**蓝牙协议的学习**

**第一章 蓝牙的概述**

**一、蓝牙版本信息**

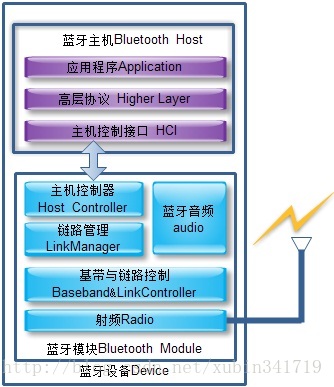
蓝牙共有六个版本V1.1/1.2/2.0/2.1/3.0/4.0  版本信息：  
**1、V1.1版本** 传输率约在748~810kb/s，因是早期设计，容易受到同频率之产品所干扰下影响通讯质量。  
**2、V1.2版本** 同样是只有748~810kb/s 的传输率，但在加上了(改善 Software)抗干扰跳频功能。  
**3、V2.0+EDR版本** 是 1.2 的改良提升版，传输率约在1.8M/s~2.1M/s，开始支持双工模式——即一面作语音通讯，同时亦可以传输档案/高质素图片，2.0 版本当然也支持 Stereo 运作。  
 应用最为广泛的是Bluetooth2.0+EDR标准，该标准在2004年已经推出，支持Bluetooth 2.0+EDR标准的产品也于2006年大量出现。虽然Bluetooth 2.0+EDR标准在技术上作了大量的改进，但从1.X标准延续下来的配置流程复杂和设备功耗较大的问题依然存在。  
**4、V2.1版本** 更佳的省电效果：蓝牙2.1版加入了SniffSubrating的功能，透过设定在2个装置之间互相确认讯号的发送间隔来达到节省功耗的目的。  
**5、V3.0+HS版本** 2009年4月21日，蓝牙技术联盟(Bluetooth SIG)正式颁布了新一代标准规范"Bluetooth Core Specification Version 3.0 High Speed"(蓝牙核心规范3.0版 )，蓝牙3.0的核心是"GenericAlternate MAC/PHY"(AMP)，这是一种全新的交替射频技术，允许蓝牙协议栈针对任一任务动态地选择正确射频。最初被期望用于新规范的技术包括802.11以及UMB，但是新规范中取消了UMB的应用。  
**6、V4.0 版本** 蓝牙4.0包括三个子规范，即传统蓝牙技术、高速蓝牙和新的蓝牙低功耗技术。蓝牙 4.0的改进之处主要体现在三个方面，电池续航时间、节能和设备种类上。拥有低成本，跨厂商互操作性，3毫秒低延迟、100米以上超长距离、AES-128加密等诸多特色此外，蓝牙4.0的有效传输距离也有所提升。3.0版本的蓝牙的有效传输距离为10米(约 32英尺)，而蓝牙4.0的有效传输距离最高可达到100米(约328英尺)。

**7、典型蓝牙与BLE蓝牙对比**

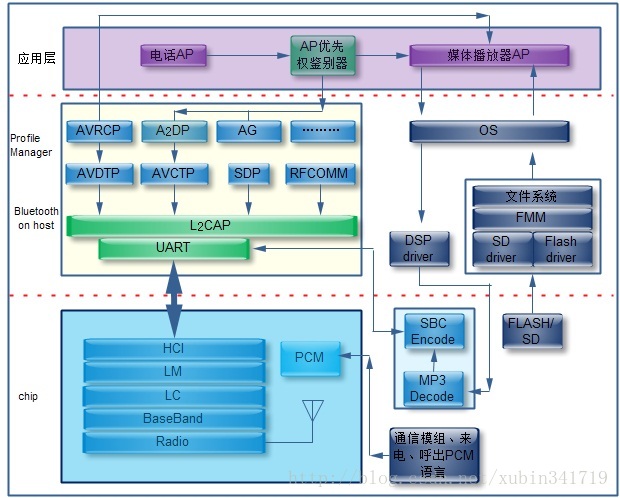


**二、蓝牙的技术特点** 简单地说，蓝牙是一种短程宽带无线电技术，是实现语音和数据无线传输的全球开放性标准。它使用跳频扩谱（FHSS）、时分多址（TDMA）、码分多址（CDMA）等先进技术，在小范围内建立多种通信与信息系统之间的信息传输。  
**1、Bluetooth的主要技术特点：  
（1）、工作频段**：2.4GHz的工科医（ISM）频段，无需申请许可证。大多数国家使用79个频点，载频为(2402+k)MHz（k=0，1, 2…78），载频间隔1MHz。采用TDD时分双工方式。  
**（2）、传输速率**：1Mb/s（V2.0以上版本）  
**（3）、调试方式**：BT=0.5的GFSK调制，调制指数为0.28-0.35。  
**（4）、采用跳频技术：**跳频速率为1600跳/秒，在建链时（包括寻呼和查询）提高为3200跳/秒。蓝牙通过快跳频和短分组技术减少同频干扰，保证传输的可靠性。  
**（5）、语音调制方式：**连续可变斜率增量调制（CVSD，ContinuousVariable Slope Delta Modulation），抗衰落性强，即使误码率达到4%，话音质量也可接受。  
**（6）、支持电路交换和分组交换业务：**蓝牙支持实时的同步定向联接（SCO链路）和非实时的异步不定向联接（ACL链路），前者主要传送语音等实时性强的信息，后者以数据包为主。语音和数据可以单独或同时传输。蓝牙支持一个异步数据通道，或三个并发的同步话音通道，或同时传送异步数据和同步话音的通道。每个话音通道支持64kbps的同步话音；异步通道支持723.2/57.6kbps的非对称双工通信或433.9kbps的对称全双工通信。  
**（7）、支持点对点及点对多点通信**：蓝牙设备按特定方式可组成两种网络：微微网(Piconet)和分布式网络(Scatternet)，其中微微网的建立由两台设备的连接开始，最多可由八台设备组成。在一个微微网中，只有一台为主设备（Master），其它均为从设备（Slave），不同的主从设备对可以采用不同的链接方式，在一次通信中，链接方式也可以任意改变。几个相互独立的微微网以特定方式链接在一起便构成了分布式网络。所有的蓝牙设备都是对等的，所以在蓝牙中没有基站的概念。  
**（8）、工作距离：**蓝牙设备分为三个功率等级，分别是：100mW（20dBm）、2.5mW（4dBm）和1mW（0dBm），相应的有效工作范围为：100米、10米和1米。

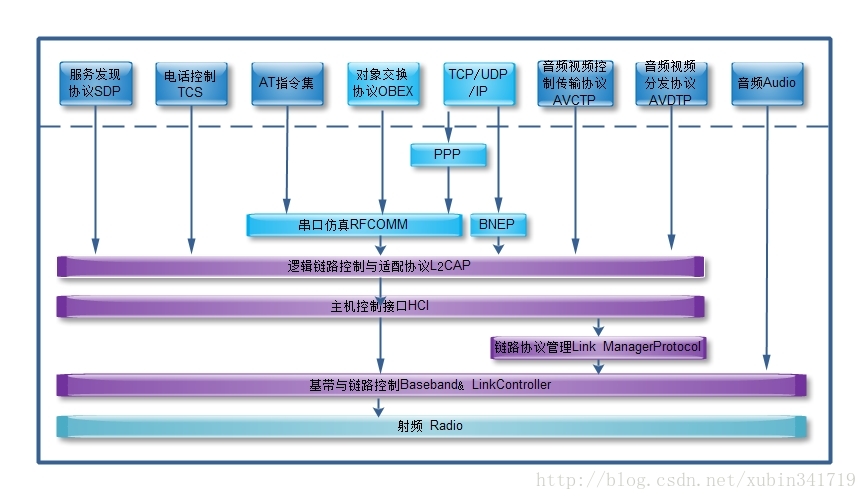
**三、Bluetooth的系统构成**



**1、无线射频单元(Radio)：**负责数据和语音的发送和接收，特点是短距离、低功耗。蓝牙天线一般体积小、重量轻，属于微带天线。  
**2、基带或链路控制单元(LinkController)：**进行射频信号与数字或语音信号的相互转化，实现基带协议和其它的底层连接规程。  
**3、链路管理单元(LinkManager)：**负责管理蓝牙设备之间的通信，实现链路的建立、验证、链路配置等操作。  
**4、蓝牙软件协议实现：**如上图紫色部分，这个后面我们做详细说明。



**四、蓝牙协议规范**传输协议、中介协议、应用协议；  
**1、传输协议** 负责蓝牙设备间，互相确认对方的位置，以及建立和管理蓝牙设备间的物理链路；  
 **底层传输协议：** 蓝牙射频（Radio）部分、基带链路管理控制器（Baseband&Link Controller）、链路管理协议（Link ManagerProtocol LMP）。负责语言、数据无线传输的物理实现以及蓝牙设备间的联网组网。  
 **高层传输协议：**逻辑链路控制与适配器（LogicalLink Control and Adaptation Protocol）L2CAP 、主机控制接口（HostControl Interface，HCI）。为高层应用屏蔽了跳频序列选择等底层传输操作，为高层程序提供有效、有利于实现数据分组格式。  
**2、中介协议**    为高层应用协议或者程序，在蓝牙逻辑链路上工作提供必要的支持，为应用提供不同标准接口。  
     串口仿真协议：RFCOMM、服务发现协议：SDP、互操作协议IrDA、网络访问协议：PPP、IP、TCP、UDP、电话控制协议：TCS、AT指令集。

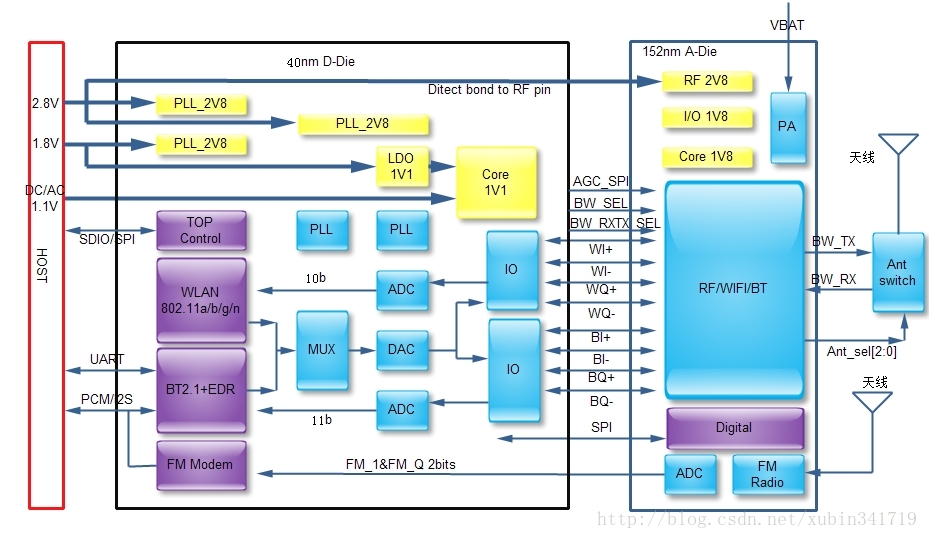


**3、应用协议**

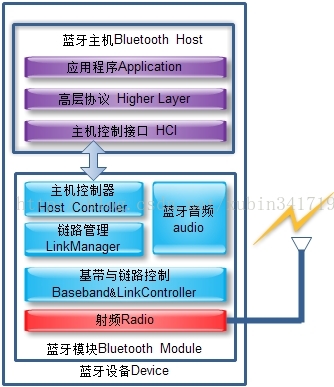
      蓝牙协议栈之上的应用软件和所涉及到的协议，如：拨号上网、语言功能的应用程序。

**蓝牙的应用框架如下：  
（1）、通用应用类框架：查询、建立连接服务等；  
（2）、蓝牙电话应用类框架：电话控制、语言；  
（3）、蓝牙连网应用类框架：网络应用相关；  
（4）、对象交互服务类框架：IrDA、OBEX；  
（5）、蓝牙音视频控制类框架。**

**五、硬件接口**一般蓝牙芯片通过UART、USB、SDIO、I2S、PcCard和主控芯片通信。如下图所示，通过UART和主控芯片通信。

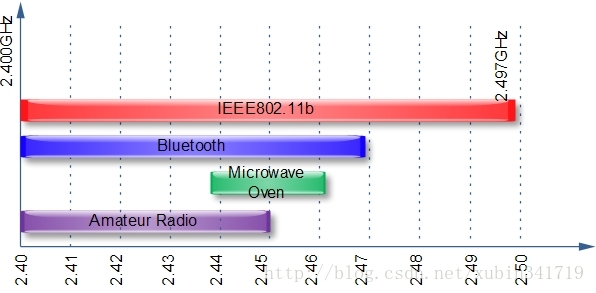


**第二章 蓝牙协议规范（射频、基带链路控制、链路管理）**

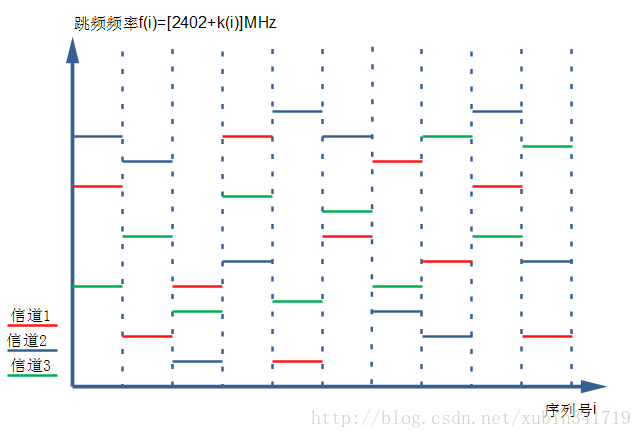
****

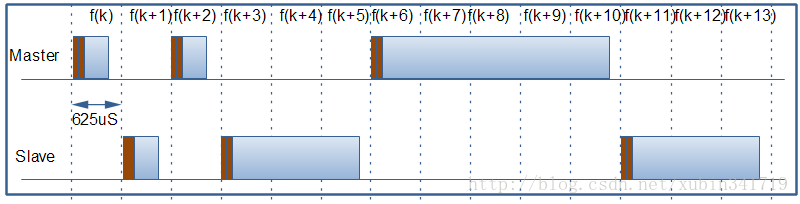
蓝牙协议是蓝牙设备间交换信息所应该遵守的规则。与开放系统互联（OSI）模型一样，蓝牙技术的协议体系也采用了分层结构，从底层到高层形成了蓝牙协议栈，各层协议定义了所完成的功能和使用数据分组格式，以保证蓝牙产品间的互操作性。

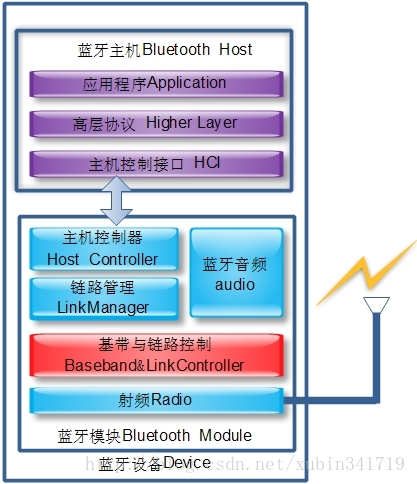
**一、射频协议** 射频位置如上图红色部分。  
**1、工作频率** 蓝牙工作在2.4GHz ISM频段上，蓝牙采用跳频扩谱技术主动的避免工作频段受干扰（微波炉的工作频率也是2.4GHz）。



|  |  |  |
| --- | --- | --- |
| 地理位置 | ISM频段范围 | 射频信道频率 |
| 中国、美国、欧洲 | 2400.0～2483.5MHz | F=(2402+k)MHz,k在0、1、……78中随机取值 |
| 法国 | 2446.5～2483.5MHz | F=(2454+k)MHz,k在0、1、……22中随机取值 |
| 日本 | 2471.0～2497.0MHz | F=(2473+k)MHz,k在0、1、……22中随机取值 |
| 西班牙 | 2445.0～2475.0MHz | F=(2449+k)MHz,k在0、1、……22中随机取值 |

我国的蓝牙频率在2.402GHz～2.483GHz,蓝牙每个频道的宽度为1MHz，为了减少带外辐射的干扰，保留上、下保护为3.5MHz和2MHz，79个跳频点中至少75个伪随机码跳动，30S内任何一个频点使用时长不能超过0.4S。   
**2、跳频技术、发射功率、时隙  
（1）、发射功率：**蓝牙发射功率分三级：一级功率100mW(20dBm)；二级功率2.5mW(4dBm)；三级功率1mW(0dBm)；  
**（2）、物理信道：**蓝牙物理信道有伪随机序列控制的79个跳频点构成，不同跳频序列代表不同的信道。  
  
**（3）、时隙：**蓝牙跳频速率为1600次/s,每个时间为625uS(1S/1600)称为一个时隙；



**二、基带与链路控制协议  
**

蓝牙发送数据时，基带部分将来自高层的数据进行信道编码，向下发给射频进行发送；接收数据时，将解调恢复空中数据并上传给基带，基带进行信道编码传送给上层。

作用：跳频选择、蓝牙编址、链路类型、信道编码、收发规则、信道控制、音频规范、安全设置。

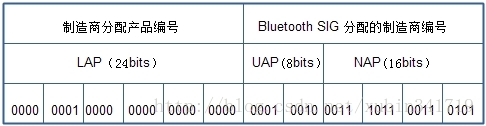
**1、蓝牙分组编码为小端模式；**

**2、蓝牙地址**

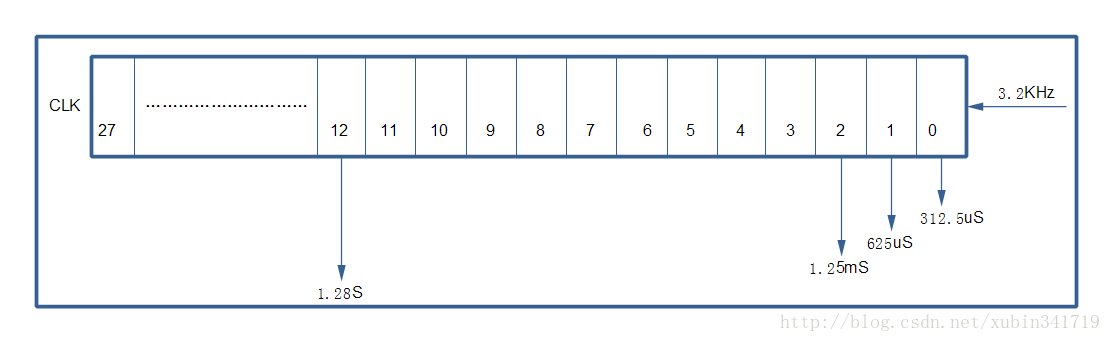
BD\_ADDR：BluetoothDevice Address；

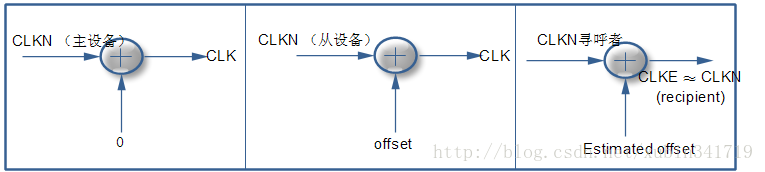
LAP:LowerAddress Part 低地址部分；

UAP: UpperAddress Part 高地址部分；

NAP: Non-significantAddress Part 无效地址部分。  


**3、蓝牙时钟** 每个蓝牙设备都有一个独立运行的内部系统时钟，称为本地时钟（Local Clock），决定定时器的收发跳频。为了与其他设备同步，本地时钟要加一个偏移量（offset），提供给其他设备同步。  
 蓝牙基带四个关键周期：**312.5uS、625uS、1.25mS、1.28S**。



**CLKN：**本地时钟：  
**CLKE:**预计时钟，扫描寻呼过程中用到；  
**CLK：**设备实际运行的时钟频率。  
CLKE、CLK由CLKN加上一个偏移量得到的。  


**4、蓝牙物理链路：** 通信设备间物理层的数据连接通道就是物理链路。  
 ACL（Asynchronous Connectionless）异步无连接链路；对时间要求不敏感的数据通信，如文件数据、控制信令等。  
 SCO（Synochronous Connection Oriented）同步面向连接链路；对时间比较敏感的通信，如：语音；最多只支持3条SCO链路，不支持重传。  
 ACL用于数据传输；  
**5、蓝牙基带分组：** 基带分组至少包括：接入码、分组头、有效载荷；  


**（1）、接入码**用于同步、直流、载频泄漏偏置补偿标识；  
**（2）、分组头**包含链路信息，确保纠正较多的错误。  
**分组类型如下：**

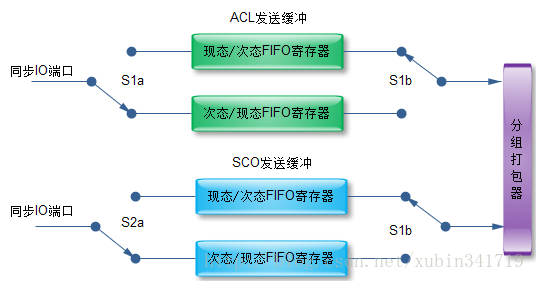
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 分组类别 | Type(b3b2b1b0) | 时隙 | SCO | ACL |
| 链路控制分组 | 0000 | 1 | NULL | NULL |
| 0001 | POLL | POLL |
| 0010 | FHS | FHS |
| 0011 | DM1 | DM1 |
| 单时隙分组 | 0100 | 1 | 未定义 | NULL |
| 0101 | HV1 |
| 0110 | HV2 |
| 0111 | HV3 |
| 1000 | DV |
| 1001 | NULL | AUX1 |
| 3时隙分组 | 1010 | 3 | 未定义 | DM3 |
| 1011 | DH3 |
| 1100 | 未定义 |
| 1101 |
| 5时隙分组 | 1110 | 5 | 未定义 | DM5 |
| 1111 |

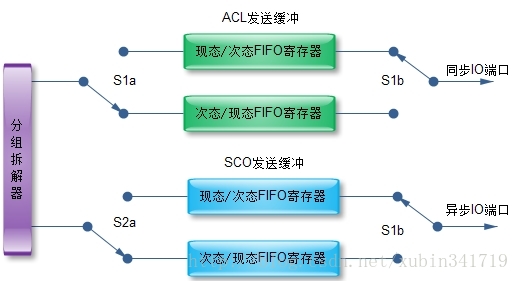
**ACL分组形式为：**D(M|H)（1|3|5）,D代表数据分组，M代表用2/3比例的FEC的中等速率分组；H代表不使用纠错码的高速率分组；1、3、5分别代表分组所占用的时隙数目；  
 DM1、DM3、DM5、DH1、DH3、DH5  
 SCO分组形式为：HV(1|2|3)。HV代表高质量语言分组，1、2、3有效载荷所采用的纠错码方法。1为1/3比例FEC，设备2个时隙发送一个单时隙分组；2为2/3比例FEC，设备4个时隙发送一个单时隙分组；3为不使用纠错码，设备6个时隙发送一个单时隙分组  
 HV1、HV2、HV3  
**ALC 分组：**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 类型 | 有效载荷头/字节 | 用户有效载荷/字节 | FEC | CRC | 对称最大速率/kbps | 非对称速率/kbps | |
| 前向 | 后向 |
| DM1 | 1 | 0～17 | 2/3 | 有 | 108.8 | 108.8 | 108.8 |
| DH1 | 1 | 0～27 | 无 | 有 | 172.8 | 172.8 | 172.8 |
| DM3 | 2 | 0～121 | 2/3 | 有 | 258.1 | 387.2 | 54.4 |
| DH3 | 2 | 0～183 | 无 | 有 | 390.4 | 585.6 | 86.4 |
| DM5 | 2 | 0～224 | 2/3 | 有 | 286.7 | 477.8 | 36.3 |
| MH5 | 2 | 0～339 | 无 | 有 | 433.9 | 723.2 | 57.6 |
| AUX1 | 1 | 0～29 | 无 | 无 | 185.6 | 185.6 | 185.6 |

**SCO分组：**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 类型 | 有效载荷头/字节 | 用户有效载荷/字节 | FEC | CRC | 有效载荷长度 | 同步速率/kbps | 占用Tsco数目/语言长度 |
| HV1 | 无 | 10 | 1/3 |  | 240位 | 64 | 2/1.25ms |
| HV2 | 20 | 2/3 | 4/2.5ms |
| HV3 | 30 | 无 | 6/3.75ms |
| DV | 1D | 10+(0-9)D | 2/3D | 有D |  | 64+57.6D |  |

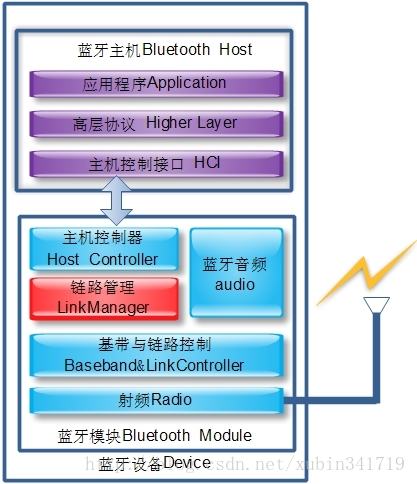
注释：D 只对数据段有用，DV分组包含数据段，也包含语言段。  
**（3）、有效载荷** 分语言有效载荷、数据有效载荷。  
**6、蓝牙的逻辑信道** 链路控制信道：LinkControl  LC  
 链路管理信道：Link Manage LM  
 用户异步数据信道：User AsynchronizationUA  
 用户同步数据信道：UserSynchronization US  
 用户等时数据信道：UserIsochronous UI  UI  
**7、蓝牙的收发规则  
  
** 上图为RX缓存。



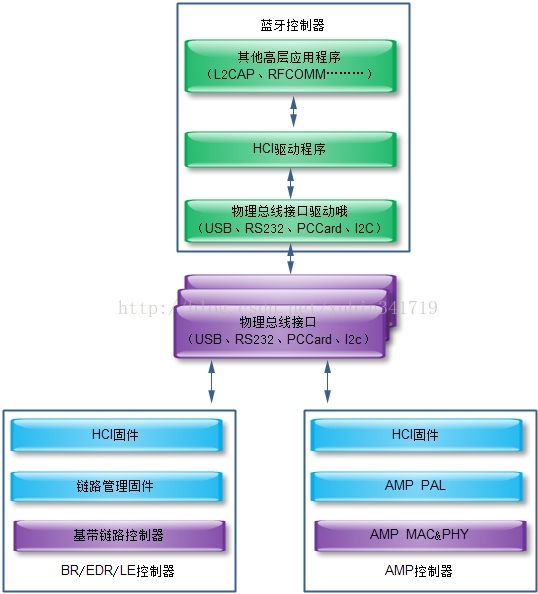
上图为TX缓存。  
新分组到达时，ACL链路的RX缓存器要流量控制，SCO数据不需要流量控制；  
**8、蓝牙基带信道和网络控制  
1）、链路控制器状态：** 待机、连接  
 寻呼page、寻呼扫描pagescan、查询inquiry、查询扫描inquiry scan、主设备相应Master Response、从设备相应Slave Response、查询相应inquiry response  
**2） 、连接状态** 激活模式active、呼吸模式sniff、保持模式hold、休眠模式park。  
**3）、待机状态**         待机状态是蓝牙设备缺省低功耗状态，此状态下本地时钟以低精度运行。蓝牙从待机转入寻呼扫描状态，对其他寻呼进行响应**成为从设备**；也可以从待机状态进入查询扫描状态，完成一个完整的寻呼，**成为主设备**。  
**9、接入过程**注释：  
 IAC Inquiry AccessCode 查询接入码；  
 GIAC:通用查询接入码 DIAC：专用查询接入码；  
 DAC：DeviceAccess Code 设备接入码；  
LAP：  
         建立连接，必须使用查询、寻呼；查询过程使用IAC，发现覆盖区域内的设备、设备的地址及其时钟；连接过程使用DAC，建立连接的设备处理寻呼过程，成为主设备。**、（1）、查询过程** 蓝牙设备通过查询来发现通信范围内的其他蓝牙设备。查询信息分为GIAC、DIAC两种。查询发起设备收集所有相应设备的地址、时钟信息。  
 一设备进入查询状态去发现其他设备，查询状态下连续不断的在不同频点发送查询消息。查询的跳频序列有GIAC的LAP导出。  
 一设备想被其他设备发现，就要周期性进入 查询扫描状态，以便相应查询消息。如：我们选择设备多长时间可见，其实就是  进入查询扫描状态。  
**A、查询扫描** 查询扫描状态下，接收设备扫描接入码的时间长度，足以完成对16个频率的扫描。扫描区间长度Twindow inquiry scan。扫描在同一个频率上进行，查询过程用32跳专用查询跳频序列，此序列有通用查询的地址决定，相位有本地时钟决定，每隔1.28S变化一次。  
**B、查询** 与寻呼类似，TX用查询跳频序列、RX用查询相应跳频序列。  
**C、查询相应** 从设备响应查询操作。每个设备都有自己的时钟，使用查询序列相位相同的几率比较小。为了避免多个设备在同一查询跳频信道同时激活，从设备查询响应规定：从设备收到查询消息，产生0-1023只觉得额一个随机数，锁定当时相位输入值进行跳频选择，从设备此后的RAND时隙中返回到连接或者待机状态。  
**（2）、寻呼扫描** DAC：DeviceAccess Code 设备接入码  
 寻呼扫描状态下的设备扫描窗口Twindowpage scan内监听自己的DAC。监听只在一个跳频点进行。Twindow page scan足够覆盖16个寻呼扫描频点。  
 寻呼扫描状态，扫描在同一个频率上进行，持续1.28S，在选择另一个不同频率。

|  |  |  |
| --- | --- | --- |
| SR模式 | Tpage scan | 寻呼次数Npage |
| R0 | 连续 | >=1 |
| R1 | <=1.28S | >=128 |
| R2 | <=2.56S | >=256 |
| 预留 | -- | -- |

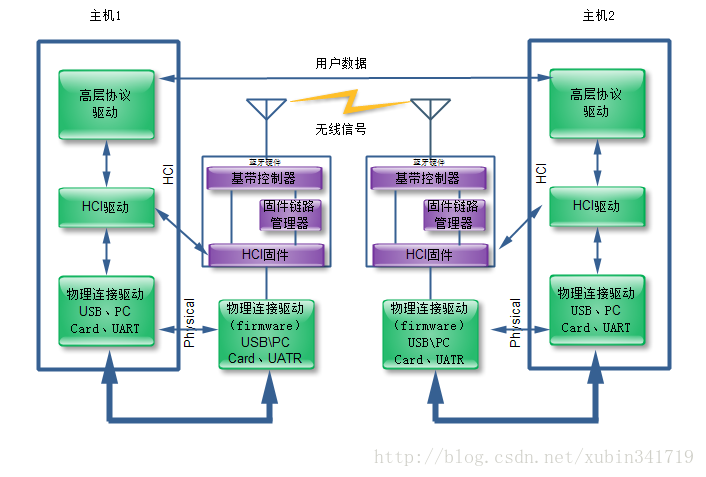
**（3）、寻呼** 主设备使用寻呼发起一个主—从设备连接，通过在不同的跳频点上重复发送从设备DAC来扑捉从设备，从设备在寻呼扫描状态被唤醒，接收寻呼。  
**（4）、寻呼相应过程  
三、链路管理器**

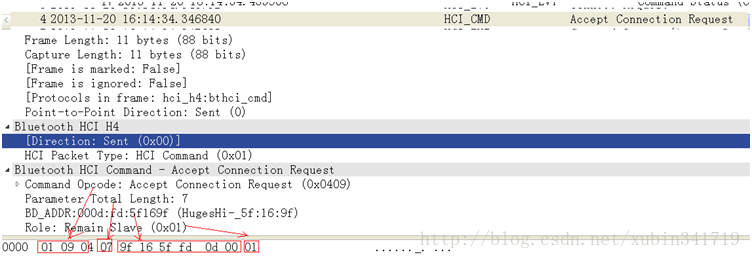
  
 如上图红色部分，负责完成设备：功率管理、链路质量管理、链路控制管理、数据分组管理、链路安全管理。  
**1、链路管理协议数据单元**         蓝牙链路管理器接收到高层的控制信息后，不是向自身的基带部分分发控制信息，就是与另一台设备的链路管理器进行协商管理。这些控制信息封装在链路管理协议数据单元LMP\_PDU中，由ACL分组的有效载荷携带。  
**2、链路管理器协议规范  
（1）、设备功率管理**         RSSI保持模式、呼吸模式、休眠模式。  
**（2）、链路质量管理 QoSQuality of Service** A、ACL链路。  
 B、SCO链路。  
**（3）、链路控制管理** 设备寻呼模式、设备角色转换、时钟计时设置、信息交换:版本信息、支持特性、设备名称；建立连接、链路释放。  
**（4）、数据分组管理**

**第三章 蓝牙协议规范（HCI、L2CAP、SDP、RFOCMM）**

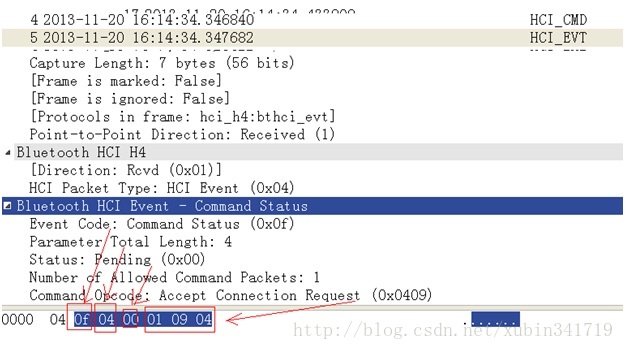
**一、主机控制接口协议  HCI** 蓝牙主机-主机控模型  


蓝牙软件协议栈堆的数据传输过程：

  
**1、蓝牙控制器接口数据分组：**指令分组、事件分组、数据分组  
**（1）、指令分组**

****  


如：Accpet Connection Request  
 Opcode为：0x0409  
 参数长度为: 07   
 参数中蓝牙地址为：00:0d:fd:5f:16:9f   
 角色为：从设备  0x01  
大端数据模式  
 指令为：09 04 07 9f 16 5f fd 0d 00 01  
**（2）、事件分组**



如上图：  
 Opcode :0x0409  
 状态： 0x00  
 总长度： 4字节  
 命令状态：0x0f  
**（3）、数据分组**ACL 数据分组

|  |  |  |  |
| --- | --- | --- | --- |
| 连接句柄（12bit） | PB(2bit) | BC(2bit) | 数据长度（16bit） |
| 数据………… | | | |

注：PB  Packet\_Boundary  BC Broadcast Flag  
SCO 数据分组

|  |  |  |
| --- | --- | --- |
| 连接句柄（12bit） | 保留（4bit） | 数据长度（16bit） |
| 数据………… | | |

**（4）、RS232分组指示器:**

|  |  |
| --- | --- |
| HCI 分组类型 | RS232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 |
| HCI错误消息分组 | 0x05 |
| HCI协商分组 | 0x06 |

**2、HCI控制命令**

**（1）、链路控制指令**

|  |  |  |
| --- | --- | --- |
| 命令 | OCF | 概述 |
| Inquiry | 0x0001 | 蓝牙设备进入查询模式，搜索临近设备 |
| Inquiry Cancel | 0x0002 | 退出查询模式 |
| Periodic Inquiry Mode | 0x0003 | 蓝牙设备在指定周期内自动查询 |
| Exit Periodic Inquiry Mode | 0x0004 | 退出自动查询模式 |
| Create Connection | 0x0005 | 按指定蓝牙设备的BD\_ADDR创建ACL链路 |
| Disconnect | 0x0006 | 终止现有连接 |
| Add SCO Connection | 0x0007 | 利用连接句柄参数指定的ACL连接创建SCO |
| Cancel Create Connection | 0x0008 |  |
| Accept Connection Request | 0x0009 | 接收新的呼入连接请求 |
| Reject Connection Request | 0x000A | 拒绝新的呼入连接请求 |
| Link Key Request Reply | 0x000B | 应答从主机控制器发出的链路密钥请求事件，并指定存储在主机上的链路密钥做为与BD\_ADDR指定的蓝牙设备进行连接使用的链路密钥请求事件 |
| Link Key Request Negative Reply | 0x000C | 如果主机上没有存储链路密钥，作为与BD\_ADDR指定的蓝牙设备进行连接使用的链路密钥，就应答从主机控制器发出的链路密钥请求事件 |
| PIN Code Request Reply | 0x000D | 应答从主机控制器发出的PIN请求事件，并指定用于连接的PIN |
| PIN Code Request Negative Reply | 0x000E | 当主机不能指定连接的PIN时，应回答从机控制器发出的PIN请求事件 |
| Change Connection Packet Type | 0x000F | 改变正在建立连接的分组类型 |
| Authentication Request | 0x0011 | 指定连接句柄关联的两个蓝牙设备之间建立身份鉴权 |
| Set Connection Encryption | 0x0013 | 建立取消连接加密 |
| Change Connection Link Key | 0x0015 | 强制关联了连接句柄的两个设备建立连接，并生成一个新的链路密钥 |
| Master Link Key | 0x0017 | 强制关联了连接句柄的两个设备利用主设备时链路密钥或常规密钥 |
| Remote Name Request | 0x0019 | 获取远端设备的名称 |
| Cancel Remote Name Request |  |  |
| Read Remote Supported Features | 0x001B | 请求远端设备所支持的特性列表 |
| Read Remote Extended Features |  |  |
| Read Remote Version Information | 0x001D | 从远端设备读取版本信息 |
| Read Clock Offset | 0x001F | 读取远端的时钟信息 |

**（2）、链路策略指令**

|  |  |  |
| --- | --- | --- |
| 命令 | OCF | 简介 |
| Hold Mode | 0x0001 | 改变LM状态和本地及远程设备为主模式的LM位置 |
| Sniff Mode | 0x0003 | 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 | 0x0004 | 结束连接句柄在当前呼吸模式里的呼吸模式 |
| Park State | 0x0005 | 改变LM状态和本地及远程设备为休眠模式的LM位置 |
| Exit Park State | 0x0006 | 切换从休眠模式返回到激活模式的蓝牙设备 |
| QoS Setup | 0x0007 | 指出连接句柄的服务质量参数 |
| Role Discovery | 0x0009 | 蓝牙设备连接后确定自己的主从角色 |
| Switch Role | 0x000B | 角色互换 |
| Read Link Policy Settings | 0x000C | 为指定连接句柄读链路策略设置。链路策略设置允许主机控制器指定用于连接句柄的LM连接模式 |
| Write Link Policy Settings | 0x000D | 为指定连接句柄写链路策略设置。链路策略设置允许主机控制器指定用于连接句柄的LM连接模式 |
| Read Default Link Policy Settings | 0x000E |  |
| Write Default Link Policy Settings | 0x000F |  |
| Flow Specification | 0X0010 |  |

**（3）、主机控制器与基带指令**

|  |  |  |
| --- | --- | --- |
| Set Event Mark | 0x0001 | 使能主机过滤HCI产生的事件 |
| Reset | 0x0003 | 复位蓝牙控制器、链路管理器、基带链路管理器 |
| Set Event Filter | 0x0005 | 使能主机指定不同事件过滤 |
| Flush | 0x0008 | 针对指定的蓝牙句柄，放弃所有作为当前待传输数据，甚至当前是属于多个在主机控制器里的L2CAP指令的数据块 |
| Read PIN Type | 0x0009 | 主机读取指定主机的PIN类型是可变的还是固定的 |
| Write PIN Type | 0x000A | 主机写入指定主机的PIN类型是可变的还是固定的 |
| Create New Unit Key | 0x000B | 创建新的单一密钥 |
| Read Stored Link Key | 0x000D | 读取存放在蓝牙控制器中的单个或者多个密钥 |
| Write Stored Link Key | 0x0011 | 写入存放在蓝牙控制器中的单个或者多个密钥 |
| Delete Stored Link Key | 0x0012 | 删除存放在蓝牙控制器中的单个或者多个密钥 |
| Write Local Name | 0x0013 | 修改蓝牙设备名称 |
| Read Local Name | 0x0014 | 读取蓝牙设备名称 |
| Read Connection Accept Timeout | 0x0015 | 读连接识别超时参数值，定时器终止后蓝牙硬件自动拒绝连接 |
| Write Connection Accept Timeout | 0x0016 | 写连接识别超时参数值，定时器终止后蓝牙硬件自动拒绝连接 |
| Read Page Timeout | 0x0017 | 读寻呼超时参数值，本地设备返回连接失败前，该值是允许蓝牙硬件定义等待远程设备连接申请时间 |
| Write Page Timeout | 0x0018 | 写寻呼超时参数值，本地设备返回连接失败前，该值是允许蓝牙硬件定义等待远程设备连接申请时间 |
| Read Scan Enable | 0x0019 | 写出扫描允许参数值---用来控制蓝牙设备周期性查询 |
| Write Scan Enable | 0x001A | 读出扫描允许参数值---用来控制蓝牙设备周期性查询 |
| Read Page Scan Activity | 0x001B | 读寻呼扫描间隔、寻呼扫描区间参数 |
| Write Page Scan Activity | 0x001C | 写寻呼扫描间隔、寻呼扫描区间参数 |
| Read Inquiry Scan Activity | 0x001D | 读查询扫描间隔、查询扫描区间参数 |
| Write Inquiry Scan Activity | 0x001E | 写查询扫描间隔、查询扫描区间参数 |
| Read Authentication Enable | 0x001F | 读取鉴权允许参数---控制蓝牙设备是否对每个连接进行鉴权 |
| Write Authentication Enable | 0x0020 | 写取鉴权允许参数---控制蓝牙设备是否对每个连接进行鉴权 |
| Read Encryption Mode | 0x0021 | 读加密模式数值---控制蓝牙设备是否对每个连接进行加密 |
| Write Encryption Mode | 0x0022 | 写加密模式数值---控制蓝牙设备是否对每个连接进行加密 |
| Read Class Of Device | 0x0023 | 读取设备类型参数值，用于区别设备能力 |
| Write Class Of Device | 0x0024 | 写设备类型参数值，用于区别设备能力 |
| Read Voice Setting | 0x0025 | 读取语音设置参数值，控制语音连接的各种设置 |
| Write Voice Setting | 0x0026 | 写语音设置参数值，控制语音连接的各种设置 |
| Read Automatic Flush Timeout | 0x0027 | 对指定句柄，读取刷新超时值 |
| Write Automatic Flush Timeout | 0x0028 | 对指定句柄，写入刷新超时值 |
| Read Num Broadcast Retransmissions | 0x0029 | 读取设备的广播重复发送次数，重复发送提高广播消息的可靠性 |
| Write Num Broadcast Retransmissions | 0x002A | 写入设备的广播重复发送次数，重复发送提高广播消息的可靠性 |
| Read Hold Mode Activity | 0x002B | 读取Hold Mode Activity的参数值，用来确定Hold挂起的时间 |
| Write Hold Mode Activity | 0x002C | 写入Hold Mode Activity的参数值，用来确定Hold挂起的时间 |
| Read Transmit Power Level | 0x002D | 对指定句柄，读取传输功率的参数值 |
| Read Synchronous Flow Control Enable | 0x002E | 读取SCO流量控制设置。通过使用该设置，主机控制器决定是否主机控制器发送与SCO连接句柄相关的完成分组事件的数量 |
| Write Synchronous Flow Control Enable | 0x002F | 读写入SCO流量控制设置。通过使用该设置，主机控制器决定是否主机控制器发送与SCO连接句柄相关的完成分组事件的数量 |
| Set Host Controller To Host Flow Control | 0x0031 | 主机控制器的打开、关闭，主机控制器到主机的流量控制 |
| Host Buffer Size | 0x0033 | 主机通知主机控制器自己的ACL、SCO数据缓冲区大小。主机控制器分段传输数据，而数据不会超出这个范围 |
| Host Number Of Completed Packets | 0x0035 | 当主机对于任何连接的句柄准备接受较多的HCI指令时，该指令用于通过主机指出主机控制器 |
| Read Link Supervision Timeout | 0x0036 | 读取连接管理超时参数。主从蓝牙设备用该参数监视链路丢失情况 |
| Write Link Supervision Timeout | 0x0037 | 写入连接管理超时参数。主从蓝牙设备用该参数监视链路丢失情况 |
| Read Number of Supported IAC | 0x0038 | 读取查询扫描期间本地蓝牙扫描的查询识别码（ICA）的数值 |
| Read Current IAC LAP | 0x0039 | 读取创建在查询扫描期间本地蓝牙设备正同时扫描的蓝牙识别码的LAP |
| Write Current IAC LAP | 0x003A | 写入创建在查询扫描期间本地蓝牙设备正同时扫描的蓝牙识别码的LAP |
| Read Page Scan Period Mode | 0x003B | 读取本地蓝牙设备的强制寻呼扫描区间模式 |
| Write Page Scan Period Mode | 0x003C | 写入本地蓝牙设备的强制寻呼扫描区间模式 |
| Read Page Scan Mode | 0x003D | 读取本地蓝牙设备的默认寻呼扫描区间模式 |
| Write Page Scan Mode | 0x003E | 写入本地蓝牙设备的默认寻呼扫描区间模式 |

**（4）、信息指令参数**

|  |  |  |
| --- | --- | --- |
| Read Local Version Information | 0x0001 | 读取本地蓝牙版本信息 |
| Read Local Supported Features | 0x0003 | 读取本地蓝牙设备特征表 |
| Read Local Extended Features | 0x0004 |  |
| Read Buffer Size | 0x0005 | 返回HCI缓冲容量。缓冲容量用于传输缓冲数据 |
| Read Country Code [Deprecated] | 0x0007 | 读取国家代码状态参数值 |
| Read BD ADDR | 0x0009 | 读取BD\_ADDR的参数值 |

**（5）、状态指令参数**

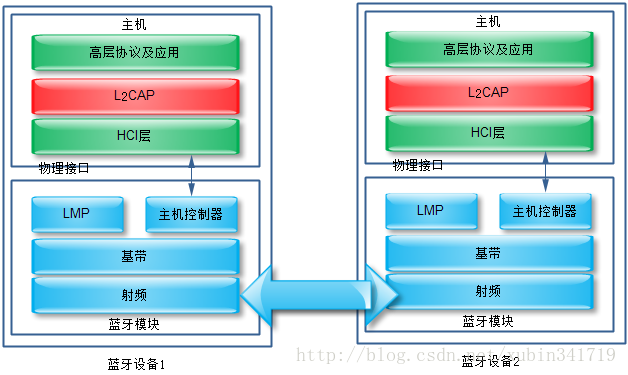
|  |  |  |
| --- | --- | --- |
| Read Failed Contact Count | 0x0001 | 读取对于其他设备特殊连接的Failed Contact Count参数值。Failed Contact Count记录在刷新时终止及当前正在传输的L2CAP数据指令被自动刷新后，主单元或从单元不能连续响应事件次数 |
| Reset Failed Contact Count | 0x0002 | 复位时对于其他设备的连接的Failed Contact Count的参数值。Failed Contact Count记录在刷新时终止及当前正在传输的L2CAP数据指令被自动刷新后，主单元或从单元不能连续响应事件次数 |
| Get Link Quality | 0x0003 | 读取指定连接句柄的Link Quality的值 |
| Read RSSI | 0x0005 | 读取对于其他蓝牙设备连接句柄的接收信号强度指示 |
| Read AFH Channel Map | 0x0007 |  |
| Read BD Clock | 0x0009 |  |

**（6）、测试指令**

|  |  |  |
| --- | --- | --- |
| Read Loopback Mode | 0x0001 | 读取主机端控制器会送模式的设置值。回送模式设置可以确定信息发送路径 |
| Write Loopback Mode | 0x0002 | 写入主机控制器会送模式的设置值。回送模式设置可以确定信息发送路径 |
| Enable Device Under Test Mode | 0x0003 | 允许本地蓝牙设备模块通过LMP测试指令接入测试模式。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场景，则发送该指令 |

**（7）、错误代码**

|  |  |  |  |
| --- | --- | --- | --- |
| 错误代码 | 错误含义 | 错误代码 | 错误含义 |
| 0x01 | 位置HCI指令 | 0x14 | 由于另一端引起连接中断：资源限制 |
| 0x02 | 不能连接 | 0x15 | 由于另一端引起连接中断：关机 |
| 0x03 | 硬件故障 | 0x16 | 本机中断连接 |
| 0x04 | 寻呼超时 | 0x17 | 重复尝试 |
| 0x05 | 身份验证失败 | 0x18 | 不允许匹配 |
| 0x06 | 键丢失 | 0x19 | 未知LMP PDU |
| 0x07 | 存储器已满 | 0x1A | 不支持远端特性 |
| 0x08 | 连接超时 | 0x1B | 拒绝SCO补偿 |
| 0x09 | 最大连接数 | 0x1C | 拒绝SCO间歇模式 |
| 0x0A | 连接到设备A的最大SCO连接数 | 0x1D | 拒绝SCO无线模式 |
| 0x0B | ACL连接已存在 | 0x1E | 非法链路管理参数 |
| 0x0C | 指令非法 | 0x1F | 未特别指明错误 |
| 0x0D | 由于资源有限，主机被拒绝 | 0x20 | 不支持链路管理器协议参数 |
| 0x0E | 由于安全原因，主机被拒绝 | 0x21 | 不允许角色改变 |
| 0x0F | 由于远端设备单连接设备，主机拒绝 | 0x22 | 链路管理响应超时 |
| 0x10 | 主机超时 | 0x23 | 链路管理错误处理事务冲突 |
| 0x11 | 不支持特性或参数值 | 0x24 | 不允许LMP PDU |
| 0x12 | 非法主机控制接口指令 | 0x25~0xFF | 保留 |
| 0x13 | 由于另一端引起连接中断：用户中断连接 |  |  |
|  |  |  |  |

**二、逻辑链路控制与适配协议  L2CAP** L2CAP位于基带之上，将基带的数据分组转换为便于高层应用的数据分组格式，并提供协议复用和服务质量交换等功能。L2CAP只支持ACL数据传输，不支持SCO数据。  
 L2CAP本身不提供加强信道可靠性和保证数据完整性的机制，其信道的可靠性依靠基带提供。  


**1、协议复用：**底层传输协议没有提供对高层协议的复用机制，因而L2CAP支持高层协议复用，L2CAP层可以区分其上的SDP、RFCOMM、TCS等。

**2、分段重组：**L2CAP层帮助实现基带的短PDU和高层的长PDU相互传输，L2CAP本身不完成任何PDU的分段重组，具体的分段重组有低层和高层来完成。

**3、服务质量 Qualityof Serivce 信息的交换：**蓝牙建立连接的过程中，L2CAP允许交互蓝牙所期望的服务质量，建立完成后，通过监视资源的使用情况，来保证服务质量。

**4、组抽象：**L2CAP忽略地址组概念，他只关心数据。

L2CAP信道有三种类型：

**A、面向连接信道：**Connection-OrientedCO，用于两个设备之间的数据通信。

**B、无连接信道：**Connection-LessCL，用来向一组设备广播方式传输数据。CID为固定值：0x0002。

**C、信令信道：**Signaling，用于创建CO通道，可以通过协商改变CO信道的特性。

CL信道的L2CAP\_PDU

|  |  |  |  |
| --- | --- | --- | --- |
| 长度（2bytes） | 信道ID（0x0002） | PSM(最小为2bytes) | 有效载荷 |

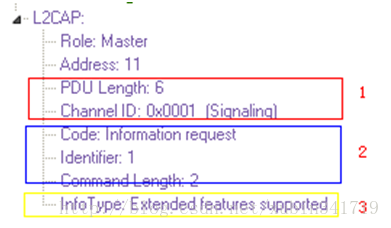
PSM为 协议/服务复用器Protocol/Service Multiplexer，一般为SDP、RFCOMM、TCS等中介协议复用。小于0x1000的值，0x0001对应SDP，0x0003对应RFCOMM、0x0005对应TCS。  
**（1）、蓝牙逻辑链路控制与适配协议信令：** L2CAP的信令通道的CID为0x0001

**信令指令分组：**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 长度（2byte） | CID(0x0001) | 指令1 | 指令2 | …………… | 指令n |
| L2CAP 分组头部分 | |  | | | |

**信令指令格式：**

|  |  |  |  |
| --- | --- | --- | --- |
| 代码（1byte） | 标识符（1byte） | 长度(2byte) | 数据 |
| 信令指令头 | | | |



如上图所示，一条L2CAP信令，1为L2CAP分组头，2为信令指令头，3为数据部分。

L2CAP:

         Role:Master

         Address:11

         PDULength: 6  //指令的长度，值为06 00

         ChannelID: 0x0001  (Signaling)//L2CAP的信令通道，值为01 00

         Code:Information request//信息请求，值为0a

         Identifier:1//标识符，值为01

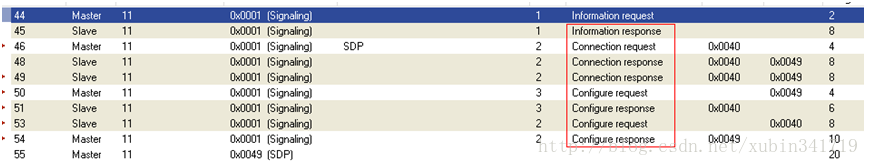
         CommandLength: 2//命令长度，值为02 00

         InfoType:Extended features supported//02 00

所以这条指令完整的为：

06 00 01 00 0a 01 02 00 02 00

**信令的其他操作如下：**

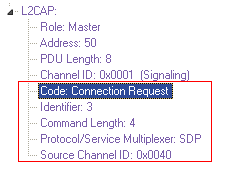


**L2CAP信令指令码：**

|  |  |  |
| --- | --- | --- |
| Code | Description |  |
| 0x00 | RESERVED | 保留 |
| 0x01 | Command reject | 拒绝命令 |
| 0x02 | Connection request | 连接请求 |
| 0x03 | Connection response | 连接响应 |
| 0x04 | Configure request | 配置请求 |
| 0x05 | Configure response | 配置响应 |
| 0x06 | Disconnection request | 断开请求 |
| 0x07 | Disconnection response | 断开响应 |
| 0x08 | Echo request |  |
| 0x09 | Echo response |  |
| 0x0A | Information request | 信息请求 |
| 0x0B | Information response | 信息响应 |

**1）、连接请求Connection\_Request Code=0x02**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 代码（0x02） | 标识符（1字节） | 长度（2字节） | PSM（2字节） | 源CID（2字节） |

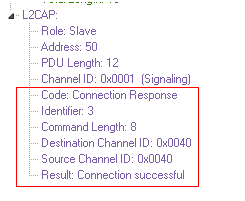
例如：SDP 连接请求  


如上红框所示：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 代码（0x02） | 标识符（1字节） | 长度（2字节） | PSM（2字节） | 源CID（2字节） |
| 0x02 | 3 | 4 | SDP | 0x0040 |

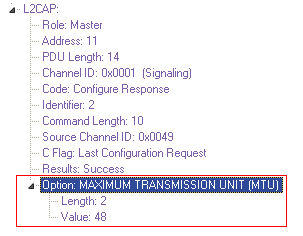
**2）、连接相应Connection\_Response Code=0x03**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 代码（0x03） | 标识符 | 长度 | 目标CID | 源CID | 结果 | 状态 |

例如：SDP请求响应  


如上面红框所示：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 代码（0x03） | 标识符 | 长度 | 目标CID | 源CID | 结果 | 状态 |
| 0x03 | 3 | 8 | 0x0040 | 0x0040 | 0x0000 |  |

**（2）、MTU MAXIMUMTRANSMISSION UNIT最大传输单元  
**

**MTU最大传输单元，L2CAP应用必须支持最小为48字节的MTU，默认值为672**

**（3）、QoS 服务质量**

**三、服务发现协议   SDP**

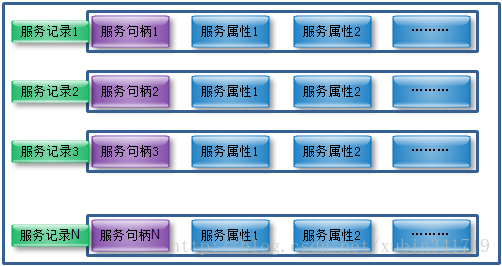
SDP两种服务发现模式：   
 **1）、服务搜索：**查询具有特定服务属性的服务；   
 **2）、服务浏览：**简单的浏览全部可用服务。  
**（1）、PDU 格式：（协议数据单元）**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| PDU ID（1byte） | Transaction ID（2byte） | 参数长度（2byte） | 参数1 | …… | 参数N |
| Header | | |  | | |

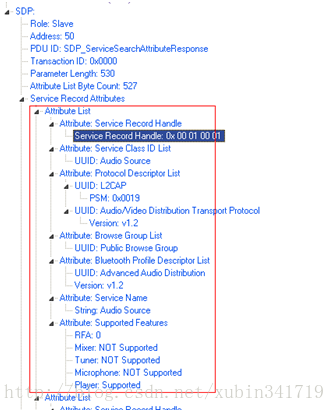
不同PDU ID实现SDP的不同功能，概述如下表格：

|  |  |  |
| --- | --- | --- |
| Value | Parameter Descirption |  |
| 0x00 | Reserved | 保留 |
| 0x01 | SDP\_ErrorResponse | 错误响应 |
| 0x02 | SDP\_ServiceSearchRequest | 服务搜索请求 |
| 0x03 | SDP\_ServiceSearchResponse | 服务搜索响应 |
| 0x04 | SDP\_ServiceAttributeRequest | 服务属性请求 |
| 0x05 | SDP\_ServiceAttributeResponse | 服务属性响应 |
| 0x06 | SDP\_ServiceSearchAttributeRequest | 服务搜索属性请求 |
| 0x07 | SDP\_ServiceSearchAttributeResponse | 服务搜索属性响应 |
| 0x08-0xff | Reserved | 保留 |

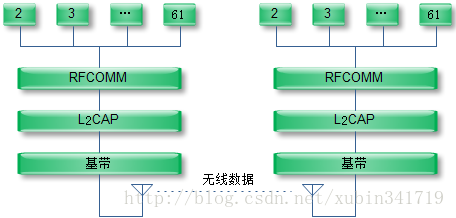
**（2）、服务记录表** SDP的服务记录表对每一个服务进行描述，每条记录包含服务句柄、一组服务属性：



Service Record Attributes：服务记录；  
Service Record Handle 服务句柄；  
Attribute 服务属性；



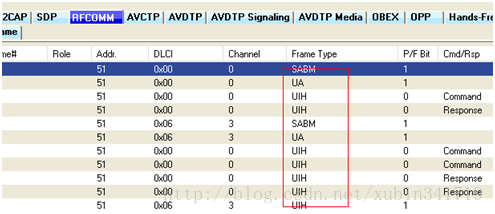
**四、串口仿真协议   RFCOMM**

为建立在串口之上的传统应用提供环境接口，使他们可以做比较少协议改动就可以在蓝牙无线通信无线链路上工作。多路串口仿真是RFCOMM的重要功能，通过多路复用器(multiplexer)，一条L2CAP链路可以同时 多个串行应用。  
 两台设备间的串口仿真:  


RFCOMM 两个蓝牙设备之间可以支持多达60多路仿真串口。

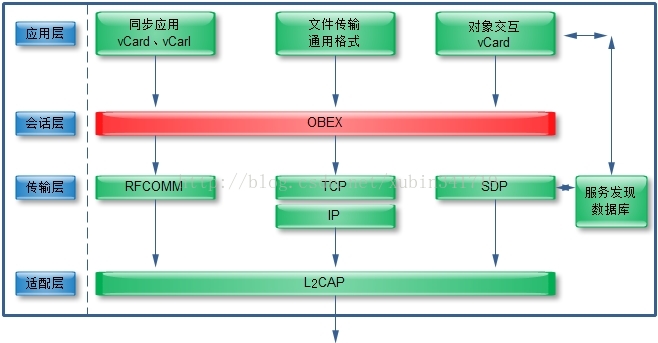
**RFCOMM帧类型如下：**

|  |  |
| --- | --- |
| SABM | 异步平衡模式设置指令 |
| UA | 未加编号的确认响应 |
| DM | 断开连接模式响应 |
| DISC | 断开连接指令 |
| UIH | 带头校验的未编号信息命令和响应 |



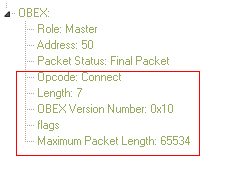
**第四章 蓝牙协议规范（irOBEX、BNEP、AVDTP、AVCTP）**

**一、IrDA互操作协议** IrOBEX 红外对象交互协议，简称OBEX，使高层协议同时运作在蓝牙和红外的无线链路之上。

  
 主要操作指令有：连接操作、断开操作、Put操作、Get操作。

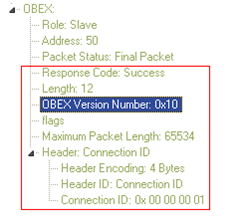
**1、连接操作 ,操作码0x80**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 字节0 | 字节1、2 | 字节3 | 字节4 | 字节5、6 | 字节7～n |
| 0x80 | 连接请求分组长度 | OBEX版本号 | 标志 | 客户端可接收最大的OBEX分组长度 | 可选头 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 字节0 | 字节1、2 | 字节3 | 字节4 | 字节5、6 | 字节7～n |
| 0x80 Connect命令 | 7 | 0x10 | 标志 | 65534 | 可选头 |

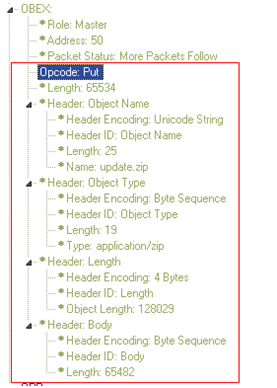
**连接响应**



**2、断开操作**  操作码为0x81

**3、Put操作**操作码为0x02

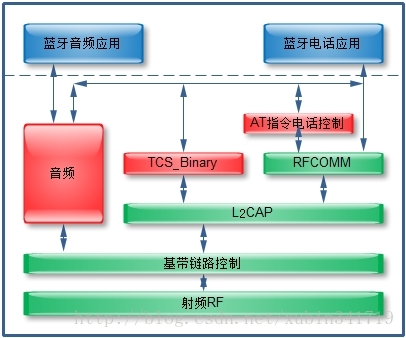
连接成功后，客户端通过Put请求向服务器“推送”对象，如果对象较大，Put请求可以用多个Put请求分组。



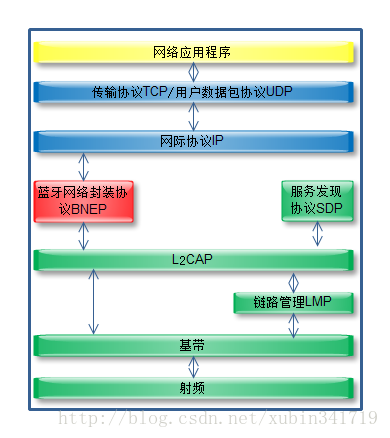
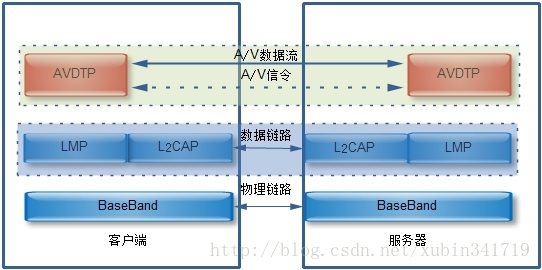
**4、Get操作**操作码为0x03

**二、音频与电话控制协议**

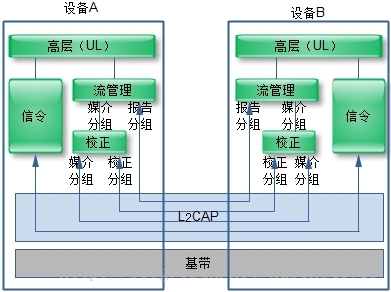
**1、框架部分**

****

蓝牙音频如上图协议栈所示：音频通过基带传输同步面向连接分组实现，没有以规范的形式给出，不是协议栈的一部分。  
 TCS\_Binary是一种基于分组电话控制二进制编码指令集，位于L2CAP之上。实现蓝牙无绳电话、对讲机功能。  
 RFCOMM用于AT指令，拨号上网、蓝牙耳机、耳麦、传真通过AT发送指令控制。  
**2、音频部分** 64kbps电信级语言质量音频流  
 CVSD  continuous variable slope delta 连续可变斜率增量。  
 PCM  pulse code modulation 。  
 PCM存在斜率效应。CVSD使用音节压缩算法，编码步长根据信号斜率变化自动调整，是现在比较好的编码方案，提高语言的抗干扰能力。  
**3、电话控制部分** TCS-Binary电话控制部分。  
（1）、电话呼叫  
 呼叫控制、呼叫建立、呼叫拆除；  
（2）、组管理  
 访问权限请求、分布式配置、快速内部成员访问。  
**三、网络封装协议  BNEP** BNEP BluetoothNetworkEncapsulation Protocol 网络封装协议。  
 为了使集成蓝牙技术的电脑、电话、PDA、家用电器等网络设备交换信息，需要在网络层统一数据分组。网络封装协议将来自不同网络的数据分组重新封装，通过L2CAP进行传输。这部分协议感觉在现实中用处不大，有更多简单便捷的方法去实现网络功能。  
 BNEP支持Ipv4、Ipv6、IPX

  
**四、音视频分发协议AVDTP** AVDTPAudio/Video Distribution Transport Protocol音视频分发传输协议

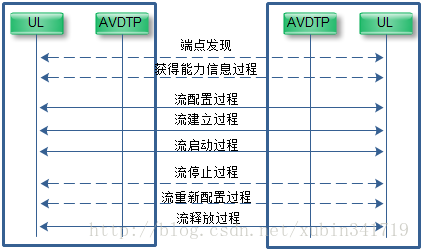
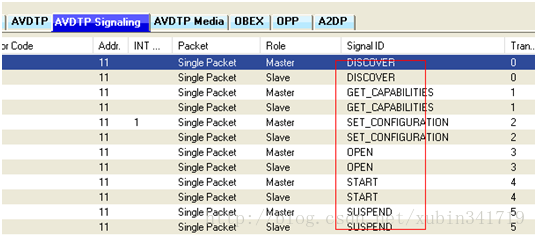
有关A/V的协议 AVDTP音视频分发传输协议、AVCTP音视频控制传输协议、GAVDP通用音视频分发框架、A2DP高级音频分发框架、AVCRP音视频遥控框架  
**1、基本概念术语  
 流stream:**流是音视频传输的数据形式，单向传输，在AVDTP中被分为媒介分组。流有句柄HS统一标识。



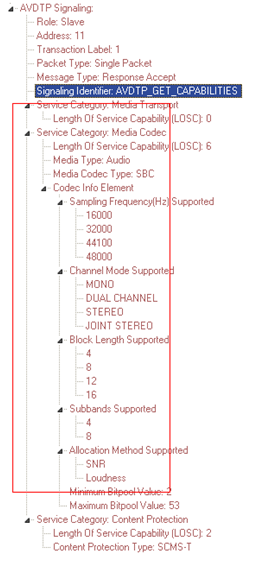
**2、信令** AVDTP信令列表

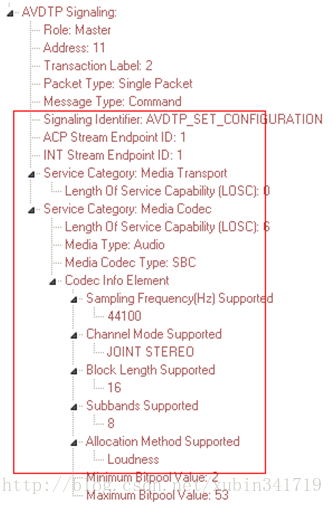
|  |  |  |
| --- | --- | --- |
| 命令 | 信令标识符 | 描述 |
| AVDTP\_DISCOVER | 0x01 | 发现设备中的流端点 |
| AVDTP\_GET\_CAPABILITIES | 0x02 | 获得流端点的信息能力 |
| AVDTP\_SET\_CONFIGURATION | 0x03 | 对SEP进行配置 |
| AVDTP\_GET\_CONFIGURATION | 0x04 | 获取SEP当前配置 |
| AVDTP\_RECONFIGURE | 0x05 | 对SEP重新配置 |
| AVDTP\_OPEN | 0x06 | 成功的配置SEP后，打开流 |
| AVDTP\_START | 0x07 | 流被打开：用于开始形成流；流暂停时：用于重新形成流。 |
| AVDTP\_CLOSE | 0x08 | 对SEP关闭 |
| AVDTP\_SUSPEND | 0x09 | 请求SEP暂停 |
| AVDTP\_SECURITY\_CONTROL | 0x0A | 设置设备内容保护、或者请求设备状况信息 |
| AVDTP\_ABORT | 0x0B | 中断正在建立或者传输的过程 |
| AVDTP\_GET\_ALL\_CAPABILITIES |  |  |
| AVDTP\_DELAYREPORT |  |  |

这部分信令，实现了蓝牙的A2DP 数据流的控制；  
**（1）、流的信令管理流程**

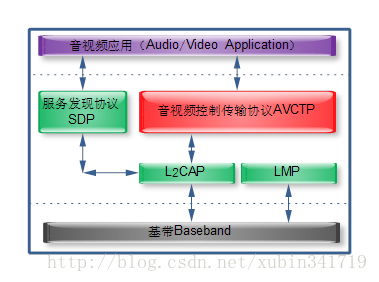
  


**（2）、get capabilities  获取支持特性**

****

**（3）、set configuration 配置音频参数  
**

其他指令类似去上面两个的操作。  
**五、音视频控制传输协议AVCTP**

**** AVCTP可以使音视频设备同时支持多个应用框架，每个应用框架定义了各自相应的消息格式与应用规则。  
 这部分操作，在现实的应用中也有不足的地方，蓝牙传输的数据量有限，实现这些功能有一定的不足。随着科学技术的发展，蓝牙在无线通信方面的优点、缺点都凸显出来，找的合适的方向，合理的发展方向是硬道理。

蓝牙芯片厂商：

CSR公司（Cambridge Silicon Radio）(目前最大的蓝牙芯片的全球供应商)

Broadcom公司

ISSC公司

TI公司 (CC2541)

MTK公司（MT6620）