802.11a Measurement Techniques and Network Issues

by Herb Petrat, Senior Software Engineer, Berkeley Varitronics Systems, Inc.

In the continuously changing world of wireless networks, new standards for 802.11 are constantly evolving. The most popular standards currently are 802.11a, 802.11b, and 802.11g.

Each technology has its own pros and cons in regards to successful network deployment. **Table 1** shows a summary of these pros and cons. Rows marked with a * rank the technologies from 1-3, 1 being the best. 802.11a and 802.11g both have a 5 to 1 edge in maximum throughput with the ability to transmit up to 54 Mb/s. 802.11b tops out at 11 Mb/s.

802.11a has an advantage of operating in the cleaner 5 GHz band which contains less RF interference than the heavily trafficked 2.4 GHz band. 802.11b and 802.11g operate in this band, which contains interference from microwave ovens, cordless phones, BLUETOOTH™ devices, etc. Some newer cordless phones work up in the 5 GHz band.

Also, the RF sensitivity for 802.11b is approximately 9 dB better than for 802.11a receivers.

802.11b equipment, being on the market the longest, is the most inexpensive of the trio. 802.11g and 802.11a equipment escalate up the price scale from the base of 802.11b. A main reason is that there is much more competition from 802.11b equipment manufacturers, thereby lowering the cost to the consumers.

802.11a equipment cost is high for a couple of reasons. First, the actual equipment is higher-priced on the market. Secondly, due to the smaller coverage distance for 802.11a propagation, more access points would be required over the same area than for another technology.

Of course, for a home office network, usually only one access point is needed to acceptably cover the average size home.

802.11b and 802.11g access points cover a greater area than 802.11a AP's. 802.11a and 802.11g allow more users to access the network than 802.11b at the same time. Finally, 802.11a does not penetrate clutter (such as office walls) as well as 802.11b and 802.11g due to the higher frequency band in which it operates.

	802.11a	802.11b	802.11g
Maximum Data Rate	54 Mb/s	11 Mb/s	54 Mb/s
Frequency Band	5 GHz	2.4 GHz	2.4 GHz
RF Interference Concerns *	1	3	3
Modulation	OFDM	DSSS	OFDM
Equipment Cost	High	Low	Medium
Coverage Distance *	3	1	1
Clutter Interference Concerns *	3	1	1
Number of Users *	1	3	1

Table 1: 802.11 Technology Summary

These are some of the major comparisons used by network administrators to make the decision on which technology to use when deploying a wireless interface into the network architecture.

This discussion will focus on the 802.11a technology and measurement techniques to verify network availability, security, and throughput. When deploying a wireless network and later maintaining it during use, several factors must be taken into account. These include such factors as:

1. The network must have complete coverage over the intended client domain.
2. The network must be at least as secure as an equivalent wired network.
3. The network must process transactions in a timely manner such that it maintains a data rate that is satisfactory to meet productivity goals.

In order to meet these requirements, a wireless network test tool is very useful in becoming a network administrator's aide in detecting and troubleshooting various problem areas.

This tool will be needed over the lifetime of the wireless network. The reason for this is that there will be constant changes in the RF environment over time. These changes are not seen in a wired network (with the exception of network load) because the environment is contained within wires and (hopefully) contains a firewall. This firewall protects against external anomalies (such as viruses) and intruders.

The RF environment WILL change, however, due to such actions as:

1. Building construction (more cubicles, less walls, etc.)
2. Cordless phone usage
3. Microwave oven usage
4. Other new sources of interference

This is where the correct test equipment becomes extremely important. The test tool we will use for reference in this discussion is the new Berkeley Varitronics Systems, Inc. YellowJacket™ 802.11a tool. This tool contains a proprietary 802.11a RF module (high-speed I&Q A/D converters, DSP, memory, and I/O) that connects to an iPAQ™ display and user-input device through the CF serial input.

Figure 1: BVS Yellowjacket™ for 802.11a

One important feature of this tool, which other test tools do not have, is the ability to do a spectrum analysis on the RF environment. It is as necessary to be able to see non 802.11a traffic in the 5GHz band to determine if the network is being compromised by interference.

Using a directional antenna, one could determine the actual direction of the interfering party. A directional antenna is also useful in detecting the location of unauthorized MAC (Media Access Control) addresses that are interfering with the network.

The unauthorized MAC addresses of a network may be trying to attack the network with a denial of service attack. This is an attack where the unauthorized addresses log into the network illegally and then create a lot of unnecessary traffic to bring down the throughput of the network.

Using the YellowJacket, a list can be set up using the MAC addresses of authorized access points and clients on the network. When the YellowJacket sees a MAC address that is not authorized, an alarm is set off, warning of a potential intruder and threat to the

BVS, Con't on pg 57

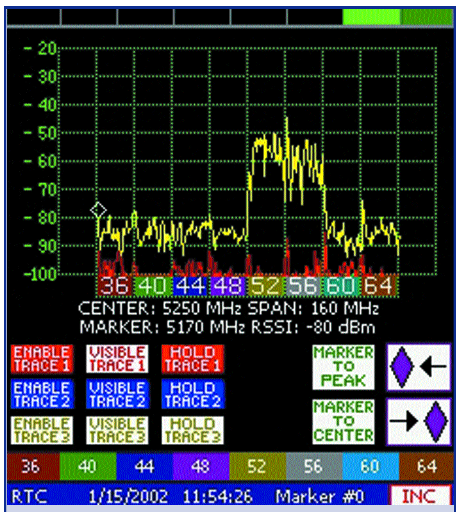


Figure 2: Yellowjacket™ Spectrum Screen

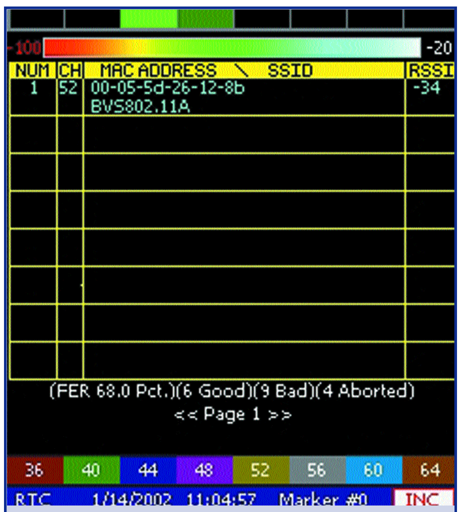


Figure 3: Yellowjacket™ AP Screen

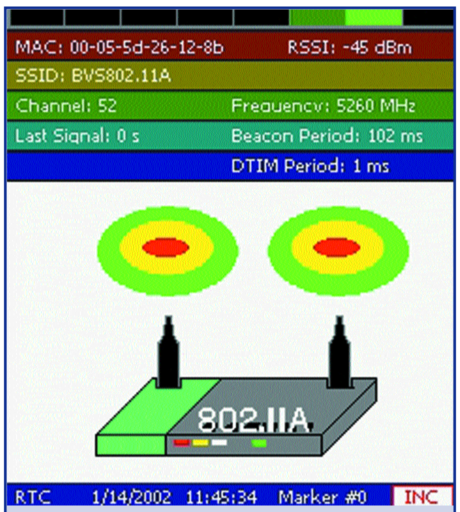


Figure 4: Yellowjacket™ AP Search Screen

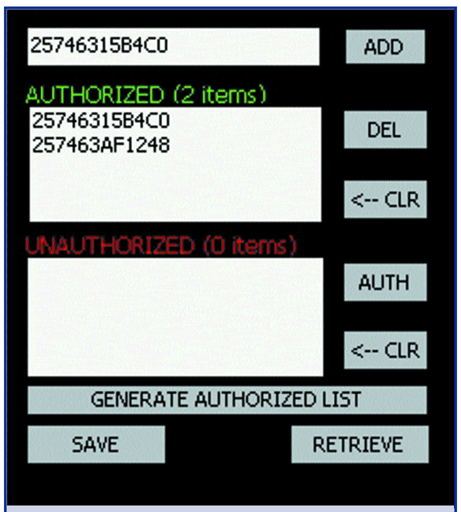


Figure 5: Yellowjacket™ Security Screen

BVS, Con't from pg 48

security of the network.

Going into the AP Search screen, the unauthorized intruder can be located with the directional antenna. By fanning the antenna back and forth, the unauthorized MAC address would have a stronger RSSI value when in the direct path of the antenna. Once the direction is found, proceeding towards the MAC address would be produce even higher readings until the user is right on top of the intruder.

A game that the network hackers play is another denial-of service attack. Two clients set up within range of the network in question. They log into their own network. They transfer high amounts of data as quickly as they can. This interferes and reduces throughput of any legal network traffic in the same area.

These culprits can be found in the same manner as the other ones. Use a directional antenna and the AP search screen to zero in on the intruder.

Performing site surveys is another important step in maintaining a wireless network.

An associated software package that is an option with the YellowJacket is BirdsEye Site Initiator, Site Supervisor, and Site Investigator. This application package performs site surveys and analyzes coverage issues in current network environments. The result is a printable color report of site coverage and interference.

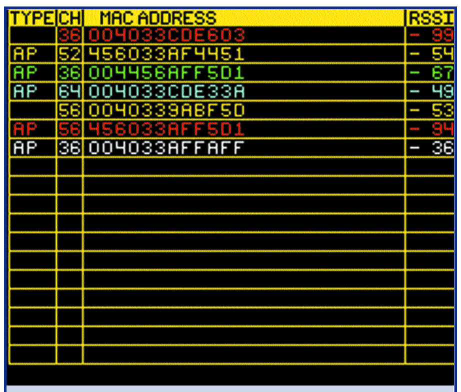
There are three applications associated with the BirdsEye™ package. The first is the Site Initiator application which runs on any Windows desktop or laptop. This program imports bitmapped floor plans for use in the site survey. Associated landmarks may be added to the drawing. These landmarks include AP's, cordless phones, microwaves, and text messages for different areas of the floor plan.

The finished site is saved and imported into the Site Supervisor application. This application runs on the iPAQ Pocket PC that controls the YellowJacket hardware. The site is pulled up on the iPAQ. Then the user walks around the site, tapping the current point in the floor plan with the attached stylus. The YellowJacket performs a quick scan of all 8 channels at each point, recording any access points that are found. The user only has to make sure that enough sample points are taken throughout the site. A good rule of thumb is taking a point every 40-60 square feet.

After the survey has been complet-

BVS, Con't on pg 60

BVS, Con't from pg 57



TYPE	CH	MAC ADDRESS	RSSI
	36	004033CDE603	- 99
AP	52	456033AF4451	- 54
AP	36	004456AFF5D1	- 67
AP	64	004033CDE33A	- 49
	56	0040339ABF5D	- 53
AP	56	456033AFF5D1	- 94
AP	36	004033AFFAFF	- 36

Figure 6: Yellowjacket™ Access Point MAC List

ed, the resulting data is transferred off of the iPAQ back onto the desktop or laptop. Here is where Site Investigator is used. This application will plot out the data from the Site Survey and prepare a visual and/or printed report of the coverage for the site in question. In the figure shown for Site Investigator, a typical analysis is shown. The different colors represent different access points.

As you can see from the diagram, access point markers were placed on the site using Site Initiator. The colors for the RSSI (Received Signal Strength Indicator) data for the associated access points get noticeably darker as they get closer to the markers of the actual location of the access points. The shade of the colors will get darker as the RSSI values increase. For example, a value of -40 dBm will result in a darker shade than a value of -80 dBm.

BirdsEye™ software with YellowJacket™ hardware combines to provide a network administrator with a tool to constantly monitor the wireless network environment. Coverage holes would show up in the resulting reports as colorless (white). Then the user could turn around and use the YellowJacket™ to determine why there is a network hole.

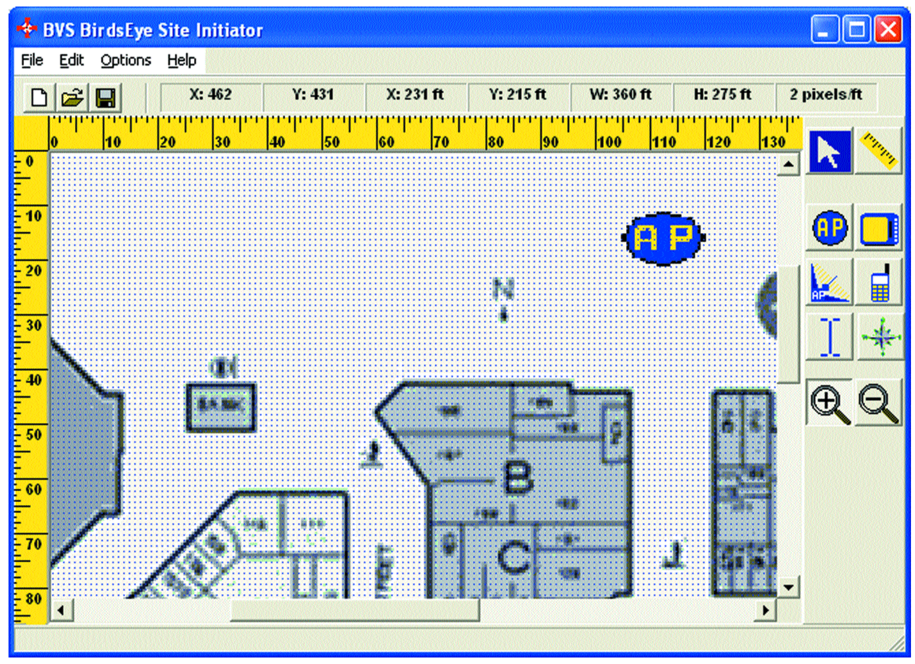


Figure 7: Birdseye™ Site Initiator

There could simply be a need for another access point. If it seems that a nearby access point should have covered the hole, outside RF interference could be the culprit. The user can take the YellowJacket™ spectrum screen to see if that is indeed the case.

There could be co-channel interference. BirdsEye™ can map the area by channel and it can be seen whether or not there are two adjoining access points that are using the same channel.

It could also be that certain clutter is preventing an access point signal from reaching the designated area. Clutter such as copper-lined walls could cause a signal to not propagate and simply reflect.

Combining BirdsEye™ with the YellowJacket™ is one of the more effective tools in the battle against constantly changing RF environments for 802.11a networks.

There are a number of issues that must be considered when deciding how and when to deploy an 802.11a wireless network for home or corporate use. A test tool such as the YellowJacket™ is extremely useful in network setup and troubleshooting and can make an IT manager's daily work less strenuous as well provide a baseline archive of a wireless network's performance.

The key is being able to maintain your wireless network amidst constantly evolving security and environmental concerns. The right test tool helps reduce the amount of labor cost involved with network maintenance.

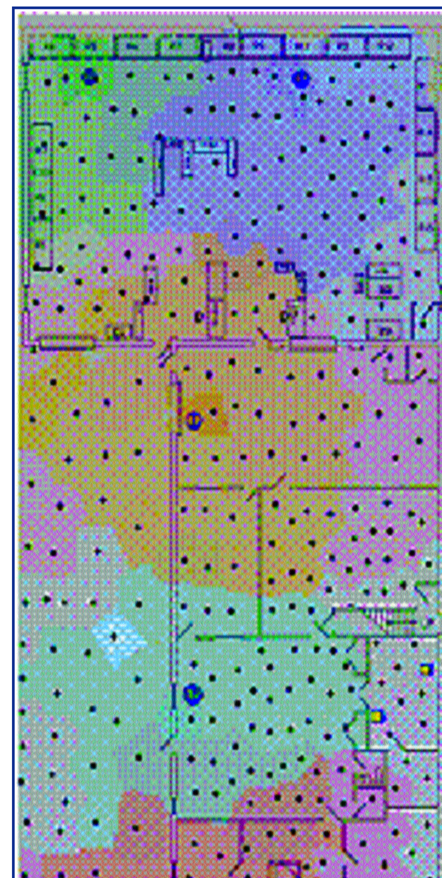


Figure 8: Birdseye™ Site Investigator

1. BLUETOOTH is a trademark owned by Telefonaktiebolaget L M Ericsson, Sweden.
2. YellowJacket and BirdsEye are trademarks of Berkeley Varitronics Systems, Inc. of Metuchen, NJ 732-548-3737 www.bvsystems.com
3. iPAQ is a trademark of Compaq Corporation

Take the W-LAN Test Challenge

A WLAN system's RF environment challenges designers, installers and administrators with planning re-use patterns, interference detection and system coverage in both installation and maintenance. These challenges are also found in seemingly more complicated cellular phone systems. Frequency re-use patterns, coverage mapping, interference from neighbors, locating unauthorized users and locating stolen equipment must be considered in addition to the standard PER and throughput metrics. Installing and maintaining a large WLAN system can rival the complexity of a cellular phone system. The author presents a comparison of equipment that is available to designers, installers and administrators to measure and overcome these challenges. Spectrum analyzers, standard WLAN cards and RF equipment specifically designed to measure 802.11 on the air are examined. Examples are drawn from the author's experience in designing WLAN test equipment; parallels are also drawn to methods and equipment that are found in the relatively mature cellular phone industry.

Introduction

The installation of an 802.11b Wireless LAN system to cover a large office setting can be very challenging and techniques found in cellular system engineering are often required. WLAN systems have the added complexity of operating in an unlicensed band where interference may not be under control of the WLAN manager, and the WLAN often operates in a harsher indoor RF environment.

Large WLAN installations will in many ways resemble a cellular phone system. Access Points (APs) are analogous to Base Stations. APs connect to the clients within their coverage area. APs have a "backhaul", Ethernet, which ties them together and into the network. Adjacent APs must be channelized so that they do not interfere with each other.

The most basic and readily available test tool is a laptop with an 802.11b card. The measurements vary with manufacturer, but the ability to measure signal strength and signal quality is common. These measurements are often relative, scaled 1–10. Specialized test tools are available that measure to traceable quantities, dBm, and have more types of measurements available. The tool or set of measurement tools should detect and measure interference, measure AP signal strength and Packet Error Rate (PER) from an AP.

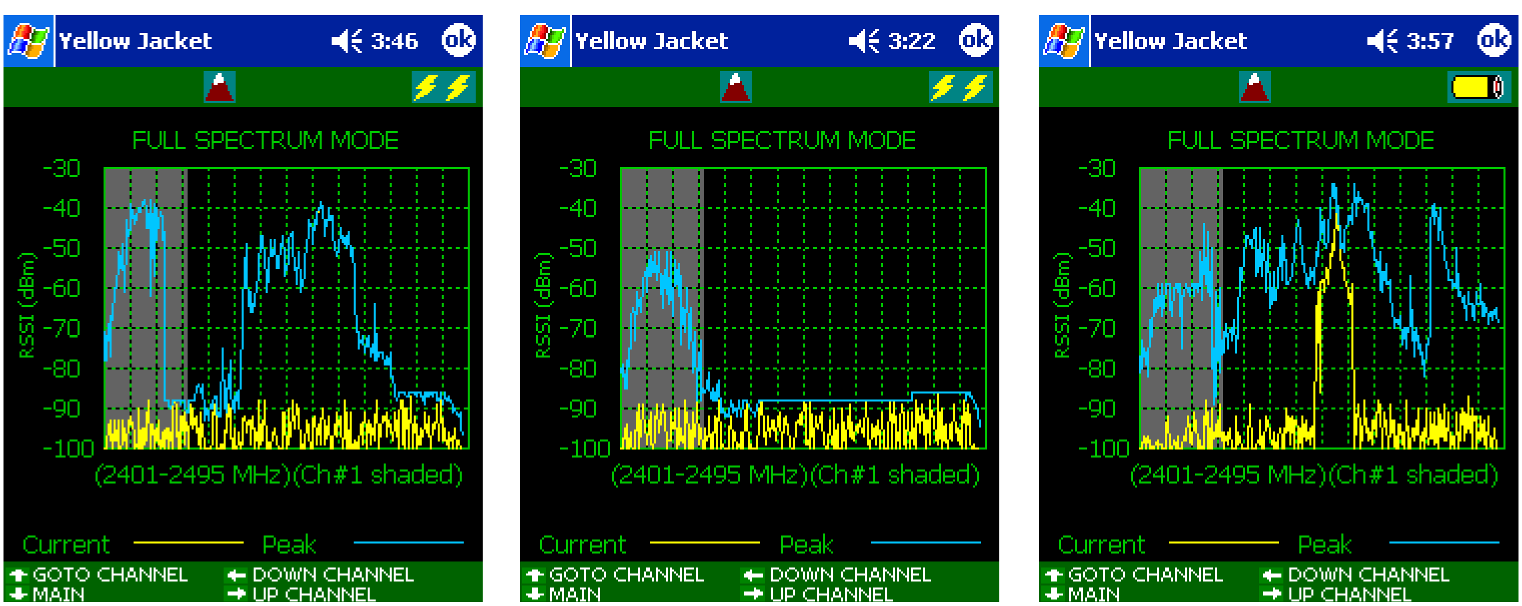
Measuring the Existing RF Environment for Interference

The place to start an 802.11 installation is to measure the existing interference. Microwave ovens, 2.4 GHz cordless telephones, other 802.11b WLANs, 802.11 frequency hoppers and bluetooth devices can all interfere with and degrade the performance of an 802.11b system.

Figure 1 illustrates a frequency sweep of an 802.11b channel with several types of common interference. A specialized WLAN test tool or spectrum analyzer is used to measure the interference and is moved throughout the coverage area of the WLAN system. A peak hold or logging of the data is essential to establish the "noise floor" that will be interfering with the WLAN in different areas. A more rigorous check would leave the instrument measuring for perhaps a day or more with data logging and then moved to different locations in the coverage area. The tool or spectrum analyzer should have a sensitivity of at least –90dBm.

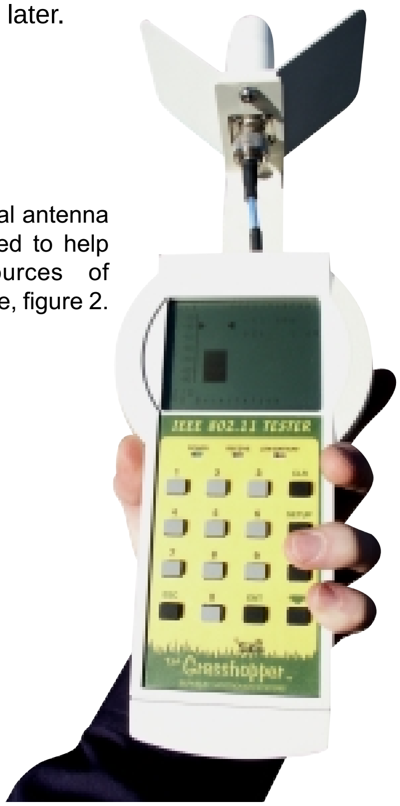
The spectrum scan detects energy present in the band from all sources and is best to scan for all types of interference. A test tool or 802.11b card should also be used to demodulate any existing 802.11b interference on the air. Testing for 802.11b interference via demodulation yields more information about these interferers and is more sensi-

Figure 1 illustrates a frequency sweep of an 802.11b channel with several types of common interference. We see a frequency hopper (left), an 802.11b access point (center) and a microwave oven (right).



tive.

A directional antenna can be used to help locate sources of interference, shown in figure 2. As many interferers should be eliminated as possible. Microwave ovens may be moved, and bluetooth devices and cordless phones can be banned from the office. Some interference may be impractical to eliminate. A neighboring business may also have an 802.11 system or some other interfere. In these areas, plan to have a higher density of APs, spend more time planning channelization and use some special techniques that are discussed later.



A directional antenna can be used to help locate sources of interference, figure 2.

Measuring the Coverage of an Access Point

The coverage area of an Access Point is experimentally found by simply locating the AP at a candidate site and measuring the signal strength and PER with a test tool. A spectrum analyzer could be used, but it can only measure signal power in the channel; and this measurement may also include interference, other Access Points other than the one being measured or even energy from a different AP on an overlapping adjacent channel. A test tool with demodulation is desirable because it can measure the signal strength of the AP coverage under test and the signal to noise is indirectly measured by the PER.

A typical signal level required for adequate coverage is around -80 dBm or stronger. This level includes some margin for typical interference and signal fading. The signal strength required will be greater in areas with interference levels greater than -90 dBm. Figure 3 tabulates typical signal strengths required with varying amounts of interference.

BER	Min Eb/No Required	Eb (Min) required for thermal noise = -100 dBm	Eb (Min) required for interference = -90 dBm
10^{-4}	10	-90 dBm	-80 dBm
10^{-5}	12	-88 dBm	-78 dBm

Note:Figures estimated from Harris HFA3861B data sheet.

Figure 3: Required Received Power (Eb) for various Bit Error Rates (BER) and Noise/Interference Levels (NO).

Measuring Coverage and Co-Channel System Interference

After testing AP coverage in several locations, the APs required for adequate coverage and overlap can be located. This may require an educated estimate or specialized propagation software. Neither method is perfect, so additional APs may need to be added or locations adjusted with testing.

Channelization is required so that neighboring APs do not interfere with each other. Figure 4 depicts a typical hexagonal frequency reuse pattern for three frequencies. For continuos coverage, APs must overlap, and the frequencies in these overlap areas should be different for each AP to avoid interference in these overlap areas.

The installation site must be surveyed to insure that all areas have sufficient signal strength, good PER from at least one AP and is without significant co-channel interference. Co-channel interference is when energy on the same channel is received from different APs. Co-channel interference should be at least 15dB weaker than the stronger AP. This survey requires that 3 frequencies be measured for a reuse pattern of 3, figure 5.

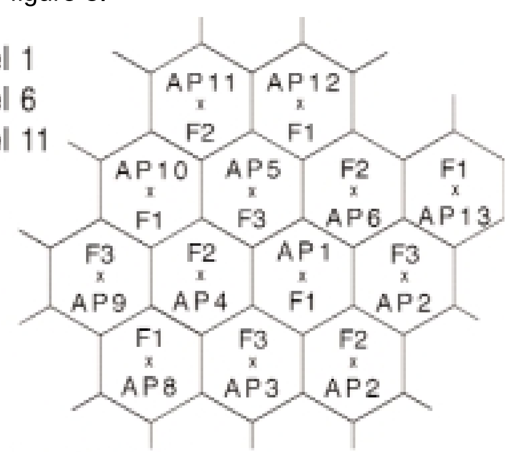


Figure 4: Coverage layout for 3 frequencies.
Three frequencies were chosen because there are only 3 non-overlapping channels available for 802.11b in the U.S.. Co-channel interference near AP1 can be received from other APs transmitting on the same frequency (AP8, AP10, AP12...).

Fixing Problem Areas

A site survey or the operation of the WLAN itself will probably reveal areas where coverage is not adequate. Adding or moving an AP closer to an area with high interference will boost the signal level. Directional antennas such as corner reflectors can direct more energy to your coverage area and reduce the amount of received interference. This is a useful technique for existing with a neighboring WLAN system; use directional antennas on the AP to direct coverage into the coverage area and to reduce interference received from outside the coverage area. A directional antenna may also be used at the client.

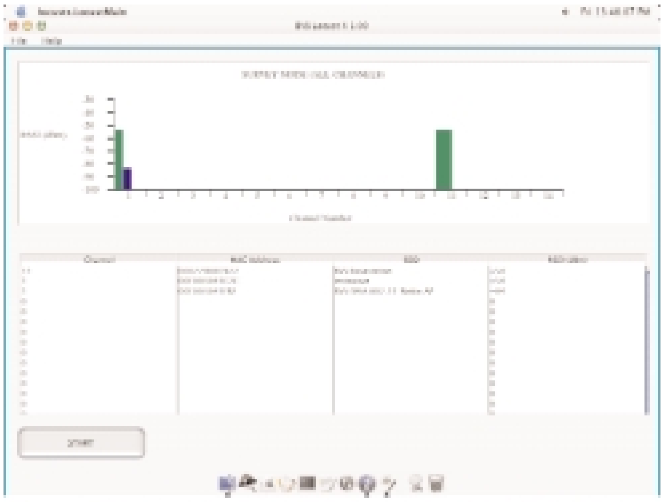


Figure 5: Site survey showing multiple frequencies and multiple APs. Note the co-channel interference on channel 1.

Keep the tools ready for Problems

Periodic checks and monitoring can avoid problems, but be prepared for a client with little or no throughput. Tools can quickly verify the RF link for signal level, PER and interference. The tools can help debug a new interfering AP a neighbor has set-up or to find the antenna that has been knocked over.

A directional antenna and receiver are very useful for locating interference or even an unauthorized user or stolen equipment. The directional set-up shown in figure 2 can be used to direction find a node with a specific MAC address.

Summary of tools and techniques

A microwave oven, a client with slightly weak signal strength or another interferer with short transmissions should not bring down the network or significantly degrade performance. The guidelines presented here are conservative, aim for them when planning and setting up a network. An outage or a drop in performance will justify the cost of WLAN RF test tools.

A laptop with an 802.11b card is a good test tool and may be adequate for small installations and maintenance of small systems where interference is not significant. For larger installations and maintenance or in areas with significant interference, a tool or set of tools with the following characteristics is recommended:

Spectrum Analysis: sensitivity at least -90dBm, with peak hold, and data logging is a plus. Best used to check for and measure interference of any type.

Demodulation Analysis: Signal strength (measured in dBm is a plus), PER, and scanning of multiple channels is a plus. Best used to measure 802.11b interference, coverage of APs, channelization and co-channel interference.

Directional antenna: Can be used to locate interference or an unauthorized user.