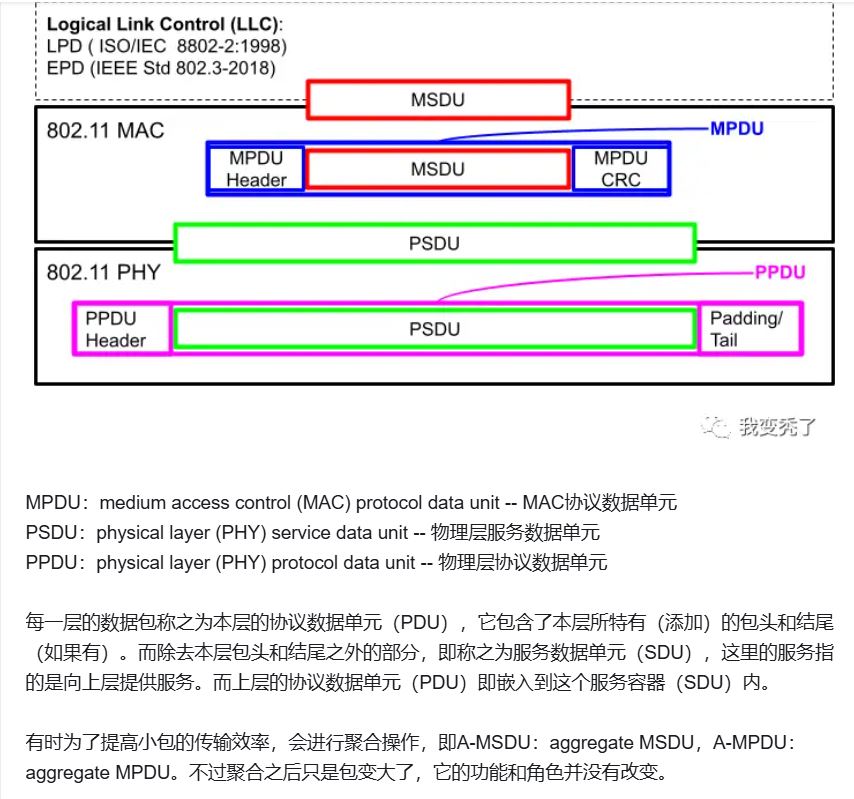
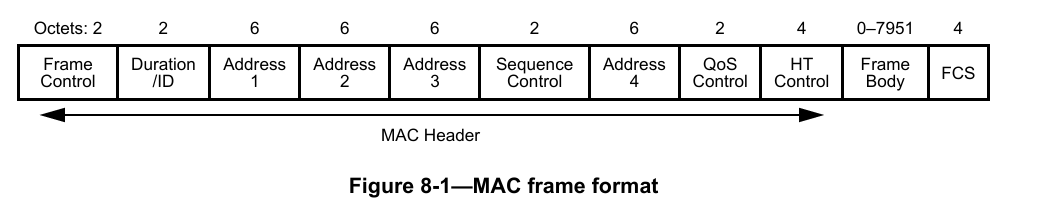
一、发射，接收，等待状态切换

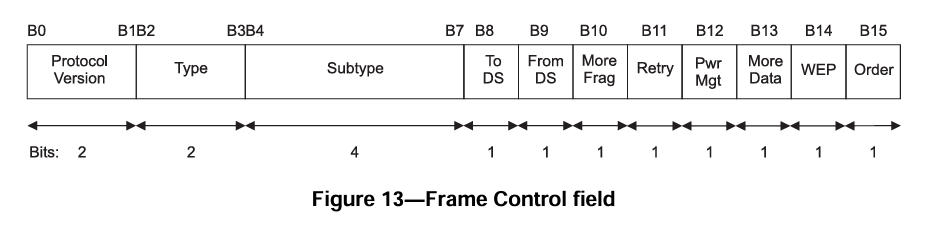
二、物理层发射机。

三、物理层接收机。



MAC层主要格式



FrameControl主要规定帧类型、分为管理帧、数据帧、控制帧，用于AP/STA信标帧、接入、认证、连接等，控制帧用于控制对物理信道的占用，发送方向、帧聚合是否有更多分片、是否是重传帧、电源省电模式、缓存中是否有更多数据、是否用WEP加密、是否为数据帧。Tpye和Subtype规定帧类型，需要信息具体查表建议80211-2012（修订后的80211n）  


Duration/ID用于更新NAV向量，AID用于表示AP与STA之间的连接ID

Address：BSSID，Destination Adress，Source Adress，Reciever Adress，Transmitter Adress。不一定全都有。

Qos表示数据包优先级

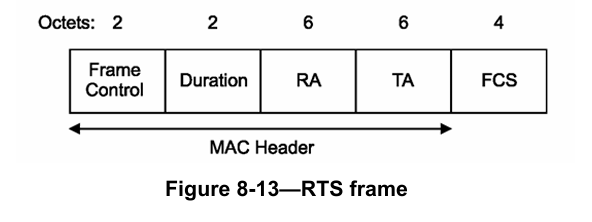
HtControl表示对HT模式的一些控制

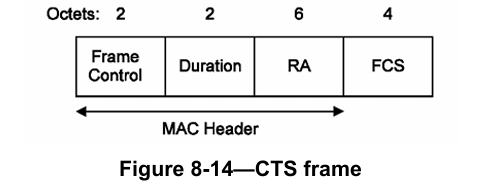
FrameBody最大长度在不同版本下不同，80211a/g最大长度为2312

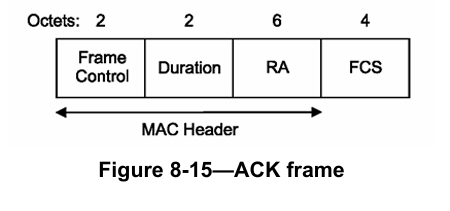
Sequence Control：分片序号和队列序号。

FCS：校验

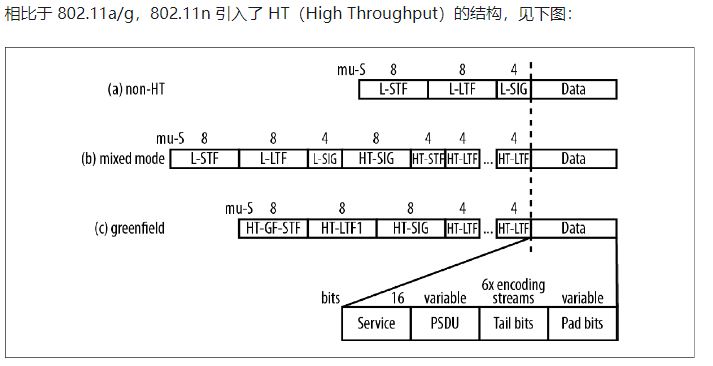
特殊帧有具体的格式如CTS、RTS、ACK，如最重要的RTS、CTS、ACK具体需要查看协议。

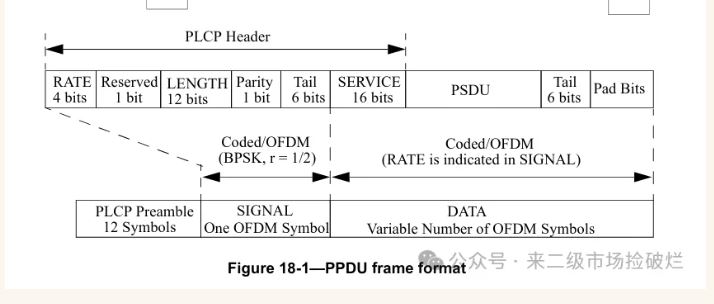






物理帧主要格式：





**PLCP**为前导训练序列，L\_STF为频域生成,调整到对应子载波位置上作64点IFFT，截取前16个周期时域点，10个sym，10\*16samples；L\_LTF为频域生成调整到对应子载波位置上作64点IFFT，2个sym，需要截取1/2循环前缀32点，共160samples，共10\*800ns+8us = 16us。

**SIGNAL**为各版本WIFI共同继承的L\_SIGNAL。1个sym，(24\*2+4+12)+16=80samples。bit0-3表示RATE传输速率，HT模式默认6Mbps，bit4保留为0，bit5-16,LENGTH表示无符号MAC请求传输的PSDU的字节数，bit17为前17个的偶校验位，LSB先发送，6个bit的tail保留为0,不进行加扰，按卷积效率1/2，bpsk调制，不进行打孔，以6Mbps的速率发送。4us。

**HT\_SIGNAL**，2个sym，160samples，48个数据点(96个编码点)如果检测到rate为6M，检查L-SIG和HT-SIG的BPSK星座点，L-SIG为0,1同相，HT-SIG为正交，检测正交分量样本多于同相，

MCS: only supports 0 - 7.

CBW 20/40: channel bandwidth. OpenOFDM only supports 20 MHz channel (0).

Reserved: must be 0.

STBC: number of space time block code. OpenOFDM only supports 00 (no STBC).

FEC coding: OpenOFDM only supports BCC (0).

Short GI: whether short guard interval is used.

Number of extension spatial streams: only 0 is supported.

CRC: checksum of previous 34 bits.

Tail bits: must all be 0

MCS（7bit）：0-76中的某一种来表示发送数据字段的调制编码方案

20/40MHz（1bit）：用来指示发送的是20MHz还是40MHz带宽。

长度（16bit）：指示数据的长度

平滑（1bit）：在进行Tx波束成型和空间扩展后，得到发射机和接收机之间的信道可以超过800ns。高延迟传输可解除相邻子载波的相关性。某些Tx波束成型也会导致相邻子载波间相位的不连续。在使用子载波平滑技术时，这两种情况会削弱信道估计。在这两种情况下，发射机应该将平滑比特设置为0，以通知接收机只是用每载波信道估计。

非探测（1bit）：设为0时发送的是探测分组。探测分组用于收集Tx波束成型和链路适应的信道状态信息。为了将探测扩展到数据字段之外的额外空间域上，扩展空间流数字段所设的值大于0。

保留位（1bit）

聚合（1bit）：表示有效载荷包含单个MPDU（为0）或一个MPDU聚合（为1）。

STBC（2bit）：表示STBC操作的维度

FEC编码（1bit）：为0时表示数据为BCC编码，为1时表示数据为LDPC编码。

短GI（1bit）：为1时表示使用400ns短保护间隔，为0时表示使用800ns标准长保护间隔。

扩展空间流数（1bit）：见非探测描述。

CRC（8bit）：生成多项式为G(D)=D^8+D^2+D^1+1

**HT\_STF、HT\_LTF，**1个sym,5\*16=80samples，用于改进mimo系统中的自动增益控制，用于MIMO系统的调整，20Mhz序列和l-stf一样，40Mhz通过将20MHz的序列幅值并旋转上半部分的子载波

暂时没有实现40Mhz的，不用mimo

**DATA**用于PSDU的数据填充，是实际传输的上层数据。SERVICE+DATA+TAIL+PAD。SERIVICE为16bit，bit0-6 set to 0，用于同步解扰器;bit7-15 reserved to 0。DATA就是PSDU填充，TAIL共6bit，set to 0，用于接收机卷积器复位。PAD用于填充数据到整OFDM符号数，80211n及之前即64的倍数。

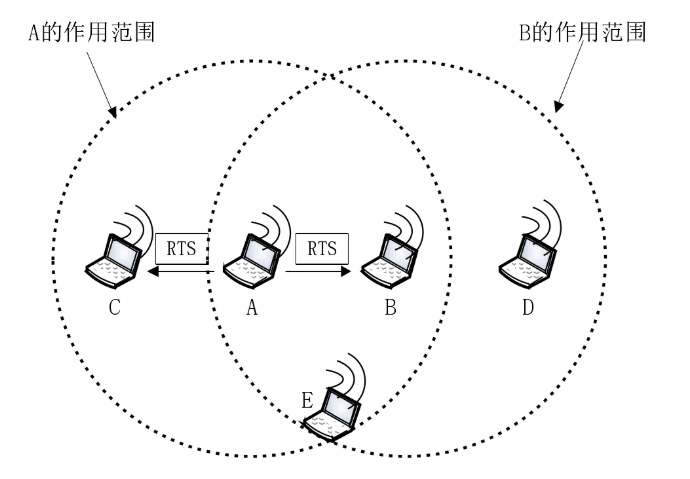
这里的数据组帧是最后的OFDM符号组帧，不同域的数据不一定经过完整信道编码，如SIGNAL不进行加扰等。

CSMA/CA的理解：

Ad Hoc网络中所有的节点地位平等，节点不仅包含普通移动终端所需的功能，而且具有分组转发能力，作为一个多节点之间都能互相通信的通信系统，工作在同一频率下，且能够实现多跳功能，需要工作在tdd半双工下。空间上某一频率/频带的电磁场信道只有一个，如果没有一个公平且合理的占用信道方式，各自管各自的传输，信号之间就会发生很多碰撞，传输效率很低。MAC协议大致可以分为基于竞争和基于调度两大类，LTE作为调度的代表，WIFI则成为了竞争的代表。

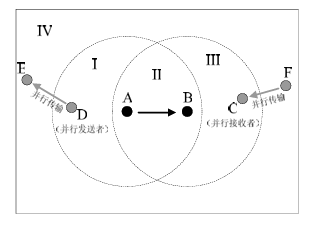
为了达到以合理的方式占用信道，每个节点在占用信道前都会先进行物理上的载波侦听，如果在当前频率，当前时间上有一定强度的信号，认为信道忙，进行静默等待，信道空闲后进行一个随机时隙长度的退避，如二进制指数随机退避，开始竞争信道。但这种完全随机的占用信道也会产生很多碰撞，所以在协议上进行了人为的虚拟载波监听，每个MAC上都会携带Duration字段，内容是下一个MAC帧的持续时间，用于指示占用信道的时间，其他节点在解析出Duration后用于更新自己的NAV倒数，只有在NAV为0且信道空闲后才能进行随机退避。

另外，在tdd下有暴露站和隐藏站的问题



隐藏站问题下，C向A发送数据，但是B听不到C的数据，认为信道空闲，也向A发送数据，导致A接收数据一直错误。所以A在收到C发送数据请求RTS后，进入接收C的数据状态前，广播一个我要准备接收C的指令CTS，B听到后CTS后进入静默状态开始倒数NAV，C在接收CTS后赶紧开始发送数据，一个正常的数据交换都会有RTS-CTS-DATA-ACK四次握手。CTS/RTS确实也某种程度上解决了隐藏站问题。但是，如果B在收A的CTS时正好有D发送信号，B会认为信道冲突且解不出CTS，只会等待时间后进行随机退避，可能干扰C向A传输DATA，所以引入了分fragment传输，降低因冲突产生的误码。但多个ACK降低信道占用率

暴露站问题下，A在向B发送数据，D在听到A在发送数据后进入静默，即使有向E发送数据的需要也需要静默，但D向E发送数据是不会影响A的，而且F向C也应该不受影响。从某种意义上讲，RTS/CTS反而造成了暴露站问题。



收发双方在成功完成RTS/CTS握手后，DATA/ACK帧交换无法100%的成功。CSMA/CA协议之所以在大负载的情况下性能会急剧恶化，一个重要的原因就是，随站点数和负载的增加，共享信道的竞争程度将增大，这样上述问题发生的可能性就会大大增加，从而导致数据帧或者ACK帧的接收被冲突。

可以归结于两句话：同个时刻下，一个接收站的通信范围内只允许一个发送站发送数据有效；一个发送站的通信范围内只允许一个接收站接收数据有效。

RTS-CTS-DATA-ACK的多次握手会导致：两个节点想要正常通信，必须保证一个节点不被其范围内的节点干扰，且另一节点不被他范围内的节点干扰，任何过程被干扰都会导致握手失败，引发不同的后果，这也成为竞争式MAC应用在移动自组网的限制。

ZYNQ PS 接口

S\_AXI\_ACP：接openwifi：interconnect2 控制dma1，用于side\_ch，用于应用层sdrctl工具探针数据采集

S\_AXI\_HP3：接openwifi：interconnect0 控制dma0，用于tx\_intf，存储发射数据

M\_AXI\_GP0：控ADI的axi\_ad9361IP核，axi\_gpreg，一般gpreg

M\_AXI\_GP1：控主模块的七个大IP

IRQ\_F2Q：控制主模块七个IP核中断

SPI：目前实际只是用了一个SPI总线：实际使用4线SPI：SPI0\_SCLK\_O，SPI0\_MOSI\_O(连接至XPU选择发送指令，由ad9361驱动或直接写入写24bit的指令控制本振分频器的开关，实现快速切换的tdd工作模式)，SPI0\_MISO\_I(直连9361)，SPI0\_SS\_O

OPENWIFI主模块接口：

S00\_AXI：接PS的M\_AXI\_GP1

M00\_AXI：接PS的S\_AXI\_ACP3

M00\_AXI1：接S\_AXI\_HP3

Input:

adc\_clk：40Mhz，从AXI\_ad9361核l\_clk100Mhz（查询IP手册后固定为160M，输入160Mdata\_clk）时钟4分频，用于同步处理adc数据

adc\_data[63:0]：ad9361芯片工作于lvds模式双发双收，经axi\_ad9361处理打包为64位数据，[I0,Q0,I1,Q1]

adc\_rst：adc复位

adc\_valid：adc有效

ext\_reset\_in：PS外部复位

gpio\_status[7:0]：ad9361芯片实时状态，用于计算和校准实际rssi

m\_axi\_mm2s\_aclk：经l\_clk100Mhz分频倍频后而来，用于主模块处理adc数据，l\_clk分频倍频后为100Mhz

spi：三线，片选spi0\_csn，时钟spi0\_sclk，主出从入spi0\_mosi

output：

dac\_data[63:0]：最后给axi\_ad9361分解为2路iq信号的lvds信号的dac数据

dac\_valid：dac有效

中断：mm2s\_inrout，mm2s\_introut1，rx\_pkt\_intr，s2mm\_introut，s2mm\_introut1，tx\_itrpt，

Spi0\_sdo\_o：4线spi的主出从入，最后接到ad9361。

七个主模块接口

OPENOFDM\_TX

AXI总线用于应用层配置参数

INPUT：

bram\_din[63:0]：来自TX\_INTF数据选择，队列管理后，交给TX待发射的数据

phy\_tx\_start：来自TX\_INTF，数据使能

phy\_tx\_arestn：来自PS的异步复位

result\_iq\_hold：来自TX\_INTF的tx\_hold

OUTPUT：

phy\_tx\_done：发射结束

phy\_tx\_started：发射已开始

result\_i：最后调制后的I路数据

result\_q：最后调制后的Q路数据

TX发射主要状态机

State1：signal和ht\_signal域组帧 State11为子状态机，为data域组帧

state2：加扰后的卷积、打孔、交织、导频插入和IFFT

state3：最后整个数据的输出

plcp\_bit\_cnt：用于计数PLCP头的比特位置。

psdu\_bit\_cnt：计数PSDU（数据部分）的比特数。

ofdm\_cnt\_FSM和ofdm\_cnt\_FSM2：分别记录不同状态机处理的OFDM符号数量。

dbps\_cnt\_FSM1和dbps\_cnt\_FSM2：记录每个OFDM符号中的数据比特数。

OPENOFDM\_RX

模块主要分为一个看门狗和dot11接收机

Sync\_short:

1. 输入IQ样本经过幅度平方计算mag\_sq\_inst，得到瞬时能量mag\_sq。
2. 对能量进行移动平均处理mag\_sq\_avg\_inst，得到平均能量mag\_sq\_avg。
3. 输入样本经过延迟线fifo\_sample\_delay延迟一定样本数，得到sample\_delayed。
4. 将当前样本与延迟后的样本共轭相乘，计算延迟相关乘积prod。
5. 对相关乘积结果进行双通道移动平均，得到prod\_avg，并计算其幅度delay\_prod\_avg\_mag。
6. 将平均能量mag\_sq\_avg进行阈值缩放，不同场景用不同阈值，得到prod\_thres，作为检测阈值。
7. 比较相关乘积的幅度与阈值，当超过阈值时开始计数，满足一定条件（如持续计数超过min\_plateau）后触发短前导码检测。

在always块中，处理逻辑主要围绕检测相关乘积的幅度是否超过动态阈值，并通过计数机制确保信号持续满足条件。其中，pos\_count和neg\_count用于跟踪正负样本的数量，确保前导码中存在正负交替变化，避免误检。当满足最小正负计数和平台计数时，输出short\_preamble\_detected，并更新相位偏移phase\_offset。

判断条件：信号有正有负，滑16点窗自相关幅度大于信号强度阈值缩放点数大于100

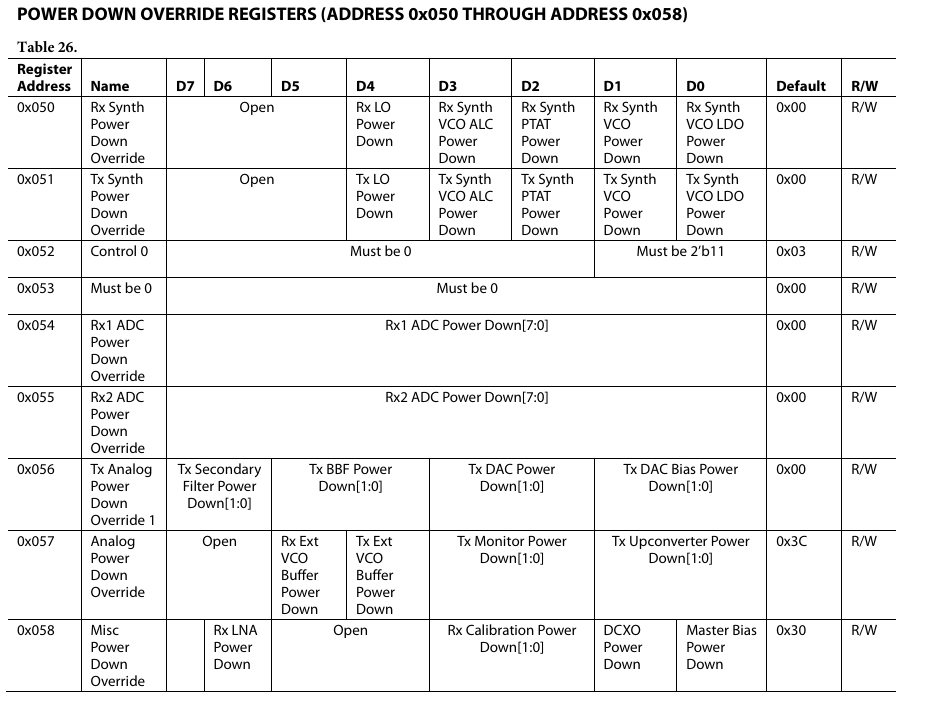
Tsf\_timer：

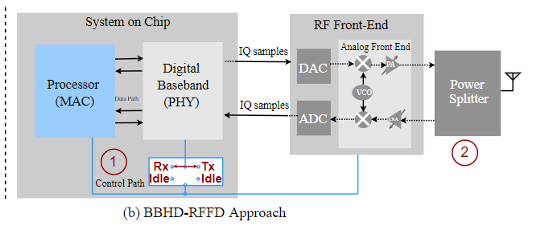
用于产生一个1MHz的脉冲信号用于同步，64位的计数器用于产生时间戳

XPU中SPI模块，交换MOSI输出数据控制权，写入特定SPI数据控制收发切换

《AD9361\_Register\_Map\_Reference\_Manual\_UG-671》《AD9361\_Reference\_Manual\_UG-570》

24’h008A01和24‘h088A01，data[0] = 1表示写入，data[3:1] = 000表示transfer 1 byte，data[5:4] = 00保留字不使用，data[15:6] = 0x051表示对该地址操作，写入00或10控制本振压控振荡器开关。根据论文《Achieving Self-Interference-Free Operation on》，《An\_Approach\_to\_Achieve\_Zero\_Turnaround\_Time\_in\_TDD\_Operation\_on\_SDR\_Front-End》《Improved TDD operation on Software-Defined Radio platforms towards》收变到发状态需要640ns(480ns以50M写入24位数据+160ns混频器开启时间)，发变到收需要480ns，一个wifi短训练序列是800ns，可能会让第一个序列不完整？





CCA是物理上进行信道评估，根据实时计算出的rssi、发射机状态还有一些接收状态给出物理上信道空闲的信号，NAV是MAC上对信道的预约机制，根据MAC帧的duration对NAV进行倒数和更新。NAV和物理上都空闲，表明可以进行csma/ca的随机退避选择。

一般来说，sifs = 5G信道?16：10，表示的是最短帧间间隔，用于一些回应高优先级的MAC帧，用于高优先级帧的快速响应，确保关键控制帧（ACK回应、RTS/CTS握手，PS-POLL省电模式缓存数据发送，大数据包分片传输）能够优先抢占信道，从而避免冲突并提高传输效率，考虑的是aRxRFDelay(射频接收信号) + aRxPLCPDelay （捕获、头定时解析等）+ aMACProcessingDelay + aRxTxTurnaroundTime，。SIFS的长度在所有 帧间间隔里面最短，其目的就是要使处于帧交换序列中的站点具有最高的优先级 接入信道，保证帧交换序列不会被中断或打乱。

Slot\_time = 5G信道？9：（短slot？9：20），aCCATime + aRxTxTurnaroundTime + aAirPropagationTime + aMACProcessingDelay

difs = sifs + 2slot\_time，用于正常发送数据前的倒数，通常为34（16+18）或50（10+20\*2）

Eifs = sifs + difs + ack时间，传输失败后的等待帧间间隔，用于发送数据后未收到ACK

A-MSDU和A-MPDU改善频繁ACK导致信道占用率下降的情况