Wi-Fi 101

Fundamentals, Design and Troubleshooting

Who am i

Troy Martin @troymart

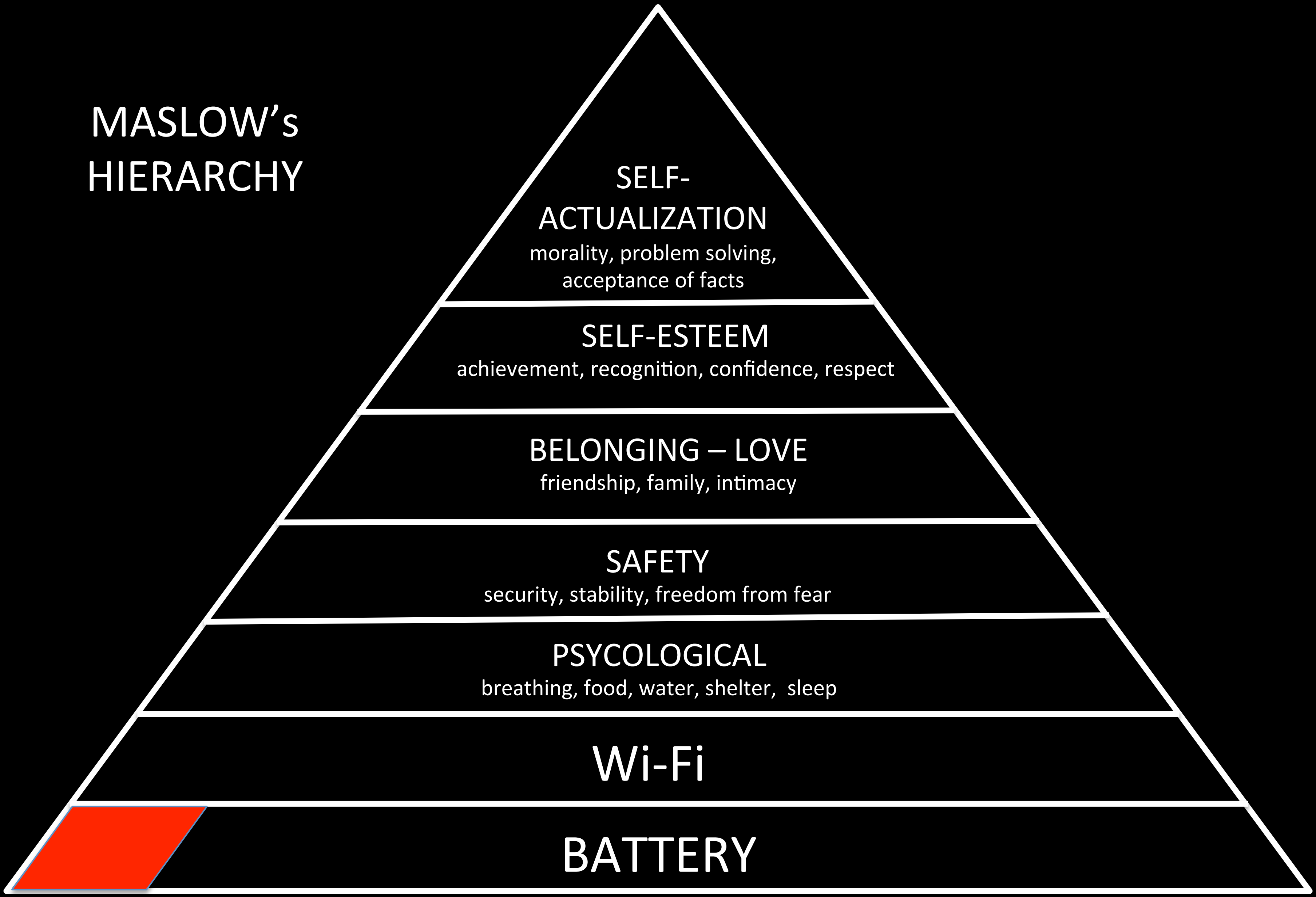
- Systems Engineer with Aerohive Networks
- Wanted to be a philosophy major
- Took Electrical Engineering instead
- Worked on networks with >60,000 APs

What are we going to cover?

- Quickly review RF fundamentals
- Design Tips/Guidelines
- Arbitration
- Troubleshooting
- Additional resources…always more to learn

Some one said “They first heard of Wi-Fi on Friday…. by Monday, everybody had it.”

MASLOW's HIERARCHY



SELF-ACTUALIZATION
morality, problem solving, acceptance of facts

SELF-ESTEEM
achievement, recognition, confidence, respect

BELONGING – LOVE
friendship, family, intimacy

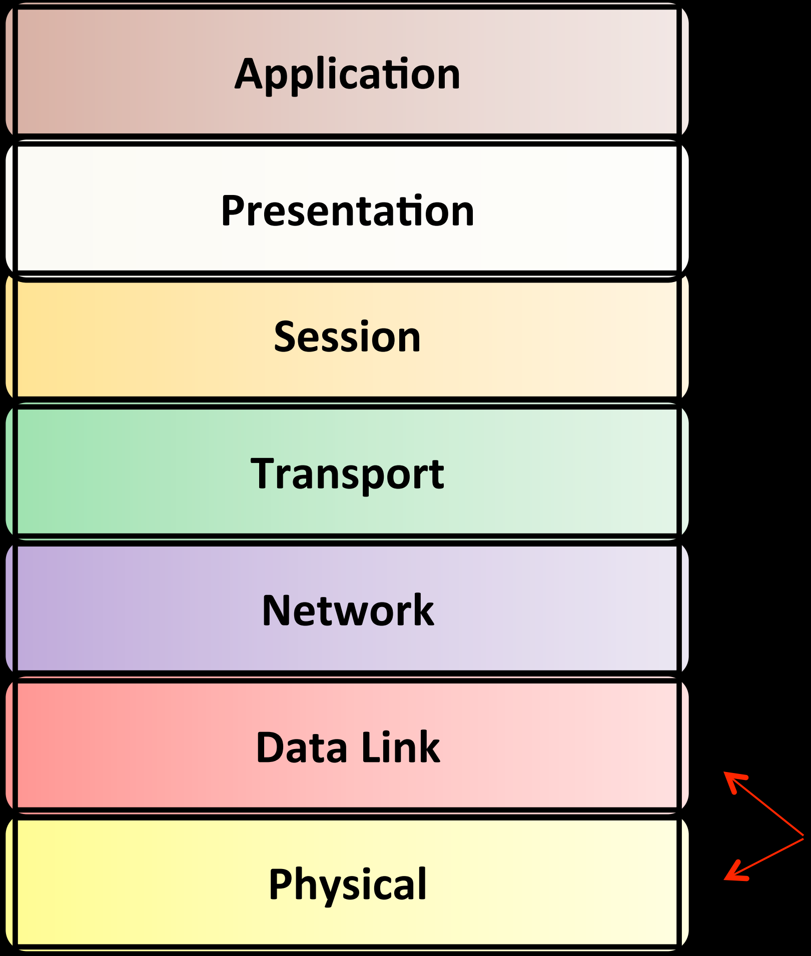
SAFETY
security, stability, freedom from fear

PSYCOLOGICAL
breathing, food, water, shelter, sleep

Wi-Fi

BATTERY

OSI Model



Application

Presentation

Session

Transport

Network

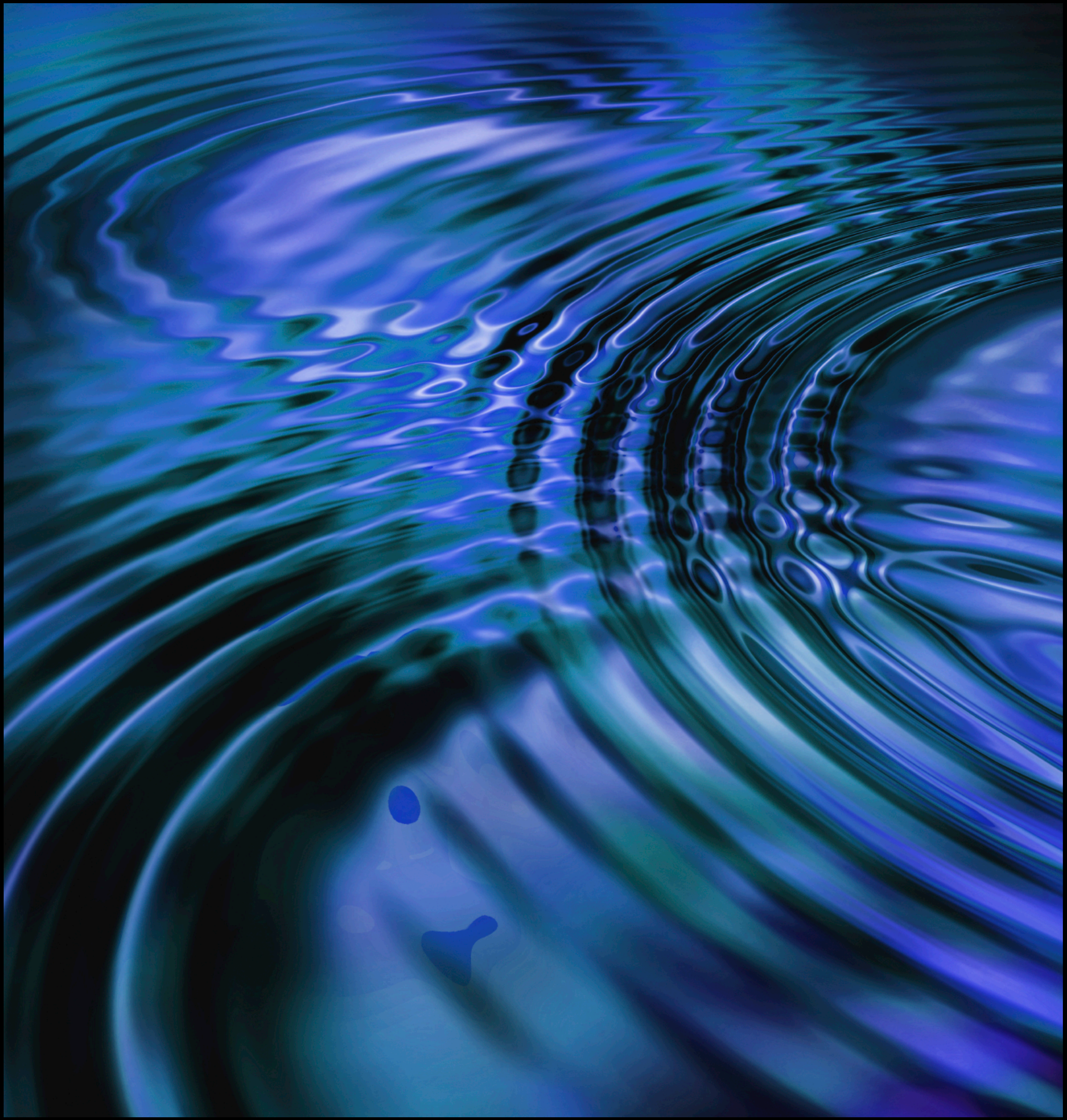
Data Link

Physical

Wi-Fi operates at layers one and two

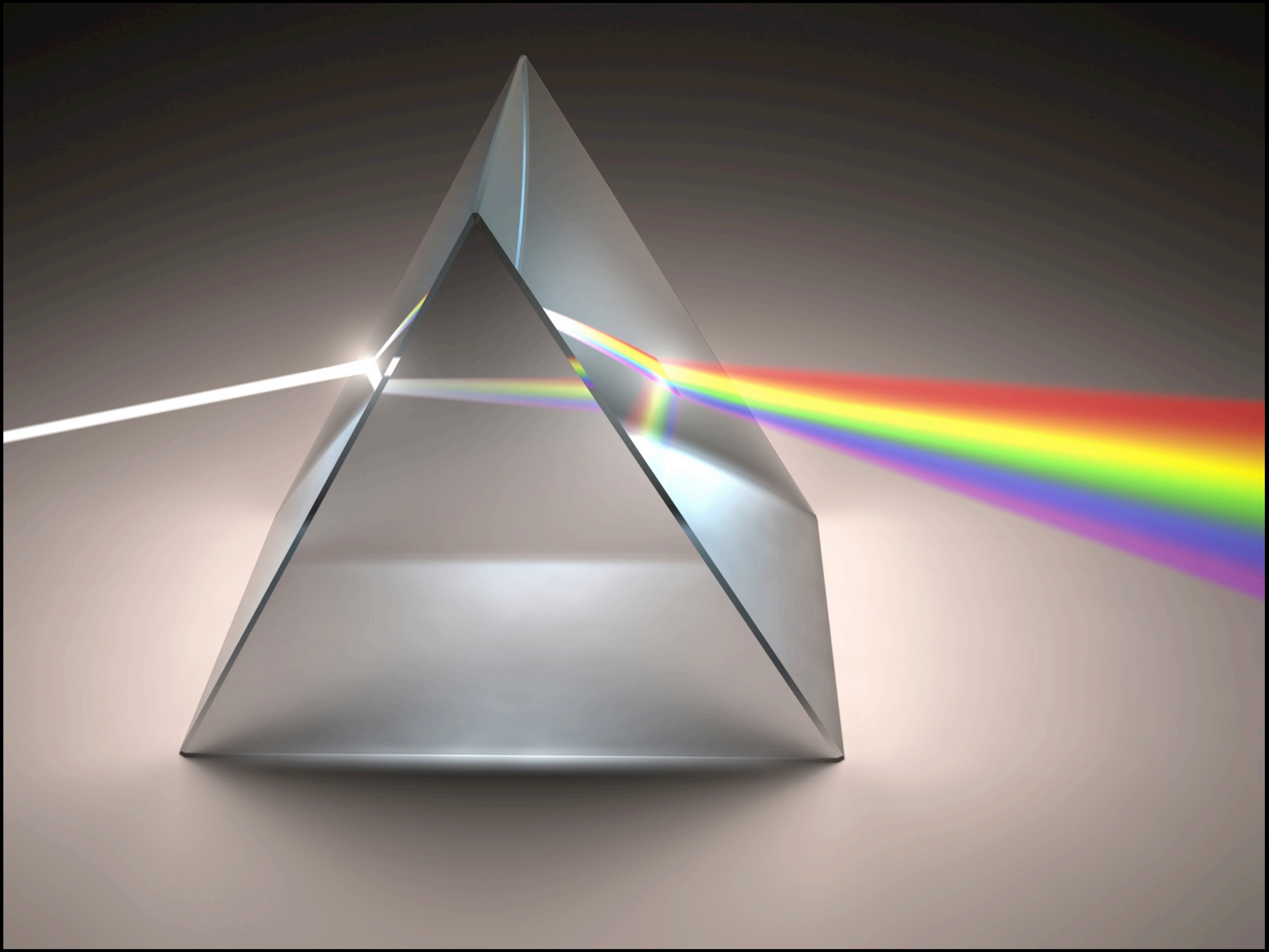
Wireless LAN's provide access to the distribution systems of wired networks. This allows the users the ability to have untethered connections to wired network resources.

One Transmitter



Three Transmitters

Many Transmitters (Reality)



Refraction

Reflection

Terminology (sound like a "Pro")

- Wi-Fi – sounds cool - means nothing, Wireless Fidelity is a myth

- SSID – ESS-ESS-EYE-DEE, not SID
- Access Point – AP, not WAP
- MIMO – My-Moe, not Mee-Moe (IEEE voted)
- WLAN – "W" or "Wireless" LAN
- Antenna(s) – insects have antennae, circuits have antennas
- 802.1X, not 802.1x

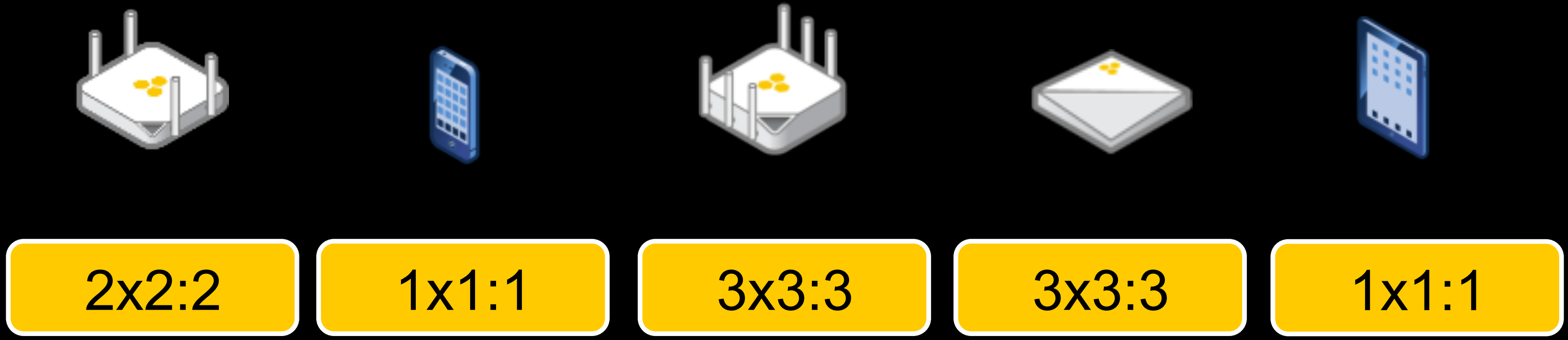
Amendments and Rates

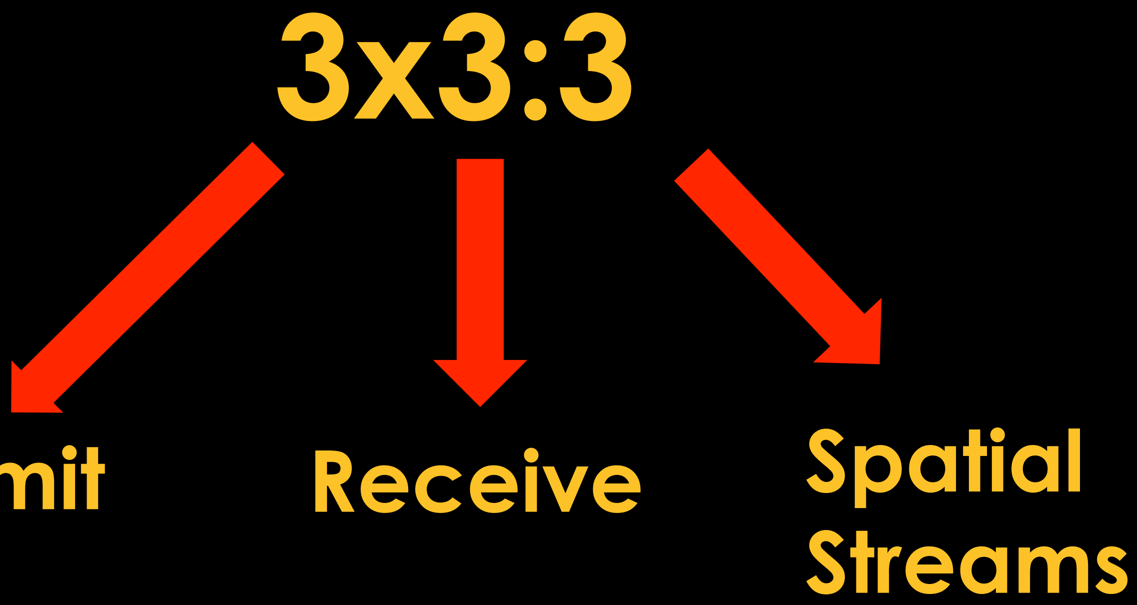
Standard	Supported Data Rates	2.4 GHz	5 GHz	RF Technology	Radios
802.11 legacy	1, 2 Mbps	Yes	No	FHSS or DSSS	SISO
802.11b	1, 2, 5.5 and 11 Mbps	Yes	No	HR-DSSS	SISO
802.11a	6 - 54 Mbps	No	Yes	OFDM	SISO
802.11g	6 - 54 Mbps	Yes	No	OFDM	SISO
802.11n	6 - 600 Mbps	Yes	Yes	HT	MIMO
802.11ac	Up to 6.933 Gbps*	No	Yes	VHT	MIMO

*First generation 802.11ac chipsets support up to 1.3 Gbps

DSSS	**Direct Sequencing Spread Spectrum**
FHSS	**Frequency Hopping Spread Spectrum**
OFDM	**Orthogonal Frequency Division Multiplexing**
HT	**High Throughput**
VHT	**Very High Throughput**
SISO	**Single Input, Single Output**
MIMO	**Multiple Input, Multiple Output**

802.11n, 802.11ac and MIMO radios




3x3:3

Transmit

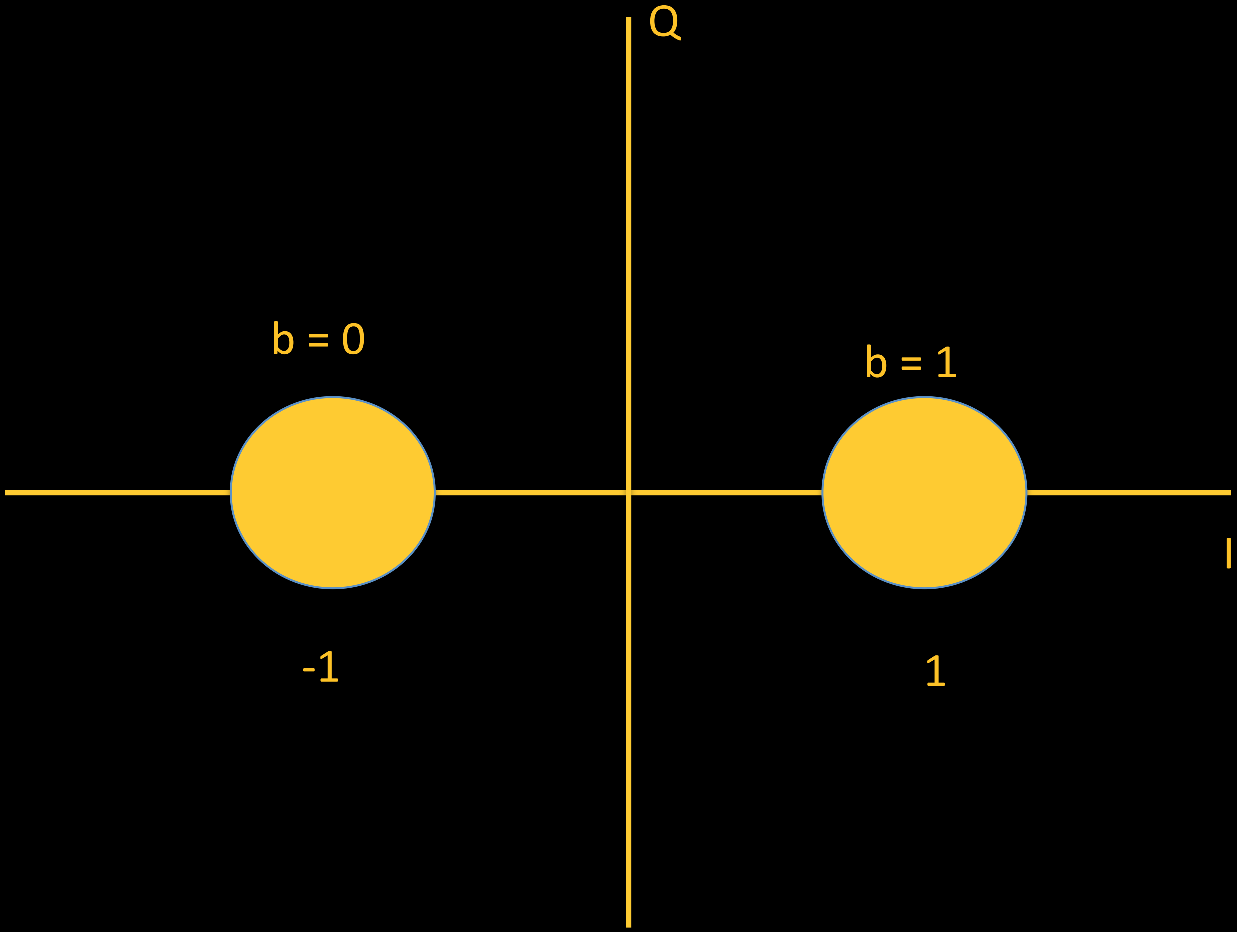
Receive

Spatial Streams

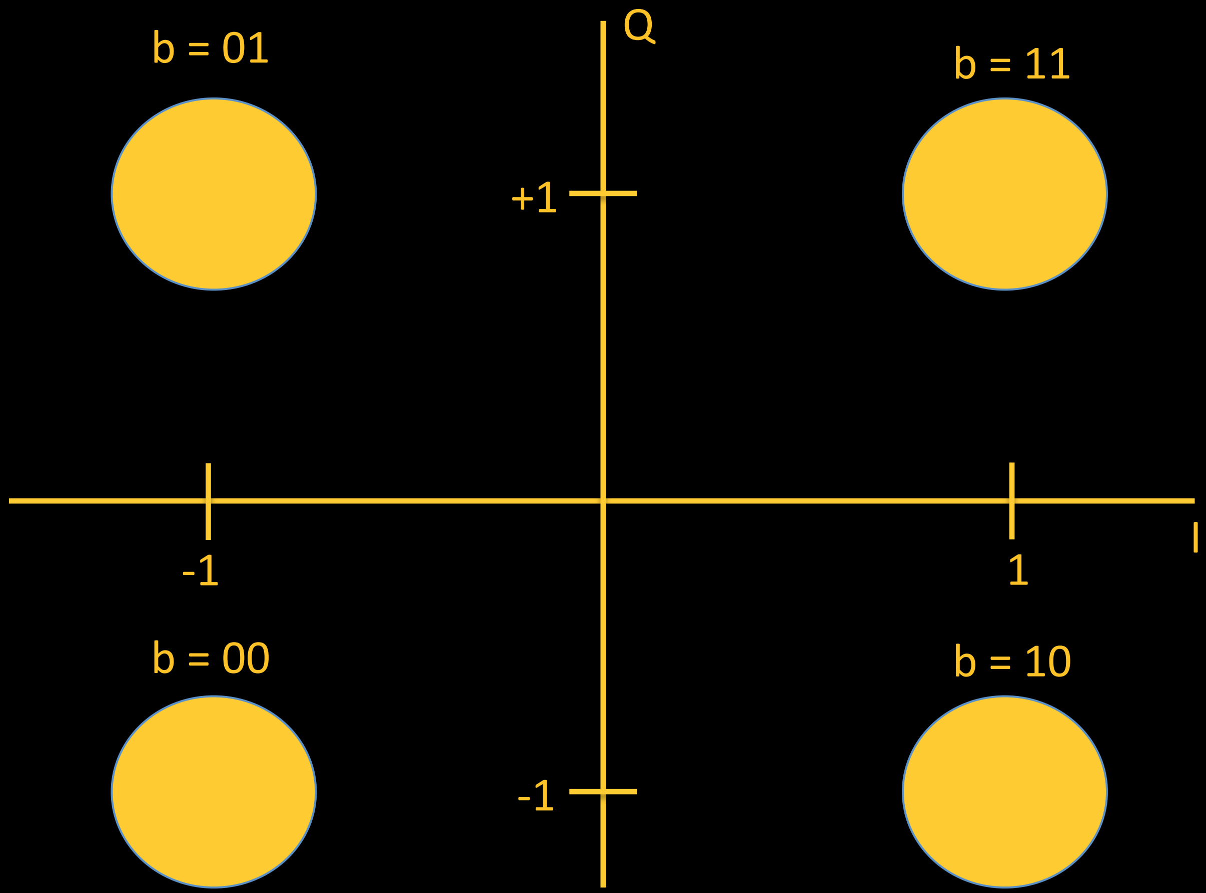
What’s new with 802.11ac

- 5 GHz ONLY
- MU-MIMO (multi-user)
- Up to 8 spatial streams
- 256 QAM
- Updated Modulation and Coding schemes
- 20/40/80/80+80/160 MHz wide channels
- Beamforming (only one type this time – explicit with Null Data Packet - NDP)

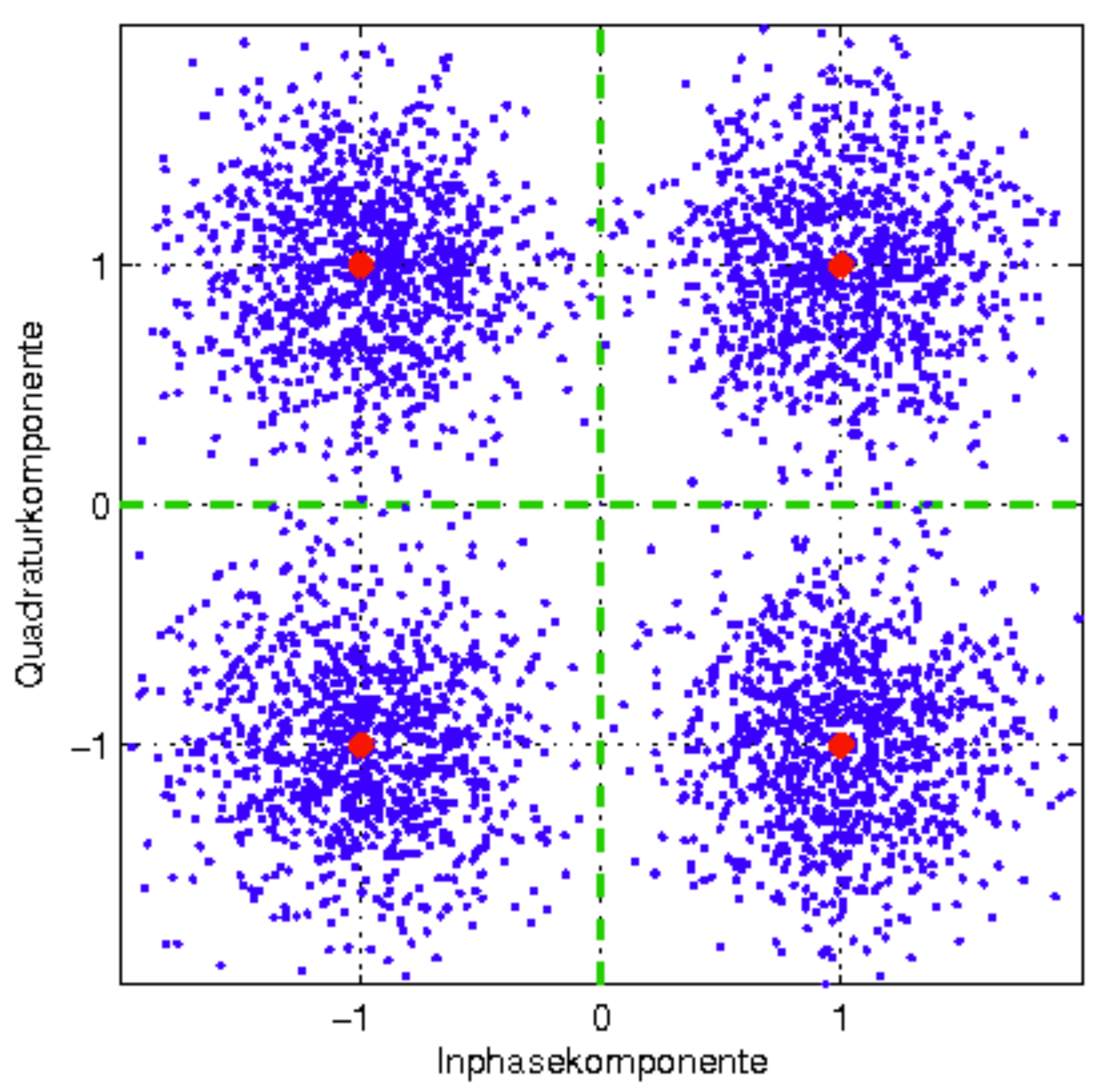
Binary Phase Shift Key - BPSK



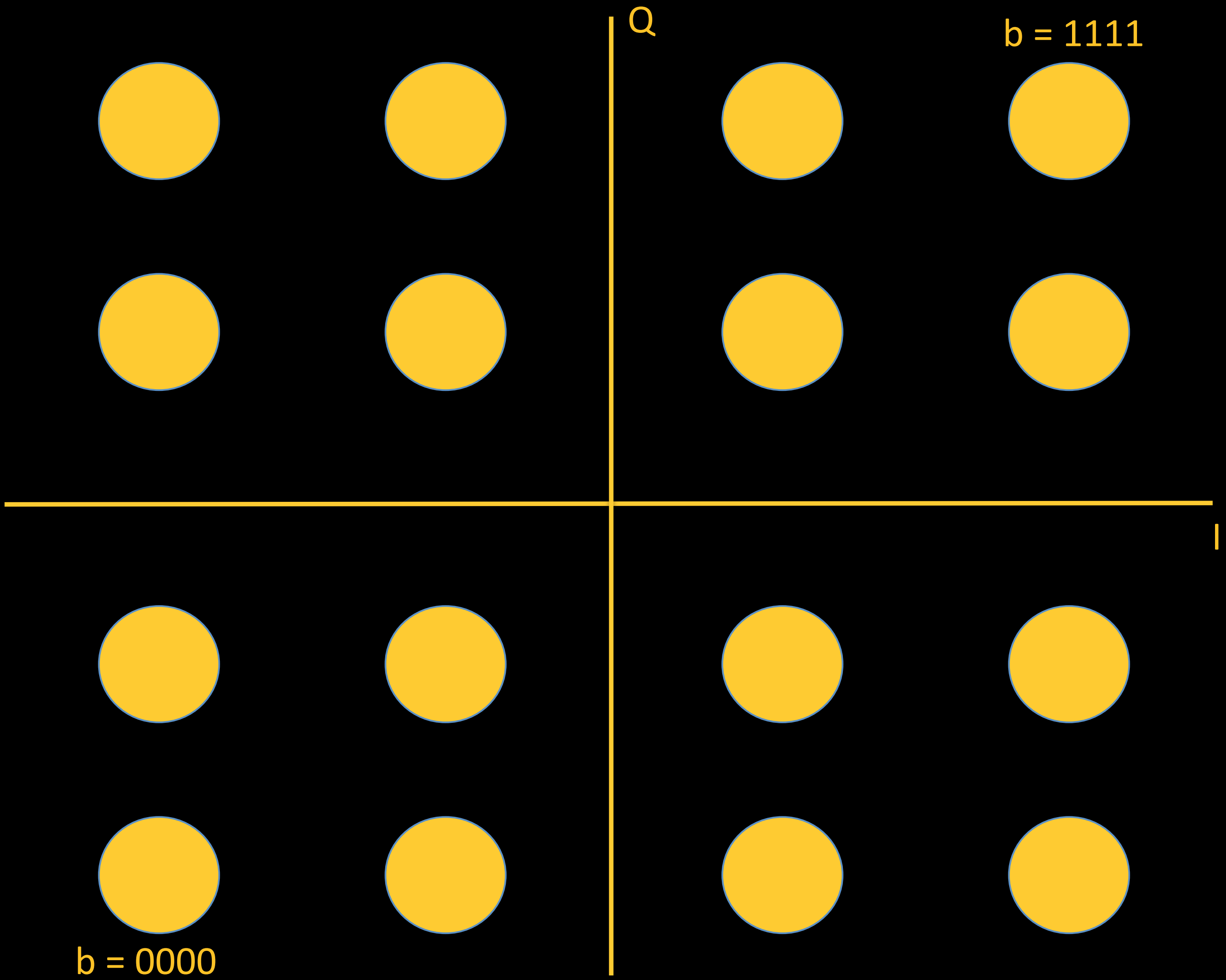
Quadrature Phase Shift Key - QPSK



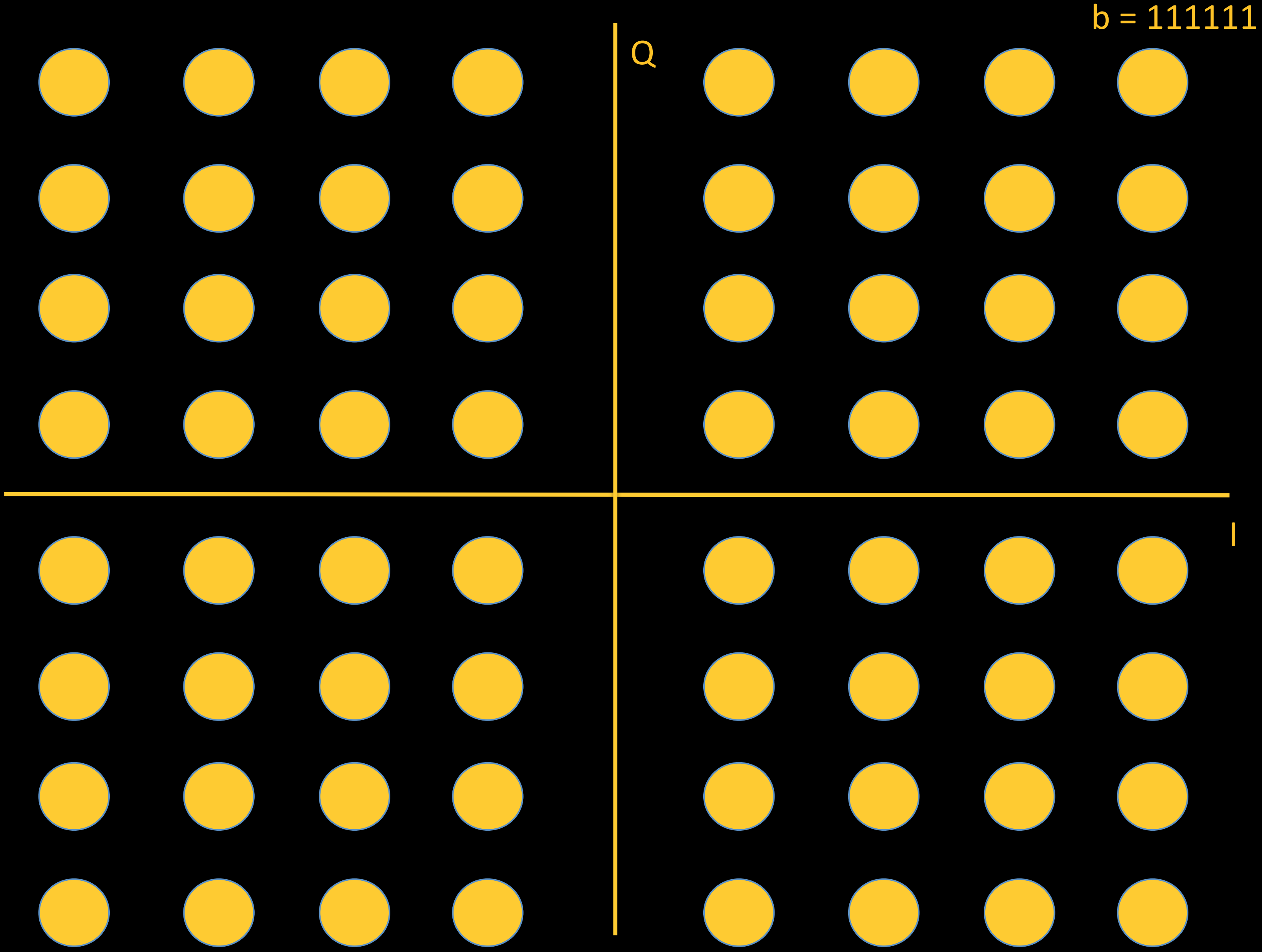
Quadrature Phase Shift Key - QPSK



QAM – 16-bit



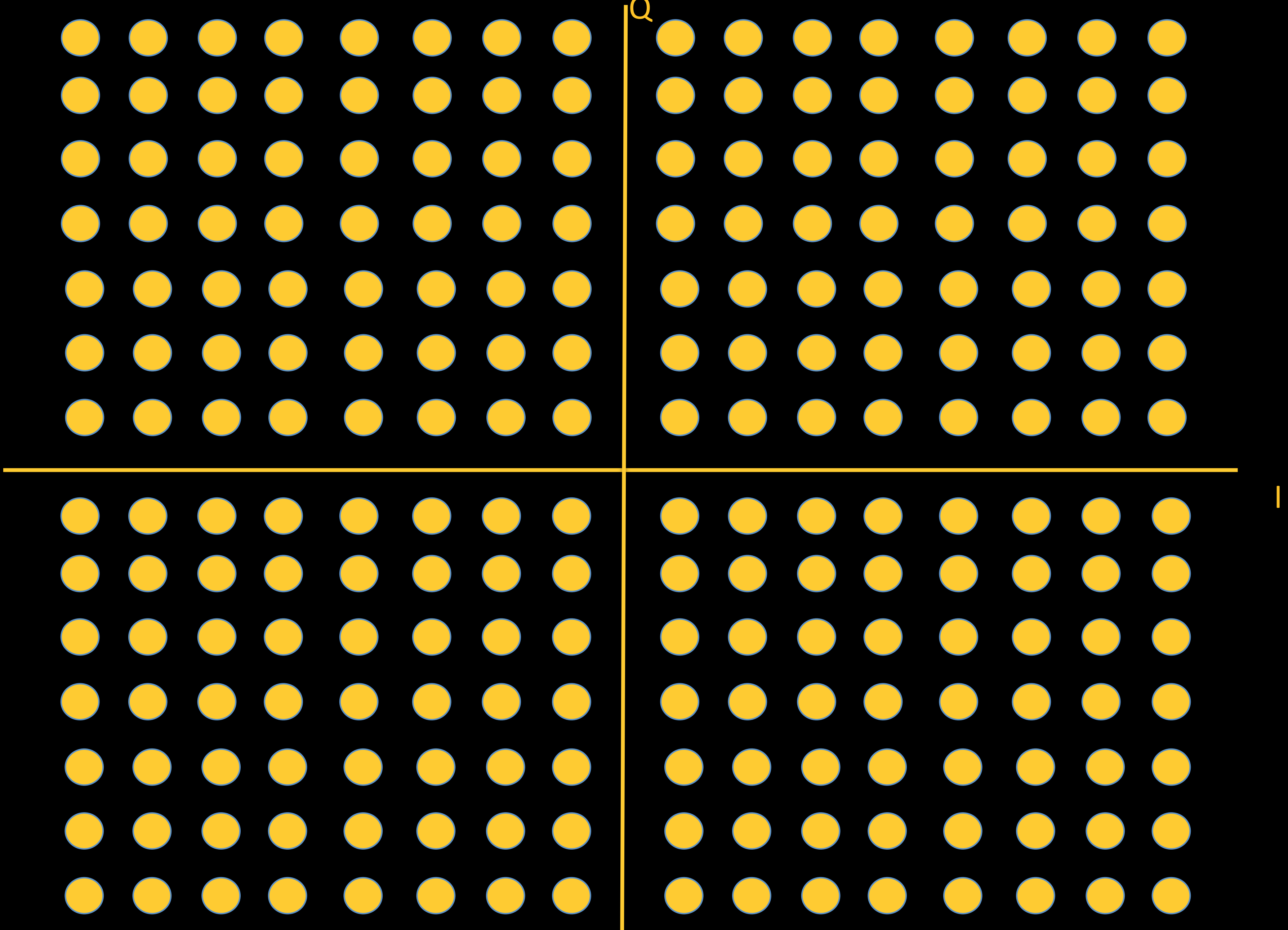
QAM – 64-bit



]

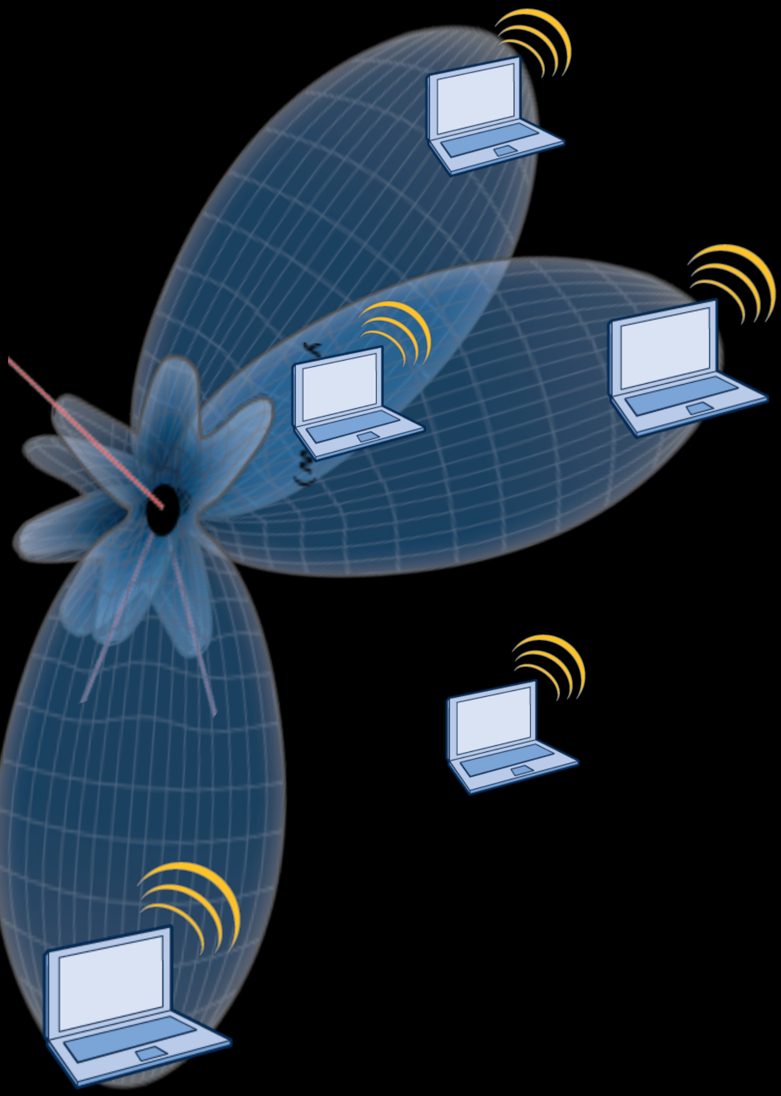
QAM – 256-bit

b = 11111111



MU-MIMO

- Maximizes available Spatial Streams on APs
- Downstream direction only
- “Aiming” sequence, then transmit data to multiple clients
- Each client must acknowledge its frame



dBm and mW conversions

dBm	**milliwatts**	
+60dBm	1,000,000 mW	1000 Watt (~Microwave Oven)
+30 dBm	1000 mW	1 Watt
+20 dBm	100 mW	1/10th of 1 Watt
+10 dBm	10 mW	1/100th of 1 Watt
0 dBm	1 mW	1/1,000th of 1 Watt
–10 dBm	.1 mW	1/10th of 1 milliwatt
–20 dBm	.01 mW	1/100th of 1 milliwatt
–30 dBm	.001 mW	1/1,000th of 1 milliwatt
–40 dBm	.0001 mW	1/10,000th of 1 milliwatt
–50 dBm	.00001 mW	1/100,000th of 1 milliwatt
–60 dBm	.000001 mW	1 millionth of 1 milliwatt
–70 dBm	.0000001 mW	1 ten-millionth of 1 milliwatt
–80 dBm	.00000001 mW	1 hundred-millionth of 1 milliwatt
–90 dBm	.000000001 mW	1 billionth of 1 milliwatt
–95 dBm	.0000000002511 mW	Noise Floor

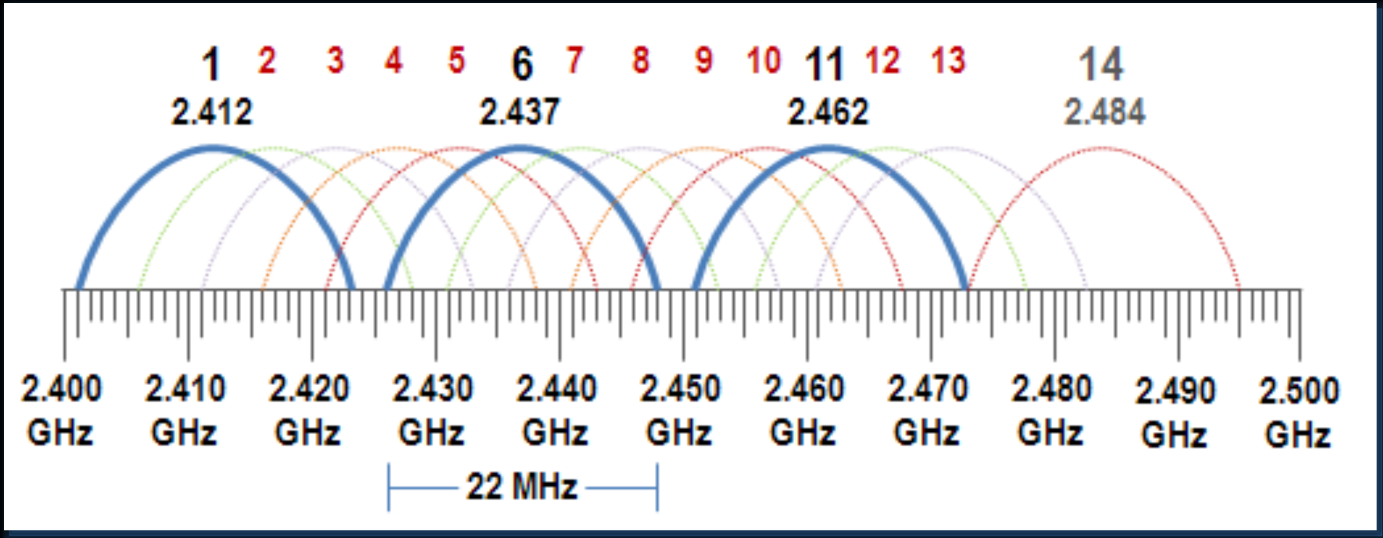
Decibel (dB) Math

Simple and fast way to get close to RF signal strength values
For every 10 dB of gain you multiply signal strength by 10.
If calculating loss, for every 10 dB of loss you divide signal strength by 10.

For every 3 dB of gain multiply the signal strength by 2.
If calculating loss, for every 3 dB of loss divide the signal strength by 2.

"If management doesn't think 3 dB is a lot, I'd like a 3 dB raise."
- crafty RF Engineer

2.4 GHz Channels
Used for 802.11b/g/n

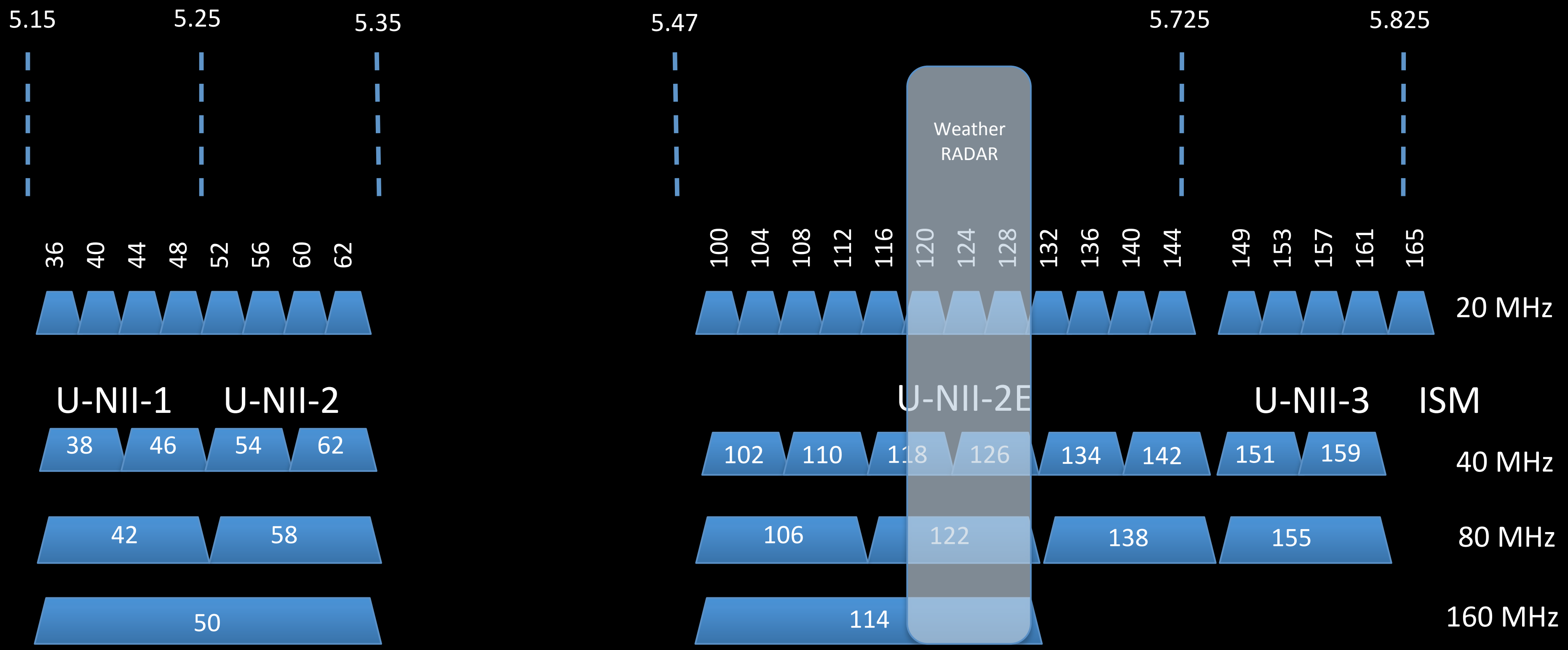


Channels 1, 6, and 11 are the only non-overlapping channels between 1 and 11 with most channel re-use

Using channels that cause overlap may cause CRC and other wireless interference and errors

If you are in a country that has channels 1 – 13 or 14 available, you may still want to use 1, 6, and 11 for compatibility with mobile users from other countries

5 GHz Channels
- Used for 802.11 a/n/ac



802.11n defines the use of 40 MHz wide channels.
802.11ac defines dynamic channel sizes up to 160 MHz wide.

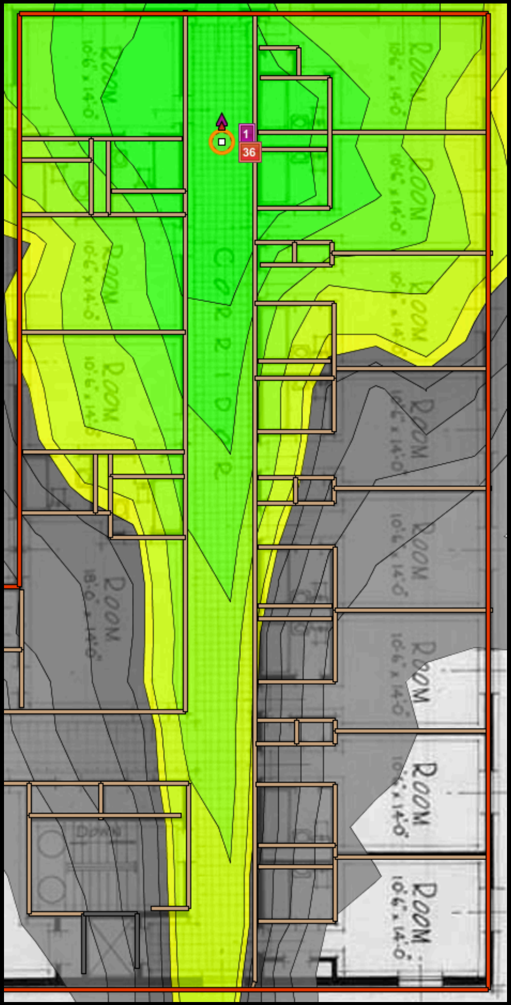
Design

Gathering the Design Requirements

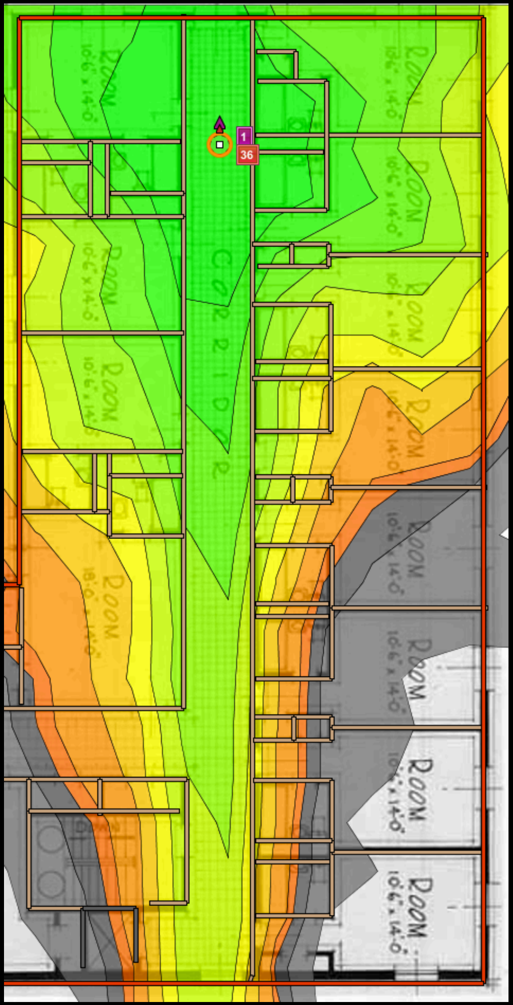
- **Information Gathering (The "Interview")**
  - Types of Environments
  - Client device types to be used
  - Applications to be used
  - Expected Growth vs. Current Needs
- **Access Points to be used**
  - Mounting Concerns
  - Coverage vs. Capacity Planning
  - Device Density
  - Security Enterprise and Guest use

Knowing the Device Types and Applications to be used will greatly assist you in planning and deploying successful networking solutions.

AP heat map

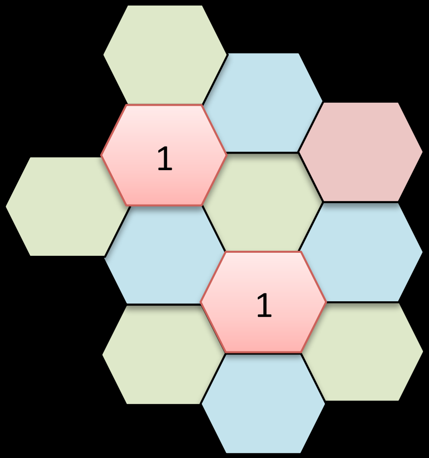


-67 dBm cutoff

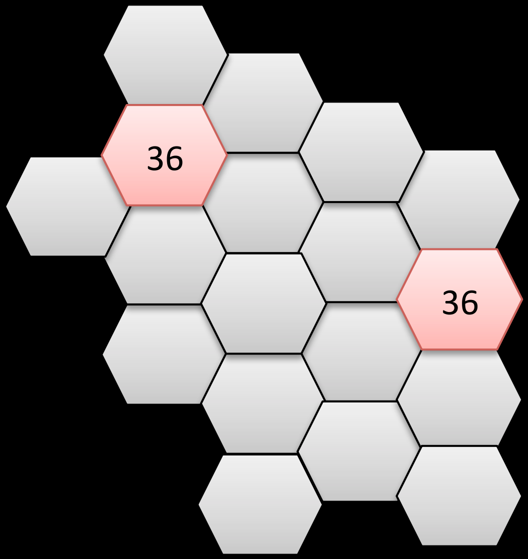


-82dBm cutoff

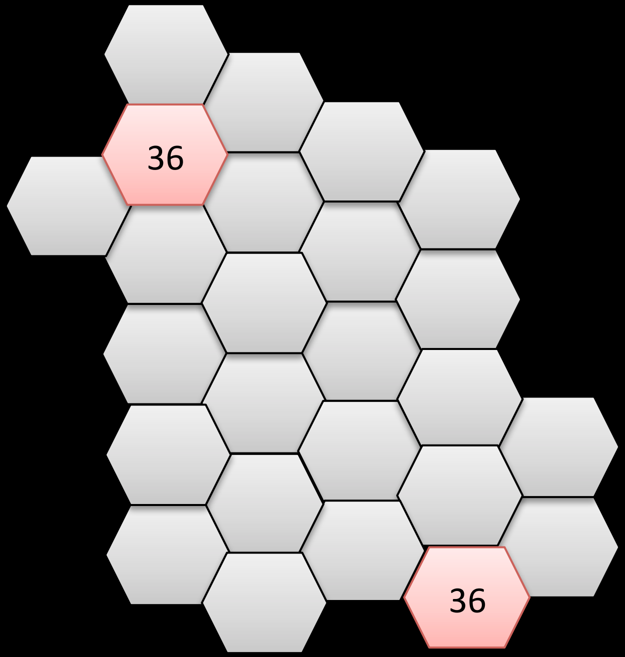
Channel Re-use



3 ch (2.4GHz)

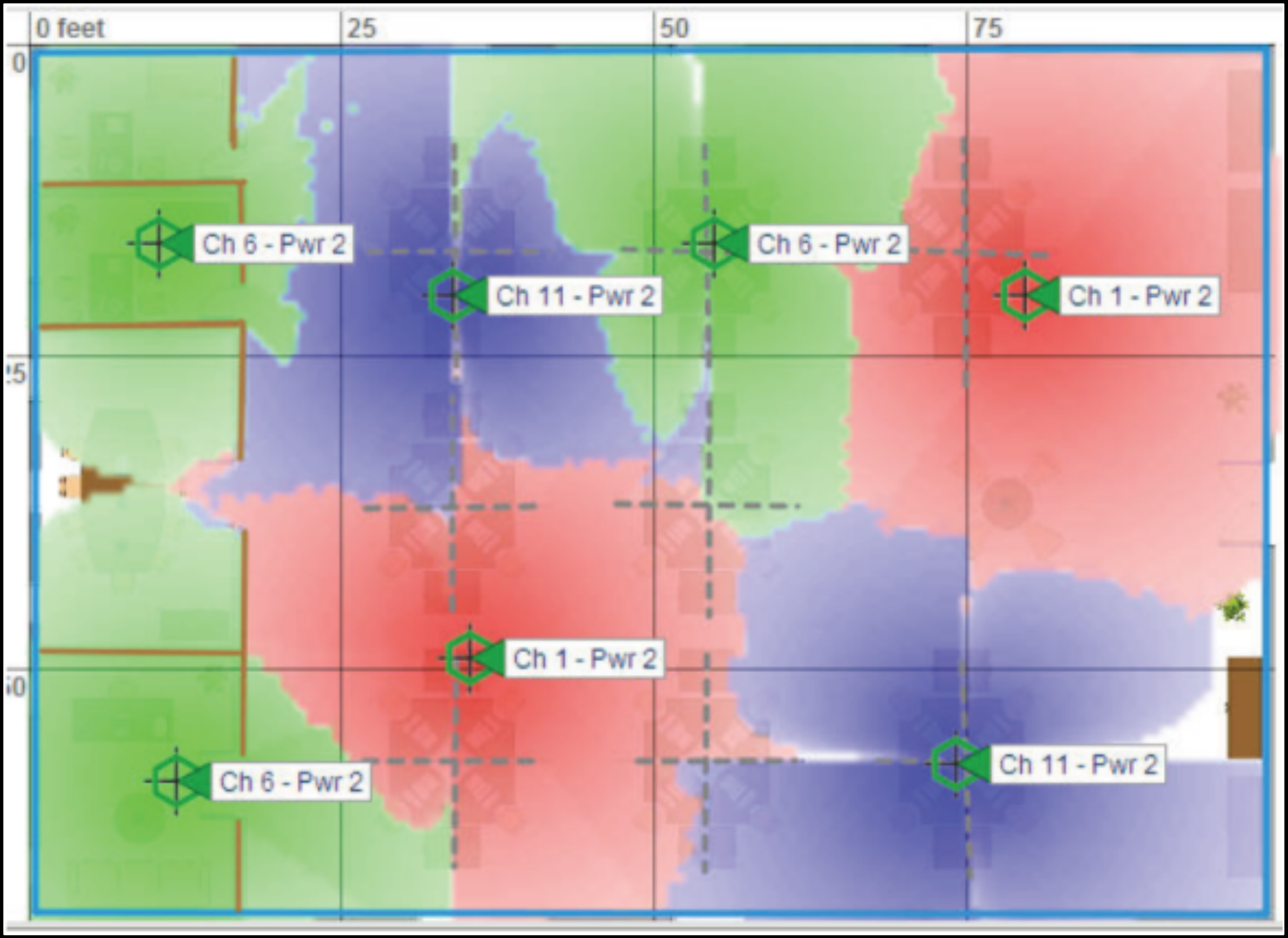


8 ch (5GHz, non-DFS)



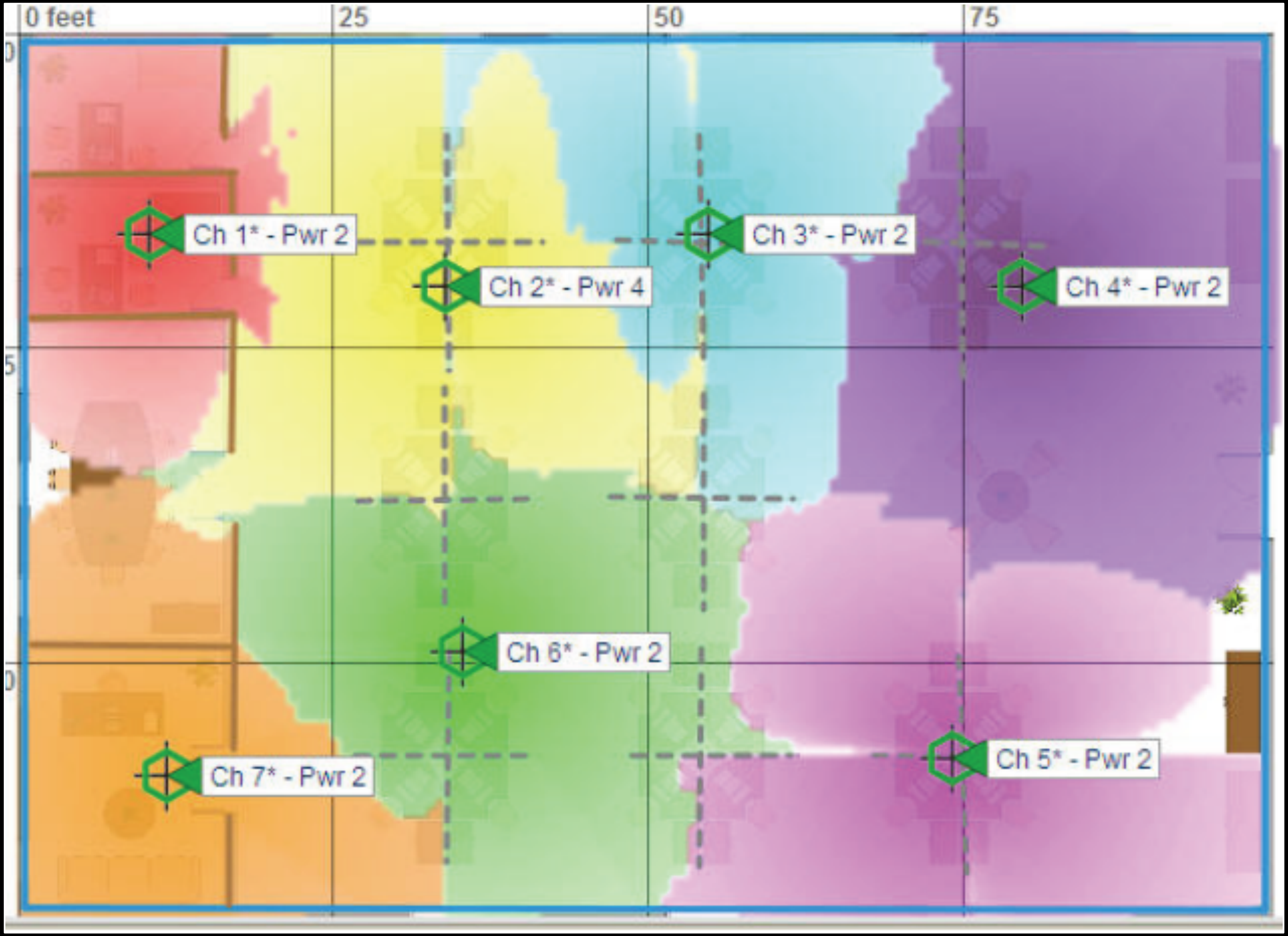
20 ch (5GHz, with DFS)

Channel Reuse Pattern



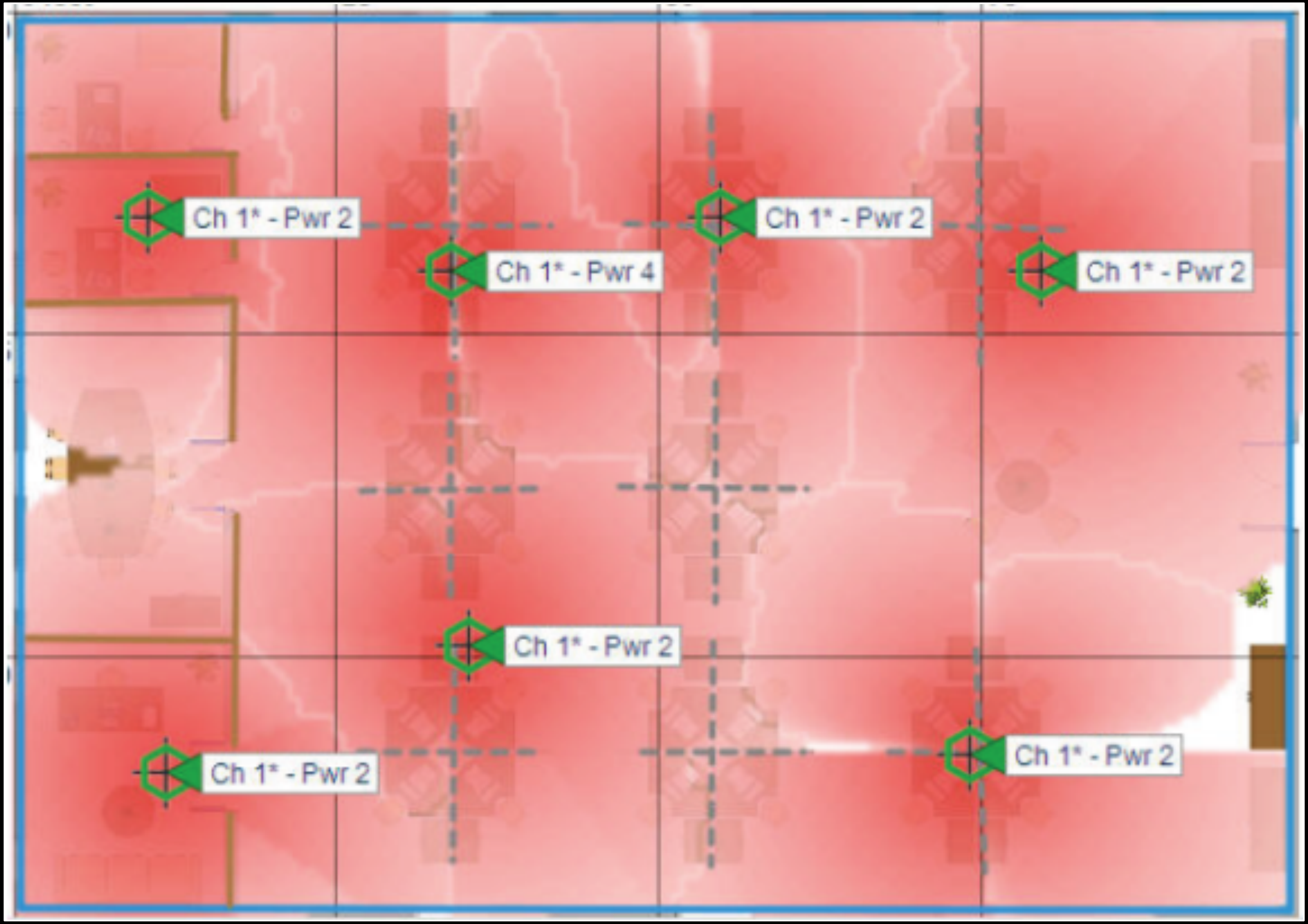
In this plan only the non-overlapping channels of 1, 6 and 11 are used.

Adjacent Interference/Cooperation



Improper designs use overlapping channels in the same physical area.

Co-Channel Interference/Cooperation



Improper design using the same channel on all AP's in the same physical area.

Wi-Fi is just wireless Ethernet?

Carrier Sense Multiple Access – Collision Detection

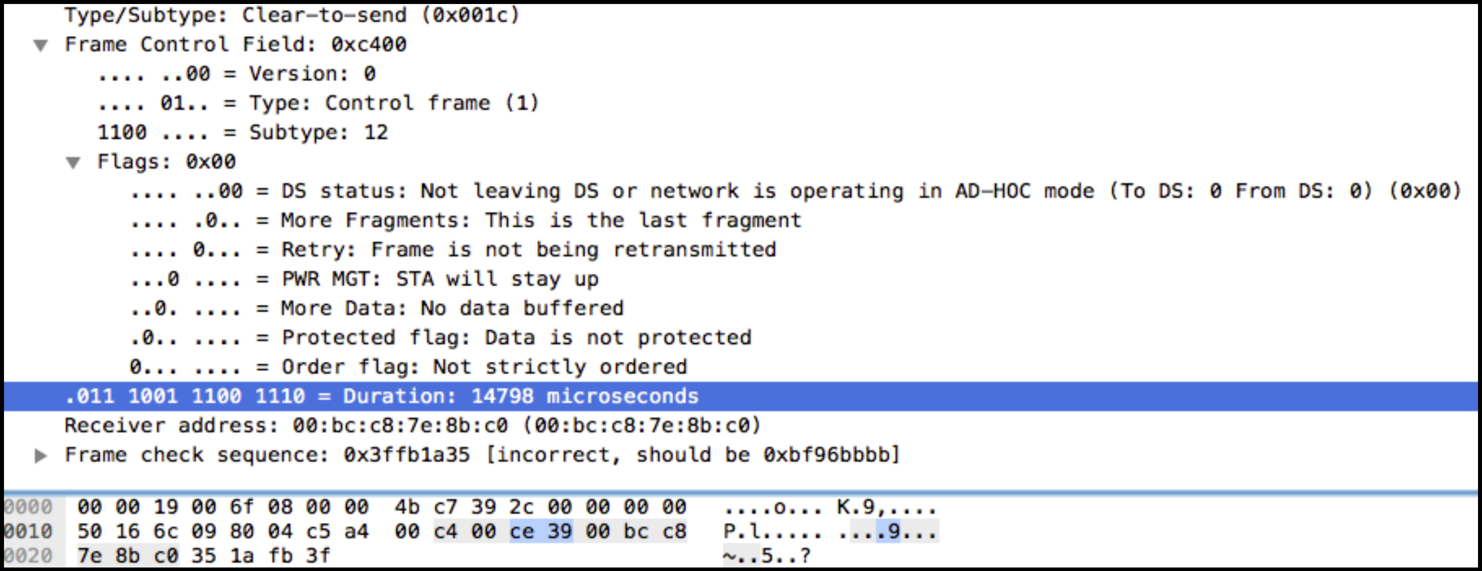
- Collision handling happens after a collision occurs

Carrier Sense Multiple Access – Collision Avoidance

- Collision handling happens before any data is transmitted

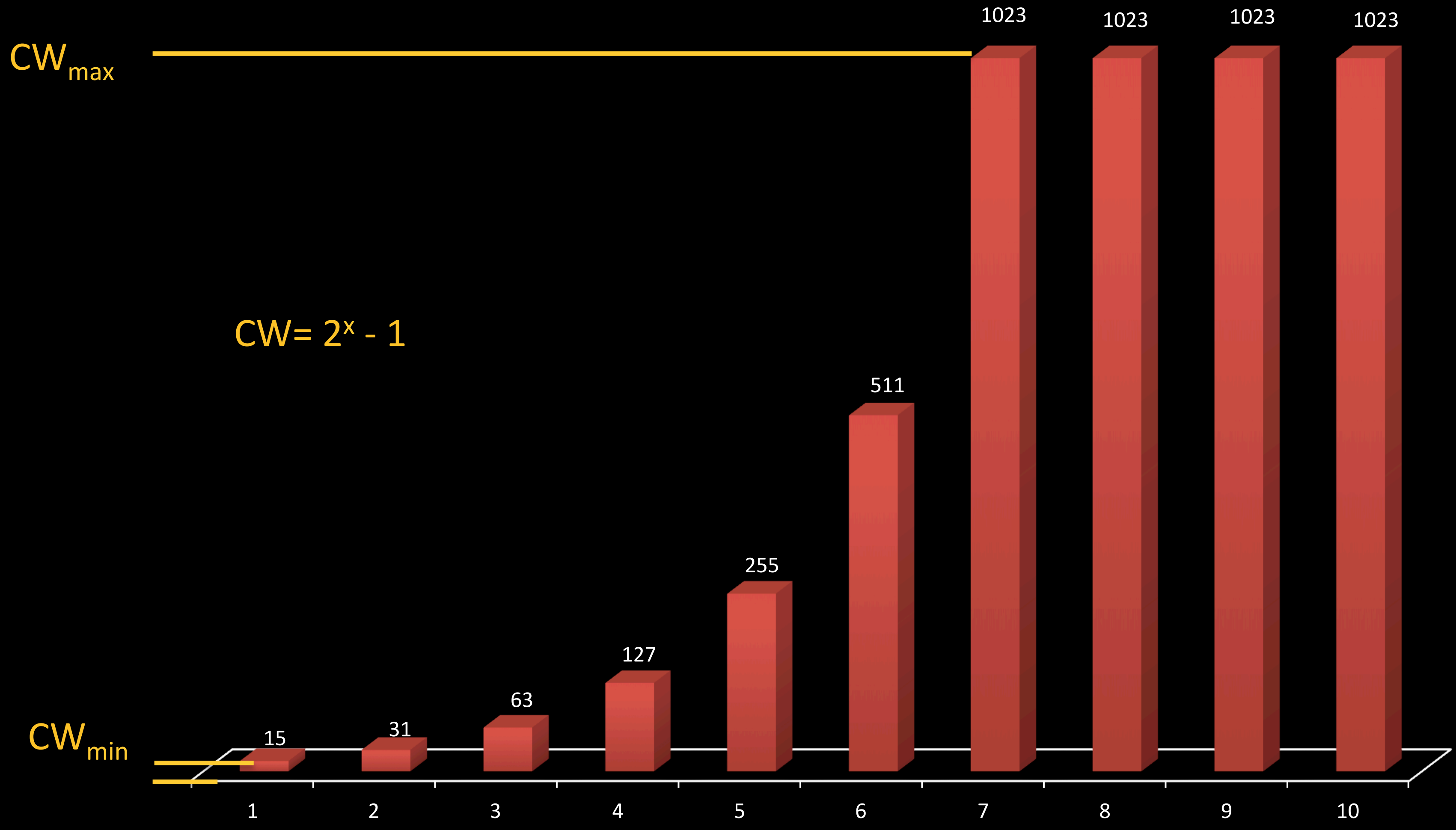
Arbitration

- Physical carrier sense
  - Clear Channel Assessment – CCA
- Virtual carrier sense
  - Network Allocation Vector – NAV
  - Value carried in the 802.11 header



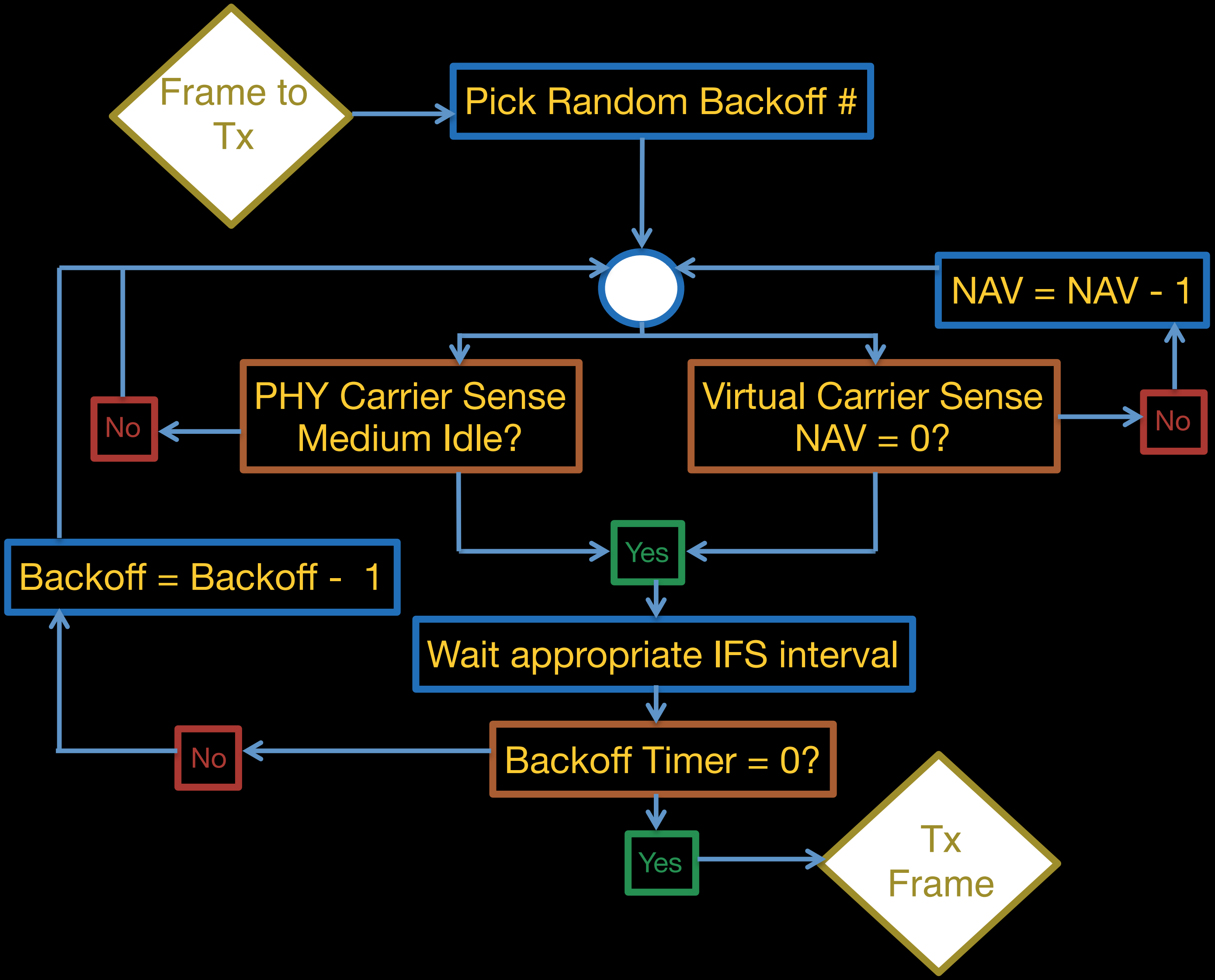
```
    Type/Subtype: Clear-to-send (0x001c)
▼   Frame Control Field: 0xc400
        .... ..00 = Version: 0
        .... 01.. = Type: Control frame (1)
        1100 .... = Subtype: 12
    ▼   Flags: 0x00
            .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = Protected flag: Data is not protected
            0... .... = Order flag: Not strictly ordered
    .011 1001 1100 1110 = Duration: 14798 microseconds
    Receiver address: 00:bc:c8:7e:8b:c0 (00:bc:c8:7e:8b:c0)
▶   Frame check sequence: 0x3ffb1a35 [incorrect, should be 0xbf96bbbb]

0000  00 00 19 00 6f 08 00 00  4b c7 39 2c 00 00 00 00   ....o... K.9,....
0010  50 16 6c 09 80 04 c5 a4  00 c4 00 ce 39 00 bc c8   P.l..... ....9...
0020  7e 8b c0 35 1a fb 3f                               ~..5..?
```

Contention Window



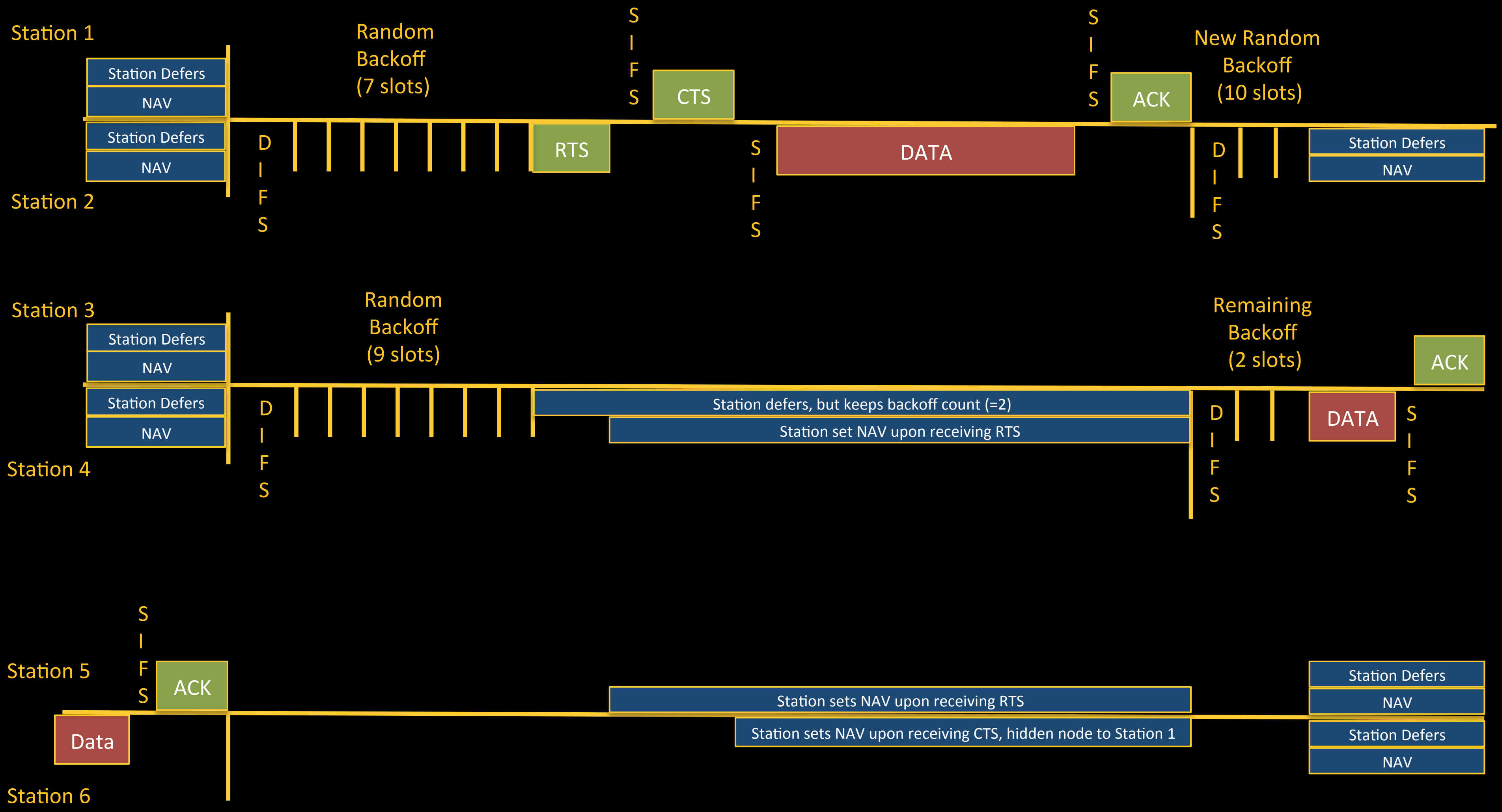
CW= 2^x - 1

Wi-Fi Arbitration



Birthday Paradox

Multiple Stations



Station 1

Station Defers

NAV

Random Backoff (7 slots)

S I F S

CTS

S I F S

ACK

New Random Backoff (10 slots)

Station Defers

NAV

D I F S

RTS

S I F S

DATA

D I F S

Station Defers

NAV

Station 2

Station 3

Station Defers

NAV

Random Backoff (9 slots)

Remaining Backoff (2 slots)

ACK

Station Defers

NAV

D I F S

Station defers, but keeps backoff count (=2)

Station set NAV upon receiving RTS

D I F S

DATA

S I F S

Station 4

S I F S

Station 5

ACK

Station sets NAV upon receiving RTS

Station Defers

NAV

Data

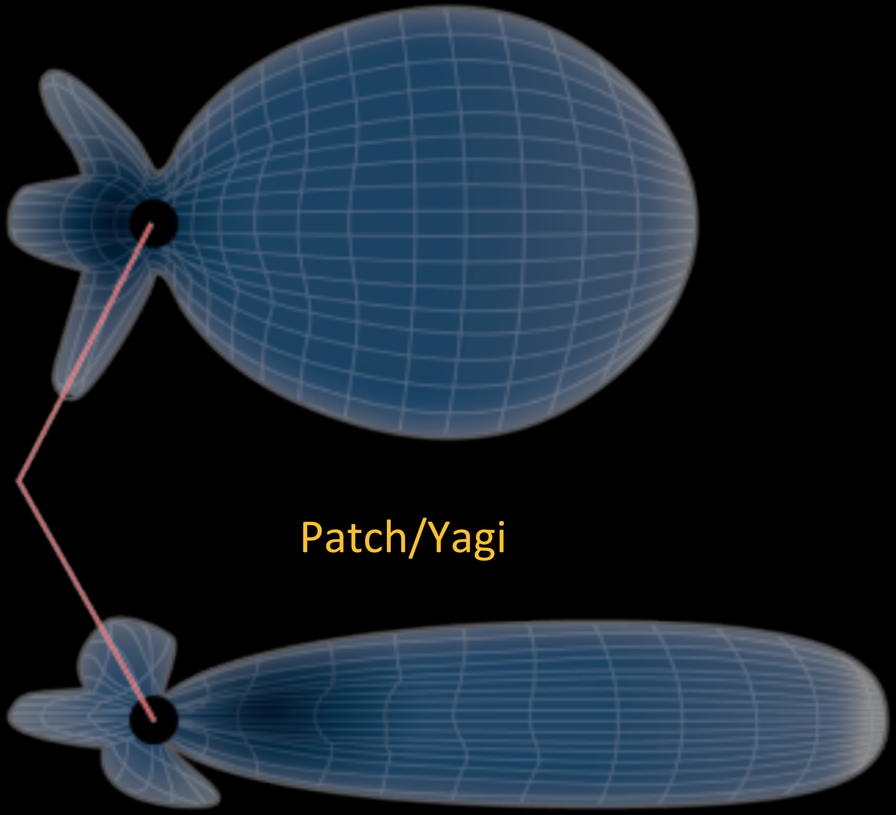
Station sets NAV upon receiving CTS, hidden node to Station 1

Station Defers

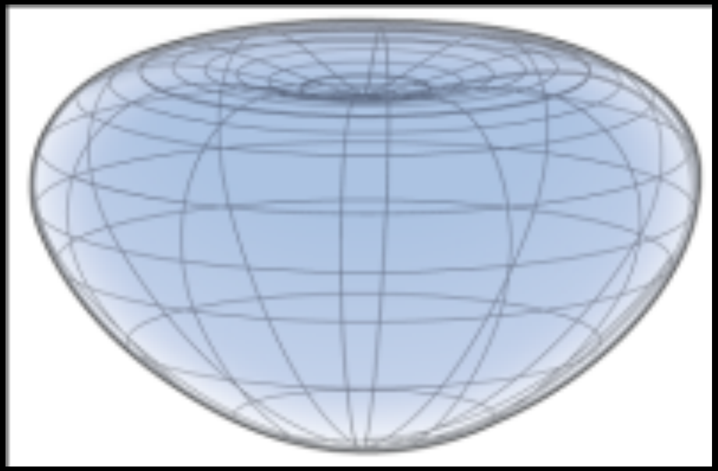
NAV

Station 6

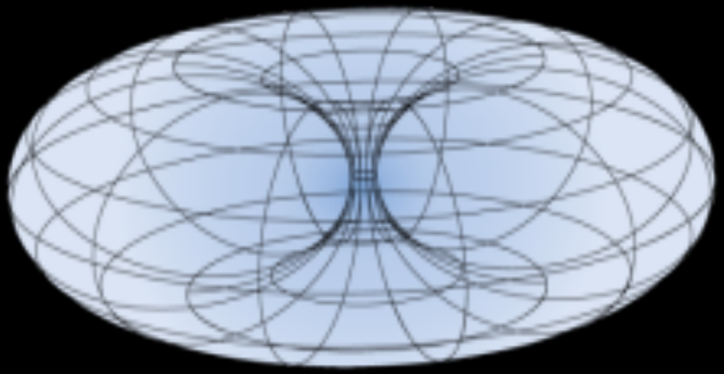
Antenna Patterns



Patch/Yagi



Internal

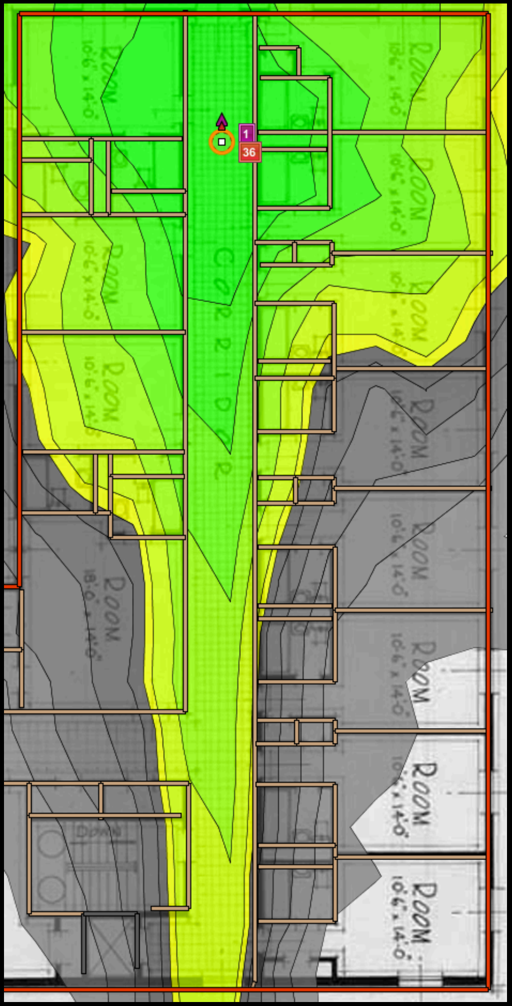


Rubber-Duck

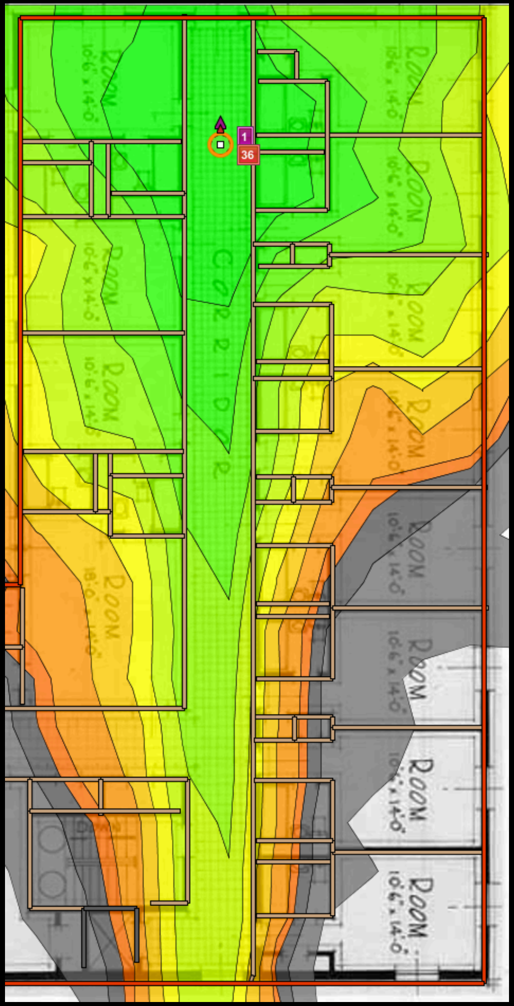
Troubleshooting

Clients are responsible for when to roam and which AP to roam.

AP heat map



-67 dBm cutoff



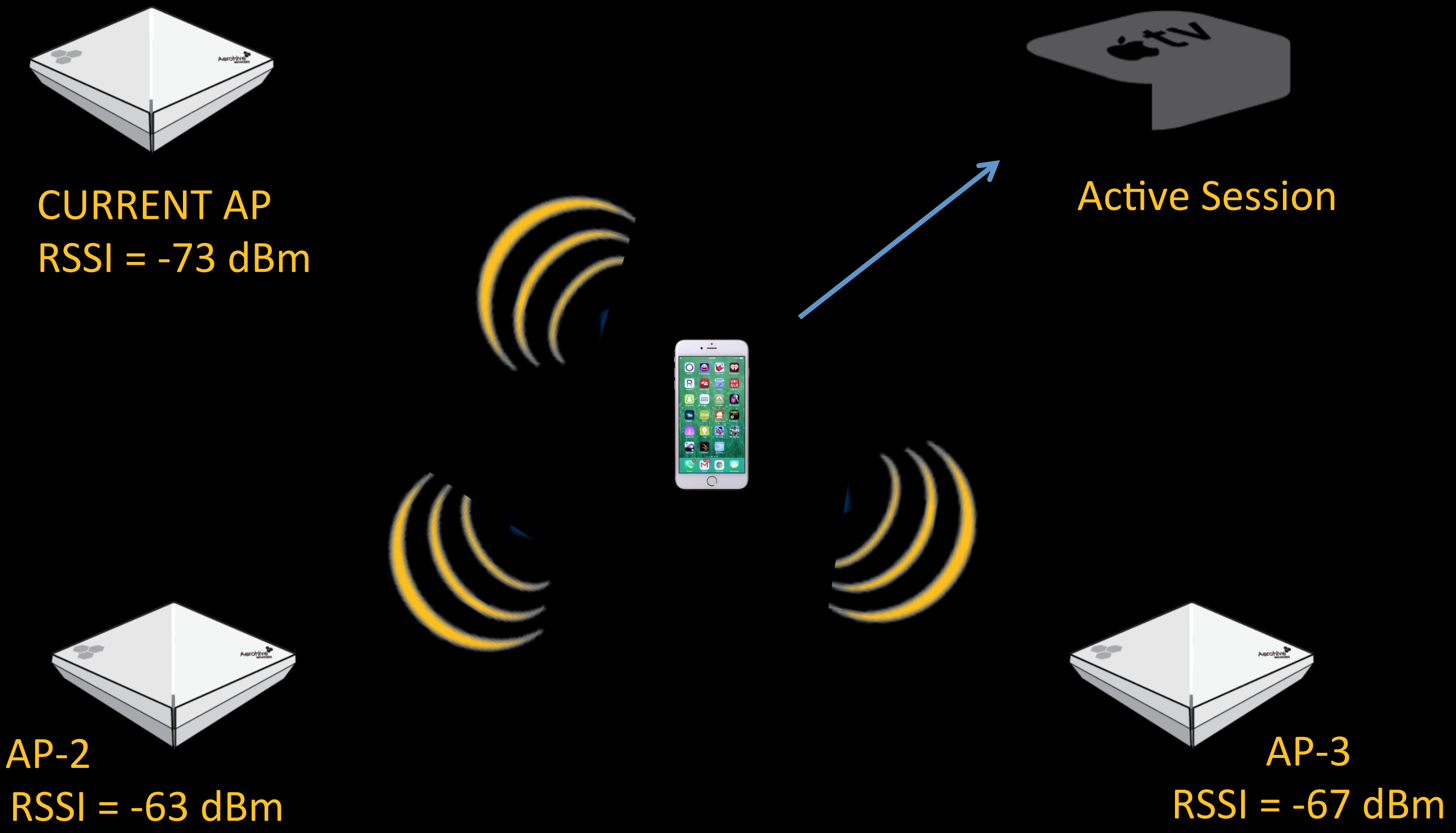
-82 dBm cutoff

iOS Client Roaming

- Trigger roam at -70dBm
- During active session – next hop AP must have RSSI 8dB+ than current RSSI
- During unactive session – next hop AP must have RSSI 12dB+ than current RSSI

https://support.apple.com/en-us/HT203068

iOS Client



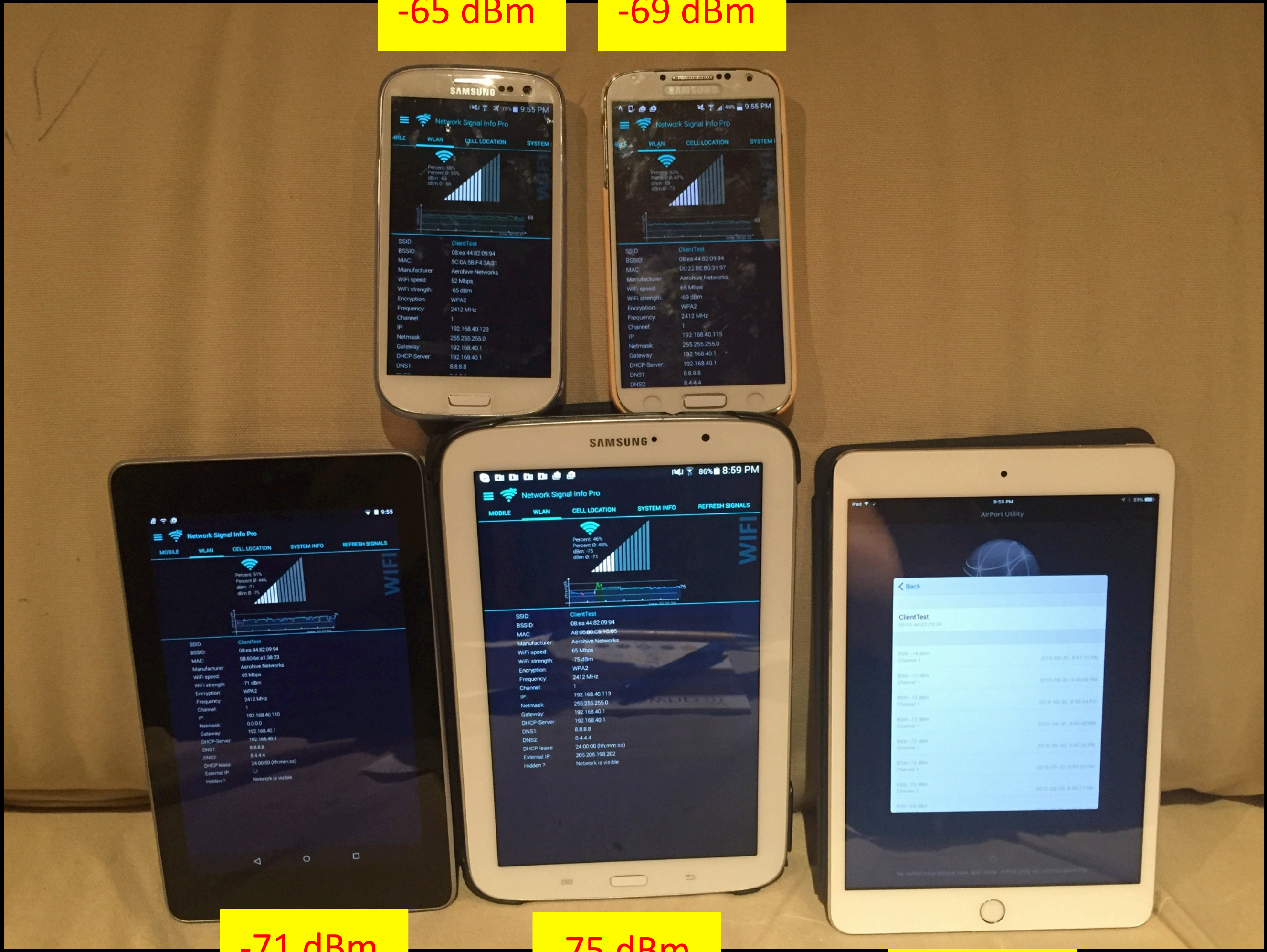
CURRENT AP
RSSI = -73 dBm

Active Session

AP-2
RSSI = -63 dBm

AP-3
RSSI = -67 dBm

RSSI from different clients



-65 dBm

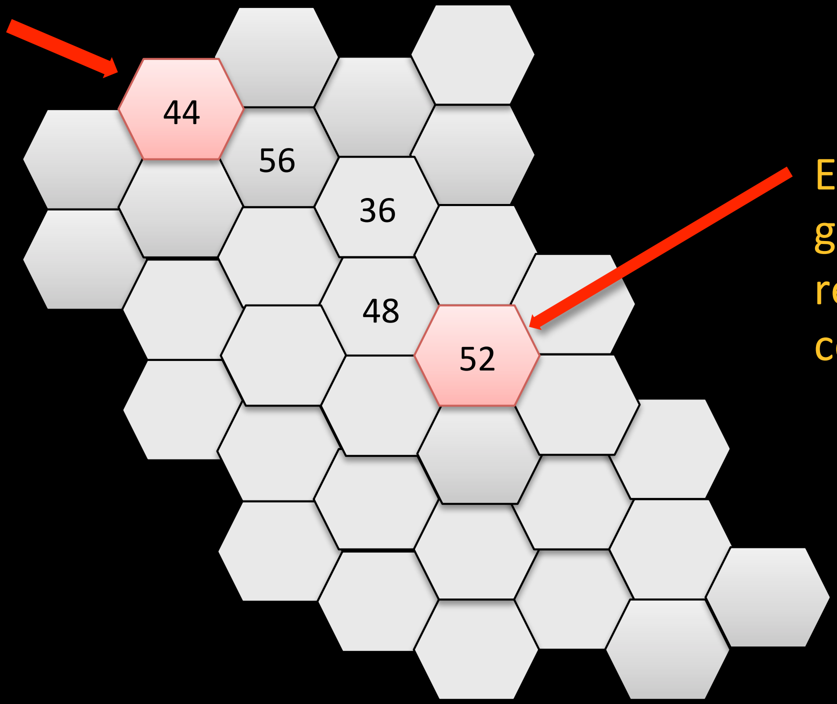
-69 dBm

-71 dBm

-75 dBm

-73 dBm

Sticky Client

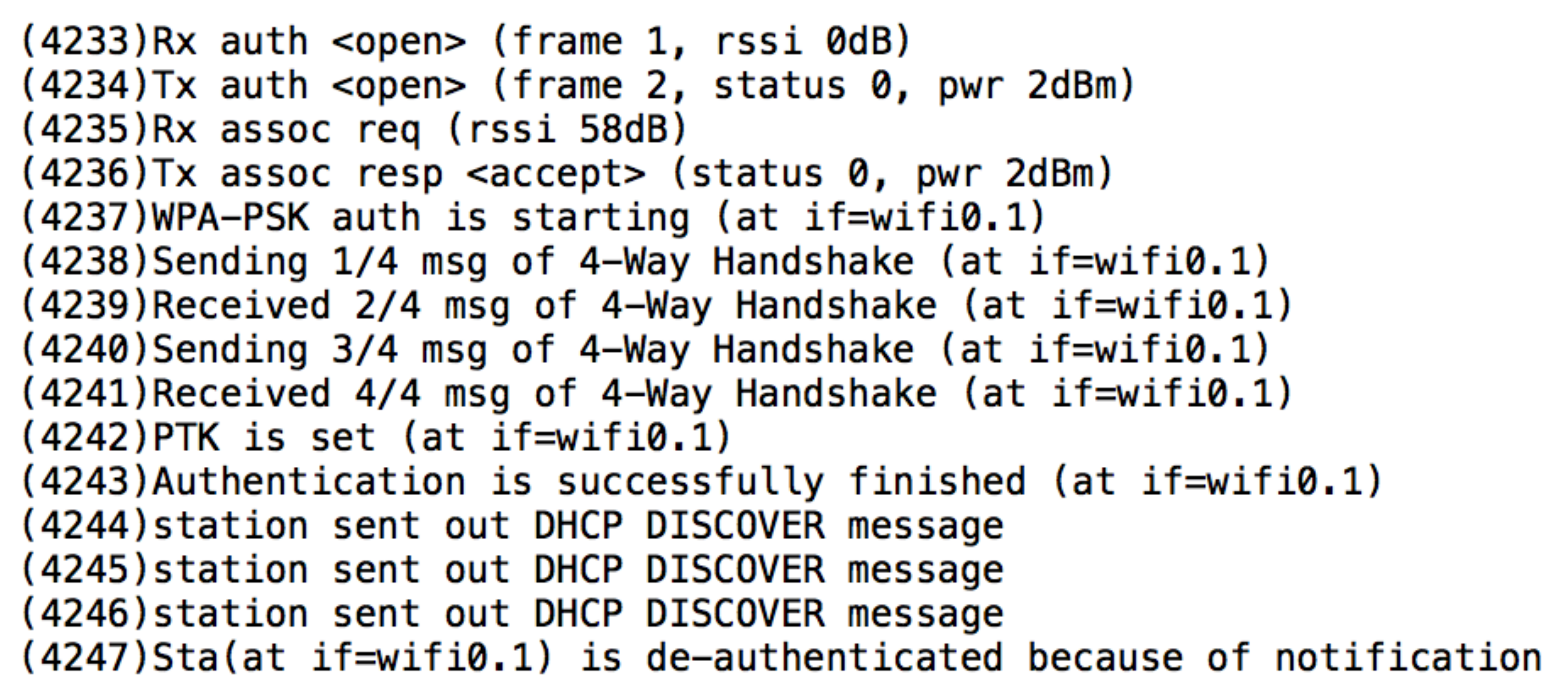


Building entrance – 1st association

Even though cell 53 has greater RSSI, client remains connected to cell 44

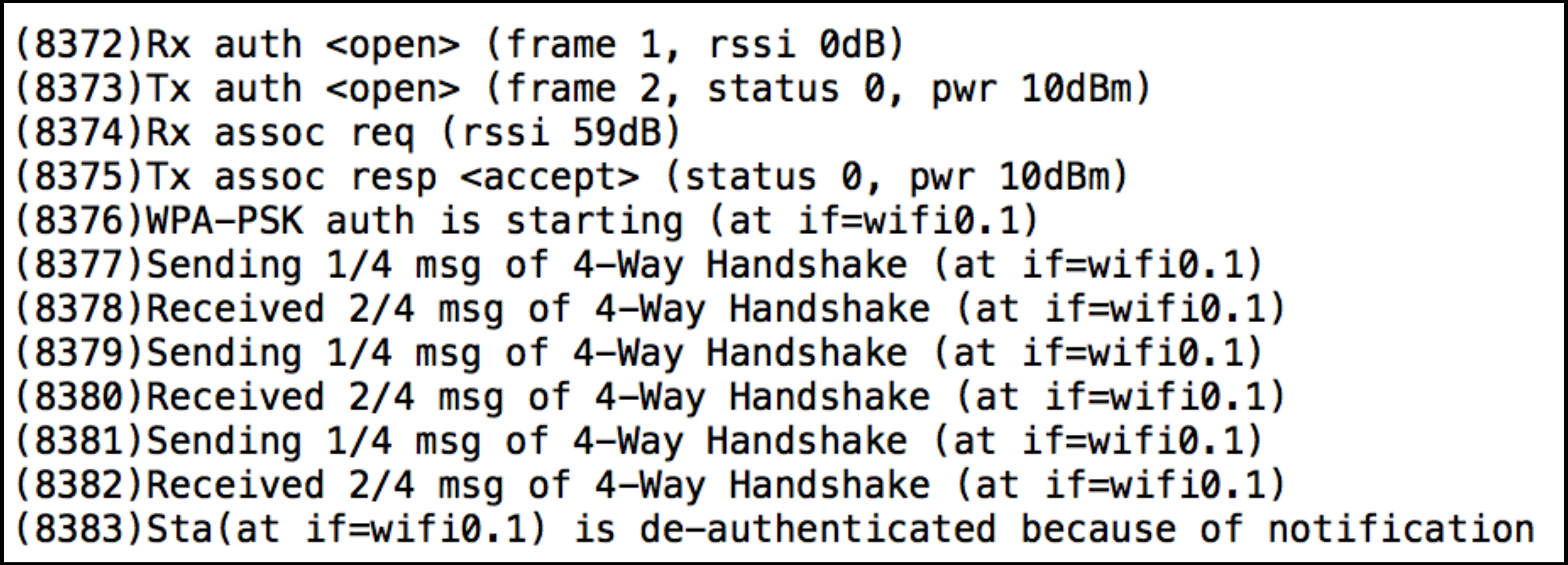
Some clients prefer to stay connected to a AP they know rather than take chance connecting to a new AP

Client Connection Problem #1



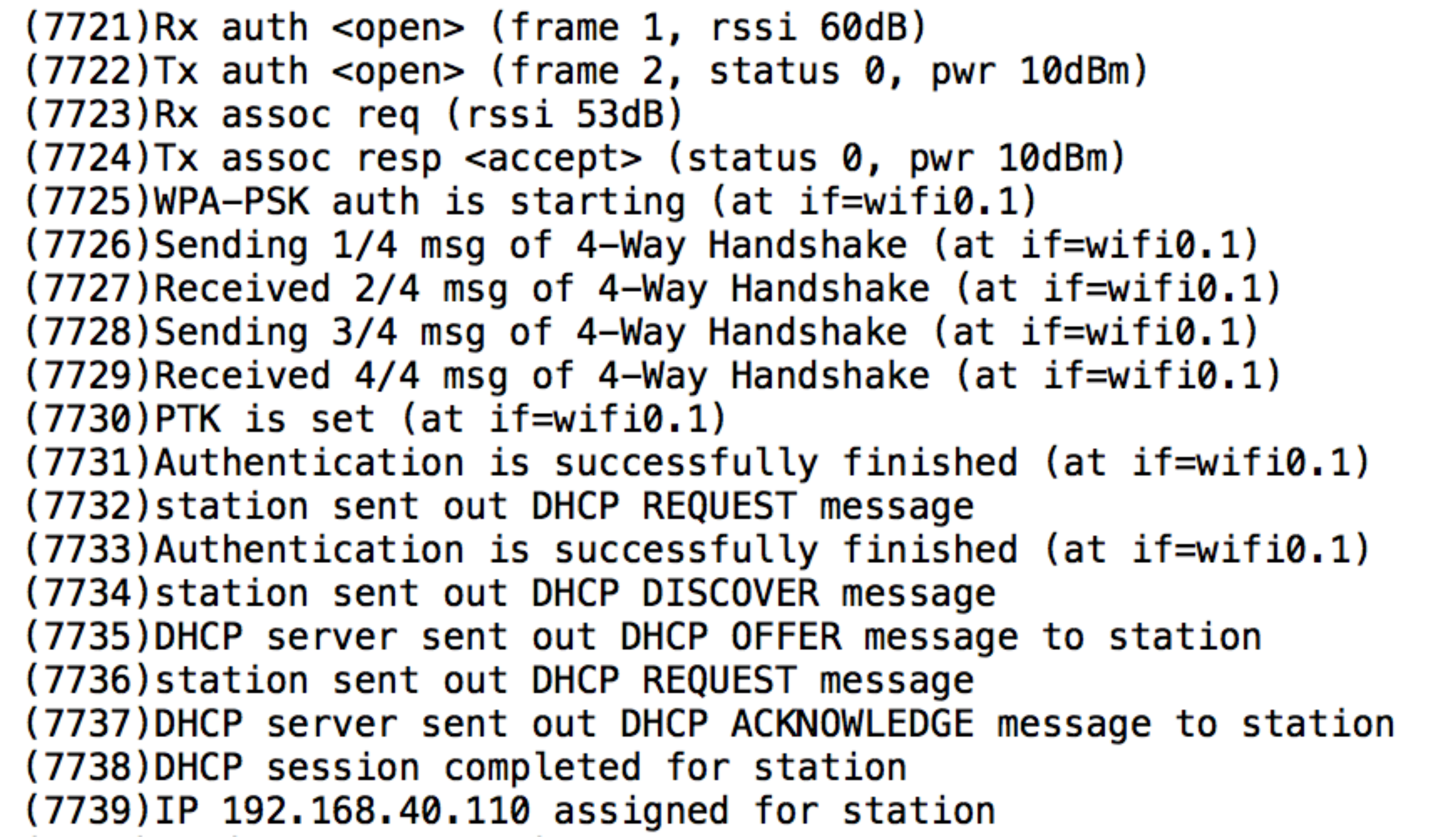
```
(4233)Rx auth <open> (frame 1, rssi 0dB)
(4234)Tx auth <open> (frame 2, status 0, pwr 2dBm)
(4235)Rx assoc req (rssi 58dB)
(4236)Tx assoc resp <accept> (status 0, pwr 2dBm)
(4237)WPA-PSK auth is starting (at if=wifi0.1)
(4238)Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1)
(4239)Received 2/4 msg of 4-Way Handshake (at if=wifi0.1)
(4240)Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1)
(4241)Received 4/4 msg of 4-Way Handshake (at if=wifi0.1)
(4242)PTK is set (at if=wifi0.1)
(4243)Authentication is successfully finished (at if=wifi0.1)
(4244)station sent out DHCP DISCOVER message
(4245)station sent out DHCP DISCOVER message
(4246)station sent out DHCP DISCOVER message
(4247)Sta(at if=wifi0.1) is de-authenticated because of notification
```

Client Connection Problem #2



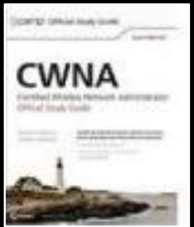
```
(8372)Rx auth <open> (frame 1, rssi 0dB)
(8373)Tx auth <open> (frame 2, status 0, pwr 10dBm)
(8374)Rx assoc req (rssi 59dB)
(8375)Tx assoc resp <accept> (status 0, pwr 10dBm)
(8376)WPA-PSK auth is starting (at if=wifi0.1)
(8377)Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1)
(8378)Received 2/4 msg of 4-Way Handshake (at if=wifi0.1)
(8379)Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1)
(8380)Received 2/4 msg of 4-Way Handshake (at if=wifi0.1)
(8381)Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1)
(8382)Received 2/4 msg of 4-Way Handshake (at if=wifi0.1)
(8383)Sta(at if=wifi0.1) is de-authenticated because of notification
```

Client Connection Success

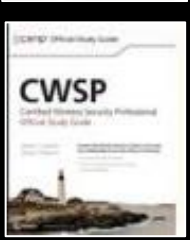


```
(7721)Rx auth <open> (frame 1, rssi 60dB)
(7722)Tx auth <open> (frame 2, status 0, pwr 10dBm)
(7723)Rx assoc req (rssi 53dB)
(7724)Tx assoc resp <accept> (status 0, pwr 10dBm)
(7725)WPA-PSK auth is starting (at if=wifi0.1)
(7726)Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1)
(7727)Received 2/4 msg of 4-Way Handshake (at if=wifi0.1)
(7728)Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1)
(7729)Received 4/4 msg of 4-Way Handshake (at if=wifi0.1)
(7730)PTK is set (at if=wifi0.1)
(7731)Authentication is successfully finished (at if=wifi0.1)
(7732)station sent out DHCP REQUEST message
(7733)Authentication is successfully finished (at if=wifi0.1)
(7734)station sent out DHCP DISCOVER message
(7735)DHCP server sent out DHCP OFFER message to station
(7736)station sent out DHCP REQUEST message
(7737)DHCP server sent out DHCP ACKNOWLEDGE message to station
(7738)DHCP session completed for station
(7739)IP 192.168.40.110 assigned for station
```

Books

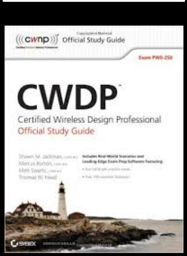


CWNA Certified Wireless Network Administrator Official Study Guide -> Wi-Fi 101

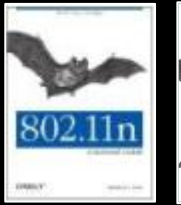


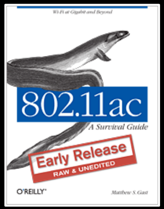
CWSP Certified Wireless Security Professional Official Study Guide -> Wi-Fi Security

CWAP Certified Wireless Analysis Professional Official Study Guide -> Wi-Fi the Protocol


((cwnp)) Official Study Guide
CWDP
Certified Wireless Design Professional
Official Study Guide

CWDP Certified Wireless Design Professional Official Study Guide -> Wi-Fi Design





802.11 Wireless Networks: The Definitive Guide, Second Edition by **Matthew Gast**

802.11n: A Survival Guide by **Matthew Gast**

802.11ac: A Survival Guide by **Matthew Gast**

W-Fi Community

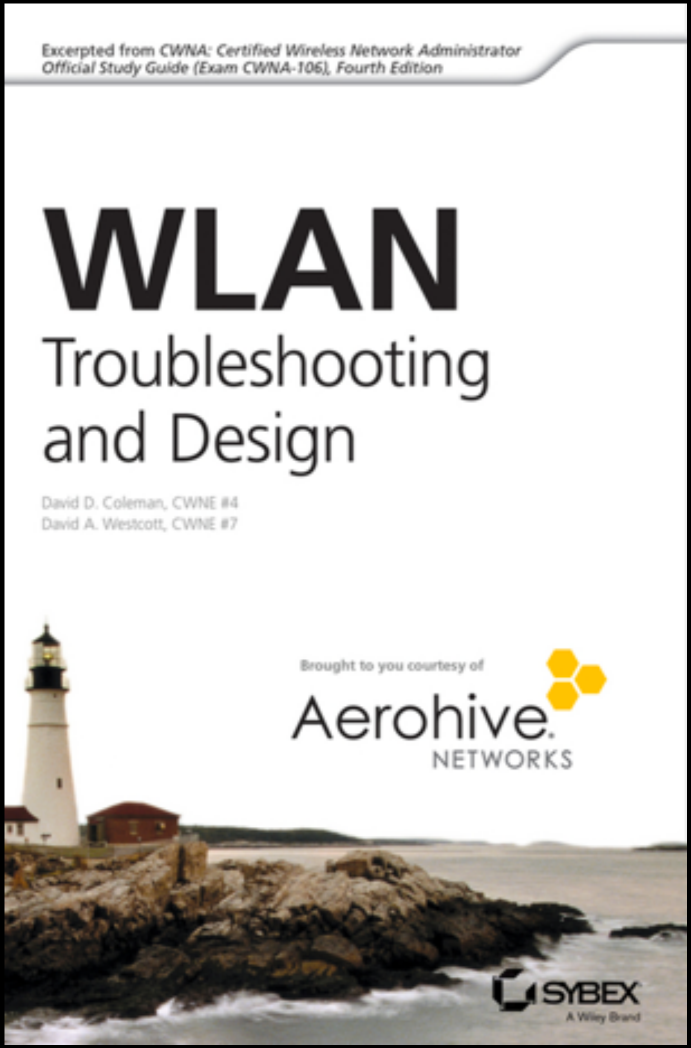
- Social Media
- Vendor Communities
- User groups
- Blogs
- Wi-Fi conferences

The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.

Wi-Fi Conferences

- CWNP Conference
- WFD – Wireless Field Day
- WLPC – WLAN Professional Conference
- WBA – Wireless Broadband Alliance
- Defcon – Wireless Village

Free Troubleshooting Book



Excerpted from *CWNA: Certified Wireless Network Administrator Official Study Guide (Exam CWNA-106), Fourth Edition*

WLAN

Troubleshooting and Design

David D. Coleman, CWNE #4
David A. Westcott, CWNE #7

Brought to you courtesy of

Aerohive. NETWORKS

SYBEX
A Wiley Brand

https://goo.gl/8Dv2qg

or

https://community.aerohive.com/aerohive/topics/download-a-free-booklet-about-wlan-troubleshooting

QUESTIONS?

FIN ACK