TOM BRIDGE, TECHNOLUTIONARY
CHRIS DAWE, WHEELWRIGHTS

# FUNDAMENTALS OF WI-FI

# TOM & CHRIS'
# WI-FI DEATH MARCH

# WI-FI NETWORKS ARE AN ARGUMENT WITH PHYSICS

Kurt Cobain (RIP)

# TODAY'S AGENDA

- A Brief History of 802.11
- Terminology and Jargon
- Building Good Networks
- Tools & Troubleshooting

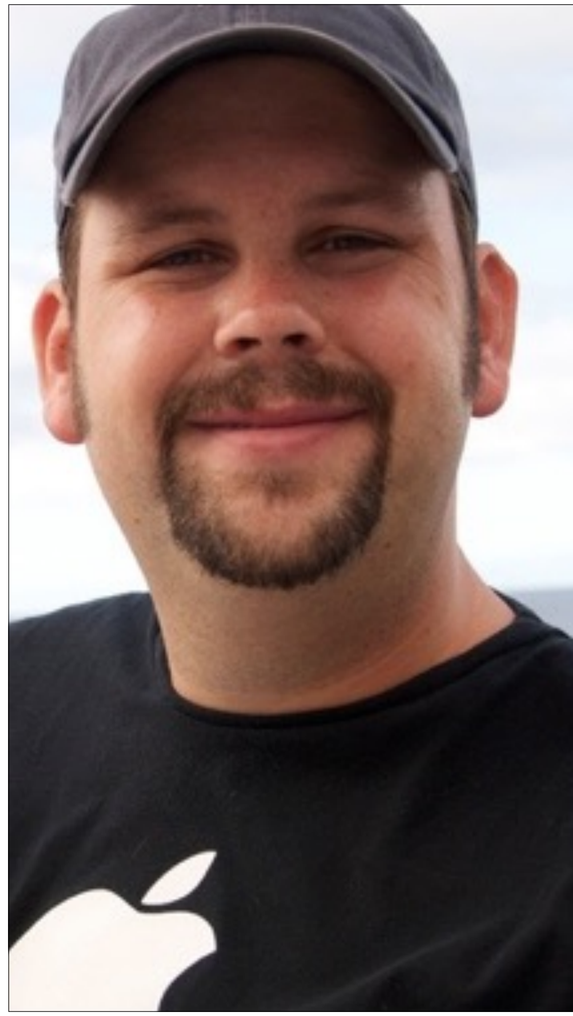
## A (NOT SO) BRIEF HISTORY OF 802.11

- The Birth of Wi-Fi
- Standards We Care About (802.11a/b/g/n/ac)
- The 2.4 and 5Ghz spectra
- The Physical Constraints of Wi-Fi

WHEELWRIGHTS, LLC
SEATTLE, WA

# CHRIS DAWE

Chris Dawe is Principal Systems Engineer at Wheelwrights, LLC, in Seattle, Washington. Chris focuses on MacOS, iOS, and networking, and handles everything from customer assessment to system design, deployment, and support. When not working, Chris reads, cooks, and appreciates both whiskey and whisky.



TECHNOLUTIONARY, LLC
WASHINGTON, D.C.

# TOM BRIDGE

Tom Bridge is a founding partner at Technolutionary LLC, based in Washington DC. Technolutionary supports 400 users from small business to medium enterprise in a mix of Mac and PC, with a dash of Linux and a healthy serving of iOS devices. He lives in Brookland, DC, with his wife, Tiffany, their son Charlie, and their cats, Macro and Bokeh.

# WI-FI IS EVERYWHERE

Wi-Fi is everywhere. Wi-Fi has grown from a technological curiosity to an ubiquitous and non-negotiable service over the last ten years. So, why is it so nebulously handled by IT admins? Why does conference Wi-Fi so often stink to high heaven? Tickets to troubleshoot it land in the help desk's lap, but most of the time, the fixes and administration are handled elsewhere, leaving the average admin out in the cold when it comes to understanding how Wi-Fi works, how to troubleshoot it smartly, and how to handle planning of medium- and large-scale wireless networks that work well.

QUESTION: How many IT Directors? Consultants? Help Desk? Other?

# HOW DID WE GET HERE?

This workshop will start at the very beginning, with the 802.11 standards, a clear understanding of the physics properties of wireless networking and the basic challenge of the medium. We intend to provide a good physics background for the operating methodology of Wi-Fi, in both the 2.4 and 5Ghz spectrums. Building upon that, we will lay down the clear terminology and nomenclature for thinking and speaking correctly about Wi-Fi.

But first we have to cover some of the basics.

HOW DID WE GET HERE?!


In 1985, the FCC set aside the 2.4-2.5Ghz spectrum for use by the Industrial, Scientific and Medical communities. This meant you no longer had to have an FCC broadcaster's license (something that required lawyers, money and domain knowledge to acquire)

In the early 1990s, the IEEE standards bodies realized that really what they needed, if they wanted to make this wireless thing work, would be some standards. Much as networks evolved and coalesced around the 802.3 Ethernet standard, they could coalesce and standardize around a wireless standard.

Enter 802.11.

The goals were: reliable, fast, inexpensive and robust.
How'd they do? Meh, 1mbps, Several hundred $, supported 10-20 clients.

# WHY 2.4GHZ?

# BECAUSE OF THE SCIENCE OVEN.

In the case of 2.4Ghz, it's because this particular part of the spectrum belonged to the area called ISM, and it didn't require an operator's license. The ISM - Industrial, Scientific, Mechanical - section is for open use by industry. In specific, the 2.4Ghz area was one that was already full of *some* interference from your basic kitchen microwave. These were everywhere, and they were totally deleterious to everything else around them. They


IGN

# THE GROUND RULES OF WI-FI

## PHYSICAL LAYER

- Each radio is like one big hub - that requires Collision control.
- There is no Collision Detection in Wi-Fi
- There is only Collision Avoidance
- All your comms are Half Duplex

| | Layer |
|---|---|
| Host layers | 7. Application |
| | 6. Presentation |
| | 5. Session |
| | 4. Transport |
| Media layers | 3. Network |
| | 2. Data link |
| | 1. Physical |

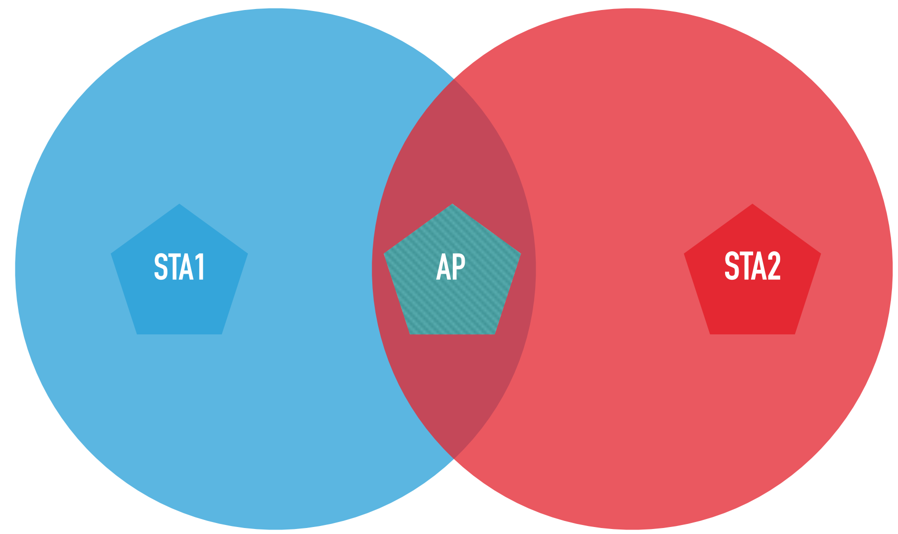
Wi-Fi is a bunch of packets running dead toward your receiver at full tilt. Only, without any kind of traffic cop in the mix.

# DETECTION VS AVOIDANCE

When it comes to Wi-Fi one of the biggest problems you're going to face is the difference between Carrier Sense Multiple Access Collision Detection (CSMA/CD) and Carrier Sense Multiple Access Collision Avoidance (CSMA/CA). Collision Avoidance means that clients are less aggressive with their communications, and you're going to see an increase in the number of necessary retransmits due to the focus of the medium.

Some signals are going to take longer to transmit, especially when you consider as clients increase on a radio, so will collisions. This is where Request to Send and Clear to Send traffic directions come into play.

# WHY AVOIDANCE?

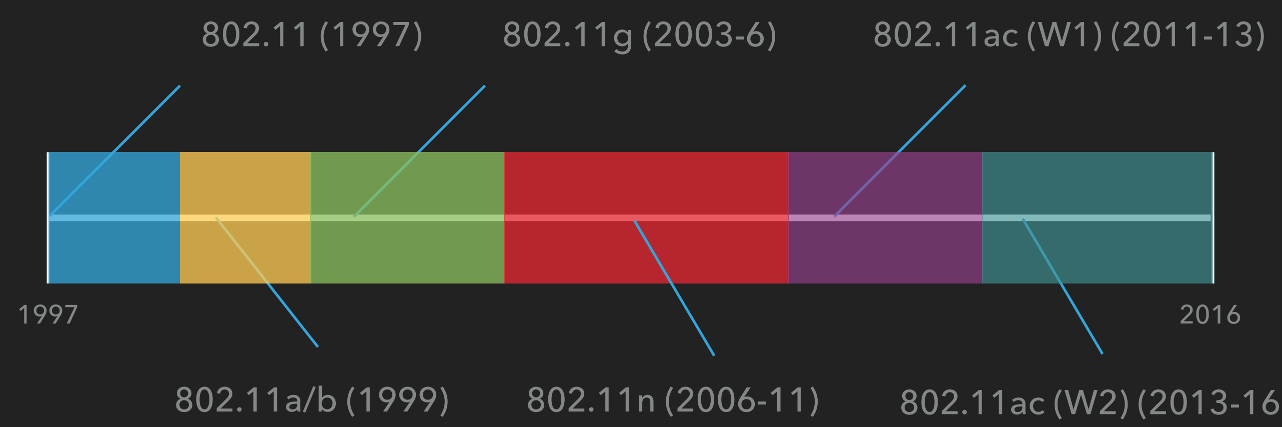



Welcome to Wi-Fi's single biggest pain in the ass: the Hidden Node Problem.

Station 1 on the left can hear the AP, and the AP can hear it. Station 2 on the left can hear the AP, and the AP can hear it.

Stations 1 and 2 cannot hear each other.This creates a huge problem for which Collision Avoidance is the only solution.

# WI-FI TIMELINE



# 802.11 (1997)

- 2.4Ghz
- 2Mbps
- Sets the 20Mhz Channel Width
- Sets original 11 Channels
- Frequency Hopping or DSSS

# 802.11A/B (1999)

- 2.4GHz for 802.11b, 5.8 GHz for 802.11a
- 11Mbps for 802.11b, 54Mbps for 802.11a
- WEP Encryption only
  (40-bit, then 128-bit, both insecure)
- Beacon rates can slow the network substantially
- Uses CCK in 802.11b, OFDM in 802.11a

CCK = Complimentary Code Key
OFDM = Orthogonal Frequency Division Multiplexing

# 802.11G (2003–2006)

- Adds WPA Encryption (still vulnerable)
- Switch from CCK to OFDM to improve interference handling
- But has to support CCK mode for 802.11b compatibility, which can slow whole networks down
- 54Mbps comes to 2.4GHz

> "BUT TOM, WHAT ABOUT
> WIRELESS DISTRIBUTION SYSTEM?"

– Conference Workshop Attendee, Probably

# WIRELESS DISTRIBUTION SYSTEM

- What happens when you extend wireless *with* wireless?
- Consists of Main Base Station, Relay Base Stations, Remote Base Stations
- Use the same channel, encryption type and key
- Each WDS link halves the bandwidth

Wireless Distribution System is a fairly specialized way to extend your wireless network. It was popular in the early days of 802.11g, and it uses techniques that sounds good at the time.

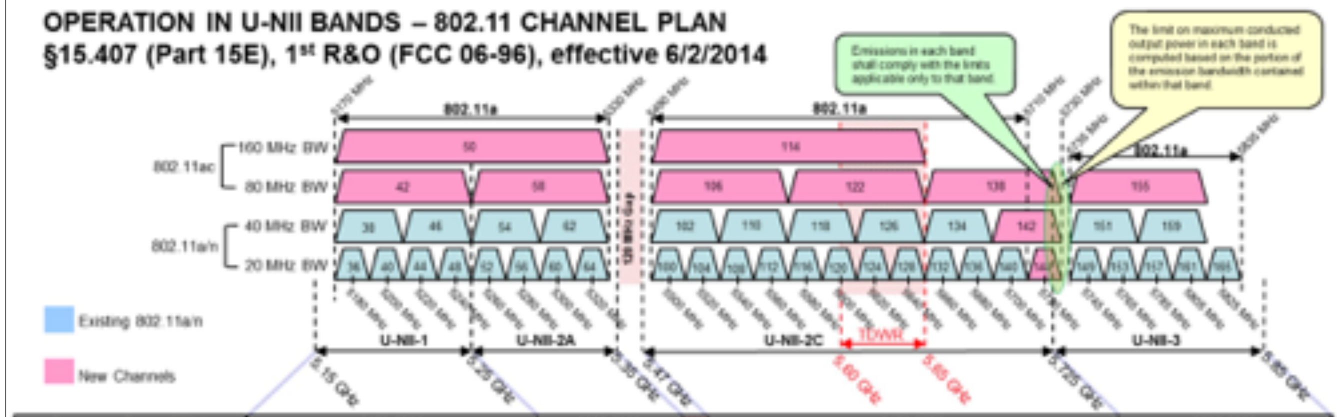
TEXT

# 802.11N (2006–2011)

- 2.4 or 5GHz
- 20 OR 40 MHz channel widths
- 600Mbps theoretical max
- Hello, MIMO
- WPA2 Introduced, TKIP deprecated, AES introduced

5GHz was an optional add-on for 802.11n, and many of the networks

**OPERATION IN U-NII BANDS – 802.11 CHANNEL PLAN**
**§15.407 (Part 15E), 1st R&O (FCC 06-96), effective 6/2/2014**




What's DFS?
Dynamic Frequency Selection
Because part of the 802.11n 5 GHz spectrum is shared with Terrain Doppler Weather Radar and other radars, the standard includes a requirement for WiFi equipment to be able to detect radar signals and adjust frequency to avoid interfering.
Is there a reliable database of places where you would expect DFS to be an issue?
http://udia.spectrumbridge.com/udia/home.aspx
Practical effects of DFS interference detection
Your APs have to use it if they're transmitting above 500mW
And they will be. (standard is 1W)
They will listen for maximum interference (100% of power) in the space, and then move if necessary.
It is unlikely that *all* the DFS channels will be in use at one time. Unless you backup on a military base AND a weather station AND some other user of that spectrum
Implications for design
Your geography will affect your ability to use these channels
If you do use these channels and they pick up a radar, your network is going to adjust itself automatically, and that will probably look like a loss of service, however briefly.
As a secondary issues, when your APs reconfigure themselves, you're in danger of them doing it in such a way as to generate co-channel interference


East Brunswick
Reading
Trenton
Lancaster
Norristown
Lakewood
Philadelphia
Chester
Wilmington
Newark
Bel Air South
Vineland
Frederick
Baltimore
Atlantic City
Columbia
Dover
Leesburg
Wheaton-Glenmont
Annapolis
Washington
Chantilly
Burke
Dale City
St. Charles

# MIMO

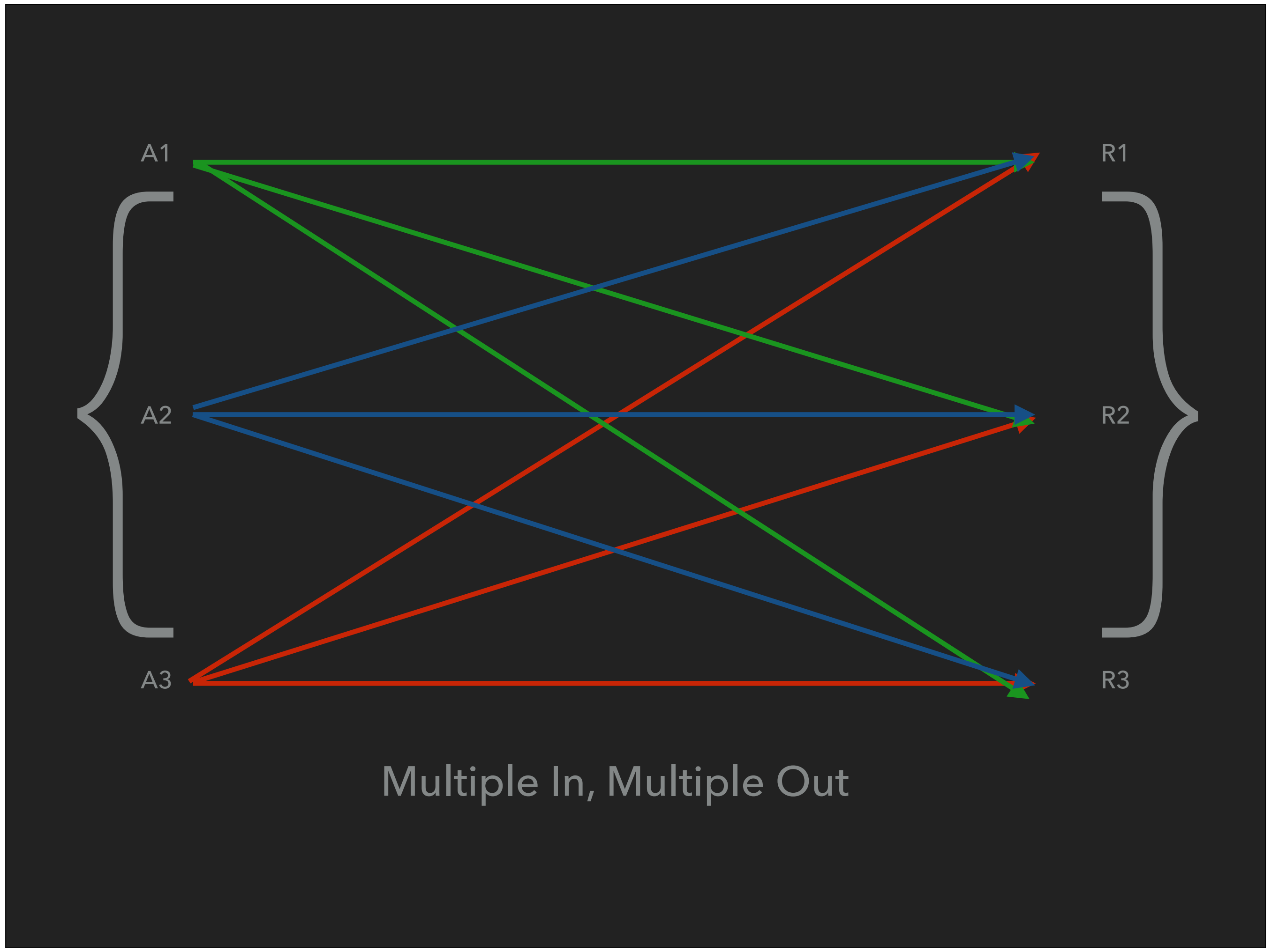
Notation is: T x R : S

Transmit radios, receive radios, Streams

You will often see 2x2:2, 3x3:2, and 3x3:3 in access points. Know the difference and why that matters.

Also recognize that most of your iOS devices (pre-iPhone 5s, iPad Air 2) are single stream devices that won’t benefit from MIMO in the same way that multiple stream devices will.

Plan for the network you want in the future, but recognize the choke points for older devices.


A1
A2
A3
R1
R2
R3
Multiple In, Multiple Out

T × R : S

# 802.11AC WAVE 1 (2013)

- 5GHz only
- 20/40/80 MHz channel widths
- 1.2Gbps Theoretical Max
- Can use up to 4 streams
- Can use 256 QAM

With great bandwidth comes great responsibility. Welcome to the scary world of 802.11ac.

# 802.11AC WAVE 2 (2014)

- 5GHz only
- 20/40/80/160 MHz channel widths
- 6.9Gbps Theoretical Max
- That means you need 10GbE to your AP!
- Up to 8 streams (4 in practice)
- MU-MIMO!

# 802.11AX (2018/2019)

- 5GHz only
- 80 or 160 MHz channel widths
- 10Gbps Theoretical Max
- OFDMA (powers LTE)