1. ble-mesh web：https://blog.csdn.net/zhanghuaishu0/article/details/78770486

1.1以消息为中心的通信。

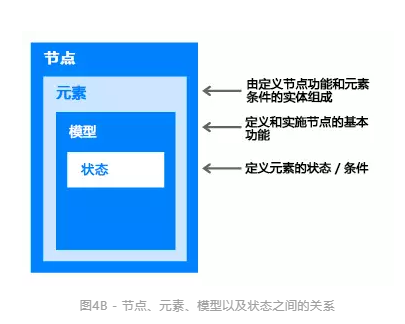
1.2 TTL 进行传送距离的改变

1.3 协议栈





1.4 节点模型

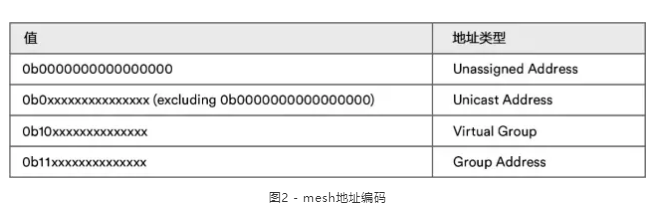


每个模型都有唯一的标识符。蓝牙技术联盟采用16位的模型，而供应商采用32位。

蓝牙mesh网络可借助消息，通过客户端 - 服务器架构进行通信

元素是节点内唯一可被寻址的实体

1.5 地址相关







1.6 message

1.6.1 消息的本地

* 控制消息（Control Message） - 与蓝牙mesh网络操作有关的消息，例如心跳（heartbeat）和friend的请求消息。
* 接入消息（Access Message） - 该类消息允许客户端模型检索或设置服务器模型中的状态值，或被服务器用于报告状态值。接入消息分为两类：经确认的(acknowledged)和未经确认的(unacknowledged)。
* 消息可被操作码（opcode）识别，并具有相关参数。操作码可识别消息的操作。

例如：

Generic OnOff Get – 用于为通用模型识别OnOff状态Generic。

Generic OnOff Set – 用于设置通用模型的OnOff状态

参数:

OnOff – 目标值（开或关）

TID – 事务标识符（Transaction Identifier）– 消息是新的还是转发的

转换时间（Transition Time）– 元素从一种状态转换到另一种状态所需时长

延迟（Delay）– 消息执行延迟

1.6.2 消息的安全

所有蓝牙mesh网络消息的安全保障都来自网络密钥（NetKey）和应用密钥（AppKey）对消息的加密和验证。

NetKey用于网络层通信。假设蓝牙mesh网络没有子网，则该mesh网络内的所有通信都使用相同的网络密钥。

AppKey用于应用程序的数据。网络中的一些节点具有特定应用，并且根据应用的需要对一些潜在敏感数据的访问进行限制。如 中继节点（relay node）（如灯泡或墙壁开关）通常具有有效的NetKey，能够在网络内中继敏感性消息。然而，这些节点无法访问各种限制区域（如楼宇控制或HVAC系统）的特定AppKey，，亦无法解密应用程序的数据。

1.6.3 消息交换

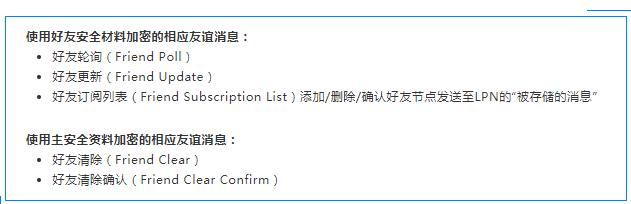
蓝牙mesh网络使用发布/订阅 (publish/subscribe) 模型来进行消息传输。生成消息的节点会发布消息。需要接收消息的节点会订阅它们所需的地址。

消息可被发布至单播、群组或虚拟地址。如：当模型发送回复消息时，使用消息始发处的源地址作为目标地址。发送非请求消息时，模型将使用模型的发布地址作为目标地址。节点中的每个模型都有一个发布地址。

订阅消息的模型使用模型的订阅列表来定义用于接收消息的有效地址。



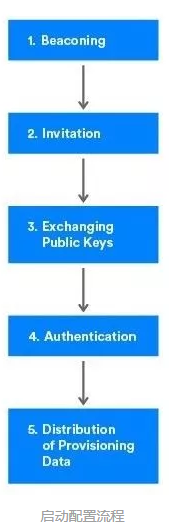
1.7 Friend 节点

“友谊”可在某些情况下终止：

如果在PollTimeout计时结束之前，好友节点未收到“ 好友轮询”、“好友订阅列表添加”或“好友订阅列表删除”消息，则友谊终止。

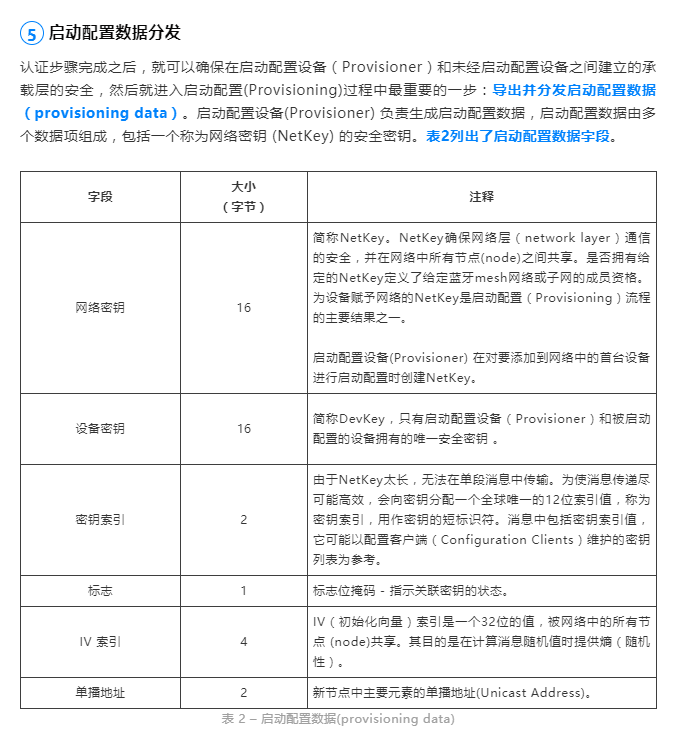
LPN可以通过将“好友清除”消息发送给好友节点，以启动友谊终止程序，“友谊”就会被好友节点终止。

1.8 新设备入网过程（配置过程）



1.9 mesh安全机制

* 蓝牙mesh采用称为“应用密钥（AppKey） ”的安全密钥来保护应用层消息。
* 蓝牙mesh网络中的所有节点都拥有一个或多个网络密钥（NetKey），每个网络密钥对应一个子网，它也可能是主要子网
* 节点还拥有一个唯一的安全密钥，称为设备密钥（DevKey），用于节点的启动配置（Provisioning）和配置流程。
* 由NetKey导出的隐私密钥(Private Key)用于对网络PDU (Payload Data Unit) 的报头值进行模糊化
* 这种保护是基于分别称为序列号（SEQ, Sequence Number）和IV索引(IV Index)的两个网络PDU字段。每次发布消息时，元素会增加SEQ值。节点从元素接收消息，如果元素包含的SEQ值小于或等于上一个有效消息中的SEQ值，则节点会将消息丢弃，因为这则消息可能与中继攻击有关。



1.10 sences

16-bit scenes number