Teletics Application Note

The ISM Band:

Technical Considerations and Product Design Practices for 2.4 & 5.8 Ghz

Rev 1.3 – November 2011

Contents

Purpose and Scope:

Many customers considering implementing a communications product that uses 2.4 or 5.8 GHz radio freqencies are concerned about possible issues arising from using a public band where other equipment might be operating.

The purpose of this document is to provide some basic technical background on how equipment designed for the 2.4 GHz and 5.8 GHz ISM bands works. Additionally, we will discuss key technical considerations that customers may need to be aware of when implementing equipment in these bands, and how Teletics design engineers have worked to improve reliability and security of our products in these bands, as well as co-existence with other equipment which may be in the area.

Radio Types

2.4 and 5.8 GHz radio bands are public frequencies, which means that anyone can design a product to use these bands, provided that they submit their radio designs to government approved labs for certification to predefined standards of operation.

A few of the restrictions in these standards worth mentioning are power output, maximum time intervals the radio may use the band, and how big a chunk of the band the radio can use at one time. These three restrictions, combined with the modulation technology used in these bands, called spread spectrum, attempt to create a level playing field between similar devices operating in the same area. Equipment from different vendors, owned by different customers, should behave as though they are independent of each other and not significantly degrade the performance of one another. Another way to think of this is that it divides the band up into little mail slots where packets can be placed and addressed from one radio to another. No one is allowed to fill up more than one slot at once.

According to the certification rules, 2.4 and 5.8 GHz radios also have two different ways to jump around within the band. One method is called direct sequence, and the other is called frequency hopping. Each has its own technical advantages, but the vast majority of new unlicensed spread spectrum radio designs have standardized on direct sequence for a number of reasons. Direct sequence radios provide higher data throughput, and multiple direct sequence radios in the same operating area co-exist with each other better than a community of frequency hoppers. Stated another way, direct sequence radios “play well” with other direct sequence radios. Your neighbors WiFi access point doesn’t really affect the performance of yours very much.

There are lots of reasons why your WiFi (or Hotspot) access performance is not noticeably degraded when one of your neighbors adds another access point. The most significant of these is a basic rule of magnetic energy. Your fridge magnets may snap back to the fridge when you let them go and they are a slightly away from the fridge, but if you hold them an inch away, there is a good chance they'll drop to the floor. The reason for this is that magnetic force decreases at the square of the distance. Another technical term for radio is electromagnetic radiation. So, if you and your neighbor have the same access point, and your laptop computer is 10 yards from your access point, and 20 yards from your neighbor's access point, signal levels are not even close to the same level. Throw in the losses from walls and his equipment is hardly even a consideration. Signal levels that show up on your laptop regarding WiFi signal are is dB, which is not linear either. A difference of 3 dB between signals indicates that one signal is one half of the power of the other.

Consumers also like paying as little as possible for their electronics. This directly affects the power output of the WiFi equipment in a negative way. 2.4 GHz and 5.8 GHz radios are not very efficient at how they use power. So a radio manufacturer can not be competitive with a WiFi access point that has any more power than is needed to get through a few wood framed inside walls. In fact, a number of WiFi access point manufacturers do not even publish specifications for power output on their datasheets or product packaging, since they are very low, and most consumers only care if they can use their laptop in the next room.

Back to frequency hopping spread spectrum for a second. In the 2.4 GHz band, these types of radios were among the first 2.4 GHz spread spectrum radios to come to market in the late 1980s and 1990s. These radio systems were generally installed by radio professionals, since there was an understanding required on how to design the link along with antenna and cable selection. Their cost was very high in comparison to todays WiFi access points, so they did not enjoy the market size that today's access points have achieved.

Frequency hopping 2.4 GHz radios are still around, however the custom nature of these radio designs makes them more expensive than direct sequence radios, and therefore installations where they are used are much more specialized. You generally will not see them in general computer applications, but in areas of industrial control. There were a number of older 2.4 GHz frequency hoppers used to connect rural schools, but those are disappearing in favor of higher data rate direct sequence radio technology.

Frequency hopping radio is generally more interference tolerant than direct sequence. However, the slower data rate of these radios and the fact that they may create interference with newer direct sequence radios have made them suitable strictly for very specialized applications. There is also a significant difference is the deployment

numbers for 5.8 GHz frequency hopping radios versus the 2.4 GHz models. Since 2.4GHz frequency hoppers were first to market, there are still a few around. In 5.8 GHz, the number of frequency hoppers installed is almost negligible. Almost every 5.8 GHz radio installed today is a direct sequence radio.

Antennas

The antennas that fall out of the box with most 2.4 GHz equipment is a small omni-directional antenna. Why?

First, they are cheap to make. But most importantly, they scatter the radio energy they produce everywhere, and they listen in all directions as well. This is so a home user with no idea about antennas work can "slap it up" just about anywhere with reasonable success. Bigger antennas do not increase the output power, but they will focus it somewhere. Different antennas focus the radio energy in different ways, but the basic concept can be demonstrated by a five dollar flashlight. If you take the flashlight apart and use the bulb without the shiny reflector in a darkened room, the light scatters everywhere. If you use the reflector behind the bulb, you can then point all the light towards where you want to look. The type of antenna that looks and listens in one particular direction is called a planar or panel antenna. There are many types of antennas, but you should always keep one thing in mind. Antennas focus output radio power and constrict where the radio "hears" from. An antenna does not increase the power output of the radio itself, but provides effective gain through concentrating the energy. Also, similar to what happens when you pass light through a lens, antennas polarize the electromagnetic radiation, and therefor have a "polarity", referring to how they must be mounted to work properly. You cannot increase distance without sacrificing area covered.

If you would like to understand more about how antennas work, we suggest that you do a web search for basic antenna theory. There are a number of excellent articles.

Security

Since anyone can run to the corner store and buy a wireless access point and set it up for home use, how can you protect the link you own from prying eyes? Again, there are a number of methods.

First, there are no Teletics products that are designed to provide public access. All of our links are designed to communicate with only other Teletics products within the same product line. There are no DHCP servers anywhere inside our radios, and the connections are designed to be private networks.

Next, there is a common code that is used by all the equipment that accesses one particular radio system. The Teletics term for this is GroupID. Teletics products that are part of a system must have the same GroupID, and we provide software to set this in our equipment. Customers may also change this if they wish. Working in conjunction with this GroupID is another code that is proprietary to Teletics, which ensures no third party equipment may connect with our radios. This code cannot be changed by the customer.

Encryption is also widely used in the spread spectrum world, and there are a number of encryption standards in use. All of Teletics current products use 256 bit encryption.

Encryption methods used in almost any communications product need to be standard encryption methods in order to obtain the legal right to be sold in most countries, in order to meet national security and law enforcement requirements. One such standard is AES, which was considered for many years to be the entry level encryption standard acceptable by government and military agencies.

One of the newest access standards introduced for radio equipment operating in public frequencies is WPA. There are two versions of WPA. One is a version for a server based system, the other (called PSK for Pre-Shared Key), is designed for equipment operating without a server environment. For this reason, Teletics equipment runs a variant of WPA-PSK which uses the stronger enhanced encryption protocol called CCMP, which uses the 256 bit AES based encryption cypher. This encryption is the strongest commercially available open standard currently being used in wireless equipment other than that being sold directly to military. WPA2 is newer, but again uses CCMP, so for purposes of security is identical.

The encryption methodology used in the ZipLine and WOPX G4 radio systems is WPA-PSK with CCMP and a 22 character passphrase established at the factory, and the second passphrase set in the factory with 9 characters , but changeable by the customer in the field up to 30 characters. The 22 character factory passphrase that is hard coded into each Teletics radio in the factory is set using automation software that does not disclose this key to any manufacturing staff and is not published in any documentation. Additionally, there are no software back doors available in any Teletics product. If a factory reset is required when a device comes to Teletics from the field, the device has to be dismantled to reset it.

For details on how to set the customer passphrase (GroupID) in each Teletics product, the customer should consult the programming software manual for the product. These manuals are generally available on the Teletics website or by request from Teletics support.

Field Experiences

Consumer or corporate WiFi has not created issues for any known Teletics customers to date, in either 2.4 GHz or 5.8 GHz installations. The primary reason for this is the difference in power and type of antennas used.

In the Teletics ZipLine product, the integrated antennas used are designed to ignore all but the front 30 degrees, both horizontally and vertically. This "aperture" is chosen to provide isolation while still allowing some error factor in aiming during installation. In our other point to point products, such as the WOPX G4, the antenna selection is usually done by experienced radio designers who will typically specify a more stringent path between the two antennas.

Additionally, the power output of any "commercial grade" product, such as any Teletics radio, will simply overcome the relatively feeble radio outputs of most WiFi radios. Most WiFi radios on the market today do not even publish an RF power output specification. This market is driven primarily by price. Higher power radios cost more to make, and to be fair to these manufacturers, their customers only want coverage inside their building anyway. They do not want everyone outside the building to see their network.

Our customers that do not have the luxury of knowing where they may be operating, such a drilling rigs or public safety organizations, typically choose our equipment operating in the 5.8 GHz band. The reason for this is twofold. First, this band is currently less crowded, and secondly, this band is almost exclusively occupied by newer generation radios which are almost exclusively direct sequence. Direct sequence radios generally cooperate very well. Even if interference from another system operating nearby is enough to cause lost packets, the system will not demonstrate enough degradation for the customer to notice. A good example of this is that we can operate two WKSU-PA 5.8 GHz systems on the bench simultaneously with different GroupIDs, and the only noticeable issue is very slightly lower data speeds on the ethernet networks than would occur with only one system operating.

In point to multipoint radio installations, such as the WKSU-PA or String installations, higher gain antennas which take into consideration the location of the other stations in the system are chosen. This is done with the help of Teletics technical staff, or Teletics distributors. Most importantly, these antennas provide maximum signal power to the areas of the site that need it, and create radio nulls where there is no requirement for signal.

Summary

Unlicensed public radio bands have seen a number of different products over the past two decades. Initially, these bands were used by radio engineers and systems designers for telemetry and control applications. These systems were constructed by people with significant experience in radio frequency design, and generally were used outdoors, or to cover vast areas.

The introduction of WiFi and consumer grade equipment to use these bands has created concern about security, interoperability and coexistence with other equipment operating on the same frequency. Many improvements have been made, and will continue to be made in the future regarding these technical issues.

Teletics continues to follow standards based design in its radio products. Our products fall into an outdoor use class of spread spectrum, public radio band equipment which immediately differentiates it from consumer grade WiFi and similar radio equipment.

Under normal circumstances, when used in the markets the equipment was designed for, our customers can enjoy secure, reliable communications without concern for issues arising from interference or security risks when using Teletics products “out of the box”.

However, for customers with a desire to implement and design their own security methods, Teletics products provide programming capability to allow customization as desired.

Further discussions on this topic are always welcome. You may engage Teletics support, or our company management through our support team, distributors, or representatives at any time. Contact information for us is on our website at www.teletics.com