# NAV in 802.11

## TXOP下的Duration时间设置

在802.11e之前的协议中，都是“竞争一次，传输一个帧”，用协议的说法，即是“length based transmission”，length指的就是每个帧的长度，当节点竞争成功后，其就传输其对应数据帧的长度，也就是获得单个数据帧的信道传输时间。

单个帧（非TXOP）的传输是通过物理载波监听来保证的。

在802.11e中引入的TXOP，实际上是“竞争一次，获得一段传输时间”，协议的说法为，“duration based transmission”，即节点竞争成功后，其获得了一段信道使用时间，在这段时间内，其可以传输多个数据帧。这种传输方式也经常用“Burst ”这个词描述。

TXOP的传输时间是通过虚拟载波监听（NAV）来保证的。

TXOP和静态帧分片： 都是可以竞争一次传输多次数据，但是静态帧分片本质还是传输单个MSDU，但是TXOP是传输多个PPDU。

在TXOP中，通常开启是采用四种帧，分别是：

1）Qos\_Data，利用普通QoS数据帧起始TXOP时间，

2）QoS\_Null，有PHY\_Header和MAC\_Header，没有MAC层的SDU，

3）QoS(+)\_CF-Poll，用于HCCA中的TXOP机制，

4）RTS/CTS，多功能的控制帧。

然后对应TXOP的传输模式（ACK模式），其实都是与ACK有关的，分别是

1）Normal ACK：一个包一个ACK反馈，

2）无ACK反馈，

3）无显示的ACK反馈，这个比如PCF里面会用到的多功能帧，ACK+Poll这样的组合帧，

4）突发传输（Burst Transmission），Block ACK反馈，。其实我们一开始看到的DD-WRT下面可以设置的无ACK也是基于802.11e的特性。

[802.11协议精读41：EDCA TXOP和Polled TXOP - 知乎 (zhihu.com)](https://zhuanlan.zhihu.com/p/437156457)

## 基础概念：

[802.11协议精读42：(Data)Duration Field与EIFS - 知乎 (zhihu.com)](https://zhuanlan.zhihu.com/p/410583159)

PIFS和DIFS都是在SIFS的基础上增加几个slot时间。PIFS的一个典型应用是Beacon帧的发送。

PIFS = aSIFSTime + aSlotTime

DIFS = aSIFSTime + 2 x aSlotTime

EIFS应用于数据帧接收失败的情况，此时无法设置NAV，如果后面又接收到ACK的话则可以重新设置NAV并执行DIFS，否则就执行EIFS。下面EIFS的时长设置也包含了一个ACK的时长，考虑到了ACK正常发送却没被接收的情况。

EIFS = aSIFSTime + AckTxTime + DIFS

aSIFSTime= aRXRFDelay（射频延迟）＋aRXPLCPDelay（物理层头部接收延迟）＋aMACProcessingDelay（MAC层处理延迟） + aRxTxTurnaroundTime（发送接收天线转换时间）

aSlotTime= aCCATime（CCA时间）＋aRxTxTurnaroundTime（发送接收天线转换时间）＋aAirPropagationTime（传播延迟）＋aMACProcessingDelay（MAC层处理延迟）

## 载波监听：（cs）

### 物理载波监听 physical carrier-sensing -- CCA机制

在CSMA/CA中，CCA由能量检测和载波检测一起完成：

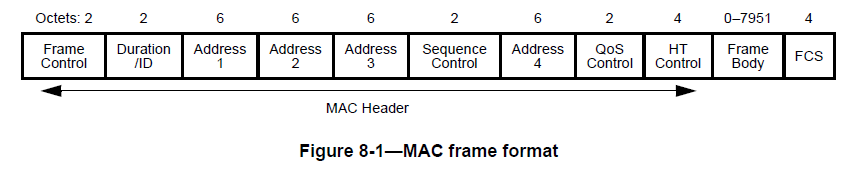
* 能量检测（Energy Detection）：是直接用物理层接收的能量来判断是否有信号进行接入，若信号强度大于ED\_threshold，则认为信道是忙，若小于ED\_threshold，则认为信道是闲。同时该ED\_threshold的设置与发送功率有关，比如发送功率大于100mW，那么ED\_threhold约为-80dBm，发送功率在50mW至100mW之间，那么ED\_threshold应该为-76dBm。不过至于具体的数值，需要查看其具体所对应版本的802.11协议。
* 载波侦听（Carrier Sense）：载波监听的方法指的是用来识别802.11数据帧的物理层头部（PLCP header）中的preamble部分。简单的说，802.11中的preamble部分采用特定的序列所构造，该序列对于发送方和接收方都是已知的，其用来做帧同步以及符号同步。在实际监听过程中，节点会不断采样信道信号，用其做自相关或者互相关运算，其中自相关在基于OFDM的802.11技术中常用，比如802.11a，而互相关在基于DSSS技术中常用，比如802.11b。与能量检测类似，相关计算值需要与一个阈值进行判断，若大于，则认为检测到了一个信号，若小于则没有检测到。

协议中规定，两种检测方式同时采用，且只要两者检测方式中，有一种判断信道是busy的话，那么就认为信道是busy的，只有两者都认为信道空闲时，那么再判断虚拟载波监听机制是否为0，以上条件都满足时，那么才可以进行backoff倒数。

### 虚拟载波监听（virtual carrier-sensing）-- NAV机制

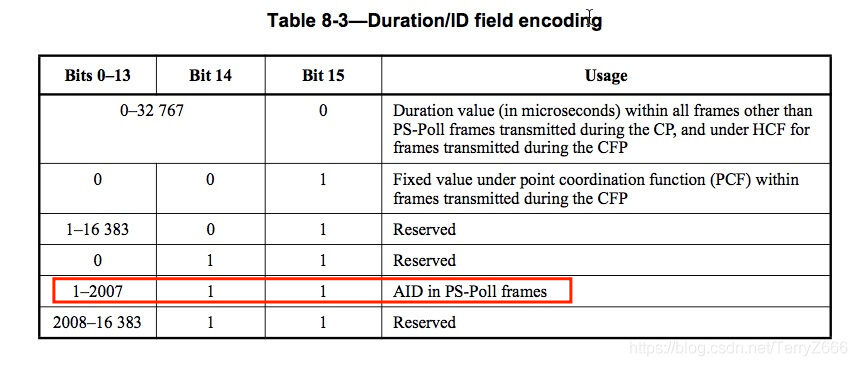
Network allocation vector （NAV）是虚拟载波监测技术。

在MAC layer Header中，存在duration id一项，表示这个包的传输时间

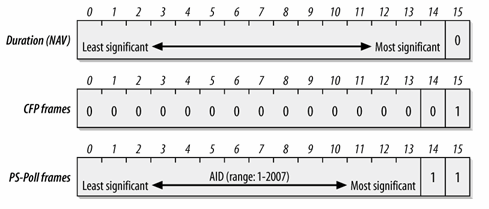


在这段时间内，即认为介质是繁忙的

所有发送端读取介质中包的duration id这一项，并设定自身的NAV，表示在这段时间介质繁忙，因此不能发包



duration id总共占16位，其中前15位表示duration的时间，单位为微秒，最多可到32767微秒。



Duration：设定 NAV  
**当第 15 个 bit 被设定为 0 时**， Duration/ID 位就会被用来设定 NAV。此数值代表目前所进  
行的传输预计使用介质多少微秒。工作站必须监视所收到的任何帧头，并据以更新 NAV。任何  
超出预计使用介质时间的数值均会更新 NAV，同时阻止其他工作站访问介质。  
免竞争期间所传送的帧

在免竞争期间（ contention-free period，简称 CFP），**第 14 个 bit 为 0 而第 15 个 bit 为 1。**  
其他所有 bit 均为 0，因此 duration/ID 位的值为 32768。这个数值被解读为 NAV。它让没有收  
到 Beacon（信标）帧『注』的任何工作站，得以公告免竞争期间，以便将 NAV 更新为适当的  
数值，避免干扰到免竞争传输。  
  
PS-Poll 帧  
在 PS-Poll（省电模式－轮询）帧中，**第 14 与第 15 个 bit 会被同时设定为 1**。移动式工作  
站可以关闭天线以达到省电目的。休眠中的工作站必须定期醒来。为确保不致丢失任何帧，从休  
眠状态醒来的工作站必须送出一个 PS-Poll 帧，以便从基站取得之前暂存的任何帧。此外，醒来  
的工作站会在 PS-Poll 帧中加入连接识别码（ association ID，简称 AID），以显示其所隶属的  
BSS。 AID 包含在 PS-Poll 帧中，其值介于 1-2,007。而介于 2,008-16,383 的值目前保留并未使  
用。

目的地为**广播或组播**地址的帧（Address 1 位设定了群组 bit），**其持续时间为 0**。此类

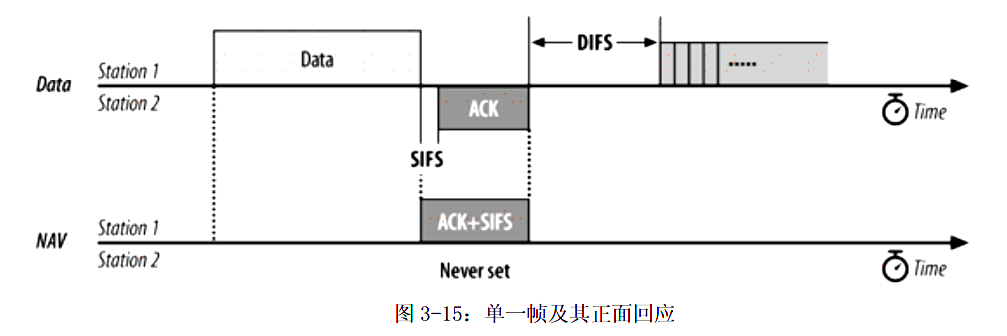
帧并非基本交换过程的一部分，接收端也不会加以应答，因此竞争式介质访问可以在广

播或组播数据帧结束后立即开始。 NAV 在帧交换过程中是用来保护传输介质。既然广

播或组播帧之后不会有来自链路层的应答，因此没有必要为后续帧锁住介质使用权。

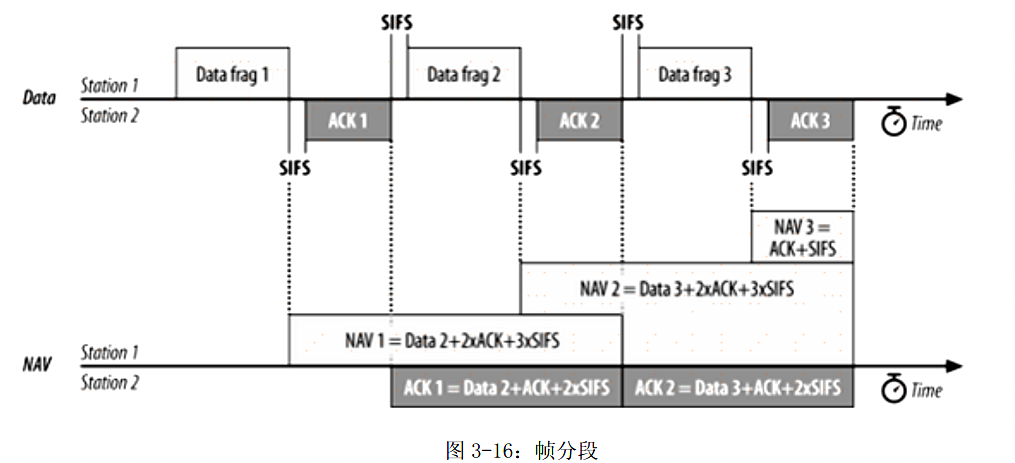
## NAV场景(单NAV)

### 场景一：单一帧及其正面响应



此帧会利用 NAV 为本身、应答及 SIFS 预定介质使用权。设定较长的 NAV，是为了替整个交换程序锁住虚拟载波，以保证接收端可以传送应答。因为此交换程序是以 ACK 做为结束，所以没有必要再锁住虚拟载波，因此该 ACK 中 NAV 会被设定为 0。

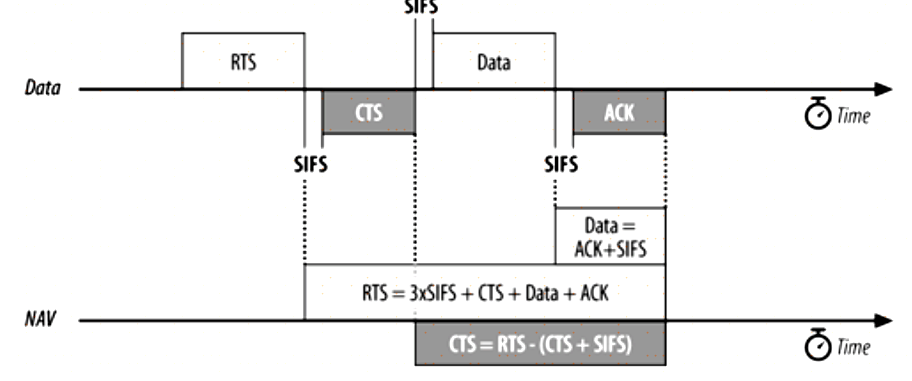
### 场景二：帧分段



最后两个帧和之前的交换过程没有两样， NAV 的设定也完全相同。不过，倒数第二个帧之前所有帧均会使用 NAV,为下一个帧锁住介质。第一个数据帧会将 NAV 的时间设定至足以涵盖ACK1,下一个帧片段及其回应（ ACK2）。 为了表示其为帧片段， MAC 会将帧标头控制位的 **More Fragmentsbit 设定为 1**。最后一个回应（ ACK3）除外，其余回应都会继续为下一个数据片段及其回应延长锁住介质的时间。后续的数据帧会继续延长 NAV 以涵盖后续的回应，直到最后一个数据帧才会将 More Fragmentsbit 设定为 0，而最后一个回应（ ACK3）则会将 NAV 设定为 0。帧片段的数目并无限制，不过虚空总长度必须短于 PHY 对交换过程所做的限制。

帧分段是由 MAC 的 fragmentation threshold(切割门限)参数所控制。大部分的网卡驱动程序都允许使用者设定此参数。 任何超过分段门限的帧都会被加以分段， 分段方式因实际情况而异。调高分段门限意味着帧的传输负担较小，不过帧丢掉和损害的成本较高，因为将会有较多的数据必须丢弃与重传。调低分段门限意味着传输负担较重，不过在面临较恶劣的环境时，这种做法可以提供较佳的稳定性。

### 场景三：RTS/CTS



RTS 帧会试图预定介质使用权，供帧交换程序使用，因此 RTS 帧发送者必须计算 RTS 帧

结束后还需要多少时间。图 4-14 说明了整个交换过程，总共需要三个 SIFS、一个 CTS、最后

的 ACK，加上发送第一个帧或帧片段所需要的时间。（ fragmentation burst〔片段宣泄期〕会使

用后续的帧片段来更新 Duration 位。）传输所需要的微秒数经过计算后会置于 Duration 位。假

使计算的结果不是整数，就会被修正为下一个整数微秒。

用来应答 RTS 时， CTS 帧的发送端会以 RTS 帧的 duration 值作为持续时间的计算基准。

RTS 会为整个 RTS-CTS-frame-ACK 交换过程预留介质使用时间。不过当 CTS 帧被发送出后，

只剩下其他未帧或帧片段及其回应待传。CTS 帧发送端会将 RTS 帧的 duration 值减去发送 CTS

帧及其后短帧间隔所需的时间，然后将计算结果置于 CTS 的 Duration 位。图 4-16 显示了 CTS

duration 与 RTS diratopm 的关系。用于防护交换（ protection exchanges）时， CTS 帧所依循

的规则将留在防护机制一并讨论。

依照 ACK 信号在整个帧交换过程中位居何处， duration 的值可以有两种设定方式。在完整

的数据帧及一连串帧片段的最后一个片段中， duration 会被设定为 0。数据发送端会将 Frame

Control（帧控制）位中的 More Fragments（尚有片段） bit 设定为 0，表示数据传输已经结束。

如果 More Fragments bit 为 0，表示整个传输已经完成，没有必要再延长对无线信道的控制权，

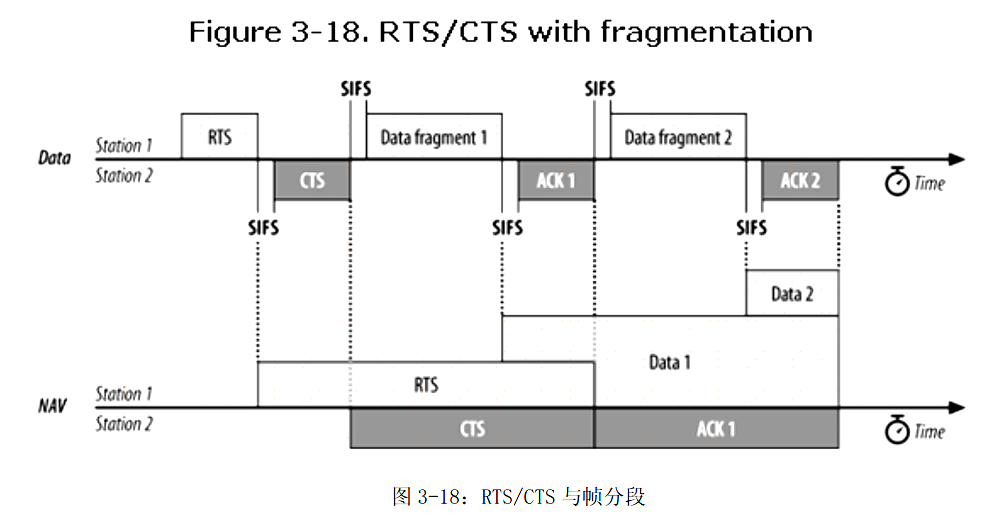
因此会将 duration 设定为 0。

如果 More Fragments bit 为 1， 表示尚有帧片段仍在发送中。 此时 Duration 位的用法和 CTS

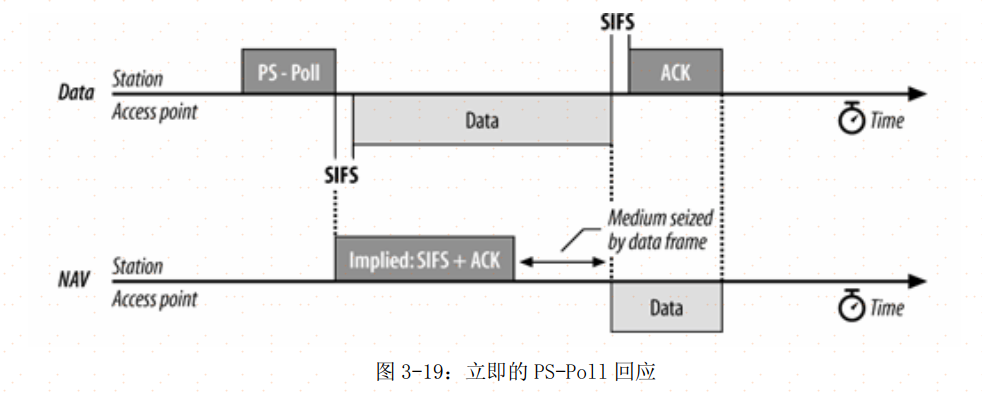
帧中的 Duration 位相同。发送 ACK 以及短帧间隔所需要的时间，将由最近帧片段所记载的

duration 中减去。如果不是最后一个 ACK 帧， duration 的计算方式类似 CTS duration 的计算方

式。事实上， 802.11 的规格书将 ACK 帧中的 duration 设定称为虚拟 CTS。



场景：PS-POLL



基站可以对 PS-Poll（省电模式－轮询）帧立即作出应答。经过一段 SIFS(短帧间隔)时间，

基站即可传送帧。如图 3-19 所示， PS-Poll 帧隐含了一 NAV。 PS-Poll 帧的 Duration/ID 位中包

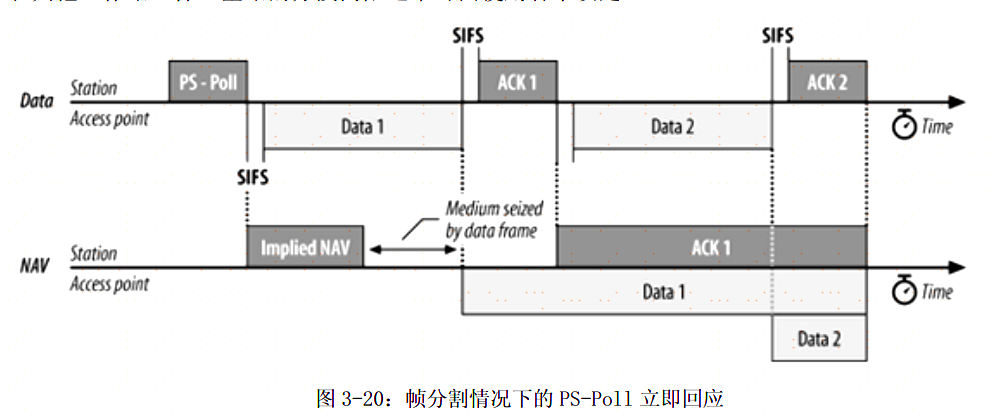
含了 Association ID（连接识别码），因此基站可以判断有哪些帧是为该工作站所暂存的。不过，

MAC 规格书要求所有收到 PS-Poll 的工作站都必须更新 NAV， 将 NAV 的值设定为一个 SIFS 加

上一个 ACK 的时间。虽然此 NAV 对数据帧而言过短，但基站会取得介质使用权，而所有工作

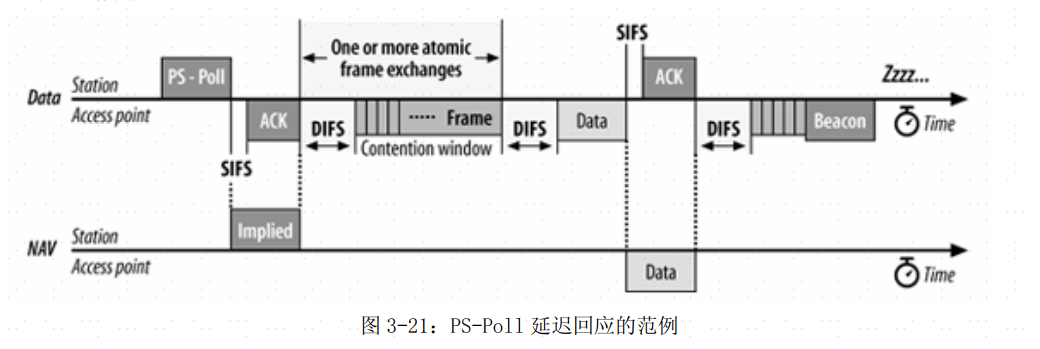
站都会为了这个数据帧而延后访问介质。但数据帧传送结束时， NAV 随即更新以反映数据帧标

头中的数值。



如果暂存的帧过大，则必须进行分段。图 3-20 说明了帧分段情况下的 PS-Poll 立即应答。

和其他工作站一样，基站的分段门限通常可由使用者来设定。



除了立即应答，基站可以先回复一个简单应答。这种做法称为延迟应答（ deferred

response），因为基站虽然回应了访问暂存帧的要求，但未并立即采取实际的发送行动。使用

延迟应答的优点之一，在于基站方面的软件较易实现，因为应答信息可以通过芯片组立即传送，

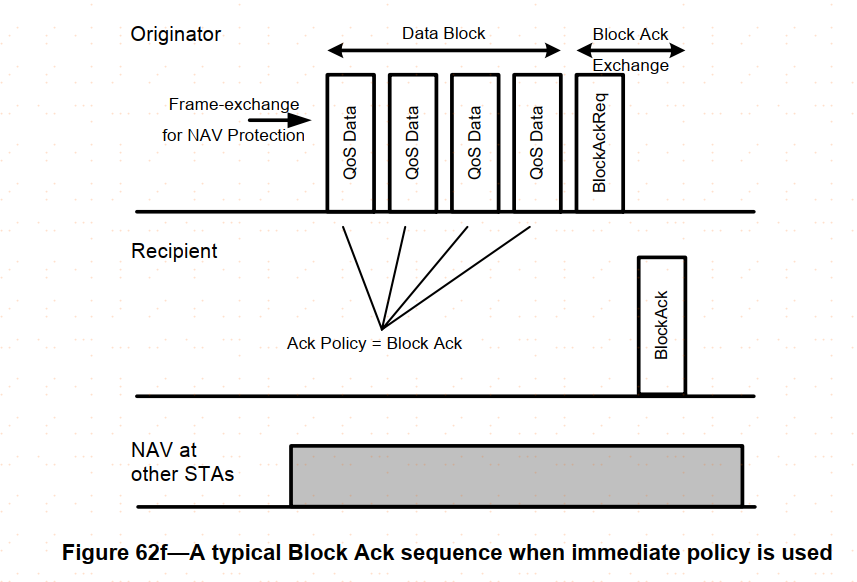
至于数据则可以先予以暂存，然后依正常过程传输。

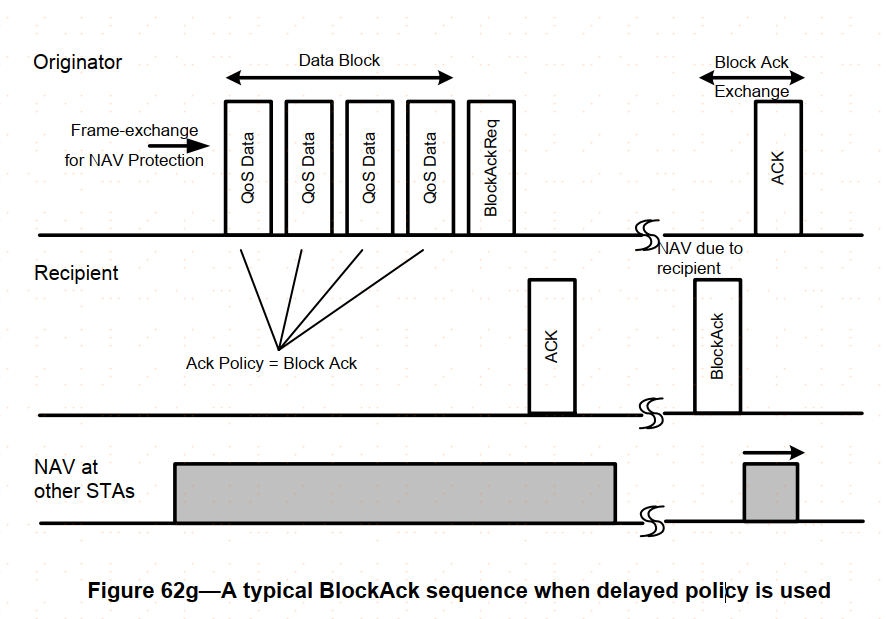
通过 PS-Poll 要求帧的工作站必须保持清醒， 直到该帧传输完成。 不过， 在竞争式服务期间，

基站可能在任何时间传递帧。此时工作站不能返回省电模式，除非接收到一个 Beacon 帧，其中

对应该工作站的 TIM（数据待传） bit 已被清除。

### BAR/BA





## 802.11ax：双重NAV机制

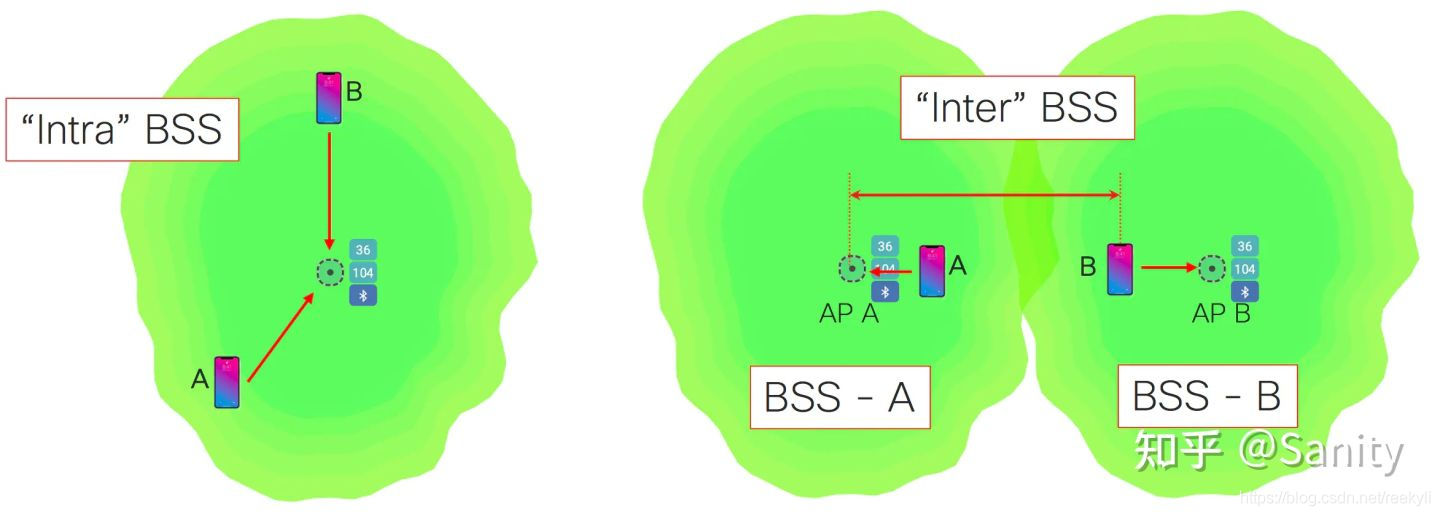
#### bss color in 802.11ax

[Wi-Fi 6(802.11ax)解析7：BSS Coloring技术 - 知乎 (zhihu.com)](https://zhuanlan.zhihu.com/p/76362759)

802.11ax设备通过向PHY头部添加字段（即BSS Coloring字段）来区分BSS，节点在竞争时，根据检测到物理层头部的BSS Coloring字段来分配MAC层的竞争行为。

若BSS Coloring字段信息相同，那么代表在同一个BSS内(intra-BSS)。

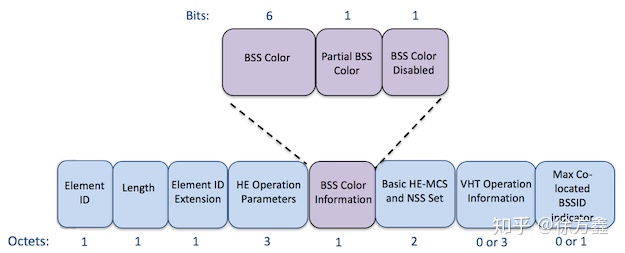
若BSS Coloring字段信息不同，那么代表这里是重叠覆盖区域，在多个BSS间(inter-BSS)。



在传统802.11中，若在BSS间(inter-BSS)，当节点检测到信道忙时，需要推迟自己的传输，直到信道空闲才可以发送。在802.11ax中，引入了自适应CCA机制(adaptive CCA)。通过提高BSS间(inter-BSS)信号检测阈值，同时保持BSS内(intra-BSS)的较低信号检测阈值（两个阈值，大约4dB左右的差值），来减少MAC层竞争时的竞争问题，提升MAC层效率。

是用于识别重叠基本服务集（OBSS）的方法

BSS Coloring的信息是同时被添加在PHY层和MAC层中的。在802.11ax PHY头部的Preamble中，其SIG-A字段包含6个Bit的BSS Coloring信息字段。该字段可以识别多达63个BSS [1-63]。



在802.11**管理帧**中也可以看到BSS Coloring信息(如上图所示)。在Beacon帧中的**HE Element**中，包含BSS Coloring的子字段。其也是6个Bit的BSS Coloring信息字段，可以标识63个BSS。

BSS着色中的颜色实际上是从1到63的索引号，该索引号与信道分配一起手动或通过无线资源管理（RRM）协调地分配给各个接入点。在同一附近共享同一信道的接入点应具有不同的颜色。如果在同一通道上运行的两个BSS具有相同的颜色，则这是颜色重叠。在颜色重叠的情况下，**检测站发送颜色冲突报告以警告所连接的接入点**。接入点可以随时通过在每个**信标和探测响应帧**中发送的BSS颜色变化通知元素来通知BSS颜色变化。

from（26.17.3.3）去使能BSS COLOR

在一定场景下，HE STA需要关闭BSS COLOR功能（比如检测到OBSS内的BSS冲突）

通过将字段 **HE Operation element.BSS Color Disabled** = 1

如果收到一个AP发来的帧，其中BSS Color Disable字段为1，则：

**non-AP HE STA忽略RX\_VECTOR中的BSS\_COLOR以及TXOP\_DURATION字段，通过MAC地址以及Duration/ID来更新其intra-NAV**

否则，一个HE STA需要使用BSS\_COLOR来决定是否要更新其intra-BSS NAV

#### 区别Intra-BSS and inter-BSS PPDU（26.2.2）

inter-BSS PPDU:

* 收到的RX\_VECTOR 中的BSS\_COLOR指示和STA所在的BSS\_COLOR不同，并且非0
* 收到VHT PPDU，RX\_VECTOR中GROUP\_ID是0，并且Partial\_AID和BSSID[39:47]不同
* Partial BSS Color 场景下，收到VHT PPDU，RX\_VECTOR中的Partial\_AID[5:8]不等于BSS COLOR的低4位
* 一个AP收到了VHT\_MU\_PPDU/HE\_MU\_PPDU，RX\_VECTOR.UPLINK\_FLAG=0
* PPDU中的BSSID和本STA连接的BSSID不一致
* PPDU不包含BSSID，但是存在RA和TA字段，并且TA/RA和本BSSID都不一致

intra-BSS PPDU:

* 收到的RX\_VECTOR 中的BSS\_COLOR指示和STA所在的BSS\_COLOR相同
* 收到VHT PPDU，RX\_VECTOR中GROUP\_ID是0，并且Partial\_AID和BSSID[39:47]相同
* Partial BSS Color 场景下，收到VHT PPDU，RX\_VECTOR中的Partial\_AID[5:8]等于BSS COLOR的低4位
* PPDU中的BSSID或者RA或者TA，和本STA的BSSID相同
* PPDU包含一个控制帧，没有TA，但是RA地址和当前BSS的TXOP Holder地址相同

除了以上情况，PPDU定义为非inter-BSS，非intra-BSS PPDU

如果基于MAC地址的判断结果既是inter又是intra BSS PPDU，则判定为intra-BSS PPDU;

如果根据BSS\_COLOR判断为intra-BSS PPDU，但是通过MAC地址判断为inter-BSS PPDU，则后者优先

#### 802.11ax UL MU CS机制 (26.5.2.5 UL MU CS mechanism)

一个non-AP HE STA收到一个trigger帧，

* 如果CS Required subfield字段为0，可以忽略CCA检测以及basic/intra-BSS NAV状态，直接进行上行数据传输。
* 始终忽略intra-NAV的状态，但是要查看basic-NAV状态

#### Dueling NAV

在802.11ax中已经引入了BSS Coloring机制，以适应在OBSS环境下，自适应调节空闲信道评估阈值（即adaptive CCA)，以增加空间信道的复用率，提供更多并行传输的可能性。

在BSS Coloring中引入的adaptive CCA也可以和虚拟载波监听的NAV组合使用，由于adaptive CCA中已经引入了两个不同的监测阈值，那么意味着其和NAV机制组合使用时，也需要两个独立的NAV定时器。在802.11ax中，目前已经新定义了两个NAV定时器：BSS内部的NAV定时器（intra-BSS NAV timer），和基本NAV定时器（basic NAV timer）。

* BSS内部NAV定时器（intra-BSS NAV timer）：其只够通过来自于同一个BSS内部的终端来设置，通过BSS内部终端传输的Duration/ID字段来设置NAV定时器的数值。
* 基本NAV定时器（basic NAV timer）：其可由来自于**不同BSS区域**的终端来设置，也是根据这些终端传输的Duration/ID字段来设置NAV定时器的数值。

以上两个NAV定时器同时工作，如果由任意一个NAV设置为非0，也就是正在定时中，那么就认为信道是忙，正在被占据。

**HE STA更新intra-BSS NAV的情况：（满足以下所有条件）**

1. 收到的是intra-BSS PPDU
2. 该PPDU中包含的Duration/ID值比本地的intra-BSS大
3. 该PPDU中RA字段指示的不是本STA的MAC地址；或者本STA不是TXOP Holder并且收到的帧不需要立即回复；或者该帧是一个trigger帧。

**HE STA更新basic-BSS NAV的情况：（满足以下所有条件）**

1. 收到的是inter-BSS PPDU或者不能识别为inter/intra BSS PPDU
2. 包含的Duration/ID值比本地的inter-BSS大
3. 收到的PPDU中RA不等于本地MAC地址

**根据TXOP\_DURATION更新intra-BSS NAV：**

如果STA是TXOP Holder，不需要根据RX\_VECTOR中的TXOP\_DURATION信息进行更新本地intra-BSS NAV；

如果STA不是TXOP Holder，在收到一个HE PPDU之后，满足以下所有条件，需要更新其intra-BSS NAV:

1. RX\_VECTOR中包含了有效的TXOP\_DURATION相关信息
2. 该PPDU是intra-BSS PPDU
3. 该PPDU不包含MAC Duration信息
4. TXOP\_DURATION比本地intra-BSS NAV值大

**根据TXOP\_DURATION更新basic-BSS NAV：**

1. RX\_VECTOR中包含了有效的TXOP\_DURATION相关信息
2. 收到的是inter-BSS PPDU或者不能识别为inter/intra BSS PPDU
3. 该PPDU不包含MAC Duration信息
4. TXOP\_DURATION比本地basic-BSS NAV值大

如果STA收到的HE PPDU中既包含Duration/ID信息，又包含有效的TXOP\_DURATION信息，则忽略后者。

CHECK: 10.3.2.9, 10.3.2.11, and 26.5.2.5 10.3.2.4. 10.3.2.1

**NAV Reset场景：（CTS超时以及TXOP截断）**

* 如果HE STA在收到RTS或者MU-RTS更新本地NAV之后的一段时间内没有收到下一个数据包，即没有收到来自物理层的PHY-RXSTART.indication消息，则判定为RTS超时，需要重置其NAV（PHY-CCARESET.request），超时时间设定为：

**2 × aSIFSTime + CTS\_Time + aRxPHYStartDelay + 2 × aSlotTime**

* non-AP HE STA在收到CF-END帧时，如果当前没有和AP建立连接，需要重置其NAV
* 单NAV的HE AP，收到了CF-END帧，需要重置其NAV，除非出现以下场景：
  + - 收到的CF-END帧是inter-BSS PPDU，但是该AP NAV最近一次更新是基于intra-BSS PPDU
    - 收到的CF-END帧是intra-BSS PPDU，但是该AP NAV最近一次更新是基于inter-BSS PPDU
* 双NAV的HE STA（包括AP），根据收到的CF-END帧是inter-BSS 还是 intra-BSS PPDU来分别重置对应的NAV
* 双NAV的HE STA（包括AP），如果收到CF-END帧是intra-BSS PPDU，并且当前的inter-BSS NAV最近一次更新是基于非inter-BSS以及非intra-BSS PPDU，则需要重置两个NAV定时器

当所有NAV定时器被重置之后，不需要进行IFS等待，可以直接开始介质竞争过程。

## 协议摘要

### 9.2.5 Duration/ID field (QoS STA)

|  |  |  |
| --- | --- | --- |
| **QD9** | **Duration/ID rules for QoS STA** | **9.2.5** |

NAV计算：

1. 时间单位为微秒us，0-32767(16bits)
2. 计算时向上取整
3. 如果小于0，则NAV为0

STA发起TXOP传输可选两种NAV模式：（TODO，相关协议字段？）

Single protection：通过NAV值保护单独的一个帧。

Multiple protection：通过NAV值保护多个帧，sender通过预测计算NAV。

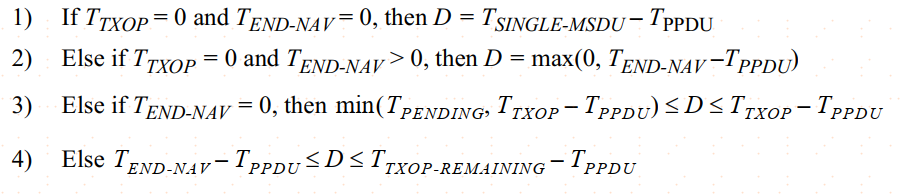
STA在发起TXOP之后的第一个帧就决定了采用单独的还是多重TXOP保护，后续所有的帧都采用相同的duration等级。

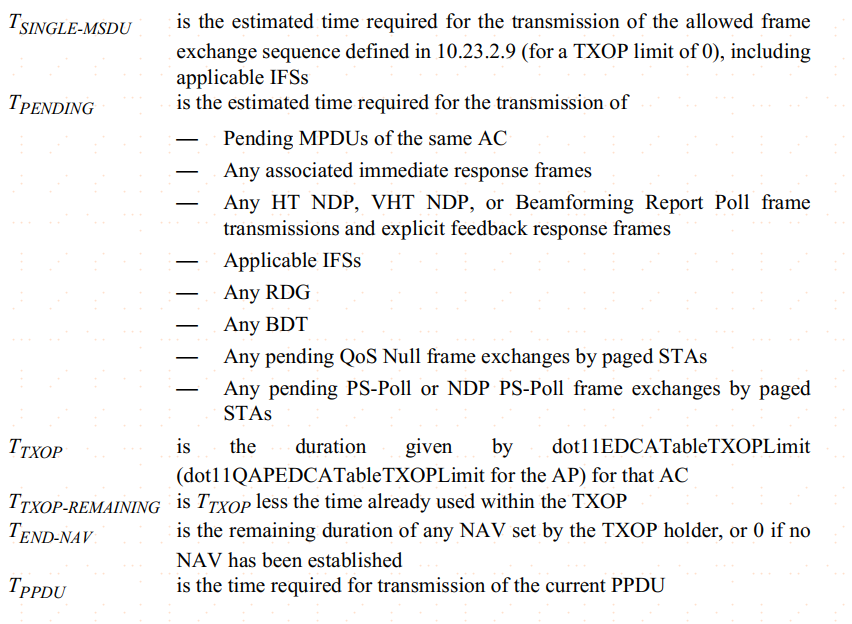
Duration/ID字段的设置：

单帧保护：

1. RTS：DATA+CTS+ACK/BA+n\*SIFS
2. CTS: DATA+ACK/BA+n\*SIFS
3. BAR: 如果是立即响应的话，设置为BA+SIFS；如果是延迟响应的话，设置为ACK+SIFS
4. BA：如果是对BAR的响应的话（显式BAR），设置为0；如果是隐式BAR的话，设置为 ACK+SIFS;
5. 管理帧/non-QOS Data/使用ACK的单播包：如果是TXOP中的最后一帧，设置为 ACK + SIFS；否则，设置为DATA(next) + ACK + n\*SIFS
6. Qos Data不需要ACK/广播包：如果是TXOP最后一帧，设置为0；否则设置为DATA(next)+Ack+SIFS

多帧保护：

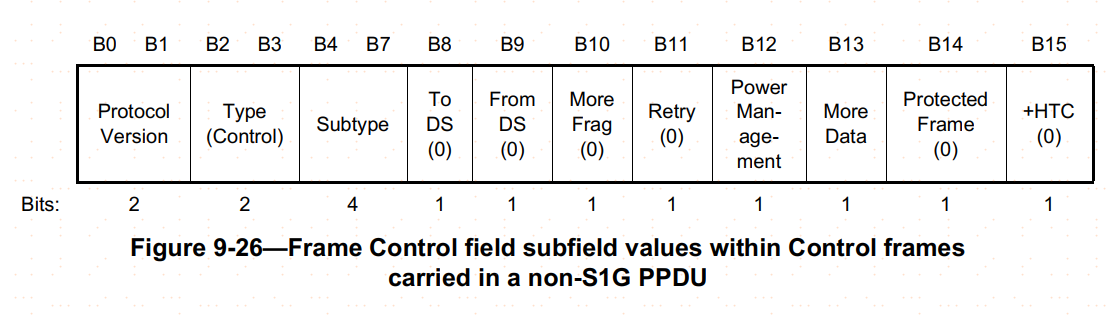




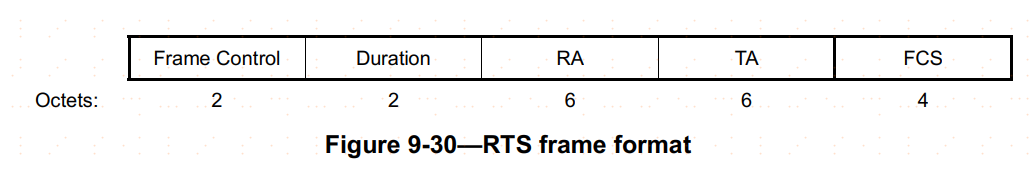
### 9.3 Format of individual frame types

#### 9.3.1 控制帧

帧结构：

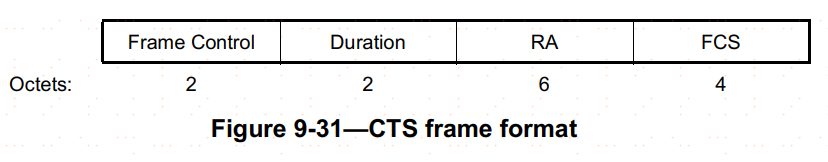


##### 9.3.1.2 RTS



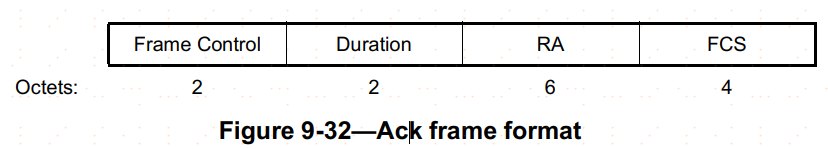
* non-Qos STA: duration = 数据/管理帧 + CTS + ACK + 3\*SIFS （单位为us，计算时向上取整）
* Qos STA: 参考[9.2.5](#_9.2.5 Duration/ID field (QoS STA))

##### 9.3.1.3 CTS



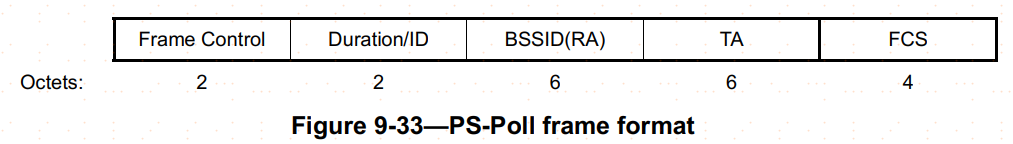
* 如果该CTS是RTS的响应，RA设置为RTS的TA，单播/组播bit位设置为0（单播）；如果是self-CTS，RA设置为本地MAC地址
* non-Qos STA & RTS/CTS : duration = RTS中设置的时间 - CTS本身发送时间 - SIFS
* non-Qos STA & self-CTS & ACK: duration = 后续的数据/管理帧 + ACK + 2\*SIFS
* non-Qos STA & self-CTS (NO ACK): duration = 后续的数据/管理帧 + SIFS
* Qos STA: 参考[9.2.5](#_9.2.5 Duration/ID field (QoS STA))

##### 9.3.1.4 Ack



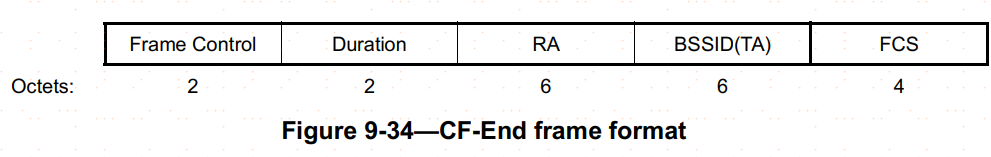
* non-Qos STA & More\_Fragments\_bit==0 ： Duration=0
* non-Qos STA 其他： Duration = Duration(Last) - ACK -SIFS
* Qos STA: 参考[9.2.5](#_9.2.5 Duration/ID field (QoS STA))

### 9.3.1.5 PS-Poll



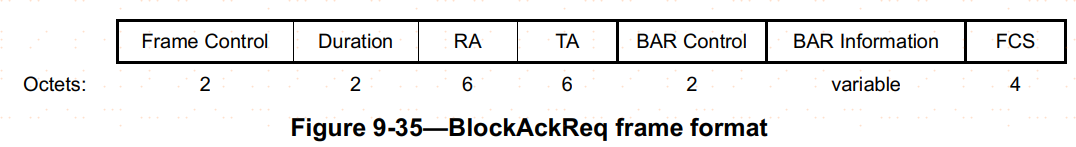
Duration = AID

##### 9.3.1.6 CF-End



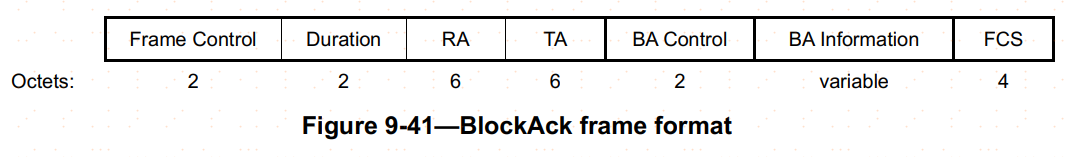
non-DMG and non-S1G STA：Duration = 0

##### 9.3.1.7 BlockAckReq



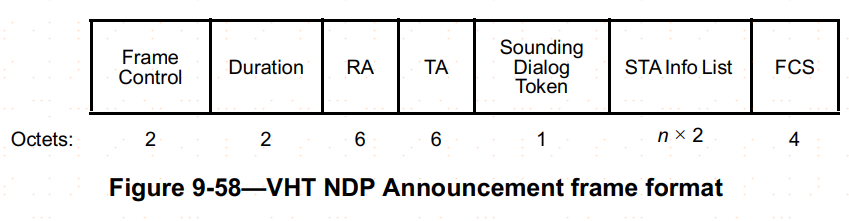
Duration设置参考[9.2.5](#_9.2.5 Duration/ID field (QoS STA))

##### 9.3.1.8 BlockAck



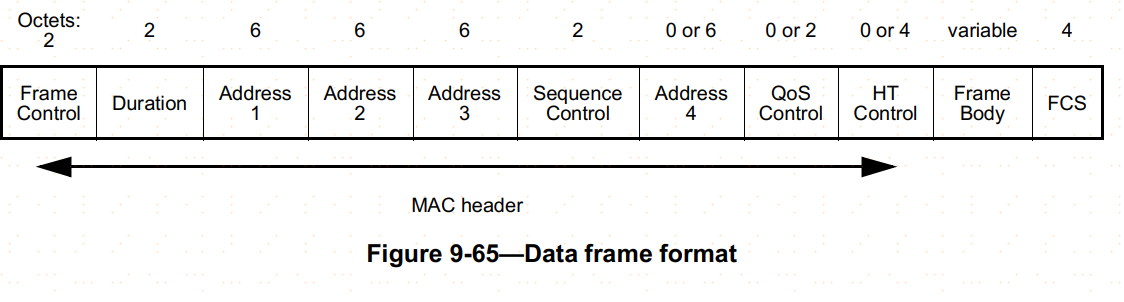
Duration设置参考[9.2.5](#_9.2.5 Duration/ID field (QoS STA))

##### 9.3.1.19 VHT NDP Announcement



Duration设置参考[9.2.5](#_9.2.5 Duration/ID field (QoS STA))

##### 9.3.2 Data frames

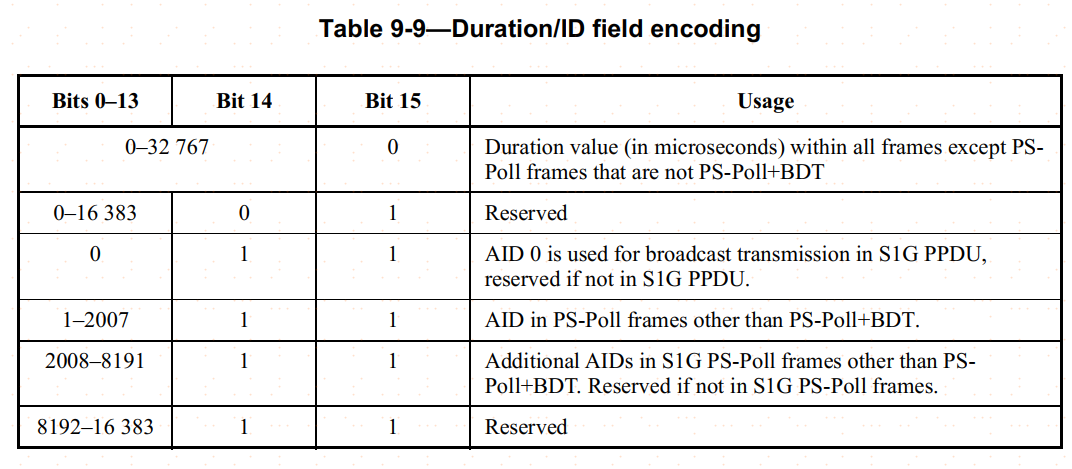


可选字段：（参考9.2.4）

Address4：由Frame Control中的TO/FROM DS字段决定

Qos Control：由Frame Control 中的 Subtype决定

HTC：由Frame Control控制。



* Duration for Qos STA: 参考[9.2.5](#_9.2.5 Duration/ID field (QoS STA))
* Duration for non-Qos STA:

如果是组播数据，Duration=0

如果是单播数据，不分段，Duration=ACK + SIFS

如果是单播数据，分段：Duration= ACK + SIFS + 下一段数据 + SIFS + ACK + SIFS

### 9.7 Aggregate MPDU (A-MPDU)

|  |  |
| --- | --- |
| **HTM7** | **Duration/ID rules for A-MPDU and TXOP** |

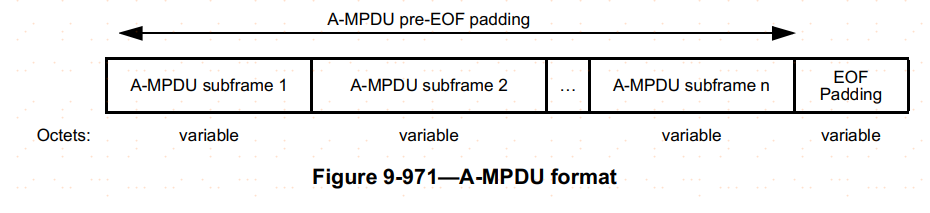
在test\_mac\_tx\_ampdu\_frame的scoreboard中新增AMPDU中MPDU Duration字段检测。协议规范要求AMPDU中所有的MPDU中的Duration一致。

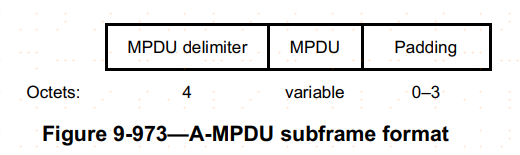
802.11ax:

The Duration/ID fields in the MAC headers of all MPDUs in an A-MPDU carry the same value. The

Duration/ID fields in the MAC headers of the MPDUs in the A-MPDUs carried in a VHT MU

PPDU and an HE MU PPDU carry the same value.





### 10.3.2.1 CS mechanism 载波帧听机制

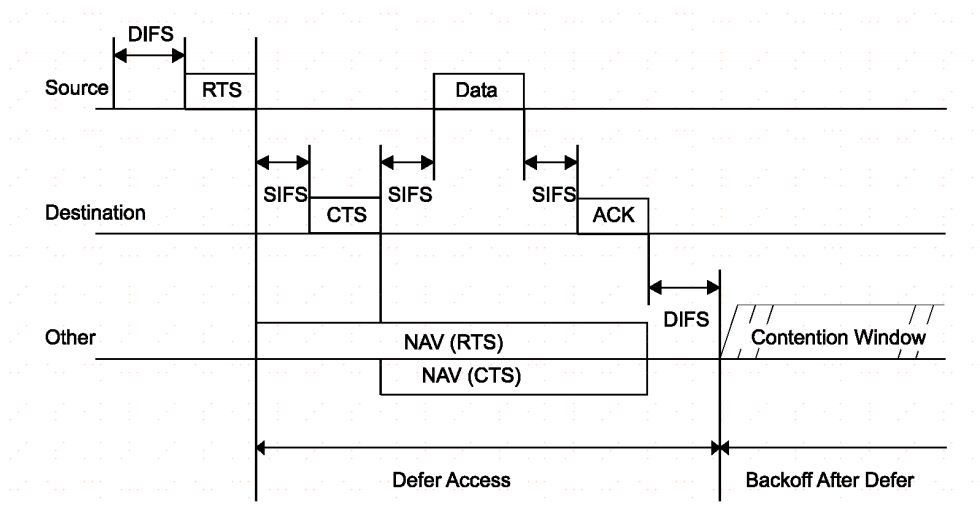
|  |  |
| --- | --- |
| **PC3.1** | **Network allocation vector (NAV) function** |

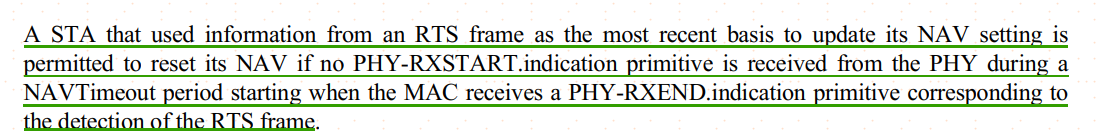
**The NAV maintains a prediction of future traffic on the medium based on duration information that is announced in RTS/CTS frames by non-DMG STAs and RTS/DMG CTS frames by DMG STAs prior to the actual exchange of data.**

### 10.3.2.4 Setting and resetting the NAV

* STA通过有效的PSDU中的Duration字段来更新本地的NAV值。
* 如果RA(Receive Address)是本地地址，则不更新NAV，说明是和本机进行通信的帧。
* 否则检查收到的帧的duration字段，如果大于本地NAV定时器当前值，则更新为最新值。
* NAV字段的计算采用向上取整的方式进行。
* 如果收到的是PS\_POLL帧，在MAC头中并不包含duration字段，默认将duration值置为Time(ACK+SIFS)，虽然此 NAV 对数据帧而言过短，但基站会取得介质使用权，而所有工作站都会为了这个数据帧而延后访问介质。但数据帧传送结束时， NAV 随即更新以反映数据帧标头中的数值。（详见NAV场景解析）
* NAV的重置都是在RX接收完成之后，根据物理层的PHY-RXEND指示进行。

RTS/CTS/DATA/ACK场景的NAV设置：





[802.11ac-2016协议DCF解析 - 知乎 (zhihu.com)](https://zhuanlan.zhihu.com/p/351446011):

如果在NAVTimeout时间内没有PHY-RXSTART.indication 一个STA允许更新NAV来重置。NAVTimeout周期等于(2 x aSIFSTime) + (CTS\_Time) + aRxPHYStartDelay + (2x aSlotTime) 参考（[10.3.7](#_10.3.7 DCF Timing Relation)）

L-SIG的duration信息也可以用于更新NAV（TODO 参考802.11n）

NAV(RTS) = 3\*SIFS+CTS+DATA+ACK

NAV(CTS) = 2\*SIFS+DATA+ACK = NAV(RTS) - SIFS - CTS

（支持双NAV的HE STA参考后续章节 26.2.4）

802.11ax补充如下：

HE AP（NOT TXOP holder）：如果收到一个RX\_VECTOR，符合**全部**以下条件，则更新本地NAV

1. RX\_VECTOR中包含TXOP\_DURATION具体信息
2. 没有收到有效的PPDU信息以获取Duration/ID信息
3. RX\_VECTOR中的TXOP\_DURATION长度大于本地NAV长度

HE AP(TXOP holder)：如果收到一个RX\_VECTOR，符合全部以下条件，则更新本地NAV

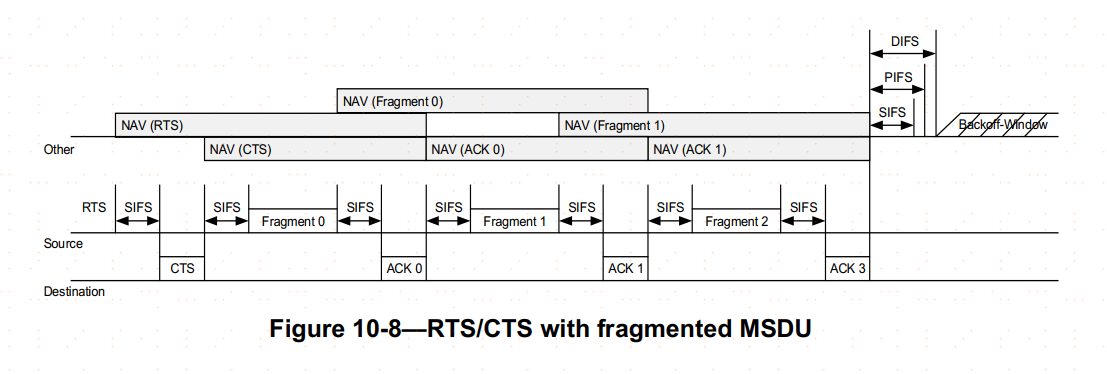
1. RX\_VECTOR中包含TXOP\_DURATION具体信息
2. 没有收到有效的PPDU信息以获取Duration/ID信息
3. RX\_VECTOR中的TXOP\_DURATION长度大于本地NAV长度
4. RX\_VECTOR中的BSS\_COLOR信息和本地BSS COLOR信息不一致（TODO BSS COLOR机制）

注意：一个非AP的802.11ax STA有两个NAV但是HE AP可能只有一个。

如果STA同时收到了RXVECTOR和PPDU中的duration信息，以PPDU信息为准，TXVECTOR中的TXOP\_DUR会被忽略。

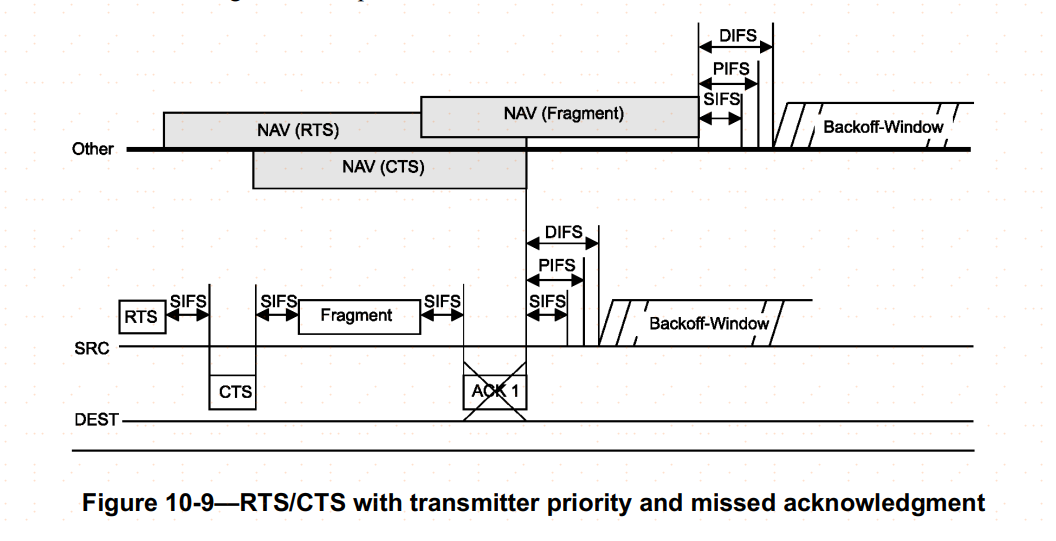
补充MU-RTS触发帧的相关处理，参考文档：[Wi-Fi 6(802.11ax)解析14：下行OFDMA接入机制（DL-OFDMA） - 知乎 (zhihu.com)](https://zhuanlan.zhihu.com/p/77527893)

### 10.3.2.6 RTS/CTS with fragmentation



每个分段data+ack事实上扮演了RTS/CTS的作用，用于对空口资源的继续占用以及对其他STA的通知。

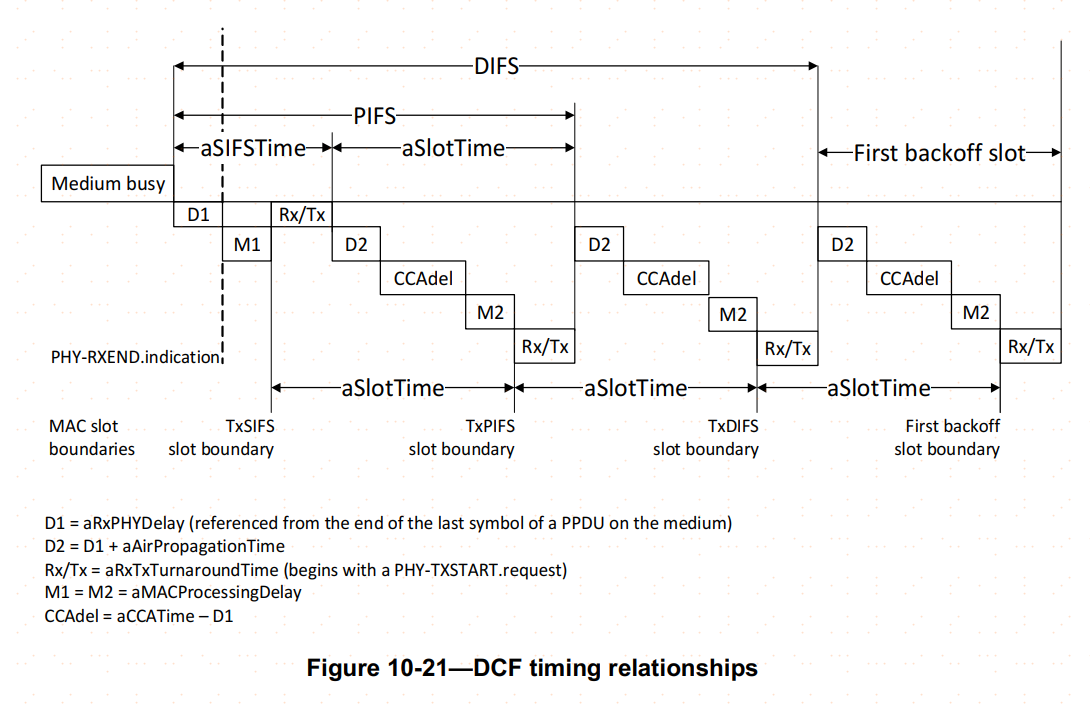
**ACK丢失场景：**

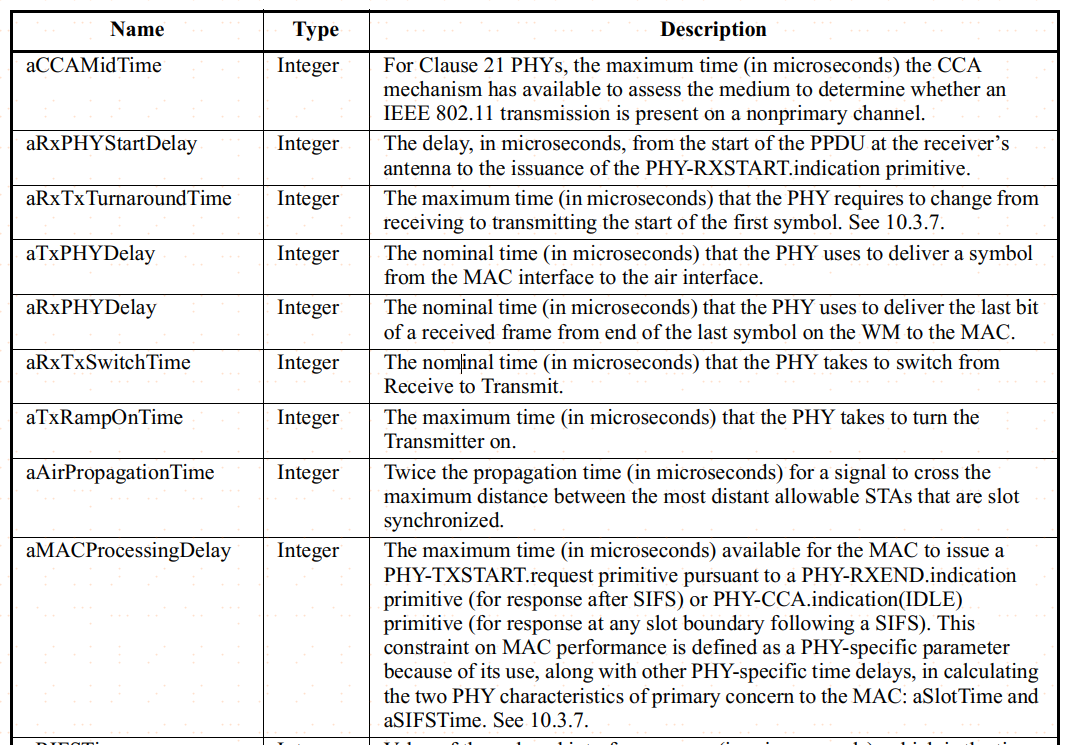


### 10.3.2.9 CTS and DMG CTS procedure

### 10.3.2.11 Acknowledgment procedure

### 10.3.7 DCF Timing Relation





### 10.3.2.15 NAV distribution

如果一个STA需要占用信道发送一些非常规数据业务，可以采用self-CTS。

发送一个CTS帧到，RA填本地MAC地址，同时在mac头中设置适当的duration值，用来占用信道以及保证可能存在的ACK帧。

该方式比RTS/CTS效率更加高，但是安全性低，可能会导致隐藏节点问题。

### 10.23.2.9 TXOP LIMIT

The TXOP limits are advertised by the AP in the EDCA Parameter Set element in Beacon and Probe Response

frames transmitted by the AP.

**A TXOP limit of 0** indicates that the TXOP holder may transmit or cause to be transmitted (as responses) the

following within the current TXOP:

a) One of the following at any rate, subject to the rules in 10.6

1) One or more SU PPDUs carrying fragments of a single MSDU or MMPDU

2) An SU PPDU or a VHT MU PPDU carrying a single MSDU, a single MMPDU, a single

A-MSDU, or a single A-MPDU

3) A VHT MU PPDU carrying A-MPDUs to different users (a single A-MPDU to each user)

4) A QoS Null frame or PS-Poll frame that is not an PS-Poll+BDT frame

b) Any required acknowledgments

c) Any frames required for protection, including one of the following:

1) An RTS/CTS exchange

2) CTS-to-self

3) Dual CTS as specified in 10.3.2.10

d) Any frames required for beamforming as specified in 10.31, 10.36.5, and 10.42.

e) Any frames required for link adaptation as specified in 10.32

f) Any number of BlockAckReq frames

### 10.39.10 Updating multiple NAVs (DMG STA)

多NAV更新流程，只能是DMG STA，802.11ax。

### 10.27 Protection mechanisms

|  |  |  |  |
| --- | --- | --- | --- |
| **PC30** | **Update NAV is long enough to cover frame and any response** | **10.27** | |
| **PC33** | **Update NAV** | |

### 11.38.5 NAV assertion in a VHT BSS

|  |  |  |  |
| --- | --- | --- | --- |
| **VHTM8.3** | **CCA on primary 20 MHz, secondary 20 MHz, and secondary 40 MHz channels** | **11.38.5** | |
| **VHTM8.4** | **CCA on secondary 80 MHz channels for 160 MHz and 80+80 MHz** | | **11.38.5** | |

A VHT STA shall update its NAV as described in 10.3.2.4 using the Duration/ID field value in any frame that

does not have an RA matching the STA’s MAC address and that was received in a 20 MHz PPDU in the

primary 20 MHz channel or received in a 40 MHz PPDU in the primary 40 MHz channel or received in

an 80 MHz PPDU in the primary 80 MHz channel or received in a 160 MHz or 80+80 MHz PPDU.

NOTE—The PHY might filter out a PPDU as described in 21.3.20 or not receive a PPDU due to VHT TXOP power

saving described in 11.2.3.17. If so, frames in the PPDU are not received by the MAC and have no effect on the NAV.

更新接收测试用例：  
在VHT/HE模式下，构造不同接收带宽下的数据包，设置正确的NAV值，查看物理层是否能正确过滤数据包，传递给MAC层，然后MAC层根据PPDU中的信息更新本地NAV.

如果没有在主20M带宽上收到有效PPDU数据包，PHY不应该给MAC发送PHY\_RXSTART.ind指示。

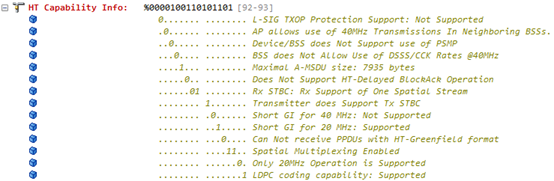
1. PHY-CCA.indication(Busy)
2. PHY\_RXSTART.ind
3. PHY-DATA.indication(DATA)
4. PHY-RXEND.indication(NoError)

### 10.26.5 L-SIG TXOP protection(From 802.11n-2016)

实现通过L-SIG进行TXOP保护（可选）

实现STA对L-SIG中的NAV进行检测以及更新（必选）

[beacon帧字段结构最全总结（二）——HT字段总结 - fengf233 - 博客园 (cnblogs.com)](https://www.cnblogs.com/fengf233/p/10919436.html)



1. L-SIG TXOP保护： Legacy Signal Transmission Opportunity（传统信号域传输机会）。在L-SIG TXOP保护方式下，HT帧的L-SIG域包含一个时间值（~~此时间值应等于MAC帧头中的MAC持续时间值~~），要求传统设备直到这个时间结束后再进行正常收发。传统设备因无法接收在L-SIG持续时间范围内开始的PPDU，故在L-SIG TXOP内，传统接收机不会收到任何帧。若11n下支持L-SIG TXOP保护，HT Capability Info中的L-SIG TXOP Protection位应该置1，0代表不支持。

[802.11n Protection Mechanisms: Part 2 (cwnp.com)](https://www.cwnp.com/802-11n-protection-mechanisms-part-2/)

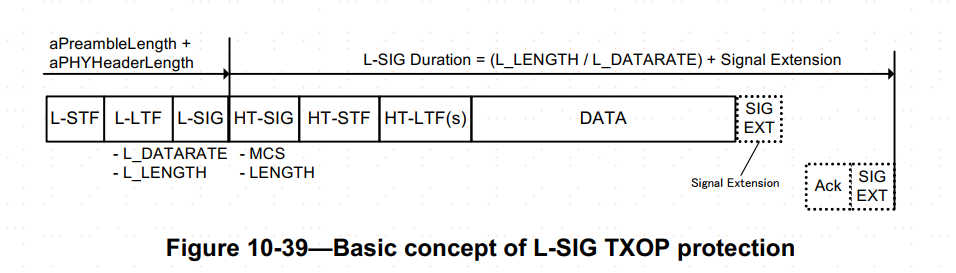
An HT STA must indicate whether it supports L-SIG TXOP Protection in its **L-SIG TXOP Protection Support capability field** in **Association Requests and Probe Responses**.

The AP determines whether all HT stations associated with its BSS support L-SIG TXOP Protection and indicates this in the **L-SIG TXOP Protection Full Support field** of its **HT Information Element**. This field is set to 1 only if the L-SIG TXOP Protection field is set to 1 by **all HT station** in the BSS.

Under L-SIG TXOP Protection operation, the L-SIG field with an HT mixed format PHY preamble represents a duration value equivalent to the sum of:

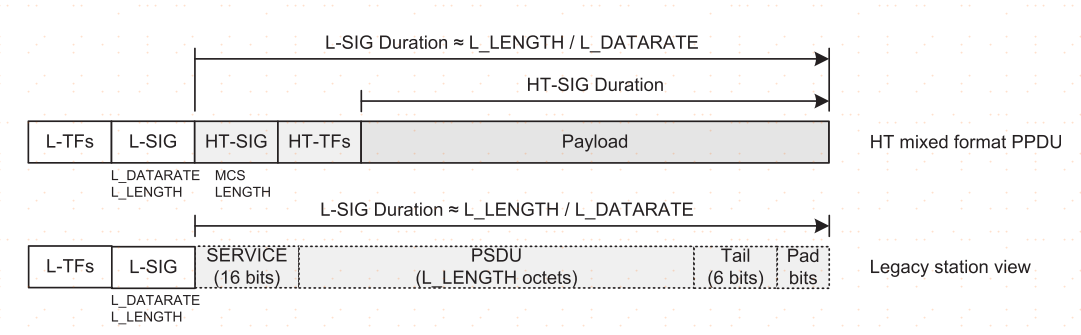
**a) the value of Duration/ID field contained in the MAC header, and**

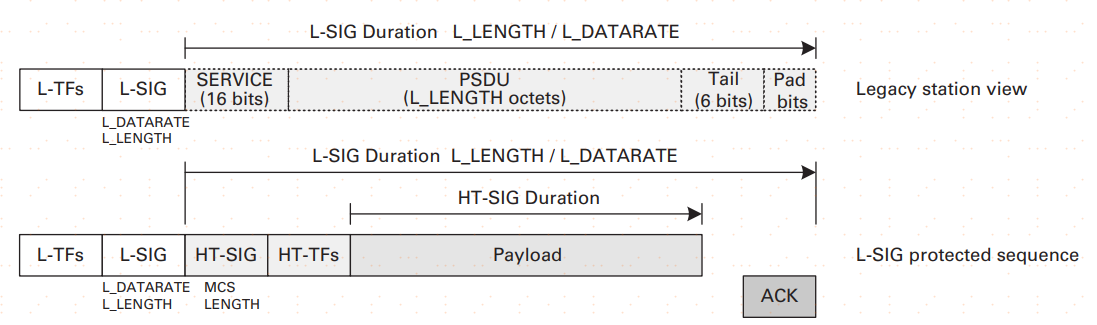
**b) the duration remaining in the current packet (from the end of the symbol containing the L-SIG field to the end of the last symbol of the packet).**

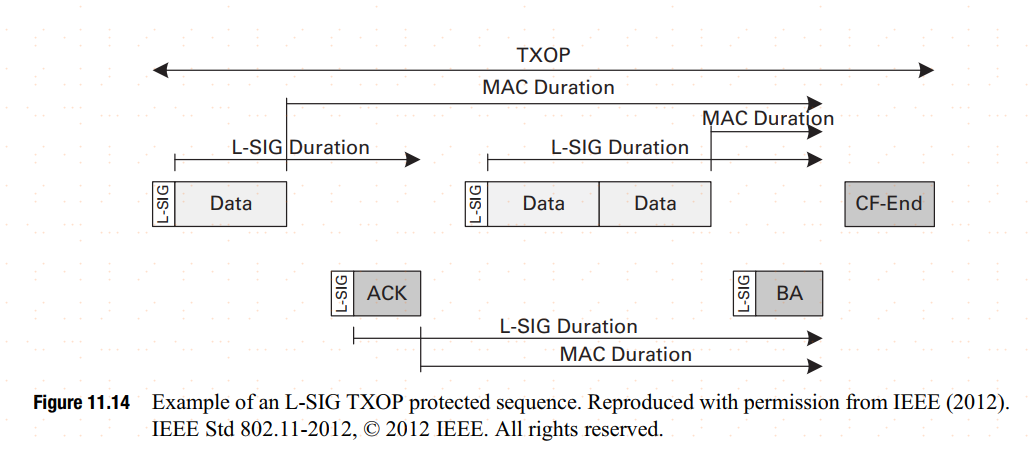


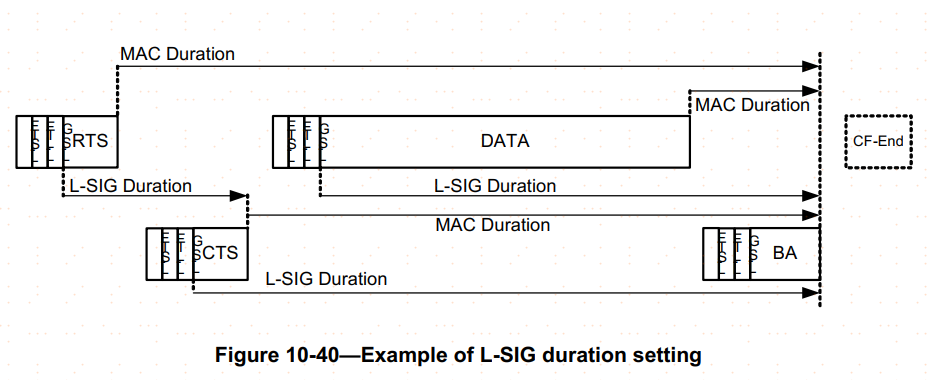
《Cambridge 802.11n》

11.5.10 L-SIG TXOP protection









1. 发送对象只能是支持802.11n L-SIG TXOP保护功能的STA ，MAC头中的Duration字段还是正常设置。
2. 一个支持该功能的HT STA，如果收到了L-SIG TXOP保护的PPDU，并且没有从MSDU中解到Duration信息，则使用L-SIG Duration-T(PPDU) 来更新自己的NAV。
3. 收到L-SIG TXOP保护的响应帧（ACK/BA），如果数据解析正常，会使用收到的Duration信息来更新L-SIG Duration以及MAC头Duration，通过Duration(receive) - T(SIFS) - T(Preamble)
4. 缺点：传统的不支持该功能的STA无法解调包含L-SIG TXOP保护的数据帧，所以会采用EIFS机制来进行解调失败之后的信道竞争。 所以在采用L-SIG TXOP保护机制的数据序列传输结束时，支持该功能的HT STA会正常进行BackOff介质竞争过程，等待一个DIFS时间，而传统的STA会等待EIFS时间，从而导致竞争失败或者优先级降低。解决办法是：发起者在数据sequence结束之后发送一个采用 non-HT格式的CF-END帧，保证所有的接收STA都能正确收到数据结束通知，然后发起公平竞争。
5. 只有802.11n的终端/ap才能支持L-SIG TXOP保护；
6. 只有BSS中所有HT-STA支持，HT-AP才能宣布支持。
7. 除非收到的DATA包含L-SIG Duration，否则反馈不需要包含L-SIG Duration

HT STA NAV更新规则：

1. L-SIG TXOP Protection Support field = 1
2. RXVECTOR.FORMAT = HT\_MF
3. RXVECTOR.LSIGVALID = TRUE
4. 没有从MPDU中解析到有效的Duration值
5. 设置NAV = L-SIG duration - TXTIME(PPDU) + (aPreambleLength + aPHYHeaderLength)

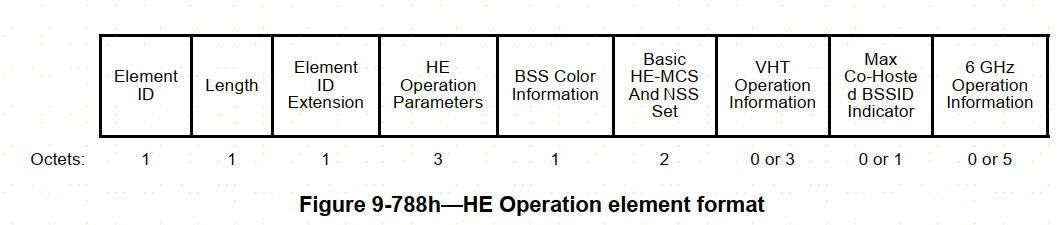
### 26.2 HE channel access

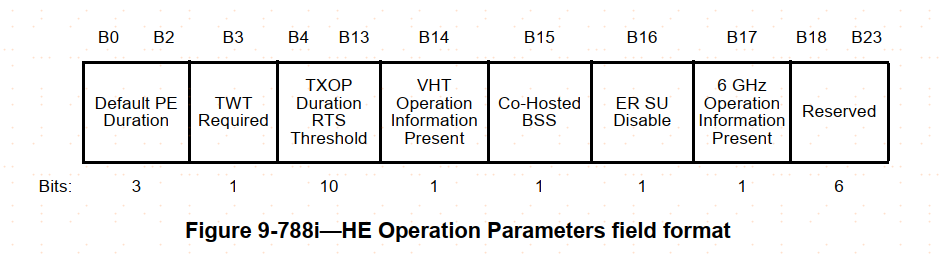
### 26.2.1 TXOP duration-based RTS/CTS

**首先说明： 该功能是AP用于控制STA来进行TXOP获取的一种手段。**

**HE STA如何开启基于RTS/CTS的TXOP保护：**

AP通过Beacon帧对功能使能进行控制：HE Operation.HE Operation Parameters field.**TXOP Duration RTS Threshold** （1-1022）





The TXOP Duration RTS Threshold subfield enables an **HE AP** to manage RTS/CTS usage by non-AP HE

STAs that are associated with it (see 26.2.1). The TXOP Duration RTS Threshold subfield contains the

TXOP duration RTS threshold in units of 32 µs, which enables the use of RTS/CTS, except for the value

1023. The value 1023 indicates that TXOP duration-based RTS is disabled. The value of 0 is allowed in

Beacon and Probe Response frames and indicates that the previously announced TXOP duration RTS

threshold remains in effect. In all other frames, the value of 0 is reserved.

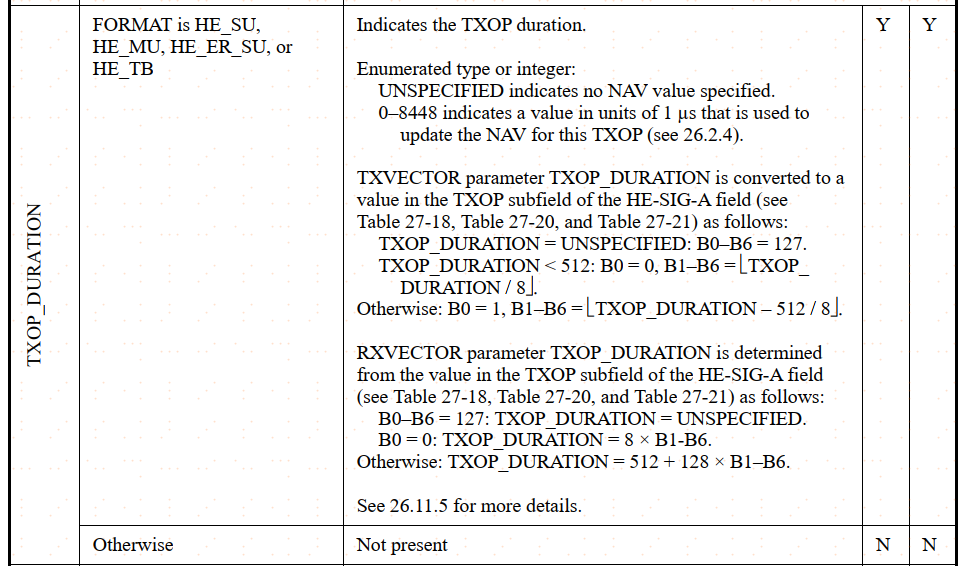
**non-ap STA 收到有效的TXOP Duration之后，更新本地的****dot11TXOPDurationRTSThreshold值。如果本地该值为1023，则说明TXOP Duration功能关闭。**

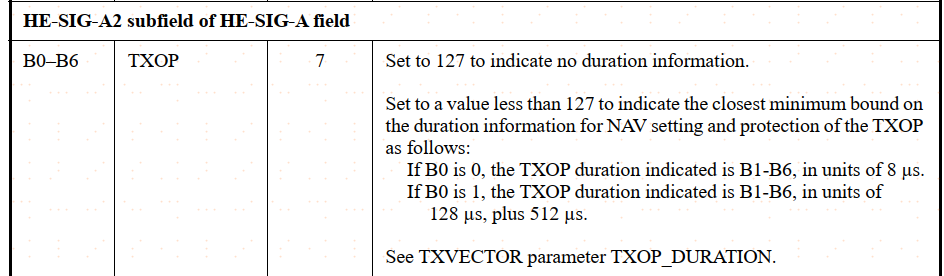
**如果dot11TXOPDurationRTSThreshold小于1023，并且符合以下条件,STA需要通过RTS/CTS来获取TXOP Duration：**

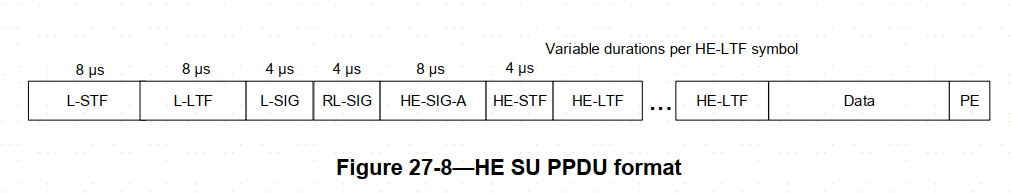
1. **STA需要向AP发送单播数据**
2. **TXOP Duration大于等于32us\*dot11TXOPDurationRTSThreshold**

**否则：对于RTS/CTS的使用限制由****dot11RTSThreshold控制。**

**RX/TX VECTOR中的 TXOP Duration字段：**







### 26.2.4 Updating two NAVs(From 802.11ax 2021)

|  |  |  |  |
| --- | --- | --- | --- |
| **HEM8** | **NAV update** | **26.2.4** |  |
| **HEM8.1** | **Update basic NAV** | **26.2.4** | **CFHE:M** |
| **HEM8.2** | **Update IntraBSS NAV** | **26.2.4** | **CFAP AND CFHE: O  CFIndepSTA AND CFHE:M** |

A non-AP HE STA shall maintain two NAVs, and an HE AP may maintain two NAVs: an intra-BSS NAV

and a basic NAV. The intra-BSS NAV is updated by an intra-BSS PPDU. The basic NAV is updated by an

inter-BSS PPDU or a PPDU that cannot be classified as intra-BSS or inter-BSS.

intra-BSS NAV由BSS内PPDU负责更新，基础NAV由其他非intra-BSS PPDU更新。

802.11ax引入的新NAV机制： 双重NAV机制，包含Inter/intra NAV

The 802.11 Task Group working on High-Efficiency Wireless will possibly include not just one NAV field, but two different NAVs to the 802.11ax standard. Having an intra-BSS NAV and an inter-BSS NAV could help STAs to predict traffic within their own BSS and feel free to transmit when they know the state of overlapping traffic.

[Wi-Fi 6(802.11ax)解析9：双重NAV技术（Dueling NAVs） - 知乎 (zhihu.com)](https://zhuanlan.zhihu.com/p/77365487)

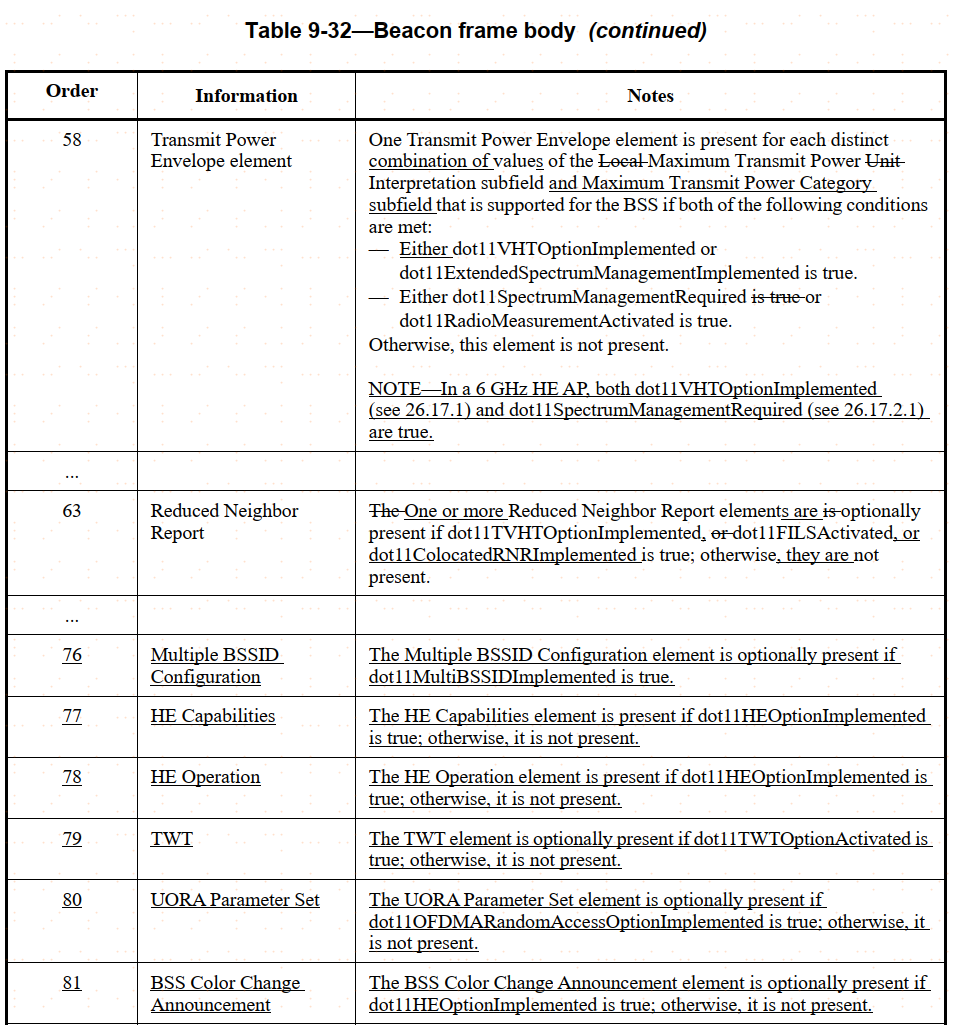
[Wi-Fi 6(802.11ax)解析26：Wi-Fi 6的一些理念（基本思想+接入机制） - 知乎 (zhihu.com)](https://zhuanlan.zhihu.com/p/461494392)

### 26.11 Rules for setting some TXVECTOR parameters for PPDUs transmitted by an HE STA

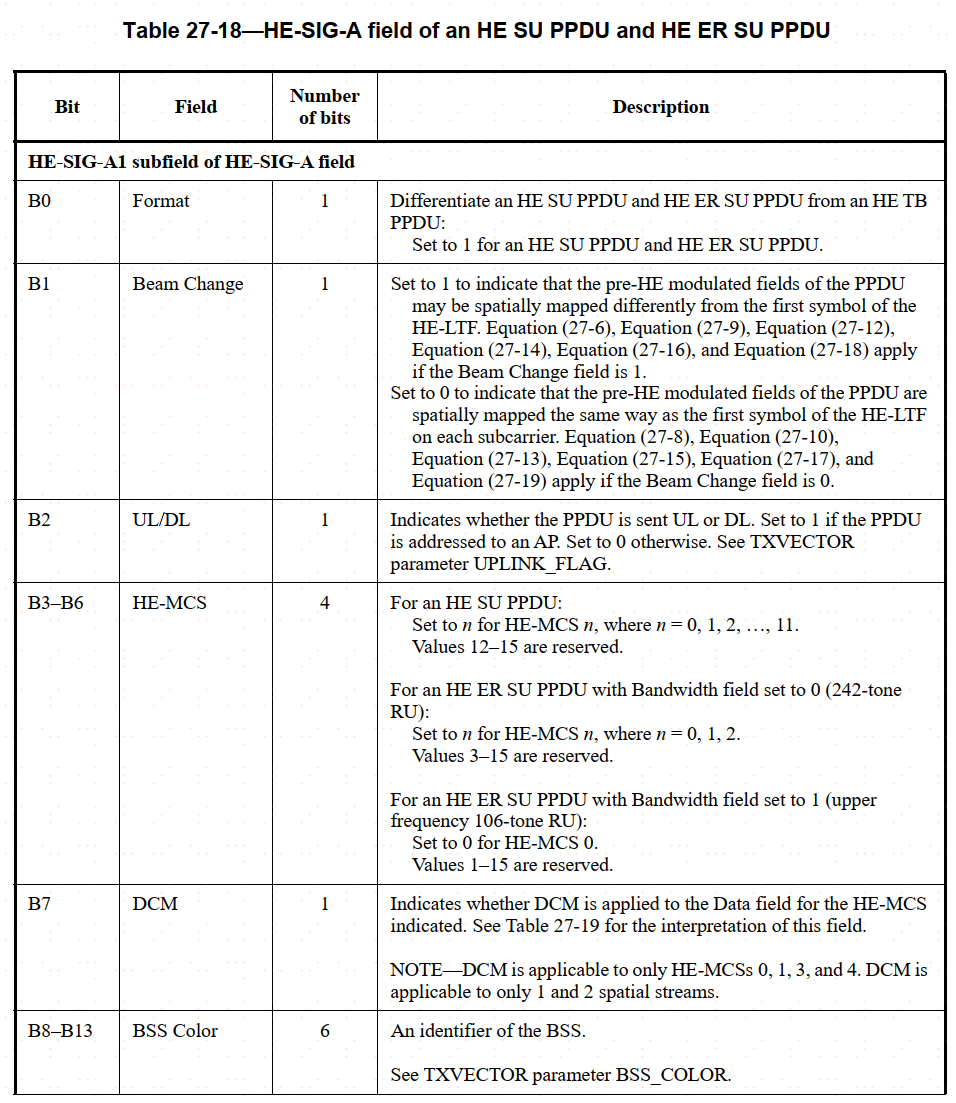
#### 1. 关于BSS COLOR

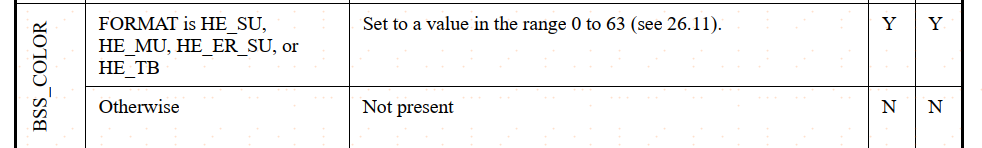
HE STA在HE Operation element中会选择并且填充一个BSS COLOR字段

HE Operation element in Beacon Frame:



BSS\_COLOR in TX/RX VECTOR





### 802.11ax TXOP Duration

