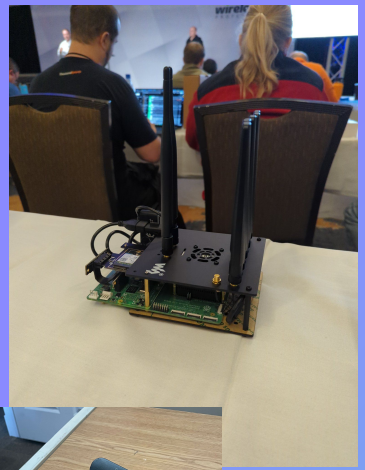
CBRS PI – SECRETS IN THE CBRS AIRWAVES

“In the interests of simplicity CBRS equipment vendors seek to shield network engineers from excessive complexity.”
-Aruba Whitepaper

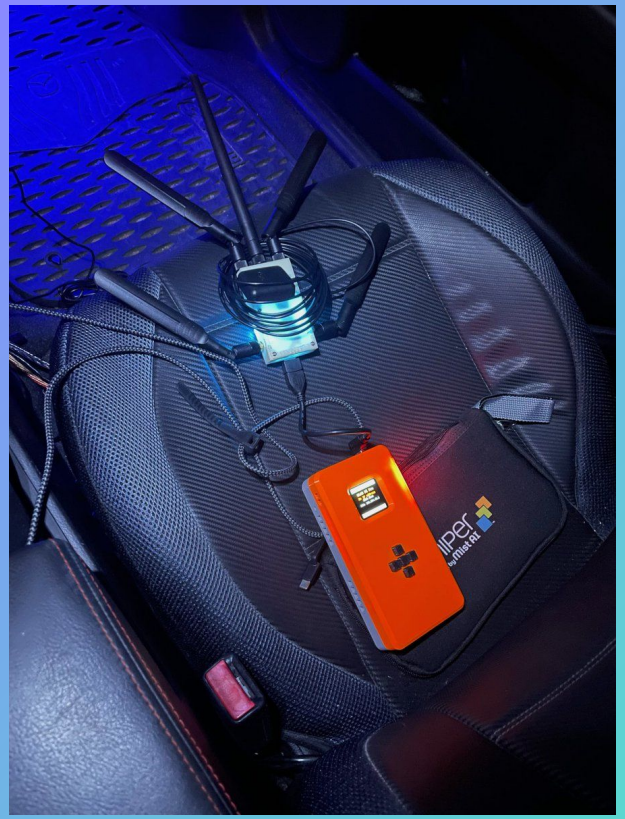
CWISA says similar.. It’s just magic.. 🤫

Um, I’m Sherlock Peter..
I want to know how it works!

So I built the CBRS Pi..



Tool captures PCAPs as well as captures EARFCN, RSRP, RSSI, and PhyCell ID (PCI)



Most channels are encrypted. The captures work because the modem exposes a diagnostic promiscuous mode port

Then talked about it at WLPC Prague and WLPC Mexico..

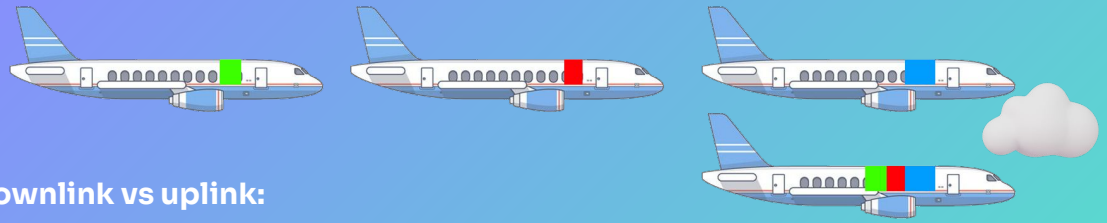
Then Peter and others asked me..

What's the modulation of LTE/5G?

How does the protocol work?

Aren't all of the frames encrypted?

What's the modulation scheme for LTE/5G on CBRS?



Different modulation schemes for downlink vs uplink:

Uses OFDM -> OFDMA for Downlink, Single Carrier-FDMA (SC-FDMA) for Uplink

15khz Subcarriers Spacing - 1.4, 3, 5, 10, 15, and 20 Mhz channels (CBRS uses 10 and 20mhz)

>20Mhz Channel Bonding is called Carrier Aggregation, can be non-contiguous (ie 20+20mhz)

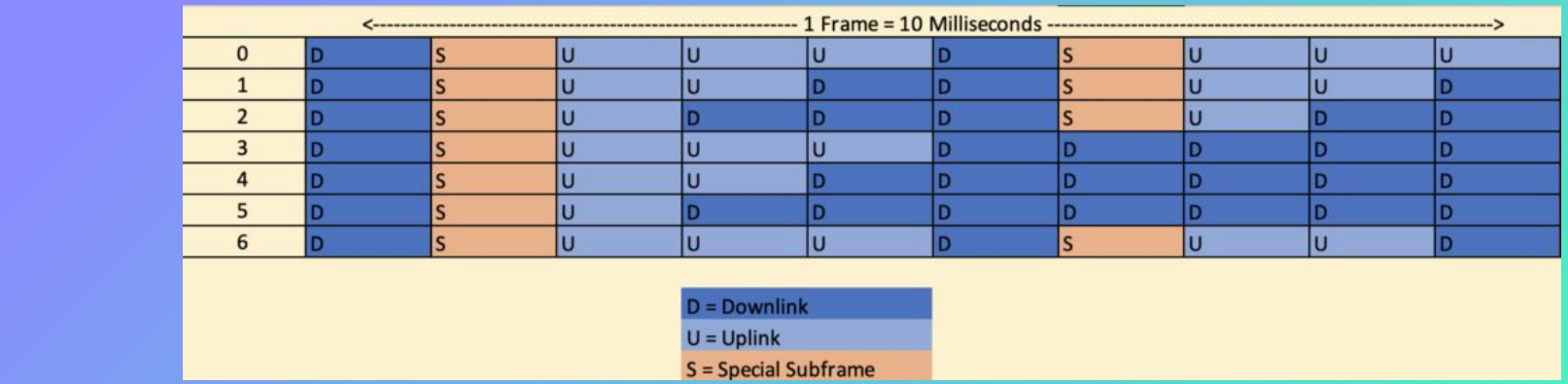
LTE supports QPSK, 16-QAM, and 64-QAM with up to 40mhz Carrier Aggregation

5G adds support for BPSK and 256-QAM with up to 100mhz Carrier Aggregation

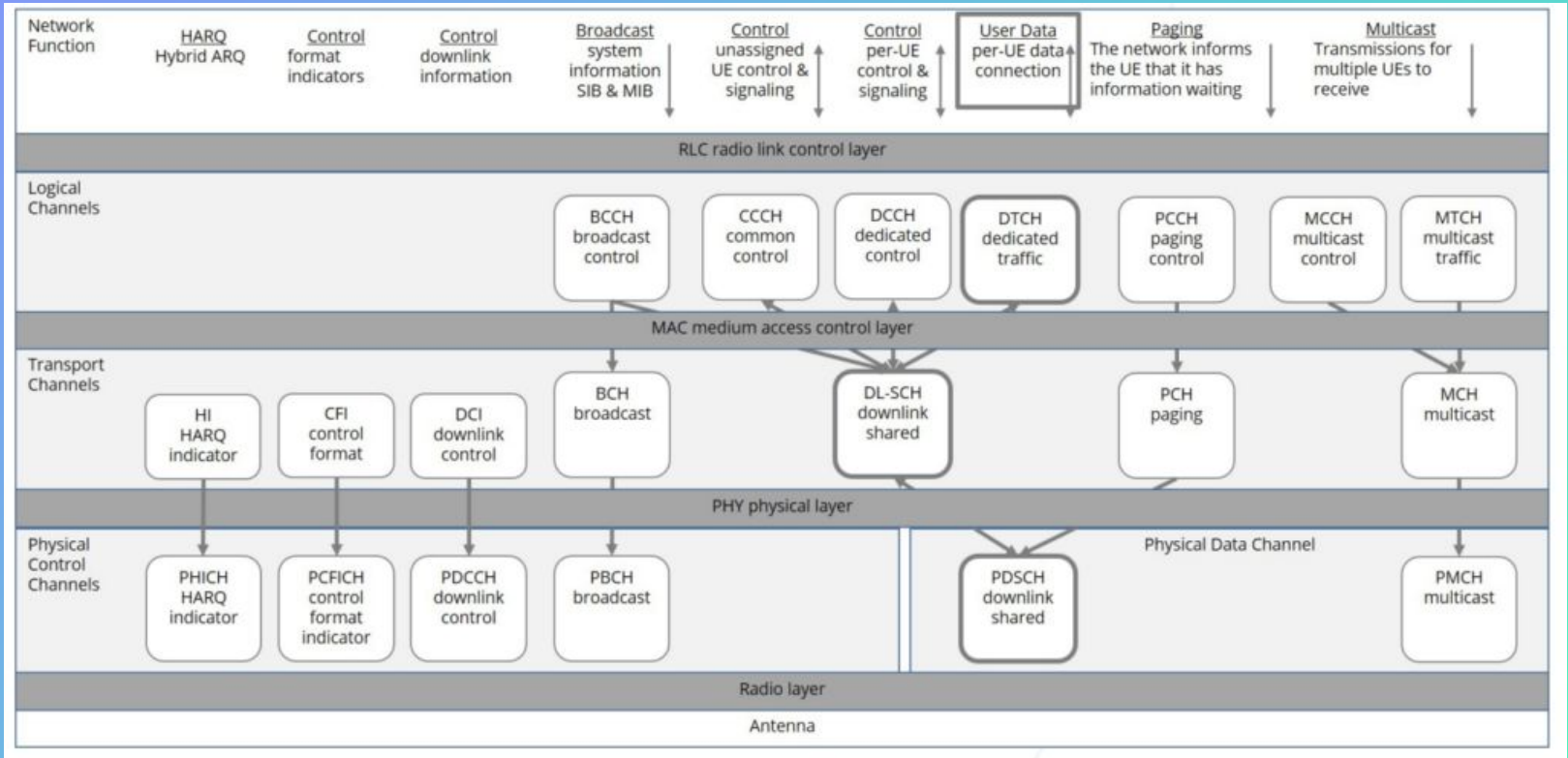
LTE/5G is a more efficient use of the spectrum than Wifi 6 due to central control and scheduling

TDD Configuration Subframe Assignment

- SA1 is a 50:50 downlink to uplink split, SA2 is a 60:40 split
- Possible source of interference if mismatched radios on same channel
- TDD is the structure, the radio uses OFDMA/SC-FDMA, QoS, and other factors for scheduling
- Recommended to use SA2 Outdoors - Verizon and DeWi are using SA2 on Band 48

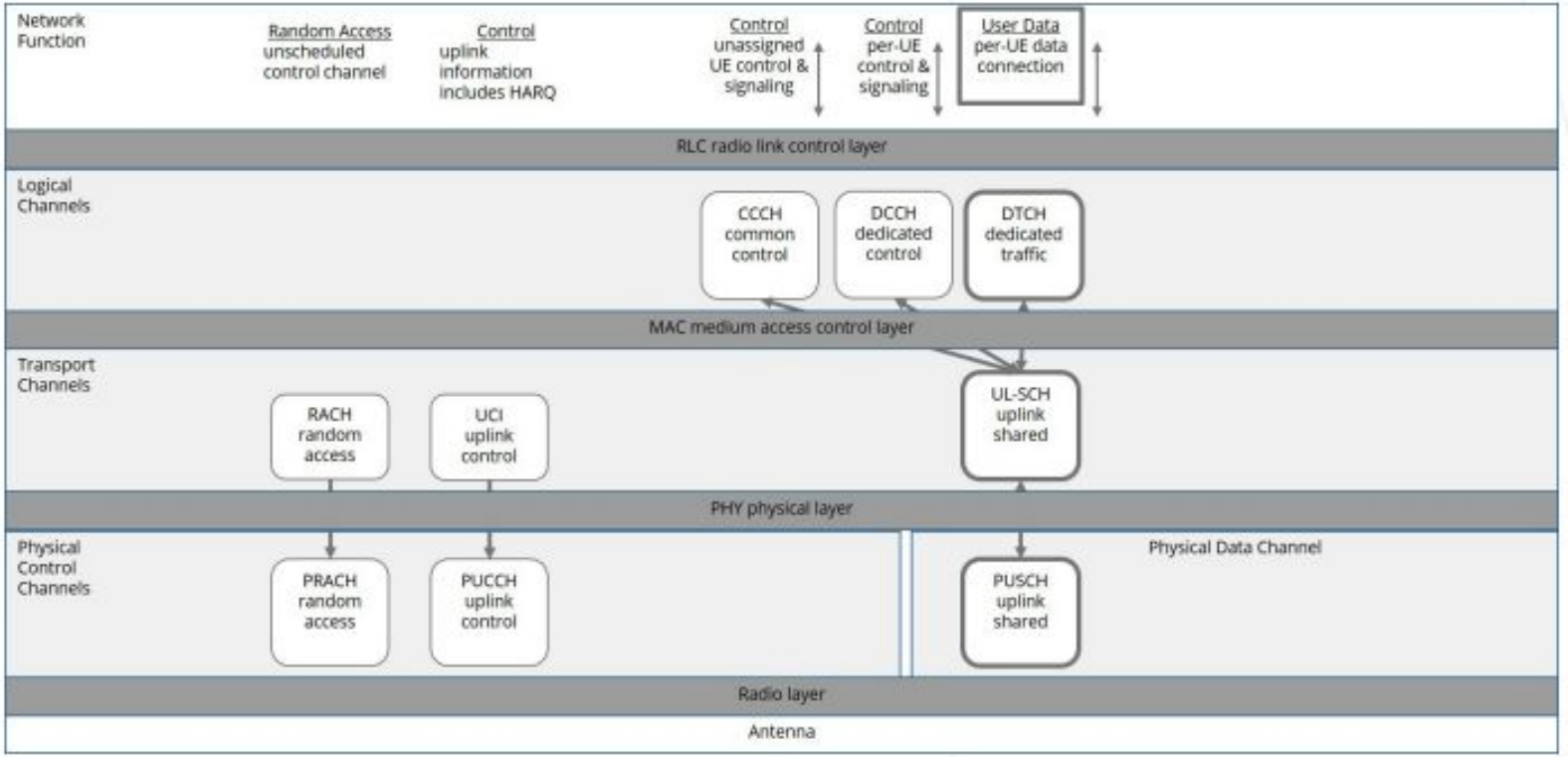


LTE Downlink Channels



Source: https://www.arubanetworks.com/assets/wp/WP_CBRS-Signaling-and-Control.pdf

LTE Uplink Channels

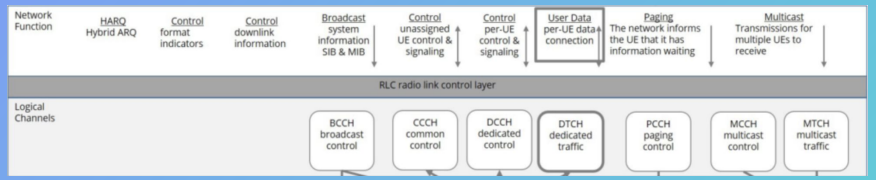


Source: https://www.arubanetworks.com/assets/wp/WP_CBRS-Signaling-and-Control.pdf

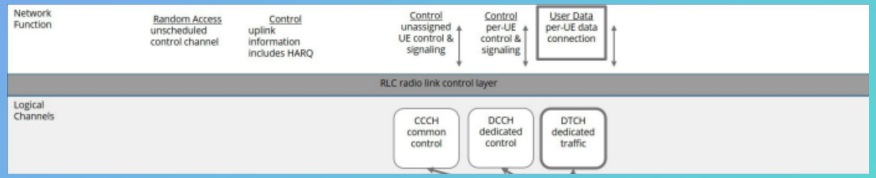
LTE Logical Control Channels

Dedicated channels ensures data rate for control traffic

Downlink



Uplink



BCCH (Broadcast Control) - MIB and SIBs - contains PLMN, subframeAssignments, specialSubframePatterns, TAI, and CBRS-NID. User Endpoints (UE) client's cell selection and reselection are controlled on this channel. Broadcast to all. Downlink only.

CCCH (Common Control) - Contains the connection and association for an unassigned UE device. Both Uplink and Downlink directions.

DCCH (Dedicated Control) - Control and Signaling per UE. Unicast communication between individual UE and eNodeB. Provides measurement reports to the radio which contains UE info such as RSRP and RSRQ ranges. UL-DCCH may contain capabilities and supported bands of UE. Both Uplink and Downlink directions.

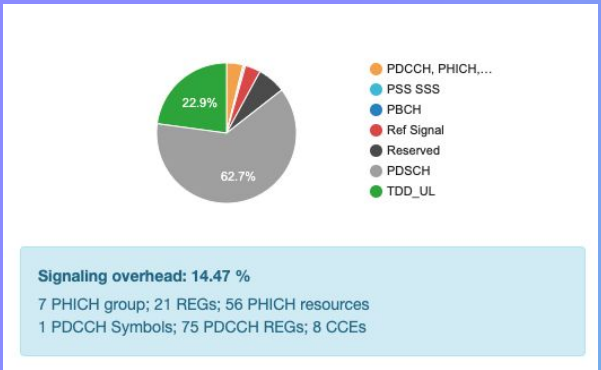
DTCH (Dedicated Traffic) - Contains all data and telephony traffic. Encrypted from UE to the EPC Core. Broken into voice and data subchannels. Not captured! Both Uplink and Downlink directions.

PCCH (Paging Control) - "Paging a UE." Informs UE devices there is traffic or messages that are waiting at the base station such as a text message or phone call. Power saving mechanism. Page Data is received on the DTCH. Broadcast to all. Downlink only.

No.	Absolute Time	Delta Time	Relative Time	Protocol	Length	ARFCN	freqBand	MCC-MNC-Digit	subfran	specialSub	tracking	cellIdentity	IMSI	dl-Bai	SIB-Type	APN	Info
11865	00:46:26.957590	0.000192	2746.706…	LTE RRC BCCH_BCH	73	0								n100			MasterInformationBlock (SFN=186)
11866	00:46:26.961067	0.003477	2746.710…	LTE RRC DL_SCH	92	0	48	0,1,0,3,1,5	sa2	ssp7	0020	81c74250			sibType3,…		SystemInformationBlockType1
11867	00:46:27.047398	0.086331	2746.796…	LTE RRC BCCH_BCH	73	0								n100			MasterInformationBlock (SFN=188)
11868	00:46:27.067398	0.020000	2746.816…	LTE RRC BCCH_BCH	73	0								n100			MasterInformationBlock (SFN=188)
11869	00:46:27.067580	0.000182	2746.816…	LTE RRC BCCH_BCH	73	0								n100			MasterInformationBlock (SFN=188)
11870	00:46:27.121062	0.053482	2746.870…	LTE RRC DL_SCH	92	0	48	0,1,0,3,1,5	sa2	ssp7	0020	81c74250			sibType3,…		SystemInformationBlockType1
11871	00:46:27.195978	0.074916	2746.945…	LTE RRC DL_SCH	102	0											SystemInformation [SIB2]
11872	00:46:27.207403	0.011425	2746.956…	LTE RRC BCCH_BCH	73	0								n100			MasterInformationBlock (SFN=192)
11873	00:46:27.207581	0.000178	2746.956…	LTE RRC BCCH_BCH	73	0								n100			MasterInformationBlock (SFN=192)
11874	00:46:27.221010	0.013429	2746.970…	LTE RRC DL_SCH	92	0	48	0,1,0,3,1,5	sa2	ssp7	0020	81c74250			sibType3,…		SystemInformationBlockType1
11875	00:46:27.235878	0.014868	2746.985…	LTE RRC DL_SCH	74	0											SystemInformation [SIB4]
11876	00:46:27.241605	0.005727	2746.990…	GSMTAP/NAS-EPS	182	0							31501000…				Attach request, PDN connectivity re
11877	00:46:27.241794	0.000189	2746.991…	LTE RRC UL_CCCH	76	0											RRCConnectionRequest
11878	00:46:27.524033	0.282239	2747.273…	LTE RRC DL_CCCH	104	0											RRCConnectionSetup
11879	00:46:27.528396	0.004363	2747.277…	LTE RRC UL_DCCH/NAS-EPS	187	0							31501000…				RRCConnectionSetupComplete, Attach
11880	00:46:27.544027	0.015631	2747.293…	LTE RRC DL_SCH	81	0											SystemInformation [SIB3]
11881	00:46:27.544133	0.000106	2747.293…	LTE RRC DL_CCCH	104	0											RRCConnectionSetup
11882	00:46:27.640935	0.096802	2747.390…	LTE RRC DL_DCCH/NAS-EPS	109	0											DLInformationTransfer, Authenticat
11883	00:46:27.641132	0.000197	2747.390…	GSMTAP/NAS-EPS	106	0											Authentication request
11884	00:46:27.759196	0.118064	2747.508…	GSMTAP/NAS-EPS	81	0											Authentication response
11885	00:46:27.759401	0.000205	2747.508…	LTE RRC UL_DCCH/NAS-EPS	84	0											ULInformationTransfer, Authenticat
11886	00:46:27.810935	0.051534	2747.560…	LTE RRC DL_DCCH/NAS-EPS	90	0											DLInformationTransfer, Security mo
11887	00:46:27.811112	0.000177	2747.560…	GSMTAP/NAS-EPS	87	0											Security mode command
11888	00:46:27.811128	0.000016	2747.560…	GSMTAP/NAS-EPS	81	0											Security mode command
11889	00:46:27.811896	0.000768	2747.561…	GSMTAP/NAS-EPS	83	0											Security mode complete
11890	00:46:27.812042	0.000146	2747.561…	GSMTAP/NAS-EPS	89	0											Security mode complete
11891	00:46:27.812165	0.000123	2747.561…	LTE RRC UL_DCCH/NAS-EPS	92	0											ULInformationTransfer, Security mo
11892	00:46:27.835984	0.023819	2747.585…	LTE RRC DL_SCH	102	0											SystemInformation [SIB2]
11893	00:46:27.841014	0.005030	2747.590…	LTE RRC DL_SCH	92	0	48	0,1,0,3,1,5	sa2	ssp7	0020	81c74250			sibType3,…		SystemInformationBlockType1

```
> Frame 11874: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> User Datagram Protocol, Src Port: 13337, Dst Port: 4729
> GSM TAP Header, ARFCN: 0 (Downlink), TS: 0, Channel: PCH (5)
v LTE Radio Resource Control (RRC) protocol
  v BCCH-DL-SCH-Message
    v message: c1 (0)
      v c1: systemInformationBlockType1 (1)
        v systemInformationBlockType1
          > cellAccessRelatedInfo
          > cellSelectionInfo
            p-Max: 23 dBm
            freqBandIndicator: 48
          > schedulingInfoList: 4 items
          v tdd-Config
              subframeAssignment: sa2 (2)
              specialSubframePatterns: ssp7 (7)
            si-WindowLength: ms20 (5)
            systemInfoValueTag: 16
```

LTE OFDMA PHY Uplink/Downlink

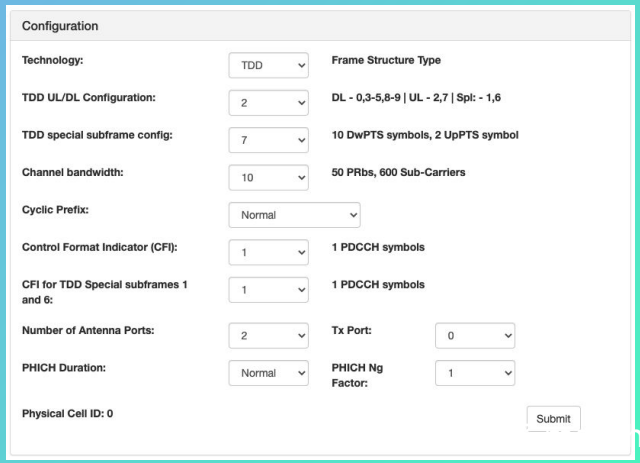


https://dhagle.in/LTE

Configuration: TDD, SA2, SSP7, 10mhz bandwidth

10Mhz has 50 PRBs (ie. grey rows). 20Mhz has 100 PRBs. Rows are Sub Carrier. Each box is a Symbol. Left to Right is Time ie TDD Configuration.

Lower left graph: White are downlink, green are uplink, others are control traffic. Shows 1.4Mhz channel with 6 PRBs for ease of display.



Resources

https://blogs.arubanetworks.com/corporate/explaining-cbrs-and-wireless/

https://www.arubanetworks.com/assets/wp/WP_CBRS-The-Radio.pdf

https://www.arubanetworks.com/assets/wp/WP_CBRS-Signaling-and-Control.pdf

https://www.arubanetworks.com/assets/wp/WP_CBRS-LTE-Technology-for-the-Enterprise.pdf

https://www.cwnp.com/c5s/

https://www.youtube.com/playlist?list=PLW8PqCtRwgZPeb934BwXXrC79V1czJoBH

https://www.youtube.com/playlist?list=PLW8PqCtRwgZPGHAd6R1jz-aYoLmoeS58y

https://www.google.com/get/spectrumdatabase/cpi/

Thank you!
markhoutz.com