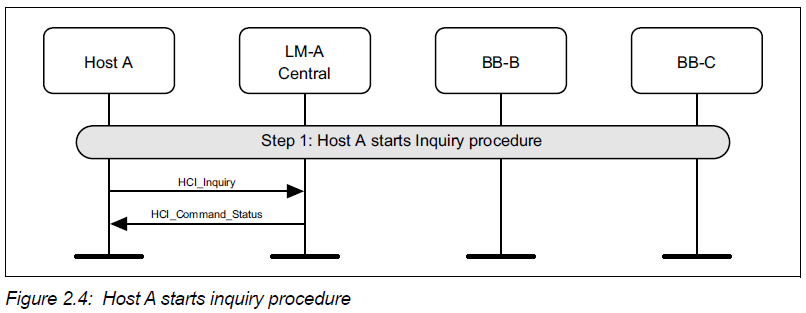
# Inquiry Substate Induction

## Inquiry流程简介

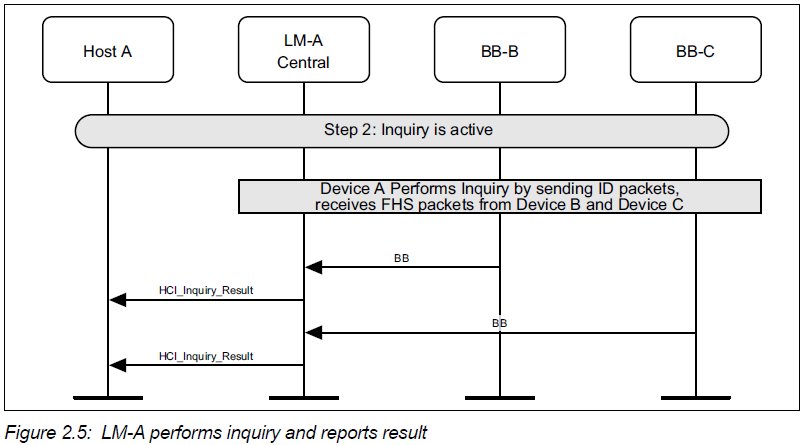
inquiry流程有两种，一种是one time inquiry（一次性询问） 和 periodic inquiry（周期性询问）。需要周期性地搜索蓝牙设备的情况下才会采用周期性询问这种方式，但是由于该种模式使用的场景有限且对功耗是个不小的负担

### One time inquiry

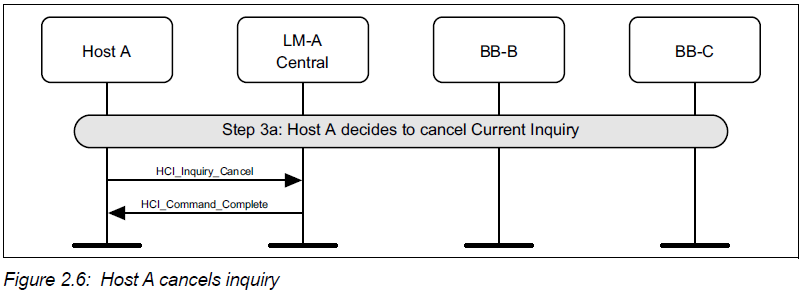
步骤1：蓝牙Host通过命令HCI\_Inquiry告知控制器Controller进入查询模式，用于发现周围环境中的其他蓝牙设备。



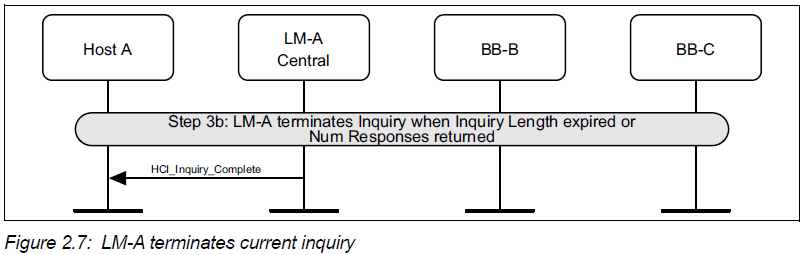
步骤2：蓝牙控制器Controller接收到上层开启搜索指令后将以指定的查询访问代码（IAC）和查询时长启动蓝牙基带搜索查询流程，对外发送ID包。周围环境中的蓝牙设备接收到ID包后会将自己的设备信息封装到FHS包中做出响应，控制器解析FHS包获取所需的信息，并使用一个或多个查询结果事件将找到的设备相关信息返回给主机Host。



步骤3（a）：如果主机Host希望停止搜索查询，则使用HCI\_Inquiry\_Cancel命令通知控制器Controller立即停止查询过程，控制器接收到指令就会停止对外发送ID包执行停止查询流程。

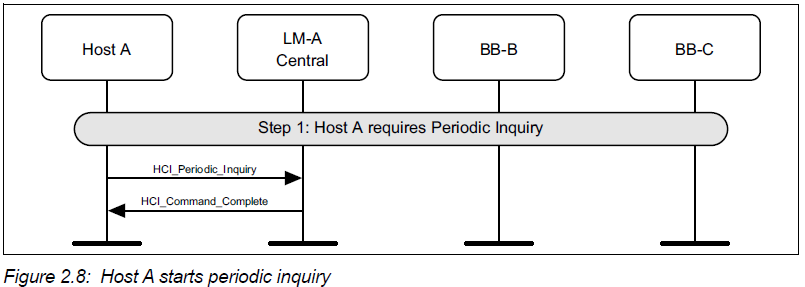


步骤3（b）：如果主机Host没有主动停止查询，则控制器Controller会在查询上报的结果已达数量限制或者查询时长已到而停止查询，并将查询的完成事件上报给Host。

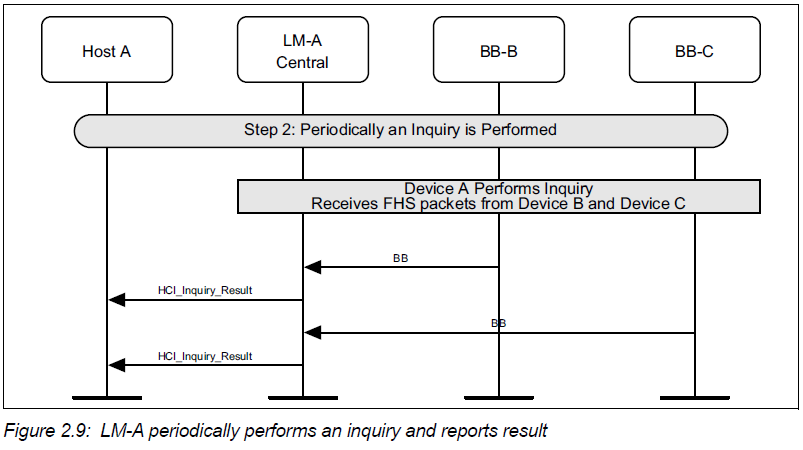


### Periodic inquiry

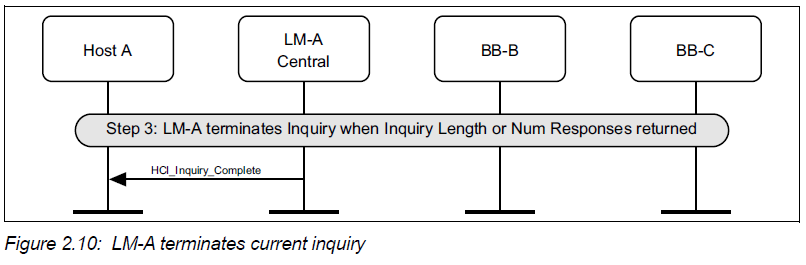
步骤1：蓝牙Host通过命令HCI\_periodic\_Inquiry告知控制器Controller进入查询模式，用于发现周围环境中的其他蓝牙设备。



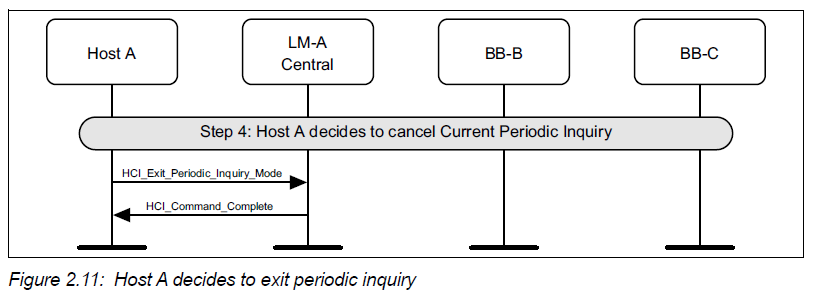
步骤2：蓝牙控制器Controller接收到上层开启搜索指令后,将周期性的查询周围蓝牙设备，在查询过程中，控制器会向Host返回一个或多个查询结果事件。



步骤3（a）：当inquiry结束，会返回一个HCI\_Inquiry\_Complete事件。



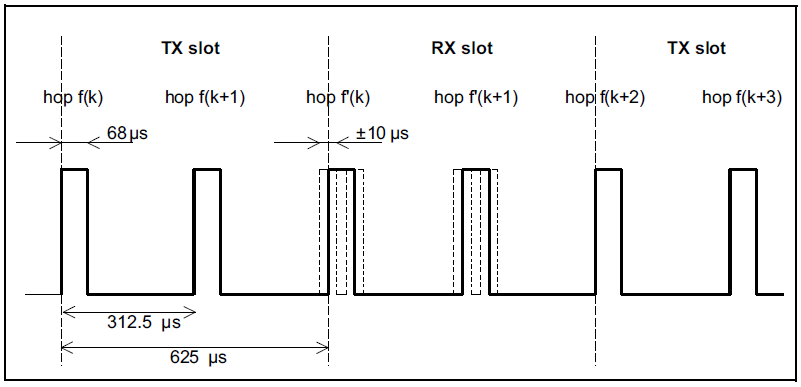
步骤3（b）：Host也可以通过使用HCI\_Exit\_Periodic\_Inquiry\_Mode命令，来终止periodic inquiry。



## Timing

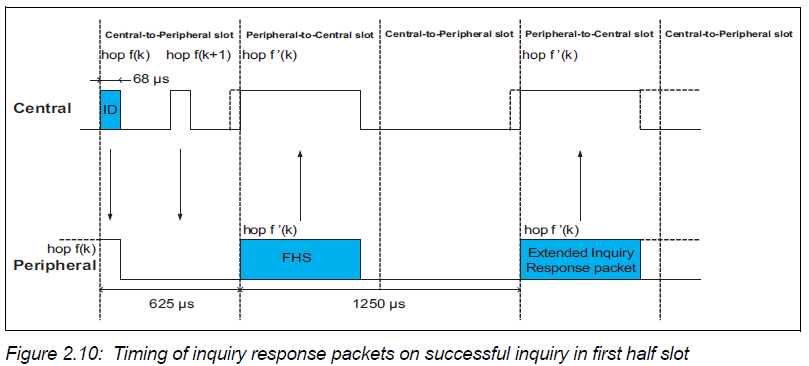
### Inquir timing

Inquiry过程中，由于需要发送的数据包（ID packet）较短，可以在单个TX slot中，分别由两个不同的频率各发送一次，跳频速率达到3200次/s（注意：只有在TX slot中会进行发送，RX slot中不会发送，所以总体速率不会达到3200次/s）。在单个RX slot也会在两个不同频率上发送和侦听各一次，在侦听时，会有10us的uncertainty window，提高数据接收的成功率和完整度（防止central和peripheral在始终对其上有偏移）。

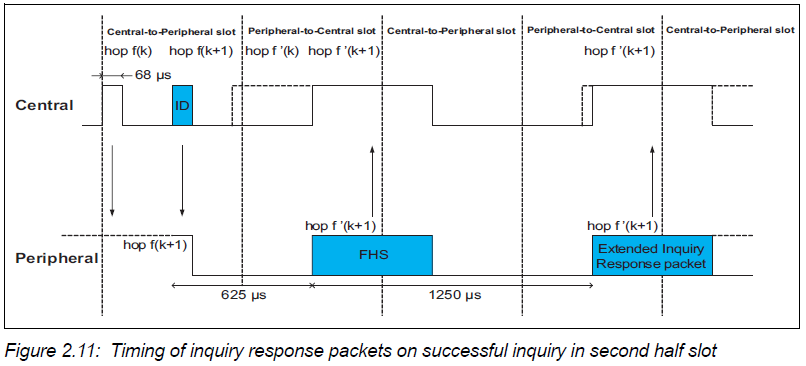


### Inquiry response timing

外设在收到central的ID packet 625us后，会向central发送查询回复包（FHS），并在此1250us后，又发生额外查询回复包（EIR），两次回复的频率一致。

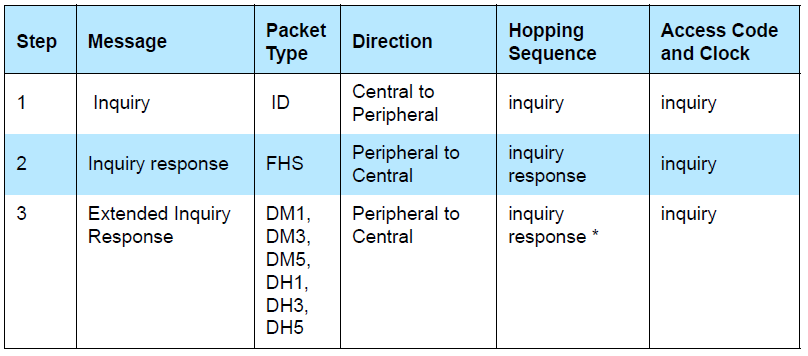


当外设收到的是该slot中发送的第2个ID packet时，则其相应的其他的回复也会往后挪半个slot，两次回复的频率也都换成f’(k+1)。



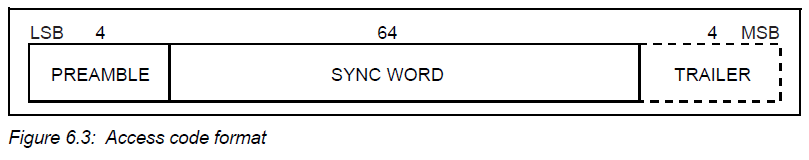
## Packet

本过程中涉及到三种数据包，下面分别简单介绍一下。



### ID packet

在inquiry中，使用的是68位的shortened access code，仅由preamble、sync word两部分组成。起到Synchronization、DC offset compensation、Identification这三个作用。



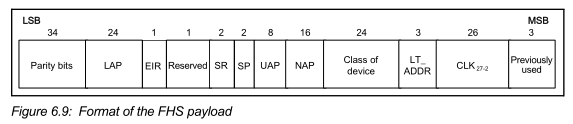
preamble的取值与sync word中的LSB位有关，当LSB为0时，preamble为0101；当LSB为1时，preamble为1010。



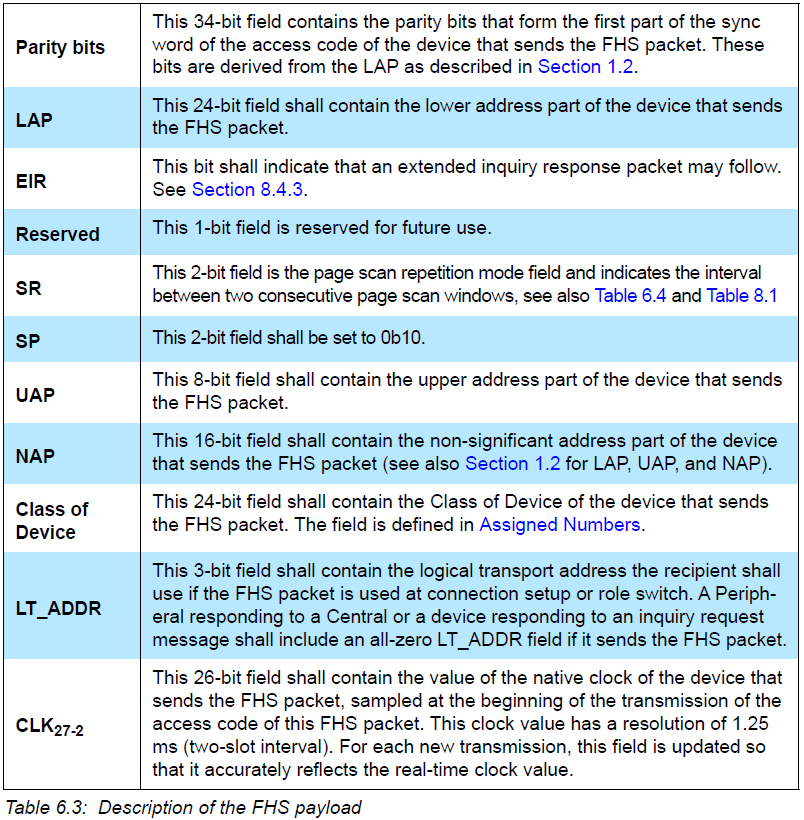
Sync word即同步字，其作用类似于数据包的header，作为数据信息开始的部分，表明其后为正式的数据信息。

### FHS packet

其包含的主要内容有蓝牙设备地址（the Bluetooth Device Address）和发送方时钟（the clock of the sender）。他由144位information，16位CRC，再加上通过使用rate 2/3 FEC进行编码，一共是240位。

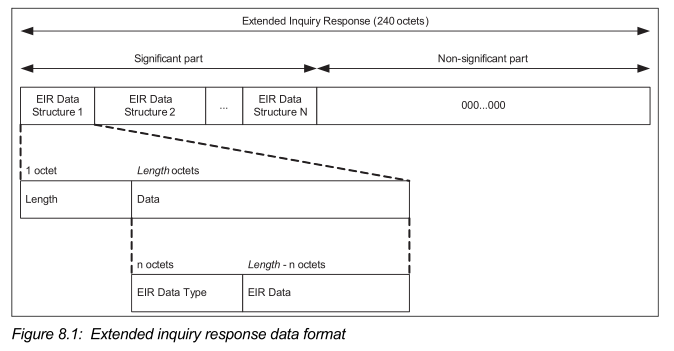


其各参数信息如下：



### Extended inquiry response packet

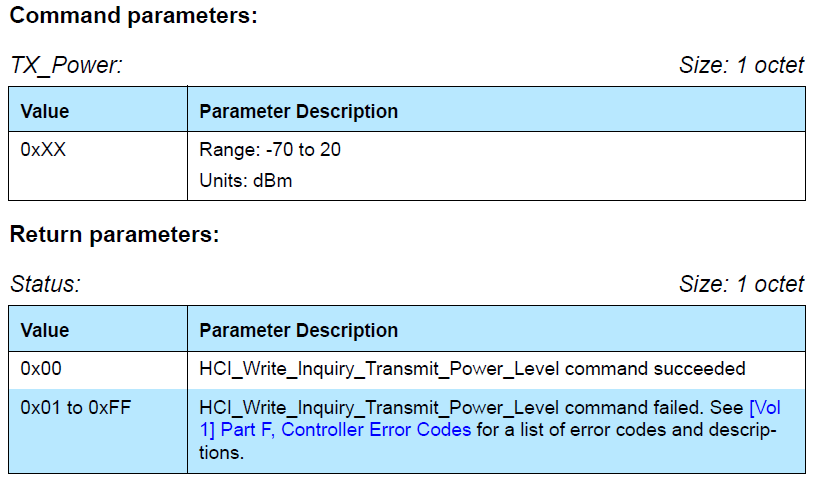
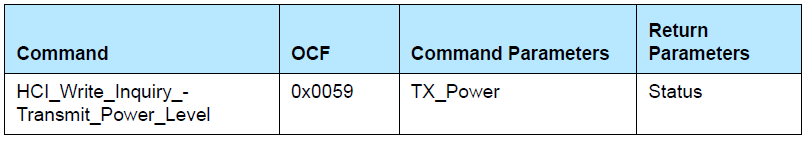
该数据包中主要包含有一些设备的相关信息。其数据结构组成包括，n个有意义的EIR数据结构，每个数据结构有1 octet 长度数据L和L octets数据，该数据由前n octets表示EIR数据类型，后面的L-N octets数据取决于EIR数据类型的值，成为EIR数据。最后用0整个数据扩展到240 octets。



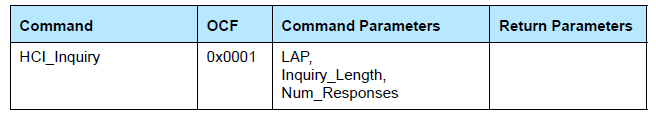
## 相关命令事件

### Write Inquiry Transmit Power Level command

在inquiry过程之前，首先需要通过该命令设置向外发送ID包的功率，通过调节参数TX\_Power进行设置。



### Inquiry command

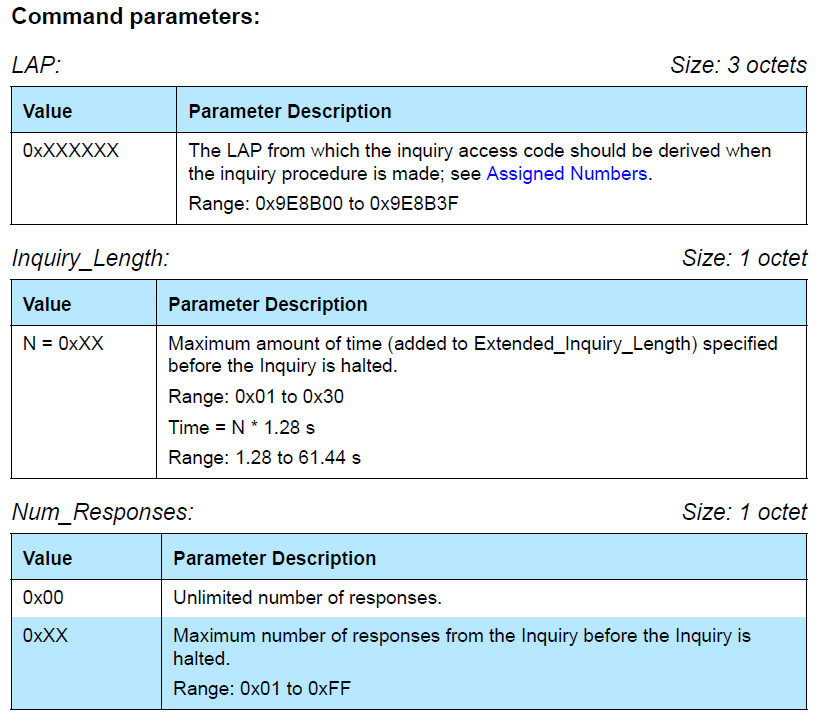


LAP：IAC就是从该值派生得到的，具体取值范围为是0x9E8B00 ~ 0x9E8B3F，但是只有 0x9E8B00 和 0x9E8B33 这两个数值是有效的，其他值保留供将来使用。

0x9E8B33 代表一般/无限制查询访问代码（GIAC）

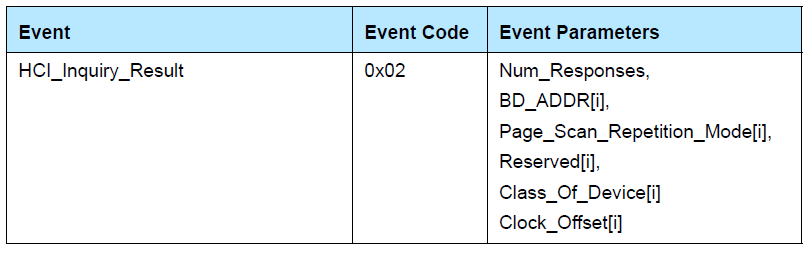
Inquiry\_Length：查询模式的总持续时间，当此时间超时后查询将被停止

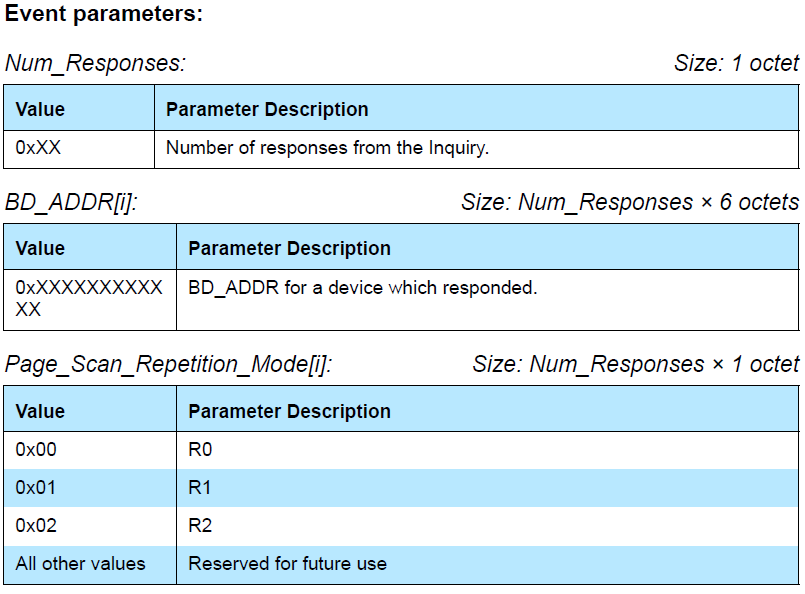
Num\_Responses：在查询停止之前可以接收的响应数，当响应数达到该值后，控制器Controller停止当前的查询，并上报Host查询完成事件。

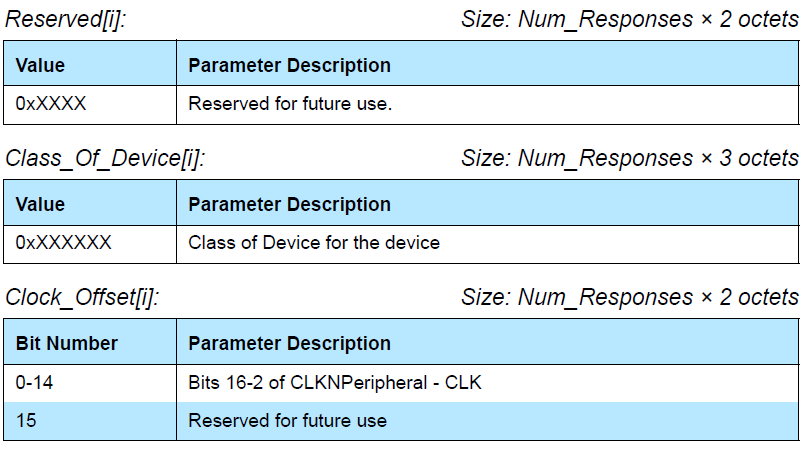


### Inquiry Result event

表示控制器在查询过程中的一种相应，该事件可以返回一个或多个查询响应。

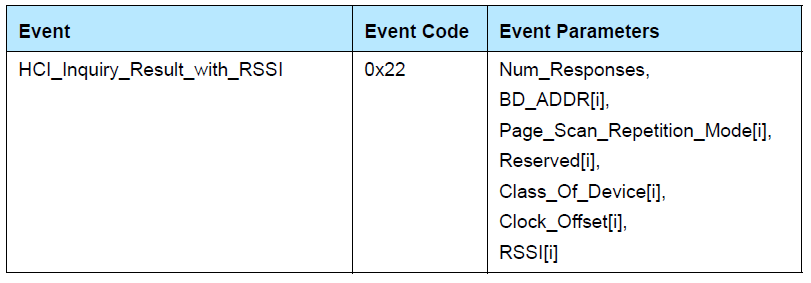




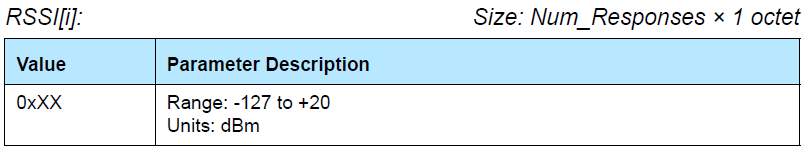


### Inquiry Result with RSSI event

RSSI:the Received Signal Strength Indication，与上一个事件的区别，就是事件会多返回一个关于首位蓝牙设备返回的信号质量的参数。

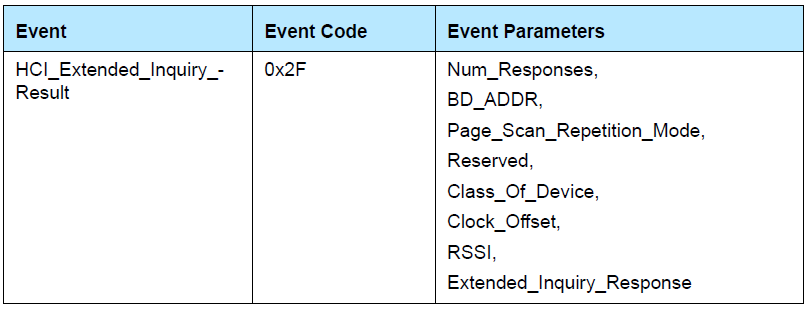


下面是参数介绍，除RSSI外，其余参数在上个事件中已经介绍，此处不再赘述。

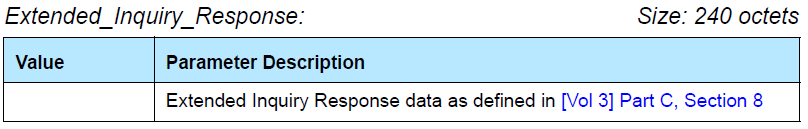


### Extended Inquiry Result event

与上述两个事件不同的是，该事件每个事件只能对应一个响应，即Num\_Responses=1，且会返回一些关于设备的信息，包括remote name、支持的UUID等。只有当inquiry response packet：EIR=1，且同时Inquiry\_Mode = 0x02，才能收到Inquiry Result with RSSI event。

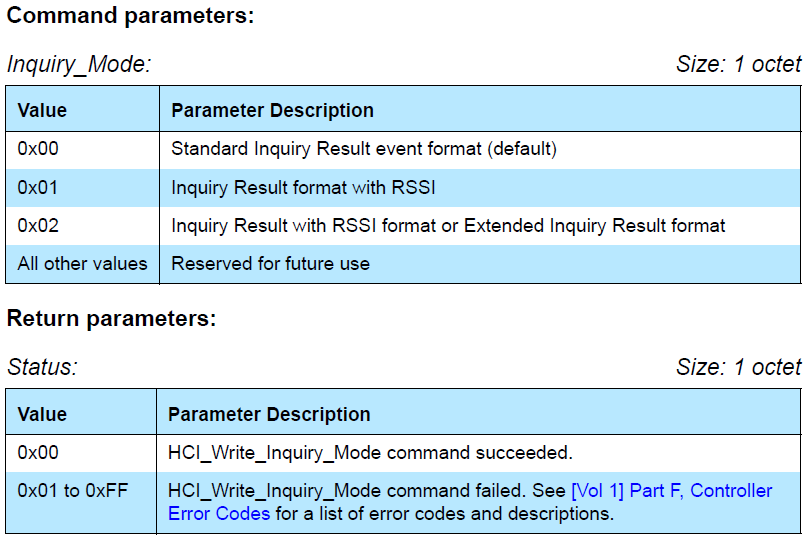
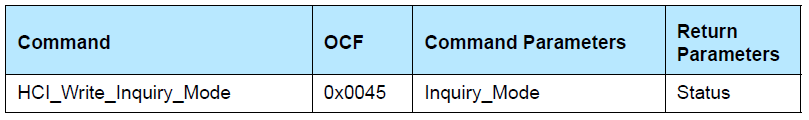


下面是参数介绍，除Extended\_Inquiry\_Response外，其余参数在上个事件中已经介绍，此处不再赘述。



### Write Inquiry Mode command

这个命令用来设置本地BR/EDR Controller 的Inquiry\_Mode。Inquiry\_Mode（1 Octet）：搜索模式，0x00表示标准的inquiry result result event，0x01表示inquiry result with RSSI，0x02表示inquiry result with RSSI or Extened inquiry result 。



# Inquiry Scan Substate Induction

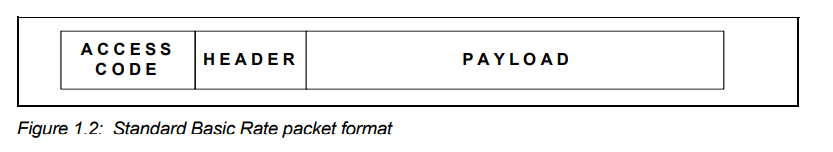
## 一、基础概念

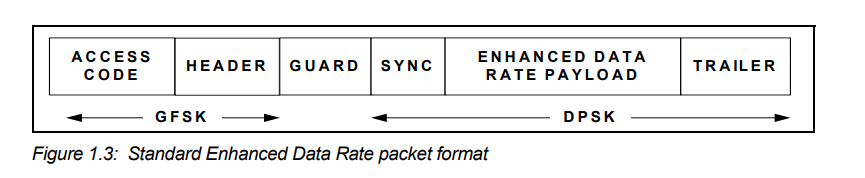
1. 标准基础速率包格式

基础数据速率包主要包扩访问码，包头，以及有效载荷体三部分

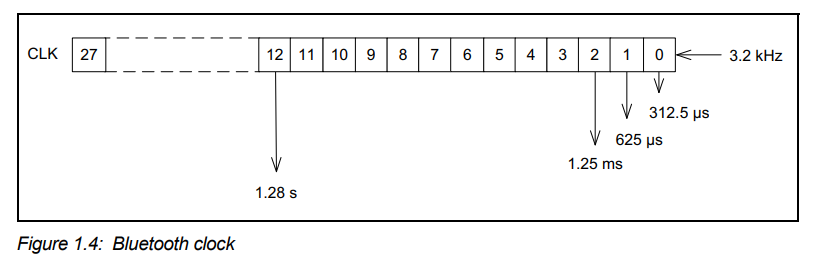
1. 标准增强数据速率包格式

增强数据速率包主要包括访问码，包头，保护字段，同步字段，以及增强速率数据有效载荷体和包尾。





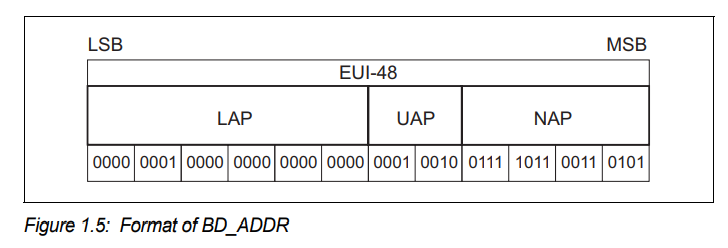
1. 蓝牙时钟



每个蓝牙设备都有一个本地时钟，时钟使用28位的计数器实现，最低有效位以312.5μs为单位，时钟频率为3.2kHz。

1. 蓝牙地址

每个蓝牙设备都应分配⼀个唯⼀的48位蓝牙设备地址(BD\_ADDR)，蓝牙设备为查询操作保留64个连续LAP值；其中有一个通用的LAP保留值用于设备的⼀般查询，其余63个LAP保留值用于特定类别设备的专用查询。保留的 LAP 地址为 0x9E8B00 到 0x9E8B3F。



1. 访问码

在蓝牙系统中，物理信道上的所有传输都以访问码开始。所有访问代码均来⾃设备地址或查询地址的LAP。通用查询访问码（GIAC）用于通用查询操作，专用查询访问码（DIAC）用于专用查询操作。访问码还将向接收者指示数据包的到达，并且还将用于时序同步和偏移补偿。访问码也是物理信道的属性，当多个设备在同一个频段发送信息时，接受者通过访问码识别该信息是否属于自己。访问码始终出现在数据包的头部。访问码分为以下三种

• device access code (DAC)

• channel access code (CAC)

• inquiry access code (IAC) **:**

-general inquiry access code(GIAC)

-dedicated inquiry access codes (DIAC)

## 二、INQUIRY SCAN PHYSICAL CHANNEL介绍

1.1在查询和查询扫描中，一般将查询设备称之为Central，将查询扫描设备称之为Peripheral，在查询和查询扫描中都是用设备的本地时钟作为查询时钟。

1.2查询扫描信道遵循比微微网物理信道更慢的跳频模式，通过在射频信道的一个短的伪随机序列中实现。查询扫描信道的时序由扫描设备的本地蓝⽛时钟决定，⽽跳频序列由通⽤查询访问码（GIAC）决定。

1.3 在查询扫描物理信道上拥有32个唤醒频率，平均分布在79 MHz上，周期长度为 32。查询响应跳频序列具有与当前查询跳频序列一一对应的 32 个响应频率。

## 三、Inquiry scan过程

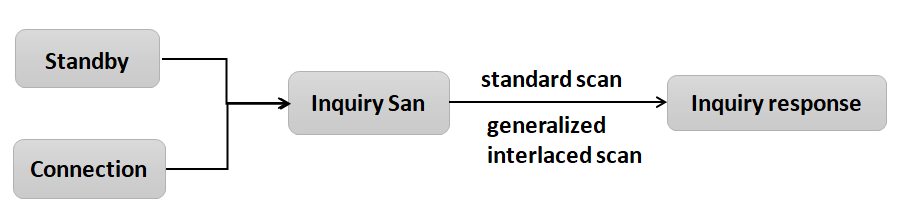


图1蓝牙状态切换图

如图1设备可以从待机状态或者连接状态进入查询扫描子状态。在待机状态下，尚未建立连接，设备可以使用所有数据包容量进行查询扫描。在从“连接”状态进入“查询扫描”子状态之前，设备应保留尽可能多的数据包容量用于扫描。如果需要，设备可以将 ACL 逻辑传输置于嗅探模式或保持模式。

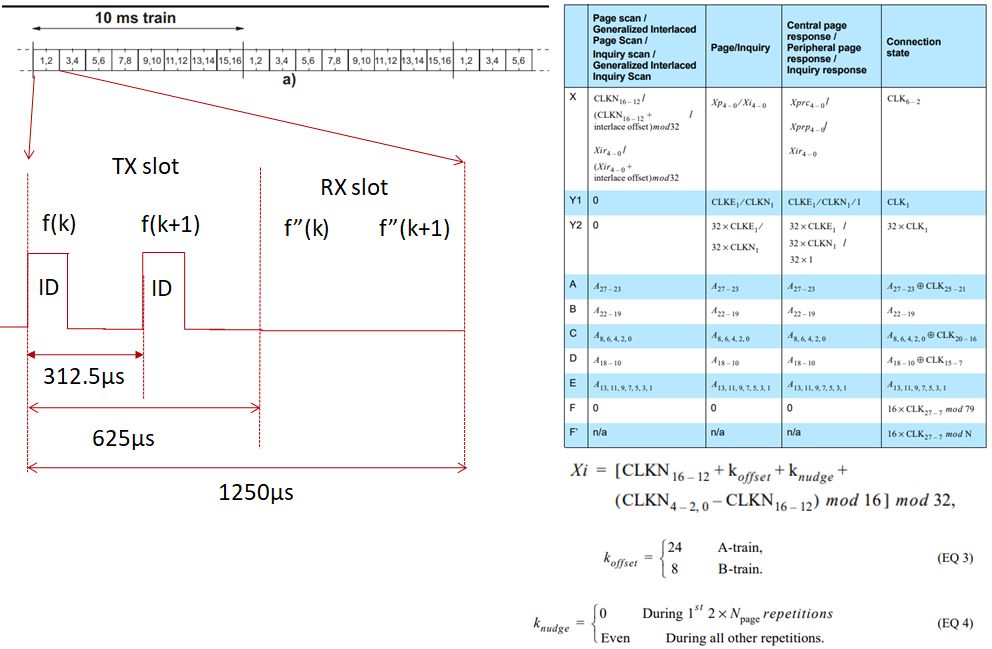


图2 Inquiry过程分析

如图2所示，在inquiry过程中，一个TX slot中，查询设备分别以f(k)和f(k+1)两个频率发送两个ID包，两次发送间隔为312.5μs,在接下来的RX slot中，查询设备分别在f”(k)和f”(k+1)两个频率监听是否有响应。整个查询过程在一个包含16个频率点的序列上循环执行。一个周期的时间为10ms。其中频率切换主要是由图中Xi输入决定，在Xi的计算公式中，主要由CLKN4-2,0和CLKN16-12决定其值得变化。CLKN4-2,0表示时钟计时器的0和2-4位发生变化时，对应的CLKN4-2,0值加1，对应的Xi值发生变化，切换频率。对应上述发送ID包过程。CLKN16-12表示时钟计时器的12-16位发生变化时，对应的CLKN16-12值加1，对应的Xi值发生变化，切换频率。CLKN16-12值改变对应时间为1.28秒。

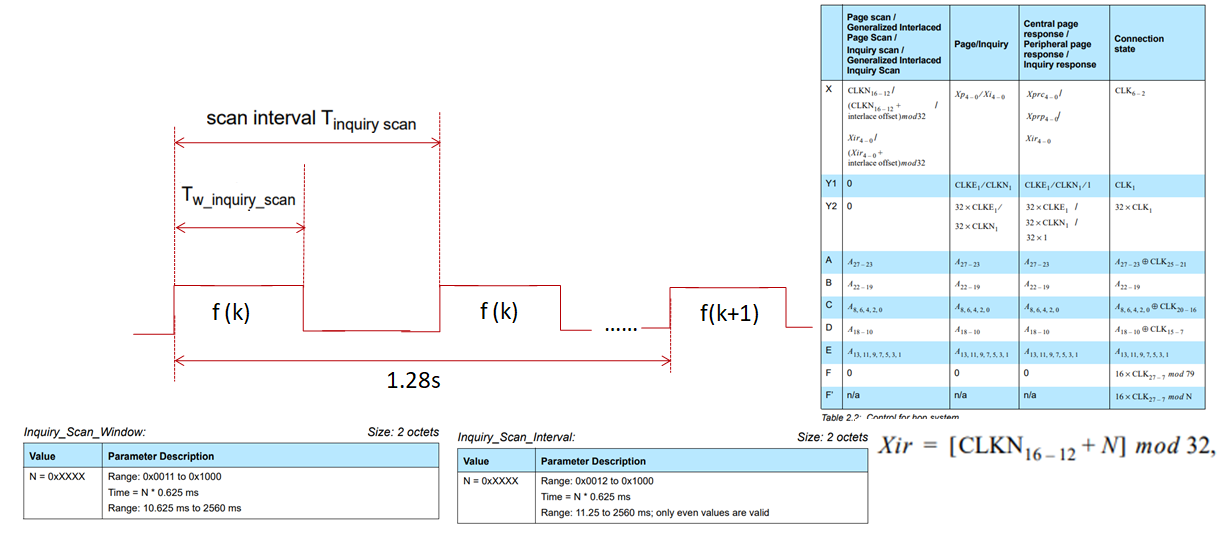
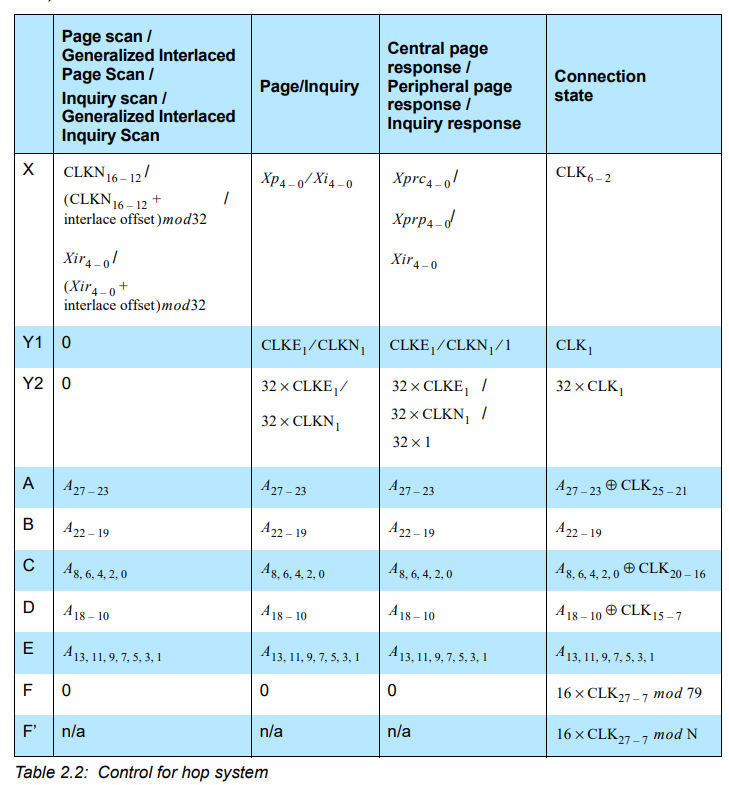


图3 Inquiry Scan过程分析



在图3中，设备进入查询扫描子状态状态后，在一个查询扫描窗口Tw\_inquiry\_scan内通过f(k)频率扫描，其中Tinquiry sacn为扫描间隔。查询扫描频率的选择与Xir有关，而Xir的值主要由CLKN16-12决定，当经过1.28s后，CLKN16-12的值加1，查询扫描切换到下一个频率，继续进行一个频率的周期性扫描。

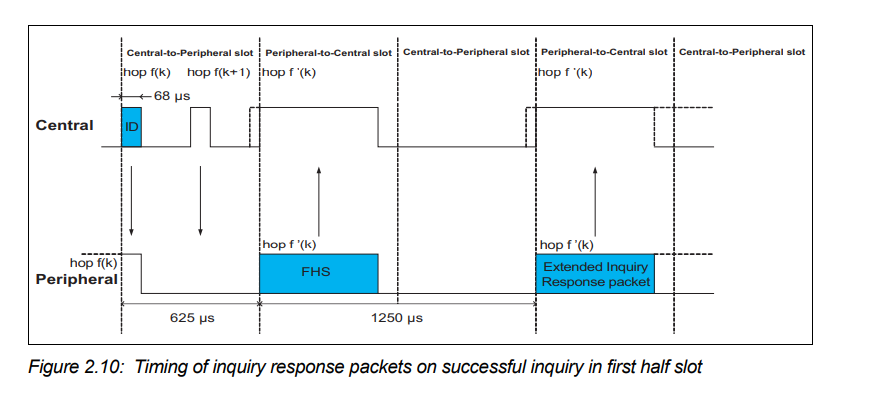
在上述的查询和查询扫描的跳频规则中，查询设备每隔10ms会扫描完16个频率点，而扫描查询设备每隔1.28s切换一次频率，这样一块一慢的频率切换，最终会使得查询扫描设备与查询设备在某个时刻某个频率相遇，从而使得查询扫描设备接收到查询设备发送的ID packet。

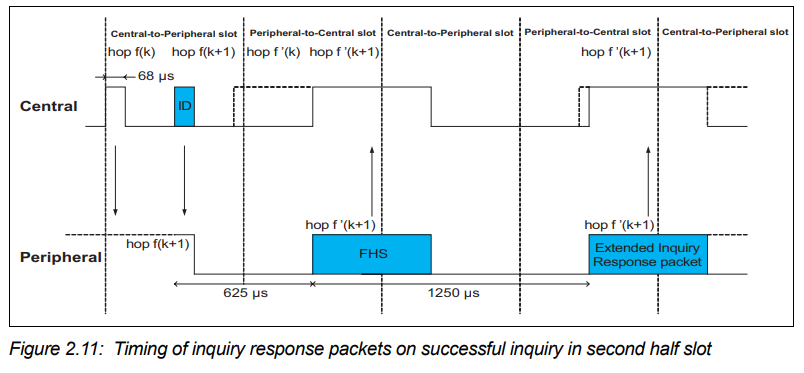
当设备进入查询扫描子状态后，设备通过在16个查询频率中扫描查询访问码。通常有两种扫描类型，标准扫描和广义隔行扫描。在标准扫描中，扫描窗口的长度为Tw\_inquiry\_scan（默认为11.25ms）,其以Xir4-0定义的单跳频频率来工作。在广义隔行扫描中，由背对背的两次扫描组成， Tw\_inquiry\_scan为扫描窗口，第一次扫描为正常的跳频频率扫描，第二次扫描定义频率为[Xir4-0 + interlace\_offset] mod 32进行扫描。如果扫描间隔不是扫描窗口的至少两倍，那么广义的隔行扫描将不被使用。

查询扫描过程使用查询跳频序列中特定的32个跳频。这些频率由一般查询地址决定。相位由执行查询扫描的设备的本机时钟确定。相位每1.28秒变化一次。interlace\_offset值的范围从 0 到 31。如果在查询唤醒期间收到查询消息，设备应进入查询响应子状态。

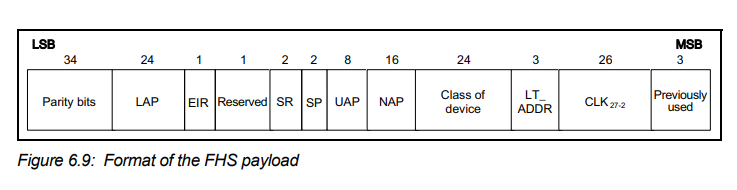
当在查询扫描子状态中接收到查询消息时，进入查询响应子状态，在间隔625μs后如下图所示接收方应返回一个查询响应（FHS）包，其中包含接收方的设备地址（BD\_ADDR）和其他参数。 如果接收方有非零扩展查询响应数据要发送，它应在 FHS 包之后返回一个扩展查询响应包。

在查询扫描子状态中收到第一个查询消息时，外围设备应进入查询响应子状态。如果 Peripheral 有非零扩展查询响应数据要发送，它应在收到查询消息后 625 μs 向 Central 返回一个 EIR 位设置为 1 的 FHS 数据包。然后它应在 FHS 数据包开始后 1250 μs 返回一个扩展查询响应数据包。如果外设的扩展查询响应数据全为零，则外设应仅返回 EIR 位设置为零的 FHS 数据包。

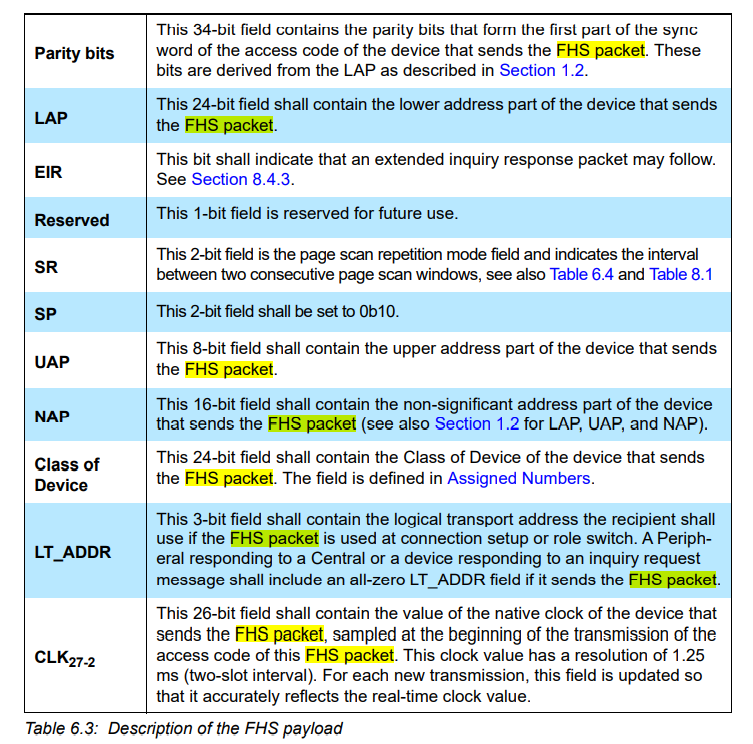




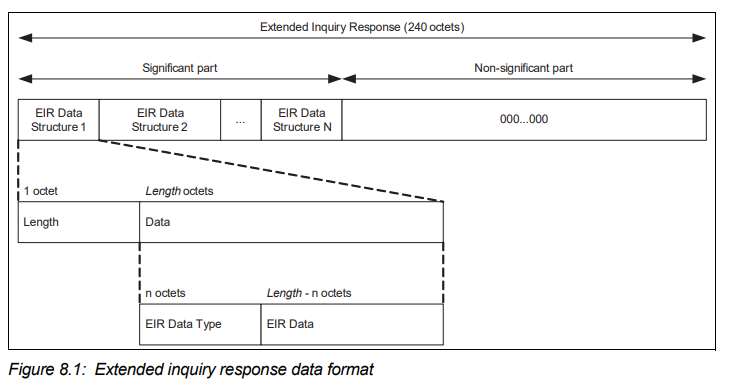
上述过程中的FHS包格式如下图所示：



对应的个字段含义如下表所示：



Extended Inquiry Response packet的格式如下图所示：



当几个设备靠近查询设备并且都同时响应查询消息时，可能会出现争用问题。然而，因为每个设备都有一个自由运行的时钟，所以它们都使用查询跳跃序列的相位相同的可能性很小。为了避免在同一查询跳信道中同时唤醒的设备之间的重复冲突，设备应回退一段随机时间。因此，如果设备收到查询消息并返回 FHS数据包，它应生成一个随机数RAND，介于 0 和MAX\_RAND。对于大于1.28 s 的扫描间隔，MAX\_RAND 应为 1023，但是，对于小于1.28 s 的扫描间隔，MAX\_RAND 可能小至 127。使用特殊 DIAC 的配置文件可以选择使用小于 1023 的 MAX\_RAND，即使扫描间隔大于1.28 秒。外设应在至少 RAND 时隙的持续时间内返回连接或待机状态。在返回连接和待机状态之前，设备可能会经历页面扫描子状态。在至少 RAND 时隙之后，设备应在查询跳序列中的相位中添加 1 的偏移量并再次返回查询扫描子状态。如果外设再次触发，它应使用新的 RAND 重复该过程。每次返回 FHS 数据包时，时钟的偏移量就会累积。在探测窗口期间，外设可能会多次响应，但频率不同，时间也不同。

保留的同步时隙应优先于响应数据包；也就是说，如果响应包与保留的同步时隙重叠，则不应发送，而是等待下一个查询消息。如果设备具有要发送的扩展查询响应数据，但扩展查询响应数据包与保留的同步时隙重叠，则可以发送 FHS 数据包，并将 EIR 位设置为零。