

# 解密蓝牙mesh系列 | 第七篇

2017-10-19 小码哥 蓝牙技术联盟

## 蓝牙mesh网络

### 市场上的低功耗蓝牙设备



#### 低功耗蓝牙

低功耗蓝牙（Bluetooth Low Energy）是一项相当成功的无线技术。如今已经很难找到不支持低功耗蓝牙的智能手机或平板电脑了。可以说它是可穿戴技术兴起的关键因素。**在医疗设备、智能家居设备、传感器等很多设备中，低功耗蓝牙的身影随处可见。**

目前有数十亿支持低功耗蓝牙的设备已投入使用。那么，**这些设备都能成为蓝牙mesh网络的一员吗？**这也是本文将会回答的问题。知道你已经迫不及待，早想对着电脑屏幕、平板电脑或手机大喊“天呐，快告诉我吧！”，我就不卖关子啦：

**答案就是YES。**

**低功耗蓝牙设备只要具有正确的低功耗蓝牙功能和一些附加软件，就能加入蓝牙mesh网络中。**以智能手机为例，可能只需要一个可以与蓝牙mesh网络对话的普通应用程序（App）就足够了。换句话说，这是任何开发者都能编写的应用程序。

未来充满无限可能性，现在就让我们一探究竟吧！

## 承载层 ( bearer layer )

要了解非mesh低功耗蓝牙设备如何成为蓝牙mesh网络的一员，我们需要回顾一下蓝牙mesh协议栈（见《解密蓝牙mesh系列 第二篇》）。



图 1 – 蓝牙mesh协议栈

**蓝牙mesh网络采用低功耗蓝牙作为其射频通信协议栈。**而具体如何使用，则是蓝牙mesh网络协议栈最底层的承载层需要负责的工作。

目前定义了两个承载层：**广播承载层 (advertising bearer)**和**GATT承载层 (GATT bearer)**。蓝牙mesh网络设备默认使用的是广播承载层，它负责在低功耗蓝牙广播数据包内收发蓝牙mesh数据包。

具有低功耗蓝牙协议栈、能够进行广播和扫描的设备具有基本的、必备的低功耗特性，因此能够支持广播承载层、乃至完整的蓝牙mesh网络协议栈。

**既不支持也无法升级使用广播承载层的设备，则必须使用GATT承载层。**使用GATT承载层时需要将蓝牙mesh协议数据单元（PDU）封装在代理协议（Proxy Protocol）中，我们将在下文中对此进行详细介绍。

## 节点与特性

**成为蓝牙mesh网络中一员的设备被称为节点(Node)。**很多种产品类型都能够成为节点：照明灯、灯具开关、温控器、窗锁、占用传感器等。然而，无论产品类型如何，节点都可能提供某些超出其产品本身功能的特定蓝牙mesh网络服务。

蓝牙mesh规格定义了**节点可能拥有的特性**。具有这些特性中的一个或多个，即表示节点可以在网络中扮演相应的特殊角色。定义的特性包括：

中继 ( Relay )	中继节点可通过广播承载层，接收并重新发送蓝牙mesh消息。中继特性能让蓝牙mesh消息在设备之间实现多次跳跃，传送距离可超过两台设备之间直接进行无线电传输的范围，从而覆盖整个网络。
好友(Friend)	好友节点能够存储发往相关低功耗节点的消息，随后再进行转发。
低功耗节点 (LPN)	低功耗节点功率受限，可借助好友节点的支持，在蓝牙mesh网络中有效地运作，借此大幅降低空占比。
代理(Proxy)	代理节点可通过承载层（广播承载层或GATT承载层）接受信息，并通过另一个广播承载层或GATT承载层重新发送消息。

### 代理节点 ( Proxy Node )

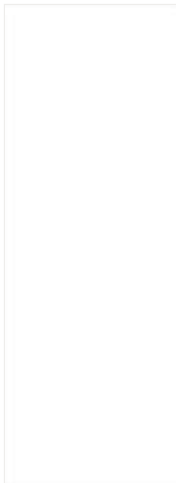


图 2 – 代理节点

非mesh低功耗蓝牙设备成为蓝牙mesh网络成员的过程中，代理节点是关键。**代理节点的根本目的是执行承载层转换。它能够实现从广播承载层到GATT承载层的转换，反之亦然。**因此，不支持广播承载层的设备可通过GATT连接来收发各类蓝牙mesh消息。

节点可通过在特性字段中设置代理特性位（ proxy feature bit ），来表示自身可用作代理节点。特性字段是所有节点都具有的成分数据状态的一部分。

### 蓝牙mesh代理服务

代理节点(Proxy Node)可实施称为mesh代理服务的GATT服务，即本文中的“代理服务器(Proxy Server)”。**mesh代理服务包含两个GATT特性：**

**mesh代理数据输入和mesh代理数据输出。**代理客户端(Proxy Client) 使用 “GATT Write Without Response” 子程序，将代理协议（见下图）PDU 写入mesh代理数据输入特性，并从GATT通知中的mesh代理数据输出特性接收代理协议PDU。这就是互联GATT设备通过代理节点在蓝牙mesh网络中进行数据交换的机制。

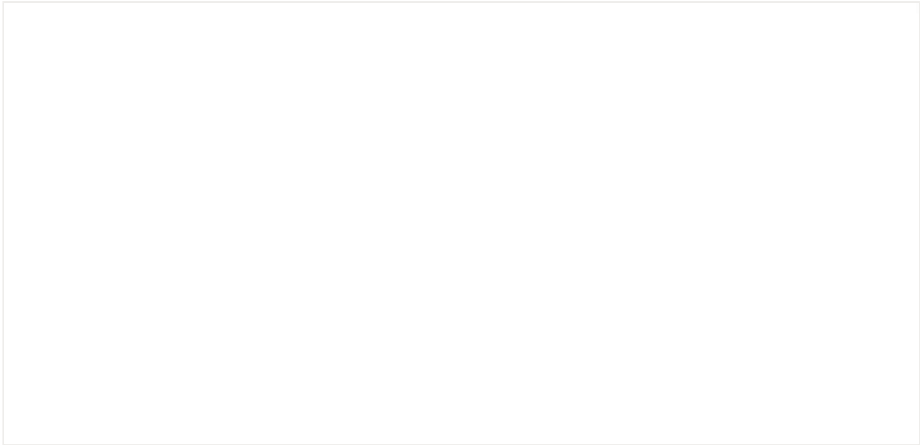


图 3 – 代理服务器与代理客户端

**发现代理节点**

低功耗蓝牙设备使用GAP广播来帮助其他设备发现自己。蓝牙mesh代理节点使用完全相同的技术，即通过 “GAP 可连接型广播（connectable advertising）数据包”，对自身的可用性、可作为代理节点的角色、及其身份进行广播。

**GAP广播数据包中包含各类字段，称为广播类型（AD Type）。**核心规格附录中对广播类型进行了定义。代理节点会在广播数据包中包含以下字段：

广播类型	注释
标识	表示通用可被发现模式（General Discoverable Mode）
完整的16位服务UUID列表 或 不完整的16位服务UUID列表	包括mesh代理服务的UUID
服务数据	包含与mesh代理服务相关的数据，可识别该代理是在为哪个网络或节点所提供服务

表 1 – mesh代理广播

服务数据广播类型的内容还需经过进一步检查。

服务数据字段	注释
识别类型	此字段中的值能够正确解释“识别参数”字段的内容。  0x00：网络ID（Network ID）类型 0x01：节点标识（Node Identity）类型
识别参数	可以是网络ID或节点标识，具体取决于识别类型

**网络ID是从网络密钥（NetKey – 参照《解密蓝牙mesh系列 | 第六篇》）派生而来的唯一公共标识符。**节点标识由代理服务器节点的单播地址和网络标识符的组合派生而来，例如启用该标识的子网的网络ID。

如果代理服务器是多个子网的成员，则它将对包含每个子网的网络ID广播数据包进行交替操作，每次处理一个广播数据包。

**节点标识广播的主要用途是将启动配置设备（Provisioner）快速连接至刚刚完成启动配置的节点，从而完成新节点的配置。**

## 代理协议

**代理客户端和代理服务器使用代理协议进行通信，并向对方发送代理PDU。**这些PDU就像是存放各类蓝牙mesh PDU的容器。

蓝牙mesh接入消息使用核心蓝牙mesh协议栈，因此消息包含在网络PDU内。网络PDU可被封装在代理PDU中。

蓝牙mesh配置文件规格中定义了各种Beacon，包括未经启动配置的设备Beacon、以及安全网络Beacon。可通过代理协议将蓝牙mesh Beacon纳入网络。

**启动配置过程涉及其自身协议，且启动配置PDU也可在代理PDU内进行交换。**

最后，代理客户端和代理服务器可以交换特殊的代理配置消息，这些消息也可被封装于代理PDU中。

大多数类型的mesh数据可使用代理协议进行交换，因此可通过连接至代理节点的GATT客户端进行收发。

不同设备代理PDU的大小各异，PDU的大小是根据低功耗蓝牙属性协议（ATT）的最大传输单元（MTU）进行动态设置的，这是通过GATT连接来传输代理PDU的基础。此外，代理协议可以将完整的蓝牙mesh消息封装在代理PDU或多段消息的各个段中，借此来容纳较长的蓝牙mesh消息。

需要注意的一点是，**任何蓝牙mesh节点（而非只有代理节点）都可以实施代理协议，从而支持基于GATT连接的直接交互。**这在启动配置（provisioning）场景中非常有用。

关于代理协议的更多信息，包括代理PDU的格式，可参考蓝牙mesh配置文件规格: <https://www.bluetooth.com/specifications/mesh-specifications>。

## 代理过滤器和代理配置

---

代理客户端可通过对代理服务器所应用的过滤器进行配置，对接收到的网络流量进行精确的控制。**过滤器采用白名单和黑名单的形式，同时这些名单会指定各自的目标地址列表。**列表中的地址可能是其所支持的地址类型的任意组合，即单播、群组或虚拟地址。如果消息的目标地址未包含在白名单过滤器中，则消息会被代理服务器的代理过滤器（Proxy Filter）滤掉。同样，如果消息的目的地址包含在黑名单过滤器中，也会被滤过。

代理配置（Proxy Configuration）消息在代理客户端和代理服务器之间进行交换，并实现代理过滤器的配置。

## 使用低功耗蓝牙智能手机或平板电脑启动配置

---

**通常使用智能手机或平板电脑执行启动配置流程，以将新设备添加至蓝牙mesh网络。**大多数此类设备不会实施完整的蓝牙mesh网络协议栈，而且与蓝牙mesh网络进行的所有交互（包括启动配置）都很可能会使用代理协议。如前所述，启动配置PDU可被封装于代理PDU中，因此可通过代理服务器节点、利用GATT连接进行交换。蓝牙mesh配置文件规格中将采用代理协议的启动配置协议称为PB-GATT。

在上期《解密蓝牙mesh系列 | 第六篇》中介绍了启动配置流程，本系列后续文章中将进一步深挖有关启动配置安全性的细节问题。

## 借助代理节点使用代理协议时需要注意什么？

---

**智能手机等设备要想通过代理节点、借助代理协议与蓝牙mesh网络通信，则必须扫描并连接至代理节点。**换句话说，它必须支持GAP中央设备的角色。

此外，**必须首先对智能手机进行启动配置。**如果未经启动配置，任何设备都无法与蓝牙mesh网络中的节点进行交互。

## 结论

---

通过GATT、代理协议和蓝牙mesh代理节点对当前市场上的低功耗蓝牙设备提供支持，这绝对值得上新闻头条了！它为人们手中已有的海量设备打开了通往蓝牙mesh网络世界的大门，光是想想就觉得令人兴奋了呢！你也有同感吗？留言告诉我吧~

蓝牙技术联盟EMEA技术项目经理

Martin Woolley

小码哥

点击“[阅读原文](#)”，下载超全[mesh技术概览](#)！

[阅读原文](#) 阅读 753 8

[投诉](#)

### 精选留言

[写留言](#)



伍小勇

你好博主，android上面有接入mesh的example了吗

谢谢

2017年12月19日



城东

你好，请问怎么看本系列文章的目录

2017年12月4日

作者回复

可以在后台回复关键词: mesh

2017年12月11日



阿飞

小马哥，请问能详细描述下“节点标识广播的主要用途”的实际用途吗？没有看懂这个的用途是什么

2017年11月17日

..... 以上留言由公众号筛选后显示 .....

[了解留言功能详情](#)