# 蓝牙Mesh基本介绍

## 前言

本文对蓝牙Mesh做一个基本的介绍

## 蓝牙Mesh诞生

蓝牙Mesh脱胎于CSR倡导的私有协议-CSR Mesh，该技术诞生于2014年。蓝牙技术联盟于17年7月19日正式宣布，蓝牙(Bluetooth)技术开始全面支持Mesh网状网络。

全新的Mesh功能提供设备间多对多传输，并特别提高构建大范围网络覆盖的通信能力，适用于楼宇自动化、无线传感器网络等需要让数以万计个设备在可靠、安全的环境下传输的物联网解决方案。

蓝牙Mesh网络是用于建立多对多（many：many）设备通信的基于BLE协议的网络拓扑，是一种纯软件协议。各个节点间并没有用实际的连接，而是使用广播功能发送数据，数据中有密钥与地址，只有对应的网络和节点能够收到消息。也就是蓝牙Mesh是没有路由的，基于一种网络泛洪的方式在网络发射消息。

## 蓝牙MESH基本概念

### 网状网(mesh)

Mesh网络，就是一个多对多网络(Many to Many)。每个设备节点都可以和别的节点自由通讯。在这种拓扑中，因为很多节点可以中继（relay）收到的消息(Message)，所以端对端的通信可以比原来单点之间的通讯距离要远很多。就好像小组讨论自由发言，如果做的太远听不见的话，别人也可以代为传话。

### 设备和节点（Devices and Nodes）

如果一个设备成为了蓝牙mesh网络的一部分，我们就把它叫做节点(node)。反之，我们就把它叫做“未配网的设备”（unprovisioned devices）。把未配网的设备变成节点的过程我们把它叫做“配网”（provisioning）。

### 元素(element)

三个子灯组成一大灯，每个子灯都可以通过寻址访问，子灯就称之为元素(element),大灯称之为节点(node)。

### 消息（Messages）

当一个节点需要查询别的节点的状态(Status)或者控制别的节点的时候，就需要发一个对应类型的消息。当一个节点向别人报告状态改变的时候，他也需要发出一个消息。在蓝牙mesh里面定义了很多种类型的消息，每种消息都有对应的操作码(opcode)。消息可以按照有应答（acknowledged）和没应答（unacknowledged）来分类。和大多数的通讯系统一样，有应答的消息需要接收节点给个响应。“发给你了”“收到两条了”。这样做有两个目的：一是告诉你我收到了。二是可以返回一些需要的值。如果发现没有收到应答，发送端可以再次发送。当然，如果是不用应答的消息，接收端收到就算了，不会告诉发送端的。

### 地址（Addresses）

蓝牙mesh定义了三种类型的地址：单播地址（unicast address），组播地址（group address）和虚拟地址（virtual address）。

#### 单播地址

网络内每个元素都有一个单播地址，一个有多个元素的节点也就有多个单播地址

单播地址具有唯一性可以识别出一个元素

这个地址是在配网的时候分配给设备的

一个mesh网络可以有32767个单播地址

单播地址范围为1- 0x7fff

#### 组播地址

组播地址是一个及以上个元素共有的广播地址

地址范围为0xc000 - 0xffff(中间包括特定群组地址和部分保留区域)

群组地址一般由Provisioner设置，在数据库中进行统一的分配和管理，防止网络中发生群组地址冲突

组播地址可以由蓝牙SIG来定义(SIG Fixed Group Addresses)，也可以动态分配

目前SIG定义了4个组播地址，分别是“All-proxies”, “All-friends”,“All-relays” and “All-nodes”

动态分配的组播地址是设计成在用户配置的时候，可以分配代表一些实际的场所，比如可以定义几个组播地址代表几个不同的房间。一共可以有16384个组播地址，其中SIG保留了256个，其他16128个都是动态分配的。

虚拟地址基本可以认为是组播地址的一个扩展，厂家自定义的地址类型。

虚拟地址： 虚拟地址是由节点的label UUID通过hash处理生成的，设置虚拟地址时，Provisioner会将label UUID发送给对应的设备，对应设备在收到目的地址是虚拟地址的数据后，会尝试用之前设置的label UUID进行验证。故Provisioner不用在数据库中维护虚拟地址的分配管理。虚拟设备也可以不经过Provisioner，由两个设备通过协商来生成。

————————————————

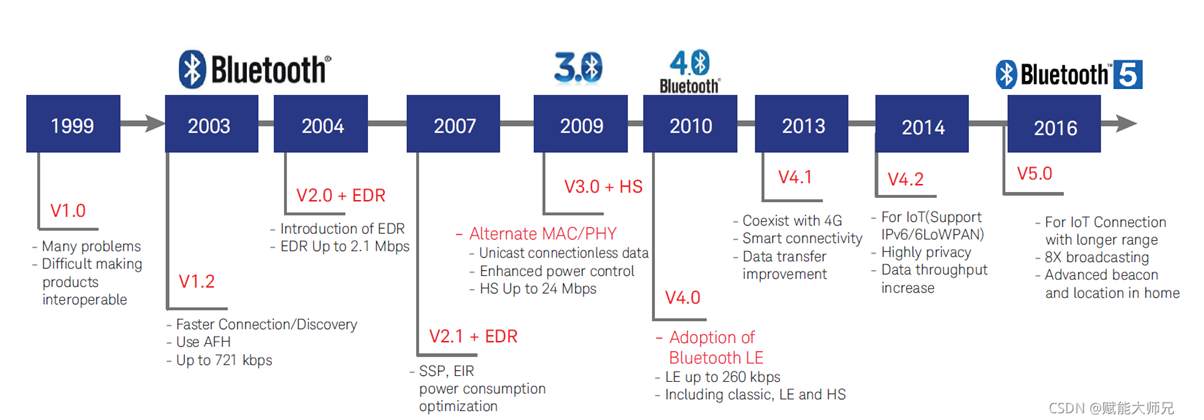
版权声明：本文为CSDN博主「kv110」的原创文章，遵循CC 4.0 BY-SA版权协议，转载请附上原文出处链接及本声明。

原文链接：https://blog.csdn.net/kv110/article/details/119361264

关于蓝牙这个名字的由来还有一个小故事。“蓝牙”这名称来自10世纪的丹麦国王哈拉尔德(Harald Gormsson)的外号。出身海盗家庭的哈拉尔德统一了北欧四分五裂的国家，成为维京王国的国王。由于他喜欢吃蓝莓，牙齿常常被染成蓝色，而获得“蓝牙”的绰号，当时蓝莓因为颜色怪异的缘故被认为是不适合食用的东西，因此这位爱尝新的国王也成为创新与勇于尝试的象征。1998年，爱立信公司希望无线通信技术能统一标准而取名“蓝牙”。

“蓝牙”的形成背景是这样的：1998年5月，爱立信、诺基亚、东芝、IBM和英特尔公司等五家著名厂商，在联合开展短程无线通信技术的标准化活动时提出了蓝牙技术，其宗旨是提供一种短距离、低成本的无线传输应用技术。这五家厂商还成立了蓝牙特别兴趣组，以使蓝牙技术能够成为未来的无线通信标准。芯片霸主Intel公司负责半导体芯片和传输软件的开发，爱立信负责无线射频和移动电话软件的开发，IBM和东芝负责笔记本电脑接口规格的开发。1999年下半年，著名的业界巨头微软、摩托罗拉、三星、朗讯与蓝牙特别小组的五家公司共同发起成立了蓝牙技术推广组织，从而在全球范围内掀起了一股“蓝牙”热潮。全球业界即将开发一大批蓝牙技术的应用产品，使蓝牙技术呈现出极其广阔的市场前景，并预示着21世纪初将迎来波澜壮阔的全球无线通信浪潮。

## 蓝牙发展轨迹



### 前期发展

1998年当年蓝牙推出 0.7 规格，支持 Baseband 与 LMP（Link Manager Protocol）通讯协定两部分。

1999 年先后推出 0.8 版、0.9 版、1.0 Draft 版。完成了 SDP（Service Discovery Protocol）协定和 TCS（Telephony Control Specification）协定。

1999 年 7 月 26 日正式公布 1.0A 版，确定使用 2.4GHz 频段。和当时流行的红外线技术相比，蓝牙有着更高的传输速度，而且不需要像红外线那样进行接口对接口的连接，所有蓝牙设备基本上只要在有效通讯范围内使用，就可以进行随时连接。

1999 年下半年，微软、摩托罗拉、三星、朗讯与蓝牙特别小组的五家公司共同发起成立了蓝牙技术推广组织，从而在全球范围内掀起了一股“蓝牙”热潮。

到2000年4月，SIG 的成员数已超过 1500，其成长速度超过任何其他的无线联盟。

### 第一代蓝牙：关于短距离通讯早期的探索

1999 年：蓝牙 1.0

早期的蓝牙 1.0 A 和 1.0B 版存在多个问题，有多家厂商指出他们的产品互不兼容。同时，在两个设备“链接”（Handshaking）的过程中，蓝牙硬件的地址（BD\_ADDR）会被发送出去，在协议的层面上不能做到匿名，造成泄漏数据的危险。

因此，当 1.0 版本推出以后，蓝牙并未立即受到广泛的应用。除了当时对应蓝牙功能的电子设备种类少，蓝牙装置也十分昂贵。

2001 年：蓝牙 1.1

蓝牙 1.1 版正式列入 IEEE 802.15.1 标准，该标准定义了物理层（PHY）和媒体访问控制（MAC）规范，用于设备间的无线连接，传输率为 0.7Mbps。但因为是早期设计，容易受到同频率之间产品干扰，影响通讯质量。

2003 年：蓝牙 1.2

蓝牙 1.2 版针对 1.0 版本暴露出的安全性问题，完善了匿名方式，新增屏蔽设备的硬件地址（BD\_ADDR）功能，保护用户免受身份嗅探攻击和跟踪，同时向下兼容 1.1 版。此外，还增加了四项新功能：

AFH（Adaptive Frequency Hopping）适应性跳频技术，减少了蓝牙产品与其它无线通讯装置之间所产生的干扰问题；

eSCO（Extended Synchronous Connection-Oriented links）延伸同步连结导向信道技术，用于提供 QoS 的音频传输，进一步满足高阶语音与音频产品的需求；

Faster Connection 快速连接功能，可以缩短重新搜索与再连接的时间，使连接过程更为稳定快速；

支持 Stereo 音效的传输要求，但只能以单工方式工作。

代表作：爱立信第一台蓝牙手机 T39mc

### 第二代蓝牙：发力传输速率的 EDR 时

2004 年：蓝牙 2.0

蓝牙 2.0 是 1.2 版本的改良版，新增的 EDR（Enhanced Data Rate）技术通过提高多任务处理和多种蓝牙设备同时运行的能力，使得蓝牙设备的传输率可达 3Mbps。

蓝牙 2.0 支持双工模式：可以一边进行语音通讯，一边传输文档/高质素图片。

同时，EDR 技术通过减少工作负债循环来降低功耗，由于带宽的增加，蓝牙 2.0 增加了连接设备的数量。

2007 年：蓝牙 2.1

蓝牙 2.1 新增了 Sniff Subrating 省电功能，将设备间相互确认的讯号发送时间间隔从旧版的 0.1 秒延长到 0.5 秒左右，从而让蓝牙芯片的工作负载大幅降低。

另外，新增 SSP 简易安全配对功能，改善了蓝牙设备的配对体验，同时提升了使用和安全强度。

支持 NFC 近场通信，只要将两个内置有 NFC 芯片的蓝牙设备相互靠近，配对密码将通过 NFC 进行传输，无需手动输入。

代表作：正在以蓝牙与无线耳机沟通的 Sony Ericsson P910i PDA 手机

### 第三代蓝牙：High Speed，传输速率高达 24Mbps

2009 年：蓝牙 3.0

蓝牙 3.0 新增了可选技术 High Speed，High Speed 可以使蓝牙调用 802.11 WiFi 用于实现高速数据传输，传输率高达 24Mbps，是蓝牙 2.0 的 8 倍，轻松实现录像机至高清电视、PC 至 PMP、UMPC 至打印机之间的资料传输。

蓝牙 3.0 的核心是 AMP（Generic Alternate MAC/PHY），这是一种全新的交替射频技术，允许蓝牙协议栈针对任一任务动态地选择正确射频。

功耗方面，蓝牙 3.0 引入了 EPC 增强电源控制技术，再辅以 802.11，实际空闲功耗明显降低。

此外，新的规范还加入 UCD 单向广播无连接数据技术，提高了蓝牙设备的相应能力。

代表作：蓝牙适配器

### 第四代蓝牙：主推” Low Energy”低功耗

2010 年：蓝牙 4.0

蓝牙 4.0 是迄今为止第一个蓝牙综合协议规范，将三种规格集成在一起。其中最重要的变化就是 BLE（Bluetooth Low Energy）低功耗功能，提出了低功耗蓝牙、传统蓝牙和高速蓝牙三种模式：

”高速蓝牙“主攻数据交换与传输；“传统蓝牙”则以信息沟通、设备连接为重点；”低功耗蓝牙“以不需占用太多带宽的设备连接为主，功耗较老版本降低了 90%。

BLE 前身是 NOKIA 开发的 Wibree 技术，本是作为一项专为移动设备开发的极低功耗的移动无线通信技术，在被 SIG 接纳并规范化之后重命名为 Bluetooth Low Energy（后简称低功耗蓝牙）。这三种协议规范还能够互相组合搭配、从而实现更广泛的应用模式。

蓝牙 4.0 的芯片模式分为 Single mode 与 Dual mode。Single mode 只能与蓝牙 4.0 互相传输无法向下与 3.0/2.1/2.0 版本兼容；Dual mode 可以向下兼容 3.0/2.1/2.0 版本。前者应用于使用纽扣电池的传感器设备，例如对功耗要求较高的心率检测器和温度计；后者应用于传统蓝牙设备，同时兼顾低功耗的需求。

此外，蓝牙 4.0 还把蓝牙的传输距离提升到100米以上（低功耗模式条件下）。拥有更快的响应速度，最短可在 3 毫秒内完成连接设置并开始传输数据。更安全的技术，使用 AES-128 CCM 加密算法进行数据包加密和认证。

^ 代表作：苹果 iPhone 4S 是第一款支持蓝牙 4.0 标准的智能手机

2013 年：蓝牙 4.1

蓝牙 4.1 在传输速度和传输范围上变化很小，但在软件方面有着明显的改进。此次更新目的是为了让 Bluetooth Smart 技术最终成为物联网（Internet of Things）发展的核心动力。

支持与 LTE 无缝协作。当蓝牙与 LTE 无线电信号同时传输数据时，那么蓝牙 4.1 可以自动协调两者的传输信息，以确保协同传输，降低相互干扰。

允许开发人员和制造商「自定义」蓝牙 4.1 设备的重新连接间隔，为开发人员提供了更高的灵活性和掌控度。

支持「云同步」。蓝牙 4.1 加入了专用的 IPv6 通道，蓝牙 4.1 设备只需要连接到可以联网的设备（如手机），就可以通过 IPv6 与云端的数据进行同步，满足物联网的应用需求。

支持「扩展设备」与「中心设备」角色互换。支持蓝牙 4.1 标准的耳机、手表、键鼠，可以不用通过 PC、平板、手机等数据枢纽，实现自主收发数据。例如智能手表和计步器可以绕过智能手机，直接实现对话。

2014 年：蓝牙 4.2

蓝牙 4.2 的传输速度更加快速，比上代提高了 2.5 倍，因为蓝牙智能（Bluetooth Smart）数据包的容量提高，其可容纳的数据量相当于此前的10倍左右。

改善了传输速率和隐私保护程度，蓝牙信号想要连接或者追踪用户设备，必须经过用户许可。用户可以放心使用可穿戴设备而不用担心被跟踪。

支持 6LoWPAN，6LoWPAN 是一种基于 IPv6 的低速无线个域网标准。蓝牙 4.2 设备可以直接通过 IPv6 和 6LoWPAN 接入互联网。这一技术允许多个蓝牙设备通过一个终端接入互联网或者局域网，这样，大部分智能家居产品可以抛弃相对复杂的 WiFi 连接，改用蓝牙传输，让个人传感器和家庭间的互联更加便捷快速。

LE链接安全

从Spec定义上蓝牙4.0和4.1的配对加密环节都是基于AES-CCM加密，但是由于蓝牙4.1双方共享同一密钥，所以存在被破解风险和漏洞。蓝牙4.2的pairing环节，采用Diffie-Hellman Key Exchange密钥交换算法进行加密，每一个设备有一对密钥对，公钥和私钥，私钥自己保存，公钥公开给对方，数据交互时，一方通过自己的私钥和对方的公钥进行加密文件，接收方通过自己私钥和传输方的公钥进行解密，从而有效的防止中间人破解密钥的事件发生。

历代蓝牙标准性能

隐私保护

蓝牙在广播过程中会携带自己的BD address (bluetooth device address)即为蓝牙唯一的MAC地址，在某些应用，比如物流追踪应用当中是非常有帮助的，可以根据BD address固定物流设备。

但是在某些应用不希望自己的BD address暴露在主端设备的监控下，蓝牙4.2给出了灵活的选择，蓝牙4.2规定，从机设备可以选择在广播模式下发送随机BD address，这样主端设备除了接该到设备之后才能获取其真实BD address，除此该设备广播模式的BD address为随机序列。

### 第五代蓝牙：开启「物联网」时代大门

2016 年：蓝牙 5.0

蓝牙 5.0 在低功耗模式下具备更快更远的传输能力，传输速率是蓝牙 4.2 的两倍（速度上限为 2Mbps），有效传输距离是蓝牙 4.2 的四倍（理论上可达 300 米），数据包容量是蓝牙 4.2 的八倍。

支持室内定位导航功能，结合 WiFi 可以实现精度小于 1 米的室内定位。

针对 IoT 物联网进行底层优化，力求以更低的功耗和更高的性能为智能家居服务。

低功耗版蓝牙与经典版蓝牙参数

Mesh 网状网络：实现物联网的关键”钥匙“

Mesh 网状网络是一项独立研发的网络技术，它能够将蓝牙设备作为信号中继站，将数据覆盖到非常大的物理区域，兼容蓝牙 4 和 5 系列的协议。

传统的蓝牙连接是通过一台设备到另一台设备的「配对」实现的，建立「一对一」或「一对多」的微型网络关系。

而 Mesh 网络能够使设备实现「多对多」的关系。Mesh 网络中每个设备节点都能发送和接收信息，只要有一个设备连上网关，信息就能够在节点之间被中继，从而让消息传输至比无线电波正常传输距离更远的位置。

这样，Mesh 网络就可以分布在制造工厂、办公楼、购物中心、商业园区以及更广的场景中，为照明设备、工业自动化设备、安防摄像机、烟雾探测器和环境传感器提供更稳定的控制方案。

办公楼里的 Mesh 网络

物联网：未来蓝牙技术的新主场

2019年1月：蓝牙5.1

增加AoA/AoD，号称厘米级误差定位

2019年12月31：蓝牙5.2

增加BLE audio,LC3的编解码方式