第3章 无线局域网技术

无线局域网(Wireless LAN,WLAN)技术是计算机网络与无线通信技术相结合的产物,WLAN以自由空间中的无线电波取代了有线电缆中的电磁波或光缆中的光波,可以不受有线电缆或光缆束缚、自由移动,因此可以解决因有线电缆或光缆布线困难所带来的布线问题,具有组网灵活、扩容方便等优点。无线局域网非常适合移动办公用户的需要,具有广阔的应用市场,目前无论是在家庭,还是在工作单位,无线局域网的使用已经越来越普及。因此在现在的网络工程实践中,应用WLAN技术已经成为一项基本的工程设计任务,本章将重点讲解WLAN中的IEEE 802.11标准及其应用。

3.1 无线局域网概述

无线局域网中的通信标准有很多,主要有HiperLAN、蓝牙技术、HomeRF、IEEE 802.11等。从现在的应用市场来说,IEEE 802.11标准在性能、价格等各方面均已超过了蓝牙、Home RF等技术标准,在以太网的无线接入应用中成为使用最为广泛的标准。

3.1.1 HiperLAN技术

HiperLAN是欧盟在1992年提出的一个WLAN标准。在IEEE制定802.11系列WLAN标准的同时,欧洲通信标准学会(ETSI)则在大力推广HiperLAN1/HiperLAN2标准。HiperLAN1发布于1996年,它工作于5GHz频带,数据速率最高可达25Mb/s。整体上看,HiperLAN1与IEEE802.11b是相当的。HiperLAN2是HiperLANl的第二代版本,于2000年年底通过ETSI批准成为标准。它对应于IEEE的802.11a,工作在5GHz频带,支持最高数据速率为54Mb/s。HiperLAN2标准也是目前较完善的WLAN协议,支持HiperLAN2标准的厂商主要集中在欧洲地区。

3.1.2 蓝牙技术

蓝牙(Bluetooth)技术是由爱立信、诺基亚、Intel、IBM和东芝5家公司于1998年5月共同提出开发的。蓝牙技术的本质是设备间的无线连接,主要用于通信与信息设备。由于使用低功率的无线电传输技术,让不同产品(例如打印机、PDA、PC、传真机、键盘、Notebook)于短距离进行数据传输及沟通,因此蓝牙不必使用任何有线的传输线路(例如电线或缆线),就能连接各种数字设备,让所谓的移动通信成为事实。蓝牙技术已经成为移动通信领域的基本技术,也是移动电话、个人计算机、笔记本型计算机和其他电器设备的标准功能。

蓝牙技术与红外光无线传输技术(IrDA)相似,皆为短距离的无线传输。但是红外光无线传输装置在进行数据传输时需将两传输装置对准,而蓝牙为“点”传输技术,在进行传输时,数据从发射点以球状向四面八方进行传输,故在应用性及方便性上,蓝牙技术优于红外光无线传输技术。

3.1.3 HomeRF 技术

HomeRF 技术是专为家庭用户设计的无线传输技术,由微软、英特尔、惠普、摩托罗拉和康柏等公司提出,其主要目标是为家庭用户建立具有互操作性的话音和数据通信网,工作频段为 2.4GHz。HomeRF 技术基于共享无线接入协议(Shared Wireless Access Protocol,SWAP),SWAP 使用 TDMA+CSMA/CA 方式,适合语音和数据业务。在进行语音通信时,它采用数字增强无绳电话(DECT)标准,DECT 使用 TDMA 时分多址技术,适合于传送交互式语音和其他时间敏感性业务。在进行数据通信时它采用 IEEE 802.11 的 CSMA/CA 协议,CSMA/CA 适合于传送高速分组数据。

3.1.4 IEEE 802.11 技术

IEEE 802.11 技术标准是 IEEE 制定的无线局域网标准,主要对物理层与媒体访问控制子层(MAC 子层)进行了相关规定,物理层定义了工作在 2.4GHz 的 ISM 频段上的两种扩频作调制方式和一种红外线传输的方式,总数据传输速率设计为 2Mb/s。两个设备之间可以自行构建临时网络,也可以在基站(Base Station,BS)或者接入点(Access Point,AP)的协调下相互通信。为了在不同的通信环境下取得良好的通信质量,采用 CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)协议。目前使用的 IEEE 802.11 标准主要有 4 种,分别是 802.11a、802.11b、802.11g、802.11n。

1. IEEE 802.11a

IEEE 802.11a 是对 IEEE 802.11 原始标准的一个修订标准,使用与原始标准相同的核心协议,工作频率为 5GHz,采用了 52 个正交频分多路复用载波技术,最大原始数据传输率为 54Mb/s。随着传输距离的增加或背景噪声的增大,数据传输率会不断递减。

需要注意的是此标准与其他标准如 802.11b/g/n 不兼容。

2. IEEE 802.11b

IEEE 802.11b 工作于 2.4GHz 频率,支持最高为 11Mb/s 的传输速率,在低速率 2Mb/s 或 1Mb/s 下与 IEEE 802.11 标准兼容。此标准最大的贡献是增加了两个新的速率:5.5Mb/s 与 11Mb/s,为了更好地支持有噪声的环境,802.11b 使用了动态速率调节技术,允许用户在不同的环境中自动使用不同的连接速率。在理想环境下,用户可以 11Mb/s 速率传输,而当用户环境恶化后,802.11b 可以将速率自动按序降低到 5.5Mb/s、2Mb/s、1Mb/s;而当用户环境改善后,其速率可以反向增加到 11Mb/s。这些变化及调节均在物理层自动实现,对用户及上层协议没有任何影响。

3. IEEE 802.11g

IEEE 802.11g 标准工作于 2.4GHz 频率,并具有两个明显特征:高速率、兼容 802.11b。IEEE 802.11g 使用了与 802.11a 相同的正交频分多路复用载波技术,因此可以实现最高为 54Mb/s 的数据传输速率。在同样 54Mb/s 的数据传输速率下,802.11g 可以提供大约两倍

于 802.11a 的距离覆盖；802.11g 同时保留了 802.11b 的编码技术，可以实现与 IEEE 802.11b 的兼容。

4. IEEE 802.11n

IEEE 802.11n 标准是 802 系列标准中最新的标准，此标准具有向下兼容的能力，能够与 802.11b/g 混合通信。802.11n 的数据传输速率可以达到 100Mb/s 以上，最高可以达到 600Mb/s，是 802.11g 标准的 10 倍左右。此标准使用智能天线技术，可以通过多组独立天线组成天线阵列系统，动态调整无线电波的方向，保证用户可以接收到稳定的无线信号，其覆盖范围可以扩大到几平方千米。

3.2 基于 IEEE 802.11 的无线局域网

在如今的网络工程应用中，基于以太网进行无线接入的需求越来越多，使用 IEEE 802.11 标准体系组建 WLAN 的应用也越来越普及，因此了解基于 IEEE 802.11 标准的 WLAN 对于网络工程应用的设计非常重要。本节将从无线局域网使用的调制技术、CSMA/CA 协议、安全协议等方面介绍 IEEE 802.11。

3.2.1 调制技术

根据无线电标准的定义，调制是改变载波的特性使其与承载信息的信号相一致的过程或过程的结果，调制的目的是将信号覆盖到载波上。调制的基本方法主要有调幅、调频、调相，大多数通信系统都部分或组合地使用这三种基本调制技术。这些通信技术在极端情况还会使用幅移键控、频移键控、相移键控等技术。在 IEEE 802.11 的无线标准中同样使用了多种不同的调制技术，根据数据率的不同，这些具体标准使用了不同的调制技术。

1. 802.11a

802.11a 使用了三种必需的和一种可选的调制技术。

(1) 二进制相移键控(BPSK)：对于一位的二进制数据，用一个相位来代表二进制的 1，用另一个相位代表二进制的 0。

(2) 正交相移键控(QPSK)：载波有 4 种相位的变化，因而它可以表示两个二进制位的数据。通常用于在 2Mb/s 的速率下发送数据。

(3) 16 位的正交调幅(16QAM)：每 Hz 编码 4 位，数据率可达 24Mb/s。

(4) 64 位的正交调幅(64QAM)：此调制技术为可选技术，每个周期编码 8 位或 10 位，相当于每个 300kHz 的信道编码最多 1.125Mb/s 的数据，数据率可达 54Mb/s。

2. 802.11b

802.11b 使用了三种不同类型的调制技术。

(1) 二进制相移键控：通常用于在 1Mb/s 速率下发送数据。

(2) 正交相移键控：通常用于在 2Mb/s 的速率下发送数据。

(3) 补码键控(CCK)：使用一个称为补码的复杂函数来发送更多的数据。CCK 比类似的调制技术有一个优势，那就是它可以避免多路干扰。CCK 用于在 5.5Mb/s 和 11Mb/s 的速率下发送数据。

3. 802.11g

802.11g 使用与 802.11a 相同的调制技术，同时也支持 CCK 调制技术。这就是 802.11g 支持 54Mb/s 的客户端并后向兼容 802.11b 客户端的原因。

4. 802.11n

802.11n 使用了 OFDM(Orthogonal Frequency Division Multiplexing，正交频分复用技术)技术，此技术是 MCM(Multi-Carrier Modulation，多载波调制)技术的一种，其核心思想是将信道分成许多进行窄带调制和传输正交子信道，并使每个子信道上的信号带宽小于信道的相关带宽，用以减少各个载波之间的相互干扰，同时提高频谱的利用率的技术。OFDM 还通过使用不同数量的子信道来实现上行和下行的非对称性传输。802.11n 在使用 OFDM 技术的同时，还融入了 MIMO(多入多出)天线技术，从而使 802.11n 的有效传输速率有质的提升，其数据传输速率最高可以达到 600Mb/s。

3.2.2 CSMA/CA 协议

IEEE 802.11 的各类标准一般都工作在 2.4GHz 或 5GHz 频段中，这些频率都属于 ISM 频段，是未加管制的频段。这意味着在无线电信号覆盖的空间中，不同站点之间同时发送数据可能会引起信号叠加即冲突，因此在无线局域网中必须采取措施来解决信号冲突的问题，目前在 IEEE 802.11 标准中使用的解决技术被称为 CSMA/CA(Carrier Sense Multiple Access with Collision Avoidance，带冲突避免的载波监听多路访问)，此协议与以太网中的 CSMA/CD 协议类似，都是用于共享信道的通信协议，但又有明显的不同：CSMA/CD 协议用于在共享以太网中检测冲突，而 CSMA/CA 则用于无线信道中避免冲突。

CSMA/CA 使用的载波监听机制与共享以太网使用的 CSMA/CD 协议类似，站点在发送数据前监听信道，若信道忙则需要等待一个随机时间后继续监听；但与 CSMA/CD 协议不同的是当 CSMA/CA 协议监听到信道空闲后，并不是立即开始数据帧的发送，而是等待一个随机的时间后再发送，这样做的目的是使发送的无线电信号发生碰撞的概率减至最小，这种机制也被称为 CSMA/CA 的随机退避机制。

虽然使用了随机退避机制，但冲突仍然可能出现，因此 CSMA/CA 为了保证协议工作的稳定性，专门设置了 ACK 应答帧用来指示是否发生了冲突，同时还使用虚拟载波检测机制：发送方在发送的数据帧中加入持续期字段，该字段存放有一个称为网络分配矢量(NAV)的持续时间。持续期字段用于通知其他站点在此时间段内不必监听信道，其他站点通过 NAV 设置计时器并进行倒计时，计时器不为零表示信道有载波不空闲(即使此时信道空闲)。

3.2.3 安全技术

WLAN 最基本的特点是在数据通信过程中使用无线电信号传输数据，而在无线电信号覆盖的空间中，任何站点均可对通信的数据进行窃听或伪造。因此如何在无线局域网中提高用户的通信安全，是 WLAN 必须考虑的重要问题。不断改进并提高 WLAN 的安全，是 WLAN 在安全领域内的重要内容，本节重点介绍当前 WLAN 中常见的几种安全技术。

1. 配置 SSID

SSID(Service Set Identifier，服务集标识)是相邻无线网络区分的标志，这个标志通常

使用字符串表示，是当前无线局域网中唯一的字符串，通常 SSID 被配置在无线接入点（AP）或无线路由器（WRouter）中。使用 SSID 可以将一个无线空间分为几个需要不同身份验证的 WLAN，每一个 WLAN 都可以使用独立的身份验证，只有通过身份验证的用户才可以进入相应的 WLAN，从而可以防止未被授权的用户进入网络。任何用户在连接 WLAN 时，都必须提供这个唯一的 SSID 字符串，但是由于无线电信号广播的特性，此 SSID 字符串在无线空间中是很容易被窃听到的，因此配置 SSID 只是 WLAN 中最基本、同时也是最不安全的技术手段。

2. MAC 地址过滤

MAC 地址过滤技术可以在 AP 或 WRouter 中配置一个允许用户接入的用户 MAC 地址清单，接入用户的 MAC 地址若不在当前 MAC 地址清单中，则 AP 或 WRouter 将拒绝其接入请求。这种安全技术一般只适用于用户数量很少的轻量级 WLAN（例如家庭使用的 WLAN），在用户数较多或安全要求较高的 WLAN 中，一般不建议使用 MAC 地址过滤技术。其原因在于用户的 MAC 地址在 WLAN 中属于明文传输形式，攻击者只要监听无线信道便可获得相应用户的 MAC 地址，并可以轻易将自己无线网卡的 MAC 地址改为此 MAC 地址，从而可以伪装成另一个用户进入 WLAN。这种 MAC 地址控制属于硬件认证，对于网管而言，一旦用户数达到一定规模，通过 MAC 地址进行过滤的工作量将非常巨大且无效率。真正具有应用价值的安全认证还是需要使用更高层次的用户认证。

3. WEP 协议

WEP（Wired Equivalent Privacy，有线等效保密）协议是对两台设备间无线传输的数据进行加密的协议，用来防止非法用户窃听或入侵 WLAN，可以提供访问控制、数据加密和安全性检验等功能，是 IEEE 802.11 中的第一个安全协议，同时也是一种可选的链路层安全机制，其加密技术来源于 RSA 数据安全公司的 RC4 对称加密技术，可以满足用户更高层次的安全需求。RC4 用在 IEEE 802.11 的数据链路层中，只有当用户的加密密钥与 AP 的密钥相同时，用户才能获取网络资源。

WEP 的工作原理是通过一组 40 位或 128 位的密钥作为认证口令，当 IEEE 802.11 启用 WEP 功能时，每个合法站点使用这个认证口令，将要发送的明文数据进行加密形成密文数据，并通过无线电传输；其他接收站点同样使用此认证口令对接收的密文数据进行解密，从而可以获得明文数据。

由于 WEP 加密技术自身的技术缺陷，目前这种安全技术已经很少被使用，也不建议在 IEEE 802.11 的 WLAN 中使用 WEP 加密技术。

4. WPA 协议

WPA（Wi-Fi Protected Access，Wi-Fi 保护性接入）协议是继承了 WEP 基本原理、同时又解决了 WEP 自身缺陷的一种全新加密技术。WPA 的基本原理是根据通用密钥，配合站点的 MAC 地址和分组信息的序列号，为每个分组生成不同的加密密钥。然后使用与 WEP 一样的方式，将此加密密钥用于 RC4 协议进行加密处理。通过这种技术，所有站点发送的分组都将使用不同的加密密钥进行加密，可以防止数据被中途篡改，并实现认证功能。

目前有 WPA 和 WPA2 两个标准，WPA2 是 WPA 的升级版，与 WPA 的主要差别在于其使用了更安全的 AES 加密技术。因此建议在 IEEE 802.11 的 WLAN 中使用最新的 WPA2 协议。

3.2.4 Wi-Fi 联盟与 WAPI

IEEE 802.11 的相关协议及技术标准还有很多，本章只是有针对性地进行了一些简单介绍与说明。在深入学习与了解 WLAN 的标准时，将不得不了解与 WLAN 标准有着非常密切关系的 Wi-Fi 联盟及 WAPI。

Wi-Fi 联盟(Wi-Fi Alliance，WFA)是一个商业联盟，拥有 Wi-Fi 的商标，负责 Wi-Fi 认证及商标授权的工作。该联盟的成员有来自世界各地的公司及厂家，其成员的产品通过认证后，有权标明这些产品的 Wi-Fi 标志。认证过程简单来说是测试产品是否符合 IEEE 802.11 标准的相关规定，以及 WPA 和 WPA2 等安全标准的实现。因此 Wi-Fi 认证是建立在 IEEE 802.11 标准上的认证技术，目前在 WLAN 领域内的影响力非常大，在网络工程中使用的无线设备也基本都来自 Wi-Fi 联盟(即通过 Wi-Fi 认证的产品)。

WAPI(WLAN Authentication and Privacy Infrastructure，无线鉴别和保密基础结构)是一个关于无线局域网的中华人民共和国国家标准(GB 15629.11—2003)。虽然它被设计为基于 Wi-Fi 运行，但其与 IEEE 802.11 的 WLAN 标准所用安全协议存在兼容性问题。WAPI 起初是为了解决 WEP 协议中的安全漏洞而设计的，主要由 WAI(WLAN Authentication Infrastructure，无线局域网鉴别基础结构)和 WPI(WLAN Privacy Infrastructure，无线局域网保密基础结构)两部分组成。WAI 定义了 WLAN 中身份鉴别和密钥管理的安全方案，WPI 定义了 WLAN 中数据传输保护的安全方案，包括数据加密、鉴别和重放保护等。WAPI 标准中使用了 SM4 分组密码算法、ECDSA 椭圆曲线数字签名算法以及 ECDH 密钥交换算法，其中，SM4 分组密码算法由国家商用密码管理办公室发布，根据不同的情况，也可以使用 AES 来替代 SM4 算法。2006 年 3 月，ISO 通过 802.11i 加密标准，并驳回 WAPI 提案；2009 年 6 月，中国重新提交 WAPI 标准申请，但在 2011 年 11 月 21 日，将此申请撤回，ISO 随即将 WAPI 项目取消。

3.3 常见的无线设备

无线设备是组建 WLAN 时必须使用的设备，目前无线产品的种类及功能众多，为了保持网络最大的兼容性及后期网络管理的统一性，在选择无线设备产品时，应当尽量选用支持以太网技术的同一厂商、同一系列或同一标准的产品。本节将介绍 WLAN 中最常见的三类无线设备：无线网卡、无线 AP、无线路由器，这些无线设备在网络工程实践中经常使用。

3.3.1 无线网卡

无线网卡是无线用户接入 WLAN 的必备设备，现在绝大多数移动设备(例如笔记本、智能手机等)都通过集成方式内置了无线网卡，没有集成无线网卡的设备(例如台式计算机)可以通过安装无线网卡接入 WLAN。这些可安装的无线网卡根据接口类型的不同，可以将无线网卡分为以下三种。

USB 无线网卡：通过 USB 接口连接设备，适用于没有内置无线网卡的笔记本或普通台式计算机，具有支持热插拔、兼容性强的特点，是目前网络工程应用中最为简便的无线网卡解决方案。

PCI 无线网卡：适用于普通的台式计算机，通过主板的 PCI 插槽连接 PCI 无线网卡。在网络工程应用中的缺点是需要打开计算机的机箱进行操作，不仅工作量大，而且对于某些在保修期内的计算机而言，机箱是不能打开的。

PCMCIA 无线网卡：仅用于早期没有集成无线网卡的笔记本，同样支持热插拔功能，但目前在网络工程应用中几乎看不到这类无线网卡了。

如图 3.1 所示的是 TP-LINK 公司的三种无线网卡，从左到右分别是 USB、PCI、PCMCIA 无线网卡。其他厂商的无线网卡形状与此基本类似。

图 3.1　三种不同的无线网卡

3.3.2　无线 AP

无线 AP(Access Point)是无线网络与有线网络之间的节点设备，无线客户端通过无线网卡接入无线 AP 设备后，就可以通过 WLAN 相互访问，还可以通过无线 AP 与有线以太网相互通信。

无线 AP 根据管理方式的不同，可以分为胖 AP 与瘦 AP 两种。

胖 AP 相当于功能较强的无线路由器，除了可以提供无线接入功能外，一般还支持 DHCP、DNS、VPN、防火墙等功能。胖 AP 的应用场合仅限于小型无线网络(例如家庭无线网络)，对于大规模无线部署，如大型企业网无线应用、行业无线应用以及运营级无线网络，则不适合使用胖 AP。

瘦 AP 属于轻型无线 AP，必须借助无线网络控制器进行配置和管理，瘦 AP 不能独立工作。通过无线网络控制器加瘦 AP 的组网模式，可以将密集型的无线网络(例如大型企业网无线应用)及安全控制功能从无线 AP 转移到集中的无线网络控制器中，进行统一的配置和管理；而瘦 AP 只负责无线数据的发送与接收，基本可以做到零配置。

无论是胖 AP 还是瘦 AP，其工作模式都是共享背板总线带宽，因此当接入无线 AP 的用户数量增加到一定数量时将严重影响无线 AP 的数据传输速率。一般建议无线 AP 实际接入的无线用户数量控制在 30 个左右。

有些无线 AP 的生产厂家为了方便客户的使用，在生产无线 AP 时会将胖、瘦两种 AP 融合在一起，由客户在使用时自己决定无线 AP 的管理方式；有些无线 AP 也会使用一些附加的功能，如以太网供电(PoE)功能，这样客户就可以简化掉无线 AP 在网络工程施工中的电源布线工程。例如，TP-LINK 的无线 AP 产品 TL-AP450I-PoE 就采用了这种胖瘦一体、PoE 供电的设计模式，其产品形状如图 3.2 所示。

图 3.2　胖瘦一体无线 AP(型号 TL-AP450I-PoE)

3.3.3 无线路由器

无线路由器属于扩展型的无线 AP，一般融合了宽带路由器与无线 AP 两者的功能。其中的宽带功能用于接入互联网，为 WLAN 中的用户提供上网功能；而无线 AP 用于将无线客户端接入到有线的以太网中。无线路由器在提供无线接入功能的同时，也会提供若干个有线以太网接口（一般有 4 个以太网接口）用于连接有线网络中的计算机。此设备是小型无线局域网应用（例如家庭无线网络）中最常见的无线设备，这种设备既可实现无线客户端的接入，也可以实现有线客户端的接入，同时还能为这些客户端提供接入互联网的服务。

图 3.3 无线路由器的一般形状

如图 3.3 所示图片为无线路由器常见的形状，无线路由器一般使用独立电源适配器供电，有显式的天线用于无线电信号的发送与接收，有的设备可能配备两根或 4 根天线以增加无线电信号的覆盖范围；图 3.3 中的第一个 RJ-45 端口用于连接小区宽带进来的以太网线，实现互联网的接入功能；后面的 4 个 RJ-45 端口用于连接有线的计算机网卡，这 4 个端口连接的计算机构成一个小型的 LAN。

3.4 WLAN 的配置及应用

WLAN 中使用的设备型号虽说众多，但不同产品的配置方法大同小异。为了实验的方便，本节将使用思科的 Packet Tracer 软件模拟 WLAN 中常见的无线 AP 与无线路由器的配置。

3.4.1 无线 AP 的配置

为了说明无线 AP 的配置及其应用模式，本节使用思科的 Packet Tracer 软件设计了如图 3.4 所示的网络拓扑结构。图中的路由器端口 f0/0 连接以太网交换机，用于模拟当前以太网的网关 10.1.1.254/24，路由器同时为当前 LAN 提供 DHCP 服务；交换机分别连接一台计算机 PC1 与无线 AP 的以太网端口；计算机 PC2 用于模拟使用无线网卡的客户端；PC1 与 PC2 均使用路由器的 DHCP 服务。

图 3.4 所描述的拓扑图在实际网络工程应用中很常见，本节就以此拓扑为例详细说明无线 AP 的具体配置与应用，其操作的基本过程如下所示。

1. 首次连接无线 AP

在模拟软件 Packet Tracer 中，计算机默认都是使用以太网网卡进行网络的连接。为了连接无线 AP，必须将 PC2 中的以太网网卡移除，并添加一个无线网卡。其操作的方法（可以参考 1.3 节）如下。

单击图 3.4 所示界面中的 PC2 图标，打开 PC2 的配置窗口；选择其中的 Physical 选项卡，在 Physical Device View 视图区中单击计算机的电源开关，关闭计算机的电源后，将计算机下方的以太网网卡移除；选择 Modules 列表中的第一个选项“WMP300N 选项”（此选项表示 Linksys 的无线网卡型号），使用鼠标将配置窗口右下角的无线网卡图示拖到

Physical Device View 视图区中计算机的网卡位置；单击计算机的电源开关，打开计算机的电源。此时仔细观察 Packet Tracer 模拟软件的工作区，将会发现图 3.4 中的 PC2 会自动与无线 AP 设备建立一条无线连接的示意线。

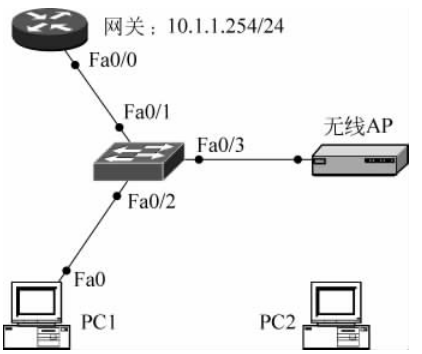

图 3.4　无线 AP 的配置及应用

图 3.4 中的 PC2 之所以能够自动连接无线 AP，是因为此时的无线 AP 没有进行任何配置，无线 AP 上也没有使用任何安全措施，任何无线客户端均可以自动连接到此无线 AP 上。在实际的无线 AP 产品中，一般也都会使用默认无安全措施的参数，以便让无线客户端可以很方便地连接到无线 AP 上进行首次配置。即使部分厂商为了安全，使用了 Web 登录的安全措施，但登录的用户名与密码一般也会使用简单的字符串，例如使用 admin 作为用户名及密码。因此在实际的网络工程应用中，对于新的无线 AP 设备，计算机一般通过无线网卡都可以很方便地连接到无线 AP 上；如果不能成功连接到无线 AP 设备，可以长按无线 AP 设备上专门设置的 Reset 按钮 5s 以上，则无线 AP 会自动重新初始化所有参数回到默认值。等待无线 AP 重新启动成功后，无线客户端就可以自动连接到使用默认参数的无线 AP 设备上。

2. 配置无线 AP 的安全参数

当计算机 PC2 连接到无线 AP 后，紧跟着必须马上实施的一项配置是为无线 AP 配置安全技术参数及网络参数。在模拟软件 Packet Tracer 中，单击图 3.4 中的无线 AP 图标，打开无线 AP 的配置窗口，打开其中的 Config 选项卡，在左边的列表中选择 Interface 中的 Port1 选项，在配置窗口右边配置无线 AP 相关的参数，其配置界面如图 3.5 所示。

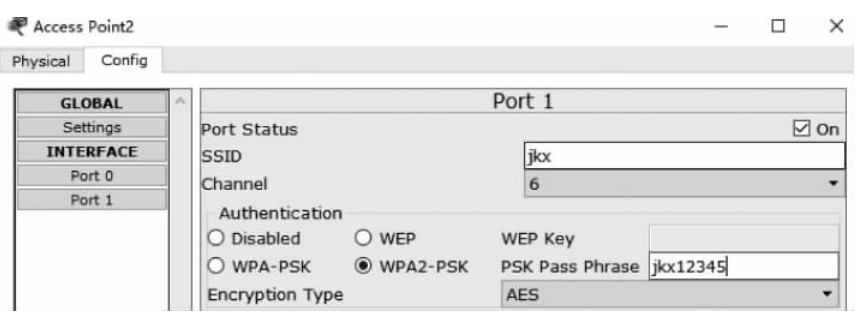

图 3.5　无线 AP 的参数

在图 3.5 中，分别配置 SSID 为 jkx、Authentication 方式选择 WPA2-PSK 选项、密钥短语为“jkx12345”。完成以上参数后，仔细观察图 3.4 中的 PC2，会发现 PC2 与无线 AP 之间的无线连接已经断开。原因是此时的无线 AP 已经被配置了安全参数，网络中的无线客户端必须使用这些安全参数才能接入到此无线 AP，没有这些安全参数则不能接入到无线 AP。

需要说明的是在实际的网络工程应用中，如图 3.5 所示的界面多数通过无线 AP 设备上的 Web 服务提供。当无线客户端通过默认没有安全参数的方式首次连接无线 AP 时，可

以使用一个默认的 IP 地址参数(一般使用 192.168.1.*/24 形式,具体参数需要查阅产品说明书)连接到无线 AP。然后客户端用户就可以使用 Web 浏览器打开无线 AP 的 Web 页面,Web 浏览器浏览的地址一般为 192.168.1.1(代表无线 AP 的 IP 地址需要查阅产品说明书),这些页面的内容虽说各不相同,但基本都具有如图 3.5 所示的类似参数。

3. 重新配置无线客户端

在模拟软件 Packet Tracer 中,单击图 3.4 中的 PC2 图标,打开 PC2 的配置窗口;打开 Desktop 选项卡;单击选项卡中的 PC Wireless 图标打开无线 AP 的配置界面,如图 3.6 所示。

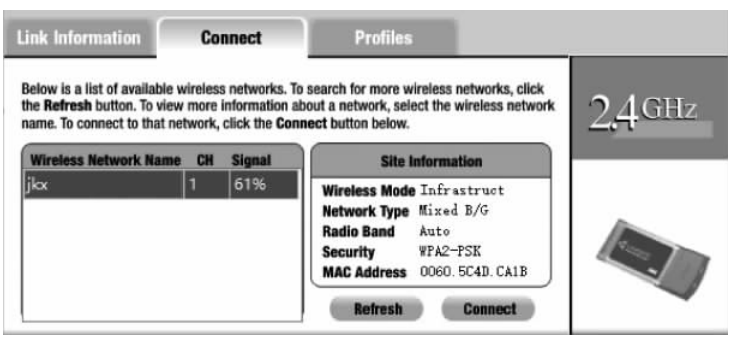

图 3.6　无线客户端的配置界面

在图 3.6 中,打开 Connect 选项卡,PC2 将自动识别出当前的无线 AP 名称,即 SSID 为 jkx 的无线 AP。单击下方的 Connect 按钮,打开如图 3.7 所示的界面。

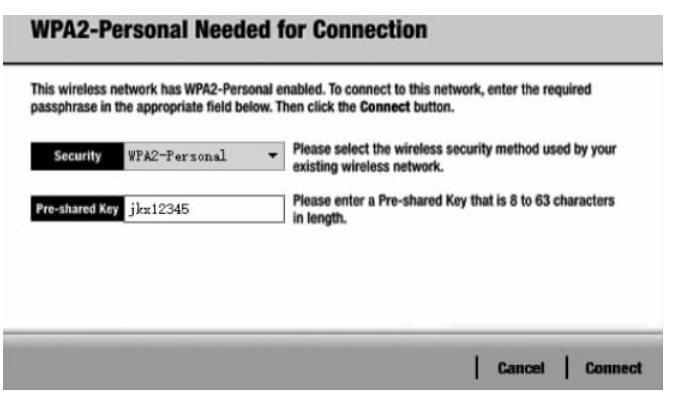

图 3.7　设置 WPA2 的密钥短语

在图 3.7 中使用默认的安全协议 WPA2-Personal,并输入无线 AP 中已经配置的密钥“jkx12345”,然后单击 Connect 按钮进行连接。如果图 3.7 中配置的参数与无线 AP 中配置的安全参数相同,则会发现图 3.4 中 PC2 与无线 AP 之间的无线连接再次出现。这表明 PC2 作为无线客户端已经成功连接到了无线 AP。

在图 3.6 所示界面中配置无线客户端参数时,也可以使用 Profile 选项卡配置客户端,其操作的过程如下。

单击对话框下方的 Edit 链接打开 Available Wireless Networks 对话框;继续单击对话

框下方的 Advanced Setup 链接，打开 Wireless Mode 对话框；此时有两个选项：Infrastructure Mode 与 Ad-hoc Mode，其中的 Infrastructure Mode 用于连接无线网络，并要求存在一个无线 AP，加入 WLAN 的无线 AP 和所有的无线客户端都必须配置相同的 SSID；而 Ad-hoc Mode 是一种专为无线设备设计，让它们可以直接互相进行通信的模式，运行于 Ad-hoc 模式下，允许所有无线设备在彼此的射程之内发现对方并进行点对点的通信，而无须通过中心访问点。若要建立一个 Ad-hoc 无线网络，则每个无线设备都必须配置为 ad-hoc 模式而不是 infrastructure 模式，并且使用相同的 SSID 和 channel 号。

这里使用默认的 Infrastructure Mode，并在下方的文本框中输入无线 AP 的 SSID：jkx，然后连续单击 Next 链接，在配置 WPA2 密钥短语的文本框中输入无线 AP 配置的密钥：jkx12345，单击 Next 链接直至完成操作。

3.4.2 无线路由器的配置

无线路由器设备在企事业单位的部门科室应用较多，它不仅可以提供无线客户端接入有线以太网的服务，还可以用于连接少量使用有线网卡的 PC，如图 3.8 所示的网络拓扑图是此类应用常见的拓扑结构。

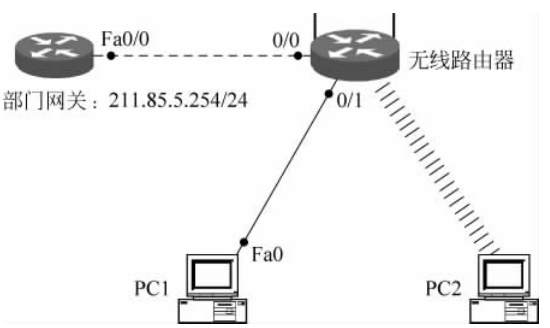

图 3.8　无线路由器的应用案例

在图 3.8 中：左边的路由器充当部门网关设备，与无线路由器的 WAN 端口连接，用于将无线网络接入到单位的现有网络中，其网关地址为 211.85.5.254/24；无线路由器是 Cisco Packet Tracer 模拟软件模拟的设备，其型号为 WRT300N；计算机 PC1 连接无线路由器的 LAN 端口 0/1，模拟使用有线网卡的计算机通过无线路由器接入网络的情形，而计算机 PC2 安装无线网卡连接到无线路由器，模拟无线客户端通过无线路由器接入网络的情形。

本节以图 3.8 所示的拓扑结构为例，详细说明无线路由器在应用时会使用的常规配置，其操作过程大致如下。

1. 首次连接无线路由器

无线路由器设备与前面介绍的无线 AP 一样，在没有配置安全参数前，任何无线客户端都可以直接接入无线路由器，如图 3.8 所示，PC2 就已经自动连接到了无线路由器。对于多数的无线路由器设备而言，一般在提供无线接入的功能之外，还会提供 4 个以太网 RJ-45 端口（有的无线路由器产品可能还会提供更多的端口），用于连接使用有线网卡的普通计算机，这些端口连接的计算机与无线接入的计算机共同构成了此无线路由器本地的小型局域网。

因此在首次连接无线路由器时，除了使用无线客户端进行无线接入配置外，还可以通过网线连接普通计算机到无线路由器上进行配置，且这种方式相对更简单。

无论是通过有线的 PC1、还是无线的 PC2，首次连接无线路由器时，只需要将计算机的 IP 地址参数设置为自动获得即可（也称为 DHCP 方式）。在 PT 模拟软件中，单击 PC1 图标，打开 PC1 的配置窗口，选择 Desktop 选项卡，单击其中的 IP Configuration 图标，打开 IP Configuration 对话框，如图 3.9 所示。在图 3.9 所示界面中，单击 DHCP 选项，此时 PC 将通过无线路由器默认提供的 DHCP 服务获得一个动态 IP 地址参数：192.168.0.103/24，如图 3.9 所示。PC 获得的 IP 地址一般均为 RFC 1918 文档中定义的私有 IP 地址，不同的无线路由器产品分配的私有 IP 地址可能会有些不同，有的产品使用 192.168.0.0/24，也有的产品使用 192.168.1.0/24 地址。

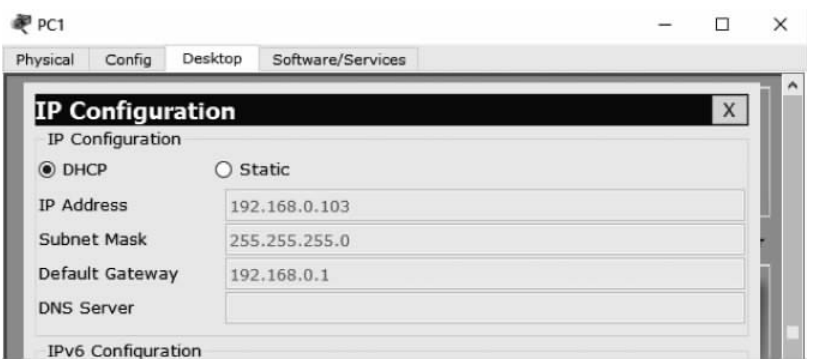

图 3.9　配置 PC 的 DHCP 方式

在 PC2 同样需要进行上述操作，以便获得一个能够连接无线路由器 Web 页面的 IP 地址参数。

2. 配置无线路由器的相关参数

当 PC 通过上一步得到相应的 IP 地址参数后，计算机就可以通过自己的 Web 浏览器打开无线路由器提供的 Web 页面。打开方法是在 Desktop 选项卡中单击 Web Browser 图标，在弹出的 Web 浏览器地址栏中输入代表无线路由器的 IP 地址，此 IP 地址一般为计算机通过 DHCP 获得的 IP 地址参数中的网关地址（例如本例的网关为 192.168.0.1）。打开 Web 页面后，无线路由器会要求输入用户名与密码，默认的用户名与密码都是 admin，如果输入后不正确，则需要查阅相应的产品说明书。此时在计算机上打开的 Web 页面一般会与图 3.10 所示的界面基本类似。

1）配置外网端口的 IP 地址参数

图 3.10 中所示的页面是默认的 Setup 选项卡界面，此页面用于设置无线路由器连接外网的端口 IP 参数。由于网络拓扑结构中，无线路由器连接的网关为 211.85.5.254/24（如图 3.8 所示），因此在图 3.10 中需要选择 Internet Connection Type 列表中的 Static IP 选项，并在其下的选项中依次输入 IP 地址为 211.85.5.100、子网掩码为 255.255.255.0、默认网关为 211.85.5.254、DNS 为 211.85.1.1。这些参数在不同的网络拓扑设计中，肯定会有所不同，无线路由器的 WAN 端口参数必须与其外连的网络 IP 规划保持一致。

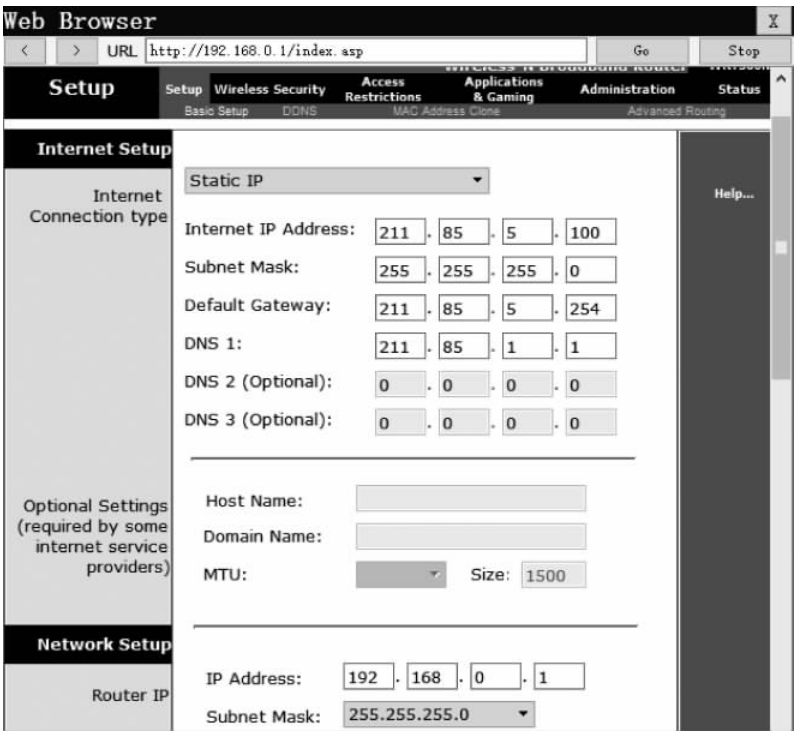

图 3.10　配置无线路由器的 Web 页面

2）配置内网的网关地址参数

无线路由器通过 LAN 端口及无线连接的计算机形成了一个小型的 LAN 环境，这个 LAN 必须配置一个网关参数才能使 LAN 中的 PC(无论是 PC1 还是 PC2)能够与其他网络通信。

图 3.10 所示界面下方的 Router IP 区域就是配置 LAN 网关参数的位置，PT 模拟软件使用的默认参数为 192.168.0.1/24，即当前内网的网关为 192.168.0.1/24；如果需要修改默认的网关参数，可以直接在此区域输入新的 IP 地址及子网掩码参数。这个操作不是必需的操作步骤，这里可以不进行修改。

3）配置无线参数

完成内外网参数配置后，就可以接着配置无线参数，其配置界面对应图 3.10 中的 Wireless 选项卡。打开此选项卡后，将出现如图 3.11 所示的界面。在图 3.11 所示的 Basic Wireless Settings 界面中，选择 Network Mode 列表中的 Wireless-N only 选项，在 SSID 文本栏中输入“jkx”。最后单击页面下方的 Save Settings 按钮保存以上参数。在图 3.11 所示界面中单击 Wireless 选项卡下的 Wireless Security 项，可以打开 Wireless Security 配置界面，如图 3.12 所示。

在图 3.12 中首先选择 Security Mode 列表中的 WPA2 Personal 选项，Encryption 列表中选择 AES 选项，然后在 Passphrase 文本栏中输入无线密码串“jkx12345”，最后单击界面下方的 Save Settings 按钮保存以上参数。此时无线路由器的基本配置已经完成，其他参数如 MAC 地址过滤、防火墙等，本节不做介绍。

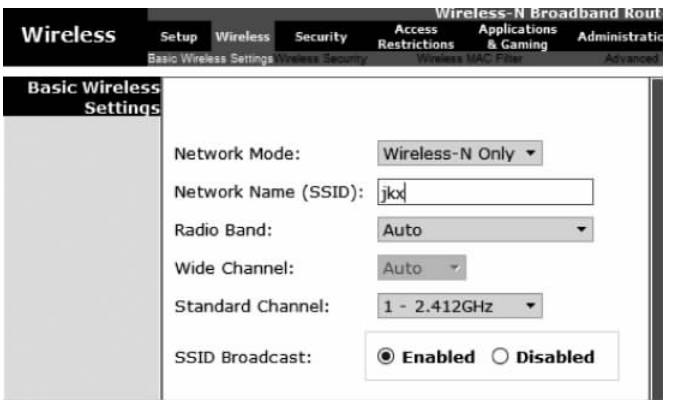

图 3.11　无线参数设置界面

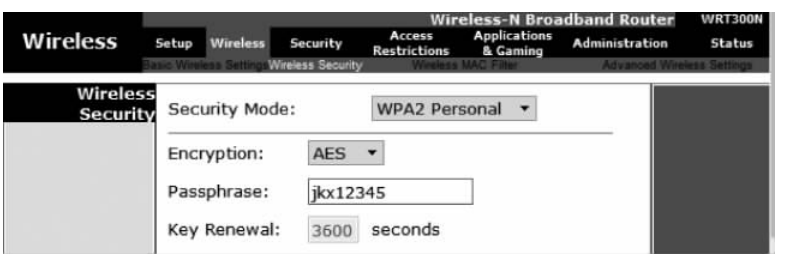

图 3.12　无线安全参数设置界面

3. 重新配置无线客户端

此时仔细观察网络拓扑图中的 PC2，会发现 PC2 与无线路由器的无线连接已经消失。其原因与上一节中出现的现象是一样的，因为无线路由器在上一步操作中已经使用了新的安全参数及密钥，无线客户端没有这些参数将不能连接到无线路由器。因此在完成无线路由器的参数修改后，需要重新配置无线客户端 PC2 的参数，以便让其可以再次连接到无线路由器。需要注意的是有线客户端 PC1 不需要重新配置任何参数，因为上一步中所修改的只是有关无线的参数，对于通过 LAN 端口连接的有线计算机而言是没有任何影响的。无线客户端 PC2 的配置过程与 3.4.1 节中的第 3 步完全一样，这里就不再重复介绍其操作步骤了。