

# 《无线局域网技术项目教程》

## 图书基本信息

书名：《无线局域网技术项目教程》

13位ISBN编号：9787894360755

10位ISBN编号：7894360759

出版时间：2012-7

出版社：东软电子出版社

作者：胡云 编

页数：237

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：[www.tushu000.com](http://www.tushu000.com)

# 《无线局域网技术项目教程》

## 内容概要

《教育部高等学校高职高专计算机类专业教学指导委员会规划教材:无线局域网技术项目教程》以组建无线局域网的实例为主线,介绍了无线局域网的基本原理、协议标准、技术规范、通信传输、组网拓扑、设备功能、设备类型、工程安装、网络配置、监控优化、网络安全、网络规划、行业应用、故障排除等关键技术。《教育部高等学校高职高专计算机类专业教学指导委员会规划教材:无线局域网技术项目教程》注重分析无线网络与有线网络的关系,理解计算机网络架构的拓展,使读者更全面完整地认识计算机网络。

## 书籍目录

### 第1章无线网络概述1

#### 学习目标1

#### 1.1无线网络的起源与演进2

#### 1.2无线网络的优势2

#### 1.3无线网络的分类3

##### 1.3.1无线广域网3

##### 1.3.2无线城域网4

##### 1.3.3无线局域网6

##### 1.3.4无线个域网6

#### 思考与操作12

### 第2章SOHO无线局域网组建15

#### 项目情境描述15

#### 学习目标17

#### 专业知识17

#### 2.1WLAN技术概述17

##### 2.1.1WLAN的定义17

##### 2.1.2WLAN的特点18

##### 2.1.3WLAN的局限性18

##### 2.1.4WLAN与有线局域网的比较19

#### 2.2无线电频谱19

##### 2.2.1无线电管理部门20

##### 2.2.2无线电频段的划分21

##### 2.3802.11 协议标准24

##### 2.3.1802.11 系列标准24

##### 2.3.2802.11的逻辑结构25

##### 2.3.3802.11 b/g/a/n协议标准32

#### 2.4WLAN的组成36

##### 2.4.1STA36

##### 2.4.2无线网卡37

##### 2.4.3无线路由器38

##### 2.4.4分布式系统39

#### 2.5WLAN拓扑结构39

##### 2.5.1Ad-hoc模式39

##### 2.5.2Infrastructure模式40

##### 2.5.3无线分布式系统41

#### 工作任务43

##### 任务1:构建对等结构无线局域网43

##### 任务2:构建基础结构无线局域网54

##### 任务3:构建WDS无线局域网65

#### 思考与操作69

### 第3章中型企业无线局域网组建72

#### 项目情境描述72

#### 目录学习目标73

#### 专业知识73

#### 3.1无线局域网射频（RF）73

##### 3.1.1RF通信基础73

##### 3.1.2微波传播路径75

- 3.1.3RF信号强度与衰减78
- 3.2WLAN设备的天线79
  - 3.2.1天线的功能与类型79
  - 3.2.2天线的主要电气参数80
- 3.3WLAN的主要设备85
  - 3.3.1无线AP85
  - 3.3.2无线局域网控制器88
  - 3.3.3以太网供电 ( PoE ) 92
- 3.4无线局域网部署95
  - 3.4.1传统AP架构模式的WLAN95
  - 3.4.2基于WLC的集中型WLAN96
  - 3.4.3基于锐捷无线交换机的WLAN96
- 3.5CAPWAP协议98
  - 3.5.1CAPWAP协议的产生98
  - 3.5.2基于CAPWAP协议的WLAN构成98
  - 3.5.3CAPWAP协议的隧道传输99
  - 3.5.4MP的启动工作方式100
- 3.6无线局域网漫游102
  - 3.6.1无线漫游102
  - 3.6.2基于无线控制器架构的漫游103
- 3.7无线网桥104
- 3.8无线Mesh网络106
  - 3.8.1无线Mesh网络概念106
  - 3.8.2无线Mesh网络的接入点设备107
  - 3.8.3无线Mesh网络的结构与应用场景108
- 工作任务110
  - 任务1:构建中型企业分公司无线局域网110
  - 任务2:组建中型企业总部园区无线局域网120
  - 任务3:构建中型企业无线网络的漫游功能132
- 思考与操作139
- 第4章无线局域网安全管理143
  - 项目情境描述143
  - 学习目标143
  - 专业知识144
    - 4.1WLAN安全概述144
      - 4.1.1WLAN安全标准145
      - 4.1.2WLAN安全威胁分析146
      - 4.1.3WLAN加密和认证简介147
    - 4.2有线等效保密 ( WEP ) 148
    - 4.3Wi-Fi访问保护 ( WPA ) 149
    - 4.4802.11i标准150
      - 4.4.1802.11i的安全机制150
      - 4.4.2802.1x认证体系151
      - 4.4.3TKIP ( 临时密钥完整性协议 ) 153
      - 4.4.4CCMP153
    - 4.5WEB认证技术154
      - 4.5.1Web认证系统的组成154
      - 4.5.2Web认证的CHAP认证过程154
      - 4.5.3Web认证的PAP认证过程155

4.6WAPI技术	156
4.6.1产生WAPI的背景	156
4.6.2WAPI基本功能	157
4.7WLAN认证	159
4.7.1链路认证	159
4.7.2用户接入认证	160
4.8WLAN IDS	162
4.8.1WLAN IDS简介	162
4.8.2无线入侵检测系统架构	162
4.8.3检测Rogue设备	162
4.8.4检测IDS攻击	163
工作任务	165
任务1：组建企业基本无线局域网	165
任务2:使用WEP加密保护客户中心信息	172
任务3:使用WPA加密保护运行维护中心信息	175
任务4:使用WEB加密保护销售中心信息	178
任务5:利用802.1x+RADIUS保护技术中心信息	182
任务6:无线网络的MAC认证	189
任务7:禁用无线网络的广播功能	194
任务8:开启无线网络的二层隔离功能	196
思考与操作	197
第5章无线局域网工程规划及维护	201
项目情境描述	201
学习目标	203
专业知识	203
5.1WLAN设计目标	203
5.2WLAN现场工勘	204
5.2.1WLAN工勘的准备工作	204
5.2.2WLAN工勘需要记录的信息	206
5.2.3WLAN工勘的具体过程	207
5.3WLAN覆盖设计	209
5.3.1覆盖设计原则	209
5.3.2WLAN拓扑结构选择	209
5.3.3频率规划	210
5.3.4覆盖规划	210
5.3.5链路预算	212
5.3.6容量规划	213
5.3.7WLAN覆盖设计举例	214
5.4WLAN网络规划	214
5.5WLAN项目方案的编写	215
5.6WLAN设备安装	217
5.7WLAN网络验收	217
5.7.1设备安装测试	218
5.7.2网络功能测试	218
5.7.3信号强度测试	219
5.7.4传输性能测试	221
5.8WLAN的维护	224
5.8.1WLAN设备的维护	225
5.8.2WLAN常见故障排除	227

5.8.3 WLAN典型故障排除案例分析229

工作任务231

任务1:编写瑞达电子科技有限公司WLAN覆盖项目书231

任务2:瑞达电子科技有限公司WLAN覆盖项目实施231

思考与操作235

参考文献237

版权页：插图：4.8.1 WLAN IDS简介 802.11网络很容易受到各种网络威胁的影响，如未经授权的AP用户、Ad-hoc网络、拒绝服务型攻击等。Rogue设备对于企业网络安全来说更是一个很严重的威胁。无线入侵检测系统（Wireless Intrusion Detection System，WIDS）可以对有恶意的用户攻击行为和入侵行为进行早期检测，保护企业网络和用户不被无线网络上未经授权的设备访问。WIDS可以在不影响网络性能的情况下对无线网络进行监测，从而提供对各种攻击的实时防范。WLAN IDS涉及的常用术语：（1）Rogue AP：网络中未经授权或者有恶意的AP，它可以是私自接入到网络中的AP、未配置的AP、邻居AP或者攻击者操作的AP。如果在这些AP上存在安全漏洞，黑客就有机会危害无线网络安全。（2）Rogue Client：非法客户端，网络中未经授权或者有恶意的客户端，类似于Rogue AP。（3）Rogue Wireless Bridge：非法无线网桥，网络中未经授权或者有恶意的网桥。（4）Monitor AP：这种AP在无线网络中通过扫描或监听无线介质，检测无线网络中的Rogue设备。一个AP可以同时作为接入AP和Monitor AP，也可以只作为Monitor AP。（5）Ad-hoc mode：把无线客户端的工作模式设置为Ad-hoc模式，Ad-hoc终端可以不需要任何设备支持而直接进行通讯。

### 4.8.2无线入侵检测系统架构

无线入侵检测系统有集中式和分散式两种。集中式无线入侵检测系统通常用于连接单独的Sensors（探测器，俗称探头），搜集数据并转发到存储和处理数据的中央系统中。分散式无线入侵检测系统通常包括多种设备来完成IDS的处理和报告。分散式无线入侵检测系统比较适合较小规模的无线局域网，因为它价格便宜且易于管理。当过多的Sensors需要检测时，Sensors的数据处理将被禁用。所以，多线程处理和报告的Sensors管理比集中式无线入侵检测系统花费更多的时间。无线局域网通常被配置在一个相对大的场所。为了更好的接收信号，需要配置多个无线基站（WAPS），在无线基站的位置上部署Sensors，会提高信号的覆盖范围。这种物理架构能够检测到大多数的黑客行为，并且加强了同无线基站（WAPS）的距离，从而能更好地定位黑客的详细地理位置。

### 4.8.3检测Rogue设备

一般可以把网络中的设备分为两种类型：非法设备（Rogue设备）和合法设备。Rogue设备可能存在安全漏洞或被攻击者操纵，因此会对用户网络的安全造成严重威胁或危害。

# 《无线局域网技术项目教程》

## 精彩短评

- 1、还行，不是特别符合要求
- 2、大概看了一下内容，内容很丰富，很实在，实用性强，值得收藏



# 《无线局域网技术项目教程》

## 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:[www.tushu000.com](http://www.tushu000.com)