**BLE知识总结**

**一、蓝牙低功耗协议栈基础知识**

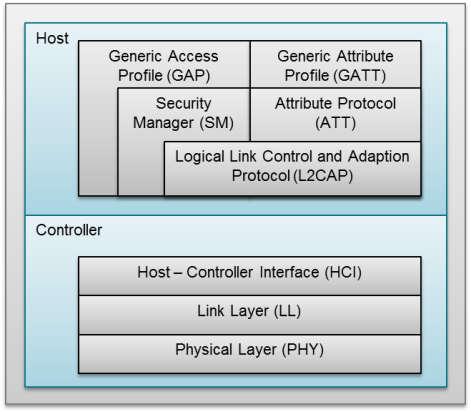


图1. 蓝牙低功耗协议栈

1. 蓝牙低功耗协议栈（或协议栈）由控制器和主机组成。任何配置文件和应用程序都位于协议堆栈的GAP和GATT层之上。
2. 物理层（PHY）是在未经许可的2.4-GHz ISM（工业，科学和医疗）频段中操作的1-Mbps自适应跳频GFSK（高斯频移键控）无线电。
3. 通用访问配置文件(GAP)控制设备的RF状态，设备处于以下五种状态之一:

.Standby ----> 空闲状态

.Advertising ----> 广播状态

.Scanning ----> 扫描状态

.Initiating ----> (主机)发起连接请求，等待连接的状态(建立链路的过程) ---> 主机才拥有此状态

.Connected ----> 连接状态

1. 广播的设备在没有连接的情况下传输数据，而扫描的设备则扫描广播。启动器( initiator)是响应具有连接请求的广播的设备。 如果广播的设备接受连接请求，则广告设备和扫描设备都进入连接状态。连接设备时，它将作为主设备或从设备连接。启动连接的设备成为主设备，接受请求的设备成为从设备。
2. HCI层通过标准化接口提供主机和控制器之间的通信。该层可以通过软件API或硬件接口(如UART，SPI或USB)实现。
3. 通用访问概要文件(GAP)层直接与应用程序和/或概要文件进行接口，以处理设备的设备发现和与连接相关的服务。GAP处理安全特性的初始化。
4. ATT层允许设备向另一个设备公开某些数据或属性。
5. 通用属性概要(GATT)层是一个服务框架，它定义了使用ATT的子过程。BLE连接中两个设备之间发生的数据通信通过GATT子程序处理。应用程序和/或配置文件将直接使用GATT。
6. **通用访问配置文件（GAP）**
7. BLE协议栈的GAP层负责连接功能。这一层处理设备的访问模式和过程，包括设备发现、链路建立、链路终止、安全特性启动和设备配置。

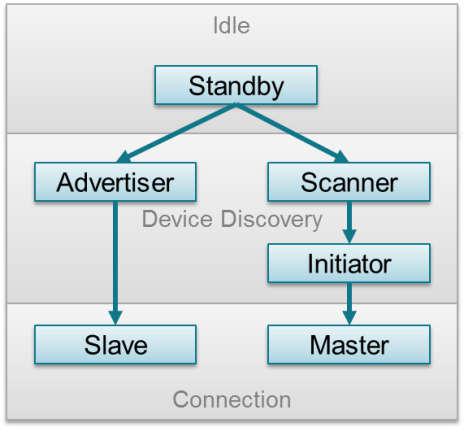


图2. GAP状态图

Standby(待机/空闲)：设备在复位时处于初始空闲状态。

Advertiser(广播设备)：该设备使用特定的数据进行广告，让任何初始化设备知道它是一个可连接的设备（此广告包含设备地址，并且可以包含一些其他数据，例如设备名称）。

Scanner(扫描设备)：当接收广播时，扫描设备向广告设备发送扫描请求。广播设备以扫描响应进行响应。此过程称为设备发现(device discovery)。扫描设备知道广播设备并且可以发起与其的连接。

Initiator(启动器)：启动时，启动器必须指定要连接的对等设备地址。如果接收到与对等设备的地址匹配的广播，则发起设备发出请求，使用连接参数中描述的连接参数与广播设备建立连接(链接)

从机(Slave)/主机(Master)：当形成连接时，广播设备充当从设备；发起连接设备，则充当主设备。

1. 连接参数

**连接间隔(Connection Interval )** - 在BLE连接中，使用跳频方案。这两个设备各自仅在特定时间在特定信道上相互发送和接收数据。集中点(峰值)是两个设备发送和接收数据的地方，称为连接事件。如果没有要发送或接收的应用数据，则两个设备交换链路层数据以维持连接。 **连接间隔**是两个连接事件之间的时间量，以1.25 ms为单位。 连接间隔的范围可以从最小值6（7.5 ms）到最大值3200（4.0 s）。

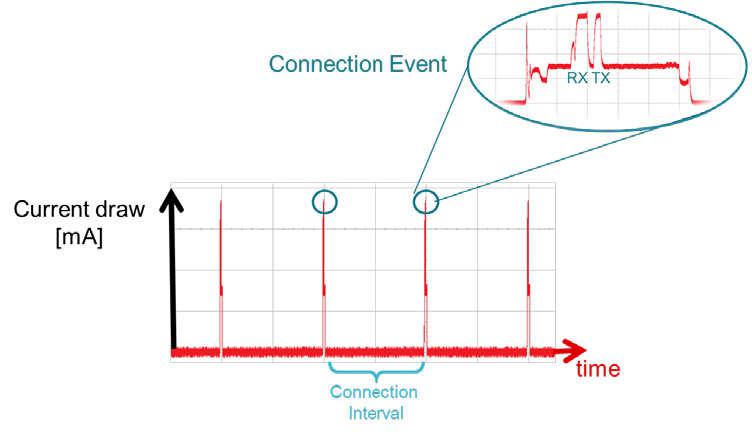
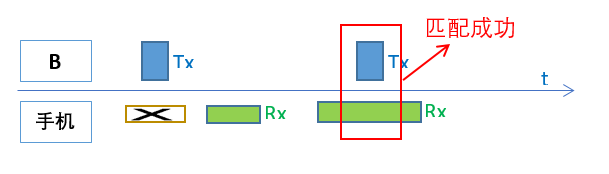


图3. 连接事件和间隔

设备B不断发送广播信号给手机（Observer），如果手机不开启扫描窗口，手机是收不到设备B的广播的，如下图所示，不仅手机要开启射频接收窗口，而且只有手机的射频接收窗口跟广播发送的发射窗口匹配成功，手机才能收到设备B的广播信号。由于这种匹配成功是一个概率事件，因此手机扫到设备B也是一个概率事件，也就是说，手机有时会很快扫到设备B，比如只需要一个广播事件，手机有时又会很慢才能扫到设备B，比如需要10个广播事件甚至更多。



**从机延时(Slave Latency)** - 此参数为从属（外围设备）设备提供跳过多个连接事件的选项。这种能力为外围设备提供了一些灵活性。如果外围设备没有任何数据要发送，它可以跳过连接事件，保持睡眠状态并节省电量。外围设备根据每个连接事件选择是否唤醒。外围设备可以跳过连接事件，但必须跳过从服务器延迟参数允许的范围，否则连接将失败。

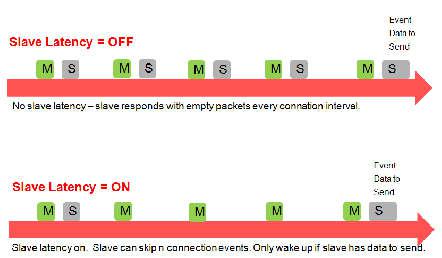


图4. 从机延迟

**监控超时(Supervision Time-out)** - 此超时是两次成功连接事件之间的最长时间。如果此时间没有成功连接事件，则设备终止连接并返回到未连接状态。该参数值以10毫秒为单位表示。监督超时值的范围可以从最小10（100 ms）到3200（32.0 s）。超时必须大于有效连接间隔。

(3)有效连接间隔

有效连接间隔等于两个连接事件之间的时间量，假设从机在允许从机延迟时跳过最大可能事件数（如果从连接延迟设置为0，则有效连接间隔等于实际连接间隔）。

从机延迟值表示可以跳过的最大事件数。此数字的范围可以从最小值0（表示不能跳过任何连接事件）到最大值499.最大值不能使有效连接间隔（参见下面的公式）大于16秒。可以使用以下公式计算有效连接间隔：

**Effective Connection Interval = (Connection Interval) \* (1 + [Slave Latency])**

**例子如下：**

Connection Interval: 80 (100 ms)

Slave Latency: 4

Effective Connection Interval: (100 ms) \* (1 + 4) = 500 ms

**当没有数据从从设备发送到主设备时，从设备在连接事件期间每500毫秒发送一次。**

(4)连接参数注意事项

**减少连接间隔的步骤如下**：

.增加两个设备的功耗

.增加两个方向的吞吐量

.减少向任一方向发送数据的时间

**增加连接间隔的步骤如下**：

.降低两种设备的功耗

.降低双向吞吐量

.增加向任一方向发送数据的时间

**减少从属延迟（或将其设置为零）**：

.增加外围设备的功耗

.减少外围设备接收从中央设备发送的数据的时间

**增加从属延迟如下**：

.在外围设备没有数据发送到中央设备期间，降低外设的功耗

.增加外围设备接收从中央设备发送的数据的时间

(5)连接参数更新

在某些情况下，中心设备在请求与外围设备建立连接时，会请求一些不利于外围设备的连接参数。外围设备可能希望根据外围应用程序在连接中间更改参数。外围设备可以通过发送连接参数更新请求(Connection Parameter Update Request)来请求中心设备改变连接设置。对于支持蓝牙4.1和4.2的设备，此请求由链路层直接处理。对于蓝牙4.0设备，协议栈的L2CAP层处理请求。BLE堆栈会自动选择更新方法。

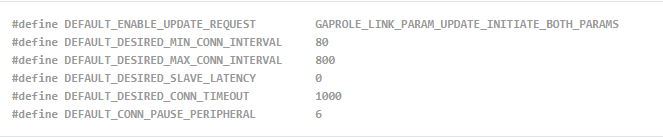
此请求包含四个参数：最小连接间隔，最大连接间隔，从机延迟和超时(minimum connection interval, maximum connection interval, slave latency, and time-out)。这些值表示外围设备连接所需的参数（连接间隔以范围给出）。当中心设备接收到该请求时，它可以接受或拒绝新参数。

发送连接参数更新请求(Connection Parameter Update Request)是可选的，中心设备不需要接受或应用请求的参数。某些应用程序尝试以更快的连接间隔建立连接，以便更快地进行服务发现和初始设置。这些应用程序稍后请求更长（更慢）的连接间隔以允许最佳功率使用。

根据具体情况GAPRole，连接参数更新可以与GAPRole\_SendUpdateParam（）或 GAPCentralRole\_UpdateLink（）命令异步发送。外设GAPRole可以配置为在建立连接后自动发送参数更新一定时间。

假设DEFAULT\_CONN\_PAUSE\_PERIPHERAL的值设置为X，那么在建立连接后的X秒后，从设备会向主机发出连接参数更新请求。

simple\_peripheral应用程序使用以下预处理器定义的符号：



建立连接六秒后，GAP层自动发送连接参数更新。可以通过更改DEFAULT\_ENABLE\_UPDATE\_REQUEST的值禁用此操作GAPROLE\_LINK\_PARAM\_UPDATE\_WAIT\_REMOTE\_PARAMS。

(6)连接终止

主服务器或从服务器可以出于任何原因终止连接。一方启动终止，另一方必须在两个设备退出连接状态之前响应。

(7)GAP的抽象概念

应用程序和配置文件可以直接调用GAP API函数来执行与BLE相关的功能，例如广播或连接。大多数GAP功能由GAPRole任务处理。GAP抽象概念显示了这种抽象层次结构。

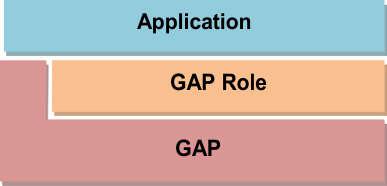


图5. GAP抽象概念

通过直接调用或GAPRole任务访问GAP层，如GAPRole任务中所述。尽可能使用GAPRole任务，而不是直接调用。

(8)配置GAP层

GAP层功能主要在库代码中定义。函数头可以gap.h在协议栈项目中找到。大多数这些函数都由GAPRole使用，不需要直接调用。

有几个参数可能需要在启动GAPRole之前修改。可以通过GAP\_SetParamValue()和GAP\_GetParamValue()函数设置或获取这些参数，包括广播间隔和扫描间隔、窗口等等。

1. **GAPRole 任务**

(1)GAPRole任务是一个独立的任务，它从应用程序中卸载了处理大部分GAP层功能的任务，也就是说大部分GAP层功能的任务都由GAPRole任务去执行，大都从应用程序中剥离出来。

应用程序在初始化期间启用和配置此任务。基于这种配置，许多BLE协议栈事件都由GAPRole任务直接处理，并且从未传递给应用程序。存在回调，应用程序可以向GAPRole任务注册，这样应用程序任务就可以得到某些事件的通知并相应地进行。

(2)根据设备的配置，GAP层始终以**四种角色**之一运行：

.广播设备 - 该设备是**不可连接**的广告客户。

.扫描设备 - 设备**扫描广播**但**无法发起连接**。

.外围设备 - 设备是**可连接**的广播设备，在单个链路层连接中作为**从设备**运行。

.中心设备 - 设备**扫描广播并发起连接**，并在单个或多个链路层连接中作为主设备运行。BLE中心设备协议栈最多支持三个同时连接。

蓝牙核心规范4.2版允许多种角色的特定组合，这些角色由BLE协议栈支持。

(3)中心设备

可以使用GAPCENTRAL\_MAX\_SCAN\_RES参数设置一次扫描期间可以发现的最大扫描响应量。在充满广告/扫描响应的环境中，这会对堆使用产生巨大影响，从而可能破坏堆栈。

在最糟糕的情况下，在扫描期间找到最大数量的广告/扫描响应（n），所有这些都具有最大数据大小，其中应用程序一直在处理，使得它不处理任何堆栈的消息，堆可以增长：（8 + 87 \* n字节）。例如，如果 GAPCENTRALROLE\_MAX\_SCAN\_RES设置为10，则必须至少有878个字节可用于从堆中分配。这包括完全填充的GAP\_DEVICE\_DISCOVERY\_EVENT。如果此分配失败，则为GAP\_DEVICE\_DISCOVERY\_EVENT将尝试分配错误状态而不是8字节。因此，为了使系统在上述场景中继续运行，堆必须具有至少分配空间（8 + 79 \* n字节）。

(4)建立连接

用于建立连接的API是针对中心角色的gapcentralrole\_established link()或针对多角色的gaprole\_established link()。这两个api都只是填写适当的结构并调用gap\_ishlinkreq()。

存在这样的情况：可以在一般扫描期间（即通过发现GAP\_DEVICE\_INFO\_EVENT）检测广告设备，但是在连接启动扫描期间可以不检测广告设备。（例如，用户走开，或电池死亡）。出于这个原因，可能需要为应用程序中的启动创建超时。链接层中的初始连接任务可以通过以下方式停止：GAPCentralRole\_TerminateLink（）或 GAPRole\_TerminateConnection（），并将连接句柄设置为 GAP\_CONNHANDLE\_INIT。

四、通用属性配置文件（GATT）

(1)正如GAP层处理大多数与连接相关的功能一样，BLE协议栈的GATT层被应用程序用于两个连接设备之间的数据通信。数据以特征的形式传递和存储，特征存储在BLE设备的内存中。从GATT的观点来看，当两个设备连接在一起时，它们分别扮演两种角色中的一种:

GATT服务端：包含由GATT客户端读取或写入的特征数据库的设备。

GATT客户端: 从GATT服务器读取数据或向GATT服务器写入数据的设备。

图6.显示了BLE连接示例中的这种关系，其中外围设备（即 CC2640R2F LaunchPad）是GATT服务器(Server)，中心设备（即智能手机）是GATT客户端(Client)。

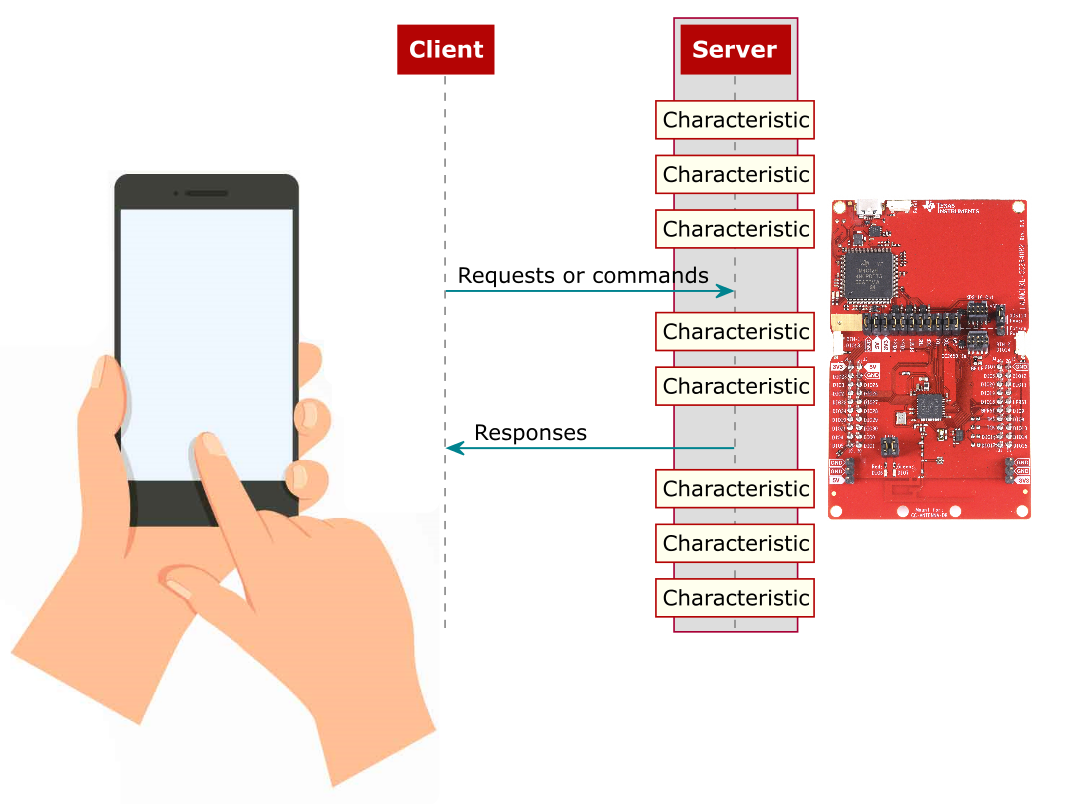


图6. GATT客户端和服务器交互概述

客户端和服务器的GATT角色独立于外围设备和中央设备的GAP角色。外围设备可以是GATT客户端或GATT服务器，中心设备可以是GATT客户端或GATT服务器。外围设备可以充当GATT客户端和GATT服务器。

(2)GATT的特征和属性(GATT Characteristics and Attributes)

虽然特性和属性有时在提到蓝牙低能耗时可以互换使用，但是可以将特性看作一组称为属性的信息。属性是设备之间实际传输的信息。特征组织并使用属性作为数据值、属性和配置信息。

.特征值(Characteristic Value)

特征值的数据

.特征声明(Characteristic Declaration)

存储特征值的属性、位置和类型的描述符

.客户端特征配置(Client Characteristic Configuration)

允许GATT服务器配置要通知的特性(异步发送消息)或指示的特性(通过确认异步发送消息)的配置

.特征用户描述(Characteristic User Description)

描述特征的ASCII字符串

.句柄(Handle)

表中属性的索引(每个属性都有一个惟一的句柄)。

.类型(Type)

指示属性数据表示什么(称为UUID[通用惟一标识符])。其中一些蓝牙SIG定义的，一些是自定义的。)

.权限(Permissions)

执行GATT客户机设备是否可以访问属性值以及如何访问属性值

(3)GATT客户端抽象概念

GATT客户端没有属性表或配置文件，因为它们正在收集信息，而不是提供信息。大多数与GATT层的接口直接来自应用程序。

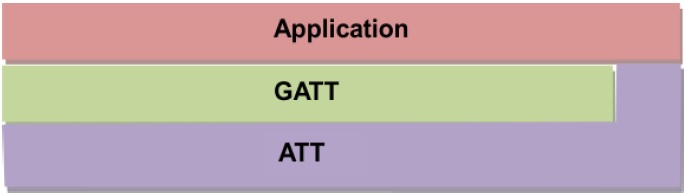


图7. GATT客户端抽象的可视化

(4)GATT服务器抽象

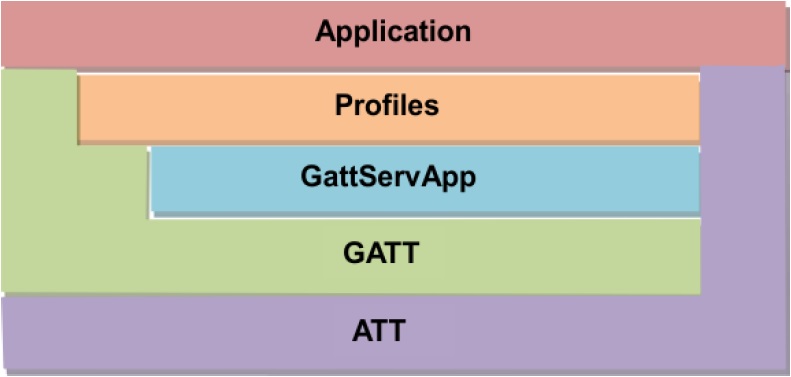


图8. GATT Server抽象的可视化

(5)GATT服务及简介(GATT Services and Profile)

GATT服务是一个特征的集合。可以将多个服务组合在一起形成一个Profile。许多Profile只实现一个服务，因此这两个术语有时可以互换使用。

(1)simple\_gatt\_profile包含以下特征：

.SIMPLEPROFILE\_CHAR1

可以从GATT客户端设备读取或写入的1字节值

.SIMPLEPROFILE\_CHAR2

1字节值，可从GATT客户端设备读取但无法写入

.SIMPLEPROFILE\_CHAR3

1字节值，可以从GATT客户端设备写入但无法读取

.SIMPLEPROFILE\_CHAR4

无法直接从GATT客户端设备读取或写入的1字节值（此值可通知：此值可配置为将通知发送到GATT客户端设备。）

.SIMPLEPROFILE\_CHAR5

可从GATT客户端设备读取（但不写入）的5字节值

