Check TTL : YES
Config type : normal-vrrp
Backup-forward : disabled
Create time : 2021-05-11 11:39:18
Last change time : 2021-05-26 11:38:58

1.5　无线通信网络

1.5.1　无线局域网

1. WLAN 的基本概念

无线局域网（Wireless Local Area Network，WLAN）技术分为两大阵营：IEEE 802.11 标准体系和欧洲邮电管理委员会（CEPT）制定的 HIPERLAN（High Performance Radio LAN）标准体系。IEEE 802.11 标准由面向数据通信的计算机局域网发展而来，采用无连接的网络协议，目前市场上的大部分产品都是根据这个标准开发的；HIPERLAN-2 标准则是基于连接的无线局域网，致力于面向语音的蜂窝电话。

IEEE 802.11 标准的制定始于 1987 年，当初是 802.4 L 小组将其作为令牌总线的一部分来研究的，其主要目的是用作工厂设备的通信和控制设施。1990 年，IEEE 802.11 小组正式独立出来，专门从事制定 WLAN 的物理层和 MAC 层标准的工作。1997 年颁布的 IEEE 802.11 标准运行在 2.4GHz 的 ISM（Industrial Scientific and Medical）频段，采用扩频通信技术，支持 1Mb/s 和 2Mb/s 的数据传输速率。随后又出现了几个新的标准，1998 年推出的 IEEE 802.11b 标准也是运行在 ISM 频段，采用 CCK（Complementary Code Keying）调制技术，支持 5.5Mb/s 和 11Mb/s 的数据传输速率。1999 年推出的 IEEE 802.11a 标准运行在 U-NII（Unlicensed National Information Infrastructure）频段，采用 OFDM 调制技术，支持最高达 54Mb/s 的数据传输速率。2003 年推出的 IEEE 802.11g 标准运行在 ISM 频段，与 IEEE 802.11b 兼容，数据传输速率提高到 54Mb/s。早期的 WLAN 标准主要有 4 种，如表 1-7 所示。

表 1-7　IEEE 802.11 标准

名称	发布时间	工作频段	调制技术	数据传输速率
802.11	1997 年	2.4GHz ISM 频段	DB/SK DQPSK	1Mb/s，2Mb/s
802.11b	1998 年	2.4GHz ISM 频段	CCK	5.5Mb/s，11Mb/s
802.11a	1999 年	5GHz U-NII 频段	OFDM	54Mb/s
802.11g	2003 年	2.4GHz ISM 频段	OFDM	54Mb/s

IEEE 802.11 定义了两种无线网络拓扑结构，一种是基础设施网络（Infrastructure Networking），另一种是特殊网络（Ad Hoc Networking），如图 1-23 所示。在基础设施网络中，无线终端通过接入点（Access Point，AP）访问骨干网设备。接入点如同一个网桥，它负责在 802.11 和 802.3

MAC 协议之间进行转换。一个接入点覆盖的区域叫作一个基本服务区（Basic Service Area，BSA），接入点控制的所有终端组成一个基本服务集（Basic Service Set，BSS）。把多个基本服务集互相连接就形成了分布式系统（Distributed System，DS）。DS 支持的所有服务叫作扩展服务集（Extended Service Set，ESS），它由两个以上 BSS 组成，如图 1-24 所示。

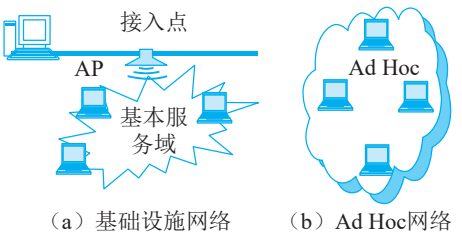


图 1-23　IEEE 802.11 定义的网络拓扑结构

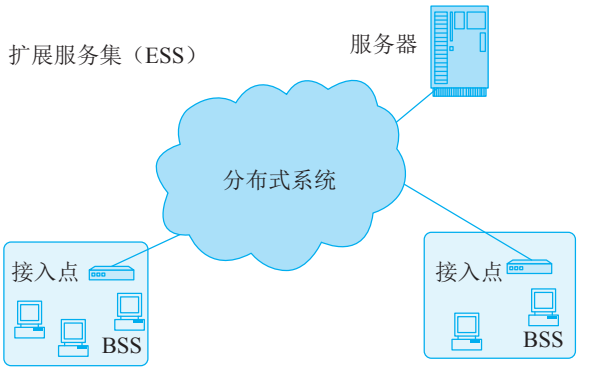


图 1-24　IEEE 802.11 定义的分布式系统

Ad Hoc 网络是一种点对点连接，不需要有线网络和接入点的支持，终端设备之间通过无线网卡可以直接通信。这种拓扑结构适合在移动情况下快速部署网络。802.11 支持单跳的 Ad Hoc 网络，当一个无线终端接入时首先寻找来自 AP 或其他终端的信标信号，如果找到了信标，则 AP 或其他终端就宣布新的终端加入了网络；如果没有检测到信标，该终端就自行宣布存在于网络之中。还有一种多跳的 Ad Hoc 网络，无线终端用接力的方法与相距很远的终端进行对等通信。

无线网可以按照使用的通信技术分类。现有的无线网主要使用三种通信技术：红外线、扩展频谱和窄带微波技术。

2. IEEE 802.11 的体系结构

802.11WLAN 的协议栈如图 1-25 所示。MAC 层分为 MAC 子层和 MAC 管理子层。MAC 子层负责访问控制和分组拆装，MAC 管理子层负责 ESS 漫游、电源管理和登记过程中的关联管理。物理层分为物理层会聚协议（Physical Layer Convergence Protocol，PLCP）子层、物理介质相关（Physical Medium Dependent，PMD）子层和 PHY 管理子层。PLCP 主要进行载波监听和物理层分组的建立，PMD 用于传输信号的调制和编码，而 PHY 管理子层负责选择物理信道和调谐。另外，IEEE 802.11 还定义了站管理功能，用于协调物理层和 MAC 层之间的交互作用。

<table>
<tr><td rowspan="2">数据链路层</td><td>LLC</td><td></td><td rowspan="4">站管理</td></tr>
<tr><td>MAC</td><td>MAC管理</td></tr>
<tr><td rowspan="2">物理层（PHY）</td><td>PLCP</td><td rowspan="2">PHY管理</td></tr>
<tr><td>PMD</td></tr>
</table>

图 1-25　WLAN 协议模型

1）物理层

IEEE 802.11 定义了三种 PLCP 帧格式来对应三种不同的 PMD 子层通信技术。

（1）FHSS（跳频技术）。对应于 FHSS 通信的 PLCP 帧格式如图 1-26 所示。SYNC 是 0 和 1 的序列，共 80 位，作为同步信号。SFD 的位模式为 0000110010111101，用作帧的起始符。PLW 代表帧长度，共 12 位，所以帧最大长度可以达到 4096 字节。PSF 是分组信令字段，用来标识不同的数据传输速率。起始数据传输速率为 1Mb/s，以 0.5 的步长递增。PSF=0000 时，代表数据传输速率为 1Mb/s，PSF 为其他数值时则在起始速率的基础上增加一定倍数的步长。例如，若 PSF=0010，则 1Mb/s+ 0.5Mb/s×2=2Mb/s；若 PSF=1111，则 1Mb/s+0.5Mb/s×15=8.5Mb/s。16 位的 CRC 是为了保护 PLCP 头部所加的，它能纠正 2 位错。MPDU 代表 MAC 协议数据单元。

SYNC(80)	SFD(16)	PLW(12)	PSF(4)	CRC(16)	MPDU（≤4096字节）

图 1-26　用于 FHSS 方式的 PLCP 帧

在 2.402 ～ 2.480GHz 的 ISM 频带中分布着 78 个 1MHz 的信道，PMD 层可以采用以下三种跳频模式之一，每种跳频模式在 26 个频点上跳跃：

（0，3，6，9，12，15，18，…，60，63，66，69，72，75）

（1，4，7，10，13，16，19，…，61，64，67，70，73，76）

（2，5，8，11，14，17，20，…，62，65，68，71，74，77）

具体采用哪一种跳频模式由 PHY 管理子层决定。三种跳频点可以提供三个 BSS 在同一小区中共存。IEEE 802.11 还规定，跳跃速率为 2.5 跳 / 秒，推荐的发送功率为 100mW。

（2）DSSS（直接序列扩频技术）。图 1-27 所示为采用 DSSS 通信时的帧格式，与前一种不同的字段解释如下：SFD 字段的位模式为 1111001110100000。Signal 字段表示数据传输速率，步长为 100kb/s，比 FHSS 精确 5 倍。例如 Signal 字段 =00001010 时，10×100kb/s=1Mb/s；Signal 字段 =00010100 时，20×100kb/s=2Mb/s。Service 字段保留未用。Length 字段指 MPDU 的长度，单位为 μs。

SYNC(128)	SFD(16)	Signal(8)	Service(8)	Length(16)	FCS(8)	MPDU

图 1-27　用于 DSSS 方式的 PLCP 帧

图 1-28 所示为 IEEE 802.11 采用的直接系列扩频信号，每个数据位被编码为 11 位的 Barker 码，图中采用的序列为 [1，1，1，−1，−1，−1，1，−1，−1，1，−1]。码片速率为 11Mc/s，占用的带宽为 26MHz，数据传输速率为 1Mb/s 和 2Mb/s 时分别采用差分二进制相移键控（DB/SK）和差分四相相移键控（DQPSK），即一个码元分别代表 1 位或 2 位数据。

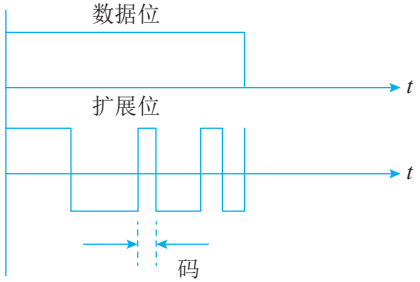


图 1-28　DSSS 的数据位和扩展位

ISM 的 2.4GHz 频段划分成 11 个互相覆盖的信道，其中心频率间隔为 5MHz，如图 1-29 所示。接入点 AP 可根据干扰信号的分布在 5 个频段中选择一个最有利的频段。推荐的发送功率为 1mW。

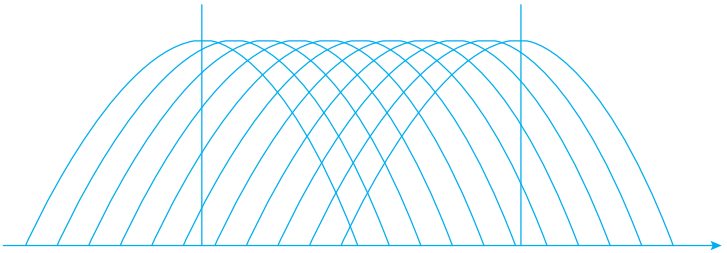


图 1-29　DSSS 的覆盖频段

（3）DFIR（漫反射红外线）。图 1-30 所示为采用 DFIR 时的 PLCP 帧格式。DFIR 的 SYNC 比 FHSS 和 DSSS 的都短，因为采用光敏二极管检测信号不需要复杂的同步过程。Data rate 字段＝ 000，表示 1Mb/s；Data rate 字段＝ 001，表示 2Mb/s。DCLA 是直流电平调节字段，通过发送 32 个时隙的脉冲序列来确定接收信号的电平。MPDU 的长度不超过 2500 字节。

SYNC（57-73）	SFD（4）	Data rate（3）	DCLA（32）	Length（16）	FCS（16）	MPDU

图 1-30　用于 DFIR 方式的 PLCP 帧

2）MAC 子层

MAC 子层的功能是提供访问控制机制，它定义了三种访问控制机制：CSMA/CA 支持竞争访问，RTS/CTS 和点协调功能支持无竞争的访问。

（1）CSMA/CA 协议。CSMA/CA 类似于 802.3 的 CSMA/CD 协议，这种访问控制机制叫作载波监听多路访问 / 冲突避免协议。在无线网中进行冲突检测是有困难的。例如，两个站由于距离过大或者中间障碍物的分隔从而检测不到冲突，但是位于它们之间的第三个站可能会检测到冲突，这就是所谓的隐蔽终端问题。采用冲突避免的办法可以解决隐蔽终端的问题。802.11 定义了一个帧间隔（Inter Frame Spacing，IFS）时间。另外，还有一个后退计数器，它的初始值是随机设置的，递减计数直到 0。基本的操作过程如下：

① 如果一个站有数据要发送并且监听到信道忙，则产生一个随机数设置自己的后退计数器并坚持监听。

② 听到信道空闲后等待 IFS 时间，然后开始计数。最先计数完的站开始发送。

③ 其他站在听到有新的站开始发送后暂停计数，在新的站发送完成后再等待一个 IFS 时间继续计数，直到计数完成开始发送。

两次 IFS 之间的间隔是各个站竞争发送的时间。这个算法对参与竞争的站是公平的，基本上是按先来先服务的顺序获得发送的机会。

（2）分布式协调功能。802.11 MAC 层定义的分布式协调功能（Distributed Coordination Function，DCF）利用了 CSMA/CA 协议，在此基础上又定义了点协调功能（Point Coordination Function，PCF），如图 1-31 所示。

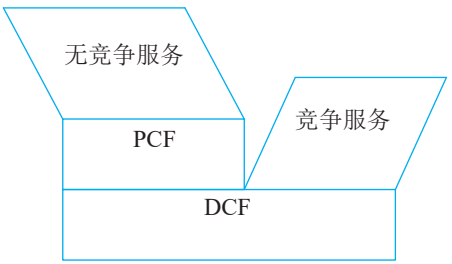


图 1-31　MAC 层功能模型

DCF 是数据传输的基本方式，作用于信道竞争期。PCF 工作于非竞争期。两者总是交替出现，先由 DCF 竞争介质使用权，然后进入非竞争期，由 PCF 控制数据传输。

为了使各种 MAC 操作互相配合，IEEE 802.11 推荐使用三种帧间隔（IFS），以便提供基于优先级的访问控制。

- DIFS（分布式协调IFS）：最长的IFS，优先级最低，用于异步帧竞争访问的时延。
- PIFS（点协调IFS）：中等长度的IFS，优先级居中，在PCF操作中使用。
- SIFS（短IFS）：最短的IFS，优先级最高，用于需要立即响应的操作。

DIFS 用在前面介绍的 CSMA/CA 协议中，只要 MAC 层有数据要发送，就监听信道是否空闲。如果信道空闲，等待 DIFS 时段后开始发送；如果信道忙，就继续监听并采用前面介绍的后退算法等待，直到可以发送为止。

IEEE 802.11 还定义了带有应答帧（ACK）的 CSMA/CA。图 1-32 所示为 AP 和终端之间使用带有应答帧的 CSMA/CA 进行通信的例子。AP 收到一个数据帧后等待 SIFS 再发送一个应答帧（ACK）。由于 SIFS 比 DIFS 小得多，所以其他终端在 AP 的应答帧传送完成后才能开始新的竞争过程。

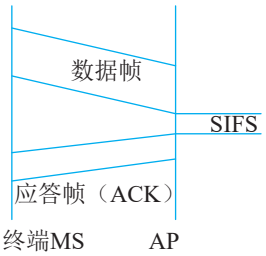


图 1-32　带有 ACK 的数据传输

SIFS 也用在 RTS/CTS 机制中，如图 1-33 所示。源终端先发送一个“请求发送”帧（RTS），其中包含源地址、目标地址和准备发送的数据帧的长度。目标终端收到 RTS 后等待一个 SIFS 时间，然后发送“允许发送”帧（CTS）。源终端收到 CTS 后再等待 SIFS 时间，就可以发送数据帧了。目标终端收到数据帧后也等待 SIFS，发回应答帧。其他终端发现 RTS/CTS 后就设置一个网络分配矢量（Network Allocation Vector，NAV）信号，该信号的存在说明信道忙，所有终端不得争用信道。

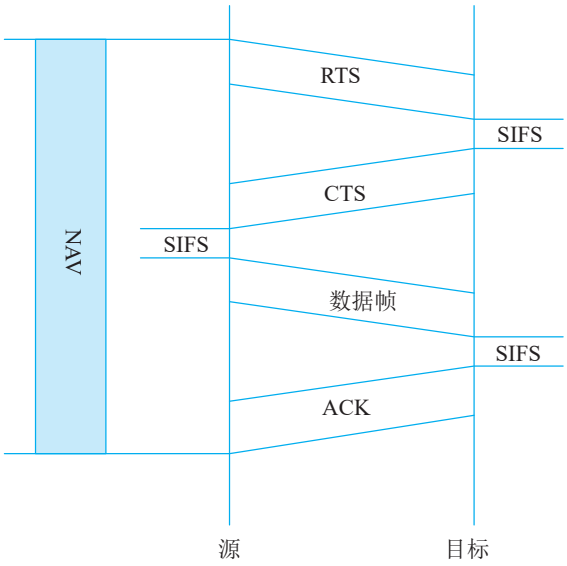


图 1-33　RTS/CTS 工作机制

（3）点协调功能。PCF 是在 DCF 之上实现的一个可选功能。所谓点协调就是由 AP 集中轮询所有终端，为其提供无竞争的服务，这种机制适用于时间敏感的操作。在轮询过程中使用 PIFS 作为帧间隔时间。由于 PIFS 比 DIFS 小，所以点协调能够优先 CSMA/CA 获得信道，并把所有的异步帧都推后传送。

在极端情况下，点协调功能可以用连续轮询的方式排除所有的异步帧。为了防止这种情况的发生，802.11 又定义了一个称为超级帧的时间间隔。在此时段的开始部分，由点协调功能向所有配置成轮询的终端发出轮询。随后在超级帧余下的时间允许异步帧竞争信道。

3）MAC 管理子层

MAC 管理子层的功能是实现登记过程、ESS 漫游、安全管理和电源管理等功能。WLAN 是开放系统，各站点共享传输介质，而且通信站具有移动性，因此，必须解决信息的同步、漫游、保密和节能问题。

（1）登记过程。

信标是一种管理帧，由 AP 定期发送，用于时间同步。信标还用来识别 AP 和网络，其中包含基站 ID、时间戳、睡眠模式和电源管理等信息。

为了得到 WLAN 提供的服务，终端在进入 WLAN 区域时，必须进行同步搜索以定位 AP，并获取相关信息。同步方式有主动扫描和被动扫描两种。

所谓主动扫描就是终端在预定的各个频道上连续扫描，发射探试请求帧，并等待各个 AP 的响应帧；收到各 AP 的响应帧后，工作站将对各个帧中的相关部分进行比较以确定最佳 AP。

终端获得同步的另一种方法是被动扫描。如果终端已在 BSS 区域，那么它可以收到各个 AP 周期性发射的信标帧，因为帧中含有同步信息，所以工作站在对各帧进行比较后，确定最佳 AP。

终端定位了 AP 并获得了同步信息后就开始了认证过程，认证过程包括 AP 对工作站身份的确认和共享密钥的认证等。

认证过程结束后就开始关联过程，关联过程包括终端和 AP 交换信息，在 DS 中建立终端和 AP 的映射关系，DS 将根据该映射关系来实现相同 BSS 及不同 BSS 间的信息传送。关联过程结束后，工作站就能够得到 BSS 提供的服务了。

（2）移动方式。

IEEE 802.11 定义了三种移动方式：无转移方式，是指终端是固定的，或者仅在 BSA 内部移动；BSS 转移，是指终端在同一个 ESS 内部的多个 BSS 之间移动；ESS 转移，是指从一个 ESS 移动到另一个 ESS。

当终端开始漫游并逐渐远离 AP 时，它对 AP 的接收信号将变坏，这时终端启动扫描功能重新定位 AP，一旦定位了新的 AP，工作站随即向新 AP 发送重新连接请求，新 AP 将该终端的重新连接请求通知分布式系统（DS），DS 随即更改该工作站与 AP 的映射关系，并通知原来的 AP 不再与该工作站关联。然后，新 AP 向该终端发射重新连接响应。至此，完成漫游过程。如果工作站没有收到重新连接响应，它将重启扫描功能，定位其他 AP，重复上述过程，直到连接上新的 AP。

（3）安全管理。

无线传输介质使得所有符合协议要求的无线系统均可在信号覆盖范围内收到传输中的数据包，为了达到和有线网络同等的安全性能，IEEE 802.11 采取了认证和加密措施。

认证程序控制 WLAN 接入的能力，这一过程被所有无线终端用来建立合法的身份标志，如果 AP 和工作站之间无法完成相互认证，那么它们就不能建立有效的连接。IEEE 802.11 协议支持多个不同的认证过程，并且允许对认证方案进行扩充。

IEEE 802.11 提供了有线等效保密（Wired Equivalent Privacy，WEP）技术，又称无线加密协议（Wireless Encryption Protocol）。WEP 包括共享密钥认证和数据加密两个过程，前者使得没有正确密钥的用户无法访问网络，后者则要求所有数据都必须用密文传输。

认证过程采用了标准的询问 / 响应方式，AP 运用共享密钥对 128 字节的随机序列进行加密后作为询问帧发给用户，用户将收到的询问帧解密后以明文形式响应；AP 将收到的明文与原始随机序列进行比较，如果两者一致，则认证通过。有关 WLAN 的安全问题，将在下面进一步论述。

（4）电源管理。

IEEE 802.11 允许空闲站处于睡眠状态，在同步时钟的控制下周期性地唤醒处于睡眠状态的空闲站，由 AP 发送的信标帧中的 TIM（业务指示表）指示是否有数据暂存于 AP，若有，则向 AP 发探询帧，并从 AP 接收数据，然后进入睡眠状态；若无，则立即进入睡眠状态。

3. 移动 Ad Hoc 网络

IEEE 802.11 标准定义的 Ad Hoc 网络是由无线移动节点组成的对等网，无须网络基础设施的支持，能够根据通信环境的变化实现动态重构，提供基于多跳无线连接的分组数据传输服务。在这种网络中，每一个节点既是主机，又是路由器，它们之间相互转发分组，形成一种自组织的 MANET（Mobile Ad Hoc Network），如图 1-34 所示。

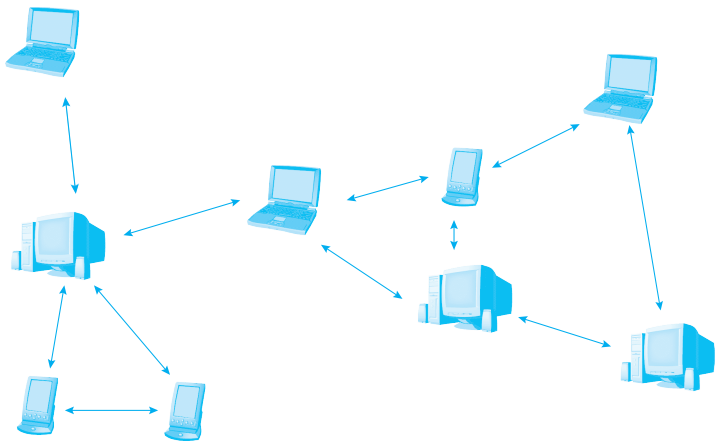


图 1-34　MANET

MANET 的部署非常便捷和灵活，因而在战场网络、传感器网络、灾难现场和车辆通信等方面有着广泛的应用。

与传统的有线网络相比，MANET 具有以下特点：

- 网络拓扑结构是动态变化的，无线终端的频繁移动可能导致节点之间的相互位置和连接关系难以维持稳定。
- 无线信道提供的带宽较小，而信号衰落和噪声干扰的影响却很大。由于各个终端信号覆盖范围的差别，或者受地形地物的影响，还可能存在单向信道。
- 无线终端携带的电源能量有限，应采用最节能的工作方式，因而要尽量减小网络通信开销，并根据通信距离的变化随时调整发射功率。
- 由于无线链路的开放性，容易招致网络窃听、欺骗、拒绝服务等恶意攻击的威胁，所以需要采取特别的安全防护措施。

目前，已经提出了各种 MANET 路由协议，用户可以根据采用的路由策略和适应的网络结构对其进行分类。根据路由策略可分为表驱动的路由协议和源路由协议；根据网络结构可分为扁平的路由协议、分层的路由协议和基于地理信息的路由协议。表驱动的路由协议和源路由协议都是扁平的路由协议。

1.5.2 无线个人网

IEEE 802.15 工作组负责制定无线个人网（Wireless Personal Area Network，WPAN）的技术规范。这是一种小范围的无线通信系统，覆盖半径仅 10m 左右，可用来代替计算机、手机、PDA、数码相机等智能设备的通信电缆，或者构成无线传感器网络和智能家庭网络等。

在人手可及的范围内，多个电子设备可以组成一个无线 Ad Hoc 网络，802.15 把这种网络叫作 Piconet，通称微微网。802.15.3 给出的 Piconet 网络模型如图 1-35 所示。这种网络的特点是各个电子设备可以独立地互相通信，其中一个设备可以作为通信控制的协调器，负责网络定时和向电子设备发放令牌，获得令牌的设备才可以发送通信请求。通信控制的协调器还具有管理 QoS 需求和调节电源功耗的功能。IEEE 802.15.3 定义了微微网的介质访问控制协议和物理层技术规范，适合于多媒体文件传输的需求。

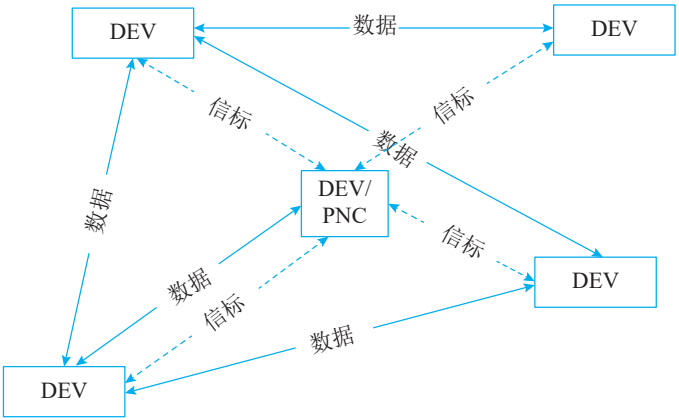


图 1-35　Piconet 网络模型

1. 蓝牙技术

1998 年 5 月，爱立信、IBM、Intel、东芝和诺基亚 5 家公司联合推出了一种近距离无线数据通信技术，其目的被确定为实现不同工业领域之间的协调工作，例如可以实现计算机、无线手机和汽车电话之间的数据传输。行业组织人员用哈拉尔德国王的外号来命名这项新技术，取其“统一”的含义，这样就诞生了“蓝牙”（Bluetooth）这一极具表现力的名字。后来成立的蓝牙技术联盟（SIG）负责技术开发和通信协议的制定，2001 年，蓝牙 1.1 版被颁布为 IEEE 802.15.1 标准。同年，加盟蓝牙 SIG 的成员公司超过 2000 家。

1）核心系统体系结构

根据 IEEE 802.15.1-2005 版描述的 MAC 和 PHY 技术规范，蓝牙核心系统的体系结构如图 1-36 所示。最下面的 Radio 层相当于 OSI 的物理层，其中的 RF 模块采用 2.4GHz 的 ISM 频段实现跳频通信（FHSS），信号速率为 1Mb/s，数据传输速率为 1Mb/s。

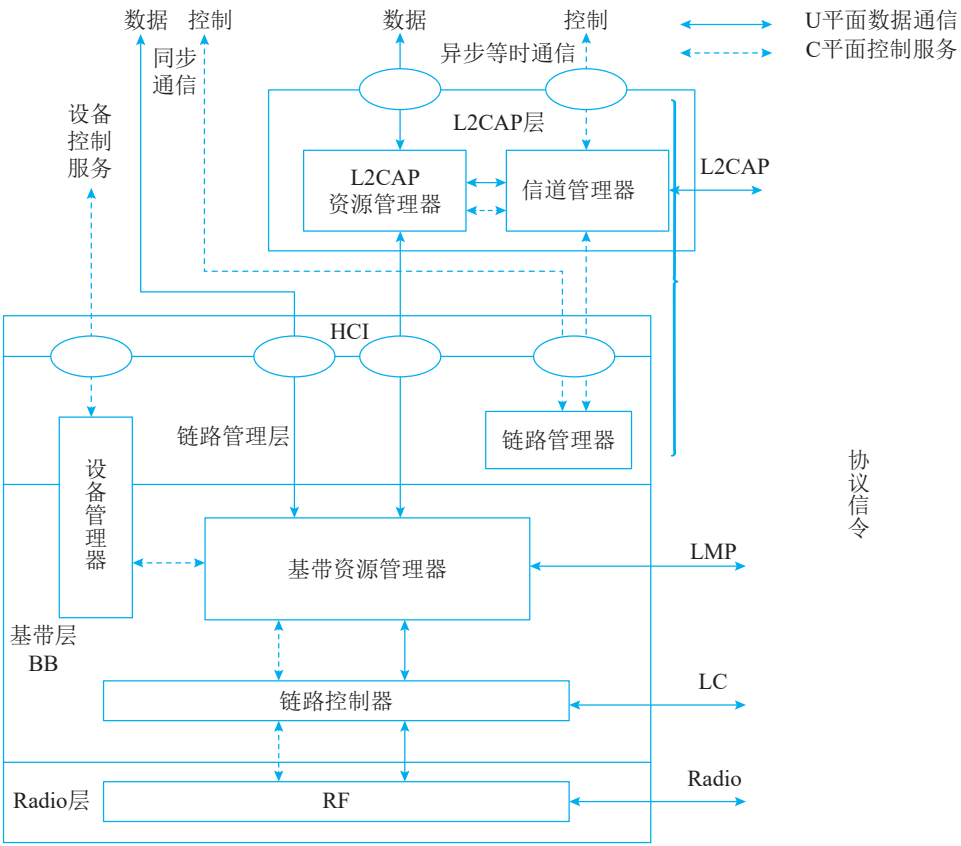


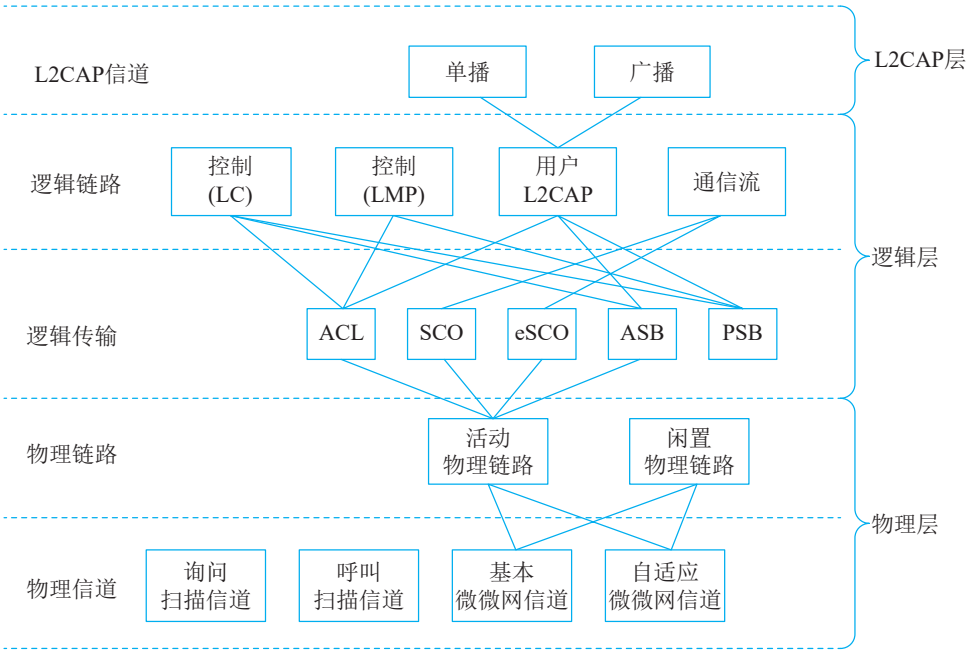
图 1-36　蓝牙核心系统的体系结构

在多个设备共享同一物理信道时，各个设备必须由一个公共时钟同步，并调整到同样的跳频模式。提供同步参照点的设备叫作主设备，其他设备则是从设备。以这种方式取得同步的一组设备构成一个微微网，这是蓝牙技术的基本组网模式。

微微网中的设备采用的具体跳频模式由设备地址字段指明的算法和主设备的时钟共同决定。基本的跳频模式包含由伪随机序列控制的 79 个频率。通过排除干扰频率的自适应技术可以改进通信效率，并实现与其他 ISM 频段设备的共存。

物理信道被划分为时槽，数据被封装成分组，每个分组占用一个时槽。如果情况允许，一系列连续的时槽可以分配给单个分组使用。在一对收发设备之间可以用时分多路（TTD）方式实现全双工通信。

物理信道之上是各种链路和信道层及其有关的协议。以物理信道为基础，向上依次形成的信道层次为物理链路、逻辑传输、逻辑链路和 L2CAP（Logical Link Control and Adaptation Protocol）信道，如图 1-37 所示。



ACL—Asynchronous Connection-Oriented Logical transport

SCO—Synchronous Connection-Oriented

eSCO—extended SCO

ASB—Active Slave Broadcast（无连接）

PSB—Parked Slave Broadcast（无连接）

图 1-37　传输体系结构实体及其层次

在物理信道的基础上，可以在一个从设备和主设备之间生成物理链路。一条物理链路可以支持多条逻辑链路，只有逻辑链路才可以进行单播同步通信、异步等时通信或者广播通信，不同的逻辑链路用于支持不同的应用需求。逻辑链路的特性由与其相关联的逻辑传输决定。所谓的逻辑传输实际上是逻辑链路传输特性的形式表现，不同的逻辑传输在流量控制、应答和重传机制、序列号编码以及调度行为等方面有所区别，用于支持不同类型的逻辑链路。异步面向连

接的逻辑传输 ACL 用来传送管理信令，而同步面向连接的逻辑传输 SCO 用于传送 64kb/s 的 PCM 话音。具有其他特性的逻辑传输用来支持各种单播的和广播的、可靠的和不可靠的、分组的和不分组的数据流。

基带层和物理层的控制协议叫作链路管理协议（Link Manager Protocol，LMP），用于控制设备的运行，并提供底层设施（PHY 和 BB）的管理服务。每个处于活动状态的设备都具有一个默认的 ACL 用于支持 LMP 信令的传送。默认的 ACL 是当设备加入微微网时随即产生的，需要时可以动态生成一条逻辑传输来传送同步数据流。

逻辑链路控制和自适应协议 L2CAP 是对应用和服务的抽象，其功能是对应用数据进行分段和重装配，并实现逻辑链路的复用。提交给 L2CAP 的应用数据可以在任何支持 L2CAP 的逻辑链路上传输。

核心系统只包含 4 个低层功能及其有关的协议。最下面的三层通常被组合成一个子系统，构成了蓝牙控制器，而上面的 L2CAP 以及更高层的服务都运行在主机中。蓝牙控制器与高层之间的接口叫作主机控制器接口（Host Controller Interface，HCI）。

设备之间的互操作通过核心系统协议实现，主要的协议有 RF（Radio Frequency）协议、链路控制协议（Link Control Protocol，LCP）、链路管理协议（LMP）和 L2CAP 协议。

核心系统通过服务访问点（SAP）提供服务，如图 1-36 中的椭圆所示。所有的服务分为三类：

- 设备控制服务：改变设备的运行方式。
- 传输控制服务：生成、修改和释放通信载体（信道和链路）。
- 数据服务：把数据提交给通信载体来传输。

主机和控制器通过 HCI 通信。通常，控制器的数据缓冲能力比主机小，因而 L2CAP 在把协议数据单元提交给控制器使其传送给对等设备时要完成简单的资源管理功能，包括对 L2CAP 服务数据单元（SDU）和协议数据单元（PDU）分段，以便适应控制器的缓冲区管理，并保证需要的服务质量（QoS）。

基带层协议提供了基本的 ARQ 功能，然而 L2CAP 还可以提供任选的差错检测和重传功能，这对于要求低误码率的应用是必要的补充。L2CAP 的任选特性还包括基于窗口的流量控制功能，用于接收设备的缓冲区管理。这些任选特性在某些应用场景中对于保障 QoS 是必需的。

2）核心功能模块

（1）信道管理器：负责生成、管理和释放用于传输应用数据流的 L2CAP 信道。信道管理器利用 L2CAP 协议与远方的对等设备交互作用，生成 L2CAP 信道，并将其端点连接到适当的实体。信道管理器还与本地的 LM 交互作用，必要时生成新的逻辑链路，并配置这些逻辑链路，以提供需要的 QoS 服务。

（2）L2CAP 资源管理器：把 L2CAP 协议数据单元分段，并按照一定的顺序提交给基带层，而且还要进行信道调度，以保证一定 QoS 的 L2CAP 信道不会被物理信道（由于资源耗尽）所拒绝。这个功能是必要的，因为体系结构模型并不保证控制器具有无限的缓冲区，也不保证

HCI 管道具有无限的带宽。L2CAP 资源管理器的另一个功能是实现通信策略控制，避免与邻居的 QoS 设置发生冲突。

（3）设备管理器：负责控制设备的一般行为。这些功能与数据传输无关，例如发现邻近的设备是否出现，以便连接到其他设备，或者控制本地设备的状态，使其可以与其他的设备建立连接。设备管理器可以向本地的基带资源管理器请求传输介质，以便实现自己的功能。设备管理器也要根据 HCI 命令控制本地设备的行为，并管理本地设备的名字以及设备中存储的链路密钥。

（4）链路管理器（LM）：负责生成、修改和释放逻辑链路及其相关的逻辑传输，并修改设备之间的物理链路参数。本地 LM 模块通过与远程设备的 LM 进行 LMP 通信来实现自己的功能。LMP 协议可以根据请求生成新的逻辑链路和逻辑传输，并对链路的传输属性进行配置，例如可以实现逻辑传输的加密、调整物理链路的发送强度以便节约能源、改变逻辑链路的 QoS 配置等。

（5）基带资源管理器：负责对物理层的访问。它有两个主要功能：其一是调度功能，即对发出访问请求的各方实体分配物理信道的访问时段；其二是与这些实体协商包含 QoS 承诺的访问合同。访问合同和调度功能涉及的因素很多，包括实现数据交换的各种正常行为，逻辑传输的特性的设置，轮询覆盖范围内的设备，建立连接，设备的可发现、可连接状态管理，以及在自动跳频模式下获取未经使用的载波等。

在某些情况下，逻辑链路调度的结果可能是改变了目前使用的物理链路，例如在由多个微微网构成的散射网（scatternet）中，使用轮询或呼叫过程扫描可用的物理信道时都可能出现这种情况。当物理信道的时槽错位时，资源管理器要把原来物理信道的时槽与新物理信道的时槽重新对准。

（6）链路控制器：负责根据数据负载和物理信道、逻辑传输和逻辑链路的参数对分组进行编码和译码。链路控制器还执行 LCP 信令，实现流量控制以及应答和重传功能。LCP 信令的解释体现了与基带分组相关的逻辑传输特性，这个功能与资源管理器的调度有关。

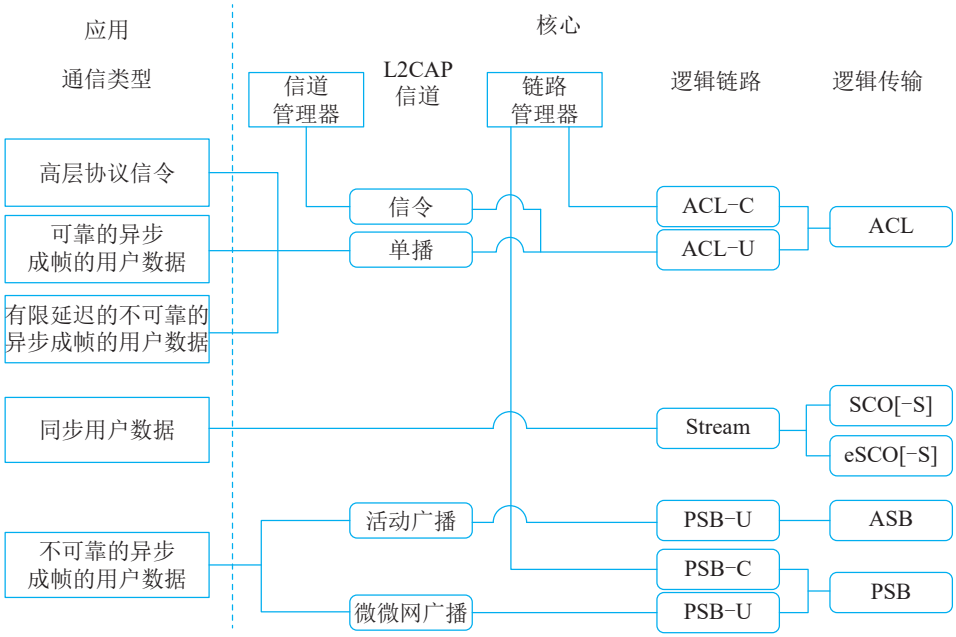
（7）RF：这个模块用于发送和接收物理信道上的数据分组。BB 与 RF 模块之间的控制通路用来控制载波定时和频率选择。RF 模块把物理信道和 BB 上的数据流转换成需要的格式。

3）*数据传输结构*

核心系统提供各种标准的传输载体，用于传送服务协议和应用数据。在图 1-38 中，圆角方框表示核心载体，而应用则画在图的左边。通信类型与核心载体的特性要进行匹配，以便实现最有效率的数据传输。

L2CAP 服务对于异步的（asynchronous）和等时的（isochronous）用户数据提供面向帧的传输。面向连接的 L2CAP 信道用于传输点对点单播数据。无连接的 L2CAP 信道用于广播数据。L2CAP 信道的 QoS 设置定义了帧传送的限制条件，例如可以说明数据是等时的，因而必须在其有限的生命期内提交；或者指示数据是可靠的，必须无差错地提交。

如果应用不要求按帧提交数据，也许是因为帧结构被包含在数据流内，或者数据本身是纯流式的，这时不应使用 L2CAP 信道，而应直接使用 BB 逻辑链路来传送。非帧的流式数据使用 SCO 逻辑传输。



字母C表示承载LMP报文的控制链路；
字母U表示承载用户数据的L2CAP链路；
字母S表示承载无格式同步或等时数据的流式链路。

图 1-38　通信载体

核心系统支持通过 SCO（SCO-S）或扩展的 SCO（eSCO-S）直接传输等时的和固定速率的应用数据。这种逻辑链路保留了物理信道的带宽，提供了由微微网时钟锁定的固定速率。数据的分组大小、传输的时间间隔等，这些参数都是在信道建立时协商好的。eSCO 链路可以更灵活地选择数据传输速率，而且通过有限的重传提供了更大的可靠性。

应用从 BB 层选择最适当的逻辑链路类型来传输它的数据流。通常，应用通过成帧的 L2CAP 单播信道向远处的对等实体传输 C 平面信息。如果应用数据是可变速率的，则只能把数据组织成帧通过 L2CAP 信道传送。

RF 信道通常是不可靠的。为了克服这个缺陷，系统提供了多种级别的可靠性措施。BB 分组头使用了纠错编码，并且配合头校验和来发现残余差错。某些 BB 分组类型对负载也进行纠错编码，还有的 BB 分组类型使用循环冗余校验码来发现错误。

在 ACL 逻辑传输中实现了 ARQ 协议，通过自动请求重发来纠正错误。对于延迟敏感的分组，不能成功发送时立即丢弃。eSCO 链路通过有限次数的重传方案来改进可靠性。L2CAP 提供了附加的差错控制功能，用于检测偶然出现的差错，这对于某些应用是有用的。

2. ZigBee 技术

ZigBee 是基于 IEEE 802.15.4 开发的一组关于组网、安全和应用软件的技术标准。802.15.4 与 ZigBee 的角色分工如同 802.11 与 Wi-Fi 的关系。802.15.4 定义了低速 WPAN 的 MAC 和 PHY 标准，而 ZigBee 联盟则对网络层协议、安全标准和应用架构（Profile）进行了标准化，并制定

了不同制造商产品之间的互操作性和一致性测试规范。

ZigBee 联盟由 Ember、Emerson、Freescale 等 12 家半导体器件和控制设备制造商发起，加盟的公司有 300 多家，其主要任务如下：

- 定义ZigBee的网络层、安全层和应用层标准。
- 提供互操作性和一致性测试规范。
- 促进ZigBee品牌的全球化市场布局。
- 管理ZigBee技术的演变。

图 1-39 所示为 ZigBee 联盟指导委员会定义的 ZigBee 技术规范（2005），描述了 ZigBee 网络的基础结构和可利用的服务。图 1-39 中下面两块是 IEEE 802.15.4 定义的 MAC 和 PHY 标准，上面是 ZigBee 联盟定义的网络层（NWK）和应用层（APL），应用对象由网络开发商定义。开发商可提供多种应用对象，以满足不同的应用需求。ZigBee 网络层提供了建立多跳网络的路由功能。应用层包含了应用支持子层（APS）和 ZigBee 设备对象（ZDO），以及各种可能的应用。ZDO 的作用是提供全面的设备管理，APS 的功能是对 ZDO 和各种应用提供服务。

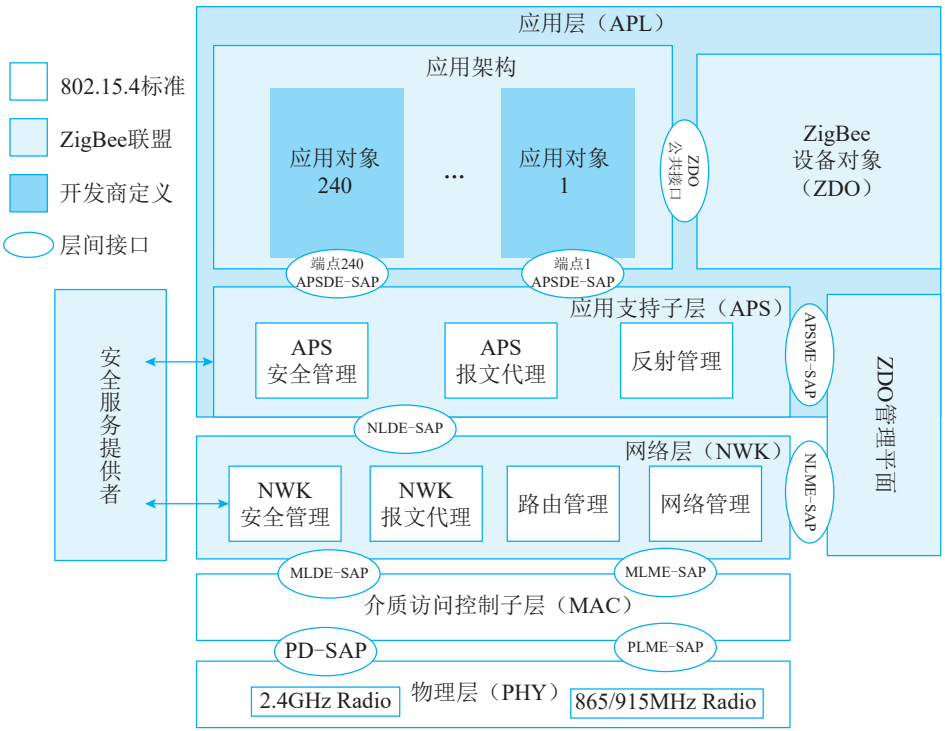


图 1-39　ZigBee 协议栈

ZigBee 的安全机制分散在 MAC、NWK 和 APS 层，分别对 MAC 帧、NWK 帧和应用数据进行安全保护。APS 子层还提供建立和维护安全关系的服务。ZigBee 设备对象（ZDO）管理安全策略和设备的安全配置。

ZigBee 的网络层和 MAC 层都使用高级加密标准 AES，以及结合了加密和认证功能的

CCM* 分组加密算法。分组加密也称块加密（Block Cipher），其操作方式是将明文按照分组算法划分为 128 位的区块，对各个区块分别进行加密，整个密文形成一个密码块链。

ZigBee 协调器管理网络的路由功能，其路由表结构如图 1-40 所示。其中的地址字段采用 16 位的短地址，3 位状态位指示的状态如下：

（1）0x0：活动。

（2）0x1：正在发现。

（3）0x2：发现失败。

（4）0x3：不活动。

（5）0x4 ～ 0x7：保留。

目标地址	状态	下一跳地址
……	…	……
……	…	……

图 1-40　路由表

ZigBee 采用的路由算法是按需分配的距离矢量协议（AODV）。当 NWK 数据实体要发送数据分组时，如果路由表中不存在有效的路由表项，则首先要进行路由发现，并对找到的各个路由计算通路费用。

假设长度为 L 的通路 P 由一系列设备 $D_1,D_2,\cdots,D_L$ 组成，如果用 $[D_i, D_{i+1}]$ 表示两个设备之间的链路，则通路费用可计算如下：

$$C\{P\}=\sum_{i=1}^{L-1}C\{[D_i,D_{i+1}]\}$$

其中，$C\{[D_i,D_{i+1}]\}$ 表示链路费用。链路 l 的费用 $C\{l\}$ 用下面的函数计算：

$$C\{l\}=\begin{cases}7,\\ \min\left(7,\ \text{round}\left(\dfrac{1}{p_l^4}\right)\right)\end{cases}$$

其中，p_l 表示在链路 l 上可进行分组提交的概率。

可见，链路的费用与链路上可提交分组的概率的 4 次方成反比，一条链路的费用的值位于区间 [0...7] 中。

1.5.3　移动通信网络

1. 蜂窝通信系统

1978 年，美国贝尔实验室开发了高级移动电话系统（Advanced Mobile Phone System，AMPS），这是第一个具有随时随地通信能力的大容量移动通信系统。AMPS 采用模拟制式的频分双工（Frequency Division Duplex，FDD）技术，用一对频率分别提供上行和下行信道。AMPS 采用蜂窝技术解决了公用移动通信系统所面临的大容量要求与频谱资源限制的矛盾。到了 1980 年中期，欧洲和日本都建立了第一代蜂窝移动电话系统。

蜂窝网络把一个地理区域划分成若干个称为蜂窝的小区（Cell）。在模拟移动电话系统中，一个话音连接要占用一个单独的频率。如果把通信网络覆盖的地区划分成一个一个的小区，则在不同小区之间就可以实现频率复用。在图 1-41 中，一个基站覆盖的小区用一个字母来代表，