallynetworked.com/pg/wireless_networking_bkgrounder.htm

BAWUG (Bay Area Wireless Users Group) - Access Point Matrix http://www.bawug.org/ap_table.html

VERMANet - Pringles Can Antenna <http://verma.sfsu.edu/users/wireless/pringles.php>

O'Reilly Network: Antenna on the Cheap (er, Chip) [July 29, 2002] <http://www.oreillynet.com/cs/weblog/view/wlg/448>

Homebrew antenna shootout <http://www.turnpoint.net/wireless/has.html>

Wireless software tools (use Internet Explorer 5.5+, Netscape 4.79 doesn't like this page) <http://aptools.sourceforge.net>

And for those who like news mixed with press releases, there is the following set of links.

Wireless in the News

Network Computing Wireless and Mobile links <http://www.networkcomputing.com/core/core3.html>

Network Computing database of Wireless LAN White Papers http://techlibrary.networkcomputing.com/data/rlist?t=sys_10_34_4_2_np

IEEE Wireless News Sites

<http://standards.ieee.org/wireless/newssites.html>

What is a WLAN?

Wireless LAN is the term being used for 802.11-based wireless networks. Bluetooth is now regarded as a Personal Area Network (PAN). I'm tempted to speculate about the future of Bluetooth (much hype, less delivery, few users?), but will mostly refrain.

Just like Ethernet, a wireless LAN of course requires a network interface in your PC or host computer. The wireless networking device you connect to is a Wireless Access Point (WAP, not to be confused with the WAP protocol suite). The WAP may connect to other WAPs but in larger networks, it probably connects to your wired LAN network. For the rest of this article, we'll assume a WAP is wireless and just use AP.

Wireless LAN vs. Wired LAN

An IEEE 802.11 wireless LAN does not exactly work like an Ethernet LAN but shares some similarities. The WLAN access method is CSMA/CA where CA stands for Collision Avoidance. Notice that's not the same as Collision Detection, where all clients are guaranteed of hearing each other's transmission. With a WLAN, it is quite possible for two clients, located on two sides of an AP, to both communicate with the AP, yet not hear each other. Plus the radio medium has a vastly poorer bit error rate, around 0.1%, compared to a wired LAN rate of 1.0E-10. Hence more frames will require retransmission. All 802 WLANs employ a handshaked transmission to compensate, with the client NIC and the AP responsible for positive acknowledgment with retransmission. But this adds overhead and reduces throughput by 50-60%! A WLAN is like push-to-talk radio - it is a half-duplex broadcast access method. In this regard it is analogous to a hub (repeater) of a wired LAN, where all stations (should) hear each others' transmissions and all compete for the shared bandwidth.

Most organizations have deployed layer two switches (bridges) across campuses to provide dedicated bandwidth. In some case, the second generation of layer two switches has been deployed, with higher speeds and QoS functionality. WLANs will be a step backward. Slower speeds, half duplex, shared media. (Is that three steps backwards?) When you become unfettered from the wire, you gain freedom, but you give up something in return.

A wireless access point (AP) usually is a layer two bridge, performing store and forward of frames between a wired LAN and a wireless LAN. When we combine the hub-like nature of the WLAN, an AP is really more like the combination of a two-port bridge with a wireless hub on one side.

Since the AP acts as a layer two bridge, it should also be capable of performing Spanning Tree Protocol (STP) on both the wired and wireless sides. Note that if two APs share the same frequency channel, they will indeed create a STP loop via their combined WLAN. (The airwaves are no different than a crossover cable on the wired side!) This is one reason why APs should only be installed as part of an integrated campus design.

WLAN Standards

"Standards are a wonderful thing. That's why we have so many."

"Should I choose 802.11b - the products seem mature? But 802.11a is so much faster, yet the products are immature. Or should I wait for 802.11g in 2003, which will be backward compatible with 802.11b? And what about 802.11h, 802.11i, and Bluetooth, and so on? My head hurts!"

For the uninitiated: IEEE 802.11a and 802.11b are the current standards with shipping products. IEEE 802.11b was ratified second but has had more than a year head start in the marketplace. 802.11a is emerging but more challenging for the engineers to build. 802.11a provides higher speeds but no backwards compatibility with 802.11b. And 802.11g is "coming real soon now" and should be backwards compatible with 802.11b (but not 802.11a).

Here is a brief summary of where things are right now:

WLAN Attribute	802.11b	802.11a	802.11g
Frequency	2.4 GHz	5 GHz	2.4 GHz
Number of non-overlapping channels	3	8	3

Max speed (Mbps)	11	54	54
Real throughput (Mbps)	4-6	22-27	22-27
Interference: microwaves, portable phones, Bluetooth	Yes	No	Yes
Distance for max speed	120-140 ft.	1-2 ft.	120-140 ft.
Distance for half speed	120-140 ft.	60 ft.	??? ft.
Maturity	Very mature	Early	Pre-standard products only

Let's discuss some of these a bit further:

- Frequency/Interference - Microwave ovens and 2.4 Ghz portable phones may interfere with 802.11b. In an enterprise office environment, this is not usually a big issue. What is problematic is interference with other WAPs in a multi-tenant office building. Also, if your IT organization doesn't have APs under control, and they're being bought in ad hoc fashion, expect to spend lots of quality time troubleshooting design and interference issues. The 2.4Ghz bands are unlicensed by the FCC so channel coordination and lower AP power output (cell size) are the only workarounds. And as Bluetooth-enabled devices appear in numbers, there could be a clash since Bluetooth shares the same spectrum. Intersil, the leading WLAN chip vendor, already has a hybrid "Blue802" combination 802.11b/Bluetooth chipset. For 802.11a, there is no likely 5 Ghz interference source in a typical office, other than other APs.
- Frequency/Distance - it's hard to argue with physics. A 5 Ghz signal is attenuated more than a 2.4 Ghz signal. This makes distance far more critical for 802.11a. It also results in smaller cells and potentially more APs to service the same office space.
- Non-overlapping channels - this determines the overall capacity for a section of a building. Although 802.11b has 11 available channels, only three are non-overlapping so as to not interfere with one another - 1, 6, and 11. By carefully laying out coverage areas using a repeating "triad" of these three channels, one can maximize the total capacity in an area. But it must be done in three dimensions, not two! The eight non-overlapping channels of 802.11a are clearly superior.
- Maturity of standards and products - 802.11b chipsets are plentiful and so are products, both for SOHOs and enterprises. Prices have plummeted to the point where many laptops are now integrating 802.11b clients. PDAs and the latest cell phones now have 802.11b. And interoperability between clients and APs is quite good with the exception of security.
- By comparison, there are few shipping 802.11a products and most use the Atheros AR5000 chipset, although that has been changing in the last few months as Intersil, Lucent/Agere, Cisco, and others have begun to catch up. Moreover, chipset vendors have begun sourcing dual-mode chipsets that combine both 802.11a and .11b.
- Quite a number of 802.11b "hotspots" are commercially available in hotels, airports, and even cafes. There are entire web sites devoted to locating and sharing the particulars of free wireless access spots. So what is one to do with as the home and the traveller infrastructure fills in with 802.11b while the enterprise office is 802.11a? The combo a/b clients may be the answer, rather than carrying around two separate NICs.
- The fate of the 802.11g standard was saved in November 2001 only after Intersil and Texas Instruments compromised on a single solution. Products are not expected until late 2002 or early 2003. By then, it is expected that 802.11a products will have matured and prices will have fallen to today's 802.11b levels. But 802.11g promises backward compatibility with 802.11b. It's quite a guess whether 802.11g may offer too little, too late. But it does seem quite likely that multiple standards will proliferate. Many enterprises that are rolling out WLANs now are deploying dual-mode a/b APs, perhaps only populating the 802.11b capability/slot at first.
- Interoperability between clients and APs - with the exception of security approaches, 802.11b products are highly compatible. The Wireless Ethernet Compatibility Alliance (WECA), a vendor consortium, tests products submitted by its members and awards passing products its "Wi-Fi seal of approval". This has greatly increased customer confidence and caused laptop and PDA manufacturers to begin integrating 802.11b client capability, as well as hotels, airports, and cafes to install services. Intel has announced that its Banais Pentium 4 will incorporate 802.11b in 2003. And PC chipset vendors are beginning to integrate 802.11b into motherboards. WECA will begin Wi-Fi5 testing of 802.11a products this summer. Side note: WECA recently caused quite a stir and confusion when it decided to reclassify Wi-Fi 802.11b as "full-speed" and Wi-Fi5 as "high-speed". They seem to be rethinking this.

The wireless space standards all come from the IEEE. The nearest thing the IETF has is the Mobile IP working group. You have to pay for fresh IEEE standards (less than 6 months). The stale ones are discounted, as in free. See the Get IEEE 802 link [below](#) .

IEEE and Wireless

IEEE Standards Wireless Zone

<http://standards.ieee.org/wireless/>

IEEE Standards Wireless Zone - Overview

<http://standards.ieee.org/wireless/overview.html#802.11>

IEEE P802.11, The Working Group for Wireless

<http://grouper.ieee.org/groups/802/11/index.html>

LANs

IEEE Standards "Get IEEE 802(TM): Wireless
(IEEE 802.11) (Older 802.11 standards)

<http://standards.ieee.org/getieee802/802.11.html>

Vendor Offerings

The marketplace is rich with 802.11b products, many at very low prices. Client choices abound - some add-on, some integrated. These will continue to evolve rapidly so it is not = "c1">practical in most enterprises to dictate a particular vendor or model of WLAN client. Rather, IT can suggest what it has confidence in and can support, while insisting on interoperability. This is analogous to the wired LAN where IT selects the access/closet switches but does not dictate the NIC within a desktop, or provides a list of approved NICs.

In the selection of access points, you need to ensure the integrity of the network, by choosing the vendors and models of enterprise-class APs, and by overseeing the placement and configuration of all APs as part of the overall network design.

Individual offices or business units must not be permitted to create their own WLANs, nor connect them to the campus network, lest service outages and security breaches result. But users can only be expected to comply if the central IT group is responsive to their wireless needs, and offers (funds) service quickly.

It is important to differentiate enterprise-class APs costing \$500-\$1000 from consumer-class ones that sell for \$100-\$200. Commodity features include Wi-Fi certification, auto-rate adaptation, and rudimentary security features such as wired equivalent privacy (WEP). Enterprise APs add capabilities such as:

- Higher and variable transmission power. (Cisco uses 100mw vs. 30mw for others)
- External antennas for improved coverage (~15% greater range). (Cisco, Proxim/Lucent)
- Little throughput degradation with encryption enabled.
- Line-power via the wired Ethernet cable. (Cisco, Proxim/Lucent)
- Multi-radio chassis - 802.11b + 802.11a. (Cisco Aironet 1200, Proxim/Lucent AP-2000)
- Ease of management via console, Telnet, WWW.
- Ease of backing up and restoring configurations (TFTP, etc.)
- Troubleshooting and management features such as detailed counters, client accounting, Syslog, SNMP, timestamps, etc.
- Per-user administrator access control with range of privileges.
- Proprietary channel load balancing and AP handoff for same-vendor clients. (Cisco, Proxim/Lucent)
- Roaming between IP subnets. (Proxim/Lucent)
- Hot Standby AP. (Cisco)
- VLAN support. (Cisco in a future software release)
- Lockable case. (Cisco)
- Filtering (ACL) by protocol and port/application. (Cisco - all, Proxim/Lucent - by IP address)
- Quality of Service (QoS), needed if you plan VoIP over wireless (some people really like challenges!)
- Enhanced security features - 802.1x, IEEE 802.11i draft, proprietary extensions.

The vendors that compete in the enterprise space are Cisco, Enterasys, Proxim/Lucent. We will not make any corporate viability judgments here.

When comparing purchase costs of APs, it is important to remember that the hardware cost is a small part of the total. Installation, configuration and management, staff training, and end-user support will dominate.

Note: some industry consolidation has already begun -- Proxim recently acquired the Orinoco wireless division of Lucent/Agere. Proxim's initial intention is to keep the Orinoco name and line of APs for the enterprise space. You do need to distinguish which devices in their product line support the above features. See <http://www.proxim.com/about/pressroom/pressrelease/pr2002-06-17a.html>.

Proxim has been the early leader with its Harmony 802.11a products. Initial testing by labs, magazines, and wireless enthusiasts have shown that the clients work well in ad hoc (peer-to-peer) mode, but have anomalies and significantly-reduced throughput while in infrastructure (AP) mode. Some of this is to be expected as Proxim rushed to be first to market. From <http://www.pcmag.com/article/0,2997,s=25412&a=26048,00.asp>, "We could not achieve a stable signal at most test markers and had to rerun tests many times to get a meaningful average throughput value. Throughput consistently under 20 Mbps was not what we expected to see." For ad hoc performance of the 802.11a card, see <http://www.seattlewireless.net/index.cgi/ProximComments>,

Proxim has chosen an intriguing master-slave approach with its APs. The actual APs are intentionally dumb; they are totally configured and managed by a separate AP controller. In fact, the APs do not perform as standalone bridges; rather they tunnel all WLAN traffic over the wired campus network to the AP controller. The latter forwards the actual WLAN payload onto the wired network, while implementing any policy controls. At first, this sounds like a VPN-type approach, except that no encryption is performed over the wired portion. Proxim touts the ease of centralized management and the ability of users to easily roam from subnet to subnet. But the down side to this approach is that the AP controller becomes a single point of failure. Moreover, it creates a performance bottleneck, especially for 802.11a, where a single controller can handle only seven APs, all combined into one 100Mb wired LAN connection. This just won't scale. Proxim has been developing a "managed mode" that gives more autonomy to the AP. See also <http://www.nwc.com/1225/1225sp1.html> , and <http://www.proxim.com/support/all/harmony/technotes/tn2002-02-13.html> .

Cisco Systems entered the WLAN market through its acquisition of Aironet and has garnered considerable market share within its huge enterprise customer base. Its Aironet 350 AP and clients have received top marks in reviews of its 802.11b products, especially for stable reliable throughput at long distances. See also <http://www.pcmag.com/article/0,2997,s=25412&a=26048,00.asp> , and <http://www.nwfusion.com/reviews/2001/0205rev.html> . One obvious factor seems to be that the Cisco APs operate at 100mw instead of the 30mw power level of competing products. Cisco also has a superior built-in diversity antenna pair in its AP.

The Aironet 1200 AP is Cisco's first dual-radio chassis and provides its entry into the 802.11a product space. But the 802.11a module began beta testing in March and FCS is slated for August 2002. One reason for this is that Cisco chose not to OEM chipsets from Atheros, but to rely on its own chipset, borne from its acquisition of Radiata in November 2000. This will give Cisco a proprietary edge in the future, as it can choose to add capabilities to the chipsets, rather rely on what is available from Intersil, Atheros, and others. Cisco has not abandoned its relationship with Intersil, insisting that it will continue to rely on Intersil for all 802.11b chipsets. Also, Cisco and Intersil have been partnering on an OEM reference design for 802.11g; early reports say it will incorporate Cisco's proprietary LEAP security support.

The Cisco APs offer extensive troubleshooting tools, both from a browser interface and from a text-based console or Telnet session. The text mode also has low-level debug-like commands. The packet capture and logging can be performed on a per-client basis.

Proxim/Lucent's ORiNOCO line has been a solid 802.11b contender for several years. Customers and reviewers have raved about the client's GUI tools, but haven't had nearly the same compliments for the high-end APs - the AP-1000 and now the AP-2000. The AP-2000 is Lucent's dual-radio platform for future 802.11a support, when the card is available in 3Q2002. This puts them in roughly the same time frame as Cisco. Both APs use a custom Agere chipset. Management is by browser only, although initial setup can be performed via a console port.

Cisco Wireless LAN

Some links to interesting Cisco pages:

Interesting Cisco Pages

Cisco - Cisco Aironet 350 Series Product Literature <http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/index.shtml>

Cisco - Cisco Aironet 1200 Series Product Literature <http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/index.shtml>

Cisco Small/Medium Business Wireless Solutions <http://www.cisco.com/warp/public/779/smbiz/netsolutions/find/wireless.shtml>

Cisco also has some interesting web pages for general wireless and mobile wireless. See http://www.cisco.com/warp/public/779/servpro/solutions/wireless_mobile/ to get started.

Books

The following looked interesting. No, I don't own them and have not read them. Do your own searches on Amazon if you don't like my picks!

Book

- Avoid Security Threats by Deploying 'Safe' Wireless LANs [DOWNLOAD: PDF], by Gartner (Author)** An inexpensive e-book from the Gartner (Group?). <http://www.amazon.com/exec/obidos/ASIN/B00005RZ19/> Food for management?
- Hack Proofing Your Wireless Network, by Christian Barnes, Tony Bautts, Donald Lloyd, Eric Ouellet (Editor), Neal O'Farrell (Editor)** Hey, I liked the title. <http://www.amazon.com/exec/obidos/ASIN/1928994598/>
- 802.11 Wireless Networks: The Definitive Guide, (O'Reilly Networking) by Matthew S. Gast** O'Reilly books are generally high quality. <http://www.amazon.com/exec/obidos/ASIN/0596001835/>

Cisco Press doesn't currently show any wireless matches, but I suspect you'll want to keep looking there. If nothing else, Cisco has sold a lot of wireless access points, and they're aware of that.

Conclusion

We haven't really talked about implementation and design issues, operational issues, nor security. (Some would claim "wireless security" is an oxymoron.) These are all the *interesting* (nasty!) issues in wireless. For smaller organizations, they may not be a big deal. If you've got a couple of big campuses and are facing hundreds of access points, you'd better have a scalable way to deploy, manage and secure them. And you don't want to have to go out and troubleshoot interference, spacing, and related design problems one WAP at a time.

We'll talk about some of these things in next month's article.

Dr. Peter J. Welcher (CCIE #1773, CCSI #94014) is a Senior Consultant with Chesapeake NetCraftsmen. NetCraftsmen is a high-end consulting firm and Cisco Premier Partner dedicated to quality consulting and knowledge transfer. NetCraftsmen has nine CCIE's, with expertise including large network high-availability routing/switching and design, VoIP, QoS, MPLS, network management, security, IP multicast, and other areas. See <http://www.netcraftsmen.net> for more information about NetCraftsmen. Pete's links start at <http://www.netcraftsmen.net/welcher> . New articles will be posted under the Articles link. Questions, suggestions for articles, etc. can be sent to pjw@netcraftsmen.net .

Marty Adkins (CCIE #1289, CCSI #93021) is also a Senior Consultant with Chesapeake NetCraftsmen. Marty specializes in network design and strategic advice, as well as troubleshooting. Marty's expertise includes routing, switching, ATM and wireless. Marty has taught the Cisco Internetwork Troubleshooting (CIT) course for years, using the "salvo" approach with many problems to fix. His teaching and advice has helped many down the path to their CCIE. He also used to run "instructor boot camp" and produced many fine Cisco certified instructors.

8/6/2002

Copyright (C) 2002, Peter J. Welcher