



## Tutorial

# How to Implement Wireless Networks

by Ken Chipps

### Introduction

#### Concepts to Understand about Wireless Networks

Planes

Polarization

Loss

Gain

Decibels

*dBm*

*dB*

Noise

*Signal-to-Noise Ratio*

EIRP

Factors That Affect Radio Wave Propagation

*Free Space Path Loss*

*Absorption*

*Reflection*

*Refraction*

*Diffraction*

*Scattering*

*The Combined Effect of Signal Loss Factors*

Regulation of Wireless Systems

*Regulatory Bodies*

*Major Regulations*

*Differences Among the Regulations*

*The Effect of the Regulations*

Commonly Used Radio Frequency Bands

*900 MHz*

*2.4 GHz*

*5 GHz*

### How Wireless Networks Work

Infrastructure Network

CSMA/CA

Speeds

Access Points

NICs

### Deployment of Wireless Networks

Selecting an Antenna Type For a Particular Deployment

*Antenna Radiation Patterns*

Site Survey Process

*Assess the RF Environment*

*Access Point Survey*

*Access Point Locations*

*Centralized Site Survey Tools*

*Do Not Bother With a Site Survey*

*Notes on Surveying*

*Verifying the Layout with Throughput Tests*

[Deployment of Wireless Networks](#)

[Access Point Naming Plan](#)

[Access Point Configuration](#)

[Access Point Mounting](#)

[Electrical Power](#)

[Physical Security](#)

[Safety](#)

[Appearance](#)

[Redundancy](#)

[Warehouse Deployment Considerations](#)

[Campus Area Network Deployment Considerations](#)

## **[Troubleshooting](#)**

[Types of Wireless Network Errors](#)

[Interference In All Its Forms](#)

[Technology Problems](#)

[Hidden Node](#)

[Near/Far](#)

[Low Throughput](#)

[Fragmentation](#)

[Network Analyzer](#)

## **[Management](#)**

## **[Conclusion](#)**

## **[References](#)**

# Introduction

This Tutorial on wireless networks expands on the CCIE-level Study Guide "[Networking Without a Net](#)" by Dennis Laganieri, adding the details on the common tasks a CCNA-level staff person would be expected to do as part of a wireless network installation. These tasks include the site survey, deployment planning, installation, and management of the wireless equipment. It is assumed that the site has already been deemed appropriate for a wireless network. All that the CCNA staff need do is properly set up the site for use.

The focus of this how-to tutorial is on a typical wireless extension to a wired local area network in an office building. Then, the differences that occur when this type of network is deployed in a warehouse are covered. Finally, the changes required when the network connection is outside are illustrated by a point-to-point campus area network link.

# Concepts to Understand about Wireless Networks

Let's briefly review a few concepts to keep in mind as the practical information on site surveys, installation, and management of wireless networks is discussed later in this tutorial. A more extensive discussion of these topics is available in Laganieri.

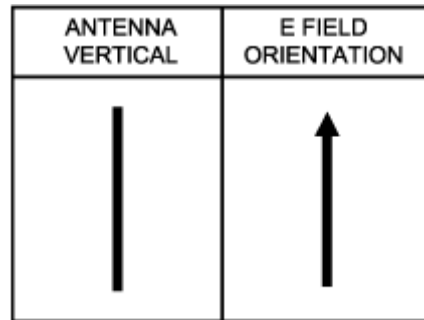
## Planes

As the Laganieri Tutorial pointed out, a radio uses radio waves to send and receive information. These radio waves are part of the electromagnetic spectrum. Electromagnetic radiation fields consist of two planes. It is necessary to understand what a plane is in relation to a radio wave front because it has an impact on the ability of two ends of a wireless radio link to communicate. These planes are:

**E Field (Electric Field)** - Exists in a plane parallel to the antenna

**H Field (Magnetic Field)** - Exists in a plane perpendicular to the antenna

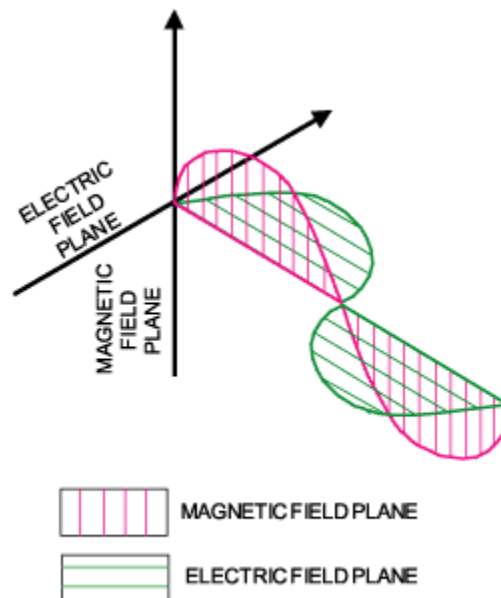
In other words, the E field lines up with the antenna. Using a dipole antenna as an example of this the E field aligns this way.



[NA-Wire-WP1-01]

## Polarization

Related to the two planes exhibited by an antenna is the polarization of the signal. Radio frequency signals are polarized. The polarization aligns with the E field. If the electric field lines are parallel with the surface, then the polarization is horizontal. When those electrical field lines are perpendicular to the surface, the polarization is vertical. The antenna type and alignment determine the polarization of the radio wave. For maximum signal strength, the antennas at both ends of the transmission must use the same polarization. This is difficult to do in a wireless local area network. However, it must be done for the longer length connection used in a point-to-point campus area network.



[NA-Wire-WP1-02]

Even if the two ends of a wireless network have their polarization perfectly aligned, signal strength is still lost due to several factors that affect the flow from the transmitter to the receiver.

## Loss

All radio links suffer from loss. This loss can be due to the parts used or the environment through which

the signal travels. Loss cannot be eliminated, just controlled.

## Gain

Amplifiers produce gain in a radio. In general, do not change or add an amplifier to a radio system you buy. There are arguments for and against this practice. I do not use add-on amplifiers. If more gain is required, the gain of the antennas -- which is different from amplifier-produced gain -- should be changed instead.

## Decibels

To measure loss or gain, a common unit is required. The decibel is the unit used. In the systems we are discussing it takes several forms.

### *dBm*

Because the decibel is a ratio between two power values, such as input and output power, another measure is needed to express power in terms of a fixed reference point. This is the dBm. This uses 1 mW (milliwatt) as the standard.  $1 \text{ mW} = 0 \text{ dBm}$ .

### *dBi*

The dBi refers to the gain of an antenna in relation to a theoretical isotropic radiator. The isotropic radiator radiates in a perfect sphere around the antenna. The radiation pattern looks like a soccer ball or basketball with the antenna element in the center. When gain in dBi is produced, it is through redirection, or focusing, of the antenna's output. This behavior is similar to a light bulb that has no reflector, outputting its light in all directions, compared to a flashlight's reflector that focuses the beam in a particular direction. The light bulb maintains its output level, but it is focused, or concentrated, in a particular direction. Antenna gain is always redirection. Only amplifiers increase the real gain in a system. Think of this perfect sphere now as a balloon. If one side of the balloon is pulled out in a single direction, the size of the balloon is not changed. It is just redirected. This is what happens when a real antenna replaces the theoretical pinpoint antenna in the middle of the radiation sphere. The different shapes and sizes of the real antenna always redirect or distort this perfect spherical radiation pattern. Therefore, any real antenna has some gain, but only in relation to the perfect radiation sphere of an isotropic radiator.

## Noise

The first of the environmental factors that produce loss is noise. Noise consists of all undesired radio signals, whether produced by humans or naturally occurring. Noise makes the reception of useful information difficult. The radio signal's strength is of little use if the noise power is greater than the received signal power. This is why the *signal to noise ratio* is important. Increasing receiver amplification cannot improve the signal to noise ratio since both signal and noise will be amplified equally and the ratio will remain the same.

Naturally occurring noise has two main sources: atmospheric noise, such as thunderstorms, from 0 to 5 MHz; and galactic noise, such as stars, at higher frequencies. Both of these sources generate sharp pulses of electromagnetic energy over all frequencies. The pulses are propagated according to the same laws as the desirable signals being generated by the radio equipment. The receiving system must accept them along with the desired signal.

The noise produced by human beings is part of modern life. It is generated almost anywhere that there is electrical activity, such as automobile ignition systems, power lines, motors, arc welders, fluorescent lights, and so on. Each occurrence is small, but there are so many that together they can completely hide a weak signal in an urban area that would be above the natural noise in a less populated area. This

is also one form of a DoS attack that may be performed on a wireless network. An attacker can intentionally transmit garbage in the same frequency range as the wireless network and, providing they do so at sufficient power, will render the WLAN unusable.

## Signal-to-Noise Ratio

The measure of the effect of the noise in the environment is the signal-to-noise ratio (SNR). If the signal is more powerful than the noise, then reception is possible. The signal to noise ratio is the difference between the signal and the noise dBm values. To compute the SNR, given values in dBm, use this formula.

$$\text{SNR (in dB)} = \text{Signal\_strength} - \text{Noise\_strength (in dBm)}$$

For example, for a signal value of -45 dBm and a noise reading of -92 dBm, subtract -92 from -45. The result is a SNR of 47 dB. Some site survey programs, such as the Cisco Aironet Client Utility may show a slightly different value.

SNR can also be calculated using the ratio of the signal and noise power levels (in Watts, for instance):

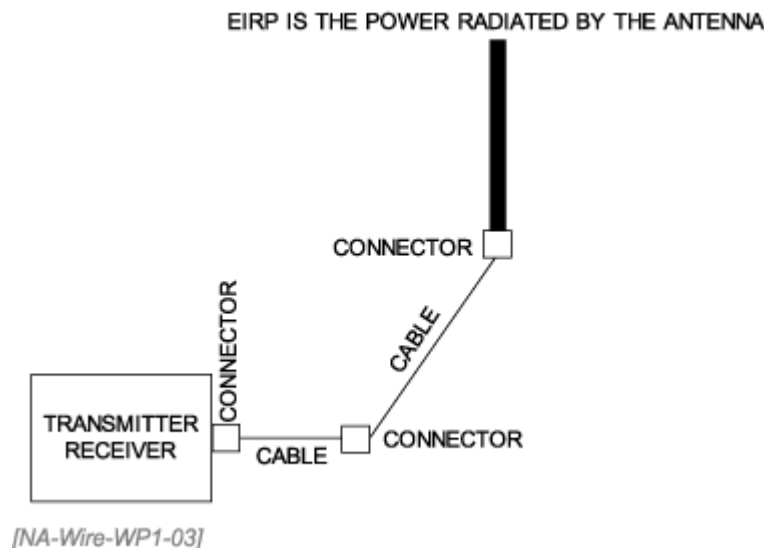
$$\text{SNR} = 10 * \text{Log}_{10}(\text{Signal\_Power} / \text{Noise\_Power})$$

Many site survey programs show the computed SNR along with the signal and noise values.

## EIRP

Effective Isotropically Radiated Power (EIRP) is the power actually radiated by the radio system. It is the product of the power supplied to the antenna from the radio and the gain of the antenna. Governmental authorities regulate this power level.

For example



## Factors That Affect Radio Wave Propagation

Keep in mind that the radio frequency environment is dynamic. In this way, the radio wave environment is similar to the weather. Just like the weather, we know quite a bit about how large

systems operate. What we cannot predict is the microclimate for a locality. This is also true of radio frequency performance. The propagation of radio waves is well understood. Exactly how these waves will or will not penetrate a particular building is not. This is the main reason for the fade margin or fudge factor. This fade margin is used below when the site survey procedure calls for a line to be drawn connecting the 20 dB SNR points identified during the survey.

As radio waves move along their journey from here to there, many things act them upon. Most of these things are not good. Everything a radio frequency (RF) signal encounters on its journey has an effect on the signal. The effect is usually to make the signal smaller or to change its direction in some way.

## *Free Space Path Loss*

The first of these impediments is free space path loss. This type of loss occurs regardless of whether the signal is transmitted inside or outside a building. Free space loss is the widening out of the signal as it moves away from the antenna. The result is lower signal strength at the receiving end of the link. Propagation loss increases with respect to both distance and frequency. In other words, higher frequency signals lose more than lower frequency signals, because the short wavelengths of the higher frequencies cannot bend around objects as well as longer wavelengths. The practical effect of this is that short wavelengths are line of sight links. This is not a consideration for the size of networks discussed here: local and campus area. However, it is a consideration for a longer link.

## *Absorption*

Free space loss is only one of the losses suffered by the signal as it goes from here to there. Absorption is another loss. It is caused by things that the signal runs into. For the wavelengths and networks of interest to us, the amount of loss experienced by a radio wave from absorption depends on the materials the wave encounters on its journey.

Inside an office building, the absorption is from the building materials, furniture, and so forth that the signal encounters. As human beings are basically large bags of water, it is assumed -- and has been reported in the trade press -- that too many humans in a space will cause signal levels to drop. My informal testing in classrooms does not confirm these anecdotal reports. However, a fairly rigorous study by Intel does show loss due to water in the path of the signal in a residential environment. This water was not in humans, but jugs of water placed between the two radios. In a warehouse, the impact of water on the signal coverage is more pronounced. For example, a beverage packaging operation I examined sees the coverage area of each of the access points in their product warehouse reduced by up to 60 percent when the warehouse is full versus when almost empty. However, it is difficult in this instance to separate the effect of the metal beverage cans from the liquid they contain. More work is needed on this topic.

In the types of systems used to create campus area connections, the main outside absorption problem is vegetation. There are no firm numbers for this problem, but some general statements can be made. The absorption is due to the water content of the vegetation and the frequency of the signal. For full foliage trees in the Northern Hemisphere, research suggests these values for the absorption effect of vegetation:

Frequency	Absorption	
	dB per meter of foliage	dB per tree
870 MHz	0.2 to 1.3	11
1.6 GHz	0.5 to 1.3	11
5 GHz	1.2 to 2	20

Studies suggest that the wood part of the tree is the major factor in tree-related attenuation at

frequencies from 870 MHz to 4 GHz. Leaves add up to 35% additional attenuation at 870 MHz, plus an additional 15% at 1.6 GHz. At 20 GHz, the wood and leaves are both important. An International Telecommunication Union (ITU) study on this subject states that the attenuation caused by vegetation varies widely due to the irregular shape of vegetation, as well as the wide range of sizes, shapes, densities, and water content of various species.

## *Reflection*

Reflection is a change in direction of the signal caused by something the signal cannot penetrate. The amount of reflection depends on the wavelength, the material the object is made of, and the angle at which the signal strikes the object. Reflection occurs when the object has a very large dimension compared to the wavelength. As most of the wavelengths used in wireless systems are very short in comparison to the objects they encounter, many things in the environment cause reflection. If the material does not absorb the entire signal, some must bounce off (i.e., be reflected). A smooth metal surface with good electrical conductivity exhibits severe reflection. Reflection appears as multipath.

## *Refraction*

Refraction is the bending of a wave as it passes through an object. It is not reflected, but mostly passes through the object. The signal that passes through goes off in a direction different from that in which it entered the object. The obstruction that causes the refraction is not always obvious. Usually both refraction and reflection occur at the same time.

## *Diffraction*

Diffraction occurs when an RF wave is obstructed by a surface that has sharp edges, such as the corner of a hall or the edge of a building. The signal moves around the object and back to the other side. But a shadowed area appears behind the object.

## *Scattering*

Scattering occurs when radio waves hit a large number of objects whose dimensions are smaller than the wavelength. In the frequencies of interest to us, common causes of this are signs in halls, foliage, and other such things found in the environment. In the wavelengths used by the unlicensed bands, many things the wave front encounters fit this definition.

## *The Combined Effect of Signal Loss Factors*

These signal-reducing factors are intermingled. There is no way to separate and isolate the effects of one source as opposed to another source when a network is deployed in the real world. This is the reason for conducting an onsite site survey. One example of the combination of these effects is seen in a test recently done to examine signal distance with an access point in a hallway versus the access point in a room with both at table height. With the access point in the hallway of the building, the signal traveled 248 feet before the signal dropped to -82 dBm. With the access point in a room, the -82-dBm point was reached after 118 feet. In these 118 feet there are four sheetrock and metal stud walls, classroom furniture, and a few people.

For planning purposes, the results of the Intel study can be used. Measurements were taken in a residential townhouse of typical construction. This study produced these values for signal loss in dB.

Obstacle	2.4 GHz	5 GHz
Wall	10.7	14.9

Floor	5.5	7.0
Water*	3.8	14.2

\*The water was 3 gallons in one-gallon jugs arranged in a triangle

In each case, signal loss was higher for the 5 GHz frequencies. Higher loss figures can be expected in an office building where metal wall studs and concrete floors are more common.

The [CWNA Study Guide](#) suggests using these figures to estimate loss in a typical office building.

Obstacle	2.4 GHz
Wall	5 to 10
Floor	15 to 25

The figures should be somewhere in between these two studies for open plan offices.

These are all just general guidelines. In the lab, this may be science; in the field, it is all art. This discussion just emphasizes the need for the onsite site survey.

## Regulation of Wireless Systems

Since the early 1900s, the use of the radio frequency spectrum has come under more and more regulation by governmental bodies.

### *Regulatory Bodies*

As might be expected when dealing with governmental bodies and their rules, there is a multitude of regulations, including:

#### **International**

ITU-R - International Telecommunication Union, Radiocommunication Sector

#### **Europe**

CEPT - European Conference of Postal and Telecommunications Administrations

ETSI - European Telecommunications Standards Institute

ECC - Electronic Communications Committee

ERO - European Radiocommunications Office

#### **Western Hemisphere**

CITEL - Inter-American Telecommunication Commission

#### **Canada**



Industry Canada

Spectrum Management and Telecommunications Sector

### **United States of America**

FCC - Federal Communications Commission

### **Asia-Pacific**

APT - Asia-Pacific Telecommunity

### **Japan**

ARIB - Association of Radio Industries and Businesses

### **Australia**

ACA - Australian Communications Authority

### **New Zealand**

Ministry of Commerce

## *Major Regulations*

Most devices and frequencies operate under either:

- one or both of the regulations created by the FCC in the United States of America under Parts 15 and 101 of Title 47 of the Code of Federal Regulations
- ETSI EN 300 328-1, ETSI EN 300 328-2, and ETSI EN 301 893 from the ETSI in Europe.

For the unlicensed bands, most countries use the requirements of either the FCC Part 15 or the ETSI EN 300 328.

## *Differences Among the Regulations*

Harmony among the worldwide rules is desirable for equipment manufacturers. It is an advantage to users as well, because wider usage generally results in lower costs. For the unlicensed 2.4 GHz frequency range, most of the worldwide restrictions have been lifted, except for a few channel restrictions and limitations to indoor use only. France, Israel, parts of Latin America, Asia, and the Middle East are the remaining problem areas.

For the 5 GHz ranges, some parts are available everywhere. The differences are what parts can be used where, such as indoors or outdoors. The World Radiocommunication Conference held in 2003 harmonized and expanded the spectrum in the 5 GHz frequency range. Worldwide, these ranges track the US usage shown below. In addition, a range from 5.470 to 5.725 GHz will be added for use both inside and outside. Depending on the ultimate use of these frequencies in actual products, this should increase the available bandwidth for devices using these frequencies.

## *The Effect of the Regulations*

There are two key points in the regulations governing the types of networks we are discussing. First, these radio frequencies are unlicensed. This does not really mean what it seems to say. By unlicensed, the regulators mean that anyone can use these frequencies for anything as long as they conform to the rules. This means that, if a neighboring system is following the rules, but at the same time it destroys the usability of your network, you can do nothing about it. Cooperation is the key to getting along in this unlicensed space. Using a licensed frequency for this type of network is not practical. The cost for the license and the equipment is too high.

The second aspect is controlling interference in this unlicensed space. The regulations specify the power levels that can be used, the way the parts are connected to each other, and the required modulation techniques.

When installing a wireless network using these frequencies, you cannot just do anything you want to. You are limited to approved radio systems. This does not mean you must use only Cisco antennas with Cisco access points. It does mean that the supplier of the antenna must have an approval from the regulatory body for that antenna and radio combination.

## Commonly Used Radio Frequency Bands

There are a limited number of available frequency bands for use in local and campus area wireless networks. All of these frequencies are unlicensed. This means that the maximum legal power is limited and interference from other systems must be accepted.

### *900 MHz*

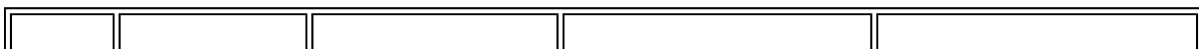
In many parts of the world, the 900 MHz frequencies are license-free in the range from 902 - 928 MHz. This total bandwidth is 26 MHz. The nominal wavelength is about 325 mm. This frequency is not currently used in the types of networks we are discussing. It was used in some early LAN equipment. It is regaining popularity in wireless Internet service provider deployments for its ability to penetrate vegetation. It is mentioned here because point-to-point campus area links may start to use it. The main problem is a lack of bandwidth. Thus, data rates are slow.

### *2.4 GHz*

The 2.4 GHz frequency range is license-free worldwide for the most part, although the channel details differ. It ranges from 2.4000 - 2.5000 GHz in the FCC scheme in the United States and from 2.4000 to 2.4835 GHz as defined by the Institute of Electrical and Electronics Engineers (IEEE), which creates standards for the use of these frequencies. The 2.4 GHz band provides 83.5 MHz of usable bandwidth. These signals are around 125 mm long. This is a fairly long-range solution, but it requires line of sight, because it does not pass through obstructions well. Water attenuation is the major problem, especially outdoors. The attenuation from trees is approximately .5 dB per meter of canopy. With a tree with a canopy of 10 meters (~30 feet), the attenuation would be about 5 dB. Just a few trees will block the signal. In the United States, Part 15 of the Code of Federal Regulations (CFR) covers the usage of this frequency. In Europe, regulation of this frequency range is covered by EN 300 328 and EN 300 826 from the ETSI. Part 15 and EN 300 328 are similar. When used inside, the IEEE 802.11b standard is the most widely deployed system. Because this frequency range is highly utilized, interference may be high.

### *5 GHz*

5 GHz systems are deployed around the world, but the allowed frequencies vary widely. For example, in the US there are four license-free subbands at 5 GHz, although two of these bands overlap each other. There is one Industrial, Scientific, and Medical (ISM) band from 5.725 to 5.850 GHz. There are three Unlicensed National Information Infrastructure (UNII) bands.



	Range (GHz)	Use	FCC Max Power (mW)	IEEE Max Power (mW)
<b>Lower</b>	5.150 - 5.250	indoor only	50	40
<b>Middle</b>	5.250 - 5.350	indoor and outdoor	250	200
<b>Upper</b>	5.725 - 5.825	outdoor only	1000	800

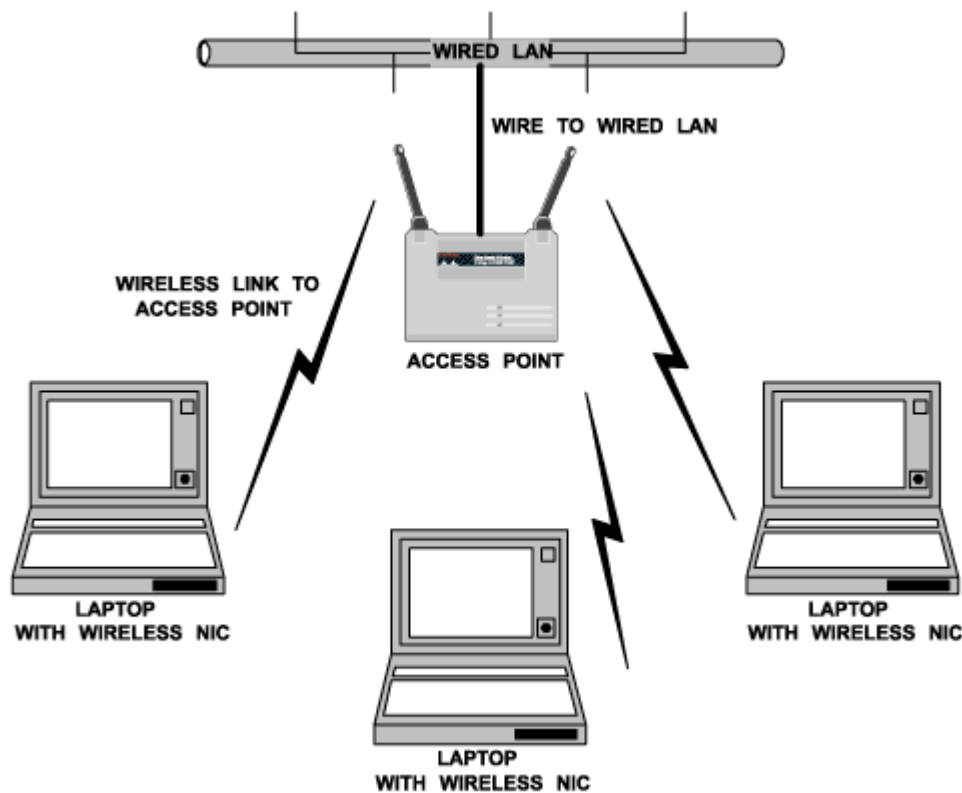
The ISM band is 125 MHz wide. Every UNII band is 100 MHz wide. The 5 GHz range wavelength is approximately 54 mm. An important point for future development is that each 5 GHz subband is wider than the entire 2.4 GHz band. It is possible to build 5-GHz wireless equipment that provides more bandwidth and more throughput than equipment for any other unlicensed band. Part 15 covers the 5 GHz band in the US. In Europe, this group of frequencies is generally defined under EN 300 440 and EN 300 683, which cover all frequencies from 1 to 40 GHz.

The attenuation from trees at 5 GHz is about 1.2 dB per meter.

## How Wireless Networks Work

### Infrastructure Network

For any wireless installation larger than a few workstations, the network should be set up in infrastructure mode. In an infrastructure-style network, access points are used to connect wireless devices to the wired network. For example:



[NA-Wire-WP1-04]

The wireless network is not a separate network. It is merely an unwired extension of a wired network. Everything in a wireless LAN operates at layers 1 and 2 of the OSI model. Security considerations may

require isolating this wireless extension to the wired LAN on its own virtual network (VLAN), but this is not a requirement for the proper functioning of a wireless network. To other network devices, the wireless workstations or even servers are indistinguishable from the wired devices.

Every wireless network needs a name. The name of the wireless network is the *SSID* (Service Set Identifier).

## CSMA/CA

When using wireless local area networks, we are going back to the old days of shared media. They operate much like the original hub-based Ethernet networks. The main difference is, unlike wire-based Ethernet, which attempts to detect collisions after the fact, CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) seeks to avoid them altogether. This method works by listening for a transmission already on the air. If it finds one, it waits. If the medium is available for at least the time defined by the *distributed interframe space* (DIFS) plus an additional random time, the station will transmit. This additional random time is determined as a multiple of the slot time. The contention window is used to determine the number of slot times to wait for the additional random time. Just in case another station does the same thing and transmits at the same time, the receiving station checks the CRC. If it is ok, then an ACK (Acknowledgement) is sent back. If not, then a retransmission takes place. After any unsuccessful transmission attempt, another backoff is performed with the contention window being doubled in size. This reduces the probability of a collision when there are multiple stations attempting to access the media's channel. The stations that deferred channel access during the channel busy period do not select a new random backoff time. They continue to count down the time of the deferred backoff after again sensing that a channel is idle. Thus the stations that did not get to transmit because their random backoff time was larger than the backoff time of other stations achieve a higher priority. After each successful transmission, the station that transmitted performs another random backoff. This is called the post-backoff, since it is done after, not before, a transmission. It is up to the upper layers to decide when too much retransmission has occurred and abandon the effort.

As this description shows, there is considerable overhead associated with this method of channel access. This slows the actual throughput to well below the theoretical capacity.

## Speeds

Unlike a wired network that either works at a single speed or not at all, a wireless local area network can reduce its speed to compensate for a reduced signal. Depending on the distance from the access point, data can be exchanged at these rates in an 802.11b network:

- 11 Mbps
- 5.5 Mbps
- 2 Mbps
- 1 Mbps

The process of *Dynamic Rate Shifting*, sometimes called ARS for Adaptive Rate Shifting, defines this reduction in the data rate that occurs as signal strength goes down.

Because this is a shared media, the actual throughput is much lower than the advertised capacity. In practice, speed is about 50 percent of capacity. For 802.11b networks, the only useful speed is 11 Mbps. When deployed, the useable speed is about 5.5 Mbps.

The 802.11a standard holds some appeal because it avoids the interference that is prevalent in the 2.4 GHz range by using 5 GHz frequencies. There is more available bandwidth in this frequency range. With more bandwidth in this range, the number of non-overlapping channels is also higher than in an

802.11b network. In an 802.11a network there are 12 available channels in the United States. There is considerable disagreement over the effective range of the 802.11a signals. In one study, the range was approximately 60 feet at the fully rated speed of 54 Mbps. In another study, the range was measured as the same as 802.11b and 802.11g, but this was from a study by Atheros, a manufacturer of 802.11a chipsets. 3Com reports that the average path loss difference between 2.4 and 5.2 GHz is approximately 7 dB in open environments and 2 to 3 dB in an office with cubicles. Cisco reports the ranges shown in the table below. The results from an Intel study are shown in the table above. You should conduct a test as part of the site survey since the environment and the premises have an impact on the data rates at various distances.

<b>Date Rate (Mbps)</b>	<b>Radius from Access Point (Feet)</b>
54	40 to 60
48	70 to 90
36	90 to 110
24	110 to 125
18	125 to 135
12	135 to 150
9	150 to 165
6	165 to 300

Speed is even more of an issue when the newest member of the 802.11 family, 802.11g, is added to the mix. Since 802.11g uses the same 2.4 GHz frequency range as 802.11b, when devices are mixed on the same network, speeds fall off for the 802.11g devices. An 802.11b user on the network requires the 802.11g access point to switch to protected mode. In this mode a CTS or an RTS/CTS exchange must be used before data transmission. The Request to Send (RTS) and Clear to Send (CTS) exchange puts even more overhead on the wireless network segment. This procedure is required so that the 802.11b devices can see and avoid the 802.11g traffic. More overhead and lower throughput is the result for all users, 802.11b and 802.11g. According to chipmaker Atheros, instead of the expected 23 Mbps, throughput falls to around 14 Mbps when using CTS and to 12 Mbps when using RTS/CTS. This reduced throughput occurs when the first 802.11b device associates with the 802.11g access point. It does not have to be sending data, just be associated.

## Access Points

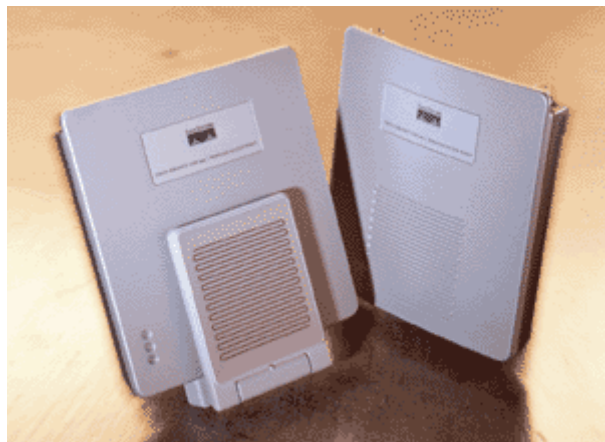
When creating a wireless extension of a wired network, two basic devices are required. The first is the gateway between the wireless and wired parts of the network. This gateway, commonly called an access point, is the on and off ramp for wireless signals. Just like the entrance ramp to a tollway, access to the wired part of the network can be controlled at this point. Two Cisco devices provide examples of the original style of access points and the newer form. The first, the Cisco Aironet 350, looks like this:



[NA-Wire-WP1-05]

From [www.cisco.com](http://www.cisco.com)

The newer Cisco access point is the 1100/1200 series. It looks like this:



[NA-Wire-WP1-06]

From [www.cisco.com](http://www.cisco.com)

## NICs

The second basic device used in a wireless extension to a network is the wireless network interface card (NIC). The wireless NIC can take many forms including PCI adaptor, PC Card, and USB adaptor.

## Deployment of Wireless Networks

Keeping the basic information that we just covered in mind, let's look at the issues faced by staff sent to a location to install a wireless network. The first consideration is the affect of the antenna. This will have a major impact on the success of the network.

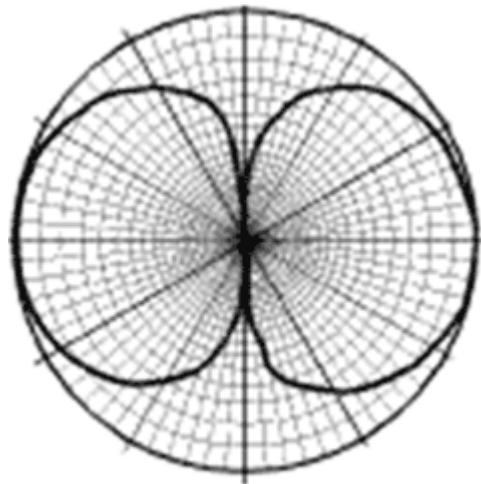
## Selecting an Antenna Type For a Particular Deployment

The antenna is a very important part of both the access point and the wireless NIC. There are many types of antennas. This discussion is limited to the types commonly used for an indoor wireless local area network and a short-range outdoor campus area link.

The types of antennas fall into three basic categories. The difference is the direction of the radiation field emitted from the antenna:

- Omnidirectional - all directions
- Semidirectional - a limited direction
- Highly Directional - one single direction

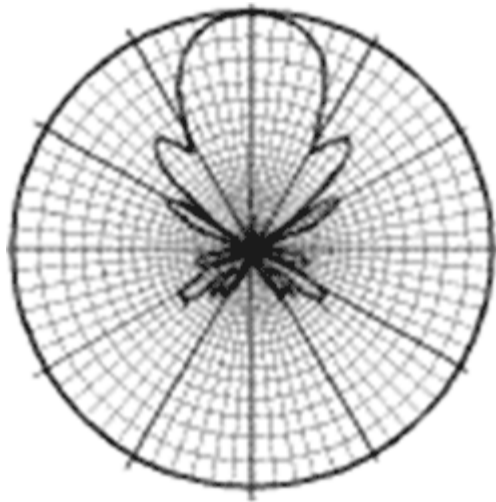
The fields are called beams or lobes. Each antenna should have a published and readily available laboratory-measured radiation pattern showing the lobes. For example:



[NA-Wire-WP1-07]

From [www.cisco.com](http://www.cisco.com)

Or



[NA-Wire-WP1-08]

From [www.cisco.com](http://www.cisco.com)

For each antenna, there are different patterns when looking at the antenna from the side or down on the antenna from the top. These two patterns are the azimuth pattern for the E-plane and the elevation pattern for the H-plane. The actual radiation field is three-dimensional, but published patterns are always two-dimensional.

## *Antenna Radiation Patterns*

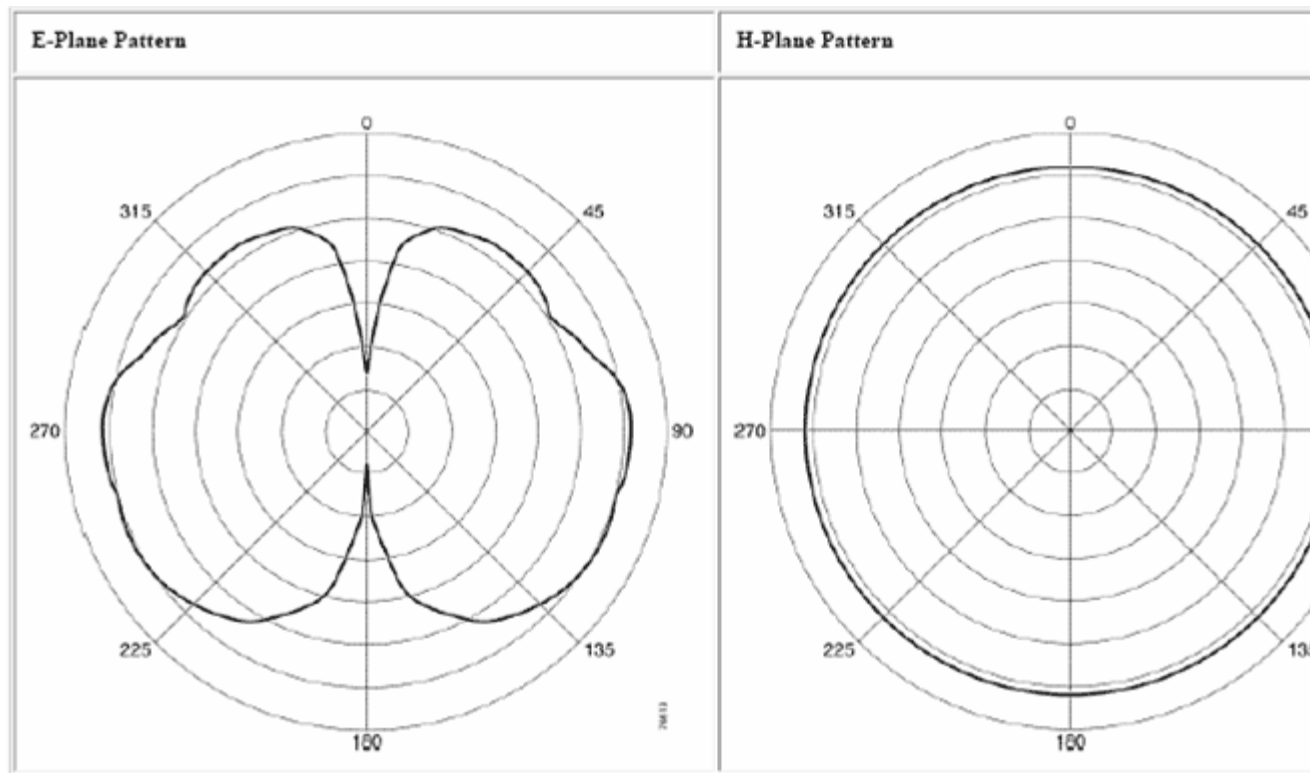
Every radio has an antenna. You may not see it, but it's there somewhere. The signal sent out or read by the antenna has a three-dimensional shape or radiation pattern. The pattern's shape differs depending on the construction of the antenna. When actually deployed in the field, the size and shape of the pattern depends on the power emitted by the radio transmitter and the obstacles the signal encounters as it propagates between the sending and receiving stations. Let's look at some example radiation patterns for common antenna types. The most common antenna used by access points is a dipole design. A simple dipole looks like this.



[NA-Wire-WP1-09]

This dipole antenna is used with the Cisco Aironet 350 series access points. The theoretical radiation pattern for this antenna looks like a figure eight when viewed from the side. When viewed from the top a dipole antenna covers all 360 degrees. Here is the pattern published by Cisco for this antenna

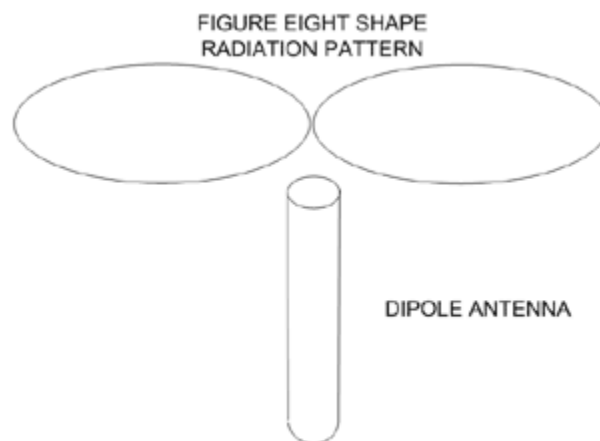




[NA-Wire-WP1-10]

From [www.cisco.com](http://www.cisco.com)

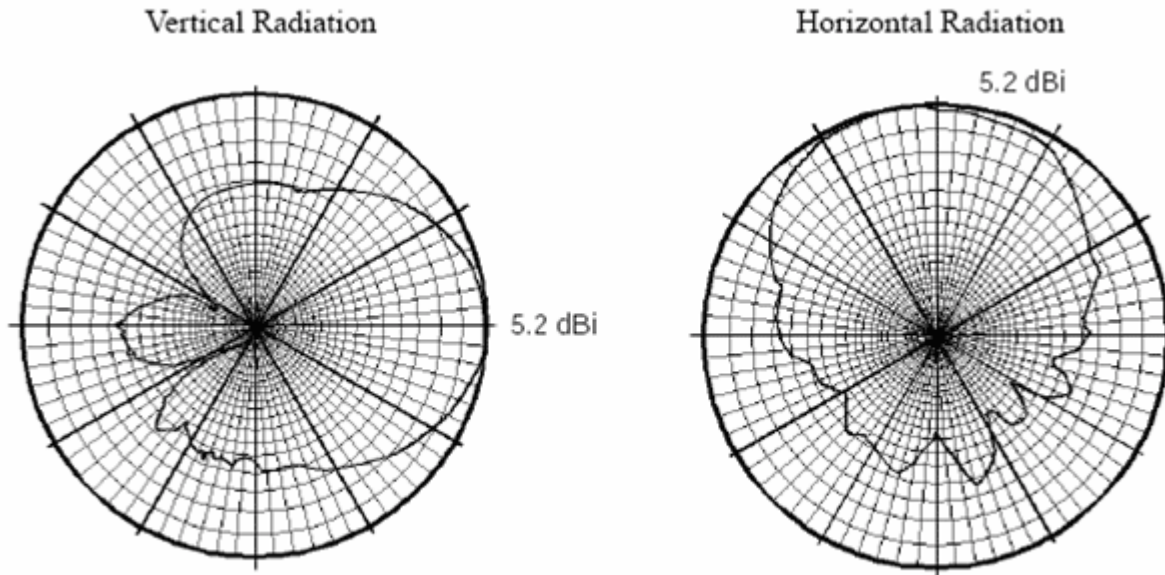
In three dimensions, the dipole pattern looks like a figure eight, such as



[NA-Wire-WP1-11]

Notice that the area of weakest signal is directly above and directly below the antenna. The main problem with a radiation pattern like this is the lack of a distance scale. The edge shown for the antenna is the 3 dB mark. This is where the power level produced at the antenna drops by 50 percent. The measurement is taken in a controlled environment in the test lab. The actual radiation pattern seen on the job will be similar, but not exact. This is one of the reasons for a site survey at the location of the wireless network. A dipole antenna is supplied with most indoor access points.

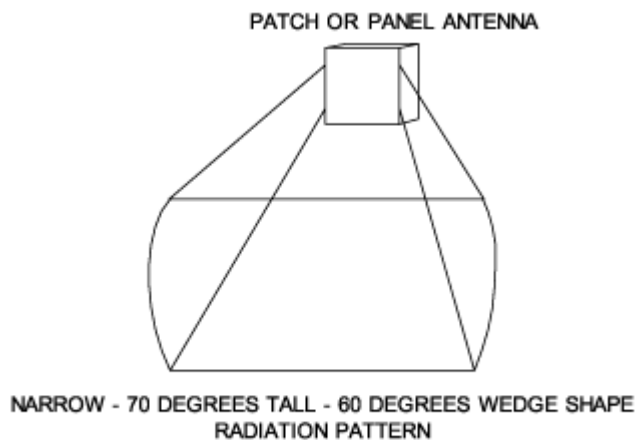
Another way to deliver signal inside a building is to locate the radio and antenna in each corner of the building or each end of a main hall. All around coverage is not desirable in this case because much of the pattern will be wasted outside the building. To keep the pattern inside the building, the power should be directed in limited directions. The patch or panel antenna is a semidirectional antenna commonly used for this application. Here is the radiation pattern for the AIR-ANT1729 patch antenna from Cisco that will work with Aironet access points.



[NA-Wire-WP1-12]

From [www.cisco.com](http://www.cisco.com)

The patch antenna's three dimensional pattern looks like a wedge.



[NA-Wire-WP1-13]

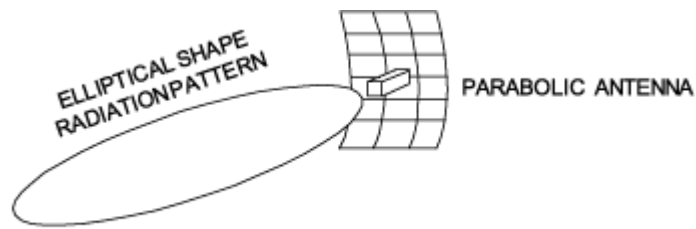
A patch antenna looks like a small box or book attached to a wall. These can be used inside or outside depending on their construction. For example:



[NA-Wire-WP1-14]

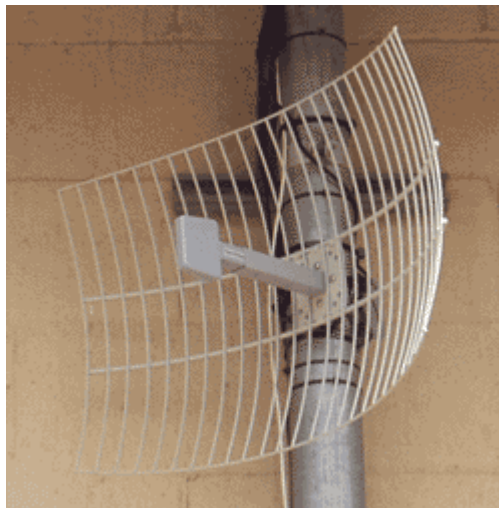
From [www.telexwireless.com](http://www.telexwireless.com)

To tighten the beam even more, a highly directional antenna such as a parabolic dish or grid antenna can be used. This type of antenna produces an elliptical pattern.



[NA-Wire-WP1-15]

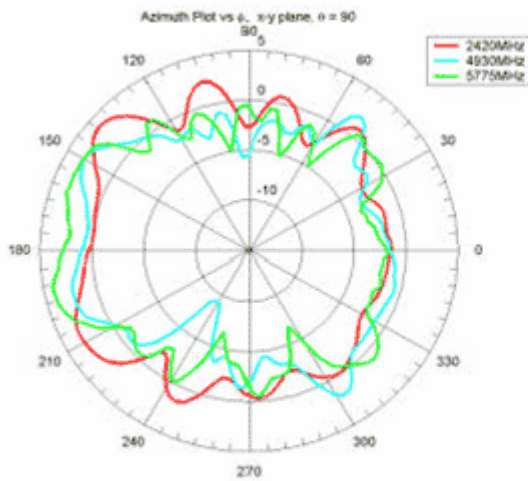
Here is an example of this type of antenna.



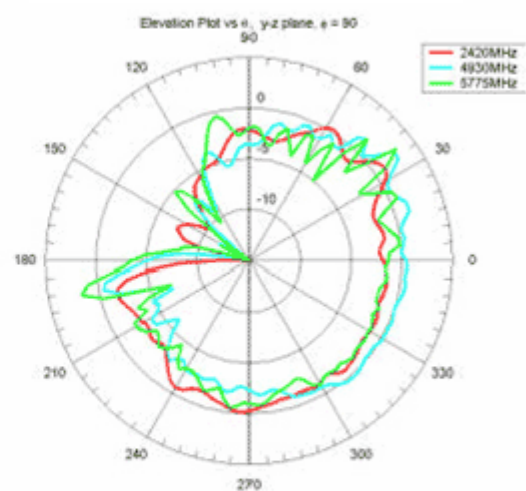
[NA-Wire-WP1-16]

Notice that we have focused on the radiation pattern from only one radio in a two-radio system. The wireless NIC card used in the end user's device also has a radio with an antenna. It is very difficult to design an antenna that must be entirely contained on a circuit board at the end of the PC Card form factor. Cisco does not even publish the radiation pattern for their AIR-PCM35 antenna used on the Aironet 350 series of wireless PC Card NICs. Typically, the gain of this type of antenna is very low. The effective gain also varies based on how the antenna is pointed. Recall the above discussion of polarization. In most cases, the radiation pattern of a laptop NIC antenna is above and below the NIC because it sticks out of the side of the laptop. For the newer laptops, the antenna is built into the case. The NIC in these laptops is a miniPCI card under the keyboard with the rest of the circuit boards. The shape of these NIC radiation patterns is usually very irregular with several null areas where no signal is received at all. Here is the radiation plot for an antenna designed to be mounted at the top of a laptop's display.

**Azimuth gain plot (dBi).**



**Elevation gain plot (dBi).**

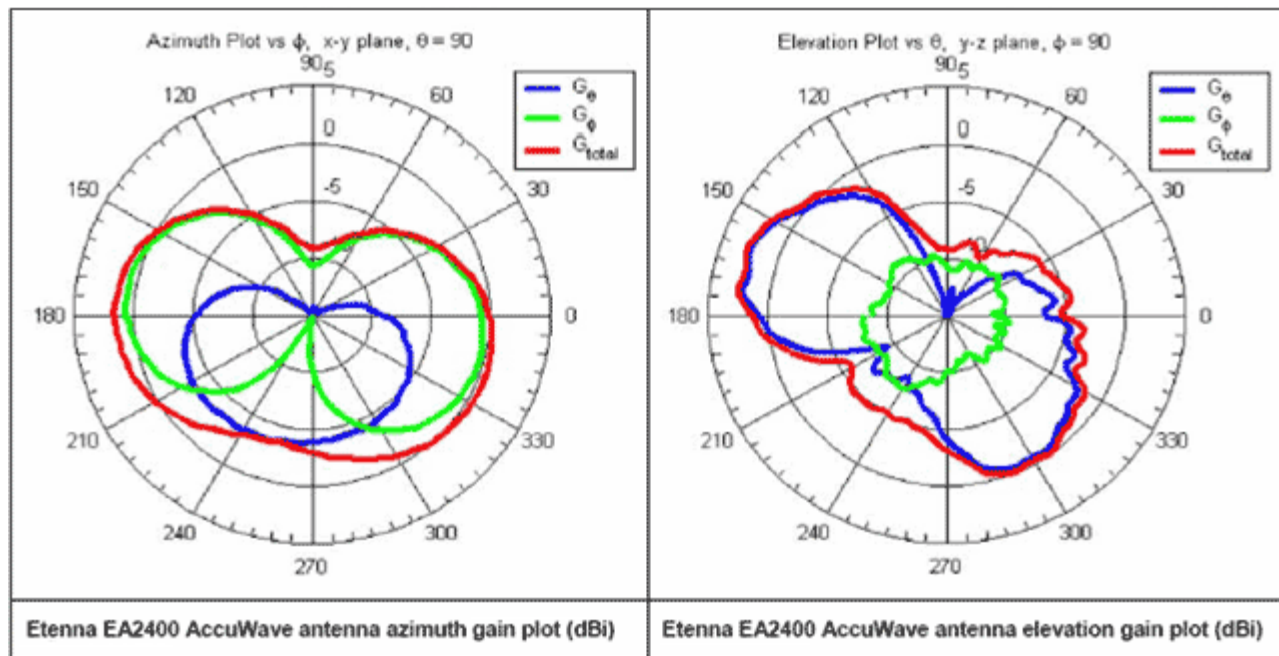


All data excludes cable losses.

[NA-Wire-WP1-17]

From [www.eten.com](http://www.eten.com)

This antenna's gain is rated at 5 dBi. This is the plot for a similar antenna designed to be mounted under the keyboard.



[NA-Wire-WP1-18]

From [www.etenna.com](http://www.etenna.com)

The gain for this antenna is 3 dBi. Desktop wireless devices use a dipole antenna.

More sophisticated antennas, adapting the phased array antenna approach, are appearing on the market. These use beam shaping to deliver customized beams to each user or area of the network. They use as many as 120 antenna elements in a single large panel. A set of radios is used to drive these antennas. This type of radio is being called a wireless switch. Companies like Vivato produce these proprietary systems. The costs are about ten times that of the price of a standard access point. There are several companies chasing this small market. Consolidation in this part of the wireless market is inevitable. Be cautious about what you buy.

If the antenna that comes with the device is replaced, it must be an approved antenna. In the United States, the FCC requires the manufacturers to have each access point and antenna combination certified together. To prevent attaching just any antenna, each manufacturer uses atypical connectors, such as those with reverse polarity. For example, Cisco antennas use an RP-TNC connector. This is a reverse polarity TNC connector. In practice, these restrictions are easy to avoid by using short adapter cables called pigtailed, but it is not legal to use them.

## Site Survey Process

Now that we have covered the concepts and basic parts, it is time to put them to use. The first network we're going to look at is the local area network. What we are looking for in a local area network is coverage area and throughput. There are two ways to look at this combination. The layout of the access points focuses on the size of the coverage area or the traffic capacity of each access point. The coverage area goal is to use the least number of access points. The capacity approach is applicable where you are dealing with high data rate applications or latency-sensitive uses. The number of access points is less important than each access point's ability to handle traffic. At the end of the site survey, you will know the location and configuration for each access point.

The site survey process will first look at what is required to perform a site survey for a local area network. We will discuss three situations. The first example is an ongoing deployment in a typical office

building. The second example addresses the adjustments required when a wireless local area network is used outside of an office. The last example is the deployment of an outside point-to-point campus area network link.

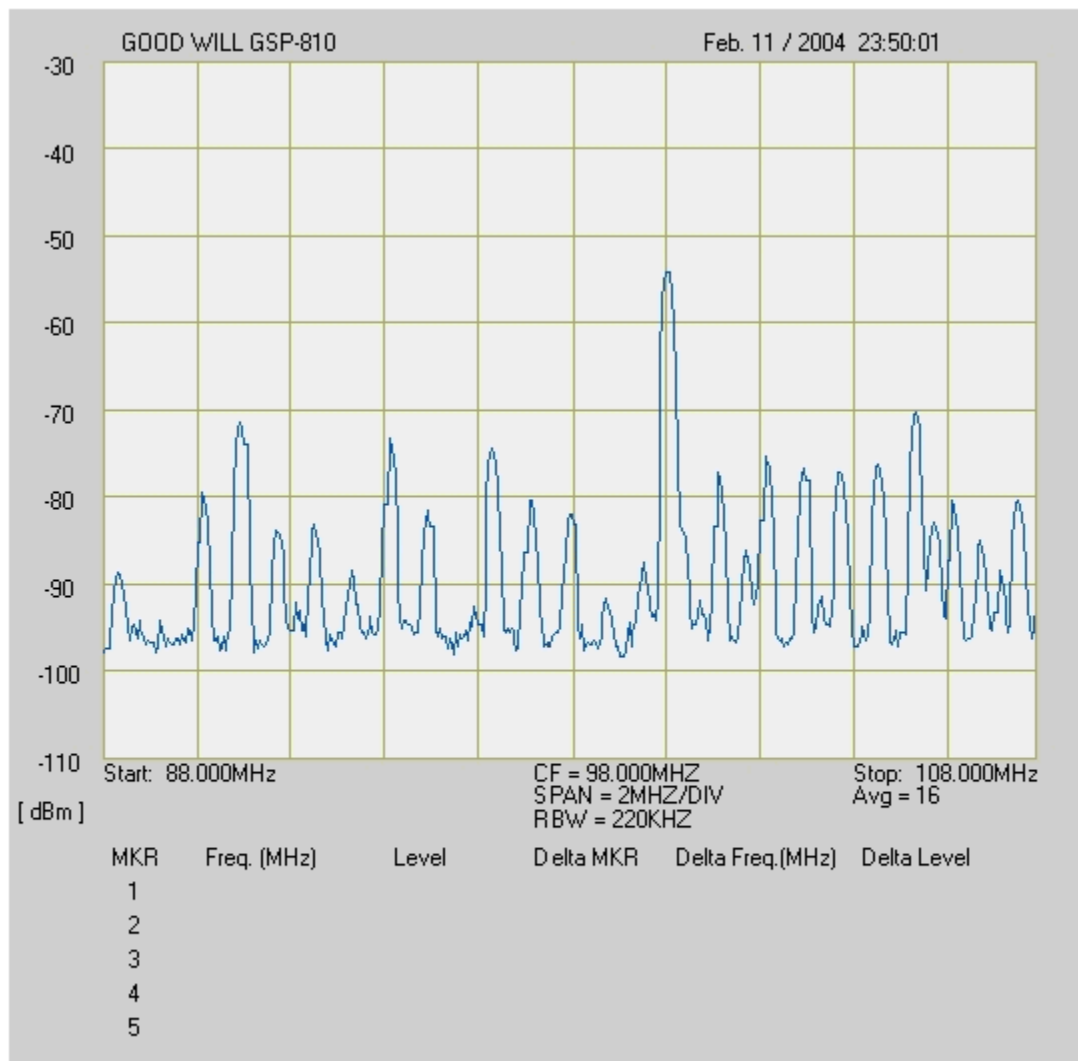
The access point locations may be determined in any of three ways. Perform the standard site survey; use a centralized management system to predict the locations; or, do not bother with the site survey just go straight to deployment.

Keeping in mind whether coverage or capacity is most important, a site survey centers on two basic tasks. First, determine what the existing radio frequency environment looks like. Second, determine the required equipment and how best to place the equipment for the new wireless network extension into that environment. Sometimes it is not possible to fit anywhere into the existing radio frequency environment. In that case, the existing environment must be altered for the new project to succeed. Because alteration of the existing environment requires that others cooperate with you, it is easier to work with what is already there.

Before beginning the site survey, ask the client, or yourself if this is your network, what devices may be out there that will interfere with the wireless network signal. Everyone has heard of the microwave oven and portable telephone interference problems. Look for these and others that are listed in the troubleshooting section.

## *Assess the RF Environment*

After the known causes of interference are identified, it is time to look for the unknown ones. There are two ways to assess the current radio frequency environment. The first way is to use a spectrum analyzer to look at the actual waveforms of the signals present in the band that the new network will occupy. Many articles on the site survey process just casually toss off this advice to examine the environment with a spectrum analyzer. They fail to tell you how to do this or what it really costs. Using a spectrum analyzer is easy, once you learn how. Interpreting the results when the signal is a spread spectrum waveform is not. Let's look at the output of a spectrum analyzer. This first screenshot shows the FM radio band from 88 to 108 MHz in my area.

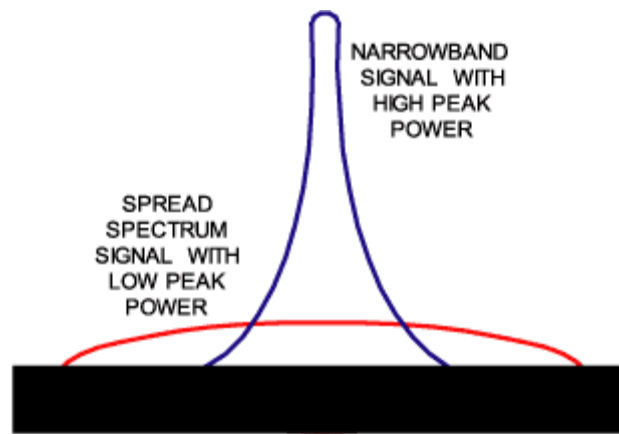


[NA-Wire-WP1-19]

Each of the peaks on the graph represents a FM radio station. This result was easy to obtain. The spectrum analyzer was tuned to the frequency at the center of the band of interest by entering the frequency 98.000 MHz using a keypad. The span each vertical line was to represent was selected the same way. Here the span is 2 MHz. The result is a graph showing quite a few FM radio stations in the area. As the graph shows, FM radio uses a high power signal at a single frequency.

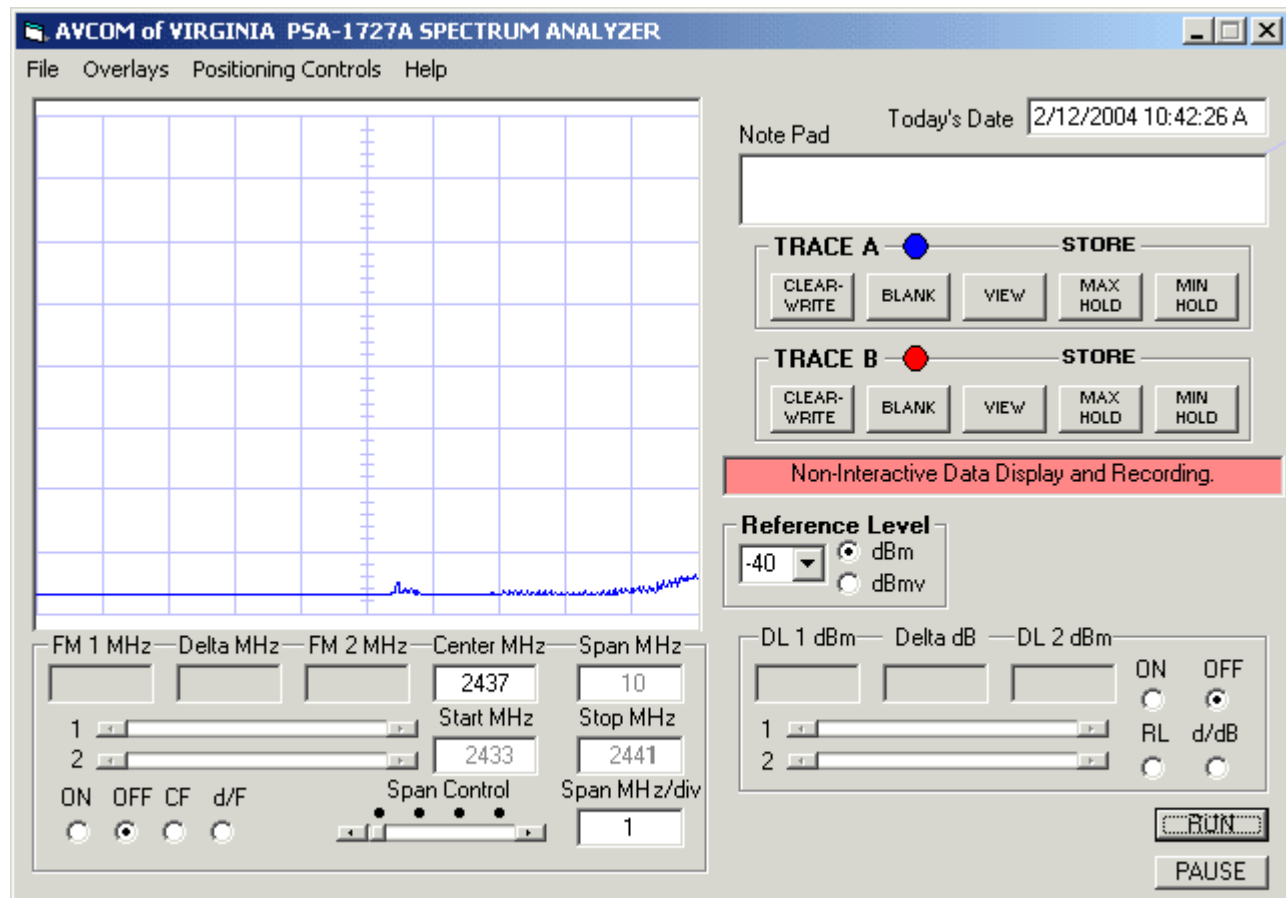
The problem in using a spectrum analyzer for a site survey, when the user has little experience with its use, is the nature of the spread spectrum signal. The spread spectrum, in this case DSSS, signal uses low power to spread the signal over a wide range. This is to prevent any strong signal in the same band from overwhelming the entire spread spectrum signal. Here is a theoretical DSSS signal in relation to a high power signal at a single frequency.





[NA-Wire-WP1-20]

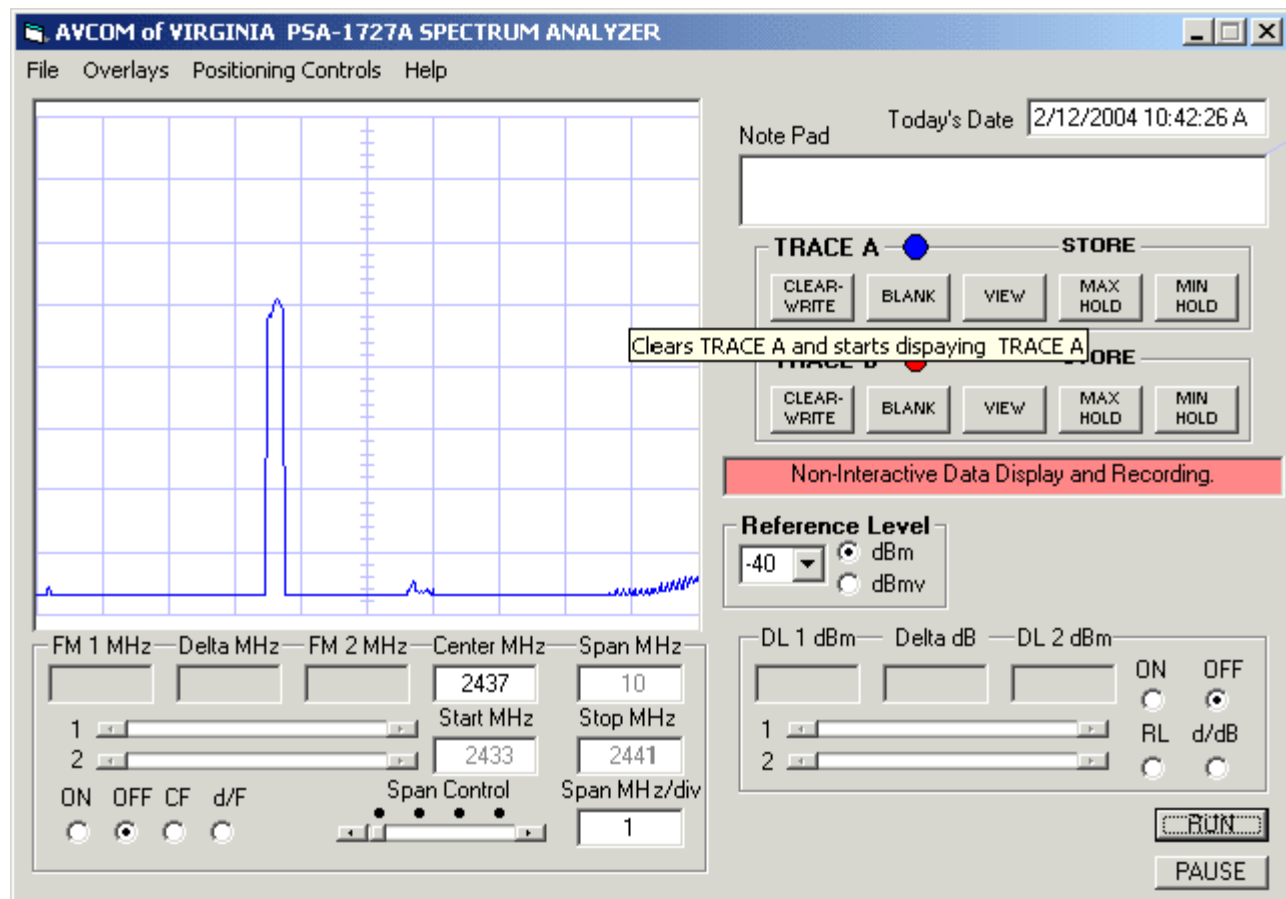
Here is an actual spread spectrum signal in the 802.11b band as captured by a spectrum analyzer.



[NA-Wire-WP1-21]

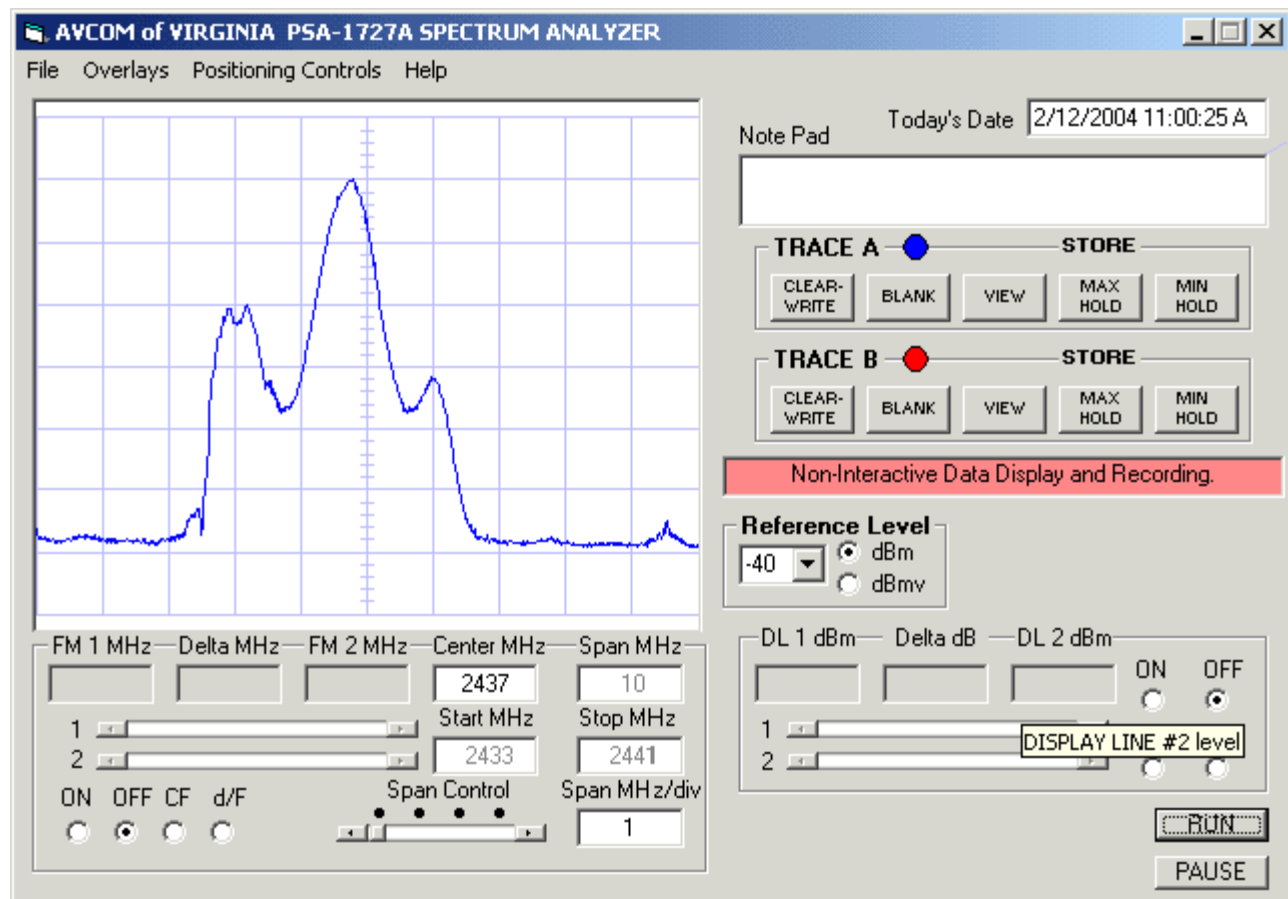
Not very useful. This is the nature of spread spectrum signals. DSSS uses low power spread over a wide area. The signal peaks briefly at different points across the band. Here is a shot that captured a single peak.





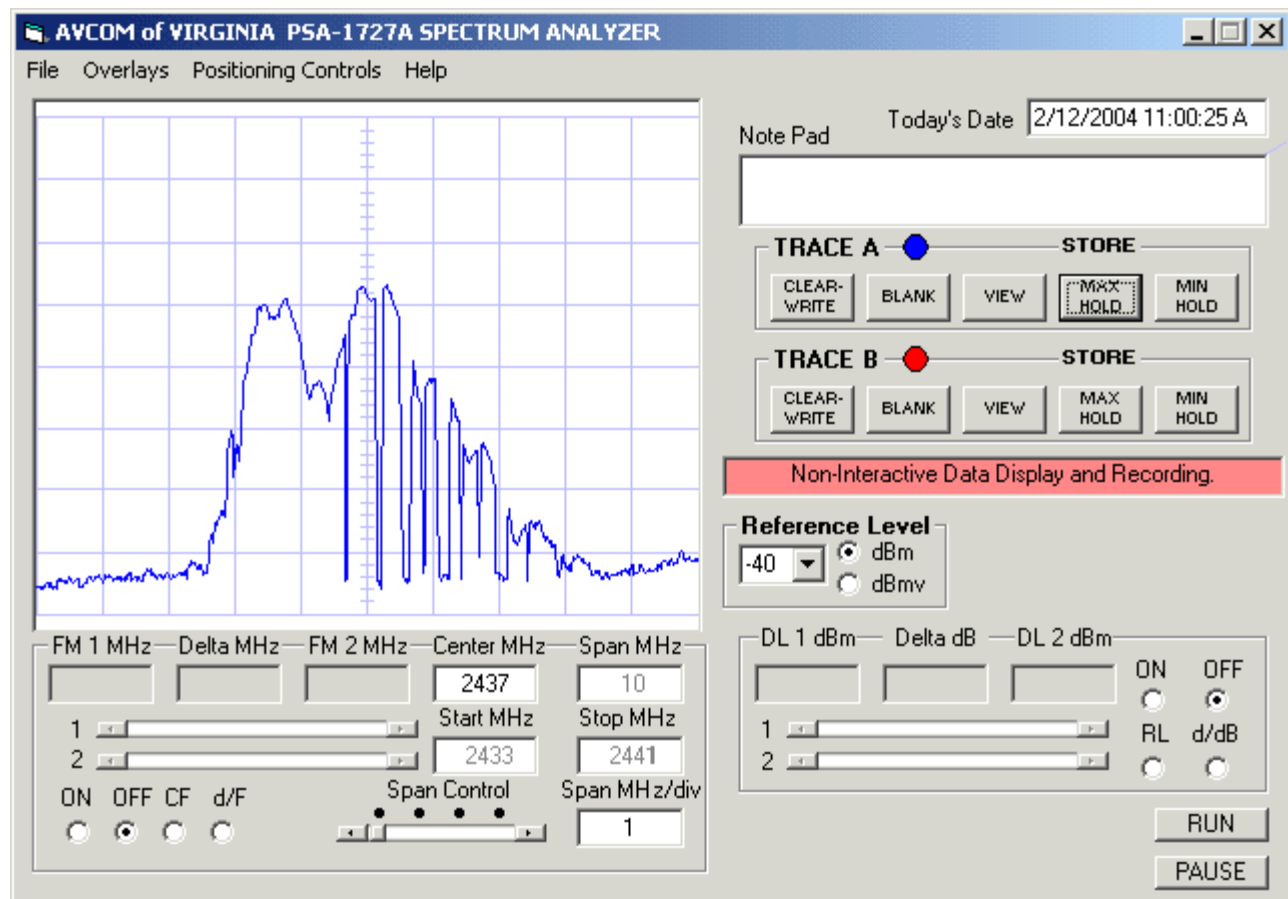
[NA-Wire-WP1-22]

The only way to capture the true DSSS waveform is to use the peak hold function of the spectrum analyzer. This function captures and holds the signal at each point. Over time, the total waveform is seen. Here is a captured DSSS signal using peak hold for 2 minutes on a low activity network.



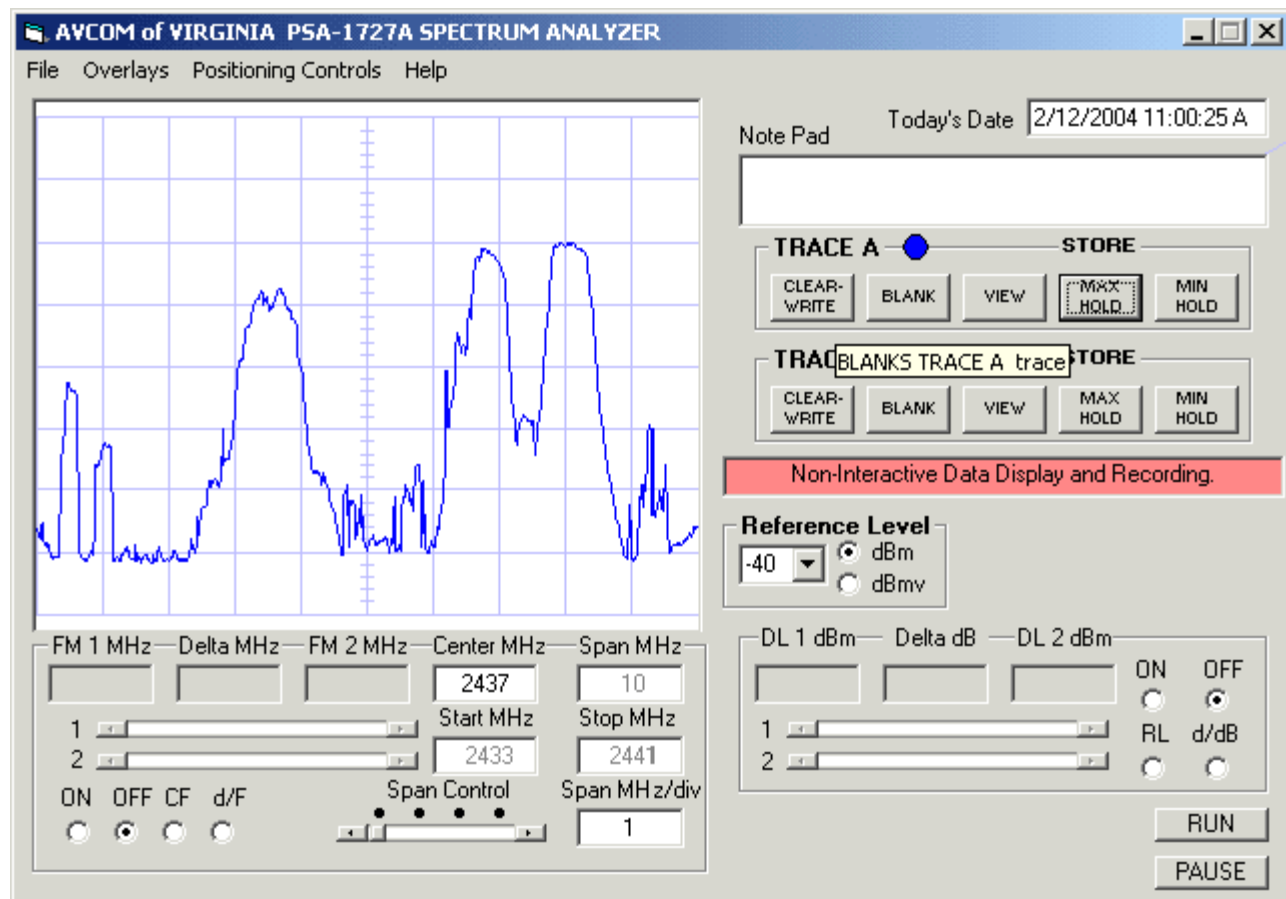
[NA-Wire-WP1-23]

Adding a second access point overlays an additional signal onto the waveform seen just above.



[NA-Wire-WP1-24]

Taking out the second access point and putting a microwave oven in its place generates this type of waveform.



[NA-Wire-WP1-25]

The figure does not show it, as it's a single point in time, but a high instantaneous peak such as that produced by a microwave oven is fairly easy to pick out when the peak hold is turned off. Sources of interference from devices such as a microwave oven, a cordless phone, or a frequency-hopping access point can be identified with a little practice with a spectrum analyzer. What cannot be easily detected are other spread spectrum signals.

A spectrum analyzer is a very useful device if you know what you are doing. If you haven't had a lot of practice with a spectrum analyzer, you will find it easier to find other DSSS signals by using a device that identifies 802.11 networks by channel. Then use the noise floor figure or signal-to-noise ratio to discover non-DSSS signals within the radio frequency environment. When these non-DSSS sources are turned off, the noise floor should drop and the signal-to-noise ratio improve.

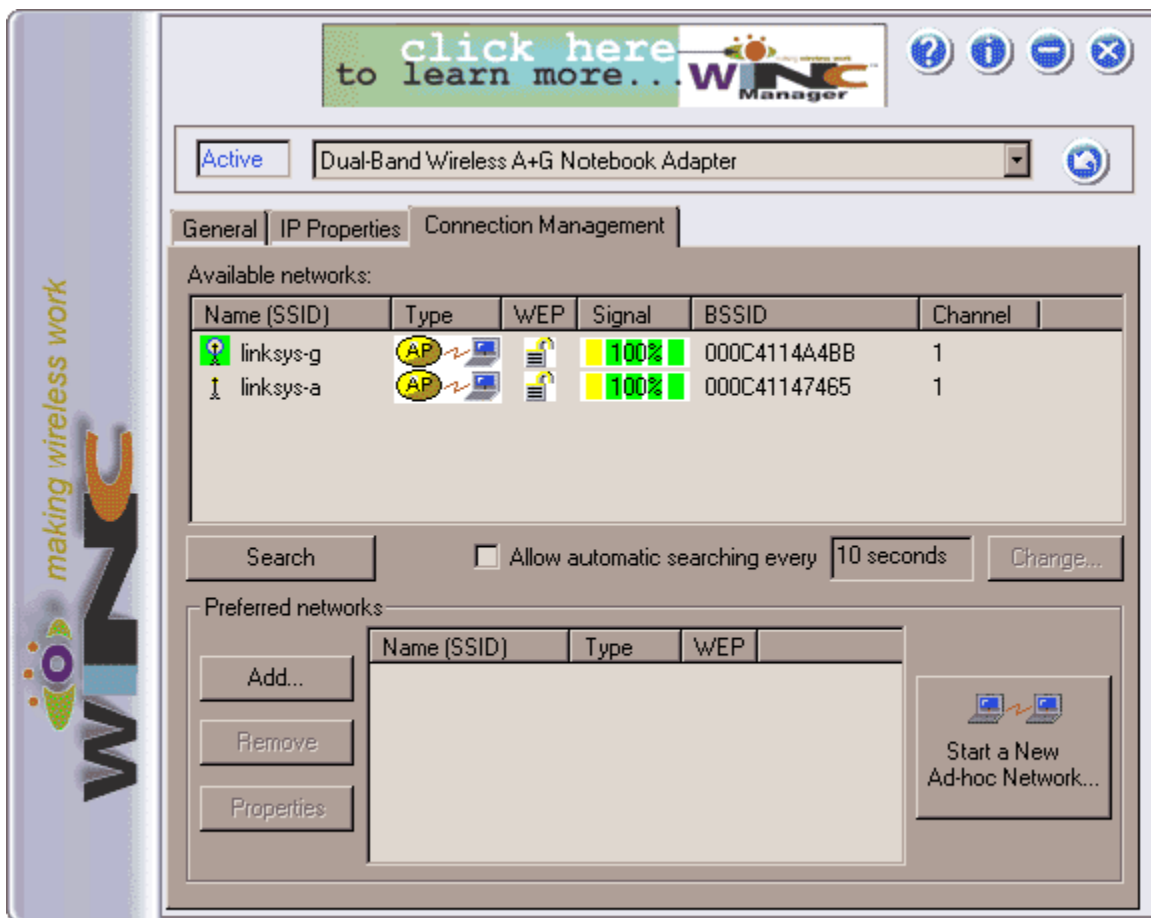
A spectrum analyzer like the Avcom 1727A, which was used to generate the above figures, costs between \$4,000 and \$15,000. The Avcom is a very nice unit at the low end of the price range. (<http://www.avcomofva.com>) If the cost of a spectrum analyzer cannot be justified, then it can be rented or someone else can be hired to do this part of the site survey. The cost for rental is a few hundred dollars. Hiring someone to do this, depending on the required time, can cost a few hundred dollars up to thousands of dollars.

The main reasons that most installations are not preceded by a full spectrum analysis are the inability of most network administrators to use a spectrum analyzer and the high probability that there will be no excessive interference in the 2.4 GHz band. That is, no interference other than another user having an 802.11 network of some sort within range. The most common sources of non-802.11 interference in the 2.4 GHz band, in addition to microwave ovens and telephones, are amateur radio operations in or near the band, lights that use 2.4 GHz signals to excite the gas in the tube, satellite radio services near the band, cellular phone cell site backhaul connections, medical devices, and high power television

station transmission from remote vehicles back to the studio that all use the same 2.4 GHz frequencies. Few of these are likely to exist inside or near an office building unless, of course, your office is a medical facility, television station, or cell site -- in which case it is fairly easy to determine which of these may affect you. The common ones that may exist, the microwave and portable phone, can be avoided with careful placement of those devices and the wireless equipment.

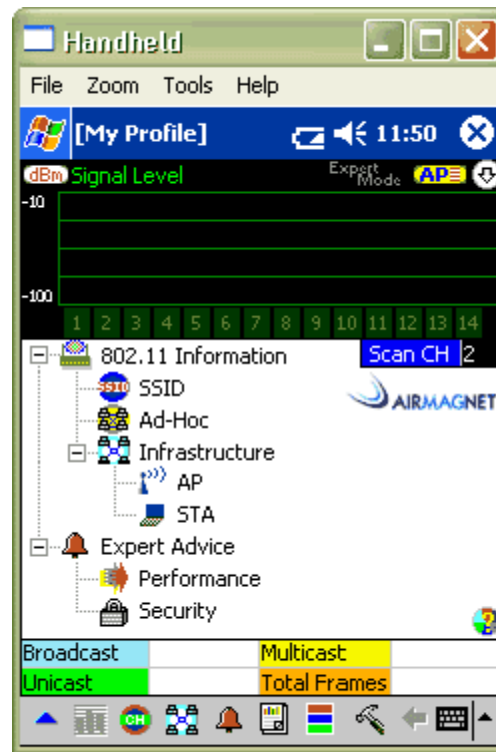
## Access Point Survey

The second type of site survey device just looks for access points. These range from low cost to high cost. Consideration at this point may also be made to determine if the purchase made for a site survey could also be used long term for rogue AP detection. The low cost approach is to download a program such as Cirond WiNc ([www.cirond.com](http://www.cirond.com)). This \$19.95 program will show all of the access points in the area. For example



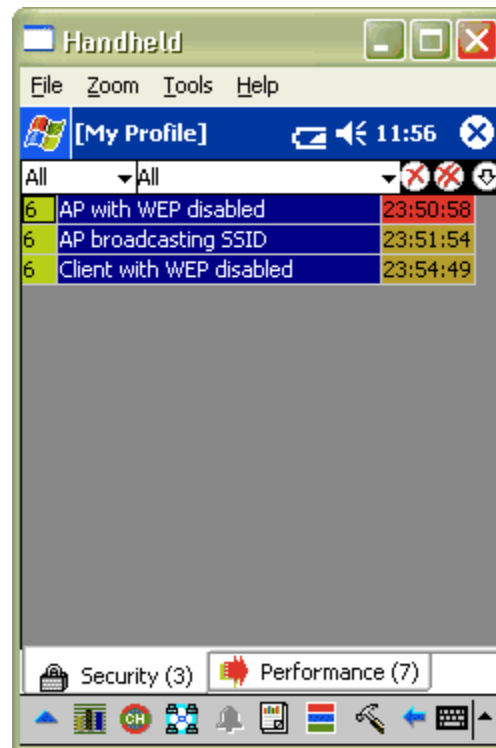
[NA-Wire-WP1-26]

At a higher cost is a device such as the Air Magnet line. These devices are much more powerful. Let's look briefly at Air Magnet. Air Magnet organizes their features into six categories. Beginning with the Start screen, it shows all of the access points and stations identified within the range of the handheld or laptop that Air Magnet is running on. Here is the opening screen.



[NA-Wire-WP1-27]

Another very useful screen is the Alarm screen. This view shows a list and details for all of the security problems detected on the wireless network.



[NA-Wire-WP1-28]

The Air Magnet device can identify unexpected signals, access points, or stations on the network. An alarm is sent to the administrator whenever any of these conditions is found. In addition to security problems, the Alarm screen shows performance problems.

Stations often have problems connecting to an access point. From the Tools screen, the Diag tool can be selected. Using this tool, the station having the problem is rebooted. The Diag function records the steps the station follows to connect to the access point. Any failures in this process are identified. This is a very nice tool.

The Find tool is also very useful. This tool helps locate rogue devices through an onscreen signal strength meter. This allows the device to be located.

Finally, the Site Survey function allows recording of data as the unit is carried from one location to another. This data is then exported as a flat file database for further analysis. One issue with using a handheld instead of a laptop is the size of the NIC. The antenna in the typical laptop NIC is bad enough already. When this is reduced to the CF form factor, it is even worse. The Air Magnet software is available for laptops as well. I suggest these for site surveys. It is also possible to use a PC Card in a handheld. Some handhelds come with a PC Card slot. Others, like the Dell Axim, can use a CF to PC Card adaptor.

The cost for the software and supported network interface card is from \$2,500 to just over \$4,000 ([www.airmagnet.com](http://www.airmagnet.com)).

## *Access Point Locations*

Once the ambient RF environment is identified, the installer can start to lay out the wireless network extension. There are four aspects of interest when laying out an extension to the wired network.

- Data Rate
- Signal
- Noise
- Signal to Noise Ratio

The data rate is very important because 802.11 networks make poor use of the network capacity. Because it is a shared environment using a collision avoidance mechanism, overhead chews up about half of the capacity. For an 802.11b network, this capacity is not the theoretical 11 Mbps, but 5.5 Mbps. Dynamic rate shifting can allow a device to maintain a link at a lower data rate, but this is not very useful. Design the network to maintain the maximum data rate. The throughput must be designed to accommodate the expected traffic. For a typical office, 5.5 Mbps may be adequate. However, this would not be adequate for a network that sends large graphic files. The number of users supported by each access point is also an issue in this shared media. A common guideline for 802.11b networks serving a typical business is 30 to 50 users per access point. If the business is a graphics firm or the area is a classroom filled with students working on database administration, then this guideline may not be appropriate. This is the reason to test the network before putting it into operation. This process is discussed later.

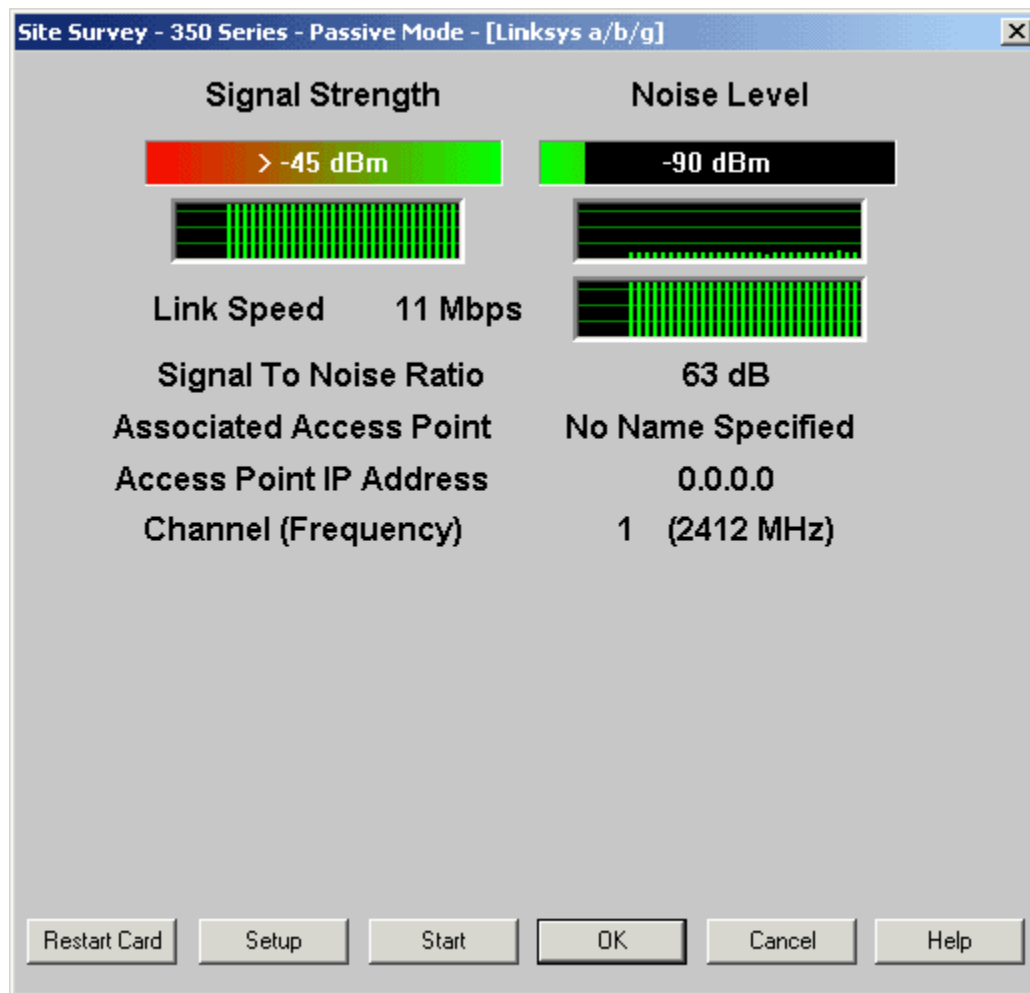
The wireless LAN equipment we are installing creates the signal. The noise is what everyone else is creating. Of course, once we finish and the next person begins a nearby installation, then our signal becomes noise to them.

The desirable signal level must remain above the receive sensitivity of the worst receiving unit that will be used in the wireless network. The receive sensitivity of wireless NICs ranges from -80 to -91 dBm at the maximum data rate for 802.11b equipment. Users might have almost any device to receive the

signal, so the worst receive sensitivity should be assumed. The receiver sensitivity is the lowest signal level that a radio can receive with a certain Bit Error Rate (BER) that allows the transfer of data at the specified data rate.

What the site survey device reports as noise is everything that the device cannot identify as a signal. In other words, what it cannot demodulate.

The easiest way to measure all of this is to use a Cisco 350 Aironet network interface card. This card, along with the Orinoco line from Proxim, is one of the few that will report values in dBm instead of a percentage of Receiver Signal Strength Indicator (RSSI). As Priscilla Oppenheimer and Joseph Bardwell thoroughly explain in "Troubleshooting Campus Networks" RSSI readings are useless. Do not let the book title fool you; this is an excellent all around troubleshooting book for any size network. The Aironet Client Utility program that comes with this NIC has a display like this.



[NA-Wire-WP1-29]

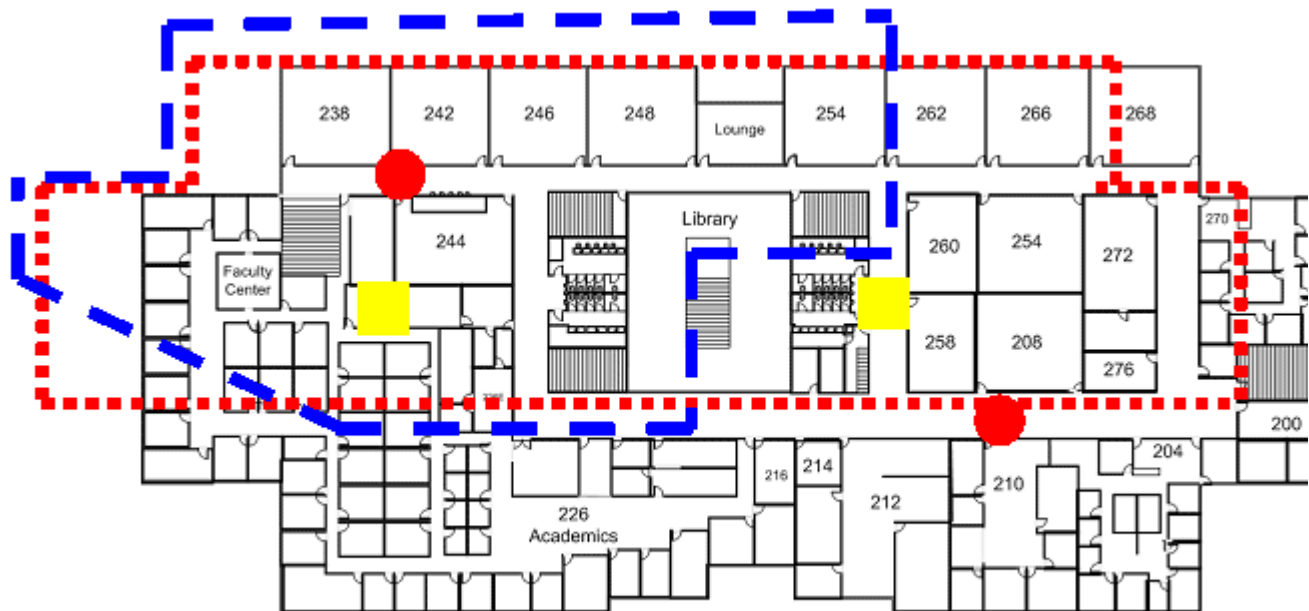
This display shows data rate, signal, noise, and signal-to-noise ratio. It is easier to record the signal strength and the noise level. Put both values in a spreadsheet and compute the signal to noise ratio. The noise floor shown above of -90 dBm is a common figure. The noise floor usually shows from -80 to -90 dBm. The highest, nearest to 0, noise floor I have heard of is Lagos, Nigeria. I was told it is around -45 dBm for the 2.4 GHz range. The Orinoco cards also have a display similar to this.

To use this utility, just walk away from the access point in different directions like the spokes of a wheel while recording the readings on a copy of the floor plan. The idea is to see where the 20 dB



signal-to-noise ratio point is. This point, where the SNR drops below 20 dB, is the edge to mark for the coverage area in that direction. This requires two people, one to hold the laptop and another to record. Some of the automatic units, such as the Air Magnet device, will do the recording for you. Record these readings on all floors and outside the building. Be sure the site survey device does not change association to another access point while performing the survey. The Cisco site survey software has a MAC address setting to prevent this. When finished, connect the dots. The result is an irregular coverage pattern surrounding each proposed access point location. This pattern is not circular as described in most publications, but highly irregular. Examine the plots for dead spots where no signal penetrated.

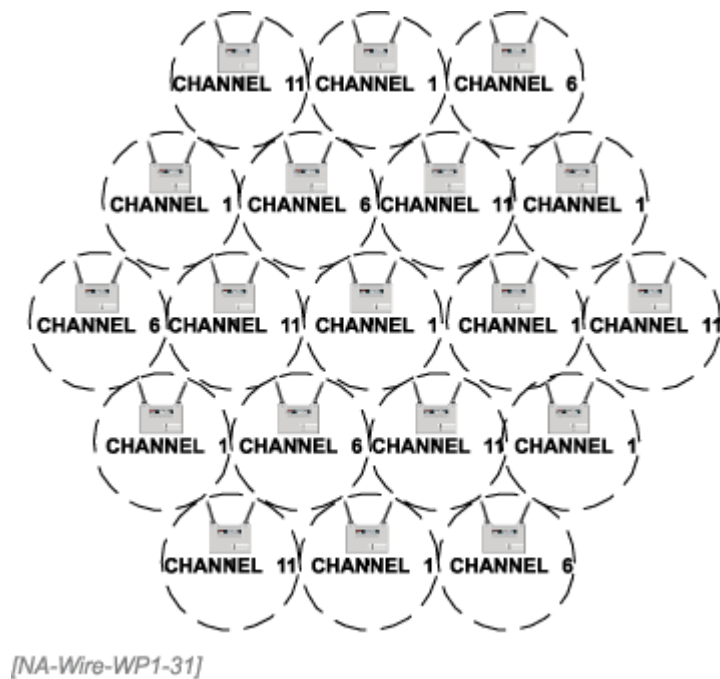
Let's look at the results of a site survey. A two-story building is being surveyed for installation of one or more 802.11b access points to provide wireless Internet access to the students in the building. Here is what the second floor looks like.



[NA-Wire-WP1-30]

The first idea for coverage was to place an access point in the ceiling at opposite ends of the two long halls. These are the red circles. The expected coverage area is the red box using the small square dots for the line. This pattern ignores the spillover to the outside for now. With this pattern, four access points can cover the entire building using two per floor. The problem with this plan was both too little coverage and too much coverage. There was much less coverage than expected inside the building and much more outside of the building. The actual signal coverage inside the building is shown as the blue dashed line. The signal also extended outside the building over 400 meters away. This coverage area was measured with the laptop-style NIC. Imagine how far away this signal could be received outside using a highly directional antenna. The revised plan places the access points further into the building where the yellow boxes are. With a reduced power setting on each access point, this covers the building and helps to keep the signal inside. Some signal still penetrates outside, but not as far. The first floor uses a similar pattern. Cell overlap is needed in the layout to ensure that a user walking around the building maintains a connection and to prevent dead spots. An overlap of 20 to 30 percent is adequate.

A channel assignment plan for the access points is needed as part of the site survey. The channels to use depend on the 802.11 standard used, the number of access points required, their location, and the purpose of the coverage. The 802.11b standard allows for only three non-overlapping channels. These are 1, 6, and 11. Some have used a four-channel set of 1, 4, 8, and 11 with success. 802.11a allows for 12 channels. 802.11g is limited to three channels, but at a higher speed than 802.11b. The channel plan for a multistory building has to be three-dimensional. This is hard to do with three channels. Here is a typical pattern used for a single floor.



In the sample local area network illustrated here, the second floor called for a modification of this pattern. The pattern will be channels 1 and 11 on the second floor, then channel 6 on the first floor below channel 1 on the second floor and channel 1 on the first floor under channel 11 on the second floor.

Another aspect of locating the access points is connecting them back to the wired network. The access point must be within the limits for cable runs from the access point to the switch.

As this site survey was being performed, the access point was initially placed in the ceiling. Because this access point, Cisco Aironet 350, uses Power over Ethernet (PoE) a cable was run to each expected location. This delayed the start of the survey while the cables were installed. As the actual pattern shows, this also placed the cables in the wrong location. As the access points were moved from location to location, pulling cable to each test location became bothersome. The question arose about placing the access point on a plastic cart instead of the ceiling. What affect would this have on the signal used for the site survey? After testing, it was found that the signal was the same near the access point's location, but worse by an average of 5 dB as the site survey device went beyond 60 feet from the access point. So there is no need to place the access points in their planned physical location above the false ceiling, at least in this building. Rolling them around on a cart doesn't provide a better signal, as would be expected, but a lower signal level. In this instance, that merely provides a higher level of fade margin. The Cisco Aironet 1200 access point draws 8 Watts RMS. A low cost 500 W UPS will power these units for four hours or more once the UPS batteries are fully charged. Be sure to fully charge the UPS and configure it to not sound an alarm when it is unplugged from the wall before using it this way. A battery pack and DC-to-AC converter can also be used. If the access point is placed in the ceiling, it can be secured with wire ties or duct tape. I dislike duct tape for this because it never completely comes off. Do not lay it on the ceiling tiles because the antennas will point up instead of down. If you are going to the trouble of placing the access points in the ceiling you might as well point them the right direction. Wire ties or anything else placed in the ceiling must meet the fire code standards.

## *Centralized Site Survey Tools*

Another way to do a site survey is to use a software tool designed for this. Trapeze Networks, Ekahau, Airespace, Aruba Wireless Networks, AirMagnet, and others are commonly mentioned in the trade press. With most of these tools, a floor plan is imported into the program. Using this floor plan and built-in values for the effect of common building obstructions, the program shows where to place the access points. The better programs can adjust this for the number of users and expected traffic levels.

These tools also attempt to implement centralized management of the wireless network after it is in operation. Management is discussed later in this tutorial.

These programs are expensive. Prices range up to \$10,000. Generally, they are justified not on the basis of the initial site survey, but on the ongoing network surveillance and management functions that they can do.

### *Do Not Bother With a Site Survey*

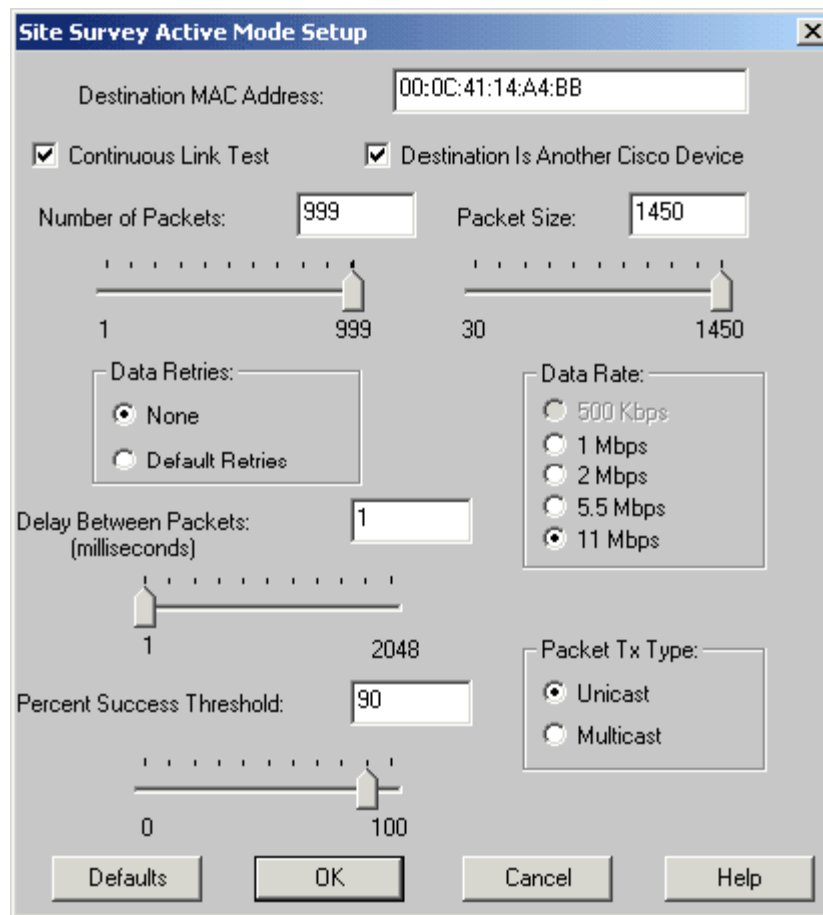
The last school of thought on site surveys for wireless LANs is: don't do one. The thinking here is that access points are so cheap it makes more economic sense to just install a few extra ones rather than paying staff or someone else to do a site survey. Using this approach, the access points are placed where a best guess suggests they go. The signal strength is turned down when an access point sends the signal into an undesirable area. Additional access points are placed in any dead areas. If the deployment will require 7-10 access points or less, the economics and simplicity may favor not doing a true survey. However, the number of wasted access points and/or problems caused by too much overlap could make it worth the cost if the wireless network gets above 15 to 20 access points. Anything larger than this without a survey and you're asking for long-term trouble. The idea of not doing a survey is an interesting concept that I have yet to try.

### *Notes on Surveying*

Although available cards, antennas, and access points should conform to 802.11 and WiFi standards, there can be deviations. If possible, before beginning the survey, obtain a sample set of the equipment to be deployed in the final network. Testing with the actual equipment to be used in production results in a much more accurately designed wireless network. Also, a digital camera can be used to photograph mounting problems or document the site survey. Doing this makes it easier to find the access points later. It may be helpful to note the time of day and traffic patterns while surveying. Doing surveys at night when there are no people around may be desirable for convenience but may not give an accurate picture of the environment when the wireless network is being used.

### *Verifying the Layout with Throughput Tests*

At the end of the site survey, the access points should be mounted in the correct locations for a throughput test. This ensures that the network is capable of handling the expected traffic. The site survey process uses a low traffic level. A test with real data rates is needed to confirm that the wireless network will work. It is difficult to both easily and cheaply simulate real user traffic on a wireless network. The site survey tool for the Cisco Aironet 350 NIC can do a form of this from the Site Survey screen, click on the Setup button. This screen appears.



**Site Survey Active Mode Setup**

Destination MAC Address: 00:0C:41:14:A4:BB

☒ Continuous Link Test      ☒ Destination Is Another Cisco Device

Number of Packets: 999      Packet Size: 1450

1 ..... 999      30 ..... 1450

Data Retries:   
☒ None   
☐ Default Retries

Data Rate:   
☐ 500 Kbps   
☐ 1 Mbps   
☐ 2 Mbps   
☐ 5.5 Mbps   
☒ 11 Mbps

Delay Between Packets: 1 (milliseconds)   
 1 ..... 2048

Percent Success Threshold: 90   
 0 ..... 100

Packet Tx Type:   
☒ Unicast   
☐ Multicast

Defaults      OK      Cancel      Help

[SA-Wire-WP1-32]

This allows a continuous test to be run. Another way to do this is to use a series of workstations or laptops to send FTP file transfers. You may even want to turn on all of the interference sources at one time to check their effect. Don't burn up those microwaves! While doing this verification test, consider especially the errors rates. Having a high data rate, but excessive errors, which call for retransmission, is the same as a low data rate without errors. However, there will always be errors in a wireless network. The point is to keep the CRC errors below 10 percent. Oppenheimer and Bardwell have a detailed discussion on this procedure.

While the throughput test is running, repeat the site survey, at a much faster pace this time, to check for coverage and seamless roaming within the coverage area.

## Deployment of Wireless Networks

With the site survey process completed, it is time to permanently install the wireless access points. Before installation, several configuration tasks should be done.

### *Access Point Naming Plan*

To track and manage the wireless network, each device should have a name. This name needs to follow a scheme that will make sense to the next network manager when they get a call in the middle of the night saying that something has failed. It may make sense to me for the pager to say "the fetlock is not responding", but it will not to everyone. More useful is "dalap23" or something similar. In any case, good written documentation with maps of access point locations is the only truly useful approach for networks of size. As part of this naming plan, decide what SSIDs to use.

## *Access Point Configuration*

Access points come out of the box with a default IP address, SSID, channel assignment, and power setting. The IP address should be static, not dynamic. These could be set on each device before it is put in place. Another option for large deployments is to note on a map the MAC address of each access point as it is installed. DHCP will assign an address when the access point boots. The administrator can then remotely connect to the access point to make all the required settings. Keep in mind that once the IP is changed, connectivity will be lost and a new connection will be required to the new IP address.

## *Access Point Mounting*

The location of each access point was determined by the site survey. The access point model and the building's construction determine the method for permanent placement of each access point.

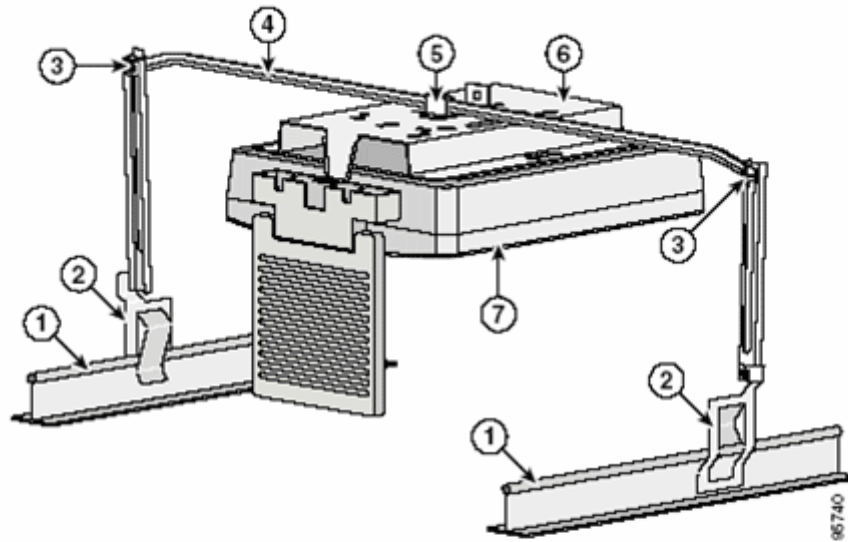
The easiest mounting is in a typical modern office building with a suspended ceiling. There are several methods commonly used to place access points in this space. Let's go through them from least desirable to preferred.

The easiest is to just place the access point on a ceiling tile. These devices do not weigh much. A ceiling tile can support this weight without any problem. The reason not to do this is the high likelihood that the access point will fall out of the ceiling as soon as someone moves any of the nearby tiles. Access to this space is required in order to maintain and service equipment. This method also points the antennas upward on models that have fixed antennas. Cisco for one recommends that the antennas point down (toward the space to be covered by the signal).

The next method uses plastic wire ties to secure the access point to any nearby structure. For example, when the APs were placed in the ceiling above the hall for the site survey discussed in this tutorial, the bracing for the air conditioning ducts was used. This is a structure that is seldom disturbed. By hanging the access point from this area, the antenna can hang down as prescribed by Cisco and others.

An access point can be secured to a wooden 2 x 4. Then the wood can be suspended across nearby supports. This almost certainly does not meet fire safety requirements.

The best method for non-secured installations is a standard T-bar box hanger. Here is the illustration from the Cisco 1200 access point installation manual showing this method.

*Mounting Bracket Parts*

1	Suspended ceiling T-rail	5	Bracket mounting clip
2	T-rail clip	6	Access point mounting bracket
3	Height adjustment screw	7	Access point
4	T-bar box hanger		

[NA-Wire-WP1-33]

From [www.cisco.com](http://www.cisco.com)

With this style of installation, the access point sits just above the ceiling tiles and the antenna points downward.

## *Electrical Power*

Each access point requires a source of electrical power. Even though these devices use low voltage DC, they expect to be plugged into a standard outlet. This requires either AC power at each access point or PoE. Generally, Power over Ethernet is far easier and cheaper than placing an outlet at each location. The IEEE standard 802.3af for PoE is new. Not everyone supports PoE and some vendors may provide PoE that does not comply with the standard. For example, Cisco provides PoE as the only option on their access points but only announced full PoE support on some Catalyst options in February 2004. Use the PoE device sold by the manufacturer for your access points unless you are certain that an 802.3af-compliant device can be used to deliver the power.

## *Physical Security*

None of the discussed methods for AP mounting provide any physical security for the device. Mounting access points out of sight in the false ceiling space provides only basic security. If someone looks in this space, the access point is easily stolen. The Cisco 1200 series access point comes with a bracket that can be secured with a padlock. The best security is to use a ceiling or wall mounted box. An example of this type of device is the WBC1 by Hubbell Premise Wiring at [www.hubbell-premise.com](http://www.hubbell-premise.com). Here is such an enclosure with a Cisco access point inside.



[NA-Wire-WP1-34]

From [www.hubbell-premise.com](http://www.hubbell-premise.com)

## *Safety*

Various codes must be adhered to during installation. For example, when installing a Cisco 1200 access point in the air space above a false ceiling, Cisco requires it to be mounted horizontally so that the antenna points down in order to meet fire safety requirements in addition to the radio performance needs. The access point itself meets all of the fire safety requirements of the National Electrical Code (NEC) Section 300-22. If power is delivered to the device using the Cisco PoE device, then the power supply unit must be kept out of the same air space. The UTP cable connecting the power supply unit to the access point can be in the air space, but it must be plenum rated. The NEC requires any mounting bracket to be grounded to building ground. There are several books and manuals on how to ground network equipment inside a building. The best sources are the BICSI Telecommunications Cabling Installation Manual and Volume 1 of the BICSI Telecommunications Distribution Methods Manual ([www.bicsi.org](http://www.bicsi.org)). These manuals tell you exactly how to do it using accepted industry methods, while referring you to the standards for backup on why it is done the way they say. If you are unsure if a device can be placed in the plenum space, see if it is UL 2043 rated. Everything that goes in the air-handling space must be rated for use there. This includes all the mounting devices such as duct tape, wooden boards, and wire ties. If it is not properly rated, don't use it.

## *Appearance*

In some environments, appearance is as important as performance. If the antennas must be mounted where they can be seen, then a patch antenna may have to be used instead of a more efficient Yagi. The patch antenna style is the least obtrusive. These can be mounted on the wall of a hallway or conference room. As previously shown, the antenna pattern is a flat wedge. This may require two antennas at opposite ends pointing at each other in order to cover the space a single omnidirectional antenna sticking down out of the ceiling could do. To further hide the wireless network equipment, it may have to be painted. In general, the bits and pieces of a wireless system can be painted. However, do not use any paint that contains a metallic substance, such as graphite, carbon, red oxide, or metallic flakes. This is especially true for the antennas.

Antennas may also be hidden in suspended ceilings by using the Armstrong i-ceilings Antenna Panel ([http://www.armstrong.com/commceilingsna/cm\\_iceilings.html](http://www.armstrong.com/commceilingsna/cm_iceilings.html)). These panels come with several antennas built into them. The panel itself looks exactly like a typical ceiling tile from the bottom.

## *Redundancy*

To maintain a reliable network, access points can be interconnected for backup. One unit is set as the primary and the other as the standby access point. Using the Hot Standby Routing Protocol (HSRP), the backup unit can seamlessly assume the load of a failed primary access point.

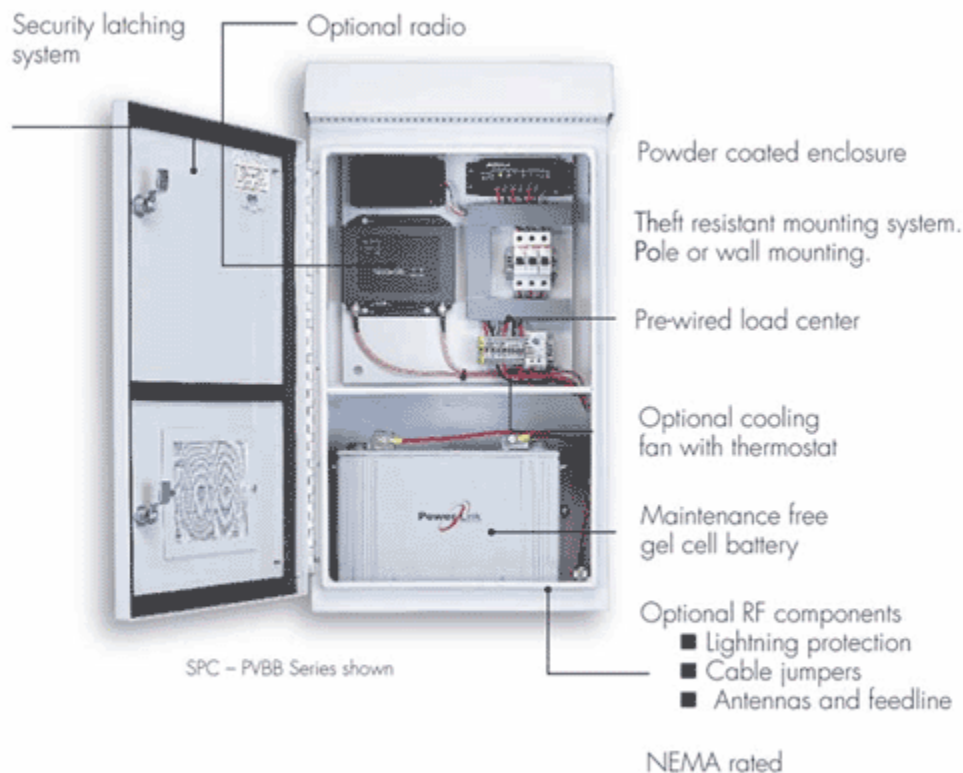
## Warehouse Deployment Considerations

When the wireless part of the network moves from inside a temperature controlled office building to a warehouse, some deployment changes are required.

Every warehouse is different. The main problems in a warehouse are long distances from the LAN room to the access points, temperature extremes, and signal blockage. Deployment in a grocery distribution warehouse illustrates these issues. In this kind of warehouse, one of the first problems encountered is distance. The set of warehouse buildings is interconnected, but in total they cover several acres. Each access point is connected back to a switch port. The distance limit is overcome by chaining a series of hubs from the access point's switch port in the network room to the access point. Recall the old Ethernet 5-4-3 rule. When coming off of a switch port, each access point is in its own collision domain. This allows the maximum Ethernet segment distance to be used from the switch port to an access point. At the low data rates used in the typical warehouse system, this works quite well.

The second difference in a warehouse setting is the ambient temperature. In a grocery warehouse, some products are stored in a -13 degrees F freezer in one building, while next door the paper goods are allowed to climb well above 100 degrees F in the summer. To protect the access points in the freezer, a heater was added to each box containing an access point. These boxes are rated to the NEMA4 specification for use in hostile environments. NEMA is the National Electrical Manufacturer Association ([www.nema.org](http://www.nema.org)). There is a range of NEMA ratings with NEMA3R, 4, and 4X being the most commonly used for radio equipment mounting. Each one is rated for a different combination of factors. For example, the NEMA4X box is rated for protection against falling dirt, rain, sleet, snow and windblown dust, splashing water, hose-directed water, and corrosion. They are also undamaged by external formation of ice on the enclosure.

Here is a typical NEMA box.



[NA-Wire-WP1-35]



From [www.talleycom.com](http://www.talleycom.com)

These boxes support heaters and cooling fans as required.

This is an example of an access point in a NEMA box in the warehouse. The white tube sticking out the bottom is an omnidirectional antenna. Each of these is powered with 110 AC from an outlet run to each access point. Providing an electrical outlet for each access point is an added expense over PoE.



[NA-Wire-WP1-36]

Signal blockage problems in a grocery warehouse are interesting. Here is a photograph of the inside of this warehouse.



[NA-Wire-WP1-37]

Notice the large number of metal shelves. On these shelves are product containers made of metal.

Many of the containers hold water in one form or another. This is a very unfriendly environment for radio waves. To work around this, the signals sent are kept very simple. This system uses a Symbol Technologies frequency hopping radio link at 2 Mbps. To simplify things even more, the client devices used by the warehouse handlers create a telnet session back to the central server. This keeps data errors to a minimum. In this warehouse, some of the client units are handheld and others are forklift mounted. The forklift unit is in two parts. On the forklift photo, the screen at the upper left is the display. The scanner is similar to the handheld unit shown next. It is in the lower right of the forklift photograph.

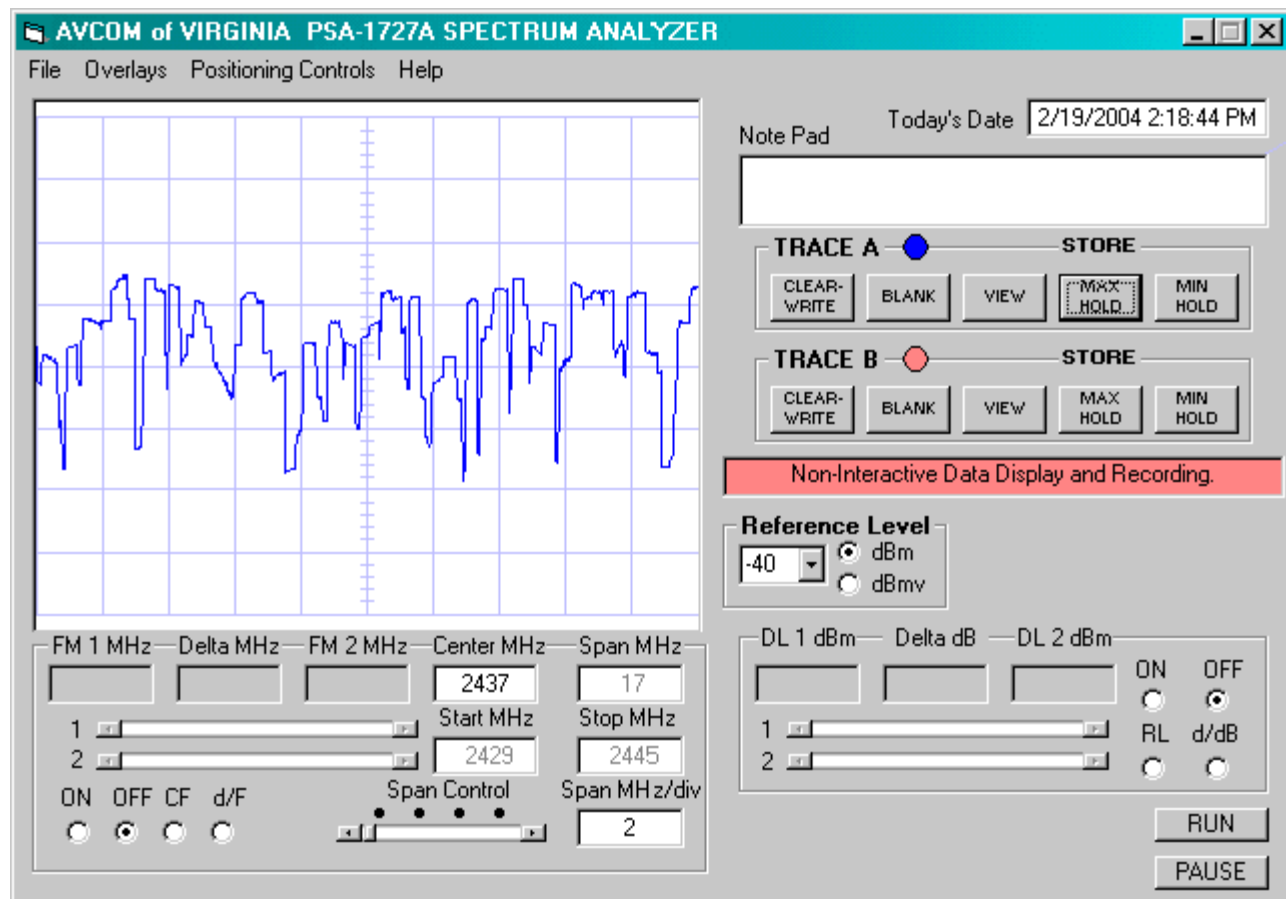


[NA-Wire-WP1-38]



[NA-Wire-WP1-39]

Frequency-hopping signals appear on a spectrum analyzer like a combination of FM radio and DSSS signals. Here is a screenshot captured over three minutes while the network was experiencing low activity levels.



[NA-Wire-WP1-40]

Notice that the pattern shows that the system does exactly what it says, hopping from frequency to frequency. This hopping helps to avoid interference from other radio signals in the area or signal blockage from the structure.

## Campus Area Network Deployment Considerations

Deploying a point-to-point campus area network link is similar to the local area network. A point-to-point link uses two access points set to bridge mode. In this mode, they operate just like the old wired bridges. If the MAC address of the destination is not on their side of the network, the bridge forwards the frame to the other side. In this case, the bridge is not a single box with two ports, but two radios talking to each other between sites. This is still a layer 2 connection of a single network that is now in two segments in different buildings. The main differences between the local area and point-to-point campus area networks are a greater chance of interference from other signals, line of sight requirements for the radio signal, antenna type, and equipment mounting problems.

Outside site surveys concentrate on the first two problems: finding interference and ensuring a clear line of sight. Finding interference is the same procedure used for inside locations. Use a spectrum analyzer, the site survey software built into the radio being used, or a wireless NIC. The line of sight requirement is important for an outdoor point-to-point link since these typically use the 5 GHz unlicensed frequencies. As discussed above, these frequencies are highly attenuated by vegetation and the atmosphere itself. In addition to the visual line of sight, the radio line of sight, as defined by the Fresnel Zone, must be clear. The Fresnel Zone is discussed in more detail in [Laganieri](#). Fresnel Zone obstruction can come from any angle, not just from below. Basically, Fresnel Zone clearance means very little that affects the radio signal can intrude into an elliptical zone around the visual line of sight between the two antennas.

For a point-to-point campus area link, a directional antenna is best. This can be a panel or grid antenna as discussed above. The tighter the beam, the higher the power received at the other end. This translates into longer distance and a more reliable connection. Security is also improved by using a tighter beam because the signal is more difficult to intercept, but there will always be leakage into the surrounding area.

Once the site survey finds an unused channel and a clear line of sight is identified, then the equipment can be mounted. Equipment mounting is frequently the main problem in outside wireless networks. Let's look at an actual deployment as an illustration. Two buildings are to be connected with a wireless bridge. The purpose of the wireless connection is to show students on this campus how such an installation is done as well as practice the management of a link like this. The first building is a two-story building, surrounded by trees. Because trees surround the building, the obvious approach is to mount the antenna on the roof of the building. In this case, there is an unused, non-penetrating mount already on the roof. A non-penetrating mount can be used on flat and peaked roofs. This is a quick and low cost solution to outside mounting.



[NA-Wire-WP1-41]

This solution works from a radio frequency perspective, but not for teaching. The only access to the roof is via a flight of narrow, dark stairs through a hatch in the ceiling.

The next option to be considered was to place the unit on the side of the building clear of the trees and near a window. The students could look out the window and see the radio/antenna combination. There is a location on the building currently clear of trees. It is outside a meeting room window. Of course trees grow, but this location should work. The only problem is that the tenant does not own the building. This is a very common business practice. The tenant occupies the entire building. All of the signs on the building and the surrounding area carry the tenant's name. However, to mount something to the outside of the building, the building's management agent must give permission. To obtain permission to mount this radio to the side of the building, the following was done over a span of several weeks.

Met with a representative of the building owner onsite to examine the proposed location. Explained to the representative the means of mounting and purpose of the device.

Supplied detailed documentation on the unit including size, weight, and method of attachment.

After receiving tentative approval, the building owner asked for a written request.

A week after submitting the written request the management company asked for a letter from the neighboring building owner agreeing to the deployment.

All of this took a month. Another way of mounting the equipment that bypasses the permission problem and solves the student access problem is to mount the equipment inside the building. This is an outdoor campus area connection, but that does not mean the equipment has to be outside. An arm, similar to the type used to mount a television, can be mounted to the structural ceiling. The only problem with this method is signal blockage caused by the glass in the window. Some reflective coatings have a metallic base. In this building, there is no significant blockage.

The second mounting consideration for any outside connection is water intrusion. Keeping water out of the radio, the cables, and the connectors is critical. Failure to do this is the main cause of outside equipment failure. There are several ways to accomplish this. No one agrees on the best way. The important things to do are to use drip loops and to seal the connections. The drip loop keeps water from running along the wire to the outside unit. To seal the connection, the most common method is three wraps of electrical tape going in opposite directions. First is a layer of 3M Scotch 33+ tape, then 3M 2210 vinyl mastic tape, and finally another layer of 3M Scotch 33+. The first layer of electrical tape creates a protective layer between the connector and the mastic, which is sticky. The next layer of the vinyl tape covers the mastic and keeps the gooey stuff from sticking to something it should not, as well as keeping out the water. For additional protection the mastic can be covered with three layers of tape instead of one. The first is wrapped from bottom to top, then from top to bottom, and finally a last one from bottom to top. When wrapping any of the mastic or tape, start at the bottom and wrap upward. This creates a shingling effect to help keep water out. Also be sure that the tape lays down nice and flat with no bubbles or bulges. The mastic discussed above is basically a thick sticky tape. It is sticky on one side. The sticky material is covered with a peel-off cover. This substance is about 1/8" thick.

A second way to seal the connection is to use a product called CoaxSeal. ([www.coaxseal.com](http://www.coaxseal.com)) Coax-Seal is a putty-like material in tape form. Waxed paper keeps it from sticking to itself. Cisco mentions this method in some of their documentation.

The third outside mounting problem is delivering power, data, and lightning protection to the device. If it uses PoE, then one cable is enough. The cable must be outdoor-rated. Shielded cable is best, but the connectors for this type of cable are difficult to work with. Special connectors are available that have room for the larger than normal outside jacket that an outdoor-rated shielded cable has around the wires. Then the shield must be connected to the connector. The shield attachment is the semicircular part shown below.



[NA-Wire-WP1-42]



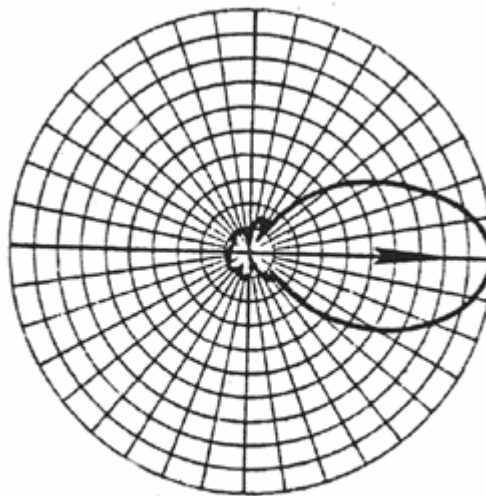
From [www.cablewholesale.com](http://www.cablewholesale.com)

For the short connection from the side of the building to the radio unit, a steel conduit with outdoor-rated fittings can be used. This avoids the need for special cable and connectors. Any radio device mounted outside must be grounded to a single point ground for the building. This is primarily for lightning protection. There are volumes written on the topic of lightning protection because few agree on exactly how to do it. The safest thing to do is to follow the NEC Article 250 and 810 requirements. Article 250 details how to create the ground point connection to the building ground. Article 810 details the requirement for a lightning strike surge protector on the data line coming into the building, unless the line is in steel conduit. The shield or the steel conduit must still be grounded where it enters the building. The BICSI manuals are a very good source for the details on how to accomplish this. Somewhere in the data line, a UTP surge suppressor should be inserted between the outdoor unit and the inside network. An example of this type of device is the IX Data Protection device made by PolyPhaser. PolyPhaser is a major manufacturer of lightning protection devices ([www.polyphaser.com](http://www.polyphaser.com)).

Another frequently encountered outside mounting problem is the need to separate the antenna from the rest of the radio. This is done by attaching a cable with the proper connectors between the radio and the antenna. Do not make this distance any greater than absolutely necessary. Every foot of cable reduces the signal strength. Be certain that each connector is the correct impedance, which is 50 ohms for this type of equipment. If you buy approved parts this will not be a problem.

When a highly directional antenna is used for the point-to-point link antenna, aiming becomes an issue. Some radios include a utility program or a set of lights to guide the aiming process. Over the distances of a campus area network connection, this is not a major issue, but always check the connection for maximum signal strength.

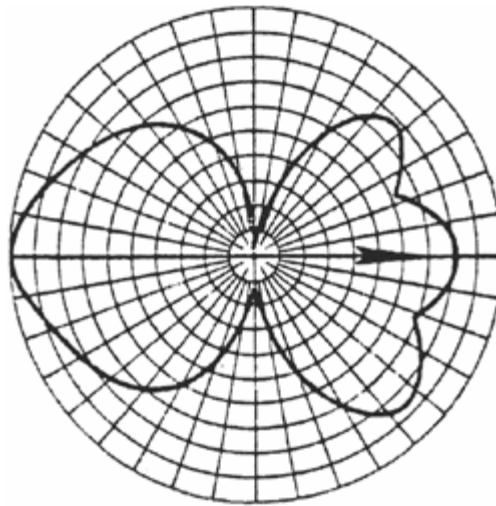
In some environments, depending on the size and shape of the antenna required for the point-to-point link, ice formation could be a problem. Ice always degrades the antenna's performance, which is one reason for a fade margin. The higher the frequency, the worse the problem. Studies on the phenomena attribute it to the following factor. The dipole elements of an antenna radiate radio waves into free space. The impedance of free space is 377 ohms. If the air surrounding the elements is replaced by ice, which has lower impedance, then the impedance match and radiation pattern of the antenna will change. For example, for a 10-element Yagi antenna at 502 MHz, the radiation pattern looks like this.



[NA-Wire-WP1-43]

From [www.tiltek.com](http://www.tiltek.com)

When coated with 0.20 inches of ice, the radiation pattern looks like this.



[NA-Wire-WP1-44]

From [www.tiltek.com](http://www.tiltek.com)

In this situation, for these antenna sizes, the only answer is a generous fade margin. Larger antennas can be protected with covers or heaters can be added. If the distance of the link is very long, these solutions may have to be considered.

## Troubleshooting

Once the network is in operation or during the site survey process, problems may occur. Most of these problems will be the result of interference or limitations in the signal handling ability of the equipment.

### Types of Wireless Network Errors

#### *Interference In All Its Forms*

Wireless networks see the following types of interference:

- Narrowband
- All band
- Adjacent channel
- Co-channel
- Multipath

Narrowband interference is basically another signal at a single or narrow range of frequencies. As such, it blocks out part of the spread spectrum signal. An advantage to spread spectrum technology is its ability to work around limited narrowband interference. To get rid of the narrowband interference, shield it, turn it off, or change channels on the wireless network equipment.

All band interference is from one end of the band to the other. A microwave oven is an example of this type of interference. About the only solution to all band interference, other than getting rid of the

source, is to change bands, such as from 802.11b to 802.11a.

Adjacent channel interference is produced by co-locating access points where the channels somewhat or completely overlap. A spectrum analyzer or a program that will identify all of the access points is required to detect this problem. To prevent this, do not use channels that overlap. Move the access points far enough apart so that the cells do not overlap, or turn down the power.

Co-channel interference is a direct overlap of channels. An example would be two different organizations using the same channels. One is on floor 1 and the other is on floor 2 or in an adjacent office on the same floor. A spectrum analyzer or a program that will identify all of the access points is required to detect this problem. To prevent this, use channels that do not overlap, move the access points far enough apart so that the cells do not overlap, turn the power down, or change the orientation of the antennas -- one to horizontal and the other to vertical.

Another type of interference is multipath. When a radio frequency wave leaves an antenna, it can be reflected. This creates multiple wave fronts, one for each reflection point. Some of these waves go off in space, but others reach the receiving antenna along with the original wave front. Since the reflected waves cover the distance from the transmitter to the receiver in a different time interval than the original wave, there is a delay between the arrival of the original wave front and the reflected waves. The time between the arrival of the original wave and the last reflected wave is the delay spread. The value for delay spreads will vary. Multipath causes several problems including decreased signal amplitude (downfade), corruption, nulling out of the signal, and increased signal amplitude (upfade). With decreased signal amplitude, the reflected waves are added to the original wave. If the reflected waves are out of phase with the original wave, then a decrease in amplitude is seen. If a reflected signal is even more out of phase, then the reduction may be so great that the received signal cannot be read at all or only partially read due to corruption. This results in a low signal-to-noise ratio. In nulling, the phase of the reflected signal entirely cancels the original signal. When a reflected signal is in phase with the original signal, the total signal may be larger in amplitude. This causes higher signal strength than would normally be expected at the antenna, but still lower than the transmitted signal strength.

Multipath cannot be directly measured. Only its effects can be seen. From these effects, multipath is deduced. For example, if a link budget calculation is performed but the measured signal is less, then multipath can be a reason. Holes or areas where no signal is detected when doing a site survey may also be caused by multipath.

There is no single solution for multipath problems. Moving objects that reflect the signal or moving the antennas so as to avoid the multipath path are possible solutions. Antenna diversity is another possible solution to multipath. Antenna diversity is the use of multiple antennas, inputs, and receivers. Several types of antenna diversity are commonly used. Non-active diversity uses multiple antennas and a single receiver input. Active diversity uses multiple antennas and multiple inputs to a single receiver. It reads the signal from one antenna at a time. Switching diversity uses multiple antennas and multiple receivers. It switches receivers based on the signal strength at each antenna. Transmission diversity transmits out the last antenna used for reception. It can alternate antennas for retransmissions.

In 802.11-based networks, interference of any type will show up as increased fragmentation, decreased transmission rates, and increased retransmissions.

## Technology Problems

In addition to interference, 802.11-type networks suffer from limitations inherent to the technology.

### *Hidden Node*

The hidden node problem occurs when one node cannot hear another node transmitting. This occurs when they are separated by an obstruction or when they are too far apart. Both nodes can see the access point, but not each other. This causes excessive collisions on the network, retransmissions, and therefore reduced throughput.



Degraded throughput on the network is the common sign of hidden node. Examining the layout of the network may show hidden nodes. Moving or disconnecting possible hidden nodes and then examining the throughput may show these as well. This is a trial and error process.

The solutions for hidden node depend on the type of network. For a LAN solution, these include: use of RTS/CTS, adjusting the point where the wireless packets are fragmented, increasing the power used by the far nodes and decreasing the power used by the nearby nodes, removing the obstacle, moving the node closer, or using a polling mechanism to control access. RTS/CTS does not solve the hidden node problem, but it may improve the throughput if the node or obstacle cannot be moved.

To enable RTS, lower the RTS threshold. Cisco recommends adjusting the RTS/CTS parameter by reducing the packet size from its default of 2048 to a value where CRC errors become acceptable. Adjusting the fragmentation level to a value where more and more packets are fragmented may increase throughput as well. By being smaller in size, the packet may make it to the access point before colliding with another packet.

## *Near/Far*

The near/far problem occurs when there are nodes near the access point that have high power settings and other nodes far from the access point with low power settings. The near, high power nodes overwhelm the far, low power nodes. To detect this, check the network design. Look at the power output level of the nodes. Possible solutions to the near/far problem include: reducing the power of the nearby nodes, increasing the power of the far off nodes, moving the far off nodes closer to the access point, and moving the access point to a more central location.

## *Low Throughput*

The throughput of a wireless system is dependent on:

- Amount of interference
- Type of interference
- Security solutions that add overhead
- Distance, since the data rate falls off as distance increases
- Older, slower computers
- Fragmentation
- Use of RTS/CTS

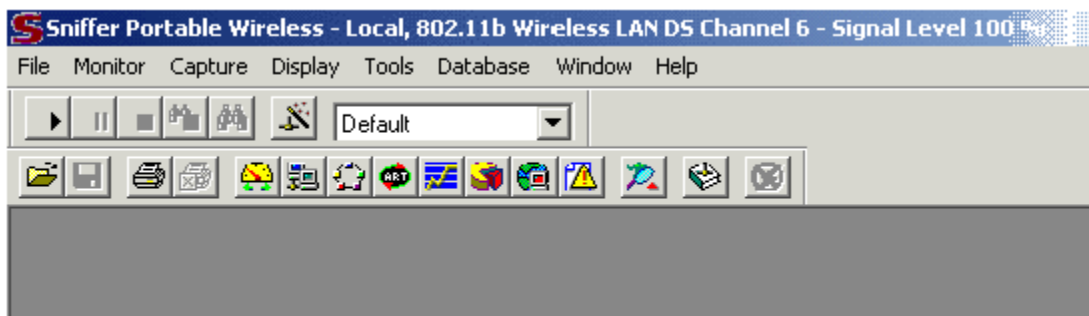
The most common solution to low throughput is the co-location of access points in a single area. For 802.11b, for example, three non-overlapping channels are possible: 1, 6, and 11. A single AP will provide from 4.5 to 5.5 Mbps. In theory three APs should provide 15 Mbps or so. Of course it is possible to use fewer than three APs; two may be used on channels 1 and 11. This may make sense if three access points, each producing 4 Mbps, are compared to two producing 5.5 Mbps each. It may also make sense to force fragmentation thus producing smaller frames. This means that the lost frames when retransmitted are smaller. However, when a packet must be fragmented, this adds overhead because each fragment requires an ACK.

## *Fragmentation*

Fragmentation can be adjusted to improve efficiency on the network. If the network is experiencing high packet error rates, then increase the fragmentation threshold. This is done by starting with the maximum size and gradually dropping the threshold until an improvement is seen. As the frame size is increased, there is less overhead, but increased chance of collision. As the frame size decreases there is more overhead, but less chance of collision. Start with a setting of 1024 bytes. In a network where the average packet size is greater than 800 bytes, it may benefit the network to lower the fragmentation setting. Then see if performance improves. As Oppenheimer and Bardwell point out this can be determined by transferring a large file, such as 1GB, because the test data must be larger than the fragmentation threshold, and timing how long the transfer takes. Adjust the value in 100 byte increments above and below 1024 bytes and see when the most improvement occurs.

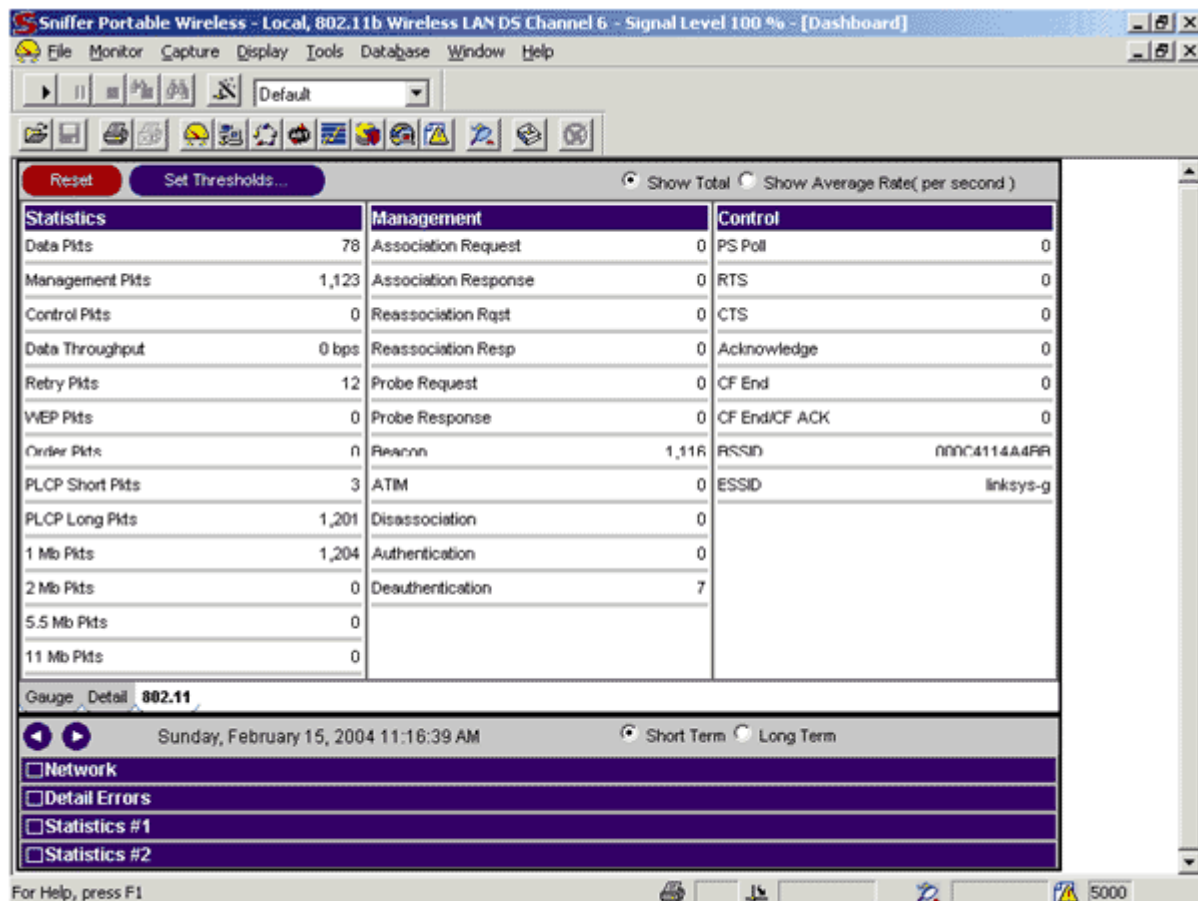
## Network Analyzer

The main troubleshooting tool for any network problem is the network or protocol analyzer. There are several on the market. On the paid side Network Associates Sniffer Wireless and Wild Packets AiroPeek are very good (<http://www.networkassociates.com/us/products/sniffer/home.asp> and [www.wildpackets.com](http://www.wildpackets.com)). For a free version, many use Ethereal ([www.ethereal.com](http://www.ethereal.com)). Let's look at Sniffer Wireless to see what one of these programs can do. When Sniffer Wireless is started, it looks like the standard program used for wired networks, except for a few additions. Starting at the top, we see that it has found a wireless network on 802.11b channel 6 with signal strength of 100%.



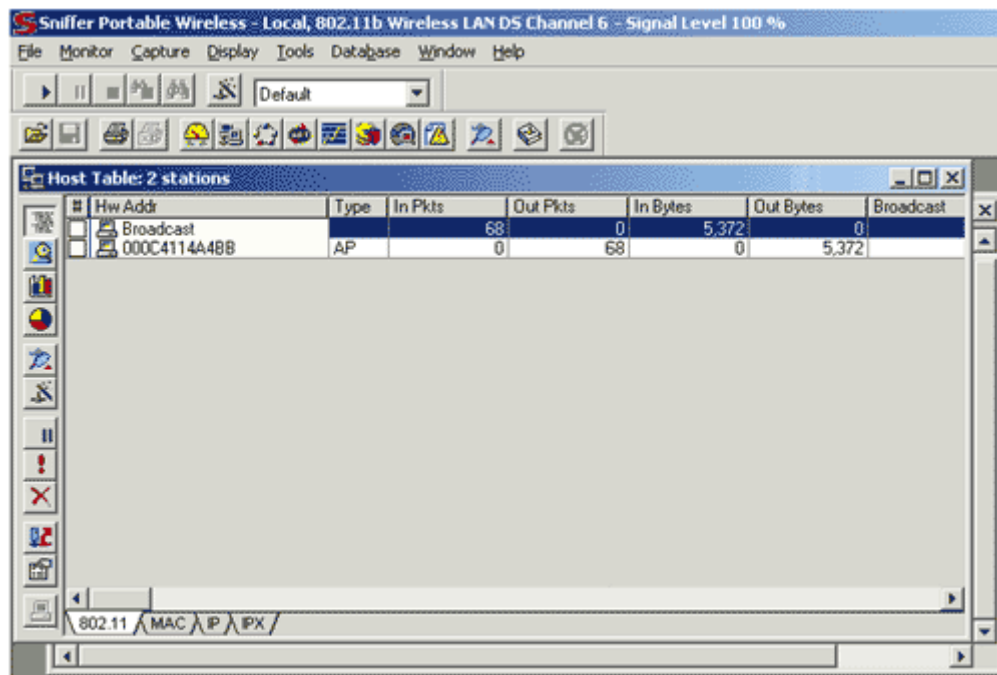
[NA-Wire-WP1-45]

The other changes from a wired network analyzer are mostly additional information. For example, on the Dashboard screen is a tab that when clicked provides details about the wireless network.



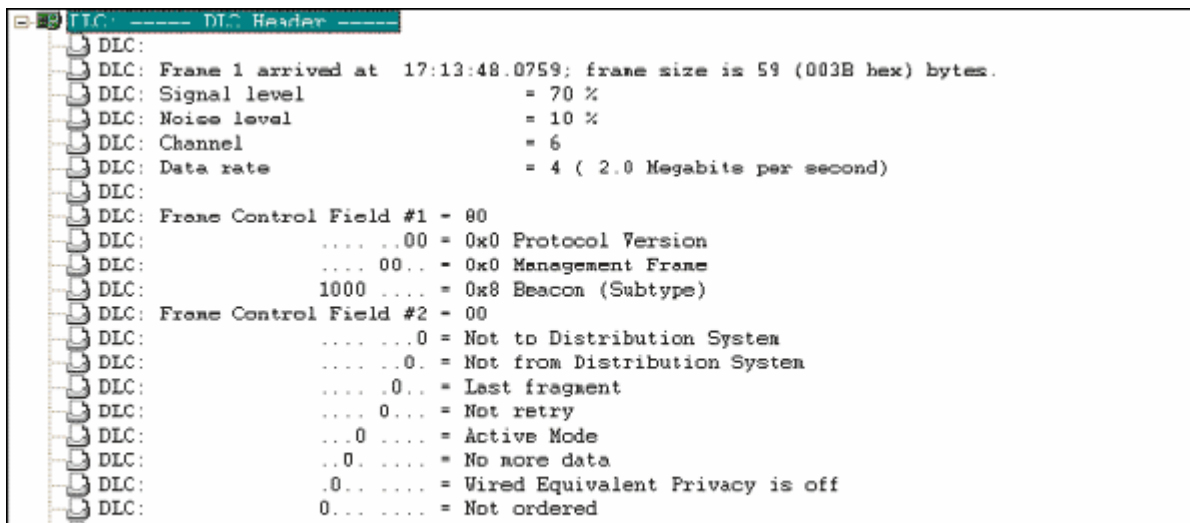
[NA-Wire-WP1-46]

The last major change is seen on the host table display, where it can be set to show only the wireless devices.



[NA-Wire-WP1-47]

Of course, like any protocol analyzer, Sniffer Wireless can be used to capture the packets crossing the air as well as the wires. Here is one example of such a capture. This is the beginning of a beacon frame.



[NA-Wire-WP1-48]

## Management

Once you install more than three or four access points in a wireless network, management of these devices becomes a headache. Out of the box, every access point must be managed, one at a time, using a telnet connection to the command line interface or through a web browser to a set of web screens. What everyone wants is a single centralized management program. This combination of software and hardware must be able to talk to all of the access points regardless of who made them. Many companies are working on this. No one yet leads the pack. Trapeze Networks RingMaster and the

other centralized site survey programs mentioned above do this now, to some extent.

Common features offered by these programs include these listed by Trapeze Networks for the RingMaster product:

- Monitoring for interference sources intruding on the wireless network
- Suggested or automatic adjustment of power levels to maintain seamless coverage of the facility
- Continuous or scheduled RF sweeps to look for unauthorized devices
- Automatic alerting of the management staff of rogue devices on the network
- Tracking of roaming history, bandwidth, and usage statistics per device and per user
- Location of devices on a floor plan by type of device
- Monitoring for configuration changes
- Enforcement of configuration consistency on the wireless network
- Comprehensive statistical history by wireless network, wired network, and user

For this purpose, Cisco offers the Wireless LAN Solution Engine. This is a combination of hardware and software. The hardware is a 1U single purpose server.

A hospital recently purchased the Cisco Wireless LAN Solution Engine to help manage their 450 access points spread over 20 locations. The server and software cost them over \$8,000. Other programs that are not wireless-specific can also be used to provide some centralized management of the wireless network at a lower cost. However, these are limited to basic management tasks, such as checking for device uptime and collecting data through SNMP. An example of these programs is WhatsUp Gold from Ipswitch ([www.ipswitch.com](http://www.ipswitch.com)). It can provide some centralized management at a lower cost than the specialized programs. At \$795, it is one-tenth the cost of the Cisco product, but cannot directly control the access points.

Regardless of the tools used to manage the network, the wireless network should be completely documented. For each access point the documentation should include:

- Location
- Make and model of the access point
- Access Point name
- VLAN assigned to
- Photograph of the mounting location so it can be found
- Mark on the floor plan showing the location
- Antenna used
- Power output setting

- Connector style
- How the unit is powered
- Assigned IP address
- Security settings
- Contact information

## Conclusion

In this tutorial, the tasks a CCNA-level staff person would be expected to do as part of a wireless network installation have been covered. The focus of this tutorial has been on the details of adding a wireless extension to an existing wired local area network. Keeping in mind the limitations of wireless connections and using the techniques covered here you should be able to successfully complete the installation of a wireless network in a variety of locations.

## References

Johannesson, Peter, *Wave Propagation through Vegetation at 3.1 GHz and 5.8 GHz*, Department of Electrosience, Electromagnetic Theory, Lund Institute of Technology, Sweden

Cheung, David and Prettie, Cliff, *A Path Loss Comparison Between the 5GHz UNII Band (802.11a) and the 2.4 GHz ISM band (802.11b)*, Intel Labs, Intel Corporation, January, 2002

CWNA Study Guide, <http://www.cwne.com/index.html>

IEEE 802.11 Working Group, <http://www.ieee802.org/11/>

Oppenheimer, Priscilla and Bardwell, Joseph, *Troubleshooting Campus Networks*, ISBN 0-471-21013-7

FCC, <http://www.fcc.gov/>

ETSI, <http://www.etsi.org/>

---

[NA-Wire-WP1-F02]  
[2004-03-25-03]