重点大学信息安全专业规划系列教材

无线网络攻防教程

易平 主编

清华大学出版社

重点大学信息安全专业规划系列教材

无线网络攻防教程

易平 主编

清华大学出版社
北京

内 容 简 介

本书是清华大学出版社出版的《无线网络攻防原理与实践》一书配套的实验教程，围绕着无线网络安全攻防技术设置了五十多个实验，主要内容包括 WiFi 无线网络基础实验、WiFi 无线网络攻防实战、无线自组织网络安全攻防与仿真、无线自组织网络硬件攻防实验等。实验内容有基础实验、基本攻防实验和综合攻防实验，内容由浅入深、循序渐进。

本书引入了大量 WiFi 无线网络攻防实验；设计了大量的 NS2 的仿真实验，并且引入了新一代仿真工具 NS3，设计了在 NS3 环境下的仿真实验；不仅设计攻防的网络仿真实验，而且专门设计了硬件平台攻防实验，在嵌入式开发平台上进行设计开发，更有助于锻炼提高网络攻防的实践能力。

本书融合了多个全国大学生创新项目的成果，可作为无线通信、网络安全的创新实验课程与创新实验项目的指导教材，也可作为通信与信息系统、电子与信息工程、计算机应用、计算机网络等相关专业的大学本科和研究生教材，还可作为相关专业的应用开发人员和工程技术人员参考书。

图书在版编目(CIP)数据

无线网络攻防教程/易平主编. --北京：清华大学出版社，2015
重点大学信息安全专业规划系列教材
ISBN 978-7-302-39456-3

Ⅰ. ①无… Ⅱ. ①易… Ⅲ. ①无线网－安全技术－高等学校－教材 Ⅳ. ①TN92

中国版本图书馆 CIP 数据核字(2015)第 036557 号

责任编辑：魏江江　赵晓宁
封面设计：常雪影
责任校对：焦丽丽
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954

印 刷 者：北京市人民文学印刷厂
装 订 者：三河市溧源装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　印　　张：21.5　　字　　数：521 千字
版　　次：2015 年 11 月第 1 版　　印　　次：2015 年 11 月第1 次印刷
印　　数：1～2000
定　　价：39.50 元

产品编号：058332-01

前言

FOREWORD

无线网络已经得到广泛应用，无线网络安全技术也在迅速发展，许多大学已经开设了有关无线网络及其安全技术的课程。但是，“无线网络安全”不仅是一门理论教学课程，更是一门实践性很强的课程，仅仅在理论上讲授一些原理方法已经不能满足教学和实践的需求。笔者在长期教学和研究工作积累的基础上，精心编写了本书，让读者能够分享我们教学与研究工作的经验和成果。

本书可与《无线网络攻防原理与实践》(清华大学出版社出版，ISBN 978-7-302-25477-5)配套使用，《无线网络攻防原理与实践》详细地讲述了无线安全理论与攻防技术，非常适用于课堂教学。本书是上述理论教材讲授以后的具体实验教程，不仅可以使初学者能够了解无线网络安全原理和技术，而且还可通过循序渐进的实验过程掌握无线网络前沿的攻防技术。

本书有三大特点：

(1) 实践性强。按照不同的层次，实验的难度循序渐进，复杂度依次增加。完成基本无线网络的攻击实验、综合实验、自主创新实验，形成逐步提高的实验过程，由易到难，引导学生理解并熟悉无线网络架构、路由协议、安全机制，提高学生的动手能力。

(2) 软件仿真与硬件平台实验结合。不仅设计了大量的NS2仿真实验，而且引入了新一代仿真工具NS3，设计了在NS3环境下的仿真实验。不仅进行攻防的网络仿真实验，而且专门设计了硬件平台攻防实验，在嵌入式开发平台上进行设计开发，更有助于提高网络攻防的实践能力。

(3) 融合最新科研成果。本书融合了多年来的研究成果，包括自然科学基金重点项目“无线自组织网络安全特性基础理论研究”和863计划“无线自组网实时入侵检测和主动防护机制研究”、“无线网状网络WMN安全关键技术研究”等多个项目，一些实验案例直接取自于国家大学生创新实验项目，其中包括“移动自组织网络安全模块设计与实现”、“基于NS2无线Mesh网络仿真实验床的设计与实现”等项目。其中许多无线网络攻防技术，包括泛洪攻击、黑洞攻击、虫洞攻击、移动防火墙等一些原先只是在理论界探讨的前沿研究成果，已经由本书设计成可行的实验案例，直接进行具体实验操作，可以进一步掌握无线攻防的前沿技术。

本书共4章，第1章介绍WiFi无线网络基础实验，主要让读者熟悉掌握无线路由器的基本配置、组网和安全设置，设计了14个相关实验。1.1节为WiFi无线路由配置实验，包括AP模式(接入点模式)、Router模式(无线路由模式)、Repeater模式(中继模式)、Bridge模式(网桥模式)4个无线路由器设置实验，让读者掌握无线路由器的基本设置方法。1.2节

为 WiFi 组网两个实验，主要练习计算机如何进行 Ad Hoc 组网。1.3 节为 WiFi 安全 8 个实验，包括 WPA-PSK/WPA2-PSK 安全配置、WPA/WPA2 Radius 安全认证等，主要掌握 WiFi 无线网络安全配置。

第 2 章介绍 WiFi 无线网络攻防实战，主要练习针对 WiFi 无线网络安全机制的攻击方法，设计了 15 个攻防实验。2.1 节为 WEP 攻防基础，学习了解 WEP 基本原理。2.2 节为 WPA-PSK 攻防实战，了解无线 WPA/WPA2 安全原理和传统无线 WPA 破解方法。2.3 节为使用 WPA hash Tables(彩虹表)破解 WPA、WPA2 实战。2.4 节为伪装 AP 攻击实战，掌握使用 Gerix 实现无线伪装的方法。2.5 节为无线 DoS 攻击实战，练习 Auth Flood 攻击、De-auth Flood 攻击、De-associate Flood 攻击等多种无线 DoS 攻击。2.7 节 WEP 注入攻击。2.6 节 WEP 高级攻击包括 chop chop 攻击和 fragmentation 攻击。

第 3 章介绍无线自组织网络安全攻防与仿真，主要练习基于无线自组织网络的安全攻防技术，分为 NS2 仿真实验和 NS3 仿真实验，共设计了 21 个安全攻防实验。3.1 节为 NS2 仿真基础实验，练习 NS2 安装并掌握 NS2 环境变量的设置。3.2 节为 NS2 仿真综合实验，包括移植实现 MFlood 协议、添加 mac 协议、AODV 协议的仿真。3.3 节为 NS2 仿真攻击专项实验，包括黑洞攻击、泛洪攻击、虫洞攻击和信道抢占攻击。3.4 节为 NS2 仿真攻击检测实验，包括黑洞攻击检测和泛洪攻击检测实验。3.5 节为 NS2 仿真攻击检测防御综合实验，练习掌握移动防火墙入侵响应策略的原理与实现方法。3.6 节 NS3 仿真基础实验，设计了 4 个基础配置实验来熟悉掌握 NS3 的仿真实验方法。3.7 节 NS3 仿真综合实验，设计了 4 个不同类型网络的实验，让读者熟悉无线城域网、无线自组织网络、无线 MESH 网络、无线传感器网络的网络协议运行机制。

第 4 章为无线自组织网络攻防硬件平台实验，主要在硬件平台上练习无线网络攻防，设计了 10 个攻防实验。4.1 节基础实验，包括硬件实验平台搭建和多跳网络流量测试 2 个实验，让读者熟悉硬件平台的搭建与配置。4.2 节攻防基础实验，包括黑洞攻击实验、黑洞检测实验、泛洪攻击实验、泛洪检测实验等 4 个硬件平台攻防实验，让读者练习在真实环境下的攻防技术。4.3 节攻防综合实验，包括黑洞检测与防御实验和泛洪检测与防御实验，体验无线网络的攻防效果。

李文超、俞敏杰、安思华等同学参与了本书的案例设计。本书在编写过程中得到上海交通大学信息安全工程学院有关专家教授的关心与支持，在此向他们表示衷心的感谢。

作者衷心感谢清华大学出版社的大力支持，尤其感谢本书的编辑为本书付出的辛勤劳动和汗水。

无线网络涉及领域宽，内容多，发展快，本书的取材有些为学术界和工程技术界的研究成果，也包括笔者的一些成果和观点。相关研究成果属于原作者，在书中均作了引用标识。我们尽量以客观的态度对待任何一项研究方法和成果，对于其中的争议甚至错误，希望留待读者进一步甄别与探究。本教程实验案例较多，为保证每个实验的完整性，部分实验内容会有交叉和重复。尽管我们力求完美，但由于水平有限，疏漏、不当与错误之处在所难免，欢迎读者批评指正。

本书得到国家自然科学基金重点项目“无线自组织网络安全特性研究”(No. 60932003)；国家高计划研究发展计划 863 资助项目“无线自组网实时入侵检测与主动防护机制研究”(2007AA01Z452)；上海市自然科学基金资助项目“无线 MESH 网络主动安全防

护模型研究”(09ZR1414900)等项目的资助。

《无线网络攻防原理与实践》由清华大学出版社出版，同时我们也开发了与本书配套的“无线网络攻防实验系统”，可供读者使用，笔者邮箱为 yiping@sjtu.edu.cn。

易 平
于上海交通大学
2015 年 11 月

目 录

CONTENTS

第 1 章　WiFi 无线网络基础实验

1.1　WiFi 无线路由配置实验

1.1.1　AP 模式(接入点模式)

【实验目的】

了解 AP 模式及其配置以及与其他模式的异同。

【实验原理】

无线接入点(Access-Point,AP)的作用是接入有线网络后把有线信号转为无线网络,计算机通过接收它发射的信号接入无线 WiFi 局域网。这一点类似交换机或无线集线器。

目前大多数无线 AP 支持多用户(30～100 台计算机)接入、数据加密、多速率发送。在家庭或办公室,一个无线 AP 便可实现所有计算机的无线接入。无线 AP 主要用于家庭 ADSL 宽带、企业内部网络。目前无线 AP 技术主要为 802.11x 系列,覆盖距离为几十米至上百米,最高可达 300m。无线 AP 一般带有接入点客户端模式,也就是说 AP 之间可以进行无线链接,从而扩大无线网络的覆盖范围。

无线 AP 的工作原理是网络信号通过双绞线传送过来,无线 AP 对信号进行编译,将电信号转换成为无线信号发送,形成无线信号的覆盖。它相当于无线交换机,仅提供无线信号发射的功能。

【实验过程】

(1) 登录路由器,如图 1-1 所示。

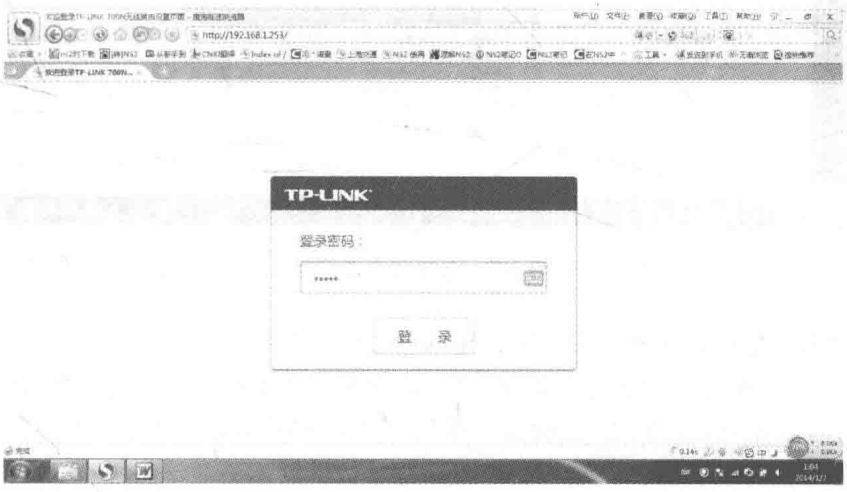

图 1-1　登录界面

(2) 单击“工作模式”,单击 AP 单选按钮,如图 1-2 所示。

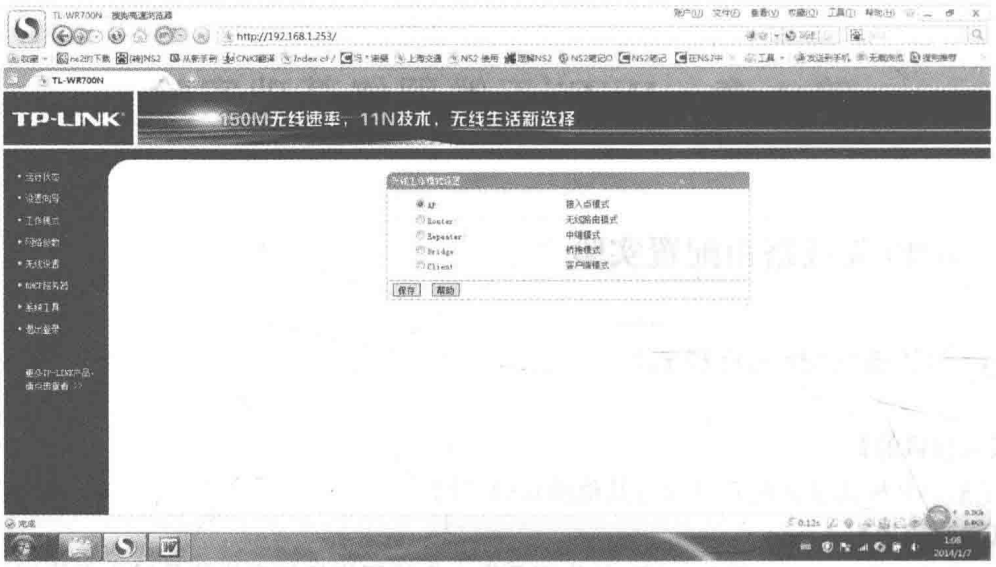

图 1-2 选择接入点模式

单击“保存”按钮,重新登录路由器会发现路由器已经工作在 AP 模式了,如图 1-3 所示。

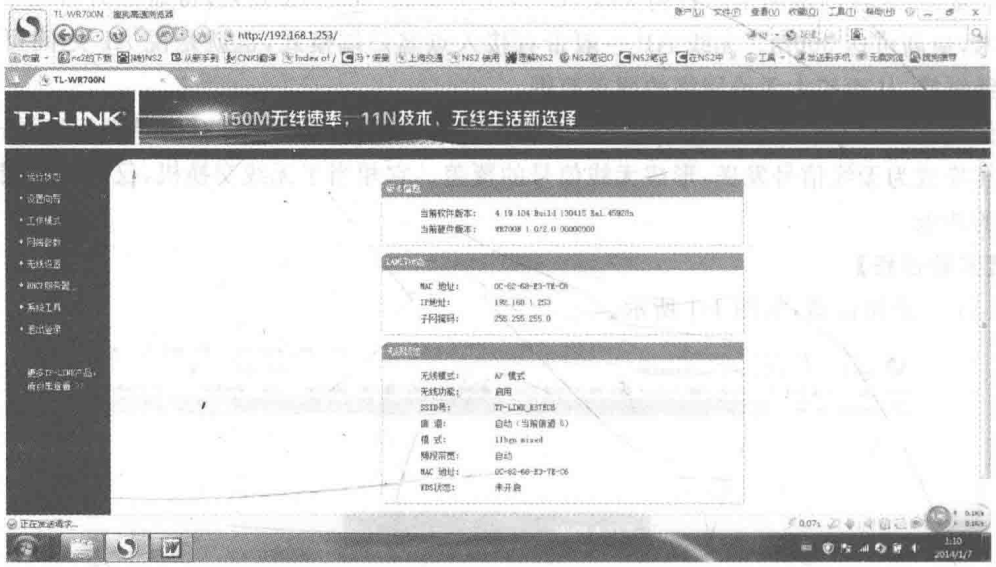

图 1-3 无线路由器信息

- SSID 号:标识无线网络的网络名称,最大支持 32 个字符。
- 信道:用于确定本网络工作的频率段,选择范围为 1～13。如果选择“自动”,设备将根据当前各个频段的信号强度,选择干扰较小的频率段,如图 1-4 所示。
- 模式:选择路由器的工作模式,推荐保持默认设置。
- 频段带宽:选择要使用的频段带宽,推荐保持默认设置。

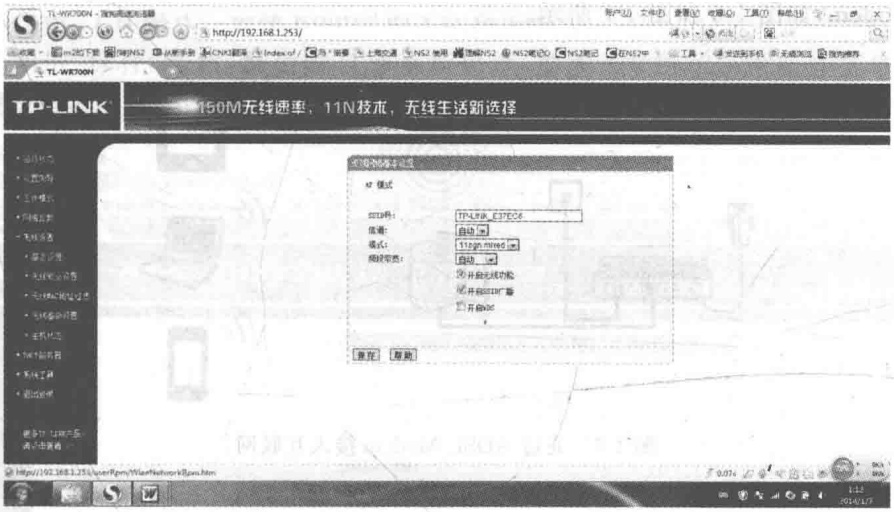

图 1-4　选择工作频率

- 开启无线功能：若要启用路由器的无线功能，请选中此项。
- 开启 SSID 广播：开启后无线工作站点将可以通过搜索无线 SSID 来发现本路由器，如图 1-5 所示。

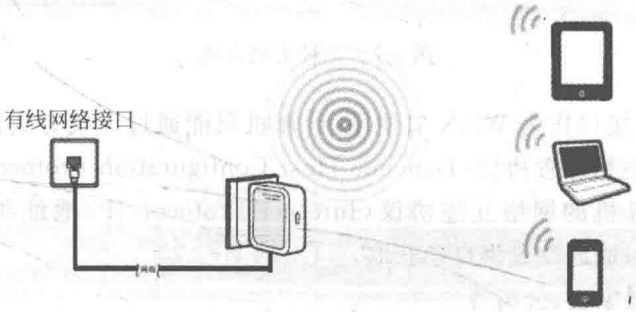

图 1-5　发现 SSID

- 开启 WDS：选择开启 WDS 功能，可以桥接多个无线局域网。注意，如果开启了这个功能，请确保信息输入正确。

【实验结果】

配置 AP 模式，理解该模式工作原理。

1.1.2　Router 模式（无线路由模式）

【实验目的】

了解 Router 模式及其配置以及与其他模式的异同。

【实验原理】

在路由模式下，是一台无线路由器，其有线接口是作为广域网（Wide Area Network，WAN）口使用，可以用网线通过 PPPoE（Point to Point over Ethernet）拨号的方式连接到

ADSL Modem，如图 1-6 和图 1-7 所示。

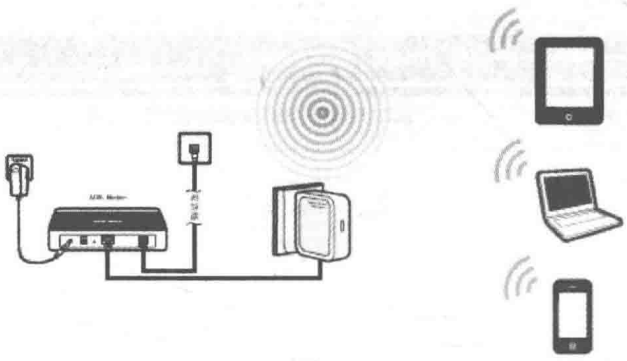

图 1-6　通过 ADSL Modem 接入互联网

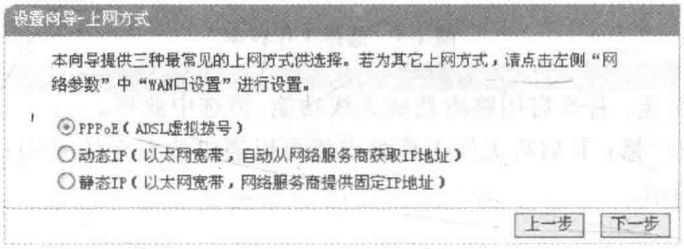

图 1-7　三种上网方式

本模式下，有线接口作为 WAN 口使用，计算机只能通过无线方式连接到无线路由器，无线路由器的动态主机配置协议（Dynamic Host Configuration Protocol，DHCP）服务器默认开启，建议将计算机的网络互连协议（Internet Protocol，IP）地址和域名服务（Domain Name Service，DNS）地址设置为自动获取。

适用环境：普通家庭、公寓等。

【实验过程】

(1) 登录路由器，如图 1-8 所示。

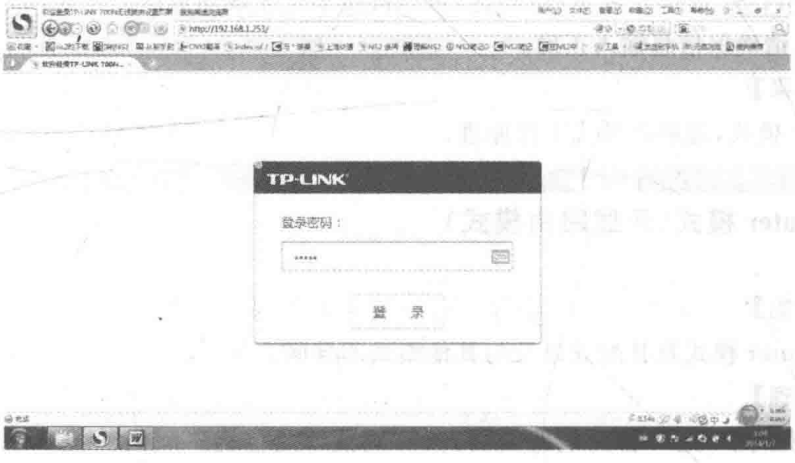

图 1-8　登录界面

(2) 单击“工作模式”,选择 Router 即无线路由模式。

(3) 单击“保存”按钮,路由器自动重新启动,如图 1-9 所示。重新连接该路由器的 SSID,登录路由器,路由器则已经工作在 Router 模式了,如图 1-10 所示。

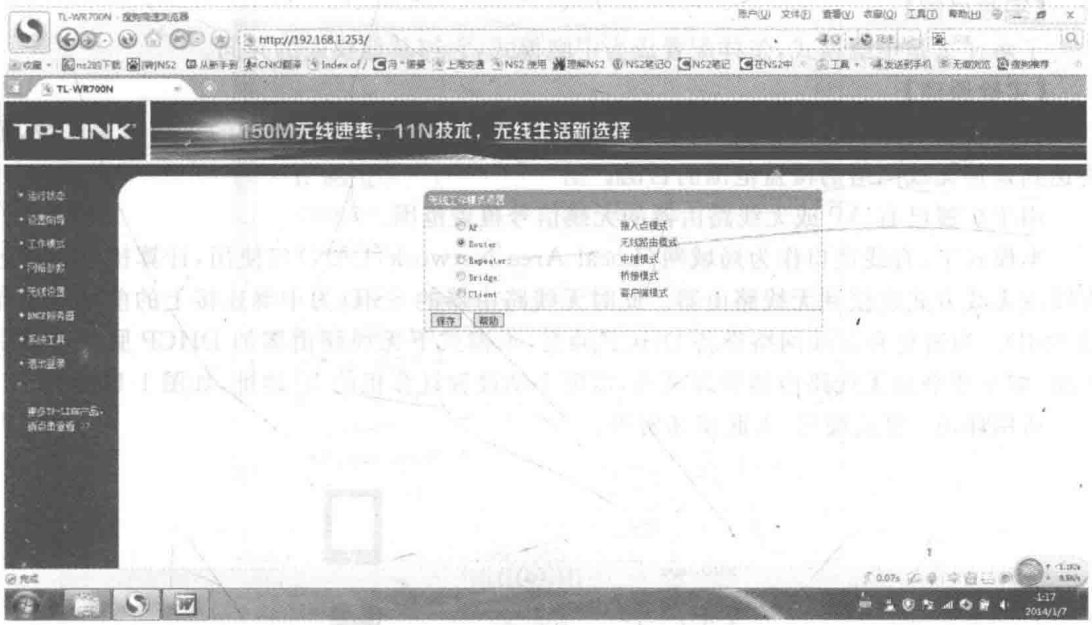

图 1-9 选择无线路由模式

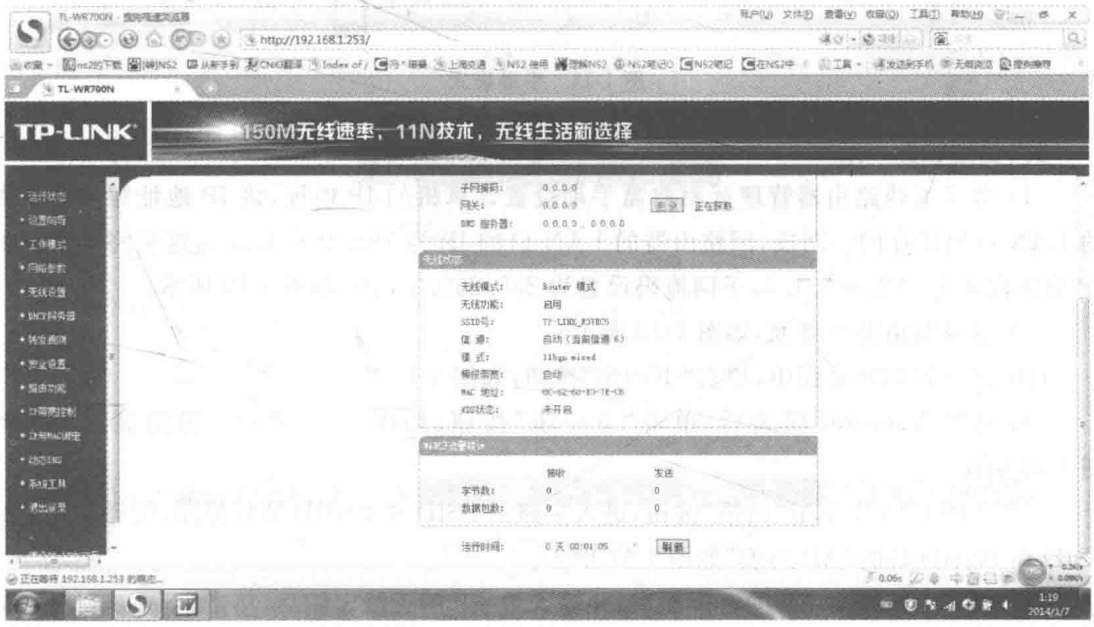

图 1-10 设置后的信息

【实验结果】

配置 Router 模式,理解该模式工作原理。

1.1.3 Repeater 模式(中继模式)

【实验目的】

了解什么是中继模式,怎样配置成为中继模式,它与其他模式的异同。

【实验原理】

利用设备的无线接力功能,实现无线信号的中继和放大,并形成新的无线覆盖区域,最终达到延伸无线网络的覆盖范围的目的。

用于扩展已有 AP 或无线路由器的无线信号覆盖范围。

本模式下,有线接口作为局域网(Local Area Network,LAN)口使用,计算机可以通过有线或无线方式连接到无线路由器。此时无线路由器的 SSID 为中继连接上的前端路由器的 SSID。为避免和前端网络设备 DHCP 冲突,本模式下无线路由器的 DHCP 服务器默认关闭,如果要登录无线路由器管理页面,需要手动设置计算机的 IP 地址,如图 1-11 所示。

适用环境:复式楼房、大面积场所等。

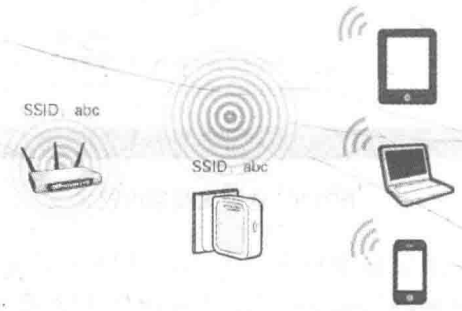

图 1-11 中继模式

【实验过程】

(1) 登录无线路由器管理页面前需手动设置计算机的 IP 地址,该 IP 地址需与路由器的 LAN 口地址在同一网段,因路由器的 LAN 口的 IP 为 192.168.1.253,这里将计算机的 IP 地址设置为 192.168.1.5,子网掩码设置为 255.255.255.0,如图 1-12 所示。

(2) 登录路由器主界面,如图 1-13 所示。

(3) 在设置向导页面中,单击“下一步”按钮,如图 1-14 所示。

(4) 选择 Repeater 模式后,单击“下一步”按钮,如图 1-15 所示。得到显示结果如图 1-16 所示。

(5) 在图 1-16 中单击“扫描”按钮,进入主路由 SSID 和 BSSID 选择界面,选择主路由的 SSID 和 BSSID 后的“AP 列表”如图 1-17 所示。

(6) 在下方选择主 AP 的密钥类型,并输入主 AP 的无线密钥后,单击“下一步”按钮,如图 1-18 所示。

(7) 单击“重启”按钮,路由器自动重启,如图 1-19 所示。

(8) 在计算机的“无线网络连接”属性中,选择“自动获得 IP 地址”单选按钮,如图 1-20 所示。

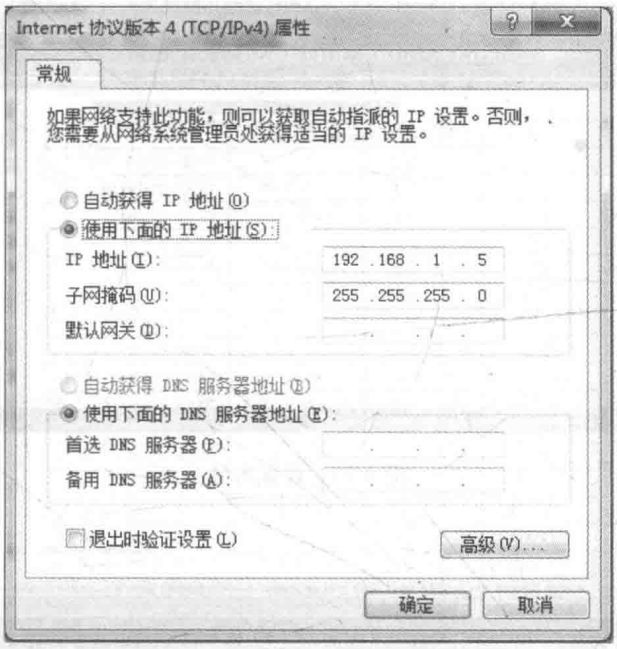

图 1-12 设置 IP 地址

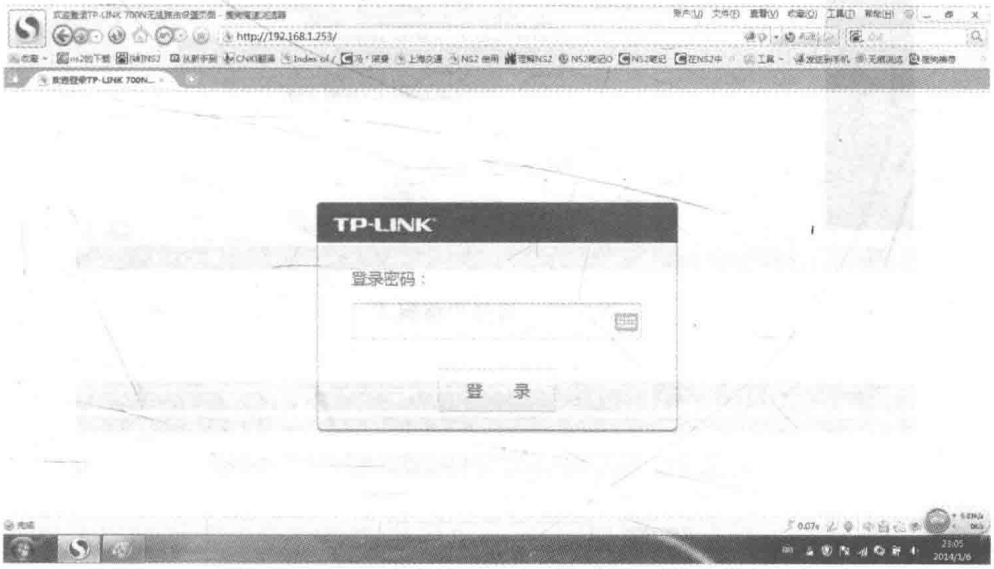

图 1-13 登录界面

(9) 可以看到中继后，附路由的 SSID 信息变成主路由的 SSID 信息了。

【实验结果】

配置 Repeater 模式，理解该模式工作原理。

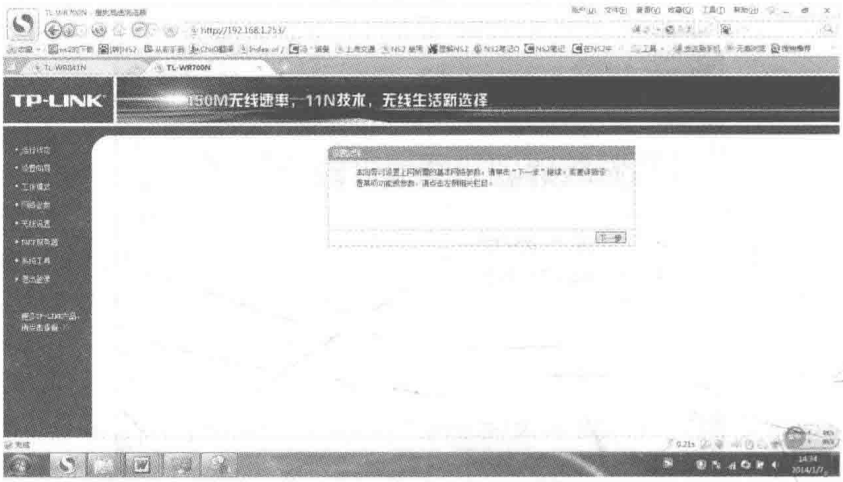

图 1-14　设置向导

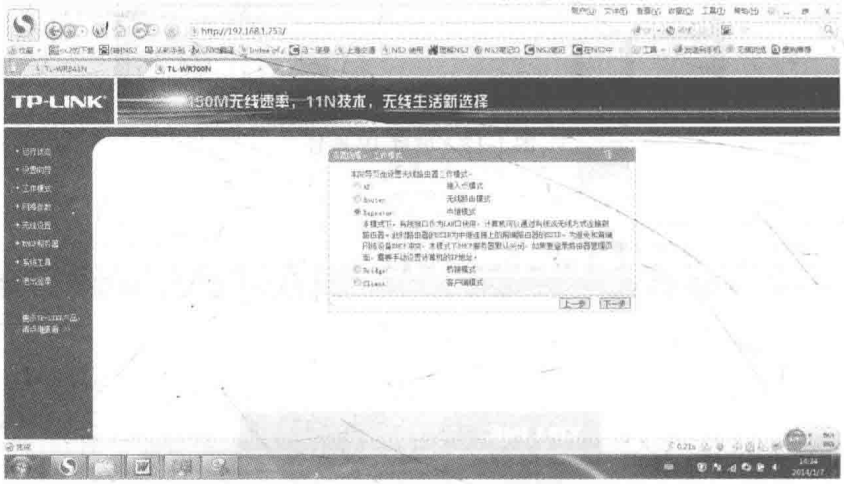

图 1-15　选择中继模式

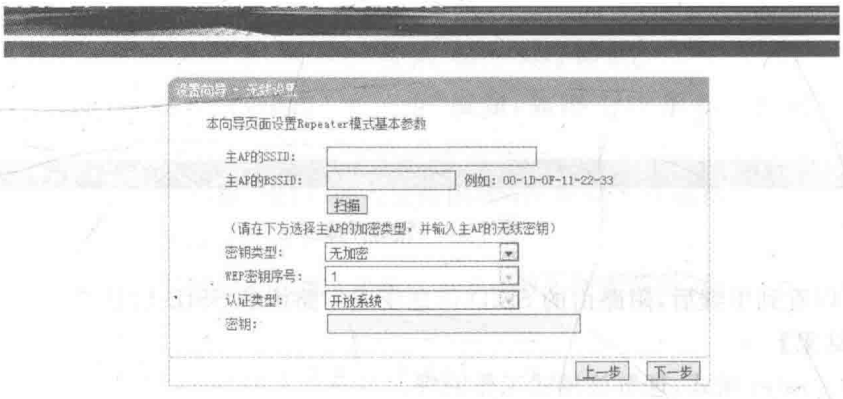

图 1-16　Repeater 模式