目录

[移动联通电信缩写 2](#_Toc32566)

[Hz单位换算 3](#_Toc8452)

[移动联通电信广电获得的频段 3](#_Toc17930)

[英文术语 4](#_Toc2522)

[Serving\_Cell 4](#_Toc28465)

[Main\_Info 4](#_Toc4235)

[LTE\_Intra 4](#_Toc19788)

[LTE\_Inter,4,Freq1 4](#_Toc13774)

[BS 4](#_Toc23659)

[TAC 4](#_Toc21211)

[ECI 4](#_Toc20645)

[ARFCN  5](#_Toc5160)

[PCI 5](#_Toc12909)

[CELL\_NAME 5](#_Toc32488)

[ADDRESS 5](#_Toc16008)

[BS\_NAME  5](#_Toc32672)

[BS\_NO 5](#_Toc11995)

[LAC 5](#_Toc12884)

[BSIC\_SERV 6](#_Toc31325)

[MCC 6](#_Toc22801)

[MNC 6](#_Toc19961)

[dbm 7](#_Toc23526)

[BAND 7](#_Toc19748)

[ulbw 9](#_Toc17800)

[dlbw 9](#_Toc24686)

[信道带宽（Channel Bandwidth） 9](#_Toc2616)

[Fc 9](#_Toc18780)

[EARFCN 10](#_Toc4763)

[FREQ 10](#_Toc11848)

[RX 10](#_Toc4783)

[RSSI 10](#_Toc9763)

[RSRP 10](#_Toc13565)

[RSRQ 10](#_Toc19265)

[SNR/RSSNR 11](#_Toc9392)

[SINR 11](#_Toc21918)

[RXLEV 11](#_Toc5455)

[CQI 11](#_Toc64)

[MEID 11](#_Toc7441)

[SSB 11](#_Toc23195)

[Beam\_num 12](#_Toc7992)

[Ssb\_id 12](#_Toc28195)

[中文术语 13](#_Toc11726)

[空口 13](#_Toc8565)

[帧 13](#_Toc18103)

[干扰和噪声 13](#_Toc19900)

[信道（Channel） 14](#_Toc11774)

[频段（Frequency Band） 14](#_Toc24632)

[频道（Channel） 14](#_Toc30648)

[小区（Cell） 15](#_Toc28953)

[扇区（Sector） 15](#_Toc9733)

[锁频段 15](#_Toc16902)

[强搜 16](#_Toc9190)

[DRX 16](#_Toc27145)

[脉冲模式 16](#_Toc27658)

[频道切换 (Channel Switching) 17](#_Toc25018)

[信号强度和信号质量测试 17](#_Toc25281)

[小区和扇区切换测试 17](#_Toc31195)

[数据速率测试 17](#_Toc25772)

[干扰检测和分析 17](#_Toc22474)

[话务量测试 17](#_Toc22512)

[功率控制 (Power Control) 17](#_Toc11881)

[自适应调制 (Adaptive Modulation) 18](#_Toc15344)

[跳频 (Frequency Hopping) 18](#_Toc24434)

[扫频（Sequential Scanning） 18](#_Toc21464)

[随机扫描（Random Scanning） 18](#_Toc20566)

[模块型号 18](#_Toc10878)

[5g模块中移动和广电共用一个基站，联通和电信共用一个基站 19](#_Toc22287)

[定位 19](#_Toc25197)

[单兵 19](#_Toc1683)

[工作流程 19](#_Toc6926)

[UE（User Equipment） 19](#_Toc8137)

[功放（功率放大器PA）（Power Amplifier） 19](#_Toc15432)

[ADC（Analog-to-Digital Converter） 20](#_Toc21288)

["单板" 21](#_Toc17437)

[基带（Baseband） 21](#_Toc8308)

[基带处理器（Baseband Processor） 22](#_Toc19963)

[常用配置 22](#_Toc19761)

# 移动联通电信缩写

NR表示5G

LTE表示4G

CM表示移动 ChinaMobile

CU表示联通 ChinaUnicom

CT表示电信 ChinaTele

网络缩写

NR-CM 移动5G

NR-CUCT 联通电信5G

NR-CUCT 联通电信5G

NR-C 广电5G

LTE-CM\TDD 移动4G

LTE-CU\FDD 联通4G

LTE-CT\CDMA4G 电信4G

LTE-C 广电4G

LTE-QS 强搜4G

TDSCDMA 移动3G

WCDMA联通3G

MGSM\GSM\GSM\_CMCC 移动2G

UGSM\GSM\_CU联通2G

CDMA\CDMA2G 电信2G

# Hz单位换算

10e3 KHz

10e6 MHz

10e9 GHz

1GHz=1000MHz=1000,1000KHz

# 移动联通电信广电获得的频段

中国电信获得3400MHz-3500MHz共100MHz带宽的5G试验频率资源；

中国移动获得2515MHz-2675MHz、4800MHz-4900MHz频段的共260MHZ带宽的5G试验频率资源。其中2515-2575MHz、2635-2675MHz和4800-4900MHz频段为新增频段，2575-2635MHz频段为重耕中国移动现有的TD-LTE（4G）频段；

中国联通获得3500MHz-3600MHz共100MHz带宽的5G试验频率资源。

最新加进来一个广电，拥有700MHz的频谱，将来怎么用这个700MHz，我们慢慢看眉目。

# 英文术语

**MCC、MNC、dbm、TAC、ECI、PCI、BAND、EARFCN、FREQ、RSSI、RSRP、RSRQ、SINR**

## Serving\_Cell

服务小区指的是当前移动设备所连接的基站提供的主要服务小区（cell）

## Main\_Info

（主要信息）：Main\_Info提供了有关设备或终端当前状态的主要信息。这些信息可能包括信号强度、频率、网络制式（如2G、3G、4G、5G）以及其他设备的运营商信息。Main\_Info通常用于识别和显示设备的基本运行状态。

## LTE\_Intra

LTE同频小区 LTE\_Intra\_Cell1 LTE同频小区1

## LTE\_Inter,4,Freq1

LTE邻频小区

## **BS**

Base Station基站

## **TAC**

（跟踪区代码）

TAC（Tracking Area Code，跟踪区代码）：由运营商自行分配，主要起移动用户定位唯一标识作用。

## **ECI**

（小区唯一标识）

ECI（E-UTRAN Cell Identifier，E-UTRAN 小区唯一标识）：在LTE中主要起移动用户定位唯一标识作用。ECI用于唯一标识全球范围内的小区。

NCI 5g

## **ARFCN**

载频号 频点 基站的位置

## **PCI**

Physical Cell Identifier，即物理小区标识 LTE的物理小区标识是用于区分不同小区的无线信号，保证在相关小区覆盖范围内没有相同的物理小区标识。ECI用于唯一标识全球范围内的小区，而PCI用于在同一频率下区分不同的邻近小区。

## **CELL\_NAME**

 小区名称 CELL 小区号

## **ADDRESS**

 基站地址 TIME 时间

## **BS\_NAME**

基站名称 BCCH 广播控制信道

## **BS\_NO**

 基站编号 BSIC 基站色码

## **LAC**

（Location Area Code）

 位置区号码 LAT 纬度，是在GSM（Global System for Mobile Communications）2g和其它基于GSM的无线通信系统中使用的一个参数，用于标识移动设备所处的位置区域。

## **BSIC\_SERV**

 当前的基站色码。基站色码（BSIC，Base Station Identity Code）是在GSM（Global System for Mobile Communications）网络中用于标识不同基站的标识码。

## **MCC**

（移动国家代码）

MCC：Mobile Country Code，移动国家代码，MCC的资源是由国际电联（duITU）统一分配和管理，用于唯一识别移动用户zhi所属的国家，共3位。中国为460。

。



## **MNC**

（移动网络代码）

MNC（Mobile Network Code，移动信号网络码）用于识别移动客户所属的移动网络，共 2~3 位数字。在同一个国家内，如果具有多个 PLMN，那么就可以通过 MNC 来进行区别。

* 中国移动系统使用 00、02、04、07
* 中国联通 GSM 系统使用 01、06、09
* 中国电信 CDMA 系统使用 03、05，电信 4G 使用 11
* 中国铁通系统使用 20
* 中国广电 15

所以，460-00 就标识中国移动，460-01就标识中国联通，460-03就标识中国电信。

## **dbm**

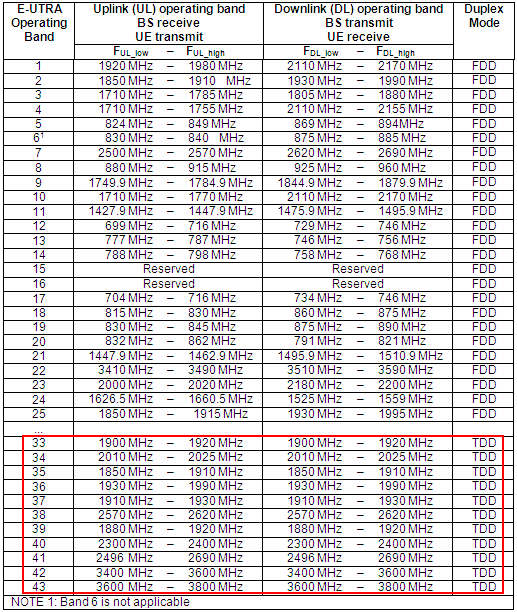
（功率绝对值）

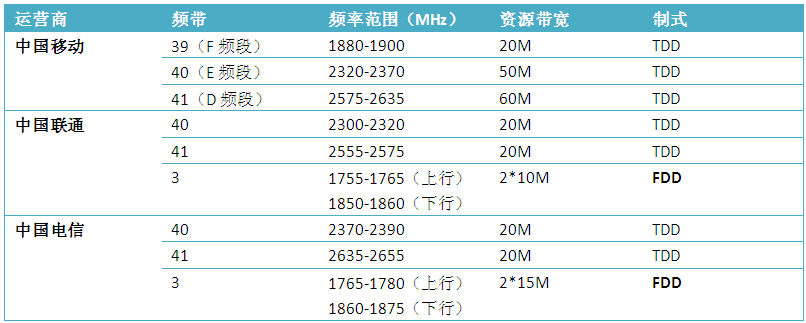
dbm是一个表示功率绝对值。dBm越大，表示周围信号越好，如-76dbm>-100dbm。

## **BAND**

（频带）

频带指的是一个频率的范围或者频谱的宽度，即无线解码器的最低工作频率至最高工作频率之间的范围，单位是Hz。为了方便起见，在LTE中，使用数字1-43来表示不同的频带（36101-V10.21.0版本协议），从而指代不同的频率范围。协议36101规定了目前LTE所有的频带、该频带的频率范围和LTE制式需要注意的是，频带1-32的上下行频率范围是不重叠的，即上行和下行在不同的频点中传输数据，这种频带也称为“****成对频带****”（Paired Frequency Band），预留给FDD使用。频带33-43的上下行频率范围一致，这种频带也称为“****非成对频带****”（Unpaired Frequency Band），预留给TDD使用。





## ulbw

上行带宽（ulbw）

## dlbw

下行带宽（dlbw）

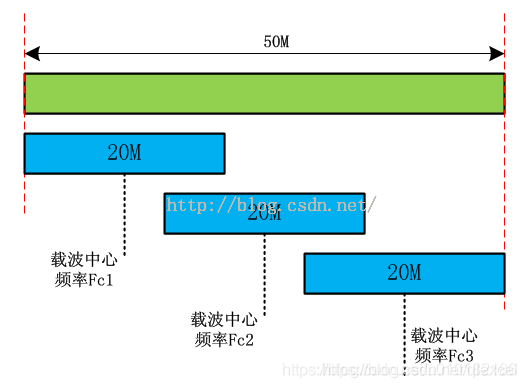
## **信道带宽（Channel Bandwidth）**

信道带宽体现了信道覆盖的频率范围的大小，限定了允许通过该信道的上下限频率，也即限定了一个频率通带。在一个频带Band中，可以灵活分配若干个不同的信道带宽。LTE系统支持信道带宽灵活可变，有6种可以配置，分别是1.4MHz，3MHz，5MHz，10MHz，15MHz，20MHz。较低的带宽1.4MHz和3MHz，规定多种带宽的目的是为了适应不同频率的使用场景，比如有些时候可用的频带不足10MHz，那么就可以将LTE系统配置成5MHz使用。

## **Fc**

载波中心频率Fc（简称载波频率），是个浮点值，不好用于空口的传输，所以在协议制定的时候使用EARFCN来表示对应的Fc，通过计算得到EARFCN。

比如：为了唯一标识某个LTE系统所在的频率范围，仅用频带和信道带宽这两个参数是无法限定的，比如移动的频带40占了50M频率范围，而LTE最大的信道带宽是20M，那么在这个50M范围里是没有办法限定这个20M具体在什么位置，这个时候就要引入新的参数：载波中心频率Fc



## **EARFCN**

（载波频点号）

EARFCN：载波频点号（E-UTRA Absolute Radio Frequency Channel Number），绝对无线频率信道号，使用16bit表示，范围是0-65535。唯一标识某个LTE系统所在的频率范围

## **FREQ**

（频率）

FREQ指的是当前网络所采用的的频率MHZ。

## **RX**

反映的是接收到的信号强度（手机侧），通常以dBm（分贝毫瓦）为单位表示。它表示设备接收到的信号的功率水平。Rx是一种综合指标，考虑了从各种干扰源（如多径衰落、阻尼、干扰等）接收到的总体信号功率。是一种通用的概念，而RSRP是在LTE中的概念。

## **RSSI**

（信号强度）（基站侧）

RSSI在无线网络中表示相对信号强度，不同设备之间的计算公式可能不一样,它随距离的增大而衰减,通常为负值,该值越接近零说明信号强度越高。RSSI持续过低，说明基站收到的上行信号太弱，可能导致解调失败。 RSSI持续过高，说明收到的上行信号太强，相互之间的干扰太大，也影响信号解调。

## **RSRP**

（参考信号接收功率）

RSRP：参考信号接收功率，是LTE小区网络中接收功率电平的测量值，平均功率是从单个参考信号接收的功率的测量值，值越大信号越好。

## **RSRQ**

（参考信号接收质量）

RSRQ（ReferenceSignalReceivingQuality）：表示LTE参考信号接收质量，这种度量主要是根据信号质量来对不同LTE候选小区进行排序。这种测量用作切换和小区重选决定的输入。RSRQ被定义为N\*RSRP/(LTE载波RSSI）之比，其中N是LTE载波RSSI测量带宽的资源块（RB）个数。RSRQ实现了一种有效的方式报告信号强度和干扰相结合的效果。

## SNR/RSSNR

（信噪比）

SNR是signal to noise ratio的缩写，即信噪比，它指规定条件下测得的有用信号电平与电磁噪声电平之间的比值。在任意点上有用信号的幅度与同一点上噪声信号的幅度之比，并用分贝(dB)表示。峰值与脉冲噪声相联系，有效值则与随机噪声相联系。一般是越大越好。RSSNR是LTE中特定的指标。

## SINR

（信号与干扰加噪声比）

SINR（Signal to Interference plus Noise Ratio）：表示接收到的有用信号的强度与接收到的干扰信号（噪声和干扰）的强度的比值。

## RXLEV

接收信号水平

## CQI

（Channel Quality Indicator）：CQI是用于衡量无线信道质量的指标。在LTE网络中，CQI用于反映下行链路的信道质量，它描述了物理信道的信号质量以及可用于传输数据的有效比特数。

## MEID

MEID是移动设备识别码（Mobil Equipment Identifer）是CDMA手机（目前是电信制式）的身份识别码。也是每台CDMA手机或通讯平板唯一的识别码。通过这个识别码，网络端可以对该手机进行跟踪和监管。

## SSB

SSB（Sync Signal Block）是在5G NR（第五代无线移动通信技术）中使用的同步信号块。

在5G NR系统中，SSB是用于网络搜索、小区识别和时间同步的重要信号之一。它包含在物理层的广播信道（PBCH）中，由基站周期性地广播到周围的设备。

SSB的作用是帮助设备进行初始接入和找到适合的小区。设备可以借助接收到的SSB来确定小区的频率、时域位置和其他相关参数，以与基站进行同步，并与网络建立连接。

## Beam\_num

表示当前邻区基站使用的波束的标识符。5G NR技术中，波束是用于无线通信的方向性天线的一个重要概念，它可以帮助优化无线信号的传输和接收。

波束编号是在通信系统中用于对不同的波束进行标识和区分的一种方式。波束（beam）通常指的是无线通信系统中发射或接收的窄束信号。每个波束都有一个唯一的编号，用于标识和管理通信系统中的不同波束。

波束编号的主要作用包括：

1. 波束管理：对于使用波束赋形技术的通信系统，波束编号可以用于管理不同的波束。系统可以根据需要动态地分配和调整波束，以实现更好的信号质量和覆盖范围。
2. 多用户干扰抑制：通过使用不同的波束编号，可以在多用户环境中实现波束间的隔离，从而减少相互之间的干扰。每个用户可以被分配到一个独立的波束，以提高信号质量和系统容量。
3. 智能天线系统：波束编号也用于智能天线系统中，使其能够跟踪和指向特定的用户或方向。通过选择正确的波束编号，智能天线可以针对性地发送和接收信号，增强信号覆盖和接收性能。

总之，波束编号在无线通信系统中起着重要的作用，可以实现对不同波束的管理、多用户干扰抑制和智能天线系统的操作。

主区（Primary Cell）作为移动设备连接的主要依赖小区，通常使用全向天线或广播信号来覆盖较广的区域。主区的目标是提供广泛的覆盖和基本的通信服务，因此不需要细分波束，也不需要波束编号。

为了提高系统容量和网络性能，现代无线通信系统中引入了波束成形（Beamforming）技术，通过将无线信号在特定方向上进行聚焦和增强的方式来提高无线信号传输的效率和质量。

邻区的波束编号可以用来指示具体的波束方向和覆盖角度，帮助移动设备进行更精确的邻区选择和切换。通过选择具有最佳波束指向的邻区，移动设备可以获得更好的信号质量和连接性能。

## Ssb\_id

<ssb\_id>：SSB标识符（SSB ID），指示邻区基站的具体SSB的标识。通过这个标识符，用户设备可以确定当前所连接的小区。

# 中文术语

## 空口

空口就是空中接口，**Air Interface**。基站到手机之间的空中'路径'就是我们所谓的接口，它定义了无线信号传输规范，包括频率、带宽、编码等等一系列内容。

## 帧

手机和基站进行通信，需要发送一系列数据，那么这一系列数据排好队，然后一个一个向基站发送，在时间上，这些数据是分开的，有规律的。这样'有组织有纪律'的'部队'，就是帧。

在时间域中，无线传输被组织成无线帧**radio frames、子帧subframes、时隙slots和符号symbols。**

## 干扰和噪声

在无线通信中，干扰（Interference）和噪声（Noise）是两个不同的概念，它们都可以对信号质量产生影响：

1. 干扰：干扰是指在通信信号传输过程中，来自其他源的电磁波或信号相互干扰的现象。干扰可以是有意或无意的。有意的干扰可能来自其他通信系统、设备或信号源，例如同频干扰、邻频干扰、多径干扰等。无意的干扰可能来自于外部环境或其他信号源，例如电源干扰、大气干扰、电子设备的干扰等。干扰通常导致信号的失真、误码率的增加以及传输性能的下降。

2. 噪声：噪声是指与有用信号不相关的随机电磁波或信号。噪声可以来自于电子元件的热噪声、天线的热噪声、大气噪声等。在接收端，噪声会被当作信号，在信号处理过程中引入额外的随机性。噪声导致信号的信噪比降低，影响了信号的可靠性和解码性能。

区别：

- 特征：干扰信号通常具有一定的结构和相关性，而噪声是随机的、无结构的。

- 影响：干扰会干扰信号的传输、导致误码率增加，而噪声会降低信号的信噪比、影响解码性能。

在无线通信中，对抗干扰和噪声的方法可能会有所不同。针对干扰，可以采取频率选择性、空域选择性或编码技术等方法进行干扰抑制。而对于噪声，通常可以通过信号增益、滤波和误差控制等方法来降低噪声的影响。

## 信道（Channel）

则更加广泛地涵盖了信息传输的整个通路，包括信号的传输、调制解调、编码解码、传输协议等。信道不仅仅表示物理层上的频率资源，还包括对信号进行处理和传输的各种技术和协议。

可以将信道视为通信链路的抽象表示，它包括了物理层、数据链路层和网络层等多个层次上的处理和传输。不同层次的信道对应着不同的处理和协议，包括信号调制解调、信道编码解码、传输错误检测和纠正、路由选择等。

## 频段（Frequency Band）

频段是指一段特定的连续频率范围，通常由最低频率和最高频率定义。频段通常用来描述可用的频谱范围，以供无线通信系统和设备使用。例如，2.4 GHz和5 GHz是常见的Wi-Fi频段，700 MHz和2.1 GHz是LTE移动通信的频段。

频段通常用于描述分配给特定通信系统的频率范围，而频带（Frequency Range）则可能更常用于一般的频率范围的描述。

特定的频段可能指的是用于蜂窝移动通信网络的频率范围，一个频带可以描述为5 GHz到6 GHz之间的频率范围，而不指定具体被用于什么通信技术。

## 频道（Channel）

频道，则表示在给定的频段内划分出的特定频率子集。频道是频段的一个子集，用于区分不同的信号或服务。通过在频段中划分不同的频道，可以同时支持多个无线通信连接或服务。每个频道具有特定的中心频率和带宽，用于无线信号的传输。

以Wi-Fi为例，2.4 GHz频段可以被划分为多个频道，例如频道1、频道6和频道11等。每个频道有一定的带宽和中心频率，用于Wi-Fi设备之间的通信。用户可以选择一个频道来与无线接入点进行连接。

频段是一个特定的频率范围，而频道是在频段内划分出的一个特定的频率子集。频段描述可用的频谱范围，而频道用于区分不同的无线通信服务或连接。

频道通常属于信道的一部分

最大的是信道，在信道上有频带表示一般的频率范围，频段表示特定的频率范围，在这段范围内有不同的频道

频段->运营商

频道->特定频道通信，避免干扰或冲突

## 小区（Cell）

小区是指一个特定的无线通信覆盖区域。在移动通信系统中，一个小区通常由一个基站或基站组成，负责提供无线信号覆盖和通信服务。每个小区拥有一个唯一的标识，通常使用一个唯一的小区ID或名称来识别。小区的大小和形状可以根据网络需求进行调整。

## 扇区（Sector）

扇区是一个更小的区域单元，它是一个小区的划分。每个小区可以被分成多个扇区，每个扇区由一个基站中的天线扇形覆盖区域组成。不同的扇区之间可能存在一定的重叠，目的是提供更好的无线信号覆盖和容量管理。扇区通常由扇区角度和方向来定义，例如120度或180度扇区。

## 锁频段

（Lock Frequency Band）是指将无线设备设置为只能在指定的频段范围内进行通信，而限制其不能跨频段进行通信。

在无线通信中，不同频段分配给不同的运营商或网络技术使用。锁频段的目的是限制设备只能连接到特定频段上的基站，以避免设备无意中切换至其他频段或与不兼容的基站进行通信。

锁频段可以用于几种情况：

1. 确保设备只连接到授权的运营商或指定的频段，以遵守特定的合规要求或服务协议。
2. 在特定的网络环境中优化设备连接，例如在拥挤的频段上选择较空闲的频段进行通信。
3. 防止设备切换至其他频段造成的连接中断或通信问题。

锁频段通常是由设备的操作系统或网络设置控制的，用户可以在设置中选择或配置要锁定的频段范围。

需要注意的是，锁频段可能会限制设备在其他频段上的通信能力和覆盖范围。因此，在锁定频段之前，应考虑到设备需要在哪些频段上进行通信，并确保所选择的频段适用于设备所需的通信要求。

## 强搜

（强制搜索）是指无线设备在当前信号较弱或没有信号的情况下，通过强制搜索来寻找可用的基站或网络。

当设备处于信号较弱的区域时，它可能无法自动连接到最优的基站或网络。这时，通过执行强制搜索，设备将主动搜索周围的基站或网络，以期找到更强的信号并建立连接。

强搜的过程可能包括以下步骤：

1. 设备向周围的基站或网络发送搜索请求。
2. 设备接收并分析接收到的搜索响应，包括各个基站或网络的信号强度、可用频段等信息。
3. 设备根据分析结果选择最强的信号，并尝试建立连接。
4. 如果成功建立连接，设备会与选定的基站或网络进行通信。如果连接不成功，设备可能会继续进行搜索直到找到可用的信号为止。

强搜对于在信号较弱或边缘区域的设备来说非常有用，能够提供更好的通信质量和连接稳定性。

需要注意的是，在进行强搜时，设备可能会消耗更多的电量和资源，因为它需要更频繁地搜索和与基站进行通信。此外，强搜也可能导致连接中断或延迟，因为设备在切换基站或网络时可能需要一定的时间。

## DRX

（Discontinuous Reception）：DRX是一种省电机制，在无数据传输时，手机可以进入睡眠状态以降低功耗。DRX周期性地唤醒设备以接收可能到达的数据，从而在保持较长待机时间的同时仍能保持对网络的连接。

## 脉冲模式

脉冲模式（Pulse Mode）是一种无线通信中常用的调制方式，它用于将数字数据转换为脉冲信号进行传输。

在脉冲模式中，数字信号被编码成短暂的脉冲形式，即高电平和低电平的突发信号。脉冲的特点是其持续时间很短，通常只有几纳秒到几微秒。短暂的脉冲表示数字数据中的1或0。

脉冲模式常用于不同的通信系统中，如雷达、红外通信、传感器网络等。它具有传输速率高、传输距离较短等优势，并且在某些特定环境中能够提供较好的抗干扰性能。

脉冲模式的传输方式可以是单极性脉冲或双极性脉冲。在单极性脉冲中，信号只有正脉冲或负脉冲，而双极性脉冲中，信号具有正负两种极性的脉冲。

需要注意的是，脉冲模式主要用于短距离的高速数据传输，不同于脉冲编码调制（PCM）等调制方式，后者则主要用于长距离的数字音频传输。

总之，脉冲模式是一种将数字信号编码成短暂脉冲信号进行传输的通信调制方式，常用于一些需要高速传输和较短距离的应用中。

## 频道切换 (Channel Switching)

在无线通信中，频道切换是指设备从当前频道切换到另一个频道的过程。这通常用于避免频谱干扰或更好地利用可用的频道资源。

## 信号强度和信号质量测试

路测中常常涉及对信号强度和信号质量的测试和测量。信号强度测试用于评估信号的接收强度，通常以信号强度指示器（RSSI）的形式报告。信号质量测试涉及诸如信噪比（SNR）、误码率（BER）、调制解调器状态等指标的测量。

## 小区和扇区切换测试

在蜂窝移动通信中，进行路测时通常会测试不同小区或扇区之间的切换性能。这包括评估切换过程的延迟、切换成功率和呼叫保持等因素。

## 数据速率测试

路测中还可以进行数据速率测试，以评估无线网络在特定位置的数据传输速率。这涉及使用特定的测试工具或应用程序来模拟数据传输，并测量传输速度和吞吐量。

## 干扰检测和分析

路测可以用于检测和分析无线网络中的干扰源。通过测量信号干扰水平、频率占用情况以及识别干扰源的类型和位置，可以帮助运营商优化网络性能和提供干净的信号环境。

## 话务量测试

路测还可以包括对基站的话务量进行测试和测量。这有助于评估无线网络在高负荷情况下的性能和容量。

## 功率控制 (Power Control)

功率控制是一种调整设备发送或接收信号功率的技术。通过控制发送功率，可以优化无线信号覆盖范围和传输质量，降低干扰，并延长设备的电池寿命。

## 自适应调制 (Adaptive Modulation)

自适应调制是一种根据当前信道条件和设备接收性能自动选择最佳调制方式的技术。通过选择适当的调制模式，可以在不同的信道环境下实现更高的数据传输速率和更低的误码率。

## 跳频 (Frequency Hopping)

跳频是一种通过在不同的频道之间进行快速切换来传输数据的技术。这有助于减少频谱干扰和提高数据传输的安全性。跳频通常用于蓝牙和无线局域网 (Wi-Fi) 等无线通信协议中。

## 扫频（Sequential Scanning）

扫频是按照一定的顺序依次扫描频率范围内的信号。通常是从低频到高频或从高频到低频的顺序进行扫描。扫频可以通过频谱分析仪或扫频仪等设备实现。扫频可以提供对频段内信号活动的全面了解，但可能需要较长的扫描时间，尤其在宽频带范围内。

## 随机扫描（Random Scanning）

随机扫描是在频率范围内以随机的方式扫描和监测信号。相对于扫频的顺序扫描，随机扫描不是按照预定的顺序进行扫描，而是随机选择频率来监测信号。随机扫描可以更快地探测到突发性信号活动或干扰源，但可能会因为随机性而无法获取到整体频谱的全面信息。

## 模块型号

SIMCOM ：8200G 8210C FG650（国产展锐（中低端），强搜）

H30只有FG650

## 5g模块中移动和广电共用一个基站，联通和电信共用一个基站

## 定位

相当于一个伪基站，可以让手机（或其他设备）连接到你的伪基站上去获取手机的信息，可以用于公安局或军队去搜索手机等，也可以获取手机位置但是移动不方便。向手机发送下行信号并获取手机的上行信号称为上号。

## 单兵

在定位的基础上去获取手机的具体位置。不发送信号只是接收定位设备发送的下行信号和手机发送的上行信号，称为锁定。可以确定手机的具体位置，更方便移动，且有天线方向限制。

## 工作流程

1. App（手机或上位机）Wifi（网线）连接定位（伪基站）设备
2. 目标设备（手机、车载等等）上号：目标与定位连接成功（通过imei）
3. app（手机或上位机）蓝牙（或Wifi、网线）连接单兵设备
4. 单兵通过获取目标设备和定位设备的信息锁定目标

工作目标：

通过移动单兵可以判断设备的远近

## UE（User Equipment）

用户设备，目标设备（手机等）

## 功放（功率放大器PA）（Power Amplifier）

是一种电子设备，用于将输入信号的功率放大到更高水平的设备。功放能够提供足够的电流和电压，以使信号能够驱动高负载和输出到更远的距离。

功放通常由放大器电路组成，其输入为低功率信号，通过放大器电路进行信号增益，并输出高功率的信号。功放一般用来驱动负载，如扬声器、天线、电机等。

功放应用广泛，例如：

音频功放：用于音响、电视、收音机等音频设备中，将低功率的音频信号放大至足够驱动扬声器的水平，以产生清晰、高质量的声音。

无线通信功放：用于无线通信系统，将发射器的低功率基带信号放大到适当的功率水平，以便在无线信号的传输过程中覆盖更大的距离或提供更好的信号质量。

射频功放：用于无线电、微波通信、雷达等高频应用，将射频信号放大到足够高功率，以满足长距离传输、高速数据通信或探测要求。

根据具体的应用需求和信号特性，功放可以采用各种不同的设计和技术，如晶体管功放、管子功放、集成电路功放等。这些功放可以根据功率级别、频率范围、效率等因素进行选择，以满足不同的应用要求。

## ADC（Analog-to-Digital Converter）

是一种将连续模拟信号转换为离散数字信号的电子设备或电路。它用于将实际世界中的模拟信号转换为数字形式，以便进行数字信号处理、存储、传输和分析等操作。

ADC的工作原理是将连续时间、连续幅度的模拟信号，按照一定的采样率进行离散采样，然后将每个采样点的幅度值量化为离散的数字数值。这样得到的数字信号可以用二进制表示，通过数字系统进行处理和操作。

ADC的主要功能是将模拟信号的幅度进行量化，并将其转换为数字形式。它通常包括采样、量化和编码三个主要步骤：

采样（Sampling）：ADC以一定的频率（采样率）对输入模拟信号进行离散采样，对连续信号在离散时间点上进行采样。

量化（Quantization）：采样得到的模拟信号值被量化为特定精度的数字数值。量化过程将连续的模拟信号幅度映射为离散的数字值，常用的量化方式包括线性量化、非线性量化（如μ-Law和A-Law等）。

编码（Encoding）：采样和量化后的数字化信号通过编码过程被转换为二进制码，以便在数字系统中存储和处理。

ADC有不同的类型和规格，包括抽样率、分辨率、速度和功耗等参数。不同应用场景和要求，可能需要选择不同性能和精度的ADC。

ADC在许多领域中得到广泛应用，包括音频处理、通信系统、测量仪器、传感器数据采集等。它是将模拟信号与数字系统有效集成和交互的关键组成部分。

## "单板"

通常指的是一块电路板或硬件模块，用于集成和实现特定功能或系统。该术语常常用于描述嵌入式系统、电子设备或计算机硬件中的主要组成部分之一。

单板通常由印制电路板（PCB）制成，上面集成了各种电子元件、芯片、接口和连接器等，并且经过布线和焊接的工艺。它们被设计和制造成一块完整的电路板，具备特定的功能和性能。

在一些应用中，单板可以是嵌入式系统的核心，包括处理器、存储器、输入输出接口以及其他必要的电子组件。在其他情况下，单板也可以指代特定的模块，如显示模块、通信模块或传感器模块等。

单板的设计和功能通常会根据特定应用或系统的需求而变化，以满足特定的功能要求和性能指标。它们可以是定制的、专用的，也可以是通用的、可扩展的，用于构建各种类型的电子设备和系统。

总之，"单板"指的是一块集成了电子组件和电路的电路板，用于实现特定功能或者作为系统的核心组件。

## 基带（Baseband）

是指在数字通信系统中，用于表示原始信号的频率范围。它是指没有经过调制的数字信号，通常是指在信号传输之前进行调制之前的信号。

在数字通信系统中，基带信号是指从信源（如语音、音频、视频等）获取的原始信号，它通常是连续的、模拟的信号。然后通过一系列的信号处理过程，将基带信号转换为数字信号，以便在数字通信系统中进行处理、传输和解码。

基带信号经过数字化之后，可以再经过一系列的调制过程，将其变换到合适的频率范围，以适应特定的无线通信信道和传输要求。这个过程涉及到将基带信号与载波进行调制，形成调制后的信号（中频信号或射频信号），然后通过无线传输将其发送出去。

在通信领域中，基带信号通常与射频信号对应。射频信号是指调制后的信号，它经过射频变频、放大、频率变换等过程，最终在无线信道中传输和接收。而基带信号是指尚未经过调制和变频的信号，用于表示数字化的原始信息。

总之，基带是指数字通信系统中用于表示原始信号的频率范围，是未经过调制和变频的数字信号。它经过一系列处理和调制过程后，最终转换为射频信号并在无线信道中传输。

## 基带处理器（Baseband Processor）

是指在无线通信系统中负责处理和调度数字信号的关键组件。它主要用于将数字信号转换为模拟信号，执行调制和解调、信道编解码、功率控制等一系列基带信号处理操作。

基带处理器通常位于无线通信设备（如手机、调制解调器等）中的主处理器或专用芯片集成电路中。它负责处理数字信号，执行各种算法和协议，以实现可靠的通信。

基带处理器的功能包括但不限于以下几个方面：

调制解调：将数字信号转换为模拟信号进行调制，或将接收到的模拟信号进行解调。

信道编解码：对数字信号进行编码和解码，以提高数据传输的可靠性和纠错能力，例如使用前向纠错编码（Forward Error Correction）。

功率控制：根据信道质量和系统需求，对发送功率进行控制和调整，以保证合适的信号传输功率。

数据调度：根据通信协议和服务质量要求，对传输的数据进行调度、管理和优先级控制。

时钟和定时：提供精确的时钟信号和定时机制，以同步和协调通信系统中的各个部分，确保数据传输的准确性和同步性。

断线重连：负责处理信号弱或中断时的断线重连操作，以保持稳定的通信连接。

基带处理器的性能和功能对于无线通信系统的质量和性能至关重要。它的设计和实现需要考虑诸多因素，如处理能力、功耗效率、算法优化、兼容性等，并根据不同无线通信标准和技术要求进行适配和优化。

# 常用配置

**热点配置：**

**定位**：G051C060015

**单兵**：G10C\_025

**定位新板**：G70\_123

**4测向** G10TS

**G758** G051C100267

**密码**：12345678

定位设备：G758、G73

单兵设备：G10、G581

**查imsi只有用小米上的软件查才可以**

我的移动5g无限流量卡imsi：

我的电信4g家庭卡9496 imsi：460115057774632

我的移动4g卡1773imsi：460077121546407√

凯：460076610502765

借的广电卡4489E：460013414961569

借的广电卡2739E：460015456226838

借的电信卡2943C：460115024457606

借的移动卡80526：SMSDONE 460074536187708

借的移动卡54493：460004393256005

46000移动B 3\ 8\34\39\40\41 N28\41\79

46001联通B1\3\5\8 N1\N3\ 78 (B41已停用变成移动的了)

46011电信B1\3\5\8 N1\N3\ 78

46015广电B 3\ 8\34\39\40\41 N28\41\79

移广 B3/B8部分：(freq > 1709 && freq < 1735) || (freq > 1804 && freq < 1830) || (freq > 888 && freq < 904) || (freq > 933 && freq < 949)

4g:

B1-B8 FDD

B34-B41 TDD

5g:

N1\N28 FDD

N41\N78\N79 TDD

**通道对应频点**

车载2+2：

通道一：N41

通道二：N1

通道三：N78/N79

通道四：N28

B97502：

通道一：N41\78\79

通道二：B3\5\8\次B40

通道三：B1\N1\28

通道四：B34\39\40\41\次B3

3G758测向：

1：N78\79

2:B1

3:N1

4:B3

5:N28\N78次

6:B40次

7:N41

8:B40

9:N3

10:B39

11:B5\B8

12:B34\B41

**Pci**

5gpci：1-1007 上次用的：300

4gpci：1-50x

**Prb\_num:**

5g:4 4g:2

**MobaXterm软件使用**

IP:192.168.1.33

账户：linaro

管理员：su 密码：root

指令：

查看xlog：tail -f /home/log/xlog.txt

查看xmessage： tail -f /home/log/oam\_msg.log

查看配置信息： vim /home/config/wpa\_supplicant.conf或vim /home/config/top\_cfg.txt

开假gps：echo 1 > /run/fake\_gps\_state

插入模式：i

保存：:wq

gps是通过有线的链接到内部才能成功连接

空口能连接成功是因为有同事开了范围内的频点，通过墙上的信号发射器连接成功

5g和4g只和cpu芯片有关系，和电话卡无关

频段 频点 Center Frequency（MHz）

N1 427250

N3 361000~376000

N41 504990

N79 723360

N78 627264（电信在用的可能比较好）

N28 154810

B1(FDD) 100 2120

B3(FDD) 1825 1867.5

B5(FDD) 2452 874.2

B8(FDD) 3683 948.3

B34(TDD) 36275 2017.5

B39(TDD) 38400 1895

B40(TDD) 38950 2330

B41(TDD) 40936 2624.6

N1联通电信？5g

N3联通电信

N41、n79 移动5g

N78 联通电信5g

N28广电5g

B1-B8 联通电信4g

B8-B41 移动4g

**软件版本：**

G73\_V1R3\_20230908\_1500 R3只支持4+4或者5+4，不支持5+5或4+5双通道

（通道一可以4、5g，通道二只能4g） 不支持双FDD

R2 只能用5g

**H20和G73**

G367

G732D是单设备便携

G735D是双设备

上不了号是因为没锁到频点，要锁一下频点。然后锁各个运营商的频点

**PA功放配置**

初始化：

一般有4的才是高发高收，默认是低发高收  
低发高收的3、4配2

高发低收的3、4配1

高发高收的3配2,4配1

16位功放后面8位自动补0

**Sdk压缩包密码：**

simple2021\*\*

simpie666

**黑匣子密码**

1234

**Wifi密码**

0020161123

**密码：**

Moba：Xpwg73

**电源接法：**

G73红色靠柱子

G758黑色靠柱子

# 指令大全

public static class **DW\_State** {

public final static int NONE = -1; // 不在线

public final static int IDLE = 0; // 空闲

public final static int BLACKLIST = 1; // 配置黑名单

public final static int GNB\_CFG = 2; // 定位参数配置

public final static int CFG\_TRACE = 3; // TRACE|CATCH|CONTROL，但还未启动

public final static int TRACE = 4; // 定位中

public final static int CATCH = 5; // 侦码中

public final static int CONTROL = 6; // 管控中

public final static int STOP = 7; // 结束 TRACE|CATCH|CONTROL

public final static int UPDATE = 8; // 升级中

public final static int GET\_LOG = 9; // 读取LOG

public final static int REBOOT = 10; // 重启中

public final static int PHY\_ABNORMAL = 11; // 基带异常

public final static int CHANGE\_WORK\_MODE = 12; // 切换工作模式：单双通道

public final static int FREQ\_SCAN = 13; // 扫频中

public final static int GETOPLOG = 14; //

}

public static class **DB\_State** {

public final static int NONE = 0; // 开机或连接中

public final static int READY = 1; // 准备就绪

public final static int START = 2; // 启动干扰|单兵

public final static int JAMING = 3; // 干扰中

public final static int STOP = 4; // 结束干扰

public final static int REBOOT = 5; // 重启

public final static int GETLOG = 6; // 读取LOG

public final static int UPGRADE = 7; // 升级

public final static int PWR\_DETECT = 8; // 单兵工作中

}

public static class **MsgType** {

public static final int GR\_NONE = 65535; // IDLE

public static final int GR\_MSG\_HELLO = 0x0001; 1

public static final int GR\_MSG\_SET\_TIME = 0x0002;

public static final int GR\_MSG\_GET\_VERSION = 0x0003;

public static final int GR\_MSG\_BT\_NAME = 0x0004;

public static final int GR\_MSG\_WIFI\_CFG = 0x0005;

public static final int GR\_MSG\_REBOOT = 0x0006; 6

public static final int GR\_MSG\_IMG\_UPGRADE = 0x0007;

public static final int GR\_MSG\_GET\_LOG = 0x0008;

public static final int BT\_MSG\_DEV\_NAME = 0x0009;

public static final int GR\_MSG\_START\_JAM = 0x0020;

public static final int GR\_MSG\_STOP\_JAM = 0x0021;

public static final int GR\_MSG\_GET\_JAM = 0x0022;

public static final int GR\_MSG\_START\_SG = 0x0023;

public static final int GR\_MSG\_STOP\_SG = 0x0024;

public static final int GR\_MSG\_START\_POS\_SCAN = 0x0030; 48

public static final int GR\_MSG\_START\_PWR\_SCAN = 0x0032; 50

public static final int GR\_MSG\_STOP\_PWR\_SCAN = 0x0033; 51

public static final int GR\_MSG\_SCAN\_REPORT = 0x0034; 52

public static final int GR\_MSG\_POWER\_REPORT = 0x0035; 53

public static final int GR\_MSG\_RX\_GAIN = 0x0040; 64

public static final int GR\_MSG\_GPIO\_CFG = 0x0041;

public static final int GR\_MSG\_DATA\_FWD = 0x012D;

}

## Cmd\_type

public class **DWProtocol** {

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

public static final int XMSG\_T\_OAM\_CFG = 0x30;

public static final int XMSG\_T\_OAM\_APK = 0x31;

public static final int XMSG\_T\_OAM\_BT = 0x32;

public static final int XMSG\_T\_OAM\_CGI = 0x33;

public static final int XMSG\_T\_OAM\_METH = 0x34;

public static final int OAM\_ACK\_OK = 0; //指令配置成功返回值

public static final int OAM\_ACK\_ERROR = 1; //指令配置失败通用返回值

public static final int OAM\_ACK\_E\_PARAM = 2; //指令配置失败参数异常

public static final int OAM\_ACK\_E\_BUSY = 3; //指令配置失败系统忙异常

public static final int OAM\_ACK\_E\_TRANSFER = 4; //指令配置失败传输异常

public static final int OAM\_ACK\_E\_SYS\_STATE = 5; //指令配置失败系统状态异常

public static final int OAM\_ACK\_E\_ASYNC\_FAIL = 6; //指令配置空口同步失败(10号消息)

public static final int OAM\_ACK\_E\_GPS\_UNLOCK = 7; //指令配置GPS同步失败(10号消息)

public static final int OAM\_ACK\_E\_HW\_CFG\_FAIL = 8; //指令配置硬件配置异常

public static final int OAM\_STR\_MAX = 32;

public static final int MAX\_TAC\_NUM = 6; //tac 递增上限100

public static final int MAX\_IMSI\_LEN = 16; /\*IMSI 数据长度\*/

public static final int MAX\_IMSI\_USE\_LEN = MAX\_IMSI\_LEN - 1; /\*有效长度\*/

public static final int MAX\_TARGET\_UE\_NUM = 3;

public static final int MAX\_BLACK\_IMSI\_NUM = 100;

public static final int MAX\_DROP\_SAVE\_IMSI = 20; // 下拉菜单最多保存20个历史数据

public static final int EXT\_GPIO\_CNT = 8; // PA 8个端口

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

public static final int UI\_NONE = 65535; // IDLE

public static final int UI\_2\_gNB\_HEART\_BEAT = 1; // APP发送心跳到单板

public static final int UI\_2\_gNB\_VERSION\_UPGRADE = 3; // 版本升级

public static final int UI\_2\_gNB\_GET\_LOG\_REQ = 4; // 获取基带板log，获取后将清除单板上的log

public static final int UI\_2\_gNB\_WRITE\_OP\_RECORD = 5; // write operation record

public static final int UI\_2\_gNB\_GET\_OP\_LOG\_REQ = 6; // get operation log

public static final int UI\_2\_gNB\_DELETE\_OP\_LOG\_REQ = 7; // delete operation log

public static final int UI\_2\_gNB\_SET\_TIME = 9; // 单板起来后进行配置

public static final int UI\_2\_gNB\_CFG\_gNB = 10; // 可多次配置，例如TA改变

public static final int UI\_2\_gNB\_LTE\_CFG\_gNB = 110; // 4G 可多次配置，例如TA改变

public static final int UI\_2\_gNB\_SET\_BLACK\_UE\_LIST = 11; // 黑名单，可多次配置，每次覆盖，最多8个UE

public static final int UI\_2\_gNB\_SET\_TX\_POWER\_OFFSET = 12; // 可多次配置

public static final int UI\_2\_gNB\_START\_CATCH = 13; // 帧码。与定位互斥

public static final int UI\_2\_gNB\_STOP\_CATCH = 14; //

public static final int UI\_2\_gNB\_START\_TRACE = 15; // 定位。与帧码互斥。支持一个目标UE。

public static final int UI\_2\_gNB\_STOP\_TRACE = 16; // 停止5G定位

public static final int UI\_2\_gNB\_START\_LTE\_BLACK\_UE\_LIST = 111; // 定位4G

public static final int UI\_2\_gNB\_START\_LTE\_TRACE = 115; // 定位4G

public static final int UI\_2\_gNB\_STOP\_LTE\_TRACE = 116; // 停止4G定位

public static final int UI\_2\_gNB\_REBOOT\_gNB = 17; // 重启

public static final int UI\_2\_gNB\_QUERY\_gNB\_VERSION = 18; // 获得版本信息，可多次请求

public static final int UI\_2\_gNB\_WIFI\_CFG = 20; // 重启设备生效

public static final int UI\_2\_gNB\_START\_CONTROL = 30; //

public static final int UI\_2\_eNB\_START\_CONTROL = 130; //

public static final int UI\_2\_gNB\_STOP\_CONTROL = 31; //

public static final int UI\_2\_eNB\_STOP\_CONTROL = 131; //

public static final int gNB\_2\_UI\_REPORT\_UE\_INFO = 103; // 定位上报

public static final int gNB\_2\_UI\_REPORT\_LTE\_UE\_INFO = 203; // 4G定位上报

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

public static final int UI\_2\_gNB\_OAM\_MSG = 1000;

public static final int OAM\_MSG\_SET\_BT\_NAME = 201;

public static final int OAM\_MSG\_GET\_METH\_CFG = 202;

public static final int OAM\_MSG\_SET\_METH\_CFG = 203;

public static final int OAM\_MSG\_GET\_FTP\_SERVER = 204;

public static final int OAM\_MSG\_SET\_FTP\_SERVER = 205;

public static final int OAM\_MSG\_GET\_GPIO\_MODE = 206;

public static final int OAM\_MSG\_SET\_GPIO\_MODE = 207;

public static final int OAM\_MSG\_GET\_SYS\_INFO = 208;

public static final int OAM\_MSG\_SET\_SYS\_INFO = 209;

public static final int OAM\_MSG\_ADJUST\_TX\_ATTEN = 210;

public static final int OAM\_MSG\_SET\_GPS\_CFG = 211;

public static final int OAM\_MSG\_SET\_DUAL\_CELL = 212;

public static final int OAM\_MSG\_SET\_RX\_GAIN = 214;

public static final int OAM\_MSG\_GET\_SYS\_LOG = 215;

public static final int OAM\_MSG\_SET\_FAN\_SPEED = 216;

public static final int OAM\_MSG\_GET\_CATCH\_CFG = 220;

public static final int OAM\_MSG\_SET\_GPS\_IO\_CFG = 224;

public static final int OAM\_MSG\_GET\_GPS\_IO\_CFG = 225;

public static final int OAM\_MSG\_START\_FREQ\_SCAN = 226;

public static final int OAM\_MSG\_FREQ\_SCAN\_REPORT = 227;

public static final int OAM\_MSG\_STOP\_FREQ\_SCAN = 228;

public static final int OAM\_MSG\_SET\_JAM\_ARFCN = 229;

public static final int OAM\_MSG\_START\_TD\_MEASURE = 230;

public static final int OAM\_MSG\_FWD\_UDP\_INFO = 231;

public static final int OAM\_MSG\_START\_BAND\_SCAN = 232;

public static final int OAM\_MSG\_FAN\_AUTO\_CFG = 233;

public static final int OAM\_MSG\_GET\_GPS\_CFG = 236;

public static final int OAM\_MSG\_CFG\_PA\_TRX=237;

public static final int OAM\_MSG\_I2C\_RW = 240;

public static final int OAM\_MSG\_RW\_USER\_DATA=242;

Dispatch DW?DB?

11,11,a5,5a,

3b,00,00,00,

28,00,00,00, length

35,00,00,00, cmd\_type

00,00,00,00, result

01,00,00,00, lock

5e,00,00,00, rsrp

00,00,00,00,

00,00,00,00,

33,33,a5,5a