BLE的广告扫描连接解析

广告 (Advertising)

为了使主机 (Central)能连接得上从机 (Peripheral)，从机必须进行广告。从机会每间隔一定的时间发送一个广告包 (Advertisement packet)，间隔的时间在 20ms 到 10.24s 之间。广告的间隔时间会影响之后启动一次连接所需要花费的时间。

主机在发送连接请求 (connection request) 启动连接之前必须接收广告包。而从机在发送完一个广播包后的一小段短时间内，只监听主机的连接请求。

一个广告包能够包含 31 个字节的数据。通常包含的内容有一个用户可读的名称、光宇设备发送包的信息、一些用于获知本设备是否能够连接等。

当主机接收到一个广告包时，它将发送一个叫做“扫描请求”(Scan Request)的请求来获得更多的广告数据，当然前提是这个活跃的扫描者(Active Scanner)已经进行了配置。然后从机通过发送一个“扫描响应”(Scan Response)来回应这个请求，这个回应可以包含额外的 31 个字节的数据。

广告，包括扫描请求和响应，它们采用三个不同的 2.4G 频率段以避开 WLAN 的干扰。

扫描（**Scanning**）

扫描是主机用来监听广告包和发送扫描请求的。有两个时序参数我们需要意识到他们的内容：“扫描窗口”（scan window 一次扫描进行的时间宽度）和“扫描间隙”（scan interval 一次扫描的总时间，包括扫描休息的时间和扫描进行的时间）。

对于每一次的扫描间距，主机扫描的时间等于“扫描窗口”，意思是说，如果“扫描窗口”等于“扫描间距”，那就意味着主机在进行连续的扫描。所以说，主机扫描的占空比就是“扫描窗口”的时间对于“扫描间隙”的时间乘以百分之百。

启动连接（**Initiating**）

当主机想要进入连接时，它将使用跟当扫描广告包时一样的程序。当启动连接时，在接收到一个广告包时，主机将发送一个连接请求（connection request）给从机。

连接（**Connection**）

根据连接中第一次数据交换来定义主机（Central）和从机（Peripheral）。当进行连接时，主机将从从机的特别定义的“间隙时间”(Interval) 请求数据。这个间隙时间称作“连接间隙”（Connection interval）。它取决于并用于主机连接，不过从机可以发送更新连接参数请求（Connection Parameter Updata Requests）给主机。根据 Bluetooth Core Specification，这个时间间隙必须在 7.5ms 到 4s 之间。

如果从机在时间帧内（time-frame）不响应这个来自于主机的包，这称作连接监管超时（Connection supervision timeout）此次连接被认为已丢失。

在每次连接间隙中通过传输多个包来获得更多的数据吞吐量是可以的。每次包的发送最多可以是 20 个字节。但是，如果当前消耗是重要的，从机没有数据发送，就可以选择忽略一定数量的间隙。被忽略的间隙被称作“从机延迟”（slave latency）。

在一次连接中，设备们将通过所有的通道在频率带中进行跳频（hop），除了广告通道，对应应用程序来说，某种程度上是完全透明的。

2015-4-10 11:45:44 木棉城。