蓝牙学习四（广播）

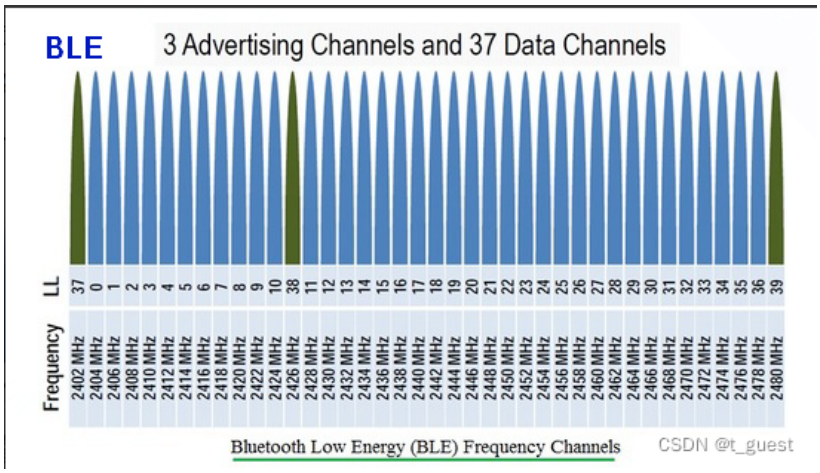
原创 t_guest 已于 2022-12-01 14:28:23 修改 3440 收藏 37 版权
分类专栏： 蓝牙 文章标签： BLE 广播

1.简介

什么叫做**广播**，顾名思义就像广场上的大喇叭一样，不停的**向外传输着信号**。不同的是，大喇叭传输的是音频信号，而蓝牙传输的是**射频信号**。

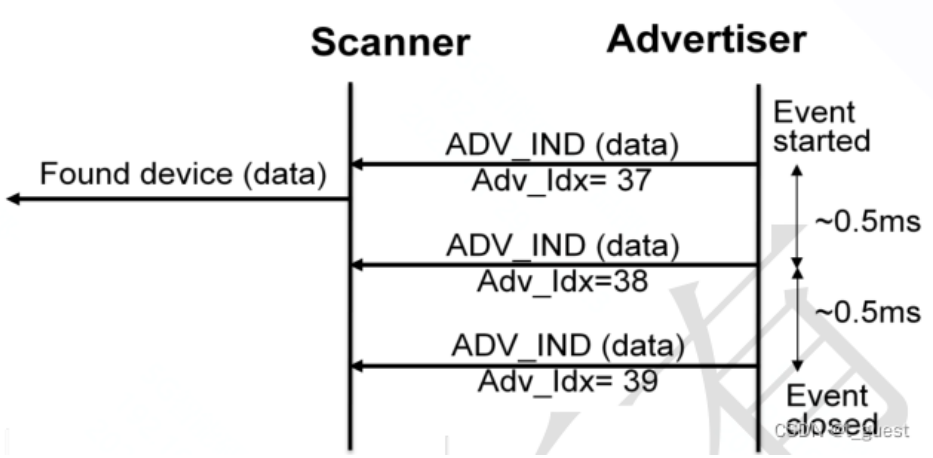
BLE 使用的是**无线电波传递信息**，就是将数据编码，调制到射频 信号中发射。BLE使用的射频频率是**2.4GHz**。跟WIFI、 Zigbee 等协议使用的是同一频段。

那如何做到使用同一频段而有不相互干扰呢？首先要知道的是2.4G指的**不是某一个频率**，而指的是一个**频段**（**2400MHz-2483.5MHz**）。在这个频段内**每隔2M**为一个信道，共**40个信道**。2.4G频段是一个用于短距离，无须执照使用的开放频段。意思就是可以**免费使用**。为了不占用更多的资源从而造成相互干扰，每个设备在使用时，同一时刻，只会在一个信道进行工作，不会占用其他信道。**一个BLE设备，在任一时刻，只能选择40个信道之中的一个进行发射或监听**。



BLE将信道划分为**广播信道**和**数据信道**。广播信道只有**3个**，**37、38、39**。剩下的37个信道全都是数据信道0-36。

在广播事件中，**每一个广播事件都会在3个广播信道中进行数据传输**，而且每一个事件都是从最小的信道编号开始传输。也就是说当广播事件来了，**数据包从广播信道37、38、39中依次进行传输**。



2. 广播间隔

设备每次广播时，会在**3个广播信道**发送相同的报文。这些报文报文的动作被称为一个**广播事件**。除了定向广播外，其他广播事件均可以选择**20ms-10.28s**不等的间隔。通常，一个广播中的设备会每一秒广播一次。两个**相邻的广播事件之**

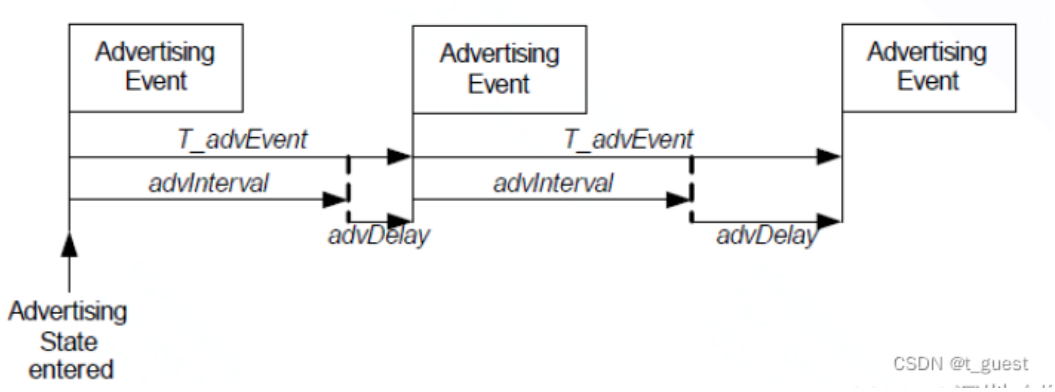
间的时间被称为“**广播间隔**”。

设备周期性的发送广播会有一个问题：由于设备间的时钟会不同程度的漂移，两个设备可能在很长一段时间同时广播而**造成干扰**。为了防止这一情况的发生，除定向广播外的其他广播类型，发送时间均会有些许波动。实现方式为，在上一次广播事件后**加入“0-10ms"的随机延迟**。这意味着，即使两个设备广播间隔相同，并在相同信道及时间点上发送造成了冲突，但他们发送下一个广播事件时也很大概率不会冲突。

所以，两个相邻的广播事件之间的时间间隔T_advEvent为：

T_AdvEvent = advInterval + advDelay

其中，advInterval必须是0.625ms的整数倍，范围是20ms-10.24s之间。对于可扫描非定向广播和不可连接非定向广播者两种广播类型，该值最好不小于100ms，即160个0.625ms。advDelay是LL层分配的一个随机数，范围为0-10ms。



在实际的设置中，通过设置**Advertising_Interval_Min（最小广播间隔）**和**Advertising_Interval_Max（最大广播间隔）**这两个参数来调整广播间隔。都是以**0.625ms为单位**。如果要**固定广播间隔**为某一个值，需要**将这两个参数设置为同一个值**即可。

3.广播类型

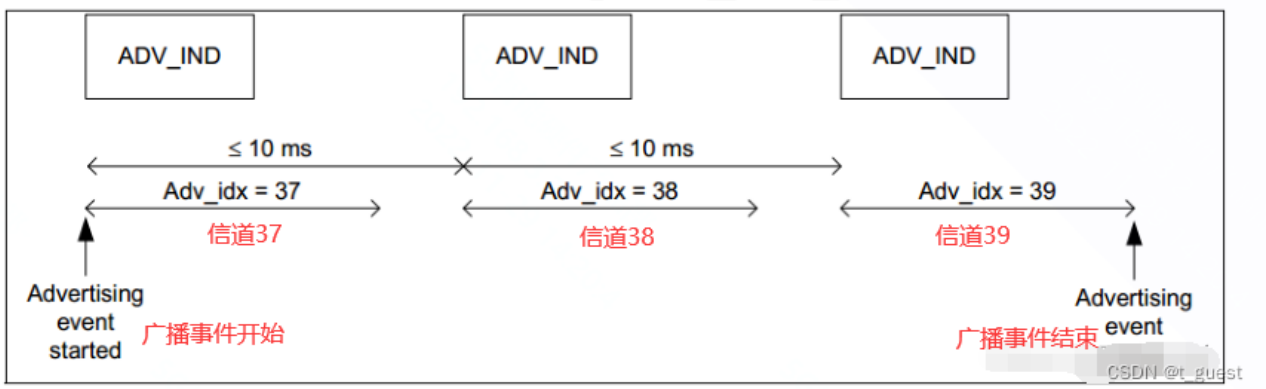
3.1 非定向可连接广播事件（ADV_IND）

ADV_IND就是**链路层通过广播信道发送广播的事件**。发送的**PDU**（Protocol Data Unit-**协议数据单元**）是ADV_IND_PDU-**通用广播报文**。这个报文发送之后可以接收由扫描者发送的SCAN_REQ_PDU-**扫描请求**，或者由发起者发送的CONNECT_REQ_PDU-**连接请求**。而接收后链路层需要在同一个信道上进行扫描或回复发起者的应答。当接收的数据报文不符合广播滤波协议，要么就用下一个广播信道进行广播，要么就停止广播事件。如果接收到的SCAN_REQ_PDU通过了滤波协议，那么广播者需要在**150±2us**内在同一信道回复SCAN_RSP_PDU-**扫描应答报文**。如果接收到CONNECT_REQ_PDU，则**进入连接状态**，这个时候并**不需要进行应答**。

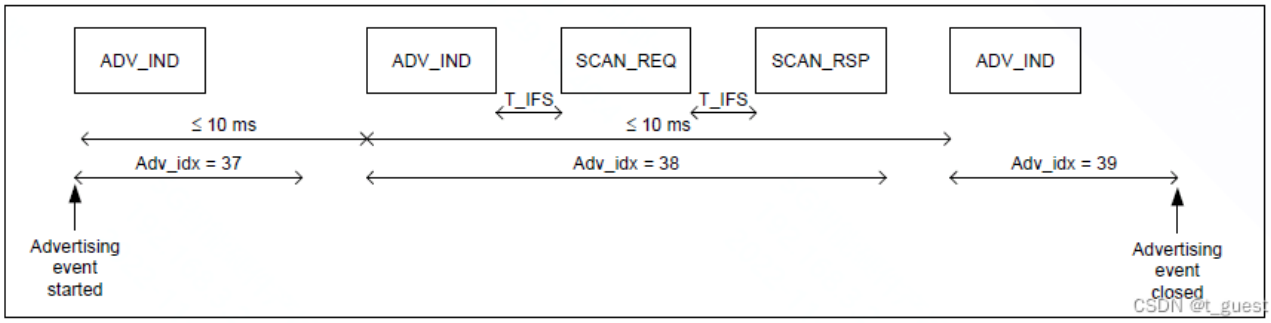
需要注意的是，一个广播事件中，相邻两个ADV_IND_PDU之间的**时间需要不大于10ms**。

接下来分类一下此类广播事件中广播包的发送情况。

（1）仅仅有广播PDUS

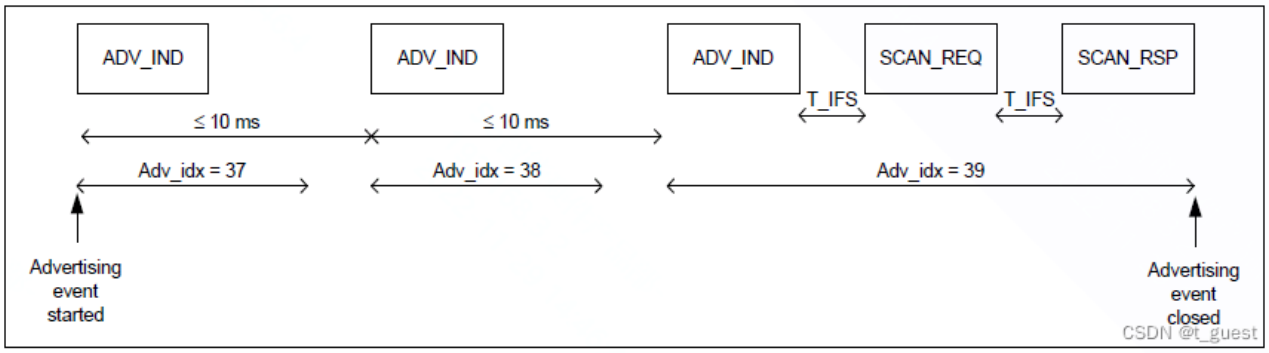


（2）在广播事件中有SCAN_REQ_PDUS和SCAN_RSP_PDUS。

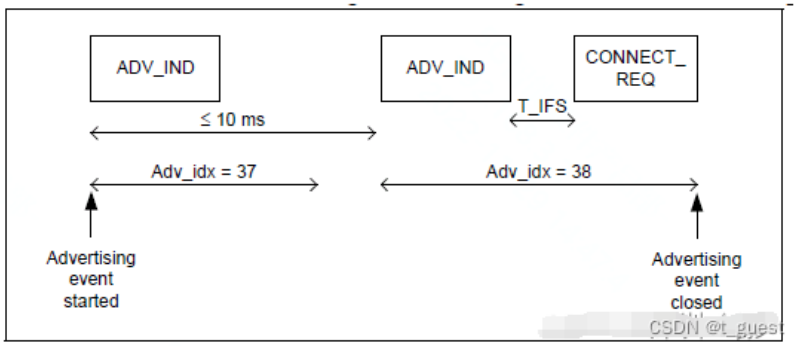


注：当有扫描请求包再广播事件中的中间信道上收到时，T_IFS（帧间隔）为150us。

（3）在广播事件的结尾有SCAN_REQ和SCAN_RSP。

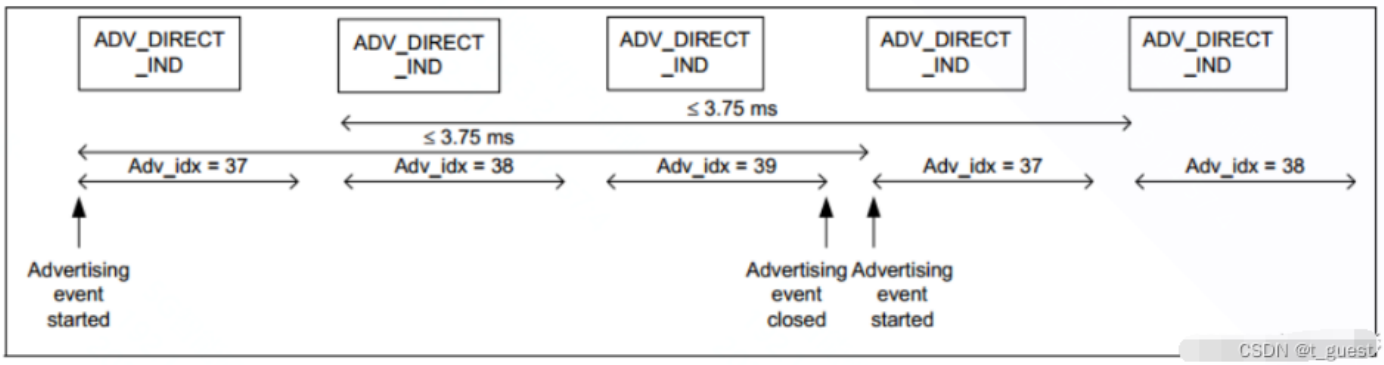


（4）在广播事件的中间接收到CONNECT_REQ-连接请求包。没有应答



3.2 定向可连接广播事件（ADV_DIRECT_IND）

这个广播是为了**快速建立链接**。这种报文包含两个地址：**广播者地址**和**发起者地址**。发起者收到发给自己的定向广播报文后，可以**立刻发送连接请求事件作为回应**，并**立刻进入连接状态**。
定向广播事件有特殊的时序要求。完整的广播事件必须每**3.75ms**之内重复一次，即**3.75ms内在37、38、39三个广播信道上全部发送一次报文**。这样的方法使得扫描设备只需要扫描3.75ms即可收到定向广播设备的消息。



如果按照定向广播的要去持续发送报文的话，广播信道将充斥着大量的定向广播报文。如此其他设备将无法进行广播。所以，蓝牙协议规定，**定向广播不能持续1.28S以上**。如果主机没有主动要求停止，或者连接没有建立，控制器会**自动停止广播**。一旦超过1.28S，主机只能使用通用广播让其他设备连接。

3.3 非定向不可连接事件（ADV_NONCONN_IND）

该广播的时间要求**与通用广播事件相同**。此外，该事件**只向外发射广播报文**，但是**不可以被连接**，也**不接收任何信息**。是**唯一**一个只有发射而没有接受的广播类型。**ibeacon**发出的就是这种类型的广播。

3.4 非定向可发现不可连接事件（ADV_DISCOVER_IND/ADV_SCAN_IND）

该广播的时间要求**与通用广播事件相同**，应答也是SCAN_REQ和SCAN_RSP。这个广播和通用广播的区别是，它**不能建立连接**。

注：所谓的**定向**和**非定向**针对的是**广播对象**，如果是针对特定的对象进行广播（**在广播包PDU中包含目标对象的MAC**），则为定向广播。反之为非定向广播。**可连接**和**不可连接**指的是**是否接受连接请求**。如果是不可连接的广播类型，它将**不应答连接请求报文**。**可扫描广播类型会回应扫描请求**。

不同的广播类型对应的扫描请求和连接请求如下图：

广播事件	发起者给广播事件的应答包	
	SCAN_REQ	CONNECT_REQ
ADV_IND(通用广播)	Yes	Yes
ADV_DIRECT_IND(定向广播)	No	Yes (地址匹配)
ADV_NONCONN_IND(不可连接广播)	No	No
ADV_DISCOVER_IND/ADV_SCAN_IND (可发现不可连接广播)	Yes	No

4. 广播响应包

广播包有两种：**广播包**（Advertising Data）和**响应包**（Scan Response）。其中广播包是每个设备**必须广播**的，而响应包是**可选**的。

广播包在蓝牙5.0协议栈核心中介绍如下：

Advertising_Data_Length: *Size: 1 Octet*

Value	Parameter Description
0x00 – 0x1F	The number of significant octets in the Advertising_Data.

Advertising_Data: *Size: 31 Octets*

Value	Parameter Description
	31 octets of advertising data formatted as defined in [Vol 3] Part C, Section 11.
	All octets zero (default).

应答包介绍如下：

Scan_Response_Data_Length: *Size: 1 Octet*

Value	Parameter Description
0x00 – 0x1F	The number of significant octets in the Scan_Response_Data.

Scan_Response_Data: *Size: 31 Octets*

Value	Parameter Description
	31 octets of Scan_Response_Data formatted as defined in [Vol 3] Part C, Section 11.
	All octets zero (default).

每个包都是**31字节**，数据包中分为**有效数据**（significant）和**无效数据**（non-significant）

有效数据部分：包含若干个广播数据单元，称为AD Structure。AD Structure的组成是：**第一个字节是长度值Len**，表示接下来的Len个字节是数据部分。数据部分的第一个自己表示**数据的类型AD Type**，剩下的len-1个字节是真正的数据AD Data。

无效数据部分：因为广播包的长度必须是31个字节，如果有效数据部分不到31字节，则剩余部分**用0补全**。

广播响应包是为了给广播一个额外的31字节数据，用于**主机在主动扫描情况下**，**反馈数据使用**。