# 蓝牙协议栈

参考链接：

<https://blog.csdn.net/XG_2013/article/details/80864527>

# GAP

## 一、前言

GAP（Generic Access Profile），主要工作是：

1. 它是一个最基础的 profile，其他的 profile 都是直接或者间接的引用了这个 profile。
2. 主要对Link Layer层（standby state、advertiseing state、initiating state、connection state）的状态进行抽象，转化成上层的概念。
3. 对广播数据进行封装，对于统一的格式和类型，从而达到互连的目的。比如我们扫描设备时，发现设备名称，该名称就是按照GAP 格式封装在adv报文中的，支持GAP的设备都可以识别该数据包，并解析里面的data.

## 二、profile stack

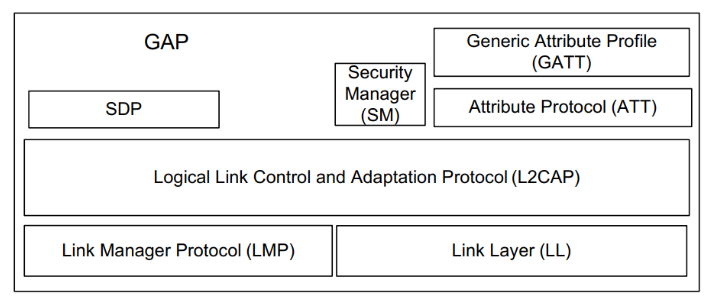


图1-1 GAP层与其他层的关系

GAP profile 描述的内容：

1. GAP的角色
2. 发现的模式和过程
3. 连接模式和过程
4. 安全模式和过程

## 三、GAP角色

GAP的角色及作用：

1. **Broadcaster设备**

broadcast 设备物理层上具备发送能力（接受能力是可选的），在Link Layer层可以处于空闲和广播状态，具备发送ADV\_NONCONN\_IND报文的能力（ADV\_SCAN\_IND的报文是可选的），不支持扫描，不支持连接

1. **Observer设备**

observer 设备物理层上具备接收能力（发送能力是可选的），在Link Layer层

可以处于空闲和扫描状态，具备被动scan能力（主动scan能力是可选的），

不支持连接，不支持广播。被动扫描指的是接收广播不发送scan\_req，主动

扫描指的是接收广播并发送scan\_req

1. **Peripheral设备**

peripheral 设备这个是我们最常用的角色，物理层上具备收发能力，在Link

Layer层可以处于空闲和广播状态，具备发送ADV\_\_IND报文的能力（其他

的广播报文是可选的），不支持扫描，支持连接，连接的时在linklayer处于

slave角色，同是支持一些连接参数的更新和加密的过程

1. **Central设备**

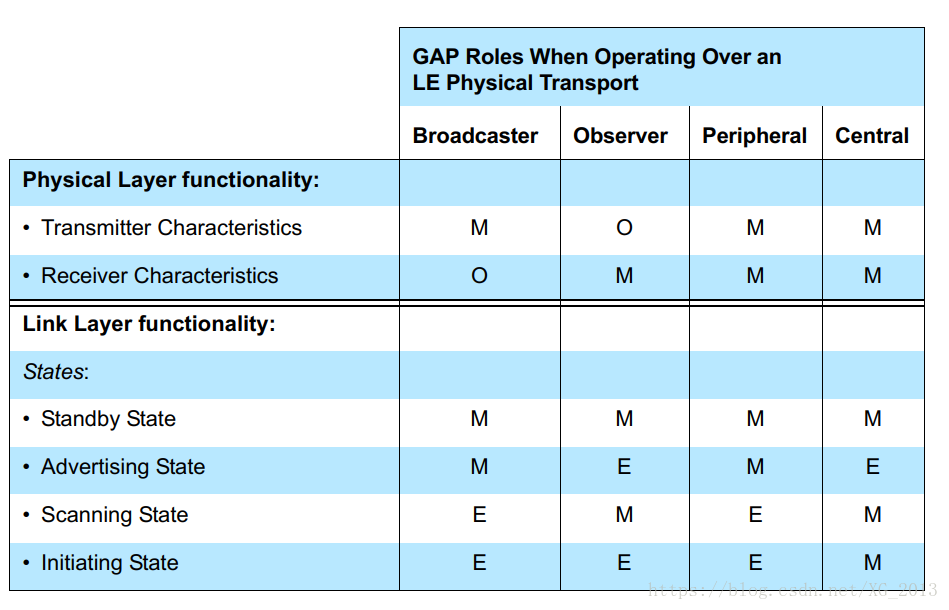
central 设备物理层上具备收发能力，在linklayer层可以处于空闲和扫描和

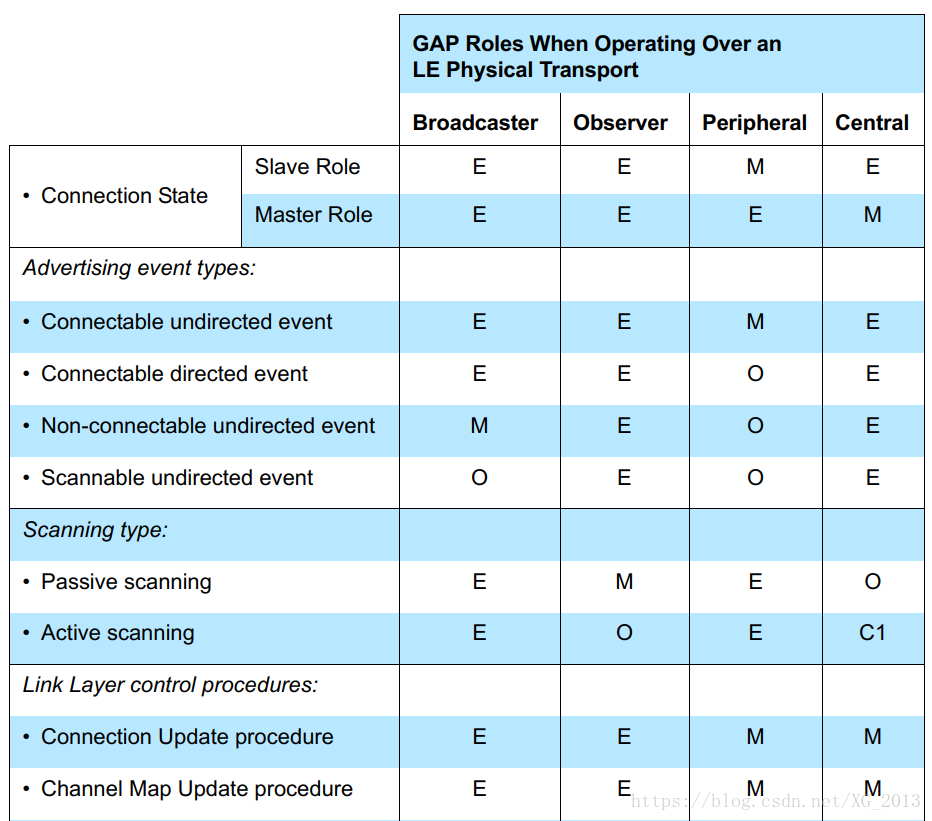
初始化状态，支持扫描，支持连接，连接的时在linklayer处于master角色，

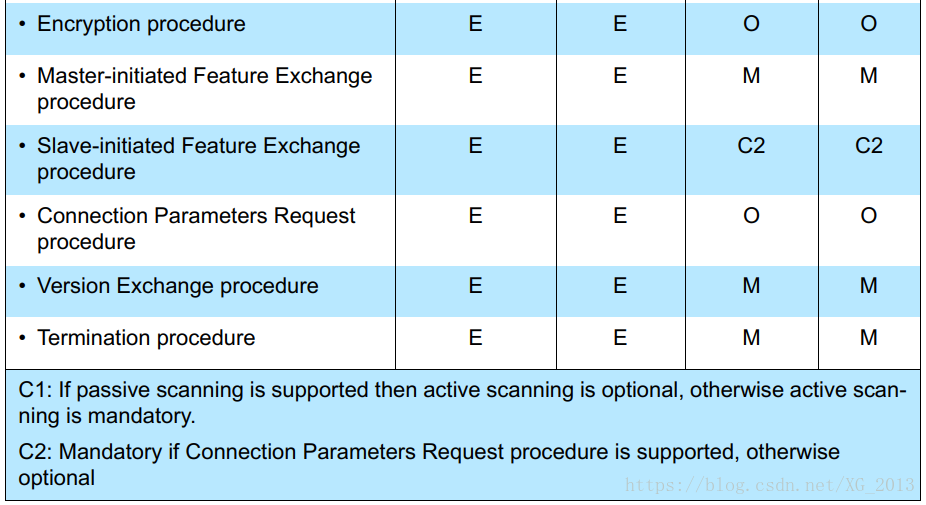
同是支持一些连接参数的更新和加密的过程

1. **注意**

设备支持多角色的，比如既是peripheral也是central







## 四、广播模式和发现过程

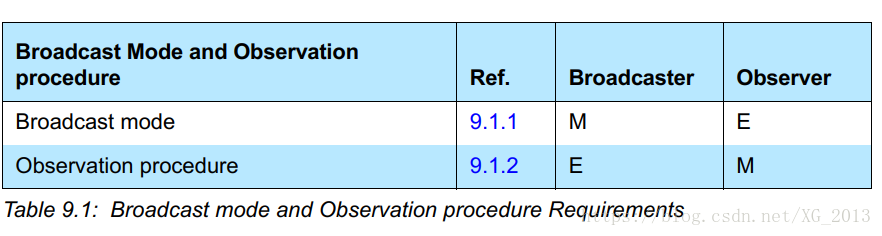


图2-3 广播模式和发现模式要求

**广播模式：**

只有broadcaster设备支持，提供了一个方法发送不可连接的广播包。一个设备处于broadcaster模式可以发送ADV\_NONOCN\_IND或者发送 ADV\_SCAN\_IND的报文。在广播报文的ADV\_TYPE格式的AD\_TYPE\_FLAGS设置成LE\_LIMITED\_DISC\_MODE或者LE\_GENERAL\_DISC\_MODE。

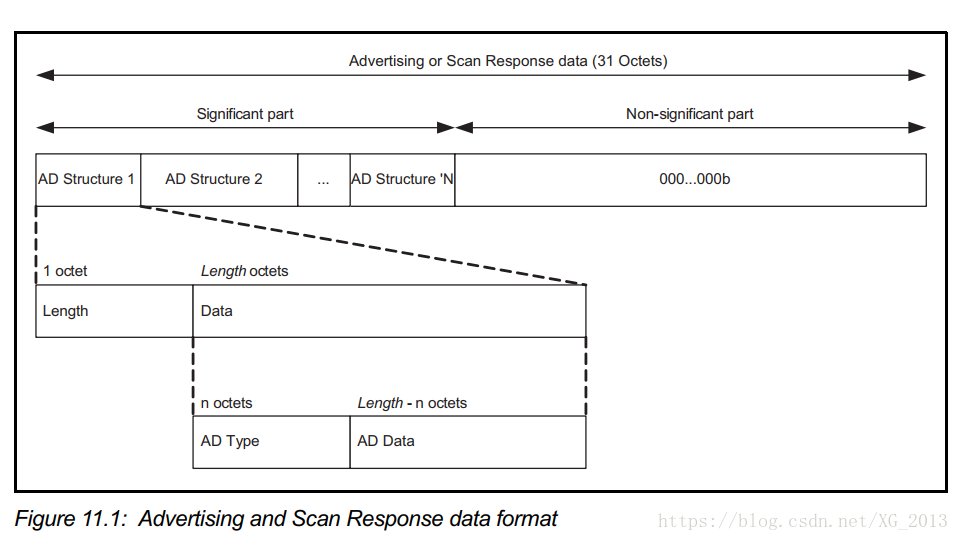


图2-4 Advertising and Scan Response data 格式

## 五、发现模式与过程

发现模式：non-discoverable和discoverable mode（discoverable mode由很多模式）

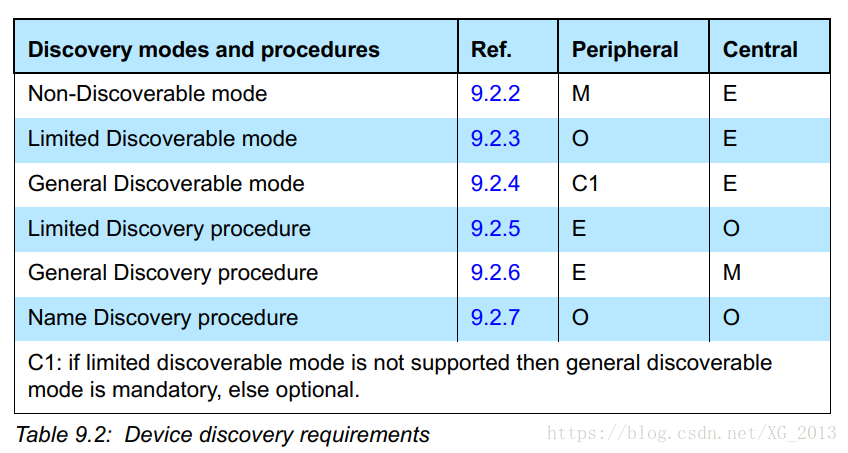


图2-5 device discovery requirements

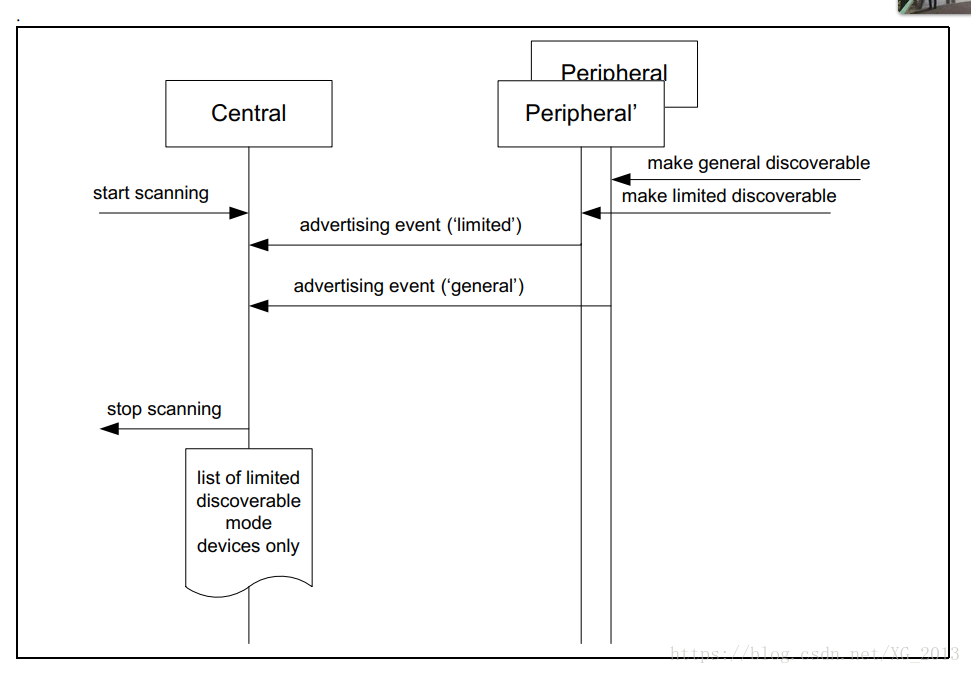
### non-discoverable mode

### 5.2 limited discoverable mode —— peripheral

作用：发送广播的时候有时限的限制，到了时间就停止广播。

### 5.3 limited discovery procedure —— central

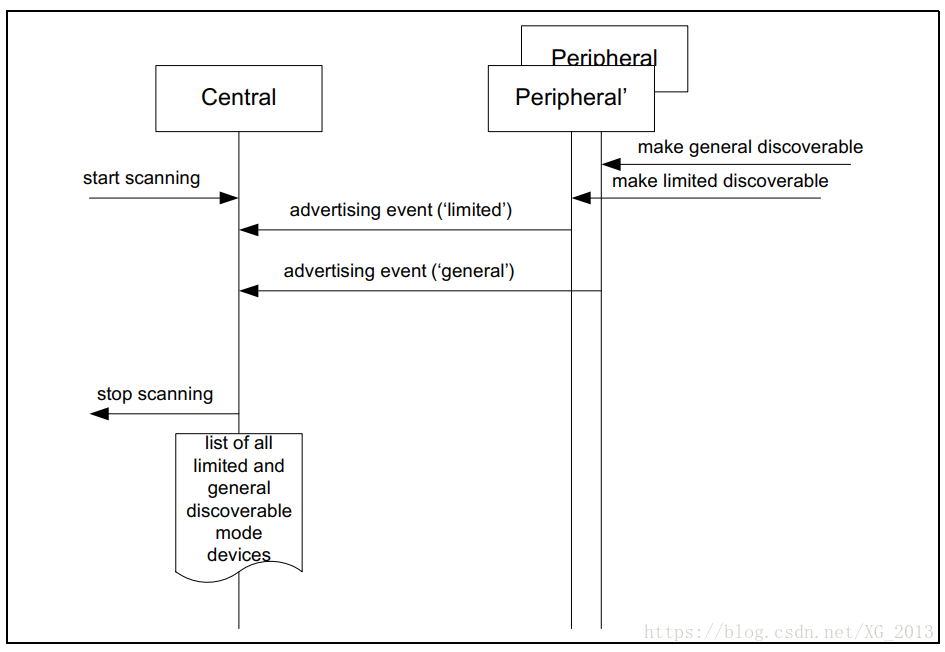
作用：它只接受limited advertising event，并且有一个scan的时限的。



### 5.4 general discoverable mode

简单的讲就是发送长时间的广播，可以通过general discovery procedure来发现

### 5.5 general discovery procedure

可以发现limited advertising event 和 general advertising event。

## 六、连接模式与过程

### 6.1 NON\_connectable mode

这个模式可以发送non-connectable undirected advertising events 或者 scannable undirected advertising events 。

peripheral、broadcaster、and observe 都支持non\_connectable mode。

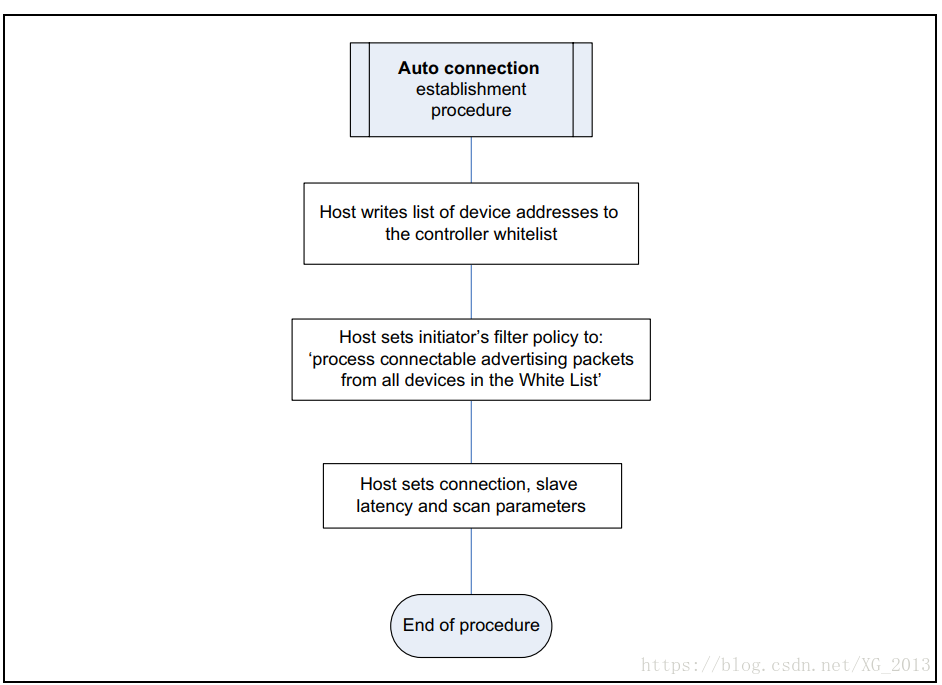
### 6.2 Directed\_connectable mode

这个模式只有peripheral角色支持，peripheral角色必须事先知道peer address.

### 6.3 Undirected\_connectable mode

这个模式只有peripheral角色支持

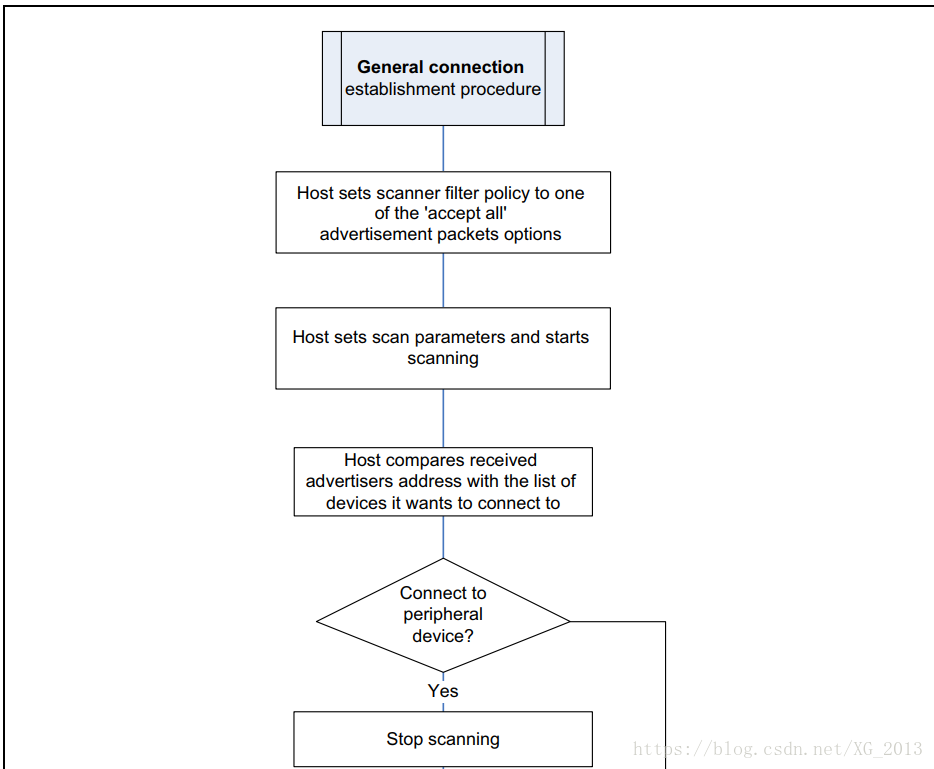
### 6.4 Auto connection establishment procedure

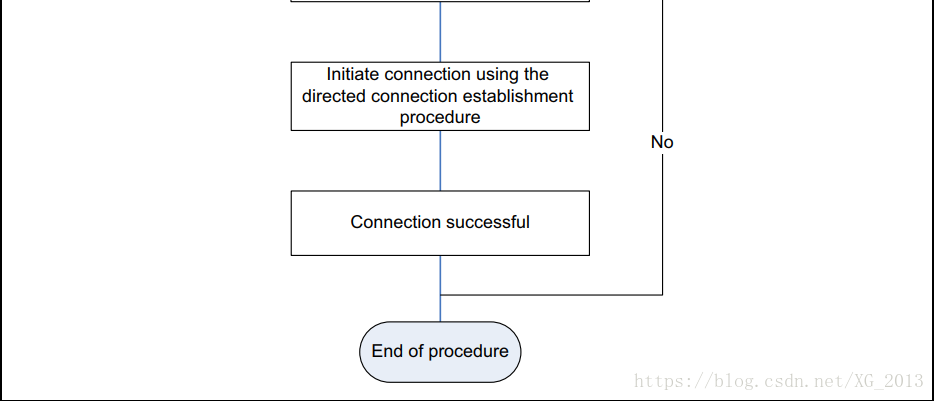


这个过程是central设备支持的，先添加白名单，设置initiator的策略运行与白名单的设备建立连接，配置连接参数，然后就ok了，很简单的过程。

### 6.5 general connection establishment procedure

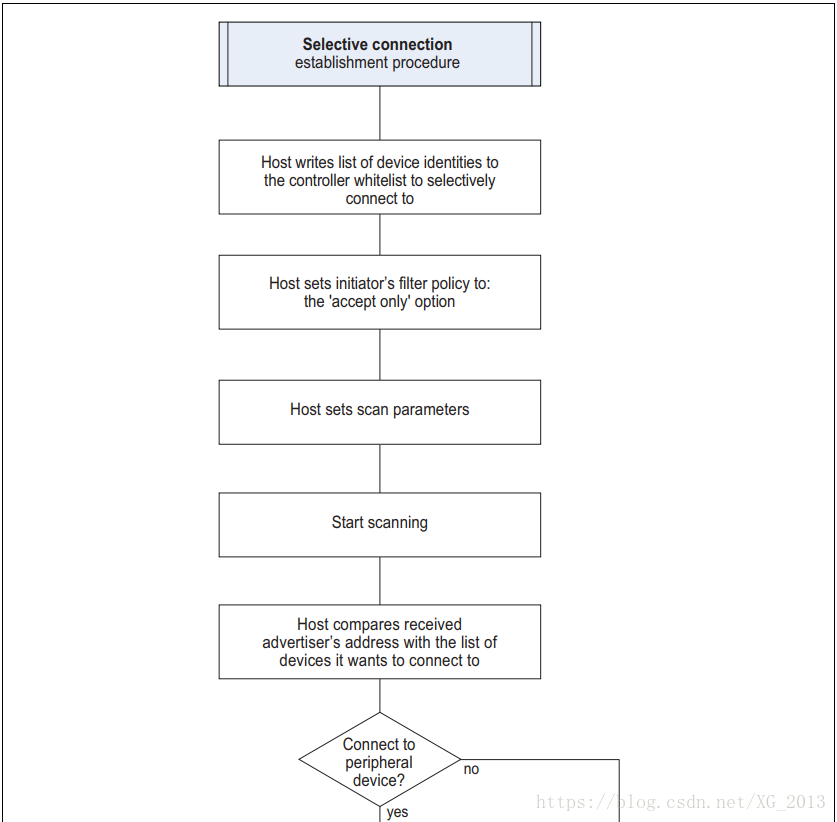
这个过程是central设备支持的，先添加白名单，设置scannig的策略可以所用设备进行扫描，获取扫描的结果，比对扫描的地址选择一个进行直接连接.

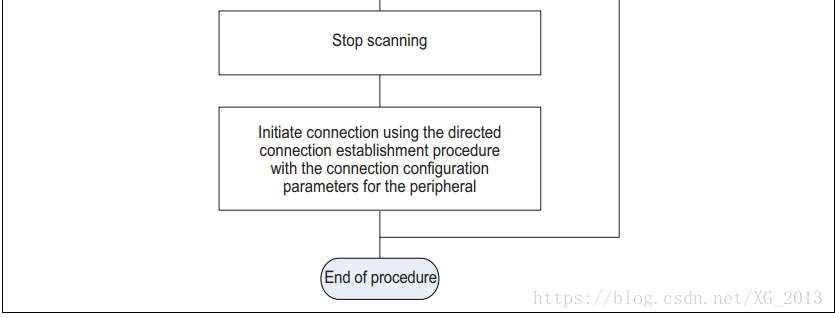




### 6.6 selective connection establishment procedure

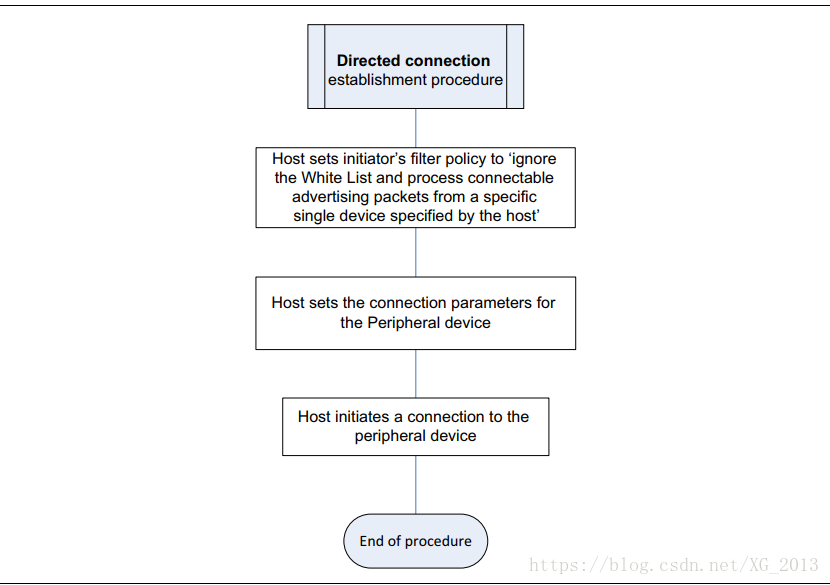
这个过程是central设备支持的，先添加白名单，设置scannig的策略只能对白名单设备进行扫描，获取扫描的结果，比对扫描的地址选择一个进行直接连接。





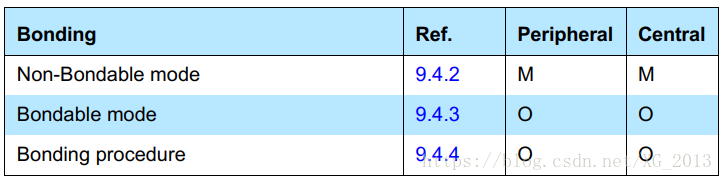
### 6.7 direct connection establishment procedure

这个也只有central设备支持，忽略白名单的策略，直接连接对方设备。



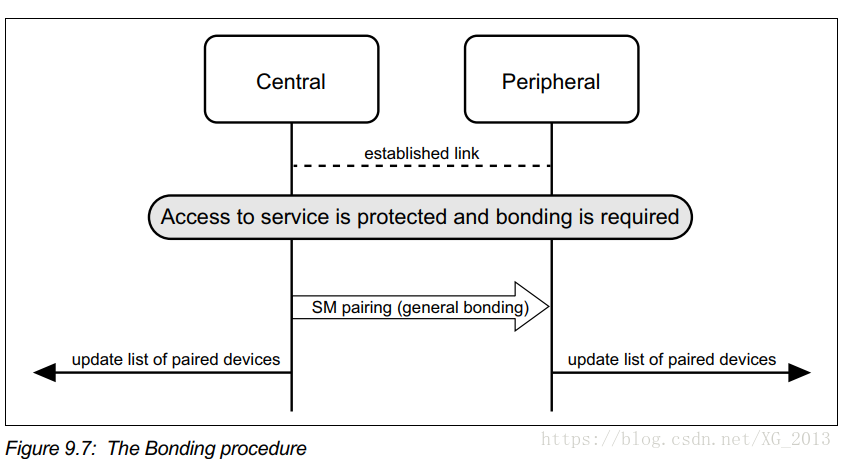
## 七、bonding 模式与过程

bonding 允许2个连接的设备创建和储存安全个识别的信息，安全和识别的信息叫做bonding information. bonding information，其实就是一大堆key.



### 7.1 bonding procedure

简单讲就是配对的交换feature的时候，双方使能bonding enable。下一次配对的时候，master会检查从机在不在bonding在绑定的list中，如果在，双方使用上一次的bonding information 进行加密通信。



# 相关问题

## BLE调试宝为什么不能搜索手机蓝牙？

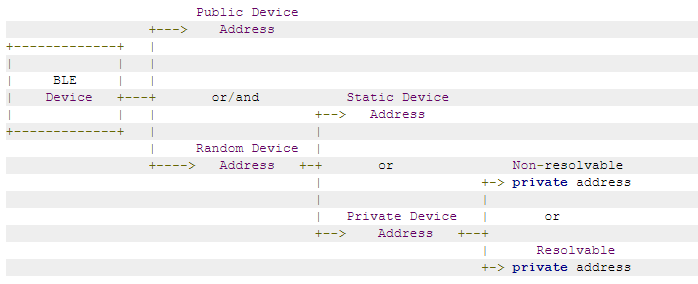
① 手机蓝牙是BT4.0之前的传统的蓝牙，二者的扫描机制、封包内容都不一样。比如传统蓝牙是广播自己的inquiry封包，对端如果收到了，就会响应，而ble是手机端去接收来自外设的广播包。

② 手机是作为Master角色，是主动连接。

## 为什么BLE设备被连接后，就收不到广播包了？

蓝牙技术联盟规定，BLE一旦被连接后，就会被掩藏。也自然就收不到蓝牙广播包了。

## MAC 地址分类



### Public Device Address

在BLE时代中，Public Device Address有什么不足？

（1）Public Device Address需要向IEEE购买。虽然不贵，但在BLE时代，相比BLE IC的成本，还是不小的一笔开销。

（2）Public Device Address的申请与管理是相当繁琐、复杂的一件事情，再加上BLE设备的数量众多（和传统蓝牙设备不是一个数量级的），导致维护成本增大。

（3）安全因素，BLE很大一部分的应用场景是广播通信，这意味着只要知道设备的地址，就可以获取所有的信息，这是不安全的。因此固定的设备地址，加大了信息泄漏的风险。

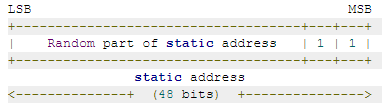
为了解决上述问题，BLE协议新增了一种地址：Random Device Address，即设备地址不是固定分配的，而是在设备启动后随机生成的。

### 3.2 Random Device Address

#### Static Device Address

Static Device Address是设备在上电时随机生成的地址。

地址格式如下：



特征可总结为：

（1）最高两个bit为“11”。

（2）剩余的46bits是一个随机数，不能全部为0，也不能全部为1。

（3）在一个上电周期内保持不变。

（4）下一次上电的时候可以改变。但不是强制的，因此也可以保持不变。如果改变，上次保存的连接等信息，将不再有效。

使用场景：

（1）46bits的随机数，可以很好地解决“设备地址唯一性”的问题，因为两个地址相同的概率很小。

（2）地址随机生成，可以解决Public Device Address申请所带来的费用和维护问题。

#### Private Device Address

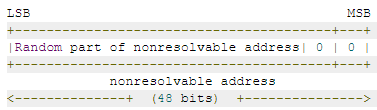
Static Device Address通过地址随机生成的方式，解决了部分问题，Private Device Address则更进一步，通过定时更新和地址加密两种方法，提高蓝牙地址的可靠性和安全性。根据地址是否加密，Private Device Address又分为两类，Non-resolvable private address和Resolvable private address

##### Non-resolvable private address

与Static Device Address的不同之处

Non-resolvable private address和Static Device Address类似，不同之处在于，Non-resolvable private address会定时更新。更新的周期称是由GAP规定的，称作T\_GAP(private\_addr\_int) ，建议值是15分钟。

地址格式如下：



特征总结如下：

（1）最高两个bit为“00”。

（2）剩余的46bits是一个随机数，不能全部为0，也不能全部为1。

（3）以T\_GAP(private\_addr\_int)为周期，定时更新。

注意：

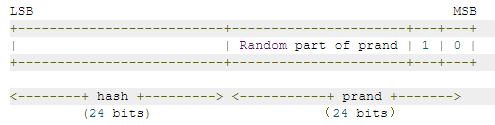
Non-resolvable private address有点奇怪，其应用场景并不是很清晰。地址变来变去的，确实是迷惑了敌人，但自己人不也一样被迷惑了吗？因此，实际产品中，该地址类型并不常用。

##### Resolvable private address

定义如下：

Resolvable private address比较有用，它通过一个随机数和一个称作identity resolving key (IRK) 的密码生成，因此只能被拥有相同IRK的设备扫描到，可以防止被未知设备扫描和追踪。其格式如下：

地址格式如下：



特征总结如下：

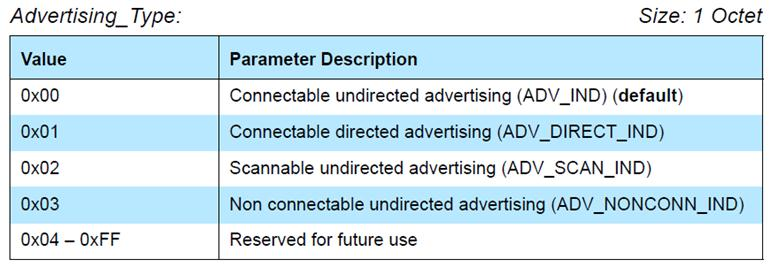
（1）由两部分组成：  
     高位24bits是随机数部分，其中最高两个bit为“10”，用于标识地址类型；低位24bits是随机数和IRK经过hash运算得到的hash值，运算的公式为hash = ah(IRK, prand)。

（2）当对端BLE设备扫描到该类型的蓝牙地址后，会使用保存在本机的IRK，和该地址中的prand，进行同样的hash运算，并将运算结果和地址中的hash字段比较，相同的时候，才进行后续的操作。这个过程称作resolve（解析），这也是Non-resolvable private address/Resolvable private address命名的由来。

（3）以T\_GAP(private\_addr\_int)为周期，定时更新。哪怕在广播、扫描、已连接等过程中，也可能改变。

（4）Resolvable private address不能单独使用，因此需要使用该类型的地址的话，设备要同时具备Public Device Address或者Static Device Address中的一种。

## 4. 广播的类型



### 4.1 可连接的非定向广播

这是一种用途最广的广播类型，包括广播数据和扫描响应数据，它表示当前设备可以接受其他任何设备的连接请求。进行通用广播的设备能够被扫描设备扫描到，或者在接收到连接请求时作为从设备进入一个连接。通用广播可以在没有连接的情况下发出，换句话说，没有主从设备之分。

### ****4.2 可连接的定向广播****

定向广播类型是为了尽可能快的建立连接。这种报文包含两个地址：广播者的地址和发起者的地址。发起者收到发给自己的定向广播报文之后，可以立即发送连接请求作为回应。

定向广播类型有特殊的时序要求。完整的广播事件必须每3.75ms重复一次。这一要求使得扫描设备只需扫描3.75ms便可以收到定向广播设备的消息。

当然，如此快的发送会让报文充斥着广播信道，进而导致该区域内的其他设备无法进行广播。因此，定向广播不可以持续1.28s以上的时间。如果主机没有主动要求停止，或者连接没有建立，控制器都会自动停止广播。一旦到了1.28s，主机便只能使用间隔长得多的可连接非定向广播让其他设备来连接。

当使用定向广播时，设备不能被主动扫描。此外，定向广播报文的净荷中也不能带有其他附加数据。该净荷只能包含两个必须的地址。

### 4.3 不可连接的非定向广播

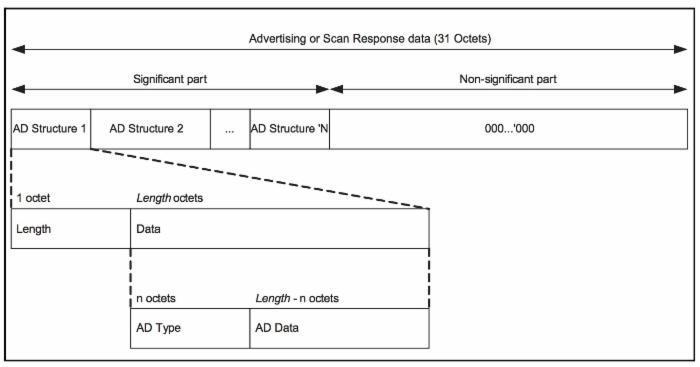
仅仅发送广播数据，而不想被扫描或者连接。这也是唯一可用于只有发射机而没有接收机设备的广播类型。不可连接广播设备不会进入连接态，因此，它只能根据主机的要求在广播态和就绪态之间切换。

### 4.4 可扫描的非定向广播

又称可发现广播，这种广播不能用于发起连接，但允许其他设备扫描该广播设备。这意味着该设备可以被发现，既可以发送广播数据，也可以响应扫描发送扫描回应数据，但不能建立连接。这是一种适用于广播数据的广播形式，动态数据可以包含于广播数据之中，而静态数据可以包含于扫描响应数据之中。

注意：① 所谓的定向和非定向针对的是广播的对象，如果是针对特定的对象进行广播（在广播包PDU中会包含目标对象的MAC）就是定向广播，反之就是非定向。② 可连接和不可连接是指是否接受连接请求，如果是不可连接的广播类型，它将不回应连接请求。③ 可扫描广播类型是指回应扫描请求。

### 4.5 广播数据包格式



每个包都是 31 字节，数据包中分为有效数据（significant）和无效数据（non-significant）两部分。

有效数据部分：包含若干个广播数据单元，称为 AD Structure 。如图所示，AD Structure 的组成是：长度 Len ，表示这个 AD Structure 的长度（除去 len本身 1）；类型ADType，标记这段广播数据代表什么，如设备名，uuid 等；数据 AD data。

无效数据部分：广播包的长度必须是 31 个 byte，如果有效数据部分不到 31 自己，剩下的就用 0 补全。这部分的数据是无效的。

## 5. discovery 类型

见GAP层