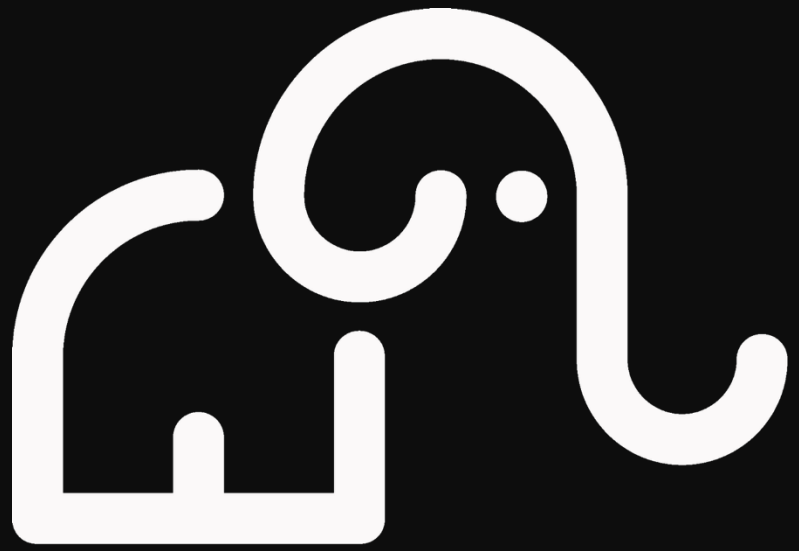
Wi-Fi HaLow & other Wireless IoT Technologies

@troymart



Wi-Co

Wireless Community

Troy Martin

Canadian Rockies

Like things wireless…

Enjoy cycling….

@troymart


#WiCo

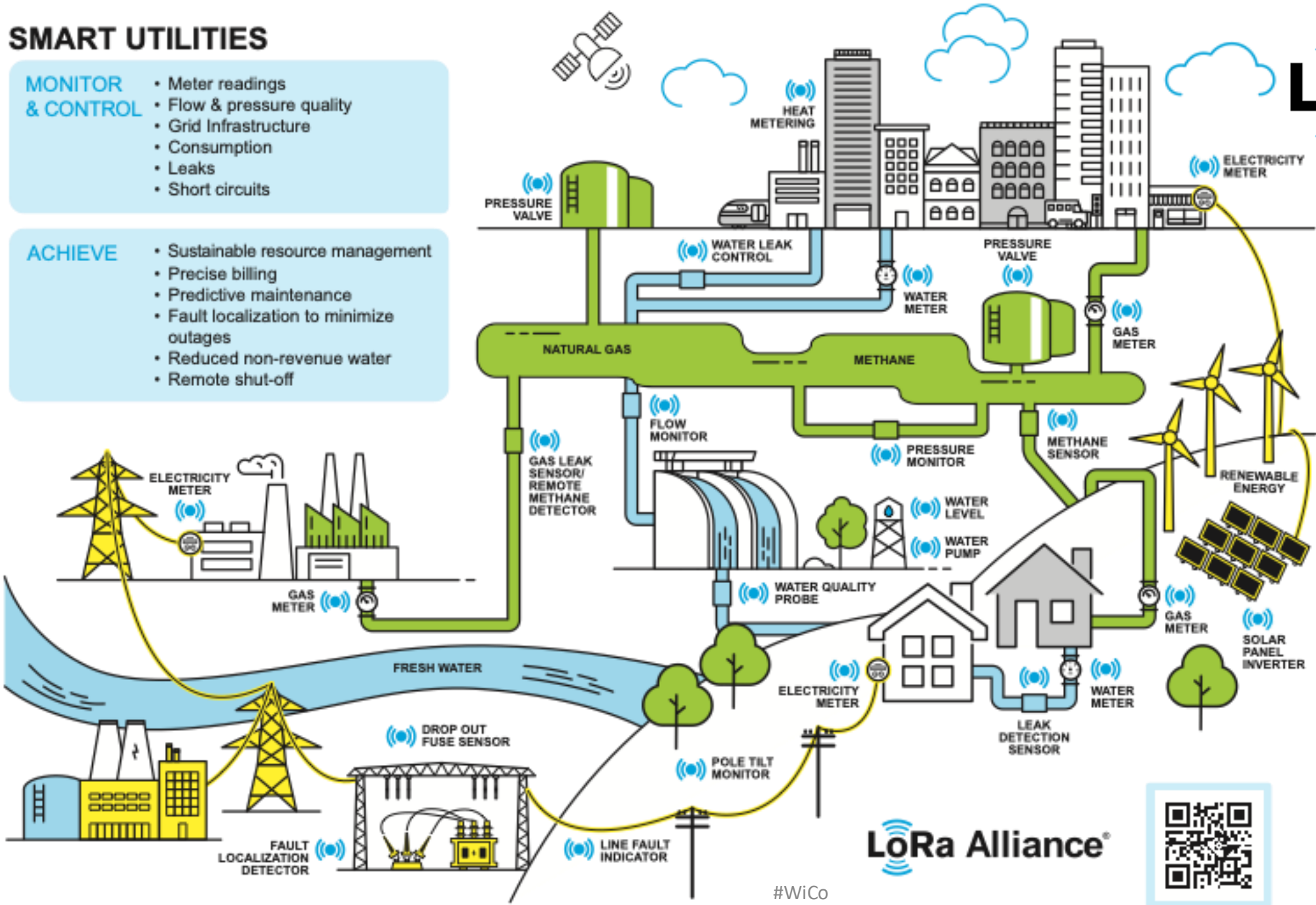
SMART UTILITIES

MONITOR & CONTROL

- Meter readings
- Flow & pressure quality
- Grid Infrastructure
- Consumption
- Leaks
- Short circuits

ACHIEVE

- Sustainable resource management
- Precise billing
- Predictive maintenance
- Fault localization to minimize outages
- Reduced non-revenue water
- Remote shut-off



LoRaWAN®

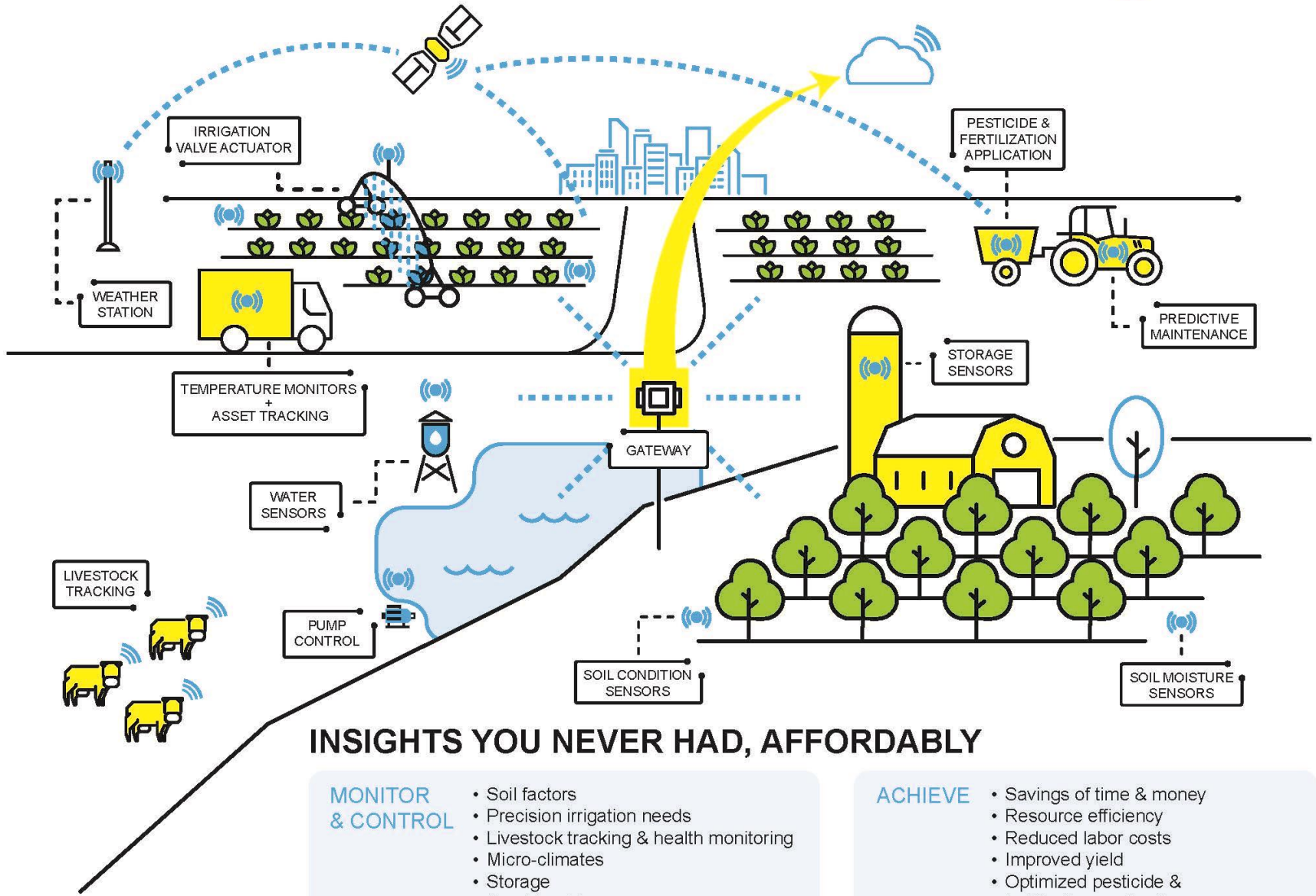
For Profitable and Efficient Utilities

LoRa Alliance®

#WiCo

LoRaWAN® FOR SMART AGRICULTURE

IoT in Difficult to Reach Locations



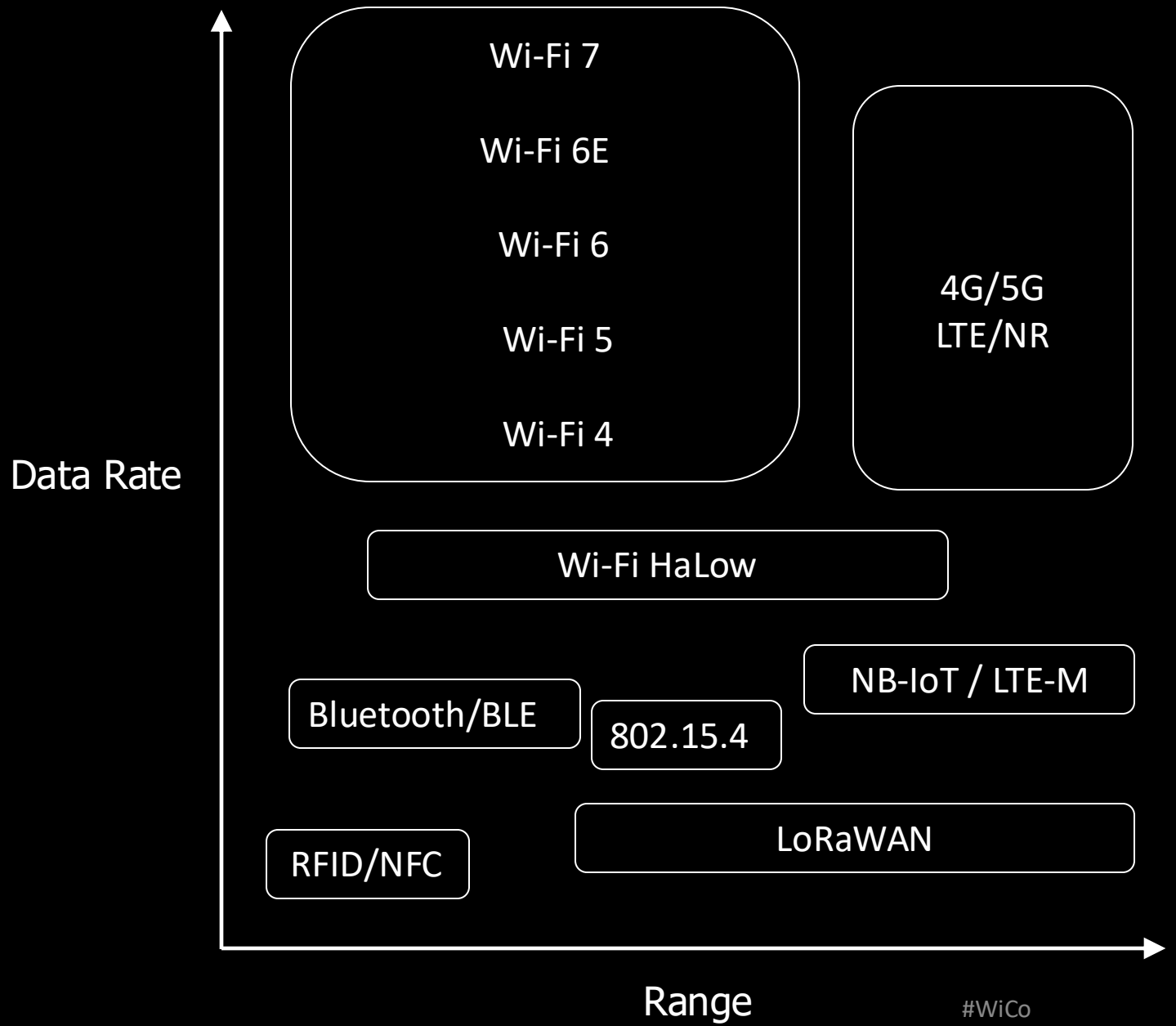
INSIGHTS YOU NEVER HAD, AFFORDABLY

MONITOR & CONTROL

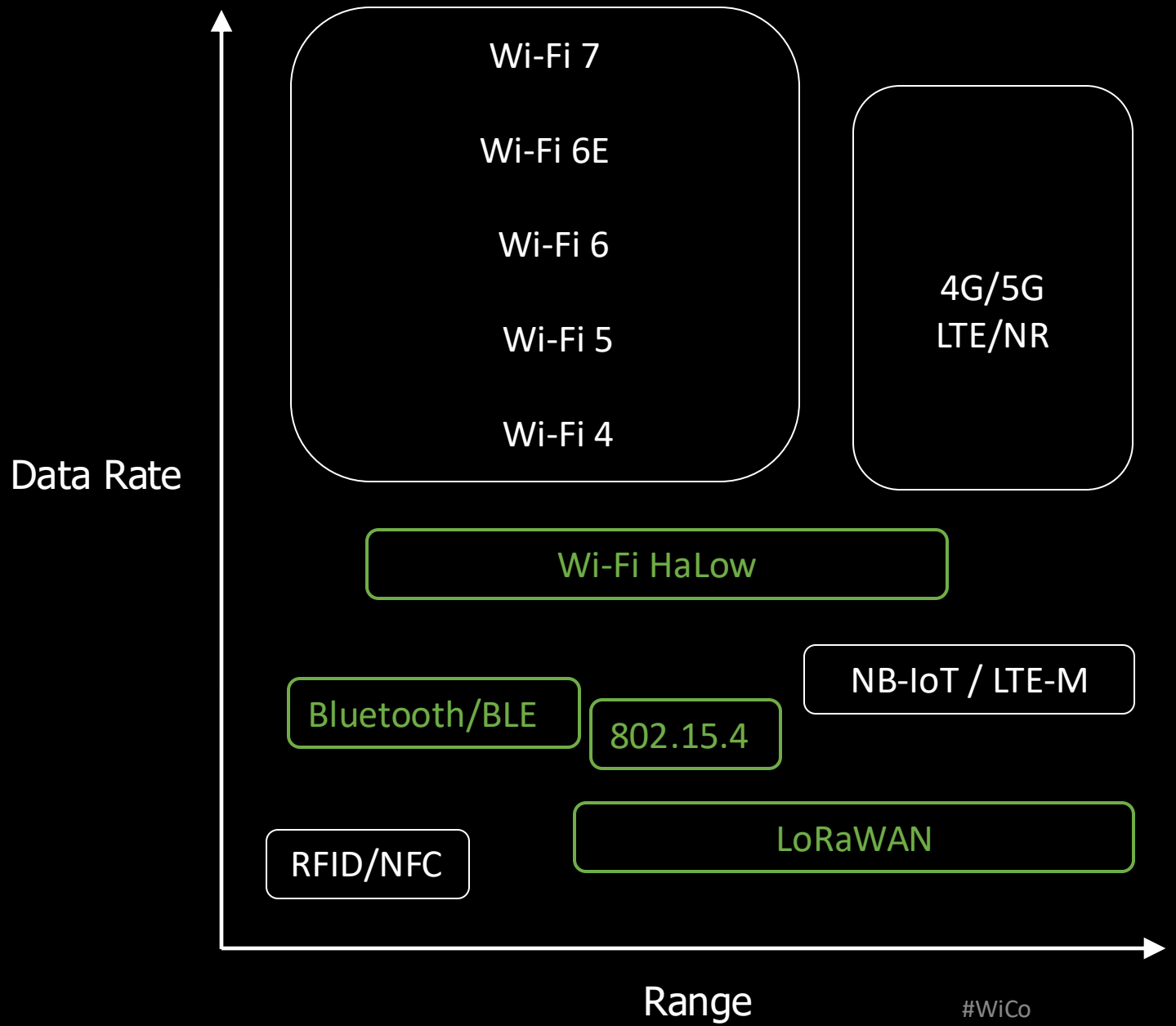
- Soil factors
- Precision irrigation needs
- Livestock tracking & health monitoring
- Micro-climates
- Storage
- Asset tracking
- Fertilizer & feed
- Irrigation valves & pump

ACHIEVE

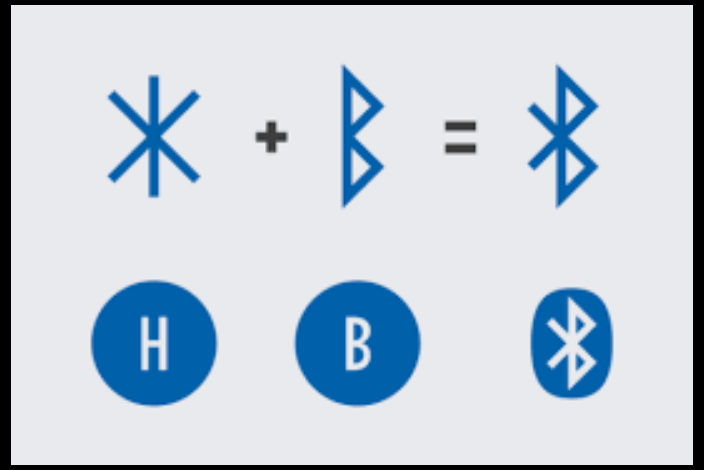
- Savings of time & money
- Resource efficiency
- Reduced labor costs
- Improved yield
- Optimized pesticide & fertilization application
- Healthier & more productive livestock
- Sustainability



"Generations of Wi-Fi prior to Wi-Fi 4 will not be assigned names." - WFA



"Generations of Wi-Fi prior to Wi-Fi 4 will not be assigned names." - WFA

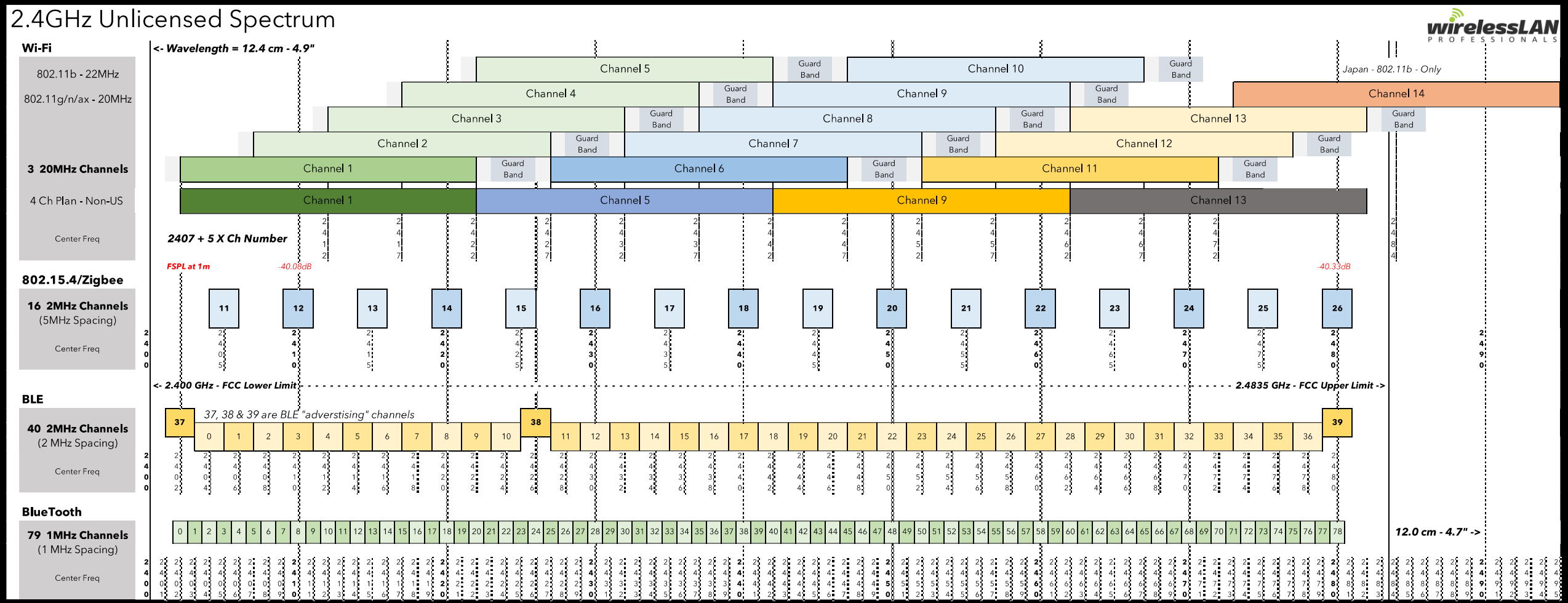


Haraldr Blátǫnn Gormsson

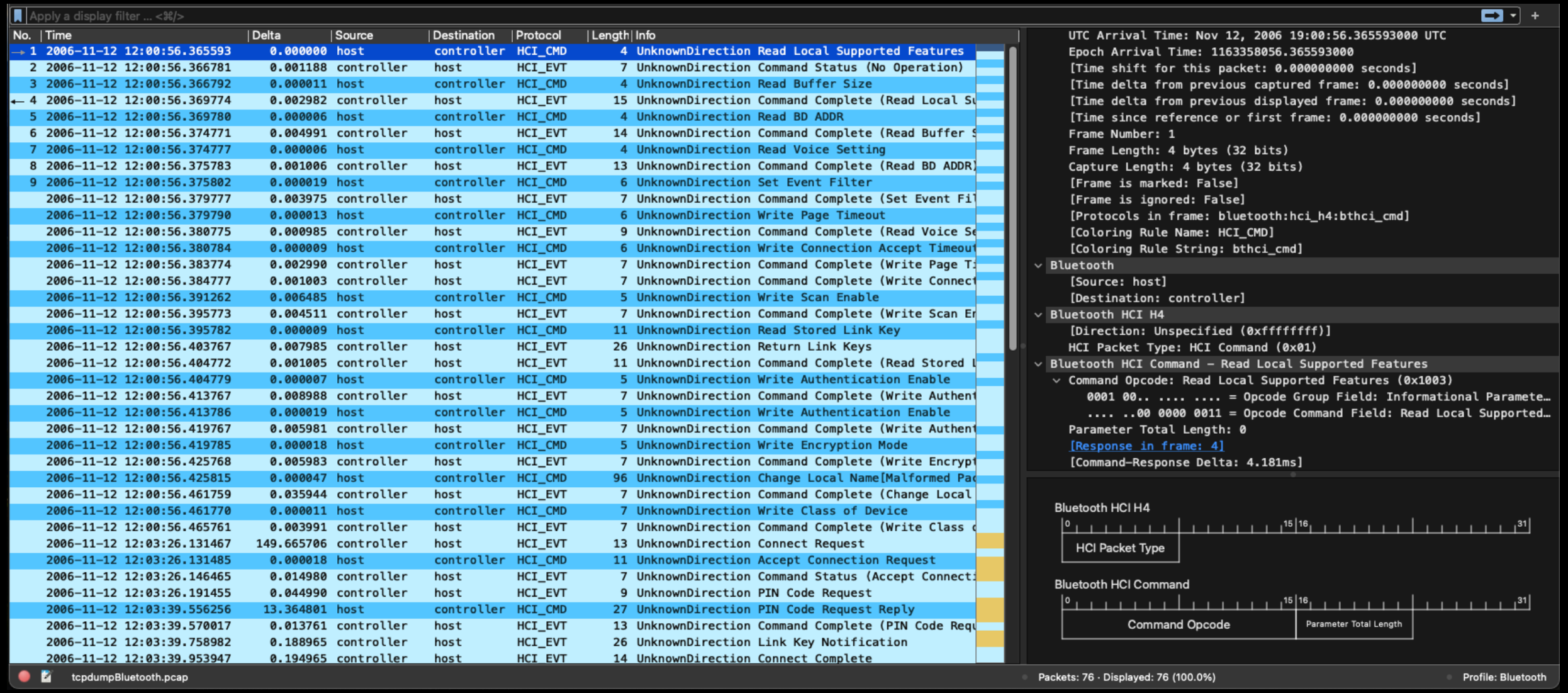
Bluetooth: connected

User: then, act like it

2.4GHz Unlicensed Spectrum



Bluetooth PCAP



Zigbee Overview

LOW POWER

BASED ON IEEE 802.15.4

2.4 GHZ ISM WITH 16 CHANNELS

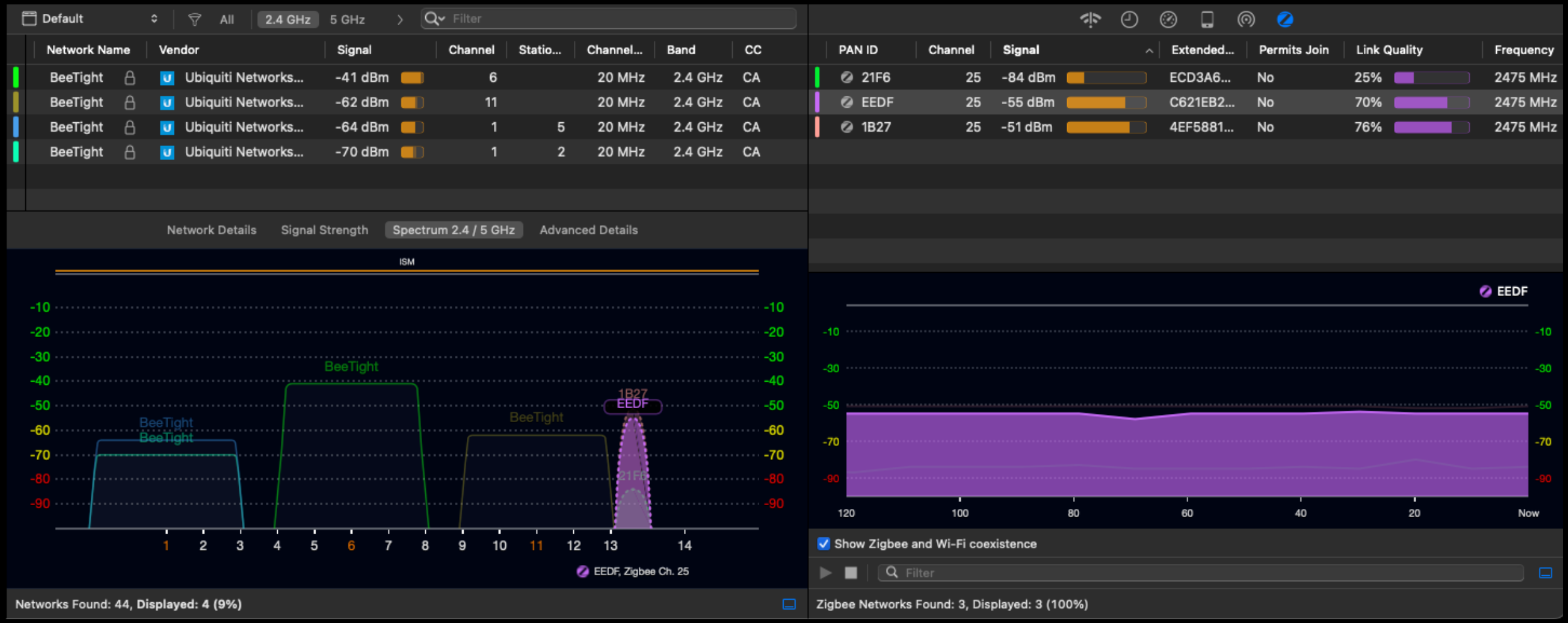
CHANNELS: 2 MHZ WIDE / 5 MHZ SPACING

SELF-FORMING, SELF-HEALING -> MESH, STAR, OR TREE TOPOLOGY

NETWORK SIZE: UP TO 65,000 NODES (V3.0)

DATA RATE: 250 Kbps

128-bit AES encryption


Default
All
2.4 GHz
5 GHz
Filter
Network Name
Vendor
Signal
Channel
Statio...
Channel...
Band
CC
BeeTight
Ubiquiti Networks...
-41 dBm
6
20 MHz
2.4 GHz
CA
BeeTight
Ubiquiti Networks...
-62 dBm
11
20 MHz
2.4 GHz
CA
BeeTight
Ubiquiti Networks...
-64 dBm
1
5
20 MHz
2.4 GHz
CA
BeeTight
Ubiquiti Networks...
-70 dBm
1
2
20 MHz
2.4 GHz
CA
Network Details
Signal Strength
Spectrum 2.4 / 5 GHz
Advanced Details
ISM
-10
-20
-30
-40
-50
-60
-70
-80
-90
BeeTight
BeeTight
BeeTight
BeeTight
1B27
EEDF
21F6
1
2
3
4
5
6
7
8
9
10
11
12
13
14
EEDF, Zigbee Ch. 25
Networks Found: 44, Displayed: 4 (9%)
PAN ID
Channel
Signal
Extended...
Permits Join
Link Quality
Frequency
21F6
25
-84 dBm
ECD3A6...
No
25%
2475 MHz
EEDF
25
-55 dBm
C621EB2...
No
70%
2475 MHz
1B27
25
-51 dBm
4EF5881...
No
76%
2475 MHz
EEDF
-10
-30
-50
-70
-90
120
100
80
60
40
20
Now
Show Zigbee and Wi-Fi coexistence
Filter
Zigbee Networks Found: 3, Displayed: 3 (100%)

UNITED STATES FREQUENCY ALLOCATIONS

THE RADIO SPECTRUM

RADIO SERVICES COLOR LEGEND

- AERONAUTICAL MOBILE
- AERONAUTICAL MOBILE SATELLITE
- AERONAUTICAL RADIONAVIGATION
- AMATEUR
- AMATEUR SATELLITE
- BROADCASTING
- BROADCASTING SATELLITE
- EARTH EXPLORATION SATELLITE
- FIXED
- FIXED SATELLITE
- INTER-SATELLITE
- LAND MOBILE
- LAND MOBILE SATELLITE
- MARITIME MOBILE
- MARITIME MOBILE SATELLITE
- MARITIME RADIONAVIGATION
- METEOROLOGICAL
- METEOROLOGICAL SATELLITE
- MOBILE
- MOBILE SATELLITE
- RADIO ASTRONOMY
- RADIODETERMINATION SATELLITE
- RADIOLOCATION
- RADIOLOCATION SATELLITE
- RADIONAVIGATION
- RADIONAVIGATION SATELLITE
- SPACE OPERATION
- SPACE RESEARCH
- STANDARD FREQUENCY AND TIME SIGNAL
- STANDARD FREQUENCY AND TIME SIGNAL SATELLITE

ACTIVITY CODE

- FEDERAL EXCLUSIVE
- FEDERAL/NON-FEDERAL SHARED
- NON-FEDERAL EXCLUSIVE

ALLOCATION USAGE DESIGNATION

SERVICE	EXAMPLE	DESCRIPTION
Primary	FIXED	Capital Letters
Secondary	Mobile	1st Capital with lower case letters

This chart is a graphic single-point-in-time portrayal of the Table of Frequency Allocations used by the FCC and NTIA. As such, it may not completely reflect all aspects, i.e. footnotes and recent changes made to the Table of Frequency Allocations. Therefore, for complete information, users should consult the Table to determine the current status of U.S. allocations.

U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Office of Spectrum Management

JANUARY 2016

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; Washington, DC area (202) 512-1800
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

* EXCEPT AERONAUTICAL MOBILE (R)

** EXCEPT AERONAUTICAL MOBILE

PLEASE NOTE: THE SPACING ALLOTTED THE SERVICES IN THE SPECTRUM SEGMENTS SHOWN IS NOT PROPORTIONAL TO THE ACTUAL AMOUNT OF SPECTRUM OCCUPIED.

#WiCo

LoRaWAN Overview

- Low-Power
- Long-Range (LoRa)
- Low data rate < 20 kbps
- Sub-1GHz
- Adaptive data rates (ADR)
- Modulation derived from Chirp Spread Spectrum (CSS) using chirp pulse
- End-to-end AES 128-bit encryption

Spread Spectrum

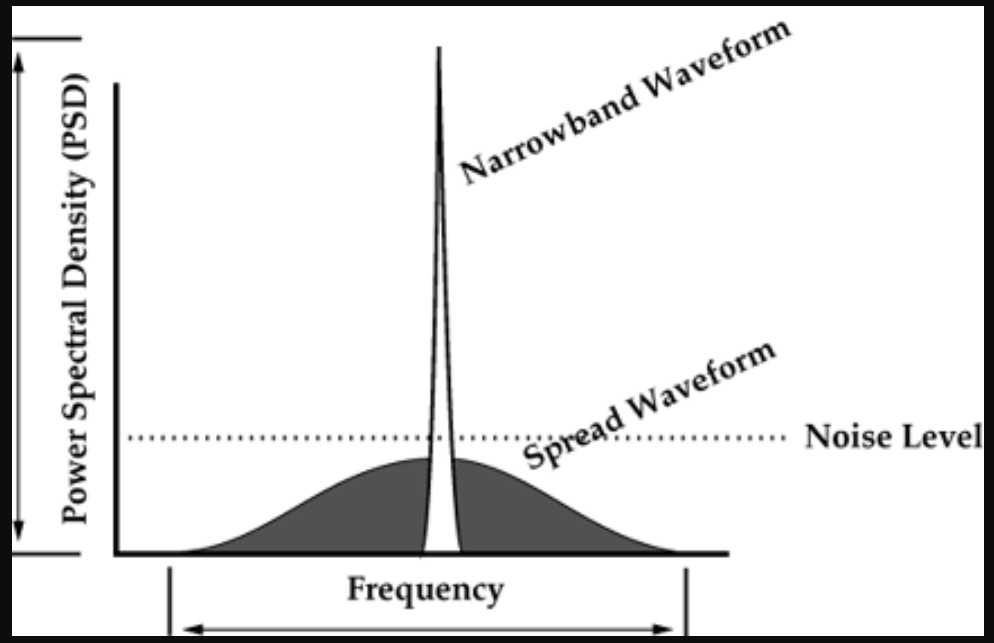
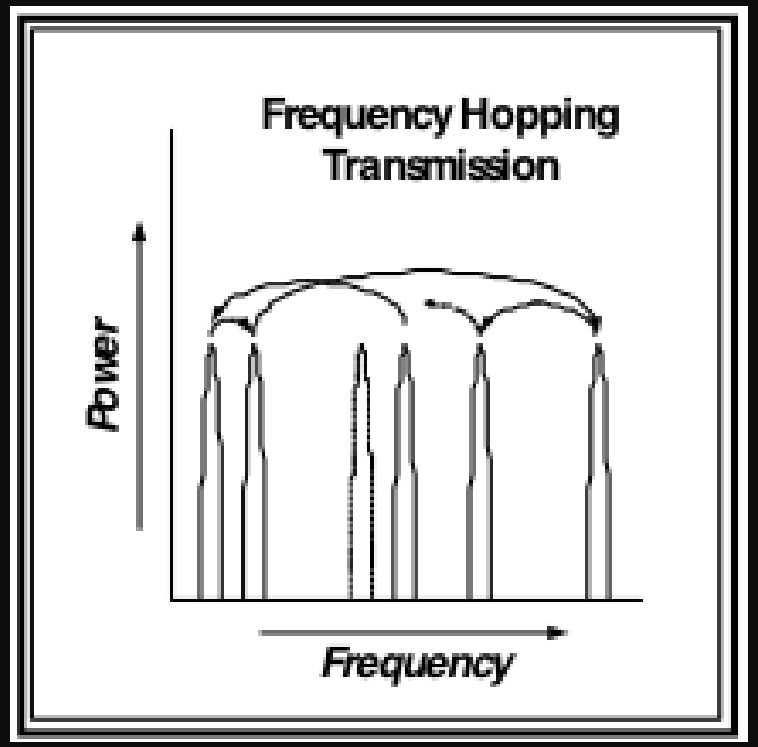


Image Source: "Spread Spectrum – it's not just for breakfast anymore!" www.gsl.net

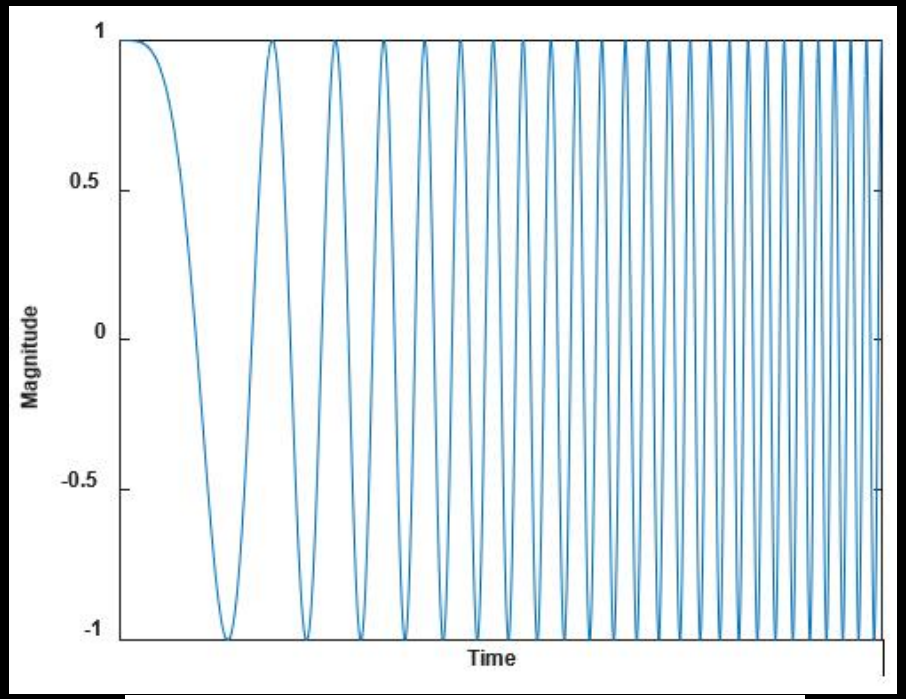


Chirp Spread Spectrum (CSS)

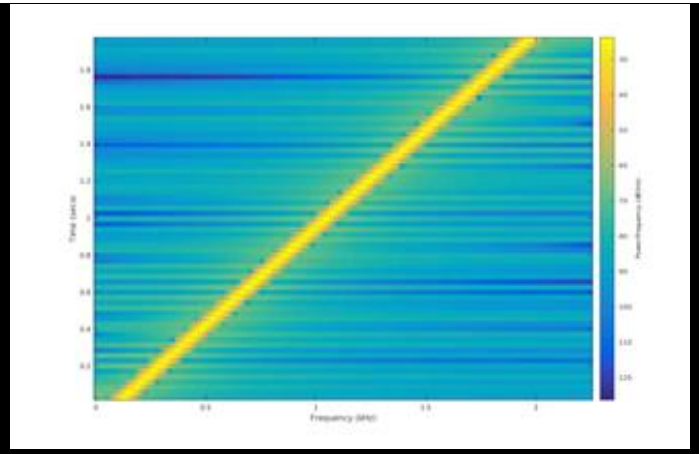
- Linear chirp waveform
- Sinusoidal wave that increase in frequency linearly over time

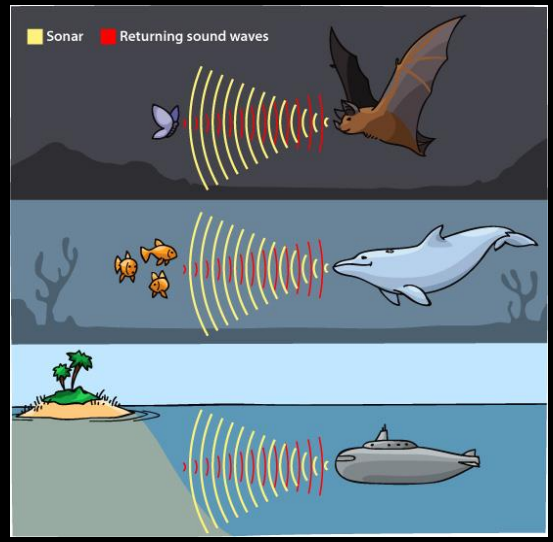
- Upchirp: frequency increase over time
- Downchirp: frequency decrease over time

Up-chirp



Spectrogram of a linear chirp





Receive Sensitivity

Lower SF
Higher DR

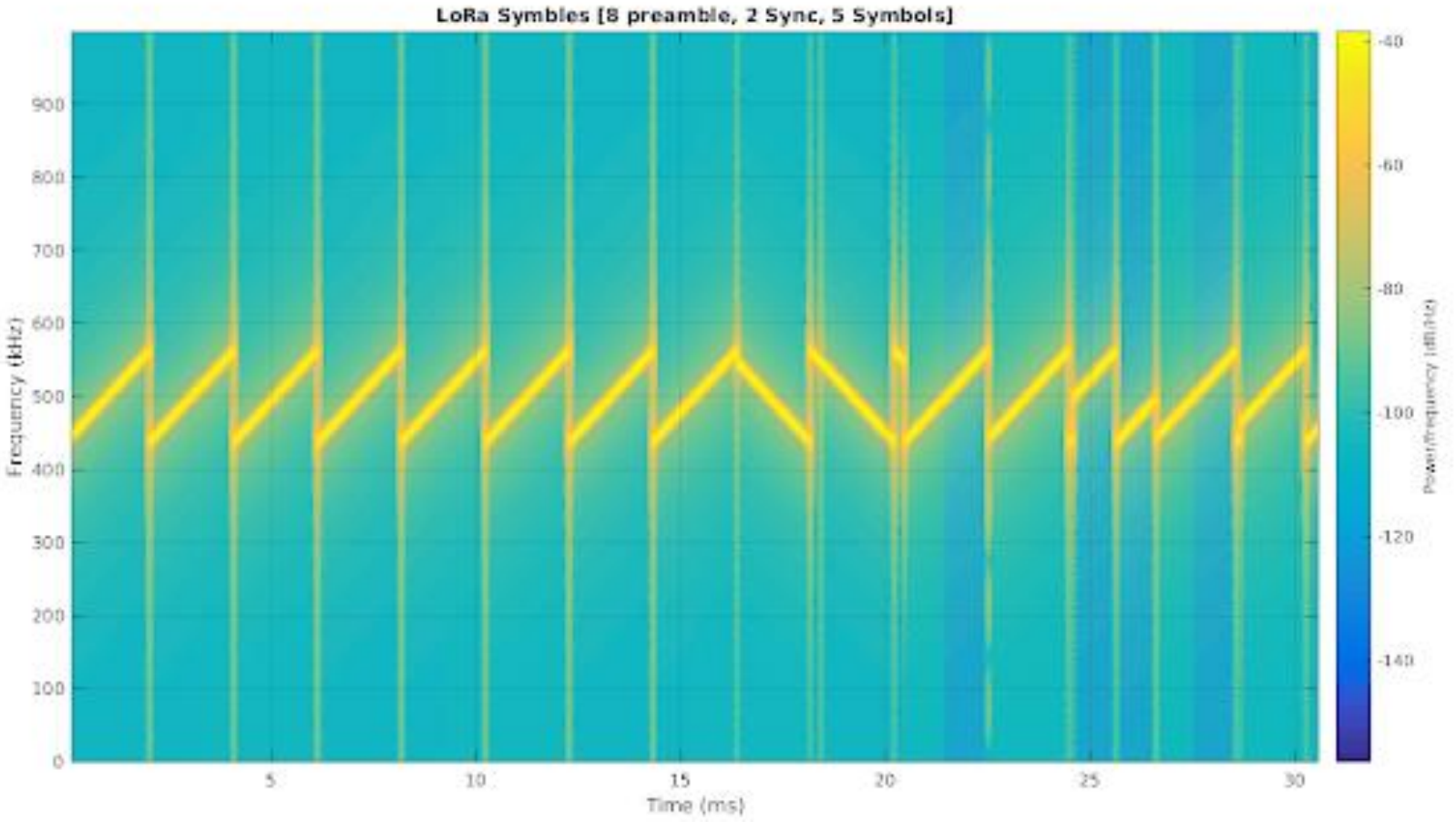
Spreading factor SF	Receiver sensitivity for bandwidth fixed at 125kHz	SNR Limit (dB)	Time on Air (ms)
SF7	-123 dBm	-7.5	46
SF8	-126 dBm	-10	82
SF9	-129 dBm	-12.5	165
SF10	-132 dBm	-15	289
SF11	-134.5 dBm	-17.5	660
SF12	-137 dBm	-20	1155

>400ms, NOT supported in US @125KHz

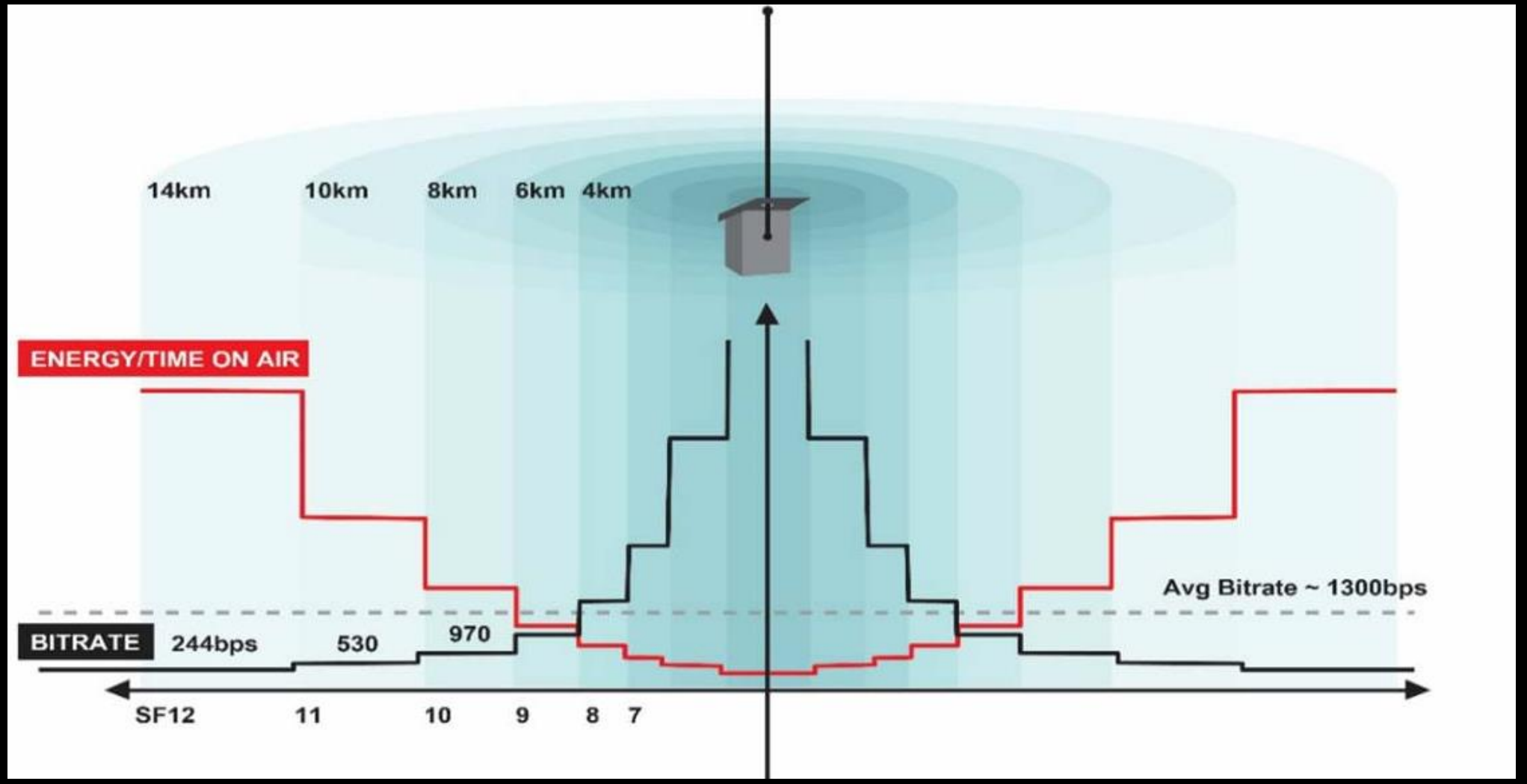
Higher SF
Lower DR

LoRaWAN Transmission

- Symbol time
- Time on air
- Coding
- Throughput



Adaptive Data Rate (ADR) Mechanism



Wi-Fi CERTIFIED HaLow™ for IoT

Features

- Sub-1 GHz spectrum operation
- Narrow band OFDM channels
- Several device power saving modes
- Native IP support
- Latest Wi-Fi® security

Benefits

- Long range: approximately 1 km
- Penetration through walls and other obstacles
- Supports coin cell battery devices for months or years
- No need for proprietary hubs or gateways

Source: Wi-Fi Alliance - https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-halow


60 GHz
For extremely high-definition or virtual reality applications, without walls
WiGig
2.4, 5, & 6 GHz
For extremely high-definition or virtual reality applications (VR/AR/XR), with walls
Wi-Fi 7
6 GHz
160 MHz channels enable next-level user experience
Wi-Fi 6E
2.4 & 5 GHz
For extremely high uplink performance, but with power management (IoT)
Wi-Fi 6R2
2.4 & 5 GHz
High capacity and speed for most advanced applications
Wi-Fi 6
5 GHz
Great for daily use and functionality; supports multiple users
Wi-Fi 5
2.4 & 5 GHz
Good coverage for every day, light bandwidth connectivity needs
Wi-Fi 4
Sub-1GHz
Best for long range, low power connectivity, penetration through walls
Wi-Fi HaLow

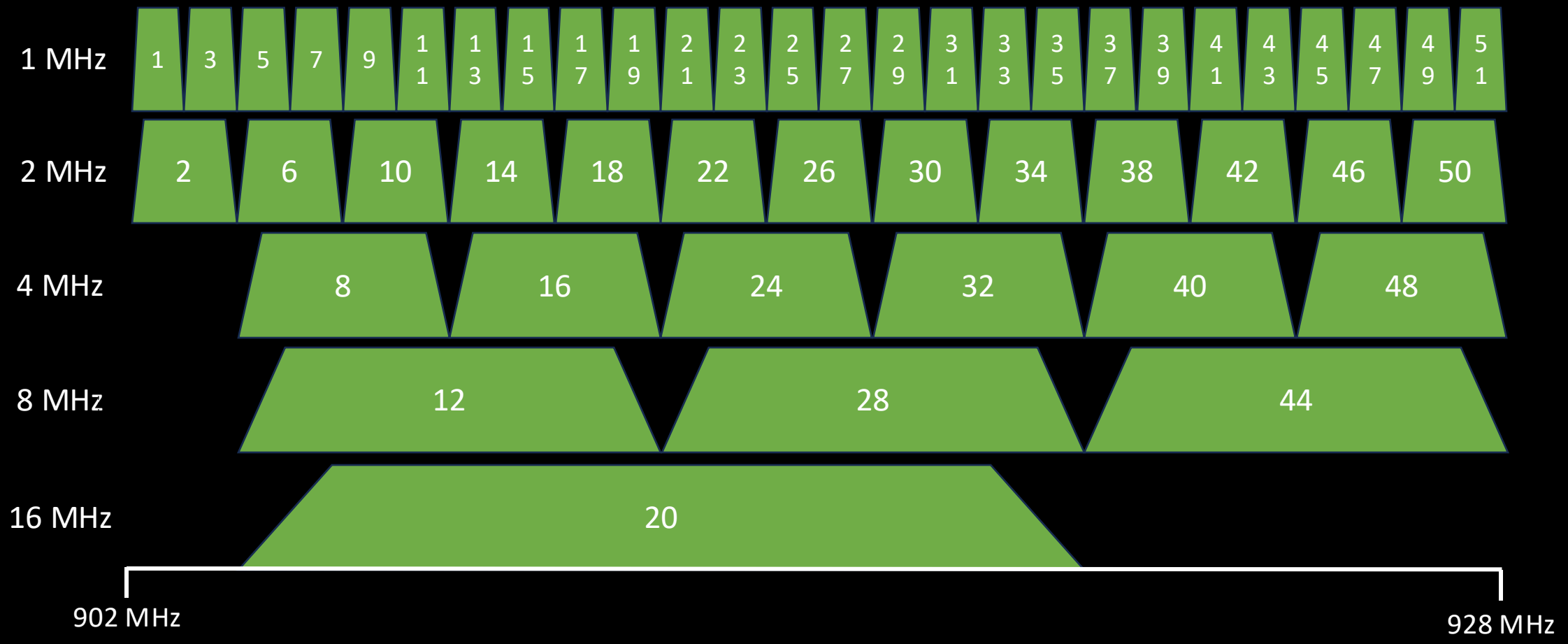
#WiCo

Wi-Fi CERTIFIED HaLow™ for IoT

Function	Wi-Fi 5 (IEEE 802.11ac)	Wi-Fi HaLow (IEEE 802.11ah)
Operating frequency band	2.4, 5, and 6 GHz (Wi-Fi 7)	Sub-1 GHz (915 MHz US, 868 MHz EU)
Channel Width	20/40/80/160 MHz	1/2/4/8/16 MHz
Max addressable stations per AP	2007	8191
Single Stream (1SS) MCS data-rate	6.5 to 866.7 Mb/s (802.11ac, Wi-Fi 5) 6.5 to 150 Mb/s (802.11n, Wi-Fi 4)	150 kb/s to 86.7 Mb/s
"Typical" Range	~ 100 m (328 ft)	~1 Km (0.62 mi)
Link Budget	REF	Upwards of 24dB improvement
MCS Index	0-9	0-9 & 10
Subcarrier Width	312.5 kHz	31.2 kHz
Symbol Time	3.2 µs (3.6 or 4.0 µs with SGI/GI)	32 µs (36 or 40.0 µs with SGI/GI)
Spatial Streams	1-8	1-4
Modulation Types	BPSK, QPSK, 16-QAM, 256-QAM	

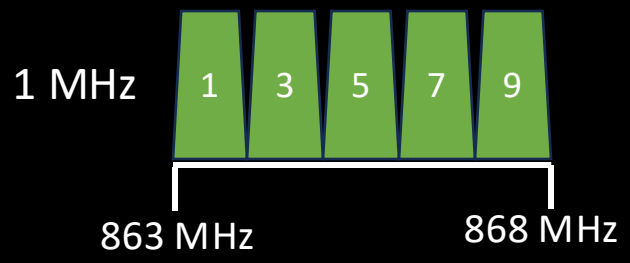
WPA3 Support

802.11ah Channels in US/CAN*



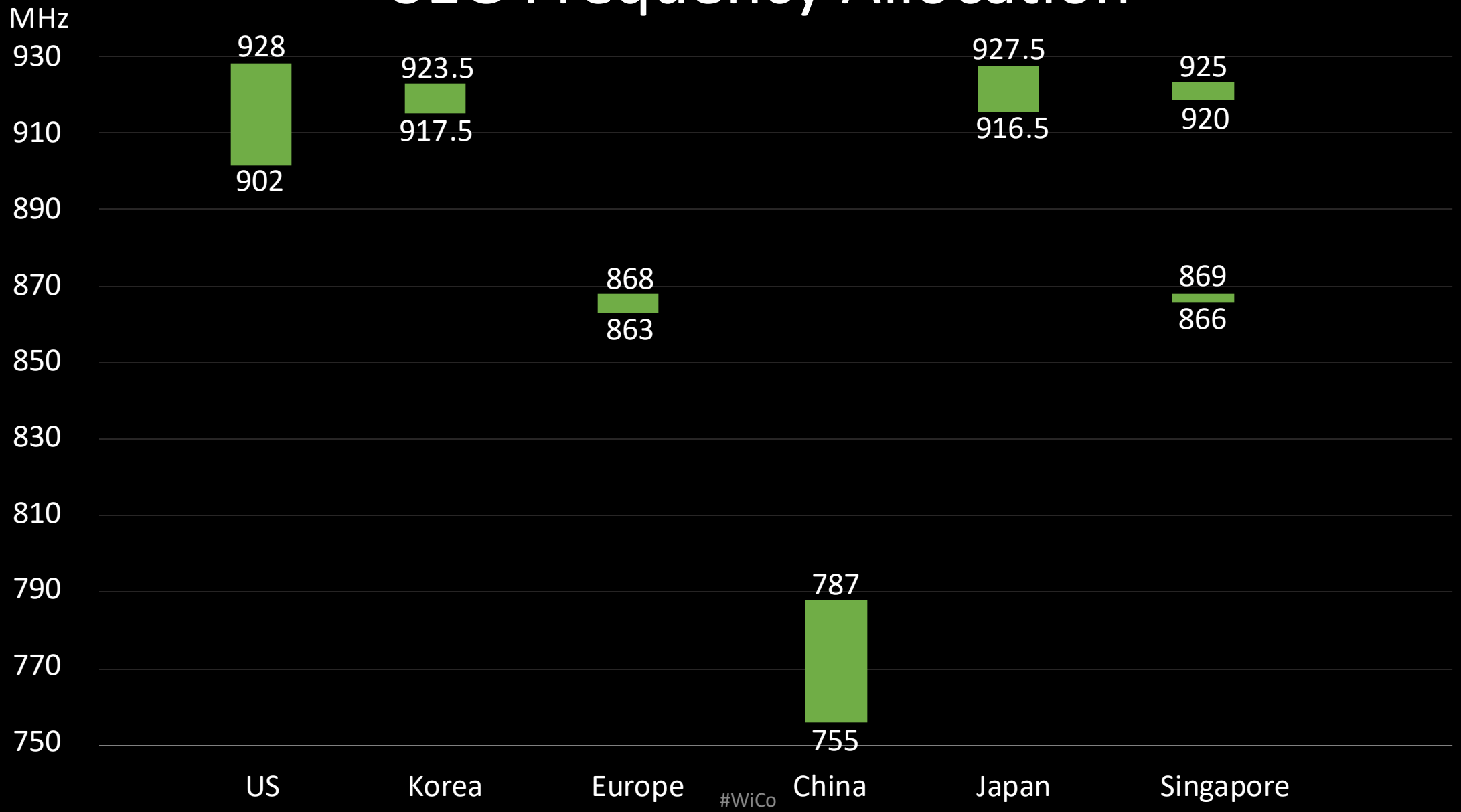
*Index values found in IEEE 802.11ah-2016

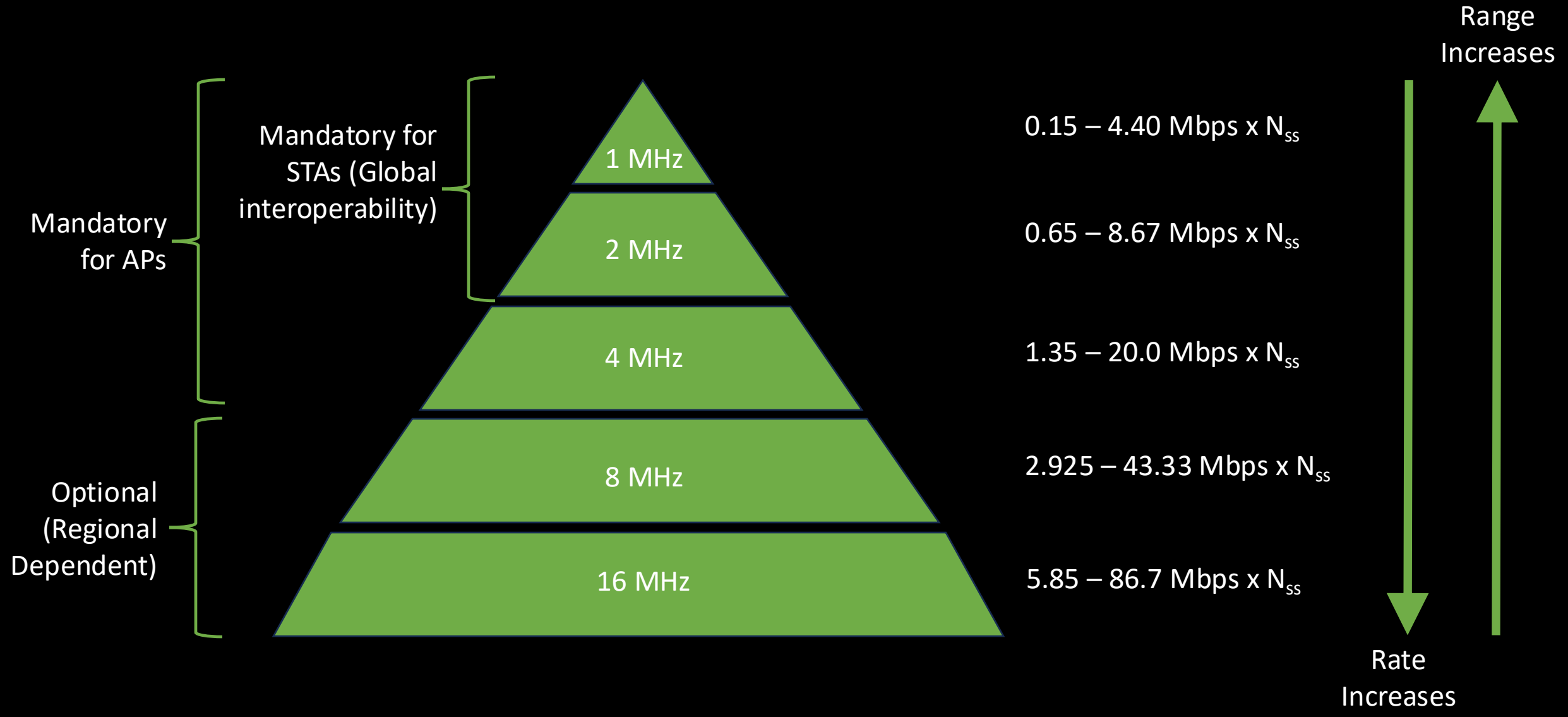
802.11ah Channels in the EU*



*Index values found in HaLow hardware configuration

S1G Frequency Allocation





N_{ss} = Number of Spatial Streams (1-4)

MCSINDEX.NET

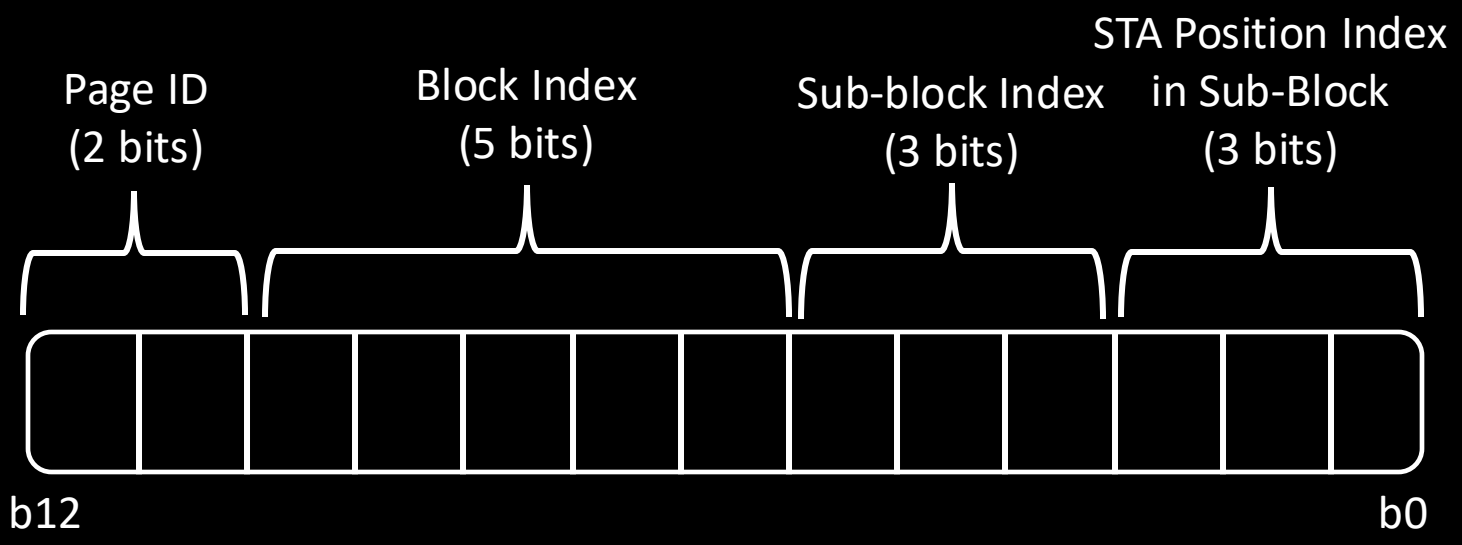
MCS Table (HT/VHT/HE) - MCSINDEX.NET

				OFDM (802.11ah) HaLow									
MCS Index	Spatial Stream	Modulation	Coding	1MHz		2MHz		4MHz		8MHz		16MHz	
				0.8µs GI	0.4µs GI	0.8µs GI	0.4µs GI	0.8µs GI	0.4µs GI	0.8µs GI	0.4µs GI	0.8µs GI	0.4µs GI
0	1	BPSK	1/2	0.3	0.33	0.65	0.7	1.35	1.5	2.925	3.3	5.85	6.5
1	1	QPSK	1/2	0.6	0.67	1.3	1.44	2.7	3.0	5.85	6.5	11.7	13.0
2	1	QPSK	3/4	0.9	1.00	1.95	2.17	4.05	4.5	8.78	9.8	17.6	19.5
3	1	16-QAM	1/2	1.2	1.33	2.6	2.89	5.4	6.0	11.7	13.0	23.4	26.0
4	1	16-QAM	3/4	1.8	2.00	3.9	4.33	8.1	9.0	17.55	19.5	35.1	39.0
5	1	64-QAM	2/3	2.4	2.67	5.2	5.78	10.8	12.0	23.4	26.0	46.8	52.0
6	1	64-QAM	3/4	2.7	3.00	5.85	6.5	12.15	13.5	26.33	29.3	52.65	58.5
7	1	64-QAM	5/6	3.0	3.33	6.5	7.22	13.5	15.0	29.25	32.5	58.5	65.0
8	1	256-QAM	3/4	3.6	4.00	7.8	8.67	16.2	18.0	35.1	39.0	70.2	78.0
9	1	256-QAM	5/6	4.0	4.44	-	-	18	20.0	39	43.3	78	86.7
10	1	BPSK	1/2 x 2	0.15	0.17	-	-	-	-	-	-	-	-
0	2	BPSK	1/2	0.6	0.7	1.3	1.4	2.7	3.0	5.85	6.5	11.7	13.0
1	2	QPSK	1/2	1.2	1.3	2.6	2.9	5.4	6.0	11.7	13.0	23.4	26.0
2	2	QPSK	3/4	1.8	2.0	3.9	4.3	8.1	9.0	17.55	19.5	35.1	39.0
3	2	16-QAM	1/2	2.4	2.7	5.2	5.8	10.8	12.0	23.4	26.0	46.8	52.0
4	2	16-QAM	3/4	3.6	4.0	7.8	8.7	16.2	18.0	35.1	39.0	70.2	78.0
5	2	64-QAM	2/3	4.8	5.33	10.4	11.6	21.6	24.0	46.8	52.0	93.6	104
6	2	64-QAM	3/4	5.4	6.0	11.7	13.0	24.3	27.0	52.65	58.5	105.3	117
7	2	64-QAM	5/6	6.0	6.67	13	14.4	27	30.0	58.5	65.0	117	130
8	2	256-QAM	3/4	7.2	8.0	15.6	17.3	32.4	36.0	70.2	78.0	140.4	156
9	2	256-QAM	5/6	8.0	8.85	-	-	35.9	39.8	77.7	86.3	155.4	173
0	3	BPSK	1/2	0.9	1.0	2.0	2.2	4.05	4.5	8.78	9.8	17.55	19.5
1	3	QPSK	1/2	1.8	2.0	1.95	4.3	8.1	9.0	17.55	19.5	35.1	39.0
2	3	QPSK	3/4	2.7	3.0	3.90	6.5	12.15	13.5	26.33	29.3	52.65	58.5
3	3	16-QAM	1/2	3.6	4.0	5.85	8.7	16.2	18.0	35.1	39.0	70.2	78
4	3	16-QAM	3/4	5.4	6.0	7.80	13.0	24.3	27.0	52.65	58.5	105.3	117
5	3	64-QAM	2/3	7.2	8.0	11.70	17.3	32.4	36.0	70.2	78.0	140.4	156
6	3	64-QAM	3/4	8.1	9.0	15.60	19.5	36.45	40.5	-	-	157.95	176
7	3	64-QAM	5/6	9.0	10.0	17.55	21.7	40.5	45.0	87.75	97.5	175.5	195
8	3	256-QAM	3/4	10.8	12.0	19.50	26.0	48.6	54.0	105.3	117.0	211	234
9	3	256-QAM	5/6	12.0	13.3	23.40	28.8	53.78	59.8	117	129	-	-
0	4	BPSK	1/2	1.2	1.3	2.6	2.9	5.4	6.0	11.7	13.0	23.4	26.0
1	4	QPSK	1/2	2.4	2.7	5.2	5.8	10.8	12.0	23.4	26.0	46.8	52.0
2	4	QPSK	3/4	3.6	4.0	7.8	8.7	16.2	18.0	35.1	39.0	70.2	78.0
3	4	16-QAM	1/2	4.8	5.3	10.4	11.6	21.6	24.0	46.8	52.0	93.6	104.0
4	4	16-QAM	3/4	7.2	8.0	15.6	17.3	32.4	36.0	70.2	78.0	140.4	156.0
5	4	64-QAM	2/3	9.6	10.7	20.8	23.1	43.2	48.0	93.6	104.0	187.2	208.0
6	4	64-QAM	3/4	10.8	12.0	23.4	26.0	48.6	54.0	105.3	117.0	210.6	234.0
7	4	64-QAM	5/6	12.0	13.3	26	28.9	54	60.0	117	130.0	234	260.0
8	4	256-QAM	3/4	14.4	16.0	31.2	34.7	64.8	72.0	140.4	156.0	280.8	312.0
9	4	256-QAM	5/6	15.9	17.7	-	-	71.71	79.7	155.4	172.6	310.8	345.3

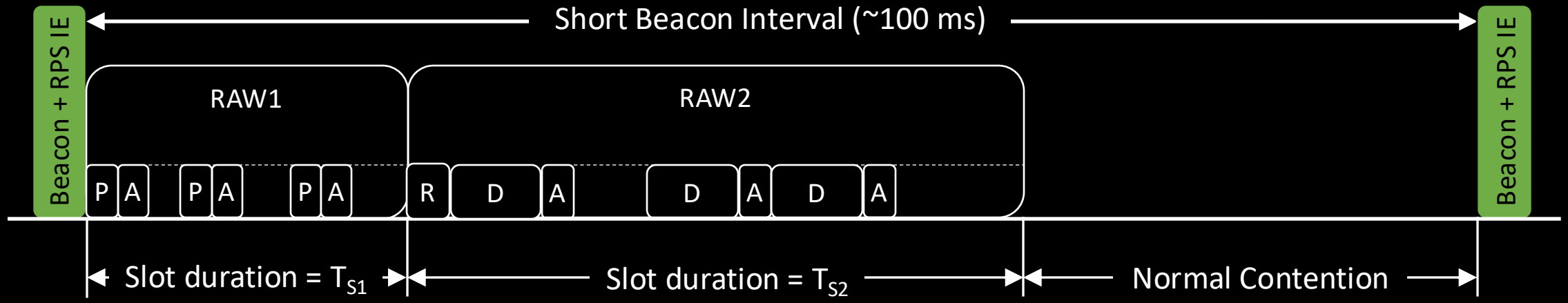
Association ID (AID)

Bits 0–13	Bit 14	Bit 15	Usage
0–32 767		0	Duration value (in microseconds) within all frames except PS-Poll frames that are not PS-Poll+BDT
0–16 383	0	1	Reserved
0	1	1	AID 0 is used for broadcast transmission in S1G PPDU, reserved if not in S1G PPDU.
1–2007	1	1	AID in PS-Poll frames other than PS-Poll+BDT.
2008–8191	1	1	Additional AIDs in S1G PS-Poll frames other than PS-Poll+BDT. Reserved if not in S1G PS-Poll frames.
8192–16 383	1	1	Reserved

Duration / ID Field



Restricted Access Window (RAW)



P: PS-Poll/Trigger frame, **D**: DATA, **A**: ACK, R: Resource Allocation

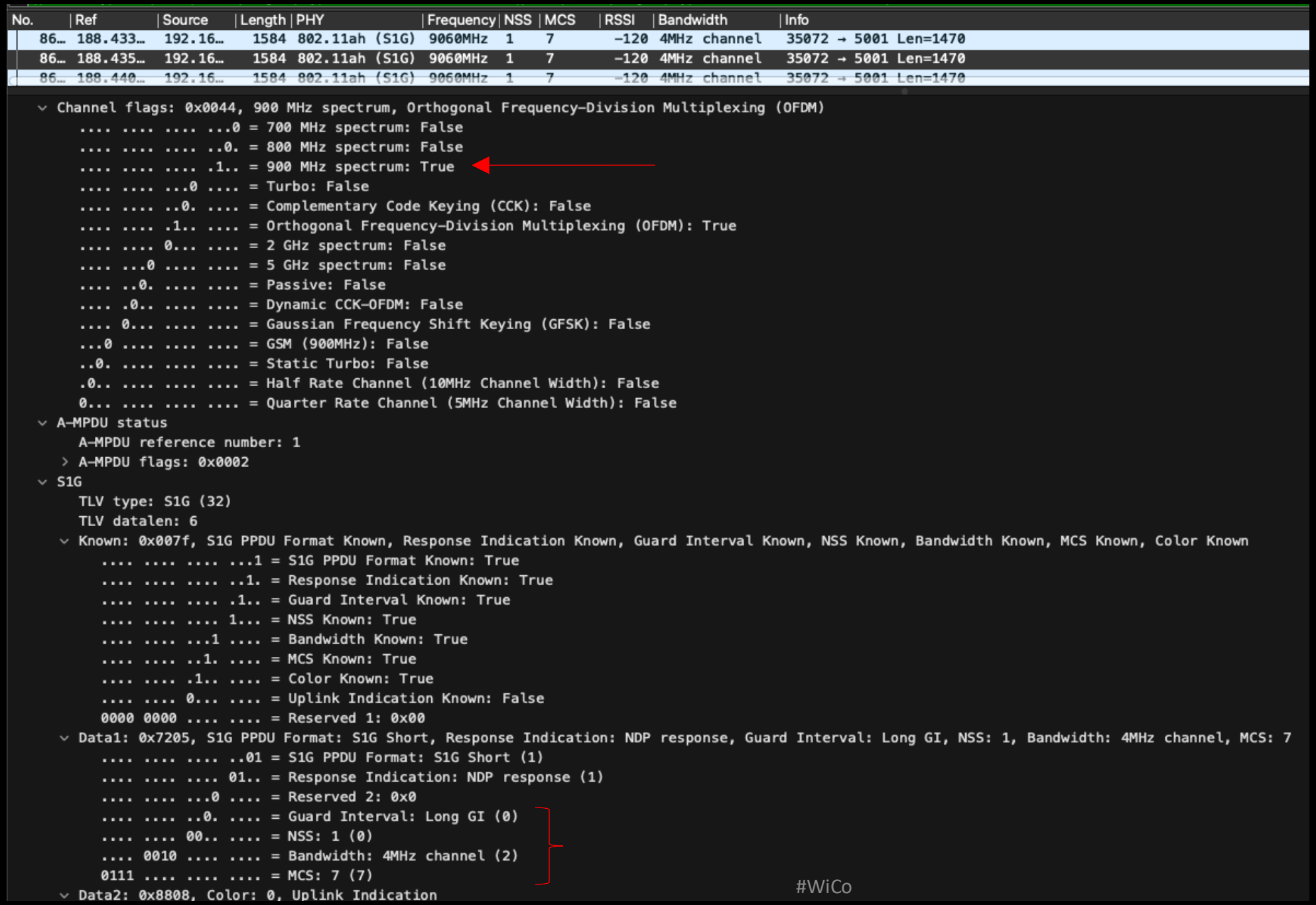
Trust measurements you make…

Obligatory HaLow Speed Test

Scenario	1 MHz (ch5)	2 MHz (ch6)	4 MHz (ch8)
Open	1.98	3.14	5.24
WPA3	1.56	2.85	4.93
UDP	2.01	3.97	5.04
2 STAs	1.20	1.97	2.93

WPA3 Support

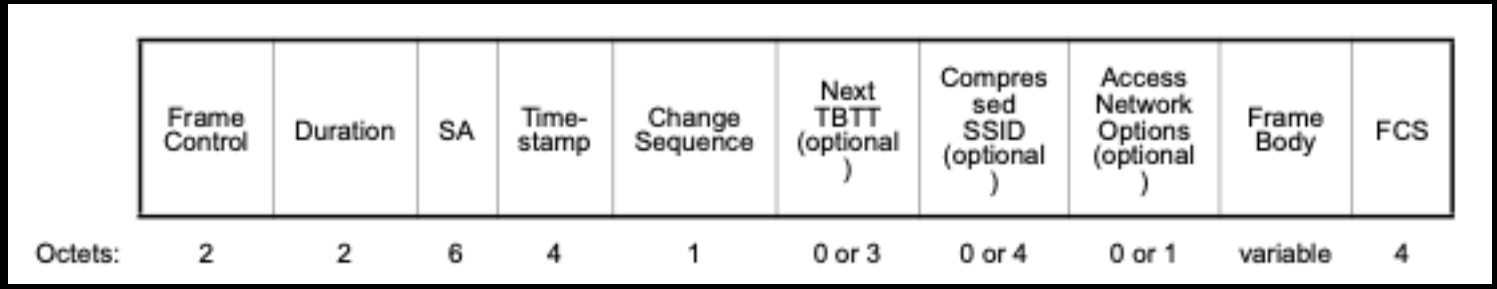
1 Spatial Stream (N_{ss} = 1)
2 STAs used UDP
Open/WPA3 used TCP
Uncontrolled environment
Results in Mbps



One packet slice from the packet blasting experiment!

Beacon details – S1G

- 2 types of beacons
  - Short beacon (transmitted ~100 TUs)
    - Compressed SSID, RPS
    - Reduce airtime consumption (beacon bloat)
  - Full beacon (transmitted ~1000 TUs)
    - QoS/WMM, Full/short beacon interval times, uncompressed SSID, and many other super exciting IEs for PCAP geeks



	Frame Control	Duration	SA	Time-stamp	Change Sequence	Next TBTT (optional)	Compressed SSID (optional)	Access Network Options (optional)	Frame Body	FCS
Octets:	2	2	6	4	1	0 or 3	0 or 4	0 or 1	variable	4

S1G Beacon Format

Beacons

Ref	Source	Length	PHY type	Frequency	NSS	MCS	Info
REF	Alfa_b…	140	802.11ah (S1G)	9045MHz	1	10	S1G Beacon, Flags=....R...C, SSID="WiFiVitae-HeyOh"
0.096395	Alfa_b…	65	802.11ah (S1G)	9045MHz	1	10	S1G Beacon, Flags=....R.FTC
0.198793	Alfa_b…	65	802.11ah (S1G)	9045MHz	1	10	S1G Beacon, Flags=....R.FTC
0.403620	Alfa_b…	65	802.11ah (S1G)	9045MHz	1	10	S1G Beacon, Flags=....R.FTC
0.505994	Alfa_b…	65	802.11ah (S1G)	9045MHz	1	10	S1G Beacon, Flags=....R.FTC
0.608415	Alfa_b…	65	802.11ah (S1G)	9045MHz	1	10	S1G Beacon, Flags=....R.FTC
0.710839	Alfa_b…	65	802.11ah (S1G)	9045MHz	1	10	S1G Beacon, Flags=....R.FTC
0.813242	Alfa_b…	65	802.11ah (S1G)	9045MHz	1	10	S1G Beacon, Flags=....R.FTC
0.915643	Alfa_b…	65	802.11ah (S1G)	9045MHz	1	10	S1G Beacon, Flags=....R.FTC
1.022443	Alfa_b…	140	802.11ah (S1G)	9045MHz	1	10	S1G Beacon, Flags=....R...C, SSID="WiFiVitae-HeyOh"

Short Beacon

"Full" Beacon

```
3.680478  Alfa_b…     65 802.11ah (S1G) 9045MHz  1    10   S1G Beacon, Flags=....R.FTC
v IEEE 802.11 S1G Beacon, Flags: ....R.FTC
    Type/Subtype: S1G Beacon (0x0031)
  v Frame Control Field: 0x1c0b
      .... ..00 = Version: 0
      .... 11.. = Type: Extension frame (3)
      0001 .... = Subtype: 1
      .... ...1 = Next TBTT Present: Present
      .... ..1. = Compressed SSID Present: Present
      .... .0.. = ANO Present: Not Present
      ..00 1... = BSS BW: 1
      .0.. .... = Security: Not supported
      0... .... = AP PM: Not supported
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Alfa_b4:74:7d (00:c0:ca:b4:74:7d)
    Source address: Alfa_b4:74:7d (00:c0:ca:b4:74:7d)
    Frame check sequence: 0x7644c14f [unverified]
    [FCS Status: Unverified]
    [WLAN Flags: ....R.FTC]
v IEEE 802.11 wireless LAN extension frame
  v Fixed parameters (12 bytes)
      Timestamp: 0x5863a0a8
      Change Sequence: 0
      Next TBTT: 0x586b70
      Compressed SSID: 0x2dcb0204
  v Tagged parameters (5 bytes)
    v Tag: Traffic Indication Map (TIM): DTIM 0 of 2 bitmap
        Tag Number: Traffic Indication Map (TIM) (5)
        Tag length: 3
        DTIM count: 0
        DTIM period: 2
      > Bitmap Control: 0x3e
```

```
No.     Source   Length Frequency NSS MCS  RSSI  Bandw Info
    19  Alfa_b…   140  9055MHz  1   10     29  1MH…  S1G Beacon, Flags=....R...C, SSID="WiFiVitae-HeyOh"
    v Bitmap Control: 0x3e
        .... ...0 = Traffic Indication: 0x0
        ..11 111. = Page Slice Number: 31
        00.. .... = Page Index: 0
  v Tag: S1G Capabilities
      Tag Number: S1G Capabilities (217)
      Tag length: 15
    v S1G Capabilities Information
      > S1G Capabilities
      v Supported S1G-MCS and NSS Set
        v Supported S1G-MCS and NSS Set: 0x0001fa00fd
            .... .... .... .... .... .... .... .... 1111 1101 = Rx S1G-MCS Map: 0xfd
            .... .... .... .... .... ...0 0000 0000 .... .... = Rx Highest Supported Long GI Data Rate: 0x000
            .... .... .... ...1 1111 101. .... .... .... .... = Tx S1G-MCS Map: 0xfd
            .... ..00 0000 000. .... .... .... .... .... .... = Tx Highest Supported Long GI Data Rate: 0x000
            .... 00.. .... .... .... .... .... .... .... .... = Rx Single Spatial Stream and S1G-MCS Map for 1MHz: 0x0
            ..00 .... .... .... .... .... .... .... .... .... = Tx Single Spatial Stream and S1G-MCS Map for 1MHz: 0x0
            00.. .... .... .... .... .... .... .... .... .... = Reserved: 0x0
  v Tag: S1G Operation
      Tag Number: S1G Operation (232)
      Tag length: 6
    v S1G Operation Information
      > Channel Width: 39: 4 MHz BSS operating channel width
        Operating Class: 2
        Primary Channel Number: 7
        Channel Center Frequency: 8
        Basic S1G-MCS and NSS Set: 0xccc4
  v Tag: Short Beacon Interval
      Tag Number: Short Beacon Interval (214)
      Tag length: 2
      Short Beacon Interval: 100
  v Tag: SSID parameter set: "WiFiVitae-HeyOh"
      Tag Number: SSID parameter set (0)
      Tag length: 15
      SSID: "WiFiVitae-HeyOh"
  v Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
      Tag Number: Vendor Specific (221)
      Tag length: 24
```

Security – WPA3™

Source	Destinatio	Length	PHY type	Frequency	NSS	MCS	Info
Alfa_b…	Raspbe…	186	802.11ah (S1G)	9050MHz	1	7	QoS Data, SN=791, FN=0, Flags=.p....FTC
Alfa_b…	Broadc…	494	802.11ah (S1G)	9050MHz	1	7	QoS Data, SN=1048, FN=0, Flags=.p....FTC
Alfa_b…	Alfa_b…	166	802.11ah (S1G)	9045MHz	1	10	Authentication, SN=0, FN=0, Flags=........C
Alfa_b…	Alfa_b…	166	802.11ah (S1G)	9045MHz	1	10	Authentication, SN=1105, FN=0, Flags=........C
Alfa_b…	Alfa_b…	102	802.11ah (S1G)	9045MHz	1	10	Authentication, SN=1, FN=0, Flags=........C
Alfa_b…	Alfa_b…	102	802.11ah (S1G)	9045MHz	1	10	Authentication, SN=1106, FN=0, Flags=........C
Alfa_b…	Alfa_b…	140	802.11ah (S1G)	9045MHz	1	10	Association Request, SN=2, FN=0, Flags=........C, SSID="WiFiVitae-HeyOh"
Alfa_b…	Alfa_b…	148	802.11ah (S1G)	9045MHz	1	10	Association Response, SN=1107, FN=0, Flags=........C
Alfa_b…	Alfa_b…	193	802.11ah (S1G)	9045MHz	1	10	Key (Message 1 of 4)
Alfa_b…	Alfa_b…	199	802.11ah (S1G)	9045MHz	1	10	Key (Message 2 of 4)
Alfa_b…	Alfa_b…	259	802.11ah (S1G)	9045MHz	1	10	Key (Message 3 of 4)
Alfa_b…	Alfa_b…	171	802.11ah (S1G)	9045MHz	1	10	Key (Message 4 of 4)
Alfa_b…	Broadc…	100	802.11ah (S1G)	9050MHz	1	7	QoS Data, SN=1049, FN=0, Flags=.p....FTC

17… Alfa_b… Alfa_b… 193 802.11ah (S1G) 9045MHz 1 10 Key (Message 1 of 4)

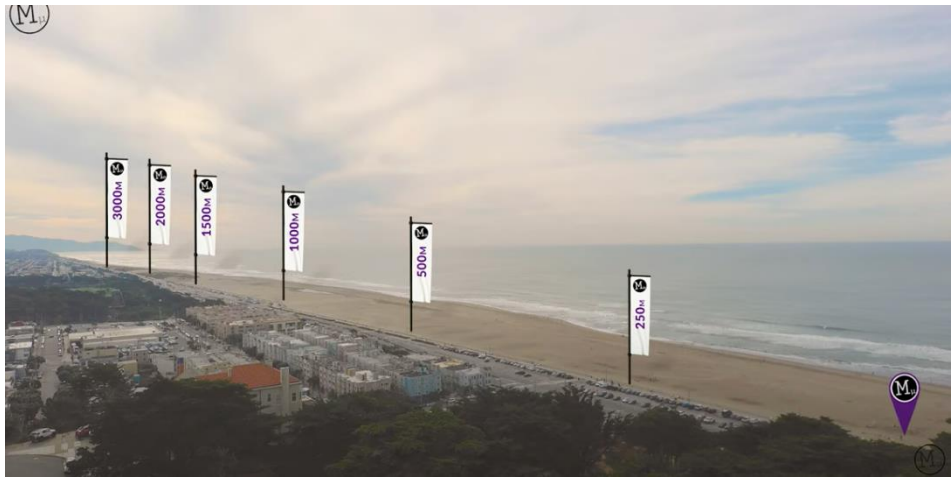
```
Organization Code: 00:00:00 (Officially Xerox, but
Type: 802.1X Authentication (0x888e)
802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 117
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 1]
  > Key Information: 0x0088
    Key Length: 16
    Replay Counter: 1
    WPA Key Nonce: ff01906f4292a6cb27f70cb19054c59bafae20e827355d2eaae06daf3ad8b2ec
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Data Length: 22
  v WPA Key Data: dd14000fac0437297f26c5e3be00af84092d66ad4209
    v Tag: Vendor Specific: Ieee 802.11: RSN PMKID
        Tag Number: Vendor Specific (221)
        Tag length: 20
        OUI: 00:0f:ac (Ieee 802.11)
        Vendor Specific OUI Type: 4
        Data Type: PMKID KDE (4)
        PMKID: 37297f26c5e3be00af84092d66ad4209
```

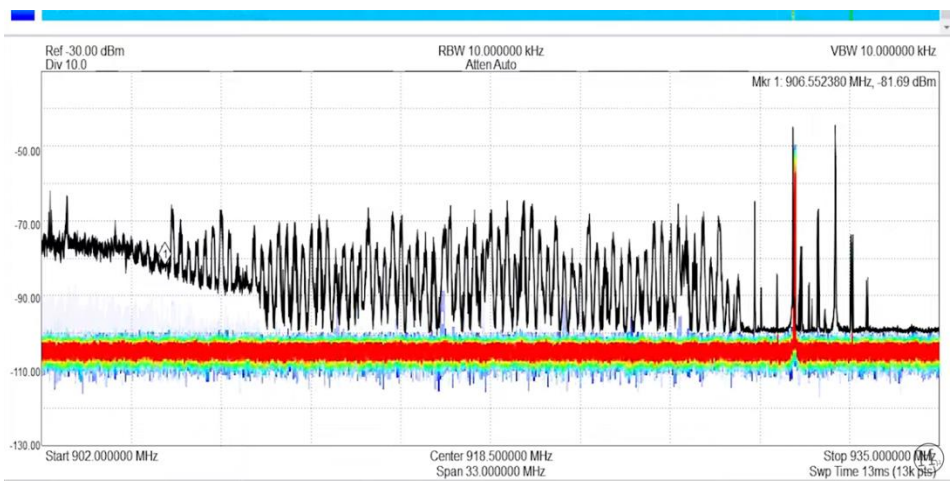
17… Alfa_b… Alfa_b… 199 802.11ah (S1G) 9045MHz 1 10 Key (Message 2 of 4)

```
802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 123
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 2]
  > Key Information: 0x0108
    Key Length: 0
    Replay Counter: 1
    WPA Key Nonce: e9af9dc0a1d06dcb2a2db4dab542ff76ac055e57d697ca55f8f08bf5d4efcb8e
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 51cae0a6e6337e253758d8ebc9b2f920
    WPA Key Data Length: 28
  v WPA Key Data: 301a0100000fac040100000fac040100000fac08c0000000000fac06
    v Tag: RSN Information
        Tag Number: RSN Information (48)
        Tag length: 26
        RSN Version: 1
      > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
        Pairwise Cipher Suite Count: 1
      > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
        Auth Key Management (AKM) Suite Count: 1
      > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) SAE (SHA256)
      > RSN Capabilities: 0x00c0
        PMKID Count: 0
        PMKID List
      > Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
```

HaLow Distance Record – 3 Km (1.86 mi)

- Using Morse Micro MM6108 SoC
- Ocean Beach, California
- Video call & TP test
- 8 MHz wide channel
- 8 Mbps @ 1500 m / 1 Mbps @ 3000 m





#WiCo

Source: Morse Micro 3Km Range Test - https://vimeo.com/900432058

HaLow

2 MHz Wide
Channel 6 (905MHz)
Ping
Open
Max Tx Power

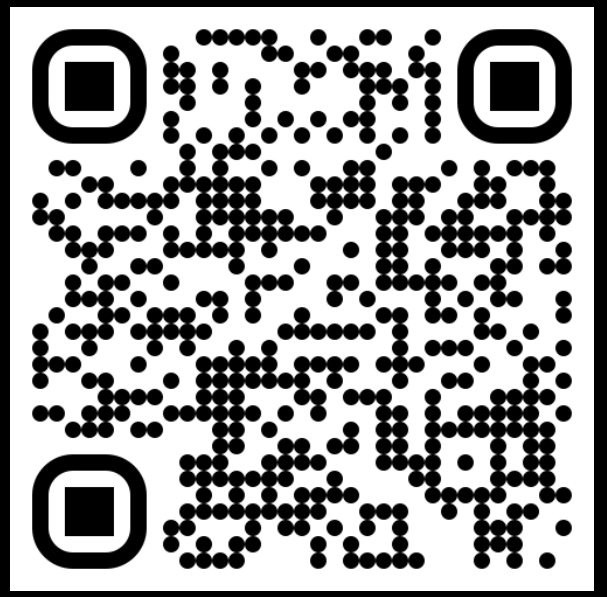
Wi-Fi 6

40 MHz Wide
Channel 144
Ping
WPA3
Tx Power: 17dBm

Attributes	Wi-Fi HaLow	Wi-Fi Legacy (n/ac)	Zigbee	BLE	LoRaWAN	NB-IoT
Frequency	S1G	2.4 / 5 GHz	S1G / 2.4 GHz	2.4 GHz	S1G / 2.4 GHz	Licensed <5 GHz
Data Rate	150 kbps – 86.7 Mbps*	6.5 Mbps– 866.7 Mbps*	250 kbps	125 kbps – 2 Mbps	300 bps – 27 kbps	20 – 127 kbps
Range (m)	<1,000	< 100	< 20	< 100	<20,000	<30,000
Modulation	OFDM over BPSK, QPSK, 16/64/256-QAM	OFDM over BPSK, QPSK, 16/64/256-QAM	BPAK / OQPSK	GFSK	CSS	QPSK
Power	Low	Med	Low	Low	Low	Low
Security	WPA3™	128-bit AES in CCMode	128-bit AES in CCMode	128-bit AES in CCMode	128-bit AES in CCMode	3GPP security
Device per AP/GW	8192	2007	65,000	Unlimited	>100,00	>100,000
OTA firmware updates	Yes	Yes	Yes	Yes	Yes	Yes

* Single spatial stream

“Be relentlessly curious.”



@troymart

Wi-Co
Wireless Community

#WiCo

Wi-Co
Wireless Community