华清远见 FARSIGHT 始于2004 | 嵌入式培训专家

10年口碑积累，成功培养50000多名研发工程师，铸就专业品牌形象

华清远见的企业理念是不仅要做良心教育、做专业教育，更要做受人尊敬的职业教育。

《物联网技术与实践》

作者：华清远见

专业始于专注 卓识源于远见

第 6 章 无线传输与组网技术

本章简介

第 5 章中了解到数据有线传输的几种方式和网络协议。如果只使用有线数据传输来实现现实生活的连接，那将会出现一个什么样的场景？走进办公室后，走在街道上，各种各样的线路铺展开来，一团乱糟的景象。针对这个问题，无线网络有它的特殊用途。本章就当前使用较为广泛的几种无线传输方式进行讲解。

专业始于专注 卓识源于远见

6.1 ZigBee 技术概述

6.1.1 低速无线网特点

随着通信事业的高速发展，无线网络进入了一个新的天地，其有标准作基础、功能强、容易安装、组网灵活、即插即用的网络连接、可移动性等优点，提供了不受限制的应用。网络管理人员可以快速而便捷地将它加入到现有的网络中运行。无线数据通信已逐渐成为一种重要的通信方式。

总之，无线数据通信不仅可以作为有线数据通信的补充和延伸，而且还可以与有线网络环境互为补充。在某种特殊环境下，无线通信是主要的甚至唯一的可行通信方式。从通信方式上考虑，多元化通信方式是现代化通信网络的重要特征。

下面将从传输方式、网络拓扑、网络接口 3 个方面来描述无线网的特点。

1．传输方式

传输方式涉及无线网采用的传输媒体、选择的频段及调制方式。

目前，无线网采用的传输媒体主要有两种，即无线电波与红外线。而采用无线电波作为传输媒体的无线网根据调制方式不同，又可分为扩展频谱方式和窄带调制方式。

1）扩展频谱方式

在扩展频谱方式中，数据基带信号的频谱被扩展至几倍甚至几十倍后再被搬移至射频发射出去。

这一做法虽然牺牲了频带带宽，却提高了通信系统的抗干扰能力和安全性。由于单位频带内的功率降低，对其他电子设备的干扰也减小了。

采用扩展频谱方式的无线局域网一般选择 ISM 频段，这里 ISM 分别取于 Industrial、Scientific 及 Medical 的第一个字母。许多工业、科研和医疗设备辐射的能量集中于该频段。例如，美国 ISM 频段由 902~928MHz，2.4~2.48GHz，5.725~5.850GHz 三个频段组成。如果发射功率及带宽辐射满足美国联邦通信委员会（FCC）的要求，则无须向 FCC 提出专门的申请即可使用 ISM 频段。

2）窄带调制方式

在窄带调制方式中，数据基带信号的频谱不做任何扩展即被直接搬移到射频发射出去。

与扩展频谱方式相比，窄带调制方式占用频带少、频带利用率高。采用窄带调制方式的无线局域网一般选用专用频段，需要经过国家无线电管理部门的许可方能使用。当然，也可选用 ISM 频段，这样可免去向无线电管理委员会申请，但带来的问题是，当临近的仪器设备或通信设备也在使用这一频段时，会严重影响通信质量，通信的可靠性无法得到保障。

3）红外线方式

基于红外线的传输技术最近几年有了很大发展。目前，广泛使用的家电遥控器几乎都是采用红外线传输技术。作为无线局域网的传输方式，红外线的最大优点是不受无线电干扰，且红外线的使用不受国家无线电管理委员会的限制。然而，红外线对非透明物体的透过性极差，这导致传输距离受限。

2．网络拓扑

无线局域网的拓扑结构可归结为两类：无中心或对等式（Peer to Peer）拓扑和有中心（Hub-Based）拓扑。

1）无中心拓扑

无中心拓扑的网络要求网中任意两个站点均可直接通信。

采用这种拓扑结构的网络一般是用公用广播信道，各站点都可竞争公用信道，而信道接入控制（MAC）协议大多采用载波监测多址接入（CSMA）类型的多址接入协议。

这种结构的优点是网络抗毁性好、建网容易且费用较低。但当网中用户数（站点数）过多时，信道竞争成为限制网络性能的主要原因。并且为了满足任意两个站点可直接通信，网络中站点布局受环境限制较大。因此这种拓扑结构适用于用户相对较少的工作群网络规模。

2）有中心拓扑

华清远见

在中心拓扑结构中，需要一个无线站点充当中心站，所有站点对网络的访问均由其控制。

这样，当网络业务量增大时网络吞吐性能及网络时延性能不会受太大影响。由于每个站点只需在中心站覆盖范围之内就可与其他站点通信，故网络中点站布局受环境限制较小。此外，中心站为接入有线主干网提供了一个逻辑接入点。

有中心网络拓扑结构的弱点是抗毁性差，中心点的故障容易导致整个网络瘫痪，并且中心站点的引入增加了网络成本。

在实际应用中，无线网往往与有线主干网络结合起来使用。这时，中心站点充当无线网与有线主干网的转接器。

3．网络接口

这涉及无线网中站点从哪一层接入网络系统的问题。一般来讲，网络接口可以选择在 OSI 参考模型的物理层或数据链路层。

所谓物理层接口，是指使用无线信道替代通常的有线信道，而物理层以上各层不变。这样做的最大特点是上层的网络操作系统及相应的驱动程序可不做任何修改，这种接口方式在使用时一般作为有线网的集线器和无线转发器以实现有线局域网间互连或扩大有线局域网的覆盖面积。

另一种接口方法是从数据链路层接入网络。这种接口方法并不沿用有线局域网的 MAC 协议，而采用更适合无线传输环境的 MAC 协议。在实现时，MAC 层及其以下层对上层是透明的，配置相应的驱动程序来完成域上层的接口，这样可保证现有的有线局域网操作系统或应用软件可在无线局域网上正常运转。

目前，大部分无线局域网厂商都采用数据链路层接口方法。

6.1.2 设备

ZigBee 的设备类型有：协调器（Coordinator）、路由器（Router）、终端设备（End Device）。

1．协调器（Coordinator）

协调器是一个 ZigBee 网络的第一个开始的设备或是一个 ZigBee 网络的启动或建立网络的设备。

协调器结点选择一个信道和网络标识符（PAN ID），然后开始组建一个网络。协调器设备在网络中还有其他作用，如建立安全机制、网络中的绑定和建立。

2．路由器（Router）

路由器的主要功能有：

- 作为普通设备使用。
- 作为网络中的转接结点，用于多级跳通信。
- 辅助其他结点完成通信。

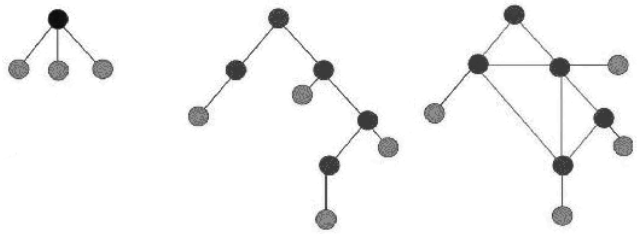
3．终端设备（End Device）

一个 ZigBee 网络的最终端，完成用户功能，如信息的收集等。

6.1.3 网络拓扑

网络中只支持两种物理设备：全功能设备（Full Function Device，FFD）和精简功能设备（Reduced Function Device，RFD）。其中 FFD 设备可提供全部的 MAC 服务，可充当任何 ZigBee 结点，不仅可以发送和接收数据，还具备路由功能，因此可以接收子结点；而精简功能设备只提供部分的 MAC 服务，只能充当终端结点，不能充当协调器和路由结点，它只负责将采集的数据信息发送给协调器和路由结点，并不具备路由功能，因此不能接收子结点，并且 RFD 之间的通信必须通过 FFD 才能完成。另外，RFD 仅需要使用较小的存储空间，这样就可以非常容易地组建一个低成本和低功耗的无线通信网络。ZigBee 标准在此基础上定义了 3 种结点：ZigBee 协调点（Coordinator）、路由结点（Router）和终端结点（End Device）。ZigBee 协议标准中定义了 3 种网络拓扑形式，分别为星形拓扑、树形拓扑和网状拓扑，如图 6-1 所示。

华清远见



星形拓扑　　树形拓扑　　网状拓扑

图 6-1　网络的 3 种拓扑形式

星形网络是 3 种拓扑结构中最简单的，因为星形网络没有用 ZigBee 协议栈，只用 802.15.4 的层就可以实现。网络由一个协调器和一系列的 FFD/RFD 构成，结点之间的数据传输都要通过协调器转发。结点之间的数据路由只有唯一的一个路径，一旦发生链路中断，那么中断的结点之间的数据通信也将中断，此外协调器很可能成为整个网络的瓶颈。

在树形网络中，FFD 结点都可以包含自己的子结点，而 RFD 只能作为 FFD 的子结点，在树形拓扑结构中，每一个结点都只能和父结点及子结点之间通信，也就是说，当从一个结点向另一个结点发送数据时，信息将沿着树的路径向上传递到最近的协调器结点然后再向下传递到目标结点。这种拓扑方式的缺点就是信息只有唯一的路由通道，信息的路由过程完成是由网络层处理，对于应用层是完全透明的。

网状网络除了允许父结点和子结点之间的通信，也允许通信范围之内具有路由能力的非父子关系的邻居结点之间进行通信，它是在树形网络的基础上实现的，与树形网络不同的是，网状网络是一种特殊的、按接力方式传输的点对点的网络结构，其路由可自动建立和维护，并且具有强大的自组织、自愈功能，网络可以通过“多级跳”的方式来通信，可以组成极为复杂的网络，具有很大的路由深度和网络结点规模。该拓扑结构的优点是减少了消息延时、增强了可靠性，缺点是需要更多的存储空间成本。

6.1.4　协议构架

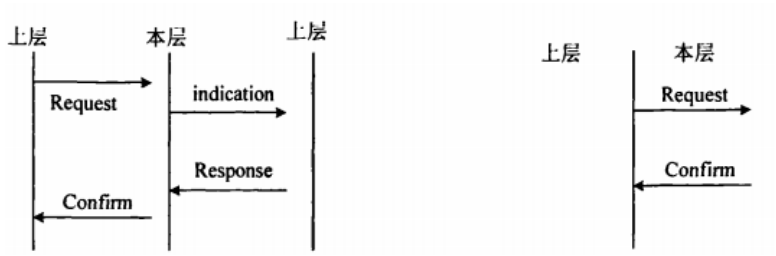
ZigBee 协议栈标准采用的是 OSI 的分层结构，其中物理层（PHY）、媒体接入层（MAC）和链路层（LLC）由 IEEE 802.15.4 工作小组制订，而网络层和应用层则由 ZigBee 联盟制订。ZigBee 协议栈的体系结构各层的分布如图 6-2 所示。

图 6-2　ZigBee 协议栈体系结构图

在 ZigBee 协议栈中，其结构包含一系列的层，每一层通过使用下层提供的服务完成自己的功能，同时向上层提供服务。层与层之间通过服务访问点 SAP（Service Access Point）连接，每一层都可以通过本层与其下层相连的调用为本层提供服务，同时通过本层与上层相连的 SAP 为上层提供服务。这些服务是设备中的实体通过发送服务原语来实现的，其中实体包括数据实体（Data-Entity）和管理实体（Menagement Entity，ME）两种。数据实体向上层提供常规的数据服务而管理实体提供向上层提供访问数据内部层的参数、配置和管理数据等机制。

6.1.5　服务原语

所谓服务原语，是代表响应服务的符号和参数的一种格式化、规范化的表示，它与服务的具体实现方式无关。原语的书写形式包含服务的实体、原语的功能及原语的类型等，如扫描原语 MLME-SCAN.request、关联确认原语 MLME-ASSOCIATE.confirm 等。另外，原语都是发送给服务实体相邻层的，层与层之间的通信原语可以分为 4 种，如图 6-3 所示。



（a）数据服务原语　　（b）管理服务原语

图 6-3　层与层的通信原语示意图

其中

Requese：请求原语，用于上层向本层请求指定的服务。

Indication：指示原语，本层发给上层用来指示本层的某一内部事件。

Response：响应原语，上层用于响应本层发出的指示原语。

Confirm：确认原语，本层用于响应上层发出的请求原语。

6.2　IEEE 802.15.4 标准

IEEE 802.15.4 网络协议栈基于开放系统互连模型（OSI），每一层都实现一部分通信功能，并向高层提供服务。

IEEE 802.15.4 标准只定义了 PHY 层和数据链路层的 MAC 子层。PHY 层由射频收发器及底层的控制模块构成。MAC 子层为高层访问物理信道提供点到点通信的服务接口。

6.2.1　物理层

物理层定义了物理无线信道和 MAC 子层之间的接口，提供物理层数据服务和物理层管理服务。物理层数据服务从无线物理信道上收发数据，物理层管理服务维护一个由物理层相关数据组成的数据库。

物理层数据服务包括以下 5 方面的功能：

- 激活和休眠射频收发器。
- 信道能量检测（Energy Detect）。
- 检测接收数据包的链路质量指示（Link Quality Indication，LQI）。
- 空闲信道评估（Clear Channel Assessment，CCA）。
- 收发数据。

信道能量检测为网络层提供信道选择依据。它主要检测目标信道中接收信号的功率强度，由于这个检测本身不进行解码操作，所以检测结果是有效信号功率和噪声信号功率之和。

链路质量指示为网络层或应用层提供接收数据帧时无线信号的强度和质量信息，与信道能量检测不同的是，它要对信号进行解码，生成的是一个信噪比指标。这个信噪比指标和物理层数据单元一道提交给上层处理。

空闲信道评估判断信道是否空闲。IEEE 802.15.4 定义了 3 种空闲信道评估模式：第一种为简单判断信道的信号能量，当信号能量低于某一门限值时就认为信道空闲；第二种是通过无线信号的特征判断，这个特征主要包括两方面，即扩频信号特征和载波频率特征；第三种模式是前两种模式的综合，同时检测信号强度和信号特征，给出信道空闲判断。

华清远见

1．物理层的载波调制

PHY 层定义了 3 个载波频段用于收发数据。在这 3 个频段上发送数据使用的速率、信号处理过程及调制方式等方面存在一些差异。3 个频段总共提供了 27 个信道（Channel）：868MHz 频段 1 个信道、915MHz 频段 10 个信道、2450MHz 频段 16 个信道。

在 868MHz 和 915MHz 这两个频段上，信号处理过程相同，只是数据传输速率不同。处理过程，首先将物理层协议数据单元（PHY Protocol Data Unit，PPDU）的二进制数据差分编码，然后再将差分编码后的每一位转换为长度为 15 的片序列（Chip Sequence），最后将 BPSK 调制到信道上。

差分编码是将数据的每一个原始比特与前一个差分编码生成的比特进行异或运算：$En=Rn \oplus E_{n-1}$，其中 En 是差分编码的结果，Rn 为要编码的原始比特，E_{n-1} 是上一次差分编码的结果。对于每个发送的数据包，R1 是第一个原始比特，计算 E1 时假定 E0=0。差分解码过程与编码过程类似：$Rn=En \oplus E_{n-1}$，对于每个接收到的数据包，E1 是第一个需要解码的比特，计算 R1 时假定 E0=0。

差分编码以后，接下来就是直接序列扩频。每一比特被转换为长度为 15 的片序列。扩频过程表 6-1 进行，扩频后的序列使用 BPSK 调制方式调制到载波上。

表 6-1　868/915MHz 比特到片序列转换表

输入比特片序列值（C1 C2…C14）
01 111101011001000000010100110111

4GHz 频段的处理过程中，首行将 PPDU 的二进制数据中每 4 位转换为一个符号（Symbol），然后将每个符号转换成长度为 32 的片序列。

在把符号转换片序列时，利用符号到片序列表进行转换，这是一个直接序列扩频的过程。扩频后，信号通过 O-QPSK 调制方式调制到载波上。

2．物理层的帧结构

物理帧第一个字段是 4 字节的前导码，收发器在接收前导码期间，会根据前导码序列的特征完成片同步和符号同步。帧起始分隔符（Start-Of-Frame Delimiter，SFD）字段长度为一字节，其值固定为 0xA7，标识一个物理帧的开始。收发器接收完前导码后只能做到数据的位同步，通过搜索 SFD 字段的值 0xA7 才能同步到字节上。帧长度（Frame Length）由一字节的低 7 位表示，其值就是物理帧负载的长度，因此物理帧负载的长度不会超过 127B。物理帧的负载长度可变，称为物理服务数据单元（PHY Service Data Unit，PSDU），一般用来承载 MAC 帧。

华清远见

6.2.2　MAC 层

IEEE 802.15.4MAC 层帧结构的设计是以用最低复杂度实现在多噪声无线信道环境下的可靠数据传输为目标的。每个 MAC 子层的帧都包含帧头、负载和帧尾 3 部分。帧头部分由帧控制信息、帧序列号和地址信息组成。MAC 子层的负载部分长度可变，负载的具体内容由帧类型决定。帧尾部分是帧头和负载数据的 16 位 CRC 校验序列。

在 MAC 子层中设备地址有两种格式：16 位（2 字节）的短地址和 64 位（8 字节）的扩展地址。16 位短地址是设备与个域网协调器关联时，由协调器分配的个域网内局部地址；64 位扩展地址则是全球唯一地址，在设备进入网络之前就分配好了。16 位短地址只能保证在个域网内部是唯一的，所以在使用 16 位短地址通信时需要结合 16 位的个域网网络标识符才有意义。两种地址类型地址信息的长度是不同的，所以 MAC 帧头的长度也是可变的。一个数据帧使用哪种地址类型由帧控制字段标识。

IEEE 802.15.4 协议共定义了 4 种类型的帧：信标帧、数据帧、确认帧和 MAC 命令帧。

1．信标帧

信标帧的负载数据单元可分为 4 部分：超帧描述字段、GTS 分配字段、待转发数据目标地址字段和信标帧负载数据：

（1）信标帧中超帧描述字段规定了该超帧的持续时间、活跃期持续时间及竞争接入期持续时间等信息。

（2）GTS 分配字段将非竞争接入期划分为若干个 GTS，并把每个 GTS 具体分配给相应设备。

（3）转发数据目标地址列出了与各域网协调器保存的数据相对应的设备地址。一个设备如果发现自己的地址出现在待转发数据目标地址字段中，则表明协调器存有属于该设备的数据，所以它就会向协调器发出请求传送数据的 MAC 命令帧。

（4）信标帧负载数据为上层协议提供数据传输接口。例如，在使用安全机制时，这个负载域将根据被通信设备设定的安全通信协议填入相应的信息。在不使用超帧结构的网络里，协调器在其他设备的请求下也会发送信标帧。此时信标帧的功能是辅助协调器向设备传输数据，整个帧只有待转发数据目标地址字段有意义。

2．数据帧

数据帧用来将上层数据传到 MAC 子层，它的负载字段包含上层需要传送的数据。数据负载传送至 MAC 子层时，被称为 MAC 服务数据单元。它的首尾被分别附加头信息和尾信息后，就构成了 MAC 帧。

MAC 帧传送至物理层后，就成为了物理帧的负载。该负载在物理层被“包装”，其首部增加了同步信息和帧长度字段。同步信息包括用于同步的前导码等。帧长度字段使用一字节的低 7 位标识 MAC 帧的长度，所以 MAC 帧的长度不会超过 127B。

3．确认帧

如果设备收到目的地址为其自身的数据帧或 MAC 命令帧，并且帧的控制信息字段的确认请求位被置 1，则设备需要回应一个确认帧。确认帧的序列号应该与被确认帧的序列号相同，负载长度为零。确认帧紧接着被确认帧发送，不需要使用 CSMA-CA 机制竞争信道。

4．命令帧

MAC 命令帧用于组建个域网、传输同步数据等。目前，定义好的命令帧主要具有 3 方面的功能：把设备关联到个域网、与协调器交换数据、分配 GTS。命令帧在格式上和其他类型的帧没有太多的区别，只是帧控制字段的帧类型位有所不同。

华清远见

6.3 ZigBee 规范

6.3.1 应用层

下面来看看典型无线传感器网络 ZigBee 的技术应用。IEEE 802.15.4 和 ZigBee 从开始就被设计用来构建包括恒温装置、安全装置和煤气读数表等设备的无线网络，这是由其主要技术优势决定的：

（1）数据传输速率低：只有 10~250Kbps，专注于低传输应用。

（2）功耗低：在低耗电待机模式下，两节 5 号干电池可使用 6 个月到 2 年，免去了充电或频繁更换电池的麻烦，这也是 BigBee 的支持者一直引以为豪的优势。

（3）成本低：ZigBee 数据传输速率低，所以大大降低了成本，且免收专利费。

（4）网络容量大：每个 ZigBee 路由器最多可支持 255 个设备。

（5）时延短：通常时延都在 15~30ms。

（6）安全：ZigBee 提供了数据完整性检查和鉴权功能，采用 AES-128 加密算法。

（7）有效范围小：有效覆盖范围为 10~75m，具体依据实际发射功率的大小和各种不同的应用模式而定，基本上能够覆盖普通的家庭或办公室环境。

（8）工作频段灵活：使用频段 2.4GHz、868MHz（欧洲）及 915MHz（美国）均为免执照频段。

与之相反，蓝牙技术基本上只是设计作为有线的替代品，通常是手机和附近的耳机或 PDA 联网用的。它可以在不充电的情况下工作几周，但无法工作几个月，更不用说几年了。

一般情况下，蓝牙设备需要入手配置和维护网络连接：它可以用来有效处理 8 个设备（1 个主设备和 7 个从设备），如果更多的话，通信速率则显著下降。而 802.11（也被称做 WiFi）也有类似的问题，虽然它是将笔记本式和台式计算机接入有线网络的很好的解决方案，但它的功耗也非常高。

ZigBee 的出发点是希望能发展一种易布建的低成本无线网络，同时其低功耗电性将使产品的电池维持 6 个月到数年，在产品发展的初期，将以工业或企业市场的感应式网络为主，提供感应辨识、灯光与安全控制等功能，再逐渐将目前市场拓展至家庭中的应用。

通常符合以下条件之一的应用，就可以考虑采用 ZigBee 技术：

（1）设备成本很低，传输的数据量很小。

（2）设备体积很小，不便放置较大的充电电池或电源模块。

（3）没有充足的电力支持，只能使用一次性电池。

（4）频繁地更换电池或者反复地充电无法做到或者很困难。

（5）需要较大范围的通信覆盖，网络中的设备非常多，但仅仅用于检测或控制。

根据 ZigBee Alliance 的特点，一般家庭可将 ZigBee 应用于以下装置：

（1）家庭自动控制，楼宇自动化。

（2）健康医疗。

（3）工业控制。

（4）无线传感器。

（5）智慧型标签。

随着 ZigBee 规范的进一步完善，许多公司都在着手开发基于 ZigBee 的产品。采用 ZigBee 技术的无线网络应用领域有家庭自动化、家庭安全、工业与环境控制与医疗护理、检测环境、监测、监察保鲜食品的运输过程及保质情况等。下面来看以下两个典型应用领域。

1．数字家庭领域

数字家庭领域可以应用于家庭的照明、温度、安全、控制等，ZigBee 模块可安装在电视、灯泡、遥控器、儿童玩具、游戏机、门禁系统、空调系统和其他家庭产品中等，通过装置 ZigBee 模块，则人们开灯就不需要走到墙壁开关处，直接通过遥控便可实现；当打开电视机时，灯光会自动减弱；当电话铃响起时或拿起话机准备打电话时，电视机会自动静音。通过 ZigBee 终端设备可以收集家庭各种信息传送到中央控制设备，或通过遥控达到远程控制的目的，提供家具生活自动化、网络化与智能化，韩国第三大移动手持设备制造商 Curitel Communications 公司已经开始研制世界上第一款 ZigBee 手机，该手机将可通过无线的方式将家中或办公室内的个人电脑、家用设备和电动开关连接起来，这种手机融入了“ZigBee”技术，能够使手机用户在远距离内操作电动开关和控制其他电子设备。

2．工业领域

通过 ZigBee 网络自动收集各种信息，并将信息回馈到系统进行数据处理与分析，以用于对工厂整体信息的掌握。如火警的感测和通知、照明系统的感测、生产机台的流程控制等，都可由 ZigBee 网络提供相关信息，以达到对工业与环境控制的目的。韩国的 NURI Telecom 在基于 Atmel 和 Ember 的平台上成功研发出基于 ZigBee 技术的自动抄表系统。该系统无须手动读取电表、天然气表及水表，从而可为公用事业节省数百万美元，此项技术正在进行前期测试。

典型无线传感器网络 ZigBee 栈体系包含一系列的层元件，包含 IEEE 802.15.4.2003 标准 MAC 层和 PHY 层，当然也包括 ZigBee 的 NWK 层。每个层的元件提供相应的服务功能。

本节描述了 ZigBee 栈的主要讲解应用层 APL（Application Layer Specification）。

APS 提供了这样的接口：在 NWK 层和 APL 层之间，从 ZDO 到供应商的应用对象的通用服务集。该服务由两个实体实现：APS 数据实体（APSDE）和 APS 管理实体（APSME）。

- APSDE 通过 APSDE 服务接入点（APSDE-SAP）。
- APSME 通过 APSME 服务接入点（APSME-SAP）。

APSDE 提供了在同一个网络中的两个或者更多的应用实体之间的数据通信。

华清远见

APSME 提供多种服务给应用对象，这些服务包含安全服务和绑定设备，并维护管理对象的数据库，也就是常说的 AIB。

典型无线传感器网络 ZigBee 中的应用框架是为驻扎在 ZigBee 设备中的应用对象提供活动的环境的。

它最多可定义 240 个相对独立的应用程序对象，对象的端点编号从 1 到 240。还有两个附加的终端结点为 APSDE-SAP 使用：端点号 0 固定于 ZDO 数据接口；另外一个端点 255 固定用于所有应用对象广播数据的数据接口功能。端点 241~254 保留（为了扩展使用）。

应用模式（也称剖面，Profiles）是一组统一的消息，消息格式和处理方法允许开发者建立一个可以共同使用的、分布式应用程序，这些应用是使用驻扎在独立设备中的应用实体。这些应用 profiles 允许应用程序发送命令、请求数据和处理命令和请求。串（也称簇，Cluster）标识符可用来区分不同的串，串标识符联系着数据从设备流出和向设备流入。在特殊的应用模式范围内，串标识符是唯一的。

ZigBee 设备对象（ZDO）描述了一个基本的功能函数，这个功能在应用对象、设备模式和 APS 之间提供了一个接口，ZDO 位于应用框架和应用支持子层之间，它满足所有在 ZigBee 协议栈中应用操作的一般需要。ZDO 还有以下作用：

- 初始化应用支持子层（APS）、网络层（NWK）、安全服务规范（SSS）。
- 从终端应用中集合配置信息来确定和执行发现、安全管理、网络管理及绑定管理。

ZDO 描述了应用框架层的应用对象的公用接口以控制设备和应用对象的网络功能。在终端结点 0，ZDO 提供了与协议栈中低一层相接的接口，如果是数据，则通过 APSDE-SAP；如果是控制信息，则通过 APSME-SAP。在 ZigBee 协议栈的应用框架中，ZDO 公用接口提供设备、发现、绑定，以及安全功能的地址管理。

设备发现是 ZigBee 设备为什么能发现其他设备的过程。以下介绍这两种形式的设备发现请求：

IEEE 地址请求和网络地址请求。IEEE 地址请求是单播到一个特殊的设备且假定网络地址已经知道。网络地址请求是广播且携带一个已知的 IEEE 地址作为负载。

服务发现是为什么一个已给设备被其他设备发现的能力的过程。服务发现通过在一个已给设备的每一个端点发送询问或通过使用一个匹配服务性质（广播或单播）。服务发现方便定义和使用各种描述来概述一个设备的能力。

服务发现信息在网络中也许被隐藏，在发现操作发生之前，设备提供的特殊服务可能不能完成。

6.3.2 网络层

典型无线传感器网络 ZigBee 堆栈是在 IEEE 802.15.4 标准基础上建立的，而 IEEE 802.15.4 仅仅定义了协议的 PHY 层和 MAC 层。ZigBee 设备应该包括 IEEE 802.15.4 的 PHY 层和 MAC 层，以及 ZigBee 堆栈层：网络层（NWK）、应用层和安全服务管理。

每个 ZigBee 设备都与一个特定模板有关，公共模板或私有模板。这些模板定义了设备的应用环境、设备类型，以及用于设备间通信的串。公共模板可以确保不同的供应商的设备在相同的应用区域中的互操作性。

设备是由模板定义的，并以应用对象（Application Objects）的形式实现。每个应用对象通过一个断点连接到 ZigBee 堆栈的余下部分，它们都是器件中可寻址的组件。

从应用角度看，通信的本质就是端点到端点的连接（例如，一个带开关组件的设备与带一个或多个灯组件的远端设备进行通信，目的就是将这些灯点亮）。端点之间的通信是通过称为串的数据结构实现的。这些串是应用对象之间共享信息所需的全部属性的容器，在特殊应用中使用的串在模板中有定义。

每个接口都能接收（用于输入）或发送（用于输出）串格式的数据。一共有两个特殊的端点，即端点 0 和端点 255。端点 0 用于整个 ZigBee 设备的配置和管理，应用程序可以通过端点 0 和 ZigBee 堆栈的其他层通信，从而实现对这些层的初始化和配置。附属在端点 0 的对象被称为 ZigBee 设备对象（ZD0）。端点 255 用于向所有端点的广播。端点 241 到 254 是保留端点。

所有端点都使用应用支持子层（APS）提供的服务。APS 通过网络层和安全拂去提供层与端点相接，并为数据传送、安全和绑定提供服务，因此能够适配不同但兼容的设备，如带灯的开关。

华清远见

APS 使用网络层（NWK）提供的服务。NWK 负责设备到设备的通信，并负责网络中设备初始化所包含的活动、消息路由和网络发现。应用层可以通过 ZigBee 设备对象（ZD0）对网络层参数进行配置和访问。

根据典型无线传感网络 ZigBee 堆栈规定的所有功能和支持，很容易推测 ZigBee 堆栈实现需要用到设备中的大量存储器资源。

ZigBee 规范定义了 3 种类型的设备，每种都有自己的功能要求。

- ZigBee 协调器是启动和配置网络的一种设备。协调器可以保持间接寻址用的绑定表格、支持关联，同时还能设计信任中心和执行其他活动。协调器负责网络正常工作及保持同网络其他设备的通信。一个 ZigBee 网络只允许有一个 ZigBee 协调器。
- 典型无线传感器网络 ZigBee 路由器是一种支持关联的设备，能够将消息转发到其他设备。ZigBee 网络或树形网络可以有多个 ZigBee 路由器。ZigBee 星形网络不支持 ZigBee 路由器。
- 典型无线传感器网络 ZigBee 终端设备可以执行它的相关功能，并使用 ZigBee 网络到达其他需要与其他通信的设备。它的存储容量要求最少。

上述 3 种设备根据功能完整性可分为全功能（FFD）和半功能（RFD）设备。其中全功能设备可作为协调器、路由器和终端设备，而半功能设备只能用于终端设备。一个全功能设备可与多个 RFD 设备或多个其他 FFD 设备通信，而一个半功能设备只能与一个 FFD 通信。

然而需要特别注意的是，网络的特定架构会戏剧性地影响设备所需的资源。NWK 支持的网络拓扑有星形、树（串）形和网格形。在这几种网络拓扑中，星形网络对资源的要求最低。

网络层（NWK）必须提供功能，以保证 IEEE 802.15.4/ZigBee 的 MAC 子层的正确操作，并为应用层提供一个合适的服务器接口。要和应用层通信，网络层的概念包括两个服务实体，提供必要的功能，如图 6-4 所示，这些服务实体是数据服务和管理服务。NWK 层数据实体（NLDE）通过其相关的 SAP、NLDE-SAP、提供了数据传输服务，而 NLME-SAP 提供了管理服务，NIME 使用 NLDE 来获得它的一些管理服务，且还维护一个管理对象的数据库，叫做网络信息库（NIB）。

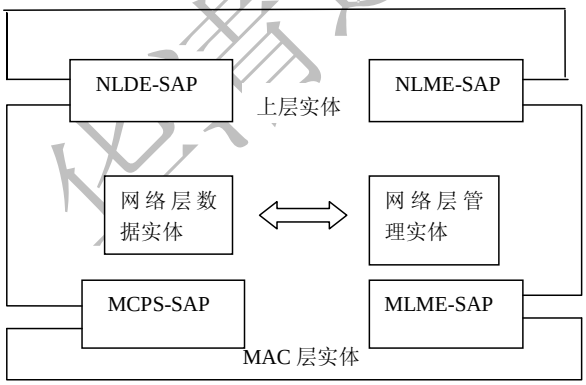


图 6-4　网络层参考模型

网络层数据实体（NLDE）应提供一个数据服务，以允许一个应用程序在两个或多个设备之间传输应用协议数据单元（APDU）。设备本身必须位于同一个网络。NLDE 将提供以下服务。

（1）生成网络级别的 PDU（NPDU）：NLDE 应该可以通过增加一个合适的协议头，从一个应用支持子层的 PDU，生成一个 NPDU。

（2）拓扑指定的路由：NLDE 应该可以传输一个 NPDU 给一个合适的设备，它是通信的最终目的地或是通信链中朝向最终目的地的下一步。

（3）安全：确保通信的真实性和机密性。

网络层管理实体（NLME）应提供一个管理服务，允许一个应用程序与协议栈相互作用，NLME 应提供以下服务：

（1）配置一个新设备：为所需的操作充分配置协议栈的功能。

（2）开始一个网络：建立一个新的网络的功能。

（3）加入、重新加入和离开一个网络：加入、重新加入和离开一个网络的功能，以及为一个 ZigBee 协调器和路由器请求一个设备离开网络功能。

（4）寻址：ZigBee 协调器和路由器给新加入网路的设备分配地址的能力。

（5）邻居发现：发现、记录和报告信息关于设备的单跳邻居的能力。

（6）路由发现：发现并记录通过网络的路径的功能，即信息可以有效地传送。

（7）接收控制：一个设备控制何时接收者是激活的，以及激活多长时间，从而使 MAC 子层同步或直接接收。

（8）路由：使用不同路由机制的能力，例如，单播、广播、多播或多对一，在网络中高效变换数据。

网络层数据实体通过网络层数据实体服务接入点（NLDE-SAP）提供数据服务，网络管理层实体通过网络层管理实体服务接入点（NLME-SAP）提供网络管理服务。网络层管理实体利用网络层数据实体完成一些网络的管理工作，并且网络层管理实体完成对网络信息库（NIB）的维护和管理。

网络层通过 MCPS-SAP 和 MLME-SAP 接口为 MAC 层提供接口。通过 NLDE-SAP 与 NLME-SAP 接口为应用层提供接口服务。

1．ZigBee 网络层帧结构

通过 6.3.1 节的介绍，了解了网络层的概况。现在来看看网络协议数据单元（NPDU）即网络层帧结构，如表 6-1 所示。

表 6-1　网络帧层结构

字节：	2	2	1	1		0/8	0/1	变长	变长
帧控制	目的地址	源地址	广播半径域	广播序列号	IEEE 目的地址	IEEE 源地址	多点传送控制	源路由帧	帧的有效载荷
网络层帧报头									网络帧的有效载荷

网络协议数据单元（NPDU）结构（帧结构）基本组成部分：网络层帧报头，包含帧控制、地址和序列信息等；网络层帧的可变长有效载荷，包含帧类型所指定的信息。

表 6-1 中表示的是网络层的通用帧结构，不是所有的帧都包含地址和序列域，但网络层的帧报头域还是按照固定的顺序出现。但是，仅仅只有多播标志值 1 时才存在多播（多点传送）控制域。

在 Zigbee 网络协议中，定义了两种类型的网络层帧，分别是数据帧和网络层命令帧。

下面分别简单讲解通用帧内各子域：

1）帧控制域

帧控制域格式如表 6-2 所示，为 16bit（位或比特），可以看到帧控制域包括帧类型、协议版本、发现路由、源路由、广播、地址、安全和保留位。

表 6-2　帧控制域格式

比特 0~1	2~5	6~7	8	9	10	11	12	13~15
帧类型	协议版本	发现路由	广播标记	安全	源路由	IEEE 目的地址	IEEE 源地址	保留

2）目的地址

在网络层帧中必须有目的地址域，其长度是 2 字节，如果帧控制域的多播标志子域值是 0，那么目的地址域是 16 位的目的设备网络地址或广播地址。如果多播标志子域值是 1，则目的地址域是 16 位目的多播组的 Group ID。值得注意的是，设备的网络地址与 IEEE802.15.4-2003 协议中的 MAC 层 16 位短地址相同。

3）源地址

在网络层帧中必须有源地址域，其长度是 2 字节，其值是源设备的网络地址。值得注意的是，设备的网络地址与 IEEE 802.15.4-2003 协议中的 MAC 层 16 位短地址相同。

4）广播半径域

广播域仅当目的地址为广播地址（0xFFFF）时，广播半径和广播序号存在。广播半径的长度为 1 字节，每个设备接收到一次该帧，则广播半径减 1，广播半径限定了传输半径。

5）广播序列号域

在每个帧中都包含序列号域，其长度是 1 字节，每发送一个新的帧序列号值加 1，帧的源地址和序列号子域是一对，在限定了序列号 1 字节的长度内是唯一的标识符。

6）IEEE 目的地址

如果存在 IEEE 目的地址域，则包含在网络层地址头中的目的地址域的 16 位网络地址相对应的 64 位 IEEE 地址，如果该 16 位网络地址是广播或多播地址，那么 IEEE 目的地址不存在。

7）IEEE 源地址

如果存在 IEEE 源地址域，则包含在网络层地址头中的源地址域的 16 位网络地址相对应的 64 位 IEEE 地址。

8）多点传送控制

多播控制域是 1 字节长度且只有在多播标志子域是 1 时存在。它分成 3 个子域：多播模式（第 0,1 位共 2 位）、非成员半径（第 2~4 位，共 3 位）、最大非成员半径（第 5~7 位，共 3 位）。

多播模式（子域）表明使用成员或非成员模式传输该帧。成员模式在目的组成员设备中使用传送多播帧。非成员模式是从不是多播组成员设备到是多播组成员设备换算多播帧。

当不是目的组成员设备转播时，非成员半径域表明成员模式多播范围，接收设备是目的组成员将设置该子域值为最大非成员半径（MaxNonmemberRadius）域的值，如果 MaxNonmemberRadius field 的值是 0，接收设备不是目的组成员时将丢弃该帧，且如果 MaxNonmemberRadius 域的值是在 0x01~0x06，那么将耗尽此域，如果 MaxNonmemberRadius 域值是 0x07，表明无限的范围且不能被耗尽。

9）源路由帧

如果帧控制域的源路由子域的值是 1，则存在源路由子帧域，它分成一个子域：应答数据（1 字节）、应答索引（1 字节）和应答列表（可变长）。

应答计数器子域表明包含在源路由子帧转发列表里的应答的数值。

应答索引子域表明传输的数据包的应答列表子域的下一转发的索引。这个域被数据包的发送设备初始化为 0，且每转发一次就加 1。

应答列表子域是结点的 2 字节短地址的列表，这个域用来进行源路由数据包向目的域转发。地址是最无意义字节格式且在源路由中有顺序地出现。

10）帧有效载荷

帧有效载荷的长度是可变的，包含了各种帧类型的具体信息。

① 数据帧。数据帧与网络层的通用帧结构相同，帧的有效载荷为网络层上层要求网络层传送的数据。在帧控制域中，帧类型子域应为表示数据帧的值。根据数据帧的用途，对其他所有的子域进行设置。

数据帧包括网络层报头和数据有效载荷域。

数据帧的网络层报头域由控制域和根据需要适当组合而得到的路由域组成。

数据帧的数据有效载荷域包含字节的序列，该序列为网络层上层要求网络层传送的数据。

② 网络层命令帧。网络层命令帧结构如表 6-3 所示。网络层帧结构与通用网络层帧结构基本相同。

表 6-3　网络层命令帧

字节	2	1	可变
帧控制	路由域	网络层命令标识符	网络层命令载荷
网络层帧报头		网络层载荷	

网络层命令帧中的网络层帧报头域由帧控制域和根据需要适当组合而得到的路由域组成。在帧控制域中，帧类型子域应表示网络层命令帧的值。根据网络层命令帧的用途，对其他所有的子域进行设置。

根据帧控制域中的设置，路由为地址域和广播域经过适当组合得到的。

华清远见

网络层命令标识符域表明所使用的网络层命令，其值如表 6-4 所示，网络层命令载荷包含网络层本身。

表 6-4 网络层命令帧标识符

命令帧标识符	命令名称	命令帧标识符	命令名称
0x01	路由请求	0x07	重新加入响应
0x02	路由应答	0x08	连接状态
0x03	路由错误	0x09	网络报告
0x04	断开	0x0A	网络更新
0x05	路由记录	0x0B~0xFF	
0x06	重新连接请求		保留

2．网络层功能介绍

在介绍网络层相关管理服务前，先来看看在 ZigBee 中原语的概念。

ZigBee 设备在工作时，各种不同的任务在不同的层次上进行，通过层的服务，完成所要执行的任务。每一层的任务主要完成两种功能：根据它的下层服务要求，为上层提供相应的服务；各项服务通过服务原语来实现。每个事件由服务原语组成，它将在一个用户的某一层，通过该层的服务接入点（SAP）与建立对等连接的用户的相同层之间传送。服务原语通过提供一种特定的服务来传输必需的信息。这些服务原语是一个抽象的概念，它们仅仅指出提供的服务内容，而没有指出由谁来提供这些服务。它的定义与其他接口的实现无关。

由代表其特点的服务原语和参数的描述来指定一种服务。一种服务可能有一个或多个相关的原语，这些原语构成了与具体服务相关的执行命令。每种服务原语提供服务时，根据具体的服务类型，可能不带有传输信息，也可能带有多个传输必需的信息参数。

原语通常分为如下 4 种类型（如下原语环境设置为一个具有 I 个用户的网络中，两个对等用户及其与 J 层或子层对等协议实体建立连接）。

（1）Request：请求原语是从 I1 用户发送到它的第 J 层，请求服务开始。

（2）Indication：指示原语是从 I1 用户的第 J 层向 I2 用户发送，指出对于 I2 用户有重要意义的内部 J 层的事件，该事件可能与一个遥远的服务请求有关或者可能是由一个 J 层的内部事件引起。

（3）Response：响应原语是从 I2 用户向它的第 J 层发送，用来表示用户执行上一条原语调用过程的响应。

（4）Confirm：确认原因是由第 J 层向 I1 用户发送，用来传递一个或多个前面服务请求原语的执行结果。

网络层确认原语通常都包括一个参数，这个参数记录回答请求原语的状态。网络层状态参数值如表 6-5 所示。

表 6-5 网络层状态参数值

名　称	值	描　述
SUCCESS	0x00	请求执行成功
INVALID_PARAMETER	0xc1	从高层发出的原语无效或者超出范围
INVALID_REQUEST	0xc2	考虑到网络层目前的状态，高层发送的请求原语无效或者不能执行
NOT_PERMITTED	0xc3	NLME-JOIN.request 原语不能接受
STARTUP_FAILURE	0xc4	NLME-NETWORK-FORMATION.request 原语启动网络失败
ALREADY_PRESENT	0xc5	产生 NLMEDIRECT-JOIN.request 原语的设备的邻居表中已经存在有地址设备提供的 NLMEDIRECT-JOIN.request 原语
SYNC_FAILURE	0xc6	用来表明在 MAC 层 NLME-SYNC.request 原语失败

华清远见

NEIGHBOR_TABLE_FULL	0xc7	LME-JOIN-DIRECTLY.request 失败，因为，没有更多的空间
UNKNOWN_DEVICE	0xc8	NLME-LEAVE.request 原语失败，因为产生原语的设备地址的邻居表中的参数列表中
UNSUPPORTED_ATTRIBUTE	0xc9	NLME-GET.request or NLME-SET.request 原语产生带有未知的属性标识符
NO_NETWORKS	0xca	没有检测到网络环境产生 NLMR-JOIN.request 原语
LEAVE_UNCONFIRMED	0xcb	设备确认从网络出发失败
MAX_FRM_CNTR	0xcc	因为帧计数器达到最大值，所以输出帧安全处理失败
NO-KEY	0xcd	输出帧尝试安全处理且失败，因为对于处理没有有效的钥匙
BAD_CCM_OUTPUT	0xce	输出帧尝试安全处理且失败，因为安全设计产生一个错误的输出
NO_ROUTING CAPACITY	0xcf	由于缺少路由表或者发现路由表能力，尝试发现路由失败
ROUTE_DISCOVERY_FAILED	0xd0	尝试发现路由失败，由于缺少路由能力
ROUTE_ERROR	0xd1	由于发送设备的路由失败，NLDE-DATA.request 原语失败
BT_TABLE_FULL	0xd2	由于没有足够的空间在 BTT，尝试发送一个广播帧或成员模式多点传送失败
FRAME_NOT_BUFFERD	0xd3	一个非成员多点传送帧丢弃未决路由发现

网络层管理实体服务接入点为其上层和网络层管理实体之传送管理命令提供接口，NLME 所支持的 NLME-SAP 接口原语，这些原语包括网络发现、网络形成、允许设备连接、路由器初始化、设备同网络的连接等。

所有的 ZigBee 设备必须提供以下功能：

（1）加入一个网络。

（2）离开一个网络。

（3）重新加入一个网络。

ZigBee 协调器和路由器必须提供以下另外的功能。

（4）允许设备使用以下方法加入网络：

① 来自于 MAC 的连接指示。

② 来自于应用层的明确的加入请求。

③ 重新加入请求。

（5）允许设备使用以下方法离开网络：

① 网络离开命令帧。

② 来自于应用程序的明确的离开请求。

（6）参与分配逻辑网络地址。

（7）维护一个相邻设备的列表。

ZigBee 协调器必须提供建立一个新网络的功能，ZigBee 路由器和终端设备在一个网络中应提供便携支持。

6.3.3 安全服务

ZigBee 技术在安全方面具体表现为如下特点：

1．提供了刷新功能

刷新检查能够阻止转发的攻击；ZigBee 设备保持输入和输出刷新计数器，当有一个新的密钥建立时，计数器就重新设置。每秒通信一次的设备，它的计数器值不能超过 136 年。

华清远见

2．提供了数据包完整性检查功能

在传输过程中，这种功能阻止攻击者对数据进行修改。完整性选项有 0、32、64 或 128 位，在数据保护和数据开销之间进行折中选择。

3．提供了认证功能

认证保证了数据的发起源，阻止攻击者修改一个设备并模仿另一个设备；认证可应用在网络层和设备层，网络层认证是通过使用一个公共的网络密钥，这阻止了外部的攻击，内存开销很少。设备层认证是在两个设备之间使用唯一的连接密钥，能阻止内部和外部的攻击，但需要很高的内存开销。

4．提供了加密功能

阻止窃听者侦听数据。它使用 128 位 AES 加密算法，这种加密保护可应用在网络层和设备层上。网络层加密是通过使用一个公共的网络密钥，这阻止了外部的攻击，内存开销很少。设备层加密是在两个设备之间使用唯一的连接密钥，能阻止内部和外部的攻击，但需要很高的内存开销。

6.4 WiFi 介绍

6.4.1 WiFi 简述

WiFi 全称 Wireless Fidelity，又称 802.11b 标准，它的最大优点是传输速率较高，可以达到 11Mbps，另外，它的有效距离也很长，同时与已有的各种 802.11 DSSS 设备兼容。目前，非常流行的笔记本电脑技术——迅驰技术就是基于该标准的。

IEEE（美国电子和电器工程师协会）802.11b 无线网络规范是 IEEE 802.11 网络规范的变种，最高带宽为 11 Mbps，在信号较弱或有干扰的情况下，带宽可调整为 5.5Mbps、2Mbps 和 1Mbps，带宽的自动调整，有效地保障了网络的稳定性和可靠性。其主要特点为：速度快、可靠性高，在开放性区域，通信距离可达 305m，在封闭性区域，通信距离为 76~122m，方便与现有的有线以太网络整合，组网的成本更低。

WiFi 无线保真技术与蓝牙技术一样，同属于在办公室和家庭中使用的短距离无线技术。该技术使用的是 2.4GHz 附近的频段，该频段目前尚属没用许可的无线频段。目前其可使用的标准有两个，分别是 IEEE 802.11a 和 IEEE 802.11b。由于该技术具有自身的优点，因此受到厂商的青睐。

6.4.2 WiFi 突出优势

无线电波的覆盖范围广，基于蓝牙技术的电波覆盖范围非常小，半径大约只有 50 英尺（约合 15m），而 WiFi 的半径则可达 300 英尺（约合 100m），办公室自不用说，就是在整栋大楼中也可使用。最近，由 Vivato 公司推出了一款新型交换机，据悉，该款产品能够把目前 WiFi 无线网络 300 英尺（接近 100m）的通信距离扩大到 4 英里（约 6.5km）。

虽然由 WiFi 技术传输的无线通信质量不是很好，且数据安全性能比蓝牙差一些，传输质量也有待改进，但传输速度非常快，可以达到 11Mbps，符合个人和社会信息化的需求。

厂商进入该领域的门槛比较低。厂商只要在机场、车站、咖啡店、图书馆等人员较密集的地方设置“热点”，并通过高速线路将 Internet 接入上述场所。这样，由“热点”发射出的电波可以达到距接入点半径数十米至百米的地方，用户只要将支持无线 LAN 的笔记本电脑或 PDA 拿到该区域内，即可高速接入 Internet。也就是说，厂商不用耗费资金进行网络布线接入，从而节省了大量的成本。

6.4.3 WiFi 组建方法

一般架设无线网络的基本配备就是无线网卡及一台 AP，如此便能以无线的模式，配合既有的有线架构来分享网络资源，架设费用和复杂程度远远低于传统的有线网络。如果只是几台计算机的对等网，也可不要 AP，只需要每台计算机配备无线网卡。AP 是 AccessPoint 的简称，一般翻译为“无线访问结点”或

华清远见

“桥接器”。它主要在媒体存取控制层 MAC 中扮演无线工作站及有线局域网络的桥梁。有了 AP，就像有线网络的 Hub 一样，无线工作站可以快速且轻易地与网络相连。特别是对于宽带的使用，WiFi 更显优势，有线宽带网络（ADSL、小区 LAN 等）到户后，连接到一个 AP，然后在计算机中安装一块无线网卡即可。普通的家庭有一个 AP 已经足够，甚至用户的邻居得到授权后，也无须增加端口，就能以共享的方式上网。

6.4.4 WiFi 联结点

1．站点（Station）

站点是网络最基本的组成部分。基本服务单元（Basic Service Set，BSS）。网络最基本的服务单元。最简单的服务单元可以只由两个站点组成。站点可以动态地联结（associate）到基本服务单元中。

2．分配系统（Distribution System，DS）

分配系统用于连接不同的基本服务单元。分配系统使用的媒介（Medium）逻辑上和基本服务单元使用的媒介是截然不同的，尽管它们物理上可能会是同一个媒介，如同一个无线频段。

3．接入点（Access Point，AP）

接入点既有普通站点的身份，又有接入到分配系统的功能。

4．扩展服务单元（Extended Service Set，ESS）

由分配系统和基本服务单元组合而成。这种组合是逻辑上，并非物理上的。不同的基本服务单元有可能在地理位置上相去甚远。分配系统也可以使用各种各样的技术。

5．关口（Portal）

关口也是一个逻辑成分，用于将无线局域网和有线局域网或其他网络联系起来。

这里有 3 种媒介：站点使用的无线的媒介、分配系统使用的媒介，以及和无线局域网集成一起的其他局域网使用的媒介。物理上它们可能互相重叠。

IEEE 802.11 只负责在站点使用的无线的媒介上的寻址（Addressing）。分配系统和其他局域网的寻址不属于无线局域网的范围。IEEE 802.11 没有具体定义分配系统，只是定义了分配系统应该提供的服务（Service）。整个无线局域网定义了 8 种服务。

4 种服务属于分配系统的任务，分别为：联接（Association），结束联接（Diassociation），分配（Distribution），集成（Integration），再联接（Reassociation）。

4 种服务属于站点的任务，分别为：鉴权（Authentication），结束鉴权（Deauthentication），隐私（Privacy）和 MAC 数据传输（MSDU delivery）。

6.4.5 WiFi 未来发展

近两年来，无线 AP 的数量迅猛增长，无线网络的方便与高效使其能够得到迅速普及。除了在一些公共地方有 AP 之外，国外已经以无线标准来建设城域网，因此，WiFi 的无线地位将会日益牢固。

WiFi 是目前无线接入的主流标准，但是，WiFi 会走多远呢？在 Intel 的强力支持下，WiFi 已经有了接班人。它就是全面兼容现有 WiFi 的 WiMAX，对于 WiFi 的 802.11x 标准，WiMAX 就是 802.16x。WiMAX 具有更远的传输距离、更宽的频段选择以及更高的接入速度等，预计会在未来几年间成为无线网络的一个主流标准，Intel 计划采用该标准来建设无线广域网络。这相比于现在的无线局域网或城域网，是质的变革，而且现有设备仍能得到支持，保护人们的每一分钱的投资。

总而言之，家庭和小型办公网络用户对移动连接的需求是无线局域网市场增长的动力，虽然到目前为止，美国、日本等发达国家仍然是 WiFi 用户最多的地区，但随着电子商务和移动办公的进一步普及，廉价的 WiFi 必将成为那些随时需要进行网络连接用户的必然之选。

华清远见

6.5 Bluetooth 介绍

6.5.1 蓝牙的起源

蓝牙的创始人是瑞典的爱立信公司，爱立信早在 1994 年就已进行研发。1997 年，爱立信与其他设备生产商联系，并激发了他们对该项技术的浓厚兴趣。1998 年 2 月，5 家世界著名的计算机和通信公司：爱立信（Ericsson）、国际商用机器（IBM）、英特尔（Intel）、诺基亚（Nokia）和东芝（Toshia），他们共同的目标是建立一个全球性的小范围无线通信技术，即现在的蓝牙。

蓝牙的名称来源于 10 世纪丹麦国王 Harald Blstsnd——英译为 Harold Bluetooth（因为他十分喜欢吃蓝梅，所以牙齿每天都带着蓝色）。在行业协会筹备阶段，需要一个极具表现力的名字来命名这项高新技术。行业组织人员，在经过一夜关于欧洲历史和未来无限技术发展的讨论后，有些人认为用 Blstsnd 国王的名字命名再合适不过了。Blstsnd 国王将现在的挪威、瑞典和丹麦统一起来；他口齿伶俐，善于交际，就如同这项即将面世的技术，该技术被定义为允许不同工业领域之间的协调工作，保持各个系统领域之间的良好交流。例如计算机、手机和汽车行业之间的工作。于是名称就这么定下来了。

6.5.2 蓝牙的概念

所谓蓝牙（Bluetooth）技术，实际上是一种低功率、短距离的无线连接技术。

由于采用了向产业界无偿转让该项专利的策略，蓝牙技术目前在无线办公、汽车工业、医疗等设备上随处可见，其应用极为广泛。利用“蓝牙”技术，能够有效地简化掌上电脑、笔记本电脑和移动电话、手机等移动通信终端设备之间的通信，也能够成功简化以上这些设备与 Internet 之间的通信，从而使这些现代通信设备与 Internet 之间的数据传输变得更加迅速高效，为无线通信拓宽道路。蓝牙采用分散式网络结构，以及快跳频和短包技术，支持点对点及点对多点通信，工作在全球通用的 2.4GHz ISM（即工业、科学、医学）频段。其数据传输速率为 1Mbps。采用时分双工传输方案实现全双工传输。通信距离为 10m 左右，配置功率放大器可以使通信距离增加。

6.5.3 蓝牙原理

蓝牙系统由 4 个功能单元组成：无线单元、链路控制单元、链路管理、软件功能。

蓝牙技术是一种无线数据与语音通信的开放性全球规范，它以低成本的近距离无线连接为基础，为固定与移动设备通信环境建立一个特别连接。其程序写在一个 9mm×9mm 的微芯片中。例如，如果把蓝牙技术引入到移动电话和膝上型电脑中，就可以去掉移动电话与膝上型电脑之间的令人讨厌的连接电缆而通过无线建立通信。打印机、PDA、桌上型电脑、传真机、键盘、游戏操纵杆，以及所有其他的数字设备都可以成为蓝牙系统的一部分。除此之外，蓝牙无线技术还为已存在的数字网络和外设提供通用接口以组建一个远离固定网络的个人特别连接设备群。

ISM 频带是对所有无线电系统都开放的频带，因此使用其中的某个频段都会遇到不可预测的干扰源。例如，某些家电、无绳电话、汽车房开门器、微波炉等，都可能是干扰。为此，蓝牙特别设计了快速确认和跳频方案以确保链路稳定。跳频技术是把频带分成若干个跳频信道，在一次连接中，无线电收发器按一定的码序列（即一定的规律，技术上叫做“伪随机码”，就是“假”的随机码）不断地从一个信道“跳”到另一个信道，只有收发双方是按这个规律进行通信的，而其他的干扰不可能按同样的规律进行干扰；跳频的瞬时带宽是很窄的，但通过扩展频谱技术使这个窄带宽成百倍地扩展成宽频带，使干扰可能的影响变成很小。

与其他工作在相同频段的系统相比，蓝牙跳频更快，数据包更短，这使蓝牙比其他系统都更稳定。FEC（Forward Error Correction，前向纠错）的使用抑制了长距离链路的随机噪声。应用了二进制调频（FM）技术的跳频收发器被用来抑制干扰和防止衰落。

蓝牙技术的整个协议体系结构分三大部分：底层硬件模块、中间协议层和高层应用。蓝牙基带协议是电路交换与分组交换的结合。在被保留的时隙中可以传输同步数据包，每个数据包以不同的频率发送。一个数据包名义上占用一个时隙，但实际上可以被扩展到占用 5 个时隙。蓝牙可以支持异步数据信道、多达 3 个的同时进行的同步语音信道，还可以用一个信道同时传送异步数据和同步语音。每个语音信道支持 64kbps 同步语音链路。异步信道可以支持一端最大速率为 721kbps 而另一端速率为 57.6kbps 的不对称连接，也可以支持 43.2kbps 的对称连接。

6.5.4 技术优势

1. 全球可用

Bluetooth 无线技术规格供全球的成员公司免费使用。许多行业的制造商都积极地在其产品中实施此技术，以减少使用零乱的电线，实现无缝连接、流传输立体声，传输数据或进行语音通信。Bluetooth 技术在 2.4GHz 波段运行，该波段是一种无需申请许可证的工业、科技、医学无线电波段。正因如此，使用 Bluetooth 技术不需要支付任何费用。但必须向手机提供商注册使用 GSM 或 CDMA，除了设备费用外，不需要为使用 Bluetooth 技术再支付任何费用。

2. 设备范围

Bluetooth 技术得到了空前广泛的应用，集成该技术的产品从手机、汽车到医疗设备，使用该技术的用户从消费者、工业市场到企业等，不一而足。低功耗、小体积及低成本的芯片解决方案使得 Bluetooth 技术甚至可以应用于极微小的设备中。请在 Bluetooth 产品目录和组件产品列表中查看成员提供的各类产品大全。

3. 易于使用

Bluetooth 技术是一项即时技术，它不要求固定的基础设施，且易于安装和设置。不需要电缆即可实现连接。新用户使用也不费力，只需拥有 Bluetooth 品牌产品，检查可用的配置文件，将其连接至使用同一配置文件的另一 Bluetooth 设备即可。后续的 PIN 码流程就如同在 ATM 机器上操作一样简单。外出时，可以随身带上你的个人局域网（PAN），甚至可以与其他网络连接。

4. 全球通用的规格

Bluetooth 无线技术是当今市场上支持范围最广泛，功能最丰富且安全的无线标准。全球范围内的资格认证程序可以测试成员的产品是否符合标准。自 1999 年发布 Bluetooth 规格以来，总共有超过 4000 家公司成为 Bluetooth 特别兴趣小组（SIG）的成员。同时，市场上 Bluetooth 产品的数量已连续 4 年成倍增长，安装的基站数量在 2005 年底达到 5 亿个。

总之，蓝牙的优势：支持语音和数据传输；采用无线电技术，传输范围大，可穿透不同物质及在物质间扩散；采用跳频展频技术，抗干扰性强，不易窃听；使用在各国都不受限制的频谱，理论上说，不存在干扰问题；功耗低；成本低。蓝牙的技术性能参数：有效传输距离为 10cm～10m，增加发射功率可达到 100m，甚至更远。

6.5.5 应用

1. 在手机上的应用

嵌入蓝牙技术的数字移动电话将可实现一机三用，真正实现个人通信的功能。在办公室可作为内部的无线集团电话，回家后可当做无绳电话来使用，不必支付昂贵的移动电话话费。在室外或乘车的路上，仍将移动电话与掌上电脑或个人数字助理 PDA 结合起来，并通过嵌入蓝牙技术的局域网接入点，随时随地都可以到 Internet 上冲浪浏览，使数字化生活变得更加方便和快捷。同时，借助嵌入蓝牙的头戴式话筒和耳机，以及语音拨号技术，不用动手就可以接听或拨打移动电话。

2. 在掌上 PC 的应用

华清远见

掌上 PC 越来越普及，嵌入蓝牙芯片的掌上 PC 将提供想象不到的便利，通过掌上 PC 不仅可以编写 E-mail，而且可以立即发送出去，没有外线与 PC 连接，一切都由蓝牙设备来传送。这样，在飞机上用掌上 PC 写 E-mail。当飞机着陆后，只需打开手机，所有信息可通过机场的蓝牙设备自动发送。有了蓝牙技术，掌上 PC 能够与桌面系统保持同步。即使是 PC 放在口袋中，桌面系统的任何变化都可以按预先设置好的更新原则，将变化传到掌上 PC 中。回到家中，随身携带的 PDA 通过蓝牙芯片与家庭设备自动通信，可以为你自动打开门锁开灯并将室内的空调或暖气调到预定的温度等。进入旅馆可以自动登记，并将你房间的电子钥匙自动传送到你的 PDA 中，从而可轻轻一按，就可打开你所定的房间。

3．其他数字设备上的应用

数码照相机、数码摄像机等设备装上 Bluetooth 系统，既可免去使用电线的不便，又可不受存储器容量的困扰，随时随地可将所摄图片或影像通过同样装备 Bluetooth 系统的手机或其他设备传回指定的计算机中，蓝牙技术还可以应用于投影机产品，实现投影机的无线连接。

总之，蓝牙系统的小功率、微型化、低成本，以及与网络时代相适应的特性，使它具有广阔的应用前景，随着技术和应用的不断发展，蓝牙技术将在信息家用电器中扮演重要角色，市场潜力巨大。

6.6 GPRS 介绍

6.6.1 GPRS 概述

GPRS 是 General Packet Radio Service 的英文简称，中文为通用无线分组业务，是一种基于 GSM 系统的无线分组交换技术，提供端到端的、广域的无线 IP 连接。相对原来 GSM 的拨号方式的电路交换数据传送方式，GPRS 是分组交换技术，具有“实时在线”、“按量计费”、“快捷登录”、“高速传输”、“自如切换”的优点。通俗地讲，GPRS 是一项高速数据处理的技术，方法是以“分组”的形式传送资料到用户手上。虽然 GPRS 是作为现有 GSM 网络向第三代移动通信过渡的技术，但是它在许多方面都具有显著的优势。

由于使用了“分组”技术，用户上网相对稳定，避免了不必要的短线带来的困扰。此外，使用 GPRS 上网的方法与 WAP 不同，用 WAP 上网就如在家中上网，先“拨号连接”，而上网后便不能同时使用该电话线，但 GPRS 下载资料和通话可以同时进行。从技术上说，声音的传送（即通话）继续使用 GSM，而数据的传送便可使用 GPRS，这样，就把移动电话的应用提升到一个更高的层次。发展 GPRS 技术也十分“经济”，因为只需沿用现有的 GSM 网络即可。GPRS 的用途十分广泛，包括通过手机发送及接收电子邮件，在互联网上浏览等。

6.6.2 GPRS 优势

GPRS 的最大优势在于它的数据传输速度不是 WAP 所能比拟的。目前的 GSM 移动通信网的传输速率为 9.6kbps，GPRS 手机在年初推出时已达到 56kbps 的传输速率，现在更是达到了 115kbps（此速度是常用 56Kmodem 理想速率的两倍）。

GPRS 是以分组交换的方式进行数据传输，由于是分组交换，因此在网络资源的利用上较电路交换有了很大的提高，而且 GPRS 可以同时进行语音与数据的传递，并且计费可以完全按照产生的流量来统计。而现有的 WAP 的承载是电路交换（CSD）方式，电路交换方式数据与语音不能同时进行，在收费模式上也是按照时长来收费。

实际上 WAP 与 GPRS 本质上不具有可比性，现有 WAP 上的内容在 GPRS 上面一样可以浏览和应用，GPRS 使现有的 CSD 方式的 WAP 更快、更方便、收费更合理，对 WAP 的服务内容也会随网络的技术进步而有较大地促进和改善。

WAP 现在用的是 CSD（电路交换数据）的 GSM 数据业务，长远来看，以后 WAP 也可以转为使用 GPRS 这种新的 GSM 网络作为承载方式。

华清远见

但是，GPRS 不会取代 WAP，举一个形象的例子：GPRS 和现在的 CSD 方式的 GSM 数据业务都是马路，WAP 则是马路上的汽车，WAP 现在行驶在两个车道上，GPRS 提高了数据传输速度，是 8 车道，所以说 GPRS 增强了 WAP 业务，现有 WAP 上的内容一样可以通过 GPRS 进行浏览和应用。

6.6.3 GPRS 与 GSM 的比较

GPRS 是在 GSM 基础上发展起来的一种分组交换的数据承载和传输方式，与原有的 GSM 比较，GPRS 在数据业务的承载和支持上具有非常明显的优势：GPRS 可以更有效地利用无线网络信道资源，特别适合突发性、频繁的小流量数据传输；GPRS 支持的数据传输速率更高，理论峰值达 115kbps；GPRS 计费方式更加灵活，可以支持按数据流量进行计费；GPRS 还能支持用户在进行数据传输的同时进行语音通话等。

HSCSD（高速电路交换数据服务）这是 GSM 网络的升级版本，HSCSD（High Speed Circuit Switched Data）能够透过多重时分同时进行传输，而不是只有单一时分，因此能够将传输速度大幅提升到平常的 2~3 倍。目前新加坡 M1 与新加坡电讯的移动电话都采用 HSCSD 系统，其传输速率能够达到 57.6kbps。

6.7 3G 介绍

6.7.1 概述

“3G”（3rd-Generation）是第三代移动通信技术的简称，是支持高速数据传输的蜂窝移动通信技术。3G 服务能同时传送声音（通话）及数据信息（电子邮件、即时通信等），代表特征是提供高速数据业务。相对于第一代模拟制式手机（1G）和第二代 GSM、CDMA 等数字手机（2G），第三代手机（3G）是能将无线通信与 Internet 等多媒体通信结合的新一代移动通信系统。未来的 3G 必将与社区网站进行结合，WAP 与 Web 的结合是一种趋势，如时下流行的微博客网站：大围脖、新浪微博等就已将此应用加入进来。

3G 与 2G 的主要区别在于传输声音和数据的速度上的提升，它能在全球范围内更好地实现无线漫游；处理图像、音乐、视频流等多种媒体形式；提供包括网页浏览、电话会议、电子商务等多种信息服务，同时也要考虑与已有第二代系统的良好兼容性。为了提供这种服务，无线网络必须能够支持不同的数据传输速度，也就是说在室内、室外和行车的环境中能够分别支持至少 2Mbps、384kbps 及 144kbps 的传输速度（此数值根据网络环境会发生变化）。

3G 是第三代通信网络，主要特征是可提供移动宽带多媒体业务。国内目前支持国际电联确定的 3 个无线接口标准，分别是中国电信的 CDMA2000、中国联通的 WCDMA 和中国移动的 TD-SCDMA。GSM 设备采用的是时分多址；而 CDMA 使用码分扩频技术，先进功率和语音激活至少可提供大于 GSM3 倍的网络容量。业界将 CDMA 技术作为 3G 的主流技术，国际电联确定了 3 个无线接口标准，分别是 CDMA2000、WCDMA、TD-SCDMA。原中国联通的 CDMA 现在卖给了中国电信。中国电信已经将 CDMA 升级到了 3G 网络。

6.7.2 3G 标准

国际电信联盟（ITU）在 2000 年 5 月确定了 W-CDMA、CDMA2000 和 TD-SCDMA 三大主流无线接口标准，并写入 3G 技术指导性文件《2000 年国际移动通信计划》（简称 IMT-2000）中。

1. W-CDMA

W-CDMA 即 Wideband CDMA，也称为 CDMA Direct Spread，意为宽频分码多重存取。W-CDMA 的支持者主要是以 GSM 系统为主的欧美厂商，如爱立信、阿尔卡特、诺基亚、朗讯、北电，日本公司也或多或少参与其中，NTT、富士通、夏普等。由于这套系统能够架设在现有的 GSM 网络上，系统提供商可以较轻易地过渡，因而，对于 GSM 系统相当普及的亚洲对这套新技术的接受度预计会相当高。因此，W-CDMA 具有先天的市场优势。

华清远见

2．CDMA2000

CDMA2000 也称为 CDMA Multi-Carrier，由美国高通北美公司为主导提出，摩托罗拉、Lucent 和后来加入的韩国三星也都有参与。韩国现在成为该标准的主导者。这套系统是从窄频 CDMA One 数字标准衍生出来的，可以从原有的 CDMA One 结构直接升级到 3G，建设成本低廉。但目前使用 CDMA 的只有日本、韩国和北美，所以 CDMA2000 的支持者不如 W-CDMA 多。不过 CDMA2000 的研发技术却是目前各标准中进度最快的，许多 3G 手机已经率先面世。

3．TD-SCDMA

TD-SCDMA 标准是中国内地独自制定的 3G 标准，1999 年 6 月 29 日，由中国原邮电部电信科学技术研究院（大唐电信）向 ITU 提出。该标准将智能无线、同步 CDMA 和软件无线电等当今国际领先技术融于其中，在频谱利用率、对业务支持灵活性、频率灵活性及成本等方面具有独特的优势。另外，由于中国庞大的内地市场，该标准受到了各大主要电信设备厂商的重视，全球一半以上的设备厂商都宣布可以支持 TD-SCDMA 标准。

6.7.3 3G 应用

3G 的核心应用包括以下几个方面。

1．宽带上网

宽带上网是 3G 手机的一项很重要的功能，届时能在手机上收发语音邮件、写博客、聊天、搜索、下载图铃等。现在不少人以为这些在手机上的功能应用要等到 3G 时代，但其实目前的无线互联网门户也已经可以提供。尽管目前的 GPRS 网络速度还不能让人非常满意，但 3G 时代的到来，手机变成小计算机已不是梦想。

2．视频通话

3G 时代，视频通话和语音信箱等新业务将是主流，传统的语音通话资费将会降低。视觉冲击力强，快速直接的视频通话会更加普及和飞速发展。

3G 时代被谈论得最多的是手机的视频通话功能，这也是在国外最为流行的 3G 服务之一。相信不少人都用过 QQ、MSN 或 Skype 的视频聊天功能，与远方的亲人、朋友“面对面”地聊天。今后，依靠 3G 网络的高速数据传输，3G 手机用户也可以“面谈”了。当你用 3G 手机拨打视频电话时，不再是把手机放在耳边，而是面对手机，再戴上有线或蓝牙耳麦，你会在手机屏幕上看到对方的影像，你自己的影像也会被录制下来传送给对方。

3．手机电视

从运营商层面来说，3G 牌照的发放解决了一个很大的技术障碍，TD 和 CMMB 等标准的建设也推动了整个行业的发展。手机流媒体软件突破技术瓶颈，在视频影像的流畅和画面质量上不断提升，将会成为 3G 时代使用最多的手机电视软件。

4．无线搜索

对用户来说，无线搜索是比较实用的移动网络服务。随时随地用手机搜索将会成为更多手机用户的一种生活习惯。

5．手机音乐

在无线互联网发展成熟的日本，手机音乐是最为亮丽的一道风景线，通过手机上网下载音乐是计算机的 50 倍。3G 时代，只要在手机上安装一款手机音乐软件，就能通过手机网络，随时随地让手机变身音乐魔盒，轻松收纳无数首歌曲，下载速度更快，耗费流量几乎可以忽略不计。

6．手机购物

华清远见

不少人都有在淘宝上购物的经历，但手机商城对于不少人来说还是新鲜事。事实上，移动电子商务是3G 时代手机上网用户的最爱。目前 90%的日韩手机用户都已经习惯在手机上消费，甚至是购买大米、洗衣粉这样的日常生活用品。专家预计，中国未来手机购物会有一个高速增长期，用户只要开通手机上网服务，就可以通过手机查询商品信息，并在线支付购买产品。高速 3G 可以让手机购物变得更实在，高质量的图片与视频会话能拉近商家与消费者的距离，提高购物体验，让手机购物变为新潮流。

7．手机网游

与计算机的网游相比，手机网游的体验并不好，但方便携带，随时可以玩，这种利用了零碎时间的网游是目前年轻人的新宠，也是 3G 时代的一个重要资本增长点。随着 3G 时代的到来，游戏平台会更加稳定和快速，兼容性更高，即“更好玩了”，像升级的版本，游戏的视觉和效果方面也会更好。

6.8 本章习题

1．简单介绍应用于无线传输的技术有哪些，并分别介绍这些技术的特点。
2．重点掌握 ZigBee 无线传输技术，了解 ZigBee 无线传输的技术特点及 ZigBee 的通信协议。

联系方式

集团官网：www.hqyj.com　　嵌入式学院：www.embedu.org　　移动互联网学院：www.3g-edu.org

企业学院：www.farsight.com.cn　　物联网学院：www.topsight.cn　　研发中心：dev.hqyj.com

集团总部地址：北京市海淀区西三旗悦秀路北京明园大学校内 华清远见教育集团

北京地址：北京市海淀区西三旗悦秀路北京明园大学校区，电话：010-82600386/5

上海地址：上海市徐汇区漕溪路银海大厦 A 座 8 层，电话：021-54485127

深圳地址：深圳市龙华新区人民北路美丽 AAA 大厦 15 层，电话：0755-22193762

成都地址：成都市武侯区科华北路 99 号科华大厦 6 层，电话：028-85405115

南京地址：南京市白下区汉中路 185 号鸿运大厦 10 层，电话：025-86551900

武汉地址：武汉市工程大学卓刀泉校区科技孵化器大楼 8 层，电话：027-87804688

西安地址：西安市高新区高新一路 12 号创业大厦 D3 楼 5 层，电话：029-68785218

华清远见