

Technical Bulletin

Wireless Networks for Retail — Course 101

PO-TECH-04:09
November 12, 2004

Does this sound familiar?

- “This wireless HH application just doesn’t work!”
- “Sometimes it works for an hour ... and then it just locks up.”
- “It runs so slowly that it just isn’t worth the effort! When it does work, it’s great – but I just can’t count on it. When I need it the most – that’s when it fails! “
- “Plus there are spots in the store that this thing never seems to work!”

In reality, problems like these most likely have nothing to do with the application running on the HH. Most often these types of problems occur as a result of improper HH and wireless network configuration. This document is designed to help provide a foundation of knowledge and understanding to help address these issues. The hope is that you will find the information provided enlightening – remember WiFi technology (Wireless Fidelity) is enjoying wide spread acceptance already, and it is growing rapidly. So enjoy!

To Your Success,

Tim

Tim Klingenberg
Manager: RBO and PocketOffice

This document and information are supplied to StoreNext Retail Technologies personnel and third parties to assist them in doing business with StoreNext. They are not to be used or distributed for any other purpose.

StoreNext Retail Technologies LLC endeavors to ensure that the information in this document is correct and fairly stated, but does not accept liability for any error or omission.

FIRST A BIT OF HISTORY

Wireless networks are not created equal. Technology has changed significantly over the last decade; in many ways things have gotten better and in some ways, perhaps things have gotten worse. Bottom line: change has and continues to occur with little likelihood of ever going back. I'll try to explain.

Remember the old narrow – band days where we had to apply to the FCC for a license and they would authorize a frequency (there were various frequency ranges but a good example is the 468.200 to 469.975 MHz range)? If we played by the rules we'd wait until the FCC granted our license and authorized a frequency before we could order the hand held and base station and MUX. This was necessary because the manufacturer had to configure the radios with the frequency provided by the FCC license. What a hassle – never mind the expense.

This good old technology screamed along at 9600 baud capable of running text – based applications specifically designed for these units. Signal strength was amazing for these ½ watt radios and although susceptible to noise and interference, it was not totally uncommon to drive a signal several miles. Once we got the hang of this technology it was really cool, we could walk into a supermarket, hang the base and MUX on the wall or even throw it under the desk, plug it in and we were up and running. Yes, we know it was a little bit more work than this but you get the idea and for those who worked with narrow band know exactly I mean. Often the problem wasn't lack of signal rather it was too much. Police and Emergency bands are often in close proximity.

As this technology caught on the FCC woke up to 2 problems: first they were running out of non-overlapping / non – conflicting frequencies in metropolitan areas. Businesses were beginning to walk on each other and the demand was just beginning to take off. And secondly the government saw these frequency ranges with extended reach would be much better served if they were eventually reserved for government / military use. Civilian use manufacturers began to scramble.

Soon thereafter, we saw a period of various designs operating in ever higher frequencies. Remember 900 MHz and how cool it was? No FCC licensing, and fast, wow, so much better than the old 9600 baud narrow band. The problem soon became apparent that it seemed everyone was using 900 MHz, from the new cordless phones to automatic door openers. Wireless hand held manufacturers went back to the drawing board. Many of us still have fond memories of our long dead 900 MHz cordless phones. Before cell phones, remember being able to walk over to your neighbor's house with your cordless phone, have coffee, and take calls as if you were still sitting in your kitchen. Try that now with the new 5.x GHz phones – you won't get out of your yard.

Skipping ahead to just a few short years ago we saw the advent of the first 2 MB wireless devices. *Wow*, 2 MB was a giant leap from the old 9600 Baud devices. There is still a ton of these devices in play today. The problem was however that those users who have found a use for the range of the old narrow band radios now discovered that although the 2 MB devices were a lot faster they also have a significantly reduced range. But for most users they still had a very simple install and range for the most part covered their entire store.

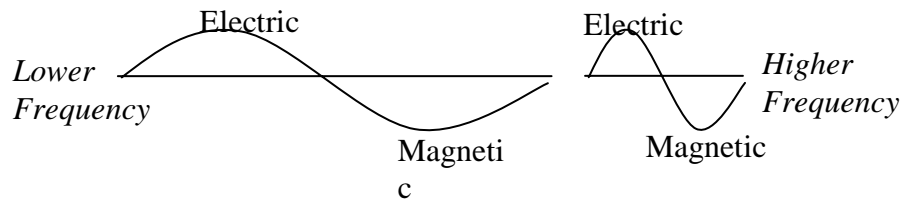
Today we have WiFi (Wireless Fidelity) 802.11. 802.11b was the first version to reach the market transmitting at 2.4 GHz and handling up to 11 megabits per second. This is the current standard used by most retail – hardened hand held suppliers. And this is the technology that will be the focus of the remainder of this document.

Note: 802.11a has since been developed. It operates at 5 GHz and can handle up to 54 megabits per second. Additionally we also have 802.11g which is a combination of both worlds. It also operates at 2.4GHz but it has the 54 megabits per second speed of 802.11a. WiFi radios that work with the 802.11b and 802.11g standards transmit at 2.4 GHz, while those that comply with the 802.11a standard transmit at 5 GHz.

Why drag you through this long history? For one important reason: 802.11b is nothing at all like the old narrow band radios of the past. Yes 802.11b is a lot faster than the old narrow band, but it is also has a much more limited range and susceptibility to noise. No longer can you drop an access point in the corner of the store and expect coverage everywhere – sorry to break the news. But there is some very good news as well. WiFi access point limited range keeps signal from bleeding potentially miles away from the store, yet these low range flexible access points can be ‘chained’ together to provide seamless coverage in significantly larger more complicated areas than ever possible with the old narrow band. So let’s take a look at this 802.11b and see now it pertains to us in some detail. Here are the primary areas you need to understand.

FREQUENCY

Frequency refers to the number of cycles of a wave passing a fixed point per unit of time. Frequency is normally measured in Hertz (Hz), equivalent to one cycle per second, and various multiples of Hertz. Therefore, the two are inversely related to each other. Shorter wavelengths create higher frequency – the longer the wavelength, the lower the frequency.



Megahertz refers to “millions of cycles per second” and a Gigahertz (GHz) refers to 1 billion cycles per second.

802.11b transmits at 2.4 GHz, providing a very fast 11 megabits per second, plenty of bandwidth for our needs. However you can easily imagine how easily a very compact signal like this is easily distorted and/or corrupted as it moves further from the source.

802.11b hand-helds generally transmit at a very weak 30 milliwatts of power. This is a very weak signal thus the reason the FCC doesn’t require a license. So 2.4 GHz (a very tight compact sign wave) coupled with a broadcast using 30 milliwatts of power – figure in your retail environment an average range of 80 – to 100 – foot radius.

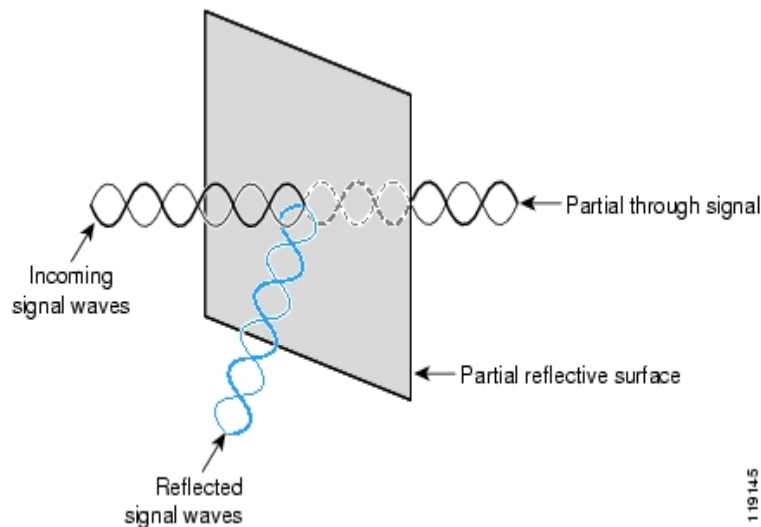
Note: A milliwatt refers to a unit of power equal to 1 thousandths of a watt. Are you amazed yet?

SIGNAL ATTENUATION

Signal attenuation: Definition: to lessen the density of, to rarify. 802.11b signal is easily absorbed and weakened as it passes through various inert materials.

For example:

- a. Plasterboard wall –3 dB (decibel)
- b. Glass with metal frame –6 dB
- c. Cinder block wall –4 dB
- d. Office Window –3 dB
- e. Metal Door –6 dB
- f. Metal door in brick wall –12 dB
- g. Human body –3 dB
- h. Additionally signal is also reflected – example below caused by a wall:



Additionally note that if there are metal air ducts, freezers, coolers, shelving or other physical barriers, signal reflection or multi – path (reflected signal) interference can occur. You guessed it – this is exactly the environment we see in retail environments. It is highly recommended that you move the antennas away from those barriers. In the case of insulated metal coolers and freezers, moving the antenna a few feet away will help eliminate the signal reflection and distortion. The same is true with air ducts in the ceiling. Understanding the fundamentals of 802.11b will go along way in helping remove the mysteries of signal coverage. Don't get discouraged – the important point to remember is that 802.11b will work in this environment but only if you know and understand the rules.

MULTI-PATH

The topic of multi-path can be complicated so we won't try to fully discover the depths of its meaning here. However we can clear a bit of the fog with minimal effort. Imagine an environment where we have a whole bunch of signals bouncing around the store, i.e. multi-pathing. Access points and HH radios have a giant task of determining which signal is the right one to pay attention to versus the extra signals that are just noise. Access points have sophisticated internal logic designed specifically for this purpose.

Important note: not all access points are created equal – some manufacturers claim a higher cost justification based on their unique capability to quickly decipher correct signal. Cost basis is certainly not determined solely on this criterion only but is certainly noteworthy within the context of this discussion.

NOISE

The throughput performance of the WLAN network is affected by unusable signals. Wireless network interference can be generated by microwave ovens, 2.4 GHz cordless phones, Bluetooth devices, or any number of other electronic equipment operating in the 2.4 GHz band. Interference also can come from other wireless access points (“WAPs”) and client devices that belong in the WLAN but that are far enough away so that their signal is weakened or has become corrupted. WAPs that are not part of the network infrastructure can also cause WLAN interference and are identified as rogue APs. Interference and multi-path distortion cause the transmitted signal to fluctuate. Interference decreases the signal-to-noise ratio (SNR) for a particular data rate. Packet retry counts go up in an area where interference and/or multi-path distortion are high. Interference is also referred to as *noise level* or *noise floor*. The strength of the received signal from its associated AP must be high enough above the receiver's noise level to be decoded correctly. This level of strength is referred to as the signal-to-noise ratio, or SNR.

ACCESS POINTS AND ANTENNAS

Access points with internal antennas offer a compact package and are excellent when properly placed in the store with the limitations well understood via a careful site survey. Access Points with removable external antenna however, open the window for using various types of specialized antenna that can greatly enhance coverage and usability without the need for such careful placement within the store.

Note: an optional 12-decibel gain external antenna can more than double the access point's ability to receive and / or transmit signal. Some antenna manufacturers boast of products with even much higher capabilities.

Not all antennas are created equal – do your research and use the correct antenna for the specific job at hand.

1. Some antennas are tuned for best transmission while others are tuned for best reception and yet others are tuned to try to make the best of both worlds.
2. Some antennas are designed for 360-degree coverage while others are designed for point to point while others are designed fit in the corner and transmit at 45 degrees.
3. Take time to know your options and based on your environment and a proper site survey make the right choices.

Every access point has the ability to transmit on any channel from 1 to 11. The default almost universally is channel 6.

1. Although there are 11 channels – the truth is that there is significant overlap and as such there is really only 3 channels with no overlap – 1, 3, and 11.
2. Two access points within signal range of each other will fight with each other. It may not kill communications but then again it very well could. The point is that doing so will create a lot of interference – best advice: ‘Don't do it’.
3. Know what other access points are out there and what channel they are running on and set yours to a channel outside competing channels wherever possible.

It will not be unusual for stores to require more than one access point to provide proper coverage within the store. This is one of the best features of 802.11. With very little effort a single hand held device can seamless roam between access points. Hand held users are totally oblivious to the wonders of this fine capability. Whenever you get into an environment requiring multiple WAP pay particular attention to the following:

1. Proper channel selection
2. Proper placement – i.e. proper overlap

3. *Never* try to mix different access points – you will almost certainly have roaming problems.
4. More info on this specific issue in the subsequent document “Wireless Networks for Retail 202”.

Access Points often transmit at 100 milliwatts and most HHs transmit at 30 milliwatts.

1. Understand the meaning of this – just because the HH can accurately receive a signal from an access point doesn’t guarantee the access point can properly receive a signal from the HH.
2. Don’t panic – the functional difference between 100 mw and 30 mw is quite minor. As stated earlier any carrier in the mw range operates at very low power.

SECURITY

1. SSID – Do not broadcast the SSID – you’re just inviting interest from the wrong element.
2. WEP – Use 128 bit WEP – don’t be foolish. It’s easy to set up and is an excellent deterrent for all but the determined hacker.
3. MAC address filtering. It is highly recommended taking the time to set the access point to only accept traffic from the MAC addresses of the devices you want. Remember every WiFi device has a unique MAC address. If an unwanted visitor tries to connect to your network via your access point and his MAC address is not defined in your access point’s MAC filter table – he’s out of luck....
4. Access Point Login and Browsing security should be enabled to prevent unauthorized people from viewing or modifying access point settings.

HAND-HELD SETUP

1. Set the HH radio to access infrastructure networks only – avoid the default of any available network. Why have the hand held distracted and attempting to connect with rogue access points nearby.
2. Set the HH preferred networks to only look for your specific SSID.
3. For example the Fujitsu iPad signal strength meter translates as follows:

i. Excellent	>=	—56 dB
ii. Very Good	<	—57 dB
iii. Good	<	—67 dB
iv. Low	<	—71 dB
v. Very Low	<	—81 dB
vi. No Signal	<	—90 dB

ACCESS POINT FIRMWARE

1. Refer often the access point manufacturer for latest firmware. Cisco for example posts new firmware versions specifically to fix bugs.
2. As much of a pain as this can be – take the time to check the manufactures web site, download and update your WAP with the latest firmware. There wouldn’t be an update if there were no problems to correct right?

3. Just one last note on WAP firmware – a lot of the problems corrected often have to do with connectivity-related issues.

HAND-HELD FIRMWARE

HH manufacturers will fix bugs. They're only human and frail like you and I – if you don't have the latest firmware – you are running a hand held with known bugs. 'Nuf said....

SITE SURVEYS

1. Measure signal strength – i.e. carrier strength
2. Signal quality – i.e. signal to noise ratio
3. Line of sight vs. signal bounce.
4. Understand propagation (the act of signal multiplication as a result of passing through or bouncing off materials such as metal, liquids, walls etc.)
5. Make sure you are performing a site survey at peak inventory levels or at times of highest activity. A store at a 50% stocking level has a very different RF footprint than the same store at an inventory level of 100%.
6. Similarly, a site survey in a store after hours (without people) will have a different RF footprint than the same area full of people during the day.
7. Microwave ovens, cooler compressors, generators and motors can produce 2.4GHz interference.
8. Access Point ideal coverage location vs. ideal accessibility location.
9. There are excellent resources available to educate, assist, and even provide this important service. Three such resources are provided here – check them out! And know however there are many other similar providers available:

<http://www.giga—wave.com/index.asp>

<http://www.wavonline.com>

<http://www.summittechnologies.com>

That it for this document. Certainly we've just scratched the surface here, but hopefully you've learned and enough additional interest is sparked to dig deeper.

And for that purpose we've also prepared the follow-on [Wireless Networks for Retail – Course 202](#) for you, dealing specifically with the most efficient and effective methods to carry out the dreaded (but surprisingly easy after all) Site Survey.

Remember WiFi is here and it's growing fast. Retailers need and want wireless benefits for a lot more than just hand-helds such as POS, scales, surveillance and more. Be wise Be prepared....