Comparative Use of Unlicensed Spectrum

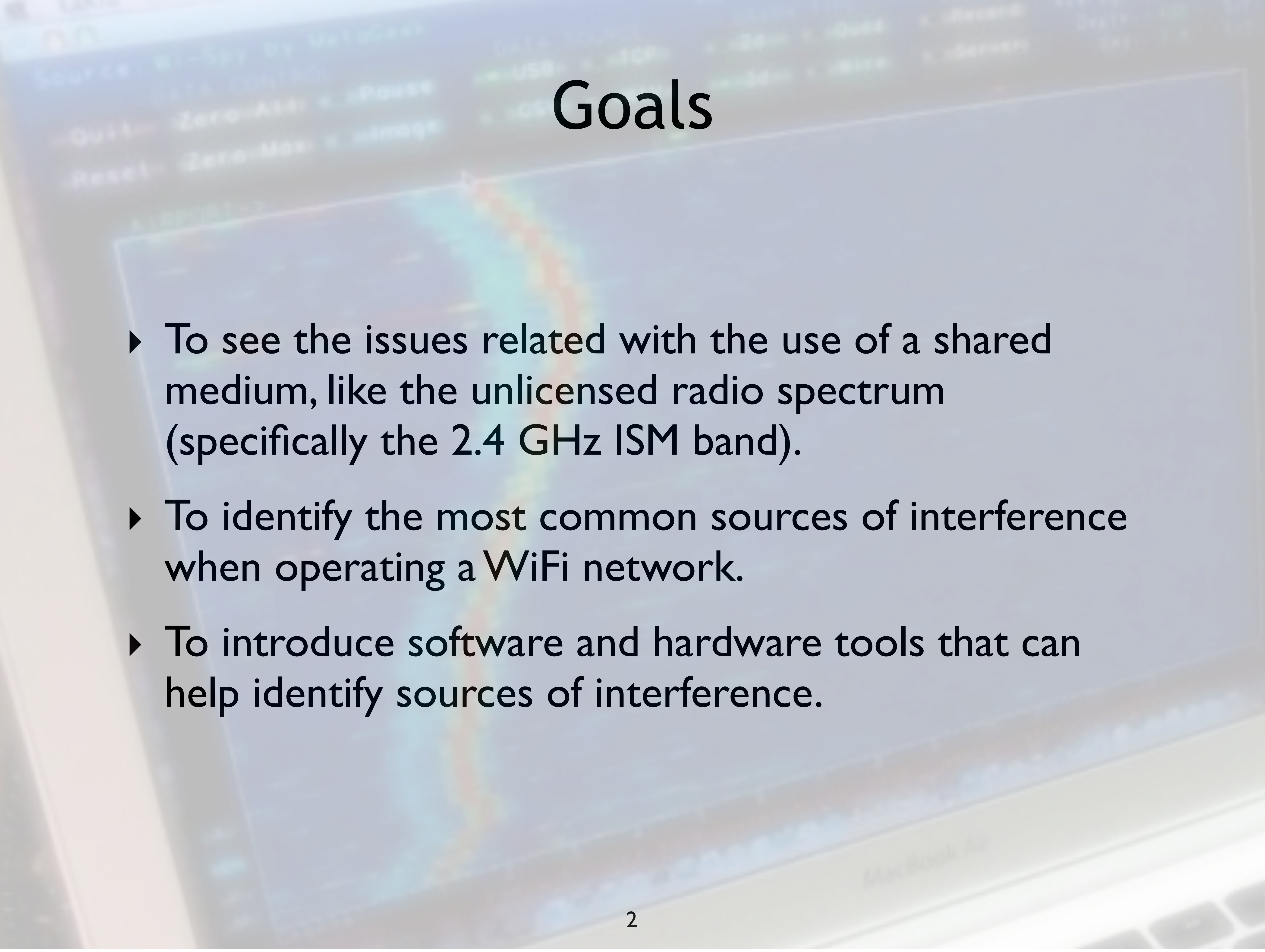
Training materials for wireless trainers

The Abdus Salam International Centre for Theoretical Physics

United Nations Educational, Scientific and Cultural Organization

This 40 minute talk is about the comparative use of unlicensed radio spectrum, specifically in the 2.4 GHz ISM band.
Version 1.2 by Rob, @2009-11-19
Version 1.3 by Rob, @2010-02-25
Version 1.4 by Rob, @2010-03-03
Version 1.5 by Rob, @2010-03-12

Goals



- To see the issues related with the use of a shared medium, like the unlicensed radio spectrum (specifically the 2.4 GHz ISM band).
- To identify the most common sources of interference when operating a WiFi network.
- To introduce software and hardware tools that can help identify sources of interference.

Sharing the air

These considerations are important to keep in mind when using devices that operate using unlicensed spectrum.

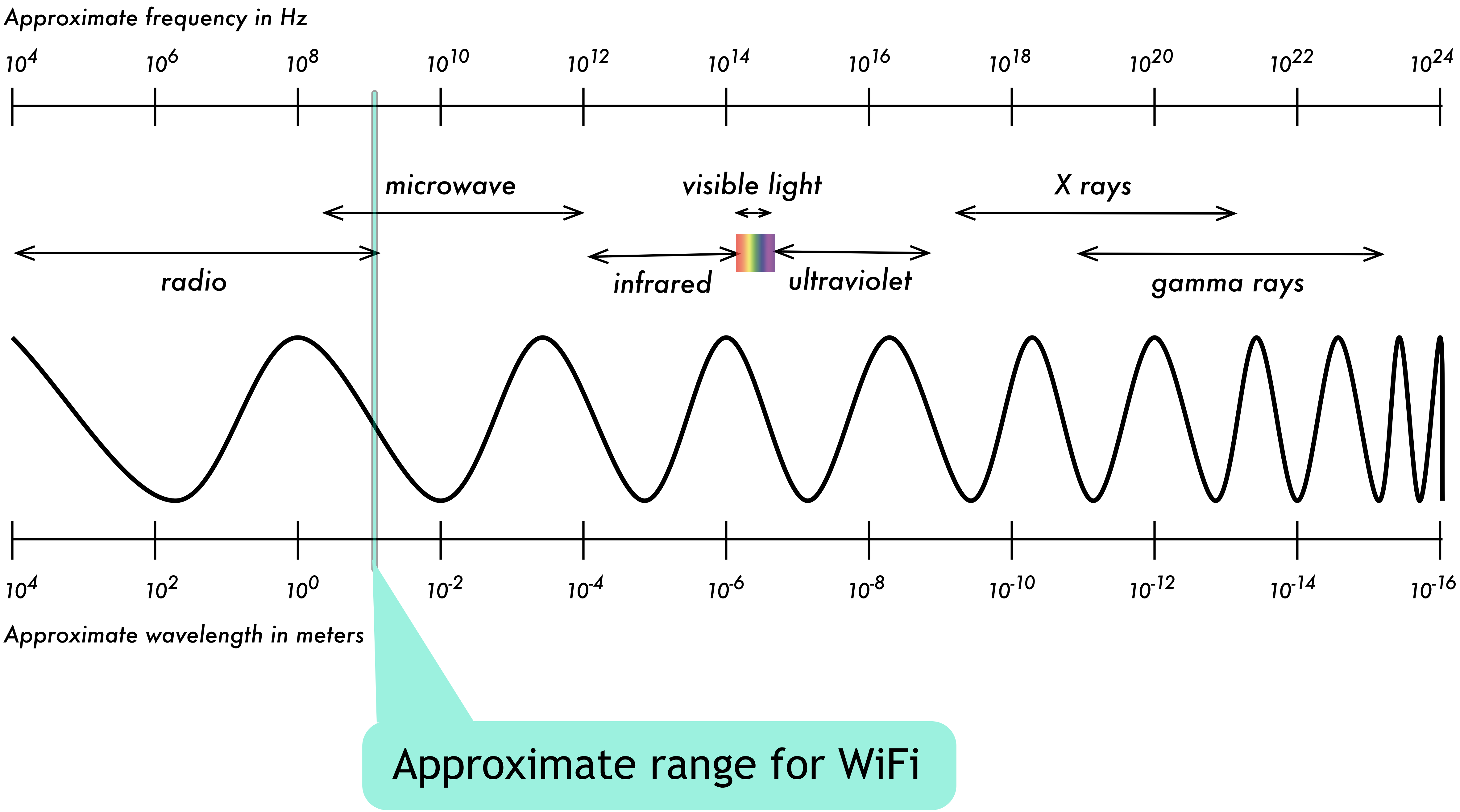
- All devices must share the available radio bandwidth.
- Devices that use different protocols are typically unaware of each other.
- This competition leads to contention, retries, noise, dropped packets, delays, or static.
- The effect and amount of interference depends on how the devices make use of the spectrum.

Different kinds of devices use different protocols that are often completely unaware of each other. Rather than attempt to cooperate and “share the air”, different devices may all attempt to transmit at the same time, causing all kinds of problems.

An analogy is useful here. This lecture can be given because we agree on a common protocol: you all agreed to “give me the floor” to present this material to the class. At the end of the lecture, you may ask questions and we can discuss the material, but only if we agree that one person may speak at a time. When the class is over, the protocol is dropped and everyone will begin to talk to each other at once, making it very difficult to communicate with the larger group.

In the wireless world, you may have a WiFi access point that speaks 802.11 WiFi. You may have another device that speaks its own "cordless phone protocol". Both devices are trying to use the same set of frequencies, but they don't speak the same protocol, resulting in unwanted interference.

Electromagnetic Spectrum



Approximate range for WiFi

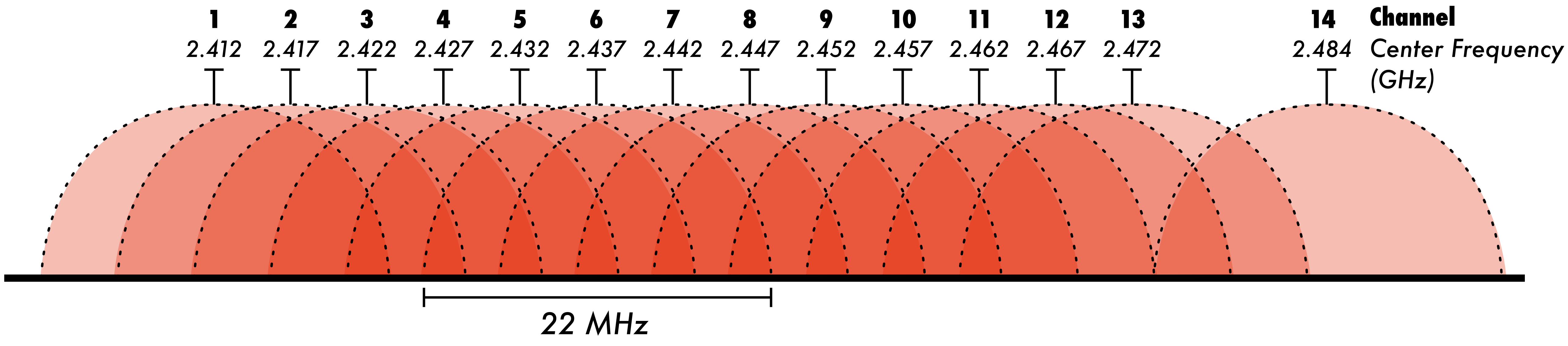
This picture represents the entire electromagnetic spectrum. It goes all the way from very low frequency radio waves on the left, to very high frequency X-rays and gamma rays on the right.

In the middle, there's a very small region that represents visible light. In the scope of the entire electromagnetic spectrum, the range of frequencies that we can actually perceive with our eyes is very small. You can see that on either side of visible light is infrared and ultraviolet.

But the area that we are interested in is the very narrow range of frequencies used by WiFi equipment. That is the very thin sliver at the low end of the microwave range.

The boundary between radio and microwave is not clearly defined. In fact it is common to refer to a microwave transceiver as a "radio".

802.11 Channels

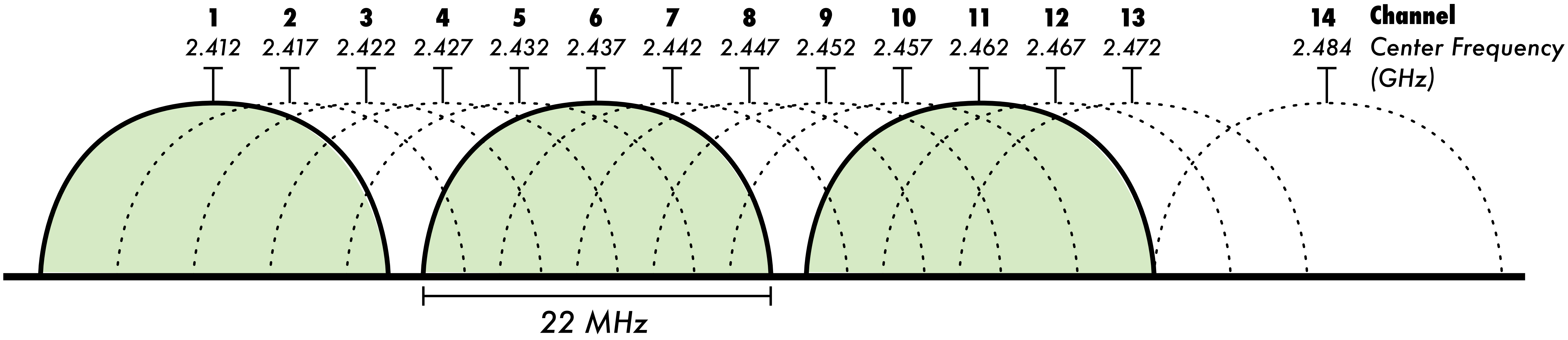


How do 802.11 WiFi devices make use of the available radio spectrum?

WiFi devices can operate at a frequency from 2.4 GHz all the way through 2.48 GHz. The 802.11 protocol chops this entire chunk of spectrum into several discreet channels. Each channel is 22 MHz wide, and each channel is separated by 5 MHz. You can see that this band plan causes the channels to overlap each other. Channel 1 is overlapped by channel 2, which is overlapped by channel 3, etc.

Channel 14 has a greater separation and it is legal only in Japan.

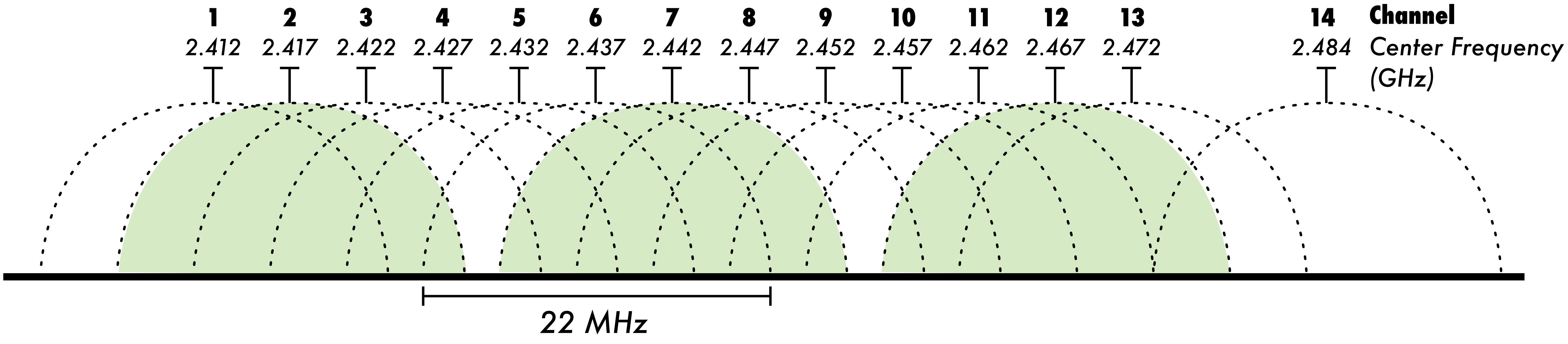
Non-overlapping channels: 1, 6, 11

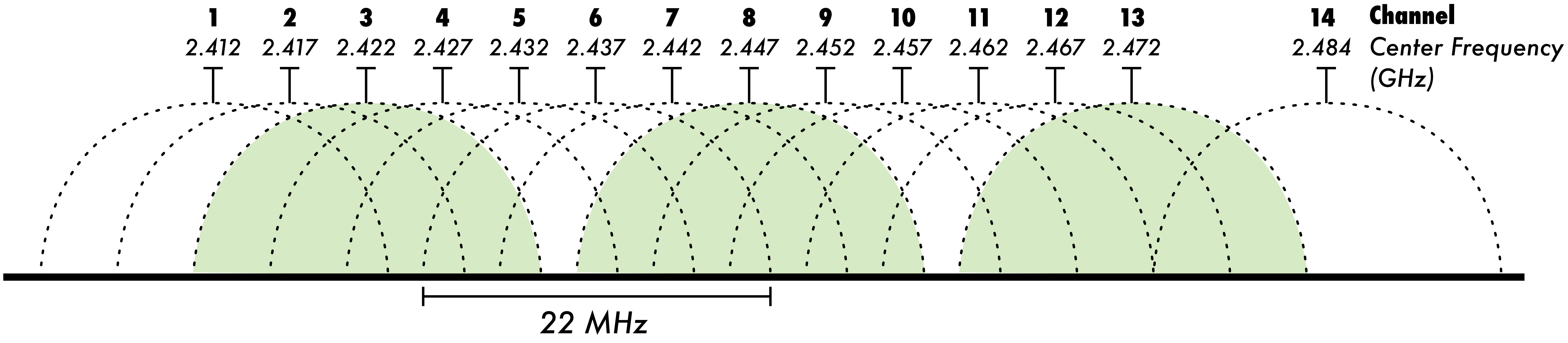


You can choose to use channels that do not overlap at all. If you operate 802.11 equipment on non-overlapping channels, they will not interfere with each other.

For example, channels 1, 6, and 11 do not overlap with each other.

Non-overlapping channels: others

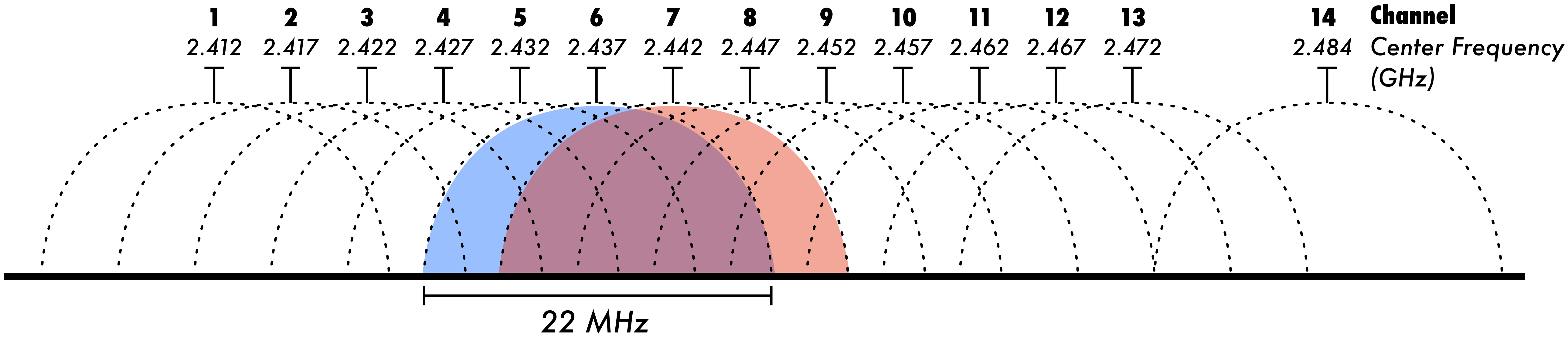




You don't have to use only channels 1, 6, and 11 of course. You can use channels 2, 7, and 12, or 3, 8, and 13. But be sure that you have the right to broadcast on a channel before transmitting. The upper channels are not available for use in every country.

For example, in the United States, unlicensed equipment may only go as high as channel 11.

Adjacent channel interference



What happens if you have no choice, and you **must** operate 802.11 WiFi equipment on overlapping channels?

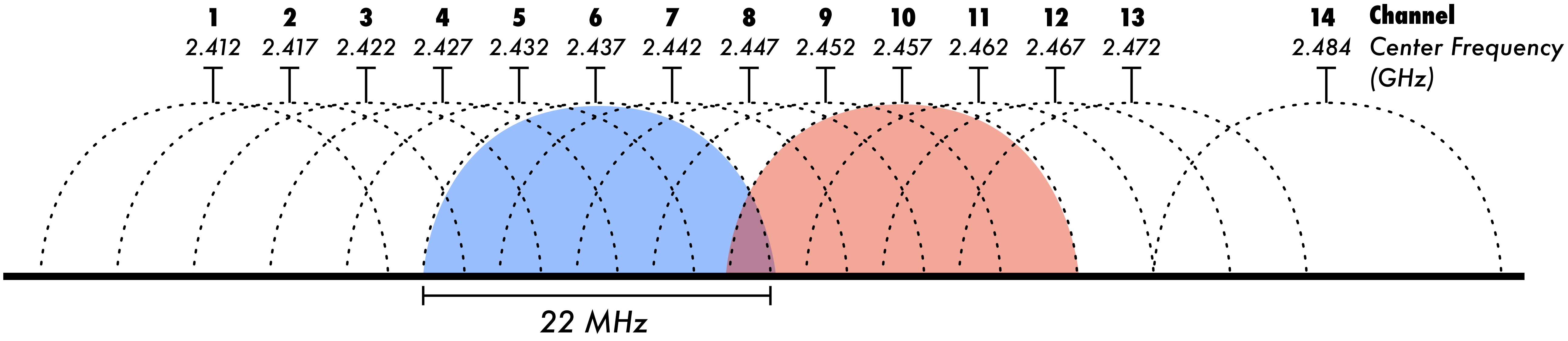
The dark area in the center represents the places where channels 6 and 7 would overlap.

If the channels are being used by non 802.11 devices (like a cordless phone or a video sender) it is better to use the space in between the occupied channels. However, if the three non overlapping channels are being used by 802.11 devices and you must add another Access Point, it is better to use EXACTLY the same center frequency of one of the occupied channels. The throughput will indeed suffer, but the media access mechanism will force one of the Access Points to defer when the other is transmitting resulting in fewer retries. If you choose an intermediate channel, there is a risk that the defer mechanism will not work thus resulting in more retries and lower overall throughput.

In the worst possible case, two access points are operating on the same channel. They would interfere with each other completely. Any time one is broadcasting, the other must defer, and vice-versa.

If you move the equipment to adjacent channels, you can see that most of the spectrum still overlaps, so you still have interference. It's not as bad as operating on the same channel, but it's still causing quite a bit of interference.

Non-adjacent channel interference



If you choose channels that are further apart, perhaps separated by four channels, you can see that the range of frequencies overlap considerably less. This would cause much less interference.

In the best case, you would choose only non-overlapping channels.

Other 2.4 GHz communications devices

Which common communication devices operate at 2.4 GHz?

- 802.11 b/g networks
- Bluetooth devices
- Cordless phones
- Video senders
- Baby monitors

Bluetooth™

What are some other common 2.4 GHz devices that would interfere with our 802.11 networks?

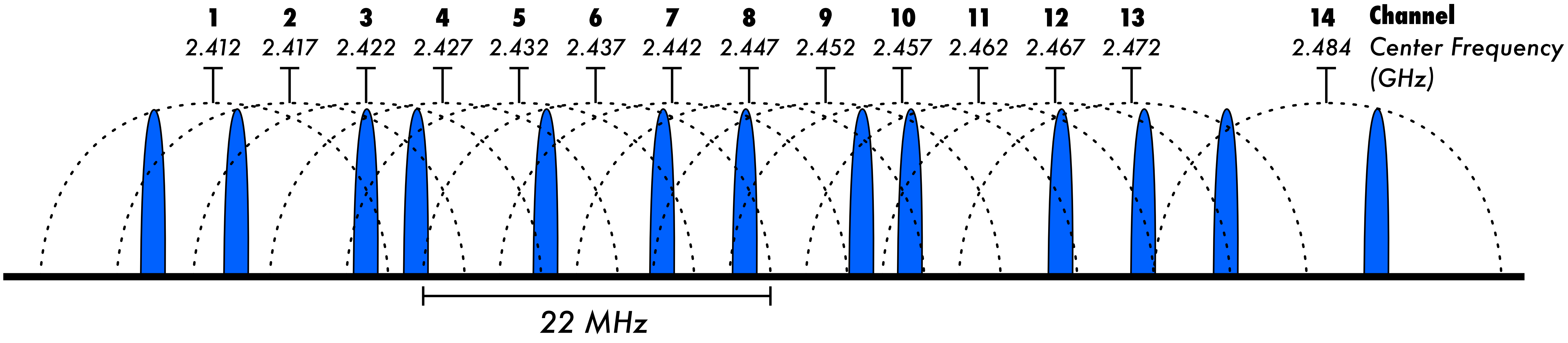
Well obviously, there are other 802.11 networks that are outside of your own control. Maybe someone in an adjacent building is using a WiFi network that could cause interference.

There are Bluetooth devices. For example when a mobile phone sends pictures to your laptop, that can potentially cause interference with your 802.11 network.

Cordless phones are very notorious for causing problems. Cordless phones use very high power and very wide channels that can cause interference.

Finally you have devices like television senders and baby monitors, which use extremely wide channels at 2.4 GHz. These can cause a tremendous amount of interference on your networks.

Bluetooth: frequency hopping

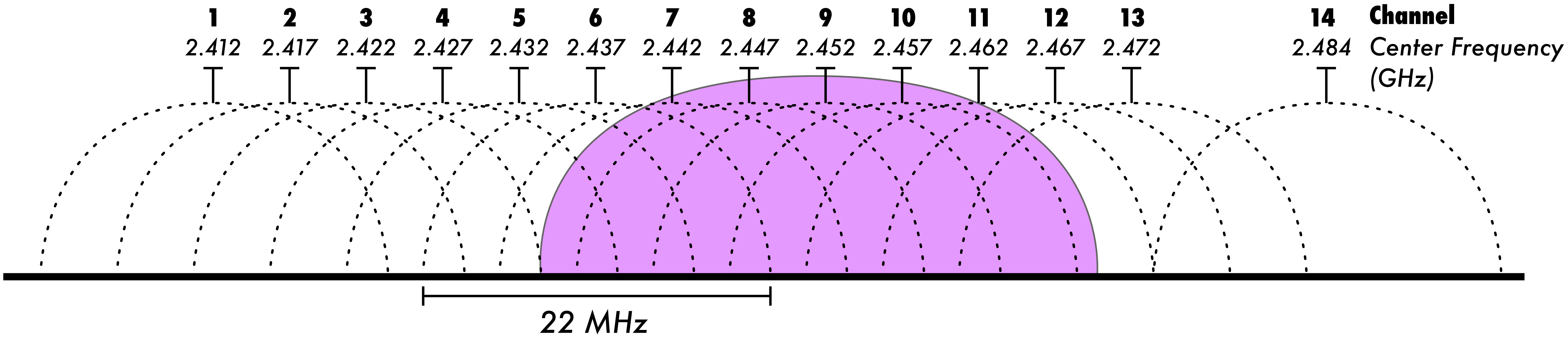


We can compare how each of these different devices characteristically use the available spectrum to better understand how they interfere with each other.

Here we have the channels for 802.11 from the previous slides. The blue shapes represent what a Bluetooth signal would look like in this same set of frequencies. Bluetooth uses a technology called frequency hopping. Instead of choosing a single discrete channel, Bluetooth divides the spectrum into many small slivers and “hops” between them very quickly. It only needs to use a few MHz at a time, but the frequency can be all over the available range and changes quickly over time.

It is unlikely that Bluetooth will completely knock a WiFi network offline, but it can cause some interference with many different channels at the same time.

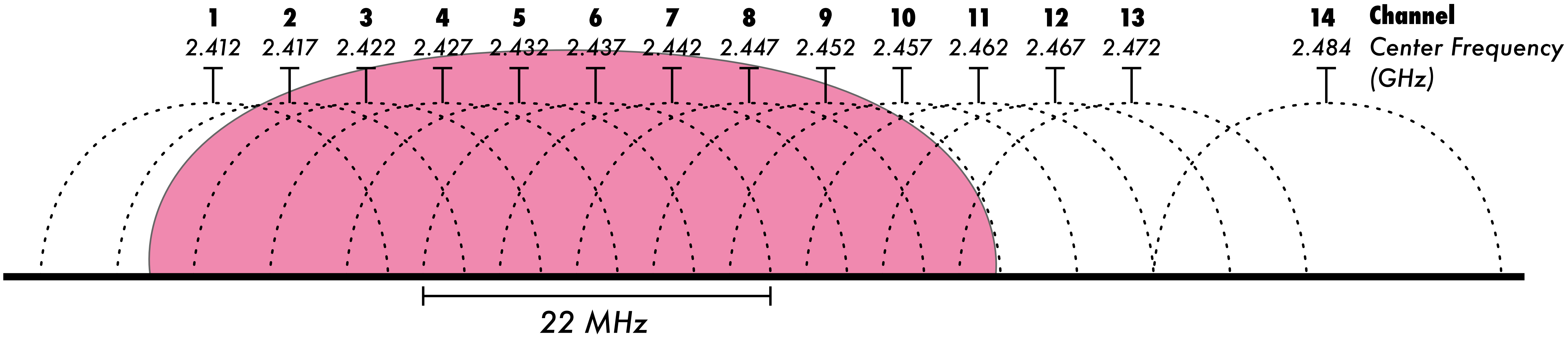
Cordless phones: wide channels



Next we have cordless phones. Cordless phones tend to have a channel even wider than the 22 MHz that 802.11 uses, but it will do it very loudly, typically with much more power than an 802.11 device. It spreads its power out according to its own band plan, with no relation to any sort of 802.11 channel boundary.

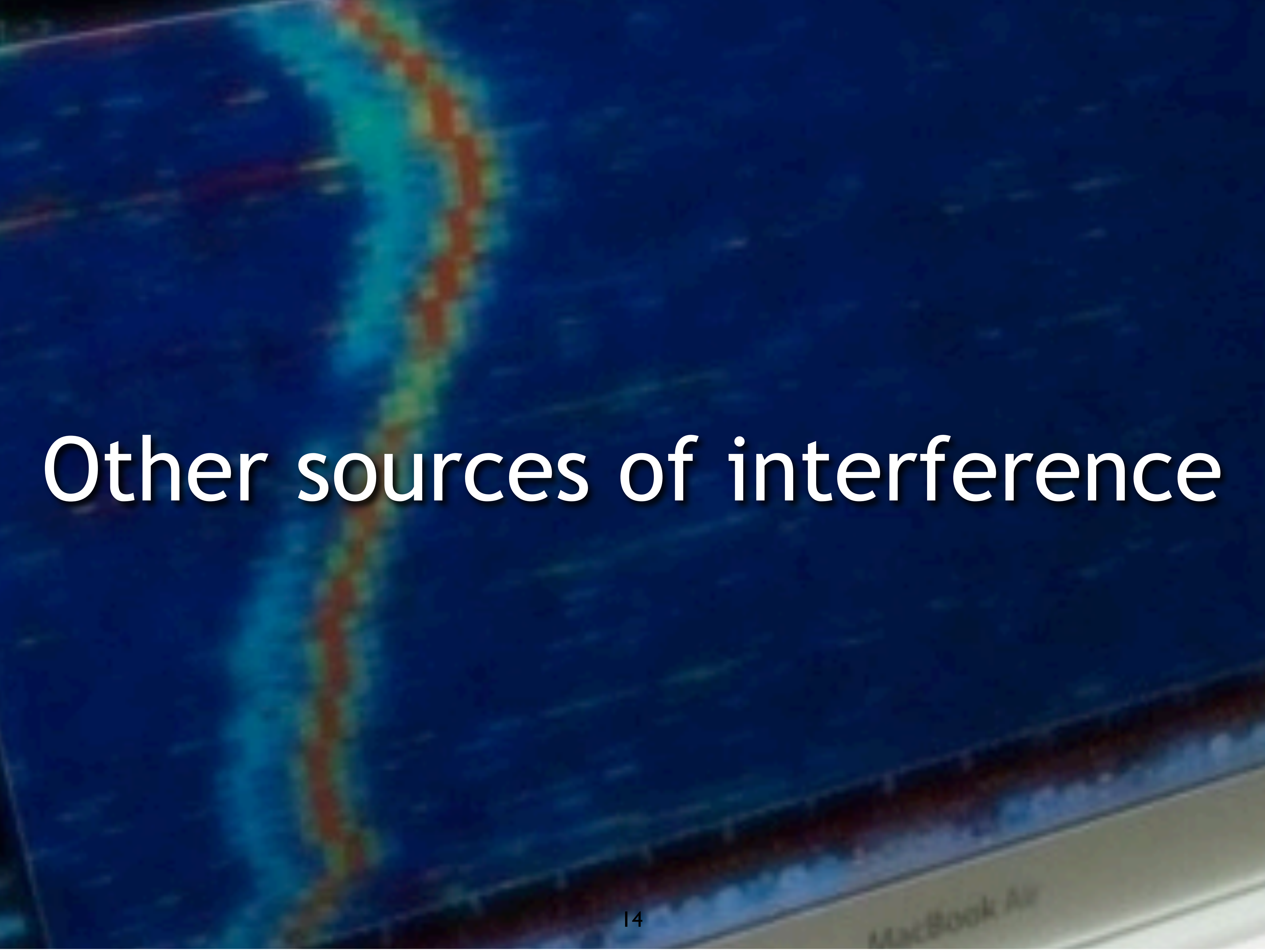
While a cordless phone is on and transmitting, may be causing interference for a great number of 802.11 channels.

Video senders: extreme interference



Finally we have the video sender, which looks a lot like a cordless phone but is even wider, and can be even louder. Video senders that operate at one or two watts are quite common. They are intended to be used with security cameras or baby monitors that can be received over a very wide range. But since video carries a lot of information, it makes use of wide channels. And since they are sending video, they transmit continuously so they are the worst offenders.

Video senders can easily knock out nearby WiFi networks and cause interference for many other 2.4 GHz devices.



Other sources of interference

That's it for communications devices. It seems like there are more communication devices every year that operate at 2.4 GHz. We have just reviewed some of the more common devices on the market now.

But what are some other sources of 2.4 GHz interference that don't even involve communications devices?

Microwave Ovens

Microwave ovens are probably the most common sources of non-communications interference. They cook food by generating huge amounts of microwave energy around 2.4 GHz. This frequency has nothing to do with the "resonant frequency" of water or food. This frequency was chosen when microwave ovens were being developed (in the 1940s) largely because no other devices were used for communications at 2.4 GHz, and turning ordinary house current into powerful 2.4 GHz waves is a relatively simple technology.

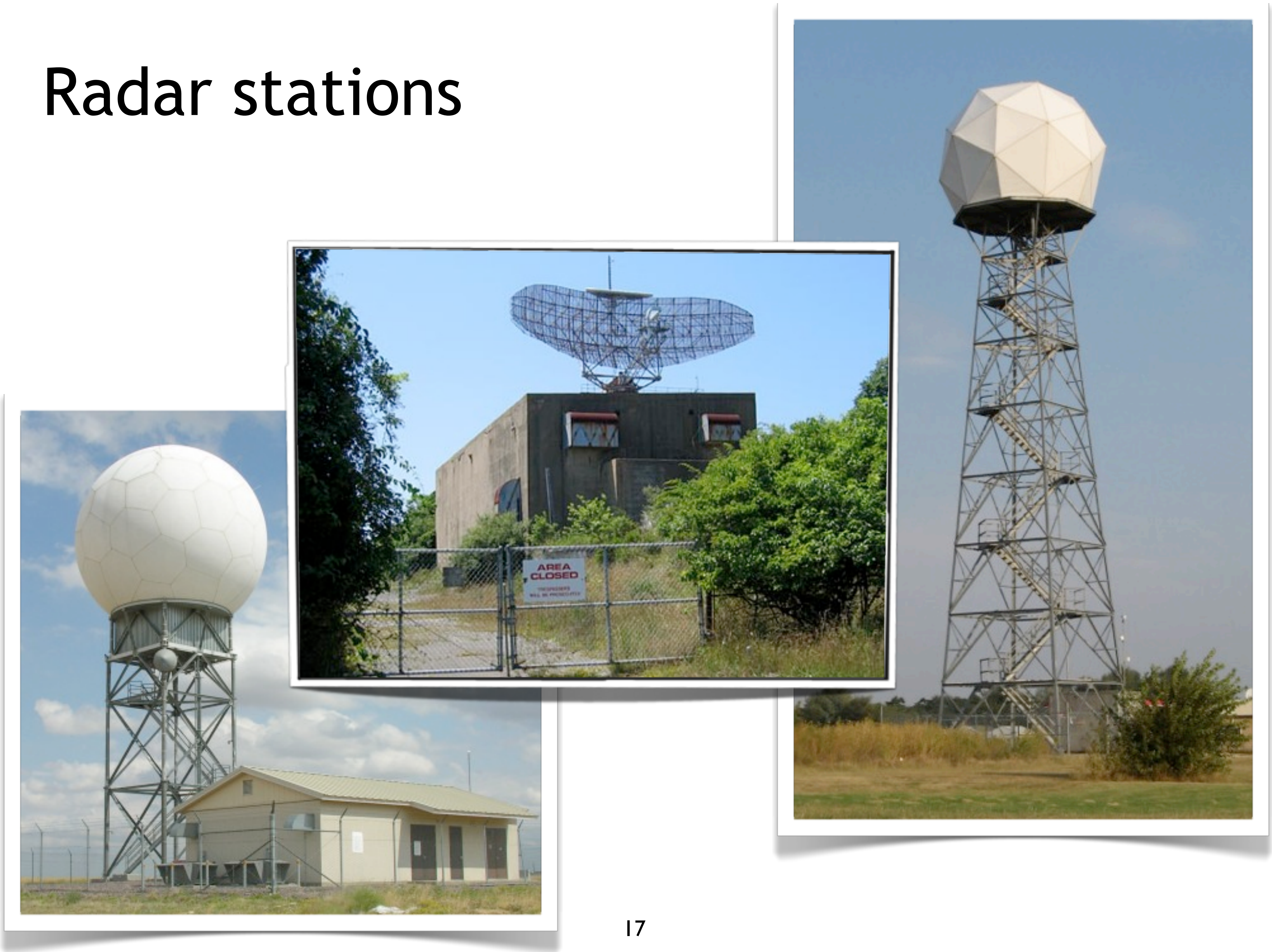
Of course, here we are years later and now we're all trying to make use of the same spectrum for communications! Microwave ovens have a great deal of shielding in order to prevent energy from leaking too far out. Obviously people don't want to cook themselves when using a microwave. But microwaves still leak a little bit of energy. While it's not dangerous to humans, can still interfere with WiFi networks.

You see this problem most often in a café setting. If you have a WiFi hotspot in a café, it's a very common story that people are sitting there, using their laptops, when the network suddenly drops... for three minutes. And then suddenly, it's back. And a little while later it drops again for five minutes. And then it's back. As it turns out, if the café is using a microwave oven, and if they've installed the access point anywhere near the oven, and if the oven is an industrial type that has been used a lot, it's almost certainly going to cause interference.

Power Supplies

Next we have sources of wideband noise. Power supplies can create noise all over the electromagnetic spectrum. PC power supplies are a source of electromagnetic interference that can interfere with WiFi communications, especially in older computers.

Radar stations



Radar stations are another source of interference for WiFi networks, and vice-versa. Radar stations that operate around 5 GHz are much more common than 2.4 GHz, but this becomes an issue if you're going to use 802.11a or 802.11n technologies. Coastal radar around 5 GHz is fairly common. Be very certain of your right to operate wireless equipment at these frequencies before transmitting!

Keep in mind that any signal will have harmonic components at frequencies that are multiple of the stated carrier frequencies. Although normally the transmitter will have filters to limit the out of band radiation, if the signal is very strong the harmonics can cause significant interference, so find out what is the operating frequency of the transmitters at your site and check if its multiples fall into the 2.4 to 2.48 GHz range.

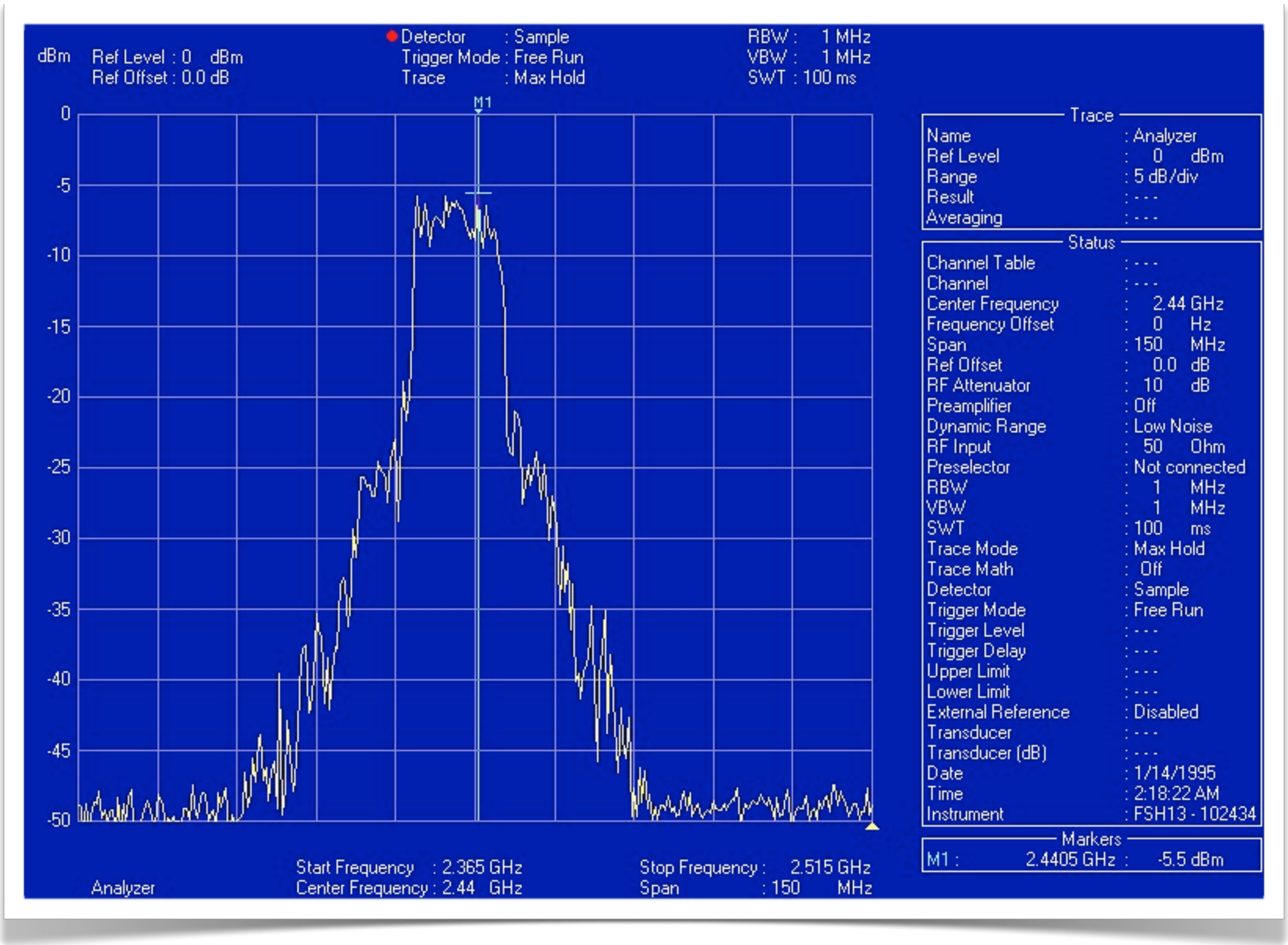
Other high-power radio sources

And finally, harmonics and near-field interactions with other high power radio sources can cause interference. Very high power radio transmitters, such as radio or television broadcast antennas, may interfere with WiFi equipment even though they are not operating at 2.4 GHz

If you install your equipment immediately next to a high-power broadcast antenna, you will certainly encounter interference. While it is possible to mitigate this interference somewhat by using expensive filters, it is usually a better idea to relocate your equipment further away from the high power source.

When co-locating a WiFi system in a tower that houses an FM Station, it is possible that the FM station that broadcasts at around 100 MHz can cause interference. This is because the data is carried to the WiFi by means of a UTP cable which carries Ethernet signals in the same frequency range. If you encounter this type of interference you might want to use STP (Shielded Twisted Pair) or FTP (Foil Twisted Pair) properly grounded to reduce the baseband interference.

Seeing the noise



```
dBm   Ref Level : 0   dBm        Detector     : Sample        RBW :  1 MHz
      Ref Offset : 0.0 dB        Trigger Mode : Free Run      VBW :  1 MHz
                                 Trace        : Max Hold      SWT : 100 ms
```

```
Trace
Name                  : Analyzer
Ref Level             :   0    dBm
Range                 : 5 dB/div
Result                : - - -
Averaging             : - - -
Status
Channel Table         : - - -
Channel               : - - -
Center Frequency      :   2.44 GHz
Frequency Offset      :   0    Hz
Span                  : 150    MHz
Ref Offset            :   0.0  dB
RF Attenuator         :  10    dB
Preamplifier          : Off
Dynamic Range         : Low Noise
RF Input              :  50    Ohm
Preselector           : Not connected
RBW                   :   1    MHz
VBW                   :   1    MHz
SWT                   : 100    ms
Trace Mode            : Max Hold
Trace Math            :  Off
Detector              : Sample
Trigger Mode          : Free Run
Trigger Level         : - - -
Trigger Delay         : - - -
Upper Limit           : - - -
Lower Limit           : - - -
External Reference    : Disabled
Transducer            : - - -
Transducer (dB)       : - - -
Date                  : 1/14/1995
Time                  : 2:18:22 AM
Instrument            : FSH13 - 102434
Markers
M1 :       2.4405 GHz :     -5.5 dBm
```

```
            Start Frequency  : 2.365 GHz     Stop Frequency :   2.515 GHz
Analyzer    Center Frequency : 2.44   GHz    Span           : 150      MHz
```

How can you detect and mitigate these sources of noise?

Unfortunately, it is very difficult to detect the noise directly only using WiFi equipment. The only indication you'll have of interference is that the network doesn't work, or it is very slow and unreliable.

Instead of using WiFi equipment to detect interference, you need to use a tool that can sense energy directly. The best tool for this job is a spectrum analyzer.

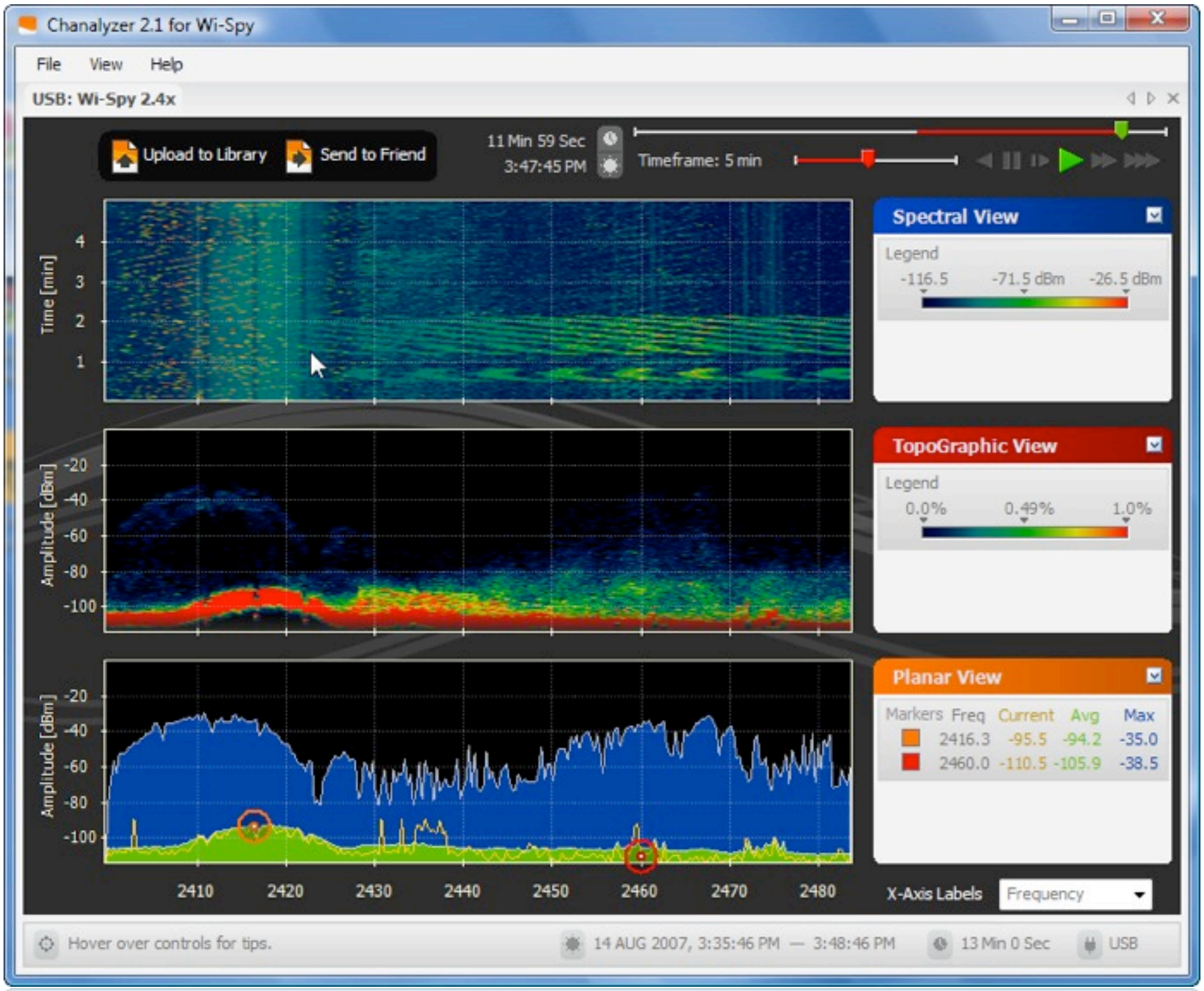
Wi-Spy spectrum analyzer

http://www.metageek.net/

One inexpensive spectrum analyzer is the Wi-Spy. It is a 2.4 GHz USB device that is designed to show you information about 2.4 GHz WiFi. It does this by tuning to a narrow channel in the 2.4 GHz band and listening for energy, then changing to another, and so on all throughout the band as quickly as it can. In this respect it acts a bit like a frequency hopping radio that never transmits. By plotting this information on a graph, you can get a very clear picture of how the 2.4 GHz spectrum is being used by devices in your area. Other versions of the Wi-Spy can also detect 900 MHz and 5 GHz signals.

There are a number of free software packages that work well with the WiSpy.

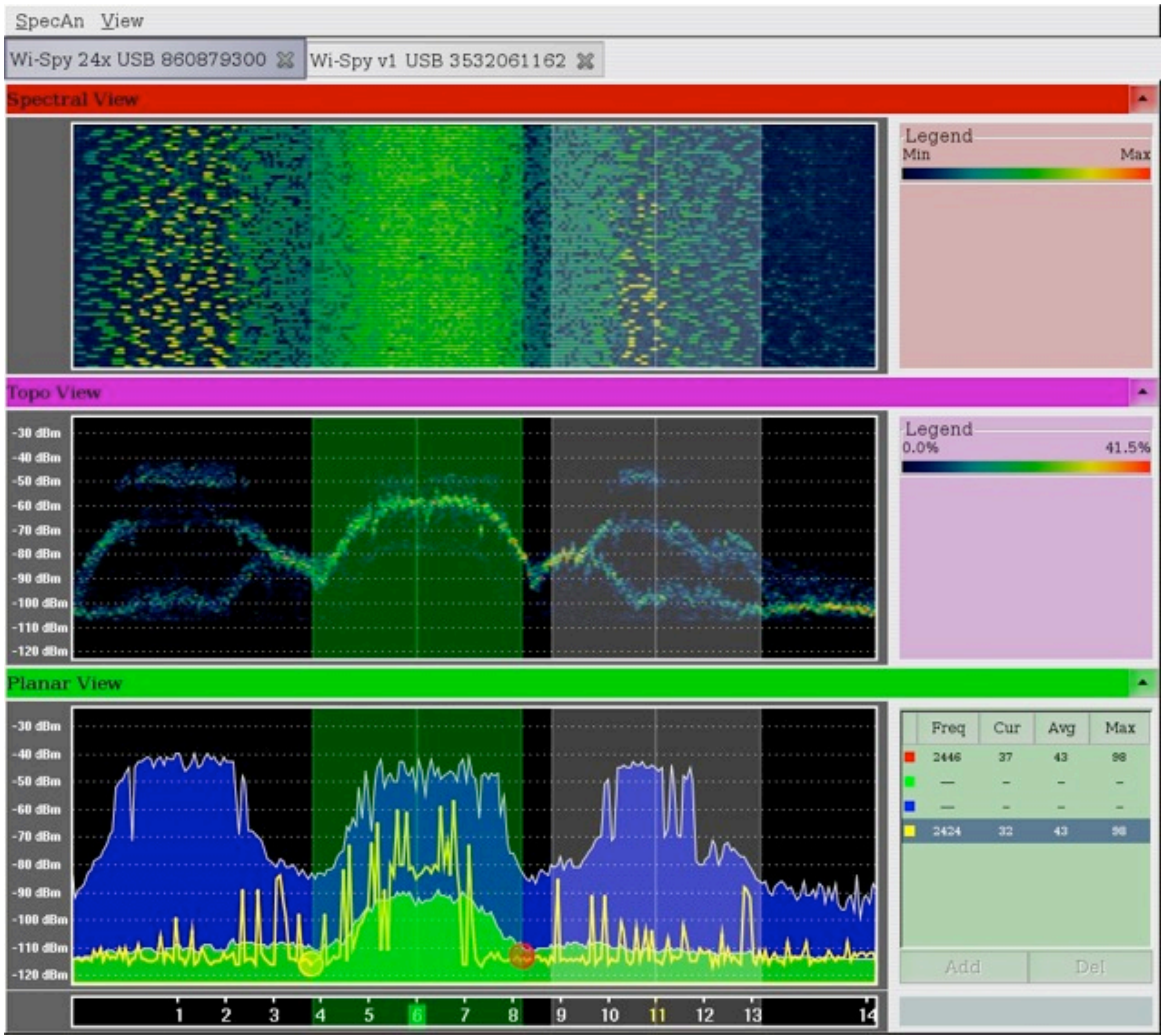
Chanalyzer



Markers	Freq	Current	Avg	Max
🟧	2416.3	-95.5	-94.2	-35.0
🟥	2460.0	-110.5	-105.9	-38.5

The manufacturer supplies very good software called Chanalyzer that works only in Microsoft Windows.

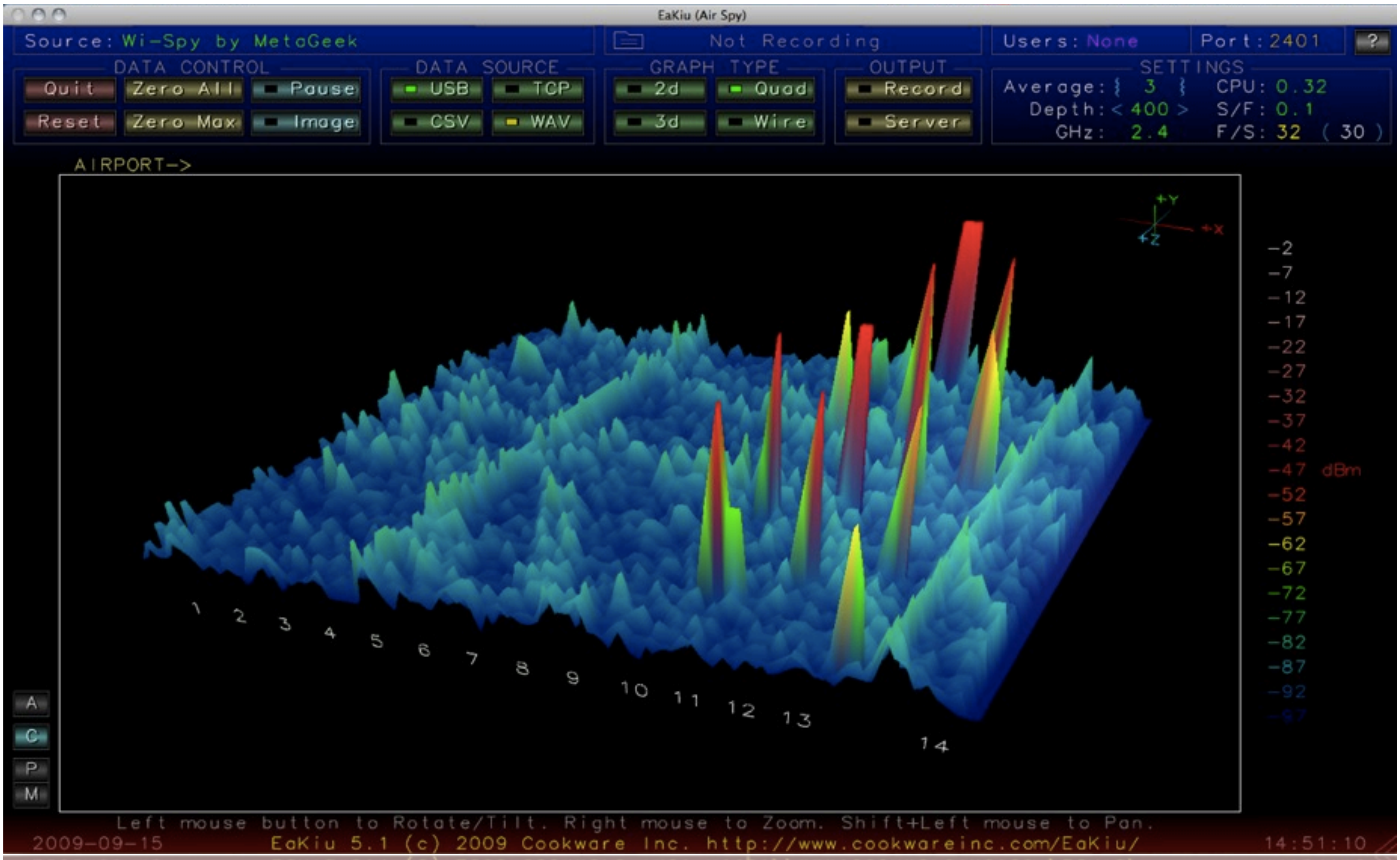
Spectools



	Freq	Cur	Avg	Max
🟥	2446	37	43	98
🟩	—	-	-	-
🟦	—	-	-	-
🟨	2424	32	43	98

The Kismet wireless project provides a package called Spectools that works with Linux, OS X, and Windows.

EaKiu


EaKiu (Air Spy)

Source: Wi-Spy by MetaGeek

Not Recording

Users: None

Port: 2401

Average: { 3 }
Depth: < 400 >
GHz: 2.4
CPU: 0.32
S/F: 0.1
F/S: 32 (30)

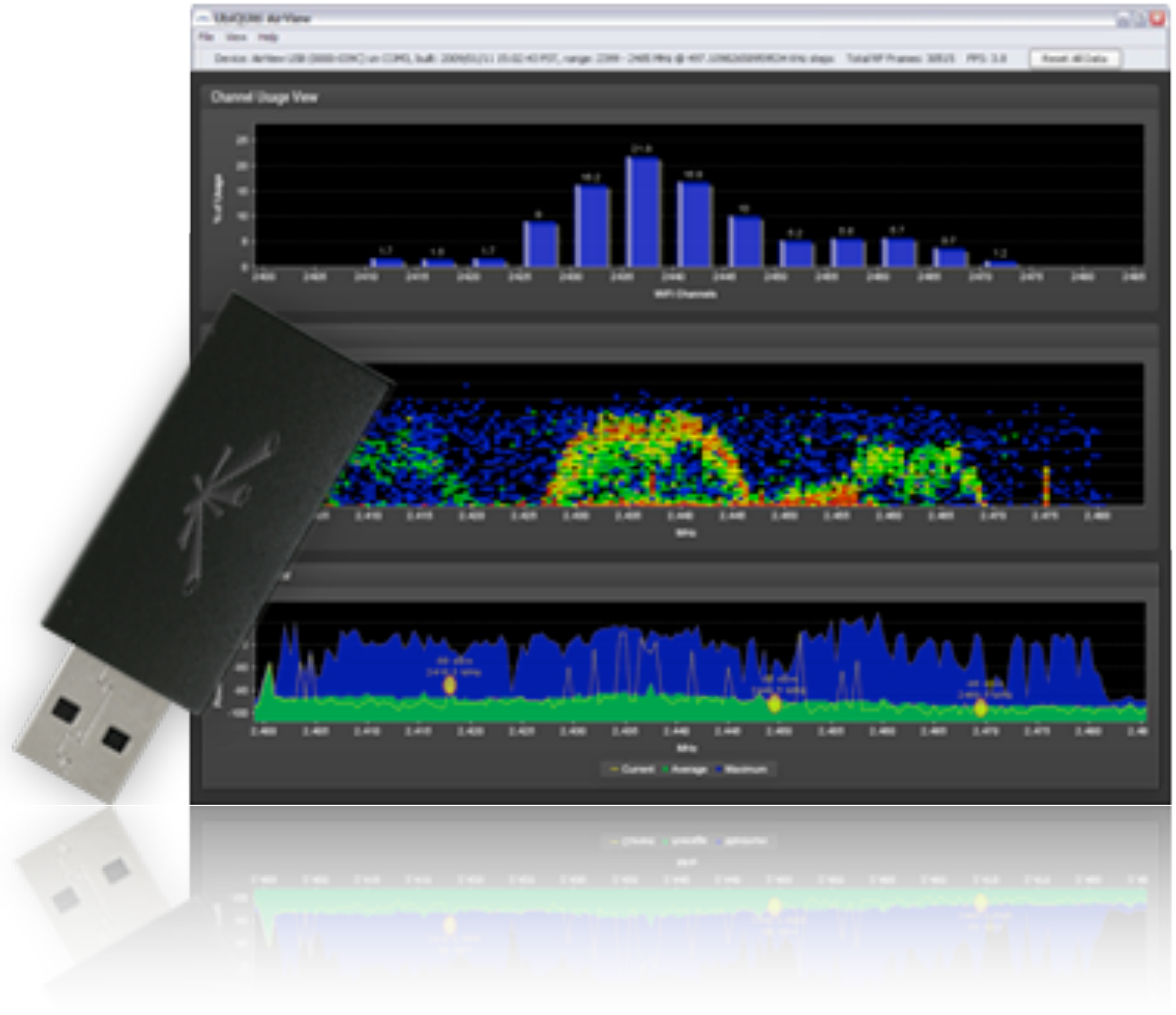
Left mouse button to Rotate/Tilt. Right mouse to Zoom. Shift+Left mouse to Pan.

2009-09-15 EaKiu 5.1 (c) 2009 Cookware Inc. http://www.cookwareinc.com/EaKiu/ 14:51:10

There is a very good package for Mac OS X called EaKiu. In addition to the standard views provided by Chanalyzer and Spectools, EaKiu provides a realtime 3D graph of everything that is happening over time, over the given range of frequencies.

Ubiquiti AirView

http://www.ubnt.com/



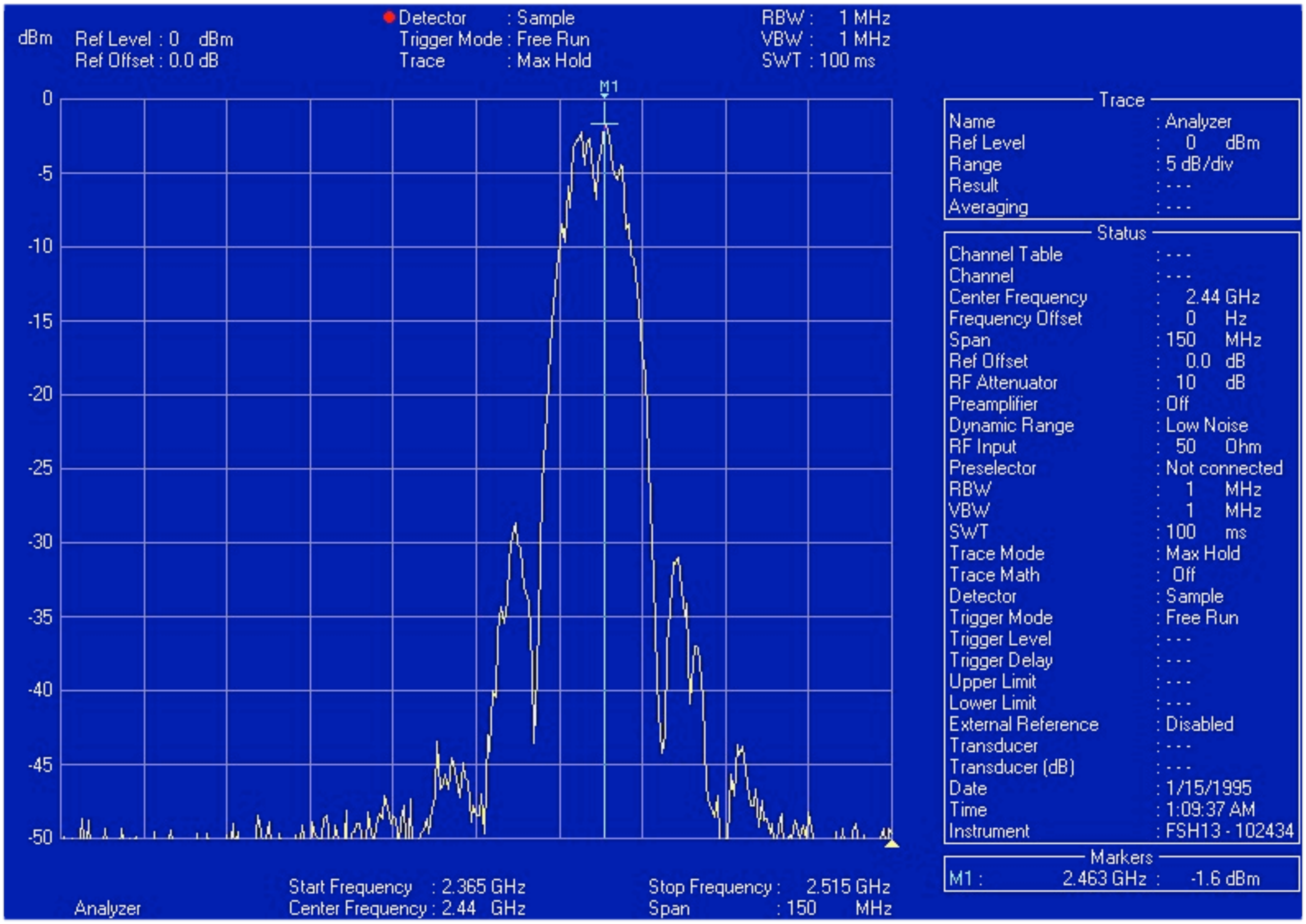
Another new USB spectrum analyzer is the AirView by Ubiquiti. It has similar features to the Wi-Spy, and is considerably cheaper. The AirView software is Java-based and runs on Windows, Mac OS X, and Linux. The AirView comes in 2.4 GHz and 900 MHz models, with or without an external antenna connector.

Spectrum Analyzer

A good spectrum analyzer is usually the best (and most expensive) tool for detecting sources of interference.

If you have one available, a traditional spectrum analyzer will show you these sources of noise. Unfortunately spectrum analyzers tend to be quite expensive. A good spectrum analyzer that operates at 2.4 GHz can cost anywhere from a several hundred to several thousand dollars.

Using a spectrum analyzer



Ref Level : 0 dBm
Ref Offset : 0.0 dB

Detector : Sample
Trigger Mode : Free Run
Trace : Max Hold

RBW : 1 MHz
VBW : 1 MHz
SWT : 100 ms

Trace

Name : Analyzer
Ref Level : 0 dBm
Range : 5 dB/div
Result : - - -
Averaging : - - -

Status

Channel Table : - - -
Channel : - - -
Center Frequency : 2.44 GHz
Frequency Offset : 0 Hz
Span : 150 MHz
Ref Offset : 0.0 dB
RF Attenuator : 10 dB
Preamplifier : Off
Dynamic Range : Low Noise
RF Input : 50 Ohm
Preselector : Not connected
RBW : 1 MHz
VBW : 1 MHz
SWT : 100 ms
Trace Mode : Max Hold
Trace Math : Off
Detector : Sample
Trigger Mode : Free Run
Trigger Level : - - -
Trigger Delay : - - -
Upper Limit : - - -
Lower Limit : - - -
External Reference : Disabled
Transducer : - - -
Transducer (dB) : - - -
Date : 1/15/1995
Time : 1:09:37 AM
Instrument : FSH13 - 102434

Markers

M1 : 2.463 GHz : -1.6 dBm

Start Frequency : 2.365 GHz
Center Frequency : 2.44 GHz
Stop Frequency : 2.515 GHz
Span : 150 MHz

Spectrum analyzers are complex tools, but the main interface is straightforward to read. The Y axis shows the received power level (typically in dBm), and the X axis shows the frequency. The analyzer samples radio energy in very small chunks (the ***sample bandwidth***) and tunes to every set of frequencies on the display (the ***span***). It then draws a line showing the received power level for the entire span. The line can be redrawn as desired to show the instantaneous reading (***clear/write***), an average, or the maximum received reading (***max hold***). A ***marker*** can be inserted anywhere on the line to see detailed information about the sample of interest. In this example, the marker shows the peak of a signal at 2.463 GHz, received at -1.6 dBm.

The particular shape of a transmitter signal as shown on a spectrum analyzer is used to verify compliance with the spectral mask. This example shows the spectrum of a 200mW (23dBm) 802.11b radio. For this type of radio the spectral mask requires that at frequencies between 11 and 22 MHz at both sides of the center frequency of the channel the signal components must be 30 dB below the maximum values. For frequencies further apart, the maximum admitted value of the components is 50 dB below the value at the center of the channel.

We'll now see some examples of how to use these tools in order to detect interference on your WiFi networks.

BEGIN DEMONSTRATION.

Thank you for your attention

For more details about the topics presented in this lecture, please see the book ***Wireless Networking in the Developing World***, available as free download in many languages at:

http://wndw.net/

WIRELESS NETWORKING
IN THE DEVELOPING WORLD
SECOND EDITION
A practical guide to planning and building low-cost telecommunications infrastructure
wndw.net

See Chapter 4 of the book for more detailed information about the material covered in this talk.