

蓝牙设备发现与同步

蓝牙设备的发现和同步简介

蓝牙设备在建立连接以前，通过在固定的一个频段内，选择跳频频率或由被查询的设备地址决定，迅速交换握手信息时间和地址，快速取得设备的时间和频率同步。建立连接后，设备双方根据信道跳变序列改变频率，使跳频频率呈现随机特性。

蓝牙系统定义了种工作状态下的跳频序列寻呼、寻呼响应、查询、查询响应和信道跳变序列，不同状态下的跳频序列产生策略不同。

蓝牙定义了32个频点为一个频段，划分为79个子频段，工作的频段及跳频顺序，取决于所输入的蓝牙主控设备时钟和主控设备地址的最低28比特有效位，即BD_ADDR[0...27]或者28比特通用查询接入码(General Inquiry Access Code, GIAC)。

1) 查询/查询扫描状态:

蓝牙设备通过查询来寻找在其周围邻近的设备，查询设备每隔312.5微秒选择一个新的频率来发送查询，被查询设备每隔1.28s选择一次新的监听频率。查询和被查询设备使用通用查询接入码(GIAC, General Inquiry Access Code)LAP(Low Address Part)作为查询地址，GIAP LAP为0x9E8B33。蓝牙标准规定不允许任何蓝牙设备使用和GIAP LAP一样的地址。产生的32个查询跳变序列(Inquiring hopping sequence) 均匀分布在79个频率信道上。

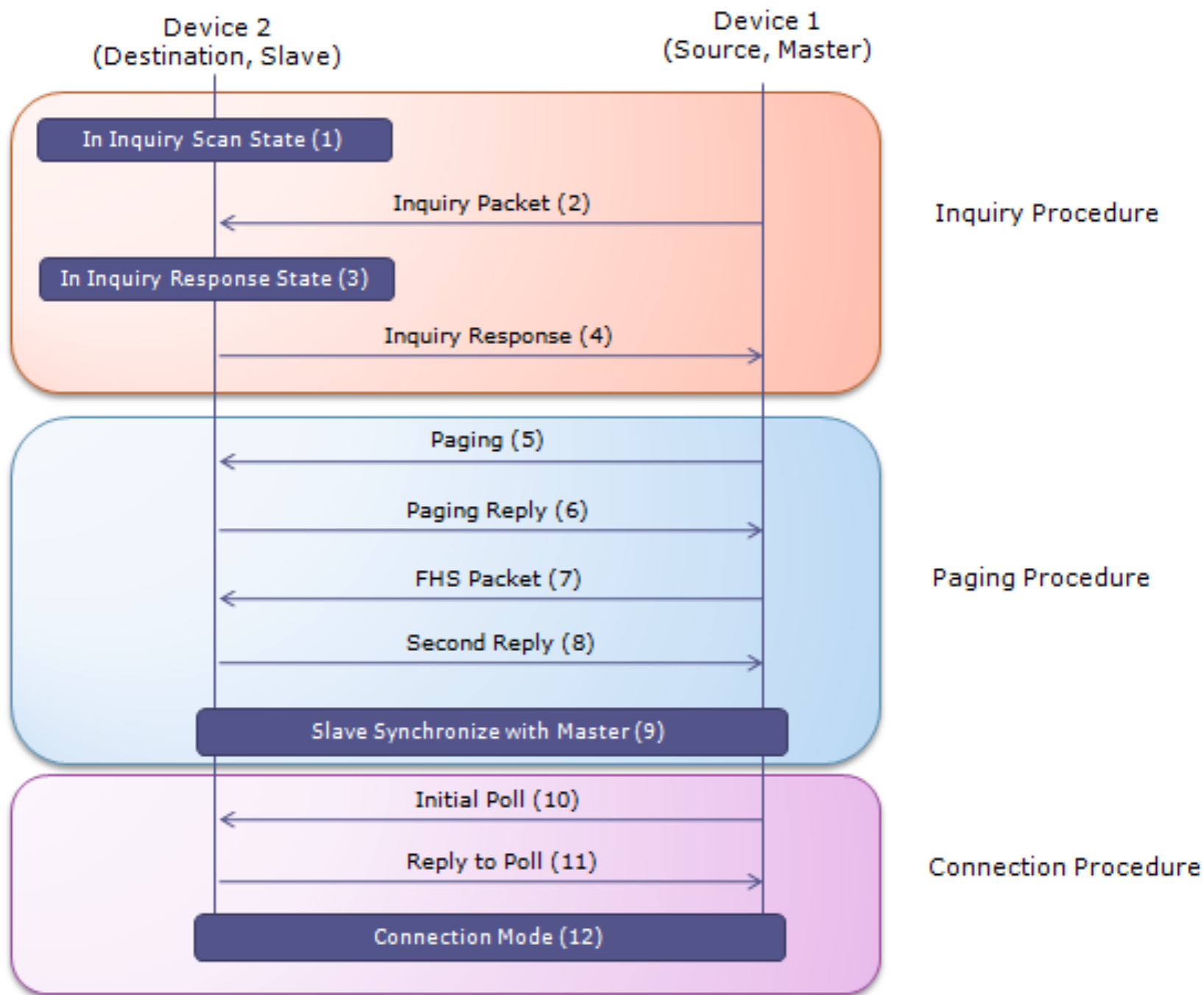
2) 寻呼/寻呼扫描状态:

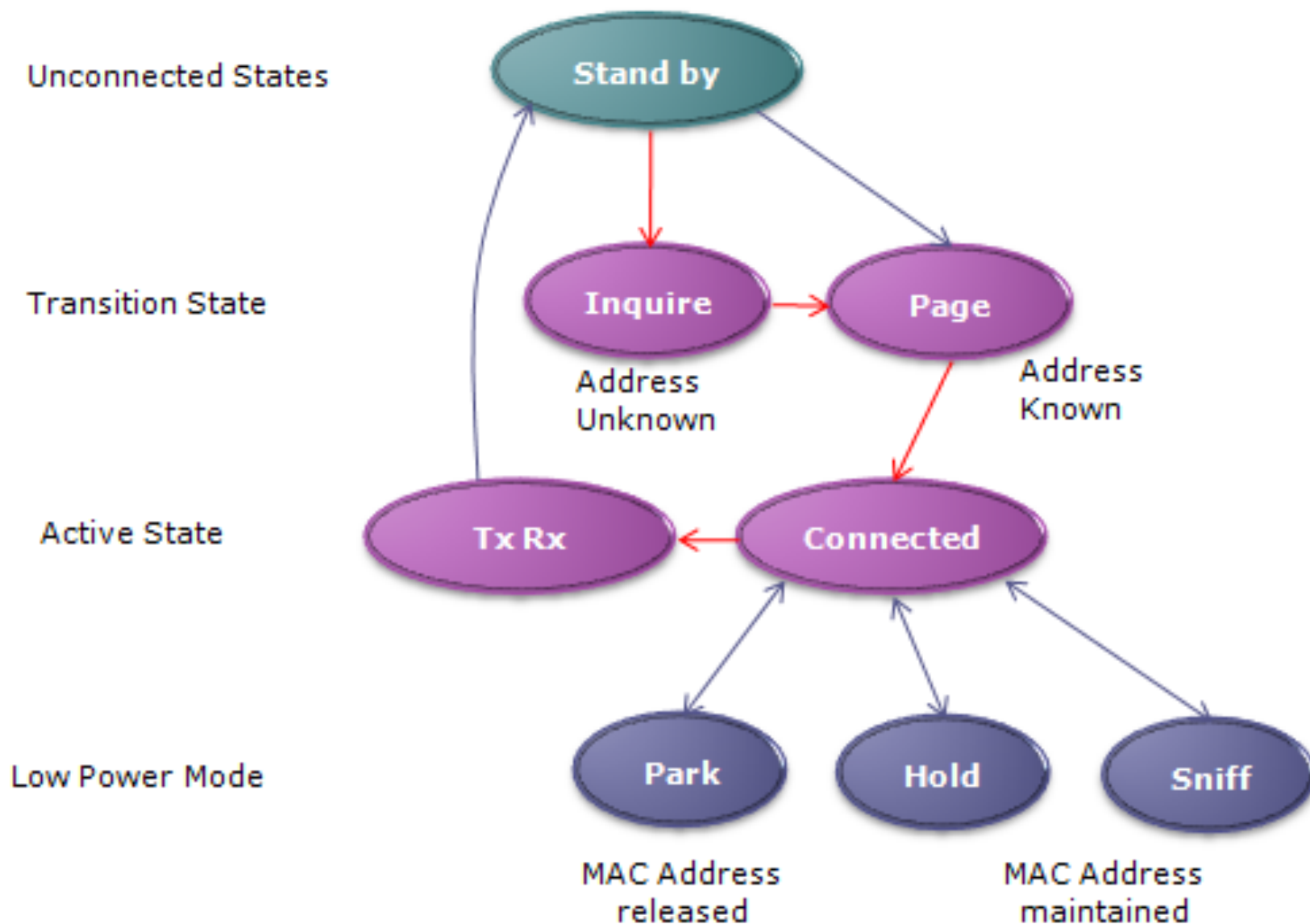
蓝牙设备通过寻呼来呼叫其它的设备加入其所在的[微微网]，寻呼设备每隔312.5微秒选择一个新的频率来发送寻呼，在寻呼扫描时，被寻呼设备每隔1.28s选择一个新的监听频率。寻呼和被寻呼设备，使用被寻呼设备地址(BT_ADDR)的低28个比特，产生的寻呼跳变序列(paging -hopping sequence)是一个定义明确的周期序列，它的各个频点均匀分布在2.4G的79个频率信道上。

3) 连接状态:

在当前状态下，蓝牙通信设备双方每隔625微秒改变一个频率，使用主设备地址的最低28位有效位，产生的信道跳变序列(Channel hopping sequence)周期非常长，而且79跳变序列在任何的一小段时间内都是接近均匀分布的。

蓝牙状态转换图:





上图是蓝牙状态转换图，从图中可以看出STANDBY状态是蓝牙设备的默认状态。此模式下设备处于低功耗状态。

- inquiry: 这就是我们通常所说的**扫描状态**，这个状态的设备就是去**扫描周围的设备**。它是不知道周围有什么设备，要去查询（调查），类似于广播（吆喝）。处于Inquiry Scan的设备可以回应这个查询。再经过必要的协商之后，它们就可以进行连接了。此处需要说明的是：Inquiry之后，不需要进入Page就可以连接上设备。
- inquiry scan: 这就是我们通常看到的**可被发现的设备**，进入该模式，才能够被别的蓝牙设备搜索到。体现在上层：我们在

android系统中点击设备可被周围什么发现，那设备就处于这样的状态。

- inquiry response：就是inquiry scan的设备，在收到inquiry的消息后，就会发送inquiry response的消息，在这之后它就会进入到了inquiry response的状态了。
- page：通常称为的连接(寻呼)，进行连接/激活对应的slave的操作我们就称为page。它是指：发起连接的设备（主设备）知道要连接设备的地址。所以可以直接传呼。
- page scan：和page对应的，就是等待被page的slave所处的状态，换句话说，若想被page到，我们就要处于page scan的状态。
- slave response：这个就是在page的过程中，slave收到了master的page消息，它会回应对应的page response消息，同时自己就进入到了slave response的状态。
- master response：master收到slave response的消息后，他就会进入到master response的状态，同时他会发送一个FHS的packet。

以上的各种状态可以总结到下面的寻呼过程中：即寻呼过程按照如下步骤进行：

- 1) 一个设备（源）寻呼另外一个设备（目的），此时处于寻呼状态（Page）
- 2) 目的设备接收到该寻呼，此时处于寻呼扫描状态（Page Scan）
- 3) 目的设备发送对源设备的回复，此时处于子设备响应状态（Slave Response）
- 4) 源设备发送FHS包到目的设备，此时处于主设备响应状态（Master Response）
- 5) 目的设备发送第二个回复给源设备，此时处于子设备响应状态（Slave Response）
- 6) 目的和源设备切换并采用源信道的参数，此时处于主设备响应状态和子设备响应状态