



## 第4章 无线个域网



# 内容提要



- 4. 1 概述
- 4. 2 IEEE 802. 15标准
- 4. 3 蓝牙技术简介
- 4. 4 蓝牙无线电规范
- 4. 5 蓝牙基带规范
- 4. 6 蓝牙链路管理器规范
- 4. 7 蓝牙逻辑链路控制和自适应协议
- 4. 8 蓝牙服务发现协议

## 4.1 概述



- 手机、PC机、汽车、音响、电视、微波炉、电冰箱等**消费类产品**非常普及，人们希望有一种短距离、低成本、低功耗的无线通信方式，实现不同功能单一设备的互联，提供小范围内设备的自组网机制，并通过一定的安全接口完成**自组小网与广域大网的互通**。
- 无线个人区域网 (Wireless Personal Area Network, WPAN, 简称无线个域网) 技术就是一种满足上述应用需求的**小范围无线连接、微小网自主组网**的通信技术。

# 无线个域网技术



- 蓝牙(Blue Tooth)
- IrDA: 红外数据组织, 市场份额最大
- HomeRF: 家庭设备无线互联的工业标准
- UWB: 超宽带, 在很宽频段内发生短脉冲
- Zigbee: 低速率低成本个域网技术

# 内容提要

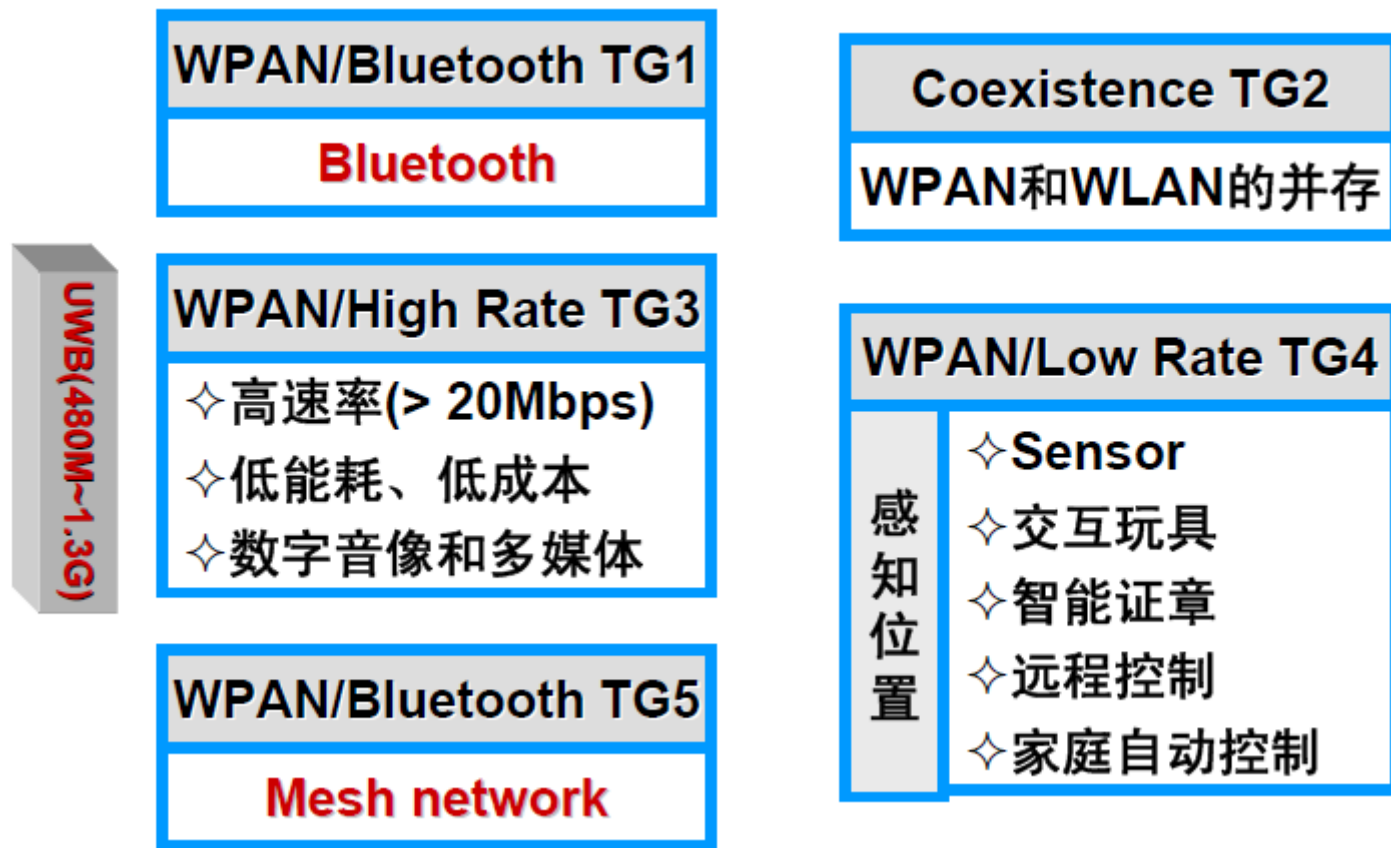


- 4. 1 概述
- 4. 2 IEEE 802. 15标准
- 4. 3 蓝牙技术简介
- 4. 4 蓝牙无线电规范
- 4. 5 蓝牙基带规范
- 4. 6 蓝牙链路管理器规范
- 4. 7 蓝牙逻辑链路控制和自适应协议
- 4. 8 蓝牙服务发现协议

## 4.2 IEEE802.15标准



IEEE 802.15工作组是IEEE针对无线个人区域网而成立的，开发有关短距离范围的WPAN标准。



## 4. 2. 1 标准构成



- 802. 15. 1是以既有蓝牙标准为基础，制定蓝牙无线通信规范的一个正式标准。
- 802. 15. 2工作组目的是要802. 11和802. 15开发共存的推荐规范。
- 802. 15. 3工作组的兴趣在开发对比于802. 11设备是低成本和低功耗的设备的标准上。
- 802. 15. 3a的目标是要在使用同样的MAC层上提供比802. 15. 3更高的数据率
- 802. 15. 4工作组则开发了一个非常低成本、非常低功耗的比802. 15. 1数据率要低的设备标准。

# IEEE802.15协议体系结构

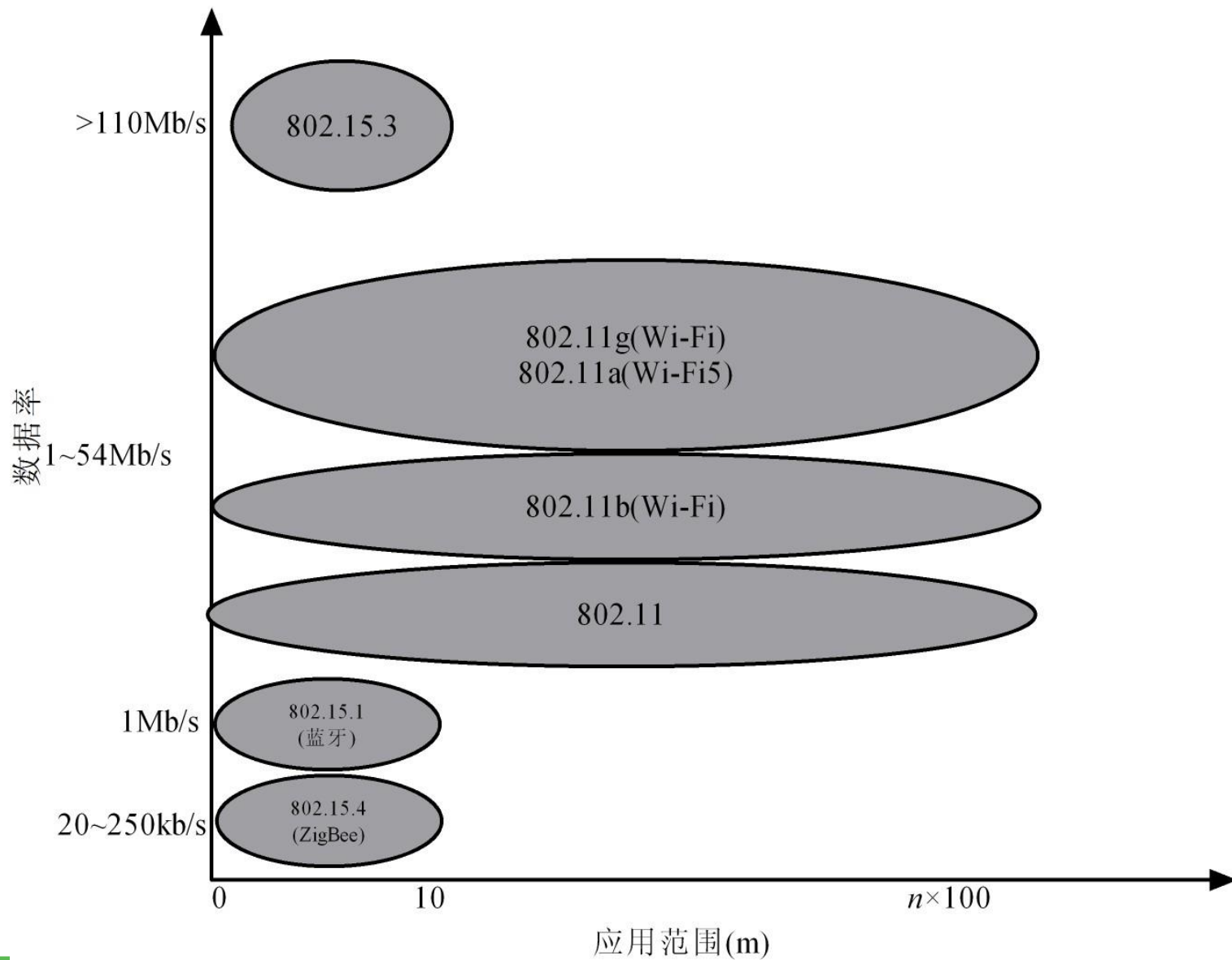


## 逻辑链路控制 (LLC)

逻辑链路控制 (LLC)					
802.15.1 MAC	802.15.3 MAC		802.15.4 MAC		
802.15.1 2.4GHz 1Mb/s	802.15.3 2.4GHz 11,22,33, 44,55Mb/s	802.15.3a ? >110Mb/s	802.15.4 868MHz 20kb/s	802.15.4 915MHz 40kb/s	802.15.4 2.4GHz 250kb/s



# WLAN与WPAN



# 内容提要



- 4. 1 概述
- 4. 2 IEEE802. 15标准
- 4. 3 蓝牙技术简介
- 4. 4 蓝牙无线电规范
- 4. 5 蓝牙基带规范
- 4. 6 蓝牙链路管理器规范
- 4. 7 蓝牙逻辑链路控制和自适应协议
- 4. 8 蓝牙服务发现协议

## 4.3.1 蓝牙技术的诞生与发展



- ❑ 1994Ericsson发起multi-communicator link的研究;
- ❑ 1998成立了特别兴趣小组（SIG）并更名bluetooth
  - 成员：Ericsson、IBM、Intel、Nokia、Toshiba
  - 目标：将计算、通信设备以及附加设备通过短程、低耗、低成本的无线电波连接起来
  - 发展：Lucent、3Com、Microsoft和Motorola加入SIG；现SIG成员超过2500个；
- ❑ 1999Bluetooth 1.0发布；
- ❑ 2002IEEE采纳了bluetooth的物理层和数据链路层，发布了IEEE802.15.1；

# 为什么叫“bluetooth”



## ❑ Ericsson借用了Harald Gormsen的昵称 blatand → “Bluetooth”

- 丹麦的国王（ A.D.940 ~ 981 ）
- 统一了丹麦和挪威



## ❑ 寓意统一不同制造商的不同设备

- Harald把基督教带到斯堪的纳维亚
- Harald统治了丹麦和挪威
- Harald思索笔记本和手机的无缝通信

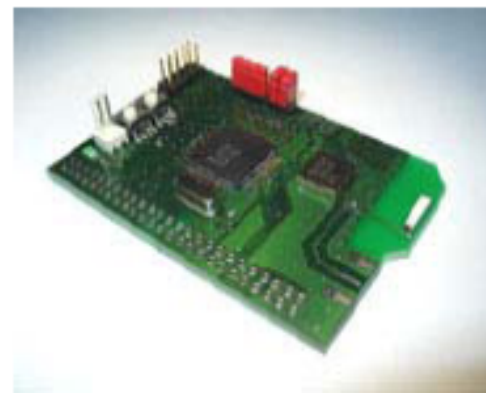
## ❑ 2000年5月发布了蓝牙应用新图标



# Bluetooth是什么

## ❑ 蓝牙是无线技术规范

- 短程：最大传输距离**10米**
- 性能中等：**721Kbps**
- 动态配置：自组联网/漫游
- 低能耗(< **2.5mW**)：适用于手持应用
- 模块大小：**9x9 mm**
- 支持语音和数据传输



# 蓝牙技术优点



- 可以随时随地用无线接口代替有线电缆连接;
- 具有很强的移植性, 可应用于多种通信场合, 如 WAP、GSM(全球移动通信系统)、DECT(欧规数字无绳通信)等, 引入身份识别后可以灵活地实现漫游;
- 低功耗, 对人体伤害小;
- 蓝牙集成电路简单, 成本低廉, 实现容易, 易于推广。

# 计算机产品中的蓝牙



## ❑ 计算机设备

- 笔记本
- PDAs
- 桌面PC
- 宽带接入点
  - ✧ Ethernet/xDSL/cable
- 打印机
- 扫描仪
- 视频播放器

## ❑ 计算机应用

- 外设连接
  - ✧ 打印机/扫描仪/视频播放器
- 网络接入
  - ✧ 宽带接入点
  - ✧ 分组无线蜂窝电话
- 文件同步操作
  - ✧ 日历/联系管理
- 文件传输
  - ✧ vCards/MP3/数字图片

# 电话和消费类产品中的蓝牙



## ❑ 电话设备

- 蜂窝耳麦
- 无线耳麦
- **PSTN**接入点
  - ✧ 投币电话
  - ✧ 酒店/居家电话

## ❑ 消费类设备

- 机顶盒
- 数码相机
- **MP3**播放器
- 家庭音响

## ❑ 电话应用

- 免提使用
- 文件同步操作
  - ✧ 日历/联系管理
- 语音和数据的线路

## ❑ 消费类应用

- 文件传送
  - ✧ **MP3**/数码相片
- 外设连接
  - ✧ 键盘/鼠标打印机



### 4.3.3 蓝牙标准文档构成



- **核心规范 (core specifications)**: 描述了从无线电接口到链路控制的不同层次蓝牙协议体系结构的细节。
- **概要规范 (profile specifications)**: 考虑使用蓝牙技术支持不同的应用。每个概要规范讨论在核心规范中定义的技术，以实现特定的应用模型 (Usage Model)。分为强制、可选和不适用。可划分为**电缆替代**或**无线音频**。

## 4.3.4 蓝牙协议体系结构

AT=注意序列(modem前缀)

IP=网际协议

OBEX=对象交换协议

PPP=点到点协议

RFCOMM=无线电频率通信

SDP=服务发现协议

TCP二传输控制协议

TCS BIN=二进制电话控制规范

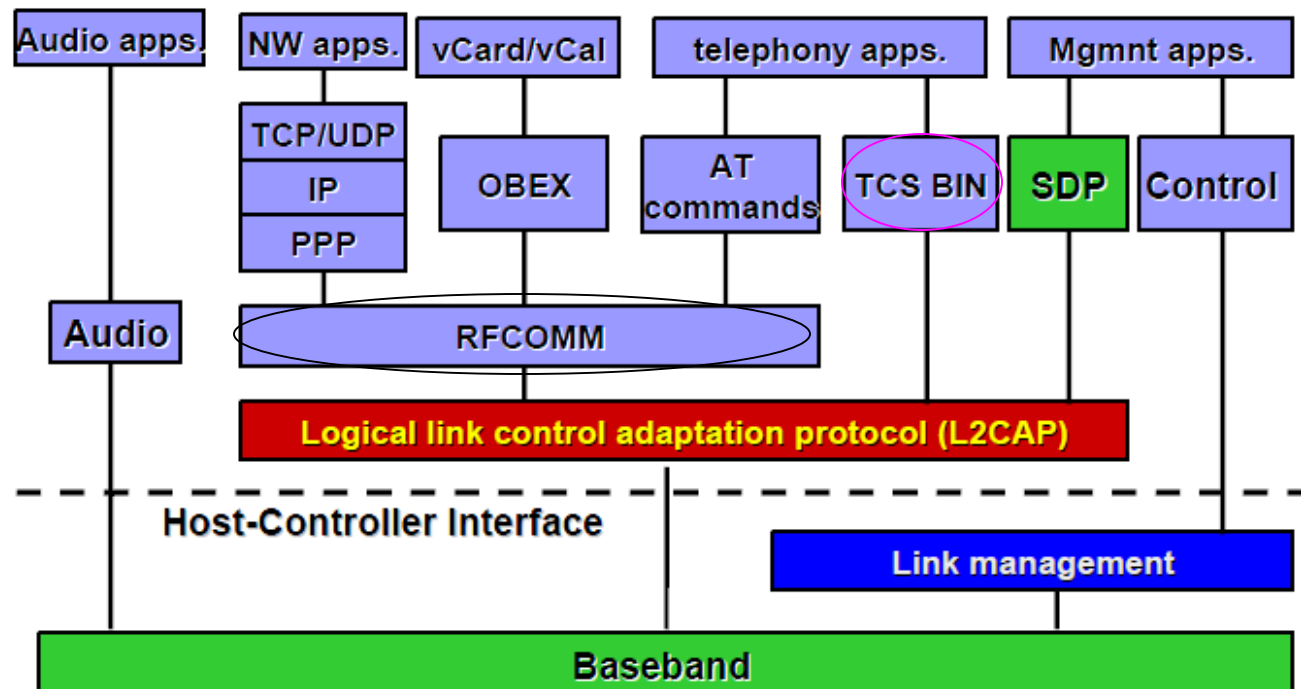
UDP=用户数据报协议

vCal=虚拟日历

vCard=虚拟卡

WAP=无线应用协议

WAE=无线应用环境



HCI在baseband和L2CAP之间提供了基带控制器和链路管理控制器的命令接口，以及硬件状态和控制寄存器的访问。

# 核心协议(core protocol)形成五层栈

- **无线电**(radio): 确定包括频率、跳频的使用、调制模式和传输功率在内的空中接口细节。
- **基带**(baseband): 考虑一个微微网中的连接建立、寻址、分组格式、计时和功率控制。
- **链路管理器协议**(link manager protocol, LMP): 负责在蓝牙设备和正在运行的链路管理之间建立链路。包括诸如认证、加密及基带分组大小的控制和协商等安全因素。
- **逻辑链路控制和自适应协议**(logical link control and adaptation protocol, L2CAP): 使高层协议适应基带层。L2CAP提供无连接和面向连接服务。
- **服务发现协议**(service discovery protocol, SDP): 询问设备信息、服务与服务特征, 使得在两个或多个蓝牙设备间建立连接成为可能。

# 概要规范及接纳协议



## 概要规范

- **RFCOMM**: 属于电缆替代, 提供虚拟串行口
- **TCS-BIN**: 属于无线音频中的电话控制协议, 二进制通话控制规范

## 接纳协议 (由其他标准制定并被纳入蓝牙体系结构)

- **PPP**: 一个在点对点链路上传输IP数据报的因特网标准协议
- **TCP/UDP/IP**: 属于TCP/IP协议簇的基础协议
- **OBEX**: 由IrDA开发的会话层对象交换协议
- **WAE/WAP**: 无线应用环境和无线应用协议

## 4.3.5 应用模型



大量应用模型定义在蓝牙的概要规范文档中。本质上，**一个应用模型一套实施特定的基于蓝牙的应用的协议**。每个概要文件定义了支持一特定应用模型的协议和协议特性。

### ❑ Bluetooth v1.1规范了13种应用+相应的协议栈

面向网络连接	面向电话	无线设备交换数据
✧LAN access ✧Dial-up networking ✧Fax	✧Cordless telephony ✧Intercom ✧Headset	✧Object push ✧File transfer ✧Synchronization

**Profile: 定义了支持特定应用的协议以及协议特性。**

其他实际应用的基础		
Generic access Service discovery	Serial port	Generic object exchange

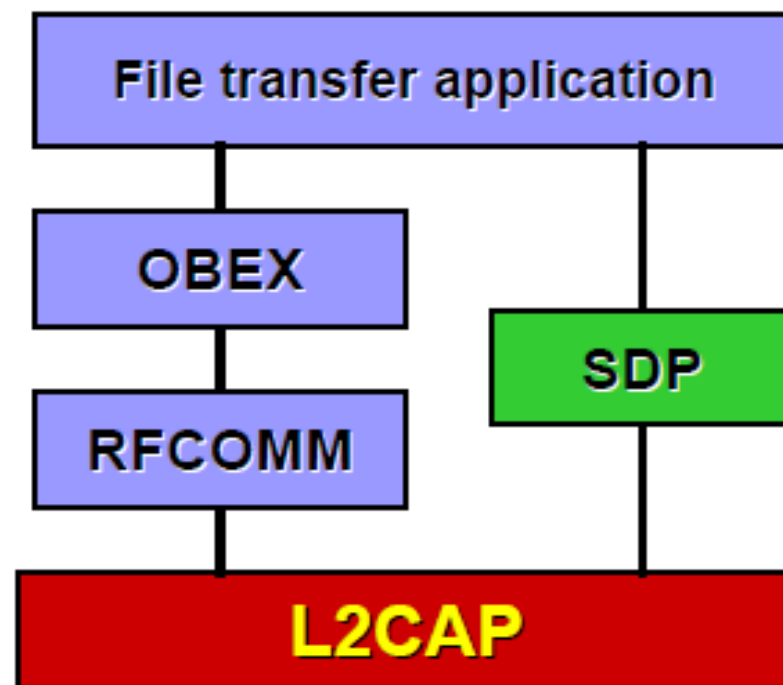
# 文件传输

## □ 传送能力

- 目录
- 文件
- 文档
- 映像
- 流媒体

## □ 浏览能力

- 文件夹

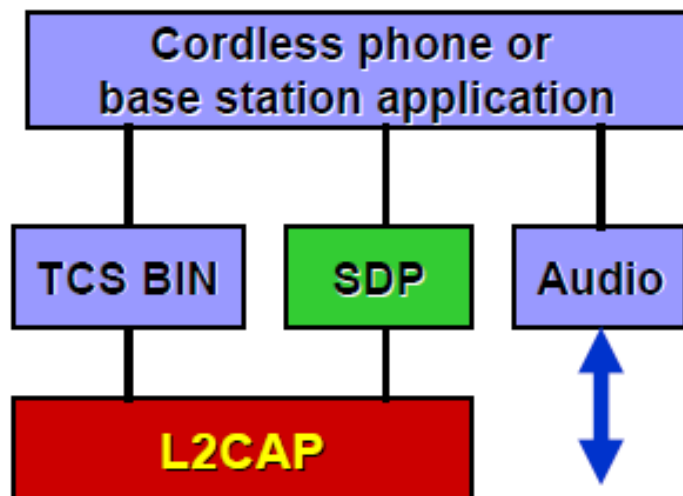


**OBEX:** 对象交换协议是由红外数据协会开发的用来交换对象的会话层协议。

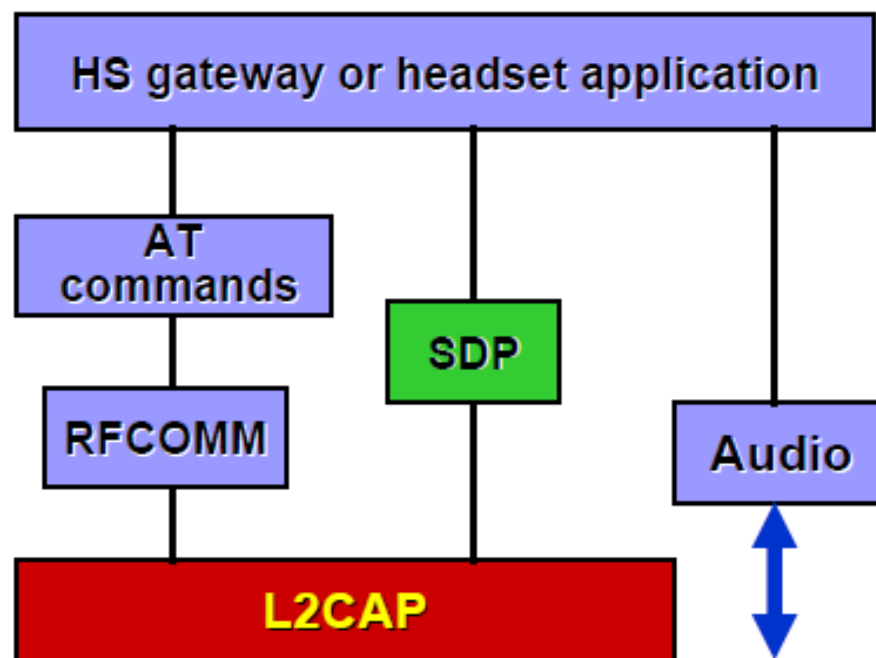
# 语音应用

## ☐ 三合一电话

○ 呼叫/移动管理/对讲



## ☐ 耳麦



- ◇ TCSBIN 定义了两个蓝牙设备之间建立语音和数据呼叫的控制信令
- ◇ ATcommands 类似于一般的调制解调器

# 其他最高优先级的应用模型



- 桥接因特网：一台PC可以无线连接到一部移动电话或无绳modem上，提供拨号上网和传真功能。
- 局域网接入：一个piconet上的设备可以接入LAN。
- 同步：为PIM信息提供设备与设备间的同步。



# 蓝牙技术应用（1）

## 连接计算机以及其他外部设备



- 整洁办公空间
- 需要电池供给能量

# 蓝牙技术应用 (2)

## 支持自组网络

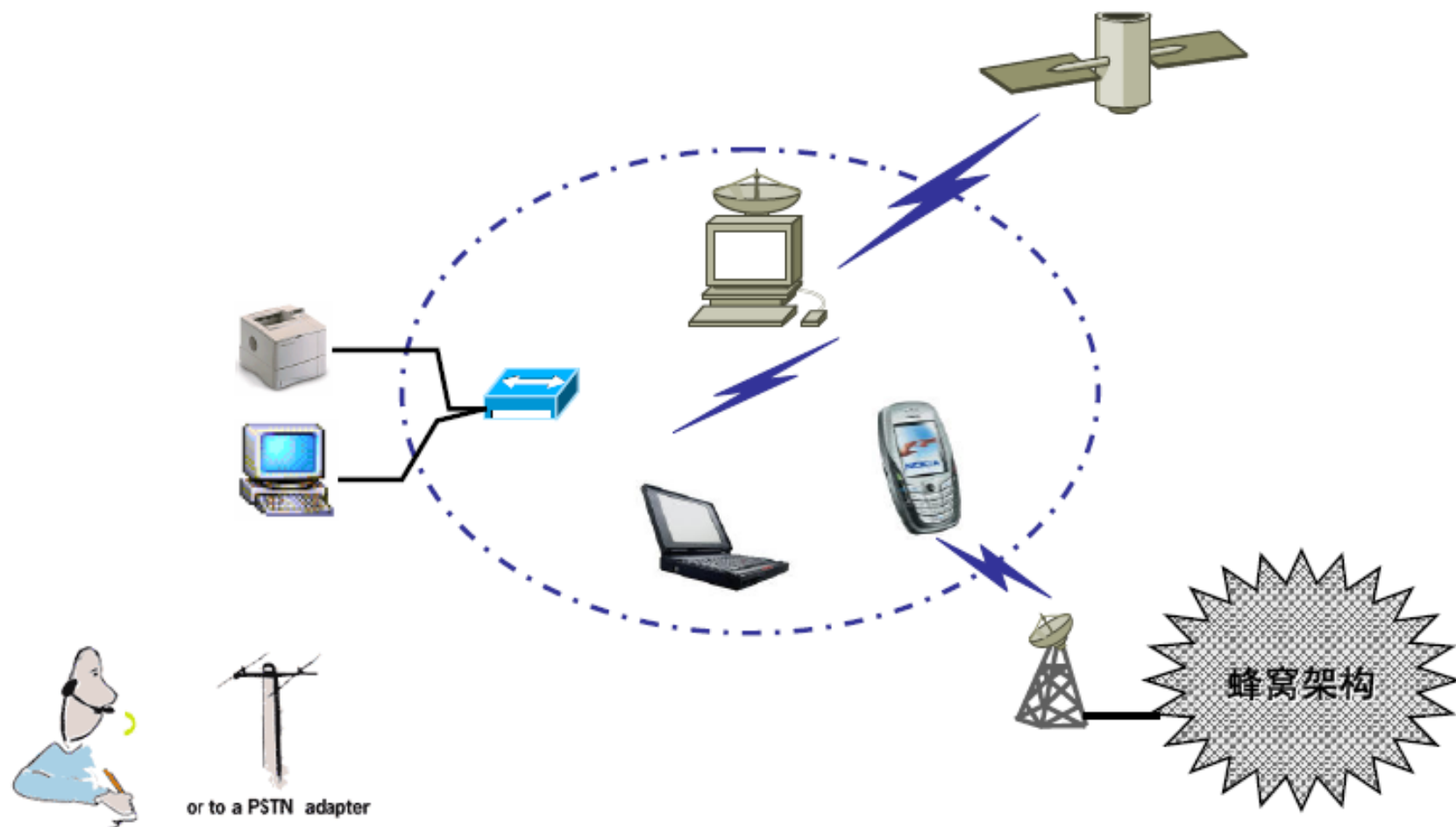


○ 临时性

○ 不需要802.11适配器

# 蓝牙技术应用 (3)

## 充当访问Internet的接入点



# 蓝牙技术应用 (4)

## 构建居家网络环境



# 蓝牙技术应用 (5)

## 运动中的连接



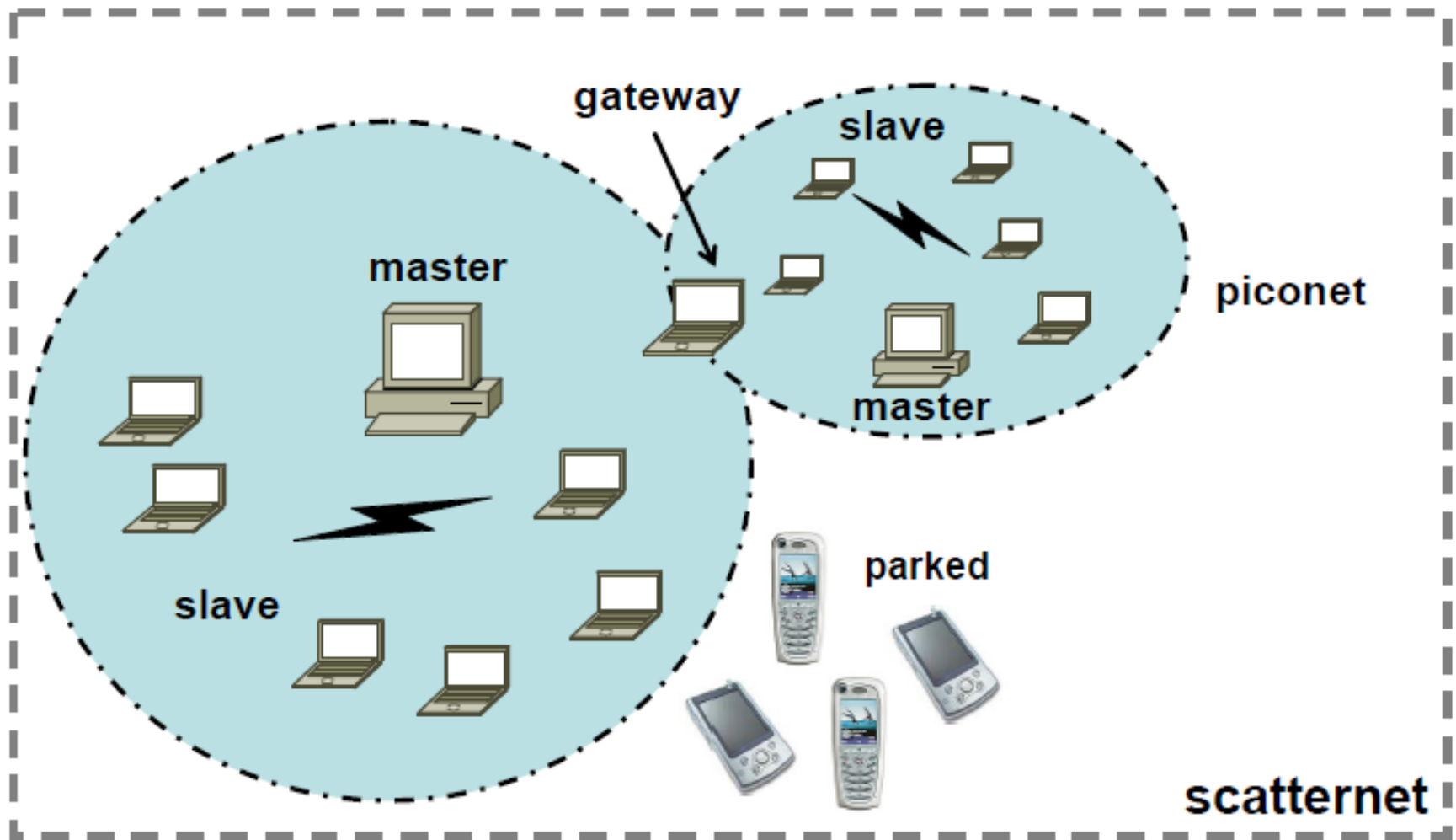
## 4.3.7 Bluetooth拓扑结构



- **点-点模式**：两个蓝牙设备直接通信
- 蓝牙基本联网单元是一个**微微网**（piconet），由一台主设备和1-7台活跃的从设备组成。
- 一个piconet中的设备也可作为另一个piconet的一部分存在，并在每个piconet中，起从设备或主设备功能，这种形式的重叠被称为**散布式网络**（scatternet）。
- 多达256个piconet可以连接成更大的网络。



# 拓扑结构



# Bluetooth中的piconet



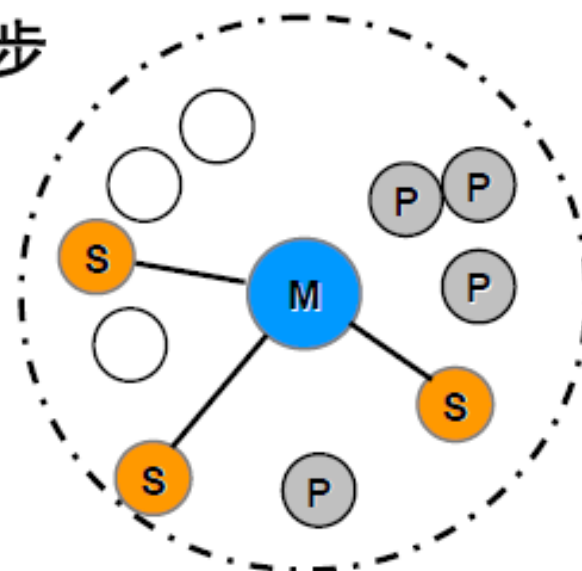
## ❑ Piconet的组成

- 1个Master节点控制FH通信的同步
- 7个Slave节点
- 255个非活跃Parked\*
  - ✧ 遵循master的跳频算法
- Stand by\*



✧ 释放MAC地址  
✧ 保持MAC地址

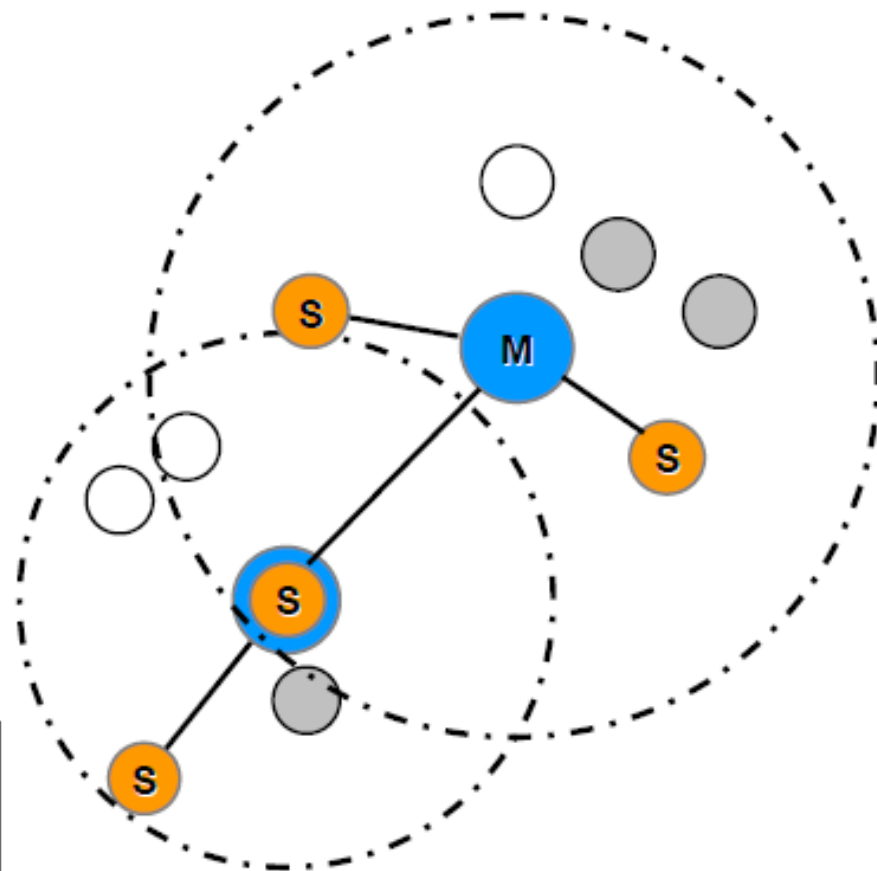
节点的操作状态





# Bluetooth中的scatternet

- 时间和空间层叠的多个 piconets 组成一个散网
- 几个 masters 连接到同一个 slave
- 一个 master 可以是另一个网络的 slave



标准只定义了scatternet的概念，并没有给出构造scatternet的机制。

# 内容提要



- 4. 1 概述
- 4. 2 IEEE802. 15标准
- 4. 3 蓝牙技术简介
- 4. 4 蓝牙无线电规范
- 4. 5 蓝牙基带规范
- 4. 6 蓝牙链路管理器规范
- 4. 7 蓝牙逻辑链路控制和自适应协议
- 4. 8 蓝牙服务发现协议

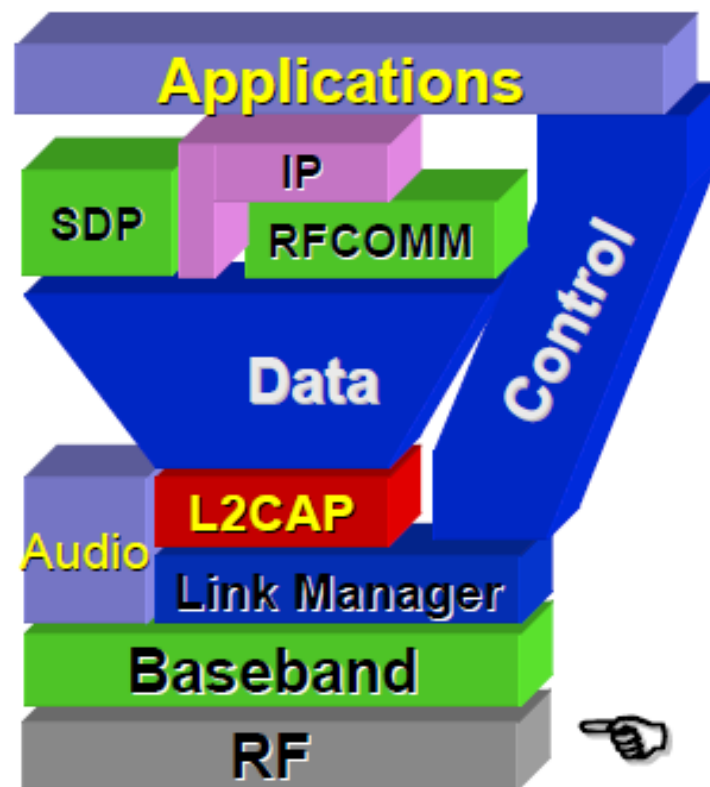
## 4.4 蓝牙无线电规范

### □ 规范

- 定义了载波频率和输出功率

### □ 特点

- 低功率
- 传输距离为10米
- 2.4GHz的ISM
- 79个信道1MHz
- 跳频扩频技术1600/s
- 收发器的能量分3级



## 4.4 蓝牙无线电规范



拓 扑	一个逻辑的星形结构中，高达7条并行链路
调制	GFSK
数据速率的峰值/Mb/s	1
RF带宽	220kHz(-3dB)， 1MHz(-20dB)
RF波段	2.4GHz,ISM波段
RF载波	23/79
载波的间隔/MHz	1
传输功率/W	0.1
微微网的接入	FH-TDD-TDMA
频跳率/跳/s	1600
分布式网络的接入	FH-CDMA

# 国际上蓝牙的频率分配



区 域	调节范围/GHz	RF信道
美国、欧洲的大部分国家和其他国家中的大部分	2.4~2.4835	$f=2.402+n\text{MHz}, n=0, \dots, 78$
日本	2.471~2.497	$f=2.473+n\text{MHz}, n=0, \dots, 22$
西班牙	2.445~2.475	$f=2.449+n\text{MHz}, n=0, \dots, 22$
法国	2.4465~2.4835	$f=2.454+n\text{MHz}, n=0, \dots, 22$

蓝牙利用波段中的2.4GHz波段。在大多数国家，此带宽足以定义79个1MHz的物理信道

# 内容提要



- 4. 1 概述
- 4. 2 IEEE802. 15标准
- 4. 3 蓝牙技术简介
- 4. 4 蓝牙无线电规范
- 4. 5 蓝牙基带规范
- 4. 6 蓝牙链路管理器规范
- 4. 7 蓝牙逻辑链路控制和自适应协议
- 4. 8 蓝牙服务发现协议

## 4.5 蓝牙基带规范



4.5.1 跳频

4.5.2 物理链路

4.5.3 分组

4.5.4 纠错

4.5.5 逻辑信道

4.5.6 信道控制

4.5.7 蓝牙音频

## 4.5.1 跳频



- 目的1：阻碍干扰和多路效应。
- 目的2：为放置在不同微微网中的设备提供多种接入的形式。
- 在一个伪随机序列中，通过从一个物理信道跳到另一个物理信道，出现了跳频。

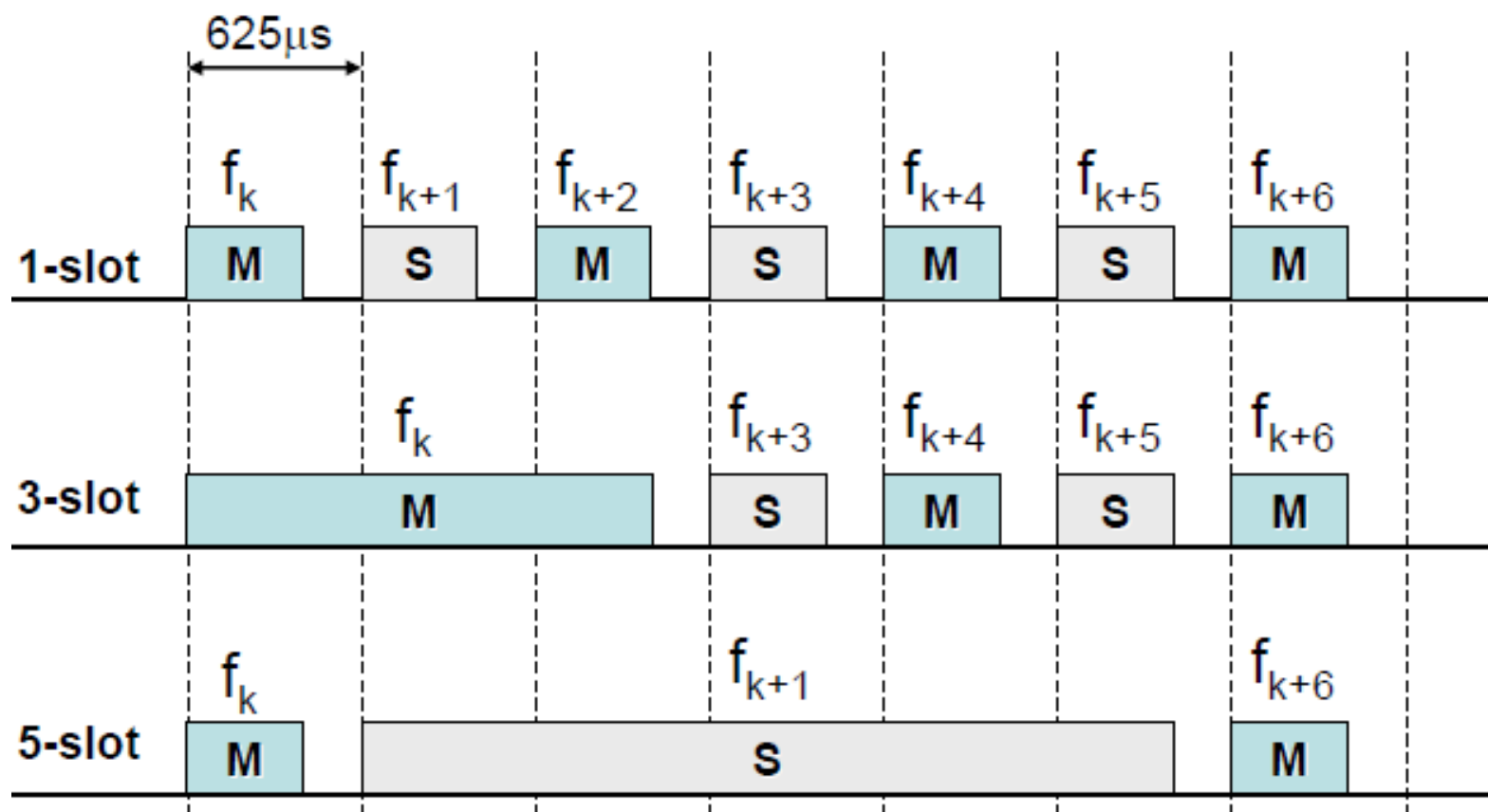


## 4.5.1 跳频（续）



○M和S交替发送（TDD模式）

○数据传输期间保持频率的跳变



## 4.5.2 物理链路（1）

### □ SCO (synchronous connection oriented) 链路

- 主要用于音频/视频传输
- M和S之间具有固定带宽的点-点连接
- M为S预留2个连续时间槽传送实时数据
- M可同时支持3个SCO
- 每个S可有2~3个SCO（64kbps）
- Full-duplex通信

#### 电话语音连接特性

- ◇ 对称
- ◇ 电路交换
- ◇ 点-点连接

SCO链路主要被用在交换需要保证数据率而不需要保证传送的限时数据

## 4.5.2 物理链路（2）



**Link: 主节点到从节点的逻辑信道**

### □ ACL (asynchronous connectionless) 链路

- 主要用于Best-effort的数据传输服务
- M和S之间的点-点/点-多点（广播）连接
- 在没有预留给SCO的时间槽传送无时间规律的分组
- 每个S节点只有1条ACL
  - ✧ 分别对应于1-slot、3-slot和5-slot分组
  - ✧ 正向最大速率：723.3Kbps(5-slot)
  - ✧ 反向最大速率：57.6Kbps
- Half-duplex通信

#### 数据应用特性

- ✧ 对称/非对称
- ✧ 分组交换
- ✧ 点-多点连接

## 4.5.2 物理链路（3）



### □ half-duplex通信(ACL)

- 一次往一个方向发送
- 不对称最大速率723.3Kbps反向为57.6Kbps
- 对称速率双向发送，每个方向可达433.9Kbps

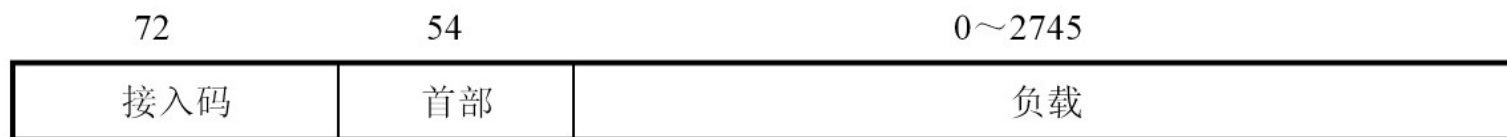
### □ full-duplex通信(SCO)

- 可同时双向发送
- 速率> 64Kbps
- 使用M预留的slot（避免同步和冲突）
- 没有为SCO链路预留的slot可用于ACL链路

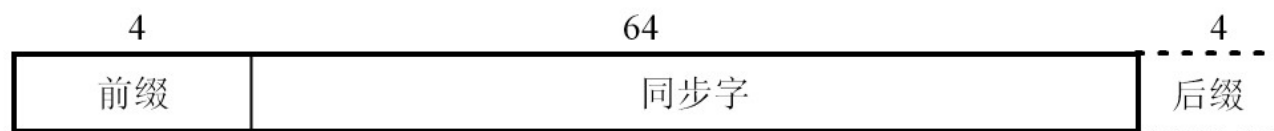
# 4.5.3 分组



位

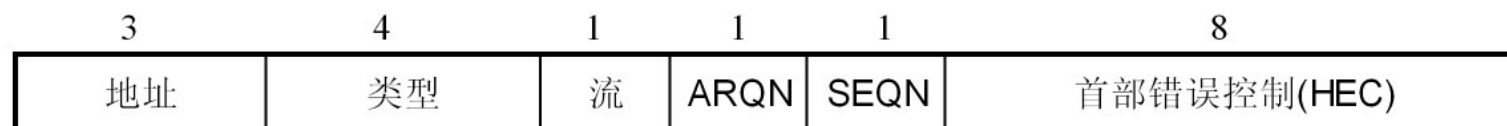


(a)包格式

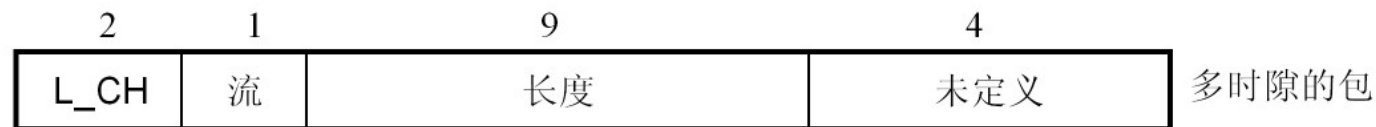
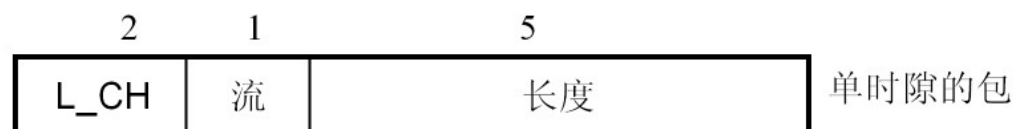


信道接入码  
设备接入码  
询问接入码

(b)接入码格式



(c)首部格式(编码之前)



(d)数据负载的首部格式

## 4.5.4 纠错



蓝牙使用三种纠错模式：

(1) 1/3比例的FEC (forward error correction, 前向纠错)。

(2) 2/3比例的FEC。

(3) ARQ (automatic repeat request, 自动重发请求)。

## 4.5.5 逻辑信道



- 链路控制(link control, LC): 在链路接口管理分组的通信流, 包含ARQ、流控制和负荷特征等。
- 链路管理(link manager, LM): 传输链路管理信息。
- 用户异步(user asynchronous, UA): 传送异步的用户数据。
- 用户等时(user isochronous, UI): 传送“等时”信息。
- 用户同步(user synchronous, US): 传送同步的用户数据。

## 4.5.6 信道控制



- 主要状态:

- (1) 待机 (standby): 默认状态。这是一个低功率状态, 只有一个本地时钟以低精度在工作。
- (2) 连接 (connection): 设备作为主站或从站连到微微网。

- 待机->连接的建立过程:

- (1) 寻呼 (page)
- (2) 寻呼扫描 (page scan)
- (3) 主站响应 (master response)
- (4) 从站响应 (slave response)
- (5) 查询 (inquiry)
- (6) 查询扫描 (inquiry scan)
- (7) 查询响应 (inquiry response)



## 4.5.6 信道控制（续）



### □ 两种管理情形

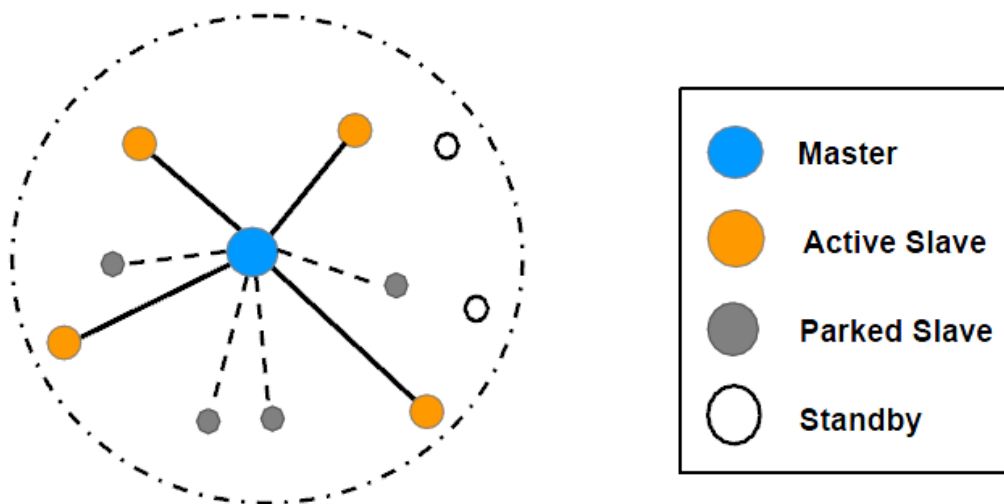
- 设备知道其他设备的参数
  - ✧ 执行paging过程
- 设备不知道其他设备的参数
  - ✧ 执行inquiring和paging过程

### □ 两个主要过程

- Page
  - ✧ 用来建立与其他节点的链路
- Inquiry
  - ✧ 用来了解时钟偏移和其他设备的地址

# 微微网的建立

- ❑ 当一个设备想建立一个piconet时
  - 79个无线电载波中有32个用来wake-up载波
  - Master依次在这32个载波上广播查询访问码（IAC）
- ❑ 一个standby设备想加入一个piconet时
  - 定期侦听IAC消息
  - 返回一个packet（设备地址和时钟信息）
- ❑ M设备根据返回的设备地址计算特殊的跳频序列
- ❑ S设备与M设备时钟同步，并启动M定义的跳频序列



## 4.5.7 蓝牙音频



- 两种编码模式：
  - (1) 脉冲编码调制 (PCM)
  - (2) 连接可变斜率增量调制 (CVSD)
- 采取哪种编码模式由两个设备的链路管理器选择

# 内容提要



- 4. 1 概述
- 4. 2 IEEE802. 15标准
- 4. 3 蓝牙技术简介
- 4. 4 蓝牙无线电规范
- 4. 5 蓝牙基带规范
- 4. 6 蓝牙链路管理器规范
- 4. 7 蓝牙逻辑链路控制和自适应协议
- 4. 8 蓝牙服务发现协议

## 4.6 蓝牙链路管理器规范

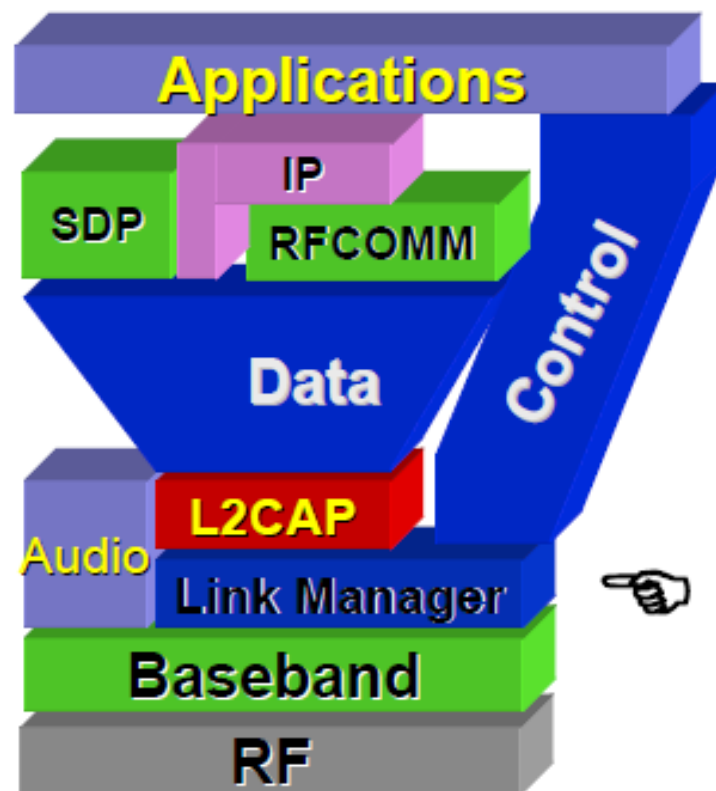


- LMP管理主站与从站间的无线电链路的各个方面。
- 协议涉及主站和从站的LMP实体间表现为LMP PDU形式的报文交换，由ALC携带。
- LMP PDU总是作为单个分组发送，带有一位标识报文类型的负载首部，和一个包含与此报文相关的附加信息的负荷实体。
- 为LMP定义的过程被分为24个功能区，其中每个都涉及一个或多个报文的交换。

## 4.6 蓝牙链路管理器规范（续）

- ❑ 能量控制：根据接收信号强度要求发送者调整发送能量
- ❑ 能力协商：交换版本号和所支持的特性
- ❑ QoS协商：轮询时间、延迟、传送能力
- ❑ 同步：修正时钟偏差或者接受特殊的同步packet
- ❑ 改变状态和传输模式：M和S角色的改变
- ❑ 链路控制：控制link活动
- ❑ 安全服务：认证、加密、密钥的分发

通过24个PDU实施基带连接的建立和管理



# Bluetooth的节能连接状态



## ❑ Sniff

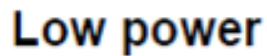
- M和S设备定期睡眠，并在早期协商的时间间隔“sniff”

## ❑ Hold

- 不释放AMA（活跃成员地址）地址
- 停止ACL传输，但可交换SCO分组

## ❑ Park

- 设备仍旧是该piconet的成员
- 释放AMA地址但获得一个PMA（parked）地址



<b>AMA: active member address(3b)</b> <b>PMA: parked member address(8b)</b>
--



# 内容提要



- 4. 1 概述
- 4. 2 IEEE802. 15标准
- 4. 3 蓝牙技术简介
- 4. 4 蓝牙无线电规范
- 4. 5 蓝牙基带规范
- 4. 6 蓝牙链路管理器规范
- 4. 7 蓝牙逻辑链路控制和自适应协议
- 4. 8 蓝牙服务发现协议

## 4.7 蓝牙逻辑链路控制和自适应协议

**逻辑链路控制和适配协议：提供了两个bluetooth设备之间具有一定QoS性质的逻辑信道。**

- ☐ 仅用于ACL
- ☐ 协议的多路复用/分用
- ☐ 接收上层分组（64KB）  
分段传输；
- ☐ 在接收端重组
- ☐ 处理服务质量

L2CAP流量控制和差错控制  
依赖于底层（基带层）

## 4.7.1 L2CAP 信道



### ❑ 无连接信道 (**CID=2**)

- 支持无连接服务。每个信道是单向的。该信道主要用于从**M**到多个**S**的广播。

### ❑ 面向连接信道 (**CID≥64**)

- 支持面向连接的服务。每个信道是双向的（全双工）。每个方向被指定了服务质量流规范。

### ❑ 信令信道 (**CID=1**)

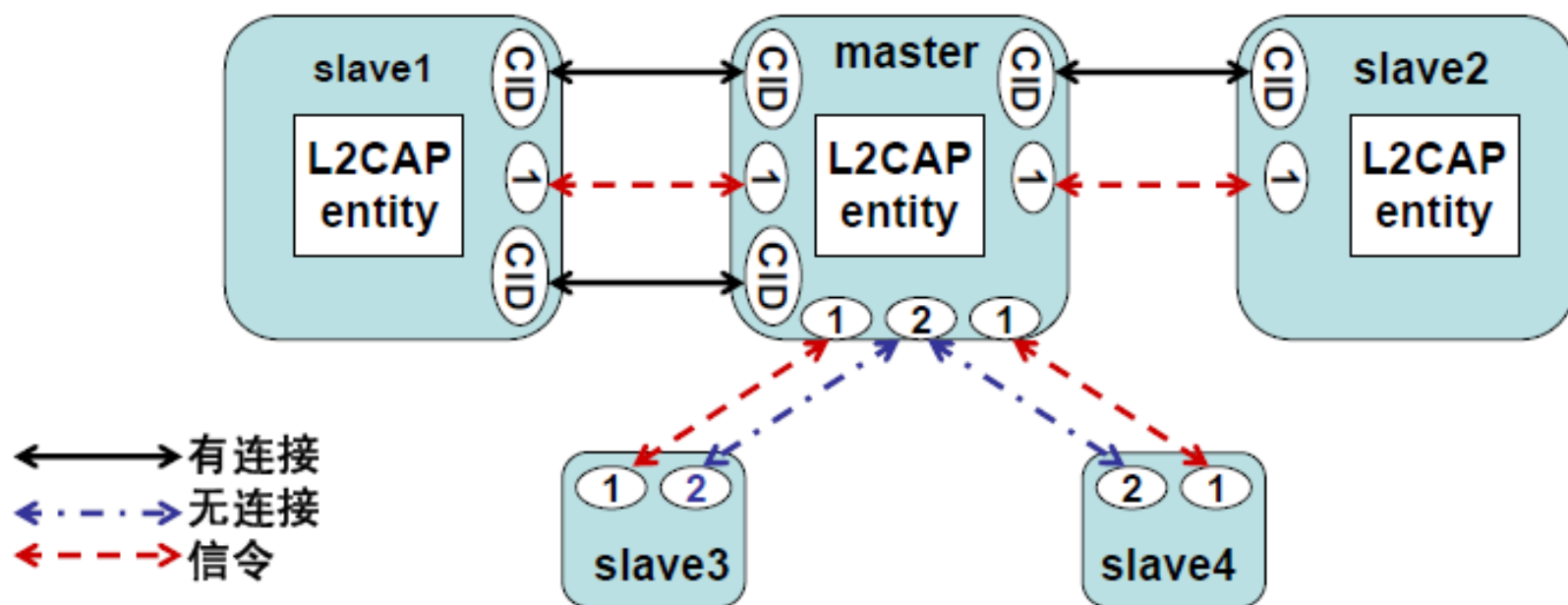
- 提供了两个**L2CAP**实体之间信令消息的交换

# 实例



CID—channel ID
1: 表示信令信道
2: 表示无连接信道

- ❑ M和S之间只能有一个无连接信道和一个信令信道
- ❑ M和S之间可有多多个面向连接信道

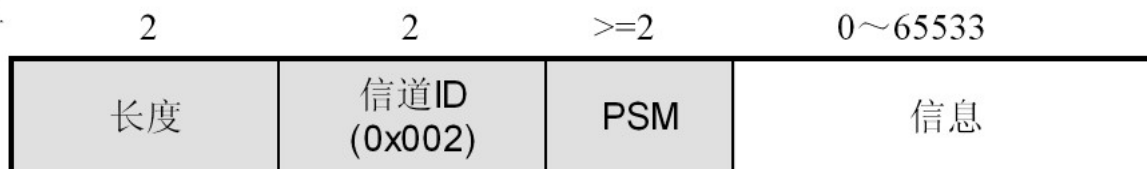


# L2CAP分组

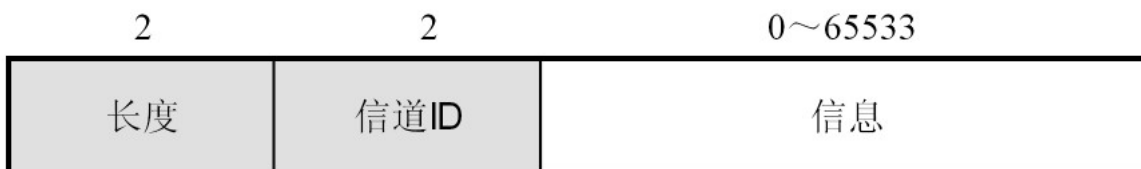


八位组

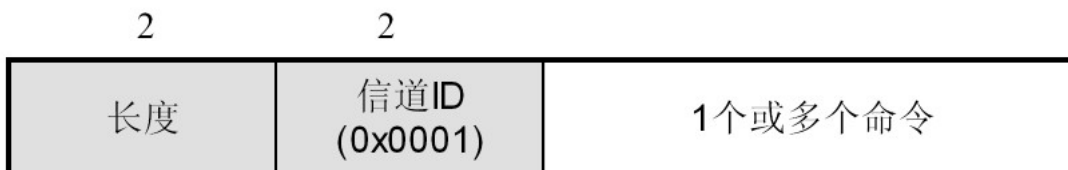
PSM: 协议/服务多路复用器, 表示高层收到分组的负载, 为SDP、RFCOM、TSC复用。



(a)无连接的PDU



(b)面向连接的PDU



(c)信令命令



匹配请求和  
回应

(d)命令格式

# 内容提要



- 4. 1 概述
- 4. 2 IEEE802. 15标准
- 4. 3 蓝牙技术简介
- 4. 4 蓝牙无线电规范
- 4. 5 蓝牙基带规范
- 4. 6 蓝牙链路管理器规范
- 4. 7 蓝牙逻辑链路控制和自适应协议
- 4. 8 蓝牙服务发现协议

## 4.8 蓝牙服务发现协议（SDP）



- 在蓝牙规范提出之前，服务发现协议已经存在。
- 在蓝牙设备的无线网络中，本地设备发现、利用远端设备所提供的服务和功能，并向其它蓝牙设备提供自身的服务，从而建立L2CAP连接，这是网络资源共享的途径，也是服务发现协议要解决的问题。
- 服务发现协议提供了服务注册的方法和访问服务发现数据库的途径。
- 服务发现可以针对特定要求的服务通过搜索、请求实现，亦可以针对所有可用服务通过浏览、请求实现。
- SIG针对蓝牙网络灵活、动态的特点，开发了蓝牙专用的服务发现协议。



The end