Wireless Network Site Verification and Analysis Tools

Joseph Bardwell – Connect802 Corporation
www.Connect802.com

After the Ladders Are Put Back On the Truck…

Your Wi-Fi network system was designed by an expert and consideration was given to signal propagation, attenuation through obstructions, signal corruption due to multi-path reflections, and other key RF issues. You took aggregate bandwidth capacity and user application requirements into consideration. You selected the right vendor's equipment to meet your specifications and then you ran the cable, screwed the radios and antennas up on the walls and ceilings, and turned the thing on. Now – will it do what was intended?

Post-installation verification and coverage gap analysis is, to either a lesser or greater degree, required after a Wi-Fi wireless network system has been brought on-line. For the hospitality sector, where guests at hotels, airports, or resorts are given limited expectations of performance, the post-installation efforts can be minimized. In a hospital (where patient monitoring is a critical function) or in a university or corporate enterprise setting (where high-capacity requirements must be met) the post-installation effort can be a complex, detailed, and time-consuming project by itself.

The present discussion is divided into two parts. Part 1, presented in this issue, describes fundamental verification methods and tools. Part 2, coming in the next issue, explores the role of RF spectrum analysis and the methodology for developing a mitigation and remediation strategy when problems are identified.

The Cheap and Dirty Ping Test

The simplest post-installation validation consists of connecting to the network with your wireless notebook computer and running a continuous Ping test back to the default gateway on the wired Ethernet side of the IP network. This is NOT a comprehensive test in any way but it does provide some degree of meaningful information regarding the operation of the wireless network.

With the Ping test running you now walk the site, making sure that your Ping responses don't time out. If more than 5% of your Ping requests are lost then you can assume that you're standing in a dead or severely weak coverage area. If it's an area that needs connectivity then you've got a problem. If, on the other hand, you have consistent Ping response times of less than 5 ms you can be confident that the network is operational to at least a minimum level of 802.11 performance.

```
Reply from 192.168.224.1: bytes=32 time=1ms TTL=64
Reply from 192.168.224.1: bytes=32 time=1ms TTL=64
Reply from 192.168.224.1: bytes=32 time=1ms TTL=64
Reply from 192.168.224.1: bytes=32 time=1ms TTL=64
Reply from 192.168.224.1: bytes=32 time=1ms TTL=64
Reply from 192.168.224.1: bytes=32 time=1ms TTL=64
Reply from 192.168.224.1: bytes=32 time=1ms TTL=64
Reply from 192.168.224.1: bytes=32 time=1ms TTL=64
Reply from 192.168.224.1: bytes=32 time=1ms TTL=64
Reply from 192.168.224.1: bytes=32 time=1ms TTL=64
Reply from 192.168.224.1: bytes=32 time=1ms TTL=64
Reply from 192.168.224.1: bytes=32 time=1ms TTL=64
Reply from 192.168.224.1: bytes=32 time=175ms TTL=64
Reply from 192.168.224.1: bytes=32 time=1ms TTL=64
Reply from 192.168.224.1: bytes=32 time=3ms TTL=64
Reply from 192.168.224.1: bytes=32 time=1ms TTL=64
Reply from 192.168.224.1: bytes=32 time=1ms TTL=64
Reply from 192.168.224.1: bytes=32 time=1ms TTL=64
Reply from 192.168.224.1: bytes=32 time=1ms TTL=64
Reply from 192.168.224.1: bytes=32 time=2ms TTL=64
Reply from 192.168.224.1: bytes=32 time=1ms TTL=64
Reply from 192.168.224.1: bytes=32 time=1ms TTL=64
```

Ping Test Results for a Typical, Properly Operating Wi-Fi Network

Shown above is a sample of what a Ping test might look like in a properly operating Wi-Fi network. Notice that there is one reply of 175 ms. When replies vary it's because Ping packets were corrupted in the air and were retransmitted through the automatic 802.11 retry mechanism. The Ping application saw the 802.11 retransmission/retry event as a time delay in getting a reply. Hence, Ping time variation is an indirect indication of packet corruption in the air.

Shown below is a sample of a Ping test in an environment that is not going to support consistent Wi-Fi service.

```
Reply from 192.168.224.1: bytes=32 time=173ms TTL=64
Request timed out.
Reply from 192.168.224.1: bytes=32 time=11ms TTL=64
Reply from 192.168.224.1: bytes=32 time=195ms TTL=64
Request timed out.
Request timed out.
Reply from 192.168.224.1: bytes=32 time=195ms TTL=64
Reply from 192.168.224.1: bytes=32 time=13ms TTL=64
Reply from 192.168.224.1: bytes=32 time=2ms TTL=64
Reply from 192.168.224.1: bytes=32 time=4ms TTL=64
Reply from 192.168.224.1: bytes=32 time=206ms TTL=64
Reply from 192.168.224.1: bytes=32 time=12ms TTL=64
Reply from 192.168.224.1: bytes=32 time=9ms TTL=64
Request timed out.
Reply from 192.168.224.1: bytes=32 time=22ms TTL=64
Request timed out.
Reply from 192.168.224.1: bytes=32 time=5ms TTL=64
Reply from 192.168.224.1: bytes=32 time=193ms TTL=64
Reply from 192.168.224.1: bytes=32 time=4ms TTL=64
Reply from 192.168.224.1: bytes=32 time=5ms TTL=64
Reply from 192.168.224.1: bytes=32 time=1ms TTL=64
Reply from 192.168.224.1: bytes=32 time=191ms TTL=64
Reply from 192.168.224.1: bytes=32 time=32ms TTL=64
```

Ping Test Results obtained in a Noisy, Error-Filled Environment

What's seen in the bad test result above is that not only do multiple requests time out but the overall Ping response times are completely inconsistent. In this case the

inconsistent Ping response times are an indication that something is disrupting the regular flow of data across the Wi-Fi network. From the Ping test alone you don't know what's causing the problem but you know that a problem exists.

Will a noisy, error-filled network like this work at all? Absolutely. Remember that when you're checking email or browsing the web the TCP protocol layer guarantees delivery of data through a comprehensive retransmission mechanism. If these were connection-oriented TCP data packets then TCP would retransmit each of the "Request timed out" failures until they finally got through. This network would work but users would perceive it as being shockingly slow.

Be careful. If you're the only user on the network (as you might well be immediately after it's installed) then your performance might seem to be acceptable. It's when multiple users try to access the system in the presence of noise and interference that lost capacity begins to become evident.

Comprehensive Data Throughput Testing

The Ping utility operates by sending a data packet using a connectionless protocol called ICMP (Internet Control Message Protocol.) An ICMP *echo request* is sent to the target IP device and the IP protocol stack knows, inherently, how to send the data block back with an *echo reply* frame. Ping, therefore, can disclose the round-trip time and the complete loss of packets but there is no indication as to how users, running real-world applications (like email, web browsing, or streaming video) will perceive the performance of the network. For this reason a comprehensive verification of wireless LAN performance must include a real-time data transfer test.

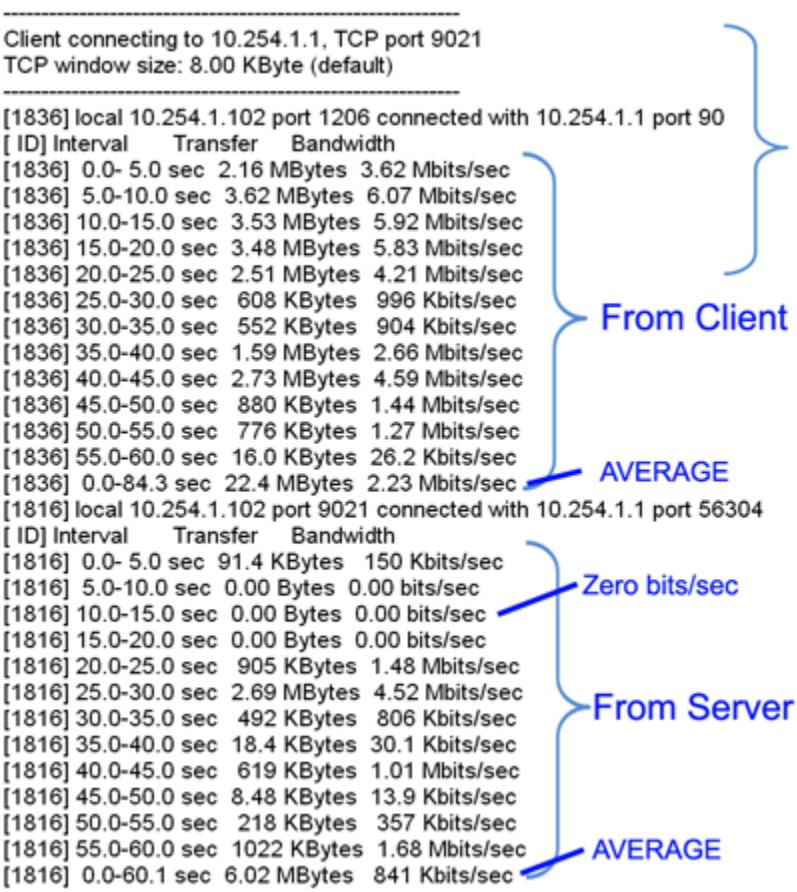
A simple performance testing tool called "iPerf" is freely downloadable from many different websites. The utility runs in an MSDOS window. A web search for "iPerf" will bring up a list of the many download sites from which you can obtain this software utility. You'll need two computers to run an iPerf throughput test. Create a directory on the root of your C: drive and copy the iPerf utility into it. Open an MSDOS window using *Run* from the Start menu and type "cmd" to access an MSDOS window. Use the CD command under MSDOS to change directories to "C:\iPerf" (or whatever you named your iPerf directory.) You'll install iPerf identically on both computers. One of them will be your iPerf server, the other your iPerf client.

Type "iPerf –help" for a complete list of commands. The simplest test can be performed using the following setup:

- On the server machine, type "iPerf –s" at the MSDOS prompt. This will activate the iPerf server function and the machine will be listening for incoming connection requests from your iPerf client.

- On the client machine type "iPerf –c 192.168.4.1 (using the IP address of the server machine.)

The iPerf utility now runs with output similar to the following:



Output from an iPerf Performance Test

Interpreting iPerf Performance Test Results

This discussion uses iPerf as an example of a performance analysis tool. There are other software tools available, some of which are very elaborate and sophisticated (and expensive) but the basic concepts presented here will still apply to assessing any performance analysis test result.

The first group of transfer results are those obtained when the iPerf Client sent blocks of data to the Server. Consider that this data transfer testing is reasonably close to real-world movement of data since the 8 Kbyte block of data must be broken up into multiple 1460 byte data segments for transfer with TCP, and receipt of the data must be acknowledged through the TCP sequence number and acknowledgement mechanism. Results like the 996 Kbps/sec or 904 Kbps/sec transfer rates are due to severe packet corruption such that even the TCP retransmission mechanism was unable compensate for 802.11 packet corruption. Remember, though, that at the end of the run the Average data transfer from the Client (22.4 Mbytes at 2.23 Mbits/sec) represents totally accurate data having been sent without ultimate loss; the TCP retransmission mechanism guarantees delivery of the data however long it takes (unless the TCP connection itself

is dropped which is possible when continuous, catastrophic packet loss occurs for periods of many seconds duration.)

In the second group the data is now being sent back from the Server side to the Client. Notice that there is a period of time from the start of the 5.0 second interval through to the end of the 20.0 second interval when 0.00 Bytes were transferred. Any 5 second interval with 0 Bytes transferred is catastrophic and here we see that fully 15 seconds elapsed with complete loss of connectivity. This is a bad thing. Further study shows that the 35.0 to 40.0 second interval only provided 30.1 Kilobits per second. The conclusion here is that while the Client hardware and 802.11 radio equipment seem to be able to successfully transmit to the Server-side receiver there's something about the Server's 802.11 radio that doesn't provide satisfactory service in this network system.

Applying the "Law of Reciprocity" to Troubleshoot This Problem

The physics professor would explain that the "Law of Reciprocity" includes the stipulation that whatever is experienced by an electromagnetic signal as it passes from a transmitter to a receiver is identical to that which is experienced by the signal when the roles of transmitter and receiver are reversed and the transmission is sent in the "other direction." For two transmitters operating with the same power output the rule can be stated simply as, "If you can hear me then I can hear you, even if your antenna differs significantly in gain or directional pattern."

The implication is that since the Client had no problem sending data to the Server there is nothing related to the antennas (gain, directionality, orientation, polarization – nothing) or to the environment (noise, interference, reflections, or other degrading characteristics) that can cause the Server to have problems sending to the Client. The Law of Reciprocity tells us that from the antenna cable connector on one antenna to the connector on the other antenna everything must have an identical impact regardless of which antenna is the transmitter and which is the receiver.

The problem must be related to either the Client's receiver circuitry or the Server's transmitter circuitry. The Server's 802.11 access point could be misconfigured at too low a power output level or it may not have a sufficiently powerful radio to operate in the specified environment. The Server's access point could also have experienced hardware failure related to the transmitter circuit. The Client's radio may have poor receiver sensitivity making it impossible for the Client to differentiate between the received signal and background noise or interference.

Comparing Data Transfer Testing to RF Signal Strength Measurement

When 802.11 signal strength testing is performed or when an RF spectrum analyzer is used during site verification there is no guarantee that a signal with appropriate strength or spectral characteristics will be usable by a receiver during the phase lock, demodulation, and bit recover process. For this reason a post-installation verification should always include actual data transfer testing with, at least, a Ping test. A full performance test (with a tool like iPerf) goes a strong step beyond simple Ping testing. Ultimately, a full post-installation verification should include actually running the

intended user applications across the WLAN. It should be noted that simply running the user applications will not provide insight into the actual data transfer behavior – for this a data transfer test is required.

The acceptability of the results are entirely dependent on the specified requirements for the wireless network being tested. The iPerf utility tests throughput based on the TCP/IP protocol which has guaranteed delivery of packets using a retransmission mechanism to overcome packet loss. This effectively emulates the performance of email systems, web browsing, and many database applications which also use TCP/IP. By exploring the iPerf help text it will be seen that simultaneous data transfer session can also be established and tested.

Isolating and Describing Problems

If Ping testing or iPerf testing indicates that there are problems with the network it's going to be time to explore the RF spectrum. In fact, walking through a site using an 802.11 analyzer or RF spectrum analyzer is always recommended as part of both the pre-installation activities as well as during post-installation verification.

There are two general categories of RF signal-related tools: packet analyzers and spectrum analyzers. When data is acquired using an 802.11 wireless LAN adapter it's received data packets that provide the analysis information. When data is acquired using an RF spectrum analyzer it's the display of power levels across a frequency range that provides analysis information.

802.11 adapters used by packet analyzers attempt to establish a phase lock on a coherent received signal. Once locked the adapter demodulates the RF signal to recover a bit stream. When an 802.11 adapter returns information relative to "noise" or "interference" it's actually a software interpretation of the degree to which the RF signal is successfully demodulated and the recovered bit stream is found to be valid. An 802.11 adapter cannot directly measure the energy level (dBm or mW) of background noise, nor, therefore, can it directly calculate "Signal-to-Noise Ratio" (SNR). The power level (dBm or mW) of a received signal presented using an 802.11 adapter is an algorithmic interpretation of an estimated power level. The algorithmic method used to calculate a dBm Received Signal Strength Indication (RSSI) varies from one manufacturer to another and while they tend to be reasonably consistent and sufficiently accurate for most purposes the dBm or mW power level reported by a tool using an 802.11 adapter to acquire data is, at best, an estimate.

One popular 802.11 tool is NetStumbler (freely available on the web from netstumbler.com.) It reports dBm signal strength and compiles tables of SSIDs and MAC addresses along with some simple signal strength graphs. The most widely used 802.11 analysis tool is the AirMagnet Laptop Analyzer which competes directly with the WildPackets AiroPeek WLAN Analyzer, Network General Sniffer Wireless, and other tools based on the 802.11 chipset. These tools go far beyond NetStumbler in that they capture and decode complete packet-level conversations to aid in troubleshooting

network configuration problems, isolating security exposures on a network, and confirm proper application software behavior.

Interpreting network protocol behavior is a complicated task and it takes significant academic training and years of practical experience before the nuances of packet-level interactions are readily understood. For this reason, full-featured packet analyzer tools have automatic, expert-system analysis capabilities built in. The expert systems evaluate network behavior and report on what may be over one hundred different problem events.

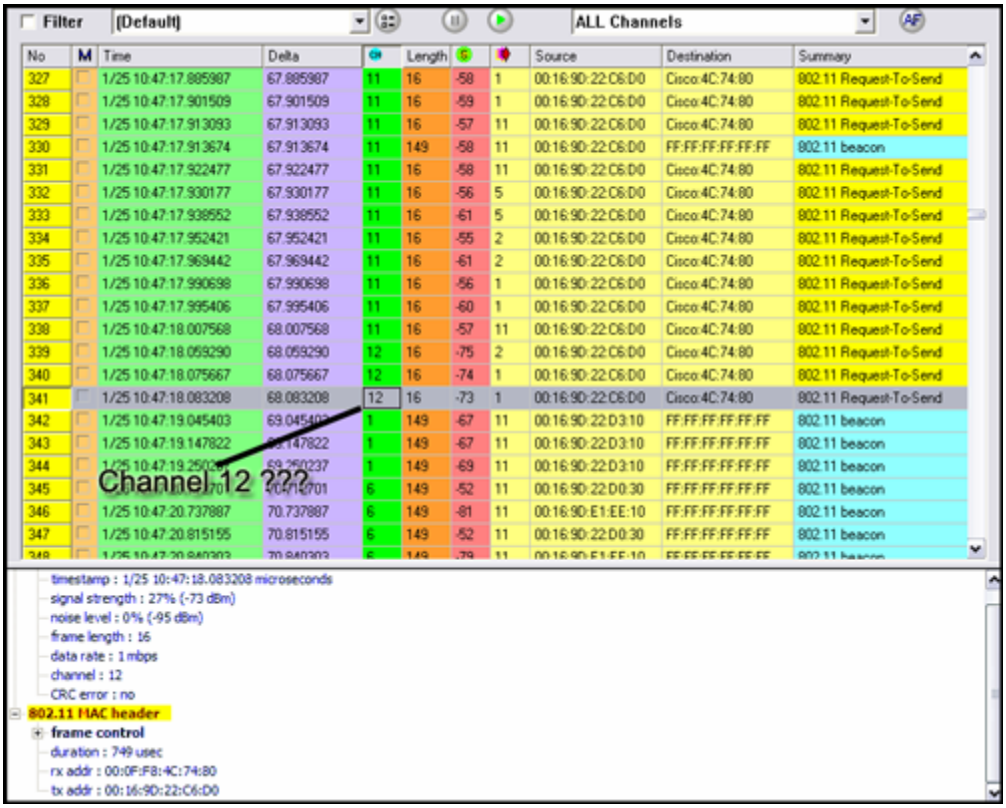
When considering purchasing a packet-level analysis tool there are three things that are always important to consider: how intuitive is the user interface relative to viewing core network statistics; how easy is it to extract information into a report format and does the tool provide automated reporting features; what is the degree to which the manufacturer supports different types of 802.11 adapters?

Most of the field use for an 802.11 packet analyzer will be related to looking at dBm signal levels, listing visible SSIDs and finding rogue devices.

802.11 Packet Analyzers

The 802.11 device driver that controls the Wi-Fi adapter in a device passes not only the extracted data packet up to the device's operating system but also includes header information related to the channel on which the packet was acquired, a relative measure of signal strength, and other basic RF-oriented information. An 802.11 chipset is incapable of providing the analog RF signal energy and frequency information that would allow a true assessment of interference and noise. That's the purpose for an RF spectrum analyzer.

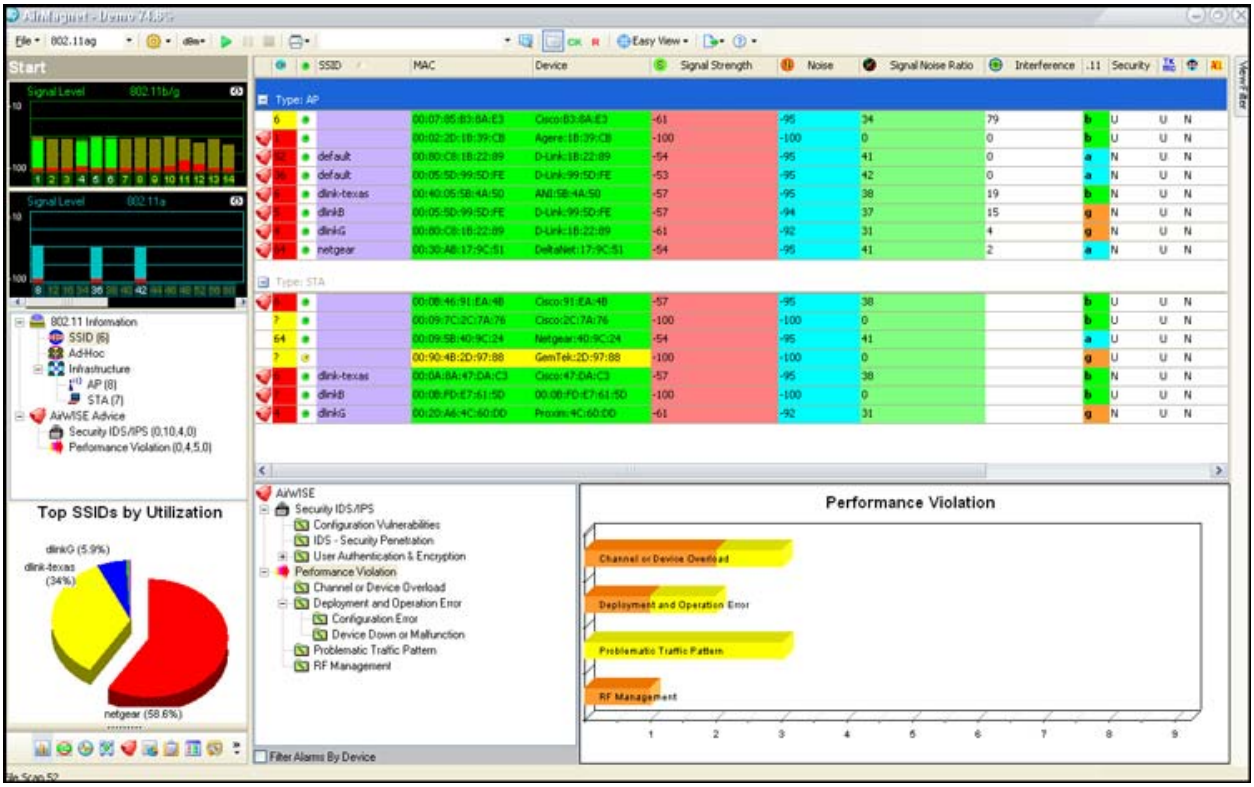
Packet analyzers can be simple network monitoring tools (like NetStumbler) which only report the basic signal strength and signal quality information. This information is extrapolated from the simple RF information provided by the 802.11 device driver. A full-function packet analyzer captures individual data packets and decodes their contents. This allows an experienced network engineer to evaluate the behavior of not only the 802.11 protocols but of higher layer protocols like DHCP, DNS, POP, SMTP, and the operation of TCP sequence numbers, acks, and retransmission events. Packet-level analysis allows detailed exploration of network configuration and capacity issues.



A Packet Analyzer Display of Individual Data Packets

In the Packet Analyzer Display image it can be seen that a device (MAC address 00:16:90:22:C6:D0) is sending a Request to Send packet to Cisco:4C:74:80 and is transmitting on 802.11 Channel 12. In North America, only Channels 1 through 11 are allowed by the FCC. This (and other) stations have evidently been misconfigured to operate using 802.11 standards intended for use outside North America. On the bottom of the screen display the detailed decode of the internal contents of the packet are shown. If one were to scroll down in the detail decode list the entire contents of the data packet would be revealed including the contents of unencrypted email, web page HTML, and anything else carried in a data packet.

Packet analysis, in conjunction with automatic expert system analysis of information, can quickly disclose significant behaviors on a network that would otherwise require lengthy, detailed exploration by an experienced network engineer.



Packet Analyzer Main Information Screen

Seen in a Packet Analyzer Main Information Screen is a synopsis of channel utilization, SSIDs, device MAC addresses, and associated signal strength and other useful information. This type of information is typical of all packet analyzers. A “freeware” packet analyzer application called WireShark (formerly called Ethereal) can be downloaded at no cost or, with an investment of between $1000.00 and $5000.00 tools like AirMagnet Laptop or WildPackets AiroPeek/OmniPeek are available.

Applying a Packet Analyzer to the Post-Installation Verification Process

Whether you’re using a basic 802.11 monitoring tool (like NetStumbler) or a full-featured packet analyzer the list of SSIDs and MAC addresses with the associated signal strength will be a key part of the post-installation process. The goal is to confirm that all parts of the intended coverage area receive the required minimum level of signal strength. Moreover, the level of noise that’s present may also be reported. Vendors of various end-user devices have minimum RF requirements stated for the suitability of coverage. It’s always necessary to ascertain, from the device manufacturers, what they require for their equipment. Some general examples of signal strength and Signal-to-Noise Ratio (SNR) are presented in the table below. These are very general guidelines intended to provide an example of how different types of user devices and applications require different levels of RF coverage. The actual requirements must be established, based on manufacturer’s specifications, for each network system design.

Type of Device	Minimum Required Signal Strength	Minimum Required Signal-to-Noise Ratio (SNR)
Typical notebook computer used for basic web, email, and file transfer	-95 dBm	10 dB
Notebook computer used in a business enterprise	-80 dBm	20 dB
Handheld inventory scanner or PDA used in a warehouse	-90 dBm	10 dB
Wireless VoIP Phone Handset	-65 dBm	25 dB
Wireless Security Camera	-75 dBm	20 dB
Medical Computer-on-Wheels Patient Management Station	-60 dBm	25 dB

Typical Signal Strength and SNR Requirements

Post-Installation Signal Strength Graphing

Even simple, no-cost 802.11 monitoring tools (like NetStumbler) provide a degree of graphing capability for signal strength measurement. The simple tools allow the generation of a graph for a single, selected MAC address. The more elaborate packet-analyzer tools often allow multiple MAC addresses to be displayed on a single graph, and may include features to allow filtering for the selection of specific devices or SSIDs.

Signal Strength Graphing

The Signal Strength Graphing example shown depicts measurement of a single access point (“CONNECT802 RF SURVEY”) while the on-site engineer walks down a long hallway. Survey walks should be denoted on a floorplan and should be included in a post-installation verification report.

As you study the graph you see that signal strength is close to -30 dBm (directly underneath the access point) and it drops down to roughly -85 dBm at the end of the walk (the right side of the graph.) What is noted in this analysis is that there are moments when the signal drops out completely. These dropouts are caused by the background fluctuations in the RF environment, possibly due to noise or interference, or possibly the result of signal reflections from metal objects. While the packet analyzer

graph discloses the presence of dropouts it has no features that enable the engineer to ascertain the cause of the dropouts. That's the job for a true RF spectrum analyzer.

RF Spectrum Analyzers

An RF spectrum analyzer is a tool that has circuitry to acquire and measure RF signal energy on the basis of individual frequencies. The greater the accuracy, frequency range, rate of signal sampling, and granularity of frequency measurement, the more expensive the tool, ranging from several hundred dollars to tens of thousands of dollars. An 802.11 adapter and some software is never a true spectrum analyzer. To measure RF signal energy specialized hardware is required. Again, this can range from a USB adapter to a case full of sophisticated electronics.

To generalize the differences, assume that any tool advertised as a spectrum analyzer that costs less than $1000.00 USD is not going to be very useful for practical field analysis –the hardware and software required for useful measurement is normally priced over this amount. Between $1000.00 and $5000.00 there are some useful spectrum analyzer tools from companies like Cognio (recently acquired by Cisco Systems), AirMagnet, and WildPackets. At the end of the day it will be found that the Cognio hardware is simply OEM'ed to AirMagnet and WildPackets and they've integrated the RF spectrum analysis capabilities into their software products. In these cases the spectrum analyzer includes an expert system that identifies the difference between a microwave oven's spectral signature, that of a Bluetooth headset, that of a cordless phone, and more. This makes it possible for someone without a background in the physics electromagnetic signal propagation to make sense out of what a spectrum analyzer presents.

At the high end, manufacturers like Anritsu, Agilent, HP, and others have advanced spectrum analyzers that can cost upwards of $40,000.00. For a high-end spectrum analyzer that's limited to use with 802.11 frequencies expect to spend between $5000.00 and $20,000.00.

The cost of a true spectrum analyzer and the need for a solid background in RF engineering to effectively interpret the displayed measurement results make using the services of an experienced 3rd-party consultant an attractive option to perform spectrum analysis work.

Understanding the RF Spectrum Analysis Process

The most fundamental measurement output provided by an RF spectrum analyzer is called the *Fast Fourier Transform* (FFT) display (pronounced Fast "Four-ye-ay" and named after the 19th century mathematician John Fourier.) When a signal is received that contains multiple frequencies (as would be the case where the range of frequencies comprising the 802.11 2.4 GHz band is concerned) the Fast Fourier Transform is the mathematical calculation performed in software to break the signal down into its component parts. The FFT display has frequency across the bottom (the X-axis) and power up the side (Y-axis). At each frequency step the associated power level is displayed in a moving graph format. This is not unlike an audio graphic equalizer which

also displays power at each frequency step from low (bass) to high (treble). An inexpensive audio graphic equalizer may only show five or six bars while a commercial graphic equalizer in a recording studio may have thirty or more bars from bass to treble frequencies. So, too, are the differences in spectrum analyzers relative to FFT.

Step, Sweep, and Dwell

The “width” of each “bar” (i.e. each measurement point) is the step frequency width. A field analyzer (like the Cognio family) may have a 1 MHz step width. That means, for example, that energy would be measured between 2415 MHz and 2416 MHz (2.415 GHz and 2.416 GHz). A more expensive instrument may have a 1 KHz step. This tool (like a high-end Anritsu, Agilent, or HP analyzer) would measure energy between 2415000 KHz and 2415001 KHz – quite a difference (which accounts for ‘quite a price’!)

Sweep time is the amount of time that the analyzer takes to measure each step from the low end of the range to the high end (i.e. from left to right across the screen.) When the sweep time is divided by the number of steps the amount of time that the analyzer has to measure the energy in each step is determined. This is called the *dwell time* – the amount of time the analyzer dwells on each step. An analyzer with a 1 second sweep time across a 1 GHz range (which is typical for a Cognio-type analyzer) is much less expensive than one that provides a 1 microsecond sweep time.

To effectively analyze an 802.11 Wi-Fi network or other similar field network (WiMAX, 900 MHz) a 1 second sweep time with 1 MHz steps is suitable. To analyze and isolate transmitter circuitry problems (as would be required by a manufacturer’s field engineering team) the milli- or micro-second sweep times are more appropriate as is the KHz (or even Hz) step range capability.

Comparing FFT and Duty Cycle

A graphic display that is somewhat similar to the FFT display is the *Duty Cycle* graph. The X-axis of the Duty Cycle graph is broken into frequency steps, exactly like the FFT graph. The Y-axis is a percentage value, from 0% to 100%. At each frequency step, the graph shows the percentage of time that signal was present within the step range. It doesn’t matter the strength of the signal, just whether or not signal was present.

By comparing FFT and Duty Cycle a solid picture can be derived regarding the electromagnetic behavior in the measured range. For example, 802.11 Channel 1 may show very strong signal because you’re close to an access point. The Duty Cycle may only be 1% because the access point is idle (no users active) and it’s only sending periodic Beacon packets. A network can tolerate interference at high power levels as long as the interference is very sporadic. Hence, interference at frequencies with a low Duty Cycle can be ignored. On the other hand, even low levels of interference or noise with a 70% or 80% Duty Cycle will cause problems with data transfer across the network.

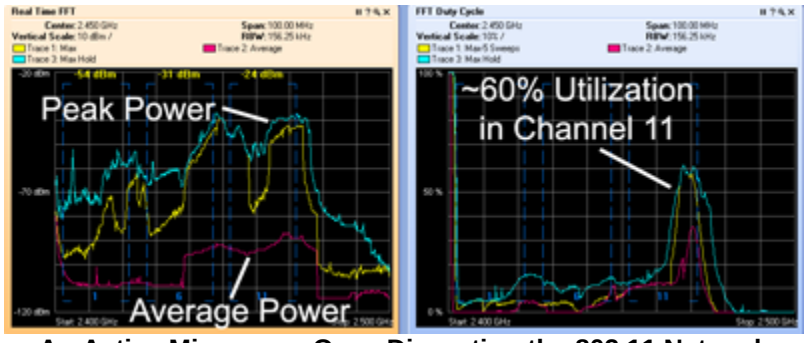
802.11 2.4 GHz Frequency Sweep

RF Characteristics Disclosed by the Spectrum Analyzer

The picture of an RF spectrum analyzer's 802.11 2.4 GHz Frequency Sweep shows the FFT display (on the left) and the Duty Cycle Graph (on the right.) Background noise, depicted by the blue trace, is seen to present greater signal power in the environment as compared to the desired signal, seen on Channels 1, 6, and 11 across the display with the yellow trace. Even though the background noise has more signal power than the desired signal it is not constant. The Duty Cycle graph shows that signal, overall, is generally present for less than 5% of the time. Although there is noise, it is sporadic and of very short duration. It can be assumed that data transfer in this environment will experience some performance degradation but the impact on the end-user community will be very slight.

Identifying and Mitigating Environmental Noise Sources

The spectrum analyzer display showing An Active Microwave Oven Disrupting the 802.11 Network depicts the RF characteristics of an environment in which catastrophic levels of noise are present. The trace shown was acquired while standing in the same location as the previous trace of the 802.11 2.4 GHz Frequency Sweep. Now, however, a microwave oven, located 10 feet from the analysis location, has been turned on.



An Active Microwave Oven Disrupting the 802.11 Network

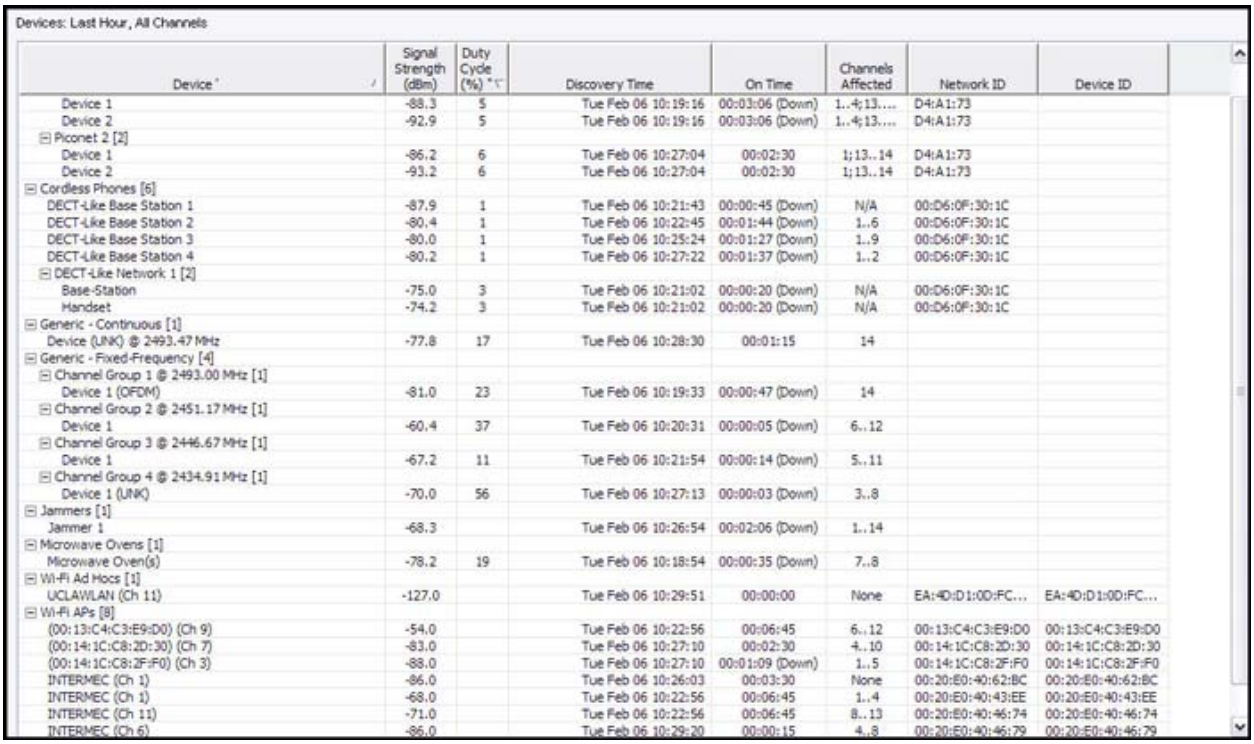
With the microwave oven active it can be seen (above) that peak noise power has risen to -40 dBm and the average signal power (bottom purple line) is hovering right around -80 dBm. Compare this to the trace with the microwave oven off and it can be seen how the level of environmental noise has risen dramatically. Note, too, that the Duty Cycle graph shows that the upper frequency range (overlapping 802.11 Channel 11) has roughly 60% utilization.

It can be seen that although strong noise energy is present across the whole 2.4 GHz b and that the lower 802.11 channels have not only lower noise power levels but the Duty Cycle drops to levels below 10%. The answer here should be obvious: Don't configure access points to operate on Channel 11 when in the presence of potential microwave oven interference; use Channel 1 if possible to get away from the impacted frequencies.

Herein is the essence of one very important aspect of RF spectrum analysis: See where the frequencies are impacted and configure to avoid those frequencies.

Spectrum Analysis Expert Systems

The job of the engineer performing a post-installation verification is facilitated when expert system software is able to speed the process of characterizing signal behavior. The Device List as seen with a Spectrum Analyzer's Expert System picture seen here shows that the analyzer not only makes it possible to identify 802.11 SSIDs and MAC addresses but also categorizes signal behavior as a "Piconet" (a Bluetooth device like a wireless headset or keyboard), DECT device (a cordless phone), continuous (analog) transmitter, microwave oven, and even devices which appear to be sending analog jamming signals.



Devices: Last Hour, All Channels

Device	Signal Strength (dBm)	Duty Cycle (%)	Discovery Time	On Time	Channels Affected	Network ID	Device ID
Device 1	-88.3	5	Tue Feb 06 10:19:16	00:03:06 (Down)	1..4;13....	D4:A1:73	
Device 2	-92.9	5	Tue Feb 06 10:19:16	00:03:06 (Down)	1..4;13....	D4:A1:73	
Piconet 2 [2]							
Device 1	-86.2	6	Tue Feb 06 10:27:04	00:02:30	1;13..14	D4:A1:73	
Device 2	-93.2	6	Tue Feb 06 10:27:04	00:02:30	1;13..14	D4:A1:73	
Cordless Phones [6]							
DECT-Like Base Station 1	-87.9	1	Tue Feb 06 10:21:43	00:00:45 (Down)	N/A	00:D6:0F:30:1C	
DECT-Like Base Station 2	-80.4	1	Tue Feb 06 10:22:45	00:01:44 (Down)	1..6	00:D6:0F:30:1C	
DECT-Like Base Station 3	-80.0	1	Tue Feb 06 10:25:24	00:01:27 (Down)	1..9	00:D6:0F:30:1C	
DECT-Like Base Station 4	-80.2	1	Tue Feb 06 10:27:22	00:01:37 (Down)	1..2	00:D6:0F:30:1C	
DECT-Like Network 1 [2]							
Base-Station	-75.0	3	Tue Feb 06 10:21:02	00:00:20 (Down)	N/A	00:D6:0F:30:1C	
Handset	-74.2	3	Tue Feb 06 10:21:02	00:00:20 (Down)	N/A	00:D6:0F:30:1C	
Generic - Continuous [1]							
Device (UNK) @ 2493.47 MHz	-77.8	17	Tue Feb 06 10:28:30	00:01:15	14		
Generic - Fixed-Frequency [4]							
Channel Group 1 @ 2493.00 MHz [1]							
Device 1 (OFDM)	-81.0	23	Tue Feb 06 10:19:33	00:00:47 (Down)	14		
Channel Group 2 @ 2451.17 MHz [1]							
Device 1	-60.4	37	Tue Feb 06 10:20:31	00:00:05 (Down)	6..12		
Channel Group 3 @ 2446.67 MHz [1]							
Device 1	-67.2	11	Tue Feb 06 10:21:54	00:00:14 (Down)	5..11		
Channel Group 4 @ 2434.91 MHz [1]							
Device 1 (UNK)	-70.0	56	Tue Feb 06 10:27:13	00:00:03 (Down)	3..8		
Jammers [1]							
Jammer 1	-68.3		Tue Feb 06 10:26:54	00:02:06 (Down)	1..14		
Microwave Ovens [1]							
Microwave Oven(s)	-78.2	19	Tue Feb 06 10:18:54	00:00:35 (Down)	7..8		
Wi-Fi Ad Hocs [1]							
UCLAWLAN (Ch 11)	-127.0		Tue Feb 06 10:29:51	00:00:00	None	EA:4D:D1:0D:FC...	EA:4D:D1:0D:FC...
Wi-Fi APs [8]							
(00:13:C4:C3:E9:D0) (Ch 9)	-54.0		Tue Feb 06 10:22:56	00:06:45	6..12	00:13:C4:C3:E9:D0	00:13:C4:C3:E9:D0
(00:14:1C:C8:2D:30) (Ch 7)	-83.0		Tue Feb 06 10:27:10	00:02:30	4..10	00:14:1C:C8:2D:30	00:14:1C:C8:2D:30
(00:14:1C:C8:2F:F0) (Ch 3)	-88.0		Tue Feb 06 10:27:10	00:01:09 (Down)	1..5	00:14:1C:C8:2F:F0	00:14:1C:C8:2F:F0
INTERMEC (Ch 1)	-86.0		Tue Feb 06 10:26:03	00:03:30	None	00:20:E0:40:62:BC	00:20:E0:40:62:BC
INTERMEC (Ch 1)	-68.0		Tue Feb 06 10:22:56	00:06:45	1..4	00:20:E0:40:43:EE	00:20:E0:40:43:EE
INTERMEC (Ch 11)	-71.0		Tue Feb 06 10:22:56	00:06:45	8..13	00:20:E0:40:46:74	00:20:E0:40:46:74
INTERMEC (Ch 6)	-86.0		Tue Feb 06 10:29:20	00:00:15	4..8	00:20:E0:40:46:79	00:20:E0:40:46:79

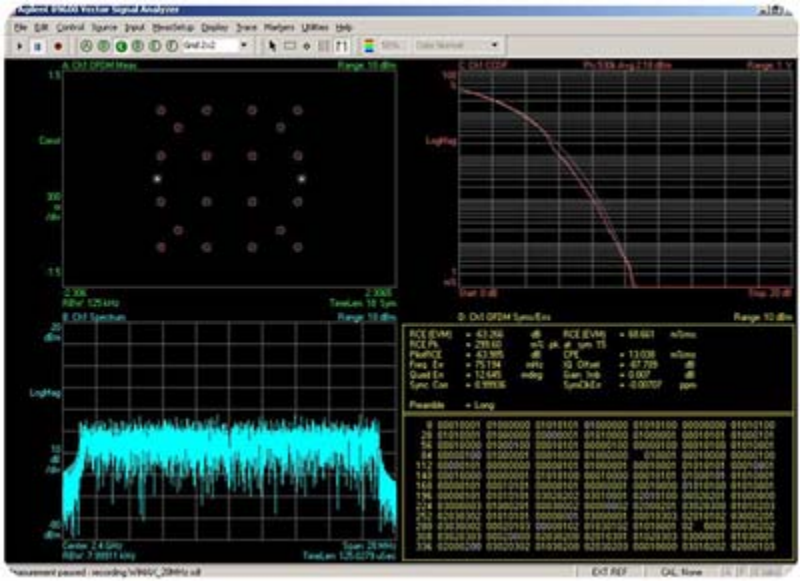
Device List as Seen with a Spectrum Analyzer's Expert System

Applications for High-End RF Spectrum Analyzers

The traces discussed and presented previously were obtained using a typical field-use spectrum analyzer in the $4000 to $6000 price range. This type of spectrum analyzer is ideally suited to post-installation verification. Shown for perspective is the type of screen display that is associated with a high-end, higher-priced RF spectrum analyzer tool. This type of analyzer is based on custom, proprietary hardware and does not run as an application that stands alone in a notebook computer. Computer software often provides enhanced analysis capabilities but the acquisition of signal and noise at the level of granularity provided by a high-end analyzer demands specialized hardware in what is typically a stand-alone device.

The screen display shows a single 802.11 channel in which the RF engineer is evaluating the correctness of the Orthogonal Frequency Division Multiplexing (OFDM) signal. This signal, used by 802.11g and 802.11a, divides a data stream into 48 separate sub-carrier frequencies and adds additional sub-carriers for control and synchronization. The high-end analyzer allows differentiation and analysis of individual sub-carriers, a task beyond the capabilities of the typical field-level RF spectrum analyzer. The engineer can evaluate the "constellation" of interleaved signal phases which differentiate the sub-carriers. The constellation diagram is seen in the upper left.

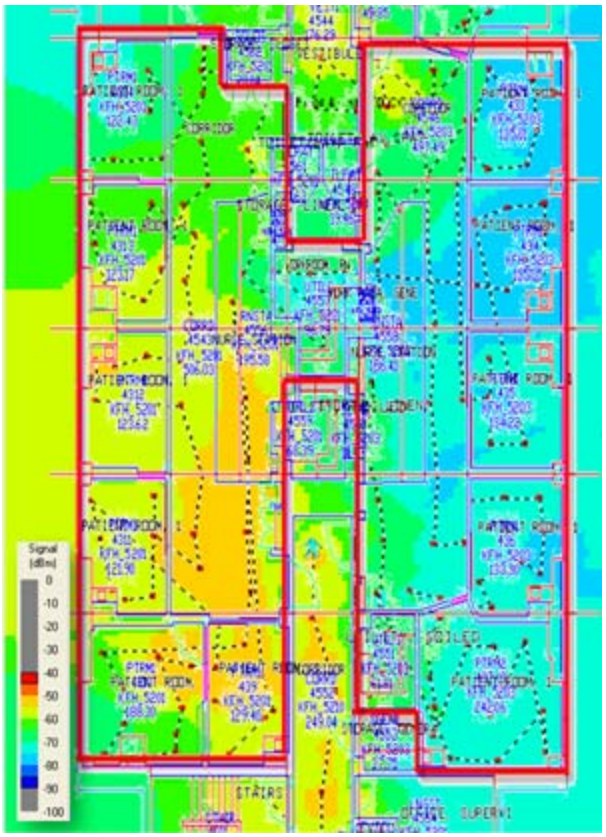
RF spectrum analysis using a high-end tool is generally beyond the capability (and budget) of an installation or end-user company. When complicated RF problems evade normal troubleshooting techniques then it's common to bring in a consultant who is armed with the experience to apply high-end spectrum analysis tools to the challenge of solving the problem.



A High-End RF Spectrum Analyzer

Coverage Gap Analysis

To analyze coverage gaps it's first necessary to identify the weak coverage areas (the "gaps") in the required coverage areas. This is most efficiently accomplished using a site survey tool that allows signal strength measurements to be recorded with a mouse click on a floorplan image. The on-site engineer walks around and records the measurements then the survey software interpolates between measurement points to create a coverage display where signal level is represented by color hue. This "heat map" is the most common depiction of actual signal coverage.



A Site Survey "Heat Map"

Consider the Site Survey "Heat Map" shown. For the network heat map shown a -70 dBm signal level was considered (by the network administrator) to be the minimum level acceptable. The legend shows that -70 dBm corresponds to green, yellow, orange, or red hue areas. Blue hues indicates a coverage gap. It can be seen that most of the right-hand side of the coverage area (enclosed in the red lined area) does not meet the system requirements for -70 dBm coverage. Evidently there are some access points that were either forgotten in the design or installation or they're mounted on the walls but not transmitting – something's wrong that must be corrected.

In Conclusion

Post-installation verification includes simple Ping testing as well as comprehensive data throughput and performance testing. Simple signal strength monitoring tools as well as fully-featured packet-level analyzers provide insight into the overall 802.11 environment and allow confirmation that minimum signal levels and maximum noise levels meet the requirements for the end-user devices and applications that will be deployed. The use of RF spectrum analysis tools gives visibility to the hidden behaviors and interactions of the propagating electromagnetic signals, both coherent, desired signals that will be demodulated to recover data bits as well as the undesired noise and interference signals present in an environment. Isolating and describing the electromagnetic behavior aids in mitigating problems and developing a strategy for coverage gap remediation. Generating a heat map of signal coverage confirms the actual signal levels across the intended areas.

What becomes clear is that post-installation verification is a very personalized process. A simple wireless network, intended for casual, non-intensive use can often be verified in a very simplistic manner applying a restricted strategy. A corporate enterprise Wi-Fi network, or a network used in healthcare or other regulated industries may require a meticulous, labor-intensive effort to verify that it will meet its intended levels of service.

What also becomes clear is that the range of software and hardware tools that are at the field-engineer's disposal is quite broad. Mastering the basic skills required for verifying a wireless LAN system is well within the grasp of most field engineers. Mastering the nuances of RF spectrum analysis or determining methods for problem mitigation or remediation may fall in the prevue of a third-party consultant who faces these issues every day.

In every case, however, a post-installation verification becomes the final step in the life cycle of a new wireless network as it is turned over the user community as a productive element of a site's infrastructure. Installer's are encouraged to make this last part of the job a top priority for all Wi-Fi system projects.