Lecture 13
Cellular IoT & LPWAN Intro

CS397/497 – Wireless Protocols for IoT

Branden Ghena – Spring 2022

Materials in collaboration
with Pat Pannuto (UCSD)

Northwestern

Today’s Goals

- Understand how modern “Cellular for IoT” fit in to the existing cellular infrastructure, and what they do at a technical level to suit IoT needs

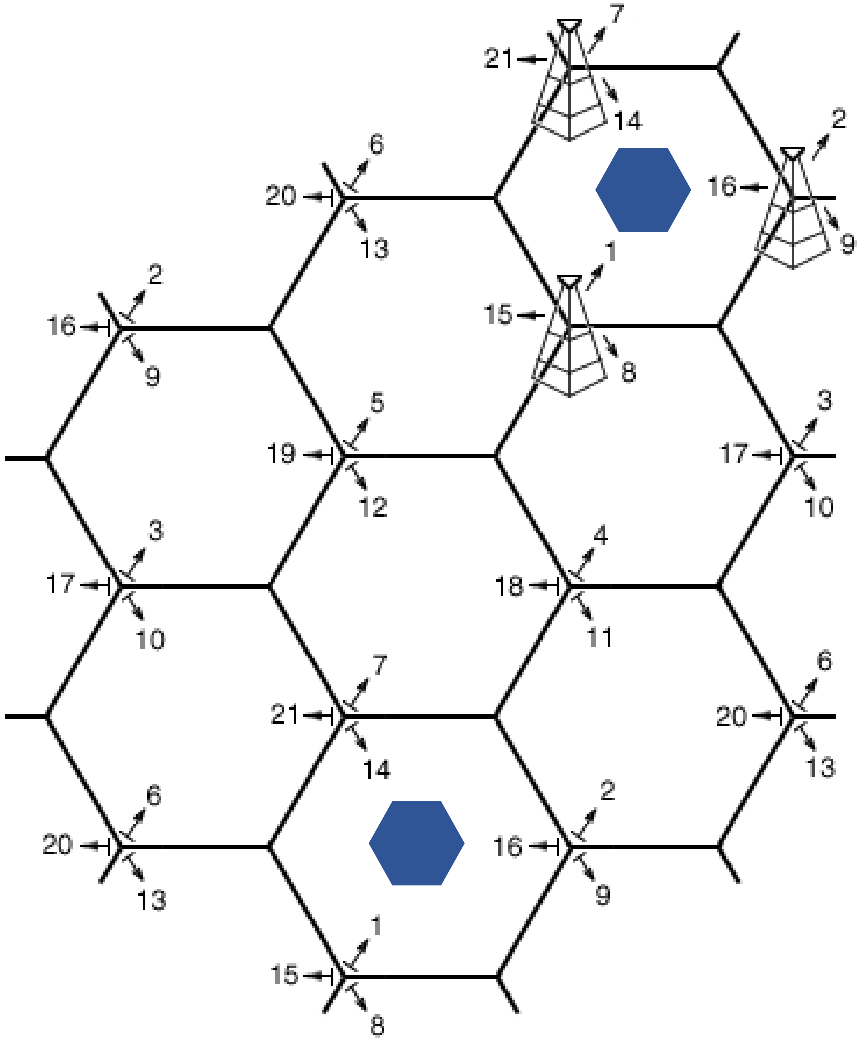
- Apply knowledge from the course to understand LPWAN design

- Overview of unlicensed-band LPWANs
  - LoRaWAN

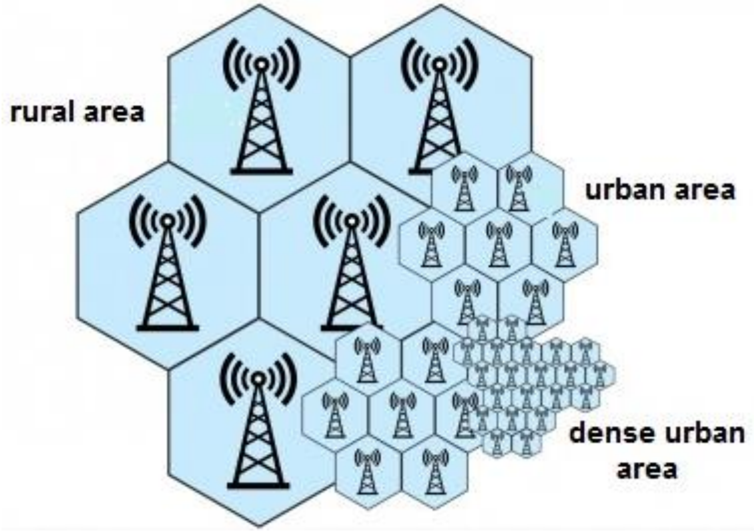
Outline

- **Cellular IoT**
- LPWAN Design
- LoRaWAN

Reminder: the **cell** in cellular technologies



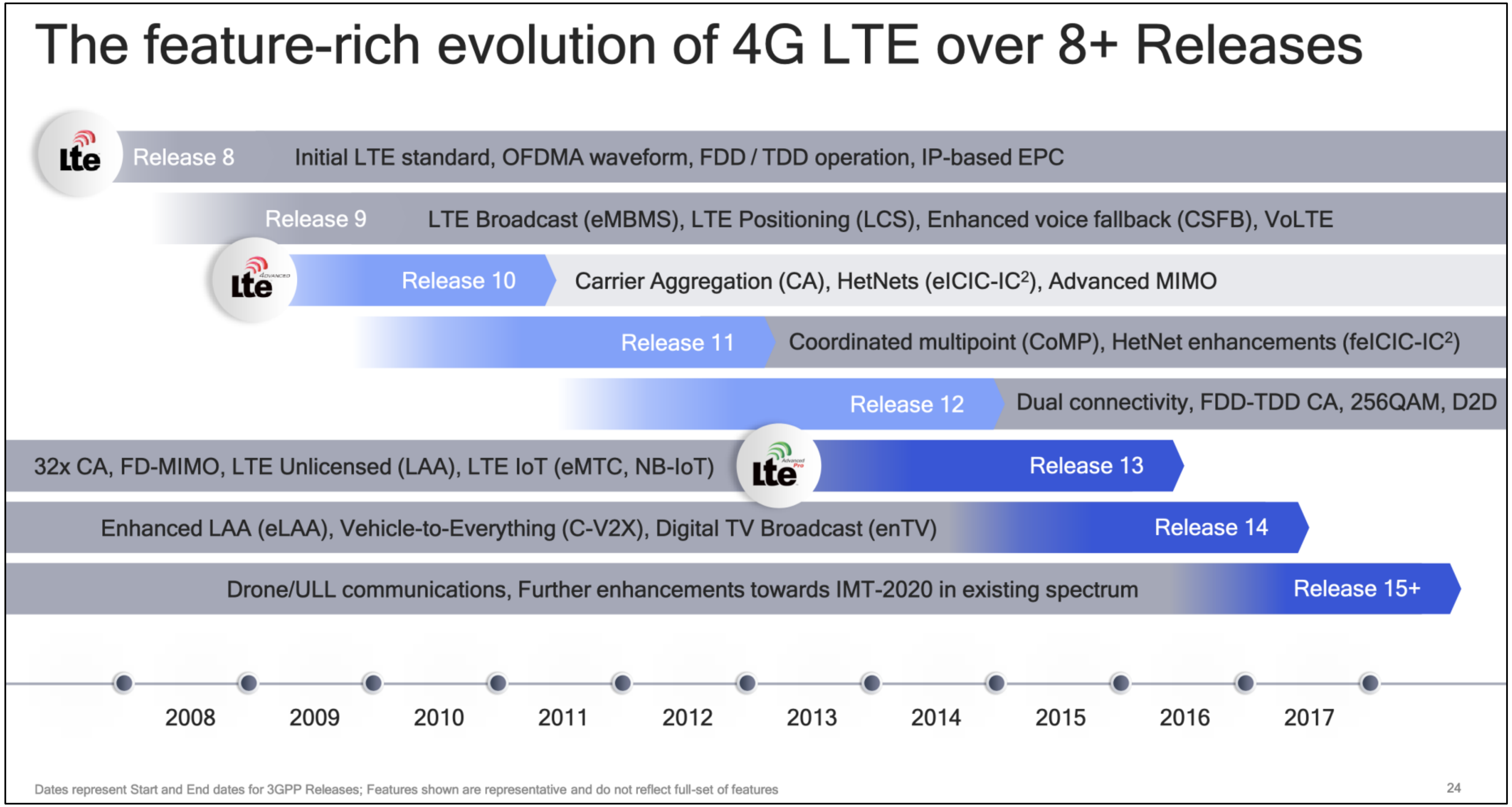
- Place towers at corners of cells
  - Directional antennas send three different frequency bands, one per cell
  - Each cell gets three tower and three bands
- Density of cells varies based on expected number of users
  - Change cell size using Power Control



3GPP
aka: the actual answer for what stuff is really doing

- 3rd Generation Partnership Project (3GPP)
- Industry alliance for development of telecoms standards
  - Established around 1998
  - Makes “Releases” which are roughly analogous to IEEE standards/versions
    - Release 8 (2008) LTE ~4G
    - Release 15 (2018) NR (New Radio) ~5G
- Focused on the practical
  - ITU post-hoc defined “4G”, 3GPP defined LTE and LTE_________

Mapping "4G", "LTE", "LTE Advanced", etc onto actual technologies



The feature-rich evolution of 4G LTE over 8+ Releases

Release 8 Initial LTE standard, OFDMA waveform, FDD / TDD operation, IP-based EPC

Release 9 LTE Broadcast (eMBMS), LTE Positioning (LCS), Enhanced voice fallback (CSFB), VoLTE

Release 10 Carrier Aggregation (CA), HetNets (eICIC-IC^2), Advanced MIMO

Release 11 Coordinated multipoint (CoMP), HetNet enhancements (feICIC-IC^2)

Release 12 Dual connectivity, FDD-TDD CA, 256QAM, D2D

32x CA, FD-MIMO, LTE Unlicensed (LAA), LTE IoT (eMTC, NB-IoT) Release 13

Enhanced LAA (eLAA), Vehicle-to-Everything (C-V2X), Digital TV Broadcast (enTV) Release 14

Drone/ULL communications, Further enhancements towards IMT-2020 in existing spectrum Release 15+

Dates represent Start and End dates for 3GPP Releases; Features shown are representative and do not reflect full-set of features

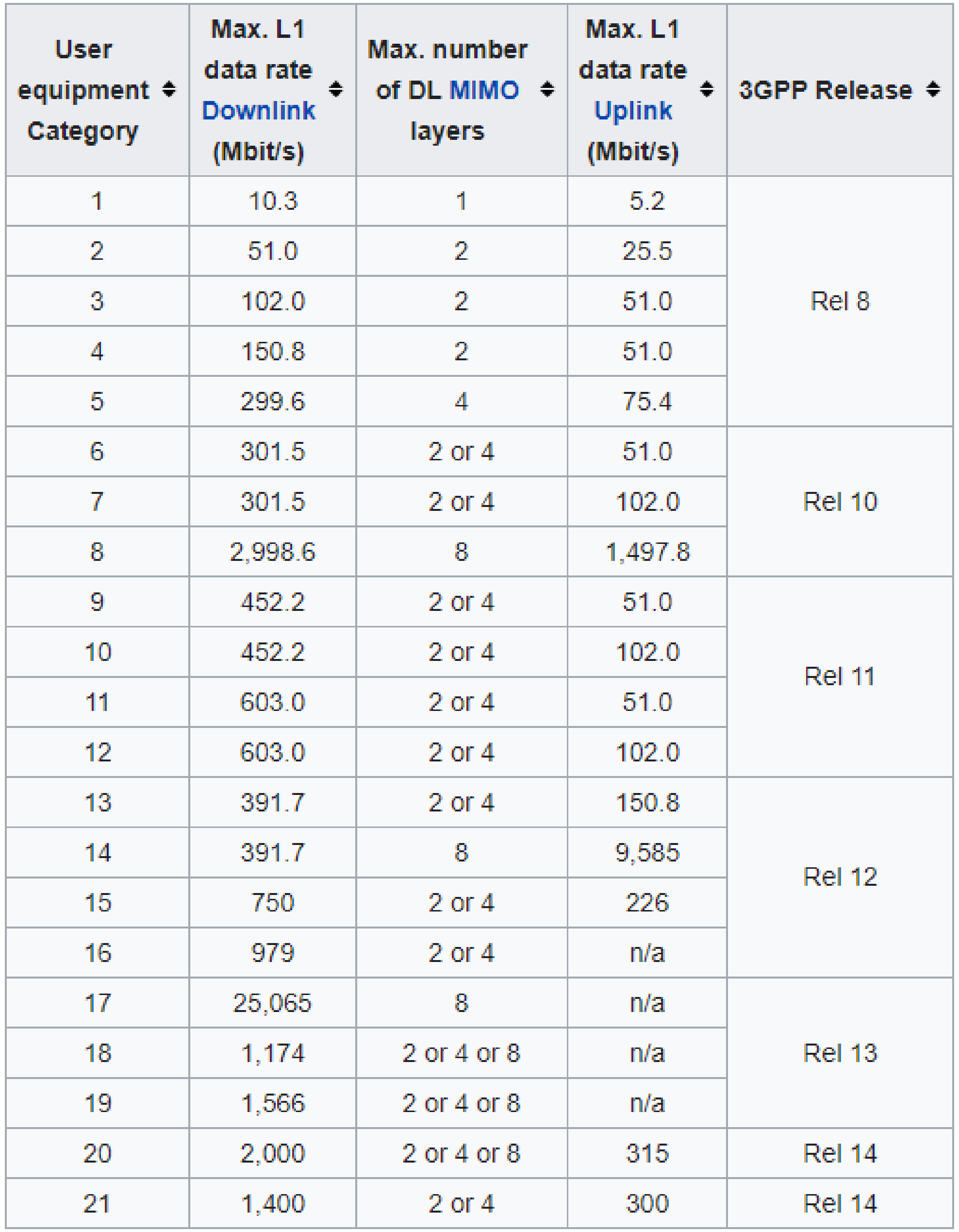
This Qualcomm presentation is great: https://www.qualcomm.com/media/documents/files/demystifying-3gpp-and-the-essential-role-of-qualcomm-in-leading-the-expansion-of-the-mobile-ecosystem.pdf

LTE Categories

- Different equipment supports different “categories” of LTE
  - Maximum MCS index supported

- Examples
  - iPhone 6 (2015): Cat 4
  - Pixel 3 (2018): Cat 16

- Aside: Hey look, *some* LTE is ”ITU 4G”!



User equipment Category	Max. L1 data rate Downlink (Mbit/s)	Max. number of DL MIMO layers	Max. L1 data rate Uplink (Mbit/s)	3GPP Release
1	10.3	1	5.2	Rel 8
2	51.0	2	25.5	
3	102.0	2	51.0	
4	150.8	2	51.0	
5	299.6	4	75.4	
6	301.5	2 or 4	51.0	Rel 10
7	301.5	2 or 4	102.0	
8	2,998.6	8	1,497.8	
9	452.2	2 or 4	51.0	Rel 11
10	452.2	2 or 4	102.0	
11	603.0	2 or 4	51.0	
12	603.0	2 or 4	102.0	
13	391.7	2 or 4	150.8	Rel 12
14	391.7	8	9,585	
15	750	2 or 4	226	
16	979	2 or 4	n/a	
17	25,065	8	n/a	Rel 13
18	1,174	2 or 4 or 8	n/a	
19	1,566	2 or 4 or 8	n/a	
20	2,000	2 or 4 or 8	315	Rel 14
21	1,400	2 or 4	300	Rel 14

Additional low-end categories for IoT

- LTE Cat 0
  - Traditional LTE, but focused on the really low end

- LTE-M (LTE Cat M1)
  - 375 kbps uplink, 300 kbps downlink (for the actually implemented mode)
  - Reduced power and maximum bandwidth
  - Increased range

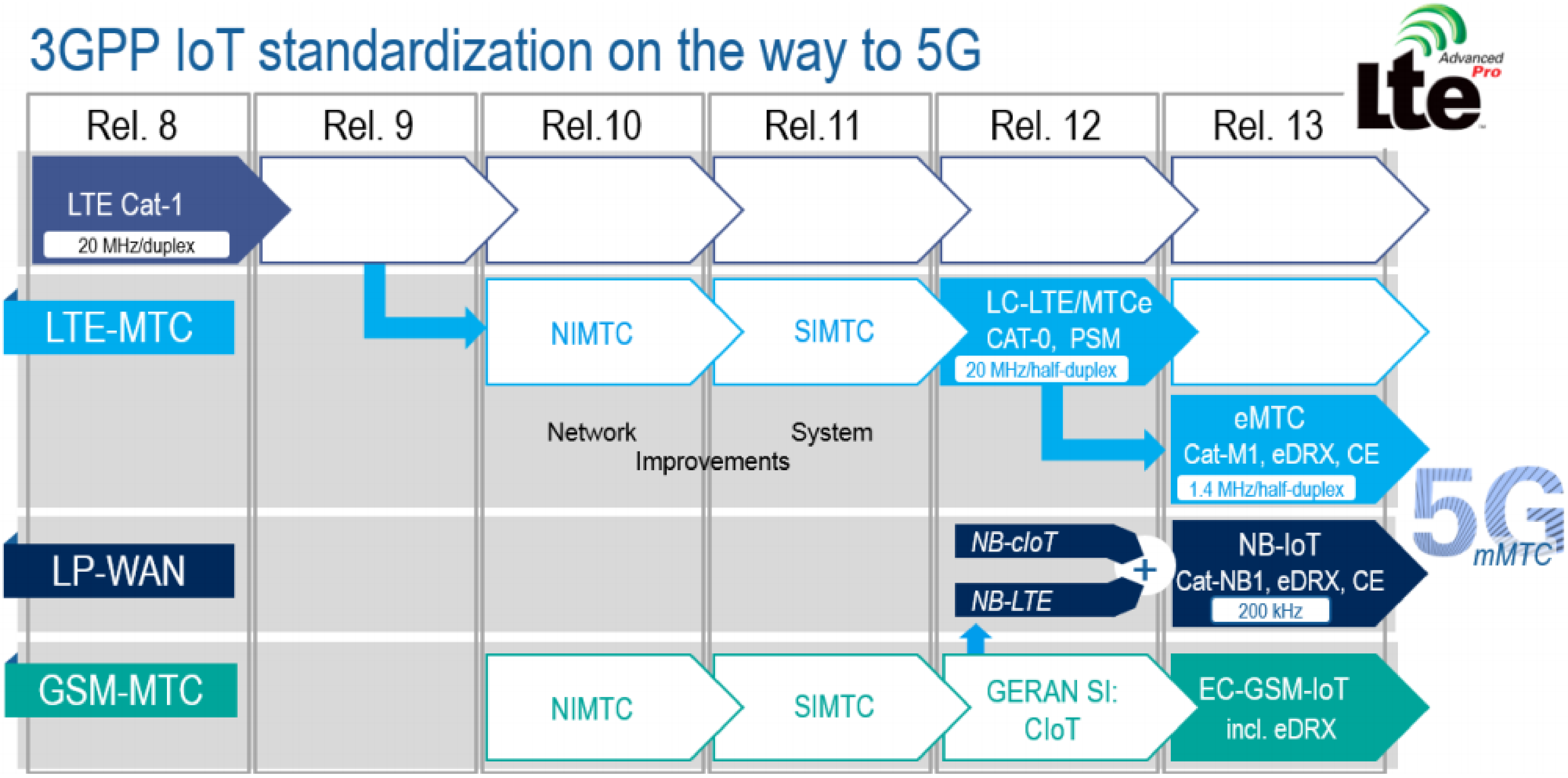
- NB-IoT (LTE Cat NB1)
  - 65 kbps uplink, 26 kbps downlink
  - Reduced power and greatly reduced bandwidth
  - Greatly increased range

Why do we need “special categories” for IoT on cell?

- Pragmatic for the end device
  - Lower power
  - Allow for long-off periods

- Pragmatic for network operators
  - *Allows for scale*– network no longer needs to assume that devices could always be on in each cell

LTE-M and NB-IoT were developed in parallel



3GPP IoT standardization on the way to 5G

Rel. 8
Rel. 9
Rel.10
Rel.11
Rel. 12
Rel. 13

LTE Cat-1
20 MHz/duplex

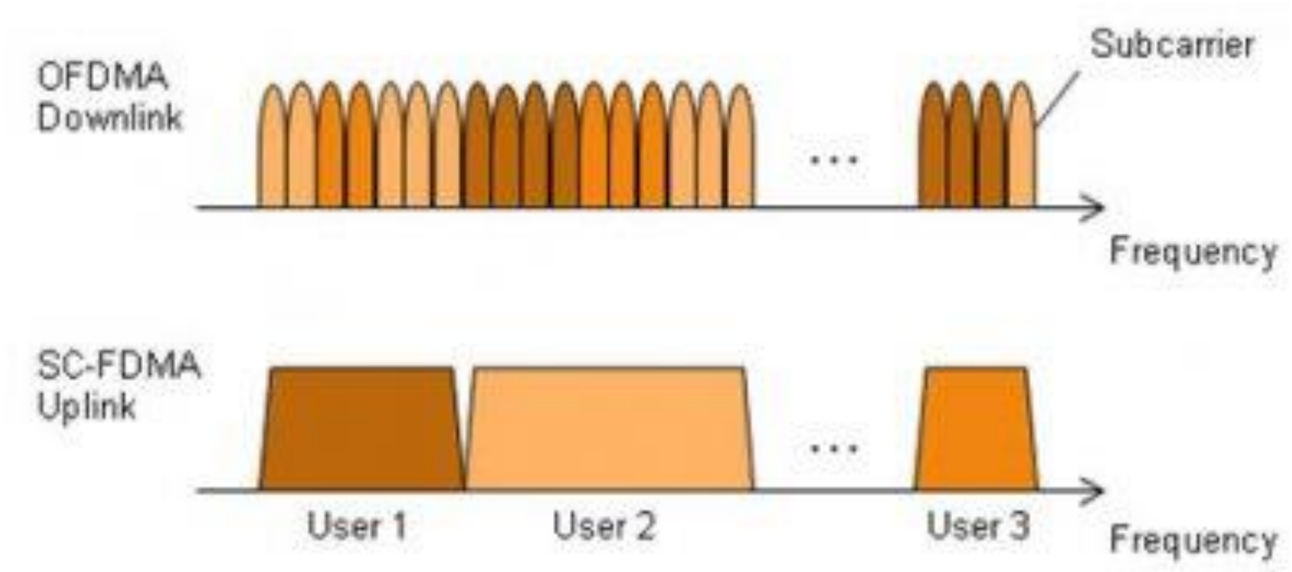
LTE-MTC
NIMTC
SIMTC
LC-LTE/MTCe
CAT-0, PSM
20 MHz/half-duplex
eMTC
Cat-M1, eDRX, CE
1.4 MHz/half-duplex

Network Improvements System

LP-WAN
NB-cIoT
NB-LTE
+
NB-IoT
Cat-NB1, eDRX, CE
200 kHz

GSM-MTC
NIMTC
SIMTC
GERAN SI:
CIoT
EC-GSM-IoT
incl. eDRX

LTE-M and NB-IoT downlink and uplink

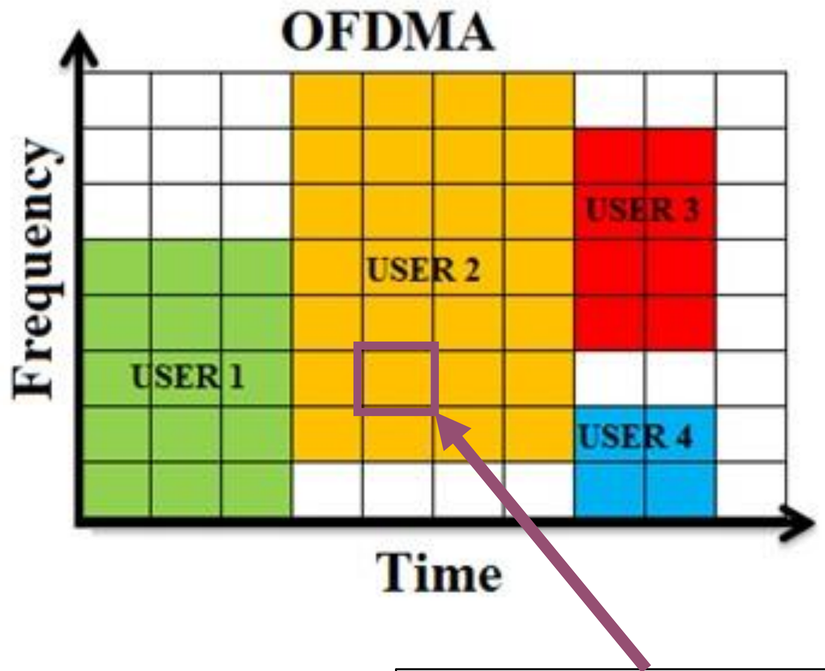


- OFDMA downlink
  - Put the more complicated hardware in the cell tower [simple FFT demodulator]

- SC-FDMA (single carrier FDMA) uplink
  - Blocks of subchannels combined into one signal
  - Similar concept, but simpler for end devices to implement

LTE resource allocation

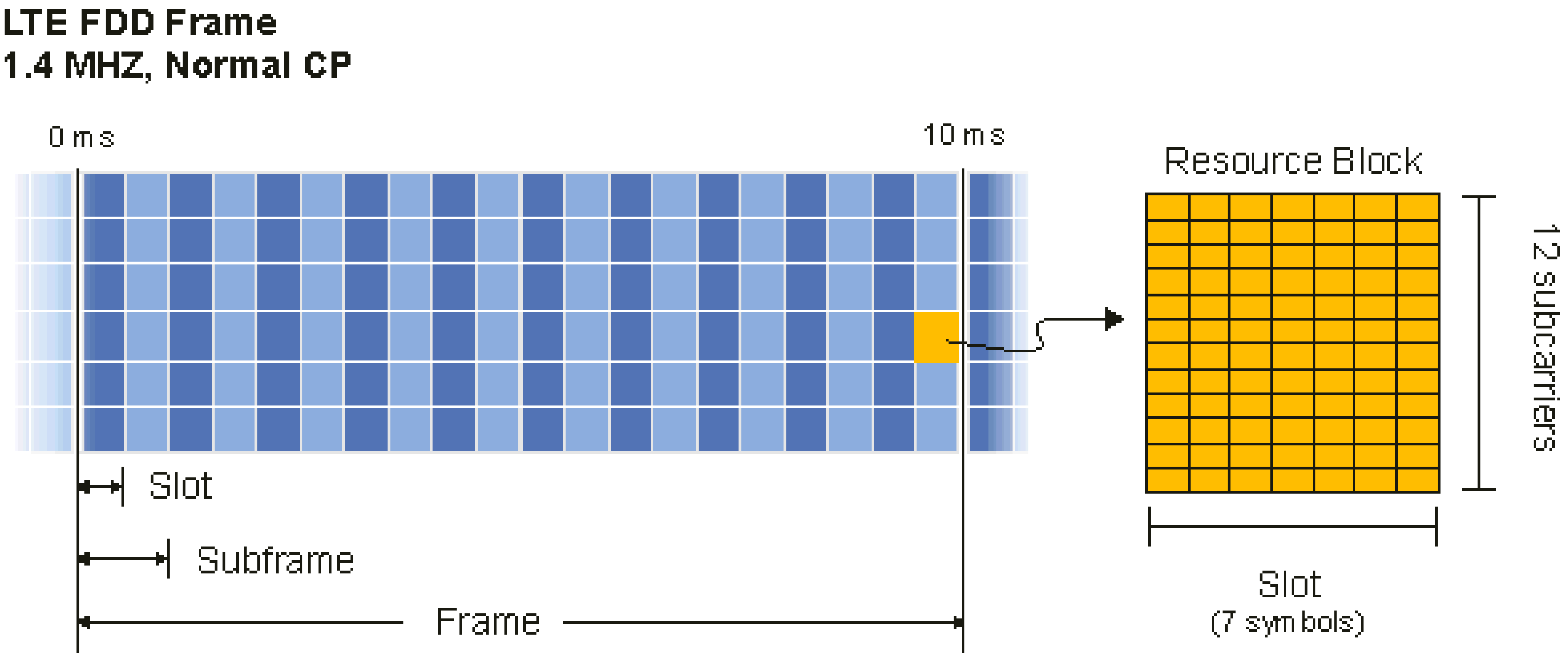
- Cellular uses OFDMA to schedule
  - Time + Frequency -> “2D Scheduling”
- Cellular uses single channels up to 20 MHz
  - Further divides these into 100 Resource Blocks
- Resource Block
  - 12 subcarriers for OFDM in frequency (15 kHz each)
  - 7 symbols in time (0.5 ms)
- Devices are allocated frequency and time based on what they are sending
  - Allocated in units of Resource Blocks



One “Resource Block”

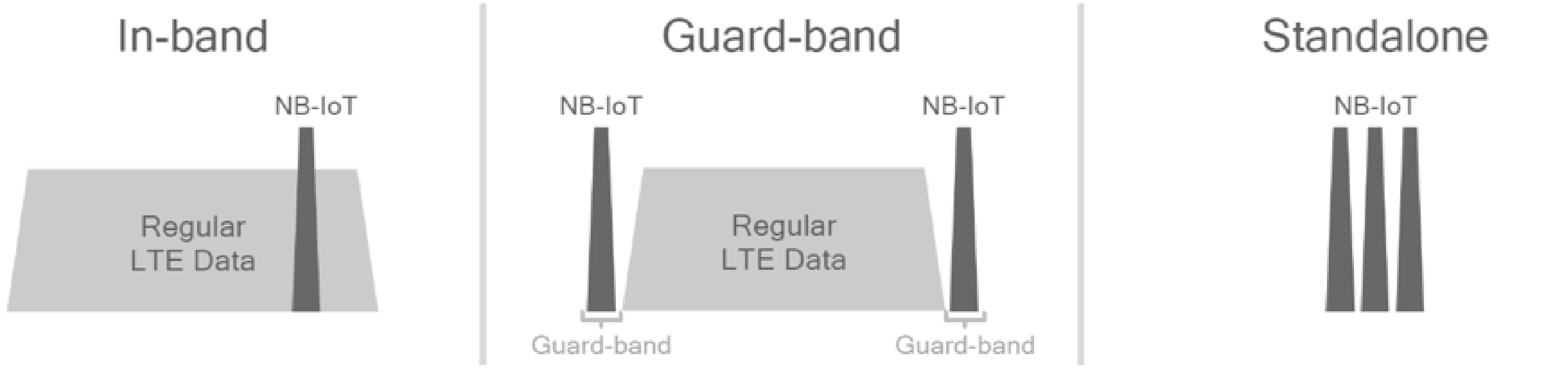
Resources used by LTE-M and NB-IoT

- LTE-M uses up to 6 resource blocks
  - 1.4 MHz of bandwidth (1.080 MHz)
  - Can co-exist with other normal LTE traffic, scheduled by cell tower
  - Limited to only some capability of LTE (**much** less throughput)



Resources used by LTE-M and NB-IoT

- NB-IoT uses up to 1 resource block
  - 200 kHz of bandwidth (180 kHz)
  - Multiple deployment options
    - Guard-band in practice



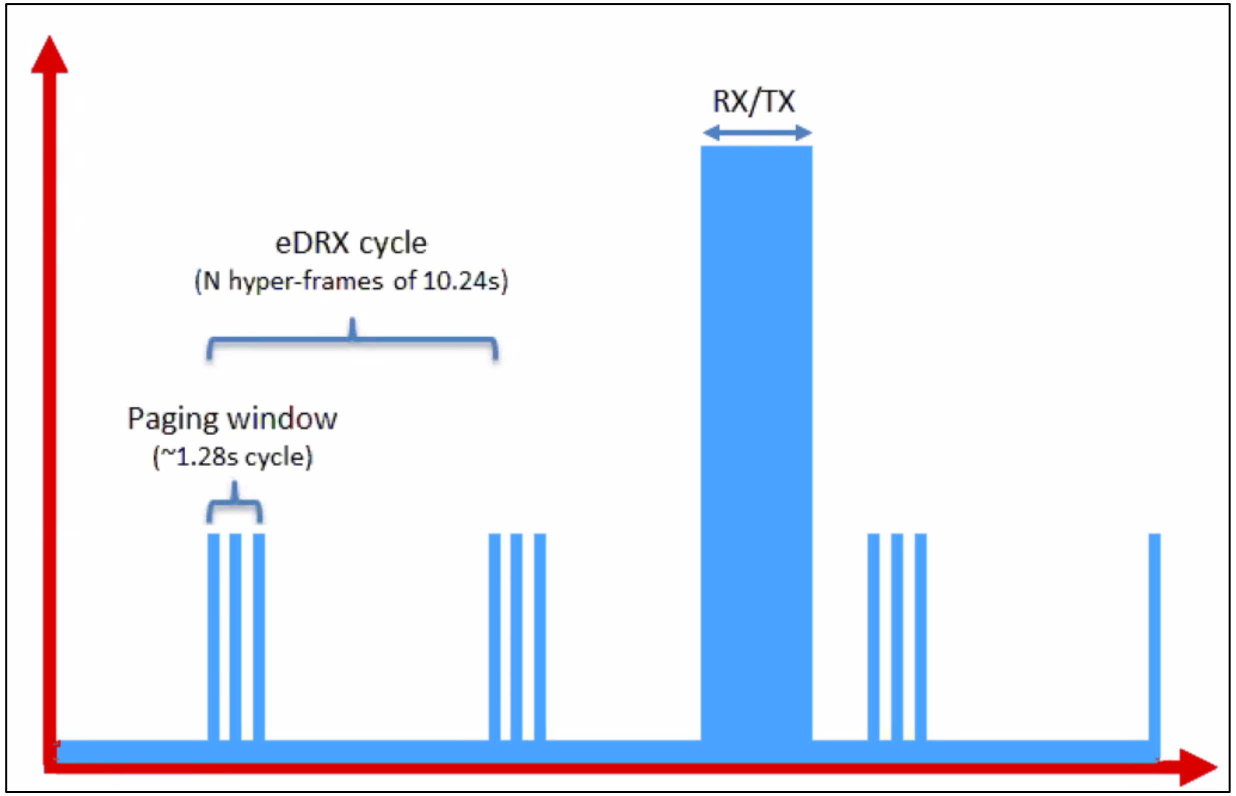
Utilizing single resource block (180kHz) within an LTE carrier

Utilizing unused resource blocks within an LTE carrier guard-band

Utilizing stand-alone 200 kHz carrier

Reducing power for IoT devices

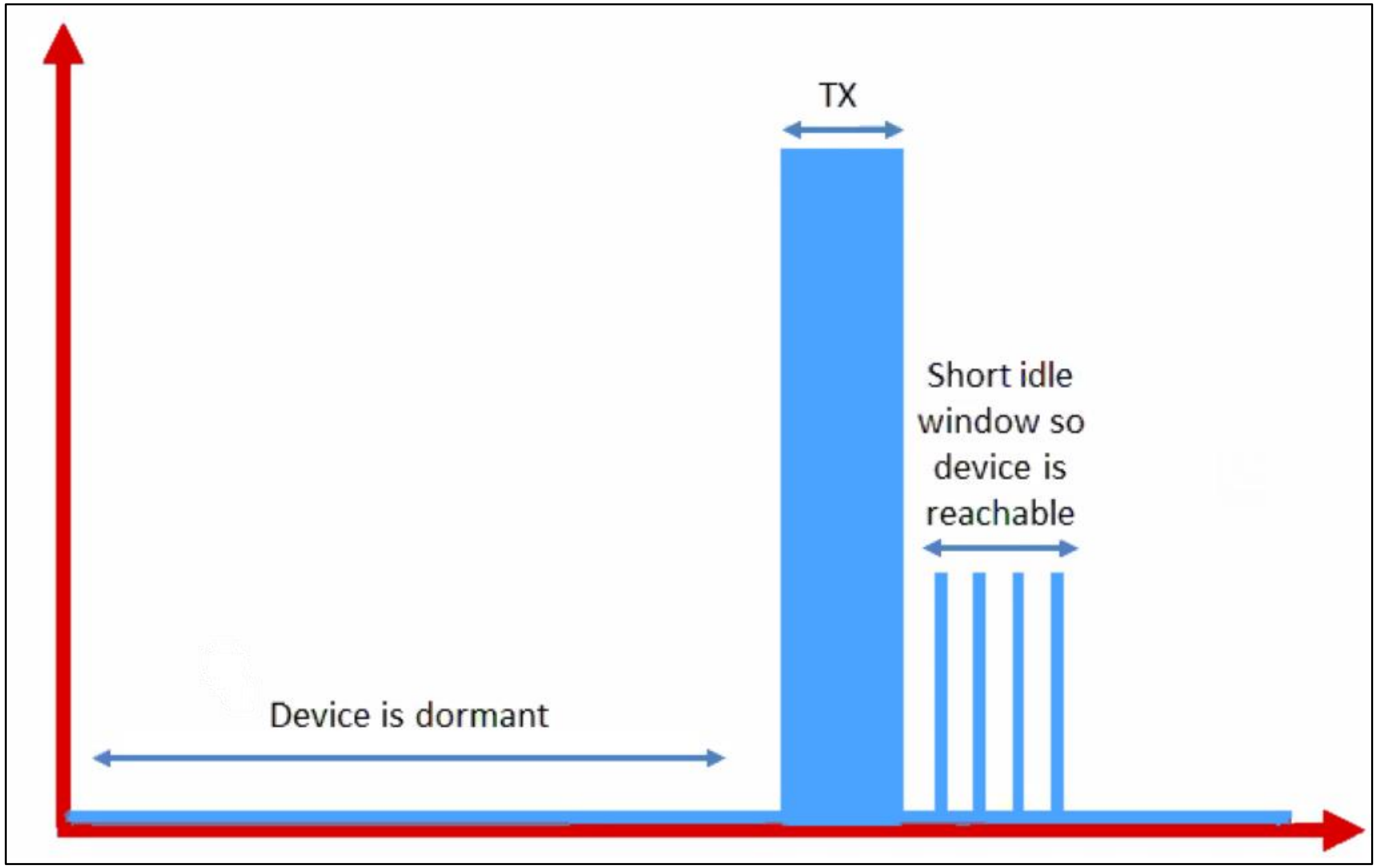
- Reduce max Tx power to 20 dBm
  - Increased receive sensitivity at tower will cover it
- Extended Discontinuous Reception (eDRX)
  - Allow devices to reduce paging period and still stay on network
  - Cell tower will hold messages
- What does this get to?
  - "For a LTE-M1 device that transmits data once per day, and wakes up every 60 hyper frames to check for commands (this would be about every 10 minutes), **a life of 4.7 years is achievable on 2 AA batteries**."



Graphics, quote from https://www.link-labs.com/blog/lte-e-drx-psm-explained-for-lte-m1

Further power reduction for simple devices

- Power Saving Mode (PSM)
  - For very simple, uplink-focused devices, allow them to turn off entirely but stay connected
  - Minutes to *days* in duration
  - Notify tower before sleeping, listen for packets after each transmission

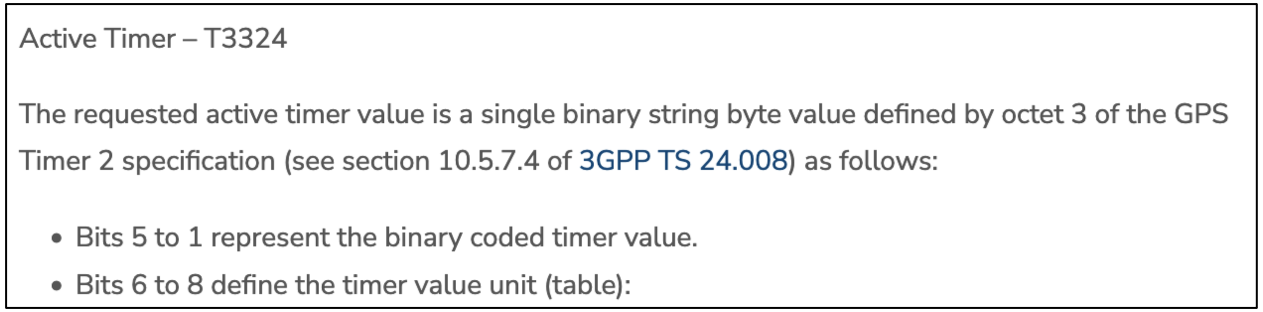


Graphics from https://www.link-labs.com/blog/lte-e-drx-psm-explained-for-lte-m1

Some numbers from an actual telecom: Aeris

[n.b. Aeris has been a leader in cellular M2M since the 90’s]

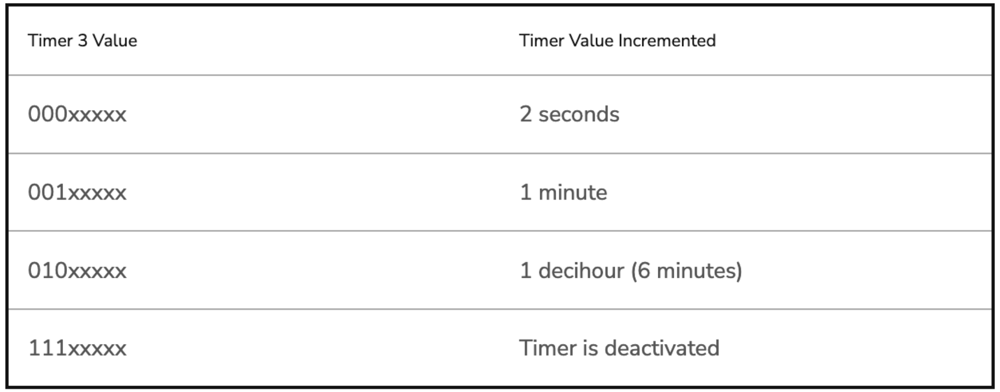
- PSM has two timers, devices *request* values, *tower chooses* actual:
  - Extended Timer (“sleep” timer)
    - 3GPP max is 35,712,00s [413.33 days]
    - Aeris timer range: Min 240m [4h]; Max 413 days
    - “Aeris Fusion” timer range: Max: 12.9 days
  - Active Timer (how long will the device stay in idle after communication?)



Active Timer – T3324

The requested active timer value is a single binary string byte value defined by octet 3 of the GPS Timer 2 specification (see section 10.5.7.4 of 3GPP TS 24.008) as follows:

- Bits 5 to 1 represent the binary coded timer value.
- Bits 6 to 8 define the timer value unit (table):



Timer 3 Value	Timer Value Incremented
000xxxxx	2 seconds
001xxxxx	1 minute
010xxxxx	1 decihour (6 minutes)
111xxxxx	Timer is deactivated

Numbers from https://aeriscom.zendesk.com/hc/en-us/articles/360049848254-Understanding-LTE-M-Power-Management-Modes

Improved range for LTE-M and NB-IoT

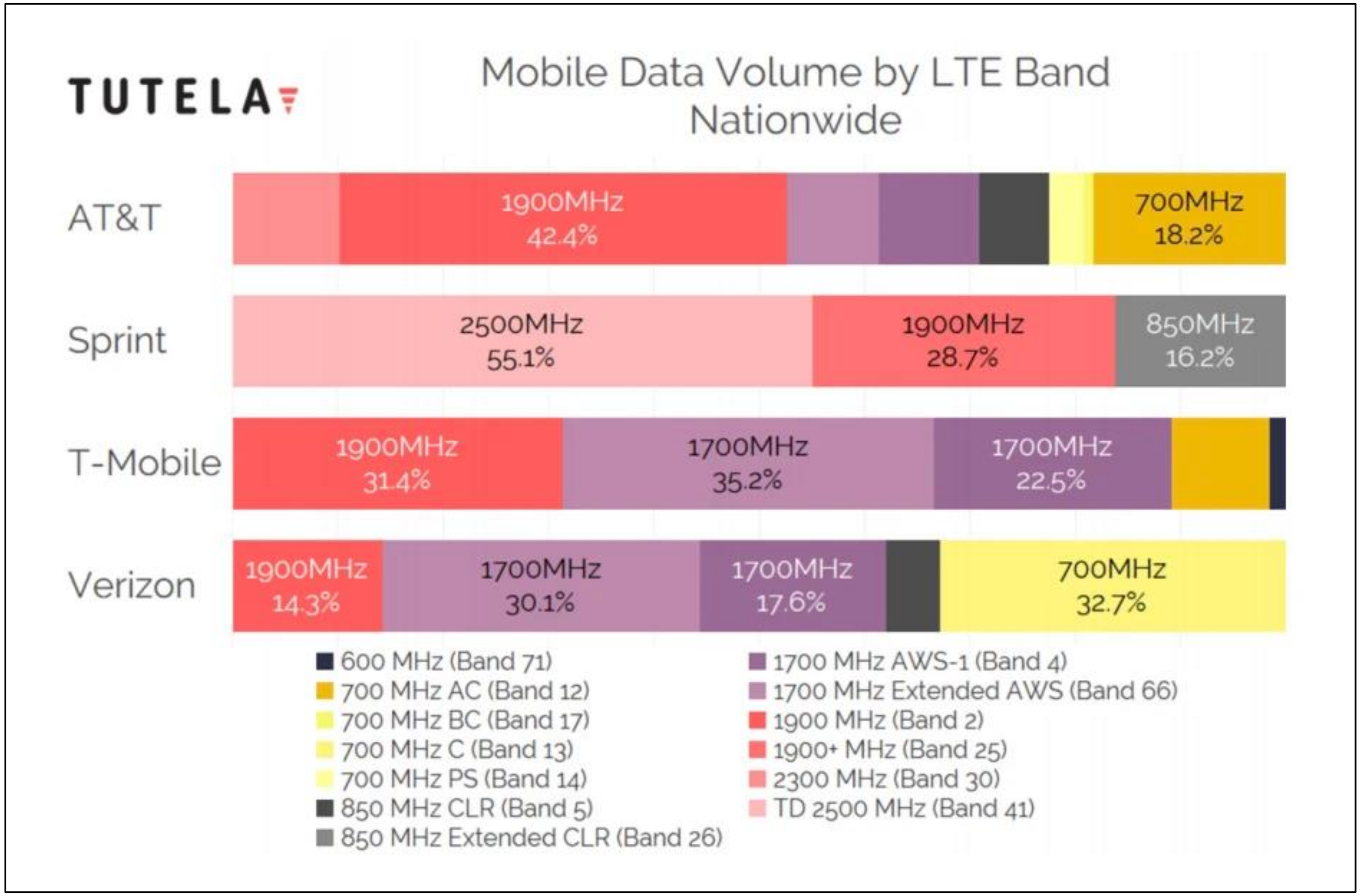
- LTE defines a Maximum Coupling Loss (MCL) a.k.a Link Budget
  - Traditional cellular: 144 dB (~2.5 km)
  - LTE-M: 160 dB (~5 km)
  - NB-IoT: 164 dB (~10 km)

  - Sigfox: ~155 dB
  - LoRaWAN: ~143 dB

- Note that many cellular bands are often on higher frequencies
  - Example: 1900 GHz

Coarsely, lower frequency -> longer range

- This was the picture circa 2019
- Why else might T-Mobile have *really* wanted to buy Sprint…



Cellular deployments

- Originally unclear which would be dominant
  - Verizon and AT&T focused on LTE-M
  - T-Mobile focused on NB-IoT
  - All rolled out services nationwide in the 2018-2019 timeframe

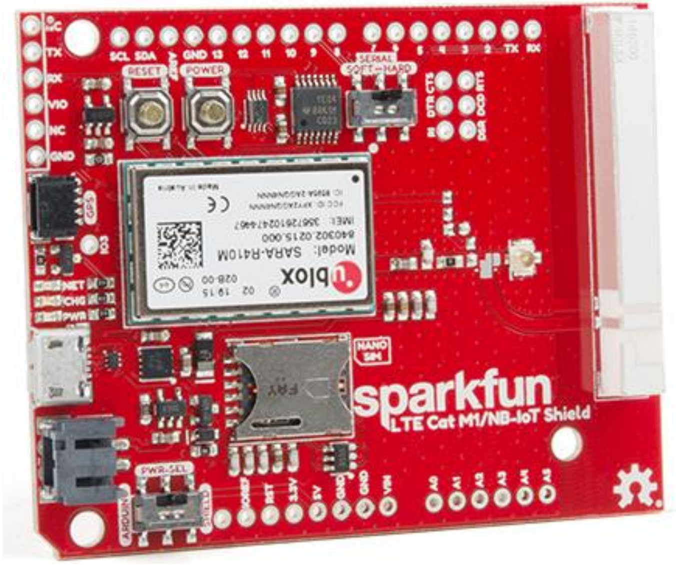
- Networks expanded provide both capabilities
  - LTE-M: AT&T, T-Mobile, Verizon, US Cellular
  - NB-IoT: AT&T, T-Mobile, Verizon

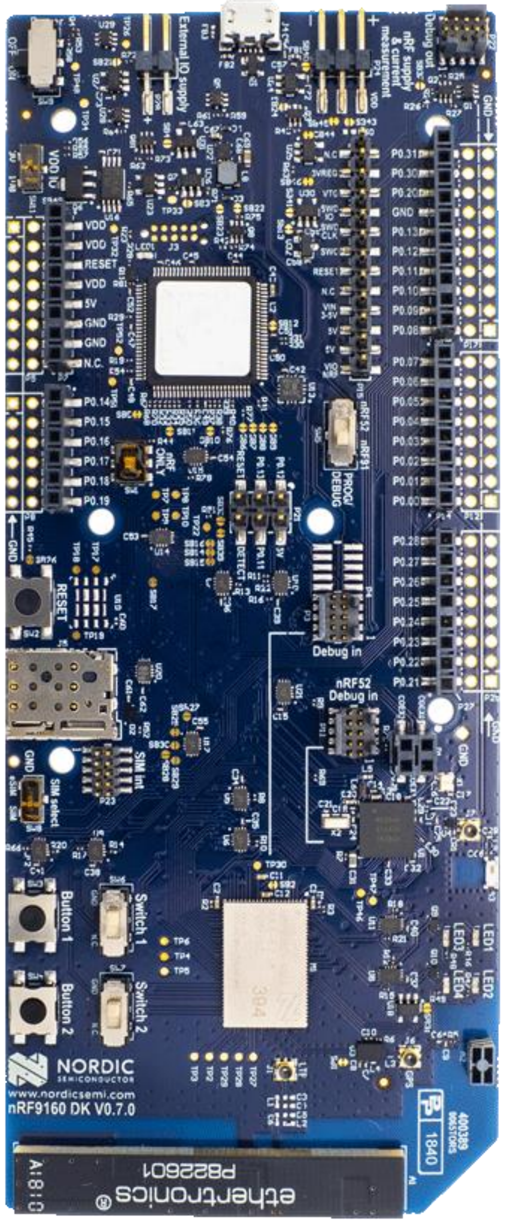
- Pricing models still very uncertain
  - NB-IoT example: $5 per device per year up to 12 MB, 10 packets per hour
  - Future adoption will greatly depend on these

Microcontroller support

- Devices need to be certified
  - Hardware and software
  - Tend to be modules or dual-core systems

- Add a SIM card to connect to network





Break + Open Question

- Cellular hardware almost always requires certified radio modules where you can’t change the code at all. Why?

Break + Open Question

- Cellular hardware almost always requires certified radio modules where you can’t change the code at all. Why?
  - Otherwise you could cheat at the protocols!!
  - Or just generally not follow them fairly.
  - Avoids “tragedy of the commons” by allowing specific trusted devices only

Outline

- Cellular IoT
- **LPWAN Design**
- LoRaWAN

LTE-M and NB-IoT design constrained by fitting within existing cellular ecosystem

- What might a fresh design look like?

- *Caveat:* In ISM bands!
  - So it’s a shared communication band

Design a wide-area network (ignore low-power for now)

- **What PHY choices would you make?**

Design a wide-area network (ignore low-power for now)

- **What PHY choices would you make?**
    - Modulation
    - Tx Power
    - Carrier Frequency Band
    - Data Throughput
    - Channel Bandwidth

Design a wide-area network (ignore low-power for now)

- **What PHY choices would you make?**
  - Modulation
    - Unclear. Can’t be too crazy for cheap devices.
  - Tx Power
    - High (much higher than 0 dBm)
  - Carrier Frequency Band
    - Low (something lower than 2.4 GHz, 915 MHz or lower?)
  - Data Throughput
    - Low (much lower than 1 Mbps)
  - Channel Bandwidth
    - Unclear. Likely smaller for lower frequency carrier.

Design a low-power wide-area network

- **Any particular MAC choices for lower power?**

Design a low-power wide-area network

- **Any particular MAC choices for lower power?**
  - Diversity of devices in network
    - High power gateway, low power devices in star topology
  - Devices should be off whenever possible
    - Listen-after send for downlink
  - Remove requirements for synchronization
    - No TDMA access control if it can be avoided
    - Aloha, ~~CSMA~~

Long-range CSMA is problematic

- Long-range makes everything more challenging
  - Kilometers of range mean kilometers between devices

- Detection of channel use is less reliable
  - Active research in clear channel assessment for LPWANs

- Hidden terminal problem has a wider range
  - Might make RTS/CTS more important

- Result: CSMA doesn’t dominate LPWANs like it does WLANs

LPWANs overview (common qualities)

- Unlicensed 915 MHz band (902-928 MHz)
- Higher power transmissions: ~20 dBm (100 mW)
- Low data rate 100 kbps or less
- Range on the order of multiple kilometers
- Simple Aloha access control

Outline

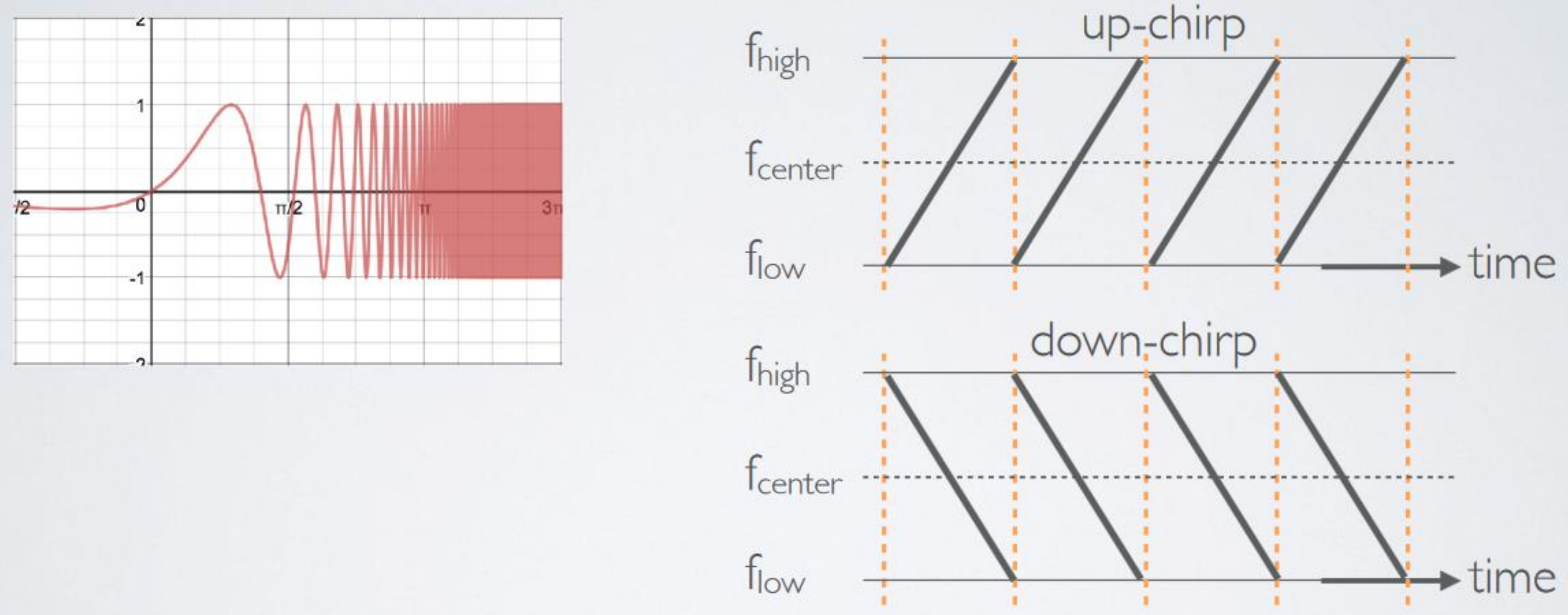
- Cellular IoT
- LPWAN Design
- **LoRaWAN**

LoRaWAN

- Open communication standard built with proprietary LoRa PHY
- Low rate (1-20 kbps) and long range (~5 km)
  - Shorter range than Sigfox but much higher bit rate
- Most popular LPWAN protocol
  - Target of academic research
  - Industry involvement in hardware and deployments

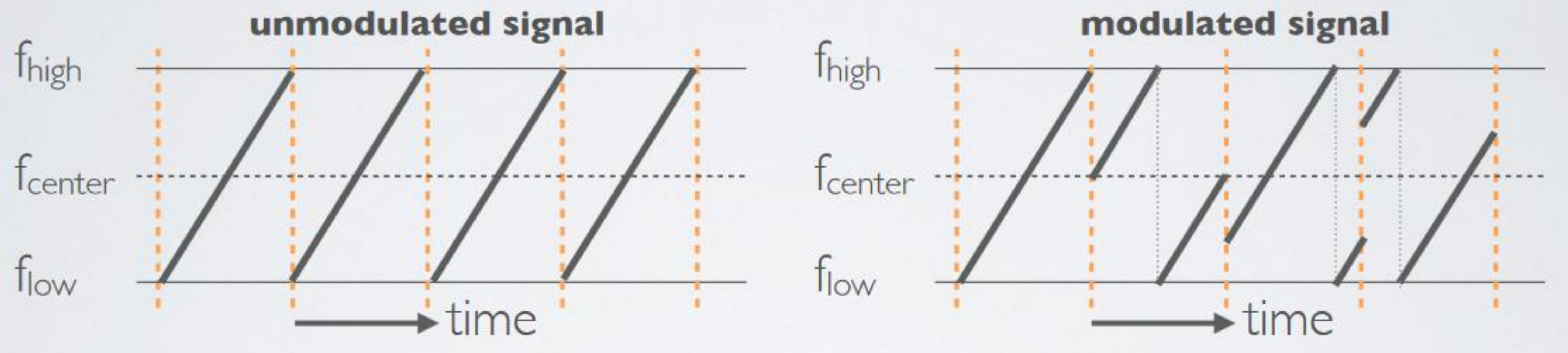
LoRa PHY uses a different modulation

- Chirp Spread Spectrum (CSS)
  - Modulation technique where frequency is varied linearly from lowest to highest within a channel



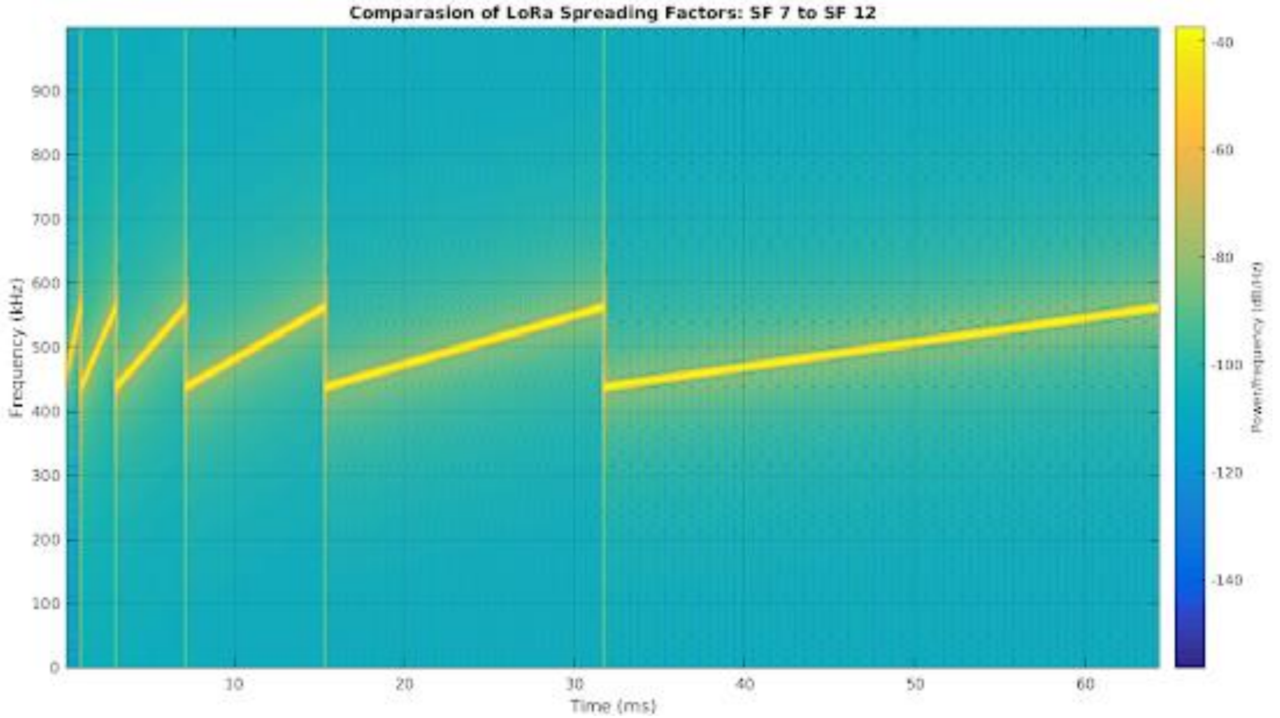
Chirp Spread Spectrum

- Data is modulated in the starting and ending points of chirp
    - Frequency increases linearly, modulo bounds of the channel

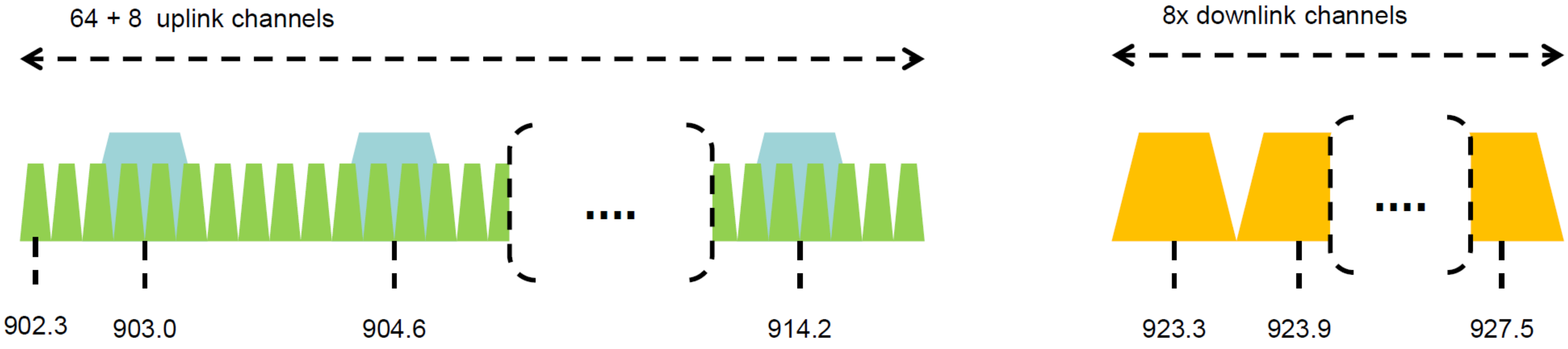


CSS has a Spreading Factor which determines bit rate

- Spreading Factor is essentially the rate-of-change of frequency
  - Slope of the line
  - Lower values of spreading factor (steeper slope) are faster data rate
- Important: different spreading factors are (mostly) orthogonal!
  - Two can overlap in time, space, and channel without a collision



LoRaWAN channels



- Sixty-four, 125 kHz uplink channels
  - Frequency Hopping over the 64 uplink channels
  - Plus eight, 500 kHz overlapping uplink channels (not well used in practice)

- Eight, 500 kHz downlink channels

LoRaWAN gateways

- No synchronization with end devices

- Instead listen to entire bandwidth simultaneously
  - Only 12 MHz total
  - Recognize preambles and allocate a hardware to decode packet
    - Normal gateways: 8 decoders
    - Good gateways: 64 decoders

LoRaWAN data rates

- Data rate options depend on channel in use
  - Unbalanced uplink and downlink
- 64-channel uplink
  - 1-5 kbps data rate
- Allowable rates based on dwell time restriction (400 ms)

Data Rate Index	**Spreading Factor**	**Bit Rate**
125 kHz Uplink Rates		
0	SF10, 125 kHz	980 bps
1	SF9, 125 kHz	1760 bps
2	SF8, 125 kHz	3125 bps
3	SF7, 125 kHz	5470 bps
500 kHz Uplink Rates		
4	SF8, 500 kHz	12500 bps
500 kHz Downlink Rates		
8	SF12, 500 kHz	980 bps
9	SF11, 500 kHz	1760 bps
10	SF10, 500 kHz	3900 bps
11	SF9, 500 kHz	7000 bps
12	SF8, 500 kHz	12500 bps
13	SF7, 500 kHz	21900 bps

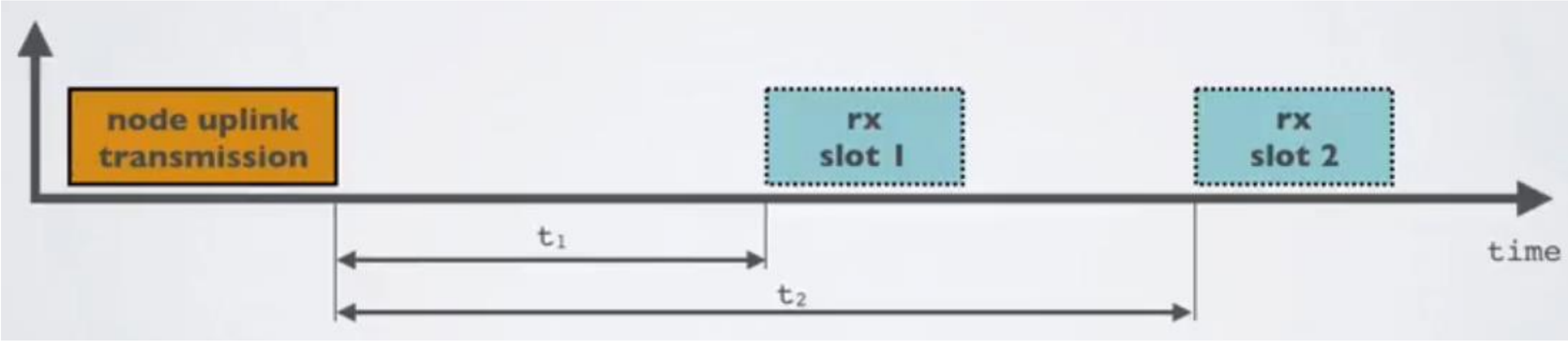
LoRaWAN link budget

- Typical TX power 20 dBm
  - Up to 30 dBm for 64-channel hopping
  - Up to 26 dBm for 8-channel hopping
- Receive sensitivity -119 dBm
  - Compare to -100 dBm for 802.15.4 and -95 dBm for BLE
- Resulting range is about a kilometer in urban environments

LoRaWAN MAC

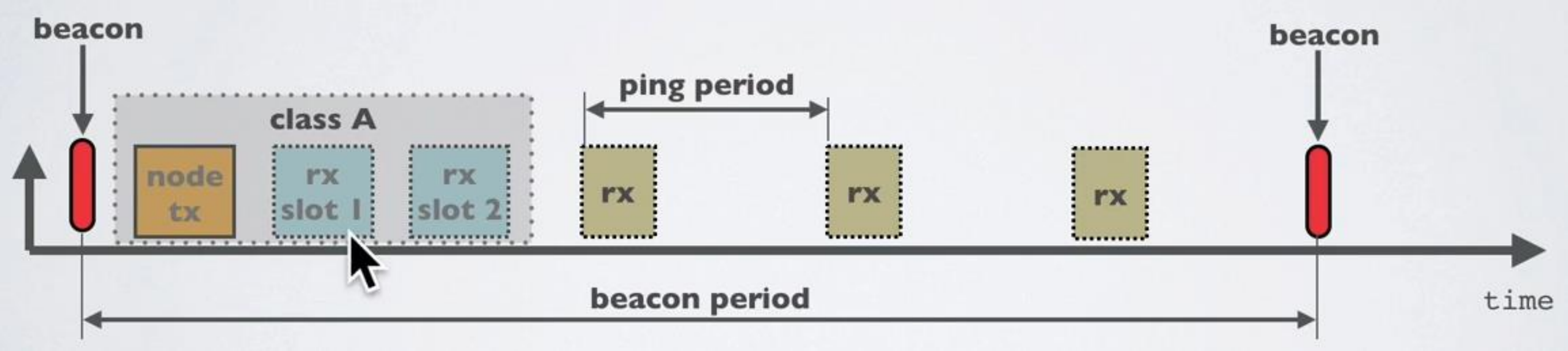
- Uplink: Aloha - transmit whenever
  - Randomly split across 64 uplink channels (reduced odds of collision)
  - Devices a different spreading factors also do not collide
  - Packets are very long though: up to 400 ms in duration

- Downlink: listen-after-send (class A device)
  - Two windows for RX on different channels



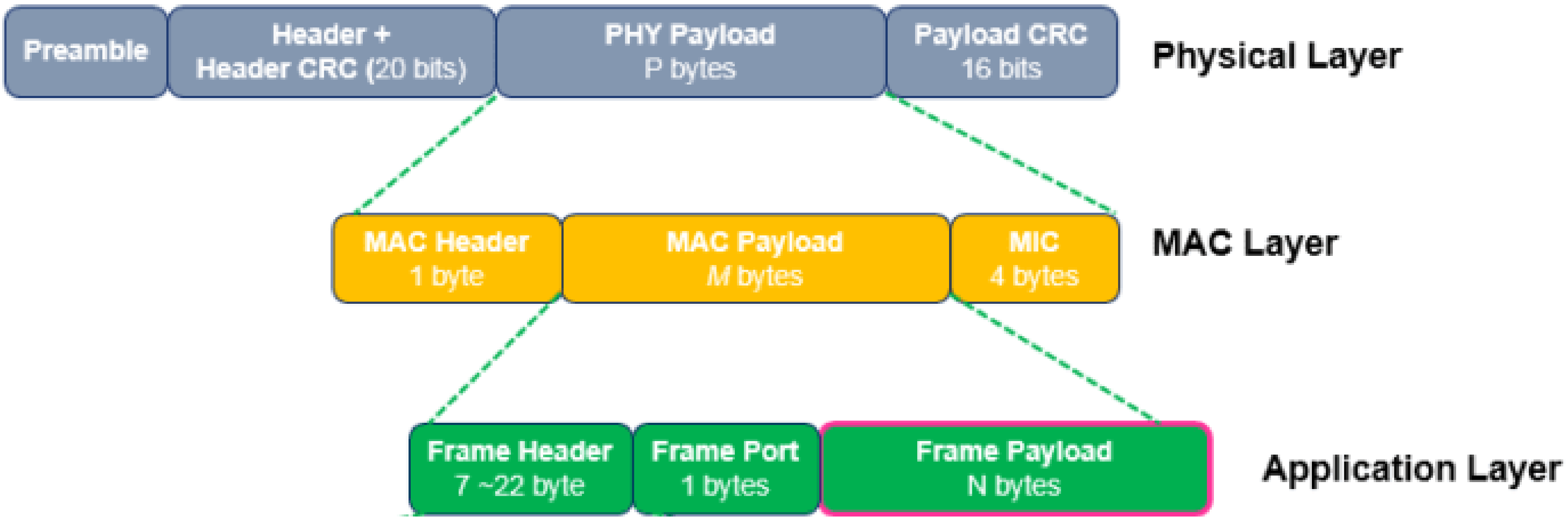
Optional downlink mechanisms

- Periodic listening (class B device)
  - Synchronized with periodic beacons
    - TX still unsynchronized Aloha
  - Mostly unused



- Continuous listening (class C device)
  - Always-on receivers

LoRaWAN packet format



Preamble | Header + Header CRC (20 bits) | PHY Payload P bytes | Payload CRC 16 bits — Physical Layer

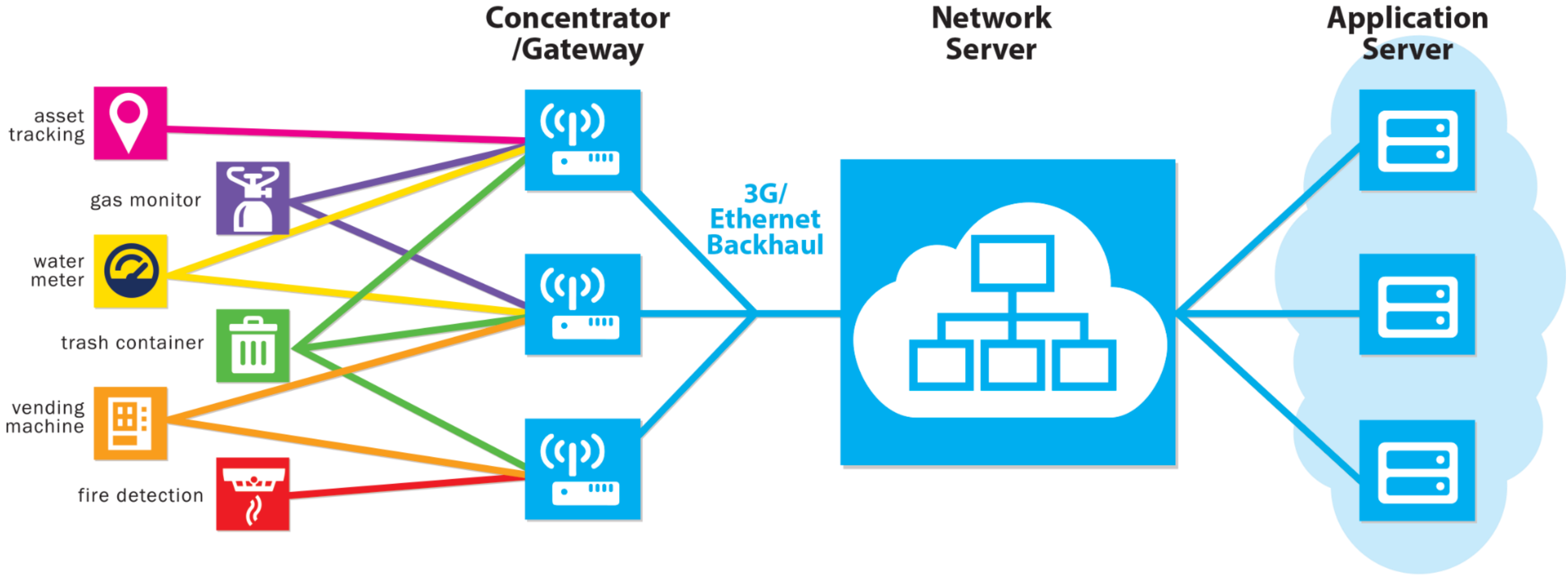
MAC Header 1 byte | MAC Payload *M* bytes | MIC 4 bytes — MAC Layer

Frame Header 7 ~22 byte | Frame Port 1 bytes | Frame Payload N bytes — Application Layer

- Frame header includes device address
- MAC Payload maximum size depends on data rate
  - Again based on dwell time in the US

Data Rate Index	**MAC Payload Size**
0	19 bytes
1	61 bytes
2	133 bytes
3	250 bytes
4	250 bytes

LoRaWAN network details



LoRaWAN hardware

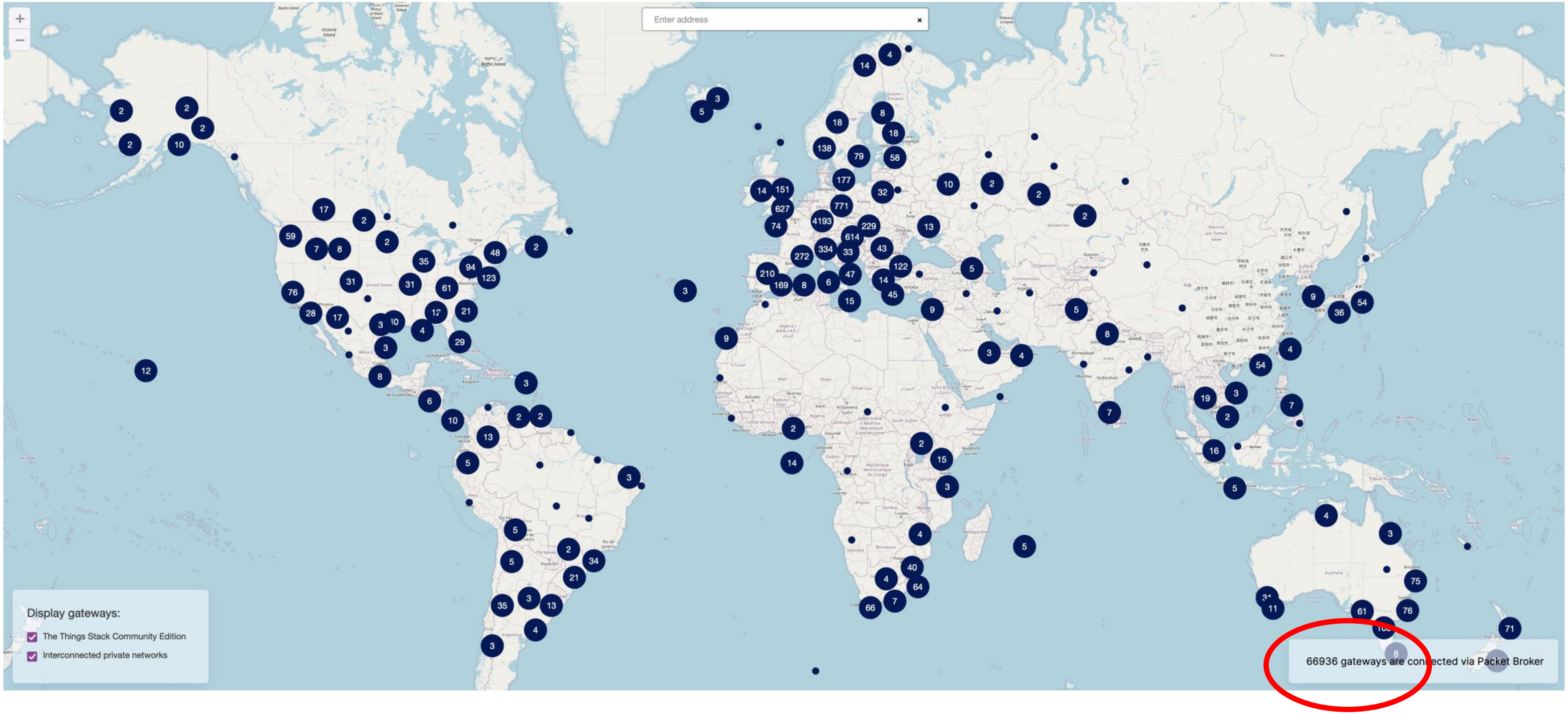
- Numerous hardware modules and development kits
  - Almost all use Semtech radio chips (Semtech owns LoRa PHY)

- Recent addition: STM32WLE5 LoRa SoC
  - Cortex-M4 + LoRa radio (analogous to nRF52840)

LoRaWAN network providers

- Somewhat-managed network providers
  - The Things Network (predominantly in Europe)
    - But available in the US too!
  - Helium
    - Any can buy and install their own gateway, which serves everyone
    - Microtransactions to pay for communication

TTN Scale [Jan 2022]



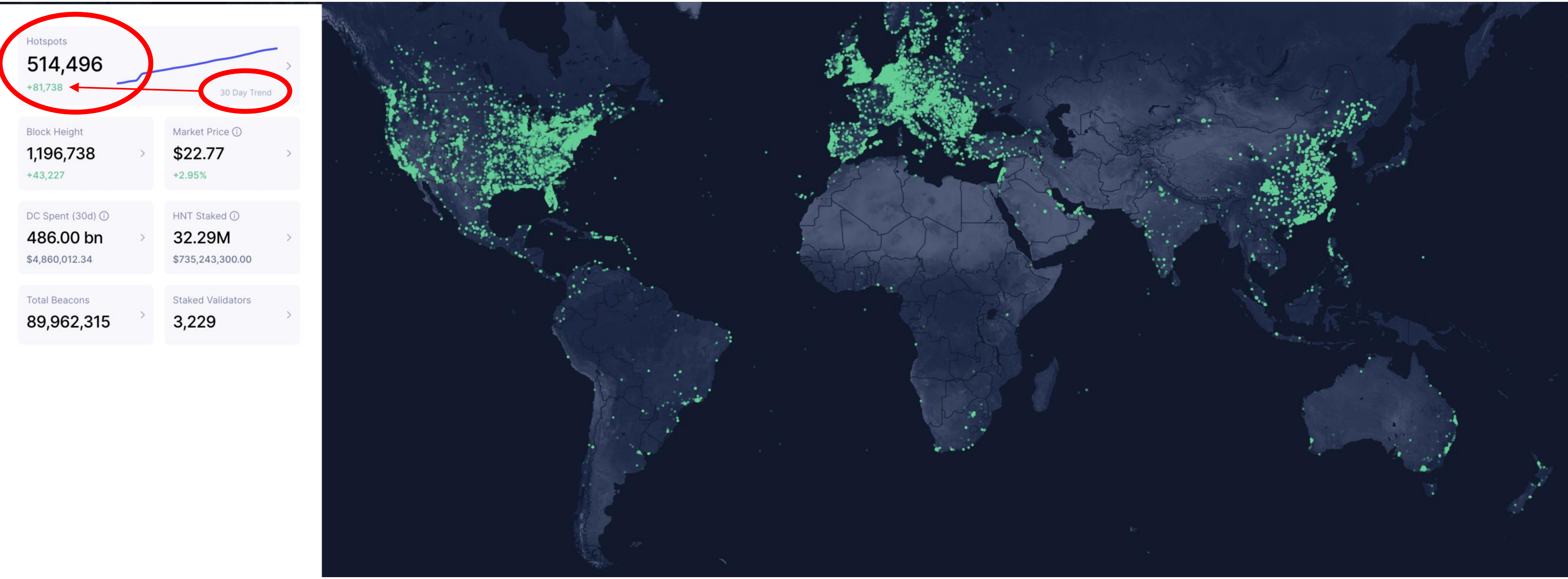
Display gateways:

☑ The Things Stack Community Edition

☑ Interconnected private networks

66936 gateways are connected via Packet Broker

Helium Scale [Jan 2022]



Hotspots
514,496
+81,738

30 Day Trend

Block Height
1,196,738
+43,227

Market Price ⓘ
$22.77
+2.95%

DC Spent (30d) ⓘ
486.00 bn
$4,860,012.34

HNT Staked ⓘ
32.29M
$735,243,300.00

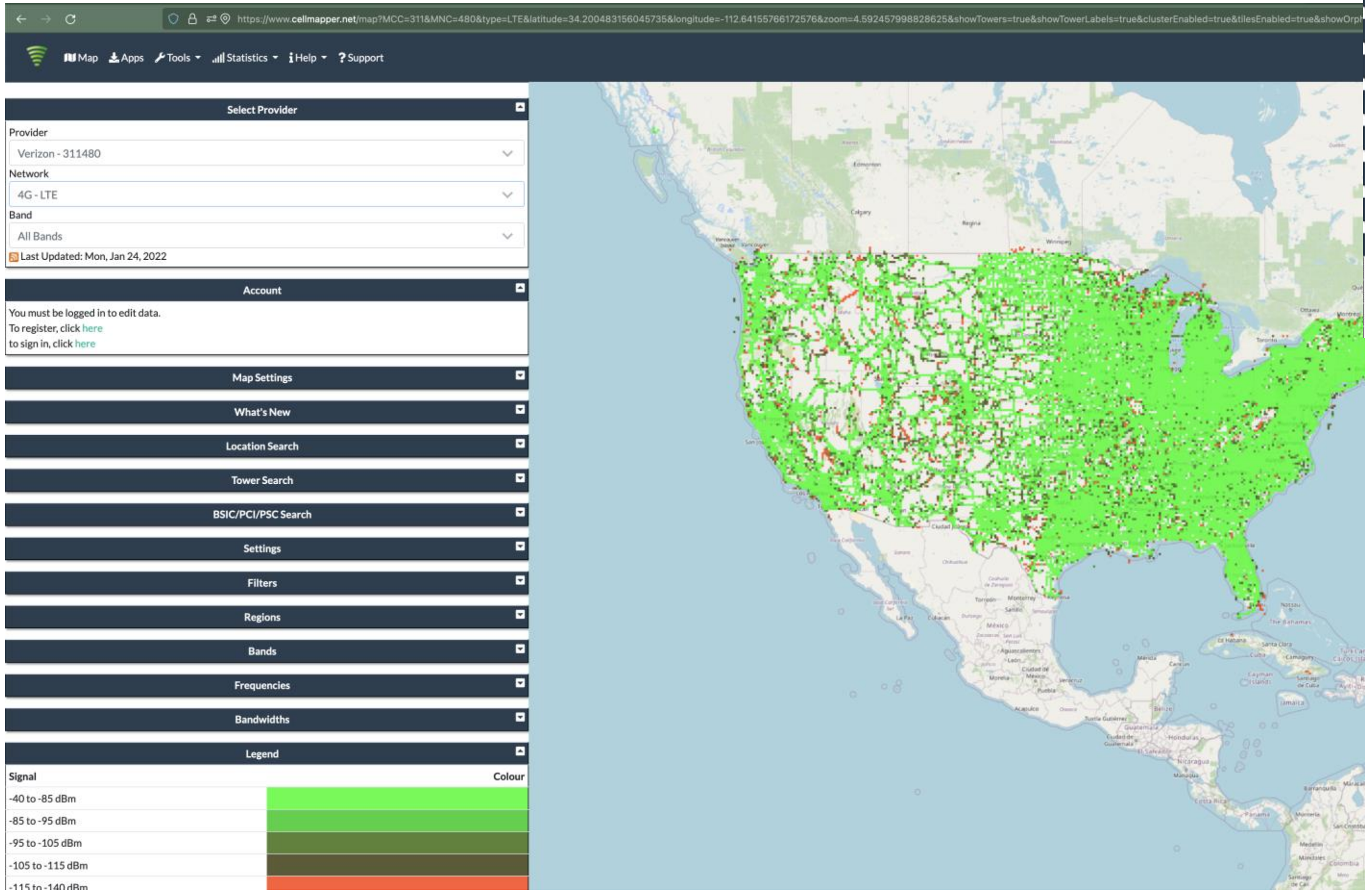
Total Beacons
89,962,315

Staked Validators
3,229

May 2022: 800,000 hotspots, with +80K in last 30 days

Quick reality check: Verizon?

- And this is just crowd-sourced data.



https://www.cellmapper.net/map?MCC=311&MNC=480&type=LTE&latitude=34.200483156045735&longitude=-112.64155766172576&zoom=4.592457998828625&showTowers=true&showTowerLabels=true&clusterEnabled=true&tilesEnabled=true&showOrp

Provider: Verizon - 311480

Network: 4G - LTE

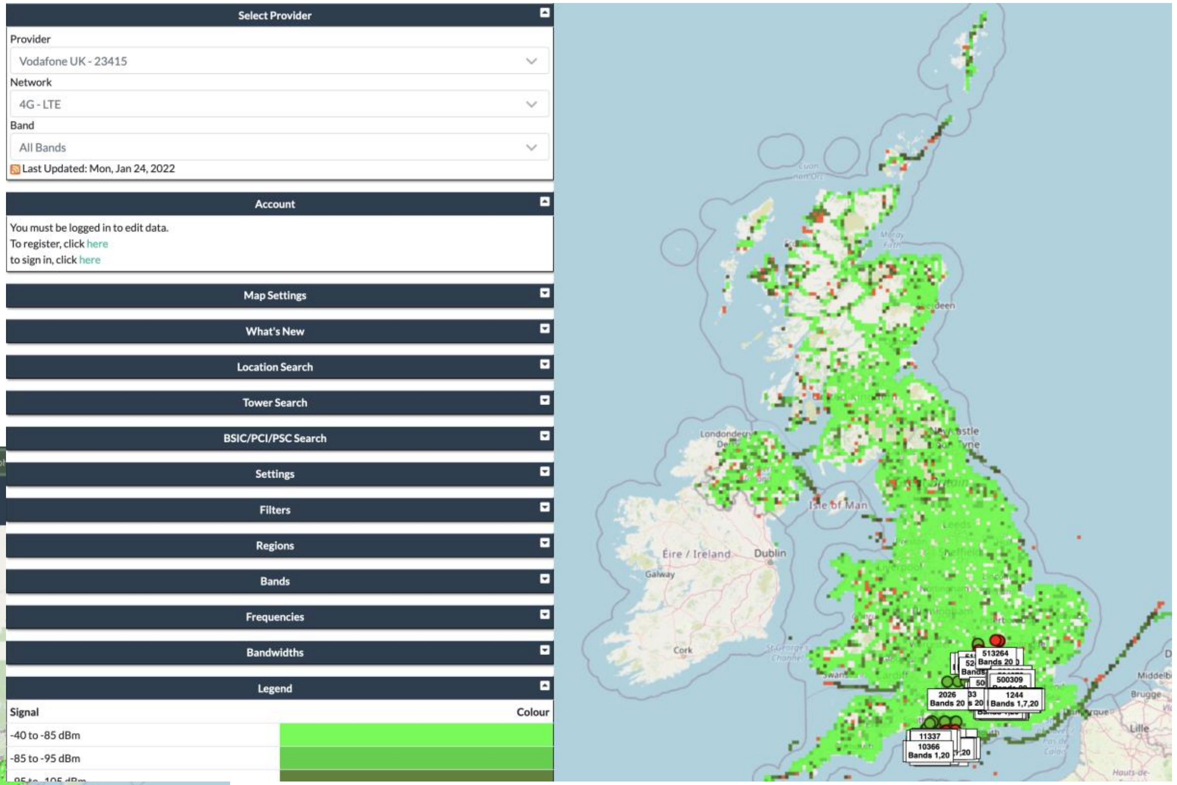
Band: All Bands

Last Updated: Mon, Jan 24, 2022

Account

You must be logged in to edit data.
To register, click here
to sign in, click here

Signal	Colour
-40 to -85 dBm	🟩
-85 to -95 dBm	🟩
-95 to -105 dBm	🟩
-105 to -115 dBm	🟫
-115 to -140 dBm	🟧



Provider: Vodafone UK - 23415

Network: 4G - LTE

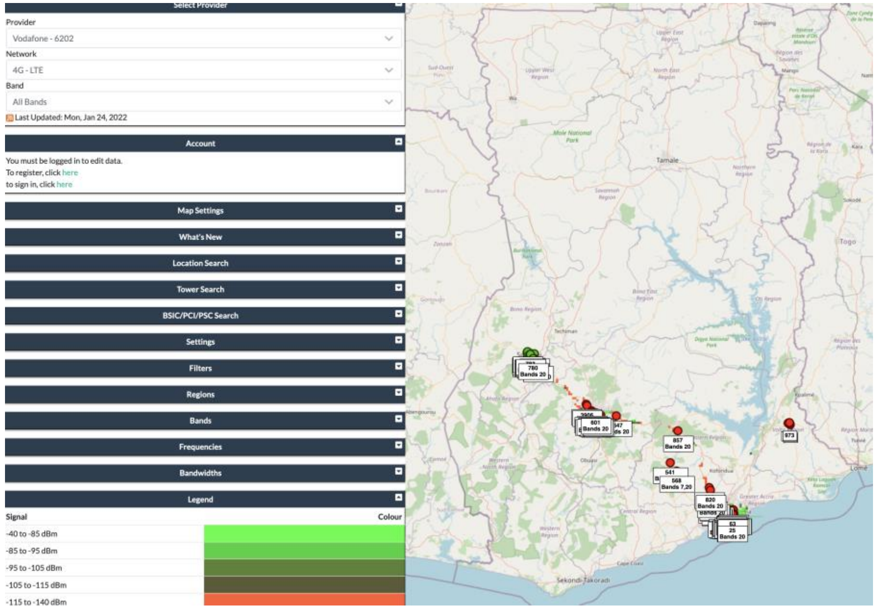
Band: All Bands

Last Updated: Mon, Jan 24, 2022

Account

You must be logged in to edit data.
To register, click here
to sign in, click here

Signal	Colour
-40 to -85 dBm	🟩
-85 to -95 dBm	🟩



Provider: Vodafone - 6202

Network: 4G - LTE

Band: All Bands

Last Updated: Mon, Jan 24, 2022

Account

You must be logged in to edit data.
To register, click here
to sign in, click here

Signal	Colour
-40 to -85 dBm	🟩
-85 to -95 dBm	🟩
-95 to -105 dBm	🟩
-105 to -115 dBm	🟫
-115 to -140 dBm	🟧

LoRaWAN interested parties

- MachineQ is a subsidiary of Comcast providing LoRaWAN networks

- Long-term goal
  - Indoor-to-outdoor LoRaWAN gateways combined with WiFi/Cellular
  - Tune down power for 100-200 meter range

- Current focus: IoT Platform-as-a-service
  - Devices, network, analytics

Outline

- Cellular IoT
- LPWAN Design
- LoRaWAN