Spectrum Analysis Primer
Part 1 - Fundamentals

Spectrum Analysis: Overview

This is part one of a three part Primer on Spectrum Analysis

I've been teaching these concepts on Spectrum Analysis for many years - now that I'm no longer teaching this full-time, I thought it appropriate to share this information in the form of a Spectrum Analysis Primer.

I'll break this into three parts - the first will cover the underlying fundamentals of RF - so we can have a shared vocabulary. As well as an explanation of the differences between WiFi NIC's and Spectrum Analysis cards.

Then on to a section two on the basics of Spectrum Analysis.

And then finally a section on interpreting Spectrum Analysis results.

Now, on to the information!

This primer will focus on the 'raw' RF spectrum analysis. We'll cover the difference between what a Wi-Fi NIC receives and reports, compared with what Spectrum Analysis devices can 'see' and report.

A simple question, what is *spectrum analysis*? Some vendors will say they offer 'spectrum analysis' because their management systems capture Wi-Fi frame data, and they categorize these details about traffic flows into channel format. Thus, you have analysis by spectrum.

We are not going in that direction at all. This short primer focuses on the 'raw' RF spectrum analysis. We'll cover the differences between what a Wi-Fi NIC receives and reports, compared with what Spectrum Analysis devices can 'see' and report. In other books you may have seen the amount of very fine detail around the organization and processing of frames to follow the IEEE's 802.11 specifications. The IEEE additionally defines many of the specific issues regarding how the RF signals must be processed. One of the abilities of spectrum analysis is to 'see' and confirm these before-unseen parts of the 802.11 protocols.

We sometimes joke when explaining many things about the unseen world of RF, "*wouldn't it be nice to have Star Trek's Geordi LaForge's visor?* "

In this fictional series, his visor could 'see' the entire Electromagnetic spectrum.

Using Packet-Analyzers as detailed throughout this book, we've shown the details surrounding 802.11 frames. Wi-Fi NICs do a great job of following these frame-based protocols. These let you 'see' the 802.11 frames and how they are processed. With a spectrum analyzer, we are getting closer to the fictional visor, something that lets you 'see' Radio Frequency transmissions.

Review of RF Fundamentals

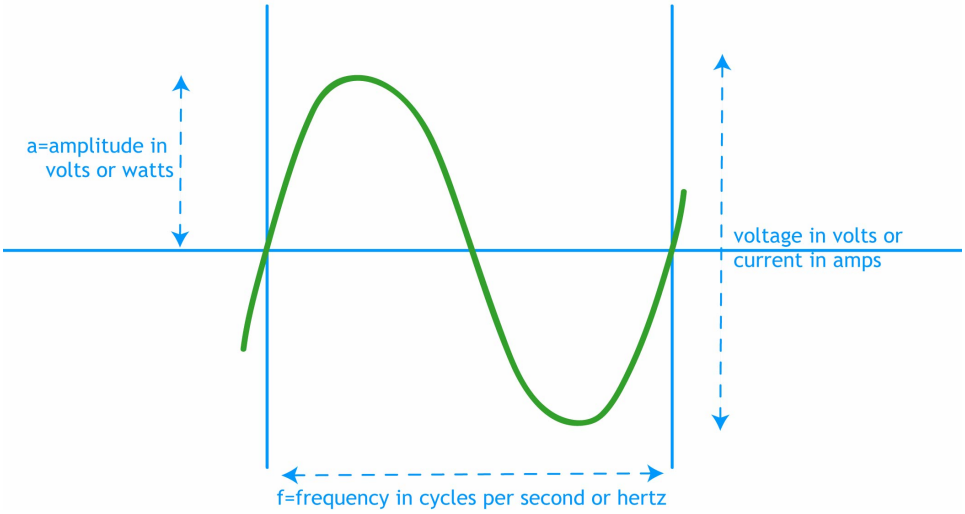
Before we move forward to explaining the processes used by Spectrum Analyzers to do their thing, and to set the proper groundwork, we first have to review the basics of both RF and Wired NICs. The RF fundamentals, because spectrum analysis relies heavily on this discipline, and wired/wireless NICs, because we'll be showing the differences between data devices, those items that can decode bits, combine them into bytes, then finally into frames. Compared with spectrum analyzer who can't even decode a single bit, yet can 'see' a wide swath of the RF spectrum in great detail.

One more little housekeeping note, there is much more detail available on both of these preliminary subjects. This is merely a quick review of the concepts and vocabulary.

Now on with the process of our journey to understand spectrum analysis. This little RF fundamentals review section shows up in the Spectrum Analysis chapter as a way to lay a foundation, and to give us a shared vocabulary of terms used in our discussion of spectrum analysis. This is by no means a detailed education in radio frequency issues, but a quick review of these terms.

Cycle

A wave form that starts at the center, climbs in energy to a peak, returns to the center, then drops to the weakest point, called the trough, then finally returns to the center point. This is one cycle. If we count those cycles for one second, that is called Hertz. A term coined for Cycles Per Second after one of the founding fathers of Radio transmission. The distance traveled of one cycle of a wave pattern is called the wavelength.



Amplitude

amplitude of a wave is defined as the height, force, or power of the wave. This is normally measured in Watts, or in our case of Wi-Fi in mill watts, or one-thousandths of a Watt, and shown with the term mW. The more energy put into the wave, the larger or taller the wave. This higher wave would have more amplitude; the difference between the lower amplitude and the new higher one is referred to as gain. The opposite of gain, is attenuation. When the wave gets smaller, or less energy, we call

that attenuation. RF waves attenuate as they pass through different materials. RF even attenuates without any material through Free Space Loss.

To help visualize RF waves - try the Emanim visualization tool here:
http://www.enzim.hu/~szia/emanim/emanim.htm

Frequency

Frequency can be defined as the number of cycles that occurs within one second For our discussion here, these are very large numbers indeed. 2.4 GHz waves go through this cycle 2.4 Billion times every second. Obviously the 5 GHz waves do it even faster. As a point of comparison, AM radio stations transmit down in the much slower range of 500,000 – 2,000,000 million cycles per second. Human speech and hearing is exponentially slower still in the range of 400 to 15,000 cycles per second. 802.11 transmissions happen in specific frequencies as defined and approved by various government entities worldwide.

Free Space Path Loss

Because of the laws of physics, and electromagnetic signal will attenuate as it travels despite the lace of attenuation caused by any materials in the way. *Free space path loss (FSPL)* is the loss of signal energy caused by the natural broadening of the waves, often referred to s beam divergence. RF signal energy spreads over larger and larger areas over time.

$$\begin{aligned} \mathrm{FSPL} &= \left(\frac{4\pi d}{\lambda}\right)^2 \\ &= \left(\frac{4\pi df}{c}\right)^2 \end{aligned}$$

where:

- λ is the signal wavelength (in metres),
- f is the signal frequency (in hertz),
- d is the distance from the transmitter (in metres),
- c is the speed of light in a vacuum, 2.99792458×10^8 metres per second.

Think of the waves emanating from a pebble dropped in a pond. At the moment of impact all the energy of the pebble converts to the wave starting at the point of impact. A second later, the wave now has a much larger circumference.

But it still has the starting amount of energy, but now must share that energy over a larger area, so the wave height drops. A second later, the wave again grows larger, and thus the wave height continues to get weaker and weaker as the wave grows larger. In the RF world we normally work in three dimensions and the RF waves also get weaker and weaker as they travel further from their source.

There is a logarithmic formula to explain this phenomena, but in short simple terms, as you double the distance from the transmitter; the received energy received has lost four times the starting energy. Double the distance, one quarter the received energy. Any materials the RF must pass through only exacerbate this loss and add even more attenuation.

Decibel (dB)

A *decibel (dB)* is a unit of comparison. We could use dB to compare sound to silence. We could use dB to compare the number of grey hairs today versus grey hairs prior to my children being teenagers. dB is merely a tool used to compare items.

When you see 'dB' replace it in your mind with the words "Compared To" - and this will usually help.

Usually for comparing items that are drastically different. Comparing 10,000,000 to 3 – now that's a big comparison. What kind of chart could we make that would realistically show the differences between 3 and 10,000,000?

Decibels take advantage of the math of logarithms. Normal intelligent people are pretty good at most simple mathematics, adding, subtracting, multiplying and possibly even doing squares and square roots. But most of us can't easily do logarithms in our heads. If you want to perform the RF math calculations using the logarithmic formulas, here they are:

$$dBm = 10 \times \log(mW)$$
$$mW = \log\text{-}1\ (dBm \times 10)$$

With respect to RF, we normally use a Milliwatt (mW) as one way to describe the amount of electromagnetic energy used in Radio transmissions. We can convert mW to dBm. That is, to use the math behind the dB logarithmic formula to change mW to dBm.

Decibel (dB) is a tool usually used to compare items that are drastically different.

For our discussion here concerning Spectrum Analysis, we'll continue to show our energy received in dB, and leave it to you to convert to mW if you so need. Most, if not all Spectrum Analysis can be performed totally in the dB arena.

Received Signal Strength Indicator (RSSI)

This metric comes by measuring the amount of energy associated with the bits received via the wireless NIC. Each vendor calculates this differently. Sometimes shown in dBm and sometimes converted into a percentage. This is the term most people refer to when they say 'signal'.

Noise Floor

This is the ambient level of radio energy on the specific channel you are analyzing. This can include modulated or encoded 802.11 bits, or non-modulated energy coming from other devices like microwave ovens, Bluetooth, portable phones, etc.

Signal Noise Ratio (SNR)

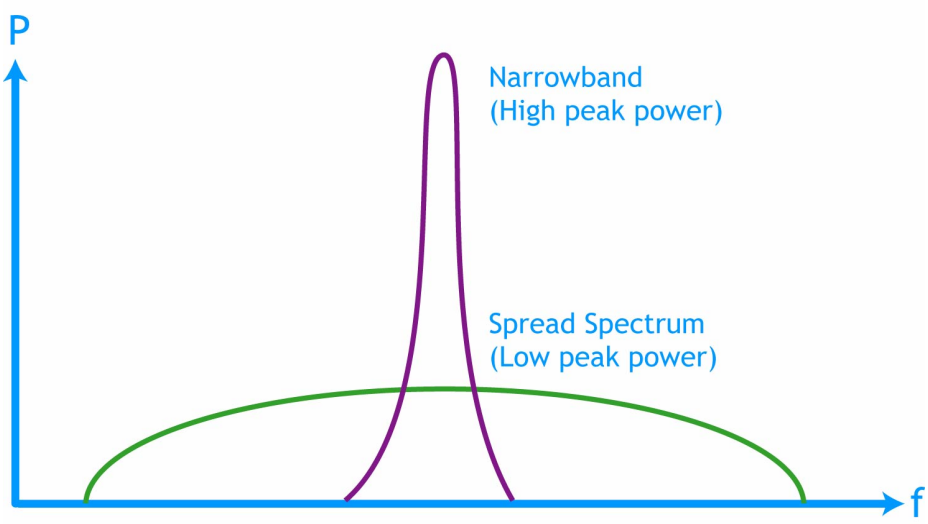
This can be presented in a dB, or the difference between the RSSI (signal) and the noise floor (Noise). For example, the RSSI is -68dBm, and the Noise Floor is -85dBm, the SNR would be -85 minus -68 or an SNR of 17dB. Different devices have been designed to work well within certain SNR metrics.

Receive Sensitivity

Different vendors develop 802.11 Wi-Fi devices with different abilities to discern a 1 from a 0 in different RF environments. This is also closely tied to Data Rates. Determining what data rate to transmit at includes this Receive Sensitivity along with RSSI and SNR, plus Retries, and Bit Error Rates (BER)s.

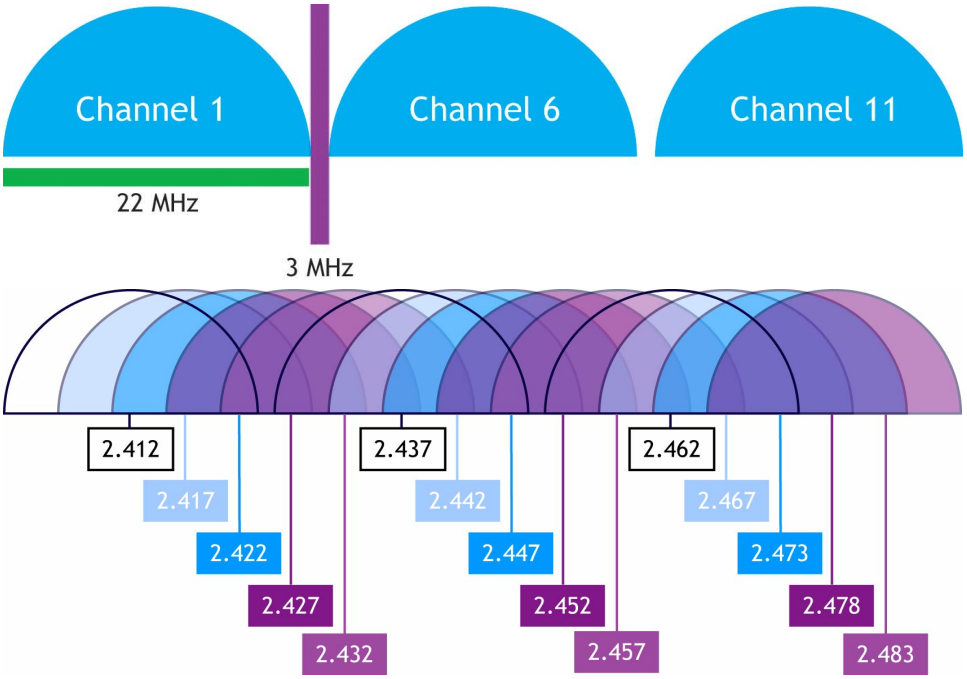
Narrow Band vs Spread Spectrum

Ever since Marconi started working with Radio signals, we've used the word Channel to define the specific frequency for transmitting and receiving. This has meant a specific narrow-band of RF energy grouped tightly around a specifically defined frequency. In developing the protocol to transmit large amounts of data, the 802.11 engineers needed a new broader spectrum to carry more information.



The word Channel has been used to define both the specific frequency for transmitting and receiving and also wider Spread Spectrum groups of frequencies.

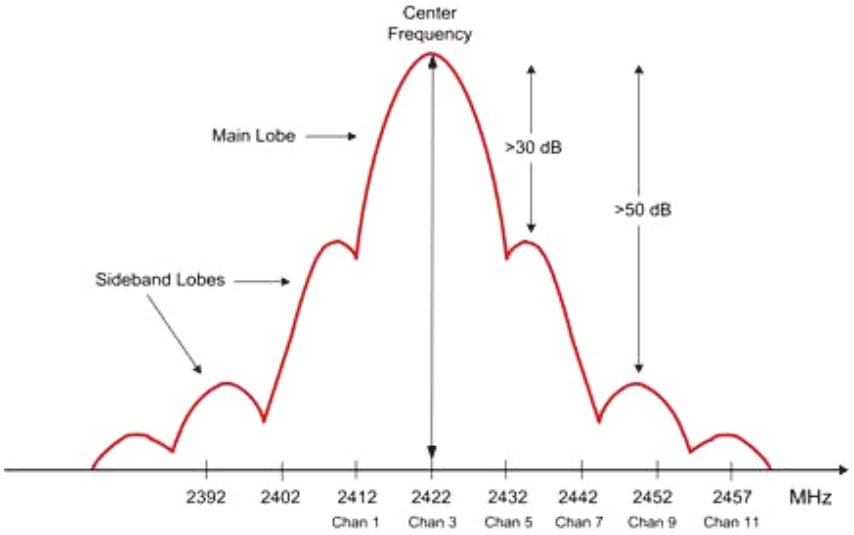
They defined new wider Spread Spectrum groups of frequencies. Sadly, they used the same word, Channel, to define these groups of frequencies. Thus we get issues with co-channel, and adjacent-channel interference because folks think of 2.4 GHz Channel 1 being completely different from Channel 2. If it was like all other channels, that would be true. But in 802.11 we are using spread spectrum channels that have significant overlap.



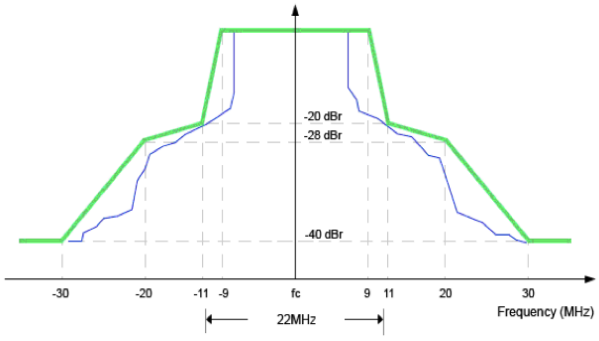
Channel Widths & Spectral Masks

One of the issues with respect to using Spread Spectrum RF energy, was a very definite use of the RF energy. To this end, the developers used something called a spectral mask. Really nothing more than a defined use of specific frequencies to transmit and receive on.

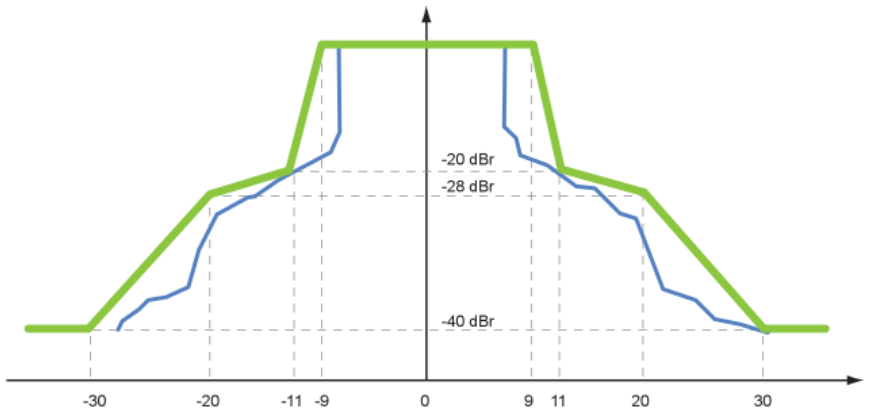
For 802.11b and it's associated data rates of 1, 2, 5.5 and 11, the following 22 MHz-wide spectral mask is used. Note the drastic falling off of energy on both sides. But also now how wide, how many frequencies are being used to carry a single channels RF energy.



For 802.11g and 802.11a that are using the OFDM encoding scheme, they use a 20MHz spectral mask that looks entirely different. OFDM allows for a more dense spectral efficiency, thus it gets higher data throughput than used in the BPSK/ QPSK of 802.11b



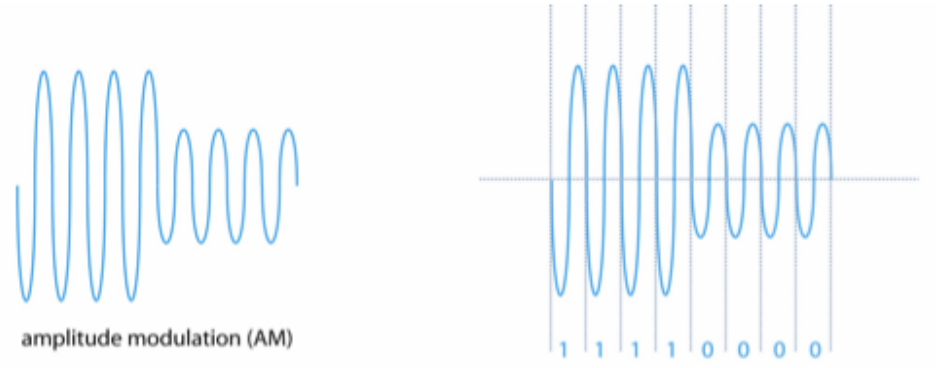
With the advent of 802.11n, we now have an additional spectral mask to deal with. This is the optional OFDM 40Mhz channel. First this is not two 20MHz channels bonded together. This is an entirely new 40MHz wide channel.



Modulation Schemes

In order to send data via radio waves, we need to find a way to take the 0s and 1s and encode those onto a radio wave is such a way as to successfully deliver those same 0s and 1s to the remote device.

We could just do a very simple encoding scheme. If I want to send a 1, then send a loud, read strong, wave. Thus, to send a 0, we would have to send a quiet, or weak wave. Using this very rudimentary method, we could send one bit per cycle. If we were transmitting on the 2.4 GHz range, we would receive 2.4 Billion bits per second.



Though this seems like quite a high rate of data transmission, it is a little misleading. Because in order to send data, we need to receive all the data bits in the proper order and not loose any.

We have a term to start with here, called Bit Error Rate. Count all the bits sent, and then compare with all the bits that showed errors. There are some very detailed and high level math ways of showing this, but we'll stop here at the simple term, Errors per Total Bits sent.

So, using our rudimentary Amplitude Modulation scheme, remember 1s are loud and 0s are soft. We can send 2.4 Billion of these bits per second. Lets see how that works out in real-world data.

```
   8 bits = 1 byte
1,500 bytes = 1 frame
        thus
1 frame = 12,000 bits
```

When we send one data frame, we send 12,000 bits. Even though we send those bits at a very high rate of speed, 2.4 billion of them every second, we might have a problem. What if our Bit Error Rate is greater than 1 in 12,000?

We send one frame, and in that frame there is only one bad bit. The receiving device collects all the bits, and then runs a CRC error check against the frame. Since one of the bits is bad, the CRC fails. Thus we must retransmit the data again. When we transmit the data a second time, the BER is still 1:12,000 and we get another error, thus another re-transmission.

The engineers who developed the modulation schemes used with 802.11 took this small issue to bear and designed in very robust, mathematically complex modulation schemes to help take care of the Bit Error Rate issues inherent in RF transmissions.

These modulation schemes used in Wi-Fi are called BPSK, QPSK, and OFDM.

With regards to spectrum analysis, the various modulation schemes tend to have different RF signatures—based on the underlying protocol associated with each technology. These

leave a ‘tell-tale’ sign, so as a wireless LAN professional, you’ll be able to deduce where and when 802.11 is being transmitted, merely by watching the spectrum analysis displays.

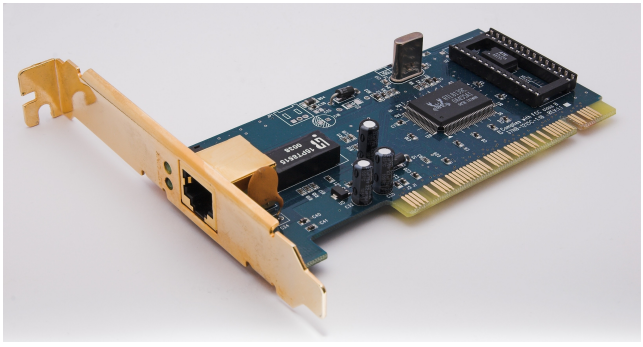
Well, there was a quick review of some of the RF fundamentals and terms we’ll need in our discussion of spectrum analysis.

Now onto another underlying principle to cover prior to delving into the main topic of actual spectrum analysis. Isn’t this a bit of a pain? Before even starting into the topic of this Primer, must we traverse these other paths of knowledge? Actually, yes! In order to fully understand the complexity and technology inherent in spectrum analysis, pardon one more extension to cover another topic.

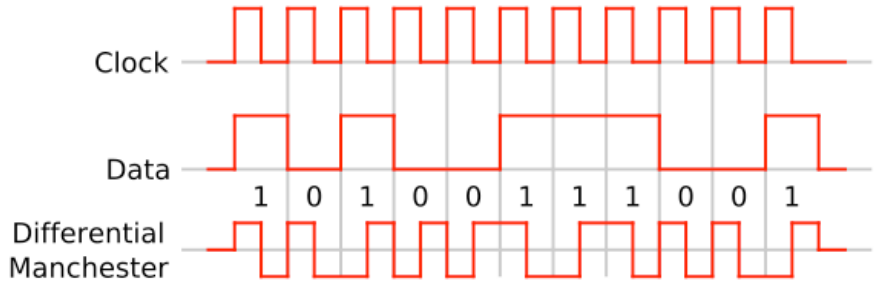
How Network Interface Cards (NICs) Work

Wired NICs

Going into the “way back machine” lets travel back to the late ‘70s. The team at 3Com took the nascent Ethernet protocol and started selling it to the public. At the time, you could purchase a Network Interface Card—the electronics on this card would allow for transmitting and receiving of frames. These frames were strings of bits. Each bit would have to be transmitted and received.



The protocol used an encoding system called Manchester Signal Encoding. This was a protocol the caused electrical current to change its state is a specific pattern to indicate a 0 or a 1. This technique allowed for up to 10 Mbs of data.



When the various Ethernet vendors were looking to speed up the data transmission speeds, they needed a new technical protocol that could work quicker at determining if the changes in electrical current represented a 0 or a 1.

So 100 Mbs Ethernet we started using a new encoding scheme called Non-Return-to-Zero, Invert-on-one NRZI, and it's partner in crime, Multiple Level Transition - 3 levels (MLT-3). *And to answer your question, you don't need to remember those. Just making a point, each change in network capability required a change in the encoding methodology.*

Finally, as we are back the current time, we are using 1Gbs Ethernet connections, and yes, you've got it, it has it's own encoding process. This one is even more complex and mathematically intricate, and is called 8B/10B encoder/decoder, and works on entire octets of data rather than single bits. As we move toward 10 Gb options, we'll see further refinements in the encoding schemes.

In each of these options, the wired NIC listens across its copper pairs, sensing the changes in electrical current, and turns those into strings of bits. These strings of bits make up a frame. Constituted by the Preamble, Header, Data Payload, and finally a Frame Check Sequence or CRC to determine if all the enclosed bits were received accurately.

NIC strips off the Preamble, checks the Destination MAC Address to see if the frame is targeted at this specific NIC. If not destined for this specific NIC, the frame might be sent to a Broadcast or Multicast address. If none of the above the NIC discards the frame. But if this frame is supposed to be on this MAC address, the header is then stripped and the data payload is sent up the protocol stack to the OS as a designated and approved frame.

Wireless NICs

Enough with the wired side, lets talk about Wireless Networks!

Right enough. On to the wireless NICs of today. Unlike their wired counterparts, wireless NICs don't have the advantage of a bounded media like copper or fiber to access. So instead of using the changes in current or voltage across a copper pair, wireless NICs had to add an additional couple of features.

Instead of the copper connection of an Ethernet NIC, a wireless 802.11 NICs has an antenna. The job of the antenna is to allow past just the RF energy sources designed to work with this specific NIC. In the case of 802.11b/g we're talking about 2.4 GHz radio waves. The antenna is designed specifically to listen to only this frequency. Here again, there are some pretty complex mathematics around antenna design, but for the sake of our discussion, these antennas try and block all radio waves except 2.4 GHz.

Think of all the radio waves that are bumping into every minutes, AM, FM, Satellite Radio, Police Bands, Aviation Bands, HAM operator bands, Cell Phones, Broadcast TV, Portable Phones, Garage Door Openers, and many, many more. The little antennas in 802.11 devices are designed to block all of those that are not in the 2.4 GHz band.

So the first line of defense for the wireless NIC is it's antenna, out there blocking all but the 2.4 GHz waves. Still some non-802.11 radio signals will get through. The 2.4 GHz band is an un-licensed band and many things are legally able to transmit in this range. Thus your wireless NIC's antenna lets through portable phones, Bluetooth transmissions, wireless security cameras, and even microwave oven radiation. All use the 2.4 GHz frequencies.

So the developers of the wireless NICs came up with a second line of defense. This is designed to filter out all unwanted RF. Thus we return to our encoding schemes. We can't use the encoding schemes used by 10/100/100 Ethernet because they are copper dependent. Instead the engineers designed robust, complex protocols to be able to discern 0s from 1s out of RF energy.

These are those we mentioned above. BPSK, QPSK, and OFDM. Like in the ever increasing and ever more complex world of Ethernet. As we moved from 10, to 100, to 1000 Ethernet, the encoding systems increased in complexity. Here too, in 802.11, we've improved the speeds of our data transmission by moving from BPSK used in 1 and 2 Mbs data rates, to QPSK

used in 5.5 and 11 Mbs, and finally on to the even higher 54 Mbs supported by OFDM.

As the radio signal passes this filter, and the filter is based on the encoding system supported by the wireless NIC, we now finally see the bits. Just like in the wired NIC, the bits are strung together into a string of 0s and 1s, and in the format of Preamble, Header, Frame Body, and FCS. Again, just like the wired NIC the Preamble is discarded, the header consulted over Destination MAC Address, and finally the FCS calculated to insure all the included bits were accurate.

All of that is just like a wired NIC. A few of the differences between wired and wireless NICs, first the wireless needs to use it's antenna and encoding filter to keep out all unwanted RF signal, thus unwanted bits as well. There is another significant difference. The NIC will use some of the specific information gleaned from the RF to Bit transition process to add information to the frame. This is added at the receiving station, and is in addition to the bits sent from the source. This added information is called the Radio Tap Header. It includes Date and Time Stamps, Channel Stamp, Signal Stamp and a Noise Stamp.

```
⊟ Radiotap Header v0, Length 26
    Header revision: 0
    Header pad: 0
    Header length: 26
  ⊞ Present flags: 0x0000186f
    MAC timestamp: 161412602
  ⊞ Flags: 0x10
    Data Rate: 1.0 Mb/s
    Channel frequency: 2437 [BG 6]
  ⊞ Channel type: 802.11b (0x00a0)
    SSI Signal: -81 dBm
    SSI Noise: -84 dBm
    Antenna: 0
    SSI Signal: 3 dB
```

The Date and Time stamps are obvious. The Channel stamp is based on the frequency the NIC was on while it received this bit-stream. The next has it's own name and is called Received Signal Strength Indicator (RSSI). This is an integer from 0-255 and represents the average energy of all the bits received in this frame. Since each vendor calculates this differently, we'll just treat RSSI as the RF Signal received by the device.

Though RSSI may be calculated slightly differently by various vendors, we still use it, and put trust in the number as the true amount of RF energy received by the NIC.

The final bit of information in the Radio Tap Header concerns a variable for Noise. To re-emphasize, the wireless NIC is not a spectrum analyzer, and though it can transmit and receive data at a prodigious rate, it cannot see raw ambient RF. Since the only thing getting past the encoding filter are bits, all the information reported by the NIC must needs come from the bits it received.

If you turn on a microwave oven near a wireless NIC, but there are no data bits floating around in the area, the NIC will always report a Noise variable of zero. This is because wireless NICs require bits in order to do their magic. By the way, we'll stop here for a moment to let that last sentence sink in a minute. In the absence of encoded RF signals coming from other 802.11 devices, the Noise variable cannot be used to report the noise floor.

Wait, you've seen lots of screens in your various 802.11 devices that work with Signal (from the RSSI variable) and something called SNR or Signal Noise Ratio, and is a comparison between the RSSI and the Noise floor.

The developers of the wireless NICs knew the RF folks out there "Live, Breath, and Die" by Signal, Noise, and Signal Noise Ratio. These RF engineers demanded a Noise variable in order to do there calculations. So various vendor organizations came up with unique ways to guess on the noise floor. Since NICs only

can process bits, they needed to come up with algorithms to calculate a Noise variable based on the bits going through the NIC.

By the way, like RSSI, each vendor selling 802.11 equipment calculates Noise a different way. Some vendors flatly refused to make up a number for Noise only based on bits. Other vendors have developed very sophisticated algorithms for calculating noise.

Lately some 802.11 chip manufactures have figured out how to turn off the encoding filters and use the RF signals coming through the antenna to become a rudimentary spectrum analyzer. But this is in lieu of being an 802.11 NIC capable of processing data. These new chips can be either lightweight spectrum analyzer OR a Wi-Fi card processing data. But never at the same time.

Just lately the access point vendors are also using these extra-capable Wi-Fi chips and are adding spectrum analysis as an option for an access point. Examples would be the Intel 5300 chip or Aruba's AP-105 and AP-125s with the appropriate software to take advantage of this extra ability.

NOTE: It would be very nice if all wireless NIC vendors, both stations and access points, would adopt a standard for calculating and presenting RF information from their various devices. But, alas, I don't foresee this happening any time in the near future.

With this data resulting from the Radio Tap Header information, a wireless NIC can learn about the environment around it, by scanning—listening to the different channels available. Many Wi-Fi tools use this technique to learn of the RF environment. Some of the more infamous titles are things like NetStumbler, or inSSIDer.

Some vendors also use this same technique of listening in on channels to determine data points to help in their automatic channelizing and power balancing systems. But none of these can see raw ambient RF, they only see what comes in the form of bits, or modulated RF encoded in one of our protocols.
We've come a long way towards preparing you for the true topic of this chapter—spectrum analysis. Hopefully we've prepared you, and perhaps even whet your appetite for the upcoming subject. Finally, on to spectrum analysis.

Wireless LAN Training/Consulting
Keith R. Parsons, CWNE #3
Managing Director
Institute for Network Professionals
281 South Vineyard Road - #104
Orem, UT 84058-2005
+1 801 223 9444 - office
keith@inpnet.org
http://WirelessLANProfessionals.com
http://twitter.com/keithrparsons