目　　录

第1章　无线技术规范

1. 概述

蓝牙传输设备工作在 2.4GHz ISM（工业、科学、医学）频段，本规范确立了蓝牙传输设备的专用工作频段范围。

据此而论，蓝牙系统必须符合下述两个必要条件：

- 工作在蓝牙系统中的各无线电设备之间，必须具有兼容性。
- 应确定系统容量。

蓝牙传输设备应遵循由附录 A 及附录 B 所阐述的完整操作规范的操作条件，无线电收、发设备的参数必须按射频（RF）测试标准的所述方法测试。目前世界上主要采用的是欧洲、日本及北美三种测试标准，这三种测试标准也仅作为一种参考标准，它们随时根据无线电设备技术的发展而被修改和完善。

例如：在美国无线电传输设备由美国联邦通信委员会（FCC）来制定其测试标准，而在欧洲，除西班牙、法国外，其它国家都采用欧洲电信设置标准（ETSI）。

2. 频段及信道分配

由于蓝牙系统工作在 2.4GHz ISM 频段，而该频段根据有关法规属于工业、科学、医学等领域的工作频段，所以世界上绝大多数国家将该频段的带宽定为 2400—2483.5GHz，然而有些国家对该频段作了一些限制。为满足这些限制，使设备能处于正常工作状态，因而产生了符合自身国情的各种跳频算法。没有采用这些算法的常规产品在那些有限制的地区是不能且也不允许工作的。若为满足这些地区的使用而专门生产符合该地区限制的专用产品，显然是非常不合算的。蓝牙 SIG 推荐的设备可以克服这种不便，使其设备可在任何不同的地区使用。

这里用一个表格形式来说明世界上几种主要地区频带分配情况。

表 1.1 工作频段

地　　区	频 率 范 围	射 频 波 道
美国、欧洲及大部分其它国家①	2400∽2.4835 GHz	f =2402+ kMHz k=0,.....,78
西班牙②	2.445∽2.475 GHz	f=2449+ kMHz k=0,.....,22
法国③	2.4465∽2.4835 GHz	f=2454+ kMHz k=0,.....,22

注：① 日本于 1999 年 10 月初 MPT 公布了将原频段范围扩展为：2.4～2.4835 GHz，并立即生效。然而通过 TELEC 设备的测试，为完成这种改变还需要有一段时间，所以预先专门设计的复盖 2.471～2.497 GHz 跳频算法仍作为一种选择。

② 西班牙提出建议将国家频段范围扩展为 2.403～2.4835 GHz。为达到全面的一致，蓝牙 SIG 已与西班牙的相关管理机构接洽，可望在 2000 年初能得到结果。

③蓝牙 SIG 已与法国的管理机构确立了良好的关系，紧接的就是全面的发展。在频段分配上，美国、欧洲（西班牙、法国除外）及大多数国家都采用 2.400～2.483GHz 标准频段，射频信道为：f=2402+kMHz，k=0，1，2，…78。由于信道间隔为 1MHz。各国为遵循带外规定，均在低边带和高边带设置了保护带宽。如表所示：

表 1.2 防护带

地　　区	低 边 带	高 边 带
美国	2MHz	3.5MHz
欧洲（除西班牙、法国外）	2MHz	3.5MHz
西班牙	4MHz	26MHz
法国	7.5MHz	7.5MHz
日本	2MHz	2MHz

3. 发射机特性

需要说明的是，当设备与天线模拟器相连时，则对发系统按不同的输出功率分别进行阐述。在阐述前我们首先假设天线的功率增益为 0dBi，设备与天线模拟器的连接为无损耗作为天线参考条件。

由于辐射在测量时对精确度要求的准确性极难得以保证，因此，采用全等效的天线模拟器来代替整个天线系统。

如果在测试中天线实际增益大于 0dBi，则可利用 ETSI 300 328 和 FCC 的第 15 节对其校正。

发射机可按输出功率分为三种类型。

功率分类 1：最大输出功率（Pmax）是：100mW(20dBm)。
一般输出功率是：N/A。
最小输出功率是：1 mW (0dBm)。
功率控制：Pmin<+4 dBm 到 Pmax。
Pmin 到 Pmax 可选择。

功率分类 2：最大输出功率（Pmax）是：2.5 mW(4dBm)。
一般输出功率是：1 mW(0dBm)。
最小输出功率是：0.25Mw(-6dBm)。
Pmin 到 Pmax 可选择。

功率分类 3：最大输出功率（Pmax）是：1mW(0dBm)。
一般输出功率是：N/A。

最小输出功率是：N/A。

Pmin 到 Pmax 可选择。

上述所提的最小输出功率是相对于最大功率所言，而且最低功率限制 Pmin<-30 dBm 也仅是一个建议，并不需严格遵循这种规定，它可以根据实际应用的需要而选择。

当发射机输出功率为第一种类型时，则具有功率控制能力。该功能可控制发射机功率超过 0dBm 的情况，在 0dBm 下时，发射机功率控制是可选的，为此可获取最佳功率损耗及干扰。功率输出增益控制选择采用了一种单调序列步进方式（即：线形方式）这种步进增益由两种方式组成，一种是高步进增益（每步 8 dB），另一种是低步进增益（每步 2 dB）。当类型 1 设备是使用最大传输功率（+20dBm）时，在实际使用中一般控制在低于 4dBm 的情况或更小。

具有功率控制功能的发射机，在工作过程中使用 LMP（具体内容见链接管理协议）来获得最佳输出功率。若发射功率出现波动时，发射机设备由 RISS 测量并回送测试结果。

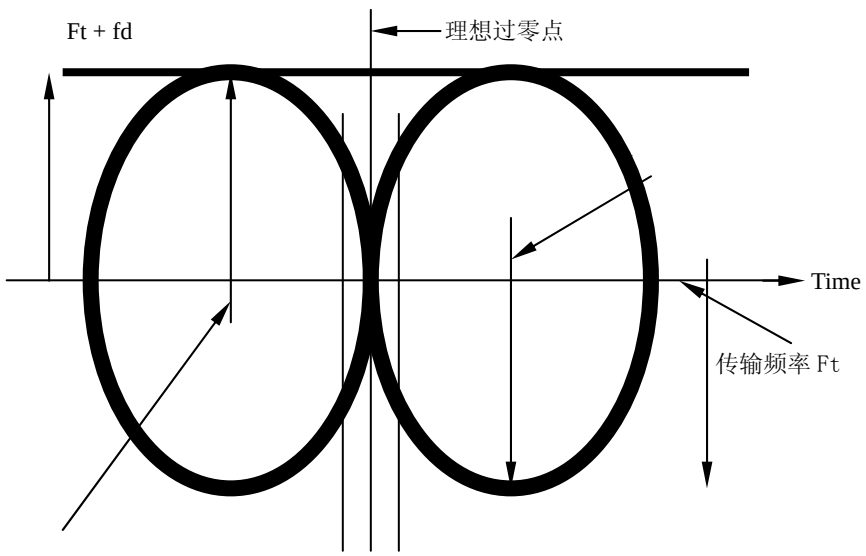
3.1 调制特性

调制是用 BT=0.5 的 GFSK，调制指数在 0.28~0.35 之间。二进制数所表示的“1”代表频率正偏差，而“0”代表频率负偏差。符号 **Timing** 表明优于±20ppm。

对每个传输信道，符合 1010 序列的最小频偏（Fmin≤{Fmin+，Fmin-}）将不小于按 00001111 序列的频偏（fd）的±80%，另外最小频偏将决不会小于 115KHz。

理想信号正交于零点时，应是无误差的（正交清晰，无扩散）。本规范定义了实际信号过零正交时的扩散与理想状况相比其范围（正交模糊度）小于±1/8。

在此用眼图的形式来描述调制特性。



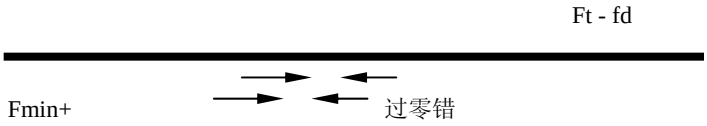


图 1.1 眼图

3.2 寄生辐射

带内及带外寄生辐射使用跳频发射机在单频上的跳频来测量。这就是说在接收时隙和发射时隙之间，频率必须是同步地改变，，从而使收、发信机始终是同步在同一传输频率上。

3.2.1 带内寄生辐射

在 ISM 带内的发射机将遵循下表所提参数通过频谱框架。

表 1.3 传输频谱框架

频 率 偏 移	传 输 功 率
±550 KHz	-20 dBC
｜M-N｜=2	-20 dBm
｜M-N｜≧3	-40 dBm

频谱必须符合 FCC 的-20dB 带宽精度声明，并将据此精度测量。另外 FCC 规定，在相邻信道上的相邻信道功率不同于两个或两个以上相邻信道数定义的相邻信道功率。该相邻信道功率定义为在 1MHz 信道内功率测量的总和。发射机功率以最大保持为 100KHz 带宽来测量。如发射机在 M 信道上发射，而相邻信道功率在信道 N 上测量。发射机是用发射一个伪随机数据帧通过测试。

注：若输出功率小于 0dBm，那么无论如何，FCC 的 20dB 有关规定将否定如上所述的绝对相邻信道功率规定。

除允许增加到 3 个 1MHz 宽的频带以外，中心频率是一个 1MHz 的若干整倍数，而且必须符合-20 dBm 的绝对值。

3.2.2 带外寄生辐射

功率测量以 100 KHz 带宽测量。

其测量数据如下：

表 1.4 带外寄生辐射规格

通 频 带	运 行 模 式	理 想 模 式
30 MHz—1GHz	-36 dBm	-57 dBm
1 GHz—12. 75 GHz	-30 dBm	-47 dBm
1. 8 GHz—1. 9 GHz	-47 dBm	-47 dBm

5. 15 GHz—5. 3 GHz	-47 dBm	-47 dBm

3.3　设备频率容许偏差

发射机初始中心频率精度必须是取自F_C的±75kHz。在任何信息传输前，初始频率精度作为频率精度标准。但我们需注意，频率漂移规定不包含在±75KHz内。

分组里的发射中心频率漂移以下表说明，而不同的分组在基带规范说明中给出。

表 1.5 分组里的频率漂移

报 文 类 型	频 率 漂 移
单时隙分组	±25kHz
三时隙分组	±40kHz
五时隙分组	±40kHz
最大漂移率※	400Hz/μs

注：※最大漂移率允许出现在分组的任何位置。

4．接收机特性

为测试误码率性能，接收机设备必须具有“回传”功能，设备回传译码信息。该功能在测试模式规范里确定。在该节内容中涉及到的参考灵敏度电平为-70dBm。

4.1 实际灵敏度电平

实际灵敏度电平以 0. 1%固有误码率（BER）输入电平形式定义。蓝牙技术中的接收机实际灵敏度电平应是-70dBm 或更好。接收机设备必须达到-70dBm 灵敏度电平，以适应蓝牙技术中在发射机特性内容中所提到的发射机设备特性。

4.2 干扰特性

同频和 1MHZ 及 2MHZ 的相邻干扰特性是希望信号用 10dB 以上的参考灵敏度电平来测试，在所有其它频率上，希望信号是一个 3dB 以上的参考灵敏度电平来测试。干扰信号的频率分布在带外 2400~2497 MHz，带外衰减详细说明后面将会描述。干扰信号将被蓝牙调制，调制方法也在后面叙述。BER≤10%。信号的干扰比率如下表所示：

表 1.6 干扰特性

要　　求	比　率
同频干扰（C/I co-channel）	11 dB
相邻（1 MHz）干扰（C/I 1MHz）	0 dB
相邻（2 MHz）干扰（C/I 2MHz）	-30 dB

相邻（≥3 MHz）干扰（C/I ≧3MHz）	-40 dB
图象频率干扰（C/I image）	-9 dB
带内图象频率相邻（1 MHz）干扰（C/I image±1MHz）	-20 dB

注：上述标准是一个暂定标准，在蓝牙 1.0 版本发布后的 18 个月内上述标准可以成为正式标准。以蓝牙 1.0 版本发布之日起，经三年的观察期后，标准最终必须达到完善。在这样的一个观察期间，设备一定需满足+14 dB 的同频干扰阻抗、+4 dBACI（@1 MHz）阻抗、-6 dB 的图象频率干扰阻抗和-16 dB 的 ACI 带内图象频率干扰阻抗。另外，暂订标准中所提到的图象干扰频率是指带内图象频率。若该图象频率≠n*1 MHz，那么图象干扰频率取其最接近的 n*1 MHz 频率，若相邻信道标准可适用于同信道，则标准的实用性就显得更为宽松一些。

这些规范仅以常温条件测试，同时接收机的使用是加载在单频上。它意指在收—发信机之间的频率合成器必须改频，但总是回到同频接收。

无线电设备频率不会遇到寄生响应频率。从≥2 MHz 间隔的获取信号中，在频率里允许有五个寄生响应频率，在这些寄生响应频率上会见到 C/I= -17dB 的不严格的干扰标准。

4.3　带外阻塞

带外阻塞是用超过参考灵敏度电平 3dB 的信号来测试。干扰信号将形成连续的漂移信号，且 BER 将 ≤0.1%。带外阻塞将满足下述标准。

表 1.7　带外阻塞规格

干扰信号频率	干扰信号功率电平
30MHz～2000 MHz	-10 dB
2000MHz～2399 MHz	-27 dB
2498MHz～3000 MHz	-27 dB
3000MHz～12. 75 GHz	-10 dB

除 24 信道被允许作为给定的接收频率之外，若中心频率都取 1MHz 的整倍数，在产生寄生响应频率的 19 信道，干扰可能是 BER 为 0.1% 的 -50 dB 的功率电平。余下其间的产生寄生响应频率的 5 个信道，功率电平是随机的。

4.4　交叉调制特性

在 BER=0. 1%时，频率灵敏度会以如下所述情况出现：

- 用超过参考灵敏度电平 6 dBm 的功率电平有效信号频率 f_0 处。
- 静态正弦波信号在功率电平为 -39 dBm 的 f_1 处。
- 蓝牙调制信号（见后述）在功率电平为 -39 dBm 的 f_2 处。

这样 $f_0=2f_1-f_2$ 及 $|f_2-f_1|=n*1MHz$，此处 n 取值可为 3、4 或 5，且蓝牙系统必须满足三个选择条件之一。

4.5　最大有效电平

接收机最大有效输入电平以优于 -20dBm 运行。 BER 的值将小于或等于 -20dBm 输入功率的 0. 1%。

4. 6　　寄生辐射

蓝牙接收机的寄生辐射不会多于下述描述：

表 1.8 带外寄生辐射

频　　带	规格
30MHz～1GHz	-57 dBm
1GHz～12.75GHz	-47 dBm

被测功率以 100KHz 带宽测试。

4.7　接收机场强指示（ 随机值 ）

作为功率控制连接的收发信机必须可以测量它自身接收信号强度来确认连接在另一端发射机输出功率的增加或减少，该功能由接收机场强（RSSI）来实现。

功率控制的方法以最佳的接收功率为规定标准。该最佳接收功率用一个低限和一个高限区域来表示。RSSI 必须有一个等于该区域最小变化范围。当接收信号功率是 -20dBm 时，RSSI 必须有一个±4dBm 或更好的绝对精度值。另外起始于-60 dB 向上 20±6dBm 的最小区域必须被复盖。

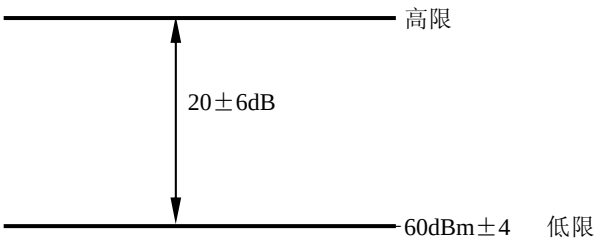


图 1. 2 RSSI 动态区域和精度

4.8　干扰信号定义基准

蓝牙调制干扰信号作如下定义：

调制：GFSK。

调制指数：0. 32±1%。

BT：0. 5±1%。

比特率：1Mbps±1ppm。

调制数据：PRBS9。

频率精度优于±1ppm。

5.1　标称测试条件（NTC）

5.1.1 常温

测试的常温一般选择为 +15℃ 到 +35℃。当用该条件测试的结果来说明其真实性是不实际时，所以被测设备的环境温度一定要标注。同时在测试过程中的实测数据应在测试报告中记录。

5.1.2 电源

5.1.2.1 主电源

作为与主体设备相连的标称测试电源应是主电源。标称电压应是明确给出或在设计设备时用能够明确表明电压的任何其它形式标明。测试电压的频率应符合主体交流电源的标称频率 2% 内的规定。

5.1.2.2 车载酸性电池电源

当无线电设备准备用车载酸性电池或交流电机作为设备运行电源时，标称测试电压应是电池（6V，12V 等）的标称电压的 1.1 倍。

5.1.2.3 其它电源

对其它电源或电池类作为设备运行电源时，标称测试电压应在设备详细说明书中标出来，并在测试报告中记录。

5.2 临界测试条件（ETC）

5.2.1 临界温度

临界温度区域经组合以最大温度区域来确定。

- 最小温度区间 0℃+35℃。
- 在设备产品说明书中应提供产品工作温度范围。

临界温度区域范围和工作温度范围的说明应在测试报告中注明。

5.2.2 临界电源电压

当电源以这种临界工作条件作为设计指标时，其目的是考虑把这种电源产品作为其它设备或系统的工作电源而运行。而下面所述的临界电源测试指标并不作为一个必要要求，它只说明在这种特殊要求的环境下，主设备或主系统的限压条件将起作用。正确的限压范围由制造厂商提供并应在测试报告中有记录。

5.2.2.1 主电源

连接到交流电源的设备做临界电压测试时，其临界电压应是标称电压±10%偏差。

5.2.2.2 车载酸性电源

当无线电设备用车载酸性电池或交流电机作为设备运行主电源时，临界测试电压是电池（6V，12V 等）的标称电压的 1.3 和 0.9 倍。

5.2.2.3 其它类型电池电源

使用下述类型电池作为设备的电源系统时，其低端临界测试电压是：

- 作为碱性或锂类电池其标称电压是 0.85 倍。

● 作为汞或镍-镉类电池其标称电压是 0.9 倍。

上述两类电池的高端临界测试电压是电池的标称电压的 1.15 倍。

5.2.2.4 其它类型电源

使用其它类或适应各类电源（一次或二次）的设备，标称测试电压应在技术说明书中给出或在测试报告中有记录。

5. 附录 B

下表中设备参数应据表中所提条件测试。

表 1.9

参　　数	温度	电源
输出功率	ETC	ETC
功率控制	NTC	NTC
调制指数	ETC	ETC
初始载频精度	ETC	ETC
载频漂移	ETC	ETC
带内寄生辐射	ETC	ETC
带外寄生辐射	ETC	ETC
灵敏度	ETC	ETC
干扰特性	NTC	NTC
交叉调制特性	NTC	NTC
带外阻塞	NTC	NTC
最大可用电平	NTC	NTC
接收机场强	NTC	NTC

注：表中 ETC 为临界测试条件，NTC 为标称测试条件。

第 2 章　基带规范

本节描述蓝牙链路控制器的一些技术框架。蓝牙链接控制器应遵循基带协议和一些其它低层链接规定。

1. 概述

蓝牙技术是以近距离无线连接为基础，而欲代替使用电缆连接的固定或移动的电子设备。该技术的使用，使系统具有操作简单、功耗低、价格低等特点。

蓝牙工作在全球通用的 2. 4MHz 的 ISM 频段，收发信机采用跳频技术来达到抗干扰和抑制信号衰减作用，利用二进制调频（FM）模式使收、发信机的复杂性得以简化。符号速率为 1Ms/s。 信道时隙以 625μs 的标称时隙长度作为应用标准。由于蓝牙系统采用了全双工分时（TDD）传输信息技术，所以在信道里，信息以分组结构的方式进行信息交换。在传输过程中，各信息分组用不同的跳频算法实现信息传输。理论上讲，一个分组复盖一个单时隙，实际上一个分组可扩展复盖 5 个时隙。

蓝牙协议使用了电路和分组切换的组合方式，时隙可以作为同步分组保留。同时，蓝牙也能支持一个异步数据信道乃至三个同步话音传输信道或同时支持异步数据信息和同步话音信道。

每个话音信道支持 64Kb/s 同步话音信道连接。异步信道最大可不对称地支持 723. 2kb/s（且回程为 57. 6kb/s）或对称地支持 433. 9kb/s。

蓝牙系统由无线电设备部分（见前述的无线电设备内容）、链接控制部分、链接管理支持部分和主终端接口功能组成。其结构图如下表示：

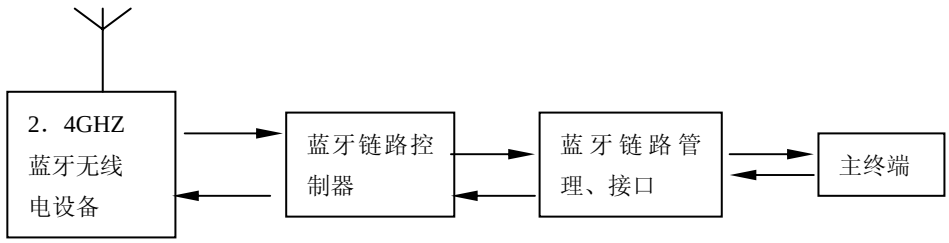
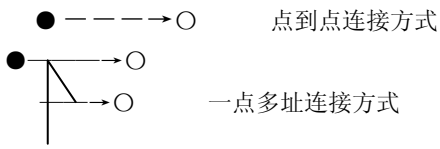


图 2. 1

该节内容描述的是执行基带协议和其它低层链接规定的蓝牙控制目的的详细说明。作为链接设立及控制的链接层信息在后面的链接管理协议中章节再详细介绍。

蓝牙系统提供点对点连接方式（即：蓝牙中仅有两点）或一点多址连接方式，其连接方式如图所示：



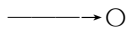


图 2.2

其中：“●”代表主单元，“○”代表从单元。

在一点多址连接方式中，信道是分在几个蓝牙单元中。分在同一信道中的两个或两个以上的单元形成一个匹克网（Piconet）。一个蓝牙单元作为匹克网的主单元，其余的可作为从单元看待。在一个匹克网中最多可有七个活动从单元。另外，更多的从单元被锁定在休眠状态中。这些处于休眠状态的从单元在该信道中不能被激活，但对主单元来讲它们仍由主单元同步。无论对激活或休眠状态来讲，信道访问都由主单元控制。

具有重叠复盖域的多匹克网形成一个散射网络（Scatternet）结构。每个匹克网只能具有一个单独主单元，然而从单元可分享基于时分多址的不同匹克网。另外，在一个匹克网中主单元可视为另一个匹克网的从单元。且各匹克网间不再是以时间或频率同步，各匹克网有自己的跳频信道。

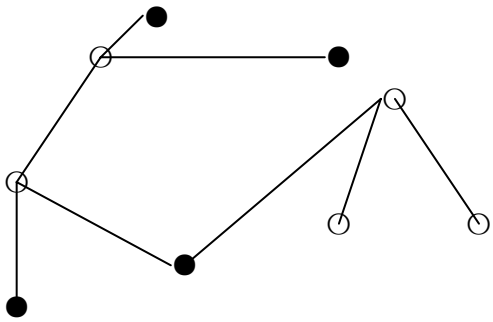


图 2.3 散射网络结构

1. 物理信道

2.1 频带及射频（RF）信道

蓝牙技术工作在 2.4 MHz 的 ISM 频段。虽然该频段为全球通用，但实际上准确的频率和带宽在各国有一些差异。在美国和欧洲，使用的带宽为 83.5 MHz ，在该频段里，以 1 MHz 的带宽为间隔设立了 79 个射频跳频点。在日本、西班牙和法国，缩减了带宽，在该频段里设立的 23 个射频跳频点，其带宽仍以 1 MHz 为间隔。在这里可以用一个表格形式来说明：

表 2.1 可用射频信道

地 区	频 率 范 围	射 频 信 道
欧洲及美国	2400～248.5 MHz	F=2402+k MHz K=0，1……78
日 本	2471～2497 MHz	F=2473+kMHz K=0，1……22

西 班 牙	2445～2475 MHz	F=2449+kMHz K=0，1……22
法 国	2446. 5～2483. 5 MHz	F=2454+k MHz K=0，1……22

2. 2 信道定义

信道使用一组伪随机跳频序列经 79 或 23 个射频跳频点跳频来表示。跳频序列对匹克网是唯一的，而且由蓝牙主单元的设备编址来确立，跳频序列的相位由蓝牙主单元的时钟确定。信道被分成时隙（时间片）的形式，且每个时隙符合 RF 跳频，跳频序列符合不同的射频跳频模式，最大跳频速率是 1600 跳/s，在匹克网中的全部蓝牙单元同时且同步跳入一个信道。

2.3 时隙

每个信道被分成长度为 625μs的时隙，时隙据蓝牙匹克网中主单元的时钟来编号。时隙编号区域从 0~2^{27}-1 且循环周期是 2^{27}，在这个时隙里，主和从单元都能传输分组。

由于蓝牙系统中主—从单元的分组传输采用是分时双工（TDD）交替传输方式，所以在系统中主单元都是采用偶数编号时隙来实现信息传输，而从单元却采用奇数编号时隙来实现信息传输。分组的起始位置与时隙起始点相吻合。由主或从单元完成的分组传输可以扩展到 5 个时隙，TDD 和定时工作方式如图所示：

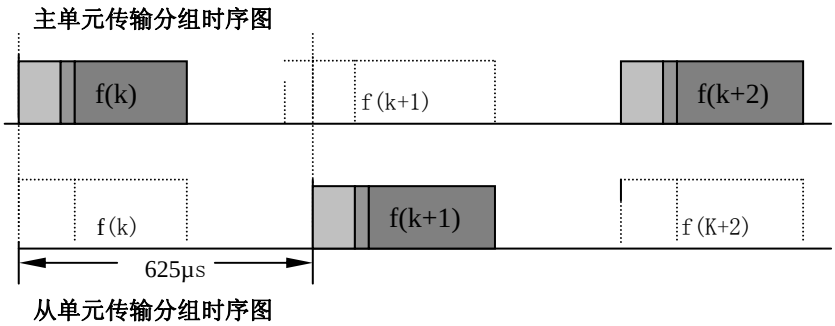


图 2. 4

射频（RF）跳频将以分组的持续时间作为一个固定时间值。对单时隙分组来讲 RF 跳频以当前蓝牙时钟值作为基点。对于多时隙分组来讲，RF 跳频以蓝牙中第一个分组时隙里的时钟值作为整个分组基点。在多时隙分组的第一个时隙里的 RF 跳频将被认为由当前蓝牙时钟值确定的频率。下图举例说明了单时隙分组和多时隙分组的跳频定义。若分组占有多于一个的时隙时，跳频就是用于以开始分组传输的起始点来作为时隙的跳频。

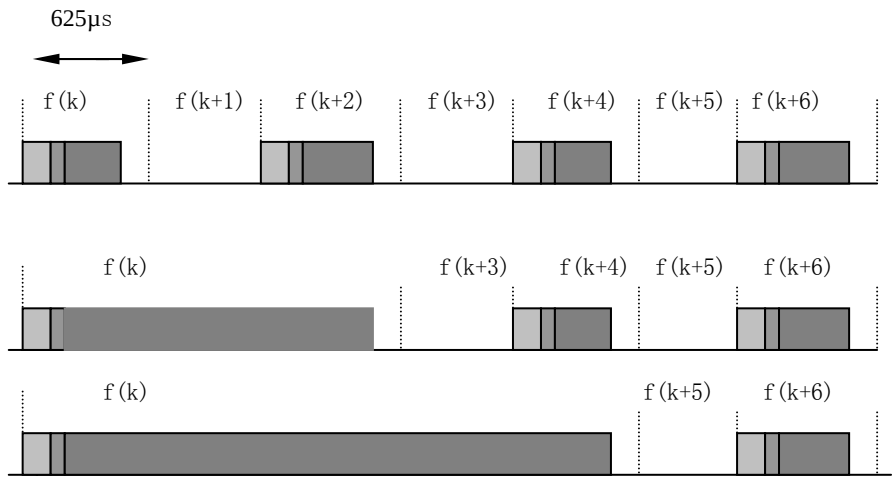


图 2.5　多时隙分组

2.4　调制与比特率

数据传输是以 1MS/s 的符号率进行传输。高斯型二进制 FSK 模式用于 0. 5 的蓝牙产品。二进制“1”代表正频偏，二进制“0”代表负频偏，最大频偏是在 140 KHz 到 175 KHz 之间。

3.　物理链接

3.1　概要

在主单元和从单元之间，可以确定不同的类型链接关系。如下定义了两种链接类：

- 同步定向链接（SCO）。
- 异步无链接（ACL）。

同步定向链接（SCO）是在匹克网中主单元和从单元之间实现点到点链接。主单元通过有规律的使用保留时隙来维持 SCO 链接。而 ACL 链接是主单元与共存于匹克网中的所有从单元之间实现一点多址的连接方式。在这种连接方式中，主单元并不以时隙来保留 SCO 链接，主单元在每个时隙基上建立对任何其它从单元的 ACL 链接。其中包括已预定用 SCO 链接方式中的从单元。

a)　SCO 链接

SCO 链接是在主单元与指定的从单元之间实现点到点的同步连接。SCO 链接方式采用保留时隙来传输分组，因此该方式可看作是在主单元和从单元之间实现电路交换连接。SCO 链接主要用于支持类似于象话音这类

时限信息。从主单元方面看，它可以支持多达 3 路的相同从单元或不同从单元的 SCO 链接。而从从单元方面看，针对同一主单元它可以支持多达 3 路的 SCO 链接。若链接来源于不同主单元，此时从单元只能支持 2 路 SCO 链接，在此种情况下决不能再传输 SCO 分组。

主单元以有规律的时间间隔来发送分组，所以在保留的主－从时隙里，称到从单元的 SCO 间隔为 Tsco（记数时隙）。在主－从时隙里 SCO 从单元总是允许响应 SCO 分组传输。但若先前的主－从时隙是使用不同的编址，此时这种传输是不能使用。如果在分组头里，SCO 从单元对从单元的编址码有解码错，在保留的 SCO 时隙里它仍允许返回一个 SCO 分组。

SCO 链接由主单元发送 SCO 建立消息，经链接管理（LM）协议来确立。该消息分组含定时参数（如 SCO 间隔 Tsco 和规定保留时隙补偿 Dsco）等。

为防止时钟隐藏问题，在LMP中设置信息的初始化标志应指出是初始化方式 1 或是初始化方式 2 被采用，从单元将通过初始化标志指示采用的初始化模式。若当前主时钟（CLK_{27}）的MSB是 0 时，主单元使用初始化模式 1。当前主时钟（CLK_{27}）的MSB是 1 时，主单元使用初始化模式 2。由主从保留的主－从SCO时隙取决于满足下述等式的时隙上被初始化。

$CLK_{27-1} \mod Tsco = Dsco$。 初始化方式 1

（CLK_{27-1}，$\overline{CLK_{26-1}}$）$\mod Tsco = Dsco$。 初始化方式 2

主－从 SCO 时隙直接跟随保留主－从 SCO 时隙。在初始化后，作为下一个主－从 SCO 时隙的时钟值 CLK（K+1），是通过加固定间隔 Tsco 到当前主－从 SCO 时隙的时钟值来建立。

CLK（K+1）=CLK（K）+ Tsco。

1.3 ACL 链接

在 SCO 链接不保留的时隙里，主单元可以与任何属于每个时隙基里的从单元进行分组交换。ACL 链接提供在主单元与所有在匹克网中活动从单元的分组交换链接，异步和等时两种服务方式均可采用。在主－从之间，若仅是单个 ACL 链接存在时，对大多数 ACL 分组来说，分组重传是为确保数据的完整性而设立。

在从－主时隙里，当且仅当先前的主－从时隙已被编址，则从单元允许返回一个 ACL 分组。如果在分组头的从单元地址解码失败，它就不允许传输。

ACL 分组未编址作为广播分组的指定从单元且各从单元可读分组。如果在 ACL 链接上没有传输数据及没有轮询申请，那么在 ACL 链接上就不存在发生传输过程。

2. 分组

3.1 一般格式

当在基带里作分组和消息的详细说明时，位排序必须遵循下列规则（即：Little Endian 格式）。

- b_0 代表最低有效位（LSB）。
- LSB 是第一个发送位。
- 在例中 LSB 被放在左边位置上。

基带控制器认为来自高层软件层中的第一位是b_0。即：这是经无线发送的第一位。而且，数据帧在基带电平内产生。如头帧信息和有效信息头长度信息，用LSB先发送。例如：X=3 的 3 位参数，其传输码值是$b_0\ b_1\ b_2$ =110，数位“1”首先经空中发送，最后才是数位“0”。

在匹克网信道上的数据以分组形式传输，一般格式如下：

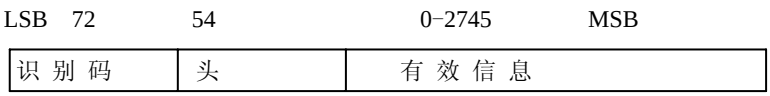


图 2.6 标准分组格式

每个分组由三个实体组成：识别码、头和有效信息，在格式中每个实体的位数也给出。

识别码和头是一个固定值，分别用 72 位和 54 位表示，有效信息可表范围从 0 到最大为 2745 位。分组也具有几种不同的类型格式。如：分组可仅由识别码组成（ 压缩格式，该方式参看本书中有关 ID 分组的内容 ），也可以是用识别码和头组成的分组，或“识别码－头－有效信息分组”。

4.2 识别码

每个分组都是用识别码作开始表示，若头信息紧随其后，则识别码长度是 72 位，否则识别码长度是 68 位。这种识别码主要用于同步、DC 补偿平衡和识别。识别码识别所有在匹克网的信道上的交换分组。在同匹克网中发送的所有分组优先相同信道识别码。在蓝牙系统接收机里，滑动相关器关联于识别码，且当超过门限电平时被激发，该激发信号被用于确定接收定时。

识别码也被用于呼出和查询过程。在这种情况下，识别码自身就被当作一个信令消息，且既不是头也不是有效信息的表示。

识别码由头、同步字或许有尾组成。如图所示：

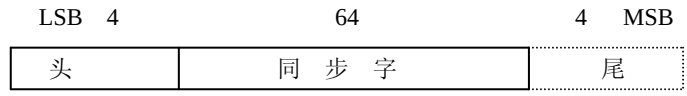


图 2.7 识别码格式

4.2.1 识别码类型

这儿描述了三种不同类型的识别码：

- 信道识别码（CAC）。
- 设备识别码（DAC）。
- 查询识别码（IAC）。

各识别码类型用在蓝牙系统中不同的操作模式中。信道识别码定义了一个匹克网。该代码包含在匹克网信道上的所有交换分组中。设备识别码用作一个特定的信令过程，如呼出或呼出响应。查询识别码有两个变量：一个称为一般查询识别码（GIAC），该查询码为所有设备公用，GIAC可用来检测在指定范围内有否其它蓝牙单元。另一个称为专用查询识别码（DIAC），该查询识别码为在蓝牙系统中具有公共属性的专用设备组使用，DIAC可以用于发现在该范围里的这些专用蓝牙单元。CAC由头、同步字和尾组成，而且它的整个长度是 72 位。当CAC是当作没有头的自包含消息使用时，则DAC和IAC就不能包含有尾且长度值是 68 位。不同识别码类型用了不同的低地址部分（LAP_S）来创建同步字，关于基带（BD）地址的LAP字段问题参看蓝牙设备的编址部分内容，这儿仅是列出了不同识别码类的概要。

表 2.2 识别码类小结

代码类	LAP	代码长度	注释
CAC	主单元	72	具体内容见识别码部分
DAC	呼入单元	68/72*	
CIAC	保留	68/72*	
DIAC	专用	68/72*	

注:“*”注释长度为 72，只能配合用于 FHS 分组。

4.2.2 头

头是一个方便用于DC补偿的固定0－1四位符号模式。该序列或是1010或是 0101，取决于下述同步字的 LSB 分别是 1 或 0。头表述格式如下：

LSB MSB LSB LSB MSB LSB

图 2.8

4.2.3 同步字

同步字是一个来自于 24 位地址（LAP）的 64 位代码字；对于CAC使用主单元的LAP，对于GIAC和DIAC、保留字、使用专用LAP；对于DAC使用从单元的LAP。基于不同的LAP_S 在同步字之间建立一个足够大的海明空间。另外，一个较好的同步字自相关特性可以改善定时同步过程。同步字的推论参见识别码的内容。

4.2.4 尾

尾同下面的识别码的数据头一样是一个附加的同步字，这是一种使用 CAC 的典型情况。但是尾也被用在 DAC 和 IAC 的情形中。此时这些代码用于在呼叫响应和查询响应过程中的 FHS 分组交换。

尾也是一个四个字符的固定模式。尾与同步字的三位MSB_S一起形成一个用于扩展DC补偿的 0，1 交替的 7 位模式，尾序列究竟是 1010 或是 0101 取决于同步字的MSB分别是 0 或 1。尾选择如图所示：

（ A ） （ B ）

图 2.9

其中（A）代表当同步字 MSB 是“0”时，CAC 中的尾；（B）代表当同步字 MSB 是“1”时，CAC 中的尾。

4.2 分组头

头包含链接控制（LC）信息并由六个字段组成。

- AM_ADDR 3 位：活动成员地址。
- TYPE 4 位：类型码。
- FLOW 1 位：流控制。
- ARQN 1 位：确认指示。
- SEQN 1 位：序列号。
- HEC 8 位：头错误校验。

包含 HEC 的整个头信息由 18 位组成，且该头信息以 1/3 比例前向纠错码编码（有关内容详见本书的纠错部分），导致头信息为 54 位编码格式。但要注意，AM_ADDR 和 TYPE 信息字段使用它们自身的 LSB 首先被发送。头其它不同字段的功能稍后再逐一解释，其头信息的格式安排如下：

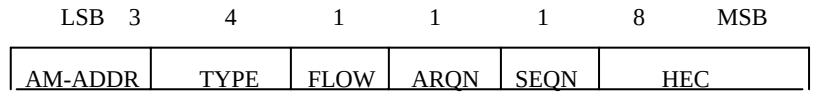


图 2.10 头格式

4.3.1 AM _ADDR

AM_ADDR 代表成员地址而且用来区分在匹克网上的不同的活动成员。在匹克网中有一个或多个从单元与主单元相连，为分别识别每个从单元，所以各个从单元在它们处于活动状态时都分配一个临时 3 位地址值。在主单元和从单元之间进行分组交换时，每个从单元都带有自身的 AM_ADDR 信息。即：在主－从分组和从－主分组里都要使用从单元的 AM_ADDR。

若主－从之间采用广播分组方式，那么保留所有的“全 0”地址。但 FHS 分组格式除外，在 FHS 分组格式中可以使用“全 0”成员地址，但它不是广播消息。从单元可以是处于脱离链接或暂时放弃它们的 AM_ADDR 状态，但当它们重新进入匹克网时，则必须重新分配新的 AM_ADDR。

4.3.1 类型

分组可以有 16 种不同类型。4 位类型码正好指出了这十六种不同类型结构。特别值得注意的是，类型码的解释取决于与分组相关的物理链接类型。首先它需要确认分组是以 SCO 链接或是以 ACL 链接发送，其次它还需要确认是以 SCO 分组或以 ACL 分组接收。同时类型码也展现了当前分组将有多少个时隙出现，这种方法使没有编址的接收设备不能在时隙的持续期间从传输信道里监听传输信息。有关各类分组的描述可见本书的有关章节内容。

4.3.1 流量

该位被用于额外 ACL 链接分组的流量控制。当以 ACL 方式链接，其接收器的 RX 缓冲区已满或 RX 正处于忙碌状态时，停止（STOP）指示（FLOW=0）将返回暂时停止数据的传输。注意，STOP 信号只涉及到 ACL 分组，分组包含链接控制信息（ID，POLL 和 NULL 分组）或仍可以接收的 SCO 分组。当 RX 缓冲区为空时，则继续（GO）指示信息（FLOW=1）将返回。当没有分组可以接收或接收头信息有错，则 GO 将以隐含的方式指示出来。

4.3.1 ARQN

普遍使用 1 位 ARQN 指示来表明使用 CRC 的有效载荷的正确传输。该确认指示可以是一个以 ACK 表示的有效确认或是一个以 NAK 表示的无

效确认。若接收是成功的，则 ACK（ARQN=1）返回，否则 NAK（ARQN=0）返回。当没有接收到涉及确认返回信息时，系统将以 NAK 形式隐含指示出来，实际上我们可将 NAK 看作是默认返回的信息。

ARQN 在返回分组头信息里稍带确认。接收正确的校验由循环冗余校验（CRC）码来校验。使用未编码的 ARQ 方式意指 ARQN 与来自同一源的最后接收到的分组有关。关于如何初始化和正确使用该信息位本书将在后面有关章节中叙述。

4.3.2 SEQN

SEQN 提供一个序列码方式来排列分组流的顺序。对每个包含使用 CRC 数据新的传输分组，SEQN 位将反相。这就要求在接收点滤出重传过程。重传过程出现是因 ACK 失败，导致收端将再重复接收一次同样的分组。通过对相邻分组的 SEQN 比较，则正确接收的重传过程就可以不考虑。SEQN 必须存在头格式里，究其原因是因为在未编码的 ARQ 方式里缺少分组编号。关于 SEQN 位的初始化及如何合理使用该信息位，本书在后面有关章节中叙述。同时有关广播分组序列方法确定也在本书后面有关章节中叙述。

4.3.3 HEC

为检测头完整性，每个头都有一个“头校验错”信息字。HEC 由一个 8 位字组成，该字由多项式 647（八进制数）生成。HEC 生成器用 8 位值进行初始化。若 FHS 分组以**主呼叫响应**状态发送，从单元使用高地址部分（UAP）。若 FHS 分组以**查询响应**方式发送，此时就使用缺省校验初始化（DCI）。在其它情况里，主设备都采用 UAP 方法。关于蓝牙系统中设备编址的定义，请参看蓝牙编址章节内容。在初始化后，HEC 形成 10 位头。在校验 HEC 之前，接收装置必须以适当的 8 位 UAP（或 DCI）来初始化 HEC 校验电路。如果 HEC 没有校验，则忽略整个分组。更详细的内容参看本书的错误校验部分。

4.4 分组类

在匹克网上使用的分组与它们使用在什么物理链接方式上有关，直到现在我们仅涉及到 SCO 和 ACL 两种链接方式。针对这两种链接方式的任一方式，都有 12 种不同类型的分组能被使用，另外四种控制分组为所有链接模式公用，它们的类型码是唯一的且与用什么链接类型方式无关。为区分链接分组上的不同分组类型，这儿采用了四位类型码不同组合来表示且将分组类分成四个字段。第一段定为四个控制分组公用所有物理链接类。第二段定为占有单时隙的分组，有六种分组类型。第三段定为占有三时隙

的分组，有两种分组类型。第四段定为占有五时隙的分组，有两种分组类型。时隙占有在分段上反映出来，而且能直接从类型码得到。以下表格形式描述了我们讨论的 SCO 和 ACL 两种链接方式分组。

表 2.3

段	类型码	占有时隙	SCO 链接	ACL 链接
1	0000	1	NULL	NULL
	0001	1	POLL	POLL
	0010	1	FHS	FHS
	0011	1	DM1	DM1
2	0100	1	未定义	DH1
	0101	1	HV1	未定义
	0110	1	HV2	未定义
	0111	1	HV3	未定义
	1000	1	DV	未定义
	1001	1	未定义	AUX1
3	1010	3	未定义	DM3
	1011	3	未定义	DH3
	1100	3	未定义	未定义
	1101	3	未定义	未定义
4	1110	5	未定义	DM5
	1111	5	未定义	DH5

4.4.1 公用分组类

共有五个公用分组，除在上表中段 1 所列的类型外，ID 分组没有列出。在这里对各个分组作出更详细的描述。

4.4.1.1 ID 分组

身份或 ID 分组由设备识别码（DAC）或查询识别码（IAC）构成，它们长度为 68 位。由于接收设备使用位环行解调电路来匹配接收分组以确认 ID 分组的位序列，所以 ID 分组是一种非常可靠的分组。为此，ID 分组常用于呼叫，查询及响应过程中。

4.4.1.2 NULL 分组

NULL 分组是没有带有效信息的分组，它仅由信道识别码和分组头组成，它的总长度（固定）为 126 位。NULL 分组用来返回链接信息给发端。用先前的传输（ARQN）是成功或当前收端 RX 缓冲区（FLOW）的状态

来说明。NULL 分组自身并不需要确认。

4.4.1.3 POLL 分组

POLL 分组非常类似于 NULL 分组，它也不带有效信息。与 NULL 分组相比，它需要一个从收端来的确认。它并不是作为 ARQ 方案的一部分。POLL 分组并不影响 ARQN 和 SEQN 字段。在 POLL 分组的收端从单元必须用一个分组来响应，该返回分组是 POLL 分组的一个隐含答复。这种分组可被用于在匹克网中主单元查询从单元的过程。在这种过程中，就是主单元没有任何信息送出，从单元也必须响应。

4.4.1.4 FHS 分组

FHS 分组一种专用控制启动分组，其中包括对蓝牙设备地址和发端时钟，有效信息包含 144 位信息并加 16 位 CRC 码。有效信息采用 2/3 比例前向纠错码，其总有效信息长度达 240 位。FHS 分组复盖一个单时隙。

FHS 有效信息及其格式如图表示：

LSB 34	24	2	2	2	6	16	24	3	26	3	MSB
奇偶位	LAP	未定义	SR	SP	UAP	NAP	设备类	AM_ADDR	CLK_{27}	呼叫扫描模式	

图 2.11

在 FHS 分组中有效信息有 11 个字段，这样 FHS 分组一般常用于呼叫主响应、查询响应和主从交换。在呼叫主响应和主从交换中，在它的响应被确认或超时超出之前，它都是一个可重复传输的分组。在查询响应中，对 FHS 分组可不必确认。FHS 分组含有实时时钟信息，时钟信息在每次重传之前被修正。它们的相同部分在每次重传过程中，FHS 有效信息的重传稍有点不同于普通有效载荷重传。

FHS 分组在匹克网信道被确定之前或当从现有的一个匹克网转到一个新的匹克网时，使用同步跳频技术。

在前一种情况里，收端若还没有被分配一个活动成员地址，此时，FHS 分组头里的 AM_ADDR 字段就设成一个全“0”。然而，FHS 分组就不再考虑作为广播分组。

在后一种情况里，在当前匹克网中从单元已有一个 AM_ADDR 时，在 FHS 分组的同步信息可以使用在下面列出 FHS 中各字段的描述。

奇偶位：34 位。该字段发送 FHS 分组主体识别码同步字第一部分的奇偶位，这些位来自于 LAP。具体内容参见本书中识别码部分内容。

LAP：24 位。该字段含有发送 FHS 分组主体的低地址部分。

未定义：2 位。该字段作为将来应用保留且被清除为“0”。

SR：2 位。该字段用来扫描重复字段和指示在两个连续扫描窗口之间

的间隔。具体内容见本书中识别码部分内容。

SP：2 位。该字段为扫描周期字段并指出在查询响应信息被传输后，命令呼叫扫描模式周期。

UAP：8 位。该字段含有发送 FHS 分组单元的高地址部分。

NAP：16 位。该字段含有发送 FHS 分组单元的非有效地址部分。

设备类：24 位。该字段含有发送 FHS 分组单元的设备类。

AM_ADDR：3 位。该字段作用为，若 FHS 分组用于呼叫建立或主－从交换时，它含有将被用作接收的成员地址。若仅发送 FHS 分组，从单元回复主单元响应或单元响应查询申请分组就含了全“0” AM_ADDR 字段。

CLK_{27-2}：26 位。该字段用于全发送FHS分组部件的本地系统时钟值。就该FHS分组识别码传输示例来说，该时钟值有 1. 25ms（两个时隙间隔）的分辨率。作为每次新的传输，该字段都被修改，所以它准确的反映了实时时钟值。

呼叫扫描模式：3 位。经发送 FHS 分组缺省指出扫描模式。呼叫扫描模式的详细定义下面将列出。这里是基本支撑一种命令扫描模式及多达三种可选扫描模式。

表 2.4　SR 字段内容

SR位格式b_1 b_0	SR 模式
00	R0
01	R1
10	R2
11	保留

表 2.5　SP 字段内容

SP位格式b_1 b_0	SP 模式
00	P0
01	P1
10	P2
11	保留

表 2.6　呼叫扫描模式字段内容

位格式b_2 b_1 b_0	呼叫扫描模式
000	命令扫描模式
001	选择扫描模式 I
010	选择扫描模式 II

011	选择扫描模式III
100	保留备用
101	保留备用
110	保留备用
111	保留备用

LAP、UAP 和 NAP 共同形成发送 FHS 分组单元的 48 位 IEEE（国际电子电气工程师协会）地址。使用奇偶位和 LAP，接收单元可直接地创建 FHS 分组发送者的信道识别码。

4.4.1.5 DM1 分组

在任何链接类型里为支撑控制信息，DM1 服务作为段 1 的部分。尽管如此，它也经常传输用户数据。由于 DM1 分组在 SCO 链接上被认可，所以它也可中断同步信息去传送控制信息。关于 DM1 分组作为 ACL 分组认可问题，可参见本书 ACL 分组内容。

4.4.2 SCO 分组

SCO 分组用于同步 SCO 链接，分组不包括循环冗余检测（CRC）码而且不允许重传。SCO 分组发送到同步 I/O（语音）端口。迄今为止有三种完整的 SCO 分组以作定义。另外，SCO 分组除含有同步话音字段外，还含有同步数据字段。SCO 分组到目前为止都主要用于 64Kb/s 话音传输。

4.4.2.1 HV1 分组

HV1 分组含有 10 个信息字节。该字节使用 1/3 比例前向纠错码保护，未使用 CRC 表示。有效载荷长度被固定在 240 位，无有效信息头。

HV分组的典型应用是传输话音，HV支持高保真话音，话音分组是不可重复传输且不需要CRC码。HV1 分组可载有 64Kb/s速率的 1.25ms话音信息，在这种情况下，HV1 分组每两个时隙（T_{SCO}=2）必须进行一次传输。

4.4.2.2 HV2 分组

HV2 分组含有 20 个信息字节。该字节使用 2/3 比例前向纠错码保护，未使用 CRC 表示。有效载荷长度被固定在 240 位，无有效信息头。

若HV2 分组用作 64Kb/s速率话音，它可载有 2.5ms的话音信息，在这种情况下，HV2 分组每四个时隙（T_{SCO} =4）必须进行一次传输。

4.4.2.3 HV3 分组

HV3 分组含有 30 个信息字节。该字节没用比例前向纠错码保护，也

未使用 CRC 表示。有效载荷长度被固定在 240 位，无有效信息头。

若HV3 分组用作 64Kb/s速率话音，它可载有 3.75ms的话音信息在这种情况下，HV3 分组每六个时隙（T_{SCO} =6）必须进行一次传输。

4.4.2.4 DV 分组

DV 分组由数据－话音分组组成。有效载荷被分成 80 位的话音字段和高达 150 位的数据字段。其格式如图所示：

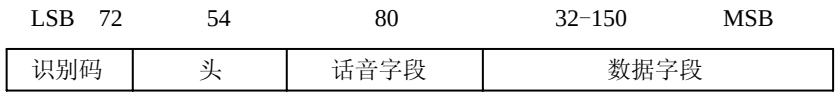


图 2.12

话音字段不由 FEC 保护，数据字段含有 10 个信息字节（包含 1 字节有效信息头）和 CRC。数据字段用 2/3 比例前向纠错码编码，必要时使用填入附加“0”的方法来保证有效信息位的总数先于比例前向纠错码前是 10 的整倍数。因 DV 分组含有同步（话音）内容，所以 DV 分组必须是以有规律的间隔进行传输，所以它在 SCO 分组类下列出。话音和数据字段完全分别处理。话音字段如一般 SCO 数据一样处理而且不允许重复传输，即：话音字段总是新的信息。数据字段可以进行错误校验的工作，必要时数据信息可重复传输。

4.4.3 ACL 分组

ACL 分组用于异步链接方式。分组内信息可以是用户数据或是控制数据，包括 DM1 分组已定义了七种 ACL 分组。ACL 分组中有六种含有 CRC 码，若非正常接收情况确认已收到时，ACL 分组可重传（执行刷新操作过程除外）。第七种分组（AUX1 分组），没有 CRC 码且不能重传。

4.4.3.1 DM1 分组

DM1 分组是一种只能带数据信息的分组。DM 是中速数据的表示。有效信息含有多到 18 个信息字节(其中一个字节是有效信息头)加 16 位 CRC 码。DM1 分组可复盖一个单时隙。有效信息加上 CRC 位用 2/3 前向比例纠错码编码，形成每 10 位信息段加上五位奇偶位。必要时，在 CRC 位后增补一些“0”来保证总数位（信息位、CRC 位和尾位）为 10 的整倍数。在 DM1 分组内的有效信息头仅一字节长，在有效信息头里的长度指示器指出了用户字节量（有效信息头和 CRC 码除外）。

4.4.3.2 DH1 分组

该分组类似于 DM1 分组。除分组里有效信息外，其余信息都没有用

FEC 编码。为此，DH1 分组可用于多达 28 个字节加 16 位 CRC 码。DH 是高速数据的表示。DH1 可以复盖单时隙。

4.4.3.2 DM3 分组

DM3 分组是一种使用扩展有效载荷的 DM1 分组。DM3 分组可复盖 3 个时隙。有效信息含有多达 123 个信息字节（其中两个字节是有效信息头）加 16 位 CRC 码。DM3 分组的有效信息头仅两字节长，在有效信息头里的长度指示器指出了用户字节量（有效信息头和 CRC 码除外）。当 DM3 分组进行发送或接收时，在三时隙持续期间，RF（射频）跳频不发生改变（第一个时隙是信道识别码传输时隙）。

4.4.3.4 DH3 分组

该分组类似于 DM3 分组。除分组里有效信息外，其余信息都没用 FEC 编码。为此，DH3 分组可含有多达 185 个信息字节（包括两字节信息头）加 16 位 CRC 码。

DH3 分组可复盖三个时隙。当 DH3 分组被发送或接收时，在三时隙持续期间，跳频不发生改变（第一个时隙是信道识别码传输时隙）。

4.4.3.5 DM5 分组

DM5 分组是一种使用扩展有效载荷的 DM1 分组。DM5 分组可复盖五个时隙。有效信息含有多达 226 个信息字节（其中两个字节是有效信息头）加 16 位 CRC 码。DM5 分组的有效信息头仅两字节长，在有效信息头里的长度指示器指出了用户字节量（有效信息头和 CRC 码除外）。当 DM5 分组进行发送或接收时，在五时隙持续期间 RF（射频）跳频不发生改变（第一个时隙是信道识别码传输时隙）。

4.4.3.6 DH5 分组

该分组类似于 DM5 分组。除分组里有效信息外，其余信息都没用 FEC 编码。为此，DH5 分组可含有多达 341 个信息字节（包括两字节信息头）加 16 位 CRC 码。

DH5 分组可复盖五个时隙。当 DH5 分组被发送或接收时，在五时隙持续期间，跳频不发生改变（第一个时隙是信道识别码传输时隙）。

4.4.3.7 AUX1 分组

该分组类似于 DM5 分组，但没有 CRC 码。AUX1 分组可含有多达 30 个信息字节（包括一字节有效信息头）。AUX1 分组可复盖单时隙。

4.5 有效信息格式

在前面的分组综述里，有几种有效信息格式需考虑。在有效信息里，有两个字段应区分：（同步）话音字段和（异步）数据字段，具有两种字段的 DV 数据段除外，其中 ACL 分组只有数据字段和 SCO 分组只有话音字段。

4.5.1 话音字段

话音字段是一个定长字段。作为 HV 分组，话音字段的长度是 240 位。作为 DV 分组，话音字段长度是 180 位 ，不带有效信息头。

4.5.2 数据字段

数据字段由三个段组成：有效信息头、有效信息主体或 CRC 码（仅 AUX1 分组不具有 CRC 码）。

1. 有效信息头

仅数据字段具有有效载荷头，该头长度是一个或两个字节。若段内是一个或两个分组，就只有一字节有效信息头，若段内有三个或四个分组，就应有两字节有效信息头。有效信息头指出了逻辑信道（两位 L_CH 表示）。逻辑信道里的控制流（一位 FLOW 表示），有效信息长度指示器（分别用五位或九位表示一字节或两字节有效信息头）。在两字节有效信息头的情况下，长度指示器有四位扩展到下一字节，第二字节的剩余四位留作备用或设置成“0”。一字节或两字节有效信息头的格式如下所示：

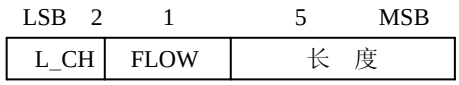


图 2.13 单时隙有效信息头格式

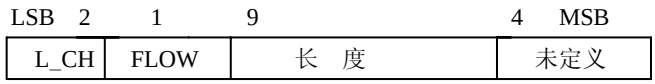


图 2.14 多时隙有效信息头格式

L_CH 字段最先传输，余后是长度字段。而下面以表格形式描述了有关 L_CH 字段的详细内容。

表 2.7 逻辑信道的 L_CH 字段内容

L_CH码b_1 b_0	逻辑信息	信息
00	NA	未定义。
01	UA/UI	L2CAP 信息的连续分段。

10	UA/UI	L2CAP 信息的开始或非分段。
11	LM	LMP 信息。

一个 L2CAP 信息可以分成几种分组段，代码 10 被用作载有这类信息第一分段的 L2CAP 分组，代码 01 用作连续分段。若没有分段，对每个分组来说都采用代码 10。代码 11 表示了 LMP 消息，代码 00 留作备用。

有效信息中的流指示器用来在 L2CAP 层控制流量。在实际应用中，它用来控制每个逻辑信道中流量。FLOW=1 表示开--流（“发送 OK“），当在 FLOW=0 时。表示关--流（“发送停止”）。在有效信息头里，流位没有严格的实时要求，最后正确接收有效信息头的流位确定了流状态，链接管理器用于响应有效信息头流位的设置及处理。

实时流控制通过链接控制器，经过分组头里的流位在分组层上执行。使用有效载荷流位，来自远程终端的通信可以受到控制。使用有效信息装入长度“0”的 ACL 分组，流位允许创建和发送。当有效信息长度为“0”时（即：在 L2CAP 分组发送过程的中间，空起始段将不发送），L2CAP 起始和连续分段指示（L_CH=10 及 L_CH=01）也保留它们的信息。使用有效载荷长度等于“0”和 L_CH=0 发送 ACL 分组总是安全的。有效载荷流位对每个逻辑信道（UA/I 或 LM）有它自己的含义。如表所示：

表 2.8 逻辑信道上有效信息头流位的使用

L_CH码b_1 b_0	ACL 有效信息头流位的用法及语义
00	无定义，备用。
01 或 10	UA/I 信道（用做发送 L2CAP 信息）流控制。
11	传输和忽略接收位上，FLOW 总被置“1”。

另外，在 LM 信道上，无流控制申请和有效信息流位总是置“1”。

除有效信息头和 CRC 码外的有效信息外（即只有有效信息主体），长度指示器指出了在有效信息里的字节数(即 8 位字)。在一字节头里的 MSB 长度字段是有效信息头里的最后（最右）位，在二字节头里的 MSB 长度字段是有效信息头里的第二字节第四位（从左数）。

2. 有效信息主体

有效信息主体包括用户主体信息和确定用户吞吐量的有效性。有效信息主体的长度由有效信息头的长度字段指出。

3. CRC 代码发生器

在有效信息里的 16 位循环冗余校验码通过 CRC—CCITT 多项式

210041（8 进制表示）产生，并以相同的方法产生 HEC。在确定 CRC 码之前，用一个 8 位值来初始化 CRC 发生器。对于在 FHS 分组里的 CRC 码，发送**主呼叫响应状态** ，使用从单元的 UAP。对于在 FHS 分组发送查询响应状态，从单元使用 DCI。而对所有其它的分组，使用主单元的 UAP。

8 个二进制数放在 LFSR 电路的 8 个不重要（最左边）的位置，而其余 8 位同时设置为“0”。其后，CRC 码安排在信息上。若 CRC 码作为附加在信息中，则 UAP（或 DCI）被忽略。在接收端的接收信息校验前，CRC 电路以相同的方法使用 8 位 UPA（DCI）被初始化。更详细的内容参看错误校验章节内容。

4.6 分组汇总

分组的汇总和其它的特征下面用三个表格描述出来，用户有效信息表示除 FEC、CRC 和有效信息头外的分组有效信息。

表 2.9 链接控制分组

类型	用户有效信息（字节）	FEC	CRC	对称最大比例	不对称最大比例
ID	Na	Na	na	na	na
NULL	Na	Na	na	na	na
POLL	Na	Na	na	na	na
FHS	18	2/3	yes	na	na

表 2.10 ACL 分组

类型	有效信息头（字节）	用户有效信息(字节)	FEC	CRC	对称最大比例(Kb/s)	非对称最大比例（Kb/s）	
						正向	反向
DM1	1	0－17	2/3	Yes	108.8	108.8	108.8
DH1	1	0－27	no	Yes	172.8	172.8	172.8
DM3	2	0－121	2/3	Yes	258.1	387.2	54.4
DH3	2	0－183	no	Yes	390.4	585.6	86.4
DH5	2	0－339	no	Yes	433.9	723.2	57.6
AUX1	1	0－29	no	No	185.6	185.6	185.6

表 2.11 SCO 分组

类型	有效信息头(字节)	用户有效信息（字节）	FEC	CRC	对称最大比例(Kb/s)
HV1	na	10	1/3	no	64.0
HV2	na	20	2/3	no	64.0
HV3	na	30	No	no	64.0

DV	1D	10+（0-9）D	2/3D	yesD	64. 0+57. 6D

在 SCO 分组中凡属具有“D”的项只涉及到数据字段。

5. 纠错

在蓝牙技术中使用了三种纠错方案：

- 1/3 比例前向纠错码。
- 2/3 比例前向纠错码。
- 用于数据的 ARQ 方案。

对数据有效信息使用 FEC 方案目的是减少重发次数。这样虽然提高了数据的可靠性，但 FEC 的采用增加了一些不必要时间开销，从而导致数据吞吐量下降。因此，分组究竟采用或不采用 FEC 码的选择，提出了在链接方式中应选用什么方式的分组问题。一般在 ACL 链接中使用 DM 和 DH 分组，而在 SCO 链接中使用 HV 分组。分组头总以 1/3 比例前向纠错码保护，它含有很重要的链接信息，能容忍多位错。

有关话音解码里的错误屏蔽和纠错测试不包含在这部分内容中，该问题将在本书的有关章节中讨论。

5.1 1/3 比例前向纠错码

这是一种较简单的纠错码格式。它在分组头里 FEC 码用一种简单的 3 倍重复格式，既重复码对每位信息重复三次来实现。其结构如图所示：

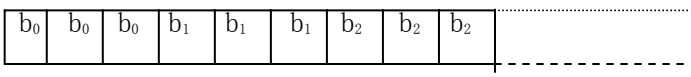
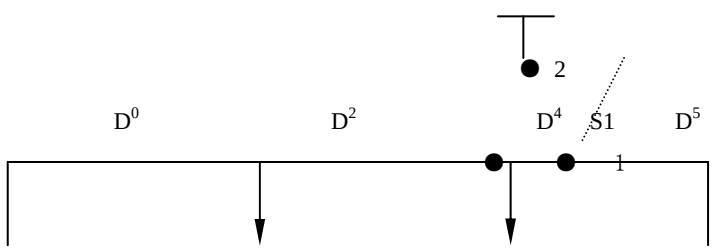


图 2.15

在整个分组头里都采用了三位重复码，同时在 HV1 分组里的话音字段也采用了这种编码格式。

5.2 2/3 比例前向纠错码

另一种FEC方案采用了一种（15，10）缩短海明码表示方式。产生的多项式为：g(D) = (D+1) (D^4+D+1)。它符合八进制数 65 表示。 线性反馈移位寄存器（LFSR）产生的这种代码如图所示：



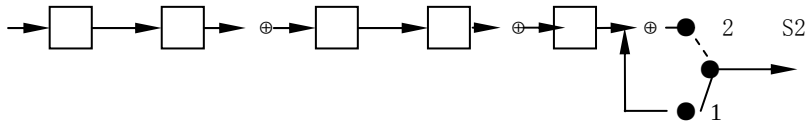


图 2.16　数据输入(先 LSB)

所有的寄存器单元在初始化时被清除为“0”。 把开关 S1 和 S2 设置在位置 1 上，10 信息位顺序地进入 LFSR。在输入完后，开关 S1 和 S2 被置于位置 2 上，五个奇偶位移出，奇偶位附加在信息位里。因此，每 10 个信息位块被编码成 15 位代码字，该代码字能在各个代码字中纠所有单错和检测所有双错。

这种 2/3 比例前向纠错码用在 DM 分组，DV 分组中的数据字段，FHS 分组和 HV2 分组中。由于编码操作采用长度为 10 的信息段，所以用“0”的尾部位可附加在 CRC 位后。整个编码的位数（即：有效信息头、用户数据、CRC 和尾部数位）必须是 10 的整倍数，于是附加在尾部的位数是最不可能达到（即：在间隔 0……9 里），这些尾部位不包含在有效信息长度指示器里。

5.3 ARQ（自动重复请求）方案

使用自动重复请求方案，DM、DH 和 DV 分组的数据字段传输或重发，直到收端（或超时执行）返回成功接收确认信息为止。该确认信息包含在返回分组头里，故称为**稍带确认法（Piggy - backing)**。为确定有效信息正确与否，循环冗余校验码就加载在有效信息中。ARQ 方案只工作在分组有效信息上（仅有效信息具有 CRC）。分组头和话音有效信息不由 ARQ 保护。

5.3.1　无编号的 ARQ

蓝牙使用快速，无编号确认方案。在响应前次接收分组的接收中返回 ACK（ARQN=1）或 NAK（ARQN=0）。从单元直接在跟随主一从时隙后的从—主时隙里响应。主单元将在下一个事件中将被编址为同一从单元来响应（即：在考虑成上次是接收来自从单元的分组和主单元响应该分组之间，主单元可编址为另一从单元）。尽管是正确接收分组，至少也需对 HEC 校验。另外，若必要时 CRC 也必须校验。

在一次新的链接开始时，它可能是呼叫、呼叫扫描、主一从切换、激活、主单元发送 POLL 分组来核对链接。在该分组里，主单元初始化 ARQN 位为**无效确认（NAK)**，而响应分组经从单元发送时，也将 ARQN 位设置成 NAK，随后的分组遵循下列规定。

ARQ 位仅受到含 CRC 和空时隙的分组影响。依据 CRC 的接收成功，ARQN 位被置成**确认（ACK)**。若在从单元里的任何接收时隙里或在主单元分组里的接收时隙流传输发现没成功的代码被检测到时，HEC 校验或

CRC 分组的 CRC 校验失败，此时 ARQN 位被置成 NAK。

如图所示：

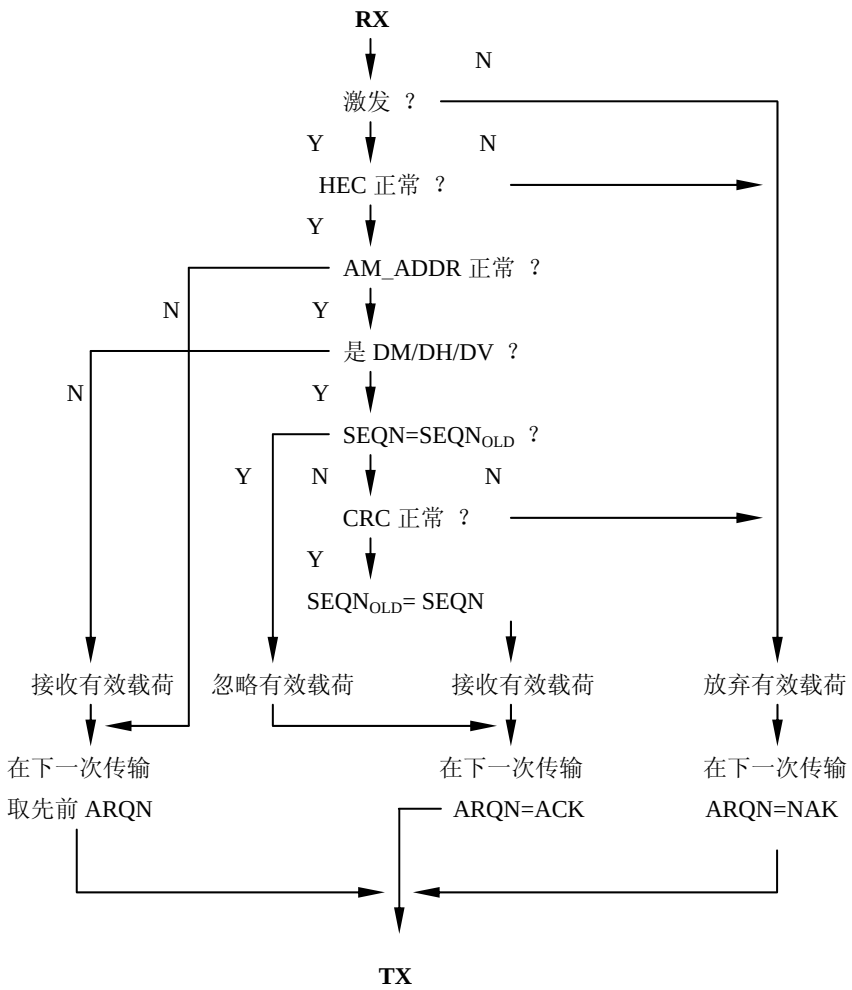


图 2.17　确定 ARQN 位接收协议

具有正确 HEC 的分组尽管被编址为其它从单元，或不同于 DH、DM 或 DV 结构的分组，皆不影响 ARQN 位。在这种情况下，ARQN 位位于左侧且作为分组最先接收。若具有正确头的 CRC 分组同先前接收的分组一样有着相同的 SEQN，则 ARQN 位被设置为 ACK，而且若没进行 CRC 校验，有效信息将不予处理。

在 FHS 分组里的 ARQ 位没有意义。在 FHS 分组里的 ARQN 位的内容不校验。

广播分组在错误使用 CRC 时被校验，但没有使用 ARQ 方案。广播分组也不需要确认。静止链接模式 HOLD（保持）和 SNIFF（呼吸）不影响

ARQ 方案，在从这类模式返回后，分组继续使用来自设置成保持/呼吸模式前的值。

5.3.2 重发过滤

在主动确认信息收到前（或超时超出），有效载荷数据一直都处于重发状态。重发是一个执行过程，它用于分组自身传输失败或因稍带确认在返回分组中传输失败（在后一种情况中，故障率较低的原因是在头中有相当多的附加代码）。在后一种情况里，收端屡次保留接收相同有效信息。在收端为过滤出重传，SEQN 位加在头里，通常每当新的 CRC 数据有效信息传输时，SEQN 位交替发生变化。在重发过程中，SEQN 位不改变，所以收端可以将当前的 SQEN 位与以前的 SQEN 位进行比较。如果比较结果不同，表明是新的信息已到达，当比较结果相同时，表明是相同有效载荷，同时收端忽略该信息。只有新的数据有效信息才能转交到链接管理器。要值得注意的是：CRC 数据有效信息只能由 DM、DH 或 DV 分组携带。

在新的链接开始时，其链接方式可以是：呼叫、呼叫扫描、主一从切换或激活、主单元发送 POLL 分组校验链接的任何一种方式，从单元以分组形式表示回答。第一个 CRC 分组的 SEQN 位（主、从两边）被置“1”，随后的分组遵循如下原则：

每当一次新的 CRC 分组发送时，SEQN 位都反相一次。CRC 分组重发时都是相同的 SEQN 值，它的改变是在 ACK 被收到或分组被刷新的情况下出现。当 ACK 收到时，SEQN 位产生反相而且新的有效信息将发送。当分组刷新时，即一个新有效信息发送，SEQN 位不必改变。然而在新分组发送前，ACK 被收到，则 SEQN 位反相。由于传输过滤，该过程防止了消息（在刷新命令已给出后）的第一个分组丢失。

在 FHS 分组里的 SEQN 位没有实际意义， 该位可以任何值发送。在 FHS 分组中的 SEQN 内容不必校验。在另外所有其它类型的分组传输期间，SEQN 位仍保持它在先前分组中的值。

在静态链接的 HOLD/SNIFF（保持/呼吸）模式不影响 SEQN 方案。在从这些状态退出后，分组继续使用在进入保持/呼吸模式前的值。

SEQN 位只由 CRC 分组影响，而 CRC 分组传输过滤如图所示：

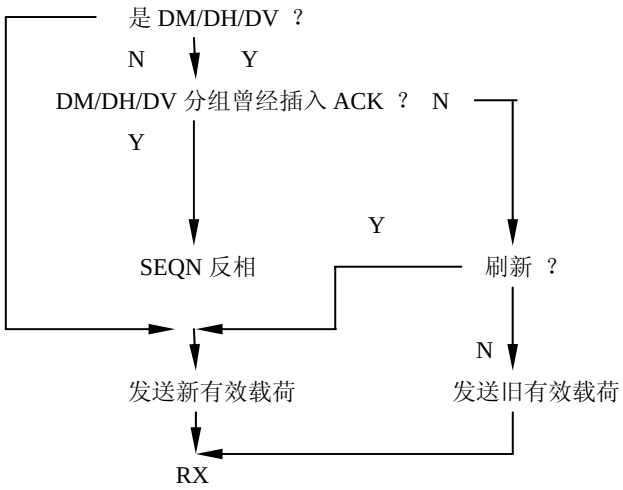


图 2.18　CRC 分组重发过滤

5.3.3　有效信息刷新

由于重发的插入确保了数据准确转接，所以在通话流里 ARQ 方案能引起可变延迟。一旦通信链接方式确定，只能是有限量的延迟是允许的，所以重传被定为：当前的有效信息应忽略，而下一个有效信息必须考虑的一种限制。

另外。数据转接作为等时通信被指出，它意指为继续下一个数据有效信息，重传过程必须中止。中止重传过程是通过刷新旧数据和强迫蓝牙控制器取下一个更换数据。

刷新导致逻辑链接控制和适配协议（L2CAP）消息的剩余部分的损耗，因此分组流刷新有一个 L_CH（逻辑信道）=10 的起始分组指示，该指示放入作为下个 L2CAP 消息的有效信息头里，它说明了刷新的目的，同时刷新不会改变 SEQN 位值。

5. 3. 4　多—从单元考虑

在具有多个从单元的匹克网情况里，主单元独立于各个从单元执行 ARQ 协议。

5.3.5　广播分组

广播分组是通过主单元同时将分组传送给所有从单元的方式。广播分组是通过全“0”的激活成员地址（AM_ADDR）指出，广播分组不需确认（至少不在 LC 层上）。但需注意 FHS 分组是一个可以全“0”地址编码而不是广播分组的唯一的一种分组。

由于广播分组不需确认，所以每次广播分组可以重复发送次数为一固

定值。在下一次广播相同消息的广播数据重复以前，广播分组重复N_{BC}次。

重复广播方案如图所示：

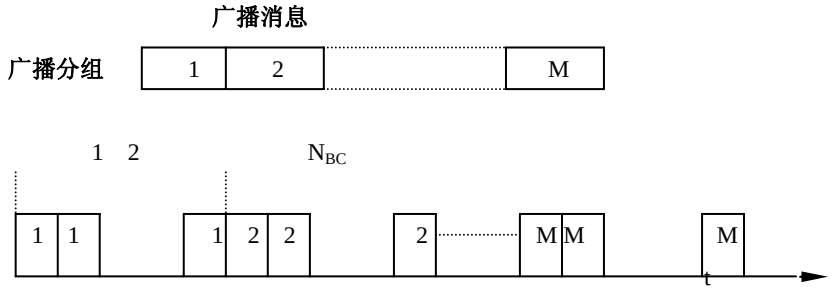


图 2.19 广播重复方案

使用 CRC 的广播分组有它自身的序号。使用 CRC 的第一次广播分组的 SEQN 由主单元置 SEQN=1，此后每次用 CRC 的新分组，都使 SEQN 反相，不用 CRC 的广播分组不影响序号。从单元接收第一个广播分组的 SEQN 时，并且在接收链接中校验下一广播分组中 SEQN 的变化。因广播消息没有确认而且无结束标志指示，所以正确地接收起始分组显得尤其重要。为确保这点，凡是 L2CAP 起始分组和链接管理协议（LMP）分组的广播分组的副本将不滤出，这类分组由在有效信息头里 L_CH=1X 指出，只有 L2CAP 连续分组的副本要被滤出。

5.4 错误校验

利用信道识别码头里的 HEC 及有效信息中的 CRC，我们可以校验分组错或传输错。在接收分组时，首先校验识别码。由于在信道识别码中的 64 位同步字源自于 24 位主单元的低地址部分（LAP），如果 LAP 的这种校验是正确的，那么可防止接收来自其它匹克网的分组。

HEC 和 CRC 用来检测数据错及地址错，为此对地址空间增加了八位来表示。高地址部分（UAP）通常被包含在 HEC 和 CRC 检测中，甚至具有相同识别码的分组（即：具有相同 LAP 和不同 UAP 设备的识别码）也必须通过识别码测试。当 UAP 位不匹配时，在 HEC 和 CRC 测试后，分组将被放弃。有一种情况例外，就是在收发两端没有公共的 UAP 是可用的，当 HEC 和 CRC 在查询响应状态作为 FHS 分组产生时，此时使用默认检测初始化（DCI）值，DCI 以 0X00（十六进制）定义。

在计算 HEC 和 CRC 之前，HEC / CRC 发生器中的移位寄存器用 8 位 UAP（或 DCI）值初始化，则头和有效载荷信息分别（先 LSB）移入 HEC 和 CRC 发生器。

HEC 和 CRC 的产生及检测用图表示如下：

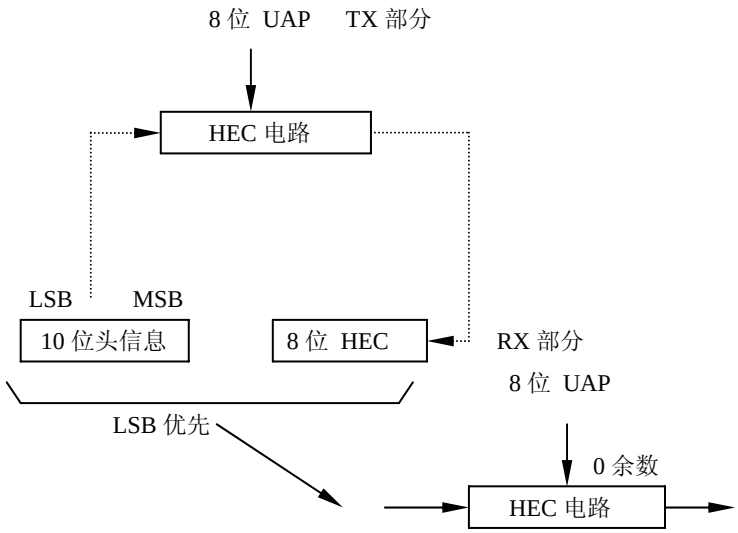


图 2.20 HEC 发生器和检测

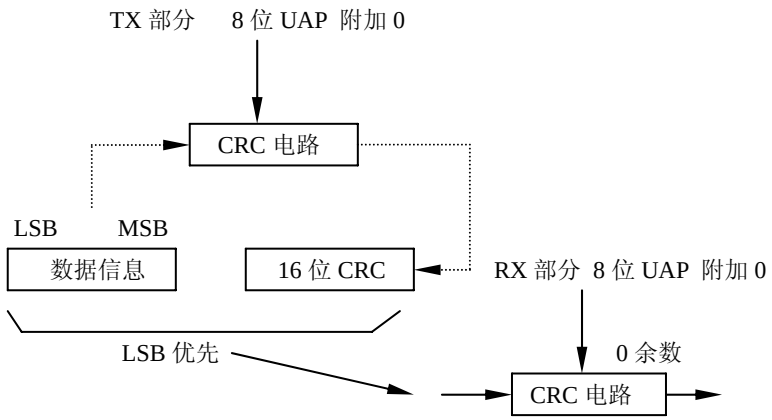


图 2.21 CRC 发生器和检测

HEC 产生 LFSR 过程如图描述：

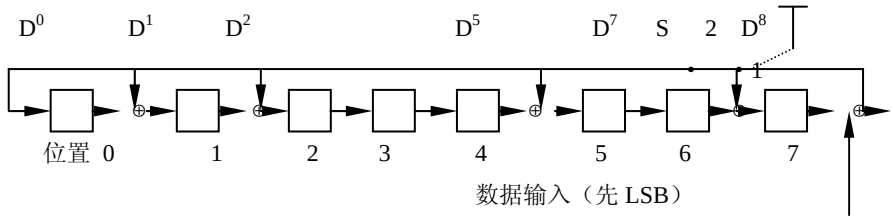


图 2.22　HEC 产生 LFSR 电路

在以上过程中将产生一个多项式为：

$$g(D) = (D+1)(D^7+D^4+D^3+D^2+1) = D^8+D^7+D^5+D^2+D+1。$$

初始化该电路的方法是使用先装入的八位UAP标志UAP_0进入最左的移位寄存器单元，而UAP_7进入最右单元。HEC LFSR的初始化状态用图表示如下：

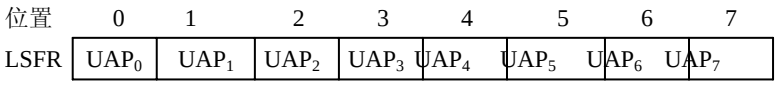


图 2.23　HEC 发生器电路的初始化状态

数据移入设置在位置 1 上的开关 S，当最后一个数据位已进入 LFSR，开关 S 被设置在位置 2 且 HEC 可以在寄存器中读出。LFSR 位从右到左被读出（即：位置 7 的位首先被传输，仅随其后是在位置 6 上位等）。

作为 CRC 的 16 位 LSFR 同样使用 CRC-CCITT 来创建并产生多项式：

$$g(D) = D^{16}+D^{12}+D^5+1。$$

如图所示：

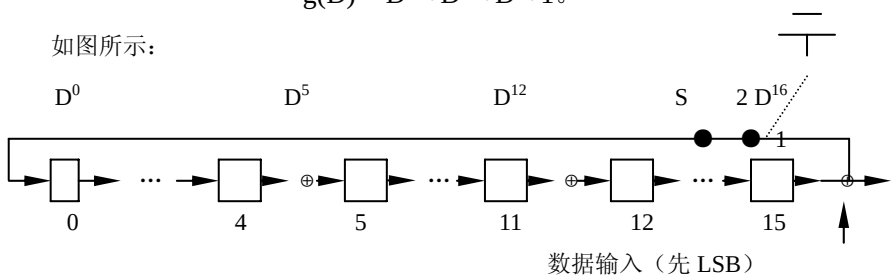


图 2.24　产生 CRC 的 LFSR 电路

对于这种情况，最左边八位被设置成“0”，16 位 LFSR 的初始化状态如图所示：

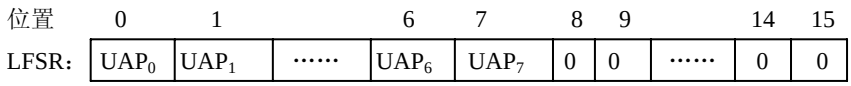


图 2.25　CRC 发生器电路的初始化状态

当数据被移入时，开关 S 设置在位置 1，在最后一位进入 LSFR 后，

开关 S 被设置在位置 2，寄存器内容从右往左被传输（即：开始用位置 15，然后是位置 14 等）。

6．逻辑信道

在蓝牙系统中规定了五种逻辑信道：

- 链接控制器（LC）控制信道。
- 链接管理器（LM）控制信道。
- UA 用户信道
- UI 用户信道
- US 用户信道

控制信道 LC 和 LM 分别用在链接控制层和链接管理层，UA、UI 和 US 用户信道分别用于异步、等时和同步用户信息。LC 信道传送分组头，而其它的信道传送分组有效信息。 LM、UA 和 UI 信道在有效信息头里的 L_CH 字段标出。US 信道只经 SCO 链接传输，UA 和 UI 信道一般经 ACL 链接传输。然而它们也能在 SCO 链接上以 DV 分组里的数据传送，LM 信道既可以用 SCO 链接传送也可用 ACL 链接传送。

6.1 LC 信道（链接控制）

LC 控制信道映射到分组头上，该信道传送类似于 ARQ、流控制和有效信息特征的低层链接控制信息。没有分组头的 ID 分组除外，LC 信道可传送各种分组。

6.2 LM 信道（链接管理）

LM 控制信道用来传送主单元和从单元链接管理器之间的互换控制信息。典型的 LM 信道使用 DM 分组保护模式，LM 信道经在有效信息头里 L_CH 代码 11 指定。

6.3 UA/UI 信道（用户异步/等时数据）

UA 信道传送 L2CAP 表示的异步用户数据，该数据可以用一个和多个基带分组传送。对于分段消息，在起始分组使用有效信息头的 10L_CH 代码，余下的连续分组使用 L_CH 代码 01，如果没有使用分段消息，所有的分组都使用 L2CAP 开始代码 10。

等时数据信道由高层正确定时开始分组支持。在基带层里，L_CH 代码用法同 UA 信道一样。

6.4 US 信道（用户同步数据）

US 信道传送明显表示的同步用户数据，该信道在 SCO 链接上执行。

6.5 信道映射

LC 信道被映射到分组头上。所有其它的信道被映射到有效信息上。US 信道只能映射到 SCO 分组，而所有其它的信道映射到 ACL 分组或 SCO DV 分组。如果涉及到较高优先权信息，LM、UA 和 UI 信道可以中断 US 信道。

5. 数据加噪

在传输之前，头和有效信息使用数据噪声字加扰，其目的使用来自较高冗余模式随机码去最小化在分组里的 DC 位移。这种加扰过程先于 FEC 编码完成。

在收端，接收数据也使用相同噪声字发生器进行解扰，解扰过程在 FEC 解码后完成。

噪声字利用多项式$g(D) = D^7+D^4+1$（即八进制数 221）使用头和有效信息的异或操作（EXORed）紧随其后。噪声字使用线性反馈移位寄存器产生。

如图所示：

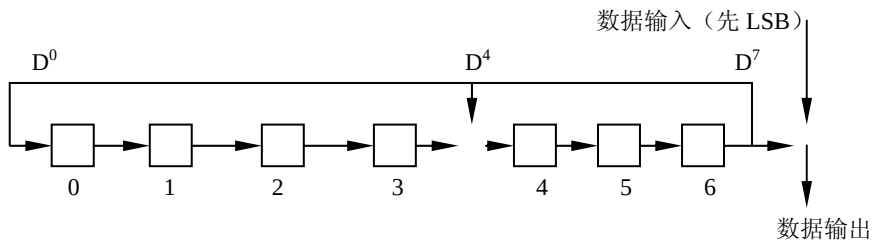


图 2.26 数据加噪 LFSR

在每次传输前，移位寄存器都使用主蓝牙时钟的一部分如CLK_{6-1}来初始化，用MSB的值 1 来扩充。该初始化用CLK_1 写入位置 0，用CLK_2 写入位置 1 等方式来执行。形成跳频采集期间FHS 分组发送除外，噪声寄存器的初始化执行方式都不同。代替主时钟的X—输入用于查询或呼叫响应（取决于当前状态）常规方式，具体内容分别见后续有关 79 跳和 23 跳系统的表格所示。在 79 跳系统情况下，5 位值用两个值 1 的MSB_S扩展，在 23 跳系统情况下，4 位值用 3 位扩展，两个MSB_S 置成 1，而第三个最重要的位置“0”。在寄存器初始化期间，LSB的X（即：X_0）位置写成 “0”，

X_1位置写成 “1”等。

初始化后，数据头和有效信息（包含 CRC）被加扰，有效信息噪声仍取自 FEC 结束的 FFSR 的噪声状态。在分组和有效信息之间不存在移位寄存器上有二次初始化问题。“Data In”序列的第一位是分组头的最低位（LSB）。

6. 收/发例行测试

为支持 ACL 及 SCO 链接的通信，该节描述了前面所述的分组使用方法，作为单从单元及多从单元两种链接方式的考虑，另外对使用 TX 及 RX 缓冲区的常规方法也作了说明。

下面内容中对 TX 和 RX 常规使用方法描述仅是一种格式特征，而最终执行结果可以是不同的。

8.1 TX 例行测试

对各种 ACL 链接和各种 SCO 链接，TX 常用方法是不同的。TX 常规用法中 ACL 和 SCO 缓冲区的使用如图所示：

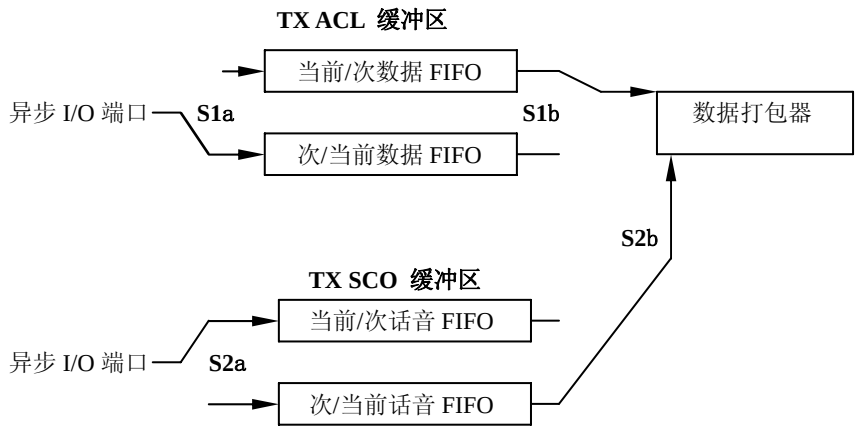


图 2.27 TX 缓冲区的功能图

在图中都是用单 TX ACL 缓冲区和单 TX SCO 缓冲区来描述。在主单元中，对每个从单元都分别有一个 TX ACL 缓冲区。另外，对每个 SCO 从单元（不同的 SCO 链接可以公用相同的 TX SCO 缓冲区或各自带有的

独立的T X SCO 缓冲区）可以有一个或多个 TX SCO 缓冲区，每个 TX SCO 缓冲区由两个 FIFO（先进先出）寄存器组成。为构成分组，由蓝牙控制器识别和读出的寄存器成为**现态寄存器**，而由蓝牙链接管理器识别和装入新信息的寄存器称为**次态寄存器**。开关 S1 和 S2 的位置确立了是现态寄存器或次态寄存器，开关由蓝牙链接控制器控制，在 FIFO 寄存器里输入和输出的开关决不会同时和同一寄存器相连。

公用在 ACL 和 SCO 链接（ID、NULL、POLL、FHS、DM1）分组中，只有 DM1 分组带有可在链接控制器和链接管理器之间可交换的有效信息，该公用分组获得了对 ACL 缓冲区的使用。话音部分由 SCO 缓冲区处理且数据部分由 ACL 缓冲区处理的 DV 分组除外，所有 ACL 分组获得 ACL 缓冲区的使用，所有 SCO 分组获得 SCO 缓冲区使用。在下一节里，将展开对 ACL 通信、SCO 通信和在 SCO 链接上的组合数据—话音通信的操作讨论。

8.1.1 ACL 通信

在纯（异步）数据情况下，只有 TX ACL 缓冲区必须考虑。在此时，只有 DM 和 DH 分组可以使用且它们具有不同长度值，分组长度在有效信息头里指出，究竟选用高速数据或中速数据取决于链接的质量。当链接质量较好时，在数据有效信息里的 FEC 可以忽略，导致 DM 形成 DH 分组，否则只能用 DM 分组。

在纯数据通信里的默认 TYPE 是 NULL，它意指在没有数据传输（数据通信是异步的且在没有效载荷时出现暂停状态）或没有从单元需 POLL 时，为发送链接控制信息到其它蓝牙单元（举例来说作为接收数据的 ACK/STOP 信息），此时插入 NULL 分组发送过程。当链接控制信息无效时（无须确认或不必停止 RX 流），则完全没有分组发送。

TX 常规工作方法如下所述：

蓝牙链接管理器装入新数据在开关 S1a 位置上的寄存器，紧接着给出刷新命令到蓝牙链接控制器，该链接控制器强迫开关 S1 发生改变（S1a 和 S1b 开关同时执行）。当需发送有效信息时，分组打包器读当前寄存器（取决于分组类）并建立一个附加在信道识别码和头上的有效信息，并随后被传输。在该响应分组里（如果涉及到主单元传输是在下一个 RX 时隙到达，则涉及到从单元传输，它可能被推迟到以后的 RX 时隙）应将传输的结果返回。在 ACX 情况里，开关 S1 应改变位置；如果 NAK（明显或隐含）插入接收，开关 S1 就不改变位置。在这种情况下，相同的有效信息在下一个 TX 时机完成重传。

只要链接管理器保证新信息装入寄存器，蓝牙链接控制器将自动地传输有效信息。另外，重发过程在错误情况下自动实施。当没有新信息装入

时，链接控制器将发送 NULL 或什么都不作。如果没有新信息装入在次态寄存器里，在最后一个传输期间，当最后传输被确认后且次态寄存器变成现态寄存器时，分组打包器指向空寄存器。如果新数据就装在次态寄存器里，刷新命令要求转换 S1 开关到适当的寄存器。在各个 TX 时隙之前，只要链接管理器持续装入数据和类型寄存器，则数据就由链接控制器自动地处理。这是因 S1 开关，在响应时由接收的 ACK 信息来控制。然而如果来自于链接管理器的通信曾经被中断过而且默认分组插入发送，刷新命令要求继续在链接控制器里流动。

刷新命令也可以用于限时（等时）数据情况。在链接较差的情况里，多次重传是必要的。在一个确定的应用中，数据应是限时的。如果因链接错导致有效信息在整个时间都是重发，其有效载荷可能成为过时数据，且此时系统可能决定使用最近的数据来代替原数据同时跳过该有效信息，这也由刷新命令来完成。当刷新时，开关 S1 被强迫改变且链接控制器强迫考虑下一数据有效信息并取消 ACK 控制。

8.1.2 SCO 通信

在SCO链接方式下，我们只用了HV分组类，同步端连续的装入数据到SCO缓冲区中的次态寄存器，S2 开关遵循 T_{SCO} 间隔变化，该 T_{SCO} 间隔是在以SCO链接时间被确定的主单元和从单元之间进行处理。

对每个新的 SCO 时隙，在 S2 开关发生改变后，分组打包器从现态寄存器读出数据。如果在 SCO 时隙里，主单元和 SCO 认为从单元之间或主单元和其它的从单元之间为发送涉及到控制分组较高优先权的控制信息时， 分组打包器将放弃 SCO 信息并用控制信息插入，该控制信息必须在 DM1 分组里发送。在使用 DV 或 DM1 分组的主单元和 SCO 从单元之间，数据或链接控制信息也能相互交换。

任何分组的 ACL 类都能用于发送数据或链接控制信息给其它的 ACL 从单元。

8.1.3 数据一话音混合通信

DV 分组前面已说明可以在 SCO 链接中同时使用数据和话音。当 TYPE 是 DV 时，链接控制器读数据寄存器去填充数据字段和话音寄存器去填充话音字段，其后开关 2 被改变。然而 S1 的位置取决于类似于 ACL 链接上的传输结果。如果 ACK 被接收到，则 S1 开关改变位置。

在各个 DV 分组里，话音信息总是新的。但数据信息因前面传输失败，它可能还因重发而保留原数据。如果没有数据发送，在数据一话音混合传输之前，SCO 链接自动地从 DV 分组变成当前 HV 分组类使用。

注意：当数据流被中断而且新数据到达时，必须使用刷新命令。

如果在信道吞吐量容忍的情况下，组合数据一话音传输（除 SCO 链接外），也能单独使用 ACL 链接来实现。

8.1.4 默认分组类

在 ACL 链接上，主和从单元中的默认类都是 NULL。它意指没有用户信息需要发送，或具有 ACK 或 STOP 信息的 NULL 分组发送，或完全没有分组发送。NULL 分组可通过主单元分配给下个从一主时隙到一确定从单元（即一个编址） 来使用。一般情况下，从单元可以不必强制响应来自于主单元的 NULL 分组。如果主单元要求响应，它必须发送一个 POLL 分组。

当 SCO 链接确立时，SCO 分组类在 LM 层上处理，对 SCO 链接来说认可的分组也是一个默认分组类。

8.2 RX 例行测试

RX 常规用法分别为 ACL 链接和 SCO 链接使用。与主单元 TX ACL 缓冲区相比，单个 RX 缓冲区分在所有从单元中。作为 SCO 缓冲区来讲，它随 SCO 链接方式不同来区分外部 SCO 缓冲区需要否。下图描述了 RX 常规用法中 ACL 和 SCO 缓冲区的使用。

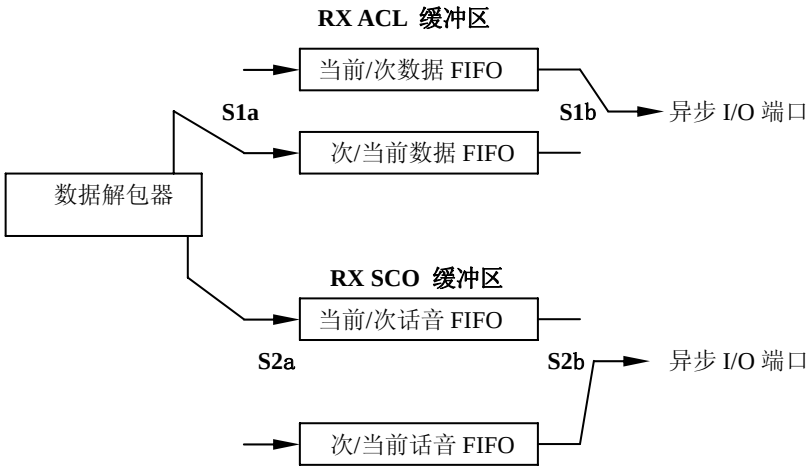


图 2.28 RX 缓冲区功能图

RX ACL 缓冲区由两个 FIFO 寄存器组成。一个寄存器经蓝牙链接控制器用来识别和装入最近的 RX 分组的有效信息，另一个寄存器经蓝牙链接管理器识别来读出先前的有效信息。RX SCO 缓冲区也由两个 FIFO 寄存器组成，一个寄存器由新到的话音信息填入，而另一个寄存器由处理单元读出。

由于接收的分组头有 TYPE 指示器，它指出了有效信息是否含有数据

与话音、数据或话音信息。分组解包器能直接自动地与特有缓冲区通信，链接管理器每读一次旧的寄存器，开关 S1 就改变一次。如果在 RX 寄存器为空前，下一个有效信息到达，STOP 指示必须在返回的下一个 TX 分组的分组头里。只要 RX 寄存器一旦空闲，STOP 指示就再次移走。SEQN 字段在新的 ACL 有效信息被存入 ACL 寄存器前被校验（在 L_CH 里的刷新指示和广播消息影响 SEQN 字段的译码）。

每个T_{SCO} 都将改变S2 开关。有时由于头的错误，尽管没有新的话音信息到达，开关仍将发生改变。为保证正确话音部分，话音处理单元能处理话音信号。

8.3 流控制

流控制用来解决新的有效信息到达对 RX ACL 缓冲区添满问题。如前所述，在返回 TX 分组里的头字段 FLOW 用 STOP 或 GO 来控制新数据传输。

8.3.1 收端控制

只要数据不能接收，STOP 指示由链接控制器自动将它插入返回有效信息头里进行传输。只要 RX ACL 缓冲区不为空，STOP 由链接管理器返回。当新的数据可以再次接收时，GO 指示返回。GO 是一个系统默认值。

注意：所有分组类不包含一直可以被接收的数据。例如话音通信不受流控制影响，同时也要注意，虽然蓝牙单元不能接收新数据，但它仍能传输信息。流控制就是用来区分各种用法说明。

8.3.2 发端控制

在 STOP 信号接收上，链接控制器将自动地切换到默认分组类。当前，TX ACL 缓冲区状态冻结。只要一收到 STOP 指示，则默认分组就被发送。当没有分组收到时，就假设 GO 隐含。

注意：默认分组含有对接收方来讲（它可以一直开启）的链接控制信息和话音（HV 分组）。当 GO 指示收到时，链接控制器当作当前在 TX ACL 缓冲区里重新传输数据。

在多从结构里，只有发出 STOP 信号的从单元停止传输。这就说明以前讨论的在主单元的常规用法中涉及到的 TX ACL 缓冲区，该缓冲区符合不能瞬间接收数据的从单元。

8.4 比特流处理

在使用无线接口发送信息之前，为增加发送信息的可靠性和安全性，几个位处理需在发端完成。对分组头要增加 HEC ，头位用噪声字加扰及

使用 FEC 编码。在收端，执行过程相反。

下面用图来描述收—发两端分组头的执行过程情况：在处理过程中两端的所有头位处理过程必须遵循。

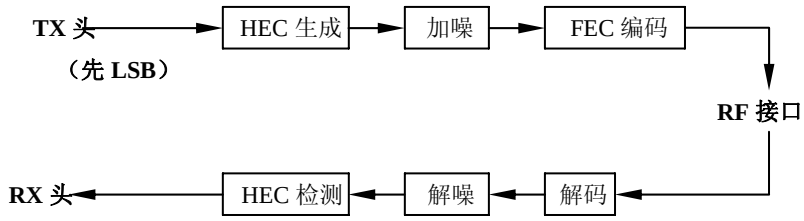


图 2.29 头位处理过程

对有效信息来讲，类似的过程一样被执行，但执行过程中还要取决于分组类。

其执行过程如图所示：

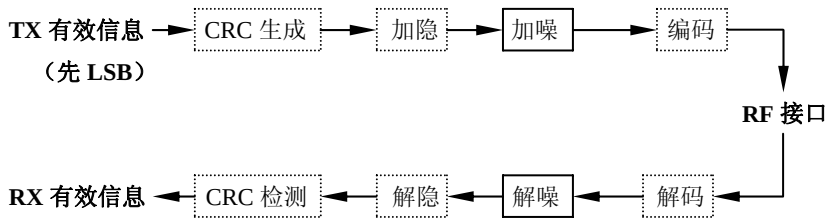


图 2.30 有效信息位处理过程

另外，过程定义了分组头，加密用于有效信息，只有加噪和解噪为每个有效信息必须强制执行。其它所有的过程选择取决于分组类和激活模式，图中凡属选择过程皆用虚线描出。

9 发 / 收定时

蓝牙发射机用于分时双工（TDD）方案。这表明了在蓝牙技术中同步收发交替方式。蓝牙单元使用什么样的 TDD 定时方案取决于蓝牙单元的模式。

在常规链接模式里，主发射机总是用偶数时隙（主 CLK1=0）作为起始，而从发射机总是采用奇数时隙（主 CLK1=1）来作为起始。因分组类复盖多个单时隙，主发射机可能持续在奇数时隙里，而从发射机可能持续在偶数时隙里。

在本节内容中全部定时图示基于在天线里的信号，术语“精确”用在定时描述涉及到理想传输或接收时，在这种条件下是忽略了微小定时偏差

和不完整的时钟频率。

主分组发送的平均定时不能偏差快于相对于 625μs的理想时隙定时的20ppm，瞬间定时不能偏差大于来自于平均定时的 1μs。于是分组时隙边界 k 的传输绝对定时值t_k 必须满足等式。

$$t_k = \left(\sum_{i=1}^{k} (1+d_i) \right) T_N + j_k + offset,$$

在等式中，T_N是一个标称时隙长度（625μs），j_k指出在时隙K里的抖动（$|j_k| \leq 1\mu s$），而d_k指出在时隙K的偏差（$|d_k| \leq 20ppm$）。在给定的各时隙限制里，抖动偏差是非常随机的。而“offset”是一种随机且固定常量，对于活动、休眠和呼吸模式，偏差和抖动参数将在后面的链接管理协议内容中具体说明。

9.1 主 / 从定时同步

匹克网（Piconet）由主单元的系统时钟同步，在匹克网的存在期间，主单元决不会调整它的系统时钟。在连续传输期间，它维持 M x 625 μs 的准确间隔（此处 M 是一个大于 0 的正整数同时也是一个偶数）。为匹配主时钟，从单元使用定时补偿来适合它们自身的时钟值，这种定时补偿在每完成一次从主单元接收分组后就得修改。通过用接收分组的精确 RX 定时值与估计 RX 定时值相比，从单元都能正确地补偿任何定时失调。注意：由于从单元只有信道识别码要求同步，所以，从单元 RX 定时可以用任何主一从时隙发送的分组来修改。

从单元 TX 定时基于最近从单元 RX 定时，RX 定时又基于在主一从时隙期间最后一次正确触发。作为 ACL 链接来讲，该触发在主一从时隙里必须发生，而且要先于当前从传输。对 SCO 链接来讲，在从单元允许发送一个 SCO 分组，甚至如果先于前主一从时隙没有接收到数据前，触发可以在几个主一从时隙里发生。只要定时不匹配值被保持在不稳定期±10 μs 内，从单元就可以接收分组和调整 RX 定时。

主单元 TX 定时严格地依照主时钟确定，主单元维持 M x 1250μs 准确间隔（此处 M 是一个大于 0 的正整数）。在连续传输启动开始之间，RX 定时基于用准确地 N x 625 μs 移位（此处 N 为奇数且是一个大于 0 的正整数）的这个 TX 定时。

在主单元 RX 周期中，主单元也使用±10 μs 误差间隔来允许从单元的失调，主单元将据慎重考虑后分组的 RX 处理过程来调整。但对于随后的 TX 和 RX 周期，主单元将不再调整它的 RX/TX 定时。定时行为可稍有差异，这取决于单元的当前状态。

9.2 联机状态

在蓝牙联机模式里，收、发信机的发送和接收过程是交替进行的。其运行模式以下两图来分别说明。

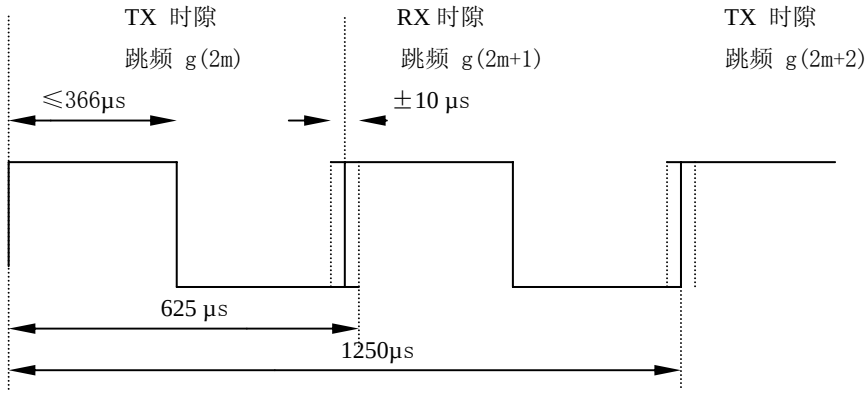


图 2. 31 在单时隙有效信息标准模式里蓝牙主收发信机的 RX/TX 周期

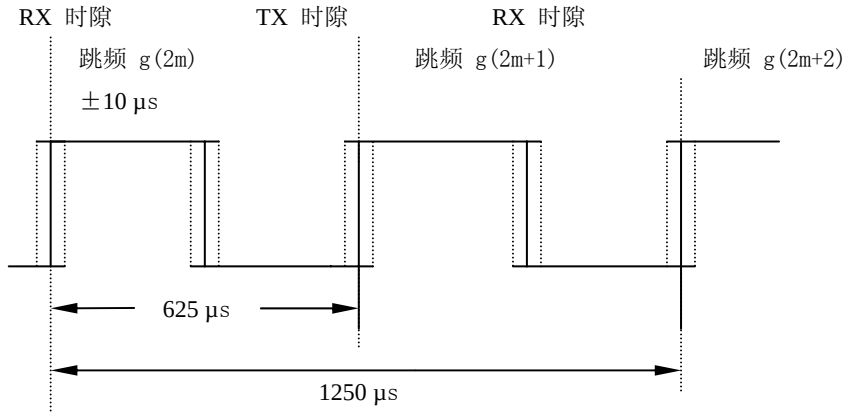


图 2.32 在单时隙有效信息标准模式里蓝牙从收发信机的 RX/TX 周期

在这两个图中都是用单时隙分组来举例说明。在收、发过程中，每次 RX 和 TX 传输都以不同的跳频点来实现，并且传输过程取决于分组类和有效信息长度。分组量值可达 366μs。对多时隙分组来说，同一分组可能复盖 n 个时隙，因此第一个时隙的跳频将用在整个传输过程中。

在本节内容的图中所表示的 f(k)为呼叫跳顺序的频率，f′(k)表示相应呼叫响应顺序频率。g(m)指出了跳频信道。在传输后，在 TX 上升沿的起始点处，返回分组期望为 N x 625 μs，此处的 N 是一个奇数且为正整数，N 取决于传输分组的类型。为允许有些时间误差，不稳定期与准确接收定时偏差很小。在正常操作中，时隙不稳定期宽度为 20μs，这就是说允许

RX 上升沿可提前早到 10μs 或延后推迟晚到 10μs。在 RX 开始的周期中，识别相关器搜索在不稳定期间上的当前信号识别码。如果没有激发事件产生，接收机进入休眠状态直到下一次 RX 事件发生。如果在搜索中，相互输出关系决不会超出最终限值的情况日趋明显时，接收机可以提前进入休眠转态。如触发事件一旦产生，接收机就被打开而进入准备接收剩余信息的状态。

当前主单元传输基于先前的主单元传输，在前主单元 TX 上升沿开始处，预定为 M x 1250 μs， 此处的 M 取决于传输和接收分组类。注意，主单元 TX 定时不会受从单元的时间偏移所影响。如果在若干连续时隙期间没有传输过程发生，主单元将取最后一次 TX 上升沿的 TX 定时作为基准。

从单元传输预定为 N x 625 μs。以从单元的 RX 上升沿开始后算，若从单元的 RX 定时发生漂移，结果将导致从单元 TX 定时。如果在若干连续时隙期间没有接收产生，从单元将取最后一次 RX 上升沿的 RX 定时作为基准。

9.3 退出保持模式

在联机状态里，蓝牙单元可以工作在保持模式中。此时，蓝牙的收、发信机既不发送信息也不接收信息。当返回到正常操作时，蓝牙单元退出保持模式后，从单元必须在可以发送信息之前听命于主单元。

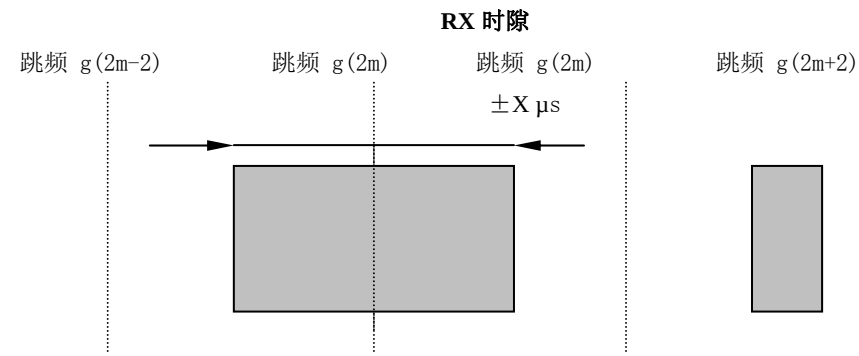
在这种情况里，从单元里的搜索不稳定期可以从±10 μs 增加到较大值 X μs。我们在此用一个图的描述来说明这个问题。

注意：该图仅用于 RX 跳频中，若用于主一从（RX）时隙的跳频也用在不稳定期，并可以扩展到常用于从一主（TX）时隙的前述时间间隔。

如果搜索不稳定期超过 625 μs，连续空间将不在 RX 跳频的开始处：g(2m)，g(2m+2) …… g(2m+2i)（此处“i ”是一个整数）；g(2m)，g(2m+4) …… g(2m+4i)； 甚至 g(2m)， g(2m+6) …… g(2m+6i)等的中心点上。为避免搜索不稳定期迭加，RX 跳频使用符合 RX 时隙数。

单时隙分组用于从保持模式返回的最小同步时间只是一种推荐性意见，尤其在长期的保持模式后，要求搜索不稳定期超过 625 μs。

主 TX 的评估状态



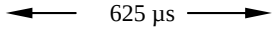


图 2.33　从单元从保持模式中返回 RX 定时

9.4 唤醒休眠状态

休眠模式类似于保持模式。休眠从单元定期地由主单元或要求同步的时钟补偿来唤醒。如从保持模式返回相似，休眠从单元唤醒是可以将搜索不稳定期从±10 µs 增加到较大值 X µs。其关系表现在从单元从保持模式返回的 RX 定时图中。

9.5 呼叫状态

在呼叫状态里，主传输设备识别码（ID 分组）应与链接的从设备相符。因 ID 分组是一个很短的分组，而跳频速率可以从 1600 跳/s 增加到 3200 跳/s。所以跳频差异是相当大的。在单 TX 时隙间隔里，呼出主单元传输在两个不同跳频点上。在单 RX 时隙间隔里，呼出收、发信机在这两个不同跳频点监听。

在 TX 时隙期间，呼出单元以 TX 跳频 f(k)和 f（k+1)发送一个 ID 分组。在 RX 时隙里，它遵循 RX 跳频 f′（k)和 f′（k+1)的响应。在收到符合呼出分组后，侦听周期精确定时为 625 µs，其中包括±10 µs 不稳定期。

如下图所示：

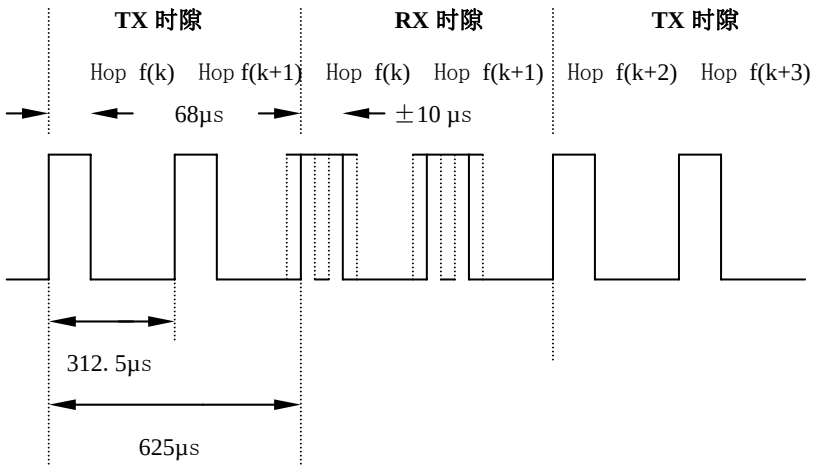


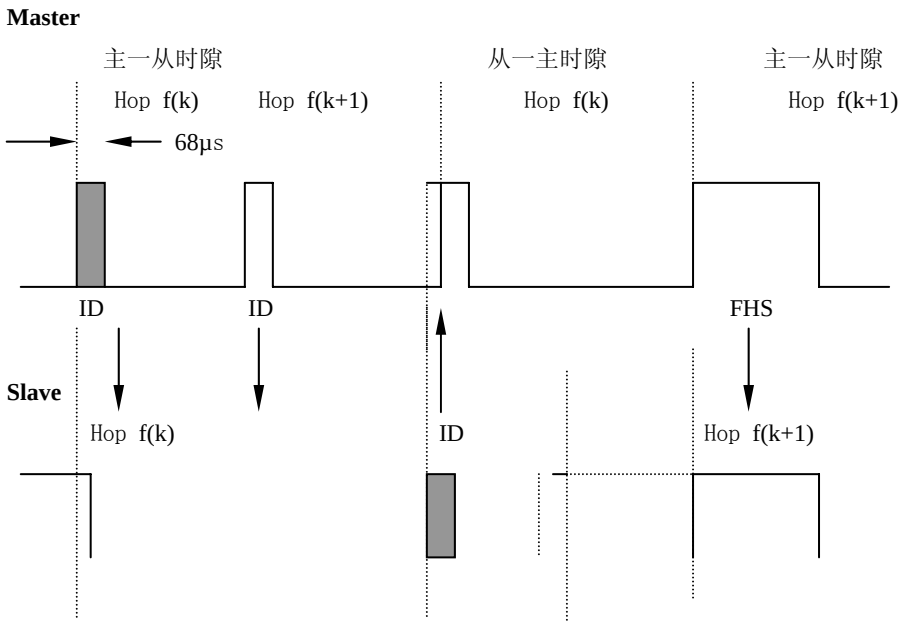
图 2.34 呼叫模式蓝牙收发信机的 RX/TX 周期

9.6 FHS 分组

在链接建立和主一从交换期间，FHS 分组由主单元转接到从单元。该分组将确立定时和同步频率。在从单元已收到呼叫消息后，它将返回一个响应消息，该消息是在收到呼叫消息后，由 ID 分组和仅随其后的 625 μs 准确值重新组成。据主单元的 RX/TX 定时，在 TX 时隙主单元发送 FHS 分组，在仅随其后的 RX 时隙里， 主单元接收从单元响应。在响应和 FHS 消息之间的时差取决于从单元接收的呼叫消息的定时。

从单元接收到呼叫消息先在主一从时隙里发送。然后它将在从一主时隙里前半部里以 ID 分组格式响应。FHS 分组的定时基于前次主一从时隙里的最先发送的呼叫消息的定时。在第一次呼叫消息和 FHS 分组之间，有一个准确的 1250 μs 延迟，分组在跳频点 f(k+1)发送，该跳频点是紧随在呼叫消息被接收处的跳频点 f(k)后。

从单元接收呼叫消息是在其后的主一从时隙里。这个用 ID 分组的响应过程是在收到呼叫消息后的从一主时隙 625 μs 准确值的后半部分。FHS 分组的定时仍基于前次主一从时隙里的首先发送呼叫消息的定时。在第一次呼叫消息和 FHS 分组之间，有一个准确的 1250 μs 延迟，分组在跳频点处 f(k+2)发送，该跳频点是紧随在呼叫消息接收到的 f(k+1)的跳频点处。如图所示：



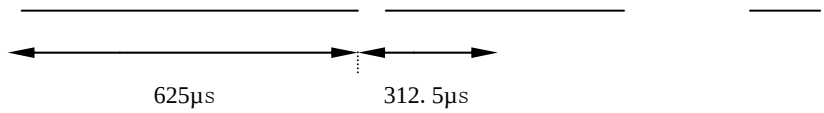


图 2.35 成功呼叫 FHS 分组的定时前半部分时隙

从单元调整它的 RX/TX 定时是依据 FHS 分组的接收，而不是根据呼叫消息的接收。即 FHS 分组接收确认的二次响应消息在 FHS 分组开始后的 625 μs 被传输。

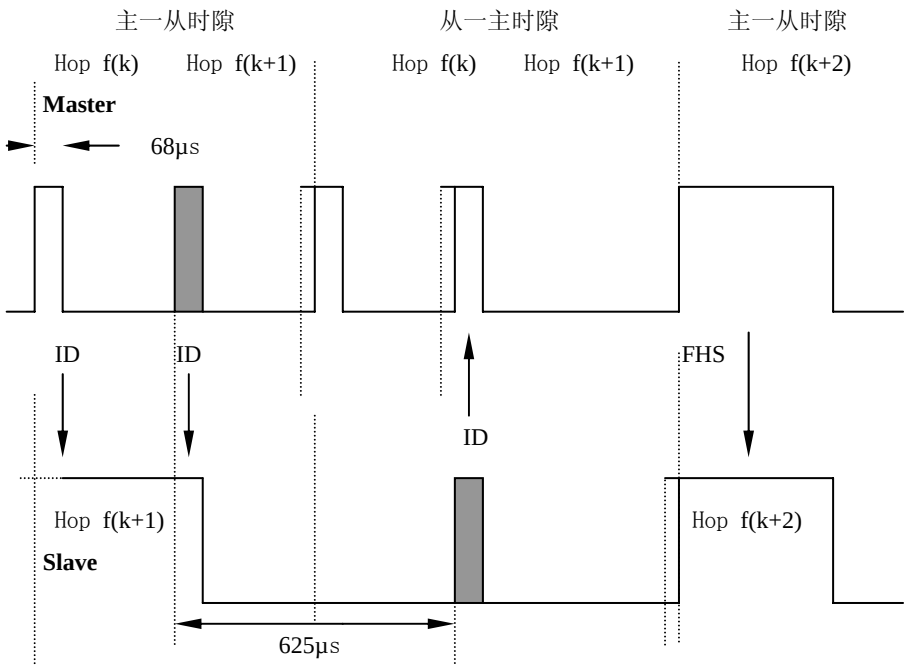
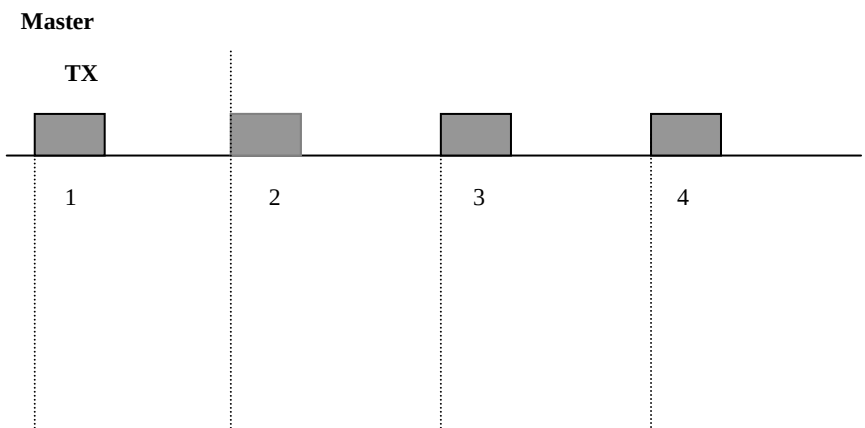


图 2.36 成功呼叫 FHS 分组的定时后半部分时隙

9.7 多一从结构

正如在本章开始处所提到的主单元总是以偶数时隙开始传输，而从单元总是以奇数时隙开始它的传输。这就表明了主单元的定时经过一个时隙（625 μs）发生转换。如图所示：



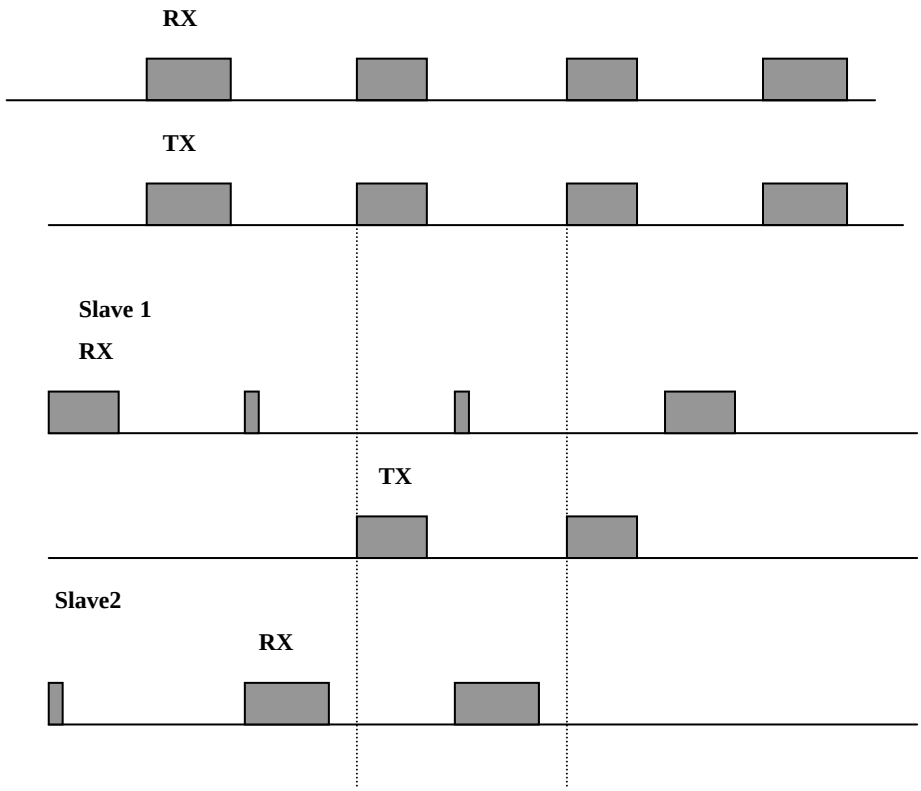


图 2.37　多一从结构 RX/TX 定时

在下一次从一主时隙里，只有经过它自身 AM_ADD 编址的从单元可以返回。如果没有有效的 AM_ADD 值收到且涉及到保留的 SCO 从一主时隙，只有从单元可以响应。在广播消息的情况里，从单元不允许返回分组。在休眠模式里，鉴权请求的识别期是一个例外。

10.　信道控制

10.1　概述

本书的该部分描述了如何实现匹克网的信道建立、单元增加及释放过程，为支持这些功能定义了几种蓝牙单元的操作状态。另外，对多匹克网操作共享区域（即散射网络）也作了讨论，并将 FH　同步中起主要作用的蓝牙时钟作为了一个专题。

10.2　主－从定义

匹克网中的信道特性完全由匹克网的主单元来确定，主单元蓝牙设备

地址（BD_ADDR）确定了跳频序列及信道识别码，主单元的系统时钟确立了跳频序列的状态和定时设置。另外主单元通过轮询（POLL）方式控制信道通信。

通过定义，实施链接的蓝牙单元表明为主单元（与一个或多个从单元链接）。注意：主和从的取名只因涉及到信道协议，由于蓝牙每个单元的权是完全一样的，也就是说任何一个单元都可能成为匹克网的主单元，所以一旦匹克网建立，主－从角色就完全可以进行互换，有关这方面的详细内容参看匹克网间通信。

10.3 蓝牙时钟

每一个蓝牙单元都有一个内部系统时钟，它决定了收、发信机的定时和跳频。因蓝牙时钟取自一个自由运转的时钟，该时钟永不会被调整和关闭。 作为与其它单元的同步，仅有时钟补偿值对该时钟作为相互同步的临时蓝牙时钟。应当注意：蓝牙时钟与每天的时间无关，因此，它可用任何值初始化。蓝牙时钟作为蓝牙收、发信机的时钟，它的分辨度至少是TX或RX的时隙长度的一半或者 312. 5μs，该时钟周期约为一天。如果时钟用计数器来实现，那么 28 位计数器的计数值范围是 2^{28}–1。在 312. 5μs的各单元LSB点，给出的时钟频率是 3. 2KHz。

在匹克网信道上的定时和跳频由主单元的蓝牙时钟来确定。当匹克网确立时，主单元时钟值通过通信链接传送给从单元，各从单元在自己的本地时钟上增加一个补偿值以求得与主时钟同步。由于时钟不能受控，所以该补偿值必须有规律的进行更新。

在蓝牙接收机里，时钟确定了临界时间并激发事件。对蓝牙系统来说有四个时间段非常重要：312. 5μs，625μs，1. 25ms 和 1. 28S。这些时间段分别于定时器位 CLK0、CLK1、CLK2 和 CLK3 对应。如图所示：

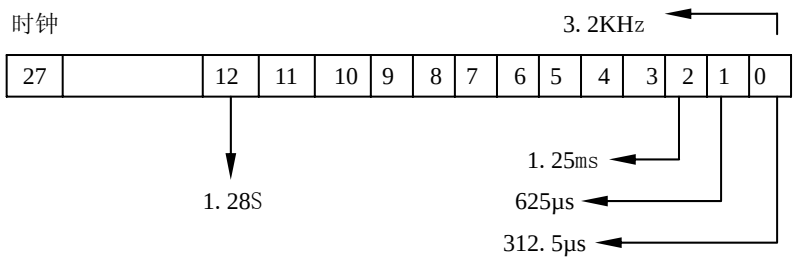


图 2.38 蓝牙时钟

当 CLK0、CLK1 都为“0”时，主一从传输以偶数时隙开始。

在不同的模式和状态里的蓝牙单元可具有不同的时钟特性：

- CLKN 本地时钟
- CLKE 预计时钟

● CLK 主时钟

CLKN 是一个自由运转的时钟，而且是所有其它时钟特性的参考。在高度活跃状态下，本地时钟用精度为+/-20ppm 晶体振荡器产生。在低度活跃状态下，如待机（STANDBY）、保持（HOLD）、休眠（PARK），本地时钟可以用相对精度较差的 +/-250 ppm 低功耗振荡器（LOP）产生。

CLKE 和 CLK 通过增加一个补偿值取自 CLKN 基准。CLKE 是一个处理接收器的本地时钟估算呼叫单位，即：在呼叫 CLKN 上加补偿近于接收的 CLKN。通过使用接收的 CLKN，呼叫加速了链接建立。

CLKE 导出见图所示：

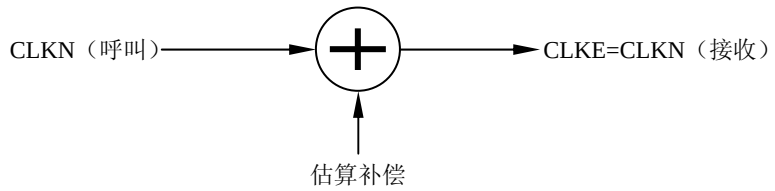


图 2.39

CLK 是匹克网的主时钟，它用于匹克网中所有定时和时序安排。所有的蓝牙设备都使用 CLK 来安排它们传输和接收时序。CLK 通过在本地时钟 CLKN 的基础上增加一个补偿值获得。因为 CLK 同它自己的本地时钟 CLKN 是完全等同的，所以对主单元来说，补偿值是“0”。而对各个从单元来说，都对自身的 CLKN 加上一个适当的补偿值，以求得与主单元的 CLKN 一致。虽然在蓝牙设备里所有 CLKN 都以相同的标称速率运行，但相互之间的漂移引起了 CLK 的不准确性。因此在从单元里的补偿必须定期的修改，以致 CLK 近似于主单元的 CLKN。

主单元和从单元的 CLK 导出如图所示：

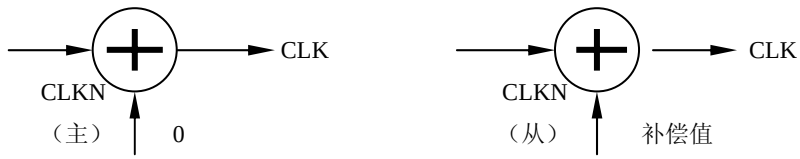


图 2.40

10.4 状态综述

下面我们将以一个图的结构来说明用于蓝牙链接控制器的不同状态。这里有两种主要状态 STANDBY（待机）和 CONNECTION（联机）。另外还有七种子状态：呼叫、呼叫扫描、查询、查询扫描、主响应、从响应和从查询。子状态是用来在匹克网中增加新的从单元的过渡状态。

要从一个状态转到另一个状态，要么使用蓝牙链接管理器命令，要么

使用链接控制器的内部命令（像来自于相关器或超时信号的激发信号）。

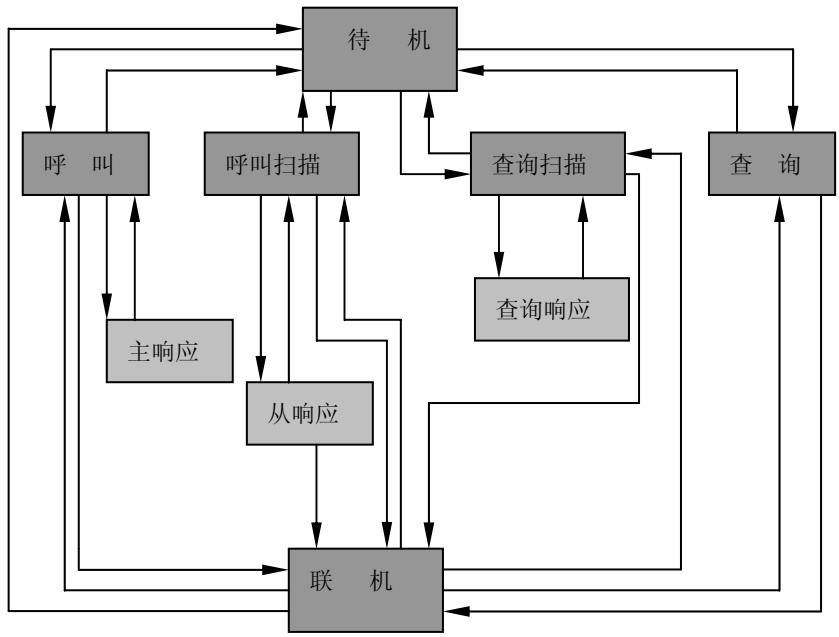


图 2.41 蓝牙链接控制器状态图

10.5 待机状态（STANDBY STATE）

待机状态是蓝牙单元中的默认状态。在这个状态下，蓝牙单元处于低功耗模式，只有本地时钟以 LOP 精度（或更好的）运行。

控制器可以脱离待机状态去扫描呼叫、查询消息、呼叫或自身查询。当对一个呼叫消息响应时，该单元不会再返回到待机状态，而是作为一个从单元进人联机状态。当执行呼叫成功时，该单元将作为一个主单元进人联机状态。有关用扫描活动间隔来执行的内容将在呼叫扫描和查询扫描中讨论。

10.6 识别过程

10. 6. 1 概述

为了建立新的联机就应使用查询和呼出过程。查询过程使一个单元能发现那些单元在范围之内以及它们的设备地址和时钟是多少。通过呼出过程，一个实际的联机就能确定。只有蓝牙设备地址才要求建立联机。确立了联机的单元，可以执行呼叫过程并自动的成为联机的主单元。

在呼出和查询过程中，分别使用设备识别代码（DAC）和查询识别代

码（IAC）。在呼叫扫描和查询扫描子状态里的单元依靠这些各自的识别码和匹配相关器相关。

对于呼出过程，几种呼出方案可以使用。有一种必须是由各蓝牙设备支持的强制呼出方案。当单元是第一次使用时，就使用强制呼出方案，而且呼出过程直接跟随查询过程。曾经使用强制呼出 / 扫描方案联机的两个单元可以决定选择强制呼出 / 扫描方案。选择呼出方案附录VII中作了讨论，而在本节中，只考虑强制呼出方案。

10.6.2 呼叫扫描

在呼叫扫描子状态里，单元在 Tw page scan 扫描期间规定自身设备识别码，并在该扫描期间单元以独立跳频方式获取与它设备识别码的相关器匹配。扫描期间应有足够宽度来完成 16 跳呼叫扫描频率。

当单元进入呼叫扫描子状态时，它依据同这个单元一致的呼叫跳频序列来选择扫描频率。该序列是一个 32 跳的序列（或假设为一个 16 跳的简化跳频系统），在这里面每一个跳频是唯一的。呼叫跳频序列通过单元的蓝牙设备地址（BD_ADDR）来确定。在序列中的时段由单元的本地时钟 $CLKN_{16-12}$来确定（$CLKN_{13-12}$假设为一个 16 跳的简化跳频系统）。也就是说，每隔 1.28s就要选择一个不同的频率。

如果在呼叫扫描期间相关器超过了触发门限，单元将进入从响应子状态，有关内容参看后续的从响应描述。

呼叫扫描子状态可以从待机状态或联机状态进入。在待机状态下，未建立任何联机的单元可以使用全部性能来实现呼叫扫描。在从联机状态进入呼叫扫描子状态前，单元尽可能多地保留扫描性能。如有可能的话，单元可以在保持模式设置的 ACL 联机甚至休眠模式中使用。具体内容见保持模式和休眠模式的描述。SCO 联机更希望不要被呼叫扫描中断，在这种情况下，呼叫扫描模式可以由具有更高优先权的 SCO 保留时隙中断，SCO 分组应当要求用最小容量 (HV3 分组)。扫描期间将增加一个最小的设置延迟。如果使用 HV3 分组的一个 SCO 链接出现且 Tsco=6 的时隙，建议使用一个至少 36 时隙 (22.5ms) 的总扫描期间 Tw page scan；如果使用 HV3 分组的两个 SCO 链接出现且 Tsco=6 的时隙，建议使用一个至少 54 时隙 (33.75ms)的总扫描期间。

扫描间隔 Tpage scan 定义为两个连续的呼叫扫描之间的间歇。其差异构成在扫描间隔等于扫描期间 Tw page scan (连续扫描) 的情况，扫描间隔最大为 1.28s 或扫描间隔最大为 2.56s，这三种情形决定了呼出单元的特性。也就是说，呼出单元使用 R0，R1 还是 R2 见后面的有关内容。

下面用表的形式来阐明 Tpage scan 和模式 R0，R1 和 R2 之间的关系。

虽然在 R0 模式下扫描是连续的，但扫描可以被类似于保留 SCO 时隙

打断。扫描间隔信息包含在 FHS 分组中的 SR 字段。

表 2.12 在扫描间隔、重复序列及 R0、R1 和 R2 呼出模式之间的关系

SR 模式	Tpage scan	Npage
R0	连续	≥1
R1	≤1. 28s	≥128
R2	≤2. 56s	≥256
保 留	..	..

在呼叫扫描过程中，蓝牙单元可以选择任意扫描模式(但查询响应消息返回后的呼叫扫描情况除外)。具体内容参看查询响应章节。

10. 6. 3 呼叫

呼叫状态用在主单元（源）激活并链接一个定时唤醒在呼叫扫描状态中从单元（目的）场合。主单元用不同的跳频信道反复地传输从单元的设备识别码（DAC）来达到与从单元的链接。由于主单元和从单元的蓝牙时钟并不同步，主单元就不能确切地知道从单元什么时间该唤醒且工作在什么跳频点上。因此，它在不同的跳频点上传送一系列相同的设备识别码，并在传输间隔中监听来自从单元的接收响应。

主单元中的呼叫过程由许多步构成。首先，从单元的设备地址用来决定呼叫的跳频序列，这是主单元到达从单元的序列。对于序列中的阶段，主单元使用从单元的时钟估算值。这个估算值可作为取自定时信息的例子，即最后一次遇到使用该特定设备（在那时作为活动主单元）期间切换或来自于查询过程。通过使用从单元的蓝牙时钟估算 CLKN，主单元能够预测从单元在什么时间唤醒和处在那一个跳频点上。

在从单元中蓝牙时钟的估算值可能会完全是错误的。虽然主单元和从单元使用了相同的跳频序列，但是它们在序列里使用了不同阶段而且永远不能彼此相遇。为了补偿时钟漂移，在若干唤醒频率上的短时间隔期间，主单元将发送自身呼叫消息，实际上主单元也在当前时间的前后跳频点上传送预测跳频。在各个 TX 时隙里，主单元连续地在两个不同的跳频点上传送。由于呼叫消息是一个仅有 68 位的 ID 分组，在下面的 RX 时隙中有充足的时间 (最短 224. 5μs) 切换频率合成器，接收机将连续地监听 ID 分组两个完全一致的 RX 跳频，RX 跳频又将依据呼叫响应跳频序列来选择，呼叫响应跳频序列也严格地符合呼叫跳频序列。在呼叫状态中的 RX/TX 定时已在前面作了描述。在下一个 TX 时隙中，主单元将传送不同于前面跳频序列的两个跳频序列。频率合成器跳频的速率可增加到 3200 跳/秒。

在 79 跳系统和 23 跳系统之间应有差别。首先考虑 79 跳系统。正如以上描述的增加跳频速率，发射机能复盖在 16 时隙或 10 毫秒内复盖 16 个不同的跳频。呼叫跳频序列被分成 16 种频率的A和B两个呼叫序列。序列A中包括围绕当前预测跳频f(k)的 16 种跳频。这里k由时钟估算值$CLKN_{16-12}$来决定。 所以第一个序列由跳频f(k-8),f(k-7),…,f(k),…,f(k+7)组成。

当主单元和从单元的蓝牙时钟差别在−8*1. 28s和+7*1. 28s之间时，由主单元使用的频率之一将是从单元获取的跳频。然而，由于主单元不知道从单元什么时间将进入呼叫扫描状态，主单元就必须重复序列A Npage次或直到收到响应为止。如果从单元扫描间隔与R1 一致，重复次数至少是 128；如果从单元扫描间隔与R2 一致，重复次数至少是 256。注意，$CLKN_{16-12}$每 1. 28 秒改变一次。因此，每 1. 28 秒，序列包含为呼叫跳频设置的不同频率。当主单元和从单元的蓝牙时钟差别小于−8*1. 28 秒或大于+7*1. 28 秒时，就要试用更多的跳频点。 总的来说，由于只有 32 种专用唤醒跳频点，所以，更多的跳频点是仍未使用过的跳频点。余下的 16 个跳频点用于新的 10ms 序列 B 形式。第二个序列由跳频f(k-16),…,f(k-15),…,f(k-9),…,f(k+8),…,f(k+15)组成。序列B重复Npage次。如果没有得到回答，序列A先再重复Npage次，然后序列A和序列B交替使用，直到收到一个回答或超时呼叫TO的执行。如果在监听场合下，响应由从单元返回，主单元进入响应状态。

这儿给出的呼出和呼叫扫描过程的描述是对应于美国和欧洲使用的 79 跳系统而讲解的，作为在日本及某些欧洲国家所使用的 23 跳系统来说，该过程就稍有不同。在 23 跳系统的情况下，呼叫跳频序列的长度被压缩为 16，为此，仅有一个单独的序列 (序列A) 包含了所有呼叫的跳频频率。呼叫跳频序列步不是$CLEK_{16-12}$而是$CLEK_{15-12}$不一定非要对从单元时钟作一个估算。呼叫状态可以从待机状态或联机状态中进入。在待机状态下，无链接已经确立且单元可以使用所有的性能来呼叫。

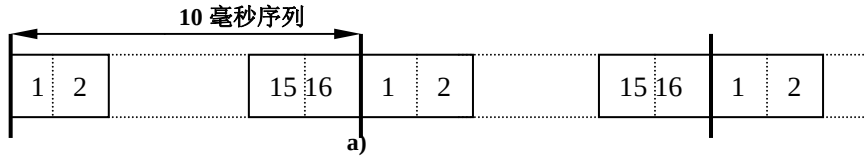
在从联机状态进入呼叫子状态之前，单元应当尽可能多的释放容量来扫描。为了保证这点，建议在保持或休眠状态上设置 ACL 链接。然而，SCO 链接不应被呼叫打扰，这就意味着呼叫只能被具有更高优先级保留 SCO 时隙中断。为了使呼出获得更多的容量，建议使用具有少量容量的 SCO 分组 (HV3 分组)。若是 SCO 链接，单序列的重复次数 Npage 将增加。这儿用一个表来说明，此处我们假设是用的具有 Tsco=6 的 HV3 分组，该分组符合 64kb/s 链接。

表 2. 13 当为 SCO 链接时在重复序列和 R0、R1 和 R2 呼出模式相互间的关系

SR 模式	非 SCO 链接	单 SCO 链接（HV3）	双 SCO 链接（HV3）
R0	Npage≥1	Npage≥2	Npage≥3

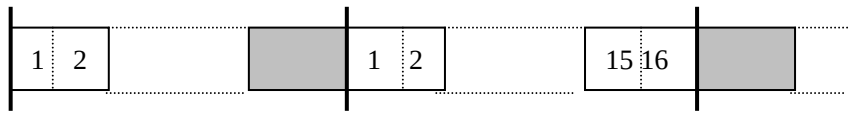
R1	Npage≥128	Npage≥256	Npage≥384
R2	Npage≥256	Npage≥512	Npage≥768

呼叫序列的建立不依赖于 SCO 链接的存在。即，SCO 分组在保留时隙上传送但并不影响用于非保留时隙上的跳频。



a)

图 2.42



SCO 时隙

b)

图 2.43

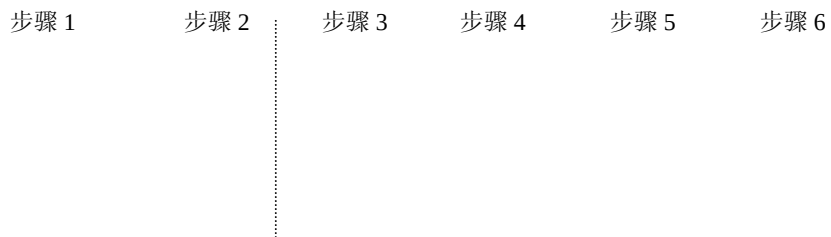
10.6.4 呼叫响应过程

当呼叫消息由从单元成功的接收时，在主单元和从单元之间有一个近似的 FH 同步。双方都进入互换继续建立联机的重要信息应答规范。匹克网联机的重要性是双方蓝牙单元都使用相同信道识别码、相同信道跳频序列和同步时钟，这些参数取自主单元。初始化联机的单元 (启动呼叫) 作为主单元 (仅在匹克网存在期有效)。信道识别码和信道跳频序列取自主单元的蓝牙设备地址(BD_ADDR)。定时取决于主单元时钟，从单元的本地时钟在临时加上补偿后应与主单元时钟同步。在开始时，必须把主单元的参数传送给从单元。在主单元和从单元之间的开始消息在这一节将讨论。

主单元和从单元之间的初始化消息如下表及图所示：

表 2.14 开始过程的初始化消息

步骤	消　　息	方　向	跳频序列	识别码及时钟
1	从单元 ID	主一从	呼叫	从单元
2	从单元 ID	从一主	呼叫响应	从单元
3	FHS	主一从	呼叫	从单元
4	从单元 ID	从一主	呼叫响应	从单元
5	第一分组主单元	主一从	信道	主单元
6	第一分组从单元	从一主	信道	主单元



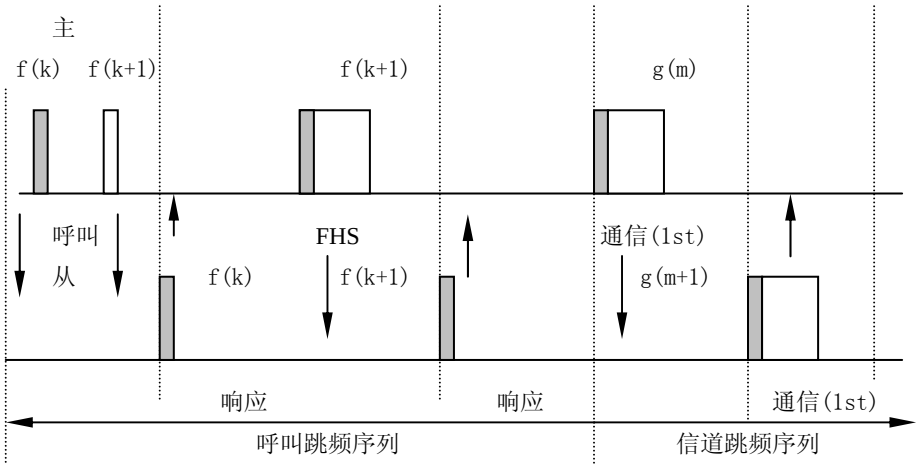


图 2.44 当从单元响应第一次呼叫消息时的联机通信初态

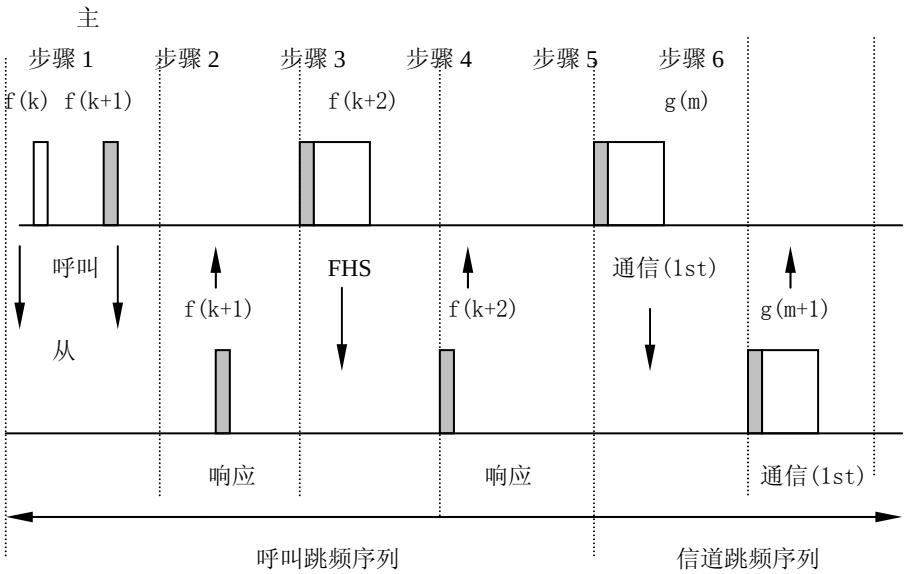


图 2.45 当从单元响应第二次呼叫消息时联机通信初态

两图中，频率 f(k)，f(k+1)，等是从单元的 BD_ADDR 确定的呼叫跳频序列的频率。频率 f’(k)，f’(k+1)等是相应的呼叫响应频率(从一主)。频率 g(m)属于信道跳频序列。

在步骤 1 里，主单元处于呼叫状态，而从单元处于呼叫扫描状态。假设在这一步里，呼叫消息（从单元的设备识别码）由主单元传送从单元，经从单元设备识别码辨认，从单元进入第二步的从单元响应。此时主单元等待从单元的回答且当在第二步时得到从单元的回答，主单元就进入第三步的主单元响应。注意，在最初的信息交换中，所有的参数都取自从单元的 BD_ADDR，而且只能使用呼叫跳频和呼叫响应跳频序列 (它们也来自

于从单元的 BD_ADDR)。

应当注意，当主单元和从单元进入响应状态时，它们输入的呼叫时钟和呼叫响应跳频选择被冻结，具体内容见呼叫响应部分的描述。

10.6.4.1 从单元响应

从单元在第一步中收到自身的设备识别码后，在第二步就传送一个应答消息，该应答消息也仅由从单元的设备识别码构成。在开始接收呼叫消息 (从单元ID分组) 和在应答跳频符合呼叫消息接收的跳频后，从单元将以 625μs传送该应答消息。因此从单元传输时间应与主单元传输时间匹配。在最初的通信中，从单元仍然使用呼叫应答跳频序列向主单元返回信息。时钟输入$CLKN_{16-12}$被冻结为一个值，该值就是呼叫消息接收到的时间值。

在发出响应消息后，激活从单元的接收器，并等待 FHS 分组的到来。注意：FHS 分组在呼叫消息到达后可提前 312.5μs 到达。而且不像通常 RX/TX 定时情况下的 625μs 后。

如果联机状态在得到前建立失败，则将执行以下过程。只要没收到 FHS 分组直到呼叫响应超出前，从单元就持续监听。然而，每隔 1.25 毫秒，它就要据呼叫跳频序列来选取下一个主一从跳频。如果在呼叫响应后没有收到任何东西，从单元就作为一个扫描周期返回到呼叫扫描状态。扫描周期的长度取决于 SCO 时隙的存在，如果在这个附加的扫描周期内，没收到呼叫消息，从单元以它固有的扫描间歇重新开始扫描并返回到优于第一次呼叫扫描状态的状态。

如果FHS分组经从单元在从响应状态下收到，从单元就在第 4 步返回一个应答信号（ 只能是从单元的设备识别码 ）确认FHS分组的接收（仍使用呼叫响应跳频序列）。该响应分组的传输基于FHS分组的接收，然后从单元改变从FHS分组中接收到的信道（主单元的）识别码和时钟。只有主时钟的 $26MSB_S$转接，定时假设如CLK_1和CLK_0都为“0”时，FHS分组时间只有在主单元以偶数时隙传输时才能收到。从FHS分组的主时钟里，主单元时钟和从单元时钟之间的补偿取值被确定并报告给从单元的链接管理器。

最后从单元在第 5 步进入联机状态，从那时起，从单元将使用主单元的时钟而且主单元的 BD_ADDR 决定了信道跳频序列和信道识别码。联接模式以主单元传送一个 POLL 分组开始，从单元以任何类型的分组响应。如果从单元没收到 POLL 分组或主单元没收到应答分组，那么，在 FHS 分组确认后并在新的联机时隙数内，主单元和从单元将分别返回到呼叫与呼叫扫描状态。

10.6.4.2 主响应

当主单元在第二步里收到了来自于从单元的应答消息，它将进入主应答惯例。它冻结输入到呼叫跳频选择方案的当前时钟，然后主单元在第三步传送一个 FHS 分组，该分组包含了主单元的实时蓝牙时钟，主单元的 48 位 BD_ADDR 地址，BCH 奇偶位和设备的分类。如果没有要求准确的指明主单元设备地址，FHS 分组就包含了构成所有信道识别码的信息。在紧跟着从单元已响应时隙的主一从时隙的初期，FHS 分组被传送。 因此 FHS 的 TX 定时并不是基于从单元的应答分组接收，FHS 分组可以接收到应答分组后的 312. 5μs 后被送出，而不像通常 RX/TX 定时情况下接收分组的 625μs 后。

在主单元已送出 FHS 分组后，它在 FHS 分组接收确认的第四步就等待来自从单元的第二次应答。如没收到应答（这次也仅是从单元的设备识别码）， 主单元就重新传送 FHS 分组，但是时钟要被修改且仍使用从单元的参数，重传（每次重传的时钟都要作修改）将持续到第二次收到从单元应答或呼叫应答超时。在后一种情况里，主单元将返回到呼叫状态，并向链接管理器传送一个出错信息。在 FHS 分组的重传过程中，主单元将一直使用呼叫跳频序列。

如果确实收到了从单元的应答，主单元改变主单元参数，如信道识别码和主时钟。在FHS分组传送的开始时，低时钟位CLK_0和CLK_1都为“0”而且不包含在FHS分组中。最后，在第 5 步主单元进入联机状态，主单元的BD_ADDR用来改变新的跳频序列和信道跳频序列。信道跳频序列在（伪）随机方式中用了所有 79 个跳频信道。现在主单元用新（主）参数以确定的跳频可以把它的第一个通信分组传送出去。该第一分组将是POLL分组。

现在主单元用新（主）参数以确定的跳频可以把它的第一个通信分组传送出去。该状态里的第一分组是一个主单元传送的 POLL 分组。这个分组将在 FHS 分组的确认已收到后，该分组在新联机时隙数内发送，从单元以任何类型的分组作为响应。如果 POLL 分组没被从单元收到或 POLL 分组的响应没有被主单元在新联机时隙数内收到，那么主单元和从单元将分别返回到呼叫和呼叫扫描状态。

10.7 查询过程

10. 7. 1 概述

在蓝牙系统中，查询过程被定义为收端设备地址并不为发端所知。人们可以认为是类似于如打印机，传真机或通向网关的普通设备。从而，查询过程可以用于发现其它的蓝牙单元在范围内否。在查询状态中，发现单元搜集所有的蓝牙设备地址和响应查询消息所有单元时钟。如果需要的话，它可以通过以前所述的呼叫过程方式同其中任何一个建立联系。

通过发端广播的查询消息不包含任何有关发端的信息。然而，它能指出应答设备的类型。有一种通用的查询设备识别码（GIAC）可以查询任何蓝牙设备和只用于查询确定类型设备的专用查询识别码（DIAC）的数量。查询识别码取自于保留的蓝牙设备字。

希望发现有其它蓝牙单元进入查询状态情况时，它连续地以不同的跳频传送查询消息 (它就是 ID 分组)。查询跳频序列总是取自 GIAC 的 LAP，这样，当 DIAC 被使用时，应有跳频序列从 GIAC 的 LAP 产生。允许自身被发现的单元有规律的进入查询扫描状态以回答查询消息。以下各节描述了在查询应答中的消息变换和竞争。查询响应是任意可选的：单元并不强迫要求响应查询消息。

10.7.2 查询扫描

查询扫描状态非常类似于呼叫扫描状态。然而，不同的是作为单元设备识别码的扫描，查询识别码的接收器扫描只要足够完成 16 种查询频率扫描，扫描周期的长度被定称为 Tw-inquiry-scan。扫描采用单跳频执行方式，就像在呼叫过程中一样，根据查询跳频序列扫描过程中使用 32 种专用查询跳频，这些频率由通用查询地址来决定。该状态由执行查询扫描单元的本地时钟来决定，这个阶段每 1.28 秒改变一次。

通用查询识别码的替换或增加，单元可以扫描一个或更多专用查询识别码。然而，扫描将紧随由通用查询地址决定的查询跳频序列。如果查询消息在查询唤醒期被辨别出来，那么蓝牙单元就进入查询应答状态。

查询扫描状态可以从待机状态或联机状态进入。在待机状态下，没有建立任何联接，单元可以使用所有的能力执行查询扫描。在从联机状态进入查询扫描状态之前，单元尽可能多的保留用于扫描的能力。如果希望单元可以在 HOLD 模式下设置 ACL 链接，甚至使用休眠模式，请见保持模式（HOLD）内容。SCO 链接不能被查询扫描中断。在这种情况下，查询扫描可以被具有更高优先级的 SCO 时隙中断。SCO 分组应当具有最低限的请求能力 (HV3 分组)。扫描期 Tw iquiry scan 应当增加一个向查询消息作应答的可能。如果为使用 HV3 和 Tsco=6 的一个 SCO 链接时隙，建议使用用至少 36 时隙 (22.5ms) 的完整扫描期。如果使用 HV3 和 Tsco=6 的两个 SCO 链接时隙，建议使用一个至少达 54 时隙的（33.75ms）扫描期。

扫描间歇 Tinquiry scan 定义为在连续的两个查询扫描之间的间隔。查询扫描间隔最多为 2.56 秒。

10.7.3 查询

查询状态由企图找到新设备的单元使用。该状态非常类似于呼叫状态，TX / RX 定时也同样类似于呼出过程。TX 和 RX 频率紧跟着查询跳频

序列和查询应答跳频序列，而且经通用查询识别码和发现设备的本地时钟确定。在查询传输期间，蓝牙接收器扫描查询响应消息，当发现整个响应分组（ 实际上就是 FHS 分组 ）读到时，此后，查询单元继续执行查询传输。所以在查询状态里的蓝牙单元并不要求确认查询响应消息，它继续试着使用不同的跳频信道及监听响应分组。如呼叫状态一样，定义了两个 10ms 的 A 和 B 队列，把 32 个频率的查询跳频链分为两个 16 跳频的部分。每个单独的队列在一个新序列队列使用之前，必须重复至少 Ninquiry=256 次。为了搜集可能出错情况下的所有响应，至少要发生 3 次序列切换。结果，查询状态至少持续 10. 24 秒，除非查询器搜集到足够的响应并决定忽略早期查询状态。为在对通信质量要求不高的情况下接收到所有的响应，查询器可延长查询状态。如果一个查询过程自动的定期启动 (比如说每分钟 10 秒周期)，那么在两个查询过程之间的间隔的确定必须是随机确定。这样做是为了避免两个蓝牙单元同步他们的查询过程。

查询转态一直持续到被蓝牙链接管理器停止 (当它决定它有了足够的响应量时)，或超时发生时。

查询状态可以从待机状态或联机状态进入。在待机状态下，没有建立任何联接，单元可以使用所有的能力执行查询。在从联机状态进入查询状态之前，单元尽可能多的保留用于扫描的能力。为作到这点建议在保持和休眠状态下使用 ACL 链接。然而，SCO 链接不应被查询干扰，这就意味着查询可以被具有更高优先级的保留 SCO 时隙中断。为了获得更多的查询能力，最好少量的容量 (HV3) 建议使用 SCO 分组。如果使用 SCO 链接，就要增加 Ninquiry 重复次数。

这里假设具有 Tsco=6 时隙间隔的 HV3 分组被使用，同时将符合一个 64kb/s 的话音链接。见下表：

表 2.15

	无 SCO 链接	单 SCO 链接（HV3）	双 SCO 链接（HV3）
Ninquiry	≥256	≥512	≥768

10. 7. 4 查询响应

对于查询操作，只有从单元响应，而没有主单元响应。主单元在作为响应的查询消息之间监听，但读取响应后，它继续传送查询信息。从单元响应惯例完全不同于呼叫响应惯例。在查询扫描状态下收到查询消息时，应返回一个含有接受器地址的响应消息，该响应消息是一个普通的带有单元参数的 FHS 分组。然而，当几个蓝牙单元在物理层上与查询单元处于近程链接，并且都在同时向查询单元作出响应时， 就会出现一个竞争问题。首先，每个蓝牙单元都有自己的运行时钟，因此，他们都使用相同的查询

跳频序列的同一阶段是几乎不可能的。然而为了避免在两个单元之间真的出现在同一个查询跳频信道同时唤醒的冲突，从单元的查询响应必须使用以下协议。如果从单元收到一个查询消息， 就在 0 到 1023 之间产生一个随机数。另外，它释放当前输入值（阶段）到跳频选择体系，从单元在 RAND 时间时隙期间返回到联机或待机状态。在回到联机或待机状态之前，单元可以浏览呼叫扫描状态，该呼叫扫描必须遵循呼叫扫描的方式。至少在 RAND 时隙之后，单元才返回到查询响应状态.。收到第一个查询消息时，从单元就向主单元返回一个 FHS 响应分组。如果在扫描期间的超时限制内没有发生触发事件，从单元就返回到待机或联机状态。如果从单元收到查询消息并返回了一个 FHS 分组，它就在查询跳频序列(这个阶段有一个 1. 28 秒的分辨力)中的阶段增加一个 1 的补偿，并且再次进入查询状态。如果从单元被再次激发，它就使用一个新的 RAND 来重复上述过程，每次 FHS 分组的时钟积累补偿被返回。在一个 1. 28 秒的探查期中，从单元平均响应 4 次，但每次以不同的时间和不同的频率响应。SCO 时隙应当比响应分组具有更高的优先级，那就是说，如果一个响应分组被和 SCO 时隙复盖时，它就不能被传送，需等到下一个查询消息到来。

查询惯例间的消息如下表所示，在第一步中，主单元使用用查询识别码和它自己的时钟发布一个查询消息信息，从单元以含有从单元的设备地址，本地时钟和其它从单元信息的 FHS 分组作响应。该 FHS 分组在一个部分随机时间返回。FHS 分组在查询惯例中不需确认，但只要主单元正以查询消息作探查，它应在其它时间或其它频率执行重传过程。

表 2.16

步骤	消息	方　向	跳频序列	识别码
1	ID	主一从	查询	查询
2	FHS	从一主	查询响应	查询

如果扫描单元使用选择扫描方式，在用 FHS 分组响应查询应答后，它将用强制呼叫扫描方式在强制呼叫扫描时间内完成呼叫扫描。每次单元用强制呼叫扫描时间启动定时器并将查询响应送出。在每次新的查询响应中，定时器被清除。当单元完成呼叫扫描时，在 SR 模式下它将使用强制呼叫方式来作为整个自身呼叫扫描间隔，直到定时器溢出。在查询过程允许所有单元都链接甚至所有单元都不支持选择扫描模式后，使用强制呼叫方式。另外，使用强制呼叫扫描方式和选择呼叫扫描方式可并行使用强制呼叫扫描时间。

强制呼叫扫描时间包含在查询响应惯例返回 FHS 分组的 SP 字段中。该时间值如下表指出：

表 2.17 P0、P1、P2 扫描区间模式的强制扫描期

SP 模式	强制呼叫扫描时间
P0	≥20s
P1	≥40s
P2	≥60s
保留	—

10.8 联机状态

在联机状态下，联机已建立分组可以接收和发送。在两个单元里，使用信道 (主) 识别码和主蓝牙时钟。跳频方案使用信道跳频序列。主单元在偶数时隙 (CLK_{1-0}=00) 开始传输，从单元在奇数信道 (CLK_{1-0}=10)开始传输。

联机状态以主单元用 POLL 分组发送开始去核查主单元的定时和信道跳频切换，从单元以任何类型的分组响应。如果从单元没收到 POLL 分组或主单元没收到新的联机时隙数响应，两边设备都返回到呼叫 / 呼叫扫描子状态。

在联机状态中第一个信息分组包含了表述链接特性和有关蓝牙单元更多细节的控制消息。这些消息在单元的链接管理器间进行互换，例如，它定义了 SCO 链接和呼吸参数，然后用户信息的传输由传送和接收分组交替运行。

联机状态通过 detach 和 reset 命令结束。如果链接以正常方式结束,就使用 detach 命令，此时在蓝牙链接控制器的所有设置数据仍然有效。reset 命令是整个控制器处理强制清除。在清除后，控制器必重新须设置。

在联机状态里，蓝牙单元可以具有多种操作模式。如：活动模式、呼吸模式、保持模式和休眠模式，以下将详细描述这些模式。

10.8.1 活动模式

在活动模式里，蓝牙单元活跃地分享信道。主单元调度传输基于来自不同的从单元通信要求。另外，它还支持有序传输以保持从单元和信道同步。活动从单元监听主一从分组时隙。如果活动从单元没编址，它可以在下一个新的主单元传送之前处于睡眠状态。据分组中类型指示，可以得到主单元为它的传送所保留的时隙数。在该时间期间，无编址的从单元不能监听主一从时隙。主单元传输周期要求从单元和信道保持同步。由于从单元只需要信道识别码用于同步，所以任何类型的分组都可用于此目的。

10.8.2 呼吸方式

在呼吸方式下，从单元的监听有效区域压缩。如果从单元参与了 ACL 链接，它必须监听主单元通信的每个 ACL 时隙。在呼吸模式下，主单元实现对指定的从单元传送的时隙可以压缩，也就是说，主单元只能在特定的时间时隙实现传送。所以这些称为呼吸时隙是有规律的使用 Tsniff 间隔空间。

从单元必须在 Dsniff 时隙上监听 Nsniff attempt 的 Tsniff 次数。如果从单元在 Nsniff attemptRX 时隙上的任一时隙接收到一个分组，只要它收到的分组是与它有关的 AM_ADDR，它应继续监听。一旦它停止接收分组，它应当继续监听 Nsniff timeout RX 时隙， 或 RX 时隙的 Nsniff attempt 数的余量是最大的。

为进入呼吸模式，主单元经LM协议发出呼吸命令，该消息包含呼吸 Tsniff 间隔和Dsniff补偿。呼吸模式的定时和SCO链接相似地确定。另外，初始化标志表明初始化过程 1 还是过程 2 在使用。当前主单元时钟(CLK_{27})的MSB是“0”时，它就使用初始化过程 1，当前主单元时钟（CLK_{27}）的MSB是“1”时，它就使用初始化过程 2。从单元应当如初始化标志表述的那样运用初始化方法而不考虑它自己的时钟位值CLK_{27}，主一从呼吸时隙通过主和从在时钟满足以下等式时隙上的初始化而确定。

CLK_{27} mod Tsniff = Dsniff 初始化过程 1

（CLK_{27}，CLK_{26} ）mod Tsniff = Dsniff 初始化过程 2

主一从呼吸时隙通过主单元和从单元在时隙上的初始化而决定，该时隙应当在上面定义的时隙之后定义。初始化后，下一次主一从呼吸（SNIFF）时隙通过增加固定间隔 Tsniff 到当前主一从的呼吸时隙的时钟值上来获得时钟值 CLK(k+1)：

CLK（K+1）= CLK(k)+Tsniff

10.8.3 保持模式

在联机状态下，对从单元的 ACL 链接可以放在 HOLD 模式中。这就意味着从单元暂时不再支持信道上的 ACL 分组 (注意：可能 SCO 链接将仍被支持)。使用保持模式，从单元的能力可被随意的用于其它事请，如扫描，呼叫，查询或加入另一匹克网。在保持模式下的单元也可进入低能耗的睡眠模式。在保持模式中，从单元仍维持它自己的活动成员地址 (AM_ADDR)。

在先前进入保持模式里，主单元和从单元应使从单元在保持模式里持续时间达成一致，并对定时器以 hold TO 值初始化。当定时时间到时，从单元将被唤醒并在信道上同步通信等待主单元的进一步指示。

10.8.4 休眠模式

当从单元退出匹克网信道时，但仍需与信道同步，此时可以进入休眠模式，该模式是从单元处于一种具有很小活力的低能耗模式。在休眠模式下，从单元放弃了它的活动成员地址 AM_ADDR，取而代之的是两个在休眠模式下的新地址：

- PM_ADDR：8 位休眠成员地址。
- AR_ADDR：8 位识别请求地址。

PM_ADDR 把休眠的从单元与其它休眠从单元区别开来，该地址用于主单元初始化非休眠过程。除 PM_ADDR 外，休眠从单元也可以由它的 48 位的 BD_ADDR 唤醒。全 0 的 PM_ADDR 是一个保留的地址：如果休眠单元是全 0 的 PM_ADDR，它只能被 BD_ADDR 唤醒。在那种情况下，PM_ADDR 没有意义。AR_ADDR 在从单元初始化唤醒过程使用。由于缺少 AM_ADDR，则所有送往休眠从单元的消息必须通过广播分组 (全 0 的 AM_ADDR) 传送。.

休眠的从单元为了再次同步和校验广播消息，它被定期间隔地唤醒并监听信道。为了支持同步和休眠从单元的信道识别，主单元提供一个将在下一节中要描述的信标信道。当从单元处于休眠状态时，标志结构传送给从单元。当标志结构改变时，休眠从单元通过广播消息来修改。

休眠模式除了用于低能耗外，还用于向一个主单元提供多于 7 个从单元的链接情况。无论何时，最多只能同时激活 7 个从单元。然而通过交换活动和在匹克网内的休眠从单元分时出现，事实上可以链接的从单元数目可以很大 (若使用 PM_ADDR 时，从单元为 255 个，如使用 BD_ADDR 时，从单元数目可更大)。可被休眠的从单元数目是不受限的。

10.8.4.1 信标信道

为了支持休眠从单元，当一个或多个从单元休眠时，主单元就建立一个信标信道。信标信道由一个信标时隙或等距信标时隙链构成，该链以固定时间间隔作定时性的传送。信标信道如图所示：

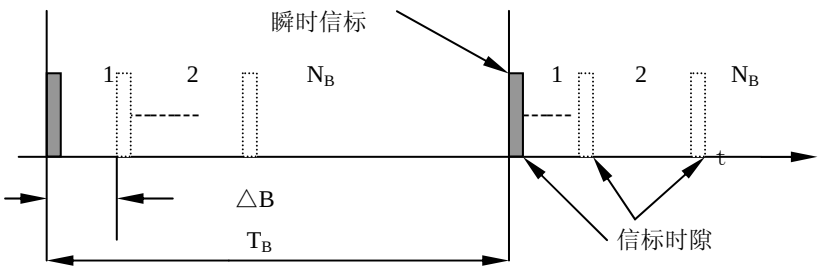


图 2.46 通用信标信道格式

N_B（$N_B \geqslant 1$）信标时隙链由T_B时隙定义。

在链里的信标时隙由△B分开，第一个信标时隙的起点归类于**beacon instant**（瞬时信标）同时作为信标定时参考。如此选取信标参数N_B和T_B是为了在通信质量要求不高的情况下一个确定的时间期内，有充足的信标时隙保证休眠从单元同步。

当休眠时，从单元将通过LMP命令接收信标参数。另外，信标瞬时的定时通过补偿D_B指明。就如SCO链接一样，初始化过程 1 和 2 需使用。 如果当前主单元时钟 (CLK_{27}) 的MSB是 0 时，使用初始化过程 1。如果当前主单元时钟 (CLK_{27}) 的MSB是 1 时主使用初始化过程 2。 在LMP命令中，初始化过程的选择也由初始化标志来执行。从单元应按照初始化标志指出的初始化方法进行初始化而不考虑它的时钟位CLK_{27}。在信标瞬时主一从时隙位置以满足下等式时钟的时隙初始化。

$$CLK_{27-1} \quad \text{mod} \quad T_B = D_B$$

初始化 1

$$(\overline{CLK_{27}}, CLK_{26-1}) \quad \text{mod} \quad T_B = D_B$$

初始化 2

初始化后，下一次信标瞬时的时钟值CLK (k+1) 通过加一个固定间歇T_B到当前信标瞬时的时钟值上得到：

$$CLK\ (k+1) = CLK\ (k) + T_B$$

信标信道用于四个目的：

1. 休眠从单元用于重新同步的主一从分组传送。
2. 向休眠从单元传输改变信标参数消息。
3. 向休眠从单元传输普通广播消息。
4. 唤醒一个或多个休眠从单元。

因为从单元可以和任何分组同步，只要分组前面是合适的信道识别码，在信标时隙上传送的分组不一定必须含有特定的可以和休眠从单元同步的广播分组；能使用的任何分组。置于信标时隙上的唯一要求是有主一从出现。如果无信息可以传送，通过主单元可以传送 NULL 分组。如果确实有广播信息要发送给休眠从单元，广播消息的第一个分组应当在信标时隙链上的每个信标时隙上进行重复传送。然而，类似于 SCO 链接上的同步通信可以中断信标传输。

10.8.4.2 信标识别期

除信标时隙外，休眠从单元可以发送申请要求唤醒的时间点就定义为识别期。为增加可靠性，识别期可以重复 Maccsess 次 (Macccess≧1)，在瞬时信标之后，识别期以一个固定的延迟 Daccess 开始。识别期的宽度为 Taccess。如图所示：

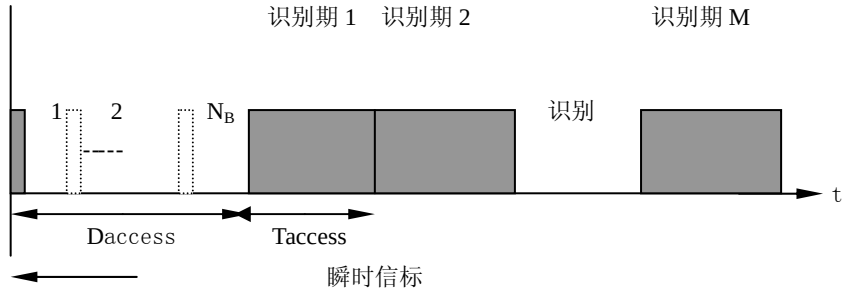


图 2.47 识别期定义

识别期可以支持不同的从单元识别技术，如：POLL 随机识别或其它形式的识别。在该阶段只定义了 POLL 技术。POLL 技术形式如图所示：

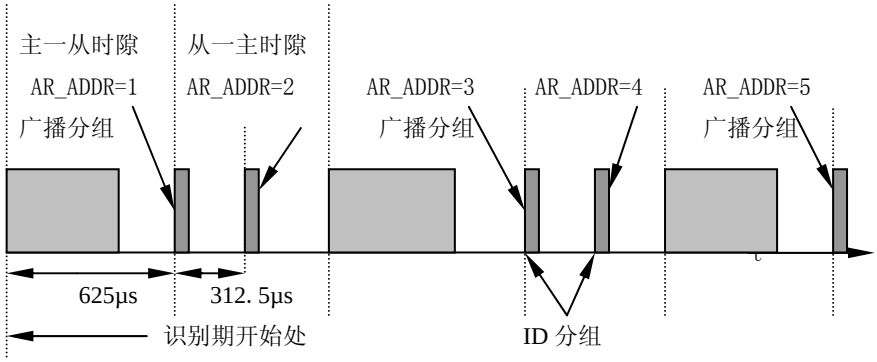
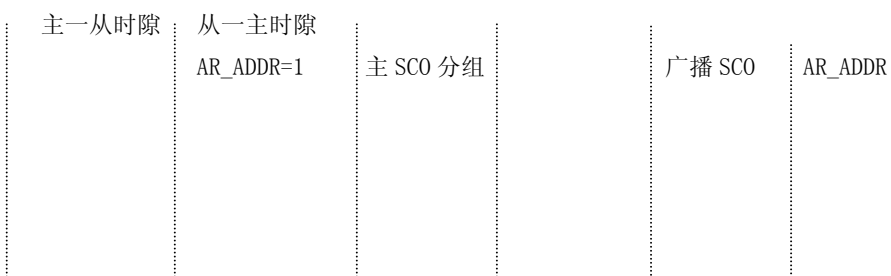


图 2.48 用在轮询技术里的识别过程

相同的 TDD 结构用到了匹克网信道中，即：主一从的传输由从一主传输所替换。从一主时隙被分成了两个都为 312. 5μs 的半时隙。半时隙的休眠从单元允许符合自身识别申请地址 (AR_ADDR) 的应答。半时隙计数决定了识别申请时隙，识别期的开始处使用。

如果在先前的主一从时隙上已接收到了一个广播分组，才允许从单元在适当的从一主半时隙上送出一个识别申请。以这种方法，主单元轮询休眠从单元。

然而，如果有必要的话，识别期上的时隙也可以用于匹克网上的通信。举例来说，如果必须支撑 SCO 联机状态，作为 SCO 链接保留的时隙可以以传送 SCO 信息而不用作识别申请，即：如果识别期中的主一从时隙包含了不同于广播分组的分组，接下来的从一主时隙就不能用于从单元识别申请。据识别结构的定义，在识别期中的时隙不受到仍被使用的通信影响。如果没有中断发生，识别过程仍继续。



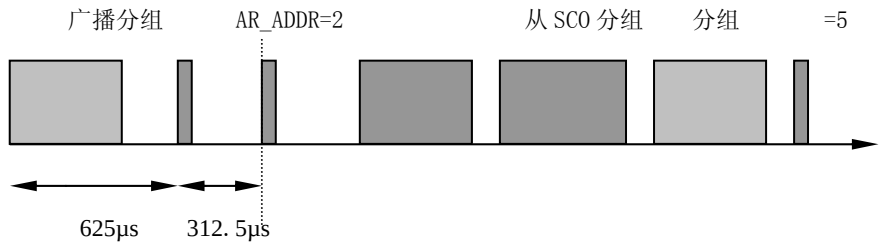


图 2.49 经 SCO 通信识别期的干扰

当从单元休眠时，就决定了将要使用什么样的识别方式。对于 POLL 方式，标出了从一主识别时隙 Nacc-slot 数目。经默认，识别期总是存在的。然而，它的活动取决于主单元在识别期中适当的时隙上向从单元发送广播消息。在信标时隙中的广播 LMP 命令可以指出下一个将不活动的识别期。这避免了要求申请识别休眠从单元的不必要扫描。

10. 8. 4. 3 休眠从单元的同步

休眠从单元大部分的时间都处于睡眠状态。然而，他们定期的唤醒同信道同步。对于同步，在信道上的任何分组交换都是可用的。由于在信标时隙上主单元的传送是强制性的，所以休眠从单元将试着用该信标信道进行重新同步。休眠从单元以信标唤醒而不是在第一个信标时隙上读分组发送。如果失败，它将在信标链重新试下一时隙。总的来说，每个信标有N_B可能性而不是再同步。在查找过程中，从单元可以扩大它的查找期。在信标链里信标时隙间分离△B被选择，以致连续搜寻期不会被复盖。

休眠从单元不必在每个信标瞬间唤醒。睡眠间隔可以比信标间隔T_B宽。

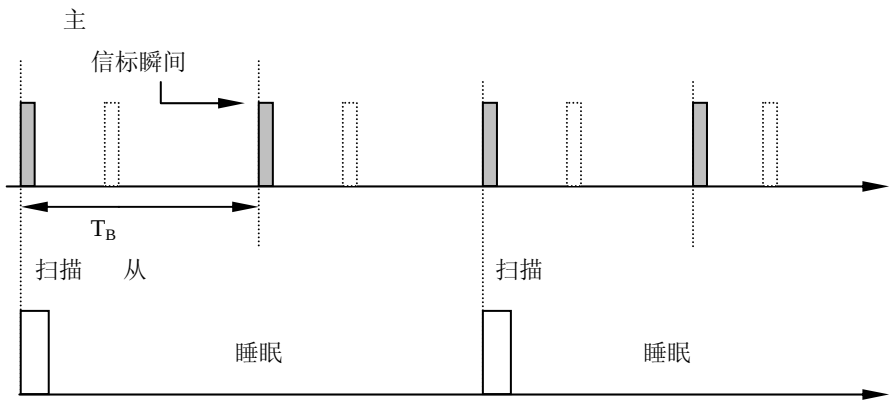


图 2.50 休眠从状态的扩充睡眠间隔

从单元睡眠期必须是T_B 的N_B sleep乘积。从单元唤醒的准确瞬时信标

由使用 D_B sleep 的主单元指出，该D_B sleep指出了关于瞬时信标 （0＜ D_B sleep＜ N_B sleep-1 ）的补偿（ T_B的乘积 ）。 *为初始化唤醒期，下列的等式必须使用：

CLK_{27-1} mod （ D_B sleep * T_B ） = D_B + D_B sleep * T_B 初始化 1

（CLK_{27}，CLK_{26-1}）mod （N_B sleep *T_B ）= D_B + D_B sleep * T_B 初始化 2

如果当前主单元时钟的 MSB 是“0”时，选择初始化 1，在当前主时钟的 MSB 为“1”时，选择初始化 2。

当主单元需传送广播消息给休眠从单元时，作为这些广播消息，它可以使用信标时隙。然而，如果N_B ＜ N_{BC}，在信标链里的紧跟在最后一个信标时隙后的时隙将用于剩下的N_{BC}－N_B广播分组。如果N_B > N_{BC} ，广播消息在所有N_B信标时隙上被重复。

在被唤醒的信标时隙里，休眠从单元至少读传送的广播信息。最小唤醒活动就是要读取用于重新同步的信道识别码和用于广播消息的分组头。

10.8.4.4 休眠

主单元可以通过一个或几个 LMP 命令的交换来休眠一个活动从单元。在进入休眠模式前，从单元要分配一个 PM_ADDR 和 AR_DDR。每个休眠从单元具有一个唯一的 PM_ADDR，而 AR_DDR 却不一定是唯一的。当从单元休眠时，信标参数也由主单元给出，随后从单元放弃它的 AM_DDR 而进入休眠模式。主单元一次只能休眠一个从单元。休眠消息通过普通的数据分组来传送且从单元通过它的 AM_DDR 编址。

10.8.4.5 主激活解除休眠

主单元可以通过传送专用的 LMP 含有休眠从单元地址的解除休眠命令，来激活一个休眠的从单元。该消息在信标时隙上的广播分组传送，要么使用从单元的 PM_ADDR，要么使用它的整个 BD_ADDR。在从单元重新进入匹克网后含有活动成员地址 AM_ADDR 的消息从单元可使用。唤醒消息可含有从单元地址的数目，所以多个从单元可同时唤醒。对每个从单元都赋予了一个不同的 AM_ADDR。.

在收到解除休眠消息后，休眠从单元匹配 PM_ADDR 或 BD_ADDR 并退出休眠模式而进入活动模式。它将持续地从主单元处监听信息直到它 AM_ADDR 经主单元批准。经主单元发送的第一个分组是一个 POLL 分组，

对 POLL 分组的应答返回分组证实了从单元已解除了休眠。如果在信标重复期结束后，作为新联机时隙数 POLL 分组从单元还没收到，从单元用相同的信标参数返回到休眠状态。在证实了从单元为活动状态后，主单元将决定从单元继续采用什么模式。

10.8.4.6 从激活解除休眠

从单元可以通过定义的识别期要求识别信道。识别期含有几个从一主半时隙，这些半时隙从单元可以发出识别请求消息。特定的半时隙从单元允许响应，当从单元休眠时，符合它接收到的识别请求地址（AM_ADDR）。半时隙的次序没固定，在信标时隙里的 LMP 命令可以重设识别期。当从单元企图登录信道时，它就在一个合适的从一主半时隙上发出一个申请登录消息。从单元的申请登录消息是包含主单元设备识别码 (DAC) 的 ID 分组 (在这种情况下，ID 分组是一个没有分组尾的信道识别码)。当在先前的主一从时隙上收到一个广播分组时，只允许休眠从单元在半时隙上传送一个申请登录信息，这个广播信息可以包含任何一种广播信息，而不一定和休眠从单元有关。如果没有广播信息，就应当传送一个广 播 NULL 或广播 POLL 分组。

在发出一个识别申请后，休眠从单元监听来自主单元的解除休眠信息。只要没接收到解除休眠信息，从就在接下来的识别期中重复识别申请。在最后一个识别期 (总共有 Maccess 个期) 之后，休眠从单元监听附加的解除休眠消息 Npoll 个时隙。如果在 Npoll 时隙内没收到解除消息，在上次识别期结束后，从单元可返回睡眠状态而且在下一个瞬时信标后可重试登录申请。

在收到解除休眠消息后，匹配 PM_ADDR 或 BD_ADDR 的休眠从单元将退出休眠模式而进入活动模式。它将继续监听主单元，直到主单元通过它的 AM_ADDR 完成编址。由主单元第一个传送的分组应是一个 POLL 分组。在响应 POLL 分组的返回分组证实从单元已被解除休眠。如果来自从单元接收的新联机时隙数没有应答分组，在最后一个识别期结束后，主单元将再次发送解除消息给从单元。如果从单元在 Npoll 时隙后没收到用于新联机时隙数的 POLL 分组，在最后一个识别期结束后，从单元将以相同的信标参数返回休眠状态。在证实了从单元是活动状态后，主单元就决定从单元将工作于什么模式。

10.8.4.7 广播扫描期

在信标链里，主单元可以支持对休眠从单元广播消息。然而，通过指明较多紧随信标链后广播信息的分组从单元，其主单元的广播能力可以扩充。在限定的时间期内，休眠从单元 (活动从单元一样) 监听广播消息信

道经特定的 LMP 命令序列来实现。该时间以瞬时信标开始并且持续到在信标尾作为指出 LMP 命令发送的时间。

10.8.5 轮询（Polling）方式

10.8.5.1 活动模式下的轮询

主单元总是完全控制匹克网。由于严格的 TDD 方式，从单元只能同主单元进行通信而不能同其它从单元进行通信。为了防止在 ACL 链接上的冲突，当通过在先前的主一从时隙分组头中的 AM_ADDR 编址时，从单元才允许在从一主时隙上传送信息。如果在先前时隙上的 AM_ADDR 不匹配，或 AM_ADDR 不能从先前的时隙里分离出来，从单元就不允许传送信息。

在 SCO 链接上，轮询规则可稍作修改。从单元允许在 SCO 链接保留的时隙上传输信息，除非先前时隙里的 (有效的) AM_ADDR 指出了另一个不同的从单元。如果无有效 AM_ADDR 能从先前时隙里分离出来，从单元仍允许在保留的 SCO 时隙上传送信息。

10.8.5.2 休眠模式下的轮询

在休眠模式下，休眠从单元允许在识别期传送识别请求，该识别期提供了在先前主一从时隙中接收到的广播分组。在活动模式下的从单元不再紧随广播分组后的从一主时隙上传送信息，它只允许以特定编址传送信息。

10.8.6 时隙保留方式

SCO链接的建立是通过链接管理器之间的协商来完成的。该链接管理器包含有类似于经 LMP消息的T_{SCO}和D_{SCO}重要SCO定时参数的交换。

10.8.7 广播方式

匹克网中的主单元可以广播能到达所有从单元的信息。广播分组具有全零的 AM_ADDR 特性。每个新的广播信息 (许多分组都带有) 都由刷新指示开始 (L_CH=10)。

广播分组不需确认。在通信质量要求不高的环境中，主单元可以执行N_{BC}次重传，以增加无差错传送的可能性。

为了支持休眠模式，主单元传输将以固定间隔实现。主单元传输作为从单元可同步的信标动作。如果在信标事件中没有通信产生，将传送广播分组。

10.8 散射网

10.9.1 概述

一个相同区域可具有多个匹克网。由于各匹克网有自己的主单元（匹克网的跳频相互独立）， 所以各匹克网有自己的信道跳频序列和状态且由各自的主单元确定。另外，处于信道分组前的不同信道识别码由主单元设备地址决定。由于增加了较多的匹克网，冲突的可能性也增加了，在跳频及扩频系统里，性能的适当降低是常见的。

如果多匹克网复盖了相同区域，一个单元可通过使用时间多路复用器为两个以上的复盖匹克网共享。为了共享适当的信道，它将使用相关的主单元设备地址和适当的时钟补偿来获取正确的时段。一个蓝牙单元能够在几个匹克网里当作从单元活动，但单个匹克网里只能有一个是主单元。由于使用相同主单元的两个匹克网是同步的，而且使用了相同的跳频序列，所以它们就成了同一个匹克网。构成不同匹克网间链接的一组匹克网就称为散射网。

主单元或从单元通过另外匹克网的主单元呼叫，能够变为另一个匹克网中的从单元。换句话说，一个匹克网的单元可以呼叫另一个匹克网中的主单元或从单元。由于呼叫单元总是以主单元身份出现，如果需要一个从单元时，就要有一个主一从角色互换。

10.9.2 匹克网间通信

时间多路复用器用于匹克网间切换。假使只有 ACL 链接，单元可以在当前匹克网里进入保持或休眠模式，此时它可通过改变信道参数而加入另外的匹克网。呼吸模式下的单元，在两个呼吸时隙之间，有充足的时间访问另外的匹克网。如果 SCO 链接已经建立，只能在链接两者间的非保留时隙上访问其它匹克网。如果有单个 SCO 链接，使用 HV3 分组是唯一可能的。在四时隙的链接间，一个其它的匹克网可以被访问。由于多匹克网不能被同步，为说明未对准，保护时间必须撤离。这意指 HV3 分组间，只有两个时隙能被有效地用于访问另外的匹克网。

因为不同匹克网中的两个主单元时钟不同步，由两个匹克网共享的从单元必须兼顾两个补偿，加它自己的本地时钟外，再创建一个或其它的一个主时钟。由于两个主时钟独立地发生时间漂移，为保证从单元与两个主单元同步，所以定期地修改补偿值。

10.9.3 主一从切换

原则上讲，创建匹克网的单元是主单元。然而，当从单元企图变成主单元时，主一从 (MS) 切换产生。对于包含在切换中的两个单元，MS 切换导致了它们 TX 和 RX 定时的颠倒：TDD 切换。然而，因匹克网参数取

自设备地址和主时钟地址，主一从切换也自然包含了匹克网的重新定义：匹克网切换。新的匹克网中的参数取自从单元的设备地址和时钟，正如匹克网切换推论，不包含在切换中匹克网的其它从单元必须进入新的匹克网，改变它们的定时和跳频方式。新的匹克网参数必须传给每一个从单元。为实现下面的描述，假设单元 A 欲想成为主单元；单元 B 是以前的主单元。步骤出现如下：

- 从单元 A 和主单元 B 同意互换角色。
- 当两个单元确认后，从单元 A 和主单元 B 作 TDD 切换，但保留以前的跳频序列（仍然使用单元 B 的设备地址和时钟），所以还未产生匹克网切换。
- 单元 A 现在是匹克网的主单元。因旧的和新的主单元时钟是异步的，FHS 分组中提供的 1.25ms 时钟信息分辨率还不足以划分两个匹克网的时隙上下限。在传送 FHS 分组之前，新的主单元 A 传送一个 LMP 分组给出在旧的主一从时隙和新的匹克网信道间延迟。该定时信息可取 0 到 1249μs 之间的值，其分辨率是 1μs。当切换到新主单元定时器时，在 FHS 分组确认后，它和 FHS 分组的时钟信息一起用来精确定位相互关系期。
- 在时间对准 LMP 信息后，主单元 A 送出一个包含新的 AM_ADDR 的 FHS 分组给从单元 B （FHS 分组头的 AM_ADDR 是全零的地址）仍用原来的匹克网参数。在 FHS 确认后，构成了 ID 分组，该分组在原跳频序列上由从单元传送，主单元 A 和从单元 B 转向通过 FHS 和时间对准 LMP 分组（至少对 A 一 B 联机）指出新匹克网的新信道参数。
- 在各个从单元上匹克网切换是单独实施。主单元 A 送出一个时间校准和一个 FHS 分组并等待确认。FHS 分组的传送和确认在单元 B 的旧匹克网参数上继续。经从单元发送用 ID 分组的 FHS 在确认后，从单元继续使用单元 A 的新设备地址和时钟通信。传送给每个从单元的 FHS 分组有在 FHS 分组头里旧的 AM_ADDR 和在 FHS 分组有效载荷里它们的新 AM_ADDR（新的 AM_ADDR 可能与旧的 AM_ADDR 相同）。
- 在接收到 FHS 分组确认后，新的主单元 A 切换它的定时并传送一个 POLL 分组来核查该切换。主单元和从单元都在用新联机 FHS 分组确认超时上启动。如果没有响应接收到，主单元发送 POLL 分组直到新联机收到。在超时后，从单元和主单元都返回到旧的匹克网定时（但仍是 TDD 切换）。 主单元再次传送 FHS 分组且该过程重复。
- 在旧的匹克网中，对每个从单元，新的主单元重复以上过程。

总之，MS 切换分两步完成：首先考虑主单元和从单元的 TDD 切换，然后所有参与者的匹克网切换。当所有的从单元都确认收到 FHS 分组时，每个单元都使用由新的主单元和匹克网定义新的匹克网参数是实际的。旧

从单元的 AM_ADDR,PM_ADDR 和其它属性信息,由旧主单元传送给新主单元,该过程的传送范围不在过程之内。休眠从单元的激活（使用旧休眠参数),变为新的匹克网参数，然后使用新的休眠参数返回休眠模式。

10.10 电量管理

为了确保低功耗，蓝牙具有一些特性。当处理分组时这些特性都是微观级且在微观级使用特定操作模式。

10.10.1 分组处理

为了减少功耗，分组处理在 TX 和 RX 方面被最小化。在 TX 方面，功率通过仅传送有效载荷实现最小化。这意味着如果只有链接控制信息需要交换的话，将使用 NULL 分组。如果没有链接控制信息或者只涉及到 NAK (NAK 是固有不响应的)，就完全没有传输执行。如果有数据传送，只传送有价值数据字节，则有效载荷长度适合的。在 RX 方面，分组加工发生在不同步步骤里。如果在搜索期没有发现有效识别码，收、发信机器返回到睡眠状态，如果发现了识别码，唤醒接收机单元并开始加工分组头。如果 HEC 失败，在分组头后单元将返回到睡眠。有效头指出是否有有效载荷紧随其后及含有多少时隙。

10.10.2 时隙占用

分组类型指出了分组可占用多少时隙。在第一个时隙中，未编址的从单元可用分组占有的剩余时隙中进入睡眠。它可从 TYPE 代码中读出。

10.10.3 低功耗模式

在减少功耗的联机状态中，描述了三种模式。如果我们把这些模式按功耗递增顺序排序，那么呼吸模式功耗较高，然后是保持模式，具有最低功耗的是休眠模式。

10.11 链接管理

有很多原因都能引起联机中断，如一台设备超出了功率故障范围。这种情况的发生是没有任何提前告警，所以当 AM_ADDR 重新分配给另一个从单元时，链接主单元和从单元两边的监控器尽可能的避免这种冲突。

为能管理链接损失，主单元和从单元都使用了链接管理定时器，T supervision。只要收到经过 HEC 校验的分组和有正确的 AM_ADDR，定时器就被复位。如果在联机转态的任何时间，定时器达到管理值，联机复位。SCO 和 ACL 联机都使用同一个超时值。

超时期间在 LM 层上处理，它的值经选择后，导致管理超时比保持和呼

吸期要长。休眠从单元链接管理将通过对从单元的解除休眠和重新休眠来实现。

11．跳频选择

总共有 10 类跳频序列。79 跳和 23 跳系统各占 5 类。使用圆括号内的数字与 23 跳系统有关，其序列为：

- **呼叫跳频序列：** 该序列带有 32 (16) 个唯一唤醒频率分布在 79 (23) MHz 上，具有 32 (16) 的长度区域。
- **呼叫响应序列：**该序列复盖 32 (16) 个唯一与当前呼叫跳频序列一一对应的响应频率。主单元和从单元使用不同规则获得相同序列。
- **查询序列：** 该序列带有唯一的在 79 (23) MHz 上分布的 32 (16) 唤醒频率，具有 32 (16) 的长度区域。
- **查询响应序列：**该序列复盖 32 (16) 个唯一与当前查询跳频一一 对应的响应频率。
- **信道跳频序列：**该序列有一个非常长时期，它并不表明重复模式复盖短时间间隔，在短时间间隔中，该序列分布在 79 (23) 跳频频率上。

对于呼叫跳频序列来说，重要的是我们能很容易的使状态前后漂移，所以我们需要从计数器到跳频序列的 1-1 映射。对于每种情况，都需要从一主和主一从的两种跳频序列。

查询和查询响应序列总是利用 GIAC LAP 作为低地址而 DCI 作高地址部分。这些是取自于跳频序列的过程中，甚至和 DIAC 查询有关。

11.1 一般选择方案

选择方案由两部分组成：

- 选择一个序列；
- 在跳频频率上映射该序列；

跳频选择方案的一般框图如图所示：

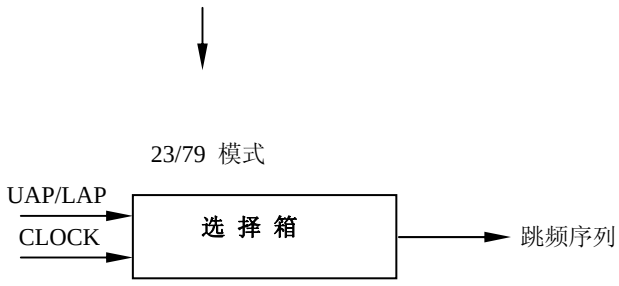


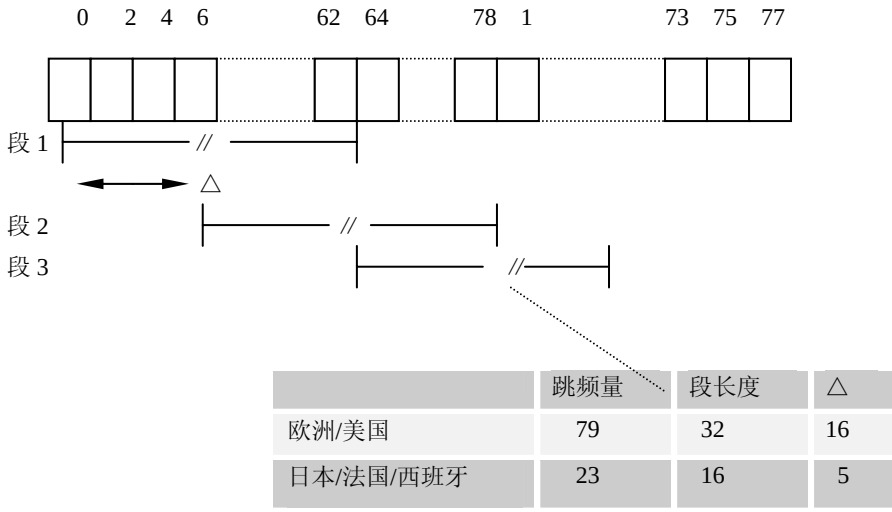
图 2.51 跳频选择方案的一般框图

从输入到特定的跳频序列映射在选择箱内完成。基本上，输入是本地时钟和当前地址。在联机状态下，本地时钟 (CLKN) 经相等主时钟 (CLK)

的 补偿修改，只有时钟的 27 位MSB_S才被使用。在呼叫和查询分状态下，时钟的整个 28 位都要使用。然而，在呼叫状态下，本地时钟将被修改为对呼叫单元的主单元的估算值。

地址输入由 28 位组成，即整个 LAP 和 UAP 的 4LSB。在联机状态里，使用主单元的地址。在呼叫状态下使用呼叫单元地址。当为查询状态时，使用和 GIAC 对应的 UAP/LAP。输出由一个伪随机序列构成，或复盖 79 跳或复盖 23 跳系统，取决于是什么状态。

对于 79 跳系统，选择方式选定生成约 64MHz 的 32 跳频段，并以随机次序访问这些跳频点一次。接下来选择一个不同的 32 跳频段，依次类推。对于呼叫和呼叫响应状态，使用同一 32 跳段 (该段由地址选择，不同的单元将有不同的呼出段)。 在联机状态下，输出由在 79 跳或 23 跳里变动的伪随机序列构成，这依取决于选择的跳频系统。对于 23 跳系统，段大小是 16，其原理如图所示：

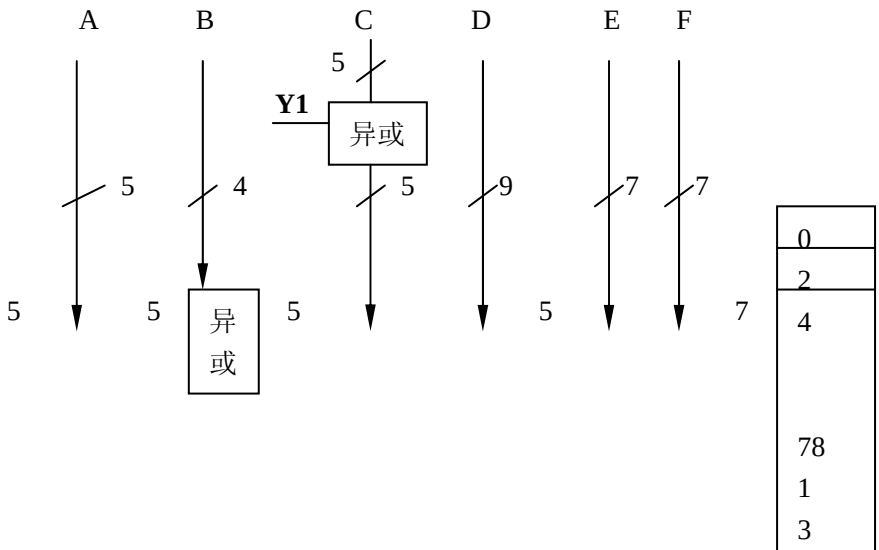


	跳频量	段长度	△
欧洲/美国	79	32	16
日本/法国/西班牙	23	16	5

图 2.52 联机状态下的跳频选择方案

11.2 选择内核

79 跳和 23 跳系统的跳频选择内核如图所示：



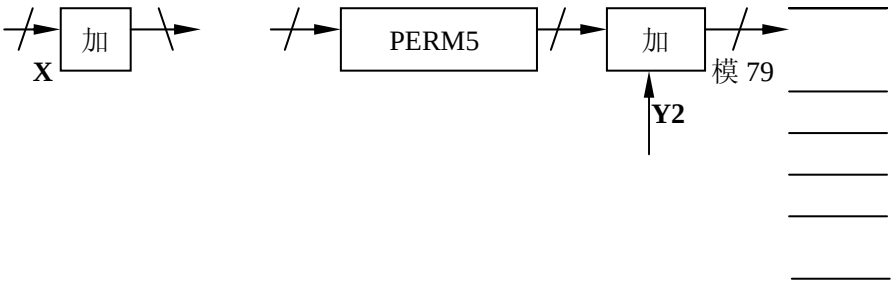


图 2.53　79 跳频系统跳频选择内核框图

X 输入决定了 32 跳频段，Y1 和 Y2 在主一从及从一主传输之间选择。输入 A 到 D 决定了段内顺序，输入 E 到 F 决定了对跳频频率的映射。内核编址含有跳频频率的寄存器。该序列将以先是所有偶数跳频频率，然后是所有奇数跳频频率创建。这样，32 跳系统将跨越 64MHz，而 16 跳系统将跨越总共 23MHz。

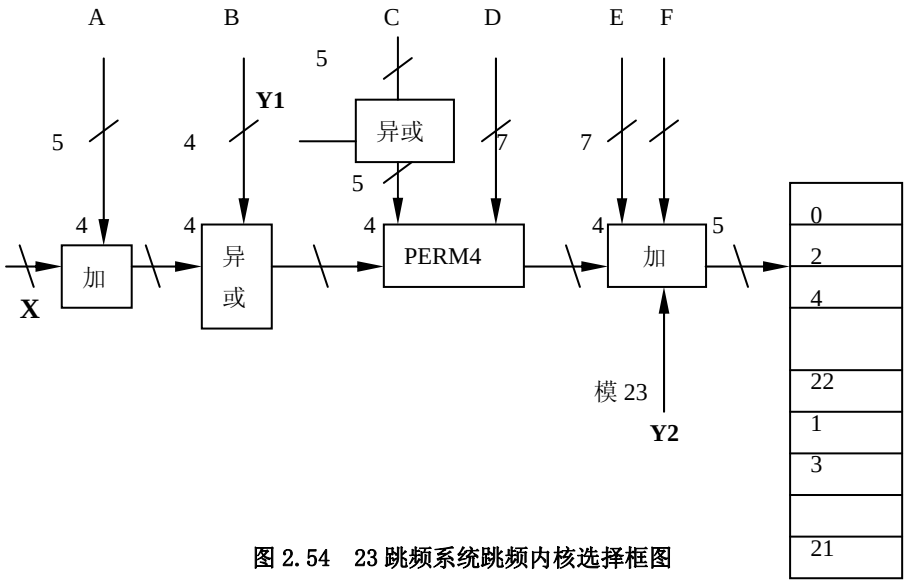


图 2. 54　23 跳频系统跳频内核选择框图

选择过程由第一加法操作，XOR操作，排列操作，第二加法操作和最终寄存器选择组成。在本章的其余部分，记号A_J用来表示BD_ADDR的第J位。

11. 2. 1　第一加法操作

第一加法操作仅在该阶段上加一个常数并对 32 或对 16 求模。对于呼叫跳频序列，第一加法是冗余的，因为它仅在段内改变状态。然而，当不同段的链接 (就像在信道跳频序列中一样) 时，第一加法操作将给结果序列造成影响。

11.2.2 XOR 操作

用Z'来表示第一加法的输出。在XOR操作中，Z'的 4 个LSB与地址位$A_{22\text{-}29}$作模 2 的异或运算。该操作如图所示：

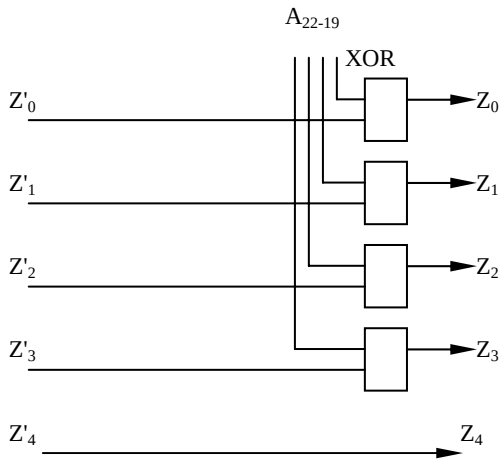


图 2.55 79－跳频系统的 XOR 操作

11.2.3 排列操作

排列操作包含了从 5 输入到 5 输出 79 跳系统中切换和 4 输入到 4 输出 23 跳系统中切换。采取由控制字控制的方式。用图来说明排列和切换箱。蝶型操作由 7 个步骤构成，下表说明了经控制信号P对蝶型控制。注意：$P_{0\text{-}8}$对应$D_{0\text{-}8}$，而Pi+9 对应于Ci ⊕Y1 i=0, 1. . . . 4。

表 2.18 79 跳系统蝶型控制

控制信号	蝶 型	控制信号	蝶 型
P0	{Z_0，Z_1}	P8	{Z_1，Z_4}
P1	{Z_2，Z_3}	P9	{Z_0，Z_3}
P2	{Z_1，Z_2}	P10	{Z_2，Z_4}
P3	{Z_3，Z_4}	P11	{Z_1，Z_3}
P4	{Z_0，Z_4}	P12	{Z_0，Z_3}
P5	{Z_1，Z_3}	P13	{Z_1，Z_2}
P6	{Z_0，Z_2}		
P7	{Z_3，Z_4}		

表 2.19 23 跳系统蝶型控制

控制信号	蝶 型	控制信号	蝶 型

P0	{Z_0，Z_1}	P8	{Z_0，Z_2}
P1	{Z_2，Z_3}	P9	{Z_1，Z_3}
P2	{Z_0，Z_3}	P10	{Z_0，Z_3}
P3	{Z_1，Z_2}	P11	{Z_1，Z_2}
P4	{Z_0，Z_2}	P12	{Z_0，Z_1}
P5	{Z_1，Z_3}	P13	{Z_2，Z_3}
P6	{Z_0，Z_1}		
P7	{Z_2，Z_3}		

就像前一节描述的那样，Z 输入是 XOR 操作输出。蝶型操作可用以前描述的多路复用器来实现。

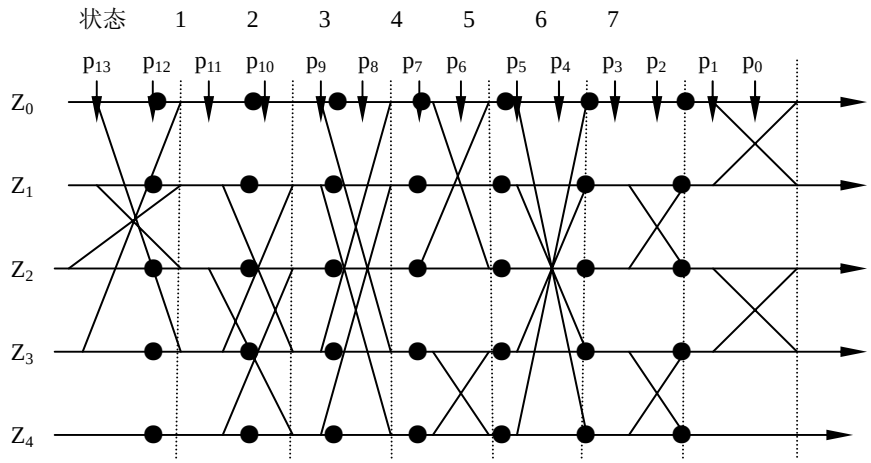
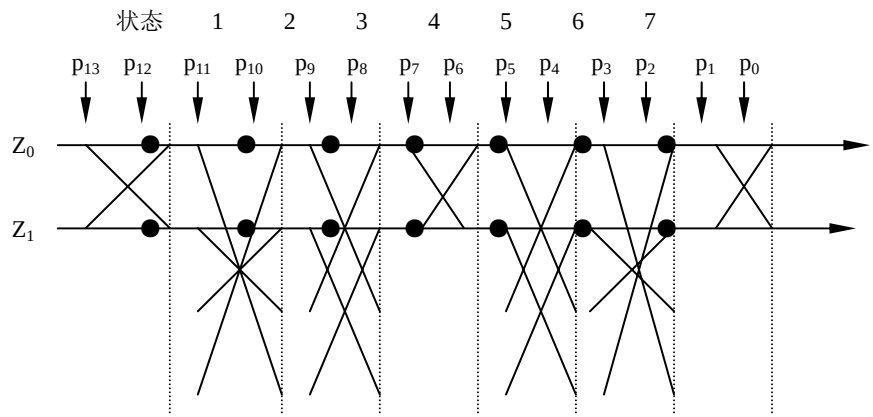


图 2.56 79 跳系统的排列操作



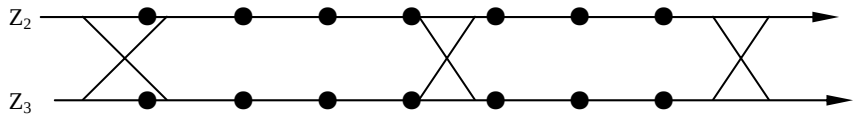


图 2.57　23 跳系统的排列操作

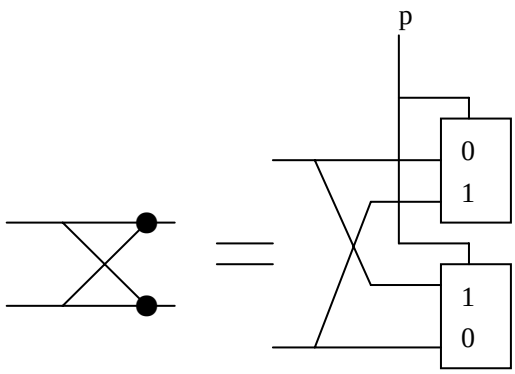


图 2.58　蝶型实现

11.2.4　第二加法操作

加法操作只在排列操作输出上增加一个常数。结果 16 跳或 32 跳的段映射到不同的跳频频率上。加法采用模 79 或模 23 取决于系统类型　(欧洲/美国或其它国家)。

11.2.5　寄存器组

加法器的输出编址为 79 或 23 跳系统寄存器组。寄存器用符合跳频频率 0 到 78 或 0 到 22 的同步代码字装入。注意：寄存器组的高半部分包含偶数跳频频率，寄存器组的低半部分包含奇数跳频频率。

11.3　控制字

在下节中，Xj-i，i<j，表示矢量X的i ，i+1，j位，X_0，是矢量X的有效低位。

核心控制字P由控制信号X，Y1，Y2，和A到F来控制。在呼叫和查询过程中，输入A到输出E使用上述两表中相应栏中所给出的地址值。另外，还使用输入X，Y1 和Y2。没使用输入F。在 79 跳系统中，时钟位CLK_{6-2} (即输入X) 指定长度为 32 的序列中的状态，而在 23 跳系统中，CLK_{5-2}指定长度为 16 的序列中的状态。对两种系统来说，CLK_1 (即输入Y1 和Y2) 都用于TX和RX之间的选择。输入地址决定了段内的序列顺序。对跳频的最终

映射由寄存器内容决定。

以下，我们将对时钟的三种类型作出区分，这三种时钟类型是：匹克网的主时钟、蓝牙单元的本地时钟和呼叫蓝牙单元的时钟估算值。这些类型以下形式标注：

1．CLK_{27-0}：　当前匹克网的主时钟。

2．$CLKN_{27-0}$：　单元的本地时钟。

3．$CLKE_{27-0}$：　呼叫单元本地时钟的呼叫单元估算。.

在联机状态中，输入 A，C 和 D 是地址与时钟的 XOR 结果，这将在下面两表中说明 (两个 MSB 一起作 XOR，第二个 MSB 一起作 XOR 等)。因而，在每一个 32 (16) 时间时隙后，在 79 跳 (23 跳频) 系统中，就选择一个新的长度为 32 (16) 的段。在一个特定段中序列顺序在很长时间内不被重复。于是，整个跳频序列由各个 32 跳段构成。由于每个 32 跳序列都跨越了 79MHz 频带 80%多的部分，希望扩频在短时间隔上获得。

表 2.20 控制 79 跳系统

	呼叫/查询扫描	呼叫/查询	呼叫/查询响应（主/从）	联机状态
X	$CLKN_{16-12}$	$Xp_{4-0}^{(79)}/Xi_{4-0}^{(79)}$	$Xprm_{4-0}^{(79)}/Xirs_{4-0}^{(79)}$	$CLKN_{6-2}$
Y1	0	$CLKE_1/CLKN_1$	$CLKE_1/CLKN_1$	CLK_1
Y2	0	$32 \times CLKE_1$ / $32 \times CLKN_1$	$32 \times CLKE_1$ / $32 \times CLKN_1$	$32 \times CLK_1$
A	A_{27-23}	A_{27-23}	A_{27-23}	$A_{27-23} \oplus CLK_{25-21}$
B	A_{22-19}	A_{22-19}	A_{22-19}	A_{22-19}
C	$A_{8,\ 6,\ 4,\ 2,\ 0}$	$A_{8,\ 6,\ 4,\ 2,\ 0}$	$A_{8,\ 6,\ 4,\ 2,\ 0}$	$A_{8,\ 6,\ 4,\ 2,\ 0} \oplus CLK_{20-16}$
D	A_{18-10}	A_{18-10}	A_{18-10}	$A_{18-10} \oplus CLK_{15-7}$
E	$A_{13,\ 11,\ 9,\ 7,\ 5,\ 3,\ 1}$	$A_{13,\ 11,\ 9,\ 7,\ 5,\ 3,\ 1}$	$A_{13,\ 11,\ 9,\ 7,\ 5,\ 3,\ 1}$	$A_{13,\ 11,\ 9,\ 7,\ 5,\ 3,\ 1}$
F	0	0	0	$16 \times CLK_{27-7} \bmod 79$

表 2.21　控制 23 跳系统

	呼叫/查询扫描	呼叫/查询	呼叫/查询响应（主/从）	联机状态
X	$CLKN_{15-12}$	$Xp_{3-0}^{(23)}/Xi_{3-0}^{(23)}$	$Xprm_{3-0}^{(23)}/Xirs_{3-0}^{(23)}$	$CLKN_{5-2}$
Y1	0	$CLKE_1/CLKN_1$	$CLKE_1/CLKN_1$	CLK_1
Y2	0	$16 \times CLKE_1$ / $16 \times CLKN_1$	$16 \times CLKE_1$ / $16 \times CLKN_1$	$16 \times CLK_1$

A	A_{27-23}	A_{27-23}	A_{27-23}	$A_{27-23} \oplus CLK_{25-21}$
B	A_{22-19}	A_{22-19}	A_{22-19}	A_{22-19}
C	$A_{8, 6, 4, 2, 0}$	$A_{8, 6, 4, 2, 0}$	$A_{8, 6, 4, 2, 0}$	$A_{8, 6, 4, 2, 0} \oplus CLK_{20-16}$
D	A_{18-10}	A_{18-10}	A_{18-10}	$A_{18-10} \oplus CLK_{15-7}$
E	$A_{13, 11, 9, 7, 5, 3, 1}$	$A_{13, 11, 9, 7, 5, 3, 1}$	$A_{13, 11, 9, 7, 5, 3, 1}$	$A_{13, 11, 9, 7, 5, 3, 1}$
F	0	0	0	$8 \times CLK_{27-6}$ mod 23

11.3.1 呼叫扫描和查询扫描状态

在呼叫扫描中，扫描单元的蓝牙设备地址用作地址输入。在查询扫描中，GIAC LAP和DCI （如：A_{27-24}）的四个LSB_S用作跳频序列的地址输入。通常，传送识别码和接收器的相关器中使用GIAC和DIAC。决定使用哪一个查询识别码的使用取决于查询的目的。

5 个 X 输入位变化取决于单元的当前状态。在呼叫扫描和查询扫描状态中，使用本地时钟(CLKN)。在联机状态中，主单元时钟 (CLK) 用作输入。对于其它状态，情况有些复杂。

11.3.2 呼叫状态

在 79 跳系统的呼叫状态中，呼出单元将使用 A 队列启动，即：{f(k-8),...f(k),...f(+7),...}，这里 f(k)是在呼入单元里当前接收器频率的估算。很清楚，标志 k 是所有输入的一个函数。在每 1.28 秒间隔中，就有 32 个可能的呼出频率。这些频率中的一半属于 A 队列，剩下的 (即：{f(k+8),...f(k+15),f(k-16),...f(k-9)}) 属于 B 队列。为了到达 A 队列的-8 补偿，可以在时钟位上加一个常数 24 (这就相当于对模 32 减 8 求其补数)。很明显，B 队列可以通过对 8 加补偿来实现。为避免在呼出和扫描单元间可能重复的匹配，队列内顺序也要作周期性地变化。于是：

$Xp^{(79)} = [CLKE_{16-12}+k_{offset}+(CLKE_{4-2,0}-CLKE_{16-12}) \text{ mod } 16] \text{ mod } 32$ （等式 2）

这里，

$$k_{offset}=\begin{cases}24 & \text{A 队列}\\ -8 & \text{B 队列}\end{cases}$$

（等式 3）。

两者挑一地，A和B队列的每次切换都可以通过在k_{offset}当前值上增加 16 来完成 (初始值为 24)。

在 23 跳系统的呼叫状态中，呼出单元只使用 A 队列。为了使用 f(k-8)开始，使用 8 的常量补偿。此外，因以 16 为模作加法，所以只需要 4 位。.因此：

$$Xp^{(23)} = [CLKE_{15-12}+8+CLKE_{4-2,0}] \quad mod \quad 16$$

（等式 4）。

11.3.3 呼叫响应

11.3.3.1 从单元响应

在呼叫扫描分状态中的单元确认自己的识别码就进入从单元响应状态。由于不符合本地时钟CLKN和主单元的时钟估算值CLKE，为了消除因链接而造成损耗可能性，四个$CLKN_{16-12}$,位必须以当前值冻结。这个值被冻结为接受器识别码被检测的时隙中的内容。注意，实际本地时钟并没停止；仅仅是用来产生X-输入的位被固定了一会儿。然后，冻结的值用星号(*)作标志。

对每一个响应时隙，呼入单元将使用一个 X-输入值，不再大于（模 32 或 16）先前响应时隙。然而，第一次响应时，用 X-输入保持为识别码被确认时的值来构成。设 N 是从 0 开始的记数器，那么，第 (N+1) 次响应时隙 (第一次响应时隙紧随在现在响应呼叫时隙后的时隙) 的 X-输入成为：

$$Xprs^{(79)} = [CLKE^{*}_{16-12}+N] \quad mod \quad 32$$

（等式 5）

$$Xprs^{(23)} = [CLKE^{*}_{15-12}+N] \quad mod \quad 16$$

（等式 6）

以上等式分别为作为 79 跳和 23 跳系统。

在从单元确认呼叫的时隙里的计数器N被置为零。然后，每次$CLKN_1$被置为零时计数器的值就加 1，它符合主单元的TX 时隙的开始。在该从单元使用在FHS分组里收到的参数进入联机状态后，以该方式构成的X-输入直到第一个FHS分组收到和接下来响应分组被传输。

11.3.3.2 主单元响应

呼出单元收到从单元的响应就进入主单元响应状态。很明显，主单元也必须把它的从时钟的估算值冻结为引发被呼叫单元而来响应值。当接收从单元响应时 (因为只有$CLKE_1$与相应的呼叫传送不同)，相当于使用时钟估算计值。这样，当从单元的ID分组接收到时，其值被冻结。除使用时钟位外，k_{offset}的当前值也必须冻结。主单元将以呼入单元的做法一样调整它的X-输入，即：在每一次$CLKE_1$置为 0 时此值加 1。在发送FHS 分组到呼入单元前，第一次增值应完成。设N为从 1 开始的计数器，形成X-输入的规则为：

$Xprm^{(79)} = [CLKE^{*}_{16-12} + k_{offset}{}^{*} + (CLKE^{*}_{4-2\cdot0} - CLKE^{*}_{16-12}) \bmod 16 + N] \bmod 32$
（等式 7）

$Xprm^{(23)} = [CLKE^{*}_{15-12} + 8 + CLKE^{*}_{4-2\cdot0} + N] \bmod 16$
（等式 8）

以上等式分别为 79 跳和 23 跳系统。

每次 CLKE1 的值置为 0 时，N 值加 1，这与主单元的 TX 时隙的启动相符。

11.3.4 查询状态

查询状态的 X-输入与呼叫状态中使用的 X-输入十分相似。因为没有实际单元被编址，所以使用查询者的本地时钟 CLKN。此外，两个队列补偿的哪一个作为启动在这个状态中无关紧要的。因而，

$$Xi^{(79)} = [CLKE_{16-12} + k_{offset} + (CLKE_{4-2\cdot0} - CLKE_{16-12}) \bmod 16] \bmod 32$$
（等式 9）

这里k_{offset} 由 (EQ3) 来确定。这个补偿的初始值的选择是任意的。. 对于 23 跳系统

$$Xi^{(23)} = [CLKE_{15-12} + 8 + CLKE_{4-2\cdot0}] \bmod 16$$
（等式 10）

GIAC LAP和四个LSB_S (A_{27-24}) 用作跳频序列发生器的地址输入。

11.3.5 查询响应

查询响应状态类似于接收X-输入的从单元响应状态。 这样 (EQ5) 和 (EQ6) 保持。然而，计数器N不是在$CLKN_1$的基础上增加，而是在每次FHS分组被传送给查询者作为响应后增加。

GIAC LAP和DCI的四个LSB_S (A_{27-24}) 用作跳频序列发生器的地址输入。发生器的其它输入位与呼叫响应情况形一样。

11.3.6 联机状态

在联机状态中，在信道跳频序列产生中使用的时钟位总是依照于主时钟 CLK。地址位取自主单元的蓝牙设备地址。

12. 蓝牙音频

在蓝牙无线接口上，或是 64kb/s 的对数 PCM 形式（ A-规则或 μ-规则)，或使用 64kb/s 的 CVSD（连续变化斜率增量调制器）形式。后一种形式适用于音节压扩增量调制算法。

在线路接口上的语音代码应当有和64kb/s 对数PCM一样或更好的质

量。下表列出了无线接口所支持的语音编码方式。在链接管理器间协商后来选择合适的语音编码。

表 2.22 在无线界面上支持的语音编码方式

语音编码	
线性	CVSD
8-位对数	A-规则
	μ-规则

12.1 对数 PCM 编译码器（CODEC）

由于在无线接口上的语音信道可以支持 64kb/s 的信息流，所以传输中可以使用 64kb/s 对数 PCM 通讯。可使用或 A-规则或 μ-规则压缩。有线接口使用 A-规则和无线接口使用 μ-规则或使用 A-规则到 μ-规则转换替代算法的事件实现。跟随 ITU- T 的压缩方法着重新推荐 G. 711。

12.2 连续变化斜率增量调制 编译码器 （CVSD CODEC）

对于无线接口语音的较稳定格式是增量调制。该调制方式输出位波形指出是小于预定值或大于输入波形。为了减少斜率过载影响，要用音量压扩技术：步长根据平均信号斜率来修改。输入到 CVSD 编码器是 64Kksamples 的线性 PCM。CVSD 编码器和 CVSD 译码器的结构图如下所示，系统以 64KHz 来定时。

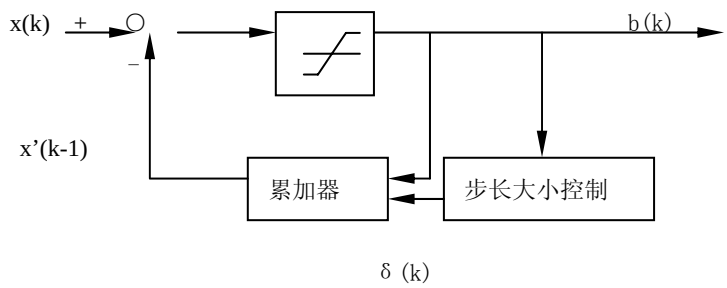


图 2.59 具有声音压扩的 CVSD 编码器框图

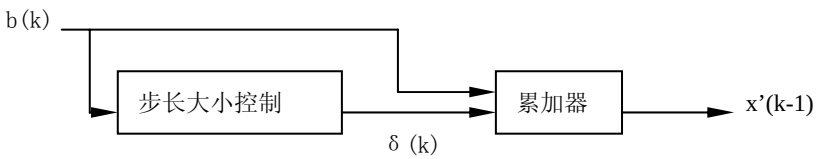


图 2.60 具有声音压扩的 CVSD 解码器框图

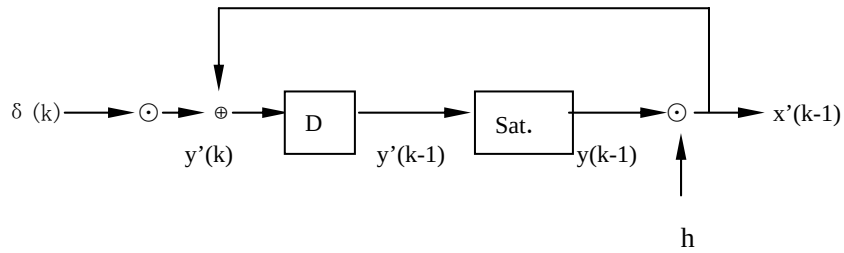


表 2.61　累加器过程

x≥0 时，sgn(x) = 1，否则，sgn(x) = -1。在空中，这些数字用信号位来表现；即：负数映射为“1”，正数映射为“0”。CVSD 指出输出位 b(k)，累加内容 y(k)，步长 δ(k)。因此，设 η 为累加器的衰变因子，β 表示步长的衰变因子，α 表示音节压扩参数。后一个参数通过考虑最近输出位 K 监控斜率。

x'(k) = hy(k)

（等式 11）

然后,CVSD 编码间隔状态依据以下等式来修改：

b(k) = sgn { x(k) – x' (k-1) }

（等式 12）

α ⎧ 1，如果在上次 K 输出位里的 J 位是相等的 =

（等式 13） ⎩ – 0，　否则

δ ⎧ min{δ(k-1)+δmin, δmax}，　α=1, =

（等式 14） (k)

⎩ – max{β δ(k-1), δmin}，　α=0,

y(k) ⎧ min { y'(k) ， y_{max} }， =

（等式 15） ⎩ – max { y'(k) ， y_{min} }，

这儿

y'(k) = x'(k-1) + b(k) δ (k) 。

（等式 16）

在这些等式中 δ min和 δ max是最小步长和最大步长。而y_{min}和y_{max}分别是累加器的正，负饱合度。

对于 64 kb/sCVSD，必须使用下表列出的参数。

表 2.23 CVSD 参数值。

参 数	值
η	1-1/32
β	1-1/1024
J	4
K	4
Δmin	10
Δmax	1280
y_{min}	-2^{15}或$-2^{15}+1$
y_{max}	$2^{15}-1$

这些数字基于累加器输出的 16 位带符号数。这些值导致了累加器衰减 0.5 毫秒时间和步长衰减 16 毫秒时间。

12.3 错误处理

在 DV 和 HV3 分组中，话音不受 FEC 保护。在通信质量要求不高的情况下，话音的质量取决于话音编码方式的稳定性。尤其 CVSD 对在白噪声背景中的随机位错不敏感。然而，因信道识别码或 HEC 测试不成功而拒绝分组时，就必须采取措施来填补丢失的话音部分。

HV2 分组中的话音有效载荷受 2/3 的 FEC 的保护。如果发生了不可纠正的错误，这些错误应当被忽略。那就是说，从无纠错的 15 位 FEC 段中，在 FEC 译码前发现的 10 位信息部分应当使用。HV1 分组由 3-重复 FEC 保护，在大部分检测方式中，无纠错不能出现。

12.4 一般音频要求

这些说明有些不明确，这将在蓝牙说明 1.0 版本草案基础发行后的 18 个月内确定下来。

12.4.1 信号层

对于 A_规则或 η_规则的对数 PCM 的编码信息来说，要求信号层求遵循 ITU-T G.711。.

16 位线性 PCM 和 CVSD 编码器的接口处的全摆动定义为 3dBm0。数字 CVSD 编码测试信号由站点上的有效测试文件提供。该信号由一个参考 CVSD 编码器的软件工具所产生。数字编码器输入信号 (1020Hz，正弦波)

产生的测试信号有一个-15 dBm0 的标称功率。当 CVSD 编码的测试信号经 CVSD 接收链馈送时，标称输出功率能量应为 -15±1.0 dBm0。

12.4.2 CVSD 音频质量

蓝牙的音频质量要求由传输器方面决定。64 ksamples/s 线性 PCM 输入信号必须有 4KHz 以上的频谱功率密度。基准输入信号的设置由基准译码器 (在站点上有效) 传输和发送编码。以 64 ksamples/s 线性 PCM 输出在译码信号的 4~32 KHz 带内的功率频谱密度，应当比 0~4KHz 范围内的最大值低于 20dB。

13. 蓝牙编址

13.1 蓝牙设备地址 (BD_ADDR)

蓝牙的收、发信机都分配有一个 48 位的蓝牙设备地址 (BD_ADDR)。该地址取自 IEEE802 标准。这个 48 位地址被分为三个部分：

- LAP 字段： 由 24 位构成的低地址部分。
- UAP 字段： 由 8 位构成的高地址部分。
- NAP 字段：由 16 位构成的非有效地址部分。

LAP和UAP 形成BD_ADDR的有效部分，获得整个地址空间为 2^{32}。如图所示：

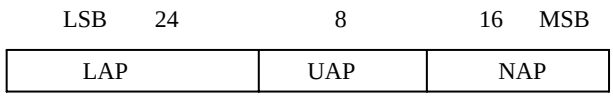


图 2.62 BD_ADDR 格式

13.2 识别码

在蓝牙系统中，有 72 位和 68 位的识别码用作信号目的。共定义了三种不同的识别码。

- 设备识别码 (DAC)
- 信道识别码 (CAC)
- 查询识别码 (IAC)

对于一般查询操作有一个一般的 IAC (GIAC)， 而对于指定查询操作有 63 个指定的 IAC (DIAC)。所有代码取自 BD_ADDR 中的 LAP。设备识别码用于呼叫，呼叫扫描和呼叫响应状态中。它是一个取自单元的 BD_ADDR 代码，匹克网信道的信道识别码特性和在信道上所有分组交换的头格式。信道识别码取自主单元的 BD_ADDR 的 LAP。最后，查询识别码用于查询操作。一般查询识别码为所有蓝牙单元公用，指定查询识别码

的设置用于设备类型的查询。

识别码也用于对接收器指出分组的到来。它用于定时同步和补偿校正。在识别码里接收机与整个同步字无关，它提供了一个十分完整的信号。在信道建立过程中，代码本身当作一个 ID 分组来支持采集过程，另外，在休眠状态下，它用于随机识别过程。

识别码由头，同步字和尾构成，以下两节描述了同步字的产生。

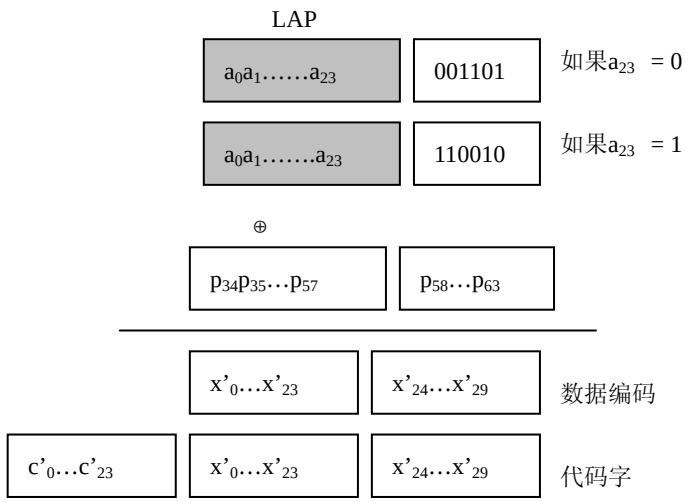
13.2.1 同步字定义

同步字基于 (64，30) 使用复盖（按位 XOR 方式）64 位全长 PN 序列的删除代码块。删除代码保证了基于不同地址上的同步字之间大海明距离 (dmin = 4)。PN 序列改善了识别码的自相关能力。以下各步描述了如何产生同步字：

1. 产生信息序列；
2. PN 复盖序列的信息复盖部分作 XOR；
3. 产生代码字；
4. 用 PN 复盖序列的所有 64 位与代码字作 XOR；

信息序列通过在 24 位LAP上附加 6 位产生 (第一步)。如果LAP的MSB等于 0，那么附加位为 0011101。如果LAP的MSB为 1，那么附加位为 110010。LAP MSB连同附加位一起构成了一个长度为 7 的**Barker**序列。包含**Barker**序列的目的是为了进一步改善自相关能力。在第 2 步里，信息与伪随机噪声 (PN) 序列的P_{34} ••• P_{63}位通过XOR操作实现预加扰。在产生BCH代码字 (第 3 步) 后， 完成PN序列与代码字作XOR (第 4 步)。 这一步解扰代码字的信息部分，同时代码字的部分位被加扰。因此，起始的LAP和**Barker**序列保证是识别码同步字的一部分，而且BCH代码字的循环特性去掉。

原理如图所示：



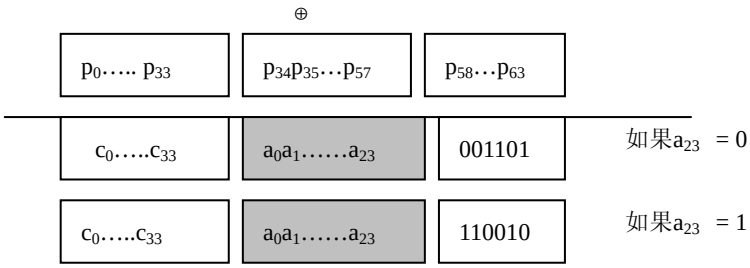


图 2.63　同步字的创建

以后，二进制序列将通过它们相应的D-传输 (这里D^i在表示I次单元延时) 来表示。设$P'(D) = P'_0 + P'_1D + \cdots + P'_{62}$，$D^{62}$为 63 位的伪随机序列，这里$P'_0$是离开PRNG的第一位 (LSB)，而$P'_{62}$是最后一位 (MSB)。为了获得 64 位，在该序列的末尾还要附加一个额外的零 (这样，P' (D)就不会改变)。为记忆方便，该扩展多项式的倒数$P'(D) = D^{63}p(1/D)$用于在序列里。这是保留次序中的序列。我们用$a(D) = a_0 + a_1D + \cdots + a_{23}D^{23}$（$a_0$是蓝牙地址的LSB）24 位蓝牙地址的低地址部分（LAP）表示。

块代码发生器符号 (64，30) 用 g(D) = (1+D)g'(D)表示，这里，g'(D)是初始二进制 (63,30) BCH 代码的发生器多项式 1557464165547 (八进制数)。这样按八进制符号，我们有：

$$g(D) = 260534236651$$

（等式 17）

最左边位与和高序列 (g_{34})系数相对应。DC-空闲四位序列0101和1010可以分别写为：

$$\begin{cases} F_0(D) = D + D^3, \\ F_1(D) = 1 + D^2, \end{cases}$$

（等式 18）

另外我们定义：

$$\begin{cases} B_0(D) = D^2 + D^3 + D^5, \\ B_1(D) = 1 + D + D^4, \end{cases}$$

（等式 19）

该等式用来建立一个长度为 7 的 **Barker** 序列。然后，识别码由以下过程产生：

1．初始化编码的 30 个信息位：

$$x(D) = \alpha(D) + D^{24}\beta a_{23}(D)。$$

2．增加 PN 复盖序列的复盖信息：

$x'(D) = x(D) + p_{34} + p_{35}D + \ldots\ldots + p_{63}D^{29}$。

3．产生扩展 BCH 代码的奇偶位：

$c'(D) = D^{34}x'(D) \mod g(D)$。

4．产生 BCH 代码字：

$s'(D) = D^{34}x'(D) + c'(D)$。

5．增加 PN 序列：

$s(D) = s'(D) + p(D)$。

6．附加 (DC−空闲) 头和尾：

$y(D) = Fc_0(D) + D^4 s(D) + D^{86}Fa_{23}(D)$。

13.2.2 伪随机噪音序列发生器

我们使用原语多项式h (D) = 1 + D + D^3 + D^4 + D^6 产生伪随机噪声序列。LFSR和它的启始状态如图所示：

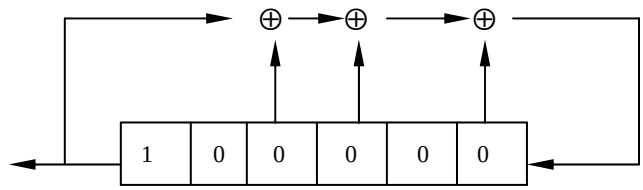


图 2.64 LFSR 及生成 P'（D）的起始状态

PN 序列产生 (包括额外结尾“0”) 成为 83848D96BBCC54FC。LFSR 输出以 PN 序列的最左位开始。这与前节的 P' (D)相对应。这样，使用 P(D)的倒数复盖给出的 64 位序列。

p = 3F2A33DD69B121C1

(等式 20)

这里最左边的位P_0=0 (在 16 进制数字 3 的二进制表示中的有两个初始零)。 最右边的位是P_{63} = 1。

13.2.3 GIAC 和 DIAC 的保留地址

蓝牙查询操作保留有一个 64 连续LAP_S的块；一般查询保留有一个蓝牙设备公用的LAP。余下的 63LAP_S保留用作蓝牙设备特定类的指定查询。相同的 64−块用于UAP和NAP内容的忽略。因此，这些LAP_S无一能是用户BD_ADDR的部分。

当初始化HEG和CRC用作查询响应的FHS分组时，UAP由DCI替代。同样，随时用作产生跳频序列保留BD_ADDR_S的FHS分组，UAP将由DCI替换。

保留 LAP 地址暂时选择为：0X9E8B00~0X9E8B3F。一般查询 LAP

暂时选择为：0X9E8B33。所有地址在最右边位置有以十进制表示的 LSB。

13.2 活动成员地址

在匹克网中的每一个活动从单元都赋予一个 3 位活动成员地址（AM_ADDR）。全零的 AM_ADDR 为广播消息保留。主单元不具有 AM_ADDR。它的定时将它与从单元区分开来。从单元用匹配 AM_ADDR 和广播消息分组接收分组。AM_ADDR 放在分组头里。只要从单元在信道上是活动状态，AM_ADDR 仅是一个值。一旦从单元脱离链接或进入休眠，它的 AM_ADDR 将丢失。

当从单元激活时，主单元就分配一个 AM_ADDR 给从单元，即：或是联机状态建立或是从单元被唤醒。在联机状态下，AM_ADDR 放在 FHS 有效载荷里（FHS 头它自身带有全“0” AM_ADDR）。当处于唤醒状态时，AM_ADDR 放在唤醒消息里。

13.3 休眠成员地址（PM_ADDR）

在休眠模式里的从单元能够通过它的 BD_ADDR 或通过专用休眠成员地址（PM_ADDR）鉴别。后者地址是一个分散休眠从单元的八位成员地址。只要从单元是休眠的，那么 PM_ADDR 有效。当从单元激活时，它被分配一个 AM_ADDR，但丢失 PM_ADDR。PM_ADDR 分配给从单元在休眠时刻。

13.4 接收要求地址（AR_ADDR）

接收要求地址用于休眠从单元在接收区间确定从一主半时隙，在该半时隙里它可以允许发送接收要求消息。当从单元登录为休眠模式时 AR_ADDR 分配给从单元且只要从单元休眠，则 AR_ADDR 就有效。同时 AR_ADDR 并不必一定是唯一的；即：不同的休眠从单元可以共享同一个 AR_ADDR。

14. 蓝牙安全性

蓝牙技术实现了超短距离的同级通信。为具有使用保护和信息保密，系统必须在应用层和链接层上提供安全测试，该测试适用于同级环境。

在各蓝牙单元里的测试、鉴权和加密规则以同样方法实现。在链接层里有四种不同的实体用来维护安全。每个用户有一个唯一的公共地址，两个加密字和每次新的处理都具有不同的随机数。四个实体和它们的长度值如表所示：

表 2.24 用于鉴权和加密的实体

实　　体	长　　度
BD_ADDR	48 位
私有用户字，鉴权	
私有用户字，加密 结构长度（字节-方式）	8～128 位
随机数	128 位

蓝牙设备地址（BD_ADDR）对每个蓝牙单元有唯一的 48 位 IEEE 地址。蓝牙地址是公开的而且可经 MMI 交换，或自动地，或经蓝牙单元查询规则获得。

加密字取决于初始化期间且不会被取消。通常加密字在加密过程中取决于鉴权字。鉴权算法字一般是 128 位。加密字长度可在八进制数 1~16 间变化（8~128 位）。加密字长度以两种前提确认，第一种前提是，在不同的国家有很多不同的要求必须施加于加密算法上。一般情况下，导出规则和权限属性趋于保密。第二个前提条件是，若没有算法及加密硬件以昂贵价格重新设计的必要，易于升级是安全的一条捷径。增加有效字长度是以相反的观念反对增加计算量的一种最简单的方法。当前（1999）似乎给出的 64 位加密字长度足以满足大部分用户的保护。

加密字完全不同于鉴权字，每次加密的激活都将产生新的加密字。因此加密字的生命期不必与鉴权字一致。

可以预测鉴权字比加密字在初期更为严谨，蓝牙设备一旦实际应用运行过程进行，就决定在什么时间或如何去改变加密字。为强调鉴权字的基本重要性，应指出特定的蓝牙链接，它将以链接字作基准。

RAND 是一个取自蓝牙单元里的随机或伪随机过程中的随机数，它并不是一种稳定的参数且经常改变。

该章的其余部分用户和应用都将涉及到相同的概念和指明收、发两端的实体。

14.1 随机数发生器

每个蓝牙单元都带有随机数发生器。随机数在安全性能方面有很多的用途。例如：质询方案，鉴权和加密字产生过程等。理论上讲，一个真正的随机数发生器基于某些内在随机数使用的物理过程。举例来讲，其过程就是来自于元器件、电阻及各种振荡器的不稳定性所产生的热噪声。作为实际工程，软件宁可使用基于随机数发生器的算法，通常这完全不同于伪随机序列的随机数分类。在蓝牙里，未用随机数的设备是因它们为非重复和随机产生。

非重复表示的意思为，在鉴权字生命期内，它并不像有些值需要多次重复。例如：非重复值可为计数器的输出而并不要求在鉴权字或数据/时间

标记的生命期中重复。

随机产生意指，它不可能预测它大于“0”含义的偶然性值（即：大于作为L位的字长度的 $1/2^L$）。

显然，LM可用这样的发生器作用于各种目的。即：随机数可能随时需要（如：$RAND_S$、 单元字、Kinit、Kmaster、及补偿或等待时间）。

14.2 字管理

在特定单元里，加密字的长度不能由用户设定是至关重要的，它必须由生产方预置。为防止用户超越字长度允许，蓝牙基带处理器并不接收由高层软件提供的加密字。无论何时需要新加密字，它都必须以加密术来产生 E-3 字。

链接字的改变也通过基带处理器定义来产生，该过程取决于链接字是什么类型而是取决于需要。

14.2.1 字类

链接字是 128 位随机数，它分散在两个以上的组内而且是在这些组内间整个安全事务的基础。链接字自身就用于鉴权规则加工，当加密字导出时，链接字也作为其参数之一。

以下将单元时间间隔定义的话路为一个实际匹克网成员。因此，当单元脱离匹克网链接时，话路终止。

链接字或许是半永久性的或许是临时的。半永久性链接字存放在随机存储器里，而且在当前话路终止后仍可以使用。因而一旦半永久性链接字被定义，它就可用在蓝牙单元共享它们间的一系列后续联机的鉴权。半永久性名，通过改变它的可能性是合理的。

临时链接字的生命期经当前话路的生命期先于受限。它不能在后续的话路里重新使用。典型的是在一点多址结构里，一个相同的信息安全地分布在几个接收器里。

公用加密字是完全有用的。为完成这点，特定的链接字（主单元字表示）能临时替换当前链接字。

以后，我们有时涉及到当前链接字表示的意思。这是一个简单地用于当前瞬间的链接字，它可以是半永久性的或临时的。因此，当前链接字用于整个鉴权和在线联机（话路）里整个加密字的产生。

为适应不同类型的应用要求，链接字的四种类型定义如下：

- 组合字K_{AB}。
- 单元字K_A。
- 临时字 Ktmaster。
- 初始化字 Kinit。

另外，这些字都具有加密字K_C，且字取自当前链接字。加密字随时可

经LM命令激活且自动地实现修改。若没有依据鉴权过程的削弱，区分鉴权字和加密字是方便较短加密字的使用。鉴权算法依据不具有政府行为，但有些国家，加密算法依据的限制仍存在。

对蓝牙单元来说，组合字K_{AB}和单元字K_A是不可区分的功能。它们产生的方法不同，单元字K_A产生依据单个单元A。单元字产生后一旦装入蓝牙单元，此后它就很难再改变。组合字取自单元A和单元B的信息，它总是依赖于着两个单元。组合字导出两个蓝牙单元的各种新组合。

单元字和组合字的使用取决于应用和设备的使用。蓝牙单元有一个小存储器来存储字。当字被安装在设备里时，它必须为其它大量用户所识别，而且它完全使用它们的自身单元字。在这种情况下，它们必须把单个字存起来。在要求较高安全性层次的使用场合，人们宁可使用组合字。由于各种链接到不同蓝牙单元的组合链接字必须存储起来，所以这种应用将需要较大的存储空间。

主单元字，Ktmaster 只用于在当前话路中的链接字。它只能由原链接字临时地替换。例如：当主单元希望能同时在两个以上的蓝牙单元里使用同一加密字时，就可使用这种方法。

当没有组合或单元字被定义及交换或当链接字已丢失时，就使用初始化字 Kinit。初始化字保护初始化单元的传输。当字取自随机数：L-八位字节、PIN 代码及申请单元的 BD_ADDR 时，该字只能用在初始化过程中。

PIN 可以是一个由蓝牙单元（如：在 PSTN 插件里没有 MMI 时）提供的固定值。PIN 可由用户随意地选择其一，且两个单元登录时必须匹配。当两个单元都具有 MMI 时（如：电话或变携式计算机）可使用后一种过程。在双方单元里登录 PIN 方式比在任一个单元中使用固定 PIN 安全，而且可以随时使用。在固定 PIN 使用时，PIN 可能会改变，这主要是防止曾经已具有 PIN 用户的再次初始化问题。如果 PIN 是无效的，默认值“0”就被使用。

在很多应用里，PIN 代码与一串短数有关。典型地它可由四位十进制数组成，甚至在很多情况里它都可充分满足安全的需要，但这里也存在着无数其它较敏感和不太可靠的情况。因此，PIN 应从 1~16 位（八进制）任何组合中选择。对于较长的长度，我们可以想象，单元交换 PIN 不是由机械（即人工）交互，而是使用应用层软件来支撑。例如：这可能是 Diffle—Hellman 字协议。此处，字的互换是在双方单元里经过了 Kinit 的发生过程，就如在较短的 PIN 代码的情况里一样。

14.2.2 字生成和初始化

链接字在蓝牙单元使用鉴权的过程中生成及分布。由于链接字必须是安全的，所以它不能象蓝牙地址那样通过查询规则来获得。在初始化过程

中，字变换产生必须是意欲完成鉴权和加密的两个单元。实现整个初始化的过程分别由下面五步组成：

- 生成初始化字。
- 鉴权。
- 生成链接字。
- 互换链接字。
- 在各个单元里生成加密字。

初始化过程后，单元可以实现通信或联机可以脱离。若执行加密，选用取自当前链接字合适的加密字可使用E_0算法。在单元A和单元B之间任何新的联机过程的建立，代替曾经从PIN导出多Kinit，作为鉴权，它们将用作公共链接字。新的加密字取自下次加密被激活时创建的实际链接字。

若链接字是无效的，LM 在初始化过程中自动地启动。

14.2.2.1 生成初始化字 Kinit

链接控制字在初始化过程中导出：初始化控制字Kinit。该字从申请单元的BD_ADDR经 E_{22}算法导出，PIN码，PIN（八位字节数）的长度，及经校验器列举（创建）的随机数IN_RAND_A。从E_{22}输出的 128 位将用于在链接字生成的期间实现字的交换。当两个单元以前还没有链接字的记录时，该初始化字也用作鉴权。当单元完成链接字的交换时，初始化字被放弃。

当初始化字生成时，PIN 用申请单元的 BD_ADDR 鉴权。因用于鉴权的 PIN 最大长度不能超出八进制 16，有时还有并不是 BD_ADDR 的整个八进制数都要使用的情况。该过程确保 Kinit 随想与它联机单元的特性而定（至少在使用短 PIN 代码时）。非法用户蓝牙单元通过每次申请另外的 BD_ADDR 可以企图去测试 PIN 的一个大数，但通过取计数器测量值来遏制这种破坏性现象是应用中的一种目的。如果设备地址是保持固定的，到下次链接的等待间隔允许按指数规律递增。

14.2.2.2 鉴权

鉴权的执行过程在后面的内容中将描述，此处只是概念引入。以前如果两个单元没有链接，初始化字 Kinit 当作链接字使用。注意，在每次鉴权期间，新AU_RAND_A将发布。

相互鉴权首先是在一个方向实现鉴权过程的完成，如果成功的话，立即紧跟在相反方向实现鉴权过程。

作为成功鉴权过程的结果端辅助参数，鉴权计算补偿 （ACO）， 将进行计算。ACO 将用作字生成计算。在相互鉴权情况下，来自第二个鉴权的 ACO 值被返回。然而，在有些情况下，鉴权事件可以同时在两个设备中开始。当在这种情况时，就没法区分第一和第二事件。此时，两个单元都使

用来自主单元的质询产生的 ACO 结果。

申请 / 校验状态由 LM 确定。

14.2.2.3 生成单元字

当蓝牙单元是第一次操作时，单元字 K_A 生成，即：非各初始化。单元字由E_{21}算法生成。单元字就存储在非易失性存储器里同时决不（几乎不）改变。如果初始化后单元字改变，则以前的初始化单元就具有一个错误链接字。初始化时，如链接字一样，申请必须确定提供单元字的两部分之一。典型情况下，它是存储容量有限的单元，因为这种单元只能记录它自身单元字。单元字传输到其它部分并作为一个特殊部分链接字存储起来。例如，单元A的单元字 K_A 用作联机 A - B 的链接字；单元 A 发送单元字K_A到单元 B；单元B 把K_A当作链接字K_{BA}存储起来。对另一个初始化，以单元C作例子，单元A再使用单元字K_A，而单元C将它作为存储K_{CA}。如图所示：

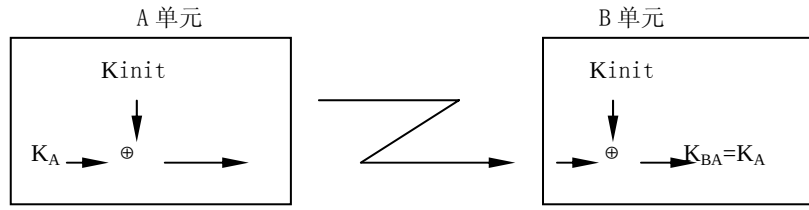


图 2.65 单元字的生成,当单元字已互换时,双方单元的初始化字都放弃

14.2.2.4 生成组合字

若要使用组合字，该字首先在初始化过程中生成。组合字是分别在单元A和单元B里生成两数的组合。首先，在各单元里生成随机数，LK_RAND_A和LK_RAND_B。然后，以随机数和自身BD_ADDR使用E_{21}，两个随机数：

$$LK\_K_A = E_{21}(LK\_RAND_A, BD\_ADDR_A),$$ （等式 21）

$$LK\_K_B = E_{21}(LK\_RAND_B, BD\_ADDR_B),$$ （等式 22）

分别在单元A和单元B里产生。这些数构成实现创建的组合字。然后，两个随机数LK_RAND_A，LK_RAND_B用当前链接字，比如说K，通过XOR命令实现安全互换。于是，单元A 送出$K \oplus LK_RAND_A$到单元B，而单元B 送$K \oplus LK_RAND_B$到单元A。显然，若在初始化过程中作该工作，链接字K = Kinit。

当随机数LK_RAND_A和LK_RAND_B已相互交换时，各单元重算有助于组合字的其它单元。由于各单元知道其它单元的蓝牙设备地址，所以这是可行的。于是，单元A 计算（EQ21）且单元B计算（EQ20）。此后，两单元组合两数以生成 128 位的链接字。组合操作是一个简单的按位模 2 加（即：XOR）。结果在单元A 里以链接字K_{AB}存储，在单元B里以链接字K_{BA}存储。当两个单元已导出新的组合字时，为确认处理成功。相互鉴权过程将开始。在成功

互换新的组合字后旧的链接字被放弃。下面用图描述了在主单元和从单元之间的消息以及创建组合字的原理。

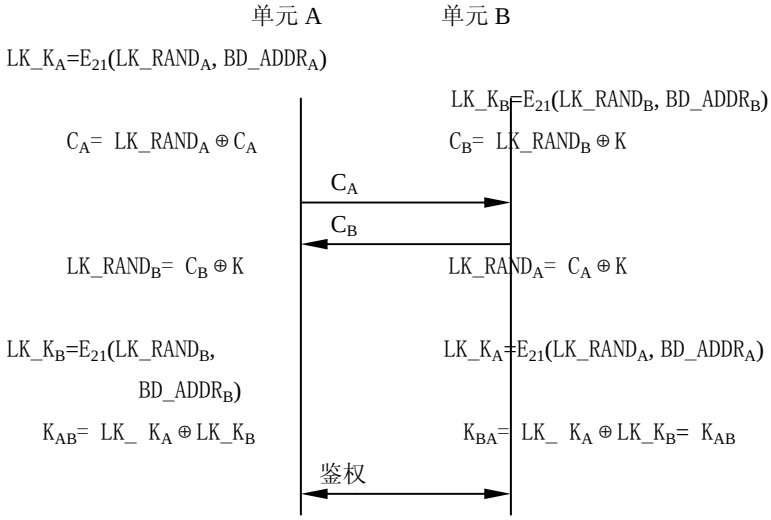


图 2.66 组合字的生成。在新的组合字已成功互换后，旧的链接字（K）放弃。

14.2.2.5 创建加密字

加密字 K_C ，（从当前链接字经算法 E_3 导出），具有 96 位计算补偿数（COF） 和 128 位随机数。COF以两种方法导出。如果当前链接字是主单元字，COF从主单元的BD_ADDR导出，否则，COF的值在鉴权过程中设置成ACO的值。用等式表示为：

$$\text{COF（等式 23）} = \begin{cases} \text{BD\_ADDR} \cup \text{BD\_ADDR} & \text{若链接字是主单元字} \\ -\text{ACO} & \text{否则} \end{cases}$$

当LM激活加密时，有一次明显的E_3调用。每次单元登录加密模式时，加密字自动地改变。

14.2.2.6 一点多址结构

主单元对一点多址结构里的各从单元以激活算法使用多个加密字是完全可能的。如果应用要求多于一个以上的从单元监听相同有效载荷，那么每个从单元必须要求单独编址。这可能导致匹克网的容量损失。加之，蓝牙单元（从单元）不能够实时（即：在头里见到 AM_ADDR 后）的在两个以上的加密字间进行切换，于是，主单元不能用不同加密字来广播消息和任择其一地址来通信。主单元可以告诉几个从单元公用链接字（因此也可直接地公用加密字）和广播加密信息。在很多应用中，该字仅是暂时唯一的。结果，该字标注是 Kmaster。

必要参数传输的保护问题前面以作了讨论。在各从单元成功接收确认后，主单元发布一个命令给从单元用新的（暂时）主单元字替换各当前链接字。在加密激活前，主单元也必须生成和分发命令 EN_RAND 给所有有关的从单元。用该随机数和最新导出主单元字，各从单元生成新的加密字。

注意：主单元必须协调每个意图使用主单元字的各从单元各自使用的加密字的长度。由于主单元早已与每个从单元协调好，所以主单元已了解各个从单元能接受的长度值。显然，可能出现有些单元的允许字是不相容的情况，此时，主单元必须限制从单元数。

当所有从单元已收到必要数据时，主单元能够使用从新临时链接字中导出的加密字在匹克网上安全地实现通信。显然，各拥有主单元字的从单元都能够监听整个加密通信，不仅是计划中的自身通信。如出现该情况，主单元能通知所有参与者同时退回到它们的原链接字。

14.2.2.7 修改链接字

在确定情况下，链接字的修改是可行的。链接字基于可变的单元字，但并非容易。在曾经第一次使用时，单元字产生。由于几个单元分配有如链接字一样的相同单元字，所以改变单元字并不具有可取之处。改变单元字将引起试图联机的所有单元重新初始化。但在某些情况里，这种处理又是必要的，例如，否决先前已登录的单元。

如果字改变涉及到组合字，宁可该过程直接前推。该过程完全等同于前面所述的生成组合字内容。在鉴权和加密开始后，该过程能在任何时间执行。事实上，因组合字符合单个链接，该链接建立能保证在各个时间修改。由于每次通信后，原字丢失了它们的合法性，这将提高系统的安全性。

当然，整个新的初始化过程重新开始也是可行的，此时，因在鉴权和加密过程里需要 PIN，所以用户的交互是必须的。

14.2.2.8 生成主单元字

至今描述的改变字的规则都是半永久性的。为创建主单元链接字，在初始化期间，主单元字可用当前链接字替换。首先，主单元从 128 位 RAND1 和 RAND2 里建立新的链接字。如下定义：

$$Kmaster = E_{22}(RAND1, RAND2, 16)$$

（等式 24）

显然，该字是 128 位随机数。使用E_{22}输出和不直接地选择作为字的随机数的理由是，为避免在蓝牙单元里随机数发生器的不良执行降低了随意性的可能问题。

然后，第三个随机数，比如说：RAND，传输给从单元。用具有当前链接字的E_{22}和RAND作为输入，主单元和从单元都以复盖 128 位计算。主

单元送出按位XOR的复盖及新的链接字给从单元。知道复盖的从单元计算Kmaster。为证实这种互换的成功，使用新的链接字（主单元作为校验而从单元作为申请）单元可完成鉴权过程。各接收新链接字的从单元将重复该过程。当主单元希望全部退回到原先链接字（非临时）时，涉及鉴权的ACO值不用当前存在ACO（该ACO需要重新计算一个计算字）字替换。

当如这种情况，主单元通过LM命令激活加密，但主单元字在实际分配后不久就消失，因此在操作之前，主单元必须要求所有从单元接受相同的随机数，比如说：EN_RAND。由于加密字通过在所有鉴权单元里各自E_3方法导出，则各个从单元用新的加密字计算，

$$K_C = E_3(\text{Kmaster}, \text{EN\_RAND}, \text{COF}), \qquad \text{（等式 25）}$$

这儿 COF 的值通过给定的等式 22 从主单元的 BD_ADDR 导出。在主单元和从单元之间，当主单元字生成时消息流的原理如下图描述。注意：在这种情况下，当计算加密字时，鉴权过程中的 ACO 没使用。

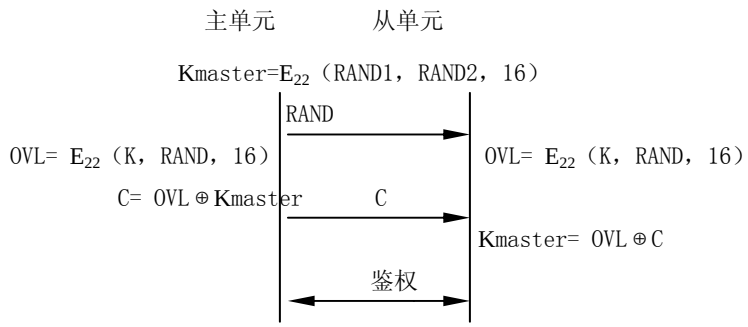


图 2.67　主单元字及相应加密字计算

14.3　加密

用户信息通过匹克网的加密保护；识别码和分组头不加密。有效信息的加密用称为对每个有效载荷重同步的E_0加密流执行。原理如图所示：

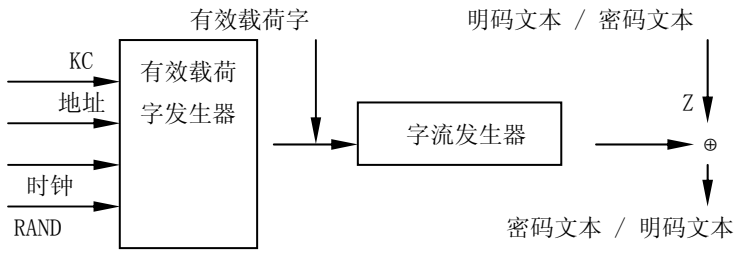


图 2.68　蓝牙的加密流

加密流系统E_0由三部分组成。第一部分实现初始化（有效载荷字的生成），第二部分产生字流位，第三部分完成加密和解密。有效载荷字发

生器很简单，它仅仅以适当序列组合输入位，然后移出它们到字流发生器的四位FLSR。第二部分是加密系统的主要部分并也用于初始化中。字流位通过取自于因 Massey 和 Rueppel 流加密求和发生器的方法来生成。这是一种好的研究方法并有着谈到目前密码分析方法力度的好的评价。虽然求和发生器用在称为“相互攻击”方面有弱点，但重同步的高密度将抑制这类攻击。

14.3.1 加密字长度协调

用在基带规范里的各蓝牙设备需要定义一个字最大允许长度参数Lmax。1≤Lmax≤16（字里的八进制数）。作为各种应用，参数Lmin定义为实际应用最小可接受字长度。在加密字产生前，涉及到的单元必须协调决定实际应用的字的长度。主单元送出一个暗示值$Lsug^{(M)}$到从单元。最初暗示值设成$Lmax^{(M)}$。如果$Lmin^{(S)} \leq Lsug^{(M)}$，而且从单元支持该暗示值长度，则从单元确认且该值为这种链接的加密字。如果两个条件都不满足，从单元送出一个新的建议$Lsug^{(S)} < Lsug^{(M)}$到主单元。该值将是在所有可支持长度中最大值但小于先前主单元的暗示值。主单元在从单元的暗示上完成响应的测试。该过程一直持续到字一致为止，或一个单元协调异常中止。该异常中止可由支持 Lsug 的缺乏和如果在某个单元里 Lsug< Lmin 引起。在异常中止情况里，蓝牙链接加密字不能使用。

建立安全链接失败的可能性是，允许申请决定是否接受或拒绝暗示字长度的必然结果。然而这是一种必要的预防措施，否则一个非法用户单元通过申请一个小的最大字长度在链接上实行强制弱保护。

14.3.2 加密字模式

如果从单元具有半永久链接字（即：组合字或单元字），它只能在自身（当然在主单元的相反方向）个别地址时隙上接受加密字。特别是假设广播消息不是加密字，可行的通信模式如表所示：

表 2.25 使用半永久链接字从单元的可行通信模式

广播通信	个别地址通信
无加密	无加密
无加密	加密，半永久链接字

当在表里的登录项涉及到链接字时，它意指加密 / 解密引擎使用从链接字导出的加密字。如果从单元接收主单元字，就有如表所示的三种可能的组合。

表 2.26

广播通信	个别地址通信
无加密	无加密
无加密	加密，Kmaster
加密，Kmaster	加密，Kmaster

在这种情况下，匹克网中的所以单元都使用公共链接字， Kmaster。由于主单元使用从匹克网上整个安全通信的链接字中导出的加密字，避免参与使用加密字的从单元多义性是可能的。在这种情况下，默认方式是无加密的广播消息。对于广播和个别地址通信，特定的 LM 命令用来激活加密。主单元能够发布 LM 命令到从单元并通知它们后退到它们先前半永久链接字，且不管它们以前处于什么模式，都将结束在使用半永久链接字从单元的可行通信模式表上第一行的无加密模式上。

14.3.3 加密概念

作为加密惯例，密码算法流用在发送到无线接口的加密位和按位模 2 和的数据流上。有效载荷加密附加在 CRC 位后，但它们先于 FEC 编码。

各分组是单独加密。密码算法E_0使用的随机数EN_RAND_A，主单元蓝牙地址，主单元实时时钟（CLK_{26-1}）的 26 位和加密字作为输入。如图所示：

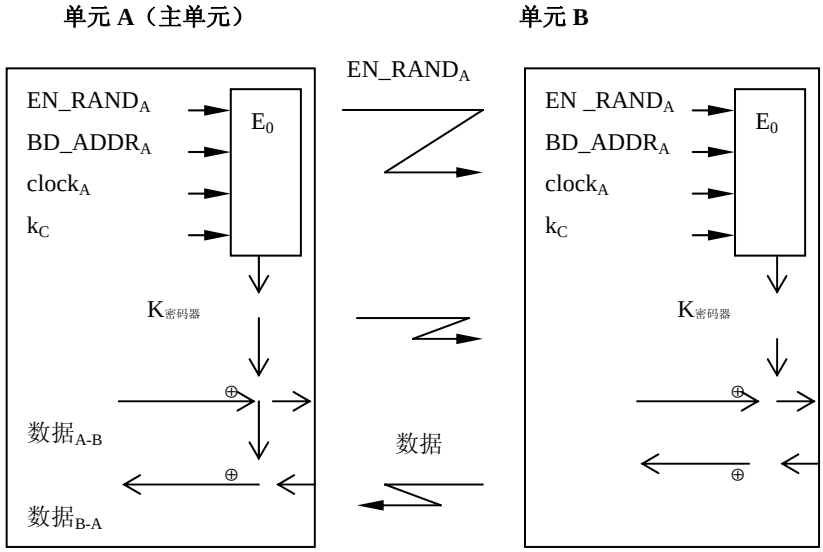


图 2.69 编码过程

EN_RAND_A在登录加密模式前通过主单元发布。注意：EN_RAND_A是公开的，因为在空中它是一个明码文本。该 128 位随机数部分可用加密字部分（保密）替换，结果在加密字里的保密位和要求的字长度一致。详细

内容请见LFSR初始化。

实时时钟是各时隙的增量。各新分组（即：对于主一从与从一主相同传输）的开始E_0算法初始化。在两次传输之间，通过使用CLK_{26-1}至少一位改变。在每次重新初始化后，新字流生成。因分组复盖多余单时隙，在第一时隙里找到的蓝牙时钟用于整个分组。

加密字以 K_C 标注。该字的最大值由生产商预置，而且在 1 到 16(8-128 位)之间可设置成任何八的倍数。该字导出过程见用于E_3-字生成功能内容。加密算法E_0生成二进制字流，Kcipher，该字流是加密的模 2 和数据。密码是对称的；解密使用完全和加密相同的字和相同的方法实现。

14.3.4 加密算法

使用线形反馈移位寄存器（$LFSR_S$）的系统输出是一个有 16 个状态的简单有限状态机（称作求和合成器）的组合。该状态机的输出是字流序列，或在初始化中的状态中随机的初始化开始值。算法由加密字K_C提供，48 位蓝牙地址，主单元时钟位CLK_{26-1}和 128 位RAND值。设置如图所示：

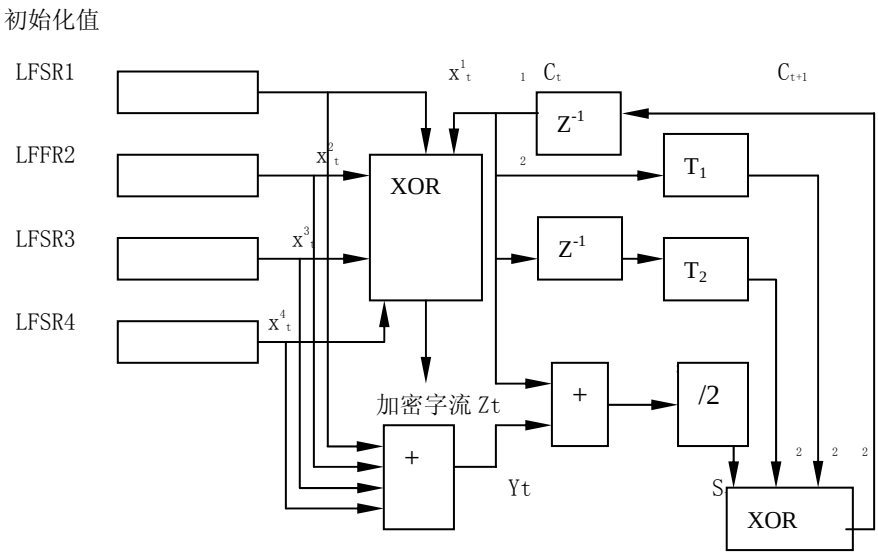


图 2.70 加密引擎概念

具有L_1=25，L_2=31，L_3=33 和L_4=39 长度的四个$LFSR_S$（$LFSR_1$，•••••，$LSFR_4$），用如表所示指定的反馈多项式。

表 2.27 四个原语反馈多项式

i	Li	反馈 fi(t)	权
1	25	$t^{25}+t^{20}+t^{12}+t^{8}+1$	5
2	31	$t^{31}+t^{24}+t^{16}+t^{12}+1$	5
3	33	$t^{33}+t^{28}+t^{24}+t^{4}+1$	5
4	39	$t^{39}+t^{36}+t^{28}+t^{4}+1$	5

寄存器组的总长度是 128 位。这些多项式全是原语的。整个反馈多项式的海明权都选成 5 ，其理由是在硬件实现需减少 XOR 门的数量及为获得生成序列好的统计特性之间的综合。

让 $X^i t$ 表示 LSFRi 的符号t^{th}。从四元组$X^1 t$，..... $X^4 t$，我们导出值 y_i。

$$y_i = \sum_{i=1}^{4} X^i t \quad \text{（等式 26）}$$

这儿和以整数结束。于是y_i可取值 0，1，2，3 或 4。加法器的输出现通过下面等式给出。

$$y_i = X^1 t \oplus X^2 t \oplus X^3 t \oplus X^4 t \oplus C^0 t \in \{0, 1\}, \quad \text{（等式 27）}$$

$$s_{t+1}=(s^1_{t+1}, s^0_{t+1})=(y_i+C_i)/2 \in \{0, 1, 2, 3\}, \quad \text{（等式 28）}$$

$$c_{t+1} = (c^1_{t+1}, c^0_{t+1}) = s_{t+1} \oplus T_1[c_t] \oplus T_2[c_{i-1}], \quad \text{（等式 29）}$$

这儿T_1 [.]和T_2 [.]是在GF（4）上的两个不同的线形双射。假设GF（4）是通过不能简化的多项式x^2+x+1，而且让在GF（4）里多项式的 α 为“0”时产生。映射T_1和T_2如下定义：

T_1：GF（4）→ GF（4）

x ⟼ x

T_2：GF（4） GF（4）

x ⟼ （α +1） x

我们可以用二进制矢量写 GF（4）的元素。这在下表中给出：

表 2.28 T_1 和T_2映射

x	T_1 [x]	T_2 [x]

00	00	00
01	01	11
10	10	01
11	11	10

T_1：$(x_1, x_0) \longmapsto (x_1, x_0)$，

T2：$(x_1, x_0) \longmapsto (x_0, x_1 \oplus x_0)$。

14.3.4.1 密码操作

如图所示给出了及时操作的概述。

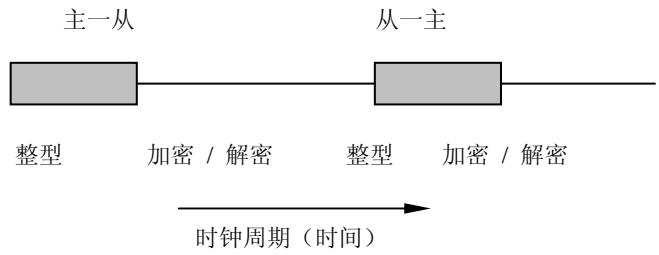


图 2.71 加密引擎操作的概述

在发射和接收新分组开始前，加密算法通过初始化过程运行。因此，对于整数分组，密码用在整数序列里第一个时隙的时钟值初始化。

14.3.5 LFSR 初始化

字流生成器需要用四个 $LFSR_S$（总长 128 位）的起始值和C_0及C_{-1} 的特定四位值装入。该 132 位起始值通过使用它自身的字流生成器四个输入导出。输入参数是字，K_C，128 位随机数RAND，48 位蓝牙地址和主单元时钟位CLK_{26-1}的 26。

加密字的有效长度在 8~128 位之间任选。注意：从 E3 获取的实际字长度为 128 位，然而，E0 内的字长度因通过在 KC 和多项式要求的级数之间求模操作被减少。在减少后，为抑制开始状态的不一致性，结果使用块代码编码。操作以（等式 29）定义。

当加密字已经创建而且用它们的起始值装入$LFSR_S$，然后，由生成器选择创建的 200 密码流位，这些位中，后 128 位作为四个$LFSR_S$的起始值馈给字流发生器，Ct和Ct−1 的值保持。从这点上看，当定时加、解密序列发生过程时，将与发射或接收的有效载荷按位求模 2 和（XOR）。

下面，我们通过符号 X[i] 标注二进制序列 X 的八位字节数 i。我们定义 X 的“0”位是 LSB，而 X[i]的 LSB 对应于序列 X 的位 8 i，X[i]的

MSB 是 X 的位 8 i +7。例如，蓝牙地址的 24 位是 ADR[3]的 LSB。

初始化的详细内容如下：

● 创建加密字使用保密字K_C的 128 位和公开的EN_RAND的 128 位。 设L是八位字节数有效字长度（1≤L≤16）。因而加密字用K_C标注：

$$K'c(x) = g_2^{(L)}(x)(Kc(x) \bmod g_1^{(L)}(x))。$$ （等式 30）

这儿，度$(g_1^{(L)} = 8L)$ 和 度（$g_2^{(L)}(x)$）≤128-8L。多项式在表中定义。

表 2.29

L	deg	$g_1^{[1]}$
1	[8]	00000000 00000000 00000000 0000011d
$g_2^{[1]}$	[119]	00e275a0 abd218d4 cf928b9b bf6cb08f
2	[16]	00000000 00000000 00000000 0001003f
	[112]	0001e3f6 3d7659b3 7f18c258 cff6efef
3	[24]	00000000 00000000 00000000 010000db
	[104]	000001be f66c6c3a b1030a5a 1919808b
4	[32]	00000000 00000000 00000001 000000af
	[96]	00000001 6ab89969 de17467f d3736ad9
5	[40]	00000000 00000000 00000100 00000039
	[88]	00000000 01630632 91da50ec 55715247
6	[48]	00000000 00000000 00010000 00000291
	[77]	00000000 00002c93 52aa6cc0 54468311
7	[56]	00000000 00000000 01000000 00000095
	[71]	00000000 000000b3 f7fffce2 79f3a073
8	[64]	00000000 00000001 00000000 0000001b
	[63]	00000000 00000000 a1ab815b c7ec8025
9	[72]	00000000 00000100 00000000 00000609
	[49]	00000000 00000000 0002c980 11d8b04d
10	[80]	00000000 00010000 00000000 00000215
	[42]	00000000 00000000 0000058e 24f9a4bb
11	[88]	00000000 01000000 00000000 0000013b
	[35]	00000000 00000000 0000000c a76024d7
12	[96]	00000001 00000000 00000000 000000dd

	[28]	00000000 00000000 00000000 1c9c26b9
13	[104]	00000100 00000000 00000000 0000049d
	[21]	00000000 00000000 00000000 0026d9e3
14	[112]	00010000 00000000 00000000 0000014f
	[14]	00000000 00000000 00000000 00004377
15	[120]	01000000 00000000 00000000 000000e7
	[7]	00000000 00000000 00000000 00000089
16	[128]	1 00000000 00000000 00000000 00000000
	[0]	00000000 00000000 00000000 00000001

- 在 3 输入K_C里移位蓝牙地址，时钟和六位常数 111001 到$LFSR_S$。在整个 208 位移入里：

  1）打开所有开关。

  2）排列输入位如图所示，所有移位寄存器元素内容为“0”，设置 t=0。

画图 14.8

图 2.72

  3）开始移位到$LFSR_S$。各级的最右位是首先登录到相应LFSR。

  4）当级 i 的最先输入位到达 LFSR i 的最右位，关闭 LFSR 的开关。

  5）在 t=39（当 LFSR 4 的开关是关闭时），复位混合寄存器 $C_{39}=C_{39-1}=0$；到此时，Ci 和 Ci-1 还没有考虑。然而从该时刻起，它们的内容将用作计算输出序列。

  6)现在输出符号产生。余下的输入位继续移进它们对应的移位寄存器。当最后一位移入时，移位寄存器用输入为“0”定时；注意：当完成时，$LFSR_1$具有用反馈关闭的有效定时 30 次，$LFSR_2$有效定时 24 次，$LFSR_3$有效定时 22 次和$LFSR_4$用反馈关闭的有效定时 16 次。

- 对于最小初始数据，继续定时直到 200 符号已经产生且所有的开关关闭（t =239）。
- 保持混合寄存器Ci 和Ci-1，据图所示，在t =240 处，并行装入后 128

位到$LFSR_S$。

画图 14。9

图 2.73

在第 4 项并行装入后，混合寄存器的内容将作为随后时钟被更新。

在 2）中所述图里，所有位以最少有效位（LSB）移入起始点。例如，八进制 3 的地址ADR[2]，首先是ADR_{16}登录，随后是ADR_{17}，等等。加之，CL_0对应CLK_1，....，CL_{25}对应CLK_{26}。

注意：输出符号，Xt^i，i= 1，....，4 分别取自于$LFSR_1$ ，$LFSR_2$ ，$LFSR_3$ 和$LFSR_4$的 24，24，32，32 位置（计数器最左位置是数 1）。在输出符号后 128 位的图描述中，128 个二进制输出符号Z_0，....，Z_{127}安排用八进制表示Z[0]，Z[15]。Z[0]的LSB对应这些系统的开始，Z[15]的MSB是发生器的最后输出，将这些位跟据图装入$LFSR_S$。它并行装入且混合寄存器不需更新，第一个输出符号同时产生。在左边位置上（即：以前反方向）八进制数写进有LSB的寄存器。例如：Z_{24}装入$LFSR_4$的位置 1。

14.3.6 字流序列

当初始化完成时，从加法器的输出用作加密或解密。使用的第一位是并行装入的第一过程，即：在 t =240 处。电路运行当前有效载荷的登录长度，然后在反向开始前，在输入参数上使用更新值，重复登录初始化过程。加密输出序列的取样数据可在“附录Ⅳ”里看到。必要但不充分的条件是，整个蓝牙遵循实现是产生这些与初始化值一样的加密流过程。

14.4 鉴权

用于蓝牙里登录鉴权采用竞争－响应方案，该方案里申请者的密钥字结构通过使用对称的密钥字经 2－MOV协议校验。后者暗指当前申请者 / 校验对共享同一密钥字，比如说：K。在竞争一响应方案里，校验竞争鉴权随机数输入申请者，以AU_RAND_A标注，以E1 标注的鉴权代码和返回到校验的SRES。如图所示。图中也说明输入到E1 的蓝牙由AU_RAND_A和申请者的蓝牙设备地址(BD_ADDR)组成。该地址的使用防止了简单反射攻击[1]。密钥 K 由为当前链接字的单元A和单元B共享。

由于整个服务要求基于 FIFO 为基础，所以在蓝牙里反射攻击实际上没形成危害。当抢先占有导出时，该攻击具有潜在的危害。

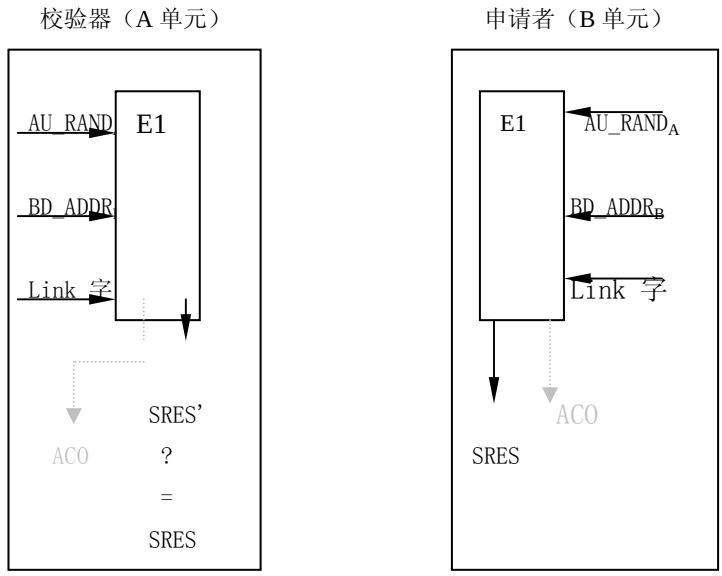


图 2.74　蓝牙竞争响应

用于蓝牙里的对称字竞争一响应方案如图所示：

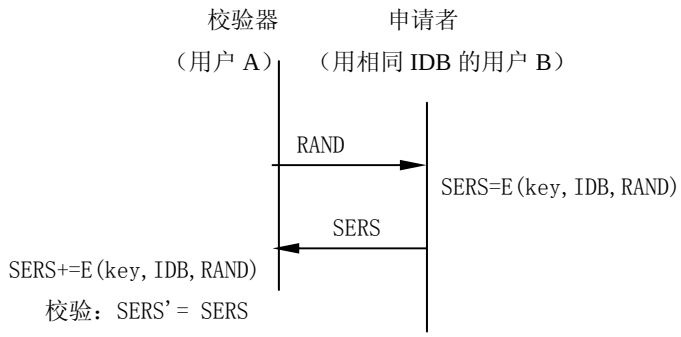


图 2.75 对称字竞争一响应方案

在蓝牙里，主单元并非必须校验。必须鉴权的申请者已指出。确定的申请者只要求单方向鉴权。然而，在某些点对点的通信场合，人们宁可相互鉴权，原因是在两个鉴权过程中，各单元其后就是竞争（校验）。LM通过申请者确定哪个方向的鉴权必须产生而确定鉴权优先选择。当用共享单元相互鉴权的图方式时，在单元A 已成功地鉴权单元B后，单元B通过发送AU_RAND_B（不同于单元A发布的AU_RAND_A）到单元A来鉴权单元A，而且从新的AU_RAND_B导出SRES和SRES'，单元A的地址和链接字K_{AB}。

如果鉴权ACO的值是成功的，它通过E_1过程保留。

14.4.1　重试

当鉴权意图失败时，在新的鉴权意图可构成前，必须经历一个确定的

等待间隔。用相同蓝牙地址的后续鉴权意图失败时，等待间隔将以指数规律递增。即：在每次失败后，每次新的意图能构成前，等待间隔将是先前意图间隔的两倍。等待间隔用了一个最大值加以限制。最大等待间隔取决于执行。在确定的时间区内，当没有新的失败意图形成时，等待时间将以指数规律递减到最小。该过程防止非法使用者使用大量不同字重复鉴权过程。

为使系统少受拒绝服务攻击破坏，各蓝牙单元在确立链接时，将保持一个相互独立的等待间隔表。显然，该表的大小受到必须只包含最近链接已构成的 N 个单元限制。不同单元数 N 的变化取决于可用存储器大小和用户环境。

14.5 鉴权和字生成函数

该节描述的算法意指支撑蓝牙在鉴权和字生成上安全要求。

14.5.2 证明函数E_1

为蓝牙提出的证明函数E_1是一种可计算的安全鉴权码，或常称为 MAC。E_1用作加密函数称SAFER+。该算法是一种现有 64 位块密码 SAFER-SK128 的增强型版本，而且可随意使用。在块密码结果里用函数 Ar来标注，它映射在 128 位字下，128 位输入到 128 位输出，即：

$$Ar：\{0，1\}^{128} * \{0，1\}^{128} \rightarrow \{0，1\}^{128}$$

$$（\quad k \quad |\!\rightarrow * \quad x \quad ） \qquad t$$

（等式 31）

Ar 的详细描述在下节给出。函数用 Ar 构成。如下表示：

$$E1：\{0，1\}^{128} * \{0，1\}^{128} * \{0，1\}^{48} \rightarrow \{0，1\}^{32} * \{0，1\}^{96}$$

$$（K,RAND,address） \quad |\!\rightarrow (SRES,ACO)$$

（等式 32）

这儿 SRES = Hash（K，RAND，address，6）[0，.....，3]，这儿 Hash 是一个键控混编函数。其定义为：

$$Hash：\{0，1\}^{128} * \{0，1\}^{128} * \{0，1\}^{8*L} \rightarrow \{6，12\} * \{0，1\}^{128}$$

$$（K，I_1，I_2，L） |\!\rightarrow A'r（[K]，[E（I_2，L）+_{16}（A\ r（K，I_1）_{16} \oplus I_1）]）$$

（等式 33）

$$E：\{0，1\}^{8*L} * \{6，12\} \rightarrow \{0，1\}^{8*16}$$

$$（X[0,.....,L-1]，L） |\!\rightarrow （X[i（mod L）] \quad （i =0,,,,, 15）$$

（等式 34）

而且这儿是一个L的展开式，八进制字X为 128 位字。于是我们看到作

为每次E_1的计算，函数Ar必须作两次计算。对于Ar（实际A’r）的第二次使用密钥K’是来自如下的K的补偿。

K[0] =（K[0]+233） mod 256, K[1] = K[1] ⊕ 229，

K’[2] =（K[2]+233）mod 256, K[3] = K[3] ⊕ 193，

K’[4] =（K[4]+179）mod 256, K[5] = K[5] ⊕ 167，

K’[6] = （ K[6]+149 ） mod 256, K[7] = K[7] ⊕ 131 ，（等式 35）

K’[8] = K[8] ⊕233， K’[9] =（K[9]+229） mod 256,

K’[10] = K[10] ⊕233， K’[11] =（K[11]+193）mod 256,

K’[12] = K[12] ⊕179， K’[13] =（K[13]+167）mod 256,

K’[14] = K[14] ⊕149， K’[15] =（K[15]+131）mod 256,

E_1的计算数据流程图如图所示：

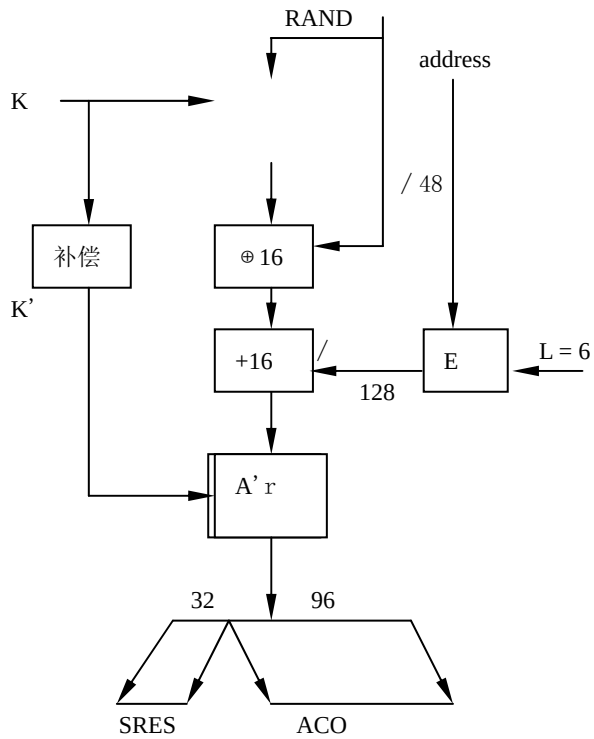


图 2.76 E_1算法的数据流

E_1也用作传递经E3 在计算密钥生成的ACO参数（验证计算补偿），见等式 23 和 24。ACO的值通过在等式 33 定义的Hash函数输出的八进制 4 到 15 而形成。即：

ACO = Hash(K, RAND, address, 6)[4, ... , 15] （等式 36）

14.5.3 函数 Ar 和 Ar’

函数 Ar 同 SAFER+一样。它由 8 层设置组成（每层称作一个循环）和一个生成子密钥 Kp[j],p=1,2,.....,17 的并行机制，用在各个循环里的子密钥称为循环密钥。函数将从 128 位“随机”输入流里和 128 位“密钥”里产生一个 128 位结果。除 Ar 函数外，归类于 Ar’的稍作修改的版本用于循环 1 的输入加在第 3 循环的输入上。这种做法构成一个不能颠倒的修改版本并且防止了 Ar’作为加密函数。详情见图所示：

画图 14.13

图 2.77

14.5.2 循环计算

各循环的计算是加密和循环密钥，替换，下次循环密钥的加密以及最终 Pseudo Hadamard Transform（PHT）组合。循环里计算如 Ar’函数详情描述图所述。循环的子密钥 r，r = 1，2，.....，8 标注为：K2r-1[j],K2r[j],j=0,1，.....，15。在最后循环 K17[j]后，整个以前

的奇数密钥以相同方式使用。

14.5.2.1 替换框“e”和“l”

上图中出现了标有“e”和“l”的两个框。这些框完成用在 SAFER+相同替换；即：它们完成

e，l ： {0,.....,255} → {0,.....,255},

e ： i |→ $(45^{i}(\mathrm{mod}257))$ (mod256),

l ： i |→ js.t.i=e (j)。

在 SAFER+算法里，它们的任务是导出非线形。

14.5.2.2 密钥时序安排

在各个循环里，需要两批八位字节宽的密钥。这些循环密钥通过指定在SAFER+里的密钥时序安排导出。下图给出了循环密钥Kp[j]如何确定的概述。位移向量B_2，B_3，. . . . . , B_{17}据等式算出。

（等式 37）

画图 14.14

图 2.78

14.5.3 鉴权E_2密钥生成函数

用于鉴权的密钥通过该图所示的过程导出。

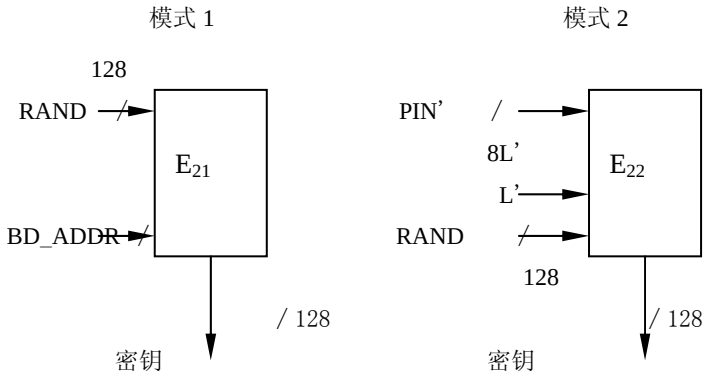


图 2.79

密钥生成算法E_2及两种模式。模式 1 用于单元和组合字，模式 2 用于Kmaster和Kinit。

该图说明了两种算法操作的不同模式。在第一种模式里，函数E_2在 128 位RAND输入值和 48 位地址，128 位链接密钥K上产生。当创建单元密钥和组合密钥时，该模式得以应用。在第二种模式里，函数E_2在 128 位RAND输入值和L八位字节PIN用户，128 位链接密钥K上产生。第二种模式用于创建初始化密钥和主单元密钥的随机发生场合。当初始化密钥生成时，PIN用申请单元的BD_ADDR扩充。该扩充利用直接跟随在PIN最有效的八位字节地址的最小有效八位字节的开始。由于用于算法里的PIN最大长度不能超过 16 个八位字节，所以可能并非一定要使用BD_ADDR的整个八位字节。

该密钥算法再次开拓了加密函数。E_2形式上能以模式 1（标注E_{21}）表示。

$$E_{21}: \{0, 1\}^{128} * \{0, 1\}^{48} \rightarrow \{0, 1\}^{128}$$

$$(\quad RAND \quad , \quad address \quad) \qquad A'r(x, y)$$

（等式 38）

这儿（模式 1）

$$X = RAND[0,,,,, 14] \cup (RAND[15] \oplus 6)$$

$$15$$

（等式 39）

$$Y = \bigcup_{i=0}^{15} address\,[i \pmod 6]$$

设 L 是用户 PIN 八位字节的数。算法通过等式 40 定义，

$$PIN' = \begin{cases} PIN[0,,,,, L-1] \cup BD\_ADDR_B[0,,,,, \min\{5, 15-L\}], & L<16, \end{cases}$$

（等式 40）

$$-\ \mathrm{PIN}[0,,,,,\ L-1], \qquad L=16,$$

等式中假设单元B是申请者。然而，在模式 2 里，E_2（标注E_{22}）能够表示为：

$$E_{22}: \{0,\ 1\}^{8L'} * \{0,\ 1\}^{128} * \{1,\ 2\ ,,,,,\ 16\} \rightarrow \{0,\ 1\}^{128}$$

$$(\ \mathrm{PIN'}\ ,\ \ \mathrm{RAND}\ \vdash\!\!\rightarrow \mathrm{L'}\ ) \qquad A'r(x,y)$$

（等式 41）

这儿

$$\begin{cases} X = \bigcup_{i=0}^{15} \mathrm{PIN'}[i\ (\ \mathrm{mod}\ L')], \end{cases}$$

（等式 42）

$$-\ Y = \mathrm{RAND}[0,,,,,\ 14]\ \cup\ (\mathrm{RAND}[15] \oplus L'),$$

等式中 L’ = min{16，L+6}是在 PIN 里八位字节的数。

14.5.4 加密E_3密钥生成函数

加密密钥K_C经E_3产生的E_0用过。函数E_3是使用如下的A’r构成，

$$E_3: \{0,\ 1\}^{8L'} * \{0,\ 1\}^{128} * \{0,\ 1\}^{96} \rightarrow \{0,\ 1\}^{128}$$

$$(K, RAND, COF) \vdash\!\!\rightarrow \qquad Hash(K, RAND, COF, 12)$$

（等式 43）

等式中Hash是一个如等式 33 定义的混合函数。注意，产生密钥的长度是 128 位。然而，在E_0内使用前，加密密钥K_C将被压缩为当前加密密钥长度。E_3的块方案如图所示。

图中 COF 的值通过等式 23 指定来确定。

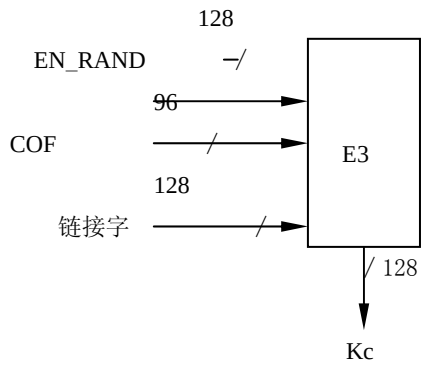


图 2.80 生成加密字

第 3 章 链路管理器协议

本规范描述链路管理器协议（LMP）。该协议用于链路设置和控制。通过该协议，收方链路管理器对信号进行识别和筛选，而不再转发到更高协议层。

目录

1. 概述

LMP 消息用于建立链路、加密和控制。它们是以有效载荷而不是以 L2CAP 的方式来传送，并通过有效载荷头 L_CH 域的保留值加以区别。该消息由接收方 LM 过滤和解释，并不得转发到更高协议层。

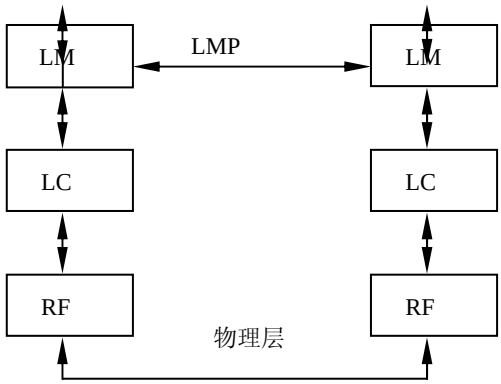


图 3.1 链路管理器全局视图

链路管理器消息具有比用户数据更高的优先级。这就是说，尽管链路管理器消息发送会被个别基带数据分组延迟,但不得被 L2CAP 通信延迟。

既然，LC 提供了可靠连接，我们则不必对 LMP 消息十分了解。（参见基带规范）。

根据过程规则，收到承载有 LMP PDU 的基带数据分组和发送承载有合法应答 PDU 的基带数据分组之间的时间不能大于 LMP 的最大应答延时。该最大应答延时为 30 秒。

LMP 格式

LMP PDU 总是以单时隙分组的方式发送，因此有效载荷头只占用一个字节。由有效载荷头的两个最低位确定逻辑信道。对于 LMP PDU，这些位设置为:

表 3.1 逻辑信道 L_CH 域内容

L_CH 代码	逻辑信道	信息
00	NA	未定义

01	UA/1	继续发送 L2CAP 消息
10	UA/1	开始发送 L2CAP 消息
11	LM	LMP 消息

有效载荷头通常只有一个 FLOW 位，并被接收方忽略。每个 PDU 都分配了一个 7 位的操作码，用于唯一标识不同类型的 PDU。操作码与一个 1 位的事务 ID 设置于有效载荷的首字节。事务 ID 则位于该字节最低位。如果 PDU 属于由主单元发起的事务，则事务 ID 为 0；如果 PDU 属于由从单元发起的事务，则事务 ID 为 1。如果 PDU 分组含一个或多个参数，则这些参数位于有效载荷的第二个字节。字节数根据参数长短确定。如果存在一个使用 HV1 数据分组的 SCO 链路，并且其内容长度不足 9 个字节，那么 PDU 可以 DV 数据分组发送，否则使用 AM1 分组发送。所有的参数都用小端格式，即首先发送最低位字节。

协议数据单元的源地址和目的地址由消息头的 AM_ADDR 决定。

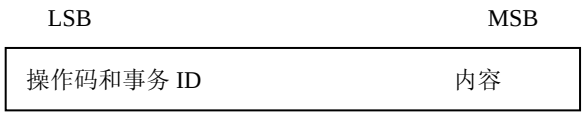


图 3.2　LMP PDU 被发送时的有效载荷

每个 PDU 可以为必选或可选的。必选或可选项在第三节的表里已列出。LM 不能发送可选的 PDU。如果需要应答，则按第三节的过程规则发送一个有效应答， LM 则必须识别所有收到的可选 PDU。其原因在于 LMP 不支持的特性。如果不需要应答收到的可选 PDU，则不发送应答消息。

过程规则与 PDU

每一过程都是以序列图形式进行描述，以下符号用于序列图：

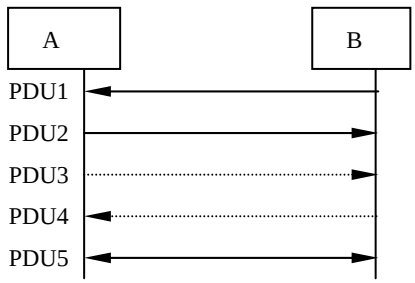


图 3.3 用于序列图的符号

PDU 1 是由 A 传到 B 的协议数据单元。PDU 2 是由 B 传到 A 的协议数据单元。PDU 3 是从 A 传到 B 的可选协议数据单元。PDU 4 是从 B 传到 A 的可选协议数据单元。PDU 5 是从 A 或 B 发出的协议数据单元。垂直线表示可

选择发送更多的协议数据单元。

3.1 通用应答消息

LMP_accepted 与 LMP_not_accepted 协议数据单元在不同过程中用作其它 PDU 的应答消息。LMP_not_accepted 协议数据单元分组含接受消息的操作码，LMP_not_accepted 协议数据单元分组含未接受消息的操作码以及未接受该消息的原因。

表 3.2 通用应答消息

m/o	PDU	内容
M	LMP_accepted	操作码
M	LMP_not_accepted	操作码 原因

3.2 认证

认证过程基于竞争应答模式（参见基带规范）。验证器发送一个 LMP_au_rand PDU 给请求者，该 PDU 分组含一个随机数（或竞争码）。请求者计算出应答值，该应答是竞争码、请求者 BD_ADDR 和保密字的函数。然后将应答发回验证器验证应答是否正确。计算应答值的过程参阅基带规范。认证应答的正确计算需要两设备共享同一保密字。主单元和从单元都可作为验证器。以下协议数据单元可用于认证过程：

表 3.3 用于认证的 PDU

M/O	协议数据单元	内容
M	LMP_au_rand	随机数
M	LMP_sres	鉴定应答

3.2.1 请求者具有链接字

如果请求者具有与验证器关联的链接字，则请求者计算出应答值并连带 LMP_ sres 发送到验证器，由验证器检查其应答值。如果应答值不正确，验证器则发送附加原因码 authentication failure 的 LMP_ detach 终止连接。

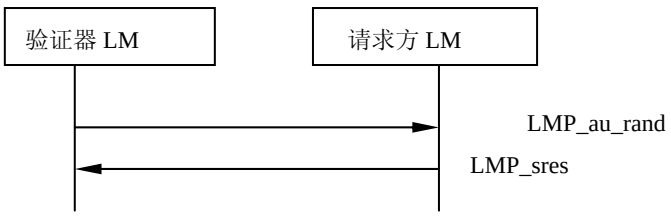


图 3.4 认证、请求者具有链接字

3.2.2 请求者无连接键

如果请求者没有与验证器关联的连接键，在 LMP_ au_rand 收到后，请求者则发送附加原因码 key missing 的 LMP_not_accepted 消息。

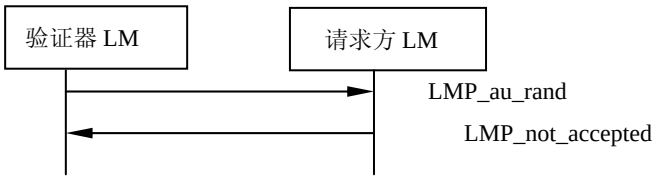


图 3.5 认证失败、请求者无链接字

3.2.3 重试

验证失败后，实施基带规范所述方案，以防入侵者短时间尝试多个字。

3.3 匹配

当两台设备无共用链接字时，则基于PIN和随机数创建初始化键K_{init}。在验证器向请求者发出LMP_in_rand时创建K_{init}键。如何创建键请参阅基带规范。然后进行认证，其计算过程基于K_{init}键，而非链接字。通过认证后，链接字即被创建。用于匹配过程的PDU为：

表3.4 用于匹配过程的PDU

M/O	协议数据单元	内容
M	LMP_in_raand	随机数
M	LMP_au_rand	随机数
M	LMP_sres	认证应答值
M	LMP_comb_key	随机数
M	LMP_unit_key	键

3.3.1 请求者接受匹配

验证器发出LMP_in_rand，而请求者用LMP_accepted应答。两设备计算出K_{init}键，然后基于此键进行认证。验证器检查认证应答值，如正确，就创建链接字；否则，验证器则发送附加原因码认证失败（authentication failue）的LMP_detach终止连接。

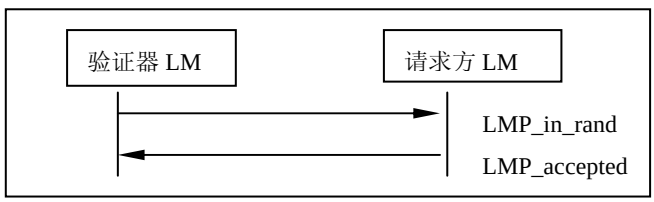


图3.6 请求者接受匹配

3.3.2 请求者请求成为验证器

如果请求者有一固定的 PIN,就可以通过生成一个随机数请求进行“请求者—验证器”角色切换，并在LMP_in_rand中发回该随机数。如果启动匹配过程的设备具有变量 PIN,它必须接受这个变量并用LMP_accepted应答。这样角色就成功地进行了切换。

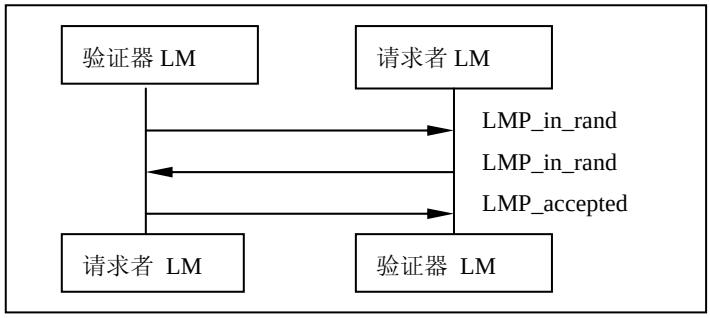


图3.7 请求者接受匹配并请求成为验证器

如果启动匹配过程的设备有固定的PIN,而另一设备请求进行角色切换,则可以通过发送 附加原因码匹配不允许（pairing not allowed）的LMP_not_accepted拒绝进行切换,然后终止该匹配过程。

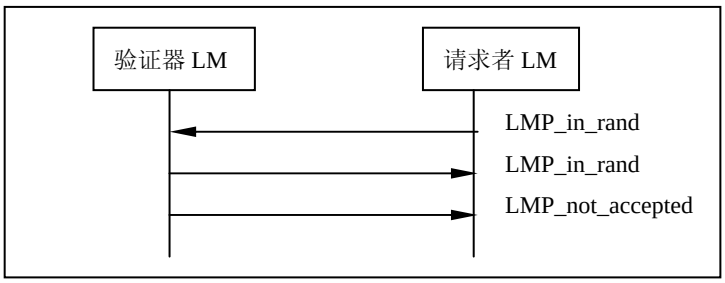


图3.8 不成功的“请求者—验证器”角色切换过程

3.3.3 请求者拒绝匹配

如果请求者拒绝匹配，则在收到LMP_in_rand 后发出附加原因码不允许（not allowed）的LMP_not_accepted。

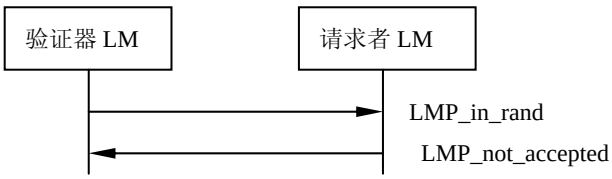


图3.9 请求者拒绝匹配

3.3.4 创建链接字

认证结束后，必须创建链接字。该链接字用于两设备间的所有后续连接的认证，直到该链接字改变为止。匹配过程中创建的链接字可以是组合键，或者是一个单元的单元键。以下规则用于链接字的选择：

* 如果一单元发送 LMP_unit_key，另一个单元发送 LMP_comb_key，那么该单元键即为链接字；
* 如果两单元都发送 LMP_unit_key，那么主单元键即为链接字；
* 如果两个单元都发送 LMP_comb_key，链接字将按基带规范所述过程进行计算。

LMP_unit_key 的内容是单元键与K_{init} 进行XOR操作的结果值。P_comb_key 的内容是LK_RAND与K_{init} 进行XOR操作的结果值。任何配置为使用组合键的设备都将该链接字存储在固定存储器中。

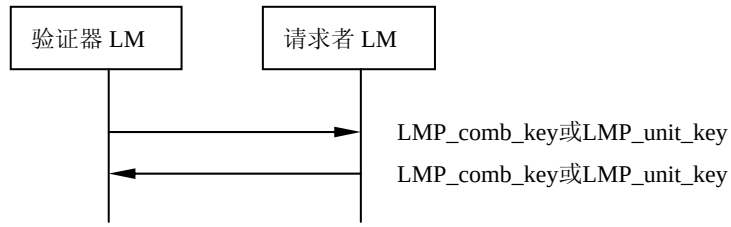


图3.10 创建链接字

3.3.5 重试

由于认证应答出错而引起处于匹配过程中的认证失败时，则执行重试方案。这样，可防止入侵者在短时间内使用大量不同PIN的侵入企图。

3.4 改变链接字

如果两设备匹配，且链接字来自于组合键，那么就可以改变链接字。如果链接字就是单元键，则必须完成匹配过程后才能改变链接字。而PDU内容可以通过与当前链接字进行XOR运算得到保护。

表3.5 用于改变链接字的PDU

M/O	协议数据单元	内容
M	LMP_comb_key	随机数
M	LMP_unit_key	键

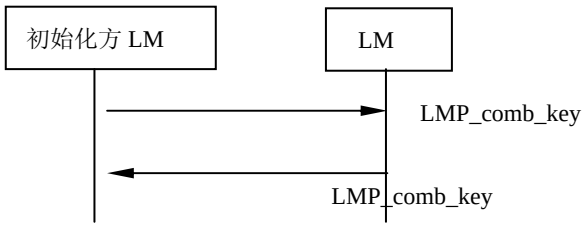


图3.11 改变链接字

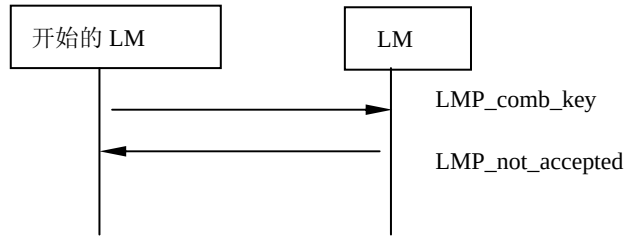


图3.12

因另一单元使用单元键而不能进行链接字改变,如果成功改变链接字,就将新链接字存储在固定存储器中，而旧链接字则被删除。直到该链接字再次改变为止，新链接字将作为链接字用于两设备间的以下连接。新链接字即成为当前链接字。新链接字将一直作为当前链接字，直到再次发生改变，或者创建临时链接字为止。

如果正在对该链路加密，且当前链接字为临时链接字，则可以调用改变链接字过程立即终止加密。然后，可重新再启动加密过程。这样就可保证当半永久性链接字成为当前链接字时，不会使用匹克网中其它设备已知加密参数的加密过程。

3.5 改变当前链接字

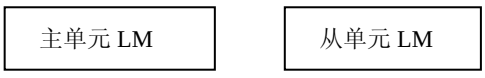
当前链接字可以是半永久性链接字或临时链接字。可以临时改变它，但改变只对本次会话有效。参见第151页基带规范14.2.1节。如果匹克网支持加密广播，则必须将当前链接字改变为临时链接字。

表3.6 用于改变当前链接字的PDU

M/O	协议数据单元	内容
M	LMP_temp_rand	随机数
M	LMP_temp_key	键
M	LMP_use_semi_permanent_key	

3.5.1 改变为临时链接字

通过创建主键 K_{master} 启动主单元后,主单元发出一随机码 RAND，并将它分组含在LMP_temp_rand中 发往从单元。然后双方进行叠加运算，得到OVL = E_{22}(当前链接字，RAND，16)，主机再将附加OVL的模为2的K_{master} 在LMP_temp_key中发往从单元。而识别OVL的从单元则计算 K_{master}。这样K_{master}即成为当前链接字，并且将一直保持到创建新的临时链接字，或者改变该连接键。



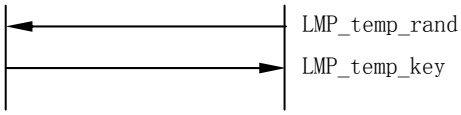


图3.13 改变为临时链接字

3.5.2 将半永久性链接字置为当前链接字

当前链接字变为K_{master}后，可以撤销该改变，并将半永久性链接字恢复为当前链接字。如果链路已加密，则将通过调用恢复为半永久性键的过程立即停止加密。可重新再启动加密过程。这样就可保证当半永久性链接字成为当前链接字时,不会使用匹克网中其它设备已知加密参数的加密过程。

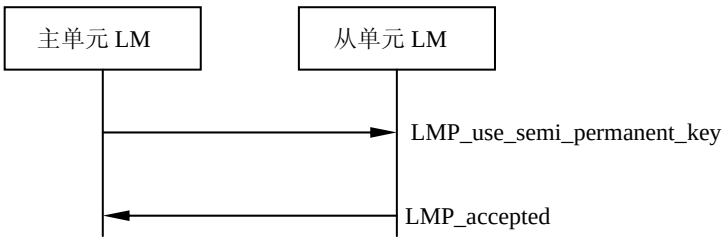


图3.14 链接字改变为半永久性链接字

3.6 加密

只有执行了至少一次的认证过程，才可以使用加密。如果主单元要求匹克网中所有从单元使用相同加密参数，那么在开始加密之前，主机必须发送临时键（K_{master}），并将该键置为匹克网中所有从单元的当前链接字。如果要对广播数据分组加密,必须执行该过程。

表3.7 用于加密的PDU

M/O	协议数据单元	内容
O	LMP_encryption_mode_req	加密模式
O	LMP_encryption_key_size_req	键长度
O	LMP_start_encryption_req	随机码
O	LMP_stop_encryption_req	

3.6.1 加密模式

首先，主、从单元在是否使用加密，是否对点与点的数据分组加密，是否对点与点和广播数据分组都加密等方面必须保持一致。如果主、从机一致采用加密模式，主单元将继续发出更多关于加密的信息。

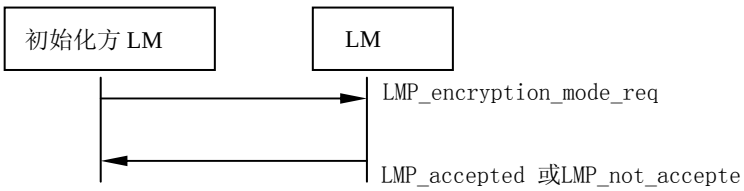


图3.15 协商加密模式

3.6.2 加密字长度

然后，将决定加密字长度。以下我们使用与基带规范相同的术语。主单元发出分组含键长度推荐值 Lsug，m 的LMP_encryption_key_size_req，该键与L max，m相等。如果L min，s ≤ L sug，并且从单元支持 Lsug,m ，那么它将返回 LMP_accepted ，键的长度则设置为Lsug。如果两条件都不能满足，从单元将返回分组含从单元长度推荐值Lsug,s 的LMP_encryption_key_size_req。该值是从单元所支持的最大的键长度，但它比Lsug,m 小。然后主单元将按照从单元推荐值执行相应测试。此过程将重复执行，直到主从双方确定了一致的键长度，或者明确知道不能确定键长度。一旦确定了一致的键长度，任一单元最后将发送 LMP_accepted 以及键的长度。

接下来，将使用 LMP_encryption_key_size_req，然后开始加密。如果没有确定一致的键长度，任一单元则发送 LMP_not_accepted，该LMP_not_accepted 附加原因码Unsupported parameter value（不支持的参数值），这时主从单元将不能使用蓝牙链路加密进行通信。

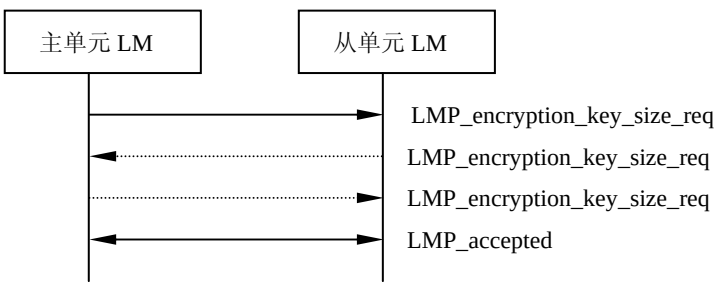
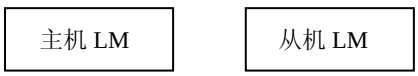


图3.16 加密字长度协商成功



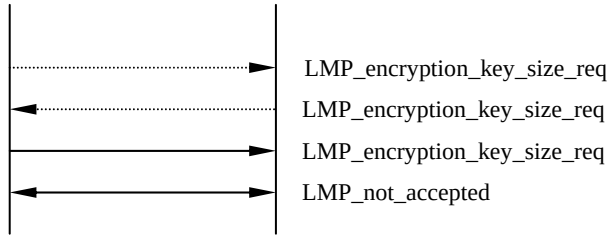


图3.17 加密字长度协商失败

3.6.3 开始加密

最后，开始加密。主机发送随机数 EN_RAND 并计算出加密字为 K c =E 3 （当前连接键，EN_RAND, COF ）。参见基带说明的COF定义。如果匹克网支持加密广播，该随机数必须在所有从单元上保持一致。然后，主机发送分组含 EN_RAND的 LMP_start_encryption_req。 收到该消息并通过LMP_accepted确认后，从单元计算Kc值。对于主从单元，Kc和 EN_RAND都被用作加密运算法则Eo的输入参数。

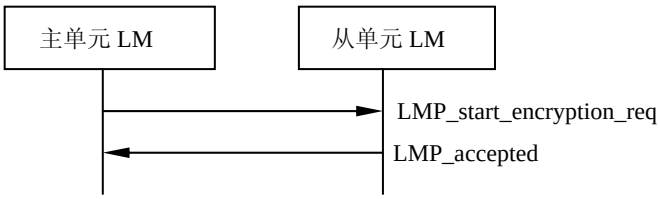


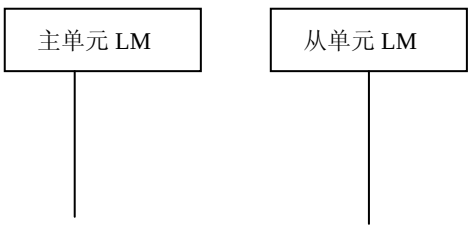
图3.18 开始加密

开始加密前，必须暂时停止高层数据通信，以防收到错误数据。加密启动过程可分为三步：

1. 设置主单元，以传输未加密数据分组，并接收加密数据分组。
2. 设置从单元传输和接收加密数据分组。
3. 设置主单元传输和接收加密数据分组。

在一、二步之间，已传输LMP_start_encryption_req后，可以进行主单元到从单元的数据传输。当从单元收到LMP_start_encryption_req时，激活第二步。在第二、三步之间，已传输LMP_accepted后，可以进行从单元对主单元传输。当主机收到LMP_accepted时，激活第三步。

3.6.4 停止加密



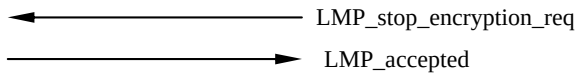


图3.19 停止加密

停止加密以前，必须临时停止高层数据通信，以防收到错误数据。停止加密过程分成三步，与开始加密的过程相同。

1. 设置主单元，传输未加密数据分组，并接收加密数据分组。
2. 设置从单元，传输和接收加密数据分组。
3. 设置主单元，传输和接收未加密数据分组。

第一、二步之间，已发送LMP_stop_encryption_req后，可进行主单元到从单元的通信。当从单元收到LMP_stop_encryption_req时，激活第二步。在第二、三步之间，已发送 LMP_accepted后，可进行从单元到主单元的通信。当主单元收到LMP_accepted时，激活第三步。

3.6.5 改变加密模式，键或随机数

如果需要改变加密模式、加密字或加密随机数，必须首先停止加密，然后再用新的参数重新启动。

3.7 请求时钟补偿

当从单元收到调频（FHS）分组时，就可以计算出从单元时钟值与主单元时钟值之差，主单元时钟值分组含在FHS有效载荷内。每次从主单元接收数据分组时都要计算该时钟补偿值。连接过程中主单元可在任意时间请求该时钟补偿。通过记录时间补偿，主单元就可以知道从单元离开匹克网后在哪一条RF信道上被激发过来进行呼叫扫描。这样，可以在下次该设备被叫时，缩短呼叫时间。

表3.8 用于时钟补偿请求的PDU

M/O	协议数据单元	内容
M	LMP_clkoffset	
M	LMP_clkoffset_res	时钟补偿

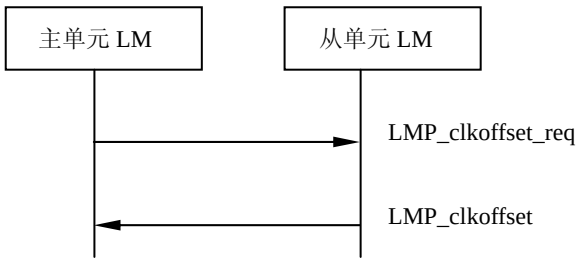


图3.20 时钟补偿请求

3.8 时钟补偿信息

通过利用LMP_slot_offset，就可以传输不同匹克网之间时间补偿信息。协议数据单元携带时钟补偿和BD_ADDR参数。该时钟补偿以μs为单位。该时间补偿也就是第一个匹克网中主单元TX时隙的开始时间,到第二个匹克网主单元TX时隙开始时间之间的时间。其中，第一个匹克网用于传输PDU，而第二个匹克网的主单元地址为BD_ADDR。

在进行主从单元切换之前，就可以从切换为主单元的设备发送PDU。如果由主单元初始化该切换过程，则从单元在发送LMP_accepted前应先发送LMP_slot_offset。如果由从单元初始化该切换过程，从单元在发送LMP_switch_req前应先发送 LMP_slot_offset。PDU也可以用于匹克网与匹克网之间的通信。

表3.9 用于时钟补偿信息的PDU

M/O	协议数据单元	内容
O	LMP_slot_offset	时隙补偿 BD_ADDR

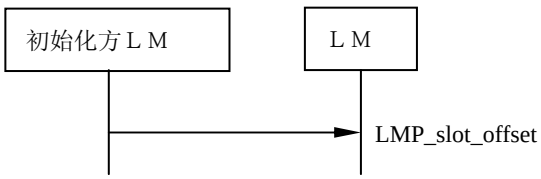


图3.21 发送时钟补偿信息

3.9 计时精度信息请求

LMP支持计时精度请求。当准备返回挂起状态并增加扫描窗口最大挂起时间时，该信息能够针对给定保持时间最小化扫描窗口。而且，该信息也可在扫描呼吸模式时隙和扫描休眠模式信标数据分组时，用于最小化扫描窗口。返回的计时精度参数是drift和jitter，其中drift以ppm为单位，jitter以在挂起、呼吸和休眠模式中使用时钟的μs为单位。这些参数对于一台特定设备固定不变，而且要求在多次请求中都应保持一致。如果设备不支持计时精度信息，那么当它收到该信息请求时，就发送附带原因码unsupported LMP feature（不支持的LMP特性）的LMP_not_accepted消息。请求方设备在这种情况下必须采用计时精度底限值（drift=250 ppm，jitter=10μs）。

表3.10 用于请求计时精度信息的PDU

M/O	协议数据单元	内容
O	LMP_timing_accuracy_req	
O	LMP_timing_accuracy_res	drift jitter

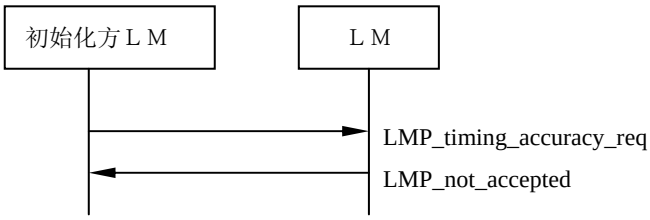


图3.22 被请求设备支持计时精度信息时的处理过程

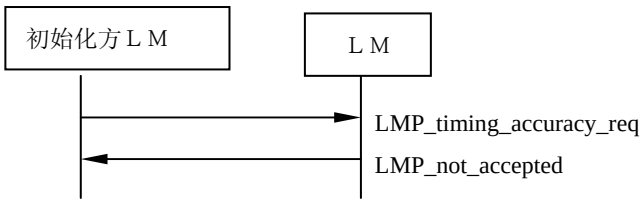


图3.23 被请求设备不支持计时精度信息的处理过程

3.10 LMP版本

LMP支持对LMP协议版本的请求。被请求设备将发送响应消息,该消息具有三个参数: VersNr, CompId 和 Sub-VersNr。VersNr说明设备支持的蓝牙LMP规范版本。CompId 用于跟踪低层蓝牙可能出现的问题。任何创建连接管理器各自执行版本的厂商都具有自己的 CompId。同样这些公司也要负责管理和维护 SubVersNr。建议所有厂商为每一RF/BB/LM执行版本创建各自的SubVersNr。对于某一给定VersNr和CompId,每发布一个新的执行版本, SubVersNr 的值就必须随之增加。对于 CompId 和 SubVersNr, 0xFFFF 的值表示没有使用合法值。不能针对LMP版本执行协商机制。以下序列用于交换参数。

表3.11 用于LMP版本请求的PDU

M/O	协议数据单元	内容
M	LMP_version_req	VersNr Compld SubVersNr
M	LMP_version_res	VersNr Compld

		SubVersNr

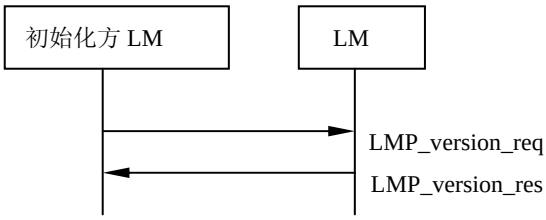


图3.24 LMP版本请求

3.11 蓝牙支持特性

蓝牙无线电和链路控制器只支持基带规范和无线电规范中所定义的数据分组类型和特性的部分子集。LMP_features_req 与 LMP_features_res 等PDU就是用于交换这一信息。一台设备在获得其它设备支持特性信息之前，只能发送ID、FHS、NULL、POLL 和 DM1数据分组。只有在执行了特性请求后，才能够发送通信双方共同支持的数据分组类型。一旦发出一个请求，该请求必须与其它设备的支持特性相兼容。例如，当建立一个 SCO 链路时，如果其它设备不支持 HV3数据分组，建议初始化方也不使用HV3数据分组。只有LMP切换**注册**和时钟偏移信息例外，当两蓝牙设备建立连接，并且请求方还未获知另一方特性以前，它们可以作为第一个LMP消息发送出去（切换是可选特性）。

表3.12 用于特性请求的PDU

M/O	协议数据单元	内容
M	LMP_features_req	features
M	LMP_features_res	features

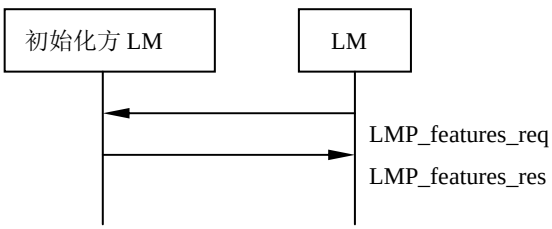


图3.25 请求支持特性的过程

3.12 主从角色切换

由于呼叫设备一般都是匹克网的主单元,因此有时需要进行主从单元角色切换。假设设备A为从单元，设备B为主单元,初始化切换的设备将结束

当前 L2CAP 消息的传输，然后再发送LMP_switch_req。

如果接受切换，另一设备将结束当前 L2CAP消息的传输，并以LMP_accepted应答。然后，执行基带规范的过程。

如果拒绝切换，另一设备以LMP_not_accepted应答，不进行切换。

表3.13 用于主从切换的PDU

M/O	协议数据单元	内容
O	LMP_switch_req	

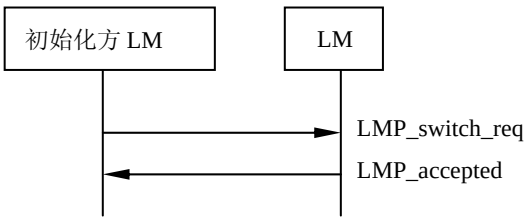


图3.26 接受主从切换

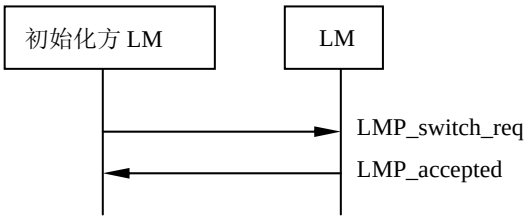


图3.27 未接受的主从切换

3.13 请求命名

LMP支持向另一蓝牙设备请求命名。名字是与蓝牙设备相关联的名字。根据UTF-8 标准，名字最大可由 248 个编码字节构成。名字分为一个或多个DM1数据分组。当发送 LMP_name_req 时，名字偏移表示需要哪一段。对应的 LMP_name_res 具有相同的名字偏移，名字长度表示蓝牙设备名字的总字节数和名字段,这里:

- 如果(N+名字偏移)<名字长度， 名字段(N)=名字(N+名字偏移)
- 否则,名字段（N）= 0

其中,0 ≤ N ≤ 13。在第一个发出的LMP_name_req中，名字偏移=0。同时重复序列25，直到初始化方收集到所有名字段。

表3.14 用于名字请求的PDU

M/O	协议数据单元	内容

	LMP_name_req	名字偏移
	LMP_name_res	名字偏移 名字长度 名字段

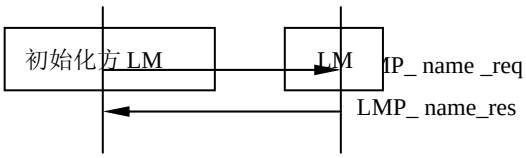


图3.28 请求的设备名及其响应

3.14 断开连接

两蓝牙设备间的连接可在任意时间由主单元或从单元关闭。同时，在通知另一方的消息中分组含通信关闭原因的参数。

表3.15 用于断开连接的PDU

M/O	PDU	内容
M	LMP_detach	原因

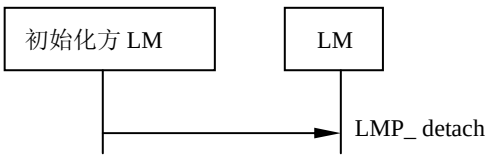


图3.29 通过发送LMP_detach关闭通信

3.15 挂起模式

两设备间的 ACL链路可在指定挂起时间内置为挂起状态。在这段时间里，主单元不再发送 ACL数据分组。一般如果在相当长的一段时间内不必要发送数据，那么就可进入挂起模式。而且为了节能，应关闭收发器。但是如果设备要搜索其它设备或被其它蓝牙设备搜索到，或者要加入其它匹克网时，可使用挂起模式。实际上，设备在挂起时间内的动作不是由挂起消息决定的，而是由各设备自己决定。

表3.16 用于挂起模式的PDU

M/O	协议数据单元	内容
O	LMP_hold	控制时间

0	LMP_hold_req	控制时间

3.15.1 主机强制挂起模式

如果存在预先已经接受的挂起模式请求，就可以使用主单元强制挂起模式。当请求挂起模式时，挂起时间分组含于PDU，同时主单元强制模式不得长于从单元已接受的任何挂起时间。

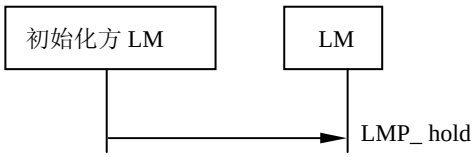


图3.30 主单元强制从单元进入控制模式

3.15.2 从机强制挂起模式

如果存在预先已经接受的挂起模式请求，就可使用从单元强制挂起模式。当请求挂起模式时，挂起时间分组含于PDU，同时从单元强制模式不得长于主单元已接受的任何挂起时间。

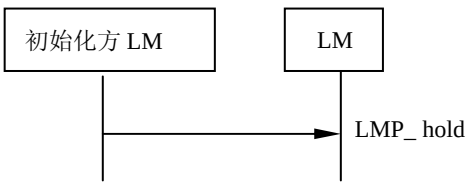
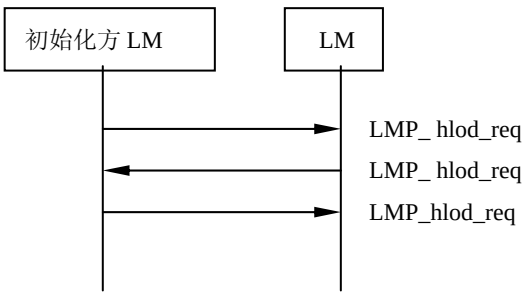


图3.31 从单元强制挂起模式

3.15.3 挂起模式请求

主单元或从单元可以请求进入挂起模式。一旦收到该请求，将返回含有经修改参数的相同请求，否则将终止协商。如果达成一致，LMP_accepted 则终止协商，并将ACL链路置为挂起模式。如果未达成一致，LMP_not_accepted 则终止协商，LMP_not_accepted 不含原因码 unsupported parameter value，且不能进入挂起模式。



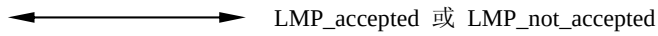


图3.32 挂起模式协商

3.16 呼吸模式

为了进入呼吸模式，主从单元将就呼吸间隔T_{sniff}，以及呼吸偏移D_{sniff}进行协商。二者说明了呼吸时隙计时方式。呼吸偏移确定第一个呼吸时隙的持续时间，然后按照呼吸间隔T_{sniff}周期性生成呼吸时隙。为了避免在初始化时时钟隐含的问题，应针对第一次时隙的计算选择其中两参数中的一个。主单元发出消息中的计时控制标志即表示使用哪一个参数。注意：只有域中第一位有效。当链路处于呼吸模式时，主单元只能在呼吸时隙中进行数据传输。由以上两个参数控制从单元的侦听动作。呼吸尝试确定呼吸时隙开始计时时，从单元必须侦听的时隙的个数。即使还没收到一个含有AM 地址的数据分组，也是如此。如果从单元继续接收只含有AM地址的数据分组，呼吸尝试参数将确定决定从单元必须侦听的时隙的个数。

表3.17 用于呼吸模式的PDU

M/O	协议数据单元	内容
O	LMP_sniff	计时控制标志，D_{sniff} T_{sniff} 呼吸尝试 呼吸超时
O	LMP_sniff_req	呼吸控制标志，D sniff T sniff 呼吸尝试 呼吸超时
O	LMP_unsniff_req	-

3.16.1 主机强制从机进入嗅模式

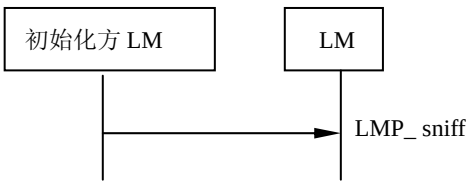


图3.33 主单元强制从单元进入呼吸模式

3.16.2 主单元或从单元请求呼吸模式

主单元或从单元可以请求进入呼吸模式。一旦收到该请求，将返回含有经修改参数的相同请求，否则将终止协商。如果达成一致，LMP_accepted 则终止协商，并将ACL 连接置于呼吸模式。如果未达成一致，LMP_not_accepted 则终止协商，LMP_not_accepted 不含原因码 unsupported parameter value，且不能进入呼吸模式。

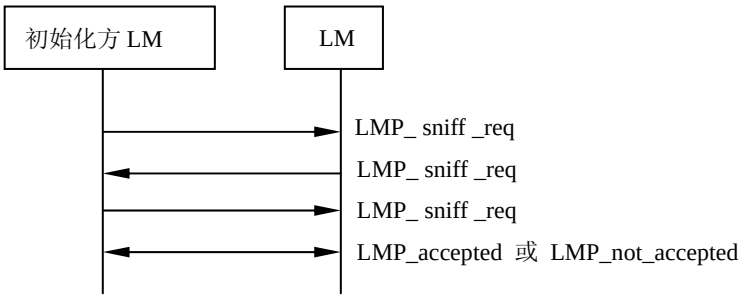


图3.34 呼吸模式协商

3.16.3 将从单元从呼吸模式转为活动模式

通过发送LMP_unsniff_req协议数据单元可以结束呼吸模式。被请求设备必须以LMP_accepted 应答。如果是从单元请求，则在收到 LMP_accepted 后进入活动模式。如果是主单元请求，从单元则在收到 LMP_unsniff_req 后进入活动模式。

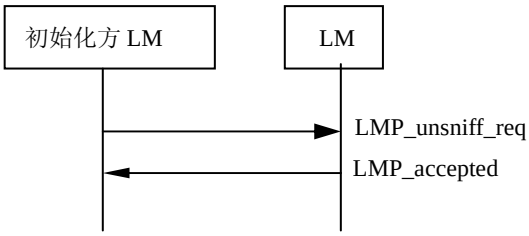


图3.35 从单元从呼吸模式转为活动模式

3.17 休眠模式

如果从单元不加入信道，但仍然要执行调频同步。那么它应置为休眠模式。这一模式中,设备放弃其AM_ADDR，但该设备仍然可以通过信标间隔开的信标实例被唤醒并与信道重新同步。信标间隔、信标偏移量和一个表示第一个信标实例计算方法的标志确定了第一个信标实例。此后，则以预先定义的信标间隔周期性发送信标实例。在信标实例中，休眠从单元能由主单元激活，主单元也能改变休眠模式参数，并传输广播信息或使休眠从单元请求访问信道。

广播就是从主单元向休眠从单元发送所有的PDU。这些PDU（LMP_set_broadcast_scan_window, LMP_modify_beacon, LMP_unpark_BD_addr_req 和 LMP_unpark_PM_addr_req）是仅有的能够发送到休眠从单元或用于广播的PDU。为了增加广播可靠性，数据分组应尽量短。所以，LMP的协议数据单元格式可有些不同。其参数不总以字节序列进行排列，而且PDU长度也可变。

控制休眠模式的消息分组含许多参数，这些参数都在基带规范中定义。一旦将一从单元置于休眠模式，也就同时给它指定了唯一的PM_ADDR。

主单元利用PM_ADDR可以解除从单元的休眠模式。如果PM_ADDR各位全部为零,则表示该PM_ADDR不合法。如果给一设备指定PM_ADDR，那么在该设备解除休眠模式时该PM_ADDR必须与AM_ADDR一致。

表3.18　用于休眠模式的PDU

M/O	协议数据单元	内容
O	LMP_park_req	-
O	LMP_park	计时控制标记 D_b T_b N_b Δ_b PM_ADDR AR_ADDR N_{Bsleep} D_{Bsleep} D_{access} T_{access} $N_{acc-slots}$ N_{poll} M_{access} 存取方案
O	LMP_sep_broadcast_scan_window	计时控制标志 D_b(可选) 广播扫描窗口
O	LMP_modify_beacon	计时控制标志 D_b(可选) T_b N_b Δb D_{access} T_{access} $N_{acc-slots}$ N_{poll} M_{access} 存取计划
O	LMP_unpark_PM_ADDR_req	计时控制标志 D_b(可选) AM_ADDR PM_ADDR AM_ADDR(可选) PM_ADDR(可选) (AM_ADDR, PM_ADDR合计的1-7对)
O	LMP_unpark_BD_ADDR_req	计时控制标志 D_B (可选) AM_ADDR BD_ADDR

		AM_ADDR(可选) BD_ADDR(可选)

3.17.1 主单元强制从单元进入休眠模式

主单元能够执行强制休眠模式。主单元可以结束当前 L2CAP消息的传输，并发送LMP_park。当收到该PDU时，从单元将结束当前 L2CAP消息的传输， 并发送LM_accepted。

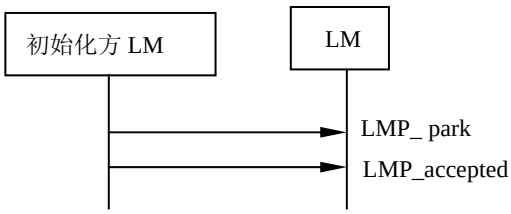


图3.36 从单元强制休眠模式

3.17.2 主单元请求从单元进入休眠模式

主单元能够请求休眠模式。主单元可以结束当前L2CAP消息传输，并发送LMP_park_req。如果从单元同意进入休眠模式，它将结束当前 L2CAP 消息传输，并发送LMP_accepted 应答。最后主单元将发出LMP_park。如果从单元拒绝进入休眠模式，则发送LMP_not_accepted。

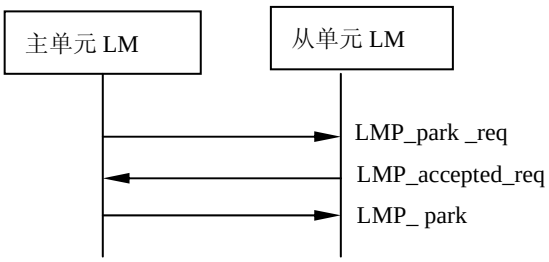


图3.37 从单元同意进入休眠模式

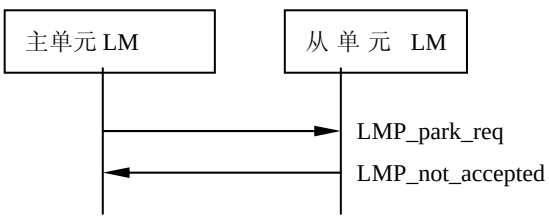


图3.38 从机拒绝进入休眠模式

3.17.3 从单元请求置于休眠模式

从单元能够请求休眠模式。从单元将结束当前L2CAP消息传输，并发送LMP_park_req。如果主机接受休眠模式，它将结束当前 L2CAP消息传输，

并发送 LMP_park。如果主机拒绝休眠模式，则发送LMP_park_req。

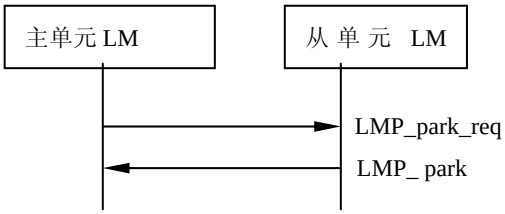


图3.39 主单元同意将从单元置为休眠模式

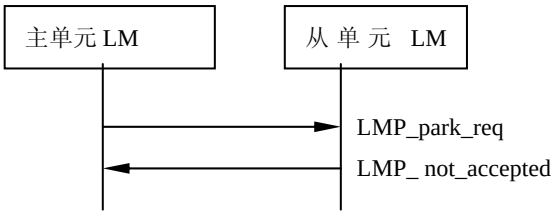


图3.40 主单元拒绝将从单元置为休眠模式

3.17.4 主机建立广播扫描窗口

如果需要比信标队列更大的广播能力，主单元将通过发送LMP_set_broadcast_scan_window，通知从单元会有更多广播信息在信标队列后传递过来。LMP_set_broadcast_scan_window通常是在信标时隙中以广播数据分组的形式发送。扫描窗口在信标实例中启动，并且只对当前信标有效。

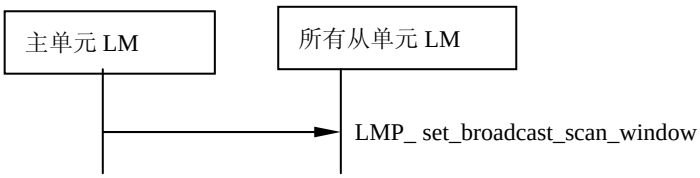
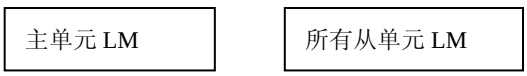


图3.41 主机通知所有从单元广播能力增加

3.17.5 主单元修改信标参数

当信标参数变化时，主单元将通过发送 LMP_modify_beacon把这个变化通知所有休眠从单元。该消息通常在信标时隙中以广播数据分组形式传输。



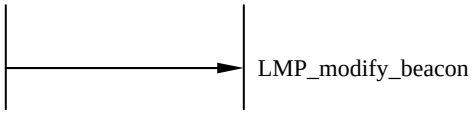


图3.42 主单元修改信标参数

3.17.6 解除休眠的从单元

主单元能够通过发送广播LMP消息解除一个或多个从单元的休眠状态。该广播LMP消息分组含设备的 PM_ADDR 或 BD_ADDR，而这些设备即主单元要在信标时隙中解除休眠的从单元。该广播LMP消息也分组含主单元分配给从单元的AM_ADDR。发送此消息后，主单元必须通过轮询每一个解除休眠的从单元(也就是发送 POLL 分组)检查解除休眠过程是否成功,以使该从单元获得可访问信道的授权。已解除休眠的从单元必须通过发送LMP_accepted进行应答。如果主单元发出解除休眠消息以后，在一定时间内没有从从单元收到LMP_accepted，则解除休眠失败，而主单元必须考虑从单元是否仍处于休眠模式。

有两种消息可供使用。对于以PM_ADDR标识的休眠设备使用一种,对于以BD_ADDR标识的休眠设备则使用另一种。两种消息都具有可变长度,其长度依赖于主单元要解除休眠的从单元的个数。对于主单元要解除休眠的每一从单元，AM_ADDR 分组含在有效载荷中，并且AM_ADDR 位于设备PM/BD_ADDR之后，而该设备地址则指定为AM_ADDR。如果从单元由 PM_ADDR 标识，那么利用同一消息最多可将七个从单元解除休眠。如果从单元由BD_ADDR标识，那么利用同一消息只能将两个从单元解除休眠。

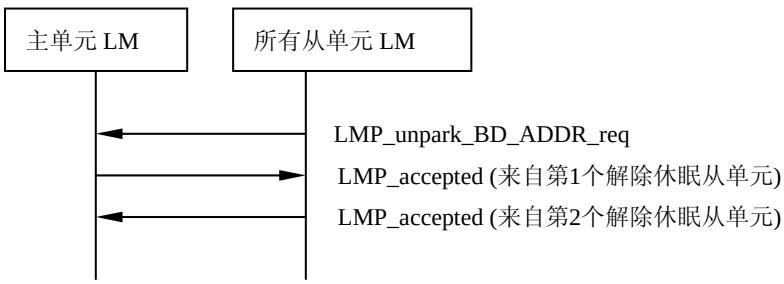
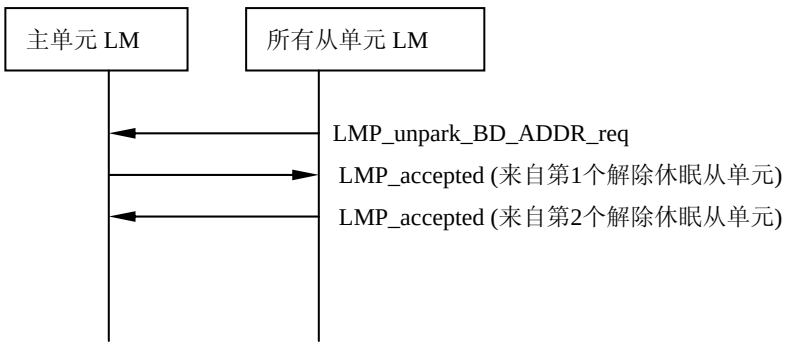


图3.43 主机将地址为 BD_ADDR 的从单元解除休眠



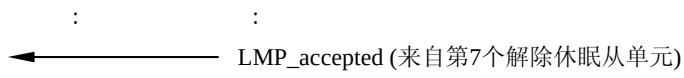


图3.44 主机将地址为 PM_ADDR 的从单元解除休眠

3.18 功率控制

如果 RSSI 值与蓝牙设备约定值差别太大，它可以增加或降低其它设备的 TX功率。一旦收到这一消息，输出功率出就增强或降低一个等级。主单元侧的 TX 功率完全独立于其它从单元；从单元的请求只能影响相对于同一从单元的主单元 TX 功率。

表3.19 用于功率控制的PDU

M/O	协议数据单元	内容
O	LMP_incr_power_req	保留（1 个字节）
O	LMP_decr_power_req	保留（1 个字节）
O	LMP_max_power	-
O	LMP_min_power	-

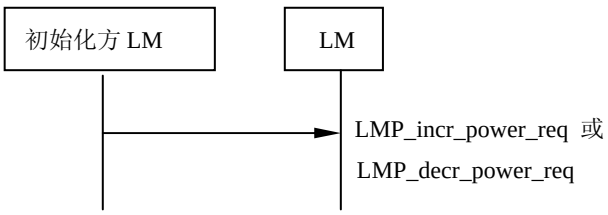


图3.45 一台设备请求改变其它设备的 TX 功率

如果LMP_incr_power_req的接收者已经使用最大功率进行发送，则返回LMP_max_power。如果设备已进行至少一次的功率降低请求，那它只能再进行一次功率增大请求。同样，如果 LMP_decr_power_req的接收者已经使用最小功率进行发送，则返回LMP_min_power，如果设备已请求至少一次的功率增加，那它只能再请求一次功率降低。

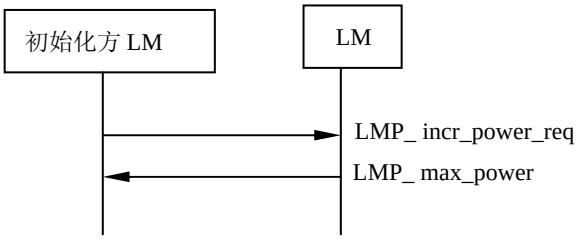


图3.46 不能增强TX功率

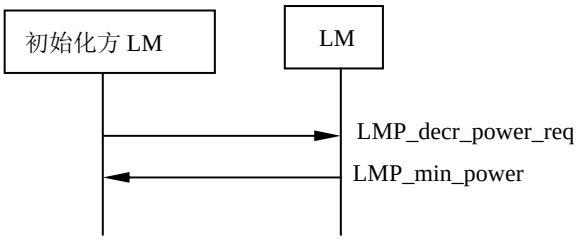


图3.47 不能降低TX功率

LMP_incr/decr_power_req中的一个字节保留作为将来用途。例如，它有可能用于作为约定RSSI与实际测试到的RSSI之间匹配的差值。LMP_incr/decr_power_req的接受者就可以利用该值来马上将功率调节为正确值，而不是每收到一次请求才改变一个等级。在没定义以前，参数值在所有的LMP版本中都必须为0x00。

3.19 DM和DH之间基于质量的信道变化

一台设备通常可以设置为使用DM数据分组，或DH数据分组，或根据信道质量自动调整使用的数据分组类型。但是，所有设备都能够传送DM和DH数据分组。DM与DH的区别在于DM数据分组通过2/3 FEC前向纠错码保护有效载荷，而 DH中的有效载荷不受任何FEC前向纠错码的保护。如果一设备需要自动调节使用DM或DH数据分组类型，它就要向其它设备发送LMP_auto_rate。基于LC质量测试，设备可以通过数据分组类型的变化确定是否将增加吞吐量。如果要增加，就向其它设备发送LMP_preferred_rate。其中，使用到的PDU如下：

M/O	协议数据单元	内容
O	LMP_auto_rate	-
O	LMP_preferred_rate	数据误码率

表3.20 用于质量驱动的数据误码率变化的PDU

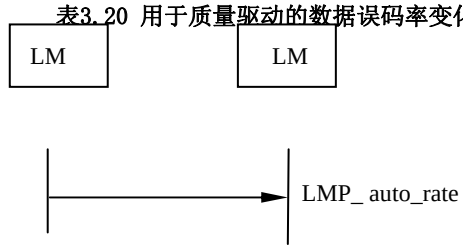


图3.48 左手单元设置为自动改变使用DM或DH

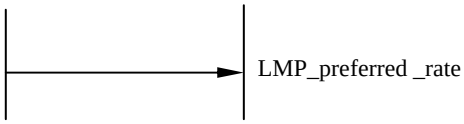


图3.49右手设备命令左手设备改变数据误码率

3.20 (QoS)服务质量

链路管理提供支持服务质量的能力。从主单元到特定从单元的连续传输之间的最大间隔时间称为轮询间歇时间。轮询间歇用于支持带宽分配和延迟控制。除了发生呼叫冲突、呼叫扫描冲突、查询冲突和查询扫描冲突的情况以外，应保证轮询间歇时间。

另外，主从单元应就广播数据分组(NBC)的重复次数进行协商。

表3.21 用于QoS的PDU

M/O	协议数据单元	内容
M	LMP_qualityPof_service	Polling interval N_{Bc}
M	LMP_quality_of_service_req	Poll interval N_{Bc}

3.20.1 主单元服务质量通知从单元

在这种情况下，主单元将新的轮询间歇时间和N_{BC}通知从单元。从单元不得拒绝该通知。

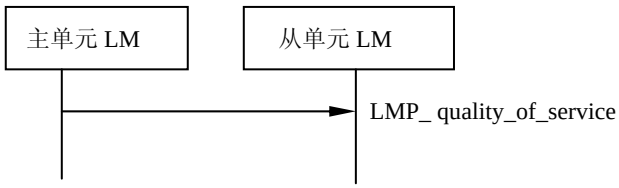


图3.50 主单元将新的服务质量通知从单元

3.20.2 设备请求新的服务质量

在这种情况下，主单元或从单元将请求一个新的轮询间歇时间和N_{BC}。N_{BC}参数只有在从主单元发往从单元时才有意义。对于从从单元发来得LMP_quality_of_service_req 协议数据单元，主机将忽略该参数。请求可以被接受或拒绝，这样，主从单元可以就所需服务质量进行动态协商。

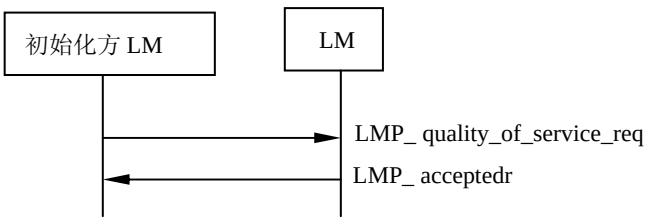


图3.51 设备接受新的服务质量

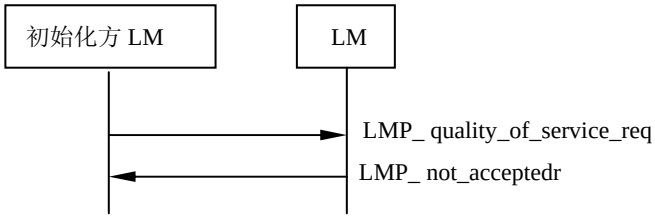


图3.52 设备拒绝新的服务质量

3.21 SCO 链路

当在两蓝牙设备之间建立起连接时，该连接由 ACL 链路组成。然后，就可以建立一条或多条SCO 链路。SCO 链路保留由SCO间歇时间(SCO interval)、T sco分开所得到的时隙。SCO链路保留的第一个时隙由 Tsco、SCO 延迟、D sco定义。此后，SCO 时隙将按照SCO间歇时间周期性发送。为了避免SCO链路初始化过程中时钟带来的隐含问题，应在从主单元发出的消息中分组含一个标志。该标志表示第一个 SCO 时隙是如何计算出来的。注意：只有该域的第0位和第1位有效。SCO链路通过 SCO 句柄相互区别。不能使用SCO零句柄。

表3.22 用于管理 SCO 链路的PDU

M/O	协议数据单元	内容
O	LMP_SCO_link_req	SCO 句柄 计时控制标志 Dsco Tsco SCO数据分组 无线模式
O	LMP_remove_SCO_link_req	SCO 句柄 原因

3.21.1 主单元初始化SCO链路

建立SCO链路时，主单元发送带参数的请求，这些参数就用于SCO链路的计时方式、数据分组类型和编码方式进行说明。对于蓝牙支持的每一个SCO数据分组，在无线接口方面，蓝牙支持三种不同的声音编码格式：μ-law log PCM, A-law log PCM and CVSD。

用于SCO链路的时隙由主单元控制的三个参数决定。这三个参数是Tsco、Dsco 和表示第一个SCO时隙计算方式的标志。发出第一个时隙以后，将按照Tsco周期性发送SCO 时键片。

如果从单元不接受SCO链路，而是愿意考虑接受另一SCO参数集，那么

它就可以在LMP_not_accepted 出错原因域里标识它不能接受哪些参数。而主单元就有可能发送一个经过含有已修改参数的新请求。

该消息中的SCO句柄必须区别于已存在的 SCO链路。

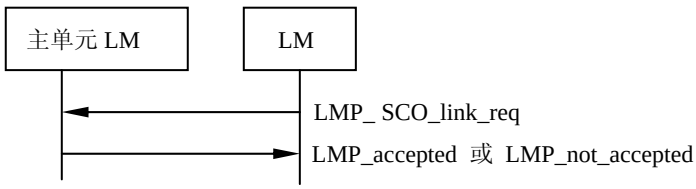


图3.53 主机请求 SCO 链路

3.21.2 从单元初始化SCO链路

从单元也可以进行SCO链路建立初始化。从单元可以发送LMP_SCO_link_req，但其中计时控制标志、Dsco都应置为无效，而SCO句柄值应为零。如果主机不能建立SCO链路，就通过发送LMP_not_accepted 作出应答。否则它将返回LMP_SCO_link_req。该消息分组含指定的SCO 句柄、Dsco 和计时控制标志。而且，主机应尽量采用从单元请求中的其它相同参数；如果主单元不能满足该请求，也可以使用其它参数值。而从单元则必须使用 LMP_accepted 或 LMP_not_accepted 进行响应。

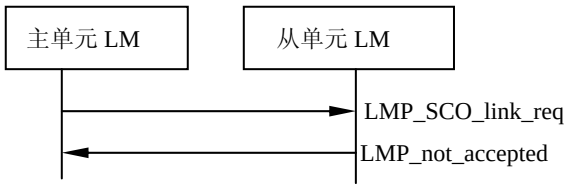


图3.54 主单元拒绝从单元的建立SCO链路的请求

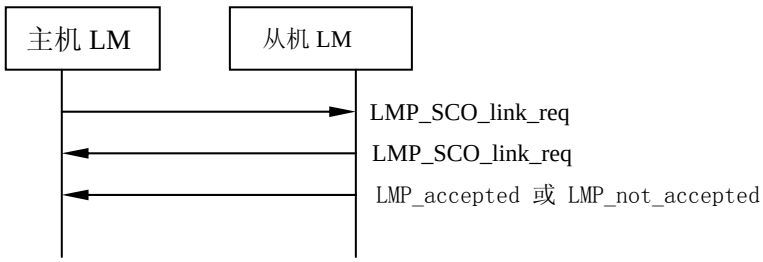


图3.55 主单元接受从单元使用SCO链路的请求

3.21.3 主单元请求改变SCO参数

主单元发送LMP_SCO_link_req。其中，SCO 句柄是主单元希望改变参数的 SCO链路的句柄。如果从单元接受了新参数，它就用 LMP_accepted 应答，并且SCO链路的参数将变为新参数。如果从单元不接受新参数，它就用 LMP_not_accepted 应答，而 SCO 链路保持不变。当从单元以 LMP_not_accepted应答时，它将在出错原因参数里镖表示不会接受哪些参数。然后，主单元能用修改后的参数再次改变 SCO 链路。

3.21.4 从单元请求改变SCO参数

从单元发送LMP_SCO_link_req。其中，SCO 句柄是从单元希望改变参数的SCO链路的句柄。该消息中的计时控制标志和Dsco参数都应置为无效。如果主单元不接受新参数，就发送 LMP_not_accepted应答，而SCO 连接则保持不变。如果主单元接受新参数，就发送 LMP_SCO_link_req应答，且必须使用与从单元请求中相同的参数。如果从单元不接受新参数，则在收到主单元应答消息时发送LMP_not_accepted应答。而SCO链路保持不变。如果从单元接受新参数，就发送LMP_accepted应答，SCO链路改变为新参数。

3.21.5 撤销SCO连接

主从单元可以通过发送特定请求撤销SCO链路，该请求分组含需要撤销的 SCO 链路句柄，以及撤销SCO链路的原因。接收方必须以LMP_accepted 应答。

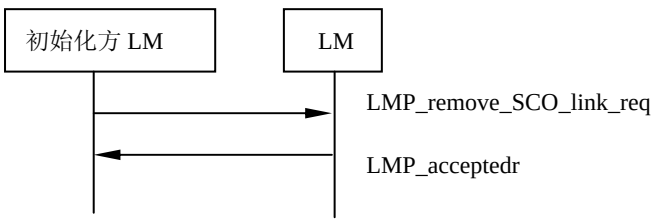


图3.56 撤销SCO链路

3.22 多时隙分组控制

从单元使用的时隙数量可在返回分组中进行限制。主单元允许从单元通过发送提供最大时隙参数的LMP_max_slots协议数据单元，使用最大数量的时隙。而从单元则可以通过发送含有最大时隙参数的LMP_max_slot_req协议数据单元，使用最大数量的时隙。其默认值是1 slot。也就是说，如果没有利用时隙数量信息通知从单元，从单元就只能使

用1-slot分组。用来控制多时隙分组的PDU有两类:

表3.23 用于控制多时隙分组的PDU

M/O	协议数据单元	内容
M	LMP_max_slot	最大时隙数量
M	LMP_max_slot_req	最大时隙数量

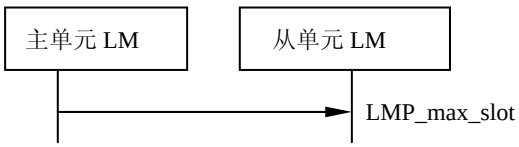


图3.57 主单元允许从单元使用时隙的最大数量

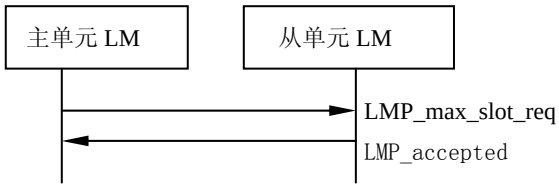


图3.58 主机接受从单元请求使用最大数量的时隙

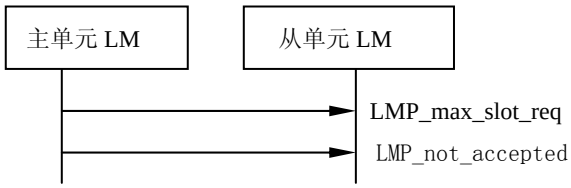


图3.59 主单元拒绝从单元请求使用最大数量的时隙

3.23 呼叫方案

除了强制呼叫方案外，蓝牙还设置了可选呼叫。LMP提供了一种协商呼叫方案的方法。该方法用于下次有匹克网单元被呼叫时。

表3.24 请求呼叫方案的PDU

M/O	协议数据单元	内容
O	LMP_page_mode_req	呼叫方案 呼叫方案设置
O	LMP_page-scan_mode_req	呼叫方案 呼叫方案设置

3.23.1 呼叫模式

当设备A呼叫设备B时，由设备A启动该过程，并就呼叫方案进行协商。由设备A提出一个分组含参数的呼叫方案，而设备B也可接受或拒绝它。如拒绝则表示原设置保持不变。可以拒绝切换回强制方案的请求。

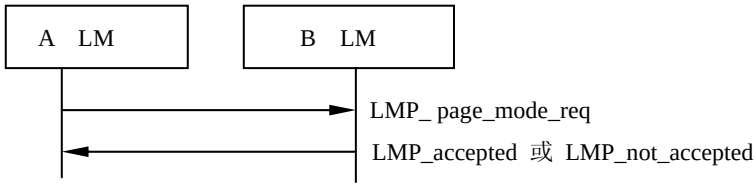


图3.60 呼叫模式协商

3.23.2 呼叫扫描模式

当设备B呼叫设备A时，由设备A启动该过程，并就呼叫方案进行协商。设备A提出一个分组含参数的呼叫方案，而设备B也可接受或拒绝它。如拒绝则表示原设置保持不变，必须接受切换回强制方案的请求。

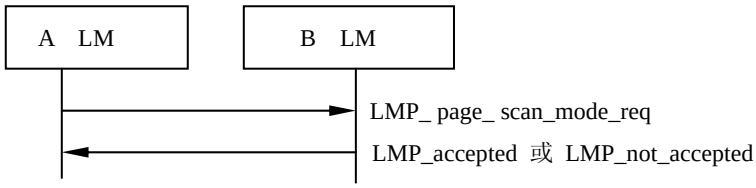


图3.61 呼叫扫描模式协商

3.24 链路监控

每一蓝牙链路都具有一个用于链路监控的计时器。该计时器用于检测因设备移出范围而引起的链路丢失、设备关机、或者其它通信失败的情况。本方案在基带规范中说明。LMP过程用于设置监控超时。

表3.25 用于设置监控最大持续时间的PDU

M/O	协议数据单元	内容
M	LMP_supervision_timeout	监控超时

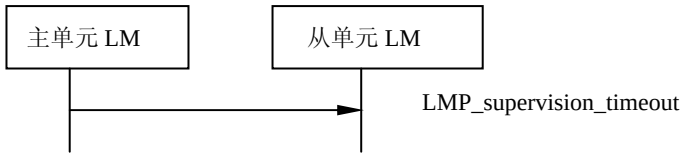


图3.62 设置链路监控最大持续时间

4. 建立连接

呼叫过程执行以后，主单元必须通过发送POLL或NULL分组轮询从单元，然后执行LMP过程，该过程不需要介于LM和被叫方主机之间的接口。

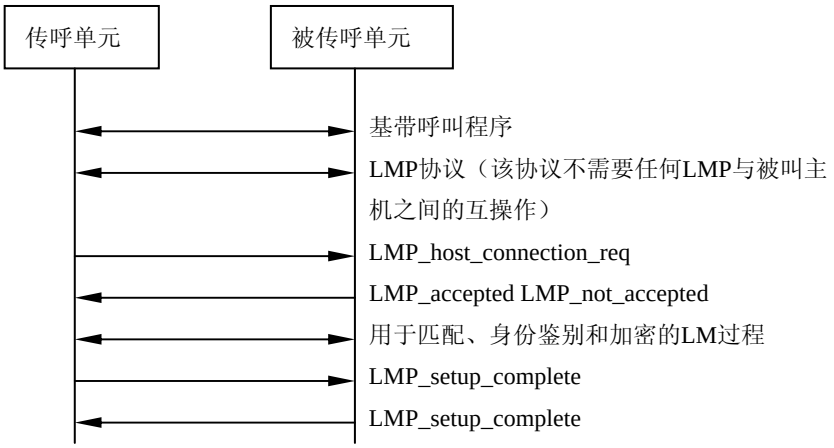


图3.63 连接建立

如果要创建LM以上层次的连接,主叫设备应发送LMP_Host_Connection_req。一旦呼入方收到这一消息，同时也将通知主机呼入连接的建立。远程设备可以通过发送 LMP_accepted 或 LMP_not_accepted 来接受或拒绝连接请求。

如果设备不需要进一步的连接建立过程,应发送LMP_Setup_complete。而且，设备仍然必须对其它设备的请求作出应答。当其它设备准备建立连接时，应发送 LMP_setup_complete。然后在与LMP不同的逻辑信道上发送第一个分组。

表3.26 用于建立连接的PDU

M/O	协议数据单元	内容
M	LMP_host_connection_req	-
M	LMP_setup_complete	-

1. 协议数据单元总结

表3.27 不同LMP协议数据单元编码

LMP PDU	长度（字节）	操作码	分组类型	传输方向	内 容	在有效载荷中的位置
LMP_accepted	2	3	DM1/DV	m↔s	操作码	2

LMP_au-rand	17	11	DM1	m↔s	随机数	2-17
LMP_auto_rate	1	35	DM1/DV	m↔s	-	
LMP_clkoffset_req	1	5	DM1/DV	m→s	-	
LMP_clkoffset_res	3	6	DM1/DV	m←s	时钟偏移	2-3
LMP_comb_key	17	9	DM1	m↔s	随机数	2-17
LMP_decr_power_req	2	32	DM1/DV	m↔s	保留	2
LMP_detach	2	7	DM1/DV	m↔s	原因	2
LMP_encryption_key_size_req	2	16	DM1/DV	m↔s	键长度	2
LMP_encryption_mode_req	2	15	DM1/DV	m↔s	加密模式	2
LMP_features_req	9	39	DM1/DV	m↔s	特性	2-9
LMP_features_res	9	40	DM1/DV	m↔s	特性	2-9
LMP_host_connection_req	1	51	DM1/DV	m↔s	-	
LMP_hold	3	20	DM1/DV	m↔s	挂起时间	2-3
LMP_hold_req	3	21	DM1/DV	m↔s	挂起时间	2-3
LMP_incr_power_req	2	31	DM1/DV	m↔s	保留	2
LMP_in_rand	17	8	DM1	m↔s	随机数	2-17
LMP_max_power	1	33	DM1/DV	m↔s	-	
LMP_max_slot	2	45	DM1/DV	m→s	最大时隙数量	2
LMP_max_slot-req	2	46	DM1/DV	m←s	最大时隙数量	2
LMP_min_power	1	34	DM1/DV	m↔s	-	
					计时控制标志 D_B T_B N_B	2 3-4 5-6 7 8

LMP_modify_beacon	11或13	28	DM1	m→s	Δ_B D_{access} T_{access} $N_{acc-slots}$ N_{poll} M_{access} 访问方案	9 10 11 12 13:0-3 13:4-7
LMP_name_req	2	1	DM1/DV	m↔s	名字偏移	2
LMP_name_res	17	2	DM1	m↔s	名字偏移 名字长度 名字分段	2 3 4-17
LMP_not-accepted	3	4	DM1/DV	m↔s	操作码 原因	2 3
LMP_page_mode_req	3	53	DM1/DV	m↔s	呼叫方案 呼叫方案 设置	2 3
LMP_page_scan_mode_req	3	54	DM1/DV	m↔s	呼叫方案 呼叫方案 设置	2 3
LMP_park	17	26	DM1	m→s	计时控制 标志 D_B T_B N_B Δ_B PM_ADDR AR_ADDR N_{Bsleep} D_{Bsleep} D_{access} T_{access} N_{acc_slots} N_{poll} M_{access} 访问方案	2 3-4 5-6 7 8 9 10 11 12 13 14 15 16 17:0-3 17:4-7
LMP_park_req	1	25	DM1/DV	m↔s	-	
LMP_preferred_rate	2	36	DM1/DV	m↔s	误码率	2
LMP_quality_of_service	4	41	DM1/DV	m→	轮询间隔 N_{BC}	2-3 4
LMP_quality_of_service_req	4	42	DM1/DV	m↔s	轮询间隔 N_{BC}	2-3 4

LMP_remove_SCO_link_req	3	44	DM1/DV	m↔s	SCO句柄 原因	2 3
LMP_SCO_link_req	7	43	DM1/DV	m↔s	SCO句柄 计时控制标志 Dsco Tsco SCO 分组 无线模式	2 3 4 5 6 7
LMP_set_broadcast_scan_window	4或6	27	DM1	m→s	计时控制标志 D_B 广播扫描窗口	2 3-4 5-6
LMP_setup_complete	1	49	DM1	m↔s		
LMP_slot_offset	9	52	DM1/DV	m↔s	时隙 BD_ADDR	2-3 4-9
LMP_sniff	10	22	DM1	m→s	计时控制标志 D_{sniff} T_{sniff} 呼吸尝试 呼吸超时	2 3-4 5-6 7-8 9-10
LMP_sniff_req	10	23	DM1	m↔s	计时控制标志 D_{sniff} T_{sniff} 呼吸尝试 呼吸超时	2 3-4 5-6 7-8 9-10
LMP_sres	5	12	DM1/DV	m↔s	认证应答	2-5
LMP_strat_encryption_req	17	17	DM1	m→	随机数	2-17
LMP_stop_encryption_req	1	18	DM1/DV	m→s	-	
LMP_supervision_timeout	3	55	DM1/DV	m↔s	监控超时	2-3
LMP_switch_req	1	19	DM1/DV	m↔s	-	
LMP_temp_rand	17	13	DM1	m→s	随机数	2-17
LMP_temp_key	17	14	DM1	m→s	键	2-17

LMP_timing_accuracy_req	1	47	DM1/DV	m↔s	-	
LMP_timing_accuracy_res	3	48	DM1/DV	m↔s	Drift Jitter	2 3
LMP__unit_key	17	10	DM1	m↔s	键	2-17
LMP_unpark_BD_ADDR_req	变量	29	DM1	m→s	计时控制标志 D_B AM_ADDR 1st unpark AM_ADDR 2nd unpark BD_ADDR 1st unpark BD_ADDR 2nd unpark	2 3-4 5:0-3 5:4-7 6-11 12-17
LMP_unpark_PM_ADDR_req	变量	30	DM1	m→s	计时控制标志 D_B AM_ADDR 1st unpark AM_ADDR 2nd unpark PM_ADDR 1st unpark PM_ADDR 2nd unpark	2 3-4 5:0-3 5:4-7 6 7
LMP_unsniff_req	1	24	DM1/DV	m↔s	-	
LMP_use_semi_Permanent_key	1	50	DM1/DV	m→s	-	
LMP_version_req	6	37	DM1/DV	m↔s	VersNr Compld SubVersNr	2 3-4 5-6
LMP_version_res	6	38	DM1/DV	m↔s	VersNr Compld SubVersNr	2 3-4 5-6

注 ①：对于 LMP_set_broadcast_scan_window, LMP_modify_beacon, LMP_unpark_BD_ADDR_req 和 LMP_unpark_PM_ADDR_req，参数D_B是可选项。该数据只在计时控制标志（bit 0）为0时给出。如果不分组含该参数，则所有D_B后的参数的有

效载荷中的位置减2。

②:对于LMP_unpark_BD_ADDR,第二台已解除休眠的从单元的 AM_ADDR 和 BD_ADDR 是可选的。如果只有一个从单元解除休眠，则AM_ADDR 2nd unpark应为零，而BD_ADDR 2nd unpark则被省略。

③：对于LMP_unpark_PM_ADDR，第二至第七台已解除休眠从单元的AM_ADDR和PM_ADDR都为可选项。如果第N个从单元被解除休眠，则应给出第二项至第N个休眠从单元域。如果N为奇数，则第（N+1）个被解除休眠的 AM_ADDR 必须是 0。如果 N 为偶数，消息长度 = x + 3N/2；如果 N 为奇数，消息长度 = x + 3(N+1)/2 –1。其中，x = 2 或 4。X的取值取决于PDU中是否分组含D_B参数(参见注1)。

5.1 参数说明

表3.28 LMP协议数据单元参数

名字	长度（字节）	类型	单位	细节
访问方案	1	u_int4		0：轮询技术 1-15:保留值
无线模式	1	u_int8		0： μ-law log 1：A-law log 2：CVSD 3-255：保留值
AM_ADDR	1	u_int4		
AR_ADDR	1	u_int8		
认证应答	4	多字节		
BD_ADDR	6	多字节		
广播扫描窗口	2	u_int16	Slots	
时钟偏移	2	u_int16	1.25ms	$(CLKN_{16-2}$ 从单元 – $CLKN_{16-2}$ 主单元)mod 2^{15} 不使用Msbit
Compld	2	u_int16		参见第1018页2.1节的BT指定数据
D_{access}	1	u_int8	Slots	
D_B	2	u_int16	Slots	
D_{Bsleep}	1	u_int8	Slots	
误码率	1	u_int8		0：中等 1：高 2-255:保留值
drift	1	u_int8	Ppm	
D_{sco}	1	u_int8	Slots	
D_{sniff}	2	u_int16	slots	
加密模式	1	u_int8		0：不加密 1：点到点加密 2：点到点加密和广播加密

				3-255:保留值
特性	8	多字节		参见第234页图5.3
挂起时间	2	u_int16	Slots	
jitter	1	u_int8	Ms	
键	16	多字节		
键长度	1	u_int8	字节	
M_{access}	1	u_int4	Slots	
最大时隙	1	u_int8	Slots	
$N_{acc-slots}$	1	u_int8	Slots	
名字分段	14	多字节		UTF-8 字符
名字长度	1	u_int8	字节	
名字偏移	1	u_int8	字节	
N_B	1	u_int8		
N_{BC}	1	u_int8		
N_{Bsleep}	1	u_int8	Slots	
N_{poll}	1	u_int8	Slots	
操作码	1	u_int8		
呼叫方案	1	u_int8		0:强制方案 1:可选方案 2-255:保留值
呼叫方案设置	1	u_int8		对于强制方案： 0：R0 1：R1 2：R2 3-255：保留值 对于可选方案： 0：保留值 1：R1 2：R2 3-255：保留值
PM_ADDR	1	u_int8		
轮询间隔	2	u_int16	Slots	
随机数	16	多字节		
原因	1	U_int8		参见第235页图5.4
SCO 句柄	1	U_int8		
SCO 分组	1	U_int8		0：HV1 1：HV2 2：HV3 3-255：保留值
时隙	2	U_int16	μs	
呼吸尝试	2	U_int16	Slots	
呼吸超时	2	u_int16	slots	
SubVersNr	2	u_int16		由各厂商定义
监控超时	2	u_int16	slots	

T_{access}	1	u_int8	Slots	
T_{B}	2	u_int16	Slots	
定时控制标志	1	u_int8		bit0 = 0:无定时变化 bit0 = 1:定时变化 bit1 = 0:使用初始化 1 bit1 = 1:使用初始化 2 bit2 = 0:访问窗口 bit2 = 1:无访问窗口 bit3-7:保留值
T_{sco}	1	u_int8	Slots	
T_{sniff}	2	u_int16	Slots	
VersNr	1	u_int8		0：蓝牙LMP 1.0 1-255:保留值
Δ_{B}	1	u_int8	时隙	

5.1.1 编码特性

本参数实际就是有关设备支持的蓝牙无线电、基带和LMP特性信息表。如果支持某一特性，则该位为 1。未在表格 5.3中定义的特性参数位为 0。

表3.29 参数特性编码

字节	位	支持特性
	0	3-slot分组
	1	5-slot分组
	2	加密
	3	时隙偏移
0	4	定时精度
	5	切换
	6	挂起模式
	7	呼吸模式
	0	休眠
	1	RSSI
	2	信道质量驱动的传输误码率
	3	SCO链路
1	4	HV2 分组
	5	HV3 分组
	6	μ-law log
	7	A-law log
	0	CVSD
2	1	呼叫方案
	2	功率控制

i. 出错原因列表

下面的表格是用于 LMP 的出错原因码。

表 3.30 错误原因列表

原因	说明
0x05	身份认证失败
0x06	字丢失
0x0A	与设备 A 的最大 SCO 连接数（已达到与特定设备的最大 SCO 连接数。可以使用所有与该设备关联的连接句柄。）
0x0D	因资源有限而导致主机拒绝（由于远程主机没有额外资源接受连接,而导致远程主机拒绝连接。）
0x0E	由于安全原因导致主机拒绝（由于远程主机认为本地主机未满足其安全标准,主机拒绝连接。）
0x0F	由于本地设备只是个人设备导致主机拒绝（由于远程主机是个人设备， 以及只接受来自特定远程主机的连接，而导致主机拒绝。）
0x10	主机超时(在连接接受超时时使用该主机超时，在连接接受计时器失效前,主机拒绝应答呼入连接尝试,。）
0x13	另一端已终止连接，即用户已终止连接
0x14	另一端已终止连接：低资源
0x15	另一端已终止连接：准备关闭电源
0x16	本地主机终止连接
0x17	重复尝试（原身份认证或匹配失败后，马上进行身份认证或匹配尝试。）
0x18	不允许匹配
0x19	未知的 LMP PDU
0x1A	不支持的 LMP 特性
0x1B	拒绝 SCO 时隙
0x1C	拒绝 SCO 间歇
0x1D	拒绝 SCO 无线模式
0x1E	非法 LMP 参数
0x1F	未说明的错误
0x20	不支持的参数值
0x21	不允许切换
0x23	LMP 出错处理冲突
0x24	不允许的协议数据单元

5.2 缺省值

蓝牙设备在对其它值进行协商以前必须使用这些值。

表 3.31 默认值

参数	值
Drift	250
Jitter	10
最大时时隙数	1
轮询间隔	40

6 。测试模式

LMP具有支持不同蓝牙测试模式的PDU。测试模式用于认证和兼容蓝牙无线电和基带测试。

6.1 激活和解除测试模式

可以通过向中试设备（DUT）发送 LMP_test_activate 激活测试模式。DUT通常作为从单元。链路管理器必须能够在任何时候接收该消息。如果能在本地进入DUT测试模式，DUT则采用 LMP_accepted 应答，并进入测试模式。否则，DUT采用LMP_not_accepted 应答，并且 DUT保持正常操作状态。LMP_not_accepted 的原因码应为PDU not allowed。

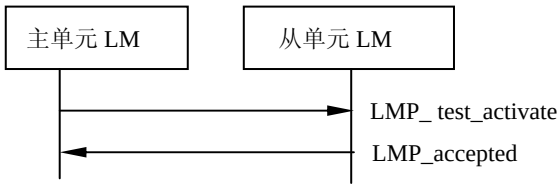


图3.64 成功激活测试模式

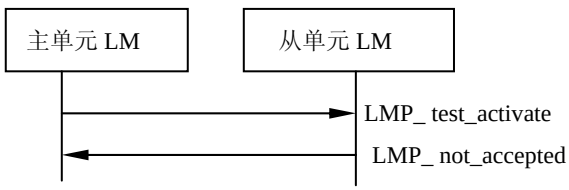
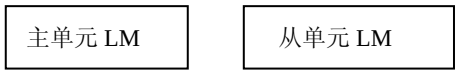


图3.65 测试模式激活失败

测试模式能用两种方法撤销。一种方法是:通过发送测试场景置为”退出测试模式”的LMP_test_control退出测试模式，从单元返回与主单元保持连接的正常工作状态。另一种方法是:通过LMP_detach 发送到 DUT，从而同时终止测试模式和连接。

6.2 测试模式的控制

当 DUT 进入测试模式时，可以向DUT发送协议数据单元LMP_test_control从而启动指定测试。该协议数据单元通过LMP_accepted确认。如果一个没有处于测试模式的设备收到 LMP_test_control，它就用LMP_not_accepted 应答，应答消息的原因码为PDU not allowed。



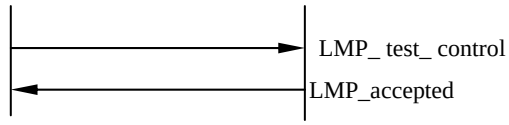


图3.66 测试模式控制成功

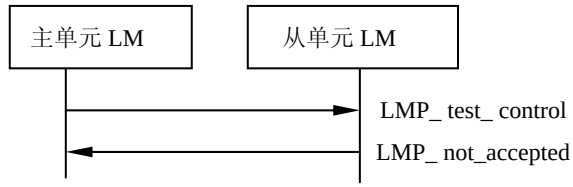


图3.67 由于从单元没有处于测试模式而导致测试模式控制被拒绝

6.3 测试模式PDU

下面的表格是全部的测试模式PDU类型。

表3.32 测试模式PDU

M/O	LMP PDU	长度	操作码	分组类型	方向	内容	在有效载荷中的位置
M	LMP_test_activate	1	56	DM1/DV	m→s	-	
M	LMP_test_control	10	57	DM1	m→s	测试场景 跳频模式 TX 信道 RX 信道 功率控制模式 轮询周期 分组类型 测试数据的长度	2 3 4 5 6 7 8 9-10

7. 出错处理

如果链路管理器收到含有不能识别操作码的PDU，就用LMP_Not_accepted 应答，并且 LMP_not_accepted 中含有原因码unknown LMP PDU。返回的操作码参数同样也是不能识别的操作码。

如果链路管理器收到含有非法参数的PDU，就用 LMP_not_accepted 应答，LMP_not_accepted含有原因码invalid LMP parameters（非法LMP参数）。

如果发现超过了最大响应时间或检测到链路丢失，等待应答的一方就可以认为该过程已终止。

信道出错或发送方系统出错都会引起发送错误的消息。为了检测通信

的最近状况，LM应监监测错误消息数量，一旦超过阀值就将其断开。该阀值根据实际应用情况而不同。

在链路双方的LM初始化同一过程且都没有成功情况下，由于没有实时解析LMP PDU，就会发生冲突。这时，主单元将通过发送含有原因码“LMP Error Transaction Collision”（LMP出错处理冲突）的LMP_not_accepted消息，拒绝由从单元进行初始化的过程。然后，才终止由主单元初始化的过程。

第4章 逻辑链路控制和适配协议规范

本文件主要对逻辑链路控制和适配协议协议（L2CAP）做出描述。该协议支持高层协议多路复用、数据分段和重组,并且支持传送服务质量信息。本文件主要针对协议状态自动机、分组格式及构成，以及用于蓝牙测试和认证的测试接口做出详细阐述。

7.17 启用无连接通信

附录: 配置MSCs及实现准则

1．总论

本部分定义逻辑连接控制和适配协议,缩写为 L2CAP。L2CAP基于基带协议，位于数据链路层中，参见图1.1。L2CAP通过协议多路复用、分段重组操作和组概念,向高层提供面向连接的和无连接的数据服务。L2CAP 允许高层协议和应用传输和接收长达64 Kb的L2CAP数据分组。

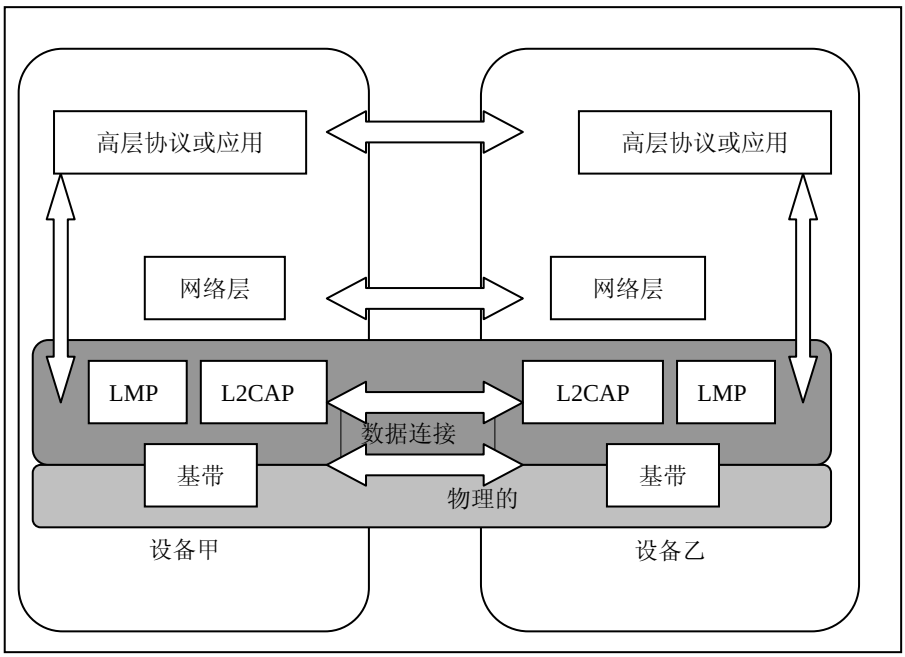


图4.1 协议层内的L2CAP

基带规范定义了两种链路类型:同步面向连接链路(SCO)和异步无连接链路(ACL)。SCO 链路采用保留带宽支持实时语音通信。ACL链路支持最佳通信。L2CAP规范仅定义ACL链路而不支持 SCO链路。在ACL 链路上禁止使用 AUX1 分组。该类型分组不支持数据完整性校验(无 CRC)。因为 L2CAP在基带上依靠完整检查来保护传输的信息，而AUX1分组却不能传输 L2CAP分组。

下面是ACL有效载荷的格式。下两图表示单时隙分组头和多时隙分组头。它们的唯一差别是长度段的大小。分组类型则(基带分组头中的一个域)用于区分单时隙包与多时隙包区。

图4.2 用于单时隙分组的 ACL有效载荷头

图4.3

下表定义的 2 位逻辑信道(L_CH)域用于区分L2CAP分组与链路管理器协议分组。其余编码则保留以备将来使用。

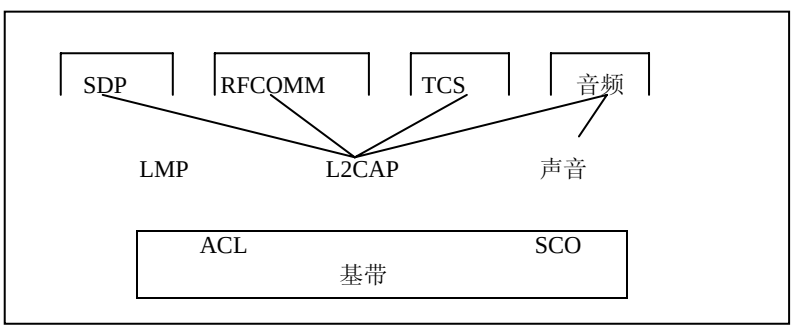
表4.1 逻辑信道 L_CH 域的内容

L_CH 信道	逻辑信道	信息
00	RESERVED	保留
01	L2CAP	L2CAP包的延续
10	L2CAP	L2CAP分组起始位
11	LMP	链路管理协议

链路控制器(LC)作为一个基带执行实体，实施对ACL 报文头的FLOW位的管理。当不再在ACL链路上进行L2CAP通信时，该位通常设置为0(停止发送)。而发送FLOW位设置为1的L2CAP分组则意味着重新开始接收L2CAP分组流。参见“基带规范”详细描述。

1.1 L2CAP功能要求

L2CAP的功能要求包括协议复用、分段与重组(SAR),以及组管理。下图说明 L2CAP如适配蓝牙协议协议栈。L2CAP处于基带协议上一层,并与蓝牙服务搜索协议(SDP)、RFCOMM和电话控制(TCS)等其它通信协议具有通信接口。基带 SCO 链路常用作语音和电话应用的语音信道。经过分组的语音数据,如IP电话, 通过使用L2CAP上层的通信协议进行发送的。



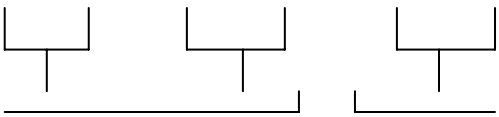


图4.4 蓝牙协议体系结构中的L2CAP

L2CAP的必要协议要求包括简单和低拥塞。L2CAP适用于具有计算资源有限的设备。由于蓝牙无线设备降低了功耗,L2CAP应该不会过分耗费耗电。协议实施的内存要求也应保持最小化。

协议复杂性应该适应由蓝牙支持的个人计算机、个人数字助理、数字蜂窝电话、无线耳机，游戏杆和其它无线设备。而且,协议应该能够达到相当高的带宽利用效率。

- **协议复用**

  L2CAP应支持协议复用，因为基带协议不支持任何‘类型’域，而这些类型域则用于标识要复用的更高层协议。L2CAP必须能够区分高层协议，例如，服务搜索协议，RFCOMM，和电话控制。

- **分段与重组**

  与其它有线物理介质相比，由基带协议定义的分组在大小上受到限制。输出与最大基带有效载荷(DH5分组中的341字节)关联的最大传输单位(MTU)限制了更高层协议带宽的有效使用，而高层协议要使用更大的分组。大 L2CAP分组必须在无线传输前分段成为多个小基带分组。同样,收到多个小基带分组后也可以重新组装成大的单一的 L2CAP 分组。在使用比基带分组更大的分组协议时,必须使用分段与重组(SAR)功能。

- **服务质量**

  L2CAP 连接建立过程，允许交换有关两蓝牙单元之间服务质量的信息。每个L2CAP设备必须监视由协议使用的资源并保证服务质量（QoS）的完整实现。

- **组**

  许多协议包括地址组的概念。基带协议支持匹克网的概念，匹克网为能够使用同一时钟进行同步工作的一组设备。L2CAP 组概念可以实现在匹克网上的有效协议映射。如果没有组概念，为有效管理组，高层协议就必须直接与基带协议和链路管理器打交道。

1.2 假设

协议基于下列假设为依据而设计：

- 使用链路管理器协议在两单元间建立ACL链路。基带提供数据分组的有序传输，但也可能有个别分组损坏或重复。任两台设备之间只会有一条ACL链路。
- 基带通常提供全双工信道。但这并不是说所有L2CAP 通信都是双向的。多点传送和单向通信(例如，视频)并不要求双工信道。
- 通过使用基带层提供的机制，L2CAP提供了一条可靠的信道。当收到请求和重发数据时，基带通常要执行数据完整性校验，直到数据成功确认或发生超时。由于可能会丢失确认报文，所以甚至在数据成功发送后也会发生超时。基带协议使用长度为1位的序列号,该序列号用于删除重复发送的分组。由于所有广播的L2CAP数据分组的首段都以同一序列位为起始位，如果需要提供可靠传输,就应禁止使用基带广播分组。

1.3 适用范围

以下特性不属L2CAP适用范围：

- L2CAP 不传输由 SCO链路所指定的音频数据。
- L2CAP 不能进行可靠信道传输或保证数据完整性,即：L2CAP不会重发或数据校验。
- L2CAP 不支持具有可靠性的广播信道。
- L2CAP 不支持一个全局组名的概念。

2 主要操作

逻辑链路控制和适配协议(L2CAP)是以信道概念为基础的。通过信道识别符引用每条 L2CAP 信道的端点。

2.1 信道标识符

信道标识符(CIDs)是表示逻辑信道本地端设备的名字。从 0x0001 到 0x003F 的标识符保留用于特定的 L2CAP 功能。空标识符(0x0000)则定义为一个非法标识符，并且不得用于目标端。可以根据实际应用目的和情况，以合适方式自由管理其余的CID。但在本地设备与多个远端设备存在多个并发L2CAP信道的情况下,同一CID不得重新用作本地L2CAP信道端。下表对CID命名空间的定义和划分进行的总结。

CID的指定与特定设备有关，一台设备可以独立于其他设备指定CID(如果它不使用在下表列出的保留CID的话)。这样,即使通过连接到一个本地设备的多个远程设备，将同一CID值指定给(远程)信道端，本地设备仍然能够将远端CID与每一不同的远程设备联系起来。

表4.2 CID定义

CID	说明
0x0000	无效标识
0x0001	正在发信号的信道
0x0002	无连接的接收信道
0x0003-0x003F	保留
0x0040-0xFFFF	动态分配

2.2 设备间操作

下图说明了CID在不同设备对等L2CAP实体间通信中的使用方式。面向连接的数据信道提供了两设备间的连接，而CID则用于标识信道的每一端。无连接信道限制数据向单一方向的流动。这些信道用于支持一个信道“组”，在该信道“组”里发送端CID用于表示一个或多个远程设备。因此保留了一些CID以备将来特殊用途使用。信号信道是一个保留信道的实例。该信道用于创建和建立面向连接的数据信道，并可对这些信道的特性变化进行协商。L2CAP实体必须支持信号信道。另一CID则保留用于呼入的无连接数据通信。在下面的例子中,CID用于标识由设备#3和设备#4组成的组。而来自ID信道的数据则被发往保留用于无连接数据通信的远程信道。

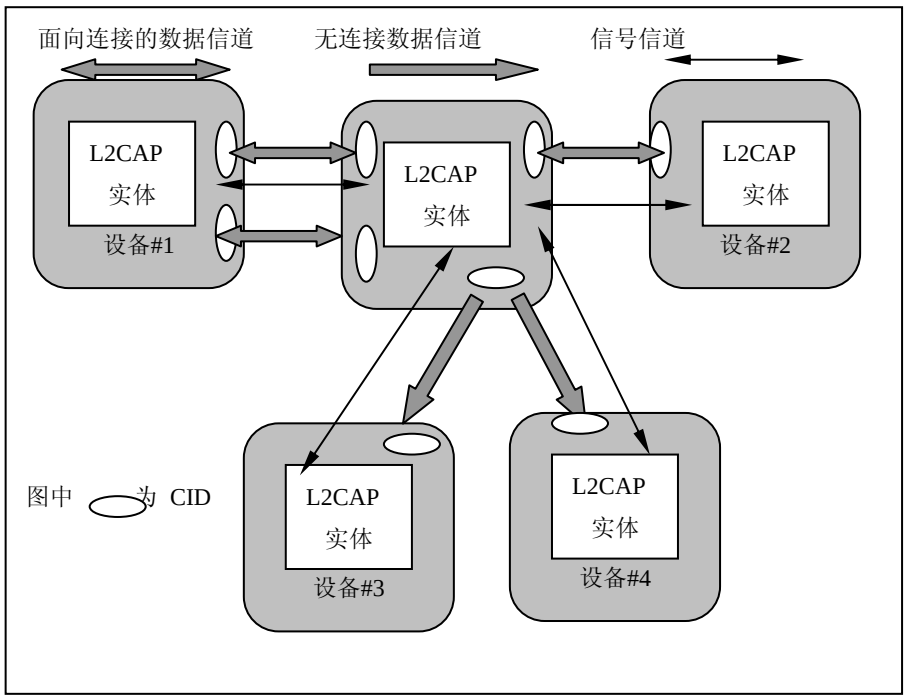


图4.5 设备间信道

下表描述了不同信道及其主端和目标端标识。可以创建一条范围为

0x0040 到 0Xffff的"已分配"信道代表本地信道端。

表4.3 信道标识类型

信道类型	当地的 CID	远程 CID
连接导向	动态分配	动态分配
无连接数据	动态分配	0x0002(固定值)
发信号	0x0001(固定值)	0x0001(固定值)

2.3 层间操作

L2CAP的实施应遵循下述总体体系结构，并可在高层协议和低层协议间传送数据。本文件列出了一些L2CAP应用必须实现的服务。每个应用都必须支持一组用于L2CAP 应用间通信的信号指令。L2CAP应用还应准备从低层接受某类型的事件，并可向高层生成事件。事件如何在层间传递则根据实际应用情况而定。

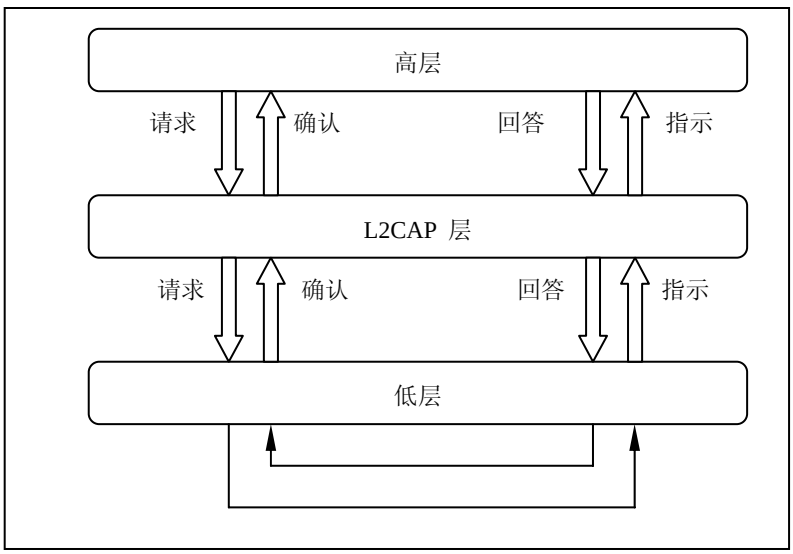


图4.6 L2CAP体系结构

2.4 分段和重组

分段和重组（SAR）操作用于通过支持最大传输单位（MTU）来提高传输效率。MTU的长度大于最大的基带数据包。这样，就可以通过在网络广播和传送高层协议分组降低拥塞。所有L2CAP 分组都可以在基带分组基础上进行分段。L2CAP协议并不执行任何分段和重组操作，但是其分组格式支

持调整到更小物理帧长度。L2CAP提出发送出的(即,远程主机所接收的)MTU并把上层分组分为可通过主控制器接口(HCI)传送到链路管理器的"数据块"。在接受端，L2CAP应用接收到来自HCI的"数据块"后，就可以利用通过HCI提供的来自分组头的信息，把这些"数据块"重组成 L2CAP分组。

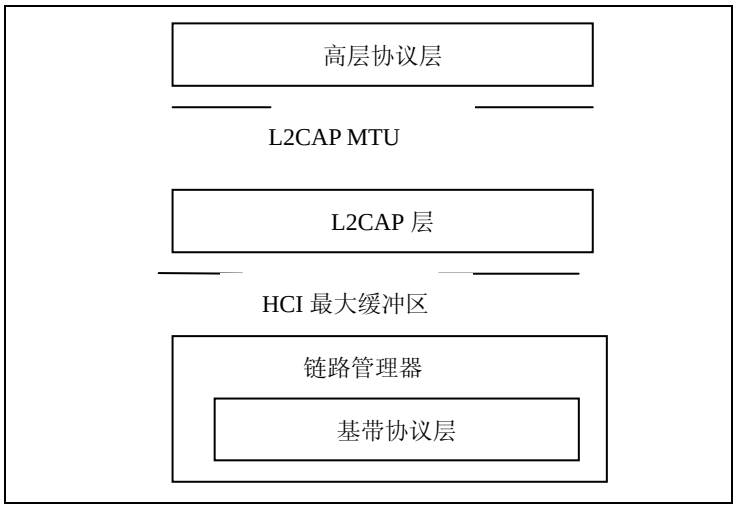


图4.7 L2CAP SAR变量

执行分组和重组只使用了很小的代价。位于基带分组有效载荷的第一个字节(也叫帧头)的两个 L_CH位用于表示 L2CAP分组的开始和附加部分。L_CH为'10'表示L2CAP分组的第一段，而为"01"则表示它的其余部分。下图即SAR的示例。

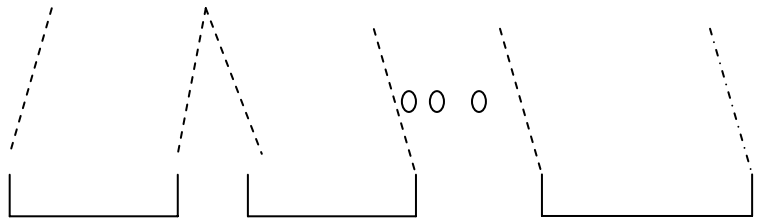


图4.8 L2CAP 分段

2.4.1 分段过程

通过使用专用服务接口可以输出L2CAP的最大传输单元(MTU)。高层协议负责在MTU限制限制内限制发往L2CAP层的分组大小。而L2CAP应用则将该分组分段成为协议数据单元(PDUs)，并送到下层。如果L2CAP直接位于基带的上一层，L2CAP就应把分组分段成为用于无线传输的基带数据包。典型情况下，L2CAP在主控制器接口上运行,就应把整块"数据块"发送到主控制器，再由主控制器将它们分段成为基带数据包。在目的地址为同一单元的其它L2CAP分组发送以前，所有与L2CAP分组相关联的L2CAP分组都必须先传送到基带。

2.4.2 重组过程

基带协议按顺序发送ACL分组，并利用16位 CRC 保证数据的完整性。基带也可以利用自动重复请求(ARQ)机制支持可靠连接。当基带控制器收到 ACL分组时，它可以在每个基带分组到达时通知L2CAP层，也可以在接收缓冲区溢满或定时器失效之前收集一定数量的分组，然后再通知L2CAP层。

L2CAP应用必须使用L2CAP分组头里的长度域，进行一致性校验,并丢弃与长度域不匹配的L2CAP分组。如果不考虑信道可靠性，将丢弃长度不合适的分组。如果考虑信道的可靠性，L2CAP必须通知上层信道已不可靠。通过具有无限刷新超时值定义可靠信道。

下图表示了如何使用分段和重组操作传送一个高层协议数据单元(PDU)。注意当存在高层PDU和 L2CAP分组之间的一对一映射时，分段和重组规则所用的段大小将取决于实际应用情况，并且在发端和收端之间也可以不同。

补图 2.5: 具有HCI的（注解1）单元的分段与重组服务

※ 注解1.为简洁起见，在创建基带包(Air_1 , Air_2 ,等等)以前，任何附加的 HCI 和 USB 特别信息段串都没在图中表示出来。

3 状态机

本节描述 L2CAP 的面向连接信道的状态机，定义了导致状态转换的状态和事件，以及用于响应事件的动作。该状态机仅与双向CID有关，它既不代表信号信道，也不代表单向信道。

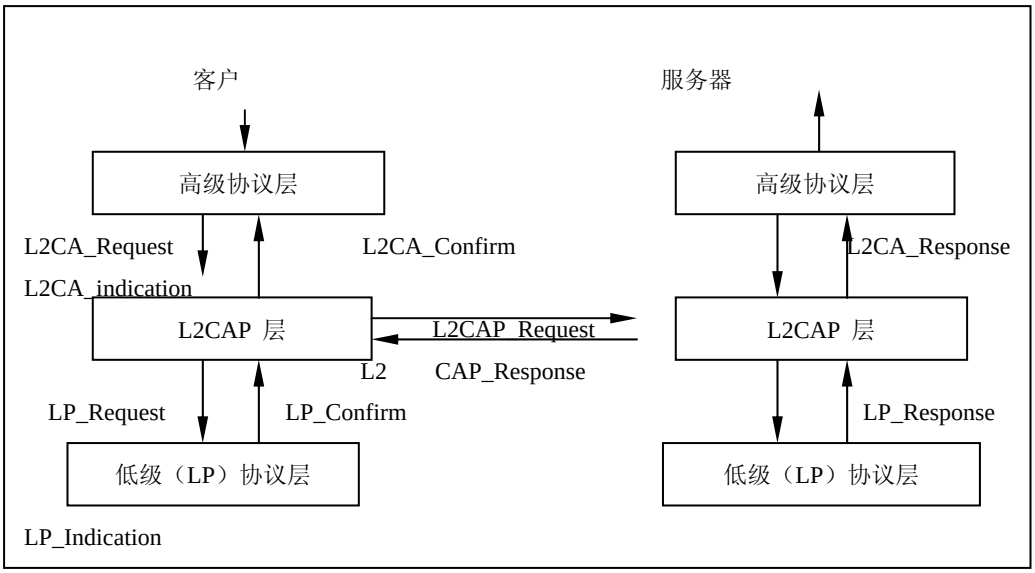


图4.9 L2CAP 层互操作

上图说明由L2CAP层应用所执行的事件和动作。客户和服务器分别代表请求的发起方和接收方。一个应用层次的客户可以发起,也可以接受请求。以下是命名规则。两层间的接口(纵向接口)使用向高层提供服务的低层前缀，如L2CA。两同层实体之间的接口(横向接口)则使用协议前缀(把P加到协议层标识上)，如L2CAP。来自高层的事件称作请求(Req)，而相应的答复则称为确认(Cfm)。来自低层的事件称为指示(Ind)，而相应的答复则称为应答(Rsp)。需要进一步处理的应答称为中间应答(Pnd)。用于确认和应答的概念表示肯定答复。否定答复则应标有‘Neg’后缀，例如L2CAP_ConnectCfmNeg。

一个来自高层的动作请求的结果通常是相应的确认,无论对该动作的确认成功与否。而来自低层的指示的结果却不总是相应的应答。如果指示知道本地的触发事件，则就会发生后一种情况，参见LP_QoSViolationInd和 L2CA_TimeOutInd的例子。

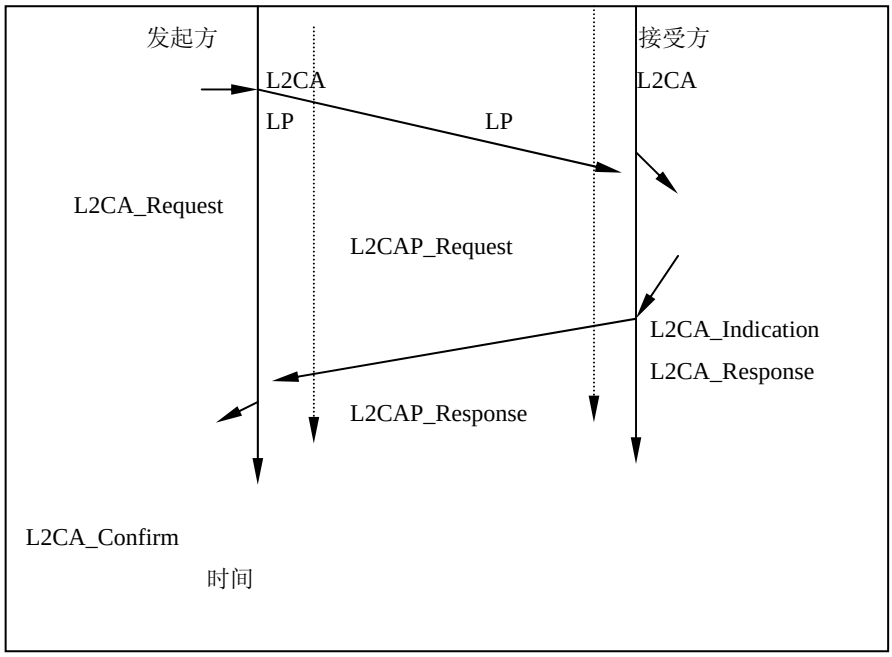


图4.10

该图使用报文序列图(MSC)来解释事件的正常序列。两条外部垂直直线表示发起方(发出请求的设备)和接受方(应答发起方请求的设备)之间的L2CA接口。L2CA接口的请求指令将导致发出协议定义请求。当协议向接受者传递请求时，远程L2CA实体将向上层协议发送指示。当接受方的上层协议应答时,应答将由协议打包并发回发起方。最后，再用确认报文把结果发回发起方的上层协议。

3.1 事件

事件是与最大延迟时间一起发送到L2CA层的呼入报文。事件划分为5类:来自低层的指示和确认、来自高层的要求和应答、来自对等层的数据、来自对等层的信号请求和应答，以及由定时器失效引起的事件。

3.1.1 低层协议(LP)到L2CAP的事件

- LP_ConnectCfm

确认建立低层(基带)连接的请求(参见LP_ConnectReq)。如果需要在建立物理链路时进行身份认证，就应包括对认证进行认证。

- LP_ConnectCfmNeg

确认建立低层(基带)连接失败的请求失败(参见LP_ConnectReq)。这可能是因为设备联系不上，或请求被拒绝，或对LMP身份认证的认证失败。

- LP_ConnectInd

表示低层协议已成功建立连接。对于基带，是一条ACL链路。可以利用一个 L2CAP 实体跟踪物理链路信息。

- LP_DisconnectInd
  表示低层协议(基带)已被LMP指令或一个超时事件关闭。
- LP_QoSCfm
  确认给定服务质量请求(参见LP_QoSReq)。
- LP_QoSCfmNeg
  确认给定服务质量请求失败(参见LP_QoSReq)。
- LP_QoSViolationInd
  表示低层协议已检测到违反LP_QoSReq规定的QoS协定的情况。

3.1.2 从L2CAP到L2CAP的信号事件

在交换对应L2CAP 信号PDU以后，由每个L2CAP 实体生成从L2CAP到L2CAP的信号事件。正如其它 L2CAP PDU一样,该事件通过低层指示事件从低层进行接收。为阐述简洁，我们不对该过程进行详细说明，而且我们假信号事件可以直接在 L2CAP对等实体之间进行交换。

- L2CAP_ConnectReq
  已收到一个连接请求报文。
- L2CAP_ConnectRsp
  已收到连接应答报文, 该报文指示连接已经建立。
- L2CAP_ConnectRspPnd
  已收到连接应答报文，该报文指示远端已收到该请求并正在进行处理。
- L2CAP_ConnectRspNeg
  已收到连接请求报文, 该报文指示不能建立连接。
- L2CAP_ConfigReq
  已收到配置请求报文，该报文指示远端希望参与有关信道参数的协商。
- L2CAP_ConfigRsp
  已收到配置应答报文，该报文指示远端同意所有正在协商的参数。
- L2CAP_ConfigRspNeg
  已收到配置应答报文，该报文表示远端不同意应答报文中的参数。
- L2CAP_DisconnectReq
  已收到断开请求报文，信道必须启动连接断开过程。 L2CAP信道连接断开过程结束后, L2CAP 实体应将本地CID放回到"未分配"CID池中。
- L2CAP_DisconnectRsp
  已收到连接断开应答报文。收到该信号以后,接收方L2CAP 实体可以将相应的本地CID返回到未分配的 CID 池中。由于该断开请求肯定成功，所以也就没有相应否定应答。

3.1.3 从L2CAP到L2CAP的数据事件

- L2CAP_Data

  数据分组已收到。

3.1.4 高层到L2CAP的事件

- L2CA_ConnectReq

  请求与创建到远程设备的信道,该请求来自L2CAP的上层。

- L2CA_ConnectRsp

  远程设备请求指示的应答,该应答来自协议高层(参见L2CA_ConnectInd)。

- L2CA_ConnectRspNeg

  远程设备连接请求的否定应答, 该应答来自协议高层(拒绝),(参见L2CA_ConnectInd)。

- L2CA_ConfigReq

  请求(重新)设置信道, 该请求来自协议上层。

- L2CA_ConfigRsp

  对(重新)设置请求的应答, 该应答来自协议高层。(参见L2CA_ConnectInd)。

- L2CA_ConfigRspNeg

  对(重新)设置请求的否定回答,该应答来自协议高层。(参见L2CA_ConnectInd)。

- L2CA_DisconnectReq

  请求信道立即断开, 该请求来自协议高层,。

- L2CA_DisconnectRsp

  用于响应连接断开请求的指示,该响应来自协议上层(参见L2CA_ConnectInd)。由于没有相应的否定应答,因此必须执行连接断开指示。

- L2CA_DataRead

  请求将收到的来自L2CAP 实体的数据转发到高层,该请求来自协议高层。

- L2CA_DataWrite

  请求在一开放信道上将来自协议高层的数据,转发到L2CAP 实体。该请求来自协议高层。

3.1.5 定时器事件

- RTX

当远端不对信令请求作出应答时,采用应答超时失效（The Response Timeout eXpired,RTX）定时器终止信道。当发送信令请求到远程设备时，定时器开始工作。当收到应答时，该定时器失效。如果初始化方定时器失效，将发送一则完全相同的请求报文，否则将断开由请求所标识的信道。如果已发出同样的请求报文，则应将RTX超时设置为一个新值,该值至少应为原值的两倍。

在断开信道前，应用负责确定在L2CAP层次上执行的最大请求转发数。该决定应该基于信号连接的冲洗超时。该决定应基于信令信道的刷新超时时间，超时时间越长，物理层次上执行转发的次数越多。如果要减少L2CAP层次上的转发次数，则应改进信道可靠性。例如,如果刷新超时无限大,那么在L2CAP层次上将不会执行转发操作了。

该定时器值因实际应用情况而异:最小值为1秒，而最大值为60秒。对于每一信令请求，包括每一回应请求都存在一个RTX 定时器。当收到应答，或物理链路丢失时，定时器在最后失效时消失。在定时器起始阶段和信道断开起始阶段(如果没有收到应答的话)之间的共用时间最大值为 60秒。

- ERTX

当怀疑远端正在执行对请求信令的附加处理的时候，扩展应答超时终止定时器（ERTX）用于替代应答超时终止定时器(RTX)。当远端应答说明请求为中间应答时,将启动该定时器。例如,当收到 L2CAP_ConnectRspPnd 事件时，定时器就会开始工作。当收到正式应答或物理链路丢失时，将停用该定时器。如果最初的定时器失效，将发送同一请求，或断开信道。如果发出同一请求，则ERTX定时器将消失，代之以一个新RTX 定时器。然后，整个定时过程将如前述RTX定时器那样重新启动。

ERTX定时器的值是根据实际应用情况而不同:最小值为60秒,而最大值为300秒。与 RTX 一样的是，对于每一收到中间应答的请求都必须至少有一个 ERTX 定时器，但对于每一请求则最多只能有一个RTX或ERTX。在该定时器起始阶段和信道断开起始阶段(如果应答没收到)之间的最长共用时间为 300 秒。

3.2 动作

动作分为五类:面向高层的确认和指示、面向低层的请求和应答、面向对等协议层的请求和应答、面向对等协议层的数据传输、定时器设置。

3.2.1 从低层到L2CAP的动作

- LP_ConnectReq

L2CAP请求低层协议创建连接。如果不存在到远程设备的物理链路，则应发送该报文到协议低层以建立物理连接。既然我们假定在两设备之间可

能存在不止一条ACL链路，那么两设备之间的其它L2CAP信道必须共享同一基带ACL链路。

在处理请求之后，低层将返回LP_ConnectCfm或LP_ConnectCfmNeg报文，以指示是否已对该请求进行了确认。

- LP_QoSReq

L2CAP请求协议低层以兼容一个特定QoS 参数集。在处理该请求以后，低层将返回 LP_QoSCfm 或LP_QoSCfmNeg以指示是否已对该请求进行了确认。

- LP_ConnectRsp

接受以前连接指示请求的主动回答(参见LP_ConnectInd)。

- LP_ConnectRspNeg

拒绝以前连接指示请求的否定应答(参见LP_ConnectInd).

3.2.2 L2CAP to L2CAP信令动作

本节包括除与报文传输有关动作以外的相同术语，且不仅限于报文接收部分。

3.2.3 L2CAP to L2CAP数据动作

数据传输对于本节就是一种动作。

3.2.4 从L2CAP到高层的动作

- L2CA_ConnectInd

标识已收到一个发自远程设备的连接请求 (参见L2CA_ConnectReq)。

- L2CA_ConnectCfm

在收到来自远程设备的连接报文后，确认该连接请求已被接受(参看L2CAP_ConnectReq)。

- L2CA_ConnectCfmNeg

连接请求的否定确认(参见L2CA_ConnectReq)。对于该连接请求将触发一个RTX定时器失效事件(参见L2CA_TimeOutInd)，不是一个消极连接应答,最后执行本动作。

- L2CA_ConnectPnd

确认已收到来自远程设备的连接应答(中间应答)。

- L2CA_ConfigInd

表示已收到从来自远程设备的配置请求。

- L2CA_ConfigCfm

在收到来自远程设备的配置应答后，确认已收到该配置请求 (参见L2CA_ConfigReq)。

- L2CA_ConfigCfmNeg
  配置请求的消极确认(参见L2CA_ConfigReq)。对于该连接请求将触发一个RTX定时器失效事件((参见 L2CA_TimeOutInd), 而不是一个消极连接应答,最后再执行本动作。
- L2CA_DisconnectInd
  表示已收到一个来自远程设备连接断开请求，或者是由于应答信令请求失败而导致远程设备断开。
- L2CA_DisconnectCfm
  收到远程设备的连接断开应答后,确认断开请求已由远程设备处理(参见 L2CA_DisconnectReq)。对于该连接请求将触发一个RTX定时器失效事件((参见 L2CA_TimeOutInd), 而不是一个消极连接应答,最后再执行本动作。一旦收到该事件，协议上层即获知L2CAP 信道已被终止。没有对应的消极确认。
- L2CA_TimeOutInd
  表示RTX 或 ERTX 定时器已失效。本动作将在 L2CAP 放弃并发送L2AC_ _DisconnectInd 以前多次执行,执行次数根据实际应用而定。
- L2CA_QoSViolationInd
  表示违反服务质量协定。

3.3 信道操作状态

- CLOSED
  在该状态下, 不存在与 CID关联的信道。本状态是不存在链路层次连接(基带)时的唯一状态。链路断开将强制其它状态转为CLOSED状态。
- W4_L2CAP_CONNECT_RSP
  在该状态下,CID代表当本地终端，以及已经发送与本地终端有关的L2CAP_ConnectReq 报文，并且该终端正在等待对应的L2CAP_ConnectRsp报文。
- W4_L2CA_CONNECT_RSP
  在该状态下，存在远程终端， 且本地L2CAP 实体已收到L2CAP_ConnectReq连接请求报文。同时已发送L2CA_ConnectInd到协议上层，而正对收到的L2CAP_ConnectReq报文进行处理的本地L2CAP 实体的一部, 将等待相应应答。应答需要进行安全校验。
- CONFIG
  在该状态下,已建立连接，但通信双方正在对信道参数进行协商。如果信道参数正在重新协商，也将进入该配置状态。进入GONFIG状态以前,由于要对数据通信参数重新协商, 应暂停呼出的数据通信。但在远程终端进入CONFIG之前, 应一直接收呼入的数据通信。

在该状态下，通信双方必须分发L2CAP_ConfigReq报文:如果只使用缺省值，则发送空报文，如果要对多数参数进行协商，则应发送多个报文以避开MTU限制，并进行增量协商。

从CONFIG状态迁移到OPEN状态需要双方都应做好准备。当一个L2CAP实体收到对它的最后请求的肯定应答时,即表示它已做好准备。然后，该L2CAP实体将对远程设备的最后请求作出肯定应答。

- OPEN
  在该状态下，已建立和配置连接，并且可以继续执行数据流。
- W4_L2CAP_DISCONNECT_RSP
  该状态表示,正在关闭连接，而且L2CAP_DisconnectReq 报文已发送。该状态表示正在等待对应应答。
- W4_L2CA_DISCONNECT_RSP
  该状态表示,远程终端连接正在关闭，且已收到L2CAP_DisconnectReq报文。同时向协议上层发送L2CAP_DisconnectInd报文,以通知该CID的所有远程终端关闭。

3.4 事件到行为的映射

下表定义了在特定状态下，为响应事件而采取的动作。没在该表中列出的事件，或者没标记 N/C (没有变化)的动作,都假定为错误且丢弃。

数据输入输出事件仅为OPEN和CONFIG状态定义。不能在最初的Configration状态期间接收数据，但当为了重新配置而再次进入Configuraton状态时，就可以接收数据。在其它状态下接收的数据将被丢弃。

表4.4 L2CAP 信道状态机

事件	当前状态	行动	新状态
LP_ConnectCfm	关闭（CLOSED）	如上所述标识物理链路,并初始化 L2CAP 连接	关闭（CLOSED）
LP_connectCfmNeg	关闭（CLOSED）	如下所述标识物理链路,并通过向上层发送L2CA_ConnectCfmNeg 报文拒绝服务连接请求。	关闭（CLOSED）
LP_Connectlnd	关闭（CLOSED）	如上所述标识链路。	关闭（CLOSED）
LP_Disconnectlnd	关闭（CLOSED）	如下所述标识连接。	关闭（CLOSED）
LP_Disconnectlnd	除关闭（CLOSED）以外的任何状态	将 L2CA_Disconnectlnd 报文发往上层。	关闭（CLOSED）
LP_QoSViolationlnd	除打开（OPEN）以外的任何状态	丢弃	N/C

LP_QoSViolationlnd	打开（OPEN）	将 L2CA_QoSViolationlnd 报文发往上层，如果能够保证服务水平，则终止信道。	打开（OPEN）或者
L2CAP_ConnectReq	关闭（CLOSED）。（CID 从免费的联营分配来的）	将 L2CA_Connectlnd 发往上层。可选择是否将 L2CAP_ConnectRspPnd 发往对等协议层。	W4_L2CA_CONNECT_RSP
L2CAP_ConnectRsp	W4_L2CAP_CONNECT_RSP	把 L2CA_ConnectCfm 报文发往上层。终止 RTX 定时器。	配置（CONFIG）
L2CAP_ConnectRsp Pnd	W4_L2CAP_CONNECT_RSP	将 L2CA_ConnectPnd 报文发往上层。终止 RTX 定时器并启动 ERTX 定时器。	N/C
L2CAP_ConnectRsp Neg	W4_L2CAP_CONNECT_RSP	将 L2CA_ConnectCfmNeg 报文发往上层。并将 CID 返回自由池。终止RTX/ERTX 定时器。	关闭（CLOSED）
L2CAP_ConfigReq	关闭（CLOSED）	将 L2CAP_ConfigRspNeg报文发往对等协议层。	N/C
L2CAP_ConfigReq	配置（CONFIG）	将 L2CA_Configlnd 报文发往上层。	N/C
L2CAP_ConfigReq	打开（OPEN）	将 L2CA_Configlnd 报文发往上层。	配置（CONFIG）
L2CAP_ConfigRsp	配置（CONFIG）	将L2CA_ConfigCfm报文发往上层。终止 RTX 定时器。如果已收到L2CAP_ConfigReq报文并且已主动应答，则进入OPEN状态，否则仍保持CONFIG状态。	N/C 或者打开（OPEN）
L2CAP_ConfigRsp Neg	配置（CONFIG）	将L2CA_ConfigCfmNeg报文发往上层。终止 RTX 定时器。	N/C
L2CAP_DisconnectReq	关闭（CLOSED）	将L2CAP_DisconnectRsp报文发往对等协议层。	N/C
L2CAP_DisconnectReq	除关闭（CLOSED）以外的任何状态	将 L2CA_Disconnectlnd 报文发往上层。	W4_L2CA_DISCONNECT_RSP
L2CAP_DisconnectRsq	W4_L2CAP_DISCONNECT_RSP	将 L2CA_DisconnectCfm 报文发往上层。终止 RTX 定时器。	关闭（CLOSED）
L2CAP_Data	打开（OPEN）或配置（CONFIG）	如果收到完整L2CAP分组，将L2CA_Read 确认发往上层。	N/C
L2CA_ConnectReq	关闭（CLOSED）（CID从免费的联	将L2CAP_ConnectReq 报文发往对等协议层。启动 RTX	W4_L2CAP_CONNECT_RSP

	营分配来的。）	定时器。	
L2CA_ConnectRsp	W4_L2CA_CONNECT_RSP	将L2CAP_ConnectRsp报文发往对等协议层。	配置（CONFIG）
L2CA_ConnectRsp Neg	W4_L2CA_CONNECT_RSP	将L2CAP_ConnectRspNeg报文发往对等协议层。将CID返回至自由池（free pool）。	关闭（CLOSED）
L2CA_ConfigReq	关闭（CLOSED）	将L2CA_ConfigCfmNeg报文发往上层。	N/C
L2CA_ConfigReq	配置（CONFIG）	将L2CAP_ConfigReq 报文发往对等协议层。启动 RTX 定时器。	N/C
L2CA_ConfigReq	打开（OPEN）	在合适的时候暂停数据传输。并将L2CAP_ConfigReq报文发往对等协议层。启动RTX 定时器。	配置（CONFIG）
L2CA_ConfigRsp	配置（CONFIG）	将L2CAP_ConfigRsp报文发往对等协议层。如果所有L2CAP_ConfigReq报文都收到肯定应答，则进入OPEN状态。否则仍保持CONFIG状态。	N/C 或者打开（OPEN）
L2CA_ConfigRspNeg	配置（CONFIG）	将 L2CAP_ConfigReqNeg报文发往对等协议层。	N/C
L2CA_DisconnectReq	打开（OPEN）或配置（CONFIG）	将L2CAP_DisconnectReq报文发往对等协议层。启动RTX 定时器。	W4_L2CAP_DISCONNECT_RSP
L2CA_DisconnectRsp	W4_L2CA_DISCONNECT_RSP	将L2CAP_DisconnectRsp报文发往对等协议层。将CID返回到自由池。	关闭（CLOSED）
L2CA_dataRead	打开（OPEN）	如果完成有效载荷加载，则将该有效载荷转发到InBuffer。	打开（OPEN）
L2CA_dataWrite	打开（OPEN）	将L2CAP_Data报文发往对等协议层。	打开（OPEN）
Timer_RTX	任何状态	将L2CA_TimeOutlnd 报文发往上层。如果最终失效，则将CID返回到自由池，否则重新发出请求。	关闭（CLOSED）
Timer_ERTX	任何状态	将L2CA_TimeOutlnd报文发往上层。如果最终失效，则将CID返回到自由池，否则重新发出请求。	关闭（CLOSED）

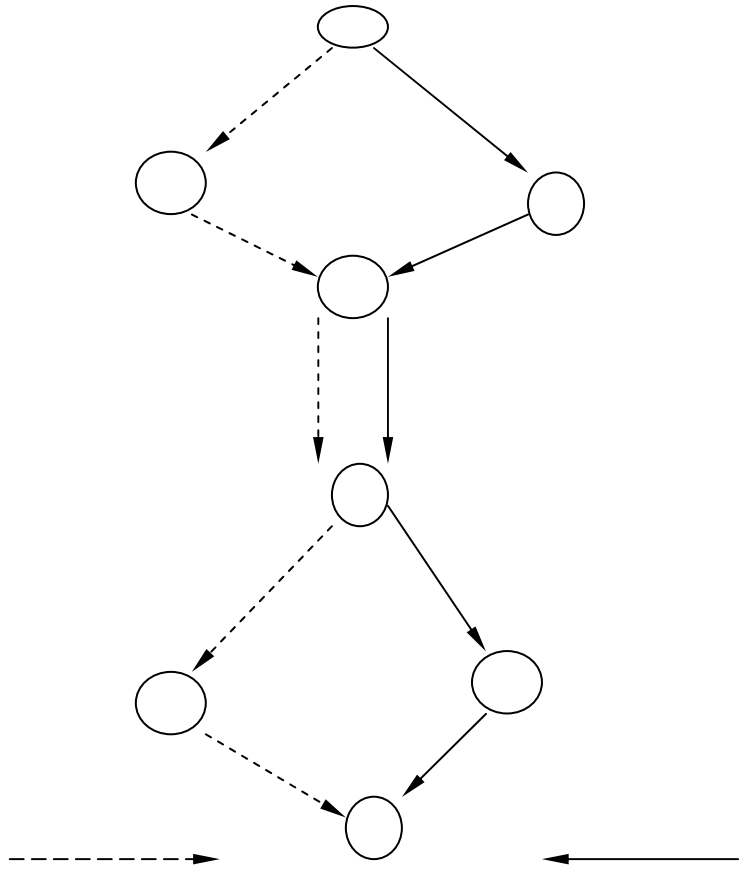


图4.11 状态机实例

该图表示了一个简单状态自动机,以及由初始化方和接收方所采用的状态间典型转换路径。该状态机显示了,由哪一事件导致状态转换,以及在状态转换发生时采取哪一动作。为避免表述不清,该简单状态机并没有将表中所列所有事件包括在内。

下图表示了基于设备通信报文序列的事件和动作。本实例中,由初始化方创建第一条L2CAP信道。通信双方都开始于CLOSED状。收到来自上层的请求后,实体将请求下层建立物理链路。如果不存在物理链路,则采用LMP指令创建设备间物理链路。一旦该物理链路建立,将在该链路上传输L2CAP信令。

该图只是一个例子,并不是所有启动事件序列都与下图一致。

图4.12 基本操作的报文序列图

4 数据分组格式

L2CAP基于分组，但它实际上遵循的是一个基于信道的通讯模型。一条信道代表远程设备上两 L2CAP 实体间的一数据流。信道可以是面向连接的，也可以是无连接的。所有分组中的域都使用小端字节命令。

4.1 面向连接信道

下图说明了在面向连接信道内的 L2CAP分组格式（也称之为 L2CAP PDU ）。

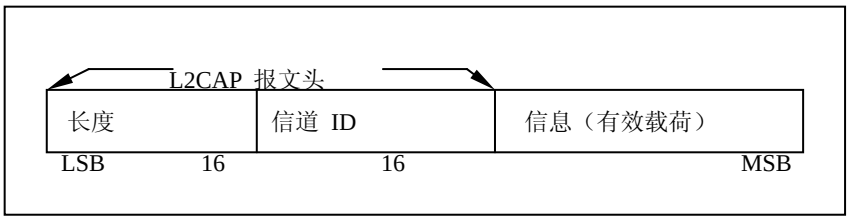


图4.13 L2CAP 分组 (各域以比特为单位)

各域描述如下：

长度：2 个八位字节(16位)

长度指除了 L2CAP 报文头长度以外的信息有效载荷的大小,单位为字节。信息有效载荷的长度可长达65535个字节。长度域作为接收端经重组的L2CAP分组的简单完整性校验位。

信道 ID：2个八位字节

信道 ID用于标识分组的目标信道终端。信道ID取值与接受分组的设备相关。

信息：0到65535个八位字节

信息包含来自上层协议(发出的包)的有效载荷或者发送到协议上层的有效载荷。免相连接分组MTU的最小值将在信道设置期间进行协商。用于信令分组的MTU 的最小值为48字节。

4.2 无连接数据信道

除了面向连接信道以外， L2CAP也支持面向组信道的概念。送到‘组’信道的数据将送往组中所有成员。由于组不提供服务质量，因此组信道通常并不可靠。L2CAP不能保证发往组的信息能够成功到达组中所有成员。如果需要可靠的组传输，它必须在协议高层中执行。

向组的数据传输毫无例外地被传送到该组中所有成员。但本地设备不能成为组成员，而且高层协议将把任何数据流发回到本地设备。毫无例外意味着非组成员也可以接收组传输，而可利用更高层次或链路层次的加密支持私有通信。

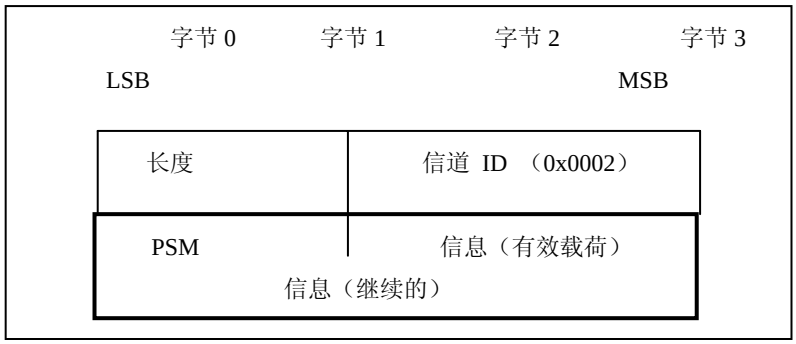


图4.14 无连接分组

各域描述如下：

长度：两个八位字节（16位）。

除去 L2CAP 报文头的长度，长度是信息有效载荷与PSM域长度的和。

信道 ID：两个八位字节

信道 ID（0x0002）保留用于无连接通信。

协议/服务复用(PSM)：2个八位字节(最小)

PSM段以地址段ISO 3309 扩展机制为基础。PSM 段的左右内容,即PSM 值,必须是奇数。也就是说,最低字节的最低位必须为‘1’。而且,所有的 PSM 值的最高字节的最高位应等于‘ 0 ’。这样, PSM 段就可以扩充到16位以上。PSM 值定义主要针对L2CAP,并由蓝牙SIG指定。为了解有关PSM 段的更多信息。

信息：0～65533 个八位字节

该有效载荷信息将分发到组中所有成员。如果没有就其它值达成一致,应用应支持670字节的M最小无连接MTU(MTU$_{cnl}$)。对于遵守某一使用特定无连接通信蓝牙标准的操作设备,其MTU将可小于MTU$_{cnl}$。

L2CAP 组服务接口提供组管理机制，通过该机制可以创建组，给组增加成员，从组中删除成员。但不能够预先规定组。

5．信令

本节描述远程设备上两L2CAP 实体间传递的信令指令。所有信令指令都将送至CID 0x0001。L2CAP应用必须能够确定发出该指令设备的蓝牙地址（BD_ADDR)。下图就包含信令命令的所有 L2CAP 分组通用格式做出描述。可在一个（L2CAP）分组中发送多条指令，该分组将送至CID 0x0001。MTU指令采用请求和应答方式。所有L2CAP应用都必须支持接收MTU小于48字节的信令分组。在没有对该应用是否支持更大信令分组进行测试的情况下,L2CAP应用不得使用超过48字节的信令分组。

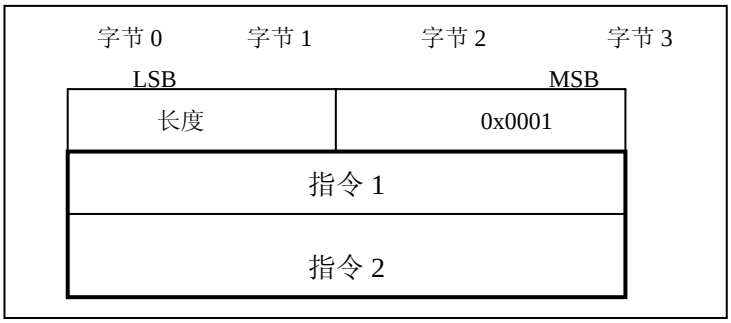


图4.15 信令指令分组格式

下图表示所有信令分组通用格式

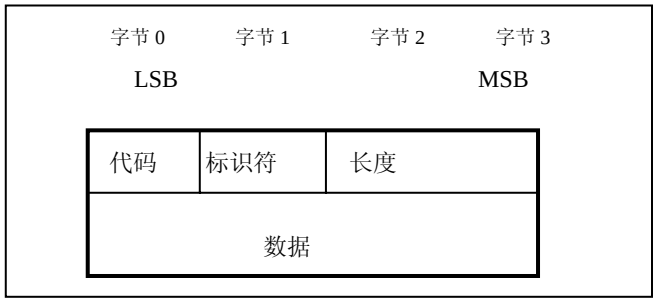


图4.16 指令格式

各域描述如下：

编码：1 个八位字节

编码码段长为一个八位字节，用于标识指令类型。在收到一个含有未知编码域的分组时,作为应答将发出一个指令拒绝分组。 分配编码的当前值在最近的蓝牙‘分配号码’文件中加以说明。所有编码在最左边的位置上以最高位指定。

表4.5 信令指令代码

代码	说明
0x00	保留
0x01	指令拒绝
0x02	连接请求
0x03	连接应答
0x04	配置请求
0x05	配置应答
0x06	连接断开请求
0x07	连接断开应答
0x08	回应请求
0x09	回应应答
0x0A	信息请求
0x0B	信息应答

标识符：1 个八位字节

标识符域长为一个八位字节,用于请求与应答间的匹配。请求方设备设置该域,而应答设备在应答中使用相同值。每个最初的指令必须用不同的标识符。在使用该标识符的最初指令转换开始后的360秒里，不得重复使用标

识符。RTX或ERTX定时器终止时，如果重发同一请求，也应使用同一标识符。收到同一请求的设备也应以同一应答回答。含有非法标识符的应答则应被悄悄丢弃。信令标识符 0x0000被定义为非法标识符，并且不得在任何指令中使用。

长度：2 个八位字节

长度域长为2个八位字节，并只用于以字节为单位表示指令数据域的大小。也就是说，该数据域大小不包含代码、标识符和长度域在内。

数据：任意个八位字节

数据域长度可变。可以使用长度域得到数据域长度。代码域决定数据域格式。

5.1 指令拒绝(代码 0x01)

为了响应含有未知指令编码的指令分组，或者当不适于发送对应指令的时候,才可以发送指令拒绝分组。下图列出分组格式。该标识符应与含有未标识代码域的标识符相匹配。应用通常采用这些分组来应答未标识的信令分组。

当在一个L2CAP分组里包含多条指令,并且该分组超过接收方的MTU时,将以一个指令拒绝分组应答。该标识符应与L2CAP分组的首条请求指令相匹配。如果只有应答被识别，那么将丢弃该分组。

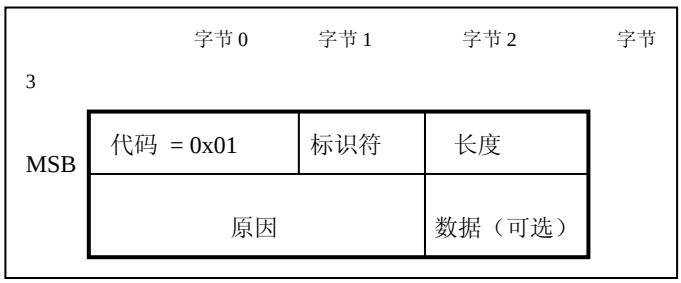


图4.17 指令拒绝分组

长度 = 0x0002或更多的八位字节

原因：2 个八位字节

原因段描述为什么拒绝请求包。

表4.6 原因编码描述

原因值	说明
0x0001	未理解该指令
0x0002	超出信令MTU
0x0003	请求中存在非法CID

其它	保留值

数据： 任意个八位字节

数据段的长度和内容取决于原因代码。如果原因代码是0x0000，即“命令未被理解”,那么就不会使用数据段。如果原因代码是 0x0001，即“超出信令MTU”，那么该两字节数据域将表示该分组接收方收到的最大信令MTU。

如果指令指向一条错误的信道，那么将返回原因编码0x0002。显然，由于该信道不存在,则该信道为非法。指令拒绝的4字节长数据域将包含被争用信道的本地端和远端。远端从对应的被拒绝指令中获取。如果该拒绝指令只包含其中一个信道终端，则用无效的CID 0x0000代替另一端。

表4.7 原因数据值

原因码	数据长度	数据值
0x0000	0 个八位字节	N/A
0x0001	2 个八位字节	实际MTU
0x0002	4 个八位字节	被请求的 CID

5.2 连接请求（代码 0x02）

连接请求分组用于创建一条介于两设备之间的信道。信道连接应在配置开始前建立。下图就连接请求分组做出说明。

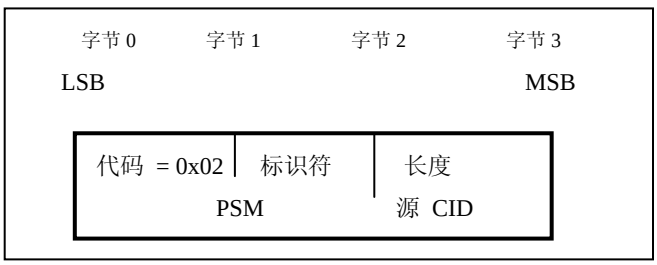


图4.18 连接请求分组

长度 = 0x0004或更多字节

协议/服务复用（ PSM ）：2 个字节(最小)

PSM段长为2个字节(最小)。PSM段结构以地址段的 ISO 3309扩展机制为基础。所有PSM值都必须是奇数,也就是说,最低位字节的最低位必须为‘ 1 ’。而且,所有PSM 值的最高字节的最低位应等于‘0’。这样, PSM段将可以扩展到16位以上。PSM 值被分成两部分。第一部分的值由蓝牙SIG及其协议分配。第二部分的值则可以动态分配，并与服务搜索协议（SDP）一起使用。动态分配的值可以用于支持一个特定协议的多种执行版本,如L2CAP上层的RFCOMM或试验性协议原型。

图4.8 PSM值

PSM 值	说明
0x0001	服务搜索协议
0x0003	RFCOMM
0x0005	电话控制协议
<0x1000	保留
[0x1001-0Xffff]	动态分配

源 CID(SCID): 2 个字节

本地源CID长为2个字节，并可用于标识发送请求设备上的一个信道终端。一旦信道设置，则来自请求发送方的数据分组将被发往该CID。在本节中，源 CID表示发送请求和接收应答的设备上的信道终端,而目标CID则表示接收请求和发送应答设备上的信道终端。

5.3 连接应答(代码 0x03)

当一个单元收到连接请求分组时，它必须发送一个连接应答分组。下图给出了连接应答分组格式。

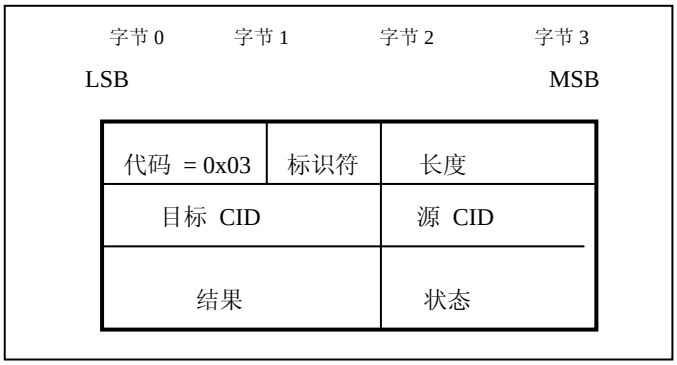


图4.19 连接应答分组

长度 = 0x0008字节

目标信道标识符(DCID): 2 个字节

该段包含发送应答分组设备上的信道终端。

源信道标识符(SCID): 2 个字节

该段包含接收该应答分组备上的信道终端。

结果: 2 个八位字节

结果段指示连接请求的结果。结果值 0x0000 表示连接请求成功，而

非零值则表示连接请求失败。收到成功结果，即建立一条逻辑信道。下表定义了该段的值。如果结果段非零，那么就应忽略DCID 和 SCID 段。

表4.9 结果值

值	说明
0x0000	连接成功
0x0001	正在连接
0x0002	连接被拒绝- 不支持PSM
0x0003	连接被拒绝- 安全块
0x0004	连接被拒绝- 无可用资源
其它	保留值

状态：2 个字节

即中间应答，只有结果段对此做出定义。表示连接状态。

表4.10 状态值

值	说明
0x0000	无更多可用信息
0x0001	正在进行身份验证
0x0002	正在进行授权
其它	保留值

5.4 配置请求(代码 0x04)

配置请求分组用于在两L2CAP实体间建立一个初始逻辑链路传输协定，如果合适，还可以重新对该协定进行协商。在重新协商会话期间，该信道上的所有数据通信都应在得到协商结果之前暂停。配置请求的每个配置参数只能与呼出数据通信和呼入数据据通信两者之一有关。如果L2CAP 实体在等待应答时收到配置请求，那么它也不能阻塞发送配置应答，否则该配置进程将会死锁。

如果没有需要协商的参数，那么也就没有必要插入任何选项，而C-位应被清除。如果不接受缺省值，远程设备上的L2CAP 实体必须就本文件中定义的所有参数进行协商，无论何时缺省值都不能被接受。任何丢失的配置参数都可被假定为它最近的接受值。即使可接受所有缺省值，都必须发送不含有选项段的配置请求分组。暗中接受的值可以是本文件中指定配置参数的任何缺省值，但这些缺省值并没有就设置中信道明确地进行协商。

每一配置参数都是单向的，并且都与配置请求发送方给出方向有关。如果设备需要建立反向的配置参数值，而不是由配置请求给出的参数值，那么就要在与原连接请求相反的方向上发送新的配置请求，而该配置请求将含有希望得到的反向配置参数值。

在终止协商之前，如何确定仲裁信道参数所用时间(报文)的数量将根

据实际应用情况而定,但不能超过 120 秒。

下图定义了配置请求分组的格式。

图4.20 配置请求分组

长度 = 0x0004 或更多字节。

目标 CID(DCID): 2 个八位字节。

该段包含接受该请求分组的设备上的信道终端。

标志: 2 个八位字节。

下图表示了该两字节长的标志段，注意:左边是最高位。

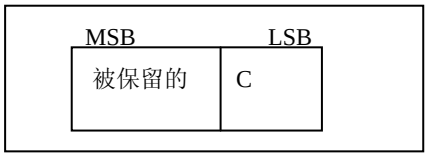


图4.21 配置请求标志段格式

C：当设置为1时，将发送更多的配置请求。该标志表示由于正在发送更多的参数协商报文,在确认这些参数后，远程设备不应进入OPEN状态。如果参数超过MTU_{sig}，则有必要对配置请求分组进行分段。其它标志保留,但应被清空。L2CAP应用应忽略这些位。

配置选项:

包括参数列表以及需要协商参数值。配置请求可以不包含任何选项(可以看作配置请求为空)，并能用于请求一个应答。对于一个为空的配置请求，长度段应设置为0x0004。

5.5 设置应答 （代码 0X05 ）

为回应配置请求分组,必须发送设置应答分组。每一在配置应答中的配

置参数值都反映了对已发出配置参数值的‘调整’。例如,如果配置请求中的配置参数与从设备A到设备B的通信有关，那么该配置应答发送方将根据从设备A到设备B的同一通信流,对该值作出调整。应答中的选项取决于结果段的值。下图对配置应答分组的格式进行了定义。

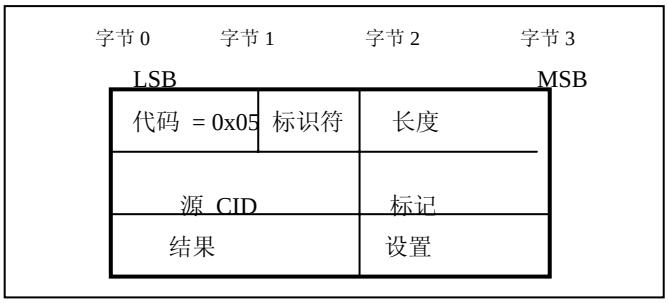


图4.22 配置应答分组

长度 = 0x0006 或更多字节。

源 CID(SCID): 2 个八位字节。

该段包含接受该应答分组设备上的信道终端。接收应答的设备必须检查:标识符段是否与相应配置请求指令中的同一段匹配, SCID是否与匹配于原DCID的本地CID相匹配。

标志：2 个八位字节。

下图表示 2 个八位字节标记段，注意:左边为最高位。

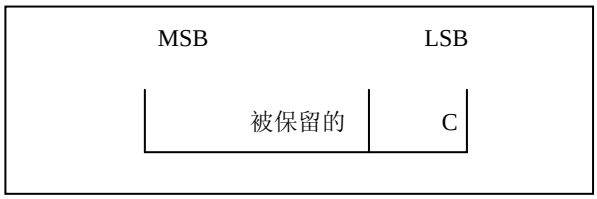


图4.23 配置应答标志段格式

C：在设置为1时,将发送更多配置应答。该标志表示应答参数是发送应答分组设备的一部分参数子集。其它标志应保留,但需清空。L2CAP应用应忽略这些位。

结果：2 个八位字节

结果段指示是否可接受请求（参看下表了解可能出现的结果编码。）

表4.11 配置应答结果代码

结果	说明

0x0000	成功
0x0001	失败-不可接受的参数
0x0002	失败-遭拒绝（没有原因）
0x0003	失败-未知的选择
其它	被保留

配置选项：

该段包含正在协商的参数表。在成功的结果上，这些参数包含任何野卡参数的回值。

当发生参数不能被接受的情况(结果 = 0x0001)时，肯定是返回参数中既包含了被拒绝参数也包含了可能被接受的值。任何丢失的配置参数都被假定为它们最近（互相）的接受值，而且如果需要改变配置参数的话，它们也可以包含在配置应答中。每一配置参数都为单向并与配置请求发送方的指示方向相关。如果配置应答发送方需要在反方向上建立一个配置参数值，而不是原配置请求的指示方向，那么就应在与原连接请求相反的方向上,发送含有所希望的配置参数值的新配置请求。

当出现一个未知选项时(Result = 0x0003),在应答中肯定包含了请求接受方所不理解的选项类型。注意由于不能理解而被跳过的请求选项,不能包括在应答报文里，而且也不能作为拒绝请求的唯一原因。

由应用决定在终止协商之前,花费在确定信道参数上的时间长短或报文数量。

5.6 断开请求(代码0x06)

如果要终止一条L2CAP信道，就需要发送连接断开请求分组，并由断开连接应答分组进行确认。由于发往目的信道的所有其它L2CAP分组都将自动传递到协议上层，则可以通过信令信道请求断开连接。下图表示了连接断开请求分组格式。在初始化连接断开过程以前，接受方必须保证源 CIDs 和目标CIDs 的匹配。一旦断开请求发出，将丢弃在L2CAP信道中传输的所有呼入数据，并且也不允许再对外发送新的数据。一旦接受信道的断开请求，所有在该信道排队等待发送的数据也可能被丢弃。

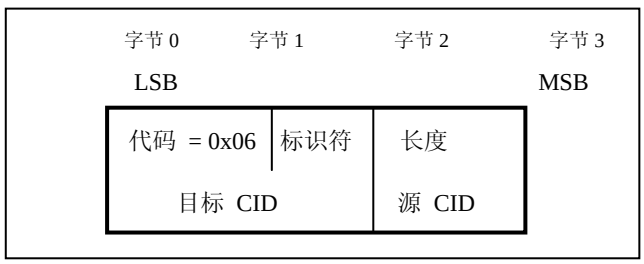


图4.24 连接断开请求分组

长度 = 0x0004 字节。

目标 CID(DCID): 2 个八位字节。

该段用于标识在设备收到该请求时,将被关闭的信道终端。

源 CID(SCID): 2 个八位字节。

该段用于标识在设备发送该请求时, 将被关闭的信道终端。

SCID 和 DCID 与请求发送方有关, 并且必须与将被断开的信道相匹配。如果报文接收方没能识别该DCID, 那么就必须以含有‘无效 CID’结果码的CommandReject报文应答。如果接收方发现只有DCID匹配而SCID却不匹配, 则应丢弃该请求。

5.7 连接断开应答(代码 0x07)

为了响应每一连接断开请求, 应发送连接断开应答。

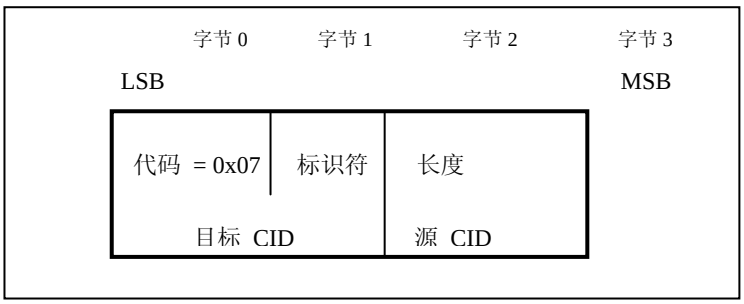


图4.25 连接断开应答分组

长度 = 0x0004 个八位字节。

目标 CID(DCID): 2 个八位字节。

该段用于标识发送应答设备的信道终端。

源 CID(SCID): 2 个八位字节。

该段用于标识接受应答设备的信道终端。

DCID 和 SCID (与请求发送器有关),以及标识符段必须与对应的连接断开请求指令相匹配。如果 CID不匹配, 应在接收方丢弃该应答。

5.8 回应请求(代码 0x08)

回应请求用于请求来自远程L2CAP实体的应答。该请求可以用于测试链路, 或利用可选数据段传递厂商指定信息。L2CAP 实体必须采用回应应答分组来对结构完整的回应请求分组进行应答。数据段可选, 并且可以]根据实际应用情况而定。L2CAP实体应该忽略该段内容。

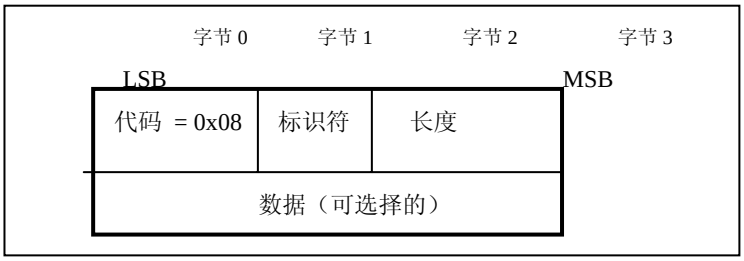


图4.26 回应请求分组

5.9 回应应答(代码 0x09)

一收到回应请求分组就应发送回应应答分组。应答标识符必须与请求标识符匹配。可选的与根据应用而定的数据段可以包含于请求报文中数据段的内容，也可以包含不同数据，或者根本就不包含数据。

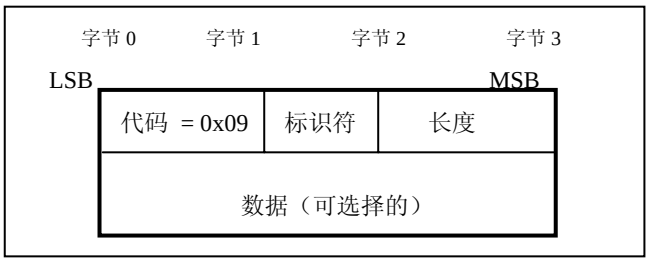


图4.27 回应应答分组

5.10 信息请求 （代码 0X0A)

信息请求用于从远程 L2CAP 实体请求应用指定信息。L2CAP 实体必须使用信息应答分组回应结构完整的信息请求分组。

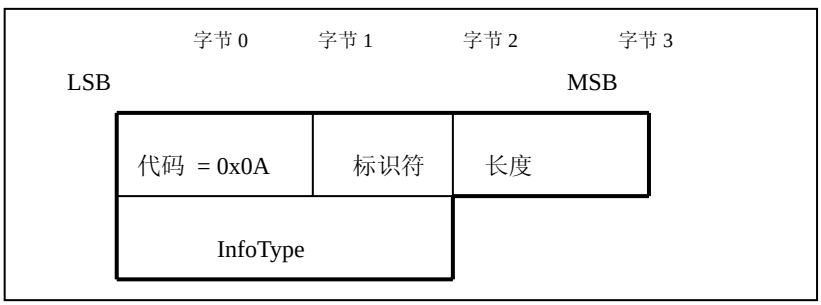


图4.28 信息请求分组

长度 = 0x0002 个八位字节。

信息类型：2 个八位字节。

信息类型定义被请求的应用指定信息的类型。

表4.12 信息类型定义

值	说明
0x0001	无连接最大传输单位 （MTU）
其它	被保留

5.11 信息应答 （代码 0X0B）

一收到信息请求包，就应发送信息应答。应答标识符必须与请求标识符匹配。可选的数据段可以包含请求数据段的内容，可以包含不同的数据，或根本就不包含数据。

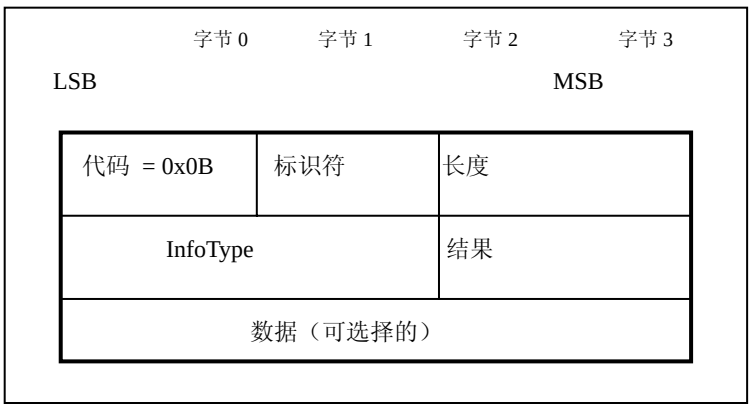


图4.29 信息应答分组

信息类型 ： 2 个八位字节。

在请求中发送的是同样的值。

结果：2 octets 结果：2 个八位字节。

结果包含请求成功与否的信息。如果结果是“成功”，那么数据段包含在下表说明的信息。如果结果为“不支持的信息”，则不会返回任何数据。

表4.13 信息请求结果值

值	说明
0x0000	成功
0x0001	不支持
其它	保留

数据：0 个以上个八位字节。

数据段内容取决于信息类型。对于连接MTU请求，数据段包含远程实体的 2 字节可接受的无连接MTU。

表4.14 信息请求数据段

InfoType	数据	数据长度（以字节计算）
0x0001	无连接最大传输单位 （MTU）	2

6． 配置参数选项

选项是一种用于扩展不同连接要求协商能力的机制。选项以信息单元的形式传输，这些信息单元由选项类型、选项长度和一个以上的选项数据段组成。下图说明选项格式。

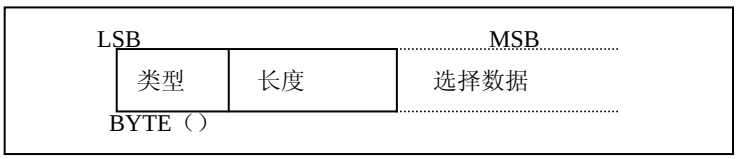


图4.30 配置选项格式

类型： 1 个字节。

选项类型段定义正在设置的参数。如果没能识别出选项，则由选项类型的最高位决定要采取得的动作。以下位取值的含义解释。

0 选择—— 必须识别该选项;表示拒绝配置请求

1 选择—— 表示跳过该选项,继续处理

长度： 1个八位字节

长度段定义选项有效载荷的字节数。无有效载荷的选项类型的长度段值为0。

选项数据：

该段内容取决于选项类型。

6.1 最大传输单位（ MTU ）

该选项说明发送方能够接受的有效载荷大小。类型为0x01，并且有效载荷长度为2个字节。有效载荷携带一两字节的MTU大小值作为唯一信息单元。由于所有L2CAP应用都能够支持最小L2CAP分组大小,MTU不仅可以协商,

而且还是发往远程设备的一个信息参数,该参数表示本地设备能够在本信道中接纳大于最小值的MTU。只有在很少的情况下，远程设备才有可能在该信道中发送比本地设备给出的MTU大的L2CAP分组。然后,该配置请求将会收到一条否定应答。在该应答里,远程设备包含要传输的MTU值。在这种情况下，本地设备是继续配置过程还是维护该信道,将因应用情况而定。

主动配置应答中的远程设备将包括用于本信道到本地设备的通信数据流的实际MTU，该MTU为最小值{在 configReq 的MTU,远程设备的输出MTU的大小}。当远程设备发送自己的配置请求时，将在该信道上，为相反方向通信数据流建立该MTU。

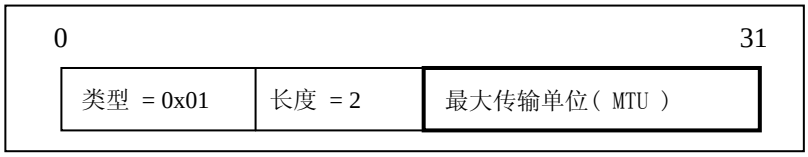


图4.31 最大传输单位(MTU) 选项格式

最大传输单位(MTU)大小： 2 个八位字节。

最大传输单位(MTU)段表示以字节为单位的最大L2CAP分组有效载荷，并且该MTU可以为请求发起方接受。MTU是不对称的。而且请求发送方将定义可从信道接收的MTU,其值与缺省值不同。L2CAP应用必须支持至少48字节的MTU最小长度。缺省值为 672字节。

注 ①:选择缺省MTU，应以由两基带DH5分组(2*341=682)减去基带ACL分组头(2*2=4)与L2CAP 报文头(6)的和为基础。

6.2 刷新超时选择

本选项用于在放弃和刷新分组之前,起始链路控制器/链路管理器传输L2CAP段所耗时间通知接收方。其类型为0x02, 并且有效载荷大小为 2 个字节。

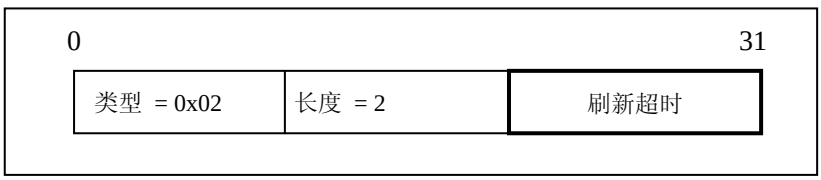


图4.32 刷新超时

刷新超时：

该值表示以毫秒为单位的时间单元。该值为1时表示，由于最小轮询间隔为1.25ms,不能执行基带层次的重发操作。为1的所有值都表时可无限制

地进行重发。这也就是‘可靠信道’的特点。在这种情况下，链路管理器将持续重发一个段，直到物理链路丢失。该值为不对称值，并且如果它与0xFFFF缺省值不同，那么请求发送方将指定自己的刷新超时。

6.3 服务质量(QOS)选项

该选项说明与RFC 1363 [1]类似的流控制规范。如果没有协商QoS 配置参数，那么链路就应假设为以下缺省参数。QoS 选项为类型 0x03 。

当该选项包含于配置请求时，用于描述从发送请求设备到接收请求设备的呼出数据流。如果该选项包含于主动配置应答,从发送该应答的设备角度来看,它用于描述呼入数据流协定。从当该选项包含于消极配置应答时,从发送应答设备的角度来看，它用于描述呼入数据流。

L2CAP应用只需要支持‘最大化’服务；对于其它任何服务类型是可选的。最大化服务并不需要任何授权。如果没有将QoS 选项置于请求中，必须假定为最大化服务。如果需要任何 QoS 授权，则必须发送QoS 配置请求。

远程设备将取决于结果段值的信息置入配置应答。如果为了服务授权而请求,那么应答将包含为在应答中的任何令牌参数的指定值(参见通信速率和令牌最大长度的描述)。如果该结果是“失败—不能接受该参数”，那么应答将可能包含一系列呼出流控制规范参数和参数值，这些参数值可以生成一个来自本地设备的新的连接请求,而本地设备必须能够为远程设备接受。明确定义的配置请求或暗含的配置参数中的引用值都将包含于配置应答。所有来自配置请求的丢失的配置参数将假定为最近接受的值。为了实现最大化和经授权的服务，当配置应答中包含QoS 选项时，配置请求中将包含“无关项”值。

0x03	长度 = 22	标记	服务类型
标志率			
标记桶长度（字节）			
高峰带宽（字节/秒）			
潜伏期（微秒）			
迟滞变化			

表4.15 服务质量说明规范

标志： 1个八位字节。

保留以备以后使用，并且必须设置为 0。

服务类型： 1 个八位字节。

该段表示需要的服务层次。表6.1对不同的可用服务做出定义。如果选择了无通信’,由于在呼出方向上不会从信道中发送任何数据,则其余段将被忽略。

如果选择了缺省值‘最大化’,则其余段应由远程设备作为暗含要求。远程设备可能会忽略这些段,以努力满足该暗含要求, 但不提供应答(在应答信息中省略了QoS 选项),或者以要满足的设置来应答。

表4。16 服务类型定义

值	说明
0x00	无通信
0x01	最大化（缺省值）
0x02	经授权
其它	保留

通信速率：4 个八位字节。

该段值用于表时通信速率,以字节/秒为单位。一个应用可以按照该速率连续发送数据。而 突发数据可以以最大令牌长度发送(参看以下内容)。突发数据发送完毕后,应用必须限制其通信速率。0x00000000 值表示没有指定通信速率。该值为缺省值，它与通信速率并无不同。0xFFFFFFFF值代表一张与最大可用通信速率相匹配的令牌。该值含义取决于与服务类型有关的语义。对于最大化服务，该值表示应用需要尽可能多的带宽。对于授权服务，在请求时该值表示最大可用带宽。

最大令牌长度：4 个八位字节。

该段值以字节为单位表示最大令牌长度。如果达到最大令牌长度，应用程序就必须等待,或者将数据丢弃。0x00000000 的值表示不需要最大令牌长度,该值为缺省值。0xFFFFFFFF值表示与最大令牌长度相匹配的令牌。该值含义取决于与服务类型有关的语义。对于最大化服务，该值表示应用需要一个尽可能大的令牌长度。对于授权服务，该值表示请求时最大可用缓冲区。

带宽峰值：4 个八位字节。

该段值表示,以字节/秒为单位,来自应用的分组连续传输速率。中间系统可以利用该信息进行更有效的资源分配。缺省值0x00000000表示最大带宽是未知的。

延迟：4 个八位字节。

该段值是指发送端传输一位和首次无线传输之间的最大可接受延迟，

以微秒为单位。对该数量的精确解释取决于服务类指定的授权水平。缺省值0xFFFFFFFF表示该值无关。

延迟区间：4 个八位字节。

单位为微秒，该段值是指分组的最大延迟时间和最小延迟时间之差。应用采用该值来确定接收方所需缓冲区的大小，以恢复原有数据传输模式。缺省值0xFFFFFFFF表示该值无关。

6.4 配置处理

对信道参数的协商包括3步：

1．将本地接受的非缺省参数通知远端。

2．使远端同意或拒绝这些参数值(包括缺省值)；可以根据需要重复第(1步和第(2)步。

3．在反方向上重复第(1)步和第(2)步动作，即在远端到本地方向上。

该处理可抽象成为一条请求协商路径和应答协商路径。

6.4.1 请求路径

请求路径就呼入MTU、刷新超时和呼出流量规范进行协商。下表定义了配置选项，这些配置选项可置入配置请求报文及其语义中。

表4.17 可置入请求的参数

参数	说明
最大传输单位 (MTU)	呼入MTU信息
FlushTO	呼出刷新超时
OutFlow	呼出流量信息

6.4.2 应答路径

应答路径就呼出MTU(即:远端呼入MTU)、远端刷新超时和呼入流量规范(即:远端呼出流量规范)进行协商。如果请求报文中没有包含面向请求的参数(恢复为缺省值)，远端通过将推荐值包含在消极应答报文中，协商非缺省值。

表4.18 允许在应答中使用的参数

参数	说明
最大传输单位 (MTU)	呼出MTU信息
FlushTo	呼入刷新超时
InFlow	呼出流量信息

6.4.3 配置状态机

以下配置状态机图示了两条路径。在离开CONFIG状态并进入OPEN状态之前，两条路径必须闭合。请求路径要求本地设备接收主动应答以进入闭合状态，而应答路径要求本地设备发送主动应答以进入闭合状态。

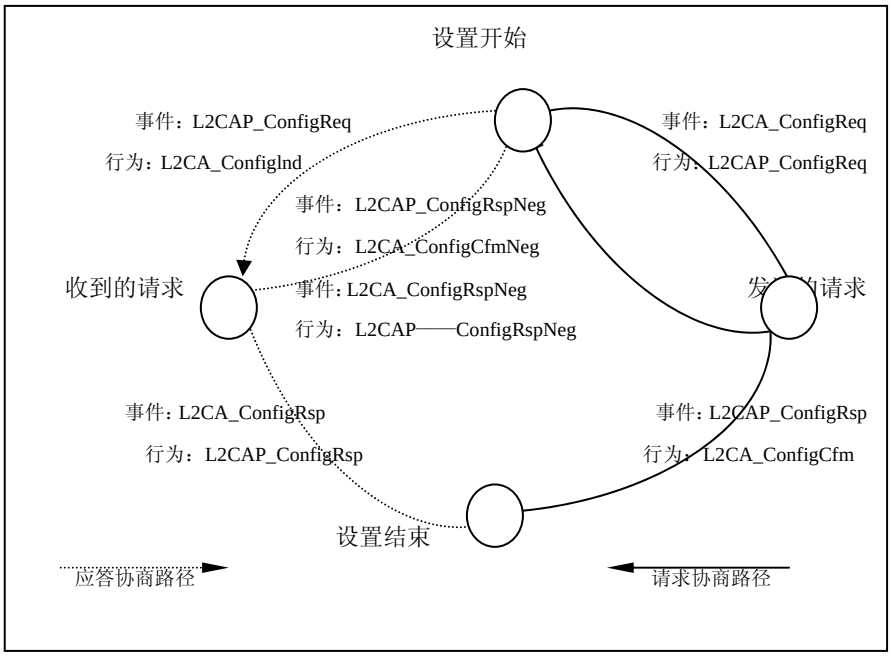


图4.33 配置状态机

配置 MSCs 将提供一些配置实例。

7． 服务原语

本节按照由L2CAP给出的服务原语和参数对服务作出抽象描述。而服务接口需要进行测试。接口在不同应用平台上分别进行描述。所有数据值都采用LITTLE EDIAN CODE。

7.1 事件指示

表4.19

服务	输入参数	输出参数
EventIndication	事件,回呼	结果

描述：

当选择的指示事件发生时，使用原语需要请求回叫信号。

输入参数：

事件 类型：uint 大小：2 个八位字节

表4.20

值	说明

0x00	保留值
0x01	L2CA_Connectlnd
0x02	L2CA_Configlnd
0x03	L2CA_Disconnectlnd
0x04	L2CA_QoSViolationlnd
其它	保留

回叫　　类型:功能　　大小:N/A

表4.21

事件	回叫功能输入参数
L2CA_Connectlnd	BD_ADDR,CID,PSM,标识符
L2CA_Configlnd	CID,OutMTU,InFlow,InFlushTO
L2CA_Disconnectlnd	CID
L2CA_QoSViolationlnd	BD_ADDR

输出参数:

结果　　类型：uint　　大小：2 个八位字节

表4.22

值	说明
0x0000	事件注册成功
0x0001	事件注册失败

7.1.1 L2CA_ConnectInd 回叫

回叫功能包括分发连接请求的远程设备地址参数、代表被请求信道的本地CID、包含于请求的标识符和请求目标PSM值等四个部分。

7.1.2 L2CA_ConfigInd 回叫

该回叫功能包括表示请求发往信道本地CID的参数、呼出MTU(可通过信道发送的最大分组)的长度，以及描述呼入数据的流量规范等三个部分。如果远程设备没有专门提供参数，则将所有其它参数设置为其缺省值。

7.1.3 L2CA_DisconnectInd 回叫

该回叫功能包括包括标志请求发往信道本地CID的参数。

7.1.4 L2CA_QoSViolationInd 回叫

该回叫功能包括表示蓝牙设备地址的参数，这些蓝牙设备违背了服务质量协定。

7.2 连接

表4.23

服务	输入参数	输出参数
L2_ConnectReq	PSM,BD_ADDR	LCID,结果，状况

描述:

该原语初始化发送L2CA_ConnectReq报文并独占，并且阻塞，直到收到相应 L2CA_ConnectCfm(Neg) 或 L2CA_TimeOutInd报文。

使用原语请求创建一条信道，该信道代表与一个物理地址的逻辑链路。其输入参数是目标协议(PSM)和远程设备的 48 位地址(BD_ADDR)。输出参数是由本地L2CAP实体分配的 CID(LCID)，以及请求的Result域。如果Result指示连接成功，LCID 值包含当地终端的标识。否则返回的LCID 应设置为 0。如果Result表示一则未发出的通知，其Status值包含有关通过什么处理可以推迟连接建立的信息。否则应忽略该Status值。

输入参数:

PSM 类型：uint 长度：2 个八位字节

表4.24

值	说明
0xXXXX	由连接提供的目标PSM

BD_ADDR 类型：uint 长度：6 个八位字节

表4.25

值	说明
0xXXXXXXXXXXXX	目标设备的唯一蓝牙地址

输出参数:

LCID 类型：uint 长度：2 个八位字节

表4.26

值	说明
0xXXXX	如果Result = 0x0000，信道 ID 代表通信信道的本地终端，否则设置为0。

Result 类型：uint 长度：2 个八位字节

表4.27

值	说明
0x000	连接成功，CID 标识本地终端。忽略Status参数。
0x001	正在连接。检查Status参数以了解更多信息。
0x002	连接被拒绝，由于PSM服务未注册。

0x03	连接被拒绝，由于远端安全体系机构怀疑该请求。
0xEEEE	连接超时。由于连接确定报文中含有定时器终止指示。

Status 类型：uint 长度：2 个八位字节

表4.28

值	说明
0x0000	无进一步信息
0x0001	正在进行身份鉴定
0x0002	正在授权

7.3 连接应答

表4.29

服务	输入参数	输出参数
L2_ConnectRsp	BC_ADDR,标识符,LCID, 应答,状况	结果

描述：

该原语代表L2CA_ConnectRsp。该原语的使用为连接请求事件指示发送一则应答报文。其输入参数包括远程设备的48位地址、在请求中发送的标识符、本地CID、应答码，以及附加到应答代码的Status参数等五个参数。输出参数为服务请求的Result段。在收到回呼指示后，原语只能调用一次。一旦本地L2CAP实体验证该请求，将返回该原语。返回成功表示应答已通过无线接口发送。

输入参数：

BD_ADDR 类型：unit 长度：6 个八位字节

表4.30

值	说明
0xXXXXXXXXXXXX	目标设备的唯一蓝牙地址

标识符 Type:类型：uint 长度：1 个八位字节

表4.31

值	说明
0xXX	该值必须与 L2CA_Connectlnd 事件中收到的值相匹配。

LCID 类型: uint 长度：2 个八位字节

表4.32

值	说明
0xXXXX	信道 ID 代表信道的本地终端。

应答 类型：uint 长度：2 个八位字节

表4.33

值	说明
0x0000	连接成功
0x0001	正在进行连接
0x0002	连接被拒绝—不支持 PSM
0x0003	连接被拒绝—安全块
0x0004	连接被拒绝—无可用资源
0xXXXX	其它连接应答代码

状态 类型：uint 长度：2 个八位字节

表4.34

值	说明
0x0000	无进一步可用信息
0x0001	正在进行身份鉴定
0x0002	正在进行授权
0xXXXX	其它Status代码

输出参数：

结果 类型：uint 长度：2 个八位字节

表4.35

值	说明
0x0000	成功发出应答
0x0001	未能与连接请求匹配

7.4 配置

表4.36

服务	输入参数	输出参数
L2CA_ConfigReq	CID,InMTU,OutFlow, OutFlushTO, LinkTO	Result,InMTU, OutFlow, OutFlushTO,

描述：

该原语开始发送一条L2CA_ConfigReq报文，并且阻塞住，直到收到一个相应的 L2CA_ConfigCfm (Neg)或 L2CA_TimeOutInd报文。

原语的使用请求将信道重新设置为新的信道参数集。输入参数包括本地CID终端、可接收的新呼入MTU(InMTU)、刷新和链路超时和新呼出流量规范等四个参数。构成 L2CA_ConfigCfm(Neg)报文输出参数包括Result、已

接受的呼入MTU(InMTU）、远端流量请求,以及刷新和连接超时。注意：只有在本地L2CAP实体移出CONFIG状态后（也可以又回到CONFIG状态)，才返回输出结果。

输入参数：

CID 类型：uint 长度：2 个八位字节

表4.37

值	说明
0xXXXX	本地CID

InMTU 类型：uint 长度：2 个八位字节

表4.38

值	说明
0xXXXX	该信道能接受的最大传输单位

OutFlow 类型：Flow 长度：x 个八位字节

表4.39

值	说明
flowspec	服务质量参数，用于处理送出数据流的通信特征。

OutFlushTO 长度：2 个八位字节

表4.40

值	说明
0xXXXX	在卸载未能在物理层确认的分组之前,所需的等待时间(以微秒为单位。)
0x0000	请求使用已有刷新超时值，否则就使用缺省值（0xFFFF）
0x0001	不在基带层上执行重发
0xFFFF	在基带层上执行重发，直到发生连接超时而终止该信道

LinkTO 长度：2 个八位字节

表4.41

值	说明
0Xxxxx	在链路超时终止信道之前用于等待时间(以微秒为单位)

输出参数：

Result 长度：2 个八位字节

表4.42

值	说明
0x0000	配置成功。参数包含双方一致同意的值

0x0001	失败—非法CID
0x0002	失败—参数不可接受
0x0003	失败—超出信令MTU
0x0004	失败—未知选项
0xEEEE	发生配置超时。这是包含于配置确认的定时器终止指示的结果

InMTU 长度：2 个八位字节

表4.43

值	说明
0xXXXX	远程单元将通过该信道发送的最大传输单元（可能小于或等于 InMTU 输入参数）

OutFlow 长度：2 个八位字节

表4.44

值	说明
FlowSpec	服务质量参数. 如果Result成功，用于处理发出数据流的通信特征;否则,则用于代表被请求的服务质量

OutFlushTO 长度：2 个八位字节

表4.45

值	说明
0xXXXX	在 L2CAP 包不能在物理层被确认而丢失以前,用于等待的时间,以微秒为单位—使用该值可查询用于发出分组的实际值。它小于或等于输入参数OutFlushTO。

7.5 配置应答

表4.46

服务	输入参数	输出参数
L2CA_ConfigRsp	CID,OutMTU,InFlow	Result

描述：

该原语代表 L2CAP_ConfigRsp。

原语的使用将向配置请求事件指示发出应答。输入参数包括本地CID终端、发出的 MTU（等于或小于L2CA_ConfigInd事件中的OutMTU 参数），以及为呼入通信接受的流量规范 。输出参数是Result值。

输入参数：

LCID 类型：uint 长度：2 个八位字节

表4.47

值	说明
0xXXXX	本地信道标识符。

OutMTU 类型：uint 长度：2 个八位字节

表4.48

值	说明
0xXXXX	该信道将要发送的最大传输单元

InFlow 类型：流动 长度：x个八位字节

表4.49

值	说明
FlowSpec	服务质量参数，用于处理呼入数据流的通信特征

输出参数:

Result 长度：2 个八位字节

表4.50

值	说明
0x0000	配置成功。参数包含双方一致同意的值
0x0001	配置失败—不能接受的参数
0x0002	配置失败—被拒绝
0x0003	配置失败—错误的 CID
0x0004	配置失败—未知选项
0xXXXX	保留

7.6 连接断开

表4.51

服务	输入参数	输出参数
L2CA_DisconnectReq	CID	Result

描述:

该原语代表L2CAP_DisconnectReq，其返回输出参数要么表示对应L2CAP_DisconnectRsp，要么表示RTX 定时器失效。

使用该原语需要请求断开信道。输入参数为表示当地信道终端的CID。输出参数是Result。如果收到 L2CAP_DisconnectRsp，则Result为零,否则将返回非零值。一旦请求连接断开，没有任何处理能够成功读写CID。正在进行的写操作应继续。

输入参数:

CID 类型：uint 长度：2 个八位字节

表4.52

值	说明
0xXXXX	信道ID代表通信信道的本地端

输出参数：

Result 类型：uint 长度：2 个八位字节

表4.53

值	说明
0x0000	由于收到断开应答报文而成功断开连接。
0xEEEE	发生连接断开超时

7.7 写

表4.54

服务	输入参数	输出参数
L2CA_DataWrite	CID,Length,OutBuffer	长度，Result

描述：

使用原语需要通过该信道转发数据。如果数据长度超出OutMTU，那么只会发出首个OutMTU 字节。该字节可用于面向连接和无连接的通信。

输入参数：

CID 类型：uint 长度：2 个八位字节

表4.55

值	说明
0xXXXX	信道 ID 代表通信信道的本地端

长度 类型：uint 长度：2 个八位字节

表4.56

值	说明
0xXXXX	以字节为单位的缓存大小，在该缓存里存储了用于发送的数据

OutBuffer 类型：指针 长度：N/A

表4.57

值	说明

N/A	用于存储报文的输入缓存器地址

输出参数:

长度 类型：uint 长度：2 个八位字节

表4.58

值	说明
0xXXXX	传输的字节数

Result 类型:uint 长度:2字节

表4.59

值	说明
0x0000	成功写
0x0001	错误—刷新定时器失效
0x0002	错误—链路终止

读

表4.60

服务	输入参数	输出参数
L2CA_DataRead	CID,Length,InBuffer	Result,N

描述:

使用该原语需要请求接受数据。当数据可用或链路终止时，将返回该请求。返回的数据代表唯一的L2CAP有效载荷。如果没有足够的可用数据,该命令将阻塞,直到数据到达或链路终止。如果有效载荷大于缓冲区，那么只有适合该缓冲区的部分有效载荷才被返回，而有效载荷的其余部分将被丢弃。该指令可用于面向连接和无连接的通信。

输入参数:

CID 类型：uint 长度：2 个八位字节

表4.61

值	说明
0xXXXX	CID

长度 类型：uint 长度：2 个八位字节

表4.62

值	说明
0xXXXX	以字节为单位的缓存大小，收到的数据将被存储在该缓存中。

InBuffer 类型：pointer 长度：N/A

表4.63

值	说明
N/A	用于存储报文的缓存器地址

输出参数：

Result

表4.64

值	说明
0x0000	成功

N 类型：uint 长度：2 个八位字节

表4.65

值	说明
0xXXXX	发送到InBuffer的字节数

7.9 创建组

表4.66

服务	输入参数	输出参数
L2CA_GroupCreate	PSM	CID

描述：

使用该原语要求请求创建一个CID,以提供一条到多个设备的逻辑连接。输入参数是用于标记呼出无连接通信的PSM值，而过滤器则用于呼入通信。输出参数是代表本地端的CID。在创建时，组为空，而预定义为PSM值的呼入通信应可读。

输入参数：

PSM 类型：uint 长度： 2 个八位字节

表4.67

值	说明
0xXXXX	协议/服务复用器值

输出参数：

CID 类型：uint 长度：2 个八位字节

表4.68

值	说明
0xXXXX	信道ID代表通信信道的本地端

7．10 关闭组

表4.69

服务	输入参数	输出参数
L2CA_GroupClose	CID	Result

描述：

使用该原语可关闭组。

输入参数：

CID 类型：uint 长度：2 个八位字节

表4.70

值	说明
0xXXXX	信道 ID 代表通信信道的本地端

输出参数：

结果 类型：uint 长度：2 个八位字节

表4.71

值	说明
0x0000	成功关闭信道
0x0001	非法CID

7．11 增加组成员

表4.72

服务	输入参数	输出参数
L2CA_GroupAddMember	CID,BD_ADDR	Result

描述：

可使用该原语请求增加一个组成员。输入参数包括代表组的CID和新增成员的BD_ADDR。输出参数Result用于确认请求成功与否。

输入参数：

CID 类型：uint 长度：2 个八位字节

表4.73

值	说明
0xXXXX	代表通信信道的本地端的信道 ID

BD_ADDR 类型：uint 长度：6 个八位字节

表4.74

值	说明
0xXXXXXXXXXXXX	远程设备地址

输出参数：

结果 类型：uint 长度：2 个八位字节

表4.75

值	说明
0x0000	成功
0x0001	未能与远程设备建立连接
其它	保留

7．12 删除组成员

表4.76

服务	输入参数	输出参数
L2CA_GroupRemoveMember	CID,BD_ADDR	Result

描述：

可使用该原语请求从一个组里删除一个成员。输入参数包括代表组的CID和将要被删除的组成员的BD_ADDR。输出参数Result确定请求是否成功。

输入参数：

CID 类型：uint 长度：2 个八位字节

表4.77

值	说明
0xXXXX	代表通信信道的本地端的信道 ID

BD_ADDR 类型：uint 长度：6 个八位字节

表4.78

值	说明
0xXXXXXXXXXXXX	将被删除的唯一蓝牙设备地址

输出参数：

Result 类型：uint 长度：2 个八位字节

表4.79

值	说明
0x0000	成功
0x0001	失败—设备不是组成员
其它	保留值

7.13 得到组成员描述表13得到组成员描述

表4.80

服务	输入参数	输出参数
L2CA_GroupMembership	CID	Result,N,BD_ADDR_Lst

描述:

可使用该原语请求有关组成员的报告。输入参数CID表示被查询的组。输出参数Result确定用于确认操作是否成功。如果Result成功，则BD_ADDR_Lst是组内N个成员的蓝牙地址列表。

输入参数:

CID 类型：uint 长度：2 个八位字节

表4.81

值	说明
0xXXXX	代表通信信道本地端的信道ID

输出参数:

结果 类型：uint 长度：2 个八位字节

表4.82

值	说明
0x0000	成功
0x0001	失败—组不存在
其它	保留值

N 类型：uint 长度：2 个八位字节

表4.83

值	说明
0x0000-0Xffff	由信道端CID确定的组设备数量。如果Result指示失败，N应设为0。

BD_ADDR_List 类型：pointer 长度：N/A

表4.84

值	说明
0xXXXXXXXXXXXX	由信道端点 CID 确定的 N 个特定蓝牙地址。如果Result指示失败，返回地址只能是全部为零的地址。

7.14 PING

表4.85

服务	输入参数	输出参数
L2CA_Ping	BD_ADDR, ECHO_DATA,Length	结果，ECHO_DATA,长度，

描述:

该原语表示L2CA_EchoReq指令的开始和相应的 L2CA_EchoRsp 指令的接收。

输入参数:

BD_ADDR 类型：uint 长度: 6 个八位字节

表 4.86

值	说明
0xXXXXXXXXXXXX	目标设备的唯一蓝牙地址

ECHO_DATA 类型：指针 长度：N/A

表 4.87

值	说明
N/A	缓冲器包含将要在回应请求指令的数据有效载荷中发送的内容

长度 类型：uint 长度: 2 个八位字节

表 4.88

值	说明
0xXXXX	缓冲区中以字节为单位的数据长度

输出参数:

结果 类型：uint 长度: 2 个八位字节

表 4.89

值	说明
0x0000	已收到应答
0x0001	发生超时

ECHO_DATA 类型：指针 长度：N/A

表 4.90

值	说明
N/A	缓冲器包含将要在回应请求指令的数据有效载荷中发送的内容

长度 类型：uint 长度: 2 个八位字节

表 4.91

值	说明
0xXXXX	在缓冲器中以字节为单位的数据长度

7.15 GETINFO

表4.92

服务	输入参数	输出参数
L2CA_Getinfo	BD_ADDR, InfoType	Result, InfoData,

描述：

该原语表示L2CA_InfoReq 命令的开始和相应的 L2CA_InfoRsp 命令的接收。

输入参数：

BD_ADDR 类型：uint 长度: 6 个八位字节

表 4.93

值	说明
0xXXXXXXXXXXXX	目标设备的唯一蓝牙地址

InfoType 类型：uint 长度: 2 个八位字节

表 4.94

值	说明
0x0001	最大的无连接 MTU 长度

输出参数：

结果 类型：uint 长度: 2 个八位字节

表 4.95

值	说明
0x0000	已收到应答
0x0001	不支持
0x0002	PDU 被拒绝，远程设备不支持
0x0003	发生超时

InfoData 类型：pointer 长度：N/A

表 4.96

值	说明
N/A	缓冲器包含将要在回应请求指令的数据有效载荷中发送的内容

长度 类型：uint 长度: 2 个八位字节

表 4.97

值	说明
0xXXXX	InfoData 缓冲区中以字节为单位的数据大小

7.16 中止无连接通信

表4.98

服务	输入参数	输出参数
L2CA_DisableCLT	PSM	Result

描述:

本原语为中止无连接分组接收的通用请求。输入参数是表示应该被堵住的服务的PSM 值。这个指令可以用来逐渐地停用一套 PSM 值。使用‘有病的’ PSM 0x0000 会堵住所有的无连接的通讯。输出参数结果显示命令是成功或是故障。一台有限的设备只能支持一般堵塞而不能支持 PSM 特定的堵塞，并且不能堵塞任何其中不含零的 PSM 值。

输入参数：

PSM 类型：uint 长度: 2 个八位字节

表 4.99

值	说明
0x0000	堵塞所有的无连接通讯量
0xXXXX	协议/服务多路器段将被堵塞

输出参数：

结果 类型：uint 长度: 2 个八位字节

表 4.100

值	说明
0x0000	成功
0x0001	失败—不支持

7.17 启用无连接通讯

表4.101

服务	输入参数	输出参数
L2CA_EnableCLT	PSM	结果

描述:

该原语是启用无连接包接收进程的通用请求。输入参数是指示应解锁

设备的PSM值。该命令可以用于逐步启用一组PSM 值。’非法’ PSM值0x0000的使用将启用所有无连接通信。输出参数Result将指示该指令是否成功。一台受到限制的设备只支持通用启用过程,而不能支持指定PSM的过滤器,并且不能启用任何非零的PSM 值。

输入参数:

PSM 类型：uint 长度: 2 个八位字节

表4. 102

值	说明
0x0000	启用所有无连接通信
0xXXXX	要启用的协议/服务复用段

输出参数:

结果 类型：uint 长度: 2 个八位字节

表 4. 103

值	说明
0x0000	成功
0x0001	失败—不支持

8． 总结

逻辑链路控制和适配协议(L2CAP)是在基带之上工作的两链路层协议之一。L2CAP 负责高层协议复用、提取MTU、组管理，以及将服务质量信息传送到链路层次。

定义信道支持协议复用。每一信道将采用多对一方式绑定于单一协议。复用信道可以被绑定在同一协议上，但是一条信道不能绑定于多重协议。在信道上收到的每一L2CAP 分组都指向合适的高层协议。

L2CAP提取由基带协议使用的不同大小的分组。而且，它可以使用低成本的分段重组机制，支持达64 K B的分组。

组管理协议提供允许在匹克网成员与组之间有效映射的单元组概念。组通信是无连接的和不可靠的。当组只由一对单元组成时，组将提供无连接信道，以代替L2CAP面向连接信道。

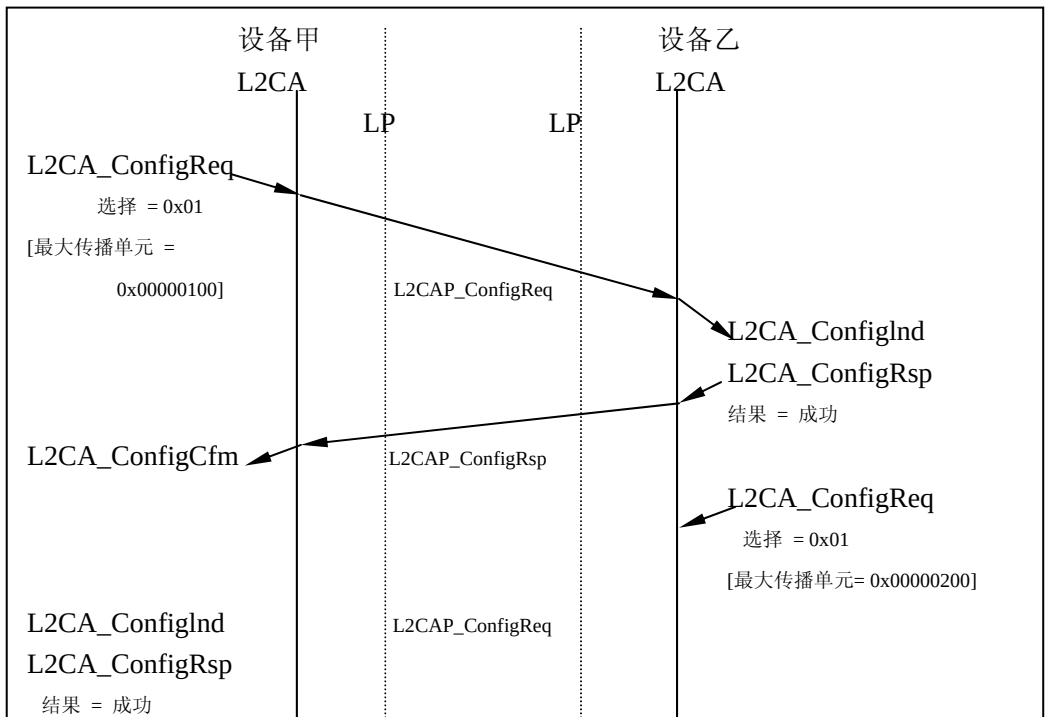
L2CAP可以通过信道传输QoS信息，并且提供授权控制，以避免其它信道违反Q Os协定。

附录: 配置MSC及执行准则

本附录中的给出一个含有可能发生的多个配置场景的实例。现在作为建议提出这些场景,但它们在规范下一版本中可能改变。

下图描述了基本配置进程。在该例中，设备交换MTU信息。所有其它值

都假定为缺省值。


设备甲
L2CA
LP
LP
设备乙
L2CA
L2CA_ConfigReq
选择 = 0x01
[最大传播单元 =
0x00000100]
L2CAP_ConfigReq
L2CA_Configlnd
L2CA_ConfigRsp
结果 = 成功
L2CA_ConfigCfm
L2CAP_ConfigRsp
L2CA_ConfigReq
选择 = 0x01
[最大传播单元= 0x00000200]
L2CA_Configlnd
L2CA_ConfigRsp
结果 = 成功
L2CAP_ConfigReq

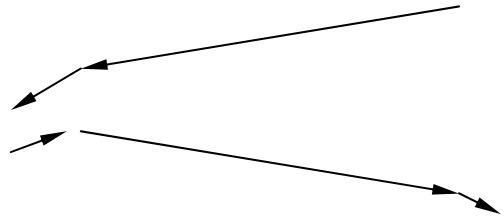
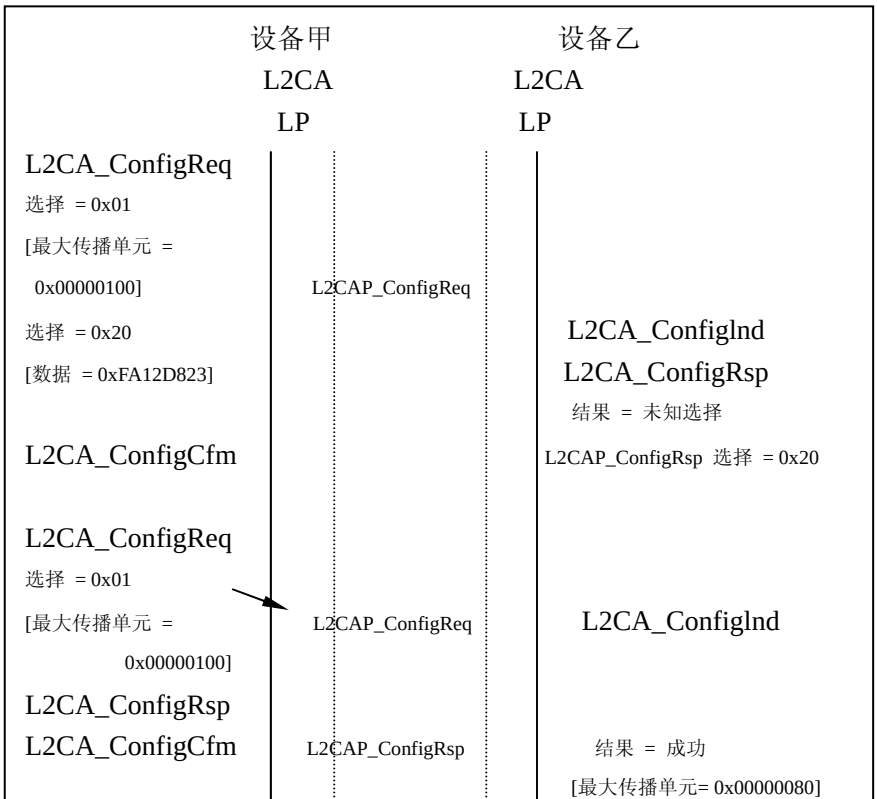


图4.34 基本MTU的交换

下图解释了在一台设备比另一设备支持更多选项的情况下,两设备如何实现互操作。设备A是升级版本。为了实现链路层安全,它采用了一个假设已定义的选项类型0x20。设备B使用配置应答分组拒绝该指令,该配置应答分组含有通知设备A'未知参数',而设备A并不能理解选项0x20。然后,设备A将重发一个省略选项0x20的请求。设备B注意到它并不需要那么大的MTU,从而接受该请求。但设备B将在通知设备B的应答中包括该MTU,而且设备B不会在信道中发送大于0x80字节和含有效载荷的L2CAP分组。一收到应答,设备A就减少分配的缓冲区以暂停呼入通信。



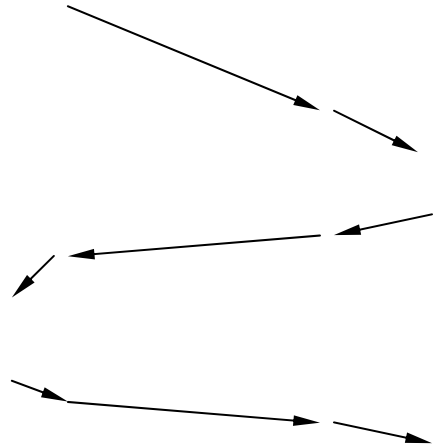
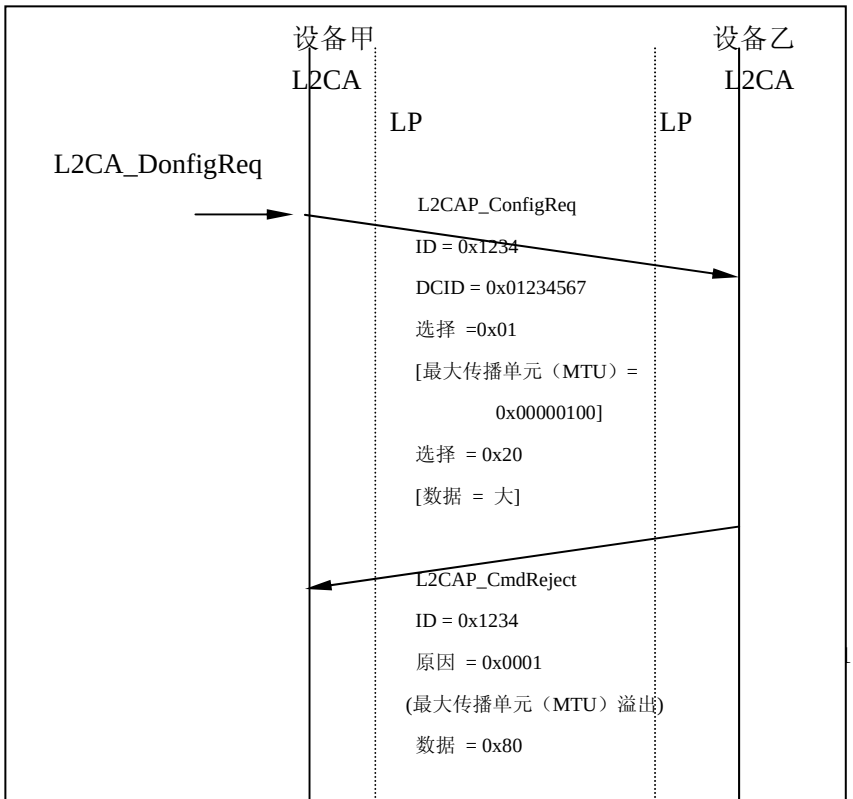


图4.35 处理未知选项

下图说明了一个未成功的配置请求。本例中描述了两个问题。第一问题是在 L2CAP分组中的配置请求由于长度太大,而不能为远程设备接受。而远程设备将使用指令拒绝报文将该问题通知发送方。这时，设备A将用两个更小的L2CAP_ConfigReq报文重发配置选项。

第二个问题是尝试用非法CID设置信道。例如,设备B可能在该非法CID上保持一条开放连接，本例中该非法CID为0x01234567)。



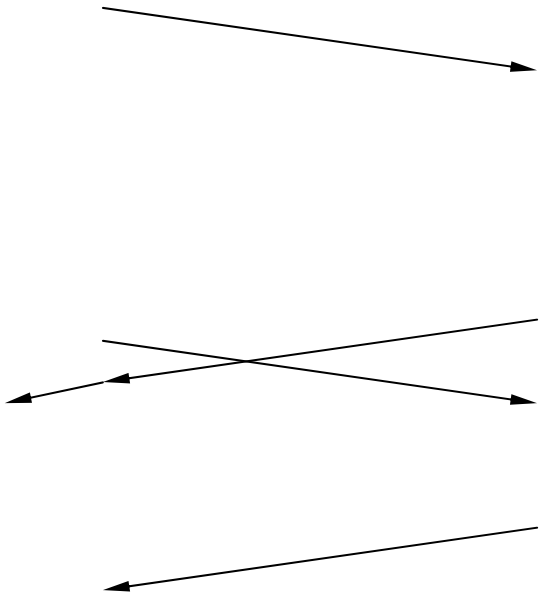


图4.36 不成功的配置请求

执行准则

本节包含一些执行准则。这些准则也就是全部的兼容性测试。但它们只是如何解决困难的一些简单建议。

RTX 定时器

应用不能在L2CAP连接请求分组上启动该定时器，除非已建立物理链路。否则,基带呼叫机制将不断增加请求成本，该成本将超出最小超时值时的成本。如果执行要通过某种形式的安全校验，最好在查询安全管理器之前将连接中间应答发回，该安全管理器可以执行基带身份验证指令。如果安全检验需要用户交互，连接将等待用户输入PIN。

映射到LM和L2CAP应用的QOS

通信速率

链路管理器（LM）应当保证采用该速率从传输缓冲区中删除数据。LM应保证轮询间隔足够快,以能够支持该速率。如果分组类型发生变化，也应调整轮询间隔。如果缓冲区溢出，并且服务类型已得到授权，那么就应报告违反QoS的情况。如果服务类型是最大化的，并且通信速率非零，那么也应报告违反QoS的情况。

假设给定通信速率为0xFFFFFFFF，并且服务类型已得到授权,那么LM应拒绝来自远程设备的其它连接，而且暂停所有周期性扫描。

最大令牌长度:

L2CAP应用应确保达到该长度要求的缓冲区已分配给信道。如果没有可用缓冲区，而且服务类型已得到授权,那么应拒绝该请求。如果无可用的合适大小的缓冲区,并且服务类型为最大化,那么应给信道分配最大可用缓冲区。

带宽峰值:

如果最大令牌长度缓冲区溢出，应导致QoS出错。

延迟:

LM应保证轮询间隔至少大于等于该值。如果轮询间隔小于该值，则应使用更小值。

如果不支持该轮询间隔，则应该引起QoS出错。

延迟区间:

由于在没有要求LM解析L2CAP分组的长度段的情况下,在L2CAP分组延迟和必要轮询之间没有明确进行映射，LM可以忽略该值。

冲突表

表4.104 第二个连接超时请求的结果

当前值	请求的值	结果
X	X	X
X	Y	如果（X<Y）那么X，否则Y

表4.105 第二个刷新超时请求的结果

当前值	请求的值	结果
N	0	N
N	N	N

N	M! = N	拒绝

第5章 服务搜索协议（SDP）

本规范对用于查找蓝牙设备提供服务的协议进行定义。

目录

附录二： SDP事务实例

1 介绍

1.1 总论

服务搜索协议(SDP)提供了应用发现可用服务,以及确定可用服务特点的方法。

1.2 动机

根据移动设备的临频动态改变服务的蓝牙服务搜索，与传统的基于网络的服务搜索具有相当大的不同。本规范定义的服务搜索协议用于描述蓝牙环境的唯一特征。参见附录A:背景信息可得到更多的关于该主题的信息。

1.3 必要条件

下列性能被认定为服务搜索协议 1.0 版的必要条件。

1. SDP 将为客户提供搜寻所需服务的能力。
2. SDP 允许基于服务类型搜索服务。
3. SDP 可以执行服务浏览，而不用预先知道服务特征。
4. SDP 将提供一种方法来搜索新的服务。当设备进入客户设备邻频或处于客户邻频的设备的新服务可用时,这些服务才可用。
5. SDP将提供一种机制来确定在设备离开客户设备邻频时,或者当处于客户设备邻频的设备上的新服务不可用时, 设备在何时变为不可用。
6. SDP将提供对服务、服务类型和属性的唯一标识。
7. SDP应允许在一方设备上的客户在另一方设备上搜索服务,而不用查询第三方设备。
8. SDP 应适于在不太复杂的设备上使用。
9. SDP应提供一种可增量搜索设备所提供服务信息的机制。这样将可以减少必须交换的数据量， 以便确定客户是否不需要某一特定服务。
10. SDP应可通过中介代理支持服务搜索信息缓存，以提高搜索进程的速度或效率。
11. SDP应可独立传输。
12. SDP将在把L2CAP作为其传输协议时工作。
13. SDP应允许搜索和使用能够提供对其它服务搜索协议访问的服务。
14. SDP应支持和定义新的服务，而不需要向中心授权机构申请注册。

1.4 非必要条件和延时必要条件

蓝牙 SIG 认为下列能力与服务搜索有关。这些项目并未在SDP1.0 版

本中给出。但是,有一些可能将在将来规范修订本中给出。

1. SDP1.0不能存取服务。它仅仅提供对服务有关信息的访问。
2. SDP1.0不提供服务中介。
3. SDP1.0不提供对服务参数的协商。
4. SDP1.0不提供对服务使用的计费。
5. SDP1.0不向客户提供控制或改变服务操作的方法。
6. 在服务或服务有关信息不可用时，SDP 1.0不提供事件通知。
7. 当服务属性被修改时，SDP 1.0 不提供事件通知。
8. 本规范没有定义SDP应用编程接口。
9. SDP1.0不提供服务汇总、服务注册等服务代理功能。

1.5 协定

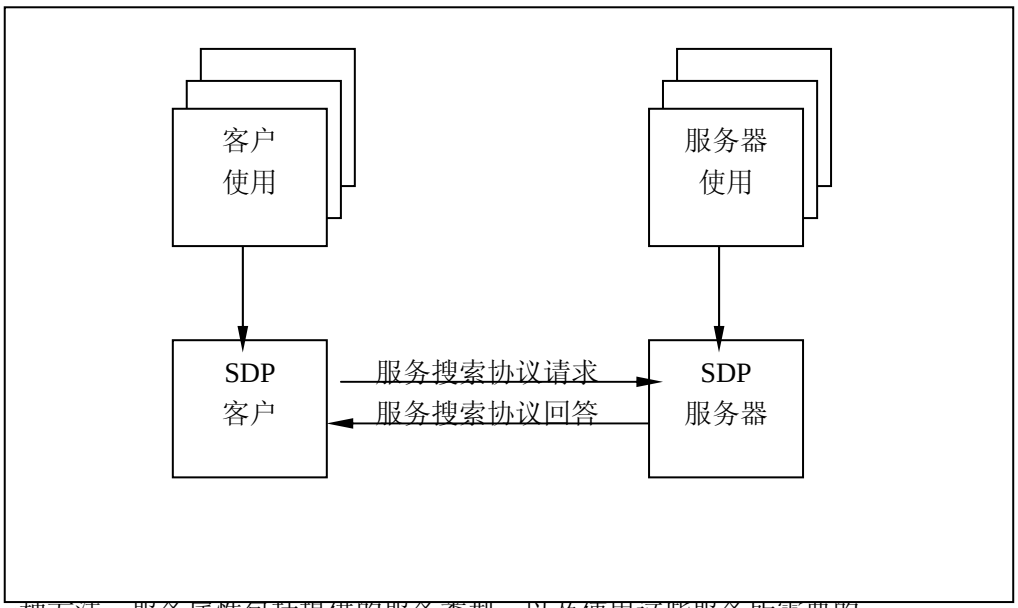
1.5.1 比特与字节排序规定

当在一个字节里包含多比特域时，并且多比特域在本规范示意图中表示出来时，高位在左，低位在右。

多字节域则是高位字节在左边,而低位字节在右。多字节域应以网络字节顺序传递（参见 ‘传输字节顺序’）。

2 一般观察

2.1 客户服务器交互



的一种方法。服务属性包括提供的服务类型，以及使用这些服务所需要的机制或协议。

就服务搜索协议（SDP）而言，图2.1 所示配置可以简化为图2.2 所示配置。

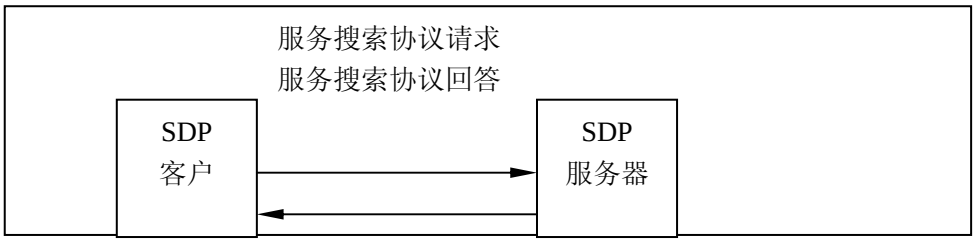


图 5.2

服务搜索协议(SDP) 包括SDP 服务器与SDP 客户之间的通信。服务器保持一张描述服务器有关服务特征的服务记录表。每一服务记录都包含一项服务信息。客户可以通过发送SDP请求,从由SDP服务器维护的服务记录中检索信息。

如果客户或与客户有关的应用决定使用一种服务,它就必须打开一个到服务提供方的连接。SDP 提供一种搜索服务及其属性(包括相关服务访问协议)的机制,但它不提供使用这些服务的机制(如发送服务访问协议)。

蓝牙设备与SDP服务器应一一对应, 且存在一个最大的对应数。(如果一台蓝牙设备仅仅充当一个客户, 那它就不需要SDP服务器。) 一台蓝牙设备既可以作为一个 SDP 服务器也可以同时作为一个 SDP 客户。如果一台设备的多个应用程序同时提供服务,那么可以将SDP服务器作为处理服务相关信息请求的服务提供方。

同样,多个客户应用也可以作为一个SDP客户, 代表客户应用去查询服务器。

对于SDP客户可用的SDP服务器组,可以基于服务器到客户的邻频实现动态改变。当服务器可用时,应通过SDP以外的方法通知潜在客户, 以使客户能够利用SDP查询服务器相关服务。但是,当一个服务器离开邻频或者由于某些原因而不可用时,将无法通过服务搜索协议显式通知客户。然而,客户可以使用SDP轮询服务器。如果服务器长时间无应答,客户就可推断出服务器不可用。

其它有关应用与SDP交互的信息将在蓝牙服务搜索框架文本中进行描述。

2.2 服务记录

服务是任何一个能够提供信息、执行动作、或代表另一实体控制资源的实体。服务可以以软件、硬件、或硬软件混合的形式执行。

由SDP服务器所维护服务的所有信息都包含于一条服务记录中。该服务记录全部由一张服务属性表组成。

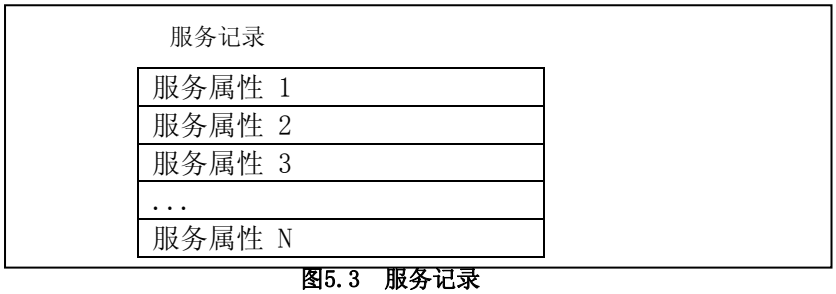


图5.3 服务记录

服务记录句柄是一个专门用于唯一标识SDP服务器内每一服务记录的32位的值。总的来说,必须注意的是,每个句柄在每个 SDP 服务器内都是唯一的。如果SDP服务器S1和SDP服务器S2同时包含同一服务记录(代表同一服务),用于引用该相同服务记录的服务记录句柄则是完全独立的。如用于引用S1设备上服务的句柄指向S2，那么该句柄并无任何含义。

当向SDP服务器增加或删除服务记录时，服务搜索协议并不提供通知客户的机制。当与 服务器建立一条L2CAP (逻辑链路控制与适配协议)连接时,从服务器获取的服务记录句柄将保持有效,除非它所代表的服务记录被删除。如果某一服务被从服务器中删除，在从L2CAP 连接获取服务记录句柄期间，又采用该服务记录句柄向服务器提出进一步请求，将会引起表示该服务记录句柄非法的出错应答。SDP服务器应确保在保持L2CAP连接期间，不会重用任何服务记录句柄）记录句柄。注意：当 ServiceDatabaseState 属性保持不变时，服务记录句柄在连续 L2CAP 连接中也仍然保持有效（参见属性定义里的ServiceRecordState和 ServiceDatabaseState 属性)。

存在一个适用于所有SDP服务器的服务记录处理句柄。该服务记录句柄值为0x00000000，并且该句柄也就是代表SDP服务器的服务记录的句柄。该服务记录句柄包含SDP服务器属性及其支持的协议。例如,它的属性之一是服务器支持的SDP 协议版本列表。服务记录句柄值0x00000001-0x0000FFFF保留使用。

2.3 服务属性

服务属性用于描述某一服务的一个特征。服务属性的实例如下：

ServiceClassIDList	用于标识由服务记录代表的服务类型。也就是说，该服务属性也就是一个类列表，该服务仅是某一类的一个实例。
ServiceID	唯一标识某一服务实例
ProtocolDescriptorList	表示可用于使用某一服务的协议栈
ProviderName	提供某一服务的个人或组织的文本名

IconURL	表示被某一图标引用的URL，该图标可用于代表某一服务L
ServiceName	含有服务名称的文本串
ServiceDescription	描述服务的文本串

所有服务记录通用属性定义，可参见通用属性定义，服务供应方也可以定义其自己的服务属性。

服务属性由两个部分组成:属性 ID 和属性值。

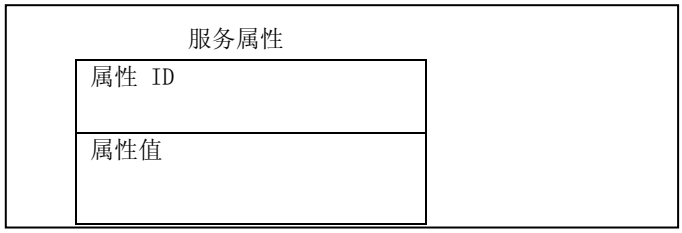


图 5.4 服务属性

2.4 属性 ID

属性ID是16位无精度整数，可用于在服务记录中将不同服务属性区分开来。属性ID也能够区分与属性值关联的不同语义。

服务类型定义是指服务类的属性ID,并为关联于每一属性ID的属性值给出一定含义。

例如,假设服务类C指出：与属性ID12345关联的属性值是一个包含服务创建日期的文本串。

并且，服务A是该服务类C的一个实例。如果服务A的服务记录包含一个属性ID为12345的服务属性，那么该属性值必然就是一个包含服务A 创建日期的文本串。然而,非服务类C实例的服务可给ID 12345分配一个不同含义。

所有属于某一给定服务类将为每一特定属性ID 分配同样的含义（参见服务类型）。

在服务搜索协议里,属性 ID通常代表一个数据元。参见第3节数据表示。

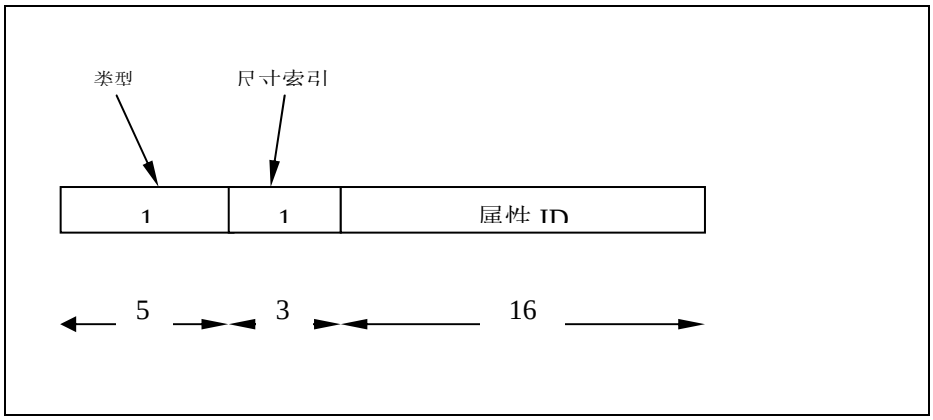


图5.5

2.5 属性值

属性值也就是可变长度域，其含义由与其关联的属性ID和包含该属性ID的服务的服务类决定。在服务搜索协议中，属性值代表一个数据元。通常,任一类型数据元都可以允许作为属性值,并受到服务类型定义的限制。该服务类型定义将属性ID指定给该属性，并为该属性值指定一个含义。参见服务属性定义的属性值实例。

2.6 服务类

每一服务都是服务类的一个实例。服务类定义提供对所有包含于服务记录中属性的定义，而这些服务记录就代表一个类实例。每一属性定义将给出该属性ID的数字值、该属性值的用法及其格式。服务记录包含服务类的专用属性，以及用于所有服务的通用属性。

每一服务类将指定一个唯一标识符。该服务类标识符包含于ServiceClassIDList属性的属性值，并表示为 UUID。由于服务记录中的某些属性的格式和含义依赖于服务记录的服务类,因此ServiceClassIDList属性非常重要。在使用任一类指定属性之前，应检查或验证它们的值。由于服务记录的所有属性必须遵循所有的服务类，包含于ServiceClassIDList属性中的服务类标识符也与此有关。特别要说明的是,每一服务类都是另外一类的子类，该父类的标识符包含在ServiceClassIDList列表中。服务子类定义与其父类不同，子类中包含该其它子类特定的属性定义。ServiceClassIDList 属性中的服务类标识符，按照从底层类到高层类的顺序一一列出。

在定义本身是另一服务类子类的新服务类时，该新类将保留父类定义的所有属性。同时，也将定义专用于新服务类的其它属性。换句话说，向已有服务类的某些实例添加新属性的机制将创建一个新的服务类，该服务类是已有服务类的子类。

2.6.1 打印机服务类举例

双工彩色打印机可遵循四个服务类定义，并具有一个含UUID的ServiceClassIDList，包括以下服务类ServiceClasses ：

DuplexColorPostscriptPrinterServiceClassID,

ColorPostscriptPrinterServiceClassID,

PostscriptPrinterServiceClassID,

PrinterServiceClassID

注意：本例仅是一个描述性例子，而并不是实际的打印机类层次结构。

2.7 服务搜索

一旦SDP客户具有服务记录句柄，它将很容易地请求特定属性值，但该客户如何才能获取用于服务记录的服务记录句柄呢？服务搜索事务允许客户基于服务记录包含的属性值，搜索特定服务记录的服务记录句柄。

本协议并未提供基于强制值的服务记录搜索能力。相反,只提供了搜索值为通用定位符UUID（注1）的属性。可用于搜索服务的重要服务属性表示为UUID。

注1：UUID 的格式由国际标准化组织在 ISO/ IEC 11578 里定义的:1996年。

2.7.1 UUID

UUID是经授权可在所有时空中保持唯一的通用定位符。UUID可以分布的方式独立创建，而且不需要指定UUID的中心注册机构。UUID值长度为128位。

为了减少存储压力，并便于128 位UUID 值的转换,UUID值域已经为了常用和注册的目的进行预先分配。在该已分配域的第一个UUID作为蓝牙基UUID，具有来自蓝牙号码分配文件的值00000000-0000-1000-7007-00805F9B34FB。在该已分配域的UUID值都具有16位或32位的别名。这些别名常被称为16位或32位UUID。但每一别名实际上都代表一个128 位UUID 。

可以通过一个简单的数学运算计算16位或32位UUID的全部128位值。

128位值 = 16位值 * 2^{96} + 蓝牙基UUID

128位值 = 32 位值 * 2^{96} + 蓝牙基UUID

通过对16位值进行零扩展，将16位UUID转换成为32位UUID格式。另外一个转换方法是将16位值加到所有位都为零的32位UUID 。

注 ：可以直接对两个16位UUID或32位UUID或128位UUID进行比较,如果要对不同大小的UUID 进行比较，短UUID必须在比较前转换成为长UUID格式。

2.7.2 服务搜索模式

服务搜索模式是一个用于定位匹配服务记录的UUID表。如果服务搜索模式中的UUID包含于任一服务记录属性值，服务搜索模式应可匹配一条服务记录。UUID不必包含于任何特定属性，也不必在服务记录中以任何特定顺序排序。如果服务搜索模式包含的UUID在服务记录属性值中， 构成了UUID子集，服务搜索模式将匹配一条服务记录。只有在服务搜索模式包含不止一个包含于服务记录属性值的UUID时，服务搜索模式才不与服务记录匹配。同时注意：一个合法服务搜索模式必须含有至少一个UUID 。

2.8 服务浏览

通常，一个客户基于某些服务特性（由UUID表示）搜索服务。然而有时候，也可以搜索由SDP服务器服务记录进行描述的服务类型，这些服务器服务记录不含服务预定义信息。该寻找服务的过程叫做浏览。在SDP中，该浏览服务机制以各服务类共享属性为基础。该属性称为 BrowseGroupList 属性。该属性值包含一张UUID表。每一UUID采用出于浏览目的而关联的服务代表一个浏览组。

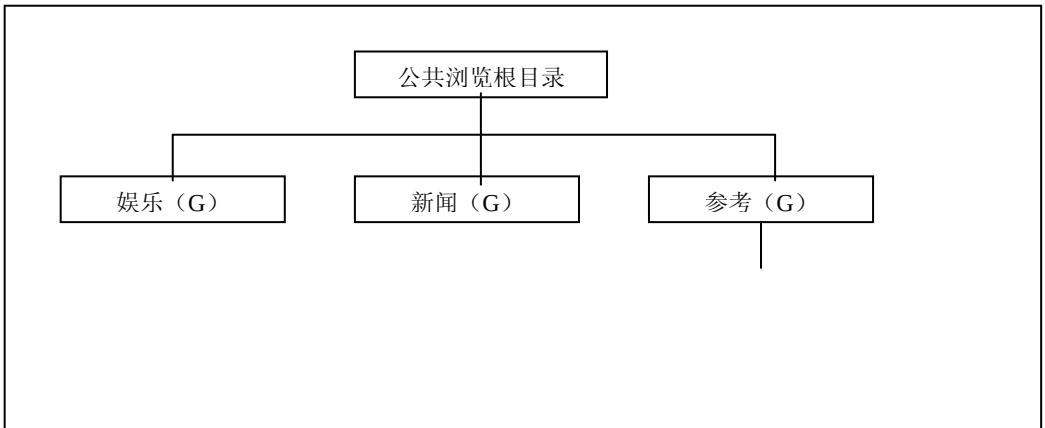
当客户需要浏览SDP服务器的服务时,它将创建包含UUID的服务搜索模式，而该UUID表示根浏览组。所有可以在顶层浏览的服务，可以通过把根浏览组的UUID作为BrowseGroupList属性值，从而构成根浏览组。

通常,如果SDP 服务器没有多少服务，它所有的服务将被放在根浏览组里。然而,由SDP服务器提供的服务，可以通过在根浏览组的下层定义其它浏览组，以浏览组层次结构形式组织起来。这些下层浏览组都由服务记录，采用BrowseGroupDescriptor 服务类进行描述。

浏览组描述符服务记录可以通过其组ID属性定义新浏览组。为了获取包含于可浏览的新定义浏览组的服务，必须可以对新浏览组的浏览组描述符服务记录进行浏览。由浏览组描述符服务记录提供的可浏览服务的结构层次，允许对SDP服务器提供的服务进行增量浏览。并且，在服务包含许多服务记录时，该服务层次非常有用。

2.8.1 服务浏览层次举例

这是一个描述浏览组描述符用法的虚拟服务浏览层次结构。浏览组描述符服务记录标识为(G)，其它服务记录标识为（S)。



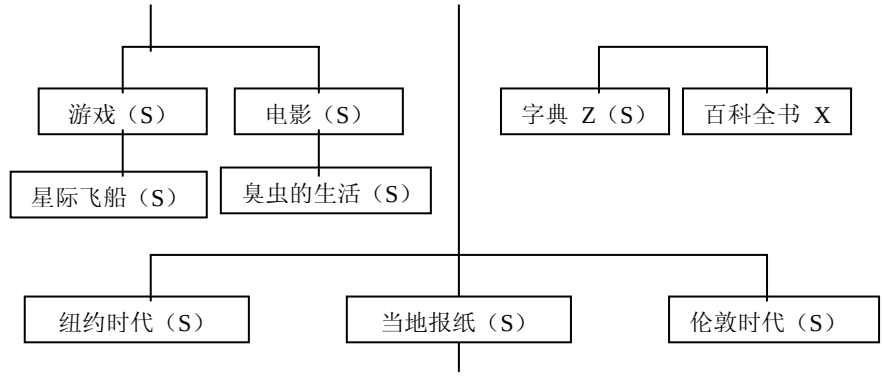


图5.6

该表列出了执行浏览层次所需的服务记录和服务属性。

表5.1

服务名	服务类别	属性名	属性值
娱乐	BrowseGroupDescriptor	BrowseGroupList	PublicBrowseRoot
		GroupID	EntertainmentID
新闻	BrowseGroupDescriptor	BrowseGroupList	PulicBrowseRoot
		GroupID	NewsID
参考	BrowseGroupDescriptor	BrowseGroupList	PulicBrowseRoot
		GroupID	ReferenceID
游戏	BrowseGroupDescriptor	BrowseGroupList	EntertainmentID
		GroupID	GamesID
电影	BrowseGroupDescriptor	BrowseGroupList	EntertainmentID
		GroupID	MoviesID
星际飞船	视频游戏类 ID	BrowseGroupList	GamesID
臭虫的生活	电影类 ID	BrowseGroupList	MoviesID
字典 Z	字典类 ID	BrowseGroupList	ReferenceID
百科全书 X	百科全书类 ID	BrowseGroupList	ReferenceID
纽约时代	报纸类 ID	BrowseGroupList	NewspaperID
伦敦时代	报纸类 ID	BrowseGroupList	NewspaperID
地方报纸	报纸类 ID	BrowseGroupList	NewspaperID

3 数据表示

属性值可以包含具有强制复杂性的各种类型的信息，从而使得能够在不同服务类和环境中使用属性表。

SDP定义了一个描述包含于属性值中数据的简单机制。其基本结构单元为数据元。

3.1 数据元

一个数据元表示一个打印数据。它由两个段组成:报文头段和数据段。报文头段又由两部分组成:一个类型描述符和一个尺寸描述符。该数据是一个字节序列，其长度在尺寸描述符中定义（参见数据尺寸描述符），其含义由类型描述符（部分）定义。

3.2 数据元素类型描述符

数据元类型由5位长的类型描述符代表。数据元头包含在数据元报文头首字节的最高5位中。下列类型已被定义。

表5.2

类型描述符值	有效尺寸 描述符值	类型描述
0	0	Nil, the null type
1	0,1,2,3,4	无精度整数
2	0,1,2,3,4	两位整数
3	1,2,4	UUID, 通用唯一标识符
4	5,6,7	文本串
5	0	逻辑
6	5,6,7	数据元序列，数据段是一个数据元序列的数据元。
7	5,6,7	可选数据元，数据段是一个数据元序列的数据元，从顺序中选出数据成分
8	5,6,7	URL, 统一资源定位
9-31		保留

3.3 数据元尺寸描述符

数据元尺寸描述符由一个后面紧跟0 、8 、16 、或 32 位的3位尺寸索引字表示。该尺寸索引字包含于数据元头首字节的最低位中。该尺寸索引编码如下。

表 5.3

尺寸索引	额外的字节	数据大小
0	0	1 个八位字节。除非数据成分类为零，那么数据尺寸就为 0 个字节
1	0	2 个字节
2	0	4个字节
3	0	8个字节
4	0	16个字节
5	8	数据大小包含在另外8位中，这8位为无精度整数
6	16	数据大小包含在另外16位中，这16位为无精度整数
7	32	数据大小包含在另外32位中，这32位为无精度整数

3.4 数据元举例

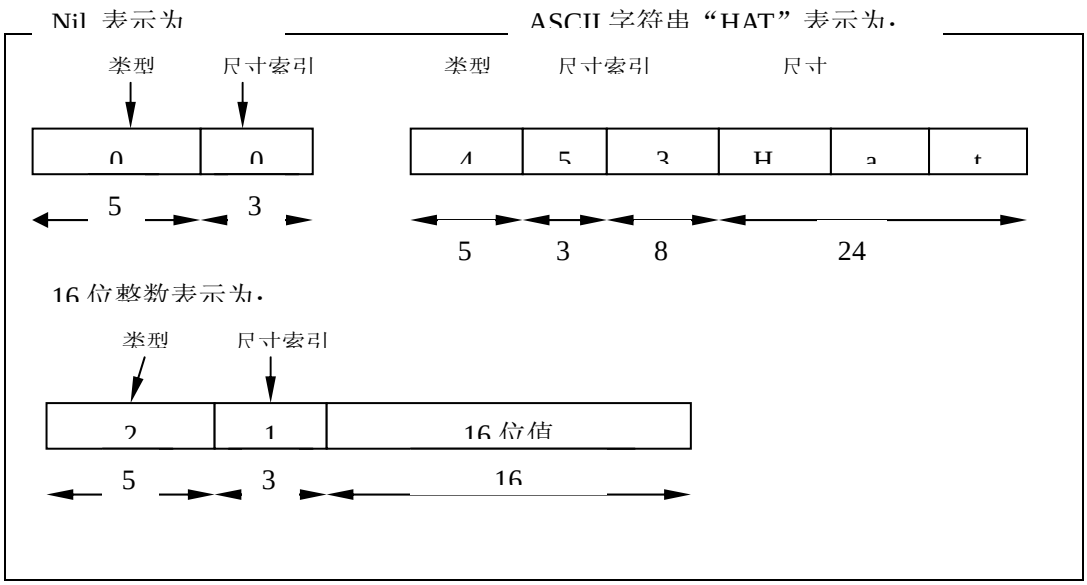


图5.7

4．协议说明

SDP是一个对通信要求最少的简单协议。它可工作于可靠分组传输模式(如果客户实现超时并且可在有必要时进行重复请求，那么也可以工作于不可靠分组传输模式)。

SDP使用一个请求/应答模型。在模型中，每一处理事务由请求协议数据单位(PDU)和应答协议数据单位(PDU)组成。然而,请求和应答实际上都可以不按次序进行传输。

在服务搜索协议使用蓝牙L2CAP传输协议的特定情况下，可以在一个L2CAP分组中传输多个SDP PDU，在每一连接上只能发送一个这样的L2CAP给指定SDP服务器。限制SDP发送确认分组成为流控制形式的一种。

附录B——SDP处理事务实例可对理解协议实例有所帮助。

4.1 字节传输顺序

服务搜索协议可按标准网络字节顺序（BIG EDIAN）传输多字节域，其中高位字节先于低位字节传输。

4.2 协议数据单元格式

每一SDP协议数据单元(PDU)都由PDU头和PDU指定参数组成。报文头包含三个域:协议数据单元ID、事务ID和 参数长度ParameterLength 。PDU头域随后描述。参数包括一个后续状态参数,下面给予描述；每一PDU类型的指定参数在后面的PDU描述中分别说明。

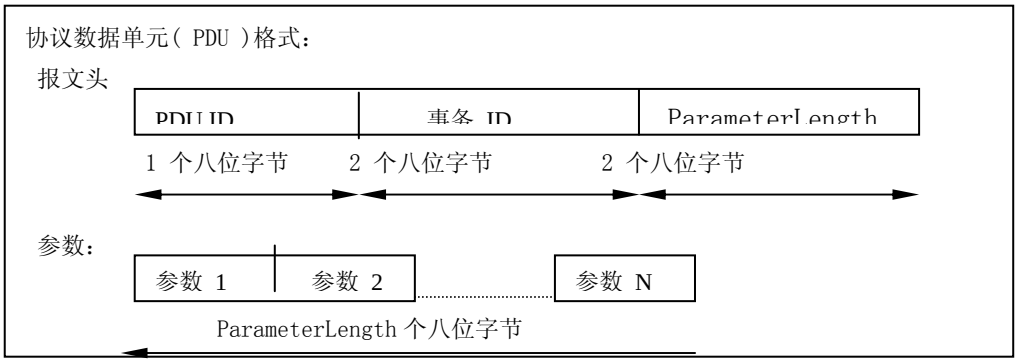


图 5.8

PDU ID

大小: 1字节

表5.4

值	参数说明
N	PDU ID 域标识PDU 类型, 即其定义与指定参数
0x00	保留
0x01	SDP_ErrorResponse
0x02	SDP_ServiceSearchRequest
0x03	SDP_ServiceSearchResponse
0x04	SDP_ServiceAttributeRequest
0x05	SDP_ServiceAttributeResponse
0x06	SDP_ServiceSearchAttributeRequest
0x07	SDP_ServiceSearchAttributeResponse
0x07-0xFF	保留

TransactionID: 大

小: 2字节

表5.5

值	参数说明
N	TransactionID域唯一标识请求PDU, 并被用于将应答PDU与请求PDU相匹配。SDP客户可给请求TransactionID 指定任意值, 只要该值与所有发出请求不同。应答 PDU 的TransactionID 要求与应答的请求PDU值一致。

ParameterLength: 大

小：2字节

表5.6

值	参数说明
N	ParameterLength 域指定包含于PDU的所有参数，单位为字节

4.3 局部应答和延续状态

一些SDP请求可以要求比单个应答PDU更大的应答分组。这时，SDP服务器将生成含有后续状态参数的局部应答。客户可以通过在以后的请求中提供后续状态参数，以检索完全应答的下一部分。延续状态参数是可变长度域，其首字节中包含后续信息的附加字节数目。在SDP服务器中并没有统一后续信息格式标准。每个延续状态参数只有对产生它的 SDP 服务器才有意义。

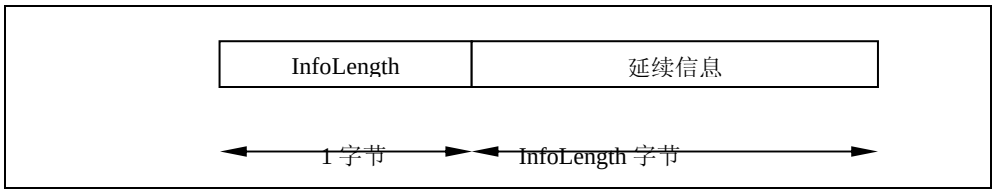


图5.9 后续状态格式

在客户收到局部应答及其后续状态参数后,它将重发最初的请求(含新事务ID)，并在发往服务器的新请求中包含后续状态参数，以表示它想获得最初应答的其余部分。InfoLength域中允许的最大值为16 （ 0x10 ）。

注意当SDP服务器生成局部应答时，SDP服务器可以在任意强制边界上分割应答。SDP服务器根据应答内容选择进行分割的边界，但并不是必须要这样做。

4.4 出错处理

每一事务都由一个请求和一个应答PDU组成。通常,每种请求PDU类型都对应于一种应答PDU类型。但是,如果服务器确认请求格式不正确或由于某种原因，服务器不能采用合适的PDU类型进行应答时,该服务器将采用SDP_ErrorResponse协议数据单元应答。

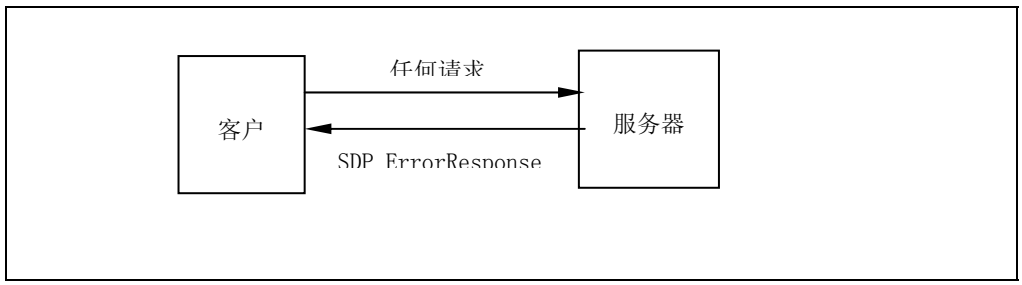


图 5.10

4.3.1 SDP_ErrorResponse

表5.7

PDU 类型	PDU ID	参数
SDP_ErrorResponse	0x01	ErrorCode, ErrorInfo

SDP服务器生成本PDU类型，以对未正确格式化的请求PDU进行应答，或者在SDP服务器由于某些原因而不能生成合适的应答PDU时进行应答。

PDU参数：

ErrorCode: 类型：2 个八位字节

表5.8

值	参数说明
N	ErrorCode标识SDP_ErrorResponse PDU 生成的原因
0x0000	保留
0x0001	无效/不支持的SDP版本
0x0002	无效的服务记录句柄
0x0003	无效的请求语法
0x0004	无效的PDU尺寸
0x0005	无效的后续状态
0x0006	满足请求的资源不足
0x0007-0xFFFF	保留值

Errorinfo: Size: N Bytes

表5.9

值	参数说明
Error-specific	ErrorInfo是根据ErrorCode而定的参数。其含义取决于Errorcode参数。当前定义的 ErrorCode 值不能指定ErrorInfo域的格式。

4.5 服务搜索处理

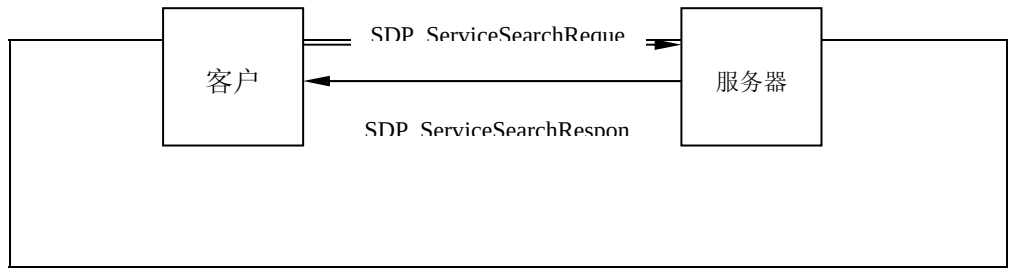


图 5.11

4.5.1 SDP_ServiceSearchRequest PDU

表5.10

PDU 类型	PDU ID	参数
SDP_ServiceSearchRequest	0x02	ServiceSearchPattern, MaximumServiceRecordCount,ContinuationState

描述：

SDP客户生成一个SDP_ServiceSearchRequest以定位匹配给定服务搜索模式的服务记录，该服务搜索模式是该PDU的首个参数。一收到该请求，SDP服务器将检查其服务记录数据库，并将返回包含服务记录句柄的SDP_ServiceSearchResponse，该服务记录匹配于给定服务搜索模式。

注意：并未提供任何可以获取所有服务记录信息的机制。但是,可以参见服务浏览部分内容，可以找到，在不了解服务的情况下，允许对非指定服务进行浏览的机制。

PDU参数：

ServiceSearchPattern: 尺寸：多样化

表5.11

值	参数说明
数据元序列	ServiceSearchPattern 是一个数据元序列，在该序列中，每一个数据元都是一个UUID。该序列必须包含至少一个UUID。该序列中最大的UUID值为12*。服务搜索模式由UUIDs表构成。

*.在服务搜索的范围和搜索请求协议数据单元（PDU）的大小之间，值12为折衷值。在服务搜索模式中使用的UUID不得多于 12 个。

MaximumServiceRecordCount: 尺寸：2 个八位字节

表5.12

值	参数说明
N	MaximumServiceRecordCount是一个16位计数器，该计数器指定用于应答该请求的返回服务记录句柄的最大数。SDP服务器不应返回比此值更多的句柄。如果有多于N的服务记录与请求匹配，SDP服务器需要确定采用哪些匹配的服务记录句柄应答。 范围：0x0001-0Xffff

ContinuationState: 尺寸：1 至 17 个八位

字节

表5.13

值	参数说明
连续状态	ContinuationState由一个8位计数器N、连续状态信息字节数，以及服务器发回的N 个字节连续状态信息构成。N必须小于或等于16。如果请求中不含连续状态参数，N设置为 0。

4.5.2 SDP_ServiceSearchResponse PDU

表5.14

PDU	PDU ID	参数
SDP_ServiceSearchResponse	0x03	TotalServiceRecordCount CurrentServiceRecordCount, ServiceRecordHandleList, ContinuationState

描述：

在SDP服务器器收到一有效服务搜索请求SDP_ServiceSearchRequest时，将生成一个服务请求应答SDP_ServiceSearchResponse。该应答包含与该请求服务搜索模式相匹配的服务记录的服务记录句柄表。值得注意的是，如果生成局部应答，则它必须包含整数个完整的服务记录句柄；而且不必将服务记录句柄值在多个PDU中分割开来。

协议数据单元（PDU）参数:

TotalServiceRecordCount: 尺寸：2 个八位字节

表5.15

值	参数说明
N	TotalServiceRecordCount为一包含服务记录数目的整数,，该服务记录须与请求的服务搜索模式匹配。如果无服务记录与请求的服务搜索模式匹配，则参数设置为0。N不得大于SDP_ServiceSearchRequest的最大服务记录数MaximumServiceRecordCount。当使用多个局部应答时，每一局部应答都应包含本参数的相同值。

CurrentServiceRecordCount: 尺寸：2 个八位字节

表5.16

值	参数说明
N	CurrentServiceRecordCount 是一个整数，用来指示包含下一个参数的服务记录句柄的数。如果无服务记录与请求的服务搜索模式匹配，这个参数就设置为0。N 决不能大于在当前应答的CurrentServiceRecordCount 的值。

	范围：0x0000-0xFFFF

ServiceRecordHandleList: 尺 寸 ：
(CurrentServiceRecordCount*4) 个八位字节

表5.17

值	参数说明
32位句柄表	ServiceRecordHandleList 包含一个服务记录句柄表。句柄数已在CurrentServiceRecordCount里列出。表中的每一句柄都指的是一个服务记录，该记录与请求的服务搜索模式匹配。注意该服务记录句柄表不包括数据元格式，不包括头域，而只包括32位服务记录句柄。

ContinuationState: 尺寸： 1 个至 17 个八位字节值

表5.18

值	参数说明
连续状态	ContinuationState 由8位计数器N、连续状态信息字节数，以及连续信息的 N 个字节构成。如果结束当前应答，本参数由为0的单个字节构成。如果PDU包括局部应答，ContinuationState参数就包括在后续请求中，以检索应答的其余部分。

4.6 服务属性事务

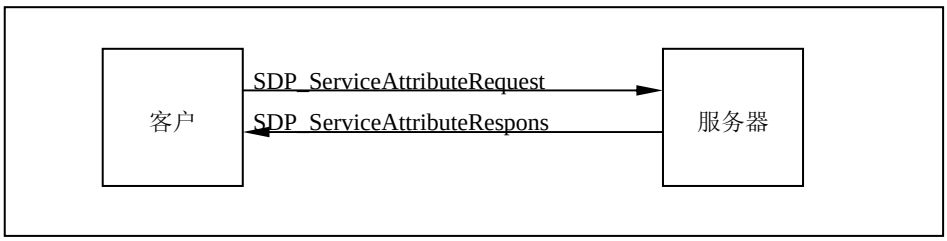


图5.12

图 4.5:

4.5.1 SDP_ServiceAttributeRequest PDU

表5.19

PDU 类型	PDU ID	参数
SDP_ServiceAttributeRequest	0x04	服务记录句柄ServiceRecordHandle,

		最大属性字节数MaximumAttributeByteCount, 属性表AttributeIDList, 后续状态ContinuationState

描述：

SDP客户将生成一个SDP_ServiceAttributeRequest协议数据单元，以从一指定服务记录中检索指定属性值，并提供所需服务的服务记录句柄和从服务记录中检索的属性ID表作为参数。

命令参数：

ServiceRecordHandle: 尺寸：4 个八位字节

表5.20

值	参数说明
32 位句柄	ServiceRecordHandle 参数根据检索到的属性值指明服务记录，可以通过前面的 SDP_ServiceSearch 事务中获取句柄。

MaximumAttributeByteCount: 尺寸：2 个八位字节

表5.21

值	参数说明
N	MaximumAttributeByteCount给出将在响应该请求的应答中返回的属性数据的最大字节数。SDP服务器不得返回多于N个字节的应答。如果被请求属性多于N个字节，则由SDP服务器确定如何截断该表。

AttributeIDList: Size: Varies 尺寸：多变化

表5.22

值	参数说明
数据元序列	AttributeIDList为一数据元序列。其中，该表中每一数据元要么是属性 ID 要么是一个属性ID的取值范围。每一属性ID都编码为16位低精度整数数据元。每一属性取值范围都编码为32位低精度整数数据元，其中高段16位定为属性ID的起始段，低段16位定为属性ID的结束段。AttributeIDList的属性ID必须以递增的顺序列表，且属性ID值不得重复。注意所有的被请求属性都指定在0x0000-0xFFFF 范围内。

ContinuationState: 尺寸:1 至 17 个八位字节

表5.23

值	参数说明
连续状态	ContinuationState 由 8 位计数的连续状态信息的字节数构成，后面是连续状态信息的 N 个字节，这个字节是从以前应答的服务器发回来。N 必须小于或等于 16。如果在请求中无连续状态，N 就设置为 0。

4.5.2 SDP_ServiceAttributeResponse PDU

表5.24

PDU 类型	PDU ID	参数
SDP_ServiceAttributeResponse	0x05	属性列表字节数AttributeListByteCount, 属性列表AttributeList, 后续状态ContinuationState

描述：

在SDP服务器收到有效SDP_ServiceAttributeRequest报文时，将生成一个 SDP_ServiceAttributeResponse应答。该应答包含被请求服务记录属性列表(属性ID和属性值)。

协议数据单元（PDU）参数：

AttributeListByteCount: 尺寸：2 个八位字节

表5.25

值	参数说明
N	AttributeListByteCount的值为AttributeList参数的字节数。N不得大于在SDP_ServiceAttributeRequest 中定义的属性最大字节数MaximumAttributeByteCount。 范围：0x0002-0xFFFF

AttributeList: 尺寸：AttributeListByteCount

表5.26

值	参数说明
数据成分顺序	AttributeList为一数据元序列，包含属性ID和属性值。该序列的第一个数据元包第一个返回属性的属性ID。序列的第二个数据元包含该属性对应的属性值。后面数据元对将包含其它的属性ID和值对。AttributeList 中只包SDP_ServiceAttributeRequest指定的服务记录非空属性值及其属性ID。如果服务录的属性ID或属性值为空，则不得包含于该AttributeList中。

ContinuationState: 尺寸: 从1 到 17 个八位字节

表5.27

值	参数说明
连续状态	ContinuationState由8位计数器N、后续状态信息字节数，以及后续信息的N个字构成。如果当前应答结束，则该参数由为0的单个字节构成。如果PDU包含局部应则后续状态ContinuationState参数将包含在在后续请求中，以检索应答的其余分。

4.7 SERVICESEARCHATTRIBUTE 服务搜索属性事务

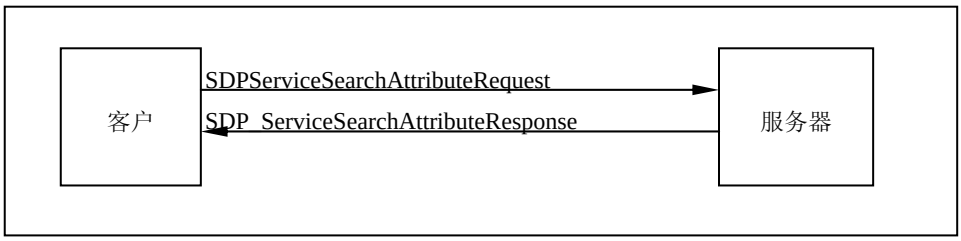


图5.13

4.7.1 SDP_ServiceSearchAttributeRequest 服务搜索属性请求PDU

表5.28

PDU 类型	PDU ID	参数
SDP_ServiceSearchAttributeRequest	0x06	服务搜索模式ServiceSearchPattern, 最大属性字节数MaximumAttributeByteCount, 属性ID列表AttributeiDList 后续状态ContinuationState

描述：

SDP_ServiceSearchAttributeRequest 事务综合 SDP_ServiceSearchRequest和 SDP_ServiceAttributeRequest 二者功能于一个请求中。作为参数，它既包含服务搜索模式，又包含一张属性表，该属性表从与服务搜索模式匹配的服务记录中检索。SDP_ServiceSearchAttributeRequest及其应答与SDP_ServiceSearch和 SDP_ServiceAttribute 两者相比，显得更复杂并且可能需要更多的字节。但是,使用 SDP_ServiceSearchAttributeRequest 可以减少总的SDP事务量,特别是当检索多条服务记录时。

要求注意的是，对于每一服务记录，每一服务记录的服务记录句柄将都包含于该服务的ServiceRecordHandle属性中，并且会与其它属性一起接受请求。

协议数据单元（PDU） 参数：

ServiceSearchPattern: 尺寸：任意

表5.29

值	参数说明
数据元序列	ServiceSearchPattern 为一数据元序列，该序列中每一数据元都是一个UUID。该序列必须包含至少一个UUID。序列中UUID的最大值为12*。UUID 表构成服务搜索模式。

*.12作为服务搜索范围和搜索请求PDU之间的折衷值。并且服务搜索模式中使用的UUID不得多于 12 个。

MaximumAttributeByteCount: 尺寸：2 个八位字节

表5.30

值	参数说明
N	MaximumAttributeByteCount指定请求应答所返回属性数据的最大字节数。SDP服务器在应答中不得返回多余N个字节的属性数据。如果被请求属性要求多于N个字节，则由SDP服务器决定如何截断该表。 范围：0x0009-0Xffff

AttributeIDList: 尺寸:不定长

表5.31

值	参数说明
数据元序列	AttributeIDList 为一数据元序列。其中，该表中数据元为属性ID，或该属性的取值范围。每一属性ID都编码为16位低精度整数数据元。每一属性范围都编码为32位低精度整数数据元，其中高段16位为属性ID起始段，低段16位为属性ID的结束段。AttributeIDList的属性ID必须以递增顺序在表中排列，且属性ID值不得重复。注意所有的属性值都应在 0x0000-0xFFFF 范围内。

ContinuationState: 尺寸：1 至 17 个八位字节

表5.32

值	参数说明
连续状态	ContinuationState 由8位计数器N、后续状态信息字节数，以及服务器前一个应答中返回的N个字节的后续状态信息组成。N必须小于或等于 16。如果该请求不包括后续状态参数，则N设置为 0。

4.7.2 SDP_ServiceSearchAttributeResponse PDU

表5.33

PDU 类型	PDU ID	参数
SDP_ServiceSearchAttributeResponse	0x07	属性列表字节数AttributelistsByteCount, 属性列表Attributelists, 后续状态ContinuationState

说明:

在SDP 服务器有效SDP_ServiceSearchAttributeRequest时将生成一个SDP_ServiceSearchAttributeResponse应答。该应答包含一张服务记录属性表(属性 ID 和属性值)，该服务记录要求与所请求的服务搜索模式匹配。

协议数据单元（PDU）参数：

AttributeListsByteCount: 尺寸：2 个八位字节

表5.34

值	参数说明
N	AttributeListsByteCount 包含AttributeList 参数的字节数总值。N不得大于在SDP_ServiceAttributeRequest中定义的 最大属性字节数MaximumAttributeByteCount值。 范围：0x0002-0xFFFF

AttributeLists: 尺寸：不定长

表5.35

值	参数说明
数据成分顺序	AttributeLists为一数据元序列，该序列中每一数据元实际又是一个代表一张属性表的数据元序列。每一属性表都包含服务记录属性ID及其属性值。每一属性表中的第一个数据元都包含为该服务记录返回的第一个属性的属性ID。属性表中的第二个数据元则包含该属性所对应属性值。后面的数据元对

	将包含其它的属性ID和值对。AttributeList中只包括SDP_ServiceAttributeRequest指定的服务记录非空属性值及其属性ID。如果服务记录的属性ID或属性值为空，则不得包含于该AttributeList中。每一属性列表中，属性都以属性ID值的增序列出。

ContinuationState: 尺寸:1 至 17 个八位字节

表5.36

值	参数说明
连续状态	ContinuationState 由8位计数器N、后续状态信息字节数，以及服务器前一个应答中返回的N个字节的后续状态信息组成。如果当前应答完成，则该参数由值为0单字节组成。如果给出局部应答，则该参数将在后续应答中给出，以检索应答的其余部分。

5 服务属性定义

本文件中的服务类和属性只是由SDP支持的服务类和属性表的一部分。本文件只包括直接支持SDP服务器的服务类。其它服务类将在其它文件或本文件将来的修订版中定义。而且,将来会有其它属性能够用于支持更多的服务集，而这些属性将被增补到本文件将来修订版的通用属性表中。

5.1 通用属性定义

通用属性是指其定义适用于所有服务记录的服务属性。但是，这并不意味着每一服务记录都必须包含所有这些服务属性值。然而,如果服务记录属性具有一个分配为通用属性的属性ID，则该属性值必须符合通用属性定义。

在服务记录实例中，只允许存在两个属性；服务记录句柄ServiceRecordHandle（属性ID 0x0000）和服务类ID列表ServiceClassIDList(属性ID 0x0001)。而所有其它服务属性对于服务记录都是可选项。

5.1.1 ServiceRecordHandle服务记录句柄属性：

表5.37

属性名	属性 ID	属性值类型
ServiceRecordHandle	0x0000	32-位低精度整数

描述：

服务记录句柄为一32位数，它唯一标识SDP服务器的每一服务记录。特别要注意是,一般每一句柄在每一SDP服务器内是唯一的。如果SDP服务器S1和SDP服务器S2包含同一服务记录(代表同一服务),那么用来引用这些服务

的句柄则是完全独立的。一般，用于应用S2服务的句柄将对于S2毫无意义。

5.1.2 ServiceClassIDList服务类ID列表属性

表5.38

属性名	属性 ID	属性值类型
ServiceClassIDList	0x0001	数据元序列

描述：

ServiceClassIDList 属性由一个数据单元顺序构成，在该序列中每一数据元都是一个 UUID，该 UUID 代表某个服务记录所遵循的服务类。UUID 按照从具体类到通用类的顺序进行列表。服务类 ID 列表 ServiceClassIDList 必须包含至少一种服务类 UUID 。

5.1.3 ServiceRecordState服务记录状态属性

表5.39

属性名	属性 ID	属性值类型
ServiceRecordState	0x0002	32-位低精度整数

描述：

ServiceRecordState 是一个用于缓存ServiceAttributes服务属性的32位的整数。如果该属性包含于一条服务记录，那么当在该服务记录中增删或改变其它属性值时，该值也一定会改变。这样客户就可以检查该唯一属性的值了。如果该值从上次检查后就一直没发生变化，客户就可以推知服务记录的其它属性值也没有发生变化。

5.1.4 ServiceID服务ID属性

表5.40

属性名	属性 ID	属性值类型
ServiceID	0x0003	UUID

描述：

ServiceID是一个可以普遍和唯一标识由服务记录描述的服务实例的UUID。如果同一服务在不只一个SDP服务器的服务记录中描述过，那么该服务属性将非常有用。

5.1.5 ProtocolDescriptorList协议描述符列表属性

表5.41

属性名	属性 ID	属性值类型
ProtocolDescriptorList	0x0004	数据元序列或备选数据元

描述：

ProtocolDescriptorList属性描述可用于访问由服务记录所描述服务的一个或多个协议栈。

如果ProtocolDescriptorList只描述单个的协议栈，则它将采用数据元序列的形式，在该序列中每一序列数据元都是一个协议描述符。反过来，每一协议描述符又都是一个数据元序列；其第一个数据元就是一个用于标识该协议的UUID，而后面的数据元则是协议指定参数。潜在的协议指定参数是一个协议版本号和一个连接端口号。协议描述符按照从低层协议到高层协议的顺序列出，以用于对服务进行访问。

如果有一个以上的用于访问服务的协议栈，ProtocolDescriptorList将采用备选数据元的形式，其中每一数据元都是一个数据元序列，如上段所述。

协议描述符

协议描述符唯一标识一则通信协议，并且提供协议指定参数。协议描述符以数据元序列表示。

该序列中的第一个数据元必须是可唯一标识协议的UUID。其它数据元则可以有选择性地提供协议指定信息,以下面的L2CAP协议/服务多路复用器（ PSM ）和 RFCOMM 服务器信道号（ CN ）为例。

ProtocolDescriptorList 举例

本规范并未对每一协议的参数格式作出定义。

在前两个示例中，假设L2CAP层的上层存在一个RFCOMM实例。在这种情况下，L2CAP协议指定信息（ PSM ）将指向该RFCOMM实例。在最后一个示例中，则是在L2CAP层的上层存在两个不同但相互独立的RFCOMM实例。在这种情况下，L2CAP协议指定信息（ PSM ）指向可识别每一RFCOMM实例的唯一标识符。根据 L2CAP规范，该标识符取值范围为0x1000-0xFFFF。

IrDA-like打印机

（（ L2CAP, PSM=RFCOMM ），（ RFCOMM, CN=1 ），（ PostscriptStream ））

IP网络打印

（（ L2CAP, PSM=RFCOMM ），（ RFCOMM, CN=2 ），（ PPP ），（ IP ），（ TCP ），（ IPP ））

同步协议描述符举例

（（L2CAP, PSM=0x1001 ），（RFCOMM, CN=1 ），（Obex ），（vCal ））（（L2CAP, PSM=0x1002 ），（ RFCOMM, CN=1 ），（ Obex ），（ 其它同步应用 otherSynchronisationApplication ））

5.1.6 BrowseGroupList浏览组列表属性

表5.42

属性名	属性 ID	属性值类型
BrowseGroupList	0x0005	数据元序列

描述：

BrowseGroupList属性由一个数据元序列组成，在序列中每一数据元就是一个代表一个浏览组的UUID，而服务记录就属于该浏览组。

顶级浏览组ID称为PublicBrowseRoot公共浏览根目录,即浏览层次结构的根，在蓝牙指定号码文件中该ID的值为：00001002-0000-1000-7007-00805F9B34FB（UUID16：0x1002）。

5.1.7 LanguageBaseAttributeIDList语言基本属性ID列表属性

表5.43

属性名	属性 ID	属性值类型
LanguageBaseAttributeIDList	0x0006	数据元序列

描述：

为在一条服务记录中，支持人们可读的多种自然语言属性，可以服务记录中用到的每一自然语言分配一个基本属性ID。这样，就可以使用属性ID偏移，而不用绝对属性ID来定义人们可读的通用属性。该偏移来自于每一基本值。

LanguageBaseAttributeIDList属性实际就是一张列表。对于服务记录中的每一种自然语言，该表包括一个语言标识符、一个字符编码标识符和一个基本属性ID。LanguageBaseAttributeIDList属性由一个成员为16位低精度整数的数据元序列组成。该三个数据元组成一个三元组。

每一三元组的第一个数据元包含一个可表示自然语言的唯一标识符。该语言根据ISO 639:1988（E/F）：“语言名字表示代码”。

每一三元组的第二个数据元包含一个用于该语言字符编码方式的唯一标识符。字符编码值可在IANA数据库（注1）中找到。这些编码的值可称作MIBE-num 值。推荐字符编码方式为UTF-8 。

每一三元组的第三个数据元包含作为服务记录中自然语言基本属性ID的一个属性ID。同一服务器中的不同服务记录可对同一语言使用不同基本属性ID值。

为了便于采用一种主要语言实现对可读通用属性的检索,该由服务记录支持的主要语言基本属性ID值必须为0x0100。并且,如果服务记录包含LanguageBaseAttributeIDList属性，那么其第一个数据元的基本属性ID必须为0x0100。

5.1.8 ServiceInfoTimeToLive服务信息可用时间属性

表5.44

属性名	属性 ID	属性值类型
ServiceInfoTimeToLive	0x0007	32位低精度整数

描述：

ServiceTimeToLive 属性为一个32位整数。它包含了以秒为单位的，希望服务记录中信息保持有效和不变的时间长度。该时间间隔从SDP服务器检索属性值开始计起。但是，该值并不意味着服务记录将始终保持可用或不变。也可以说，客户可以用它来确定一个重新校验服务记录内容的轮询间隔时间。

注 2 ： 见 http://www.isi.edu/in-notes/iana/assignments/character-sets

5.1.9 ServiceAvailability 服务可用性属性

表5.45

属性名	属性 ID	属性值类型
ServiceAvailability	0x0008	8位低精度整数

描述：

ServiceAvailability属性为一个 8 位低精度整数，它用于表示服务是否具有接受其它客户的相关能力。值0Xff表示服务现在没有在使用中并完全可用，而值0x00则意味着服务现在没有接受新的客户。对于支持多个并发客户的服务，中间值表示服务的相关线性利用率。

例如，可接受三个客户的服务应当提供服务利用率：当有客户数为0时，该服务利用率值为0xFF；当有客户数为1时，该服务利用率值为0xAA；当有客户数为2时，该服务利用率值为0x55；当有客户数为3时，该服务利用率值为0x00。0xAA 值近似于(2/3)* 0Xff，表示2/3的利用率；而0x55 值近似于(1/ 3)* 0xFF，表示1/3的利用率。利用率值可以近似等于：

(1 -(当前客户数 / 最大客户数))* 0xFF

如果最大客户数很大，则须修改该公式以确保服务利用率ServiceAvailability的值0x00 和 0xFF被保留，并分别用于表示利用率为0和利用率为1的情况。

注意根据服务可支持的最大客户数，可以根据服务当前客户使用资源的情况而不同。

非零的ServiceAvailability并不保证可使用该服务。它只是表示可利用状态的近似值。

5.1.10 BluetoothProfileDescriptorList蓝牙标准描述符列表属性

表5.46

属性名	属性 ID	属性值类型
BluetoothProfileDescriptorList	0x0009	数据元序列

说明：

BluetoothProfileDescriptorList属性由一个数据元序列组成，该序列中的每一数据元都是一个包含有关该服务所遵循蓝牙标准信息的标准描述符。每一标准描述符都是一个数据元序列，其第一个数据元为赋给该标准的UUID，其第二个单元是一个16位的标准版本号。

标准的每一版本号都分配一个16位低精度整数，包含两个8位域。高端的8位包含主版本号域，低端的8位包含次版本号域。每一标准的最初版本具有为1的主要版本和一个为0的次要版本。标准作向上兼容的改变时，将增长次版本号。如果标准作不兼容的改变，则将增长主版本号。

5.1.11 DocumentationURL文档URL属性

表5.47

属性名	属性 ID	属性值类型
DocumentationURL	0x000A	URL

说明：

该属性是一个指向服务记录所描述服务文档的URL。

5.1.12 ClientExecutableURL 客户端可执行URL属性

表5.48

属性名	属性 ID	属性值类型
ClientExecutableURL	0x000B	URL

说明：

该属性是一个指示应用所在位置的URL,该应用可用于使用服务记录所代表的服务。由于不同操作环境要求不同执行格式，那么就可以定义一种机制，以允许该属性可被用于定位适用于客户操作环境的执行程序。在使用该URL之前,客户应用程序可用代表操作环境的一个字符串，替代该URL属性的首字节(ASCII字符'*')，该字节值为0x2A。

蓝牙号码分配文件中给出了代表操作环境的标准化字符串列表。

例如，假设 ClientExecutableURL 属性值为 http://my.fake/public/*/ client.exe。在一台能够执行 SH3 WindowsCE 文件的设备上，该 URL 将变为 http://my.fake/public/sh3-microsoft-wince/client.exe。在能够执行 Windows 98 二进制代码的设备上，该 URL 将变为 http://my.fake/public/i86-microsoft-win98/ client.exe.

5.1.13 IconURL 属性

表5.49

属性名	属性 ID	属性值类型
IconURL	0x000C	URL

说明：

该属性包含一个指向某图标位置的URL，该图标用于标识由服务记录描述的服务。由于不同硬件设备需要不同的图标格式，那么就可以定义一种机制，以使该属性可以用于定位适于该客户端设备的图标。在使用该URL之前，客户可采用一个代表所希望图标格式的字符串代替URL数性值中值为0x2A的首字节。

蓝牙号码分配文件中给出了代表图标格式的标准化字符串列表。

例如，假设IconURL 属性值为 http://my.fake/ public/icons/*。在256色的24 x 24图标所在的设备上，该URL将变为http://my.fake/public/icons/24x24x8.png。而在单色的10 x 10图标所在的设备上，该URL将变为http://my.fake/public/icons/10x10x1.png。

5.1.14 ServiceName 服务名属性

表5.50

属性名	属性 ID	属性值类型
ServiceName	0x0000	字符串

说明：

ServiceName属性包含一个由服务记录所表示服务的名称字符串。它应简短并便于表现由服务记录表示的服务图标。必须将偏移量0x0000与属性ID基地址相加(位于 LanguageBaseAttributeIDList属性)，以便为本属性计算属性ID。

5.1.15 ServiceDescription 服务描述属性

表5.51

属性名	属性 ID	属性值类型
ServiceDescription	0x0001	字符串

说明：

该属性是一个包括服务简短说明的字符串。其长度不到200个字符。应将偏移0x0001与属性ID基地址相加(位于 LanguageBaseAttributeIDList属性里)，以便为该属性计算属性 ID 。

5.1.16 ProviderName提供方名字属性

表5.52

属性名	属性 ID	属性值类型
ProviderName	0x0002	串

说明：

该属性是一个包含提供服务的人名或组织名称的字符串。应将偏移0x0002与属性ID相加(位于LanguageBaseAttributeIDList属性里)，以便为该属性计算属性 ID 。

5.1.17 保留的通用属性ID

0x000D-0x01FF范围内的属性ID保留。

5.2 “服务搜索服务器”服务类属性定义

本服务类描述包含服务搜索服务器本身的服务记录。本节中所列属性只在 服务类ID列表（ServiceClassIDList）属性包含服务搜索服务器服务类ID（ServiceDiscoveryServerServiceClassID）的情况下有效。注意，ServiceDiscoveryServer 类的服务记录包含所有通用属性。

5.2.1 ServiceRecordHandle 服务记录句柄属性

已在 ServiceRecordHandle 的通用属性定义里对 ServiceRecordHandle 属性进行描述。

值

值为0x000000000的32位整数。

5.2.2 ServiceClassIDList服务类ID列表属性

ServiceClassIDList属性已在ServiceClassIDList的通用属性定义中描述。

值

一个代表 ServiceDiscoveryServerServiceClassID的UUID 。

5.2.3 VersionNumberList版本号列表属性

表5.53

属性名	属性 ID	属性值类型
VersionNumberList	0x0200	数据元序列

说明：

VersionNumberList是一个数据元序列，该序列中的每个数据元都是SDP服务器支持的版本号。版本号是一个包含两个域的16位低精度整数。高段8位包含主版本号域，而低段8位则包含次版本号域。SDP最初版本具有一

个主版本号1和一个次版本号0。当协议作向上兼容的改变时，将增长次版本号。如果SDP作非兼容改变时，将增长主版本号。这将保证客户和服务器是否支持一个通用主版本号。如果客户和服务器都支持一个次版本号，并只使用次版本规范特性，它们就可以相互通信。

5.2.4 ServiceDatabaseState服务数据库状态属性

表5.54

属性名	属性 ID	属性值类型
ServiceDatabaseState	0x0201	32-位低精度整数

说明：

ServiceDatabaseState位一个便于实现服务记录缓存的32位整数。如果存在该属性，则当从服务器数据库中添加或删除其它服务记录时，必须保证改变该属性值。如果该值自从上次客户查询以来一直没变，那么客户就可以推知：a) 没有增加或删除SDP所维护的所有其它服务记录；b) 服务器获得的任一服务记录句柄仍然有效。当到服务器的连接建立时，客户可以在使用前一连接期间获取的服务记录句柄之前，查询该值。

值得注意的是，当已有服务记录被修改时，包含增加、移动、或服务属性修改，服务记录的服务数据库状态（ServiceDatabaseState）属性将保持不变。服务记录的服务记录状态 （ServiceRecordState）属性则表示服务记录何时被修改。

5.2.5 保留的属性ID

在0x0202-0x02FF的范围内的属性ID将保留。

5.3 BROWSEGROUPDESCRIPTOR“浏览组描述符”服务类属性定义

本服务类描述由蓝牙设备支持的，为每一浏览组描述符（BrowseGroupDescriptor）服务所提供的服务记录（ServiceRecord）。只有在服务类ID列表ServiceClassIDList属性包含浏览组描述符服务类ID（BrowseGroupDescriptorServiceClassID）时，本节所列属性才有效。注意：所有通用属性都将包含在浏览组描述符（BrowseGroupDescriptor）类的服务记录里。

5.3.1 ServiceClassIDList服务类ID列表属性

ServiceClassIDList属性已在服务类ID列表（ServiceClassIDList）通用属性定义中描述。

值

一个代表浏览组描述符服务类ID（BrowseGroupDescriptorServiceClassID）的UUID。

5.3.2 GroupID组ID属性

表5.55

属性名	属性 ID	属性值类型
GroupID	0x0200	UUID

说明：

该属性包含一个可用于定位浏览组成员服务的UUID，该服务由服务记录描述。

5.3.3 保留的属性ID

在0x0201-0x02FF的范围内的属性ID保留。

附录一：背景信息

A1.服务搜索

随着计算过渡到以网络为中心的阶段，如何查找和使用网络中可用的服务变得越来越重要。服务可以包括打印、寻呼、传真等普通服务,以及远程会议、网络桥接和访问点、 电子商务设施等各种信息访问服务，甚至包括更多可能由服务器或服务供应商提供的各类服务。除了对搜索可用服务的标准方法的需求，还应考虑:如何获取对服务的访问(包括发现并获取协议,访问方式,“引擎”和其它利用服务的代码等)，如何控制对服务的访问,如何宣传服务,如何在各种服务中进行选择,如何为服务付账,等等。目前，已经广泛认识到这些问题;许多公司、标准化组织和协会正在以不同方式在不同层次上从事于这些问题的解决，如服务定位协议（SLP)、Jini™等。

A2.蓝牙服务搜索

服务搜索协议(SDP)专门用于蓝牙环境下的服务搜索。它充分针对蓝牙环境的高度动态特性进行了优化。SDP主要关注于如何通过或利用蓝牙设备搜索可用服务。SDP并不定义访问服务的方式;一旦用 SDP 搜索到服务，则可以采用各种各样的方法对服务进行访问。这可能包括使用其它的服务搜索和访问机制;SDP为其它协议提供一种可以在这些环境中与其一起使用的途径，这将非常有用。当SDP能与其它服务搜索协议共存时，它将不需要这些协议。在蓝牙环境中，可用SDP搜索服务，并采用蓝牙定义的其它协议访问服务。

第 6 章　基于 TS 07.10 的 RFCOMM 串口仿真

本文件定义 RFCOMM 协议，其中包括根据蓝牙技术进行修正的 ETSI TS07.10 标准的一个子集。

1．介绍

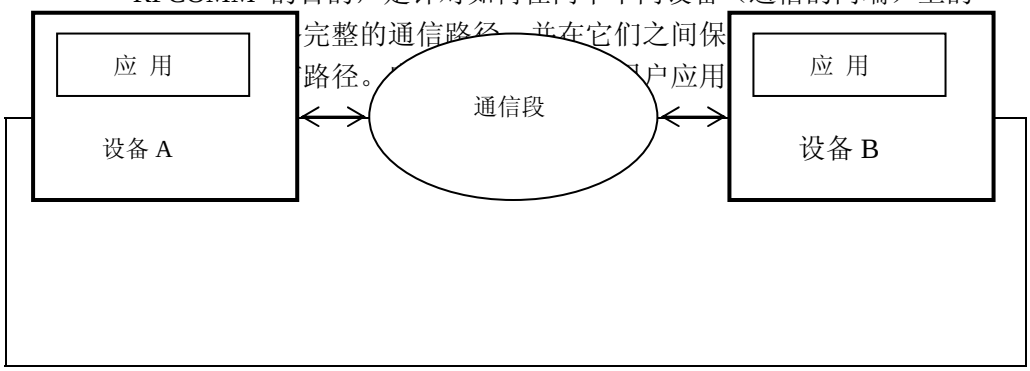
RFCOMM 协议提供对基于 L2CAP 协议的串口仿真。协议基于 ETSI 标准 TS 07.10。本文件并不包括完整的规范，其中部分相关内容可参见 TS 07.10 标准。本文件中只利用了 TS 07.10 标准一个子集，并根据蓝牙技术作出适当修正。

1．1 概 述

RFCOMM 是一个简单传输协议，其中针对 9 针 RS-232（EIATIA-232-E）串口仿真附加了部分条款。RFCOMM 协议可支持在两个 BT 设备之间同时保持高达 60 路的通信连接。可由 BT 设备利用的同时连接数量根据实际应用情况定义。

1．2 设备类型

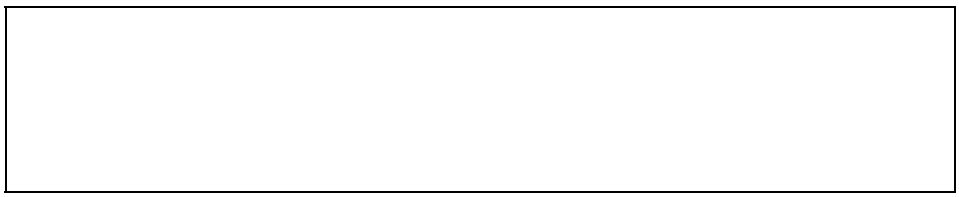
RFCOMM 的目的，是针对如何在两个不同设备（通信的两端）上的完整的通信路径，并在它们之间保路径。户应用



协议或作为终端用户应用的的其它服务。

图 6.1 RFCOMM 通信段

RFCOMM 准备把利用设备串口进行通信的应用覆盖在内。在一个简单配 通信段就是设备之 ，如图 1.2。如果通信 BT 用于在设备 如 Modem）之间建立 只 BT 互连 或者是设备与网络接入设备之间的互连。RFCOMM 支持其它的配置方式，如一端采用 BT 通信，另一端采用有线接口，如图 1.3。这些设备不只是调制解调器,而且提



供简单服务。

图 6.2 利用 COMM 口的 RFCOMM

通信两端设备必须兼容于 RFCOMM 协议。第一类设备是诸如计算机、

打印机等通信终端设备。第二类设备是通信段的一部分，如 Modem。但是为了简化协议内容，RFCOMM 协议对这两种设备不作区分。

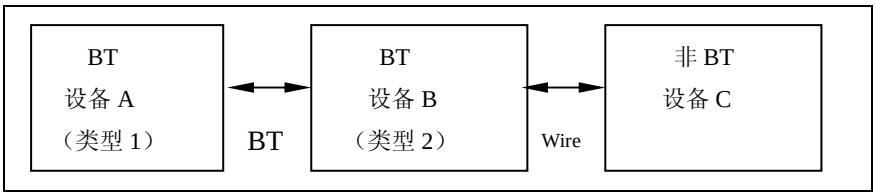


图 6.3 利用 COMM 设备的 RFCOMM

在两个 RFCOMM 实体间传输信息也都支持这两类设备，其中有些信息只用于第二类设备。本协议中也没有对两类设备所用信息进行严格划分。而是由本协议的用户决定使用哪些信息。由于一个设备并不知道通信路径上的其它设备的类型，所以每一个设备都应按照协议规定发送所有可用信息。

1．4 字节序列

本文件采用与 TS07.10 相同的字节序列方式。所有二进制数字都按照从低位到高位的顺序，从左至右读。

2． RFCOMM 服务概述

RFCOMM 仿真 RS-232（EIATIA-232-E）串口。该仿真过程包括非数据通路状态的传输。RFCOMM 内置空 modem 仿真标准框架。

如果通过 RFCOMM 服务接口设定指定端口的波特率，也不会影响 RFCOMM 的实际数据吞吐量。也就是说，RFCOMM 不限制人工速率或步长。但是，如果通信链路两端的设备都是负责将数据转发到其它通信介质的第二类设备，或在两端 RFCOMM 设备接口上进行数据传输，实际数据吞吐一般将反映波特率的设置。

RFCOMM 支持两个设备间的多串口仿真，也支持多个设备间多串口的仿真。

2．1 RS-232 控制信令

RFCOMM 提供对 9 针 RS-232 接口的仿真。其通路如下：

表 6.1 RFCOMM 中的仿真 RS-232 通路

针	通路名称
102	公用信号
103	发送数据（TD）
104	接收数据（RD）
105	请求发送（RTS）
106	清除发送信号（CTS）
107	数据准备就绪（DSR）

108	终端准备就绪（DTR）
109	数据载波监听（CD）
125	铃声报警（RI）

2.2 空 MODEM 仿真

RFCOMM 基于 TS 07.10。当设备准备传输非数据通路的状态信息时，TS 07.10 不区分 DTE 和 DCE 设备，而是通过 RS-232 控制信号来表示 DTE/DCE 各自的信号。下面通过列表反映 TS07.10 信号与 RS-232 控制信号之间的对应关系。

表 6.2 TS07.10 串口控制信号

TS07.10 信号	对应的 RS-232 控制信号
RTC	DSR、DTR
RTR	RTS、CTS
IC	RI
DV	DCD

当两同类设备互连时，TS07.10 传输 RS-232 控制信号的方式就会创建空 MODEM。图 2.1 体现了在两个 DTE 设备通过 RFCOMM 互连时空 MODEM 的创建过程。虽然，没有一种空 MODEM 有线传输方案能够满足所有情况下的通信要求，但 RFCOMM 所提供空 MODEM 方案能够满足大多数情况下的通信要求。

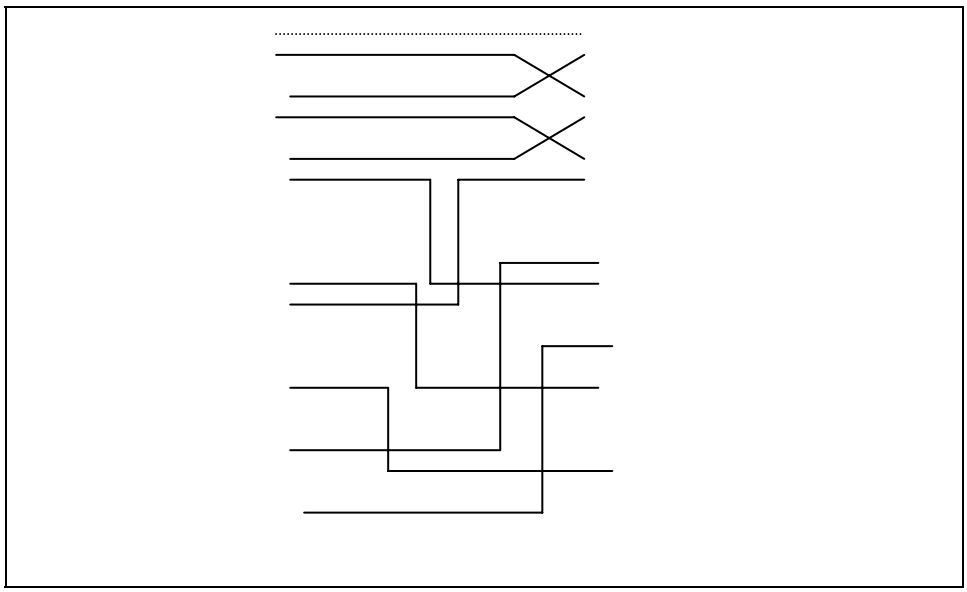


图 6.4 RFCOMM DCE-DTE 空 MODEM 仿真

2.3 多串口仿真

2．3．1 两设备间的多串口仿真（如图 2.2）

两个采用 RFCOMM 进行通信的 BT 设备有可能同时打开多个串口。RFCOMM 支持同时打开 60 个仿真端口。但是，一个设备打开端口数根据实际实现而不同。

一个数据链接标志（DLCI）唯一标识一对客户和服务器之间的持续连接。DLCI 长度为 6 字节，其无效值区间为 2 至 61。TS07.10 中，DLCI 0 为控制信道，DLCI 1 根据服务器信道概念不能使用，DLCI 62-63 保留使用。DLCI 在两个设备间的 RFCOMM 会话中保持一致。这部分内容将在下节中进一步阐述。

在一次 RFCOMM 会话中，客户和服务器应用可以分布在通信的两端，每[illegible]可以独立发起建立通信连接。因此，[illegible]器信道的概念将 DLCI 值域空间在两个正在进行通信的设备间进行划分。[illegible]在 RFCOMM 服务器信道的 DLCI 定位节[illegible]

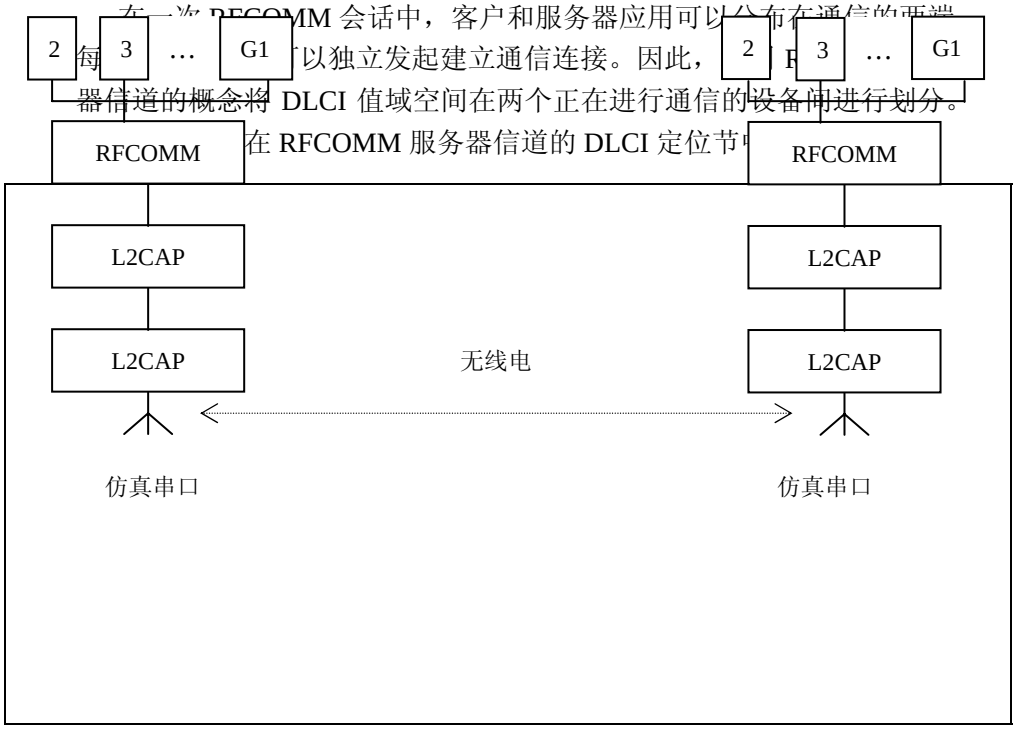


图 6.5 多串口仿真

2.3.2 多仿真串口和多 BT 设备

如果 BT 设备支持多串口仿真，通信连接两端允许使用不同 BT 设备，那么 RFCOMM 实体必须能够运行多个 TS07.10 多路复用器会话，参见图 2.3。每一多路复用器都使用其 L2CAP 信道 ID（CID）。RFCOMM 可以选择支持 TS07.10 多路复用器的多个会话。

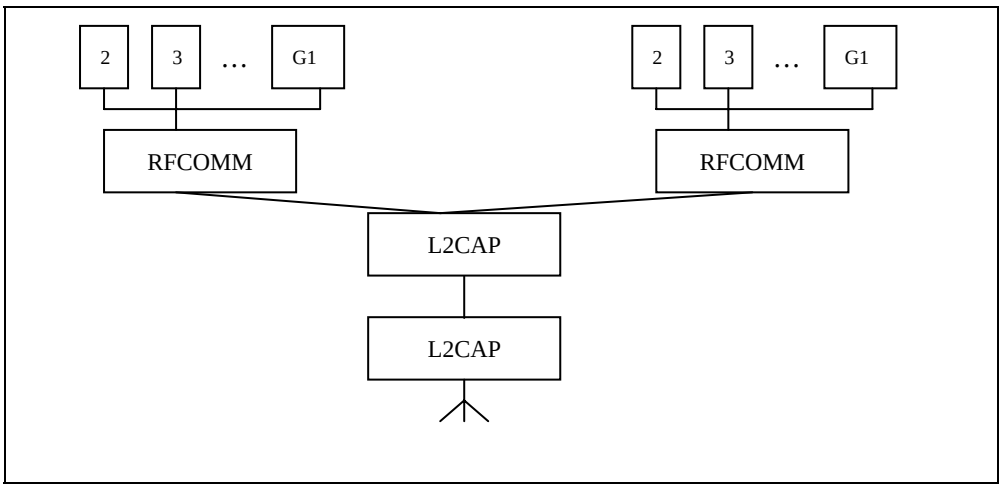


图 6.6 两 BT 设备的多串口仿真

3. 服务接口描述

RFCOMM 目的在于定义一个能够利用仿真串口的协议。大多数系统中，RFCOMM 将成为包括串口仿真实体的端口驱动程序的一部分。

3.1 服务定义模型

下图图示了 RFCOMM 如何适应于典型系统的模型。此图提出了 RFCOMM 参考模型。

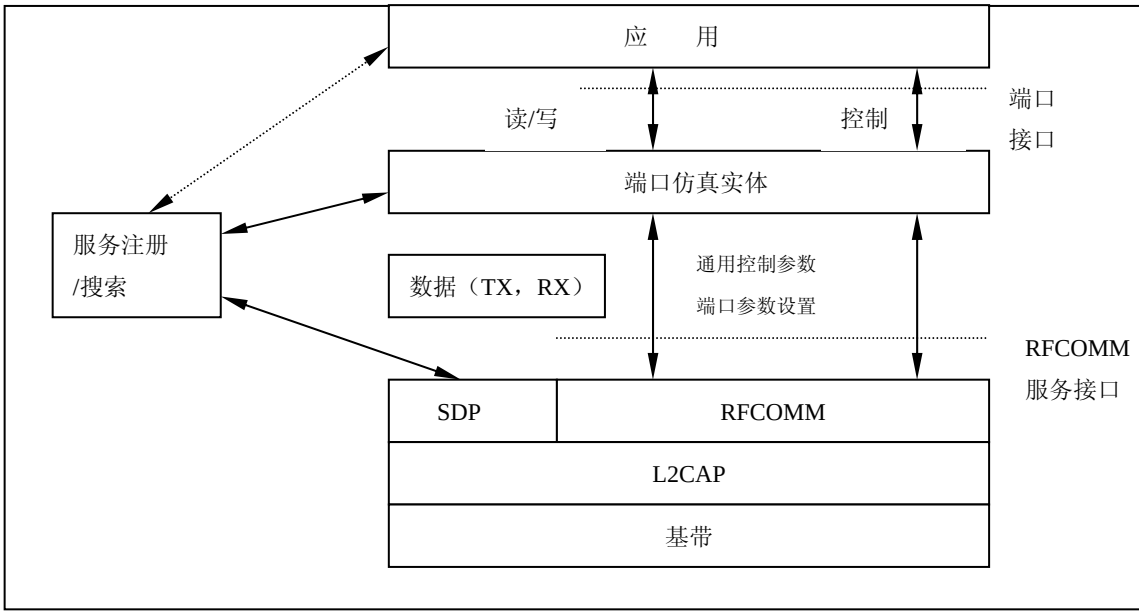


图 6.7 RFCOMM 参考模型

RFCOMM 参考模型组成部分描述如下：

表 6.3

组成部分	描　　述
应用	利用端口通信接口
端口仿真实体	端口仿真实体将系统通信接口映射到 RFCOMM 服务。端口仿真实体与 RFCOMM 组成端口驱动程序。
RFCOMM	基于 L2CAP 信道提供透明数据流和控制通道，复用多个仿真串口
服务注册/搜索	服务器应用注册在本地服务上，并向客户端应用提供获取其它服务上服务器端应用的服务。
L2CAP	协议复用，SAR
基带	BT 定义的基带协议

3. RFCOMM 支持的 TS07.10 子集

4.1 选项和模式

RFCOMM 利用 TS07.10 的基本选项进行定义。

4.2 帧类型

表 4.1 列出 RFCOMM 支持的帧类型。

表 6.4　RFCOMM 支持的帧类型

帧类型
异步平衡模式设置(SQBM)指令
未加标记的确认（DM）应答
断开模式(DM)指令
连接断开（DISC）指令
带头校验的未标记信息（UIH）指令和应答

RFCOMM 不支持“未加标记信息(UI)指令和应答”帧类型。另外，RFCOMM 的任一种帧格式都不支持 TS07.10 协议的纠错机制。

4.3　指令集

TS07.10 定义了一种可以具有完整控制通道 DLCI0 的多路复用器。控制通道用于在两个多路服用器之间传递信息。下列 TS07.10 指令得到 RFCOMM 的支持：

表 6.5

支持的控制通道指令集
测试指令（Test）
流控制打开指令（Fcon）
流控制关闭指令（Fcoff）
Modem 状态指令(Msc)

远程端口协商指令（RPN）
远程通路状态（RLS）
DLC 参数协商（PN）
对未被支持的指令的应答（NSC）

无论何时收到未支持的指令类型，NSC 帧就作为应答信息发出。

4.4 聚集层

RFCOMM 只支持 TS07.10 中的第一种聚集层类型。

Modem 状态指令（MSC）应用于传递 RS-232 控制信号和仿真串口的断开信号。

5．根据 RFCOMM 对 TS07.10 的修正

5．1 介质调整

RFCOMM 不使用 TS07.10 基本帧格式中的开始和结束标志，而仅仅使用包含在 L2CAP 层和 RFCOMM 层间交换标志中的那些域。

图 6.6 基本帧结构，但注意：在 RFCOMM 中不采用 TS07.10 规定开始和结束标志

标志 0111 1101	地址	控制	长度标志	信息	FCS	标志 0111 1101
	8 字节	8 字节	8 字节或 16 字节	不定长，但是整数个 8 字节长度	8 字节	

5.1.1 FCS 运算

TS07.10 中，帧校验序列（FCS）根据不同帧类型在不同域集上进行运算。下面列出需要进行帧运算的域：

对于 SABM、DISC、UA、DM 帧：在地址、控制和长度标志域上进行运算；

对于 UIH 帧：在地址和控制域上进行运算。

※注：为了便于表达清楚和制定 RFCOMM 标准，FCS 运算中的域都在 TS07.10 7.0.0 版本中进行了修改，但是 RFCOMM 没有对上面的 FSC 运算方案进行改动。

5．2 TS07.10 多路复用器的启用和关闭过程

RFCOMM 不支持 TS07.10 第 5 .7 节中定义的启用和关闭过程。也就是说，RFCOMM 不支持 AT 指令 AT+CMUX 和多路复用器的关闭指令。

任意两设备之间最多只能保持一个 RFCOMM 会话。当建立一个新的

DLC 链路时，如果已经存在一个 RFCOMM 会话，应检查会话发起一方，然后在上面建立新 DLC。一个会话由两通信终端的蓝牙 BD_ADDR 唯一标识。

5.2.1 启用程序

由建立两设备间的第一个仿真串口连接的设备负责建立多路复用控制通道。这包括以下步骤：

- 利用 L2CAP 基本服务，建立与对等 RFCOMM 实体之间的 L2CAP 通路，参见 L2CAP 基本服务。
- 通过在 DLCI0 上发送 SABM 启动 RFCOMM 多路复用器，并等候对等实体的 UA 应答。当然也有可能进行进一步的协商。

经过以上步骤，用于用户数据通讯的 DLC 通路就被建立起来。

5．2．2 关闭程序

关闭指定会话上最后一个连接（DLC）的设备负责通过关闭相应 L2CAP 通路关闭多路复用器。可以根据具体实现决定是否通过在 DLCI0 上发送 DISC 指令帧关闭多路复用器，但必须直接用 UA 应答 DISC 指令。

5．2．3 链路丢失处理

如果收到 L2CAP 链路丢失通知，本地 RFCOMM 实体应负责向每一条激活的 DLC 链路端口仿真/代理实体发送链路丢失通知，然后释放所有与此 RFCOMM 会话有关的资源。

而端口仿真/代理实体采取的动作则取决于高层 API。例如，假设该设备为 DTE，对于一个仿真串口（vCOMM），就应撤销 CD、DSR 和 CTS 信号。

5．3 系统参数

下表包括了 TS07.10 多路复用的 RFCOMM 执行版本的所有应用系统参数。

表 6.7 系统参数取值

系统参数	值
帧的最大尺寸（N1）	缺省为 127，可以为 23-32767 之间的任意值
确认时钟（T1）	60 秒
多路复用控制通路的应答时钟（T2）	60 秒

其中，时钟 T1 是发送 P/F 位为 1 的帧的所需超时（在 RFCOMM 中只适用于 SABM 和 DISC 帧）。T2 是以 DLCI 0 上 UIH 帧格式发送指令所需

超时。

因 RFCOMM 依赖于低层提供可靠传输，超时时其缺省动作为关闭多路复用会话。

唯一的例外是在已有会话上试图建立新的 DLC 链路时，也就是等待对 SABM 指令的 UA 应答时。这时，如果会话发起方知道通信延时主要来源于用户交互时，就会将会话超时不定期延长。

无论如何，建立连接最终都要考虑超时问题。会话发起方应在同一 DLSI 通路上发送一个类似于 SABM 指令帧的 DISC 指令帧，目的在于通知其它实体该连接已被放弃。然后，会话发起方等待 DISC 指令的 UA 应答。

5.4 利用 RFCOMM 服务器通道进行 DLCI 定位

在一次 RFCOMM 会话中，服务器和客户可以同时位于会话的两端，每一客户端都可以独立建立连接。这样，DLCI 值域就将被两个利用 RFCOMM 服务器通道和方向位概念的通信设备划分。

RFCOMM 服务器通道号实质上是 TS01.10 帧中地址域 DLCI 部分位的子集。

表 6.8 地址域格式

位	1	2	3	4	5	6	7	8
TS07.10	EA	C/R	DLCI					
RFCOMM	EA	C/R	D	服务器端通道				

注册为 RFCOMM 服务接口的服务器端应用应在 1 至 30 范围内，指定一个服务器端通道号(在 TS07.10 中，0 和 31 由相应 DLCI 保留使用)。该值应在服务搜索数据库中登记。

对于一次 RFCOMM 会话，发起方设备方向位(Direction bit)设为 D=1(相反,把 D=0 赋给其它的设备)。当在已有的 RFCOMM 会话上建立一条新的数据链接时,方向位(Direction bit)用于与服务器端通道相关，以确定其 DLCI，从而建立到特定应用的连接。连接建立后，DLCI 就在两端间的两个方向上传输数据分组。

DLCI 值域实际上分为两部分:非发起方设备上的应用使用 DLCI 偶数号(2,4,…,60)访问，发起方设备上的应用则使用 DLCI 奇数号(3,5,…,61)访问。注意: 对于一个支持多路同步 RFCOMM 会话的设备而言，方向位不一定在所有会话中都一致。

一个在已有会话上建立新 DLC 的 RFCOMM 实体，将其它设备应用使用的服务器端通道和该会话方向位的求反值组合为 DLCI。

RFCOMM 将 DLCI1 和 62-63 保留，并不使用。

5.5 多路复用控制指令

在 TS07.10 中，一些附属于 DLCI 的多路复用控制指令在相应 DLC 建立起来之前，可在 DLCI0 上进行交换(参见 PN 和 RPN 指令)。在收到 DISC 指令帧或从本地关闭 DLC 时，与单条 DLC 相关的所有状态都应被重置为缺省值。也就是说，同一会话连接上的所有 DLC 的创建或重建都可以预见其结果，而与该会话历史无关。

5.5.1 远程端口协商指令(RPN)

RPN 指令可以在新的 DLC 打开前使用，并且只能在端口设置发生改变时使用。

RPN 指令在 TS07.10 中设置为可选项，但在 RFCOMM 中则为协议必要正式内容。

5.5.2 远程线路状态指令(RLS)

该指令用于指示远程端口状态。

RPN 指令在 TS07.10 中设置为可选项，但在 RFCOMM 中则为协议正式必要内容。

5.5.3 DLC 参数协商(PN)

该指令用于指示远程端口状态。

RPN 指令在 TS07.10 中设置为可选项，但在 RFCOMM 中则为协议正式必要内容。

该指令于新的 DLC 打开之前使用。

用于传递不用于 RFCOMM 信息的 PN 指令具有一些参数。因此，这些参数域必须由发送方预先赋值，并且接受端必须忽略该参数域。上述参数域包括:

- l1-14 应设置为 0。 (即:使用 UIH 帧);
- CL1-CL4 应设置为 0。(即:使用第一类聚集层);
- T1-T8 应设置为 0。(即:确认定时器 T1，在 RFCOMM 为硬性规定);
- NA1-NA8 应设置为 9。(转发 N2 代码，在 RFCOMM 常置为 0);
- K1-K3 应设置为 0。(用于定义纠错模式下窗口大小，不适用于 RFCOMM);

如果任一命令的任一参数域收到非法值或无法访问的值，就应发出一个 DLC 参数协商应答，该应答包含可由应答设备接受的值。

6. 流控制

有线端口通常使用 RTS/CTS 等流控制控制通信。另一方面 ,RFCOMM 和低层 L2CAP 间的流控制则取决于实际支持的服务接口。而且，RFCOMM 也有其自有流控制机制。本节就对这两种流控制机制进行讨论。

6.1 L2CAP 流控制概述

L2CAP 依赖于基带链路管理层提供的流控制机制。而 L2CAP 和 RFCOMM 层间的流控制机制根据具体实现定义。

6.2 有线端口的流控制

有线串行端口流控制分为两大类:利用 XON/XOFF 等字符的软件流控制，和利用 RTS/CTS 或 DTR/DSR 电路的流控制。有线链路两端可能同时采用这两种方法，也可能只在一端进行。

6．3 RFCOMM 流控制

RFCOMM 协议提供两类流控制机制:

1. RFCOMM 协议定义了能对两 RFCOMM 实体之间全部数据流操作的流控制指令，对所有的 DLCI 都起作用。Fcon 和 Fcoff 控制通路指令参见 5.4.6.3 节中的定义。
2. 5.4.6.3 节中定义的调制解调器状态指令实质就是可操作单个 DLCI 的流控制机制。

6．4 端口仿真实体串行流控制

对于第一类设备，端口驱动程序（即加载 RFCOMM 的端口仿真实体）需要提供其仿真 API 中定义的流控制服务。应用可以请求 XON/XOFF 或 RTS/CTS 等指定流控制机制，并可通过端口驱动程序处理流控制。

对于第二类设备，端口驱动程序在通道的非 RFCOMM 部分（即 RS-232 端口）上执行流控制。该流控制是由通常是由第一类设备的对等 RFCOMM 实体发出的控制参数定义。本节中流控制描述主要用于第一类设备的端口驱动程序。

由于 RFCOMM 已经具有流控制机制,因此端口驱动程序不再需要利用应用请求的方式执行流控制。理想情况下，由应用设定流控制机制，并假定其实现细节由 COMM 系统处理。这样，端口驱动程序就可以忽略该请求而直接利用 RFCOMM 的流控制。由此，应用就能够发送和接收数据，而不用关心端口驱动程序没有通过请求机制进行流控制。但是，在实际中这种方式存在一些问题：

•基于 RFCOMM 的端口驱动程序在基于分组的协议上运行，数据可能会在通信链路中某个地方缓存。而在有线通信的同样情况下，端口驱动程序

就不能执行流控制；

• 应用可以自己决定采用流控制机制，而不仅仅是通过端口驱动程序请求流控制；

这些问题说明端口驱动器必须为执行流控制仿真作更多的工作。下面是流控制仿真的基本规则：

• 端口驱动程序不能仅仅依靠应用请求的流控制机制，而且可以使用多种流控制混合机制；

• 端口驱动程序必须清楚应用请求的流控制机制。并且，当它发现非数据环路（硬件流控制方式）或输入数据中的流控制字符（软件流控制方式）时，端口驱动程序采取与有线通信相同的工作方式。例如，如果有线方式下需要卸载 XOFF 和 XON 字符，那么基于 RFCOMM 的端口驱动程序也必须这样做；

• 如果应用通过端口驱动程序接口设定流控制机制并触发该机制，端口驱动程序必须采取与有线方式相似的操作。例如，如果有线条件下需要传输 XOFF 和 XON 字符，那么端口驱动程序也必须传输这些字符；

这些基本规则可应用于每一种有线控制机制的仿真。而且，可以同时设定多种流控制。TS 07.10（v6.3.0）的 5.4.8 节对每种流控制机制都做出了定义。

7. 与其它实体的互操作

7.1 端口仿真和端口代理实体

本节定义 RFCOMM 协议如何仿真串口。RFCOMM 协议支持的两类设备如图 7.1 所示。

第一类设备是计算机和打印机等通信端设备，第二类设备是通信段的一部分，如 MODEM。

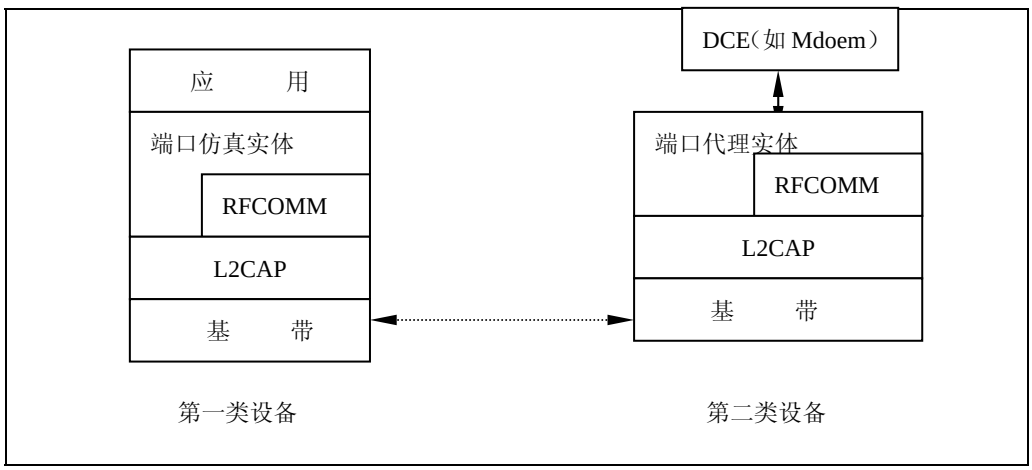


图 6.8 RFCOMM 通信模型

7．1．1 端口仿真实体

端口仿真实体将系统指定通信接口（API）映射于 RFCOMM 服务。

7．1．2 端口代理实体

端口代理实体将数据从 RFCOMM 转发至链接 DCE 设备的外部 RS-232 接口。RS-232 接口的通信参数根据接收的 RPN 指令进行设置，参见 5.5.1 节。

7.2 服务注册和搜索

在原有非蓝牙应用上运行的蓝牙配置应用，主要负责一些应用或服务的注册。这些应用或服务包含可用于访问 RFCOMMM 服务器通道的信息。

下面是一个特定 RFCOMM 服务记录的开发模板或范例。它利用单个服务类和两个协议的协议描述列表（ProtocolList）解释了服务类列表（ServiceClassList）的内涵。尽管在 RFCOMM 之上可能有更多的协议。本例表现了其它服务属性（ServiceName）的使用。对于每个运行在 RFCOMM 之上的服务，应采用合适的已定义 SDP 的通用属性或服务属性。对于服务记录的更多信息，参见 2.2 节 SDP 定义。

那些客户端用于连接 RFCOMM 之上服务的属性至少应包括服务类列表和协议描述符列表(ProtocolDescriptorList)，它对应于下表中的阴影行。

表 6.9

项目	定义	类型/大小	取值	属性 ID
ServiceClassList			Note1	0x001
ServiceClass0	Note5	UUID/32 bits	Note1	
ProtocolDescriptorList				0x004
Protocol0	L2CAP	UUID/32 bits	L2CAP/Note1	
Protocol1	RFCOMM	UUID/32 bits	RFCOMM/Note1	
ProtoclSpecificParameter0	服务器通道	Unit8	N=某服务器通道	
（其它协议）		UUID/32 bit	Note1	
[其它协议指定参数]	Note3	Note3	Note3	
ServiceName	可显示的文本名	数据元/字符串	‘服务实例’	Note2
其它适合于服务的公共属性	Note4	Note4	Note4	Note4
[指定服务属性]	Note3	Note3	Note3	Note3

注释：

①定义于“蓝牙分配号码”；

②对于支持‘可显示’文本字符串属性的其它语言，应根据该语言对语言基本属性列表（LanguageBaseAttributeList）值增加偏移量（参见 5.1.14 节的 SDP 定义）；

③根据具体服务定义；
④对于具体服务，可以采用一些定义 SDP 的公共属性(参见 5.1 节的 SDP 定义）；
⑤表示服务类。对于大多数的服务类都只有一个入口或列表；

7．3 低层约束

7．3．1 可靠性

RFCOMM 利用 L2CAP 服务建立连接到其它服务上 RFCOMM 实体的 L2CAP 通道。一 L2CAP 通道用于 RFCOMM/TS07.10 多路复用器会话。根据 5.1 节进行适当修正的 TS07.10 帧就通过该通道发出。

一些帧类型(SABM 和 DISC)，以及 DLCI0 上发出的带有多路复用器控制指令的 UIH 帧，通常需要远程实体的应答，以便进行 RFCOMM 层次上的确认。(当无确认时不重发,参见“系统参数”一节)。RFCOMM 协议中对数据帧不需要进行应答和确认。

因此，RFCOMM 需要 L2CAP 提供具有最大可靠性的通道，以确认按次序和不重复地传输所有帧。如果 L2CAP 通道不能够提供该特性，RFCOMM 则需要由 RFCOMM 处理链路丢失通知，参见“链路丢失处理”一节。

7.3.2 节能模式

如果所有指向某设备的 L2CAP 通道在一段时间内空闲，应将该设备置为节能模式。(即使用挂起、呼吸或休眠状态，参见基带定义)。RFCOMM 对此未作解释，但给出了 L2CAP 的潜在要求。低层可根据该信息决定使用何种节能模式。

然而，RFCOMM 协议不能接受节能模式引起的潜在通信延迟，本文未注明 RFCOMM 操作最大延时。可能允许的延时决定于应用需求，也就是说，RFCOMM 服务接口可以通过某种方式体现可能的延时要求，并通过 RFCOMM 应用进行汇总并传输到 L2CAP。

8．参考文献

9．名词和缩写

DTE Data Terminal Equipment 数据终端设备：在串行通信中，DTE 指通信路径一端的设备，典型的如计算机或终端；
DCE Data Circuit-Terminating Equipment 数据电路接收设备：在串行通信中，DCE 指在通信路径上介于两端之间的设备，其功能在于使通信得以进

行，如 Modem;

RFCOMM 初始化端：初始化 RFCOMM 会话的设备；或者说，在 L2CAP 上创建通道，并通过 DLCI0 的 SABM 指令帧启动 RFCOMM 多路复用的设备。

RFCOMM 客户端：指向另一应用（RFCOMM 服务器）发送连接指令的应用；

RFCOMM 服务器：指等待另一设备 RFCOMM 客户端连接请求的应用；

RFCOMM 服务器通道：指 TS07.10DLCI 的子域值。该术语用语允许服务器和客户端应用可以同时运行在一个 RFCOMM 会话的两端。

第 7 章 IrDA 互操作性

IrOBEX 协议用于蓝牙技术。在蓝牙技术中，该协议提供相对于 IrDA 协议层次的相应特性，能够使应用在蓝牙协议栈上运行，而与在 IrDA 协议栈上相同。

目 录

1. 介 绍

本文件目的在于指导在短距离 RF 和 IR 介质上开发应用项目。这两类介质各有优缺点，但目标都在于运行应用。因此，与其说本文件内容在于划分应用范围，不如说在于定义蓝牙应用与 I r DA 应用间的互操作性。其互操作点为 IrOBEX。

IrOBEX 是由 IrDA 定义的会话协议。蓝牙技术现将该协议同时用于支持蓝牙无线技术和 IrDA IR 技术应用。IrDA 和蓝牙技术都是设计用于短距离无线通信，但是它们仍在低层协议上具有根本的不同。因此，IrOBEX 才单独制定用适用于蓝牙的低层映射协议。

本文件定义了 IrOBEX 在 RFCOMM 和 TCP/IP 间的映射方式。最初，OBEX(Object Exchang Protocol)对象交换协议的开发目的是在红外线链路上实现对象交换，并被置于 IrDA 协议层次内。但是，它在目前的 RFCOMM 和 TCP/IP 协议层次中居于传输层之上。那么我们可以说，OBEX over TCP/IP 可以作为支持 OBEX 协议蓝牙设备的可选特性。

IrOBEX 提供了一个对象表示模型和一个会话协议。这两个协议确定了两设备间的会话框架。IrOBE 协议遵循客户/服务器的请求/应答会话模式。

虽然 IrDA 同时定义了无连接 OBEX，但蓝牙只使用面向连接的 OBEX。采用面向连接策略的原因在于：

- 在蓝牙体系结构中，OBEX 映射于面向连接的协议之上；
- 大部分采用蓝牙和 OBEX 技术的应用框架需要一个面向对象的 OBEX，以提供这些应用框架中定义特性所描述的功能；
- 无连接的 OBEX 与面向连接的 OBEX 的通信都会带来互操作的问题；

1.1 OBEX 和蓝牙体系结构

图 1.1 解释了蓝牙体系结构的部分层次，揭示了 OBEX 协议及其应用在该体系结构框架中所处的层次（参见第 5 节）。该协议能够与服务搜索数据库进行通信。

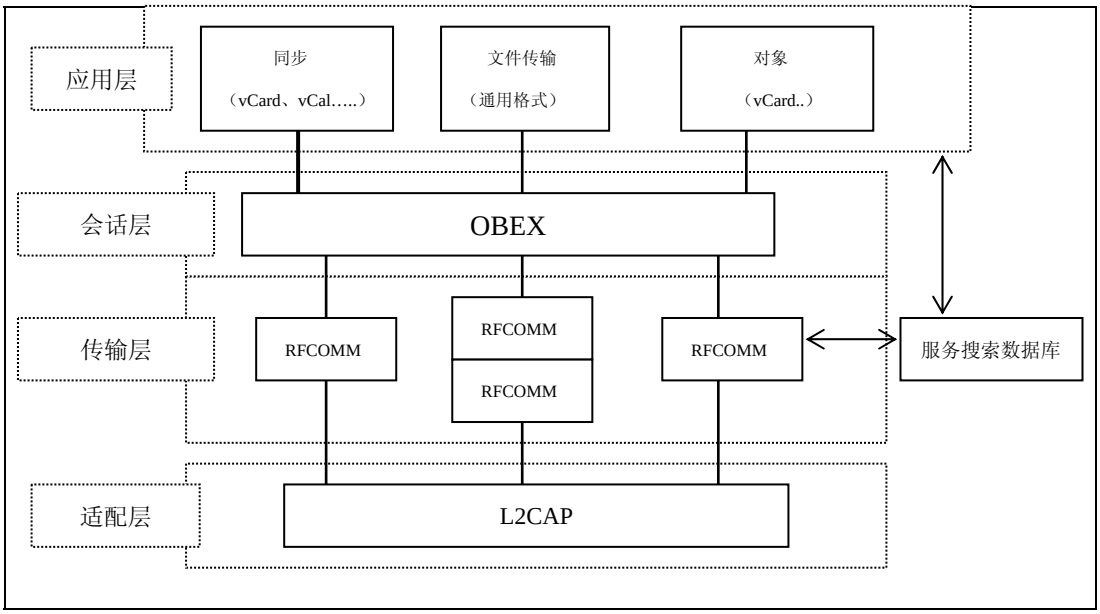


图 7.1　部分蓝牙协议层次

蓝牙系统中，OBEX 协议的目的在于实现数据对象交换。典型例子是将业务卡片（business card）对象‘推’到网络中其它实体。还有更复杂的例子，如多个 OBEX 设备间的时钟同步问题。对于‘推’对象和同步应用，其内容格式可以是 vCard、vCal、vMessage 和 vNote 格式。vCard、vCal、vMessage 和 vNote 格式分别描述了电子业务卡片、电子时钟和计划、电子报文和邮件、电子便签等的格式。

1.2　　与 OBEX 相关的蓝牙技术规定

蓝牙技术文本包括五个与 OBEX 及其应用有关的规定细则：

1．蓝牙 IrDA 互操作性规定，该规定

- 定义应用如何同时在蓝牙和 IrDA 之上运行；
- 定义 OBEX 如何在 RFCOMM 和 TCP/IP 之间映射；
- 定义 OBEX over BlueTooth 的应用总体要求；

2．蓝牙通用对象交换框架规范包括：

- OBEX 应用框架的一般性互操作的规范；
- 用于应用框架的协议低层（如基带和 LMP）的互操作性定义；

3．蓝牙同步应用框架规范，包括：

- 同步应用的应用框架；
- 对同步应用框架中的应用互操作性要求的定义；
- 不对基带、LMP、L2CAP、RFCOMM 的同步应用条件做出定义；

4. 蓝牙文件传输框架规范,包括:
- 文件传输应用的应用框架;
- 对文件传输应用框架中的应用互操作性要求的定义;
- 不对基带、LMP、L2CAP、RFCOMM 的文件传输应用条件做出定义;

5. 蓝牙‘推’对象框架规定,包括:
- ‘推’对象应用的应用框架;
- ‘推’对象应用框架中的应用互操作性要求的定义;
- 不对基带、LMP、L2CAP、RFCOMM 的‘推’对象应用条件做出定义;

1.3 其它的 IROBEX 执行情况

除在 IP 之上，OBEX 还应用在 IrCOMM 和 Tiny IP 上。蓝牙技术并没有像针对 OBEX 定义传输层那样定义这些协议,但它们都可以得到独立软件供应商的支持。

2. OBEX 对象和协议

本节用于描述 OBEX 对象模型和 OBEX 会话协议，并推荐参阅 IrOBEX 规范。

2.1 对象

OBEX 对象模型对 OBEX 对象做出描述。OBEX 协议能够通过‘推‘、‘拉’操作传输对象。一个对象可以通过多个‘推’请求和‘拉’应答进行交换。

该模型处理对象及其有关信息。对象由对象头组成，对象头由若干个头 ID 和包含的值组成。头 ID 描述了对象头的组成及其格式，以及头 ID 所定义的各位值的格式和含义。头一般包括计数器(Count)、名字(Name)、类型(Type)、长度(Length)、时间(Time)、描述(Description)、目的地址(Target)、HTTP 协议、主体(Body)、主体结束标志（End of Body)、宿主标识、连接 ID（ConnectionID)、应用参数（ApplicationParameter)、认证字（Authenticate Challenge)、认证应答字（Authenticate Response)、对象类别（Object Class)，以及用户自定义头。细节参见 IrOBEX 规范的 2.2 节。

2.2 会话协议

OBEX 操作采用应答-请求模式。请求由客户端发出，由服务器端应答。在发出请求之后和发出下一个新的请求之前,客户端将等待服务器的应答。每一个请求分组由一个 1 比特长的操作码、一个 2 比特的长度标识和数据组成。每一个应答分组由一个 1 比特长的应答码、一个 2 比特长的长度标识和数据组成，其数据则可有可无。

在下面章节里将对 OBEX 操作作详尽介绍。

2．2．1 连接操作

当应用第一次请求发送 OBEX 对象时，则启动一个 OBEX 会话。一个 OBEX 客户启动一次 OBEX 会话建立过程。该会话自连接请求发出开始。该请求格式如下：

表 7.1

0	1 3	4	5	7 n	
0x80 位置码	连接请求分组长度	OBEX 版本号	标志	OBEX 分组 最小长度	可选头

注释：PDU（请求和应答信息包）的比特序列格式在 OBEX 与在 IrOBEX 中一样采用大 Endian 码格式，即 MSB 在左边，LSB 在右边。

连接请求由在远程主机的 OBEX 服务器接收。服务器通过向客户端发出成功应答确认连接，通过发送其它应答信息到客户端表示建立连接失败。其应答格式为：

表 7.2

0	1 3	4	5	7 n	
应答码	连接请求分组长度	OBEX 版本号	标志	OBEX 分组 最大长度	可选头

应答码如 IrOBEX 规范 3.2.1 节中所列。第 5 和 6 字节定义了 OBEX 报文最大长度，由服务器接收。该值与长度部分不同，以便能够为客户端接收。连接请求和应答报文尺寸和格式都应一致。

连接一旦建立便始终保持激活状态，只能通过由请求/应答或失败断开，也就是说，在所有 OBEX 对象完全传输后连接也不会自动断开。

2．2．2 连接断开操作

当 OBEX 连接所需应用被关闭，或应用要改变目的主机的时候，OBEX 会话将断开。客户端将连接断开请求发往服务器。该请求格式如下：

表 7.3

0	1byte	3byte
0x81	分组长	分组头（可选）

服务器不能拒绝该请求，而且它还要发回应答，其格式为：

表 7.4

0	1byte	3byte
0xA0	应答分组长度	应答分组头（可选）

2．2．3 PUT 操作

当服务器和客户端间的连接建立之后，客户端就可以向服务器‘推’（push）对象了。‘推’请求用于推一个 OBEX 对象。该请求格式如下：

表 7.5

0	1byte	3byte
0X02 (当末位设定时为 0X82)	分组长度	分组序列

一个‘请求’可由一个或多个请求分组组成，这取决于传送对象的大小和分组尺寸。每一个‘推’请求分组都需要一个发自服务器的应答分组。组成一个 OBEX 对象的多个请求分组不能只有一个应答分组。其应答格式如下：

表 7.6

0	1byte	3byte
应答码	应答分组长度	应答头（可选）

2．2．4 GET 操作

连接在服务器和客户端间建立之后，客户端也可以从服务器拉（pull）对象。GET 操作就是用于‘拉’OBEX 对象（参见 3.3.4 节）。该请求格式如下：

表 7.7

0	1byte	3byte
0x03（当末位设定时为 0x83）	应答分组长度	以名字起始的应答分组头（可选）

对象以分组头序列方式返回，而客户端必须为每一个应答分组发送请求分组，其应答格式为：

表 7.8

0	1BYTE	3BYTE
应答码	应答分组长度	应答头（可选）

2．2．5 其它操作

其它 OBEX 操作包括设置路径（SetPath）和放弃（Abort）。在 IrOBEX 规范 3.3.5-6 节对此做出了详细解释。需要说明的是，客户端可以在每一

次应答后，甚至在请求/应答操作过程中发出放弃请求。而且，在发出放弃请求之前不必接收整个 OBEX 对象。

除了这些操作，IrOBEX 规范还可支持自定义操作，但在蓝牙技术中可不作支持。

1. OBEX OVER RFCOMM

本节阐述了 OBEX 在 RFCOMM 上的映射，该映射基于 ETSI TS07.10 的多路复用和传输层，而且它提供了对串行电缆仿真的支持。支持 OBEX 协议的蓝牙设备需满足以下要求：

支持 OBEX 的设备可以单独作为服务器、客户端或者同时作为两者；

所有同时运行在一个设备上的服务器应用应各自使用其 RFCOMM 服务器通道；

使用 OBEX 的应用（服务/服务器）能够将信息在服务搜索库中注册，不同应用框架是在框架规范文件中定义的。

3．1 RFCOMM 上的 OBEX 服务器启动

当客户端发出一个连接请求时，服务器假定已经准备好接收请求。但是，在服务器准备接收和进入侦听状态之前，应满足以下前提条件：

1．服务器应打开一个 RFCOMM 服务器通道；

2．服务器必须将其功能注册到服务搜索库；

在此之后，主机才能找到所需服务器，服务器才能对客户端请求进行侦听。

3.2 从串口接收 OBEX 包

如上所述，一个对象可以通过一个或多个 PUT 请求和 GET 应答操作进行交换，也就是说，一个对象可以由一个或多个数据分组进行传输。 然而，如果 OBEX 可以直接在串口运行，它就不会从 RFCOMM 数据分组。一个比特流则可以通过 OBEX 由 RFCOMM 仿真串口接收。

为了检测比特流中的一个数据分组，OBEX 查找是应答码还是操作码，取决于该数据分组是请求数据分组还是应答数据分组。操作码和应答码可以看作是数据分组的起始标志。OBEX 数据分组中不存在结束标志。数据分组长度信息则由操作码和应答码后的两个字节接收。因而，可以通过这样获得整个数据分组的长度，并确定两数据分组的边界。

所有未识别的数据都应被丢掉，而这会产生同步问题。但是根据 OBEX 协议的实质，这对于 RFCOMM 不是问题，反而提供了基于蓝牙的可靠传输。

3．3 连接建立

由客户端初始化一个连接。但是，在客户端能够发出第一个数据请求前，需执行下列任务：

1. 通过使用 SDP 规定中的 SD 协议，客户端必须搜索到与要建立连接服务器相关的明确信息；
2. 客户端利用搜索到的 RFCOMM 信道，建立 RFCOMM 连接；
3. 客户端向服务器发出连接请求，以建立一个 OBEX 会话。客户端如接收到服务器发出的一个成功应答，会话就可以直接建立起来。

3．4 连接断开

一个基于 RFCOMM 的 OBEX 会话可以直接通过连接断开请求断开。当客户端收到应答后，便关闭指定给 OBEX 客户的 RFCOMM 信道。

3．5 在 RFCOMM 上推、拉 OBEX 包

通过 PUT 请求在 RFCOMM 上的利用 OBEX 数据分组传输数据。应答必须在每一次请求后和下一次请求之前发出。

通过发出 GET 请求从远程主机‘拉’数据。数据分组含于 OBEX 应答数据分组。每次应答后，可以发出新的‘拉’数据请求。

2. OBEX over TCP/IP

本节阐述 OBEX 如何在 TCP/IP 上映射，并提供可靠的面向连接 OBEX 连接，本规范不对 TCP/IP 到蓝牙的映射关系进行定义。

支持 OBEX Over TCP/IP 协议的蓝牙设备必须满足以下要求：

（1）支持 OBEX 的设备可以单独作为服务器、客户端或同时作为两者；

（2）服务器 TCP 端口号 650 由 IANA 指定。该端口号应小于 1023。一般推荐使用 IANA 定义的 TCP 端口号 650。0-1023 号由 IANA 保留使用；

（3）客户端必须使用一个不在 0-1023 范围内的端口号；

（4）使用 OBEX 的客户服务器应用必须能够将明确的信息注册到服务搜索库。不同应用的信息都在框架规定中阐述。

4．1 TCP/IP 的 OBEX 服务器启动

当客户端发出一个 PUT 或 GET 请求时，服务器假定已经准备好接收请求。但是，在服务器准备接收和进入侦听状态之前，应满足以下前提条件：

（1）服务器应把 TCP 端口初始化为 650 或大于 1023 的值；

（2）服务器必须将其能力注册到服务搜索库；

在此之后，主机才能找到所需的服务器，服务器才能对客户端请求进行侦听。

4．2 连接建立

由客户端初始化一个连接。但是，在客户端能够发出第一个数据请求前，需执行下列任务：

（1）通过 SDP 规范中的 SD 协议，客户端须搜索到与建立连接服务器相关的明确信息；

（2）客户端初始化大于 1023 的 TCP 端口号相关套接字，并与服务器主机建立一个 TCP 连接；

（3）客户端向服务器发出连接请求，以建立一个 OBEX 会话。客户端如果接收到服务器发出的一个成功应答，会话可以直接建立起来。

4．3 连接断开

一个基于 RFCOMM 的 OBEX 会话可以直接通过连接断开请求断开。当客户端收到应答后，便关闭指定给 OBEX 客户的 RFCOMM 通道。

4．4 基于 TCP/IP 实现推拉 OBEX 数据

参见 3.5 节

3. 利用 OBEX 的蓝牙应用概述

蓝牙 SIG（专业兴趣小组）定义了三种不同的 OBEX 应用框架。本节就对这些框架进行简要介绍。

5.1 同步

同步就是通过比较和调整两个对象存储的时钟操作并使之一致。支持同步的蓝牙设备可以是 PC、笔记本电脑、PDA、移动电话和无绳电话。

蓝牙同步框架面向兼容于 IrMC 同步(IrDA 制定)的服务器和客户应用。蓝牙同步服务器和客户支持 IrMC 规定的 LEVEL 4 同步功能。在客户端设备上实现同步运算的同步引擎机制可以根据实际情况制定。这一点由软件服务商所提供，而不列入蓝牙标准。

同步服务不只限于一种类型的应用。蓝牙同步服务(IrMC 同步)支持四种不同的服务类型：

（1）通讯录——提供管理通讯录的服务；

（2）日历——便于用户对日程和任务进行管理。

（3）发消息——管理用户信息，如 EMAIL；

（4）记事本——管理用户短信息；

蓝牙同步标准的互操作要求在同步标准和通用对象交换框架标准中进行定义。

5．2 文件传输

文件传输标准用于向蓝牙设备发送和从蓝牙设备接收通用类型文件。文件传输服务支持浏览远程蓝牙设备文件夹。

蓝牙文件传输标准的互操作性要求在文件传输标准和通用对象交换标准规范中进行定义。

5．3 对象‘推’操作

对象推操作标准是用于发送对象和有选择地'拉'缺省对象的文件传输标准的特例。它可以提供业务卡片交换等服务。

蓝牙对象‘推’操作框架的互操作性要求,在对象推操作标准和通用对象交换标准规范中进行定义。

4. 参考文献

5. 同义词和缩写

GEOP 通用对象交换框架
IrDA 红外线数据协会
IrMC Ir 移动通信
L2CAP 逻辑链路控制协议及其修正
LSB 最低位
MSB 最高位
OBEX 对象交换协议
PDU 协议数据单元
RFCOMM 基于 ETSI TS07.10 的串行电缆仿真协议
SD 服务搜索
SDP 服务搜索协议
SDDB 服务搜索数据库
TCP/IP 传输控制协议/网间网协议

第 8 章　电话控制协议控制

TCS 二进制

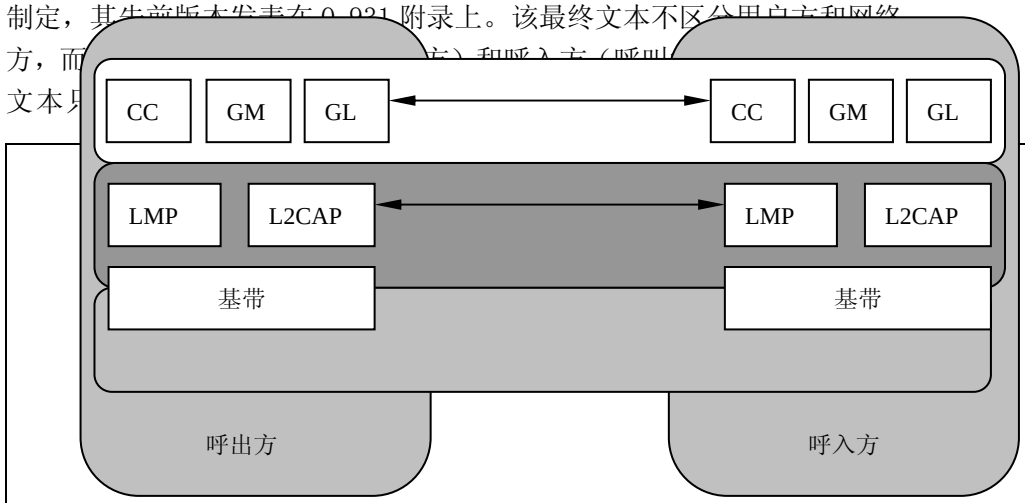
本文件采用面向比特的二进制协议规范,描述了蓝牙电话控制协议二进制规范(TCS 二进制)。该协议定义用于在蓝牙设备间建立语音会话和数据呼叫的呼叫控制信号，以及用于处理蓝牙 TCS 设备的移动管理过程。

目　录

1. 概 述

1.1 概述

蓝牙电话控制二进制协议（TCS 二进制）规范基于 ITU-T 推荐书 Q.931 制定，其先前版本发表在 Q.931 附录上。该最终文本不区分用户方和网络方，而[illegible]方）和呼入方（呼叫[illegible]文本只[illegible]



Q.931 的内容。

图 8.1 蓝牙栈中的 TCS

TCS 包括以下功能：

• 呼叫控制（CC）——指示蓝牙设备间语音会话和数据呼叫的建立和释放；
• 组管理——方便蓝牙设备组的处理
• 无连接 TCS（CL）——与非正在进行的呼叫进行相关信号信息交换的条款；

1．2 设备间操作

TCS 采用点到点通信和点到多点的通信模式。在已知要建立呼叫的目标蓝牙设备的情况下，使用点到点信号。如果有多个可用于建立呼叫的目标蓝牙设备，可使用点到多点信号。例如对于一个呼入信号，本地基站需要唤醒本地所有通话。

点对点信号映射于一个面向连接的 L2CAP 通道，点到多点信号映射于无连接的 L2CAP，但后者在匹克广播通道上以广播信息的形式发送。

图 1.2 图示了点对点信号在单点配置方式下建立语音和数据呼叫的过程。首先，利用点对点信道 A 通知另一个设备有呼叫请求。第二步，在该信道上建立语音会话或数据信道。

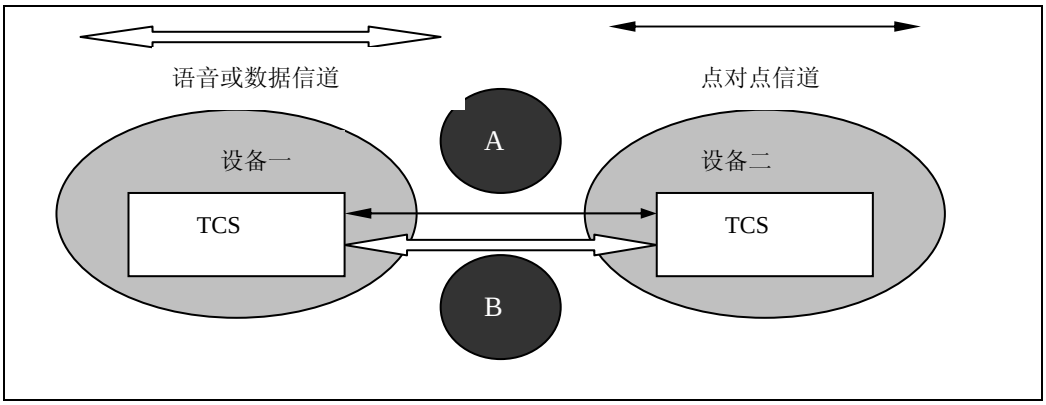


图 8.2 单点配置中点到点信令

图 1.2 表现了利用点到多点信号和点对点信号在多点配置上如何建立话
语音会话或数据通道
利
点对点信令通道
知
点对多点信令通道
叫请求。第二步，在该信道上建立会话或数据信道。

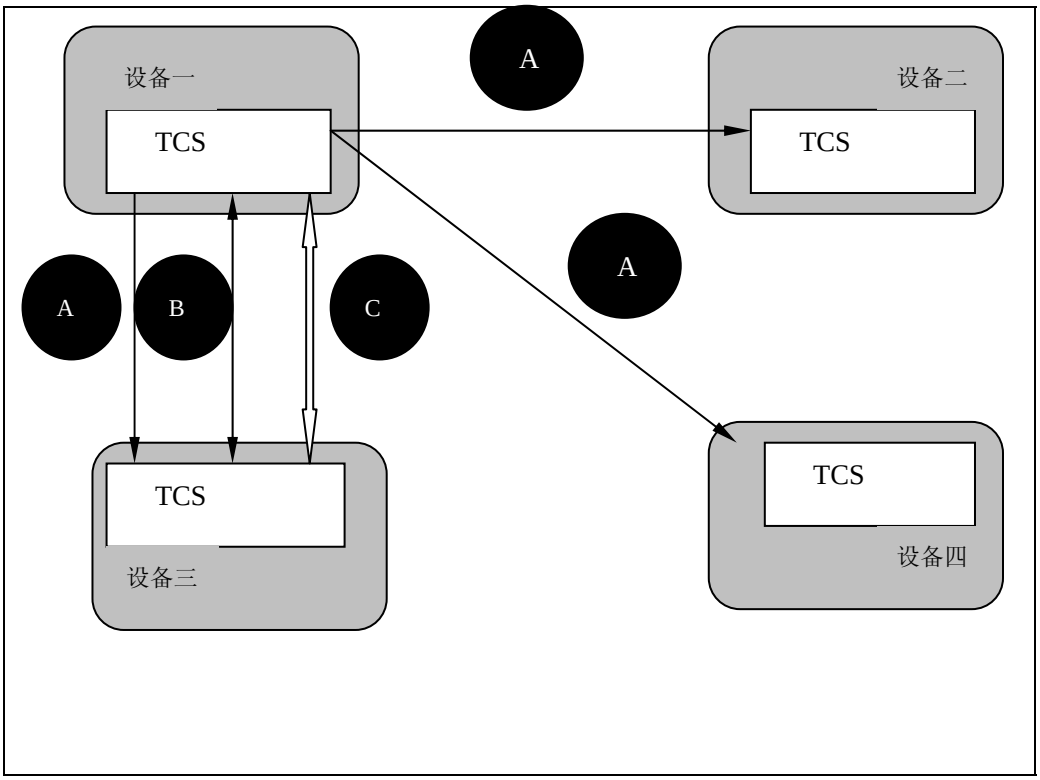


图 8.3 多点配置信令

1.3 层间操作

TCS 的执行版本在下图中通用体系结构中描述（为了简化，数据呼叫处理没有画入）。

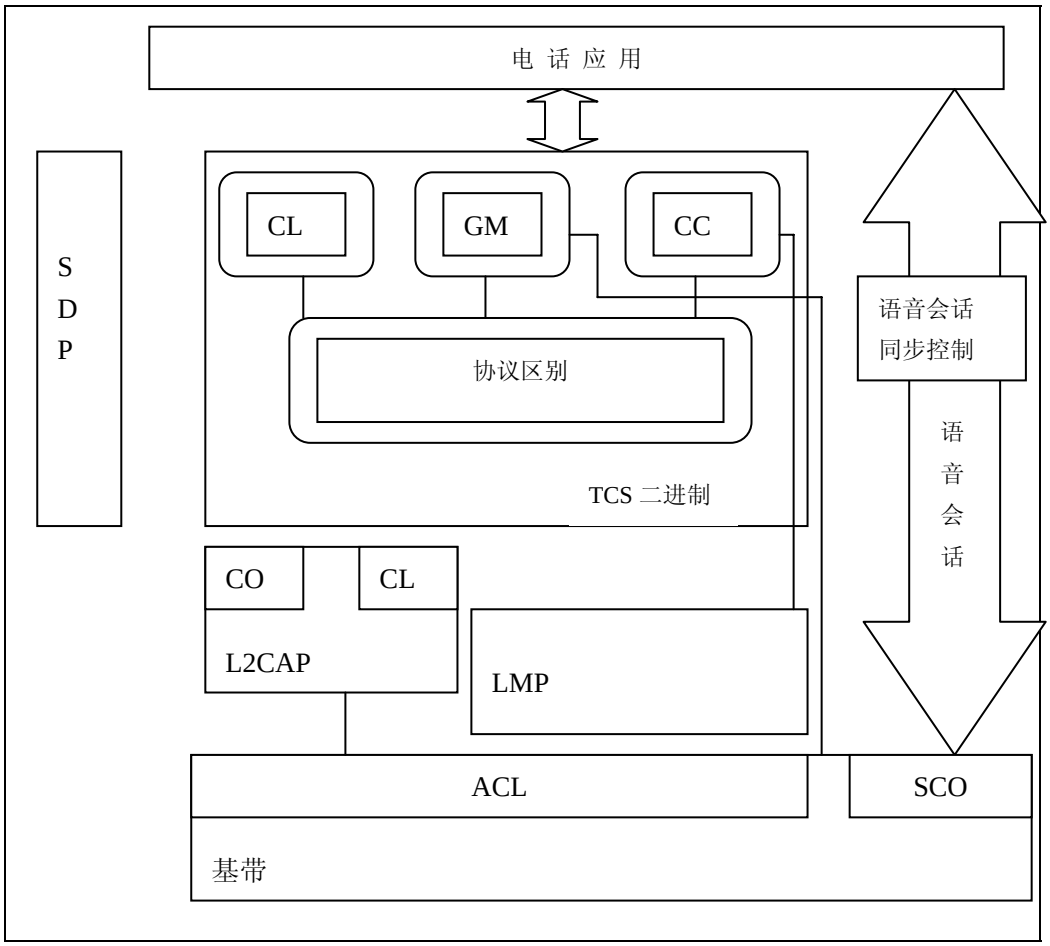


图 8.4 TCS 体系结构

二进制 TCS 内部结构包括功能实体呼叫控制、组管理和无连接。作为补充还包括 TCS 内部协议识别码不同的协议，以及到功能实体的路径流量控制。

为处理更多的并发呼叫，可以同时存在二进制 TCS 的多个实例。各实例之间根据 L2CAP 通道标识相互区别。

二进制 TCS 为多个蓝牙实体提供接口，以向应用提供电话服务。该接口如图 4.1 所示。信息通过这些接口交换，以实现：

A. 当连接到会话路径时，呼叫控制实体向会话同步控制提供信息。该信息基于呼叫控制信息,如接受连接确认指令（CONNECT ACKNOWNLEDGE）和连接断开指令（DISCONNECT）。

B. 利用点到多点通信发送 SETUP 报文(见 2.2.2 节),通过 L2CAP 接口在无连接通道中进行传输,并利用该接口通知 TCS 已收到利用无连接通道传输的 SETUP 报文。无连接的 L2CAP 信道映射于匹克广播通道；

C.无论何时利用点对点通信发出 TCS 报文,该报文都是通过 L2CAP 接口在面向连接通道上进行传输。在 L2CAP 信道建立过程中,必须指定连接服务质量，特别是节能模式的使用（L2CAP 将接口 F 有关信息通知 LMP）。

D.为了建立和释放 SCO 链接，呼叫控制实体应直接控制 LMP；

E 和 G. 组管理实体为了在初始化过程中控制查询、呼叫访问和匹配而直接控制 LMP 和 LC/基带。

2. 呼叫控制（CC）

2．1 呼叫状态

对于用户端，TCS 使用的呼叫状态在 Q.931[1]中定义。对于 TCS，由于计算资源限制，只要求使用该状态集的一个子集。该子集命名为**精简 TCS**。

该协议集如下，其中黑体字是精简 TCS 的硬性规定部分。

通用状态：

Null(0) 空状态

Active(10) 激活状态

Disconnect request(11) 连接断开请求

Disconnect indication(12) 连接断开指示

Release Request(19) 释放请求

呼出端状态：

Call Initiated (1) 初始化呼叫

Overlap sending (2) 重发

Outgoing call proceeding (3) 呼叫进行

Call delivered (4) 呼叫转发

呼入端状态:

Call present(6) 正在呼叫

Call received(7) 接受状态

Connect request(8) 连接请求

Incomming Call proceeding (9) 呼入呼叫正在进行

Overlap receiving(25) 重复接收

这些状态及它们之间的转换都在附录 1——TCS 呼叫状态中阐述。为了描述清楚，精简 TCS 对各状态信息又分别给予解释。

2．2 建立呼叫

面向连接的 L2CAP 必须在呼叫控制程序开始运作之后,在呼出端和呼入端之间建立通道。而且，在多点配置当中，必须在呼出端和呼入端之间

建立无连接 L2CAP 通道。

2．2．1 呼叫请求

发送端通过发送 SETUP 报文和启动 T303 定时器初始化呼叫。

在点对点配置情况下，通过面向连接的通道传输 SETUP 报文。

在多点配置情况下，通过无连接通道传输 SETUP 报文。而该 SETUP 报文在每一结点上以广播报文形式传输。

如果在 T303 定时器失效之前,没有收到从呼入端发回的应答报文，呼出端：

（1）如果 SETUP 报文通过无连接通道传输，将返回 NULL 状态。中止传输 SETUP 报文。

（2）如果 SETUP 报文通过面向连接的通道传输，将向呼入端发送 RELEASE COMPLETE 报文。该报文将包括#102 号事件 recovery on timer expiry（当定时器失效时恢复）；

SETUP 报文通常包括呼叫类别，以及呼入端需要的所有信息。如果被呼叫方号码信息位数不够，则需要重新发送。SETUP 报文将包括完整的号码信息。

在 SETUP 报文发送之后，呼出端则进入呼叫初始化（Call Initiated）状态。呼入方在接收到 SETUP 报文后进入正在呼叫（Call present）状态。

2．2．2 选择信道类别

在呼叫请求中发送的 SETUP 报文可以包括信道容量信息元，以表示被请求信道。接收方通过 SETUP 报文的第一个应答报文中包含信道容量信息对被请求信道进行协商。

信道容量信息元表示如何在呼叫中利用低层资源（信道）。如果信道为‘同步面向连接’（SCO）类别，将采用 SCO 链路，并使用给定数据分组类别和用于语音会话呼叫的语音编码。如果信道为‘异步无连接’（ACL）类别，将使用 ACL 链路。在此之上是用于数据呼叫的具有 QoS 要求的 L2CAP 通道。如果信道类别信息为‘NONE’，就不会建立单独的信道。

注：本规范负责确认信道容量可用于该呼叫。

2．2．3 重复发送

如果接收到的 SETU 报文不包括发送完成指示信息元，并存在以下两种情况中的一种：

a)被叫号码信息不完整；

b)呼入方不能确认被叫号码信息完整；

那么，呼入方将启动定时器 T302，并向呼出方发送 SETUP ACKNOWLEDGE 报文，并进入重复接收状态。

当接收到 SETUP ACKNOWLEDGE 报文时，呼出方将进入重复发送状态，并中止定时器 T302，而启动定时器 T304。

在接收到 SETUP ACKNOWLEDGE 报文后，呼出方将采用被叫号码发送其余信息。该信息可以是一条或多条 INFORMATION 报文。

当每条 INFORMATION 报文发出时，呼出方将重新启动定时器 T304。

完成信息发送任务的最后一条 INFORMATION 报文将包括一个发送结束标志。如果呼入方不能确定被叫号码是否完整，那么将在接收到每一条不包含发送结束标志的 INFORMATION 报文时重新启动定时器 T302。

在定时器 T304 失效时，呼出方将初始化呼叫清除过程。该过程同时触发#102 事件。

在定时器 T302 失效时，呼入方：

- 当呼入方无法确认呼叫信息是否完整时，将初始化呼叫清除过程，并触发#28 事件非法号码格式。
- 否则，呼入方将回复一个 CALL PROCEEDING ALERTIN 或 CONNECT 报文；

2.2.4 呼叫进行

2.2.4.1 进行整块发送

如果使用整块发送(如呼入方能够确定它从呼出方接收到的 SETUP 报文中包含了全部建立呼叫所需信息)，呼入方就会向呼出方发送一个 CALL PROCEEDING 报文，以确认收到 SETUP 报文和表示呼叫正在进行。当收到 CALL PROCEEDING 报文时，呼出方就进入呼出呼叫进行状态，并中止定时器 T302，启动定时器 T304。发送 CALL PROCEEDING 报文后，呼入方就会进入呼入呼叫进行状态。

2.2.4.2 呼叫进行，重复发送

当以下情况发生时：

- 呼入方接收到报文发送完毕指示；
- 呼入方认为所有影响呼叫建立的呼叫信息都已收到；

呼入方就会向呼出方发送一个呼叫进行报文，并中止定时器 T302，进入呼入呼叫进行状态。

当收到 CALL PROCEEDING 报文时，呼出方就进入呼出呼叫进行状态，并中止定时器 T304，如果可能将启动定时器 T302。

2.2.4.3 定时器 T310 失效

定时器 T310 失效时，如呼出方没有收到 ALERTING、CONNECT、DISCONNECT 或 PROGRESS 报文时，呼出方将按照 2.3.1 节中的#102 事件“定时器失效时恢复”初始化呼叫清除。

2．2．5 呼叫确认

当呼入方接收到被叫地址上的用户报警时，就会发出 ALERTING 报文，并进入呼叫接收状态。当呼出方接收到 ALERTING 报文时，呼出方将启动一个内部生成的报警指示，并进入呼叫传递状态。呼出方将启动定时器 T304，以避免重复发送，中止定时器 T303 或 T310（如果正在运行），启动定时器 T301（如果没有另一内部报警优先级更高的定时器时）。

T301 定时器失效时，呼出方将按照 2.3.1 节中的#102 事件“定时器失效时恢复”初始化呼叫清除。

2．2．6 呼叫连接

呼入方通过向呼出方发送 CONNECT 报文和中止用户报警表示接受呼入呼叫。当发送 CONNECT 报文时，呼入方将启动定时器 T313。

当接收到 CONNECT 报文时，呼出方将中止任一个内部生成的报警信息，中止定时器 T301、T303、T304 和 T310，建立到呼出方的被叫信道，并发送连接确认报文和进入激活（Active）状态。

CONNECT ACKNOWLEDGE 报文标志被叫信道的建立。当收到 CONNECT ACKNOWLEDGE 报文，呼入方将连接到信道，中止定时器 T313，并进入激活状态。

收到 CONNECT ACKNOWLEDGE 报文之前且时钟 T313 失效时，呼入方将按照#102 事件“定时器失效时恢复”初始化呼叫清除。

2．2．7 呼叫信息

处于激活状态时，发送方和接收方可以交换与当前呼叫有关的信息，该呼叫使用信息（INFORMATION）报文。

2．2．8 主动的用户清除

当在多点配置的无连接信道上传输呼叫时，除了向呼入方发送 CONNECT ACKNOWLEDGE 报文，呼出方还要向其它为应答 SETUP 报文而发送 SETUP ACKNOWLEDGE、CALL PROCEEDING、ALERTING 或 CONNECT 报文的呼入方发送 RELEASE 报文。该 RELEASE 报文通知这些呼入方将不再向它们提供呼叫。

2．2．9 带内语音和广播

当呼入方提供带内语音和广播，并且如果被呼叫信道正在进行语音呼叫，呼入方将首先立即建立信道。然后，则与带内语音和广播同时发送进度指示#8 带内信息或合适模式(in-band informatio or appropriate pattern)。该进度指示也可以包含在任一允许包含进度指示信息元的控制报文中，或者在呼叫状态没有变化的情况下也可包含在 PROGRESS 报文中。

当收到该报文后,呼出方就可以连接到通信通道以接收带内语音/广播信息。

2．2．10 呼叫建立失败

在当前呼叫中如果有重复接收、呼叫进行或呼叫已接收状态的情况，呼入方将初始化呼叫清除过程。下面的值将在重复接收、占线情况下中止当前呼叫：

#1 未分配的号码
#3 无到目的地址的路径
#17 用户忙
#18 无用户应答
#22 号码改变
#28 非法号码格式（非完整号码）
#34 无可用回路/信道
#44 无可用被请求回路/信道
#58 当前无可用信道容量
#65 当前无信道容量

当呼入方处于呼叫已接受状态时，清除当前呼叫可使用下列事件值:

#19 无来自用户的回答（提醒用户）
#21 用户拒绝呼叫

2.2.11 呼叫建立报文流

下图提供了在成功建立呼叫过程中交换信息的完整视图。其中，实线表示精简 TCS 的一部分，即必需的报文；虚线表示可选报文，三角形表示正在运行的定时器。

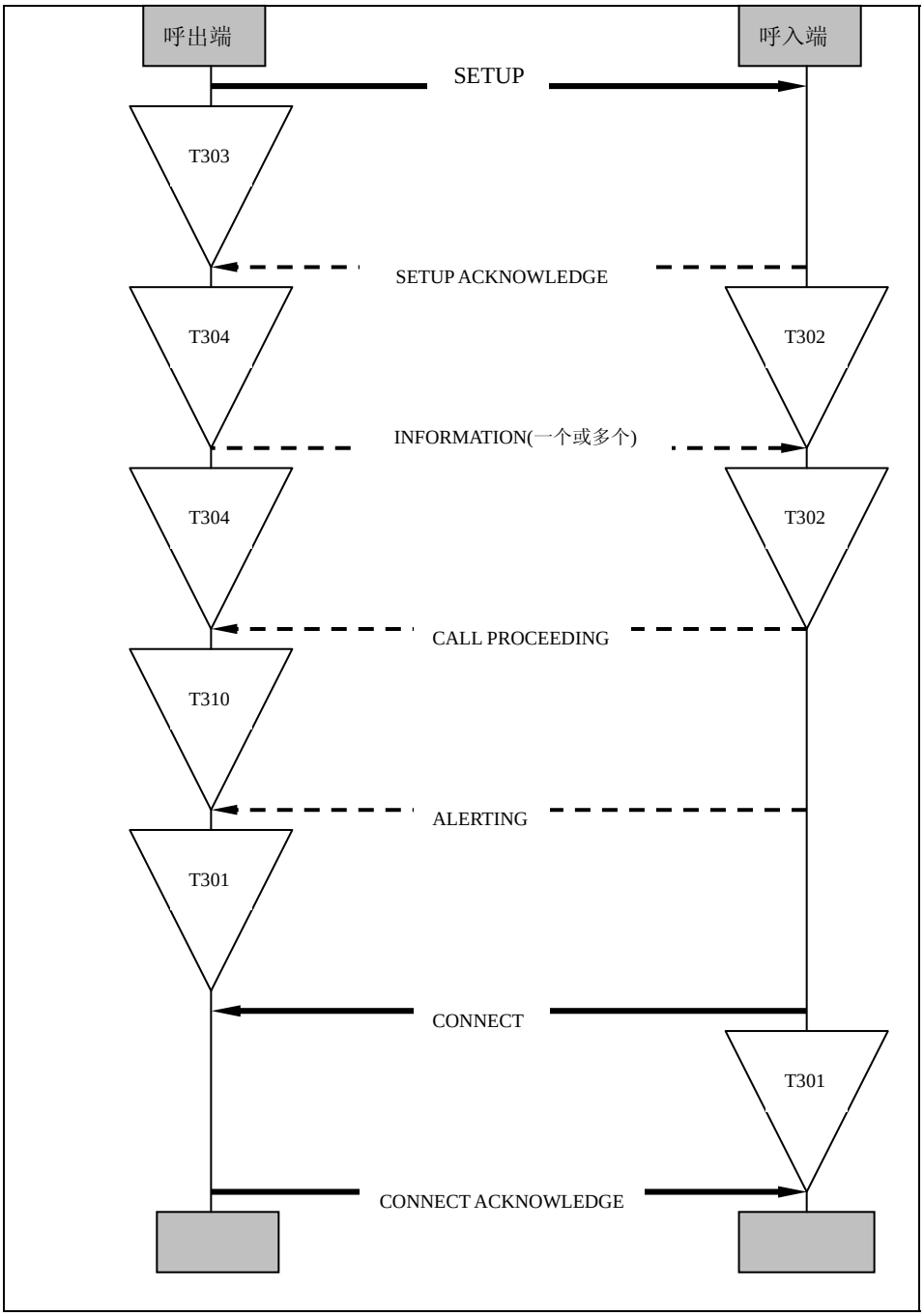


图 8.5 建立呼叫报文流

2．3 呼叫清除

2.3.1 正常呼叫清除

除在下节说明的例外情况以外,呼出方和呼入方都可以启动呼叫清除过程。为了叙述清楚，下面只对呼出方初始化呼叫清除过程进行描述。

当发送或接收到任何呼叫清除报文,应终止除了 T305 或 T308 以外的协议定时器。

呼出方通过发送 DISCONNECT 报文，启动定时器 T305，从信道断开，进入请求断开状态，从而初始化呼叫清除过程。

呼入方将在接收到 DISCONNECT 报文时进入断开指示状态。该报文通知呼入方断开与信道的连接。一旦用于呼叫的通道被断开，呼入方将向呼出方发送 RELEASE 报文，启动定时器 T308，并进入释放请求状态。

接收到 RELEASE 报文后，呼出方将取消定时器 T305，释放占用信道，发送 RELEASE COMPLETE 报文，返回 NULL 空状态。

从呼出方接收到 RELEASE COMPLETE 报文后，呼入方将终止定时器 T308，释放占用信道，返回 NULL 空状态。

如果呼出方在定时器 T305 失效之前没有收到应答 DISCONNECT 报文的 RELEASE 报文，它将向呼入方发送包含 DISCONNECT 报文中呼叫号码的 RELEASE 报文，启动定时器 T308，进入释放请求状态。

如果一方处于 Release request 释放请求状态，且没有在定时器 T308 失效之前收到 RELEASE COMPLETE 报文，它将返回 NULL 空状态。

由采用自定义语音/广播信息的被叫用户执行的呼叫清除：

除了上述呼叫清除过程以外，如果被请求信道正在进行语音呼叫，呼出方将在呼叫清除阶段采取带内语音/广播信息。当提供了带内语音/广播信息时，呼出方将终止占用信道（如果该信道未使用），然后发送包含进度指示#8 带内信息或合适模式的连接断开报文。

接收到该报文后,呼入方就可以接入信道并接收带内语音/广播信息并进入连接断开指示状态。

呼入方在收到呼出方发出的 RELEASE 报文之前，将通过与信道断开连接，启动定时器 T308，进入释放请求状态来进行呼叫清除过程。

2．3．2　非正常呼叫清除

正常情况下，呼叫清除由发送 DISCONNECT 报文的任何一方进行初始化，其过程在上节中进行定义。上述规则的唯一例外如下所列：

A）为应答 SETUP 报文，呼入方可以因为无可用资源等原因而拒绝呼叫。如果没有其它应答信息发出的话，拒绝呼叫过程通过发送 RELEASE COMPLETE00 报文实现，然后呼入方进入 NULL 空状态。

B）在多点配置情况下，可以通过呼出方发出的 RELEASE 报文进行非用户主动选择的呼叫清除；

C）在多点配置情况下，SETUP 报文通过无连接通道发送。如果呼入方在呼叫建立过程中接收到远程呼叫用户的断开指令，无论呼入方已经应答还是正要应答，呼叫都将被 RELEASE 报文清除掉，呼叫清除过程如上节所述。呼出方将在呼叫清除过程完成后进入 NULL 空状态；

2．3．3 清除冲突

当呼入方和呼出方同时发出 DISCONNECT 报文时将发生清除冲突。当任一方在连接断开请求状态下收到 DISCONNECT 报文时，该方将中止定时器 T305，如果信道连接没有断开就断开信道连接，并发送 RELEASE 报文，启动定时器 T308，进入释放请求状态。

清除冲突也有可能在呼叫双方同时发送 RELEASE 报文时发生。处于释放请求状态和接收到 RELEASE 报文的实体将终止定时器 T308，释放信道，并进入 NULL 空状态，而不再需要发送 RELEASE COMPLETE 报文。

2．3．4 呼叫清除报文流

下图提供正常呼叫清除情况下报文交换的完整视图。所有的报文都是强制要求的：

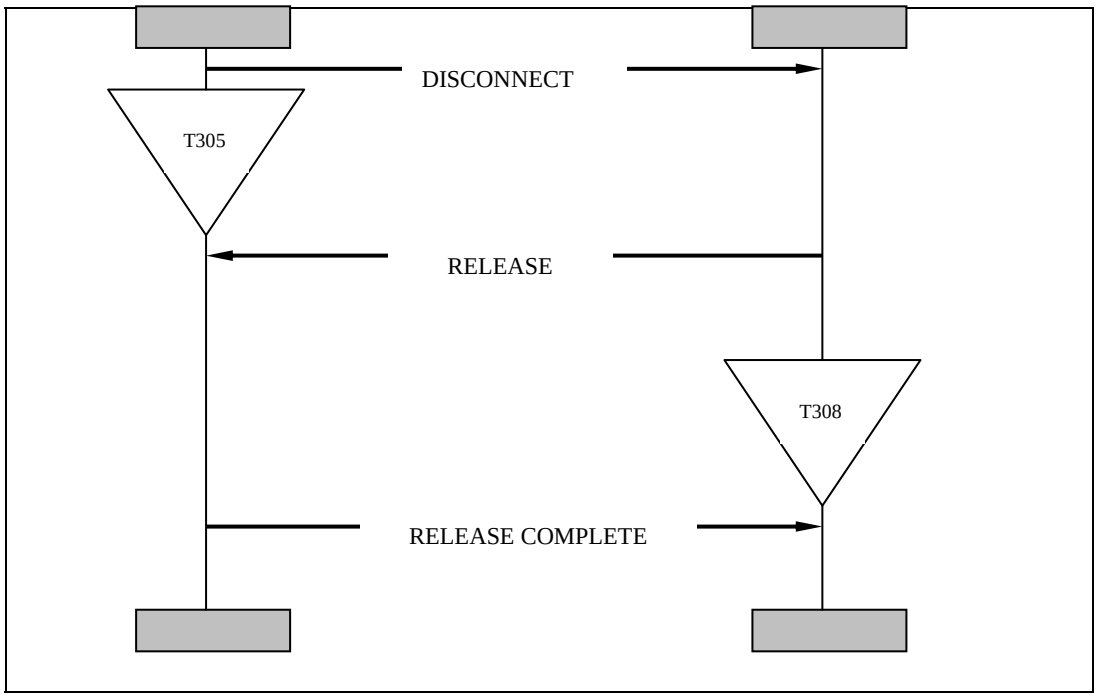


图 8.6 呼叫清除报文流

3. 组管理（GM）

3．1 概述

组管理实体提供了管理一组设备的程序，如下所述：

- 获取访问权限，使被请求设备能够使用组里其它设备的电话服务；
- 配置分布，使处理和操作一组设备成为可能；
- 组员间快速访问，实现同组设备间的快速通信；

在任一组管理过程实现之前，应首先建立设备间面向连接的 L2CAP 通道。

对于小组管理，将使用无线用户组（WUG）的概念。

无线用户组（WUG）

3．2．1 描述

一个 WUG 由多个支持 TCS 的蓝牙单元组成。其中一台设备称为 WUG 管理员。WUG 管理员实质就是一个典型的网关，以提供给组内其它蓝牙设备——称为 WUG 成员——访问外部网络的能力。所有范围内 WUG 成员都是一个激活或休眠的匹克网成员。该匹克网管理员通常也就是 WUG 管理员。

WUG 主要的特点是：

- 所有 WUG 内的单元互相都知道谁是 WUG 管理员，谁是 WUG 成员。所有的 WUG 成员都从 WUG 管理员那里接收到这些配置信息；
- 当一个新的单元能够与 WUG 管理员通信时，它也能够与其它任一个 WUG 成员通信和进行身份验证与加密，而不需要进一步的匹配/初始化。WUG 管理员为各成员提供必要的身份验证和加密参数。

所有有关特性都通过配置分布过程进行维护。

3．2．2 WUG 中的加密

为在无连接L2CAP通道上进行加密传输，WUG管理员发布了一个临时关键字（K_{master}）。因为一个蓝牙单元不能够在两个或多个加密字之间实时切换，该关键字通常也能够在面向连接通道上进行加密传输。该通道实行单独编址通信。由于WUG管理员将可能不间断地进行周期操作，因此K_{master}将进行周期变动。

为了允许不同 WUG 成员间进行身份认证和加密，WUG 管理员将使用配置分布发放链接关键字，以使 WUG 成员能够用来相互通信。建立通信的两个 WUG 成员之间只能使用唯一的链接关键字。

配置分布通常通过加密链接进行。因此与其说K_{master}用于加密，不如说是给已知地址的WUG成员使用的类似于参数的关键字。

3．2．3 随机匹配

对于 TCS，与 WUG 管理员匹配也就意味着与所有 WUG 成员匹配。这一点通过配置分布实现。同时，这也避免了该外部设备分别与 WUG 中的每一成员单独匹配。

在蓝牙中，匹配不只是与特定服务匹配，同时也是与特定设备匹配。建立匹配关系后，如果没有禁止特定的应用或设备，则可以访问所有由该设备提供的服务。

如果没有其它的问题，将一个设备与 WUG 管理员匹配，也就意味着该设备提供的所有服务可以由所有 WUG 成员访问。反之亦然，该设备也可以访问所有 WUG 成员提供的所有服务。

因此，在使用 TCS——特别是配置分布——时，建议加入以下规范条款：

1）一个进入 WUG 的新的设备，不必通过初始化获取访问权限过程而成为该 WUG 的成员，而只要能够使用由 WUG 管理员提供的服务就可以了；

2）WUG 管理员可以拒绝一个要求获得访问权限的请求；

3）WUG 成员在配置分布过程中不必接收配对信息；

这些要求不只应用于提供 TCS 相关服务的设备。

3．3 获取访问权限

利用获取访问权限过程，一个设备能够获得使用另一个 WUG 设备电话服务的权限。

3．3．1 过程描述

一个设备通过发送 ACCESS RIGHTS REQUEST 报文和启动定时器 T401 来请求访问权限。接收方设备在接收到 ACCESS RIGHTS REQUEST 报文后，通过发送 ACCESS RIGHTS ACCEPT 报文接受请求。

请求方设备接收到 ACCESS RIGHTS ACCEPT 报文时，启动定时器 T401。这样，整个访问权限过程就成功完成。

如果定时器 T401 失效前没有收到应答，请求方设备将重新考虑访问权限请求。

如果在收到 ACCESS RIGHTS REQUEST 报文时，接收方设备由于某种原因不能接受访问权限，它将应答 ACCESS RIGHTS REJECT 报文，请求方设备也将终止定时器 T401 并重新考虑访问权限请求。

3．3．2 报文流

下图提供在获取访问权限过程中交换报文的完整视图

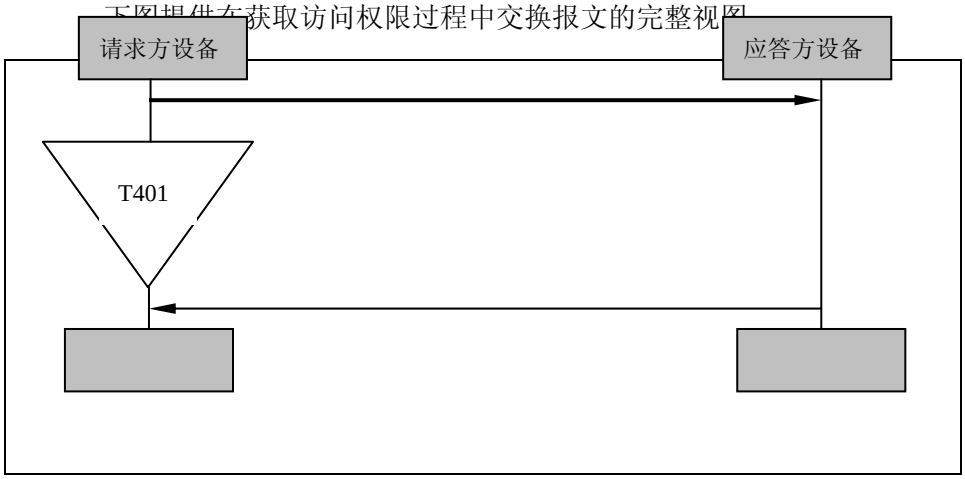


图 8.7 获取访问权限报文流

3．4 配置分布

WUG 中发生的诸如添加或删除一个单元等变化都需要随时通知 WUG 中所有单元。配置分布即用于交换该数据。

当发生 WUG 配置变动时，WUG 管理员将启动每一 WUG 成员的配置分布过程。WUG 管理员将追踪任何一个被通知到 WUG 配置发生变动的 WUG 成员。

可能会有一些 WUG 成员在通信范围之外而未被通知到，但当它们重新与 WUG 管理员建立关联后将更新这些成员。

3．4．1 过程描述

WUG 管理员通过启动定时器 T403 和发送 INFO SUGGEST 报文初始化配置分布过程。INFO SUGGEST 报文包含完整的 WUG 配置信息。收到 INFO SUGGEST 报文后，WUG 成员将发送 INFO ACCEPT 报文，以确认收到明确的 WUG 配置信息。

当 WUG 管理员收到 INFO ACCEPT 报文后，将终止定时器 T401，从而成功完成配置分布过程。在定时器 T403 失效后，配置分布过程也将被终止。

3.4.2 报文流

下图即给出了在配置分布情况下进行消息交换的完整视图.

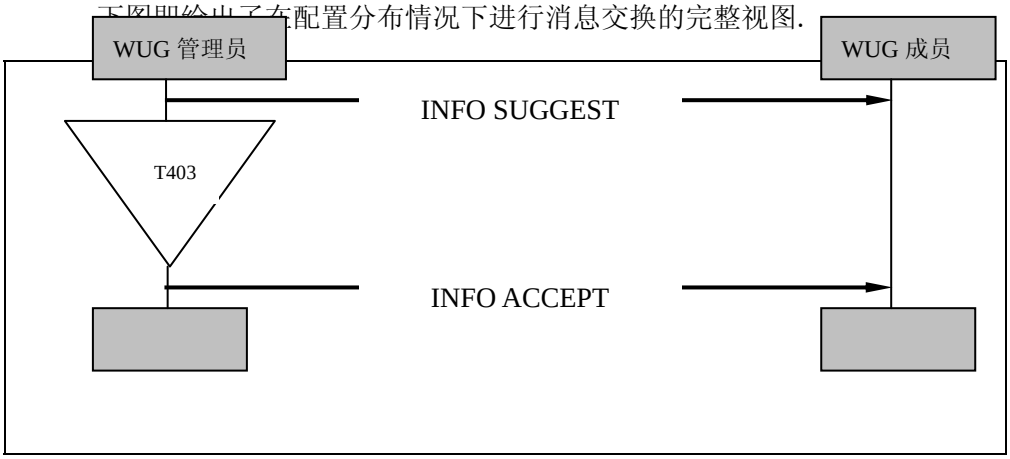


图 8.8 配置分布报文流

3.5 成员间快速访问

当WUG主匹克网中的两个成员都处于激活状态时,其中一个WUG成员就能够使用成员间快速访问过程快速访问另一方。通过成员间快速访问过程，宿主成员将从目的方获取时钟信息，并强制目的方在指定时间（T406）内进入 PAGE_SCAN 状态。

3．5．1 请求侦听

宿主 WUG 成员通过启动定时器 T404 和向 WUG 管理员发送 LISTEN REQUEST 报文，指出希望建立联系的 WUG 成员，从而初始化成员间快速访问过程。

在定时器 T404 失效前，宿主方如果没有收到 LISTEN REQUEST 的应答报文， 将终止该成员间快速访问过程。

3．5．2 接受侦听

收到LISTEN REQUEST报文时,WUG管理员会判断出被访问一方是否WUG成员。如果是,WUG管理员就会通过启动定时器T405,向目的方发送LISTEN SUGGEST 报文，从而初始化成员间快速访问。

当收到 LISTEN SUGGEST 报文时，目的 WUG 成员将通过向 WUG 管理员发送 LISTEN ACCEPT 报文确认该内部呼叫。该报文包括目的 WUG 成员的时隙信息。发送 LISTEN ACCEPT 报文后，目的 WUG 成员将进入呼叫扫描状态，持续 T406 时长，从而由宿主 WUG 成员建立连接。

收到 LISTEN ACCEPT 报文时，WUG 管理员终止定时器 T405，同时通过发送 LISTEN ACCEPT 报文通知宿主 WUG 成员成员间快速访问的结果。LISTEN ACCEPT 报文包括目的 WUG 成员的时隙信息。收到 LISTEN ACCEPT 消息时，宿主 WUG 成员将终止定时器 T404，并开始呼叫目的 WUG 成员。

定时器 T405 第一次失效前，如果 WUG 管理员没有收到 LISTEN SUGGEST 报文的应答报文，WUG 管理员将利用#102 事件，通过向宿主方和目的方 WUG 成员发送 LISTEN REJECT 报文，终止成员间快速访问过程。

3．5．3 由 WUG 管理员执行的侦听拒绝过程

如果 WUG 管理员拒绝成员间快速访问过程，它就会向宿主 WUG 成员发送 LISTEN REJECT 报文。

合法事件值为:

#1,Unallocated(unassigned)number(当给定 WUG 成员并非 WUG 成员时使用)

#17,User busy(在目的 WUG 成员正与外部呼叫关联时使用)

#20,Subscriber absent(在与目的 WUG 成员建立关联失败时使用)

以及,任一由目的 WUG 成员发出或接收到的 LISTEN REJECT 报文中包括的事件值。

收到 LISTEN REJECT 报文时，宿主 WUG 成员将终止定时器 T404，并中止该过程。

3．5．4 由 WUG 成员执行的侦听拒绝过程

如目的 WUG 成员拒绝了收到的 LISTEN SUGGEST 报文中的建议动作，它就会向 WUG 管理员发一则 LISTEN REJECT 报文。合法事件值为#17“用户忙”。

接收到 LISTEN REJECT 消息时，WUG 管理员终止定时器 T405。

3．5．5 报文流

下图提供了在内部成员快速访问过程中交换报文的一个视图。成功的内部成员快速访问过程终止于目的 WUG 成员进入呼叫扫描状态时，以便允许目的 WUG 成员直接访问它。

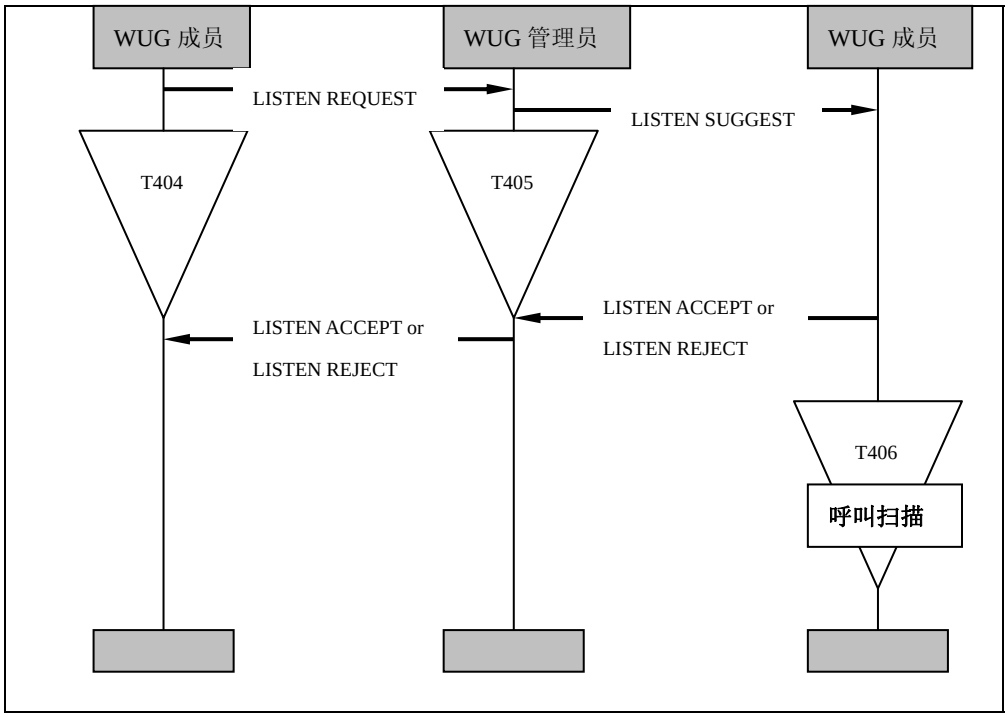


图 8.9 内部成员快速访问报文流

4. 无连接 TCS（CL）

无连接 TCS 报文不需要建立 TCS 呼叫就能够用来交换信号信息。这也是一个 TCS 提供的无连接服务。

一个无连接 TCS 报文就是一个 CL_INFO 报文（参见 6.3.1 节定义）。

发送 CL_INFO 报文之前，可以利用呼出方和呼入方间的面向连接的 L2CAP 通道；

注:面向连接通道可以推迟通道终时间，以获得更多时间交换更多的 CL INFO 报文。

在多点配置中，CL_INFO 发送前，可以利用无连接的 L2CAP

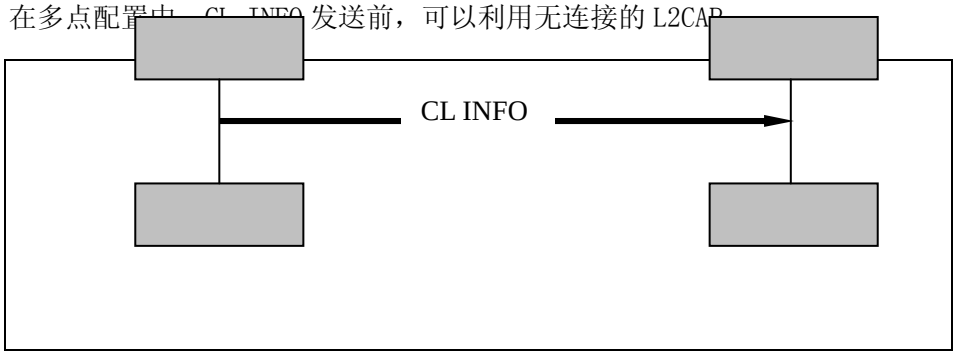


图 8.10 无连接 TCS 报文流

5. 补充服务（SS）

TCS 只明确提供一种补充服务，即呼叫线路识别。

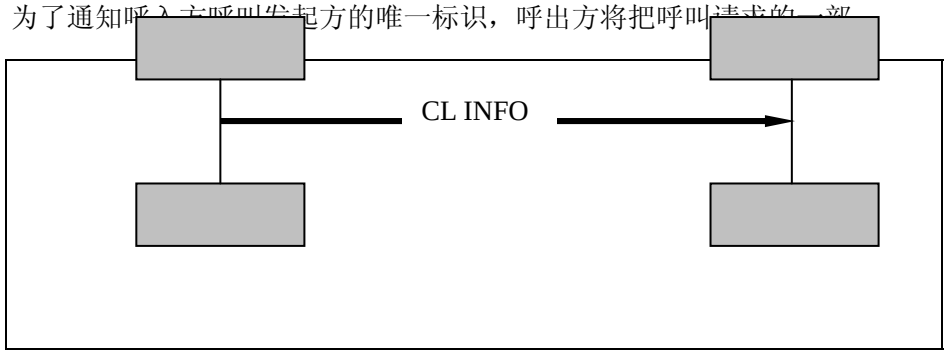
对于外部网络提供的补充服务，可以利用 DTMF 序列实现附加服务的激活/失效和查询，支持 DTMF 启动/终止过程（见 5.2 节）。该过程支持完整和不完整的语音长度。、

5.3 节阐述如何支持由外部网络提供的某一附加服务，该服务称为注册重呼。

本节没有定义其它的附加服务控制方式。该服务控制方式可以利用服务呼叫，或者厂商指定信息元，或者二者兼而有之，进行识别。

5．1 呼叫线路识别

为了通知呼入方呼叫发起方的唯一标识，呼出方将把呼叫请求的一部



分——主叫号

图 8.11 呼叫线路识别报文流

码信息单元包含在传输的 SETUP 报文中。

5．2 DTMF 启动和终止

DTMF 启动和终止过程支持在 PSTN 网络上提供补充服务控制。

从 DTMF 原理上说，报文可以由呼入和呼出中任一方接收，但实际应用当中，一般都是由接入外部网络的一方（网关）接收。

DTMF 报文只能在呼叫激活状态下进行传输，语音生成过程在呼叫断开时也将终止。

5.2.1 启动 DTMF 请求

用户可以通过某种手段生成 DTMF 语音；例如使用关键字解压缩。相关操作将作为要在已建立信道上以 START DTMF 报文形式所发送 DTMF 数据位的请求进行解释。该报文包括需要传输的数据位的值(0,1,2,...,9,A,B,C,D,*,#) 。

每一 START DTMF 报文中只传输单一数据位。

5.2.2 启动 DTMF 应答

收到START DTMF报文的一方将重新将接收到的数据位恢复为远程用户可使用的 DTMF 语音，并向初始化端返回 STAT DTMF ACKNOWLEDGE 报文。该确认表示已成功传输。

5.2.3 终止 DTMF 请求

当用户表示 DTMF 发送应结束时(如通过释放关键字)，初始化方将向其他方发送 STOP DTMF 报文。

5.2.4 终止 DTMF 应答

收到 STOP DTMF 报文后，接收方将停止发送 DTMF 语音，并向初始化方返回 STOP DTMF ACKNOWLEDGE 报文。

5.2.5 报文流

下图提供了在需要生成单个 DTMF 时交换报文的视图

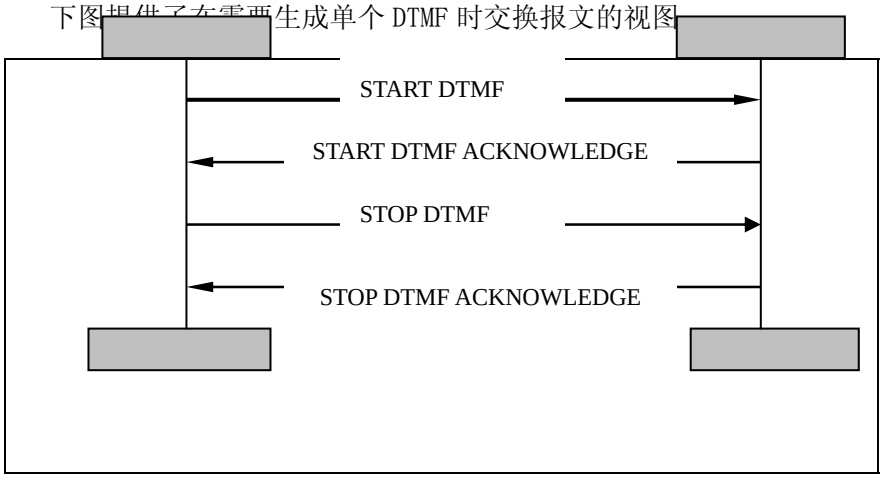


图 8.12 DTMF 启动/终止报文流

5. 3 注册重呼

注册重呼指利用语音拨号获取注册，以准许输入数据或其它操作。注册重呼通过发送含有键盘信息元素的 INFORMATION 报文,实现注册重呼(16位)。以后的数据发送按照上节所示程序进行。

6. 报文格式

本节提供本规范使用的报文结构完整视图，定义每一类报文的功能和信息内容。

按照呼叫控制、组管理、无连接 TCS 三节规定，无论何时发出报文，

该报文都将含有必选信息元，以及本节中定义的某些可选信息。

报文通常以单个 L2CAP 数据分组的形式进行传输。报文起始位置也就是 L2CAP 数据内容的起始位置。

定义内容包括：

A）报文流向和用途的简要描述；

B）报文中信息元顺序列表(所有报文类别具有一致顺序)；

C）该表中各信息元的含义，一般包括

- 描述该信息元的规范的章节
- 是否标记必须信息‘M’或可选择信息‘O’；
- 信息元长度，这也可能因不同应用而定；

D）必要的注释信息

所有报文都以 8 个字节为单位进行解释。

6．1 呼叫控制报文格式

6．1．1 ALERTING

该报文由呼入方发送，表示被叫用户报警已被初始化。

报文类别：ALERTING

流向：从呼入方到呼出方

表 8.1 ALERTING 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1
信道容量	7.4.3	O[note 1)]	4（26）
进度指示	7.4.13	O	2
SCO 句柄	7.4.14	O	2
目的 CID	7.4.11	O	4
厂商指定信息	7.4.9	O	3

注：只允许在呼入方发出的第一个报文中使用

6．1．2 CALL PROCEEDING

本报文由呼入方发送，表示请求呼叫建立过程已初始化，不再接收其它的呼叫建立信息。

报文类别：CALL PROCEEDING

流向：从呼入方到呼出方

表 8.2 CALL PROCEEDING 报文内容

信息元	参见	类别	长度

报文类别	7.3	M	1
信道容量	7.4.3	0 note 1)	4（26）
进度指示	7.4.13	0	2
SCO 句柄	7.4.14	0	2
目的 CID	7.4.11	0	4
厂商指定信息	7.4.9	0	3-*

注：只允许在呼入方发出的第一个报文中使用

6．1．3 CONNECT

本报文由呼入方发送，表示被叫用户已接收到呼叫。

报文类别：CONNECT

流向：从呼入方到呼出方

表 8.3 CONNECT 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1
信道容量	7.4.3	0 note 1)	4（26）
SCO 句柄	7.4.14	0	2
厂商指定信息	7.4.9	0	3-*

注：只允许在呼入方发出的第一个报文中使用

6．1．4 CONNECT AKNOWLEDGE

本报文由呼出方发送，表示确认收到 CONNECT 报文。

报文类别：CONNECT AKNOWLEDGE

流向：从呼出方到呼入方

表 8.4 CONNECT AKNOWLEDGE 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1
信道容量	7.4.14	0	4（26）
SCO 句柄	7.4.11	0	4
厂商指定信息	7.4.9	0	3-*

6．1．5 DISCONNECT

本报文可由任意一方发送，请求中止呼叫。

报文类别：DISCONNECT

流向：双向

表 8.5 DISCONNECT 报文内容

信息元	参见	类别	长度

报文类别	7.3	M	1
信道容量	7.4.7	O	2
进度指示	7.4.13	O	2
SCO 句柄	7.4.14	O	2
目的 CID	7.4.11	O	4
厂商指定信息	7.4.9	O	3-*

6．1．6 INFORMATION

本报文可由任一方发送，在重复呼叫情况下，用以在呼叫建立过程中提供附加信息。

报文类别：INFORMATION

流向：双向

表 8.6 INFORMATION 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1
发送完成	7.4.15	O	1
键盘功能	7.4.12	O	2
被叫方号码	7.4.5	O	3-*
语音控制	7.4.2	O	3-*
厂商指定信息	7.4.9	O	3-*

6．1．7 PROGRESS

本报文由呼入方发送，表示在工作情况下，或在附加带内信息/模式时任一方的呼叫进度。

报文类别：PROGRESS

流向：呼入方到呼出方

表 8.7 PROGRESS 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1
进度指示	7.4.13	O	2
SCO 句柄	7.4.14	O	2
目的 CID	7.4.11	O	4
厂商指定信息	7.4.9	O	3-*

6．1．8 RELEASE

本报文用于表示发送报文的设备已断开连接，并准备释放通道，而接收方也将在发送 RELEASE COMPLETE 后释放通道。

报文类别：RELEASE

流向：双向

表 8.8RELEASE 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1
原因	7.4.7	O note 1)	2
厂商指定信息	7.4.9	O	3-*

注 1：必须在首次呼叫清除报文里。

6．1．9 RELEASE COMPLETE

本报文用于表示发送报文的设备已经释放通道，此通道可以被重用。

报文类别：RELEASE COMPLETE

流向：双向

表 8.9 RELEASE COMPLETE 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1
原因	7.4.7	O note 1)	2
厂商指定信息	7.4.9	O	3-*

注 1：在首次呼叫清除报文里必须使用。

6．1．10 SETUP

本报文由呼出方发送，以初始化呼叫建立。

报文类别：SETUP

流向：呼出方到呼入方

表 8.10 SETUP 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1
呼叫类	7.4.4	M	2
完成发送	7.4.14	O	1
信道容量	7.4.3	O	4(26)
信号	7.4.16	O	2
主叫方号码	7.4.6	O	3-*
被叫方号码	7.4.5	O	3-*
厂商指定信息	7.4.9	O	3-*

6．1．11 SETUP ACKNOWLEDGE

本报文由呼入方发出，表示已初始化呼叫建立过程，但需要附加信息。

报文类别：SETUP ACKNOWLEDGE

流向：呼入方到呼出方

表 8.11 SETUP ACKNOWLEDGE 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1
信道容量	7.4.3	O note 1)	4(26)
进程指示	7.4.13	O	2
SCO 句柄	7.4.14	O	2
目的 CID	7.4.11	O	4
厂商指定信息	7.4.9	O	3-*

注 1：仅可用于呼入方发送的首个报文。

6．1．12 START DTMF

本报文包括其他方应转为远程用户使用的 DTMF 双音多频语音的数据位

报文类别：START DTMF

流向：双向

表 8.12 START DTMF 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1
键盘功能	7.4.12	M	2

6．1．13 START DTMF ACKNOWLEDGE

该报文表示 START DTMF 报文所需操作已成功初始化。

报文类别：START DTMF ACKNOWLEDGE

流向：双向

表 8.13 START DTMF ACKNOWLEDGE 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1
键盘功能	7.4.12	M	2

6．1．14 START DTMF REJECT

本报文表示不能接收 START DTMF 报文。

报文类别：START DTMF REJECT

流向：双向

表 8.14 START DTMF REJECT 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1
原因	7.4.7	O	2

6．1．15 STOP DTMF

本报文终止向远程用户发送 DTMF 语音信息。
报文类别：STOP DTMF
流向：双向

表 8.15 STOP DTMF 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1

6．1．16 STOP DTMF ACKNOWLEDGE

本报文表示终止向远程用户发送 DTMF 语音信息。
报文类别：STOP DTMF ACKNOWLEDGE
流向：双向

表 8.16 STOP DTMF ACKNOWLEDGE 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1
键盘功能	7.4.12	M	2

6．2 组管理报文格式

6．2．1 请求访问权限

发送本报文表示初始化一方请求获取访问权限。
报文类别：ACCESS RIGHTS REQUEST

表 8.17 ACCESS RIGHTS REQUEST 报文内容

流向：双向信息元	参见	类别	长度
报文类别	7.3	M	1
厂商指定信息	7.4.19	O	3-*

6．2．2 接受访问权限

由应答方发送本报文表示访问权限授权。
报文类别：ACCESS RIGHTS ACCEPT
流向：

表 8.18 ACCESS RIGHTS ACCEPT 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1
厂商指定信息	7.4.19	O	3-*

6．2．3 拒绝访问权限

由应答方发送本报文表示拒绝访问权限。

报文类别：ACCESS RIGHTS REJECT
流向：

表 8.19 ACCESS RIGHTS REJECT 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1
厂商指定信息	7.4.19	O	3-*

6．2．4 INFO SUGGEST

由 WUG 管理员发送的本报文表示 WUG 配置已变化。
报文类别：INFO SUGGEST
流向：WUG 管理员到 WUG 成员

表 8.20

信息元	参见	类别	长度
报文类别	7.3	M	1
配置数据	7.4.10	M	*
厂商指定信息		O	3-*

6．2．5 INFO ACCEPT

由 WUG 成员发送本报文表示已接受 WUG 配置更新。
报文类别：INFO ACCEPT
流向： WUG 成员到 WUG 管理员

表 8.21 INFO ACCEPT 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1
厂商指定信息	7.4.9	O	3-*

6．2．6 LISTEN REQUEST

由 WUG 成员发送本报文,用于向 WUG 管理员请求对 WUG 成员进行成员间快速访问。
报文类别：LISTEN REQUEST
流向： WUG 成员到 WUG 成员

表 8.22 LISTEN REQUEST 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1
被叫方号码	7.4.6	M	3-*
厂商指定信息	7.4.9	O	3-*

6．2．7　LISTEN SUGGEST

本报文由 WUG 管理员发送，表示存在对 WUG 成员允许成员间快速访问的请求。

报文类别：LISTEN SUGGEST

流向：　WUG 管理员到 WUG 成员

表 8.23　LISTEN SUGGEST 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1
厂商指定信息	7.4.9	O	3-*

6.2.8　ISTEN ACCEPT

发送本报文表示接受先前的成员间快速访问请求。

报文类别：LISTEN ACCEPT

流向：　双向

表 8.24　LISTEN ACCEPT 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1
时隙	7.4.8	O	4
厂商指定信息	7.4.9	O	3-*

1. LISTEN REJECT

发送本报文表示拒绝先前的成员间快速访问请求。

报文类别：LISTEN REJECT

流向：　双向

表 8.25 LISTEN REJECT 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1
原因	7.4.7	O	2
厂商指定信息	7.4.9	O	3-*

3. TCS 无连接报文格式

6．3．CL INFO

由任何一方发送此报文表示将按照无连接模式提供附加信息。

报文类别：CL INFO
流向： 双向

表 8.26 CL INFO 报文内容

信息元	参见	类别	长度
报文类别	7.3	M	1
语音控制			
厂商指定信息			

7. 报文编码

本节图文描述报文内容。报文按位从低位到高位的序列传输。发出的报文都应按本节所述编码方式编码。

7.1 概述

编码规则遵循 ITU-T 的 Q.931 建议，但按照 TCS 需要进行了调整和修改。

每一个报文都由下列部分组成：

a)协议标识

b)报文类别

c)其它所需信息元

协议标识和报文类别是每一个 TSC 报文的基本组成部分，其它信息元则根据报文类别而定。

表 8.27 通用报文格式

8 7 6 5 4 3 2 1

协议标识	报文类别
其它信息元	

一个信息元只能在给定报文中出现一次。

缺省值只有在不使用指定值或没有备选值协商机制时使用。

当一个域分布在几个字节上,每一位取值的顺序将递减,而字节号递增。该域的最小位由最高位字节的最低位比特表示。总之，每个字节的第一位包括该段的最低位。

7.2 协议标识

协议标识的作用是将报文划分为不同的功能组。报文第一部分就是协议标识。

协议标识按照图 8.13 和表 8.28 方式编码。

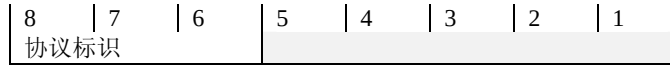


图 8.13　协议标识

表 8.28 协议标识

位			
8	7	6	
0	0	0	蓝牙 TCS 呼叫控制
0	0	1	蓝牙 TCS 组管理
0	1	0	蓝牙 TCS 无连接
保留其它所有值			

7.3　报文类型

报文类型用于标识发出报文的功能。报文第一部分就是报文类型标识。

报文类型按照图 8.14 和表 8.29 方式编码。

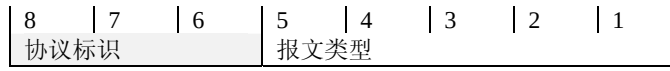


图 8.14　报文类型

表 8.29 报文类型

位					
5	4	3	2	1	
					呼叫控制报文
					建立呼叫
0	0	0	0	0	ALERTING
0	0	0	0	1	CALL PROCEEDING
0	0	0	1	0	CONNECT
0	0	0	1	1	CONNECT ACKNOWLEDGE
0	0	1	0	0	PROGRESS
0	0	1	0	1	SETUP
0	0	1	1	0	SETUP ACKNOWLEDGE
					呼叫清除
0	0	1	1	1	DISCONNECT
0	1	0	0	0	RELEASE

0	1	0	0	1	RELEASE COMPLETE
					混合
0	1	0	1	0	INFORMATION
1	0	0	0	0	START DTMF
1	0	0	0	1	START DTMF ACKNOWLEDGE
1	0	0	1	0	START DTMF REJECT
1	0	0	1	1	STOP DTMF
1	0	1	0	0	STOP DTMF ACKNOWLEDGE
					组管理报文
0	0	0	0	0	INFO SUGGEST
0	0	0	0	1	INFO ACCEPT
0	0	0	1	0	LISTEN REQUEST
0	0	0	1	1	LISTEN ACCEPT
0	0	1	0	0	LISTEN SUGGEST
0	0	1	0	1	LISTEN REJECT
0	0	1	1	0	ACCESS RIGHTS REQUEST
0	0	1	1	1	ACCESS RIGHTS ACCEPT
0	1	0	0	0	ACCESS RIGHTS REJECT
					无连接报文
0	0	0	0	0	CL INFO

7.4 其它信息元

]7.4.1 编码规则

本节主要描述其它信息元的编码规则。

信息元分为三大类：

1）单字节信息元（见图 8.15）

2）双字节信息元（见图 8.16）

3）不定长位组信息元（见图 8.17）

表 8.30 将本规范中用于信息元的信息元编码规则进行汇总。

8	7	6	5	4	3	2	1
1	信息元标识						

字节 1

图 8.15 单字节信息元格式

8	7	6	5	4	3	2	1

1	信息元标识	字节 1
信息元内容		字节 2

图 8.16 单字节信息元格式

8	7	6	5	4	3	2	1	
1	信息元标识							字节 1
信息元内容长度								字节 2
信息元内容								字节 2

图 8.17 双字节信息元格式

表 8.31 信息元标识编码

编码									参考	最大长度(字节)
8	7	6	5	4	3	2	1			
1								单字节信息元	7.4.15	1
	0	1	0	0	0	0	1	发送完成		
1								双字节信息元		
	1	0	0	0	0	0	0	呼叫类	7.4.4	2
	1	0	0	0	0	0	1	原因	7.4.7	2
	1	0	0	0	0	1	0	进度指示	7.4.13	2
	1	0	0	0	0	1	1	信号	7.4.16	2
	1	0	0	0	1	0	0	键盘功能	7.4.12	2
	1	0	0	0	1	0	1	SCO 句柄	7.4.14	2
0								变长信息元		
	0	0	0	0	0	0	0	时隙	7.4.8	4
	0	0	0	0	0	0	1	配置数据	7.4.2	*
	0	0	0	0	0	1	0	信道容量	7.4.3	4(26)
	0	0	0	0	0	1	1	目的 CID	7.4.11	4
	0	0	0	0	1	0	0	主叫号码	7.4.6	*
	0	0	0	0	1	0	1	被叫号码	7.4.5	*
	0	0	0	0	1	1	0	语音控制	7.4.2	*
	0	0	0	0	1	1	1	厂商指定信息	7.4.9	*

下面的信息元描述将按字符顺序排列。但报文中信息元的实际排列顺序与此不同。对于不定长信息元格式的信息元标识编码值将根据报文信息元的实际顺序按升序排列。信息接收设备可以直接检测出某一信息位是否缺失，而不用对整个报文进行扫描。

本规范中的信息元可以包含被赋值为‘0’的空位。为了适应将来的变化，报文不能由于某空位值置为‘1’被拒绝。

不定长信息元的第二个字节标识信息元内容总长，与第一个字节的编码无关。也就是说，长度从第三个字节开始计算。长度值实际就是内容字节数的二进制编码。

报文可以包括一个可选的变长信息元，但它为空（长度为 0）。而如果不包括该信息元，接受方也应能解释。简单地说，接受方应能对为空的信息元进行解释。

7.4.2 语音控制

语音控制信息元用于表示与语音控制相关的信息。

8	7	6	5	4	3	2	1	字节
0	0	0	0	0	0	0	0	1
信息元内容长度								2
控制信息								3

图 8.18

表 8.32 语音控制信息元编码

控制信息(第 3 字节)								
比特								
	7	6	5	4	3	2	1	
	0	0	0	0	0	0	0	音量增大
	0	0	0	0	0	0	1	音量减小
	0	0	0	0	0	1	0	麦克风音量增大
	0	0	0	0	0	1	1	麦克风音量减小
	0	X	X	X	X	X	X	蓝牙标准保留使用
	1	X	X	X	X	X	X	厂商指定信息

7.4.3 信道容量

信道容量信息元用于指示一种被请求的或可用的服务。

如果没有该信息元，缺省的信道容量为带有 HV3 类型包的同步面向连接链接，该连接采用用户信息层 CVSD 编码方式。

8	7	6	5	4	3	2	1	字节
0	0	0	0	0	0	1	0	1
信息元内容长度								2
链接类型								3

图 8.19

链接类型元编码=00000000（SCO）。

用户信息层 1	数据分组类型	第 4 字节

图 8.20

链接类型元编码=00000001（ACL）。

标志		4
服务类型		5
令牌率		6
		7
		8
		9
令牌尺寸(字节)		10
		11
		12
		13
带宽缝值(字节/秒)		14
		15
		16
		17
应答时间(微秒)		18
		19
		20
		21
延迟(微秒)		22
		23
		24
		25
用户信息层 3	用户信息层 2	26

图 8.21

注：由于只有 TCS 具有端到端服务质量条件，服务质量在 TCS 层次上重复。

表 8.32 信道容量信息元编码

链接类型(第 3 字节)								
比特								
8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	0	同步面向连接
0	0	0	0	0	0	0	1	异步无连接
0	0	0	0	0	0	01	0	无
保留所有值								
字节 4 编码(链接类型信息元编码=000000000)								
数据分组类型(字节 4)								
	5	4	3	2	1			
	0	0	1	0	1	HV1		
	0	0	1	1	0	HV2		
	0	0	1	1	1	HV3		
	0	1	0	0	0	DV		
保留所有值								

用户信息层 1(字节 4)				
比特				
	8	7	6	
	0	0	1	
	0	1	0	
	0	1	1	
保留所有值				
字节 4-26 编码(链接类型信息元编码=000000001)				
字节 4-25 编码细节可在 L2CAP 中找到				
用户信息层 2(字节 26)				
比特				
4	3	2	1	
0	0	0	0	RFCOMM over L2CAP
保留所有值				
用户信息层 3(字节 26)				
比特				
8	7	6	5	
0	0	0	0	未定义
0	0	0	1	PPP
0	0	1	0	IP
保留所有值				
字节 4 编码(链接类型信息元编码=000000010)				
缺少字节 4				

7.4.4 呼叫类别

呼叫类别用于表示被请求服务的基本情况。该信息元允许用户指出缺省属性的用途，并缩短 set-up 报文的长度。

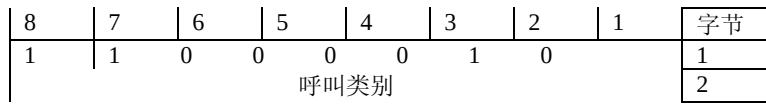


图 8.22

表 8.33 呼叫类别信息元编码

呼叫类别(字节 2)

	比特							
8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	0	外部呼叫
0	0	0	0	0	0	0	1	内部呼叫
0	0	0	0	0	0	1	0	服务呼叫
0	0	0	0	0	0	1	1	紧急呼叫
	保留所有值							

注：

- 外部呼叫是指一个对外部网络（如 PSTN）的呼叫或来自于外部网络的呼叫；
- 内部呼叫是指蓝牙设备之间的呼叫；
- 服务呼叫是指出于配置目的的呼叫；
- 紧急呼叫是指一个利用紧急呼叫号码和某些特性的外部呼叫；

7.4.5 被叫号码

被叫号码信息元用于唯一标识呼叫的被叫方。

8	7	6	5	4	3	2	1	字节
0	0	0	0	0	1	0	1	1
信息元内容长度								2
0	号码类别			编号计划标识				3
0	号码位(IA5 字符), 注							4

图 8.23

注:多个第 4 位号码数字输入顺序一致，也就是说，第一个输入的数字位于第一个字节 4。

表 8.34 被叫方信息元编码

号码类别(字节 3)				
	比特			
	7	6	5	
	0	0	0	未知
	0	0	1	国际号码
	0	1	0	国内号码
	0	1	1	网络指定号码
	1	0	0	用户号码
	1	1	0	缩写号码
	1	1	1	保留
	保留所有值			
	比特			
	4	3	2	1
	0	0	0	0 未知

	0	0	0	1	ISDN/电话编号方案 E.164
	0	0	1	1	数据编号方案 REC.X.121
	0	1	0	0	保留
	1	0	0	0	国内标准编号方案
	1	0	0	1	私用编号方案
	保留所有值				

7. 4. 6 主叫号码

主叫号码信息元用于标识呼叫的来源。

8	7	6	5	4	3	2	1	字节
0	0	0	0	0	1	0	0	1
	信息元内容长度(字节)							2
0	号码类别			编号方案标识				3
0	标识			0	0	0	显示标识	4
	数据位(IA5 字符)							5 等

图 8. 24

表 8. 35 主叫方信息元编码

号码类别(字节 3)				
	比特			
	7	6	5	
	0	0	0	未知
	0	0	1	国际号码
	0	1	0	国内号码
	0	1	1	网络指定号码
	1	0	0	用户号码
	1	1	0	缩写号码
	1	1	1	保留
	保留所有值			
	编号方案标识(字节 3)			
	比特			
	4	3	2	1
	0	0	0	0 未知
	0	0	0	1 ISDN/电话编号方案 E.164
	0	0	1	1 数据编号方案 REC.X.121
	0	1	0	0 保留
	1	0	0	0 国内标准编号方案

	1	0	0	1	私用编号方案
	保留所有值				
	标识(字节 4)				
	比特				
	7	6			
	0	0			允许的标识
	0	1			限制的标识
	1	0			不能用于互操作的号码
	1	1			保留
	显示标识				
	比特				
	2	1			
	0	0			用户提供,不显示
	0	1			用户提供,校验通过
	1	0			用户提供,校验失败
	1	1			网络提供
	保留所有值				

7.4.7 出错原因

出错原因用于指示引起被请求服务失败的远端原因。

8	7	6	5	4	3	2	1	字节
1	1	0	0	0	0	0	1	1
出错原因值								2

图 8.25

表 8.36 出错原因信息元编码

出错原因(字节 2)							
	比特						
8	7	6	5	4	3	2	1

0	这 7 位采用类似于 ITU-T 建议 Q.850 中的原因值子域编码方法进行编码

7.4.8 时隙

时隙信息元用于表示使用的蓝牙时隙。

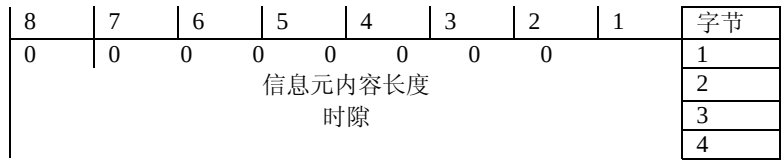


图 8.26 时隙信息元编码

表 8.37 厂商指定信息

号码类别(字节 3)															
	比特															
	字节 3								字节 4							
8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1
	0	0	0	包括蓝牙时钟的 2-16 位											

厂商指定信息元用于发送非标准信息。

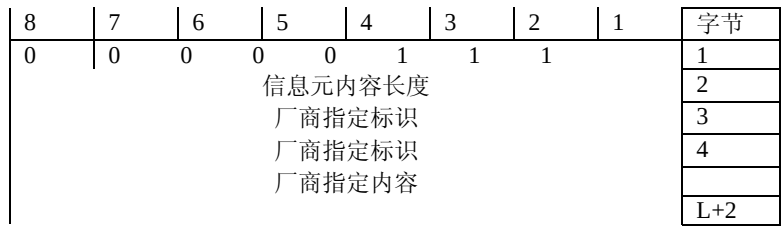


图 8.27

厂商标识编码(字节 3 和字节 4)															
	比特								比特							
	字节 3								字节 4							
8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	爱立信
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	诺基亚移动电话
0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	INTEL 公司
0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	IBM 公司
0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	东芝公司
保留所有值																

图 8.28 厂商指定信息元编码

7.4.10 配置数据

配置数据信息元用于表示配置数据。

8	7	6	5	4	3	2	1	字节
0	0	0	0	0	0	0	1	1
信息元内容长度								2
0	WUG 成员 1 的内部号码(IA5 字符)							3
0	WUG 成员 1 的内部号码(IA5 字符)							4
WUG 成员 1 的蓝牙地址								5
								…
								10
用于 WUG 成员 1 的链接关键字								11
								…
								26
…….								
0	WUG 成员 n 的内部号码(IA5 字符)							3+((n-1)*24)
0	WUG 成员 n 的内部号码(IA5 字符)							4+((n-1)*24)
WUG 成员 n 的蓝牙地址								5+((n-1)*24)
								…
								10+((n-1)*24)
用于 WUG 成员 n 的链接关键字								11+((n-1)*24)
								2+(n*24)

图 8.29

注:内部号码(两位)出现在第 3 字节和第 4 字节,其顺序与输入顺序相同。也就是说,第一个输入的数据位位于字节 3。

注: 对于所有的 n WUG 成员重复字节 3-26。

7.4.11 目的 CID

目的 CID 信息元用于使远端能够将已建立的 L2CAP 通道与正在进行的呼叫相关联。目的 CID 唯一对应于以配置请求包形式交换目的 CID。(参见 L2CAP)

8	7	6	5	4	3	2	1	字节
0	0	0	0	0	0	1	1	1

信息元内容长度(字节)	2
DCID 字节 1	3
DCID 字节 0	4

图 8.30

7. 4. 12 键盘设置

键盘功能信息元的目的在于传输 IA5 字符，如由终端键盘输入的字符。

8	7	6	5	4	3	2	1	字节
1	1	0	0	0	1	0	0	1
0	键盘功能信息(IA 字符)							2

图 8.31

7. 4. 13 进度指示

进度指示信息元用于描述在呼叫生命周期中发生的事件。

8	7	6	5	4	3	2	1	字节
1	1	0	0	0	0	1	0	1
0	进度指示							2

图 8.32

表 8.38 进度指示信息元编码

进度信息(字节 2)							
比特							
7	6	5	4	3	2	1	
0	0	0	1	0	0	0	带内信息或合适模式现在可用
保留所有值							

7.4.14 SCO 句柄

SCO 句柄信息元用于使远端能够将已建立的 SCO 链接与正在进行的呼叫相关联。SCO 句柄唯一标识一个由匹克网管理员发出的以 LMP_SCO_link_req 形式交换的 SCO 句柄。

8	7	6	5	4	3	2	1	字节
1	1	0	0	0	1	0	1	1
0	SCO 句柄值							2

图 8.33

7.4.15 发送完成

发送完成信息元用于表示被叫方号码结束。

8	7	6	5	4	3	2	1	字节
1	0	1	0	0	0	0	1	1

图 8.34

7．4．16 信号

信号信息元的用于向与语音和报警信号有关的用户发送信息。

8	7	6	5	4	3	2	1	字节
1	1	0	0	0	0	1	1	1
0	信号值							2

图 8.35

表 8.39 信号信息元编码

信号值(字节 2)								
	比特							
8	7	6	5	4	3	2	1	
0	1	0	0	0	0	0	0	外部呼叫
0	1	0	0	0	0	0	1	内部呼叫
0	1	0	0	0	0	1	0	回呼
0	X	X	X	X	X	X	X	蓝牙标准保留
1	X	X	X	X	X	X	X	厂商指定

8 报文出错处理

8.1 协议标识出错

当收到的报文除了包括 7.2 节中定义的信息元以外，还有已编码的协议标识，那么，该报文应被忽略。

8.2 报文太短或未被识别

如果收到的报文太短，不足于包含完整的报文类别信息元，则忽略该报文；

如果收到的报文包含完整的报文类别信息元，但不能被识别，则忽略该报文。

8.3 报文类别或报文顺序出错

除了在 NULL 状态下以外，无论何时收到除了 RELEASE 或 RELEASE COMPLETE 以外的报文，则应忽略该报文；

当收到一个未知的 RELEASE 报文，接收方应断开和释放已建立的信道，并返回 RELEASE COMPLETE 报文，中止所有定时器，进入 NULL

状态。

当收到一个未知的 RELEASE COMPLETE 报文，接收方应断开和释放已建立的信道，并返回 RELEASE COMPLETE 报文，中止所有定时器，进入 NULL 状态。

8.4 信息元出错

报文中的信息元应按第 6 节中所示的顺序进行排列。

当收到的报文缺少必需的信息元，或必需的信息元包括不合法内容，则忽略该报文。

为避免在 SETUP 报文中必需信息元出错，应返回 RELEASE COMPLETE 报文和#96 出错信息，‘缺少必需信息元’或#100 出错信息，‘信息元内容非法’。

当收到的报文包含未识别信息元，或包含含有非法内容的可选信息元，或包含未定义的可识别信息元，接收方应忽略该信息元。

信息元超长则视为该信息元含有非法内容。

9 协议参数

9.1 协议时钟

表 8.40 定时器值

定时器名	值
T301	至少 3 分钟
T302	15 秒
T303	20 秒
T304	30 秒
T305	30 秒
T308	4 秒
T310	30-120 秒
T313	4 秒
T401	8 秒
T402	8 秒
T403	4 秒
T404	2.5 秒
T405	2 秒
T406	20 秒

10．参考文献

附录 1 TCS 呼叫状态

第 9 章 WAP 信道下蓝牙互操作性要求
PPP 修正稿

对于无线应用协议，蓝牙设备与目的平台共享一些特性。某些情况下，同一设备能够支持两种通信技术。本规范描述为了满足 WAP 协议和应用需求，利用 PPP 作为信道的蓝牙互操作性要求。

目　　录

1. 介 绍

1.1 适用范围

本文用于在 WAP 环境和协议下，利用蓝牙环境的动态等其它特性，提供对增值服务的访问。

蓝牙在 WAP 客户和服务器之间提供通信物理介质和链接控制。本文件对基于 PPP 的通信方式进行描述。

本文件当然不足以支持 WAP 客户或服务器端服务，而只包括以下信息：

• 概述蓝牙环境下对 WAP 的使用，解释了符合蓝牙版本的增值服务概念，并提供利用 WAP 增值服务如何适应蓝牙应用模型的实例；

• WAP 服务概述的目的在于将 WAP 环境置于相同的环境当中，并将介绍 WAP 组件，及其与同层次 INTERNET 协议的比较；

• 对蓝牙匹克网中的 WAP 进行论述，并描述蓝牙通信结构关联 WAP 服务的方式；

• 最后，阐述为在两个支持蓝牙技术的 WAP 设备间实现互操作而需提供的蓝牙特性；

1．蓝牙环境中的 WAP 应用

2.1 增值服务

一个设备的通信能力并不仅仅限于其自身。终端用户通常并不关心技术，而只是对技术能够帮助他们作什么感兴趣。

传统的电信技术只是依靠语音通信作为唯一的技术应用，而且该应用方式在市场中取得了成功。而当数据通信服务变得越来越广泛地得到应用时，如何更好更多地利用数据服务则变得越来越重要了。

无线应用协议论坛目标就是创建一个标准框架，在该框架中对能够提供的增值服务和互操作层次做出定义。

2 .2 用途

蓝牙用于增值服务的唯一优点是能够在有限范围内建立通信链接。理想情况下，支持蓝牙的设备能够满足与位置无关的服务需要。下面就是一些 WAP 客户/服务器模型应用于蓝牙用途的实例。

2.2.1 短信息

短信息服务允许用户的笔记本电脑或移动电话进行无用户干扰的通信，主要用于更新用户电子邮件。用户可从手机中浏览收到的消息，而不需要将笔记本电脑从皮包里取出来。

2.2.2 强制信息

强制信息与短信息相似。用户可以将消息组织在一个没有拨号连接的环境里。过一段时间,等笔记本电脑唤醒以后,就检查移动电话，看是否可以发送刚才未发送的信息.如果存在可用通信链接,就可以发出电子邮件。

2.2.3 WAP 网站信息

WAP 网站信息使用户能够连接到移动 PC 或手持设备，以与公共 WAP 网站相连。网站可以根据该设备所处位置向该设备提供信息。例如，航班信息、机场登机口、购物中心的商店位置、火车时刻表或者铁路目的地。

3. WAP 服务概述

无线应用协议用于向那些在多方面受到限制的设备提供 Internet 或类似于 Internet 的访问。有限的通信带宽、内存、不间断电源、显示能力和输入设备都是促进 WAP 发展的因素。尽管某些设备具有上述限制，但 WAP 仍然为这些设备提供了大量可用之处。

典型的 WAP 环境由三类设备组成：WAP 客户端设备、WAP 代理/网关和 WAP 服务器。在某些情况下，代理/网关也包括服务器的一些功能。

3.1 WAP 实体

3.1.1 WAP 客户端

WAP 客户端设备通常都是用户手持设备。该设备可以是功能强大的便携计算机，也可以是移动电话。客户端的必要特性是必须要有显示和输入设备。

WAP 客户端通过无线网络与 WAP 代理/网关相连。该网络可能基于某些可用的技术。WAP 协议允许网络具有低可靠性和高延迟，但不能中断服务。

3.1.2 WAP 代理/网关

WAP 代理/网关作用在于提供无线网络和 Internet 之间的接口。代理的主要功能在于能够向 WAP 客户端设备提供 DNS 域名解析服务，以及将 Internet 协议和内容格式翻译到 WAP 相应层次。

3.1.3 WAP 服务器

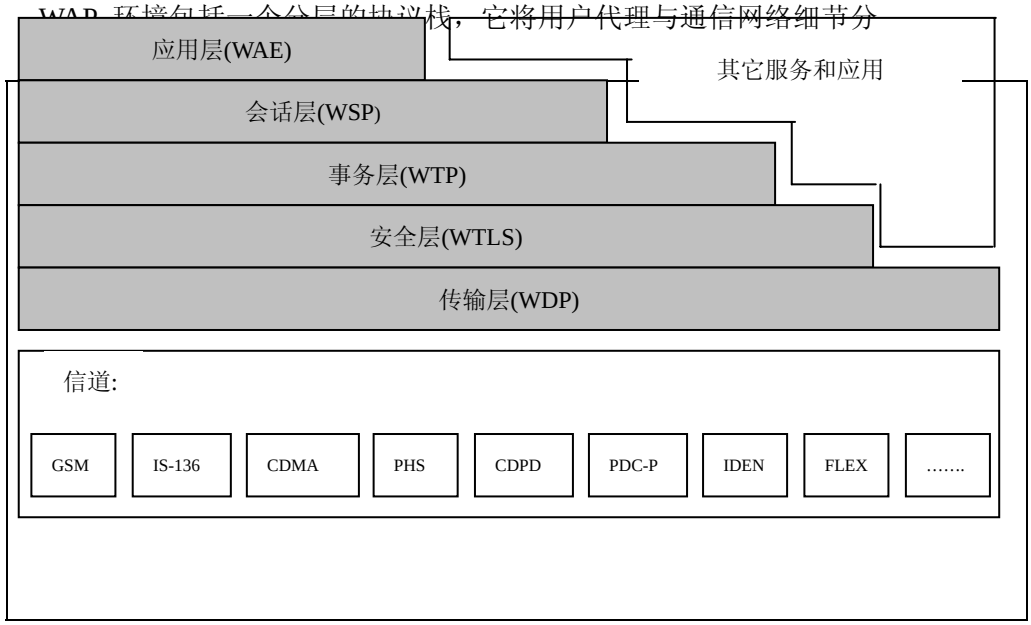
WAP 服务器的功能类似于 Internet 上的服务器。实际上，WAP 服务器通常就是一个 HTTP 服务器。该服务器作为用户经常访问信息存放处。其内容包括文本、图像、甚至是允许客户端设备执行的服务器端代码。

WAP 服务器日志与代理/网关放在同一个物理设备上，或者在代理/网关能够访问到的网络中任何地方。

这样，一个服务器可以作为一个 HTTP 服务器，一个 WSP 服务器，或者两者兼而有之。

3.2 WAP 协议

WAP 环境包括一个分层的协议栈，它将用户代理与通信网络细节分



开。

图 4.1 就表示了 WAP 协议栈的综合结构。蓝牙提供了附加数据信道服务，在图中的底部。

图 10.1 WAP 协议栈

3.2.1 无线数据分组协议

WDP 层提供一个服务接口，该接口作为基于套接字 UDP 的执行版本。对于一个基于 IP 的信道服务,该层是 UDP。对于不能提供 UDP 服务接口的信道，应提供 WDP 应用作为适配层，以允许在本信道进行基于套接字的数据分组传输。

3.2.2 无线传输协议（WTP）

WTP 层在 WDP（UDP）协议层之上提供可靠的数据分组服务。

3.2.3 无线传输层安全性（WTLS）

WTLS 层对于能够在客户端 WSP 会话与其对应服务器 WSP 会话之间提供安全数据管道的协议栈而言,是一个可选的组件。在 WAP 规范的当前版本中，会话终止于服务器端。现在，在 WAP 论坛之前就有一个关于代理协议的建议。该建议将允许中间 WAP 代理能够在不对数据流解密的情况下，通过代理/网关传输 WTLS 数据分组。

3.2.4 无线会话协议（WSP）

WSP 层在客户端应用与 WAP 服务器之间建立关联。这样就可以长时间保持会话，而且在服务中断时仍能够保持。WSP 利用 WTP 服务提供到目的代理/网关的可靠传输。

3.3 WAP 和 INTERNET 间的协议转换

WAP 协议栈要解决的问题和应用都与 IETF 组织所定义的协议和应用相关。WAP 论坛的基本目标就是对那些因不能应用 INTERNET 协议而受到限制的设备提供 INTERNET 内容。

本节就是将对比 WAP 协议栈各层与 IETF 中的对应协议层次。

3.3.1 UDP/WDP

在大多数的基本协议层次上，WAP 和 INTERNET 相同。与 INTERNET 中传输层相同，WAP 协议栈也利用基于套接字的数据分组模型。

一些 INTERNET 协议也采用 UDP 服务，但大多数协议都是采用面相连接报文流协议（TCP）。

3.3.2 WTP/TCP

无线传输协议（WTP）在某些方面提供与 TCP 要求相同的服务。INTERNET 传输协议（TCP）提供基于 IP 服务的可靠、面向连接和字符流的协议。比较而言，WTP 能够提供单向的可靠或非可靠的报文传输，也能够提供双向可靠的报文传输。这种经过优化的传输方式适于 WAP 的‘短请求、长回应“的会话特点。WTP 提供报文拼接，以减少报文传输数量。

3.3.3 WTLS/SSL

无线传输层安全性（WTLS）是由安全套接字协议（SSL）发展而来的。因此，它也提供与 SSL 相同的身份鉴别和加密服务。

3.3.4 WSP/HTTP

WAP 中的会话服务由无线会话协议（WSP）提供。该协议与 HTTP 1.1 的术语和功能定义保持一致，但增加了对长时间会话、‘推’数据和会话挂起、会话继续的支持。另外，协议利用压缩编码方法以适应窄带通信要求。

3.3.5 WML/HTML

WAP 使用的标记语言是与 HTML 相同的经过精简的版本，但经过针对手持设备应用的优化。WML 成为一种符合 XML 定义的标记语言。

3.3.6 WML Script/JavaScript

WAP 具有与 JavaScript 相同的编码语言，但该语言根据 WAP 目标设备类型进行了修正。

4. WAP 在蓝牙匹克网中的应用

蓝牙技术在很多方面都可以应用在其它类似于 WAP 的无线网络中。蓝牙技术能够用于在 WAP 客户端与其邻近 WAP 服务器之间提供数据传输信道。

此外，蓝牙本质上可以提供只能由 WAP 协议统一浏览的能力。

4．1 WAP 服务器通信

WAP 通信的传统组成包括一个能够利用 WAP 协议与服务器/代理设备通信的客户端设备。在这种情况下，蓝牙中介可以提供由 WAP 体系结构规定的信道服务。

4.1.1 客户端设备初始化

当一个 WAP 设备处于对蓝牙设备的有效侦听状态，它就能利用蓝牙服务搜索协议搜索 WAP 服务器。

在图 10.1 中，第一步中 WAP 客户端设备进入 WAP 代理/网关匹克网范围。当客户端检测到 WAP 代理/网关的存在，它就能自动地或在客户端请求下与服务器建立连接。

3.1.1.1 服务搜索

客户端应能够确定已检测到 WAP 代理/网关的特性。蓝牙服务搜索协议应能够获取服务器的下列信息：

- 服务器名——应是用户能够理解的描述性名字；
- 服务器主页文本名字——即服务器的主页链接。本信息可选。
- 服务器/代理功能——表示该设备是否是一个 WAP 内容服务器，还是一个代理或两者都是。如果设备是一个代理，它必须能够解析不是服务器/代理设备地址的 URL。

在图 4.1 第二步中，该设备正在与 WAP 代理/网关通信，可以正常使用所有的 WAP 数据服务。

3.1.2 客户端设备终止

在图 4.1 第三步中，该设备退出匹克网。当该设备检测到与 WAP 代理/网关的通信链接已经丢失，它就会决定是否利用搜索到的信息决定是否继续保持通信连接.

例如，支持多个信道的客户端设备，在给出了服务器功能信息后，将查询服务器的其它地址信息。由于客户端设备随时会离开匹克网而导致搜索的信息不再有用，应将这些信息缓存起来以便以后的访问。

在前面的 WAP 网站例子里，如果用户想要在超出蓝牙范围时仍能够接收信息，该网站应向客户端设备提供 INTERNET 地址。当蓝牙通信连接失效时，该设备就可以利用单元数据分组继续客户/服务器会话。

该功能根据实际情况不同而不同。

3.1.3 服务器设备初始化

在客户与服务器之间初始化通信的另外一个方法就是服务器周期性轮询有无可用的客户端设备。当服务器设备发现一个客户具有 WAP 客户功能的时候，服务器可以连接该设备并向它‘推’送数据。

客户端设备则由终端用户决定选择是否忽略被‘推’过来的数据。

3.1.3.1 服务搜索

通过蓝牙服务搜索协议，该服务器能够确定以下有关客户端的信息：

- 客户名——经过格式化的描述客户端设备的描述性名字；
- 客户端特性——服务器可以通过该信息确定有关客户端蓝牙特性的

信息；

3.2 蓝牙环境下的 WAP 应用

为了有效支持 WAP OVER BLUETOOTH，应充分考虑设备特性。

3.2.1 WDP 管理实体

在 WAP 协议栈中，与 WDP 协议层关联的实体负责管理由该层提供的服务。WDP 管理实体（WDP-ME）作为控制协议栈的扩展机制。

3.2.1.1 异步通知

当某种事件发生时，WDP-ME 需要能够生成发往应用层的异步通知。异步通知的例子有：

- 侦测到新的客户端结点；
- 侦测到新的服务器端结点
- 丢失客户端结点信号
- 丢失服务器端结点信号
- 侦测到服务器“推”操作，而并未请求该内容

对于这些事件的支持因实际情况而异。所有列出的服务器推操作异常事件都从蓝牙主机控制器接口中引申而来。

3.2.1.2 备选信道

某个设备的 WAP 应用可以支持多个信道。有关信道选择方法的讨论超出了本文本范围。接下来的过程根据实际应用情况而不同。

3.2.2 寻址

在 WAP 环境中使用两种基本的寻址方式：用户寻址和代理/网关寻址。用户寻址描述对象在网络中的位置。它与所在信道无关。代理/网关寻址描述与之通信的 WAP 代理/网关的位置。代理/网关寻址方式取决于信道类型。

用户主要处理统一资源定位（URL）。这些地址是用于描述被访问文档的文本串。如代理/网关就与 INTERNET 域名紧密相关。

服务器将这些地址解析成为网络地址。

WAP 代理/网关地址通常是一个由用户或网络管理员配置的静态值。当用户输入 URL，也就是向配置好的 WAP 代理/网关发送请求。如果 URL 在 WAP 代理/网关域之外，WAP 代理/网关就会利用 DNS 解析确定文本所在的服务器的 IP 地址。

客户端设备首先标识一个可以由蓝牙访问的代理/网关，然后就利用服务搜索协议向用户提供服务器名或对服务器的描述。当用户选择了一个服

务器，客户端就会下载服务器主页。一旦用户浏览该服务器主页，那么所有的下级 URL 就都会与该主页相关联。该情况假设 WAP 代理/网关和 WAP 内容服务器都位于蓝牙设备上，尽管互操作性并不要求具有这种结构。

WAP 代理/网关/服务器提供含有服务器主页内容的缺省 URL。一个只作为代理的设备并不提供 URL 或相关内容。

3.3 对 WAP 的网络支持

下面对协议栈作出规定。该协议栈可以在 WAP 组件下进行利用。可以支持其它的协议栈，并且应通过蓝牙服务搜索协议体现出来。

3.3.1 PPP/RFCOMM

作为利用 PPP 的 WAP 服务所在的信道，支持蓝牙的设备提供对下列协议栈的支持：

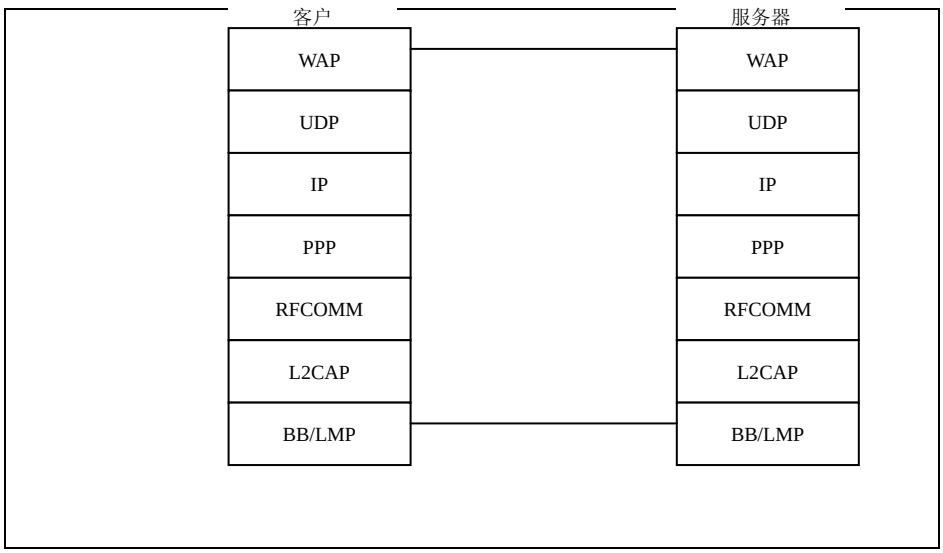


图 10.2 对 WAP 协议的支持

为实现互操作性，本文本假设 WAP 客户端扮演基于 PPP 的局域网访问规范所定义数据终端的角色。此外，还假设 WAP 服务器或代理设备作为局域网访问点。

基带、LMP 和 L2CAP 是 OSI 的第一层和蓝牙协议的第二层。RFCOMM 是 GSM TS07.10 的蓝牙版本。SDP 是蓝牙服务搜索协议。

PPP 即 IETF 点对点协议。WAP 是无线应用协议栈和应用环境。

5. 互操作性要求

5．1 第一步 基本的互操作性

对 WAP Over Bluetooth 的第一步互操作性（必须）：

- 提供对 A 级 WAP 设备的兼容；
- 通过服务搜索机制，为支持 WAP 代理/网关功能的设备提供网络地址；

5．2 第二步 高级互操作性

对 WAP Over Bluetooth 的第二步互操作性（必须）：

- 支持所有第一步的互操作性要求
- 通过服务搜索，提供有关服务器/代理性能的信息和服务器名
- 通过服务搜索，提供有关客户特性信息和客户名
- 对服务器的异步通知
- 对客户的异步通知

6. 服务搜索

6．1 SDP 服务记录

服务记录是 WAP 客户端设备和代理/网关动态查找对方的一种机制。这种用途与其它在两设备间短暂的 WAP 信道不同。也就是说，蓝牙设备不会有一个配置或存储指定代理/网关的具体信道地址。

客户端和代理/网关会在它们互相接近时侦测到对方。蓝牙服务搜索协议使设备能够互相查询对方特性，该特性在互操作性要求一节中定义。

表 10.1 列出了 WAP 代理/网关设备的服务记录

表 10.1 WAP 代理/网关设备的服务记录格式

项目	定义	类型	值	属性 ID	是否必须
ServiceClassIDList				0x0001	M
ServiceClass0	WAP 代理/网关	UUID	WAP		M
BluetoothProfile DescriptList					M
ProfileDescriptor0				0x0009	M
Profile	支持的标准	UUID	LANAccess UsingPPP[4]		M
Version	标准版本	Uint16			M
Protocol DescriptorList					O
Descriptor0	UDP	UUID	UDP		O
Parameter0	WSP 无连接会话端口号	Uint16	9200(缺 省值)		O
Parameter1	WTP 会话端口号	Uint16	9201		O
Parameter2	WSP 安全无连接端口号	Uint16	9202		O

Parameter3	WTP 安全会话端口号	Uint16	9203		O
Parameter4	WAP vCard 端口号	Uint16	9204		O
Parameter5	WAP vCard 端口号	Uint16	9205		O
Parameter6	WAP vCard 安全端口号	Uint16	9206		O
Parameter7	WAP vCard 安全端口号	Uint16	9207		O
ServiceName	可显示的文本名字	String	变量		
NetworkAddress	服务器网络 IP 地址	Uint32	变量		M
WAPGateway*	指示设备是原服务器或代理	Uint8	0x01=原服务器 0x02=代理 0x03=原服务器和代理		M
HomePageURL	主页 URL	URL			C1+

*.第二步互操作性要求

+.如果忽略参数,将指定原服务器的缺省URL: http://networkaddress/index.wml

表 10.2 SDP 协议数据单元

项目	定义	类型	值	属性 ID	是否必需
ServiceClassIDList				0x0001	M
ServiceClass0	WAP 客户	UUID	WAP_CLIENT		M
BluetoothProfile DescriptorList					M
ProfileDescriptor0	支持的标准		LANAccessUsingPPP		M
Profile	标准版本	UUID	变量		M
Version		Uint16	变量		M
ServiceName	可显示的客户端文本名字	String			M

表 10.2 列出了 WAP 互操作性要求的 SDP 协议数据单元。

表 10.3 SDP PDU

PDU 号	SDP PDU	发送能力		检索能力	
		WAP 客户	WAP 代理	WAP 客户	WAP 代理
1	SdpErrorResponse	M	M	M	M
2	sdpServiceSearceAttributeRequest	M	M	M	M
3	sdpServiceSearchAttributeResponse	M	M	M	M

6.1 服务搜索过程

信号发送过程可表示如下:

WAP 客户或代理		WAP 客户或代理
	SdpServiceSearceAttributeRequest =====================➔	
	sdpServiceSearchAttributeResponse ➔=========================	

图 10.3

WAP 服务搜索过程是对称的。每一设备都必须能够处理 PDU，而与设备当前角色无关。至少必须返回服务名字符串。

7. 参考文献

第 11 章 主控制器接口功能规范

本文件对主控制器接口（HCI）的功能作出描述。HCI 提供了对基带控制器和链路管理器的命令接口，以及对硬件状态和控制注册成员的访问。该接口提供了对蓝牙基带容量的统一访问模式。

目 录

1. 介 绍

本文件阐述主控制器接口（HCI）功能规范。HCI 提供访问蓝牙硬件的统一接口。下两节则概要论述蓝牙软件栈和底层蓝牙硬件。第二节提供对主机上底层 HCI 设备驱动器接口的概述；第三节对在主机和主控制器间的流控制进行描述。第四节详细阐述 HCI 命令，并标识出每一命令的参数，列出每一命令相关事件。

1.1 蓝牙软件栈底层

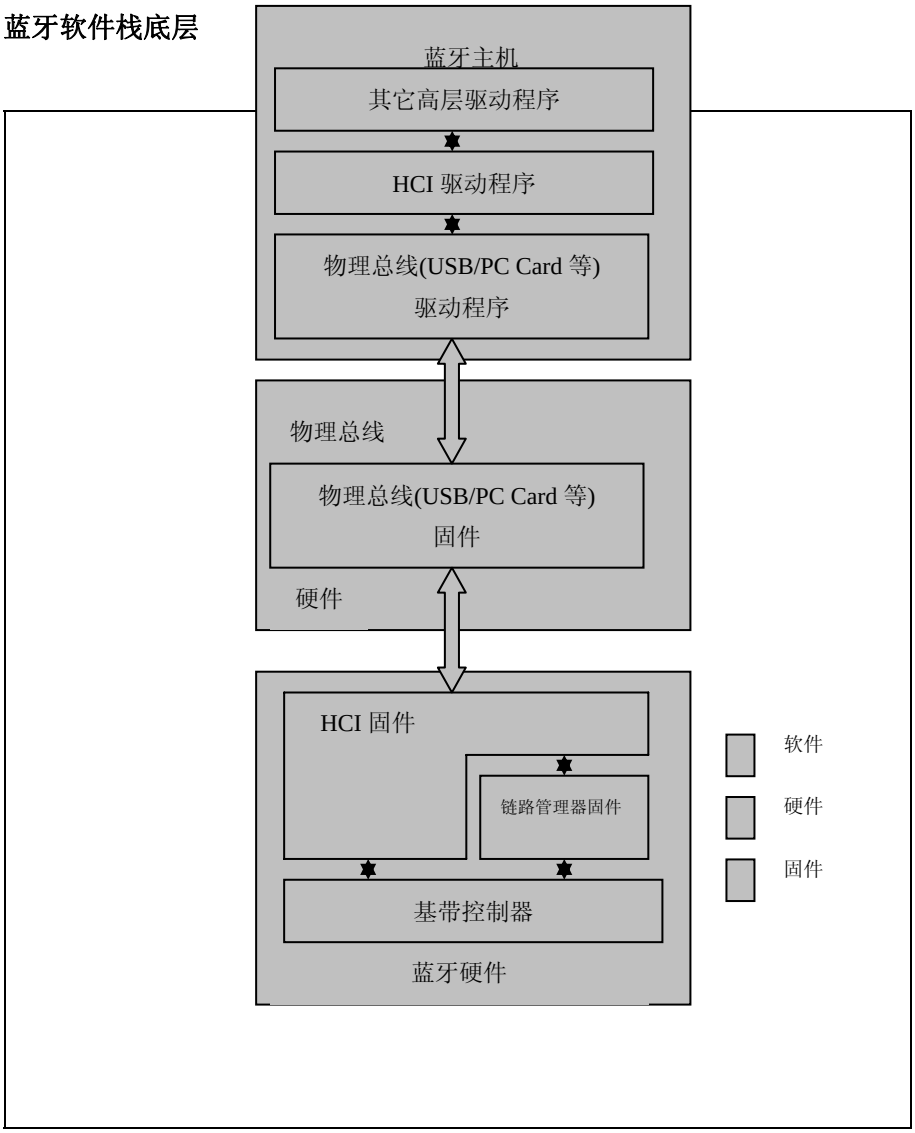


图 11.1:底层软件概览

图 11.1 提供了对软件层低层的概述。通过访问基带命令对如链路管理器、硬件状态注册器、控制注册器、事件注册器等的访问，HCI 规范实现了蓝牙硬件 HCI 命令。

在主机系统 HCI 驱动程序和蓝牙硬件 HCI 基础间存在许多层次。这些中间层和主控制器传输层提供了在没有数据描述信息的情况下传输数据的能力。

图 11.2 用于传输数据的软件低层端对端概览

图 11.2 表现了数据在设备之间的传输路径。主机 HCI 驱动程序在蓝牙硬件上与 HCI 基础交换数据和命令。主机控制传输层的驱动程序（如物理总线）为 HCI 两层提供互相交换信息的能力。

主机将收到 HCI 事件的异步通知，而不管正在使用哪个主控制器传输层。HCI 事件用于在事件发生时通知主机。当主机发现某事件已经发生，它就会分析接收的事件分组以确定发生的是哪个事件。

1.2 蓝牙硬件块描述

图 11.3

图 11.3 中重点全面概述了蓝牙硬件。蓝牙硬件由模拟部分和数字部分组成。模拟部分指蓝牙发射台，数字部分指主控制器。主控制器包括一个硬件信号处理部分——链路控制器（LC），一个 CPU 内核，以及主机环境接口。主控制器的硬件和软件部分如下所述。

1.2.1 链路控制器

链路控制器（LC）由硬件部分、软件部分和物理层协议组成，前两部分执行蓝牙基带处理，后者如 ARQ 协议和 FEC 编码。

链路控制器的功能包括：

- 带有指定服务质量参数的传输类型
- 利用使用硬件快速自动重新请求的授权传递进行异步传输。帧从转发缓冲区中溢出，以利用同步数据；
- 同步传输
- 语音编码。通过健壮的 64 位 CVSD 编码方式和 LOG-PCM 编码方式的硬件实现。
- 加密

1.2.2 CPU 内核

CPU 内核使蓝牙模块处理查询和过滤呼叫请求。主控制器能够通过编程应答某些呼叫消息和认证远程链接。

链路管理器(LM)软件运行在 CPU 内核上。LM 通过链路管理协议找到远程 LM 并通信，以利用底层链路控制器提供其服务。具体细节见”链路管理器协议” 。

1.3 物理总线体系结构

蓝牙设备具有多种能够用于连接蓝牙硬件的物理总线接口。这些总线具有不同的体系结构和参数。蓝牙机控制器初步支持两种物理总线体系结构: USB 和 PC 卡。

1.3.1 USB HCI 体系结构

下图中的方框表示通过 USB HCI 到远程计算机的连接。USB 支持在同一个物理通道上处理多个逻辑通道。因此控制、数据和语音通道不再需要额外的物理接口。但注意不能通过 USB 直接访问蓝牙模块的注册表/内存。如果要做到这一点,则需要使用合适的 HCI 指令和主控制器传输层接口。

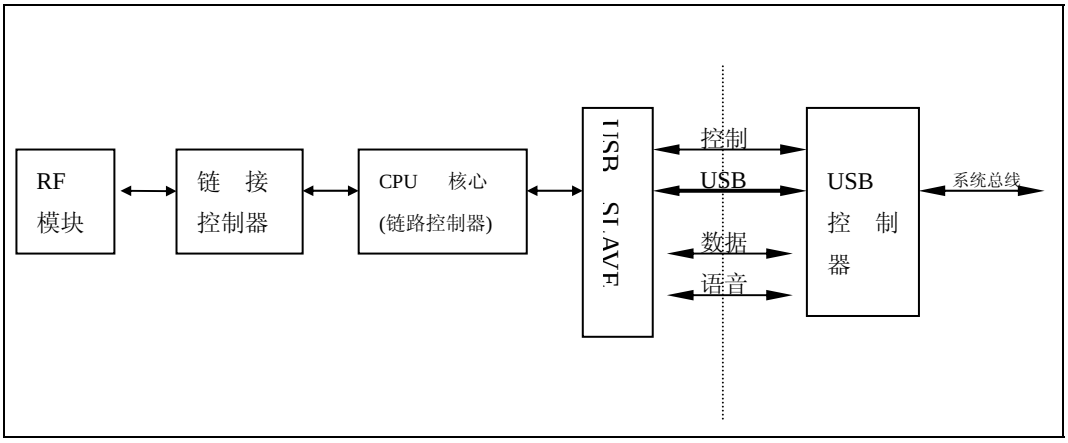


图 11.4 USB HCI 蓝牙模块配置图

1.3.2 PC Card HCI 体系结构

除了 USB 接口，改进的 ISA 总线也可以作为集成 PC 解决方案的选择。与 USB 不同，所有主机和蓝牙模块间的通信都将经过 PC 卡总线接口。在主机 PC 和蓝牙模块之间的通信将通过直接访问注册器/内存进行。下图中的方框表示 PC 卡 HCI 的数据流。

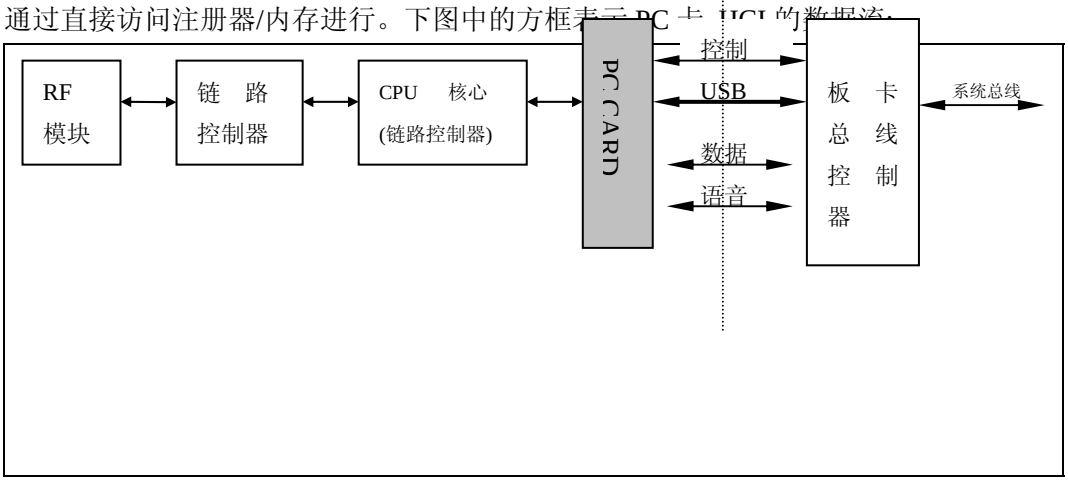


图 11.5 PC 卡蓝牙模块配置图

2 主控制器层概述

主驱动器栈具有介于主控制器驱动程序和主控制器间的传输层。在一个笔记本电脑上，该传输层可以是 PC 卡或通用串口总线(USB)。

传输层主要目的是实现透明性。与主控制器对话的主控制器驱动程序不关心它是运行在 USB 上还是在 PC 卡上。无论 USB 还是 PC 卡都不需要对主控制器驱动程序传送给主控制器的数据可见。这就使接口(HCI)或主控制器能在不影响传输层的情况下升级。

主控制器传输层在下列物理介质的说明文档中进行描述.

- HCI USB 传输层
- HCI RS232 传输层
- HCI UART 传输层

3 HCI 流控制

流控制用于在主机和主控制器之间，避免将传送到未应答远程设备的 ACL 数据溢出主控制器数据缓冲区。主机负责管理主控制器的数据缓冲区。

主机通过发送 Read_Buffer_Size 指令进行初始化。通过该指令返回的两参数可以确定从主机发往主控制器的 HCI ACL 和 SCO 数据分组(不包括报头)的最大长度。另有两返回参数

表示主控制器为等待传输可以缓存的 HCI ACL 和 SCO 数据分组数。在只有一个连接或处于本地回送的情况下,主控制器利用已完成数据分组事件控制从主机发来的数据流。事件分组括一个连接句柄列表，以及从事件返回后已经发送完成的 HCI 数据分组的应答数量。如果该事件没有返回指定连接句柄，则从连接创建开始。发送完成是指数据分组的传输、溢出和回送至主机。根据事件返回信息和存放在主控制器的 Read_Buffer_Size 指令返回参数,主机决定后面 HCI 数据分组发送哪一个连接句柄。每次发送 HCI 数据分组以后,主机假定对应于链接类型的主控制器的一部分空闲缓存空间已被 HCI 数据分组占用。主机收到新的已完成数据分组事件，获取自上次事件返回以后减少的可用缓存空间大小。它就可以计算当前实际可用缓存。当主控制器在其缓存中存放有 HCI 数据分组时,它必须向主机周期性持续发送已完成数据分组事件，直到最终所有 ACL 数据分组都已发送完毕或溢出。事件发送频率由厂商指定。注意: 如果 SCO 流控制失效,则已完成数据分组事件号就不能在 SCO 连接句柄中进行报告(参见 Read/Write_SCO_Flow_Control_Enable)。

对于每一连接句柄,数据都应按照它在主机内的创建顺序,以 HCI 数据分组的形式发送到主控制器。主控制器也以相同的顺序传输从主机收到的数据。同样，从其它设备收到的数据也可作相同处理。这就意味着应在连接句柄的基础上排序。对于每一连接句柄,数据顺序应与其创建时保持一致。

在某种情况下,必须在主控制器到主机的方向上采用流控制。一般采用 Set_Host_Controller_To_Host_Flow_Control 指令关闭或打开流控制。如果流控制已打开,工作方式如上所述。初始化时,主机利用 Host_Buffer_Size 指令通知主控制器发往主机的 HCI ACL 和 SCO 数据分组最大尺寸。该指令还包括其它两个参数,用以通知主控制器在主机数据缓存区中能够存储的 HCI ACL 和 SCO 数据分组的数量。主机就像主控制器利用已完成数据分组数量一样利用 Host_Number_Of_Completed_Packets 指令。Host_Number_Of_Completed_Packets 指令用于无流控制指令可用的情况下,只要存在连接或处于本地循环模式时就可以发送该指令。这就使流控制可以同样方式实现双工，而且同时不干扰正常指令流.

主机收到断开连接完成事件后,就可以认定相对于返回的 Connection_Handle 而发送到主控制器的所有 HCI 数据分组都已溢出,而且相应的数据缓存已被释放。主控制器不必再以完成数据分组事件数量的形式将此通知主机。如果在从主控制器到主机的方向上采用流控制,主控制器将在发送 Disconnection_Complete 后，认定主机收到 Disconnection_Complete 时将释放已发送的 Connection_Handle 所占用的缓存。主机不必再以 Host_Number_Of_Completed_Packets 的形式将该信息通知主控制器。

4 HCI 指令

4.1 介绍

HCI 提供一个访问蓝牙硬件的统一指令方式。HCI 链接指令使主机能够控制到其它蓝牙设备的链接层连接。这些指令通过链路控制器(LM)与远程蓝牙设备交换 LMP 指令。具体细节请参见”链路管理器协议” 。

HCI 策略指令作用于本地或远程 LM。这些策略指令向主机提供影响 LM 管理匹克网的方法。主控制器和基带、信息和状态指令可为主机提供访问主控制器中不同注册表的能力。

执行 HCI 策略指令将耗费不同时间。因此，指令结果将以事件的形式返回给主机。例如，对于大多数 HCI 指令，主控制器在该指令完成时将生成命令完成事件。该事件分组括已完成 HCI 指令的返回参数。为了在 HCI-传输层上侦测出错信息，必须定义在主控制器收到命令和发出应答之间的应答时间。由于最大应答时间取决于所采用的 HCI-传输层，因此推

荐采用 1 秒的缺省值。这个事件值也取决于在指令队列中未处理指令的数量。

4.2 术语

基带数据分组:数据的最小单位,它在各个设备之间进行传输,在'基带规范'中定义;

数据分组:是比基带包更高层次的协议报文,目前只定义了 L2CAP, 参见'逻辑链接控制和调整协议规范。其它的包类型在今后逐步定义。

连接句柄:一个连接句柄就是一个用于唯一标识蓝牙设备之间数据或语音连接的 12 位的标识符。连接句柄可以通过唯一标识两蓝牙设备间的数据管道进行访问。同时, 无论设备进入空闲、休眠还是挂起状态, 都应在连接的整个生命周期内保持连接句柄。连接句柄值在主机和主控制器间取本地值。在两个蓝牙设备间可以拥有多个连接句柄, 但只能保持一个 ACL 连接。

事件:指 HCI 用于通知主机命令完成和链接层状态变动等信息的一种机制。

4.1 数据和参数格式

- 如没有另外指定其它格式,所有值都应采用二进制或大 Edian 码;
- 另外, 当定义值时, 所有具有负值的参数必需使用两位补码.
- 参数数组采用以下两个概念进行定义:ParameterA[i], 如果参数数组的一个集合定义为如 ParameterA[i]、ParameterB[i]的格式, 那么参数数组顺序如下: ParameterA[0] 、ParameterB[0] 、 ParameterA[1] 、 ParameterB[1].....ParameterA[n] ParameterB[n];
- 如果没有另外给出说明, 所有参数值都应按小 Edian 码的格式发送和接收;
- 所有非数组的命令和指令参数, 以及所有参数数组元素都具有固定长度。参数和非数组参数的长度都包含在一条指令里, 并为每一命令或事件定义事件。参数数组内元素数量可以不定。

4.4 HCI 信息交换

主控制器传输层提供 HCI 信息的透明传输。该传输机制为主机提供向主控制器发送 HCI 指令、HCI 数据和 SCO 数据, 以及从主控制器接收 HCI 事件、ACL 数据和 SCO 数据的能力。

由于主控制器传输层提供 HCI 信息的透明传输, HCI 规范对主机和主控制器间交换的指令、事件、数据的格式进行了定义。下节就 HCI 包格式做出说明.

4.4.1 HCI 指令分组

HCI 指令分组用于从主机向主控制器发送指令。HCI 指令分组的格式如图 4.1 所示,其中每一段的定义在下面解释。当主控制器完成大多数指令的发送时,就向主机发送 Commad Complete 指令完成事件。当然,其中一些指令在它们完成后并不接收 Command Complete 指令完成事件。相反，当主控制器收到一个 HCI 指令并准备执行时, 它将向主机返回一个 Command Status 指令状态事件。然后，当与该指令相关联的动作执行后, 对应于该发出指令的事件也将由主控制器发往主机。但是，如果由于参数错误或该指令非法等原因而导致该指令不能执行时, 则不返回对应于该发出指令的事件。这时, 指令状态事件将在状态参数中返回应答的出错码。开启电源或重新启动时, 主机在收到指令完成或指令状态事件之前会一直发送一个最大长度的 HCI 指令数据分组。如果在返回指令完成事件时出错, Return_Parameter 域就不能包含该指令的返回参数, 而是返回用于解释出错原因,同时也是第一个返回值的状态参数。如果在 Status 参数后紧接着是 Connection_Handle 或 BD_ADDR 参数, 仍须返回该参数, 以便主机能够判定指令完成事件属于哪个指令实例。这时, Connection_Handle 或 BD_ADDR 参数与对应指令参数具有相同值。出错时返回参数个数根据应用不同情况确定。

注：Read_BD_ADDR 指令的返回参数 BD_ADDR 不能用于判定指令结束事件属于哪个 Read_BD_ADDR 指令实例。因此，并不强制要求主控制器在出错时返回该参数。

如果出错时,一条指令没有返回指令完成事件，那么与此指令关联事件的所有返回值都为非法值。主机必须关心哪个参数具有合法的取值，而这取决于关联于给定指令的指令完成事件的状态参数值。指令完成事件和指令状态事件分组含一个叫做 Num_HCI_Command_Packets 的参数。该参数表示主机当前允许发往主控制器的 HCI 指令分组的数量。主控制器可以缓存一个或多个 HCI 指令分组，主控制器应按照收到的顺序执行指令。但主控制器可以在前一条指令未执行完时开始执行下一条指令。因此,实际上指令并不一定按照它们最初收到时的顺序执行。主控制器必须能够接收 HCI 指令分组和除 HCI 指令报头以外的 255 字节数据。

每一指令都指定了一个 2 字节的操作码，用于唯一标识指令类型。操作码参数分为两段,操作组段(OGF)和操作码指令段(OCF) 。OGF 占用操作码的上 6 位，OCF 占用其余 10 位。OGF 的 0x3F 保留用于厂商调试, 0x3F 保留用于蓝牙标志测试。操作码的结构使得能够在不必对整个操作码完全解码的情况下即可获知附加信息。

注: OGF 由那些保留用于厂商调试指令的位组成。这些指令由厂商指定，并在生产中使用，用于升级软件或调试。

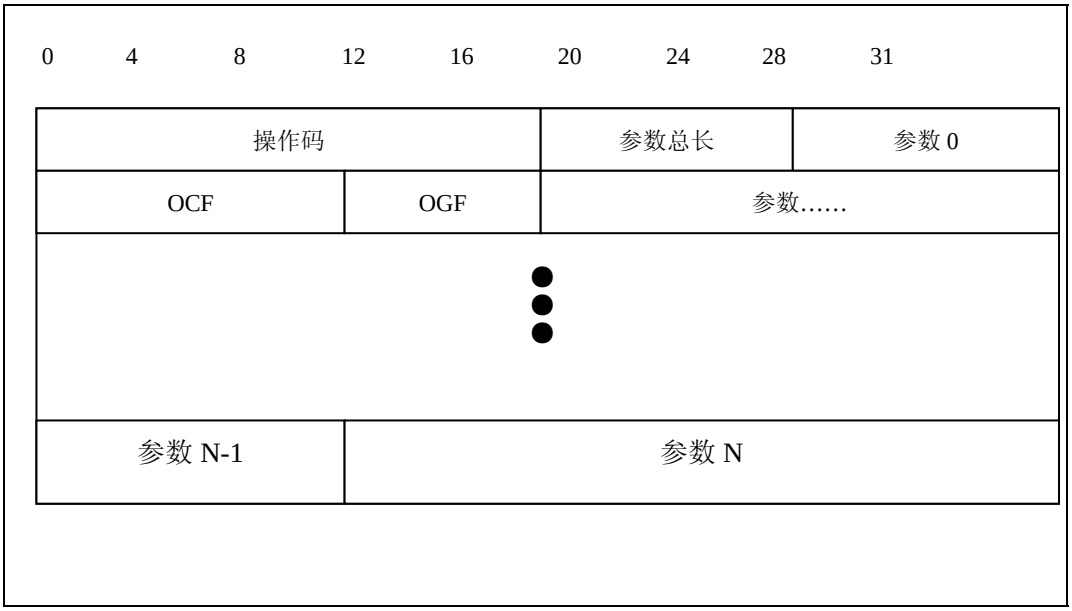


图 11.6 HCI 指令分组

操作码: 2 字节

值	参数描述
0xXXXX	OGF 占用 6 位:0x00-0x3F(0x3E 保留用于蓝牙标志测试, 0x3F 保留用于用户调试指令) OCF 占用 10 位:0x0000-0x03FF

Parameter_Total_Length: 1 字节

值	参数描述
0xXX	所有数据分组中的参数总长以字节度量

	N.B.:参数总长,不是参数个数

参数 0-N:

值	参数描述
0xXX	每一指令都有几个与其关联的参数。这些参数及其大小由指令定义，其大小一般为整数个字节。

4. 4. 2 HCI 事件分组

主控制器利用 HCI 事件分组在事件发生时通知主机。主机必须能够接收 HCI 指令和除 HCI 指令报头以外的 255 字节数据。HCI 事件分组格式如图 4.2 所示.其中每一段的定义在下面讨论。

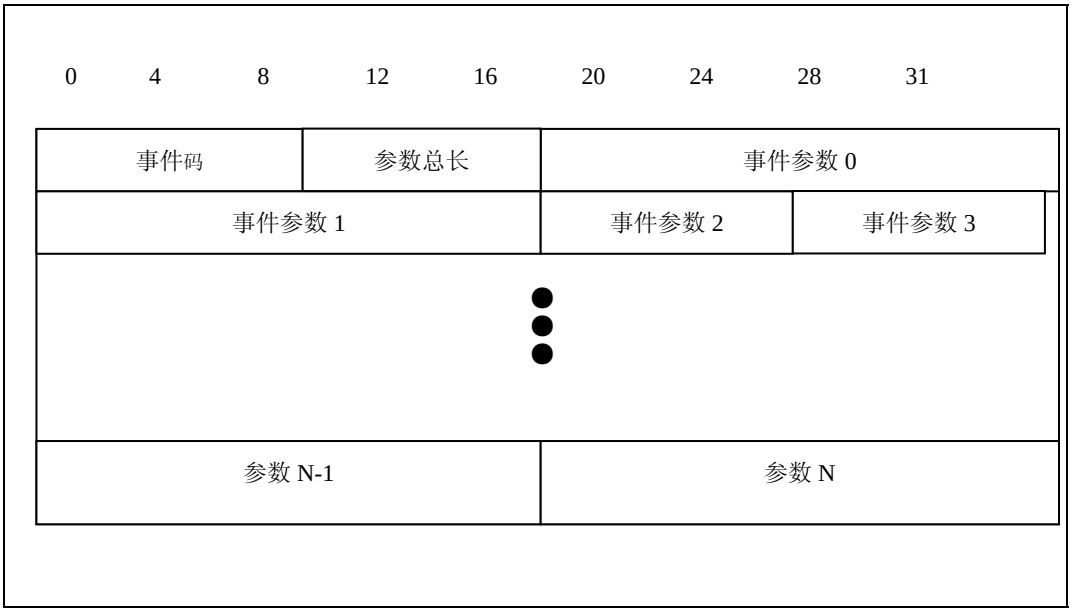


图 11.7　HCI 事件分组

操作码:　　2 字节

表 11.4

值	参数描述
0xXX	每一事件都指定 1 字节事件码，以唯一标识不同事件类型。 范围: 0x00-0xFF(事件码 0xFF 保留用于用户调试事件事件码。而且，事件码 0xFE 保留用于蓝牙标志测试。)

Parameter_Total_Length:　　1 字节

表 11.5

值	参数描述
0xXX	所有数据分组中的参数总长以字节度量。

参数 0-N:

表 11.6

值	参数描述
0xXX	每一指令都有几个与其关联的参数。这些参数及其大小由指令定义，其大小一般为整数个字节。

4.4.3 HCI 数据分组

HCI 数据分组用于在主机和主控制器之间交换数据。数据分组根据 ACL 和 SCO 数据分组类型进行定义.HCI ACL 数据分组格式如图 4.3 所示,SCO 数据分组格式如图 4.4 所示.数据分组中各域定义在下面讨论.

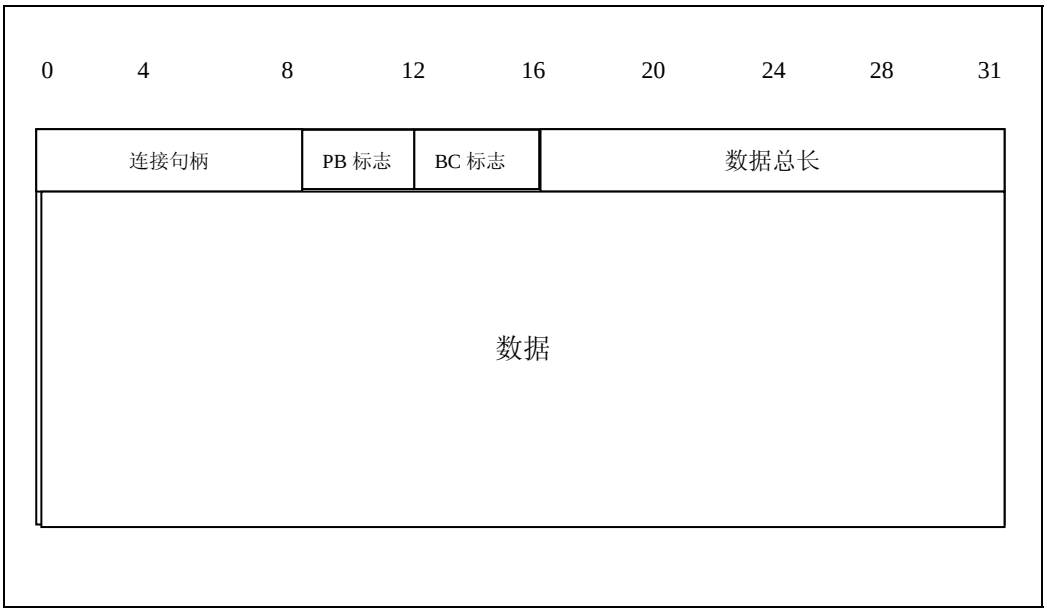


图 11.8 HCI ACL 数据分组

Parameter_Boundary_Flag : 2 位

表 11.7

值	参数描述
00	保留
01	用于高层报文的数据分组分段
10	高层报文的第一个数据分组(即: L2CAP 数据分组的开始)
11	保留

Broadcast_Flag(在主机到主控制器的报文中) : 2 位

表 11.8

值	参数描述
00	没有广播,只是点到点
01	激活的广播:包发往所有激活的从单元
10	匹克网广播(数据分组发往所有从单元, 包括休眠单元)
11	保留

Data_Total_Length: 2 字节

表 11.9

值	参数描述
0xXXXX	数据长度以字节度量

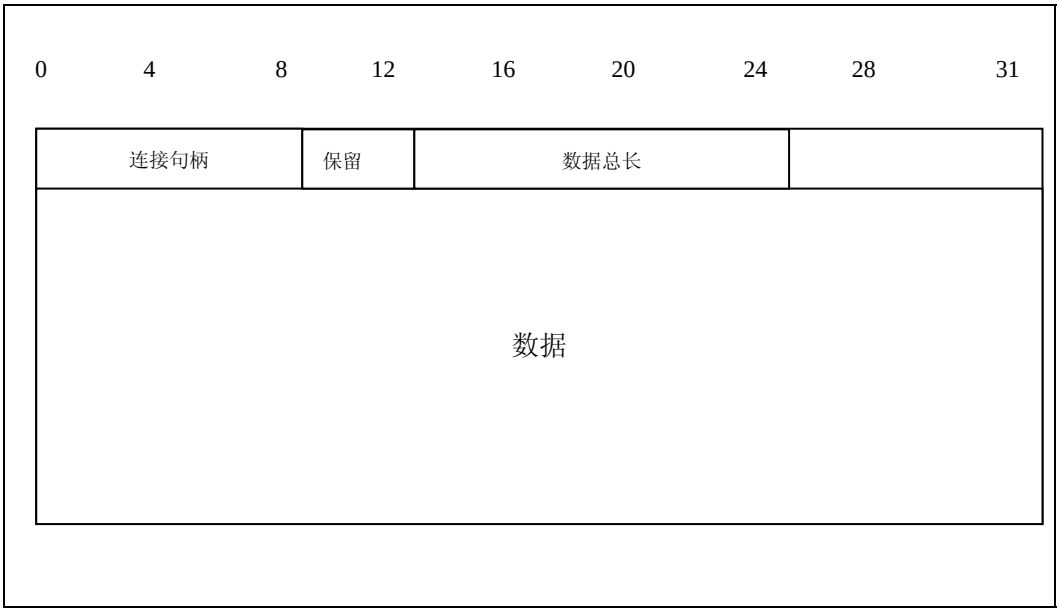


图 11.9 HCI SCO 数据分组

Connection_Handle: 12 位

表 11.10

值	参数描述
0xXXX	连接句柄用于传输数据或段 范围:0x0000-0x0EFF(0x0F00-0x0FFF 保留) 在开启电源或重启动后,主机首次发送 Broadcast_Flag 置为 01b(广播激活)或 10b(匹克网广播)的 HCI 数据分组, Connection_Handle 值必须不是现在主控制器指定的值。主机对于激活广播和匹克网广播采用不同连接句柄。 对于每一类连接, 主控制器直到重启动都要使用同一连接句柄。 注:

Connection_Handle

表 11.11

值	参数描述
0xXXX	连接句柄用于传输数据或段 范围:0x0000-0x0EFF(0x0F00-0x0FFF 保留) 在开启电源或重启动后,主机首次发送 Broadcast_Flag 置为 01b(广播激活)或 10b(匹克网广播)的 HCI 数据分组, Connection_Handle 值必须不是现在主控制器指定的值。主机对于激活广播和匹克网广播采用不同连接句柄。对于每一类连接, 主控制器直到重启动都使用同一连接句柄。 注: 主控制器一定不会发送包括用于广播的新 Connection_Handle 值的连接完成事件。 注: 有些情况下,会发生这样一种情况:主控制器在解释从主机收到的广播包之前发送连接完成事件,而且连接完成事件和 HCI 数据分组具有相同 Connection_Handle 值。为了避免这种冲突, 应作以下处理: 如果收到包含用于广播连接句柄的连接完成事件, 主机在为新的连接发送数据分组之前

	必须处于等待状态，一直要等到它收到一些已完成包事件，这些事件表示已没有属于连接句柄的广播包。此外,主机必须由用于对应广播类型的 Connection_Handle 改变为不由主控制器指定的 Connection_Handle。Connection_Handle 必须用于下面的广播类型,直到重新启动或发生相同的冲突。然而这种情况很少发生。 在上述冲突情况下，主控制器必须能够区分由主机发出的广播报文和新连接发出的报文,尽管其连接句柄值相同。 对于从 Broadcasst_Flag 为 01 或 10 的主机发送到主控制器的 HCI 数据分组，Connection_Handle 参数应包括到发送广播的主控制器的 ACL 连接的连接句柄。 注:用于广播的连接句柄不能判定一个 ACL 点到点连接,所以这些句柄不能用于含有 Connection_Handle 参数的指令,而且这些句柄不能在具有 Connection_Handle 参数的任何事件中返回,除了已完成包事件的数量。

标志: 大小:2bits

标志由 Packet_Boundary_Flag 和 Broadcast_Flag 组成. 在第二类 HC。ACL 数据分组 Packet_Boundary_Flag 位于第 4 位和第 5 位, Broadcast_Flag 位于第 6 位和第 7 位。

表 11.12

值	参数描述
0xXXX	连接句柄用于按段传输 SCO 数据分组。 范围:0x0000-0x0EFF(0x0F00-0x0FFF 保留)

保留位由 HCI SCO 数据分组中第 2 字节的 4 到 7 位组成。

保留字: 4 位

表 11.13

值	参数描述
XXX	保留

Data_Total_Length: 1 字节

表 11.14

值	参数描述
0xXX	SCO 数据长度以字节度量

4.5 链路控制指令

链路控制指令允许主控制器控制到其它蓝牙设备的连接。使用链路控制指令时，链路管理器(LM)负责控制如何建立和保持蓝牙匹克网和散射网。这些指令指示 LM 创建和修改与蓝牙远程设备的链接层连接，执行对范围内其它蓝牙设备和 LM 指令的查询。对于链路控制指令, OGF 设为 0x01。

表 11.5

指令	指令描述
Inquiry	该指令使蓝牙设备进入查询模式，查询模式用于搜索邻近的蓝牙设备.
Inquiry_Cancel	Inquiry_Cancel 使处于查询模式的蓝牙设备取消 Inquiry 模式.
Periodic_Inquiry_Mode	Periodic_Inquiry_Mode 指令用于将蓝牙设备配置为能够基于指定周期执行自动查询.
Exit_ Periodic_Inquiry_Mode	Periodic_Inquiry_Mode 指令用于终止轮询模式,如果本地设备处于轮询模式

Create_Connection	Create_Connection 指令使链路管理器能够利用指令参数定义的 BD_ADDR 创建到蓝牙设备的 ACL 连接.
Disconnect	本指令用于中止现有连接
Add_SCO_Connection	Add_SCO_Connection 指令使链路管理器能够利用连接句柄指令参数指定的 ACL 连接创建 SCO 连接
Accept_Connection_Request	Accept_Connection_Request 指令用于接收新的呼入连接请求.
Reject_Connection_Request	Reject_Connection_Request 指令用于拒绝新的呼入连接请求
Link_Key_Request_Reply	Link_Key_Request_Reply 指令用于应答从主机控制器发出的链接关键字请求事件,并指定存储在主机上的链接关键字作为与 BD_ADDR 指定的蓝牙设备进行连接用的链接关键字
指令	指令描述
Link_Key_Request_Negative_Reply	如果主机上没有存储的链接关键字作为与 BD_ADDR 指定的蓝牙设备进行连接用的链接关键字,Link_Key_Request_Negative_Reply 指令用于应答从主机控制器发出的链接关键字请求事件,
PIN_Code_Request_Reply	PIN_Code_Request_Reply 指令用于应答从主控制器发出的 PIN 编码请求事件,并指定用于连接的 PIN 编码.
PIN_Code_Request_ Negative_Reply	该指令指令用于在主机不能指定用于连接的 PIN 编码.,应答从主控制器发出的 PIN 编码请求事件
Change_Connection_Packet_Type	Change_Connection_Packet_Type 指令用于改变用于正在建立的连接的包类型.
Authentication_Requested	该指令用于在与指定连接句柄关联的两个蓝牙设备之间建立身份认证.
Set_Connection_Encryption	该指令用于建立和取消链接层次的加密
Change_Connection_Link_Key	该指令用于强制关联到连接句柄的两个设备建立连接,并生成一个新的连接关键字
Master_Link_Key	该指令用于强制关联到连接句柄的两个设备利用主设备临时链接关键字或常规关键字.
Remote_Name_Request	Remote_Name_Request 指令用于获取另一蓝牙设备的用户名
Read_Remote_Supported_Features	该指令请求远程设备所支持特性的列表
Read_Clock_Offset	Read_Clock_Offset 指令允许主机读取远程设备时隙信息.

4.5.1 Inquiry

表 11.16

指令	OCF	指令参数	返回参数
HCI_Inquiry	0x0001	LAP,Inquiry_length,Num_Response	

描述:

该指令使蓝牙设备进入查询模式。查询模式用于搜索邻近的蓝牙设备。LAP 输入参数包含当进行查询过程时从查询访问码中得到的 LAP。Inquiry_Length 参数指定查询模式的持续时间。超出该时间则中止查询。Num_Response 参数指定查询中止前能收到的应答数量。当查询指令由蓝牙设备开始启动时，主控制器将指令状态事件发往主机。当查询进程结束时，主控制器也向主机发送一指令状态事件，表示已完成查询。查询指令事件的事件参数将从查询进程中得到一个结果集。该结果集报告邻近发出应答的蓝牙设备数量。当蓝牙设备应答查询报文时，将发生应答结果事件，以通知主机搜索结果。

一个在查询或查询周期内应答的设备，通常应在查询结果事件中向主机报告已在当前查询或查询周期中报告该设备，以及该设备是否已用 Set_Event_Filter 指令过滤掉。是否报告这些情况取决于实际执行情况。也就是说，取决于先前结果是否已保存到主控制器，以及已经保存了多少应答信息.。推荐使用在一个查询或查询周期内主控制器只报告一个特定设备。

指令参数:

LAP 长度: 3 字节

表 11.17

值	参数描述
0x9E8B00-0X9E8B3F	当开始访问进程时，访问识别码将从 LAP 引申而来。参见’蓝牙分配号码’部分。

Inquiry_Length: 长度:1 字节

表 11.18

值	参数描述
N=0xXX	查询最长持续时间。 大小:1 字节 范围:0x01-0x30 时间=N*1.28 秒 范围:1.28 – 61.44 秒

Num_Response

表 11.19

值	参数描述
0x00	缺省值,不限制应答次数
0xXX	从查询开始的最大应答次数 范围:0x01-0xFF

返回参数: 无

在没有屏蔽的情况下生成的事件:

当主控制器启动查询进程时，从主控制器向主机发送一个指令状态事件。

对每一个应答查询消息的蓝牙设备都要创建一个查询结果集事件而且,多个应答查询消息的蓝牙设备将生成同一事件。当查询进程结束时,生成一个查询结束事件。

注:主控制器不是通过发出指令完成事件来表示指令完成，而是通过发送查询完成事件来表示。取消查询进程不会生成查询完成事件。

4.5.2 Inquriy_Cancel

表 11.20

指令	OCF	指令参数	返回参数
HCI_ Inquriy_Cancel	0x0002		Status

描述:

该指令使蓝牙设备能够终止当前查询。该指令允许主机中断蓝牙设备当前运行任务并请求蓝牙设备执行另一任务。该指令只能在查询指令发出和收到查询指令的指令状态事件后,查询完成事件发生之前发出。

返回参数:

status:

表 11.21

值	参数描述
0x00	Inquiry_Cancel 指令执行成功
0x01-0xFF	Inquiry_Cancel 指令执行失败.

在没有屏蔽的情况下生成的事件:

当查询取消事件完成时，生成一个指令完成事件。对于已取消的查询进程不会生成查询完成事件。

4.5.3 Periodic_Inquiry_Mode

表 11.22

指令	OCF	指令参数	返回参数
HCI_Periodic_Inquiry_Mode	0x0003	Max_Period_length, Min_Period_length, LAP,Inquiry_length,Num_Response	Status

描述:

Periodic_Inquiry_Mode 指令用于配置蓝牙设备进入执行自动查询的轮询模式。Max_Period_Length 和 Min_Period_Length 参数定义两个连续发生的查询之间的间歇时间长度，该时间指从上一次查询的开始到下一次查询的开始之间的这段时间。主控制器利用这个时间范围在两次连续查询之间确定一次新的查询随机时间。当查询进程开始后, LAP 输入参数包括查询识别码引申来的 LAP。Inquiry_Length 参数指定查询模式的的持续时间。时间超出时将中止查询。Num_Response 参数指定查询中止前能够接收的应答次数。当蓝牙设备一启动查询进程，也就结束该指令。当每一次轮询完成后，主控制器将向主机发送查询完成事件，表示最近一次轮询已经完成。查询完成事件的参数含有将含有前一次轮询进程的结果集。该结果集报告邻近发出应答的蓝牙设备数量。当一个蓝牙设备对查询报文做出应答时，就可以通过查询结果事件通知搜索到的主机.

注: Max_Period_Length> Min_Period_Length> Inquiry_Length

在查询或查询周期内应答的设备,通常应在查询结果事件中向主机报告:在当前查询或查询周期内是否已报告了该设备，以及是否已经用 Set_Event_Filter 指令将该设备过滤。如果在当前查询或查询周期内已报告了该设备,是否再报告它取决于实际应用情况。推荐在一次查询或查询周期内只对指定设备报告一次。

指令参数:

Max_Period_Length: 大小:2 字节

表 11.23

值	参数描述
N=0xXXXX	两个连续查询之间的最大时间间隔 大小:2 字节 范围:0x03 – 0Xffff 时间=N*1.28 秒 范围:3.84-83884.8 秒 0.0 – 23.3 小时

Min_Period_Length: 大小:2 字节

表 11.24

值	参数描述
N=0xXXXX	两个连续查询之间的最小时间间隔 大小:2 字节 范围:0x02 – 0Xffff 时间=N*1.28 秒 范围:2.56 - 83883.52 秒 0.0 – 23.3 小时

LAP 大小:3 字节

表 11.25

值	参数描述
0x9E8B00 –0X9E8B3F	当查询进程开始后,LAP 输入参数包括查询访问码来源的 LAP.

Inquiry_Length: 大小:1 字节

表 11.26

值	参数描述
N=0xXX	指定查询模式的的持续时间. 大小:1 字节 范围:0x01-0x30 时间=N*1.28 秒 范围:1.28 – 61.44 秒

Num_Response: 大小:1 字节

表 11.27

值	参数描述
0x00	缺省值,未限制应答次数
0xXX	在查询中止前应答查询的最大次数 范围:0x01 – 0Xff

返回参数:

Status: 大小:1 字节

表 11.28

值	参数描述
0x00	轮询模式指令成功
0x01- 0xFF	轮询模式指令失败,

在未屏蔽的情况下生成的事件:

当主控制器向主机发送该指令的指令完成事件，则轮询模式开始。应答查询报文的每一蓝牙设备都将创建一个查询结果事件。此外，应答查询报文的多个蓝牙设备也将组合为同一事件。每次轮询进程结束时将生成一条查询完成事件。取消查询进程不生成任何查询完成事件。

4.5.4 Exit_Periodic_Inquiry_Mode

表 11.29

指令	OCF	指令参数	返回参数
HCI_ Exit_Periodic_Inquiry_Mode	0x0004		Status

描述:

退出周期性查询模式指令用于在本地设备处于周期性查询模式时,终止周期性查询模式. 如果本地设备当前处于查询进程中，则将直接终止查询进程. 而且主控制器将不在执行周期性查询，直至周期性查询指令再次发出.

指令参数：无

返回参数：

S tatus: 大小： 1 字节

表 11.30

值	参数描述
0 x00	退出周期性查询指令成功
0 x01-0xFF	退出周期性查询失败.

在未屏蔽的情况下生成的事件:

本指令的指令完成事件在本地设备不再处于周期性查询模式时发生. 对于取消的查询进程不会生成查询完成事件.

4.5.5 Create_Connection

表 11.31

指令	ＯＣＦ	指令参数	返回参数
HCI_Create_Connection	0x0005	BD_ADDR,Packet_Type, Page_Scan_Repetition_Mode, Page_Scan_Mode,Clock_Offset, Allow_Role_Switch	

描述:

本指令将使链路管理器创建与由指令参数指定 BD_ADDR 的蓝牙设备的相互间连接. 本指令使本地蓝牙设备开始呼叫进程以创建一链路层连接. 链路管理器将确定新的ＡＣＬ连接如何建立． ＡＣＬ连接由设备和匹克网的当前状态，以及要连接的设备的状态决定. Packete_Type 指令参数指定链路管理器为ＡＣＬ连接使用何种分组类型. 链路管理器为了发送ＨＣＩ ＡＣＬ数据分组只能使用由 Packete_Type 指令参数指定的分组类型. 可以通过执行不同分组类型间位异或操作为分组类型参数指定多个分组类型. 链路管理器将选择

从可接受分组类型列表中选择哪一分组类型．Page_Scan_Repetition_Mode 和 Page_Scan_Mode 参数指定ＢＤ＿ＡＤＤＲ代表设备的呼叫扫描模式．这就是在查询进程中的所需参数．Clock_Offset 参数是其本地时钟与ＢＤ＿ＡＤＤＲ所代表远程设备时钟之间的偏差．只能使用 2 到１６位的偏差，且它们也将各自直接映射到参数的 0 到１４位．Clock_Offset 的第１５位 Clock_Offset_Valid_Flag 即用于表示时钟偏差是否合法．在连接完成事件中将为该连接返回一连接句柄．Allow_Role_Switch 参数说明当远程设备在连接初始化过程中请求主从角色切换时（在本地主控制器返回连接完成事件之前），本地设备是接受还是拒绝该请求．不同分组类型定义见＂基带规范＂。

注意：必须至少指定一种分组类型．主机最好能够启用尽量多的分组类型，以使链路管理器能够高效执行．但是，主机不能启用本地设备不支持的分组类型。

指令参数：

ＢＤ＿ＡＤＤＲ 大小：６字节

表 11.32

值	参数描述
0 xXXXXXXXXXXXX	要连接设备的ＢＤ＿ＡＤＤＲ

Ｐacket_Type: 大小：２字节

表 11.33

值	参数描述
0x0001	保留
0x0002	保留
0x0004	保留
0x0008	ＤＭ１
0x0010	ＤＨ１
0x0020	保留
0x0040	保留
0x0080	保留
0x0100	保留
0x0200	保留
0x0400	ＤＭ３
0x0800	ＤＨ３
0x1000	保留
0x2000	保留
0x4000	ＤＭ５
0x8000	ＤＨ５

Ｐage_Scan_Repetition_Mode: 大小：１字节

表 11.34

值	参数描述
0x00	Ｒ０
0x01	Ｒ１
0x02	Ｒ２
0x03-0xFF	保留

Page_Scan_Mode: 大小：1 字节

表 11.35

值	参数描述
0x00	强制呼叫扫描模式
0x01	呼叫扫描模式 1(可选)
0x02	呼叫扫描模式 2(可选)
0x03	呼叫扫描模式 3(可选)
0x04-0xFF	保留

Clock_Offset: 2 字节

表 11.36

值	参数描述
Bit 14.0	
Bit15	Clock_Offset_Valid_Flag 非法时隙=0 合法时隙=1

Allow_Role_Switch:

表 11.37

值	参数描述
0x00	本地设备为主设备,它不会在连接建立时接受由远程设备请求的主从互换.
0x01	本地设备为主设备.但在连接建立时可以接受由远程设备请求的主从互换,变为从设备
0x02-oxFF	保留

返回值:无

在没有屏蔽的情况下生成的事件:

当主控制器接收到连接创建指令时，主控制器向主机发送指令状态事件。而且,当 LM 确定连接已经建立起来时，在两个蓝牙设备上形成连接的主控制器将向每一主机发送连接完成事件。如果该指令执行成功，则连接完成事件将包括连接句柄。

注:主控制器不是通过发出指令完成事件来表示指令完成，而是通过发送连接完成事件来表示。取消查询进程不会生成查询完成事件。

4.5.6 Disconnect

表 11.38

指令	OCF	指令参数	返回参数
HCI_Disconnet	0x0006	Connection_Handle, Reason	

描述:

Disconnection 指令用于终止现有连接。Connection_Handle 指令参数表示要断开哪个连接。Reason 指令参数表示终止连接的原因。远程蓝牙设备将在连接断开完成事件中接收

Reason 指令参数。在物理链接上 ACL 连接断开前,同一物理连接上所有 SCO 连接都将被断开。

指令参数:

Connection_Handle 大小:2 字节,即 12 位

表 11.39

值	参数描述
0Xxxxx	要断开的连接的连接句柄 范围:0x0000-0x0FFF 保留使用

Reason: 大小:1 字节

表 11.40

值	参数描述
0x13-0x15,0x1A	其它端终止连接出错码(0x13-0x15),以及其它未给出的远程部件出错码(0x1A) 范围:0x0000-0x0FFF 保留使用

返回值:无

在没有屏蔽的情况下生成的事件:

当主控制器接收到 Disconnect 指令时，它向主机返回指令状态参数。当连接终止时每一主机都将发生连接断开完成事件，指示该指令已执行。

注: 主控制器不是通过发出指令完成事件来表示指令完成，而是通过发送查询完成事件来表示。取消查询进程不会生成查询完成事件。

4.5.7 Add_SCO_Connection

表 11.41

指令	OCF	指令参数	返回参数
HCI_Add_SCO_Connection	0x0007	Connection_Handle, Packet_Type	

描述:

该指令能够使链路管理器利用 Connection_Handle 指令参数指定的 ACL 连接，创建一个 SCO 连接。该指令能够使本地蓝牙设备创建 SCO 连接。由链路管理器确定如何建立新连接。该连接由设备和匹克网的当前状态，以及要连接设备的状态等因素确定。Packet_Type 指令参数用于说明链路管理器将在此连接上使用何种报文类型。链路管理器只能使用由 Packet_Type 指令参数指定的报文类型，以用于发送 HCI SCO 数据分组。可以通过执行不同报文类型的逻辑 OR 操作，由 Packet_Type 指令参数指定多个报文类型。链路管理器可以在多个可接收的报文类型中进行选择。在连接完成事件中返回该连接的连接句柄。

注: SCO-连接只能在 ACL 连接已经存在时创建。不同报文类型的定义,参见'基带规范';

注: 至少应指定一种数据分组。主机应尽量支持更多的报文类型，以使链路管理器能够更有效工作。但是，主机不能采用本地设备不支持的报文类型。

指令参数:

Connection_Handle 大小:2 字节

表 11.42

值	参数描述
0xXXXX	用于 SCO 连接地 ACL 连接的句柄 范围:0x0000-0x0EFF,保留使用

Packet_Type: 大小:2 字节

表 11.43

值	参数描述
0x0001	保留
0x0002	保留
0x0004	保留
0x0008	保留
0x0010	保留
0x0020	HV1
0x0040	HV2
0x0080	HV3
0x0100	保留
0x0200	保留
0x0400	保留
0x0800	保留
0x1000	保留
0x2000	保留
0x4000	保留
0x8000	保留

返回参数:无

在没有屏蔽的情况下生成的事件:

当主控制器接收到 Add_SCO_Connection 指令时，将向主机发送指令状态事件。此外，当 LM 确认连接已建立，构成连接两设备的主控制器将向每一个主机发送连接完成事件。如果指令成功执行，则连接完成指令分组括连接句柄。

注: 主控制器不是通过发出指令完成事件来表示指令完成，而是通过发送连接完成事件来表示。

4.5.8 Accept_Connection_Request

表 11.44

指令	OCF	指令参数	返回参数
HCI_Accept_Connection_Request	0x0009	BD_ADDR,Role	

描述:

Accept_Connection_Request 指令用于接受最新的呼入连接请求。Accept_Connection_Request 指令只能在连接请求事件发生后发出。连接请求事件将返回请求连接设备的 BD_ADDR。该指令使链路管理器能够利用由该指令参数指定的 BD_ADDR 创建到蓝牙设备的连接。由链路管理器确定如何建立新的连接，该连接由设备和匹克网的当前状态，以及要连接设备的状态确定。Role 指令参数允许主机指定链路管理器是否执行主-从切换，以及是否成为连接的主设备。而且，在本地蓝牙模块上连接超时之前应确定是否接受连接。

指令参数:

BD_ADDR: 大小:6 字节

表 11.45

值	参数描述
0XxxxxXXXXXXXX	要连接设备的 BD_ADDR

Role: 大小:1 字节

表 11.46

值	参数描述
0x00	成为连接的主设备.LM 将执行主/从切换
0x01	保持为连接的从设备, LM 不执行主/从切换

返回参数:无

在没有屏蔽的情况下生成的事件:

当主控制器开始创建连接时，Accept_Connection_Request 主控制器发送指令状态事件.此外，当链路管理器确认链接已建立.在链接的两端上蓝牙设备的主控制器将向主机发送链节完成事件.如果该指令成功完成,则链接完成事件分组括连接句柄。

注: 主控制器不是通过发出指令完成事件来表示指令完成，而是通过发送连接完成事件来表示。

4.5.9 Reject_Connection_Request

表 11.47

指令	OCF	指令参数	返回参数
HCI_Reject_Connection_Request	0x000A	BD_ADDR,Reason	

描述:

Reject_Connection_Request 指令用于拒绝新的呼入请求。只有在连接请求事件发生后才呼叫 Reject_Connection_Request。连接请求事件将返回请求连接设备的 BD_ADDR。Reason 指令参数将在状态参数中返回，表示拒绝的是哪条连接。该状态参数是指返回到连接设备主机的连接完成事件的状态参数。

指令参数:

BD_ADDR 大小:6 字节

表 11.48

值	参数描述
0xXXXXXXXXXXXX	拒绝连接宿主设备的 BD_ADDR

Reason: 大小:1 字节

表 11.49

值	参数描述
0x0D – 0x0F	主机拒绝出错码.

返回值:无

在没有屏蔽的情况下生成的事件:

当主控制器接收到 Reject_Connection_Request 指令时，主控制器向主机发送指令状态事件，并发送连接完成事件到本地主机和要建立连接的主机。连接完成事件的状态参数,用于发送到主机设备以建立连接，包括 Reason 指令参数。

注：主控制器不是通过发出指令完成事件来表示指令完成，而是通过发送连接完成事件来表示。

4.5.10 Link_Key_Request_Reply

表 11.50

指令	OCF	指令参数	返回参数
HCI_Reject_Connection_Request	0x000B	BD_ADDR,Link_Key	状态, BD_ADDR

描述:

Link_Key_Request_Reply 指令用于应答从主控制器发送的链接关键字请求事件，并指定存储在主机的链接关键字。该关键字用于作为与由 BD_ADDR 指定其它蓝牙设备连接的链接关键字。

当主控制器按序列为本地链路管理器生成链接关键字请求事件，以应答从远程链路管理器发送来的请求时,(该链接关键字请求事件实质上也就是远程主机发送的 Create_Connection 或 Authentication 的结果集)本地主机必需在远程链路管理器侦测到 LMP 应答超时之前，利用 Link_Key_Request_Reply 或 Link_Key_Request_Negative_Reply 应答。

指令参数:

BD_ADDR 大小:6 字节

表 11.51

值	参数描述
0Xxxxxxxxxxxx	与链接关键字相关的设备的 BD_ADDR

Link_Key: 大小:16 字节

表 11.52

值	参数描述
0xXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXX	关联 BD_ADDR 的链接关键字

返回参数:

状态(Status) 大小:1 字节

表 11.53

值	参数描述

0x00	Link_Key_Request_Reply 指令成功
0x01 – 0xFF	Link_Key_Request_Reply 指令失败

BD_ADDR: 大小:6 字节

表 11.54

值	参数描述
0xXXXXXXXXXXXX	链接关键字请求应答完成的设备的 BD_ADDR

在没有屏蔽的情况下生成的事件:

Link_Key_Request_Reply 指令使指令完成事件生成。

4.5.11 Link_Key_Request_Negative_Reply

表 11.55

指令	OCF	指令参数	返回参数
HCI_Reject_Connection_Negative_Request	0x000C	BD_ADDR	状态, BD_ADDR

描述:

如果主机没有用于与由 BD_ADDR 指定的其它蓝牙设备连接的链接关键字, 就可以利用 Link_Key_Request_Negative_Reply 指令应答从主控制器发出的链接关键字请求事件。

当主控制器按序列为本地链路管理器生成链接关键字请求事件,以应答从远程链路管理器发送来的请求时,(该链接关键字请求事件实质上也就是远程主机发送的 Create_Connection 或 Authentication 的结果集)本地主机必需在远程链路管理器侦测到 LMP 应答超时之前, 利用 Link_Key_Request_Reply 或 Link_Key_Request_Negative_Reply 应答。

指令参数:

BD_ADDR: 大小:6 字节

表 11.56

值	参数描述
0xXXXXXXXXXXXX	链接关键字请求应答完成的设备的 BD_ADDR

返回参数:

状态: 大小:1 字节

表 1.57

值	参数描述
0x00	Link_Key_Request_Negative_Reply 指令成功
0x01 – 0xFF	Link_Key_Request_Negative_Reply 指令失败

BD_ADDR: 大小:6 字节

表 11.58

值	参数描述
0xXXXXXXXXXXXX	链接关键字请求应答完成的设备的 BD_ADDR

在没有屏蔽的情况下生成的事件:

Link_Key_Request_ Negative_Reply 指令使指令完成事件生成.

4.5.12 PIN_Code_Request_Reply

表 11.59

命令	OCF	命令参数	返回参数
Hci_PIN_Code_Request_Reply	0x000D	BD_ADDR, PIN_Code_Length, PIN_Code	Status, BD_ADDR

说明：

PIN_Code_Request_Reply 命令用来答复主控制器的代码申请事件及说明用于联机的 PIN 码。当远程初始化设备有配对申请时，将产生 PIN 码申请事件。当本地链接管理器响应远程链接管理器申请事件时，主控制器产生 PIN 码申请事件(作为远程主设备创建联机 Create_Connection 或鉴权申请 Authentication_Requested 命令结果)，在远程链接管理器检测 LMP 响应超时前，本地主设备必须响应 PIN_Code_Request_Reply 或 PIN_Code_Request_Negative_Reply 命令 。

命令参数：

BD_ADDR: 6 字节

表 11.60

值	参数说明
0xXXXXXXXXXX	设备的 BD_ADDR 值。

PIN_Code_Length: 1 字节

表 11.61

值	参数说明
0xXX	被使用的 bd_addr 代码长度,0x01-0x10

PIN_Code 16 字节

表 11.62

值	参数说明
0xXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	PIN 码用于联机。主设备应保证 PIN 码使用。 PIN 码最大可到 128 位。 PIN 码的 MSB 占据字节零。

返回参数 ：

Status: 1 字节

表 11.63

值	参数说明
0x00	PIN_Code_Request_Reply 命令成功。
0x01-0xFF	PIN_Code_Request_Reply 命令失败。

BD_ADDR: 6 字节

表 11.64

值	参数说明
0xXXXXXXXXXXXX	BD_ADDR 代码申请答复完成

事件产生(非屏蔽)：

PIN_Code_Request_Reply 命令将导致一个命令结束事件产生。

4.5.13 PIN_Code_Request_Negative_Reply

表 11.65

命令	OCF	命令参数	返回参数
Hci_PIN_Code_Request_Negative_Reply	0x000e	BD_ADDR	Status, BD_ADDR

说明：

当主控制器不能指定用于联机的PIN码时,PIN_Code_Request_Reply 命令用于响应来自主控制器 PIN 码申请事件。该命令将导致远程设备申请对失败。

当本地链接管理器响应远程链接管理器申请事件时，主控制器产生 PIN 码申请事件作为远程主设备创建联机（Create_Connection） 或鉴权申请(Authentication_Requested 命令结果)，在远程链接管理器检测 LMP 响应超时前,本地主设备必须响应 PIN_Code _Request _Reply 或 PIN_Code_Request_Negative_Reply 命令 。

命令参数：

BD_ADDR： 6 字节

表 11.66

值	参数说明
0xXXXXXXXXXXXX	该命令设备的 BD_ADDR 正在响应。

返回参数：

Status： 1 字节

表 11.67

值	参数说明
0x00	PIN_Code_Request_Negative_Reply 命令成功。
0x01-0xFF	PIN_Code_Request_Negative_Reply 命令失败。

BD_ADDR： 6 字节

表 1.68

值	参数说明
0xXXXXXXXXXXXX	消极应答 PIN 码设备的 BD_ADDR 完成。

事件产生(非屏蔽)：

PIN_Code_Request_Negative_Reply 命令将导致命令结束事件产生。

4.5.14 Change_Connection_Packet_Type

表 11.69

命令	OCF	命令参数	返回参数
HCI_Change_Connection_Packet_Type	0x000f	Connection_handle, Paket_type	

说明：

Change_Connection_Packet_Type 命令用于当前确立联机的分组类交换。为支持不同类型的用户数据，该命令允许当前联机动态修改。分组类命令参数指定用于联机的链接管理器的分组类。链接管理器只能使用由发送 HCI 数据分组 Packet_Type 命令参数指定的分组类。Packet_Type 命令参数值的解释将取决于在联机建立时，联机完成事件里的 Link _Type 命令参数返回。

多分组类可通过不同分组类按位 OR 操作的 Packet_Type 命令参数来指定。

注意：至少一种分组类型必须被确定。为保证链接管理器有效执行，主控制器应允许尽可能多地分组类。然而，主机不允许本地设备不支持的分组类。

命令参数：

Connect_Handle: 2 字节(12 位有意义)

表 11.70

值	参数说明
0xxxxx	联机句柄用于发射和接收声音或数据。从创建联机里返回。范围：0x0000-0x0EFF （ 0x0F00 – 0x0FFF 保留）

Packet_Type: 2 字节

ACL 链接类

表 11.71

值	参数说明
0x0001	保留
0x0002	保留
0x0004	保留
0x0008	DM1
0x0010	DH1
0x0020	保留
0x0040	保留
0x0080	保留
0x0100	保留
0x0200	保留
0x0400	DM3
0x0800	DH3
0x1000	保留
0x2000	保留

0x4000 0x800	dm5 DH5

SCO 链接类

表 11.72

值	参数说明
0x0001	保留
0x0002	保留
0x0004	保留
0x0008	保留
0x0010	保留
0x0020	HV1
0x0040	HV2
0x0080	HV3
0x0100	保留
0x0200	保留
0x0400	保留
0x0800	保留
0x1000	保留
0x2000	保留
0x4000	保留
0x8000	保留

返回参数： 无。

事件产生（非屏蔽）：

当主控制器收到变化联机分组类命令时，主控制器发送命令状态事件到主机。另外，当链接管理器确定因联机分组已发生变化时，本地设备的主控制器将发送联机分组类变化事件给主机。该过程仅在本地方面实现。

注意：无命令完成事件通过主控制器发送来指出该命令已完成，代替了联机分组类变化事件指出的该命令已完成。

4.5.15 Authentication_Requested

表 11.73

命令	OCF	命令参数	返回参数
HCI_Authentication_Requested	0X0011	Connection_Handle	

说明：

Authentication_Requested 命令用于期望鉴权指定联机句柄的远程设备。主机不发布使用与加密链接相符联机句柄的 Authentication_Request ed 命令。在鉴权失败时，主控制器或链接管理器将不能自动分离。如果操作适当，主机可靠发布断开命令以终止链接。

注意：联机句柄命令参数用来识别联机形式的其它蓝牙设备，联机句柄是 ACL 联机方式的联机句柄。

命令参数：

Connecioc_Handle: 2 字节(12 位有意义)

表 11.74

值	参数说明
0Xxxxx	用来设置鉴权的联机句柄，对于所有用相同蓝牙设备端点联机句柄的联机句柄。 范围: 0x0000-0x0EFF (0x0F00 - 0x0FFF 保留)

返回参数：无。

事件产生(非屏蔽)：

当主控制器收到 Authentication_Requested 命令时，它发送命令状态事件到主机。当联机的鉴权完成时，鉴权完成事件出现而且指出该命令已完成。

注意：通过主控制器传送的无命令完成事件指出该命令已完成，代替了鉴权完成事件指出的该命令已完成。

注意：当本地或远程主控制器没有链接字作为指定的 Cnnecton_Hand le 时，在本地主机最后收到鉴权完成事件前，它将申请来自于主机的链接字。

4.5.16 Set_Connecion_Encryption

表 11.75

命令	OCF	命令参数	返回参数
HCI_Set_Connectio n_Encryption	0x0013	Connection_Handle Encryption_Enable	

说明：

Set_Connection_Encryption 命令用于允许和禁止链接层加密。

注意：联机句柄命令参数用来识别联机形式的其它蓝牙设备。联机句柄应是 ACL 联机句柄。当加密正在被改变时，由于联机句柄与远程设备有关，所以整个 ACL 通信必须关闭。

命令参数：

Connection_Handle: 2 字节(12 位有意义)

表 11.76

值	参数说明
0Xxxxx	使用相同蓝牙设备终点当作指定联机句柄的全部联机句柄用于允许和禁止链接层加密。 范围: 0x0000-0x0EFF (0x0F00 - 0x0FFF 保留)

Encryption_Enable: 1 字节

表 11.77

值	参数说明
0x00	关闭链接层加密。
0x01	打开链接层加密。

返回参数：无。

事件产生 (非屏蔽)：

当主控制器收到 Set_Connection_Encryption 命令时，主控制器发送命令状态事件到主机。当链接管理器为链接完成了允许 / 禁止加密时，本地蓝牙设备上的主控制器将发送加

密变化事件到主机，而且远程设备上的主控制器也产生加密变化事件。

注意：通过主控制器传送的无命令完成事件指出该命令已完成，代替了加密变化事件指出的该命令已完成。

4. 5。17 Change_Connection_Link_Key

表 11.78

命令	OCF	命令参数	返回参数
HCI_Change_Connection_Link_Key	0x0015	Connection_Handle	

说明：

Change_Connection_Link_Key 命令强制使用联机句柄的双方产生新的链接字，链接字用作联机的加密和鉴权。

注意：Connection_handle 命令参数用来识别联机形式的其它蓝牙设备。联机句柄是 ACL 联机形式的联机句柄。如果允许联机加密和使用当前临时链接字，则蓝牙主单元设备将自动重新加密。

命令参数：

Connection_Handle: 2 字节(12 位有意义)

表 11.79

值	参数说明
0Xxxxx	用来识别联机的联机句柄。 范围: 0x0000-0x0EFF （ 0x0F00 - 0x0FFF 保留）

返回参数： 无。

事件产生(非屏蔽)：

当主机控制器收到 Change_Connection_Link_Key 命令时，主机控制器发送命令状态事件到主机。当链接管理器为联机改变了链接字时，本地蓝牙设备上的主控制器将发送链接字标志信息事件和改变联机链接字完成事件到主机，且远程设备上的主控制器也产生链接字标志信息事件。链接字标志信息事件指出新链接字对于联机是有效的。

注意：通过主控制器传送的无命令完成事件指出该命令已完成，代替了改变联机链接字完成事件指出的该命令已完成。

4.5.18 Master_Link_Key

表 11.80

命令	OCF	命令参数	返回参数
HCI_MASTER_LINK_KEY	0x0017	KEY_FLAG	

说明：

Master_Link_Key 命令强迫匹克网中主单元使用主单元设备的临时链接字或半永久链接字。该临时链接字用在匹克网内广播消息的加密，而半永久链接字用于点对点通讯单独加密。 Key_Flag 命令参数用来指出使用那个链接字(主单元临时链接字，或半永久链接字)。

命令参数：

Key_Flag： 1 字节

表 11.81

值	参数说明
0x00	使用半永久链接字。
0x01	使用临时链接键。

返回参数：无。

事件产生(非屏蔽)：

当主控制器收到 Master_Link_Key 命令时，主控制器发送命令状态事件到主机。当链接管理器改变链接字时，在本地和远程设备上的主控制器发送主单元链接字完成事件到主机。主单元方的链接句句柄是现有的联机从单元之一的联机句柄。从单元方的联机句柄是初始化主单元联机句柄。主单元链接字完成事件包含该命令的状态。

注意：通过主控制器传送的无命令完成事件指出该命令已完成，代替了主单元链接字完成事件指出的该命令已完成。

4.5.19 Remote_Name_Request

表 11.82

命令	OCF	命令参数	返回参数
HCI_Remote_Name_Request	0X0019	BD_ADDR Page_Scan_Repetition_Mode Page_Scan_Mode Clock_Offset	

说明：

Remote_Name_Request 命令用来获得其它蓝牙设备用户界面友好名。用户界面友好名用来区分另外一台蓝牙设备。BD_ADDR 命令参数用来识别用户界面友好名获得的设备。

Page_Scan_Repetition_Mode 和 Page_Scan_Mode 命令参数，指出由使用 BD_ADDR 的远程设备支持的呼叫扫描模式，该信息在查询过程期间获得。Clock_Offset 参数在本地时钟和用 BD_ADDR 远程设备的时钟之间有差异，不同的 16 位仅有 2 位使用且它们分别作为 0 到 14 位映射到该参数。Clock_Offset_Valid_Flag 定义在 Clock_Offset 命令参数的 15 位，用来指出时钟补偿是否有效。

注意：如果在本地设备和相应 BD_ADDR 的设备之间无联机存在，临时链接层联机将确立获得远程设备名。

命令参数：

BD_ADDR： 6 字节

表 11.83

值	参数说明
0xXXXXXXXXXXXX	命名设备的 BD_ADDR

Page_Scan_Repetition_Mode： 1 字节

表 11.84

值	参数说明
0x00	R0
0x01	R1
0x02	R2
0x03-oxFF	保留

Page_Scan_Mode： 1 字节

表 11.85

值	参数说明
0x00	强制呼叫扫描模式。
0x01	可选呼叫扫描模式 I。
0x02	可选呼叫扫描模式 II.
0x03	可选呼叫扫描模式 III.
0x04-0xFF	保留

Clock_Offset： 2 字节

表 11.86

值	参数说明
位 14.0	clkslave-clkmaster 的 16.2 位
位 15	Clock_Offset_Valid_Flag 无效时钟补偿 Offfset = 0 有效时钟补偿 Offfset = 1

返回参数：无。

事件产生(非屏蔽)：

当主控制器收到 Remote_Name_Request 命令时，主控制器发送命令状态事件到主机。当链接管理器已完成 LMP 消息获得远程名时，本地蓝牙设备上的主控制器将发送远程名申请完成事件到主机。

注意：通过主控制器传送的无命令完成事件指出该命令已完成，代替了远程名申请事件指出的该命令已完成。

4.5.20 Read_Remote_Supported_Features

表 11.87

命令	OCF	命令参数	返回参数
HCI_Read_Remote_Supported_Features	0x001B	Connection_Handle	

说明：

该命令申请通过联机句柄参数识别远程设备支持特征的一张表。联机句柄必须是 ACL 联机方式联机句柄。阅读远程支持特征完成事件将返回 LMP 特征的表。

命令参数：

2 字节(12 位有意义)

表 11.88

值	参数说明
0xXXXX	指出得到哪个联机句柄的 LMP 支持特征表。 范围：0x0000-0x0EFF （ 0x0F00 - 0x0FFF 保留）

返回参数：无。

事件产生（非屏蔽）：

当主控制器收到 Read_Remote_Supported_Features 命令时，主控制器发送命令状态事件到主机。当链接管理器已完成 LMP 消息并确立远程特征时，本地蓝牙设备上的主控制器将发送读远程支持特征完成的事件到主机。读远程支持特征完成事件包含该命令的状态，而且参数描述远程设备的支持特征。

注意：通过主控制器传送的无命令完成事件指出该命令已完成，代替了读远程支持特征完成事件指出的该命令已完成。

4.5.21 Read_Remote_Version_Information

表 11.89

命令	OCF	命令参数	返回参数
HCI_Read_Remote_Version_Information	0x001D	联机句柄	

说明：

该命令通过连接句柄参数识别远程蓝牙设备版本信息的获取值。联机句柄必须是 ACL 联机方式联机句柄。

命令参数：

Connection_Handle 2 字节(12 位有意义)

表 11.90

值	参数说明
0xXXXX	指出获得哪个联机句柄的版本信息。 范围：0x0000-0x0EFF （ 0x0F00 - 0x0FFF 保留）

返回参数：无。

事件产生(非屏蔽)：

当主控制器收到 Read_Remote_Version_Information 命令时，主控制器发送命令状态事件到主机。当链接管理器完成 LMP 确定远程版本信息时，本地蓝牙设备上的主控制器将发送读远程版本信息完成事件到主机。读远程版本信息完成事件包含了该命令的状态，而且参数描述了通过远程设备使用 LMP 的版本及损坏。

注意：通过主控制器传送的无命令完成事件指出该命令已完成，代替了读远程版本信息完成事件指出的该命令已完成。

4.5.22 Read_Clock_Offset

表 11.91

命令	OCF	命令参数	返回参数
HCI_Read_Clock_Offset	0x001F	联机句柄	

说明：

使用系统时钟和远程设备的时钟补偿来确定用于呼叫扫描的远程设备采用的跳频频率。该命令允许主机读远程设备的时钟补偿。联机句柄必须是 ACL 联机方式的联机句柄。该命令易于从一台蓝牙设备到另外一台蓝牙设备链接。

命令参数：

Connection_Handle: 2 字节(12 位有意义)

表 11.92

值	参数说明
0xXXXX	指出返回哪个链接时钟补偿参数 范围: 0x0000-0x0EFF (0x0F00 - 0x0FFF 保留)

返回参数：无。

事件产生(非屏蔽)：

当主控制器收到 Read_Clock_Offset 命令时，主控制器发送命令状态事件到主机。如果该命令在主单元和链接管理器已完成获得时钟补偿信息的 LMP 消息时被申请，本地蓝牙设备上的主控制器发送读时钟补偿完成事件到主机。

注意：通过主控制器传送的无命令完成事件指出该命令已完成，代替了只读时钟补偿完成事件指出的该命令已完成。如果命令在从单元方申请，且没有 LMP PDU 的互换， LM 将直接发送命令状态事件和读时钟补偿事件到主机。

4．6 链接策略命令

链接策略命令提供了主控制器如何影响匹克网链接管理器消息的方式。当链接策略命令使用时，LM 控制蓝牙匹克网和散射网怎样建立和维持，取决于可调的策略参数。

这些策略命令修改了链接管理器的状态，而且能导致用蓝牙远程设备链接层联机的变化。

注意：在两个蓝牙设备之间，仅有一种 ACL 联机方式存在，因此对各个物理链接层联机来说，仅存在着唯一的 ACL HCI 联机句柄。蓝牙主控制器提供策略调整机制来支持多种策略。此能力允许用一种蓝牙模型来支持多种不同模型，和同一蓝牙模型能在多种不同类蓝牙设备里被合为一体。链接策略命令， OGF 定义为 0x02

表 11.93

命 令	命令说明汇总
Hold_Mode	该命令用来改变 LM 状态和本地及远程设备为主模式的 LM 位置。
Sniff_Mode	该命令用来改变 LM 状态和本地及远程设备为呼吸模式的 LM 位置。
Exit_Sniff_Mode	该命令用来结束联机句柄在当前呼吸模式里的呼吸模式。
Park_Mode	该命令用来改变 LM 状态和本地及远程设备为休眠模式的 LM 位置。

Exit_Park_Mode	该命令用来切换从休眠模式返回到活动模式的蓝牙设备。
QoS_Setup	该命令用来指出联机句柄的服务参数质量。
Role_Discovery	该命令用于蓝牙设备确定设备正在履行特殊联机句柄的角色。
Switch_Role	该命令用于蓝牙设备切换当前正在履行指定蓝牙设备特殊联机的设备角色。
Read_Link _Policy_Seting	该命令为指定联机句柄读链接策略设置。链接策略设置允许主控制器指定可用于指定联机句柄的 LM 链接模式。
Write_Link _Policy_Seting	该命令为指定联机句柄写链接策略设置。链接策略设置允许主控制器指定可用于指定联机句柄的 LM 链接模式。

4.6.1 Hold_Mode

表 11.94

命令	OCF	命令参数	返回参数
HCI_Hold_mode	0x0001	Connection_handle Hold_mode_maxinterval Hold_mode_min_interval	

说明：

Hold_Mode 命令用来改变链接管理器的状态，并通过指定联机句柄为保持模式相关的 ACL 基带联机位置。 Hold_Mode_Max_Interval 和 Hold_Mode_Min_Interval 命令参数确定主控制器想置联机为保持模式的时间长度。本地和远程设备协调在保持模式里的长度。

Hold_Mode_Max_Interval 参数用来指出主控制器在协调远程设备后实际进入保持模式的保持间隔最大长度。保持间隔定义为保持模式开始和保持模式完成之间的时间量。

Hold_ Mode_Min_Interval 参数被用来指出主控制器在协调远程设备后实际进入保持模式的保持间隔最小长度。因此 Hold_Mode_Min_Interval 不能大于 Hold_Mode_Max_ _Interval。如果命令是成功的，主控制器将在模式变化事件的间隔参数里返回实际的保持间隔。该命令使主控制器能够为自己或若干其它的蓝牙设备提供低功耗策略，而且允许设备进入查询扫描和许多其它的可能行为。

注意：联机句柄不能是 SCO 链接类型。

命令参数：

Connection_handle: 2 字节(12 位有意义)

表 11.95

值	参数说明
0xXXXX	用来识别联机的联机句柄。 范围: 0x0000-0x0EFF （ 0x0F00 - 0x0FFF 保留）

Hold_Mode_Max_Interval: 2 字节

表 11.96

值	参数说明
N = 0xXXXX	在保持模式基带时隙的最大可接收量。 保持时间长度＝N＊0.625ms（单基带时隙） N的范围: 0x0001-0xFFFF

	时间：0.625ms – 40.9 秒

Hold_Mode_Min_Interval： 2 字节

表 11.97

值	参数说明
N = 0xXXXX	在保持模式基带时隙最小可接收量。 保持时间长度＝N＊0.625ms（单基带时隙） N的范围：0x0001-0xFFFF 时间：0.625ms – 40.9 秒

返回参数： 无。

事件产生（非屏蔽）：

当收到了 Hold_Mode 命令时，主控制器发送命令状态事件到主机。当保持模式开始时，模式变化事件将发生。而且保持模式为指定联机句柄完成时，模式变化事件甚至将再次发生。如果事件是远程蓝牙设备，则保持模式的模式变化时间信号结束是确定保持模式的终止。

注意：通过主控制器传送的无命令完成事件指出该命令已完成，代替了模式变化事件指出的该命令已完成。如果错误出现在命令状态事件发生后，那么在模式变化事件里的状态将指出其错误。

4.6.2 Sniff_Mode

表 11.98

命令	OCF	命令参数	返回参数
HCI_Sniff_Mode	0x0003	Connection_handle Sniff_Max_Interval , Sniff_Min_Interval , Sniff_Attempt Sniff_Timeout	

说明：

呼吸模式命令用来改变链接管理器的状态，并通过指定联机句柄为呼吸模式相关的 ACL 基带联机位置。联机句柄命令参数用来识别 ACL 链接联机在呼吸模式里的位置。

Sniff_Max_Interval 和 Sniff_Min_Interval 命令参数用于指出在呼吸模式里申请可接受的最大和最小区间。Sniff_Min_Interval 不能大于 Sniff_Max_Interval。呼吸间隔定义了在各连续呼吸间隔之间的时间量。如果命令是成功的，主控制器应在模式改变事件的间隔参数里返回实际呼吸间隔。通过 Sniff_Attempt 命令参数作为区间指定，从单元在每个实际呼吸间隔的结束处监听。只要从单元接收分组，它将继续监听经 Sniff_Timeout 指出的附加期分组。该命令允许主控制器支持自己或几个其它的蓝牙设备的低功耗策略，而且允许设备进入查询扫描，呼叫扫描和一些其它的可能行为。

注意：另外，联机句柄不能是 SCO 链接类型之一。

命令参数：

Connection_Handle: 2 字节(12 位有意义)

表 11.99

值	参数说明
0xXXXX	用来识别联机的联机句柄。 范围：0x0000-0x0EFF （ 0x0F00 - 0x0FFF 保留）

Sniff_Max_Interval： 2 字节

表 11.100

值	参数说明
N = 0xXXXX	在各呼吸区间之间，基带时隙的最大可接受值。 长度=N * 0.625ms（单基带时隙） N 的范围：0x0001-0xFFFF 时间:0.625ms-40.9s

Sniff_Min_Interval： 2 字节

表 11.101

值	参数说明
N = 0xXXXX	在各呼吸区间之间，基带时隙的最大可接受值。 长度=N * 0.625ms（单基带时隙） N 的范围：0x0001-0xFFFF 时间:0.625ms-40.9s

Sniff_Attempt: 2 字节

表 11.102

值	参数说明
N = 0xXXXX	作为呼吸期望的基带时隙数。 长度=N * 0.625ms（单基带时隙） N 的范围：0x0001-0xFFFF 时间:0.625ms-40.9s

Sniff_Timeout: 2 字节

表 11.103

值	参数说明
N = 0xXXXX	作为呼吸超时的基带时隙数。 长度=n*0.625ms（单基带时隙） N 的范围：0x0001-0xFFFF 时间:0.625ms-40.9s

返回参数:无。

事件产生(非屏蔽)：

当收到 Sniff_Mode 命令时，主控制器发送命令状态事件到主机。对于指定的联机句柄当呼吸模式开始时，将出现模式改变事件。

注意：通过主控制器传送的无命令完成事件指出该命令已完成，代替了模式变化事件指出的该命令已完成。如果错误出现在命令状态事件发生后，那么在模式变化事件里的状态将指出其错误。

4.6.3 Exit_Sniff_Mode

表 11.104

命令	OCF	命令参数	返回参数
HCI_Exit_Sniff_Mode	0x0004	Connection_ Handle	

说明：

Exit_Sniff_Mode 命令用于作为联机句柄的呼吸模式的结束处。链接管理器决定和发布适当的 LMP 命令给与联机句柄有关的远程呼吸模式。

注意：另外，联机句柄不能是 SCO 链接类型之一。

命令参数：

Connection_handle: 2 字节(12 位有意义)

表 11.105

值	参数说明
0xXXXX	用来识别联机的联机句柄。 范围: 0x0000-0x0EFF (0x0F00 - 0x0FFF 保留)

返回参数：无。

事件产生(非屏蔽)：

当主控制器已收到 Exit_Sniff_Mode 命令时，该命令的命令状态事件将出现。对于指定的联机句柄当呼吸模式已结束时，模式改变事件出现。

注意：通过主控制器传送的无命令完成事件指出该命令已完成，代替了模式变化事件指出的该命令已完成。

4.6.4 Park_Mode

表 11.106

命令	OCF	命令参数	返回参数
HCI_Park_Mode	0x0005	Connection_Handle Beacon_Max_Interval Beacon_Min_Interval	

说明：

休眠模式命令用来改变链接管理器的状态，并通过指定联机句柄为休眠模式相关的 ACL 基带联机位置。联机句柄命令参数用来识别 ACL 链接联机在休眠模式里的位置。联机句柄必须是 ACL 联机方式的联机句柄。信标间隔命令参数指出信标间可接受的间隔最长度。然而，远程设备可申请较短的间隔。 Beacon_Max_Interval 参数指出信标之间的间隔可接受的最长长度。 Beacon_Min_Interval 参数指出信标之间的间隔可接受的最短的长度。最小信标间隔不能大于最大信标间隔。如果命令成功，主控制器将在模式变化事件中的间隔参数里返回一个实际的信标间隔。该命令允许支持主控制器自身或若干其它的蓝牙设备低功耗策略，允许设备进入查询扫描，呼叫扫描，在单个匹克网里提供支持大量的蓝牙设备和多种可行的活动。

命令参数：

Connection: 2 字节(12 位有意义)

表 11.107

值	参数说明
0xXXXX	用来识别联机的联机句柄。 范围: 0x0000-0x0EFF (0x0F00 - 0x0FFF 保留)

Beacon_Max_Interval: 2 字节

表 11.108

值	参数说明

N = 0xXXXX	在连续信标之间基带时隙最大可接受数。 间隔长度 = N * 0.625ms（单基带时隙） N 的范围：0x0001-0xFFFF 时间区域：0.625ms-40.9s

Beacon_Max_Interval： 2 字节

表 11.109

值	参数说明
N = 0xXXXX	在连续信标之间基带时隙最小可接受数。 间隔长度= N * 0.625ms（单基带时隙） N 的范围：0x0001-0xFFFF 时间区域：0.625ms-40.9s

返回参数：无。

事件产生（非屏蔽）：

当收到 Park_Mode 命令时，主控制器发送命令状态事件宿主机。对于指定的联机句柄，当休眠模式开始时，模式变化事件发生。

注意：通过主控制器传送的无命令完成事件指出该命令已完成，代替了模式变化事件指出的该命令已完成。 如果错误出现在命令状态事件发生后，那么在模式变化事件里的状态将指出其错误。

4.6.5 Exit_Park_Mode

表 11.110

命令	OCF	命令参数	返回参数
HCI_Exit_Park_Mode	0x0006	联机句柄	

说明：

Exit_Park_Mode 命令用于蓝牙设备从休眠模式切换到活动模式。当设备与在休眠模式里指定联机句柄相关时，该命令才可以发出。联机句柄必须是 ACL 链接方式的联机句柄。该函数不能直接地完成。

命令参数：

Connection_Handle: 2 字节(12 位有意义)

表 11.111

值	参数说明
0xXXXX	用来识别联机的联机句柄。 范围：0x0000-0x0EFF （ 0x0F00 - 0x0FFF 保留）

返回参数：无。

事件产生（非屏蔽）：

当主控制器收到 Exit_Park_Mode 命令时，该命令的状态事件发生。对于指定的联机句柄，当休眠模式结束时，模式变化事件发生。

注意：通过主控制器传送的无命令完成事件指出该命令已完成，代替了模式变化事件指出的该命令已完成。

4.6.6 QoS_Setup

表 11.112

命令	OCF	命令参数	返回参数
HCI_QoS_Setup	0x0007	Connection_Handle, Flag, Service_Type, Token_Rate, Peak_Bandwidth , Latency, Delay_Variation	

说明：

QoS_Setup 命令用于指出联机句柄的服务参数的质量。联机句柄必须是 ACL 联机方式的联机句柄。这些 QoS 参数与 L2CAPQoS 参数一样。它允许链接管理器具有宿主机正在申请各个联机的所有信息。LM 将决定是否能遇见 QoS 参数。主单元和从单元双方的蓝牙设备都能使用该命令。当设备是从单元时，该命令将激发 LMP，要求主单元提供一个经 LM 确定的指定 QoS 从单元。当设备是主单元时，该命令用来申请接受指定 QoS 从设备，该指定 QoS 通过主单元的 LM 确定。联机句柄命令参数用来识别哪个 QoS 申请联机。

命令参数：

Connection_handle: 2 个字节(12 位有意义)

表 11.113

值	参数说明
0xXXXX	用来识别 QoS 建立联机的联机句柄。 范围：0x0000-0x0EFF （ 0x0F00 - 0x0FFF 保留）

Flags: 1 字节

表 11.114

值	参数说明
0x00-0xFF	保留

Service_Type: 1 字节

表 11.115

值	参数说明
0x00	无传播
0x01	最大能力
0x02	保证
0x03-0xFF	保留

Token_Rate： 4 字节

表 11.116

值	参数说明
0xXXXXXXXX	每秒字节令牌率。

Peak_Bandwidth： 4 字节

表 11.117

值	参数说明

0xXXXXXXXX	每秒字节带宽峰值。

Latency: 4 字节

表 11.118

值	参数说明
0xXXXXXXXX	微秒等待时间。

Delay_Variation: 4 字节

表 11.119

值	参数说明
0xXXXXXXXX	微秒延期变化。

返回参数：无。

事件产生(非屏蔽)：

当主控制器收到 QoS_Setup 命令时，主控制器发送命令状态事件到宿主机。当链接管理器完成确立申请 QoS 参数的 LMP 消息时，本地蓝牙设备的主控制器将发送 QoS 建立完成事件到主机，如果有 LMP 消极应答，事件可以也在远程方产生。然而 QoS 建立完成事件的参数值不同与初始化和远程方。QoS 建立完成事件通过在包含该命令状态的本地主控制器上返回，而且返回的 QoS 参数描述了对于联机 QoS 的支持。

注意：通过主控制器传送的无命令完成事件指出该命令已完成，代替了 QoS 建立完成事件指出的该命令已完成。

4.6.7 Role_Discovery

表 11.120

命令	OCF	命令参数	返回参数
HCI_Role_ Discovery	0x0009	Connection _Handle	Status, Connection_handle, Current_Role

说明：

Role_Discovery 命令用于确定蓝牙设备，该蓝牙设备的任务正在完成特殊联机句柄。该联机句柄必须是 ACL 联机方式的联机句柄。联机句柄必须是为一个 ACL 链接的一联机句柄。

命令参数：

Connection_handle: 2 字节(12 位有意义)

表 11.121

值	参数说明
0xXXXX	用来识别联机的联机句柄。 范围：0x0000-0x0EFF （ 0x0F00 - 0x0FFF 保留）

返回参数：

Status: 1 字节

表 11.122

值	参数说明
0x00	Role_Discovery 命令成功。
0x01-0xFF	Role_Discovery 命令失败。

Connection_Handle: 2 字节(12 位有意义)

表 11.123

值	参数说明
0Xxxxx	用来识别联机的联机句柄。 Role_Discovery 命令被发出。 范围: 0x0000-0x0EFF (0x0F00 - 0x0FFF 保留)

Current_Role: 1 字节

表 11.124

值	参数说明
0x00	对于该联机句柄来说当前角色是主单元。
0x01	对于该联机句柄来说当前角色是从单元。

事件产生(非屏蔽):

当 Role_Discovery 命令完成时，命令完成事件产生。

4.6.8 Switch Role

表 11.125

命令	OCF	命令参数	返回参数
HCI_Switch_Role	0x000B	BD_ADDR, Role	

说明:

Switch_Role 命令用于切换当前设备角色的蓝牙设备，该设备正在完成与另外指定的蓝牙设备特殊联机。 BD_ADDR 命令参数指出哪种联机角色切换完成。角色指出本地设备完成的新角色申请。

注意: BD_ADDR 命令参数必须指出已存在联机的蓝牙设备。

命令参数:

BD_ADDR: 6 字节

表 11.126

值	参数说明
0xXXXXXXXXXXXX	完成角色切换的链接设备的 BD_ADDR。

Role: 1 字节

表 11.127

值	参数说明
0x00	对于该 BD_ADDR 改变自身角色为主单元。
0x01	对于该 BD_ADDR 改变自身角色为从单元。

返回参数：无。

事件产生(非屏蔽)：

当主控制器收到 Switch_Role 命令时，该命令的命令状态事件发生。当角色切换完成时，角色交换事件出现并指出角色已改变，而且双方主机将进行通信。

注意：通过主控制器传送的无命令完成事件指出该命令已完成，代替了角色改变事件指出的该命令已完成。

4.6.9 Read_Link_Policy_Settings

表 11.128

命令	OCF	命令参数	返回参数
HCI_Read_Link_Policy_Settings	0x000C	Connection_Handle	Status, Connection_Handle, Link_Policy_Settings

说明：

该命令对于指定的联机句柄读链接策略设置。当链接管理器或从远程设备接收申请，或确定自身主一从角色改变或进入保持、呼吸、休眠模式时，Link_Policy_Settings 参数确定了本地链接管理器的行为。本地链接管理器可自动地接收或拒绝远程设备申请，甚至可以自动申请自己，取决于相应联机句柄的 Link_Policy_Settings 参数值。

当对于确定的联机句柄的 Link_Policy_Settings 参数值改变时，该命令完成后，新值仅用于远程设备或本地链接管理器自身提出的申请。联机句柄必须是 ACL 联机方式的联机句柄。通过分别启动各个模式，主控制器能选择任何组合需要支持各种操作模式。

对于 Link_Policy_Settings 参数，通过不同活动类型的按位“OR”操作，可指定多重 LM 策略。

命令参数：

connection_handle: 2 字节(12 位有意义)

表 11.129

值	参数说明
0xXXXX	用来识别联机的联机句柄。 范围：0x0000-0x0EFF （ 0x0F00 - 0x0FFF 保留）

返回参数：

Status: 1 字节

表 11.130

值	参数说明
0x00	Read_Link_Policy_Settings 命令成功。
0x01_0xFF	Read_Link_Policy_Settings 命令失败。

Connection_Handle: 2 字节(12 位有意义)

表 11.131

值	参数说明
0xXXXX	用来识别联机的联机句柄。 范围：0x0000-0x0EFF （ 0x0F00 - 0x0FFF 保留）

Link_Policy_Settings: 2 字节

表 11.132

值	参数说明
0x0000	禁止所有 LM 模式。
0x0001	启动主从切换。
0x0002	启动保持模式。
0x0004	启动呼吸模式。
0x0008	启动休眠模式。
0x0010-0x8000	保留

事件产生(非屏蔽):

当 Read_Link_Policy_Settings 命令完成时，命令完成事件产生。

4.6.10 write_link_policy_setting

表 11.133

命令	OCF	命令参数	返回参数
HCI_Write_Link_Policy_Settings	0x000D	Connect_Handle, Link_Policy_Settings	Status, Connection_Fandle,

说明:

该命令将为指定的联机句柄写链接策略设置。当链接管理器或从远程设备接收申请，或确定自身主一从角色改变或进入保持、呼吸、休眠模式时，Link_Policy_Settings 参数确定了本地链接管理器的行为。本地链接管理器可自动地接收或拒绝远程设备申请，甚至可以自动申请自己，取决于相应联机句柄的 Link_Policy_Settings 参数值。

当对于确定的联机句柄的 Link_Policy_Settings 参数值改变时，该命令完成后，新值仅用于远程设备或本地链接管理器自身提出的申请。联机句柄必须是 ACL 链接方式的联机句柄。通过分别启动各个模式，主控制器能选择任何组合需要支持各种操作模式。

对于 Link_Policy_Settings 参数，通过不同活动类型的按位“OR”操作，可指定多重 LM 策略。

命令参数:

Connection_Handle: 2 字节(12 位有意义)

表 11.134

值	参数说明
0xXXXX	用来识别联机的联机句柄。 范围: 0x0000-0x0EFF (0x0F00 - 0x0FFF 保留)

Link_Policy_Settings: 2 字节

表 11.135

值	参数说明
0x0000	禁止所有 LM 模式。
0x0001	启动主从切换。
0x0002	启动保持模式。

0x0004	启动呼吸模式。
0x0008	启动休眠模式
0x0010-0x8000	保留

返回参数：

Status: 1 字节

表 11.136

值	参数说明
0x00	Write_Link_Policy_Settings 命令成功。
0x01-0xFF	Write_Link_Policy_Settings 命令失败。

Connection: 2 字节(12 位有意义)

表 11.137

值	参数说明
0xXXXX	用来识别联机的联机句柄。 范围：0x0000-0x0EFF （ 0x0F00 - 0x0FFF 保留）

事件产生(非屏蔽)：

当 Write_Link_Policy_Settings 命令完成时，命令完成事件产生。

4．7 主控制器与基带命令

主控制器与基带命令提供识别和控制各种蓝牙硬件的能力。这些参数提供蓝牙设备的控制和主控制器、链接管理器及基带的能力。主机可利用这些命令修改本地设备的行为。对于 HCI 控制和基带命令，PGF 定义为 0x03。

表 11.138

命令	命令说明汇总
Set_Even_mask	控制主机经 HCI 产生的事件。
Reset	复位蓝牙主控制器、链接管理器和无线设备。
Sel_event_Filter	经主机指定不同事件过滤器。对于不同类型或同类型的过滤器，主机可多次发送该命令申请多种条件。
Flush	对于指定的联机句柄，放弃所有作为当前待传输数据，甚至当前是属于多个在主控制器里的 L2CAP 分组的数据块。
Read_Pin_Type	主机读出由指定主机支持的可变 PIN 还是固定 PIN 值。
Write_Pin_Type	主机写入由指定主机支持的可变 PIN 还是固定 PIN 值。
Creat_New_Unit_Key	创建新单元字。
Read_Store_Link_Key	提供读出存放在蓝牙主控制器里的单个或多个链接字的能力。
Write_Store_Link_Key	提供写入存放在蓝牙主控制器里的单个或多个链接字的能力。
Delete_Store_Link_Key	提供删除存放在蓝牙主控制器里的单个或多个链接字的能力。

Change_Local_Name	提供修改蓝牙设备的用户友好名的能力。
Read_Local_Name	提供读存储的蓝牙设备用户友好名的能力。
Read_Connection_Accept_Timeout	读联机识别超时结构参数值，在指定区域出现后，该命令允许蓝牙硬件自动拒绝联机申请和拒绝新的联机。
Write_Connection_Accept_Timeout	写联机识别超时结构参数值，在指定区域出现后，该命令允许蓝牙硬件自动拒绝联机申请和拒绝新的联机。
Read_Page_Timeout	读呼叫响应超时结构参数，在本地设备返回联机失败前，该值是允许蓝牙硬件定义等待远程设备联机申请的时间量。
Write_Page_Timeout	写呼叫响应超时结构参数，在本地设备返回联机失败前，该值是允许蓝牙硬件定义等待远程设备联机申请的时间量。
Read_Scan_Enable	读出扫描允许结构参数值，该值的控制不管蓝牙设备是处于呼叫期望的周期性扫描或是其它蓝牙设备的查询申请。
Write_Scan_Enable	写入扫描允许结构参数值，该值的控制不管蓝牙设备是处于呼叫期望的周期性扫描或是其它蓝牙设备的查询申请。
Read_Page_Scan_Activity	读出呼叫扫描间隔和呼叫扫描区间结构参数。呼叫扫描间隔定义为在连续呼叫扫描之间的时间量。呼叫扫描区间定义为在呼叫扫描的期间。
Write_Page_Scan_Activity	写入呼叫扫描间隔和呼叫扫描区间结构参数。呼叫扫描间隔定义为在连续呼叫扫描之间的时间量。呼叫扫描区间定义为在呼叫扫描的期间。
Read_Inquiry_Scan_Activity	读出查询扫描间隔和查询扫描区间的结构参数。查询扫描间隔定义为在连续查询扫描之间的时间量。查询扫描区间定义为在查询扫描的期间。
Write_Inquiry_Scan_Activity	写入查询扫描间隔和查询扫描区间的结构参数。查询扫描间隔定义为在连续查询扫描之间的时间量。查询扫描区间定义为在查询扫描的期间。
Read_Authentication_Enable	读出鉴权允许参数值。该值控制蓝牙设备使用其它蓝牙设备各种联机的鉴权申请。
Write_Authentication_Enable	写入鉴权允许参数值。该值控制蓝牙设备使用其它蓝牙设备各种联机的鉴权申请。
Read_Encryption_Mode	读出加密模型参数值。该值控制蓝牙设备使用其它蓝牙设备各种联机的加密申请。
Write_Encryption_Mode	写入加密模型参数值。该值控制蓝牙设备使用其它蓝牙设备各种联机的加密申请。
Read_Class_Of_Device	读出设备类参数值。用来指出别的设备能力。
Write_Class_Of_Device	写入设备类参数值。用来指出别的设备能力。
Read_Voice_Setting	读出话音设置参数值。控制所有话音联机的各种设置。
Write_Voice_Setting	写入话音设置参数值。控制所有话音联机的各种设置。
Read_Automatic_Flush_Timeout	对指定的联机句柄，读出刷新超时参数值。
Write_Automatic_Flush_Timeout	对指定的联机句柄，写入刷新超时参数值。
Read_Num_Broadcast_Retransmissions	读出设备的广播重发次数值。广播分组不需确认而且不可靠。该参数通过多次重传广播消息来提高广播消息的可靠性。
Write_Num_Broadcast_Retransmissions	写入设备的广播重发次数值。广播分组不需确认而且不可靠。该参数通过多次重传广播消息来提高广播消息的可靠性。

Read_Hold_Mode_Activity	读出主控模型活动参数值。当设备为主控模型时，该值用来确定设备的活动做什么。
Write_Hold_Mode_Activity	写入主控模型活动参数值。当设备为主控模型时，该值用来确定设备的活动做什么。
Read_Transmit_Power_Level	对于指定的联机句柄，读出传输功率电平参数值。
Read_SCO_Flow_Control_Enable	读出 SCO 流控制允许设置。通过使用该设置，主控制器能决定是否主控制器对于 SCO 联机句柄送出完成分组事件的数。
Write_SCO_Flow_Control_Enable	写入 SCO 流控制允许设置。通过使用该设置，主控制器能决定是否主控制器对于 SCO 联机句柄送出完成分组事件的数。
Set_Host_Controller_To_Host_Control	用于主控制器直接打开或关闭主控制器到主机的流控制。
Host_Buffer_Size	通过主机修改主控制器有关 ACL 和 SCO 数据缓冲区的大小。主控制器将从主控制器到主机分段传送数据，所以包含在 HCI 数据分组里的数据将不会超出这个区域。
Host_Number_Of_Completed_Packets	当主机对于任何联机句柄准备接收较多的 HCI 分组时，该命令用于通过主机指出主控制器。
Read_Link_Supervision_Timeout	对于设备读出链接管理超时参数。该参数通过主或从蓝牙设备到损失监控链接使用。
Write_Link_Supervision_Timeout	对于设备写入链接管理超时参数。该参数通过主或从蓝牙设备到损失监控链接使用。
Read_Number_Of_Supported_ICA	读出在查询扫描期间本地蓝牙设备正同时扫描的查询识别码（ICA）数的值，
Read_Current_ICA_LAP	读出用于创建在查询扫描期间本地蓝牙设备正同时扫描的查询识别码（ICA）的 LAP（s）。
Write_Current_ICA_LAP	写入用于创建在查询扫描期间本地蓝牙设备正同时扫描的查询识别码（ICA）的 LAP（s）。
Read_Page_Scan_Period_Mode	用于读出本地蓝牙设备的强制呼叫扫描区间模式。
Write_Page_Scan_Period_Mode	用于写入本地蓝牙设备的强制呼叫扫描区间模式。
Read_Page_Scan_Mode	用于读出本地蓝牙设备的默认呼叫扫描模式。
Write_Page_Scan_Period_Mode	用于写入本地蓝牙设备的默认呼叫扫描模式。

4.7.1 Set_Event_Mask

表 11.139

命令	OCF	命令参数	返回参数
HCI_Set_Event_Mask	0x0001	Event_Mask	状态

说明：

Set_Event_Mask 命令通过主机的 HCI 用来控制哪个事件产生。如果在 Event_Mask 的位置成 1，则与该位有关的事件产生。主机必须处理由蓝牙设备发生的每个事件。事件屏蔽允许主机控制中断数量。

注意：命令完成事件、命令状态事件和完成分组事件数不能屏蔽。这些事件总是出现。事件_屏蔽是整个事件指定的屏蔽位。

命令参数：

Event_Mask: 8 字节

表 11.140

值	参数说明
0x0000000000000000	无事件指定
0x0000000000000001	查询完成事件
0x0000000000000002	查询结果事件
0x0000000000000004	联机完成事件
0x0000000000000008	联机申请事件
0x0000000000000010	断开完成事件
0x0000000000000020	鉴权完成事件
0x0000000000000040	远程名申请完成事件
0x0000000000000080	加密变化事件
0x0000000000000100	变化联机链接字完成事件
0x0000000000000200	主单元链接字完成事件
0x0000000000000400	读远程支持特征完成事件
0x0000000000000800	读远程版本信息完成事件
0x0000000000001000	QoS 建立完成事件
0x0000000000002000	命令完成事件
0x0000000000004000	命令状态事件
0x0000000000008000	硬件错误事件
0x0000000000010000	刷新发生事件
0x0000000000020000	角色变化事件

表 11.141

值	参数说明
0x0000000000040000	完成分组事件的数
0x0000000000080000	模式变化事件
0x0000000000100000	返回链接字事件
0x0000000000200000	PIN 码申请事件
0x0000000000400000	链接字申请事件
0x0000000000800000	链接字注释事件
0x0000000001000000	反馈命令事件
0x0000000002000000	数据缓冲区溢出事件
0x0000000004000000	最大时隙变化事件
0x0000000008000000	读时钟补偿完成事件
0x0000000010000000	联机分组类型改变事件
0x0000000020000000	QoS 违例事件
0x0000000040000000	呼叫扫描模式改变事件
0x0000000080000000	呼叫扫描重复模式变化事件
0x0000000100000000-0x8000000000000000	保留
0x00000000FFFFFFFF	缺省(所有事件允许)

返回参数：

Status: 1 字节

表 11.142

值	参数说明
0x00	Set_Event_Mask 命令成功。

0x01-0xFF	Set_Event_Mask 命令失败。

事件产生(非屏蔽)：

当 Set_Event_Mask 命令完成时，命令完成事件产生。

4.7.2 Reset

表 11.143

命令	OCF	命令参数	返回参数
HCI_Reset	0x0003		Status

说明：

Reset 命令复位蓝牙主控制器、链接管理器和无线设备，而且放弃当前的操作选择，同时也放弃分组排队。在复位完成后，蓝牙设备进入待机模式。

注意：在复位完成后，主控制器自动还原到被定义在该说明里的默认参数值。

命令参数： 无。

返回参数：

Status: 1 字节

表 11.144

值	参数说明
0x00	复位命令成功，收到且将执行。
0x01-0xFF	复位命令失败。

事件产生(非屏蔽)：

4.7.3 Set_Event_Filter

表 11.145

命令	OCF	命令参数	返回参数
HCI_Set_Event_Filter	0x0005	Filter_Type, Filter_Condition_Type condition	Status

说明：

Set_Event_Filter 命令用来通过主机指定不同的事件过滤器。

对于同类事件过滤器或不同类事件过滤器，主机可多次发送各种联机申请。事件过滤器通过主机指定有关的对象，这些对象允许主控制器只发送与主机有关的事件。仅有一部分事件具有事件过滤器。

默认（开机和复位后）方式无过滤器设置，而且自动识别标志关闭（引入的联机不是自动识别）。每次从主机发送该命令时，都加入事件过滤器，Filter_Condition_Type 不等于 0x00（旧的事件过滤器不会重写）。为清除所有事件过滤器，使用 Filter_Type = 0x00,Auto_Accept
_Flag(自动识别标志)设置成关闭。

清除事件过滤器只能是确定的 Filter_Type，使用 Filter_Condition

_Type = 0x00。查询结果过滤器允许主控制器滤出查询结果事件。如果查询结果事件遇到由主机设置指定条件之一，查询结果过滤器允许主机指定主控制器只发送查询结果到主机。对于查询结果过滤器，主机可指定一个或多个下列过滤器联机类型：

1. 新设备响应查询过程。
2. 使用指定设备类的设备响应查询过程。
3. 使用指定 BD_ADDR 的设备响应查询过程。

查询结果过滤器使用查询和循环查询命令合取。如果事件遇到由主机指定的设置之一，则联机建立过滤器允许主机指出主控制器只发送联机完成和联机申请事件。作为联机建立过滤器，主机可指定一个或多个下列过滤器联机类型：

1. 允许与所有设备联机。
2. 允许与指定设备类的设备联机。
3. 允许用指定 BD_ADDR 的设备联机。

对于这些联机类型，自动识别标志参数允许主机指出，联机实现时应作什么样的动作。自动识别标志参数允许主机指出引入联机是否是自动识别（在自动识别情况下，当联机完成时，主控制器送出联机完成事件给主机，或是否由主机作出抉择，在这种情况下，主控制器送出联机申请事件给主机，在联机上引出抉择）。

联机建立过滤器用在 Read / Write_Scan_Enable 命令的合取上。如果本地设备处于呼叫扫描的过程，而且是在由主机设置的联机上的另一设备呼入，同时自动识别标志针对该设备已处于关闭状态，则联机申请事件通过主控制器发送到主机。在主机已响应引入联机期望后，联机完成事件随后送出。以同样的例子，如果自动识别标志是开启的，则联机完成事件通过主控制器送给主机（该情况下，无联机申请事件发送）。

主控制器在随机存储器里存储这些过滤器，直到主机使用 Set_Event _Filter 命令清除事件过滤器，或直到复位命令发出。主控制器存储的事件过滤器的次数是独立的实现。如果主机希望设立多于主控制器能存储的过滤器，主控制器将返回“存储器满”的错误码同时过滤器不能再存入。

注意：清除所有过滤器具有无过滤器条件或状态。

注意：在联机是处于自动识别状态时，链接字申请事件及可能是 PIN 码申请事件和链接字标志事件通过主控制器在联机完成事件发送前实现发送。如果在事件过滤器之间有矛盾，则后发送的事件过滤器将复盖先发送的事件过滤器。

命令参数：

Filter_Type: 1 字节

表 11.146

值	参数说明
0x00	清除的所有滤波器。（注意：在这种情况下，Filter_Condition_Type 和联机参数将不给出，其长度为 0 字节。Filter_Type 仅是参数。）
0x01	查询结果。
0x02	联机设置
0x03-0xFF	保留

过滤器联机类型：对于各个过滤器类型允许存在多个过滤器联机类型。

Inquiry_Result_Filter_Condition_Type: 1 字节

表 11.147

值	参数说明
0x00	响应查询过程的新设备。
0x01	响应查询过程指定设备类的设备。
0x02	响应查询过程指定 BD_ADDR 的设备。
0x03-0xFF	保留

Connection_Setup_Filter_Condition_Type: 1 字节

表 11.148

值	参数说明
0x00	允许所有的设备联机。
0x01	允许指定设备类的设备联机。
0x02	允许指定 BD_ADDR 的设备联机。
0x03-0xFF	保留

条件：各过滤器联机类型定义了查询结果过滤器和联机设置过滤器，要求的无联机参数或多个联机参数取决于过滤器联机类及过滤器类。

条件：Inquiry_Result_Filter_Condition_Type = 0x00。

Condition: 0 字节

表 11.149

值	参数说明
	没使用条件参数。

条件：Inquiry_Result_Filter_Condition_Type = 0x01。

长度：6 字节

Class_of_Device: 3 字节

表 11.150

值	参数说明
0x000000	缺省,返回所有的设备。
0xXXXXXX	相关设备类。

Class_of_Device_Mask: 3 字节

表 11.151

值	参数说明
0xXXXXXX	屏蔽位决定设备参数类的哪些位是无关项。屏蔽零值位指出设备类的哪些位是无关项。

条件：Inquiry_Result_Filter_Condition_Type = 0x02。

长度：6 字节

BD_ADDR: 6 字节

表 11.152

值	参数说明
0xXXXXXXXXXXXX	相关设备的 BD_ADDR

条件：Inquiry_Result_Filter_Condition_Type = 0x00。
长度：1 字节

Auto_Accept_Flag: 1 字节

表 11.153

值	参数说明
0x01	非自动识别联机。
0x02	自动识别联机。
0x03-0xFF	保留

条件：Inquiry_Result_Filter_Condition_Type = 0x01。
长度：7 字节

Class_of_Device: 3 字节

表 11.154

值	参数说明
0x000000	默认,返回所有设备。
0xXXXXXX	相关设备类。

Class_of_Device_Mask: 3 字节

表 11.155

值	参数说明
0xXXXXXX	屏蔽位决定设备参数类的哪些位是无关项。屏蔽零值位指出设备类的哪些位是无关项。

Auto_Accept_Flag: 1 字节

表 11.156

值	参数说明
0x01	非自动识别联机。
0x02	自动识别联机。
0x03-0xFF	保留

条件：Inquiry_Result_Filter_Condition_Type = 0x01。
长度：7 字节

BD_ADDR: 6 字节

表 11.157

值	参数说明
0xXXXXXXXXXXXX	相关设备类的 BD_ADDR

Auto_Accept_Flag: 1 字节

表 11.158

值	参数说明
0x01	非自动识别联机。
0x02	自动识别联机。
0x03-0xFF	保留。

返回参数：

Status: 1 字节

表 11.159

值	参数说明
0x00	Set_Event_Filter 命令成功。
0x01	Set_Event_Filter 命令失败。

事件产生(非屏蔽)：

当主控制器允许事件过滤时，该命令完成事件发生。当条件之一遇见时，指定事件发生。

4.7.4 刷新

表 11.160

命令	OCF	命令参数	返回参数
HCI_Flush	0x0008	Connection_handle	Status, connection_handle

说明：

刷新命令用来放弃对于主控制器所指联机句柄当前待传输的数据。甚至当前是属于大于主控制器里 L2CAP 分组的数据块。在此之后，发送到相同联机句柄主控制器的所有数据通过主控制器放弃，直到使用 Packet_Boundary_Flag（0x02）开始的 HCI 数据分组收到。

当此过程发生时，新的传输期望构成。在主控制器里的当前待传所有数据刷新前，该命令将允许高层软件控制联机句柄基带期望重传基带分组长度。

注意：刷新命令仅用于 ACL 联机方式。除刷新命令外，在指定刷新定时器终止后，自动刷新定时器能自动地刷新当前正发送的 L2CAP。

命令参数：

Connection: 2 字节(12 位有意义)

表 11.161

值	参数说明
0xXXXX	用来识别刷新联机的联机句柄。 范围：0x0000-0x0EFF(0x0F00-0x0FFF 保留)。

返回参数：

Status: 1 字节

表 11.162

值	参数说明
0x00	刷新成功的命令。
0x01-0xFF	刷新失败的命令。

Connection: 2 字节(12 位有意义)

表 11.163

值	参数说明
0xXXXX	用来识别发出刷新命令的联机句柄。 范围: 0x0000-0x0EFF （ 0x0F00 – 0x0FFF 保留）

事件发生（非屏蔽）:

一旦刷新命令执行，刷新发生事件发生。刷新发生事件由自动刷新引起或通过主机发出刷新命令引起。当刷新命令完成时，命令完成事件产生，并指出引起刷新的主机。

4.7.5 Read_PIN_Type

表 11.164

命令	OCF	命令参数	返回参数
HCI_Read_PIN_Type	0x0009		Status, pin_type

说明:

Read_PIN_Type 命令用于主机读出链接管理器假设由主机支持可变的 PIN 码仅为固定 PIN 码。蓝牙硬件在配对期间使用 PIN 类信息。

命令参数 无。

返回参数:

Status: 1 字节

表 11.165

值	参数说明
0x00	Read_PIN_Type 命令成功。
0x01-0xFF	Read_PIN_Type 命令失败。

PIN_Type: 1 字节

表 11.166

值	参数说明
0x00	可变 pin。
0x01	固定 Pin。

事件产生(非屏蔽):

当 Read_PIN_Type 命令完成时，命令完成事件产生。

4.7.6 Write_PIN_Type

表 11.167

命令	OCF	命令参数	返回参数
HCI_Write_PIN_Type	0x000a	Pin_type	Status

说明：

Write_PIN_Type 命令用于主机写入链接管理器假设主机支持可变的 PIN 码仅为固定 PIN 码。蓝牙硬件在配对期间使用 PIN 类信息。

命令参数：

PIN_Type: 1 字节

表 11.168

值	参数说明
0x00	可变 pin。
0x01	固定 Pin。

返回参数：

Status: 1 字节

表 11.169

值	参数说明
0x00	写 PIN 类命令成功。
0x01-0xFF	写 PIN 类命令失败。

事件产生(非屏蔽)：

当 Write_PIN_Type 命令完成时，命令完成事件产生。

4.7.7 Create_New_Unit_Key

表 11.170

命令	OCF	命令参数	返回参数
HCI_Create_New_Unit_Key	0x000b		Syatus

说明：

Create_New_Unit_Key 命令用来创建新单元字。 蓝牙硬件产生一个用于产生新单元字的随机启动源。所有新的联机将使用新单元字，但旧单元字仍被用于所有的当前联机。

注意：该命令对不使用单元字的设备没有任何影响（即：仅使用组合字的设备）。

命令参数： 无。

返回参数：

Status 1 字节

表 11.171

值	参数说明
0x00	创建新单元字命令成功。
0x01-0xFF	创建新单元字命令失败。

事件产生(非屏蔽)：

当 Create_New_Unit_Key 命令完成时，完成事件命令产生。

4.7.8 Read_Stored_Link_Key

表 11.172

命令	OCF	命令参数	返回参数
HCI_Read_Stored_ Link_Key	0x000d	Bd_addr Read_all_flag	Status Max_num_keys Num_keys_read

说明：

Read_Stored_Link_Key 命令提供读出一个或多个存储在蓝牙主控制器里的链接字。对于其它的蓝牙设备的蓝牙主控制器只能提供存储有限的链接字。链接字为两个蓝牙设备共享，而且用于两设备间安全处理。当需要时，主机可增加存储量，为再装入蓝牙主控制器的连接字提供存储需要。Read_All_Flag 参数来指出是否整个链接字将返回。

如果 Read_All_Flag 指出所有链接字将返回，那么命令参数的 BD_ADDR 必须忽略。BD_ADDR 命令参数用来识别读出哪个链接字。存储链接字通过一个或多个返回链接字事件来返回。

命令参数：

BD_ADDR: 6 字节

表 11.173

值	参数说明
0xXXXXXXXXXXXX	读存储链接字的 BD_ADDR

Read_All_Flag: 1 字节

表 11.174

值	参数说明
0x00	返回指定 BD_ADDR 的链接字。
0x01	返回所有存储链接字。
0x02-0xFF	保留

返回参数：

Status: 1 字节

表 11.175

值	参数说明
0x00	Read_Stored_Link_Key 命令成功。
0x01-0xFF	Read_Stored_Link_Key 命令失败。

Max_Num_Key: 2 字节

表 11.176

值	参数说明
0xXXXX	主控制器能存储链接字的最大量。 范围：0x0000-0xFFFF

Num_Keys_Read: 2 字节

表 11.177

值	参数说明

0xXXXX	读链接字数 范围：0x0000-0xFFFF

事件产生(非屏蔽)：

命令发出后，没有或多个返回链接字事件发生。当没有链接字存储时，无返回链接字事件返回。当有链接字存储时，指定在各返回链接字事件里的链接字返回数执行。

当 Read_Stored_ Link_Key 命令完成时，命令完成事件产生。

4.7.9 write_store_link_key

表 11.178

命令	OCF	命令参数	返回参数
HCI_Write_Stored_Link_Key	0X0011	NUM_KEYS_TO_WRITE BD_ADDR LINK_KEY	STATUS NUM_KEYS_WRITEN

说明：

Write_Stored_Link_Key 命令提供写入一个或多个存储在蓝牙主控制器里的链接字。对于其它的蓝牙设备蓝牙主控制器只能存储有限的链接字。如果在蓝牙主控制器里没有有效的附加空间，就不能存储附加的链接字。如空间有限，则所有链接字要存储在有限空间里是不合适的。正确的链接字表序列可确定哪些链接字被存储。首先在表开始处的链接字被存储。

NUM_KEYS_WRITE 参数返回成功存储的链接字数。如果没有附加的存储空间，在任何附加链接字存储前，主机必须删除一个以上的已存储链字。

链接字替换算法通过主机完成而不是主控制器来执行。链接字替换算法由主机执行和不由主机控制器执行。

链接字为两个蓝牙设备共享，而且用于两设备间安全处理。当需要时，主机可增加存储量，为再装入蓝牙主控制器的连接字提供存储需要。

注意：通过该命令的发出，只能存储链接字。

命令参数：

Num_Keys_To_Write: 1 字节

表 11.179

值	参数说明。
0xXX	写入链接字数。

BD_ADDR: 6 字节

表 11.180

值	参数说明
0xXXXXXXXXXXXX	与链接字有关的 BD_ADDR。

Link_Key: 16 字节

表 11.181

值	参数说明

0xXXXXXXXXXXXXXXXXXXXXXXXX	与 BD_ADDR 有关的链接字。

返回参数：

Status: 1 字节

表 11.182

值	参数说明
0x00	Write_Stored_Link_Key 命令成功。
0x01-0xFF	Write_Stored_Link_Key 命令失败。

Num_Keys_Written: 1 字节

表 11.183

值	参数说明
0xXX	成功写入的链接字数。 范围：0x00-0xFF

事件产生（非屏蔽）：

当 Write_Stored_Link_Key 命令完成时，命令完成事件产生。

4.7.10 delete_store_link_key

表 11.184

命令	OCF	命令参数	返回参数
HCI_Delete_Stored_Link_Key	0x0012	Bd_addr Delete_all_flag	Status Num_keys_deleted

说明：

Delete_Stored_Link_Key 命令提供删除一个以上的存储在蓝牙主控制器里的链接字。蓝牙主控制器只能为其它蓝牙设备存储有限的链接字。链接字为两个蓝牙设备共享，而且用于两设备间安全处理。

Delete_all_flag 参数用来指出是否所有的存储链接字都要删除。

如果 Delete_All_Flag 指出所有的链接字被删除，那么 BD_ADDR 命令参数必须忽略该命令提供在设备之间达成安全协议能力。BD_ADDR 命令参数用来识别删除哪个链接字。如果链接字是用于当前的联机，当所有的联机断开时，则链接字被删除。

命令参数：

BD_ADDR: 6 字节

表 11.185

值	参数说明
0xXXXXXXXXXXXX	被删除链接字的 BD_ADDR。

Delete_All_Flag: 1 字节

表 11.186

值	参数说明
0x00	仅删除指定 BD_ADDR 链接字。
0x01	删除所有存储链接字。

0x02-0xFF	保留

返回参数：

Status: 1 字节

表 11.187

值	参数说明
0x00	Delete_Stored_Link_Key 命令成功。
0x01-0xFF	Delete_Stored_Link_Key 命令失败。

Num_Keys _Deleted: 2 字节

表 11.188

值	参数说明
0xXXXX	删除的链接字数。

事件产生(非屏蔽)：

当 Delete_Stored_Link_Key 命令完成时，命令完成事件产生。

4.7.11 Change_Local_Name

表 11.189

命令	OCF	命令参数	返回参数
HCI_Change_Local_Name	0x0013	Name	Status

说明：

Change_Local_Name 命令提供蓝牙设备用户友好名的修改能力。蓝牙设备可发送申请得到另外蓝牙设备的用户友好名。用户友好名提供用户把蓝牙设备与另外蓝牙设备区分开来的能力。名命令参数编码是长度可达 248 个字节的 UTF-8。如果 UTF-8 编码不到 248 个字节，名命令参数应是空终止(0x00)。

注意：名参数以名第一字节开始发送。传输多字节参数小 Endian 序列格式是一个例外。

命令参数：

Name: 248 字节

表 11.190

值	参数说明
	UTF-8 用户友好编码描述了设备名称。 UTF-8 编码名长度可达的 248 个字节。如果它小于 248 个字节，用空字节(0x00)指出结束。
	空终止零长度，**默认**。

返回参数：

Status: 1 字节

表 11.191

值	参数说明
0x00	Change_Local_Name 命令成功。

0x01-0xFF	Change_Local_Name 命令失败

事件产生了(非屏蔽)：

当 Change_Local_Name 命令完成时，命令完成事件产生。

4.7.12 Read_Local_Name

表 11.192

命令	OCF	命令参数	返回参数
HCI_Read_Local_Name	0x0014		Status, name

说明：

Read_Local_Name 命令提供读蓝牙设备存储用户友好名能力。用户友好名提供用户把蓝牙设备与另外蓝牙设备区分开来的能力。名返回参数编码是长度可达 248 个字节的 UTF-8。如果 UTF-8 编码不到 248 个字节，名返回参数应是空终止(0x00)。

注意：名参数以名第一字节开始发送。传输多字节参数小 Endian 序列格式是一个例外。

命令参数： 无。

返回参数：

Status: 1 字节

表 11.193

值	参数说明
0x00	Read_Local_Name 命令成功。
0x01-0xFF	Read_Local_Name 命令失败。

Name: 248 字节

表 11.194

值	参数说明
	UTF-8 用户友好编码描述了设备名称。 UTF-8 编码名长度可达的 248 个字节。如果它小于 248 个字节，用空字节(0x00)指出结束。

事件产生(非屏蔽)：

当 Read_Local_Name 命令完成时，命令完成事件。

4.7.13 Read_Connection_Accept_Timeout

表 11.195

命令	OCF	命令参数	返回参数
HCI_Read_Connection_Accept_Timeout	0x0015		Satus, conn_accept_timeout

说明：

该命令读出 Connection_Accept_Timeout 结构参数值。在指定周期已出现并且新的联

机还没识别后， Connection_Accept_Timeout 参数允许蓝牙硬件自动地拒绝联机申请。该参数定义为从当主控制器发出联机申请事件起到主控制器自动拒绝引入联机止的时间区间。

命令参数： 无。

返回参数：

Status: 1 字节

表 11.196

值	参数说明
0x00	Read_Connection_Accept_Timeout 命令成功。
0x01-0xFF	Read_Connection_Accept_Timeout 命令失败。

Conn_Accept_Timeout: 2 字节

表 11.197

值	参数说明
N=0xXXXX	在基带时隙的数里联机识别超时测量。 Interval Length = N * 0.625 msec(单基带时隙) 范围：0.625ms – 29s

事件产生(非屏蔽)：

当 Read_Connection_Timeout 命令完成时，命令完成事件产生。

↕

4.7.14 Write_Connection_Accept_Timeout

表 11.198

命令	OCF	命令参数	返回参数
HCI_Write_Connection_Accept_Timeout	0x0016		Status

说明：

该命令写入 Connection_Accept_Timeout 结构参数值。在指定周期已出现并且新的联机还没识别后， Connection_Accept_Timeout 参数允许蓝牙硬件自动地拒绝联机申请。该参数定义为从当主控制器发出联机申请事件起到主控制器自动拒绝引入联机止的时间区间。

命令参数：

Conn_Accept_Timeout: 2 字节

表 11.199

值	参数说明
N = 0xXXXX	在基带时隙的数里联机识别超时测量。 Interval Length = N * 0.625 msec(单基带时隙) N 的范围：0x0001 – 0xb540 时间范围：0.625ms – 29s 默认：N = 0x1FA0 时间=5s

返回参数：

Status: 1 字节

表 11.200

值	参数说明
0x00	Write_Connection_Accept_Timeout 命令成功。
0x01-0xFF	Write_Connection_Accept_Timeout 命令失败。

事件产生(非屏蔽)：

当 Write_Connection_Accept_Timeout 命令完成时，命令完成事件产生。

4.7.15 Read_Page_Timeout

表 11.201

命令	OCF	命令参数	返回参数
HCI_Write_Connection_ Accept_Timeout	0x0017		Status Page_timeout

说明：

该命令读出 Page_Timeout 结构参数值。 Page_Timeout 结构参数定义本地链接管理器等待基带呼叫响应的最大时间，该基带呼叫响应来自于本地初始化联机期望的远程设备。如果该时间终止和远程设备没在基带级上响应呼叫，联机期望将认为是失败。

命令参数： 无。

返回参数：

Status: 1 字节

表 11.202

值	参数说明
0x00	Read_Page_Timeout 命令成功。
0x01-0xFF	Read_Page_Timeout 命令失败。

Page_Timeout: 2 字节

表 11.203

值	参数说明
N = 0xXXXX	在基带时隙数里的呼叫超时测量。 间隔长度= N * 0.625ms (单基带时隙) N 的范围：0x0001 - 0xFFFF 时间范围：0.625ms - 40.9s

事件产生(非屏蔽)：

当 Read_Page_Timeout 命令完成时，命令完成事件产生。

4.7.16 Write_Page_Timeout

表 11.204

命令	OCF	命令参数	返回参数
HCI_Write_Page_Timeout	0x0018	Page_Timeout	Status

说明：

该命令写入 Page_Timeout 结构参数值。 Page_Timeout 结构参数定义本地链接管理器等待基带呼叫响应的最大时间，该基带呼叫响应来自于本地初始化联机期望的远程设备。如果该时间终止和远程设备没在基带级上响应呼叫，联机期望将认为是失败。

命令参数：

Page_Timeout: 2 字节

表 11.205

值	参数说明
0	非法呼叫超时。必须大于 0。
N = 0xXXXX	在基带时隙数里的呼叫超时测量。 间隔长度= N * 0.625ms N 的范围：0x0001 - 0xFFFF 时间范围：0.625ms - 40.9s 默认：N = 0x2000 时间=5.12s

返回参数：

Status: 1 字节

表 11.206

值	参数说明
0x00	Write_Page_Timeout 命令成功。
0x01-0xFF	Write_Page_Timeout 命令失败。

事件产生(非屏蔽)：

当 Write_Page_Timeout 命令完成时，命令完成事件产生。

4.7.17 Read_Scan_Enable

表 11.207

命令	OCF	命令参数	返回参数
HCI_Read_Scan_Enable	0x0019		Status Scan_enable

说明：

该命令读出 Scan_Enable 参数值。Scan_Enable 参数控制蓝牙设备是否周期性地扫描其它蓝牙设备的呼叫期望或查询申请。

如果 Page_Scan 允许，则设备将基于 Page_Scan_Interval 和 Page_Scan_Window 参数进入呼叫扫描模式。

如果 Inquiry_Scan 允许，则设备将基于 Inquiry_Scan_Interval 和 Inquiry_Scan_window 参数进入查询扫描模式。

命令参数： 无。

返回参数：

Status: 1 字节

表 11.208

值	参数说明
0x00	Read_Scan_Enable 命令成功了。
0x01-0xFF	Read_Scan_Enable 命令失败。

Scan_Enable 1 字节

表 11.209

值	参数说明
0x00	无扫描允许。
0x01	查询扫描允许。 呼叫扫描禁止。
0x02	查询扫描禁止。 呼叫扫描允许。
0x03	查询扫描允许。 呼叫扫描允许。

事件产生(非屏蔽)：

当 Read_Scan_Enable 命令完成时，命令完成事件产生。

4.7.18 Write_Scan_Enable

表 11.210

命令	OCF	命令参数	返回参数
HCI_Write_Scan_Enable	0x001A	Scan_Enable	status

说明：

该命令写入 Scan_Enable 参数值。Scan_Enable 参数控制蓝牙设备是否周期性地扫描其它蓝牙设备的呼叫期望或查询申请。

如果 Page_Scan 允许，则设备将基于 Page_Scan_Interval 和 Page_Scan_Window 参数进入呼叫扫描模式。

如果 Inquiry_Scan 允许，则设备将基于 Inquiry_Scan_Interval 和 Inquiry_Scan_window 参数进入查询扫描模式。

命令参数：

Scan_Enable: 1 字节

表 11.211

值	参数说明
0x0	无扫描允许，**默认**。
0x01	查询扫描允许。 呼叫扫描禁止。
0x02	查询扫描禁止。 呼叫扫描允许。
0x03	查询扫描允许。

	呼叫扫描允许。

返回参数：

Status: 1 字节

表 11.212

值	参数说明
0x00	Write_Scan_Enable 命令成功。
0x01-0xFF	Write_Scan_Enable 命令失败。

事件产生(非屏蔽)：

当 Write_Scan_Enable 命令完成时，命令完成事件产生。

4.7.19 Read_Page_Scan_Activity

表 11.213

命令	OCF	命令参数	返回参数
HCI_Read_Page_Scan_活动	0x001B		Status Page_Scan_Interval, Page_Scan_Window

说明：

该命令读出 Page_Scan_Activity 结构参数值。Page_Scan_Interval 结构参数定义为连续呼叫扫描之间的时间量。该时间间隔被定义为主控制器上次呼叫扫描的开始处到下次呼叫扫描的开始。Page_Scan_Window 结构参数定义为呼叫扫描持续时间。

Page_Scan_Window 只能是小于或等于 Page_Scan_Interval。

注意：当 Page_Scan 允许时，仅呼叫扫描执行。改变 Page_Scan _Interval 能改变本地的 Page_Scan_Repetition_Mode。

命令参数： 无。

返回参数：

Status: 1 字节

表 11.214

值	参数说明
0x00	Read_Page_Scan_Activity 命令成功。
0x01-0xFF	Read_Page_Scan_Activity 命令失败。

Page_Scan_Interval: 2 字节

表 11.215

值	参数说明
N=0xXXXX	长度：2 字节 范围：0x0012-0x1000 时间= N * 0.625ms 范围：11.25ms - 2560ms

Page_Scan_Window: 2 字节

表 11.216

值	参数说明
N=0xXXXX	长度：2 字节 范围：0x0012 - 0x1000 时间= N * 0.625ms 范围：11.25ms - 2560ms

事件产生(非屏蔽)：

当 Read_Page_Scan_Activity 命令完成时，命令完成事件产生。

4.7.20 Write_Page_Scan_Activity

表 11.217

命令	OCF	命令参数	返回参数
HCI_Write_Page_Scan_Activity	0x001C	Page_Scan_Interval, Page_Scan_Window	Status

说明：

该命令写入 Page_Scan_Activity 结构参数值。Page_Scan_Interval 结构参数定义为连续呼叫扫描之间的时间量。该时间间隔被定义为主控制器上次呼叫扫描的开始处到下次呼叫扫描的开始。Page_Scan_Window 结构参数定义为呼叫扫描持续时间。

Page_Scan_Window 只能是小于或等于 Page_Scan_Interval。

注意：当 Page_Scan 允许时，仅呼叫扫描执行。改变 Page_Scan _Interval 能改变本地的 Page_Scan_Repetition_Mode。

命令参数：

Page_Scan_Interval: 2 字节

表 11.218

值	参数说明
N=0xXXXX	长度：2 字节 范围：0x0012 - 0x1000 时间 = N * 0.625ms 范围：11.25ms - 2560ms 默认：N = 0x0800 时间 = 1.28s

Page_Scan_Window: 2 字节

表 11.219

值	参数说明
N=0xXXXX	长度：2 字节 范围：0x0012 - 0x1000 时间 = N * 0.625ms 范围：11.25ms - 2560ms

	默认: N = 0x0012 时间 = 11.25ms

返回参数 ：

Status: 1 字节

表 11.220

值	参数说明
0x00	Write_Page_Scan_Activity 命令成功。
0x01-0xFF	Write_Page_Scan_Activity 命令失败。

事件产生(非屏蔽)：

当 Write_Page_Scan_Activity 命令完成时，命令完成事件产生。

4.7.21 Read_Inquiry_Scan_Activity

表 11.221

命令	OCF	命令参数	返回参数
HCI_Read_ Inquiry_Scan_ Activity	0x001D		Status Inquiry_Scan_Interval, Inquiry_Scan_Window

说明：

该命令读出 Inquiry_Scan_Activity 结构参数值。Inquiry_Scan _Interval 结构参数定义为连续查询扫描之间的时间量。该时间间隔被定义为主控制器上次查询扫描的开始处到下次查询扫描的开始。

Inquiry_Scan_Window 结构参数定义为呼叫查询持续时间。

Inquiry_Scan_Window 只能是小于或等于 Inquiry_Scan_Interval。

注意：当 Inquiry_Scan 允许时，仅查询扫描执行。

命令参数： 无。

返回参数：

Status: 1 字节

表 11.222

值	参数说明
0x00	Read_Inquiry_Scan_Activity 命令成功。
0x01	Read_Inquiry_Scan_Activity 命令失败。

Inquiry_Scan_Interval: 2 字节

表 11.223

值	参数说明
N=0xXXXX	长度：2 字节 范围：0x0012 - 0x1000 时间 = N * 0.625ms 范围：11.25ms - 2560ms

Inquiry_Scan_Window: 2 字节

表 11.224

值	参数说明
N=0xXXXX	长度：2 字节 范围：0x0012 - 0x1000 时间 = N * 0.625ms 范围：11.25ms-2560ms

事件产生(非屏蔽)：

当 Read_Inquiry_Scan_Activity 命令完成时，命令完成事件产生。

4. 7。22 Write_Inquiry_Scan_Activity

表 11.225

命令	OCF	命令参数	返回参数
HCI_Write_Inquiry_Scan_Activity 0x001E	0x001E	Inquiry_Scan_Interval Inquiry_Scan_Window	Status

说明：

该命令写入 Inquiry_Scan_Activity 结构参数值。Inquiry_Scan _Interval 结构参数定义为连续查询扫描之间的时间量。该时间间隔被定义为主控制器上次查询扫描的开始处到下次查询扫描的开始。

Inquiry_Scan_Window 结构参数定义为呼叫查询持续时间。

Inquiry_Scan_Window 只能是小于或等于 Inquiry_Scan_Interval。

注意：当 Inquiry_Scan 允许时，仅查询扫描执行。

命令参数：

Inquiry_Scan_Interval: 2 字节

表 11.226

值	参数说明
N=0xXXXX	长度：2 字节 范围：0x0012 - 0x1000 时间 = N * 0.625ms 范围：11.25ms - 2560ms 默认：N = 0x0800 时间 = 1.28s

Inquiry_Scan_Window: 2 字节

表 11.227

值	参数说明
N=0xXXXX	长度：2 字节 范围：0x0012 - 0x1000 时间 = N * 0.625ms

	范围：11.25ms – 2560ms 默认：N = 0x0012 时间 = 11.25ms

返回参数：

Status: 1 字节

表 11.228

值	参数说明
0x00	Write_Inquiry_Scan_Activity 命令成功。
0x01-0xFF	Write_Inquiry_Scan_Activity 命令失败。

事件产生(非屏蔽)：

当 Write_Inquiry_Scan_Activity 命令完成时，命令完成事件产生。

4. 7。23 Read_Authentication_Enable

表 11.229

命令	OCF	命令参数	返回参数
HCI_Read_Authentication_Enable	0x001F		Status Authentication_enable

说明：

该命令读出 Authentication_Enable 参数值。Authentication_ Enable 参数控制是否由本地设备申请在联机设置（在创建联机命令或引入 ACL 联机的接收而且符合联机完成事件）下鉴权远程设备。在联机设置下，只有使用 Authentication_Enable 参数允许的设备可期望鉴权其它的设备。

注意：改变此参数不影响现存的联机。

命令参数： 无。

返回参数：

Status: 1 字节

表 11.230

值	参数说明
0x00	Read_Authentication_Enable 命令成功。
0x01-0xFF	Read_Authentication_Enable 命令失败。

Authentication_Enable: 1 字节

表 11.231

值	参数说明
0x00	鉴权禁止。
0x01	允许所有的联机鉴权。
0x02-0xFF	保留

事件产生(非屏蔽)：

当 Read_Authentication_Enable 命令完成时，命令完成事件产生。

4.7.24 Write_Authentication_Enable

表 11.232

命令	OCF	命令参数	返回参数
HCI_Write_Authentication_Enable	0x0020	Authentication_Enable	Status

说明：

该命令写入 Authentication_Enable 参数值。Authentication _Enable 参数控制是否由本地设备申请在联机设置（在创建联机命令或引入 ACL 联机的接收而且符合联机完成事件）下鉴权远程设备。在联机设置下，只有使用 Authentication_Enable 参数允许的设备可期望鉴权其它的设备。

注意：改变此参数不影响现存的联机。

命令参数：

Authentication_Enable: 1 字节

表 11.233

值	参数说明
0x00	鉴权禁止。**默认**
0x01	允许所有联机鉴权。
0x02-0xFF	保留

返回参数：

Status: 1 字节

表 11.234

值	参数说明
0x00	Write_Authentication_Enable 命令成功。
0x01-0xFF	Write_Authentication_Enable 命令成功。

事件产生(非屏蔽)：

当 Write_Authentication_Enable 命令完成时，命令完成事件产生。

4.7.25 Read_Encryption_Mode

表 11.235

命令	OCF	命令参数	返回参数
HCI_Read_Encryption_Mode	0x0021		Status, Encryption_Mode

说明：

该命令读出 Encryption_Mode 参数值。Encryption_Mode 参数控制是否由本地设备申请在联机设置（在创建联机命令或引入 ACL 联机的接收而且符合联机完成事件）下加密远程设

备。在联机设置下，只有使用 Authentication_Enable 参数允许和 Encryption_Mode 参数允许的设备可期望加密其它的设备。

注意：改变此参数不影响现存的联机。

命令参数： 无。

返回参数：

Status: 1 字节

表 11.236

值	参数说明
0x00	Read_Encryption_Mode 命令成功。
0x01	Read_Encryption_Mode 命令失败。

Encryption_Mode: 1 字节

表 11.237

值	参数说明
0x00	加密禁止。
0x01	仅为点对点的分组加密。
0x02	为点对点和广播分组加密。
0x03-0xFF	保留。

事件产生(非屏蔽)：

当 Read_Encryption_Mode 命令完成时，命令完成事件产生。

4.7.26 Write_Encryption_Mode

表 11.238

命令	OCF	命令参数	返回参数
HCI_Write_Encryption_Mode	0x0022	Encryption_Mode	Status

说明：

该命令写入加密模式参数值。Encryption_Mode 参数控制是否由本地设备申请在联机设置（在创建联机命令或引入 ACL 联机的接收而且符合联机完成事件）下加密远程设备。在联机设置下，只有使用 Authentication_Enable 参数允许和 Encryption_Mode 参数允许的设备可期望加密其它的设备。

注意：改变此参数不影响现存的联机。

当广播和点对点通信加密时，必须使用临时链接字。

虽然该参数用于申请远程设备的加密能力，但主机不必指定比本地设备支持的加密能力

更多的 Encryption_Mode 参数。

注意：当本地设备不支持加密时，主机不要求使用 Encryption_Mode 参数的命令设成 0x01 或 0x02。当本地设备不支持广播加密时，也注意到主机不要求使用 Encryption_Mode 参数的命令设成 0x02。

注意：当本地设备申请多于远程设备支持的加密能力时，对于只支持部分能力的新的联机（或联机完成事件），实际 Encryption_Mode 在事件里返回。例如，当远程设备不支持加密时，在事件里返回 0x00，当只支持点对点的加密时，返回 0x00 或 0x01。

命令参数：

Encryption_Mode: 1 字节

表 11.239

值	参数说明
0x00	加密禁止，**默认。**
0x01	仅为点对点的分组加密。
0x02	为点对点和广播分组加密。
0x03-0xFF	保留

返回参数：

Status: 1 字节

表 11.240

值	参数说明
0x00	Write_Encryption_Mode 命令成功。
0x01-0xFF	Write_Encryption_Mode 命令失败。

事件产生(非屏蔽)：

当 Write_Encryption_Mode 命令完成时，命令完成事件产生。

4.7.27 Read_Class_of_Device

表 11.241

命令	OCF	命令参数	返回参数
HCI_Read_Class_of_Device	0x0023		Status Class_of_Device

说明：

该命令读出 Class_of_Device 参数值。Class_of_Device 参数用来指出本地设备到其它设备的能力。

命令参数： 无。

返回参数：

Status: 1 字节

表 11.242

值	参数说明
0x00	Read_Class_of_Device 命令成功。
0x01	Read_Class_of_Device 命令失败。

Class_of_Device: 3 字节

表 11.243

值	参数说明
0xXXXXXX	设备类型。

事件产生(非屏蔽)：

当 Read_Class_of_Device 命令完成时，命令完成事件产生。

Write_Class_of_Device

表 11.244

命令	OCF	命令参数	返回参数
HCI_Write_Class_of_Device	0x0024	Class_of_Device	Status

说明：

该命令写入 Class_of_Device 参数值。Class_of_Device 参数用来指出本地设备到其它设备的能力。

命令参数：

Class_of_Device: 3 字节

表 11.245

值	参数说明
0xXXXX	设备类型。

返回参数：

Status: 1 字节

表 11.246

值	参数说明
0x00	Write_Class_of_Device 命令成功。
0x01	Write_Class_of_Device 命令失败。

事件产生(非屏蔽)：

当 Write_Class_of_Device 命令完成时，命令完成事件产生。

4.7.28 Read_Voice_Setting

表 11.247

命令	OCF	命令参数	返回参数
HCI_Read_Voice_Setting	0x0025		Status Voice_Setting

说明：

该命令读出Voice_Setting 参数值。Voice_Setting 参数控制所有语音联机的各种设置。这些设置用于所有语音联机但不能设置成单个语音联机。Voice_Setting 参数控制语音联机的配置：输入编码，无线编码格式，输入数据格式，输入采样容量，和线性 PCM 参数。

命令参数： 没有。

返回参数：

Status: 1 字节

表 11.248

值	参数说明
0x00	Read_Voice_Setting 命令成功了。
0x01	Read_Voice_Setting 命令失败了。

Voice_Setting: 2 字节(10 位有意义)

表 11.249

值	参数说明
00XXXXXXXX	输入编码：线性
01 XXXXXXXX	输入编码： μ-law 输入编码
10 XXXXXXXX	输入编码：A-law 输入编码
11 XXXXXXXX	保留
XX 00XXXXXX	输入数据格式：反码
XX01XXXXXX	输入数据格式：补码
XX10XXXXXX	输入数据格式：信号幅度
XX11XXXXXX	保留
XXXX0XXXXX	输入采样容量： 8 位(仅为线性 PCM)
XXXX1XXXXX	输入采样容量：16 位(仅为线性 PCM)
XXXXXnnnXX	Linear_PCM_Bit_Pos：采样的 MSB#位位置总是从 MSB（仅为线性 PCM）开始。
XXXXXXXX00	无线电编码格式 CVSD
XXXXXXXX01	无线电编码格式 μ_law
XXXXXXXX10	无线电编码格式 A_law
XXXXXXXX11	保留

事件产生(非屏蔽)：

当 Read_Voice_Setting 命令完成时，命令完成事件产生。

4.7.29 Write_Voice_Setting

表 11.250

命令	OCF	命令参数	返回参数

HCI_Write_Voice_Setting	0x0026	Voice_Setting	Status

说明：

该命令写入Voice_Setting参数值。Voice_Setting参数控制所有语音联机的各种设置。这些设置用于所有语音联机但不能设置成单个语音联机。Voice_Setting参数控制语音联机的配置：输入编码，无线编码格式，输入数据格式，输入采样容量，和线性PCM参数。

命令参数：

Voice_Setting: 2字节(10 位有意义)

表 11.251

值	参数说明
00XXXXXXXX	输入编码：线性
01 XXXXXXXX	输入编码： μ-law输入编码
10 XXXXXXXX	输入编码：A-law输入编码
11 XXXXXXXX	保留
XX 00XXXXXX	输入格式：反码
XX01XXXXXX	输入格式：补码
XX10XXXXXX	输入格式：信号幅度
XX11XXXXXX	保留
XXXX0XXXXX	输入采样容量：8位(仅为线性PCM)
XXXX1XXXXX	输入取样容量:16位(仅为线性PCM)
XXXXXnnnXX	Linear_PCM_Bit_Pos：采样的MSB#位位置总是从MSB（仅为线性PCM）开始。
XXXXXXXX00	无线电编码格式：CVSD
XXXXXXXX01	无线电编码格式： μ_law
XXXXXXXX10	无线电编码格式：A_law
XXXXXXXX11	保留
0001100000	默认条件

返回参数：

Status: 1字节

表 11.252

值	参数说明
	Write_Voice_Setting 命令成功。
	Write_Voice_Setting 命令失败。

事件产生(非屏蔽)：

当 Write_Voice_Setting 命令完成时，命令完成事件产生。

4.7.31 Read_Automatic_Flush_Timeout

表 11.253

命令	OCF	命令参数	返回参数
HCI_Read_Automatic_Flush_Timeout	0x0027	Connection_Handle	Status, Connection_Handle, Flush_Timeout

说明：

该命令对于指定的联机句柄读出 Flush_Timeout 参数值。Flush_ Timeout 参数仅用于 ACL 链接。Flush_Timeout 参数定义在所有 L2CAP 分组块前的时间量，基带分组当前正在发送时，由主控制器自动刷新。当传输期望构造 L2CAP 分组的第一个基带分组时，超时区域开始。如果没有主机发送刷新命令时，它允许 ACL 分组自动地刷新。

Read_Automatic_ Flush_Timeout 命令提供对等时数据的支持，例如图象。当此时正在传输的 L2CAP 分组被自动地“刷新”时，失败计数器增加 1。指定联机句柄的传输的下一个 L2CAP 分组的第一块可预先存储在主控制器里。在这种情况下，含有 L2CAP 分组数据的第一个基带分组的传输可直接地开始。

如果下一个 L2CAP 分组没存在主控制器里，在相同联机句柄刷新后，发送给主控制器的所有数据通过主控制器放弃，直到具有 Packed_Boundary Packed_Boundary_Flag(0x02)开始的 HCI 数据分组收到。当该种情况发生时，一次新的传输期望构成。

命令参数：

Connection_handle: 2 字节(12 位有意义)

表 11.254

值	参数说明
0xXXXX	指定读哪个联机句柄的刷新超时。 范围: 0x0000-0x0EFF （ 0x0F00 - 0x0FFF 保留）

返回参数：

Status: 1 字节

表 11.255

值	参数说明
0x00	Read_Automatic_刷新时间命令成功。
0x01	Read_Automatic_刷新时间命令失败。

Connection_Handle: 2 字节(12 位有意义)

表 11.256

值	参数说明
0xXXXX	指定哪个联机句柄的刷新超时已读过。 范围: 0x0000 - 0x0EFF （ 0x0F00 - 0x0FFF 保留）

Flush_Timeout: 2 字节

表 11.257

值	参数说明
0	超时 = ∞; 无自动刷新
N=0xXXXX	刷新超时 = N * 0.625ms 长度: 11 字节 范围: 0x0001 - 0x07FF

事件产生(非屏蔽)：

当 Read_Automatic_刷新时间命令完成时，命令完成事件产生。

4.7.32 Write_Automatic_ Flush_Timeout

表 11.258

命令	OCF	命令参数	返回参数
HCI_Write_Automatic_Flush_Timeout	0x0028	Connection_Handle, Flush_Timeout	Status 联机句柄

说明：

命令对于指定的联机句柄写入 Flush_Timeout 参数值。Flush_ Timeout 参数仅用于 ACL 链接。Flush_Timeout 参数定义在所有 L2CAP 分组块前的时间量，基带分组当前正在发送时，由主控制器自动刷新。当传输期望构造 L2CAP 分组的第一个基带分组时，超时区域开始。如果没有主机发送刷新命令时，它允许 ACL 分组自动地刷新。

Read_Automatic_ Flush_Timeout 命令提供对等式数据的支持，例如图象。当此时正在传输的 L2CAP 分组被自动地'刷新'时，失败计数器增加 1。指定联机句柄的传输的下一个 L2CAP 分组的第一块可预先存储在主控制器里。在这种情况下，含有 L2CAP 分组数据的第一个基带分组的传输可直接地开始。

如果下一个 L2CAP 分组没存在主控制器里，在相同联机句柄刷新后，发送给主控制器的所有数据通过主控制器放弃，直到具有 Packed_Boundary_Flag(0x02)开始的 HCI 数据分组收到。当该种情况发生时，一次新的传输期望构成。

命令参数：

Connection_Handle: 2 字节(12 位有意义)

表 11.259

值	参数说明
0xXXXX	指定写哪个联机句柄的刷新超时。 范围: 0x0000 – 0x0EFF (0x0F00 – 0x0FFF 保留)

Flush_Timeout: 2 字节

表 11.260

值	参数说明
0	超时 = ∞; 无自动刷新，**默认**。
N=0xXXXX	刷新超时 = N * 0.625ms 长度: 11 字节 范围:0x0001-0x07FF

返回参数：

Status: 1 字节

表 11.261

值	参数说明
0x00	Write_Automatic_刷新时间命令成功。
0x01	Write_Automatic_刷新时间命令失败。

Connection_Handle: 2 字节(12 位有意义)

表 11.262

值	参数说明
0xXXXX	指定哪个联机句柄的刷新超时已写过。

	范围：0x0000 – 0x0EFF （ 0x0F00 – 0x0FFF 保留）

事件产生（非屏蔽）：

当 Write_Automatic_刷新时间命令完成时，命令完成事件产生。

4.7.33 Read_Num_Broadcast_Retransmissions

表 11.263

命令	OCF	命令参数	返回参数
HCI_Read_Num_ Broadcast_Retrans mission	0x0029		Status, Num_Broadcast_R etran

说明：

该命令读出作为广播重传次数设备的参数值。广播分组不需确认且不可靠，广播重传次数参数通过多次重传广播消息来提高广播消息的可靠性。该参数定义了设备重传广播数据分组的次数，同时该参数随链接质量测量变化而被调整。

命令参数： 无。

返回参数：

Status: 1 字节

表 11.264

值	参数说明
0x00	Read_Num_Broadcast_Retransmissions 命令成功。
0x01-0xFF	Read_Num_Broadcast_Retransmissions 命令失败。

Num_Broadcast_Retran: 1 字节

表 11.265

值	参数说明
N = 0xXX	广播重发次数 = N 范围：0x00-0xFF

事件产生(非屏蔽)：

当 Read_Num_Broadcast_Retransmission 命令完成时，命令完成事件产生。

4.7.34 Write_Num_Broadcast_Retransmissions

表 11.266

命令	OCF	命令参数	返回参数
HCI_Write_Num_Bro adcast_ Retransmissions	0x002A	Num_Broadcast_Retran	Status

说明：

该命令写入作为广播重传次数设备的参数值。广播分组不需确认且不可靠，广播重传次

数参数通过多次重传广播消息来提高广播消息的可靠性。该参数定义了设备重传广播数据分组的次数，同时该参数随链接质量测量变化而被调整。

命令参数：

Num_Broadcast_Retran: 1 字节

表 11.267

值	参数说明
N = 0xXX	广播重发次数 = N 范围： 0x00 – 0xFF 默认: N = 0x01

返回参数：

Status: 1 字节

表 11.268

值	参数说明
0x00	Write_Num_Broadcast_Retransmissions 命令成功。
0x01-0xFF	Write_Num_Broadcast_Retransmissions 命令失败。

事件产生(非屏蔽)：

当 Write_Num_Broadcast_Retransmissions 命令完成时，命令完成事件产生。

4.7.35 Read_Hold_Mode_Activity

表 11.269

命令	OCF	命令参数	返回参数
HCI_Read_Hold_Mode_Activity	0x002B		Status, Hold_Mode_Activity

说明：

该命令读出 Hold_Mode_Activity 参数值。当设备处于保持模式时，Hold_Mode_Activity 值用于确定活动是否挂起。在保持时期终止后，设备返回原操作模式。通过执行不同活动类型的按位“OR”操作，多保持模式活动可由 Hold_Mode_Activity 参数指定。

如果没有活动被挂起，则在保持模式期间，所有当前设置的定期查询、查询扫描和呼叫扫描仍然有效。如果 Hold_Mode_Activity 参数设置成挂起呼叫扫描、挂起查询扫描和挂起定期查询，则在保持模式期间，设备可进入低功耗状态，同时所有活动都被挂起。通过执行不同活动类型的按位“OR”操作，多挂起模式活动可由 Hold_Mode_Activity 参数指定。如果整个联机处于保持模式，只有保持模式活动是有效的。

命令参数： 无。

返回参数：

Status: 1 字节

表 11.270

值	参数说明
0x00	Read_Hold_Mode_Activity 命令成功。
0x01	Read_Hold_Mode_Activity 命令失败。

Hold_Mode_Activity: 1 字节

表 11.271

值	参数说明
0x00	维持当前功率状态。
0x01	挂起呼叫扫描。
0x02	挂起查询扫描。
0x04	挂起定期查询。
0x08-0xFF	保留。

事件产生(非屏蔽)：

当 Read_Hold_Mode_Activity 命令完成时，命令完成事件产生

4.7.36 Write_Hold_Mode_Activity

表 11.272

命令	OCF	命令参数	返回参数
HCI_Write_Hold_Mode_Activity	0x002C	Hold_Mode_Activity	Status

说明：

该命令写入 Hold_Mode_Activity 参数值。当设备处于保持模式时，Hold_Mode_Activity 值用于确定活动是否挂起。在保持时期终止后，设备返回原操作模式。通过执行不同活动类型的按位“OR”操作，多保持模式活动可由 Hold_Mode_Activity 参数指定。

如果没有活动被挂起，则在保持模式期间，所有当前设置的定期查询、查询扫描和呼叫扫描仍然有效。如果 Hold_Mode_Activity 参数设置成挂起呼叫扫描、挂起查询扫描和挂起定期查询，则在保持模式期间，设备可进入低功耗状态，同时所有活动都被挂起。通过执行不同活动类型的按位“OR”操作，多挂起模式活动可由 Hold_Mode_Activity 参数指定。如果整个联机处于保持模式，只有保持模式活动是有效的。

命令参数：

Hold_Mode_Activity: 1 字节

表 11.273

值	参数说明
0x00	维持当前功率状态，**默认**。
0x01	挂起呼叫扫描。
0x02	挂起查询扫描。
0x04	挂起定期查询。
0x08-0xFF	保留。

返回参数：

Status: 1 字节

表 11.274

值	参数说明
0x00	Write_Hold_Mode_Activity 命令成功。
0x01	Write_Hold_Mode_Activity 命令失败。

事件产生(非屏蔽)：

当 Write_Hold_Mode_Activity 命令完成时，命令完成事件产生。

4.7.37 Read_Transmit_Power_Level

表 11.275

命令	OCF	命令参数	返回参数
HCI_Read_Transmit_Power_Level	0x002D	Connection_handle Type	Status, Connection_Handle , Transmit_Power_Level

说明：

该命令对于指定的联机句柄读出 Transmit_Power_Level 参数值。联机句柄必须是 ACL 方式的联机句柄。

命令参数：

Connection_handle: 2 字节(12 位有意义)

表 11.276

值	参数说明
0xXXXX	指定读出哪种联机句柄的功率电平设置。 范围: 0x0000-0x0EFF (0x0F00 - 0x0FFF 保留)

Type: 1 字节

表 11.277

值	参数说明
0x00	读当前传输功率电平。
0x01	读最大传输功率电平。
0x02-0xFF	保留

返回参数

Status: 1 字节

表 11.278

值	参数说明
0x00	Read_Transmit_Power_Level 命令成功
0x01-0xFF	Read_Transmit_Power_Level 命令失败

Connection_handle: 2 字节(12 位有意义)

表 11.279

值	参数说明
0xXXXX	指定返回哪个联机句柄传输的功率电平设置。 范围: 0x0000-0x0EFF (0x0F00 - 0x0FFF 保留)

Transmit_Power_Level 1 字节

表 11.280

值	参数说明

N=0xXX	长度：1 字节（带符号整数） 范围：-30 ≤ N ≤ 20 单位：dBm

事件产生(非屏蔽)：

当 Read_Transmit_Power_Level 命令完成时，命令完成事件产生。

4.7.38 Read_SCO_Flow_Control_Enable

表 11.281

命令	OCF	命令参数	返回参数
HCI_Read_SCO_Flow_Control_Enable	0x002E		Status, SCO_Flow_Control_Enable

说明：

Read_SCO_Flow_Control_Enable 命令提供读出 SCO_Flow_Control _Enable 设置的能力。通过使用该设置，主机能决定对于 SCO 联机句柄，是否主控制器将送出完成分组事件数。该设置能允许主机启动及禁止 SCO 流控制。

注意：如果不存在联机情况，只能改变 SCO_Flow_Control_Enable 设置。

命令参数： 无。

返回参数：

Status: 1 字节

表 11.282

值	参数说明
0x00	Read_SCO_Flow_Control_Enable 命令成功。
0x01-0xFF	Read_SCO_Flow_Control_Enable 命令失败。

SCO_Flow_Control_Enable: 1 字节

表 11.283

值	参数说明
0x00	禁止 SCO 流控制。对于 SCO 联机句柄，主控制器里无完成分组事件数送出。
0x01	允许 SCO 流控制。对于 SCO 联机句柄，主控制器里有完成分组事件数送出。

事件产生(非屏蔽)：

当 Read_SCO_Flow_Control_Enable 命令完成时，命令完成事件产生。

4.7.39 Write_SCO_Flow_Control_Enable

表 11.284

命令	OCF	命令参数	返回参数
HCI_Write_SCO_Flow_Control_Enable	0x002F	SCO_Flow_Control_Enable	Status

说明：

Write_SCO_Flow_Control_Enable 命令提供写入 SCO_Flow_Control _Enable 设置的能力。通过使用该设置，主机能决定对于 SCO 联机句柄，是否主控制器将送出完成分组事件数。该设置能允许主机启动及禁止 SCO 流控制。

注意：如果不存在联机情况，只能改变 SCO_Flow_Control_Enable 设置。

命令参数：

SCO_Flow_Control_Enable: 1 字节

表 11.285

值	参数说明
0x00	禁止 SCO 流控制。对于 SCO 联机句柄，主控制器里无完成分组事件数送出，默认。
0x01	允许 SCO 流控制。对于 SCO 联机句柄，主控制器里有完成分组事件数送出。

返回参数：

Status: 1 字节

表 11.286

值	参数说明
0x00	Write_SCO_Flow_Control_Enable 命令成功。
0x01	Write_SCO_Flow_Control_Enable 命令失败。

事件产生(非屏蔽)：

当 Write_SCO_Flow_Control_Enable 命令完成时，命令完成事件产生。

4.7.40 Set_host_Controller_To_host_Flow_Control

表 11.287

命令	OCF	命令参数	返回参数
HCI_Set_host_Controller_To_host_Flow_Control	0x0031	Flow_Control_Enable	Status

说明：

该命令用在主机在主控制器到主机方向打开或关闭流控制。如果流控制关闭，主机就不发送 Host_Number_Of_Completed_Packed 命令。如果该命令已由主机发送且流控制是关闭的，则该命令通过主控制器忽略。

命令参数：

Flow_Control_Enable: 1 字节

表 11.288

值	参数说明
0x00	从主控制器到主机方向关闭流控制，**默认**。
0x01	从主控制器到主机方向开启流控制。
0x02-0xFF	保留

返回参数：

Status: 1 字节

表 11.289

值	参数说明
0x00	Set_host_Controller_To_host_Flow_Control 命令成功。
0x01	Set_host_Controller_To_host_Flow_Control 命令失败。

事件产生(非屏蔽)：

当 Set_host_Controller_To_host_Flow_Control 命令完成时，命令完成事件产生。

4.7.41 Host_Buffer_Size

表 11.290

命令	OCF	命令参数	返回参数
HCI_host_Buffer_Size	0x0033	host_ACL_Data_Packet_Length，host_SCO_Data_Packet_Length，host_Total_Num_ACL_Data_Packets，host_Total_Num_SCO_Data_Packets	Status

说明：

Host_Buffer_Size 命令用于主机通知主控制器，有关从主控制器到主机 HCI ACL 和 SCO 数据分组发送的数据部分的最大长度。根据长度规定，主控制器将分段传输这些数据，所以 HCI 数据分组包含最大使用长度。Host_Buffer_Size 命令也通知主控制器，能够存放在主机数据缓冲区的 HCL ACI 和 SCO 数据分组的总数。

如果从主控制器到主机的控制被关闭，而且 Host_Buffer_Size 命令还没通过主机发布，这意味着，主控制器可随意的使用任何长度发送 HCI 数据分组到主机，同时可假设数据缓冲区是无限的。

如果从主控制器到主机的流控制是打开的，则 Host_Buffer_Size 命令必须在电源打开或复位后，通过主机在第一次 Host_Number_Of _ComplCompleted_Packed 命令发送前发送。（Set_Host_Controller_To_Host_Flow_Control 命令用来打开或关闭流控制）Host_ACL_Data_Packet_Length 命令参数用来确定包含在 ACL 数据分组内的 L2CAP 段的长度，该分组从主控制器传送主机。Host_SCO_Data_Packet_Length 命令参数用来确定 HCI SCO 数据分组的最大容量。主机和主控制器双方都必须支持该命令和事件分组，此处在分组里的数据部分（含头）长度是 255 个字节。

Host_Total_Num_ACL_Data_Packets 命令参数包含有可存储在主机数据缓冲区里的 HCI ACL 数据分组 的总数。主控制器可确定在不同联机句柄间缓冲区如何划分问题。

Host_Num_SCO_Data_Packets 命令参数给出 HCI SCO 数据分组的同样信息。

注意：Host_ACL_Data_Packet_Length 和 Host_SCO_Data _Packet_Length 命令参数不包括 HCI 数据分组头的长度。

命令参数：

Host_ACL_Data_Packet_Length: 2 字节

表 11.291

值	参数说明
0xXXXX	主机能接受的各个 HCI ACL 数据分组的数据部分最大长度（在字节里）。

Host_SCO_Data_Packet_Length: 1 字节

表 11.292

值	参数说明
0xXX	主机能接受的各个 HCI SCO 数据分组的数据部分最大长度（在字节里）。

Host_Total_Num_ACL_Data_Packets: 2 字节

表 11.293

值	参数说明
0xXXXX	能存储在主机数据缓冲区的 HCI ACL 数据分组总数。

Host_Total_Num_SCO_Data_Packets: 2 字节

表 11.294

值	参数说明
0xXXXX	能存储在主机数据缓冲区的 HCI SCO 数据分组总数。

返回参数：

Status: 1 字节

表 11.295

值	参数说明
0x00	host_Buffer_Size 命令成功。
0x01	host_Buffer_Size 命令失败。

事件产生(非屏蔽)：

当 host_Buffer_Size 命令完成时，命令完成事件产生。

4.7.42 Host_Number_Of_Completed_Packets

表 11.296

命令	OCF	命令参数	返回参数
HCI_host_Number_Of_Completed_P	0x0035	Number_Of_Handles , Connection_handle, Host_Num_Of_Completed	

ackets		_Packets	

说明：

由于先前 Host_Number_Of_Completed_Buffers 命令参数已送到主控制器，所以该命令（Host_Number_Of_Completed_Packets）用于由主机指出主控制器完成每次联机句柄的 HCI 数据分组数。这意指在主机里的相应缓冲区空间已释放。

基于 Host_Buffer_Size 命令的该信息，Host_Total_Num_Data_ _Packets 及 Host_Total_Num_SCO_Data_Packets 命令参数，主控制器可以确定紧随 HCI 数据分组的哪个联机句柄将送往主机。如果从主控制器到主机方向的流控制是打开的，而且至少有一个联机句柄，或主控制器处于本地回送模式，则该命令由主机发布。否则，该命令由主控制器忽略。

当主机在自己的缓冲区中具有 HCI 数据分组时，它必须定期持续的发送 Host_Number_Of_Completed_Packets 命令到主控制器，直到最终报告在主机里的所有缓冲空间通过 ACL 数据分组已释放。使用该命令的频率由生产厂商指定。

（Set_Host_Controller_To_Host_Flow_Control 命令参数用于打开或关闭流控制）。如果从主控制器到主机方向的流控制是打开的，则在 Host_Buffer_Size 命令总是在打开电源和复位后在第一个 Host_Number_
Of_Completed_Packets 命令发送前由主机发送。

注意：Host_Number_Of_Completed_Packets 命令是一个特定命令，它意指在命令已完成后，一般无事件产生。当至少有一个联机，或主控制器是处于独立于其它的命令本地回送模式，则该命令通过主机可在任何时候发送。

通常命令流控制都不用作 Host_Number_Of_Completed_Packets 命令。

命令参数：

Number_Of_Handles: 1 字节

表 11.297

值	参数说明
0xXX	联机句柄数及包含在该命令里的 Host_Number_Of_Completed_Packets 参数对。 范围：0 – 255

Connection: Number_Of_Handles * 2 字节(12 位有意义)

表 11.298

值	参数说明
0xXXXX	联机句柄 范围：0x0000 – 0x0EFF （ 0x0F00 – 0x0FFF 保留）

Host_Num_Of_Completed_Packets： Number_Of_Handles * 2 字节

表 11.299

值	参数说明
N=0xXXXX	由于前次事件已返回，与联机句柄有关的 HCI 数据分组的数已完成。 N 的范围：0x0000 – 0xFFFF

返回参数： 无。

事件产生（非屏蔽）：

通常，在 Host_Number_Of_Completed_ Packets 命令完成后无事件产生。然而，如果 Host_Number_Of_ Completed_Packets 命令包含一个以上无效参数，则主机用失败状态返回一个命令完成事件，并指出无效 HCI 命令参数的错误代码。

当至少有一个联机或主控制器处于本地回送模式时，主机可在任何时候发送 Host_Number_Of_Completed_Packets 命令。通常命令流控制不作为该命令。

4.7.43 Read_Link_Supervision_Timeout

表 11.300

命令	OCF	命令参数	返回参数
Hci_ Read_Link_S upervision_ Timeout	0x0036	Connection_handle	Status Connection_handle Link_Supervision_Ti meout

说明：

该命令为设备读出 Link_Supervision_Timeout 参数值。

Link_Supervision_Timeout 参数由主单元或从单元蓝牙设备用来监视链接损失。无论如何，若从联机句柄无基带分组收到的持续期大于 Link_Supervision_Timeout，则联机断开。对于由联机句柄指定的设备，SCO 和 SCL 联机方式都使用同样的超时值。

注意：用于该命令的联机句柄必须是 ACL 联机方式的适当设备。该命令针对为该设备其它的 SCO 联机句柄设置 Link_Supervision_Timeout 值。

注意：通过设置 Link_Supervision_Timeout 为 No Link_Supervi- sion_Timeout (0x0000)将禁止对指定的联机句柄 Link_Supervision _Timeout 校验。这就没有必要每约 40 秒就要使匹克网的主单元解除休眠及休眠每个蓝牙设备。

通过使用 No Link_Supervision_Timeout 设置，休眠模式的可伸缩性是无限制的。

命令参数：

Connection_Gandle: 2 字节(12 位有意义)

表 11.301

值	参数说明
0xXXXX	指定读出哪个联机句柄的链接监督超时值。 范围: 0x0000 - 0x0EFF （ 0x0F00 - 0x0FFF 保留）

返回参数：

Status: 2 字节

表 11.302

值	参数说明
0x00	Read_Link_Supervision_Timeout 命令成功。
0x01	Read_Link_Supervision_Timeout 命令失败。

Status:1 字节

表 11.303

值	参数说明

0xXXXX	指定读出哪个联机句柄的链接监督超时值。 范围：0x0000 – 0x0EFF （ 0x0F00 – 0x0FFF 保留）

Link_Supervision_timeout: 2 字节

表 11.304

值	参数说明
0x0000	无 Link_Supervision_Timeout 。
N=0xXXXX	测量基带时隙数 link_supervision_timeout = N * 0.625ms N 的范围：0x0001 – 0xFFFF 时间范围：0.625ms – 40.9s

事件产生(非屏蔽)：

当 Read_Link_Supervision_Timeout 命令完成时，命令完成事件产生。

4.7.44 write_Link_Supervision_Timeout

表 11.305

命令	OCF	命令参数	返回参数
HCI_Write_Link_Supervision_Timeout	0x0037	Connection_Handle Link_Supervision_Timeout	Status Connection handle

说明：

该命令为设备写入 Link_Supervision_Timeout 参数值。

Link_Supervision_Timeout 参数由主单元或从单元蓝牙设备用来监视链接损失。无论如何，若从联机句柄无基带分组收到的持续期大于 Link_Supervision_Timeout，则联机断开。对于由联机句柄指定的设备，SCO 和 SCL 联机方式都使用同样的超时值。

注意：用于该命令的联机句柄必须是 ACL 联机方式的适当设备。该命令针对为该设备其它的 SCO 联机句柄设置 Link_Supervision_Timeout 值。

注意：通过设置 Link_Supervision_Timeout 为 No Link_Supervision_Timeout (0x0000)将禁止对指定的联机句柄 Link_Supervision_Timeout 校验。这就没有必要每约 40 秒就要使匹克网的主单元解除休眠及休眠每个蓝牙设备。

通过使用 No Link_Supervision_Timeout 设置，休眠模式的可伸缩性是无限制的。

命令参数：

Connection_Handle: 2 字节(12 位有意义)

表 11.306

值	参数说明
0xXXXX	指定写入哪个联机句柄的链接监督超时值。

	范围: 0x0000 - 0x0EFF (0x0F00 - 0x0FFF 保留)

Link_Supervision_Timeout: 2 字节

表 11.307

值	参数说明
0x0000	无 Link_Supervision_Timeout 。
N=0xXXXX	测量基带时隙数 link_supervision_timeout = N * 0.625ms N 的范围: 0x0001 - 0xFFFF 时间范围: 0.625ms - 40.9s 默认: N = 0x7D00 link_supervision_timeout = 20s

返回参数:

Status: 1 字节

表 11.308

值	参数说明
0x00	Write_Link_Supervision_Timeout 命令成功。
0x01	Write_Link_Supervision_Timeout 命令失败。

Connection_handle: 2 字节(12 位有意义)

表 11.309

值	参数说明
0xXXXX	指定写入哪个联机句柄的链接监督超时值。 范围: 0x0000 - 0x0EFF (0x0F00 - 0x0FFF 保留)

事件产生 (非屏蔽):

当 Write_Link_Supervision_Timeout 命令完成时，命令完成事件产生。

4.7.45 Read_Number_Of_Supported_IAC

表 11.310

命令	OCF	命令参数	返回参数
HCI_Read_Number_Of_Supported_IAC	0x0038		Status Num_support_IAC

说明:

该命令读出本地蓝牙设备在查询期间能同时监听的查询识别码数(IAC)的值。所有的蓝牙设备要求至少支持一种 IAC，(GIAC 或 UIAC)，但是有些蓝牙设备支持附加的 IACs 。

命令参数: 无

返回参数:

Status: 1 字节

表 11.311

值	参数说明
0x00	Read_Number_Of_Supported_IAC 命令成功。
0x01	Read_Number_Of_Supported_IAC 命令失败。

Num_Support_IAC: 1 字节

表 11.312

值	参数说明
0xXX	指定本地蓝牙设备在查询期间可同时监听支持的 ICA 量。 范围: 0x01 – 0x40

事件产生(非屏蔽):

当 Read_Number_Of_Supported_IAC 命令完成时，命令完成事件产生。

4.7.46 Read_Current_IAC_LAP

表 11.313

命令	OCF	命令参数	返回参数
HCI_Read_Current_IAC_LAP	0x0039		Status Num_current_IAC, IAC_lap

说明:

该命令读出用于创建查询期间本地蓝牙设备能同时扫描的查询识别码的 LAP（s)。所有的蓝牙设备要求至少支持一种 IAC，(GIAC 或 UIAC)，但有些蓝牙设备支持附加的 IACs 。

命令参数: 无。

返回参数:

Status: 1 字节

表 11.314

值	参数说明
0x00	Read_Current_IAC_LAP 命令成功。
0x01	Read_Current_IAC_LAP 命令失败。

Num_Current_IAC: 1 字节

表 11.315

值	参数说明
0xXX	指定查询期间通过本地蓝牙设备当前使用的 IACs 的数。 范围: 0x01 – 0x40

IAC_LAP: 3 字节 * Num_Current_IAC

表 11.316

值	参数说明
0xXXXXXX	用于创建 IAC 的 LAPs，IAC 为在查询期间当前用于本地蓝牙设备同时监听的参数。 范围: 0x9E8B00 – 0x9E8B3F

事件产生 (非屏蔽):

当 Read_Current_IAC_LAP 命令完成时，命令完成事件产生。

4.7.47 Write_Current_IAC_LAP

表 11.317

命令	OCF	命令参数	返回参数
HCI_Write_Current_IAC_LAP	0x003A	Num_Current_IAC, IAC_LAP	Status

说明：

该命令写入用于创建查询期间本地蓝牙设备能同时扫描的查询识别码的 LAP（S）。所有的蓝牙设备要求至少支持一种 IAC，（ GIAC 或 UIAC ），但有些蓝牙设备支持附加的 IACs 。因此，用于创建 GIAC 或 UIAC 的 LAP 必须是在该命令的 IAC_LAP 中。

注意：该命令通过蓝牙设备使用改写了当前的 IACs。如果 Num_Current_IAC 的值大于支持 IACs 的数，仅为“1”，X 查询识别码（ X 等于支持 IACs 的数）以无任何错误的形式被存储。

命令参数：

Num_Current_IAC 1 字节

表 11.318

值	参数说明
0xXX	指定查询期间通过本地蓝牙设备当前使用的 IACs 的数。 范围：0x01 – 0x40

IAC_LAP: 3 字节 * Num_Current_IAC

表 11.319

值	参数说明
0xXXXXXX	用于创建 IAC 的 LAPs，IAC 为在查询期间当前用于本地蓝牙设备同时监听的参数。 范围：0x9E8B00 – 0x9E8B3F GIAC 是使用的默认 IAC。如果支持附加的 IACs，附加默认 IAC 由生产厂商确定。

返回参数

表 11.320

值	参数说明
0x00	Write_Current_IAC_LAP 命令成功。
0x01	Write_Current_IAC_LAP 命令失败。

事件产生(非屏蔽)：

当 Write_Current_IAC_LAP 命令完成时，命令完成事件产生。

4.7.48 Read_Page_Scan_Period_Mode

表 11.321

命令	OCF	命令参数	返回参数

HCI_Read_Page _Scan_Period_Mode	0x003B		Status, Page_Scan_ Period_Mode

说明：

该命令用来读出本地蓝牙设备的强制 Page_Scan_Period_Mode。每次查询响应消息发送时，蓝牙设备启动定时器(T_mandatory_pscan)，该定时器的值取决于 Page_Scan_Period _Mode。

只要该定时器没终止，蓝牙设备将使用所有后面呼叫扫描的 Page_Scan_Period_Mode。

注意：在每次新的查询响应时，定时器 T_mandatory_pscan 将被复位。

在传输一个或多个查询响应（FHS）分组作为查询扫描过程时，本地蓝牙设备使用强制呼叫扫描模式，而不管 scan_Enable 参数的设置，允许进入呼叫扫描状态。

命令参数：无。

返回参数：

Status: 1 字节

表 11.323

值	参数说明
0x00	Read_Page_Scan_Period_Mode 命令成功。
0x01	Read_Page_Scan_Period_Mode 命令失败。

Page_Scan_Period_Mode: 1 字节

表 11.324

值	参数说明
0x00	P0
0x01	P1
0x02	P2
0x03-0xFF	保留

事件产生（非屏蔽）：

当 Read_Page_Scan_Period_Mode 命令完成时，命令完成事件产生?

4.7.49 Write_Page_Scan_Period_Mode

表 11.325

命令	OCF	命令参数	返回参数
HCI_Write_Page_ Scan_Period_Mode	0x003C	Page_Scan _Period_Mode	Status

说明：

该命令用来写入本地蓝牙设备的强制 Page_Scan_Period_Mode。每次查询响应消息发送时，蓝牙设备启动定时器(T_mandatory_pscan)，该定时器的值取决于 Page_Scan_Period _Mode。

只要该定时器没终止，蓝牙设备将使用所有后面呼叫扫描的 Page_Scan_Period_Mode。

注意：在每次新的查询响应时，定时器 T_mandatory_pscan 将被复位。

在传输一个或多个查询响应（FHS）分组作为查询扫描过程时，本地蓝牙设备使用强制呼叫扫描模式，而不管 scan_Enable 参数的设置，允许进入呼叫扫描状态。

命令参数：

Page_Scan_Period_Mode: 1 字节

表 11.326

值	参数说明
0x00	P0
0x01	P1
0x02	P2
0x03-0xFF	保留

返回参数：

Status: 1 字节

表 11.327

值	参数说明
0x00	Write_Page_Scan_Period_Mode 命令成功。
0x01	Write_Page_Scan_Period_Mode 命令失败。

事件产生(非屏蔽)：

当 Write_Page_Scan_Period_Mode 命令完成时，命令完成事件产生。

4.7.50 Read_Page_Scan_Mode

表 11.328

命令	OCF	命令参数	返回参数
HCI_Read_Page_Scan_Mode	0x003D		Status Page-Scan-Mode

说明：

该命令用来读出本地蓝牙设备的默认呼叫扫描模式。Page_Scan_Mode 参数指出用于默认呼叫扫描的呼叫扫描模式。当前定义了一个强制呼叫扫描模式和 3 个选择呼叫扫描模式。如果基带定时器 T_mandatory_pscan 没终止，随后的查询响应必须使用强制呼叫扫描模式。

命令参数： 无。

返回参数：

Status: 1 字节

表 11.329

值	参数说明
0x00	Read_Page_Scan_Mode 命令成功。

0x01	Read_Page_Scan_Mode 命令失败。

Page_Scan_Mode: 1 字节

表 11.330

值	参数说明
0x00	强制呼叫扫描模式
0x01	选择扫描模式 I
0x02	选择扫描模式 II
0x03	选择扫描模式 III
0x04-0xFF	保留

事件产生(非屏蔽)：

当 Read_Page_Scan_Mode 命令完成时，命令完成事件产生。

4.7.51 Write_Page_Scan_Mode

表 11.331

命令	OCF	命令参数	返回参数
HCI_Write_Page_Scan_Mode	0x003E	Page_Scan_Mode	Status

说明：

该命令用来写入本地蓝牙设备的默认呼叫扫描模式。Page_Scan_Mode 参数指出用于默认呼叫扫描的呼叫扫描模式。当前定义了一个强制呼叫扫描模式和 3 个选择呼叫扫描模式。如果基带定时器 T_mandatory_pscan 没终止，随后的查询响应必须使用强制呼叫扫描模式。

命令参数：

Page_Scan_Mode: 1 字节

表 11.332

值	参数说明
0x00	强制呼叫扫描模式，**默认**。
0x01	选择呼叫扫描模式 I
0x02	选择呼叫扫描模式 II
0x03	选择呼叫扫描模式 III
0x04-0xFF	保留

返回参数：

Status: 1 字节

表 11.333

值	参数说明
0x00	Write_Page_Scan_Mode 命令成功。
0x01	Write_Page_Scan_Mode 命令失败。

事件产生(非屏蔽)：

当 Write_Page_Scan_Mode 命令完成时，命令完成事件产生。

4.8 信息参数

信息参数由蓝牙硬件制造商固定。这些参数提供有关蓝牙设备的信息和主控制器、链接管理器及基带的能力。主机不能修改这些参数的任何东西。对于信息参数，OGF 定义为 0x04。

表 11.334

命令	命令说明汇总
Read_Local_Version_Information	Read_Local_Version_Information 命令读出本地蓝牙设备的版本信息值。
Read_Local_Supported_Features	Read_Local_Supported_Features 命令申请本地设备支持特征表。
Read_Buffer_Size	Read_Buffer_Size 命令返回HCI缓冲区的容量。通过主控制器这些缓冲区用于传输缓冲数据。
Read_Country_Code	Read_Country_Code 命令读出国家代码状态参数值。国家代码定义了 ISM2.4GHz 波道的那些频段由设备使用。
Read_BD_ADDR	Read_BD_ADDR 读出 BD_ADDR 的参数值。BD_ADDR 是蓝牙设备的一个 48 位唯一标识符。

4.8.1 Read_local_Version_Information

表 11.335

命令	OCF	命令参数	返回参数
HCI_Read_local_Version_information	0x0001		Status, HCI Version, HCI Revision, LMP Version, Manufacurer_Name, LMP Subversion

说明：

该命令读出本地蓝牙设备版本信息值。版本信息由 2 个参数组成：版本和修正参数。

版本参数定义了蓝牙硬件的主要硬件版本。当蓝牙硬件新版本为新的蓝牙 SIG 说明生产时，只有版本参数改变。版本案参数由 SIG 控制。

修订参数由制造商控制，当需要时，可以修改。Manufacturer_Name 参数指出本地蓝牙模型的制造商，并通过 LMP 定义的该参数指定。子版本参数由制造商控制，当需要时可以修改。定义的蓝牙硬件各个版本的各种修正子版本参数，将作为设计进程变化和错误固定而通过。它允许由软件来确定正在使用什么样的蓝牙硬件，如有必要，硬件可在各类故障范围工作。

命令参数：无。

返回参数：

Status: 1 字节

表 11.336

值	参数说明
0x00	Read_local_Version_Information 命令成功。
0x01	Read_local_Version_Information 命令失败

HCI_Version 1 字节

表 11.337

值	参数说明
0xXX	蓝牙硬件的当前 HCI 版本。 蓝牙 HCI 规范 1.0。 0x01 – 0xFF: 保留。

LMP_Version: 1 字节

表 11.338

值	参数说明
0xXX	蓝牙硬件的当前 LMP 版本。

Manufacturer_Name: 2 字节

表 11.339

值	参数说明
0xXXXX	蓝牙硬件制造商名。

LMP_Subversion: 2 字节

表 11.340

值	参数说明
0xXXXX	蓝牙硬件的当前 LMP 子版本。

事件产生(非屏蔽)：

当 Read_local_Version_Information 命令完成时，命令完成事件产生。

4.8.2 Read_local_Supported_Features

表 11.341

命令	OCF	命令参数	返回参数
HCI_Read_local_Supported_Features	0x0003		Status, LMP_feature

说明：

该命令为本地设备申请支持特征表。该命令返回 LMP 特征表。

命令参数： 无。

返回参数：

Status: 1 字节

表 11.342

值	参数说明
0x00	Read_local_Supported_Features 命令成功。
0x01	Read_local_Supported_Features 命令失败。

LMP_Features: 8 字节

表 11.343

值	参数说明
0xXXXXXXXX XXXXXXXX	LMP 特征的位屏蔽表

事件产生(非屏蔽)：

当 Read_本地_Supported_Features 命令完成时，命令完成事件产生。

4.8.3 Read_Buffer_Size

表 11.344

命令	OCF	命令参数	返回参数
HCI_Read_Buffer_Size	0x0005		Status, HC_ACL_Data_Packet_Length, HC_SCO_Data_Packet_Length, HC_Total_Num_ACL_Data_Packets, HC_Total_Num_SCO_Data_Packets

说明：

Read_Buffer_Size 命令用来读出从主机到主控制器发送 HCI ACL 和 SCO 数据分组的数据部分最大值。主机根据这些分组大小，分段从主机传输到主控制器，以便 HCI 数据分组包含这类大小的数据。

Read_Buffer_Size 命令也返回能存储在主控制器缓冲区里的 HCI ACI 和 SCO 数据分组的总数。Read_Buffer_Size 命令必须在主机发送任何数据到主控制器前，由主机发布。

HC_ACL_Data_Packet_Length 返回参数用来确定包含在 ACL 数据分组里的 L2CAP 段的大小，从主机传输主控制器的 L2CAP 段通过链接管理器分散进入基带分组。

HC_SCO_Data_Packet_Length 返回参数用来确定 HCI SCO 数据分组最大的容量。主机和主控制器双方都必须支持该命令及事件分组，此时，包含在分组里的数据部分(除头外)是 255 个字节。

HC_Total_Num_ACL_Data_Packets 返回参数包含存储在主控制器数据缓冲区的 HCI ACL 数据分组总数。主机将确定在不同的联机句柄之间缓冲区如何进行划分。如果没有 HCI SCO 数据分组，HC_Total_Num_SCO_ Data_Packet 返回参数给出了相同信息。

注意: HC_ACL_Data_Packet_Length 和 HC_SCO_Data_Packet_Length 返回参数不包括 HCI 的数据分组头的长度。

命令参数： 无。

返回参数：

Status: 1 字节

表 11.345

值	参数说明
0x00	Read_Buffer_Size 命令成功。
0x01	Read_Buffer_Size 命令失败。

HC_ACL_Data_Packet_Length: 2 字节

表 11.346

值	参数说明
0xXXXX	主控制器可接受的各 HCI ACL 数据分组的数据部分最大长度。

HC_SCO_Data_Packet_Length: 1 字节

表 11.347

值	参数说明
0xXX	主控制器可接受的各 HCI SCO 数据分组的数据部分最大长度。

HC_Total_Num_ACL_Data_Packets: 2 字节

表 11.348

值	参数说明
0xXXXX	能存储在主控制器数据缓冲区里的HCI ACL 数据分组总数。

HC_Total_Num_SCO_Data_Packets: 2 字节

表 11.349

值	参数说明
0xXXXX	能存储在主控制器数据缓冲区里的HCI SCO 数据分组总数。

事件产生(非屏蔽):

当 Read_Buffer_Size 命令完成时，命令完成事件产生。

4.8.4 Read_Country_Code

表 11.350

命令	OCF	命令参数	返回参数
HCI_Read_Country_Code	0x0007		Status, Country_Code

说明:

该命令读出 Country_Code 返回参数值。Country_Code 定义 ISM 2.4GHz 波道的哪些频带可被设备使用。各国根据自身的行规调整可使用的 2.4GHz 频率范围。

命令参数: 无。

返回参数:

Status: 1 字节

表 11.351

值	参数说明
0x00	Read_Country_Code 命令成功。
0x01	Read_Country_Code 命令失败。

Country_Code: 1 字节

表 11.352

值	参数说明
0x00	北美洲与欧洲（西班牙、法国除外）
0x01	法国
0x02	西班牙
0x03	日本
0x04-FF	保留

事件产生(非屏蔽)：

当 Read_Country_Code 命令完成时，命令完成事件产生。

4.8.5 Read_BD_ADDR

表 11.353

命令	OCF	命令参数	返回参数
HCI_Read_BD_ADDR	0x0009		Status, BD_ADDR

说明：

该命令读出 BD_ADDR 参数值。BD_ADDR 是 48 位蓝牙设备的唯一标识符。

命令参数： 无。

返回参数：

Status: 1 字节

表 11.354

值	参数说明
0x00	Read_BD_ADDR 命令成功。
0x01	Read_BD_ADDR 命令失败。

BD_ADDR: 6 字节

表 11.355

值	参数说明
0xXXXXXXXXXXXX	设备 BD_ADDR

事件产生(非屏蔽)：

当 Read_BD_ADDR 命令完成时，命令完成事件产生。

4.9 状态参数

主控制器可修改所有状态参数。这些参数提供有关主控制器、链接管理器和基带的当前状态信息。主机不能修改这些参数的任何部分，除复位确实指定的参数。对于状态和基带，OGF 定义为 0x05。

表 11.356

命令	命令说明汇总
Read_Failed_Contact_Counter	Read_Failed_Contact_Counter 读出对于其余设备特殊联机的 Failed_Contact_Counter 参数值。Failed_Contact_Counter 记录在刷新超时终止及当前正在传输的 L2CAP 数据分组被自动刷新后，主单元或从单元不能响应连续事件次数。
Reset_Failed_Contact_Counter	Reset_Failed_Contact_Counter 复位对于其余设备特殊联机的 Failed_Contact_Counter 参数值。Failed_Contact_Counter 记录在刷新超时终止及当前正在传输的 L2CAP 数据分组被自动刷新后，主单元或从单元不能响应连续事件次数。
Get_Link_Quality	Get_Link_Quality 命令读出指定联机句柄的 Link_Quality 的值。
Read_RSSI	Read_RSSI 命令读出对于其它蓝牙设备联机句柄的场强值。

4.9.1 Read_Failed_Contact_Counter

表 11.357

命令	OCF	命令参数	返回参数
HCI_Read_Failed_Contact_Counter	0x0001	Connection_handle	Status Connection_handle Failed_Contact_Counter

说明：

该命令读出其余设备特殊联机的 Failed_Contact_Counter 参数。联机句柄必须 ACL 方式的联机句柄。Failed_Contact_Counter 记录了在刷新超时终止和当前正在传输的 L2CAP 分组被自动刷新后，主单元和从单元没响应的连续事件次数，当该情况出现时，Failed_Contact_Counter 的值增 1。在下列条件里，联机的 Failed_Contact_Counter 复位为“0”。

1．当一个新联机确立时。

2．当 Failed_Contact_Counter 大于“0”和作为联机的 L2CAP 分组被确认。

3．当 Reset_Failed_Contact_Counter 命令发出。

命令参数：

Connection_Handle: 2 字节(12 位有意义)

表 11.358

值	参数说明
0xXXXX	读出哪个 Failed_Contact_Counter 联机的联机句柄。 范围: 0x0000 - 0x0EFF (0x0F00 - 0x0FFF 保留)

返回参数：

Status: 1 字节

表 11.359

值	参数说明
0x00	Read_Failed_Contact_Counter 命令成功。
0x01	Read_Failed_Contact_Counter 命令失败。

Connection_Handle: 2 字节(12 位有意义)

表 11.360

值	参数说明
0xXXXX	已读出哪个 Failed_Contact_Counter 联机的联机句柄。 范围: 0x0000 - 0x0EFF (0x0F00 - 0x0FFF 保留)

Failed_Contact_Counter: 2 字节

表 11.361

值	参数说明
0xXXXX	相应联机句柄的联机连续失败的次数。

事件产生(非屏蔽):

当 Read_Failed_Contact_Counter 命令完成时，命令完成事件产生。

4.9.2 Reset_Failed_Contact_Counter

表 11.362

命令	OCF	命令参数	返回参数
HCI_Reset_Failed_Contact_Counter	0x0002	Connection_Handle,	Connection_Handle, Status

说明:

该命令复位其余设备特殊联机的 Failed_Contact_Counter 参数。联机句柄必须 ACL 方式的联机句柄。Failed_Contact_Counter 记录了在刷新超时终止和当前正在传输的 L2CAP 分组被自动刷新后，主单元和从单元没响应的连续事件次数，当该情况出现时，Failed_Contact_Counter 的值增 1。在下列条件里，联机的 Failed_Contact_Counter 复位为“0”。

1 .当一个新联机确立时。

2 .当 Failed_Contact_Counter 大于“0”和作为联机的 L2CAP 分组被确认。

3 .当 Reset_Failed_Contact_Counter 命令发出。

命令参数:

Connection_handle: 2 字节(12 位有意义)

表 11.363

值	参数说明
0xXXXX	复位哪个 Failed_Contact_Counter 联机的联机句柄。 范围: 0x0000 - 0x0EFF (0x0F00 - 0x0FFF 保留)

返回参数:

Status: 1 字节

表 11.364

值	参数说明
0x00	Reset_Failed_Contact_Counter 命令成功。
0x01	Reset_Failed_Contact_Counter 命令失败。

Connection_Handle: 2 字节(12 位有意义)

表 11.365

值	参数说明
0xXXXX	已复位哪个 Failed_Contact_Counter 联机的联机句柄。 范围: 0x0000-0x0EFF (0x0F00 - 0x0FFF 保留)

事件产生 (非屏蔽):

当 Reset_Failed_Contact_Counter 命令完成时，命令完成事件产生。

4.9.3 Get_Link_Quality

表 11.366

命令	OCF	命令参数	返回参数
HCI_Get_Link_Quality	0x0003	Connection_Handle	Status, Connection_Handle, Link_Quality

说明:

该命令返回指定联机句柄的 Link_Quality 值。联机句柄必须是 ACL 联机方式的联机句柄。该命令将返回在两个蓝牙设备之间表示的链接质量的从 0 ∽ 255 的 Link_Quality 值。该值越高，链接质量就越好。各蓝牙模型供应商将决定怎样测量链接质量。

命令参数:

Connection_Handle: 2 字节(12 位有意义)

表 11.367

值	参数说明
0xXXXX	读出哪种联机质量参数联机的联机句柄。 范围: 0x0000 - 0x0EFF (0x0F00 - 0x0FFF 保留)

返回参数:

Status: 1 字节

表 11.368

值	参数说明
0x00	Get_Link_Quality 命令成功。
0x01	Get_Link_Quality 命令失败。

Connection_Handle: 2 字节(12 位有意义)

表 11.369

值	参数说明
0xXXXX	已读出哪种联机质量参数联机的联机句柄。 范围: 0x0000 - 0x0EFF (0x0F00 - 0x0FFF 保留)

Link_Quality: 1 字节

表 11.370

值	参数说明
0xXX	在本地设备和通过联机句柄指出的远程设备之间，链接联机的当前质量。 范围：0x00 - 0xFF 值越高，链接质量就越好。

事件产生(非屏蔽)：

当 Get_Link_Quality 命令完成时，命令完成事件产生。

4.9.4 Read_RSSI

表 11.371

命令	OCF	命令参数	返回参数
HCI_Read_RSSI	0x0005	联机句柄	Status, 联机句柄, RSSI

说明：

对于其它蓝牙设备，在测量场强和最佳接收电平区域限制之间，该命令读出的不同值。联机句柄必须是 ACL 联机方式的联机句柄。通过主控制器返回的任何 RSSI 正值指出超过 RSSI 上限的多少 dB, 任何 RSSI 负值指出低于 RSSI 下限的多少 dB。值“0”指出在最佳设备功率区域内的 RSSI。

注意：dB 值精确度取决于蓝牙硬件。对硬件的唯一要求是蓝牙设备能判定 RSSI 是否在最佳接收功率范围内、上限或下限。

命令参数：

Connection_Handle: 2 字节(12 位有意义)

表 11.372

值	参数说明
0xXXXX	读出哪个 RSSI 联机的联机句柄。 范围：0x0000 - 0x0EFF (0x0F00 - 0x0FFF 保留)

返回参数：

Status: 1 字节

表 11.373

值	参数说明
0x00	Read_RSSI 命令成功。
0x01	Read_RSSI 命令失败。

Connection_Handle: 2 字节(12 位有意义)

表 11.374

值	参数说明
0xXXXX	已读出哪个 RSSI 联机的联机句柄。

	范围：0x0000 – 0x0EFF （ 0x0F00 – 0x0FFF 保留）

RSSI： 1 字节

表 11.375

值	参数说明
N = 0xXX	长度：1 字节（带符号整数） 范围：– 128 ≤ N ≤ 127 单位：dB

事件产生(非屏蔽)：

当 Read_RSSI 命令完成时，命令完成事件产生。

4.10 测试指令

测试指令用于提供测试蓝牙硬件不同功能的能力，并为测试提供安排不同条件的能力。对于测试指令，OGF 定义为 0x06。

表 11.376

指令	指令综述
Read_Loopback_Mode	Read_Loopback_Mode 将读取主控制器回送模式的设置值。回送模式设置可以确定信息发送路径。
Write_Loopback_Mode	Write_Loopback_Mode 将写入主控制器回送模式的设置值。回送模式设置可以确定信息发送路径。
Enable_Device_Under_Test_Mode	Enable_Device_Under_Test_Mode 指令允许本地蓝牙模块通过 LMP 测试指令进入测试模式。当主机要求本地设备作为待测试设备，实现蓝牙测试模式文件中规定测试情景时，则发送该指令。

4.10.1 Read_loopback_Mode

表 11.377

指令	OCF	指令参数	返回参数
HCI_Read_loopback_Mode	0x0001		Status Loopback_Mode

说明：

本指令将读取主控制器回送模式参数值。回送模式设置可以确定信息发送路径。在非测试模式操作中，回送模式设置为非测试模式，而其信息路径则由蓝牙规范指定。在本地回送模式中，每一数据分组(ACL 和 SCO)和从主机发送到主控制器的指令分组，也将由主控制器不加任何改变地返回。当蓝牙主控制器进入本地回送模式时,它可以四种连接完成事件应答,其中一种用于 ACL 通道和三种用于 SCO 通道，以便当发送 ACL 和 SCO 数据时，主机能够获取连接句柄。当处于本地回送模式时，主控制器将向主机回送指令和数据。回送指令事件用于主机向主控制器发送回送指令。

在本地回送模式中有一些指令将不会被回送，包括 Reset、Set_Host_Controller_To_host_Flow_Control，Host_Buffer_Size，Host_Number_Of_Completed_Packets，Read_Buffer_Size，Read_loopback_Mode 和 Write_loopback_Mode。指令 Reset 和 Write_loopback_Mode 可用于退出本地回送模式。如

果 Write_loopback_Mode 用于退出本地回送模式,则将向主机发送四种连接断开完成事件,这四种事件对应于进入本地回送模式时发送的连接完成事件。而且,本地回送模式不得允许任何连接。如果存在一个连接,且存在设备进入本地回送模式的尝试，则主控制器将拒绝呼入连接尝试。这将不允许使用其它变量对主控制器传输层进行测试。

如果一设备设置为远程回送模式，它将无线发回所有数据（ACL 和 SCO）。它最大可允许同时保持一条 ACL 连接和三条 SCO 连接。而这与远程设备相同。如果存在不止一条指向远程设备的连接，并且存在设置本地设备为远程回送模式的尝试，而该尝试将被拒绝。参见 697 页图 4.6，其中最右边的设备设置为远程回送模式，最左边设备设置为非测试模式。可以不使用任何其它变量测试蓝牙无线链路。

指令参数： 无。

返回参数：

Status 大小：1 字节

表 11.378

值	参数说明
0x00	Read_loopback_Mode 指令成功
0x01	Read_loopback_Mode 指令失败，参见 260 页表 2 的错误代码

Loopback_Mode: 大小：1 字节

表 11.379

值	参数说明
0x00	未启用回送模式，缺省
0x01	启用本地回送
0x02	启用远程回送
0x03-0xFF	保留

生成事件(如未屏蔽)：

当完成 Read_loopback_Mode 指令时，将生成指令完成事件。

4.10.2 Write_Loopback_Mode

表 11.380

指令	OCF	指令参数	返回参数
HCI_ Write_loopback_Mode	0x0002	Loopback_Mode	Status

说明：

Write_Loopback_Mode 将写入主控制器回送模式的设置值。回送模式设置可以确定信息发送路径。在非测试模式操作中，回送模式设置为非测试模式，而其信息路径则由蓝牙规范指定。在本地回送模式中，每一数据分组(ACL 和 SCO)和从主机发送到主控制器的指令分组，也将由主控制器不加任何改变地返回。

当蓝牙主控制器进入本地回送模式时，它可以四种连接完成事件应答,其中一种用于 ACL 通道和三种用于 SCO 通道，以便当发送 ACL 和 SCO 数据时，主机能够获取连接句柄。当处于本地回送模式时，主控制器将向主机回送指令和数据。回送指令事件用于主机向主控制器发送回送指令。

在本地回送模式中有一些指令将不会被回送，包括 Reset、Set_Host_Controller_To_host_Flow_Control，Host_Buffer_Size，Host_Number_Of_Completed_Packets，Read_Buffer_Size，Read_loopback_Mode 和 Write_loopback_Mode。这些指令可以常规执行方式执行。指令 Reset 和 Write_loopback_Mode 可用于退出本地回送模式。

如果 Write_loopback_Mode 用于退出本地回送模式,则可向主机发送四种连接断开完成事件，以对应于进入本地回送模式时的连接完成事件。而且,本地回送模式不得允许任何连接。如果存在一个连接,且存在设备进入本地回送模式的尝试，则主控制器将拒绝呼入连接尝试。这将允许不使用其它变量对主控制器传输层进行测试。

如果一设备设置为远程回送模式，它将无线发回所有数据（ACL 和 SCO）。它也最大可允许同时保持一条 ACL 连接和三条 SCO 连接。而这与远程设备相同。如果存在不止一条指向远程设备的连接，并且存在设置本地设备为远程回送模式的尝试，而该尝试将被拒绝。参见 697 页图 4.8，其中最右边的设备设置为远程回送模式，最左边设备设置为非测试模式。可以不使用任何其它变量测试蓝牙无线链路。

指令参数：

Loopback_Mode: 容量：1 字节

表 11.381

值	参数说明
0x00	未启用回送模式
0x01	启用本地回送
0x02	启用远程回送
0x03-0xFF	保留

返回参数：

Status: 大小：1 字节

表 11.382

值	参数说明
0x00	Write_loopback_Mode 指令成功
0x01	Write_loopback_Mode 指令失败

生成事件(如未屏蔽)：

当完成 Write_loopback_Mode 指令时，将生成指令完成事件。

4.10.3 Enable_Device_Under_Test_Mode

表 11.383

指令	OCF	指令参数	返回参数
HCI_Enable_Device_Under_ Test_Mode	0x0003		Status

说明：

Enable_Device_Under_Test_Mode 指令将允许本地蓝牙模块通过 LMP 测试指令进入测试模式。细节参见 185 页“链路管理器协议”。当主机要求本地设备成为 DUT，并进入蓝牙测试模式中的测试情景时，主机将发送该指令。当主控制器收到该指令时，它将通过指令完成事件完成该指令。主控制器将正常操作，直至远程测试装置发出 LMP 测试指令将本地设备进入

测试模式。为了终止并退出测试模式，主机将发送 HCI_Reset 指令。该指令将阻止远端蓝牙设备不先发出该指令就将本地蓝牙设备置为测试模式。

指令参数：无

返回参数：

Status: 大小：1 字节

表 11.384

值	参数说明
0x00	Enter_Device_Under_Test_Mode 指令成功
0x01	Enter_Device_Under_Test_Mode 指令失败

生成事件(如未屏蔽)：

当完成 Enter_Device_Under_Test_Mode 指令时，将生成指令完成事件。

5. 事件

5.1 事件

除以下列出事件以外，事件代码 0xFF 将保留作为厂商调试事件的事件代码，和事件代码 0xFE 保留用于蓝牙标识测试。

表 11.385 支持事件列表

事件	事件总述
查询完成事件	查询完成事件表示查询已完成
查询结果事件	查询结果事件表示在当前查询进程中已有一个或多个蓝牙设备应答
连接完成事件	连接完成事件指示构成连接的两主机已建立一个新的连接。
连接请求事件	连接请求事件用于表示正在建立一个新的呼入连接。
连接断开完成事件	连接断开完成事件当连接中止时发生
认证完成事件	认证完成事件当指定连接认证完成时发生
远程命名请求事件	远程命名请求事件用于表示远程命名请求已完成。Remote_Name 事件参数为一长度可达 248 字节的 UTF-8 编码字符串。
加密改变事件	加密改变事件用于表示对于由 Connection_Handle 事件参数指定连接句柄已完成加密改变
连接链接字改变完成事件	连接链接字改变完成事件用于表示由 Connection_Handle 事件参数指定连接句柄的链接字改变已完成
主单元链接字完成事件	主单元链接字完成事件用于表示蓝牙主单元一方的临时链接字或半永久链接字改变已完成
远端支持特性读取完成事件	远端支持特性读取完成事件用于表示链路管理器进程已完成，该链路管理器包含由Connection_Handle

	事件参数指定远程蓝牙设备支持的特性。
远程版本信息读取完成事件	远程版本信息读取完成事件用于表示链路管理器进程已完成，该链路管理器包含由Connection_Handle事件参数指定远程蓝牙设备的版本信息
QoS 启用完成事件	QoS 启用完成事件用于表示启用 QoS 的链路管理器进程已完成，该过程由 Connection_Handle 事件参数指定远程蓝牙设备完成
指令完成事件	指令完成事件由主控制器用于为每一 HCI 指令传递指令返回状态和其它事件参数
指令状态事件	指令状态事件用于表示已收到 Command_Opcode 参数所描述指令，且主控制器正在执行该指令任务
硬件故障事件	该事件用于表示蓝牙设备硬件故障类别
刷新事件	该事件用于表示对于指定连接句柄，要传输的当前用户数据已删除
角色改变事件	角色改变事件用于表示与特定连接相关的当前蓝牙角色已改变
完成分组数事件	完成分组数事件由主控制器用于通知主机自前一完成分组数事件发送后，对于每一连接句柄已完成了多少 HCI 数据分组。
模式改变事件	模式改变事件用于指示与连接句柄相关的设备何时在激活、挂起、呼吸和休眠模式间变化
返回链接字事件	返回链接字事件用于在使用Read_Stored_Link_Key指令后，返回保存的链接字
PIN 码请求事件	PIN 码请求事件用于表示需要一个 PIN 码以创建连接的新链接字
链接字请求事件	链接字请求事件用于表示需要一链接字以建立与 BD_ADDR 指定设备的连接
链接字通知事件	链接字通知事件用于通知主机与 BD_ADDR 指定设备连接的链接字已创建
回送指令事件	回送指令事件用于回送大多数主机发往主控制器的指令
数据缓冲区溢出事件	数据缓冲区溢出事件用于表示由于主机发出分组数超出允许数量，主控制器数据缓冲区已溢出
时隙读取完成事件	时隙读取完成事件用于表示包含时隙信息的 LM 进程已完成
连接分组类型改变事件	连接分组类型改变事件用于表示改变 Connection_Handle 所指定分组类型的链路管理器进程已完成
违反 QoS 事件	违反 QoS 事件用于表示链路管理器不能提供连接句柄的当前 QoS 要求
呼叫扫描模式改变事件	呼叫扫描模式改变事件表示采用指定 Connection_Handle 连接的远程蓝牙设备已成功改变 Page_Scan_Mode
呼叫扫描竞争模式改变事件	呼叫扫描竞争模式改变事件表示采用指定 Connection_Handle 连接的远程蓝牙设备已成功改变 Page_Scan_Repetition_Mode
最大时隙改变事件	该事件用于在 LMP_Max_Slots 值改变时将该值通知主机

5.2 事件说明

这些事件提供返回参数和与每一事件有关数据的方法。

5.2.1 查询完成事件

表 11.386

事件	OCF	事件代码
Inquiry complete	0x01	Status Num_Responses

说明：

查询完成事件表示查询结束。该事件包含一个状态参数,该参数用于表示查询成功完成与否。另外,Num_Responses 参数包含在最近一次查询中应答的蓝牙设备的数量。

事件参数：

Status: 大小: 1 字节

表 11.387

值	参数说明
0x00	查询指令成功完成
0x01	查询指令失败

Num_Responses: 大小: 1 字节

表 11.388

值	参数说明
0xXX	查询的应答数

5.2.2 查询结果事件

表 11.389

事件	OCF	事件代码
查询结果事件	0x02	Num_Responses,BD_ADDR , Page_Scan_Repetition_Mode , Page_Scan_Period_Mode , Page_Scan_Mode,Class_of_device,Clock_Offset

查询结果事件表示在当前查询进程中已有一个或多个蓝牙设备应答。如果远程设备只支持强制呼叫方案，则一旦从远程设备收到一查询应答，主控制器将向主机发送该事件。主控制器可将查询回答排队，并在一个查询结果事件中发送多个蓝牙设备信息。该事件可用于在一个事件中返回一个或多个查询应答。该事件包括对应于应答上一次查询的蓝牙设备的 BD_ADDR， Page_Scan_Repetition_Mode， Page_Scan_Period_Mode， Page_Scan_Mode，Clock_Offset 和 Class of Device。

事件参数：

Num_Responses: 大小: 1 字节

表 11.390

值	参数说明
0xXX	查询的应答数

BD_ADDR [I]: 大小: 6 个字节*

表 11.391

值	参数说明
0xXXXXXXXXXXXX	每一应答设备的 BD_ADDR

Page_Scan_Repetition_Mode [I]: 大小: 1 字节

表 11.392

值	参数说明
0x00	R0
0x01	R1
0x02	R2
0x03-0xFF	保留

Page_Scan_Period_Mode [I]: 大小: 1 字节

表 11.393

值	参数说明
0x00	P0
0x01	P1
0x02	P2
0x03-0xFF	保留

Page_Scan_Mode: 大小: 1 字节

表 11.394

值	参数说明
0x00	强制呼叫扫描
0x01	可选呼叫扫描模式 I
0x02	可选呼叫扫描模式 II
0x03	可选呼叫扫描模式 III
0x04-0xFF	保留

Class_of_Device: 大小: 3 字节

表 11.395

值	参数说明
0xXXXXXX	设备类型

Clock_offset: 容量: 1 字节

表 11.396

位格式	参数说明
14.0 位	16.2 位的 CLKslave-CLKmaster
第 15 位	保留

5.2.3 连接完成事件

表 11.397

事件	OCF	事件代码
连接完成事件	0x03	Status, Connection_Handle BD_ADDR, Link_Type Encryption_mode

说明：

连接完成事件指示构成连接的两主机已建立一个新的连接。该事件也可通知发送 Create_Connection Add_SCO_Connectionn 或 Accept_Connection_Request 或 Reject_Connection 指令的主机，并接收表示指令是否成功完成的指令状态事件。

事件参数：

Status: 大小：1 字节

表 11.398

值	参数说明
0x00	连接成功完成
0x01	连接未完成

Connection_Handle: 大小：2 个字节(其中 12 位有意义)

表 11.399

值	参数说明
0xXXXX	连接句柄用于识别蓝牙设备间连接。连接柄也可用作发送和接收语音或数据的标识符。 范围：0x0000-0x0EFF （ 0x0F00 - 0x0FFF 保留使用）

BD_ADDR: 大小：6 字节

表 11.400

值	参数说明
0xXXXXXXXXXXXX	构成连接的另一连接设备的 BD_ADDR

Link_Type: 大小：1 字节

表 11.401

值	参数说明
0x00	SCO 连接(语音通道)
0x01	ACL 连接(数据通道)
0x02-0xFF	保留使用

Encryption_Mode: 大小：1 字节

表 11.402

值	参数说明
0x00	加密停止
0x01	只对点对点分组加密
0x02	对点对点和广播分组加密。
0x03-0xFF	保留

5.2.4 连接请求事件

表 11.403

事件	OCF	事件代码
Connection request	0x04	BD-ADDR Class_of_device Link_Type

说明：

连接请求事件用于表示正尝试建立一新的连接。连接可被接受或也可被拒绝。如果该事件被屏蔽，并且存在一呼入连接尝试，主控制器将自动拒绝该连接尝试。当主机收到该事件时，它将在 Conn_Accept_Timeout 定时器失效前，以 Accept_Connection_Request 或 Reject_Connection_Re- quest 指令应答。

事件参数：

BD_ADDR： 大小：6 字节

表 11.404

值	参数说明
0xXXXXXXXXXXXX	请求连接设备的 BD_ADDR

Class_of_Device： 大小：3 字节

表 11.405

值	参数说明
0xXXXXXX	请求连接设备的设备类型

Link_Type： 大小：1 字节

表 11.406

值	参数说明
0x00	SCO 连接(语音通道)
0x01	ACL 连接(数据通道)
0x02-0xFF	保留使用

5.2.5 连接断开完成事件

表 11.407

事件	OCF	事件代码
Disconnection Complete	0x05	Status Connection_handle,Reason

说明：

连接断开完成事件当连接中止时发生。状态参数表示连接断开是否成功。如果连接断开成功，则原因参数表示连接断开原因。如果连接断开失败，主机将忽略原因参数值。例如，如果主机已发出连接断开指令，并存在参数错误，则不允许该指令执行，或给出不能应答连接的连接句柄。

注意:当物理链路失败时，将在物理链路上为每一逻辑通道返回连接断开完成完成事件，相应连接句柄作为其参数。

事件参数：

Status: 大小：1 字节

表 11.408

值	参数说明
0x00	连接断开完成
0x01	连接断开未完成

Connection_Handle: 大小：2 字节(其中 12 位有意义)

表 11.409

值	参数说明
0xXXXX	断开连接句柄。 范围：0x0000-0x0EFF(0x0F00-0x0FFF 保留)

Reason: 大小：1 字节

表 11.410

值	参数说明
0x08 ,0x13- 0x16 , 0x1A	连接超时(0x08),其它终端连接终止错误代码(0x13-0x15)，由本地主机终止的连接(0x16),以及未支持的远端特性错误代码(0x1A)。

5.2.6 认证完成事件

表 11.411

事件	OCF	事件代码
认证完成事件	0x06	Satus, Connection_Handle

说明：

当指定连接的认证已完成时，认证完成事件发生。

Connection_Handle 是 ACL 连接的 Connection_Handle。

事件参数：

Status: 大小：1 字节

表 11.412

值	参数说明
0x00	认证请求成功完成
0x01	认证请求未完成

Connection_Handle: 大小：2 个字节(其中 12 位有意义)

表 11.413

值	参数说明
0xXXXX	执行认证的连接句柄 范围：0x0000-0x0EFF(0x0F00-0x0FFF 保留)

5.2.7 远程命名请求完成事件

表 11.414

事件	OCF	事件代码
远程命名请求完成事件	0x07	Status BD_ADDR Remote_name

说明：

远程命名请求事件用于表示远程命名请求已完成。Remote_Name 事件参数为一长度可达 248 字节的 UTF-8 编码字符串。如果 UTF-8 编码字符串不到 248 个字节，则 Remote_Name 事件参数尾段用空值(0x00)填充。BD_ADDR 事件参数则用于标识获取名字的设备。

注意：Remote_Name 参数从名字的第一字节开始接收。这也是用于传输多字节参数的小 Endian 码的一个例外。

事件参数：

Status: 大小：1 字节

表 11.415

值	参数说明
0x00	Remote_Name_Request 指令成功
0x01	Remote_Name_Request 指令失败

BD_ADDR: 大小：6 字节

表 11.416

值	参数说明
0xXXXXXXXXXXXX	被请求设备的 BD_ADDR

Remote_Name: 大小：248 字节

表 11.417

值	参数说明
名称[248]	远程设备的 UTF-8 编码的描述性名字。 UTF-8 编码名字可长达 248 字节。如果它短于 248 字节，则用 0x00 进行填充.

5.2.8 加密模式改变事件

表 11.418

事件	OCF	事件代码
加密模式变化事件	0x08	Status Connetion_handle Encryption_enable

说明：

加密模式改变事件用于表示已完成由 Connection_Handle 事件参数指定连接句柄的加密模式改变。Connection_Handle 为 ACL 连接的 Connection_Handle。Encryption_Enable 事件参数指定由 Connection_Handle 指定的连接句柄启用新的加密模式。该事件将在连接两端设备上发生，以通知两主机加密模式已改变。

事件参数：

Status: 大小：1 字节

表 11.419

值	参数说明
0x00	加密模式改变成功。
0x01	加密模式改变成功

Connection_Handle: 大小:2 字节(其中 12 位有意义)

表 11.420

值	参数说明
0xXXXX	同一蓝牙设备终端的所有连接句柄中启用或终止链路层加密的连接句柄。 范围：0x0000-0x0EFF(0x0F00-0x0FFF 保留)

Encryption_Enable: 大小：1 字节

表 11.421

值	参数说明
0x00	停用链路层次加密。
0x01	启用链路层次加密。

5.2.9 连接链接字改变完成事件

表 11.422

事件	OCF	事件代码
连接链接字改变完成事件	0x09	Status, Conection_handle

说明：

连接链接字改变完成事件用于表示由 Connection_Handle 事件参数指定连接句柄的链接字改变已完成。Connection_Handle 为 ACL 连接的 Connection_Handle。该事件只发往发送 Change_Connection_Link_Key 指令主机。

事件参数：

Status: 大小：1 字节

表 11.423

值	参数说明
0x00	Change_Connection_Link_Key 指令成功
0x01	Change_Connection_Link_Key 指令失败

Connection_Handle: 大小：2 字节(其中 12 位有意义)

表 11.424

值	参数说明
0xXXXX	同一蓝牙设备终端的所有连接句柄中改变链接字的连接句柄。 范围：0x0000-0x0EFF(0x0F00-0x0FFF 保留)

5.2.10 主单元链接字完成事件

表 11.425

事件	OCF	事件代码
主单元链接字完成事件	0x0A	Status， Connection_Handle Key_Flag

说明：

主单元链接字完成事件用于表示匹克网蓝牙主单元的临时链接字或半永久链接字改变已完成。Connection_Handle 为 ACL 连接句柄。连接所使用的链接字将为主设备的临时链接字，或由 Key_Flag 表示的半永久链接字。Key_Flag 事件参数用于表示当前在匹克网中使用的是哪个链接字(主单元临时链接字，或半永久链接字)。

注意:对于一主单元，从临时链接字到半永久链接字的变化将影响所有与匹克网有关的所有连接句柄。对于一从单元，此变化将仅仅影响某指定连接句柄。当广播和点对点通信都需要加密时，则必须使用临时链接字。

事件参数：

Status: 大小：1 字节

表 11.426

值	参数说明
0x00	Master_Link_Key 指令成功
0x01	Master_Link_Key 指令失败

Connection_Handle: 大小：2 字节(其中 12 位有意义)

表 11.427

值	参数说明
0xXXXX	对于同一匹克网中所有设备，链接字已改变的连接句柄。 范围：0x0000-0x0EFF(0x0F00-0x0FFF 保留)

Key_Flag: 大小：1 字节

表 11.428

值	参数说明
0x00	使用半永久链接字
0x01	使用临时链接字

5.2.11 远程支持特性读取完成事件

表 11.429

事件	OCF	事件代码
远程支持特性读取完成事件	0x0b	Status Connection_handle LMP_features

说明

该事件用于表示获取由 Connection_Handle 指定远程蓝牙设备支持特性的链路管理器进程的结束。Connection_Handle 为一 ACL 连接的连接句柄。事件参数则包括 LMP 特性表。具体细节参见“链路管理器协议”。

事件参数：

Status: 大小：1 字节

表 11.430

值	参数说明
0x00	Read_Remote_Supported_Features 指令成功
0x01	Read_Remote_Supported_Features 指令失败

Connection_Handle: 大小：2 字节(其中 12 位有意义)

表 11.431

值	参数说明
0xXXXX	连接句柄用于 Read_Remote_Supported_Features 指令，范围：0x0000-0x0EFF(0x0F00-0x0FFF 保留)

LMP_Features: 大小:8 字节

表 11.432

值	参数说明
0xXXXXXXXX XXXXXXXX	LMP 屏蔽位列表，参见“链路管理器协议”

5.2.12 远程版本信息读取完成事件

表 11.433

事件	OCF	事件代码
远程版本信息读取完成事件	0x0c	Status Connection_handle LMP_version Manufacturer_name LMP_subversion

说明：

该事件表示用于获取远程蓝牙设备版本信息的链路管理器进程的结束。该版本信息由 Connection_Handle 指定。Connection_Handle 为一 ACL 连接的连接句柄。LMP_Version 事件参数定义蓝牙硬件的主要硬件方案。只有符合新蓝牙 SIG 规范的蓝牙新硬件版本出现时，该事件参数才变化;也就是说，该事件参数由 SIG 控制。Manufacturer_name 参数表示远程蓝牙模块制造商。LMP_Subversion 事件参数应由制造商控制，并且可根据需要改变。LMP_Subversion 事件参数定义了当设计进程变化和错误得到修改时，蓝牙硬件的每一修订版本。该事件允许软件确定正在使用哪种蓝牙硬件，并且如果必要,将能够在硬件出错的环境下工作。

事件参数：

Status: 大小：1 字节

表 11.434

值	参数说明
0x00	Read_Remote_Version_Information 指令成功
0x01	Read_Remote_Version_Information 指令失败

Connection_Handle： 大小：2 字节(其中 12 位有意义)

表 11.435

值	参数说明
0xXXXX	连接柄用于 Read_Remote_Version_Information 指令 范围：0x0000-0x0EFF(0x0F00-0x0FFF)保留)

LMP_Version： 大小：1 字节

表 11.436

值	参数说明
0xXX	远程蓝牙硬件当前 LMP 版本

Manufacturer_name: 大小：2 字节

表 11.437

值	参数说明
0xXXXX	远程蓝牙硬件制造商名称

LMP_Subversion: 大小：2 字节

表 11.438

值	参数说明
0xXXXX	远程蓝牙硬件的当前 LMP 子版本

5.2.13 QoS 设置完成事件

表 11.439

事件	OCF	事件代码
QoS 设置完成事件	0x0d	Status Conection_handle Flags Service_type Token_rate Peak_bandwidth Latency Delay_variation

说明：

该事件表示由 Conection_handle 事件参数指定的远程蓝牙设备 QoS 的链路管理器设置进程结束。Conection_handle 为一 ACL 连接连接句柄。具体细节参见“逻辑链路控制和适配协议规范”。

事件参数：

状态： 大小：1 字节

表 11.440

值	参数说明
0x00	QoS_Setup 指令成功

0x01	QoS_Setup 指令失败

Conection_handle: 大小: 2 字节(其中 12 位有意义)

表 11.442

值	参数说明
0xXXXX	连接柄用于 Qos_setup 指令 范围: 0x0000-0x0EFF(0x0F00-0x0FFF 保留)

Flags: 大小: 1 字节

表 11.443

值	参数说明
0x00-0xFF	保留

Service_Type: 大小: 1 字节

表 11.444

值	参数说明
0x00	无可用通信
0x01	允许最大传输能力
0x02	可用授权
0x03-0xFF	保留

Token_Rate: 大小: 4 字节

表 11.445

值	参数说明
0xXXXXXXXX	允许 Token_Rate，单位为字节/秒

Peak_Bandwidth: 大小: 4 字节

表 11.446

值	参数说明
0xXXXXXXXX	允许峰值带宽

latency: 大小: 4 字节

表 11.447

值	参数说明
0xXXXXXXXX	允许延时，单位微秒

Delay_Variation : 容量 4 字节

表 11.448

值	参数说明
0xXXXXXXXX	允许延迟值，单位微秒

5.2.14 指令完成事件

表 11.449

事件	OCF	事件代码
指令完成事件	0x0e	Num_hci_command_packets Command_opcod Return_parameters

说明：

该事件由主控制器用于传递大多数指令返回状态，以及其它已发出 HCI 指令的事件参数。Num_HCI_Command_Packets 事件参数允许主控制器指出主机可发往主控制器 HCI 指令分组个数。如果主控制器要求停止送指令，Num_HCI_Command_Packets 事件参数将设置为零。为了通知主机主控制器已准备好接收 HCI 指令分组，主控制器将生成 Command_Opcode 为 0x0000 的指令完成事件，并且 Num_HCI_Command_Packets 事件参数将设置为 1 或更大值。Command_Opcode（0x0000）为 NOP(空操作),并且用于改变主机进入等待状态前可发送的 HCI 指令分组的个数。

事件参数：

Num_HCI_Command_Packets: 大小：1 字节

表 11.450

值	参数说明
N=0xXX	可从 host 发往主控制器的 HCI 指令分组个数 N 取值范围：0-255

Command_Opcode： 大小：2 字节

表 11.451

值	参数说明
0xXXXX	可引发该事件的指令的操作码

Return_Parameter： 大小:取决于代码事件参数指令完全的 0x0E

表 11.452

值	参数说明
0xXX	Command_Opcode 事件参数指定指令的返回参数，参见与该指令相关的返回参数列表

5.2.15 指令状态事件

表 11.453

事件	OCF	事件代码
指令状态事件	0x0F	Status Num_HCI_command_packets Command_Opcode

说明：

该事件表示已收到由 Command_Opcode 参数描述的指令,且主控制器正在执行该指令任

务。该事件需提供异步操作机制,以防止主机一直处于等待指令完成的状态。如果指令不能执行(可能由于参数错误或指令不允许),指令状态事件参数将包含相应出错代码，并且由于指令未执行则不会生成该指令完成事件。Num_HCI_Command_Packets 事件参数允许主控制器表示主机能发送至主控制器的 HCI 指令分组个数。如果主控制器要求停止发送指令，Num_HCI_Command_Packets 事件参数将置为 0。为了通知主机主控制器已准备好接收 HCI 指令分组，主控制器将生成状态为 0x00、Command_Opcode 为 0x0000，以及 Num_HCI_Command_Packets 事件参数为 1 或更大值的指令状态事件。Command_Opcode（0x0000）为 NOP(空操作)，并且用于改变主机进入等待状态前可接收 HCI 指令分组的个数。

事件参数：

Status: 大小: 1 字节

表 11.454

值	参数说明
0x00	指令当前正在执行
0x01	指令失败

Num_HCI_Command_Packets： 大小: 1 字节

表 11.455

值	参数说明
N = 0xXX	允许从主机发往主控制器的 HCI 指令分组数 N 取值范围:0-255

Command_Opcode： 大小:2 字节

表 11.456

值	参数说明
0xXXXX	引发该事件，且正在执行指令的操作码

5.2.16 硬件故障事件

表 11.457

事件	OCF	事件代码
硬件故障事件	0x10	Hardware_code

说明：

硬件故障事件用于表示蓝牙设备的硬件故障类型。该事件也用于通知主机蓝牙模块已发生故障。

事件参数：

Hardware_Code： 大小: 1 字节

表 11.458

值	参数说明
0x00	Hardware_Codes 因不同实现而定，且可指定为不同硬件故障

5.2.17 刷新事件

表 11.459

事件	OCF	事件代码
刷新事件	0x11	Connection_handle

说明：

刷新事件用于表示对于特定连接句柄，已将用于传输的当前用户数据删除。Connection_handle 为 ACL 连接的连接句柄。这主要是由于刷新指令，或发生自动刷新。在主控制器中，一 L2CAP 分组的多个数据块已待定。如果 L2CAP 分组的基带分组部分被刷新，则 L2CAP 分组的 HCI 数据分组的其余部分也必须刷新。

事件参数：

Connection_handle： 大小：2 字节(其中 12 位有意义)

表 11.460

值	参数说明
0xXXXX	已刷新连接句柄 范围：0x0000-0x0EFF(0x0F00-0x0FFF 保留)

5.2.18 角色变化事件

表 11.461

事件	OCF	事件代码
角色变化事件	0x12	Status BD_ADDR NEW_ROLE

说明：

角色变化事件用于表示与特定连接有关的当前蓝牙角色已改变。只有当与 BD_ADDR 事件参数相关的远端和本地蓝牙设备已完成其角色变化时，该事件才发生。当角色已改变后，该事件将通知连接两端设备。

事件参数：

状态： 大小：1 字节

表 11.462

值	参数说明
0x00	发生角色变化
0x01	角色变化失败

BD_ADDR: 大小：6 字节

表 11.463

值	参数说明
0Xxxxxxxxxxxx	角色改变设备的 BD_ADDR

New_Role： 大小：1 字节

表 11.464

值	参数说明
0x00	对应于指定 BD_ADDR 的主单元
0x01	对应于指定 BD_ADDR 的从单元

5.2.19 完成分组数事件

表 11.465

事件	OCF	事件代码
完成分组数事件	0x13	Number_of_handles Connection_handle Hc_num_of_completed_packets

说明：

该事件由主控制器用于通知主机自从前一完成分组数事件发往主机后，对于每一连接句柄，已完成(发送或刷新) 传输的 HCI 数据分组个数。也就意味着，主控制器相应缓冲区空间也已释放。基于该信息，以及 Read_Buffer_Size 指令的返回参数 HC_Total_Num_ACL_Data_Packets 和 HC_Total_Num_SCO_Data_Packets,主机就能确定以后的 HCI 数据分组将使用何连接句柄发往主控制器。在相应连接完成事件发生前，不应发送该事件。当主控制器在其缓冲区缓存 HCI 数据分组时，它必须向主机周期性持续发送完成分组数事件,直到它最终报告所有待处理 ACL 数据分组都已发送或刷新为止。事件及其发送速率由制造商指定。

注意：如果停用 SCO 流控制，将不能报告对应于 SCO 连接句柄的完成分组数事件。

事件参数：

Number_of_Handles： 大小：1 字节

表 11.466

值	参数说明
0xXX	本事件包含的 Num_HCI_Data_Packets 参数对和连接句柄数量。范围：0-255

Connection_handle[I]： 大小:Number_of_Handles*2 字节
(其中 12 位有意义)

表 11.467

值	参数说明
0xXXXX	连接句柄 范围:0x0000-0x0EFF(0x0F00-0x0FFF 保留)

HC_Num_Of_Completed_Packets： 大小：2 字节

表 11.468

值	参数说明
N = 0xXXXX	自从前一事件返回后，对应于相关连接句柄的已完成(发送或刷新)的 HCI 数据分组数 N 取值范围:0x0000-0xFFFF

5.2.20 模式变化事件

表 11.469

事件	OCF	事件代码

模式变化事件	0x14	Status Connection_handle Current_mode Interval

说明：

该事件用于表示与特定连接句柄相关联的设备在激活、保持、呼吸和休眠模式之间何时发生变化。Current_mode 为一 ACL 连接的连接句柄。Current_mode 事件参数用于表示模式变化事件相对于哪一个连接句柄发生。该参数也可用于表示连接当前处于哪一状态。Interval 参数则用于指定每一状态的持续时间。每一与已发生模式变化的连接句柄相关联的主控制器都将发送一模式变化事件到主机。

事件参数： 大小：1 字节

表 11.470

值	参数说明
0x00	发生模式变化事件
0x01-0xFF	Hold_Mode、Sniff_Mode、 Exit_Sniff_Mode、 Park_Mode，或 Exit_Park_Mode 指令失败。

Connection_handle: 大小：2 字节(其中 12 位有意义)

表 11.471

值	参数说明
0xXXXX	连接句柄 范围：0x0000-0x0EFF(0x0F00-0x0FFF 保留)

crrent_Mode： 大小：1 字节

表 11.472

值	参数说明
0x00	激活模式
0x01	保持模式
0x02	呼吸模式
0x03	休眠模式
0x04-0xFF	保留

间歇： 大小：2 个字节

表 11.473

值	参数说明
N = 0xXXXX	保持： 保持模式等待的基带时隙数。 保持间隔= N * 0.625 ms N 取值范围：0x0000-0xFFFF 时间范围：0-40.9 秒 呼吸： 呼吸间隔之间的基带时隙数

	呼吸间隔之间的时间= 0.625 ms N 取值范围：0x0000-0xFFFF 时间范围：0-40.9 秒 休眠： 连续信号灯之间的基带时隙数。 间隔时间= N * 0.625 ms N 取值范围：0x0000-0xFFFF 时间范围：0-40.9 秒

5.2.21 链接字返回事件

表 11.474

事件	OCF	事件代码
链接字返回事件	0x15	Num_keys BD_ADDR Link_key

说明：

该事件由主控制器用于向主机发送一个或多个存储链接字。在 Read_Stored_Link_Key 指令发出以后,将不发生或发生多个事件实例。当无存储链接字时，将不返回链接字事件。

当有存储链接字时，在每一链接字返回事件中返回的链接字数量将根据具体实现而定。

事件参数：

Num_Keys： 大小：1 字节

表 11.475

值	参数说明
0xXX	该事件所包含的链接字数 范围：0x01-0xFF

BD_ADDR [I]: 大小：6* Num_Keys 字节

表 11.476

值	参数说明
0xXXXXXXXXXX	对应于相关链接字的 BD_ADDR

Num_Keys Link_Key [I]: 大小:16 字节

表 11.477

值	参数说明
0xXXXXXXXXXX XXXXXXXXXX XXXXXXXXXX	对应于相关 BD_ADDR 的链接字

5.2.22 PIN 码请求事件

表 11.478

事件	OCF	事件代码
Pin code request	0x16	BD_ADDR

说明：

该事件用于表示需要一 PIN 码以创建新的链接字。主机是采用 PIN 码请求应答，还是采用 PIN 码消极请求应答，取决于主机是否能够为主控制器提供 PIN 码。

注意:如果 PIN 码请求事件被屏蔽,则主控制器就假设主机无 PIN 码。

当主控制器生成一 PIN 码请求事件,以便本地链路管理器对来自远程链路管理器的请求应答时(作为来自远程主机的 Create_Connection 或 Authentication_Requested 指令的结果),本地主机必须在远程链路管理器检测到 LMP 应答超时之前,使用 PIN_Code_Request_Reply 或 PIN_Code_Request_Negative_Reply 指令应答。(参见"链路管理器协议")。

事件参数:

BD_ADDR: 大小: 6 字节

表 11.479

值	参数说明
0XxxxxxxXXXXXX	新链接字所属设备的 BD_ADDR

5.2.23 链接字请求事件

表 11.480

事件	OCF	事件代码
链接字请求事件	0x17	BD_ADDR

说明:

该事件用于表示需要针对指向 BD_ADDR 指定设备的连接创建一链接字。如果主机具有被请求链接字,则主机将使用 Link_Key_Request_Reply 指令将该被请求链接字送往主控制器。如果主机不含被请求链接字,则主机将使用 Link_Key_Request_Negative_Reply 指令通知主机该主机不含被请求链接字。

注意:如果链接字请求事件被屏蔽,则主控制器将假设主机不含其它链接字。

当主控制器生成一链接字请求事件,以便本地链路管理器对来自远程链路管理器的请求应答时(作为来自远程主机的 Create_Connection 或 Authentication_Requested 指令的结果),本地主机必须在远程链路管理器检测到 LMP 应答超时之前,使用 Link_Key_Request_Reply 或 Link_Key_Request_Negative_Reply 指令应答。(参见"链路管理器协议")。

事件参数:

BD_ADDR: 大小:6 字节

表 11.481

值	参数说明
0xXXXXXXXXXXXX	储存链接字所属设备的 BD_ADDR

5.2.24 链接字通知事件

表 11.482

事件	OCF	事件代码
链接字通知事件	0x18	BD_ADDR Link_key

说明:

该事件用于通知主机已针对指向 BD_ADDR 指定设备的连接创建了一个新链接字。主机将在其存储设备中保存该新链接字，以便将来使用。并且，主机将使用 Link_Key_Request_Reply 指令将该链接字存储在主控制器的链接字存储设备中。

事件参数：

BD_ADDR： 大小：6 字节

表 11.483

值	参数说明
0xXXXXXXXXXXXX	生成新链接字设备的 BD_ADDR

Link_Key： 大小:16 字节

表 11.484

值	参数说明
0xXXXXXXXXXX XXXXXXXXXX XXXXXXXXXX	与 BD_ADDR 相关联的链接字

5.2.25 回送指令事件

表 11.485

事件	OCF	事件代码
回送指令事件	0x19	HCI_command_packet

说明：

处于本地回送模式时，主控制器将回送指令和数据到主机。回送指令事件用于返回含例外情况的所有从主机发往主控制器的命令。参见“Read_Loopback_Mode”中有关不能回送指令的情况。HCI_Command_Packet 事件参数包含所有包含头的 HCI 分组。

注意:事件分组有效载荷最大值为 255 字节。由于 HCI 指令头数据长为 3 字节,则只返回开始 252 字节的指令参数。

事件参数：

HCI_Command_Packet: 大小:因指令而异

表 11.486

值	参数说明
0xXXXXXX	HCI 指令分组,包括头

5.2.26 数据缓冲区溢出事件

表 11.487

事件	OCF	事件代码
数据缓冲区溢出事件	0x1A	Link_type

说明：

该事件用于表示主控制器数据缓冲区已溢出。如果主机发送分组数量超过限制时将引发该事件。Link_Type 参数用于表示溢出是由 ACL 数据还是由 SCO 数据引起的。

事件参数：

Link_Type： 大小：1 字节

表 11.488

值	参数说明
0X00	SCO 缓冲区溢出(语音信道)
0X01	ACL 缓冲区溢出(数据信道)
0x02-0xFF	保留

4.10 测试指令

测试指令用于提供测试蓝牙硬件不同功能的能力，并为测试提供安排不同条件的能力。对于测试指令，OGF 定义为 0x06。

表 11.489

指令	指令综述
Read_Loopback_Mode	Read_Loopback_Mode 将读取主控制器回送模式的设置值。回送模式设置可以确定信息发送路径。
Write_Loopback_Mode	Write_Loopback_Mode 将写入主控制器回送模式的设置值。回送模式设置可以确定信息发送路径。
Enable_Device_Under_Test_Mode	Enable_Device_Under_Test_Mode 指令允许本地蓝牙模块通过 LMP 测试指令进入测试模式。当主机要求本地设备作为待测试设备，实现蓝牙测试模式文件中规定测试情景时，则发送该指令。

4.10.1 Read_loopback_Mode

表 11.490

指令	OCF	指令参数	返回参数
HCI_Read_loopback_Mode	0x0001		Status Loopback_Mode

说明：

本指令将读取主控制器回送模式参数值。回送模式设置可以确定信息发送路径。在非测试模式操作中，回送模式设置为非测试模式，而其信息路径则由蓝牙规范指定。在本地回送模式中，每一数据分组(ACL 和 SCO)和从主机发送到主控制器的指令分组，也将由主控制器不加任何改变地返回，参见图 4.5。

当蓝牙主控制器进入本地回送模式时,它可以四种连接完成事件应答,其中一种用于 ACL 通道和三种用于 SCO 通道，以便当发送 ACL 和 SCO 数据时，主机能够获取连接句柄。当处于本地回送模式时，主控制器将向主机回送指令和数据。回送指令事件用于主机向主控制器发送回送指令。

在本地回送模式中有一些指令将不会被回送，包括 Reset、Set_Host_Controller_To_host_Flow_Control，Host_Buffer_Size，Host_Number_Of_Completed_Packets，Read_Buffer_Size，Read_loopback_Mode 和 Write_loopback_Mode。指令 Reset 和 Write_loopback_Mode 可用于退出本地回送模式。如果 Write_loopback_Mode 用于退出本地回送模式,则将向主机发送四种连接断开完成事件,这四种事件对应于进入本地回送模式时发送的连接完成事件。而且,本地回送模式不得允许任何连接。如果存在一个连接,且存在设备进入本地回送模式的尝试，则主控制器将拒绝呼入连接尝试。这将不允许使用其它变量对主控制器传输层进行测试。

如果一设备设置为远程回送模式，它将无线发回所有数据（ACL 和 SCO)。它最大可允许

同时保持一条 ACL 连接和三条 SCO 连接。而这与远程设备相同。如果存在不止一条指向远程设备的连接，并且存在设置本地设备为远程回送模式的尝试，而该尝试将被拒绝。参图 4.6，其中最右边的设备设置为远程回送模式，最左边设备设置为非测试模式。可以不使用任何其它变量测试蓝牙无线链路。

指令参数：无。

返回参数：

Status： 大小：1 字节

表 11.491

值	参数说明
0x00	Read_loopback_Mode 指令成功
0x01	Read_loopback_Mode 指令失败，参见 260 页表 2 的错误代码

Loopback_Mode ： 大小：1 字节

表 11.492

值	参数说明
0x00	未启用回送模式，缺省
0x01	启用本地回送
0x02	启用远程回送
0x03-0xFF	保留

生成事件(如未屏蔽)：

当完成 Read_loopback_Mode 指令时，将生成指令完成事件。

4.10.2 Write_Loopback_Mode

表 11.493

指令	OCF	指令参数	返回参数
HCI_ Write_loopback_Mode	0x0002	Loopback_Mode	Status

说明：

Write_Loopback_Mode 将写入主控制器回送模式的设置值。回送模式设置可以确定信息发送路径。在非测试模式操作中，回送模式设置为非测试模式，而其信息路径则由蓝牙规范指定。在本地回送模式中，每一数据分组(ACL 和 SCO)和从主机发送到主控制器的指令分组，也将由主控制器不加任何改变地返回，参见图 4.7。

当蓝牙主控制器进入本地回送模式时，它可以四种连接完成事件应答,其中一种用于 ACL 通道和三种用于 SCO 通道，以便当发送 ACL 和 SCO 数据时，主机能够获取连接句柄。当处于本地回送模式时，主控制器将向主机回送指令和数据。回送指令事件用于主机向主控制器发送回送指令。

在本地回送模式中有一些指令将不会被回送，包括 Reset、Set_Host_Controller_To_host_Flow_Control，Host_Buffer_Size，Host_Number_Of_Completed_Packets，Read_Buffer_Size，Read_loopback_Mode 和 Write_loopback_Mode。这些指令可以常规执行方式执行。指令 Reset 和 Write_loopback_Mode 可用于退出本地回送模式。

如果 Write_loopback_Mode 用于退出本地回送模式,则可向主机发送四种连接断开完成事件，以对应于进入本地回送模式时的连接完成事件。而且,本地回送模式不得允许任何连接。如果存在一个连接,且存在设备进入本地回送模式的尝试，则主控制器将拒绝呼入连接尝试。这将允许不使用其它变量对主控制器传输层进行测试。

如果一设备设置为远程回送模式，它将无线发回所有数据（ACL 和 SCO）。它也最大可允许同时保持一条 ACL 连接和三条 SCO 连接。而这与远程设备相同。如果存在不止一条指向远程设备的连接，并且存在设置本地设备为远程回送模式的尝试，而该尝试将被拒绝。参见图 4.8，其中最右边的设备设置为远程回送模式，最左边设备设置为非测试模式。可以不使用任何其它变量测试蓝牙无线链路。

指令参数：

Loopback_Mode ： 大小：1 字节

表 11.494

值	参数说明
0x00	未启用回送模式
0x01	启用本地回送
0x02	启用远程回送
0x03-0xFF	保留

返回参数：

Status: 大小：1 字节

表 11.495

值	参数说明
0x00	Write_loopback_Mode 指令成功
0x01	Write_loopback_Mode 指令失败，参见表 6.1 的错误代码

生成事件(如未屏蔽)：

当完成 Write_loopback_Mode 指令时，将生成指令完成事件。

4.10.4 Enable_Device_Under_Test_Mode

表 11.496

指令	OCF	指令参数	返回参数
HCI_Enable_Device_Under_ Test_Mode	0x0003		Status

说明：

Enable_Device_Under_Test_Mode 指令将允许本地蓝牙模块通过 LMP 测试指令进入测试模式。细节参见“链路管理器协议”。当主机要求本地设备成为 DUT，并进入蓝牙测试模式中的测试情景时，主机将发送该指令。当主控制器收到该指令时，它将通过指令完成事件完成该指令。主控制器将正常操作，直至远程测试装置发出 LMP 测试指令将本地设备进入测试模式。为了终止并退出测试模式，主机将发送 HCI_Reset 指令。该指令将阻止远端蓝牙设备不先发出该指令就将本地蓝牙设备置为测试模式。

指令参数：无

返回参数：

Status: 大小：1 字节

表 11.497

值	参数说明
0x00	Enter_Device_Under_Test_Mode 指令成功
0x01	Enter_Device_Under_Test_Mode 指令失败，参见 745 页表 6.1

生成事件(如未屏蔽)：

当完成 Enter_Device_Under_Test_Mode 指令时，将生成指令完成事件。

5 事件

5.1 事件

除以下列出事件以外，事件代码 0xFF 将保留作为厂商调试事件的事件代码，和事件代码 0xFE 保留用于蓝牙标识测试。

表 11.498 支持事件列表

事件	事件总述
查询完成事件	查询完成事件表示查询已完成
查询结果事件	查询结果事件表示在当前查询进程中已有一个或多个蓝牙设备应答
连接完成事件	连接完成事件指示构成连接的两主机已建立一个新的连接。
连接请求事件	连接请求事件用于表示正在建立一个新的呼入连接。
连接断开完成事件	连接断开完成事件当连接中止时发生
认证完成事件	认证完成事件当指定连接认证完成时发生
远程命名请求事件	远程命名请求事件用于表示远程命名请求已完成。Remote_Name 事件参数为一长度可达 248 字节的 UTF-8 编码字符串。
加密改变事件	加密改变事件用于表示对于由 Connection_Handle 事件参数指定连接句柄已完成加密改变
连接链接字改变完成事件	连接链接字改变完成事件用于表示由 Connection_Handle 事件参数指定连接句柄的链接字改变已完成
主单元链接字完成事件	主单元链接字完成事件用于表示蓝牙主单元一方的临时链接字或半永久链接字改变已完成
远端支持特性读取完成事件	远端支持特性读取完成事件用于表示链路管理器进程已完成，该链路管理器包含由 Connection_Handle 事件参数指定远程蓝牙设备支持的特性。
远程版本信息读取完成事件	远程版本信息读取完成事件用于表示链路管理器进程已完成，该链路管理器包含由 Connection_Handle 事件参数指定远程蓝牙设备的版本信息
QoS 启用完成事件	QoS 启用完成事件用于表示启用 QoS 的链路管理器进程已完成，该过程由 Connection_Handle 事件参数指定远程蓝牙设备完成
指令完成事件	指令完成事件由主控制器用于为每一 HCI 指令传递指令返回状态和其它事件参数
指令状态事件	指令状态事件用于表示已收到 Command_Opcode 参数所描述指令，且主控制器正在执行该指令任务
硬件故障事件	该事件用于表示蓝牙设备硬件故障类别
刷新事件	该事件用于表示对于指定连接句柄，要传输的当前用户数据已删除
角色改变事件	角色改变事件用于表示与特定连接相关的当前蓝牙角色已改变
完成分组数事件	完成分组数事件由主控制器用于通知主机自前一完成分组数事件发送后，对于每一连接句柄已完成了多少 HCI 数据分组。
模式改变事件	模式改变事件用于指示与连接句柄相关的设备何时在激活、挂起、呼吸和休眠模式间变化
返回链接字事件	返回链接字事件用于在使用 Read_Stored_Link_Key 指令后，返回保存的链接字
PIN 码请求事件	PIN 码请求事件用于表示需要一个 PIN 码以创建连接的新链接字
链接字请求事件	链接字请求事件用于表示需要一链接字以建立与 BD_ADDR 指定设备的连接
链接字通知事件	链接字通知事件用于通知主机与 BD_ADDR 指定设备连接的链接字已创建
回送指令事件	回送指令事件用于回送大多数主机发往主控制器的指令

数据缓冲区溢出事件	数据缓冲区溢出事件用于表示由于主机发出分组数超出允许数量，主控制器数据缓冲区已溢出
时隙读取完成事件	时隙读取完成事件用于表示包含时隙信息的 LM 进程已完成
连接分组类型改变事件	连接分组类型改变事件用于表示改变 Connection_Handle 所指定分组类型的链路管理器进程已完成
违反 QoS 事件	违反 QoS 事件用于表示链路管理器不能提供连接句柄的当前 QoS 要求
呼叫扫描模式改变事件	呼叫扫描模式改变事件表示采用指定 Connection_Handle 连接的远程蓝牙设备已成功改变 Page_Scan_Mode
呼叫扫描竞争模式改变事件	呼叫扫描竞争模式改变事件表示采用指定 Connection_Handle 连接的远程蓝牙设备已成功改变 Page_Scan_Repetition_Mode
最大时隙改变事件	该事件用于在 LMP_Max_Slots 值改变时将该值通知主机

5.2 事件说明

这些事件提供返回参数和与每一事件有关数据的方法。

5.2.1 查询完成事件

表 11.499

事件	OCF	事件代码
Inquiry complete	0x01	Status Num_Responses

说明：

查询完成事件表示查询结束。该事件包含一个状态参数,该参数用于表示查询成功完成与否。另外,Num_Responses 参数包含在最近一次查询中应答的蓝牙设备的数量。

事件参数：

Status: 大小：1 字节

表 11.500

值	参数说明
0x00	查询指令成功完成
0x01	查询指令失败

Num_Responses ： 大小：1 字节

表 11.501

值	参数说明
0xXX	查询的应答数

5.2.2 查询结果事件

表 11.502

事件	OCF	事件代码
查询结果事件	0x02	Num_Responses,BD_ADDR ， Page_Scan_Repetition_Mode ，Page_Scan_Period_Mode ， Page_Scan_Mode,Class_of_device ，Clock_Offset

查询结果事件表示在当前查询进程中已有一个或多个蓝牙设备应答。如果远程设备只支持强制呼叫方案，则一旦从远程设备收到一查询应答，主控制器将向主机发送该事件。主控

制器可将查询回答排队，并在一个查询结果事件中发送多个蓝牙设备信息。该事件可用于在一个事件中返回一个或多个查询应答。该事件包括对应于应答上一次查询的蓝牙设备的 BD_ADDR， Page_Scan_Repetition_Mode， Page_Scan_Period_Mode， Page_Scan_Mode，Clock_Offset 和 Class of Device。

事件参数：

Num_Responses ： 大小：1 字节

表 11.503

值	参数说明
0xXX	查询的应答数

BD_ADDR [I]: 大小：6 个字节*

表 11.504

值	参数说明
0xXXXXXXXXXXXX	每一应答设备的 BD_ADDR

Page_Scan_Repetition_Mode [I]: 大小：1 字节*

表 11.505

值	参数说明
0x00	R0
0x01	R1
0x02	R2
0x03-0xFF	保留

Page_Scan_Period_Mode [I]: 大小：1 字节

表 11.506

值	参数说明
0x00	P0
0x01	P1
0x02	P2
0x03-0xFF	保留

Page_Scan_Mode ： 大小：1 字节

表 11.507

值	参数说明
0x00	强制呼叫扫描
0x01	可选呼叫扫描模式 I
0x02	可选呼叫扫描模式 II
0x03	可选呼叫扫描模式 III
0x04-0xFF	保留

Class_of_Device 大小：3 字节

表 11.508

值	参数说明
0xXXXXXX	设备类型

Clock_offset 容量: 1 字节

表 11.509

位格式	参数说明
14.0 位	16.2 位的 CLKslave-CLKmaster
第 15 位	保留

5.2.3 连接完成事件

表 11.510

事件	OCF	事件代码
连接完成事件	0x03	Status Connection_handle BD_ADDR Link_Type Encryption_mode

说明:

连接完成事件指示构成连接的两主机已建立一个新的连接。该事件也可通知发送 Create_Connection Add_SCO_Connection 或 Accept_Connection_Request 或 Reject_Connection 指令的主机，并接收表示指令是否成功完成的指令状态事件。

事件参数:

Status: 大小: 1 字节

表 11.511

值	参数说明
0x00	连接成功完成
0x01	连接未完成，参见表 6.1

Connection_Handle: 大小: 2 个字节(其中 12 位有意义)

表 11.512

值	参数说明
0xXXXX	连接句柄用于识别蓝牙设备间连接。连接柄也可用作发送和接收语音或数据的标识符。 范围: 0x0000-0x0EFF （ 0x0F00 - 0x0FFF 保留使用）

BD_ADDR : 大小: 6 字节

表 11.513

值	参数说明
0xXXXXXXXXXXXX	构成连接的另一连接设备的 BD_ADDR

Link_Type: 大小: 1 字节

表 11.514

值	参数说明
0x00	SCO 连接(语音通道)
0x01	ACL 连接(数据通道)
0x02-0xFF	保留使用

Encryption_Mode: 大小：1 字节

表 11.515

值	参数说明
0x00	加密停止
0x01	只对点对点分组加密
0x02	对点对点和广播分组加密。
0x03-0xFF	保留

5.2.4 连接请求事件

表 11.516

事件	OCF	事件代码
Connection request	0x04	BD-ADDR Class_of_device Link_Type

说明：

连接请求事件用于表示正尝试建立一新的连接。连接可被接受或也可被拒绝。如果该事件被屏蔽，并且存在一呼入连接尝试，主控制器将自动拒绝该连接尝试。当主机收到该事件时，它将在 Conn_Accept_Timeout 定时器失效前，以 Accept_Connection_Request 或 Reject_Connection_Request 指令应答。

事件参数：

BD_ADDR ： 大小：6 字节

表 11.517

值	参数说明
0xXXXXXXXXXXXX	请求连接设备的 BD_ADDR

Class_of_Device ： 大小：3 字节

表 11.518

值	参数说明
0xXXXXXX	请求连接设备的设备类型

Link_Type ： 大小：1 字节

表 11.519

值	参数说明
0x00	SCO 连接(语音通道)
0x01	ACL 连接(数据通道)
0x02-0xFF	保留使用

5.2.5 连接断开完成事件

表 11.520

事件	OCF	事件代码

Disconnection Complete	0x05	Status Connection_handle,Reason

说明：

连接断开完成事件当连接中止时发生。状态参数表示连接断开是否成功。如果连接断开成功，则原因参数表示连接断开原因。如果连接断开失败，主机将忽略原因参数值。例如，如果主机已发出连接断开指令，并存在参数错误，则不允许该指令执行，或给出不能应答连接的连接句柄。

注意:当物理链路失败时，将在物理链路上为每一逻辑通道返回连接断开完成完成事件，相应连接句柄作为其参数。

事件参数：

Status: 大小：1 字节

表 11.521

值	参数说明
0x00	连接断开完成
0x01	连接断开未完成，参见表 6.1

Connection_Handle: 大小：2 字节(其中 12 位有意义)

表 11.522

值	参数说明
0xXXXX	断开连接句柄。 范围：0x0000-0x0EFF(0x0F00-0x0FFF 保留)

Reason: 大小：1 字节

表 11.523

值	参数说明
0x08 ,0x13- 0x16 , 0x1A	连接超时(0x08),其它终端连接终止错误代码(0x13-0x15)，由本地主机终止的连接 (0x16),以及未支持的远端特性错误代码(0x1A)。参见表 6.1

5.2.6 认证完成事件

表 11.524

事件	OCF	事件代码
认证完成事件	0x06	Satus, Connection_Handle

说明：

当指定连接的认证已完成时，认证完成事件发生。Connection_Handle 是 ACL 连接的 Connection_Handle。

事件参数：

Status: 大小：1 字节

表 11.525

值	参数说明
0x00	认证请求成功完成
0x01	认证请求未完成

Connection_Handle: 大小：2 个字节(其中 12 位有意义)

表 11.526

值	参数说明
0xXXXX	执行认证的连接句柄 范围：0x0000-0x0EFF(0x0F00-0x0FFF 保留)

5.2.7 远程命名请求完成事件

表 11.527

事件	OCF	事件代码
远程命名请求完成事件	0x07	Status BD_ADDR Remote_name

说明：

远程命名请求事件用于表示远程命名请求已完成。Remote_Name 事件参数为一长度可达 248 字节的 UTF-8 编码字符串。如果 UTF-8 编码字符串不到 248 个字节，则 Remote_Name 事件参数尾段用空值(0x00)填充。BD_ADDR 事件参数则用于标识获取名字的设备。

注意：Remote_Name 参数从名字的第一字节开始接收。这也是用于传输多字节参数的小 Endian 码的一个例外。

事件参数：

Status: 大小：1 字节

表 11.528

值	参数说明
0x00	Remote_Name_Request 指令成功
0x01	Remote_Name_Request 指令失败，参见表 6.1

BD_ADDR : 大小：6 字节

值	参数说明
0xXXXXXXXXXXXX	被请求设备的 BD_ADDR

Remote_Name : 大小：248 字节

表 11.529

值	参数说明
名称[248]	远程设备的 UTF-8 编码的描述性名字。 UTF-8 编码名字可长达 248 字节。如果它短于 248 字节，则用 0x00 进行填充.

5.2.8 加密模式改变事件

表 11.530

事件	OCF	事件代码
加密模式改变事件	0x08	Status Connetion_handle Encryption_enable

说明：

加密模式改变事件用于表示已完成由 Connection_Handle 事件参数指定连接句柄的加密模式改变。Connection_Handle 为 ACL 连接的 Connection_Handle。Encryption_Enable

事件参数指定由 Connection_Handle 指定的连接句柄启用新的加密模式。该事件将在连接两端设备上发生，以通知两主机加密模式已改变。

事件参数：

Status: 大小：1 字节

表 11.531

值	参数说明
0x00	加密模式改变成功。
0x01	加密模式改变成功

Connection_Handle: 大小:2 字节(其中 12 位有意义)

表 11.532

值	参数说明
0xXXXX	同一蓝牙设备终端的所有连接句柄中启用或终止链路层加密的连接句柄。 范围：0x0000-0x0EFF(0x0F00-0x0FFF 保留)

Encryption_Enable ： 大小：1 字节

表 11.533

值	参数说明
0x00	停用链路层次加密。
0x01	启用链路层次加密。

5.2.9 连接链接字改变完成事件

表 11.534

事件	OCF	事件代码
连接链接字改变完成事件	0x09	Status, Conection_handle

说明：

连接链接字改变完成事件用于表示由 Connection_Handle 事件参数指定连接句柄的链接字改变已完成。Connection_Handle 为 ACL 连接的 Connection_Handle。该事件只发往发送 Change_Connection_Link_Key 指令主机。

事件参数：

Status: 大小：1 字节

表 11.535

值	参数说明
0x00	Change_Connection_Link_Key 指令成功
0x01	Change_Connection_Link_Key 指令失败

Connection_Handle: 大小：2 字节(其中 12 位有意义)

表 11.536

值	参数说明
0xXXXX	同一蓝牙设备终端的所有连接句柄中改变链接字的连接句柄。 范围：0x0000-0x0EFF(0x0F00-0x0FFF 保留)

5.2.10 主单元链接字完成事件

表 11.537

事件	OCF	事件代码
主单元链接字完成事件	0x0A	Status Connection_handle Key_flag

说明：

主单元链接字完成事件用于表示匹克网蓝牙主单元的临时链接字或半永久链接字改变已完成。Connection_Handle 为 ACL 连接句柄。连接所使用的链接字将为主设备的临时链接字，或由 Key_Flag 表示的半永久链接字。Key_Flag 事件参数用于表示当前在匹克网中使用的是哪个链接字(主单元临时链接字，或半永久链接字)。

注意:对于一主单元，从临时链接字到半永久链接字的变化将影响所有与匹克网有关的所有连接句柄。对于一从单元，此变化将仅仅影响某指定连接句柄。当广播和点对点通信都需要加密时，则必须使用临时链接字。

事件参数：

Status: 大小：1 字节

表 11.538

值	参数说明
0x00	Master_Link_Key 指令成功
0x01	Master_Link_Key 指令失败，参见表 6.1

Connection_Handle: 大小：2 字节(其中 12 位有意义)

表 11.539

值	参数说明
0xXXXX	对于同一匹克网中所有设备，链接字已改变的连接句柄。 范围：0x0000-0x0EFF(0x0F00-0x0FFF 保留)

Key_Flag ： 大小：1 字节

表 11.540

值	参数说明
0x00	使用半永久链接字
0x01	使用临时链接字

5.2.11 远程支持特性读取完成事件

表 11.541

事件	OCF	事件代码
远程支持特性读取完成事件	0x0b	Status Connection_handle LMP_features

说明

该事件用于表示获取由 Connection_Handle 指定远程蓝牙设备支持特性的链路管理器进程的结束。Connection_Handle 为一 ACL 连接的连接句柄。事件参数则包括 LMP 特性表。具体细节参见“链路管理器协议”。

事件参数：

Status: 大小：1 字节

表 11.542

值	参数说明
0x00	Read_Remote_Supported_Features 指令成功
0x01	Read_Remote_Supported_Features 指令失败，参见表 6.1 的出错代码列表。

Connection_Handle: 大小：2 字节(其中 12 位有意义)

表 11.543

值	参数说明
0xXXXX	连接句柄用于 Read_Remote_Supported_Features 指令，范围：0x0000-0x0EFF(0x0F00-0x0FFF 保留)

LMP_Features ： 大小:8 字节

表 11.544

值	参数说明
0xXXXXXXXX XXXXXXXX	LMP 屏蔽位列表，参见“链路管理器协议”。

5.2.12 远程版本信息读取完成事件

表 11.545

事件	OCF	事件代码
远程版本信息读取完成事件	0x0c	Status Connection_handle LMP_version Manufacturer_name LMP_subversion

说明：

该事件表示用于获取远程蓝牙设备版本信息的链路管理器进程的结束。该版本信息由 Connection_Handle 指定。Connection_Handle 为一 ACL 连接的连接句柄。LMP_Version 事件参数定义蓝牙硬件的主要硬件方案。只有符合新蓝牙 SIG 规范的蓝牙新硬件版本出现时，该事件参数才变化;也就是说，该事件参数由 SIG 控制。Manufacturer_name 参数表示远程蓝牙模块制造商。LMP_Subversion 事件参数应由制造商控制，并且可根据需要改变。LMP_Subversion 事件参数定义了当设计进程变化和错误得到修改时，蓝牙硬件的每一修订版本。该事件允许软件确定正在使用哪种蓝牙硬件，并且如果必要,将能够在硬件出错的环境下工作。

事件参数：

Status: 大小：1 字节

表 11.546

值	参数说明
0x00	Read_Remote_Version_Information 指令成功。
0x01	Read_Remote_Version_Information 指令失败，参见表 6.1 出错代码列表

Connection_Handle： 大小：2 字节(其中 12 位有意义)

表 11.547

值	参数说明
0xXXXX	连接柄用于 Read_Remote_Version_Information 指令 范围：0x0000-0x0EFF(0x0F00-0x0FFF)保留)

LMP_Version ： 大小：1 字节

表 11.548

值	参数说明
0xXX	远程蓝牙硬件当前 LMP 版本，参见表 5.2 链路管理协议指定值

Manufacturer_name: 大小：2 字节

表 11.549

值	参数说明
0xXXXX	远程蓝牙硬件制造商名称

LMP_Subversion: 大小：2 个字节

表 11.550

值	参数说明
0xXXXX	远程蓝牙硬件的当前 LMP 子版本

5.2.13 QoS 设置完成事件

表 11.551

事件	OCF	事件代码
QoS 设置完成事件	0x0d	Status Conection_handle Flags Service_type Token_rate Peak_bandwidth Latency Delay_variation

说明：

该事件表示由 Conection_handle 事件参数指定的远程蓝牙设备 QoS 的链路管理器设置进程结束。Conection_handle 为一 ACL 连接连接句柄。具体细节参见“逻辑链路控制和适配协议规范”。

事件参数：

状态: 大小：1 字节

表 11.552

值	参数说明
0x00	QoS_Setup 指令成功
0x01	QoS_Setup 指令失败

Conection_handle: 大小：2 字节(其中 12 位有意义)

表 11.553

值	参数说明
0xXXXX	连接柄用于 Qos_setup 指令 范围：0x0000-0x0EFF(0x0F00-0x0FFF 保留)

Flags: 大小：1 字节

表 11.554

值	参数说明
0x00-0xFF	保留

Service_Type ： 大小：1 字节

表 11.555

值	参数说明
0x00	无可用通信
0x01	允许最大传输能力
0x02	可用授权
0x03-0xFF	保留

Token_Rate ： 大小：4 字节

表 11.556

值	参数说明
0xXXXXXXXX	允许 Token_Rate，单位为字节/秒

Peak_Bandwidth ： 大小：4 字节

表 11.557

值	参数说明
0xXXXXXXXX	允许峰值带宽

latency: 大小：4 字节

表 11.558

值	参数说明
0xXXXXXXXX	允许延时，单位微秒

Delay_Variation ： 大小：4 字节

表 11.559

值	参数说明
0xXXXXXXXX	允许延迟值，单位微秒

5.2.14 指令完成事件

表 11.560

事件	OCF	事件代码
指令完成事件	0x0e	Num_hci_command_packets Command_opcod Return_parameters

说明：

该事件由主控制器用于传递大多数指令返回状态，以及其它已发出 HCI 指令的事件参数。Num_HCI_Command_Packets 事件参数允许主控制器指出主机可发往主控制器 HCI 指令分组个数。如果主控制器要求停止送指令，Num_HCI_Command_Packets 事件参数将设置为零。为了通知主机主控制器已准备好接收 HCI 指令分组，主控制器将生成 Command_Opcode 为 0x0000 的指令完成事件，并且 Num_HCI_Command_Packets 事件参数将设置为 1 或更大值。Command_Opcode（0x0000）为 NOP(空操作),并且用于改变主机进入等待状态前可发送的 HCI 指令分组的个数。

事件参数：

Num_HCI_Command_Packets: 大小：1 字节

表 11.561

值	参数说明
N=0xXX	可从 host 发往主控制器的 HCI 指令分组个数 N 取值范围：0-255

Command_Opcode ： 大小：2 字节

表 11.562

值	参数说明
0xXXXX	可引发该事件的指令的操作码

Return_Parameter ： 大小:取决于代码事件参数指令完全的 0x0E

表 11.563

值	参数说明
0xXX	Command_Opcode 事件参数指定指令的返回参数，参见与该指令相关的返回参数列表

5.2.15 指令状态事件

表 11.564

事件	OCF	事件代码
指令状态事件	0x0F	Status Num_HCI_command_packets Command_Opcode

说明：

该事件表示已收到由 Command_Opcode 参数描述的指令,且主控制器正在执行该指令任务。该事件需提供异步操作机制,以防止主机一直处于等待指令完成的状态。如果指令不能执行(可能由于参数错误或指令不允许),指令状态事件参数将包含相应出错代码，并且由于指令未执行则不会生成该指令完成事件。Num_HCI_Command_Packets 事件参数允许主控制器表示主机能发送至主控制器的 HCI 指令分组个数。如果主控制器要求停止发送指令，Num_HCI_Command_Packets 事件参数将置为 0。为了通知主机主控制器已准备好接收 HCI 指

令分组，主控制器将生成状态为 0x00、Command_Opcode 为 0x0000，以及 Num_HCI_Command_Packets 事件参数为 1 或更大值的指令状态事件。Command_Opcode（0x0000）为 NOP(空操作)，并且用于改变主机进入等待状态前可接收 HCI 指令分组的个数。

事件参数：

Status: 大小：1 字节

表 11.565

值	参数说明
0x00	指令当前正在执行
0x01	指令失败，参见出错代码列表

Num_HCI_Command_Packets ： 大小：1 字节

表 11.566

值	参数说明
N = 0xXX	允许从主机发往主控制器的 HCI 指令分组数 N 取值范围:0-255

Command_Opcode ： 大小:2 字节

表 11.567

值	参数说明
0xXXXX	引发该事件，且正在执行指令的操作码

5.2.16 硬件故障事件

表 11.568

事件	OCF	事件代码
硬件故障事件	0x10	Hardware_code

说明：

硬件故障事件用于表示蓝牙设备的硬件故障类型。该事件也用于通知主机蓝牙模块已发生故障。

事件参数：

Hardware_Code ： 大小：1 字节

表 11.569

值	参数说明
0x00	Hardware_Codes 因不同实现而定，且可指定为不同硬件故障

5.2.17 刷新事件

表 11.570

事件	OCF	事件代码
刷新事件	0x11	Connection_handle

说明：

刷新事件用于表示对于特定连接句柄，已将用于传输的当前用户数据删除。Connection_handle 为 ACL 连接的连接句柄。这主要是由于刷新指令，或发生自动刷新。在

主控制器中，一 L2CAP 分组的多个数据块已待定。如果 L2CAP 分组的基带分组部分被刷新，则 L2CAP 分组的 HCI 数据分组的其余部分也必须刷新。

事件参数：

Connection_handle： 大小：2 字节(其中 12 位有意义)

表 11.571

值	参数说明
0xXXXX	已刷新连接句柄 范围：0x0000-0x0EFF(0x0F00-0x0FFF 保留)

5.2.18 角色变化事件

表 11.572

事件	OCF	事件代码
角色变化事件	0x12	Status BD_ADDR NEW_ROLE

说明：

角色变化事件用于表示与特定连接有关的当前蓝牙角色已改变。只有当与 BD_ADDR 事件参数相关的远端和本地蓝牙设备已完成其角色变化时，该事件才发生。当角色已改变后，该事件将通知连接两端设备。

事件参数：

状态: 大小：1 字节

表 11.573

值	参数说明
0x00	发生角色变化
0x01	角色变化失败，参见 745 页表 6.1 出错代码列表

BD_ADDR ： 大小：6 字节

值	参数说明
0Xxxxxxxxxxxx	角色改变设备的 BD_ADDR

New_Role ： 大小：1 字节

表 11.574

值	参数说明
0x00	对应于指定 BD_ADDR 的主单元
0x01	对应于指定 BD_ADDR 的从单元

5.2.19 完成分组数事件

表 11.575

事件	OCF	事件代码
完成分组数事件	0x13	Number_of_handles Connection_handle Hc_num_of_completed_packets

说明：

该事件由主控制器用于通知主机自从前一完成分组数事件发往主机后，对于每一连接句

柄，已完成(发送或刷新) 传输的 HCI 数据分组个数。也就意味着，主控制器相应缓冲区空间也已释放。基于该信息，以及 Read_Buffer_Size 指令的返回参数 HC_Total_Num_ACL_Data_Packets 和 HC_Total_Num_SCO_Data_Packets,主机就能确定以后的 HCI 数据分组将使用何连接句柄发往主控制器。在相应连接完成事件发生前，不应发送该事件。当主控制器在其缓冲区缓存 HCI 数据分组时，它必须向主机周期性持续发送完成分组数事件,直到它最终报告所有待处理 ACL 数据分组都已发送或刷新为止。事件及其发送速率由制造商指定。

注意：如果停用 SCO 流控制，将不能报告对应于 SCO 连接句柄的完成分组数事件。

事件参数：

Number_of_Handles ： 大小：1 字节

表 11.576

值	参数说明
0xXX	本事件包含的 Num_HCI_Data_Packets 参数对和连接句柄数量。范围：0-255

Connection_handle[I]: 大小:Number_of_Handles*2 字节(其中 12 位有意义)

表 11.577

值	参数说明
0xXXXX	连接句柄 范围:0x0000-0x0EFF(0x0F00-0x0FFF 保留)

HC_Num_Of_Completed_Packets ： 大小：2 字节

表 11.578

值	参数说明
N = 0xXXXX	自从前一事件返回后，对应于相关连接句柄的已完成(发送或刷新)的 HCI 数据分组数 N 取值范围:0x0000-0xFFFF

5.2.20 模式变化事件

表 11.579

事件	OCF	事件代码
模式变化事件	0x14	Status Connection_handle Current_mode Interval

说明：

该事件用于表示与特定连接句柄相关联的设备在激活、保持、呼吸和休眠模式之间何时发生变化。Current_mode 为一 ACL 连接的连接句柄。Current_mode 事件参数用于表示模式变化事件相对于哪一个连接句柄发生。该参数也可用于表示连接当前处于哪一状态。Interval 参数则用于指定每一状态的持续时间。每一与已发生模式变化的连接句柄相关联的主控制器都将发送一模式变化事件到主机。

事件参数：

Status: 大小：1 字节

表 11.580

值	参数说明
0x00	发生模式变化事件
0x01-0xFF	Hold_Mode 、 Sniff_Mode 、 Exit_Sniff_Mode 、 Park_Mode ， 或 Exit_Park_Mode 指令失败。

Connection_handle: 大小：2 字节(其中 12 位有意义)

表 11.581

值	参数说明
0xXXXX	连接句柄 范围：0x0000-0x0EFF(0x0F00-0x0FFF 保留)

crrent_Mode ： 大小：1 字节

表 11.582

值	参数说明
0x00	激活模式
0x01	保持模式
0x02	呼吸模式
0x03	休眠模式
0x04-0xFF	保留

间歇: 大小：2 个字节

表 11.583

值	参数说明
N = 0xXXXX	保持： 保持模式等待的基带时隙数。 保持间隔= N * 0.625 ms N 取值范围：0x0000-0xFFFF 时间范围：0-40.9 秒 呼吸： 呼吸间隔之间的基带时隙数 呼吸间隔之间的时间= 0.625 ms N 取值范围：0x0000-0xFFFF 时间范围：0-40.9 秒 休眠： 连续信号灯之间的基带时隙数。 间隔时间= N * 0.625 ms N 取值范围：0x0000-0xFFFF 时间范围：0-40.9 秒

5.2.21 链接字返回事件

表 11.584

事件	OCF	事件代码
链接字返回事件	0x15	Num_keys BD_ADDR Link_key

说明：

该事件由主控制器用于向主机发送一个或多个存储链接字。在 Read_Stored_Link_Key 指令发出以后,将不发生或发生多个事件实例。当无存储链接字时，将不返回链接字事件。

当有存储链接字时，在每一链接字返回事件中返回的链接字数量将根据具体实现而定。

事件参数：

Num_Keys ： 大小：1 字节

表 11.585

值	参数说明
0xXX	该事件所包含的链接字数 范围：0x01-0xFF

BD_ADDR [I]: 大小：6* Num_Keys 字节

表 11.586

值	参数说明
0xXXXXXXXXXX	对应于相关链接字的 BD_ADDR

Num_Keys Link_Key [I]: 大小:16 字节

表 11.587

值	参数说明
0xXXXXXXXXXX XXXXXXXXXX XXXXXXXXXX	对应于相关 BD_ADDR 的链接字

5.2.22 PIN 码请求事件

表 11.588

事件	OCF	事件代码
Pin code request	0x16	BD_ADDR

说明：

该事件用于表示需要一 PIN 码以创建新的链接字。主机是采用 PIN 码请求应答，还是采用 PIN 码消极请求应答，取决于主机是否能够为主控制器提供 PIN 码。

注意:如果 PIN 码请求事件被屏蔽,则主控制器就假设主机无 PIN 码。

当主控制器生成一 PIN 码请求事件,以便本地链路管理器对来自远程链路管理器的请求应答时(作为来自远程主机的 Create_Connection 或 Authentication_Requested 指令的结果），本地主机必须在远程链路管理器检测到 LMP 应答超时之前，使用 PIN_Code_Request_Reply 或 PIN_Code_Request_Negative_Reply 指令应答。(参见“链路管理器协议”)。

事件参数：

BD_ADDR: 大小：6 字节

表 11.589

值	参数说明
0XxxxxxxXXXXXX	新链接字所属设备的 BD_ADDR

5.2.23 链接字请求事件

表 11.590

事件	OCF	事件代码
链接字请求事件	0x17	BD_ADDR

说明：

该事件用于表示需要针对指向 BD_ADDR 指定设备的连接创建一链接字。如果主机具有被请求链接字，则主机将使用 Link_Key_Request_Reply 指令将该被请求链接字送往主控制器。如果主机不含被请求链接字，则主机将使用 Link_Key_Request_Negative_Reply 指令通知主机该主机不含被请求链接字。

注意:如果链接字请求事件被屏蔽,则主控制器将假设主机不含其它链接字。

当主控制器生成一链接字请求事件，以便本地链路管理器对来自远程链路管理器的请求应答时(作为来自远程主机的 Create_Connection 或 Authentication_Requested 指令的结果），本地主机必须在远程链路管理器检测到 LMP 应答超时之前，使用 Link_Key_Request_Reply 或 Link_Key_Request_Negative_Reply 指令应答。(参见“链路管理器协议”)。

事件参数：

BD_ADDR ： 大小:6 字节

表 11.591

值	参数说明
0xXXXXXXXXXXXX	储存链接字所属设备的 BD_ADDR

5.2.24 链接字通知事件

表 11.592

事件	OCF	事件代码
链接字通知事件	0x18	BD_ADDR Link_key

说明：

该事件用于通知主机已针对指向 BD_ADDR 指定设备的连接创建了一个新链接字。主机将在其存储设备中保存该新链接字，以便将来使用。并且，主机将使用 Link_Key_Request_Reply 指令将该链接字存储在主控制器的链接字存储设备中。

事件参数：

BD_ADDR ： 大小: 6 字节

表 11.593

值	参数说明
0xXXXXXXXXXXXX	生成新链接字设备的 BD_ADDR

Link_Key ： 大小:16 字节

表 11.594

值	参数说明
0xXXXXXXXXXX XXXXXXXXXX XXXXXXXXXX	与 BD_ADDR 相关联的链接字

5.2.25 回送指令事件

表 11.595

事件	OCF	事件代码
回送指令事件	0x19	HCI_command_packet

说明：

处于本地回送模式时，主控制器将回送指令和数据到主机。回送指令事件用于返回含例外情况的所有从主机发往主控制器的命令。参见“Read_Loopback_Mode”中有关不能回送指令的情况。HCI_Command_Packet 事件参数包含所有包含头的 HCI 分组。

注意:事件分组有效载荷最大值为 255 字节。由于 HCI 指令头数据长为 3 字节,则只返回开始 252 字节的指令参数。

事件参数：

表 11.596 HCI_Command_Packet　　大小:因指令而异

值	参数说明
0xXXXXXX	HCI 指令分组,包括头

5.2.26 数据缓冲区溢出事件

表 11.597

事件	OCF	事件代码
数据缓冲区溢出事件	0x1A	Link_type

说明：

该事件用于表示主控制器数据缓冲区已溢出。如果主机发送分组数量超过限制时将引发该事件。Link_Type 参数用于表示溢出是由 ACL 数据还是由 SCO 数据引起的。

事件参数：

表 11.598 Link_Type　　大小: 1 字节

值	参数说明
0X00	SCO 缓冲区溢出(语音信道)
0X01	ACL 缓冲区溢出(数据信道)
0x02-0xFF	保留

5　错误码表

6.1 错误码表

本节列出各种可能的错误码。当一指令失败时，将返回指示错误原因的错误码。错误码长度为一个字节,错误码允许范围是 0X01-0XFF。 6.2 节给出了错误码的用法描述。

表 5.56

错误码	描述
0X01	未知的 HCI 指令
0X02	不能连接
0X03	硬件故障
0X04	呼叫超时
0X05	身份验证失败
0X06	键丢失
0X07	存储器已满
0X08	连接超时
0X09	最大连接数
0X0A	连接到设备 A 的最大 SCO 连接数
0X0B	ACL 连接已存在
0X0C	指令非法
0X0D	由于资源有限，主机被拒绝
0X0E	由于安全原因，主机被拒绝

0X0F	由于远程设备是一个人设备，主机被拒绝。
0X10	主机超时
0X11	不支持的特性或参数值
0X12	非法的主控制器接口指令参数
0X13	由于另一端引起连接中断：用户中断连接
0X14	由于另一端引起连接中断：资源限制
0X15	由于另一端引起连接中断：关机
0X16	本地主机中断连接
0X17	重复尝试
0X18	不允许匹配
0X19	未知的 LMP PDU
0X1A	不支持的远程特性
0X1B	拒绝 SCO 补偿
0X1C	拒绝 SCO 间歇模式
0X1D	拒绝 SCO 无线模式
0X1E	非法链路管理器协议（LMP）参数
0X1F	未特别指明的错误
0X20	不支持的链路管理器协议参数值
0X21	不允许的角色改变
0X22	链路管理器协议响应超时
0X23	链路管理器协议错误处理事务冲突
0X24	不允许的 LMP PDU
0X25-0XFF	保留

6.2 主控制器接口，错误码用法描述：

本节目的是给出错误码的具体描述。这远远超出了本文件所给出的使用错误码具体描述的范围，使用方式根据具体实现而定。但是，一些特殊情况下错误码的使用描述应更详尽、通俗易懂。

下面错误码仅仅用于链路管理器协议报文，因此本节不作描述：

未知的链路管理器协议的协议数据单元 （ 0x19 ）

同步面向连接拒绝（ 0x1B ）

同步面向连接间隔拒绝（ 0x1C ）

同步面向连接 无线模式拒绝（ 0x1D ）

错误的链路管理器协议参数（ 0x1E ）

可以根据具体实现，决定是在指令状态事件中还是在发出指令相关事件中（跟随一个带有状态=0x00 的状态指令）返回错误码。在这些情况下，不能由于错误而执行该指令，因此推荐使用指令状态事件。采用该动作的原因在于指令状态事件不可能适用于所有软件体系结构。

6.3 未知的主控制器接口指令（ 0X01 ）

当主控制器收到带有不能识别操作码的主控制器接口指令分组时，主控制器在指令完成事件的状态参数中或在指令状态事件中返回“ 未知的主控制器接口指令”。给定操作码可能不对应于任何一个本文件中定义的操作码，或任何厂商指定操作码，或是可能还未执行的指令。如果返回一个指令完成事件，状态参数是唯一包含在 Return_parameters 事件参数中的参数 。使用何事件应根据具体实现而定。

6.4 不能连接 （ 0X02 ）

当主机发出一个请求连接的指令，并且当前不存在一个对应于指定连接句柄或 BD 地址的连接时，主控制器将在某一事件的状态参数中返回“ 不能连接”错误码。如果发出指令为一条要求必须返回指令完成事件的指令，则该包含错误码的事件就是指令完成事件。否则，该包含错误码的事件是指令状态事件或与发出指令有关的事件。这取决于实际情况。

6.5 硬件故障(0X03)

当主机发出了一条指令，但该指令由于硬件故障不能执行时，主控制器将在事件状态参数中返回错误码---“硬件故障”。如果发出指令为一要求必须返回指令完成事件的指令，那么该包含错误码的事件为指令完成事件。否则，该包含错误码的事件为指令状态事件或与发出指令有关的事件（在收到状态=0x00 的指令状态事件之后）。

6.6 呼叫超时(0X04)

如果主机发出一个 Create_Connection 指令，而且要连接的设备在呼叫定时器失效前没有在基带层次上进行应答，主控制器将在连接完成事件的状态参数中返回错误码‘呼叫超时’。当主机已发出 Remote_Name_Request 指令以建立临时连接，但又发生呼叫超时的时候，也可以在 Remote_Name_Request 的状态参数中返回错误码。（呼叫超时用 Write_Page_Timeout 指令设置）

6.7 验证失败(0X05)

当由于丢失 PIN 码或链接字导致匹配/验证计算结果错误，进而引起匹配或验证失败时，主控制器将在连接完成事件或验证完成事件的状态参数中返回“验证失败”错误码。

6.8 键丢失(0X06)

当由于失去 PIN 码而导致匹配失败时，主控制器将在连接完成事件或验证完成事件的状态参数中返回“键丢失”错误码。

6.9 存储器已满(0X07)

当主机发出一指令时，该指令要求主控制器保存新参数，但主控制器制器并无对该指令的存储能力，主控制器将在指令完成事件的状态参数中返回“存储器已满”错误码。这种情况可能是在 Set_Event_Filter 指令发出以后。对于 Write-Stored-Link-Key 指令，当主控制器不能够存储更多连接字时，将不返回错误码。主控制器根据可用于保存链接字的空闲空间存储连接字，并且将把可存储链接字的数量通知主机。

6.10 连接超时(0X08):

注意：该错误码可用于指示连接断开的原因。它通常在连接断开完成事件的原因参数中返回。因此在下述描述中它可称为原因码。

当链路监控定时器(看后面的“基本频带定时器”)失效，并因此考虑释放链路时，主控制器将在一事件中发出“连接超时”原因码。连接监控超时可使用 Write_Link_Supervision 超时进行设置。返回该原因码的事件通常是连接断开完成事件。连接双方将返回该事件，而主控制器则将采用对应于连接到其他设备的物理链路连接句柄，向主机发送一连接断开完成事件。(当连接完成事件中返回原因码时，将可以在连接建立期间检测链路丢失)。

6.11 最大连接数(0X09)

当蓝牙模块不能再设置连接时，主控制器将在指令状态事件、连接完成事件或远程命名请求完成事件的状态参数中返回“最大连接数”错误码。是在连接完成事件，还是在指令状

态事件(其中，指令状态事件中状态=0x00)之后的事件中返回该错误，这取决于实际实现情况。该错误原因可能是由于硬件或固件限制而引起的。在返回错误以前，主机发出Create_Connection 指令、Add_SCO_Connection 或 Remote_Name_Request。当需要建立一个临时连接以请求一名字时，可以在远程命名请求完成事件中返回“最大连接数”错误码。

6.12 设备最大 SCO 连接数（0X0A）

当达到设备最大 SOC 连接数时，主控制器将在指令状态事件或连接完成事件的状态参数中返回此错误码。而到底使用这两个事件中的哪一个取决于实际实现。该设备应是由先前发出的 Add_SCO_Connection 指令指定的设备。

6.13 ACL 连接已存在”（ 0X0B ）

当与一设备已有ACL连接，并且主机又试图使用Create_Connection建立另外一个连 接时，主控制器将在指令状态事件或连接完成事件的状态参数中返回“ACL 连接已存在”错误码。其中，连接完成事件在状态=0x00 的指令状态事件之后)。具体使用哪一事件取决于实际实现。

6.14 指令不允许（ 0X0C ）

当主控制器处于准备接收带有某些操作码的指令，并且收到的 HCI 指令分组不包含这些操作码时，主控制器将在指令完成事件或指令状态事件的参数中返回“指令不允许”错误码。如果发出指令是一个要求返回指令完成事件的指令，应使用指令完成事件。否则，则使用指令状态事件。主控制器不必使用“未知的 HCI 指令”错误码，因为这会需要对收到的操作码进行不必要的处理。何时使用“指令不允许”错误码主要根据实际实现情况而定。例如，有些应用在连接请求、链路字请求或 PIN 码请求事件之后只能接受合适的 HCI 应答指令。

注:通常允许复位指令。

6.15 由于某种原因主机被拒绝（ 0X0D-0X0F）

注意:这些错误码通常用于指示拒绝呼入连接的原因。因此在下列描述中它们将被称为原因码。

当主机已收到一个连接请求事件，并且主机通过发出 Reject_Connection_Request 指令拒绝呼入连接时，就可以使用一个原因码作为原因参数的值。在发出 Reject_Connection_Request 指令后，由主控制器返回的指令状态事件（STATUS=0x00）将紧接着返回状态参数含已发出原因码的连接完成事件。而在 Reject_Connection_Request 指令的原因参数中的原因代码也将通过无线发出,其目的就是使它能在初始化方的连接完成事件中返回。在此之前，初始化方应已发出 Create_Connection 指令或 Add_SCO_Connection 指令，并已收到指令状态事件(状态参数=0x00).

6.16 主机超时（ 0X10 ）

注意:该错误码用于指示拒绝呼入连接的原因。因此在下列描述中它将被称为原因码。

假定主机已收到一个连接请求事件,而且在连接定时器(其连接接受超时可使用 Write_Connection_Accept_Timeout 进行设置）终止前，主机没有发出 Accept_Connection_Request 指令或 Reject_Connection_Request 指令。在这种情况下，主控制器将发出一状态参数中含 " 主机超时 " 原因码的连接完成事件。该原因码可通过无线发送，以便可在初始化方连接完成事件中返回。在这以前，初始化方已发出一条 Create_Connection 指令或 Add_SCO_Connection 指令，并已收到一指令状态事件(状态参数=0x00)。

6.17 不支持的特性或参数值(0X11)

当主控制器收到了含有一个或多个不被硬件支持的参数值的指令时,主控制器将在事件状态参数中返回 " 不支持特性或参数值 " 错误码。但是,这些参数应在本文件指定允许的参数范围以内。如果发出指令为一要求返回指令完成事件的指令,那么该包含错误码的事件为一指令完成事件。否则,该包含错误码的事件为一指令状态事件或与发出指令有关的事件(在含有状态参数=0x00 的指令状态事件之后)。

6.18 HCI 指令参数非法(0X12)

当总的参数长度(或收到指令中的一个或多个参数值)不符合本文件所指定长度,主控制器将在事件的状态参数中返回 " 错误的 HCI 指令参数 " 错误码。

尽管参数值在允许参数范围内,但如果该参数值当前不被允许,也将返回错误码。例如:当一指令需要一个 ACL 连接句柄,但主机已将 SCO 连接句柄作为参数的情况下。还有,主控制器通过事件请求一个链接字、一个 PIN 码或一个呼入连接应答时,主机使用含未收到请求 BD_ADDR 的应答指令进行应答。

如果发出指令是要求返回指令完全事件的指令,则包含错误码的事件为指令完成事件。否则,包含错误码的事件为指令状态事件或与发出指令有关的事件(在 STATUS=0x00 指令状态事件跟随一个带有状态=0x00 的指令状态事件)。

6.19 其它终端终止连接 (0X13-0X15)

注意:该错误码用于指示连接断开原因。因此它们在以下描述中称为原因码。

当主单元发出连接断开指令时,将把一个原因码作为原因参数值使用。“本地主机终止连接”原因参数将于主控制器在发出连接断开指令之后,返回连接断开事件(状态=0x00),并在此之后在连接断开完成事件的原因参数中返回。连接断开指令的原因参数中发出的原因代码将通过无线发出,以便能够在远程连接断开完成事件的原因参数中再次返回。

6.20 本地主机终止连接(0X16)

参见 6.19 节说明。由于它在连接断开完成事件的原因参数中返回,该错误码称为原因码。

6.21 重复尝试(0X17)

当设备由于验证或匹配失败的原因而没有更多时间再进行验证或匹配时,主控制器将在连接完成事件或验证完成事件的状态参数中返回 " 尝试重复 " 错误码。参见“链路管理器协议”中对重复尝试工作机制的描述。

6.22 不允许匹配(0X18)

当设备由于某些原因不允许匹配时,主控制器将在连接完成事件或验证完成事件的状态参数中返回“不允许匹配”错误码。例如: PSTN 适配器就只允许在按下该适配器的一个按键之后的某一时间段内进行匹配(在适配器的一个按键被按了以后)配对。

6.23 “不支持的远程特性”(0X1A)

当指令参数中指定的远程设备不支持与发出指令有关的特性时,主控制器将在与发出指令有关事件的状态参数中返回”不支持的远程特性”错误码。该错误码也可用作连接断开指令的原因参数值。该错误码将通过无线方式发送,以便它能够在远端连接断开事件的原因参数中返回。在连接断开指令发出方的指令状态事件(状态=0X00)之后的连接断开完成事件中,

原因参数将包含原因码“本地主机终止连接”.("不支持远程特性"错误码在 LMP 规范中称为“不支持的 LMP 特性”,参见“链路管理器协议”。)

6.24 未定义错误(0X1F)

当本文件没有指定适用错误码时，适用“未定义错误”错误码。

6.25 不支持的 LMP 参数值(0X20)

当指令参数中指定的远程设备返回包含 LMP 错误码 0x20（即：不支持的 LMP 参数值）的 LMP 消息时，主控制器将在与发出指令有关事件的状态参数中返回“不支持的 LMP 参数值”错误码(参见 LMP)。

6.26 不允许的角色变化(0X21)

当不允许角色变化时,主机在连接完成事件或角色变化事件状态参数中返回“不允许的角色变化”错误码。如果本地主机发出 Switch_Role 指令，但远程设备拒绝角色变化,那么错误码将在角色变化事件中返回。如果由于设备接受一个呼入 ACL 连接和角色变化请求，而角色变化又被初始化设备拒绝,从而引起连接失败时,错误码将在两端连接完成事件中返回。

6.27 LMP 应答超时(0X22)

当远程设备在 LMP 最大应答时间内，不能对来自本地设备的 LMP PDU 进行应答时，主控制器将在指令完成事件或与发出指令（在状态=0X00 的指令状态事件之后）有关事件的状态参数中返回“LMP 应答超时”错误码。(参见 LMP)

6.28 LMP 错误处理冲突(0X23)

当指令参数所指定的远程设备返回包含 LMP 错误码(0x23)--“LMP 错误处理冲突”的 LMP 消息，主控制器将在与发出信号有关的事件状态参数中返回“LMP 错误处理冲突”错误码。(参见 LMP)。

6.29 不允许的链路管理器协议 PDU(0X24)

当指令参数所指定的远程设备返回包含 LMP 错误码 0x24—“不允许的链路管理器协议 PDU”的 LMP 消息时，主控制器将在与发出信号有关的事件状态参数中返回本错误码.(参见 LMP)。

7. 同义词和缩写

ACL 异步无连接
BD_ADDR 蓝牙设备地址
DH 高速
DIAC 精确查询识别码
DM 中速
DUT 中试设备
DV 数据语音
GIAC 通用查询识别码
HCI 主控制器接口
L2CAP 逻辑链路控制和适配协议
L_CH 逻辑信道

LAP	低地址段
LC	链路控制器
LM	链路管理器
LMP	链路管理器协议
OCF	操作码指令域
OGF	操作码组域
RF	射频
RSSI	接收信号场强
SCO	异步面向连接
TBD	待定义
UA	用户异步
US	用户同步
USB	通用串口总线

第 12 章 HCI USB 传输层

HCI 文件附录之一

本文件描述 USB 传输层（介于主机和主控制器之间）、HCI 指令，以及该层的事件和数据分组流，但该层不对分组进行解码。

目 录

1.概述

本文件描述蓝牙硬件 HCI（USB）的要求。读者应熟悉 USB、USB 设计、高级配置电源接口（ ACPI ）、综合蓝牙体系结构，以及无线接口基础。读者也应熟悉蓝牙主控制器接口。

参见下图 1.1,本文件讨论标有“USB 功能”双向箭头的实现细节。

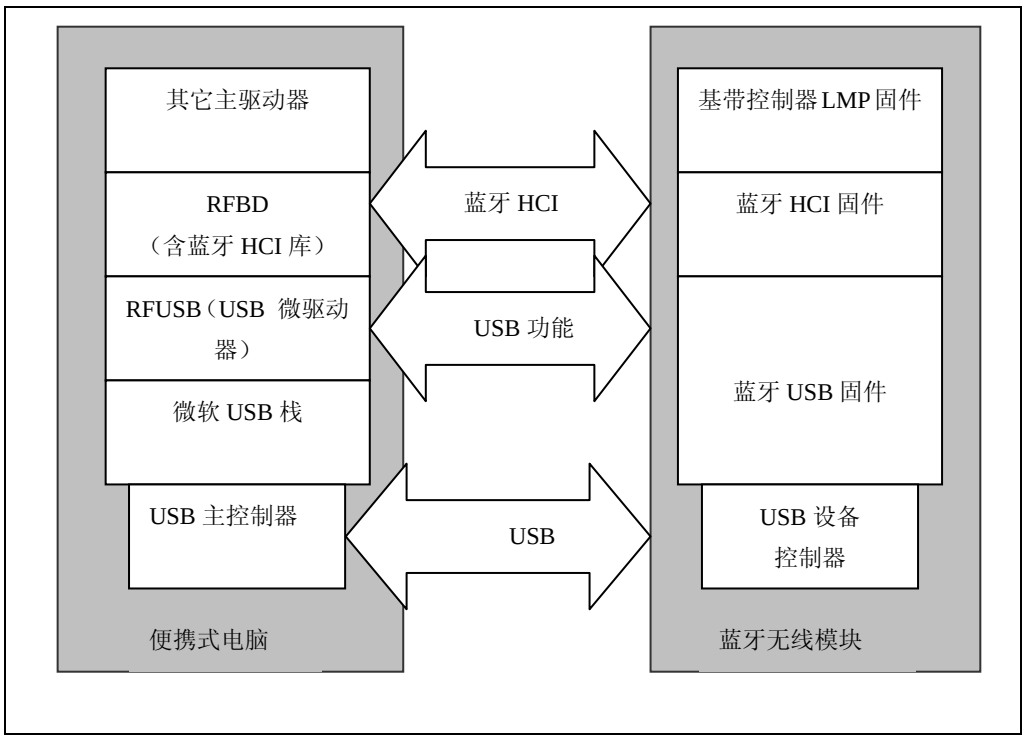


图 12.1　主机和蓝牙无线模块之间的关系

USB 硬件可以两种方式嵌入：

1．作为一个 USB 加/解密芯片 ，

2．集成到笔记本主板；

最后，对于两蓝牙设备之间的连接建立过程参见图 1.2。

图 12.2 两蓝牙设备间的数据流向

2. HCI 终端要求

本节概述用于与主机更好工作的 USB 终端。本节假定读者基本熟悉 USB。终端号（以下称为“建议终端地址”）可在驱动程序初始化时动态识别。这将根据具体实现而定。

2.1 描述符概述

USB 设备可看作高速设备。其固件配置由两个接口组成。第一个接口(接口 0)为固定设置，并包含 BULK 和中断终端。第二个接口(接口 1)提供可扩展的同步带宽占用方式。该接口方式提供四种设置，以提供基于同步带宽需求的占用方式。其缺省接口为空,以使设备能够支持非同步带宽。

一个 HCI 帧，包含一个 HCI 头和 HCI 数据，应包含于一 USB 事务中。一 USB 事务为一个或多个包含 I/O 请求数据的 USB 帧。例如,包含 256 字节的 ACL 数据分组(包括 HCI 头和 HCI 数据)将在一 I/O 请求中通过 BULK 终端发送。该 I/O 请求将需要四个 64 字节的 USB 帧，并组成一个事务。

当通过选择接口呼叫调整同步带宽占用方式时,终端可自由选择两种接口,以便不会中断或重新提交任何中间 BULK 或中断事务。下表描述所需配置：

表 12.1

接口号	可选设置	推荐端地址	端类型	推 荐 最大分组尺寸
HCI 指令				
0	0	0X00	控制	8/16/32/64
HCI 事件				
0	0	0X81	中断（IN）	16
ACL 数据				
0	0	0X82	BULK（IN）	32/64
0	0	0X02	BULK（OUT）	32/64
无激活语音信道（兼容 USB）				
1	0	0X83	ISOCH（IN）	9
1	1	0X03	ISOCH（OUT）	9
一条 8 位编码的语音信道				
1	1	0X83	ISOCH（IN）	9
1	1	0X03	ISOCH（OUT）	9
两条 8 位编码的语音信道和一条 16 位编码的语音信道				
1	2	0X83	ISOCH（IN）	17
1	2	0X03	ISOCH（OUT）	17

三条 8 位编码的语音信道				
1	3	0X83	ISOCH（IN）	25
1	3	0X03	ISOCH（OUT）	25
两条 16 位编码的语音信道				
1	4	0X83	ISOCH（IN）	33
1	4	0X03	ISOCH（OUT）	33
三条 16 位编码的语音信道				
1	5	0X83	ISOCH（IN）	49
1	5	0X03	ISOCHOUT）	49

下面两例描述了终端给定数据流。

语音信道数 1	语音数据持续时间 3ms/ IO 请求	编码 8 位

表 12.2

时 间（微秒）	USB 数据（数据头参照 HCI 头，发自主机）	数 据 队 列（读/写）	时间（微秒）	无线数据	收/发 数量（微秒）
0	收到 0 个字节，发送 9 个字节（3 个头，6 个数据）	0/6	0	发送 0	0/0
		10/6	0．625	收到 10	1．25/0
1	收到 0 个字节，发送 9 个字节（9 个字节 HCI 数据）	10/15	1．25	发送 0	1．25/0
		20/15	1．875	．收到 10	2．50/0
2	收到 0 个字节，发送 9 个字节（9 个字节 HCI 数据）	20/24	2．50	SEND 0	2．50/0
		30/24	3．125	收到 10	3.75/0
3	收到 9 个字节(3 个头,6 个数据，发送 9 个字节(3 个头,6 个数据	24/20	3.75	发送 10	3.75/1.25
4	收到 9 个字节(9 个字节数据)，发送 9 个字节(9 个字节 HCI 数据)	25/29	4.375	收到 10	5.0/1.25
5	收到 9 个字节(9 个字节数据)，发送 9 个字节(9 个字节 HCI 数据)	16/28	5.0	发送 10	5.0/2.5
		26/28	5.625	收到 10	6.25/2.5

6	收到 9 个字节(3 头,6 数据，发送 9 个字节(3 头,6 数据	20/24	6.25	发送 10	6.25/3.75
		30/24	6.875	收到 10	7.5/3.75
7	收到 9 个字节(9 个字节数据)，发送 9 个字节(9 个字节 HCI 数据)	21/23	7.5	发送 10	7.5/5.0
8	收到 9 个字节(9 个字节数据)，发送 9 个字节(9 个字节 HCI 数据)	22/32	8.125	收到 10	8.75/5.0
		22/22	8.75	发送 10	8.75/6.25
9	收到 9 个字节(9 个字节数据)，发送 9 个字节(9 个字节 HCI 数据)	26/28	9.375	收到 10	10.0/6.25
10	收到 9 个字节(9 个字节数据)，发送 9 个字节(9 个字节 HCI 数据)	17/27	10	发送 10	10.0/7.5
		27/27	10.625	收到 10	11.25/7.5
11	收到 9 个字节(9 个字节数据)，发送 9 个字节(9 个字节 HCI 数据)	18/26	11.25	发送 10	11.25/8.75

因为无线发送器平均以每 1 毫秒发送 8 字节语音数据的速度，而 USB 每 1 毫秒发送 8 字节语音数据，所以将要求聚集。

表 12.3

语音信道数	语音数据持续时间	编码
2	每一 IO 请求 3 毫秒	8 位

1	信道#1 收到 0 个字节，信道#1 发送 17 个字节(17 个字节 S,HCI 数据)	C1-20/31 C2-0/0	1.25	发送 0 到 C2	C1-2.5/0 C2-0/0

时间（毫秒）	USB（数据头参照 HCI 头，并发自主机）	数据队列（读/写）	时间（毫秒）	无线数据	收/发数量（毫秒）
0	信道#1 收到 0 个字节，信道#1 发送 17 个字节(3 头,14 数据)	C1-0/14 C2-0/0	0	发送 0 到 C1	C1-0/0 C2-0/0
		C1-20/14 C2-0/0	0.625	C1 收到 20	C1-2.5/0 C2-0/
		C1-20/31 C2-20/0	1.875	C2 收到 20	C1-2.5/0 C2-2.5/0

2	信道#1 收到 0 个字节，信道#1 发送 17 个字节(17 个字节 S,HCI 数据)	C1-20/28 C2-20/0	2.50	发送 20 到 C1	C1-2.5/2.5 C2-2.5/0
		C1-40/28 C2-20/0	3.125	C1 收到 20	C1-5.0/2.5 C2-2.5/0
3	信道#2 收到 0 个字节，信道#2 发送 17 个字节(3 头,14 数据)	C1-40/28 C2-20/14	3.75	发送 0 到 C2	C1-5.0/2.5 C2-2.5/0
4	信道#2 收到 0 个字节，信道#2 发送 17 个字节(17 个字节 S,HCI 数据)	C1-40/28 C2-40/31	4.375	C2 收到 20	C1-5.0/2.5 C2-50/0
5	信道#2 收到 0 个字节，信道#2 发送 17 个字节(17 个字节 S,HCI 数据)	C1-40/8 C2-40/48	5.0	发送 20 到 C1	C1-5.0/5.0 C2-5.0/0
		C1-60/8 C2-40/48	5.625	发送 20 到 C1	C1-7.5/5.0 C2-7.5/2.5
6	信道#1 收到 17 个字节，信道#1 发送 17 个字节(3 个头,14 个数据)	C1-46/22 C2-40/48	6.25	发送 20 到 C2	C1-7.5/5.0 C2-5.0/2.5
		C1-46/22 C2-60/48	6.875	C2 收到 20	C1-7.5/5.0 C2-7.5/2.5
7	信道#1 收到 17 个字节，信道#1 发送 17 个字节(17 个字节 S,HCI 数据)	C1-29/19 C2-60/48	7. 5	发送 20 到 C1	C1-7.5/7.5 C2-7.5/2.5
8	信道#1 收到 17 个字节，信道#1 发送 17 个字节(17 个字节 S,HCI 数据)	C1-32/36 C2-60/28	8.125	C1 收到 20	C1-10/7.5 C2-7.5/5.0
		C1-32/36 C2-60/8	8.75	C2 发送 20	C1-10/7.5 C2-7.5/5.0
9	信道#2 收到 17 个字节，信道#2 发送 17 个字节(3 头,14 数据)	C1-32/36 C2-54/22	9.375	C2 收到 20	C1-10/7.5 C2-10/5.0
10	信道#2 收到 17 个字节(17 个字节数据)，信道#2 发送 17 个字节(17 个字节 S HCI 数据)	C1-32/16 C2-37/39	10	发送 20 到 C1	C1-10/10 C2-10/5.0
		C1-52/16 C2-37/39	10.625	C1 收到 20	C1-12.5/10 C2-10/5.0

11	信道#1 收到 17 个字节，信道#1 发送 17 个字节(17 个字节 S,HCI 数据)	C1-52/16 C2-20/36	11. 25	发送 20 到 C2	C1-12.5/10 C2-10/7.5

2.2 控制终端要求.

终端 0 用于配置和控制 USB 设备。终端 0 还可用于允许主机向主控制器发送特定 HCI 指令。当 USB 固件在具有蓝牙类别码的终端上收到一个分组时,它应将该分组视为一 HCI 指令分组。

2.3 BULK 终端要求

数据完整性是 ACL 数据的一个关键方面。它与带宽请求一起成为使用 BULK 终端的原因。每毫秒应通过总线传输多个 64 字节分组。推荐批最大分组尺寸为 64 字节。BLUK 能够通过总线每毫秒传输多个 64 字节的分组帧。

BLUK 能够进行检错和纠错。通过该管道的数据流可流向多个从设备。为了避免阻塞，推荐主控制器采用类似于共享终端模型的流控制模型。

2.4 中断终端要求

中断终端能够保证事件以可预测并及时的方式传递。事件分组可以在一定允许延时条件下通过 USB 发送。中断终端应有 1 毫秒的时间间隔。

USB 软件和固件不必对传送到主控制器的事件充分了解。

2.5 同步终端要求

同步终端与无线主控制器相互传输 SCO 数据。时间是该数据类型的重要因素。USB 固件应将数据内容传递到主控制器的 SCO 先进先出队列（FIFO）。如果 FIFO 满，则应用新数据覆盖原有数据。终端应有 1 毫秒的时间间隔，参见 USB 规范 1.0 和 1.1 要求。

无线收发器可支持 3 个 64KB/S 语音信道,可以接收不同编码方式的数据---16 位线性音频编码要求最大数据量)。该终端推荐最大分组尺寸至少为 64 字节。但是，如果不需要支持 3 条 16 位编码的语音信道，32 字节作为最大分组尺寸也可接受。

3 .类别码

类别码将用于所有 USB 蓝牙设备。这将允许调用合适的驱动程序,而不需要考虑设备由哪家厂商提供。它也允许通过控制终端区分 HCI 指令和 USB 指令。

类别码(bDeviceClass)为 0xE0,无线控制器

子类码(bDeviceSubClass)为 0X01—— 射频控制器

协议码（bDeviceProtocol）为 0X01—蓝牙编程

4 .设备固件升级

固件升级能力并非必须的特性。但如果实现，固件升级应兼容于“设备固件升级通用串行总线设备类别规范”(1.0 版，1999/05/13)，参见USB论坛网址http://www.USB。

5 .限制

5.1 功率限制

目前,支持 USB 的设备的主控制器被置于如 PIIX4 的芯片内。当系统处于 S3 或 S4 时,USB 主控制器将不能接收信号。只有当系统处于 S1 或 S2 时，USB 才能被唤醒.

USB 主控制器的另一特性是，当一设备被连接上时,USB 主控制器将不断检查存储器，以确认是否有需要完成的工作。检查存储器的频率是 1 毫秒。这将阻止处理器进入 C3 节能状态。由于笔记本处理器不能进入 C3 状态而将导致显著的电能损失。这对商业用户是一个大问题，因为一个典型的商业用户将在 C3 状态中花费 90%的时间。

5.2 其它限制

同步终端可能导致数据差错。终端 1 和 2 都可能会有数据差错。

USB在所有数据传输时都提供 16 位循环冗余校验。USB误码率为 10^{-3}。

注意：当加密狗从系统中取出时，无线收发器将不再工作(假定这是一台总线驱动的设备)。这也就意味着设备将丢失连接。

第 12 章 HCI RS232 传输层

目录

1.前言

HCI RS232 传输层的目标在于在蓝牙主机和蓝牙主控制器之间物理 RS232 接口上使用蓝牙 HCI。

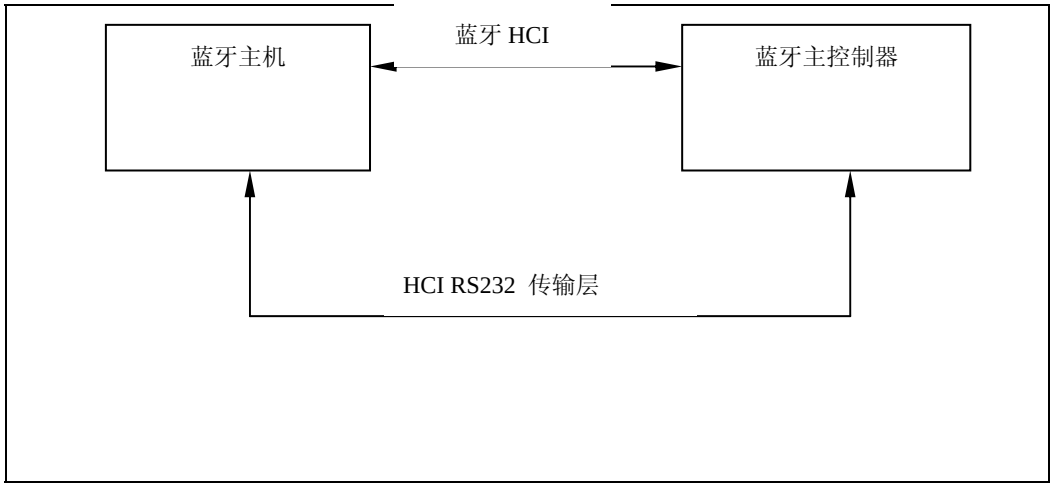


图 1.1

2. 概述

通过 RS232 传输层可发出四种 HCI 分组，包括：HCI 指令分组、HCI 事件分组、HCI ACL 数据分组和 HCI SCO 数据分组(参见“主控制器接口功能规范”)。HCI 指令分组仅能用于发送到蓝牙主控制器，HCI 事件分组仅能由蓝牙主控制器发送,HCI ACL/SCO 数据分组则可由蓝牙主控制器自由发送和接收。

但是，主控制器接口不能区分四种 HCI 类型。因此,如果通过一通用物理接口发出一个 HCI 分组,则 HCI 分组指示器必须根据下表执行加操作。

表 2.1 HCI RS232 分组头

HCI 分组类型	HCI 分组指示器
HCI 指令分组	0X01
HCI ACL 数据分组	0X02
HCI SCO 数据分组	0X03
HCI 事件分组	0X04
错误消息分组	0X05
协商分组	0X06

除这四种 HCI 分组类型外,还有两种分组类型用于支持动态协商和错误报告。接收端使用错误消息分组(0x05)将错误报告给发送端。协商分组(0x06)则用于协商通信设置和协议。

当每次发送一个以上 HCI 分组时，HCI 分组指示器将在一个 8 位序列号上每次加 1，除非转发分组作为纠错的一部分。HCI 分组紧跟在该序列号域后。所有四种 HCI 分组都有一长度域,该域用于确定 HCI 分组长为多少字节。尽管协商分组能够达到 7 个以上字节，但错误消息分组和协商分组都是基于扩展域（Extension）值的定长分组。

基本 RS232 传输分组的帧如下：

LSB

MSB

分组类型 (8-位)	序列号 (8 位)	HCI 分组 或错误消息/协商分组有效载荷

最低位先发送。

3. 协商协议

在 RS232 链路上发送任何字节之前，应当在主控制器和主机之间对波特率、奇偶校验值类型、终止位和协议模式进行协商。Tdetect 是发射机检测 CTS 状态变化的最大时间，加上如果 RTS/CTS 用于发送器错误指示和重新同步时刷新传输缓冲区所需的时间。否则，Tdetect 代表本地中断延时。主机将使用协议模式=0x13，首先发送一个含最大推荐值的协商分组，加上在缺省 UART 设置下 Ack 码=000b 的主机 Tdetect 值。同时，主控制器方也将其 UART 配置设置为初始化参数，并等待来自主机的协商分组。

如果主控制器方能够接受来自主机的推荐值，它将回送含同样 UART 设置值，以及 Ack = 001b 的主控制器 Tdetect 值的协商分组。然后，主机返回含同样 UART 设置值的协商分组，以及 Ack= 001b 的 Tdetect 值作为最终确认，然后将主机 UART 设置为新值。在收到来自主机的最终确认分组以后，主控制器也将其 UART 设置为新值。

另一方面,如果主控制器方不能接受推荐值，它应发送一新推荐值集，以及 Ack=010b 的 Tdetect 值。每一方都将继续执行这些步骤，直到双方收到可接受的 Ack 代码值。初始化协商期间的出错检测和出错恢复将以协议模式 0x13 方式执行。

协商可由任何一方在任意时间重新初始化，以协商新值，或通知新的 Tdetect 时间。当协商在数据传输期间重新初始化时，它将使用先前的协商设置，以交换新参数，而不是使用缺省值。

初始参数为：

波特率：9600bps

奇偶校验值类型：无奇偶校验值

数据位数：8 位(注：只允许 8 位数据长度)

终止位 ： 1

协议模式：0x13 (HDLC，采用 COBS/CCITT-CRC 帧分方式)

协商分组格式：

LSB MSB

分组类型头 0x06 8 位	序列号 8 位	UART 设置和 ACK (8 位)	波特率 16 位	Tdetect 时间 (16 位)	协议模式 （8 位）

序列号：

8 位，每传输一分组增加 1，不包含重发分组。使用小 Endian 码格式。

UART 设置和 ACK 域：

位 0-1	位 2	位 3	位 4	位 5-7
保留	终止位 1 位	启用奇偶校验 1 位	奇偶校验类型（1 位）	ACK 码（3 位）

终止位：

0：1 终止位

1：2 终止位

启用奇偶校验

0：奇校验

1：偶校验

ACK 代码：

000b：请求

001b：接受

010b：不接受新推荐值

011b-111b:保留

波特率：

波特率=27,648,000/N 时输入 N

N=0 非法

最大可能速率为 27.648Mbps

最小可能速率为 421.88bps

使用无类型小 Endian 格式，最低位最先发送。

Tdetect 时间：

16 位域，以发射机检测 CTS 变化所需最大时间，加上如果 RTS 和 CTS 用于重新同步而用于刷新传输先进先出队列（FIFO）的时间进行填充。否则，它将以本地中断延迟填充。

以 100 微秒为时间单位。

使用无类型小 ENDIAN 格式，最低位首先发送。

协议模式 ：

位 0	位 1	位 2	位 3	位 4	位 5	位 6	位 7
使 用 CRC	使用分界符	使用 RTS/CTS	RTS/CTS 模式	使用纠错	Ext0	Ext1	Ext2

使用 CRC：

0:分组末尾不附属 CRC-CCITT；

1:分组末尾附属 CRC-CCITT；

16 位 CRC 使用 RTS/CTS 或分界符,尽管当使用分界符时本规范只说明一种情况。

多项式发生器=$x^{16}+x^{12}+x^5+1$ ：

使用分界符：

0:分界符,0x7E,未使用。

1:分界符,0x7E,与 COBS 一起使用。（缺省）

使用 RTS/CTS：

0:未使用 RTS/CTS。（缺省）

1:使用 RTS/CTS。

RTS/CTS 模式：

0:RTS/CTS 用于错误指示和重新同步。（缺省）

1:RTS/CTS 用于硬件流控制，参见 HCI UART 传输层。

使用纠错：

0:未支持纠错

即使不支持纠错，也将发送错误消息。

1:支持纠错（缺省）

如果 RTS/CTS 用于同步，则纠错将重发含有错误的分组和所有其它分组。另一方面,如果 0x7E 用作分界符，其中 COBS 作为同步机制，然后纠错将只重发含有错误的分组。

Ext2,Ext1,Ext0：

这 3 位为附属于协商分组后的额外字节，用于今后扩充。

4．分组传输协议

分组传输可以提供或不提供检错机制，如奇偶校验或无奇偶校验，CRC 校验或无 CRC 校验。这将取决于应用环境。

可以选择 RTS/CTS 或分界符作为一种同步机制。RTS/CTS 的使用可以减少 COBS 编码计算时间，但它需要 2 根额外的铜芯，而铜丝则不适用于某些应用。如果必须使用 3 芯电缆,或不使用可编程 RTS/CTS,则分界符、0x7E 就能够与 COBS 一起使用。

但是,这两种方案的纠错差别很小。如果 RTS/CTS 用于再次同步，它将简单重发所有分组，并以含有错误的分组作为起始分组。如果使用分界符，发送端将仅重发含有错误的分组。可以不使用纠错，但当接收端检测到错误时仍要将错误消息分组发到发送端。

HCI RS232 传输层通常使用 8 位数据长度,并且本规范假定为里 little Endian 格式。并且最低位先发。

主控制器可以仅支持一种协议模式，但主机必须能够支持任何形式。

以下章节定义了两种通用方案(协议模式= 0x13 和 0x14)，用来解释每种模式的用法

5 使用含有 COBS 的分界符同步

本节说明含有 COBS 的分界符如何用于同步,以及分界符作为同步机制时如何执行纠错过程。整个过程采用协议模式 0x13。

5.1 使用含 COBS 和 CRC 的分界符,协议模式 0X13

在不能使用 RTS/CTS，或者它们通过物理连接而作为硬件流控制时，将采用类似于 HDLC 的含 16 位 CRC(CRC-CCITT)的帧，和含 COBS 的分界符 0x7E (COBS)[2]，作为检错和重新同步的手段。

CRC-CCITT将使用以下多项式生成 16 位的校验和：$x^{16}+x^{12}+x^5+1$。该 16 位CRC应附加于分组末尾，同时又正好在结束分界符 0x7E之前。起始分界符 0x7E之后为分组类型指示域。

CONSISTENT OVERHEAD BYTE STUFFING 是 PPP 最近的改进，不考虑数据模式，它将产生不到 0.5%的开销。它将使用两个步骤替换分界符 0x7E。第一步骤将消除 0 并在起始和结束分界符之间用 0x00 替代所有 0x7E。

在此采用一种简单纠错方案以降低因支持纠错而产生的开销。当接收端检测到任何错误时，它将向发出方返回一含错误类型的错误消息分组。错误消息分组包括一个含错误域的序列数 (含错误信息的 SEQ NO)，以标示是那个分组检测到错误。每一分组的序列号域都是一个 8 位域。它们将在传输每一分组时增加 1，重发分组出外。重发分组应在序列号（SEQ NO ）域中包含原序列号。

发送端应只重发含错误的 HCI 分组。该分组序列号域用于指示该错误。而接收端将负责记录分组的正确顺序。如果发送端在重发保持缓冲区内的分组序列号不正确,它应发送错误类型为 0x81 的错误消息分组，以及错误域为重发分组丢失序列号的序列号（SEQ No)，以便接收端能够检测丢失分组。在这种情况下，不能执行完整的纠错过程。但是,接收端至少能检测分组的丢失。

接收端能够在等待重发分组时和超时以前,等待的时间至少 4 倍于远程 Tdetect、本地 Tdetect、错误消息分组传输时间,加上该重发分组时间之和。当发生超时时，接收端可以通过发送另一错误信息分组（错误类型=0x09）重新请求，或放弃并将情况报告上层。

。。5.2 帧分（Framing）

BOF(0x7E)、CRC-CCITT 和 EOF（0x7E）将加入本文件所描述基本分组

中。当 CRC 送出时，应首先送出最低位字节。

LSB （微秒）B

0X7E BOF（8 位）	分组类型（8 位）	序列号 SEQ NO（8 位）	有效载荷	CRC（16 位）	0X7E EOF（8 位）

5.3 错误消息分组

错误消息分组格式如下表：

表 5.1 可用错误类型

分组类型，0X05（8 位字段）	序列号（8 位字段）	错误类型（8 位字段）	含错误的序列号（8 位字段）

错误类型	描述
0X00	保留
0X01	数据速率不匹配错或超时错
0X02	奇偶校验错
0X03	保留
0X04	帧分错误
0X05-0X07	保留
0X08	CRC 错误
0X09	丢失序列号
0X0A-0X80	保留
0X81	重发分组丢失
0X82-0XFF	保留

5.4 一致开销字节填充法

代码	后面内容	描述
0X00		未使用
0X01-0XCF	N-1 字节数据	N-1 字节数据加隐含的零
0XD0	N-1 字节数据	N-1 字节数据不含零
0XD1		未使用
0XD2		保留
0D3-0DF	缺省	一个 N-0XD0 零的运行
0XE0-0FE	N-E0 字节数据	隐含两个零的数据
0XFF		未使用

COBS 要求两步编码。

第一步是消除零。如果启用 CRC 校验，则在增加起始和结束分界符（0x7E）以前，附加 16 位 CRC 之后，进行本步骤。每一 COBS 代码块包括后面为零或更多数据字节的 COBS 代码。代码字节 0x00、0xD1、0xD2 和 0Xff 不得使用。COBS 零消除过程查找首先出现零值的分组。为简化编码，将在 CRC 之后临时增加一个零值在分组末端，作为临时占用位。字节数和是否包含首个零决定使用的编码。如果该数为 207 或更小，则它将作为 COBS 编码字节，后面紧跟非零数据字节，但不包括为零的末字节。另一方面，如果该数大于 207，则使用编码字节 0xD0，且后面紧跟首个 207 非零字节。该过程将重复执行直至分组所有字节，包括末位临时占用的零位，都已完成编码。如果在 0～30（8 进制）非零字节之后检测到一对 0x00，将使用字节数与 0xE0 的和作为 COBS 编码使用，其后为非零字节，但不包括这对零。如果有 3 个到 15 个 0x00 字节被检测到，则将该 0X00 字节数与 0xD0 的和用作编码，后面不再跟其它字节。

第二步用 0x00 替代 0x7E。这两个步骤可以循环方式一起执行，以减少编码时间。

具体细节和参考编码，参见“PPP 一致字节填充法（COBS）”

6. 使用 RTS/CTS 同步

本节描述如何使用 RTS/CTS 重新同步，以及在使用 RTS/CTS 作为同步机制时如何执行纠错过程。该过程使用协议模式 0x14 进行描述。

6.1 不采用 CRC，使用 RTS/CTS 同步，协议模式 0X14

HCI 分组传输流由两 MODEM 控制/状态信号- RTS 和 CTS 处理。CTS 和 RTS 以空 MODEM 方式连接，也就意味着本地-RTS 应连接到远程-CTS，而本地-RTS 应连接到远程-RTS。这些末 MODEM 控制/状态信号用于将错误检测结果通知其它方，同时在检测到错误后与分组起始端重新同步。本节采用一个简单纠错方案以减小支持本功能的开销。

只有 CTS 位为 1 时，才发送 HCI 分组。 如果在 HCI 分组传输期间或在末尾字节传输之后，CTS 位变为 0，这就表示有错误发生。接收端一旦检测到任何错误，将马上撤销 RTS，并将把含错误类型的错误分组返回发送端。该错误分组包括含错误域的序列号，该错误域指示是哪个分组错误。每一分组的序列号域都是一个 8 位域。该域在除重发分组以外的每次传输任何类型分组时都加 1。该重发分组应包括 SEQ NO 字段中原来的序列号。

当发送端任何时候检测到 CTS 位从 1 变为 0 时，都将挂起传输并等待，直至在恢复传输前收到错误分组。当接收端准备接收新数据时，它应在最小 Tdetect 时间后确认 RTS。Tdetect 时间是发送端用于检测 CTS 位状态

变化的最大时间，加上它刷新传输缓冲区时间的和。在协商期间，每一端的 Tdetect 值都应互相通知对方。本地 Tdetect 值和远端 Tdetect 值，以及波特率，能够用于估算重发占用缓冲区所需队列长度。在接收端再次确认 RTS 之前,它应刷新 RX 缓冲区。

发送端应自错误分组开始重发所有 HCL 分组,错误分组的错误由错误域的序列号 SEQ No 指明。在重发之前，应刷新可能缓存自前一丢弃分组开始以后其它分组的传输缓冲区。当它从重发占用缓冲区中重发分组时,应采用其 SEQ No 与错误相匹配的序列号所在分组，来开始传输。如果发送端在重发占用缓冲区中不包含具有正确序列号的分组,发送端应发送一错误类型为 0x81 的错误消息分组，并且它将跳过序列号在缓冲区中可用的分组。在这种情况下，不能执行完整纠错过程。但接收端至少能够检测分组丢失。

6.2 错误消息分组

错误消息分组格式如下：

表 6.1 可用错误类型

LSB MSB

分组头 0X05（8 位域）	序列号 SEQ (8 位域)	错误类型(8 位域)	错误序列号(8 位域)

错误类型	描述	评述
0X00	保留	
0X01	速率不匹配或超时	
0X02	奇偶校验错	
0X03	保留	
0X04	帧错误	
0X05-0X07	保留	
0X08	CRC 错	
0X09	序列号丢失	
0X0A-0X80	保留	
0X81	重发分组丢失	
0X82-0FF	保留	

6．3 信令示例

6.4 流控制实例

6.4.1 实例 1：正常恢复处理

控制方 主机方

0) 声明 CTS，且检测已声明 CTS	声明 RTS，且检测已声明 CTS
	1) 送出控制/数据[n]，并在重发保持缓冲区中存储控制/数据[n]
2)收到错误的控制/数据[n]。	
3) 撤销声明 RTS 4a)发送[n]错误消息，并在 TX 重发保持缓冲区中存储[n]的错误消息 4b)清除 RX 先进先出队列并等待 Tdetect(主机)时间长度。	4)检测到撤销声明的 CTS
	5a)停止进一步传输，并等待直到 TX 先进先出队列清空(如果允许，刷新先进先出队列) 5b)收到[n]错误消息。
6)声明 RTS	
	7)检测到声明的 CTS 8)重发控制/数据[n]

6.4.2 实例 2：双方同时检测到错误

控制器方	主机方
0) 声明 RTS 并检测已声明的 CTS 1) 发送控制/数据[n]，并在重发保持缓冲区中存储控制/数据[n] 2)收到错误的控制/数据[n] 3) 撤销声明 RTS 4) 检测到已撤销声明的 RTS 5a)停止进一步传输，并等待直到 TX 先进先出队列清空(如果允许，可刷新该先进先出队列) 5b) 清空 RX 先进先出队列并且等待 Tdetect (控制器)的时间长度 6) 声明 RTS 7) 检测已声明的 CTS 8) 发送错误消息[x]，并在 TX 重发保持缓冲区中存储错误消息[x] 9)收到错误消息[x] 10)重发控制/数据[x]	0) 声明 RTS，并检测已声明的 CTS 1) 发送控制/数据[n]，并在重发保持缓冲区中存储控制/数据[n] 2) 收到错误的控制/数据[n] 3) 撤销声明 RTS 4) 检测到已撤销声明的 RTS 5a) 停止进一步传输，并等待直到 TX 先进先出队列清空(如果允许，可刷新该先进先出队列) 5b) 清空 RX 先进先出队列并且等待 Tdetect (控制器)的时间长度 6) 声明 RTS 7) 检测已声明的 CTS 8) 发送错误消息[x]，并在 TX 重发保持缓冲区中存储错误消息[x] 9)收到错误消息[n] 10)重发控制/数据[x]

6.4.3 实例 3：错误信息

控制方	主机方
0) 声明 RTS 并检测已声明的 CTS	0) 声明 RTS 并检测已声明的 CTS
	1) 发送控制/数据[n]，并在重发保持缓冲区中存储控制/数据[n]
2)收到错误的控制/数据[n]	
3) 撤销声明 RTS	
4a）发送错误消息[n]（Err[n]），并在 TX 重发保持缓冲区中存储 Err[n] 4b）清空 RX 先进先出队列并且等待 Tdetect（主机)时间长度	
	5a）停止进一步传输，并等待直到 TX 先进先出队列清空(如果允许，可刷新该先进先出队列) 5b）收到错误消息[n]
6）声明 RTS	6a）撤销 RTS 声明 6b）清空 RX 先进先出队列并且等待 Tdetect (控制器)时间长度。
7）检测已撤销声明的 CTS	
8）停止进一步传输，并等待直到 TX 先进先出队列清空(如果允许，可刷新该先进先出队列)	8）检测到声明的 CTS
	9a）发送 Err[n]的错误消息，并在 TX 重发保持缓冲区中存储 Err[n]的错误消息 9b）声明 RTS
10a）收到 Err[n]的错误消息 10b）检测到声明的 CTS	
11）重发错误消息[n]	
	12）收到错误消息[n]
	13）重发控制/数据[n]