cwnp Official Study Guide

Certified Wireless Network Professional

Exam PW0-105

CWNA 官方学习指南（第3版）：认证无线网络管理员PW0-105

CWNA: Certified Wireless Network Administrator Official Study Guide: Exam PW0-105, Third Edition

[美] David D. Coleman (CWNE #4) 著
David A. Westcott (CWNE #7)
朱志立 (CWNE #134) 译
蒋楠

包含真实场景，提供动手练习和前沿备考软件：

- 自定义考试引擎
- 考试习题
- 350多张电子抽认卡
- 术语表
- 白皮书、视频和演示软件等

SYBEX SERIOUS SKILLS

清华大学出版社

提供各种书籍pdf下载，如有需要，请联系 QQ: 461573687

PDF制作说明:

本人可以提供各种PDF电子书资料，计算机类，文学，艺术，设计，医学，理学，经济，金融，等等。质量都很清晰，而且每本100%都带书签和目录，方便读者阅读观看，只要您提供给我书的相关信息，一般我都能找到，如果您有需求，请联系我 **QQ: 461573687**, 或者 **QQ: 2404062482**。

本人已经帮助了上万人找到了他们需要的PDF，其实网上有很多PDF,大家如果在网上不到的话，可以联系我QQ。因PDF电子书都有版权，请不要随意传播，最近pdf也越来越难做了，希望大家尊重下个人劳动，谢谢！

备用QQ:2404062482

PW0-105考试官方学习指南

《CWNA官方学习指南(第3版)：认证无线网络管理员PW0-105》是供你备考PW0-105 CWNA认证考试的最新版书籍。本书内容全面，涵盖备考需要掌握的全部内容，包括射频基础知识、射频组件、无线LAN拓扑、无线接入、入侵监控、无线攻击、故障排除以及其他许多重要主题和概念。

主要内容

- 全面系统讲述所有考试目标，助你自信备考
- 实用的“动手练习”帮你巩固关键技能
- “真实场景”将你所学的理论知识运用于实际工作中
- 每章末尾的“复习题”颇具挑战性，可用于为考试热身
- 每章的“考试要点”列出考前必须熟练掌握的要点，这是本书的一个重要特色
- 本书提供的易撕考点卡详细列出所有官方考试目标，指出每个目标对应的章号，以便你对照每个目标跟踪备考情况

作者简介

David D. Coleman，CWNE #4、CWTS、CWNA、CWSP、CWNT，担任Aerohive网络公司的全球培训经理，曾撰写多本Wi-Fi技术图书和大量白皮书，也是微软和思科认证专家。Coleman是CWNE圆桌组织的成员之一(该组织由全球最知名无线专家组成)，曾参与撰写前两版CWNA学习指南。

David A. Westcott，CWNE #7、CWTS、CWNA、CWSP、CWNT。作为一名独立咨询师和技术培训师，Westcott拥有23年IT工作经验、15年以上认证讲师经验，是CWNE圆桌组织的成员之一，曾参与撰写前两版CWNA学习指南。

配套学习资源

www.sybex.com
www.sybex.com/go/cwna3e

Sybex备考工具

从www.sybex.com/go/cwna3e下载个套电子版工具，该工具可以帮助你全面备考，其中包含：

- 每章复习题
- 三套全真模拟考题
- 350多张电子抽认卡
- 术语表
- 附赠的PDF、白皮书和演示软件等

下载模拟题和章节复习题

用350多张电子抽认卡自测备考情况

ABOUT THE CWNP PROGRAM

CWNP is the industry standard for vendor-ne
enterprise WLAN certifications. The focus
educate IT professionals in the technology be
all enterprise WLAN products and to enable
professionals to manage wireless LAN enter
infrastructures, regardless of the vendor so
utilized. CWNP is a privately held corpor
based in Atlanta, Georgia. For more inform
visit www.cwnp.com.

ISBN 978-7-302-35276-1
9 787302 352761 >
定价：79.00元

清华大学出版社数字出版网站
WQBook 书文局泉
www.wqbook.com

Sybex®
An Imprint of
WILEY

CWNA 官方学习指南(第 3 版):
认证无线网络管理员 PW0-105

[美] David D. Coleman
David A. Westcott 著

朱志立 蒋楠 译

清华大学出版社

北 京

David D. Coleman，David A. Westcott
CWNA: Certified Wireless Network Administrator Official Study Guide: Exam PW0-105, Third Edition
EISBN：978-1-118-12779-7
Copyright © 2012 by John Wiley & Sons, Inc., Indianapolis, Indiana.
All Rights Reserved. This translation published under license.

本书中文简体字版由 Wiley Publishing, Inc. 授权清华大学出版社出版。未经出版者书面许可，不得以任何方式复制或抄袭本书内容。

北京市版权局著作权合同登记号 图字：01-2012-4747

Copies of this book sold without a Wiley sticker on the cover are unauthorized and illegal.

本书封面贴有 Wiley 公司防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

图书在版编目(CIP)数据

CWNA 官方学习指南(第 3 版)：认证无线网络管理员 PW0-105/(美)科尔曼(Coleman, D.D.)，(美)韦斯科特(Westcott, D.A.) 著；朱志立，蒋楠 译. —北京：清华大学出版社，2014

书名原文：CWNA: Certified Wireless Network Administrator Official Study Guide: Exam PW0-105, Third Edition

ISBN 978-7-302-35276-1

Ⅰ. ①C… Ⅱ. ①科… ②韦… ③朱… ④蒋… Ⅲ. ①计算机网络管理—指南 Ⅳ. ①TP393.07-62

中国版本图书馆 CIP 数据核字(2014)第 016340 号

责任编辑：王　军　韩宏志
装帧设计：牛静敏
责任校对：曹　阳
责任印制：杨　艳

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
印 刷 者：清华大学印刷厂
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　印　张：36　插　页：1　字　　数：857 千字
版　　次：2014 年 2 月第 1 版　　印　　次：2014 年 2 月第 1 次印刷
印　　数：1～4000
定　　价：79.00 元

产品编号：047995-01

译 者 序

您拿在手上这本书是很重要的、很特别的，我相信对你们的学习和工作也是很有价值的，它由两名美国无线网络技术权威所写，他们都是 CWNE，也都是 CWNP 体系圆桌会议成员，拥有多年的无线网络工作经验。

近年来全球的 WLAN 发展得非常迅速，这种情况当然也发生在中国，以至于很多公司和个人再也无法离开 Wi-Fi 所带来的便捷。但是在中国市场上，几乎没有涉及无线局域网基础理论和应用技术的优秀书籍和培训体系，设计部署无线局域网的专业人员也多凭估计或臆想，没有理论支撑。而 CWNP 是目前全球唯一中立的无线培训体系，成了 Wi-Fi 培训的事实标准。它与各大无线厂商的具体产品没有直接关系，非常适合掌握无线局域网的全局理论，也是很多知名无线企业(如 Aruba、Aerohive、Cisco、Fluke、Motorola 等)强烈推荐学习的课程。CWNA 是该体系中无线网络管理员级别的认证，涵盖的内容非常广泛，既适合有经验的无线网络技术人员，也适合初学者。

这本书的翻译，因翻译期间进行了改版，加上其他事务耽搁，前后历时两年，耗费了非常多的精力。在翻译过程中，结合自己多年的 WLAN 培训经验，力求还原原书宗旨，但因为国内对于无线术语尚无统一标准，可能会在阅读过程中产生混淆，这时请大家参考原始英文进行比对，这点提醒大家注意。

需要感谢我的家人对我的理解和支持，我的母亲张征芬、太太莎和儿子琢，这两年陪伴你们的时间确实太少了。

需要感谢本书的合作译者蒋楠，正是他前期与出版社的沟通让这本书的翻译成为现实，他翻译的前一版的几乎一半的章节译文质量很高，也为本版的顺利完成打下了良好的基础。

当然还要感谢我的老师 David Westcott，也就是这本书的合著者之一，是他在早期对我进行了无线网络的培训。他把两件事当成一生的爱好和工作，一个是直升机飞行，另一个就是无线网络，而这两个事件都有一个共同点，那就是自由，这也是我希望追求的。还要感谢 Neil Bhave，正是他让我走上了无线网络这条不归路，还要感谢思科中国公司的冯洪敏先生。感谢他们三位在我申请 CWNE 时做的背书。

还要感谢清华出版社，以及王军和韩宏志两位编辑，对他们对这本书翻译所花费的漫长时间展现出的耐心和理解表示感谢。

成为中国第一个 CWNE 的时候，CWNP 的 Julia Baldini 问我为什么对无线这么感兴趣，我总结了三个 F，就是有趣(funny)、未来(future)和自由(freedom)。当你进行无线分析的时候，这件事看似看不见摸不着，但经过对协议的理解，利用一些专用的工具可以把这些无形的东西转成有形的时候，你会觉得很有趣。当大家无论在工作还是生活中，离不开 Wi-Fi 的时候你会觉得，它应该很有前途和未来；当你不愿受到拘束，无论生活还是内心，你会发现无线有时能满足自由这个特征。我希望大家通过这本书也能够喜欢 Wi-Fi 技术，并把它当成爱好或者事业。

好了，下面就请大家就打开本书的第一页，开始成为无线网络真正的专业者吧。

朱志立

作 者 简 介

David D. Coleman 是 Aerohive 网络公司的全球培训经理，该公司是屡获殊荣的协作控制无线局域网架构的创立者，网址是 www.aerohive.com。Coleman 负责 Aerohive 合作伙伴和客户的培训事务，为来自全球各地的 IT 专业人员讲授无线网络管理、无线网络安全和无线帧分析课程。Coleman 著有多本无线网络领域的书籍和白皮书，他被认为是 802.11 技术领域的权威，是 CWNE #4。Coleman 平时居住在美国乔治亚州的亚特兰大。你可以通过电子邮件 mistermultipath@gmail.com 联系到他，Twitter 地址是 www.twitter.com/mistermultipath。

David Westcott 是具有 23 年以上 IT 经验的咨询师和培训师，他专注于无线网络和安全领域。Westcott 获取认证讲师的时间超过了 19 年，除了向企业客户提供咨询和指导外，还为世界各地的政府机构、公司和大学提供培训。Westcott 已经为 5 大洲和美国 40 多个州提供了培训。Westcott 担任波士顿大学企业教育中心兼职教员超过 10 年。Westcott 合著了 5 本有关无线网络的书籍并撰写了众多白皮书和最佳实践指南文档。他还为无线网络、无线 Mesh 网络、无线数据包分析、有线网络和网络安全制定了课件和培训视频。Westcott 从 1999 年就安装了第一个无线网络，目前是认证的无线网络培训师、管理员、安全专家和分析专家。他获得了 Cisco、Aruba、Microsoft、EC-Council、CompTIA 和 Novell 公司的认证。Westcott 平常住在美国马萨诸塞州的康科德城。Westcott 是 CWNE #7，可通过电子邮件 david@westcott-consulting.com 联系到他。

致　　谢

David Coleman：再次感谢我的孩子 Brantley 和 Carolina，感谢他们的耐心并理解我为整本书的写作工作，我非常爱你们。我还想感谢我的母亲 Marjorie Barnes 和我的继父 William Barnes 多年来给予的支持和鼓励。

David Westcott：要感谢我的父母 Kathy 和 George 给予的支持，我从你们身上学到了很多，我爱你们。我还要对 Janie、Jennifer 和 Samantha 的耐心、在人生道路上对我的指引以及在这本书的整个写作过程中给予的理解和支持表示感谢。

我们还要首先感谢 Sybex 的组稿编辑 Jeff Kellum 最初找到我们并一起完成这个工作。Jeff 极其耐心，并且一共发行了我们的 5 本书。还要感谢编辑 Tom Cirtin。还需要特别感谢编辑经理 Pete Gaughan、制作编辑 Christine O'Connor 和文字编辑 Liz Welch。我们还需要向技术编辑 Marcus Burton 大声说：你很棒，哥们！

我们还要特别感谢 Revolution Wi-Fi 的 Andrew vonNagy 对本书预览和反馈，特别感谢 CWNP 公司(www.cwnp.com)的 Socrates Sakellaropoulos、Abbey Cole 和 Kevin Sandlin。无论是以前的还是现在的所有 CWNP 员工都应该为创建了企业级 Wi-Fi 行业的教育标准的国际知名的无线认证品牌而感到荣幸。在过去 10 年里与你们一起工作非常愉快。

感谢 Proxim 公司和 Ken Ruppel (kenruppel@gmail.com)允许我们把“video Beam Patterns and Polarization of Directional Antennas”视频放到本书的在线资源网站上(访问地址：www.sybex.com/go/cwna3e)。

感谢 Andras Szilagyi 开发的 EMANIM 软件，并为本书的不同版本提供了定制支持。

还要感谢下列组织和个人对本书的支持和贡献：

Aerohive Networks (www.aerohive.com)的 Devin Akin 和 Paul Levasseur

Aruba Networks (www.arubanetworks.com)的 Carolyn Cutler、Susan Wells、Kevin Hamilton 和 Chris Leach

CACE Technologies (www.cacetech.com)的 Janice Spampinato

Metageek (www.metageek.com)的 Mark Jensen 和 Wendy Fox

WLAN Professionals (www.wlanpros.com)的 Keith Parsons

Welch Allyn (www.welchallyn.com)的 Jeffrey Walker

Wi-Fi Alliance (www.wi-fi.org)的 Trisha Campbell 和 Tom Sciorilli

序 言 一

亲爱的读者，感谢你们选择本书。本书是优秀的 Sybex 系列丛书中的一员，由实践经验和教学经验丰富的优秀作者撰写。

Sybex 创建于 1976 年。30 多年来，我们致力于出品优秀书籍，致力于努力工作以创立行业新标准。从我们打印的每张纸到和我们一起工作的作者，我们共同的目标就是带给你最好的书籍。

我希望你能明白所有反映在书籍每一页的内容，并且很有兴趣听取你的意见及反馈，以便指导我们今后的工作。如果对本书或其他 Sybex 书籍有任何意见，请给我发电子邮件，我的电子邮件是 nedde@wiley.com。如果在本书中发现任何技术性错误，请访问 http://sybex.custhelp.com。你的反馈对 Sybex 至关重要。

Sybex 副总裁兼发行人 Neil Edde

序 言 二

本书上一版的序言是 CWNP 的共同创办人 Devin Akin 撰写的。第一句话就是“无线局域网似乎无处不在”。Devin 是正确的，但是这本书的第二版于 2009 年 4 月出版以来，Wi-Fi 已经发生了极大的变化！当时的前言甚至都没有提到 802.11n，而 802.11ac 和 802.11ad 修正案的情况也根本无法预知。今天的 Wi-Fi 不是“似乎”无处不在，而是“真的”无处不在。有 Wi-Fi 的日子真好！

让我们看看还有什么在 2009 年初尚未出现。第一个是我们已经提到过的 802.11n，但它几乎就在那个时间点得到批准。当这项修正案刚成为议题时，它被冠以“草案”和“Pre-”等限定符。不久后，802.11n 修正案成为企业采纳 Wi-Fi 作为主流和关键网络通信技术的催化剂。如今 802.11n 已无处不在，如果你是一名网络专业人士，你一定知道它是构成 Wi-Fi 的基本要素。

iPhone 出现于 2009 年初，那时智能设备还不多，也没有 iPad 或其他 pad 设备。你知道这个东西最令人叫绝的事情是什么吗？它是无线的，它没有 RJ45 插孔！网络行业的几个大玩家(Cisco、IDC 及无线宽带联盟)都发布了预测报告，预测 Wi-Fi 会成为网络中占据统治地位的通信媒介，而非 3g/4g/LTE 和有线网络。所以当我们说“无线”或“流动性”时，我们就是指 Wi-Fi。

在 2009 年，还没有 CWAP 和 CWDP 认证！CWNA 是认证的入门级别，最终认证级别是 CWNE。

今天 Wi-Fi 已无处不在，这的确是美妙时光。但对于无线网络来说。我们刚刚起步。今天，如果你有一个最大、最先进的双频 802.11n AP 和兼容的客户端设备，此类设备理论上具有约 900Mbps 的数据传输率，但真正的吞吐量只有不到理论值的一半。但当提笔撰写本序言的时候，我发现 802.11ac 产品已经开始出现在市场上。我们现在开始谈论千兆 Wi-Fi，就像我们三年前谈论 802.11n 一样。让我们回顾一下 802.11n 在过去对网络产生的巨大影响，并类比考虑一下未来 802.11ac 和 802.11ad 标准会带来的影响吧！

现在就开始抓紧时间阅读本书吧。Wi-Fi 时代已经到来了，如果你希望自己成为无线网络工程师，就必须知道 Wi-Fi 的来龙去脉。David Coleman 和 David Westcott 再次更新了这本引人注目的 Wi-Fi 书籍。在此我不得不再次介绍下他们。他们是 CWNA、CWSP 和 CWAP 官方学习指南的作者，也为 CWDP 做出贡献。感谢他们两位所做的一切。

再次向你即将开始研究 Wi-Fi 的核心知识表示祝贺。你不会对开始阅读本书所做的决定后悔，你未来的雇主和客户也不会。

CWNP 公司 CEO 及共同创始人 Kevin Sandlin

前　　言

如果你已经购买或者正在考虑购买本书，你可能对参加 CWNA 认证考试或学习 CWNA 认证考试所涉及的知识感兴趣。恭喜你开始迈出第一步，也希望本书可以帮你走完这段旅程。无线网络是市场上最热门的技术之一。随着无线网络技术的快速发展，合格人才的数量远远不能满足市场需要。CWNA 认证是证明你拥有这个快速增长行业所需的知识和技能的途径之一。本学习指南也是基于这个目的而撰写的。

本书可以传授给你有关无线网络方面的知识，从中学到的知识不仅可以帮助你通过 CWNA 认证考试，还能教你如何设计、安装和支持无线网络。每一章都设定了复习题以帮助你测试知识和进行考试准备。本书网站(www.sybex.com/go/cwna3e)上还有实验、白皮书、视频和演示文稿以进一步方便你的学习。

在了解有关认证过程和要求前，我们必须提醒你，在参加考试时，可能考试信息已经发生了变化。所以我们建议：在准备考试的时候访问 www.cwnp.com 网站以了解最新的考试目标和要求。

不要只看本书的复习题和答案！本书的复习题仅用于测试 CWNA 考试所要求的概念和目标，与真实认证考试的题库是不同的！理解考试目标和主题对于备考大有裨益。

关于 CWNA 和 CWNP

如果你曾经准备参加一门不熟悉的技术认证考试，你就知道不仅要学习不同技术，还要了解你并不熟悉的这个行业。下面将介绍 CWNP。

CWNP 是认证无线网络专业的简称，它不是一门考试。CWNP 开发了计算机网络行业的无线局域网技术的教材和认证考试，它是一门厂商中立的培训体系。

CWNP 用来考查人员的无线网络技术能力，并不针对某厂商的产品。当然本书的作者和认证的创立者会谈论甚至教授使用某个产品，但目的是帮助你总体上了解无线技术而不是了解产品本身。打个比方说，如果要学开车，你可能需要找辆车坐进去并开始练习。事后回忆时，你可能不会告诉别人你在学习开福特车，而是会告诉别人我只是在用福特车学习驾驶技术。

下面是 CWNP 认证体系中的 7 种无线认证：

CWTS: Certified Wireless Technology Specialist

CWTS 是 WLAN 的入门级企业认证，被推荐作为 CWNA 认证的前一阶段认证。这个认

证适合 WLAN 销售人员或者企业级 WLAN 行业的支持人员。CWTS 认证考查 WLAN 销售和支持人员的 WLAN 基础知识、工具和术语，以便更好地支持和销售 WLAN 产品。

CWNA: Certified Wireless Network Administrator

CWNA 认证考试是 Wi-Fi 认证体系中的基础级认证，但非入门级别。参加本考试(PW0-105)的人员必须很好地掌握网络基础知识(例如 OSI 模型、IP 寻址、PC 硬件和网络操作系统等)。许多考生已经获得了其他行业证书，如 CompTIA、思科的 CCNA 证书，他们的考试目的是强化或补充知识技能。

CWSP: Certified Wireless Security Professional

CWSP 认证考试(PW0-204)专注于基于标准的无线安全协议、安全策略和无线网络安全设计。本认证会考查无线网络入侵者采用的技术和技能及网络管理员保护网络需要采取的手段。随着无线网络安全的发展，现在的 WLAN 已经比有线网络更加安全。

CWDP: Certified Wireless Design Professional

CWDP 认证考试(PW0-250)是一门专家级别的职业认证，它适用于已经通过 CWNA 认证的网络人士，要求考生对于 RF 技术和 802.11 网络应用非常熟悉。这门认证考查 WLAN 专业人员能否在不同环境中为不同应用程序正确设计无线局域网。

CWAP: Certified Wireless Analysis Professional

CWAP 认证考试(PW0-270)是一门专家级别的职业认证，它适用于已经通过 CWNA 认证的网络人士，要求考生对于 RF 技术和 802.11 网络应用非常熟悉。这门认证会深入考查 802.11 协议，并要求考生能够进行无线数据包分析和频谱分析。

CWNE: Certified Wireless Network Expert

CWNE 是 CWNP 认证体系中的最高级认证。完成 CWNE 的认证要求，你将拥有当今无线局域网市场最先进的技术技能。CWNE 认证要求通过 CWNA、CWAP、CWDP 和 CWSP 认证。为获取 CWNE 认证，还要填写一份严格的申请，必须得到 CWNP 审阅团队的认可。

CWNT: Certified Wireless Network Trainer

CWNT 是 CWNP 认证的培训讲师，可向 IT 人士传授 CWNP 培训课程。CWNT 是无线技术、产品和解决方案方面的技术和培训专家。为了确保客户的学习体验，CWNP 要求只有 CWNT 才可以传授 CWNP 课程。

如何通过 CWNA 认证?

要通过 CWNA，必须完成两件事：遵守和同意 CWNP 保密协议条款并通过 CWNA 认证考试。

CWNP 保密条款可在 CWNP 网站上找到。

在进入考场准备正式参加考试之前，你必须同意保密协议才可以继续考试。在单击同意后，便可以开始考试，如果最终通过考试，你便成为 CWNA 的一员了。

考试信息如下：

- 考试名称：Wireless LAN Administrator
- 考试编号：PW0-105
- 费用：175 美元
- 考试时间：90 分钟
- 考题数：60
- 通过分数：70% (教师是 80%)
- 考试语言：英语
- 注册方式：Pearson VUE(www.vue.com/cwnp)

CWNA 认证有效期为三年，重认证需要你通过最新的 PW0-105 考试、CWSP、CWAP 或 CWDP 考试中的一门。通过认证考试后，你需要登录 CWNP 跟踪系统，确定联系信息后，就可以请求 CWNP 发送证书。

谁应该买这本书？

如果想获得扎实的无线网络基础知识或者想通过考试，这本书就是为你准备的。在本书中，可以找到高水平专业能力所需要掌握的对概念的明确解释和大量的帮助信息。

本书是为那些想要获得实际操作技能和无线网络深入知识的人士编写的。如果你想成为认证的 CWNA，这本书绝对适合你。然而，如果只是想试图通过考试，而不愿真正了解无线知识，那么本自学指南不适合你。

如何使用本书和本书在线资源？

本书和配套的在线资源(www.sybex.com/go/cwna3e)已经涵盖了考试的一些特点。这些工具可以帮你记住重要的考试内容并为真正的考试做准备。另外，其中一部分材料也可在 http://www.tupwk.com.cn/downpage 上找到；打开该网页后，输入本书中文书名或 ISBN 即可进入下载页面。

考前准备

本书开始部分有一个评估测试，用来检查你对考试是否准备就绪。在开始阅读本书之前做下这个测试，以便明确需要提高的部分。评估测试的答案就在最后一道测试题后面，会对每一道题进行解释，并注明到哪个章节查询具体信息。

章末复习题

为考查学习过程中的阶段性成果，每章末都有一些复习题。学习完每章后回答问题，然后进行检查。正确答案显示在附录 A 中。如果回答错误，可以重读这个部分，确保下次测试的时候回答正确。

电子抽认卡

本书的在线资源(www.sybex.com/go/cwna3e)包含电子抽认卡片，这些问题和答案很简洁，类似于学校的学习卡片。你可在 PC 上回答这些问题，也可以下载到智能手机上进行快捷复习。

测试引擎

本书的在线资源(www.sybex.com/go/cwna3e)还包含 Sybex 测试引擎，它包含所有前面提到的测试要点，并帮你发现知识的薄弱点并巩固所学的内容。

除了评估测试和章节复习题外，测试引擎还提供三次额外考试。使用测试引擎进行考试练习，可以帮你身临其境地体验真实考试进程。当完成第一套模拟考试题后，可以单击下一个来巩固考试技巧。一旦你得到 95%的正确率，就可以准备参加真正的认证考试了。

试验和练习

本书有几章包含使用软件的练习、数据表和视频资料，这些内容都可以在本书的在线资源(www.sybex.com/go/cwna3e)上找到。实验和练习环节可以通过动手实验和循序渐进的问题解决方法给你提供更广泛的学习体验。

白皮书

本书多个章节提到的白皮书可以通过本书的在线资源(www.sybex.com/go/cwna3e)下载。这些白皮书是准备 CWNA 考试的辅助参考资料。

考试目标

CWNA 考试会考查 RF 行为的基础知识、无线局域网组成元素的特性和功能，还会考查无线局域网硬件外围设备、无线协议的排错以及无线局域网的安装配置技能知识。

CWNA 考试所考查的知识技能要求源于对无线网络专家和专业人士的调查。调查结果用来对考试内容和主题进行权重分配。

下表是考试的分解部分及每部分的考试权重：

考察内容	分值比重
射频(RF)技术	21%
802.11 规定和标准	17%
802.11 协议和设备	17%
802.11 网络部署	20%
802.11 网络安全	10%
802.11 RF 现场勘测	15%
合计	100%

1. 射频技术——21%

1.1 射频基础

1.1.1 定义和解释射频行为的基本概念

- 增益
- 损耗
- 反射
- 折射
- 衍射
- 漫射
- VSWR
- 返回损失
- 放大
- 衰减
- 吸收
- 波的传播
- 自由空间路径损耗
- 延迟扩展

1.2 射频计算

1.2.1 理解和应用射频计算的基本组成部分

- 瓦特
- 毫瓦
- 分贝
- dBm
- dBi
- dBd
- 信噪比
- RSSI
- SOM
- 衰落容限
- 链路预算
- 主动辐射体
- EIRP

1.3 射频信号和天线

1.3.1 了解射频信号特性、基础 RF 天线概念及天线部署方案

- 可视视距
- 射频视距
- 菲尼尔区
- 波束宽度
- 方位角和仰角
- 被动增益
- 各向同性辐射体
- 极化方式
- 简单天线分集
- MIMO 分集
- 射频链(Radio Chain)
- 空间复用(SM)
- 传输波束成形(TxBF)(静态、动态和基于芯片的三种传输波束成形技术)
- 最大比混合(MRC)
- 空时分组编码(STBC)
- 循环延迟分集(CSD)
- 波长
- 频率
- 振幅
- 相位

1.3.2 解释物理射频天线的应用和天线系统类型，了解天线的基本特性、目的和功能

- 全向天线
- 半定向天线
- 高度定向天线
- 扇形天线
- MIMO 天线
- 天线阵列

1.3.3 描述安装天线的方法及正确选位

- 立杆固定
- 天花板固定
- 墙面固定
- 户外和室内固定考虑因素

1.4 射频天线附件

1.4.1 了解如何使用下列 WLAN 附件，解释如何选择和安装 WLAN 附件以便优化性能并遵循无线监管规定

- 放大器
- 衰减器
- 避雷器
- 接地棒/接地线
- 射频电缆
- 射频连接头
- 射频信号分离器

2. 802.11 规定和标准——17%

2.1 扩频技术

2.1.1 了解下列扩频技术的使用

- WLAN
- WPAN
- WMAN
- WWAN

2.1.2 理解并解释不同扩频技术的差别及其与 IEEE 802.11-2007 标准(已批准的修正案和 IEEE 802.11n)的 PHY 条款的关系

- DSSS
- HR-DSSS
- ERP
- OFDM
- HT

2.1.3 了解扩频技术的工作原理

- 调制
- 编码

2.1.4 了解和应用扩频技术功能

- Co-location
- 信道中央与信道宽度(所有 PHY 标准)
- 主信道和次信道
- 重叠信道与不重叠信道
- 载频
- 吞吐量和数据率
- 带宽
- 通信抗逆力
- CSMA/CA
- 虚拟载波侦听(NAV)

2.2 IEEE 802.11-2007 标准(已批准的修正案和 802.11k、802.11r、802.11n、802.11y、802.11w 及 802.11u)

2.2.1 了解、解释和应用 802.11-2007 标准定义的帧类型和帧交换顺序

2.2.2 了解和应用地区无线监管要求

- DFS
- TPC
- 可用信道
- 输出功率

2.2.3 802.11-2007 标准及修正案影响的 OSI 模型层次

2.2.4 Wi-Fi 网络中使用的 ISM 和 UNII 信道

2.2.5 每个 802.11-2007 PHY 支持的数据率

2.2.6 理解 IEEE 标准的创立和修改过程，了解 IEEE 标准的命名惯例

- 草案
- 批准的修正案
- 增补条款
- 推荐实践
- 标准

2.2.7 Wi-Fi 新技术及其对 WLAN 部署的影响

- Wi-Fi Direct
- Voice Enterprise

2.3 802.11 行业组织及角色

2.3.1 定义下面组织在 Wi-Fi 产业的方向性、凝聚力和可核查性中的角色

- 政府无线监管机构
- IEEE
- Wi-Fi 联盟
- IETF

3. 802.11 协议和设备——17%

3.1 802.11 协议架构

3.1.1 认证和关联流程的汇总

- 802.11 状态机
- 开放认证、共享密钥认证和解除认证
- 关联、重关联和解除关联

3.1.2 定义、描述并应用 WLAN 服务集相关概念

- 终端与 BSS
- 基本服务集区域(BSA)
- 启动和加入 BSS

- BSSID 与 SSID
- Ad Hoc 模式与 IBSS
- Infrastructure 模式与 ESS
- 分布系统(DS)
- 分布系统介质(DSM)
- layer 2 和 layer 3 漫游

3.1.3 解释和应用下列 WLAN 电源管理功能

- 主动模式
- 节电模式
- 非计划自动节电交付(U-APSD)
- WMM 节电模式(WMM-PS)
- 节电多次轮询(PSMP)
- 空间复用节电(SMPS)
- TIM/DTIM/ATIM

3.2 802.11 MAC 与 PHY 技术

3.2.1 描述和应用下列 WLAN 帧相关概念

- IEEE 802.11 帧格式与 IEEE 802.3 帧格式
- IEEE 802.11 帧支持的第三层协议
- 术语回顾：帧、包和数据报
- 术语回顾：比特、字节和八位组
- 术语回顾：MAC 层和 PHY 层
  - Guard Interval (GI)
  - PSDU
  - PPDU
  - PPDU 格式
  - MSDU
  - MPDU
  - A-MPDU
  - A-MSDU
  - 802.11 帧格式
  - 802.11 帧类型
  - 帧间空隙(RIFS、SIFS、PIFS、DIFS、AIFS 和 EIFS)
  - 块确认
- jumbo 帧支持(layer 2)
- MTU 发现及功能特性(layer 3)

3.2.2 了解 802.11-2007 标准中关于 WLAN 加入和连接维护的方法

- 主动扫描(Probe)

- 被动扫描(Beacon)
- 动态速率切换

3.2.3 定义、描述和应用 802.11 协调功能和信道访问方法及可用的 RF 媒介数据流优化特性

- DCF 和 HCF 协调功能
- EDCA 信道访问方法
- RTS/CTS 与 CTS-to-Self 协议
- HT 信道宽度
- HT 操作模式
- 分片
- 通话公平
- 频带控制

3.3 WLAN 基础架构和客户端设备

3.3.1 了解下列 WLAN 基础架构设备的作用并描述如何对其进行安装、配置、保护和管理

- 自治型 AP
- 轻量型 AP
- Mesh AP/路由器
- 企业级 WLAN 控制器
- 分布式 WLAN 架构
- 远程分支型 WLAN 控制器
- PoE 注入器(单端口和多端口)及 PoE 以太网交换机
- WLAN 网桥
- 家用 WLAN 路由器

3.3.2 了解下列 WLAN 客户端设备的作用，解释如何对其进行安装、配置和管理以及如何保证安全

- PC 卡(Express Card、CardBus、PCMCIA)
- USB2、CF、SD 卡
- PCI、Mini PCI、Mini PCIe、半高 Mini PCIe 卡
- 工作组网桥

4. 802.11 网络部署——20%

4.1 802.11 网络设计、部署和管理

4.1.1 了解在下列垂直市场中的 WLAN 技术角色。

- 企业数据接入与终端用户的移动性
- 网络延伸到远端
- 建筑物之间的桥接
- 无线运营商(WISP)——最后一英里的数据交付
- 小型办公室/家庭办公(SOHO)

- 移动办公网络
- 教育/教室使用
- 工业——仓储和制造
- 医疗保健——医院与办公室
- 市政网络
- 热点——公共网络接入
- 交通网络(火车、飞机、汽车)
- 执法网络

4.2 802.11 网络排错

4.2.1 了解和解释如何利用企业级 WLAN 设备中的可用功能解决 WLAN 部署难题

- 系统吞吐量
- 同频与邻频干扰
- 射频噪声及本底噪声
- 窄频和宽频干扰
- 多路径现象(SISO 和 MIMO 环境下)
- 隐藏节点
- 近/远问题
- 天气

4.3 PoE

4.3.1 802.3-2005 第 33 条款(前身为 IEEE 802.3af)

4.3.2 HT(802.11n)设备供电考虑

- 专有的中跨 PSE 和端接式 PSE
- 802.3at 中跨 PSE 和端接式 PSE

4.4 WLAN 架构

4.4.1 自治型 AP 的定义、描述和部署

- 网络连接
- 一般特性
- 配置、安装及管理
- 优点和局限性

4.4.2 WLAN 控制器的定义、描述和部署(集中式转发和分布式转发)

- 网络连接
- 一般特性
- 核心层、分布层和接入层转发
- 基于控制器的 AP、Mesh 及 Portal AP
- 扩展性
- 控制器内与控制器间客户端切换

- 配置、安装和管理
- 优点与局限性
- 隧道、QoS 与 VLAN

4.4.3 定义、描述和部署分布式 WLAN 网络架构

- 网络连接
- 一般特性
- 配置、安装和管理
- 扩展性
- AP 间切换
- 优点与局限性
- 隧道、QoS 与 VLAN

4.4.4 定义、描述和部署管理 AP 和 WLAN 控制器的 WNMS

- 网络连接
- 一般特性
- 配置、安装和管理
- 优点与局限性

4.4.5 定义、描述和部署多信道架构

- BSSID 与 ESSID 配置
- 现场勘测方法
- 网络吞吐量
- 同频与邻频干扰
- 蜂窝规划(微蜂窝)
- 协调传输
- 信道堆栈

4.4.6 定义、描述和部署单信道架构网络模型

- BSSID 与 ESSID 配置(包括虚拟 BSSID)
- 现场勘测方法
- 网络吞吐量
- 同频与邻频干扰
- 蜂窝规划(微蜂窝)
- 协调传输
- 信道堆栈

4.4.7 定义和描述其他 WLAN 架构

- WLAN 阵列
- Mesh 网络
- WLAN 云管理

4.5 WLAN 部署类型

4.5.1 了解如下通用 WLAN 应用与设备的设计和部署要点

- 数据
- 语音
- 视频
- 实时定位系统(RTLS)
- 移动设备(平板电脑与智能手机)
- 高密部署

5. 802.11 网络安全——10%

5.1 IEEE 802.11 网络安全架构

5.1.1 了解和描述下列 IEEE 802.11 安全相关主题的优缺点、应用场合与部署

- 传统无线网络安全机制
  - WEP 加密组
  - 开放系统认证
  - 共享密钥认证
  - MAC 地址过滤
  - SSID 隐藏
- 当今无线网络安全机制
  - WPA-/WPA2 Enterprise
  - WPA-/WPA2 Personal
  - TKIP 与 CCMP 加密组
  - 802.1X/EAP
  - 预共享密钥(PSK)/密码认证
  - PPSK
  - WPS
- 其他机制
  - 设备安全管理协议(HTTPS、SNMPv3、SSH2)
  - RBAC
  - 强制门户与访客网络
  - 管理帧保护(802.11w)
  - 快速安全漫游方法

5.2 802.11 安全分析、性能分析与排错

5.2.1 对下面无线安全解决方案使用场合进行描述、解释

- WIPS
  - 安全监控、抑制与报告
  - 性能监控与报告
  - 排错分析

- 协议分析仪
  - 安全与性能监控
  - 排错分析
  - 集成式协议分析仪与独立式协议分析仪

5.3 802.11 网络安全策略基础

5.3.1 描述以下通用安全策略要素

- 适用人员
- 风险评估
- 影响分析
- 安全审计
- 策略执行
- 监控、响应和报告
- 资产管理

5.3.2 描述下列安全策略要素：

- 设计和部署最佳实践
  - SOHO
  - SMB
  - 企业
- 密码策略
- 可接受的用户策略(AUP)
- 培训需求
- 物理安全
- 社会工程学

6. 802.11 RF 现场勘测——15%

6.1 802.11 网络现场勘测基础

6.1.1 解释手动和预测性 RF 现场勘测的信息收集的重要性及相关流程(这些通常发生于 RF 现场勘测的准备期间)

- 业务需求信息收集
- 与经理和用户面谈
- 定义物理安全和数据安全需求
- 收集与勘测现场相关文档
- 记录现有网络现状
- 收集许可及分区需求
- 室内与室外信息
- 了解基础架构连通性及电源需求
- 了解射频覆盖需求

- 了解数据容量和客户端密度需求
- VoWiFi 部署对延迟和抖动的要求
- 客户端连通性需求
- 天线使用考虑因素
- 跟踪系统考虑因素
- WIPS 探测器考虑因素

6.1.2 解释执行手动和预测性 RF 现场勘测设计的技术要点(这些通常发生于 RF 现场勘测期间)

- 定位和识别 RF 干扰源
- 确定使用的 AP 与天线类型
- 确定 AP 与天线的安装位置
- 确定 AP 的发射功率与信道分配
- 确定同频与邻频干扰
- 测试应用程序能否正常工作
- 根据设计需求测试性能参数

6.1.3 描述手工和预测性 RF 现场勘测的报告及后续流程(这些通常发生于 RF 现场勘测完成后)

- 报告方法
- 客户的报告需求
- 硬件推荐和材料清单
- 覆盖与容量验证方面的应用分析

6.2 802.11 网络现场勘测系统与设备

6.2.1 了解执行预测性现场勘测所要求的设备、应用程序与系统特性

- 预测性分析/模拟程序(也称为 RF 规划与管理工具)
- WLAN 控制器的集成预测性现场勘测特性
- 现场勘测验证工具和/或应用程序
- 室内与室外现场勘测

6.2.2 了解执行手动现场勘测所要求的设备、应用程序与系统特性

- 现场勘测硬件设备
- 频谱分析仪
- 协议分析仪
- 主动现场勘测工具和/或应用程序
- 被动现场勘测工具和/或应用程序
- VoWiFi 现场勘测最佳实践
- 厂商客户端应用程序

6.2.3 了解自管理 RF 技术所涉及的设备、应用程序和方法论

- 自动射频资源管理

CWNA 考试术语

CWNP 考试使用 CWNP 特定的术语。这些最常用的术语与 Wi-Fi 联盟和 IEEE 802.11-2007 标准使用的相同。最新的 IEEE 802.11 标准版本为 IEEE 802.11-2007，它包括了在文档发布之前已批准的所有修正案。IEEE 等标准机构也往往在标准正式“滚动到”已批准的修正案之前发布几个修正案，这些已批准的修正案就是最后定稿或批准的版本。

准备 CWNA 考试时，考生应该百分之百熟悉这些 CWNP 要求的术语。本书定义和覆盖了所有术语。要求也要熟悉 CWNP 字典中的简写、术语和定义。

参加 CWNA 考试提示

以下是考试有关的一些提示：

- 携带两份身份证件

其中一份必须有照片，如驾驶证。另一份证件可以是信用卡或护照。两份证件都必须包含签名。

- 提前到达考场可以放松心情，并且可以回顾下学习资料，特别是可以了解考试相关信息列表
- 仔细阅读题目

不要提前下结论，确信了解题目含义。

- 有些题目是多项选择题

对于多项选择题，屏幕底部的消息会提示你“选择两个”或“选择所有答案”。确信你了解这一点。

- 针对多选题，如果不确定答案，可以尝试排除最明显错误的答案
- 不要在一道题上花费过多的时间

这是一项基于表单的考试，但在考试期间不可以返回查看。在移到下一道题之前必须回答当前题目，之后你可以移到下一题目，此时你无法返回并改变你上一题的回答。

- 时刻了解你的考试时间

这是一项 60 题 90 分钟的考试。平均回答一题的时间为 90 秒。你可以决定在一道题目上花费的时间，但考试时间只有 90 分钟。所以时刻了解进度，45 分钟的时候，你应该回答至少 30 题。如果没有，不要惊慌，你只需在下面的时间里回答得快一点。如果你在剩下的 30 题里，每题加快 4 秒钟，你就可以补回两分钟的时间。再次提醒，不必惊慌，自我调节好即可。

- 关于最新的考试价格与注册流程，请访问 CWNP 官网 www.cwnp.com

自测题

1. At which layers of the OSI model does 802.11 technology operate? (Choose all that apply.)

A. Data-Link

B. Network

C. Physical

D. Presentation

E. Transport

2. Which Wi-Fi Alliance certification defines the mechanism for conserving battery life that is critical for handheld devices such as barcode scanners and VoWiFi phones?

A. WPA2-Enterprise

B. WPA2-Personal

C. WMM-PS

D. WMM-SA

E. CWG-RF

3. Which of these frequencies has the longest wavelength?

A. 750 KHz

B. 2.4 GHz

C. 252 GHz

D. 2.4 MHz

4. Which of these terms can best be used to compare the relationship between two radio waves that share the same frequency?

A. Multipath

B. Multiplexing

C. Phase

D. Spread spectrum

5. A bridge transmits at 10 mW. The cable to the antenna produces a loss of 3 dB, and the antenna produces a gain of 20 dBi. What is the EIRP?

A. 25 mW

B. 27 mW

C. 4 mW

D. 1,300 mW

E. 500 mW

6. What are some possible effects of voltage standing wave ratio (VSWR)? (Choose all that apply.)

A. Increased amplitude

B. Decreased signal strength

C. Transmitter failure

D. Erratic amplitude

E. Out-of-phase signals

7. When installing a higher-gain omnidirectional antenna, which of the following occurs? (Choose two.)

A. The horizontal coverage increases.

B. The horizontal coverage decreases.

C. The vertical coverage increases.

D. The vertical coverage decreases.

8. 802.11a OFDM radio cards are backward compatible with which IEEE 802.11 radios?

A. FHSS radios

B. ERP radios

C. DSSS radios

D. HR-DSSS radios

E. HT radios

F. None of the above

9. Which IEEE 802.11 draft amendment specifies the use of the 5.850 to 5.925 GHz frequency band?

A. IEEE 802.11a

B. IEEE 802.11h

C. IEEE 802.11p

D. IEEE 802.11g

E. IEEE 802.11u

10. Which of the following are valid ISM bands? (Choose all that apply.)

A. 902–928 MHz

B. 2.4–2.4835 MHz

C. 5.725–5.825 GHz

D. 5.725–5.875 GHz

11. What signal characteristics are common in spread spectrum signaling methods? (Choose two.)

A. Narrow bandwidth

B. Low power

C. High power

D. Wide bandwidth

12. A service set identifier is often synonymous with which of the following?

A. IBSS

B. ESSID

C. BSSID

D. Basic service set identifier

E. BSS

13. Which ESS design scenario is defined by the IEEE 802.11-2007 standard?

A. Two or more access points with overlapping coverage cells

B. Two or more access points with overlapping disjointed coverage cells

C. One access point with a single BSA

D. Two basic service sets connected by a DS with co-located coverage cells

E. None of the above

14. What CSMA/CA conditions must be met before an 802.11 radio card can transmit? (Choose all that apply.)

A. The NAV timer must be equal to zero.

B. The random back-off timer must have expired.

C. The CCA must be idle.

D. The proper interframe space must have occurred.

E. The access point must be in PCF mode.

15. Beacon management frames contain which of the following information? (Choose all that apply.)

A. Channel information

B. Destination IP address

C. Basic data rate

D. Traffic indication map (TIM)

E. Vendor proprietary information

F. Time stamp

G. Spread spectrum parameter sets

16. Anthony Dean was hired to perform a wireless packet analysis of your network. While performing the analysis, he noticed that many of the data frames were preceded by an RTS frame followed by a CTS frame. What could cause this phenomenon to occur? (Choose all that apply.)

A. Because of high RF noise levels, some of the stations have automatically enabled RTS/CTS.

B. Some stations were manually configured for RTS/CTS.

C. A nearby 802.11g OFDM radio is causing some of the nodes to enable a protection mechanism.

D. The network is a mixed-mode environment.

17. What is another name for an 802.11 data frame that is also known as a PSDU?

A. PPDU

B. MSDU

C. MPDU

D. BPDU

18. Which WLAN device uses self-healing and self-forming mechanisms and layer 2 routing

protocols?

A. WLAN switch

B. WLAN controller

C. WLAN VPN router

D. WLAN mesh access point

19. Which WLAN device offers AP management, user management, intrusion detection, and spectrum management?

A. Sectorized array

B. Autonomous AP

C. WLAN controller

D. Enterprise wireless gateway (EWG)

E. All of the above

20. Wi-Fi technology is used in many different vertical markets. In which of these verticals markets are you most likely to still find legacy 802.11 FHSS technology?

A. Healthcare

B. Manufacturing

C. Education

D. Law enforcement

E. Hotspots

21. Wireless mesh routers often have two radio cards. One radio is used for client connectivity, and the other is used for backhaul. Which of these statements best meets this model? (Choose all that apply.)

A. A 2.4 GHz radio is used for distribution, whereas a 5 GHz radio is used for access.

B. An ERP radio is used for client connectivity, whereas an HR-DSSS radio is used for backhaul.

C. An ERP radio is used for client connectivity, whereas an OFDM radio is used for backhaul.

D. A 2.4 GHz radio is used for access, whereas a 5 GHz radio is used for distribution.

22. If IEEE 802.1X/EAP security is in place, what type of roaming solution is needed for timesensitive applications such as VoWiFi?

A. Nomadic roaming solution

B. Proprietary layer 3 roaming solution

C. Mobile IP solution

D. Fast secure roaming solution

23. The hidden node problem occurs when one client station's transmissions are not heard by all the other client stations in the coverage area of a basic service set (BSS). What are some of the consequences of the hidden node problem? (Choose all that apply.)

A. Retransmissions

B. Intersymbol interference (ISI)

C. Collisions

D. Increased throughput

E. Decreased throughput

24. What are some potential causes of layer 2 retransmissions? (Choose all that apply.)

A. Multipath

B. Mismatched client and AP power settings

C. Dual-frequency transmissions

D. Fade margin

E. Multiplexing

25. Which of these solutions would be considered strong WLAN security?

A. SSID cloaking

B. MAC filtering

C. WEP

D. Shared Key authentication

E. CCMP/AES

26. Which security standard defines port-based access control?

A. IEEE 802.11x

B. IEEE 802.3b

C. IEEE 802.11i

D. IEEE 802.1X

E. IEEE 802.11s

27. Which is the best tool for detecting an RF jamming denial-of-service attack? (Choose all that apply.)

A. Time-domain analysis software

B. Layer 2 distributed WIPS

C. Spectrum analyzer

D. Layer 1 distributed WIPS

E. Oscilloscope

28. Which of these attacks can be detected by a wireless intrusion detection system (WIDS)? (Choose all that apply.)

A. Deauthentication spoofing

B. MAC spoofing

C. Rogue ad hoc network

D. Association flood

E. Rogue AP

29. You have been hired by the XYZ Company based in the United States for a wireless site survey. What government agencies need to be informed before a tower is installed of a height that exceeds 200 feet above ground level? (Choose all that apply.)

A. RF regulatory authority

B. Local municipality

C. Fire department

D. Tax authority

E. Aviation authority

30. You have been hired by the ABC Corporation to conduct an indoor site survey. What information will be in the final site survey report that is delivered? (Choose two.)

A. Security analysis

B. Coverage analysis

C. Spectrum analysis

D. Routing analysis

E. Switching analysis

31. Name potential sources of interference in the 5 GHz UNII band. (Choose all that apply.)

A. Perimeter sensors

B. Nearby OFDM (802.11a) WLAN

C. Cellular phone

D. DSSS access point

E. Bluetooth

F. Nearby HT (802.11n) WLAN

32. Which of these measurements are taken for indoor coverage analysis? (Choose all that apply.)

A. Received signal strength

B. Signal-to-noise ratio

C. Noise level

D. Path loss

E. Packet loss

33. What problems may result due to access points with too much transmission amplitude? (Choose all that apply.)

A. Poor client capacity

B. Co-channel interference

C. Layer 3 roaming failure

D. Access point buffer overflow

34. What must a powered device (PD) do to be considered PoE compliant (IEEE 802.3-2005 clause 33)? (Choose all that apply.)

A. Be able to accept power in either of two ways (through the data lines or unused pairs).

B. Reply with a classification signature.

C. Reply with a 35 ohm detection signature.

D. Reply with a 25 ohm detection signature.

E. Receive 30 watts of power from the power sourcing equipment.

35. An HT network can operate on which frequency bands? (Choose all that apply.)

A. 902–928 MHz

B. 2.4–2.4835 GHz

C. 5.15–5.25 GHz

D. 5.47–5.725 GHz

36. What are some of the methods used to reduce MAC layer overhead as defined by the 802.11n-2009 amendment? (Choose all that apply.)

A. A-MSDU

B. A-MPDU

C. MRC

D. MCS

E. PPDU

自测题答案

1. A、C。IEEE 802.11-2007 标准仅在 OSI 模型的物理层与数据链路层的 MAC 子层定义了通信机制。详细内容请参阅第 1 章。

2. C。WMM-PS(WMM 节电)管理并调整客户设备上 Wi-Fi 无线接口处于休眠状态的时间，以达到延长设备电池续航时间的目的。对条码扫描器和 VoWiFi 电话等手持设备而言，降低电池耗电量至关重要。客户设备和接入点必须同时支持 WMM-PS 才能使用节电特性。详细内容请参阅第 1 章。

3. A。频率为 750KHz 的信号，其波长约为 1312 英尺(400 米)；频率为 252GHz 的信号，其波长约为 0.05 英寸(1.2 毫米)。请记住，电磁信号的频率越高，波长越短。采用公式 $\lambda=c/f$ 计算波长。详细内容请参阅第 2 章。

4. C。相位描述了两个同频波的波峰与波谷之间的关系。详细内容请参阅第 2 章。

5. E。10mW 功率降低 3dB 相当于将功率除 2，结果为 5mW。5mW 功率提高 20dBi 相当于将功率连续两次乘 10，结果为 500mW。详细内容请参阅第 3 章。

6. B、C、D。阻抗失配会引起一部分电压被反射回发射机，导致信号强度降低和波动，甚至使发射机出现故障。详细内容请参阅第 4 章。

7. A、D。全向天线的增益越高，其垂直覆盖范围越小，水平覆盖范围越大。详细内容请参阅第 4 章。

8. F。802.11a OFDM(条款 17)无线接口使用 5GHz UNII 频段收发数据，而 802.11 FHSS(条款 14)、802.11 DSSS(条款 15)、802.11b HR-DSSS(条款 18)与 802.11g ERP(条款 19)设备均使用 2.4GHz ISM 频段收发数据，因此 OFDM 无线接口无法向后兼容上述无线接口，但是它向前兼容 802.11n HT(条款 20)无线接口。由于 HT 无线接口既可以使用 2.4GHz，也可以使用 5GHz 频段收发数据，因此它向后兼容 DSSS、HR-DSSS、ERP 与 OFDM 无线接口。详细内容请参阅第 5 章。

9. C。IEEE 802.11p 修正案致力于完善并改进 IEEE 802.11-2007 标准，以便高速行驶的车辆与路边基础设施之间可以使用需要牌照的 5.9GHz ITS 频段相互通信。详细内容请参阅第 5 章。

10. A、D。ISM 频段包括 902MHz～928MHz、2.4GHz～2.4835GHz 与 5.725GHz～5.875GHz 频段。5.725GHz～5.825GHz 属于 UNII-3 频段。ISM 频段位于 GHz 而不是 MHz，不存在所谓的“2.4MHz ISM 频段”。详细内容请参阅第 6 章。

11. B、D。扩频信号采用超出实际所需的带宽来传输数据，并且其传输功率很低。详细内容请参阅第 6 章。

12. B。无线局域网的逻辑网络名一般被称为 ESSID(扩展服务集标识符)。ESSID 与 SSID(服务集标识符)同义，大部分无线局域网部署使用 SSID 作为逻辑网络名。详细内容请参阅第 7 章。

13. E。选项 A、B、C、D 都属于 ESS(扩展服务集)部署的例子。IEEE 802.11-2007 标准将 ESS 定义为“一个或多个互联的 BSS(基本服务集)的集合”，但是标准并没有规定具体的 ESS 实现方式。详细内容请参阅第 7 章。

14. A、B、C、D。CSMA/CA(载波侦听多路访问/冲突避免)是一种采用多种制衡手段以最大限度减少冲突的介质访问方式。可以将这些制衡手段视为避免冲突的多道防线，即确保任何时候只有一个无线接口使用介质传输数据，而其他无线接口在侦听。4 种制衡手段包括网络分配向量(NAV)、随机回退定时器(back-off timer)、空闲信道评估(CCA)与帧间间隔(IFS)。详细内容请参阅第 8 章。

15. A、C、D、E、F、G。在所有选项中，目标 IP 地址是唯一不包含在信标管理帧中的参数。所有 802.11 管理帧的帧体仅包含第二层信息，由于 IP 地址属于第三层信息，因此它不包含在管理帧中。详细内容请参阅第 9 章。

16. B、D。为诊断隐藏节点问题，通常将设备配置为在所有传输中使用 RTS/CTS。题目所给的网络也可能是一种 HR-DSSS/ERP 混合网络，网络中的 802.11g ERP 节点启用 RTS/CTS 作为保护机制。详细内容请参阅第 9 章。

17. C。802.11 数据帧的正规技术名称是 MPDU(MAC 协议数据单元)。MPDU 由第二层帧头、帧体与帧尾构成。帧尾采用 32 位 CRC(循环冗余校验)，一般将其称为 FCS(帧校验序列)。MPDU 的帧体内是 MSDU(MAC 服务数据单元)，后者包括 LLC 子层信息以及第 3～7 层数据。详细内容请参阅第 9 章。

18. D。具备自组能力的网状无线局域网由 WLAN 网状接入点构成，它可以在安装阶段自动连接接入点，并在客户端增加时动态更新路由信息。干扰发生时，具备自愈能力的网状无线局域网能自动在 Wi-Fi 网状蜂窝中重新路由数据流量，这通过专有的第二层路由协议实现。详细内容请参阅第 10 章。

19. C。WLAN 控制器又称 WLAN 交换机，它对轻量接入点进行集中管理与配置。用户管理功能通过 RBAC(基于角色的访问控制)实现。大部分 WLAN 控制器都内置有 WIDS(无线入侵检测系统)并提供频谱管理功能。详细内容请参阅第 10 章。

20. B。仓储与制造业环境通常部署有用于库存管理的条码扫描器等无线手持设备，大部分早期部署无线手持扫描器还在使用 802.11 跳频技术。目前，传统的 802.11 FHSS 无线局域

网仍然部署在某些仓储与制造业环境中。详细内容请参阅第 11 章。

21. C、D。条件允许的话，安装 Mesh 路由器时应使用至少两块无线接口卡。2.4GHz HR-DSSS 与 ERP 无线接口通常用于提供客户连接，而 5GHz OFDM 无线接口用于提供 Mesh 连接或无线回传链路。详细内容请参阅第 11 章。

22. E。在企业中部署 IEEE 802.1X/EAP 安全解决方案时，用户认证所需的平均时间为 700ms 或更长。而 VoWiFi(无线 VoIP)要求切换时间不得超过 150ms，以保持漫游时的通话连续性。因此，如果无线网络采用 802.1X/EAP 安全解决方案且需要传输时敏应用，就应部署 FSR(快速安全漫游)解决方案。早期的 FSR 解决方案都是厂商专有的，而 IEEE 802.11r 修正案定义了标准化的快速安全漫游标准机制。详细信息请参阅第 12 章。

23. A、C、E。如果设备没有发现隐藏节点，它将和隐藏节点同时开始传输数据。由于设备始终无法发现隐藏节点的存在，冲突将在半双工介质上持续发生，这会导致帧传输失败并引发重传。一旦发生重传，媒介开销就会增加，吞吐量将因此而降低。导致码间干扰的原因是多径效应而非隐藏节点问题。详细内容请参阅第 12 章。

24. A、B。在无线局域网中，许多因素都会导致第二层重传。多径效应、客户端与接入点传输功率不匹配、射频干扰、隐藏节点、邻蜂窝干扰以及信噪比较低都可能引发第二层重传。详细内容请参阅第 12 章。

25. E。尽管 SSID 隐藏可在一定程度上防止业余黑客(“脚本小子”)与普通用户搜索到无线网络，不过应该清楚地认识到，SSID 隐藏绝非一种完备的无线安全解决方案。为所有设备配置 MAC 过滤的工作量较大，而 MAC 地址又易于伪造，这使得 MAC 过滤无法成为一种可靠的企业无线安全解决方案。WEP 加密与共享密钥认证属于传统的 802.11 安全解决方案。CCMP/AES 是 IEEE 802.11i 修正案定义的默认加密方式，采用现有的手段不可能破解 AES 密码。详细内容请参阅第 13 章。

26. D。IEEE 802.1X 标准并非一种专门的无线标准，它常被误称为“802.11x”。802.1X 是 PBAC(基于端口的访问控制)标准，它定义了一种授权架构，允许或阻止流量通过认证方端口访问网络资源。详细内容请参阅第 13 章。

27. C、D。尽管第二层 WIDS(无线入侵检测系统)与 WIPS(无线入侵防御系统)也能检测到某些射频干扰攻击，不过频谱分析仪才是唯一能百分之百确定干扰信号的工具。频谱分析仪是一种频域工具，可以发现所扫描的频段范围内的任何射频信号。某些 WIPS 企业解决方案目前也具备进行第一层分布式频谱分析的能力。详细内容请参阅第 14 章。

28. A、B、C、D、E。802.11 WIDS 可以发现 100 多种针对无线局域网的攻击，它能检测到所有第二层 DoS 攻击、欺骗攻击以及大部分非法设备。详细内容请参阅第 14 章。

29. A、B、E。在美国，如果发射塔的高度在 200 英尺(61 米)以上，勘测方必须获得 FCC(美国联邦通信委员会)与 FAA(美国联邦航空管理局)的同意。其他国家和地区也有类似的高度限制，勘测方应咨询相应的射频监管与航空管理部门。市政部门可能制定了有关施工管理方面的法规，勘测人员需要取得相应的许可才能开始工作。详细内容请参阅第 15 章。

30. B、C。最终的现场勘测报告称为交付报告(deliverable)，它包括频谱分析(标识潜在干扰源)与覆盖分析(界定射频蜂窝边界)。此外，最终报告还包括对接入点布局、配置以及天线朝向的建议，而应用程序吞吐量测试通常作为附在最终报告中的可选分析报告。但是，现场

勘测报告中并不包括安全、交换、路由分析等方面的信息。详细内容请参阅第 15 章。

31. A、B、F。附近的 802.11a OFDM 无线局域网与周界传感器均使用 5GHz UNII 频段进行通信。由于 802.11n HT 无线局域网可以使用 2.4GHz 或 5GHz 频段收发数据，它也属于潜在的干扰源。DSSS 接入点与蓝牙设备使用 2.4GHz ISM 频段收发数据，蜂窝电话使用需要许可的频段进行通信，它们不会干扰到 5GHz 无线局域网。详细内容请参阅第 16 章。

32. A、B、C、E。进行室内被动现场勘测时，需要测量接收信号强度、噪声水平、信噪比、数据率等射频覆盖蜂窝数据。进行主动人工现场勘测时，可以根据需要测量丢包率。路径损耗是进行室外无线桥接勘测时需要计算的参数。详细内容请参阅第 16 章。

33. A、B。部署无线局域网时，一个常见的问题是 AP 的发射功率设置过高，这会导致隐藏节点、同频干扰以及客户端容量问题。详细内容请参阅第 12 章。

34. A、D。接入点等 PD(受电设备)必须满足以下条件才符合 IEEE 802.3-2005 标准第 33 条款(PoE 标准)：可以通过数据电缆对或空闲电缆对接受供电，并向 PSE(供电设备)返回额定值为 25kΩ 的检测签名。PD 也可以向 PSE 返回分类签名，不过这并非强制要求。根据 802.3-2005 标准第 33 条款的 PoE 标准规定，PD 可以从 PSE 接收的最大功率为 12.95W。详细内容请参阅第 17 章。

35. B、C、D。IEEE 802.11n-2009 修正案定义了 HT(高吞吐量)技术，HT 无线接口可以工作在 2.4GHz ISM 频段以及全部 5GHz UNII 频段。详细内容请参阅第 18 章。

36. A、B。为减少开销，802.11n-2009 修正案定义了两种新的帧聚合方式。帧聚合是一种将多个帧合并到单一帧传输中的机制。第一种帧聚合方式称为 MSDU 聚合(A-MSDU)，第二种帧聚合方式称为 MPDU 聚合(A-MPDU)。

CWNA 官方学习指南(第 3 版): 认证无线网络管理员 PW0-105

CWNA 考试(PW0-105)考试目标

目标	章节
1. 射频技术	
1.1 射频基础	2,4
1.1.1 定义和解释射频行为的基本概念：增益；损耗；反射；折射；衍射；漫射；VSWR；返回损失；放大；衰减；吸收；波的传播；自由空间路径损耗；延迟扩展。	
1.2 射频计算	3
1.2.1 理解和应用射频计算的基本组成部分：瓦特；毫瓦；分贝；dBm；dBi；dBd；信噪比；RSSI；SOM；衰落容限；链路预算；主动辐射体；EIRP。	
1.3 射频信号和天线概念	4,18
1.3.1 了解射频信号特性、基础 RF 天线概念及天线部署方案：可视视距；射频视距；菲尼尔区；波束宽度；方位角和仰角；被动增益；各向同性辐射体；极化方式；简单天线分集；MIMO 分集；射频链 (Radio Chain)；空间复用(SM)；传输波束成形(TxBF)；最大比混合(MRC)；空时分组编码(STBC)；循环延迟分集(CSD)；波长；频率；振幅；相位。	
1.3.2 解释物理射频天线的应用和天线系统类型：了解天线的基本特性、目的和功能：全向天线；半定向天线；高度定向天线；扇形天线；MIMO 天线；天线阵列。	
1.3.3 描述安装天线的方法及正确选位：立杆固定；天花板固定；墙面固定；户外和室内固定考虑因素。	
1.4 射频天线附件	4
1.4.I 了解如何使用下列 WLAN 附件，解释如何选择和安装 WLAN 附件以便优化性能并遵循无线监管规定：放大器；衰减器；避雷器；接地棒/接地线；射频电缆；射频连接头；射频信号分离器	
2. 802.11 规定和标准	
2.1 扩频技术	6,7,8,18
2.1.1 了解下列扩频技术的使用：WLAN；WPAN；WMAN；WWAN。	
2.1.2 理解并解释不同扩频技术的差别及其与 IEEE 802.11-2007 标准(已批准的修正案和 IEEE 802.11n)的 PHY 条款的关系：DSSS；HR-DSSS；ERP；OFDM；HT。	
2.1.3 了解扩频技术的工作原理：调制；编码。	
2.1.4 了解和应用扩频技术功能概念：Co-location；信道中央与信道宽度(所有 PHY 标准)；主信道和次信道；重叠信道与不重叠信道；载频；吞吐量和数据率；带宽；通信抗逆力；CSMA/CA；虚拟载波侦听(NAV)。	

2.2 IEEE 802.11-2007 标准(已批准的修正案、802.11k、802.11r、802.11n、802.11y、802.11w 及 802.11u) **5,6,9**

2.2.1 了解、解释和应用 802.11-2007 标准定义的帧类型和帧交换顺序

2.2.2 了解和应用地区无线监管要求：DFS；TPC；可用信道；输出功率。

2.2.3 802.11-2007 标准及修正案影响的 OSI 模型层次

2.2.4 Wi-Fi 网络中使用的 ISM 和 UNII 信道

2.2.5 每个 802.11-2007 PHY 支持的数据率

2.2.6 理解 IEEE 标准的创立和修改过程，了解 IEEE 标准的命名惯例：草案；批准的修正案；增补条款；推荐实践；标准。

2.2.7 Wi-Fi 新技术及其对 WLAN 部署的影响：Wi-Fi Direct；Voice Enterprise。

2.3 802.11 行业组织及角色 **1**

2.3.1 了解下面组织在 Wi-Fi 产业的方向性、凝聚力和可核查性中的角色：政府无线监管机构；IEEE；Wi-Fi 联盟；IETF。

3. 802.11 协议和设备

3.1 802.11 协议架构 **7,8,9**

3.1.1 认证和关联流程的汇总：802.11 状态机；开放认证、共享密钥认证和解除认证；关联、重关联和解除关联。

3.1.2 定义、描述并应用 WLAN 服务集相关概念：终端和 BSS；基本服务集区域(BSA)；启动和加入 BSS；BSSID 与 SSID；Ad Hoc 模式与 IBSS；Infrastructure 模式与 ESS；分布系统(DS)；分布系统介质(DSM)；Layer2 和 layer3 漫游。

3.1.3 解释和应用下列 WLAN 电源管理功能：主动模式；节电模式；非计划自动节电交付(U-APSD)；WMM 节电模式(WMM-PS)；节电多次轮询(PSMP)；空间复用节电(SMPS)；TIM/DTIM/ATIM。

3.2 802.11 MAC 与 PHY 技术 **8,9,18**

3.2.1 描述和应用下列 WLAN 帧相关概念：IEEE 802.11 帧格式与 IEEE 802.3 帧格式；IEEE 802.11 帧支持的第三层协议；术语回顾：帧、包和数据报；术语回顾：比特、字节和八位组；术语回顾：MAC 层和 PHY 层；Guard interval (GI)；PSDU；PPDU；PPDU formats；MSDU；MPDU；A-MPDU；A-MSDU；802.11 帧格式；802.11 帧类型；帧间空隙(RIFS, SIFS, PIFS, DIFS, AIFS, EIFS)；块确认；jumbo 帧支持(Layer 2)；MTU 发现及功能特性(Layer3)。

3.2.2 了解 802.11-2007 标准中关于 WLAN 加入和连接维护的方法：主动扫描(Probe)；被动扫描(Beacon)；动态速率切换。

3.2.3 定义、描述和应用 802.11 协调功能和信道访问方法及可用的 RF 媒介数据流优化特性：DCF 和 HCF 协调功能；EDCA 信道访问方法；RTS/CTS 与 CTS-to-Self 协议；HT 信道宽度；HT 操作模式；分片；通话公平；频带控制。

3.3 WLAN 基础架构和客户端设备 **10**

3.3.1 了解下列 WLAN 基础架构设备的作用并描述如何对其进行安装、配置、保护和管理：自治型 AP；轻量型 AP；Mesh AP/路由器；企业级 WLAN 控制器；分布式 WLAN 架构；远程分支型 WLAN 控制器；PoE 注入器(单端口和多端口)及 PoE 以太网交换机；

WLAN 网桥；家用 WLAN 路由器。

3.3.2 描述下列 WLAN 客户端设备的作用，解释如何对其进行安装、配置和管理以及如何保证安全：PC card(Express Card、CardBus、PCMCIA)；USB2、CF、SD 卡；PCI、Mini PCI、Mini PCIe、半高 Mini PCIe；工作组网桥。

4. 802.11 网络部署

4.1 802.11 网络设计、部署和管理 11

4.1.1 了解在下列垂直市场中的 WLAN 技术角色：企业数据接入与终端用户的移动性；网络延伸到远端；建筑物之间的桥接；无线运营商(WISP)——最后一英里的数据交付；小型办公室/家庭办公(SOHO)；移动办公网络；教育/教室使用；工业——仓储和制造；医疗保健——医院与办公室；市政网络；热点——公共网络接入；交通网络(火车、飞机、汽车)；执法网络。

4.2 802.11 网络排错 12

4.2.1 了解和解释如何利用企业级 WLAN 设备中的可用功能解决 WLAN 部署难题：系统吞吐量；同频与邻频干扰；射频噪声及本底噪声；窄频和宽频干扰；多路径现象(SISO 和 MIMO 环境下)；隐藏节点；近/远问题；天气。

4.3 POE 17

4.3.1 802.3-2005 第 33 条款(前身为 IEEE 802.3af)

4.3.2 HT(802.11n)设备供电考虑：专有的中跨 PSE 和端接式 PSE；802.3at 中跨 PSE 和端接式 PSE

4.4 WLAN 架构 7,10,12

4.4.1 自治型 AP 的定义、描述和部署：网络连接；一般特性；配置、安装及管理；优点和局限性

4.4.2 WLAN 控制器的定义、描述和部署(集中式转发和分布式转发)：网络连接；一般特性；核心层、分布层和接入层转发；基于控制器的 AP、Mesh 及 Portal AP；扩展性；控制器内与控制器间客户端切换；配置、安装和管理；优点与局限性；隧道、QoS 与 VLAN。

4.4.3 定义、描述和部署分布式 WLAN 网络架构：网络连接；一般特性；配置、安装和管理；扩展性；AP 间切换；优点与局限性；隧道、QoS 与 VLAN。

4.4.4 定义、描述和部署管理 AP 和 WLAN 控制器的 WNMS：网络连接；一般特性；配置安装和管理；优点与局限性；

4.4.5 定义、描述和部署多信道架构：BSSID 与 ESSID 配置；现场勘测方法；网络吞吐量；同频与邻频干扰；蜂窝规划(微蜂窝)；协调传输；信道堆栈。

4.4.6 定义、描述和部署单信道架构网络模型：BSSID 与 ESSID 配置(包括虚拟 BSSID)；现场勘测方法；网络吞吐量；同频与邻频干扰；蜂窝规划(微蜂窝)；协调传输；信道堆栈。

4.4.7 定义和描述其他 WLAN 架构：WLAN 阵列；Mesh 网络；WLAN 云管理。

4.5 WLAN 部署类型 11

4.5.1 了解如下通用 WLAN 应用与设备的设计和部署要点：数据；语音；视频；实时定位系统(RTLS)；移动设备(平板电脑与智能手机)；高密部署。

5. 802.11 网络安全

5.1 IEEE 802.11 网络安全架构 13

5.1.1 了解和描述下列 IEEE 802.11 安全相关主题的优缺点、应用场合与部署。

传统无线网络安全机制：WEP 加密组；开放系统认证；共享密钥认证；MAC 地址过滤；SSID 隐藏。

当今无线网络安全机制： WPA-/WPA2 Enterprise；WPA-/WPA2 Personal；TKIP 与 CCMP 加密组；802.1X/EAP；预共享密钥(PSK)/密码认证；PPSK；WPS。

其他机制：设备安全管理协议(HTTPS、SNMPv3、SSH2)；RBAC；强制门户与访客网络；管理帧保护(802.11w)；快速安全漫游方法。

5.2 802.11 安全分析、性能分析与排错 14

5.2.1 对下面无线安全解决方案使用场合进行描述、解释。

WIPS：安全监控、抑制与报告；性能监控与报告；排错分析；协议分析仪；安全与性能监控；排错分析；集成式协议分析仪与独立式协议分析仪；

5.3 802.11 网络安全策略基础 14

5.3.1 描述以下通用安全策略要素：适用人员；风险评估；影响分析；安全审计；策略执行；监控、响应和报告；资产管理。

5.3.2 描述下列安全策略要素：设计和部署最佳实践；SOHO；SMB；企业；密码策略；可接受的用户策略(AUP)；培训需求；物理安全；社会工程学。

6. 802.11 RF 现场勘测

6.1 802.11 网络现场勘测基础 15

6.1.1 解释手动和预测性 RF 现场勘测的信息收集的重要性及相关流程(这些通常发生于 RF 现场勘测的准备期间)：业务需求信息收集；与经理和用户面谈；定义物理安全和数据安全需求；收集与勘测现场相关文档；记录现有网络现状；收集许可及分区需求；室内与室外信息；了解基础架构连通性及电源需求；了解射频覆盖需求；了解数据容量和客户端密度需求；VoWiFi 部署对延迟和抖动的要求；客户端连通性需求；天线使用考虑因素；跟踪系统考虑因素；WIPS 探测器考虑因素。

6.1.2 解释执行手动和预测性 RF 现场勘测设计的技术要点(这些通常发生于 RF 现场勘测期间)：定位和识别 RF 干扰源；确定使用的 AP 与天线类型；确定 AP 与天线的安装位置；确定 AP 的发射功率与信道分配；确定同频与邻频干扰；测试应用程序能否正常工作；根据设计需求测试性能参数。

6.1.3 描述手工和预测性 RF 现场勘测的报告及后续流程(这些通常发生于 RF 现场勘测完成后)：报告方法；客户的报告需求；硬件推荐和材料清单；覆盖与容量验证方面的应用分析。

6.2 802.11 网络现场勘测系统与设备 16

6.2.1 了解执行预测性现场勘测所要求的设备、应用程序与系统特性：预测性分析/模拟程序(也称为 RF 规划与管理工具)；WLAN 控制器的集成预测性现场勘测特性；现场勘测验证工具和/或应用程序；室内与室外现场勘测。

6.2.2 了解执行手动现场勘测所要求的设备、应用程序与系统特性：现场勘测硬件设备；频谱分析仪；协议分析仪；主动现场勘测工具和/或应用程序；被动现场勘测工具和/或应用程序；VoWiFi 现场勘测最佳实践；厂商客户端应用程序。

6.2.3 了解自管理 RF 技术所涉及的设备、应用程序和方法论：自动射频资源管理。

目　　录

第 1 章　无线标准、组织与基础概述……1
1.1　无线局域网历史回顾……2
1.2　标准组织……3
1.2.1　美国联邦通信委员会……4
1.2.2　国际电信联盟无线电通信部门……5
1.2.3　电子与电气工程师协会……6
1.2.4　互联网工程任务组……7
1.2.5　Wi-Fi 联盟……8
1.2.6　国际标准化组织……11
1.3　核心层、分布层与访问层……12
1.4　通信基础……13
1.4.1　理解载波信号……13
1.4.2　理解键控法……15
1.5　小结……19
1.6　考试要点……19
1.7　复习题……19

第 2 章　射频基础……23
2.1　射频信号的定义……24
2.2　射频特性……25
2.2.1　波长……25
2.2.2　频率……28
2.2.3　振幅……29
2.2.4　相位……30
2.3　射频传播行为……31
2.3.1　射频波传播……31
2.3.2　吸收……32
2.3.3　反射……32
2.3.4　散射……33
2.3.5　折射……34
2.3.6　衍射……35
2.3.7　损耗(衰减)……36
2.3.8　自由空间路径损耗……37
2.3.9　多径现象……38
2.3.10　增益(放大)……41
2.4　小结……42
2.5　考试要点……42
2.6　复习题……43

第 3 章　射频组件、测量与数学……47
3.1　射频组件……48
3.1.1　发射机……48
3.1.2　天线……49
3.1.3　接收机……50
3.1.4　主动辐射器(IR)……50
3.1.5　等效全向辐射功率……50
3.2　功率单位和相对单位……51
3.2.1　瓦特……52
3.2.2　毫瓦……52
3.2.3　分贝……52
3.2.4　dBi……54
3.2.5　dBd……55
3.2.6　dBm……55
3.2.7　平方反比法则……56
3.3　射频数学……57
3.3.1　10 与 3 规则……57
3.3.2　射频数学小结……64
3.4　本底噪声……65
3.5　信噪比……65
3.6　接收信号强度指示……66

3.7 链路预算 ……68
3.8 衰落容限/系统操作容限……70
3.9 小结 ……71
3.10 考试要点 ……72
3.11 复习题……73

第 4 章 射频信号与天线概念……77
4.1 方位图与正视图
(天线辐射包络图)……79
4.2 解析极化图 ……81
4.3 波束宽度 ……83
4.4 天线类型 ……85
4.4.1 全向天线 ……85
4.4.2 半定向天线 ……87
4.4.3 高度定向天线 ……89
4.4.4 扇形天线 ……90
4.4.5 天线阵列 ……91
4.5 可视视距 ……92
4.6 射频视距 ……92
4.7 菲涅耳区 ……93
4.8 地球曲率 ……96
4.9 天线极化 ……97
4.10 天线分集 ……97
4.11 多进多出……98
4.12 MIMO 天线 ……99
4.12.1 室内 MIMO 天线……99
4.12.2 室外 MIMO 天线……99
4.13 天线连接与安装……100
4.13.1 电压驻波比……100
4.13.2 信号损耗……101
4.13.3 天线安装……101
4.14 天线配件 ……104
4.14.1 电缆……105
4.14.2 接头……106
4.14.3 分离器……106
4.14.4 放大器……106
4.14.5 衰减器……107
4.14.6 避雷器……107
4.14.7 接地棒与接地线 ……109
4.15 小结……110
4.16 考试要点……110
4.17 复习题……111

第 5 章 IEEE 802.11 标准 ……115
5.1 IEEE 802.11 原始标准……117
5.2 批准通过的 IEEE 802.11-2007
修正案……119
5.2.1 802.11b……120
5.2.2 802.11a……120
5.2.3 802.11g……121
5.2.4 802.11d……124
5.2.5 802.11h……124
5.2.6 802.11i……125
5.2.7 802.11j……126
5.2.8 802.11e……127
5.3 批准通过的 Post-2007 修正案…128
5.3.1 802.11r-2008 ……128
5.3.2 802.11k-2008……128
5.3.3 802.11y-2008……129
5.3.4 802.11w-2009……129
5.3.5 802.11n-2009……130
5.3.6 802.11z-2010……130
5.3.7 802.11u-2011……130
5.3.8 802.11v-2011……131
5.3.9 802.11s-2011 ……131
5.4 IEEE 802.11 修正案草案……132
5.4.1 802.11p……132
5.4.2 802.11aa ……132
5.4.3 802.11ac ……133
5.4.4 802.11ad……133
5.4.5 802.11ae ……133
5.4.6 802.11af……133
5.4.7 802.11ah……134
5.5 已经失效的修正案……134
5.5.1 802.11F……134
5.5.2 802.11T ……135

5.6 802.11m 任务组……136
5.7 小结……137
5.8 考试要点……137
5.9 复习题……138

第 6 章 无线网络与扩频技术……143
6.1 ISM 频段……145
6.1.1 900MHz ISM 频段……145
6.1.2 2.4GHz ISM 频段……146
6.1.3 5.8GHz ISM 频段……146
6.2 UNII 频段……146
6.2.1 UNII-1(低)频段……147
6.2.2 UNII-2(中)频段……147
6.2.3 UNII-2 扩展频段……147
6.2.4 UNII-3(高)频段……148
6.3 3.6GHz 频段……148
6.4 4.9GHz 频段……149
6.5 未来的 Wi-Fi 频段……149
6.6 窄带传输与扩频传输……150
6.7 跳频扩频……152
6.7.1 跳频序列……152
6.7.2 驻留时间……153
6.7.3 跳变时间……153
6.7.4 调制……153
6.8 直序扩频……154
6.8.1 DSSS 数据编码……154
6.8.2 调制……155
6.9 分组二进制卷积码……155
6.10 正交频分复用……156
6.10.1 卷积编码……157
6.10.2 调制……157
6.11 2.4GHz 信道……158
6.12 5GHz 信道……160
6.13 相邻信道、非相邻信道与重叠信道……162
6.14 吞吐量与带宽……163
6.15 通信抗逆力……164
6.16 小结……164
6.17 考试要点……165
6.18 复习题……165

第 7 章 无线局域网拓扑结构……169
7.1 无线网络拓扑结构……170
7.1.1 无线广域网(WWAN)……170
7.1.2 无线城域网(WMAN)……171
7.1.3 无线个人域网……171
7.1.4 无线局域网……172
7.2 802.11 拓扑结构……172
7.2.1 接入点……173
7.2.2 客户端……173
7.2.3 集成服务……173
7.2.4 分布系统……174
7.2.5 无线分布系统……175
7.2.6 服务集标识符……177
7.2.7 基础服务集……177
7.2.8 基础服务集标识符……178
7.2.9 基本服务区……178
7.2.10 扩展服务集……179
7.2.11 独立基础服务集……181
7.2.12 Mesh 基础服务集……182
7.3 802.11 配置模式……183
7.3.1 接入点模式……183
7.3.2 客户端模式……184
7.4 小结……184
7.5 考试要点……185
7.6 复习题……185

第 8 章 802.11 媒介访问……191
8.1 CSMA/CA 与 CSMA/CD……192
8.2 冲突检测……193
8.3 分布式协调功能(DCF)……193
8.3.1 帧间间隔(IFS)……194
8.3.2 Duration/ID 字段……194
8.3.3 载波侦听……195
8.3.4 随机回退计时器……196
8.4 点协调功能……197
8.5 混合协调功能……198

8.5.1 增强的分布式信道访问……198
8.5.2 HCF 控制信道访问……199
8.6 块确认……199
8.7 Wi-Fi 多媒体……200
8.8 通话公平机制……201
8.9 小结……202
8.10 考试要点……203
8.11 复习题……203

第 9 章 802.11 MAC 架构……207
9.1 数据包、帧和位……209
9.2 数据链路层……209
9.2.1 MAC 服务数据单元……209
9.2.2 MAC 协议数据单元……210
9.3 物理层……210
9.3.1 PLCP 服务数据单元……210
9.3.2 PLCP 协议数据单元……210
9.4 802.11 和 802.3 互操作性……211
9.5 三种 802.11 帧类型……212
9.5.1 管理帧……212
9.5.2 控制帧……213
9.5.3 数据帧……213
9.6 信标管理帧……214
9.6.1 被动扫描……215
9.6.2 主动扫描……216
9.7 认证……217
9.7.1 开放式系统认证……217
9.7.2 共享密钥认证……218
9.8 关联……219
9.8.1 认证状态与关联状态……219
9.8.2 基本速率与支持速率……220
9.8.3 漫游……220
9.8.4 重关联……221
9.8.5 解除关联……222
9.8.6 解除认证……222
9.9 确认帧……223
9.10 分片……224
9.11 保护机制……225
9.11.1 RTS/CTS……227
9.11.2 CTS-to-Self……228
9.12 数据帧……229
9.13 电源管理……230
9.13.1 主动模式……230
9.13.2 节电模式……230
9.13.3 流量指示图……230
9.13.4 传输流量指示消息……231
9.13.5 通告流量指示消息……232
9.13.6 WMM 节电模式与 U-APSD……232
9.13.7 802.11n 电源管理……234
9.14 频段引导……234
9.15 小结……235
9.16 考试要点……235
9.17 复习题……236

第 10 章 无线局域网架构……241
10.1 无线局域网客户端设备……242
10.1.1 无线射频(网)卡类型……242
10.1.2 无线射频(网)卡芯片组……246
10.1.3 客户端实用程序……246
10.2 管理、控制和数据平面……249
10.2.1 管理平面……249
10.2.2 控制平面……250
10.2.3 数据平面……250
10.3 WLAN 架构……250
10.3.1 自治型 WLAN 架构……250
10.3.2 无线网络管理系统……252
10.3.3 集中式 WLAN 架构……253
10.3.4 分布式 WLAN 架构……259
10.3.5 统一无线局域网结构……260
10.4 专业无线局域网基础设施……260
10.4.1 无线工作组网桥……260
10.4.2 无线局域网网桥……261
10.4.3 家用无线路由器……263

10.4.4 无线局域网 Mesh 接入点……264
10.4.5 无线局域网阵列……265
10.4.6 虚拟接入点系统……266
10.4.7 实时定位系统……266
10.4.8 Wi-Fi 语音……267
10.5 小结……268
10.6 考试要点……269
10.7 复习题……269

第 11 章 无线局域网部署和垂直市场……275
11.1 常见无线局域网应用与设备部署注意事项……276
11.1.1 数据……276
11.1.2 语音……276
11.1.3 视频……277
11.1.4 实时定位服务……277
11.1.5 移动设备……278
11.2 企业数据接入与终端用户的移动性……278
11.3 网络延伸到远端……279
11.4 建筑物之间的桥接……279
11.5 无线运营商——最后一英里的数据交付……280
11.6 小型办公室/家庭办公室……280
11.7 移动办公网络……281
11.8 教育/教室使用……281
11.9 工业——仓储和制造……282
11.10 医疗保健——医院和办公室……282
11.11 市政网络……283
11.12 热点——公共网络接入……283
11.13 交通网络……285
11.14 执法网络……285
11.15 快速应急网络……286
11.16 固网与移动网的融合……286
11.17 无线局域网与健康……287
11.18 无线局域网供应商……287
11.19 小结……289
11.20 考试要点……290
11.21 复习题……290

第 12 章 无线局域网排错……295
12.1 第 2 层重传问题……296
12.1.1 射频干扰……297
12.1.2 多径现象……300
12.1.3 邻频干扰……302
12.1.4 低信噪比……304
12.1.5 不匹配的功率设置……305
12.1.6 近/远问题……306
12.1.7 隐藏节点……307
12.2 802.11 信号覆盖要点……310
12.2.1 动态速率调整……310
12.2.2 漫游……313
12.2.3 三层漫游……316
12.2.4 同频干扰……317
12.2.5 信道复用/多信道体系结构……318
12.2.6 单信道体系结构……322
12.3 容量与覆盖……325
12.3.1 超大尺寸的覆盖蜂窝……326
12.3.2 物理环境……326
12.4 语音和数据……326
12.5 性能……327
12.6 天气影响……328
12.7 小结……329
12.8 考试要点……329
12.9 复习题……330

第 13 章 无线局域网安全架构……335
13.1 无线局域网安全基础……337
13.1.1 数据保密……338
13.1.2 认证、授权与统计……339
13.1.3 分段……339
13.1.4 监控与安全策略……339
13.2 传统的无线局域网安全机制……340
13.2.1 传统的认证方式……340

13.2.2 静态 WEP 加密 ……341
13.2.3 MAC 地址过滤……343
13.2.4 SSID 隐藏 ……343
13.3 强健安全机制……344
13.3.1 强健安全网络……345
13.3.2 认证与授权……346
13.3.3 PSK 认证 ……346
13.3.4 私有 PSK 认证 ……347
13.3.5 802.1X/EAP 架构 ……348
13.3.6 EAP 类型 ……350
13.3.7 生成动态加密密钥……352
13.3.8 四次握手……352
13.3.9 WPA/WPA2-Personal 解决方案……353
13.3.10 TKIP 加密 ……353
13.3.11 CCMP 加密 ……354
13.4 流量分段 ……355
13.4.1 虚拟局域网……355
13.4.2 基于角色的访问控制 …356
13.5 基础架构安全……357
13.5.1 物理安全……357
13.5.2 接口安全……357
13.6 VPN 无线安全……358
13.6.1 三层 VPN……358
13.6.2 SSL VPN……358
13.6.3 VPN 部署……359
13.7 访客 WLAN 安全……359
13.8 小结 ……361
13.9 考试要点 ……361
13.10 复习题 ……362

第 14 章 无线攻击、入侵监控与安全策略……367
14.1 无线攻击 ……368
14.1.1 非法无线设备……368
14.1.2 对等攻击……370
14.1.3 窃听……372
14.1.4 加密破解……374
14.1.5 认证攻击 ……374
14.1.6 MAC 欺骗 ……376
14.1.7 管理接口漏洞 ……376
14.1.8 无线劫持 ……377
14.1.9 拒绝服务攻击 ……378
14.1.10 厂商漏洞攻击 ……379
14.1.11 社会工程学 ……379
14.2 入侵监控……380
14.2.1 无线入侵检测系统 ……380
14.2.2 无线入侵防御系统 ……382
14.2.3 移动 WIDS……384
14.2.4 频谱分析仪 ……385
14.3 无线安全策略……385
14.3.1 一般性安全策略 ……386
14.3.2 功能性安全策略 ……386
14.3.3 信息安全法规 ……386
14.3.4 无线局域网安全策略建议 ……387
14.4 小结……388
14.5 考试要点……388
14.6 复习题……388

第 15 章 射频现场勘测基础……393
15.1 无线局域网现场勘测概述 ……394
15.1.1 客户简报 ……394
15.1.2 业务需求 ……395
15.1.3 容量与覆盖要求 ……395
15.1.4 现有的无线网络 ……397
15.1.5 基础架构连接性 ……398
15.1.6 安全期望 ……400
15.1.7 访客接入 ……400
15.2 文档与报告……401
15.2.1 表格与客户文档 ……401
15.2.2 交付报告 ……402
15.2.3 附加报告 ……403
15.3 垂直市场……404
15.3.1 室外勘测 ……404
15.3.2 美观 ……405

15.3.3 政府……405
15.3.4 教育……406
15.3.5 医疗……406
15.3.6 热点……406
15.3.7 零售业……407
15.3.8 仓储业……407
15.3.9 制造业……407
15.3.10 多租户大楼……408
15.4 小结……408
15.5 考试要点……408
15.6 复习题……409

第 16 章 现场勘测系统与设备……415
16.1 现场勘测定义……416
16.1.1 协议分析与频谱分析…416
16.1.2 频谱分析……417
16.1.3 覆盖分析……420
16.1.4 接入点布局与配置……423
16.1.5 应用分析……425
16.2 现场勘测工具……425
16.2.1 室内现场勘测工具……425
16.2.2 室外现场勘测工具……427
16.3 覆盖分析……429
16.3.1 手工覆盖分析……429
16.3.2 预测性覆盖分析……430
16.3.3 自组无线局域网……431
16.4 小结……432
16.5 考试要点……432
16.6 复习题……433

第 17 章 以太网供电(PoE)……437
17.1 以太网供电(PoE)历史回顾……438
17.1.1 非标准 PoE……438
17.1.2 IEEE 802.3af 修正案…438
17.1.3 IEEE 802.3-2005 标准第 33 条款……438
17.1.4 IEEE 802.3at-2009……439
17.2 PoE 设备概述……439
17.2.1 受电设备……439
17.2.2 供电设备……440
17.2.3 端接式供电设备……441
17.2.4 中跨式供电设备……443
17.2.5 供电设备引脚分配……445
17.3 规划与部署 PoE……446
17.3.1 功率规划……446
17.3.2 冗余……447
17.3.3 802.11n 与 PoE……448
17.4 小结……448
17.5 考试要点……449
17.6 复习题……449

第 18 章 高吞吐量(HT)与 802.11n……453
18.1 802.11n-2009 修正案……455
18.2 MIMO 技术……457
18.2.1 射频链……457
18.2.2 空间复用……458
18.2.3 MIMO 分集……459
18.2.4 空时分组编码……460
18.2.5 循环移位分集……461
18.2.6 传输波束成形……461
18.3 HT 信道……462
18.3.1 20MHz HT 与 20MHz Non-HT 信道……463
18.3.2 40MHz HT 信道……464
18.3.3 40MHz 不兼容……465
18.3.4 保护间隔……466
18.3.5 调制编码方案……467
18.4 HT 物理层……468
18.4.1 Non-HT 传统格式……469
18.4.2 HT 混合格式……469
18.4.3 HT 绿地格式……470
18.5 HT MAC 层……470
18.5.1 MSDU 聚合(A-MSDU)……470
18.5.2 MPDU 聚合(A-MPDU)……471
18.5.3 块确认……472

18.5.4 缩减帧间间隔……473
18.5.5 HT 电源管理 ……473
18.6 HT 工作模式 ……474
18.6.1 20/40MHz 信道工作模式 ……474
18.6.2 HT 保护模式(0～3)……474
18.6.3 RTS/CTS 与 CTS-to-Self……475
18.7 小结 ……476
18.8 考试要点……476
18.9 复习题……476
附录 A 复习题答案 ……481
附录 B 略语表、首字母缩略词及功率管理规定 ……511
附录 C 关于本书附加学习工具……525

第 1 章 无线标准、组织与基础概述

在该章中，你将学习以下内容：

- √ 无线局域网历史回顾
- √ 标准组织
  - 美国联邦通信委员会(FCC)
  - 国际电信联盟无线电通信部门(ITU-R)
  - 电子与电气工程师协会(IEEE)
  - 互联网工程任务组(IETF)
  - Wi-Fi 联盟(Wi-Fi Alliance)
  - 国际标准化组织(ISO)
- √ 核心层、分布层与访问层
- √ 通信基础

无线局域网(Wireless Local Area Network，WLAN)的漫长历史可以追溯到 20 世纪 70 年代，其根源可以追溯到 19 世纪。本章将对无线局域网技术的历史进行概述。学习一项新技术似乎颇具挑战性，因为需要去熟悉大量新的缩略语、缩写、术语和概念。学习任何课题的关键在于掌握基础。无论是学习驾车、开飞机还是安装无线计算机网络，所掌握的基本规则、原理和概念都将构成今后学习的基础。

IEEE 802.11 技术一般称为 Wi-Fi，它是一种采用射频(Radio Frequency，RF)以提供局域网(LAN)通信的标准技术。IEEE(Institute of Electrical and Electronics Engineer，电子与电气工程师协会)将 802.11-2007 标准作为指导和规范无线局域网发展的准则。许多标准组织和监管机构共同对无线技术及相关行业进行监督与管理，了解这些组织有助于理解 IEEE 802.11 技术的工作原理，也有助于理解这些标准如何发展而来以及成因。

在对无线网络有了一定了解后，读者可能希望或需要阅读不同组织制定的标准。本章将对这些标准组织进行介绍，并对它们创建的文档进行概述。

除了介绍监管和规范 Wi-Fi 技术的标准组织外，本章还将讨论无线局域网技术与基本网络设计模型之间的关系。最后，本章将回顾通信技术与数据键控的基础知识。尽管 CWNA 考试不涉及这方面的内容，掌握它们对理解无线通信大有裨益。

1.1 无线局域网历史回顾

19 世纪，包括迈克尔·法拉第(Michael Faraday)、詹姆斯·克拉克·麦克斯韦(James Clerk Maxwell)、海因里希·鲁道夫·赫兹(Heinrich Rudolf Hertz)、尼古拉·特斯拉(Nikola Tesla)、大卫·爱德华·休斯(David Edward Hughes)、托马斯·爱迪生(Thomas Edison)和伽利尔摩·马可尼(Guglielmo Marconi)在内的众多发明家与科学家开始进行无线通信的试验。这些先驱者发现并创立了与电磁射频概念有关的诸多理论。

第二次世界大战期间，美军首次将无线网络技术应用到通信中。这种无线技术使用射频作为传输介质，采用保密的加密技术穿越敌方战线传送作战计划。今天的无线局域网广泛应用了扩频无线技术，后者最初在二战期间获得专利，不过直到差不多 20 年之后才开始投入使用。

1970 年，美国夏威夷大学研制成功世界上第一种无线网络。这种网络称为 ALOHAnet，它以无线方式在夏威夷群岛之间传输数据。在无线共享介质上，ALOHAnet 采用称为 ALOHA 的局域网通信开放系统互连模型二层协议，工作频段为 400MHz。一般认为，ALOHAnet 采用的技术不仅用于 802.3 以太网 CSMA/CD(Carrier Sense Multiple Access with Collision Detection，载波侦听多路访问/冲突检测)介质访问控制技术，也构成了 802.11 无线局域网 CSMA/CA(Carrier Sense Multiple Access with Collision Avoidance，载波侦听多路访问/冲突避免)介质访问控制技术的基础。第 8 章将详细介绍 CSMA/CA 技术。

20 世纪 90 年代，商用网络厂商推出了低速无线数据网络设备，多数设备工作在 900MHz 频段。1991 年，IEEE 开始讨论对无线局域网技术进行标准化。1997 年，IEEE 批准通过了 802.11 原始标准，它也是本书所讨论的无线局域网技术的基础。

传统 802.11 技术的部署时间为 1997～1999 年，主要用于仓储与制造业环境，使用无线

条码扫描仪进行低速数据采集。1999 年，IEEE 批准通过了数据速率更高的 802.11b 修正案。802.11b 标准支持最高 11Mbps 的数据速率，且成本较之以前更低，这在 SOHO 市场引发了无线家用路由器的销售狂潮。用户很快习惯了家用无线网络带来的便捷，并开始要求雇主在工作场所也提供无线网络接入。大公司和中小企业最初对 802.11 技术有些抵触，不过它们很快意识到在企业中部署 802.11 无线技术的价值。

如果询问一般用户什么是 802.11 无线网络，他们可能会感到迷惑和不解，因为多数人习惯将这项技术称作 Wi-Fi。Wi-Fi 是一个市场术语，世界各地的人们使用“Wi-Fi”作为 802.11 无线网络的代名词。

术语 Wi-Fi 的含义

很多人误认为 Wi-Fi 是“无线保真”(wireless fidelity)的缩写，如同 hi-fi 代表“高保真”(high fidelity)一样。其实 Wi-Fi 只是用来推广 802.11 无线局域网技术的商用名称。由于 IEEE 关于无线通信的架构标准有些模糊，厂商根据各自的理解对 802.11 标准进行解释，这导致不同厂商生产的设备虽然都符合 IEEE 802.11 标准，但这些设备之间却无法相互通信。鉴于此，人们创建了 WECA(Wireless Ethernet Compatibility Alliance，无线以太网兼容性联盟)以对 IEEE 标准做进一步定义，以确保不同厂商设备之间的互操作性。WECA 目前已更名为 Wi-Fi 联盟，它选择“Wi-Fi”这个术语作为市场推广的品牌。Wi-Fi 联盟负责确保无线设备之间的互操作性。为符合 Wi-Fi 兼容性要求，厂商必须将自己的产品送交 Wi-Fi 联盟的测试实验室，并由后者对其进行全面测试，以确保产品符合 Wi-Fi 认证的各项兼容性要求。有关术语 Wi-Fi 起源的更多信息请参阅 Wi-Fi Net News 网站: http://wifinetnews.com/archives/2005/11/wi-fi_stands_fornothing_and_everything.html。

不仅有大量的企业级应用使用 Wi-Fi 无线接口，笔记本电脑、蜂窝电话、相机、电视、打印机等众多消费类设备也采用了 Wi-Fi 技术。2010 年，Wi-Fi 芯片组的出货量超过 3.5 亿。预计在之后的几年，Wi-Fi 芯片的年销售量将超过 10 亿。

据 Wi-Fi 联盟统计，2009 年第 10 亿块 Wi-Fi 芯片组被卖出。Wi-Fi 联盟的一项调查显示，68%的用户无法忍受没有 Wi-Fi 的生活。自 1997 年 IEEE 批准 802.11 原始标准以来，802.11 技术的发展越来越快，Wi-Fi 已成为世界文化的一部分。

1.2　标准组织

本章讨论的各种标准组织共同对无线网络行业进行监管和规范。

ITU-R(International Telecommunication Union Radio communication sector，国际电信联盟无线电通信部门)以及 FCC(Federal Communications Commission，美国联邦通信委员会)等各国的通信监管机构负责制定规章制度，以约束用户使用无线电发射机的行为。这些机构管理通信频率、功率水平和传输方式，并共同规范日益增长的无线用户群体。

IEEE 负责制定网络设备兼容与共存的标准，IEEE 标准必须遵循 FCC 等通信监管机构的规定。

IETF 负责制定互联网标准，其中有很多标准已经与无线网络和安全协议及标准整合。

Wi-Fi 联盟(Wi-Fi Alliance)负责对无线网络设备进行认证测试，以确保它们符合 802.11 无线局域网通信协议(如 IEEE 802.11-2007 标准)。

ISO(International Organization for Standardization，国际标准化组织)创建了 OSI(Open System Interconnection，开放系统互连)模型，后者是数据通信的体系结构模型。

以下各节将分别介绍这些机构和组织。

1.2.1 美国联邦通信委员会

简而言之，美国联邦通信委员会(FCC)的职责是管理美国境内以及往来美国的通信。FCC 根据美国《通信法》成立于 1934 年，负责监管美国各州与国际间的无线电、电视、电话、卫星和电报通信。在无线网络领域，FCC 负责管理无线通信中使用的无线电信号。FCC 对 50 个州、哥伦比亚特区以及美国属地拥有通信管辖权。多数国家和地区都有与 FCC 职能类似的监管机构。

一般来说，FCC 与其他国家的监管机构负责管理两类无线通信：需要牌照与无需牌照。二者的区别在于，用户可以免费使用无需牌照的频段进行通信，即安装无线系统之前不需要进行申请牌照的程序。监管机构通常从以下 5 个方面管理需要牌照与无需牌照的通信：

- 频率
- 带宽
- 主动辐射器(Intentional Radiator，IR)的最大输出功率
- 最大 EIRP(Equivalent Isotropically Radiated Power，等效全向辐射功率)
- 用途(室内和/或室外)

真实场景

采用无需牌照的频段进行通信的利弊

如前所述，用户在使用需要牌照的频段进行通信之前必须申请牌照，而牌照申请的费用极高。无需牌照的频段的一个主要优点是可以免费使用该频段传输数据。尽管不必付费，用户仍需遵守各种通信规定与限制。也就是说，使用无需牌照的频段传输数据是免费的，但依然有规可循。

由于无需牌照的频段对所有人开放，该频段经常拥挤不堪，不同用户之间的传输可能会相互干扰。但是，只要其他用户遵守该频段的通信管理规定，那么即使他们的设备干扰到你的传输，你也无法为此而诉诸法律。

总之，FCC 与其他监管机构负责制定约束用户射频传输行为的规定，标准组织根据这些规定制定相应的标准。监管机构和标准组织相互合作，以满足无线行业迅速增长的需求。

FCC 制定的规则公布在《美国联邦监管法典》(Code of Federal Regulations，CFR)中，该法典分为 50 个主题，每年进行更新。与无线网络有关的内容包含在第 47 主题“无线电通信”中，后者被划分为许多部分，第 15 部分“射频设备”描述了 802.11 无线网络的规则条例。

第 15 部分又被进一步划分为若干子部分与小节。一个完整例子如 47CFR15.3。

本书附录 B 中列出了 FCC 有关 2.4GHz ISM 与 5GHz UNII 频段传输功率的规定。更多信息请参阅 www.fcc.gov 和 http://wireless.fcc.gov。

1.2.2　国际电信联盟无线电通信部门

通信领域存在一个全球性的射频频谱管理体系，联合国指定国际电信联盟无线电通信部门(ITU-R)承担全球频谱管理的任务。ITU-R 维护一个全球性的频率分配数据库，并通过 5 大行政区协调频谱管理。

5 大行政区划分如下：

行政区 A：北美与南美

美洲国家电信委员会(Inter-American Telecommunication Commission，CITEL)

www.citel.oas.org

行政区 B：西欧

欧洲邮电行政会议(European Conference of Postal and Telecommunications Administrations，CEPT)

www.cept.org

行政区 C：东欧与北亚

区域通信联合体(Regional Commonwealth in the filed of Communications，RCC)

www.en.rcc.org.ru

行政区 D：非洲

非洲电信联盟(African Telecommunications Union，ATU)

www.atu-uat.org

行政区 E：亚洲与大洋洲

亚太电信组织(Asia-Pacific Telecommunity，APT)

www.aptsec.org

在各大行政区内，各国政府所属的射频通信监管机构负责管理本国的射频频谱，例如：

- 澳大利亚：澳大利亚通信与媒体管理局(ACMA)
- 日本：电波产业会(ARIB)
- 新西兰：经济发展部(MED)
- 美国：联邦通信委员会(FCC)

请注意，各个国家和地区的通信管理体制可能有所不同。例如，欧洲与北美的射频管理规定相差很大。当部署无线局域网时，请花些时间学习当地监管机构的规定与政策。因为全球各地的相关规定不同，参考各地不同的管理规定也超出了本书的讨论范围，CWNA 考试也不会考察 FCC 或任何其他国家的射频规定。

有关 ITU-R 的更多信息请参阅 www.itu.int/ITU-R/。

1.2.3 电子与电气工程师协会

电子与电气工程协会(IEEE)是一个拥有超过 40 万名会员的全球性专业组织，其使命是“鼓励技术创新，谋求人类福祉”。对网络从业人员而言，IEEE 意味着制定通信所用的标准。

IEEE 最为人所熟知的或许是它制定的局域网标准，即 IEEE 802 项目。

802 项目只是 IEEE 众多的项目之一，不过它是本书讨论的唯一一个 IEEE 项目。

IEEE 项目被划分为若干个工作组(working group)，工作组致力于开发解决特定问题或需求的标准。例如，IEEE 802.3 工作组负责制定以太网标准，IEEE 802.11 工作组负责制定无线局域网标准。每个工作组成立时都会被分配一个数字，分配给无线工作组的数字 11 表示该工作组属于 IEEE 802 项目成立的第 11 个工作组。

IEEE 还成立了任务组(task group)，后者负责对工作组制定的现有标准进行补充和完善。每个任务组按顺序被分配一个单字母(如果所有单字母都已使用，就为任务组分配多个字母)，这些字母被添加到标准数字的后面(如 802.11a、802.11g、802.3af)。某些字母闲置不用。例如，不使用字母 o 和 l，以免与数字 0 和 1 混淆。还有一些字母也不会分配给任务组，以免与其他标准混淆。例如，IEEE 并未将字母 x 分配给 802.11 任务组，因为“802.11x”容易与 802.1X 标准混淆，而且人们已经习惯采用 802.11x 作为 802.11 系列标准的总称。

有关 IEEE 的更多信息请参阅 www.ieee.org。

请记住，与很多其他标准类似，IEEE 标准是描述技术规程和设备功能的书面文档。遗憾的是，人们通常以自己的方式理解并应用标准，因此各厂商生产的早期设备之间经常互不兼容，早期的 802.11 设备也是如此。

第 5 章“IEEE 802.11 标准”详细介绍了 802.11 标准与修正案的历史。CWNA 考试(PW0-105)以目前最新版本的 802.11 标准(即 802.11-2007 标准)为基础。读者可通过以下链接下载 802.11-2007 标准：http://standards.ieee.org/getieee802/download/802.11-2007.pdf。

1.2.4　互联网工程任务组

互联网工程任务组，也就是 IETF，是以促进互联网更好地发展为目标的国际会员制组织。IETF 的使命在 RFC3935 文件中是这样描述的，即“以生产高质量、相关的技术和工程文件，以影响人们的设计、使用和管理互联网的方式，使互联网更好地工作。这些文件包括协议标准、最佳实践和各种类型的信息文件”。IETF 不收取任何会费，任何人都可以注册和参加 IETF 会议。

IETF 是国际互联网协会(ISOC)的 5 个主要团体之一。ISOC 包括以下团体：

- 互联网架构委员会(IAB)
- 互联网名称与数字地址分配机构(ICANN)
- 互联网工程指导小组(IESG)
- 互联网研究专门工作组(IRTF)

IETF 分为 8 个主题领域：应用程序、通用部分、互联网、业务和管理、实时应用程序和基础设施、路由、安全和传输。图 1-1 显示了 ISOC 的层次结构和 IETF 主题领域的细目。

图 1-1　ISOC 层级架构

IESG 提供对 IETF 的活动和互联网标准进程的技术管理。IETF 由大量工作组构成，每个组解决特定的主题。IETF 工作组由 IESG 创建，并被分配一个特定的主题。针对工作组，并没有正式的投票进程。工作组的决定也是基于粗略的共识或由工作组内的协议做出的。

工作组的工作结果通常是形成一个被称为 RFC 的文档。RFC 实际上并不像它的名字描述的那样是请求给予评论的文档，而是声明。大多数 RFC 描述的网络协议、服务或策略可能演变为一种互联网标准。RFC 按顺序依次编号，一个号码一旦被指定后，就将永远不重复使用。RFC 可能会更新或辅之以较高编号的 RFC。例如，Mobile IPv4 是 RFC 3344 描述的，在 RFC 4721 中进行了更新。RFC 3344 被创建时，使 RFC 3220 被淘汰。在 RFC 文档的顶部，它指出是否它由另一个 RFC 更新，或使其他 RFC 被淘汰。

不是所有的 RFC 都会成为标准。针对其与互联网标准化过程的关系，RFC 分为以下几种状态：信息性状态、实验性状态、标准轨道状态或历史状态。如果 RFC 处于标准轨道状态，未来它可能演变成提出标准状态、标准草案或正式互联网标准。当 RFC 成为正式标准后，会保留原 RFC 编号，但同时会增加 "STD xxxx"标记。STD 编号与 RFC 编号并非一对一的关系，可能 STD 编号会注明多个 RFC 文档编号。

IETF 产生的很多协议标准、最佳实践和信息文档影响到 WLAN 安全。在第 13 章“802.11 网络安全体系结构”中你将了解到由 IETF RFC 3748 定义的可扩展身份验证协议(EAP)。

1.2.5 Wi-Fi 联盟

Wi-Fi 联盟(Wi-Fi Alliance)是一个全球性的非营利行业协会，拥有 350 多家会员企业，致力于推动无线局域网的发展。Wi-Fi 联盟的主要任务之一是向市场推广 Wi-Fi 品牌，并增进消费者对新兴 802.11 技术的了解。由于 Wi-Fi 联盟获得了巨大的市场成功，全球 4.5 亿 Wi-Fi 用户在第一时间就认可了 Wi-Fi 标志(如图 1-2 所示)。

图 1-2 Wi-Fi 标志

Wi-Fi 联盟的主要职责是提供认证测试，以实现无线局域网设备之间的互操作性。在 802.11 标准发展的初期，Wi-Fi 联盟对标准中某些模棱两可的条款做了进一步定义，并制定了一系列准则，以确保不同厂商生产的设备可以相互兼容。如图 1-3 所示，通过 Wi-Fi 认证测试的设备将获得一张 Wi-Fi 互操作性证书(Wi-Fi Interoperability Certificate)，证书中详细列出了该设备的 Wi-Fi 认证信息。

Wi-Fi CERTIFIED™ Interoperability Certificate　Certification ID: WFAxxxxx

This certificate lists the capabilities and features that have successfully completed Wi-Fi Alliance interoperability testing. Additional information about Wi-Fi Alliance certification programs is available at www.wi-fi.org/certification_programs.php.

Certificate Date: date_of_last_product_certification
Company: company_name
Product: product_name
Model/SKU#: model_number/sku
Primary Category: primary_product_category

Tested Spatial Streams	Dual-Band Concurrent 2.4GHz	5GHz
Receive	3	3

IEEE Standard
IEEE 802.11a
IEEE 802.11b
IEEE 802.11e
IEEE 802.11g
IEEE 802.11h
IEEE 802.11n
Optional 802.11n Capabilities
- Short Guard Interval
- Greenfield Preamble
- TX A-MPDU
- STBC
- 40 MHz operation in 2.4 GHz with coexistence mechanisms
- 40 MHz operation in 5 GHz
- HT Duplicate (MCS 32)

Security
WPA™ - Enterprise/Personal
WPA2™ - Enterprise/Personal
EAP Type(s)
EAP-TLS
EAP-TTLS/MSCHAPv2
PEAPv0/EAP-MSCHAPv2
PEAPv1/EAP-GTC
EAP-SIM
EAP-AKA
EAP-FAST
Vendor EAP Type(s)
EAP-TLS
EAP-TTLS/MSCHAPv2
PEAPv0/EAP-MSCHAPv2
PEAPv1/EAP-GTC
EAP-SIM
EAP-AKA
EAP-FAST

Multimedia
WMM®
WMM Power Save

Special Features
Wi-Fi Protected Setup™
- PIN
- PBC
- Internal Registrar (APs only)
- External Registrar support options
Wi-Fi Direct™

Convergence
Voice – Personal
CWG-RF

For more information: www.wi-fi.org/certification_programs.php

图 1-3　Wi-Fi 互操作性证书

Wi-Fi 联盟成立于 1999 年 8 月，最初名为 WECA，2002 年 10 月改为现名。

自 2000 年 4 月开始互操作性测试后，Wi-Fi 联盟已经对 10 000 多种 Wi-Fi 设备进行了认证，其多个 Wi-Fi CERTIFIED™项目覆盖基本连接、安全、QoS(quality of service，服务质量)等多个方面。Wi-Fi 联盟授权世界 8 个国家 14 个独立的测试实验室对厂商设备进行互操作性测试。Wi-Fi CERTIFIED™项目对于互操作性的界定，一般以 IEEE 802.11-2007 标准及其修正案定义的重要内容作为依据。802.11 任务组中的许多工程师实际也是 Wi-Fi 联盟的赞助会员，不过请注意，IEEE 和 Wi-Fi 联盟是两个独立的组织。IEEE 802.11 任务组负责制定无线局域网标准，而 Wi-Fi 联盟负责开发互操作性认证项目。Wi-Fi CERTIFIED™项目包括以下认证项目：

核心技术与安全　核心技术与安全认证项目对 802.11a/b/g 或/和 802.11n 技术进行互操作性认证测试，以确保基本的无线数据传输符合要求。每台设备根据其能力被测试。表 1-1 列出了 4 种不同的核心 Wi-Fi 传输技术所使用的频率及其支持的最大数据传输率。

表 1-1　4 种 Wi-Fi 传输技术

Wi-Fi 技术	频　段	最大数据率
802.11a	5GHz	54Mbps
802.11b	2.4GHz	11Mbps
802.11g	2.4GHz	54Mbps
802.11n	2.4GHz、5 GHz、 2.4GHz 或 5GHz (可选), 或 2.4GHz 和 5GHz (同时支持)	450Mbps

每台经过认证的设备至少要支持一个频段，也可以支持两个频段。CWNA 考试并不使用 802.11a、802.11a/b/g/n 等术语，不过由于 Wi-Fi 联盟的基础认证项目已深入人心，这些术语已被业界普遍接受。

尽管 802.11n 理论上支持 600Mbps，但实际上截止本书撰写时并没有支持 600Mbps 的产品面世，因此 450Mbps 仍然是被测试的最大数据传输率。

此外，如果要测试设备的传输能力，需要该设备支持 RSN(Robust Security Network，强健安全网)，其最初定义在 IEEE 802.11i 修正案中。设备必须支持 WPA、WPA2-personal 或 WPA2-enterprise。此外，企业级设备必须支持 EAP 协议，其用来验证无线设备或用户的身份。第 13 章将详细介绍 WPA 和 WPA2 安全机制。

WMM——多媒体 WMM(Wi-Fi Multimedia，Wi-Fi 多媒体)以最初定义在 IEEE 802.11e 修正案中的 QoS 机制为基础。启用 WMM 的 Wi-Fi 网络将各种应用产生的流量划分为不同的优先级。如果网络中的接入点与客户设备都支持 WMM，语音或视频等时敏应用产生的流量将优先使用半双工射频介质进行传输。所有支持 802.11n 的核心认证产品都被强制要求支持 WMM。对于支持 802.11a、b 或 g 的核心认证设备而言，WMM 认证则是可选的。第 9 章将深入讨论 WMM 机制。

WMM-PS——多媒体 WMM-PS(WMM Power Save，WMM 节电)管理并调整客户设备上 Wi-Fi 无线接口处于休眠状态的时间，以便延长设备的电池续航能力。对条码扫描仪和 VoWiFi 电话等手持设备而言，降低电池耗电至关重要。客户设备和接入点必须都支持 WMM-PS 才能使用节电特性。第 9 章将深入讨论 WMM-PS 与传统的节电机制。

WPS——安全 家庭与小型企业用户可以采用 WPS(Wi-Fi Protected Setup，Wi-Fi 保护设置)方便地自动配置 WPA 与 WPA2 安全。除使用个人识别码(PIN)之外，用户还能通过接入点与客户设备上的按键轻松地为网络设置安全保护。

Wi-Fi Direct Wi-Fi Direct 使 Wi-Fi 设备无需接入点就可以互联，使它更容易使用打印、分享、同步和显示功能。Wi-Fi Direct 使移动电话、照相机、打印机、PC 和游戏设备可以建立一对一的连接，甚至使一小组设备连接起来。Wi-Fi Direct 配置简单(在某些情况下跟按下某个按钮一样简单)。与其他通过 Wi-Fi 认证的设备一样，Wi-Fi Direct 可以提供相同的性能和传输范围，并可以利用 WPA2 确保安全。

CWF-RF——多媒体 CWG-RF(Converged Wireless Group-RF Profile，融合无线组-射频性能)由 Wi-Fi 联盟和 CTIA(Cellular Telecommunications and Internet Association，蜂窝电信与互联网协会)共同开发，后者目前称为无线协会(The Wireless Association)。CWG-RF 为融合话机(converged handset)中采用的 Wi-Fi 无线接口与蜂窝无线电定义了性能指标，以确保两种技术不会相互干扰。目前，所有经过 CTIA 认证的手持话机均包含该认证。

Voice Personal——应用 Voice Personal 项目定义了如何为家庭和小型企业的 Wi-Fi 网络提供增强的语音应用。这种网络包括一个接入点和不同设备(如电话、个人计算机、打印机和其他消费者电子设备)产生的混合语音与数据流量，并支持多达 4 个并行电话呼叫。接入点与客户设备都必须通过该认证才能支持上述应用。

随着 802.11 技术的发展，Wi-Fi 联盟还会开发新的 Wi-Fi CERTIFIED™项目。Wi-Fi 联盟的下一个认证项目或许是 Voice Enterprise，它将定义如何在企业环境下提供增强的语音应用。Voice Enterprise 项目可能将对 802.11r 修正案(快速安全漫游)与 802.11k 修正案(无线资源测量)中的某些内容进行测试。请注意，所有通过 Wi-Fi 认证的产品都要满足核心技术和安全需求，这意味着 Voice Enterprise 认证产品必须支持 WPA2 和 EAP 协议。

Wi-Fi 联盟与 Wi-Fi CERTIFIED 项目

有关 Wi-Fi 联盟的更多信息请参阅 www.wi-fi.org，该网站包含很多文档、FAQ 和白皮书，来描述组织机构以及有关认证项目的其他信息。下面 5 份白皮书来自 Wi-Fi 联盟，读者可以在 www.sybex.com/go/cwna3e 上找到它们：

- Wi-Fi CERTIFIED for WMM - Support for Multimedia Applications with Quality of Service in Wi-Fi Networks
- WMM Power Save for Mobile and Portable Wi-Fi CERTIFIED Devices
- Wi-Fi CERTIFIED Voice-Personal: Delivering the Best End-User Experience for Voice over Wi-Fi
- Wi-Fi CERTIFIED n: Longer-Range, Faster-Throughput, Multimedia-Grade Wi-Fi Networks
- The State of Wi-Fi Security: Wi-Fi CERTIFIED WPA2 Delivers Advanced Security to Homes, Enterprises and Mobile Devices

1.2.6　国际标准化组织

国际标准化组织(ISO)是一个全球性的非政府组织，它界定商业、政府和社会需求，并与其他机构合作开发标准，ISO 制定的标准被很多团体和组织所采用。ISO 负责创建 OSI 模型，后者自 20 世纪 70 年代末起成为计算机数据通信的参考标准。

国际标准化组织的缩写为何是 ISO 而非 IOS？

ISO(International Organization for Standardization)并非一个拼写错误的缩略语，它源于希腊单词 isos，意为“平等的”。由于各国对缩略语的翻译可能不同，ISO 决定采用一个单词而非缩略语来表示其名称。为此，很容易理解一个标准组织为何选择“平等的”作为自己的名字。

OSI 模型是数据通信的基础，了解 OSI 模型对网络从业人员而言至关重要。OSI 模型由以下 7 层构成，如图 1-4 所示。

IEEE 802.11-2007 标准仅在 OSI 模型的物理层与数据链路层的 MAC 子层定义了通信机制，本书将详细讨论 802.11 技术在这两层的应用。

图 1-4 OSI 模型

读者应具备有关 OSI 模型的基本知识以阅读本书并准备 CWNA 考试。了解 OSI 模型各层的功能以及数据通信在不同层之间的传输过程十分重要。如果不太熟悉 OSI 模型的概念，请在参加 CWNA 考试前花些时间通过互联网或优秀的网络基础教程回顾一下 OSI 模型。有关 ISO 的更多信息请参阅 www.iso.org。

1.3 核心层、分布层与访问层

在谈到网络架构时，如果读者曾参加过网络课程或阅读过网络设计方面的书籍，那么或许听说过*核心层*(core layer)、*分布层*(distribution layer)与*访问层*(access layer)这些术语。正确的网络设计对于任何网络拓扑都是至关重要的。网络的核心层由高速骨干网构成，它相当于网络中的高速公路。核心层负责在重要的数据中心或分布区之间传输大量信息，如同高速公路连接城市与都会区一样。

核心层既不对流量进行路由，也不对数据包进行操作，它的任务是进行高速交换。核心层一般设计有冗余解决方案，以保证数据包能快速可靠地交付。网络的分布层将流量路由或发送到较小的节点簇，或者发送到网络的其他部分。

分布层在 VLAN(Virtual LAN，虚拟局域网)和子网之间路由流量，它类似于以中速在城市或都会区中分流交通的国道。

网络的访问层以低速将流量直接传输给终端用户或终端节点，它类似于直达最终用户的县道或一般街道。也就是说，访问层确保数据包的最终交付。注意，这里的速度是一个相对概念。

由于流量负载与吞吐量要求不同，数据从访问层传输到核心层时，速度和吞吐量将随之提高。不过，更高的速度与吞吐量往往意味着更高的成本。

在住宅区和社区学校之间修筑一条高速公路并不实用，同理，在类似纽约和波士顿这样

的两个大城市之间仅修筑一条双车道公路作为主干道也是不切实际的。同样的道理也适用于网络设计。核心层、分布层和访问层都有其特定的功能和用途，读者应理解无线网络与这种网络设计模型之间的关系。

无线组网时，既可以采用点对点解决方案，也可以采用点对多点解决方案。多数无线网络采用点对多点解决方案，并为每个客户端提供网络接入。这种解决方案通常在访问层使用，以便为终端用户提供网络连接。绝大多数情况下，802.11 无线网络都在访问层实现。第 10 章“无线局域网架构”将介绍自治型接入点解决方案、协作型接入点以及基于 WLAN 控制器的轻量接入点解决方案，并讨论三者之间的区别。所有接入点都部署在访问层，而 WLAN 控制器通常部署在分布层或核心层。轻量接入点将 802.11 无线流量通过隧道传输给 WLAN 控制器。

无线桥接链路一般用于在建筑物之间提供网络连接，类似于连接相邻地区交通的国道。无线桥接以无线方式连接两个独立的有线网络，而分布层通常负责在网络之间路由数据流量。一般来说，无线桥接链路无法达到核心层要求的传输速度与距离，然而它非常适于在分布层使用。802.11 桥接链路是无线技术在分布层实现的一个例子。

尽管无线技术一般不在核心层使用，但是必须记住，不同规模的企业对传输速度和距离的要求相距甚远，一个人眼中的分布层或许就是另一个人眼中的核心层。袖珍公司可能不会使用任何有线设备，而将无线作为连接整个网络的方式。可将专有的高带宽无线网桥与 802.11 网状网部署视为无线技术在核心层的实现。

1.4　通信基础

尽管人们认为 CWNA 认证是认证无线网络专家(CWNP)项目中的一项基础级认证，但它绝不是计算机行业中的基础级认证。多数 CWNA 考生都具备信息技术领域的经验，不过他们的背景和经验却迥然不同。

与那些经过多年系统培训的专家不同，大多数计算机专业人员根据自己的方式接受教育和培训。

人们在接受教育时，通常会选择学习与自身利益或工作直接相关的技能和知识，而往往忽视基础知识的学习。随着知识的积累和技能的增长，人们逐渐意识到学习基础知识的重要性。

很多计算机行业的从业人员都知道，比特在数据通信中是通过电线或电波传输的，他们也了解可以采用某种形式的电压变化或电波波动来区分比特。不过如果继续追问，多数人就不清楚电信号或电波的具体工作原理了。

下面将回顾与无线通信直接或间接相关的基本通信原理。了解这些概念有助于更好地理解无线通信的工作方式以及本行业使用的术语。

1.4.1　理解载波信号

构成数据的最小单位是比特，发射机采用某种方式发送 0 和 1，以便在两地之间传输数

据。交流或直流信号本身不具备传输数据的能力，不过如果信号发生哪怕是微小的波动或变化，发送端和接收端就可以将信号解析出来，从而成功地收发数据。转换后的信号可以区分 0 和 1，一般将其称为载波信号。调整信号以产生载波信号的过程称为调制。

可以对电波的 3 种分量进行调制以产生载波信号，这 3 种分量是振幅、频率和相位。

本章对数据传输有关的电波基础知识进行回顾，第 2 章“射频基础”将深入讨论无线电波。

所有无线电通信都采用某种方式调制并传输数据。将所传输的无线电信号以一定方式调制，就可以将 AM/FM 无线电、蜂窝电话和卫星电视信号中的数据编码。普通人并不关心信号是如何调制的，他们只关心设备是否正常工作。不过，如果希望成为一名优秀的无线网络管理员，就需要深入了解两台设备通信的具体方式。为理解载波信号与数据编码，本章其余各节将首先介绍电波的基本性质，然后对数据编码原理做一概述。

1. 振幅和波长

射频通信的基本过程如下：射频发射机产生无线电信号，并被另一端的接收机拾取或监听。射频波与海洋或湖泊中的波浪类似。波主要由波长和振幅两部分构成，如图 1-5 所示。

图 1-5 波的波长与振幅

振幅是波的高度、力度或能量。当波浪从大海袭向岸边时，大波浪的力量比小波浪要强得多。发射机的工作原理与之相同，不过它发射的是无线电波。电波越小，越不易被接收天线识别。电波越大，所产生的电信号越大，越容易被接收天线拾取。接收机根据振幅来区分波的大小。

波长是两个相邻波的相似点之间的距离。测量波时，一般将两个波峰之间的距离作为波长。幅度和波长都是波的属性。

2. 频率

频率描述了波的行为。波从产生它的源点处向外传播。波传播速度的快慢称为频率，更具体地说，频率是 1 秒钟内产生的波的数量。一个人站在码头上计算海浪多久拍击码头一次时，他实际是在计算海浪拍击码头的频率。无线电波也是如此，不过它的传播速度比海浪快

得多。如果试图计算无线网络中使用的无线电波的频率，那么在海浪拍击码头一次的时间里，数十亿次无线电波已经拍击了码头。

3. 相位

相位是一个相对术语，它描述了两个同频波之间的关系。为测定相位，将波长划分为 360 份，每一份称为 1°(如图 1-6 所示)。我们将度作为波传播的起始时间，如果一个波在 0° 点时开始传播，另一个波在 90° 点时开始传播，就称二者 90° 异相。

图 1-6　两个相同的波，不过它们彼此 90° 异相

理想情况下，一台设备产生波并将其无损地传输给另一台设备，不过现实并非如此。射频环境中存在大量干扰源与障碍物，它们会影响波的传输。第 2 章将介绍可能影响波的完整性以及终端之间通信的外界因素。

时间与相位

假设将两只手表暂停，并将二者的时间设定在中午。中午时启动第一只表，一小时后启动第二只表。第二只表比第一只表慢一小时，而且无论经过多久，第二只表总比第一只表慢一小时。虽然两只表的运行时间都是一天 24 小时，但它们彼此并不同步。波的异相与表的不同步类似。异相的两个波实际是不同时间开始传播的两个波，它们的周期都是 360°，但两个波彼此并不同相(或同步)。

1.4.2　理解键控法

收发器将数据信号发送出去后，必须对其进行调控，以便接收端能正确地识别 0 和 1。这种调控信号使其表示不同数据的方式称为键控法(keying method)。键控法将信号转换为载波信号，数据经过编码以便传输。

下面将介绍 3 种键控法，它们是幅移键控(Amplitude-Shift Keying，ASK)、频移键控(Frequency-Shift Keying，FSK)和相移键控(Phase-Shift Keying，PSK)。键控法又称调制技术，它采用两种方式表示数据：

当前状态(current state)　这种方式采用信号的当前值(当前状态)来区分 0 和 1。注意这

里的“current”并不表示与电压相对的“电流”，而表示“目前”之意。当前状态技术指定某个值或当前值代表二进制 0，另一个值代表二进制 1。对于某个具体的时间点而言，信号的当前状态决定了该时间点的二进制值。例如，可以用一扇普通的门代表 0 和 1，并每隔一分钟检查门处于开启还是关闭状态。处于开启状态的门表示 0，处于关闭状态的门表示 1。也就是说，门的当前状态(开启或关闭)决定了它所代表的是 0 还是 1。

状态转换(state transition) 这种方式采用信号的变化(转换)来区分 0 和 1。例如，状态转换技术可以采用波在某一特定时刻的相位改变代表 0，波在某一特定时刻的相位不变代表 1。对于某个具体的时间点而言，信号的变化或不变决定了该时间点的二进制值。下面的“3. 相移键控”将具体解释这个问题，不过为简单起见，这里仍然使用门的例子。我们依然每隔一分钟检查门的状态。此时，处于移动状态的门(正在开启或正在关闭)表示 0，处于静止状态的门(或是开启，或是关闭)表示 1。也就是说，门的转换状态(移动或静止)决定了它所代表的是 0 还是 1。

1. 幅移键控(ASK)

幅移键控通过改变信号的幅度或高度来表示二进制数据，它属于当前状态技术，即分别采用两种不同的幅度代表二进制 0 和 1。图 1-7 显示了采用幅移键控对 ASCII 字母 K 进行调制。幅度大的波被解析为二进制 1，幅度小的波被解析为二进制 0。

图 1-7 幅移键控示例(ASCII 大写字母 K)

这种键控法根据幅度的变化表示所传输的数据。采用幅移键控技术的接收端首先将接收到的信号划分为若干个时间段，这些时间段称为符号周期(symbol period)。接收端在符号周期内对波进行抽样以判定波的幅度，并根据幅度值确定接收到的二进制值。

本书后续章节将告诉读者，无线信号不但无法预测，而且容易受到多种干扰源的干扰。噪声或干扰通常会对信号幅度造成影响。如果信号幅度因噪声而改变，将导致接收端误判接收到的数据值，因此采用幅移键控时必须谨慎。

2. 频移键控(FSK)

频移键控通过改变信号的频率来表示二进制数据，它属于当前状态技术，即分别采用两种不同的频率代表二进制 0 和 1(如图 1-8 所示)。这种键控法根据频率的变化表示所传输的数据。接收端在符号周期内对信号抽样以判定波的频率，并根据频率值确定接收到的二进制值。

图 1-8　频移键控示例(ASCII 大写字母 K)

图 1-8 显示了采用频移键控对 ASCII 字母 K 进行调制。频率高的波被解析为二进制 1，频率低的波被解析为二进制 0。

某些传统的 802.11 无线网络部署采用频移键控。由于人们对通信速度的要求越来越高，频移键控需要采用更昂贵的技术才能支持高速传输，因此频移键控并不适合在目前的无线通信中使用。

为何我以前没有听说过键控法？

你其实听说过键控法，只是没有予以注意而已。采用调幅与调频技术的 AM/FM 广播让人们可以在家中或车中收听广播。广播电台将声音和音乐调制成发射信号，家中或车中的收音机再把它们解调出来。

3. 相移键控(PSK)

相移键控通过改变信号的相位来表示二进制数据，它是一种状态转换技术，即分别采用两种不同的相位代表二进制 0 和 1。这种键控法使用相位的变化表示所传输的数据。接收端在符号周期内对信号抽样以判定波的相位，并根据相位值确定接收到的二进制值。

图 1-9 显示了采用相移键控对 ASCII 字母 K 进行调制。以每个符号周期的起点作为参考点，相位改变被解析为二进制 1，相位不变被解析为二进制 0。

图 1-9　相移键控示例(ASCII 大写字母 K)

相移键控技术广泛用于 802.11-2007 标准定义的无线传输。接收端通常在符号周期内对信号进行抽样，并将当前抽样的相位与前一个抽样的相位进行比较以确定二者的差异。这种相位差(单位为°)称为*差分*(differential)，用于判定位值。

高级的相移键控技术可以在每个符号内编码多个位。除使用两个相位外，也可以使用 4 个相位表示二进制值。在这种表示法中，每个相位代表两个二进制值(00、01、10 或 11)而非一个二进制值(0 或 1)，这就缩短了传输时间。采用两个以上相位传输数据的相移键控技术称为*多进制相移键控*(Multiple Phase-Shift Keying，MPSK)。图 1-10 显示了采用多进制相移键控对 ASCII 字母 K 进行调制。从图中可以观察到 4 种可能的相位变化，每种相位变化被解析为两位数据而不是一位数据。与图 1-9 相比，图 1-10 采用的多进制相移键控技术减少了符号时间。

图 1-10 多进制相移键控示例(ASCII 大写字母 K)

了解有关 802.11 技术与 Wi-Fi 行业的更多信息

通读本书对初步了解 Wi-Fi 技术大有神益。由于 802.11 无线局域网技术发展很快，推荐你参阅以下信息：

Wi-Fi 联盟 前面曾经介绍过，Wi-Fi 联盟负责维护所有 Wi-Fi 认证，它代表了 Wi-Fi 行业的呼声。Wi-Fi 联盟的网址是 www.wi-fi.org，网站的知识中心提供了非常优秀的资源。

CWNP 读者可以在认证无线网络专家(CWNP)认证项目中找到大量学习资源，如用户论坛、无线局域网白皮书等。CWNP 网站(www.cwnp.com)提供了有关厂商中立无线网络认证最权威的信息。

各大无线局域网厂商的网站 尽管 CWNA 考试和本教程从厂商中立的角度推广 802.11 技术，各大厂商的网站同样提供了大量关于 Wi-Fi 网络解决方案的优秀信息。本书对许多主要的无线局域网厂商做了介绍，读者可以在第 11 章“WLAN 部署与纵向市场”中找到大部分主流厂商网站的完整列表。

Wi-Fi 博客 近年来 Wi-Fi 主题的个人博客大量涌现，其中很棒的有 CWNE #84 Andrew vonNagy: http://revolutionwifi.blogspot.com。

1.5　小结

本章回顾了无线网络的历史，并介绍了与无线网络行业有关的 4 个主要组织的职能与责任：

- FCC 与其他国家和地区的监管机构
- IEEE
- IETF
- Wi-Fi 联盟

为使读者了解网络基本概念与 802.11 技术，我们讨论了以下概念：

- OSI 模型
- 核心层、分布层与访问层

为使读者了解无线设备收发数据的基本原理，我们介绍了电波与调制：

- 载波信号
- 振幅
- 波长
- 频率
- 相位
- 键控法，包括幅移键控(ASK)、频移键控(FSK)与相移键控(PSK)

牢固掌握电波与调制技术的知识对于射频通信的排错十分重要，有助于网络工程师理解问题实质并找出解决方案。

1.6　考试要点

了解 4 个行业组织。理解各国通信监管机构、IEEE、IETF 与 Wi-Fi 联盟的职责。

理解核心层、分布层与访问层。了解 802.11 技术部署在基础网络设计模型的哪一层。

理解波长、频率、幅度与相位。了解各种射频特性的定义。

理解调制的概念。幅移键控、频移键控与相移键控是 3 种载波信号调制技术。

1.7　复习题

复习题的答案见附录 A。

1. 802.11 technology is typically deployed at which fundamental layer of network architecture?
   A. Core
   B. Distribution
   C. Access
   D. Network
2. Which organization is responsible for enforcing maximum transmit power rules in an unlicensed

frequency band?

A. IEEE

B. Wi-Fi Alliance

C. ISO

D. IETF

E. None of the above

3. 802.11 wireless bridge links are typically associated with which network architecture layer?

A. Core

B. Distribution

C. Access

D. Network

4. The 802.11-2007 standard was created by which organization?

A. IEEE

B. OSI

C. ISO

D. Wi-Fi Alliance

E. FCC

5. What organization ensures interoperability of WLAN products?

A. IEEE

B. ITU-R

C. ISO

D. Wi-Fi Alliance

E. FCC

6. What type of signal is required to carry data?

A. Communications signal

B. Data signal

C. Carrier signal

D. Binary signal

E. Digital signal

7. Which keying method is most susceptible to interference from noise?

A. FSK

B. ASK

C. PSK

D. DSK

8. Which sublayer of the OSI model's Data-Link layer is used for communication between 802.11 radios?

A. LLC

B. WPA

C. MAC

D. FSK

9. While performing some research, Janie comes across a reference to a document titled RFC3935. Which of the following organization's website would be best to further research this document?

A. IEEE

B. Wi-Fi Alliance

C. WECA

D. FCC

E. IETF

10. The Wi-Fi Alliance is responsible for which of the following certification programs? (Choose all that apply.)

A. 802.11i

B. WEP

C. 802.11-2007

D. WMM

E. PSK

11. Which wave properties can be modulated to encode data? (Choose all that apply.)

A. Amplitude

B. Frequency

C. Phase

D. Wavelength

12. The IEEE 802.11-2007 standard defines communication mechanisms at which layers of the OSI model? (Choose all that apply.)

A. Network

B. Physical

C. Transport

D. Application

E. Data-Link

F. Session

13. The height or power of a wave is known as what?

A. Phase

B. Frequency

C. Amplitude

D. Wavelength

14. Samantha received a gaming system as a gift. She would like to have it communicate with her sister Jennifer's gaming system so that they can play against each other. Which of the following technologies, if deployed in the two gaming systems, should provide for the easiest configuration of the two systems to communicate with each other?

A. Wi-Fi Personal

B. Wi-Fi Direct

C. 802.11n

D. CWG-RF

E. Wi-Fi Protected Setup

15. A modulated signal capable of carrying data is known as what?

A. Data transmission

B. Communications channel

C. Data path

D. Carrier signal

16. Which of the following wireless communications parameters and usage are typically governed by a local regulatory authority? (Choose all that apply.)

A. Frequency

B. Bandwidth

C. Maximum transmit power

D. Maximum EIRP

E. Indoor/outdoor usage

17. The Wi-Fi Alliance is responsible for which of the following certification programs? (Choose all that apply.)

A. WECA

B. Voice Personal

C. 802.11v

D. WAVE

E. WMM-PS

18. A wave is divided into degrees. How many degrees make up a complete wave?

A. 100

B. 180

C. 212

D. 360

19. What are the advantages of using unlicensed frequency bands for RF transmissions? (Choose all that apply.)

A. There are no government regulations.

B. There is no additional financial cost.

C. Anyone can use the frequency band.

D. There are no rules.

20. The OSI model consists of how many layers?

A. Four

B. Six

C. Seven

D. Nine

第2章 射频基础

在该章中，你将学习以下内容：

- √ 射频信号的定义
- √ 射频特性
  - 波长
  - 频率
  - 振幅
  - 相位
- √ 射频传播行为
  - 射频波传播
  - 吸收
  - 反射
  - 散射
  - 折射
  - 衍射
  - 损耗(信号衰减)
  - 自由空间路径损耗
  - 多径(现象)
  - 增益(信号放大)

为了掌握正确地设计、部署和管理 802.11 无线网络的方法，不仅需要了解 OSI 模型和基本的网络概念，还需要扩宽很多其他的网络技术知识范畴。譬如，管理以太网，通常需要了解 TCP/IP 协议、桥接协议、交换和路由知识。因为绝大多数 802.11 无线网络是有线网络的“门户”，管理以太网的技巧也会有助于管理无线局域网。IEEE 定义的 802.11 通信机制仅涉及物理层和数据链路层的 MAC 子层。

为充分理解 802.11 技术，你需要对无线在 OSI 模型第一层的工作方式有清晰的概念，了解射频是如何在物理层通信的。

在有线局域网中，信号被巧妙地限制在有线线路内部，产生的结果是可以预料的。无线局域网却恰好相反。尽管射频信号适用于物理定律，但有时会以一种不可预料的方式进行传播。射频信号并非像有线网络一样被“套牢”在有线线路中，无线局域网是一种永远处于变化中的网络。

但这是否意味着你必须是一名专业的射频工程师，必须进行无线局域网现场勘测或对 Wi-Fi 网络进行监控？答案是当然不需要，但是如果很好地掌握了本章中定义的射频特性和射频传播行为，你的无线网络管理技能水平将会领先于他人。例如，你会知道为什么礼堂中的无线网络信号在空旷和满座的时候大相径庭？为什么无线局域网的性能在金属货架的仓储区域明显下降？为什么 5GHz 频率的无线信号比 2.4GHz 的覆盖范围更小？这些问题在掌握射频工作和表现原理的基本知识后将会迎刃而解。

有线通信的媒介是存在边界限制的。有边界的媒介会约束或限制信号(只有很少的信号泄露)。而无线通信在无边界的媒介中进行。无边界的媒介不会约束信号，信号可以在大气中向任何方向辐射(除非某些外部影响对信号限制或重定向)。

在本章中，我们首先定义什么是射频信号，然后讨论射频特性和射频传播行为。

2.1 射频信号的定义

本书不是一本专门讲解物理学定律的综合指南。然而，了解一些与射频(RF)相关的物理学基本概念对刚刚跨入无线网络门槛的人士是非常重要的。

电磁(EM)频谱(通常简称频谱)是指所有电磁辐射的频率范围。这种辐射以一种可以在介质或真空中自动传播的电磁波形式存在。常见的电磁波如伽马射线、X 射线、可见光、无线电波。无线电波是处于电磁频谱射频频段部分的电磁波，如图 2-1 所示。

射频信号起初是由射频发射器产生交流电(AC)信号，该交流信号通过铜导线(通常是同轴电缆)，再以电磁波的形式从天线单元辐射出去。于是无线信号就产生了。在天线中电子的流动状况(或称为电流)如果发生变化，也会使天线周围的电磁场发生变化。

与电流方向始终保持一致的直流电不同，交流电(AC)的电流大小和方向不断地循环变化。交流信号的形状(即波形)称为正弦波，如图 2-2 所示。常见的正弦波也可以在光、声音和海洋中看到。交流电电压的波动被称为循环或振荡。

图 2-1 电磁频谱

图 2-2 正弦波

射频电磁信号以一种持续的模式从天线辐射出去，这种模式具有某些特性，如波长、频率、振幅和相位。此外，电磁信号可以穿透物质媒介，也可以在绝对真空中传播。当射频信号在真空中传播时，时速与光速相同，即 299 792 248 米/秒，或 186 000 英里/秒。

为简化使用光速的数学计算，我们通常近似地将光速等于 300 000 000 米/秒。本书中所指的光速均使用这个近似值。

射频信号传播时会有多种行为，也被称为传播行为。本章后面将讨论射频传播行为，如吸收、反射、散射、折射、衍射、增强和衰减等。

2.2 射频特性

这些物理学特性存在于每个射频信号中：

- 波长
- 频率
- 振幅
- 相位

下面对每一个特性进行详细阐述。

2.2.1 波长

如前所述，射频信号就是在正负电压之间持续转换的交流电。交流电的每次循环或振荡

被定义为从上到下再到上的一次变化，或者从正到负再到正的一次变化。

波长是指相邻两个波峰或波谷之间的距离，如图 2-3 所示。简而言之，波长就是射频信号行进一个周期的距离。

图 2-3 波长

希腊字母 λ (lambda)代表波长，拉丁字母 f 代表频率。拉丁字母 c 代表光速(真空中)，它源自单词 celeritas(在拉丁语中意为速度)。

理解波长和频率之间的反比关系非常重要。这个反比关系中的三个元素分别是频率(f，单位赫兹或 Hz)、波长(λ，单位米或 m)和光速(c，常数 3×10^8 m/s)。下面的公式描述了这种关系：λ=c/f 或 f=c/λ。简单来说，就是射频信号频率越高波长越短，波长越长频率越低。

调幅电台的工作频率远比无线局域网 802.11 射频低，而卫星无线发射频率又大大高于无线局域网。例如，美国亚特兰大的 WSB-AM 广播电台工作频率为 750KHz，波长为 1312 英尺(400 米)，这是射频信号传播一个周期行进的距离。而某些导航卫星的工作频率非常高，接近 252GHz，波长不超过 0.05 英寸(1.2 毫米)。图 2-4 描述了这两种差异很大的射频信号。

射频信号在空气和介质中传输时，信号强度会下降(衰减)。通常人们认为频率越高、波长越短的电磁信号衰减得越快，但实际上 RF 信号的频率和波长特性不会导致衰减，距

图 2-4 频率 750KHz 信号与频率 252GHz 信号的波长比较

离才是衰减的主因。我们把天线能够接受能量的有效区域称为天线的孔径。天线的频率越高，天线孔径所能够捕获到的 RF 能量值越低。虽说频率和波长不会导致衰减，但从表象上来看，波长短频率高的信号衰减更快。理论上电磁信号在真空中可以永久传播，然而当信号穿越地球大气层时，其强度就可能衰减至无线接收灵敏度以下。信号也许可以到达接收机，但是强度太弱以至于无法识别。波长较长的电磁信号有可能在传递较长距离后仍可以保持振幅级别在接收机灵敏度之上。

从感觉上好像是波长较短的高频信号不如波长较长的低频信号传播距离远。但事实是高频信号变得太弱低于接收灵敏度，而低频信号传播到相同点时仍然可以保持在接收灵敏度之上。无线接收机就好比人的耳朵，当你听到播放音乐的车子开过来的时候，请注意你首先听到的将会是低音(低频)信号，这个例子表明波长较长的低频信号比波长较短的高频信号可以在距离我们更远的地方被听到。

大部分无线局域网射频卡工作在 2.4GHz 或 5GHz 频段，在图 2-5 中，可以看到两种不同频段的无线局域网射频波在传播一个周期时的差异。

图 2-5 2.45GHz 波长与 5.775GHz 波长

频率越高的无线信号通过不同的物理介质(如砖墙)时衰减得越快，了解这点对无线工程师来说很重要。首先，覆盖范围与信号在空气中衰减的程度(被称为自由空间路径损耗 FSPL，在本章后面讨论)有关；其次，频率越高，能够穿透障碍物的信号越少。例如，2.4GHz 的信号在穿越墙、玻璃和门之后的强度要比 5GHz 信号穿透相同障碍物后的强度要高。例如你在很远的地方就可以收听到调幅(低频)电台节目，但你只能在相对近得多的地方收听到调频(高频)电台节目。

2.45GHz 的信号波长约为 4.8 英寸(12 厘米)。5.775GHz 的信号波长约为 2 英寸(5 厘米)。

正如图 2-4 和图 2-5 所描绘的那样，不同频率的信号波长是不同的。信号循环一次，不同的波所传播的距离是不同的。图 2-6 显示了波长公式，单位是英寸和厘米。

波长(英寸) = 11.811/频率(GHz)

波长(厘米) = 30/频率(GHz)

图 2-6 波长公式

在整个自学指南中，可以看到很多不同的公式。在 CWNA 认证考试中，这些公式不必了解，本书中这些公式仅用于论证概念并作为 CWNA 学习的参考资料。

真实场景

信号的波长与设计有何关系？

通常人们认为频率越高、波长越短的电磁信号衰减得越快，但实际上 RF 信号的频率和波长特性不会导致衰减，距离才是衰减的主因。我们把天线能够接受能量的有效区域称为天线的孔径。天线的频率越高，天线孔径所能够捕获到的 RF 能量值越低。虽说频率和波长不会导致衰减，但从表象上来看，波长短频率高的信号衰减更快。在无线链路的其他方面相似的情况下，5GHz 射频卡比 2.4GHz 射频卡的无线覆盖区域小。

无线局域网设计包括现场勘测这部分。现场勘测的目的是确定信号的无线覆盖区域。因为波长不同，2.4GHz 的无线接入点比 5GHz 的无线接入点为无线客户端提供的覆盖区域更大，就是说如果要达到与 2.4GHz 无线接入点相同的覆盖效果，使用 5GHz 无线接入点就意味着要安装的数量更多。大多数企业级 Wi-Fi 厂商会销售具备 2.4GHz 和 5GHz 的双频无线接入点。针对双频 AP 的现场勘测规划和覆盖分析应该基于更高频率的 5GHz 信号，因为信号衰减得更快。

2.2.2 频率

如前所述，射频信号在交流电中以电磁信号的形式循环。你也已知信号在一个周期内传播的距离就是该信号的波长，但在某个时间内信号循环的密度又如何表达呢？

频率是指在特定时间间隔内某个特定事件重复的次数，标准测量单位是赫兹(Hz)。赫兹的名称起源于德国物理学家海因里希·鲁道夫·赫兹(Heinrich Rudolf Hertz)。某事件一秒钟发生一次就代表 1 赫兹。325Hz 即代表该事件每秒发生 325 次。另外，电磁波的频率也是用赫兹表达的。射频信号每秒循环的次数就是它的频率，如图 2-7 所示。

常见的频率单位还有：

1 赫兹(Hz)=每秒 1 周期

1 千赫(KHz)=每秒 10^3 周期

1 兆赫(MHz)=每秒 10^6 周期

1 吉赫(GHz)=每秒 10^9 周期

图 2-7 频率

所以当谈论到2.4GHz 无线局域网网卡时，我们应该知道它的信号每秒钟大约循环了24亿次！

反比关系

请记住波长与频率存在反比关系。下面的参考公式阐述了这个关系：

$\lambda = c/f$ 或 $f = c/\lambda$，其中 f 代表频率(单位为 Hz)，λ 代表波长(单位为 m)，c 代表光速(常数，3×10^8 m/s)。简单来说就是：射频信号频率越高，波长越短。波长越长，频率越低。

2.2.3 振幅

射频信号另一个重要的属性就是振幅，也可以被简单地称为信号强度或功率。在谈及无线传输时，振幅通常是指信号的强弱。振幅被定义为连续波的最大位移，射频信号的振幅值对应于电磁波的电场。当在示波器观察射频信号时，振幅就是由正弦波的正脊或负槽来表达的。

在图 2-8 中，λ 代表波长，a 代表振幅。第一个信号振幅大，第二个信号振幅小。

图 2-8 振幅

尽管信号强度(振幅)不同，频率和波长却保持恒定。许多因素可能导致射频信号振幅减小，即信号衰减，我们会在 2.3.7 节中讨论。

在无线局域网中，信号强度通常指传送振幅或接收振幅。传送振幅指离开射频发射器时的初始振幅。例如某无线接入点发射功率为 50mW，这指的就是传送振幅。馈线和连接头会导致传送振幅减小，而天线则使传送振幅增加。射频模块接收到的射频信号的强度通常指的就是接收振幅。通过现场勘测得到的信号强度其实就是接收振幅的一个例子。

不同类型的射频技术要求的传送振幅等级也不同。调幅电台需要传输高达 50 000W 的窄带信号，而大多数室内型的 802.11 无线接入点发射功率介于 1mW 和 100mW 之间。在本书后面的章节中，你会惊奇地发现 Wi-Fi 网卡可以接收几十亿分之一毫瓦强度的微弱信号！

2.2.4 相位

相位本身并非 RF 信号的私有属性，其涉及两路或多路同频信号之间的关系，也牵涉两路波形的波峰与波谷的位置关系。

相位可以根据距离、时间或角度进行测量。如果具备相同频率的两个信号的波峰在同一时刻精确对齐，它们就处于同相位置。相反，如果两个具有相同频率的信号的波峰在同一时刻没有精确对齐，它们就处于异相位置。图 2-9 阐述了这个概念。

图 2-9 相位关系

请务必了解无线接口卡接收到多路信号时，相位对振幅的影响。两路相位差为零的同相信号的振幅叠加后会导致接收信号强度大大增加，振幅甚至有可能增加两倍。如果信号的相位差达到180°(信号的波峰对应另一路信号的波谷)，信号将会彼此抵消，导致有效信号强度降到零。相位差具有累积效应。依据两路信号相位差的大小，接收信号强度可能增加或减弱。相位差对于理解某些射频现象非常重要，例如本章稍后讨论的多径现象。

通过www.sybex.com/go/cwna3e可以下载免费的基于Windows操作系统的程序EMANIM。使用这个程序做练习2.1，这个实验可以让我们理解信号间的相位关系如何导致振幅变化。

2.3 射频传播行为

当射频信号在空气或其他媒介中传播时，会有不同的行为方式。射频传播方式包括吸收、反射、散射、折射、衍射、自由空间路径损耗、多径现象、衰减和增益。

2.3.1 射频波传播

现在你已经学习了射频信号的许多特性，这对于理解射频信号离开天线后的射频行为很重要。如前所述，电磁波可以穿越绝对真空或不同材质的媒介。射频波移动的方式(即波的传播)会根据信号传播路径的媒介材质产生极大的变化。例如石膏板墙对射频信号的影响就与金属或混凝土对射频信号的影响不同。

信号的传播方式是导致射频信号产生变化的直接原因。当我们使用传播这个术语的时候，可以试着想象射频信号离开天线进行扩展。图2-10用地震做了一个很好的比喻，请注意观察从震中开始传播的同心的地震环。射频波与地震波具有极其相似的行为方式。无线信号移动的方式通常也称为传播行为(propagation behavior)。

图2-10 传播模拟

作为无线局域网工程师，要想确保无线接入点部署在合适的位置、正确进行天线选型并对无线网络健康进行监控，理解射频传播行为至关重要。

2.3.2 吸收

最常见的射频行为之一就是吸收(Absorption)。如果射频信号没有从物体上反弹，没有绕开或者穿透物体，那么信号就被 100%吸收了。大部分物质都会吸收射频信号，但吸收程度不同。

砖墙和混凝土墙会显著地吸收信号，而石膏板墙只会吸收很小部分的信号。水是另外一种能吸收很大程度信号的媒介。吸收是导致衰减的主要原因(衰减的概念会在本章后面进行讨论)。实际上那些含水率较高的物体(如纸张、硬纸板、金鱼缸等)都会吸收信号。

真实场景

用户密度

为了确定所需的无线接入点数量和安装位置，确保必要的射频覆盖，Akin 先生为学校演讲厅做了一次无线现场勘测。然而在 10 天后，Sandlin 教授举行了一场参加者众多的商业经济演讲。在这个演讲过程中，无线局域网的信号强度和质量都远不如那次现场勘测得到的数据。这是为什么？答案就是人体吸收了信号。

成人人体由 55%～65%的水组成。水可以导致吸收，从而导致信号衰减。用户密度是设计无线网络的重要参考因素，主要原因之一就是要考虑吸收的影响，而另一个原因是可用带宽。关于可用带宽我们将在第 15 章“射频现场勘测基础”中讨论。

2.3.3 反射

反射是最重要的射频传播行为之一。当波撞击到一个比波自身更大的光滑物体时，波可能会往另一个方向传递。这种行为就是反射(Reflection)。打个比方，小孩在人行道拍球，球反弹到路面后会改变方向。图 2-11 模拟了反射的一种场景，射在镜子上的激光会根据镜子角度的变化被反射到不同的方向。射频信号反射与此类似，但遇到不同的物体和材质，情况会有所不同。

有两种主要的反射类型：天波反射和微波反射。天波反射要求信号频率低于 1GHz，即波长要很长，该信号可在地球大气层中电离层的带电粒子表面进行反弹。这也是为什么在一个晴朗的夜晚，可以在美国北卡罗来纳州的夏洛特听到来自芝加哥的 WLA-AM 的调幅电台节目。

而微波信号的工作频率为 1GHz～300GHz，相对高频信号来说，其信号的波长要小很多，所以又称之为微波(microwave)。微波可以在更小物体上反弹，例如金属门。在无线局域网环境中我们要非常关注微波反射。在室外，微波会在一些大且光滑的物体表面反射，例如建筑物、道路、水体甚至地球表面。在室内，微波会被光滑表面反射，例如门、墙和文件柜

等。由金属构成的任何物体都会导致反射。还有些材料，如玻璃和混凝土也会导致反射。

图 2-11 反射模拟

反射是导致 802.11a/b/g 无线局域网性能下降的罪魁祸首

反射可能导致传统 802.11a/b/g 无线局域网出现严重性能问题。当波从天线发出后，会经过扩展和分散。当波的部分被反射时，新的波将从反射点生成。如果这些波全部到达接收方，将产生一种被称为多径现象的干扰。

多径现象会使接收信号的强度和质量下降，甚至导致数据损坏或者信号消失(多径现象将在稍后进行讨论。弥补多径现象负面影响的硬件解决方案，例如采用定向天线或者分集天线，我们会在第 4 章中讨论)。

尽管反射和多径现象可能是传统 802.11a/b/g 无线局域网的头号敌人，然而 802.11n 无线接口卡可以通过 MIMO 天线和高级数字信号处理技术(DSP)，对多径现象加以利用。802.11n 机制会在第 18 章中阐述。

在某些案例中，反射可以被规划。有个叫 Netrepid 的无线工程公司受雇使用无线网桥连接两栋建筑物。经过现场勘测后他们发现一栋建筑物挡住了两个网桥的直线路径。然而 Netrepid 还是想办法让两个建筑物通过无线信号连到了一起。他们利用旁边一幢有玻璃幕墙的办公大楼进行信号反射，并测试表明经玻璃表面反射的信号足够可靠。

2.3.4 散射

你知道天空呈现蓝色的原因吗？这是因为光的波长小于大气分子。天空泛蓝的大气现象也被称为瑞利散射(Rayleigh Scattering)。波长较短的蓝色光被大气中的气体吸收并在所有方向辐射。这是另一种被称为散射(Scattering)的射频传播行为。

散射很容易被描述成多路反射。当电磁信号的波长大于信号将要通过的媒介时，多路反射就会发生。

有两种类型的散射。第一类散射对信号的质量和强度影响不大，当射频信号在穿过媒介时，个别电磁波被媒介中的微小颗粒反射。例如大气中的烟雾和沙漠中的尘暴会导致这种类型的散射。

当射频信号入射到某些粗糙不平的表面时，将被反射到多个方向，这种现象属于第二类散射。铁丝网围栏、树叶以及岩石地形通常会引起这种形式的散射。入射到粗糙表面的主信号被分解为多路反射信号，这将导致主信号的质量下降，甚至破坏接收信号。

图 2-12 显示的是一个闪光灯照到迪斯科舞厅镜面球体后被反射的情景。请注意主要的信号波束被多条振幅较低的光束完全取代，并被传播到多个不同的方向。

图 2-12 散射模拟

2.3.5 折射

射频信号除了可能被吸收或者反弹(通过反射或散射)外，在特定条件下，射频信号还会发生弯曲，即**折射**(Refraction)。折射的直接定义就是射频信号在穿越不同密度媒介时发生弯曲，致使波传播方向发生变化。由于大气影响的结果，射频折射现象经常发生。

在进行长距离户外桥接链路计算时，你可能要关注折射率的影响，即 k 因子。k 因子等于 1 表明射频信号没有发生弯曲。k 因子小于 1，例如 2/3，表明信号向地球外侧弯曲。k 因子大于 1，表明信号朝地球表面弯曲。通常大气条件下的 k 因子为 4/3，这意味着信号会轻微向地球方向弯曲。

水蒸气、空气温度变化和空气压力变化是三个最重要的折射产生原因。在室外，射频信号通常会轻微向地球表面折射，然而大气的变化也可能导致信号远离地球。在长距离的室外无线桥接项目中，折射现象可能是需要重点关注的方面。另外，室内的玻璃和其他室内材料

也可能使射频信号产生折射。图 2-13 列举了折射的两个实例。

图 2-13 折射

2.3.6 衍射

衍射(Diffraction)是另一种会使射频信号产生弯曲的射频传播行为，但不要与折射混淆。衍射是射频信号在物体周边发生的弯曲现象(而折射是信号穿过媒介产生的弯曲)。衍射是当射频信号遇到障碍物时出现的弯曲和扩展情形。发生衍射的条件完全取决于障碍物的材质、形状、大小以及射频信号的特性，如极化、相位和振幅。

衍射通常是由于射频信号被局部阻碍所致，例如射频发射机与接收机之间有座小山或建筑物。遇到阻碍的射频波会沿着障碍物弯曲并绕过障碍物，此时的射频波会采用一条不同且更长的路径进行传输。没有遇到阻碍的射频波不会弯曲，仍然保持原来的较短的路径传输。图 2-14 描述的是河流中间有一块岩石，河流中的大部分水流保持不变，而那些遇到岩石的水流部分将会产生反射现象，有一些会利用衍射绕过岩石。

图 2-14 衍射模拟

位于障碍物正后方的区域称为射频阴影(RF shadow)。根据衍射信号方向的变化，射频阴

影可能成为覆盖死角或在此只能收到微弱信号。了解射频阴影的概念有助于正确选择天线的安装位置。固定在柱子或墙体上的接入点可能会导致出现虚拟的射频盲点。

2.3.7 损耗(衰减)

损耗，也称为衰减(Attenuation)，被描述成信号强度或振幅下降。信号在线缆或空气中传播时强度会下降。在通信的有线部分(射频电缆)，由于同轴电缆的阻抗或其他组件(如连接器)的影响，交流信号强度会下降。

在第 4 章，我们会讨论阻抗。阻抗被用来衡量对交流电电流所起的阻碍作用程度。你会了解到如果阻抗不匹配，就会导致信号在有线侧产生损失。

衰减通常是我们极力避免的，然而在极少数情况下，射频工程师可能会在射频系统的有线侧增加硬件衰减设备以满足功率规定或达到容量设计的目的。

射频信号通过天线辐射到空气中后，其强度会因为吸收、传播距离和多径现象的负面影响产生衰减。你已经知道射频信号穿过不同的媒介会被吸收，从而导致衰减。不同的材质通常会产生不同的衰减结果。2.4GHz 信号在穿透石膏板墙后的信号会下降 3dB，也就是说振幅会下降一倍。如果 2.4GHz 信号穿透砖墙后的信号会下降 12dB，也就是说振幅比原始振幅低 16 倍。正如之前讨论，水和包括煤渣砖之类在内的致密物质是射频吸收的主要原因，所有这些都会导致衰减。

练习 2.1

本练习中，你将使用 EMANIM 这个程序查看不同材质因吸收导致的衰减影响(该程序是免费的，可在 http://www.sybex.com/go/cwna3e 下载)。

(1) 下载后，通过双击“emanim_setup.exe”安装 EMANIM 程序。

(2) 单击 EMANIM 主菜单中的 Phenomenon。

(3) 单击 Sybex CWNA Study Guide。

(4) 单击 Exercise E。

当射频波穿过物质时，物质吸收了射频波的一部分，从而导致波幅减小。消光系数决定波被单位长度物质所吸收的数量。

(5) 在练习时尝试改变 Wave 1 穿越物质的长度和消光系数，观察它们如何影响吸收量。

衰减和增益在功率上的相对改变值都可以通过分贝(dB)进行测量，我们会在第 3 章中讨论。表 2-1 列出了不同材质的衰减值。

表 2-1 不同材质的衰减值对比

材　质	信号频率(2.4GHz)
地基墙	-15dB
砖、混凝土、混凝土块	-12dB
电梯或金属障碍物	-10dB

(续表)

材　质	信号频率(2.4GHz)
金属机架	-6dB
石膏板墙或石棉水泥板	-3dB
无色玻璃窗或玻璃门	-3dB
木门	-3dB
隔间墙	-2dB

表 2-1 中的内容仅供参考，不会在 CWNA 考试中出现。实际测试量会因为场点和环境因素不同而发生变化。

请务必了解射频信号振幅也会按照一个被称为自由空间路径损耗的距离函数减小。此外，反射可能产生多径现象等负面影响，致使信号衰减。

2.3.8 自由空间路径损耗

按照物理学规律，电磁信号除了因为障碍物、吸收、反射、衍射等等造成的衰减外，还会因为传播导致衰减。自由空间路径损耗(FSPL)是指射频波因自然扩展(通常也称波束发散，beam divergence)导致信号强度下降。射频信号能量离开天线被分散到更大的区域后，信号强度将减弱。

可以用气球来模拟阐述自由空间路径损耗。在气球充满氢气前，体积较小，气球的橡胶外膜较厚。而气球被充满气球后体积变大，橡胶外膜会变得非常薄。射频信号强度下降的方式与此类同。幸运的是，信号强度减弱程度并非呈线性，按对数函数下降的。因此振幅在第二个等距段下降的程度比第一段下降的小。例如，2.4GHz 的信号在头一个 100 米会下降 80dB，而在第二个 100 米只会下降 6dB。

下面是计算自由空间路径损耗的公式：

$FSPL=36.6+(20\log_{10}(f))+(20\log_{10}(D))$

FSDL=路径损耗(单位为 dB)

f=频率(单位为 MHz)

D=天线之间的距离(单位为英里)

$FSPL=32.44+(20\log_{10}(f))+(20\log_{10}(D))$

FSDL=路径损耗(单位为 dB)

f=频率(单位为 MHz)

D=天线之间的距离(单位为千米)

自由空间路径损耗公式仅供参考，不会在 CWNA 考试中出现。本书中的许多公式都会在网站 www.sybex.com/go/cwna3e 上以计算表格的方式出现。在网站 www.airspy.com/calculators.php 上可以进行 FSPL 等的在线射频计算。

还有一个被称为 6dB 法则的估算自由空间路径损耗的方法，使用起来相当简单(请记住 dB 是用来测量增益或衰减的，详见第 3 章)。6dB 法则是指传输距离加倍将导致信号衰减 6dB。表 2-2 显示了估算的路径损耗并确认了 6dB 法则。另外请注意相同条件下 5GHz 信号的衰减要比 2.4GHz 信号的衰减大。

表 2-2 自由空间路径损耗导致的衰减值

距离(km)	衰减(dB)	
	2.4GHz	5GHz
1	100.0	106.4
2	106.1	112.4
4	112.1	118.5
8	118.1	124.5

真实场景

自由空间路径损耗为何很重要？

所有的射频设备都有所谓的接收敏感等级。射频接收机在某个固定的振幅阀值之上可以正确地解释和接收信号。例如，你对某人耳语，必须确保你的声音可以被对方听到并理解。

如果接收的信号下降至射频设备接收敏感阀值以下，该设备就无法正确地感知并解释信号。自由空间路径损耗的概念也适合解释下面的情景：你在乘轿车旅行过程中收听调幅广播电台，当车驶离一定的距离后，你就无法听清在噪音背景下的音乐了。

为正确地接收并解释信号，信号不仅要足够强以便被接收，同时还要高于背景噪声。背景噪声通常也被称为本底噪声(noise floor)。接收信号必须强于背景噪声。还拿对某人耳语来做例子，尽管你的声音很大，可以被对方听到，但如果此时有救护车鸣笛呼啸通过，对方还是无法理解你正在说什么。对于在该阀值之上的信号，射频卡可以区分信号和背景噪声。

因为自由空间路径损耗的影响，室内无线局域网和室外无线桥接链路设计都要确保射频信号不要衰减到无线射频模块的接收敏感等级以下。在室内可以通过现场勘测完成这个目标，室外桥接链路设计需要进行链路预算(link budget)(现场勘测将在第 15 章和第 16 章阐述，链路预算在第 3 章阐述)。

2.3.9 多径现象

多径(Multipath)是一种传播现象，指两路或多路信号同时或相隔极短时间到达接收天线。由于波的自然扩展，在不同环境下反射、扩散、衍射和折射等传播行为也会有区别地发生。信号可能发生的反射、散射、折射、衍射等 RF 传播行为都可能导致同一信号发生多径现象。

在室内环境中，反射信号或回波可能由长走廊、墙体、桌子、地板、文件柜和许多其他的障碍引起。有着大量金属表面的室内环境，如钢架结构的机场、仓库和厂房也是众所周知多径现象比较严重的环境。反射是诱发多径现象的主要原因。在室外平坦的公路、大型水体、

建筑物或大气条件也会导致多径现象。信号会因为弯曲和反弹在许多不同的方向传播。主信号仍然可以到达接收天线，但那些反弹或弯曲的信号可能按照不同的路径到达接收天线。换句话说，射频信号会沿多条路径到达接收方，如图 2-15 所示。

图 2-15 多径现象

反射信号因为传播的路径较长通常会比主信号花费更长的时间到达接收天线。信号之间的时间差可以用纳秒(nanosecond)来测量。按多条路径传播的时间差被称为*时延扩展*(delay spread)。在本书中你将了解到，某些扩频技术比其他时延扩展技术更具容错性。

多径问题到底会导致什么发生？在电视信号传输时，多径现象会产生一种“叠影效应”(ghost effect)的效果，主信号的右侧会出现一幅较弱的重复图像。多径现象可能导致射频信号出现建设性或破坏性的影响，但大部分都是破坏性的。由于多条路径的相位差，信号混合通常导致衰减、放大或遭到破坏。这种现象有时称为*瑞利衰落*(rayleigh fading)，名称源于一位英国物理学家洛德·瑞利(Lord Rayleigh)。

多径会产生下面 4 种可能的结果：

信号增强(Upfade) 当多路射频信号同时到达接收方且与主波同相或局部异相时，结果会导致信号强度(振幅)增加。介于 0° 和 120° 之间较小的相位差会导致信号增强。然而，由于自由空间路径损耗，最终的接收信号不会比原始发送信号强。

信号减弱(Downfade) 当多路射频信号同时到达接收方且与主波异相，结果会导致信号强度(振幅)下降。相位差在 121° 和 179° 之间会导致信号减弱。振幅下降是多径现象导致的破坏性现象。

信号消失(Nulling) 当多路射频信号同时到达接收方且与主波呈 180° 相位差，结果可能会导致信号消失。信号消失很明显也是破坏性的多径现象。

数据损坏(Data Corruption) 因为同时存在多条反射信号的事实和时延扩展的影响(主信号与反射信号存在时间差)，接收方在解调射频信号的时候会有麻烦。时延扩展的时间差可能导致比特互相重叠，最终结果就是导致数据损坏。如图 2-16 所示。这种类型的多径干扰又称码间干扰(ISI)。数据损坏是最常见的破坏性多径现象事件。

图 2-16 数据损坏 ISI

坏消息是高多径环境通常都会因时延扩展导致码间干扰，再导致数据损坏。好消息是接收方都会通过 802.11 定义的循环冗余校验(CRC)检测到错误，因为此时校验和不能正确计算。802.11 标准要求大部分单播帧在接收方用确认帧(ACK)确认，否则发送方将不得不重传。接收方不会确认 CRC 校验失败的数据帧。因此帧必须被重传，然而重传也比误判数据要好。

多径现象对无线局域网性能和吞吐量具有负面影响，因为码间干扰导致的最直接后果就是第二层重传。第二层重传会影响到 802.11 无线局域网的整体吞吐量，同时也会影响到对延迟敏感的应用(如 VoIP 等)。在第 12 章中，我们会讨论多种第二层重传的原因，学习如何对其进行排障并减少重传率。多径现象是导致第二层重传并影响传统 802.11a/b/g 无线局域网吞吐量和延迟的主要原因之一。

那么不走运的工程师应该怎么处理这些破坏性的多径问题呢？多径对于传统的 802.11a/b/g 设备网来说是一个严重的问题。使用定向天线通常可以减少反射，分集天线也可以抵消多径的负面影响。有时候在保证足够信号给远程接入端的前提下，降低发射功率或使用低增益天线也能解决这个问题。本章我们主要关注多径对传统 802.11a.b/g 无线局域网破坏性的传输影响，而对于使用了 MIMO 天线分集和最大比混合(MRC)的 802.11n 传输来说，多径现象实际上会有建设性的结果。

在配书网站上有一个免费程序 EMANIM。用这个程序做练习 2.2，它演示了相位关系对振幅的影响和多径衰减。

练习 2.2

在本练习中，你将使用 EMANIM 程序查看两个同时到达的信号由于相位不同对振幅产生的影响。

(1) 从 www.sybex.com/go/cwna3e 下载程序 emanim_setup.exe，安装 EMANIM 程序。

(2) 从 EMANIM 主菜单中，单击 Phenomenon。

(3) 单击 Sybex CWNA Study Guide。

(4) 单击 Exercise A。

两个相同、垂直极化的波进行叠加(你可能看不到有两个波，因为它们互相重叠)。结果是振幅加倍。

(5) 单击 Exercise B。

两个相同的有 70° 相位差的波叠加。结果是波振幅增加。

(6) 单击 Exercise C。

两个相同的有 140° 相位差的波叠加。结果是波振幅减小。

(7) 单击 Exercise D。

两个相同、180° 反相的垂直极化波的叠加。结果是波消失了。

2.3.10 增益(放大)

增益也被称为放大，对其最好的描述就是振幅增加或信号增强。有两种类型的增益：有源增益和无源增益。信号的振幅可以通过外部设备增大。

有源增益(active gain)的获得通常是在发射器和天线之间安装一个放大器。发射器具备按不同功率传输的能力，发射功率越高，信号振幅越大。放大器通常是双向起效的，这意味它会同时放大接收和发送的信号强度。有源增益设备要求使用外部电源。

无源增益(passive gain)利用天线把射频信号集中。天线是无源设备，无需外部电源。天线可以使信号更集中在某一个方向。

射频放大器和天线的正确使用会在第 4 章进行阐述。

尽管多径的影响通常是负面的，但还是要重申一下，当多路射频信号同时到达接收方，与主波相位相同或局部异相时，振幅将增加。然而，信号从天线辐射前，振幅增加通常是信号得到无源增益或有源增益的结果。

有两种不同的工具用来在指定点测量信号的振幅。第一个工具(频域计)被用来测量在有限频谱范围振幅的变化，一般由无线局域网工程师使用，也被称为频谱分析仪(spectrum analyzer)。第二个工具(时域计)被用来测量信号振幅如何随时间进行改变。时域计传统上又称为示波器(oscilloscope)。图 2-17 说明了这两个工具如何进行振幅测量。请注意频谱分析仪一般由无线局域网工程师在现场勘测时使用；示波器在部署无线局域网时很少使用，但是射频工程师经常会在实验室测试环境中使用。

图 2-17 射频信号测量工具

2.4 小结

本章涵盖了关于射频信号最基本的知识。为了正确设计和管理无线局域网，需要对下列射频特性和射频行为的原则有充分的理解：

- 电磁波及电磁波如何产生
- 波长、频率与光速的关系
- 信号强度及信号受不同条件影响衰减或放大
- 两个信号或多个信号之间的关系的重要性
- 信号的弯曲、反射或吸收

在排除以太网故障时，最好从第一层(物理层)开始。无线局域网故障排除也是如此，应该从物理层开始。学习位于第一层的射频基础是进行正确部署无线网络的重要一步。

2.5 考试要点

理解波长、频率、振幅和相位。了解每个射频特性以及这些特性如何影响无线局域网设计。

记住所有的射频传播行为。解释每个射频行为(反射、衍射、散射等)之间的差异以及与每个射频行为相关的不同材质。

理解导致衰减的因素。损耗可以发生在有线端或无线端。吸收、自由空间路径损耗和多径现象是衰减的所有原因。

定义自由空间路径损耗。即使没有任何障碍物，电磁波从发射器传输的时候也仍按照对数的方式进行衰减。

记住由多径和相位的关系导致出现的 4 种可能结果。多径可能导致信号下降、信号增加、信号消失和数据损坏。理解多径可能产生破坏效果，也可能产生建设性效果。

了解码间干扰和时延扩展的后果。主信号与反射信号的时间差可能导致比特遭到破坏，从而因为第二层重传导致吞吐量下降和延迟增加。

解释有源增益和无源增益的区别。射频放大器是主动设备，而天线是被动设备。

解释传输振幅与接收振幅之间的差别。传输振幅是指离开发射器后的初始化振幅。当射

频模块接收到射频信号时，接收到的信号强度通常指的就是接收振幅。

2.6 复习题

复习题的答案见附录A。

1. What are some results of multipath interference? (Choose all that apply.)
   A. Cross polarization
   B. Upfade
   C. Excessive retransmissions
   D. Absorption

2. What term best defines the linear distance traveled in one positive-to-negative-to-positive oscillation of an electromagnetic signal?
   A. Crest
   B. Frequency
   C. Trough
   D. Wavelength

3. Which of the following statements are true about amplification? (Choose all that apply.)
   A. Some antennas require an outside power source.
   B. RF amplifiers require an outside power source.
   C. Antennas are passive gain amplifiers that focus the energy of a signal in one direction.
   D. RF amplifiers passively increase signal strength by focusing the AC current of the signal.
   E. Signal strength may passively increase because of multipath upfade.

4. A standard measurement of frequency is called what?
   A. Hertz
   B. Milliwatt
   C. Nanosecond
   D. Decibel
   E. K-factor

5. When an RF signal bends around an object, this propagation behavior is known as what?
   A. Stratification
   B. Refraction
   C. Scattering
   D. Diffraction
   E. Attenuation

6. When the multiple RF signals arrive at a receiver at the same time and are_____with the primary wave, the result can be_____of the primary signal.
   A. out of phase, scattering
   B. in phase, intersymbol interference

C. in phase, attenuation

D. 180 degrees out of phase, amplification

E. in phase, cancellation

F. 180 degrees out of phase, cancellation

7. Which of the following statements are true? (Choose all that apply.)

A. When upfade occurs, the final received signal will be stronger than the original transmitted signal.

B. When downfade occurs, the final received signal will never be stronger than the original transmitted signal.

C. When upfade occurs, the final received signal will never be stronger than the original transmitted signal.

D. When downfade occurs, the final received signal will be stronger than the original transmitted signal.

8. What is the frequency of an RF signal that cycles 2.4 million times per second?

A. 2.4hertz

B. 2.4MHz

C. 2.4GHz

D. 2.4kilohertz

E. 2.4KHz

9. What is the best example of a time domain tool that could be used by an RF engineer?

A. Oscilloscope

B. Spectroscope

C. Spectrum analyzer

D. Refractivity gastroscope

10. What are some objects or materials that are common causes of reflection? (Choose all that apply.)

A. Metal

B. Trees

C. Asphalt road

D. Lake

E. Carpet floors

11. Which of these propagation behaviors can result in multipath? (Choose all that apply.)

A. Refraction

B. Diffraction

C. Reflection

D. Scattering

E. None of the above

12. Which behavior can be described as an RF signal encountering a chain link fence, causing

the signal to bounce into multiple directions?

A. Diffraction

B. Scatter

C. Reflection

D. Refraction

E. Multiplexing

13. Which 802.11 radio technologies are most impacted by the destructive effects of multipath? (Choose all that apply.)

A. 802.11a

B. 802.11b

C. 802.11g

D. 802.11n

E. 802.11i

14. Which of the following can cause refraction of an RF signal traveling through it? (Choose all that apply.)

A. Shift in air temperature

B. Change in air pressure

C. Humidity

D. Smog

E. Wind

F. Lightning

15. Which of the following statements are true about free space path loss? (Choose all that apply.)

A. RF signals will attenuate as they travel, despite the lack of attenuation caused by obstructions.

B. Path loss occurs at a constant linear rate.

C. RF signals will attenuate as they travel because of obstructions.

D. Path loss occurs at a logarithmic rate.

16. What term is used to describe the time differential between a primary signal and a reflected signal arriving at a receiver?

A. Path delay

B. Spread spectrum

C. Multipath

D. Delay spread

17. What is an example of a frequency domain tool that could be used by an RF engineer?

A. Oscilloscope

B. Spectroscope

C. Spectrum analyzer

D. Refractivity gastroscope

18. Using knowledge of RF characteristics and behaviors, which two options should a WLAN engineer be most concerned about during an indoor site survey? (Choose all that apply.)

A. Brick walls

B. Indoor temperature

C. User density

D. Drywall

19. Which three properties are interrelated?

A. Frequency, wavelength, and the speed of light

B. Frequency, amplitude, and the speed of light

C. Frequency, phase, and amplitude

D. Amplitude, phase, and the speed of sound

20. Which RF behavior best describes a signal striking a medium and bending in a different direction?

A. Refraction

B. Scattering

C. Diffusion

D. Diffraction

E. Microwave reflection

第 3 章 射频组件、测量与数学

在该章中，你将学习以下内容：

- √ 射频组件
  - 发射机
  - 接收机
  - 天线
  - 各向同性辐射体
  - 主动辐射器(IR)
  - 等效全向辐射功率(EIRP)
- √ 功率单位和相对单位
  - 瓦(W)
  - 毫瓦(mW)
  - 分贝(dB)
  - dBi
  - dBd
  - dBm
  - 平方反比定律
- √ 射频数学
  - 10s 与 3s 规则
- √ 本底噪声(Noise floor)
- √ 信噪比(SNR)
- √ 接收信号强度指示(RSSI)
- √ 链路预算(Link budget)
- √ 衰落容限/系统操作容限(SOM)

简单来说，数据通信是指计算机之间的信息传输。无论采用哪种形式通信，要保证其成功需要许多必要组件。在学习这些组件之前，先要了解保证通信成功的三个基本要求：

- 有两个或更多的设备要求互相通信。
- 有可以使用的通信媒介、通信手段。
- 通信需要一系列的使用规则(第 8 章将涵盖这部分内容)。

这三个基本要求对于所有类型的通信都是适用的，无论是一群人在宴会厅交谈，还是两台计算机通过拨号调制解调器传输数据，抑或是许多计算机通过无线网络通信。

计算机网络的存在意味着第一个要求是满足的。因为如果没有两台或更多的设备需要共享数据，我们也没必要创建网络。CWNA 认证也假定如此。另外也不必担心数据本身，因为假定已经有了数据，我们需要关注的是如何对其进行传输。

本章关注的是确保通信成功的第二个要求：通信媒介和通信手段。我们会讲述构成无线通讯媒介的射频(RF)组件，还会关注射频信号传输及传输路径中每个设备和组件的作用，另外还会探讨每个设备或组件对传输的影响。

在第 2 章中，你了解到许多射频传播行为会对信号产生影响。信号通过空气和不同的射频组件后，振幅会发生变化。某些组件会提高信号功率(增益)，而有些组件会降低功率(衰减)。在本章中，你将学习如何对无线电波的功率进行量化并对其进行测量，计算无线电波受内部和外部影响的程度。通过这些计算，你将能够准确预测设备间的无线通信能否成功。

3.1 射频组件

许多组件用于传输和接收射频信号。图 3-1 展示了在本节中介绍的一些关键组件。除了要了解这些组件的功能，更重要的是理解它们如何影响信号强度。

图 3-1 射频组件

在本章后面的射频数学部分，主要学习计算射频组件对信号的影响程度。

3.1.1 发射机

发射机(transmitter)是无线通信媒介中的初始组件。计算机将数据传递给发射机后，发射机随即开始 RF 通信。

在第 1 章中，你了解了载波信号和调制方法。当发射机收到数据后，便开始产生交流电

流(AC)信号。此交流信号决定了传输频率。对于 802.11b(HR-DSSS)或 802.11g(ERP)无线传输，交流信号每秒钟大约振荡 24 亿次。对于 802.11a(OFDM)传输，交流信号每秒振荡 50 亿次。每秒钟振荡的次数就是电磁波的频率。

确切的使用频率将在第 6 章中阐述。

发射机把计算机数据通过调制技术进行交流信号修改，并将数据在信号中进行编码。这个被调制的交流信号作为载波信号容纳需要发送的数据。载波信号随即被直接或通过馈线发送给天线。

除了生成特定频率的信号，发射机还负责确定原始的传输振幅，通常也称为发射机的*功率等级*(power level)。无线电波的振幅越高，能量就越强，传送也越远。发射机允许的功率等级由所在国家的监管部门规定，例如美国的联邦通讯委员会(FCC)。

本章单独解释了发送机与接收机，尽管从功能上看它们属于不同的组件，但通常它们属于同一个被称为*收发器*(transceiver)的设备。无线接入点、网桥和无线网卡均内置了无线收发器。

3.1.2　天线

天线在通信系统中提供两种功能。当天线连接在发射机上时，天线收集从发射机传来的交流信号，根据天线类型按特定的模式将射频波发射出去。当天线连接到接收机上时，天线把接收到的射频电波转换为交流信号后再发给接收机。接收机再将交流信号转换成比特和字节。你将在本章后面看到，接收信号的强度要远远小于信号产生时的强度。对于这种信号损失我们可以打个比方来解释一下，这有点类似于两个人在足球场两端尝试对话。由于距离(空间)的影响，从一端大声喊叫的声音强度到达另一端后与低声耳语的声响强度差不多。

天线信号通常与各向同性辐射体进行对比。各向同性辐射体(isotropic radiator)是指信号强度在各个方向均进行等效辐射的*点状发射源*(point source)。太阳是典型的各向同性辐射体。它在所有方向辐射的能量是相等的。但遗憾的是，这种完美的各向同性辐射体天线是不可能制造出来的。天线的自身结构也会影响到天线信号的输出，就像灯泡的结构会影响灯泡的发光方式一样。

有两种方法可以增强天线的输出功率。第一种方法是增加发射机功率，已在上节叙述过。另一种方法是对射频信号进行定向或聚焦辐射。这类似于用手电筒聚焦光线。如果把手电筒的聚光镜取下来，灯泡通常不会显得非常明亮，因为光线几乎朝所有的方向辐射。若要使光线更加明亮，可使用功率更强的电池或者把手电筒的聚光镜装回去。聚光镜本身并没有产生光线。它只是把光线集中到一个较窄的区域。有些天线在辐射射频电波时就好像是没有安装聚光镜的灯泡，另一些天线就好比是使用了聚光镜的手电筒。

在第 4 章中，你将了解到各种类型的天线以及如何正确有效地使用它们。

3.1.3 接收机

接收机(receiver)是无线通讯媒介中的最后一个组件。接收机从天线接收载波信号并把信号调制成 1 和 0，再把这些数据传给计算机处理。接收机的工作未必简单。接收机接收的信号因为距离和自由空间路径损耗(FSPL)的影响要比发送时的信号强度弱得多，而且信号也经常受到其他射频源的干扰和多径现象的影响。

3.1.4 主动辐射器(IR)

根据美国联邦法规(CFR)第 15 部分，主动辐射器(Intentional Radiator)定义为“主动生成并通过辐射或感应的方式发射射频能量的设备”。基本上，这是某种专门用来产生射频信号的组件，虽说有些设备也会产生射频信号，但通常只作为其主要功能的副功能。例如发动机也会附带生成射频噪声。

无线监管机构(如 FCC)会限制 IR 产生的功率。如图 3-1 所示，IR 包括从发射机到天线之间的所有组件，但不包括天线。IR 的输出功率综合了从发射机到天线之间的所有组件，但同样不包括天线。IR 组件包括发射机、所有电缆、连接器及其他设备(接地装置、避雷器、放大器、衰减器等)。IR 的功率测量点位于天线输入接头。此处是对主动辐射器测量和监管的地方，这一点也常被称为 IR，其功率级别通常以 mW 或 dBm 为单位。如果再拿手电筒做类比，IR 包含灯泡插座前的所有电器设备，但不包括灯泡和聚光镜。IR 是原始的能量或信号，灯泡和聚光镜再对这个信号进行聚焦。

3.1.5 等效全向辐射功率

等效全向辐射功率(EIRP)是指从天线发出的最大射频信号强度。为更好地理解它，我们再用手电筒来举例。假设灯泡在没有聚光镜时产生 1W 的功率。当加上聚光镜时，1W 的光线被聚焦。如果此时再观察光线，会发现它显得更亮。由于聚光作用，光线的最亮点可能会等效于 8W 灯泡的亮度。所以通过聚焦光线，可使被聚光的灯泡的等效全向辐射功率变为 8W。

有一点很重要，EIRP 被定义为等效全向辐射功率(equivalent isotropic radiated power)或有效全向辐射功率(effective isotropic radiated power)。在本书中 EIRP 按照 FCC 定义为“等效全向辐射功率，即天线输入功率与特定方向上天线增益的总和。”尽管术语首字母代表的含义不同，但 EIRP 的定义是一致的。

正如你在本章前部分了解到的那样，天线具有聚焦射频能量的能力。聚焦能力可以使天

线的有效输出比天线输入信号更强。因为这种可以放大射频信号输出的能力，FCC 等监管部门通常要限制 EIRP 值。

在本章下一节，你将学习如何计算天线实际的输入功率(IR)及天线输出功率(EIRP)。

为何 IR 与 EIRP 的测量很重要？

在第 1 章我们学过，每个国家或地区都有管理机构负责对最大传输功率做出规定。FCC 和其他无线监管机构通常会定义主动辐射器(IR)的最大功率和从天线辐射的最大等效全向辐射功率(EIRP)。在 Laymen 条款中，FCC 规定了发往天线的最大功率及从天线发出的最大功率。

你将需要了解 IR 与 EIRP 的定义。然而，CWNA 考试(PW0-105)不会考查任何关于功率方面的规定，因为不同国家，规定会有所不同。建议你要了解需要部署 WLAN 的所在地的最大传输功率要求，确保不要违反法规。

3.2　功率单位和相对单位

802.11 无线网络设计的两个关键要素是覆盖和性能。了解射频功率、功率单位及射频数学对于无线网络设计非常有帮助。

本节会介绍功率单位的分类及对比，需要掌握测量单位的类型及关系，并了解实际功率单位和相对功率单位。实际单位表示一个已知或已设置的值。

举个实际单位的例子，某男子高 6 英尺。因为该男子的高度是已知数，你确实知道他有多高。而相对单位是用于比较相似主体的相对值。比方说，如果你想告诉别人这位男子的妻子有多高，你可能会说她的高度是该男子的 5/6。相对测量的方法就是：已知其中一个单元的实际信息，由此确定另一个单元的信息。

相对测量单位对功率计算非常有用。在本章后面将看到，利用相对功率单位进行 AP 覆盖的比较。例如，利用简单的数学计算，能够确定要使 AP 的信号覆盖范围加倍，如何增加功率需求。

功率单位用来测算传输振幅和接收振幅大小。换句话说，功率单位测量的是绝对功率(absolute power)。而相对单位通常用于计算增加电缆或天线后的损耗和增益的大小。相对单位也用来计算 A 点到 B 点的功率差别。也就是说相对单位是用来测算功率变化的。

下面列出功率单位和相对功率单位，所有这些单位都会在本章后面用到。

功率单位(绝对)

- 瓦特(W)
- 毫瓦(mW)
- dBm

相对功率单位(相对)

- 分贝(dB)
- dBi
- dBd

3.2.1 瓦特

瓦特(W)是功率的基本单位，因 18 世纪苏格兰发明家 James Watt 得名。1 瓦相当于 1 伏特电压下的 1 安培电流。要更好地解释 1 瓦特，我们用水来做比喻。

许多人可能知道一种称为电动清洗机的设备。它是一个连接水源的机器，就像花园的软管，用高压水流对准物体，借助高速移动的水流清洁物体。电动清洗机的成功基于两个因素：水流压力和单位时间内使用的水量(即流量)。这两个因素决定了水流的功率。如果你加压，水流的能量增加。如果你增加水量，水流能量也会增加。水流的能量等于水流压力乘以水量。

瓦特非常类似于电动清洗机的输出能量。相对于清洗机产生的压力，电气系统对应的是伏特。相对于水流，电气系统对应的是电流(单位为安培)。功率等于伏特乘以安培。

3.2.2 毫瓦

毫瓦(mW)也是功率单位，1mW 等于千分之一瓦特。我们关注 mW 的原因是大多数 802.11 设备的传输功率都介于 1mW 和 100mW 之间。请牢记射频的传输功率会因电缆而衰减，会因天线而放大。尽管监管部门(如 FCC)可能允许 IR 输出功率为 1W，但这种情况很少见，只有点到点通信(如建筑物到建筑物的桥接链路)允许 802.11 设备的传输功率超过 300mW。

真实世界场景

Wi-Fi 供应商的发射功率指的是什么？

所有 Wi-Fi 供应商都允许对 AP 的发射功率进行调整，通常 AP 的发射功率从 1mW 到 100mW。但 Wi-Fi 供应商所指的发射功率可能有所不同，大部分供应商所指的发射功率为 IR，有一部分的供应商所指的是 EIRP。另外有些供应商用毫瓦或 dBm 来描述传输功率，例如 32mW 或+15dBm；而有些则用百分比形式来描述发射功率，例如 32%。这时就需要参考该供应商的部署指南来全面理解发射功率值。

3.2.3 分贝

你需要了解关于分贝(decibel，dB)的第一件事就是它是一个相对单位，并非绝对功率单位。因此它用来描述两个数值之间的差异。换句话说，dB 是一个相对表达式，代表了功率变化的指标。在无线网络中，贝尔通常用于比较两个发射机的功率差别，更常见的是，它用来比较发射机天线的 EIRP 输出与接收机天线接收到的功率数值之间的差异或损耗。

贝尔源自术语贝尔(Bel)。当时贝尔实验室的员工需要一种方法来描述电话线上的功率损失。他们定义两个声音的功率比为 10 比 1 时为 1 贝尔。举例来说：无线接入点的发射功率

为 100 mW。笔记本电脑 A 接收到的信号功率为 10mW，笔记本电脑 B 接收到的信号功率为 1mW。那么无线接入点的信号(100mW)与笔记本电脑 A 的信号(10mW)差别就是 100:10 或 10:1 或 1 贝尔。笔记本电脑 A 的信号(10mW)与笔记本电脑 B 的信号(1mW)差别也为 10:1 或 1 贝尔。因此无线接入点与笔记本电脑 B 的信号差别就为 2 贝尔。

贝尔值能够通过对数函数计算得到。但并不是每个人都能理解并牢记对数函数，所以我们对它们做一个小结。首先，我们需要先看下功率增加的情况。如果基数为 10，然后提升到它的三次幂($10^3 = y$)，实际上就是乘三次 10 (10×10×10)。通过计算得到 y=1000，所以答案就是 10^3=1000。如果做对数运算，计算公式会改为 10^y=1 000，这时我们再计算下 10 的几次幂等于 1000，此例中答案是 3。也可以得到如下等式 $y=\log_{10}(1\ 000)$ or $y = \log_{10}1\ 000$。最后的公式就是 $3 = \log_{10}(1\ 000)$。下面是幂与对数公式的一些例子：

$10^1 = 10$　　$\log_{10}(10) = 1$

$10^2 = 100$　　$\log_{10}(100) = 2$

$10^3 = 1\ 000$　　$\log_{10}(1\ 000) = 3$

$10^4 = 10\ 000$　　$\log_{10}(10\ 000) = 4$

现在让我们再用对数函数计算一下从无线接入点和笔记本电脑 B 的信号强度变化的贝尔值。请记住贝尔值是用来计算两个功率之间的比值。现在我们把无线接入点的功率标记为 P_{AP}，笔记本电脑 B 的功率标记为 P_{L2}。所以现在此例的公式就是 $y=\log_{10}(P_{AP}/P_{L2})$。把功率数值输入公式，$y=\log_{10}(100/1)$或 $y=\log_{10}(100)$。这个等式是问我们，10 的几次幂时等于 100？答案就是 2 贝尔(10^2=100)。

在某些情况下，用贝尔来描述功率差别不够准确，这时候我们就需要使用分贝。分贝是十分之一贝尔。计算分贝，只需将贝尔值乘以 10。所以得到贝尔和分贝的计算公式如下：

贝尔(bels)=$\log_{10}(P_1/P_2)$

分贝(decibels)=$10\times\log_{10}(P_1/P_2)$

现在再计算下无线接入点到笔记本电脑 B 的信号强度变化的分贝值。现在公式变为 $y=10\times\log_{10}(P_{AP}/P_{L2})$，把功率数值输入公式，$y=10\times\log_{10}(100/1)$或 $y=10\times\log_{10}(100)$。答案就是 +20 分贝。

在 CWNA 考试中，不会考查如何计算对数函数。在此举得几个例子是让你了解对数的概念以及如何进行对数计算。在本章后面部分，你会学到不用对数公式也可以计算分贝值的方法。

你已经了解了 dB，但你可能还是想知道为什么不用 mW 呢？实际上你完全可以使用 mW，但因为功率是遵循对数函数变化的，由此导致变化差异变得极大，处理起来会非常困难。譬如我们很容易说 100mW 的信号下降了 70dB，但是说信号下降到 0.00001mW 就很困难。表 3-1 是 mW 与 dB 变化的对照表，使用 1mW 作为参考点。通过数字的范围变化，你就可以知道为什么要使用分贝。

表 3-1 mW 与 dB 变化的对照表(相对于 1mW)

mW	dB 变化
0.0001	–40
0.001	–30
0.01	–20
0.1	–10
1	0
10	+10
100	+20
1 000	+30
10 000	+40
100 000	+50

为什么应该使用分贝？

在第 2 章中，你了解到有许多传播行为可以影响无线电波。其中之一就是自由空间路径损耗。

如果 AP 的发射功率为 100mW，而笔记本电脑距离无线接入点为 100 米(0.1 公里)，它接收到的功率只有大约 0.000 001mW。100 和 0.000 001 的数字差异太大了。很难看出两者之间的相对关系，很多人输入功率 0.00 001 的时候很可能很容易漏写一个 0(比如刚刚我就漏写了一个)。

计算本场景中的自由空间路径损耗的公式如下：

$$\text{decibels} = 32.4 + (20\log_{10}(2\ 400)) + (20\log_{10}(0.1))$$

答案为 80.004dB，即约为 80dB 损耗。这个数字很容易记忆，也很难误写。

3.2.4 dBi

本章前面比较了天线和各向同性辐射体。理论上各向同性辐射体在每个方向上辐射的信号强度都相同。因为结构自身的约束，天线无法做到这一点。某些情况下，我们也并不希望天线在每个方向上都辐射信号，而希望天线在某个方向上聚焦信号。不管怎么样，重要的是可以计算天线的辐射功率以确定距离天线某个位置的信号强度，另外有时你可能需要比较两根天线的输出差异。

天线与各向同性辐射体相比功率的增益称为 *decibels isotropic*(dBi)，或描述成“相对于各向同性辐射体的相对增益”或“与天线相关的功率改变”。因为天线用增益来测算(并非功率)，因此可以推断 dBi 是一个相对测量值，而非绝对测量值。dBi 是天线增益的测量单位。dBi 值可以在天线信号的最强点或聚焦点处测量得到。因为天线总在某一个方向聚焦能量，所以 dBi 总是正值。然而也有 dBi 值等于 0 的天线，通常称为零增益(no-gain)或单位增益(unity-gain)

天线。

无线接入点通常使用半波偶极天线。半波偶极天线是一种外形较小且通常有橡胶外套的通用天线。2.4GHz 的半波偶极天线增益为 2.14dBi。

任何时间看到 dBi，指的都是天线的增益。

3.2.5　dBd

天线行业通常用两种分贝尺度来衡量天线增益。第一种尺度，即 dBi，用来描述相对于理论的各向同性辐射天线的增益。另一种尺度称为 dBd(decibels dipole)，指与偶极天线信号相比的天线增益。在第 4 章你会了解到偶极天线也是全向天线。因此 dBd 值是对全向天线增益的测量值而不是针对定向天线的增益。偶极天线的测算单位是增益，并非功率，因此 dBd 也是相对测量值，而非功率测量值。

dBd 的定义看似非常简单，但是如果你要比较的两根天线的标称单位不同怎么办(其中一根天线的增益单位是 dBi，而另一根的增益单位是 dBd)？其实很简单，标准偶极天线的增益为 2.14dBi，如果一根天线的增益为 3dBd，意味着该天线比偶极天线增益高出 3dBi，所以 3dBd 的天线增益为 5.14dBi。

请不要忘记 dB、dBi 和 dBd 都是相对测量值，而不是功率单位。

真实场景

关于 dBd 的计算

在 802.11 设备中天线增益标记为 dBd 的情况并不多见，如果你偶尔遇到一个，那么只要简单地在 dBd 数值上加 2.14，就可以得到这根天线的 dBi 数值了。

3.2.6　dBm

在前面谈到贝尔和分贝的时候，你知道它们是用来测量两个信号间的差异或比值的。不考虑传输的功率类型，你真正从中了解的就是某信号比另一个信号强或弱多个贝尔或分贝。dBm 提供的也是对比值，但不是比较信号，而是比较信号强度与 1mW 之间的关系。dBm 指的就是相对于 1mW 的 dB 值。所以我们规定 0 dBm 代表 1mW。dBm 值是与 1mW 比较的相对值，其实就是绝对功率的测量值。因为 dB(相对值)与 1mW(绝对值)有关，可以认为 dBm 就是对相对于 1mW 的功率变化的绝对评估值。利用公式 $dBm=10\times\log_{10}(P_{mW})$，可以得出 100mW 的功率等于+20dBm。

如果你需要根据某设备的 dBm 值计算所对应的 mW 值，你也可以使用下面的公式：

$P_{mW} = 10^{(dBm + 10)}$。

请记住 1mW 是一个参考点，0dBm 等于 1mW。任何测量值为+dBm 时意味着功率大于 1mW，任何测量值为-dBm 时意味着功率小于 1mW。例如我们前面阐述的大部分 802.11 射频模块的功率通常为 1mW 到 100mW。100mW 等于+20dBm。但由于自由空间路径损耗的影响，接收信号总小于 1mW。一个非常强的接收信号通常也只有约-40dBm，相当于 0.0001mW (1/10 000 mW)。

对 mW 与 dBm 进行转换可能看起来有点荒谬。既然 mW 是一个有效的功率测量单位，为什么不干脆就用它呢？事实上却不得不使用 dBm？这是学生们经常提出的一个好问题。原因其实很简单，dBm 相对于百万分之一或十亿分之一毫瓦的数值更容易理解。大部分 802.11 无线接口卡可以识别从-30dBm(1mW 的千分之一)到-100dBm(1mW 的一百亿分之一)的接收信号强度。人们理解-100dBm 比理解 0.000 000 000 1 要容易得多。在现场勘测时，WLAN 工程师也总是通过记录接收信号强度单位为-dBm 的数值确定覆盖区域。

另一个非常现实的原因 dBm 也能用于自由空间路径损耗公式。下面是两个自由空间路径损耗的公式。第一个公式计算的是距离射频源 100 米(0.1km)以外的 2.4GHz 信号的衰减值，第二个公式计算是距离射频源 200 米(0.2km)以外的 2.4GHz 信号的衰减值。.

$$FSPL = 32.4 + (20\log_{10}(2\,400)) + (20\log_{10}(0.1)) = 80.00\,422dB$$
$$FSPL = 32.4 + (20\log_{10}(2\,400)) + (20\log_{10}(0.2)) = 86.02\,482dB$$

在这个例子中，我们观察到距离射频源距离增加一倍，信号下降约 6dB。如果你把发射机与接收机之间的距离加倍，接收信号也将下降 6dB。无论距离数值如何，只要该距离加倍，衰减就会约 6dB。这个规则意味着如果振幅增加 6dB，可用距离将会加倍。6dB 规则(6dB rule)在计算蜂窝大小、评估发射机覆盖范围和理解天线增益时非常有用，因为每 6dBi 额外的天线增益可使射频信号的可用距离增加一倍。请记住，如果你使用 mW 作为单位，这个规则就不会有关联了。把 mW 转换成 dBm，是比较信号差异的更实用方法。

请记住 6dB 规则：增加 6dB 会使可用信号距离加倍，减少 6dB 会使可用信号距离减半。

使用 dBm 也便于计算天线增益对信号的影响。如果发射机产生+20dBm 的信号，天线增加 5dBi 的增益，那么从天线辐射出的功率(EIRP)就等于两者的和，即+25dBm。

3.2.7 平方反比法则

你刚刚了解了 6dB 规则，即+6dB 的增益可以使信号可用距离加倍，-6dB 的衰减会使信号可用距离减半。这个规则和这些数字都是来自于平方反比法则(inverse square law)，该法则由艾萨克·牛顿发现。

该法则阐述了功率的变化与距离变化的平方成反比。换句话说，当离信号源的距离增加一倍时，能量被扩散到 4 倍的范围内，导致信号集中度降为原来的 1/4。

这意味着如果你正在某个距离(D)的地方接受某级别功率的信号，如果这个距离加倍(2×D)，那么新的功率级别就变为 $1 \div (2)^2$。我们可以使用公式 $P/(4*\pi*r^2)$来计算在某个特定距离的 EIRP 值，其中 P 是初始 EIRP 值，r 指原始参考距离。

再来回顾一下自由空间路径损耗的公式：

$FSPL = 36.6 + (20\log_{10}(F)) + (20\log_{10}(D))$

FSPL = 路径损耗(单位 dB)

f =频率(单位 MHz)

D=天线之间的距离(单位 mile)

$FSPL = 32.4 + (20\log_{10}(F)) + (20\log_{10}(D))$

FSPL = 路径损耗(单位 dB)

f = 频率(单位 MHz)

D = 天线之间的距离(单位 km)

FSPL 的概念也基于牛顿的平方反比法则，该法则的主要变量就是距离。而 FSPL 公式也是基于距离，但还涉及另一个变量：频率。

3.3　射频数学

谈到射频数学的话题，大多数人都会畏缩或恐慌，因为他们认为里面有许多复杂的对数函数。不必担心，下面涉及的射频数学，不使用对数函数。如果你想通过这章节更新你的数学技巧，就回顾下面的内容即可：

- 3 和 10 的加法减法
- 2 和 10 的乘法除法

不是开玩笑，如果你知道怎么对 3 和 10 进行加减法和对 2 和 10 进行乘除法，你就具备了进行射频数学计算的所有能力，下面我们会教你怎么做。

3.3.1　10 与 3 规则

在开始应用 10 与 3 规则之前，清楚下面这点很重要：使用这个规则得到的结果不如使用对数函数得到的结果精确。10 与 3 规则提供的只是估算值。如果你是一位设计无线产品的工程师，就仍需利用对数精确计算以符合射频管理规定。然而，如果你是网络规划人员，10 与 3 规则可以提供正确规划网络所需的数值依据。

这部分会教你如何一步步进行数字计算。所有计算都基于下面 4 个 10 与 3 法则：

- 每 3dB 的增益(相对值)，绝对功率(mW)加倍
- 每 3dB 的损耗(相对值)，绝对功率(mW)减半
- 每 10dB 的增益(相对值)，绝对功率(mW)乘 10
- 每 10dB 的损耗(相对值)，绝对功率(mW)除 10

例如，假设 AP 传输功率为 100mW，天线提供 3dBi 的无源增益，EIRP 就等于 200mW。

因为根据你刚学到的规则，3dB 的增益可以使 100mW 的信号强度增加一倍。相反，如果这个发射功率为 100mW 的 AP 连接了一根衰减为 3dB 的电缆，那么在电缆末尾处，功率将变为 50mW，也就是说 3dB 的电缆损耗导致 100mW 的信号强度减半。

再举个例子，如果你的无线接入点的发射功率为 40mW，天线提供 10dBi 的无源增益，EIRP 就等于 400mW。天线的 10dBi 的增益使 40mW 的信号强度增加 10 倍。相反，如果这个发射功率为 40mW 的无线接入点连接了一根衰减为 10dB 的电缆，那么在电缆末尾处，功率将变为 4mW。也就是说 10dB 的电缆损耗导致 40mW 的信号强度减少了 10 倍。

记住这个规则，你就可以进行快速的射频计算。当你按步骤计算时，请牢记 dBm 是绝对功率单位而 dB 是描述变化的相对单位。dB 是可以叠加在 dBm 之上的单位。所以如果你有+10dBm，然后增加了 3dB，那么把这两个数值叠加，你可以得到+13dBm 的结果。

练习 3.1

10 与 3 规则的使用步骤：

(1) 在一页纸上，创建两列。一列是 dBm，另一列是 mW。

dBm	mW

(2) 在 dBm 前面，设置加减符，在 mW 旁边设置乘除符。这有助你了解在 dBm 列进行的是加减运算，在 mW 列进行的是乘除运算。

+			×
−	dBm	mW	÷

(3) 在加减符左侧写上数字 3 和 10，在乘除号右侧写上数字 2 和 10。任何针对 dBm 列的运算只用数字 3 和 10。任何针对 mW 列的运算只用数字 2 和 10。

3	+		×	2
10	−	dBm	mW	÷	10

(4) 如果左边有一个“+”号，右边就需要有一个“×”号。左边有一个“-”号，右边就要有一个“÷”号。

(5) 如果左边加或减 3，右边相应就要乘以或除以 2。如果左边加或减 10，右边相应就要乘以或除以 10。

(6) 最后一步就是在 dBm 列下方放置一个 0，在 mW 列下方放置一个 1。请记住 dBm 的定义就是相对于 1mW 的分贝值。所以这张表就表示 0dBm 等于 1mW。

3	+		×	2
10	−	dBm	mW	÷	10
		0	1		

在继续其他例子之前，再次强调无论功率值是多少，±3dB 相当于功率加倍或减半。

在使用 10 与 3 规则时，我们接触的功率都是 mW 级别的，这是 802.11 设备使用的典型传输振幅度量单位。然而请了解，无论功率大小如何，+3dB 都会使功率加倍。例如 1.21 千兆瓦特的功率增加 3dB 会导致功率变为 2.42 千兆瓦特。

10 与 3 规则的模拟讲解和如下案例的解释都是通过微软公司的 PowerPoint 创建的，可以通过 http://www.sybex.com/go/cwna3e 下载。如果尚未安装 PowerPoint，可以从微软网站上下载 PowerPoint Viewer 程序以查看 PowerPoint 文件。

练习 3.2

10 与 3 规则，案例 1

本例中，将从 1mW 开始，对功率加倍三次。除了要计算新的功率(mW 为单位)，还要计算以 dBm 为单位的功率级别。

(1) 首先创建如练习 3.1 的初始表。

(2) 现在对功率进行第一次加倍。于是在右边的 1mW 处写上×2，然后在 1 下面执行计算。

(3) 目前尚未完成计算，请务必了解无论在该表的一侧进行何种运算，在另一侧都要进行相应的数学等式运算。因为在右侧乘 2，所以要在左侧加 3，得到+3dBm，即 2mW。

(4) 你已经完成了第一个功率加倍的运算。现在要做第二个及之后的加倍运算。因为这是第一次使用这个计算过程，所有步骤都用箭头进行说明，以后的案例就不再使用箭头了。

通过上面计算，我们可以知道 4mW 等于+6dBm，8mW 等于+9dBm。如果用 dBm 的转换公式计算，实际答案应该是 4mW 等于+6.0206dBm，8mW 等于+9.0309dBm。正如你看到

的，使用这个规则计算出来的数值算是准确，但仍不够精确。

练习 3.3

10 与 3 规则，案例 2

某无线网桥发射功率为 100mW，连接电缆衰减为-3dB，天线提供 10dBi 的增益，计算 IR 与 EIRP 值。

在此提醒，如图 3-2 所示，IR 是指天线处但不包括天线增益部分的信号强度，而 EIRP 是指从天线辐射的信号强度。

图 3-2 案例 2 的示意图

(1) 第一步，确定如何使用 10 或 2，以及乘或除，从 1mW 到 100mW，不难意识到 1 乘以 10 两次就可以得到 100，所以网桥的功率为 100mW 或者+20dBm。

3	+			×	2
10	−			÷	10
		dBm	mW		
		0	1		
	+10	10	10	×10	
	+10	20	100	×10	

(2) 第二步，因为天线连接电缆对信号产生了 3dB 的衰减，通过计算-3dB 的损耗影响，就可以得到 IR 值。IR 就等于+17dBm 或者 50mW。

3	+			×	2
10	−			÷	10
		dBm	mW		
		0	1		
	+10	10	10	×10	
	+10	20	100	×10	
	−3	17	50	÷2	

(3) 现在在左侧要计算天线增益对信号的增强部分。因为增益为 10dBi，在 dBm 一栏增加 10，右侧要相应做乘 10 的运算。于是得到 EIRP 为+27dBm 或 500mW。

3 +			× 2
10 −	dBm	mW	÷ 10
	0	1	
+10	10	10	×10
+10	20	100	×10
−3	17	50	÷2
+10	27	500	×10

到目前为止，案例中所选择的数字都是非常简单的，使用的都是模板里面的数值。然而在现实中并非如此。利用一些小小的创造性，可以计算任意整数的增益或衰减。但是，小数不适用于 10 与 3 规则，这时就要使用对数公式计算了。

dB 增益或衰减是可以累积的。例如，如果天线与收发机之间有三段连接电缆，每段产生 2dB 的衰减，三段就产生了 6dB 的衰减。按照 10 与 3 规则，减去 6dB 就是减去两次 3dB。分贝的计算非常灵活。

表 3-2 列出了利用 10 和 3 的组合，计算从−10 到+10dB 之间所有整数的衰减和增益的方法。花些时间看下这些数值，就能意识到通过一些小小的创造力，可以计算任何整数的增益和衰减。

表 3-2　dB 衰减和增益(−10 到+10)

增益或衰减(dB)	10 与 3 的组合
−10	−10
−9	−3−3 −3
−8	−10 −10 +3 +3 +3 +3
−7	−10 +3
−6	−3 −3
−5	−10 −10 +3 +3 +3 +3 +3
−4	−10 +3 +3
−3	−3
−2	−3 −3 −3 −3 +10
−1	−10 +3 +3 +3
+1	+10 −3 −3 −3
+2	+3 +3 +3 +3 −10
+3	+3
+4	+10 −3 −3
+5	+10 +10 −3 −3 −3 −3 −3
+6	+3 +3
+7	+10 −3
+8	+10 +10 −3 −3 −3 −3
+9	+3 +3 +3
+10	+10

练习 3.4

10 与 3 规则，案例 3

本案例有点复杂。无线接入点发射功率 50mW，天线与无线接入点间的信号衰减为-1dB，无线接入点使用+5dBi 的天线，如图 3-3 所示。计算 IR 与 EIRP 的数值。

图 3-3　案例 3 的示意图

(1) 第一步将 1mW 转为 50mW，为此，可将 1mW 增加 10 倍再除以 2。

(2) 在 dBm 栏增加两次 10，再减 3。当计算更复杂时，最好分成多个部分并添加标记。

3 +			× 2	
10 −	dBm	mW	÷ 10	
	0	1		
+ 10	10	10	× 10	
+ 10	20	100	× 10	发射机
− 3	17	50	÷ 2	

(3) 无线接入点与天线间的损耗为-1dB。表 3-2 指出-1dB 可以通过减 10 和加 3 次 3 得到。

(4) mW 列需要除 10，再 3 次乘 2。因此 IR 为 16dBm 或 40mW。

3 +			× 2	
10 −	dBm	mW	÷ 10	
	0	1		
+ 10	10	10	× 10	
+ 10	20	100	× 10	发射机
− 3	17	50	÷ 2	
− 10	7	5	÷ 10	
+ 3	10	10	× 2	连接器
+ 3	13	20	× 2	
+ 3	16	40	× 2	

(5) 天线增加 5dBi 的增益。表 3-2 说明+5dBi 可以通过两次加 10 再减 3 五次得到。

(6) mW 列需要乘 10 两次再 5 次除以 2。EIRP 等于+21dBm 或 125mW。

3 +			× 2	
10 −	dBm	mW	÷ 10	
	0	1		
+10	10	10	×10	发射机
+10	20	100	×10	
−3	17	50	÷2	
−10	7	5	÷10	连接器
+3	10	10	×2	
+3	13	20	×2	
+3	16	40	×2	
+10	26	400	×10	天线
+10	36	4000	×10	
−3	33	2000	÷2	
−3	30	1000	÷2	
−3	27	500	÷2	
−3	24	250	÷2	
−3	21	125	÷2	

练习 3.5

10 与 3 规则，案例 4

本案例中，需要用外置定向天线对仓库某区域提供无线覆盖。无线接入点传输功率 30mW。无线接入点与天线间的连接电缆产生 3dB 的衰减。天线提供 20dBi 的增益，如图 3-4 所示。计算 IR 与 EIRP 值。

图 3-4　案例 4 的示意图

有时候并不总能利用 10 与 3 规则进行计算，无论怎么做，都无法通过 10 和 2 得到 mW 值。本练习就是一个例子，无法设置 mW 与 dBm 相等，但仍可以用提供的信息得到 mW 值。

(1) 不用创建模板设置 0dBm 等于 1mW，键入发射机的发射功率，本案例中是 30mW。

(2) 在 dBm 栏中，写入未知(unknown)。尽管你不知道 dBm 值，但仍可以执行必要的计算。

3 +			× 2
10 −	dBm	mW	÷ 10
	unknown	30	

(3) 连接电缆与连接器产生了 3dB 的衰减，在 dB 栏减 3，mW 栏除 2，得到 IR 值为 15mW。

		dBm	mW		
3	+			×	2
10	−			÷	10
		unknown	30		
	−3	unknown − 3	15	÷ 2	

(4) 天线产生 20dBi 增益，在 dBm 栏增加两次 10，在 mW 列两次乘 10 得到 EIRP 值为 1 500mW。另外我们知道天线增益 20dB，馈线衰减 3dB，可以得到比原始 dBm 高 17dB 的增益。尽管你不知道原始的 dBm 值，但是你能看出它增加了 17dB。

		dBm	mW		
3	+			×	2
10	−			÷	10
		unknown	30		
	−3	unknown − 3	15	÷ 2	
	+10	unknown + 7	150	× 10	
	+10	unknown + 17	1 500	× 10	

3.3.2 射频数学小结

在射频数学章节中，涵盖了很多概念、公式和案例，现在做个小结。请务必记住：在射频系统中的不同位置计算功率及衰减和增益影响是射频数学的本质。下面是利用对数进行射频数学运算的计算公式：

$dBm = 10 \times \log_{10}(P_{mW})$

$mW = 10^{(dBm \div 10)}$

如果打算利用 10 与 3 规则，那么记住下面四项简单任务，就完全没有问题了。

- 3dB 增益= mW × 2
- 3dB 衰减= mW ÷ 2
- 10dB 增益= mW × 10
- 10dB 衰减= mW ÷ 10

表 3-3 提供了绝对功率 mW 与 dBm 的对照关系。

表 3-3 dBm 与 mW 对照表

dBm	mW	功 率 级 别
+36dBm	4 000mW	4W
+30dBm	1 000mW	1W
+20dBm	100mW	1/10W
+10dBm	10mW	1/100W
0dBm	1mW	1/1 000W
−10dBm	0.1mW	1/10mW
−20dBm	0.01mW	1/100mW
−30dBm	0.001mW	1/1 000mW
−40dBm	0.000 1mW	1/10 000mW
−50dBm	0.000 01mW	1/100 000mW

(续表)

dBm	mW	功 率 级 别
-60dBm	0.000 001mW	1/1 000 000mW
-70dBm	0.000 000 1mW	1/10 000 000mW
-80dBm	0.000 000 01mW	1/100 000 000mW
-90dBm	0.000 000 001mW	1/1000 000 000mW

3.4　本底噪声

本底噪声(noise floor)是某个特定信道的环境或背景的射频能量级别。背景能量包括来自周边 802.11 传输设备发出的调制或编码过的比特流，也包括来自非 802.11 设备发出的未经调制的能量，例如微波炉、蓝牙设备和便携电话等。任何电磁设备都有可能提高在某个特定信道的本底噪声的振幅。

本底噪声的振幅，有时也简称为背景噪声，在不同的环境下也会不同。例如 2.4GHz ISM 信道通常的本底噪声值为-100dBm，然而在嘈杂的 RF 环境下，例如制造工厂，这个值可能为-90dBm，因为有许多电子器械在工厂内运行。还应当注意的是，5GHz 信道的本底噪声几乎总是低于 2.4GHz 信道，因为在 5GHz 信道很少拥塞。

3.5　信噪比

许多 Wi-Fi 供应商把信号质量定义为信噪比(SNR)，如图 3-5，SNR 是接收信号与背景噪声水平(本底噪声)之间的差值，而不是比值。例如接收信号强度为-85dBm，而本底噪声为-100dBm 时，两者之间的差异就是 15dB，SNR 就是 15dB。

图 3-5　信噪比

如果 SNR 过低，本底噪声过于接近接收信号强度，可能导致数据传输遭到破坏并导致第二层重传。重传会对吞吐量和延迟造成负面影响。25dB 或以上的信噪比被认为信号质量很好，而 10dB 或以下的信噪比被认为信号质量很糟糕。

3.6 接收信号强度指示

接收灵敏度(Receive sensitivity)是指接收机可以成功接收所需要的射频信号功率等级。接收机可以成功接收的功率水平越低，表明接收灵敏度越好。想象我们正在观看一场曲棍球比赛。在你周边存在着来自各处的噪声。为了让你旁边的同伴听到你说话，你不得不按照某个级别的声音说话，这个级别就是接收灵敏度，即收发机在通常环境下可以正常解码所要求的最微弱的信号强度。就是说如果环境噪音比平时更强，那么可能就不得不提高喊话音量的级别。

在 WLAN 设备中，接收灵敏度通常被定义为一个与网络速度相关的函数。Wi-Fi 供应商通常指定其产品的接收灵敏阈值为不同的数据速率，如表 3-4 所示。通常数据速率越高要求接收信号的强度越高。不同的速率使用不同的调制技术和编码方式。越高的数据速率使用的调制编码方式越容易使传输数据遭到破坏，越低的数据速率所使用的调制编码方式越不容易使传输数据遭到破坏。

表 3-4 接收灵敏阈值(示例)

数 据 速 率	接收信号强度
54Mbps	-50dBm
48Mbps	-55dBm
36Mbps	-61dBm
24Mbps	-74dBm
18Mbps	-70dBm
12Mbps	-75dBm
9Mbps	-80dBm
6Mbps	-86dBm

在 802.11-2007 标准中，接收信号强度指示(Received Signal Strength Indicator，RSSI)的定义为 802.11 射频模块测量信号强度的相关指标。RSSI 测量参数范围为 0～255。无线局域网硬件制造商用 RSSI 作为 802.11 接收模块射频信号强度的相对测量值。如表 3-5，RSSI 指标通常被映射为接收敏感阈值(单位 dBm)。例如某个供应商产品的 RSSI 等于 30，表示接收信号强度为-30dBm。数值为 0 的 RSSI 指标代表-110dBm 的接收信号强度。另一个供应商产品的 RSSI 数值为 255 代表-30dBm 的接收信号强度，RSSI 数值为 0 代表-100dBm 的接收信号强度。

表 3-5 接收信号强度指示(RSSI)指标示例

RSSI	接收敏感阈值	信号强度(%)	信 噪 比	信号质量(%)
30	-30dBm	100%	70dB	100%
25	-41dBm	90%	60dB	100%
20	-52dBm	80%	43dB	90%
21	-52dBm	80%	40dB	80%
15	-63dBm	60%	33dB	50%
10	-75dBm	40%	25dB	35%
5	-89dBm	10%	10dB	5%
0	-110dBm	0%	0dB	0%

802.11-2007 标准还定义了另一个被称为信号质量(SQ)的指标，用来衡量接收模块的伪噪声(PN)代码的相关质量。简言之，信号质量就是影响编码技术(如巴克码或键控补码)的指标。任何可能导致误码率(BER)增加的因素(如较低的信噪比或多径现象)都可以触发 SQ 改变。

来自 RSSI 与 SQ 指标的信息参数可从 PHY 层传递到 MAC 子层。某些 SQ 参数可以和 RSSI 一起作为空闲信道评估(CCA)机制的一部分。尽管 SQ 指标与 RSSI 指标从技术上看是各自独立的测量方法，大部分 Wi-Fi 供应商仍然把两者都简化为 RSSI 指标。在本书中，RSSI 指标均指 SQ 与 RSSI 指标。

根据 802.11-2007 标准的描述，“RSSI 是接收到的射频能量的测量值。RSSI 与实际接收功率的映射是独立实施的。”换句话说，无线局域网供应商可以按照私有的方式定义 RSSI 值。RSSI 的范围可由供应商自己选择从 0 到最大值(小于等于 255)，许多供应商在产品文档和网站上中把 RSSI 的执行数值发布出来，而有些供应商并没有这么做。因为 RSSI 指标的规定是私有的，在比较不同制造商的无线网卡的 RSSI 值时会出现两个问题。首先，不同供应商可能选择不同的 RSSI 最大值，例如 A 供应商可能选择 RSSI 范围从 0 到 100，而 B 供应商选择从 0 到 30，于是 A 供应商表明当前信号为 25 时，B 供应商针对相同信号可能表达为 8。另外，A 供应商制造的无线网卡使用了更多的指标，在评估信号和信噪比时可能会显得更灵敏。

第二个问题是制造商可能采用不同的 RSSI 计数和比较范围。无线局域网 A 供应商可能的计数范围为 100，关联-100 到-10 的 dBm 值，而 B 供应商可能的计数范围为 60，关联-95 到-35 的 dBm 值。计数方案不同，取值范围也可能不同。

尽管 Wi-Fi 供应商采用私有的 RSSI 值，但在 RSSI 阈值取值方面是相似的，这对漫游和动态速率切换等机制很重要。在漫游过程中，客户端自行决定如何在无线接入点间移动。RSSI 阈值是客户端决定漫游切换的关键因素。RSSI 阈值也被用来进行动态速率切换(DRS)。漫游在本书的好几个章节都会阐述，动态速率切换会在第 12 章中详细论述。

真实世界场景

802.11 无线网卡可以测量出真实的本底噪声和信噪比吗？

应当理解，802.11 无线网卡(NIC)不是频谱分析仪，尽管它可以以惊人的速率收发数据，却无法看到周边的射频信号。因为唯一可以通过无线网卡编码过滤器的是比特流，由无线网卡报告的所有信息都来自于这些比特流。如果在无线网卡附近打开微波炉，无线网卡也只会显示出零噪声。来自于其他 802.11 设备的编码后的 RF 信号中的噪声变量也不能用来反映本底噪声值。可以真实测量非编码 RF 能量的只有频谱分析仪。

你可能在很多情况下看到过 802.11 设备显示出信号强度和信噪比，无线网卡的开发者通过信号、噪声和信噪比数据来了解 RF 设备的使用情况(好、一般、差)。

WLAN 专业人士在进行现场勘测计算的时候也需要知道噪声值，所以 WLAN 供应商就使用一些办法来估测本底噪声。因为 802.11 无线网卡只能处理比特，所以他们需要某种算法利用通过无线网卡的比特来计算噪声值。

与 RSSI 测量一样，每家供应商计算噪声的方法不同。有些供应商拒绝只依靠比特流估测噪声值，有些供应商则开发出了复杂的算法计算噪声值。最近有些 802.11 芯片制造商利用了

关闭编码过滤器的方法，直接利用从天线进入的 RF 信号，将 802.11 芯片变成一台初级的频谱分析仪，但这取代了 802.11 网卡处理数据的能力。这些新型芯片要么作为轻量型的频谱分析仪，要么作为普通网卡处理数据，永远无法同时拥有两个功能。因为芯片前端的过滤器能够识别 802.11 信号，把它交给 802.11 协议栈处理，而不是协议分析仪。未来可能会出现可以同时处理 802.11 协议和频谱分析的无线网卡。某些 AP 供应商也采用这些具有额外能力的 Wi-Fi 芯片为 AP 增加可选的频谱分析功能。

如果希望了解更多关于 802.11 无线网卡与频谱分析仪的区别，可以阅读 *CWAP Certified Wireless Analysis Professional Official Study Guide*(Sybex, 2011)。

3.7 链路预算

在部署无线电通信时，链路预算(Link Budget)就是指从发射机开始通过射频媒介直到接收机之间的所有增益和衰减的总和。链路预算计算的目的是确保最终的接收信号强度处于接收机的接收灵敏阈值之上。

链路预算计算包括原始传输增益、天线的无源增益和 RF 放大器的有源增益。所有增益的部分包括射频放大器和天线增益。所有衰减的部分包括衰减器、FSPL 和插入损耗(insertion loss)。在射频系统中安装的任何硬件都会导致一定程度的信号衰减，称为插入损耗。馈线一般每 100 英尺计算一次损耗，而连接器通常会增加 0.5dB 的插入损耗。

我们都知道射频信号在自由空间中传输时会产生衰减。图 3-6 描述了在点到点无线桥接链路中，由 FSPL 和各种 RF 组件产生的衰减。

图 3-6 链路预算组件

现在我们看一下图 3-7 和表 3-6 进行的点到点无线桥接链路预算的例子。本例中，天线

相距 10km，原始发射功率为+10dBm。请注意每个射频组件(如馈线和避雷器)产生的插入损耗。信号强度被天线放大后并在自由空间中传输时衰减。在桥接链路接收端接收到的最终信号强度为-65.5dBm。

图 3-7　点到点链路预算增益和衰减

表 3-6　链路预算计算

组　件	增益或衰减	信 号 强 度
收发机(原始发送信号)		+10dBm
10' LMR-600 电缆	-0.44dB	+9.56dBm
防雷器	-0.1dB	+9.46dBm
50' LMR-600 电缆	-2.21dB	+7.25dBm
抛物线天线	+25dBi	+32.25dBm
自由空间路径损耗	-120dB	-87.75dBm
抛物线天线	+25dBi	-62.75dBm
50' LMR-600 电缆	-2.21dB	-64.96dBm
防雷器	-0.1dB	-65.06dBm
10' LMR-600 电缆	-0.44dB	-65.5dBm
接收机(最终接收信号)		-65.5dBm

假设接收机的接收灵敏阈值为-80dBm，即低于-80dBm 的信号将无法识别。在最终的接收信号强度-65.5dBm 与接收灵敏阈值-80dBm 之间有 15dB 的缓冲。这 15dB 的缓冲是由链路预算计算确定的，我们称其为衰落容限(Fade Margin)，这将在下一节中讨论。

你可能想知道为什么这些数字都是负值，而之前遇到的大部分 dBm 值都是正值。图 3-8 列出了在办公环境下增益和衰减的变化。到目前为止主要计算 IR 和 EIRP，从图中看出正是

自由空间路径损耗使这些数字变成负值。在图 3-7 的计算中，接收信号是所有组件衰减和增益的汇总：

+20 dBm + 5 dBi − 73.98 dB + 2.14 dBi = −46.84 dBm

图 3-8 办公室链路预算案例

尽管最初信号传输强度几乎总在 0dBm(1mW)以上，但因为 FSPL，最终接收信号强度将总是低于 0dBm(1mW)。

3.8 衰落容限/系统操作容限

衰落容限(Fade margin)是指超过被要求信号阈值之上的部分。解释衰落容限的一个好方法就是将其想象成一个舒适区域。如果接收机的接收灵敏度是-80dBm，只要收到大于-80dBm 的信号，传输就可以成功。但问题是接收信号很容易受到外界影响而产生波动(如干扰或天气状况)。为了适应这种波动，在桥接链路中通常在射频接收灵敏阈值之上预留出 10dB 到 25dB 的缓冲，这个缓冲就称为衰落容限。

10dB 的衰落容限是绝对的最小值，适用于小于 3 英里的链路。超过 5 英里则至少需要 15dB 的衰落容限。链路越长，衰落容限应该越高。链路超过 5 英里时，推荐采用 25dB 的衰落容限。

我们来举个例子，接收机的灵敏度为-80dBm，通常接收到的信号强度为-76dBm。那么在正常条件下，通信会成功。然而因为外部影响，信号可能会增减 10dB。这意味着大多数情况下，通信虽然会成功，但是在偶发情况下，信号可能会波动到-86dBm，通信就会失败。通过在链路预算计算中增加 20dB 的衰落容限后，现在你可以宣称接收灵敏阈值变为-60dBm，从而要求接收信号大于-60dBm。当接收信号产生波动时，由于我们已经预先增加了缓冲，就不必再担心通信失败。

我们再回顾一下图 3-7，如果在-80dBm 的接收灵敏度基础上增加 10dB 的衰落容限，那么要求的链路信号强度就为-70dBm。因为该案例中计算得到的信号强度为-65.5dBm，通信会成功。如果选择 20dB 的衰落容限，被要求的信号强度就为-60dBm，基于图 3-6 的配置，你将得不到满意的信号强度来满足链路预算和 20dB 的衰落容限。

因为无线电通信会受到许多外部因素的影响，通过衰落容限提供一定级别的链路可靠性的做法很普遍。通过增加衰落容限，本质上是增加了链路的可靠性。在设计射频系统时可以把衰落容限当成接收信号缓冲或差错边界。在安装 RF 链路后，测量链路以确定实际上有多

大的缓冲是重要的。这个功能性测量就是系统操作容限(SOM)。SOM 就是实际接收信号与可靠连接必要的信号之间的差值。

真实场景

何时需要进行衰落容限计算？

无论何时进行户外无线局域网桥接链路设计，链路预算和衰落容限计算都是绝对必要的。例如，射频工程师在进行25 英里点到点桥接链路计算时，确定最终接收信号强度超过接收灵敏阀值 5dB。看起来射频通信会比较正常，然而，由于多径现象和天气状况可能会引起信号减弱，预留出一部分衰落容限的缓冲就非常必要了。一场猛烈的倾盆大雨可能使 2.4GHz 和 5GHz 频段的信号产生 0.08dB/mi(0.05dB/km)的衰减。超长距离的桥接链路，通常推荐至少 25dB 的系统操作容限来补偿由于射频行为(如多径现象)或由于天气状况(如雨、雾或雪)产生的衰减。

在进行室内无线局域网部署时，如果存在高多径或高本底噪声状况，通常最好预留出比供应商推荐的接收灵敏阀值高 5dB 的衰落容限。例如，要达到 802.11a/g 54Mbps 的数据速率，-70dBm 或者更强的信号强度是大部分 WLAN 供应商所要求的。在进行室内站点勘测过程中，-70dB 的射频测量值经常用来确定 54Mbps 的数据的覆盖范围。在高多径或高噪声环境中，采用 5dB 的衰落容限，即-65dBm 的射频测量值是被推荐的。

练习 3.6

链路预算和衰落容限

本练习中，使用一个 Microsoft Excel 文件来计算链路预算和衰落容限。需要在你的计算机中安装 Excel。

(1) 通过 http://www.sybex.com/go/cwna3e 下载文件 LinkBudget.xls，打开这个 Excel 文件。

(2) 在第 10 行中输入 25km 的链路距离。请注意在 2.4GHz 频段下 25km 的链路会产生 128dB 的路径损耗。

(3) 在第 20 行中输入 128 作为自由空间路径损耗(dB)。

(4) 在第 23 行中将射频接收灵敏度改为-80dBm。请注意现在最终接收信号是-69dBm，衰落容限只有 11dB。

(5) 尝试改变不同的组件(如天线增益和电缆损耗)确保衰落容限为 20dB。

3.9　小结

本章涵盖了射频通信的六个重要领域：

- 射频组件
- 射频测量

- 射频数学
- RSSI 阈值
- 链路预算
- 衰落容限

理解每个射频组件如何影响收发器的输出十分重要。无论何时添加、卸下或更换某组件，射频通信的输出都会发生改变。你需要理解这些变化，并且确保系统符合监管规定。本章介绍了下列射频组件和概念：

- 发射机
- 接收机
- 天线
- 各向同性辐射体
- 主动辐射器(IR)
- 等效全向辐射功率(EIRP)

除了要理解这些组件以及这些组件对传输信号的影响，还必须了解用于测量射频通信输出和改变的不同的功率单位和相对单位：

- 功率单位
  - 瓦(W)
  - 毫瓦(mW)
  - 分贝(dBm)
- 相对单位
  - dB
  - dBi
  - dBd

在熟悉射频组件及它们对于射频通信的影响并了解了不同的功率单位和相对单位后，你需要了解如何进行计算并确定射频通信是否可以成功。重要的是知道如何进行计算并了解如下影响射频链路工作的概念和术语：

- 10 与 3 规则
- 本底噪声
- 信噪比(SNR)
- 接收灵敏度
- 接收信号强度指示(RSSI)
- 链路预算
- 系统操作容限(SOM)/衰落容限

3.10 考试要点

理解射频组件。了解每一个射频组件的作用，那些组件产生增益，那些导致衰减。

理解功率单位和相对单位。确信你非常熟悉功率单位(绝对)与相对单位之间的区别，并

且了解所有功率单位和相对单位如何测量和使用。

能够进行射频数学运算。考试中不会出现对数函数，但你必须了解如何使用 10 与 3 规则，并能够基于场景计算功率值和相对变化。

了解射频数学的实际用途。该说的都说的，该做的也做了，问题是射频通信可以正常吗？理解 RSSI、SOM、衰落容限和链路预算是重要的。

了解测量 SNR 和本底噪声的重要性。理解某个信道的周边背景噪声可能破坏该信道的 802.11 数据传输。理解唯一能够测量不可解调的 RF 能量的设备是频谱分析仪。

定义 RSSI。RSSI 指标用来解释信号强度和信号质量的。802.11 无线客户端用 RSSI 指标来决定是否开启漫游和进行动态速率切换。

理解链路预算和衰落容限的必要性。链路预算就是指从发射机开始通过射频媒介直到接收机之间的所有增益和衰减的总和。链路预算计算的目的就是确保最终的接收信号强度在接收机接收灵敏阈值之上。衰落容限值是指超过被要求信号阈值之上的部分。

3.11　复习题

复习题的答案见附录 A。

1. What RF component is responsible for generating the AC signal?

   A. Antenna

   B. Receiver

   C. Transmitter

   D. Transponder

2. A point source that radiates RF signal equally in all directions is known as what?

   A. Omnidirectional signal generator

   B. Omnidirectional antenna

   C. Intentional radiator

   D. Nondirectional transmitter

   E. Isotropic radiator

3. When calculating the link budget and system operating margin of a point-to-point outdoor WLAN bridge link, what factors should be taken into account? (Choose all that apply.)

   A. Distance

   B. Receive sensitivity

   C. Transmit amplitude

   D. Antenna height

   E. Cable loss

   F. Frequency

4. The sum of all the components from the transmitter to the antenna, not including the antenna, is known as what? (Choose two.)

   A. IR

B. Isotropic radiator

C. EIRP

D. Intentional radiator

5. The highest RF signal strength that is transmitted from an antenna is known as what?

A. Equivalent isotropically radiated power

B. Transmit sensitivity

C. Total emitted power

D. Antenna radiated power

6. Select the absolute units of power. (Choose all that apply.)

A. Watt

B. Milliwatt

C. Decibel

D. dBm

E. Bel

7. Select the units of comparison (relative). (Choose all that apply.)

A. dBm

B. dBi

C. Decibel

D. dBd

E. Bel

8. 2dBd is equal to how many dBi?

A. 5dBi

B. 4.41dBi

C. 4.14dBi

D. The value cannot be calculated.

9. 23dBm is equal to how many mW?

A. 200mW

B. 14mW

C. 20mW

D. 23mW

E. 400mW

10. A wireless bridge is configured to transmit at 100mW. The antenna cable and connectors produce a 3dB loss and are connected to a 16dBi antenna. What is the EIRP?

A. 20mW

B. 30dBm

C. 2 000mW

D. 36dBm

E. 8W

11. A WLAN transmitter that emits a 400mW signal is connected to a cable with a 9dB loss.

If the cable is connected to an antenna with 19dBi of gain, what is the EIRP?

A. 4W

B. 3000mW

C. 3500mW

D. 2W

12. WLAN vendors use RSSI thresholds to trigger which radio card behaviors?

A. Receive sensitivity

B. Roaming

C. Retransmissions

D. Dynamic rate switching

13. Received signal strength indicator (RSSI) metrics are used by 802.11 radios to define which RF characteristics? (Choose all that apply.)

A. Signal strength

B. Phase

C. Frequency

D. Modulation

14. dBi is a measure of what?

A. The output of the transmitter

B. The signal increase caused by the antenna

C. The signal increase strength of the intentional transmitter

D. The comparison between an isotropic radiator and the transceiver

E. The strength of the intentional radiator

15. Which of the following are valid calculations when using the rule of 10s and 3s? (Choose all that apply.)

A. For every 3dB of gain (relative), double the absolute power (mW).

B. For every 10dB of loss (relative), divide the absolute power (mW) by a factor of 2.

C. For every 10dB of loss (absolute), divide the relative power (mW) by a factor of 3.

D. For every 10mW of loss (relative), multiply the absolute power (dB) by a factor of 10.

E. For every 10dB of loss (relative), halve the absolute power (mW).

F. For every 10dB of loss (relative), divide the absolute power (mW) by a factor of 10.

16. A WLAN transmitter that emits a 100mW signal is connected to a cable with a 3dB loss. If the cable is connected to an antenna with 7dBi of gain, what is the EIRP at the antenna element?

A. 200mW

B. 250mW

C. 300mW

D. 400mW

17. In a normal wireless bridged network, the greatest loss of signal is caused by what component?

A. Receive sensitivity

B. Antenna cable loss

C. Lightning arrestor

D. Free space path loss

18. To double the distance of a signal, the EIRP must be increased by how many dBs?

A. 3dB

B. 6dB

C. 10dB

D. 20dB

19. During a site survey in a manufacturing plant, the WLAN engineer determines that the noise floor is extremely high because of all the machinery that is operating in the plant. The engineer is worried about a low SNR and poor performance due to the high noise floor. What is a suggested best practice to deal with this scenario?

A. Increase the access points' transmission amplitude.

B. Mount the access points higher.

C. Double the distance of the AP signal with 6dBi of antenna gain.

D. Plan for coverage cells with a 5dB fade margin.

E. Increase the transmission amplitude of the client radios.

20. Which value should not be used to compare wireless network cards manufactured by different WLAN vendors?

A. Receive sensitivity

B. Transmit power range

C. Antenna dBi

D. RSSI

第 4 章 射频信号与天线概念

在该章中，你将学习以下内容：

- √ 方位图与正视图(天线辐射包络图)
- √ 解析极化图
- √ 波束宽度
- √ 天线类型
  - ▪ 全向天线
  - ▪ 半定向天线
  - ▪ 高度定向天线
  - ▪ 扇形天线
  - ▪ 阵列天线
  - ▪ 静态波束成形
  - ▪ 动态波束成形
  - ▪ 传输波束成形
- √ 可视视距
- √ 射频视距
- √ 菲涅耳区
- √ 地球曲率
- √ 天线极化
- √ 天线分集
- √ 多进多出(MIMO)
  - ▪ MIMO 天线
  - ▪ 室内 MIMO 天线
  - ▪ 室外 MIMO 天线

- √ 天线的连接与安装
  - 电压驻波比
  - 信号损耗
  - 天线安装
  - 天线布局
  - 室外装配考虑因素
  - 室内装配考虑因素
  - 正确使用与环境考虑
  - 防护等级
  - NEMA 外壳防护等级
  - ATEX 防爆指令
  - 国家电气规范危险区域(NEC)
  - 天线朝向与调校
  - 人身安全
  - 维护
- √ 天线配件
  - 电缆
  - 接头
  - 分离器
  - 放大器
  - 衰减器
  - 避雷器
  - 接地棒与接地线

两个或多个收发器之间的通信要求发射机天线必须以足够大的功率向外辐射射频信号，以便接收机接收并解析信号。天线安装对于通信成功与否至关重要。在小型办公环境中安装天线并非难事，只需将接入点放置在房间中央，并调整其发射功率至足以覆盖相应的区域即可。而在某些情况下，安装各种定向天线的难度不亚于智力拼图游戏。在正确理解天线的性质及其工作方式后，读者会发现，成功规划与安装无线网络所用的天线是一项熟能生巧的工作，它并没有想象中那么难，所获得的成就感也很大。

本章重点讨论天线的分类、类型以及它们辐射射频信号的方式。选择和安装天线类似于选择和安装家用照明灯。安装照明灯时，可供选择的灯具种类很多，比如台灯、吸顶灯、窄束或宽束定向聚光灯。第 3 章介绍了天线聚焦射频信号的概念。本章将介绍天线的类型及其辐射图，以及如何在不同环境中使用相应的天线。你还将了解全向天线的安装和对齐方式会由于接入点是否支持 802.11 n 而有所不同。

我们经常采用光的传播来解释射频辐射，不过二者并不完全相同，本章将讨论这种差异，还将介绍瞄准和调校天线的方法，读者会看到，“所见即所得”并非金科玉律。

除介绍天线本身外，本章还将介绍正确安装天线所需的配件。在办公环境中将天线与接入点相连即可，而在室外安装天线时需要使用专门的电缆、接头、避雷器和安装基座。本章将介绍安装天线所需的各种部件。

总之，本章将介绍选择、安装和调校天线所需的知识和技能，掌握这些技能有助于读者成功实施各种无线网络。无论是两栋建筑物之间的点对点无线桥接，还是为办公楼提供射频覆盖的无线网络，天线对于保证网络的良好运行都起着极为重要的作用。

4.1　方位图与正视图(天线辐射包络图)

市场上存在大量不同用途的天线，如同存在大量不同用途的灯具一样。选购家用灯具时，可将两盏灯打开并观察二者发散光的能力，以便比较它们的性能。

然而，评判不同天线的性能并非易事。工程师需要逐一观察天线，并使用射频表进行大量信号测量，然后在地面上或者代表测量环境的纸上将测量结果描绘出来。这项工作不但费时费力，结果还可能受到外界因素(如家具或附近的射频信号)的影响。为帮助潜在的客户选购天线，天线厂商为它们的产品绘制了方位图(azimuth chart)与正视图(elevation chart)，一般将二者称为辐射图。辐射图表示某一类天线辐射的信号图样，它在可控环境中绘制，其结果不受外界因素的影响。人们通常将方位图与正视图称为极化图(polar chart)或天线辐射包络图(antenna radiation envelope)。

图 4-1 显示了一种全向天线的方位图与正视图。方位图标记为 H 面，表示天线辐射图的俯视图。因为这是一根全向天线，你能从方位角图看到，它的辐射图是几乎完全圆的。正视图标记为 E 面，表示天线辐射图的侧视图。方位图和正视图上标记的度数与天线朝向不一定要保持一致，天线厂商可以按照各自的方式进行标注，用户读图时需要自行判断。

掌握以下几点有助于理解天线辐射图：

- 天线位于方位图或正视图的中央
- 方位图=H 面=俯视图

- 正视图=E 面=侧视图

极化图的外圆一般表示天线信号最强的部分。注意，极化图并不表示距离或功率(强度)大小，它只表示图中不同点功率之间的关系。

可将极化图与阴影做一个比较。手电移到距手较近的位置时，手的阴影将变大；手电移到距手较远的位置时，手的阴影将变小。阴影大小与手掌大小无关，阴影只代表手掌与手指之间的关系。对天线而言，辐射图将随着天线接收功率的变化而变化，但是信号图样以及辐射图表示的不同点功率之间的关系始终保持不变。

方位图/H 面

正视图/E 面

图 4-1 方位图与正视图

4.2　解析极化图

如前所述，一般将天线的方位图(H 面)与正视图(E 面)称为极化图。人们对极化图的理解经常有误，一个重要原因是没有理解极化图表示的是天线覆盖的分贝变换。分贝变换采用对数标度而非线性标度表示天线的辐射图。需要注意的是，对数标度是一种基于指数值的可变标度，因此极化图实际上是一种采用可变标度表示天线覆盖的可视图。

我们通过图 4-2 对极化图做一解释。最上面的图表示 4 个盒子，盒中的数字表示盒子的长度和宽度。虽然图中的 4 个盒子大小相同，但是每个盒子的长度和宽度实际上都是前一个盒子的两倍。我们不难画出 4 个物理尺寸相同的盒子，并在盒子中标明它们的实际大小。中间的图显示了 4 个盒子的实际尺寸。

图 4-2　对数/线性比较

那么，如何画出更多盒子(比如 10 个)呢？从最下面的图中可以观察到，将所有盒子表示为相同大小就能很容易画出全部盒子。在这个例子中，如果试图将每个盒子都表示为它们的实际大小(中间的图)，我们就无法在书页中画出所有的盒子。事实上，甚至整个房间可能都不够容纳这些盒子。由于标度以指数增加，为在图中画出所有的盒子，我们不必也无法按盒子的实际尺寸将它们描绘出来。

第 3 章讨论了射频数学。6dB 法则是工程上常用的一条法则，该法则指出：信号功率每降低 6dB，传输距离将减少一半；信号功率每降低 10dB，传输距离将减少约 70%。如图 4-3 所示，左侧的极化图以对数形式显示了一种全向天线的正视图，这种极化图通常在天线手册或规格表中出现。没有受过培训的工程师在读图时，可能对全向天线的垂直覆盖范围如此之大感到惊讶，但实际并非如此。读对数图时请务必记住，从信号的峰值功率开始，功率每降低 10dB，实际传输距离将减少 70%。在对数图中，每个同心圆之间的功率变化为 10dB。观察图 4-3 可以发现，第一旁瓣的功率比主瓣低 10dB。请读者理解波瓣与同心圆之间的关系。

在对数图中，功率每降低 10dB，相当于线性图中传输距离减少 70%。对比两张图可以发现，对数图中的旁瓣功率被转换到线性图中之后是微不足道的。正如读者看到的那样，图 4-3 所示的全向天线的垂直覆盖范围几乎可以忽略不计。

图 4-3 全向天线的极化图(E 面)

为进一步解释极化图，图 4-4 以对数形式显示了一种定向天线的正视图，以线性形式显示了这种天线的垂直覆盖范围。如果转动极化图并与安装在建筑物上的天线朝向保持一致，就能更清楚地观察到天线是如何对准另一栋建筑物的。

IMAGE©ARUBA NETWORKS, INC. ALL RIGHTS RESERVED. USED WITH PERMISSION.

图 4-4 定向天线的极化图(E 面)

4.3　波束宽度

许多手电的反射镜都是可调的，用户可以根据需要调节辐射光线的聚焦度。射频天线也可将辐射功率集中到一处，不过与手电不同，天线不是可调的，因此用户在购买天线之前就要确定所需的聚焦度。

波束宽度(Beamwidth)衡量了天线对信号的聚焦能力，一般在水平和垂直两个方向进行测量。如图 4-5 所示，测量波束宽度时，从天线信号的中心或功率峰值点开始，沿横轴与纵轴测量每一个信号功率降低为一半的点(−3dB 点)。通常将这些−3dB 点称为半功率点。横轴上两个半功率点之间的距离即水平波束宽度，单位为°。纵轴上两个半功率点之间的距离即垂直波束宽度，单位为°。

图 4-5　天线波束宽度

多数情况下，用户应参考厂商的产品手册以确定天线的技术规格，从而选择满足通信需要的天线。厂商一般在产品手册中提供了天线水平波束宽度与垂直波束宽度的数值，因此了解波束宽度的计算过程十分重要。

图 4-6 显示了这一过程。(1)第一步是确定极化图的标度。从图中可以观察到，实线圆分别表示功率为−10dB、−20dB 和−30dB，虚线圆分别表示功率为−5dB、−15dB 和−25dB。这些同心圆表示从信号功率峰值点开始的分贝降低。(2)为计算天线波束宽度，首先确定天线信号最强点在极化图中的位置。在图 4-6 中，数字 1 指向的点为信号功率的峰值点。(3)从峰值点沿信号图样向左右移动(数字 2 所指的两个方向)，直至到达与峰值点功率相差 3dB 的点(数字 3 所指的两个点)。这就是为何需要首先确定极化图标度的原因。(4)如图中深色虚线所示，将两个−3dB 点与极化图原点相连并测量其夹角(单位为°)，该夹角即为天线波束宽度。图 4-6 所示的天线波束宽度约为 28°。

图 4-6 波束宽度计算

虽然发射机产生的射频信号的大部分能量都被聚焦在天线波束宽度之内，但是仍有相当一部分信号会辐射到波束宽度之外。天线波束宽度之外的部分称为天线旁瓣或后瓣。观察不同天线的方位图可以看到，某些旁瓣和后瓣的尺寸相当大。尽管旁瓣和后瓣中的信号强度远小于主瓣内的信号强度，不过它们仍然在某些网络实现中发挥了重要作用。需要注意的是，调节点对点天线时，务必将其对准主瓣而不是旁瓣。

表 4-1 列出了 802.11 通信所用的各类天线及其波束宽度。

表 4-1 天线波束宽度

天 线 类 型	水平波束宽度	垂直波束宽度
全向天线	360°	7° ～80°
贴片天线/板状天线	30° ～180°	6° ～90°
八木天线	30° ～78°	14° ～64°
扇形天线	60° ～180°	7° ～17°
抛物面天线	4° ～25°	4° ～21°

表 4-1 提供的参考信息对于学习本章介绍的各类天线很有帮助。

4.4 天线类型

天线主要分为以下 3 类：

- **全向天线**　全向天线辐射射频信号的方式类似于台灯或落地灯的照明方式。全向天线可以为所有方向提供覆盖。
- **半定向天线**　半定向天线辐射射频信号的方式类似于壁灯的照明方式，与路灯照亮街道或停车场的方式也很类似，即提供大面积的定向照明。
- **高度定向天线**　高度定向天线辐射射频信号的方式类似于聚光灯的照明方式。聚光灯将光线聚焦到旗帜或标牌上，以提供高强度的照明。

3 类天线的用途各不相同。

请记住，这一节讨论的是天线类型而非照明。尽管将天线的工作方式与照明进行类比有助于理解天线的概念，但与光线不同，射频信号可以穿过墙壁与地板等坚硬的物体。

天线不仅可以作为辐射器聚焦发射信号的能量，也可以聚焦接收信号的能量。在室外用肉眼观察某颗星体时，星体看起来黯淡无光。如果使用望远镜观察，星体看起来会比较明亮一些。如果使用天文望远镜观察，则星体看起来将更加明亮。天线的工作原理与之类似，它既可以放大发射信号，也可以放大接收信号。高增益麦克风以同样的方式工作，它让观众既能通过电视看到喜爱的比赛，也能听到比赛的声音。

天线的英文复数形式

尽管这并非原则性问题，人们仍然很好奇天线的英文复数形式是 antennas 还是 antennae。简单地说，二者均可；确切地说，应视具体情况而定。当 antenna 作为生物学术语使用时，意为“触须”，其复数形式为 antennae，如“臭虫的触须”(antennae of a bug)。当 antenna 作为电子学术语使用时，意为“天线”，其复数形式为 antennas，如“接入点天线”(antennas on an access point)。

4.4.1 全向天线

全向天线向所有方向辐射射频信号。小型橡胶偶极天线(dipole antenna)是一种典型的全向天线，人们经常将其戏称为“橡皮鸭子天线”(rubber duck antenna)，这种天线也是大部分接入点默认使用的天线。第 2 章介绍了一种理论上的全向辐射器，理想的全向天线辐射射频信号的方式与之类似。最接近全向辐射器的设备是全向偶极天线。

下面这个简单例子有助于读者理解典型全向天线的辐射图。将食指竖起(代表天线)，并把一个面包圈套在食指上(表示射频信号)。如果将面包圈沿水平方向切开以便在上面涂抹黄油，那么面包圈的剖面就代表全向天线的方位图(或 H 面)。如果将面包圈沿垂直方向切开，那么面包圈的剖面就代表全向天线的正视图(或 E 面)。

第 3 章曾介绍过，天线可以聚焦或对准所辐射的信号。需要注意的是，天线的 dBi 值或 dBd 值越高，它聚焦信号的能力越强。在提到全向天线时，人们往往质疑它是如何将辐射到各个方向的信号能量集中在一起的。全向天线的增益越高，其垂直方向上的信号功率越低，水平方向上的信号功率越高。

图 4-7 显示了 3 种理论天线的正视图。从图中可以观察到，天线的增益越高，信号在水平方向上被拉伸得越厉害，即天线在水平方向上聚焦信号的能力越强。全向天线的水平波束宽度始终保持在 360°，垂直波束宽度介于 7°～80°之间，垂直波束宽度取决于天线种类。

图 4-7 全向天线的垂直辐射图

由于全向天线的增益越高，其垂直覆盖范围越窄，因此必须仔细规划全向天线的使用。如果在大楼一层安装增益较高的全向天线，其 360°的水平波束宽度足以为一层提供良好的覆盖；但是由于全向天线的垂直覆盖范围较窄，它可能无法为二层和三层提供良好的覆盖。某些情况下可能需要采用这种覆盖方式，但它并不适用于所有场合。在室内安装天线时，通常采用增益约为 2.14dBi 的低增益全向天线。

当天线单元的长度为偶分数(如 1/4 或 1/2)或波长的倍数(λ)时，天线的效率最高。2.4GHz 半波偶极天线(如图 4-8 所示)由两个天线单元构成，每个天线单元的长度为 1 英寸左右(0.025m)，方向相反。尽管图 4-8 所示的偶极天线是水平放置的，不过在实际中，偶极天线始终是垂直安装使用的。通常将若干个偶极天线彼此叠放在一起以构成增益更高的全向天线，这种天线称为共线天线(collinear antenna)。

图 4-8　半波偶极天线

全向天线一般在点对多点通信中使用。将全向天线安装在一台设备(如接入点)上，并将该设备置于一组客户设备的中央，从而为这些设备提供射频覆盖。高增益全向天线也可以用于在室外点对多点环境中连接多栋大楼，即处于中心位置的大楼屋顶安装全向天线，周围大楼安装指向中心建筑的定向天线。在这种配置中，既要确保全向天线的增益足够覆盖所要求的范围，也不能过高，以免由于垂直波束宽度过窄而无法为周围建筑提供充分的覆盖。

图 4-9 显示了由于天线增益过高导致的覆盖不足的情况。位于左侧的大楼可以正常收发数据，而位于右侧的大楼很可能无法获得良好的覆盖。为解决图 4-9 所示的这种问题，可以采用向下倾斜的扇形阵列代替高增益全向天线。本章稍后将讨论扇形天线。

图 4-9　全向天线的安装方式有误

4.4.2　半定向天线

与向所有方向辐射射频信号的全向天线不同，半定向天线设计用来在某一个方向上辐射信号。中短距离通信使用半定向天线，而远距离通信使用高度定向天线。

半定向天线普遍用于校园或街道两侧建筑物之间的桥接，高度定向天线适用于远距离通信。

半定向天线分为以下 3 类：

- 贴片天线(patch antenna)
- 板状天线(panel antenna)
- 八木天线(Yagi antenna)

贴片天线与板状天线如图 4-10 所示，准确地说，应将二者归入平板天线(planar antenna)。“贴片”是设计天线内部辐射单元的一种特殊方式。不过，人们通常并不严格区分“贴片天线”与“板状天线”这两个术语。如果无法确定天线属于哪一类，最好将其统称为“平板天线”。

平板天线可以用于 1 英里(1.6 km)之内的室外点对点通信，不过更常见的应用是作为中央设备的天线在室内环境中提供接入点到客户设备的单向覆盖。接入点普遍使用贴片天线或板状天线为大楼内的用户提供定向覆盖。平板天线可以有效覆盖图书馆、仓库、零售店等存在长直货架过道的环境。全向天线往往难以在上述环境中发挥作用，而平板天线可以安装在建筑物的侧墙上，并指向货架。由于平板天线的水平波束宽度接近 180°，因此信号几乎不会辐射到建筑物之外。在相对的两面墙上安装平板天线时，注意调整天线角度使射频信号尽可能对准过道辐射，从而提供必要的覆盖。

平板天线也经常用于为办公隔间的过道或医院走廊提供射频覆盖。将一部平板天线安装在大厅的一侧并指向走廊，就可以为走廊、房间和地面提供覆盖。平板天线的覆盖范围取决于发射机功率、天线增益、天线波束宽度(水平波束宽度与垂直波束宽度)以及建筑材料对射频信号的衰减程度。

八木天线(如图 4-11 所示)一般用于 2mi(约 3.2km)以内的中短距离点对点通信，高增益八木天线也可以用于远距离通信。

图 4-10　贴片天线外观与内部天线单元

图 4-11　八木天线外观与内部天线单元

半定向天线的另一个优点是可以安装在墙壁的高处，并向下倾斜对准需要覆盖的区域。全向天线则不具备这个优点，因为如果天线的一端向下倾斜，则另一端将向上翘起。由于信号几乎不会从半定向天线的后侧泄露出去，因此半定向天线可以提供良好的垂直覆盖。

图 4-12 显示了本节讨论的典型半定向板状天线的辐射图。需要注意，这只是某种天线的方位图与正视图，不同厂商生产的天线其辐射图可能会略有差别。

图 4-12　典型半定向板状天线的辐射图

4.4.3　高度定向天线

高度定向天线仅在点对点通信中使用，一般用于提供两栋建筑物之间的网络桥接。在所有类型的天线中，高度定向天线的波束宽度最为狭窄和集中。

高度定向天线分为抛物面天线(parabolic dish antenna)与栅格天线(grid antenna)两类。从外观上看，抛物面天线类似于安装在屋顶上的小型数字卫星电视天线。如图 4-13 所示，栅格天线类似于野外烧烤使用的烤架，其边缘略微向里弯曲。栅格天线需要接收的信号波长决定了天线网格的间距大小。

由于高度定向天线的增益很高，它非常适合在远距离点对点通信中使用，其最远传输距离可以达到 35 英里(56km)。

高度定向天线的传输距离较远，波束宽度较窄，这使得它更容易受到天线风载的影响。大风引起的天线移动或偏移称为风载(wind loading)。对高度定向天线而言，哪怕是轻微的移动都会使射频波束偏离接收天线，从而导致射频通信中断。而栅格天线的网格较大，抗风载能力很强，因此在强风环境中应考虑使用栅格天线。

图 4-13　栅格天线

除栅格天线外，强风环境中还可以考虑使用波束宽度较宽的天线。这种情况下，即使天线发生轻微的偏移，由于其覆盖范围较宽，天线仍然能接收到信号。但是请注意，波束宽度越宽，增益越低。使用抛物面天线时，强烈建议为天线增加天线罩，以便在一定程度上抵消大风对天线的影响。无论安装哪种天线，基座与天线质量对减小风载都有不可替代的作用。

4.4.4 扇形天线

扇形天线(sector antenna)是一种特殊的高增益半定向天线，它能提供型如饼状的覆盖信号图样。通常将多部扇形天线背靠背地连接起来，并安装在需要射频覆盖的区域中央。每部天线为各自的饼状区域提供覆盖，所有天线组合在一起就可以为整个区域提供全向覆盖。如图 4-14 所示，将若干扇形天线组合起来以提供 360° 的水平覆盖，这种配置称为扇形阵列(sectorized array)。

图 4-14 扇形阵列

与其他半定向天线不同，射频信号几乎不会从扇形天线的后侧(后瓣)泄露出去，这种特性使得扇形天线之间不会相互干扰。扇形天线的水平波束宽度在 60° ～180° 之间，而垂直波束宽度只有 7° ～17° 。扇形天线的增益一般在 10 dBi 以上。

与安装单一一部全向天线相比，安装一组扇形天线以提供全向覆盖具有更多的优点。首先，扇形天线可以安装在高处并向下倾斜一定角度，以对准所覆盖的区域。尽管全向天线也可以安装在高处，不过一旦全向天线的一端向下倾斜，另一端将向上翘起。

其次，每部扇形天线与一个独立的收发器相连，所有天线可以不受干扰地传输数据，这使得吞吐量大为提高。而单一一部全向天线一次只能向一台设备辐射信号。

最后，一组扇形天线可以提供远高于单一一部全向天线的增益，从而覆盖更大的区域。

扇形天线广泛用于蜂窝电话通信，并已开始在 802.11 网络中使用。

真实场景

蜂窝扇形天线无处不在

在城镇中步行或驾车时，请留意周围的无线电通信发射塔。许多发射塔周围都环绕着类似于天线环的物体，这些天线环就是扇形天线。如果一座发射塔围绕有多个天线环，说明多家手机运营商都在使用该发射塔。

4.4.5　天线阵列

从本质上说，天线阵列(antenna array)是一种天线系统，它由多个天线构成。这些天线协同进行一种被称为波束成形的工作。波束成形是一种将射频能量汇聚的方法。能量如果被汇聚意味着信号强度增强，接收方信噪比增强，因此传输效果更好。

有三种波束成形类型：静态波束成形、动态波束成形和传输波束成形。

1. 静态波束成形

静态波束成形使用定向天线，提供固定射频覆盖模式。静态波束形成使用多个定向天线，紧密地聚集在一起，从中心点向外辐射。静态波束成形也被称为室内扇形天线阵列。无线网络供应商 Xirrus 就使用室内扇形天线阵列来产生多个扇形波束。

如图 4-15 所示，每个扇形波束被分配不重叠的信道。如果使用 8 个天线覆盖 360 度，那么每个天线就必须有至少 45 度的波束宽度。如果你希望信道覆盖有轻微的重叠以提高漫游效果，可能需要在每侧考虑 5 度的覆盖，这样每个天线就需要覆盖 55 度的范围。室内扇形天线阵列可以提供 8、12 或 16 个定向天线提供 360 度高增益的覆盖。

图 4-15　静态波束成形——室内扇形天线阵列

2. 动态波束成形

动态波束成形在一个特定的方向以特定形状汇聚射频能量。像静态波束成形一样，信号的方向和形状被汇聚，但不同的是，信号的辐射模式可以在帧的基础改变。这可以为每个接收站提供最佳的信号。如图 4-16 所示，动态波束成形使用自适应天线阵列调整射频波束指向目标接收方。该技术通常被称为智能天线技术或 beamsteering。目前唯一提供动态波束形成的无线网络供应商功能是 Ruckus Wireless。动态波束形成功能不可用于在客户端上。

图 4-16 动态波束成形——自适应天线阵列

动态波束成形能够将下传方向的单播流量聚集在某个特定客户端所在的方向。但广播帧(如 Beacon)必须按照全向天线模式传输，这样处于各个方向的客户端才可以和 AP 通信。

3. 传输波束成形

传输波束成形(TxBF)通过传输多个相移信号，以便在发射机认为是接收机所处的位置同相到达。与动态波束成形不同的是，TxBF 不改变天线的辐射模式，也不存在定向波束。实际上，传输波束成形并不是天线技术；它是一种数字信号处理技术，通过在多个天线上重复传送信号，以期优化在客户端上的组合信号。通过仔细控制来自多个天线的传输信号的相位，可以提高增益，从而模拟出高增益定向天线的效果。传输波束成形的核心其实就是调整相位进行传输。

802.11n 修正案支持两种传输波束成型技术：隐式 TxBF 和显式 TxBF。隐式 TxBF 使用隐式通道探测过程优化不同射频传输链的相位差。两种 TxBF 方法都需要接收站的反馈，以便确定每个信号的相位差。较新的 802.11n 芯片组支持传输波束成形，这部分内容将在第 18 章中讨论。

4.5 可视视距

在没有阻碍的情况下，光从一点传播到另一点时，其传输路径理论上是一条直线，称为可视视距(line of sight，LOS)。不过受折射、衍射和反射等因素的影响，光的传输路径可能并非一条绝对的直线。下面是可视视距受环境影响的一个例子：夏天观察室外停车场的一个固定物体，由于路面的热气上升，因此物体看起来似乎在漂移。在射频通信中，可视视距与通信成功与否无关。

4.6 射频视距

点对点射频通信同样要求收发天线之间存在一条无阻碍的视距。安装点对点通信系统时，首先要确保可以从一部天线的安装位置直接、清楚地观察到另一部天线。不过这只是保证射频通信成功的条件之一，除此之外，可视视距的周围不能存在障碍物。环绕在可视视距

周围的区域称为菲涅耳区，一般也称其为射频视距。

4.7　菲涅耳区

菲涅耳区(Fresnel zone)是一个虚构的椭球体区域，它环绕在点对点收发天线之间的可视视距周围，如图 4-17 所示。

图 4-17　菲涅耳区

理论上讲，存在无数多个环绕可视视距的菲涅耳区(橄榄球状的同心椭球体)。如图 4-15 所示，最内侧的椭球体称为第一菲涅耳区，环绕在它周围的椭球体称为第二菲涅耳区，以此类推。本节仅讨论与射频通信有关的第一和第二菲涅耳区，为简单起见，图 4-17 只显示了这两个菲涅耳区。其他菲涅耳区对通信的影响几乎可以忽略不计。

第一菲涅耳区即使被部分阻挡，也会影响到射频通信的完整性。收发天线之间的障碍物会引起明显的反射和散射，菲涅耳区被阻挡还会使射频信号发生衍射或弯曲。信号衍射将导致天线接收到的射频能量减少，甚至导致通信链路中断。

图 4-18 显示了一条长度为 1 mi(1.6km)的链路。图中收发天线之间的直线表示可视视距，虚曲线表示第一菲涅耳区下半部分的 60%，实曲线表示第一菲涅耳区的下半部分，树木表示信号传输路径中可能存在的障碍物。

图 4-18　60%与 100%的菲涅耳区净空

对室外点对点桥接链路而言，如果传输路径中存在障碍物，那么任何情况下第一菲涅耳区被障碍物阻挡的比例都不能超过 40%，否则无法保证链路的稳定性。即使第一菲涅耳区被阻挡的区域没有超过 40%，也无法确保链路性能一定不受影响。因此，建议第一菲涅耳区被遮挡区域不超过 20%，特别是在林木茂盛的地区，因为树木的生长今后可能会影响到菲涅耳区。良好的链路设计应保证第一菲涅耳区完全可见。

传输路径中可能存在的障碍物包括树木和建筑。链路部署完毕后，应定期目测链路，以免树木生长和新建房屋阻挡到菲涅耳区。请记住，菲涅耳区是环绕在可视视距周围的立体区域。如果菲涅耳区被阻挡，可以考虑将天线移到其他位置(通常将天线升高)，或将障碍物移走(通常用链锯将树木锯掉——玩笑而已)。

为判断菲涅耳区是否被障碍物阻挡，读者需要熟悉以下几个计算菲涅耳区半径的公式。不过不必担心，CWNA 考试不会考查这些公式。

第一个公式用于计算收发天线视距中点处的第一菲涅耳区半径，该点处的菲涅耳区半径最大。公式如下：

$$r = 72.2\sqrt{\frac{D}{4F}}$$

式中 r 为菲涅耳区半径(单位：ft)，D 为链路距离(单位：mi)，F 为信号传输频率(单位：GHz)。

该公式描述了理想情况下通信链路应保持的菲涅耳区净空，但是这种理想的净空在工程中很难实现。因此下面介绍的第二个公式更为实用，它用于计算净空为 60%时的菲涅耳区半径，这是在收发天线视距中点处必须保持的最小净空值。公式如下：

$$r(60\%) = 60\% \times 72.2\sqrt{\frac{D}{4F}} = 43.3\sqrt{\frac{D}{4F}}$$

式中 r 为菲涅耳区半径(单位：ft)，D 为链路距离(单位：mi)，F 为信号传输频率(单位：GHz)。

以上两个公式都非常有用，不过它们也存在明显的局限性。两个公式都用于计算收发天线视距中点处的菲涅耳区半径。由于该点处的菲涅耳区最大，根据这两个公式就能确定天线距离地面的最小高度。如果天线的安装位置过低，地面可能会阻挡到菲涅耳区，从而导致通信质量下降。问题在于，如果已知的障碍物位于收发天线之间的其他位置，就无法使用上述公式计算菲涅耳区的半径。下面介绍的第三个公式用于计算收发天线之间任意位置处、任意菲涅耳区的半径：

$$r = 72.2\sqrt{\frac{N \times d_1 \times d_2}{F \times D}}$$

式中 r 为菲涅耳区半径(单位：ft)，N 为第几菲涅耳区(通常为 1 或 2)，d_1 为一座天线与障碍物之间的距离(单位：mi)，d_2 为障碍物与另一座天线之间的距离(单位：mi)，D 为收发天线之间的总距离($D=d_1+d_2$，单位：mi)，F 为信号传输频率(单位：GHz)。

下面举例说明如何计算菲涅耳区的半径。图 4-19 示了一条长度为 10mi(16.1km)的点对点通信链路，链路中的障碍物是一棵高为 40ft(12.2 m)的树木，树木与其中一部天线之间的距离为 3mi(4.8 km)。采用第三个公式计算 3mi(4.8 km)处的菲涅耳区半径，式中各参数的值如下：

$N = 1$(第一菲涅耳区)

$d_1 = 3\text{mi}$

$d_2 = 7\text{mi}$

$D = 10\text{mi}$

$F = 2.4\text{GHz}$

则 3mi(4.8km)处的菲涅耳区半径为

$$r = 72.2\sqrt{\frac{N \times d_1 \times d_2}{F \times D}} = 72.2\sqrt{\frac{1 \times 3 \times 7}{2.4 \times 10}} = 67.53\text{ft}$$

图 4-19　点对点通信中的潜在障碍物

如果树木的高度为 40ft(12.2 m)，该点处的菲涅耳区半径为 67.53ft(20.6 m)，则收发天线应安装在距离地面至少 108ft(40ft+67.53ft=107.53ft，四舍五入后为 108ft，即 32.9m)的位置，以确保菲涅耳区完全可见。假设允许障碍物阻挡最多 40%的菲涅耳区，这意味着需要保持 60%的菲涅耳区净空。67.53ft(20.6m)的 60%为 40.52ft(12.4m)，则天线距离地面的绝对最小高度为 81ft(40ft+40.52ft=80.52ft，四舍五入后为 81ft，即 24.7m)。下一节将介绍地球曲率，为补偿地球曲率对菲涅耳区的影响，需要将天线的安装位置调高。

由于高度定向天线的波束宽度很窄，它可以更好地聚焦发射信号。许多人认为，波束宽度越窄，菲涅耳区越小，这种看法并不正确。菲涅耳区的半径是信号频率与链路距离的函数。由于频率和距离是公式中仅有的变量，因此无论采用哪种天线和波束宽度，菲涅耳区的尺寸都是固定不变的。理论上说，第一菲涅耳区是环绕在点源周围的区域，在这一区域，电波与点源信号是同相的。第二菲涅耳区是环绕在第一菲涅耳区周围的区域，在这一区域，电波与点源信号是异相的。所有单数菲涅耳区的电波与点源信号都是同相的，所有偶数菲涅耳区的电波与点源信号都是异相的。

如果射频信号与主信号同频、异相且二者相交，则异相信号将减弱甚至抵消主信号(第 2 章讨论并采用 EMANIM 软件演示了这个问题)。由于反射是导致异相信号干扰主信号的因素之一，因此在评估点对点通信链路时，必须考虑第二菲涅耳区对信号的影响。如果第二菲涅耳区的信号由于天线高度和地形原因被反射到接收端，则链路质量可能会因此而降低。尽管这种情况并不常见，不过规划网络或排错时仍然应将第二菲涅耳区的影响考虑进去，在平坦、干旱的环境(如沙漠)中尤其要注意这个问题。此外，还应考虑菲涅耳区内的金属屋顶对信号的影响。

需要注意的是，菲涅耳区是一个三维立体区域。障碍物是否可能从上方阻挡菲涅耳区？

虽然树木不会从天空向下生长，但是铁路栈桥或高速公路可能会阻挡到下方的点对点桥接链路。如果出现这种罕见的情况，则必须为第一菲涅耳区的上半部分预留足够的净空。更常见的一种情况是在城市环境中部署点对点链路。大楼之间的通信链路上往往还存在其他建筑物，后者必然会影响无线通信。此类情况下，其他建筑物可能会从侧面阻挡到菲涅耳区。

到目前为止，所有关于菲涅耳区的讨论均与点对点通信有关。尽管菲涅耳区在所有射频通信中都存在，不过它的影响主要限于室外点对点通信。在室内环境中，墙壁和其他障碍物对信号的反射、折射、衍射与散射是影响链路质量的主要因素，菲涅耳区与通信是否成功关系不大。

4.8 地球曲率

安装远距离点对点射频通信链路时，另一个必须考虑的因素是地球曲率(earth bulge)。由于各地地貌的差异很大，因此无法严格界定地球曲率会在多远距离上影响通信链路。我们建议，如果收发天线之间的距离超过 7mi(11.3km)，则需要考虑地球曲率的影响。这是因为当链路距离超过 7mi(11.3km)时，弯曲的地表将开始阻碍菲涅耳区。为补偿地球曲率的影响，可以采用下面的公式计算天线需要升高的高度：

$$H = \frac{D^2}{8}$$

式中 H 为地球曲率的高度(单位：ft)，D 为收发天线之间的距离(单位：mi)。

根据这两节介绍的公式，不难估算出在考虑地球曲率时天线的实际安装高度。不过这个高度并非精确值，因为收发天线之间的地形可能会发生变化，而这里假设天线之间的地形保持不变。估算天线的实际高度时，需要已知或求出以下 3 个参数：

- 第一菲涅耳区半径的 60%
- 地球曲率的高度
- 任何阻挡菲涅耳区的障碍物的高度，以及障碍物与天线之间的距离

将上述 3 个参数相加，可得到计算天线实际高度的公式：

$$H = r(60\%) + H_{earth} + H_{OB} = 43.3\sqrt{\frac{D}{4F}} + \frac{D^2}{8} + H_{OB}$$

式中 H 为天线的实际高度(单位：ft)，D 为链路距离(单位：mi)，F 为信号传输频率(单位：GHz)，H_{OB} 为障碍物的高度(单位：ft)。

下面举例说明如何计算天线的实际高度。图 4-20 显示了一条长度为 12mi(19.3km)的点对点链路，链路中点处有一栋高为 30ft(9.1m)的办公楼，信号传输频率为 2.4GHz。将各参数的值用于公式，可以计算出收发天线应该安装在距离地面 96.4ft(29.4m)的位置：

$$H = 43.3\sqrt{\frac{D}{4F}} + \frac{D^2}{8} + H_{OB} = 43.3\sqrt{\frac{12}{4\times 2.4}} + \frac{12^2}{8} + 30 = 96.4\ \text{ft}$$

上面介绍的几个公式在计算菲涅耳区半径与天线高度时非常有用，不过 CWNA 考试并不会考查这些公式。

图 4-20　计算天线高度

4.9　天线极化

安装天线时需要考虑的另一个因素是天线极化(antenna polarization)。虽然很多人不太熟悉天线极化，但是它对于确保通信成功极为重要。无论安装哪种类型的天线，正确的极化校准都是必不可少的。无线电磁波从天线发出时，电磁波的振幅可能垂直或水平震荡。为了使接收信号最强，有必要使发射和接收天线极化方向相同。安装天线时采用水平极化或垂直极化均可，不过应采用同一种极化方式校准天线。

天线极化的正确术语为 antenna polarization，意指波束的方向。不应该使用 polarity，即极性。

室内环境中，由于射频信号在频繁的反射过程中经常会改变极化方式，因此极化对室内通信的影响不大。大部分接入点都使用低增益全向天线，将接入点固定在天花板时应采用垂直极化。笔记本电脑的分集天线内置在显示器两侧，当显示器与键盘相互垂直时，内置天线被垂直极化。

校准点对点或点对多点桥接链路时，采用正确的极化方式特别重要。如果链路两端测量到的接收信号电平在最好情况下仍然比预期的接收信号电平低 15dB～20dB，说明很可能发生了交叉极化。如果链路一端的接收信号电平低于预期，而另一端的接收信号电平高于预期，说明调节天线时对准的是旁瓣而非主瓣。

在 http://www.sybex.com/go/cwna3e 网站中包含一段相当不错的视频，这段长约 3 分钟名为 Beam Patterns and Polarization of Directional Antennas 的视频，介绍并演示了天线旁瓣和极化的影响。视频的文件名是 Antenna Properties.wmv。

4.10　天线分集

多径效应很容易导致无线网络(特别是室内无线网络)的性能下降。为补偿多径效应的影

响，接入点等无线网络设备普遍采用了天线分集(antenna diversity)技术。天线分集又称空间分集，接入点安装了两套共同工作的天线和接收机，以最大限度减小多径效应造成的不利影响。

由于 802.11 无线信号的波长小于 5in(12.7cm)，因此天线之间可以相隔很近而不会影响天线分集的效果。接入点侦听到射频信号时，它比较两副天线接收到的信号，并采用接收到较强信号的那副天线来接收数据帧。每接收一帧数据，接入点都会重新抽样并比较两副天线的接收信号功率，并始终采用接收到较强信号的天线接收下一帧数据。

大部分早期的 pre-802.11n 无线接口采用交换分集(switched diversity)。交换分集使用多副天线监听接收信号。到达接收机天线的信号存在多个副本，这些副本的幅度各不相同。交换分集选择幅度最好的信号，忽略其他信号。这种监听最佳接收信号的方式称为接收分集(receive diversity)。

发送信号时也可以使用交换分集，不过此时只使用一副天线。在最近一次接收信号的过程中，监听到最强信号的那副天线被选择出来，发射机将使用该天线发送当前的信号。这种采用监听到最近一次最佳接收信号的天线发送当前信号的方式称为发射分集(transmit diversity)。

如果接入点有两个用于天线分集的天线端口，应将两副天线安装在同一位置，并确保二者朝向一致。如果两副天线的方向相反，则无法获得良好的覆盖效果。天线之间的距离应为波长的因数(1/4λ、1/2λ、λ、2λ)。

由于天线之间相隔很近，人们往往怀疑天线分集的实际效果。第 3 章曾经介绍过，天线接收到的射频信号功率通常小于 10^{-8} mW(−80dBm)。在这种尺度上，接收信号之间哪怕是最微小的差异也会对通信产生巨大影响。此外，与接入点相互通信的客户设备经常分散在不同的位置，这些设备并非总是固定不动，这会进一步影响射频信号的传输路径。

接入点在收发数据时采用不同的处理方式。接入点使用多副天线向客户设备发送数据时，它无法判断客户设备将接收由哪副天线发射的信号。接入点会使用最近一次接收数据的那副天线来发送数据，这种方式一般称为发射分集，不过并非所有接入点都具备这种能力。

天线分集的种类很多。带有内部接口卡的笔记本电脑也有两副分集天线，它们内置在显示器的两侧。请记住，由于射频介质的半双工特性，采用天线分集时，任何时候只有一副天线可以收发数据。也就是说，无线接口卡使用一副天线发送数据帧时，无法同时使用另一副天线接收数据帧。

4.11 多进多出

MIMO(multiple-input multiple-output，多进多出)是一种相当复杂的天线分集技术。多径效应会影响信号质量，因此传统的天线系统都在如何消除多径效应上动脑筋。而 MIMO 系统正好相反，它利用多径效应来改善通信质量。在 MIMO 系统中，收发双方使用多副可以同时工作的天线进行通信。MIMO 系统通常采用复杂的信号处理技术来显著增强可靠性、传输范围和吞吐量。发射机采用这些技术同时发送多路射频信号，接收机再从这些信号中将数据恢复出来。

MIMO 技术定义在 802.11n 修正案中。确信来自不同无线射频链的信号按照不同路径传输是 MIMO 系统的关键目标之一，调校天线可以使信号传输路径产生差别，并引入不同 MIMO 信号的传输延迟，这一点可以提高 MIMO 接收机处理不同信号的能力。下面介绍 MIMO 天线类型；第 18 章将详细介绍 MIMO 技术，它是 802.11n 的重要组成部分。

4.12　MIMO 天线

对吞吐量和容量需求不断增加的无线网络，使用 802.11 n 接入点已经成为必然。802.11n 不只在室内的网络普遍应用，也开始应用于室外点对点无线网络。MIMO 天线选择和安装工作在这些环境中是非常重要的。

4.12.1　室内 MIMO 天线

关于室内的 MIMO 接入点，通常很少涉及天线问题。许多新型的企业级 MIMO 接入点都有集成天线，没有突出在 AP 以外的天线。如果 AP 没有集成天线，MIMO AP 上可能有三个全向天线直接。这些天线有些可拆卸，并可以选择更高增益的全向天线。

安装或配置 MIMO 天线与分集天线不同，你并不希望天线处于在相同方向。一个天线应垂直，其他两根天线应该倾斜。倾斜角度也是需要讨论的一个话题。室内环境可能存在很多反射表面，环境本身就能提供必要的多径信号。把天线倾斜 30°～45° 的做法可能是个好主意。任何两根天线都不应该处于相同的方向。倾斜天线的目标是帮助创建多径环境，但你可能不想改变天线的覆盖模式。

4.12.2　室外 MIMO 天线

大多数室外 MIMO 接入点每个射频卡都有两根天线。正如室内 AP，多径可以被 MIMO 设备利用提供更高的数据率。因此，在保证相同的射频覆盖范围的同时如何改变两根天线的辐射路径成为关键。在室外环境中，达到这个目标需要更多的支持及技术手段，通常由网络设计者和安装者来选择和布置天线。因此许多 AP 和天线制造商设计出了全向和定向 MIMO 天线。

为了彼此区分两个信号，定向 MIMO 天线将两个天线单元纳入一个物理天线中，一个垂直极化固定，另一个水平极化固定，并用两个连接头接到接入点上。如果该接入点是多频的，每个频率的射频模块都有两个天线连接头。请注意一定要确保同一天线的两根电缆与同一个射频模块接头相连。

要提供全向的 MIMO 覆盖，可以利用特别的成对全向天线。每对全向天线都由一个垂直极化的全向天线和一个水平极化的全向天线组成。因为旧式的非 802.11n 接入点使用全向天线时，需要购买相同类型的天线。但室外 MIMO 全向天线由于每个天线有不同的极化方向，通常具有不同的长度和宽度。如果不熟悉这些天线对，单看不同的天线外形，你可能以为寄错了产品。

4.13 天线连接与安装

天线本身是无线网络的重要组成部分，而天线的安装与连接对于无线收发器同样重要，连接与安装不当将抵消天线为网络带来的有利因素。与天线安装密切相关的 3 个因素是 VSWR、信号损耗与实际的天线装配。

4.13.1 电压驻波比

VSWR(voltage standing wave ratio，电压驻波比)是衡量交流信号阻抗变化的参数。在射频通信系统中，设备之间的阻抗失配或阻抗变化将产生电压驻波。阻抗是交流信号的电阻值。电阻的标准计量单位是欧姆(Ω)，以德国物理学家乔治·欧姆(Georg Ohm)的名字命名。发射机产生交流无线信号，信号沿电缆传输到天线。由于阻抗失配，一部分入射能量(正向能量)将被反射回发射机。

阻抗失配可能出现在系统的任何位置，不过引起阻抗失配的原因通常是无线发射机与电缆、电缆与天线之间的阻抗突变。反射能量的大小取决于发射机、电缆和天线之间的阻抗失配程度。电缆上同一点处反射波与入射波的电压之比称为电压反射系数(voltage reflection coefficient)，一般用希腊字母 ρ 表示。

当采用分贝形式表示电压反射系数时，后者称为回程损耗(return loss)。一个理想的系统不存在阻抗失配(系统各处的阻抗都相同)，入射能量被百分之百传输给天线(不计电缆本身的电阻损耗)，因此反射能量为零。我们称这种情况下的电缆是匹配的，此时电压反射系数为 0，回程损耗(以 dB 为单位)无穷小。如果传输线上入射波与反射波的振动方向一致但传输方向相反，则二者叠加后将形成驻波(standing wave)。驻波波形是周期性的，驻波上存在电压、电流和功率的多个波峰与波谷。

VSWR 为传输线上电压最大值(发射机产生的入射电压)与电压最小值(天线的接收电压)之比，它是衡量阻抗失配的指标。理想情况下，VSWR 等于 1:1，不过这在实际中无法实现。典型的 VSWR 在 1.1:1～1.5:1 之间，美军军用标准规定的 VSWR 为 1.1:1。

$VSWR=V_{max} \div V_{min}$

当发射机、电缆和天线的阻抗匹配时(即不存在驻波)，电缆各处的电压相等。由于电缆上不存在电压波峰与波谷，这种匹配的电缆称为平直线缆(flat line)，平直线缆的 VSWR 等于 1:1。从表 4-2 中可以观察到，阻抗失配增大时，VSWR 也会增大，传输给天线的功率将随之减小。

表 4-2 VSWR 引起的信号损耗

VSWR	辐射功率	功率损耗	功率损耗(dB)
1:1	100%	0%	0dB
1.5:1	96%	4%	接近 0dB
2:1	89%	11%	＜1dB
6:1	50%	50%	3dB

如果 VSWR 较大，意味着有很大一部分电压被反射回发射机，使得本应传输给天线的信号功率或幅度减小(出现损耗)。这种正向幅度损耗称为回程损耗，单位为 dB。此外，反射回来的功率将进入发射机。如果发射机没有采取保护措施，过大的反射功率或电压峰值可能引起发射机过热和损坏。注意，VSWR 会导致信号强度降低和波动，甚至使发射机出现故障。

为最大限度减小 VSWR，首先要确保所有无线网络设备的阻抗都是匹配的。大多数无线设备的阻抗为 50 Ω，不过用户应查阅设备手册进行确认。连接不同的系统部件时，应确保所有接头安装正确，密合严紧。

4.13.2　信号损耗

将发射机连接到天线时，应尽可能确保发射机产生的信号功率传输给天线。为此，应特别注意连接发射机与天线的电缆和接头。我们将在第 4.14“天线配件”一节中回顾电缆、接头以及安装天线时使用的其他部件。如果部件质量较差或安装不当，接入点很可能无法正常工作。

4.13.3　天线安装

前面曾经介绍过，为确保无线网络以最佳状态运行，必须正确安装天线。安装天线时需要重点考虑以下几个因素：

- 布局
- 装配
- 正确的用途
- 天线的朝向与调校
- 人身安全
- 维护

布局

天线类型决定了可用的天线布局。安装全向天线时，应将天线置于被覆盖区域的中央。请记住，全向天线的增益越低，其水平覆盖范围越小，垂直覆盖范围越大；全向天线的增益越高，其水平覆盖范围越大，垂直覆盖范围越小。由于高增益全向天线的垂直覆盖范围较小，因此它的安装位置不应过高，否则天线可能无法为地面上的客户设备提供足够的信号覆盖。

安装定向天线时，应根据水平波束宽度与垂直波束宽度调整天线指向。确保天线增益合适同样重要。如果天线的辐射功率过高，它将覆盖超出所需的范围，从而形成潜在的安全漏洞。此外，应将收发器的输出功率调低，以免覆盖区域过大。天线辐射功率过高不仅会造成安全隐患，还会影响到周围的其他用户。

安装室外定向天线时，除考虑水平波束宽度与垂直波束宽度之外，还需要正确计算菲涅耳区的尺寸并采取相应方法固定天线。

室内装配考虑因素

确定天线的安装位置之后，下一步是选择采用何种安装方式。有许多种安装室内天线的方法。大多数 AP 至少有几个孔洞，可通过螺丝固定在墙上。大多数企业级 AP 都允许将 AP

固定到天花板或者墙上。这些安装组件可以轻易地把 AP 安装到吊顶的金属导轨上。

在室内安装天线的方法很多，不过美观和安全是经常要考虑的两个问题。许多行业(特别是酒店、医院等服务性行业)都要求所安装的天线不会影响到设施的美观，使用专业机柜与吊顶板能避免将接入点和天线暴露给外界。其他行业(特别是学校和公共环境机构)更关心如何确保接入点和天线的安全。可以将接入点置于安全机柜中，接入点与天线之间通过短电缆相连。某些天线还设计有吊顶板，以便与周围环境融为一体。如果安全是需要重点考虑的因素，则应将天线安装在墙壁高处或天花板上，以防止无关人员接触天线。

如果 AP 或天线安装在天花板底下，孩童经常喜欢跳起来触碰这些天线或者投掷东西尝试让天线移动。所以也需要考虑天线安装的位置。

室外装配考虑因素

不少天线(特别是室外天线)都安装在发射塔上，通常使用装配夹钳和 U 型螺栓固定天线。安装定向天线时，可以使用特别设计的倾斜-旋转式安装工具瞄准并固定天线。在多风环境中安装天线时(存在无风的屋顶或发射塔吗？)，应考虑风载的影响，并采用正确的方法固定天线。

正确使用及环境考虑

务必不要混用室外天线与室内天线。室外天线经过特殊设计，可以抵御较大的温差变化以及雨、雪、雾等天气状况。除采用合适的天线之外，还应针对不同环境选择合适的天线架设基座。

随着无线网络的应用扩展，无线不仅可能安装在恶劣的环境，也可能安装在易燃易爆的环境下，如矿井或钻井平台。在这些环境下，AP 和天线的安装要求特殊的存储单元或特别的施工流程。

下面将介绍大约四个分类标准。前两个标准指定设备可以承受的恶劣条件，后两个标准指定允许设备运行的环境。这些只是举个四个例子来描述存在的标准和如何将它们应用到设备和环境。当在所在国家或地区安装设备时，你需要进一步研究确定是否有必须或应该满足的要求。

- 防护等级(Ingress Protection Rating)

防护等级(Ingress Protection Rating)有时也称为国际防护等级，简称 IP Code(请不要跟 TCP/IP 协议中的 IP 协议混淆)。IP 等级标准由国际电工技术委员会(IEC)颁布，等级格式为 IP 开头，后面跟两个数字或者后面一个数字和一个或两个字母。

IP 代码的第一个数字用来区分预防固体物体侵入设备可以提供的防护程度，第二个数字用来区分预防液体入侵设备可以提供的防护程度。如果没有提供以上这些防护之一的话，该数字将被替换为字母 X。

固体数字可以是 0(没有保护)到 6(防尘)之间的值。液体数字可以是 0 到 8，从 0(没有保护)、1(滴水)、4(任何方向溅水)、6(强大的水流)到 8(水浸大于一米)。

- NEMA 外壳防护等级(NEMA Enclosure Rating)

NEMA Enclosure Rating 标准由美国电气制造业协会颁布，该标准与 IP 分级标准类似，但 NEMA 标准还关注其他一些特性，如抗腐蚀、垫片老化、建筑建设方面。

NEMA 外壳防护等级标准定义在 NEMA 标准 250-2008 中的“Enclosures for Electrical

Equipment (1000 Volts Maximum)”文档中。这个文档定义了对外部固体物质如泥土、灰尘、纤维方面防护等级及外部水、油及冷却剂的防护等级。NEMA 分级标准的格式是数字或者数字紧跟一个字母，如“Type 2”或“Type 12K”。

- ATEX 防爆指令

ATEX 有两个指令：

ATEX 95　涉及的设备和防护系统在潜在的爆炸性环境中使用。

ATEX 137　适用于工作场所，目的是保护和改善爆炸性环境的工人的安全和健康。

在欧盟国家的组织机构必须遵循这些指令以保护员工。ATEX 指令的名称来自于法国的 94/9/EC 指令："Appareils destinés à être utilisés en ATmosphères Explosives"。

雇主必须将存在爆炸性环境的工作区域划分为不同的区域，区域可以划归为气雾环境或粉尘环境。本规定适用于所有设备，不论其属于机械、电气、采矿或本质安全性仪表行业。

- 国家电气规范危险区域(National Electrical Code Hazardous Locations)

国家电气规范(NEC)是进行电气设备安装架线工作的安全标准。本文档并不具备法律强制性，但是当前已经被许多美国当地和州政府采纳，在哪些地方已经成为法律规定。NEC 的子部分谈到了危险区域，并将危险区域按照类型、条件和物质的性质做了分类。

按照类型分为：

Class I——气体或烟雾

Class II——尘埃

Class III——纤维和飞毛

可以按照条件进一步细分为：

分支 1——正常条件(如装运码头上普通的一天)

分支 2——异常条件(同一个装运码头，但出现容器内物泄露)

最后的分类基于危险物质的性质。此值由大写字母 A 到 G 代表。

天线的朝向与调校

安装天线前应参考厂商提供的安装建议，安装定向天线时尤其要注意这一点。这是因为定向天线的水平波束宽度与垂直波束宽度各不相同，安装时的极化方式也不相同，正确的朝向对于保证通信成功至关重要。

天线安装大致分为以下五步：首先，确定链路两端的天线极化方向一致；其次，根据天线的安装位置确定采用何种装配方式；第三，校准天线。请注意需要调校天线的方向和垂直倾角。第四，馈线和连接头的防水及安全固定。第五，对 AP 和天线的安装记录并拍照。未来你可以更容易确定天线是否发生了移动，这有助进行故障排错。

正如本章前面提到的那样，随着户外 802.11n 和 MIMO 技术的出现，特殊的户外全向 MIMO 天线开始被设计使用，这种天线成对安装，一个能够产生垂直极化的信号，另一个产生水平极化的信号。

人身安全

安装天线时，怎样强调安全问题都不为过。由于天线一般安装在发射塔或屋顶，安装人员往往需要借助梯子才能到达这些位置。重力与大风会给安装人员和在下面协助的人员带来不便。

作业前应仔细规划，并备好安装天线所需的各种工具和设备。准备工作不足或爬上爬下

寻找工具会增加受伤的风险。

作业时应留意附近的天线。高度定向天线聚焦射频能量的能力很强，过量辐射会危害安装人员的健康。作业时不要给天线通电，也不要离周围的天线过近。你可能并不了解其他天线系统的频率或功率输出，也不了解其对健康的危害程度。

在天花板、房椽或发射塔安装天线(以及任何其他设备)时，务必确保安装牢固，不会松动。天线无论大小，从仓库顶棚掉落下来都是非常危险的。

天线安装人员应考虑参加有关射频卫生与安全的课程。这些课程介绍了 FCC(美国联邦通信委员会)和 OSHA(美国劳工部职业安全与卫生管理局)的相关法规，以及如何根据这些法规进行安全作业。

在天线杆、发射塔或屋顶等高处安装天线时，应考虑聘用专业人员。专业人员不仅经过了培训，他们也拥有必要的安全设备和工伤保险。

如果用户计划自己安装无线设备，应制定一套当地职业安全机构认可的安全策略。除射频安全培训之外，用户应参加有关攀登安全的认证培训。此外，强烈建议用户接受急救与心肺复苏(CPR)方面的培训。

维护

维护分为预防性维护与诊断性维护两类。安装天线时务必谨慎，以防日后出现问题。由于天线在安装完成之后往往难以再次接触，因此用户必须认真考虑这个看似简单的建议。采用正确的预防性措施能最大限度地减小风损和水损。安装天线时务必将所有螺母、螺栓与螺钉拧紧，并确保所有电缆密合严紧，以免因为大风而晃动。

冷缩管(cold-shrink tube)或同轴密封胶(coaxial sealant)可以降低电缆或接头渗水的风险，从而防止水损。另一种常见的方法是将电工胶带与胶泥粘在电缆或接头的表层，以保证安装时完全不透水。如果使用胶泥，务必先旋紧接头，缠紧胶带再裹胶泥。如果接头不必拆开，那么可以直接将胶泥裹在接头处。

由于热缩管(heat-shrink tube)会遇热收缩并形成绝缘表层，电缆将因受热而损坏，因此安装天线时不宜使用热缩管。硅酮(silicone)内部会产生气泡并聚集潮气，它也不宜在安装天线时使用。

另一种布线技术是滴水环(drip loop)。滴水环将电缆上的水导入环的底部并排出，以防止水沿电缆渗入接头或进入建筑物的电缆出口。

人们往往在出现问题时才想起检查天线。我们建议定期目视查看天线，以便及时发现潜在的问题。如果难以直接观察到天线的安装位置，可以使用双筒望远镜或高变焦镜头相机作为辅助工具。

4.14 天线配件

第 3 章介绍了构成射频通信系统的主要部件，不过其他部件和参数对于射频通信同样重

要。频率响应、阻抗、VSWR、最大输入功率以及插入损耗都是天线配件的关键指标。这一节将讨论天线部件和配件。

4.14.1　电缆

电缆选型或安装不当会降低射频通信的质量，这种影响比其他部件或外界因素造成的影响大得多，安装天线电缆时请牢记这一点。下面列出了选择与安装电缆时需要注意的一些问题：

- 务必选择合适的电缆。确保电缆阻抗与天线和收发器的阻抗匹配，如果阻抗失配，VSWR 造成的回程损耗将影响链路质量。
- 确保电缆支持通信所用的频率。厂商通常会在手册中提供电缆的截止频率，它是电缆可以支持的最低与最高频率，一般将其称为频率响应。例如，LMR 电缆是射频通信中普遍使用的一种同轴电缆。LMR-1200 型电缆可以用于 2.4GHz 传输，但无法用于 5GHz 传输，5GHz 传输最高只能使用 LMR-900 型电缆。
- 电缆会在通信链路中引入信号损耗，电缆厂商提供的图表或计算工具能帮助用户确定损耗大小。Times Microwave Systems 生产的 LMR 电缆的衰减表如图 4-21 所示。图表左侧列出了各类 LMR 电缆的名称。图表中，位置越靠下的电缆质量越好。一般而言，电缆的质量越好，粗度与硬度越大，造价越高，安装难度越大。图 4-21 还显示了电缆在通信链路中引入的分贝损耗，其中第一行是电缆的工作频率。例如，长度为 100ft(30.5m)的 LMR-400 型电缆会在 2.5GHz(2500MHz)链路中引入 6dB 的信号损耗。

Times Microwave Systems											
LMR 电缆\频率	30	50	150	220	450	900	1 500	1 800	2 000	2 500	5 800
100A	3.9	5.1	8.9	10.9	15.8	22.8	30.1	33.2	35.2	39.8	64.1
195	2	2.5	4.4	5.4	7.8	11.1	14.5	16	16.9	19	29.9
195UF	2.3	3	5.3	6.4	9.3	13.2	17.3	19	20.1	22.6	35.6
200	1.8	2.3	4	4.8	7	9.9	12.9	14.2	15	16.9	26.4
200UF	2.1	2.7	4.8	5.8	8.3	11.9	15.5	17.1	18	20.2	31.6
240	1.3	1.7	3	3.7	5.3	7.6	9.9	10.9	11.5	12.9	20.4
240UF	1.6	2.1	3.6	4.4	6.3	9.1	11.8	13	13.8	15.5	24.4
300	1.1	1.4	2.4	2.9	4.2	6.1	7.9	8.7	9.2	10.4	16.5
300UF	1.3	1.6	2.9	3.5	5.1	7.3	9.5	10.5	11.1	12.5	19.8
400	0.7	0.9	1.5	1.9	2.7	3.9	5.1	5.7	6	6.8	10.8
400UF	0.8	1.1	1.8	2.2	3.3	4.7	6.2	6.8	7.2	8.1	13
500	0.5	0.7	1.2	1.5	2.2	3.1	4.1	4.6	4.8	5.5	8.9
500UF	0.6	0.8	1.5	1.8	2.6	3.8	5	5.5	5.8	6.6	10.6
600	0.4	0.5	1	1.2	1.7	2.5	3.3	3.7	3.9	4.4	7.3
600UF	0.5	0.7	1.2	1.4	2.1	3	4	4.4	4.7	5.3	8.7
900	0.3	0.4	0.7	0.8	1.2	1.7	2.2	2.5	2.6	3	4.9
1200	0.2	0.3	0.5	0.6	0.9	1.3	1.7	1.9	2	2.3	不支持
1700	0.1	0.2	0.3	0.4	0.6	0.9	1.3	1.4	1.5	1.7	不支持

UF = Ultraflex (more flexible cable)

图 4-21　同轴电缆衰减表

- 频率越高，衰减越大。5GHz 的 WLAN 网络的电缆损耗大于 2.4GHz WLAN 网络。
- 应选购带有预切和预装接头的电缆，或聘用专业人员进行安装。

接头安装不当将增加通信链路的损耗，抵消使用高质量电缆带来的效果。此外，接头安装不当还会导致信号在电缆中反射，从而造成回程损耗。

4.14.2 接头

安装 802.11 设备使用的天线时，可供选择的接头种类非常多。这是因为 FCC 在 Report & Order 04-165 中要求每种放大器必须采用唯一的接头或电子识别系统，以杜绝未认证天线的使用。这项规定旨在防止用户在收发器上安装未经授权的高增益天线(无论出于有意还是无意)，因为这种天线的 EIRP 可能会超出 FCC 或其他监管机构允许的最大值。

作为对这一规定的回应，一些电缆厂商推出了尾纤适配器电缆(pigtail adapter cable)。这种电缆一般是两端带有不同接头的短电缆段，长度约为 2ft(0.6m)。尾纤电缆相当于适配器，它起到接头转换的作用，以连接不同类型的天线。

尾纤电缆通常被 Wi-Fi 爱好者或网络安装人员用于测试目的，但是监管机构并不认可这种电缆。请记住，由于尾纤电缆往往会违反射频管理规定，因此不推荐使用。

选购电缆的许多原则同样适用于选购接头和其他配件。务必确保射频接头的阻抗与其他射频设备的阻抗相匹配。此外，不同接头支持的工作频率有所不同。接头会在射频链路中引入损耗，质量较差的接头更有可能引起连接或 VSWR 方面的问题。射频接头平均会增加 0.5dB 的插入损耗。

4.14.3 分离器

分离器将射频信号分解为两路或多路独立的信号，它也被称信号分离器、射频分离器、功率分离器或功率分配器。一般而言，射频分离器仅在特殊情况下使用，例如将多部扇形天线与收发器连接在一起。使用 3 部 120° 扇形天线提供 360° 全向覆盖时，既可以将每部天线与各自的收发器相连，也可以使用三向分离器和等长的电缆将 3 部天线与一个收发器相连。这种情况下，不仅信号功率经过 3 次分解后会降低(称为通过损耗)，每个接头还会引入相应的插入损耗。由于这种分离器配置存在很多潜在的问题与变数，我们建议聘用经验丰富的射频工程师进行操作，并将其仅作为临时手段使用。

分离器更实际(不过仍不常见)的一种应用是监控传输功率。将分离器置于收发器、天线和功率表之间，可以有效监控输送给天线的功率。

4.14.4 放大器

射频放大器接收并放大收发器产生的信号，然后将其输送给天线。天线通过聚焦信号能

量以获得功率增益，而放大器通过增加信号能量以提高总功率，这种方式称为有源增益。

放大器分为单向放大器与双向放大器两类。单向放大器只能放大发射信号或者接收信号，双向放大器既可以放大发射信号，也可以放大接收信号。

放大器采用两种方式放大信号，一种是固定增益方式；另一种是固定输出方式。固定增益放大器对收发器产生的功率进行放大。与此相反，无论收发器产生的功率大小，固定输出放大器都不会对其进行放大，它只是产生一个与放大器输出相等的信号。

市场上也存在可调变增益放大器，但是我们并不推荐使用这种放大器。这是因为未经允许调整变增益放大器的输出可能会违反功率管理规定，或者导致发射功率不足。

大部分监管机构规定，主动辐射器的最大输出功率不应超过 1W。使用放大器的主要目的在于补偿电缆损耗，而不是为盲目扩大传输范围而提高信号功率。因此，应将放大器安装在尽可能靠近天线的位置。由于天线电缆存在损耗，所以电缆越短，损耗越小，输送给天线的信号功率越大。

除此之外还要注意，放大器不仅可以放大信号，也可以放大噪声。放大器将本底噪声提高 10dB 以上的情况并不鲜见。

放大器与所用的系统必须经过监管机构(如 FCC)的认证。将未经认证的放大器添加到无线网络中是不合法的。应在系统设计上下功夫，而不是单纯靠放大器增加信号功率。

4.14.5　衰减器

某些情况下可能需要降低天线辐射的信号功率。例如，安装短距离点对点链路时，用户或许希望降低天线的输出功率，以减小对周围射频设备的干扰。不过即使将收发器的功率设置为最低，输出信号的功率有时仍然可能超出实际需要。这时可以考虑在系统中增加一个固定损耗或可变损耗衰减器。衰减器(Attenuator)是一种尺寸类似于 C 型电池(2 号电池)的小型设备，两端带有电缆接头。信号通过衰减器时，其能量被后者吸收。固定损耗衰减器能衰减的能量是不变的，而可变损耗衰减器具有拨号或切换配置，用户可以根据需要调节衰减器的吸收能量。

可变损耗衰减器一般在室外站点勘测中使用，以模拟各种等级和长度的电缆造成的损耗。此外，可变衰减器还能测量点对点链路的实际衰落容限。逐渐增加衰减器的衰减幅度，直到链路中断，所获得的临界值可用来确定链路的实际衰落容限。

4.14.6　避雷器

无论是非直击雷(nearby lightning strike)引起的瞬时电流还是电子设备产生的静电，都可

以通过避雷器(lightning arrestor)重定向(分流)给大地。非直击雷或静电堆积会导致功率在短时间内急剧增加，而安装避雷器能保护电子设备的安全。读者可能注意到，这里使用了“非直击雷”一词，这是因为避雷器对直击雷(direct lightning strike)无能力为。典型的避雷器可以承受高达 5000A、50kV 的电涌。IEEE 要求避雷器在 8μs 以内将瞬时电流释放给大地，大部分避雷器只需不到 2 μs 就能完成这项工作。

避雷器安装在收发器与天线之间。由于避雷器无法保护位于避雷器与天线之间的设备，因此一般将其安装在尽可能靠近天线的位置，并将所有其他设备(放大器、衰减器等)安装在避雷器与收发器之间。图 4-22 显示了无线接口、线缆和天线的正确接地位置。避雷器在过电压作用后应整体更换，或更换其中的气体放电管(类似于保险丝)。大部分避雷器安装在建筑物的出口位置，电缆接地套件每隔 100ft(30.5m)安装在天线的周围。

图 4-22 安装防雷设备

如果将一小段光缆插入连接无线网桥与网络其他部分的以太网电缆中，就可以为系统提供额外的防雷保护。以太网–光缆适配器(称为收发器)将以太网电信号转换为适合在光缆中传输的光信号，再转换为以太网电信号。由于光缆的材质是玻璃，它使用光而不是电作为数据载体，因此光缆是绝缘的。此外，务必确保适配器电源的安全。

过高的瞬时电压或直击雷会导致避雷器失效，这时可以将光缆作为备份的防雷手段。如果天线遭到直接雷击，应考虑更换光缆与天线之间的所有部件。直击雷还可能击穿光缆链路并破坏链路另一端的设备，为避免这种情况的发生，需要将射频电缆接地。

真实场景

不仅无法预测雷击的时间，也无法预测雷击的后果

美国波士顿北区一栋具有 200 年历史的 5 层商业大厦最近遭到非直接雷击。这栋砖石褐

砂岩大厦并不是该地区最高的建筑，它坐落在一座小山脚下，周围环绕着类似的建筑。瞬时电流沿排水管穿过密集的以太网电缆，破坏了 PC 以太网卡的收发器电路和以太网集线器端口。虽然公司大约有半数的以太网设备与集线器端口出现故障，但是所有软件仍然可以正常工作，所有电源指示灯和端口指示灯也显示正常。表面上看，问题似乎出在布线上。

用户往往无法判断问题是否与雷击有关，某些表象可能会导致误判。此时，检查避雷器有助于诊断与确定问题。

4.14.7　接地棒与接地线

雷电在击中物体后总是会寻找阻碍最小的路径。更确切地说，雷电将沿阻抗最小的路径传输。防雷与接地设备的工作原理就在于此。接地系统由接地棒与接地线组成，它构成一条通向大地的低阻抗路径。雷击产生的瞬时电流沿这条低阻抗路径(而不是电子设备)被导入大地，从而保护了昂贵的电子设备。

接地棒与接地线也用于创建共同接地点。创建共同接地点的一种方法是将一根铜棒打入地面，并使用接地线将电气和电子设备与铜棒相连。接地棒的长度至少为 6ft(1.8m)，且完全打入地面，仅在上部留有缠绕接地线所需的必要空间。共同接地点构成了一条阻抗最小的路径，雷击产生的电涌将沿这条路径释放给大地，从而达到保护所有电子设备的目的。

对天线发射塔而言，接地棒应埋设在每个发射塔支柱的附近，通过 2 号镀锡铜线(No.2 tinned copper wire)并采用放热焊接将接地棒与支柱连接起来。如图 4-23 所示，虚线代表 2 号镀锡铜线，圆点代表接地棒，接地棒之间通过 2 号镀锡铜线相连形成接地环。冰桥(ice bridge)和建筑物接地应与接地环接合在一起，以提供相等的接地电势。

图 4-23　接地环

EIA/TIA 222F 标准第 12.2.2 节指出："接地应由至少两根直径为 0.625 in(1.6cm)的镀锌钢棒构成，它们打入地面的深度不少于 8ft(2.4m)……采用 6 号(或更高)镀锡裸铜线将接地棒与最近的发射塔支柱接合在一起，或将接地棒与发射塔的金属底座接合在一起。"现行标准规定，通过 2 号实心线将母线和其他部件与接地环相连，而接地环一般采用 2/0 多股绞合裸铜线。

4.15 小结

这一章重点介绍了射频信号与天线的概念，天线对于保证射频通信成功至关重要。802.11 无线局域网使用以下 4 类天线：

- 全向天线(偶极天线、共线天线)
- 半定向天线(贴片天线、板状天线、八木天线)
- 高度定向天线(抛物面天线、栅格天线)
- 扇形天线

不同天线的信号辐射图各不相同，可通过方位图与正视图来观察天线的辐射图。

这一章还回顾了安装点对点通信链路时需要重点考虑的几个问题：

- 可视视距
- 射频视距
- 菲涅耳区
- 地球曲率
- 天线极化

本章最后介绍了 VSWR 与天线安装的相关问题，并讨论了各种天线配件及其用途。

4.16 考试要点

理解无源增益与有源增益。理解天线如何产生无源增益，收发器与放大器如何产生有源增益。

了解天线的分类、类型、辐射信号的方式以及使用环境。务必了解 3 类主要的天线以及每类天线包含哪些天线。了解各种天线的异同，并理解每种天线的使用场合。务必理解方位图、正视图、波束宽度、天线极化与天线分集。

深刻理解菲涅耳区。务必理解与安装点对点通信链路有关的各种问题。尽管CWNA 考试不会考查菲涅耳区与地球曲率的计算公式，不过考生仍应了解这些概念以及应用公式的场合。

理解与天线连接、安装与配件相关的问题。收发器和天线之间的各种电缆、接头与设备都会影响到天线辐射的信号。理解产生增益与造成损耗的设备。理解 VSWR 的概念，并了解各种 VSWR 值的含义。了解天线配件的种类、用途与使用场合。

4.17 复习题

复习题的答案见附录 A。

1. Which of the following devices produce active gain? (Choose all that apply.)
   A. RF transceiver
   B. Parabolic dish
   C. RF amplifier
   D. Sector antenna
2. The azimuth chart represents a view of an antenna's radiation pattern from which direction?
   A. Top
   B. Side
   C. Front
   D. Both top and side
3. What is the definition of the horizontal beamwidth of an antenna?
   A. The measurement of the angle of the main lobe as represented on the azimuth chart.
   B. The distance between the two points on the horizontal axis where the signal decreases by a third. This distance is measured in degrees.
   C. The distance between the two –3dB power points on the horizontal axis, measured in degrees.
   D. The distance between the peak power and the point where the signal decrease by half. This distance is measured in degrees.
4. Which antennas are highly directional? (Choose all that apply.)
   A. Omni
   B. Patch
   C. Panel
   D. Parabolic dish
   E. Grid
   F. Sector
5. Semidirectional antennas are often used for which of the following purposes? (Choose all that apply.)
   A. Providing short-distance point-to-point communications
   B. Providing long-distance point-to-point communications
   C. Providing unidirectional coverage from an access point to clients in an indoor environment
   D. Reducing reflections and the negative effects of multipath

6. The Fresnel zone should not be blocked by more than what percentage to maintain a reliable communications link?

A. 20 percent

B. 40 percent

C. 50 percent

D. 60 percent

7. The size of the Fresnel zone is controlled by what factors? (Choose all that apply.)

A. Antenna beamwidth

B. RF line of sight

C. Distance

D. Frequency

8. When a long-distance point-to-point link is installed, earth bulge should be considered beyond what distance?

A. 5miles

B. 7miles

C. 10miles

D. 30miles

9. A network administrator replaced some coaxial cabling used in an outdoor bridge deployment after water damaged the cabling. After replacing the cabling, the network administrator noticed that the EIRP increased drastically and is possibly violating the maximum EIRP power regulation mandate. What are the possible causes of the increased amplitude?(Choose all that apply.)

A. The administrator installed a shorter cable.

B. The administrator installed a lower-grade cable.

C. The administrator installed a higher-grade cable.

D. The administrator installed a longer cable.

E. The administrator used a different-color cable.

10. Which of the following are true for antenna diversity? (Choose all that apply.)

A. The transceiver combines the signal from both antennas to provide better coverage.

B. Transceivers can transmit from both antennas at the same time.

C. The transceiver samples both antennas and chooses the best received signal from one antenna.

D. Transceivers can transmit from only one of the antennas at a time.

11. To establish a 4-mile point-to-point bridge link in the 2.4GHz ISM band, what factors should be taken under consideration? (Choose all that apply.)

A. Fresnel zone with 40 percent or less blockage

B. Earth bulge calculations

C. Minimum of 16dBi of passive gain

D. Proper choice of semidirectional antennas

E. Proper choice of highly directional antennas

12. The ratio between the maximum peak voltage and minimum voltage on a line is known as what?

A. Signal flux

B. Return loss

C. VSWR

D. Signal incidents

13. What are some of the possible negative effects of an impendence mismatch?(Choose all that apply.)

A. Signal reflection

B. Blockage of the Fresnel zone

C. Erratic signal strength

D. Decreased signal amplitude

E. Amplifier/transmitter failure

14. When determining the mounting height of a long-distance point-to-point antenna, which of the following needs to be considered? (Choose all that apply.)

A. Frequency

B. Distance

C. Visual line of sight

D. Earth bulge

E. Antenna beamwidth

F. RF line of sight

15. Which of the following are true about cables? (Choose all that apply.)

A. They cause impedance on the signal.

B. They work regardless of the frequency.

C. Attenuation decreases as frequency increases.

D. They add loss to the signal.

16. Amplifiers can be purchased with which of the following features? (Choose all that apply.)

A. Bidirectional amplification

B. Unidirectional amplification

C. Fixed gain

D. Fixed output

17. The signal between the transceiver and the antenna will be reduced by which of the following methods? (Choose all that apply.)

A. Adding an attenuator

B. Increasing the length of the cable

C. Shortening the length of the cable

D. Using cheaper-quality cable

18. Lightning arrestors will defend against which of the following?

A. Direct lightning strikes

B. Power surges

C. Transient currents

D. Improper common grounding

19. The radius of the second Fresnel zone is_____. (Choose all that apply.)

A. Out of phase with the point source

B. In phase with the point source

C. Smaller than the first Fresnel zone

D. Larger than the first Fresnel zone

20. While aligning a directional antenna, you notice that the signal drops as you turn the antenna away from the other antenna, but then it increases a little. This increase in signal is cause by what?

A. Signal reflection

B. Frequency harmonic

C. Side band

D. Side lobe

第 5 章 IEEE 802.11 标准

在该章中，你将学习以下内容：

- √ 原始的 IEEE 802.11 标准
- √ 批准通过的 IEEE 802.11-2007 修正案
  - 802.11b
  - 802.11a
  - 802.11g
  - 802.11d
  - 802.11h
  - 802.11i
  - 802.11j
  - 802.11e
- √ 批准通过的 Post-2007 修正案
  - 802.11r-2008
  - 802.11k-2008
  - 802.11y-2008
  - 802.11w-2009
  - 802.11n-2009
  - 802.11p-2010
  - 802.11z-2010
  - 802.11u-2011
  - 802.11v-2011
  - 802.11s-2011
- √ IEEE 802.11 修正案草案
  - 802.11p
  - 802.11aa
  - 802.11ac

- 802.11ad
- 802.11ae
- 802.11af
- 802.11ah

√ 已经失效的修正案

- 802.11F
- 802.11T

√ 802.11m 工作组

第 1 章曾经介绍过，IEEE(电子与电气工程师协会)是负责创建与维护通信标准的专业组织，例如 IEEE 定义了有线网络使用的 802.3 以太网标准。为制定无线通信标准，IEEE 成立了若干个工作组(working group，WG)。例如，802.15 工作组负责制定个人域网(PAN)通信标准，802.15 标准定义了采用射频作为传输介质的蓝牙和 ZigBee 等无线技术。宽带无线接入工作组负责制定与管理 802.16 标准，后者通常被称为 WiMAX。本书重点介绍 IEEE 802.11 标准及其技术，该标准定义的局域网(LAN)通信同样采用射频作为传输介质。

802.11 工作组由常设委员会(standing committee)、研究组(study group，SG)与若干任务组(task group，TG)构成，包括超过 250 家无线企业以及 450 多名活跃的成员。例如，宣传常设委员会(Standing Committee – Publicity，PSC)负责 802.11 标准的推广，802.11 研究组(SG)负责进行 802.11 标准完善与更新的可行性研究。

IEEE 802.11：有关工作组与 802.11-2007 标准的更多信息

有关 IEEE 802.11 工作组的快速指南请参阅：

http://grouper.ieee.org/groups/802/11/QuickGuide_IEEE_802_WG_and_Activities.htm

可通过以下链接下载 802.11-2007 标准和被批准的修正案：

http://standards.ieee.org/getieee802/802.11.html

某些标准和被批准的修正案文件是免费的，其他的(特别是刚刚被批准的文件)需要付费。

各个 802.11 任务组负责对 MAC 任务组和 PHY 任务组开发的原始标准进行更正和修订。每个任务组由字母表中的一个字母标识，通常使用术语“802.11 字母汤”(802.11 alphabet soup)指代 802.11 任务组制定的所有修正案。当任务组形成时，他们被分配给下一个最高可用字母表中的字母，尽管修正案不一定按相同顺序批准。802.11 任务组已经完成并批准了大量针对原始标准的修正案。其他一些 802.11 任务组项目仍然处于活跃状态，并以修正案草案的形式存在。

这一章将讨论 802.11 原始标准、已经被 IEEE 批准通过的修正案(大部分修正案目前都被整合到 802.11-2007 标准中)以及 802.11 任务组制定的各项修正案草案。

5.1　IEEE 802.11 原始标准

1997 年 6 月，IEEE 公布了 802.11 原始标准(IEEE Std. 802.11-1997)。它是第一项无线局域网标准，一般将其称为 802.11 Prime。IEEE 在 1999 年对原始标准做了修订，并于 2003 年重新批准并公布，称为 IEEE Std. 802.11-1999 (R-2003)。2007 年 3 月 8 日，IEEE 批准通过了 802.11-2007 标准(IEEE Std. 802.11-2007)，后者是对 802.11-1999 标准的补充和完善。802.11-2007 标准是一份完整的文档，它整合了所有当时已经批准并公布的修正案。接下来发布版本的标准预计在 2012 年。

IEEE 仅在物理层与数据链路层的 MAC 子层定义了 802.11 技术。802.11 标准的本意并非针对解决上部层 OSI 模块，虽然在 802.11MAC 层和上层参数中相互交流，如服务质量(QoS)。

PHY 任务组与 MAC 任务组共同制定了 802.11 原始标准，并定义了 3 种最初的物理层规范。

红外技术 红外(infrared)技术采用光作为传输介质。虽然 802.11 原始标准的确定义了红外介质，但是目前的无线局域网早已不采用红外技术。更多有关红外技术在现代通信中如何实现的信息请参阅红外数据协会网站：www.irda.org。本书重点讨论 802.11 射频介质。红外设备通常被称为条款 16(clause 16)设备。

跳频扩频技术(FHSS) 可将射频信号分为窄带信号和扩频信号。如果射频信号的带宽大于传输数据所需的带宽，该信号就属于扩频信号。FHSS(frequency hopping spread spectrum，跳频扩频)是一种扩频技术，于第二次世界大战期间获得专利。由于跳频技术定义在 802.11 原始标准第 14 条款中，因此 802.11 FHSS 无线射频卡通常称为条款 14(clause 14)设备。

直序扩频(DSSS) 另一种普遍使用的扩频技术称为 DSSS(direct sequence spread spectrum，直序扩频)，它是最容易实现的一种扩频技术。802.11 DSSS 无线射频卡通常称为条款 15(clause 15)设备。

什么是 IEEE 条款？

IEEE 标准是层次严密、条理清晰的结构化文档，每个章节都有各自的编号。最高级别的章节(如 7)称为条款(clause)，较低级别的章节(如 7.3.2.4)称为子条款(sub-clause)。尽管每项修正案都是独立的文档，但是 802.11 任务组在制定修正案时，仍然根据原始标准对修正案中的章节进行编号。由于每份文档的条款与子条款的编号都是唯一的，当一项标准及其修正案被整合为另一项新标准(如 2007 年批准通过的 802.11-2007 标准)时，不必对章节编号进行任何调整。尽管这本书参考了 IEEE 802.11 标准条款，但在 CWNA(PW0-105)考试中条款编号不会列入考查范围。

802.11 原始标准定义，FHSS 和 DSSS 无线射频卡均使用无需牌照的 2.4GHz ISM(Industrial, Scientific, and Medical，工业、科学与医用)频段进行通信。802.11 DSSS 无线射频卡可以使用整个 2.4 ISM 频段(2.4GHz～2.4835GHz)的信道传输数据。802.11 FHSS 无线射频卡的工作频段略窄，根据 IEEE 的定义，FHSS 设备只能在 2.402GHz～2.480GHz 范围内使用宽度为 1 MHz 的副载波传输数据。

由于大部分无线局域网部署都采用新标准定义的技术，因此传统的 802.11 设备可能无法在目前的无线网络中使用。WLAN 企业可以选择生产 FHSS(条款 14)无线射频卡或 DSSS(条款 15)无线射频卡。但是，由于两种扩频技术的工作原理不同，不能互通，且往往难以共存。与油和水无法混合在一起类似，DSSS(条款 15)无线接口与 FHSS(条款 14)无线接口也无法相互通信。虽然传统的无线局域网部署大多采用跳频技术，但也有一些部署采用 DSSS 解决方案。

802.11 网络的传输速度如何呢？根据 802.11 原始标准的定义，FHSS 与 DSSS 的数据速率均为 1 Mbps 与 2 Mbps。可以将数据速率定义如下：在一个单帧传输中，物理层每秒所传输的比特数，通常以兆比特/秒(Mbps)表示。请记住，数据速率是速度而非实际吞吐量。每种介质访问方式和通信开销不同，所获得的总吞吐量也不同，但一般不超过可用数据速率的 50%。

第 6 章将详细介绍 FHSS 与 DSSS。

5.2 批准通过的 IEEE 802.11-2007 修正案

在 802.11 原始标准公布之后，IEEE 又陆续成立了新的任务组对原始标准进行补充和完善。截至本书写作时，各任务组已经通过并公布了 18 项修正案，在 2007 年，IEEE 通过整合多个已经被批准的修正案和原始标准，形成并颁布了 IEEE 802.11-2007 标准。2007 年的 IEEE Std. 802.11 文档包括以下内容：

- IEEE Std. 802.11-1999 (R-2003)
- IEEE Std. 802.11a-1999
- IEEE Std. 802.11b-1999
- IEEE Std. 802.11d-2001
- IEEE Std. 802.11g-2003
- IEEE Std. 802.11h-2003
- IEEE Std. 802.11i-2004
- IEEE Std. 802.11j-2004
- IEEE Std. 802.11e-2005

802.11-2007 标准还对之前的标准做了更正、澄清和完善。下面将按这些修正案获批的时间顺序对它们进行介绍。

CWNA 考试术语

2007 年，IEEE 将大部分获批的修正案与 802.11 原始标准整合到一份单一的文档中，它就是 802.11-2007 标准。原来的修正案在技术上不再存在，因为它们已被纳入同一文档中了。不过，Wi-Fi 联盟与大多数无线局域网专业人员仍然习惯采用各修正案的名字来称呼它们。

过去版本的 CWNA 考试中没有提到任何 802.11 修正案的名称。CWNA 考试主要考查每项修正案所定义的技术。例如，802.11b 是一项目前已经被整合到 802.11-2007 标准中的修正案，它定义了 HR-DSSS(High-Rate DSSS，高速直序扩频)技术。尽管人们仍然习惯使用 802.11b 这个名称，不过 CWNA 考试将统一采用术语 HR-DSSS 来指代 802.11b 技术。

因为诸如 802.11/a/b/g 的术语是由 Wi-Fi 联盟和普通公众广泛使用的，所以导致在考试中产生混淆。好消息是，最新版本的 CWNA 考试(PW0-105)已经决定主要使用更常见的 802.11 修正案术语。

在参加 CWNA 考试(PW0-105)之前，考生应理解不同技术之间的差异以及每种技术的原理。掌握各项修正案定义的技术对考生的职业发展不无裨益。CWNP 项目定期更新考试术语表，可从以下链接下载目前使用的术语表：http://www.cwnp.com/exams/cwnp_exam_terms.pdf。

5.2.1 802.11b

尽管 Wi-Fi 消费市场以极其惊人的速度持续增长，实际上为市场注入第一支强心剂的就是兼容 802.11b 的无线局域网设备。1999 年，IEEE 任务组 b(TGb)公布了 802.11b 修正案(IEEE Std. 802.11b-1999)。在对该修正案进行修订和更正之后，任务组 b 将其命名为 IEEE Std. 802.11b-1999/Cor1-2001。802.11b 修正案的完整内容请参阅 802.11-2007 标准第 18 条款。

802.11b 修正案定义的物理层介质是 HR-DSSS。802.11b 无线射频卡使用无需牌照的 2.4GHz ISM 频段(2.4GHz～2.4835GHz)进行通信。

真实场景

802.11b 设备能否与传统的 802.11 设备共存？

802.11b 无线射频卡通常被称为条款 18(clause 18)设备。802.11b 修正案定义的物理层规范是 DSSS，并不包括 FHSS。由于相当一部分传统的 802.11 部署都采用 FHSS 技术，因此 802.11b 无线射频卡无法向后兼容这些系统，也不能在这些部署中使用。但是 802.11b(条款 18)无线射频卡可以向后兼容传统的 802.11 DSSS(条款 15)无线射频卡，因此从理论上讲，802.11b HR-DSSS 无线局域网设备与传统的 802.11 DSSS 无线局域网设备可以相互通信。不过请注意，不同厂商对 IEEE 标准的理解可能存在差异，许多传统设备并没有经过任何兼容性测试(如 Wi-Fi 联盟的互操作性测试项目)。

TGb 主要研究如何在 2.4GHz ISM 频段获得更高数据速率，这通过采用称为 CCK(Complementary Code Keying，补码键控)的扩频/编码技术以及相位调制技术来实现。802.11b 无线接口使用巴克码(Barker code)作为扩频技术，支持 1Mbps、2Mbps、5.5Mbps 和 11Mbps 等 4 个数据速率。802.11b 系统向后兼容数据速率为 1Mbps 与 2Mbps 的 DSSS 系统，而数据速率 5.5 Mbps 与 11 Mbps 称为 HR-DSSS。需要再次强调的是，数据速率指可用带宽而非总吞吐量。802.11b 修正案的条款 18 还定义了一种称为 PBCC(Packet Binary Convolutional Code，分组二进制卷积码)的可选调制技术。

第 6 章将深入讨论巴克码、CCK 等扩频技术以及其他调制技术，并对 PBCC 做简要介绍。

5.2.2 802.11a

在批准 802.11b 修正案的同一年，IEEE 还批准并公布了另一项重要的标准，它就是 802.11a 修正案(IEEE Std. 802.11a-1999)。任务组 a(TGa)的工程师们致力于研究如何在新分配给无线局域网通信的 5GHz UNII(Unlicensed National Information Infrastructure，无需牌照的国家信息基础设施)频段使用一种被称为正交频分复用(OFDM)的 802.11 技术。在无需牌照的 5GHz UNII 频段上，802.11a 无线射频卡可以使用 3 个 100MHz 频段、总共 12 个信道传输数据。802.11a 修正案的完整内容请参阅 802.11-2007 标准第 17 条款。

与 5GHz UNII 频段相比，2.4GHz ISM 频段极为拥挤。微波炉、蓝牙设备、无绳电话等许多设备都工作在 2.4GHz ISM 频段，它们都可能对无线局域网造成干扰。此外，由于不少 802.11 网络也部署在 2.4GHz 频段(如多租户办公楼环境)，它们同样会干扰到用户的无线网络。

将 802.11a 设备部署在 5GHz UNII 频段的优点是，该频段目前相对空闲，干扰较少。当然，这 3 个 UNII 频段最终也会变得和 2.4GHz ISM 频段一样拥挤。FCC(美国联邦通信委员会)等监管机构已经开放了更多的 5GHz 频率空间供无线局域网通信使用，IEEE 在 802.11h 修正案中对此做了定义。

802.11a 无线射频卡最初利用 UNII-1、UNII-2 和 UNII-3 频段的 12 个信道传输。然而 5GHz 频率范围和频段需要受到不同国家的 RF 监管机构管理。该修正案主要是关于引入 OFDM 技术并提供更高的速率。

第 6 章将深入讨论 ISM 与 UNII 频段。

工作在 5GHz UNII 频段的 802.11a 无线射频卡一般被称为条款 17(clause 17)设备。802.11a 修正案要求 802.11a 设备必须支持 6Mbps、12Mbps 和 24 Mbps 等 3 个数据速率，最大数据速率为 54Mbps。大部分厂商的无线射频卡采用 OFDM(Orthogonal Frequency Division Multiplexing，正交频分复用)技术，可以支持 6Mbps、9Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps 和 54 Mbps 8 个数据速率。

第 6 章将深入讨论 OFDM。

还要注意的是，802.11a 无线射频卡无法与 802.11 传统、802.11b 或 802.11g 无线射频卡相互通信，原因如下。首先，802.11a 设备采用与 802.11 传统或 802.11b 设备不同的扩频技术。其次，802.11a 设备使用 5GHz UNII 频段传输数据，而 802.11 /802.11b/802.11g 设备使用 2.4GHz ISM 频段传输数据。不过正是因为 802.11a 设备与上述设备的工作频段不同，所以它们可以共存于同一物理空间。

当 802.11a 标准首次被批准的差不多两年后，802.11a 设备才出现。另外采用 OFDM 技术的无线射频卡的主板芯片组相当昂贵。正是这两个原因导致在企业中很少广泛部署 5GHz 无线局域网。随着芯片组价格下降，5GHz 频段网络部署也随之大幅增加。大多数 WLAN 厂商生产的 AP 均为双频设备，而大多数笔记本电脑自 2007 年以来都基本配备 802.11a/b/g 或者 802.11a/b/g/n 的无线网卡，这意味着这些客户端也有双频功能。企业级的无线部署大多同时支持 2.4GHz 和 5GHz 两个频段。

5.2.3 802.11g

2003 年，IEEE 公布了一项让 Wi-Fi 业界激动不已的标准，这就是 802.11g 修正案(IEEE Std. 802.11g-2003)。802.11g 无线射频卡使用 2.4GHz ISM 频段(2.4GHz～2.4835GHz)传输数据，一

般称为条款 19(clause 19)设备。802.11g 定义了 ERP(Extended Rate Physical，扩展速率物理层)技术。802.11g 修正案的完整内容请参阅 802.11-2007 标准第 19 条款。

任务组 g(TGg)主要研究如何通过增强 802.11b 物理层来增加带宽，同时保持与 802.11 MAC 子层的兼容。802.11g 修正案定义了两种强制和两种可选的 ERP 物理层规范。

两种强制的物理层规范是 ERP-OFDM(Extended Rate Physical OFDM，扩展速率物理层-正交频分复用)与 ERP-DSSS/CCK(Extended Rate Physical DSSS，扩展速率物理层-直序扩频)。ERP-OFDM 技术支持 6Mbps、9Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps 和 54Mbps 8 个数据速率，802.11g 设备必须采用 ERP-OFDM 才能达到这些数据速率。不过与 802.11a 修正案类似，802.11g 修正案仅要求 802.11g 设备必须支持 6Mbps、12Mbps 和 24Mbps 3 个数据速率。为向后兼容 802.11DSSS 与 802.11b 网络，802.11g 修正案采用 ERP-DSSS/CCK 技术，该技术支持 1Mbps、2Mbps、5.5Mbps 和 11Mbps 等 4 个数据速率。

ERP-DSSS/CCK、DSSS 与 HR-DSSS 之间的差异

从技术角度看，三者之间并无差异。802.11g 修正案的主要目的是在提高数据速率的同时，仍然保持与 802.11 DSSS 和 802.11b 无线接口的向后兼容性。802.11g(条款 19)设备采用 ERP-OFDM 以实现更高的数据速率。DSSS 是 802.11 DSSS(条款 15)设备使用的技术，HR-DSSS 是 802.11b(条款 18)设备使用的技术，ERP-DSSS/CCK 与这两种技术并没有本质上的区别。为向后兼容早期的 802.11 DSSS 与 802.11b(HR-DSSS)无线接口，802.11g 无线接口必须支持 ERP-DSSS/CCK。第 6 章将深入讨论 DSSS 技术。

802.11g 修正案还定义了两种可选的物理层规范，它们是 ERP-PBCC(扩展速率物理层-分组二进制卷积码)与 DSSS-OFDM(直序扩频-正交频分复用)。二者超出了本书的讨论范围，且很少被无线局域网厂商采用。

OFDM 与 ERP-OFDM 之间的差异

从技术角度看，二者之间并无差异，唯一不同的是传输频率。OFDM 指 802.11a(条款 17)设备，后者使用 5GHz UNII 频段(UNII-1、UNII-2 与 UNII-3 频段)收发数据。ERP-OFDM 指 802.11g(条款 19)设备，后者使用 2.4GHz ISM 频段收发数据。第 6 章将深入讨论 OFDM 技术。

真实场景

802.11g 接入点的厂商工作模式与实际吞吐量

802.11g 修正案定义了 ERP-DSSS 与 ERP-OFDM 两种强制的物理层规范，802.11g 接入点通常可以被配置为 3 种截然不同的模式。

B-only 模式 配置为这种模式的接入点仅支持 DSSS、HR-DSSS 与 ERP-DSSS/CCK 技术，此时的接入点实际相当于一个 802.11b 接入点。只有 802.11b 客户端可以与接入点相互通信，数据速率为 11Mbps、5.5Mbps、2Mbps 和 1Mbps。在这种模式下，网络的总吞吐量与 802.11b 网络相同。

G-only 模式　配置为这种模式的接入点只能使用 ERP-OFDM 技术与 802.11g 客户端进行通信。由于接入点不支持 ERP-DSSS/CCK、HR-DSSS 与 DSSS 技术，因此 802.11b 客户端无法与接入点建立关联。只有 802.11g ERP 无线接口可以与接入点相互通信，数据速率为 6Mbps～54Mbps。这种模式下，当接入点的数据速率为 54 Mbps 时，网络的总吞吐量约为 19Mbps～20Mbps。以 G-only 模式工作的无线局域网有时也称为 Pure G 网络。

B/G 模式　这是大多数 802.11g 接入点的默认工作模式，一般将其称为混合模式。配置为该模式的接入点支持 EPR-DSSS/CCK 与 ERP-OFDM 技术，因此 802.11 DSSS、802.11b 与 802.11g 客户端都可以和接入点通信，但是这会影响到网络性能。如果 802.11 DSSS 或 802.11b HR-DSSS 客户端试图与 802.11g 接入点建立关联，接入点将在第一时间通知所有的 802.11g 客户端启用保护机制，以便 802.11 DSSS、802.11b 与 802.11g 客户端能共存于同一物理空间。但是在启用保护机制之后，网络的吞吐量立刻会严重下降。对于数据速率为 54Mbps 的 802.11b/g 接入点而言，一旦启用保护机制，总吞吐量可能会从 20 Mbps 降低到 8 Mbps。第 9 章将详细介绍保护机制。还应该注意的是 802.11g 三种操作模式的问题，在无线局域网升级到 802.11n 后将不复存在。

如前所述，802.11g 修正案要求设备必须支持 ERP-DSSS/CCK 与 ERP-OFDM。因此，802.11g 接入点可以和 802.11g、802.11b 与 802.11 DSSS 客户端相互通信。由于 802.11g 设备的数据速率更高且向后兼容早期设备，802.11g 修正案被批准通过后，它在 SOHO 与企业市场引发了 Wi-Fi 设备的销售热潮。

本章前面曾经提到过，采用不同扩频技术的设备之间是无法相互通信的，而 802.11g 修正案要求设备必须支持 ERP-DSSS/CCK 与 ERP-OFDM。换句话说，这两种技术可以共存，但不能互通。有鉴于此，802.11g 修正案定义了保护机制，以确保两种技术不会相互干扰。保护机制的作用是防止 802.11 DSSS、802.11b HR-DSSS 与 802.11g ERP 无线射频卡同时传输数据。802.11、802.11b、802.11g 与 802.11a 的总结和比较如表 5-1 所示。

表 5-1　802.11 修正案比较

	传统 802.11	802.11b	802.11g	802.11a
工作频段	2.4GHz ISM	2.4GHz ISM	2.4GHz ISM	5GHz UNII (UNII-1、UNII-2 和 UNII-3)
扩频技术	FHSS 或 DSSS	HR-DSSS(强制) PBCC(可选)	ERP-OFDM(强制) ERP-DSSS/CCK(强制) ERP-PBCC(可选) DSSS-OFDM(可选)	OFDM
数据速率	1Mbps、2Mbps	DSSS：1Mbps、2 Mbps HR-DSSS：5.5Mbps、11 Mbps	ERP-DSSS/CCK：1Mbps、2Mbps、5.5Mbps、11Mbps ERP-OFDM：6Mbps、12Mbps、24Mbps(强制)，9Mbps、18Mbps、36Mbps、48Mbps、54Mbps(可选) ERP-PBCC：22Mbps、33 Mbps	6Mbps、12Mbps、24Mbps(强制)，9Mbps、18Mbps、36Mbps、48Mbps、54Mbps(可选)
向后兼容	不存在	仅 802.11 DSSS	802.11b HR-DSSS 802.11 DSSS	无
批准时间	1997	1999	2003	1999

5.2.4 802.11d

802.11 原始标准定义了美国、加拿大、日本和欧洲的无线局域网通信，而其他国家和地区对传输频段与发射功率的规定可能会有所不同。有鉴于此，IEEE 在 2001 年公布了 802.11d 修正案(IEEE Std. 802.11d-2001)。该修正案是对原始标准的补充和完善，以规范 802.11 设备在其他国家的使用。

国家代码信息包含在称为信标帧(beacon frame)与探询响应帧(probe response frame)的管理帧中，兼容 802.11d 的设备通过该信息确认没有违反所在国的频率与功率管理规定。图 5-1 显示了一个配置在蒙古使用的接入点，接入点发送的信标帧中包含国家代码、频率和功率等信息。

图 5-1 802.11d 设置

802.11d 修正案还定义了 FHSS 接入点特有的配置信息。各国对 FHSS 参数(如跳频模式)的定义可能会有所不同，这些信息同样包含在信标帧或探询响应帧中，不过这些信息仅对采用 FHSS 技术的传统 802.11 部署有参考价值。802.11d 修正案的完整内容请参阅 802.11-2007 标准第 9.8 条款。

第 9 章将详细介绍信标帧、探询帧以及其他无线帧。

5.2.5 802.11h

2003 年，IEEE 公布了 802.11h 修正案(IEEE Std. 802.11h-2003)，该修正案定义了 DFS(Dynamic Frequency Selection，动态频率选择)与 TPC(Transmit Power Control，传输功率控制)机制。制定 802.11h 修正案的初衷是为了规范欧洲的 5GHz 无线局域网，以免其干扰到同样使用 5GHz 频段的卫星与雷达系统。不过，该修正案定义的许多管理机制目前也被 FCC 所采纳。DFS 与 TPC 的作用是确保 5GHz 的 802.11 无线局域网不会对 5GHz 雷达与卫星通信造成干扰。

如表 5-2 所示，802.11h 修正案还定义了一个包含 11 个信道的新频段供无线局域网通信使用，这个新频段称为 UNII-2 扩展(UNII-2 Extended)频段。可以将 802.11h 修正案视为对 802.11a 修正案的补充和完善。所有 UNII 频段都采用 OFDM 传输技术。虽然 IEEE 定义了用于雷达检测与避免的 DFS 和 TPC 机制，不过各国的射频监管机构仍然制定了符合本国需要

的射频管理规定。美国和欧洲规定，使用 UNII-2 与 UNII-2 扩展频段传输数据的 802.11 设备必须采用雷达探测与避免技术。

表 5-2 UNII 频段

频段范围	修正案	信道
UNII-1 (lower) 5.150GHz～5.250GHz	802.11a	4
UNII-2 (middle) 5.250GHz～5.350GHz	802.11a	4
UNII-2 Extended 5.47GHz～5.725GHz	802.11h	11
UNII-3 (upper) 5.725GHz～5.825GHz	802.11a	4

OFDM 无线设备通过 DFS 实现对 5GHz 信道的频谱管理。ERC(欧洲无线通信委员会)与 FCC 规定，5GHz 无线射频卡必须采用抗干扰机制以免干扰到雷达系统。DFS 本质上就是雷达检测和雷达干扰避免技术。DFS 服务可以满足上述管理要求。

DFS 提供以下服务：

- 接入点根据所支持的信道选择连接到自己的客户端。如果客户端成为接入点所在无线网络的成员，则称客户端与接入点建立关联(associate)。
- 接入点可将某个信道设置为静默状态，以检测该信道是否存在雷达传输。
- 在使用某个信道之前，接入点将测试该信道是否存在雷达传输。
- 接入点可以检测当前信道与其他信道是否存在雷达传输。
- 如果检测到某个信道存在雷达传输，接入点将停止使用该信道以避免干扰。
- 在检测到干扰后，接入点可能会切换到另一个信道继续传输数据，并通知所有与其建立关联的客户端。

OFDM 无线设备通过 TPC 实现对 5GHz 频段的功率管理。ERC 要求工作在 5GHz 频段的无线射频卡必须使用 TPC，以符合最大传输功率规定，并减少对其他设备的干扰。TPC 服务可以满足上述关于传输功率的管理要求。

TPC 提供以下服务：

- 客户端根据其传输功率与接入点建立关联。
- 指定某个信道允许使用的最大传输功率，以符合监管机构的规定。
- 接入点可指定任意一个或所有与其建立关联的客户端所使用的传输功率。
- 接入点可根据实际的射频环境参数(如路径损失)相应调整客户端的传输功率。

客户端与接入点通过管理帧互换 DFS 与 TPC 信息。802.11h 修正案实际定义了两种主要的增强机制：采用 UNII-2 扩展频段以增加可用的传输频率，采用雷达检测和避免技术(DFS 与 TPC)以防止干扰发生。802.11h 修正案的内容请参阅 802.11-2007 标准第 11.8 和 11.9 条款。

5.2.6 802.11i

从 1997 年到 2004 年，公布的 802.11 原始标准仅定义了最基本的无线安全机制。任何无线安全解决方案都必须解决数据保密(加密)与认证(身份验证)这两个重要的问题。七年里，在 802.11i 修正案获批之前，64 位静态 WEP(Wired Equivalent Privacy，有线等效加密)是无线局域网唯一可以采用的加密机制。

但是，WEP 加密早已被破解，它不是一种可靠的数据加密手段。802.11 原始标准还定义了两种认证方式。开放系统认证(Open System authentication)是默认方式，任何设备都能通过开放系统认证。另一种认证方式称为共享密钥认证(Shared Key authentication)，它同样会造成很大的安全隐患。

2004 年，IEEE 批准并公布了 802.11i 修正案(IEEE Std. 802.11i-2004)，后者定义了安全性更高的加密与认证方式。802.11i 修正案定义的 RSN(Robust Security Network，强健安全网)旨在更好地保护在空中传输的数据，并为收发双方构建更为坚固的防御体系。由于 802.11i 修正案规范了无线网络的安全保护机制，它无疑是对 802.11 原始标准最为重要的完善之一。802.11i 修正案主要定义了以下几种安全增强机制：

数据隐私(Data Privacy) 为满足数据保密的要求，802.11i 修正案定义了一种安全性更高的加密方式，称为 CCMP(Counter Mode with Cipher-Block Chaining Message Authentication Code Protocol，计数器模式密码块链信息认证码协议)。CCMP 采用 AES(Advanced Encryption Standard，高级加密标准)算法，一般将其简称为 CCMP/AES、AES CCMP 或 CCMP。802.11i 修正案还定义了一种称为 TKIP(Temporal Key Integrity Protocol，临时密钥完整性协议)的可选加密方式。TKIP 采用 RC-4 流密码算法，本质上属于对 WEP 加密的补充和完善。

认证(Authentication) 802.11i 修正案定义了两种认证方式，二者分别采用 802.1X/EAP 架构与 PSK(Preshared Key，预共享密钥)认证。802.1X 解决方案需要与 EAP(Extensible Authentication Protocol，可扩展认证协议)配合使用，不过 802.11i 修正案并没有定义具体的 EAP 类型。

强健安全网(RSN) 定义了一整套用于建立认证、协商安全关联、为客户端与接入点产生动态加密密钥的机制。

Wi-Fi 联盟开发了一种称为 WPA2(Wi-Fi Protected Access 2，Wi-Fi 保护接入第 2 版)的认证项目，它与 IEEE 制定的 802.11i 修正案完全兼容。WPA(Wi-Fi Protected Access，Wi-Fi 保护接入)的版本 1 属于 802.11i 修正案获批之前的过渡性方案，而 WPA2 在功能上与 802.11i 修正案完全相同。802.11i 修正案的完整内容请参阅 802.11-2007 标准第 8 条款。

对任何无线局域网部署而言，Wi-Fi 安全都是头等大事，这也是 CWNP 项目推出 CWSP(认证无线安全资深工程师)认证的原因。由于至少有 10%的 CWNA 考试内容会涉及 Wi-Fi 安全，因此第 13 章与第 14 章将详细介绍 802.1X、EAP、CCMP、TKIP、WPA 以及其他安全机制。

5.2.7 802.11j

IEEE 任务组 j(TGj)主要研究 802.11 MAC 子层与 802.11a 物理层的改进问题，以满足日本 4.9 GHz 与 5GHz 频段的使用要求，并获得日本监管机构的认可。2004 年，IEEE 批准并公布了 802.11j 修正案(IEEE Std. 802.11j-2004)。

在日本市场销售的 802.11a 无线射频卡既可以使用 5.150GHz～5.250GHz 频段(UNII-1 频段)传输数据，也可以使用需要牌照/无需牌照的 4.9GHz～5.091GHz 频段传输数据。

802.11a 无线射频卡采用 OFDM 技术，信道间隔为 20 MHz，支持 6Mbps、9Mbps、12Mbps、

18Mbps、24Mbps、36Mbps、48Mbps 和 54 Mbps 等 8 个数据速率。日本的 802.11a 无线射频卡也可以采用信道间隔为 10 MHz 的 OFDM 技术，支持 3Mbps、4.5Mbps、6Mbps、9Mbps、12Mbps、18Mbps、24Mbps 和 27Mbps 等 8 个数据速率。此时，3Mbps、6Mbps 和 12Mbps 是必须支持的 3 个数据速率。

5.2.8 802.11e

802.11 原始标准并没有为 VoIP(语音 IP)等时敏应用定义任何相应的 QoS(quality of service，服务质量)机制。VoWIP(Voice over Wireless IP，无线 VoIP)也称为 VoWLAN(Voice over Wireless LAN)或 VoWiFi(Voice over Wi-Fi)，大部分厂商和 CWNP 项目都使用 VoWiFi 这个术语。语音、音频与视频等流量要求较低的延迟和抖动，其传输优先级高于标准的数据流量。802.11e 修正案为时间敏感的应用程序定义了满足 QoS 要求的二层 MAC 机制，以便时敏应用能优先在 802.11 无线局域网中传输。

802.11 原始标准为 802.11 无线射频卡定义了两种介质访问方式，以竞争半双工介质的使用权。DCF(Distributed Coordination Function，分布式协调功能)是默认方式，它采用完全随机的方式确定哪台设备使用无线介质收发数据。原始标准还定义了另一种称为 PCF(Point Coordination Function，点协调功能)的介质访问方式。在 PCF 中，暂时取得介质控制权的接入点通过轮询客户端以决定谁可以优先使用无线介质。请注意 PCF 介质访问方法没有被任何一家 WLAN 厂商采纳。

第 8 章将详细介绍 DCF 与 PCF 这两种介质访问方式。

802.11e 修正案还定义了增强的介质访问方式以满足 QoS 要求。802.11e QoS 无线网络采用 HCF(Hybrid Coordination Function，混合协调功能)，其包括两种 QoS 访问机制。EDCA(Enhanced Distributed Channel Access，增强分布式信道访问)是对 DCF 的完善和补充，它根据上层协议划分帧的优先级别。语音或视频流量将优先使用 802.11 无线介质传输，以减少时延。

HCCA(HCF Controlled Channel Access，HCF 受控信道访问)是对 PCF 的补充和完善。在 HCCA 中，接入点根据某些条件划分客户端的优先级。也就是说，某些客户端的级别较高，可以优先使用 802.11 无线介质传输数据。与 PCF 类似，WLAN 厂商从未采用 802.11e 定义的 HCCA 介质访问方法。

Wi-Fi 联盟也开发了一种称为 WMM(Wi-Fi Multimedia，Wi-Fi 多媒体)的认证项目，它在功能上与 IEEE 802.11e 修正案完全相同。WMM 将流量按重要程度划分为 4 个访问类别。802.11e QoS 修正案内容请参阅 802.11-2007 标准第 9.9 条款。

第 8 章将深入讨论 802.11e 修正案与 WMM 认证项目。

5.3 批准通过的 Post-2007 修正案

自从 802.11-2007 标准发布后，很多重要的修正案被批准并进一步增强了 802.11 功能。其中 802.11n-2009 修正案的作用更为显著。随着 802.11n 得到广泛部署，802.11a/b/g 技术开始被认为是传统技术。802.11n-2009 修正案非常重要，第 18 章将详细阐述 802.11n PHY 和 MAC 层的增强技术。其他被批准的修正案(如 802.11r 和 802.11k)也逐渐开始成为无线射频卡的增强功能。

5.3.1 802.11r-2008

802.11r-2008 修正案一般被称为 FT(fast basic service set transition，快速基本服务集转换)修正案。当部署安全性更高的 RSN 时，采用 802.11r 修正案定义的快速安全漫游(fast secure roaming，FSR)技术可以在无线局域网小区之间实现更快的漫游切换。制定 802.11r 修正案的主要目的是解决 VoIP 等时敏应用在漫游时的快速切换问题。客户端从一个接入点漫游到另一个接入点时，平均切换时间约为几百毫秒。

部署 WPA-Enterprise/WPA2-Enterprise 安全解决方案时，802.1X/EAP 认证必须使用 RADIUS 服务器，客户端通常需要 700 ms 以上的认证时间，这将严重影响漫游的性能。为防止通话质量下降甚至掉话，VoWiFi 要求切换时间不得超过 150 ms。由于 802.1X/EAP 安全解决方案需要较长的漫游切换时间，因此它目前很少在时间敏感的环境中使用。

根据 802.11r 修正案的定义，在实际漫游之前，客户端将通过有线或无线方式与新接入点建立 QoS 流和安全关联，绕过 802.1x 认证。客户端随后开始漫游，直到与新接入点建立连接。预先配置安全关联与 QoS 服务可以节省时间，从而大大加快设备在无线局域网蜂窝之间的切换速度。

IEEE 是在 2008 年 7 月批准并公布了 802.11r 修正案(IEEE Std. 802.11r-2008)，该修正案不属于 802.11-2007 标准。应从战略高度考虑在企业中部署 802.11r 技术，因为它对增强 VoWiFi 通信的安全将起到不可忽视的作用。CWSP 考试将重点考查 802.11r 技术的细节。

5.3.2 802.11k-2008

802.11 任务组 k(TGk)负责制定有关无线资源测量(Radio Resource Measurements，RRM)的标准。根据 802.11k-2008 修正案的定义，接入点或 WLAN 控制器(WLAN controller)在物理层与数据链路层的 MAC 子层采集并处理客户端的可测统计信息(第 10 章将介绍 WLAN 控制器。为简单起见，目前可以将 WLAN 控制器视为一台管理大量接入点的核心设备)。某些情况下，客户端也可能要求接入点或 WLAN 控制器提供相应的信息。802.11k 修正案定义了以下几个重要的 RRM 参数：

传输功率控制(TPC) 802.11h 修正案定义了 TPC，以防止 5GHz 无线局域网与雷达系统相互干扰。802.11k 修正案扩大了 TPC 的使用范围，允许 TPC 在其他频段或监管机构管辖的区域中使用。

客户统计信息 客户端向接入点或 WLAN 控制器报告各种物理层信息(如信噪比、信号强度、数据速率等)以及各种 MAC 子层信息(如帧传输、重传、传输错误等)。

信道统计信息 客户端根据信道中存在的射频能量采集本底噪声信息，并将这些信息反馈给接入点。此外，客户端也可以采集并向接入点发送有关信道负载的信息。接入点或 WLAN 控制器根据这些信息分配并管理信道。

邻居报告 数字电话与蜂窝系统采用移动辅助切换(Mobile Assisted Handover，MAHO)技术以实现更好的小区切换，802.11k 修正案为接入点或 WLAN 控制器定义了类似的机制。

客户端采用专有方式维护一份已知接入点的列表，并决定何时漫游到另一个接入点。大多数客户端的漫游决定是基于接入点的信号强度。换句话说，客户端漫游是基于射频环境的个人视角。802.11k 机制能够给客户端提供额外的当前射频环境信息。

根据 802.11k 修正案的定义，接入点或 WLAN 控制器要求客户端在其他信道监听、采集和反馈附近接入点的信息，并根据这些信息生成一份邻居报告，报告中按信号质量好坏详细列出了所有可用的接入点。在漫游开始之前，客户端将要求当前的接入点或 WLAN 控制器发送邻居报告，并决定是否向邻居报告中列出的接入点漫游。客户端利用邻居报告中的射频环境信息，做出更明智的漫游决定。802.11k-2008 修正案与 802.11r-2008 可能会极大提高 802.11 漫游性能。

尽管一些 WLAN 厂商已经在接入点和控制器方面支持 802.11k 和 802.11r 技术，但大多数客户端还不支持。802.11r(安全漫游)的某些方面和 802.11k(资源管理)修正案会很快在 Wi-Fi 联盟测试，即 Voice Enterprise。一旦 Voice Enterprise 认证得到应用，802.11k 和 802.11r 机制也会在客户端上得到支持。

5.3.3 802.11y-2008

802.11 设备通常运行在无需牌照的频率中，但经过所在国家监管机构的许可也可以在需要牌照的频率运行。

美国批准允许使用 3650MHz～3700MHz 的频段，IEEE 任务组 y(TGy)致力于解决高功率 802.11 设备与其他非 802.11 设备在该频段的共存问题。要注意的是，802.11y-2008 修正案也可以用于其他国家和其他授权频率。

被准许的 3650MHz～3700MHz 频段需要利用“基于内容的协议(CBP)”来避免设备之间的干扰。WiFi 使用的媒介竞争方式(CSMA/CA)，通常能满足这种需求。但标准的 CSMA/CA 方式还不够，802.11y-2008 修正案定义了动态 STA 启动程序(DSE)作为补充。802.11 无线接口通过广播一个独特的标识符来明确其位置，从而帮助解决与非 802.11 无线接口的同频干扰。

5.3.4 802.11w-2009

针对 802.11 无线局域网的一种常见攻击是 DoS(denial-of-service，拒绝服务)攻击。DoS 攻击的种类很多，不过最普遍的 DoS 攻击发生在 2 层，通过篡改 802.11 管理帧来实现。修改解除认证帧或解除关联帧对攻击者而言并非难事，如果将伪造的管理帧重新发送到网络中，就能达到瘫痪无线网络的目的。

IEEE 任务组 w(TGw)致力于研究如何安全地传输管理帧，从而预防管理帧可以被欺骗。802.11w-2009 修正案提供保护单播、广播、组播管理帧。

802.11w 帧被称为强健管理帧(robust management frames)。管理帧保护服务可以对强健管理帧进行保护，强健管理帧包括解除关联帧、解除认证帧，强健行为帧。行为帧要求客户端在代表其他客户端时发出，并不是所有的行为帧都是强健的。

单播管理帧利用 CCMP 来实现安全。广播和组播帧保护使用广播/多播完整协议(Broadcast/Multicast Integrity Protocol(BIP))。BIP 使用加密消息认证码模式(CMAC)128 位 AES 加密算法提供数据完整性校验和重放攻击保护。需要注意的是，802.11w 修正案不会终结所有第 2 层 DoS 攻击。然而 802.11w 机制对于一些常见的第 2 层 DoS 攻击是有效的。

第 14 章将介绍一层与二层 DoS 攻击。

5.3.5 802.11n-2009

802.11n-2009 修正案的获批无疑将对 Wi-Fi 市场产生巨大影响。从 2004 年起，802.11 任务组 n(TGn)就致力于对 802.11 标准进行完善和改进，以获得更高的吞吐量。尽管此前已有不少 IEEE 802.11 修正案解决了带宽和数据速率在 2.4GHz 的问题，不过 802.11n 修正案将尝试同时提高 2.4GHz 和 5GHz 两个频段的吞吐量。802.11n 修正案定义了一种称为 HT(高吞吐量)的新技术，HT 采用物理层(PHY)与 MAC 子层增强支持高达 600Mbps，而网络吞吐量可以达到 100 Mbps 以上。

HT(条款 20)无线接口采用 MIMO(多进多出)与 ODFM 技术。传统的天线系统都在如何补偿或消除多径效应上动脑筋，而 MIMO 系统正好相反，它使用多根接收与发射天线，以便利用多径效应改善通信质量。采用 MIMO 技术可以提高吞吐量并扩大覆盖范围。802.11n 也向后兼容传统的 802.11a/b/g 无线接口。

第 18 章将深入讨论 802.11n 与 MIMO 技术。

5.3.6 802.11z-2010

IEEE 任务组 z(TGz)致力于建立并规范 DLS(Direct Link Setup，直接链路设置)机制，以便客户端之间绕过接入点直接通信。在大部分无线局域网环境中，与同一个接入点建立关联的客户端之间所有的帧交换都必须通过该接入点进行。而 DLS 机制允许客户端绕过接入点，直接与其他客户端交换数据。早期的一些修正案也定义了 DLS 机制。802.11z-2010 修正案提出了经过改进的 DLS 机制。不过注意的是，DLS 通信尚未被企业级 WLAN 厂商采纳。

5.3.7 802.11u-2011

802.11 任务组 u(TGu)致力于研究 IEEE 802.11 接入网与其他外部网络的互联和集成。为实现这个目标，802.11u 修正案定义了一套通用和标准化的机制。802.11u 修正案经常被称为与外部网络的无线互联(Wireless InterWorking with External Networks，WIEN)，着眼于无线局域网与其他外部网络(3G、4G、蜂窝电话网等)连接时的无缝切换和会话保持问题。

802.11u-2011 修正案于 2011 年 2 月通过批准，它定义了一些功能和程序，来帮助客户端进行网络发现和选择、传递来自使用 QoS 映射的外部网络信息和提供紧急服务通用机制。

5.3.8　802.11v-2011

802.11v-2011 修正案在 2011 年 2 月获批。802.11k 定义了如何从客户端获取信息，而 802.11v-2011 定义了如何从中央管理点以无线方式配置客户端。802.11v-2011 定义了无线网络管理(Wireless Network Management (WNM))机制，这个机制可以让 802.11 终端交互信息，以提高无线网络整体性能。接入点和客户端使用 WNM 协议交换信息，这样每个终端就更了解网络拓扑和状态。

除了提供网络状态信息，WNM 协议还定义了交换位置信息的机制、提供多 BSSID 支持，并且为那些因为长时间处于休眠状态而无法接收到来自接入点的帧的客户端，提供一个新的睡眠模式(WNM-Sleep mode)

5.3.9　802.11s-2011

802.11s-2011 修正案在 2011 年 7 月获批。802.11 接入点一般作为连接到分布系统(distribution system，DS)的入口设备使用。尽管大多数分布系统都是 802.3 以太网，不过 802.11-2007 标准并未规定分布系统必须使用有线介质。因此，接入点也可以作为入口设备连接到无线分布系统(wireless distribution system，WDS)。802.11s 修正案定义了一种自适应、自配置的系统，该系统在一个多跳的 Mesh 无线分布系统中支持广播、组播与单播流量。

802.11 任务组(TG)致力于对采用 IEEE 802.11 MAC 层与物理层的 Mesh 网络进行标准化。802.11s 修正案定义了 mesh point(MP)，它是支持 Mesh 服务的 802.11 QoS 设备。MP 采用 HWMP(Hybrid Wireless Mesh Protocol，混合无线网状协议)，它是一种强制的网状路由协议，使用默认的路径选择方式路由流量。厂商也可能采用专有的网状路由协议和指标。如图 5-2 所示，Mesh access point(MAP)是一种能同时提供 Mesh 功能与 AP 功能的设备，而 Mesh point portal(MPP)通常作为连接到一个或多个外部网络(如 802.3 有线骨干网)的网关使用。

图 5-2　Mesh point、mesh AP 和 mesh portal

第 7 章将深入讨论分布系统与无线分布系统，第 10 章将深入讨论 802.11Mesh 网络。

5.4 IEEE 802.11 修正案草案

今后的 802.11 无线网络将是什么样子呢？这可以从 802.11 修正案草案中一窥全豹。修正案草案是对现有标准的完善和增强，草案提出的新功能可能会在不久之后应用到 802.11 无线网络设备中。更高的吞吐量、更高或更低的频率上的应用已经初露端倪。

需要注意的是，修正案草案属于未经批准的提案。尽管一些厂商销售的产品中集成了某些修正案草案定义的功能(稍后将对此进行介绍)，不过在草案获批之前，这些功能仍然是厂商专有的。虽然厂商可能会向用户推销基于草案的产品，但是这些产品能否与基于获批修正案的产品相互兼容仍然有待观察。

CWNA 考试(PW0-105)内容涵盖了 802.11-2007 标准及之后所有被批准的修正案。CWNA 考试不会考查修正案草案。尽管考试不涉及，但我们相信这些正在被规划和发展的修正案草案仍可能会改变将来的 802.11 无线网络。

802.11n-2009 修正案引发了数据、语音和视频在无线介质上的大融合。今后的 Wi-Fi 产品将更为先进与复杂，本章其余部分将对此进行简要介绍。

需要再次强调的是，下面介绍的这些修正案草案目前还没有被 IEEE 批准，最终获批的修正案可能会有所不同。

5.4.1 802.11p

802.11 任务组 p(TGp)致力于完善与改进 802.11 标准，以支持智能交通系统(Intelligent Transportation Systems，ITS)应用。802.11p 修正案获批之后，高速行驶的车辆之间可以使用需要牌照的 5.9GHz ITS 频段交换数据，而车辆与路边基础设施将在 5GHz 频段(北美：5.850GHz～5.925GHz)上实现相互通信。

802.11p 修正案支持 1000m(3281ft)之内、速度高达 200kph(124 mph)的通信。由于某些应用对数据交付时间的要求很高(4ms～50ms)，极短的时延对于保证通信成功十分重要。

802.11p 修正案也称为车载环境下的无线接入(Wireless Access in Vehicular Environments，WAVE)，它可能为美国交通部专用短距通信(DSRC)项目奠定基础。该项目规划了一个覆盖全美的车辆/路边通信网，网络中包括车辆安全服务、堵车警报、收费系统、车辆主动避撞、自适应交通灯控制等应用。802.11p 修正案也可以用于海事通信与铁路通信。

5.4.2 802.11aa

802.11aa 修正案草案旨在对 802.11 MAC 子层进行补充和完善，以便在支持强健音频视

频流(robust audio video streaming)的同时保持与其他流量的共存。

5.4.3 802.11ac

802.11ac 和 802.11ad 修正草案经常被称为“千兆 Wi-Fi”修正案，因为其比 802.11n-2009 定义的数据率更高。802.11n 定义的数据率高达 600Mbps，除去媒介竞争开销，总吞吐量可能超过 200Mbps。802.11ac 和 802.11ad(VHT)任务组的目标是在 802.11 环境中实现 1Gbps 以上的吞吐量。

802.11ac 修正草案将定义 VHT 工作在 6GHz 频率以下。这种技术将最有可能被用于现有的 2.4GHz 和 5GHz 频段。因为需要与 802.11a/b/g/n 无线网卡共存，所以向后兼容技术非常重要。

如何让吞吐能力达到 1Gbps 仍然有待观察。802.11n-2009 修正案利用信道绑定技术将两个 20 MHz OFDM 信道绑定为一个 40MHz 的信道。信道绑定能够提高潜在的吞吐量。802.11ac 可能使用 80 MHz 和 160 MHz 宽的信道。只有在 5GHz UNII 频段才有足够的频率空间，根据不同的地区规定，三到五个不重叠的 80 MHz 信道是可能的。802.11n 定义的是使用单用户的 MIMO 技术(SU- MIMO)，VHT 可能会使用多用户 MIMO 技术(MU-MIMO))技术。当客户端在不同的物理区域时，MU-MIMO 接入点能与在同一频道的多个客户端同时通信。

802.11ac 也将可能使用具备更好的调制编码能力和更强的纠错能力的无线芯片组。

5.4.4 802.11ad

802.11ad 修正草案定义的 VHT 使用更高的 60GHz 频段，潜在吞吐量高达 7Gbps。不足之处是 60GHz 比 5GHz 的有效信号辐射范围更小。因为覆盖范围的局限性，60GHz Wi-Fi 可能更适合家庭市场而非企业。但是，60GHz Wi-Fi 在高密度接入的企业环境里也可能有巨大潜力，因为此时接入容量比覆盖范围更重要。

VHT 机制可能还需要采用新的加密机制。一些在 802.11ac 和 802.11ad 任务组工程师预计，当前的 CCMP 加密方法可能无法正确处理更高预期的数据率。CCMP 使用双链 AES 加密模式来处理 128 位的数据块。128 位的数据块也必须按照第一个 AES 加密模式到第二个加密模式这样的顺序处理。

802.11ad 修正草案建议使用 GCMP(Galois/Counter Mode Protocol)，它也是使用 AES 加密的。然而，GCMP 只需 CCMP 一半的加密操作，数据可以并行处理。

什么是无线千兆联盟(Wi-Gig)?

促进消费电子产品、手持设备和电脑使用无需牌照的 60GHz 信道的科技公司联盟。可以登录 http://wirelessgigabitalliance.org 了解更多关于 Wi-Gig 联盟的信息。

5.4.5 802.11ae

802.11ae 修正草案针对增强的 QoS 管理。

5.4.6 802.11af

802.11af 任务组正在研究在 50MHz 和 600MHz 之间的新开放的 TV 空白频率使用 Wi-Fi。尽管这些低频技术比 802.11a/b/g/n 技术的数据率更低，但潜在的长途户外传输意义更大。

5.4.7 802.11ah

802.11ah 修正草案定义的 Wi-Fi 使用频率低于 1 GHz。明显优势就是 Wi-Fi 传输范围更大。

5.5 已经失效的修正案

接下来的两个修正案已经不被批准了。但这两项修正案的主题事件(关于漫游和性能测试)是很重要的，所以我们将在这本书里讨论。

5.5.1 802.11F

2003 年，IEEE 任务组 F(TGF)公布了仅作为推荐规程存在的 802.11F 修正案(IEEE Std. 802.11F-2003)。该修正案并没有被批准通过，IEEE 于 2006 年 2 月将其撤销。

如果某个 IEEE 任务组被分配一个大写字母(如 TGF)，说明该任务组制定的修正案仅作为推荐规程存在，而不属于 802.11-2007 标准(如 802.11F)。

802.11 原始标准规定，厂商生产的接入点必须能支持漫游。可将漫游简单定义如下：与当前接入点建立关联的客户端向新接入点移动时，不会因为缺少信号覆盖而导致通信中断。最恰当的一个类比是手机的漫游。当用户一边开车一边使用手机与挚友交谈时，用户的手机将在蜂窝通信塔之间漫游，以保证通话的连续性。无缝漫游能实现真正的移动性，而后者是无线网络的核心所在。

如图 5-3 所示，客户端通过第一个接入点(AP-1)从位于有线骨干网的 FTP 服务器下载文件。需要注意的是，两个接入点的覆盖范围存在交集。随着客户端的移动，它距离第二个接入点(AP-2)越来越近，接收到的 AP-2 的信号越来越强。客户端可能会漫游到 AP-2，并通过新接入点继续进行 FTP 传输。

图 5-3 无缝漫游

尽管漫游切换的时间只有几百毫秒，不过向客户端交付的数据包仍然可能被暂时储存在原接入点中，即使客户端已经漫游到新接入点。为将缓存数据包传输给客户端，以下两步至关重要：

(1) 新接入点必须将客户端漫游的信息通知原接入点，并要求原接入点将所有缓存的数据包传输给自己。

(2) 原接入点必须通过分布系统将缓存的数据包转发给新接入点，并由后者传输给已经漫游的客户端。

图 5-4 显示了以上两个步骤。

图 5-4 漫游：分布系统介质

客户端在不同厂商的接入点之间能否实现漫游？

答案是否定的。802.11F 是为了解决不同供应商 AP 之间的漫游问题。不过 802.11F 修正案仅成为推荐规程而非标准的一个原因在于，每家厂商都希望消费者只购买自己生产的接入点，而不是其竞争对手的产品。有鉴于此，本书提出了以下“推荐规程”：不要在同一有线网段中混用不同厂商生产的自治接入点。第 7 章、第 9 章与第 12 章将详细介绍漫游。

尽管 802.11 原始标准定义了漫游，不过它并没有规定漫游的具体实现方式。IEEE 最初计划将决定权交给厂商，由厂商决定采用何种专有的方式实现接入点之间的漫游。而 802.11F 修正案试图对分布系统介质(一般为采用 TCP/IP 网络协议的 802.3 以太网)中使用的各种漫游机制进行标准化。802.11F 修正案尝试解决接入点间漫游的“厂商互操作性”问题，其最终结果是形成了一项采用 IAPP 的推荐规程。IAPP 采用通告与切换机制，自治接入点之间可以共享漫游客户端的信息。IAPP 还定义了缓存数据包的交付方式。因为 802.11F 修正案从未被批准，所以 IAPP 协议基本上也没有实际应用。

5.5.2 802.11T

IEEE 802.11 任务组 T(TGT)致力于研究与开发测量 802.11 设备性能所需的绩效指标、测

量方法以及测试条件。

IEEE 802.11T 中的大写字母 T 表示该修正案属于推荐规程而非标准。802.11T 修正案从未得到修正，已经被丢弃。

802.11T 修正案草案也被称为无线性能预测(Wireless Performance Prediction，WPP)，其最终目标是形成一份一致的、能被各方普遍接受的无线局域网测量规程。独立的测试实验室、厂商甚至终端用户都可以使用这些 802.11 性能指标与机制。

真实场景

不同厂商设备的吞吐量是否相同？

无线网络的吞吐量受多种因素制约，这些因素包括物理环境、覆盖范围以及加密类型。影响吞吐量的另一个因素是使用哪家厂商生产的无线设备传输数据。虽然 802.11-2007 标准明确定义了频率带宽、数据速率与介质访问方式，但是不同厂商设备的吞吐量仍然相差很大。进行吞吐量性能测试时，采用一家厂商生产的两块无线射频卡会观察到一种结果，而采用另一家厂商生产的两块无线射频卡经常会观察到另一种结果，两种测试结果可能相差甚远。一般来说，采用一家厂商的设备比混用不同厂商的设备可以获得更高的吞吐量。不过在某些情况下，混用不同厂商的设备也可能会获得难以置信的高吞吐量。尽管标准化的 802.11T 测试标准未被批准，Wi-Fi 联盟定义了自己的厂商中立的测试标准，用于所有的 Wi-Fi 认证项目。

5.6 802.11m 任务组

1999 年，IEEE 任务组 m(TGm)开始制定内部维护 802.11 标准技术文档所需的修正案。802.11m 修正案负责对 802.11 标准进行澄清和更正，一般也将其称为“802.11 内务处理”(802.11 housekeeping)。只有任务组 m 的工程师才需要了解 802.11m 修正案，后者对普通用户的意义不大。该任务组还负责将已经批准的修正案制成发布文档。在撰写指南出版时，最新发布的 WLAN 标准为 IEEE Std 802.11-2007 版本。在本书被翻译时已经发布了 IEEE 802.11-2012 版本(译者注)。

请注意，不存在“802.11l”与“802.11o”修正案，因为容易与 1 和 0 混淆。也没有 802.11ab 修正案被省略，避免与同时使用 802.11a 和 802.11b PHY 技术的设备混淆，这些设备通常被称为 802.11a/b 设备。同理也没有 802.11ag 修正案。同时我们注意到也没有 802.11x。由于术语 802.11x 有时可以指代所有 802.11 标准。IEEE 802.1X 标准是一种基于端口的访问控制标准，人们也经常将它误写为 802.11x。

5.7 小结

本章介绍了 802.11 原始标准及其修正案，这些修正案目前已经被整合到 802.11-2007 标准，自 2007 年也整合到 802.11 修正案中。此外，本章还讨论了今后可能获批的修正案草案我们介绍了以下内容：

- 802.11 原始标准定义的各种物理层与 MAC 层规范。
- 所有已经获批的 802.11 修正案，它们定义了更高的数据速率、不同的扩频技术、服务质量以及安全机制。
- 802.11 修正案草案提出的针对现有标准的完善和改进，包括更高的吞吐量、Mesh 网络不同频率的操作等。

目前，市场上存在大量厂商专有的 Wi-Fi 解决方案，它们在可以预见的一段时间内仍将继续存在，但是标准化对于增强产品的互操作性至关重要。802.11-2007 标准以及今后所有可能获批的修正案草案将为厂商、网络管理员和终端用户提供一个必要的参照。

CWNA 考试将考查 802.11-2007 标准以及所有相关的技术，此外，CWNA 考试还会涉及 802.11n 修正案定义的技术。虽然考生应将主要精力放在 802.11-2007 标准上，不过请注意，一旦某项 802.11 修正案草案被 IEEE 批准通过，它可能会在今后的 CWNA 考试中占有一席之地。

5.8 考试要点

了解 802.11 原始标准与 802.11-2007 标准定义的扩频技术。802.11 原始标准定义了红外技术、FHSS 与 DSSS，各种修正案(目前已经被整合到 802.11-2007 标准中)还定义了 HR-DSSS、OFDM 与 ERP。

记住每种物理层规范必须支持与可以支持的数据速率。DSSS 与 FHSS 支持的数据速率为 1 Mbps 和 2 Mbps。其他物理层规范支持更多的数据速率。例如，OFDM 与 ERP-OFDM 支持 6Mbps、9Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps 和 54Mbps 等 8 个数据速率，不过只有 6Mbps、12Mbps 和 24Mbps 是必须支持的数据速率。请注意，数据速率是速度而非总吞吐量。

了解 802.11-2007 标准定义的每种物理层规范的工作频段。802.11a 设备使用 5GHz UNII 频段传输数据，DSSS、FHSS、HR-DSSS 与 ERP(802.11g)设备使用 2.4GHz ISM 频段传输数据。请注意，802.11n 设备要么在 2.4GHz 频道要么在 5GHz 频道中传播。

解释 802.11g ERP(802.11g)接入点的 3 种厂商工作模式。802.11g 接入点可以被配置为 B-only 模式、G-only 模式或 B/G 混合模式。3 种模式使用的扩频技术不同，总吞吐量也不同。

了解 ERP(802.11g)无线局域网采用的强制与可选的物理层规范。802.11g 修正案定义了两种强制的物理层规范，它们是 ERP-OFDM 和 ERP-DSSS/CCK。802.11g 修正案还定义了两种可选的物理层规范，它们是 ERP-PBCC 和 DSSS-OFDM。

定义 TPC(传输功率控制)与 DFS(动态频率选择)。欧洲和美国的监管机构要求 5GHz 无线局域网设备必须使用 TPC 与 DFS，以免干扰到雷达传输。

解释 802.11 原始标准与 802.11i 修正案定义的无线安全标准。在 802.11i 修正案获批之前，802.11 原始标准仅定义了 WEP 作为加密方式，开放系统认证与共享密钥认证作为认证方式。而 802.11i 修正案定义的加密方式为 CCMP/AES，认证方式为 802.1X/EAP 和 PSK。

5.9 复习题

复习题的答案见附录 A。

1. An ERP (802.11g) network mandates support for which two spread spectrum technologies?
   A. ERP-OFDM
   B. FHSS
   C. ERP-PBCC
   D. ERP-DSSS/CCK
   E. CSMA/CA
2. The 802.11-2007 standard using an ERP-DSSS/CCK radio supports which data rates?
   A. 3, 6, and 12Mbps
   B. 6, 9, 12, 18, 24, 36, 48, and 54Mbps
   C. 6, 12, 24, and 54Mbps
   D. 6, 12, and 24Mbps
   E. 1, 2, 5.5, and 11Mbps
3. Which types of devices were defined in a legacy 802.11 WLAN network? (Choose all that apply.)
   A. Clause 17 OFDM
   B. Clause 15 DSSS
   C. Clause 18 HR-DSSS
   D. Clause 16 IR
   E. Clause 14 FHSS
   F. Clause 19 ERP
4. Which 802.11 amendment defines wireless mesh networking mechanisms?
   A. 802.11n
   B. 802.11u
   C. 802.11s
   D. 802.11v
   E. 802.11kJ

5. A robust security network (RSN) requires the use of which security mechanisms? (Choose all that apply.)

A. 802.11x

B. WEP

C. IPsec

D. CCMP/AES

E. CKIP

F. 802.1X

6. An 802.11a radio card can transmit on_____frequency and uses_____spread spectrum technology.

A. 5MHz, OFDM

B. 2.4GHz, HR-DSSS

C. 2.4GHz, ERP-OFDM

D. 5GHz, OFDM

E. 5GHz, DSSS

7. What are the required data rates of an OFDM station?

A. 3, 6, and 12Mbps

B. 6, 9, 12, 18, 24, 36, 48, and 54Mbps

C. 6, 12, 24, and 54Mbps

D. 6, 12, and 24Mbps

E. 1, 2, 5.5, and 11Mbps

8. When implementing an 802.1X/EAP RSN network with a VoWiFi solution, what is needed to avoid latency issues during roaming?

A. Inter-Access Point Protocol

B. Fast BSS Transition

C. Distributed Coordination Function

D. Roaming Coordination Function

E. Lightweight APs

9. The original 802.11 standard requires which data rates?

A. 1, 2, 5.5, and 11Mbps

B. 6, 12, and 24Mbps

C. 1 and 2Mbps

D. 6, 9, 12, 18, 24, 36, 48, and 54Mbps

E. 3, 6, and 12Mbps

10. What is the primary reason that OFDM (802.11a) radios cannot communicate with ERP (802.11g) radios?

A. 802.11a uses OFDM, and 802.11g uses DSSS.

B. 802.11a uses DSSS, and 802.11g uses OFDM.

C. 802.11a uses OFDM, and 802.11g uses CCK.

D. 802.11a operates at 5GHz, and 802.11g operates at 2.4GHz.

E. 802.11a requires Dynamic Frequency Selection, and 802.11g does not.

11. What two technologies are used to prevent 802.11 radios from interfering with radar transmissions at 5GHz?

A. Dynamic frequency selection

B. Enhanced Distributed Channel Access

C. Direct sequence spread spectrum

D. Temporal Key Integrity Protocol

E. Transmit power control

12. Which 802.11 draft amendments may provide for throughput of 1 Mbps or higher? (Choose all that apply.)

A. 802.11aa

B. 802.11ab

C. 802.11ac

D. 802.11ad

E. 802.11ae

F. 802.11af

13. As defined by the 802.11-2007 standard, which equipment is compatible? (Choose all that apply.)

A. ERP and HR-DSSS

B. HR-DSSS and FHSS

C. OFDM and ERP

D. 802.11a and 802.11h

E. DSSS and HR-DSSS

14. Maximum data rates of_____are permitted using OFDM radios.

A. 108Mbps

B. 22Mbps

C. 24Mbps

D. 54Mbps

E. 11Mbps

15. What are the security options available as defined in the original IEEE Std. 802.11-1999 (R2003)? (Choose all that apply.)

A. CCMP/AES

B. Open System authentication

C. Preshared keys

D. Shared Key authentication

E. WEP

F. TKIP

16. The 802.11u-2011amendment is also known as_____.

A. Wireless Interworking with External Networks (WIEN)

B. Wireless Local Area Networking (WLAN)

C. Wireless Performance Prediction (WPP)

D. Wireless Access in Vehicular Environments (WAVE)

E. Wireless Access Protocol (WAP)

17. The 802.11-2007 standard defines which two technologies for quality of service (QoS) in a WLAN?

A. EDCA

B. PCF

C. Hybrid Coordination Function Controlled Channel Access

D. VoIP

E. Distributed Coordination Function

F. VoWiFi

18. The 802.11h amendment (now part of the 802.11-2007 standard) introduced what two major changes for 5 GHz radios?

A. UNII-2 Extended

B. IAPP

C. Radar detection

D. Transmit Frequency Avoidance

E. Frequency hopping spread spectrum

19. The 802.11b amendment defined the_____PHY.

A. HR-DSSS

B. FHSS

C. OFDM

D. PBCC

E. EIRP

20. Which layers of the OSI model are referenced in the 802.11 standard? (Choose all that apply.)

A. Application

B. Data-Link

C. Presentation

D. Physical

E. Transport

F. Network

第 6 章 无线网络与扩频技术

在该章中，你将学习以下内容：

- √ ISM(工业、科学与医用)频段
  - 900MHz ISM 频段
  - 2.4GHz ISM 频段
  - 5.8GHz ISM 频段
- √ UNII(无需牌照的国家信息基础设施)频段
  - UNII-1(低)频段
  - UNII-2(中)频段
  - UNII-2 扩展频段
  - UNII-3(高)频段
- √ 3.6GHz 频段
- √ 4.9GHz 公共安全频段
- √ 未来的 Wi-Fi 频段
  - 60GHz
  - White-Fi
- √ 窄带传输与扩展传输
  - 多径干扰
- √ 跳频扩频(FHSS)
  - 跳频序列
  - 驻留时间
  - 跳变时间
  - 调制
- √ 直序扩频(DSSS)
  - DSSS 数据编码

- 调制

√ 分组二进制卷积码(PBCC)

√ 正交频分复用(OFDM)

- 卷积编码
- 调制

√ 2.4GHz 信道

√ 5GHz 信道

√ 相邻信道、非相邻信道与重叠信道

√ 吞吐量与带宽

√ 通信抗逆力

本章将讨论 802.11 标准及其修正案定义的各种扩频传输技术与相应的频段。我们将介绍这些频段如何被划分为不同的信道，并讨论使用信道时需要注意的一些问题。此外，本章还将介绍各类扩频技术、OFDM(正交频分复用)技术以及 OFDM 技术与扩频技术的异同。

本章引用了很多 FCC 规范和法规。CWNA 考试不会测试这些与监管地区有关的特定内容。FCC 的法规参考可以帮助更好地理解技术内容。重要的是要意识到不同管理域之间往往存在相似之处。因此，了解另一个国家的无线电监管规定也可以帮助理解你所在地区的监管规定。

6.1　ISM 频段

802.11 原始标准以及随后的 802.11b 和 802.11g 修正案定义了 2.4GHz～2.4835GHz 频段上的无线局域网通信，该频段属于 ISM(Industrial, Scientific, and Medical，工业、科学与医用)频段。ISM 频段包括以下 3 个频段：

- 902MHz～928MHz(宽度为 26MHz)
- 2.4000GHz～2.4835GHz(宽度为 83.5MHz)
- 5.725GHz～5.875GHz(宽度为 150MHz)

ITU-T(International Telecommunication Union Telecommunication Standardization Sector，国际电信联盟电信标准化部门)在其出版的《无线电规则》(Radio Regulations)第 5.138 与 5.150 节中对 ISM 频段做了定义。根据 ITU-T 的规定，FCC(美国联邦通信委员会)负责美国境内的 ISM 频段管理，其他国家对 ISM 频段的管理可能会有所不同。900MHz 频段称为工业频段(Industrial band)，2.4GHz 频段称为科学频段(Scientific band)，5.8GHz 频段称为医用频段(Medical band)。

需要注意的是，以上 3 个频段都属于无需牌照的频段，各频段可以使用的设备不限。例如，医用设备中的射频卡也可以在 900MHz 工业频段工作。

6.1.1　900MHz ISM 频段

900MHz ISM 频段的范围是 902MHz～928MHz，宽度为 26MHz。早期的无线网络使用该频段传输数据，不过大多数无线网络目前已转而采用更高的频段，以期获得更高的吞吐量。

制约 900MHz ISM 频段使用的另一个因素是，世界上很多国家已经将该频段的一部分划分给 GSM(Global System for Mobile Communications，全球移动通信系统)使用，作为蜂窝电话的工作频段。尽管目前已很少有无线网络部署在 900MHz ISM 频段，不过仍然有相当数量的无线设备(如婴儿监护器、无线家用电话和无线耳机)使用该频段进行通信。

虽然 802.11 射频卡不使用 900MHz ISM 频段传输数据，但是仍然有许多传统的无线网络部署在该频段。一些厂商至今还在生产使用 900MHz ISM 频段的非 802.11 无线网络设备。900MHz 频段具有比 2.4GHz 和 5GHz 频段更好的树叶穿透性(foliage penetration)，因此它受到了无线运营商的特别青睐。

6.1.2 2.4GHz ISM 频段

2.4GHz ISM 频段是无线网络最常用的工作频段。该频段的范围是 2.4 000GHz～2.4 835GHz，宽度为 83.5MHz。IEEE 802.11-2007 标准定义了 2.4GHz ISM 频段上的无线局域网通信。目前，大量 802.11 射频卡都工作在 2.4GHz ISM 频段，经常导致该频段极度拥塞。该频段包括采用以下技术的设备：

- 802.11(FHSS 或 DSSS 射频卡)
- 802.11b(HR-DSSS 射频卡)
- 802.11g(ERP 射频卡)
- 802.11n(HT 射频卡)

除无线网络设备之外，微波炉、无绳家用电话、婴儿监护器和无线摄像机也使用 2.4GHz ISM 频段进行通信。该频段已经拥挤不堪，其他设备很容易对 802.11b/g/n 射频卡造成干扰。

请记住，并非所有国家和地区的射频监管机构都允许使用整个 2.4GHz～2.4835GHz ISM 频段进行通信。IEEE 802.11-2007 标准规定，无线局域网可以使用该频段的 14 个信道传输数据，不过其他国家对信道的分配可能会有所不同。本章后面将介绍所有 2.4 GHz 信道。

6.1.3 5.8GHz ISM 频段

5.8GHz ISM 频段的范围是 5.725GHz～5.875 GHz，宽度为 150MHz。与其他两个 ISM 频段类似，婴儿监护器、无绳电话、相机等大量消费类设备也使用 5.8GHz ISM 频段传输数据。经验不足的工程师很容易混淆 5.8GHz ISM 频段与 UNII-3 频段，后者属于 5GHz UNII 频段，范围是 5.725GHz～5.825GHz。这两种无需牌照的频段拥有几乎相同的频率范围，不过 5.8GHz ISM 频段比 UNII-3 频段宽 50 MHz。

IEEE 802.11a 修正案(目前属于 802.11-2007 标准)指出，“监管机构在其业务区域内负责管理 OFDM 通信，OFDM 物理层的工作频段为 5GHz”。大多数国家允许 OFDM 通信使用 3 个 UNII 频段的信道(后面将对此进行介绍)，美国还允许 OFDM 通信使用 ISM 频段的信道 165。信道 165 的中心频率为 5.825GHz(UNII-3 频段的最高频率)，它正好位于 FCC 定义的 5.8GHz ISM 频段(5.725GHz～5.875GHz)的中央。需要注意的是，信道 165 很少用于无线局域网部署。

FCC 并未对 5.8GHz ISM 频段的输出功率做出严格限制，这使得该频段成为远距离无线桥接的首选工作频段。UNII-3 频段也可以用于室外桥接，不过严格的输出功率规定限制了 UNII-3 频段的传输距离。

6.2 UNII 频段

IEEE 802.11a 修正案规定，无线局域网可以使用 3 个 5GHz 频段传输数据，每个频段包括 4 个信道。这 3 个频段称为 UNII(Unlicensed National Information Infrastructure，无需牌照的国家信息基础设施)频段。802.11a 修正案将 UNII 频段划分为 UNII-1(低)、UNII-2(中)与 UNII-3(高)共 3 个频段。3 个频段的宽度均为 100MHz，这对于理解和记忆 UNII 频段很有帮助。

在 802.11h 修正案被批准后，IEEE 又定义了一个新的频段供无线局域网通信使用。这个频段包括 11 个信道，一般将其称为 UNII-2 扩展(UNII-2 Extended)频段。与其他 3 个 UNII 频段不同，UNII-2 扩展频段的宽度不是 100MHz，而是 255MHz。

本书采用“UNII”作为无需牌照的国家信息基础设施频段的缩写，许多文档也使用另一种缩写形式“U-NII”。两种缩写都很常见，且都为业界所接受。

目前，工作在 5GHz UNII 频段的 Wi-Fi 射频卡包括采用以下技术的设备：

- 802.11a(OFDM 射频卡)
- 802.11n(HT 射频卡)

请记住，并非所有国家和地区的射频监管机构都允许使用整个 UNII 频段进行通信。IEEE 802.11-2007 标准规定，无线局域网可以使用全部 4 个 UNII 频段、总共 23 个信道传输数据，不过其他国家对信道的分配可能会有所不同。本章后面将详细介绍所有 5GHz 信道。

6.2.1　UNII-1(低)频段

UNII-1 属于 UNII 低频段，范围是 5.150GHz～5.250 GHz，宽度为 100 MHz。FCC 规定，UNII-1 频段一般用于室内通信，主动辐射器允许使用的最大输出功率为 50mW。为符合 FCC 的功率管理要求，IEEE 将主动辐射器的最大输出功率限制为 40mW。2004 年之前，FCC 要求所有使用 UNII-1 频段通信的设备必须安装不可拆卸的天线，这意味着支持 UNII-1 频段的 802.11a 设备即便还支持其他频段或标准，也无法使用其他天线。

FCC 在 2004 年修改了原先的规定，允许设备安装可拆卸天线，前提是采用唯一的天线接头。其他在 UNII 频段与 2.4GHz ISM 频段使用的天线也需要遵守类似的规定。某些厂商允许用户将接入点配置为网桥，并使用 UNII-1 频段收发数据。部署无线网络时，请务必遵守当地监管机构的规定。

6.2.2　UNII-2(中)频段

UNII-2 属于 UNII 中频段，范围是 5.250GHz～5.350GHz，宽度为 100MHz。FCC 规定，UNII-2 频段用于室内或室外通信，主动辐射器允许使用的最大输出功率为 250mW。为符合 FCC 的功率管理要求，IEEE 将主动辐射器的最大输出功率限制为 200mW。其他国家和地区的监管机构可能会对 UNII-2 频段的使用做出其他限制，请务必遵守这些规定。

6.2.3　UNII-2 扩展频段

UNII-2 扩展频段的范围是 5.470GHz～5.725GHz，宽度为 255MHz。FCC 规定，UNII-2 扩展频段用于室内或室外通信，主动辐射器允许使用的最大输出功率为 250mW。为符合 FCC 的功率管理要求，IEEE 将主动辐射器的最大输出功率限制为 200mW。其他国家和地区的监管机构可能会对 UNII-2 扩展频段的使用做出其他限制，请务必遵守这些规定。2003 年批准通过的 802.11h 修正案首次在该频段上定义了无线局域网通信，在此之前，5GHz 无线局域网只能使用 UNII-1、UNII-2 和 UNII-3 频段传输数据。

第 5 章介绍了 802.11h 修正案定义的 TPC(Transmit Power Control，传输功率控制)与 DFS(Dynamic Frequency Selection，动态频率选择)机制，以避免无线局域网对雷达传输造成干扰。从 2007 年 7 月 20 日起，所有在美国和加拿大市场销售的 5GHz 无线局域网设备都必须支持 DFS。《FCC 条例》(FCC Rule)第 15.407 节第(h)(2)款规定，使用 UNII-2 和 UNII-2 扩展频段传输数据的 802.11 设备必须采用 DFS，以保护无线局域网通信免受军用或气象雷达系统的干扰。欧洲同样要求 802.11 设备支持 DFS。应再次强调的是，所有 UNII 频段都可能需要支持 TPC 与 DFS，各国监管机构负责制定具体的实施方案。

Wi-Fi 与需要牌照的设备同时工作时的关注点

随着 802.11n 修正案的正式批准，WLAN 网络呈现爆炸式增长，特别是在 5GHz 频段。WLAN 在 5GHz 频段应用增加的同时，使用相同的频带的其他技术(如军事和多普勒天气雷达)产生的干扰也增加了。当处理射频干扰时，你可能会发现有些难以识别的干扰源。

为了防止干扰，FCC 等监管机构会与正在使用的基于 UNII 频段的设备制造商一起来评估并试图查明干扰原因，然后提出建议，以防止干扰。例如，在存在多普勒天气雷达站点的特定区域会提出一些建议。与监管机构合作，制造商通常会让他们的客户在运行自己设备的同时而不会干扰使用其他技术的设备。

6.2.4 UNII-3(高)频段

UNII-3 属于 UNII 高频段，范围是 5.725GHz～5.825GHz，宽度为 100MHz。UNII-3 频段一般用于室外点对点桥接，不过美国等一些国家也允许室内无线局域网通信使用该频段。需要注意的是，欧洲的无线局域网通信不使用 UNII-3 频段。FCC 规定，UNII-3 频段主动辐射器允许使用的最大输出功率为 1000mW。为符合 FCC 的功率管理要求，IEEE 将主动辐射器的最大输出功率限制为 800mW。

观察表 6-1 可以发现，UNII-3 频段与 5.8GHz ISM 频段的起始频率相同。但是请注意，UNII-3 频段的宽度为 100MHz，而 5.8GHz ISM 频段的宽度为 150MHz。

表 6-1 5GHz UNII 频段

频段名称	频段范围	信道数量
UNII-1(低)	5.150GHz～5.250GHz	4
UNII-2(中)	5.250GHz～5.350GHz	4
UNII-2 扩展	5.470GHz～5.725GHz	11
UNII-3(高)	5.725GHz～5.825GHz	4

6.3 3.6GHz 频段

2008 年，802.11y 修正案正式批准。这个修正案特别针对 3.65GHz～3.7GHz 频段的使用。与其他需要牌照的频段不同，该频段的使用是排他性的，在靠近卫星地球基站附近是限制使

用的。尽管该项目是设计在美国使用的，但也被其他一些国家在没有批准一个新的修正案前被仔细设计并使用。3 它被设计在任何一个 5MHz、10MHz 或 20MHz 的信道运行。监管机构可以规定任意频率范围使用。

6.4　4.9GHz 频段

802.11-2007 标准规定 4.94GHz～4.99GHz 频段范围在美国用于公共安全和保护人民生命健康和财产安全。这个频率范围在加拿大和墨西哥也是许可的。

802.11j 修正案在 2004 年通过。它支持在日本使用 4.9GHz～5.091GHz 的频率范围，该修正案已经纳入 802.11-2007 标准。

因为这个频段接近 UNII-1 频段，所以很多无线网卡支持这个频段。

6.5　未来的 Wi-Fi 频段

2.4GHz ISM 频段是主要的无需牌照的频段，从 1997 年开始应用于 Wi-Fi 通讯。尽管 802.11a 在 1999 年就得到批准，但直到 2006 年，5GHz UNII 频段才真正开始应用。5GHz 频段持续扩展的原因是：2.4GHz 频段过于拥塞；5GHz 频段更宽，信道更多，正是由于有更多的信道，802.11n 才能利用信道绑定技术。同时 IEEE 还在着眼其他的频谱空间用于 Wi-Fi 通信。

60GHz　在第 5 章中了解到，802.11ad 修正案草案定义了 VHT 技术，可以在 60GHz 这个无需牌照的频段运行。新增强的 PHY 和 MAC 层技术使潜在速率达到 7Gbps。因为超高的频率使其很难穿透墙体等障碍物，所以这个技术最可能使用在短距离且带宽要求高的场合。图 6-1 所示的是一个三频网卡，同时支持 2.4GHz、5GHz 和 60GHz，这个三频网卡可以在 60GHz 的短距离范围及 2.4GHz 和 5GHz 的较大范围内实现无缝切换。

图 6-1　2.4GHz、5GHz 和 60GHz 三频网卡

White-Fi　如第 5 章所述，White-Fi 是一个术语，用于描述在未使用的电视射频频谱中 Wi-Fi 技术的应用，也被称为电视白色空间。802.11af 修正案草案建议在这些未使用的频率范围内应用 Wi-Fi 操作。如果这项技术成为一种现实，显著好处就是传输范围将得到扩大，因

为白色空间频率低于 1GHz。

6.6 窄带传输与扩频传输

射频传输方式主要分为窄带传输与扩频传输两类。窄带传输采用极窄的带宽来发送数据，而扩频传输采用超出实际所需的带宽来发送数据。扩频技术将需要传输的数据扩展到所使用的频率范围内。例如，窄带射频卡可能以 80W 的功率在 2MHz 宽的频率范围内传输数据，而扩频射频卡可能以 100mW 的功率在 22MHz 宽的频率范围内传输数据。

窄带信号和扩频信号的大致关系如图 6-2 所示。由于窄带信号占据的频率范围极窄，针对该频率范围的蓄意干扰或非蓄意干扰很容易破坏信号。而扩频信号占据的频率范围很宽，一般来说，除非干扰信号也扩展到与扩频信号相同的频率范围，否则外界的蓄意干扰或非蓄意干扰很难影响到扩频信号。

图 6-2 窄带信号与扩频信号的频率范围

窄带信号的传输功率远高于扩频信号。FCC 和其他国家的监管机构通常会要求用户在使用窄带发射机之前取得牌照，以降低两台窄带发射机相互干扰的概率。例如，调幅与调频广播电台所用的窄带发射机需要取得监管机构颁发的牌照，以确保同一地区或邻近地区的两个电台不会使用同一频道进行广播。

与此相反，扩频信号的传输功率极低，几乎不会对其他系统造成干扰。因此一般来说，用户在使用扩频发射机之前不需要取得当地监管机构颁发的牌照。

真实场景

谁发明了扩频技术？

扩频技术于 1942 年 8 月 11 日获得专利，申请人为影星海蒂·拉玛(Hedy Lamarr)和作曲家乔治·安泰尔(George Antheil)。扩频技术最初被设计用于鱼雷无线电制导系统，但是它后来的应用却与其设计初衷相去甚远。扩频技术的思想超前于时代，直到 1957 年，人们才对

扩频技术有了进一步研究。1962 年古巴导弹危机期间，美国军舰在对古巴的封锁中首次使用了跳频扩频技术。

如果读者希望了解更多扩频技术的有趣历史，请在互联网上搜索“Lamarr and Antheil”。读者可以找到大量介绍两位发明者的文章和网页，甚至原始专利证书的复印件。不过，该专利在扩频技术实际投入商用之前就已过期，两位发明者都没有从专利中获得任何收益。

多径干扰

影响射频通信质量的一个因素是多径干扰。反射信号在主信号之后到达接收天线会引起多径效应。图 6-3 演示了信号从客户端到达 AP 的过程。在图中可以看到三个不同信号，每个信号沿不同路径传播，这些路径的长度不同，传输时间也不同。多路径效应类似于人们听到的回声。

图 6-3　多径干扰

我们以在峡谷中呼唤朋友为例来说明多径效应。假设你对着朋友大喊：“Hello, how are you？”为了让朋友听清楚，你放慢语速，每隔 1s 喊出一个单词。如果他在听到你的声音 0.5s 之后听到回声(你的声音的多径反射)，你的朋友将听到如下声音：“HELLO hello HOW how ARE are YOU you”(大写单词表示主信号，小写单词表示回声)。由于回声在主信号(你的声音)之间进入他的耳朵，你的朋友不难理解你的话。但是，如果他在听到你的声音 1s 之后才听到回声，单词“HELLO”的回声(“hello”)将与单词“HOW”同时进入他的耳朵，你的朋友将无法分辨你在说什么。

射频数据通信的方式与声音传播的方式相同。主信号与反射信号之间的延迟称为时延扩展(delay spread)。通常在室内环境下的时延扩展在 30ns～270ns。室外环境下时延扩展通常大得多。如果时延扩展过长，反射信号会干扰到主信号的下一部分数据，这种情况称为码间干扰(inter-symbol interference，ISI)。扩频系统不易受码间干扰的影响，这是因为扩频信号占据的频率范围很宽，不同频率产生的多径延迟不同，某些波长可能会受到多径效应的影响，而另一些波长则不会。因此一般来说，扩频信号抗多径干扰的能力优于窄带信号。

802.11(DSSS)、802.11b(HR-DSSS)与 802.11g(ERP)抗时延扩展的能力有限。802.11DSSS 和 802.11b HR-DSSS 允许的最大时延扩展为 500ns。尽管系统能承受一定的时延扩展，不过时延扩展越短，系统性能越好。时延扩展增加时，802.11b 发射机将降低数据率，并使用较长的符号发送数据。但从另一方面来说，使用较长的符号可能会在码间干扰发生之前产生更长的延迟。一些 802.11b 厂商建议，当 802.11b 设备以 11Mbps 传输数据时，时延扩展应控制在

65ns 以内。

与 DSSS 相比，OFDM 抗时延扩展的能力更强，802.11g 发射机可以在时延扩展达到 150ns 时仍保持 54 Mbps 的数据率。不过这与发射机和接收机使用的 802.11g 芯片有关。某些芯片抗时延扩展的能力较差，当时延扩展较高时，芯片会切换到较低的数据率。

在 802.11n 技术应用之前，多径现象通常是个大麻烦，会严重影响 WLAN 的性能和吞吐量。随着 802.11n 和 MIMO 技术的引入，多径现象反而能够增强 WLAN 的性能。802.11n 的增强信号处理技术利用多个同时传输信号，实际上可从多径现象获益。第 18 章将介绍有关这方面的更多知识。

6.7 跳频扩频

802.11 原始标准定义了 FHSS(frequency hopping spread spectrum，跳频扩频)技术供传统的 FHSS(条款 14)设备使用。FHSS 设备工作在 2.4GHz ISM 频段，数据率为 1Mbps 和 2Mbps。大部分 FHSS 射频卡的生产时间为 1997 年～1999 年。IEEE 规定，北美 802.11FHSS 设备的工作频段为 2.402GHz～2.480GHz，宽度为 79MHz。

如图 6-4 所示，FHSS 的工作原理大致如下：使用一个很小的载频空间传输数据，然后跳到另一个很小的载频空间传输数据，再跳到其他很小的载频空间传输数据，依此反复进行。更确切地说，FHSS 发射机在一段时间内使用一个特定的频率传输数据，这段时间称为驻留时间。驻留时间结束后，发射机将跳到另一个频率，并在驻留时间内使用该频率传输数据。每次驻留时间结束后，FHSS 发射机都会跳到另一个频率继续传输数据。

图 6-4 FHSS 各分量

6.7.1 跳频序列

FHSS 射频卡采用一个预定义的跳频序列(hopping sequence)传输数据，跳频序列由一系列很小的载频构成，也称为跳频模式(hopping pattern)或跳频集(hopping set)。FHSS 射频卡并不使用一组信道或有限的频率空间传输数据，而是使用一系列称为跳(hop)的子信道传输数

据。在完成一个跳频序列后，FHSS 发射机将重复该跳频序列。图 6-4 显示了一个虚构的跳频序列，它包含 5 跳。

IEEE 802.11 原始标准规定，每一跳的宽度为 1MHz，这些跳包含在预定义的跳频序列中。北美和大部分欧洲国家采用的跳频序列包含至少 75 跳，但最多不超过 79 跳。其他国家对跳数的定义则有所不同。例如，法国采用包含 35 跳的跳频序列，而西班牙和日本采用包含 23 跳的跳频序列。为确保通信成功，所有 FHSS 发射机与接收机必须同时使用同一载频进行同步。可以在 FHSS 接入点上对 802.11 标准定义的跳频序列进行配置，接入点通过信标管理帧将跳频序列的信息传输给客户端。

6.7.2　驻留时间

驻留时间(dwell time)定义为 FHSS 系统使用某个特定频率传输数据的时间，即发射机切换到跳频序列中下一个频率之前在当前频率停留的时间。各国的射频通信监管机构通常会对驻留时间的长短做出限制。例如，根据 FCC 的规定，在任意一段 30s 的时间内，每个载频的最大驻留时间为 400ms。典型的驻留时间在 100ms～200ms 之间。IEEE 802.11 标准规定，跳频序列由至少 75 个宽为 1MHz 的频率构成。由于标准定义的最大带宽为 79MHz，因此一个跳频序列最多包含 79 跳。如果 FHSS 跳频序列由 75 跳构成，驻留时间为 400ms，则一个跳频序列的周期为 30s。在完成一个跳频序列后，发射机将重复该跳频序列。

6.7.3　跳变时间

跳变时间(hop time)并非一段具体的时间，而是 FHSS 发射机从一个频率切换到另一个频率时所消耗的时间。跳变时间通常很短，一般在 200μs～300μs 之间。与 100μs～200ms 的典型驻留时间相比，200μs～300μs 的跳变时间几乎可以忽略不计。跳变时间实际属于开销(浪费的时间)，无论驻留时间长短，跳变时间都是相同的。一般来说，驻留时间越长，发射机需要跳变的次数越少，吞吐量越高；驻留时间越短，发射机需要跳变的次数越多，吞吐量越低。

6.7.4　调制

FHSS 采用 GFSK(Gaussian frequency-shift keying，高斯频移键控)进行数据编码。二级 GFSK (2GFSK)使用两个频率表示比特 0 和 1，四级 GFSK(4GFSK)使用 4 个频率，每个频率代表两个比特(00、01、10 或 11)。由于 FHSS 在频率确定之前就开始循环，因此符号率(数据发送速率)只有大约 1Msps～2Msps(兆符号/秒)，只相当于 2.4GHz 载频的极小一部分。

驻留时间的意义

由于 FHSS 发射机在宽为 79MHz 的频率范围内跳变，窄带信号或噪声只能干扰到很小一部分频率，由此造成的吞吐量损耗几乎可以忽略不计。缩短驻留时间可以进一步减少干扰的影响。但是从另一方面来说，由于射频卡只有在驻留时间内才能传输数据，因此驻留时间越长，吞吐量越高。

802.11 FHSS 技术现在很少用到，CWNA 考试也不会考察这方面的内容。大多数 802.11 FHSS 制造商也不再生产 FHSS 的网卡和接入点，大多数机构也从 802.11 FHSS 过渡到了现在更新更快的传输方式。但理解 FHSS 的基础仍然重要，因为还有些产品(如蓝牙)仍然在使用 FHSS，尽管它的跳数、驻留时间和调频序列都与 802.11 FHSS 有很大区别。并且还要提醒大家，蓝牙也使用 2.4GHz ISM 频段，这一点与 802.11b/g/n 设备相同。

6.8 直序扩频

DSSS(direct sequence spread spectrum，直序扩频)技术最初定义在 802.11 原始标准中，工作频段为 2.4GHz，数据率为 1Mbps 和 2Mbps。802.11b 修正案也定义了 DSSS 技术，工作频段同样为 2.4GHz，数据率为 5.5Mbps 和 11Mbps。这两个数据率称为 HR-DSSS(High-Rate DSSS，高速直序扩频)。

802.11b(条款 18)设备向后兼容传统的 802.11 DSSS(条款 15)设备。也就是说，802.11b 设备既可以采用 DSSS 技术并以 1Mbps 和 2Mbps 的速率传输数据，也可以采用 HR-DSSS 技术并以 5.5Mbps 和 11Mbps 的速率传输数据。但是，802.11b 设备不采用 FHSS 技术，因此无法向后兼容 802.11 FHSS(条款 14)设备。

802.11-2007 标准第 15 条款定义了数据率为 1 Mbps 和 2 Mbps 的 DSSS 技术，第 18 条款定义了数据率为 5.5 Mbps 和 11Mbps 的 HR-DSSS 技术。

FHSS 发射机在不同频率之间跳变，而 DSSS 发射机只在一个信道上收发数据。数据被扩展到该信道的频率范围内，这个过程称为数据编码。

6.8.1 DSSS 数据编码

第 2 章曾经介绍过，多种因素都可能改变甚至破坏射频信号。由于 802.11 信号在无缚介质中传输，它极易受到射频干扰，因此必须采取措施将数据损坏的可能性降至最低。为此，每个数据比特首先被编码为多个比特，然后进行传输。

为数据添加的冗余信息称为处理增益。在设法压缩数据尺寸的今天，增加数据尺寸听起来有些不可思议。然而，添加冗余信息可以提高系统抗数据损坏的能力。系统将一个数据比特转换为一连串的比特，这些比特称为码片(chip)。数据比特与一个固定长度的比特序列 PN 码进行异或(XOR)运算，其输出即为码片。巴克码(Barker code)是一种常用的 PN 码，将巴克码与二进制数据 1 和 0 相异或，产生的码片序列如下：

二进制数据 1=1 0 1 1 0 1 1 1 0 0 0

二进制数据 0=0 1 0 0 1 0 0 0 1 1 1

产生的码片序列被扩展到一个很宽的频率空间内。如果 1 比特数据占据的频率空间

为 2MHz，则 11 个码片需要宽为 22MHz 的载频。将单个数据比特转换为一个码片序列的过程通常被称为扩展(spreading 或 chipping)。接收端将码片序列再转换回原始数据比特，这个过程称为解扩(de-spreading)。转换为码片的数据抗干扰能力很强，即使某些码片损坏，接收端射频卡仍然可以通过正确接收到的码片将数据解析出来。使用巴克码时，即使 11 个码片中有 9 个码片损坏，接收端射频卡仍可以正确解析码片序列，并将其恢复为原始数据比特。由于扩展过程使用的带宽较宽，通信几乎不会受到码间干扰的影响。

巴克码与 1 比特数据进行异或运算后将产生 11 个比特，这些比特称为码片，表示原始数据比特。也就是说，编码后的比特代表 1 比特数据。为避免混淆，最好将编码后的比特称为 Chip(码片)。

巴克码是一种长度为 11 码片的 PN 码，不过也可以采用其他长度的码片序列。为提高数据率，HR-DSSS 采用更复杂的 CCK(Complementary Code Keying，补码键控)作为调制方式。CCK 使用 8 码片 PN 码，各种比特序列都有相应的 PN 码。使用 CCK 时，如果将 4 比特数据转换为 8 个码片，则数据率为 5.5Mbps；如果将 8 比特数据转换为 8 个码片，则数据率为 11 Mbps。CCK 是一种值得研究的技术，但是 CWNA 考试并不考查 CCK 的细节。

6.8.2　调制

采用扩频技术将数据编码之后，发射机对数据进行调制，以产生包含码片的载波信号。DBPSK(differential binary phase-shift keying，差分二进制相移键控)采用两种相移，一种相移表示码片 0，另一种相移表示码片 1。为提高吞吐量，DQPSK(differential quadrature phase-shift keying，差分四进制相移键控)采用 4 种相移，每种相移可以调制 2 个码片(00、01、10、11)而非 1 个码片，速率因此提高了一倍。

表 6-2 总结了 802.11 和 802.11b 使用的数据编码与调制技术。

表 6-2　DSSS/HR-DSSS 的编码与调制方式概述

	数据率	编码方式	码片序列长度	编码比特数量	调制方式
DSSS	1Mbps	巴克码	11	1	DBPSK
DSSS	2Mbps	巴克码	11	1	DQPSK
HR-DSSS	5.5Mbps	CCK	8	4	DQPSK
HR-DSSS	11Mbps	CCK	8	8	DQPSK

6.9　分组二进制卷积码

PBCC(Packet Binary Convolutional Code，分组二进制卷积码)是一种调制技术，支持的数据率为 5.5Mbps、11Mbps、22Mbps 和 33Mbps。需要注意的是，发射机和接收机都必须支持 PBCC 才能达到较高的速率。PBCC 由 Alantro Communications 开发，后者于 2000 年被 Texas

Instruments 收购。PBCC 最初定义在 802.11b 修正案中，作为一种可选的调制方式。802.11g 修正案定义了另外两种可选的 ERP-PBCC 调制方式，其有效数据率为 22 Mbps 和 33 Mbps。

PBCC 与 ERP-PBCC 曾在 SOHO 市场中昙花一现，但是二者很少部署在企业无线局域网中。

6.10 正交频分复用

OFDM(Orthogonal Frequency Division Multiplexing，正交频分复用)是最常见的通信技术之一，广泛用于有线通信与无线通信。802.11-2007 标准规定，OFDM 的工作频段为 5GHz，ERP-OFDM 的工作频段为 2.4GHz。第 5 章曾经介绍过，OFDM 和 ERP-OFDM 本质上相同。需要注意的是，虽然 OFDM 并不属于扩频技术，但是它的特性与扩频技术比较接近，例如传输功率较低、使用超出实际所需的带宽传输数据等。由于二者的相似性，人们往往将 OFDM 归入扩频技术，不过从技术角度看，这种分法并不正确。如图 6-5 所示，OFDM 使用 52 个独立的、精确划分的频率传输数据。这些频率相隔很近，一般将它们称为子载波(subcarrier)。

图 6-5 802.11 信道与 OFDM 子载波

每个子载波的频率宽度均为 312.5KHz。虽然子载波本身的数据率较低，但是由于其数量众多，因此累积后的总数据率较高。子载波的低速率使得时延扩展在符号周期中所占的比例很小，这在很大程度上避免了码间干扰的发生。换句话说，与 DSSS 和 FHSS 两种扩频技术相比，OFDM 技术抗多径干扰的能力更强。图 6-6 显示了 52 个子载波中的 4 个，其中一个子载波以粗体显示，以方便读者理解。子载波之间的频率间隔经过精心选择，恰好能使谐波重叠，从而消除大部分不需要的信号。

图 6-6　子载波信号

52 个子载波按-26～+26 的顺序进行编号。其中 48 个子载波用于传输数据，另外 4 个子载波(编号为-21、-7、+7、+21)称为导频载波(pilot carrier)。导频载波作为接收机解调器的相位和幅度参考，用于补偿失真的 OFDM 信号。

6.10.1　卷积编码

OFDM 采用卷积编码(convolutional coding)进行纠错，以增强抗窄带干扰的能力。802.11-2007 标准将卷积编码定义为 OFDM 技术的纠错方式。卷积编码属于前向纠错，接收系统采用这种方式检测并修复损坏的比特。

卷积编码采用传输比特与编码比特之比实现不同的编码级别。二者之比越低，信号抗干扰能力越强，数据率越低。表 6-3 对 802.11a 与 802.11g 所用的调制方式和数据率进行了比较。注意，一种调制方式对应两种数据率和编码率，采用不同的编码率可以获得不同的数据率。卷积编码的原理非常复杂，CWNA 考试不会对卷积编码的细节进行考查。

表 6-3　802.11a 和 802.11g 数据率与调制方式的比较

数据率 (Mbps)	调 制 方 式	编码比特 /子载波	数据比特 /OFDM 符号	编码比特 /OFDM 符号	编码率 (数据比特/编码比特)
6	BPSK	1	24	48	1/2
9	BPSK	1	36	48	3/4
12	QPSK	2	48	96	1/2
18	QPSK	2	72	96	3/4
24	16-QAM	4	96	192	1/2
36	16-QAM	4	144	192	3/4
48	64-QAM	6	192	288	2/3
54	64-QAM	6	216	288	3/4

6.10.2　调制

OFDM 采用 BPSK(Binary Phase-Shift Keying，二进制相移键控)和 QPSK(quadrature phase-shift keying，四进制相移键控)调制以获得较低的数据率，采用 16-QAM 和 64-QAM 调制以获得较高的数据率。QAM(Quadrature Amplitude Modulation，正交调幅)是结合了调相与调幅的一种调制方式。

6.11 2.4GHz 信道

为更好地理解 802.11 DSSS、802.11b HR-DSSS 和 802.11g ERP 射频卡的工作方式，必须了解 IEEE 802.11-2007 标准是如何划分 2.4GHz 信道的。如表 6-4 所示，IEEE 将 2.4GHz ISM 频段划分为 14 个独立的信道，FCC 和其他国家的监管机构负责分配可以在本国使用的信道。表 6-4 列出了美国、加拿大与欧洲使用的信道。

表 6-4 2.4 GHz ISM 频段的信道规划

信 道 号	中心频率(GHz)	美国(FCC)	加拿大(IC)	大多数欧洲国家
1	2.412	X	X	X
2	2.417	X	X	X
3	2.422	X	X	X
4	2.427	X	X	X
5	2.432	X	X	X
6	2.437	X	X	X
7	2.442	X	X	X
8	2.447	X	X	X
9	2.452	X	X	X
10	2.457	X	X	X
11	2.462	X	X	X
12	2.467			X
13	2.472			X
14	2.484			

“X”表示支持的信道

信道由其中心频率(f_c)标识。每个信道的宽度为 22MHz，一般表示为 f_c±11MHz。例如，信道 1 的频率范围是 2.401～2.423GHz，其中心频率为 2.412GHz，因此可以将信道 1 表示为 2.412GHz±11MHz。需要注意，对 2.4GHz ISM 频段而言，两个信道中心频率的间隔只有 5 MHz。由于每个信道的宽度为 22MHz，且两个信道中心频率的间隔为 5MHz，因此信道之间会相互重叠。

图 6-7 显示了 2.4GHz 频段全部 14 个信道以及信道之间的重叠。从图中可以观察到，信道 1、6 和 11 以粗体显示，三者在频率上相隔很远且互不重叠。两个信道互不重叠的条件是，信道之间必须相隔至少 5 个信道(或 25MHz)。例如，虽然信道 2 和 9 互不重叠，但是除二者之外，无法找到第三个与信道 2 和 9 都不重叠的信道。在美国和加拿大，仅有的一组 3 个非重叠信道是信道 1、6 和 11。某些国家和地区允许使用信道 1～13，这种情况下也存在其他非重叠信道组合(如信道 1、6 和 12)，不过信道 1、6 和 11 是最常用的一组非重叠信道。

图 6-7　2.4 GHz 频段的 3 个非重叠信道

读者可能对 IEEE 802.11-2007 标准定义的 2.4GHz ISM 频段非重叠信道感到困惑，我们在此做一解释。802.11 DSSS、802.11b HR-DSSS 和 802.11g ERP 信道采用相同的编号方式，且具有相同的中心频率，但是信道的频率空间可能相互重叠。图 6-8 显示了信道 1、6 和 11，它们的中心频率之间相隔 25MHz。北美和大部分国家的 802.11b/g 网络部署基本都采用这 3 个非重叠信道。

图 6-8　802.11b HR-DSSS 的中心频率

如何判断 DSSS 或 HR-DSSS 的非重叠信道呢？802.11 原始标准规定，两个 DSSS 信道的中心频率之间必须相隔至少 30 MHz，才能认为它们互不重叠。对采用信道 1、6 和 11 的 DSSS 部署而言，由于三者中心频率之间的间隔只有 25MHz，这 3 个信道被划分为重叠信道。尽管如此，三者仍然是传统 DSSS 部署的信道复用模式中唯一可供选择的 3 个信道。这对现在的无线局域网部署影响不大，因为大部分 2.4GHz 部署目前都采用 802.11b/g/n 技术。

802.11b 修正案规定，两个 HR-DSSS 信道的中心频率之间必须相隔至少 25MHz，才能认为它们互不重叠。根据以上定义，信道 1、6 和 11 是互不重叠的。

802.11g 修正案向后兼容 802.11b HR-DSSS。前者同样规定，两个信道的中心频率之间必须相隔至少 25MHz，才能认为它们互不重叠。两个 802.11g ERP 信道的中心频率之间必须保持 25MHz 的间隔，二者才能被划分为非重叠信道。根据以上定义，无论采用 ERP-DSSS/CCK 还是 ERP-OFDM，信道 1、6 和 11 都是互不重叠的。

示意图中通常以弧线来表示一个信道的射频信号，但是实际信号的形状并非如此。如图 6-9 所示，除主载频(主频率)之外，信号还会产生边带载频。IEEE 定义了发射频谱模板(transmit spectrum mask)，并做出如下规定：第一边带载频(f_c−22MHz < f < f_c−11MHz，以及 f_c+11MHz < f < f_c+22MHz)的功率必须低于主载频 30dB 以上，其余边带载频(f < f_c−22MHz，以及 f > f_c+22MHz)的功率必须低于主载频 50dB 以上。

图 6-9 IEEE 802.11b 发射频谱模板

图 6-9 显示了 2.4GHz HR-DSSS 信道的发射频谱模板。定义发射频谱模板旨在最大限度减小采用不同频率通信的设备之间的干扰。边带载频相对于主载频的功率而言是微不足道的，如同呼喊和耳语的区别。但是只要耳语的距离足够近，它仍然可以被听到。射频设备的传输也是如此。

图 6-10 显示了信道 1、6 和 11 的射频信号，3 条信号功率电平线表示位于信道 6 的接入点接收到的信号功率。在电平 1 处，接入点只接收到功率高于电平 1 的信号，此时信道 1 和 11 的信号不会对信道 6 的信号造成干扰。在电平 2 处，信道 1 和 11 的信号会对信道 6 的信号造成轻微干扰。而在电平 3 处，信道 1 和 11 的信号会对信道 6 的信号造成严重干扰。为避免潜在的边带频率干扰，务必使各接入点在水平方向和垂直方向保持一定的距离(通常来说，5ft～10ft 已足够)。

图 6-10 边带载频干扰

6.12 5GHz 信道

802.11-2007 标准定义了 UNII-1、UNII-2、UNII-2 扩展和 UNII-3 共 4 种 5GHz UNII 频段。对 UNII-1 和 UNII-2 频段而言，最外侧的两个信道必须与其他频段相隔 30MHz；对 UNII-3

频段而言，最外侧的两个信道必须与其他频段相隔 20MHz。UNII-1、UNII-2 和 UNII-3 频段各包括 4 个互不重叠的信道，信道中心频率之间的间隔是 20MHz。UNII-2 扩展频段包括 11 个互不重叠的信道，信道中心频率之间的间隔也是 20MHz。

图 6-11 中的 3 张示意图分别显示了 UNII-1 和 UNII-2 频段的 8 个信道、UNII-2 扩展频段的 11 个信道以及 UNII-3 频段的 4 个信道。信道 36 以粗体显示，以便读者更容易区分信号的主载频及其边带频率。根据 IEEE 的定义，可以采用以下公式计算每个信道的中心频率：

$$5000+5\times n_{ch}\ \text{MHz}$$

式中 n_{ch} 是 0～200 之间的所有整数。

尽管 IEEE 并未对信道宽度做出明确定义，不过 OFDM 信道的频谱掩码约为 20MHz。

图 6-11　5GHz UNII 信道概览

观察图 6-12 显示的 OFDM 频谱掩码不难发现，边带载频的功率下降较为平缓。这会导致两个相邻信道的边带载频互相重叠，从而增加干扰发生的可能性。OFDM 最初定义在 802.11a 修正案第 17 条款中。该修正案规定，两个信道的中心频率之间只要相隔 20MHz，就可以认为它们互不重叠。5GHz UNII 频段全部 23 个信道均采用 OFDM，信道中心频率之间的间隔为 20MHz。因此根据 IEEE 的定义，所有 5GHz OFDM 信道理论上都是互不重叠的。但是，任何两个 5GHz 信道之间实际仍然存在一定程度的边带载频重叠。然而根据 802.11a 修正案定义的信道数量和信道间隔，区分相邻信道并避免干扰并非难事。

图 6-12 OFDM 频谱模板

6.13 相邻信道、非相邻信道与重叠信道

本章前面几节介绍了 IEEE 802.11-2007 标准定义的非重叠信道。两个 802.11 DSSS 信道的中心频率之间必须相隔 30MHz，才能认为它们互不重叠。对 802.11b HR-DSSS 和 802.11g ERP 而言，两个信道的中心频率之间必须相隔 25MHz，才能认为它们互不重叠。而两个 5 GHz OFDM 信道的中心频率之间必须相隔 20MHz，才能认为它们互不重叠。上述定义的重要之处在于，部署无线局域网时，相邻覆盖蜂窝之间需要规划一定的重叠以实现无缝漫游。然而相邻蜂窝使用的频率不能重叠，以免相互干扰。应进行信道复用规划，以避免因频率重叠导致网络性能下降。第 12 章将深入讨论信道复用规划的细节。

如何定义相邻信道(adjacent channel)与非相邻信道(nonadjacent channel)是人们经常争论的一个话题。802.11-2007 标准对相邻信道的定义较为宽泛。对 DSSS 和 HR-DSSS 物理层而言，所有与当前信道没有重复频率空间的信道都被定义为相邻信道；对 ERP 和 OFDM 物理层而言，只有第一个与当前信道没有重复频率空间的信道被定义为相邻信道。换句话说，IEEE 对相邻信道的定义与前面讨论的非重叠信道的定义几乎完全相同。尽管没有特别定义，单信道 2.4GHz HT 设备遵循 802.11g 的定义，单信道 5GHz HT 设备遵循 802.11a 的定义。感到困惑的读者请参考表 6-5 中 CWNP 项目对相邻信道的定义。

表 6-5　IEEE/CWNP 对相邻信道、非相邻信道和重叠信道的定义

	DSSS(802.11)	HR-DSSS(802.11b)	ERP(802.11g)	OFDM(802.11a)
频　段	2.4GHz ISM	2.4GHz ISM	2.4GHz ISM	UNII 频段
相邻信道	≥30MHz	≥25MHz	=25MHz	=20MHz
重叠信道	<30MHz	<25MHz	<25MHz	不存在

相邻信道的意义

IEEE 对相邻信道的宽松定义与无线局域网行业对相邻信道干扰(adjacent channel interference)的定义相互抵触。大多数 Wi-Fi 厂商使用“相邻信道干扰”这个术语来描述由于信道复用设计不当造成的系统性能下降。业界一般将相邻信道定义为前一个或后一个编号信道。例如，信道 3 是信道 2 的相邻信道。本书作者建议，不要理会前面介绍的 IEEE 对相邻信道的定义，因为 Wi-Fi 行业对相邻信道的定义更为常见。第 12 章将详细介绍相邻信道干扰的概念。

6.14　吞吐量与带宽

无线网络通常在有限的一段频率范围内传输数据，这个频率范围称为频段。频段即带宽，它对最终的数据吞吐量有一定影响，不过数据编码、调制、介质竞争、加密等许多因素对吞吐量的影响更大。

注意不要混淆频率带宽与数据带宽。数据编码和调制方式决定了数据率，后者有时也称为数据带宽。我们仅以 5GHz 信道和 OFDM 技术为例说明。虽然 OFDM(条款 17)射频卡支持的数据率包括 6Mbps、9Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps 和 54Mbps，但是所有 UNII 信道的频率带宽都是相同的，不同的只是调制和编码方式。采用不同的调制和编码方式可以获得不同的数据率，通常也将其称为数据带宽。

向非专业人员解释无线网络时，他们可能会对 802.11 无线局域网的实际吞吐量感到惊讶。例如，初学者在计算机专卖店中看到 802.11 设备的包装上标有 300Mbps 字样，他往往会认为这台设备可以提供的吞吐量是 300Mbps。802.11 技术采用称为 CSMA/CA(载波侦听多路访问/冲突避免)的介质访问方式，即在任何给定的时间内，有且只有一台无线设备可以使用介质收发数据。由于射频介质的半双工特性以及 CSMA/CA 产生的开销，实际的总吞吐量一般不会超过数据率的 50%。除 802.11 通信的半双工特性之外，不同的传输频率也会影响吞吐量。5GHz 和 2.4GHz 可能会利用 HT 和 OFDM 技术，2.4GHz ISM 频段存在较大的射频噪声，吞吐量通常会小于 5GHz 频段的设备。

802.11 射频介质是一种共享介质，也就是说，所有关于吞吐量的讨论均指总吞吐量(aggregate throughput)，理解这一点至关重要。例如，当数据率为 54Mbps 时，由于 CSMA/CA 产生的开销，总吞吐量可能只有 20Mbps 左右。如果 5 个客户端同时从 FTP 服务器下载一个文件，则理想情况下，每个客户端的吞吐量只有 4Mbps 左右。

其他许多因素也会增加开销，进而影响吞吐量。为保护数据帧的安全，需要对其加密和解密，这会增加帧的长度，从而增加通信开销。帧分片将一个帧分解为若干个较小的帧进行

传输，每一个拆分后的帧都有完整的 802.11 报头，这也会增加额外的开销。RTS/CTS 机制(将在第 9 章中介绍)同样会增加通信开销，从而影响系统的吞吐量。但是在某些情况下，如果由于干扰等原因导致初始吞吐量过低，采用帧分片和 RTS/CTS 机制反而可以提高吞吐量。

OSI 模型包含大量参数，几乎所有参数都会对 802.11 通信的吞吐量产生影响。请读者务必理解各种影响吞吐量的因素及其后果，以及采用何种方式(如果存在的话)能最大限度消除这些因素对总数据吞吐量的影响。

6.15 通信抗逆力

本章介绍的许多技术都具备一定程度的抗干扰能力。扩频技术将数据扩展到一个较宽的频率范围，扩频信号不易遭到窄带干扰。FHSS 抗窄带干扰的能力优于 OFDM，而 OFDM 抗窄带干扰的能力优于 DSSS。扩频技术使用很宽的一段频率传输数据，时延扩展与码间干扰只能影响一部分频率。因此从本质上讲，扩频技术具备良好的通信抗逆力。此外，数据编码也提供了一定的纠错能力，这有助于减少数据重传。

6.16 小结

本章重点介绍无线网络与扩频通信所用的各种技术。802.11、802.11b 和 802.11g 射频卡工作在 2.4GHz ISM 频段，802.11a/h 射频卡工作在 5GHz UNII 频段。802.11n HT 射频卡既可以工作在 2.4GHz ISM 频段，也可以工作在 5GHz UNII 频段。本章讨论了以下 ISM 和 UNII 频段：

- ISM 工业频段：902MHz～928MHz
- ISM 科学频段：2.4000GHz～2.4835GHz
- ISM 医用频段：5.725GHz～5.875GHz
- UNII-1(低)频段：5.150GHz～5.250GHz
- UNII-2(中)频段：5.250GHz～5.350GHz
- UNII-2 扩展频段：5.470GHz～5.725GHz
- UNII-3(高)频段：5.725GHz～5.825GHz

此外还谈到了一下频段：

- 4.94GHz～4.99GHz—US Public Safety
- 4.9GHz～5.091GHz—Japan
- 60GHz
- < 1 GHz – White-Fi

本章详细介绍了扩频技术、OFDM 技术以及卷积编码。读者应掌握以下重要的扩频技术和术语：

- FHSS
- 驻留时间

- 跳变时间
- DSSS

本章最后比较了吞吐量与带宽，并回顾了 802.11 通信使用的各种技术以及它们的抗干扰能力。

6.17　考试要点

了解所有 ISM 和 UNII 频段的技术规范。务必熟悉所有频率、带宽使用、信道以及各种技术要求的信道中心频率间隔。

了解扩频技术。扩频技术涉及的内容很多，它是一种相当复杂的技术。理解 FHSS、DSSS 和 OFDM(请注意，虽然 OFDM 不属于扩频技术，但是它具备与扩频技术类似的特性)。理解扩频技术和 OFDM 技术采用的编码和调制方式。

理解本章讨论的各种传输技术的异同。本章讨论了许多技术，读者应认真比较并理解这些技术的相似点和不同点。参加 CWNA 考试时，应特别注意题目中出现的各种细节。

6.18　复习题

复习题的答案见附录 A。

1. Which of the following are valid ISM bands? (Choose all that apply.)
   A. 902–928MHz
   B. 2.4–2.5GHz
   C. 5.725–5.825GHz
   D. 5.725–5.875GHz
2. Which of the following are valid UNII bands? (Choose all that apply.)
   A. 5.150–5.250GHz
   B. 5.47–5.725GHz
   C. 5.725–5.825GHz
   D. 5.725–5.850GHz
3. Which technologies are used in the 2.4GHz ISM band? (Choose all that apply.)
   A. FHSS
   B. ERP
   C. DSSS
   D. HR-DSSS
4. 802.11n (HT clause 20 radios) can transmit in which frequency bands? (Choose all that apply.)
   A. 2.4–2.4835GHz
   B. 5.47–5.725GHz

C. 902–928GHz

D. 5.15–5.25GHz

5. In the UNII-1 band, what is the center frequency of channel 40?

A. 5.2GHz

B. 5.4GHz

C. 5.8GHz

D. 5.140GHz

6. What is the channel and band of a Wi-Fi transmission whose center frequency is 5.300 GHz?

A. UNII-1 channel 30

B. UNII-1 channel 60

C. UNII-2 channel 30

D. UNII-2 channel 60

7. The 802.11-2007 standard requires how much separation between center frequencies for HR-DSSS (clause 18) channels to be considered nonoverlapping?

A. 22MHz

B. 25MHz

C. 30MHz

D. 35MHz

E. 40MHz

8. What best describes *hop time*?

A. The period of time that the transmitter waits before hopping to the next frequency

B. The period of time that the standard requires when hopping between frequencies

C. The period of time that the transmitter takes to hop to the next frequency

D. The period of time the transmitter takes to hop through all of the FHSS frequencies

9. As defined by the IEEE-2007 standard, how much separation is needed between center frequencies of channels in the UNII-2 Extended band?

A. 10MHz

B. 20MHz

C. 22MHz

D. 25MHz

E. 30MHz

10. When deploying an 802.11g (ERP-OFDM) wireless network with only two access points, which of these channel groupings would be considered nonoverlapping? (Choose all that apply.)

A. Channels 1 and 3

B. Channels 7 and 10

C. Channels 3 and 8

D. Channels 5 and 11

E. Channels 6 and 10

11. Which spread spectrum technology specifies data rates of 22Mbps and 33Mbps?

A. DSSS

B. ERP-PBCC

C. OFDM

D. PPtP

12. If data is corrupted by previous data from a reflected signal, this is known as what?

A. Delay spread

B. ISI

C. Forward error creation

D. Bit crossover

13. Assuming all channels are supported by a 5GHz access point, how many possible channels can be configured on the access point?

A. 4

B. 11

C. 12

D. 24

14. Which of these technologies is the most resilient against the negative effects of multipath?

A. FHSS

B. DSSS

C. HR-DSSS

D. OFDM

15. HR-DSSS (clause 18) calls for data rates of 5.5Mbps, and 11Mbps. What is the average amount of aggregate throughput percentage at any data rate?

A. 80percent

B. 75percent

C. 50percent

D. 100percent

16. As defined in the IEEE 802.11-2007 Standard, choose the answer that shows the number of channels in each of the UNII bands, listed in the following order: UNII-1, UNII-2, UNII-2e, UNII-3.

A. 4,4,14,4

B. 4,4,11,4

C. 8,4,11,4

D. 4,4,4,11

17. With the center frequency of channel 1 at 2.412GHz, what is the center frequency of channel 2?

A. 2.444GHz

B. 2.417GHz

C. 2.424GHz

D. 2.422GHz

18. What are the modulation types used by OFDM technology? (Choose all that apply.)

A. QAM

B. Phase

C. Frequency

D. Power

19. The Barker code converts a bit of data into a series of bits that are referred to as what?

A. Chipset

B. Chips

C. Convolutional code

D. Complementary code

20. OFDM uses how many 312.5KHz data subcarriers when transmitting?

A. 54

B. 52

C. 48

D. 36

第 7 章 无线局域网拓扑结构

在该章中，你将学习以下内容：

- √ 无线网络拓扑结构
  - 无线广域网(WWAN)
  - 无线城域网(WMAN)
  - 无线个人域网(WPAN)
  - 无线局域网(WLAN)
- √ 802.11 拓扑结构
  - 接入点
  - 客户端
  - 集成服务(IS)
  - 分布系统(DS)
  - 无线分布系统(WDS)
  - 服务集标识符(SSID)
  - 基础服务集(BSS)
  - 基础服务集标识符(BSSID)
  - 基本服务区(BSA)
  - 扩展服务集(ESS)
  - 独立基础服务集(IBSS)
  - Mesh 基础服务集(MBSS)
- √ 802.11 配置模式
  - 接入点模式
  - 客户端模式

计算机之间通过计算机网络相互通信。计算机网络可以被配置为对等模式、客户端-服务器模式或带有分布式哑终端的集中式中央处理器模式。在计算机网络中，节点的物理以及(或者)逻辑布局称为拓扑结构。如果读者曾经学习过网络基础课程，那么对有线网络中常用的总线、环形、星形、网状以及混合拓扑结构应该不会感到陌生。

每种拓扑结构都有其利弊。网络拓扑的规模相差很大，它既可以覆盖极小的区域，也可以作为全球性的架构存在。无线拓扑结构与无线硬件的物理和逻辑布局有关。无线技术的种类繁多，可以将这些无线技术划分到 4 类不同的无线网络拓扑中。802.11-2007 标准定义了无线局域网通信，包括 3 种称为服务集(service set)的标准拓扑结构。长期以来，厂商还生产了采用非标准拓扑结构的 802.11 硬件设备，以满足某些特定的无线组网需要。本章将介绍各种无线技术采用的拓扑结构，并讨论 802.11 技术采用的标准与非标准拓扑结构。

7.1 无线网络拓扑结构

虽然本教程主要介绍 802.11 无线局域网技术，但是也存在其他无线技术与标准，它们为不同规模的区域提供射频覆盖。除 802.11 技术外，蜂窝电话、蓝牙与 ZigBee 都是常见的无线技术。各种无线技术都可以被划分到以下 4 种无线拓扑结构中：

- 无线广域网(wireless wide area network，WWAN)
- 无线城域网(wireless metropolitan area network，WMAN)
- 无线个人域网(wireless personal area network，WPAN)
- 无线局域网(wireless local area network，WLAN)

802.11-2007 标准属于无线局域网标准。不过在某些情况下，802.11 技术也可以部署在其他无线网络架构中，这一节将对此进行讨论。

7.1.1 无线广域网(WWAN)

广域网(WAN)覆盖广阔的地理区域，它可能跨越整个州、地区、国家甚至覆盖全球。互联网是最常见的广域网。不少私营企业和上市公司的广域网由 T1 线路、光纤、路由器等硬件基础设施构成。有线广域网通信使用包括帧中继、ATM(异步传输模式)、MPLS(多协议标签交换)在内的多种协议。

无线广域网同样覆盖广阔的地理区域，所不同的是，它使用无线介质而非有线介质传输数据。典型的无线广域网采用蜂窝电话技术或者专有的、需要牌照的无线桥接技术。ATT Wireless、Verizon、Vodafone 等移动运营商采用各种蜂窝技术为用户提供服务，这些技术包括 GPRS(通用分组无线服务)、CDMA(码分多址)、TDMA(时分多址)、LTE(长期演进)和 GSM(全球移动通信系统)。手机、平板电脑、蜂窝网卡等许多设备都可以收发数据。

与 802.11 等无线技术相比，无线广域网的数据速率和带宽相对偏低。不过随着蜂窝技术的发展，蜂窝数据传输率也在逐渐提高。需要注意的是，802.11 无线局域网基础架构在当前无法扩展，因此无法部署在无线广域网中。然而 Wi-Fi 技术和蜂窝技术融合的市场正在快速发展。

7.1.2　无线城域网(WMAN)

无线城域网为都会区(如城市和周边的郊区)提供射频覆盖。开发无线城域网的目的是为了弥补其他无线技术在室外宽带无线接入方面的不足，目前的技术发展使无线城域网向实用化又迈进了一步。与无线城域网相关的技术定义在 IEEE 802.16 标准中，该标准定义的宽带无线接入有时称为 WiMAX(Worldwide Interoperability for Microwave Access，全球微波互联接入)。WiMAX 论坛(WiMAX Forum)负责进行 802.16 硬件等无线宽带设备的兼容性与互操作性测试。

业界将 802.16 技术视为其他宽带服务(如 DSL 和有线电视)的直接竞争对手。802.16 无线技术通常作为最后一英里的数据交付解决方案，不过它也可以用于提供城际范围内的用户接入。

有关 802.16 标准的更多信息请参阅 http://www.ieee802.org/16，有关 WiMAX 的信息请参阅 www.wimaxforum.org。

以往曾有大量关于 Wi-Fi 网络城际部署可能性的探讨，即采用无线局域网为都会区范围内的用户提供互联网接入。尽管 802.11 技术的设计初衷并不是为如此广阔的区域提供接入，许多城市的确曾试图在无线城域网中部署 802.11 技术以实现这种壮举。这种大规模的 802.11 部署采用专有的无线 Mesh 路由器或 Mesh 接入点。多数大规模的城际 Wi-Fi 部署计划已经搁浅。因为 Wi-Fi 技术无法扩展到整座城市。但是有些 WLAN 厂商和 4G/LTE 电信公司合作已经成功部署了多达 40 000 个接入点的 802.11 无线城域网。

7.1.3　无线个人域网

相隔很近的用户计算机设备之间通过无线个人域网(wireless personal area network，WPAN)交换数据。笔记本电脑、PDA、平板电脑、智能手机等设备可以采用多种无线技术相互通信。无线个人域网既可以用于设备之间的通信，也可以作为接入局域网以及(或者)互联网等其他高级网络的入口。蓝牙与红外技术是两种最常见的无线个人域网技术。红外线是一种光介质，而蓝牙是一种采用 FHSS(跳频扩频)技术的射频介质。

IEEE 802.15 工作组致力于开发蓝牙和 ZigBee 等无线个人域网技术。ZigBee 也是一种射频介质，它在低成本无线个人域网架构中的应用潜力很大。

有关 802.15 无线个人域网标准的更多信息请参阅 www.ieee802.org/15，有关蓝牙技术的信息请参阅 www.bluetooth.com，有关 ZigBee 技术的信息请参阅 ZigBee 联盟(ZigBee Alliance)的网站：www.zigbee.org，有关红外通信的信息请参阅红外数据协会(Infrared Data Association)的网站：www.irda.org。

802.11 技术用于无线个人域网的最好例子是对等连接。我们将在 7.2.11 一节中详细介绍 802.11 对等网络。

7.1.4 无线局域网

本书前面曾经介绍过，802.11-2007 标准定义了无线局域网(WLAN)技术。局域网为大楼或校园提供网络连接。802.11-2007 标准及其修正案定义的传输距离与速度使得 802.11 无线介质成为承载局域网通信的不二之选。实际上，大部分 802.11 无线网络部署都属于局域网，它们为企业与家庭用户提供接入。

典型的无线局域网包括多个 802.11 接入点，这些接入点通过有线骨干网相连。在企业部署中，无线局域网通常作为终端用户访问网络资源与服务的入口以及接入互联网的网关。虽然在其他无线拓扑结构中也可以使用 802.11 硬件设备，但大部分 Wi-Fi 部署都属于无线局域网，这也是 IEEE 802.11 工作组开发该技术的初衷。在谈到无线局域网时，一般即是指标准的 802.11 解决方案，不过市场上也存在其他互为竞争对手的专用无线局域网技术。

注意，大公司可在全球范围内部署和管理 802.11 WLAN。可以集中管理具有多个地理位置的企业 Wi-Fi 网络，也可以通过 VPN 进行管理。第 10 章将深入讨论 Wi-Fi 管理和规模。

7.2 802.11 拓扑结构

802.11 无线网络主要由无线射频卡构成，802.11 标准将其称为终端(station)。无线射频卡既可以位于接入点中，也可以作为客户端使用。802.11 标准定义了 3 种不同的 802.11 拓扑结构，它们称为服务集，服务集描述了无线射频卡之间的通信方式。这 3 种 802.11 拓扑结构分别是 BSS(Basic Service Set，基础服务集)、ESS(Extended Service Set，扩展服务集)与 IBSS(Independent Basic Service Set，独立基础服务集)。最近 802.11s-2011 修正案成了第四种服务集，即 Mesh 服务集(MBSS)。

在讨论各种 802.11 拓扑结构之前，我们需要首先回顾一下经常被误解的基本网络术语：单工、半双工与全双工。这些术语描述了人们的交流方式以及计算机设备之间的通信方式。

在单工通信中，一台设备只能发送数据，另一台设备只能接收数据。单工通信的例子如调频广播。计算机网络很少使用单工通信。

在半双工通信中，两台设备都可以收发数据，但是二者无法同时收发数据。半双工通信的例子如对讲机和双向无线电。IEEE 802.11 无线局域网采用半双工通信。

在全双工通信中，两台设备可以同时收发数据。例如电话通信，就属于典型的全双工通信。大部分 IEEE 802.3 设备都具备全双工通信的能力，不过在无线网络中，只有设置双信道(两个方向分别用于接收和发送)之后才能实现全双工通信。尽管某些广告声称目前的 802.11 技术能以全双工方式工作，但是这并不符合事实。

这一节将介绍 3 种 802.11 服务集以及其他非标准 802.11 拓扑结构的构成。

7.2.1　接入点

以太网集线器以半双工方式工作，它属于有线基础架构设备。有线集线器实际上是一种共享介质，即同时只有一台主机设备能收发数据。接入点也属于半双工设备，这是因为在任意给定时间内，有且只有一块无线射频卡可以使用半双工射频介质收发数据。实际上，可以将接入点视为一种带有无线射频卡和天线的集线器。接入点中的无线射频卡必须采用与客户端无线射频卡相同的方式竞争半双工射频介质的使用权。

CWNP 最初将接入点定义为一种具备类交换机智能的半双工设备，上述定义对自治接入点(autonomous access point)同样适用。第 10 章将介绍三种网络设计的逻辑平面：管理、控制和数据平面。同时还会在第 10 章介绍类交换机 AP 与基于控制器的 AP 之间的区别。基于控制器的接入点经常被称作“瘦 AP”或轻量接入点。在瘦 AP 架构中，智能位于控制器而非瘦 AP。现在还出现了许多混合模式的架构，在这种架构中，智能也存在于 AP 中。

类交换机接入点或 WLAN 控制器在二层寻址并转发无线流量，这是二者具备类交换机智能的最好例证。受控有线交换机维护一份称为内容可寻址内存(content addressable memory，CAM)的动态 MAC 地址表，后者根据帧的目标 MAC 地址将其发送到相应的端口。类似地，接入点或 WLAN 控制器作为入口设备，它们将流量发送给骨干网或无线介质。802.11 无线帧的报头通常包括 3 个 MAC 地址，不过在某些情况下，无线帧也可能包括 4 个 MAC 地址。接入点采用复杂的二层寻址方式，无线帧的 3～7 层信息被最终转发给集成服务(integration service，IS)或其他无线客户端。802.11 无线数据帧的帧体包含上层信息，后者称为 MSDU(MAC Service Data Unit，MAC 服务数据单元)。转发 MSDU 属于自治接入点或 WLAN 控制器具备的类交换机智能。人们常将类交换机智能比作 CAM 表，这种智能被称为分布系统服务(distribution system service，DSS)，稍后将对此做详细介绍。

许多接入点都支持 VLAN(虚拟局域网)。例如，接入点可以支持在受控有线交换机或 WLAN 控制器上创建的 VLAN，尽管 802.11 标准并未对此做出定义。使用 VLAN 可以减小广播域的尺寸。为保护网络安全，也可以将用户划分到不同的 VLAN 中。

7.2.2　客户端

用在接入点以外的无线射频卡一般被称为客户端。笔记本电脑、PDA、扫描仪、电话等许多移动设备都使用客户端无线射频卡。客户端必须采用与接入点无线射频卡相同的方式竞争半双工射频介质的使用权。当客户端与接入点建立二层连接后，称二者建立关联(associated)。

7.2.3　集成服务

802.11-2007 标准定义了集成服务(IS)，集成服务经由入口设备在分布系统(distribution system，DS)与非 IEEE 802.11 无线局域网之间实现 MSDU 的交付。可将集成服务简单定义为一种帧格式转换方式，而入口设备通常是接入点或 WLAN 控制器。如前所述，802.11 无线数据帧的净荷是 3～7 层信息，即 MSDU，MSDU 的最终目的地通常是有线网络基础架构(802.3 以太网)。由于 802.3 以太网属于另一种物理介质，因此 802.11 数据帧净荷必须被转换为适合

在以太网中传输的 802.3 帧。我们以 VoWiFi 电话向自治接入点发送 802.11 数据帧为例对两种帧的转换方式做一说明。802.11 帧的 MSDU 净荷是 VoIP 数据包，其最终目的地是位于 802.3 网络核心的 VoIP 服务器。集成服务首先将 802.11 帧的帧头与帧尾剥离，并将 VoIP 数据包(MSDU 净荷)封装到一个 802.3 帧中，然后将封装后的 802.3 帧发送给以太网。与之类似，集成服务也可将 802.3 帧净荷转换为适合接入点无线接口传输的 802.11 帧。

802.11-2007 标准并未定义集成服务的工作方式。集成服务通常在 802.11 介质与 802.3 介质之间传输数据帧净荷，不过也可在 802.11 介质与其他介质之间传输数据帧净荷。采用自治接入点架构时，集成服务机制位于网络边界；采用 WLAN 控制器/轻量接入点架构时，集成服务机制位于 WLAN 控制器中。

7.2.4 分布系统

802.11-2007 标准还定义了分布系统(DS)，其通过集成后的局域网将多个 BSS(基础服务集)连接在一起，从而构成一个 ESS(扩展服务集)。稍后将对服务集做详细介绍。接入点本质上属于一种入口设备。无线流量既可以被传输给无线介质，也可以被转发给集成服务。分布系统主要由以下两部分构成：

分布系统介质(distribution system medium，DSM) 分布系统介质是一种连接接入点的逻辑的物理介质，802.3 介质是最常见的分布系统介质。

分布系统服务(distribution system services，DSS) 分布系统服务提供前面介绍过的类交换机智能。内置在接入点中的系统服务一般以软件的形式存在，这种软件服务用于管理客户端关联、重关联与解除关联。分布系统服务采用 802.11 MAC 报头二层寻址，3～7 层信息(MSDU)被最终转发给集成服务或其他无线客户端。CWNA 考试不要求考生了解分布系统服务的所有细节，不过 CWAP 认证将对此做详细考查。

单一接入点或多个接入点可能与同一个分布系统介质相连。大部分 802.11 无线局域网部署将接入点作为接入 802.3 以太网骨干网的入口设备，此时以太网就是分布系统介质。接入点通常与交换以太网相连，以太网一般通过 PoE(以太网供电)为接入点供电。

接入点也可以作为接入其他有线与无线介质的入口设备。802.11-2007 标准没有规定介质的种类，也没有定义接入点在何种介质上转译和转发数据。一般将接入点描述为两种介质之间的“转译桥梁”，也就是说，接入点可以在 802.11 介质与任何分布系统介质采用的介质之间转译和转发数据。需要再次强调的是，分布系统介质在绝大多数情况下都是 802.3 以太网，如图 7-1 所示。

图 7-1 分布系统介质

7.2.5　无线分布系统

802.11-2007 标准为无线局域网通信定义了一种包含 4 个 MAC 地址的帧格式，不过标准仅描述了帧格式，并没有指明其工作方式。这种机制称为无线分布系统(wireless distribution system，WDS)，实际使用的无线分布系统包括桥接、中继器、Mesh 网以及可以同时提供覆盖与回传的接入点。一般而言，分布系统都是有线以太网骨干网，但是也存在采用无线连接的分布系统。无线分布系统通过无线回传(wireless backhaul)将接入点连接在一起。

无线分布系统既可以采用单频 802.11 无线接入点，也可以采用双频 802.11 无线接入点。图 7-2 显示了两个 802.11 接入点，二者都只有一个无线接口。接入点的无线接口不仅能提供客户端接入，也可以作为无线分布系统与其他接入点直接通信。这种解决方案的弊端在于介质的半双工特性会影响吞吐量。这对只有一个无线接口的接入点而言尤其是个问题，因为接入点无法与客户端和其他接入点同时通信，网络的吞吐量将因此而降低。

图 7-2　无线分布系统：单无线接口

最理想的分布系统

绝大多数情况下，802.3 网络都是分布系统的最佳选择。由于大部分企业已经部署了有线 802.3 基础架构，将无线网络集成到交换以太网中是顺理成章的事情。物理障碍、射频干扰等许多可能影响无线分布系统的因素并不会影响有线分布系统介质。如果接入点确实无法连接到有线网络，换用无线分布系统或许是一个切实可行的解决办法。更理想的无线分布系统解决方案采用不同的频率与无线接口来提供客户接入与分布。

图 7-3 显示了两个双频 AP，这种 AP 的两个无线接口分别工作在不同的频段。2.4GHz 无线接口为客户端提供接入，而 5GHz 无线接口作为两个接入点之间的无线分布系统链路。由于 2.4GHz 无线接口与 5GHz 回传无线接口可以同时工作，因此网络的吞吐量不会受到影响。大多数 Wi-Fi 厂家都有利用 5GHz 射频卡的 Mesh 产品。

图 7-3　无线分布系统：双无线接口

无线中继器是另一种实际使用的 802.11 无线分布系统。中继器可以将无线局域网小区的覆盖范围扩展到无法安装 802.3 以太网下行电缆的区域。如图 7-4 所示，客户端通过一个中继器接入点与连接到 802.3 以太网骨干网的根接入点建立关联并相互通信。中继器的作用是扩展覆盖范围，它并不与有线骨干网相连。802.11 帧净荷首先被转换为 802.3 以太网帧，然后被发送到骨干网中的服务器。中继器与接入点之间的 802.11 通信是一种无线分布系统。如图 7-5 所示，在无线分布系统中传输的帧包括 4 个 MAC 地址，它们是源地址、目标地址、发射机地址和接收机地址。

图 7-4　中继器小区

图 7-5　WDS 帧头

中继器与根接入点必须位于同一信道才能有效扩展根接入点的小区覆盖范围。为确保通信成功，中继器和接入点覆盖小区之间的重叠范围不能小于 50%。尽管中继器可以为无法安装下行电缆的区域提供射频覆盖，不过由于所有帧都需要传输两次，吞吐量将因此而降低，延时也会随之增加。由于接入点小区与中继器小区使用同一信道且位于相同的一层域，因此所有无线接口都必须竞争介质的使用权。此外，中继器会产生额外的介质竞争开销，这会影响网络性能。

大多数企业级 WLAN 厂商不再提供单频中继器。大多数企业级 AP 是支持 mesh 的多频 AP，可以提供 2.4GHz 接口用于客户端接入，还提供 5GHz 接口用于回传。如果在 Mesh 环境中某个用于回传的无线接口同时允许客户端接入的话，其实这个无线接口就起到了中继器的作用。

7.2.6　服务集标识符

SSID(Service Set IDentifier，服务集标识符)是标识 802.11 无线网络的逻辑名，与 Windows 工作组名类似。3 种标准的 802.11 拓扑结构都使用 SSID，无线射频卡可以通过主动扫描(active scanning)或被动扫描(passive scanning)识别彼此的身份。SSID 由最多 32 个字符组成，且区分大小写，配置在所有接入点与客户端的无线射频卡中。图 7-6 显示了一个接入点中配置的 SSID。

图 7-6　SSID(服务集标识符)

大部分接入点具备隐藏 SSID 的能力，隐藏后的网络名只对合法终端用户可见。802.11-2007 标准并没有定义 SSID 隐藏，后者在保护系统安全中所起的作用极其有限。不过，许多管理员仍然将 SSID 隐藏作为一种简单的安全手段使用。

第 9 章将详细介绍主动扫描与被动扫描，第 13 章将讨论 SSID 隐藏。

7.2.7　基础服务集

BSS(Basic Service Set，基础服务集)是 802.11 无线网络的基础拓扑结构。构成 BSS 的通信设备包括一个接入点和若干客户端。在加入接入点的无线域之后，客户端之间通过接入点交换数据。如果客户端是 BSS 的成员并与接入点建立二层连接，则称二者建立了关联。图 7-7 显示了一个标准的 BSS。

图 7-7　基础服务集(BSS)

接入点通常与分布系统介质相连，不过这并非构成 BSS 的必要条件。如果接入点作为接入分布系统的入口设备，则客户端可以经由接入点访问分布系统介质中的网络资源。需要注意的是，客户端之间的数据交换必须通过接入点进行，客户端之间无法直接通信。

7.2.8 基础服务集标识符

接入点无线射频卡的 48 位(6 字节)MAC 地址称为 BSSID(Basic Service Set Identifier，基础服务集标识符)。BSSID 的简单定义就是 AP 无线射频卡的 MAC 地址，但更精确的定义是每个 BSS 的二层标识符，大部分情况下，BSSID 即为接入点无线射频卡的 MAC 地址。

不要混淆 BSSID 与 SSID。SSID 是一个用户可配置的无线局域网逻辑名，而 BSSID 是硬件厂商提供的接入点的二层 MAC 地址。许多厂商也提供虚拟 BSSID 配置，第 10 章将对此进行介绍。

如图 7-8 所示，用于标识 BSS 的 BSSID 地址位于大多数 802.11 无线帧的帧头。BSSID 地址不仅用于 BSS 中的 802.11 流量转发，也是 BSS 唯一的二层标识符，还在漫游过程中起着重要作用。

```
802.11 MAC Header
  Version:                    0
  Type:                       %10  Data
  Subtype:                    %0000  Data Only
  Frame Control Flags=%00000010
  Duration:                   213  Microseconds
  Destination:                00:02:2D:74:67:2A
  BSSID:                      00:0C:85:62:D2:1D
  Source:                     00:0C:85:62:D2:1D
  Seq Number:                 1653
  Frag Number:                0
```

图 7-8 基础服务集标识符(BSSID)

7.2.9 基本服务区

在 BSS 中，接入点实际覆盖的区域称为基本服务区(Basic Service Area，BSA)，如图 7-9 所示。只要无线接口接收到的信号强度在 RSSI(接收信号强度指示器)阈值之上，就能确保客户端在整个覆盖区域内移动而不会失去与接入点的连接。位于基本服务区内的客户端还可以在不同的数据速率之间进行切换，这称为动态速率切换(dynamic date switching)，第 12 章将对此进行介绍。

图 7-9　基本服务区(BSA)

接入点发射功率、天线增益、物理环境等许多因素都会影响基本服务区的尺寸和形状。由于周围环境经常会发生变化，基本服务区的形状并非总是固定不变的。

7.2.10　扩展服务集

如果将 BSS 比作 802.11 拓扑结构的基石，那么 ESS(Extended Service Set，扩展服务集)就是由基石垒成的整座大厦。ESS 由一个或多个 BSS 构成，BSS 之间通过分布系统介质连接在一起。一般而言，ESS 是若干接入点和与之建立关联的客户端的集合，所有设备通过单一的分布系统介质(DSM)相连。

如图 7-10 所示，最常见的 ESS 由多个接入点构成，接入点的覆盖小区之间部分重叠，以实现客户端的无缝漫游。大部分厂商建议，小区之间的重叠面积至少应保持在 15%～25%以上。

图 7-10　扩展服务集(ESS)：无缝漫游

尽管无缝漫游是无线局域网设计中需要重点考虑的因素之一，然而保证不间断通信并不是 ESS 必须满足的条件。例如，ESS 可以由若干个接入点构成，这些接入点的覆盖小区之间不存在任何重叠，如图 7-11 所示。在这种部署中，客户端离开第一个接入点所在的基本服务区时将暂时失去连接，并在进入第二个接入点的覆盖范围后重新建立连接。这种客户端在非重叠小区之间移动的方式有时称为游动漫游(nomadic roaming)。

图 7-11 扩展服务集(ESS)：游动漫游

ESS 部署的第三个例子如图 7-12 所示，多个接入点的覆盖小区完全重合。这种 802.11 ESS 拓扑结构称为 colocation，其目的是增加客户容量。

图 7-12 扩展服务集(ESS)：colocation

需要注意，上述 3 种 ESS 共享同一分布系统。本章前面曾经介绍过，分布系统介质通常是 802.3 以太网，不过其他介质也可以作为分布系统介质。在大部分 ESS 中，所有接入点共享同一 SSID(无线局域网的逻辑名)。ESS 的网络名一般被称为 ESSID(extended service set identifier，扩展服务集标识符)。虽然 ESSID 与 SSID 本质上含义相同，但是 ESS 中的接入点不一定需要共享相同的无线局域网名。也就是说，与同一分布系统介质相连的多个接入点可能具有不同的 SSID，但是它们仍然属于同一个 ESS。需要注意的是，如果要求 ESS 支持漫游，则 ESS 中的所有接入点必须共享同一个逻辑名(SSID)，不过每个 BSS 覆盖蜂窝仍然可以使用自己的二层标识符(BSSID)。这种情况如图 7-13 所示。

图 7-13　ESS 中的 SSID 和 BSSID

7.2.11　独立基础服务集

802.11 标准定义的第三种服务集拓扑结构称为 IBSS(Independent Basic Service Set，独立基础服务集)。IBSS 中只存在客户端，不存在接入点。一个仅由两个客户端构成的 IBSS 相当于一条有线交叉电缆。IBSS 也可以由多个客户端构成，这些客户端位于同一物理区域，采用点对点(ad hoc)方式相互通信。图 7-14 显示了 4 个以对等方式进行通信的客户端。

图 7-14　独立基础服务集(IBSS)

在 IBSS 中，客户端将数据帧直接传输而非路由给其他客户端，即所有客户端的帧传输都是对等的。所有 IBSS 客户端必须竞争半双工介质的使用权，且在任意给定时间内，有且只有一个客户端可以传输数据。

除“独立基础服务集”之外，Wi-Fi 厂商还习惯将 IBSS 称为“对等网络”或“ad hoc 网络”。

为确保 IBSS 通信的成功，所有客户端必须使用同一信道收发数据。此外，构成 IBSS 的所有客户端必须共享同一个 SSID。还要注意，每个 IBSS 都会产生一个 BSSID 地址。本章

前面曾经介绍过，BSSID 定义为接入点无线射频卡的 MAC 地址。那么对于不存在接入点的 IBSS 拓扑结构而言，如何确定它的 BSSID 呢？这种情况下，第一个启动 IBSS 的客户端将以 MAC 地址的格式随机产生一个 BSSID，它是一种虚拟的二层 MAC 地址，用于标识 IBSS 的身份。

7.2.12 Mesh 基础服务集

802.11 标准很早就定义了 BSS、ESS 和 IBSS 服务集。最近批准的 802.11s-2011 为 802.11 mesh 拓扑定义了一种新的服务集。当 AP 支持 Mesh 功能时，它们可能部署在无法接入有线的网络。Mesh 提供网络流量的无线分布，并由提供 Mesh 基本服务的 AP 构建 MBSS。在 BSS、ESS 或 IBSS 要求的属性在 MBSS 中是不必要，因为 MBSS 的目的，与其他拓扑结构不同。如图 7-15 所示，一个或多个 Mesh AP 连接到有线基础设施(称为 Mesh Root、Mesh portal 或 Mesh Gate)，其他 Mesh AP 建立无线回传链路连接有线网络。Mesh BSS 功能更像网络中的路由器，即发现邻居 Mesh 节点，构建邻居关系和共享链接信息。请记住，802.11 帧在第二层交换，因此 802.11 流量在 Mesh 网络中的路由也是基于 MAC 地址的转发，而非 IP 地址。HWMP(混合无线 Mesh 协议)是 MBSS 的默认路径选择协议。还请注意，WLAN 厂商多年来一直使用私有的第二层 Mesh 协议。

图 7-15 Mesh 基础服务集(MBSS)

在上图上涉及的所有设备都会第 10 章找到详细资料。

真实场景

部署和集成 802.11 设备时应考虑的厂商问题

如果必须在非标准拓扑结构中部署 802.11 无线接口，则应尽量选购同一家厂商生产的设备，因为不同厂商的无线桥接设备可能不兼容，Mesh 产品也可能不兼容。由于拓扑结构尚未标准化，厂商互操作性将成为一个很大的问题。

802.11AP 的主要作用就是成为有线网络基础架构的入口设备。尽管 802.11 技术运行在第一层和第二层，但总归需要考虑高级层次的设计。每家 WLAN 厂商采用不同的策略融入已经存在的有线网络基础架构，所以采用同一家无线厂商的产品是最佳方法。

7.3　802.11 配置模式

802.11-2007 标准将所有无线接口都定义为终端(STA)，可以采用多种方式配置接入点和客户端的无线接口。通常将接入点配置在 BSS 中使用，不过也可以被配置在非标准拓扑结构中。客户端既可以配置在 BSS 中，也可以配置在 IBSS 中。

7.3.1　接入点模式

唯一符合 802.11 标准的接入点配置模式称为根模式(root mode)。在这种模式中，接入点主要作为接入分布系统的入口设备使用。根模式是接入点的默认配置模式，采用根模式的接入点在分布系统与 802.11 无线介质之间传输数据。并非所有的无线厂商对于这种模式有相同的叫法，例如许多厂商称之为 AP mode 而非 Root mode。

配置为根模式的接入点可在 BSS 中使用。此外，接入点也可以被配置为其他非标准模式：

网桥模式　接入点被转换为无线网桥。此时 AP 增加了额外的 MAC 层的功能，可以学习并维护到网络有线端的 MAC 地址。

工作组网桥模式　接入点被转换为工作组网桥。

中继器模式　接入点被转换为中继器接入点。

Mesh 模式　接入点作为 Mesh 环境中的无线回传设备，某些厂商还支持无线回传接口连接无线客户端。

扫描模式　接入点无线接口被转换为探测器，此时接入点属于 WIDS(无线入侵检测系统)架构的一部分。

上述几种配置都属于非标准模式，并非所有厂商都支持这些模式。这些模式都属于无线射频配置模式，可能 AP 的 2.4GHz 射频卡支持，也可能 5GHz 射频卡支持，也可能两者都支持。图 7-16 显示了一个接入点的各种配置模式。

图 7-16 接入点配置模式

7.3.2 客户端模式

客户端可以被配置为两种模式，如图 7-17 所示。默认的客户端配置模式称为基础架构模式(Infrastructure mode)。在这种模式中，客户端之间的通信必须通过接入点进行。配置为基础架构模式的客户端既可在 BSS 中使用，也可在 ESS 中使用。采用基础架构模式的客户端将数据交给接入点，并由接入点转发给 BSS 中的其他无线客户端。

客户端也可以通过接入点与分布系统中的其他网络设备(如服务器或台式机)进行通信。

第二种客户端配置模式称为点对点模式(Ad Hoc mode)，一些厂商也称其为对等模式(Peer-to-Peer mode)。配置为 Ad Hoc 模式的客户端用于 IBSS，客户端之间的通信无需通过接入点进行，所有数据传输与帧交换都是对等的。

图 7-17 客户端配置模式

7.4 小结

这一章介绍了常见的几种无线拓扑结构，并讨论了 802.11 无线局域网所用的拓扑结构：

- 各类无线技术使用的 4 种无线架构
- 802.11 标准定义的 4 种服务集以及每种服务集的作用和目的
- 接入点与客户端的标准和非标准配置模式

对无线网络管理员而言，必须深入理解 802.11 标准定义的各种服务集及其工作方式。虽然管理员一般负责 802.11 ESS 拓扑结构的规划与管理，但是他们也可能需要部署采用非标准拓扑结构的 802.11 无线接口。

7.5　考试要点

了解 4 种主要的无线拓扑结构。理解无线广域网(WWAN)、无线城域网(WMAN)、无线局域网(WLAN)和无线个人域网(WPAN)的差异。

解释 4 种 802.11 服务集。深入理解 BSS、ESS、IBSS 和 MBSS 的构成、用途和差异。理解无线射频卡在每种服务集中的通信方式。

理解 802.11 无线接口的各种用途。根据 802.11 标准的定义，无线射频卡既可以作为客户端使用，也可以在接入点内部使用。此外，802.11 无线射频卡还可以用于桥接、中继器等非标准拓扑结构。

解释分布系统的目的。了解分布系统由分布系统服务(DSS)与分布系统介质(DSM)两部分构成。理解任何介质都可以作为分布系统介质。解释无线分布系统(WDS)的功能。

定义 SSID、BSSID 和 ESSID。解释 3 种标识符的异同以及每种标识符的功能。

描述 ESS 的各种实现方式以及每种设计的用途。解释 3 种 ESS 部署以及每种部署的用途。

解释接入点与客户端配置模式。牢记接入点与客户端的所有标准和非标准配置模式。

7.6　复习题

复习题的答案见附录 A。

1. An 802.11 wireless network name is known as which type of address? (Choose all that apply.)

   A. BSSID

   B. MAC address

   C. IP address

   D. SSID

   E. Extended service set identifier

2. Which two 802.11 topologies require the use of an access point?

   A. WPAN

   B. IBSS

   C. Basic service set

   D. Ad hoc

   E. ESS

3. The 802.11 standard defines which medium to be used in a distribution system (DS)?

A. 802.3 Ethernet

B. 802.15

C. 802.5 token ring

D. Star-bus topology

E. None of the above

4. Which option is a wireless computer topology used for communication of computer devices within close proximity of a person?

A. WLAN

B. Bluetooth

C. ZigBee

D. WPAN

E. WMAN

5. Which 802.11 service set may allow for client roaming?

A. ESS

B. Basic service set

C. Colocated APs

D. IBSS

E. Spread spectrum service set

6. What factors might affect the size of a BSA coverage area of an access point? (Choose all that apply.)

A. Antenna gain

B. CSMA/CA

C. Transmission power

D. Indoor/outdoor surroundings

E. Distribution system

7. What is the default configuration mode that allows an AP radio to operate in a basic service set?

A. Scanner

B. Repeater

C. Root

D. Access

E. Nonroot

8. Which terms describe an 802.11 topology involving STAs but no access points? (Choose all that apply.)

A. BSS

B. Ad hoc

C. DSSS

D. Infrastructure

E. IBSS

F. Peer-to-peer

9. STAs operating in infrastructure mode may communicate in which of the following scenarios? (Choose all that apply.)

A. 802.11 frame exchanges with other STAs via an AP

B. 802.11 frame exchanges with an AP in scanner mode

C. 802.11 frame peer-to-peer exchanges directly with other STAs

D. Frame exchanges with network devices on the DSM

E. All of the above

10. What are the only three original topologies defined by the 802.11-2007 standard? (Choose all that apply.)

A. Bridge mode

B. Extended service set

C. BSS

D. IBSS

E. FHSS

11. Which wireless topology provides citywide wireless coverage?

A. WMAN

B. WLAN

C. WPAN

D. WAN

E. WWAN

12. At which layer of the OSI model will a BSSID address be used?

A. Physical

B. Network

C. Session

D. Data-Link

E. Application

13. The basic service set identifier address can be found in which topologies? (Choose all that apply.)

A. FHSS

B. IBSS

C. ESS

D. DSSS

E. BSS

14. Which 802.11 service set defines mechanisms for mesh networking?

A. BSS

B. DSSS

C. ESS

D. MBSS

E. IBSS

15. What method of dialog communications is used within an 802.11 WLAN?

A. Simplex communications

B. Half-duplex communications

C. Full-duplex communications

D. Dual-duplex communications

16. What are some nonstandard modes in which an AP radio may be configured? (Choose all that apply.)

A. Scanner

B. Root

C. Bridge

D. Nonroot

E. Repeater

17. A network consisting of clients and one or more access points with the same SSID connected by an 802.3 Ethernet backbone is one example of which 802.11 topology? (Choose all that apply.)

A. ESS

B. Basic service set

C. Extended service set

D. IBSS

E. Ethernet service set

18. What term best describes two access points communicating with each other wirelessly while also allowing clients to communicate through the access point?

A. WDS

B. DS

C. DSS

D. DSSS

E. DSM

19. What components make up a distribution system? (Choose all that apply.)

A. HR-DSSS

B. Distribution system services

C. DSM

D. DSSS

E. Intrusion detection system

20. What type of wireless topology is defined by the 802.11 standard?

A. WAN

B. WLAN

C. WWAN

D. WMAN

E. WPAN

第 8 章 802.11 媒介访问

在该章中，你将学习以下内容：

- √ CSMA/CA 与 CSMA/CD
  - 冲突检测
- √ 分布式协调功能(DCF)
  - 帧间间隔(IFS)
  - Duration/ID 字段
  - 载波侦听
  - 随机回退计时器
- √ 点协调功能(PCF)
- √ 混合协调功能(HCF)
  - 增强的分布信道访问(EDCA)
  - HCF 受控信道访问(HCCA)
- √ 块确认(BA)
- √ Wi-Fi 多媒体(WMM)
- √ 通话公平机制

本章的难点之一是：如果要了解无线终端如何获取媒介访问权限的概念，需要掌握许多CWNA 考试无需了解的知识细节。这些细节对于理解概念非常有用，尽管这些细节在 CWNA 考试中不会出现，但这些概念是考试需要掌握的。如果你对 802.11 通信本质的细节部分比较关注的话，你就应该考虑阅读由 David A. Westcott 和 David D. Coleman 等人所写的 *CWAP Certified Wireless Analysis Professional Official Study Guide：Exam PW0-270*)。如果决定参加 CWAP 考试，就需要知道远远超过本章所涵盖的知识，但现在只需理解无线终端访问半双工媒介的基础知识即可。

8.1 CSMA/CA 与 CSMA/CD

网络通信需要一套有效可控的网络媒介访问规则。媒介访问控制(MAC)是描述各种不同媒介访问方法时的一种通用术语。有许多媒介访问方式。早期的大型主机使用轮询方法，按顺序检查每一个终端有无数据需要处理。之后令牌传送和竞争的方法也被用于媒介访问。当前有两种媒介竞争访问形式被广泛应用：载波侦听多路访问冲突检测(CSMA/CD)和载波侦听多路访问冲突避免(CSMA/CA)。

大家可能都熟知的 CSMA/CD 用于以太网，但用于 802.11 网络的 CSMA/CA，知道的人估计不多。使用这两种访问方法的通信终端首先必须倾听是否有其他设备正在传输。如果有其他设备正在传输，该终端必须等待直到媒介可用再进行传输。CSMA/CA 与 CSMA/CD 在当某无线终端希望传输且没有其他终端传输时的处理方法有所不同。对 CSMA/CD 终端来说，此时它会立即开始传输。如果传输时发生冲突，客户端可以检测到并暂停传输。而 802.11 无线客户端因为没有同时进行传输和接收的能力，所以无法在传输时检测冲突，这也是为什么 802.11 无线网络使用 CSMA/CA 进行冲突避免，而不是利用 CSMA/CD 进行冲突检测的原因。

当 CSMA/CA 终端侦听到没有其他终端传输时，会等待一段随机的回退时间，然后再传输。在这段时间内，该终端会持续监控确保没有其他站点开始传输。因为射频媒介的半双工特性，非常有必要采用某种机制确保传输媒介在任何时间只有一个射频接口卡在占用。CAMA/CA 就是这种机制。但这个机制是否完美无瑕呢？答案是：一点也不。当两个或更多的无线电设备同时传输的时候，冲突仍会发生。IEEE 802.11-2007 标准定义了一种称为分布式协调功能(DCF)的媒介访问方法，利用其多重制衡机制减少冲突。我们也可以把这些相互制衡的机制想象成几道防线。部署各条防线的目的是希望能确保每次只有一个无线终端在传输而其他客户端处于倾听状态。CSMA/CA 机制在降低冲突风险的同时并未增加额外开销。

IEEE 802.11-2007 标准还定义了一种称为点协调功能(PCF)的可选机制，它允许无线接入点轮询客户端有无数据需要传输。IEEE 802.11-2007 标准还包含了一种用于指定高级服务质量(QoS)方法的混合协调功能(HCF)。

本章下一节将阐述更多细节。

CSMA/CA 复习

载波侦听(carrier sense)用来检测传输媒介是否繁忙。多路访问(multiple access)用来确保每一个无线终端可以进行公平的媒介访问(但每次只能有一个终端传输)。冲突避免(collision avoidance)意味着在指定时间内只有一个无线终端可以得到媒介访问能力，希望借此避免冲突。

8.2　冲突检测

在本章前面部分，我们提到 802.11 无线终端无法同时发送和接收数据，因此无法检测到冲突发生。如果无法检测冲突，那么又如何知道冲突发生？答案其实很简单。如图 8-1 描述那样，802.11 无线终端每传输一个单播帧，接收端会回复确认(ACK)帧以证明该帧被正确接收。

图 8-1　单播帧确认

大多数 802.11 单播帧必须得到确认。但广播和多播帧并不要求确认。如果单播帧遭到任何损坏，循环冗余校验(CRC)将会失败，无线接收端也不会回复 ACK 帧。如果发送端没有收到 ACK 帧，即单播帧未得到确认，该帧就不得不重传。

可这个过程并没有确定是否发生了冲突啊？换句话说，这个过程没有进行冲突检测。但如果发送端没有收到 ACK 帧，我们就假设冲突发生了。此时 ACK 帧被认为是无线帧成功交付的证据。如果没有确认传输成功的证据，发送端就假定传递失败，然后重传。

8.3　分布式协调功能(DCF)

分布式协调功能(DCF)是一种用于 802.11 通信的基本的媒介访问方法，它是一种 802.11 标准的强制访问方法。与 DCF 相对应的是另一种可选的 802.11 通信访问方法，称为点协调功能(PCF)，该方法会在本章后面部分介绍。第三种协调功能称为混合协调功能(HCF)，其融合了 802.11e 修正案的内容(802.11-2007 标准的一部分)，也会在本章后面部分介绍。在本节中，你还将了解到构成 CSMA/CA 进程的一些组件。下面是 DCF 的四个主要组成部分：

- 帧间间隔
- Duration/ID 域
- 载波侦听
- 随机回退计时器

这四部分作为制衡机制同时工作，以确保同时只有一个射频接口卡在半双工媒介中传输数据。

8.3.1 帧间间隔(IFS)

帧间间隔(IFS)是指无线帧传输之间的一段时间。有六种类型的帧间间隔，按间隔从最短到最长的时间排序如下：

- 减小的帧间间隔(RIFS)，优先级最高；
- 短帧间间隔(SIFS)，第二优先级；
- PCF 帧间间隔(PIFS)，中等优先级；
- DCF 帧间间隔(DIFS)，最低优先级；
- 仲裁帧间间隔(AIFS)，由 QoS 站使用；
- 扩展帧间间隔(EIFS)，用于重传的时间。

每个 IFS 的实际长度取决于网络的传输速度。IFS 是 CSMA/CA 用来确保在某种 IFS 后仅有某些类型的 802.11 帧可以传输。例如，在 SIFS 后只有 ACK 帧、数据帧、清除发送帧(CTS)可以传输。SIFS 和 DIFS 是最常见的两种帧间间隔。图 8-2 所示，ACK 帧是优先级最高的帧，SIFS 的使用可以确保 ACK 帧比任何其他类型的 802.11 帧都传递得早。大多数 802.11 帧都会等更长一段时间再传输，这段时间我们称为 DIFS。

图 8-2 SIFS 与 DIFS

帧间间隔决定了接下来哪种类型的 802.11 帧可以得到传输。另外它还充当了虚拟载波侦听机制的备份机制，见稍后的讨论。你需要了解帧间间隔的时间长度顺序：RIFS< SIFS < PIFS < DIFS < AIFS < EIFS。

通过进一步阅读本章，你会意识到时间在确保无线通信成功方面有多么重要。而帧间间隔只是这种紧密关系中的成员之一。

8.3.2 Duration/ID 字段

图 8-3 描述的是 Duration/ID 字段——802.11 的 MAC 头中的字段之一。当客户端发送单播帧时，Duration/ID 字段包含了一个位于 0 到 32 767 之间的数值。该图中，Duration/ID 表示

的时间值以微秒为单位，是指一个 ACK 帧加上一个 SIFS 间隔的时间，详见图 8-4。发送端会计算需要多长时间收到 ACK 帧，并把这个时间值置于发送的单播数据帧的 MAC 报头中的 Duration/ID 字段。ACK 帧 MAC 报头中的 Duration/ID 值为 0。简而言之，Duration/ID 值就表示射频媒介在其他无线终端角逐媒介访问权前要忙碌的时间。

```
802.11 MAC Header
  Version:                0
  Type:                   %10  Data
  Subtype:                %0000  Data Only
  Frame Control Flags=%00000010
  Duration:               213  Microseconds
  Destination:            00:02:2D:74:67:2A  Agere Sys:74:67:2A
  BSSID:                  00:00:85:62:D2:1D  Cisco:62:D2:1D
  Source:                 00:00:85:62:D2:1D  Cisco:62:D2:1D
  Seq Number:             1653
  Frag Number:            0
```

图 8-3　Duration/ID

图 8-4　SIFS+ACK 的 Duration 值

Duration/ID 字段主要用于重置其他终端的网络分配向量(NAV)计时器。但在少数情况下，节电轮询帧(PS-Poll)的 Duration/ID 字段被用来描述传统节电管理客户端的 ID 值(即 AID)。电源管理会在第 9 章中讨论。

8.3.3　载波侦听

802.11 CSMA/CA 设备在开始传输前执行的第一个动作就是载波侦听(Carrier Sense)。它是检查传输媒介是否被占用的方法。这有点类似于拨打电话时的忙音侦测。载波侦听有两种方式：虚拟载波侦听和物理载波侦听。

1. 虚拟载波侦听

虚拟载波侦听(Virtual Carrier Sense)使用的计时器机制称为网络分配向量(NAV)。NAV 计时器通过查看在前面传输的帧的 Duration 值来预测未来的流量。802.11 无线接口卡在传输前会进行侦听。如图 8-5 所示，当无线终端侦听到另一终端发送的帧时，会查看这个帧的报头部分，确定 Duration/ID 字段是否包含 Duration 或 ID 值。如果该字段为 Duration，监听终端将其 NAV 计时器设置为此值，然后开始进行倒计时，它将认为射频媒介在 NAV 值倒计至零之前都是繁忙的。

图 8-5 虚拟载波侦听

实质上，这一机制允许正在发送的 802.11 无线客户端通知其他客户端这段时间(Duration/ID 值)内媒介会被占用。没有传输的客户端听到 Duration/ID 值后设置倒计时计时器(NAV)，在该计时器倒数到零之前，这些客户端不会开始竞争传输媒介并传输数据；直到 NAV 计数器为 0 时，终端才会开始竞争媒介，如果终端的 NAV 为非零值，它也不会开始传输数据。如前所述，如果说 CSMA/CA 有几道防线用于防止冲突的话，第一道防线通常就是 NAV 计时器。

2. 物理载波侦听

虚拟载波侦听是当某无线终端控制媒介时，阻止其他终端传输的一种方法。不过，有可能因为无线终端没有听到其他无线设备正在传输，无法读取 Duration/ID 字段并设置 NAV 计时器。原因可能有多种，但目前我们暂时不关注它。这时 CSMA/CA 会利用另一道防线确保无线终端在其他终端传输时停止传输：*物理载波侦听*(physical Carrier-Sense)。

所有尚未开始传送或正在接收的无线站点会持续进行物理载体侦听。当某无线终端执行物理载波侦听时，实际上它会查看是否有任何其他无线发射机正在占用信道。

物理载波侦听有两个目的。第一个目的是确定是否有帧在进行入向传输以便接收。如果媒介繁忙，无线终端将尝试与该传输同步。第二个目的是确定在传输前媒介是否繁忙。这称为空闲信道评估(CCA)。空闲信道评估在物理层倾听 802.11 射频传输，确保传输前媒介必须空闲。

请务必了解虚拟载波侦听和物理载波侦听总是同时进行。虚拟载波侦听是位于 OSI 模型第二层的防线，而物理载波侦听是 OSI 模型第一层的防线。如果其中一道防线失效，无线传输会寄希望于其他防线可以阻止冲突发生。

8.3.4 随机回退计时器

802.11 无线终端可能在一段被称为竞争窗口(contention window)的时间范围内进行媒介访问权的争夺。在 CSMA/CA 进程中，无线终端会选择一个随机的回退计时器值。这个随机值

介于 0 与初始竞争窗口之间，如图 8-6 所示。回退值乘以时隙(slot time)得到的值就是随机回退计时器。时隙(Slot time)指的是一段时间，不同的扩频技术各不相同。随机回退计时器是无线终端帧传输之前使用的最后一个计时器，客户端的回退计时器开始倒计时。当时间倒计至零时，客户端会重新评估该信道是否空闲，如果信道空闲便开始传输。

图 8-6　竞争窗口时隙

随机回退计时器(Random Back-off Timer)是阻止冲突的另一道防线，它可以将终端同时进行通信的可能性降至最低，尽管这种情况无法完全阻止。如果无线终端没有收到 ACK，它会反复进行载波侦听进程。

8.4　点协调功能

除了 DCF，IEEE 802.11 标准还定义了一种可选的媒介访问方法——点协调功能(PCF)。这种访问方法采用轮询的形式。无线接入点执行点协调者(point coordinator)的功能。因为协调员的角色由无线接入点完成，所以 PCF 媒介访问方法只适用于基本服务集(BSS)，不可以用在无接入点存在的 Ad Hoc 网络。轮询由中心设备发起，因此 PCF 可以为媒介访问提供管理职能。

PCF 的使用要求接入点和无线终端都必须支持。启用 PCF 后，DCF 仍然可以正常工作。接入点可以在 PCF 与 DCF 模式间相互转换。接入点工作在 PCF 模式的时间称为无竞争期(contention-free period/CFP)。无竞争期间，接入点只会轮询那些打算发送数据且处于 PCF 模

式下的客户端。这是一种优先考虑某些客户端的方法。接入点工作在 DCF 模式的时间称为竞争期(contention period/CP)。

如果你想了解更多关于 PCF 的知识，建议你阅读 802.11-2007 标准文档，下载地址是 http://standards.ieee.org/about/get/802/802.11.html。

正如我们前面提到的，因为 PCF 是可选的访问方法，撰写本书时，我们还不知道哪家供应商的产品部署了这个机制。

8.5 混合协调功能

802.11e 服务质量修订案增加了一种新的 802.11 媒介竞争协调功能，称为混合协调功能(HCF)。802.11e 修订案和 HCF 已被合并纳入 802.11-2007 标准。HCF 结合了 DCF 和 PCF 的功能，对其进行增强，并创建了两种信道访问方法：增强的分布式信道访问(EDCA)和 HCF 控制信道访问(HCCA)。

前面讨论的 DCF 和 PCF 竞争机制允许 802.11 无线模块传输单个帧，传完这个帧后，它必须再次争夺媒介发送另一个帧。HCF 定义了 802.11 无线接口通过射频媒介连续发送多个帧的能力。当 HCF 兼容的无线终端在竞争媒介时，会被分配一段时间量用于发送帧。这段时间被称为传输机会(TXOP)。在 TXOP 期间，802.11 无线模块可以连续发送多个帧，称为帧突发(frame burst)。在帧突发期间，每个帧之间使用短帧间间隔(SIFS)，以确保没有其他无线终端进行传输。

8.5.1 增强的分布式信道访问

增强分布式信道访问(EDCA)是一种对 DCF 进行扩展的无线媒介访问方法，它使用八个用户优先级(user priority/UP)为无线终端提供差异化访问。EDCA 的媒介访问方法通过等同于 802.1D 优先级的标签对传递流量进行优先次序排列。优先级标签在 MAC 层提供一种机制用于实现服务质量(QoS)。

通过在以太网帧的帧头中添加代表用户优先级的三个比特位的 IEEE802.1Q 报头，使得可以区分不同的服务等级。802.1D 开启优先级队列(使在交换网络中某些以太网帧可以比其他帧优先转发)。图 8-7 描述了以太网侧的 802.1D 优先级标签将流量导入不同的访问队列。

EDCA 基于用户优先级(UP)定义了四个访问类别，优先级从最低到最高分别是 AC_BK (Backgroup)、AC_BE(Best Effort)、AC_VI(Video)和 AC_VO(Voice)。每个访问类别可以用一种 DCF 的增强版本来竞争传输机会(TXOP)，即增强的分布式信道访问功能(EDCAF)。具有最高优先级的访问类别的帧的随机回退值最小，因此更可能得到 TXOP。这一进程的具体细节超出了 CWNA 的考试范围。

图 8-7　EDCA 与 802.1D 优先级标签

8.5.2　HCF 控制信道访问

HCF 控制信道访问(HCCA)是一种无线媒介访问方法，利用具备 QoS 功能的集中协调者(也称为混合协调者 Hybrid coordinator/HC)来协调访问，这与 PCF 网络中的点协调者操作方法不同。HC 内置在无线接入点中，具有访问无线媒介更高的优先级，利用这种较高的优先级别，它可以将 TXOP 分配给自己或其他终端，提供有限时间的受控访问期(CAP)，在此期间进行无竞争的 QoS 数据传输。这一进程的具体细节超出了 CWNA 的考试范围。与 PCF 一样，撰写本书的时候，我们还不知道哪家供应商的产品部署了这个机制。

8.6　块确认

802.11e 修正案还引入了块确认(Block Acknowledgment/BA)机制，目前已经纳入 802.11-2007 标准。块确认通过将多个确认帧聚合成单一的确认帧来提高信道使用效率。目前存在两种块确认机制：立即块确认机制和延迟块确认机制。立即块确认机制设计用于低延迟流量，而延迟块确认机制更适于对延迟不敏感的流量。本书只讨论立即块确认机制。

图 8-8 中，原始发送端将一组 QoS 数据帧发送到接收端，并发送 BlockAckReq 帧请求对所有 QoS 数据帧进行确认。这组 QoS 数据帧由单一的块确认帧确认，而非单独进行确认。块确认帧中的某个位元用于表示所有接收到的数据帧的状态。如果只有一个帧受损，那么只有这个帧需要重传。块确认比传统的 ACK 机制更有效，减少了对无线媒介的竞争开销。

802.11n-2009 标准修正案对块确认机制的使用做了进一步的定义。在第 18 章中会有更详细的阐述。

图 8-8 立即块确认机制

8.7 Wi-Fi 多媒体

在 802.11e 修正案被采纳前，原始的 802.11 标准中没有恰当的 QoS 规程对时间敏感的应用程序(如无线语音 VoWiFi)的使用进行定义。语音、音频和视频等应用程序通信流量对延迟和抖动的容忍度很低，通常要求得到比标准通信数据更高的优先级。802.11e 修订案定义了在 IEEE802.11 无线局域网中满足时间敏感的应用程序 QoS 需求的第二层的媒介访问控制方法。Wi-Fi 联盟推出的 Wi-Fi 多媒体(WMM)认证是对应于 802.11e 修订案的子集。

真实场景

VoWiFi 与 QoS

当前的 WMM 是基于 802.11e 定义的 EDCA 机制制定的。Wi-Fi 联盟曾经提出一项基于 HCCA 的认证，被称为 WMM-SA(Scheduled Access/计划访问)，不过因为只有部分 VoWiFi 供应商对这项基于 HCCA 的机制感兴趣，这项 WMM-SA 认证实际上已经不存在了。在不久的将来，供应商是否支持 HCCA 机制仍然存在变数。此外，某些 VoWiFi 供应商还提供专有 QoS 和标准 WMM 两种解决方案。虽然这不是建议的做法，但我们还是能够经常看到使用专有 QoS 解决方案的 VoWiFi 供应商产品与使用 WMM 方案的另一个供应商产品在相同的无线局域网内共存。

因为 WMM 基于 EDCA 机制，802.1D 优先级标签被用来在以太网侧将流量导入四个访问类别优先级队列。WMM 认证为流量优先级别提供四个访问类别，见表 8-1。

表 8-1　WMM 访问类别说明

访 问 类 别	描　　述	802.1 D 标签
WMM 语音类别	最高的优先级。它允许多个并发的具有低延迟和收费的语音质量的 VoIP 流	7、6
WMM 视频类别	支持视频流量优先于其他数据流量传输。单一的 802.11g 或 802.11a 信道可以支持三到四路标清视频流或一路高清视频流	5、4
WMM 尽力传输类别	来自不能提供 QoS 功能的应用程序或设备的流量。这个流量不对延迟敏感，但长时间的延迟会造成影响，如互联网浏览流量	0、3
WMM 背景流量类别	没有严格的吞吐量或延迟要求的低优先级的通信流量。如包括文件传输和打印作业	2、1

Wi-Fi 联盟还定义了 WMM-PS(Power Save)认证。其通过先进的 802.11e 节电机制，提高了电池的续航能力。有关电源管理的详细内容，可在第 9 章中找到。802.11e 定义的 WMM 和 HCF 是极复杂的媒介访问方法，讲述这个主题可能要花费非常长的时间。

推荐的 Wi-Fi 联盟白皮书

关于 WMM，Wi-Fi 联盟有两份白皮书建议你阅读。可从在线资源 http://www.sybex.com/go/cwna3e 下载：

- Wi-Fi CERTIFIED for WMM—-Support for Multimedia Applications with Quality of Service in Wi-Fi Networks
- WMM Power Save for Mobile and Portable Wi-Fi CERTIFIED Devices

8.8　通话公平机制

802.11 的重要特征之一是它能够支持不同的数据速率。这使得旧技术仍然可以用于较新的设备通信，当设备远离接入点时，可以切换到较低数据速率，继续保持与接入点的通信。利用较低的速率对于 802.11 通信是必要的，但是也可能因此使网络的整体性能和工作在较高数据速率的设备受到影响。

802.11 是基于竞争的，每个无线设备都必须进行竞争通信媒介，传输后，继续返回竞争状态。当一个无线设备正在传输时，其他 802.11 无线设备必须等待。如果此时传输设备使用较高的数据速率，其他设备就不必等待太久。但如果它使用较低的速率，其他设备就不得不等待较长的时间。如果 802.11 无线设备按照一个非常慢的速率传输，比方说 1Mbps 和 2Mbps，对于高速率的无线设备来说就不得不忍受长时间等待所导致的媒介竞争开销。

图 8-9 可以有助于理解这一点。图的上部分表示两个站正常发送 8 个帧的情况。其中一个站按高数据速率发送 8 个帧，另一个站按照低速率发送 8 个帧。如果高低速率设备处于相同的无线局域网，它们就需要竞争传输。换句话说，尽管一个站可按更高的速率发送，两个站访问媒介的次数是相同的，对于高速率的站也没有得到更多的访问介质的待遇。最终两个站完成 8 个帧的传输时间是相同的。

图 8-9 通话公平机制案例

通话公平机制的目的不是为设备分配相同的访问机会，而是分配相同的访问时间，进行更好的 RF 媒介的访问时间管理。图 8-9 的下半部分，是在开启通话公平的情况下，你可以看到数据速率更高的传输站比数据速率低的传输站优先级拥有更高的优先待遇。因为不必保持空闲等待低数据速率传输，传输时间可以得到更好的管理。大家注意到，更快的站在更短的时间内传完 8 个帧，慢的站按跟以前一样的时间传完 8 个帧。通过降低等待时间，通话公平机制有效地达到了更好进行媒介时间管理的目的。

目前还没有 802.11 标准或者修订案定义通话公平机制和其实现机制，也没有要求供应商进行部署。大多数供应商只在从 AP 到客户端的下行链路部署通话公平机制。通话公平机制通常用来为从 AP 发送给高数据速率用户提供更高的优先级。至少有一家供应商宣称他们也提供上行流量的通话公平机制。供应商实现通话公平机制的解决方案都是专有的，但即便如此，他们都秉承一个目的：防止低速率设备占用媒介导致网络陷入停顿。

虽然每个 WLAN 供应商采用各自的方法来实现通话公平机制，但通常都是通过分析下行流量，基于当前吞吐量、客户端数据速率、SSID 和距离 AP 的距离分配不同的权重。采用某种算法来处理这些信息并确定每个客户端下行的传输机会。如果部署得当，通话公平机制可以更好地利用媒介，为高数据速率用户提供更优先的访问。

8.9 小结

本章重点介绍 802.11 的媒介访问。每个无线终端都有权进行通信，无线媒介的访问控制管理通过媒介访问控制方法进行控制。我们总结了 CSMA/CD 和 CSMA/CA 两种竞争方式的区别。CSMA/CA 使用分布式协调功能的伪随机竞争方法。DCF 使用四道防线来确保同时只有一个 802.11 无线接口在半双工媒介上进行传输。

我们还讨论了可选的无竞争协调方法(点协调功能)。802.11e 服务质量修订案添加了新的协调功能，称为混合协调功能(HCF)。介绍了由 Wi-Fi 联盟提出的 Wi-Fi 多媒体(WMM)认证，其是 802.11e 修正案的标准子集。WMM 旨在满足运行在 IEEE 802.11 之上对时间敏感的应用

程序(如音频、视频和语音)的 QoS 要求。

通话公平是供应商用来为传输更快的设备提供更好访问待遇的一种方法。

8.10　考试要点

了解 CSMA/CA 和 CSMA/CD 的异同。理解两种访问方法，并了解其异同。

定义 CSMA/CA 的 4 个制衡机制与 DCF。了解虚拟载波侦听、物理载波侦听、帧间间距和随机回退计时器等 4 个制衡机制，共同确保同时只有一个 802.11 无线终端在半双工媒介中传输帧。

定义虚拟和物理的载波侦听。理解两种载波侦听的基本机制和目的。

解释 DCF 和 PCF。定义分布式协调功能与点协调功能的基本操作。

定义 HCF 的服务质量机制。混合协调功能定义了在 EDCA 中 TXOP 和访问类别的使用方式，以及在 HCCA 中 TXOP 和轮询的使用方式。

了解 Wi-Fi 多媒体(WMM)认证和它对现在与未来的重要性。WMM 旨在为 802.11 无线网络提供服务质量功能。WMM 是 802.11e 修正案的标准镜像子集。WMM 目前通过四个访问类别提供流量优先级。

了解通话公平机制的重要性及工作原理。通话公平机制为高数据速率设备提供访问媒介的高优先级。这种优先待遇为所有的设备提供相等的访问时间，达到平等共享可用传输带宽的目的。

8.11　复习题

复习题的答案见附录 A。

1. DCF is also known as what? (Choose all that apply.)
   A. Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
   B. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
   C. Data Control Function
   D. Distributed Coordination Function
2. 802.11 collision detection is handled using which technology?
   A. Network allocation vector (NAV).
   B. Clear channel assessment (CCA).
   C. Duration/ID value.
   D. Receiving an ACK from the destination station
   E. Positive collision detection cannot be determined.
3. ACK and CTS-to-self frames follow which interframe space?
   A. EIFS
   B. DIFS

C. PIFS

D. SIFS

E. LIFS

4. The carrier sense portion of CSMA/CA is performed by using which of the following methods? (Choose all that apply.)

A. Virtual carrier sense

B. Physical carrier sense

C. Channel sense window

D. Clear channel assessment

5. After the station has performed the carrier sense and determined that no other devices are transmitting for a period of a DIFS interval, what is the next step for the station?

A. Wait the necessary number of slot times before transmitting, if a random back-off value has already been selected.

B. Begin transmitting.

C. Select a random back-off value.

D. Begin the random back-off timer.

6. If PCF is implemented, it can function in which of the following network environments? (Choose all that apply.)

A. Ad hoc mode

B. BSS

C. IBSS

D. Infrastructure mode

E. BSA

7. Which of the following terms are affiliated with the virtual carrier-sense mechanism? (Choose all that apply.)

A. Contention window

B. Network allocation vector

C. Random back-off time

D. Duration/ID field

8. The goal of allocating equal time as opposed to equal opportunity is known as what?

A. Access fairness

B. Opportunistic media access

C. CSMA/CA

D. Airtime fairness

9. CSMA/CA and DCF define which mechanisms to ensure that only one 802.11 radio can transmit on the half-duplex RF medium? (Choose all that apply.)

A. Random back-off timer

B. NAV

C. CCMP

D. CCA

E. Interframe spacing

10. The Wi-Fi Alliance certification called Wi-Fi Multimedia (WMM) is based on which media access method defined by the 802.11-2007 standard?

A. DCF

B. PCF

C. EDCA

D. HCCA

E. HSRP

11. Hybrid Coordination Function (HCF) defines what allotted period of time in which a station can transmit multiple frames?

A. Block acknowledgment

B. Polling

C. Virtual carrier sense

D. Physical carrier sense

E. TXOP

12. Currently, WMM is based on EDCA and provides for traffic prioritization via which of the following access categories? (Choose all that apply.)

A. WMM Voice priority

B. WMM Video priority

C. WMM Audio priority

D. WMM Best Effort priority

E. WMM Background priority

13. The 802.11e amendment (now part of the 802.11-2007 standard) defines which of the following medium access methods to support QoS requirements? (Choose all that apply.)

A. Distributed Coordination Function (DCF)

B. Enhanced Distributed Channel Access (EDCA)

C. Hybrid Coordination Function (HCF)

D. Point Coordination Function (PCF)

E. Hybrid Coordination Function Controlled Access (HCCA)

14. What information that comes from the wired side network is used to assign traffic into access categories on a WLAN controller?

A. Duration/ID

B. 802.1D priority tags

C. Destination MAC address

D. Source MAC address

15. What are the two reasons that 802.11 radios use physical carrier sense? (Choose two.)

A. To synchronize incoming transmissions

B. To synchronize outgoing transmissions

C. To reset the NAV

D. To start the random back-off timer

E. To assess the RF medium

16. What CSMA/CA mechanism is used for medium contention? (Choose all that apply.)

A. NAV

B. CCA

C. Random back-off timer

D. Contention window

17. Which field in the MAC header of an 802.11 frame resets the NAV timer for all listening 802.11 stations?

A. NAV

B. Frame control

C. Duration/ID

D. Sequence number

E. Strictly ordered bit

18. The EDCA medium access method provides for the prioritization of traffic via priority tags that are identical to the 802.1D priority tags. What are the EDCA priority tags known as?

A. TXOP

B. UP levels

C. Priority levels

D. Priority bits

E. PT

19. ACKs are required for which of the following frames?

A. Unicast

B. Broadcast

C. Multicast

D. Anycast

20. What QoS mechanism can be used to reduce medium contention overhead during a frame burst of low-latency traffic?

A. Delayed Block ACK

B. Contention period

C. Contention window

D. Contention-free period

E. Immediate Block ACK

第 9 章 802.11 MAC 架构

在该章中，你将学习以下内容：

- √ 数据包、帧、比特
- √ 数据链路层
  - MAC 服务数据单元(MSDU)
  - MAC 协议数据单元(MPDU)
- √ 物理层
  - PLCP 服务数据单元(PSDU)
  - PLCP 协议数据单元(PPDU)
- √ 802.11 与 802.3 互操作
- √ 802.11 帧类型
  - 管理帧
  - 控制帧
  - 数据帧
- √ 信标管理帧(beacon)
- √ 被动扫描
- √ 主动扫描
- √ 身份认证
  - 开放式系统认证
  - 共享密钥认证
- √ 关联(Association)
- √ 认证状态与关联状态
- √ 基本速率与支持速率
- √ 漫游
- √ 重关联(Reassociation)
- √ 解除关联(Disassociation)

- √ 解除认证(Deauthentication)
- √ 确认帧
- √ 分片(Fragmentation)
- √ 保护机制(Protection mechanism)
- √ 请求发送/清除发送(RTS/CTS)
- √ 自主 CTS(CTS-to-Self)
- √ 数据帧(Data frame)
- √ 电源管理(Power management)
  - 主动模式(Active mode)
  - 节电模式(Power Save mode)
  - 流量指示图(TIM)
  - 传输流量指示消息(DTIM)
  - 通告流量指示消息(ATIM)
  - WMM 节电与非计划自动节电传输(WMM-PS 与 U-APSD)
  - 802.11n 电源管理
- √ 频段引导(Band Steering)

本章介绍 802.11MAC 体系结构的所有组件。我们会讨论上层信息如何进行 802.11 帧的封装、802.11 帧的三种类型和主要子类型。我们还会讨论了很多在 MAC 层完成的功能(如主动扫描)及完成这些功能所需的特定 802.11 帧。802.11 ERP 保护机制常常被误解，本章也会介绍 802.11b 和 802.11g 无线终端共存时所使用的 RTS/CTS 和 CTS-to-Self 保护机制。接近最后的时候，会讨论传统的 802.11 电源管理和增强的 WMM-PS 电源管理，最后章节会解释频段引导。

9.1　数据包、帧和位

了解任何技术，偶尔都需要回顾一下基础知识。当问题变得困难和复杂的时候，专注于第一优先要素是很重要的。例如，对于驾驶飞机来说，主要目标就是让它飞起来。而导航和通信对于让飞机飞起来这个主要目标来说就是次要的。处理复杂技术的时候，很容易忽略主要目的，对于 802.11 通信来说也是如此。802.11 通信的主要目标就是在计算设备之间传递用户数据。

当数据在计算机间传递的过程中，它从 OSI 模型上层逐步向下移至物理层，最终在物理层被转移到其他设备。例如，用户需要将一份 Word 文档拷贝到另一台计算机的共享磁盘。该文档从应用层初步向下至物理层，在物理层被传输到另一台计算机，然后在那台计算机上按逆向顺序再返回到 OSI 模型的应用层。

数据按 OSI 模型传输时，每层都将在该数据上添加报头信息。这使得它被另一台计算机接收时可以重新组合数据。在网络层，来自 4～7 层的数据被添加 IP 报头。第 3 层的 IP 数据包封装了来自更高层的数据。在数据链路层，IP 数据包被封装在帧(frame)内并增加了 MAC 报头。最终，当帧到达物理层时，会被增加携带大量信息的物理层(PHY)报头。

最终在物理层，数据将按比特格式传输。比特(bit)是一个二进制数字，值为 0 或 1。二进制是数字通信的基本单位。1 字节等于 8 比特。

本章会从 802.11 的角度，探讨上层信息是如何在 OSI 模型中向下移动并通过数据链路层和物理层传输的。

9.2　数据链路层

802.11 数据链路层分为两个子层。上层是 IEEE802.2 逻辑链路控制(LLC)子层，这与所有基于 802 的网络完全相同，尽管并非所有的 IEEE802 网络都使用 LLC。数据链路层底层是媒介访问控制(MAC)子层，这点与所有基于 802.11 的网络是相同的。802.11 标准主要定义了 MAC 子层的操作功能。

9.2.1　MAC 服务数据单元

网络层(第 3 层)将数据发送到数据链路层，数据被移交给 LLC 后即成为所谓的 MAC 服务数据单元(MSDU)。MSDU 包含 LLC 和第 3 层～第 7 层的数据，简单来说，就是包含 IP 数

据包和一些 LLC 数据的数据净荷部分。

本章后面部分会讲述三种 802.11 帧类型。802.11 管理帧和控制帧不携带上层信息。只有 802.11 数据帧携带 MSDU 净荷。802.11-2007 标准规定 MSDU 的最大值为 2 304 字节。帧主体的最大值等于 MSDU 的最大值与用于加密的开销的总和。在 802.11n-2009 修正案中，引入了聚合 MAC 服务数据单元(A-MSDU)的概念。如果使用 A-MSDU，依赖于客户端的能力，帧主体的最大值等于最大的 A-MSDU(3839 或 7935 字节)与用于加密的开销的总和。在第 18 章中，你将学习到更多关于 A-MSDU 的知识。

9.2.2 MAC 协议数据单元

LLC 将 MSDU 发送到 MAC 子层后，需要给 MSDU 增加 MAC 报头信息。被封装后的 MSDU 称为 MAC 协议数据单元(MPDU)，它其实就是 802.11 帧，如图 9-1 所示，它包含第 2 层(数据链路层)报头、帧主体和帧尾。帧尾是 32 比特的 CRC 值，也被称为帧校验序列(FCS)。802.11MAC 报头的更多细节会在本章后面详细阐述。

图 9-1 802.11 MPDU

此时，帧已经做好传输到物理层的准备，物理层会为帧传输做进一步的准备工作。

9.3 物理层

与数据链路层相似，物理层也被分为两个子层。上层被称为物理层汇聚协议(PLCP)子层，较低层部分称为物理媒介相关(PMD)子层。PLCP 为传输数据帧做好准备，将 MAC 子层的帧变成 PLCP 协议数据单元(PPDU)。PMD 子层进行数据调制处理并按比特方式进行传输。

9.3.1 PLCP 服务数据单元

当你站在某扇门边上时，这扇门有可能是入口或者出口，这取决于你站在门的哪一边。但不管怎样，它是同一扇门。物理层的 PLCP 服务数据单元(PSDU)就是 MAC 层的 MPDU，它们的区别就在于 OSI 模型不同层次的观察角度。

9.3.2 PLCP 协议数据单元

PLCP 接收到 PSDU 后，准备要传输的 PSDU 并创建 PLCP 协议数据单元(PPDU)。PLCP 将前导部分和 PHY 报头添加到 PSDU 之上。前导部分用于同步 802.11 无线发射和接收射频

接口卡。前导部分和 PHY 报头的细节超出了本书和 CWNA 的考试范围。创建 PPDU 后，PMD 子层将 PPDU 调制成数据位后开始传输。

图 9-2 描绘了上层信息向下移动到数据链路层和物理层的流程图。

图 9-2　数据链路层与物理层

9.4　802.11 和 802.3 互操作性

通过第 7 章的学习，你知道 802.11-2007 标准定义了一种集成服务(IS)，可以使 MSDU 通过门户在分布系统(DS)与非 IEEE802.11 局域网(LAN)之间传递。集成服务更简单定义是帧格式的传输方法。门户通常是指自治性无线 AP 或 WLAN 控制器。如前所述，无线 802.11 数据帧净荷被称为 MSDU，携带了第 3 层～第 7 层信息。这个净荷的最终目的地通常是网络基础设施的有线一侧。因为有线基础设施的物理媒介不同，802.11 数据帧的有效净荷(MSDU)必须被有效地转换成 802.3 以太网帧。例如，VoWiFi 电话机向自治性 AP 发送 802.11 数据帧，帧的 MSDU 净荷部分就是最终目的地为处于网络有线部分的 VoIP 服务器的 VoIP 报文。IS 负责首先删除 802.11 标头和尾部，然后将 MSDU 净荷打包到 802.3 以太网帧中。通常情况下，IS 在 802.11 和 802.3 媒介之间传递帧净荷。不过，集成服务也可以在 802.11 媒介和其他媒介(如蜂窝电话数据网络)之间传输 MSDU。所有的 IEEE 802 帧格式具有相似的特征，802.11 帧也不例外。因为帧很相似，当帧在 802.11 无线网络和 802.3 有线网络之间传递时很容易被转换，反之亦然。

802.3 以太网帧和 802.11 无线帧差异之一是帧的长度。802.3 帧在 MSDU 为最大值 1500 字节时的最大长度是 1518 字节。如果 802.3 帧因为 VLAN 和用户优先级的需要增加了 802.1Q 标记，这时 802.3 帧的最大长度为 1522 字节，数据净荷为 1504 字节。你刚刚学到，802.11 帧能够传输 MSDU 为 2304 字节的上层(upper-layer)数据。这意味着当数据在无线和有线网络之间传递时，无线 AP 可能会收到一些对有线网络来说显得过大的数据帧。不过，由于 TCP/IP 协议簇的某些要求，这种情况很少发生。作为网络使用中最常见的通信协议簇，TCP/IP 通常

要求 IP 最大传输单元(MTU)为 1500 字节。基于 MTU 的 IP 数据包通常为 1500 字节。当 IP 数据包传递到 802.11 时，尽管 MSDU 的最大长度为 2304 字节，但还是会受限于 IP 数据包的 1500 字节。

802.3 和 802.11 帧之间的另一个区别是 MAC 地址字段。802.3 帧在第二层头中只有源地址(SA)和目标地址(DA)。而如图 9-3 所示，802.11 帧在 MAC 头中可以有四个地址字段，通常只使用其中的三个 MAC 地址字段。但是，正如第 7 章讨论的那样，在 802.11 无线分布系统(WDS)内发送的帧包含四个 MAC 地址字段。这四个字段的内容可能包括以下类型的 MAC 地址：接收者地址(RA)、发送者地址(TA)、基本服务设置标识符(BSSID)、目标地址(DA)和源地址(SA)。有些帧可能不包含某些 MAC 地址字段。尽管地址字段的数量不同，802.3 和 802.11 帧都有源地址和目标地址，并使用相同的 MAC 地址格式。前三个八位组被称为组织唯一标识符(OUI)，最后三个八位组被称为扩展标识符。

图 9-3 802.11MAC 报头

如果要深入了解 802.11 帧格式，建议阅读 CWAP Certified Wireless Analysis Professional Official Study Guide: Exam PW0-270(Sybex, 2011)。阐述 802.11MAC 报头中每个字段的功能已经超出了 CWNA 的考试范畴。但是我们要了解其中一个非常重要字段，即 Duration/ID 字段，我们已经在第 8 章讨论过它的功能，发送端的 MAC 帧报头中的 Duration 值用来重置其他正在监听的终端的 NAV 计时器。

9.5 三种 802.11 帧类型

与许多有线网络标准(如 IEEE 802.3)使用单一的数据帧类型不同，IEEE 802.11 标准定义了三种主要的帧类型：管理帧、控制帧和数据帧。这些帧类型被进一步划分为多种子类型。在第 8 章中，你了解到有可选的媒介访问方法(点协调功能)和基于服务质量的媒介访问方法(混合协调功能)。某些帧的子类型与 PCF 功能相关，但 PCF 功能是可选的，至今也没有支持这种技术的无线 AP。那些只用于 PCF 的子类型我们会在旁边声明“PCF only”，用于 QoS 的 HCF 帧的子类型我们会在旁边标识“HCF”，本书不会对它们进行解释或定义。

9.5.1 管理帧

802.11 管理帧(Management Frame)在 WLAN 帧类型中占据了多数。无线终端加入或离开基本服务集(BSS)时会使用管理帧。有线网络不需要管理帧，它可以通过物理连接电缆或断开网络电缆执行这项功能。然而，无线网络是一种无线媒介，为了接入有线网络(分布系统)，

无线终端有必要首先找到与其兼容的无线局域网(假设它们被允许连接)，然后进行无线局域网认证，最后与无线局域网关联(通常与无线 AP)。

802.11 管理帧的另一个名称是管理 MAC 协议数据单元(MMPDU)。管理帧不携带任何上层信息。MMPDU 帧主体不包含 MSDU，只有第 2 层信息字段和信息元素。在管理帧主体中，信息字段(Information field)的长度是固定，信息元素(Information element)的长度是可变的。

下面列出了 802.11 标准和修订案中定义的所有 14 种管理帧子类型：

- Association request
- Association response
- Reassociation request
- Reassociation response
- Probe request
- Probe response
- Beacon
- Announcement traffic indication message (ATIM)
- Disassociation
- Authentication
- Deauthentication
- Action
- Action No ACK
- Timing advertisement

9.5.2　控制帧

802.11 控制帧(Control Frame)按照基本速率(basic rate)传输，用来协助数据帧交付。控制帧还可以用于清除信道、请求信道，并对单播帧进行确认。它们只包含报头信息。

下面列出了 802.11 标准定义的所有 9 种控制帧子类型：

- Power Save Poll(PS-Poll)
- Request to send (RTS)
- Clear to send (CTS)
- Acknowledgment (ACK)
- Contention Free-End(CF-End)
- CF-End + CF-ACK
- Block ACK Request [BlockAckReq]
- Block ACK [BlockAck]
- Control wrapper

9.5.3　数据帧

大部分 802.11 数据帧(Data Frame)都携带来自高层协议的数据，3～7 层的 MSDU 净荷通

常出于数据私密的要求被加密。然后仍然有些数据帧不携带任何数据，它们的存在是为了在 BSS 内进行特殊的媒介访问控制。不包含 MSDU 的数据帧不必加密，因为 3～7 层的数据净荷不存在。数据帧子类型共有 15 种，但 CWNA 考试只要求你对数据子类型有所了解并知道 null 数据帧子类型即可。数据帧子类型通常指的是简单数据帧(simple data frame)。这种简单数据帧在帧主体部分封装了 MSDU 上层信息。内置在自治型 AP 和 WLAN 控制器的 IS 会处理这种简单数据帧中的 MSDU 净荷，并将 MSDU 转成 802.3 以太帧。无线客户端有时会使用 Null 帧向无线 AP 通告其节电状态的变化。

下面列出由 802.11 标准定义的所有 15 种数据帧子类型：

- Data (simple data frame)
- Null function (no data)
- Data + CF-ACK [PCF only]
- Data + CF-Poll [PCF only]
- Data + CF-ACK + CF-Poll [PCF only]
- CF-ACK (no data) [PCF only]
- CF-Poll (no data) [PCF only]
- CF-ACK + CF-Poll (no data) [PCF only]
- QoS Data [HCF]
- QoS Null(no data)[HCF]
- QoS Data + CF-ACK [HCF]
- QoS Data + CF-Poll [HCF]
- QoS Data + CF-ACK + CF-Poll [HCF]
- QoS CF-Poll(no data)[HCF]
- QoS CF-ACK + CF-Poll(no data)[HCF]

9.6 信标管理帧

信标管理帧(Beacon management frame)是最重要的无线帧类型之一，通常也称为信标(Beacon)。Beacon 本质上可以认为是无线网络的心跳。基本服务集(BSS)中无线 AP 发送 Beacon，而客户端侦听 Beacon。客户端只会在加入独立基本服务集(IBSS)(也称为 Ad Hoc 模式)时才发送 Beacon。每个信标包含一个时间戳，客户端用它来保持与无线 AP 的时钟同步。成功的无线通信大多依赖于时序，因此确保所有通信终端互相保持同步非常必要。完成练习 9-1 后，你将可以使用数据包分析软件来分析信标帧的内容。信标帧主体包含了如下一些内容：

- Time Stamp(时间戳)：携带同步信息
- Spread spectrum parameter set(扩频参数集)：指 FHSS、DSSS、ERP、OFDM 或 HT 特定信息
- Channel information(信道信息)：AP 或 IBSS 使用的信道
- Data rates(数据率)：指基本速率和支持速率
- Service set capabilities(服务集能力)：额外 BSS 或 IBSS 参数

- SSID(服务集标识)：逻辑无线局域网名称
- Traffic indication map/TIM(流量指示图)：是节电进程使用的字段
- QoS capabilities(QoS 能力)：服务质量和 EDCA 信息
- Robust Security Network capabilities(RSN 能力)：TKIP 或 CCMP 加密信息和认证方法
- Vendor proprietary information(供应商私有信息)：供应商独有或厂商特定信息

信标帧包含了客户端加入 BSS 之前需要了解的所有必要信息。信标帧大约每秒传输 10 次左右。在某些 AP 上可以配置信标帧的发送间隔，但不能禁用它。

练习 9.1

观察 Beacon 帧

(1) 通过本书的在线资源 www.sybex.com/go/cwna3e 下载 CWNA-CH9.PCAP 文件。

(2) 等文件下载之后，用数据包分析软件打开。如果没有安装数据包分析软件，可以通过 www.wireshark.org 下载 Wireshark。

(3) 打开 CWNA-CH9.PCAP 文件。大多数的数据包分析软件都会在屏幕上半部分列出捕获帧。第一列是每个数据帧的编号，编号按顺序排列。

(4) 单击前八个帧中的一个。这些帧都是信标帧。

(5) 选择一个信标帧之后，在屏幕的较下部分，可以遍历信标帧主体的信息，并且可以单击加号扩展显示。

9.6.1　被动扫描

客户端在连接到 AP 之前，首先必须发现它。客户端可以有两种方式：被动扫描或主动扫描。在被动扫描中，客户端通过侦听 AP 不断发送的信标帧来发现 AP。如图 9-4 所示。

图 9-4　被动扫描

客户端将侦听媒介中是否有与客户端软件实用程序配置了相同 SSID 的信标帧。一旦无线客户端听到该信标帧，便可以尝试连接发送信标帧的无线局域网。如果客户端侦听到多个

具有相同 SSID 的 AP 信号，它会尝试关联信号最好的无线 AP。

请务必了解主动扫描和被动扫描可以共存于一个网络。无线站点就可以用其中一种办法扫描发现网络，也可以两者都用。此外在 IBSS 模式下，因为没有 AP，处于点对点模式中的所有客户端会轮流发送信标。在这种 IBSS(Ad Hoc)模式下的被动扫描连接方式与 BSS 模式完全相同。

9.6.2 主动扫描

除了通过被动扫描，客户端还可以通过主动扫描(active scanning)发现无线 AP。在主动扫描中，客户端发送被称为探询请求(Probe request)的管理帧。这些探询请求帧可以包含客户端正在寻找的特定无线局域网的 SSID，也可以用来查看当前环境中所有无线局域网的 SSID。客户端发送 SSID 字段为 null 的探询请求帧可以探测到网络中所有无线局域网的 SSID。包含特定 SSID 信息的探询请求帧被称为定向探询请求(directed probe request)。不包含 SSID 信息的探询请求帧被称为空探询请求(null probe request)。

客户端发出定向探询请求后，支持这个特定 SSID 的所有 AP 收到请求后，通常会回复探询响应(probe response)。探询响应帧的主体所包含的信息与信标帧几乎完全相同，除了字段流量指示图(TIM)外。就像信标帧一样，探询响应帧也包含了所有客户端加入 BSS 前必须要了解的 BSS 信息。

如果发送空探询请求，所有听到请求的 AP 都应该回复探询响应，如图 9-5。

图 9-5 主动扫描

被动扫描的一个缺点就是信标帧只会在与无线 AP 相同的信道上广播。而客户端发起的主动扫描与此相反，它会在所有可用的信道上发送探询请求帧。如果一个客户端接收来自多个 AP 的探询响应，通常客户端会通过比较信号强度和信号质量来决定要连接到哪个信号最佳的 AP。客户端会按顺序在每个支持的信道上发送探询请求。事实上，即使已经关联到 AP 并正在传输数据的客户端通常也会每隔几秒在其他信道上发送探询请求。通过持续的主动扫描，客户端可以维护并更新其已知 AP 列表，如果此时客户端需要漫游，通常也会更加快捷高效。

不同厂商的客户端每秒钟进行主动的信道外(off-channel)扫描的次数是各自不同的。例如，VoWiFi 电话的 802.11 射频模块就可能比笔记本电脑的 802.11 射频模块更频繁地发送信道外的探询请求。完成练习 9.2 后，将可以看到探询请求和探询响应帧。

练习 9.2

理解探询请求帧和探询响应帧

(1) 通过本书的在线资源 www.sybex.com/go/cwna3e 下载 CWNA-CH9.PCAP 文件。

(2) 等文件下载之后，用数据包分析软件打开。如果没有安装数据包分析软件，可以通过 www.wireshark.org 下载 Wireshark。

(3) 打开 CWNA-CH9.PCAP 文件。大多数的数据包分析软件都会在屏幕上半部分列出捕获帧。第一列是每个数据帧的编号，编号按顺序排列。

(4) 单击第 1880 号帧，这是一个探询请求帧。

(5) 在屏幕下半部分，观察帧主体的 SSID 字段部分，注意到这是一个定向探询请求帧。

(6) 单击第 1881 号帧，这是一个探询响应帧。

(7) 在屏幕下半部分，遍历帧主体信息，注意到这个帧与信标帧类似。

(8) 单击第 1240 号帧，这是一个探询请求帧，查看帧主体的 SSID 字段部分，注意到这是一个 Null 探寻请求。

(9) 单击第 1244 号帧，观察这个探询响应帧的字段信息。

9.7　认证

连接到 802.11 基本服务集(BSS)需要两个步骤，第一个步骤是认证(authentication)。802.11 客户端通过 AP 将数据发送给网络上的另一个设备之前，必须按顺序执行认证和关联步骤。

身份认证过程常被人误解。很多人认为的身份认证，就是输入用户名和密码来获得网络许可，也被称为网络身份验证。但在本章中，我们对身份认证的定义就是 802.11 认证。当 802.3 设备需要与其他设备通信时，第一步是将以太网电缆插入墙上的有线网口。当插入网口后，客户端就创建了一条到有线交换机的物理链路，并可以开始传输数据帧。而 802.11 设备进行通信前，必须首先接受 AP 的身份认证，或接受其他终端的身份认证(如果是 Ad Hoc 模式的话)。这种认证就好比将有线网卡通过以太网电缆连接到有线网口。802.11 身份认证只是在客户端和 AP 之间建立了一条初始连接。即认证两台设备都是有效的 802.11 设备。

802.11-2007 标准描述了两种认证方法：开放式系统认证和共享密钥认证。下面两节会对这两种认证方法进行阐述。

9.7.1　开放式系统认证

开放式系统认证(Open System Authentication)是两种认证方法中更简单的一种。它提供了一种不进行任何类型客户端认证的身份认证。本质上就是客户端和 AP 之间进行一些 hello 包的交互。因为设备之间没有进行任何身份交换或认证，它也被认为是空身份认证。开放式系

统认证在客户端和 AP 之间的帧交互过程，可以在练习 9.3 中看到。

有线等效加密(WEP)可以用于开放体系认证；然而，在客户端通过认证和关联后，WEP 仅用于加密数据帧的上层信息。开放式系统认证经常与更先进的网络安全认证方法结合使用，例如 802.1X/EAP。

练习 9.3

开放式系统认证

(1) 通过本书的在线资源 www.sybex.com/go/cwna3e 下载 CWNA-CH9.PCAP 文件。

(2) 等文件下载之后，用数据包分析软件打开。如果没有安装数据包分析软件，可以通过 www.wireshark.org 下载 Wireshark。

(3) 打开 CWNA-CH9.PCAP 文件。大多数的数据包分析软件都会在屏幕上半部分列出捕获帧。第一列是每个数据帧的编号，编号按顺序排列。

(4) 单击第 1905 号帧，这是一个认证请求帧。

(5) 在屏幕的下方，查看 802.11 MAC 包头，注意观察源地址和目标地址。

(6) 单击第 1907 号帧，这是一个认证响应帧。查看 802.11 MAC 包头，注意到源地址是 AP 的 BSSID，目的地址是发送认证请求帧的客户端 MAC 地址。遍历帧主体部分，注意到这次认证是成功的。

9.7.2 共享密钥认证

共享密钥认证(Shared Key Authentication)使用 WEP 对客户端进行认证，要求无线终端与 AP 上配置相同的静态 WEP 密钥。除了客户端被强制使用 WEP 以外，如果通信双方的静态 WEP 密钥不匹配，身份认证也会失败。认证过程与开放式系统认证相似，但额外会增加 AP 和客户端之间的挑战与响应过程。

在共享密钥认证过程中，认证帧进行了四次握手：

(1) 客户端将认证请求发送给 AP；然后，AP 通过认证响应将明文的挑战信息发送到客户端。

(2) 客户端再加密明文形式的挑战信息，并将其封装到另一个认证请求帧中回应给 AP；

(3) AP 对无线客户端的响应帧进行解密，并与明文的挑战信息进行比较

(4) 如果它们匹配，AP 将第四个也是最后一个身份认证响应帧发送给无线终端，确认认证成功，如果它们不匹配，AP 将响应认证失败，如果 AP 不能解密挑战信息，它也会发出认证响应失败信息。

如果共享密钥认证成功，则还将共享密钥认证过程中使用的静态 WEP 密钥用于对 802.11 数据帧的加密。

虽然看起来共享密钥认证比开放式系统认证更安全，但实际上共享密钥认证可能会面临更大的安全风险。通过捕获明文挑战信息，然后捕获响应帧中的加密挑战信息，静态 WEP 密钥有可能会被推算出来。如果静态 WEP 密钥泄露，所有数据帧都有可能被解密。因此这些传统的认证方法都不足以支撑企业安全，更安全的 802.1X/EAP 认证方法会在第 13 章中讨论。

9.8　关联

无线客户端通过 AP 的认证后，下一步就要与 AP 进行关联。一旦客户端关联成功，它就成为基本服务集(BSS)的一名成员。关联(Association)意味着客户端可以通过 AP 将数据发送到分布系统媒介。在关联过程中，客户端将关联请求(associate request)发送给 AP，希望加入 BSS。AP 回应关联响应(associate response)，允许或拒绝客户端加入 BSS。关联响应帧的主体中有关联标识符(AID)，这是分配给每个关联客户端的独特关联号。在本章后面部分你会了解到 AID 可以用于电源管理。

关联发生在共享密钥或开放式系统认证后，如练习 9.4 中所示。客户端通过完成关联成为 BSS 成员后，将发送 DHCP 请求，并在收到 DHCP 响应后，开始与上层进行通信。

练习 9.4

理解关联的过程

(1) 通过本书的在线资源 www.sybex.com/go/cwna3e 下载 CWNA-CH9.PCAP 文件。

(2) 等文件下载之后，用数据包分析软件打开。如果没有安装数据包分析软件，可以通过 www.wireshark.org 下载 Wireshark。

(3) 打开 CWNA-CH9.PCAP 文件。大多数的数据包分析软件都会在屏幕上半部分列出捕获帧。第一列是每个数据帧的编号，编号按顺序排列。

(4) 单击第 1909 号帧的主体部分，这是一个关联请求帧。

(5) 单击第 1911 号帧，这是一个关联响应帧。查看帧主体，注意到关联是成功的，并且客户端获得了 AID 编号。

9.8.1　认证状态与关联状态

802.11 无线终端保持两个变量用于跟踪认证状态和关联状态。被跟踪的状态如下：

- 认证状态：未认证或已认证
- 关联状态：未关联或已关联

这两个变量构成如下三种可能状态，见图 9-6 的描述：

- 状态 1：初始启动状态，未认证且未关联
- 状态 2：已认证且未关联
- 状态 3：已认证且已关联

因为无线终端在关联前必须进行认证，所以永远不会出现未认证且已关联的状态。

图 9-6 认证和关联状态机

9.8.2 基本速率与支持速率

你已经从前面几章的学习中了解到 802.11-2007 标准定义了各种射频技术的支持速率。例如，HR-DSSS(802.11b)支持速率为 1、2、5.5 和 11 Mbps。ERP(802.11g)除支持 HR-DSSS 的数据速率外也支持 ERP-OFDM 速率(包括 6、9、12、18、24、36、 48 和 54Mbps)。

对任何自治型 AP、协作型 AP 或 WLAN 控制器，某些数据速率可以配置成必要速率(required rate)。802.11-2007 标准把必要速率定义为基本速率(basic rate)。客户端能够成功与 AP 关联的前提是必须具备与 AP 要求的基本速率进行通信的能力。如果客户端不能使用 AP 要求的所有的基本速率进行通信，客户端就不能与 AP 关联也不会获准加入 BSS。

除了基本速率以外，AP 还定义了支持速率集。支持速率集可以通过 AP 的信标帧进行通告，也可以在某些其他管理帧中通告。支持速率是 AP 与无线终端通信使用的一组数据速率集合。无线终端与 AP 关联后，将使用 AP 通告的支持速率之一与 AP 进行通信。

9.8.3 漫游

当无线局域网存在多个无线 AP 时，802.11 标准提供一种功能使客户端从一个 AP 过渡到另一个 AP 时仍保持上层应用程序的网络连接。这种功能称为漫游(Roaming)，但 802.11 标准并未专门定义漫游的含义。

漫游的决定权由客户端掌握。决定客户端是否漫游的规则由无线网卡制造商确定，通常包括信号强度、噪音水平和误码率。客户端在通信时，会持续寻找其他的无线 AP，并与那些在范围内的无线 AP 进行认证。请记住，客户端可以与多个 AP 认证，但只和一个 AP 关联。当客户端移动并远离其原本关联的无线 AP，信号强度低于预定信号阈值时，它将尝试连接

到另一个 AP，并从其当前的 BSS 漫游到新的 BSS。客户端漫游时，原来的 AP 和新的 AP 会通过分布系统媒介互相通信并共同提供客户端的完全切换。很多厂家都有自己的切换方式，但这些切换方式都没有成为 802.11 标准的正式组成部分。在基于无线控制器的无线局域网解决方案中，漫游切换机制由 WLAN 控制器控制。

9.8.4　重关联

当客户端决定漫游到一个新的无线 AP 时，会将一个重关联请求帧(reassociation)发送到新的无线 AP。它之所以被称为重关联的原因不是因为它重关联到了无线接入点，而是重关联到这个无线网络的 SSID。

在客户端与 AP 交换 6 帧后，将进行重关联，重关联过程如下：

(1) 客户端向新的无线 AP 发送重关联请求。如图 9-7 所示，重关联请求帧包含了当前正在连接的 AP(即原来的 AP)的 BSSID(MAC 地址)。

图 9-7　重关联过程

(2) 新 AP 使用 ACK 帧回应。

(3) 新的 AP 经由无线网络向客户端发送重关联响应帧。

(4) 客户端给新 AP 发送 ACK。

客户端不必向原来的 AP 发送解除关联帧，因为客户端假定两个 AP 已经通过分布系统

媒介进行了通信。

(5) 新 AP 使用 DSM 与原来的 AP 通信。

新 AP 尝试通知原 AP 有关漫游客户端的信息，并要求原 AP 转发属于漫游客户端的所有缓冲数据。请记住 AP 之间的通信标准是私有的，未在 802.11-2007 标准中定义。在基于控制器的无线局域网解决方案中，AP 之间的通信通过控制器完成。

(6) 如果通信成功，原来的 AP 通过分发系统媒介把所有缓冲的数据转发到新的无线 AP。

(7) 新 AP 会通过无线网络将这些被转发过来的数据传输给客户端。

(8) 客户端向新的无线 AP 发送 ACK 帧，确认它收到了这些数据。

如果多个数据帧被转发到新的 AP，每个帧都会重复第 7 和第 8 步。

如果重关联不成功，客户端将保持与原始 AP 的连接，继续与它通信或再次尝试漫游到另一个 AP。在练习 9.5 中，可以看到重关联请求帧和重关联响应帧。

练习 9.5

理解重关联过程

(1) 通过本书的在线资源 www.sybex.com/go/cwna3e 下载 CWNA-CH9.PCAP 文件。

(2) 等文件下载之后，用数据包分析软件打开。如果没有安装数据包分析软件，可以通过 www.wireshark.org 下载 Wireshark。

(3) 打开 CWNA-CH9.PCAP 文件。第一列是每个数据帧的编号。

(4) 单击第 6650 号帧的主体部分，这是一个重关联请求帧。

(5) 单击第 6652 号帧，这是一个重关联响应帧。查看帧主体，注意到重关联是成功的，并且客户端获得了 AID 编号。

9.8.5 解除关联

解除关联(disassociation)是一种通告，而并非请求。客户端希望解除与 AP 的关联或 AP 希望解除与客户端的关联时，双方都可以发送解除关联帧。这是一种委婉地终止关联的方式。客户端在你关闭操作系统时会这么做。因为维护的缘故，AP 被断开与网络连接的时候也会这么做。解除关联不能被任何一方拒绝，除非启用管理帧保护(由 802.11w 定义)且消息完整性校验(MIC)失败。当解除关联帧没有被另一方听到时，MAC 管理可以用来调整这种通信丢失的情况。

9.8.6 解除认证

与解除关联相似，解除认证(deauthentication)帧也是一种通告，而非请求。客户端希望解除与 AP 的认证或 AP 希望解除与客户端的认证时，双方都可以发送解除认证帧。因为认证是关联的先决条件，解除认证帧会自动导致关联解除。解除认证帧不能被任何一方拒绝，除非启用管理帧保护(由 802.11w 定义)且消息完整性校验(MIC)失败。

9.9　确认帧

确认帧(ACK)是 9 种控制帧之一，也是 802.11 CSMA/CA 媒介访问控制方法的重要组成部分。由于 802.11 是无线媒介，无法确保数据传输成功，无线站点只能通过接收站的接收通告来了解传输数据帧是否已被正确接收。这个接收通告就是确认帧。

ACK 帧是一种由 14 个字节构成的简单帧，如图 9-8 所示。当一个无线站点接收到数据后，它会等待一段很短的时间，这段时间称为短帧间间隔(SIFS)。然后会复制这个数据帧中的发送端 MAC 地址，将其置于 ACK 帧的接收地址(RA)字段，然后发送这个 ACK 帧进行回复，在练习 9.6 中你可以看到 ACK 帧。如果传输顺利，数据帧的发送端会接收到接收地址字段(RA)为其 MAC 地址的 ACK 帧，从而了解到该帧被正确接收且未受到破坏。因为媒介的半双工特性，所以 ACK 帧优先级是最高的。每个单播帧的交付都需要被确认否则将会重传。ACK 帧是用于对数据交付进行验证的。

图 9-8　ACK 控制帧

每个单播帧后面必须跟着一个 ACK 帧。如果出于某种原因单播帧被损坏，32 位的 CRC(帧校验序列)将会失败，接收端将不会发送 ACK 帧。如果单播帧后面没有 ACK 帧的确认，它将重新传输。广播和多播帧并不要求确认。

练习 9.6

ACK 帧

(1) 通过本书的在线资源 www.sybex.com/go/cwna3e 下载 CWNA-CH9.PCAP 文件。

(2) 等文件下载之后，用数据包分析软件打开。如果没有安装数据包分析软件，可以通过 www.wireshark.org 下载 Wireshark。

(3) 打开 CWNA-CH9.PCAP 文件。第一列是每个数据帧的编号。

(4) 单击第 11169 号帧，这是一个数据帧。

(5) 观察 11169 号帧与 11178 帧之间的帧的交互，注意所有的单播帧都被接收站确认了。

9.10 分片

802.11-2007 标准允许对帧进行分片。分片(fragmentation)将 802.11 帧分解成小块(或称为片段)后，将报头信息添加到每个片段，并对其单独传输。虽然实际传输的数据与未分片时相同，但每个片段都需要其自己的报头，并且每个片段传输之后都需要 SIFS 和 ACK，因此在功能正常的 802.11 网络中，分片越小，数据吞吐量会因为 MAC 子层报头的额外开销、SIFS 和 ACK 等因素下降。但是，如果网络中出现大量的数据被损坏等不正常的通信状况，降低 802.11 分片的设置有可能会提高数据吞吐量。

如果某 802.11 帧被损坏，并且需要重新传送，整个帧都必须再次发送。当 802.11 帧被分割成多个片段时，每个片段尺寸更小且传输时间更短。如果干扰发生，将不再是整个帧被损坏，而可能只是某个较小的分片被损坏，那么只有这个分片需要被重传。重传一个小分片所花费的时间会比重传较大帧更少。因此采用分片措施有可能使重传开销降低。

图 9-9 阐释了较小的片段是如何减少重传开销的(请注意这里仅作为展示，并未按比例进行。此外，为了简化描述，过程中并未包括 ACK 帧)。此图上半部分描述了 1500 字节大小的帧的传输与重传，下半部分描述了三个较小的 500 字节分片的传输与重传。如果没有射频干扰，只有实心矩形的部分需要进行传输。每个帧都额外附加了报头(H)、帧间空隙 SIFS 及 ACK 的时间，所以采用较小片段总体需要更长时间。然而，如果产生射频干扰，相较于重传较大的帧，重传一个较小片段会花费更少的时间。

图 9-9 帧分片

传输分片与传输帧采用相同的方式。因此，每个分片也必须参与 CSMA/CA 媒介访问进程，也必须由 ACK 确认。确认如果一个片段未被 ACK，也将会重传。

并不是所有无线局域网网卡都可以调整分片设置。如果设置无线网卡使用更小的分片值，你必须意识到当网卡在无线 AP 间漫游或在网络之间移动时，所有的 802.11 帧都会按配

置进行分段。这意味着，如果无线终端漫游到一个无干扰的环境，它仍将使用较小的分片值，实际性能会比分片值设为最大时有所降低。

真实场景

分片会增加吞吐量吗？

在存在大量数据损坏的环境下，采用分片可能会减少重传开销。然而，分片会引入更多的 MAC 子层开销。通常情况下，如果使用分片，额外增加的 MAC 开销将导致网络吞吐量下降。但少数情况下，调整无线 AP 的分片阈值可以减少数据损坏引起的重传开销，从而提高吞吐量。采用数据帧分片通常是一种临时解决方案，更好的解决方案当然是要找到导致数据破坏的原因并修复。第 12 章将详细讨论第二层重传的原因及如何修复。

9.11　保护机制

802.11-2007 标准强制要求 ERP(802.11g)支持 DSSS 和 OFDM 技术。当 HR-DSSS(802.11b)客户端在一个 BSS 内与 ERP(802.11g)接入点或 ERP(802.11g)客户端通信时，802.11g 设备需要对较慢的 802.11b 设备提供一种兼容性。ERP 接入点还必须向后兼容传统的 DSSS*802.11)客户端。这种混用环境通常称为混合模式(mixed mode)。与有些人认为的相反，802.11g 设备并不是简单地切换至 802.11b 模式并使用 802.11b 数据速率通信。为使 802.11g、802.11b 与传统的 802.11 无线终端在相同的 BSS 内共存，802.11g 设备需要开启保护机制，也被称为 802.11g 保护模式(Protected mode)。在第 5 章中，你了解到厂商提供了三种 802.11g 接入点配置模式：

- **802.11b-only 模式**　当 802.11g AP 运行在此操作模式下，仅支持 DSSS 和 HR-DSSS。实际上，这个 AP 已经被配置成了 802.11b 接入点。传统 802.11 DSSS 客户端、802.11b HR-DSSS 客户端、802.11g ERP-DSSS 客户端和 802.11n 客户端都能够以 1Mbps、2Mbps、5.5Mbps 和 11 Mbps 的数据速率与 AP 通信。聚合吞吐量将与 802.11b 网络相同。
- **802.11g-only 模式**　AP 仅开启 G-only 模式，此时只有使用 ERP-OFDM 调制技术的 802.11g 客户端能够与其通信。使用 DSSS 的 802.11 和使用 HR-DSSS 的 802.11b 被禁用。因此，802.11b HR-DSSS 客户端和传统 802.11 DSSS 客户端将无法与 AP 关联。因为 802.11n 设备可以向后兼容传统的无线技术，它们可以连接到这个接入点，但仅限于使用 ERP-OFDM 技术。聚合吞吐量将与 802.11a 网络相同。例如，处于 54Mbps 数据速率的 AP 的聚合吞吐量可能在 19Mbps～20Mbps 之间。仅开启 11g 的无线局域网有时称为纯 G(Pure G)网络。
- **802.11b/g 模式**　这是大多数 802.11g AP 的默认模式，通常称为混合模式。这个模式同时支持 DSSS、HR-DSSS 和 OFDM 调制方式。802.11 DSSS 客户端与 802.11b HR-DSSS 客户端能够以 1Mbps、2Mbps、5.5Mbps 和 11Mbps 数据速率与 AP 通信，而 ERP(802.11g)客户端使用 6Mbps、9Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps 和 54Mbps 等 ERP-OFDM 数据速率与 AP 通信。802.11n 客户端也可以与之通信，但必须使用 ERP 技术。

厂商产品的具体配置并非 802.11-2007 标准的一部分。尽管大多数厂商的确支持这些配置，但标准是强制支持 802.11、802.11b、802.11g 设备在 ERP BSS 中共存的。

如何能确保高速率的无线网络可以高速传输？

即使你公司的所有无线设备都支持较高的数据速率，但只要看到存在哪怕一个较低数据速率设备，WLAN 都会启用保护机制。这个设备可以是你公司的访客，也可能只是有人开车驶过你的公司建筑物，而恰好他们的笔记本电脑使用了传统模式的无线网卡，附近某个公司或家庭启用了传统无线网络也可能会使 AP 开启保护机制。如果希望无线局域网始终使用更高的数据速率，你必须配置 AP 仅支持高数据速率的客户端。请记住这样做的后果是传统的无线设备将无法连接到你的网络。

在第 8 章中，你学习了阻止冲突发生的方法之一是为无线通信终端设置倒计时计时器(即 NAV)。这种通告方式被称为 NAV 分配。NAV 通过数据帧中的 Duration/ID 字段进行分配。当数据帧传输时，帧中的 Duration/ID 字段会被监听客户端用于 NAV 的设定。不幸的是，在混合模式中这是不可能的。802.11b HR-DSSS 设备不能理解 802.11g ERP-OFDM 的传输，因此 802.11b 设备无法得知 802.11g 设备传输的数据帧中 Duration/ID 值，802.11b 设备无法设置 NAV 计时器并错误地认为媒介是可用的，于是冲突就可能发生。要防止这种情况，802.11g ERP 终端需要切换到保护模式。

在混合模式中，在 802.11g 设备希望传输数据前，会先用 802.11b HR-DSSS 终端可以理解的数据速率和调制方法发送 RTS/CTS 帧或 CTS-to-Self 帧进行 NAV 分配。RTS/CTS 帧或 CTS-to-Self 帧可以被所有的 802.11b 和 802.11g 终端理解，其中包含的 Duration/ID 值可由所有监听终端用于重置 NAV 计时器。简单来说，ERP(802.11g)设备用所有终端都可以理解的较慢的速率来通知所有终端重置 NAV 值。在 802.11g 终端通过 RTS/CTS 或 CTS-to-Self 预留媒介后，就可以使用 OFDM 调制方式传输数据帧且不必担心与 802.11b HR-DSSS 或传统 802.11 DSSS 终端冲突。

在 ERP BSS 中，HR-DSSS(802.11b)和传统 802.11 DSSS 设备被称为非 ERP(non-ERP)终端。保护机制的目的就是使 ERP(802.11g)设备可以与非 ERP 设备(802.11b 和 802.11 旧设备)共存于相同的 BSS 内。这允许 ERP 终端使用更高的 ERP-OFDM 数据速率发送和接收数据的同时仍然向后兼容较旧的非 ERP 终端。

Devin Akin 撰写的“Protect Ripple in ERP 802.11 WLANs”的白皮书更详尽的讲述了保护机制。强烈建议用它做为 CWNA 考试准备的辅助读物。该白皮书可以从本书的公共资源 http://www.sybex.com/go/cwna3e 下载。

什么情况会触发保护机制？当 ERP 无线 AP 决定使用保护机制时，它需要通知在 BSS 中的所有 ERP(802.11g)终端打开保护机制。这可以通过在信标帧中设置 Non_ERP_Present 位来实现，ERP 终端将知道需要使用保护模式。在 ERP 基本服务集中有三种场景可以触发保护机制：

- 如果一个 non-ERP 终端关联到 ERP 接入点，ERP 接入点将在自己的信标帧中启用 Non_ERP_Present 比特位，从而在 BSS 中开启保护机制。换句话说，HR-DSSS(802.11b)客户端关联会触发保护机制。
- 如果 ERP 接入点听到来自另一个 AP 的信标帧中只存在 802.11b 或 802.11 DSSS 支持速率，它将在自己的信标帧中启用 Non_ERP_Present 位，从而在 BSS 中开启保护机制。简单来说，如果 802.11g AP 听到来自 802.11 或 802.11b 接入点或 802.11b ad hoc 客户端的信标帧，将触发保护机制。
- 如果 ERP 接入点听到管理帧中(非探寻请求帧)只存在 802.11 或 802.11b 的支持速率，NonERP-Present 位也会设置为 1。

802.11n 修正版引入了新的传输技术，需要向后兼容所有的传统技术，同时也引入了新的保护机制。第 18 章将介绍 802.11n 处理混合模式网络的细节。

802.11b 对 802.11g 吞吐量有什么影响？

一个常见的误解是802.11g无线模块在启用保护机制后将返回802.11b数据速率。事实上，ERP(802.11g)无线模块仍然按较高的 ERP-OFDM 速率传输数据。不过，当 HR-DSSS(802.11b)终端导致 ERP(802.11g)BSS 启用保护机制后，在每一个 ERP-OFDM 数据传输之前会增加大量的 RTS/CTS 或 CTS-to-Self 开销。聚合数据吞吐量的下降是因为这些额外的开销而不是因为使用较慢的 802.11b 速率。未启用保护机制时，54Mbps 的数据速率通常可以提供大约 18Mbps～20 Mbps 的聚合吞吐量。启用保护机制后，开销会导致聚合数据吞吐量降至 13Mbps 以下，甚至可能低至 9Mbps。

9.11.1　RTS/CTS

无线客户端为了加入 BSS，必须能够与 AP 进行通信。这是简单并合乎逻辑的。但是，很可能客户端可以与 AP 进行通信，但不能监听到任何其他客户端或不能被其他客户端监听到。这可能会是一个问题，因为无线终端为了避免冲突，需要监听另一终端的传输(虚拟载波侦听)设置其 NAV 值并监听射频(物理载波侦听)。如果此终端不能监听到其他终端，或不能被其他终端监听到，则发生冲突的可能性很大。请求发送/清除发送(RTS/CTS)是执行 NAV 分配的一种机制，并有助于防止发生冲突。这种 NAV 分配会在数据帧传输之前进行媒介预留。

现在，让我们从略带技术的角度看 RTS/CTS。我们仅进行较基础的解释，因为深入解释超出了 CWNA 的考试范围。当无线设备启用 RTS/CTS 时，每当该设备需要传输帧前都必须执行 RTS/CTS 交换。当发送站传输数据时，它会首先发送 RTS 帧。RTS 帧的 Duration 值会重置所有监听终端的 NAV 定时器，使监听终端必须等待 CTS、DATA 和 ACK 帧传输完毕。接收站会发送 CTS 帧，它也可用于 NAV 分配。CTS 帧的 Duration 值会重置所有监听站 NAV 定时器，以使监听终端必须等待 DATA 和 ACK 帧传输完毕。

如图 9-10 所示，RTS 帧的 Duration 值等于传输 ACK/CTS/DATA 外加上三个 SIFS 间隔所需的时间(以微秒为单位)。CTS 帧的 Duration 值表示传输 DATA/ACK 外加上两个 SIFS 间隔所需的时间(以微秒为单位)。如果终端没有侦听到 RTS 帧，它应当可以监听到 CTS 帧。无

论终端听到 RTS 还是 CTS，它都将根据 RTS 或 CTS 帧设置其 NAV 值。此时 BSS 中的所有终端都重置了各自的 NAV，会等待全部数据完成交换。图 9-11 描绘了客户端和 AP 之间的 RTS/CTS 交互。

RTS/CTS 主要用于两种情况：检测隐藏节点问题(在第 12 章中介绍)或在 ERP 基本服务集中用作混合模式环境下的保护机制之一。

图 9-10 RTS/CTS Duration 值

图 9-11 RTS/CTS 帧交互

9.11.2 CTS-to-Self

CTS-to-Self 用作混合模式环境下的保护机制。作为一种保护机制，使用 CTS-to-Self 而

不是 RTS/CTS 的好处之一是吞吐量会更高，因为需要发送的帧更少。

当使用 CTS-to-Self 的某终端希望传输数据时，它会通过发送 CTS 帧进行 NAV 分配。此 CTS 帧通知其他所有终端必须等待直到 Data 和 ACK 帧传输完毕。任何听到 CTS 的终端将设置其 NAV 为由 CTS 提供的值。

CTS-to-Self 被用作混合模式下的保护机制之一。ERP(802.11g)站使用所有终端都可以理解的 DSSS 技术传输 CTS 帧，而数据和 ACK 帧将使用速度更快的 802.11g(ERP-OFDM)传输。

CTS-to-Self 更适合 AP 使用。为了预留媒介，需要确保所有终端都能听到 CTS，这一点 AP 最容易做到。如果客户端使用 CTS-to-Self，就可能因为客户端之间的距离过远而没有意识到媒介正在传输。尽管这是真的，但从我们的经验来看，在客户端上使用 CTS-to-Self 预留媒介比 RTS/CTS 方式更常见。有些供应商还允许客户端在 CTS-to-Self 和 RTS/CTS 中进行选择。

9.12　数据帧

前面提到过共有 15 种类型的数据帧(Data Frame)。最常见的数据帧是简单数据帧(simple data frame)，即在帧主体中封装 MSDU 上层信息。自治型 AP 和 WLAN 控制器的集成服务将简单数据帧的 MSDU 有效净荷转换为 802.3 以太网帧的 MSDU。因为数据隐私的关系，通常应加密 MSDU 数据净荷。

客户端使用空功能帧(null function frame)通知 AP 节电状态发生变化，这一点通过更改电源管理位(power management bit)可以做到。当一个客户端出于主动扫描的目的，离开数据传输信道进行信道外扫描时，客户端也会向 AP 发送电源管理位(power management bit)为 1 的空功能帧。如练习 9.7 所示。此时 AP 将缓冲所有该客户端的 802.11 帧。当客户端返回到 AP 的信道时，再向 AP 发送电源管理位为 0 的空功能帧。然后 AP 会把缓冲帧传回客户端。某些厂商也用空功能帧进行专用的电源管理。

练习 9.7

了解数据帧

(1) 通过本书的在线资源 www.sybex.com/go/cwna3e 下载 CWNA-CH9.PCAP 文件。

(2) 等文件下载完毕之后，用数据包分析软件打开。如果没有安装数据包分析软件，可以通过 www.wireshark.org 下载 Wireshark。

(3) 打开 CWNA-CH9.PCAP 文件。第一列是每个数据帧的编号。

(4) 单击第 68819 号帧，这是一个未加密的简单数据帧。查看帧主体，请留意帧的上层信息，如 IP 地址和 TCP 端口。

(5) 单击第 68831 帧，这是一个空功能帧。查看 802.11MAC 报头的帧控(Frame Control)字段，并注意此处电源管理位为 1。AP 现在将缓存客户端的流量。

9.13 电源管理

无线网络的主要用途之一是为客户端提供移动性。客户端移动性与客户端电池的续航能力密切相关。要增加电池续航时间，可以用更大容量、 更持久的电池或者减少电力消耗。802.11 标准包含了能够帮助增加电池续航时间的电源管理功能。电池续航时间对手持扫描仪和 VoWiFi 电话是极为重要的。手持设备的电池通常需要提供至少 8 小时的使用时长。802.11 标准支持两种传统电源管理模式：主动模式(Active mode)和节电模式(Power Save mode)。802.11 电源管理方法还通过两个已被纳入正式标准的的 802.11e 和 802.11n-2009 得到了改进。

9.13.1 主动模式

主动模式(Active mode)是大多数 802.11 终端默认的电源管理模式。当终端设置为主动模式时，总是时刻准备好传输或接收数据。主动模式有时也称为持续清醒模式(Continuous Aware mode)，并不提供电力节省功能。在 802.11 帧的 MAC 报头中，电源管理字段占用 1 位，用于说明无线终端电源管理模式。值为 0 表示终端处于主动模式。终端处于主动模式可以比处于节电模式时实现更高的吞吐量，但电池续航时间会缩短。

连接电源的终端应总是配置为主动模式。

9.13.2 节电模式

节电模式(Power Save mode)是 802.11 终端的一个可选模式。当一个客户端设置为节电模式时，它将会关闭某些收发器组件，从而节省电力消耗。无线终端会通过将电源管理位值置为 1 表示它正使用节电模式。此刻 AP 会缓存该客户端的所有 802.11 帧。无线终端工作在 BSS 或 ad hoc 模式时的节电模式有所不同，这将在本章后面阐述。

9.13.3 流量指示图

如果无线客户端加入某基本服务集(BSS)，会向 AP 通告其电源管理字段为 1，表明该客户端处于节电模式。此时如果 AP 接收到目标去往处于节电模式的客户端的所有数据，都将存储在 AP 的缓冲区。客户端与 AP 关联时，会被分配关联标识符(AID)。AP 使用 AID 来跟踪关联终端和 BSS 成员。如果 AP 正在缓存某个处于节电模式的终端数据时，在 AP 传输其下一个信标帧时，该终端的 AID 将出现在信标帧的某字段中，这个字段即流量指示图(TIM)。TIM 字段列出了有缓存数据待传送的所有无线终端的列表。每个信标帧都将包括这些无线终端的 AID，直到它们的缓存数据传递完毕。

在无线终端通知 AP 将处于节电模式后，无线终端将关闭其收发器的一部分，以节省电力。无线终端可以处于下面两个状态之一：清醒或休眠。

- 在清醒状态中，客户端可以接收和传输帧。
- 在休眠状态中，客户端无法接收或传输任何帧，并处于极低的电源状态以省电。

信标帧按一致的预定时间间隔传送，这个预定时间称为目标信标传输时间(TBTT)。因为所有终端都知道何时信标会被发出，无线终端将在一个较短的时间内保持休眠状态，并及时清醒以接收信标帧。无线终端需要保持清醒并接收每个信标帧。为节省更多电力，客户端可以休眠一段较长的时间，然后再醒来接收即将到来的信标帧。客户端醒来的频率由聆听间隔(listen interval)决定，并且通常是厂商指定的。

当终端接收到信标帧，它会检查其 AID 是否在 TIM 中，如果在则暗示有缓存的单播帧等待传输。如果出现这种情况，无线终端将保持清醒，并向 AP 发送节电轮询帧(PS-Poll)。当 AP 接收节电轮询帧后，将发送缓存的单播帧给无线终端。AP 传输缓存的单播帧时，无线终端将保持清醒。当 AP 将缓存数据发送给无线终端时，终端需要知道什么时候所有缓存的单播数据传输完毕，这样它就可以继续休眠。每个单播帧都包含一个被称为更多数据字段(More Data field)的 1 位字段。当终端接收到的缓存单播帧中的 More Data 字段被设置为 1 时，无线终端不能返回休眠，因为还有缓存数据尚未收到。当 More Data 字段设置为 1 时，无线终端需要发送另一个 PS-Poll 帧并等待接收缓存的下一个单播帧。

在所有缓存的单播帧发送完毕，最后一个缓存帧中的 More Data 字段将被设置为 0，表示当前已经没有缓存数据，此刻无线终端将返回休眠状态。AP 从 TIM 中删除该终端的 AID，在下一个 TBTT 时间到来时，再发送一个新的信标帧。无线终端将在短时间内保持休眠状态后再次清醒以接收信标帧，并再次查看 TIM 中是否有其 AID。假设没有该终端的缓存单播帧，终端的 AID 不会出现在 TIM 中，这时无线终端可以返回休眠并按时醒来再次检查。

9.13.4　传输流量指示消息

除了单播流量，网络流量还包括多播和广播流量。因为多播和广播流量被转发给所有终端，BSS 需要提供一种方法，以确保所有终端都保持清醒接收这些帧。传输流量指示消息(DTIM)就是用来确保当多播或广播的通信被发送时，所有使用电源管理的终端都保持清醒。DTIM 是一种特殊类型的 TIM。每个 Beacon 帧都包含 TIM 或 DTIM。

在 AP 上配置的 DTIM 时间间隔(DTIM interval)是用来确定 DTIM 的传输频率。DTIM 间隔为 3 意味着每 3 个信标帧就有 1 个包含 DTIM，而 DTIM 间隔为 1 意味着每个信标帧都包含 DTIM。包含 DTIM 的信标帧通知终端下一次 DTIM 何时到来。DTIM 值为 0 表示当前的 TIM 就是 DTIM。所有无线终端都会准时清醒并接收包含 DTIM 的信标。如果 AP 有多播或广播流量要发送，它会先发送包含 DTIM 的信标帧，然后立即发送多播或广播数据。

在组播或广播数据传输完毕后，如果某终端的 AID 仍然在 DTIM 中，无线终端将保持清醒，发送节电轮询帧(PS-Poll)，并着手处理从 AP 发送的缓存单播流量。如果终端未在 DTIM 中发现其 AID，便可以返回休眠状态。

DTIM 间隔的设置对于任何使用组播的应用程序是很重要的。例如，许多 VoWiFi 厂商支持将 VoIP 流量发送到组播地址的一键通(push-to-talk)功能。DTIM 间隔配置错误将导致一键通在多播数据发送期间出现性能问题。

9.13.5 通告流量指示消息

如果无线终端属于独立基本服务集(IBSS)，将不会出现可以缓存处于节电模式的终端数据的接入点。此无线终端通过将电源管理字段更改为 1，通知其他终端它已经启用了节电模式。其他终端会缓存其数据。

所有终端必须定期醒来并互相通知是否有缓存数据需要传递。所有设备都必须周期醒来并进行信息交换的时间被称为通告流量指示消息(ATIM)窗口。在 ATIM 窗口期间，如果此终端有另外一个终端的缓存数据，它将发送一个称为 ATIM 的单播帧给另一个终端。ATIM 通知无线终端必须保持清醒直到下一个 ATIM 窗口，以便它可以接收缓存数据。任何有其他终端的缓存数据或收到 ATIM 帧的终端都将保持清醒，以便可以交换缓存数据。所有无关的其他终端都可以返回休眠，等待下一次 ATIM 窗口的到来时再重复这一过程。

ATIM 窗口期间，保持清醒的终端节点通过 CSMA/CA 进程交换未发送的数据。如果终端无法在这段时间传输数据，它将在下一个 ATIM 窗口中发送另一个 ATIM 帧，然后继续尝试在 CSMA/CA 期间发送数据。

不要混淆 ATIM 帧与 TIM 字段。ATIM 是一个帧，用于 ad hoc 客户端进行电源管理。TIM 是信标帧中的一个字段，通告处于电源管理模式的客户端有其缓存的单播数据。

9.13.6 WMM 节电模式与 U-APSD

802.11e 修正案(现在是 802.11-2007 标准的一部分)关注的主要焦点部分是服务质量(QoS)。但 IEEE802.11e 修正案还引入了增强的电源管理方法，称为自动节电传输(APSD)。有两种 APSD 方法：计划自动节电传输(S-APSD)和非计划自动节电传输(U-APSD)。S-APSD 电源管理方法超出了本书的讲述范畴。Wi-Fi 联盟的 WMM 节电(WMM-PS)认证是基于 U-APSD 的。WMM-PS 是前面所述传统节能机制的增强机制。WMM-PS 的目标是让客户端设备有更多时间处于休眠状态，从而降低功耗。WMM-PS 也旨在减少电源管理过程中对时延敏感的应用程序的传输延迟，如语音。

传统的电源管理方法有一些局限性。如图 9-12 所示，使用传统电源管理的客户端在请求接收缓存单播帧前，必须首先等待携带 TIM 的信标。客户端还必须为每一个缓存的单播帧发送节电轮询帧(PS-Poll)。这种类似乒乓球运动的电源管理方法增加了对时延敏感应用程序的延迟。在“乒乓”的传输过程中，客户端还必须保持清醒，这也降低了电池续航时间。此外，客户处于休眠状态的时间由厂商提供的驱动程序决定，而不是由应用程序流量决定。

图 9-12　传统电源管理

WMM-PS 在接收缓存单播流量时使用了一种基于 WMM 访问类别的触发机制。在第 8 章我们了解到，来自以太网侧的 802.1D 优先级标记将流量导入四个不同 WMM 访问类别的优先级队列。这四个访问类别队列分别是是语音流量、视频流量、尽力传输流量和背景流量。如图 9-13 所示，客户端发送一个与 WMM 访问类别相关的触发帧通知 AP 它目前正处于清醒状态，已经做好下载 AP 可能缓存的任何该访问类别帧的准备。这个触发帧也可以是 802.11 数据帧，因此不再需要发送单独的 PS-Poll 帧。接着 AP 向客户端发送 ACK 帧，并在传输机会(TXOP)期间内执行缓存应用程序流量的“帧突发”传输。

图 9-13　WMM-PS

这种增强电源管理方法的优点包括：

- 应用程序现在可以通过设置休眠周期和发送触发帧来控制节电行为。例如 VoWiFi 电话在通话期间会频繁给触发帧发送 AP，而使用数据应用程序的笔记本电脑相对会有较长的休眠期。
- 触发和传输不再需要 PS-Poll 帧。

- 客户端可以请求下载缓存流量，不必再等待信标帧。
- 所有下行的应用程序流量在 TXOP 期间可以更快的帧突发形式进行传输。

Wi-Fi 客户端使用增强的 WMM-PS 机制必须满足三个条件：

- 客户端必须通过 Wi-Fi WMM-PS 认证；
- 无线 AP 必须支持 Wi-Fi WMM-PS 认证；
- 对延迟敏感的应用程序也必须支持 WMM-PS 认证。

应当指出，不支持 WMM-PS 的应用程序仍可以与支持 WMM-PS 的应用程序并存。来自其他应用程序的数据会按照传统节电方法传输。

本书在线资源包含一篇来自 Wi-Fi 联盟的“移动和便携式 Wi-Fi 认证设备的 WMM 节电”的白皮书。强烈建议将此白皮书列为 CWNA 考试的额外读物。

9.13.7 802.11n 电源管理

802.11n-2009 修正案还定义了两个新的电源管理方法。第一种电源管理方法称为空间复用节电(spatial multiplexing power save)或 SM 节电。SM 节电方式是指使支持 MIMO 的 802.11n 设备只保留一个射频链而关闭其他的以达到节电目的。第二种电源管理方法是节电多轮询(power save multipoll)或 PSMP，也由 HT(802.11n)定义。PSMP 是自动节电传输(APSD)的扩展，APSD 由 802.11e 修正案定义。第 18 章会对这两种电源管理方法进行更详细的讨论。

9.14 频段引导

在本章的前面部分你已经了解 802.11 是如何处理不同数据速率的设备通信的。较慢数据传输速率的设备将影响信道上的所有设备的整体性能。过去几年来，能够运行在 2.4GHz 和 5GHz 两个频段的网卡(802.11a/b/g)变得越来越普遍，而大多数的 802.11n 设备也能运行在这两个频段。

2.4 GHz 频段上 802.11b 和 802.11g 设备的大量使用，使得混合模式变得很常见。在 5GHz 频段上使用 802.11a 的很少，但 802.11n 设备使用的很普及。正因为如此，在 5GHz 频段往往不使用混合模式。

另一个重大不利情况是 2.4GHz 频段除了用于 WLAN 网络外，许多其他类型的装置也在使用，包括微波炉、婴儿监护器、无绳电话和视频摄像头。工作在相同频率范围内的所有这些设备比在 5GHz 频段有更多干扰和更高的本底噪声。此外，在 2.4GHz 频段只有 3 个非重叠信道，在 5GHz 频段(根据当地的监管领域)通常至少有 4 到 8 个可用信道，5GHz 频段可以进一步降低参与竞争传输的设备的数量。

因此，如果使用 5GHz 频段将提供更好的吞吐量和性能，我们如何鼓励客户使用这个频段？客户端通常基于要连接的 SSID 中最强的信号来决定使用何种频段连接哪个 AP。目前能

够在2.4GHz和5GHz宣告相同的SSID的接入点很常见。由于5GHz信号自然衰减超过2.4GHz信号时，客户端发现 2.4GHz 具有较强的信号，并默认连接到这个频段。一个被称为频段引导(band steering)的技术鼓励双频客户端连接到 5GHz 的 AP，而不是 2.4GHz 的 AP。

频段引导不是 IEEE 802.11 开发的技术。到目前为止，所有频段引导的实现都是私有的。但大多数厂商使用类似方法来实现这一技术。当双频客户端第一次启动时，它会在 2.4GHz 和 5GHz 频段发送探询请求帧来查找 AP。当双频 AP 听到来自同一客户端的两个频段的探询请求帧时，便知道客户端能够运行在 5GHz 频带。 AP 将仅响应使用 5GHz 频段的客户端，使用这种方法尝试引导客户端使用 5GHz 频带。通常情况下，客户端在 2.4GHz 和 5GHz 频段发送探询请求，但 AP 只在 5GHz 频段进行探询响应。尽管客户端被引导使用 5GHz 频段的 AP，但仍有客户端使用 2.4GHz 频段连接 AP。如果客户端持续尝试使用 2.4GHz 连接 AP，AP 最终会允许这个连接。

9.15　小结

本章涵盖了 MAC 体系结构的关键领域：

- 802.11 帧格式
- 主要的 802.11 帧类型
- 802.11 帧子类型
- 分片
- ERP 保护机制
- 电源管理

需要大家理解三种主要的 802.11 帧类型、802.11 帧的作用和如何在扫描、认证、关联及其他 MAC 进程中用到它们。请务必了解为什么需要 ERP 保护机制。没有保护机制，混合模式网络就无法工作。RTS/CTS 和 CTS-to-Self 提供了 ERP(802.11g)保护机制。为进一步优化混合模式网络，可以使用频段引导鼓励双频用户使用 5GHz 频段。

为帮助管理电池续航时间，电源管理可在无线终端上进行配置。主动模式不会节电，而节电模式可以提高笔记本电脑和手持计算设备的电池续航时间。WMM 和 802.11n 增强了电源管理功能。本章讨论了如下电源管理组件：

- 流量指示图(TIM)
- 传输流量指示消息(DTIM)
- 通告流量指示消息(ATIM)
- WMM 节电(WMM-PS)

9.16　考试要点

解释 PPDU、PSDU、MPDU 和 MSDU 之间的差别。了解每个数据单元操作在 OSI 模型的哪一层，并了解每个数据单元的组成。

了解 802.11 帧和 802.3 帧的异同。IEEE 创建这两种帧类型。802.11 和 802.3 帧拥有一些相似的属性，也有不同的属性。知道如何互相比较。

了解三个主要的 802.11 帧类型。请确保你知道管理、控制和数据帧的作用。知道这些帧类型的区别。数据帧包含 MSDU，而管理和控制帧不包含。了解每个单个帧子类型的作用。

了解媒介访问控制(MAC)过程和在此过程中使用的所有帧。了解以下功能：主动扫描、被动扫描、信标、探询请求、探询响应、认证、关联、重关联、解除关联和解除认证。

了解用于确认单播帧被接收且未被破坏的 ACK 帧的重要性。理解单播帧传输后，会有一个短帧间间隔(SIFS)，然后接收站发送 ACK 帧进行回复。如果这个过程成功完成，发送端就知道帧被收到且未受损。

分片带来的利弊。默认情况下，分片增加了开销，分片比未分片要更慢。如果存在射频干扰，分片可以减少重传开销，实际上增加了数据吞吐量。如果分片确实增加吞吐量，很明显存在传输问题，例如多径现象。

了解 ERP 保护机制及其运作方式。保护模式允许 ERP(802.11g)、HR-DSSS(802.11b)和传统 DSSS 设备在相同的 BSS 内共存。保护模式可以利用 RTS/CTS 或 CTS-to-Self 两种方式。CTS-to-Self 只是一种保护机制，但 RTS/CTS 阈值还可以进行手动配置，用于识别或阻止隐藏节点问题。

了解频段引导的概念和原理。频段引导被用来鼓励双频客户端使用 5GHz 传输，而非 2.4GHz。这减少了运行在 2.4GHz 使用保护机制的客户端数量，而且 5GHz 频段可以使运行性能更好，传输速度更快，而且可以使用更多的信道。

了解电源管理技术。启用电源管理可以降低功耗并延长电池持续时间。了解缓存单播帧与缓存广播和多播帧的不同方式。了解 WMM-PS 增强电源管理功能。

9.17 复习题

复习题的答案见附录 A。

1. What is the difference between association frames and reassociation frames? (Choose all that apply.)

   A. Association frames are management frames, whereas reassociation frames are control frames.

   B. Fast BSS transition only uses reassociation frames.

   C. Association frames are used exclusively for roaming.

   D. Reassociation frames contain the BSSID of the original AP.

   E. Only association frames are used to join a BSS.

2. Which of the following contains only LLC data and the IP packet, but does not include any 802.11 data?

   A. MPDU

   B. PPDU

   C. PSDU

D. MSDU

E. MMPDU

3. Which of the following are protection mechanisms? (Choose all that apply.)

A. NAV back-off

B. RTS/CTS

C. RTS-to-Self

D. CTS-to-Self

E. WEP encryption

4. The presence of what type of transmissions can trigger the protection mechanism within an ERP basic service set? (Choose all that apply.)

A. Association of an HR-DSSS client

B. Association of an ERP-OFDM client

C. HR-DSSS beacon frame

D. ERP beacon frame with the NonERP_Present bit set to 1

E. Association of an FHSS client

5. Which of the following information is included in a probe response frame? (Choose all that apply.)

A. Time stamp

B. Supported data rates

C. Service set capabilities

D. SSID

E. Traffic indication map

6. Which of the following are true about beacon management frames? (Choose all that apply.)

A. Beacons can be disabled to hide the network from intruders.

B. Time-stamp information is used by the clients to synchronize their clocks.

C. In a BSS, clients share the responsibility of transmitting the beacons.

D. Beacons can contain vendor-proprietary information.

7. If WMM-PS is not supported, after a station sees its AID set to 1 in the TIM, what typically is the next frame that the station transmits?

A. Data

B. PS-Poll

C. ATIM

D. ACK

8. When a station sends an RTS, the Duration/ID field notifies the other stations that they must set their NAV timers to which of the following values?

A. 213 microseconds

B. The time necessary to transmit the DATA and ACK frames

C. The time necessary to transmit the CTS frame

D. The time necessary to transmit the CTS, DATA, and ACK frames

9. How does a client station indicate that it is using Power Save mode?

A. It transmits a frame to the AP with the Sleep field set to 1.

B. It transmits a frame to the AP with the Power Management field set to 1.

C. Using DTIM, the AP determines when the client station uses Power Save mode.

D. It doesn't need to, because Power Save mode is the default.

10. What would cause an 802.11 station to retransmit a unicast frame? (Choose all that apply.)

A. The transmitted unicast frame was corrupted.

B. The ACK frame from the receiver was corrupted.

C. The receiver's buffer was full.

D. The transmitting station will never attempt to retransmit the data frame.

E. The transmitting station will send a retransmit notification.

11. If a station is in Power Save mode, how does it know that the AP has buffered unicast frames waiting for it?

A. By examining the PS-Poll frame

B. By examining the TIM field

C. When it receives an ATIM

D. When the Power Management bit is set to 1

E. DTIM interval

12. When is an ERP (802.11g) AP required by the IEEE 802.11-2007 standard to respond to probe request frames from nearby HR-DSSS (802.11b) stations? (Choose all that apply.)

A. When the probe request frames contain a null SSID value

B. When the AP supports only ERP-OFDM data rates

C. When the AP supports only HR/DSSS data rates

D. When the Power Management bit is set to 1

E. When the probe request frames contain the correct SSID value

13. Which of the following are true about scanning? (Choose all that apply.)

A. There are two types of scanning: passive and active.

B. Stations must transmit probe requests in order to learn about local APs.

C. The 802.11 standard allows APs to ignore probe requests for security reasons.

D. It is common for stations to continue to send probe requests after being associated to an AP.

14. What process is used by band steering to make client radios connect to the AP's 5GHz radio?

A. The AP disables the 2.4GHz radio.

B. The AP disables the 2.4GHz radios during the connection process.

C. The AP signals the client that 5GHz connectivity is preferred, triggering the client to disable its 2.4GHz radio.

D. The AP only responds to the client using the 5GHz radio.

E. Band steering is enabled on the client, not the AP, requiring the client to be configured to use band steering.

15. When a client station is first powered on, what is the order of frames generated by the client station and AP?

A. Probe request, probe response, association request/response, authentication request/response

B. Probe request, probe response, authentication request/response, association request/response

C. Association request/response, authentication request/response, probe request, probe response

D. Authentication request/response, association request/response, probe request, probe response

16. WLAN users have recently complained about gaps in audio and problems with the pushto-talk capabilities with the ACME Company's VoWiFi phones. What could be the cause of this problem?

A. Misconfigured TIM setting

B. Misconfigured DTIM setting

C. Misconfigured ATIM setting

D. Misconfigured BTIM setting

17. The WLAN help desk gets a call that all of the sudden, all of the HR-DSSS (802.11b) VoWiFi phones cannot connect to any of the ERP (802.11g) lightweight APs that are managed by a multiple-channel architecture WLAN controller. All the laptops with ERP (802.11g) radios can still connect. What are the possible causes of this problem? (Choose all that apply.)

A. The WLAN admin disabled the 1, 2, 5.5, and 11Mbps data rates on the controller.

B. The WLAN admin disabled the 6 and 9 Mbps data rates on the controller.

C. The WLAN admin enabled the 6 and 9 Mbps data rates on the controller as basic rates.

D. The WLAN admin configured all the APs on channel 6.

18. In a multiple-channel architecture, roaming is controlled by the client station and occurs based on a set of proprietary rules determined by the manufacturer of the wireless radio. Which of the following parameters are often used when making the decision to roam? (Choose all that apply.)

A. Received signal level

B. Distance

C. SNR

D. WMM access categories

19. What are some of the advantages of using U-APSD and WMM-PS power management over legacy power-management methods? (Choose all that apply.)

A. Applications control doze time and trigger frames.

B. U-APSD APs transmit all voice and video data immediately.

C. The client does not have to wait for a beacon to request data.

D. Downlink traffic is sent in a frame burst.

E. Data frames are used as trigger frames. PS-Poll frames are not used.

20. WMM-PS is based on which 802.11-2007 power-management method?

A. S-APSD

B. U-APSD

C. PSMP

D. SM Power Save

E. PS-Poll

第10章 无线局域网架构

在该章中，你将学习以下内容：

- √ 无线局域网客户端设备
  - 无线射频(网)卡类型
  - 无线射频(网)卡芯片组
  - 客户端实用程序
- √ 管理、控制和数据平面
  - 管理平面
  - 控制平面
  - 数据平面
- √ 无线局域网架构
  - 自治型 WLAN 架构
  - 无线网络管理系统(WNMS)
  - 集中式 WLAN 架构
  - 分布式 WLAN 架构
  - 统一 WLAN 架构
- √ 无线局域网基础设施
  - 无线工作组网桥
  - 无线局域网网桥
  - 企业无线网关
  - 家用 Wi-Fi 路由器
  - 无线局域网 mesh 接入点
  - 无线局域网阵列
  - 虚拟接入点系统
  - 实时定位系统
  - 无线语音(VoWiFi)

第 7 章中讨论了各种类型的 802.11 无线局域网拓扑。你了解到客户端和接入点都可以被安排在服务集中以提供某种形式的媒介访问。在这一章中，我们将讨论在 802.11 网络中可用的多种无线设备。我们会介绍可用于台式机、笔记本电脑、智能手机、平板电脑等的多种客户端无线网卡。

本章还会讨论网络运行的三个逻辑平面及其应用。我们将探讨 WLAN 基础架构设备的发展历程和多种 WLAN 架构。本章还涵盖了当今 Wi-Fi 市场中的许多无线局域网专业设备。

最后，我们会介绍一些特殊的无线局域网解决方案，如实时定位系统(RTLS)和 VoWiFi。

10.1 无线局域网客户端设备

无线局域网客户端网卡(NIC)的主要硬件组成部分是半双工的无线电收发器，可以有许多硬件格式和芯片组。所有的客户端网卡都需要特殊的驱动程序与操作系统对接，需要软件实用程序与最终用户对接。笔记本电脑网卡可以在 Windows、Linux 和 Macintosh 操作系统上使用，尽管针对不同的操作系统需要安装不同的驱动程序和客户端软件。很多制造商网卡的驱动程序可能已经包含在操作系统中，但一些较新的网卡可能需要最新的驱动程序。多数厂商会通过 CD 光盘提供驱动程序的自动化安装向导，但有些可能需要在操作系统中手动安装驱动程序。驱动程序损坏是无线局域网射频模块不能正常工作的常见原因。一般来说，重装 802.11 无线驱动程序就可以解决这种问题。

通过软件界面，终端用户可以对网卡进行认证、安全和性能等方面的配置以加入无线局域网。客户端实用程序一般是制造厂商的软件实用程序或内置在操作系统中的内部软件接口。

下面讨论各种无线网卡类型、芯片组及软件客户端实用程序。

10.1.1 无线射频(网)卡类型

802.11 无线模块既可以用于客户端网卡，也可以用于接入点。本节主要侧重于介绍用于客户端设备的无线网卡。802.11 无线模块存在许多不同的形状，意味着无线网卡也有很多形状和大小。许多如 PCMCIA 和 USB 形式的 Wi-Fi 无线网卡可以作为外部设备，但现在大多数的 Wi-Fi 设备采用内置或集成的形式。

1. 外置 Wi-Fi 无线网卡

在过去很多年，在购买 802.11 客户端 NIC 时，唯一的选择是标准 PC Card 适配器，这是许多笔记本电脑的外围设备。PC Card 类型由 PCMCIA 开发。PCMCIA 网卡也称 PC Card，如图 10-1 所示。PCMCIA 卡可以用于任何有 PC Card 插槽的笔记本电脑或手持设备。大多数 PCMCIA 卡内置集成天线，而一些卡同时具有内部集成天线和外部天线连接头。

图 10-2 所示的是另一种外置 802.11 无线射频卡类型：ExpressCard，这是一种硬件标准，用来取代 PCMCIA 卡。许多笔记本电脑厂商已经把 PCMCIA 插槽更换为较小的 ExpressCard 插槽。

感谢 Cisco Systems，Inc。未经授权，不得使用

图 10-1　PCMCIA 适配器/PC 卡

Courtesy of Belkin

图 10-2　ExpressCard 无线网卡

安全数码卡(SD)和 CompactFlash(CF)是常用在手持 PDA 上的两种无线射频卡格式。这些卡通常功耗很低，形状比火柴盒还小。CF 射频卡有时可以借助 CF-to-PCMCIA 的转换卡连接到笔记本电脑的 PC card 插槽。因为手持 PDA 和手持条码扫描器现在已经开始使用嵌入式的 802.11 射频卡，使用 SD、CF 格式的 PDA 目前已很少见了。

到目前为止，我们讨论的客户端网卡都是用在笔记本电脑或手持设备上的。802.11 客户端网卡也有用于台式机的 802.11 PCI 格式的网卡或 USB 网卡等形式。几乎所有的计算机都具有 USB 端口，因此 USB 格式的 802.11 无线网卡很受欢迎。USB 安装简单，也无需外接电源。802.11 USB 无线网卡有两种形式：类似电子狗形状的小型适配器(见图 10-3)或通过一条独立的电缆连接。第一种类型紧凑便携适用于笔记本电脑，第二种类型可以通过 USB 延长线与台式计算机相连，本身可以放置在桌面上。

图 10-3　802.11 USB 网卡

真实世界场景

外置无线网卡的优势

虽然大多数笔记本电脑都支持 Mini PCI、Mini PCI Express 或半高 Mini PCI Express 格式的无线网卡，但无法确保兼容性。使用 ExpressCards、PCMCIA 卡或 USB Wi-Fi 适配器的好处是便携并可以在不同的笔记本电脑上使用。因此无线局域网工程师通常使用 PCMCIA、ExpressCard 或 USB 格式的 802.11 无线网卡运行协议分析仪软件或现场勘测软件。这些应用通常需要特殊的驱动程序，这些驱动程序可能会覆盖原来的驱动，也可能与原来的驱动程序产生冲突。使用独立或外置的无线网卡进行现场勘测和排错通常是最佳做法，这时内置的无线网卡驱动可以保持不变。

2. 内置 Wi-Fi 无线网卡

多年来，之所以外置网卡成为标准，主要原因就是笔记本电脑没有内置 Wi-Fi 网卡。但现在大多数笔记本电脑和移动装置都会内置无线网卡。最初内置网卡的格式是 Mini PCI。Mini PCI 是外围组件互连(PCI)总线技术的变种，主要用于笔记本电脑。Mini PCI 射频模块经常用在无线接入点内部，同时也是制造商用在笔记本内部的 802.11 无线网卡射频模块的主要类型。Mini PCI Express 和更小的 Half Mini PCI Express 是下一代总线技术。今天的笔记本电脑几乎都会内置 802.11 Mini PCI 或 Mini PCI Express 无线射频卡(如图 10-4 所示)。Mini PCI 卡通常安装在笔记本电脑底部，之上连接小型分集天线并固定在显示器边缘。

图 10-4 Mini PCI 和 Mini PCI Express 无线网卡

3. 移动互联网设备

我们已经讨论了在笔记本电脑、PDA 和台式机上使用的 802.11 无线网卡类型。802.11 无线网卡还可用于许多手持设备，如条码扫描仪和 VoWiFi 电话。条码扫描仪(如图 10-5 所示的 Honeywell 设备)很多年来一直使用 802.11 无线模块。

虽然旧的手持设备没有使用前面提到的射频模块外形，大多数手持设备制造商的使用嵌入式的射频模块(通常是单芯片嵌入到主板)。图 10-6 显示了用在苹果 iPhone 手机上的单芯片 Broadcom Wi-Fi 射频模块。多年来，大部分人都认为只能使用笔记本电脑才能进行 Wi-Fi 连接。近年来，手持移动互联网设备(MID)(如智能手机和平板电脑)出现爆发式增长。现在大多数用户都期望手持移动互联网设备和笔记本电脑可以连接 Wi-Fi。当前几乎所有的 MID 都使用嵌入式芯片的形式。

应该注意到作为客户端设备使用的 802.11 无线射频(网)卡已经开始出现在许多新类型的机器和解决方案中。无线射频(网)卡已经用在许多游戏设备、立体声音响系统和摄像机产品中。设备制造商也在试验将 Wi-Fi 无线网卡安装到洗衣机和冰箱上。随着 802.11 射频模块变得更小、更便宜，应用程序和 Wi-Fi 技术的使用会持续爆发式的增长。

感谢 HONEYWELL 公司

图 10-5　条码扫描仪

图 10-6　内嵌式 802.11 射频模块

真实世界场景

网卡可在不同笔记本电脑上使用吗？

这个问题的答案完全取决于两件事：无线射频(网)卡类型和操作系统。PCMCIA 卡可以在任何有 PC CARD 插槽的笔记本电脑上使用。ExpressCard 可以在任何有 ExpressCard 插槽的笔记本电脑上使用。USB 客户端网卡可以在任何有 USB 端口笔记本电脑上使用。今天几乎所有的笔记本电脑都有 USB 端口、PC CARD 插槽或 ExpressCard 插槽。但在不同的笔记本电脑上使用相同的内部 MiniPCI 或 Mini PCI Express 无线射频卡情况会不一样。

无线电 Mini PCI 卡通常安装在笔记本电脑中，他们应该不会频繁地被插入或拔出，因此笔记本电脑制造商可能仅支持特定的 Mini PCI 或 Mini PCI Express 射频芯片组，换句通俗的话就是说：挑网卡。在更换 Mini PCI 射频卡之前应检查笔记本电脑制造商是否支持该硬件并需要提供相应驱动程序。并非所有的 Wi-Fi 客户端驱动都与操作系统和服务程序兼容。

10.1.2 无线射频(网)卡芯片组

一组被设计在一起工作的集成电路通常称为芯片组(chipset)。许多 802.11 芯片组厂商创造并向各射频卡制造商出售其芯片组技术。传统芯片组显然不支持较新的芯片组技术特性。例如，旧式芯片组可能只支持 802.11a/b/g 技术，而较新芯片组可以支持 802.11n 技术。

一些芯片组可能只支持在 2.4GHz ISM 频段，而有些芯片组既支持 2.4GHz 也支持 5GHz 频率。支持双频的芯片组用于 802.11a/b/g/n 客户端网卡。芯片制造商随着发展逐渐吸收了许多较新的 802.11 技术。许多私有技术出现在个别芯片组上，其中一些技术逐步成为日后 802.11 标准的一部分。

存在很多的芯片制造商，一些使用最广泛的芯片组的详细信息，可以通过以下网址查询：www.qca.qualcomm.com/、www.broadcom.com/或 www.intel.com。

10.1.3 客户端实用程序

最终用户可以通过一个软件配置界面，即客户端实用程序(client utilities)来配置客户端无线网卡。就像驱动程序是无线网卡与操作系统的接口，Wi-Fi 客户端实用程序实际上是无线网卡与你之间的软件接口。客户端实用程序通常可以创建多个连接配置文件。例如一个配置文件可以用于连接到工作网络，另一个用于连接到家庭网络，第三个可以连接到热点网络。

客户端实用程序的配置设置通常包括 SSID、传输功率、WPA/WPA2 安全设置、WMM QoS 和电源管理等。正如第 7 章所述，还可以配置客户端网卡处于 Infrastructure 或 Ad Hoc 模式。大多数优秀的客户端实用程序通常还会附带具有某种形式的统计信息显示工具和接收信号强度指标测量工具。

客户端实用程序存在以下三种主要类型：

- 操作系统集成的客户端实用程序
- 厂商客户端实用程序
- 第三方客户端实用程序

使用最广泛的客户端实用程序是集成在操作系统中的客户端工具。笔记本电脑用户最可能使用笔记本电脑操作系统内置的 Wi-Fi 网卡配置界面。不同操作系统的客户端实用程序有所不同。例如 Windows 7 的无线客户端实用程序就比 Windows XP 改善很多，Mac OS 10.6(Snow Leopard)与 Mac OS 10.7(Lion)的无线客户端实用程序也有区别。图 10-7 显示的 Windows 7 的客户端实用程序。某些操作系统(如 Mac OS 10.7)提供了 Wi-Fi 诊断工具，如图 10-8 所示。

图 10-7　Windows 7 内置客户端实用程序

图 10-8　Mac OS 10.7 WI-FI 诊断工具

手持设备操作系统通常也包含某种形式的 Wi-Fi 客户端实用程序。图 10-9 显示的是运行在 Apple iPad 和 iPhone 上的 iOS 5.0 的客户端实用程序界面。

厂商有时会提供特定的客户端实用程序。SOHO 客户端实用程序具有针对家庭用户的简单性和易用性。厂商特定的客户端实用程序通常用于外置无线网卡。近些年厂商特定的客户端程序也随着外置无线设备的减少而减少。企业级客户端实用程序为更加昂贵的企业级网卡提供了软件配置界面。通常情况下，企业级实用程序支持更多的配置功能，并具有更好的统

计功能。图 10-10 展示的是英特尔 PROSet 无线客户端界面(可用于具有英特尔 Wi-Fi 无线功能的 Windows 笔记本电脑)。

图 10-9 iOS 5.0 的客户端实用程序

图 10-10 企业级客户端实用程序

最后一种 802.11 无线网卡的软件配置界面是第三方的客户端实用程序，如 Juniper 公司的 Odyssey Access Client，如图 10-11 所示。与集成在操作系统上的客户端实用程序相同，第三方实用程序也可以支持不同厂商的无线网卡，使管理更加简便。第三方客户端实用程序通常支持许多种 EAP 类型，可以提供更广泛的安全选择。第三方客户端实用程序的主要缺点是通常需要付费。

图 10-11 第三方客户端实用程序

10.2　管理、控制和数据平面

通信网络通常定义了下面三种逻辑平面：

- 管理平面

  管理平面(management plane)指针对网络的管理和监控。可用于监视路由器、交换机和其他有线网络基础设施的网络管理解决方案就是管理平面的一个例子。集中式网络管理服务器可以下发网络设备配置并进行网络设备固件升级。

- 控制平面

  控制平面(control plane)由控制或信令信息组成，往往定义为网络智能或网络协议。用来转发数据的 3 层动态路由协议(如 OSPF 或 BGP)就是路由器中控制平面的一个例子。内容可寻址存储器(CAM)表和生成树协议(STP)是用于第 2 层交换机进行数据转发的控制平面机制。

- 数据平面

  数据平面(data plane)也称为用户平面，是在网络中实际转发用户流量的地方。转发数据包的路由器就是数据平面的一个例子。转发 802.3 以太网帧的交换机是数据平面的另一个例子。

在 802.11 环境中，这三个逻辑平面的操作功能是不同的，这取决于 WLAN 架构的类型和 WLAN 厂商。例如，在传统的自治型 AP 环境中，所有三个平面的操作共存在于每个独立的接入点(尽管它的控制平面机制极其简单)。当 WLAN 控制器解决方案在 2002 年首次推出后，所有三个平面的运行被转移到一个集中式设备。在现代部署，这些平面的操作可能会被分配到接入点、WLAN 控制器和无线网络管理服务器(WNMS)中。

在第 9 章中，我们讨论了三个主要 802.11 帧类型：管理帧、控制帧和数据帧。不要将管理平面、控制平面和数据平面与 802.11 MAC 帧的类型混淆。在这一章中所讨论的管理平面、控制平面和数据平面与 WLAN 网络架构运行有关。

10.2.1　管理平面

802.11 WLAN 的管理平面的功能包括：

- **WLAN 配置**。比如 SSID、安全、WMM 的配置、信道和功率设置。
- **WLAN 的监测和报告**。比如第 2 层统计信息，例如监测 ACK 帧、客户端关联、重关联、数据传输速率等。比如第三层监控和报告，例如 IP 连接、TCP 吞吐量、延迟统计、基于状态防火墙会话。
- **WLAN 固件管理**：将接入点和其他 WLAN 设备升级到最新版本的厂商操作程序。

10.2.2 控制平面

控制平面通常是为网络设备提供交互信息的协议。下面列举控制平面功能的几个例子：

- **动态射频功能** 协调多个接入点的信道和功率设置。大多数 WLAN 厂商都实现某种类型的动态射频功能。动态射频功能也称为无线资源管理(RRM)。
- **漫游机制** 漫游支持接入点之间的漫游切换机制。功能可能包括 L3 漫游、状态防火墙会话保持、缓冲数据包转发。快速安全漫游机制，比如机遇性密钥缓存(OKC)，也可以在接入点之间转发客户端的主加密密钥。
- **客户端负载平衡** 在接入点之间收集和共享客户端的负载和性能指标，以提高整体的 WLAN 业务。
- **Mesh 协议** 在多个接入点之间路由用户数据需要某种形式的 Mesh 路由协议。大多数 WLAN 厂商使用第 2 层的路由方式在网状接入点之间转发用户数据。然而也有一些厂商使用第 3 层的 Mesh 路由协议。802.11s 修正案定义了标准化的 Mesh 路由机制，但大多数 WLAN 厂商目前都使用专有方法。

10.2.3 数据平面

数据平面是转发用户数据的地方。通常参与数据平面的两个设备是 AP 和 WLAN 控制器。自治型接入点在本地处理所有数据转发工作。在 WLAN 控制器解决方案中，数据通常被集中转发到控制器，但也可以在网络边缘进行本地转发。厂商针对数据转发拥有独特的方法和建议。数据转发模型会在本章后面详细阐述。

10.3 WLAN 架构

随着 802.11 技术被企业逐渐接受，无线局域网体系结构的演进一直与之保持同步。802.11 技术的主要目的是为有线基础设施网络提供无线接入门户，有线和无线的集成方式也在持续变化。WLAN 厂商通常提供下面三种主要 WLAN 架构中的一种：

- 自治型 WLAN 架构
- 集中式 WLAN 架构
- 分布式 WLAN 架构

下面几节会对这三种架构进行更详细的阐述。

10.3.1 自治型 WLAN 架构

许多年来，传统的接入点被视为独立的 WLAN 门户设备，所有三个平面的工作都在此操作，这些 AP 通常称为胖 AP 或独立 AP。不过，传统接入点最常见的行业术语是自治型(autonomous)AP。

所有配置存储于自治型接入点本身，因此设备的管理和配置均由接入点处理。所有加密

解密和 MAC 层功能也由自治型接入点完成。你在第 7 章学习到的分布系统服务(DSS)和集成服务(IS)两个功能也是由自治型接入点完成的。因为所有用户数据都由每个独立的 AP 在本地完成，所以数据平面的功能也存在于自治型 AP 中。

如图 10-12 所描述的那样，传统的自治型 AP 之间很少共享控制平面机制信息。

图 10-12　自治型 WLAN 架构的简单组网

自治型接入点至少包含两个物理接口：通常是射频(RF)无线接口和 10/100/1000 自适应以太网端口。这些物理接口通过桥接虚拟接口(Bridge Virtual Interface，BVI)桥接在一起。BVI 会被分配由两个或多个物理接口共享的 IP 地址。

自治型接入点通常包括 802.11 协议栈和 802.3 协议栈。这些接入点可能包括以下功能：

- 多个管理界面，例如支持命令行、Web 图形用户界面和 SNMP 管理
- WEP、WPA 和 WPA2 安全功能
- WMM 服务质量功能
- 固定或可拆卸的天线
- 过滤选项，例如 MAC 过滤和协议过滤
- 连接模式，如 Root 模式、中继模式、桥接模式和扫描
- 可移除的无线射频卡
- 多射频卡和双频能力：2.4GHz 和 5GHz
- 可调节的传输功率和信道
- 支持 802.1Q VLAN
- 支持 IEEE 标准
- 支持 802.3af 或 802.3at POE

自治型接入点可能还具有下列高级功能：

- 内置 RADIUS 服务器和用户数据库
- 支持 VPN 服务器和/或 VPN 客户端
- DHCP 服务器
- 强制门户功能

自治型接入点通常部署在接入层，由接入层 PoE 交换机提供电力。内置在自治型接入点

中的集成服务将 802.11 帧转换为 802.3 帧。许多年来自治型接入点是无线局域网架构的基础。然而，大多数企业部署的自治型接入点已被更换为采用 WLAN 控制器和轻量型接入点的集中式架构解决方案。本章稍后部分将讨论该方案。

10.3.2 无线网络管理系统

对于使用无线局域网智能边缘架构的无线局域网，管理员面临的挑战之一就是管理。作为管理员，你希望单独配置 300 个自治型接入点吗？使用传统自治型接入点的一个主要缺点就是没有中央管理点。任何由 25 个或者更多自治型接入点组成的无线局域网体系结构都需要某种形式的无线网络管理系统(WNMS)。

WNMS 将管理平面从自治型 AP 中移出。WNMS 的主要目的是提供一个管理中心，配置和管理大量的自治型 AP。WNMS 可以是硬件设备或软件解决方案。WNMS 解决方案可能是厂商专用的或与厂商无关的。

提供中央管理功能是 WNMS 的主要目标，设备配置和固件升级可以推送到所有自治型接入点。WMNS 服务器部署在有线网络的核心层，与部署在接入层的自治型接入点通过 802.3 基础架构通信。尽管集中管理是 WNMS 的主要目标，但它也具有一些其他功能，如射频频谱规划和管理功能。WNMS 还可用于监控无线局域网架构，具备集成到单一管理控制台的集中报警和通知功能及网络报告、趋势分析、容量规划和策略执行功能。WNMS 还可以执行非法 AP 检测功能和 WIPS 功能。

WMNS 属于管理平面解决方案，不具备控制平面和数据平面功能。在 WNMS 和 AP 之间只有管理协议通信流量。大多数 WNMS 解决方案利用简单网络管理协议(SNMP)管理和监控无线局域网。有些 WNMS 解决方案使用 CAPWAP 作为监控和管理协议。

尽管用户流量从来不会由 AP 转发到 WNMS，802.11 客户端关联和流量信息仍然可以被监控。图 10-13 描述的是某个 WNMS 系统显示了关联到多个 AP 上的多个客户端。

图 10-13 WNMS 客户端监控

在过去，WNMS 服务器的全部功能就是提供一个对自治型接入点管理的中心点。近年来，

这个定义已经发生了变化。在本章的后面部分，你将了解到 WLAN 控制器，它被用作对轻量型接入点的管理中心点。WLAN 控制器有效地取代了 WNMS 服务器作为接入点管理中心点的位置。但是，当需要多个 WLAN 控制器进行大规模企业无线局域网部署时，大多数 WMNS 服务器可以用作对多个 WLAN 控制器的管理中心点。现在的 WNMS 服务器既可以用来管理一个厂商的多个 WLAN 控制器，也可以管理多个厂商的无线局域网基础设施，也包括自治型接入点。

10.3.3　集中式 WLAN 架构

无线局域网一体化发展的下一阶段是集中式 WLAN 架构。这种模式使用位于网络核心的中央 WLAN 控制器。在集中式的无线局域网体系结构中，基于控制器的接入点(controller-based access point)，也称轻量型接入点(或瘦接入点)取代了自治型接入点。从 2002 年开始，许多 WLAN 厂商决定采用所有三个平面操作都集中在控制器的 WLAN 控制器模式，这种模式带来了如下变化：

- **管理平面**：无线接入点由 WLAN 控制器管理和配置
- **控制平面**：动态射频、客户端负载均衡等由 WLAN 控制器完成
- **数据平面**：WLAN 控制器作为用户数据的分配点，所有 AP 将所有用户流量封装到隧道中，转发给中央控制器。

加密和解密能力可以由中央 WLAN 控制器完成，也可以由轻量型接入点完成，这取决于厂商的配置功能。第 7 章提到的分布系统服务(DSS)功能和集成服务(IS)功能现在都由 WLAN 控制器完成。而某些对时延敏感的操作仍由 AP 处理。

1. WLAN 控制器

集中式的无线局域网体系结构模型的核心是 WLAN 控制器(见图 10-14)。WLAN 控制器通常也称为无线交换机(wireless switch)，因为它们实际上是可以处理 OSI 模型数据链路层(第 2 层)数据的可管理的以太网交换机。许多 WLAN 控制器还是多层交换机，可以路由网络层(第 3 层)流量。不过，无线交换机这个称谓是一个过时的说法，不能充分描述 WLAN 控制器的功能。

图 10-14　集中式 WLAN 架构：WLAN 控制器

WLAN 控制器可能有下列功能：

- **AP 管理** 前面提到过，大多数轻量型接入点的功能(如功率、信道与支持的数据传输率)都由 WLAN 控制器配置。这样就允许集中管理和配置 AP。多数厂商在 WLAN 控制器和轻量型接入点之间使用专有通信协议。这些专有协议可以传输配置信息、进行固件更新并维护 keep-alive 状态流量。标准化的 WLAN 协议正逐渐被接受。许多 WLAN 厂商开始使用无线接入点控制和配置协议(CAPWAP)管理和监控接入点。
- **802.11 流量隧道** 大多数 WLAN 控制器的关键功能是可以在 WLAN 控制器内运行集成服务(IS)和分布系统服务(DSS)。换句话说，所有发送到有线网络资源的 802.11 流量必须首先通过无线控制器的集成服务(IS)转化为 802.3 流量后再发送到最终的有线端目的地。因此，轻量型接入点必须将 802.11 帧通过有线传输到 WLAN 控制器。

在第 9 章中我们了解到 802.11 帧格式很复杂，它只用于无线媒介，而不用于有线媒介。802.11 帧本身无法在 802.3 以太网络上传输。那么 802.11 帧如何在轻量型接入点和 WLAN 控制器之间的有线链路上传递？答案就是将其封装到 IP 隧道中。每个 802.11 帧都被完全封装到 IP 数据包内。许多无线局域网厂商使用通用路由封装协议(GRE)，这是一种常用的网络隧道协议。GRE 将 802.11 帧封装到在轻量型接入点和 WLAN 控制器之间的一条虚拟的点对点 IP 隧道中。有些无线局域网厂商不用 GRE IP 隧道，而使用其他私有隧道协议。CAPWAP 协议也可用来封装用户数据。

如图 10-15 所示，WLAN 控制器通常部署在核心层附近。轻量型接入点连接到提供 PoE 供电的第三方可管理交换机。AP 将 802.11 帧从接入层通过隧道转到核心层的 WLAN 控制器。控制器内的分布系统服务(DSS)指示流量传输，同时由集成服务(IS)将 802.11 数据帧中的 MSDU 封装到 802.3 帧中。在 802.11 数据帧被转成 802.3 帧后，就可以发送到位于有线网络的最终目的地了。

图 10-15 WLAN 控制器与 IP 隧道-核心层

大多数 WLAN 控制器部署在核心层，但也可以部署在分布层或接入层，WLAN 控制器

的部署位置取决于无线局域网厂商的解决方案和无线集成方案。多个 WLAN 控制器可能会部署在不同的层次并互相通信。

- **AP Group 配置文件**　AP Group 配置文件定义了单个接入点或一组 AP 的配置集。如信道、发射功率和支持数据传输速率等都可在 AP Group 配置文件中配置。一个接入点只能属于一个 AP Group，但可以支持多个 WLAN 配置文件。
- **WLAN 配置文件**　WLAN 控制器引入了虚拟 WLAN 的概念，通常也称为 WLAN 配置文件。WLAN 配置文件是一套 WLAN 控制器配置参数，参数可以包含无线局域网逻辑名称(SSID)、无线局域网安全设置、VLAN 分配和服务质量(QoS)参数。

无线局域网配置文件常与基于角色的访问控制(RBAC) 机制共同工作。用户在连接到虚拟 WLAN 后，会被分配一个特定角色。不要混淆 WLAN 配置文件与 AP Group 配置文件。单一接入点可以支持多个 WLAN 配置文件，但一个接入点只能属于一个 AP Group。

- **虚拟 BSSID**　在第 7 章中我们了解到每个无线局域网都有一个逻辑名称(SSID)，并且每个无线局域网的 BSS 都有独一无二的第二层标识符，即基本服务设置标识符(BSSID)。BSSID 通常是接入点的无线射频卡的 MAC 地址。WLAN 控制器具有创建多个虚拟 BSSID 的能力。正如前面学习到的，WLAN 控制器允许创建虚拟 WLAN，每个虚拟 WLAN 都有唯一的逻辑标识符(SSID)，并被分配特定的 VLAN ID。因为 BSSID 就是接入点的 MAC 地址，而且 WLAN 控制器可以支持在相同的物理接入点有许多虚拟 WLAN 网，所以通常会对每个虚拟 WLAN 分配不同的虚拟 BSSID。

如图 10-16 所示，虚拟 BSSID 通常是在射频卡的原始 MAC 地址基础上递增。如图 10-16 描绘的那样，每个轻量型接入点的覆盖范围内可以存在多个虚拟 WLAN。每个虚拟 WLAN 有一个 SSID 和 BSSID，并且每个无线局域网都映射到不同的 VLAN。换句话说，第 1 层域内可以存在多个第 2/3 层的域。可以试着想象存在多个映射到多个 VLAN 的 BSS 位于同一个 AP 的覆盖区域。

图 10-16　虚拟 WLAN、虚拟 BSSID 和虚拟局域网(VLAN)

- **VLAN** WLAN 控制器完全支持创建 VLAN 和 802.1Q VLAN 标记。WLAN 控制器支持创建多个无线用户 VLAN。支持创建用户 VLAN 是 WLAN 控制器的主要优势之一，因为 VLAN 可以提供分段和安全功能。VLAN ID 可以由 WLAN 配置文件静态指定，也可以使用 RADIUS 属性来指定。第 13 章会对无线 VLAN 进行更详细的论述。用户 VLAN 通常被封装到 IP 隧道中。
- **用户管理** WLAN 控制器通常可以提供控制谁、什么时候、在哪里可以访问的能力，即基于角色的访问控制(RBAC)机制。第 13 章会对 RBAC 进行更详细的讨论。
- **第 2 层安全支持** WLAN 控制器完全支持第 2 层的 WEP、WPA 和 WPA2 加密。认证功能包括内部数据库及与 RADIUS 和 LDAP 服务器的完全集成。
- **第 3 和第 7 层 VPN 服务器** 某些厂商的 WLAN 控制器可以作为 VPN 服务器或 PPTP、IPSec、SSL VPN 隧道的终结点。
- **强制门户(Captive Portal)** WLAN 控制器具有强制门户功能，可用于访客无线局域网。强制门户对用户进行身份验证，但加密功能非常有限，所以它很少用于访客访问网络以外的其他地方。
- **自动故障切换和负载均衡** 出于冗余目的，WLAN 控制器通常支持虚拟路由器冗余协议(VRRP)。大多数厂商还提供在多个轻量型接入点之间进行无线客户端负载均衡的专有功能。
- **内部无线入侵检测系统** 出于安全监测的目的，某些 WLAN 控制器还具有集成的 WIDS 功能。关于 WIDS 更详细的讨论请见第 14 章。
- **动态射频频谱管理** 大部分 WLAN 控制器具备动态调整射频的能力。WLAN 控制器可以从 AP 的射频卡上收集射频信息，动态地更改 AP 的配置。在 WLAN 控制器环境中，AP 监视各自信道，并通过信道外扫描(off-channel)监视其他信道频率。任何由接入点监听到的射频信息都会被汇总到 WLAN 控制器。基于来自多个 AP 的 RF 监测信息，WLAN 控制器能够动态设置 AP 的射频信息，如更改频点和发射功率。

动态射频功能有时也称为射频资源管理(RRM)。标准化的 RRM 机制已经被定义，但所有 WLAN 控制器厂商都使用私有的动态 RF 功能。动态射频功能可以提供蜂窝大小自动调整、自动监控、射频环境优化功能和故障排除功能，构建一种自组织、可自愈的无线局域网。

- **带宽管理** 带宽管道可以控制上传或下载速率。
- **防火墙能力** 某些 WLAN 控制器可以通过内置的防火墙实现基于状态的数据包检测功能。
- **第 3 层漫游支持** 完全支持跨第 3 层路由边界的无缝漫游。第 3 层漫游和 Mobile IP 标准在第 12 章会进行更详细的讨论。
- **以太网供电(PoE)** WLAN 控制器部署在接入层时可以为轻量型接入点提供直接的电源供应(PoE)。但大多数接入点由第三方的边缘交换机提供电力。
- **管理接口** 许多 WLAN 控制器提供常见的管理接口支持，例如图形用户界面、CLI 和 SSH 等。

WLAN 控制器集中式体系结构最明显的优势包括 AP 管理、用户监控、动态射频和集中式的数据分发。WLAN 控制器模式的另一个重要优势是支持快速安全漫游，这可以协助解决

在加密无线网络中漫游产生延迟的问题。

WLAN 控制器缺点之一是可能成为数据转发瓶颈，因为所有数据都必须发送到 WLAN 控制器，再由 WLAN 控制器重定向。大多数厂商可以通过提供一个可扩展的分层环境阻止这种情况发生，这会在本章后面进行讨论。QoS 策略可在 WLAN 控制器执行，如果配置不当也可能导致延迟问题。WLAN 控制器和瘦 AP 之间可能并非直连，这也可能引入网络延迟。WLAN 控制器有太多的功能和配置，以至于新手会对用户配置界面感到困惑。

2. 分离 MAC 功能

大部分 WLAN 控制器厂商提供分离 MAC 架构(Split MAC architecture)。在这种类型的 WLAN 架构之下，一部分 MAC 服务功能由 WLAN 控制器处理，一部分由轻量型接入点处理。例如，控制器负责处理集成服务、分布系统服务，WMM QoS 功能通常也由控制器完成。对 802.11 数据帧的加密和解密过程可以由控制器负责处理，也可由 AP 处理，具体取决于无线厂商。

802.11 帧被封装在瘦 AP 和 WLAN 控制器之间的隧道中，再传输到控制器。因为 WLAN 控制器上的集成服务需要将 802.11 数据帧第 3～7 层的有效净荷转换成 802.3 帧，需要为 802.11 数据帧有效载荷提供到网络资源的网关。802.11 的管理和控制帧没有上层净荷，因此永远不会转换成 802.3 帧。802.11 管理帧和控制帧也不一定需要通过隧道传输到 WLAN 控制器，因为控制器不需要为这些类型的 802.11 帧提供访问网络资源的网关。

在分离 MAC 架构中，许多 802.11 管理帧和控制帧通常只在客户端和瘦 AP 之间进行交互，一般不会通过隧道方式发送到 WLAN 控制器。例如信标帧、探询响应帧和 ACK 帧可能由瘦 AP 而不是控制器产生。应当注意的是大多数厂商使用不同的分离 MAC 架构。IETF 提出一种称为“无线接入点控制与配置协议”(CAPWAP)的 WLAN 控制器协议标准，在其中也有分离 MAC 标准的定义。

可在 IETF 的网站 www.ietf.org/html.charters/capwap-charter.html 找到有关“无线接入点控制和配置协议”(CAPWAP)标准的详细信息。

3. 控制器数据转发模式

正如前面提到的，集中式的 WLAN 架构通常是指 WLAN 控制器存在数据平面，此时所有的用户流量由 AP 进行 IP 封装发送到 WLAN 控制器。但是，WLAN 控制器也有两种类型的数据转发模式：

- 集中式数据转发

所有数据由 AP 集中转发到控制器进行处理，许多场景会使用这种模式，尤其是当需要由控制器进行加密解密或需要安全和 QoS 策略时。

- 分布式数据转发

所有数据由 AP 在本地进行转发，这种方式适于在边界进行转发，并且可以避免因为集中处理数据可能要求更高的处理能力和内存容量问题。

如图 10-17 所示，集中式数据转发要求 AP 与控制器建立 IP 隧道，由控制器完成数据转

发，在这种模式下，AP 在数据转发方面处于被动角色。

图 10-17 集中式数据转发

图10-18 中描述了分布式数据转发场景。图中 AP 负责决定用户数据在哪里和如何进行转发，而控制器并没有参与这些过程。同时数据的 QoS 应用和加密策略也由 AP 完成。一般来说，处理大部分 MAC 功能的设备也可能处理数据转发。到底是采用分布式还是集中式转发模式基于很多因素，如安全性、VLAN 和吞吐量。采用分布式数据转发的一个主要缺点就是某些控制平面机制无法工作，因为这些控制平面功能位于控制器。这些控制平面机制可能包括动态射频调整、三层漫游、防火墙策略及快速安全漫游。

图 10-18 分布式数据转发

802.11n 在大型企业网络中逐步流行开来，考虑到 WLAN 生成的流量负载，集中式转发模式变得更难实现。WLAN 控制器厂商正在通过多种不同方式使用分布式数据转发。

4. 远程办公室 WLAN 控制器

虽然 WLAN 控制器通常部署在网络核心，但也可以将它们部署在接入层，这通常是指远程办公室的无线局域网控制器，如图 10-20 所示。远程办公室 WLAN 控制器通常比核心 WLAN 控制器处理能力要弱，但是价格便宜。远程办公室 WLAN 控制器的目的是允许从单一位置对远程和分支办公室进行管理。远程 WLAN 控制器通常与中央 WLAN 控制器跨广域网链路进行通信。控制器之间安全的 VPN 隧道功能通常也可以跨广域网实现。通过 VPN 隧道，中央控制器将配置下发到远程 WLAN 控制器，然后远程控制器便可以控制并管理本地 AP。这些远程控制器可以控制的轻量型 AP 数量有限。功能通常包括以太网供电、内部防火墙和集成 NAT 和 DHCP 功能的路由器功能。

10.3.4　分布式 WLAN 架构

近来有个发展方向是从集中式 WLAN 控制器架构转向到分布式 WLAN 架构。某些 WLAN 厂商(如 Aerohive)设计了完整的分布式 WLAN 架构。这些架构采用协作式的自治型 AP，控制平面机制通过协作协议在 AP 间运行。这种架构无需控制器，而是将自治型 AP 与协作协议结合在一起。这种分布式 WLAN 架构有些类似于传统的交换和路由设计模型，采用独立的分布式算法，同时可以协同工作提供控制平面功能。

如图 10-19 所示，协作协议将独立 AP 组织起来共享控制平面信息，提供二层漫游、三层漫游、防火墙、协作射频管理、安全和 Mesh 功能。分布式架构的最佳描述就是：具有大多数 WLAN 控制器功能的自治型 AP 的组合。控制平面功能由使用私有协议的 AP 共享。

图 10-19　分布式 WLAN 架构

分布式架构中的每个 AP 独立负责本地的用户流量转发。正如前面提到的，随着 802.11n 时代的到来，WLAN 控制器厂商也开始提供分布式解决方案处理流量负载。因为分布式 WLAN 架构中完全去除了控制器，所以所有的用户流量由 AP 在本地独立处理。在分布式架

构中，数据平面位于 AP 内部，不存在无线控制器，因为数据无需通过隧道到达网络核心。

尽管数据和控制平面已经交由 AP 处理，但是管理平面仍然保持集中。AP 的配置和监控仍由 WNMS 服务器处理。

尽管不存在控制器，大多数可以由 WLAN 控制器完成的功能也可以由分布式 WLAN 系统完成，例如强制门户功能、基于状态的防火墙功能和 RBAC 功能。漫游机制和动态射频功能也可以协同工作。如前所述，所有控制平面机制位于分布式 WLAN 体系结构网络边缘的接入点中，另外 AP 使用私有的协作协议来完成控制平面功能。基于控制器的模型与无控制器模型的最大区别就是 VLAN 的变化。在控制器模型中，因为所有的用户流量均通过隧道集中封装转发，基于控制器的 AP 通常连接在接入层交换机的某一个 VLAN。而非控制器模型要求在网络边界支持多个 VLAN，因此 AP 需要连接在接入层交换机的 802.1Q 中继端口以支持多个 VLAN 标记。

尽管协作分布式的 WLAN 模型没有集中转发用户流量到核心，但 AP 也可以具备 IP 隧道能力。某些 WLAN 用户不希望访客流量进入内网，AP 可以与位于 DMZ 区的 AP 建立 IP 隧道，将访客流量通过隧道发送至 DMZ 区。AP 还可以作为 VPN 客户端或服务器与 WAN 另一端的 AP 建立 IPSec 加密隧道。

10.3.5 统一无线局域网结构

这是另一种非常好的无线局域网体系结构发展方向，将 WLAN 控制器功能完全集成到有线网络基础设施。处于核心或边缘的有线网络的交换机和路由器也可以具备 WLAN 控制器功能，从而允许对无线和有线网络进行统一管理。一些厂商已经开始部署这种统一体系结构，并将可能随着无线局域网部署变得更加普及和无缝集成的需求继续攀升，这种架构的接受程度会逐渐提高。

10.4 专业无线局域网基础设施

前几节中讨论了将 802.11 无线网络融入有线网络体系结构的无线局域网网络基础设施设备的进展。除了接入点和 WLAN 控制器以外，Wi-Fi 市场还产生了许多专业无线局域网设备。目前许多这类设备(如网桥和 Mesh)非常普遍，尽管他们运作在 802.11 标准之外。下面将介绍这些设备。

10.4.1 无线工作组网桥

工作组网桥(WGB)是为没有无线射频卡的有线基础设施设备提供无线连接的设备。WGB 内的无线射频卡与接入点关联，并作为一个客户端加入基本服务集(BSS)。如图 10-20 所示，WGB 有线侧后面连接多个以太网设备。WGB 通过与接入点关联，为有线设备提供了快速的无线连接。因为 WGB 就是一个与接入点相关联的客户端，所以不允许其他无线客户端接入。另外要注意，WGB 内只有无线射频卡可以参与竞争 802.11 无线媒体，WGB 后面的有线网卡

不能参与竞争半双工的射频媒介。

图 10-20　无线工作组网桥

大多数无线工作组网桥可以连接多达 8 个有线设备，但这取决于厂商。一些 WGB 只能连接一个有线设备，有时也称为通用客户端(universal client)。工作组网桥在为小型桌面工作组、收银机、网络打印机、其他任何有以太网端口的设备提供无线连接方面非常有用。目前 WGB 的需求大大减少，因为 802.11 射频卡正在取代许多客户端设备中的以太网卡。

10.4.2　无线局域网网桥

一种常见的非 802.11 技术标准的部署设备是无线局域网网桥(wireless LAN bridge)。桥接的目的是在两个或更多有线网络之间提供无线连接。网桥通常支持自治型接入点所支持的所有功能，但其目的是将连接有线网络，并不提供客户端的无线连接。虽然有时在室内也使用网桥，但通常它们用于室外，通过无线连接两个建筑物内部的有线网络。户外网桥经常用作建筑物之间的 T1 或光纤链路的冗余备份，甚至用来替代建筑物之间的 T1 或光纤连接，因为它们实实在在节省了开销。

无线网桥支持两种主要的配置：根网桥(Root)和非根网桥(Nonroot)。网桥之间是一种父与子类型的工作关系，处于根模式的网桥作为父网桥，非根网桥作为子网桥。

只连接两个有线网络的网桥，被称为点对点(PtP)网桥。图 10-21 显示了使用 802.11 网桥和定向天线连接两个有线网络的点对点连接。请注意，一个网桥必须配置为父根网桥，另一个必须配置为子非根网桥。

图 10-21 点到点无线局域网网桥

点到多点(PtMP)网桥连接多个有线网络。根网桥是中央网桥，多个非根网桥连接到根网桥。图 10-22 显示了四个建筑物之间的 PtMP 网桥。请注意，根桥使用高增益全向天线，而非根网桥均使用定向天线指向根网桥。此外还请注意 PtMP 连接中只有一个根网桥，永远不会有多个根网桥。

图 10-22 点对多点无线局域网桥接

网桥除了根网桥与非根网桥模式以外，还有其他配置模式：

- AP 模式(AP mode)
  转换网桥为接入点模式
- WGB 模式(WGB mode)
  转换网桥到工作组网桥模式
- 中继模式(Repeater mode)
  对根网桥的无线信号进行中继使其到达非根网桥

- 允许客户端关联的根网桥模式(Root with clients)
  根网桥允许客户端关联
- 允许客户端关联的非根网桥模式(Nonroot with clients)
  非根网桥允许客户端关联

绝对不推荐使用允许客户端关联的根网桥与非根网桥模式。如果允许客户端连接到网桥，可能使网络资源容易受到攻击，面临安全风险。客户端还会影响网桥链路的吞吐量，因为客户端增加了媒介竞争的开销。同样因为性能问题，Repeater 模式也不被推荐用在无线桥接中。如果可能，更好的网桥部署做法是使用两段独立的网桥链接，而不是采用在根网桥和非根网桥之间采用 Repeater 的方式。

在室外桥接部署时，需要考虑的因素很多，包括菲涅耳区、地球曲率、自由空间路径损耗、链接预算和衰减容限。可能还需要注意所在国家或地区的监管机构制定的 IR 和 EIRP 功率规定。

2.4GHz 频带的点对点链路可能长达 24 英里。超长距离的链路上可能出现 ACK 超时的问题。由于媒介的半双工的特性，每个单播帧都必须得到确认。因此，在一段长达 24 英里的链路上发送的单播帧必须立即从对面的网桥收到 ACK 帧，这个帧也要从相同距离的位置处发出。即使射频以光速传输，可能也无法以足够快的速度得到 ACK。如果发送端网桥在一段单位为微秒的时间内没有收到 ACK 帧，就会超时，并假定数据帧已发生冲突。发送端网桥将重新传输这个单播帧，即使前一个单播帧的 ACK 帧正在传输途中。重发本无须重发的单播流量，可能会导致高达 50%的吞吐量下降。要解决这个问题，大多数网桥都有 ACK 超时的设置，可以调整长距离链路接收 ACK 帧的超时时间。

点对多点的桥接一个常见的问题，使用高增益全向天线的根桥位置过高，如图 10-23 所示。结果会导致使用定向天线的非根网桥的垂直视距不足。这个问题可以通过使用具有电调下倾角度功能的高增益全向天线或使用可以提供全向覆盖的定向扇形天线解决。

图 10-23　常见的网桥问题

10.4.3　家用无线路由器

家用无线路由器(Home Wi-Fi Router)的主要功能是向 SOHO 网络提供互联网连接的无线共享接入，同时提供一定级别的互联网安全。这些 SOHO Wi-Fi 路由器通常价格低廉，但令人吃惊地具备很丰富的功能。

家庭无线路由器支持以下功能：

- 可配置的 802.11 无线射频卡
- 支持简单路由协议(如 RIP)
- 网络地址转换(NAT)
- 端口地址转换(PAT)
- 端口转发
- 防火墙
- 第二层安全支持(WEP 或 WPA-Personal 或 WPA2-Personal)
- DHCP 服务器
- 多端口以太网交换机(用于连接有线客户端)

请记住，任何类型的无线路由器都与接入点设备有很大区别。不像接入点使用桥虚拟接口(BVI)，无线路由器使用单独的路由接口。无线射频卡属于一个子网，而连接 WAN 的以太网端口属于另一个子网。尽管 Wi-Fi 路由器通常用于家庭，但有些 WLAN 厂商开始生产 Wi-Fi 路由器用于小型企业或者远程分支机构。随着无线网络和有限网络界限的模糊，企业级别的 Wi-Fi 路由器使用量也开始快速增加。

大多数 CWNA 考生都很熟悉家庭无线路由器，因为可能各自家中就装了一个。

10.4.4 无线局域网 Mesh 接入点

几乎所有的 WLAN 厂商都提供无线局域网 Mesh 接入点(mesh access point)。无线网接入点使用专有的第二层路由协议相互沟通，创建自行组建和自我修复的无线基础设施(Mesh)，边缘设备可以在之上进行通信，如图 10-24 所示。

图 10-24 无线局域网 Mesh

自组 Mesh 网络可以自动连接 Mesh AP 并在客户端加入时动态更新路由。因为可能出现干扰，可自我修复的 Mesh 网络会自动在 Wi-Fi 网格中重路由数据流量。私有的第二层智能路由协议基于流量、信号强度、跳数和其他参数确定动态路由。尽管 Mesh 网可能由运行在同一频率的类似于中继的接入点构成，但支持双频的 Mesh AP 现在更常见。双频段的无线局域网 Mesh 接入点通常利用 5GHz 频段射频模块提供回传，利用 2.4GHz 频段射频模块提供客户端接入。

10.4.5　无线局域网阵列

Xirrus 公司提供了一种专有解决方案，它将 WLAN 控制器和多个接入点结合成一个硬件设备，称为 Wi-Fi 阵列。CWNP 认证使用通用术语*无线局域网阵列*(WLAN array)来描述这一技术。如图 10-25 所示，多达 16 个使用扇形天线的接入点射频模块和嵌入式 WLAN 控制器共存在一台设备中。这个 WLAN 控制器显然部署在访问层，因为该设备安装在天花板上。嵌入式 WLAN 控制器提供与多数传统的 WLAN 控制器相同的功能。

特此鸣谢 XIRRUS 公司

图 10-25　无线局域网阵列

无线局域网阵列的关键点之一就是每个接入点都有扇形天线提供定向的覆盖范围。因此每个接入点提供一个扇形的覆盖范围。简单说来无线局域网阵列就是结合所有扇形接入点的单向覆盖范围提供 360 度全方位水平覆盖的室内扇形阵列解决方案。每个接入点的单向覆盖增加了覆盖范围，就像室外扇形阵列一样。无线局域网阵列中的射频模块的数量取决于型号和配置。无线局域网阵列可能有四个 AP 射频卡、八个 AP 射频卡甚至多达 16 个 AP 射频卡。一个拥有 16 个接入点的无线局域网阵列包括四个 2.4GHz 射频卡和十二个 5GHz 射频卡。这些射频卡其中之一可以作为专用的 WIDS 探测器，嵌入在控制器中。

无线局域网阵列解决方案的一个主要优点是只有很少的物理设备需要部署；因此，需要安装和管理的设备的数量也大大减少。无线局域网阵列也适用于高用户密度环境。

10.4.6 虚拟接入点系统

有几家无线局域网厂商提供被称为虚拟接入点(Virtual AP)的解决方案。虚拟接入点解决方案使用多个接入点但共享一个基本服务集标识符(BSSID)。因为多个接入点只宣告一个虚拟 MAC 地址(BSSID)，客户端会认为它们只连接到一个接入点上，尽管它们实际可能在多个物理接入点间漫游。这种解决方案的主要优点是客户端经历零切换时间(Zero handoff)，许多与漫游相关的延迟问题得以解决。所有切换和管理都由中央无线局域网交换机完成。虚拟接入点解决方案还使用了独特的无线局域网拓扑，称为单信道体系结构(SCA)。在 SCA 中接入点在相同的信道上传输，但由控制器统一协调通话时间。无线局域网厂商(如 Meru 和 Extricom)在 802.11-2007 标准约束下使用这种非常有创意的专有方法来提供虚拟的接入点和 SCA 架构。

有关单信道体系结构(SCA)和多信道体系结构(MCA)的部分会在第 12 章中详细讨论。

10.4.7 实时定位系统

WLAN 控制器和 WIDS 解决方案有一些集成功能，利用接入点作为传感器对 802.11 客户端进行跟踪。不过，它们提供的是接近实时(Near-time)的解决方案跟踪能力，精确度可能只有约 25 英尺，不能跟踪 Wi-Fi RFID 标签。AeroScout 和 Ekahau 等几家公司提供无线局域网实时定位系统(RTLS)，它可以跟踪任何 802.11 无线设备，包括主动 Wi-Fi RFID 标签，而且定位精度更高。覆盖式的无线局域网实时定位系统解决方案的组件包括已经存在的无线局域网基础设施、已经存在的无线局域网客户端、Wi-Fi RFID 标签和实时定位系统服务器。此外还可以添加额外的无线局域网实时定位传感器作为已经存在的无线局域网接入点的补充。

主动 RFID 标签和(或)标准 Wi-Fi 无线设备会按一定的时间间隔定期传输简要信息，这些信息中包含状态信息或传感器数据。图 10-26 显示的是附加在医院医疗静脉泵设备上的 RFID 标签。无需对基础结构做任何改变，这些信号被标准的无线接入点(或实时定位传感器)接收并被发送到位于核心的 RTLS 服务器的处理引擎。RTLS 服务器使用信号强度和(或)到达时间算法(TOA)来确定位置坐标。

特此鸣谢 AEROSCOUT 公司

图 10-26　主动 802.11 RFID 标签

如图 10-27 所示，一个软件应用程序界面用于查看建筑物平面图上的位置和状态数据。实时定位系统可以显示地图、启用搜索、自动报警、资产管理并可与第三方应用程序集成。

特此鸣谢 AEROSCOUT 公司

图 10-27　实时定位系统应用

10.4.8　Wi-Fi 语音

VoIP 通信已经在有线网络上存在多年。不过，在 802.11 无线局域网上使用 VoIP，因为射频环境和 QoS 的考虑，面临很多挑战。近年来，Wi-Fi 语音(VoWiFi)解决方案的需求大大

增加。无线局域网在提供所有数据应用程序使用的同时，也在同一无线局域网基础架构下提供语音通信服务。部署 VoWiFi 解决方案所需的组件包括以下内容：

VoWiFi 电话 VoWiFi 电话与手机类似，除了前者是 802.11 射频模块，后者是手机无线蜂窝模块。VoWiFi 电话是一个与接入点进行通信的 802.11 客户端，完全支持 WEP、WPA、WPA2 加密和 WMM QoS。图 10-28 展示的是 Polycom 公司的 SpectraLink 8030 VoWiFi 电话，其支持 802.11a/b/g，可以在 2.4GHz 频段或 5GHz 频段工作。VoWiFi 技术也可以用在除电话以外的形式。图 10-29 展示的图片是 VoWiFi 厂商 Vocera 销售的一款 802.11 通信传呼机，其可佩戴且重量不到两盎司。Vocera 的传呼机也是一款全功能的 VoWiFi 手机，此外还可以使用语音识别和声纹验证软件。当前大多数 VoWiFi 解决方案使用 SIP 协议作为 IP 语音通信协议。

特此鸣谢 POLYCOM 公司

图 10-28 VoWiFi 电话(SpectraLink8030)

特此鸣谢 VOCERA 公司

图 10-29 Vocera 通信传呼机

802.11 基础设施(接入点和控制器) 已存在的无线局域网基础架构提供 VoWiFi 与接入点之间的通信。自治型接入点和(或)WLAN 控制器解决方案都可以用。

PBX 专用分组交换机(PBX)用于为特定的业务或办公室提供电话交换。PBX 用于提供公司内部电话连接，还可以通过中继线路将内部电话连接到公共交换电话网(PSTN)。PBX 提供拨号音并可提供其他功能(如语音邮件)。

WMM 支持 前面几章已经提过，需要 WMM 支持 QoS。

10.5 小结

本章讨论了不同类型的射频卡类型、它们使用的芯片组和用于客户端配置的软件界面。还叙述了无线局域网设备的逻辑发展进程，从自治型接入点到 WLAN 控制器，再到分布式架构的方向。此外，我们介绍了一些专业无线局域网基础设施设备，这些设备可以完成其他

传统的无线局域网架构无法完成的功能。

本书作者建议在参加 CWNA 考试之前，获取一些针对某些无线局域网基础设施设备的实际操作经验。我们清楚大多数个人负担不起高达一万美金的价格昂贵的核心级 WLAN 控制器；但是我们建议你至少购买一块 802.11a/b/g 网卡和自治型 AP 或 SOHO 无线路由器。动手体验将巩固你在这章以及本书其他章节学习到的知识。

10.6　考试要点

了解主要无线射频卡类型。802.11 标准不要求 802.11 无线射频卡具体使用哪种类型。802.11 射频卡具有多种格式。

了解客户端网卡有操作系统接口和用户接口要求。客户端网卡需要特殊的驱动程序与操作系统通信，需要软件客户端实用程序用于用户配置。

识别三种主要类型的客户端实用程序。三种类型的客户端实用程序是企业级、集成在操作系统内的及第三方的。

定义三种逻辑操作平面。理解管理、控制和数据平面的区别。能够解释在不同的 WLAN 架构中的使用区别。

解释无线局域网体系结构的发展。能够解释自治型接入点、WLAN 控制器和分布式 WLAN 架构的异同。

了解所有传统无线局域网基础设施设备的功能。理解自治型接入点的功能。解释自治型接入点与基于控制器的接入点之间的差别。

理解 WLAN 控制器解决方案的功能。理解 WLAN 控制器解决方案提供的所有功能。能够解释 IP 隧道、分离 MAC 体系结构、虚拟 BSSID、无线局域网配置文件及动态射频功能。

解释无线局域网网桥和工作组网桥的角色和配置。CWNA 考试在网桥这块覆盖相当广泛。知道网桥所有的类型及根网桥和非根网桥之间的区别。能够解释点对点与点对多点网桥之间的差异。了解无线桥接故障问题，例如 ACK 超时，并研究本书其他章节针对网桥所需要考虑的问题，如菲涅耳区和系统操作容限(SOM)。

解释其他无线局域网专业基础设施。能够解释 RTLS 解决方案和 VoWiFi 解决方案如何与 WLAN 集成。解释其他非传统 WLAN 解决方案，如 WLAN 阵列。

10.7　复习题

复习题的答案见附录 A。

1. What type of 802.11 radio form factor is normally used in mobile Internet devices (MIDs)?
   A. Integrated single chip
   B. PCMCIA

C. Express MiniPCI

D. Mini PCI

E. Secure Digital

2. How many root bridges exist in a point-to-multipoint bridge link?

A. None

B. One

C. Two

D. Multiple

E. All of the above

3. Which radio formats can be used by 802.11 technology?

A. CF

B. Secure Digital

C. PCMCIA

D. Mini PCI

E. ExpressCard

F. Proprietary

G. All of the above

4. Which type of access points normally use centralized data forwarding?

A. Autonomous AP

B. Controller-based AP

C. Cooperative AP within a distributed WLAN architecture

D. None of the above

5. What capabilities can be found on a WLAN controller? (Choose all that apply.)

A. VRRP

B. Captive portal

C. HSRP

D. RBAC

E. Wireless intrusion detection system

6. Which protocols are used to transport 802.11 frames between a controller-based AP and a WLAN controller? (Choose all that apply.)

A. GRE

B. CCMP

C. Mobile IP

D. CAPWAP

E. Proprietary IP tunneling protocols

F. All of the above

7. Which of these WLAN architectures may require the use of a WNMS server to manage and monitor the WLAN?

A. Autonomous WLAN architecture

B. Centralized WLAN architecture

C. Distributed WLAN architecture

D. All of the above

8. What are some of the common capabilities of a WLAN controller architecture?

A. Dynamic RF

B. AP management

C. Layer 3 roaming support

D. Bandwidth throttling

E. Firewall

F. All of the above

9. Which logical plane of network operation is typically defined by protocols and intelligence?

A. User plane

B. Data plane

C. Network plane

D. Control plane

E. Management plane

10. Which option best describes a device used to provide wireless connectivity for a small number of wired clients?

A. VPN router

B. Wireless workgroup bridge

C. Wireless mesh router

D. Wireless Ethernet repeater

E. Wireless bridge

11. What are the two main components of a centralized WLAN architecture? (Choose all that apply.)

A. WLAN controller

B. Wireless network management system

C. Enterprise wireless gateway

D. Cooperative control AP

E. Controller-based AP

12. What planes of operation reside in the access points of a distributed WLAN architecture? (Choose all that apply.)

A. Radio plane

B. Data plane

C. Network plane

D. Control plane

E. Management plane

13. A network administrator is having a hard time getting two WLAN bridges to associate with one another in a PtP link. The bridge in building A is on the 172.16.1.0/24 network, and the bridge in building B resides on the 172.16.2.0/24 network. What is the most likely cause?

A. The bridges are on different subnets.

B. The bridges are both configured as nonroot.

C. The gateway address is incorrect.

D. The ACK timeout setting is short.

E. There is impedance overflow.

14. Billy must connect building A via a WLAN bridge link to building C, which is 30 miles away. He cannot make a direct connection of that distance because of regulatory power restrictions in his country. Building B sits between the two remote buildings. What is the best way for Billy to link the two buildings together using WLAN bridges?

A. Place a root bridge on building A with a highly directional antenna, a nonroot bridge on building B with an omnidirectional antenna, and a root bridge on building C with a highly directional antenna.

B. Place a root bridge on building A with a highly directional antenna, a repeater bridge on building B with an omnidirectional antenna, and a root bridge on building C with a highly directional antenna.

C. Place a nonroot bridge on building A with a highly directional antenna, a root bridge on building B with an omnidirectional antenna, and a nonroot bridge on building C with a highly directional antenna.

D. Place a root bridge on building A with a highly directional antenna, and a nonroot bridge on building B with a highly directional antenna. Set up another root bridge on building B with a highly directional antenna, and a nonroot bridge on building C with a highly directional antenna. Connect the two bridges on building B via a switch or router.

E. None of the above.

15. Which WLAN architectural models typically require support for 802.1Q tagging at the edge on the network when multiple user VLANs are required? (Choose all that apply.)

A. Autonomous WLAN architecture

B. Centralized WLAN architecture

C. Distributed WLAN architecture

D. None of the above

16. What term best describes a WLAN centralized architecture where the integration service (IS) and distribution system services (DSS) are handled by a WLAN controller while generation of certain 802.11 management and control frames are handled by a controller-based AP?

A. Cooperative control

B. Distributed data forwarding

C. Distributed hybrid architecture

D. Distributed WLAN architecture

E. Split MAC

17. Where is redundancy needed if user traffic is being tunneled in a centralized WLAN architecture?

A. Redundant radios

B. Redundant controllers

C. Redundant access switches

D. Redundant access points

E. None of the above

18. What would be needed for multiple basic service sets (BSSs) to exist within the same coverage area of a single access point and in which all the client stations would be segmented in separate layer 2 and 3 domains but all communicate within a single layer 1 RF domain? (Choose all that apply.)

A. Virtual BSSIDs

B. SSIDs

C. VLANs

D. Autonomous APs

E. None of the above

19. What are some of the parameters of a WLAN profile that can be configured on a WLAN controller? (Choose all that apply.)

A. SSID

B. Channel

C. VLAN

D. WMM

E. WPA-2

20. What are some of the necessary components of a VoWiFi architecture? (Choose all that apply.)

A. VoWiFi phone

B. SIP

C. WMM support

D. Proxy server

E. PBX

第11章 无线局域网部署和垂直市场

在该章中，你将学习以下内容：

- √ 常见无线局域网应用与设备部署注意事项
  - 数据
  - 语音
  - 视频
  - 实时定位服务(RTLS)
  - 移动设备(平板电脑与智能手机)
- √ 企业数据接入与终端用户的移动性
- √ 网络延伸到远端
- √ 建筑物之间的桥接
- √ 无线运营商(WISP)——最后一英里的数据交付
- √ 小型办公室/家庭办公(SOHO)
- √ 移动办公网络
- √ 教育/教室使用
- √ 工业——仓储和制造
- √ 医疗保健——医院与办公室
- √ 市政网络
- √ 热点——公共网络接入
- √ 交通网络
- √ 执法网络
- √ 快速应急网络
- √ 固网与移动网的融合
- √ 无线局域网和健康
- √ 无线局域网供应商

本章将介绍一些典型的无线网络部署环境，并将考查在不同环境下无线技术的利弊以及需要注意的问题。最后将对无线局域网厂商进行分类，并把它们网站的链接提供给读者。

11.1 常见无线局域网应用与设备部署注意事项

大量网络应用和网络设备受益于无线网络的发展，同时这些应用和设备也促进了无线网络的发展。尽管有些应用(如数据和视频)从无线网络的灵活性和可移动性中得到益处，但它们本质上并非无线应用。语音、实时定位服务(RTLS)和移动设备的网络访问是固有依赖无线局域网的三种用途，它们也不断深化和扩展着无线局域网的应用。无论在网络中部署什么样的应用或装置，对无线局域网的规划、设计与支持都是必须要考虑的。本部分将重点关注常用无线局域网应用和设备的部署注意事项。

如果需要进一步了解无线局域网的部署要素，请阅读书籍 CWDP: Certified Wireless Design Professional Official Study Guide:Exam PW0-250，该书的作者是 Shawn M. Jackman、Marcus Burton、Matt Swartz 和 Thomas W. Head，由 Sybex 于 2011 年出版。

11.1.1 数据

当我们在讨论面向数据的应用程序时，电子邮件和 Web 浏览是浮现在脑海中的两个最常见的应用。在规划无线或是有线的网络流量时，你需要在最初部署时先查看网络协议。协议是用于在网络上的设备之间进行通信的方法或技术。网络协议可以根据标准文档进行设计，也可以使用专有的通信方法。面向数据的应用程序因为经常使用众所周知的协议，存在大量的知识库描述它们是如何工作的，所以很容易处理。

处理面向数据的应用网络设计需要重点考虑的因素之一就是确保网络有能力处理需要转发的大量数据。大多数数据应用可以接受轻微的网络延迟，但如果数据带宽不足也可能会出现问题。设计无线网络设计时，要分析用户的数据要求，确保网络传输速率能够应付用户的数据传输。

11.1.2 语音

当设计支持语音通信的无线局域网时，切记与数据通信不同的是，语音通信不可以容忍网络的延迟、丢包和不持续连接。设计这样的网络相当具有挑战性，因为不同厂商的语音产品存在众多差异。包括语音手持设备、软件应用和网络基础架构在内的厂商都有各自独特的语音应用的设计原则。所以了解部署语音系统的最佳实践方法显得尤为重要。

与笔记本电脑不同，手持语音设备的发射功率通常较低。较强的信号发射需要消耗更多的电池能量。为了增加电池的持续供电时间，VoWi-Fi 电话的发射功率通常是小于其他设备

的，但这也同时降低了与无线接入点通讯的有效距离，因此通讯时需要无线覆盖蜂窝更小，此时需要更多的无线接入点才能确保足够的覆盖范围。

11.1.3　视频

802.11 无线局域网与视频应用结合仍然是一个相当新的技术，但这种应用一直在迅速扩大。视频的传输比语音更复杂。除了包含视频和语音的数据流以外，视频通常还包括用于通信连接建立和拆除的流量。除非是使用无线方式的实时的视频会议，视频流的重要程度通常会比音频流低。大多数情况下，视频比语音具有更高的丢包容忍度。在视频会议期间，如果声音断断续续，很可能会造成极坏的影响，导致与会者不断要求发言者重复讲述内容。然而如果语音清晰但视频效果不佳，发言者所讲述的内容还是可能在第一次就被理解的。

在视频传输方面，确定被传输的视频类型以及视频传输的功能和目的是需要重点考虑的方面。如果你询问某位普通计算机用户，他们可能会认为视频传输就是基于视频流的电影、电视节目或可供移动用户或固定用户下载的趣味视频片段。如果你询问某位经理，他们可能会认为视频传输是视频会议或网络研讨会的一部分，而使用者的位置最有可能是固定不变的。如果你询问一位设备工程师或安全人员，他们可能会认为视频传输是由永久固定在建筑物之上的无线监视摄像机产生的。无线局域网可能与上述一部分视频流或全部视频流有关。

一旦确定了无线局域网使用的视频类型，就可以规划网络了。需要评估正在传输无线视频数据的系统或软件，来确定流量和协议的类型，并确定网络负载。在协议评估过程中，要研究视频传输在使用多播传输还是 QoS。

11.1.4　实时定位服务

实时定位服务(RTLS)在过去几年已经引起了许多人的关注。大多数企业无线局域网厂商都开始使他们的产品具备某种形式的定位能力。有些厂商将定位特性内置在他们的产品中，有些则为第三方专业定位厂商(这些厂商具有与特定行业垂直市场相关的高级软件)提供集成接口。图 11-1 显示的是某 RTLS 实时对无线终端位置进行定位。

定位跟踪应用正在以难以置信的速度快速扩大，越来越多的用途被发掘出来。RTLS 可以通过无线局域网定位或跟踪人员和设备。医疗保健是采用定位技术最多的行业。由于医疗服务提供者(如医院)需要 7×24 小时运作，很多资产是共享使用的，RTLS 在紧急情况下定位和跟踪医疗设备，并确定离治疗地点最近的医生或专家是非常有必要的。

RTLS 可用于跟踪任何 802.11 无线发射器或整合了 802.11 RFID 标签的非 802.11 资产，以便它可以被跟踪并帮助防止失窃。标签也可以由企业员工、游乐场的儿童、医院的医生或患者佩戴。RTLS 供应商都会提供部署建议和最佳实践指南。

图 11-1 Ekahau Vision RTLS 软件

11.1.5 移动设备

我们惊讶地发现，从接待员到首席执行官的企业员工都开始携带自己的 802.11 设备(例如平板电脑和智能手机)来到公司，并在大多数情况下，这些设备需要接入企业网络。目前最常见的请求接入公司网络的设备是手机和平板电脑。与由 IT 部门规划和控制的企业技术升级不同，移动设备的支持功能是由最终用户持续推动的。许多企业都要求 IT 部门提供对这些设备的接入和支持能力。

但是将这些设备集成到现有网络中，有如下两点需要关注：

- 确保能够接入网络的装置具有正确的认证手段；
- 移动装置具有的加密协议可以确保其能够在网络中平滑漫游，而不会失去链接。

过去这些年，许多 802.11 无线网络被设计用来与发射功率较强的无线装置通信，例如笔记本电脑。任何 802.11 网络的单个无线接入点的覆盖蜂窝区域都需要被设计得足够小，以确保无线终端可以将信号回传给无线接入点，无线接入点的发射功率更大。手持设备通常比笔记本电脑发射功率更低，如果一个网络被设计成与较强发射功率的装置通信，很可能平板电脑或智能手机没有足够的能力把信号传回给无线接入点。对于移动设备来说就可能遭遇射频盲区。许多公司在设计无线局域网时都会尽可能减小无线接入点的覆盖区域以免移动设备遭遇服务中断。

11.2 企业数据接入与终端用户的移动性

在决定是否安装无线网络时，企业通常希望无线技术能为现有的网络增加两种功能。一

种是在某些区域安装有线连接的难度较大或成本较高时，无线技术可以轻松地为上述区域增加网络接入。另一种是在公司大楼或园区环境中，无线技术可以为无线用户提供便捷的移动性。

随着由 802.11n 技术提供的无线吞吐量的增加，许多组织开始减少用于有线连接的设备数量，很多时候会淘汰一些未被使用的有线交换机，转而投入高速的无线网络。正如前面提到的，迫使组织采用无线网络的另一个重要原因是基于 Wi-Fi 的个人移动设备的增加。

安装有线网络插座的成本很高，每个插座的成本通常高达 200 美元。在人员改制与部门重组的过程中，企业网络基础架构一般也需要随之改变。在库房、会议室、生产线、研究实验室、咖啡厅等区域通常很难有效地安装有线网络，而安装无线网络可以降低企业开销，并为所有用户提供稳定的网络接入。

对企业而言，选择安装无线网络的另一个关键因素是为了在整个工作场所提供持续的接入与可用性。计算机接入与获取数据目前已成为许多人工作中不可或缺的一部分，因此，网络必须持续可用并能提供最新信息。通过在整个建筑或园区中安装无线网络，企业员工之间的会谈与讨论将变得更加容易，他们也能随时随地使用自己的笔记本电脑访问企业数据、查看电子邮件并接入互联网。

无论出于何种目的安装无线网络，企业都要认清无线网络的利弊。无线技术提供了移动性、可达性与便利性，但如果设计和部署有误，可能会导致性能、可用性与吞吐量存在问题。作为一种接入技术，无线可为终端用户设备提供网络连接。一般不应考虑将无线技术用于分布层或核心层，建筑物之间的桥接除外。即便用于桥接，也要确保无线网桥能够满足流量负载与吞吐量需求。

11.3　网络延伸到远端

细想之下，网络延伸到远端不仅是家用无线网络的驱动力之一，也有助于推动无线技术在企业环境中的应用。随着很多家庭接入互联网并购买了更多的计算机，人们希望将家中的所有计算机都连接到互联网。尽管许多人通过安装以太网线缆来连接他们的计算机，但这样做成本过高，不够实用，或者超出了一般家庭的承受能力。

目前，802.11 无线设备的价格越来越低。在家庭中安装无线网络的原因同样适用于办公室、库房以及几乎任何其他环境。不仅每台计算机安装网络线缆的成本很高，而且受建筑物设计或美观等方面的因素所限，在许多环境中安装线缆或光纤是相当困难的一件事。安装无线网络设备可以大大减少线缆的数量，而且设备的布局通常不会影响到建筑的美观。

11.4　建筑物之间的桥接

为在建筑物间提供网络连接，可在两栋建筑物之间铺设地下铜缆或者光纤，也可以租用高速的电话通信网络，或者你采用无线桥接方案。这三种解决方案都可以胜任，但是各有优缺点。

尽管铜缆或者光纤可以为用户提供最大的吞吐量，但是造价非常昂贵。如果建筑物之间距离过远或者被第三方的物业阻挡，这种方案甚至就不是可选项。在部署线缆后，因为你拥有线路的产权，所以不必支付月租费用。

租用高速的电话通信网络可以得到灵活和简便的服务，但是因为你并非线路的产权所有人，需要每月支付服务费。而且受所购买的服务类别所限，你不一定能轻易地改变通信速率。

无线桥接网络要求两栋建筑物之间存在清晰的射频视距(LOS)。确定或者构建好清晰视距之后，便可以开始安装点到点(PTP)或者点到多点(PTMP)的无线收发器和天线。安装工作对于受过培训的专业人员通常很容易。因为你拥有这些设备，所以不必支付月租费用。

对于两栋建筑物，你可以通过点到点无线桥接，对于三栋或者超过三栋建筑物互联，你可能需要点到多点的无线桥接解决方案。在点到多点的安装部署中，最靠近中心的建筑物通常是中央通信点，其他的设备与中央通信点直接通信。这就是常说的“中心辐射”(hub and spoke)或者星形连接。

对于点到多点方案而言，一个潜在问题是中央通信点可能会成为所有建筑物通信的单点故障因素。为防止单点故障并提供高速数据吞吐量，通常可以安装多个点到点桥接网络。

11.5 无线运营商——最后一英里的数据交付

术语“最后一英里”(last mile)通常指电话公司或有线电视公司为家庭用户接入他们的网络提供的最后服务区段。最后一英里服务通常是最复杂和最昂贵的，因为在此处通信线缆需要独立连接到每一个最终用户。在郊外地区这一点尤为突出，因为用户极少，而且用户之间相距甚远。在许多情况下，即便用户可以接入，也无法享受高速的互联网服务，例如 xDSL，它要求距离局端不得超过 18 000ft(5.7 km)。

无线运营商(WISP)通过无线网络提供互联网服务，他们并非通过电缆连接每一个最终用户，而是通过中心发射机发射的射频提供通信服务。无线运营商通常采用不同于 802.11 的无线技术，使他们的无线网络可以覆盖到更大范围。对无线运营商来说，虽然在小城镇部署 802.11 网状网(Mesh network)作为无线基础架构确实存在少数成功案例，但 802.11 技术通常并不用于城市范围的无线运营商部署。

无线运营商提供的服务并非完美无缺。因为对于任何射频技术，信号都会因为障碍物(如屋顶、山川、树木或者其他建筑物)的遮挡衰减或者中断。正确的设计和专业的安装可以确保系统正常工作。

11.6 小型办公室/家庭办公室

小型办公或家庭办公(SOHO)面临的一个共同主题是工作范围庞杂，职责从守卫到 IT 人员，事无巨细。小企业主和家庭办公雇员通常需要能够自给自足，因为通常很少有人去帮助

他们。无线网络有助于小企业或家庭办公人员更容易将办公室的计算机和外围设备连接在一起，包括互联网的连接。SOHO 802.11 网络通常主要用来提供到互联网网关的无线接入能力。如图 11-2 所示，许多无线 SOHO 设备也具有多个以太网端口，提供有线和无线互联网访问。

大多数小型办公/家庭办公 (SOHO) 级无线路由器的安装方法相当容易，提供的性能与安全功能与企业级产品接近。它们通常不灵活，功能也无法与企业级产品相比，但大多数 SOHO 环境并不需要那些额外的功能。小型或家庭办公人员只需要用大约企业级产品四分之一的价格就可以得到一款功能尚可的设备。市场上有数十款设备可用于 SOHO 办公人员安装和配置安全的互联网接入网络，不必花费大量金钱。许多 SOHO 无线路由器甚至可以提供访客接入能力，可以允许访客接入互联网而不允许访问内部网络。

图 11-2　D-link SOHO 级别无线路由器

11.7　移动办公网络

移动办公室有多种用途：例如用于施工期间或灾难后的临时办公或应付学生人数激增而设置临时教室。移动办公室简单来说就是办公环境的扩展。这些结构通常都是临时建筑物，可以轻松地基于需要进行短期或长期的部署。这些结构不是永久建筑，因此使用无线网络扩展企业或学校网络到这些移动办公室会更加容易。

无线网桥可用于将无线网络扩展到移动办公室。如果需要，可由另一个无线接入点为办公室的多个用户提供无线网络访问。通过提供无线通信网络，可以减少有线电缆和安装网络插口的成本。用户可以从网络连接或断开连接，而不必改变任何网络基础架构。当不再需要移动办公室时，简单地拆除无线设备即可。

许多场景会使用到可移动的无线网络，包括军事演习、救灾、音乐会、跳蚤市场，和建筑施工场所。由于便于安装和拆卸，移动无线网络可能的是一种理想的网络解决方案。

11.8　教育/教室使用

无线网络可以安全方便地连接学生和学校网络。因为大多数教室的布局是很灵活(没有固定安装的家具)，为每个学生安装有线的网络插口也是不可能的。学生在上课时连接网络插头，

下课再断开，因此即使安装了有线的网络插口，不久也会损坏。在无线网络普及之前，通常使用有线以太网的教室中的所有计算机都靠着教室墙壁放置，学生一般无法面对着老师。无线网络可以允许学生座位任意摆放，也没有网络电缆在地板布线的安全风险。

无线网络还可以让学生随时连接到网络做课程作业，而不必担心附近是否有网络插口或是否已有人使用。无线网络被部署在教室环境除了可以提供灵活性外，在许多学校，无线网络已经成为必需品，因为平板电脑正在迅速普及成为教学设备，它们完全依赖无线网络提供的网络接入能力。

由于教室之间墙体材料的缘故，学校通常需要部署更多无线接入点。为了减轻噪音，大多数教室的墙壁是由煤渣砌块构成。这些煤渣砌块会导致 2.4GHz 和 5GHz RF 信号显著衰减。为了提供-70dBm 的信号强度及更大的覆盖范围，通常需要至少每隔一间教室部署一个无线接入点。

无线桥接在校园环境也非常流行的。许多大学和学院使用多种类型的无线网桥(包括 802.11)连接校园内的建筑物。

11.9 工业——仓储和制造

仓储和制造业环境中的无线网络已经使用了很多年，甚至在 802.11 标准创建之前就已经开始使用了。因为空间开阔和在这些环境中办公人员的移动特性，为员工提供移动网络接入可以提高他们的工作效率。仓储和制造环境通常会部署无线手持设备用于库存控制，如条码扫描器。

这些环境中部署的大多数 802.11 网络设计的重点是覆盖范围，而不是带宽需求。手持设备通常不会消耗大量带宽，但需要较大的覆盖范围，以提供确实的移动性。早期在制造和仓库环境中部署的大多数设备采用 802.11 跳频技术(FHSS)，现在这些老式的 802.11 FHSS 设备仍然存在。无线网络可为仓库环境提供覆盖和移动需求，性价比很高。

11.10 医疗保健——医院和办公室

虽然医疗机构(例如医院、诊所和医生办公室)可能看起来与其他行业不同，但基本上有相同的网络需求：数据访问和终端用户的移动性。医疗行业需要能够快速、安全、 准确地访问患者和医院的数据，并对此做出反应和决定。无线网络可以提供移动性和快速访问数据的能力，重要数据可以直接发往医生或护士携带的手持无线终端。医疗手推车可以输入和监控病人信息，通常也会有到护士站的无线连接。一些公司甚至将 802.11 无线适配器直接集成到设备中，用于监视和跟踪病人的生命体征。例如图 11-3 所示的监控系统，其使用 Wi-Fi 技术将患者的心电图和生命体征传输到护士站。

图 11-3　Welch Allyn Propaq

VoWiFi 是另一个在医疗环境中常见的 802.11 技术应用，无论医务人员在什么地方，都可以即时通话。使用 802.11 技术的 RFID 标签用于资产控制的实时定位系统(RTLS)解决方案也非常普遍。

医院存在的许多形式的基于专有标准或行业标准的无线通信，可能会对 802.11 无线网络射频造成潜在干扰。很多医院都会指派专人或专业部门，跟踪医院内的生物医学设备和频率使用以减少射频冲突。

为满足政府私隐条例，医院通常需要有高等级的安全要求。

11.11　市政网络

在过去几年中，市政网络受到诸多关注。许多城市宣布他们为整个地区的市民提供无线网络接入的计划。许多城市视此为一种为市民提供互联网接入服务的办法。虽然这项想法本意不错，但各个团体通常会评估这些项目的规模和成本，许多纳税人不希望他们的钱花在他们认为不必要的服务上。虽然很多 802.11 市政网络被取消，但仍有一些地区提供有限的 802.11 网络覆盖和服务，这些网络其中有些由市政建设，有些由个人或商业团体建设。

11.12　热点——公共网络接入

术语“热点”通常指免费或收费使用的无线网络。当人们一想到热点时，通常就会联想起咖啡厅、书店、酒店或会议中心等接待型业务。热点可作为企业吸引顾客的有效手段。商务旅行者经常频繁出入可提供免费上网的食肆或咖啡厅，这些机构可以通过提供热点服务而

增加业务。免费热点使大家对 802.11 无线行业产生更多关注，也有助于更多人认识到这项技术的好处。

有些热点提供商收费高达每月 40 美元，这让人难以接受。许多机场和连锁酒店已安装了收费热点。目前存在许多服务提供商，每家都会提供一种单独的订购服务，这对消费者通常不是很实用。

大多数热点提供商在进行网络身份验证时，使用一种特殊类型的称为强制门户的 Web 页面。当用户连接到热点时，必须打开 Web 浏览器。无论用户尝试访问任何 Web 页面，将总是显示出需要认证的 Web 页面，即强制门户页面，如图 11-4。如果该热点提供的是收费服务，用户必须输入他们的订购信息或信用卡信息。很多免费的热点也会使用强制门户要求用户在访问互联网前必须同意互联网使用政策。如果用户同意政策条款，他们被要求输入一些基本信息或者单击按钮，证明他们同意该政策。很多公司也使用强制门户要求访客在使用他们的网络前进行身份验证。

图 11-4 强制门户的例子

真实场景

热点能提供数据安全性吗？请务必记住热点服务提供商(无论免费还是收费)并不关心数据的安全性。热点服务提供者通常提供免费的互联网接入服务，以鼓励你经常造访他们的所在地，例如咖啡馆，然后购买他们的一些产品。收费热点会要求进行身份验证，以确保你是付费用户，在通过验证之后便可以接入互联网。热点服务提供商很少提供任何形式的数据加密。为此，商务用户在使用热点时，经常使用 VPN 客户端通过加密隧道连回公司网络。许多公司也要求员工在使用公共热点服务时必须使用 VPN 以保证数据的传输安全。第 14 章会对热点使用的相关安全问题做进一步讨论。

11.13　交通网络

在谈论交通网络中的 Wi-Fi 应用时，有三种主要形式——火车、飞机和汽车会经常提及。另外还有两种方式也需要关注，第一个是船，包括邮轮和往返渡轮；第二个是巴士，与汽车类似，但是有区别。

为任何一种交通形式提供 Wi-Fi 无线上网服务都很容易。只需在交通工具中简单安装一个或多个接入点即可。除了邮轮和大型货轮，大多数交通形式只需要几个接入点就可以提供 Wi-Fi 覆盖。构建这些网络的主要目的是为终端用户提供热点服务，以便他们可以访问互联网。交通网络和典型的热点之间的区别是交通网络不断移动，需要某种类型的移动上行服务。

对需要提供上行链路的列车来说，每次行进都被限制于相同的轨道路径，可沿轨道路径使用某种类型的无线城域网技术，例如 WiMAX。其他交通网络，因为行进路径不受限制，更可能的上行方法是通过某种类型的蜂窝网络。不过，如果 WiMAX 开始广泛部署，对于火车、公共汽车或汽车来说都是可接受的上行链路。

往返渡轮可以使用蜂窝网络或 WiMAX 提供的上行服务，因为它们在其服务范围内。对于离岸更远的距离的轮船或邮轮，可能需要使用卫星链路。

许多航空公司也开始在飞机上安装 Wi-Fi 网络。飞机内部的 Wi-Fi 无线上网服务由一个或多个接入点与连接到蜂窝网络的路由器组成，该路由器与地面的蜂窝基站进行通信，或者通过连接卫星的卫星路由器进行数据上行，然后通过卫星将数据传送到地面站。基于蜂窝网络的系统需要地面蜂窝接收器的支持，因为跨越大洋的飞行是无法使用这种通信方式的。这项服务通常是收费的，仅在飞机飞行且到达巡航高度时可用。通常会采用带宽限制措施防止用户独占网络。

11.14　执法网络

虽然 Wi-Fi 网络不能为执法人员提供所需的广域覆盖以达到连续无线通信的需求，但它们仍然可以协助警方打击犯罪。许多执法机构使用 Wi-Fi 作为其公共安全无线网络的补充。

除了在警局内使用 Wi-Fi 无线带来明显的移动性优点，许多城市都在警察局外和其他市政建筑外的停车场安装 Wi-Fi 作为其无线城域网的补充。这些户外网络有时被认为是安全的热点。与公共热点不同的是，这些网络能够提供身份验证和高级别的加密。市政当局除了将无线技术纳入执法，还添加了很多非 Wi-Fi 的自动化程序用于监督控制和数据采集(SCADA)设备。由于不同的无线技术使用增加，我们注意到市政部门开始指定个人或部门进行无线使用技术和频率的跟踪和记录。

市政 Wi-Fi 热点通常在警车与警务部门的内部网络间提供高速网络通信。一个有趣的例子就是交通视频文件的上传。许多警车配备了视频监控设备，这些监控视频经常被用于证据收集，将这些视频文件传送到中央服务器进行编目和存储显得很重要，也减少了警务人员花在保存证据链上的工作量。

当警车到达市政 Wi-Fi 热点附近时，车内的计算机可以自动将数据存储中的视频文件上传到中央视频库。这一过程的自动化最大限度减少了数据丢失的风险，并使警务人员可以执行其他更重要的任务。

4.9GHz 频段的特殊使用

在一些国家，公共安全和应急响应部门会使用 4.9GHz 频段。这个频段通常需要使用许可证，确保保证该频段可以被合法使用。这个频段通常部署在室外，并因为需要许可证才能使用，受到干扰的可能性很小。

11.15 快速应急网络

当医疗和消防救援人员到达发生紧急情况的现场时，很重要的是可以便捷地获取必要的资源以紧急处理危机。有的救援车辆配备了永久安装的 Wi-Fi 接入点，有的使用便于部署的独立的便携式接入点，可以快速轻易地使用 Wi-Fi 网桥将救援现场与应急人员数据网络连接在一起。在灾难中，当公共服务(如移动电话网络)通信系统出现过载或停机时， Wi-Fi 快速应急网络可以让当地人员共享访问中央数据库资源。

灾难期间，现场评估和受害者验伤分类工作(基于其损伤的严重程度对伤员进行分组)是首要任务。从历史上看，验伤分类的任务包括使用纸标签列出医疗信息和受害者状况。一些公司已创造出电子分诊标签，可以用电子方式保存病人信息并通过 Wi-Fi 网络传输。

11.16 固网与移动网的融合

当前与 Wi-Fi 有关的最热门的话题之一， 即被称为固网与移动网融合(Fixed Mobile Convergence)的 FMC。FMC 系统的目标是提供这样一个设备，它具有一个电话号码，可以在网络之间切换，但始终使用成本最低的网络。图 11-5 是 FMC 电话网络的示意图。

FMC 具有移动电话的灵活性和移动性，在办公人员位置固定并可以访问费用较低的电话网络环境(家庭或工作环境)中经常被用到。FMC 设备通常可以通过移动电话网络和 VoWiFi 网络进行通信。如果你在具有 Wi-Fi 网络的办公室或家里拥有一部 FMC 电话，FMC 电话就可以使用 Wi-Fi 网络进行电话呼叫或接收。如果你在公司外面无法访问 Wi-Fi 网络，那么 FMC 电话会使用移动网络进行电话呼叫或接收。

FMC 设备也允许跨网络漫游。所以当你利用 Wi-Fi 网络在公司内部打出一个电话，然后当你走到户外时，FMC 电话会从 Wi-Fi 网络漫游到移动网络，实现两个网络之间的无缝过渡。使用 FMC，你将能够有一个设备和一个电话号码，无论在哪里都可以使用最廉价的网络。

图 11-5　FMC 网络设计

IEEE 802.11u 修订案，即通常称为“与外部网络的无线互通”(WIEN)，实现了 802.11 和蜂窝网络之间的 FMC 通信的标准化，也很好地诠释 Wi-Fi 与其他外部网络(如移动蜂窝网络)的无缝切换和会话保持功能。

11.17　无线局域网与健康

多年来，无线电波是否会对人类和动物造成不良影响的疑问一直存在。世界卫生组织和政府机构设立标准，要求 RF 产品必须满足射频电波发射限制。实际上，测试表明无线局域网产品大大低于这些组织设定的安全发射限制。相对于其他射频信号，Wi-Fi 信号功率要低得多。世界生组织还得出结论，没有任何令人信服的科学证据可以证明微弱的射频信号(如 802.11 通信信号)会对健康产生不利影响。

你可以通过以下网站阅读到更多相关知识：

- 美国联邦通信委员会
  transition.fcc.gov/oet/rfsafety/rf-faqs.html
- 世界卫生组织
  www.who.int/peh-emf
- Wi-Fi 联盟
  www.wi-fi.org

11.18　无线局域网供应商

802.11 无线局域网市场有很多供应商，包括知名的公司，如 Aruba、Cisco、HP、Juniper 和 Motorola，还有一些初创的公司，如 Aerohive、Meraki、Ruckus 和 Xirrus 等。以下是一些

主要无线局域网厂商的列表。请注意这里只列出每个厂商的一个产品类别，尽管他们可能提供很多其他类别的产品和服务。这都是一些最知名的基础设施提供商，他们还对其产品提供附加功能，例如安全和故障排除功能。

1. 无线局域网基础架构

下列厂商生产和销售 802.11 企业级产品，包括 WLAN 控制器和无线接入点：

- Aerohive Networks：www.aerohive.com
- Aruba Networks：www.arubanetworks.com
- Cisco：www.cisco.com
- Extricom：www.extricom.com
- Hewlett-Packard：www.hp.com
- Juniper Networks：www.juniper.com
- Meraki：www.meraki.com
- Meru Networks：www.merunetworks.com
- Motorola：www.motorola.com
- Proxim Wireless Corporation：www.proxim.com
- Ruckus Wireless：www.ruckuswireless.com
- Enterasys (Siemens)：www.siemens.com
- Ubiquiti Networks：www.ubnt.com
- Xirrus：www.xirrus.com

2. 无线局域网 Mesh 基础架构

下面厂商专注于 802.11 无线网状网(mesh)解决方案：

- BelAir Networks：www.belairnetworks.com
- Firetide：www.firetide.com
- MeshDynamics：www.meshdynamics.com
- Strix Systems：www.strixsystems.com
- Tropos Networks：www.tropos.com

3. 无线局域网排错与设计解决方案

下列厂商制造或销售 802.11 协议分析仪、频谱分析仪、现场勘测软件、RTLS 软件以及其他无线局域网分析解决方案：

- AeroScout：www.aeroscout.com
- Berkeley Varitronics Systems：www.bvsystems.com
- Riverbed Technology：www.riverbed.com
- Ekahau：www.ekahau.com
- Fluke Networks：www.flukenetworks.com
- MetaGeek：www.metageek.net

- TamoSoft：www.tamos.com
- WildPackets：www.wildpackets.com
- Wireshark：www.wireshark.org

4. 无线局域网安全解决方案

下列厂商提供无线安全解决方案、无线局域网入侵检测系统解决方案或 802.1X/EAP 客户端与服务器解决方案：

- AirTight Networks：www.airtightnetworks.com
- Cloudpath Networks：www.cloudpath.net
- Fortress Technologies：www.fortresstech.com

5. VoWiFi 解决方案

下列厂商提供 802.11 VoWiFi 电话和 VoIP 语音网关解决方案：

- Ascom：www.ascom.com
- Polycom：www.polycom.com
- Vocera：www.vocera.com

6. 无线局域网固网与移动网融合(FMC)解决方案

下列厂商提供 802.11 与移动网络融合解决方案：

ShoreTel Networks：www.shoretel.com

7. 无线局域网 SOHO 产品供应商

下列供应商提供家用 Wi-Fi SOHO 解决方案：

- Apple：www.apple.com
- Buffalo Technology：www.buffalotech.com
- Belkin International：www.belkin.com
- D-Link：www.dlink.com
- Hawking Technology：www.hawkingtech.com
- Linksys：www.linksys.com
- Netgear：www.netgear.com
- SMC Networks：www.smc.com

11.19　小结

本章涵盖了无线网络使用场景中的设计、实施和管理的一些内容。这些场景类似，但各有特色。请务必了解这些差异之处以及无线网络通常是如何部署的。

11.20 考试要点

了解不同的无线局域网垂直市场。无线网络可以在许多环境中使用，每个不同的垂直市场都有针对无线网络不同的关注点，了解在这些环境中部署 802.11 无线网络的主要理由。

了解固网与移动网络融合(FMC)。移动蜂窝网络和 Wi-Fi 网络如此普遍，以至于供应商开始提供使两个网络得以融合的电话，并提供在它们之间的漫游。了解什么是 FMC 及部署它的好处。

11.21 复习题

复习题的答案见附录 A。

1. Which of the following are objectives of fixed mobile convergence? (Choose all that apply.)

   A. Have a single phone number

   B. Have a single device

   C. Always use the best-performing network

   D. Use the lowest-cost network

2. Which of the following is another form of a public hotspot network? (Choose all that apply.)

   A. Law enforcement network

   B. First-responder network

   C. Transportation network

   D. Municipal network

3. Which type of organization often has a person responsible for keeping track of frequency usage inside the organization?

   A. Law enforcement

   B. Hotspot

   C. Hospital

   D. Cruise ship

4. On which of these transportation networks is satellite a functional solution for providing uplink to the Internet?

   A. Bus

   B. Automobile

   C. Train

   D. Cruise ship

5. Fixed mobile convergence provides roaming across which of the following wireless technologies? (Choose all that apply.)

   A. Bluetooth

B. Wi-Fi

C. WiMAX

D. Cellular phone

6. Which of the following is typically the most important design goal when designing a warehouse WLAN?

A. Capacity

B. Throughput

C. RF interference

D. Coverage

7. Corporations often install wireless networks to provide which of the following capabilities? (Choose all that apply.)

A. Easy mobility for the wireless user within the corporate building or campus environment

B. High-speed network access comparable to wired networking

C. Internet access for visitors and guests.

D. The ability to easily add network access in areas where installation of wired connections is difficult or expensive

8. Last-mile Internet service is provided by which of the following? (Choose all that apply.)

A. Telephone company

B. Long-distance carrier

C. Cable provider

D. WISPs

9. Which of the following is the main purpose of a SOHO 802.11 network?

A. Shared networking

B. Internet gateway

C. Network security

D. Print sharing

10. Which of the following are examples of mobile office networking? (Choose all that apply.)

A. Construction-site offices

B. Temporary disaster-assistance office

C. Remote sales office

D. Temporary classrooms

11. Warehousing and manufacturing environments typically have which of the following requirements? (Choose all that apply.)

A. Mobility

B. High-speed access

C. High capacity

D. High coverage

12. Which of the following is least likely to be offered by a hotspot provider?
    A. Free access
    B. Paid access
    C. Network authentication
    D. Data encryption
13. Which of the following are good uses for portable networks? (Choose all that apply.)
    A. Military maneuvers
    B. Disaster relief
    C. Construction sites
    D. Manufacturing plants
14. Which of the following terms refer to a PTMP network design? (Choose all that apply.)
    A. PTP
    B. Mesh
    C. Hub and spoke
    D. Star
15. Most early deployments of 802.11 FHSS were used in which type of environment?
    A. Mobile office networking
    B. Educational/classroom use
    C. Industrial (warehousing and manufacturing)
    D. Healthcare (hospitals and offices)
16. When using a hotspot, you should do which of the following to ensure security back to your corporate network?
    A. Enable WEP.
    B. Enable 802.1X/EAP.
    C. Use an IPsec VPN.
    D. Security cannot be provided, because you do not control the access point.
17. What are some popular 802.11 applications used in the healthcare industry? (Choose all that apply.)
    A. VoWiFi
    B. Bridging
    C. RTLS
    D. Patient monitoring
18. Multiple point-to-point bridges between the same locations are often installed for which of the following reasons? (Choose all that apply.)
    A. To provide higher throughput
    B. To prevent channel overlap
    C. To prevent single point of failure
    D. To enable support for VLANs

19. What are some of the key concerns of healthcare providers when installing a wireless network? (Choose all that apply.)

A. RF interference

B. Faster access to patient data

C. Secure and accurate access

D. Faster speed

20. Public hotspots typically provide clients with which of the following security features?

A. Server Authentication.

B. Encryption.

C. TKIP.

D. No client security is available.

第 12 章 无线局域网排错

在该章中，你将学习以下内容：

- √ 第 2 层重传
  - 射频干扰
  - 多径现象
  - 邻频干扰
  - 低信噪比
  - 不匹配的功率设置
  - 近/远问题
  - 隐藏节点
- √ 802.11 信号覆盖要点
  - 动态速率调整
  - 漫游
  - 三层漫游
  - 同频干扰
  - 信道复用/多信道体系结构
  - 单信道体系结构
  - 容量与覆盖
  - 超大尺寸的覆盖蜂窝
  - 物理环境
- √ 语音与数据
- √ 性能
- √ 天气影响

用于排除 802.3 有线网络故障的诊断方法在进行无线局域网故障排除时是适用的。分析 OSI 参考模型的自下而上的方法也适用于无线网络。无线网络管理员应首先尝试确定问题是否存在于 OSI 第一层和第二层。对于大多数网络技术，问题通常与第一层有关。第一层问题(例如接入点未接电或客户端卡驱动程序故障)往往是导致连接或性能问题的根本原因。由于无线局域网使用射频收发数据，无线局域网的故障排除比典型的有线环境存在更多来自物理层的挑战。本章大部分内容讨论了许多发生在第一层的潜在问题以及解决第 1 层问题的方案。频谱分析仪诊断第一层问题时往往很有用。

在排除第一层可能的故障来源后，无线局域网管理员应尝试确定在第二层数据链路层是否存在问题。接入点、WLAN 控制器和客户端软件的安全配置和管理配置错误经常导致认证和关联问题。无线局域网协议分析仪在排除第二层故障问题时通常是非常重要的工具。

本章会讨论在部署 802.11 无线网络时遇到的射频覆盖和故障排除问题。射频传播行为和射频干扰会影响到性能和无线局域网覆盖。无线局域网环境中客户端经常移动，所以经常发生漫游问题，这也必须予以关注。无线传输媒介的半双工特性也带来了通常在全双工环境中不会出现的独特的挑战。另外户外 802.11 无线部署易受天气条件影响，也要给予特别关注。这一章将讨论如何判断、排除、预防和修复潜在的无线局域网问题。

12.1 第 2 层重传问题

影响无线局域网性能的大敌是发生在数据链路层 MAC 子层的第 2 层重传。如你所知，所有单播 802.11 帧必须被确认。如果发生冲突或单播帧受损，那么循环冗余校验(CRC)将会失败，接收方的 802.11 射频卡将不会向发送方回应 802.11ACK 帧。如果原来的发送方没有接收到 ACK 帧，该单播帧未得到确认，将不得不重传。

过度的第 2 层重传将以两种方式影响无线局域网。第一，第 2 层重传增加链路开销，并因此导致吞吐量下降。很多因素可能影响吞吐量，无线局域网环境出现大量第 2 层重传是其中之一。

第二，如果应用程序数据在第 2 层不得不重传，应用程序数据交付就会延迟或不连续。而某些应用程序(如 VoIP)很依赖 IP 数据包能及时和连续的传递。过度的第 2 层重传通常会导致对时间敏感的应用程序(如语音和视频)出现延迟和抖动问题。当谈及 VoIP 时，经常会混淆延迟和抖动的概念：

- 延迟(Latency)

延迟是指从源设备交付 VoIP 数据包到目标设备所需的时间。由于第 2 层重传可能会延迟交付 VoIP 数据包，导致语音出现回声现象。

- 抖动(Jitter)

抖动指延迟的变化程度。抖动程度可以通过测试每个数据包的延迟与平均延迟值的差异来评估。如果所有数据包按相同的速度通过网络，抖动值将为零。802.11 第 2 层重传也是导致高抖动问题的常见原因。抖动会导致音频通信不连贯并减少 VoWiFi 手机的电池续航时间。

Wi-Fi 网络中的大多数数据应用程序可以承受第 2 层的重传率高达 10%，且不会导致明显的性能下降。不过，像 VoIP 等对时间敏感的应用程序则要求高层 IP 数据包的丢失率不超过 2%。因此，VoWiFi 网络为了确保 VoIP 数据包可以及时且连续地传递，要求第 2 层重传率为 5%或更低。

如何测试第 2 层重传？如图 12-1 所示，任何优秀的 802.11 协议分析仪都可以对整个 WLAN 进行第 2 层重传统计。802.11 协议分析仪还可以跟踪某个无线接入点和客户端的重传统计信息。WLAN 控制器或者 WNMS 也可以集中监控整个 WLAN 企业网络的第 2 层重传统计信息。

不幸的是，太多问题会导致第 2 层重传。多径现象、射频干扰和低信噪比等第 1 层的问题也会导致第 2 层重传。此外隐藏节点、近远效应、功率设置不匹配和邻频干扰等也会导致第 2 层重传，这些通常是由无线局域网设计不当引起的。

图 12-1　第 2 层重传统计

12.1.1　射频干扰

各种类型的射频干扰可能极大地影响 802.11 无线局域网的性能。干扰设备可能阻止 802.11 无线传输，从而导致拒绝服务(DOS)。如果另一个射频源传输强振幅信号，802.11 射频卡在空闲信道评估(CCA)过程中可以感应到能量存在并延迟传输。射频干扰的另一个典型

结果是导致 802.11 帧受损。如果帧因射频干扰损坏，就会发生过量的重传，并使吞吐量大大下降。下面介绍几种不同类型的射频干扰。

1. 窄带干扰(Narrowband interference)

窄带射频信号占据的频率空间较小且有限，并不会导致出现整个频段的拒绝服务(DoS)，例如整个 2.4GHz ISM 频段。窄带信号通常振幅很高，可能导致其所在频率空间的通信中断。窄带信号可以破坏一个或多个 802.11 信道。

窄带射频干扰也会导致帧损坏及第 2 层重传。消除窄带干扰的唯一方法是通过频谱分析仪找到干扰设备源头。要解决干扰问题，使用频谱分析仪确定受影响的信道并在窄带干扰信号附近设计信道复用规划。图 12-2 显示的是频谱分析仪捕获的靠近 2.4GHz ISM 频段第 11 信道的窄带信号。

图 12-2 窄带 RF 干扰

2. 宽带干扰(Wideband interference)

会导致整个频段通信能力破坏的干扰源通常被视为宽带干扰。宽带干扰器可使整个 2.4GHz ISM 频段遭遇拒绝服务(DoS)。消除宽带干扰的唯一方法是通过频谱分析仪找到干扰设备源并清除干扰设备。图 12-3 显示的是频谱分析仪捕获到的平均振幅达-60dBm 的 2.4GHz ISM 频段宽带信号。

图 12-3　宽带射频干扰

3. 全波段干扰(All-band interference)

术语“全波段干扰”(all-band interference)通常与跳频扩频(FHSS)通信有关，会破坏 2.4GHz 的 802.11 通信。在前面的章节中，你了解到 FHSS 不断在整个频段跳动，间歇地在很小的子载波频率空间传输。例如，传统的 802.11 FHSS 射频模块以 1MHz 的频宽跳跃性地传输。FHSS 设备在频率空间跳跃并驻留时，将占用 HR-DSSS 或 ERP-OFDM 信道的一部分。虽然通常 FHSS 设备不会造成拒绝服务，但 802.11b 及 802.11g 设备传输的帧可能会被在全波段传输的 FHSS 信号破坏。

真实场景

什么设备会导致射频干扰？

包括无绳电话、微波炉、摄录机在内的大量设备，都会造成射频干扰和 802.11 无线局域网性能下降。2.4GHz 的 ISM 频段极度拥挤，有许多已知的干扰设备。干扰设备也可能在 5GHz UNII 频段工作，但 2.4GHz 的频率空间更加拥挤。通常来自附近无线局域网的信号是最大的干扰源。如果无法消除 2.4GHz 频段的射频干扰，应该特别考虑是否将无线局域网部署在不那么拥挤的 5GHz 频带。查找干扰源需要频谱分析仪。

在第 16 章中，我们将讨论到适当的频谱分析技术应该作为无线现场勘测的一部分。第 16 章还列出了可能导致 2.4GHz 和 5GHz 频率范围内的传输出现问题的许多干扰设备。

蓝牙(bluetooth)是一种在无线个人网络(WPAN)中使用的短距离射频技术。蓝牙使用 FHSS 技术，在 2.4GHz ISM 频段每秒跳跃 1600 次。较老的蓝牙设备会造成严重的全波段干扰。但较新的蓝牙设备利用自适应机制，可以避免干扰到 802.11 无线局域网。数字增强型无线通信系统(DECT)无绳电话也使用跳频通信技术。Home RF 作为现在已经消失的无线局域网技术也使用 FHSS；因此 Home RF 设备可能引起全波段干扰。你可能还会偶然遇到一些类型的医疗遥测单元也使用跳频技术。尽管迄今提到过的所有 FHSS 干扰都发生在 2.4GHz ISM 频段，但干扰 5GHz 频段的跳频设备也存在。

跳频传输通常不会像固定频段传输那样导致严重的数据传输破坏，但如果有限的空间中存在大量跳频发射器，将导致某些 802.11 数据损坏及第 2 层重传。消除全波段干扰的唯一方法是通过频谱分析仪找到干扰设备并清除它。图 12-4 显示的是频谱分析仪捕获的在 2.4GHz ISM 频段传输的跳频通信信号。

图 12-4 全波段 RF 干扰

12.1.2 多径现象

在第 2 章中已经讨论过，多径现象可能会导致码间干扰(ISI)，这将导致数据损坏。由于原始信号和反射信号之间的时间差，也被称为延迟传播(delay spread)，接收器在解调射频信号信息的时候会产生问题。延迟传播的时间差会导致数据损坏。如果数据因为多径问题遭到损坏，会导致第 2 层重传。

多径现象在使用传统 802.11abg 设备的时候会是一个严重问题。可以通过使用定向天线减少了大量反射，天线分集也用来弥补多径现象带来的负面影响。多年来，多径现象在旧式 802.11abg 网络的一直扮演破坏者角色。但是随着越来越多的 WLAN 升级到 802.11n 技术，多径现象不再成为敌人。在采用多入多出(MIMO)天线分集和最大比混合(MRC)信号处理技术的 802.11n 传输中，多径现象扮演了正面的角色。

第 16 章将讨论主动和被动的现场勘测技术。主动现场勘测的主要目的是了解第 2 层重传的比率。如果确定在现场勘测的频谱分析的过程中没有发生射频干扰，那么第 2 层重传的最可能原因就是多径问题。如图 12-5 所示，WLAN 厂商 Berkeley Varitronic System(BVS 公司)生产了一系列无线局域网排错工具，可以检测并对多径问题和延迟传播问题进行形象的图形化显示。

PHOTO COURTESY OF BERKELEY VARITRONICS SYSTEMS

图 12-5　多径现象分析排错工具

没有办法“修复”室内的多径问题，因为反射总会发生，相同信号总是会有多个路径。然而，许多多径现象的负面影响(包括码间干扰)能够使用分集天线得到修正，这在第 4 章中已经谈及。高多径环境存在的室内环境，如较长的走廊区域和有金属存在的方法(例如有金属货架的仓库)，如果仍然部署 802.11abg 网络的话，强烈建议使用室内分集平板天线。使用这种定向天线可以减少反射，从而减少数据损坏和第 2 层重传。

802.11n 部署也会使用 MIMO 平板天线，但目的并非减少多径现象，而是为了提供定向覆盖。请记住多径现象在 802.11n 部署中是具有积极影响的。

某些射频技术可以更好地弥补多径带来的负面影响。使用 OFDM 技术的 802.11 无线射频卡处理多径问题时比使用直接序列扩频技术的无线射频卡更富弹性。因此，使用 OFDM 的 802.11a 和 802.11g 射频卡比传统的 802.11b 可以更好地处理多径。第 18 章中，我们讨论了 802.11n 标准，它定义了高吞吐量(HT)中无线射频卡的使用规定。802.11n 射频卡使用多入多出(MIMO)技术，其实际上利用了多径现象。应该指出，802.11n 需要向下兼容旧式 802.11a/b/g 网卡。802.11n 接入点不能解决旧式客户端可能遭遇的多径问题，因为旧式客户端仍会受到多径产生的负面影响。

真实场景

多径现象真的是一个问题吗？

简答：对于使用传统 802.11a/b/g AP 和客户端，如果处于一个高多径现象的室内环境(例如走廊或存在大量金属反射体的房间)，多径现象仍然是一个问题。

然而 802.11n 作为一个现代技术，行业持续升级基于 802.11n 接入点的企业 WLAN 基础架构，而且随着大多数客户端使用 802.11n 芯片以及传统 802.11a/b/g 被 802.11n 取代，用多径现象的思维进行故障排除的方式已经落后，因为 802.11n 技术需要利用多路径现象才可以更好的工作。

12.1.3 邻频干扰

大部分 Wi-Fi 厂商使用术语邻频干扰(ACI)代表由于不当的信道复用设计出现信道重叠进而导致无线局域网性能下降的现象。在无线局域网行业，邻频通常是指下一个或上一个编号的信道。例如，毗邻信道 2 的信道 3。

在第 6 章中我们了解到，802.11-2007 标准要求：为了避免信道重叠，802.11bg 信道的中心频率要求相隔 25MHz。如图 12-6 所示，如果需要三个信道，在美国只有 1、6 和 11 的信道才可以满足 2.4GHz ISM 频段的 IEEE 要求。信道 2 和 7、3 和 8、4 和 9、5 和 10 都是互为不重叠信道。要记住的重要一点是相邻的覆盖蜂窝必须要求间隔 5 个信道。一些国家允许在 2.4GHz ISM 频段使用所有的 14 个 IEEE 802.11 定义的信道，但由于中心频率的位置，可以使用的不重叠信道也不超过三个。即使所有的 14 个信道都可用，大多数厂商和最终用户仍选用信道 1、6 和 11。

只有三个信道不重叠

图 12-6 2.4GHz 不重叠信道

设计无线局域网时，为了提供漫游，需要覆盖蜂窝存在重叠区域。然而，重叠蜂窝不应出现频率重叠。在美国 2.4GHz ISM 频段可提供最多的不重叠信道只有 1、6 和 11 信道。具有重叠频率的重叠覆盖蜂窝会造成所谓的邻频干扰(adjacent cell interference)。如果重叠的覆盖蜂窝也有重叠的频率，传输帧将受到损坏，接收方将不会发送 ACK 帧，第 2 层重传也将大大增加。在这一章的后面部分，我们将讨论用于降低邻频干扰的信道复用模式。

IEEE 在 5GHz UNII 频带定义了 23 个可用信道，在 5GHz ISM 频带定义了一个 165 信道。如图 12-7 所示。因为有 20MHz 的中心频率间隔，这 23 个信道在技术上被视为不重叠信道。实际上每个 OFDM 信道的旁带仍然会带来一些频率重叠。好消息是 5GHz 频带所有的 24 个信道都可以用于信道复用模式，这会在本章后面进行讨论。

图 12-7　5GHz 不重叠信道

12.1.4 低信噪比

信噪比(SNR)是一个重要的值，如果背景噪音强度太接近接收信号强度或接收信号强度太低，数据可能会受损，重传将会增加。信噪比不是实际比率。它只是接收到的信号与背景噪声(噪底)之间的分贝差别，如图 12-8 所示。802.11 设备接收到的信号强度为-70dBm，噪底为-95dBm，接收信号与背景噪音的差别是 25dB。因此，信噪比是 25dB。

图 12-8 信噪比

数据传输可能因信噪比过低而崩溃。如果本底噪声的幅度太接近接收信号振幅，将发生数据损坏现象并导致第 2 层重传。25dB 或更高的信噪比被认为是很好的信号质量，10dB 或更低的信噪比被认为是很差的信号质量。为确保帧传输不会崩溃，许多厂商建议在数据无线局域网中最低信噪比为 18dB ，对于语音无线局域网建议最低信噪比为 25dB。

在设计阶段的现场勘测时，通常推荐不低于-70dBm 的信号强度。而在设计 VoWiFi 网络时，-67dBm 或以上的信号强度是被推荐的。图 12-9 显示本底噪声为-95dBm。当客户端得到从 AP 发过来的信号强度为-70dBm 时，SNR 为 25dB，因此数据传输不会崩溃。然而，如果另一个客户端的接收信号强度较弱，仅为-88dBm 时，此时的 SNR 也仅为 7dB。因为接收信号强度太接近于本底噪声，数据传输崩溃并导致第 2 层重传。

图 12-9 不同的信噪比

测试信噪比

请记住测试 SNR 需要能够测试原始的本底噪声的周边 RF 能量的仪器。请理解 802.11 无线网卡不是频谱分析仪，尽管它可以惊人的速率传输和接收数据，却无法看到原始的周边射频信号。无线网卡可以解码来自于另一个无线网卡的调制数据，却无法测试本底噪声。因此测试无法解码的射频能量和信噪比的最佳设备是频谱分析仪。

12.1.5　不匹配的功率设置

一个经常被忽略的导致第 2 层重传的原因是接入点和客户端之间的功率设置不匹配。如果客户端发射功率小于接入点传输功率，通信可能发生故障。当客户端移到覆盖蜂窝的外边缘处，客户端可以“听”到接入点；然而，接入点无法“听”到客户端。

如图 12-10 所示，如果接入点传输功率为 100 毫瓦，而客户端传输功率为 20 毫瓦，客户端将听到来自接入点的单播帧，因为客户端接收到的信号强度在其接收灵敏度范围内。然而，当客户端向接入点发送 ACK 帧时，因为客户端的传输信号幅度下降到低于接入点的射频接口接收灵敏度阀值，接入点将无法“听取”ACK 帧，然后接入点必须重传这个单播帧。客户端传输的所有信息都会被接入点认为是噪声，第 2 层重传就不可避免了。

图 12-10　接入点/客户端功率不匹配

如何防止因接入点和客户端之间功率设置不匹配导致第 2 层重传？最好的办法是确保所有客户端传输功率设置与接入点的发射功率设置匹配。对于传统 AP 的功率设置的最佳实践是不应超过客户端中设置的最低功率值。但是 AP 接收敏感度的显著改善已经从本质上改善了因为客户端和 AP 功率不匹配产生的许多问题。

测试是否存在接入点/客户端功率不匹配问题的一种方法是使用协议分析仪。如果在接入点附近测试发现客户端发送的帧已损坏，而在客户端附近测试发现来自接入点的帧未被损坏，则可以确定存在接入点/客户端功率不匹配问题。

为了增加覆盖范围，接入点通常会按最大功率部署，这时接入点/客户端功率不匹配问题

通常就会发生。为了增加覆盖范围，提高接入点功率是一种错误的方法。如果希望增加覆盖范围，最好的解决办法是增加接入点天线的增益。大多数人不明白天线双向互惠(antenna reciprocity)的概念，这意味着天线即可以放大接收信号，也可以放大传输信号。接入点上的高增益天线放大了接入点的传输信号，扩展了可接收信号范围，同时也会放大来自远程客户端的信号强度。

应当指出的是，许多 WLAN 控制器厂商使用的动态射频管理能力是导致轻量型接入点和客户端之间功率不匹配的原因之一。WLAN 控制器可能会动态增加轻量型接入点功率，并超过客户端的发射功率。接入点传输功率的动态变化也是导致 VoWiFi 手机出现问题的原因。如果因为功率不匹配使 AP 不能“听”到电话返回的信号，可能出现声音不连贯或完全断开的现象。802.11k 修正案可以让 AP 告知客户端可以使用传输功率控制(TPC)功能动态更改其传输功率以匹配 AP 的发射功率。不过，在目前 802.11k 机制在客户设备中大多数都是专用的，未得到广泛支持。

12.1.6 近/远问题

多个客户端之间的发射功率设置不一致也可能导致在基础服务集(BSS)内的通信出现问题。如果大功率客户端离 AP 很近，离 AP 较远的低功率客户端可能无法被 AP 听到。大功率客户端提高了 AP 附近的本底噪声。较高的本底噪声可能会损坏来自远处客户端的传入帧，阻止低功率的客户端被 AP 听到，如图 12-11 所示。这种问题不仅仅是因为本底噪声水平提高导致的，更通常是由于当出现较强信号后再接收较弱信号时，AP 射频卡无法进行自动的增益控制而产生的。这有点像你刚听完演唱会后，离开时努力想听到别人低声讲话一样。这需要对导致近远问题的高度差别的信号进行快速适应。这就是远/近(Near/Far)问题。

图 12-11 近/远问题

传输媒介的半双工性质通常可以避免大多数近/远问题。你可以使用协议分析仪按分析接入点/客户端不匹配功率问题来进行近/远问题的故障诊断。

请理解下面的话：采用 CSMA/CA 媒介访问方法通常可以避免近/远问题，近远问题并不像接入点/客户端功率不匹配问题那么常见。一个规划良好、可以达到-70dBm 或更好信号覆盖的 WLAN 可以忽略这种问题的影响。

12.1.7　隐藏节点

在第 8 章中，你学习到物理载波侦听和空闲信道评估(CCA)。CCA 是指无线节点在物理层侦听 802.11 射频传输媒介，并在传输前要求媒介必须保持空闲。物理载波侦听的问题在于并非所有节点都可以互相侦听到对方。请时刻牢记无线传输媒介的半双工特性，在任何给定的时间，只有一个无线射频卡可以发送帧。如果一个客户端在执行完 CCA 后，并没有侦听到其他正在传输的无线节点，会发生什么事情哪？如果无线节点在执行 CCA 的过程中没有检测到任何射频能量，它便会开始传输。两个节点同时传输的结果就是帧发生碰撞破坏，重传将会发生。

当某客户端被接入点听到，但没有被 BSS 中的其他客户端听到，就会出现隐藏节点(hiddnen node)问题。客户端互相听不到对方，因此会同时传输。接入点如果听到两路相互干扰的传输信号，入向的传入就会失败。

图 12-12 显示了接入点的覆盖范围。请注意，一堵厚墙位于某客户端和所有其他客户端之间，这些客户端均与接入点关联。即使所有节点都可以听到接入点发出的传输信号，但这个单独的客户端的传输信号不能被所有其他节点“听到”。这个不能被“听到”的无线节点就是隐藏节点。每次隐藏节点传输信号，而其他节点之一也同时传输时就会发生冲突。隐藏节点会持续与在空闲信道评估过程中没有探测到该隐藏节点的所有节点发生碰撞。持续的冲突导致第 2 层重传，最终结果是吞吐量下降。隐藏节点可能使重传率达 15%～20%，甚至更高。重传当然也会影响吞吐量，产生延迟和抖动等问题。

图 12-12　隐藏节点——障碍物

拙劣的无线局域网设计或因为障碍物(如新建墙体或新安装的书架等)的影响都可能导致

隐藏节点问题。用户移动到某障碍物之后可能会导致隐藏节点问题。VoWiFi 电话往往也会成为隐藏节点，因为用户会考虑去安静的角落或地区接听电话，而在那些地方电话的射频信号无法被其他客户端侦听到。台式机用户通常将无线网卡置于金属桌子的底部，这很容易将该无线网卡转换成不为所知的隐藏节点。

隐藏节点在两个客户端位于 RF 覆盖蜂窝的两端时，有时也会发生，因为它们互相听不到对方，如图 12-13 所示。这在接入点发射功率过大导致更大的覆盖范围时经常发生。在本章后面部分你将学习到，通常推荐禁用接入点 2.4GHz 射频卡的 1Mbps 和 2Mbps 数据传输率以满足无线接入容量的目的。禁用这些数据速率的另一个原因是 2.4GHz 的 1Mbps 和 2Mbps 的覆盖蜂窝相当大，通常会导致隐藏节点。如果隐藏节点问题发生，可能需要 RTS/CTS 机制。这会在本章后面部分详细讨论。

客户端 A 和客户端 B 听不到对方信息

图 12-13 隐藏节点——较大的覆盖蜂窝

导致隐藏节点问题的另一个原因是分布式天线系统。制造商设计的分布式天线系统由同轴电缆和多个天线单元组成。分布式系统中的每根天线都有其自己的覆盖范围。出于节约成本的目的，许多公司部署分布式天线系统(DAS)。作为一种特殊解决方案，分布式天线系统和漏泄电缆系统也可以为蜂窝电话提供覆盖。如图 12-14 所示，如果只有一个 AP 连接 DAS 上时，隐藏节点问题几乎总会发生。即便要使用 DAS 解决方案，也要使用多个 AP。

图 12-14 隐藏节点——分布式天线系统

你是如何解决隐藏节点问题的？如果终端用户抱怨吞吐量下降，可能的原因之一就是隐藏节点。协议分析仪在确定隐藏节点问题时，是一个很有用的工具。如果协议分析仪显示某客户端比其他客户端重传率更高，隐藏节点就很可能存在。某些协议分析仪甚至可以基于重传阈值产生隐藏节点警报。

另一种方法是使用请求发送/清除发送帧(RTS/CTS)来诊断问题。为此可以尝试降低 RTS/CTS 阈值到约 500 字节。这个数值可以根据通信类型进行调整。例如，如果部署在仓库环境中的终端仿真应用存在隐藏节点问题，此时 RTS/CTS 阈值应设置为更小的值，如 50 字节。协议分析仪可用来确定这一阈值。在第 9 章中，我们知道 RTS/CTS 是客户端用来预留传输媒介的一种方法。图 12-15 描述的是隐藏节点启用 RTS/CTS 交换的过程。

图 12-15　隐藏节点与 RTS/CTS

障碍物另一边的无线终端可能听不到隐藏节点发出的 RTS 帧，但可以听到 AP 发出的 CTS 帧。接收到 CTS 帧的无线终端将重置其 NAV 值，确保这段时间隐藏节点可以传输数据帧并接收 ACK 帧。在隐藏节点上执行 RTS/CTS 可以预留传输媒介并强制所有其他无线节点暂停传输，碰撞和重传将会因此减少。

隐藏节点导致的碰撞和重传将使吞吐量降低。启用 RTS/CTS 机制通常也会降低吞吐量。但是，如果在被怀疑的隐藏节点上执行 RTS/CTS，吞吐量有可能因为碰撞和重传的减少而增加。如果被怀疑的隐藏节点在启用 RTS/CTS 后吞吐量反而增加，证明隐藏节点确实存在。

RTS/CTS 通常不应被视为解决隐藏节点的方法。RTS/CTS 只能临时解决隐藏节点问题，通常只用于诊断。但针对点到多点桥接(PtMP)是个例外。PtMP 方案中的非根网桥因为相隔很远，互相不能听到对方。RTS/CTS 应该部署在非根网桥上以消除因不能听到对方而产生的隐藏节点问题带来的冲突。

下面的方法可用来解决隐藏节点问题：

- 使用 RTS/CTS 诊断隐藏节点问题

使用协议分析仪或 RTS/CTS 进行隐藏节点问题诊断。RTS/CTS 还可用作临时解决隐藏节点问题的方法。

- 增加所有无线客户端的功率

大多数客户端具备固定的传输功率。但是，如果客户端的输出功率可以调整，增大发射功率可以增加客户端的传输范围。客户端互相听到对方的可能性就会随之增加。但是这不是推荐的解决方案，正如前面我们学过的，最佳实践是要求 BSS 中的所有无线节点具备相同的传输功率。

- 消除障碍物

如果确定某种形式的障碍物阻止客户端互相听到对方，简单的消除障碍物就可以解决这个问题。很明显，你不能随意拆除一堵墙，但如果障碍物是一张金属桌子或一个文件柜，可以将它简单换个地方就可以解决这个问题。

- 移动隐藏节点

如果一个或两个无线终端无法被其他节点侦听到，只需将其移动到其他节点的传输范围内，就可以解决这个问题。

- 添加新的接入点

添加新的接入点是解决隐藏节点问题最好的办法。如果无法移动隐藏节点，那么就在隐藏节点所在区域添加一个新的接入点即可纠正这个问题。

12.2 802.11 信号覆盖要点

无线局域网设计中良好的覆盖和容量设计能够解决许多问题。漫游问题和干扰问题常常可以因为正确的无线局域网设计和全面的现场勘测而提前避免。下面将讨论为在 802.11 覆盖区域提供合适的覆盖范围、容量和性能需要考虑的诸多因素。

12.2.1 动态速率调整

当客户端逐渐远离接入点，带宽也将逐步下降，这个过程称为*动态速率调整*(Dynamic Rate Switching，DRS)。接入点可以支持的数据速率取决于接入点无线射频卡采用的扩频技术。例如 802.11b 射频卡支持 11Mbps、5.5Mbps、2Mbps 和 1Mbps。在图 12-16 中，接入点和无线客户端之间的传输速率增加还是下降取决于信号质量。信号质量与距离 AP 的位置有一定的关系。当移动客户端距离 AP 越来越远时，AP 和客户端都会切换到较低速率，因为速率越低所需要的编码调制计划(MCS)越简单。例如两个 802.11b 无线射频卡之间的传输速率在 30ft 时可能为 11Mbps，但在 100ft 时就只有 2 Mbps 了。

图 12-16　动态速率转换

DRS 也称为动态速率切换、自适应速率选择或自动速率选择。所有这些术语都是指无线局域网客户端接收速度随来自发射端的入射信号质量下降而下降的反馈方式。DRS 的目标是优化速率和改善传输性能。较低的数据速率将比更高的数据速率有更大覆盖区域，如图 12-17 所示。

图 12-17　不同速率下的覆盖区域

动态速率切换的算法通常是私有的，由无线网络厂商定义。多数厂商的动态速率调整基于接收信号强度指示(RSSI)阈值、数据包错误率和重传率等因素。而 RSSI 度量值通常基于信

号强度和信号质量。换句话说，无线节点的数据速率可能根据接收信号强度和信噪比(SNR)值上下波动。因为厂商采用不同的方式实现 DRS，于是可能出现这样的情况：两个不同厂商的客户端无线网卡处于相同的位置，与 AP 的连接速率可能一个为 5.5Mbps 而另一个为 1Mbps。例如，一家厂商在-75dBm 时数据速率可能从 11Mbps 下降到 5Mbps，而另一个厂商可能在-78dBm 时才会进行相同的切换。请记住，DRS 适用于所有的 802.11 物理层标准。例如，802.11ag 网卡都会在 54Mbps、48Mbps、36Mbps、24Mbps、18Mbps、12Mbps、9Mbps 和 6Mbps 数据率之间进行切换。因此信号质量与离 AP 的距离之间有相关性。

在设计 2.4GHz 的 802.11b/g/n 网络时，通常推荐关闭最低的 1Mbps 和 2Mbps 数据速率。无线局域网管理员考虑禁用 802.11b/g 接入点最低的两个数据速率有三个原因：客户端不漫游问题、传输媒介竞争问题和隐藏节点问题。在图 12-18 中，多个客户端处于 1Mbps 区域，只有一个客户端处于 11Mbps 区域。请记住无线媒介是半双工特性，同时只能有一个无线射频卡可以传输数据。

图 12-18 帧传输时间

当 802.11 射频网卡以非常低的速率传输时(例如1Mbps或2Mbps)，它们将使高速率客户端传输由于较长的等待时间产生很大的媒介竞争开销。所有射频卡访问媒介时都依照由 CSMA/CA 定义的伪随机方式。射频设备以 11Mbps 的速率传输 1500 字节的数据帧可能会占用媒介 300 微秒。另一种射频设备按每秒 1Mbps 的速率传输相同的 1500 字节需要占用 3300 微秒。传输速度较慢的射频卡将占据媒介更长时间，而较快的射频卡不得不等待。如果位于外层蜂窝边缘的多数无线网卡持续按较慢的传输速度传输数据，更高速率的无线网卡不得不等待较慢的网卡数据传输完成。因此位于 1Mbps 和 2Mbps 蜂窝内如果存在太多的无线客户

端将会显著影响吞吐量。

第 8 章已经讲述了通话公平机制。大多数厂商会利用私有的通话公平机制针对来自 AP 的下传流量进行处理。通话公平机制通常会对从 AP 发往高速率客户端的流量优先处理。如果部署得当，可能就无需关闭较低的 2.4GHz 速率。

关闭较低的数据速率的另一个原因是隐藏节点问题，这在本章前面部分已经阐述过了。

12.2.2　漫游

从本书中你已经了解到，漫游(Roaming)就是客户端在射频覆盖蜂窝之间进行无缝移动的方法。客户端移动时需要在不同 AP 间进行通讯转换，而在扩展服务集(ESS)内的覆盖区域之间进行无缝通信对于确保无线节点的不间断漫游至关重要。现实中最常见的无线故障之一也是漫游。漫游问题通常是由拙劣的网络设计引起的。由于漫游方法的私有性质，在存在多个厂商无线网卡的网络时，可能会出现漫游问题。无线局域网环境的变化也会导致漫游问题。

客户端对是否在接入点之间漫游具有决定权，这个权利不由接入点掌控。可能一些厂商的接入点或 WLAN 控制器也参与漫游决定，但最终是由客户端发送重关联请求帧启动漫游进程。客户端决定漫游的方法完全是私有的。各个厂商无线客户端使用的漫游算法可能由一系列私有规则决定，通常是由接收信号强度指标(RSSI)阈值决定的：RSSI 阈值通常与信号强度、噪声强度及比特错误率有关。客户端在通讯过程中，不断通过探针查询寻找其他 AP，并且学习这些 AP 的信号强度。决定漫游最重要的因素还是接收信号强度。当来自原始接入点的信号强度变弱，而来自另一个已知接入点的信号变强，无线节点将启动漫游过程。但是，其他变量(如信噪比、错误率和重传率)也可能影响漫游决定。

如图 12-19 所示，当客户端逐渐远离之前关联的原始 AP，信号将低于预定阈值，客户端开始尝试连接具有更强信号的目标接入点。客户端通过发送重关联请求帧开启漫游进程。

图 12-19　漫游

因为漫游方法是私有的，某厂商的客户端可能比其他厂商的客户端更早发生漫游。一些厂商鼓励客户端漫游，而有些厂商的客户端使用的漫游算法在接收到更低的接收信号时才会漫游。在一个存在不同厂商无线客户端的环境中确实能看到不同的漫游行为。无线局域网管

理员总是面临因为漫游的不同行为导致的独特挑战。第 5 章中所述的 802.11k 修正案描述了如何使用无线资源测量(RRM)和邻居报告(neighbor report)来增强漫游性能。802.11r 修正案还定义了在使用强健安全网络(RSN)所定义的强健安全性无线局域网蜂窝间漫游时的快速切换。

802.11k 与 802.11r 在客户端方面的支持

尽管某些厂商已经在其 AP 和控制器上支持 802.11k 和 802.11r，但大多数厂商仍未支持。Wi-Fi 联盟很快将开始用一种新的认证来测试厂商产品是否支持 802.11r(安全漫游)和 802.11k(资源管理)的某些方面，这个认证称为企业级语音(Voice Enterprise)。一旦 Voice Enterprise 成为现实，我们就可以期待客户端对 802.11r 和 802.11k 的支持。

确保无缝漫游的最佳方式要从正确的设计和全面的现场勘察开始。在设计 802.11 网络时，大多数厂商推荐所需的信号覆盖蜂窝要有 15%～30%的-70dBm 信号区域的重叠。检测蜂窝重叠情况是否正常的唯一方法是进行正确设计和现场勘测。多年来，来自 WLAN 厂商的白皮书和设计指南都引用 15%～30%的蜂窝重叠比例，如图 12-20 所示。但问题是如果才能计算和测试蜂窝重叠程度。蜂窝重叠可以用周长、直径或半径测量吗？WLAN 厂商白皮书，甚至包括本书都利用插图来描述覆盖蜂窝为完美的圆形区域。实际上覆盖蜂窝有着很奇怪的形状，好像变形虫或星爆体。如果每一个覆盖蜂窝都有不同的形状，怎么测试蜂窝重叠比例呢？

图 12-20 蜂窝重叠

Wi-Fi 现场勘测专家 Keith Parson 多年来一直在纠正 AP 覆盖重叠区域测试的误区。覆盖重叠区域应该是指 Wi-Fi 客户端的重复区域。应该完成适当的现场调查，确保客户端始终适当地“复制”了多个 AP 的覆盖区域。换句话说，每个无线客户端都应该至少能够听到一个特定 RSSI 的 AP 及另一个不同 RSSI 的 AP。大多数厂商的 RSSI 阈值要求在-70dBm 以上，以达到较高的数据率。因此客户端需要听到至少两个达到-70dBm 的 AP，以满足客户端漫游的需求。确定客户端是否拥有足够重复区域的唯一办法就是执行覆盖分析现场勘测。第 16 章会详细讨论正确的现场勘测程序。

如果没有足够的蜂窝范围重叠，漫游就会发生故障。重叠太少会产生漫游盲区，无线连接甚至可能会暂时丢失。另一方面，蜂窝重叠过度也会产生漫游故障。例如，无线客户端可能一直保持与原始接入点的关联而不连接到第二个接入点，即使无线客户端就位于第二个接入点的正下方。另外还可能会导致客户端设备不断地在两个或多个不同信道的接入点之间来回切换。如果客户端可以听到很多具有相同信道且信号很强的 AP，会导致通信性能下降，原因在于媒介竞争开销的影响。

另一个重要的设计问题是延迟。802.11-2007 标准定义了在企业中使用的 802.1X/ EAP 安全方案。认证过程所花费的平均时间大概是 700 毫秒或更长的时间。当部署 802.1X/RAP 安全解决方案后，客户端每次漫游到一个新的访问点，都要求重新认证。但认证过程产生的时间延迟可能导致对时间敏感的应用程序严重中断。漫游时，VoWiFi 要求在漫游切换时不超过 150 毫秒的延迟。如果 802.1X/EAP 安全性和时间敏感的应用程序在无线网络中同时使用，就需要利用*快速安全漫游*(fast secure roaming/FSR)解决方案。目前大多数厂商部署的是非标准的 FSR 方法，这种方法称为*机遇性密钥缓存*(OKC)。IEEE 定义了*快速基础服务集转换*(FT)作为标准的快速安全漫游标准，但客户端仍然很少支持 FT。正如前面提到的，只有当 Wi-Fi 联盟开始实施 Voice Enterprise 认证之后，标准化的 FT 机制才会逐步变成现实。

非标准的快速安全漫游机制(如 OKC)及标准的快速基础服务集切换(FT)不是 CWNA 考试的范畴。但是快速安全漫游机制在 CWSP 考试中所占的比例很重。

无线局域网环境的变化也会导致令人头痛的漫游问题。射频干扰总是会影响无线网络的性能，也会导致漫游问题。在建筑物中的很多新建工程会影响无线局域网覆盖范围，并产生新的覆盖盲区。无线局域网所在的物理环境更改，覆盖设计可能也不得不随之更改。经常定期进行覆盖勘测总是个好主意。

使用协议分析仪对漫游故障进行排除是很棘手的，因为漫游的重关联过程需要在多个信道上进行数据帧交互。如果要对在信道 1、6 和 11 间漫游的客户端进行排错，你需要三个单独的协议分析仪安装到三个单独的笔记本电脑上进行三个信道的数据帧帧捕获。CACE 提供了一种叫 AirPcap 的 USB 802.11 无线产品。如图 12-21 所示，三个 AirPcap USB 射频接口被配置为同时捕获 1、6 和 11 信道的帧。所有三个射频接口都连接到一个 USB 集线器，将所有三个信道捕获的帧保存到一个具有单一时间戳的捕获文件中。AirPcap 解决方案允许只用单个协议分析仪进行多信道监测。

图 12-21　AirPcap 提供多信道监控和漫游分析

12.2.3 三层漫游

设计无线局域网需要考虑的一个重要因素是当客户端跨第三层边界进行漫游时，会发生什么事情？Wi-Fi 运行在第二层，漫游本质上也是第二层的过程。如图 12-22 所示，客户端在两个接入点之间漫游，在第二层是无缝进行的，但两个接入点被路由器分隔处于两个不同子网。换句话说，漫游发生时客户端将失去第 3 层连接，因为其必须获取一个新的 IP 地址。任何运行时需要重新建立第 3 层连接的客户端的面向连接的应用程序将不得不重新启动。例如，VoIP 会话会断开，这种情况下，将不得不重建呼叫。

图 12-22 第三层漫游边界

当然我们可以只在相同的第 3 层域内进行 Wi-Fi 蜂窝重叠设计。但是，因为 802.11 无线网络通常会与原有的有线拓扑集成，跨越第 3 层边界通常难以避免，在大型部署中尤其如此。穿越第 3 层子网仍然保持上层通信的唯一方法是提供移动 IP(Mobile IP)解决方案或专有的第 3 层漫游解决方案。移动 IP(Mobile IP)是互联网工程任务组(IETF)的标准协议，允许移动设备用户从在第 3 层间移动时保持其原始的 IP 地址。移动 IP 在 IETF RFC 3344 中定义。移动 IP 和专有解决方案都使用某种类型的隧道和 IP 头封装方法，以允许数据包在第 3 层域间传输时维持上层通讯。基于标准的移动 IP 或专有的第 3 层漫游解决方案都超出了本书讨论范围；目前大多数 WLAN 控制器都支持某种类型的第三层漫游技术。如图 12-23。

移动客户端在本地网络获取的 IP 地址，称为本地地址。移动客户端必须把它的本地地址注册到一个被称为本地代理(Home Agent)的设备上。位于客户端本地网络上的 WLAN 控制器将成为本地代理。本地代理是漫游客户端在三层漫游过程中唯一的联系点。本地代理与另一个称为外部代理(Foreign Agent，FA)的设备共享客户端的 MAC 地址和 IP 地址数据库，这个数据库也称为本地代理表(HAT)。在本例中，外部代理是另一台 WLAN 控制器，代表漫游客户端与本地代理进行所有的移动 IP 通信。外部代理 IP 地址称为 Care-of address。当客户端进行三层漫游时，客户端漫游到外部代理(FA)所在的网络。FA 通过 HAT 表定位客户端的 HA 后，与 HA 建立移动 IP 隧道。发送给 HA 的客户端流量由 HA 负责拦截，然后通过通过移动

IP 隧道返回 FA。FA 将数据再传给客户端，客户端的本地地址得以保持。在本例中，移动 IP 隧道位于两台 WLAN 控制器之间，对于有些无需控制器的厂商，该隧道是在 AP 间建立的。

图 12-23　Mobile IP

虽然采用第三层漫游可以维持上层通讯，但由此增加的延迟通常会是一个问题。另外，第 3 层漫游可能并无必要。简单的基础架构经常使用扁平二层架构。对于大型的企业网络，因为存在大量用户，需要创建许多不同子网的 VLAN，这时才需要三层漫游解决方案。

12.2.4　同频干扰

很多企业在首次部署无线局域网时遇到的最常见错误是同频干扰，即在同一信道上配置多个接入点。如果所有接入点都处于同一信道，就会产生很多不必要的媒介竞争开销。如你所知，CSMA/CA 规定在半双工通信期间，同一信道上只有一个无线设备可以进行传输。

如图 12-24 所示，如果接入点在信道 1 传输，附近同一信道的所有接入点和客户端都将推迟传输。其结果是，吞吐量受到不利影响：附近的接入点和客户端传输前要等待很长时间，因为它们要轮流传送。因所有接入点处于同一信道导致的不必要的媒介竞争开销称为同频干扰(co-channel interference/CCI)。在现实中，802.11 的射频操作完全由 CSMA/CA 机制定义，这种行为实际上应该称为同频协作(co-channel cooperation)。同频干扰造成的不必要的媒介竞争开销是错误的信道复用设计的结果，这将在下一节中讨论。

请不要混淆同频干扰与邻频干扰。不过邻频干扰问题也是错误地信道复用设计的结果。如图 12-25 所示，交叠的覆盖蜂窝和交叠的相邻频率空间会导致数据损坏和第 2 层重传。请参阅图 12-6，图中信道 1 和 4、4 和 7、7 和 11 在频率空间存在交叠部分。由于数据损坏和第 2 层重传，邻频干扰比同频干扰带来的影响更加严重。解决同频和邻频干扰的方法是进行正确的信道复用设计。

图 12-24 同频干扰

图 12-25 邻频干扰

12.2.5 信道复用/多信道体系结构

为避免同频与邻频干扰，信道复用设计非常必要。另外，重叠的 RF 覆盖蜂窝是漫游必须的，但必须避免频率重叠。在 2.4GHz ISM 频段只有三个信道满足这些条件，在美国这三个信道是 1、6 和 11。因此重叠的覆盖蜂窝应按如图 12-26 中的信道复用(channel reuse)方式进

行设计。无线局域网信道复用方式也称为多信道体系结构(multi-channel architecture/MCA)。2.4GHz利用三个信道或5GHz利用更多信道进行重叠覆盖蜂窝设计的无线局域网架构被称为多信道体系结构。

图 12-26　2.4GHz 多信道架构

应当指出的是，在 2.4GHz 频段采用三信道复用方式是无法避免全部同频干扰问题的，因为很难避免信号在相同信道的重叠。如果在信道复用模式中只有三个信道可以利用，AP 会有相当大的机会出现信道相同且位于可以互相听到的区域。在欧洲和世界其他一些地区，在 2.4GHz ISM 频段范围可以有更多合法信道，于是四信道部署模式有时也会出现(即 1、5、9、13 信道)。尽管四信道之间可能存在少量重叠，但总体性能因为同频干扰减少的原因在某些场景下会有所提高。然后四信道规划存在下列缺点：

- 如果附近 AP 部署在传统的 1-6-11 信道，将对四信道规划的 AP(1-5-9-13)产生严重的邻频干扰；
- 所有北美的 Wi-Fi 射频卡都受到严格限制，不得使用信道 13。这些地区购买的笔记本电脑、IPad 或其他移动设备将无法连接使用信道 13 的 AP。

出于这些原因，更加传统的三信道规划在欧洲使用更加普遍。四信道规划在美国或加拿大从来没有部署过。

另外还要注意，客户端之间也会因为媒介竞争产生同频干扰。如图 12-27，如果一个位于某信道边缘的客户端发出的信号传播到了另一个具备相同信道的 AP，在该 AP 蜂窝内的客户端也会延迟传输。

图 12-27 客户端与同频干扰

信道复用模式也可在 5GHz 频段使用。如果所有 5GHz 频段都可以合法使用，总共将有 24 个信道。在美国可以利用 24 个信道中的 21 个。信道 120～128 在美国被预留给机场多普勒天气雷达(TDWR)使用；因此 FCC 定义了 DFS 规定限制 5600MHz～5650MHz 频率的使用。在欧洲不可以使用信道 165 及 UNII-3 信道，因此只有 19 个可用信道。根据地区的不同，可能还有 8 信道、12 信道、19 信道、21 信道或者其他 WLAN 信道复用模式。图 12-28 描述了使用 UNII-1、UNII-2、UNII-3 中 12 个信道的复用模式。尽管根据 IEEE 的定义，所有 5GHz 信道之间是不重叠的，但实际上相邻信道仍然存在部分的边带重叠。推荐相邻蜂窝的信道至少相隔 2 个信道，不要使用相邻频率。遵守这个简单的规则就可以避免由于边带重叠导致的邻频干扰。

相同信道至少间距两个蜂窝

图 12-28 5GHz 多信道架构

正如图 12-28 中看到的，5GHz 信道复用设计中，第二个推荐原则是：相同频率的 AP 间至少相隔两个蜂窝单元。遵循这个原则可以防止来自 AP 的同频干扰和来自客户端的大部分同频干扰。在到达另一个相同频率的蜂窝区域之前，客户端的信号不得不传播更远的距离，信号强度会衰减到本底噪声以下。

真实世界场景

我应该在 5GHz 信道复用模式中使用多少个信道？

在规划 5GHz 信号复用模式时应该考虑下面几个因素：

- 第一个需要考虑的因素是所在国家或地区可以合法使用的信道是什么？

在欧洲，最常见的模式是使用 UNII-1、UNII-2、UNII-2E 频段中的 19 个信道。由于相关规定，不可以使用 UNII-3 的信道。

- 第二个需要考虑的因素是客户端支持的信道是什么。

在美国，复用模式可以使用 21 个信道；但是只使用由 UNII-1 和 UNII-3 组成的非 DFS 频段的 8 信道模式是最佳选择。如图 12-29 所示。

图 12-29　示意图

为避免和雷达干扰，Wi-Fi 射频卡必须通过在动态频率选择(DFS)信道传输的认证。很可能客户端没有通过在 UNII-2 和 UNII-2e DFS 信道的认证。尽管 AP 通过认证，可以在 DFS 信道工作，但是客户端没有通过认证，只能在 UNII-1 和 UNII-3 信道工作，导致 Non-DFS 客户端无法连接工作在 UNII-2 和 UNII-2e 的 AP。

- 第三个需要考虑的因素是 VoWiFi 电话在漫游时进行 AP 查找所执行的被动或主动的离频扫描。如果客户端扫描的信道越多，它在漫游时选择最佳 AP 的时间越长。过度扫描也会对 VoWiFi 客户端的电池续航能力造成负面影响。

在进行多信道架构复用设计时总是进行三维模式思考是必要的。如果接入点部署在同一幢的多个楼层，复用模式将很有必要，如图 12-30。执行现场勘察一个常见的错误是在每一层相

同的位置千篇一律的部署处于同一信道的接入点。执行现场勘察时对所有楼层通常需要采用三维复用模式错开接入点信道。此外，每个接入点的覆盖蜂窝不应该超出该接入点上面一个或下面一个楼层。不要误认为接入点信号覆盖到其他楼层仍可以提供足够的信号强度和质量。某些情况下，各层楼面的混凝土或钢筋只能通过很少量的射频信号。因此，调查是绝对必要的。

图 12-30 三维信道复用

大部分企业级接入点具有双频功能，在同一区域可以同时部署 2.4GHz 和 5GHz 无线网络。接入点的 802.11a/n 5GHz 信号比 802.11b/g/n 2.4GHz 的无线信号衰减得更快。因此，在执行双频无线局域网部署现场勘测时，推荐先执行 5GHz 的勘测，并确定接入点位置。确定这些位置后，再使用信道复用模式进行频点规划。

12.2.6 单信道体系结构

在撰写这本书时有两个厂商 Meru 和 Extricom 提供称为单信道体系结构(single channel architecture/SCA)的无线局域网信道设计解决方案，试着想想一个 WLAN 中有多个接入点处于同一信道且共享相同的 BSSID。SCA 就是这样一种架构。客户端观察到一个 SSID(逻辑

WLAN 标识符)只位于一个信道且只存在一个 BSSID(第 2 层标识符)。这样从客户端的角度看，就只有一个 AP 存在。这种类型的 WLAN 体系结构，网络中的所有接入点只可以在 2.4GHz 或 5GHz 频带的一个信道上部署。WLAN 控制器在一个 802.11 信道上进行上行和下行传输的协调控制，将同频干扰的影响降到最低。

让我们首先讨论单一的 BSSID。单信道体系结构由 WLAN 控制器和多个轻量级接入点构成。如图 12-31 所示，每个接入点都有自己的射频卡和 MAC 地址；然而，它们广播相同的虚拟 BSSID。

图 12-31　单信道体系结构

因为多个接入点只宣告一个虚拟 MAC 地址(BSSID)，所以客户端在漫游时跨越多个物理 AP 时只认为它们连接在一个接入点之上。漫游由客户端决定，但在单信道体系结构系统(SCA)中，客户端认为只有一个接入点与之关联，所以它们永远不会进行第 2 层漫游。所有实际的漫游切换由中央 WLAN 控制器处理。

如图 12-32 所示，SCA 的主要优势是客户端在漫游时经历了零切换(Zero handoff)时间，漫游延迟问题可以得到解决。SCA 所采用的虚拟 AP 方案与 VoWiFi 手机和 802.1X/EAP 解决方案是潜在的绝佳组合。正如我们刚才讨论的，EAP 认证过程所涉及的平均时间可能达 700 毫秒或更长。当部署 802.1X/EAP 安全解决方案时，客户端每次漫游到一个新的接入点，都需要重新进行认证。VoWiFi 要求漫游切换时间不超过 150 毫秒。虚拟 BSSID 消除了在单信道体系结构中进行物理漫游的重认证需求，并在漫游时产生零切换时间。

图 12-32 零切换时间

在 MCA 架构环境中，客户端做最终的漫游决定。但在 SCA 环境中，客户端并不知道它们发生了漫游。但客户端仍然必须是移动并在物理 AP 之间传输第 2 层通讯信息。所有客户端的漫游机制此时由 WLAN 控制器处理，客户端侧的漫游决定权被取消。SCA WLAN 控制器维护所有客户端的关联并管理所有轻量级接入点。SCA 控制器为每个客户端分配一个 AP 处理下行链路。当控制器接收到入方向的客户端传输时，SCA 控制器会评估客户端的 RSSI 值。基于传入的 RSSI 测量值，SCA 控制器可以分配一个特定的 AP 进行下行链路传输。客户端认为它只与单一的 AP 相关联。但是，基于控制器进行的 RSSI 测量评估，客户端会在不同物理 AP 之间切换。

单信道体系结构的一大优势是邻频干扰不再是一个问题。如果所有接入点都位于同一信道，因频率重叠导致的邻频干扰就不可能发生。但如果所有接入点都在同一信道，难道不会产生同频干扰吗？如果在 MCA 架构中所有 AP 处于同一信道，不必要的媒介竞争开销就会发生。在典型的 MCA 环境中，每个接入点都有单独的 BSSID 和单独的信道，以及每个接入点的覆盖蜂窝都是一个冲突域。而在 SCA 无线环境中，冲突域由基于 RSSI 算法的 SCA 控制器动态管理。控制器确保同一信道的相邻设备不在同一时间传输。SCA 厂商用于集中管理同频干扰的机制并未公开，这超出了本书的讨论范围。

SCA 架构的主要缺点是传输容量问题，因为只有一个信道是可用。在 2.4GHz SCA 部署中，多个 AP 可以通过使用三个信道和三个虚拟 BSSID 部署在一起。SCA 的多 AP 共处的设计通常被称为信道堆栈(channel stacking)。每层的多个 AP 使用同一虚拟 BSSID 被称为一个信道地毯(channel blanket)或者信道跨越(channel span)。虽然在理论上这听起来像个好主意，但大多数客户不愿意花三倍的钱来部署无线局域网。另一个可能的缺点是竞争域过大。尽管通过 SCA 控制器通过协调 AP 传输了减少了 AP 间的冲突，但因为 SCA 机制高度封闭，无法确保客户端的传输可以得到控制。

12.3　容量与覆盖

设计无线网络时，通常互相竞争的两个概念就是容量(capacity)和覆盖(coverage)。无线网络建设早期，我们通常会安装一个 AP 并将其功率设置为最高水平，以提供最大的覆盖范围。这通常可以接受，因为无线客户端很少，加之 AP 价格非常昂贵，所以公司经常试图使用最少数量的 AP 覆盖尽量大的范围。图 12-33 表明了在 MCA 结构中由三个 AP 对建筑物进行覆盖的区域轮廓。如果仅有几个客户端，这种类型的无线设计是完全可以接受的。

图 12-33　使用三颗 AP 进行建筑射频覆盖(无线客户端很少)

随着无线设备的增加，网络设计也开始发生变化。正确的网络设计现在不仅需要提供必要的覆盖面，同时还尝试限制同时连接到单个 AP 的设备数量。这就是所谓的“容量和覆盖”的意思。如你所知，连接到一个单一的接入点的所有客户端共享该接入点的吞吐量。因此，限制同时连接到一个单一接入点的客户端数量是一项重要的设计内容。首先要确定你想要连接到 AP 的最大客户端数量(这取决公司网络使用情况)。在 MCA 环境中，你需要确定能提供恰当容量的蜂窝的大小，然后需要调整 AP 的功率级别，以创建所需大小的蜂窝。

图 12-34 显示的是同一栋建筑物的轮廓，但因为存在很多无线客户端，无线蜂窝的尺寸减小而蜂窝的数量增加。调整传输功率以限制覆盖范围的方式称为蜂窝调校(cell sizing)，这是在 MCA 环境中满足容量需求的最常用方法。

图 12-34　蜂窝调校——多信道架构

因为无线客户端的爆发性增加，无线局域网的高密度用户部署越来越成为关注点。无线

客户端不再只有笔记本电脑，大多数用户希望他们的 iPad 和智能手机也接入 WLAN。幸运的是，802.11n 可以提供更高的带宽。但是现在即便是 802.11n AP 也难以负担。大多数 WLAN 厂商使用私有的负载均衡、频带操控和其他 MAC 层机制来满足高密度用户环境下的容量需求。

12.3.1 超大尺寸的覆盖蜂窝

在部署时将 AP 调整至最大功率是经常犯下的错误。尽管大多数 AP 可以达到最高 100mW 的功率，在实际部署中却很少按最大功率部署。虽然这延伸了接入点的范围，但也导致了很多问题，这些已经在本章讨论了。过大的射频覆盖通常不能满足容量需求。超大的覆盖蜂窝也可能导致隐藏节点问题。全功率发射的接入点可能无法侦听到较低发射功率的客户端。全功率接入点也会大大增加同频干扰的几率。因为上述原因，通常室内 AP 的发射功率设置为最大传输功率的四分之一或三分之一。在高密度用户部署中，甚至将 AP 的发射功率设置为最低的 1mW。如果关注接入点的覆盖区域，增加覆盖范围的最佳方法是增加 AP 的天线增益，而不是增加发射功率。

12.3.2 物理环境

虽然物理环境不会导致射频干扰，但物理障碍物确实可以扰乱和破坏 802.11 信号。例如受钢丝网围栏或内嵌金属丝网的安全玻璃影响产生的射频散射效应。信号被分散后便形同虚设。消除物理干扰的两个方法是移除障碍物或添加 AP。请记住每个建筑物和楼层的物理环境不同，无线蜂窝的形状和大小也不同。处理物理环境的最佳方法是进行正确的现场勘测，这会在第 16 章中详细说明。

12.4 语音和数据

正如你在前面部分已经学到的，大多数 Wi-Fi 应用可处理第 2 层高达 10%的重传且不会有任何明显的性能下降。不过，如 VoIP 等对时间敏感的应用程序则要求高层 IP 数据包丢失不得超过 2%。因此，VoWiFi 网络需要限制第 2 层重传率不超过 5%以保证及时和一致的 VoIP 数据包传递。当第 2 层重传超过 5%时，延迟问题可能发生并极可能出现抖动问题。

金丝雀与蟑螂的故事

金丝雀与煤矿的类比通常用于描述无线局域网环境中语音通信和其他数据应用程序通信的区别。早期的煤矿没有安装矿井通风系统，所以矿工会将装在笼子里的金丝雀一同带入。金丝雀比人类对甲烷和一氧化碳气体更加敏感，这使它们适合用来检测危险气体。只要那只金丝雀(语音通信)在歌唱，矿工们就知道空气供应是安全的。金丝雀死亡就意味着致命气体存在，矿工会撤离或戴上防毒面罩。但是，某些物种，如一只蟑螂(数据通信)在煤炭矿井中存在致命气体时仍能生存，尽管在不存在恶劣条件的情况下活得更好一点。

很多时候，企业部署无线局域网时没有进行任何类型的现场勘测。此外，许多无线局域网最初旨在提供针对数据应用程序的无线覆盖，而不是语音。大多数企业数据应用程序在这样设计不佳的无线局域网内运行，由于缺乏现场勘测或因勘测错误，也无法进行运行优化。许多公司决定将 VoWiFi 应用添加到无线局域网中，但他们很快发现无线局域网存在很多问题。VoWiFi 电话可能有断断续续的音频或回声问题。VoWiFi 电话可能会中断或者像那只金丝雀一样“死掉”。将语音添加到无线局域网中通常会暴露存在的问题：因为数据应用程序能够承受更高的第 2 层重传率，在无线局域网中存在的问题可能被忽视。如表 12-1 所示，IP 语音通信更容易受到因第 2 层重传导致的延迟或数据包不连续的影响。

表 12-1　IP 语音和 IP 数据对比

IP 语音(金丝雀)	IP 数据(蟑螂)
报文小，尺寸固定	报文长度不固定
平均，可预测的交付	突发交付
易受不连续的报文交付或延迟影响	不易受不连续的报文交付或延迟影响
Better never than late(时延敏感)	Better late than never(时延不敏感)

为支持语音通信，优化无线局域网可使所有的无线客户端受益，不仅包括语音应用的客户，还包括运行数据应用程序的客户。正确的现场勘察可以减少第 2 层重传，并提供 VoWiFi 网络所需的无缝覆盖环境。

12.5　性能

设计和部署无线局域网时，你总会同时关注覆盖和容量参数。许多因素可以影响到无线蜂窝的覆盖范围，许多因素还会影响到 802.11 无线局域网的聚合吞吐量。下列变量可能影响到无线局域网的覆盖范围：

- 发射功率

原始发射功率会影响到射频蜂窝的范围。在假设使用相同天线的情况下，30mW 的 AP 比 1mW 的 AP 覆盖区域更大。AP 的传输振幅太高可能会导致很多问题，这些已经在本章讨论过。

- 天线增益

天线是可将原始信号聚集传输的被动增益设备。一个 30mW 的 AP 使用 6dBi 天线将比使用 3dBi 天线的传输范围更大。如果你要为客户增加覆盖范围，最好增加 AP 的天线增益。

- 天线类型

天线具有不同覆盖模式。使用正确的天线可以得到适当的覆盖范围，并减少多径现象和附近的干扰。

- 波长

高频率信号的波长较小，将比具有较大波长的低频信号衰减得更快。在所有条件都相同的情况下，由于波长的差别，2.4GHz 的接入点比 5GHz 接入点的覆盖范围更大。

- 自由空间路径损耗

在任何射频环境中，自由空间路径损耗(FSPL)都按照距离和频率的函数进行衰减。

- 物理环境

因为吸收与其他射频传播行为，墙和其他障碍物会导致信号衰减。采用混凝土墙结构的建筑物将比采用石膏板墙的建筑物需要更多的接入点，因为混凝土比石膏板墙更密实，衰减也更快。

正如在前面的章节中你已经学到，恰当的无线局域网设计必须考虑到覆盖和容量因素。刚才提及的所有变量可以影响覆盖范围。但容量性能与覆盖范围同样重要。请记住，802.11 数据速率指的是数据带宽而不是吞吐量。以下是会影响无线局域网吞吐量(throughput)的多个变量。

- 载波侦听多路访问/冲突避免(CSMA/CA)

使用帧间间距、物理载波侦听、虚拟载波侦听和随机回退计时器的媒介访问方法，产生开销并消耗带宽。在传统的 802.11a/b/g 网络中媒介竞争引起的开销通常达 50%甚至更高，80211n 网络此类开销通常是 20%～30%。

- 加密

只要实现加密，都需要给 802.11 数据帧主体增加额外开销。WEP/RC4 加密方式为每个帧添加 8 个字节的系统开销；TKIP/RC4 加密方式为每个帧添加 20 个字节的系统开销；CCMP/AES 加密方式为每个帧添加 16 个字节的系统开销。第 3 层 VPN 通常使用 DES 或 3DES 加密，这两种方式也会消耗大量带宽。近年来，由于处理能力的增强和 802.11n 的高数据率能力，已经使加密开销不再成为严重问题。

- 应用程序

不同类型的应用程序对带宽消耗的影响也不同。VoWiFi 和数据收集扫描通常不需要大量带宽。而文件传输或数据库访问等应用程序往往是带宽密集型。

- 客户端数目

请记住无线局域网是一个共享媒介。所有吞吐量都是聚合的，所有可用带宽都是共享的。

- 第 2 层重传

本章中已经讨论了各种可能导致帧损坏的问题。如果帧受损，它们将需要重传，吞吐量也将受到影响。

12.6 天气影响

在部署户外无线网状网络或户外桥接网络时，无线局域网管理员必须考虑到天气的不利影响。必须考虑以下的天气影响：

- 闪电

直接和间接的闪电可能会损坏无线局域网设备。避雷器应该用于对瞬态电流的保护。避雷针、铜或光纤收发器解决方案也可以提供电击防护。

- 风

由于较长的距离和天线狭窄的波速宽度，高增益定向天线很容易受到移动或风的影响。

即使轻微的移动，高增益定向天线也可能偏离接收天线，导致通信中断。在高风环境，栅格天线通常比碟型天线更稳定。其他固定措施也有助于保持天线稳定，避免移动。

- 水

如雨、雪和雾等气象条件带来了两个独特挑战。第一，所有户外设备必须防止因水引起的损害。水渍破坏往往会对电缆和连接器造成损坏。采用滴水弯和同轴套管密封可以保护连接器防止受侵害。应该定期检查电缆和连接器是否损坏。应该使用天线罩(全天候保护罩)来防止水对天线造成损害。

户外桥接设备、接入点和网状网路由器应该采用符合国家电气制造商联盟(NEMA)标准的密封单元防止水的侵害。冰雹可能导致射频信号衰减。一场倾盆大雨可以在 2.4GHz 和 5GHz 的频率范围内使信号产生高达每英里 0.08dB(0.05dB/公里)的衰减。部署远程桥接网络时，通常建议系统采用 20dB 的系统操作容限(SOM)以补偿因雨、雾或雪带来的衰减。

- 空气分层

在高空中，空气温度的变化被称为空气分层(air stratification)。空气温度变化会导致折射。长距离点对点链接的射频信号的弯曲可能导致信号失调和性能问题。可能需要计算 K 因子以弥补长途链路上的折射衰减。

- 紫外线/太阳

如果错误使用电缆类型，长时间的紫外线和来自屋顶的热量也可能损坏电缆。

12.7　小结

本章讨论了许多 802.11 无线覆盖需要注意的事项。很多时候正确的网络设计和全面的现场勘察就可以解决无线覆盖、容量和性能的问题。我们讨论了很多第 2 层重传的原因及其对无线局域网的负面影响。因为无线网络是不断变化的环境，如漫游、隐藏节点和干扰问题必定会出现。

在对第 2 层和第 1 层问题进行故障排除时，协议分析仪、频谱分析仪是重要工具。我们讨论并比较了多信道体系结构和单信道体系结构之间的差异。我们还讨论了可能影响覆盖范围和吞吐量的多项性能变量。我们讨论了部署语音和数据 WLAN 的挑战。最后，我们讨论了影响户外射频通信的因素及防止天气条件侵害的步骤。

12.8　考试要点

- 解释第 2 层重传的影响和原因

了解第 2 层重传可能由多径、隐藏节点、功率设置不匹配、射频干扰、低信噪比、近/远问题及邻频干扰引起。第 2 层重传可以影响吞吐量、产生延迟和抖动。

- 定义动态速率切换

了解无线节点之间数据传输率切换的过程。动态速率切换也称为动态速率转移、自适应速率选择和自动速率选择。解释通常为什么推荐关闭两个较低的 802.11b/g 数据速率。

- 解释漫游

据了解漫游的特有性质。客户端决定开启漫游进程的变量不同。理解覆盖蜂窝适当重叠的重要性。描述可能出现的漫游延迟问题。了解为什么跨越第三层边界可能导致出现问题及解决方案。

- 定义邻频干扰和同频干扰的差异

了解邻频干扰与同频干扰的负面影响。解释为什么信道复用模式可以最大限度地减少问题发生。在 2.4GHz 和 5GHz 多信道结构中如何设计信道复用模式。

- MCA 和 SCA 的无线局域网设计之间的差别

理解 MCA 使用蜂窝大小调整来满足容量需求，而 SCA 使用信道堆栈来满足容量需求。解释虚拟 BSSID 和其他方面的 SCA 设计。

- 各种类型的无线干扰

知道全波段、窄带、宽带、物理干扰、符号间干扰等干扰类型。频谱分析仪是最佳的干扰故障排除工具。

- 解释隐藏节点问题

找出所有可能产生隐藏节点问题的原因。解释如何确定隐藏节点故障以及如何修复隐藏节点问题。

- 定义近/远问题

解释什么原因导致发生近/远问题及如何纠正。

- 影响 RF 性能的因素

解释影响基本服务集内 RF 覆盖和吞吐量的所有因素。

- 了解天气的影响

解释在水、风，闪电和空气分层等天气条件下可能引起的问题。解释了解决这些问题的可能方法。

12.9 复习题

复习题的答案见附录 A。

1. What type of solution must be deployed to provide continuous connectivity when a client station roams across layer 3 boundaries? (Choose all that apply.)

A. Nomadic roaming solution

B. Proprietary layer 3 roaming solution

C. Seamless roaming solution

D. Mobile IP solution

E. Fast secure roaming solution

2. If the access points transmit on the same frequency channel in an MCA architecture, what type of interference is caused by overlapping coverage cells?

A. Intersymbol interference

B. Adjacent channel interference

C. All-band interference

D. Narrowband interference

E. Co-channel interference

3. What variables might affect range in an 802.11 WLAN? (Choose all that apply.)

A. Transmission power

B. CSMA/CA

C. Encryption

D. Antenna gain

E. Physical environment

4. What can be done to fix the hidden node problem? (Choose all that apply.)

A. Increase the power on the access point.

B. Move the hidden node station.

C. Increase power on all client stations.

D. Remove the obstacle.

E. Decrease power on the hidden node station.

5. Layer 2 retransmissions occur when frames become corrupted. What are some of the causes of layer 2 retries? (Choose all that apply.)

A. Multipath

B. Low SNR

C. Co-channel interference

D. RF interference

E. Adjacent channel interference

6. What scenarios might result in a hidden node problem? (Choose all that apply.)

A. Distributed antenna system

B. Too large coverage cell

C. Too small coverage cell

D. Physical obstruction

E. Co-channel interference

7. What are some of the negative effects of layer 2 retransmissions? (Choose all that apply.)

A. Decreased range

B. Excessive MAC sublayer overhead

C. Decreased latency

D. Increased latency

E. Jitter

8. Several users are complaining that their VoWiFi phones keep losing connectivity. The WLAN administrator notices that the frame transmissions of the VoWiFi phones are corrupted when listened to with a protocol analyzer near the access point, but are not corrupted when listened to with the protocol analyzer near the VoWiFi phone. What is the most likely cause of this

problem?

A. RF interference

B. Multipath

C. Hidden node

D. Adjacent channel interference

E. Mismatched power settings

9. A single user is complaining that her VoWiFi phone has choppy audio. The WLAN administrator notices that the user's MAC address has a retry rate of 25 percent when observed with a protocol analyzer. However, all the other users have a retry rate of about 5 percent when also observed with the protocol analyzer. What is the most likely cause of this problem?

A. Near/far

B. Multipath

C. Co-channel interference

D. Hidden node

E. Low SNR

10. What type of interference is caused by overlapping cover cells with overlapping frequencies?

A. Intersymbol interference

B. Adjacent channel interference

C. All-band interference

D. Narrowband interference

E. Co-channel interference

11. Based on RSSI metrics, concentric zones of variable data rate coverage exist around an access point due to the upshifting and downshifting of client stations between data rates. What is the correct name of this process, according to the IEEE 802.11-2007 standard?

A. Dynamic rate shifting

B. Dynamic rate switching

C. Automatic rate selection

D. Adaptive rate selection

E. All of the above

12. Which of these weather conditions is a concern when deploying a long-distance point-topoint bridge link?

A. Wind

B. Rain

C. Fog

D. Changes in air temperature

E. All of the above

13. What variables might affect range in an 802.11 WLAN?

A. Wavelength

B. Free space path loss

C. Brick walls

D. Trees

E. All of the above

14. Given: Wi-Fi clients can roam seamlessly at layer 2 if all the APs are configured with the same SSID and same security settings. However, if clients cross layer 3 boundaries, a layer 3 roaming solution will be needed. Which device functions as the home agent if a Mobile IP solution has been implemented in an enterprise WLAN environment where no WLAN controller is deployed?

A. Wireless network management server (WNMS)

B. Access layer switch

C. Layer 3 switch

D. Access point on the original subnet

E. Access point on the new subnet

15. Which of the following can cause roaming problems? (Choose all that apply.)

A. Too little cell coverage overlap

B. Too much cell coverage overlap

C. Free space path loss

D. CSMA/CA

E. Hidden node

16. What are some problems that can occur when an access point is transmitting at full power? (Choose all that apply.)

A. Hidden node

B. Co-channel interference

C. Mismatched power between the AP and the clients

D. Intersymbol interference

17. Why would a WLAN network administrator consider disabling the two lowest rates on an 802.11b/g access point? (Choose all that apply.)

A. Medium contention

B. Adjacent channel interference

C. Hidden node

D. Intersymbol interference

E. All of the above

18. Which type of interference is caused by destructive multipath?

A. Intersymbol interference

B. All-band interference

C. Narrowband interference

D. Wideband interference

E. Physical interference

19. In a multiple-channel architecture (MCA) design, what is the greatest number of nonoverlapping channels that can be deployed in the 2.4 GHz ISM band?

A. 3

B. 12

C. 11

D. 14

E. 4

20. What factors should be taken into consideration when designing a channel reuse plan for 5 GHz access points? (Choose all that apply.)

A. Regulatory channels permitted

B. Number of VLANs permitted

C. Encryption

D. DFS support the clients

E. DFS support for the APs

第13章 无线局域网安全架构

在该章中，你将学习以下内容：

- √ 无线局域网安全基础
  - 数据保密
  - 认证、授权与统计(AAA)
  - 分段
  - 监控与安全策略
- √ 传统的无线局域网安全机制
  - 传统的认证方式
  - 静态 WEP 加密
  - MAC 地址过滤
  - SSID 隐藏
- √ 强健安全机制
  - 强健安全网络(RSN)
  - 认证与授权
  - PSK 认证
  - 私有 PSK 认证
  - 802.1X/EAP 架构
  - EAP 类型
  - 动态加密密钥的生成
  - 四次握手
  - WPA/WPA2-Personal 解决方案
  - TKIP 加密
  - CCMP 加密

- √ 流量分段
  - 虚拟局域网(VLAN)
  - 基于角色的访问控制(RBAC)
- √ 基础架构安全
  - 物理安全
  - 接口安全
- √ VPN 无线安全
  - 三层 VPN
  - SSL VPN
  - VPN 部署
  - 访客无线网络安全
  - 强制门户(Captive portal)

本章和下一章将介绍备受关注的 802.11 无线局域网安全问题。这一章将讨论传统的 802.11 安全解决方案，并介绍 802.11-2007 标准定义的更多的强健安全机制。WLAN 安全多年来备受诟病，其实确实如此。传统的 IEEE 定义的安全机制不能满足在移动环境中必需的用户认证和数据私密性要求。尽管没有任何措施能百分之百保证安全，但是采用合适的解决方案有助于增强无线网络抵御攻击的能力。

无线网络存在大量安全隐患，第 14 章将讨论各种针对无线局域网的攻击以及监控这些攻击的手段。

部署合适的安全架构可以抵御许多针对 802.11 网络的攻击，这一章将对此进行介绍。但是，现有的监控手段对相当一部分攻击无能为力。面对这些攻击，管理员可能束手无策。

CWNA 认证有十分之一左右的内容涉及无线局域网安全。CWNP 还开发了一项名为 CWSP(认证无线安全资深工程师)的认证，该认证考查与无线局域网安全有关的各种内容，要求考生对 802.11 安全架构有较深入的了解。第 13 章与第 14 章将对无线安全的基础知识做一介绍，掌握这些知识不仅对 CWNA 的备考大有裨益，也有助于读者正确部署无线安全解决方案。

13.1　无线局域网安全基础

802.11 无线安全解决方案通常涉及以下 5 方面重要内容：

- 数据保密
- 认证、授权与统计(AAA)
- 分段
- 监控
- 安全策略

由于射频信号传输的自由性与开放性，为保护数据安全，必须对信息进行加密。802.11 无线网络一般作为连接到其他有线基础架构(如 802.3 以太网骨干网)的入口使用。为保护这个入口的安全，必须采用合适的认证解决方案，以确保只有授权用户才能通过无线接入点访问网络资源。用户获得授权后，还需要采用 VLAN(Virtual LAN，虚拟局域网)与基于身份的机制以进一步限制用户可以访问的网络资源。条件允许的话，应考虑部署 WIDS(无线入侵检测系统)对 802.11 无线网络进行持续监控。一套完善的解决方案应将上述安全机制与企业的安全策略有机结合起来。

有线网络与无线网络的安全是企业始终需要考虑的问题。某些无线局域网仅部署了传统的安全解决方案，这些解决方案目前已经无法提供有效的保护。2004 年，IEEE 批准并公布了 802.11i 修正案(已被整合到 802.11-2007 标准中)，后者采用安全性更高的加密与认证方式。802.11i 修正案为无线局域网定义了 RSN(强健安全网络)，本章稍后将对此进行介绍。部署合适的加密与认证解决方案可以使无线网络的安全性得到极大增强，甚至与有线网络相比也毫

不逊色。掌握本章和下一章节讨论的 802.11 安全的五要素将为选择和实施 802.11 安全解决方案奠定坚实基础。

13.1.1 数据保密

802.11 无线网络使用无需牌照的频段传输数据，且所有信息都暴露在空中传输。保护有线网络的数据安全相对简单，因为普通人很难接近受到严密保护的有线介质。与之相反，任何人都可以接触到监听范围之内以无线方式传输的信息。有鉴于此，必须采用密码加密技术保护数据的安全。密码(cipher)是用于实施加密的一种算法。

RC4 算法(“RC”表示“Ron's code”或“Rivest cipher”)与 AES(Advanced Encryption Standard，高级加密标准)算法是两种最常见的加密算法。各种算法对信息的加密方式不同，信息可以被加密为连续的数据流，也可以被加密为区块。

RC4 算法是一种流加密算法(stream cipher)，经常用于加密 SSL(Secure Sockets Layer，安全套接层)等互联网流量。RC4 算法也可以加密 802.11 无线数据，WEP 与 TKIP 都以 RC4 算法为基础，本章稍后将对二者进行介绍。

AES 算法是一种分组加密算法(block cipher)，最初被称为 Rijndael 算法，其安全性优于 RC4 流加密。AES 算法也用于加密 802.11 无线数据，CCMP(计数器模式密码块链信息认证码协议)即以 AES 算法为基础，本章稍后将介绍这种加密机制。AES 算法将信息加密为固定长度的数据区块，可供选择的密钥长度为 128 位、192 位或 256 位。美国政府规定，敏感与机密信息必须采用 AES 算法进行加密。

第 9 章介绍了 3 种主要的 802.11 无线帧。由于管理帧的帧体中只包含无线局域网运行所需的二层信息，因此管理帧不被加密。控制帧不存在帧体，因此也不必加密。而数据帧的帧体中包含上层信息，这些信息的安全必须得到保护。请注意，所有 802.11 数据帧中的 MSDU(MAC Service Data Unit，MAC 服务数据单元)是在二层被加密。这一章讨论的大部分加密方式均属于二层加密，被加密的是数据帧中的 3～7 层信息。练习 13.1 使用 802.11 协议分析仪来查看 802.11 数据帧中的 MSDU 净荷部分。

练习 13.1

未加密数据帧与加密数据帧

(1) 在 http://www.sybex.com/go/cwna3e 下载 CWNA_CHAPTER9.PCAP 文件。

(2) 从 www.wireshark.org 下载数据包分析软件并安装。

(3) 用数据包分析软件打开 CWNA_CHAPTER9.PCAP 文件。大多数的数据包分析软件都在屏幕上半部分列出捕获的帧，各帧在第 1 列中按顺序编号。

(4) 查看#8 帧，它是一个未加密的简单数据帧。观察这个帧，并留意上层信息(如 IP 地址及 TCP 端口)。

(5) 查看#136 帧，它是一个加密的简单数据帧，观察这个帧，你会发现它采用了 WEP 加密，无法看到上层信息。

13.1.2　认证、授权与统计

AAA(authentication, authorization, and accounting，认证、授权与统计)是一种常见的计算机安全概念，它定义了保护网络资源的方式。

认证是验证用户身份与资格的过程。用户必须表明自己的身份并提供可以证实其身份的凭证(如用户名、密码或数字证书)。安全性较高的认证系统采用多要素认证，用户必须提供至少两种不同的身份凭证。

授权是给予用户访问网络资源与服务的权限。用户必须首先通过认证才能访问网络资源。

统计对用户使用网络资源的情况进行跟踪，它是网络安全的重要组成部分。统计将用户身份、访问资源的种类、时间以及地点记录在案。一般而言，许多行业规范(如 PCI)都要求系统保留详细的统计记录备查。

如前所述，802.11 无线网络一般作为连接到 802.3 有线网络的入口使用。为保护这个入口的安全，必须采用强有力的认证解决方案，以确保只有合法用户才能获得访问网络资源的权限。

13.1.3　分段

强有力的加密与 AAA 解决方案是保护企业无线网络最重要的手段，不过分段在无线安全中占有同等重要的地位。分段用于分离网络中的用户流量。早期的无线安全体系不堪一击，在 802.11i 修正案获批之前，相对于 802.3 有线网络而言，整个 802.11 无线网络都是不安全、不受信任的。

随着安全解决方案的发展，无线局域网与有线基础架构的集成变得越来越平滑和安全。与传统网络类似，将用户划分到相应的组中仍是一种重要的安全措施。在用户获得授权之后，系统还可以采用防火墙、路由器、VPN 和 VLAN 等多种手段进一步限制用户所能访问的网络资源。大部分企业无线局域网通过创建 VLAN 以实现三层分段。分段与 RBAC(基于角色的访问控制)通常密不可分，本章稍后将对此进行介绍。

13.1.4　监控与安全策略

虽然加密、AAA 以及分段等安全机制有助于保护数据和网络资源的安全，但是仍然需要一种专职的监控解决方案以检测针对无线局域网的攻击。第 14 章将讨论各种潜在的第一层与第二层攻击，并介绍 WIDS 监控这些攻击的方法。此外，第 14 章还将介绍无线安全策略

的基本构成，安全策略是 Wi-Fi 安全体系的基石。因风险评估级别的不同，并非所有组织都需要监控解决方案，但是如果预算允许的话，高度推荐。

13.2 传统的无线局域网安全机制

802.11 原始标准仅定义了最基本的安全机制，这些机制并不能为 Wi-Fi 网络提供有效的保护。原始标准定义的认证方式其作用相当有限，入侵者很容易就能接入有线网络基础架构。原始标准定义的加密方式早已被破解，它无法承担起保护数据安全的责任。下面将介绍这些传统的安全机制。在 1997 年到 2004 年之间，它们是无线局域网仅有的安全手段。802.11i 修正案目前已经被整合到 802.11-2007 标准中，稍后将讨论该修正案定义的强健安全机制。

13.2.1 传统的认证方式

第 9 章曾经介绍过传统的认证方式。802.11 原始标准定义了两种认证机制，它们是开放系统认证(Open System authentication)与共享密钥认证(Shared Key authentication)。一提到认证，大家都会想到在接入或登录网络时进行用户身份认证，但 802.11 认证很不相同。传统的认证方法并不太关注用户的身份，而看起来更像是对接入能力的认证。可以把这些传统的认证方法看成是对其是有效支持 802.11 设备的验证方法。

开放系统认证不对用户身份做任何验证，在整个认证过程中，通信双方仅需交换两个认证帧。客户端向接入点发送认证请求帧、接入点向客户端返回认证响应帧之后即完成认证。开放系统认证不要求用户提供任何身份凭证，客户端通过这种简单的认证后就能与接入点建立关联，进而获得访问网络资源的权限。在客户端与接入点相互认证并建立关联之后，也可以采用静态 WEP 密钥加密二者之间的数据帧传输，不过实施静态 WEP 加密并非开放系统认证的强制要求。

第 9 章曾经介绍过，共享密钥认证要求 802.11 设备必须支持 WEP 加密，且客户端与接入点必须配置匹配的静态 WEP 密钥。如果双方的静态 WEP 密钥不匹配，客户端也无法通过认证。共享密钥认证与开放系统认证类似，但是采用共享密钥认证的无线接口卡之间还需要交换质询(challenge)与响应消息。在整个认证过程中，通信双方一共需要交换 4 个认证帧。

(1) 客户端向接入点发送认证请求帧。

(2) 接入点向客户端返回包含明文质询消息的认证响应帧。

(3) 客户端使用静态 WEP 密钥将质询消息加密，并通过另一个认证请求帧发给接入点。

(4) 接入点使用静态 WEP 密钥将客户端的质询消息解密，并与原始质询消息进行比较。如果二者匹配，接入点将向客户端发送第四个也是最后一个认证帧，确认客户端成功通过认证。如果二者不匹配或接入点无法解密客户端的质询消息，接入点将拒绝客户端的认证请求。

客户端成功通过共享密钥认证后，采用同一静态 WEP 密钥加密随后的 802.11 数据帧传输。

开放系统认证与共享密钥认证

初看起来，共享密钥认证的安全性似乎比开放系统认证要高，但是前者实际上存在巨大的安全漏洞。如果入侵者截获接入点发送的明文质询消息以及客户端返回的加密质询消息，就可能从中提取出静态 WEP 密钥。入侵者一旦掌握静态 WEP 密钥，就可以解密所有数据帧，网络对入侵者将再无秘密可言。总之，这两种传统的认证方式都无法为企业无线局域网提供有效保护。稍后将介绍安全性较高的 802.1X/EAP 认证机制。

13.2.2　静态 WEP 加密

WEP(Wired Equivalent Privacy，有线等效加密)是一种以 RC4 流加密为基础的二层加密机制，802.11 原始标准先定义了 64 位 WEP 版本，之后不久又定义了 128 位两种版本的 WEP。WEP 加密的 3 个主要预期目标是机密性、访问控制以及数据完整性。

机密性指在数据传输之前对其进行加密，以保护信息安全。

访问控制本质上相当于授权，客户端只有配置与接入点相同的静态 WEP 密钥才能获得访问网络资源的权限。

数据完整性是值发送方在加密数据之前将计算 ICV(Integrity Check Value，完整性校验值)，以防止信息在传输过程中遭到篡改。

尽管 802.11 原始标准定义了两种 WEP，不过美国政府最初只允许向其他国家出口 64 位 WEP 技术。在美国政府放宽对密钥长度的出口限制之后，无线接口卡厂商开始生产支持 128 位 WEP 加密的设备。如图 13-1 所示，64 位 WEP 由 40 位静态密钥与 24 位 IV(Initialization Vector，初始化向量)构成。IV 由无线接口卡的驱动程序产生，它以明文形式发送，每一帧的 IV 都不相同。需要注意的是，由于一共只存在 2^{24}(16 777 216)个不同的 IV，因此所有 IV 值在一段时间后必定会重复。40 位静态密钥与 24 位 IV 混合后的有效密钥长度为 64 位，104 位静态密钥与 24 位 IV 混合后的有效密钥长度为 128 位。

图 13-1　静态 WEP 加密密钥与初始化向量 IV

管理员通常使用十六进制字符(0～9 与 A～F)或 ASCII 码输入静态密钥。请注意，接入点与客户端配置的静态密钥必须匹配。40 位静态密钥由 10 个十六进制字符或 5 个 ASCII 码构成，104 位静态密钥由 26 个十六进制字符或 13 个 ASCII 码构成。不过，客户端或接入点

不一定能同时支持两种编码系统。如图 13-2 所示，管理员可以为大部分客户端与接入点配置最多 4 把独立的静态密钥，并选择其中一把作为默认的传输密钥。传输密钥属于静态密钥，发方无线接口使用传输密钥加密数据。客户端或接入点可使用一把密钥加密发送流量，并使用另一把密钥解密接收流量。但是通信双方所用的密钥必须严格匹配，以便正确地加密和解密数据。

图 13-2 传输密钥

可以将 WEP 的工作原理简述如下：系统对需要加密的明文数据进行循环冗余校验(CRC)，然后将校验结果(ICV)添加到数据末尾。系统生成一个 24 位 IV，并与静态密钥进行混合。二者作为密钥材料(seeding material)，通过伪随机算法生成一系列称为密钥流(keystream)的随机比特，密钥流在长度上与需要加密的明文数据相等。密钥流与明文数据比特进行异或运算，输出即为 WEP 密文，也就是经过加密的数据。最后，明文 IV 被添加到加密数据的头部，完成整个加密过程。图 13-3 显示了这一过程。

图 13-3 WEP 加密过程

如前所述，WEP 存在大量已知的安全漏洞，下面列出了 4 种会对 WEP 造成极大危害的攻击：

IV 碰撞攻击(IV Collisions) 由于 24 位 IV 以明文形式传输且每一帧的 IV 都不相同，对一个流量很大的 WEP 加密网络而言，全部 2^{24} 个 IV 在一段时间后必定会重复。有限的 IV 空

间将导致 IV 值碰撞，从而方便入侵者破解加密密钥。

弱密钥攻击(Weak Key)　RC4 算法会生成一部分弱 IV 密钥，如果入侵者获得这些弱密钥，就能更容易地破解加密密钥。

再注入攻击(Reinjection)　对于流量相对较少的网络，入侵者可使用黑客工具实施数据包再注入攻击，以加快收集弱 IV 密钥。

比特翻转攻击(Bit-Flipping)　WEP 采用 ICV 以实现数据完整性校验，但是 ICV 的安全性较差，这可能导致 WEP 加密数据包被篡改。

目前的 WEP 破解工具混合使用上述前 3 种攻击手段作为破解手段，可在 5 分钟之内破解 WEP 密钥。入侵者在取得静态 WEP 密钥后，就能解密所有数据帧。本章稍后将介绍 TKIP 与 CCMP。TKIP 是对 WEP 的完善和改进，而 CCMP 采用 AES 算法，其安全性更高。802.11 原始标准将 WEP 定义为一种可选的加密方式。WEP 早已被破解，它无法为企业无线局域网提供有效的保护，但部署 WEP 加密总好过网络完全不设防。

13.2.3　MAC 地址过滤

每块网卡都有一个称为 MAC 地址的物理地址，它由 12 个十六进制数构成。前面曾经介绍过，所有 802.11 客户端的 MAC 地址都是唯一的，接入点根据 MAC 地址转发流量。大部分厂商的接入点都具备配置 MAC 地址过滤的功能，即允许或阻止来自特定 MAC 地址的流量。

一般而言，MAC 地址过滤仅允许特定客户端的流量通过，这种过滤基于客户端唯一的 MAC 地址。如果一个客户端的 MAC 地址没有出现在允许列表中，接入点将禁止该客户端的流量通过其虚端口进入分布系统介质。然而，MAC 地址可能被欺骗(spoofing)或伪造。只要将 MAC 地址伪装成某个出现在允许列表中的客户端的 MAC 地址，就能轻易绕过 MAC 地址过滤，这点连业余黑客也不难做到。为所有设备配置 MAC 地址过滤的工作量较大，而 MAC 地址又易于伪造，这使得 MAC 地址过滤无法成为一种可靠的企业无线安全解决方案。802.11 标准没有定义 MAC 地址过滤，所有实现都是厂商专有的。

MAC 地址过滤常用于保护传统的无线接口，这些无线接口不支持更强健的加密方式。例如，老式的手持条码扫描仪无线接口可能仅支持静态 WEP 加密，这种情况下不妨考虑部署 MAC 地址过滤。不过为更好地保护无线网络的安全，建议根据厂商的 OUI 地址(MAC 地址的前 3 个字节，不同厂商的 OUI 地址可能有所不同)将手持设备划分到独立的 VLAN 中。

13.2.4　SSID 隐藏

还记得《星际迷航》中罗米兰人的太空船在“隐身”后仍然被柯克船长发现吗？其实，也可以设法让 SSID(服务集标识符)“隐身”。大部分接入点都具备封闭网络(Closed Network)或广播 SSID(Broadcast SSID)的能力，启用封闭网络或禁用广播 SSID 可将无线网络的逻辑名隐藏起来。

启用封闭网络后，信标帧中的 SSID 字段被置为空，采用被动扫描监听信标帧的客户端

将无法获得 SSID 的信息。SSID 经常被称为 ESSID(扩展服务集标识符)，它是无线局域网的逻辑标识符。SSID 隐藏旨在阻止没有配置相应 SSID 的客户端与无线局域网建立关联。

采用主动扫描搜索接入点时，无线客户端将向外发送 SSID 字段为空的探询请求帧。用户还可以使用许多流行且免费的 WLAN 扫描软件(如 inSSIDer、NetStumbler 和 iStumbler)搜索周围可用的无线网络。这些软件采用主动方式扫描接入点，并向外发送空探询请求帧。不同的 WLAN 厂商在启用 SSID 隐藏后的工作方式有所不同。有些厂商的 AP 再启用了 SSID 隐藏在收到空探询请求帧之后，将返回一个 SSID 字段同样为空的探询响应帧，也就是说，无线网络将在一段时间内被“隐藏”起来。不过，启用封闭网络的接入点仍然会对发送定向探询请求帧(包含特定的 SSID)的客户端做出响应。这可以保证合法的终端用户通过认证并与接入点建立关联，而没有正确配置 SSID 的客户端则无法连接到接入点。

虽然启用 SSID 隐藏的确能阻止 WLAN 发现工具扫描到用户网络的 SSID，但是从另一方面讲，只要入侵者使用二层无线协议分析软件拦截到任何合法终端用户发送的无线帧，就能获得以明文形式传输的 SSID。也就是说，采用合适的工具在几秒钟之内就可以发现隐藏的 SSID。许多无线专家认为 SSID 隐藏所起的作用十分有限，不过也有工程师表示，启用 SSID 隐藏有助于提高网络的安全系数。

尽管 SSID 隐藏可以在一定程度上防止业余黑客(“脚本小子”)与普通用户搜索到无线网络，不过应该清楚地认识到，SSID 隐藏绝非一种完备的无线安全解决方案。802.11 标准没有定义 SSID 隐藏，所有实现封闭网络的方式都是厂商专有的。也就是说，传统的无线网卡之间以及不同厂商的无线网卡之间可能互不兼容，从而导致连接性出现问题。有鉴于此，启用封闭网络之前请务必了解所用设备的特性。此外，实施 SSID 隐藏还可能带来管理与技术支持方面的问题。终端用户为无线网卡配置 SSID 时，经常会因为配置不当而不得不寻求客服人员的帮助。

真实场景

SSID 隐藏

隐藏 SSID 适用的一个场景是某组织需要支持大量的访客接入，例如医院。医院无线网络可能存在多个 SSID(如员工、语音和访客)。为减少因访客连错网络的问题，医院通常会隐藏员工和语音的 SSID，同时广播访客 SSID，此时访客尝试连接无线网络时只能看到访客 SSID，就减少了偶尔连到其他两个网络的情况。

在隐藏公司 SSID 前，重要是要控制客户端的规模，以免因为兼容性问题导致大量连接故障。

13.3 强健安全机制

IEEE 于 2004 年批准并公布了 802.11i 修正案，后者目前已经被整合到 802.11-2007 标准

中。802.11-2007 标准定义 802.1X/EAP 作为企业无线局域网的认证方式，定义预共享密钥(preshared key，PSK)或密码短语(passphrase)作为 SOHO 无线局域网的认证方式，但后者也可以在企业网中部署。此外，标准还定义了两种安全性更高的动态加密密钥生成方式，其中 CCMP/AES 属于默认加密方式，TKIP/RC4 属于可选加密方式。

早在 IEEE 批准 802.11i 修正案之前，Wi-Fi 联盟就开发了一种称为 WPA(Wi-Fi Protected Access，Wi-Fi 保护接入)的认证项目。WPA 属于 802.11i 修正案获批之前的过渡性方案，仅支持 TKIP/RC4 动态加密。WPA-Enterprise 用于企业环境，采用 802.1X/EAP 作为认证方式；WPA-Personal 用于 SOHO 环境，采用密码短语作为认证方式。

在 802.11i 修正案获批之后，Wi-Fi 联盟又开发了 WPA2(Wi-Fi 保护接入第 2 版)认证项目。WPA2 在功能上与 802.11i 修正案完全相同，支持 CCMP/AES 与 TKIP/RC4 两种动态加密机制。WPA2-Enterprise 用于企业环境，采用 802.1X/EAP 作为认证方式；WPA2-Personal 用于 SOHO 环境，采用密码短语作为认证方式。在 2005 年之后制造的 802.11 无线设备大多符合 WPA2 的要求。如果符合 WPA 要求，则可能仅支持 TKIP/RC4 加密。如果无线设备符合 WPA2 要求，则支持更强大的 CCMP/AES 动态加密。表 13-1 比较并总结了 IEEE 制定的安全标准与 Wi-Fi 联盟开发的认证项目。

表 13-1　安全标准与认证

802.11 标准	Wi-Fi 联盟认证项目	认证方式	加密方式	算法	密钥生成
802.11 传统		开放系统认证 共享密钥认证	WEP	RC4	静态
	WPA-Personal	WPA 密码短语(也称为 WPA PSK 和 WPA 预共享密钥)	TKIP	RC4	动态
	WPA-Enterprise	802.1X/EAP	TKIP	RC4	动态
802.11-2007 (RSN)	WPA2-Personal	WPA2 密码短语(也称为 WPA2 PSK 和 WPA2 预共享密钥)	CCMP(强制) TKIP(可选)	AES(强制) RC4(可选)	动态
802.11-2007(RSN)	WPA2-Enterprise	802.1X/EAP	CCMP(强制) TKIP(可选)	AES(强制) RC4(可选)	动态

13.3.1　强健安全网络

802.11-2007 标准定义了 RSN(Robust Security Network，强健安全网络)与 RSNA(robust security network association，强健安全网络关联)。两台终端必须通过四次握手(4-Way Handshake)过程相互认证、建立关联并创建动态加密密钥，二者之间的这种关联称为 RSNA。也就是说，每对无线接口使用的动态加密密钥都是唯一的。RSN 采用 CCMP/AES 作为强制加密方式，采用 TKIP/RC4 作为可选加密方式。

RSN 是仅允许创建 RSNA 的一种网络，它由信标帧、探询响应帧、关联请求帧以及重关

联请求帧中的 RSNIE(RSN Information Element，RSN 信息元素)字段加以标识。RSNIE 字段还声明了 802.11 设备使用的密码。除 RSNA 之外，802.11-2007 标准还定义了 pre-RSNA。换句话说，BSS(基本服务集)同时支持传统的安全机制与强健安全机制。如果 RSN 安全机制与传统安全机制(如 WEP)可在同一个 BSS 中共存，则称这种网络为 TSN(transition security network，过渡安全网络)。

13.3.2 认证与授权

如前所述，认证是验证用户身份与凭据的过程，用户必须表明自己的身份并提供可以证实其身份的凭证(如用户名、密码或数字证书)。授权是给予用户访问网络资源与服务的权限，用户只有首先通过认证才能访问网络资源。

接下来，我们将详细介绍更多的高级认证和授权。读者还将了解到，动态加密密钥也可能是这些更强认证解决方案的副产品。

13.3.3 PSK 认证

802.11-2007 标准定义了身份验证和密钥管理(AKM)服务。AKM 服务要求身份验证过程和加密密钥的生成和管理过程。身份验证和密钥管理协议(AKMP)可以采用预共享 (PSK)认证或是在 802.1X 身份验证过程中使用 EAP 协议。802.1X EAP 协议需要 RADIUS 服务器，并要求高级技能配置和支持它。通常家庭无线上网用户不理解 802.1X/EAP，也无法在他们的客厅里安装一台 RADIUS 服务器。没有办法使用更强的企业 802.1X 认证解决方案，在 SOHO 环境中需要使用 PSK 认证。WPA/WPA2-Personal 就是 PSK 认证，而 WPA/WPA2- Enterprise 指的就是 802.1X / EAP 认证解决方案。

大多数 SOHO 无线网络使用 WPA/WPA2-Personal 机制。在 IEEE 802.11i 被批准之前，Wi-Fi 联盟推出 Wi-Fi 保护访问(WPA)认证，看起来就像尚未发布的“802.11i 修正案快照”，但 WPA 仅支持 TKIP/RC4 动态加密密钥。802.1X/EAP 认证要求在企业中使用。WPA-Personal 密码身份验证方法在 SOHO 环境中使用。

WPA-Personal 的预期目标是无需固定长度的密钥，不必限制输入指定的十六进制和 ASCII 码。WPA/WPA2-Personal 允许最终用户输入一个简单的 ASCII 字符字符串(称为密码短语)，任何 8 到 63 个字符长度。在后台，密码短语再映射成 PSK。因此，所有用户都知道这个单一的、私密的密码短语，以允许访问 WLAN，如图 13-4 所示。

2004 年 6 月，IEEE 802.11 TGi 工作组正式批准了 802.11i，其增加了对 CCMP/AES 加密的支持。Wi-Fi 联盟将以前的 WPA 修订为 WPA2，并纳入了 CCMP/AES 加密。因此，WPA 和 WPA2 的唯一实际区别就是加密算法。WPA-Personal 和 WPA2-Personal 都使用 PSK 认证方法，然而 WPA-Personal 使用 TKIP/RC4 加密，WPA2-Personal 使用 CCMP/AES 加密。WLAN 厂商针对 PSK 认证有许多叫法，例如 WPA/WPA2-Passphrase、WPA/WPA2-PSK 及 WPA/WPA2 预共享密钥。

图 13-4　PSK 认证的客户端配置

13.3.4　私有 PSK 认证

请记住，WPA/WPA2-personal 定义的简单的 PSK 认证方法是一种弱认证方法，很容易受到暴力字典的攻击。因为密码是静态的，PSK 认证也容易受到社会工程学攻击。

虽然密码短语和 PSK 认证本意是在 SOHO 环境中使用，但在现实中，WPA/WPA2-personal 也经常用于在企业中。例如，即使快速安全漫游(FSR)机制现在是可能实现的，但很多旧 VoWiFi 手机和其他手持设备还不支持 802.1X/EAP。所以这些设备能所使用的最强级别安全方案就是 PSK 认证。成本问题也可能推动小企业使用更简单的 WPA/WPA2-Personal 解决方案，而不是为了使用 802.1X / EAP 认证而去安装、配置和支持 RADIUS 服务器。

在企业中使用 PSK 认证的最大隐忧就是社会工程学。所有 WLAN 设备上的 PSK 都是相同的。如果最终用户不小心把 PSK 泄露给黑客，WLAN 的安全性将遭到破坏。如果某个雇员离开公司，为保证安全，所有设备就必须重新配置一个新的 256 位的 PSK。因为密码短语或 PSK 由大家共享，所以需要执行严格的政策，只有 WLAN 安全管理员知道 PSK。当然，创建另一个密码还需要手动配置每个设备。

有些 WLAN 厂商提出了一些具有创造性的使用 WPA/WPA2-personal 的解决方案，解决了 WLAN 使用单个密码短语的问题。在这些方案中，每个设备或用户将有自己独有的 PSK，每个用户都可以映射到一个独特的 WPA/WPA2-personal 密码短语。映射到用户名或客户端的独特的 PSK 数据库必须存储在 AP 或集中式无线局域网控制器上。这个映射过程可以是动态或静态创建的。如图 13-5 所示，authenticator 维护一个数据库，数据库为每个客户映射一个独特的 PSK。这个生成的 PSK 也有过期日期。基于时间的独特的 PSK 可还用于在访客 WLAN

环境中，作为更传统的用户名/密码认证方案的替代认证方法。

图 13-5 专有 PSK

目前，有两家 WLAN 供应商提供专有的 PSK 解决方案，他们为每个用户提供独特的 PSK。这两家公司分别是提供私有 PSK 的 Aerohive 公司和动态 PSK 的 Ruckus 公司。专有 PSK 解决方案提供的方法不必部署更复杂的 802.1X/ EAP 的解决方案。社会工程学和暴力字典攻击还是可能发生的，但如果采用较强的独特 PSK，将使这个过程及其困难。如果某个 PSK 遭到破解，管理员只需撤消这个 PSK 凭据，而不必重新配置所有接入点和最终用户设备。但某些 WLAN 客户端设备只有限支持 802.1X/EAP，这种情况下，比起采用标准 WPA/WPA2-personal，专有 PSK 解决方案是一个巨大进步，专有 PSK 解决方案中，用户凭证是独特的，而且不需要进行 802.1X/EAP 所需的复杂配置。尽管如此，仍然建议为使用专有的 PSK 认证的设备提供某种形式的 ACL 或防火墙策略。

13.3.5 802.1X/EAP 架构

IEEE 802.1X 标准并非一种专门的无线标准，它常被误称为 802.11x。802.1X 是基于端口的访问控制(port-based access control)标准，它定义了一种授权架构，允许或阻止流量通过端口访问网络资源。802.1X 架构既可以用于无线环境，也可以用于有线环境，它主要由以下 3 部分构成：

请求方(supplicant) 向系统要求认证以访问网络资源的主机。每个请求方具有唯一的身份凭证，并由认证服务器加以验证。

认证方(authenticator) 允许或拒绝流量通过其端口实体的设备。一般而言，在请求方的身份得到验证之前，认证方只允许认证流量通过，拒绝所有其他流量通过。认证方维护两个虚端口，它们是非受控端口(uncontrolled port)与受控端口(controlled port)。非受控端口允许 EAP 认证流量通过，受控端口拒绝所有其他流量通过，直到请求方通过认证。

认证服务器(authentication server，AS) 对请求方提供的身份凭证进行验证，并将认证结果通知认证方。除自身维护的用户数据库之外，认证服务器也可以使用外部用户数据库对用户身份进行认证。

在 802.3 以太网中，请求方为台式机，认证方为可管理的交换机，认证服务器一般为 RADIUS (Remote Authentication Dial-In User Service，远程认证拨号用户服务)服务器。如图 13-6 所示，在 802.11 无线局域网中，请求方为要求访问网络资源的无线客户端，认证服务

器一般为 RADIUS 服务器。对自治型接入点架构而言，认证方为自治型接入点；对 WLAN 控制器架构而言，认证方为控制器而非轻量型接入点。目录服务通常由 LDAP 服务器提供，RADIUS 服务器可以与其直接通信。请注意有些 WLAN 厂商的自治型 AP 或 WLAN 控制器可以作为 RADIUS 服务器直接进行 LDAP 查询，这样可以避免使用外置的 RADIUS 服务器。

图 13-6　802.1X 解决方案：自治型接入点架构与 WLAN 控制器架构

如图 13-7 所示，在 802.11 桥接网络中部署 802.1X/EAP 安全解决方案时，认证方为根桥，请求方为非根桥。

图 13-7　802.1X 解决方案：802.11 桥接

请求方、认证方与认证服务器相互协作，三者构成了 802.1X 架构，不过实际认证时还需要认证协议的配合。EAP(Extensible Authentication Protocol，可扩展认证协议)用于验证用户身份，它是一种灵活的二层认证协议，可在 PPP(Point-to-Point Protocol，点对点协议)中使用。请求方与认证服务器采用 EAP 相互通信，EAP 流量通过认证方的非受控虚端口在请求

方与认证服务器之间传输。在认证服务器确认请求方提供的身份凭证之后，它将向认证方返回一个请求方已经通过认证的消息。之后，认证方开启虚拟受控端口，允许所有其他流量通过。图 13-8 显示了 802.1X/EAP 帧交换的一般过程。

图 13-8 802.1X/EAP 认证过程

无线网络中部署 802.1X/EAP 解决方案的目的在于验证用户的身份，并给予客户端访问有线网络基础架构的权限。

13.3.6 EAP 类型

如前所述，EAP 是“可扩展认证协议”的缩写，这里的关键词是“可扩展”(extensible)。EAP 是一种非常灵活的二层协议，它包括许多种类。EAP 既可以是厂商专有的，也可以是基于标准的。前者如 LEAP(Lightweight Extensible Authentication Protocol，轻量可扩展认证协议)是思科专有的，后者如 PEAP(Protected Extensible Authentication Protocol，受保护的可扩展认证协议)是标准协议。有些 EAP 仅能提供单向认证，而有些可提供双向认证(mutual authentication)。在双向认证中，不仅认证服务器需要对请求方的身份进行验证，请求方也必须对认证服务器的身份进行验证，以防止自己提供的用户名和密码被非法或假冒的认证服务器窃取。大部分要求双向认证的 EAP 采用服务器证书对认证服务器的身份进行验证。

表 13-2 比较并总结了各种 EAP 的特点供读者参考。请注意，本书与 CWNA 考试不会涉及 EAP 的具体特性，而 CWSP 考试将重点考查考生对各种 EAP 工作机制的理解。

表 13-2　各种 EAP 的比较与总结

	EAP-MD5	EAP-LEAP	EAP-TLS	EAP-TTLS	PEAPv0 (EAP-MSCHAPv2)	PEAPv0 (EAP-TLS)	PEAPv1 (EAP-GT)	EAP-FAST
安全解决方案	RFC-2284	Cisco 专有技术	RFC-5216	RFC-5281	IETF 草案	IETF 草案	IETF 草案	RFC-4851
客户端数字证书	不支持	不支持	支持	可选	不支持	支持	可选	不支持
服务器端数字证书	不支持	不支持	支持	支持	支持	支持	支持	不支持
客户密码认证	支持	支持	不适用	支持	支持	不支持	支持	支持
客户端 PAC	不支持	不支持	不支持	不支持	不支持	不支持	不支持	支持
服务器端 PAC	不支持	不支持	不支持	不支持	不支持	不支持	不支持	支持
身份凭证安全性	弱	弱(与密码强度有关)	强	强	强	强	强	强(前提是阶段 0 安全)
加密密钥管理	不支持	支持	支持	支持	支持	支持	支持	支持
双向认证	不支持	有争议	支持	支持	支持	支持	支持	支持
隧道化认证	不支持	不支持	可行	支持	支持	支持	支持	支持
Wi-Fi 联盟是否支持	不支持	不支持	支持	支持	支持	不支持	支持	支持

13.3.7 生成动态加密密钥

虽然实施加密并非 802.1X/EAP 架构的强制要求，但是它对于保护信息的安全至关重要。本章前面曾介绍过，802.1X/EAP 架构旨在提供用户认证与授权，动态加密密钥在认证过程结束之后产生并分发给通信各方。换句话说，采用双向认证的 EAP 可以提供创建动态加密密钥所需的密钥材料。到目前为止，我们只介绍了静态 WEP 密钥。为所有设备配置静态密钥是一项耗费精力的工作，而且入侵者通过社会工程学攻击(social engineering attack)可以很容易获得多个用户共享的同一把静态密钥。而动态密钥的优点在于所有用户的动态密钥都不同，入侵者不可能通过社会工程学攻击取得动态密钥。

认证服务器与请求方通过在双向认证中交换 EAP 帧，并通过凭据的交换以掌握彼此的信息，并采用这些信息作为生成动态加密密钥所需的密钥材料。动态密钥用于加密二者之间传输的流量，它以每会话每用户(per session per user)为基础产生。也就是说，每次客户端进行认证时都会生成一个新密钥，且每个用户的密钥都是唯一和独立的。

动态 WEP 加密

在 2004 年之前，许多厂商部署了以动态 WEP 加密为基础的解决方案，以期提高 WEP 密钥的安全性。不过动态 WEP 加密并未被标准化，可将其视为 TKIP 与 CCMP 出现之前的过渡性方案。

动态 WEP 加密作为一种过渡性的加密密钥管理解决方案，之前在未通过 WPA 认证的设备上使用。动态 WEP 密钥的生成与分发属于 EAP 认证过程的副产品，不再需要使用静态密钥，也不必手工输入密钥，其安全性优于已被淘汰的静态 WEP 密钥，而且每个用户的动态 WEP 密钥都是独立的，即使某个用户的动态密钥被盗，入侵者也只能解密该用户的流量。但是，动态 WEP 密钥仍然可以被破解，破解后的动态密钥仍然会危害数据帧的安全。也就是说，动态 WEP 密钥并非绝对安全。

此外，不要混淆动态 WEP 密钥与同样通过动态方式生成的 TKIP 或 CCMP 密钥。WPA/WPA2 解决方案定义了 TKIP/RC4 与 CCMP/AES 动态加密密钥，二者的安全性更高，它们同样是 EAP 认证过程的副产品。

13.3.8 四次握手

如前所述，802.11-2007 标准定义了 RSN 与 RSNA。两台终端必须通过一个被称为“四次握手”的过程相互认证、建立关联并创建动态加密密钥。

RSNA 在创建动态加密密钥的过程中，一共会生成 5 个独立的密钥。本书不对整个密钥产生过程做全面剖析，仅对该过程做一概述。RSNA 过程将首先产生两个主密钥，它们是 GMK(Group Master Key，组主密钥)与 PMK(Pairwise Master Key，成对主密钥)，PMK 可以通过 802.1X/EAP 认证生成，也可以通过 PSK 认证生成。主密钥作为密钥材料，用于创建实际加密和解密数据所需的动态密钥。最终生成的加密密钥称为 PTK(Pairwise Transient Key，成对瞬时密钥)与 GTK(Group Temporal Key，组临时密钥)。PTK 用于加密和解密单播流量，GTK

用于加密和解密广播与多播流量。

通信双方在交换 4 个 EAP 帧(四次握手)之后将生成 PTK 与 GTK。请注意，在 802.1X/EAP 认证或 PSK 认证结束之后，都要通过四次握手过程以生成实际使用的动态密钥。也就是说，四次握手是创建 TKIP/RC4 或 CCMP/AES 动态密钥不可或缺的一步。此外，客户端无线接口在每次漫游时都要重新进行四次握手，以便产生新的、唯一的动态密钥。

动态加密密钥的产生过程最初定义在 802.11i 修正案中，目前的 CWNA 考试不涉及这方面的内容，而 CWSP 考试将对此做重点考查。Devin Akin 撰写的一个白皮书名为 802.11i Authentication and Key Management(AKM)，它讨论了无线安全中的先有鸡还是先有蛋的因果难定问题。本书作者推荐将该白皮书作为延伸阅读材料。

13.3.9　WPA/WPA2-Personal 解决方案

受资金和条件所限，家庭用户和小型企业通常难以购置 RADIUS 服务器，这意味着在 SOHO 环境中无法部署 802.1X/EAP 架构。WPA/WPA2-Enterprise 解决方案采用 802.1X/EAP 以实现双向认证，这需要认证服务器的支持。由于大部分人的家中都没有 RADIUS 服务器，为满足 SOHO 用户的需求，802.11-2007 标准还定义了一种简化的认证解决方案。该方案采用预共享密钥，用户需要为接入点以及所有准备连接到无线网络的客户端手动输入匹配的密码短语。密码短语通过某种算法被转换为 PMK，再通过四次握手过程生成最终使用的动态加密密钥。

这种简化的解决方案称为 WPA/WPA2-Personal，后者有时也称为 WPA/WPA2 Preshared Key 或 WPA/WPA2 PSK。虽然 WPA/WPA2-Personal 的安全性明显优于静态 WEP 加密与开放系统认证，但为所有设备配置密码短语并不是一项轻松工作。此外，WPA/WPA2-Personal 抵御社会工程学攻击和离线词典攻击的能力较差，第 14 章将对此进行介绍。有鉴于此，应尽量避免在企业环境中使用 WPA/WPA2-Personal。条件允许的话，应采用 WPA/WP2-Enterprise 作为保护无线网络安全的首选方式。

13.3.10　TKIP 加密

RSN 将 TKIP(Temporal Key Integrity Protocol，临时密钥完整性协议)定义为可选的加密方式。TKIP 同样采用 RC4 流加密，它解决了大量已知的 WEP 安全漏洞，可以将其视为对 WEP 的改进和增强。

TKIP 由 128 位临时密钥、48 位 IV、源 MAC 地址以及目标 MAC 地址通过复杂的每包密钥混合(per-packet key mixing)过程生成，这种密钥混合过程有助于降低 IV 碰撞攻击与弱密钥攻击造成的危害。为抵御针对 WEP 的再注入攻击，TKIP 引入了排序机制。此外，TKIP 采用 MIC(Message Integrity Check，消息完整性校验)作为数据完整性校验机制。MIC 的长度为 8 字节，它能有效降低比特翻转攻击(bit-flipping)造成的危害，人们有时也根据发音将其亲

切地称为“Michael”。所有 TKIP 加密密钥均以动态方式生成，它们是四次握手过程的最终产物。

实施 WEP 加密将为整个 802.11 数据帧增加 8 字节的额外开销。由于 TKIP 的 IV 较长(48 位)且采用 MIC，实施 TKIP 加密将为整个 802.11 数据帧增加 20 字节的额外开销。TKIP 同样采用 RC4 算法，它实际上属于 WEP 的增强版本。因此，大部分厂商都发布了 WPA 固件升级补丁，仅支持 WEP 加密的传统无线接口卡在进行固件升级之后就可以使用 TKIP 加密。

13.3.11 CCMP 加密

802.11i 修正案定义的默认加密方式称为 CCMP(Counter Mode with Cipher-Block Chaining Message Authentication Code Protocol，计数器模式密码块链信息认证码协议)，其以 AES 算法(Rijndael 算法)为基础。CCMP/AES 使用 128 位加密密钥，信息被加密为 128 位的定长区块。CCMP/AES 密钥同样包含一个 8 字节的 MIC，不过其安全性远优于 TKIP/RC4 使用的 MIC。此外，由于 AES 算法非常安全，因此不必再使用每包密钥混合。所有 CCMP 加密密钥均以动态方式生成，它们是四次握手过程的最终产物。

实施 CCMP/AES 加密将为整个 802.11 数据帧增加 16 字节的额外开销。AES 算法需要消耗大量处理器资源，传统的 802.11 设备不具备运行 AES 算法所需的处理能力，且无法通过固件升级以支持 WPA2。也就是说，早期设备通常需要进行硬件升级才能支持 AES，这使得 WPA 向 WPA2 的过渡过程在初期十分缓慢。

练习 13.2

802.1X/EAP 与四次握手过程

(1) 在 http://www.sybex.com/go/cwna3e 下载 CWNA_CHAPTER9.PCAP 文件。

(2) 从 www.wireshark.org 下载数据包分析软件并安装。

(3) 用数据包分析软件打开 CWNA_CHAPTER9.PCAP 文件。大多数的数据包分析软件都在屏幕上半部分列出捕获的帧，各帧在第 1 列中按顺序编号。

(4) 在主界面中观察 EAP 帧交换过程(第 209 号帧到第 246 号帧)。

(5) 在主界面中观察四次握手过程(第 247 号帧到第 254 号帧)。

真实场景

如何在企业局域网中部署认证与加密？

前面曾经介绍过，认证旨在验证用户的身份，加密旨在保护数据的安全。由于 TKIP 或 CCMP 动态密钥在 802.1X/EAP 或 PSK 认证结束之后生成，因此认证与加密实际上是互为依存、相辅相成的。如图 13-9 所示，在部署 WPA/WPA2-Enterprise 解决方案时，请求方与认证服务器必须支持相同的 EAP 协议，而请求方与认证方必须支持相同的动态加密机制。

图 13-9　示意图

为防止潜在的社会工程学攻击与离线词典攻击，一般情况下应避免在企业环境中采用 PSK 认证(WPA/WPA2-Personal)。但从另一方面讲，802.1X/EAP 认证会造成延时，而 PSK 认证则不存在这种问题。有鉴于此，为满足时敏应用对漫游切换时间的要求(不得超过 150ms)，大部分企业 VoWiFi 部署仍采用 PSK 认证作为安全解决方案。在快速、安全的漫游机制得到广泛应用之前，这种情况可能一直持续下去。此外，应尽可能采用 802.1X/EAP 认证(WPA/WPA2-Enterprise)作为企业无线局域网安全解决方案。

虽然 TKIP 加密目前尚未被破解，但是截至本书撰写时，人们已经发现了某些与完整性以及校验和有关的 TKIP 漏洞。而 CCMP 加密采用安全性极高的 AES 密码，应将其作为保护数据安全的首选方式。

13.4　流量分段

本章前面曾经介绍过，分段是网络设计的重要组成部分。在用户获得授权之后，系统还可以采用防火墙、路由器、VPN、VLAN 等多种手段进一步限制用户所能访问的网络资源。大部分企业无线局域网通过创建 VLAN 以实现三层分段。此外，分段与 RBAC 通常密不可分。

13.4.1　虚拟局域网

虚拟局域网(VLAN)用于创建独立的二层广播域并限制用户可以访问的网络资源，其划分一般与网络的物理拓扑结构无关。VLAN 广泛用于 802.3 交换网络的安全和用户划分。

在无线局域网环境中，每个 SSID 被映射到一个 VLAN。系统根据 SSID/VLAN 对划分用户，所有数据交换均通过接入点进行。此外，可为每个 SSID 配置独立的安全参数。大部分厂商的产品支持最多 16 个无线 VLAN，用户可被划分到多个独立的三层域中。如图 13-10 所示，一种常见的策略是在网络中创建访客、语音、数据等 3 个 VLAN。

访客 VLAN 不存在任何安全措施，所有访客 SSID 被路由到互联网网关，它们无法接触到网络资源。

语音 VLAN 采用中等强度的安全解决方案(如 WPA2-Passphrase)，VoWiFi 电话被路由到提供专有 QoS 服务的 VoIP 服务器。

数据 VLAN 采用高强度的安全解决方案(如 WPA2-Enterprise)，并通过 ACL(访问控制列表)过滤用户，通过认证的数据用户可以访问所有网络资源。

在 WLAN 控制器环境中，WLAN 控制器负责创建 VLAN 并配置 SSID 与安全参数，并将所有设置分发给轻量型接入点。在自治型或协作型接入点架构中，第三方交换机负责创建 VLAN，并将其映射到配置在自治型接入点上的 SSID 与安全参数。

SSID: 访客—VLAN 2— 安全 —Open System/No encryption
SSID: 语音—VLAN 3— 安全 —WPA-Personal
SSID:数据—VLAN 4— 安全 —WPA2-Enterprise

图 13-10 无线 VLAN

13.4.2 基于角色的访问控制

基于角色的访问控制(RBAC)是一种仅允许授权用户访问网络资源的机制，大部分 WLAN 控制器解决方案都具有 RBAC 功能。RBAC 主要由用户(user)、角色(role)与许可(permission)构成。

管理员可创建不同的角色(如销售角色或营销角色)，并将这些角色分配给个人或用户组。

许可被映射到角色，可以将其定义为二层许可(MAC 地址过滤)、三层许可(ACL)、4～7 层许可(状态防火墙规则)以及带宽许可。所有许可都可以配置时间条件。在通过认证之后，802.11 用户将继承任何已经分配给它们的角色及其许可。例如，关联到访客 SSID 的用户被划分到独立的访客 VLAN 中。在通过网络强制门户认证之后，用户将被分配一个访客角色。访客角色具有严格的带宽许可限制(如可用带宽只有 100kbps)，且系统在工作时段仅开放 80 端口(HTTP)、25 端口(SMTP)与 110 端口(POP)供访客用户使用，以避免访问互联网的访客用户占用过多带宽。在上午 9 时到下午 5 时之间，访客用户只能浏览网页与收发电子邮件。通过在无线局域网环境中部署 RBAC，管理员可以实现对无线用户的精确控制与管理。

13.5　基础架构安全

人们往往忽视无线基础架构设备的安全问题。除做好 Wi-Fi 硬件的防盗工作之外，务必确保只有经过授权的管理员才能接触到管理接口。在企业无线局域网中，保护硬件设备与接口的安全至关重要。

13.5.1　物理安全

接入点等 802.11 硬件设备非常昂贵，不少企业级接入点的售价高达 1000 美元。虽然接入点通常都安装在天花板或靠近天花板的位置，但是仍然不能忽视防盗工作。为避免接入点失窃，可以将其置于天花板或墙壁上的带锁机柜内。安全机柜不仅能阻止不法分子通过串行电缆或 Console 线连接到接入点，还能避免将接入点暴露给外界，从而满足某些行业对 802.11 设备安装的美观要求。

13.5.2　接口安全

管理员必须经由管理接口访问所有无线基础架构设备。一般而言，可通过命令行接口、Web 接口或 SNMP(简单网络管理协议)对企业无线局域网设备进行配置。为安全起见，应禁用所有不使用的接口。例如，如果管理员仅通过 CLI 配置接入点，则应关闭接入点的 Web 接口功能。即使不采取其他安全措施，也至少应更换所有配置选项的出厂默认密码。需要注意的是，某些管理接口支持多种默认的用户组(如管理员、高级用户与访客)，这些用户组的密码同样需要重新配置。

一般而言，无线基础架构设备应支持某种形式的加密管理功能。大部分 802.11 硬件目前都可以使用 SSH(安全外壳协议)、HTTPS(安全超文本传输协议)或 SNMPv3(简单网络管理协议第 3 版)，但是早期设备可能不支持加密登录。基于安全考虑，强烈建议仅通过网络的有线端配置 802.11 基础架构设备。如果采用无线方式配置设备，则无线数据包可能被入侵者拦截，从而影响网络的安全。此外，以无线方式配置 802.11 硬件设备还可能导致管理员无法访问设备。

13.6 VPN 无线安全

尽管 802.11-2007 标准已经明确定义了二层安全解决方案，不过管理员仍可以考虑为无线局域网部署上层 VPN(Virtual Private Network，虚拟专用网)解决方案。通常并不建议在企业环境中部署 VPN，这是因为 VPN 会增加开销，而且更为快速和安全的二层解决方案目前完全可以实现 VPN 的功能。但从另一方面讲，由于 VPN 解决方案已经在有线基础架构中得到了广泛应用，因此管理员往往也采用 VPN 保护无线局域网传输。VPN 在 Wi-Fi 安全中仍占有一席之地，它不仅在远程接入中扮演了重要角色，也经常在无线桥接环境中使用。VPN 拓扑结构主要分为两类：网关到网关(router-to-router)模式与客户/服务器(client/server)模式。

为保护远程接入时的通信安全，必须采用 VPN 技术。终端用户往往在公司之外的公共场所通过 Wi-Fi 热点传输数据，而大部分热点都不具备安全措施，因此用户需要自行部署 VPN 解决方案，以便为信息传输提供一条安全通道。在接入任何公共 802.11 网络时，用户都应实施 VPN 解决方案并配合个人防火墙，这对于保护数据的安全至关重要。

13.6.1 三层 VPN

VPN 可以提供加密、封装、认证、数据完整性等功能，它以安全隧道技术为基础，将一个 IP 数据包封装在另一个 IP 数据包中进行传输。VPN 技术将第一个数据包(原始数据包)封装在第二个数据包内，并将第一个数据包的目标 IP 地址、源 IP 地址以及数据净荷加密，从而达到保护原始数据包的目的。三层 VPN 采用三层加密机制，被加密的净荷是 4～7 层信息。为在隧道端点之间进行数据传输，第二个数据包的目标 IP 地址与源 IP 地址仍然为明文形式，它们分别指向 VPN 服务器以及 VPN 客户端的虚拟 IP 地址。

PPTP(Point-to-Point Tunneling Protocol，点对点隧道协议)与 IPSec(Internet Protocol Security，IP 安全协议)是两种主要的三层 VPN 技术。

PPTP 采用以 RC4 算法为基础的 128 位 MPPE(Microsoft Point-to-Point Encryption，微软点对点加密协议)作为加密方式，能提供一定程度的数据保护，不过其安全性仍然比较薄弱。PPTP 采用 MS-CHAPv2 作为用户认证方式，但 MS-CHAPv2 容易遭到离线词典攻击。有鉴于此，基于 PPTP 的 VPN 通常仅在小型 SOHO 环境中使用。

IPSec VPN 使用更强大的加密方法和更安全的认证方法，是最常部署的 VPN 解决方案。IPSec VPN 支持 DES、3DES、AES 等多种加密算法，并采用服务器端证书或预共享密钥以实现设备认证，其安全性较高。IPSec VPN 要求将客户端软件安装在连接到 VPN 服务器的远程设备上。大多数 IPSec VPN 都采用 NAT 穿越(NAT-transversal)，所以要求防火墙至少要对远程节点开放 UDP4500 和 UDP500 端口。本书并不打算深入讨论 IPSec 技术，读者只需了解 VPN 技术通常在企业环境中使用即可。

13.6.2 SSL VPN

在其他 OSI 模型层次上的 VPN 技术确实存在，例如 SSL 隧道。与 IPSec VPN 不同的是，SSL VPN 不需要在最终用户的计算机上安装和配置客户端软件。用户通过 Web 浏览器

连接到 SSL VPN 服务器，在 Web 浏览器和 SSL VPN 服务器之间的通信流量采用 SSL 协议或传输层安全(TLS)加密。TLS 和 SSL 在传输层以上加密数据，对隐私和密钥消息身份验证代码消息的可靠性进行非对称加密。

虽然大多数 IPSec VPN 解决方案采用 NAT 穿越技术，因为 NAT 或者防火墙策略受限，在远程仍然会选择 SSL VPN。

13.6.3　VPN 部署

VPN 通常在连接公共 WLAN 或者不提供安全的热点的客户端上使用。因为大多数热点不提供 L2 安全，在用户端的部署安全措施就显得尤为重要。VPN 可以为远程用户连接公共 WLAN 时提供必要程度的安全。如图 13-11，因为当远程站点的用户通过没有加密的公共 WLAN 接入时，需要 VPN 来提供数据的私密性。

图 13-11　通过公共热点建立 VPN

VPN 的另一个常见用途就是在远程分支与总部之间建立站到站的安全连接。多数 WLAN 厂商现在都可以在他们的 AP 或控制器内提供 VPN 功能，如图 13-12，分支 WLAN 控制器利用 VPN 将客户端流量封装到隧道并桥接到公司网络的有线端。有些 WLAN 厂商还能在 AP 间将用户流量进行隧道封装。

图 13-12　站到站 VPN

13.7　访客 WLAN 安全

大多数企业会向访客提供 Wi-Fi 服务。访客无线网络允许承包商、学生或销售人员访问互联网。许多企业都知道，需要使访客能够访问互联网，特别是电子邮件。通常做法就是企

业提供一个访客 SSID 和用户 VLAN，通常会使用防火墙限制访客用户功能及带宽。访客 WLAN 用户与公司 WLAN 用户的安全性不同。访客 WLAN 的主要安全目标是，为客人提供方便的互联网无线接入门户，同时限制其访问其他公司资源，访客 WLAN 安全要求通常包括以下内容：

- **访客 SSID** 多数企业的 AP 会广播 SSID，宣告一个不采用 WPA/WPA2 加密的开放网络，使访客很容易发现该网络。尽管通常不向访客提供加密，但有些 WLAN 厂商开始使用动态 PSK 提供安全的访客接入方案。
- **访客 VLAN** 访客流量通过特殊的 VLAN 与公司用户流量隔离。访客流量也经常被路由到 DMZ 区。
- **防火墙策略** 访客 WLAN 防火墙策略通常非常严格，通常只允许 DHCP 和 DNS 等服务，严格限制访问 10.0.0.0/8、192.168.0.0/16 及 172.16.0.0/12 等私有网段，之所以限制这些私有网段，主要是因为企业的网络服务器和网络资源通常就处于这些网段。访客防火墙策略通常把访客流量直接路由到互联网网关后再发送出去。
- **强制 Web 门户** 访客在接入互联网之前通常必须登录一个强制 Web 门户。强制门户解决方案实际上将 Web 浏览器转换成认证设备。为进行认证，用户必须启动 Web 浏览器，用户无论输入什么网址，都会被重定向到这个 Web 门户。强制门户可以基于 IP 重定向、DNS 重定向或 HTTP 重定向等方法将未经认证的用户重定向到登录页面。
- **访客管理解决方案** 大多数访客 WLAN 要求来宾通过强制 Web 门户输入认证凭据。因此需要创建用户凭据数据库。与事先已经存在的活动目录数据库不同，访客用户数据库是动态创建的。访客信息通常在用户到达某公司时被收集起来，然后由专人管理并创建访客用户数据库。IT 管理人员无暇创建和管理访客数据库，这个工作一般由前台接待人员负责。大多数 WLAN 厂商都提供访客管理系统(就是 RADIUS 服务器或其他类型的数据库服务器的简单管理账户)，系统管理员有权创建访客账户。

强制门户

大多数热点和访客网络都使用强制门户。强制门户就是防火墙与 Web 认证的结合体。尽管强制门户经常用于热点和无线访客网络，但这个技术与无线网络本身没有特殊关联。无论用户是通过有线还是无线方式连接到访客网络，其发出任何报文都会被中断，并且拒绝其访问网关，直到用户通过强制门户的认证。图 13-13 显示了一个强制门户(captive portal)的登录界面。

强制门户可以是一个独立的软件，但大多数 WLAN 厂商将这个功能集成到控制器或者 AP 内。如图 13-14 所示，WLAN 厂商支持自定义的强制门户界面，你可以在上面增加公司 logo、插入可接受的使用条款(AUP)或者配置登录需求。

强制门户认证一般需要用户输入用户名和密码信息。用户名和密码会被 RADIUS 数据库验证，如果信息正确，用户会被允许访问某些资源(如互联网)，但防火墙策略通常会阻止用户访问公司资源。

图 13-13　强制门户登录界面

图 13-14　自定义强制门户

并非所有强制门户页面都要求输入用户名和密码信息，有些厂商现在开始使用动态 PSK 作为用户凭据。访客管理解决方案利用这些独特的 PSK 作为凭据并用 WPA/WPA2 加密提供数据安全。

有些企业的访客无线网络不需要输入任何凭据，但仍然显示可接受的使用条款(AUP)，要求访客网络必须合法使用。强制门户也可以使用自注册的方式。

13.8　小结

本章介绍了涉及无线安全的五个方面的内容。强有力的加密解决方案用于保护数据帧，双向认证解决方案确保只有合法用户才能使用网络资源，而分段解决方案可以进一步限制用户所能访问的网络资源类型。为更好地保护无线局域网的安全，还应对无线网络实施持续监控并执行无线安全策略。

本章讨论了传统的 802.11 认证与加密机制及其缺陷，并介绍了 802.1X/EAP 认证解决方案与动态加密密钥的优点，还讨论了 802.11-2007 标准定义的安全机制以及相关的 WPA/WPA2 认证项目。802.11-2007 标准定义了一套完整的二层强健安全机制，其采用 802.1X/EAP 或预共享密钥作为认证方式，采用 CCMP/AES 或 TKIP/RC4 作为动态加密方式。本章最后讨论了保护基础架构与接口安全的重要性，并对无线局域网环境中使用的 VPN 技术做了介绍。

对管理员而言，了解准备部署的 802.11 无线设备的性能与不足十分重要。条件允许的话，应采用 802.1X/EAP 认证机制与 CCMP/AES 加密机制将设备划分到不同的 VLAN 中。手持设备、VoIP 电话、移动扫描仪、移动打印机等设备往往不支持高级的安全功能，进行网络设计时必须将这些因素考虑在内，以确保最具动态且安全的网络。

13.9　考试要点

定义 AAA 安全概念。解释认证、授权与统计之间的区别，理解它们在无线局域网安全中所起的作用。

解释数据保密与网络分段的作用。解释加密数据帧的原因，了解加密密钥之间的区别，理解采用 VLAN 与 RBAC 机制可以进一步限制用户所能访问的网络资源。

理解传统的 802.11 安全机制。识别并掌握开放系统认证与共享密钥认证的原理。理解 WEP 加密的工作方式及其安全漏洞。

解释 802.1X/EAP 架构。解释 802.1X 解决方案的构成与 EAP 认证协议。理解动态加密密钥属于双向认证的副产品。

理解 RSN 采用的安全机制。理解 802.11-2007 标准专门为 RSN 定义的加密与认证方式，并比较 WPA 与 WPA2 认证项目的区别。

理解 TKIP/RC4 与 CCMP/AES。解释两种动态加密机制的基本原理，理解 RSN 为何采用二者作为加密方式。

解释 VLAN 与 VPN。理解 VLAN 一般用于无线网络分段。了解 VPN 技术的基本知识以及它在无线局域网中所起的作用。

理解访客 WLAN 安全。能够解释访客无线接入部署的安全机制的目的，了解强制门户、防火墙限制和访客管理系统。

13.10 复习题

复习题的答案见附录 A。

1. What WLAN security mechanism requires that each WLAN user have unique authentication credentials?

   A. WPA-Personal

   B. 802.1X/EAP

   C. Open System

   D. WPA2-Personal

   E. WPA-PSK

2. Which wireless security standards and certifications call for the use of CCMP/AES encryption? (Choose all that apply.)

   A. WPA

   B. 802.11-2007

   C. 802.1X

   D. WPA2

   E. 802.11 legacy

3. 128-bit WEP encryption uses a user-provided static key of what size?

   A. 104 bytes

   B. 64 bits

   C. 124 bits

   D. 128 bits

   E. 104 bits

4. What three main components constitute an 802.1X/EAP framework? (Choose all that apply.)

A. Supplicant

B. Authorizer

C. Authentication server

D. Intentional radiator

E. Authenticator

5. The 802.11 legacy standard defines which wireless security solution?

A. Dynamic WEP

B. 802.1X/EAP

C. 64-bit static WEP

D. Temporal Key Integrity Protocol

E. CCMP/AES

6. Jimmy has been hired as a consultant to secure the Donahue Corporation's WLAN infrastructure. He has been asked to choose a solution that will both protect the company's equipment from theft and hopefully protect the access point's configuration interfaces from outside attackers. What recommendations would be appropriate? (Choose all that apply.)

A. Mounting all access points in lockable enclosure units

B. Using an IPsec VPN

C. Configuring all access points via Telnet

D. Configuring access points from the wired side using HTTPS or Secure Command Shell

E. Implementing 802.1X/EAP

7. Which security solutions may be used to segment a wireless LAN? (Choose all that apply.)

A. VLAN

B. WEP

C. RBAC

D. CCMP/AES

E. TKIP/RC4

8. What wireless security solutions are defined by Wi-Fi Protected Access? (Choose all that apply.)

A. Passphrase authentication

B. LEAP

C. TKIP/RC4

D. Dynamic WEP

E. CCMP/AES

9. Name the three main components of a role-based access control solution.

A. EAP

B. Roles

C. Encryption

D. Permissions

E. Users

10. What does 802.1X/EAP provide when implemented for WLAN security? (Choose all that apply.)

A. Access to network resources

B. Verification of access point credentials

C. Dynamic authentication

D. Dynamic encryption-key generation

E. Verification of user credentials

11. Which technologies use the RC4 cipher? (Choose all that apply.)

A. Static WEP

B. Dynamic WEP

C. CCMP

D. TKIP

E. MPPE

12. What must occur before dynamic TKIP/RC4 or CCMP/AES encryption keys are generated? (Choose all that apply.)

A. Shared Key authentication and 4-Way Handshake

B. 802.1X/EAP authentication and 4-Way Handshake

C. Static WEP and 4-Way Handshake

D. PSK authentication and 4-Way Handshake

13. For an 802.1X/EAP solution to work properly, which two components must both support the same type of EAP? (Choose all that apply.)

A. Supplicant

B. Authorizer

C. Authenticator

D. Authentication server

14. When using an 802.11 wireless controller solution, which device would be considered the authenticator?

A. Access point

B. RADIUS database

C. LDAP

D. WLAN controller

E. VLAN

15. Identify some aspects of the Temporal Key Integrity Protocol. (Choose all that apply.)

A. 128-bit temporal key

B. 24-bit initialization vector

C. Message integrity check

D. 48-bit IV

E. Diffe-Hellman Exchange

16. In a point-to-point bridge environment where 802.1X/EAP is used for bridge authentication, what device in the network acts as the 802.1X supplicant?

A. Nonroot bridge

B. Controller

C. Root bridge

D. RADIUS server

E. Layer 3 core switch

17. CCMP encryption uses which AES key size?

A. 192 bits

B. 64 bits

C. 256 bits

D. 128 bits

18. Identify the security solutions that are defined by WPA2. (Choose all that apply.)

A. 802.1X/EAP authentication

B. Dynamic WEP encryption

C. Optional CCMP/AES encryption

D. Passphrase authentication

E. DES encryption

19. The IEEE 802.11-2007 standard mandates encryption for robust security network associations and optional use of encryption.

A. WEP, AES

B. IPsec, AES

C. MPPE, TKIP

D. TKIP, WEP

E. CCMP, TKIP

20. Which layer 2 protocol is used for authentication in an 802.1X framework?

A. Extensible Authorization Protocol

B. Extended Authentication Protocol

C. Extensible Authentication Protocol

D. CHAP/PPP

E. Open System

第14章 无线攻击、入侵监控与安全策略

在该章中，你将学习以下内容：

- √ 无线攻击
  - 非法无线设备
  - 对等攻击
  - 窃听
  - 加密破解
  - 认证攻击
  - MAC 地址欺骗
  - 管理接口漏洞
  - 无线劫持
  - 拒绝服务攻击
  - 厂商漏洞攻击
  - 社会工程学
- √ 入侵监控
  - 无线入侵检测系统(WIDS)
  - 无线入侵防御系统(WIPS)
  - 移动 WIDS
  - 频谱分析仪
- √ 无线安全策略
  - 一般性安全策略
  - 功能性安全策略
  - 信息安全法规
  - PCI 合规
  - 无线局域网安全策略建议

第 13 章介绍了传统的 802.11 安全解决方案以及 802.11-2007 标准定义的强度更高的安全机制。本章将讨论针对 802.11 无线网络的各种攻击。采用强有力的加密与双向认证解决方案能减轻某些攻击造成的危害，但是对另外一些攻击而言，现有手段只能发现而无法阻止它们。这一章将讨论可以检测到一层与二层攻击的无线入侵检测系统。正确规划与贯彻企业安全策略对于保护无线网络的安全极为重要，本章将介绍无线安全策略的基本构成，安全策略是 Wi-Fi 安全体系的基础。

14.1 无线攻击

本书前面的章节曾经介绍过，802.11 无线局域网主要作为接入有线网络基础架构的入口。必须采用强有力的认证机制保护这个入口的安全，确保只有合法用户才能访问网络资源。如果不采取合理的保护措施，未授权用户将通过 802.11 入口访问网络资源，这会造成难以预料的后果。入侵者可能接触到金融数据库、企业商业秘密或个人医疗信息，还可能破坏网络资源。

如果入侵者使用无线网络作为跳板中断或关闭 SQL 服务器或电子邮件服务器，企业将为此付出高昂的代价。任何怀有不良动机的个人都可以通过不设防的 802.11 入口上传病毒、木马、击键监控程序或远程控制软件，这会严重危害有线网络的安全。不设防的无线网关也为垃圾邮件、盗版软件、远程入侵等非法行为大开方便之门。

在有线网络资源遭到入侵者攻击的同时，无线网络资源的安全也会受到威胁。任何在空中传输的信息都可能被截获和破解，入侵者还可能接入不受保护的 Wi-Fi 设备的管理接口。许多无线用户没有采取任何保护措施，将自己完全暴露给对等攻击。此外，针对无线网络的拒绝服务攻击始终存在。不法分子可以利用合适的工具在一段时间内瘫痪 Wi-Fi 网络，从而阻止合法用户访问网络资源。

下面将介绍所有可能危害 802.11 无线网络安全的攻击。

14.1.1 非法无线设备

Wi-Fi 安全领域一个非常新潮的词语是非法接入点(rogue access point)，其实就是在公司希望保护的有线网络上开了一个开放的不受保护的入口，如图 14-1。第 13 章曾经介绍过，可采用 802.1X/EAP 认证解决方案拒绝未经授权的访问。但是，如何阻止个人安装与骨干网络相连的无线入口设备呢？可将非法接入点定义为任何连接到有线基础架构但不在网络管理员监控之下的 Wi-Fi 设备。如果将价格只有 50 美元的 SOHO 无线接入点或路由器插入一个活动的数据端口，它就成为一个接入有线网络基础架构的入口。由于非法设备没有采用授权、认证等安全措施，任何攻击者都可以通过这个开放的入口入侵网络资源。

在部署无线网络之后，企业可能会忽视无线网络的存在，这种情况屡见不鲜。大部分情况下，安装非法接入点的并不是黑客，而是企业员工，他们没有意识到这样做的后果。统计

数据显示，使用 Wi-Fi 网络已经变成了当下的流行趋势，人们早已习惯 Wi-Fi 带来的便捷和移动性。因此，员工往往会在工作场所自行安装无线设备，以弥补企业尚未部署无线网络带来的不便。尽管这些自行安装的接入点可能会提供员工所需的无线接入，然而它们几乎是完全开放的。每个非法接入点都是一个潜在的安全漏洞，都可能危害到企业极力保护的有线基础架构。其实，一个不设防的无线入口就足以将网络资源暴露给入侵者，而许多大公司实际上发现了大量由员工自行安装的非法接入点。

图 14-1　非法接入点

Ad hoc 网络也可能被攻击者用作入侵企业网的跳板。员工经常通过笔记本电脑或台式机中的以太网卡与有线网络相连，并通过 Wi-Fi 无线接口与其他员工建立 ad hoc 连接。这种连接可能是员工有意为之，也可能是因为对厂商的默认配置不太了解。如图 14-2，由于以太网连接与 Wi-Fi 无线接口可以相互桥接在一起，入侵者不难通过 ad hoc 无线网络路由到以太网连接，从而进入有线网络。

正因为如此，许多政府机构和企业都禁止员工使用 ad hoc 网络。可以在大部分企业客户设备上禁用 ad hoc 网络。

图 14-2 桥接的 Ad Hoc 无线网络

如前所述，多数非法接入点都是员工自行安装的，他们并没有意识到攻击者可以利用这些开放的入口入侵网络资源。此外，除非从物理上加以隔绝，否则无法阻止入侵者使用以太网电缆将非法接入点连接到墙壁上的活动数据端口。稍后将讨论可以检测并阻止非法接入点与 ad hoc 客户设备的入侵防御系统。

如果无线网络部署了 802.1X 解决方案，也可以将其用于保护有线网络中的网络端口。有些 WLAN 厂商已经开始利用 MACsec 进行有线端的端口控制。802.11AE，也就是 MACsec，利用一系列协议来保护数据传输安全。此时，任何接入点在访问有线网络之前都必须通过认证。这不仅能充分利用现有资源，还能防止非法接入点危害有线网络的安全。

大多数企业不使用 802.1 X/EAP 解决方案进行有线端口控制。因此，需要部署无线入侵检测系统(WIDS)，也被称为 WLAN 监控解决方案，来检测潜在非法设备。大多数 WIDS 厂商更愿意把自己的产品称为无线入侵预防系统(WIPS)，原因是这些产品能够减缓来自非法 AP 和非法客户端的攻击。

14.1.2 对等攻击

如前所述，无线网络资源的安全也可能受到威胁。人们往往忽视对等攻击(peer-to-peer attack)造成的危害。前面的章节曾经介绍过，可将 802.11 客户端配置为基础架构模式(Infrastructure mode)或点对点模式(Ad Hoc mode)。采用点对点模式的无线网络称为 IBSS(独立基本服务集)。IBSS 中不存在接入点，所有通信都是对等进行的。由于 IBSS 本质上属于对等连接，因此两个无线相连的客户设备可以共享彼此的资源。ad hoc 网络通常用于用户之间

以无线方式共享文件，但是这种共享可能在无意间将文件或其他资源暴露给攻击者。为减轻对等攻击造成的危害，一般应安装个人防火墙。某些客户设备也可以禁用对等通信功能。也就是说，设备只能连接到特定网络，未经允许无法与其他设备建立对等连接。

不仅 IBSS 用户容易遭到对等攻击，与同一个接入点建立关联的用户也会遭到对等攻击。由于针对企业网络安全的威胁经常来自内部，因此保护无线网络也要保证授权用户的安全。所有与同一个接入点相连的用户都是同一个 BSS(基本服务集)的成员，它们属于同一个二层域和三层域并被划分到同一个 VLAN，这些用户很容易遭到对等攻击。在大部分无线局域网部署中，Wi-Fi 客户设备仅与有线网络中的设备(如电子邮件服务器或 Web 服务器)交换数据，Wi-Fi 设备之间无需进行对等通信。为此，大部分厂商都开发了专有的保护机制，以防用户在无意间共享文件或者在设备间桥接数据流量。如果无线客户设备之间需要交换数据，则流量将被三层交换机或其他网络设备路由给目标客户设备。

接入点或 WLAN 控制器经常开启客户端隔离(Client isolation)功能，以阻止同一 VLAN 中的无线客户端之间交换数据。客户端隔离功能通常意味着达到 AP 无线接口的数据包不再通过无线发送给其他无线客户端，这使得无线网络中的终端用户相互隔离，无法建立二层或三层连接。其他厂商也开发了名称不同、功能类似的机制。客户端隔离属性通常可以基于每 SSID 进行配置，每个 SSID 绑定到一个不同的 VLAN。开启客户端隔离功能后，客户端之间就无法通过无线网络直接通讯，如图 14-3。

图 14-3　客户端隔离

尽管客户端隔离(client isolation)是最常用的术语，但是有些厂商把类似的功能称为 peer-to-peer blocking、interuser bridge 或公共安全包转发(PSPF)。有些 WLAN 厂商并不是将这个功能部署在单一 AP 上的一个 SSID 或 VLAN 上，有些厂商可以跨 AP 部署。

请注意，某些应用需要使用对等连接。许多 VoWiFi 电话具备采用组播的“一键通”功能，它们通常被划分到一个独立的 VLAN，并与其他无线数据客户相互隔离。如果需要使用“一键通”多播，切记不要在 VoWiFi 设备所在的 VLAN 中启用客户端隔离机制。

14.1.3 窃听

本书前面曾经介绍过，802.11 无线局域网采用无需牌照的频段进行通信，所有数据均在空中传输。由于任何人都可以接触到范围之内的无线传输，因此必须采用高强度的加密机制保护数据安全。监控无线通信的方式包括非恶意窃听(casual eavesdropping)与恶意窃听(malicious eavesdropping)两种。

非恶意窃听通常也称为 WLAN discovery，即采用软件程序(称为 WLAN 发现工具)，利用 802.11-2007 标准中明确定义的 802.11 帧交换方法，搜索开放的无线局域网。

许多无线客户端驱动程序在进行主动扫描时，发送不包含 SSID 的空探询请求帧。例外还有许多免费 WLAN 发现程序，例如 inSSIDer、NetStumbler 和 iStumbler。这些程序在所有无需牌照的 802.11 信道中发送空探询请求帧，以期收到包含无线网络信息(SSID、信道、加密方式等)的探询响应帧。有些 WLAN 发现工具也可以利用被动扫描的方法。如图 14-4 所示，inSSIDer 是一个十分流行的免费 WLAN 扫描发现工具，它可以在 www.metageek.net 下载。

图 14-4 MetaGeek inSSIDer

WLAN 扫描一般被认为是无害的，它也被称为战争驾驶(war driving)。战争驾驶者通常在一辆移动的交通工具上进行无线网络的扫描发现。这个术语起源于 1983 的电影战争游戏(War Games)。黑客利用一种很古老的技术“War dialing”，通过计算机和调制解调器自动扫描成千上万的电话号码，试图发现可以被入侵的计算机。最常见的战争驾驶工具是 NetStumbler，如图 14-5 所示。

图 14-5　NetStumbler

从本质上说，802.11 被动扫描与主动扫描的目的是搜索对所有开放的 802.11 网络信息。由于二者是 802.11 无线局域网的必要功能，因此驾驶攻击不构成犯罪。然而，不少驾驶攻击者的目的是搜索开放的 802.11 无线网络，以便利用它们免费访问互联网。大部分国家仍在争论这种行为是否违法，不过多数驾驶攻击者并非怀有恶意的黑客，他们只是希望能暂时免费使用互联网而已。目前尚不清楚未经许可使用他人的无线网络是否违法，但是的确已经有驾驶攻击者因为这种行为被逮捕并起诉。

我们不鼓励或支持未经授权使用无线网络，建议用户仅连接到经过授权的无线网络。

实施驾驶攻击时所需的工具

在进行驾驶攻击之前，用户需要准备一块 802.11 客户网卡、一种 WLAN 发现工具和一辆汽车。互联网上有不少免费的 WLAN 发现工具，包括用于 Windows 环境的 inSSIDer 和 NetStumbler、用于 Mac OS 环境的 WiFi Scanner 以及用于 Linux 环境的 Kismet。用户也可从 www.netstumbler.com 下载该软件，从 www.wlanbook.com 下载 WiFi Scanner，从 www.metageek.net 下载 inSSIDer。

此外，用户还可以准备一根高增益外置天线，并通过尾纤接头(pigtail connector)与无线网卡相连。在搜索到某个接入点发射的信号后，不少驾驶攻击者通过 GPS 精确定位该接入点的经纬度坐标，然后将这些信息上传到互联网的大型动态地图数据库，如 WiGLE(Wireless Geographic Logging Engine，无线地理日志引擎)。WiGLE 包含超过 4 300 万个可供搜索的接入点信息，用户可访问 www.wigle.net 并输入自己的地址，查看周围是否存在已经被驾驶攻击者发现并上传的无线接入点。

与非恶意窃听相反，恶意窃听在未经授权的情况下使用协议分析仪拦截无线通信，它通常是非法的。大部分国家的法律规定，窃听电话通话以及任何电磁通信(包括 802.11 无线传输)均属违法行为。

市场上有不少商用与免费的 802.11 协议分析仪，网络管理员可以利用协议分析仪捕捉自己网络的 802.11 流量，以便分析并排除无线网络的故障。协议分析仪是一种工作在射频监控模式的被动扫描设备，能捕捉到范围之内的各种无线传输。然而，协议分析仪也可能被怀有不良动机的个人用来获取 802.11 流量。因为 WIDS 并不能探测到以被动方式获取 802.11 帧的协议分析仪，所以也无法发现正在进行的恶意窃听。由于入侵者可以截获任何未经加密的

明文消息(如电子邮件和 Telnet 密码)，因此必须采用强有力的动态加密解决方案(TKIP/RC4 或 CCMP/AES)保护数据安全。以明文形式传输的 802.11 帧可以在 OSI 模型的上层被重组，窃听者不难通过重组后的电子邮件、Web 页面与即时消息读取其中包含的信息。此外，窃听者还可以重组 VoIP 数据包，并将其保存为后缀名为.wav 的声音文件。这种恶意窃听属于严重的违法行为。由于窃听以被动方式进行，它无法被安全系统发现，因此必须始终对数据进行加密。

恶意窃听的主要对象是在公共场所提供接入的热点。一般而言，公共热点没有采取任何安全措施，数据以明文形式通过热点传输，这使得热点用户成为窃听者的主要目标。有鉴于此，移动用户在连接到企业网之外的外部网络时，必须采用 VPN 解决方案保护数据安全。

14.1.4 加密破解

第 13 章曾经介绍过，WEP(有线等效加密)目前已经被破解。利用互联网上免费的破解工具，可在短短 5 分钟之内实现 WEP 破解。破解 WEP 加密的方式有很多，不过攻击者通常只需使用协议分析仪捕捉几十万加密数据包，并通过如图 14-6 所示的 WEP 破解软件运行这些截获的数据即可。破解软件一般在几秒之内就能获得 40 位或 104 位密钥，破解后的密钥可以用于解密任何加密流量。也就是说，此时攻击者可以对采用 WEP 加密的网络实施窃听。在解密流量后，攻击者不难重组数据并读取其中包含的信息，网络对攻击者将再无秘密可言。

```
* Got  286716! unique IVs | fudge factor = 2
* Elapsed time [00:00:03] | tried 1 keys at 20 k/m

KB    depth   votes
 0    0/  1   DA(  60) 70(  23) 55(  15) A2(   5) CD(   5) 3E(   4)
 1    0/  2   BD(  57) 2A(  32) 29(  22) 1D(  13) F9(  13) 9F(  12)
 2    0/  1   8C(  51) 67(  23) 48(  15) DD(  15) D6(  13) FA(  12)
 3    0/  3   1D(  30) A5(  17) 07(  15) 7B(  12) 4B(  10) 63(  10)
 4    0/  1   43(  66) B1(  15) D2(   6) 1A(   5) 20(   5) 21(   5)
 5    0/  5   92(  27) 23(  25) 02(  18) 2F(  17) C1(  16) 36(  12)
 6    0/  1   C6(  51) 54(  17) 50(  15) 66(  15) 01(  13) 4A(  13)
 7    0/  2   84(  29) C0(  17) EE(  13) 80(  12) 49(  11) F6(  11)
 8    0/  1   81(1808) 09( 119) 99( 116) 32(  75) 49(  75) 9D(  65)
 9    0/  1   C4(1947) E1( 125) FC( 123) BD( 105) 8C(  98) 2F(  85)
10    0/  1   8A( 580) 41( 120) 18(  93) ED(  85) B0(  65) 97(  60)
11    0/  1   08(  97) FF(  29) 5D(  20) 1E(  17) 18(  15) 5E(  15)
12    0/  1   1B( 145) DD(  21) 46(  20) 1C(  15) 76(  15) 07(  13)

                KEY FOUND! [ DABD8C1D4392C68481C48A081B ]
```

图 14-6 WEP 破解软件

14.1.5 认证攻击

前面的章节曾经介绍过，可采用 802.1X/EAP 认证解决方案或预共享密钥(PSK)对要求访问网络资源的用户进行认证。802.11-2007 标准并没有定义在 802.11 无线局域网中使用哪种具体的 EAP 认证协议，而每种 EAP 的安全程度也不尽相同。例如，LEAP(轻量可扩展协议)

曾经广泛用于 802.1X/EAP 解决方案，但它很容易遭到离线词典攻击。LEAP 认证过程中使用的散列密码响应非常脆弱，容易被破解。

如图 14-7 所示，攻击者只需在 LEAP 用户进行认证时截获帧交换，并通过离线词典攻击软件运行截获的文件，就能在几秒之内获得 LEAP 认证使用的密码与用户名。攻击者可以使用破解后的密码与用户名冒充用户通过认证，从而入侵所有对合法用户开放的网络资源。使用隧道认证的 EAP 认证协议的安全性较高，不易遭到离线词典攻击。

```
Finished - root asleap - Konsole
Session  Edit  View  Bookmarks  Settings  Help
        0025 0215 0025 1101 0018 b1b6 6613 94b9  .%...%......f...
        a076 15e7 07b3 5234 3033 0b55 4b30 f276  .v....R403.UK0.v
        12a4 7465 7374 32                        .. david


Captured LEAP auth success:

        0040 96a6 deca 0012 014d b400 888e 0100  .@.......M......
        0004 0315 0004 0000 0000 0000 0000 0000  ................
        0000 0000 0000 0000 0000 0000 0000 0000  ................
        0000 0000 0000 0000 0000 0000            ............


Captured LEAP exchange information:
        username:          david
        challenge:         373931a2d1888e58
        response:          b1b6661394b9a07615e707b3523430330b554b30f27612a4
        Attempting to recover last 2 of hash.
        hash bytes:        f2d8
        Starting dictionary lookups.
        NT hash:           f70da7fad38a37d803d9f737a286f2d8
        password:          123abc123abc
Reached EOF on pcapfile.
```

图 14-7　离线词典攻击

任何认证攻击的最大风险是当身份验证凭据受到破坏时所有网络资源将受到攻击。认证攻击的威胁类似于非法接入点。如果授权的 WLAN 入口受到损害，黑客将获得认证凭据，网络资源也将面临风险。由于这些严重的风险，因此利用 RADIUS 服务器结合隧道认证 EAP 协议的 802.1X/EAP 解决方案非常必要，这已经在第 13 章谈到了。

因为大部分家庭没有使用 RADIUS 服务器，只好采用预共享密钥的 WPA/WPA2-Personal 方法，但这种方法同样容易遭到离线词典攻击，它们并不是可靠的认证方式。攻击者利用黑客软件实施离线词典攻击，可以获得 WPA/WPA2-Personal 使用的密码短语，并利用破解后的密码短语与 WPA/WPA2 接入点建立关联。更严重的是，攻击者在获得密码短语之后就能解密动态生成的 TKIP/RC4 或 CCMP/AES 加密密钥。第 13 章曾介绍过，密码短语通过算法被转换为 PMK(成对主密钥)，四次握手(4-Way Handshake)过程采用 PMK 生成用于实际加密数据的动态密钥。如果攻击者取得密码短语并破解四次握手过程，就可以重新生成动态加密密钥，从而解密流量。一旦密码短语被破解，攻击者就能入侵网络资源并解密流量，因此 WPA/WPA2-Personal 并非一种可靠的企业安全解决方案。但是，如果不存在 AAA 服务器或客户设备不支持 802.1X/EAP 解决方案，则推荐部署私有的 PSK 认证解决方案，即独特的 PSK 解决方案。

要部署 WPA/WPA2-Personal 解决方案，应制定严格的安全策略，规定必须采用高强度的密码短语(至少 20 个字符)。静态密码短语还可能遭到社会工程学攻击，为此必须在安全策略

中规定，只有管理员掌握所有静态密码短语，禁止向终端用户泄露密码短语。

14.1.6 MAC 欺骗

每块 802.11 无线网卡都有一个称为 MAC 地址的物理地址。MAC 地址位于 802.11 帧的二层帧头，由 12 个十六进制数构成，并未加密。大部分 Wi-Fi 厂商的接入点都具备 MAC 过滤功能，即仅允许来自特定客户端的流量通过接入点。MAC 过滤基于每个客户端唯一的 MAC 地址。如果一个客户端的 MAC 地址没有出现在允许列表中，接入点将禁止该客户端的流量通过其虚端口进入分布系统介质。当传统客户端(如手持扫描枪)不支持更安全的认证加密方法时，经常使用 MAC 过滤功能。

然而，MAC 地址可以被欺骗或伪造。业余黑客只要将自己的 MAC 地址伪装成某个出现在允许列表中的客户端的 MAC 地址，就能轻易绕过 MAC 过滤。这可以通过在 Windows 设备管理器中修改无线网卡的 MAC 地址或简单编辑注册表来实现。图 14-8 显示一种用于实施 MAC 欺骗的第三方软件。

图 14-8 MAC 欺骗软件

由于 MAC 地址易于伪造且配置工作较为繁琐，因此 MAC 过滤并非一种可靠的企业无线安全解决方案，应仅将其作为最后的安全手段使用。某些情况下，如果客户设备不支持 802.1X/EAP，则可以考虑将 MAC 过滤作为整体安全措施的一部分。

14.1.7 管理接口漏洞

与管理有线基础架构硬件设备类似，管理员通过各种接口对无线基础架构硬件设备(如自治接入点与 WLAN 控制器)进行管理。一般而言，可以通过 Web 接口、命令行接口、串口、控制台连接以及(或者)SNMP(简单网络管理协议)访问设备。

前面曾经介绍过，保护这些接口的安全至关重要。应禁用所有不使用的接口、选择高强

度的密码并尽量采用经过加密的登录功能(如 HTTPS)。

用户可在互联网上找到所有主流厂商生产的接入点的默认设置，不过请注意，黑客也经常使用这些信息寻找潜在的安全漏洞。入侵者往往会利用管理接口存在的安全漏洞重新配置接入点，从而导致合法用户与管理员无法访问无线网络设备，这种情况屡见不鲜。

在取得管理接口的控制权之后，攻击者还可以实施无线硬件设备的固件升级，并在升级过程中突然关闭设备电源。这会造成设备故障，用户不得不将设备返回原厂维修。

有鉴于此，必须在安全策略中规定，只能通过网络的有线端配置所有无线局域网基础架构设备。如果管理员试图以无线方式配置 802.11 设备，则配置改变后，管理员可能无法访问设备。某些 WLAN 厂商提供一种安全无线控制台连接方法以进行配置和排错。

14.1.8　无线劫持

无线劫持(wireless hijacking)是一种经常会给网络安全造成很大压力的攻击，又被称为双面恶魔攻击(evil twin attack)。攻击者在其笔记本电脑中安装无线热点软件，有些尺寸很小的 USB WiFi 网卡也可以变成 AP，并配置与公共热点相同的 SSID。此后，攻击者向网络发送伪造的解除关联帧或解除认证帧，强制与公共热点建立关联的用户中断与热点的连接，并漫游到双面恶魔接入点。这时候，无线客户端在二层被攻击者劫持。通过解除认证帧或射频干扰器都可以让客户端漫游到 evil twin AP，从而开始无线劫持。

攻击者一般还会在双面恶魔接入点上配置为客户端分配 IP 地址的 DHCP(动态主机配置协议)服务器。这时候，无线客户端在三层被攻击者劫持，攻击者可以毫无阻碍地对被劫持的用户发动对等攻击。用户的计算机一旦连接到双面恶魔 AP 就变成了 DHCP 攻击的牺牲品，攻击者利用 DHCP 除了分配 IP 以外，还将 root kit 或者其他恶意程序注入到用户计算机上。

如图 14-9 所示，攻击者还可以使用笔记本电脑中的第二块无线网卡实施中间人攻击(man-in-the-middle attack)。这种情况下，第二块无线网卡作为客户端与热点建立关联。操作系统中的网卡可以被桥接在一起以路由流量，攻击者利用这个性质将第二块无线网卡与作为双面恶魔接入点使用的无线网卡桥接起来。用户从原接入点被劫持之后，该恶意接入点将用户和原接入点之间的流量路由给第二块无线网卡，再由后者路由给原接入点。这种情况下，虽然用户一直处于被劫持状态，但是由于流量仍然通过网关被路由回原接入点，用户始终无法发现自己被劫持。攻击者处于合法接入点与用户之间，可以随意发动对等攻击而完全不会暴露。

无线劫持的另一种形式是 Wi-Fi 钓鱼攻击(Wi-Fi phishing attack)。为实施这种攻击，攻击者需要配置 Web 服务器软件与强制网络门户软件。用户被劫持到双面恶魔接入点之后，将被重定向到一个与热点的登录页面完全相同的页面，这个伪造的登录页面会要求被劫持的用户输入信用卡号。钓鱼攻击在互联网上较为普遍，公共热点目前也深受其害。

唯一能阻止无线劫持、中间人攻击与 Wi-Fi 钓鱼攻击的方法是采用双向认证解决方案。双向认证不仅对要求连接网络的用户进行认证，也对用户正在连接的网络进行认证。802.1X/EAP 解决方案规定，通信双方必须首先交换双向认证的身份凭证，只有合法用户才能通过授权并获得 IP 地址，这就防止了用户受到劫持。

图 14-9 无线劫持/中间人攻击

14.1.9 拒绝服务攻击

在各种针对无线网络的攻击中，最容易被忽视的攻击是 DoS(denial of service，拒绝服务)。不法分子可以利用合适的工具阻止合法用户访问网络资源，从而在一段时间内瘫痪 Wi-Fi 网络。尽管监控系统能在第一时间发现并识别 DoS 攻击，但是除非确定攻击源的位置并将其彻底消除，否则无法阻止 DoS 攻击。

DoS 攻击针对 OSI 模型的物理层或数据链路层。一层攻击称为射频干扰攻击(RF jamming attack)，两种最常见的射频干扰攻击是蓄意干扰和非蓄意干扰。

攻击者使用信号生成器干扰无需牌照的频段，这种干扰属于蓄意干扰。窄带与宽带干扰器都能对 802.11 通信实施干扰，从而破坏所有数据。此外，802.11 无线接口卡在实施空闲信道评估(CCA)时，会因为蓄意干扰的存在而始终无法使用介质传输数据。

相对于恶意的蓄意干扰，非蓄意干扰更为普遍。来自微波炉、无绳电话和其他设备的非蓄意干扰都可能导致网络的拒绝服务。尽管非蓄意干扰未必是针对无线网络的攻击，不过它造成的危害并不亚于蓄意干扰攻击。

唯一能检测到所有第一层蓄意干扰与非蓄意干扰的工具是频谱分析仪。

黑客发动的各种第二层 DoS 攻击更为普遍，第二层 DoS 攻击通过篡改 802.11 帧来实现。例如，伪造解除关联帧或解除认证帧是最常见的一种第二层 DoS 攻击。攻击者修改这两种管理帧的帧头，在目标地址字段或源地址字段中伪造接入点或客户端的 MAC 地址，然后向网络持续发送伪造后的解除关联帧或解除认证帧。由于这两种管理帧属于通告而非请求，通信双方必须接受，因此 802.11 设备将始终处于无法通信的状态。

第二层 DoS 攻击的种类很多，包括关联帧泛洪、认证帧泛洪、PS-Poll 帧泛洪以及虚拟

载波攻击。目前的 WIDS 都能在第一时间发现第二层 DoS 攻击并通知管理员。为确保管理帧的传输安全，802.11w-2009 修正案定义了管理帧保护(management frame protection，MFP)机制，它可以防止某些类型的 802.11 管理帧的欺骗。802.11w 帧也被称为强健管理帧，这些强健安全帧包括解除关联帧、解除认证帧和强健行为帧，可以由管理帧保护服务加以保护。其中的行为帧被用来要求无线终端在代表其他无线终端的时候必须采取某些动作，并非所有的行为帧都是强健安全的。

不过 802.11w 修正案能否彻底阻止所有第二层 DoS 攻击还有待观察。此外，802.11w 管理帧保护机制还未得到客户端的广泛支持。但是一旦厂商开始部署 802.11w 机制的话，大部分基于第二层的 DoS 攻击都可以被阻止。

频谱分析仪是检测第一层 DoS 攻击的最佳工具，协议分析仪或 WIDS 是检测第二层 DoS 攻击的最佳工具。但是，唯有采用完善的物理安全措施才能阻止所有 DoS 攻击。本书作者建议用户配备护卫犬并安装带刺的铁丝网，或采用其他可以发现第一层与第二层入侵的解决方案。

如何了解无线局域网的安全风险评估？

这一章讲述 Wi-Fi 安全攻击和监测的基本知识。虽然有许多关于无线攻击的书籍，但我们推荐 *CWSP Certified Wireless Security Professional Official Study Guide*，考试编号：PW0-204 (Sybex，2010 年)。此外还有许多用于 Wi-Fi 渗透测试的 WLAN 安全审核工具。

BackTrack 大概是最受欢迎的基于 Linux 的渗透测试工具。最新的 Backtrack 有 300 多个最新工具，是按照安全专业人员的工作流程组成的。BackTrack 平台可以直接从 CD-ROM 驱动器或者从虚拟化映像(如 VMware)启动运行。可从 www.remote-exploit.org/backtrack.download.html 下载免费的 ISO 映像。

另一个不错的网站提供了关于 WLAN 审计软件工具的信息：Wirelessdefence.org，呈现了用于审计 802.11 网络的精辟提示意见，并为 WLAN 安全审计人员经常需要完成的任务提供“一站式指导”。可从 http://wirelessdefence.org 下载许多 WLAN 审计工具。

还有一些商用的 WLAN 渗透工具。Immunity 公司就可以提供安全评估和渗透测试解决方案。有关 immunity 的 WLAN 安全评估解决方案、SILICA、SILICA-U 等信息可以在它的网站上找到，网址是 www.immunityinc.com。

14.1.10　厂商漏洞攻击

某些自治型接入点与 WLAN 控制器厂商的固件代码可能存在安全漏洞，黑客经常利用这些漏洞实施缓存溢出攻击(buffer overflow attack)。无线局域网厂商在发现针对自己产品的攻击后，一般会及时发布固件升级补丁。用户应时刻关注厂商发布的安全信息，以保护设备的安全。

14.1.11　社会工程学

使用黑客软件或工具入侵有线或无线网络并非攻击者的首选，危害计算机安全的主要因

素是社会工程学攻击(social engineering attack)。社会工程学是一种诱使人们泄露机密信息(如计算机密码)的技术，阻止社会工程学攻击的最好方法是严格执行安全策略，以防机密信息外泄。

所有静态信息都极易遭到社会工程学攻击。WEP 加密采用静态密钥，WPA/WPA2-Personal 采用静态预共享密钥或静态密码短语。由于静态信息的安全性很差，应避免在企业无线网络中采用 WEP 或 WPA/WPA2-Personal。

14.2 入侵监控

在提到无线时，大部分人只想到无线网络提供的接入和移动功能，而忽视了针对无线网络的攻击或入侵。本章前面介绍的各种攻击都可能危害到无线网络的安全，因此持续监控无线网络的运行状况势在必行。企业在部署 802.11 无线网络的同时也部署了入侵检测系统，以监控针对无线网络的攻击。许多企业十分关注非法接入点带来的安全隐患。在部署提供用户接入的无线网络之前，企业可能会首先部署 WIDS，这种情况并不鲜见。

无线入侵监控已取得了长足发展。目前，大部分入侵监控系统都能阻止或减轻一部分已知无线攻击造成的危害。大型企业多采用易于扩展的分布式入侵监控系统，不过某些厂商也推出了可以在笔记本电脑上运行的单机版入侵监控系统。虽然无线入侵监控的对象主要是二层攻击，但是目前也存在能扫描一层攻击的无线入侵监控系统。

14.2.1 无线入侵检测系统

目前，即使某些场所不允许部署 802.11 无线局域网，也可能需要安装 WIDS(Wireless Intrusion Detection System，无线入侵检测系统)。攻击者可以利用无线网络入侵网络资源。企业必须对有线数据端口进行监控，以防员工或其他人员安装非法接入点。为消除安全隐患，在部署提供用户接入的 802.11 无线网络之前，金融机构(如银行)、医院等许多行业都会选择首先安装 WIDS。802.11 网络部署完毕后，同样必须使用 WIDS 监控针对 Wi-Fi 的各种攻击(如 DoS 攻击与无线劫持)。典型的 WIDS 采用客户端/服务器架构，由以下 3 部分组成。

WIDS 服务器 基于软件或硬件，作为中央管理点，进行数据收集。服务器利用签名分析、行为分析、协议分析和射频频谱分析对潜在威胁进行检测。签名分析通过与通常的 WLAN 攻击进行模式比对来发现威胁。行为分析可以探测到 802.11 异常动作。协议分析会仔细分析来自于 802.11 帧的 MAC 层信息，也可以查看未被加密的 802.11 数据帧的 3～7 层的信息。频谱分析监控射频统计(如信号强度、信噪比)。性能分析测量 WLAN 健康状态(如覆盖与容量)。

管理控制台 是一个软件接口，作为客户端与 WIDS 服务器相连，对服务器和传感器进行管理和配置。它可以对无线网络进行不间断监控。

传感器 基于硬件或软件，置于各个重要的位置，用于监控并捕获所有 802.11 通信。它就像 WIDS 的眼睛和耳朵，它利用 802.11 射频卡对 WLAN 流量进行采集和分析。

图 14-10 显示了大部分 WIDS 采用的客户端/服务器模式。

传感器实际上是一种工作在持续监听模式的无线接口，它属于被动监测设备。硬件传感器较为常见，其外观类似于接入点。传感器具备一定的智能，但必须与中央 WIDS 服务器相

互通信。集中式服务器能够处理大量远端传感器采集的数据，以满足许多大型企业的监控需要。管理控制台也可以安装在远端并与中央服务器相连，同时对所有装有传感器的远端无线局域网实施监控。图 14-11 显示了 AirTight Networks 的 WIDS 管理控制台。

图 14-10　无线入侵检测系统(WIDS)

图 14-11　WIDS 管理控制台

由于传感器仅配置为监听模式，因此它不提供客户接入功能。传感器一般对 2.4GHz ISM 频段全部 14 个信道以及 5GHz UNII 频段全部 24 个信道实施不间断扫描，少数情况下也可以将传感器设置为仅监听一个或一组信道。AP 还可以作为“兼职”传感器，此时它可以使用离频扫描的方法监视其他信道，但仍把大部分时间留给主信道，用来提供客户端访问服务。

WIDS 最适合监控针对无线网络的二层攻击，如 MAC 欺骗、解除关联攻击以及解除认证攻击。大部分 WIDS 都能发现多达 100 种潜在的安全漏洞。部署 WIDS 时，必须设置合适的策略与告警机制。入侵检测系统经常会出现误报，这可以通过定义合适的策略和阈值加以解决。此外，应根据严重程度将各种警报划分为不同的级别，并发送相应的告警通知。例如，设备向外广播 SSID 可能不会对安全构成重大威胁，这时可以关闭这个警告。而解除认证欺骗攻击是一种严重危害网络安全的行为，应将其划分为高危等级，并向管理员自动发送电子邮件消息或寻呼机通知。

WIDS 通常用于监控系统安全，不过许多 WIDS 也可以用于监控系统性能。例如，如果带宽消耗过大或 VoWiFi 电话漫游与重认证的次数过于频繁，WIDS 将发出性能警报。

目前存在以下 3 种 WIDS 设计模型：

覆盖型(overlay) 是最安全的 WIDS 模型，部署在现有无线网络之上。覆盖型 WIDS 采用厂商生产的专用 WIDS，可以对任何现有或规划中的无线局域网实施监控。覆盖型 WIDS 功能齐全，但价格昂贵。覆盖型解决方案由 WIDS 服务器与专职传感器构成，传感器不提供客户接入。

集成型(integrated) 许多 WLAN 控制器厂商在其产品中集成了全面的入侵检测功能。在集成型 WIDS 中，WLAN 控制器作为中央 WIDS 服务器使用，轻量接入点可以被配置为专职传感器，也可以在不作为接入点使用时被配置为兼职传感器。在 WLAN 控制器架构中，轻量接入点采用“信道外扫描”(off-channel scanning)以实现动态射频频谱管理，还能作为兼职传感器为 WIDS 服务器提供监控数据。建议同时部署一定数量的轻量接入点作为专职传感器使用。集成型 WIDS 的功能没有覆盖型 WIDS 齐全，但价格低于后者。

集成启用型(integration enabled) Wi-Fi 厂商常将自己的接入点和管理系统与主流 WIDS 厂商的产品集成在一起。Wi-Fi 厂商生产的接入点集成有软件代码，可以将接入点转换为与第三方 WIDS 服务器通信的传感器。自治型接入点或基于控制器的 AP 可以转换为与第三方 WIDS 服务器通信的全职传感器，为其提供安全监控信息。

14.2.2 无线入侵防御系统

大部分 WIDS 厂商更愿意将它们的产品称为 WIPS(Wireless Intrusion Prevention System，无线入侵防御系统)，因为他们的产品都能降低非法接入点与客户端造成的威胁。WIPS 把设备分为以下 4 类(也可能更多)：

基础架构设备 企业无线网络中的授权客户端或接入点被标记为基础架构设备。在 WIPS 检测到某个无线射频卡后，管理员可以人工将其标记为基础架构设备，也可以将所有企业无线接口卡的 MAC 地址导入系统。

未知设备 任何检测到但不属于非法设备的 802.11 无线接口被自动标记为未知设备。未知

设备被视为干扰设备，一般会对其进行进一步的分析，以确定它属于邻居设备还是安全隐患。

已知设备　任何检测到且身份已知的客户端或接入点被标记为已知设备。已知设备最初被视为干扰设备，通常由管理员人工将其标记为不会对网络安全构成威胁的邻居设备。

非法设备　任何对网络造成干扰或可能威胁网络安全的客户端或接入点被标记为非法设备。大部分 WIPS 将非法接入点定义为与骨干网实际相连、但不属于已知设备或不在管理员控制之下的设备。WIPS 厂商采用各种专有方式检测是否有非法接入点连接到有线基础架构。

大多数 WIPS 厂商使用不同的术语来分类设备。例如有些 WIPS 系统把所有的非授权设备都称为非法设备，而有些 WIPS 系统只认为那些与有线网络连接的 AP 或 WLAN 设备才是非法设备。

在某个客户端或接入点被划分为非法设备之后，WIPS 将采取相应的措施以减轻非法设备造成的危害。WIPS 厂商采用多种手段消除安全隐患，伪造解除认证帧是其中最常用的一种手段。如图 14-12，WIPS 系统激活传感器，将非法接入点与客户端的 MAC 地址写入解除认证帧，并将其发送到网络中。WIPS 使用这种已知的二层 DoS 攻击作为反制手段，强迫非法设备终止与有线网络的连接。这种方法可以用于消除非法接入点、单一客户端与非法 ad hoc 网络造成的危害。

图 14-12　无线非法抑制

此外，WIPS 也可以采用 SNMP 作为反制非法设备的手段。大部分 WIPS 都能发现连接到有线基础架构的非法接入点，并通过 SNMP 关闭非法接入点所连接的受控交换机端口。一旦将交换机端口关闭，攻击者就无法通过非法接入点入侵网络资源。

WIPS 厂商还采用其他专有的方法消除非法接入点与客户端造成的危害，但是这些方法通常并不会向外界公布。WIPS 目前主要用于抑制并消除非法设备，不过今后也可能会用于阻止其他无线攻击。

真实场景

WIPS 能保护有线网络不受所有已知非法设备的侵害吗？

简单地说：不能。虽然 WIPS 可以减轻大部分非法设备造成的危害，但它无法检测出所

有非法设备。一般而言，WIPS 传感器中的无线接口卡可以对 2.4GHz ISM 频段与 5GHz UNII 频段实施监控，也可以对 4.9GHz 频段范围和 5GHz 的 ISM 频段的 165 信道进行监控。而某些早期的无线网络设备使用 900MHz ISM 频段收发数据，这些设备并不能被 WIPS 发现。

此外，WIPS 传感器中的无线接口卡采用 DSSS(直序扩频)与 OFDM(正交频分复用)技术，因此无法发现采用 FHSS(跳频扩频)技术、使用 2.4GHz ISM 频段传输数据的无线网络设备。唯一能百分之百地监控 900MHz 频段或发现 FHSS 非法接入点的设备是频谱分析仪。

并非所有的 WIPS 系统都有频谱分析能力，尽管分布式的频谱分析正在普及。即便 WIPS 具有频谱分析功能，它也只能在某个频率范围内进行，通常这个频率范围与其作为 WIPS 所监控的频率相同。WIPS 需要具备监控所有信道的能力，这种监控不应受地域限制。例如，攻击者往往将非法设备配置在 2.4GHz 频段的信道 14，而许多国家的无线局域网并不能使用该信道。

14.2.3 移动 WIDS

部分厂商还推出了可在笔记本上使用的无线入侵检测系统。移动 WIDS 是一种协议分析程序，它能解码数据帧并具备一定的物理层分析能力。移动 WIDS 采用标准的 Wi-Fi 客户无线射频卡作为传感器，但是它主要用于实施独立的移动安全与性能分析。移动 WIDS 具有与分布式解决方案相同的策略、告警与检测功能，可以将其视为一种集传感器、服务器和控制台于一身的单机版解决方案。移动 WIDS 的优点是便于携带，不过它只能发现监听范围之内的无线攻击。除检测非法接入点与客户端之外，移动 WIDS 还能对非法设备进行跟踪。在移动 WIDS 锁定非法设备发射的射频信号后，管理员可采用定向天线确定非法设备的位置。图 14-13 显示了大部分移动 WIDS 具有的定位功能。

图 14-13 移动 WIDS 定位工具

我们强烈建议读者实际体验一下移动 WIDS 提供的各种功能。Motorola AirDefense Solutions 开发的 AirDefense Mobile 是一种移动 WIDS 解决方案，读者可从以下网址下载该软件的 30 天全功能试用版：www.airdefense.net/products/admobile/unique_trial.php。

14.2.4　频谱分析仪

第 15 章与第 16 章将介绍在无线现场勘测中使用频谱分析仪的优点，而无线局域网管理员已经开始意识到频谱分析仪在保护网络安全中所起的重要作用。处于 OSI 第二层的 WIDS 厂商一直宣称其产品具备检测一层 DoS 攻击(射频干扰)的能力，不过事实并非如此。虽然 WIDS 可以发现所有针对无线网络的第二层攻击，但是由于传感器的无线射频卡并非频谱分析仪，WIDS 无法有效检测出第一层攻击。

频谱分析仪是一种频域工具，可以检测所扫描的频段中是否存在射频信号。监控 2.4GHz ISM 频段的频谱分析仪能发现各种蓄意干扰与非蓄意干扰设备。某些频谱分析仪还能根据干扰信号的射频签名将设备划分为相应的类别，如微波炉、蓝牙发射器或 802.11FHSS 无线接口。此外，频谱分析仪也可以用于确定 900MHz 或 FHSS 非法接入点的位置。

频谱分析系统包括移动与分布式两类。大部分频谱分析仪都属于独立的移动解决方案，不过某些 WIPS 厂商也开发了分布式频谱分析系统(distributed spectrum analysis system，DSAS)，后者由一台集中式服务器与若干远端硬件频谱分析仪卡式总线传感器构成。此外，一些 WIPS 厂商也利用第二层 WIDS 传感器的 802.11 无线射频卡已有的射频功能提供分布式频谱分析。分布式频谱分析系统(DSAS)相当于一种第一层 WIDS，它能检测并根据频率签名划分射频干扰的类别，这有助于干扰设备的分类与定位。大多数 DSAS 系统都利用集成在 AP 中与无线射频卡独立的频谱分析卡进行频谱分析，有些厂商的 AP 利用 802.11 射频卡来完成较低水平的频谱分析。

14.3　无线安全策略

第 13 章介绍了 802.11 无线网络采用的各种认证、加密与 RBAC 机制，而这一章前面几节介绍了用于监控安全威胁的无线入侵检测系统。网络保护与漏洞监控固然重要，但是二者只有配合相应的安全策略才能真正发挥作用。如果终端用户将密码随意公布，使用 802.1X/EAP 解决方案还有什么意义？如果尚未制定处理非法接入点的策略，购置入侵检测系统又有多大用处呢？

越来越多的企业已开始修改自己的网络使用策略，并在其中增加了有关无线安全方面的内容。尚未修改安全策略的企业请务必考虑制定保护无线局域网的方针。读者可以从 SANS 协会(美国系统与网络安全协会)和 NIST(美国国家标准与技术研究院)获取有关计算机安全策略与最佳实践的信息。

SANS 协会提供了有关安全策略的模板，下载地址为：www.sans.org/resources/policies/。

NIST 提供了有关无线安全的特种文献(800-48)，下载地址为：http://csrc.nist.gov/publications/nistpubs。

14.3.1 一般性安全策略

制定无线安全策略时，必须首先定义一般性策略。一般性策略描述了企业或组织制定无线安全策略的目的。即使企业尚未规划部署无线网络，也应制定处理非法设备的相关措施，这是确保网络安全的最低要求。一般性无线安全策略定义了以下内容：

策略制定 规定策略的制定者以及支持策略实施的高管人员。

适用对象 定义策略面向的群体(员工、访客与承包商)。

违规汇报流程 规定策略的执行方式，包括采取的措施以及策略执行的监督者。

风险评估与威胁分析 定义潜在的无线安全漏洞与威胁，评估企业无线网络遭到攻击后的经济损失情况。

安全审计 定义内部审计流程以及独立的外部审计需求。

14.3.2 功能性安全策略

功能性策略从技术角度定义了无线安全，即采用何种措施和手段保护无线网络的安全。功能性无线安全策略定义了以下内容：

策略基础 定义基本的安全规程，如密码策略、培训以及如何正确使用无线网络。

基准惯例 定义最低限度的无线安全惯例，如配置清单、分期与测试程序等。

设计与实现 定义实际采用的认证、加密与分段方式。

监控与响应 定义各种无线入侵检测流程以及相应的告警机制。

14.3.3 信息安全法规

大部分国家都制定了相关的法规以保护政府机构数据通信的安全。在美国，NIST 负责维护 FIPS(Federal Information Processing Standards，联邦信息处理标准)。与无线安全有关的是 FIPS 140-2 标准，它定义了加密模块的安全要求。美国政府规定，所有非涉密通信必须采用经过验证的加密模块。其他国家也接受 FIPS 140-2 标准或制定了类似的法规。

为保护相关行业的信息与通信安全，美国还制定了其他法规，包括：

健康保险流通与责任法案(HIPAA) 该法案是关于电子医疗保健交易、供应商、健康保险计划以及雇主的国家标准，旨在保护患者的信息安全与个人隐私。

塞班斯法案(Sarbanes-Oxley Act) 该法案于 2002 年颁布，法案对上市公司财务制度及审核程序做出了极为严格的规定，旨在进一步明确上市公司的责任并加强对财务信息披露的管理。

格雷姆-里奇-比利雷法案(Gramm-Leach-Bliley Act，GLBA)　该法案要求金融机构向客户解释其有关信息共享的政策和规定，以保护信用卡号、社会安全号、姓名、地址等敏感的个人信息。

有关 FIPS 的信息请参阅 http://csrc.nist.gov/publications/FIPS，有关健康保险流通与责任法案的更多信息请参阅 www.hhs.gov/ocr/hippa，有关塞班斯法案的一般信息请参阅 www.sarbanes-oxley-101.com，有关格雷姆-里奇-比利雷法案的更多信息请参阅 www.ftc.gov。

PCI 合规

因为越来越多的的人持续依靠信用卡付款，因不安全的处理过程，持卡人信息有可能被泄露。支付卡行业(PCI)意识到为了维持持续的业务增长，必须采取措施，以保护客户数据和卡号。PCI 安全标准委员会(SSC)已为处理和存储持卡人信息制定标准，即 PCI 标准。在此标准范围内规范无线设备的使用。请访问如下网站，以了解关于 PCI 标准的更多信息：

www.pcisecuritystandards.org

www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf

14.3.4　无线局域网安全策略建议

制定详尽、全面的安全策略必不可少，我们强烈建议安全策略中包括以下 5 方面有关无线安全的内容：

远程接入无线局域网策略　大部分终端用户可能在公司以外的场所(如家中或公共热点)使用笔记本电脑或手持设备接入互联网。由于不少远端无线网络并未部署任何安全措施，因此必须严格执行远程接入无线局域网策略。该策略应包括采用 IPSec VPN 解决方案进行设备认证与用户认证，并加密所有无线数据流量。公共热点是恶意窃听的主要目标，应在所有远端计算机中安装个人防火墙以阻止对等攻击。尽管个人防火墙对劫持攻击无能为力，但是它能防止攻击者接触到大部分重要信息。为保护数据安全，可以部署端点无线局域网策略执行软件解决方案，强制终端用户在访问外部无线网络时使用 VPN 与防火墙。公共热点的安全性很差，大部分攻击都针对热点，因此必须强制采用远程接入策略。

非法接入点策略　禁止任何终端用户在企业网中自行安装无线设备(接入点、无线路由器、无线硬件 USB 客户端、无线网卡等)，因为这可能对主体基础架构网络的安全造成严重危害。必须严格执行该策略。

ad hoc 策略　禁止任何终端用户设置 ad hoc 或对等网络。对等网络几乎不对数据传输加密，它不但本身容易遭到对等攻击，还可能成为攻击者入侵有线基础架构网络的跳板(配合计算机的以太网端口)。

合理使用无线局域网策略　制定正确使用与实现企业主体无线网络的详尽策略，包括正确的安装规程、正确的安全实现以及允许在无线局域网中使用的应用。

入侵检测系统策略　制定正确处理 WIDS 告警信息的策略。例如，检测到非法接入点之

后应采取的必要措施。

读者可以参考上述内容制定本企业的无线安全策略。由于 Windows XP 内置的 Wi-Fi 客户端程序 WZC(无线零配置)存在大量已知的安全漏洞，本书作者建议始终禁用 WZC。此外，建议用户使用同一家厂商的客户端程序。如果必须支持多家厂商的无线网卡，则应考虑安装第三方客户端程序。

14.4 小结

本章介绍了各种潜在的无线攻击与安全威胁。非法接入点是危害无线网络安全的罪魁祸首，其次是社会工程学攻击，但其他攻击(如对等攻击与窃听)造成的危害并不亚于非法接入点与社会工程学攻击。本章还讨论了 DoS 攻击，监控系统可以发现但无法消除 DoS 攻击。我们还介绍了用于入侵监控的各种解决方案。大部分入侵检测解决方案采用分布式的客户端服务器架构，某些解决方案具备阻止非法设备的能力。此外，本章还介绍了制定无线安全策略的必要性，完善的安全策略是无线安全解决方案的基础。

14.5 考试要点

理解非法接入点造成的危害。解释攻击者可以通过非法接入点入侵网络资源的原因，理解大部分非法接入点都是企业员工自行安装的。

定义对等攻击。理解攻击者可以通过接入点或 ad hoc 网络发动对等攻击，并解释如何抵御这种攻击。

了解窃听造成的危害。解释非恶意窃听与恶意窃听的区别，并解释加密在保护数据安全中所起的作用。

定义认证与劫持攻击。解释二者对无线网络造成的危害，理解部署 802.1X/EAP 解决方案能有效缓解这些攻击。

解释无线 DoS 攻击。了解一层与二层 DoS 攻击的区别。解释监控系统只能发现但无法消除 DoS 攻击的原因。

理解各种无线入侵监控解决方案。解释 WIDS 与 WIPS 的区别。理解大部分解决方案采用分布式主从架构，了解入侵监控解决方案的构成以及各种 WIDS 模型。理解 WIDS 可以发现与可以阻止的攻击。

理解制定无线安全策略的必要性。解释一般性策略与功能性策略的区别。

14.6 复习题

复习题的答案见附录 A。

1. Which of these attacks are considered denial-of-service attacks? (Choose all that apply.)

   A. Man-in-the-middle

B. Jamming

C. Deauthentication spoofing

D. MAC spoofing

E. Peer-to-peer

2. Which of these attacks would be considered malicious eavesdropping? (Choose all that apply.)

A. NetStumbler

B. Peer-to-peer

C. Protocol analyzer capture

D. Packet reconstruction

E. PS polling attack

3. Which of these attacks will not be detected by a wireless intrusion detection system (WIDS)?

A. Deauthentication spoofing

B. MAC spoofing

C. Rogue access point

D. Protocol analyzer

E. Association flood

4. Which of these attacks can be mitigated with a mutual authentication solution? (Choose all that apply.)

A. Malicious eavesdropping

B. Deauthentication

C. Man-in-the-middle

D. Wireless hijacking

E. Authentication flood

5. Select two types of rogue devices that cannot be detected by a layer 2 wireless intrusion prevention system (WIPS):

A. 900 MHz radio

B. 802.11h-compliant device

C. FHSS radio

D. 802.11b routers

E. 802.11g mixed-mode device

6. When designing a wireless policy document, what two major areas of policy should be addressed?

A. General policy

B. Functional policy

C. Rogue AP policy

D. Authentication policy

E. Physical security

7. What can happen when an intruder compromises the PSK or passphrase used during WPA/WPA2-Personal authentication? (Choose all that apply.)

A. Decryption

B. ASLEAP attack

C. Spoofing

D. Encryption cracking

E. Access to network resources

8. Which of these attacks are considered layer 2 denial-of-service attacks? (Choose all that apply.)

A. Deauthentication spoofing

B. Jamming

C. Virtual carrier attacks

D. PS-Poll floods

E. Authentication floods

9. Which of these can cause unintentional RF jamming attacks against an 802.11 wireless network? (Choose all that apply.)

A. Microwave oven

B. Signal generator

C. 2.4 GHz cordless phones

D. 900 MHz cordless phones

E. Deauthentication transmitter

10. Which of these tools will best detect frequency hopping rogue devices? (Choose all that apply.)

A. Stand-alone spectrum analyzer

B. Distributed spectrum analyzer

C. Distributed layer 2 WIDS

D. Mobile layer 2 WIDS

E. Layer 2 WIPS

11. Select two solutions that can help mitigate peer-to-peer attacks from other clients associated to the same 802.11 access point:

A. Personal firewall

B. Client isolation

C. OSPF

D. MAC filter

E. Access control lists

12. What type of solution can be used to perform countermeasures against a rogue access point?

A. WIDS

B. 802.1X/EAP

C. WIPS

D. TKIP/RC4

E. WINS

13. Select the four labels that a WIPS uses to classify an 802.11 device:

A. Infrastructure

B. Known

C. Enabled

D. Disabled

E. Rogue

F. Unknown

14. Scott is an administrator at the Williams Lumber Company, and his WIPS has detected a rogue access point. What actions should he take after discovering the rogue AP? (Choose the best two answers.)

A. Enable the layer 2 rogue containment feature that his WIPS provides.

B. Unplug the rogue AP from the electrical outlet upon discovery.

C. Call the police.

D. Call his mother.

E. Unplug the rogue AP from the data port upon discovery.

15. Which of these attacks are wireless users susceptible to at a public-access hotspot? (Choose all that apply.)

A. Wi-Fi phishing

B. Happy AP attack

C. Peer-to-peer attack

D. Malicious eavesdropping

E. 802.11 sky monkey attack

F. Man-in-the-middle

G. Wireless hijacking

16. Select two components that should be mandatory in every remote access wireless security policyd:

A. Encrypted VPN

B. 802.1X/EAP

C. Personal firewall

D. Captive portal

E. Wireless stun gun

17. MAC filters are typically considered useless in most cases because of what type of attack?
    A. Spamming
    B. Spoofing
    C. Phishing
    D. Cracking
    E. Eavesdropping
18. WLAN controllers typically deploy which type of WIDS deployment model?
    A. Integrated
    B. Overlay
    C. Access distribution
    D. Edge distribution
    E. Overlay enabled
19. Which of these encryption technologies have been cracked? (Choose all that apply.)
    A. 64-bit WEP
    B. TKIP/RC4
    C. CCMP/AES
    D. 128-bit WEP
    E. Wired Equivalent Privacy
20. What is another name for a wireless hijacking attack?
    A. Wi-Fi phishing
    B. Man-in-the-middle
    C. Fake AP
    D. Evil twin
    E. AirSpy

第15章 射频现场勘测基础

在该章中，你将学习以下内容：

- √ 无线局域网现场勘测概述
  - 客户简报
  - 业务需求
  - 容量与覆盖要求
  - 现有的无线网络
  - 基础架构连接性
  - 安全期望
  - 访客接入
- √ 文档与报告
  - 表格与客户文档
  - 交付报告
  - 附加报告
- √ 垂直市场
  - 室外勘测
  - 美观
  - 政府
  - 教育
  - 医疗
  - 热点
  - 零售业
  - 仓储业
  - 制造业
  - 多租户大楼

第 16 章将从技术角度介绍无线现场勘测，并讨论实施正确的覆盖、频谱与性能分析所需的各种流程与工具。这一章将从管理角度介绍无线现场勘测。在实际进行无线局域网现场勘测之前，必须做好充分准备。勘测方应预先确定无线局域网的需求，并向客户询问相关的问题。

这一章将介绍无线局域网现场勘测的前期准备工作、勘测开始之前应取得的文档以及勘测完成之后提交给客户的最终报告。本章最后还将对不同垂直市场实施无线现场勘测时需要考虑的因素做一概述。

15.1 无线局域网现场勘测概述

现场勘测是否必不可少？这个问题的答案非常明确：是的，现场勘测对于无线网络的部署极为重要。不同用户对现场勘测的要求并不相同。一家小型零售花店的店主希望在店中安装无线网络，这种现场勘测并不复杂，只需将家用(SOHO)无线网关置于花店的中央、调整其发射功率并确保连接成功即可。而对于大中型企业而言，实施现场勘测将耗费大量的时间和精力。在实际勘测开始之前，勘测方应与客户进行一次深入的现场勘测面谈，以确定客户的需求并帮助他们了解现场勘测的重要性。

现场勘测面谈时，应向询问客户相关的问题，以便勘测时选用合适的工具，并提高勘测效率。全面、细致的面谈与勘测能确保无线局域网满足各种预期的移动性、覆盖与容量要求，这对保证无线网络的良好运行极其重要。下面几节将对现场勘测面谈时需要认真考虑的问题做一介绍。

15.1.1 客户简报

自 1997 年 802.11 技术诞生以来，对无线网络的误解就始终存在。不少企业和个人对以太网已经相当熟悉，他们以为“即插即用”也是无线网络的铁律。如果你的公司或潜在客户计划部署无线网络，我们强烈建议与管理层接触，向他们简要介绍 802.11 无线网络，并解释现场勘测的重要性以及如何实施现场勘测。当然，和管理层阐述 OFDM 或 DCF 的工作原理并无必要，不过介绍无线局域网的利弊是个不错的主意。

如果终端用户对移动性的呼声甚高，或者企业正在考虑部署 VoWiFi 等应用，则企业很可能准备安装无线网络。那么，从简要介绍移动性的优点入手会收到良好的效果。

此外，向客户解释当前 802.11a/b/g/n 技术的带宽和吞吐量的局限性同样重要。企业用户已经习惯于有线网络 100Mbps 以上的全双工传输速度，加之厂商的炒作，人们往往认为 Wi-Fi 网络也会提供与有线网络接近的带宽和吞吐量。实际上，由于开销等因素，无线局域网的总吞吐量通常不会超过所宣称的数据率的一半，这一点应向管理层解释清楚。

本书前面曾经介绍过，如果数据率为 54Mbps，则总吞吐量只有数据率的 50%或更低。请告诉客户，802.11 通信采用半双工介质而非全双工共享介质传输数据。通常客户对 WLAN 带宽和吞吐量的概念都有一些误解。802.11n 无线局域网能解决日益增长的吞吐量需求，这可在一定程度上消除客户对带宽和吞吐量的担心。但是随着人们对网络速度的要求越来越高，

今后我们一定需要解释为何 802.11n 网络的速度仍然远远低于千兆以太网。幸运的是，IEEE 已经计划通过 802.11ac 和 802.11ad 修正案来大大提高通信速率。

此外，还应向客户介绍实施现场勘测的必要性。请用几句话概括射频信号的传输和衰减方式，以便管理层更好地了解射频现场勘测在确保合适的覆盖与提高系统性能方面的重要作用。讨论并比较 2.4 GHz 与 5 GHz 无线局域网同样有助于增强客户对无线网络和现场勘测的认识。如果能让管理层对 Wi-Fi 的基本知识以及现场勘测的重要性有所了解，则对接下来讨论技术性问题大有帮助。

15.1.2　业务需求

第一个应向客户提出的问题是：无线局域网的用途是什么？如果客户对无线网络的用途有一个完整的认识，则对更好地设计无线局域网大有帮助。例如，VoWiFi 网络与流量极大的数据网络相比，二者的设计要求存在天壤之别。如果无线局域网仅作为接入互联网的网关使用，则安全与分段要求又会有所不同。仓储环境(例如，使用 200 台手持扫描仪)与办公环境的无线网络部署几乎完全不同，医院与机场无线网络的业务需求同样差别很大。以下是应询问客户的一些业务需求问题：

哪些应用将在无线局域网中使用？　这个问题实际上包含容量与 QoS(服务质量)两个方面。仅有无线条码扫描仪的无线网络与交换大量图形文件的无线网络相比，后者显然比前者需要更多的带宽。如果要求无线网络支持语音或视频等时敏应用，则需要处理专有的 QoS 需求。应部署标准化的 802.11e/WMM 解决方案以满足相应的 QoS 需求。

哪些用户将使用无线局域网？　不同类型的用户对容量和性能的需求不同。可将用户按组织的需求进行隔离。不同的用户组可按 SSID、VLAN 甚至频率进行分类。安全角色的考虑对保护网络安全也是至关重要的。

哪些设备将连接到无线局域网？　可以将手持设备按种类或工作频率划分到不同的 VLAN。VoWiFi 电话始终应被划分到独立的一个 VLAN，以便与使用笔记本电脑的数据用户分开。不少手持设备目前仍然使用老式的 802.11b(HR-DSSS)无线接口，只能在 2.4GHz ISM 频段收发数据。设备的特性可能会影响到采用何种安全、频率、技术与数据率方案。

不同垂直市场的业务需求差别很大，本章后面将对此进行讨论。预先定义无线局域网的用途可以提高现场勘测的效率，对无线局域网的最终设计也至关重要。

15.1.3　容量与覆盖要求

在明确界定无线局域网的用途之后，下一步是询问客户各种相关的问题，以便进行现场勘测规划与无线网络设计。尽管无线局域网设计在现场勘测结束之后才算最终完成，不过我们建议根据客户的容量和覆盖要求开展初步设计。勘测人员应研究勘测区域的楼层平面图复印件，并询问客户需要射频覆盖的区域。一般而言，客户会要求无线网络覆盖所有区域。

例如，规划 VoWiFi 部署时，无线网络应覆盖每一个角落，因为用户可能在大楼的任何位置使用 VoWiFi 电话。如果无线局域网仅作为数据网络使用，则不一定需要地毯式覆盖。笔记本电脑数据用户是否需要在仓储区或户外庭院接入网络？前台人员是否需要使用一般

部署在库房中的手持条码扫描仪？上述这些问题的答案往往取决于无线局域网的用途。然而，如果能确定某些区域不需要射频覆盖，实际勘测时就可以节省客户的开支与勘测人员的时间。

考虑无线设备的增长

客户端的爆炸式增长通常意味着 RF 覆盖范围扩展到了大多数建筑物和场点。在过去，Wi-Fi 网络主要为便携式计算机用户提供接入，但近年来使用 Wi-Fi 移动设备快速增长。智能手机、平板电脑、扫描仪和其他许多移动互联网设备(Mobile Internet Devices，MID)都在使用 Wi-Fi。MID 是具备多媒体能力的移动设备，可以提供无线接口接入互联网。虽然 MID 最初的目的是供个人使用，但大多数员工已经在公司的工作场所使用 MID。员工现在也希望将自己的多个设备接入到企业的无线局域网。

根据大楼布局以及内部使用的建筑材料，可能需要预先规划某些区域使用的天线类型。例如，覆盖长廊或过道时，应采用室内半指向天线而非全向天线。实施站点勘测时，将对此进行确认或根据实际情况做相应调整。

现场勘测开始前，最容易被忽视的一个问题是确定无线局域网的容量需求。第 11 章曾介绍过，必须同时考虑覆盖与容量需求。如有必要，可以采用蜂窝调校以及(或者)Colocation(在相同地点放置不同信道的多颗 AP)解决客户的容量需求。为满足无线终端用户的性能要求，必须确定连接到每个接入点的平均用户数量。容量与诸多因素有关，包括前面提到的无线局域网的用途。在手持数据扫描仪占主导地位的仓储环境中，容量并非大问题。而在流量很大的数据无线局域网中，容量将是影响系统性能的重要因素。以下列出进行容量规划时需要考虑的一些因素。

数据应用 无线网络中运行的应用将直接影响到每个接入点可以支持的平均用户数量。那么，每个接入点平均容纳多少用户比较合适呢？需要再次强调的是，这个问题的答案完全取决于无线局域网的用途以及所运行的应用。但对一个普通的 802.11a/b/g/n 网络而言，每个接入点通常可以支持 30～35 个数据用户。很多 WLAN 厂商号称一个 802.11n 接入点可以支持 100 或 200 个用户，由于共享媒介的半双工特性，这个数字不可现实的。一个双频的 802.11n 接入点的每个无线射频卡连接 35 个用户用于普通应用(例如浏览网页)是比较现实的。

用户密度 以下是 3 个与用户有关的重要问题。第一，目前有多少用户需要无线接入？第二，今后有多少用户可能需要无线接入？这两个问题有助于勘测人员规划每个接入点足够支持的用户数量，并为今后的用户增长预留空间。第三个也是极为重要的问题是，用户分布在哪里？勘测方应与网络管理人员进行沟通，并在建筑物的楼层平面图中标出所有高密度用户区域。例如，一家公司的每间办公室可能只有一两名员工，而另一家公司将公共区划分为若干隔间，以容纳 30 名或更多的员工。其他高密度用户区域包括客服中心、教室和演讲厅。应考虑在工作时间(存在用户)而不是非工作时间(不存在用户)进行现场勘测，因为射频信号会因为人体的吸收而急剧衰减。

高峰/非高峰时段 务必询问客户高峰时段的分布，即确定何时的无线局域网负荷最大。例如，会议室可能只在每天或每月使用一次。此外，某些应用可能在某些时段频繁接入无线

局域网，从而导致网络负荷增大。高峰时段还包括员工交接班的时候。

现有的发射机　这并非指已经部署的 802.11 网络，而指微波炉、无线耳机、无绳电话、无线机械装置等干扰设备，这些设备极易被人们忽略。如果将服务台设置在安装有无线网络的一大片开放区域中，则容量是需要考虑的一个问题。然而，如果勘测人员不清楚客户的员工正在使用 2.4GHz 无线耳机或蓝牙键盘和鼠标，那么网络设计注定会失败。

移动(mobile)与移动性(mobility)　移动性既可以指具备移动的能力，也可以指拥有真正的移动性。我们以销售经理发言为例解释两种移动性的区别。销售经理发言后将文件保存在共享网络中，并希望在董事会会议室继续他的发言。经理拿起笔记本电脑，合上盖子，走到会议室，然后打开电脑，连接到无线网络并继续他的发言。这种情况属于具备移动的能力。虽然用户没有一直使用无线网络，但这并不妨碍他的工作。而拥有真正的移动性意味着用户在任何区域、任何时间都能连接到无线网络，这方面的典型例子如 VoWiFi 电话和仓库扫描应用。如前所述，大多数用户都使用某种类型的 MID(如智能手机)，因此，要求真正的移动性也就不难理解了。确定需要何种连接性不仅对排除现有网络的故障至关重要，对设计新网络也是必不可少的。

针对传统设备的向后兼容性　容量规划开始之前，务必了解以下事实：如果网络需要向后兼容传统客户端，则启用保护机制后吞吐量必然会降低。802.11n 网络的保护机制不会导致严重后果，但是针对 802.11b/g 网络来说就很严重。一般而言，大多数企业部署都要求提供对 802.11a/b/g 设备的兼容性，这些设备经常存在于手持设备、VoWiFi 电话或老式笔记本电脑中。许多手持 MID 设备(例如老式的条码枪)不具备 802.11n 网卡，就需要网络具有向后兼容性。

现场勘测开始前应仔细规划覆盖与容量需求，这有助于确定接入点功率设置、天线类型、蜂窝尺寸等设计参数。实施现场勘测时，应对以上参数进行验证，并根据实际情况调整覆盖与容量需求。

真实场景

接入点可以同时支持多少个 VoWiFi 电话呼叫？

蜂窝带宽、平均使用率和厂商规范等多种因素决定了接入点可以同时支持的 VoWiFi 电话呼叫数量。全球领先的 VoWiFi 电话厂商 Polycom 建议，每个 11Mbps 蜂窝支持的最大呼叫数量为 12 个。受带宽所限，建议每个 2Mbps 蜂窝支持最多 7 个呼叫。对一个典型的呼叫而言，速率为 11Mbps 时需要的带宽为接入点带宽的 4.5%，速率为 2Mbps 时需要的带宽为接入点带宽的 12%。不同厂商的接入点特性也会影响并行呼叫的数量，建议对此进行大规模测试。由于并非每个 VoWiFi 电话用户都会同时进行呼叫，预测 VoWiFi 流量时也可以采用概率模型。概率流量公式采用厄郎(Erlang)作为电信流量的单位，1 厄郎等于 1 小时内的电话流量。读者可从 www.erlang.com 下载在线 VoWiFi 厄郎流量计算器。

15.1.4　现有的无线网络

网络工程师在处理客户现有网络部署的问题时，往往会进行无线局域网现场勘测。根据

专业现场勘测公司的统计，多达 40%的业务涉及对现有无线局域网的排错。这通常意味着需要实施第二次现场勘测，然而，客户也可能根本未曾进行过现场勘测。

随着企业和个人对 802.11 技术的了解逐渐深入，上述比例将明显下降。遗憾的是，不少未经培训的客户只是将接入点草草安装了事，根本不对默认的功率和信道设置做任何调整。一般而言，如果网络性能下降或漫游出现问题，则必须进行现场勘测。同频干扰、多径效应以及其他干扰源往往会导致网络性能下降，而漫游问题可能与干扰有关，也可能因为缺乏足够的覆盖以及(或者)合适的蜂窝重叠。下面列出了进行修复性现场勘测前需要询问客户的一些问题。

当前的无线局域网目前存在哪些问题？ 询问客户以明确界定存在的问题。例如，这些问题是否与吞吐量有关？是否频繁掉线？漫游是否可以正常进行？大楼的哪些区域最经常出现问题？多久出现一次？是否采取了某些导致问题恶化的举动？

是否存在已知的射频干扰源？ 客户通常并不清楚这个问题的答案，不过询问一下也无妨。例如，周围是否有微波炉？客户是否使用无绳电话或无线耳机？客户是否使用蓝牙键盘或鼠标？勘测人员应参照上述问题进行频谱分析，这是唯一能确定周围是否存在影响今后 802.11 通信的手段。某些因素(如周围出现了新的无线运营商)可能会对客户网络的信道造成干扰。

是否存在已知的覆盖盲区？ 这个问题与漫游有关，某些区域可能并没有获得良好的覆盖。请记住，覆盖范围过小或过大都会导致漫游和连接出现问题。

是否能找到之前现场勘测的数据？ 客户很可能在部署无线网络前根本未曾进行过现场勘测。如果客户保留有上一次现场勘测的文档，则对解决网络目前存在的问题大有裨益。需要注意的是，除非之前采集的量化数据显示了 dBm 强度，否则应极为谨慎地对待之前的勘测报告。

目前安装了哪些设备？ 询问客户目前正在使用的设备类型(如 5GHz 802.11a 设备或 2.4GHz 802.11b/g 设备)与品牌。客户希望升级到 802.11n 吗？客户通常并不清楚这些问题的答案，因此勘测人员需要亲自确定所安装的设备类型和故障原因。此外，应检查设备的 SSID、WEP 或 WPA 密钥、信道、发射功率、固件版本等配置是否正确。很多问题往往并不复杂。例如，所有接入点被错误地配置为使用同一信道收发数据；如果缓冲区出现问题，只需将固件升级到最新版本即可。

根据现有无线网络排错的情况，往往需要实施第二次现场勘测，后者包括覆盖分析与频谱分析。实施新的现场勘测一般足以调整现有 802.11 设备的设置，然而最糟的情况是将当前无线局域网的设计全部推倒重来。请记住，一旦有必要进行第二次现场勘测，则所有为新勘测(即“绿地勘测”)准备的问题都要在第二次勘测开始之前向客户提出。如果无线网络的使用要求有所变化，重新进行网络设计或许是最好的选择。

15.1.5 基础架构连接性

前面的章节介绍过，无线局域网一般用于提供客户移动性，并作为接入当前有线网络基础架构的入口使用。勘测面谈时应询问客户相关的问题，以便无线局域网与当前的有线基础架构能完美地集成在一起。强烈建议勘测人员向客户索取一份有线网络拓扑图的复印件。

但是，基于安全方面考虑，客户或许不希望向外界透露其有线拓扑。勘测方可能需要签署一份保密协议，以便以集成商的身份合法地开展工作。务必确保勘测方具备签署协议的资质。

了解客户现有的网络拓扑同样有助于规划无线局域网分段并提出安全建议。无论是否能获得客户的网络拓扑，应重点考虑以下几方面问题，它们对于实现良好的基础架构连接性至关重要：

漫游　是否需要漫游？移动性是无线网络优越性的重要体现，因此大多数情况下漫游都是必不可少的。所有运行面向连接应用的设备都需要支持无缝漫游，部署手持设备以及(或者)VoWiFi 电话时必须能实现无缝漫游。随着智能手机和平板电脑的普及，多数用户希望具备移动性。

然而出乎意料的是，许多客户并不要求无线网络覆盖大楼的每个角落。前面曾介绍过，这种情况下，具备移动能力(being mobile)即可。某些网络管理员可能希望将一个或一组用户的漫游限制在某些区域。例如，销售团队的移动设备只能在 1 楼和 2 楼的接入点之间漫游，禁止漫游到 3 楼和 4 楼的接入点，而市场团队的移动设备可以在所有楼层的接入点之间漫游。因此网络需要分配不同的 SSID 或将其划分为不同的 VLAN。

另一个需要考虑的重要因素是，用户是否需要跨越三层边界进行漫游？如果要求客户端在子网之间漫游，应采用移动 IP(Mobile IP)或专有的三层漫游解决方案。应特别注意网络延时对 VoWiFi 设备漫游的影响。对现有网络而言，必须确定有线网络基础架构是否支持所有新的无线特性。例如，管理员希望为不同的 VLAN 配置 5 个 SSID，但是并没有检查客户的网络交换机是否支持使用 VLAN，这可能会造成很大麻烦。

配线室　配线室位于何处？预留安装接入点的位置是否在配线室下行电缆的 328ft(100m)范围之内？

天线结构　部署室外网络或点对点桥接应用时，可能需要安装某些附属结构以固定天线。建议向客户索取屋顶的建筑图纸，以确定结构梁和现有的屋顶渗透。由于天线的安装重量有所不同，勘测人员可能需要就此咨询结构工程师。

集线器/交换机　接入点是否通过 5 类线缆与集线器或受控交换机相连？配置 VLAN 时需要二层交换机。基于安全和性能方面的考虑，不建议将接入点与集线器相连。这是因为流量被广播到集线器的所有端口，如果接入点连接到集线器的某个端口，则任何经过接入点的流量也会被集线器的其他端口收到。交换机是否具有足够的端口？哪些人员负责 VLAN 的编程？

PoE(以太网供电)　如何为接入点供电？由于接入点一般安装在天花板上，可能需要采用 PoE 为接入点远程供电。客户往往没有部署 PoE 解决方案，这意味着需要追加投资。如果客户已经部署了 PoE 解决方案，勘测人员必须确定该解决方案是否兼容 802.3af(15.4W)、802.3at(25W)或是专用的 POE 解决方案。此外，客户采用端接式 PoE 还是中跨式 PoE？务必确保客户已有的 PoE 解决方案与勘测人员建议安装的系统相互兼容。如果需要安装 PoE 注入器，应保证有足够的电源插座，否则应确定负责安装插座的人员。安装 802.11n 接入点时，可能需要采用专有的 802.3at PoEat Plus 解决方案来支持所有 MIMO 无线设备。

分段　如何将无线局域网及其(或者)用户与有线网络区分开？整个无线网络是否位于一

个独立的 IP 子网？是否准备采用 VLAN？有无必配置访客 VLAN？是否准备采用防火墙或 VPN(虚拟专用网)进行分段？无线网络是否属于有线网络的自然延伸，并采用与有线基础架构相同的布线、编号与设计方案？所有这些问题的答案与客户的安全期望直接相关。

命名规则 客户是否有自己的一套线缆与基础架构设备命名规则？如果没有，是否需要为无线局域网制定一套这样的规则？

用户管理 勘测方应与客户讨论 RBAC、带宽限制与负载均衡等问题。客户是否部署有 AAA(认证、授权与结算)服务器？如果没有，是否需要部署 AAA 服务器？用户名与密码储存在何处？

基础架构管理 如何管理无线局域网远端接入点？是否需要采用中央管理解决方案？是否采用 SSH2、SNMP 或 HTTP/HTTPS 对设备进行管理？客户是否有一套标准的身份凭证以便登录设备的管理接口？

通过深入的面谈和沟通，勘测方可以获得客户对基础架构连接性要求的详细反馈，从而为进行全面、细致的现场勘测与无线网络设计打下坚实的基础。一个运行良好的无线网络得益于 75%的前期准备工作，而一个准备充分的前期工作是其他一切工作的基础。

15.1.6 安全期望

勘测方必须与网络管理人员进行沟通，以了解客户的安全期望。应讨论数据保密与加密方面的各种需求，并将所有 AAA 要求记录在案。此外，应确定客户是否计划部署防御非法接入点和其他无线攻击的 WIDS(无线入侵检测系统)或 WIPS(无线入侵防御系统)。三层 VPN 等安全解决方案采用的加密方式可能会额外增加无线局域网的开销，规划容量时应将这些开销考虑在内。EAP 认证过程耗时较长，这可能会影响到 VoWiFi 设备的漫游，对此应特别注意。

与客户详细讨论安全期望方面的要求之后，勘测方应参考这些信息制定一份详尽的安全建议，并在现场勘测结束后、网络部署开始前交给客户。制定安全建议时，应将健康保险流通与责任法案(HIPAA)、格雷姆-里奇-比利雷法案(Gramm-Leach-Bliley Act)、塞班斯法案(Sarbanes-Oxley Act)等相关的行业规范考虑进去。美国政府部门的无线网络部署必须严格遵循 FIPS 140-2 标准(Federal Information Processing Standards 140-2，联邦信息处理标准 140-2)，所有安全解决方案都要符合该标准。

上述问题有助于勘测方确定是否存在实现相关功能所需的硬件和软件，否则勘测方需要考虑如何满足客户的安全要求。

15.1.7 访客接入

Wi-Fi 技术在企业环境中已经得到了广泛应用，大部分公司目前都提供某种形式的无线访客接入方案。访客用户被分配一个访客 SSID，并通过相同的接入点与 WLAN 控制器连接到无线局域网。所不同的是，使用访客 SSID 的用户将被重定向到强制网络门户(captive portal)。访客强制网络门户有两个作用：

首先，登录界面强制访客用户阅读并同意一份免责声明；

其次，访客用户在登录之后可以接入互联网网关。为安全起见，所有使用访客 SSID 的用户只能连接到互联网网关。他们被划分到一个独立的访客 VLAN，以便与其他网络资源隔离开。部署访客无线局域网时，采用防火墙与带宽限制也极为普遍。另一个主题是由谁来管理 Guest 网络。

15.2　文档与报告

现场勘测面谈时(以及勘测开始之前)，务必向客户索取设施和网络的相关资料。勘测人员应起草一份现场勘测清单，并在实际勘测时严格加以遵守。勘测结束之后，勘测方需要向客户提交一份专业、全面的最终报告。如有必要，最终报告还可以包括附加报告以及对客户的建议。最终报告应详细描述如何安装与配置网络，以便客户了解勘测方的意图。

15.2.1　表格与客户文档

开始现场勘测面谈之前，务必向客户索取以下重要文档：

设计图　勘测方需要一份楼层布局平面图，以便和网络管理人员讨论覆盖与容量需求。前面曾经提到过，在研究楼层布局平面图时，应对容量与覆盖要求做一预先规划。勘测人员应将楼层平面图复制一份，以便实际勘测时记录射频测量的数据与硬件设备的布局。某些勘测软件可以导入楼层平面图，并自动记录勘测数据。由于勘测软件能大大简化最终报告的编辑，我们强烈推荐勘测人员使用这些软件。

如果客户无法提供大楼的设计图，勘测人员可以通过以下方式寻找设计图。大楼原来的建筑方可能仍然保留有设计图纸的复印件，市政厅、消防局等政府部门也保留有大量公共建筑与私人楼宇的楼层平面图。公司和商户设施通常会贴出消防逃生图，如果无法找到设计图，现场勘测时可使用这些按比例绘制的逃生图。最糟的情况是，勘测人员必须在坐标纸上手绘出楼层平面图。第 16 章将介绍能进行预测性容量与覆盖模拟的射频建模软件。设计图中标有建筑材料的详细信息，使用预测性分析软件时需要输入这些信息。矢量图格式(扩展名为.dwg 和.dwf)的设计图可以被导入预测性分析软件，也可以由勘测人员手工扫描进去。

图 15-1　地形图

地形图　规划室外现场勘测时需要地形图，后者也称为等高线图(contour map)。地形图显示了海拔、森林覆盖、河流位置和其他水体等地形信息，如图 15-1 所示。进行桥接计

算(如计算菲涅耳区)时，地形图也是必不可少的。

网络拓扑图 掌握客户目前的有线网络基础架构布局不仅能加快现场勘测的速度，也可以在设计阶段更好地规划无线局域网。计算机网络拓扑图标明了配线室位置、三层边界等重要信息。无线局域网拓扑可以被尽可能精确地集成到有线基础架构中。为安全起见，通常在有线网络和无线网络中使用 VLAN。强烈建议向客户索取网络拓扑图，以便更好地设计和集成无线局域网。出于安全等方面的考虑，一些机构或组织或许不希望向外界透露有线网络拓扑图。这种情况下，勘测方可能需要通过安全调查并且(或者)与客户签署保密协议，以便接触这些文档。

安全凭据 某些情况下，勘测人员需要获得相应的安全授权以进入勘测区域。在医院、政府机构以及许多商业设施的某些区域进行勘测时，勘测人员必须佩戴铭牌和通行证，甚至需要专人陪同。勘测开始之前，勘测方应与保安人员以及(或者)设施负责人进行接触，以确保不会违反任何安全规定。如果勘测人员到达勘测现场，却被告知由于没有安排陪同人员而无法开始工作，这将是一件非常尴尬的事情。无论客户的安全要求如何，勘测方应设法让网络管理员通知所有员工即将进行的现场勘测。

勘测人员应根据需要预先准备一份在面谈和实际勘测时使用文档或清单。下面列出了几类勘测清单：

面谈清单 应预先整理一份详细的清单，其中包括所有面谈时需要询问客户的问题。本章前面提到过的各种问题都应在清单上出现。

安装清单 不少勘测人员习惯将所有安装数据记录在楼层平面图上。此外，也可以在安装清单中详细列出硬件布局、接入点位置、天线类型与朝向、安装设备和电源等信息。

设备清单 为清晰起见，最好列出勘测时使用的所有硬件和软件工具。第 16 章将介绍室内与室外现场勘测所需的各种工具。

15.2.2 交付报告

现场勘测面谈与实际勘测完成之后，勘测方必须向客户提交一份最终报告。现场勘测时采集的信息经过编辑和汇总形成专业的技术报告，以供客户审阅。交付报告(deliverables)中应包含以下经过整理的信息：

目的陈述 描述无线局域网的用途(即客户要求与业务需求)。

频谱分析 确定潜在的干扰源。

射频覆盖分析 界定射频蜂窝的边界。

硬件布局与配置 提出对接入点布局、天线朝向、信道复用模式、功率设置、安装技术、电缆敷设等方面的建议。

性能分析 列出应用程序吞吐量测试结果，应用分析通常作为附在最终勘测报告中的可选分析报告。

第 16 章详细介绍了编辑各种必要的分析数据所需的方法和工具，所有信息经过汇总成为最终报告。由于勘测区域的规模差别很大，一份详细的现场勘测报告可能多达数百页。报告中通常包括一些勘测时使用数码相机拍摄的照片，从这些照片中可以了解接入点的布局、

勘测区域存在的射频干扰设备以及网络部署中可能遇到的问题(如坚硬的天花板或混凝土墙壁)。勘测人员还可以使用专业的现场勘测软件并按预设格式生成专业质量的报告。

本书的在线资源中包含一份专业现场勘测报告的样本。该报告由 Netrepid 提供，后者是一家提供专业无线服务的公司。报告的文件名是 sitesurvey.pdf。

15.2.3　附加报告

除提交现场勘测报告之外，勘测方也可以向客户提出其他建议，供客户在安装设备和部署安全解决方案时参考。一般而言，客户会聘用实施现场勘测的人员以及(或者)公司安装无线网络，不过客户也可能根据现场勘测报告提供的信息自行部署无线网络。无论哪一方负责安装工作，勘测方都应向客户提交现场勘测报告以及其他相关的建议和报告：

厂商建议　可供选择的企业无线厂商很多，强烈建议现场勘测与网络部署时采用同一家厂商生产的设备。尽管 IEEE 为确保设备的互操作性制定了很多标准，Wi-Fi 厂商仍然可能按照自己的标准生产设备。本书前面曾经介绍过，许多漫游机制都是厂商专有的。不同厂商的无线射频卡使用不同的 RSSI 阈值，这一点就足以说明勘测和安装时采用同一家厂商设备的重要性。不少现场勘测人员都备有多种厂商的工具包，以适应不同勘测的需要。例如，勘测人员可能同时准备了适合自治接入点架构和 WLAN 控制器架构部署的工具包。勘测公司可使用两家不同厂商生产的设备实施现场勘测，并由客户自行选择采用哪一种方案，这种情况并不鲜见。一般而言，双方通常会在勘测面谈时确定采用哪家厂商的设备进行勘测。

实施图纸　勘测方根据勘测时采集的数据向客户提供一份最终的设计图纸。大体来说，实施图纸是一种无线拓扑图，图中标明了接入点的安装位置以及无线网络与当前有线基础架构集成的方式。接入点布局、VLAN 与三层边界等信息均应在实施图纸上明确标出。

材料清单　除实施图纸外，勘测方应向客户提供一份详细的物料清单(BOM)，后者逐一列出了最终安装无线网络所需的各种硬件与软件。物料清单中应包括每种设备(接入点、网桥、无线交换机、天线、线缆、接头、避雷针等)的型号与数量。

项目进度与成本　勘测方应起草一份详细的日程安排，包括所有时间表、设备成本与人工成本。应特别注意交付时间、许可等项目关联性(schedule dependence)。

安全解决方案建议　本章前面曾经提到过，现场勘测面谈时应与客户讨论安全期望。勘测方将根据面谈结果制定一份完善的无线安全建议，建议中应包括认证、授权、结算、加密和分段等方面的要求。

无线安全策略建议　安全建议中还可以包括对企业无线安全策略的建议。如果客户尚未制定相应的无线安全策略，勘测方可能需要协助客户起草这样一份策略。

培训建议　部署新的无线解决方案时，最容易被忽视的一个方面是对相关人员的培训。强烈建议安排客户网络部门的员工参加无线管理与安全的培训课程，并安排所有终端用户参加简单的培训。

15.3 垂直市场

所有企业都有其自身的需求、问题与考虑，因而没有两次现场勘测是完全相同的。室内勘测并非现场勘测的全部，某些企业可能需要实施室外勘测。垂直市场(vertical market)是一类特殊的行业或商业群体，它们开发并推广类似的产品或服务。接下来将简要讨论在不同垂直市场中规划无线局域网时需要考虑的因素。

15.3.1 室外勘测

本书以及 CWNA 考试侧重于讨论和考查建立桥接链路时进行的室外现场勘测。室外桥接勘测时需要计算大量参数，包括菲涅耳区、地球曲率、自由空间路径损耗、链路预算与衰落容限。实施室外勘测也可以为提供一般性的室外无线接入扫除障碍，这种应用日益增多。随着无线 Mesh 网逐渐普及，室外无线接入将越来越普遍。进行这种室外现场勘测时，应准备带有无线 Mesh 路由器的工具包。

进行室外勘测时，必须考虑闪电、冰雪、热气、大风等天气状况。室外部署中需要首先考虑固定天线的设备。如图 15-2 所示，如果硬件设备不是专为室外部署而设计，则必须将其置于符合 NEMA(National Electrical Manufacturers Association，美国电气制造商协会)标准的机柜中，以抵御气候变化。NEMA 防水机箱的品种很多，包括加热、冷却和 PoE 接口。

在此鸣谢 NETREPID, INC 提供的本照片

图 15-2 NEMA 机箱

安全对于室外部署极为重要。应考虑聘用专业安装人员，或参加注册的发射塔攀登、安全与救援培训。

有关射频健康与安全课程的信息请参阅 www.sitesafe.com。在发射塔上作业的危险性较大，有关发射塔攀登与安全培训的信息请参阅 www.comtrainusa.com。

进行室外勘测时，应遵守各国监管机构制定的射频功率规定。使用发射塔前应联系相关的政府机构。市政部门可能制定了有关施工管理方面的法规，绝大多数情况下，勘测人员需要取得相应的许可才能开始工作。在美国，如果发射塔的高度在 200ft(61m)以上或者位于机场一定范围以内，勘测方必须获得 FCC(联邦通信委员会)与 FAA(联邦航空管理局)的同意。如果在屋顶安装高于 20ft(6m)的设备，也可能需要联系 FCC 与 FAA。其他国家和地区也有类似的高度限制，勘测方应咨询相关的射频监管与民航管理部门。

15.3.2　美观

安装无线设备时，美观是需要重点考虑的一个因素。大部分企业和商户不希望将无线硬件设备暴露给外界，而美观问题对于零售业与服务性行业(餐厅和酒店)尤其重要。需要与接触公众的行业都不希望 Wi-Fi 硬件设备出现在人们的视野中，或至少将其固定在某个不显眼的位置。WLAN 厂商一直在完善设计，使接入点与天线更加美观。一些厂商甚至将接入点伪装成烟雾报警器。为避免接入点暴露在外，可以将其置于类似图 15-3 所示的室内机柜中。请注意，大部分机箱都可以上锁，以防止昂贵的 Wi-Fi 硬件被盗。

在此鸣谢 NETREPID，INC 提供的本照片

图 15-3　室内机箱

15.3.3　政府

在政府机构实施无线现场勘测时，安全是不容忽视的一个问题。除了与客户在勘测面谈时讨论安全期望之外，勘测方应认真考虑各种规划的安全问题。包括美国军方在内的许多政府部门规定，所有无线解决方案必须符合 FIPS 140-2 标准。一些政府部门可能要求在某些时

段完全屏蔽或切断无线网络。在向其他国家出口设备时，务必确保没有违反出口管制规定。例如，美国禁止向某些国家出口 AES 加密技术。其他国家和地区也有类似的规定和海关要求。

绝大多数情况下，勘测人员在政府机构进行现场勘测之前必须取得相应的安全许可。勘测人员在工作时通常需要佩戴身份铭牌或通行证。在某些敏感区域进行勘测时，需要有专人陪同。

15.3.4 教育

与在政府机构进行现场勘测类似，在教育机构进行现场勘测之前通常也需要取得相应的安全许可。此外，接入点应置于上锁的机柜中以防失窃。不少学生和教职工在校园中使用苹果电脑，应部署支持 Macintosh 驱动程序的客户端无线射频卡。由于人流量较大，规划容量与覆盖时还应考虑高密度部署。校园中的大部分建筑都需要无线接入，建筑之间的连接一般通过桥接实现。某些老式的教育设施同时具备避难所的功能，这种环境会极大限制无线信号的传播。很多学校的建筑物为了保证教室间的隔音效果，隔墙材质选用煤渣砌块，而这种材料对 RF 信号衰减很大，通常需要每个教室部署一个 AP 来满足覆盖需求。

15.3.5 医疗

由于不少生物医学设备都使用 ISM 频段传输数据，对医疗环境中的无线局域网而言，最大的威胁来自生物医学设备的干扰。例如，手术室中使用的烧灼设备已经被证实会对无线网络造成干扰。同样，802.11 无线接口也可能干扰到生物医学设备。

勘测方应与负责维护与检修所有生物医学设备的部门进行交流。某些医院有专人负责跟踪并管理各种射频设备。

采用频谱分析仪进行全面彻底的频谱分析至关重要。建议对勘测区域进行多次扫描并比较各次扫描的结果，以最大限度发现潜在的干扰设备。由于 2.4GHz ISM 频段存在大量干扰源，为避免同频干扰，医疗机构往往将无线局域网设备部署在 5GHz 频段。通常密集部署也需要 5GHz 提供更多信道以避免同频干扰。不少医院的规模很大，因此现场勘测可能耗时较长。在实际勘测中，长廊、多楼层、防火安全门、反射材料、混凝土建筑、衬铅 X 光室、丝网安全玻璃都是可能遇到的材质。

勘测面谈与实际勘测时，应将医疗机构使用的各种应用考虑在内。例如，医生使用手持 PDA 传输 X 光片等大文件，医疗车载无线接口将患者数据返回给护理办公室。护理人员使用 VoWiFi 电话进行通话，医用 VoWiFi 部署目前已相当普遍。采用有源 802.11 RFID 标签的无线实时定位系统(Real-Time Location System，RTLS)广泛用于医院的资产管理跟踪。为不影响患者治疗，勘测人员通常需要取得相应的安全许可，并由专人陪同进入勘测区域。许多应用都是面向连接的，连接中断并不利于这些应用的运行。

15.3.6 热点

随着热点的应用日趋普及，许多商家都在寻求为顾客提供无线互联网接入。由于大部分

普通的公共热点目前仍然使用 2.4GHz 无线射频卡，因此无法提供 5GHz 接入。热点的尺寸通常较小，应采用低功率的单接入点以限制热点的射频覆盖区域。但机场、会议中心等大型场所已经开始提供无线接入，这些场所显然需要更多的接入点以覆盖更大范围。由于热点通常只采用强制门户对用户进行简单认证，因此其安全性不高。

15.3.7　零售业

零售业环境中一般存在大量潜在的 2.4GHz 干扰源。用于店内演示的无绳电话、婴儿监护器以及其他使用 ISM 频段收发数据的设备都会对无线局域网造成干扰。库存货架、货箱甚至产品本身都可能引起多径干扰。用户密度也是需要考虑的因素，也就是说，零售环境中的现场勘测应选择在购物旺季(如圣诞节期间)而不是淡季(如 1 月下旬)进行。

零售店中使用的无线应用包括用于数据采集与资产管理的手持扫描仪。收银机等 POS 设备也可能带有无线接口，这些设备一般采用老式的跳频技术，可能在 2.4GHz 频段(802.11b/g/n 网络)造成全频带干扰。条件允许的话，应考虑升级这些老式设备。对部署在零售业环境中的无线网络而言，覆盖比容量更重要，这是因为无线数据采集设备所需的带宽一般很少，且区域中的用户数量不多。

15.3.8　仓储业

某些初期的 802.11 技术曾用于仓储环境中的库存管理与数据采集。大部分手持设备目前仍然使用 2.4GHz 无线接口，因此仓储环境中的无线局域网通常以 2.4GHz 部署为主。规划仓储环境的无线网络时，覆盖是首要因素，而容量并非一个大问题。库房中堆满了金属货架和各种货物，它们会导致信号反射和多径干扰。大部分情况下都需要在仓储环境中使用定向天线。由于库房的屋顶较高，设备安装和信号覆盖可能是个问题。室内铁丝网围栏常用于隔离不同的区域，它们会导致 2.4GHz 射频信号发散，甚至完全阻塞信号。为保证手持设备移动时的连接性，必须实现无缝漫游。库房中经常使用快速移动的叉车装卸货物，这些叉车也可能安装了带有无线接口的计算设备。目前，不少传统的 802.11 FHSS 硬件设备以及(或者)900MHz 无线接口仍在仓储环境中使用。

在仓储环境中实施现场勘测时，库存量是需要重点考虑的因素之一。建议在高峰时段进行勘测，以获得最差情况时的覆盖数据。还要注意的是，库房可能是变化最频繁的射频环境。库存较低与较高时的射频环境差别很大，建议针对这两种情况进行勘测，以便比较结果。出货与进货时，可能需要相应调整射频功率电平。某些采用控制器架构的无线局域网可以监测无线网络运行状况，并根据环境变化相应调整每个接入点所用的信道与功率电平。但是，采用动态射频技术的 WLAN 控制器解决方案有时会使 VoWiFi 部署出现问题。

15.3.9　制造业

从多径干扰与覆盖规划上讲，制造业环境与仓储环境较为类似。但是在工厂进行现场勘测时会遇到许多其他场合不会遇到的问题，如人身安全和工会等。重型机械与遥控设备可能

会对勘测人员的安全构成威胁，而安装接入点时必须特别小心，以免被其他机械损坏。由于许多工厂使用有害的化学品和材料，勘测人员应穿着合适的防护服，并考虑安装经过加固的接入点或机柜。在进入科技制造厂的无尘室进行勘测之前，勘测人员应穿着防尘服，并遵守无尘室的相关规定。

许多工厂都要求雇员必须限期加入工会(即所谓的 union shop)。如有必要，勘测方应与工会代表进行接触，以确保所要进行的勘测不会违反工会的政策法规。

15.3.10 多租户大楼

在多租户大楼中进行现场勘测时遇到的最大问题是周围用户的无线局域网设备。办公楼中充斥着大量 2.4GHz 802.11b/g 无线网络。几乎可以肯定的是，所有其他用户的无线局域网都以最大功率工作。此外，某些设备使用非标准信道(如信道 2 和 8)进行通信，不同用户的设备之间很可能相互干扰。条件允许的话，应尽量考虑将无线局域网部署在 5GHz UNII 频段。

位于美国宾夕法尼亚州费城的 Netrepid 最近进行的一次现场勘测显示，某面积为 8000 平方英尺(743 m^2)的楼层中已经部署了 50 多个 2.4GHz 接入点，没有部署任何 5GHz 接入点。这种情况下，就无法在 2.4GHz ISM 频段部署任何新的无线网络了。

15.4 小结

本章介绍了实施无线现场勘测时的各项准备工作，以及勘测开始前必须了解的问题。勘测方应与客户进行现场勘测面谈，以帮助客户了解现场勘测的重要性并确定客户的无线需求。界定无线网络的商业用途能提高勘测的效率。勘测面谈时，应与客户讨论容量、覆盖与基础架构连接性规划等问题。面谈开始前，应向客户索取设计图或地形图等重要文档。请提前准备好面谈与安装清单，以便在勘测面谈和实际勘测时使用。各种垂直市场对现场勘测的要求不尽相同。勘测结束后，勘测方应向客户提交一份最终的勘测报告以及其他附加报告和建议。

15.5 考试要点

定义现场勘测面谈。解释无线现场勘测开始之前与客户进行面谈的重要性。理解面谈可以帮助客户了解勘测的基本知识，并明确界定客户的无线需求。

确认用于确定容量与覆盖需求的各种问题。理解正确进行容量与覆盖规划的重要性。定义规划射频蜂窝覆盖、带宽与吞吐量时需要考虑的各种问题。

解释与现有无线网络排错有关的各种问题。解释在实施第二次现场勘测之前，与现有无线局域网排错有关的各种问题。

定义与基础架构连接性有关的各种问题。理解为确保无线局域网与当前有线基础架构完美集成而必须询问客户的各种问题。

确认现场勘测文档与表格。确认现场勘测开始之前必须整理的各种文档，熟悉出现在最

终报告中的各种数据和记录。

解释垂直市场因素。理解各种垂直市场的业务需求，以及这些需求对现场勘测和最终部署的影响。

15.6　复习题

复习题的答案见附录 A。

1. You have been hired by the XYZ Company for a wireless site survey. Which statements best describe site survey best practices when choosing vendor equipment to be used during the survey? (Choose two answers.)

A. When conducting a wireless site survey with a WLAN switch, you should use both autonomous and lightweight access points.

B. When conducting a wireless site survey with autonomous access points, you should use different vendors' APs together.

C. When conducting a wireless site survey with a WLAN controller, you should use a WLAN controller and lightweight access points from the same vendor.

D. When conducting a wireless site survey with autonomous access points, you should use autonomous access points from the same vendor.

E. When a wireless site survey is conducted, proprietary security solutions are often implemented.

2. Name a unique consideration when deploying a wireless network in a hotel or other hospitality business. (Choose the best answer.)

A. Equipment theft

B. Aesthetics

C. Segmentation

D. Roaming

E. User management

3. Which of the following statements best describe security considerations during a wireless site survey? (Choose all that apply.)

A. Questions will be asked to define the customer's security expectations.

B. Wireless security recommendations will be made after the survey.

C. Recommendations about wireless security policies may also be made.

D. During the survey, both mutual authentication and encryption should be implemented.

4. The ACME Corporation has hired you to design a wireless network that will have data clients, VoWiFi phones, and access for guest users. The company wants the strongest security solution possible for the data clients and phones. Which design best fits the customer's requirements?

A. Create one wireless VLAN. Segment the data clients, VoWiFi phones, and guest users

from the wired network. Use an 802.1X/EAP authentication and CCMP/AES encryption for a wireless security.

B. Create three separate VLANs. Segment the data clients, VoWiFi phones, and guest users into three distinct VLANs. Use an 802.1X/EAP authentication and TKIP encryption for security in the data VLAN. Use WPA2-Personal in the voice VLAN. The guest VLAN will have no security other than possibly a captive portal.

C. Create three separate VLANs. Segment the data clients, VoWiFi phones, and guest users into three distinct VLANs. Use an 802.1X/EAP authentication with CCMP/AES encryption for security in the data VLAN. Use WPA2-Personal in the voice VLAN. The guest VLAN will have no security other than possibly a captive portal.

D. Create two separate VLANs. The data and voice clients will share one VLAN while the guest users will reside in another. Use an 802.1X/EAP authentication and CCMP/AES encryption for security in the data/voice VLAN. The guest VLAN will have no security other than possibly a captive portal.

5. What are some additional recommendations that can be made along with the final site survey report? (Choose all that apply.)

A. Training recommendations

B. Security recommendations

C. Coverage recommendations

D. Capacity recommendations

E. Roaming recommendations

6. What documents might be needed prior to performing an indoor site survey for a new wireless LAN? (Choose all that apply.)

A. Blueprints

B. Network topography map

C. Network topology map

D. Coverage map

E. Frequency map

7. What roaming issues should be discussed during an interview for a future VoWiFi network? (Choose all that apply.)

A. Layer 2 boundaries

B. Layer 3 boundaries

C. Layer 4 boundaries

D. Latency

E. Throughput

8. You have been hired by the Barry Corporation to conduct an indoor site survey. What information will be in the final site survey report that is delivered? (Choose all that apply.)

A. AP placement

B. Firewall settings

C. Router access control lists

D. Access point transmit power settings

E. Antenna orientation

9. The Kellum Corporation has hired you to troubleshoot an existing WLAN. The end users are reporting having difficulties when roaming. What are some of the possible causes? (Choose all that apply.)

A. Clients stations can only hear a –70dBm signal from one access point.

B. Clients stations hear a –70dBm signal from 30 access points.

C. The RF coverage cells are co-located.

D. There is interference from the cellular network.

E. There is interference from 2.4GHz portable phones.

10. After conducting a simple site survey in the office building where your company is located on the fifth floor, you have discovered that other businesses are also operating access points on nearby floors on channels 2 and 8. What is the best recommendation you will make to management about deploying a new WLAN for your company?

A. Install a 2.4GHz access point on channel 6 and use the highest available transmit power setting to overpower the WLANs of the other businesses.

B. Speak with the other businesses. Suggest that they use channels 1 and 6 at lower power settings. Install a 2.4GHz access point using channel 9.

C. Speak with the other businesses. Suggest that they use channels 1 and 11 at lower power settings. Install a 2.4GHz access point using channel 6.

D. Recommend installing a 5GHz access point.

E. Install a wireless intrusion prevention system (WIPS). Classify the other businesses' access points as interfering and implement de-authentication countermeasures.

11. The Harkins Corporation has hired you to make recommendations about a future wireless deployment that will require more than 300 access points to meet all coverage requirements. What is the most cost-efficient and practical recommendation in regard to providing electrical power to the access points?

A. Recommend that the customer replace older edge switches with new switches that have inline PoE.

B. Recommend that the customer replace the core switch with a new core switch that has inline PoE.

C. Recommend that the customer use single-port power injectors.

D. Recommend that the customer hire an electrician to install new electrical outlets.

12. The Chang Company has hired you to troubleshoot an existing legacy 802.11a/b/g WLAN. The end users are reporting having difficulties with throughput performance. What are some of the possible causes of the difficulties? (Choose all that apply.)

A. Multipath interference

B. Co-channel interference

C. Colocation interference

D. Inadequate capacity planning

E. Low client cards transmit power

13. What factors need to be considered when planning for capacity and coverage in a 5GHz WLAN? (Choose all that apply.)

A. Data applications

B. User density

C. Peak usage level

D. DFS channels

E. All of the above

14. During the interview process, which topics will be discussed so that the WLAN will integrate properly into the existing wired architecture?

A. PoE

B. Segmentation

C. User management

D. Infrastructure management

E. All of the above

15. The Jackson County Regional Hospital has hired you for a wireless site survey. Prior to the site survey, employees from which departments at the hospital should be consulted? (Choose all that apply.)

A. Network management

B. Biomedical department

C. Hospital security

D. Custodial department

E. Marketing department

16. Typically what are the biggest concerns when planning for a WLAN in a warehouse environment? (Choose all that apply.)

A. Capacity

B. Coverage

C. Security

D. Roaming

17. What type of hardware may be necessary when installing APs to be used for outdoor wireless coverage? (Choose all that apply.)

A. NEMA enclosure

B. Parabolic dish antennas

C. Patch antennas

D. Outdoor ruggedized core switch

18. What is a telecommunications unit of measurement of traffic equal to 1 hour of telephone traffic in 1 hour of time?

A. Ohm

B. dBm

C. Erlang

D. Call hour

E. Voltage Standing Wave Ratio

19. What additional documentation is usually provided along with the final site survey deliverable? (Choose all that apply.)

A. Bill of materials

B. Implementation diagrams

C. Network topology map

D. Project schedule and costs

E. Access point user manuals

20. The WonderPuppy Coffee Company has hired you to make recommendations about deploying wireless hotspots in 500 coffee shops across the country. What solutions might you recommend? (Choose all that apply.)

A. WPA2-Personal security solution

B. 802.11a/b/g/n access points at 100mW transmit power

C. 802.11a/b/g/n access points at 1 to 5mW transmit power

D. NEMA enclosures

E. Captive portal authentication

F. 802.1X/EAP security solution

第16章 现场勘测系统与设备

在该章中，你将学习以下内容：

- √ 现场勘测定义
  - 协议分析与频谱分析
  - 独立分析工具
  - 集成分析工具
  - 频谱分析
  - 覆盖分析
  - 接入点布局与配置
  - 应用分析
- √ 现场勘测工具
  - 室内现场勘测工具
  - 室外现场勘测工具
- √ 覆盖分析
  - 手工覆盖分析
  - 预测性覆盖分析
  - 自组无线局域网

第 15 章从管理角度介绍了无线现场勘测，并讨论了实际勘测开始之前需要收集的信息与制定的计划。这一章将从技术角度讨论无线现场勘测。一次完整的现场勘测应包括频谱分析与覆盖分析，以确保 802.11 网络的性能达到最佳状态。通过现场勘测可以确定 802.11 设备的布局和配置，这对于保证无线网络的良好运转至关重要。勘测人员应具备一定的射频信号传播知识，以便规划目前和今后使用的射频覆盖模式。墙壁、地板、屋门、管道、窗户、电梯、建筑、树木、山脉等许多因素都会直接影响到接入点或无线网桥的覆盖。本章将讨论如何实施现场勘测、现场勘测的种类以及勘测时所用的工具。不少勘测专业人员采用自己独特的技术方法进行现场勘测，如同艺术家按照各自的理解进行创作一样。本章将提供勘测所需的基础知识，以帮助读者成为无线现场勘测领域的毕加索。

16.1 现场勘测定义

大多数人将无线现场勘测定义为确定射频覆盖的过程。在早期无线网络中因为客户端很少，这种定义不存在任何问题。但是对于现在的无线网络勘测，不仅需要提供早期网络所需的覆盖需求，还经常需要为高密度部署的客户端提供高吞吐量需求。为达到这个目标，现场勘测不仅包括确定覆盖需求，还包括许多其他内容，例如搜索潜在的干扰源以及确定 802.11 硬件设备和相关部件合适的布局、安装与配置方式。接下来将介绍现场勘测中往往被忽视、却是必不可少的频谱分析要求。本章还将讨论经常遭到误解的覆盖分析要求。覆盖分析用于确定合适的接入点布局、接入点无线接口卡的发射功率以及正确的天线使用方法。

实施 802.11 无线现场勘测时，覆盖性能测试与应用测试是勘测项目的关键部分。只有在了解无线网络的用途之后才能选择相应的勘测工具，因此勘测面谈与规划至关重要。本章其余部分将介绍勘测人员需要准备的各种工具。

16.1.1 协议分析与频谱分析

十年前，无线网络进行规划设计，无需像现在那样考虑来自其他网络的干扰，因为无线设备比现在要少得多。随着大多数家庭和企业开始部署无线网络，加上在工作和家庭环境中存在其他许多无线设备，现在的现场勘测要求都需要针对环境进行协议分析和频谱分析。

使用基于 PC 的频谱分析仪比传统分析仪所需要了解的先进无线局域网技术知识要少得多，而且更简单。此外，因为频谱分析仪成本大幅降低，甚至中小企业都开始利用频谱分析仪。频谱分析仪将帮助确定是否有 802.11 设备或其他设备可能会干扰 WLAN。如果干扰是来自于 802.11 设备，可以使用协议分析仪进行进一步调查。

Wi-Fi 协议分析器可以检测 802.11 帧，分析 SSID、BSSID 信息以及数据包和安全信息，可以监视记录信号强度和信道信息，提供对当前 802.11 RF 环境概况。即使无线被加密，协议分析器仍然可以从 802.11 管理帧中提取信息片断。一些无线网络协议分析仪被专门设计用于现场勘测，这些分析仪把从测试 AP 收集的无线数据与平面图结合起来，并把 AP 信号整合到平面图上以期达到显示覆盖状况的目的。

Wi-Fi 频谱分析仪和协议分析仪可分为两类： 独立的和集成的。下面介绍这些两种类型

的系统之间的差异。

1. 独立分析工具

无线网卡和频谱分析仪在观察 RF 环境的方式稍有不同。无线网卡可以看到通过射频媒介的帧和经过调制的比特。协议分析仪对无线网卡接收到的数据进行分析，而频谱分析仪监测的是射频信号本身。

频谱分析仪是一件运行在 PC 上的昂贵测试设备或软件，它需要连接一个 USB 频谱适配器，可以监测到特定频率范围内的射频信号。因为无线网络接收器和频谱分析仪接收器都是独立设备，它们监测到不同类别的信息，各自执行独立的任务。

2. 集成分析工具

频谱分析仪不仅需要了解和识别各种射频干扰特征，还要评估对无线局域网的干扰影响。把频谱分析集成到 Wi-Fi 网络进行 802.11 分析是一个亮点，这可能是具备这个特性的厂商与竞争对手竞争的秘密武器。通过把原始射频信息与无线网卡获取的数据关联起来，可以更好地了解不同情况对无线网络的影响。可想而知，这种功能不会出现在成本较低的产品中。

许多频谱和协议分析仪厂商正在进行频谱分析卡和无线网卡一体化集成。应根据自己的需要确定恰当的集成级别你对射频基础知识和 802.11 基础知识了解得越少，就越需要从内置这些集成产品的专家分析软件中获取需要的信息。

16.1.2　频谱分析

进行覆盖分析勘测之前，必须确定潜在的干扰源。遗憾的是，由于硬件频谱分析仪价格昂贵，不少现场勘测只能跳过频谱分析。但随着这几年基于 PC 的频谱分析仪价格不断下降，频谱分析已经成了多数现场勘测的规范要求之一。

频谱分析仪是一种用于测量电磁信号幅度与频率的频域测量设备，售价高达 100 000 美元，许多企业无法负担如此高昂的费用。不过一些公司为 802.11 现场勘测频谱分析专门开发了基于硬件和软件的解决方案，这使得成本大幅降低。图 16-1 显示了一种基于 PC 的频谱分析仪，它使用 USB 适配器，可执行 2.4GHz 和 5GHz 的频谱分析。

图 16-1　Wi-Spy DBx 2.4GHz 和 5GHz 基于 PC 的频谱分析仪

为进行全面、详尽的 802.11 频谱分析勘测，频谱分析仪必须能扫描 2.4GHz ISM 与 5GHz UNII 频段。一些公司目前推出了专门针对 802.11 现场勘测的软件解决方案，这种软件解决方案采用特殊分析卡或 USB 适配器，可以正确识别微波炉和无绳电话等设备发出的能量脉冲。但是，选择软件解决方案时必须慎重。某些解决方案仅能测量 802.11 设备发出的脉冲，它们并非真正的频谱分析仪，而后者可以拾取任何发射源的射频能量。

为什么频谱分析在现场勘测中是必不可少的呢？当 2.4GHz ISM 或 5GHz UNII 频段上的背景噪声级别高于-85dBm 时，无线网络的性能将受到严重影响。噪声会破坏 802.11 数据，通常会出现如下情况：

- 导致循环冗余校验(CRC)失败。此时，接收方 802.11 无线接口不会向发送方 802.11 无线接口返回确认帧。
- 如果发送方未收到确认帧，它将认为单播帧传输失败并重发该帧。
- 如果无线局域网由于微波炉等设备的干扰导致重传率超过 10%，网络性能或吞吐量将严重下降。

通常来说，大部分 802.11 数据应用可以承受最高 10%的第二层重传比率，网络性能不会受到太大影响。然而，VoIP 等时敏应用要求上层 IP 包的丢包率不能超过 2%。对 VoWiFi 网络而言，第二层重传率应控制在 5%以下，以确保 VoIP 包的及时交付。

802.11 无线接口也可能因为干扰设备的阻碍而无法通信。当其他射频源以高功率向外发射信号时，802.11 无线接口将在空闲信道评估(CCA)阶段侦听到媒介中存在射频能量，并推迟自己的传输。如果干扰源持续向外发射信号，802.11 无线接口必须一直推迟传输以等待媒介空闲。换句话说，用户的 802.11 客户端和接入点无线接口将因强射频干扰源的阻碍而完全无法传输数据。

建议在所有频段(特别是 2.4GHz ISM 频段)实施频谱分析，这是因为 2.4GHz～2.5GHz ISM 频段极其拥挤。以下是 2.4GHz ISM 频段存在的潜在干扰源：

- 微波炉
- 2.4GHz DSSS/FHSS 无绳电话
- 荧光灯
- 2.4GHz 摄像机
- 升降电动机
- 烧灼设备
- 等离子切割机
- 蓝牙无线接口
- 附近的 2.4GHz 无线局域网(802.11、802.11b、802.11g 或 802.11n)

现场勘测面谈时必须首先确定所有微波炉的位置。微波炉的功率一般为 800W～1000W。尽管微波炉的炉腔经过屏蔽，不过随着时间的推移，微波炉仍然可能出现微波泄露。与许多零售店销售的折价微波炉相比，商用微波炉的屏蔽效果更好。虽然大小为-40dBm(10^{-4} mW)的接收信号仅相当于 1mW 的万分之一，但是这对 802.11 通信而言已属极强。一台 1000W 的微波炉即使存在百万分之一的泄露，也会对 802.11 无线接口造成干扰。

图 16-2 显示了一种微波炉的频谱图，注意其工作频率位于 2.4GHz ISM 频段的正中。需

要注意的是，某些微波炉可能会干扰到整个 2.4GHz 频段。勘测人员还应检查客服中心、前台或其他员工是否在使用蓝牙鼠标、键盘或耳机，因为蓝牙设备也会对无线局域网造成很大的干扰。

图 16-2　微波炉频谱图

由于 2.4GHz ISM 频段极拥挤，不少企业部署已开始转而采用工作在 5GHz UNII 频段的 802.11a 设备。5GHz UNII 频段目前相对空闲且具有更多的信道复用模式，因此将企业无线局域网部署在该频段不失为一个明智的选择。5GHz 频段的非 802.11 干扰设备较少，可能干扰到用户网络的其他 802.11a 网络也不多。虽然 5GHz 频段的干扰远远少于 2.4GHz 频段，但是这种情况今后可能会发生改变。如同所有人从 900MHz 频段转向 2.4GHz 频段以避免干扰一样，“频段跳变”导致的拥挤最终也会出现在 5GHz 频段。

尽管 5GHz 的无线网络越来越多，但仍有许多 Wi-Fi 电话和平板电脑只支持 2.4GHz。为兼容这些设备，企业大多部署双频 AP，同时支持 2.4GHz 和 5GHz，在提供更快更强的 5GHz 网络接入能力的同时也兼容 2.4GHz 网络。以下是目前 5GHz UNII 频段存在的潜在干扰源：

- 5GHz 无绳电话
- 雷达
- 周边传感器(perimeter sensor)
- 数字卫星
- 附近的 5GHz 无线局域网
- 室外 5GHz 无线网桥

802.11-2007 标准定义了 DFS(动态频率选择)与 TPC(传输功率控制)机制，以避免 5GHz 无线局域网干扰到 5GHz 雷达系统。前面的章节介绍过，兼容 802.11h 的无线接口必须检测 5GHz 频段是否存在雷达传输。如果发现正在工作的雷达系统，802.11 设备必须停止自己的

传输以避免干扰。在规划部署无线局域网的区域实施现场勘测时，使用 5GHz 频谱分析仪有助于勘测人员确定该区域是否存在雷达传输。

虽然许多设备都可能干扰到 2.4GHz 和 5GHz 无线局域网，但是最普遍的一种干扰来自于其他无线局域网。附近无线局域网发射的高功率信号是一个非常让人头疼的问题，这在多租户大楼环境中尤其严重。勘测人员或客户可能需要与附近的用户进行协商，以说服他们将接入点的传输功率调低，并使用不会干扰到其他接入点的信道。需要再次强调的是，由于许多无线局域网设备都部署在 2.4GHz 频段，不少企业目前已转而采用 5GHz 无线局域网解决方案。

确定干扰源后，最简单可靠的方法是将其彻底消除。如果微波炉干扰到无线网络，可以考虑购买售价更高但干扰更小的商用微波炉。务必使 2.4GHz 无绳电话等可能引起干扰的设备远离无线局域网，并严格执行限制这些设备使用的政策。5.8GHz 无绳电话使用 5.8GHz ISM 频段进行通信，该频段(5.725GHz～5.875GHz)与 UNII-3 频段(5.725GHz～5.825GHz)有所重叠。因此，室内用 5.8GHz 电话会干扰到工作在 UNII-3 频段的 5 GHz 无线接口。

如果无法彻底消除 2.4GHz ISM 频段存在的干扰设备，则应考虑转向干扰较少的 5GHz UNII 频段。如前所述，VoWiFi 网络的第二层重传率应控制在 5%以下，为此必须在 2.4GHz ISM 频段实施全面、彻底的频谱分析。早期的 VoWiFi 电话采用 HR-DSSS 技术，只能使用极为拥挤的 2.4GHz ISM 频段。一些无线局域网厂商目前推出了采用 OFDM 技术的 VoWiFi 电话，后者可部署在干扰较少的 5GHz UNII 频段。无论企业无线局域网需要支持数据应用、语音应用或是同时支持两种应用，都必须实施全面彻底的频谱分析。

确定采用何种频段之前，请务必熟悉客户设备的特性。如果所有或一部分客户设备只能使用 2.4GHz 频段传输数据，则该频段将是网络部署的唯一选择，勘测人员需要考虑如何在这种环境中规划和设计无线局域网。

16.1.3 覆盖分析

频谱分析现场勘测结束之后，接下来需要确定合适的 802.11 射频覆盖范围，这是极为重要的一步。勘测方应在实际勘测开始之前与客户讨论并确定容量和覆盖要求。如果某些勘测区域的用户密度较大或应用对带宽的需求较大，则可能需要在这些区域中规划较小的蜂窝或进行 Co-Location 处理。

确定所有容量与覆盖要求之后必须进行射频测量，以确保这些要求得到满足，并确定接入点与天线合适的布局与配置。勘测人员应使用接收信号强度测量工具进行正确的覆盖分析。这种测量工具既可以是无线网卡客户软件自带的接收信号强度计，也可以是昂贵、复杂的现场勘测软件包。前者的功能通常是有限的，只适用于小型部署，或用于局部位置检查。稍后将详细介绍所有测量工具。

如何进行正确的覆盖分析是业内人士经常争论的一个问题。尽管每个人的方法不同，不过本书将尝试对覆盖分析的基本程序做一介绍。不少勘测人员在勘测时所犯的第一个错误往往是没有改变接入点无线接口的默认功率设置，仍然使接入点以最大功率工作。对一个 100mW 的 2.4GHz 无线射频卡而言，其发射功率通常已足以干扰到其他接入点的覆盖蜂窝。此外，许多

传统客户端无线网卡的最大发射功率仅为 30mW，如果这些客户端位于 100mW 接入点覆盖蜂窝的边缘，其射频信号可能无法被接入点成功接收。现场勘测时，应首先将 2.4GHz 接入点的发射功率设置为 30mW，勘测结束后再根据实际覆盖情况提高或降低发射功率。

在进行现场勘测的覆盖分析设计时，通常建议的最佳实践是-70dBm 或更强的接收的信号，这个强度远远高于底噪强度。当进行 VoWiFi 设计时，则建议-67dBm 或更强的信号强度。

覆盖分析现场勘测中最棘手的问题往往是确定第一个接入点的位置以及第一个射频蜂窝的覆盖范围。下面对此做一概述，图 16-3 详细显示了这一过程：

图 16-3　第一个覆盖蜂窝

(1) 将参考接入点置于大楼的一角，并设置其发射功率为 30mW。

(2) 从参考接入点开始，沿对角线向大楼的中央走动，直到接收信号强度降为-70dBm，此处为放置第一个接入点的位置。

(3) 将第一个接入点临时固定在此处，然后在大楼内走动，并找出所有-70dBm 端点，这些端点也称为蜂窝边界或蜂窝边缘。

(4) 根据第一个覆盖蜂窝的形状和尺寸，调整功率设置并且(或者)将第一个接入点移走。一次正确的覆盖分析勘测可能需要进行反复不断的尝试。

确定第一个覆盖蜂窝及其边界之后，接下来需要找出放置第二个接入点的位置。与确定第一个接入点的位置类似，可确定第二个接入点的位置。

考虑第一个接入点的蜂窝边缘，信号是-70dBm，将此作为初始起点，就像将大楼一角作为初始起点一样，然后执行以下操作：

图 16-4　第二个覆盖蜂窝

(1) 以第一个接入点(信号功率为 30mW)为起点，沿大楼一侧平行走动，直到信号接收信号强度降为-70dBm(此处为第一个接入点覆盖蜂窝的边界)。将参考接入点置于此处，如图 16-4 所示。

(2) 从参考接入点开始，沿大楼一侧平行走动，直到接收信号强度降低为-70dBm。

(3) 如果要求蜂窝之间存在重叠，则第二个接入点应略微靠近参考接入点，即位于参考接入点与最远点之间连线的 15%～20%处(根据蜂窝重叠要求而定)。

(4) 将第二个接入点临时固定在该位置。

(5) 并继续在大楼内走动，直到找出所有-70dBm 端点(蜂窝边界)。

(6) 类似地，根据第一个覆盖蜂窝的形状和尺寸，调整功率设置并且(或者)将第二个接入

点移走。

请注意，蜂窝之间的重叠区域不应过大，以免因为频繁的漫游导致网络性能下降。勘测人员应根据大楼结构以及各种建筑材料对信号的衰减程度调整各接入点的位置，以获得合适的蜂窝重叠。在确定第二个接入点的位置及其蜂窝边界之后，可以采用类似的方法找出其他接入点的位置。接下来的勘测仅仅是不断重复上述过程，直到确定大楼内所有的覆盖蜂窝。

在 WLAN 厂商的设计指南和白皮书中规定基于漫游的目的常常采用 15%～30%蜂窝覆盖。然而，没有方法来测量覆盖蜂窝的重叠程度。蜂窝覆盖重叠的程度实际上是从无线客户端的角度来衡量的。正确的现场勘测应该要确保客户端总是处于多个接入点的覆盖范围内。换句话说，每个无线客户端站需要听到一个主要的在特定 RSSI 强度的接入点和另一个不同 RSSI 信号强度的备份接入点。通常大多数厂商要求-70dBm 的接收信号阈值以达到较高的通信数据率。因此，客户端需要看到至少两个信号强度在-70dBm 接入点，以便客户端在必要的情况下可以漫游。

以下是现场勘测时需要测量的蜂窝边界参数：

- 接收信号强度(单位：dBm)，也称为接收信号级别(RSL)
- 噪声级别(单位：dBm)
- 信噪比(单位：dB)

现场勘测时测量的接收信号强度通常与无线局域网的用途有关。如果无线局域网只用于提供覆盖而容量无关紧要，那么重叠蜂窝边界的接收信号强度在-73dBm 也是可以接受的。如果吞吐量和容量是需要考虑的问题，建议接收信号强度至少应达到-70dBm。VoWiFi 网络可能要求-67dBm 或以上的信号强度。信噪比是通信中的重要指标之一，如果接收信号过于接近背景噪声，则会导致数据损坏，从而增加重传次数。如图 16-5 所示，信噪比是接收信号与背景噪声之间的差值，以 dB 表示。许多厂商建议，数据网络的信噪比至少应达到 18dB，而语音网络的信噪比至少应达到 25dB。

SNR 信噪比测试要求

请注意，信噪比要求设备能够测量背景噪音的 RF 能量。而 802.11 无线网卡不是频谱分析仪，尽管其可以极快速率发送和接收数据，但却无法感知周边的原始 RF 信号强度。Wi-Fi 网卡可以通过解码的方法得知来自其他 Wi-Fi 网卡的调制后的比特，却无法测量背景噪音。Wi-Fi 网卡可以测量接收信号强度，但是真正可以测试那些无法解码的 RF 能量的设备只能是频谱分析仪。因此测量 SNR 的最佳工具是频谱分析仪。

图 16-5 信噪比

有些现场勘测专业人员更习惯使用数据率而非接收信号强度来确定蜂窝边界。问题在于，厂商定义的 RSSI(接收信号强度指示器)阈值各不相同，无线接口卡的数据速率会因 RSSI 的不同而变化。当然，如果企业计划在部署 WLAN 时仅采用一家厂商生产的无线接口，则使用该厂商定义的 RSSI 阈值进行蜂窝设计也未尝不可。由于数据速率和 RSSI 阈值依赖于厂商，为增强通用性，现场勘测时应考虑使用接收信号强度。采用数据率或者专有的信号强度测量阈值的现场勘测无法在不同厂商的产品之间进行。当数据无线局域网采用同一家厂商的高灵敏无线接口卡时，应达到的最低接收信号强度与信噪比如表 16-1 所示。

表 16-1　数据无线局域网蜂窝：厂商推荐值

数 据 速 率	最低接收信号强度	最低信噪比
54Mbps	-71dBm	25dB
36Mbps	-73dBm	18dB
24Mbps	-77dBm	12dB
12/11Mbps	-82dBm	10dB
6/5.5Mbps	-89dBm	8dB
2Mbps	-91dBm	6dB
1Mbps	-94dBm	4dB

大部分 VoWiFi 厂商要求接收信号强度在-67dBm 以上。为保证足够的衰落容限，VoWiFi 网络覆盖蜂窝的接收信号强度应达到-60dBm。建议 VoWiFi 网络的信噪比至少达到 25dB，蜂窝之间保持 15%～20%的重叠，且同频的 AP 信号强度应相隔 20dB 以上。图 16-6 显示了推荐采用的 VoWiFi 网络覆盖模式。

图 16-6　建议采用的 VoWiFi 覆盖蜂窝

尽管示意图中经常将射频覆盖蜂窝表示为标准、对称的圆形，不过实际情况并非如此。覆盖蜂窝的边界往往是不规则的，读者可以想象下海星的形状或巴勃罗·毕加索的抽象画作。

16.1.4　接入点布局与配置

上一节介绍过，覆盖分析用于确定合适的接入点布局与功率设置。进行现场勘测时，勘

测人员需要在楼层平面图的复印件上记录所有蜂窝边界的测量数据、每个接入点的精确位置、接入点无线接口卡的传输功率级别以及所有配线室的位置。需要注意的是，受 5 类线缆的距离所限，所有接入点都必须位于配线室电缆敷设路径的 100m 范围(包括垂直方向和水平方向)之内。

覆盖分析中经常会忽视半定向天线的使用。不少无线局域网部署都采用厂商默认的低增益全向天线，其增益一般为 2.14dBi。由于建筑物的结构千差万别，其中往往存在长廊和过道，因此使用室内半定向天线更合适。在尚未采用 802.11n 的仓库更容易受到多径现象的影响。如果勘测区域存在金属架、文件柜和金属储物柜，则最好使用定向天线以减少反射。

使用室内半定向天线同样能减少反射并降低多径现象的不利影响，从而防止时延扩展和码间干扰(ISI)破坏数据。数据传输的成功率越高，重传的可能性越低，无线局域网的性能越好。在布满长廊和金属货架的仓库中使用半定向天线时，可以参考图 16-7 所示的布局。

勘测人员应准备各种全向天线和半定向天线，以满足不同勘测的需要。在大部分建筑物中实施勘测时，将低增益全向天线与室内半定向天线配合使用可以获得最佳的覆盖效果，如图 16-8 所示。

图 16-7 半定向天线的正确使用方式

图 16-8 全向天线与半定向天线配合使用

使用半定向天线时仍然需记录接收信号强度、信噪比、噪声级别等参数，以便确定覆盖边界。半定向天线的实际覆盖范围应与产品手册提供的辐射图非常接近。勘测时，只需沿天线覆盖的定向路径以及定向路径的边缘记录信号的测量值即可。

16.1.5　应用分析

在 802.11 无线现场勘测中，频谱分析与覆盖分析是强制性的，直到现在，应用分析仍然属于可选的勘测项目。容量规划需要同时考虑用户容量与带宽容量，它已经成为现场勘测的重要部分。实施覆盖分析时，应考虑规划蜂窝调校或 co-location。

厂商开发了用于无线局域网应用压力测试的工具，这种工具通常在网络部署阶段使用，也可以在勘测即将结束时使用。一些公司推出了能模拟多台并行虚拟无线客户端的 802.11a/b/g/n 多终端模拟硬件。这种模拟器不仅可为不同虚拟客户端配置独立的安全特性，也可对漫游性能进行测试，还能配合其他设备对数以百计的协议进行仿真，并通过虚拟客户端产生双向流量。这种多终端模拟器特别适合模拟并测试需要支持数据和语音应用的无线网络。

16.2　现场勘测工具

无线网络部署开始之前，勘测人员应准备好相应的勘测工具及辅助设备。信号测量软件无疑是现场勘测的主要工具，它与勘测人员的无线客户卡相连，用于实施信号分析。虽然互联网上有不少预打包的现场勘测工具包出售，但是大部分勘测人员仍然习惯根据自己的需要选取工具。室内勘测与室外勘测本质上差别很大，这一节将分别介绍两种勘测所用的工具。

16.2.1　室内现场勘测工具

前面曾经介绍过，频谱分析仪用于确定潜在干扰源的位置。而接收信号强度测量工具在覆盖分析中扮演了主要角色，它既可以是无线网卡客户软件自带的接收信号强度计，也可以是昂贵、复杂的现场勘测软件包。此外，实际勘测时还要用到许多辅助工具。下面列出了室内现场勘测可能用到的一些工具：

频谱分析仪　用于频谱分析。

设计图　大楼的设计图或楼层平面图用于绘制射频覆盖图并记录射频测量数据。勘测人员可以使用 CAD 软件查看和编辑电子设计图。

信号强度测量软件　用于射频覆盖分析。

802.11 客户端网卡　与信号测量软件配合使用。最好在勘测和部署阶段采用同一家厂商生产的客户端接口卡。

接入点　至少准备一个接入点，可能的话，最好准备两个接入点。现场勘测时，自治接入点可以作为独立的设备使用，而轻量接入点需要与 WLAN 控制器配合使用。

WLAN 控制器　大部分无线局域网部署目前都采用集中式架构，该架构由一台 WLAN 控制器以及若干轻量接入点构成。多数厂商的轻量接入点都要通过隧道才能与 WLAN 控制器进行通信。大部分 WLAN 控制器厂商开发了适合分公司和远端办公室使用的小型控制器，其自重仅为 2lb(0.9kg)。与自重达 30lb(13.6kg)的核心 WLAN 控制器相比，这种小型远端 WLAN 控制器在现场勘测中更便于操作。

电池组 电池组是现场勘测中的重要配件。当现场勘测工程师需要临时固定接入点时，使用电池组可以免去拉线供电的麻烦。电池组不仅能为接入点供电，而且降低了拉线供电的危险。勘测人员可以便捷地将使用电池组供电的接入点移到其他位置。

望远镜 室内勘测使用望远镜似乎有些难以理解，不过在大型仓库和会议中心实施勘测时就能体现出望远镜的重要性。此外，检查天花板上方的压力通风系统(plenum space)时也需要借助望远镜。

手电筒 有时光线太暗，在黑暗的角落或天花板处，大功率的定向手电筒会带来方便。

对讲机或移动电话 在办公环境中进行现场勘测时，勘测人员需要尽量将声音放低，以免影响他人的工作。务必不要在房间里叫喊，通话时应使用对讲机或手机。请记住，由于射频信号在空间中的传播是立体的，因此勘测人员经常需要在不同的楼层中测试接收信号。

天线 进行室内 802.11 现场勘测时，必须准备各种室内全向天线与单向天线。

临时固定工具 现场勘测时，勘测人员经常需要将接入点临时固定在天花板上，一般采用橡皮筋、塑料绳或高质量的老式胶带完成这项工作。此外，也可将接入点固定在三脚架的拉杆上，如图 16-9 所示。由于三脚架便于携带，这可以省去临时固定接入点的麻烦。

图 16-9 802.11 现场勘测三脚架

数码相机 用于拍摄接入点布局的精确位置。无论哪一方负责随后的安装，这些照片都能提供直观的参考。照片上的拍摄日期和时间也有助于日后查看照片。

测轮或激光测量仪 用于确保接入点的实际安装位置在配线室电缆敷设路径的 100m 范围之内。请记住，100m 电缆敷设路径还包括连接增压室的 5 类线缆的长度。测轮或激光测量仪用于测量接入点与配线室之间的距离。由于激光设备的功能经常不尽如人意，使用测轮往往是一个更好的选择。

着色电工胶带 大家可能还记得在格林童话《汉赛尔与格雷特》(Hansel and Gretel)中，主人公用面包屑标记出回家的道路。着色胶带相当于现场勘测中的“面包屑”，它用于标记接入点的预定安装位置。现场勘测时，勘测人员应在需要临时固定接入点的地方留下一小块着色电工胶带，以便随后的安装人员辨认。此外，还可以使用不同的颜色区分信道。例如，采用红色胶带标识信道 1，绿色胶带标识信道 6，蓝色胶带标识信道 11。

梯子或叉车 将接入点临时固定在天花板上时，可能需要使用梯子以及(或者)叉车。

我们强烈建议勘测和部署时使用同一种 802.11 接入点。这是因为厂商对 RSSI 的定义和实现各不相同，不同厂商生产的设备之间可能互不兼容。覆盖分析勘测与网络部署时使用完全不同的接入点并不是一个明智的选择。许多著名的现场勘测公司都有针对不同厂商的勘测方案和工具，以满足客户的各种需求。

16.2.2　室外现场勘测工具

上一章曾经提到过，本书以及 CWNA 考试侧重于讨论和考查建立桥接链路时进行的室外现场勘测。另一方面，实施室外勘测也可以为提供一般性的室外无线接入扫除障碍，这种应用日益增多。室外接入点或网状路由器通常用于在室外环境中提供用户接入，二者也是室外现场勘测使用的主要工具。室外与室内 802.11 现场勘测所用的设备基本相同，不过室外勘测还可能配备用于记录经纬度坐标的 GPS。需要注意的是，虽然室外 802.11 部署也可以提供客户接入，但是室外现场勘测通常都是为监控摄像头或者电子监控设备提供无线桥接或者无线回传而言的。无线网桥位于分布层，它以无线方式将两个或多个有线网络连接在一起。

室外桥接现场勘测与室外 802.11 现场勘测所用的工具截然不同。为确保桥接链路的稳定性，勘测人员还需要计算大量参数。前面的章节曾经介绍过，部署室外桥接链路时需要计算菲涅耳区、地球曲率、自由空间路径损耗、链路预算、衰落容限等参数。此外，还应考虑各国射频监管机构对 IR(主动辐射器输出功率)和 EIRP(等效全向辐射功率)的限制。所有室外现场勘测都要将天气因素考虑在内，并安装合适的防雷和防风设备。室外无线桥接勘测通常需要两名勘测人员协同作业。下面列出了室外桥接现场勘测可能用到的一些工具：

地形图　楼层平面图用于室内勘测，而标记有海拔、位置等信息的地形图用于室外勘测。

链路分析软件　点对点链路分析软件与地形图配合使用，用于生成桥接链路配置文件并进行必要的计算(如菲涅耳区和 EIRP)。桥接链路分析软件属于预测性建模工具。

计算器　软件计算器与电子报表用于计算链路预算、菲涅耳区、自由空间路径损耗、衰落容限等必要的参数。计算电缆衰减与 VSWR(电压驻波比)时可以采用其他工具。

最大树木长势数据　树木是阻碍菲涅耳区的潜在因素之一。只要树木还没有完全成熟，它就有可能继续生长。将阻挡通信链路的树木全部砍伐掉并不现实，因此根据树木长势规划合适的天线高度至关重要。勘测人员可能需要咨询当地的农林部门，以获得有关树木生长的信息。

望远镜　可通过望远镜观察可视视距，不过确定射频视距时需要计算菲涅耳区净空。如果链路距离大于 5mi(8km)，则很难获得无阻碍的射频视距。规划桥接链路时，需要对地形和地球曲率等信息有较为深入的了解。

对讲机或移动电话　802.11 桥接链路可能绵延数英里，因此勘测团队中的工程师们需要使用通信工具相互通话。

信号发生器与功率表　信号发生器与功率表配合使用，可以测试线缆、接头以及其他配件的信号损耗与 VSWR。部署开始前，应使用两种工具测试线缆和接头。部署结束后，应定期使用两种工具检查线缆和接头是否受到环境因素(如水)的影响。信号发生器与功率表如图 16-10 所示。

图 16-10 信号发生器与功率表

可变损耗衰减器 这种设备带有表盘，能调节吸收能量的大小。可变损耗衰减器用于在室外现场勘测中模拟不同长度的电缆或电缆损耗。

测斜仪 用于测定障碍物的高度，这对于确保链路畅通至关重要。

GPS 规划网络时，务必将发射地(transmit site)、障碍物或兴趣点(point of interest)的经纬度记录在案。通过 GPS 可以很容易得到这些信息。

数码相机 用于拍摄设备的安装位置、电缆路径、接地位置、室内安装位置以及障碍物的照片。

频谱分析仪 用于测试发射地的环境射频级别。

高功率聚光灯或日光反射器 进行室外无线桥接勘测时必须确保勘测方向正确。随着链路距离的增加，辨认屋顶或发射塔将变得越来越难。为此，可考虑使用高功率聚光灯(相当于 300 万支蜡烛发出的光亮)或日光反射器。光的传播距离很远，勘测人员借助聚光灯能更好地观察远方区域，从而确保正确的勘测方向。

桥接现场勘测中一般不使用天线与接入点。为减少安装支座或其他附属设施带来的麻烦，勘测中很少使用桥接硬件设备。因为如果所有桥接测量数据和计算准确无误，桥接链路应可以正常工作。实施 Mesh 网络室外现场勘测时，需要配备 Mesh 接入点和天线。

练习 16.1

电缆损耗计算

请在 Times Microwave 网站 www.timesmicrowave.com 上进行在线免费计算。

(1) 从 Product 文本框中选择等级为 LMR-1700-DB 的电缆。

(2) 在 Frequency 文本框中输入 2500，并在 Run Length 文本框中输入 200ft。

(3) 然后单击 Calculate 按钮。注意观察该等级的电缆在每 100ft(30.5m)距离上的损耗。

(4) 从 Product 文本框中选择等级为 LMR-400 的电缆。

(5) 在 Frequency 文本框中输入 2500，并在 Run Length 文本框中输入 200ft。

(6) 然后单击 Calculate 按钮。可以观察到，该等级的电缆在每 100ft(30.5m)距离上的损耗更大。

16.3　覆盖分析

本章前面讨论了覆盖分析中需要考虑的各种因素。下面将介绍两种主要的现场勘测覆盖分析类型：手工勘测和预测性勘测。我们还将讨论这两种覆盖分析勘测使用的软件工具，并介绍动态与自适应无线局域网技术。

16.3.1　手工覆盖分析

早期的手工现场勘测是最常见的一种覆盖分析。手工覆盖分析采用前面介绍过的技术确定蜂窝边界，它分为以下两大类：

被动勘测　在被动手工勘测中，无线射频卡收集信号强度(单位：dBm)、噪声级别(单位：dBm)、信噪比(单位：dB)等射频数据。但在勘测过程中，客户端适配器并没有与接入点建立关联，所有信息均来自于接收到的 OSI 第一层和第二层的无线信号。

主动勘测　在主动手工勘测中，客户端无线接口卡与接入点建立关联与二层连接，以便进行低级别的帧传输。如果二者还建立有三层连接，则可以通过 802.11 数据帧发送低级别的数据流量(如 ICMP ping)。由于客户端与这个接入点建立了关联，主动勘测不仅能测量物理层射频数据，还能测量丢包率、第二层重传率等上层参数。

大多数厂商建议同时实施被动勘测与主动勘测，并将两种勘测所获得的数据进行比较和对照。可能的话，最终覆盖分析报告中应分别列出两种勘测的结果。那么，可以使用哪些测量软件采集被动勘测与主动勘测所需的数据呢？市场上有大量免费的现场勘测工具，如用于 Windows 的 InSSIDer 和 Macintosh 系统的 iStumbler，它们可以用于被动覆盖分析勘测。

大部分 Wi-Fi 厂商的客户端软件都提供至少一种用于测量接收信号强度与信噪比的被动勘测工具。某些厂商的客户端软件也具备主动勘测的能力。在 Macintosh 系统上，如果你按住 Option 和 Airport status 按钮，在菜单栏，你可以观察到 PHY 模式、BSSID、信道、安全性、RSSI 和传输速率，如图 16-11 所示。如果处于 802.11n 模式，你甚至可以看到 MCS 参数。

图 16-11　Macintosh 的 Wi-Fi 详细信息

VoWiFi 电话或 Wi-Fi 条码扫描仪等手持设备可能内置有具备现场勘测能力的软件。手工

现场勘测中一个常见的错误是平握 VoWiFi 电话进行射频信号测量。由于 VoWiFi 电话的内置天线是垂直极化的，平握电话会导致信号测量结果有误。正确方法是直握电话，以便电话与接入点天线的极化方向一致。商业射频现场勘测应用软件(如图 16-12 所示)已经得到了业界的普遍接受。

图 16-12 商业覆盖分析应用软件

商业勘测软件可以导入建筑物的楼层平面图，且支持大部分图形文件格式。请注意，楼层平面图必须是按比例绘制的。商业勘测软件使用 802.11 客户端无线接口，采用被动或主动手工模式测量射频数据。勘测工程师在大楼内测量射频数据，并将结果记录在软件显示的楼层平面图中。勘测软件将被动和主动勘测采集的数据进行整合，然后在楼层平面图中生成射频足迹(RF footprint)或覆盖蜂窝的可视化图像。

这些信息储存在商业勘测软件中，用于今后的离线建模。换句话说，通过调整信道和功率设置，无线局域网设计工程师就能模拟不同条件下的网络运行状况。在进行容量规划时，勘测工程师也可使用商业勘测软件确定每蜂窝、每 VLAN 的数据速率。此外，大部分商业勘测软件都能加载多层建筑的楼层平面图，并进行三维覆盖分析。此外，商业勘测软件内置有 GPS 功能，可在室外勘测中记录设备的经纬度坐标。

16.3.2 预测性覆盖分析

第二种射频覆盖分析采用具备射频仿真与建模设计能力的应用软件。预测性覆盖分析软件根据建模算法和衰减值生成射频覆盖蜂窝的可视化模型，从而不必去实际测量射频数据。

使用模型算法和衰减值来创建预测的蜂窝覆盖区域。

设计图与楼层平面图一般为矢量图格式(.dwg 和.dwf)，包含所用的建筑材料类型等多层信息。预测性分析软件支持矢量图与栅格图格式(.bmp、.jpg 和.tif)，允许导入不同格式的楼层平面图。无线局域网设计工程师需要在楼层平面图中标明所用的建筑材料。目前，预测性分析软件的数据库中储存有石膏板、混凝土、玻璃等各种建筑材料的衰减值，软件采用预测算法与这些衰减信息建立预测模型。下面列出了预测模型包含的一些信息：

- 信道复用模式
- 覆盖蜂窝边界
- 接入点布局
- 接入点功率设置
- 接入点数量
- 数据率

预测性分析软件在楼层平面图上生成虚拟接入点，后者可以被置于楼层平面图的任何位置。通过调整虚拟接入点的功率设置、信道设置或天线类型，勘测工程师就能模拟不同条件下的网络运行状况。在尚未竣工的大楼中实施现场勘测时，就可以通过预测性分析软件与大楼设计图配合使用进行预测性的规划设计。

手工勘测和预测性勘测在进行覆盖勘测时哪种更好？

如果有时间和财力支持，传统的手工现场勘测仍然是最好的，尽管可能预测性勘测软件可能省时。不过许多勘测工程师已经开始采用这种软件，以缩短实际现场勘测所需的时间。勘测工程师首先使用预测性软件生成勘测区域的预测模型，再通过手工现场勘测加以验证。

需要注意的是，虽然预测性覆盖分析软件是一种强大的工具，但是仍应进行手工现场勘测以确认覆盖模拟的结果是否正确。近些年来预测性勘测越来越普遍。手工勘测目前通常被认为是一种“快速验证”方法，用来验证预测性分析的覆盖是否真实。

16.3.3　自组无线局域网

手工现场勘测是否还有存在的必要呢？业界对此颇有争议。大部分勘测人员坚称，手工覆盖分析总是必不可少的。不过许多无线局域网厂商也表示，手工现场勘测的作用由于动态射频技术的发展而大大弱化，甚至可能完全被动态射频技术所取代。

目前，一些厂商开发了基于软件和硬件的射频频谱管理(RFSM)解决方案。集中设备通过手机轻量接入点或自治型接入点无线射频卡在一段时间内采集的射频信息，统一管理和动态调整接入点的发射功率和信道设置，从而实现对整个射频覆盖蜂窝的动态调整。

RFSM 技术对各接入点实施动态负载均衡，从而解决了无线局域网的容量需求问题。RFSM 技术能实现自动蜂窝调校、自动监控、排错与射频环境优化，具备上述特征的无线局域网通常被称为自组无线局域网(self-organizing WLAN)。RFSM 无法弥补糟糕的网络规划，但可以帮助调整网络利用率。

真实场景

无线局域网厂商的动态射频技术是否会取代现场勘测？

由于几乎所有 WLAN 控制器厂商的产品都提供某种形式的动态 RFSM 解决方案，该技术近年来已被业界广泛接受，不少厂商的客户在采用动态射频部署之后也获得了巨大成功。WLAN 控制器厂商的销售代表往往宣称，他们的 RFSM 解决方案具备动态和自组特性，完全可以取代现场勘测。但这种说法并不正确。尽管动态 RFSM 技术在最近几年获得了长足发展，本书作者仍然强烈建议在部署开始之前实施现场勘测。手工和/或预测性勘测始终是无线网络规划中不可缺少的环节。动态射频技术通常在部署后的无线网络中起作用。

在 WLAN 控制器架构中，轻量型接入点不仅监控自己使用的信道，还通过离频扫描(off-channel scanning)监控其他信道，并将所有监听到的射频信息反馈给 WLAN 控制器。WLAN 控制器根据接入点反馈的射频信息动态调整各接入点的配置，如改变接入点的工作信道或功率设置。

16.4 小结

本章介绍了强制和可选的无线现场勘测要求。过去，频谱分析与覆盖分析是必须进行的，但现在应用测试与吞吐量测试也经常成为强制要求。这一章介绍了利用频谱分析仪确定潜在干扰源的重要性，并讨论了覆盖分析勘测的必要步骤。

本章还介绍了室外与室内现场勘测所需的各种工具。两种主要的覆盖分析以及自组无线局域网技术。实施全面、详尽的无线现场勘测将为无线局域网设计和管理奠定良好基础。

16.5 考试要点

定义频谱、覆盖与应用分析。理解为何频谱分析与覆盖分析是必须进行的，而应用分析通常并非强制要求。

识别无线局域网干扰源。描述 2.4GHz ISM 与 5GHz UNII 频段中可能存在的各种干扰设备。

解释如何进行射频测量。解释实施覆盖分析的步骤，并解释接收信号强度、信噪比等各类射频测量参数。

理解接入点布局与配置。解释覆盖分析中涉及的接入点布局、功率与信道配置。

识别各种现场勘测工具。理解室外与室内现场勘测的区别，识别勘测所用的各种工具。

解释两种主要的覆盖分析方法。描述手工勘测和预测性勘测之间的区别，并解释自组无线局域网技术。

16.6 复习题

复习题的答案见附录 A。

1. The Crocker company has generated a visual model of RF coverage for their corporate headquarters by using predictive modeling site survey software. The next step requires validation with a manual site survey. What modeling parameters should be validated during the manual site survey? (Choose all that apply.)

A. AP placement and power settings

B. Throughput

C. Coverage boundaries

D. Encryption settings

E. Roaming parameters

2. Which potential regional weather conditions can adversely affect an outdoor wireless bridge link and should be noted during an outdoor site survey? (Choose all that apply.)

A. Lightning

B. Dew point

C. Wind

D. Cloud cover

E. Thunder

3. Name the major types of coverage analysis site surveys. (Choose all that apply.)

A. Assisted

B. Self-organizing

C. Manual

D. Capacity

E. Predictive

4. ACME Hospital uses a connection-oriented telemetry monitoring system in the cardiac care unit. Management wants the application available over a WLAN. Uptime is very important because of the critical nature of the monitoring system. What should the site survey engineer be looking for that might cause a loss of communication over the WLAN? (Choose all that apply.)

A. Medical equipment interference

B. Safety glass containing metal mesh wire

C. Patients

D. Bedpans

E. Elevator shafts

5. Which type of coverage analysis requires a radio card to be associated to an access point?

A. Associated

B. Passive

C. Predictive

D. Assisted

E. Active

6. Which of the following tools can be used in an indoor site survey? (Choose all that apply.)

A. Measuring wheel

B. GPS

C. Ladder

D. Battery pack

E. Microwave oven

7. Which of the following tools might be used in an outdoor site survey used to provide outdoor coverage? (Choose all that apply.)

A. Spectrum analyzer

B. NEMA grade access point

C. Outdoor blueprints or topography map

D. Mesh routers

E. GPS

8. Name potential sources of interference in the 5GHz UNII band. (Choose all that apply.)

A. Microwave oven

B. Cordless phones

C. FM radios

D. Radar

E. Nearby 802.11b/g WLAN

9. Which of these measurements are taken during a passive manual site survey? (Choose all that apply.)

A. SNR

B. dBi

C. dBm signal strength

D. dBd

10. Which of the following tools is not necessary for an outdoor bridging site survey?

A. Inclinometer

B. Digital camera

C. Blueprints

D. Spectrum analyzer

E. GPS

11. Name the necessary calculations for an outdoor bridging survey under 5 miles. (Choose all that apply.)

A. Link budget

B. Free space path loss

C. Fresnel zone

D. Fade margin adjustment

E. Height of the antenna beamwidth

12. Name potential sources of interference that might be found during a 2.4GHz site survey. (Choose all that apply.)

A. Toaster oven

B. Nearby 802.11 FHSS access point

C. Plasma cutter

D. Bluetooth headset

E. 2.4GHz video camera

13. Which of the following tools can be used in an indoor 802.11 site survey? (Choose all that apply.)

A. Multiple antennas

B. 902 to 928 MHz spectrum analyzer

C. Client adapter

D. Access point

E. Floor plan map

14. Brandon Burmeister is a site survey engineer who is planning to deploy a wireless controller solution with dual-radio, dual-frequency lightweight access points. The employees will be assigned to the 5GHz network, and the guest users will be assigned to the 2.4GHz network. CCMP/AES encryption will be required for the employees, while the guest users will use only static WEP. Name the best possible choice that Brandon has for coverage analysis. (Choose the best answer.)

A. Conduct a predictive site survey for the 5GHz network and an assisted site survey for the 2.4GHz network.

B. Conduct manual coverage analysis for the 2.4GHz network first and then conduct manual coverage analysis for the 5GHz network.

C. Conduct a predictive site survey for the 2.4GHz network and an assisted site survey for the 5GHz network.

D. Conduct manual coverage analysis for the 5GHz network first and then conduct manual coverage analysis for the 2.4GHz network based on the AP placement of the 5GHz APs.

15. Bob has to perform a site survey for a WLAN by using a multiple-channel architecture (MCA) system in a 20-story building with multiple tenants. What should Bob consider during the planning and implementation stages of the site survey? (Choose all that apply.)

A. Other tenants' WLANs should be considered.

B. Only WLAN controller solutions with lightweight APs should be deployed and not autonomous access points.

C. Access points should use high-gain omnidirectional antennas to provide coverage across multiple floors.

D. Access points should be at full transmit power to provide coverage across multiple floors.

E. The cell coverage of each access point should extend to only one floor above and one floor below to create a three-dimensional channel reuse pattern.

16. Which of the following tools may be found within an indoor site survey kit? (Choose all that apply.)

A. Digital camera

B. Colored electrical tape

C. Grid antenna

D. Access point enclosure unit

E. Temporary mounting gear

17. Jane Barrett is a site survey engineer who has to deploy eighty 2.4GHz thin access points in a warehouse with long corridors and metal racks. A WLAN controller will be used to manage all the access points. Six hundred 802.11g bar code scanners are currently deployed throughout the warehouse using WPA2-Personal for security. Which is the most important site survey tool to ensure the best performance throughout the warehouse?

A. 802.11a/b/g multistation emulator

B. Directional antennas

C. Security analysis software

D. All of the above

18. What access point settings should be recorded during manual coverage analysis? (Choose all that apply.)

A. Power settings

B. Encryption settings

C. Authentication settings

D. Channel setting

E. IP address

19. Which type of manual coverage analysis does not require a radio card to be associated to an access point?

A. Associated

B. Passive

C. Predictive

D. Assisted

E. Active

20. Which type of site survey uses modeling algorithms and attenuation values to create visual models of RF coverage cells?

A. Associated

B. Passive

C. Predictive

D. Assisted

E. Active

第 17 章 以太网供电(PoE)

在该章中，你将学习以下内容：

- √ 以太网供电(PoE)历史回顾
  - 非标准 PoE
  - IEEE 802.3af 修正案
  - IEEE 802.3-2005 标准第 33 条款
  - IEEE 802.3at-2009
- √ PoE 设备概述
  - 受电设备(PD)
  - 供电设备(PSE)
  - 端接式供电设备
  - 中跨式供电设备
  - 供电设备引脚分配
- √ 规划与部署 PoE
  - 功率规划
  - 冗余
  - 802.11n 与 PoE

在这一章中，你将了解到使用以太网电缆为网络设备提供电力的各种方法。以太网供电(PoE)不是 Wi-Fi 技术，也并非无线设备专用。然而，它却是为企业级接入点供电的主要方法，从而使其成为一个讨论无线网络时必要且重要的主题。

17.1 以太网供电(PoE)历史回顾

在开始这一章之前，我们首先解释一下什么是 PoE(Power over Ethernet，以太网供电)。多年以来，典型的计算机网络一直由固定的、连接到有线网络的电子计算机系统构成。这里的“计算机”既可以指台式机，也可以指服务器或大型机。随着技术的不断发展，大型计算机逐渐让位于小型计算机，笔记本电脑和便携设备开始崭露头角。在网络设备的小型化(物理尺寸和电子设计方面)达到一定程度后，采用以太网电缆同时传输数据并为设备供电成为可能。

自从电话出现之后，人们就提出了通过网络为设备供电的概念。时至今日，电话依然通过电话网接受供电。桌面 VoIP 电话、相机和接入点等计算机网络设备一般采用 PoE 供电。以太网电缆由 4 对电缆构成，对于 10Mbps 和 100Mbps 以太网来说通常只有两对电缆用于收发数据，另外两对电缆闲置不用，对于千兆以太网来说，所有电缆用来接收和发送数据。本章之后你会发现这不会是一个问题，因为 PoE 可在用于数据传输的电缆上传递电力。

如果采用同一条以太网电缆为 PoE 设备传输数据并输送电量，则一条普通的低压电缆就能解决全部问题。PoE 技术的应用让电缆和插座大为减少，人们不必再为设备拉线供电。这不仅能大幅降低网络设备的安装成本，还能增加设备的灵活性。无论设备安装在何处，都可以通过一条以太网电缆同时完成数据传输与电量输送的任务。

17.1.1 非标准 PoE

与大多数新技术的发展历程类似，一些公司首先注意到用户对 PoE 技术的需求，并开发了第一批采用专有解决方案的 PoE 设备。IEEE 从 1999 年开始制定相关标准，并于 4 年后批准通过了 PoE 标准。与此同时，市场上也出现了大量厂商专有的 PoE 解决方案。但是，这些解决方案使用的电压各不相同，混用不同厂商的方案可能导致设备损坏。

17.1.2 IEEE 802.3af 修正案

IEEE 802.3af 以太网供电委员会制定了 802.3 PoE 修正案，其正式名称为“IEEE 802.3 修正案：通过介质馈电接口(MDI)为数据终端设备(DTE)供电”(IEEE 802.3 Amendment: Data Terminal Equipment (DTE) Power via Media Dependent Interface)。IEEE 802.3 修正案于 2003 年 6 月 12 日被批准通过，它定义了如何通过 PoE 为 10BaseT(标准以太网)、100BaseT(快速以太网)与 1000BaseT(千兆以太网)设备供电的方法。

17.1.3 IEEE 802.3-2005 标准第 33 条款

2005 年 6 月，IEEE 批准了经过修订的 802.3 标准，修订后的标准称为 IEEE 802.3-2005

标准。该标准整合了 4 项修正案，802.3af 是其中之一。虽然大部分人仍然习惯于将 PoE 称为 802.3af，但其正式名称为 IEEE 802.3-2005 标准第 33 条款(IEEE Std. 802.3-2005, Clause 33)，该标准在 2008 年经过修改。

17.1.4　IEEE 802.3at-2009

2009 年 9 月，IEEE 批准通过了 802.3at 修正案。802.3at 又称 PoE+，它是对 PoE 标准的完善和增强。802.3at 任务组主要研究如何为受电设备输送更多的电量，同时向后兼容条款 33 设备。由于接入点的速度越来越快，采用的新技术(如 MIMO)越来越多，它们对电量的需求也越来越大。集成了 802.at 技术的交换机和 WLAN 控制器不仅能为传统的接入点供电，还能为耗电量更大的新型接入点提供充足电量。对使用多条射频链路的双频 802.11n 接入点而言，其耗电量很可能超过 15.4 W。一些 802.11n 企业厂商目前正在开发输出功率高于 15.4W 的专有 PoE 技术，以便为 802.11n 接入点供电。IEEE 802.3at 修正案通过利用两对电缆能够提供高达 25.5W 的电力。802.3at 修正案定义 Type1 和 Type2 型 PoE 设备。可以支持 802.3at 标准的设备称为 Type2 设备，而不支持更高电力的设备称为 Type1 设备。

通常当 802 修正案被创建和批准的时候，修正案是针对基础标准进行一系列补充、删除、编辑、修改和更新后文档。对 802.3at 来说，802.3-2008 标准的第 33 条款中的 PoE 章节已经完全被 802.3at 修正案取代了。

17.2　PoE 设备概述

PoE 标准定义了两种相互通信的 PoE 设备：PD(Powered Device，受电设备)与 PSE(Power-Sourcing Equipment，供电设备)，二者构成了 PoE 基础架构。

17.2.1　受电设备

受电设备(PD)向 PSE 要求供电或从 PSE 接受供电。PD 必须能从以太网电缆的数据电缆对或空闲电缆对接受最高达 57V 的电量。此外，PD 必须能通过电源的任意极性(模式 A 或模式 B)接受供电，如表 17-1 所示。

表 17-1　PD 引脚

导体引脚	模式 A	模式 B
1	正电压、负电压	
2	正电压、负电压	
3	负电压、正电压	
4		正电压、负电压
5		正电压、负电压
6	负电压、正电压	
7		负电压、正电压
8		负电压、正电压

PD 必须向 PSE 返回检测签名(detection signature)，以通知对方自己是否准备接受供电。PSE 也可以通过检测签名判断 PD 是否符合 IEEE 802.3-2008 标准第 33 条款。如果 PD 不符合 PoE 标准，则 PSE 拒绝向 PD 供电。准备接受供电的 PD 会向 PSE 提供一个可选的分类签名(classification signature)，以便 PSE 确定 PD 所需的电量。Type2 型的设备会进行一次物理层或数据链路层检测，以识别 Type2 型 PD 是连接在 Type1 型还是 Type2 型 PSE 上。如果相互认证无法完成，设备只能按 Type1 型工作。

表17-2 列出了用于标识不同分类签名的电流值。假如测量到的电流值不在上述范围之内，PD 将被划分为 0 类设备。如果 PSE 无法确定 PD 的类别，它将以最大功率向 PD 供电。如果 PSE 能确定 PD 的类别，它将仅以 PD 所需的功率向 PD 供电，从而更好地分配电量。正确划分设备类别不仅有助于减少耗电，还可以在一台 PoE 交换机或控制器上连接更多的设备。

表 17-2 PD 分类签名测量电流值

参 数	条 件	电 流 范 围
0 类	14.5V～20.5V	0mA～4mA
1 类	14.5V～20.5V	9mA～12mA
2 类	14.5V～20.5V	17mA～20mA
3 类	14.5V～20.5V	26mA～30mA
4 类	14.5V～20.5V	36mA～44mA

某些厂商采用专有的设备分类技术。虽然这些技术有助于电源管理并减少耗电，但是它们互不兼容，无法在不同厂商生产的设备中使用。

表 17-3 列出了 PoE 设备的类别，以及每类设备使用的最大功率范围。

表 17-3 PD 功率分类与用途

类 别	用 途	最大可用功率范围	类 别 描 述
0	默认	0.44W～12.95W	无法分类
1	可选	0.44W～3.84W	非常低的电力
2	可选	3.84W～6.49W	低电力
3	可选	6.49W～12.95W	中等电力
4	Type2 型设备	12.95W～25.5W	高电力

17.2.2 供电设备

供电设备(PSE)向 PD 供电，额定供电电压为 48V(44V～57V)。PSE 采用直流检测信号搜索是否有 PD 与自己相连。如果 PD 符合 PoE 标准，则 PSE 开始向 PD 供电。如果 PD 没有响应检测签名，则 PSE 拒绝向 PD 供电，以免损坏设备。

对比表 17-4 和表 17-3 可以发现，在各个类别上，PSE 的最小输出功率均大于 PD 的最大接收功率。这是因为考虑到 PSE 与 PD 之间的电缆和接头损耗，PSE 必须为可能存在的电量损失预留空间。所有 PD 的最大接收功率均为 25.5W。PSE 也可以通过 PD 提供的分类签名划分其类别。PD 连接到 PSE 之后，PSE 将持续监控 PD 的连接状态和电气条件(如短路)，并在 PD 断开连接时停止供电。PSE 分为端接式 PSE(endpoint PSE)与中跨式 PSE(midspan PSE)两类。

表 17-4　PSE 的最小输出功率

分　类	PSE 的最小输出功率
0	15.4W
1	4.0W
2	7.0W
3	15.4W
4	30W

17.2.3　端接式供电设备

端接式 PSE(Endpoint PSE)既可以传输以太网数据信号，也可以为 PD 供电，它通常是具备 PoE 功能的以太网交换机或 WLAN 控制器等专业设备，如图 17-1 所示。

图 17-1　内置 PoE 线路接口卡的 Aruba 6000 型无线控制器

端接式设备可以采用备选方案 A(Alternative A)或备选方案 B(Alternative B)为 PD 供电。

Alternate A：PSE 通过数据电缆对为 PD 输送电量，图 17-2 显示了 10BaseT/100BaseTX 端接式供电设备使用 Alternative A 方案；图 17-3 显示了 1000BaseT 端接式供电设备采用 Alternative A 方案。

图 17-2　10BaseT/100BaseTX 端接式 PSE：Alternative A

图 17-3 1000BaseT 端接式 PSE：Alternative A

Alternate B：10BaseT/100BaseTX 环境下 PSE 通过空闲电缆对为 PD 输送电量，如图 17-4 所示。而 1000BaseT 端接式 PSE 也可以使用 Alternate B 方式为 PD 供电，如图 17-5，它利用了 1000BaseT 数据电缆对的两对传输电力。Alternate B 兼容 10BaseT(标准以太网)、100BaseTX(快速以太网)与 1000BaseT(千兆以太网)。需要注意的是，在 802.3af 最初被批准的时候 1000BaseT(千兆以太网)设备只能通过端接式设备接受供电。在下节，你会发现情况有所变化，在批准的 802.3at 标准中，1000BaseT 设备既可以由端接式 PoE 也可以由中跨式 PoE 供电。

图 17-4 10BaseT/100BaseTX 端接式 PSE：备选方案 B

图 17-5　1000BaseT 端接式 PSE：备选方案 B

17.2.4　中跨式供电设备

中跨式 PSE 相当于一种为以太网段供电的传递设备。中跨式设备采用 PoE 为现有网络输送电量，无需替换当前的以太网交换机或 WLAN 控制器。中跨式 PSE 位于以太网源设备(如以太网交换机)与 PD 之间，中跨式 PSE 类似于一个以太网中继器。最初 802.3af 中跨设备只能利用 Alternative B 方案，而且只适用于 10BaseT 和 100BaseTX 受电设备。随着 802.3at 得到批准，中跨设备现在既可以使用 Alternative A 也可以使用 Alternative B 方案，而且都支持 1000BaseT 设备。

图 17-6 表明 10BaseT 和 100BaseTX 中跨 PSE 如何使用 Alternative A 方案进行供电。图 17-7 表明 1000BaseT 中跨设备如何使用 Alternative A 方案进行供电。图 17-8 表明 10BaseT 和 100BaseTX 中跨 PSE 如何使用 Alternative B 方案进行供电。图 17-9 表明 1000BaseT 中跨设备如何使用 Alternative B 方案进行供电

图 17-6　10BaseT 和 100BaseTX 中跨式 PSE：Alternative A

图 17-7　1000BaseT 中跨式 PSE：Alternative A

图 17-8　10BaseT 和 100BaseTX 中跨式 PSE：Alternative B

图 17-9　1000BaseT 中跨式 PSE：Alternative B

图 17-10 显示了一台单口中跨式设备与三台多口中跨式设备。中跨式 PSE 通常称为电源注入器(单口设备)或 PoE 集线器(多口设备)。

图 17-10　PowerDsine 电源注入器和 PoE Hub

图 17-11 显示了 PD 的 3 种供电方式。第一种方式采用内置供电模块的端接式 PoE 交换机，能同时向接入点传输以太网数据并供电。第二种和第三种方式均采用中跨式供电。第二种方式采用多口中跨式 PSE，后者通常称为内联电源转接板(inline power patch panel)；第三种方式采用单口中跨式 PSE，后者通常被称为单口电源注入器。

图 17-11　3 种 PSE 解决方案

17.2.5　供电设备引脚分配

PoE 技术采用两种合法的 4 线引脚连接。在这两种配置中，两对导体引脚输送大小和极性相同的额定电流。当采用备选方案 A 为设备供电时，正电压与 PSE 的发送线对相匹配。以太网电缆的输入对必须连到设备电缆的输出对，即 MDIX。许多设备具有自动调整 MDI 与 MDI-X 的能力(也称为“Auto MDI-X”或“自动交叉”)，则端口也可以选择 Alternative A 方案定义的极性选项，如表 17-5 所示。

表 17-5 PSE 引脚分配

导体引脚	Alternate A(MDI-X)	Alternate A(MDI)	Alternate B(全部)
1	负电压	正电压	
2	负电压	正电压	
3	正电压	负电压	
4			正电压
5			正电压
6	正电压	负电压	
7			负电压
8			负电压

17.3 规划与部署 PoE

早期的桌面 VoIP 电话与接入点不支持 PoE，每台连接到网络的设备都要通过电源插座供电，这些插座在大楼或校园中随处可见。随着技术的发展，配线室或数据中心目前都可以通过 PoE 接受供电。

17.3.1 功率规划

目前，一台或几台 PSE 就可以承担起为大量设备输送电量的任务，而无需像过去那样为每台设备拉电源线供电。考虑到 PD 的最大接收功率，PSE 必须能为每台 PoE 设备提供 15.4W 或 30W 的电量，这取决于你的设备是否需要 PoE+。假如设备不要求 PoE+，也就是说，对一台典型的 24 口 PoE 以太网交换机而言，其输出功率必须达到 370W(15.4W×24＝369.6W)才能满足所有端口的需要，这还不包括交换机自身的耗电量。判断交换机是否有能力为所有设备供电时，可以采用以下简单方法：首先确定等效非 PoE 交换机的输出功率，再计算与交换机相连的 PoE 设备的总耗电量(PoE 设备的数量乘以 15.4W 或者 30W)，最后与交换机的输出功率相加，所得结果即为交换机需要提供的总功率。

110 V/30A 电源的最大输出功率为 3300 W(110V×30 A)，配线柜也经常只提供 1650W 的功率(100 V×15 A)。企业级 PoE 交换机通常包括若干个安装在机架上的 48 口线路接口卡。机架本身的功耗为 1000W～2000W；如果每个端口的功耗为 15.4W，则 48 口线路接口卡的总功耗为 740W。不难计算出，3300W 可能只够为机架和两到三个全功能 48 口线路接口卡供电。

由于 802.11 接入点、摄像机、桌面 VoIP 电话等许多设备都要耗电，交换机可能无法为所有 PoE 端口输送足够的电量。网络工程师已经开始认识到功率预算(power budget)的必要性和重要性。为满足所有 PD 的供电需要，必须仔细规划功率预算。如果 PD 能提供分类签名，则对降低耗电量以及减少在功率预算中的比例大有帮助。一台耗电量为 3W 但无法提供分类签名的设备将被划分为默认的 0 类设备，功率预算中需要为其分配 15.4 W 的电量，这意味着实际有 12 W 的电量被浪费。如果同一台设备向 PSE 提供分类签名，它将被划分为 1 类设备，

则功率预算中只需为其分配 4 W 电量。随着 802.11 PoE 部署的逐渐普及，分类签名的重要性将越来越明显。

为适应市场对 PoE 设备的需求，不少交换机厂商开始用 220V/20 A 电源替换 110V/30 A 电源，并着手研发输出功率更大的 PoE 交换机，以满足不断增长的供电需求。某些 PoE 交换机的输出功率可达 9000W。由于 PoE 设备的数量越来越多，相应的管理和排错需求也随之增加。图 17-12 显示了一种测试设备，可以将其置于 PSE 和 PD 之间，以便排除 PoE 链路的故障。

图 17-12　Fluke NetTool Series II 在线型网络测试仪

PoE 设备在网络中的应用日渐普及，这使得人们更关心如何满足数据中心或配线室的能耗需求。随着耗电量的增加，PoE 交换机供电电路的规模将随之增大，配线室的温度也将随之升高，这往往意味着需要更多的散热设备。使用高功率电源时，建议部署冗余电源作为备份。

17.3.2　冗余

小时候，一想到停电时也可以打电话，心里就觉得很踏实。随着年龄的增长，我们知道，即使出现紧急情况(如电气故障)也不会影响电话的使用。这是我们乐见的一种服务状态。即使 VoIP 和 VoWiFi 电话已经开始取代传统的电话，这种不受外界影响的服务也必须延续下去。为此，应确保所有 PSE 与不间断电源相连，并为 PD 提供双以太网连接。

PoE 使用忠告

PoE 可为 AP 和 VoIP 电话提供电力，使用越来越普及。办公室也开始部署更多的 PoE 接口。PoE 必要功能之一是当插入设备时，PSE 可以确定设备是否支持 PoE，如果支持，就提供电力。如果该设备不支持 PoE，就只提供一个无电力输出的以太口接入服务。

有些型号和品牌的 PoE 交换机，在 PoE 设备拔出交换机端口后几秒钟内仍然保持 PoE 供电状态，即使现在这个端口没有接任何设备。如果这时快速地将另一设备插入相同的端口，这时 PoE 交换机仍然会在该端口提供电力输出，如果它不是一个 PoE 设备，就可能被损坏。

要避免这种风险发生，在拔出任何以太网设备后，应该习惯性地等待 5 到 10 秒，再将另一个设备插入该端口。这 5 到 10 秒钟的延迟足够该端口禁用 PoE。当另一个设备连接到该端口时，该端口会判断新的设备是否支持 PoE。

17.3.3 802.11n 与 PoE

在第 18 章中，你会了解到大多数企业级 802.11 AP 会使用 2x3:2 或 3x3:3 MIMO 射频卡，并支持两个频段。换句话说，一颗企业级双频 802.11n AP 共有 6 个射频链(三个 2.4GHz 传输射频链和三个 5GHz 传输射频链)需要电力供应。802.3af PSE 可以轻而易举地为 2x2:2 双频 AP(四个射频链)提供电力。但很多情况下，12.95W 的电力面对双频 6 个射频链的 MIMO AP 时就显得力不从心。某些多射频卡的 AP 可能需要多达 20W 的输入功率。有的厂商的双频 3x3:3 MIMO AP 也可以支持 802.3af，而有的厂商就需要 802.3at，相同厂商的不同型号的产品对电力的需求也不尽相同。

802.11 n 接入点最好部署支持 POE+ (802.3at)的 PSE，它能够提供 30W 的功率。尽管现在 802.11 n 接入点可能不需要 802.3at，但未来传输速度更快的 AP 会需要 802.3at 提供更强电力。当前 3×3:3 双频 MIMO AP 正在普及，但用不了多久 4×4:4 双频 MIMO AP 或 802.11ac AP 就要进入市场。与快速增长的无线网络相比，交换机的更新周期通常较慢，但如果需要新购 PoE 交换机，就应考虑支持 802.3at 标准的产品。

许多公司和 WLAN 客户还未升级到 PoE+，仍在使用 802.3af PSE 设备。当前 WLAN 厂商使用传统供电方式为支持 6 个甚至更多射频链的 AP 供电时可采用如下方案：

使用双 802.3af 以太口 有些厂商就是简单地利用两个 802.3af 端口提供双倍电力。每个端口能为每根电缆提供 15.4W 电力。这个方案的缺点就是需要两根以太网电缆。

MIMO 能力降级 某些厂商的 3×3 的 802.11n AP 在使用 802.3af PSE 时只开启一路发射器以降低电力需求。这种方案的缺点就是部分 MIMO 传输能力消失。

挤压 POE(Squeeze the POE) 某些新型的 3×3:3 双频 MIMO AP 可使用传统的 802.3af PoE 全功能运行，其对电力的消耗更小，利用新型硬件进行更好的电力控制。但是六个传输射频链所需要的电力可能超过传统 802.3af 所能提供的 12.95W，它需要从输出功率为 15.4W 的 PSE 中获取 14W 的功率，这就需要 WLAN 厂商从 PSE 中挤压一部分功率出来。这种非标准的 POE 应用场景需要五类或更好的以太网电缆。

使用电源插头 AP 供电当然可以使用电源插头，但 AP 部署的区域经常无法提供电源插头。

17.4 小结

本章重点讨论了 PoE 以及向 PD 供电所需的设备和技术。PoE 可以通过专有方式或标准方式(即 802.3af 修正案，该修正案已经被整合到 IEEE 802.3 标准第 33 条款中，之后更新到 802.3at)实现。

基于标准的 PoE 包括以下重要设备：

- PD(受电设备)
- PSE(供电设备)
- 端接式 PSE
- 中跨式 PSE

上述设备相互协作，构成了一个有效的 PoE 网络。

本章最后介绍了规划与部署 PoE 时需要考虑的因素：

- 功率规划
- 冗余

17.5　考试要点

了解 PoE 的发展历史。务必了解 PoE 的发展历史以及 IEEE 最初制定的 802.3af 修正案、IEEE 802.3 标准第 33 条款及 802.3at。

熟悉各种 PoE 设备以及它们的工作方式。务必了解各种 PoE 设备及其用途，务必理解 PD(受电设备)、PSE(供电设备)、端接式 PSE 和中跨式 PSE 的工作方式。

了解各种设备分类以及如何划分设备的类别。务必了解 5 种设备分类以及如何确定 PD 的类别。了解用于标识不同设备的电流范围以及 PSE 向每类设备输送的电量。

17.6　复习题

复习题的答案见附录 A。

1. The IEEE 802.3af amendment has been incorporated into the IEEE Std. 802.3 revised standard and is defined in which clause, which was later replaced by the ratification of the 802.3at amendment?

   A. Clause 15
   B. Clause 17
   C. Clause 19
   D. Clause 33
   E. Clause 43

2. If a classification signature is not provided, the device is considered to be in what class?

   A. 0
   B. 1
   C. 2
   D. 3
   E. 4

3. Which types of PoE devices are defined by the standard? (Choose all that apply.)

   A. PSE
   B. PPE
   C. PD
   D. PT

4. A powered device (PD) must be capable of accepting up to how many volts from either the data lines or the unused pairs of the Ethernet cable?

A. 14.5 volts

B. 20.5 volts

C. 48 volts

D. 57 volts

5. To qualify as compliant with the 802.3at amendment, a powered device (PD) must do which of the following? (Choose all that apply.)

A. Be able to accept power over the unused data pairs.

B. Reply to the PSE with a detection signature.

C. Accept power with either polarity from the PSE.

D. Reply to the PSE with a classification signature.

6. A VoIP telephone is connected to a 24-port PoE midspan PSE. If the telephone does not provide a classification signature, how much power will the PSE provide to the telephone?

A. 0 watts (The telephone would not be recognized as a PD.)

B. 4.0 watts

C. 7.0 watts

D. 15.4 watts

7. An endpoint PSE that provides power by using Alternative B is capable of providing power to devices by using which of the following Ethernet technologies? (Choose all that apply.)

A. 10BaseT

B. 100BaseTX

C. 1000BaseT

D. 100BaseFX

8. What is the range of maximum power used by a class 4 PD?

A. 0.44 to 12.95 watts

B. 3.84 to 6.49 watts

C. 6.49 to 12.95 watts

D. 12.95 to 25.5 watts

E. 15 to 30 watts

9. At maximum power requirements, a 24-port 802.3at-compliant PoE Ethernet switch must be able to provide about how many total watts of power to PoE devices on all ports?

A. 15.4 watts

B. 370 watts

C. 720 watts

D. 1000 watts

E. Not enough information is provided to answer the question.

10. If an 802.3at AP is equipped with two radios and requires 7.5 watts of power, how much power will the PSE provide to it? (Choose all that apply.)

A. 7.5watts

B. 10.1watts

C. 15watts

D. 15.4watts

E. 30.0watts

11. The PSE provides power within a range of_____volts, with a nominal value of _____volts.

A. 14.5 to 20.5, 18

B. 6.49 to 12.95, 10.1

C. 12 to 19, 15.4

D. 44 to 57, 48

12. Tim has installed an Ethernet switch that is compliant with 802.3at. He is having problems with his APs. Which of the following could be causing his problems?

A. Many PoE VoIP telephones are connected to the same Ethernet switch.

B. Most of the Ethernet cables running from the switch to the APs are 90 meters long.

C. The Ethernet cables are only Cat 5e.

D. The switch is capable of 1000BaseT, which is not compatible with VoIP telephones.

13. You are designing an 802.3at network and are installing a 24-port Ethernet switch to support 10 Class-1 VoIP phones and 10 Class-0 APs. The switch requires 500watts to perform its basic switching functions. How much total power will be needed?

A. 500watts

B. 694watts

C. 808watts

D. 1000watts

14. You are designing an 802.3at network and are installing a 24-port Ethernet switch to support 10 Class-2 cameras and 10 Class-3 APs. The switch requires 1000watts to perform its basic switching functions. How much total power will be needed?

A. 1080watts

B. 1224watts

C. 1308watts

D. 1500watts

15. When a powered device is first connected to a PSE, it presents itself as having a resistance level of what?

A. 25 ohms

B. 50 ohms

C. 25k ohms

D. 50k ohms

16. How much voltage does the PSE apply while trying to identify the detection signature?

A. 5volts

B. 10.1volts

C. 12volts

D. 48volts

17. What is the maximum power used by a PD Class 0 device?

A. 3.84W

B. 6.49W

C. 12.95W

D. 15.4W

18. The PSE will apply a voltage of between 14.5 and 20.5 and measure the resulting current to determine the class of the device. Which current range represents Class 2 devices?

A. 0 to 4mA

B. 5 to 8mA

C. 9 to 12mA

D. 13 to 16mA

E. 17 to 20mA

19. A PD must be capable of accepting power with either polarity from the power supply. In mode A, on which conductors/wires does the PD accept power?

A. 1, 2, 3, 4

B. 5, 6, 7, 8

C. 1, 2, 3, 6

D. 4, 5, 7, 8

20. A Type 2 PSE will perform a two-event physical layer classification or data link layer classification. If mutual identification cannot be completed, what does the Type 2 device do?

A. Defaults as a Category 0 device.

B. PoE cannot be enabled.

C. Operates as a Type 1 device.

D. Provides 15.4 watts of power using Alternative A.

第18章 高吞吐量(HT)与802.11n

在该章中，你将学习以下内容：

- √ 802.11n-2009 修正案
- √ Wi-Fi 联盟认证项目
- √ 多入多出(MIMO)技术
  - 射频链
  - 空分复用
  - MIMO 分集
  - 空时分组编码(STBC)
  - 循环移位分集(CSD)
  - 传输波束成形(TxBF)
- √ HT 信道
  - 20MHz HT 与 20MHz non-HT 信道
  - 40MHz HT 信道
  - 40MHz 不兼容
  - 保护间隔(GI)
  - 调制编码方案(MCS)
- √ HT 物理层
  - Non-HT 传统格式
  - HT 混合格式
  - HT 绿地格式
- √ HT MAC 层
  - MSDU 聚合(A-MSDU)
  - MPDU 聚合(A-MPDU)

- 块确认(Block Ack)
- 缩减帧间间隔(RIFS)
- HT 电源管理

√ HT 操作

- 20/40MHz 信道工作模式
- HT 保护模式(0～3)
- RTS/CTS 与 CTS-to-self

这一章将介绍目前备受关注的无线局域网新技术，这个新技术被定义在 802.11n-2009 修正案中，其主要目标是大大提高 2.4GHz 和 5GHz 频段的数据率和吞吐量。在 802.11n 定义的这种新的技术 HT 采用物理层和 MAC 子层增强机制，可提供高达 600Mbps 的数据率。

802.11n 定义了 MIMO(multi-input multi-output，多入多出)技术，后者采用多个无线接口与多副天线，完全颠覆了现有的物理层架构。前面的章节曾经介绍过，多径现象是一种射频行为，它往往会导致传统 802.11a/b/g 无线局域网的性能下降，而 MIMO 技术却利用多径现象提高吞吐量并扩大传输范围。

除 MIMO 技术外，802.11n 修正案还定义了其他 HT 机制以提高吞吐量。这一章将介绍如何利用 40MHz 信道以获得更多频率带宽。帧聚合(frame aggregation)属于 MAC 子层增强技术，它同样能提高吞吐量。802.11e 修正案定义了经过改进的电源管理机制，而 802.11n 修正案定义了全新的电源管理机制。

本章最后将介绍 HT 网络的各种工作模式，并讨论 HT 技术与本书讨论的其他技术在同一无线局域网中的共存问题。

802.11n 与 HT 技术的原理极其复杂，一本专门论述该技术的书籍恐怕也无法涵盖全部内容。不过这一章将介绍 HT 技术的所有关键细节，这些内容有助于读者备考 CWNA 认证。

18.1　802.11n-2009 修正案

802.11n-2009 修正案定义了 HT(条款 20)无线接口，并采用 MIMO(多入多出)技术与 OFDM(正交频分复用)技术。MIMO 技术能提高吞吐量并扩大传输范围。802.11n 修正案还对数据链路层的 MAC 子层进行改进，以进一步提高吞吐量。

虽然 802.11n 修正案定义的机制与 802.11a/b/g 技术差别很大，但是 HT(条款 20)无线接口必须能向后兼容 HR-DSSS(条款 18)、OFDM(条款 17)与 ERP(条款 19)无线接口，简而言之就是 802.11n 必须向后兼容 802.11a/b/g。目前我们常说的 802.11n 双频网卡通常就是 802.11a/b/g/n 网卡。

前面的章节曾介绍过，802.11b HR-DSSS(条款 18)和 802.11g ERP(条款 19)无线接口只能使用 2.4GHz ISM 频段进行通信，802.11a OFDM(条款 17)无线接口只能使用 5GHz UNII 频段进行通信。而 HT(条款 20)无线接口不依赖于频段，它可以使用 2.4GHz ISM 与 5GHz UNII 两个频段收发数据。自从 2009 年 IEEE 正式批准通过 802.11n 修正案后，具备 802.11n 能力的 Wi-Fi 网卡开始大量出现。

Wi-Fi 联盟认证项目

Wi-Fi 联盟开发了称为 Wi-Fi CERTIFIED 802.11n 的厂商认证项目，表 18-1 列出了 802.11n 产品需要通过的强制与可选基准特性测试。所有经过认证的产品还必须支持 WMM QoS 机制与 WPA/WPA2 安全机制。Wi-Fi CERTIFIED n 产品能够在 2.4GHz 和 5GHz 两个频段工作，向后兼容 802.11a/b/g 认证产品。某些特性只用于接入点测试。

表 18-1 Wi-Fi CERTIFIED 802.11n 基准要求

特　性	解　释	类　型
支持两路空间流	要求接入点发送和接收时均至少支持两路空间流，客户端发送和接收时只要求至少一路空间流	强制
支持三路空间流	接入点与客户设备在发送和接收时具有三路空间流的能力	可选。实施时进行测试
接收时支持 A-MPDU 与 A-MSDU，发送时支持 A-MPDU	所有设备。减少 MAC 层开销	强制
支持块确认(Block ACK)	所有设备。通过发送单一的 Block ACK 帧来确认多个接收帧	强制
支持 2.4 GHz 频段通信	设备可以仅支持 2.4GHz 频段、仅支持 5GHz 频段或同时支持双频通信；两种频段均列在表中作为可选特性	可选。实施时进行测试
支持 5 GHz 频段通信		可选。实施时进行测试
2.4GHz 与 5GHz 频段并发操作	该模式仅用于 AP。具备在两个频段操作能力的 AP 能够被认证为“并发双频”	可选。实施时进行测试
在 5GHz 频段中使用 40MHz 信道	2 个相邻的 20MHz 先到。被绑定成 1 个 40MHz 信道。提供双倍频宽	可选。实施时进行测试
2.4GHz 频段下 20/40Mhz 并存机制	如果 AP 支持 2.4GHz 频段下的 40MHz 信道，需要支持并存机制。默认 2.4GHz 信道宽度为 20MHz	可选。实施时进行测试
绿地前导码	传统设备无法识别绿地前导码；如果 802.11n 网络中不存在传统设备，使用绿地前导码能提高通信效率	可选。实施时进行测试
在 20MHz 与 40MHz 信道中采用较短的保护间隔(GI)	传统的保护间隔为 800ns，较短的保护间隔为 400ns。将数据率提高 10%	可选。实施时进行测试
空时分组编码(STBC)	通过多副天线对数据流进行块编码以改善接收效果。用于对 AP 的认证	可选。实施时进行测试
HT 复制模式	允许 AP 在 40MHz 信道内的每个 20MHz 信道同时发送相同的数据	可选。实施时进行测试

实际上，Wi-Fi 联盟在 802.11n-2009 修正案获批之前，开始认证 802.11n 产品。但在 Wi-Fi CERTIFIED™ 802.11n 认证项目出现之前，不少无线局域网厂商就已向 SOHO 市场推出了 pre-802.11n 产品。但是，这些产品之间大多无法互通，它们与经过认证的 Wi-Fi 联盟产品也不兼容。pre-802.11n 的产品从未在企业环境中部署。

可在 http://www.sybex.com/go/cwna3e 上下载 Wi-Fi 联盟发布的白皮书，白皮书名为 Wi-Fi CERTIFIED n Longer-Range, Faster-Throughput, Multimedia-Grade Wi-Fi Networks。

18.2　MIMO 技术

多入多出(MIMO)技术构成了 802.11n 修正案物理层增强机制的核心。MIMO 系统包括若干条射频链(radio chain)，后者由多个无线接口与多副天线构成。本章后面部分会对射频链进行定义。MIMO 利用多径同时通过多个射频信号传输数据。

传统的 802.11 环境下，多径现象会导致很多麻烦。多径现象是指相同信号通过两条或更多条路径同时或相隔若干时间到达同一接收天线。由于电磁波的天然特性，会产生反射、散射、衍射和折射行为，这些会导致多径现象。第 2 章讨论过多径会导致信号强度下降和数据破坏。有趣的是，在 802.11n 技术中，多径现象是朋友而不是敌人。

通常在室内环境中，MIMO 射频卡利用多条路径发送多路信号至 MIMO 接收方。如图 18-1，三个原始信号的多个拷贝被多副天线接收，MIMO 接收方能够利用高级数字信号处理器(DSP)甄别出原始发送信号。高度多径环境有助于 MIMO 接收方区分出通过多个 RF 信号传输的单一信号。事实上，如果 MIMO 发射机传输的所有信号同时到达接收机，这些信号将相互干扰，导致 MIMO 系统与非 MIMO 系统的性能并无太大区别。

图 18-1　MIMO 操作与多径

此外，MIMO 技术通过空间复用(Spatial Multiplexing，SM)同时传输多条数据流以提高吞吐量，并利用传统 802.11 网络极力避免的多径效应。MIMO 系统也可以使用多副天线以实现更好的传输和接收天线分集，从而扩大传输范围和传输可靠性。有多种传输与接收分集技术。STBC 与 CSD 都属于传输分集技术，它们都将相同数据从多幅天线发出。STBC 可能只在 802.11n 设备间通信。CSD 分集信号既可以被 802.11n 设备接收，也可以被传统设备接收。传输波束成形(Transmit BeamForming，TxBF)将相同信号从多幅天线发出，这些天线类似于相控天线。MRC 是一种接收分集技术，它将多个接收信号混合，以改善接收灵敏度。SM 与分集技术会在下面详细讲解。

18.2.1　射频链

传统的 802.11 无线射频卡采用 SISO(Single-Input Single-Output，单入单出)系统收发射频信号。SISO 系统使用一个射频链。可将射频链定义为一个射频接口与所有配套设备(混频器、

放大器、模数转换器等)的集合。

MIMO 系统由多条射频链构成，每条射频链都有各自的天线。可以通过射频链使用的发射机与接收机的数量划分 MIMO 系统的类别。例如，一个 2×3 MIMO 系统由 3 条射频链构成，其中发射机的数量为 2 个，接收机的数量为 3 个。一个 3×3 MIMO 系统由 3 条射频链构成，其中发射机的数量为 3 个，接收机的数量为 3 个。在 MIMO 系统中，第一个数字代表发射机(Tx)，第二个数字代表接收机(Rx)。

图 18-2 显示了两种 MIMO 系统，它们分别是 2×3 与 3×3 MIMO 系统。需要注意的是，虽然两种系统都由 3 条射频链构成，但是 3×3 系统包括 3 个发射机，而 2×2 系统只包括两个发射机。

图 18-2 2×3 与 3×3 MIMO 系统

在 MIMO 系统中，多个发射机通过空间复用发送更多的数据，多个接收机采用先进的 MIMO 天线分集技术以提高信噪比。接下来将详细介绍空间复用和天线分集在 802.11n 系统中的重要作用。802.11n 标准允许使用最多 4 条射频链的 4×4 MIMO 系统。每条射频链都需要消耗电力，所以 4×4 MIMO 系统的耗电量远远大于 2×2 MIMO 系统。

18.2.2 空间复用

MIMO 无线接口同时发送多路无线信号，每路无线信号通过独立的无线接口与天线传输给接收机。MIMO 系统实际上利用了多径效应。每路独立的信号称为空间流(spatial stream)，不同无线接口发送的空间流包含不同的数据。由于发射天线之间至少相隔半个波长的距离，这些数据流将沿不同的路径到达接收机，这称为空间分集(spatial diversity)。利用空间分集发送多路独立的数据流通常也被称为空间复用(SM)或空间分集复用(Spatial Diversity Multiplexing，SDM)。

同时发送多路独立的数据流能极大提高吞吐量。如果 MIMO 接入点向 MIMO 客户端发送两路独立的数据流，且客户端可以成功接收这两路数据流，则吞吐量将增加为原来的两倍。如果 MIMO 接入点向 MIMO 客户端发送 3 路独立的数据流，且客户端可以成功接收这 3 路数据流，则吞吐量将增加为原来的 3 倍。

不要混淆数据流的数量与发送机的数量。通常 MIMO Radio 指的就是各有几个发送和接收射频卡。WIFI 厂商一般利用三个数字来描述 MIMO 的能力，第一个是指发送机的数量，

第二个是指接收机的数量，第三个是指发送和接受的数据流的数量。

例如 3×3:2 MIMO 就代表各有三个发送机和接收机，但只有 2 个数据流。3×3:3 MIMO 指的是各有三个发送机和接收机，但有 3 个数据流。

从图 18-3 中可以观察到，一个 3×3:3 MIMO 接入点向 3×3:3 MIMO 客户端发送了 3 路独立的数据流。

图 18-3　多路空间流

注意，并非所有 802.11n 射频卡具备的 MIMO 能力都相同。许多 802.11nAP 属于 3×3:2 或 3×3:3 的 MIMO 系统。而客户端情况会比较复杂。许多笔记本电脑也会使用 3×3:2 或 3×3:3 的 MIMO。许多手持设备可能仍然只支持 802.11a/b/g 的 SISO 系统。但是现在不少手持设备(如智能电话和 iPad)也开始支持某些形式的 802.11n 特性。1×1:1 的 MIMO 系统无法利用多路空间流的全部特性，但在 802.11n 的 MAC 层增强特性方面仍然可以受益。

3×3:3 AP 与 3×3:3 客户端通信时，可以利用三路空间流传输单播数据。但是 3×3:3 AP 与 2×2:2 客户端通信时，只能利用两路空间流传输单播数据。客户端在加入 BSS 时会通告 AP 其网卡的 MIMO 能力。802.11n 修正案最高支持 4×4:4 的 MIMO 系统。

发送多路空间流时，发射机可采用相同的调制方式，也可以采用不同的调制方式，前者称为平等调制(equal modulation)，后者称为非平等调制(unequal modulation)。例如，3×3:3 MIMO 无线接口既可以采用 64-QAM 发送全部 3 路数据流，也可以采用 64-QAM 发送两路数据流，而采用 QPSK 发送第三路数据流以提高信噪比。对同样一个 3×3:3 MIMO 系统而言，采用平等调制可以获得比采用非平等调制更多的吞吐量。无线局域网厂商如何在 802.11n 无线接口中实现非平等调制仍然有待观察。

18.2.3　MIMO 分集

如果用手将一只耳朵捂住，是否能听得更清楚呢？答案显然是否定的，因为两只耳朵可以听到更多声音。那么，假如人类有 3 只或 4 只耳朵，就能听得更远、更清楚。与之类似，MIMO 系统采用先进的天线分集技术，通过多副天线来提高通信质量。

人们往往混淆天线分集与 MIMO 系统使用的空间复用。无论是接收天线分集还是发射天线分集，都是通过多副天线来减少多径效应造成的不利影响。前面介绍过，MIMO 系统采用空间复用以增加数据容量，而空间复用实际利用了多径效应。换句话说，天线分集旨在弥补多径效应造成的损失，而不是利用多径效应提高通信质量。信号由于多径效应产生多个副本，这些副本信号以不同的幅度到达接收机。

第 4 章曾经介绍过，传统的天线分集由一个带有两副天线的无线射频卡构成。大部分 pre-802.11n 无线接口采用交换分集(switched diversity)，后者使用多副天线监听接收信号。到达接收机天线的信号存在多个副本，这些副本信号的幅度各不相同。交换分集选择幅度最好的信号，忽略其他信号。发送信号时也可使用交换分集，不过此时只使用一副天线。在最近一次接收信号的过程中，监听到最强信号的那副天线被选择出来，发射机将使用该天线发送当前的信号。

随着发射机和接收机之间的距离逐渐增大，接收信号幅度将越来越接近本底噪声。信噪比降低会导致数据损坏的概率增加，而监听两副天线可提高接收的成功率，因为至少能监听到一路完好信号。如果采用 3 副或 4 副天线对接收信号进行监听，则更可能接收到质高、无损的信号。交换分集系统采用 3 副或 4 副天线以提高信号接收的成功率，从而扩大了传输范围。

采用接收分集时，可以通过一种称为最大比合并(Maximal Ratio Combining，MRC)的信号处理技术将多个信号线性合并在一起。最大比合并算法对接收到的多个信号进行分析，并将它们以最优方式合并。通过采用交换分集与最大比合并技术，MIMO 系统可以有效提高接收信号的信噪比。如图 18-4 所示，非 MIMO 无线接口向 MIMO 无线接口传输数据时，为避免多径效应，最好采用最大比合并技术。最大比合并算法旨在寻找质量最好的接收信号，不过它也可以用于从嘈杂的信号中提取信息。由于原始数据以更好的方式进行重构，数据损坏的概率将大为降低。

图 18-4 最大比合并(MRC)

MRC 利用接收混合功能，对每个入射信号进行移相(phased-shifted)后进行混合，这样入射信号的信号强度(振幅)增加，SNR 也会变得更好。

18.2.4 空时分组编码

空时分组编码(STBC)是指相同信息通过两根或更多天线发送出去，它是一种发送分集技术。STBC 适用于射频链数量大于空间流数量的情况。STBC 通过在多根天线上发送相同的信息，实际上数据传输率并没有增加，但会使接收方的信号检测能力，尤其是对较低 SNR 信号的检测能力提高。也就是说，接收方的信号敏感度增加了。STBC 和 CSD 都属于发送分集技术，即通过多根天线发射相同数据。STBC 适用于 802.11n 设备之间，而 CSD 分集信号可以适用于 802.11n 或传统客户端。

18.2.5　循环移位分集

循环移位分集(CSD)是另一种 802.11n 标准定义的传输分集技术。与 STBC 不同，使用 CSD 的发送机的传输信号可以被传统的 802.11a 和 802.11g 客户端接收。对于 802.11n 与传统的 802.11a、802.11g 客户端共存的混合模式下，有必要在传输符号时在多根发送天线上增加传统的 OFDM 帧前导位。CSD 在每个传输信号上增加循环延迟，以减少多个信号之间的相关性。传统客户端会把多路接收信号认为是同一信号的多径效应版(multipath version)。循环延迟不会超过保护间隔(GI)，以免导致码间干扰(ISI)。而对 802.11n 系统来说，当然也可以利用多路信号改善 SNR。CSD 的工作原理细节不属于 CWNA 考试范畴。CSD 是 802.11n 一项出色的特性，但很少有人谈及，尽管如此，它对于设备厂商的射频卡设计仍然非常重要。

18.2.6　传输波束成形

802.11n 修正案还提出了一种称为传输波束成形(TxBF)的可选物理层技术，它是一种相位调整技术，适用于传输天线数量多于空间流数量的情况。

传输波束成形是一种 MIMO 发射机使用多副天线通过对传输信号的相位和振幅进行调整的技术。同一信号的多个副本到达接收机时，信号之间往往存在相差。但是如果 MIMO 发射机能确定接收机的位置，就可以相应调整这些信号的相位，使它们在到达接收机时同相，从而将信号异相导致的“消极”的多径转化为“积极”的多径。通过精确控制多副天线发送的信号相位，可以达到与采用一副高增益定向天线相似的效果。

传输波束成形技术利用多径效应提高通信质量，能获得更高的信噪比与更强的接收信号幅度，接入点可以覆盖更大范围内的客户端。由于信噪比提高，系统可以采用更为复杂的调制方式来编码更多的数据比特，从而提高了吞吐量。信噪比提高还能降低第二层重传的概率。

传输波束成形可与空间分集复用(SM)结合在一起使用，不过请注意，接收天线的数量决定了空间流的数量。例如，2×2 MIMO 无线接口只能接收两路空间流。4×4 MIMO 无线接口向 2×2 MIMO 无线接口传输数据时，前者只发送两路空间流，并使用其他天线实施波束成形，以便传输给 2×2 MIMO 无线接口的波束更为集中。如果空间分集复用并非最佳选择，则可以考虑采用传输波束成形。如图 18-5 所示，采用传输波束成形技术的发射机并不发送多路独立的空间流，而是发送同一射频信号的多个副本，每个副本信号的相位由发射机进行调整。

图 18-5　传输波束成形数据

传输波束成形技术依赖于发射机和接收机的隐式反馈(implicit feedback)与显式反馈(explicit feedback)。大多数支持波束成形的 802.11n 设备会利用隐式反馈，不在反馈过程中发送专用的交换帧，而是利用 ACK 帧进行 RF 反馈信息收集。可将潜艇使用的声纳与显式反馈做一类比。声纳利用声波在水下传播的特性来探测其他船只。潜艇发出声波，并根据返回声波的特性确定航线上可能存在的船只类型。利用显式反馈的 802.11n 发射机会根据接收机反馈的探空帧(sounding frame)调整信号相位。此时，发射机称为波束成形器(beamformer)，接收机称为波束成形接收器(beamformee)，二者相互向对方发送 MIMO 信道的特性信息。波束成形器向波束成形接收器发送探空请求帧，并根据波束成形接收器反馈的探空响应帧相应调整信号的相位。

包括无任务数据帧(null function data frame)在内的任何帧都可以作为探空帧使用。采用隐式反馈时，波束成形器根据波束成形接收器发送的长训练符号(training symbol)估算二者之间的 MIMO 信道。采用显式反馈时，两个 HT 无线接口之间会交换更多信息。波束成形接收器通过波束成形器发送的训练符号直接估算二者之间的 MIMO 信道，然后将该信息连同其他信息反馈给波束成形器。波束成形器根据波束成形接收器反馈的信息收发数据。应该注意，当前的大多数 802.11n 芯片组并不支持显式波束成形。

传输波束成形技术在很大程度上取决于接收方无线接口反馈的信息。如果 802.11n 客户端具备相似的特性，则可以最大限度地发挥传输波束成形的效能。只有 802.11n HT 无线接口可以采用显式反馈以及传输波束成形技术，802.11a/b/g 无线接口不具备这种能力。隐式波束成形也适合于下面场景：802.11n 可以发起隐式波束成形，而传统 802.11a/b/g 客户端回应了隐式波束成形。因此隐式反馈被大多数 WLAN 厂商采用。采用波束成形技术的接入点可以同时瞄准多个客户端，但只能进行单播传输。广播或多播传输不适用传输波束成形技术。目前，只有少数新型 802.11n 芯片集成了传输波束成形技术，Wi-Fi 联盟尚未开始对该技术进行测试。

传输波束成形与智能天线波束成形

802.11n 传输波束成形有时会与某些厂商(如 Ruckus)的智能天线波束成形混淆。动态波束成形利用动态的天线阵列根据目标客户端的位置进行波束调整。动态波束成形也经常被称为智能天线技术或者波束控制。

与动态波束成形不同，802.11n 传输波束成形(TxBF)不改变天线的辐射模式，因此并没有生成定向的波束。然而通过对多根天线的发射信号相位进行精确调整，可以起到与高增益定向天线同样的效果。802.11n TxBF 通过调整信号相位，是接收方可以收到更好更强的信号。

18.3 HT 信道

前面的章节曾经介绍过，802.11a 修正案在 5GHz UNII 频段上定义了采用 OFDM 技术的条款 17 无线接口，802.11g 修正案在 2.4GHz ISM 频段上定义了采用 ERP-OFDM 技术的条款 19 无线接口。OFDM 与 ERP-OFDM 本质上属于同一种技术，区别仅在于工作频段不同。虽然 802.11n 修正案也定义了 OFDM 信道，但是 HT(条款 20)无线接口与传统无线接口的差别很大。如前所述，HT 无线接口可以使用 2.4GHz 和 5GHz 两个频段收发数据。

前面曾经介绍过，802.11n 无线接口采用空间复用发送多路独立的数据流，空间复用是提高吞吐量的方式之一。802.11n OFDM 利用了更多子载波，而且可以支持信道绑定。HT 条款 20 使用的 OFDM 信道的带宽更宽，这同样有助于提高总吞吐量。

18.3.1　20MHz HT 与 20MHz Non-HT 信道

第 6 章曾经介绍过，802.11a/g 无线接口使用 20MHz OFDM 信道进行通信。如图 18-6 所示，每个 20MHz Non-HT 信道由 52 个 OFDM 副载波构成。其中 48 个副载波用于传输数据，另外 4 个副载波作为导频音，用于发射机和接收机之间的动态校准。此外，OFDM 技术还采用卷积编码与前向纠错技术。

图 18-6　20MHz Non-HT(802.11a/g)信道

HT(条款 20)无线接口采用与 802.11a/g 无线接口相同的 OFDM 技术，不过它既可以使用 20MHz 信道、也可以使用 40MHz 信道传输数据。与 Non-HT OFDM 信道相比，HT 无线接口使用的 20MHz HT 信道包括 4 个额外的副载波，因而可以传输更多数据。也就是说，在同样的频率空间内，使用 20MHz HT 信道能获得更大的总吞吐量。如图 18-7 所示，每个 20MHz HT 信道由 56 个 OFDM 副载波构成。其中 52 个副载波用于传输数据，另外 4 个副载波作为导频音，用于发射机和接收机之间的动态校准。

图 18-7　20MHz HT(802.11n)信道

18.3.2 40MHz HT 信道

除 20MHz OFDM 信道之外，HT(条款 20)无线接口也可使用 40MHz OFDM 信道。如图 18-8 所示，每个 40MHz HT 信道由 114 个 OFDM 副载波构成。其中 108 个副载波用于传输数据，另外 6 个副载波作为导频音，用于发射机和接收机之间的动态校准。使用 40MHz 信道可将数据传输频率带宽增加一倍。

图 18-8 40MHz HT(802.11n)信道

HT 无线接口使用的 40MHz 信道实际由两个 20MHz OFDM 信道绑定而成。每个 40MHz 信道包括一个 20MHz 主信道(primary channel)和一个 20MHz 次信道(secondary channel)，二者在频率上必须相邻。图 18-9 显示了构成 40MHz 信道的两个 20MHz 信道，它们被划分为主信道与次信道，并通过 802.11 管理帧帧体中的两个字段加以标识。主字段标明了主信道的信道号，正偏移表示次信道在频率上比主信道高一个信道，负偏移表示次信道在频率上比主信道低一个信道。

```
Additional HT Information
  Element ID:            61  Additional HT Information
  Length:                22
  Primary Channel:       36
  Srvc Int Granularity:  %000  5ms
  PSMP STAs Only:        %0  Association Requests are Accepted Regardless of PSMP Capability
  RIFS Mode:             %0  Use of RIFS Prohibited
  STA Channel Width:     %1  Use Any Channel Width Enabled Under Supported Channel Width Set
  2nd Channel Offset:    %01  Above the Primary Channel
```

图 18-9 信道绑定

标准的 20MHz HT 信道会在信道两端保留一定的带宽以避免邻道干扰。但是，当两个 20MHz HT 信道绑定在一起时，就不必在两个信道的边缘保留这种保护性带宽。换句话说，40MHz HT 信道可以使用全部 114 个(而不是 112 个)副载波。

第 12 章曾经介绍过，在多信道架构(MCA)中需要规划信道复用模式。由于 5GHz UNII 频段的信道组合非常灵活，因此在该频段部署 40MHz 信道较为可行。如图 18-10 所示，5GHz 频段总共包括 24 个 20MHz 信道，这些信道可以通过各种方式绑定在一起。也就是说，在 5GHz 频段规划 40MHz HT 信道无疑是最佳选择。

图 18-10　信道绑定：5GHz UNII 频段

与之相反，多信道架构不支持在 2.4GHz 频段部署 40MHz HT 信道。前面的章节曾经介绍过，尽管 2.4GHz ISM 频段包括 14 个信道，但是只能找到 3 个互不重叠的 20MHz 信道。如图 18-11 所示，无论采用何种方式在 2.4GHz 频段进行信道绑定，任意两个 40MHz 信道都会相互重叠。换句话说，2.4GHz ISM 频段只存在一个 40MHz 信道，在该频段根本无法规划信道复用。

图 18-11　信道绑定：2.4GHz ISM 频段

18.3.3　40MHz 不兼容

我们知道，只有一个不重叠 40MHz 通道可以部署在 2.4GHz 频段。因此在 2.4GHz 使用多个 40MHz 频道的信道复用模式是不可能的。但是，仍有可能在 2.4GHz 频带开启信道绑定。使用 40MHz 信道的 2.4GHz 接入点会对已部署了标准 1、6 和 11 的 20MHz 信道复用模式的附近 AP 产生干扰。默认情况下，802.11 n 客户端和 AP 在 2.4GHz 频带传输时，只使用

20MHz 频道，而且会通过各种 802.11 n 管理帧宣告它们不兼容 40MHz 的使用。如果任何使用 40MHz 信道的 802.11 n AP 接收到周围 802.11n 2.4GHz 客户端发送的 40MHz 不兼容的管理帧，将被迫切换回只有使用 20MHz 信道。

40MHz 不兼容是针对你的隔壁邻居可能部署 40MHz 信道，并对你的 2.4GHz 的 20MHz 信道的保护。企业无线局域网接入点在 2.4GHz 的默认设置总是 20MHz 信道。请注意，40MHz 不兼容只适用于 2.4GHz，并不适用于 5GHz。

18.3.4 保护间隔

在数字通信中，数据以比特的形式被调制到载波信号上，这些比特称为符号。802.11a/g 无线接口以 54Mbps 的速率传输数据时，每个 OFDM 符号包含 288 个比特，其中 216 个比特为原始数据，另外 72 个比特属于纠错比特。OFDM 符号包含的所有数据比特通过 20MHz Non-HT 信道中的 48 个数据副载波传输。

802.11a/g 无线接口在 OFDM 符号之间采用长度为 800ns 的保护间隔(Guard Interval，GI)。保护间隔是两个符号之间的一段空白时间，用于补偿沿较长路径到达接收机的符号所引起的延迟。多径效应导致符号沿不同路径传输，它们到达接收机的时间各不相同。在前一个符号被接收机完全接收之前，后一个符号可能已经到达接收机。这种现象称为码间干扰(InterSymbol Interference，ISI)，它往往会造成数据损坏。

前面的章节曾经介绍过码间干扰与时延扩展(delay spread)。同一信号沿不同路径传输所形成的时间差称为时延扩展，其时长一般在 50ns～100ns 之间，最大约为 200ns。为保证通信质量，保护间隔应为时延扩展的 2～4 倍。可将保护间隔视为时延扩展的缓冲，符号传输之间的保护间隔通常为 800ns。如图 18-12 所示，保护间隔不仅能补偿时延扩展，也有助于避免码间干扰，而保护间隔过短将导致码间干扰。

图 18-12 保护间隔

802.11n 既可以采用 800ns 保护间隔，也可以采用较短的 400ns 保护间隔，后者属于可选设置。采用较短的保护间隔能缩短符号时间，数据速率将因此提高 10%左右。当 802.11n 无线接口采用可选的较短 400ns 保护间隔时，虽然吞吐量有所提高，但发生码间干扰的概率也将随之增加，从而增加数据损坏的概率。数据损坏将引发第二层重传，后者会导致吞吐量降低。有鉴于此，应仅在射频环境较好时采用 400ns 保护间隔。如果采用较短的保护间隔导致吞吐量下降，则应改用默认的保护间隔设置(800ns)。

18.3.5　调制编码方案

802.11n 修正案通过调制编码方案(modulation and coding scheme，MCS)定义数据速率。采用 OFDM 技术的 Non-HT 无线接口(802.11a/g)根据所用的调制方式定义数据速率(6Mbps～54Mbps)，而 HT 无线接口根据调制方式、编码方式空间流数量、信道宽度、保护间隔等多种参数定义数据速率，调制编码方案是这些参数的不同组合。20MHz HT 与 40MHz HT 信道一共存在 77 种调制编码方案。如表 18-2 所示，802.11n 修正案为 20MHz HT 信道定义了 8 种强制的调制编码方案，它们相当于 Basic Rate(基本速率)。

表 18-2　强制的调制编码方案(20MHz 信道)

MCS 指数	调制方式	空间流数量	数据速率	
			800ns 保护间隔	400ns 保护间隔
0	BPSK	1	6.5Mbps	7.2Mbps
1	QPSK	1	13.0Mbps	14.4Mbps
2	QPSK	1	19.5Mbps	21.7Mbps
3	16-QAM	1	26.0Mbps	28.9Mbps
4	16-QAM	1	39.0Mbps	43.3Mbps
5	64-QAM	1	52.0Mbps	57.8Mbps
6	64-QAM	1	58.5Mbps	65.0Mbps
7	64-QAM	1	65.0Mbps	72.2Mbps

从表 18-2 中可以观察到，调制方式、保护间隔与空间流数量都会影响最终的数据速率。表 18-3 列出了采用 20MHz 信道、4 路空间流时的调制编码方案。

表 18-3　调制编码方案(20MHz 信道、4 路空间流)

MCS 指数	调制方式	空间流数量	数据速率	
			800ns 保护间隔	400ns 保护间隔
24	BPSK	4	26.0Mbps	28.9Mbps
25	QPSK	4	52.0Mbps	57.8Mbps
26	QPSK	4	78.0Mbps	86.7Mbps
27	16-QAM	4	104.0Mbps	115.6Mbps
28	16-QAM	4	156.0Mbps	173.3Mbps
29	64-QAM	4	208.0Mbps	231.1Mbps
30	64-QAM	4	234.0Mbps	260.0Mbps
31	64-QAM	4	260.0Mbps	288.9Mbps

表 18-4 列出了采用 40MHz 信道、1 路空间流时的调制编码方案。

表 18-4 调制编码方案(40MHz 信道、1 路空间流)

MCS 指数	调制方式	空间流数量	数据速率	
			800ns 保护间隔	400ns 保护间隔
0	BPSK	1	13.5Mbps	15.0Mbps
1	QPSK	1	27.0Mbps	30.0Mbps
2	QPSK	1	40.5Mbps	45.0Mbps
3	16-QAM	1	54.0Mbps	60.0Mbps
4	16-QAM	1	81.0Mbps	90.0Mbps
5	64-QAM	1	108.0Mbps	120.0Mbps
6	64-QAM	1	121.5Mbps	135.0Mbps
7	64-QAM	1	135.0Mbps	150.0Mbps

表 18-5 列出了采用 40 MHz 信道、4 路空间流时的调制编码方案。

表 18-5 调制编码方案(40MHz 信道、4 路空间流)

MCS 指数	调制方式	空间流数量	数据速率	
			800ns 保护间隔	400ns 保护间隔
24	BPSK	4	54.0Mbps	60.0Mbps
25	QPSK	4	108.0Mbps	120.0Mbps
26	QPSK	4	162.0Mbps	180.0Mbps
27	16-QAM	4	216.0Mbps	240.0Mbps
28	16-QAM	4	324.0Mbps	360.0Mbps
29	64-QAM	4	432.0Mbps	480.0Mbps
30	64-QAM	4	486.0Mbps	540.0Mbps
31	64-QAM	4	540.0Mbps	600.0Mbps

其他因素(如采用非平等调制)也会影响最终的数据速率。如表 18-6 所示，也可以采用不同的调制方式(非平等调制)对空间流进行调制。

表 18-6 调制编码方案(40MHz 信道、4 路空间流、非平等调制)

调制方式					数据速率	
MCS 指数	空间流 1	空间流 2	空间流 3	空间流 4	800ns 保护间隔	400ns 保护间隔
67	16-QAM	16-QAM	16-QAM	QPSK	283.4Mbps	315.0Mbps
68	64-QAM	QPSK	QPSK	QPSK	243.0Mbps	270.0Mbps

18.4 HT 物理层

前面的章节曾经介绍过，MSDU(MAC Service Data Unit，MAC 服务数据单元)指 802.11 数据帧的 3～7 层净荷，而 MPDU(MAC Protocol Data Unit，MAC 协议数据单元)在技术上指整个 802.11 帧。MPDU 由二层帧头、帧体与帧尾构成。

MPDU(802.11 帧)从数据链路层传输到物理层时，将被添加前导码(preamble)与物理层报头，封装后的 MPDU 称为 PPDU(PLCP Protocol Data Unit，PLCP 协议数据单元)。需要注意的是，CWNA 考试不会考查前导码与物理层报头的细节。前导码主要用于在物理层同步两个 802.11 无线接口之间的传输，而传输 802.11 帧(MPDU)所需的时间通过物理层报头中的信号字段加以标识。802.11n 修正案定义了 3 种 PPDU 结构，它们分别使用 3 种不同的前导码。其中一种前导码属于传统格式，另外两种前导码属于 HT 格式。

18.4.1　Non-HT 传统格式

第一种 PPDU 格式称为非 HT(non-HT)格式。Non-HT 格式用于 OFDM 传输，它最初定义在 802.11-2007 标准第 17 条款中，因此也称为传统格式。如图 18-13 所示，Non-HT PPDU 包括采用长短训练符号的前导码，前导码用于收发双方之间的同步。OFDM 符号由 12 个比特构成。信号字段包含在报头中，用于标明传输 Non-HT PPDU 净荷(即 MPDU)所需的时间。

图 18-13　802.11n PPDU 格式

802.11n 无线接口必须支持 Non-HT 传统格式，采用该格式的无线接口只能使用 20MHz 信道收发数据。Non-HT 格式与传统 802.11a/g 无线接口使用的格式在本质上并无区别。802.11n 射频卡在按照 non-HT 传统模式发送信息时，类似于 SISO 系统，只在单一天线上发送。但 802.11n 可利用多根天线进行数据接收，接收分集可以改善来自传统 802.11a/b/g 射频卡的入射传输。

18.4.2　HT 混合格式

802.11n 修正案定义了两种新的 PPDU 格式，第一种称为 HT 混合(HT Mixed)格式。如图 18-13 所示，HT 混合格式前导码的前一部分包含 Non-HT 格式的长短训练符号与信号字段，可以被传统的 802.11a/g 无线接口识别并解码；后一部分包含 HT 专用格式的长短训练符号与信号字段，无法被传统的 802.11a/g 无线接口识别并解码。

HT-SIG(HT-signal)包含 MCS、帧长、20MHz 或 40MHz 信道宽度、帧聚合、保护间隔和 STBC。HT-STF 和 HT-LTF 用于在 MIMO 射频卡之间进行同步。

Non-802.11n 接收方无法读取这个帧，但它在帧头的传统部分中了解该帧占用媒介的时间，从而可以保持静默等待，不必总是进行能量检测。由于 HT 混合格式支持 HT(802.11n)和 Non-HT(802.11a/g)无线接口中使用，它可能是应用最为广泛的 PPDU 格式。802.11n 无线射频卡必须强制支持 HT 混合格式，采用该格式的无线射频卡可使用 20MHz 或 40MHz 信道收发数据。使用 40MHz 信道时，所有广播流量必须通过传统的 20MHz 信道发送，以便 Non-HT(802.11a/g)客户端识别和接收。此外，与 Non-HT 客户端通信时也必须使用传统的 20MHz 信道。

18.4.3 HT 绿地格式

802.11n 修正案定义的第二种 PPDU 格式称为 HT 绿地(HT Greenfield)格式。HT 绿地格式的 802.11n 射频卡可以识别传统客户端发送的帧，但传统的 802.11a/g 无线接口无法识别 HT 绿地格式的前导码，因为传统客户端会把 HT 绿地模式传输的帧当成噪声。HT 绿地模式应用场景很少，因为环境中总是存在传统的 802.11a/b/g 客户端。

支持 HT 绿地格式并非强制要求，采用该格式的 802.11n 无线接口可使用 20MHz 或 40MHz 信道收发数据。处于这种模式，不必开启 HT 保护机制，不必使用 RTS/CTS 帧通告传统设备，因此总体吞吐量可能会表现很好。

18.5 HT MAC 层

到目前为止，我们讨论了所有物理层增强机制，802.11n 无线接口通过这些机制增加带宽并提高吞吐量。802.11n 修正案还为数据链路层的 MAC 子层定义了若干增强机制，以提高吞吐量并改进现有的电源管理机制。802.11n 修正案采用两种新的帧聚合方式以减少媒介竞争开销，并采用帧间间隔(interframe space，IFS)与块确认(block acknowledgment，BA)机制以减少固定的 MAC 开销。此外，802.11n 修正案还为 HT(条款 20)无线接口定义了两种新的电源管理方式。

18.5.1 MSDU 聚合(A-MSDU)

如图 18-14 所示，单播 802.11 帧在每次传输时都会产生一定数量的开销，这些开销包括物理层报头、MAC 帧头、MAC 帧尾、帧间间隔以及确认帧。由于每个帧都必须竞争媒介的使用权，因此媒介竞争开销同样无法避免。

图 18-14 802.11 单播帧开销

为减少开销，802.11n 修正案定义了两种新的帧聚合方式。帧聚合是一种将多个帧合并到单个帧传输中的机制。帧聚合不仅可以减少固定的 MAC 层开销并降低冲突发生的概率，还能将媒介竞争阶段使用随机退避定时器所产生的开销降至最低。

第一种帧聚合方式称为 A-MSDU(Aggregate MAC Service Data Unit，聚合 MAC 服务数据单元)。前面曾经介绍过，MSDU 是数据帧的 3～7 层净荷。如图 18-15 所示，多个 MSDU 被聚合到一个单帧。

图 18-15　MSDU 聚合(A-MSDU)

采用 MSDU 聚合的 802.11n 接入点在收到多个 802.3 帧后，首先将这些 802.3 帧的帧头和帧尾移除，然后将其中的 MSDU 净荷封装到单一 802.11 帧中进行传输。聚合后的 MSDU 是一个整体，具有唯一的目标地址。

整个聚合帧采用 CCMP 进行加密。需要注意的是，构成 A-MSDU 的各个 MSDU 的 802.11e QoS 访问类别必须相同。例如，语音 MSDU 无法与视频 MSDU 或尽力传输 MSDU 合并到同一个聚合帧中。

18.5.2　MPDU 聚合(A-MPDU)

第二种帧聚合方式称为 A-MPDU(Aggregate MAC Protocol Data Unit，聚合 MAC 协议数据单元)。前面曾经介绍过，MPDU 是包括 MAC 帧头、帧体与帧尾在内的整个 802.11 帧。如图 18-16 所示，多个 MPDU 被聚合到一个单帧。

聚合 MAC 协议数据单元 (A-MPDU)

图 18-16　A-MPDU

A-MPDU 中的所有 MPDU 必须具有相同的接收机地址。此外，可以采用 CCMP 对每个 MDPU 的数据净荷独立进行加密。与 A-MSDU 类似，构成 A-MPDU 的各个 MPDU 的 802.11e QoS 访问类别必须相同。语音 MPDU 无法与视频 MPDU 或尽力传输 MPDU 合并到同一个聚合帧中。需要注意的是，由于每个 MPDU 都有各自的 MAC 帧头和帧尾，因此 MPDU 聚合产生的开销要大于 MSDU 聚合。

单独的 MPDU 帧如果发生 CRC 校验错误，表明这个单独的 MPDU 帧被破坏，而整个 A-MPDU 不必重传。也就是说 A-MPDU 比 A-MSDU 更少受到噪声影响。大多数 WLAN 厂商都会采用 A-MPDU 技术。

18.5.3 块确认

前面的章节曾经介绍过，每个 802.11 单播帧都必须后跟一个用于传输验证目的的确认帧，但是广播帧与多播帧不必确认。A-MSDU 包含若干个 MSDU，这些 MSDU 被封装到一个单一的帧中，它们具有唯一的 MAC 帧头和目标地址。因此，只需一个普通的确认帧就可以对 A-MSDU 进行确认。由于 A-MPDU 包含若干个 MPDU，但是这些 MPDU 都有各自的 MAC 帧头。每个 MPDU 都必须经过确认，这通过 MTBA(Multiple Traffic ID Block Acknowledgment，多流量 ID 块确认)帧完成，其本质就是针对 A-MPDU 的块确认帧。块确认最初定义在 802.11e 修正案中，用于在帧突发(frame burst)中确认多个 802.11 帧。如图 18-17 所示，块确认帧(MTBA)也可以在 A-MPDU 传输中使用，以便一次性对多个聚合的 MPDU 进行确认。只用一个确认帧对多个帧或聚合帧进行确认，可以减少 MAC 层开销，从而达到提高吞吐量的目的。

图 18-17 块确认

18.5.4　缩减帧间间隔

802.11e QoS 修正案规定，发送方无线接口可在一个传输机会(transmit opportunity，TXOP)内发送多个帧。各帧之间由 SIFS(Short InterFrame Space，短帧间间隔)隔开，以确保帧突发期间只有一个无线射频卡使用媒介收发数据。802.11n 修正案定义了一种更短的帧间间隔，称为 RIFS(Reduced InterFrame Space，缩减帧间间隔)。802.11an 使用 SIFS 的长度为 16μs，802.11agn 使用的 SIFS 长度为 10μs。而更短的 RIFS 长度只有 2 μs。如果用 RIFS 取代 SIFS，则可以减少帧连续发生期间的开销。需要注意的是，RIFS 只能在 HT 绿地模式网络中使用。也就是说，只有 HT 无线接口才可以使用 RIFS，BSS 中不能存在任何传统无线设备。

18.5.5　HT 电源管理

随着 IEEE 对 802.11 标准的修订，电源管理机制也在不断完善之中。802.11e QoS 修正案定义了 U-APSD(Unscheduled Automatic Power Save Delivery，非计划自动节电交付)机制供 WMM-PS 规范使用，而 802.11n 修正案为 HT(条款 20)无线接口定义了两种新的电源管理机制。

802.11n 无线接口仍支持基本的节电模式(Power Save mode)，后者以 802.11 原始标准定义的电源管理机制为基础。在这种节电模式中，接入点将传输给客户端的帧暂时储存在自己的缓冲区里。在收到接入点广播的 DTIM(Delivery Traffic Indication Message，交付流量指示消息)信标帧之后，客户端从休眠状态转入活动状态，并从接入点处下载缓存数据。

802.11n 修正案定义了两种新的电源管理机制。第一种电源管理机制称为 SMPS(Spatial Multiplexing Power Save，空间复用节电)，该机制允许 802.11n MIMO 设备仅保留一个无线接口，关闭其他无线接口。例如，采用 4 条射频链的 4×4 MIMO 设备可以关闭其中 3 个无线接口以降低耗电量。SMPS 包括静态与动态两种工作模式。

采用静态 SMPS 的 MIMO 客户端仅保留一个无线接口，工作在这种模式的客户端与只能收发一路空间流的 802.11a/b/g 无线接口并无二致。MIMO 客户端向接入点发送 SMPS 动作帧(SMPS action frame)，通知接入点自己目前的状态(仅保留一个无线接口，仅能接收一路空间流)。当 MIMO 客户端再次启动所有无线接口后，它仍采用 SMPS 动作帧通知接入点自己目前的状态(可以收发多路空间流)。

采用动态 SMPS 的 MIMO 客户端同样仅保留一个无线接口，不过工作在这种模式的客户端能以更快的速度重新启动无线接口。在完成一个帧交换后，客户端关闭所有无线接口，仅保留一个无线接口。接入点通过 RTS 帧激活客户端处于休眠状态的无线接口。在收到 RTS 帧之后，客户端将启动处于休眠状态的无线接口，并向接入点返回 CTS 帧。此时，客户端可以再次收发多路空间流。MIMO 客户端采用 SMPS 动作帧通知接入点自己目前处于动态节电状态。

802.11n 修正案为 HT(条款 20)无线接口定义的第二种电源管理机制称为 PSMP(Power Save Multi Poll，节电多次轮询)，PSMP 是对 APSD(定义在 802.11e 修正案中)的扩充。U-PSMP(非计划节电多次轮询)类似于 U-APSD(非计划自动节电交付)，二者使用相同的交付启用与触发

启用机制。S-PSMP(计划节电多次轮询)可以有效传输流数据与其他计划应用，它在功能上与 S-APSD(计划自动节电交付)非常类似。

18.6 HT 工作模式

802.11n 接入点支持多种信道工作模式。虽然大部分 802.11n 接入点都支持 20/40BSS 通信，但是也可以将其手动配置为仅使用传统的 20MHz 信道收发数据。在 20/40BSS 中，支持 20MHz 通信的 802.11a/g 客户端与支持 20/40MHz 通信的 802.11n 客户端可以共存于同一蜂窝。前面的章节曾介绍过 802.11g ERP 网络的保护机制，即采用 RTS/CTS 与 CTS-to-Self 以确保 802.11b HR-DSSS 客户端不会对 ERP-OFDM 通信造成干扰。802.11n 无线接口必须保持与传统无线接口 802.1a/b/g 的兼容性。有鉴于此，802.11n 修正案定义了 HT 保护模式，以便 HT(条款 20)无线接口向后兼容 HR-DSSS(条款 18)、OFDM(条款 17)与 ERP(条款 19)无线接口。

18.6.1 20/40MHz 信道工作模式

与 HT 接入点建立关联的 20MHz 802.11a/g 客户端和 20/40MHz 802.11n 客户端可在同一蜂窝共存。传统的 802.11a/g 客户端显然只能使用 20MHz 信道收发数据。802.11n 射频卡可以工作在 20MHz 或 20/40MHz 信道模式。具备 20/40MHz 能力的 802.11n 无线射频卡之间用 40MHz 信道相互通信，与传统客户端通信使用 20MHz 信道。为保证同一个 20/40 HT BSS 中的 20MHz 与 40MHz 设备不会相互干扰，必须遵循以下原则：

- 802.11n 接入点必须在信标帧中声明自己支持的信道工作模式(20MHz 或 20/40 MHz)。
- 802.11n 客户端必须在关联帧或重关联帧中声明自己支持的信道工作模式(20MHz 或 20/40MHz)。
- 客户端在 20-only 或 20/40 AP 之间切换时，必须与接入点进行重关联。
- 当 20/40MHz 设备使用 20MHz 信道进行通信时，必须使用主信道而不是次信道。

18.6.2 HT 保护模式(0～3)

为确保向后兼容早期的 802.11a/b/g 无线接口，HT 接入点可能会通知其他 HT 客户端何时启用相应的 HT 保护模式。信标帧中有一个称为 HT Protection 的字段，后者包含 4 种可能的设置(0～3)。与 ERP 接入点类似，HT 接入点将根据客户端的实际情况(位于接入点附近尚未关联或已与接入点建立关联)动态调整所用的保护机制，可供选择的保护机制包括 RTS/CTS、CTS-to-Self、双 CTS 以及其他一些保护机制。4 种 HT 保护模式如下：

模式 0：绿地模式 该模式之所以被称为绿地模式，是因为网络中只存在 HT 无线设备。所有 HT 客户端必须具备相同的工作特性。也就是说，如果 HT BSS 为 20 MHz BSS，则所有客户端必须支持 20MHz 通信；如果 HT BSS 为 20/40 MHz BSS，则所有客户端必须支持 20/40 MHz 通信。假如上述条件得到满足，则不必启用保护机制。

模式 1：HT 非成员保护模式 在该模式中，BSS 中只存在 HT 客户端。如果 HT 接入点

监听到 Non-HT 客户端或接入点出现，则将触发保护机制。例如，当 HT 接入点与客户端使用 40MHz HT 信道相互通信时，HT 接入点检测到网络中出现了一个 802.11a 接入点或客户端，该 Non-HT 设备使用 20MHz 信道收发数据。由于这可能干扰到 HT 设备正在使用的 40MHz HT 信道(主信道或次信道)，因此 HT 接入点将启用保护机制。

模式 2：HT 20 MHz 保护模式　在该模式中，BSS 中只存在 HT 客户端，它们与 20/40MHz 接入点建立关联。如果一个只支持 20MHz 通信的 HT 客户端与 20/40MHz 接入点建立关联，则将触发保护机制。换句话说，使用 40MHz 信道收发数据时，20/40MHz HT 设备必须启用保护机制，以防 20 MHz HT 设备在同一时间占用媒介而产生冲突。

模式 3：HT 混合模式　该模式用于一个或多个 Non-HT 客户端与 HT 接入点建立关联的情况。HT BSS 既可以是 20MHz BSS，也可以是 20/40MHz BSS。如果 HR-DSSS(条款 18)、OFDM(条款 17)或 ERP(条款 19)无线接口连接到 HT BSS，将触发保护机制。由于大部分 BSS 中都可能存在传统设备，因此 HT 混合模式或许是应用最广泛的保护模式。

18.6.3　RTS/CTS 与 CTS-to-Self

HT BSS 启用 HT 保护机制时，HT STA 会向被保护客户端发送可以理解的 RTS/CTS 或 CTS-to-Self 控制帧。控制帧中的 Duration-ID 促使客户端更其网络分配向量(NAV)。40MHz 的 HT 在对传统 802.11a 或 802.11g 客户端进行传输保护时，可以在其主信道和次信道同时发送 Non-HT 控制帧。如图 18-18。

图 18-18　non-HT 复制格式

Non-HT 复制传输在 5GHz 以 802.11a 数据率发送，在 2.4GHz 按 802.11g 数据率发送。图 18-18 中，可以看到 non-HT 复制传输同时在相邻的两个 20MHz 信道(52 个子载波)发送相同的数据。这会导致在主信道和次信道的客户端都会更新 NAV 并延迟传输。Non-HT 重复模式可以改善错误率，但并未在 WLAN 厂商产品中大范围部署。

18.7 小结

这一章介绍了 802.11n 修正案的发展历史以及 Wi-Fi 联盟业已实施的 802.11n 互操作性认证测试。我们讨论了 HT(条款 20)无线接口使用的各种物理层增强机制，这些机制能提高吞吐量并扩大传输范围。此外，802.11n 修正案还为 HT 无线接口定义了 MAC 子层增强机制，以提高吞吐量并改进现有的电源管理机制。这一章最后介绍了 HT 保护机制以及相应的工作模式，采用保护机制可以确保传统的 802.11a/b/g 设备与 802.11n 设备在同一蜂窝中共存。802.11n 技术能有效提高吞吐量并扩大传输范围，它被业界视为下一代无线局域网技术。虽然 802.11n 刚刚在企业部署中崭露头角，但是随着时间的推移，该技术的前途不可限量。

18.8 考试要点

定义 MIMO 与 SISO 技术的区别。理解 SISO 设备仅使用一条射频链，而 MIMO 系统使用多条射频链。

理解空间复用。描述空间复用如何利用多径效应发送多路空间流以提高吞吐量。

解释 MIMO 分集。解释简单交换分集技术与 MIMO 天线系统使用的高级分集技术之间的区别。解释 MIMO 分集使用的最大比合并技术。

理解传输波束成形。解释波束成形技术(802.11n 修正案定义的可选智能天线技术)如何控制波束沿最佳路径传输给接收方无线接口，并理解这种技术的优点。

理解 20MHz 与 40MHz 信道。理解传统的 20MHz 信道、20MHz HT 信道与 40MHz HT 信道的性质，并了解 OFDM 技术在上述信道中的应用。解释为何在 5GHz UNII 频段部署 40MHz 信道可以获得最佳效果。解释主信道与次信道。

解释保护间隔。解释保护间隔减小码间干扰的原理，并描述 800ns 与 400ns 保护间隔的用途。

理解调制编码方案。解释如何采用调制编码方案定义数据速率，理解所有影响数据速率的参数。

解释 3 种 HT PPDU 格式。描述 Non-HT 传统格式、HT 混合格式与 HT 绿地格式的区别。

理解 HT MAC 子层增强机制。解释 A-MSDU、A-MPDU、块确认、RIFS 等 MAC 子层增强技术如何提高吞吐量。描述 802.11n 修正案为 HT 无线接口定义的两种新的电源管理方式。

解释 HT 保护模式。描述 4 种 HT 保护模式的区别。解释 Dual-CTS 的使用。

18.9 复习题

复习题的答案见附录 A。

1. A WLAN consultant has been asked to plan an 802.11n deployment using dual-frequency 3 ￥ 3:3 access points. What are the options available to provide power for the 802.11n access points?

(Choose all that apply.)

A. 802.3af PoE

B. 802.3at PoE

C. Proprietary PoE solution

D. Battery pack

E. Electrical outlet power

2. How can a MIMO system increase throughput at the Physical layer? (Choose all that apply.)

A. Spatial multiplexing

B. A-MPDU

C. Transmit beamforming

D. 40MHz channels

E. Dual-CTS protection

3. Which new power-management method defined by the 802.11n amendment conserves power by powering down all but one radio?

A. A-MPDU

B. Power Save protection

C. PSMP

D. SM power save

E. PS mode

4. The guard interval is used as a buffer to compensate for what type of interference?

A. Co-channel interference

B. Adjacent cell interference

C. RF interference

D. HT interference

E. Intersymbol interference

5. Name some of the factors that a modulation and coding scheme (MCS) uses to define data rates for an HT radio. (Choose all that apply.)

A. Modulation method

B. Equal/unequal modulation

C. Number of spatial streams

D. GI

E. Channel size

6. How can an HT radio increase throughput at the MAC sublayer of the Data-Link layer? (Choose all that apply.)

A. A-MSDU

B. RIFS

C. A-MPDU

D. Guard interval

E. MTBA

7. Explicit transmit beamforming uses what type of frames to analyze the MIMO channel before transmitting directed paths of data?

A. Trigger frames

B. Beaming frames

C. Sounding frames

D. SM power save action frames

8. A 3¥3:2 MIMO radio can transmit and receive how many unique streams of data?

A. Two.

B. Three.

C. Four.

D. Three equal and four unequal streams.

E. None—the streams are not unique data.

9. Name a capability not defined for A-MPDU.

A. Multiple QoS access categories

B. Independent data payload encryption

C. Individual MPDUs have the same receiver address

D. MPDU aggregation

10. Which HT protection modes allow only for the association of HT stations in the HT basic service set? (Choose all that apply.)

A. Mode 0—Greenfield mode

B. Mode 1—HT nonmember protection mode

C. Mode 2—HT 20MHz protection mode

D. Mode 3—HT Mixed mode

11. Which of these capabilities are considered mandatory for an 802.11n access point as defined by the Wi-Fi Alliance's vendor certification program called Wi-Fi CERTIFIED n? (Choose all that apply.)

A. Three spatial streams in receive mode

B. WPA/WPA2

C. WMM

D. Two spatial streams in transmit mode

E. 2.4GHz–40MHz channels

12. MIMO radios use which mechanisms for transmit diversity? (Choose all that apply.)

A. Maximum ratio combining (MRC)

B. Spatial multiplexing (SM)

C. Space-time block coding (STBC)

D. Cyclic shift diversity (CSD)

E. Multiple traffic ID block acknowledgment (MTBA)

13. HT clause 20 radios are backward compatible with which of the following type of 802.11 radios? (Choose all that apply.)

A. Clause 18 radios (HR-DSSS)

B. Clause 17 radios (OFDM)

C. Clause 14 radios (FHSS)

D. Clause 19 radios (ERP)

14. How does Transmit beamforming (TxBF) use multiple MIMO antennas to increase range?

A. Beamsteering

B. Phase shifting

C. Dynamic beamforming

D. Spatial multiplexing

15. Which HT PPDU formats support both 20MHz and 40MHz channels? (Choose all that apply.)

A. Non-HT legacy format

B. PCO mode

C. HT Mixed format

D. HT Greenfield format

16. A WLAN consultant has recommend that a new 802.11n HT network be deployed by using channels in the 5GHz UNII bands. Why would he recommend 5GHz over 2.4GHz?

A. HT radios do not require DFS and TPC in the 5GHz bands.

B. HT radios get better range using TxBF in the 5GHz bands.

C. 40MHz channels do not scale in the 2.4GHz ISM band.

D. 5GHz HT radios are less expensive than 2.4GHz HT radios.

17. What 802.11n mode of operation sends the same data on two adjacent 20MHz channels?

A. Greenfield mode

B. HT Mixed mode

C. Non-HT duplicate mode

D. LDPC mode

18. What frequencies are defined for clause 20HT radio transmissions? (Choose all that apply.)

A. 902–928MHz

B. 2.4–2.4835GHz

C. 5.15–5.25GHz

D. 5.25–5.35MHz

19. What PHY layer mechanism might be used to increase throughput for an HT radio in a clean RF environment with minimal reflections and low multipath?

A. Maximum ratio combining

B. 400-nanosecond guard interval

C. Switched diversity

D. Spatial multiplexing

E. Spatial diversity

20. What PHY layer mechanisms might be used to increase the range for an 802.11n radio using a MIMO system? (Choose all that apply.)

A. Maximum ratio combining

B. Guard interval

C. Transmit beamforming

D. Spatial multiplexing

附录 A 复习题答案

第 1 章

1. C。802.11 无线网络一般用于为客户端提供网络接入，客户端通过接入点访问网络资源。自治接入点与轻量接入点部署在访问层而不是核心层或分布层。物理层属于 OSI 模型，不属于网络架构模型。

2. E。不同国家和地区对射频通信的管理各不相同，本地监管机构负责制定所在国家或地区的频谱使用政策与传输功率规定。

3. B。802.11 无线桥接链路一般在分布层服务中使用。核心层设备的速度通常比 802.11 无线设备更快，因此无线网桥并非用来提供访问层服务。网络层属于 OSI 模型，不属于网络架构模型。

4. A。IEEE(电子与电气工程师协会)负责制定所有 802 标准。

5. D。Wi-Fi 联盟负责提供认证测试。Wi-Fi 设备通过测试后，将获得一张 Wi-Fi 互操作性证书。

6. C。载波信号是用于传输二进制数据的调制信号。

7. B。由于噪声对信号幅度的影响，采用幅移键控(ASK)时必须谨慎。

8. C。IEEE 802.11-2007 标准仅在 OSI 模型的物理层与数据链路层的 MAC 子层定义了通信机制。数据链路层的 LLC(逻辑链路控制)子层并未定义在 802.11-2007 标准中。WPA 是一种安全认证，而 FSK 是一种调制方式。

9. E。IETF 负责创建 RFC 文档。IEEE 标准负责 802.11 标准。Wi-Fi 联盟负责认证测试。Wi-Fi 联盟以前被称为 WECA，于 2002 年改为现在的名字。FCC 负责美国的射频监管。

10. D。WMM(Wi-Fi 多媒体)是 Wi-Fi 联盟的一种认证项目，启用 WMM 的 Wi-Fi 网络将各种应用产生的流量划分为不同的优先级。802.11-2007 属于 IEEE 标准，它定义了 WEP(有线等效加密)。802.11i 是 IEEE 的修正案，其定义了 RSN(强健安全网络)，但并不属于 802.11-2007 标准。PSK(相移键控)不是标准，而是一种编码技术。

11. A、B、C。3 种用于编码数据的键控法是幅移键控(ASK)、频移键控(FSK)和相移键控(PSK)。

12. B、E。IEEE 802.11-2007 标准仅在 OSI 模型的物理层与数据链路层的 MAC 子层定义了通信机制。

13. C。高度或能量是描述波幅度的两个术语。频率衡量了波重复自身的快慢程度。波长是波的实际长度，一般为两个波峰之间的距离。相位描述了两个波起始点之间的关系。

14. B。Wi-Fi Direct 被设计用来轻松连接无线网络设备。不存在 Wi-Fi personal。802.11n 可能被用来提供连接，但是设置的复杂性与否依赖于环境。CWG-RF 被设计为集成 WIFI 和蜂窝电话功能的手持设备服务。WPS 被设计用来简化安全设置。

15. D。载波信号是用于传输数据的调制信号。

16. A、B、C、D、E。各国和各地区的射频监管机构对所有选项描述的内容进行监督和管理。

17. B、E。Wi-Fi 联盟维护用于确保厂商互操作性的认证项目。Voice Personal 是其中一种认证项目，它定义了如何为家庭和小型企业的 Wi-Fi 网络提供增强的语音应用。WMM-PS

也是一种认证项目，它定义了节电机制，后者对客户设备 Wi-Fi 无线接口处于休眠状态的时间进行管理，以达到延长设备电池续航能力的目的。

18. D。一个波的完整周期为 360°。

19. B、C。任何人都可以免费使用无需牌照的频段传输数据。尽管无需付费，用户仍然需要遵守各种传输规定和限制。由于无需牌照的频段对所有人开放，这将导致频段拥挤。

20. C。OSI 模型有时又称为七层模型。

第 2 章

1. B、C。多径可能导致信号衰减、信号放大和信号丢失或数据损坏。如果两个信号按照同相方式一起到达，信号强度会增加，称为信号增强(upfade)。时延扩展可能导致数据比特受损，从而导致过度的第 2 重传。

2. D。波长是一个周期的波形在两个波峰或两个波谷之间的线性距离。

3. B、C、E。射频放大器通过外部电源的帮助引入有源增益。无源增益通常由天线通过信号集中获得，无需外部电源。无源增益也可能由信号增强(upfade)引入，这是多径现象可能产生的影响。

4. A。对每秒钟产生周期的次数的标准测量数值称为赫兹(Hz)。1Hz 指一秒钟传播一个周期。

5.D。衍射经常和折射混淆，衍射传播是指波在障碍物前方周围弯曲。衍射通常是由于射频信号被局部阻碍所致，例如在射频发射端和接收端存在一座小山或者建筑物。

6. F。当多路射频信号在接收端与主信号同时到达且呈 180° 相位差，可能导致信号消失。

7. B、C。当多路射频信号同时到达接收方且与主波同相或局部异相，结果会导致信号强度(振幅)增加。然而，请理解，由于自由空间路径损耗，无论受到增强还是减弱的影响，最终的接收信号不会比原始发送信号强。

8. B。 802.11 无线局域网工作在 5GHz 和 2.4GHz 频率范围，每秒振动 2.4×10^9 次为 2.4 GHz，每秒振动 2.4×10^6 次为 2.4 MHz。

9. A。示波器是一个测试信号振幅随时间改变的时域计工具。频域计工具被称为频谱分析仪，常在现场勘测使用。

10. A、C、D。这是一道很难回答的问题，因为许多相同的媒介可能导致不同的传播行为。金属总会导致反射。水是导致射频吸收的主要根源，但是，大片的水域也可能导致反射。平坦的表面(如柏油马路、天花板和墙)也会导致折射行为。

11. A、B、C、D。多径是一种传播现象，指两路或多路信号同时或相差极短时间到达接收天线。波的自然扩展，反射、散射、折射或衍射都可能导致同一信号发生多径现象。反射通常被认为是产生高多径环境的主要原因。

12. B。散射是指射频信号遭遇不平坦表面在多个方向进行反射。

13. A、B、C。 强多径环境会对传统 802.11a/b/g 网络噪声破坏性的影响，对于使用 MIMO 和 MRC 技术的 802.11n 传输来说，多径现象具有建设性的影响。多径与 802.11i 定义的安全机制无关。

14. A、B、C、D。空气分层是导致射频折射的首要原因。空气温度和空气压力的变化以

及水蒸气是产生折射的原因。雾会导致空气压力及密度发生变化，也会导致空气湿度增加。

15. A、D。由于波前的自然扩展，电磁信号从发射端离开后，振幅就会减小。自由空间路径损耗的比例是基于对数而非线性。射频信号通过不同媒介时会衰减，但这不是 FSPL 的作用。

16. D。由于反射信号需要传输更长的路径导致的时间差称为时延扩展。这种时延扩展会导致码间干扰，从而导致数据损坏和第 2 层重传。

17. C。频谱分析仪是频域计工具，用来在限定的频谱上测试振幅的大小。示波器是时域计工具。

18. A、C。砖墙因为材质密度较高，会严重影响 2.4GHz 和 5GHz 信号。由于人体主要由水分构成，因此高密度的人群会对射频信号产生吸收，由此产生信号问题。石膏板墙会导致信号衰减，但并非是因为水、煤渣砖或其他密实媒介的影响。空气温度对室内现场勘测没有影响。

19. A。频率与波长之间存在一个反比关系。射频信号频率越高，波长越短，波长越长，频率越低。

20. A。折射是指射频信号穿越媒介时产生弯曲。

第 3 章

1. C。发射机产生交流信号，并使用某种调制技术对数据进行信号编码。

2. E。各向同性辐射体也称为点源。

3. A、 B、 C、 E、 F。部署无线网络时的链路预算就是指从发射机开始通过射频媒介直到接收机之间的所有增益和衰减的总和。链路预算计算包括原始传输增益和天线的被动增益。所有的损失部分也需要包含在内，包括自由空间路径损耗。频率和距离是用来计算 FSPL 的必要参数。天线高度在计算链路预算时没有作用。

4. A、D。IR 是主动辐射器的缩写，IR 组件包括发射机、所有馈线电缆、连接头、发射机与天线之间的其他设备(包括接地柱、避雷器、放大器、衰减器等等)。IR 功率在天线输入的接头处测量。

5. A。等效各向同性辐射功率，也称为 EIRP，是天线辐射信号的最大测量值。

6. A、B、D。W、mW 和 dBm 都是绝对功率测量单位。1W 相当于 1 伏特电压下的 1 安培电流。1mW 相当于 1/1000W。dBm 是相对于 1mW 的分贝值。

7. B、C、D、E。贝尔(bel)是一种对功率变化的相对表达方式。1 分贝(dB)等于贝尔的十分之一。天线增益用 dBi 和 dBd 表达。dBi 被定义为相对于各向同性辐射体的分贝值(相对增益)。dBd 被定义为相对于偶极天线的分贝值(相对增益)。

8. C。dBd 转换为 dBi，只要在 dBd 值上增加 2.14 即可。

9. A。转换成 mW，首先观察 23 由多少个 10 与 3 构成，即 0+10+10+3。.要计算 mW 值，只要乘 1×10×10×2，即 200mW。

10. C。要得到 100mW，需要使用数字 10 和 2 及乘除法。乘两次 10 就可以得到 100mW。这意味着在 dBm 侧，你必须增加两次 10，即 20dBm。再减去 3dB 的电缆衰减，得到 17dBm。

因为在 dBm 侧减 3，100mW 必须除以 2，即 50mW。再增加 16dBi 的天线增益，相当于在 dBm 侧增加一次 10 和两次 3，得到的总 dBm 为 33。所以在 mW 栏乘一次 10，并乘两次 2，即 2000mW 或 2W。因为电缆和链接衰减是 3dB，而天线增益是 16dBi，两者叠加就得到 13dB，将此增益应用到 100mW，便可以计算得到 EIRP 值为 2000mW 或 2W。

11. A。如果原始发射功率为 400mW，电缆衰减为 9dB，那么电缆末端处功率将变为 50mW。第一个 3dB 衰减使绝对功率除 2 得到 200mW，第二个 3dB 衰减使绝对功率除 2 得到 100mW，第三个 3dB 衰减使绝对功率除 2 得到 50mW，19dBi 天线被动增益使信号强度增加到 4000mW。第一个 10dB 使绝对功率乘 10 得到 500mW，接下来 9dBi 的天线增益使信号加倍三次，得到 4W。因为电缆和链接衰减是 9dB，而天线增益是 19dBi，两者叠加就得到 10dB，将此增益应用到 400mW，便可以计算得到 EIRP 为 4000mW 或 4W。

12. B、D。RSSI 阀值是客户端决定是否启动漫游进程的关键因素。RSSI 阀值也由供应商用于实施动态速率切换。动态速率切换是指 802.11 无线客户端进行数据率切换的过程。

13. A。接收信号强度指示(RSSI)是 802.11 无线网卡测量信号强度(振幅)的指标。有些供应商使用私有的 RSSI 数值范围标明信号的质量。大部分供应商把信号质量定义为信噪比(SNR)。信噪比简单来说就是接收信号与背景噪声(本底噪声)的差值。

14. B。dBi 定义为“相对于各向同性辐射体的相对增益”或“与天线相关的功率变化”。dBi 是最常用的天线增益测量单位。

15. A、F。10 与 3 的四条规则如下：每提高 3dB 的增益(相对值)，绝对功率增加一倍(mW)。每产生 3dB 的损耗(相对值)，绝对功率减半(mW)。每提高 10dB 增益(相对值)，绝对功率乘 10(mW)。每产生 10dB 的损耗(相对值)，绝对功率除 10(mW)。

16. B。如果原始发射功率为 100mW，电缆损耗为 3dB，电缆末端的功率为 50mW。每提高 3dB 损耗(相对值)，绝对功率减半(mW)，即 50mW。具有 10dBi 增益的天线将信号增加到 500mW。7dBi 的天线增益，相当于加 10 再减 3，功率乘 10 再除 2，便得到 250mW。

17. D。100m 的距离会产生 80dB 的自由空间路径损耗，远远高于其他射频组件的影响。射频组件(如连接头、防雷器和馈线电缆)都会产生插入损耗。然而，FSPL 总是信号衰减的最大因素。

18. B。6dB 规则表明振幅每增加 6dB，将使射频信号的可用传输距离增加一倍。6dB 原则对于理解天线增益非常有用，因为每增加 6dBi 的天线增益，就可以使射频信号的可用传输距离增加一倍。

19. D。对高多径或高噪声的环境进行射频覆盖设计时，通常的最佳实践就是在供应商推荐的接收信号强度或本地噪声(取其中较大者)之上，增加 5dB 的衰落容限。

20. D。无线局域网供应商按照自己的方式定义 RSSI 指标。RSSI 的范围可由供应商自行选择，通常从 0 到某最大值(≤255)。因此 RSSI 指标不应该拿来对不同无线局域网供应商的无线产品进行对比，因为该指标没有标准的取值范围。

第 4 章

1. A、C。抛物柱面天线与扇形天线只能产生无源增益。

2. A。方位图也称为 H 面，它是天线辐射图的正视图。

3. C。沿横轴测量时，主信号两侧两个-3dB 点之间的距离称为波束宽度，单位为°。-3dB 点有时也被称为半功率点。

4. D、E。抛物柱面天线与栅格天线属于高度定向天线，其他天线属于半定向天线。扇形天线是一种特殊的半定向天线。

5. A、C、D。半定向天线的波束宽度很宽，它不适合在远距离通信中使用，但可以用于短距离通信。半定向天线也可以作为接入点的天线在室内环境中提供到客户设备的单向覆盖，也可以减少反射，降低多径的影响。

6. B。如果超过 40%的菲涅耳区被阻挡，则可能导致链路不稳定。菲涅耳区的净空越大越好。

7. C、D。菲涅耳区的尺寸由链路距离和传输频率决定，二者是菲涅耳区计算公式中仅有的两个变量。

8. B。链路距离超过 7 mi(11.3 km)时需要考虑地球曲率的影响。

9. A、C。电缆质量相同时，电缆长度越短，信号损耗越小，天线的辐射功率越大。采用高质量电缆也能减小信号损耗。

10. C、D。采用天线分集的收发器无法同时使用两副天线发送信号，否则两路信号将相互干扰。此外，收发器同时只能解析一路信号。收发器对两副天线接收到的信号进行抽样，并接收强度较高的信号。

11. A、D。为保证点对点桥接链路正常工作，菲涅耳区应保持至少 60%的净空。中短距离桥接链路采用半定向天线(如贴片天线或八木天线)，远距离桥接链路采用高度定向天线。链路距离未超过 7 mi(11.3 km)时无需考虑地球曲率的影响。

12. C。VSWR(电压驻波比)是传输线上最大电压与最小电压之比，如 1.5:1。

13. C、D、E。阻抗失配会导致一部分电压被反射回发射机，使得传输给天线的信号功率或幅度减小(出现损耗)。如果发射机没有采取保护措施，过大的反射功率或电压峰值可能引起发射机过热和损坏。注意，VSWR 会导致信号强度降低和波动，甚至使发射机出现故障。

14. A、B、D、F。菲涅耳区的尺寸由链路距离与传输频率决定。只要存在射频视距，就不必考虑可视视距。例如，虽然在雾天可能无法观察到天线，但是雾气并不会影响到射频视距。安装远距离点对点天线时需要考虑地球曲率的影响。瞄准天线时需要考虑波束宽度，不过计算天线高度时不需要考虑波束宽度。

15. A、D。所用电缆必须支持 802.11 无线网络的工作频率。频率越高，衰减越大。

16. A、B、C、D。所有 4 个选项均属于射频放大器的特性。

17. A、B、D。通过在系统中增加衰减器，可以人为引入信号损耗。电缆会造成信号损耗，电缆越长，损耗越大；电缆越短，损耗越小。换用高质量电缆可以减小信号损耗。

18. C。避雷器可以将非直击雷产生的瞬时电流分流给大地，但它对直击雷无能为力。

19. A、D。第一菲涅耳区与点源同相，第二菲涅耳区始于信号从同相转变为异相的点。由于第二菲涅耳区环绕在第一菲涅耳区的外侧，因此第二菲涅耳区的半径大于第一菲涅耳区的半径。

20. D。主信号能量分布的区域称为主瓣，旁瓣是除主瓣之外的所有波瓣。旁瓣中的信号

能量高于环绕在旁瓣周围的能量。从方位图中可以非常清楚地观察到旁瓣。边带和谐波频率与天线覆盖无关。

第 5 章

1. A、D。ERP(802.11g)无线局域网定义了两种强制的物理层规范，它们是 ERP-DSSS/CCK 和 ERP-OFDM。ERP 无线局域网还定义了两种可选的物理层规范，它们是 ERP-PBCC 和 DSSS-OFDM。

2. E。802.11g ERP 无线接口必须支持 ERP-DSSS/CCK 与 ERP-OFDM 两种扩频技术。ERP-DSSS/CCK 支持 1Mbps、2Mbps、5.5Mbps 和 11Mbps 等 4 个数据速率，且向后兼容 802.11b HR-DSSS 与 802.11 DSSS。

3. B、D、E。802.11 原始标准为传统的 802.11 网络定义了 3 种物理层规范，它们是 FHSS、DSSS 与红外技术。802.11 FHSS 无线接口卡一般称为条款 14 设备，802.11 DSSS 无线接口卡一般被称为条款 15 设备，红外设备一般被称为条款 16 设备。

4. C。802.11 任务组(TG)致力于实现使用 IEEE 802.11 MAC/PHY 层的 Mesh 网络的标准化。802.11s 修正案定义了 Mesh 点的使用，即支持 Mesh 服务的 802.11 QoS 工作站。MP 能使用强制性的 HWMP Mesh 路由协议，使用默认的路径选择标准。供应商也使用专用 Mesh 路由协议和标准。

5. D、F。RSN(即 802.11i)定义了 CCMP(计数器模式密码块链信息认证码协议)作为强制的加密方式，CCMP 采用 AES(高级加密标准)算法。RSN 还定义了一种称为 TKIP(临时密钥完整性协议)的可选加密方式。802.11i 修正案定义的认证方式为 802.1X/EAP 和 PSK(预共享密钥)。

6. D。802.11a 无线接口卡采用 OFDM 技术，使用 5GHz UNII 频段(UNII-1、UNII-2 和 UNII-3 频段)传输数据。

7. D。根据 802.11-2007 标准的规定，OFDM 与 ERP-OFDM 无线接口一般支持 6Mbps、9Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps 和 54Mbps 等 8 个数据速率，其中 6Mbps、12Mbps 和 24Mbps 是必须支持的速率，54Mbps 是标准定义的最大速率。

8. B。FT(快速基本服务集转换)也称为快速安全漫游，它定义了当部署安全性更高的 RSN 时，如何在无线局域网小区之间实现更快的漫游切换。VoIP 等时敏应用对数据包交付时间的要求很高，漫游切换速度不能超过 150 ms。

9. C。802.11 原始标准也称为 802.11 Prime，它定义了 DSSS 和 FHSS 技术，数据速率为 1Mbps 和 2Mbps。

10. D。虽然 802.11a 与 802.11g 设备均采用 OFDM 技术，但是由于二者的工作频段不同，它们无法相互通信。802.11a 设备工作在 5GHz UNII 频段，而 802.11g 设备工作在 2.4GHz ISM 频段。

11. A、E。802.11-2007 标准定义了 DFS(动态频率选择)与 TPC(传输功率控制)机制，以满足 5GHz 无线局域网的管理要求。DFS 与 TPC 最初定义在 802.11h 修正案中，后者目前属于 802.11-2007 标准。

12. C、D。 802.11ac 和 802.11ad 修正草案经常被称为“千兆 Wi-Fi”修正案，因为其比 802.11n-2009 定义的数据率更高。802.11ac 和 802.11ad(VHT)任务组的目标是在 802.11 环境中实现 1Gbps 以上的吞吐量。

13. A、D、E。802.11g ERP 设备工作在 2.4GHz 频段，它采用 ERP-OFDM 和 ERP-DSSS/CCK 技术，可以向后兼容 802.11b HR-DSSS 和 802.11 DSSS 设备。802.11b 设备工作在 2.4GHz 频段，它采用 HR-DSSS 技术，只能向后兼容 802.11 DSSS 设备，无法向后兼容 802.11 FHSS 设备。802.11h 修正案在 5GHz UNII 频段定义了 TPC 与 DFS，它是对 802.11a 修正案的改进和增强。所有兼容 802.11a 和 802.11h 的无线接口都采用 OFDM 技术。

14. D。根据 802.11-2007 标准的规定，OFDM 或 ERP-OFDM 无线接口一般支持 6Mbps、9Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps 和 54Mbps 等 8 个数据速率，其中 6Mbps、12Mbps 和 24Mbps 是必须支持的速率，54Mbps 是标准定义的最大速率。

15. B、D、E。802.11 原始标准定义了 WEP 作为加密方式，定义了开放系统认证与共享密钥认证作为认证方式。

16. A。为解决 IEEE 802.11 接入网与其他外部网络的集成问题，802.11u 修正案定义了一种通用和标准化的方式。802.11u 修正案经常被称为外部网络的无线互联(WIEN)。

17. A、C。802.11e 修正案(目前属于 802.11-2007 标准)定义了两种增强的介质访问方式以满足 QoS 要求。EDCA(增强分布式信道访问)是对 DCF 的完善和补充，HCCA(HCF 受控信道访问)是对 PCF 的完善和补充。在实际中只实现 EDCA。

18. A、C。802.11h 修正案实际定义了两种主要的增强机制：采用 UNII-2 扩展频段以增加可用的传输频率，采用雷达检测和避免技术(DFS 与 TPC)以防止干扰发生。802.11h 修正案的完整内容请参阅 802.11-2007 标准第 11.8 和 11.9 条款。

19. A。802.11b 修正案定义了 HR-DSSS(高速直序扩频)技术，后者支持的数据速率为 5.5Mbps 和 11Mbps。802.11b 设备也向后兼容 802.11 DSSS 设备，此时 802.11b 设备将使用 1Mbps 和 2Mbps 传输数据。

20. B、D。IEEE 仅在物理层与数据链路层的 MAC 子层定义了 802.11 技术，OSI 模型的上层和无线局域网通信无关。

第 6 章

1. A、B、D。3 个 ISM 频段是 902MHz～928MHz、2.4GHz～2.5GHz 和 5.725GHz～5.875GHz。5.725GHz～5.825GHz 属于 UNII-3 频段。

2. A、B、C。4 个 UNII 频段是 5.150GHz～5.250GHz、5.250GHz～5.350GHz、5.470GHz～5.725GHz 和 5.725GHz～5.825GHz。

3. A、B、C、D。802.11-2007 标准规定，802.11 FHSS(条款 14)射频卡、802.11 DSSS(条款 15)射频卡、802.11b HR-DSSS(条款 18)射频卡以及 802.11g ERP(条款 19)射频卡均使用 2.4GHz ISM 频段进行通信。

4. A、B、D。802.11n 修正案规定，802.11n HT(条款 20)射频卡可以使用 2.4GHz ISM 频段和全部 4 个 5GHz UNII 频段收发数据。

5. A。IEEE 规定，北美的 802.11 FHSS 设备使用 2.402GHz～2.480GHz 频段收发数据，频段宽度为 79MHz。

6. D。计算信道，可以利用下面的方法。例如 5300MHz 减去 5000，然后除以 5 等于 60，即信道 60。UNII-2 频段在 5.25GHz 和 5.35GHz 之间。

7. B。802.11b 修正案第 18 条款定义了 HR-DSSS。该修正案规定，两个信道的中心频率之间必须相隔至少 25 MHz，才能认为它们互不重叠。

8. C。FHSS 发射机在跳变到下一个频率之前，在当前频率停留的时间称为驻留时间。跳变时间并非必须消耗的时间，它是衡量系统跳变速度的一个指标。

9. B。OFDM 最初定义在 802.11a 修正案第 17 条款中，该修正案规定，两个信道的中心频率之间只要相隔 20MHz，就可以认为它们互不重叠。5GHz UNII 频段全部 23 个信道均采用 OFDM，信道中心频率之间的间隔为 20MHz。因此根据 IEEE 的定义，所有 5GHz OFDM 信道都是互不重叠的。不过请注意，相邻两个 5GHz 信道仍存在一定程度的边带载频重叠。

10. C、D。两个 ERP 或 HR-DSSS 信道的中心频率之间必须相隔至少 25MHz，才能认为它们互不重叠。换句话说，任意两个非重叠信道之间必须相隔至少 5 个信道。判断一个信道(目标信道)是否与当前信道重叠时，最简单的方法是将当前信道的信道号加 5 或减 5。如果结果小于或大于目标信道的信道号，说明目标信道与当前信道互不重叠。在 2.4GHz ISM 频段部署多个接入点时，一般使用 1、6 和 11 这 3 个非重叠信道。

11. B。ERP-PBCC 是一种可选的调制技术，支持的数据速率为 22Mbps 和 33Mbps。

12. B。时延扩展会引起码间干扰，后者将导致数据损坏。

13. D。802.11-2007 标准指出："监管机构在其业务区域内负责管理 OFDM 通信，OFDM 物理层的工作频段为 5GHz"。标准定义了 4 个 5GHz UNII 频段。最初定义的 3 个 UNII 频段各包括 4 个信道，频段宽度均为 100MHz；UNII-2 扩展频段包括 11 个信道，频段宽度为 255MHz。因此，UNII 频段总共包括 23 个可用的信道。第 24 个信道位于另一个无需牌照的频段。美国规定，OFDM 传输也可以使用信道 165，后者位于 5.8GHz ISM 频段。

14. D。OFDM 子载波的数据速率较低，时延扩展在符号周期中所占的比例很小，这可以在很大程度上避免码间干扰。换句话说，OFDM 技术抗多径干扰的能力优于 DSSS 和 FHSS 扩频技术。

15. C。802.11 技术采用称为 CSMA/CA(载波侦听多路访问/冲突避免)的介质访问方式，即在任何给定的时间内，有且只有一台无线设备可以使用介质传输数据。由于射频介质的半双工特性以及 CSMA/CA 产生的开销，实际总吞吐量一般不会超过数据速率的 50%。

16. B。UNII-1、UNII-2 和 UNII-3 为 100MHz 频宽，定义了 4 个信道。UNII-2e 定义了 11 个信道。

17. B。两个 2.4GHz 信道的中心频率之间相隔 5MHz。

18. A、B。OFDM 采用 BPSK 和 QPSK 调制以获得较低的数据速率，采用 16-QAM 和 64-QAM 调制以获得较高的数据速率。QAM 是混合了调相与调幅的一种调制方式。

19. B。一个数据比特被转换为一连串的比特，这些比特称为码片，代表原始数据。

20. C。OFDM 信道由 52 个子载波构成，其中只有 48 个用于传输数据。另外 4 个子载波称为导频载波，作为接收机解调器的相位和幅度参考。

第 7 章

1. D、E。SSID(服务集标识符)是用于标识无线网络的逻辑名，它由最多 32 个字符构成，且区分大小写。ESSID(扩展服务集标识符)是 ESS 使用的逻辑网络名。一般而言，ESSID 与 SSID 的含义相同。

2. C、E。802.11 标准定义了 4 种服务集(拓扑结构)。BSS(基础服务集)由一个接入点和若干与其建立关联的客户端构成。ESS(扩展服务集)由一个或多个 BSS 构成，这些 BSS 通过分布系统介质相连。IBSS(独立基础服务集)仅由客户端构成，不存在接入点。

3. E。802.11 标准有意没有规定分布系统使用的介质。分布系统介质既可以是 802.3 以太网骨干网，也可以是 802.5 令牌环网，还可以是无线介质或其他任何介质。

4. D。无线个人域网(WPAN)是短距离无线通信使用的一种拓扑结构，蓝牙和 ZigBee 是两种常见的无线个人域网技术。

5. A。最常见的 ESS 部署由多个接入点构成，接入点的覆盖蜂窝之间存在部分重叠，以实现客户端的无缝漫游。

6. A、C、D。接入点发射功率、天线增益、物理环境等许多因素都会影响基本服务区的尺寸和形状。

7. C。根模式是接入点的默认配置模式，采用根模式的接入点在分布系统与 802.11 无线介质之间传输数据。配置为根模式的接入点可在 BSS 中使用。

8. B、E、F。IBSS(独立基础服务集)是 802.11 标准定义的另一种服务集。IBSS 中不存在接入点，客户端之间以对等方式进行通信。IBSS 也被称为点对点模式或对等模式。

9. A、D。配置为基础架构模式的客户端将数据交给接入点，并由接入点转发给 BSS 中的其他无线客户端。客户端也可通过接入点与分布系统中的其他网络设备(如服务器或台式机)进行通信。

10. B、C、D。802.11 标准定义的 3 种拓扑结构(服务集)分别是 BSS(基础服务集)、ESS(扩展服务集)和 IBSS(独立基础服务集)。802.11s-2011 修正案还定义了 MBSS。

11. A。无线城域网(WMAN)为都会区(如城市和周边的郊区)提供覆盖。

12. D。BSSID(基础服务集标识符)是一个 48 位(6 字节)的 MAC 地址，后者位于 OSI 模型数据链路层的 MAC 子层。

13. B、C、E。BSSID 是 BSS 或 IBSS 的二层标识符。在 BSS 中，接入点无线接口卡的 48 位(6 字节)MAC 地址即为 BSSID。ESS 由多个接入点构成，因此存在多个 BSSID。在 IBSS 网络中，第一个启动的客户端以 MAC 地址的格式随机产生一个虚拟的 BSSID。

14. D。802.11s-2011 修正案为 802.11 Mesh 拓扑定义了一种新的服务集。当 AP 支持 Mesh 功能时，它们可能会部署在无法接入有线的网络。Mesh 提供网络流量的无线分布，并由提供 Mesh 基本服务的 AP 构建 MBSS。

15. B。半双工通信中，通信双发都可以收发，但是一次只有一个设备能够传输。对讲机或双向无线电是半双工信心的典型例子。IEEE 802.11 采用半双工通信模式。

16. A、C、E。接入点默认的标准配置模式是根模式，非标准配置模式包括网桥、工作组网桥、扫描器与中继器模式。

17. A、C。ESS(扩展服务集)由一个或多个 BSS(基础服务集)构成，BSS 之间通过分布系统介质连接在一起。一般而言，ESS 是若干接入点和与之建立关联的客户端的集合，所有设备通过单一的分布系统介质相连。

18. A。无线分布系统(WDS)采用无线回程将接入点连接在一起，同时允许客户端与接入点建立关联。

19. B、C。分布系统主要由两部分构成。分布系统介质(DSM)是一种连接接入点的逻辑的物理介质。分布系统服务(DSS)内置在接入点中，一般以软件形式存在。

20. B。802.11 标准属于无线局域网(WLAN)标准，不过 802.11 硬件设备也可以在其他无线拓扑结构中使用。

第 8 章

1. B、D。DCF 是分布式协调功能的缩写。DCF 是 CSMA/CA 的媒介访问控制方法。CSMA/CD 用于 802.3，不用于 802.11。没有数据控制功能这种说法。

2. E。802.11 技术不使用冲突检测。如果一个 ACK 帧并没有被原始发送端接获，即单播帧未得到确认，该单播帧将不得不重传。但此过程不会确定传输过程是否产生了冲突。未收到 ACK 帧意味着两点：单播帧未被目的地无线终端接收或因故未收到 ACK 帧，但终端无法确定未收到的原因。原因可能包括冲突或其他原因，例如较高的噪声等级。其他所有选项都用于防止冲突。

3. D。只有 ACK 帧和 CTS 帧可以在 SIFS 之后传输。不存在 LIFS 的说法。

4. A、B、D。NAV 计时器根据前面传输的帧中的持续时间值来预测无线媒介中未来的流量。虚拟载波侦听使用 NAV 来确定媒介的可用性。物理载波侦听通过检查射频媒介来确定媒介可用性。空闲信道评估是物理载波侦听的另一个名称。不存在信道感应窗口的说法。

5. C。首先选择随机回退计时器值，一旦该值被确定，将其乘以时隙得到具体的回退时间。然后随机回退计时器开始倒数时隙，当倒计至零时，无线终端便可开始传输。

6. B、D。PCF 需要无线接入点。Ad Hoc 模式和独立的基本服务集(IBSS)是相同的，都无需无线接入点。基本服务集(BSS)是指 802.11 客户端通过无线接入点进行通信的拓扑。基础结构模式(infrastructure mode)是默认的客户端模式，允许客户端通过无线接入点进行通信。BSA 是指基本的服务区域或 BSS 的覆盖区域。

7. B、D。Duration/ID 字段用于设置网络分配向量(NAV)，是虚拟载波侦听进程的一部分。竞争窗口和随机回退计时器是载波侦听进程执行后的回退过程的一部分。

8. D。通话公平机制的目的是分配相等的访问时间，而不是相同的访问机会。Access fairness 和 opportunistic media access 的说法不存在。CSMA/CA 是通常的 WiFi 设备媒介访问控制模式。

9. A、B、D、E。DCF 定义了四种 CSMA/CA 制衡机制。DCF 确保在半双工媒介上同时只有一个 802.11 无线接口进行传输。虚拟载波侦听(NAV)、物理载波侦听(CCA)、帧间间距及随机回退计时器通常共同工作。CCMP 是在 802.11i 中被引入的加密协议。

10. C。WMM 是基于 802.11e 修正案定义的 EDCA 机制制定的，802.11e 现在是 802.11-2007

标准的一部分。WMM 认证通过四种访问类别提供流量优先等级。EDCA 是混合协调功能(HCF)子功能之一，另一个 HCF 子功能是 HCCA。

11. E。HCF 定义了在 802.11 无线射频媒介上传输时连续发送多个帧的能力。当兼容 HCF 的射频接口在竞争访问媒介时，它会被分配到某段可用于发送帧的时间，这段时间称为传输机会(TXOP)。在此 TXOP 期间，802.11 无线接口可以连续发送多个帧，或称帧突发(frame burst)。

12. A、B、D、E。WMM Audio 优先级不存在。WMM 认证提供通过语音(Voice)、视频(Video)、尽力传输(Best Effort)、背景(Background)四个访问类别提供流量优先等级。

13. B、C、E。DCF 和 PCF 由 802.11 标准定义。802.11e 服务质量修订案添加了新的协调功能参与到媒介竞争中，这种新的协调功能称为混合协调功能(HCF)。802.11e 修订案和 HCF 已被合并纳入 802.11-2007 标准。HCF 将 DCF 和 PCF 的能力结合在一起，增强了功能，并创建了两种信道访问方法：HCF 控制信道访问(HCCA)和增强的分布式信道访问(EDCA)。

14. B。EDCA 媒介访问方法通过使用 802.1D 优先级标签提供流量的优先次序。802.1D 标记提供一种机制用于在 MAC 层实现服务质量(QoS)。通过在以太网帧的帧头中添加代表用户优先级的三个比特位的 IEEE 802.1Q 报头，使得可以区分数据帧的不同服务等级。802.1D 优先级标签可用于将以太网侧的流量导入不同的访问类别队列。

15. A、E。第一个目的是确定是否有帧在进行入向传输以便接收。如果媒介繁忙，无线终端将尝试与该传输同步。第二个目的是确定媒介在客户端传输前是否繁忙。这称为空闲信道评估(CCA)。空闲信道评估侦听在物理层发生的 802.11 射频传输，确保传输前媒介必须空闲。

16. C、D。802.11 无线接口在利用随机回退算法竞争媒介的时间窗称为竞争窗口。竞争窗口本质上是最终的倒计时器，也称为随机回退计时器。

17. C。当无线终端侦听到另一终端发送的帧时，会查看这个帧报头部分，确定 Duration/ID 字段是否包含 Duration 值或 ID 值。如果该字段为 Duration 值，监听终端将其 NAV 计时器设置为此值。

18.B。增强的分布式信道访问通过使用八种用户优先级别(UP)提供差异化的信道访问。EDCA 媒介访问方法通过使用 802.1D 优先级标签提供流量的优先次序。

19. A。所有 802.11 单播帧必须被确认。广播和多播帧并不要求被确认。不存在任播帧(anycast)。

20. E。块确认通过将多个确认帧聚合成单个确认帧来提高信道使用效率。有两种类型的块确认机制：立即块确认机制和延迟块确认机制。立即块确认机制被设计用于低延迟流量，而延迟块确认机制更适用于耐延迟的流量。

第 9 章

1. B、D。这两个帧都用来加入 BSS。重关联帧用于漫游。重关联帧包含另一个被称为当前接入点地址(Current AP Address)的字段。这个地址是客户端离开的原始接入点的 BSSID。

2. D。IP 数据包包括第 3 层～第 7 层的信息。MAC 服务数据单元(MSDU)包含 LLC 子层

和/或数据链路层以上任意层的数据。MSDU 是 802.11 数据帧主体内的净荷部分。

3. B、D。RTS/CTS 和 CTS-to-Self 提供 802.11g 保护机制或混合模式的支持。没有 NAV back-ff 和 RTS-to-Self 的说法。WEP 加密提供了数据的安全性。

4. A、C、D。ERP 线接入点使用信标帧中的 ERP 信息元素通知启用了保护机制。三种方式可以触发 ERP BSS 的保护机制。如果一个 non-ERP 终端关联到 ERP 接入点，ERP 接入点将在自己的信标帧中启用 Non_ERP_Present 位，从而在 BSS 中开启保护机制，换句话说，HR-DSSS(802.11b)客户端关联会触发保护机制。如果 ERP 接入点听到来自另一个接入点或 IBSS 终端的支持 802.11b 或 802.11 DSSS 速率的信标帧，它将在自己的信标帧中启用 Non_ERP_Present 位，从而在在 BSS 中开启保护机制。如果 ERP 接入点听到来自另一个 ERP 接入点的信标帧中的 Non_ERP_Present 位设置为 1，它也会启用保护机制。

5. A、B、C、D。探询响应帧与信标帧包含相同的信息，但流量指示图(TIM)除外。

6. B、D。信标帧不能被禁用。客户端使用信标帧的时间戳信息与无线网络上的其他终端同步。在 BSS 中只有接入点才发送信标；在 IBSS 中客户端会发送信标帧。信标可以包含私有信息。

7. B。如果无线客户端在 TIM 中找到了其 AID，表明接入点有单播数据缓存。无线终端需要保持清醒并请求下载。这种请求由节电轮询帧(PS-Poll)执行。

8. D。当 RTS 帧发送时，Duration/ID 字段的值等于传输 CTS/Data/ACK 所需的时间。

9. B。当客户端将电源管理字段设置为 1 时，表明其启用了节电模式。DTIM 不会启用节电模式，它只会通知客户端保持清醒，做好接收多播或广播流量的准备。

10. A、B。接收站可能接收到了数据，但返回的 ACK 帧可能被损坏，此时原始的单播帧将不得不重新传送。如果出于任何原因单播帧损坏，接收站将不会发送 ACK。

11. B。PS-Poll 帧被客户端用来请求缓存数据。ATIM 用于通知 IBSS 中的终端有缓存数据。电源管理位用于通知接入点，无线终端进入节电模式。DTIM 用于指示客户端多长时间醒来接收缓存的广播和多播帧。流量指示图(TIM) 是信标帧中的一个字段，接入点用 TIM 通知处于节电模式中的客户端单播帧已被缓存。

12. A、E。所有 802.11 接入点均需响应包含正确 SSID 值的定向探询请求帧。接入点还必须响应包含空 SSID 值的空探询请求帧。某些厂商提供用空探询响应(null probe response)来回应空探询请求(null probe request)的能力。

13. A、D。有两种类型的扫描：被动扫描，终端监听信标发现接入点；主动扫描，终端发送探询请求帧寻找接入点。只有执行主动扫描时，客户端才发送探询请求。客户端关联到接入点后，通常会持续了解附近的接入点。所有客户端通过主动扫描来维护一张持续更新的已知接入点列表。

14. D。当双频客户端第一次启动时，它会在 2.4GHz 和 5GHz 频段发送探询请求帧来查找 AP。当双频 AP 听到来自同一客户端的两个频段的探询请求帧时，便知道客户端能够运行在 5GHz 频带。AP 将仅响应使用 5GHz 频段的客户端，使用这种方法尝试引导客户端使用 5GHz 频带。

15. B。客户端首先尝试连接到接入点时，它将首先发送探询请求，并倾听探询响应。接收到探询响应后，它将尝试进行认证，然后关联到网络。

16. B。传输流量指示消息(DTIM)用于确保使用电源管理的所有终端在多播或广播流量被发送时保持清醒。DTIM 间隔对于使用多播的应用程序非常重要。例如，许多 VoWiFi 厂商支持 VoIP 流量发送到多播地址的一键通(push-to-talk)功能。配置错误的 DTIM 间隔将导致多播性能问题。

17. A、C。ERP(802.11g)接入点向后兼容 HR-DSSS，并支持 1Mbps、2Mbps、5.5Mbps 和 11Mbps 的数据速率及 6Mbps、9Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps、54Mbps ERP OFDM 数据速率。如果无线局域网管理员禁用 1Mbps、2Mbps、5.5Mbps 和 11Mbps 数据率，向后兼容性会被有效禁用，HR-DSSS 客户端将无法连接。802.11-2007 标准定义了基本速率(被要求的速率)的使用。如果客户端不支持接入点所使用的任何的基本速率，客户端将会被拒绝关联到 BSS。如果无线局域网管理员将 6Mbps 和 9Mbps 等 ERP OFDM 数据速率配置为基本速率，HR-DSSS 客户端将会被拒绝关联，因为它们不支持这些速率。

18. A、C。从接入点接收到的信号的振幅大小通常是客户端进行漫游决定的主要变量。客户端漫游机制通常基于 RSSI 值(包括接收信号水平和信噪比)。距离和 WMM 访问类别与客户端决定漫游到一个新的访问点无关。

19. A、C、D、E。应用程序通过设置休眠周期和发送触发帧来控制节电行为。对时延敏感的应用程序会频繁地向接入点发送触发帧，而对时延不敏感的应用程序将会有较长的休眠期。触发和传输方法不再需要 PS-Poll 帧。客户端可以请求下载缓存流量，不必等待信标帧。所有下行的应用程序流量在 TXOP 期间可以更快的帧突发形式发送。

20. B。IEEE 802.11-2007 标准引入了一种增强的电源管理方法,称为自动节电传输(APSD)。两种 APSD 方法分别是计划自动节电传输(S-APSD)和和非计划自动节电传输(U-APSD)。Wi-Fi 联盟的 WMM 节电(WMM-PS)认证基于 U-APSD。

第 10 章

1. A。近年来手持移动互联网设备(MID)出现爆发式增长。大多数用户现在希望大量手持 MID 可以和笔记本一样接入 WIFI 网络。几乎所有的 MID 都使用嵌入式芯片格式。

2. B。所有桥接链路都只可以有一个根网桥。PtP 链接只有一个根网桥，PtMP 链接也将只有一个根网桥。

3. G。802.11 标准不要求 802.11 无线射频卡必须使用哪种类型。虽然 PCMCIA 和 Mini PCI 客户端网卡是最常见的 802.11 射频卡，但也存在许多其他格式，如 CF 存储卡、SD 卡、USB 网卡、ExpressCard 和其他专有类型。

4. B。基于控制器的 AP 通常通过封装的 IP 隧道将数据集中转发至控制器。自治型和协作性 AP 通常使用本地转发。基于控制器的 AP 也可以进行本地转发。尽管协作分布式的 WLAN 模型没有集中转发用户流量到核心，但 AP 也可以具备 IP 隧道能力。

5. A、B、D、E。WLAN 控制器支持 VRRP 冗余协议。HSRP 是一种私有的冗余协议。WLAN 控制器支持强制门户功能和支持基于角色访问控制的用户管理。WLAN 控制器可能还集成 IDS 服务器。

6. A、D、E。802.11 帧在轻量型接入点和 WLAN 控制器之间传输，需要一个 IP 封装的

隧道。每个 802.11 帧都被完全封装到 IP 数据包内。许多无线局域网的供应商使用通用路由封装(GRE)协议，GRE 是一种常用的网络隧道协议。不使用 GRE IP 隧道的无线局域网供应商会采用其他专有协议。尽管 CAPWAP 用于管理，但也可以用于数据封装。

7.D。传统自治型接入点的主要缺点是缺乏中心管理点。具有 25 或更多接入点的智能边缘无线局域网体系结构将需要某种形式的无线网络管理系统(WNMS)。尽管在集中式 WLAN 架构中，控制器可用于管理无线局域网，但是如果存在多个控制器，WNMS 就需要被用来统一管理控制器。尽管在分布式架构中，控制和数据平面功能已经由 AP 运行，但是管理平面功能仍然是集中的，配置和监控所有 AP 的工作仍由 WNMS 处理。

8. F。WLAN 控制器支持第 3 层漫游功能、带宽策略、基于状态的数据包检测。控制器也动态射频和接入点管理。

9. D。网络通讯通常被定义为存在三种逻辑操作平面。控制平面由信令和控制信息组成，也经常被定义为网络智能或网络协议。

10. B。无线工作组网桥(WGB)是为没有无线射频接口的有线基础设施设备提供无线连接的无线设备。

11. A、E。在集中式无线局域网体系结构中，自治型接入点被轻量型接入点取代。所有智能集中在一个被称为 WLAN 控制器的集中设备。

12. B、C。分布式架构中，控制平面机制通过协作协议在 AP 间运行，每个独立 AP 负责用户数据段的本地转发。因此数据平面机制位于 AP 内部。管理平面机制位于 WNMS，用于对分布式 WLAN 进行配置和监控。

13. B。对于点对点网桥，一个网桥必须是根网桥，另外一个网桥必须是非根网桥。虽然它们位于不同的子网，但在关联过程中这些并不会考虑。通常情况下，网桥的 IP 地址是纯粹基于管理的目的，而对传递的流量没有影响。

14. D。因为性能的问题，中继模式也不被推荐用在无线桥接中。如果可能，更好的网桥部署做法是使用两段独立的网桥链接，而不是采用在根网桥和非根网桥之间采用中继的方式。

15. A、C。所有三种 WLAN 基础架构设计都支持 VLAN 和 802.1Q，但集中式 WLAN 架构中，用户 VLAN 通常由 AP 和控制器封装，因此只需要在边界配置一个 VLAN。然而需要在控制器和核心交换机之间配置中继。自治型 AP 和分布式 WLAN 架构都不需要控制器。如果在边界网络需要支持多个 VLAN，则非控制器架构需要 802.1Q 标记的支持，即需要将连接 AP 的接入交换机的端口配置为中继端口。

16. E。大部分 WLAN 控制器供应商采用被称为分离 MAC 的架构。使用这种类型的无线局域网架构，一部分 MAC 服务由 WLAN 控制器完成，一部分由一些基于控制器的接入点完成。

17. B。集中式 WLAN 架构中，数据流量被 AP 封装转发到位于核心的控制器上。标准的网络设计建议在核心进行控制器冗余，以避免单点失效。如果所有数据流量传输到 WLAN 控制器，而控制器失效且没有冗余，WLAN 将会失效。

18. A、B、C。大多数 WLAN 接入点都具有支持多个虚拟 BSSID 的能力。每个轻量型接入点的覆盖范围内可以存在多个虚拟无线局域网。每个虚拟无线局域网有一个逻辑名称

(SSID)和独一无二的虚拟的第 2 层标识符(BSSID)，并且每个无线局域网都映射到一个不同的第 3 层虚拟局域网(VLAN)，每一个 VLAN 映射到一个子网。第 1 层域内可以存在多个第 2/3 层的域。

19. A、C、D、E。WLAN 控制器引入了虚拟无线局域网的概念，通常也称为无线局域网配置文件。不同组的 802.11 客户端位于一个虚拟无线局域网中。无线局域网配置文件是一套 WLAN 控制器配置参数。配置文件参数可以包含无线局域网逻辑名称(SSID)、无线局域网安全设置、VLAN 分配和服务质量(QoS)参数。用户在连接到虚拟 VLAN 后，会被分配一个特定的角色。不要混淆无线局域网配置文件与 AP Group 配置文件。单一接入点可以支持多个无线局域网配置文件，但是，AP 只能属于一个 AP Group。AP Group 配置文件定义了单一接入点或一组接入点的配置设置，包括如信道、传输功率、支持数据速率等。

20. A、C、E。VoWiFi 电话是通过 WLAN 架构通讯的 802.11 客户端工作站。PBX 用于提供公司内部电话连接，还可以通过中继线路将内部电话连接到公共交换电话网(PSTN)。VoWiFi 电话和 WLAN 架构必须支持 WMM QoS 能力。当前大多数 VoWiFi 解决方案使用 SIP 协议作为语音通信的信令协议，但也有厂商使用其他协议。

第 11 章

1. A、B、D。FMC 的目标是用户拥有一个设备和一个电话号码，使用户能够在不同的网络漫游，以利用最便宜的网络通话。

2. C、D。市政和交通网络是两个特定类型的公共热点。执法网络和快速应急网络属于热点类型的网络，但它们不开放给公众使用。

3. C。为防止潜在的干扰及防止干扰的重要性，医院通常会派人负责跟踪组织内的无线频率使用。有些城市也开始这么做，因为无线网络现在不只是用于执法，现在还使用无线技术进行系统监控和数据采集(SCADA)、交通监控、交通信号灯、对讲机、点到点桥接、热点应用等。

4. D。邮轮常常不靠近陆地，无法使用移动蜂窝或 WiMAX 网络作为上行链路，因此需要使用卫星作为上行链路连接到互联网。

5. B、D。固网与移动网络融合(FMC)允许在 Wi-Fi 网络和移动电话网络之间漫游，以选择花费最低的可用网络。

6. D。在设计仓库网络时，网络设备通常是条码扫描器，它们通常不需要传输大量数据，所以高容量和高吞吐量通常是不需要的。由于数据传输要求很低，这些网络通常被设计为提供大面积覆盖。安全始终是需要关注的问题；然而它通常不是设计准则。

7. A、C、D。公司通常在有线网络安装困难或有线网络使用费用极其昂贵的地区安装无线局域网以提供移动性。虽然互联网接入也是无线网络可以提供的服务，但不是安装无线网络的驱动因素。

8. A、C、D。电话公司、Cable 互联网服务提供商和无线互联网服务提供商都可以提供最后一英里接入。

9. B。SOHO 网络的主要目的是提供接入互联网的网关。

10. A、B、D。移动办公网络的解决方案是临时的解决方案，包括除了用于远程的销售办事处以外的所有选项，远程销售办事处更有可能被归类为 SOHO 网络。

11. A、D。仓储、制造环境通常具有移动性需要，但他们的数据传输率是通常很小。因此，其网络设计依据通常是高覆盖要求，而不是高容量要求。

12. D。热点提供商不可能提供数据加密。并没有任何利益或业务的理由部署数据加密，而且很难部署。

13. A、B、C。制造工厂的环境通常是固定的，适合安装永久的接入点。

14. C、D。点到多点、中心和分支和星形架构描述的都是同一种通信技术，它通过使用中心设备连接多个设备。点对点通信只连接两个设备。Mesh 网络未定义中心点。

15. C。802.11 FHSS 技术通常由工业公司(如仓储和制造)采用。这些行业对数据传输速度要求较低，非常适合使用这种技术。

16. C。热点供应商为了方便用户无线接入，使用易用的身份验证方法，一般不提供数据加密。因此为了确保访问企业网络安全，使用 IPSec VPN 是必要的。

17. A、C、D。VoWiFi 是在医疗环境中使用很普遍的 802.11 技术应用，无论人员在医院的任何地方，都可以进行即时通话。实时定位系统使用 802.11 RFID 标签进行库存控制的解决方案也是常见的。无线局域网医疗车用于监视患者生命体征。

18. A、C。安装多个点对点桥接链路可以提供更高的吞吐量或避免单点故障。小心部署信道和天线装置以防止受到干扰。

19. A、B、C。医疗机构经常使用许多射频通信设备，因此需要关注射频干扰。快速、安全、准确地访问在医疗环境中至关重要。较快的访问速度不一定要求较快的传输速度。移动技术通常可以满足更快的访问需求。

20. D。如何只授权有效用户访问是关于公共热点最关注的问题。这需要使用身份验证。然后这只确保未授权用户不能访问网络。

第 12 章

1. B、D。保持跨越第三层子网的唯一方法是提供移动 IP 解决方案或专有的第 3 层漫游解决方案。

2. E。MCA 体系结构中，如果误将所有接入点配置成同一信道，不产生不必要的媒介竞争开销。如果一个 AP 传输，所有附近同一信道的访问点和客户端将推迟传输。其结果是吞吐量受到不利影响：附近的接入点和客户端传输前需要等待很长时间，因为他们不得不轮流传送。所有接入点处于同一信道由此产生不必要的媒介竞争开销称为同频干扰(CCI)。在现实中，802.11 的射频完全按 CSMA/CA 机制进行操作，这种行为应该称为同频协作。

3. A、D、E。传输振幅会影响射频蜂窝的范围。天线可以放大信号强度，并且可以增加覆盖范围。墙壁和其他物理障碍，会使射频信号衰减并影响覆盖范围。CSMA/CA 和加密不会影响范围，但会影响吞吐量。

4. B、C、D。当一个客户端不能听到另一个客户端的射频传输信号时，就会出现隐藏节点问题。增大客户端发射功率可以增加客户端的传输范围，增加客户端互相听到的机会。增

加客户端功率不是推荐方法，因为最佳做法要求客户端和接入点使用相同的传输功率。将隐藏节点移至其他客户端的传输范围内也可以使客户端可以互相听到对方传输。移除障碍物也可以解决问题。隐藏节点问题最好的解决办法是在隐藏节点驻留地区添加另一个接入点。

5. A、B、D、E。如果单播帧的任何部分遭到损坏，则循环冗余校验(CRC)将失败，无线接收方将不会给 802.11 无线发送方返回 ACK 帧。如果发送方没有收到 ACK 帧，即单播帧未得到确认，将不得不重传。多路径现象、射频干扰、低信噪比、隐藏节点、不匹配的功率设置，近/远问题及相邻蜂窝干扰都可能会导致第 2 层重传。同频干扰不会导致重传，但会增加不必要的媒介竞争开销。

6. A、B、D。当一个客户端听不到另一个客户端射频传输时，就会出现隐藏节点问题。分布式天线系统的多天线单元是导致隐藏节点问题的臭名昭著的原因。接入点发射功率过大导致过大的覆盖蜂窝时，位于 RF 覆盖蜂窝两端的客户端经常无法听到对方。障碍物也会导致客户端无法听到对方，如一道新落成的隔墙。

7. B、D、E。过度的第 2 层重传会以下面两种方式影响无线局域网。第一，第 2 层重传增加了 MAC 开销，并因此降低了吞吐量。第二，如果对延迟敏感的应用层数据在第 2 层必须重传，会导致通信延迟或不连续。应用程序(如 VoIP)是否通讯正常取决于 IP 数据包的及时和连续的传递。过度的第 2 层重传通常会导致对时间敏感的应用程序(如语音和视频)产生延迟和抖动的问题。

8. E。接入点和客户端传输功率不匹配是导致第 2 层重传的通常被忽略的原因。如果客户端发射功率级别小于接入点传输功率级别，通信可能被破坏。当客户端移到覆盖蜂窝的外边缘，客户端可以“听”到接入点；然而接入点却无法“听”到客户端。如果客户端发射的帧在接入点附近而不是在客户端附近被损坏，那么最可能的原因是功率设置不匹配。

9. D。如果终端用户抱怨吞吐量下降，一个可能的原因就是隐藏节点问题。在确定隐藏节点问题时，协议分析仪是一个有用的工具。如果协议分析仪指示一个客户端的 MAC 地址相比其他客户端重传率较高，代表隐藏节点已被发现。一些协议分析仪甚至有基于重传阈值的隐藏节点问题警报。另一种方法是使用请求发送/清除发送(RTS/CTS)来诊断问题。

10. B。重叠频率信号的覆盖蜂窝重叠会造成相邻蜂窝干扰，导致严重的延迟、抖动和吞吐量下降。如果重叠覆盖蜂窝也有频率重叠，帧将会损坏、重传将会增加，性能会大大降低。

11. B。当无线客户端逐渐远离接入点，带宽逐渐下降的过程称为动态速率交换(DRS)。DRS 的目标是通过向上或向下调整速率，优化和改善性能。虽然速率动态切换是这一过程的正确名称，但所有这些术语都是指无线局域网客户端在与接入点距离增加时速度下降的方式。

12. E。高增益定向天线都容易受到被称为天线风力负载的影响，即天线因风力导致移动或移位。栅格天线可能可以减轻这个问题。雨和雾也可以减弱射频信号，因此很有必要考虑 20dB 的系统操作容限(也称为衰落容限)。空气温度变化也称为空气分层，这会导致 RF 折射。也可能需要进行 K 因子计算以补偿折射带来的衰减。

13. E。高频率信号波长较短，并且比波长较长的低频信号衰减快。因此高频信号传输范围较窄。在任何射频环境中，自由空间路径损耗(FSPL)按一个与距离有关的函数对信号进行

衰减。信号强度下降会影响覆盖范围。砖墙存在于室内环境中，而树存在于室外物理环境。两者都会对使射频信号衰减，从而影响覆盖范围。

14. D。客户端在本地网络获取的 IP 地址，称为本地地址。移动客户端必须把它的本地地址注册到一个被称为本地代理(Home Agent，HA)的设备上。位于客户端本地网络上的 WLAN 控制器将成为本地代理。本地代理是漫游客户端在三层漫游过程中唯一的联系点。发送给客户端本地地址的流量由 HA 负责拦截，然后通过移动 IP 隧道返回 FA。FA 将数据再传给客户端，客户端的本地 IP 地址得以保持。

15. A、B。虽说蜂窝重叠区域是一个谬论，对于客户端来说，蜂窝重叠区域就是指可以听到的重叠蜂窝空间。如果没有足够的 RF 蜂窝重叠，漫游将会出现问题。重叠太少可能导致漫游盲区，连接可能会暂时丢失。但两个 RF 蜂窝重叠太多，无线客户端可能会保持与其原始接入点关联却不关联到第二个接入点，即使客户端就位于第二个接入点正下方。

16. A、B、C。在部署时使接入点按最大功率传输是经常犯下的错误。实际上，虽然这延伸了接入点的范围，但也导致了很多问题，这些已经在本章讨论了。过大的射频覆盖通常不能满足容量需求。超大的覆盖蜂窝也可能导致隐藏节点问题。全功率发射的接入点可能无法听到按较低功率发射的客户端。全功率接入点也会增加同频干扰的几率。如果关注接入点的覆盖区域，增加覆盖范围的最佳方法是增加接入点的天线增益，而不是增加发射功率。

17. A、C。媒介竞争，也称为 CSMA/CA，要求所有射频接口都以伪随机的方式访问媒介。传输速度较慢的射频卡将占据媒介更长的时间，更快速率的射频卡不得不等待。1Mbps 和 2Mbps 的数据传输速率可以产生非常大的覆盖蜂窝，这可能会阻止覆盖蜂窝两端的客户端彼此“听到”，从而产生隐藏节点问题。

18. A。多路径现象可能会导致符号间干扰(ISI)，这将导致数据损坏。由于原始信号和反射信号的时间差，也称为延迟扩展，接收器在解调射频信号时会产生问题。延迟传播的时间差会导致数据损坏，并因此导致第 2 层重传。

19. A。HR-DSSS(802.11b)和 ERP(802.11g)信道需要中心频率之间相隔 25MHz 才被认为是不重叠信道。在美国 1、6 和 11 信道满足这些要求。在其他国家，2、7、12；3、8、13 或 4、9、14 都是满足要求的。传统上，几乎普遍选择 1、6 和 11 信道。

20. A、D、E。在规划 5GHz 信号复用模式时应该考虑几个因素。第一个需要考虑的因素是所在国家或地区可以合法使用的信道。第二个需要考虑的因素是客户端支持的信道，为了避免和雷达干扰，Wi-Fi 射频卡必须通过在动态频率选择(DFS)信道传输的认证。很大可能客户端没有通过在 UNII-2 和 UNII-2e DFS 信道的认证。另外很多 5GHz AP 可能没有通过 DFS 信道传输认证。

第 13 章

1. B。在 802.1X 安全解决方案中，请求方是向系统要求认证以访问网络资源的 802.11 客户端。每个请求方具有唯一的身份凭证，并由认证服务器加以验证。

2. B、D。802.11-2007 标准将 CCMP/AES 定义为默认的加密方式，将 TKIP/RC4 定义为可选的加密方式。CCMP/AES 与 TKIP/RC4 最初定义在 802.11i 修正案中，该修正案目前已

经被整合到 802.11-2007 标准中。Wi-Fi 联盟开发了 WPA2 认证项目，后者在功能上与 802.11i 修正案完全相同。WPA2 支持 CCMP/AES 与 TKIP/RC4 动态加密。

3. E。128 位 WEP 密钥由用户输入的 104 位(26 个十六进制字符)静态密钥与 24 位 IV 混合而成，有效密钥长度为 128 位。

4. A、C、E。请求方、认证方与认证服务器相互协作，三者构成了 802.1X/EAP 架构。请求方要求访问网络资源，认证服务器验证请求方提供的身份凭证，认证方允许或拒绝请求方通过其虚端口访问网络资源。

5. C。1997 年获批的 802.11 原始标准定义了 64 位与 128 位两种版本的静态 WEP 加密，而动态 WEP 加密并未被标准化。802.1X/EAP、TKIP/RC4 与 CCMP/AES 定义在 802.11-2007 标准中。

6. A、D、E。为避免接入点失窃，可以将其置于带锁的机柜内。鉴于无线配置方式存在很大的安全风险，应始终从网络的有线端对接入点进行配置。应通过加密方式(如 HTTPS 与 SSH)访问管理接口，避免使用 HTTP 或 Telnet。部署 802.1X/EAP 解决方案可以确保只有授权用户才能获得 IP 地址，但是对 VPN 解决方案而言，入侵者在 IPSec VPN 隧道建立之前就可能获得 IP 地址，从而对接入点发动攻击。

7. A、C。VLAN 一般用于三层无线网络分段，大部分企业无线局域网通过 VLAN 与 RBAC 以实现分段。CCMP/AES、TKIP/RC4 与 WEP 是加密机制而非分段机制。

8. A、C。WPA 认证项目属于 802.11i 修正案获批之前的过渡性方案，仅支持 TKIP/RC4 动态加密。WPA-Enterprise 用于企业环境，采用 802.1X/EAP 作为认证方式；WPA-Personal 用于 SOHO 环境，采用密码短语作为认证方式。LEAP 是 Cisco 开发的一种认证协议，它与 WPA 无关。此外，WPA 并未定义动态 WEP 加密或 CCMP/AES 加密，而通过 WPA2 认证的设备必须支持 CCMP/AES。

9. B、D、E。RBAC 是一种仅允许授权用户访问网络资源的机制，主要由用户、角色与许可构成。

10. A、D、E。802.1X/EAP 的目的在于对用户身份进行认证，并给予用户访问网络资源的权限。虽然实施加密并非 802.1X/EAP 架构的强制要求，但是它对于保护信息的安全至关重要。动态加密密钥在 802.1X/EAP 认证过程结束之后产生并分发给通信各方。

11. A、B、D、E。所有类型的 WEP 加密均采用 RC4 算法。TKIP 属于 WEP 的增强版本，它同样采用 RC4 算法。PPTP 采用以 RC4 算法为基础的 128 位 MPPE，而 CCMP 采用 AES 算法。

12. B、D。开放系统认证与共享密钥认证属于传统的认证方式，二者无法提供生成动态加密密钥所需的密钥材料。静态 WEP 使用静态密钥。为实现可靠的安全网络关联，需要 4 帧 EAP 交换，称为四次握手。在请求方通过 802.1X/EAP 认证或 PSK 认证之后，四次握手过程(进行 4 次 EAP 帧交换)将生成 TKIP 或 CCMP 动态密钥。

13. A、D。在 802.1X/EAP 解决方案中，请求方与认证服务器必须支持相同的 EAP 协议，而请求方与认证方必须支持相同的加密方式。此外，认证方必须配置相应的 802.1X/EAP 参数，但是它并不关心请求方与认证服务器使用何种 EAP 协议。认证方和请求方必须支持相同的加密方式。

14. D。WLAN 控制器架构由控制器与轻量接入点构成，可以将轻量接入点视为一种带有无线接口卡与天线的哑终端。在 WLAN 控制器架构中部署 802.1X/EAP 解决方案时，认证方为 WLAN 控制器，受控虚端口与非受控虚端口均位于控制器上。

15. A、C、D。TKIP 由 128 位临时密钥、48 位 IV、源 MAC 地址以及目标 MAC 地址通过每包密钥混合过程产生。此外，TKIP 采用 MIC 来实现数据完整性校验。

16. A。在 802.11 桥接网络中部署 802.1X/EAP 安全解决方案时，认证方为根桥，请求方为非根桥。

17. D。AES 算法将信息加密为固定长度的数据区块，可供选择的密钥长度为 128 位、192 位或 256 位。CCMP/AES 使用 128 位加密密钥，信息被加密为 128 位的定长区块。

18. A、D。WPA2-Enterprise 用于企业环境，采用 802.1X/EAP 作为认证方式；WPA2-Personal 用于 SOHO 环境，采用密码短语作为认证方式。此外，WPA2 认证设备必须支持 CCMP/AES 动态加密，而 TKIP/RC4 属于可选加密方式。

19. E。RSN 与 RSNA 定义在 802.11-2007 标准中。RSN 采用 CCMP/AES 作为强制的加密方式，采用 TKIP/RC4 作为可选的加密方式。

20. C。请求方、认证方与认证服务器相互协作，三者构成了 802.1X 架构，不过实际认证时还需要配合 EAP 对用户身份进行验证。

第 14 章

1. B、C。DoS 攻击针对 OSI 模型的第一层或第二层。第一层攻击称为射频干扰攻击。入侵者通过篡改 802.11 帧(包括伪造解除认证帧)发动各种第二层 DoS 攻击。

2. C、D。恶意窃听在未经授权的情况下使用协议分析仪拦截无线通信。任何未经加密的 802.11 帧传输都可以在 OSI 模型的上层被重组。

3. D。协议分析仪是一种能获取 802.11 流量的被动接收设备，入侵者可以利用协议分析仪实施恶意窃听。由于 WIDS 无法检测到被动接收设备，因此只能采用高强度的加密方式防止恶意窃听。

4. C、D。唯一能阻止无线劫持、中间人攻击与 Wi-Fi 钓鱼攻击的方法是采用双向认证解决方案。802.1X/EAP 解决方案规定，通信双方必须首先交换双向认证的身份凭证，只有合法用户才能通过授权。

5. A、C。WIPS 传感器中的无线接口卡可对 2.4GHz ISM 频段与 5GHz UNII 频段进行监控，而某些早期的无线网络设备使用 900MHz ISM 频段收发数据，这些设备并不能被 WIPS 发现。此外，WIPS 传感器中的无线接口卡采用 DSSS 与 OFDM 技术，因此无法发现采用 FHSS 技术、使用 2.4GHz ISM 频段传输数据的无线网络设备。唯一能监控 900MHz 频段或发现 FHSS 非法接入点的设备是频谱分析仪。

6. A、B。一般性安全策略描述了企业或组织制定无线安全策略的目的。即使企业尚未规划部署无线网络，也应制定处理非法设备的相关措施，这是确保网络安全的最低要求。功能性安全策略定义了采用何种措施与手段保护无线网络的安全。

7. A、E。攻击者在获得密码短语后就可以连接到 WPA/WPA2 接入点，进而入侵网络资

源。虽然加密技术本身并未被破解，但是密钥可以重新生成。如果攻击者取得密码短语并破解四次握手过程，就能重新生成动态加密密钥，从而解密流量。一旦密码短语被破解，攻击者就能入侵网络资源并解密流量，因此 WPA/WPA2-Personal 并非一种可靠的企业安全解决方案。

8. A、C、D、E。第二层 DoS 攻击的种类很多，包括关联帧泛洪、解除认证欺骗、解除关联欺骗、认证泛洪、PS-Poll 泛洪以及虚拟载波攻击。射频干扰属于第一层 DoS 攻击。

9. A、C。微波炉工作在 2.4GHz ISM 频段，它经常会引起非蓄意干扰。2.4GHz 无绳电话也能引起非蓄意干扰。信号发生器一般被攻击者用作干扰设备，它产生的干扰属于蓄意干扰。900MHz 无绳电话不会对 2.4GHz 或 5GHz 无线局域网设备造成干扰。不存在所谓的“解除认证发射机”(deauthentication transmitter)。

10. A、B。目前的第二层 WIPS/WIDS 传感器无线接口卡采用 DSSS 与 OFDM 技术，因此无法检测到采用 FHSS 技术、工作在 2.4GHz ISM 频段的无线网络设备。唯一能监控 900MHz 频段或发现 FHSS 非法接入点的设备是频谱分析仪。某些 WIPS/WIDS 厂商开发了一层分布式频谱分析系统(DSAS)解决方案。

11. A、B。接入点或 WLAN 控制器可启用客户端隔离机制，以阻止同一无线网段中的无线客户端之间相互通信。安装个人防火墙也能降低对等攻击造成的危害。

12. C。WIPS 可降低非法接入点造成的危害，它采用第二层 DoS 攻击作为反制非法设备的手段。此外，WIPS 可通过 SNMP 关闭非法接入点所连接的交换机端口。WIPS 厂商还采用其他专有的方法消除非法接入点与客户端造成的危害，但是这些方法通常并不会向外界公布。

13. A、B、E、F。WIPS 将 802.11 无线接口标记为 4 或更多的类别。企业无线网络中的授权客户端或接入点被标记为基础架构设备，任何检测到但不属于非法设备的 802.11 无线接口被自动标记为未知设备，任何检测到且身份已知的客户端或接入点被标记为已知设备，任何对网络造成干扰或可能威胁网络安全的客户端或接入点被标记为非法设备。

14. A、E。企业应制定相应的安全策略以禁止员工安装无线设备，并规定各种无线攻击(包括非法接入点)的处理措施。在 WIPS 检测到非法接入点后，建议管理员暂时采用第二层非法设备抑制措施，直到确定非法设备的实际位置，然后立即将非法设备从数据端口断开。为便于取证，不要忙着关闭非法接入点的电源。从关联表和日志文件中或许能找到非法设备的安装信息。

15. A、C、D、F、G。目前不存在所谓的“快乐接入点攻击”(Happy AP attack)。公共热点没有采取任何安全措施，无线用户极易成为攻击目标。由于通信没有加密，用户容易遭到恶意窃听。由于不使用双向认证，用户容易遭到无线劫持、中间人攻击以及钓鱼攻击。由于热点可能并未禁用对等连接，用户容易遭到对等攻击。企业应制定远程接入无线安全策略，以保护终端用户访问外部网络时的安全。

16. A、C。由于公共热点没有采取任何安全措施，因此必须严格执行远程接入无线局域网策略。该策略应包括采用 IPSec VPN 解决方案进行设备认证与用户认证，并加密所有无线数据流量。公共热点是恶意窃听的主要目标，应在所有远端计算机中安装个人防火墙以阻止对等攻击。

17. B。MAC 过滤仅允许来自特定客户端的流量通过接入点，它基于每个客户端唯一的 MAC 地址。MAC 地址可以被欺骗或伪造。业余黑客只要将自己的 MAC 地址伪装成某个出现在允许列表中的客户端的 MAC 地址，就能轻易绕过 MAC 过滤。

18. A。由于许多 WLAN 控制器厂商已经在其产品中集成了全面的入侵检测功能，因此不必再部署覆盖型解决方案。在集成型 WIDS 中，WLAN 控制器作为中央 WIDS 服务器使用。

19. A、D、E。目前，64 位 WEP 与 128 位 WEP 均已被破解。无论密钥长短，破解工具都可以在几分钟之内将其破解。TKIP/RC4 与 CCMP/AES 尚未被破解。

20. D。无线劫持是一种经常会给网络安全造成很大压力的攻击，又称双面恶魔攻击。通过使用双面恶魔接入点与 DHCP 服务器，攻击者可在第二层和第三层劫持无线客户端，并进一步发动中间人攻击以及(或者)Wi-Fi 钓鱼攻击。

第 15 章

1. C、D。强烈建议现场勘测与网络部署时采用同一家厂商生产的设备。不推荐在勘测时混用不同厂商的设备，也不推荐混用自治接入点解决方案与轻量接入点解决方案。安全不是勘测时需要考虑的问题。

2. B。在酒店行业中部署无线局域网时，题目给出的所有选项都是需要考虑的因素，不过美观通常是其中最为重要因素。大部分服务行业都不希望将无线硬件设备暴露给外界。请注意，多数机柜都可以上锁，以防止昂贵的 Wi-Fi 硬件被盗。防盗也是很多行业需要考虑的问题。

3. A、B、C。安全本身不是无线局域网现场勘测时需要考虑的问题，但是勘测方应与网络管理员进行面谈，以确定客户的安全期望。勘测方应制定全面、详细的无线安全建议，后者还可以包括对企业无线安全策略的建议。现场勘测时一般不需要考虑采用何种认证与加密解决方案。

4. C。现场勘测面谈时，应与客户讨论分段、认证、授权、加密等方面的要求。第 13 章介绍了无线安全体系的构成。条件允许的话，应将 3 类用户分别划分到独立的 VLAN，且每种 VLAN 采用不同的安全解决方案。数据 VLAN 采用 802.1X/EAP 与 CCMP/AES，安全性最强；语音 VLAN 采用 WPA2 与 CCMP/AES，但不采用 802.1X/EAP，以减少延迟；为便于使用，访客 VLAN 仅采用最低限度的安全措施。

5. A、B。除现场勘测报告之外，勘测方还可以向客户提出有关培训、安全、厂商选择等方面的建议。最终现场勘测报告包括覆盖、容量和漫游要求。

6. A、C。现场勘测面谈开始之前，应向客户索取设计图，以便双方讨论覆盖与容量需求。在规划无线网络与当前有线基础架构的集成时，网络拓扑图可能会提供很大帮助。

7. B、D。只要部署了语音或视频等时敏应用，延时就是一个需要重点考虑的问题。如果客户端在漫游过程中需要跨越三层边界，则应采用移动 IP 或专有的三层漫游解决方案。

8. A、D、E。最终的现场勘测报告称为交付报告，后者包括频谱分析(标识潜在干扰源)与覆盖分析(界定射频蜂窝边界)。此外，最终报告还包括对接入点布局、配置以及天线朝向的建议，而应用程序吞吐量测试通常作为附在最终报告中的可选分析报告。但是，现场勘测

报告中并不包括防火墙设置与路由器访问控制列表。

9. A、B、E。漫游问题可能与干扰有关，也可能因为缺乏足够的覆盖以及(或者)合适的蜂窝重叠。第 12 章中曾经介绍过，工程上一般为漫游预留足够的蜂窝重叠区域，如果重叠区域不足会导致漫游故障或者漫游盲区，也可能导致连接短暂中断。但是如果重叠区域过大，也可能导致漫游问题。例如客户端一直与原始 AP 相连，即便客户已经漫游到了第二颗 AP 的正下方。另外还可能导致用户漫游过渡，即在 2 个或多个 AP 间切换。如果客户端听到在相同信道存在很多信号很强的 AP，也会因为媒介竞争的缘故导致性能下降。2.4GHz 移动电话属于潜在的干扰源。蜂窝电话与无线局域网的工作频段不同，它不会对现有的无线局域网造成干扰。

10. D。尽管答案 C 也是一个可行的解决方案，不过最好将硬件设备部署在 5GHz 频段，这样就不必担心受到来自附近 2.4GHz 网络的干扰。

11. A。最为经济和有效的解决方案是将原有的边缘交换机更换为具有内置电源、可以通过 PoE 为接入点供电的新型交换机。受电缆距离所限，核心交换机不具备 PoE 的能力。部署单口电源注入器并不实际，而聘用电工的成本又太高。

12. A、B、D。影响网络性能的两个常见原因是同频干扰。容量规划不足会使连接到一个接入点的用户过多，从而导致吞吐量降低。多径现象在尚未支持 MIMO 的传统 802.11a/b/g 环境中也会导致性能问题。

13. E。用户密度、数据应用、峰值使用率都是规划 802.11a/b/g/n 网络的容量时需要考虑的因素。部署 5GHz 无线局域网时必须考虑信道规划。传统客户端不支持 DFS 信道。

14. E。以下问题与基础架构集成有关：如何为接入点供电？如何将无线局域网及其(或者)用户与有线网络区分开？如何管理无线局域网远端接入点？此外，勘测方还应与客户讨论 RBAC、带宽限制以及负载均衡等问题。

15. A、B、C。在现场勘测和网络部署阶段，勘测人员应与客户的网络管理员沟通，以确保无线局域网与有线网络的完美集成。勘测方应与生物医学部门进行接触并讨论潜在的射频干扰。勘测方还应联系医院保安部门以取得相应的安全通行证，如有必要，勘测时需要专人陪同。

16. B、C、D。规划仓储环境的无线网络时，覆盖是首要因素，而容量并非一个大问题。由于仓储环境一般部署有手持设备，因此无缝漫游也是强制指标之一。安全是所有企业无线局域网部署都需要考虑的重要因素。

17. A、C、D。应使用经过加固的接入点或将设备置于符合 NEMA 标准的机箱中，以保护室外设备不受气候变化的影响。NEMA 防水机箱的品种很多，包括加热、冷却和 PoE 接口。部署室外桥接链路时，接入点一般与抛物柱面天线和平板天线配合使用。

18. C。概率流量公式采用厄郎作为电信流量的单位，1 厄郎等于 1 小时内的电话流量。

19. A、B、D。勘测方根据勘测时采集的数据向客户提供一份最终的设计图纸。除实施图纸外，勘测方应向客户提供一份详细的材料清单，后者逐一列出了最终安装无线网络所需的各种硬件与软件。此外，勘测方应起草一份详细的日程安排，包括所有时间表、设备成本与人工成本。

20. C、E。热点的尺寸通常较小，应采用低功率的单接入点以限制热点的射频覆盖区域。

由于热点通常只采用强制网络门户对用户进行简单的认证，因此其安全性较低。

第 16 章

1. A、B、C、E。勘测工程师首先使用预测性软件生成勘测区域的预测模型，再通过人工现场勘测加以验证。需要验证的参数包括信道复用模式、覆盖小区边界、接入点布局、接入点功率设置、接入点数量以及数据速率。吞吐量和漫游测试能够验证需求设计。

2. A、C。闪电可能危害到 802.11 桥接设备和与之相连的网络基础架构设备，而强风会导致远距离桥接链路和射频视距不稳定。进行室外现场勘测时，必须留意各种气象条件。室外部署时必须采用避雷器以及(或者)铜-纤收发器(copper-fiber transceiver)等合适的防雷设备。强风环境中应考虑使用栅格天线。露点、云层与雷声对 802.11 室外部署没有影响，现场勘测时不必考虑这些因素。

3. C、E。信号强度测量工具是人工覆盖分析的主要工具。预测性分析工具可以生成射频覆盖蜂窝的预测模型。

4. A、B、E。任何类型的射频干扰都可能导致无线局域网瘫痪。勘测人员应进行频谱分析勘测，以确定医院中是否存在可能干扰到 2.4 GHz 或 5 GHz 无线局域网的医学设备。802.11 通信还会因覆盖盲区或覆盖不充分而中断。许多医院广泛使用金属丝网安全玻璃，后者会引起射频信号散射，还可能完全阻挡信号的传播。电动升降机的材质为金属，射频信号往往无法很好地覆盖电动升降机。

5. E。在主动人工勘测中，无线接口卡与接入点建立关联与上层连接，可以进行低级别的帧传输并测量射频数据。主动现场勘测的主要目的是确定第 2 层重传率。

6. A、C、D。测轮用于测量接入点的预定安装位置与配线室之间的距离。临时固定接入点时可能需要使用梯子或叉车。电池组用于为接入点供电。GPS 用于室外勘测，室内勘测不使用 GPS。微波炉属于干扰源。

7. A、B、C、D、E。虽然室外现场勘测通常都是针对无线桥接而言的，但是也可以部署室外接入点和网状路由器。二者不仅用于在室外环境中提供用户接入，也是室外现场勘测使用的主要工具。室外与室内 802.11 现场勘测所用的设备基本相同，不过室外勘测还可能配备用于记录经纬度坐标的 GPS。

8. B、D。无绳电话使用 5GHz UNII 频段进行通信，它可能干扰到无线局域网。5GHz 频段的潜在干扰源还包括雷达。微波炉与 802.11b/g 无线局域网都工作在 2.4GHz ISM 频段。调频广播使用低频、需要牌照的窄带频段进行通信。

9. A、C。被动人工勘测时，无线接口卡测量接收信号强度(单位：dBm)、噪声级别(单位：dBm)、信噪比(单位：dB)等射频数据。信噪比是接收信号与背景噪声之间的差值，以 dB 表示。接收信号强度是一个功率绝对值，单位为 dBm。天线厂商在其产品手册中使用 dBi 或 dBd 值表示天线增益。

10. C。户外桥接网络不需要平面图，因为无线连接没有发生在建筑物内部。

11. A、B、C、D。进行室外桥接现场勘测时需要计算大量参数，这些参数包括链路预算、自由空间路径损耗、菲涅耳区以及衰落容限。室内勘测时不需要计算这些参数。

12. B、C、D、E。实施 802.11b/g 现场勘测时，应注意对 2.4GHz ISM 频段进行扫描和频谱分析。蓝牙无线接口、等离子切割机、2.4GHz 摄像机以及传统的 802.11 FHSS 接入点都是潜在的干扰设备。

13. A、C、D、E。室内无线现场勘测应包括至少一个接入点以及若干天线。客户端无线接口卡用于覆盖分析，而楼层平面图用于记录测量数据。频谱分析仪用于扫描 2.4GHz ISM 和 5GHz UNII 频段。

14. D。进行人工勘测时，由于 5GHz 信号的波长较短、传输距离较近，因此应首先实施 5GHz 覆盖分析。如果使用双频接入点，应首先对覆盖范围最小的无线接口(这种情况下是高频 5 GHz 无线接口)进行勘测。由于 2.4GHz 无线接口的覆盖范围较大，应将其发射功率调低，以便接近 5GHz 无线接口的覆盖范围。如有必要，可以关闭某些 2.4GHz 无线接口。

15. A、E。在多租户环境中，最大的射频干扰来自于其他用户的无线局域网。由于周围的大部分无线局域网设备都使用 2.4GHz 频段进行通信，用户应考虑在 5GHz 频段部署无线局域网。由于射频信号在空间中的传播是立体的，规划信道复用模式时应始终将其三维特性考虑进去。

16. A、B、E。临时接入点固定装置是现场勘测中的必备工具，数码相机与着色电工胶带用于记录接入点布局的位置，栅格天线在室外远距离桥接链路中使用，接入点机柜用于保护永久安装的接入点。

17. B。多径效应是仓储环境中影响无线网络性能的罪魁祸首，在仓储环境进行勘测时应使用定向天线。长廊和金属货架都会反射射频信号，从而引起多径干扰，使用定向天线可以很好地解决这一问题。

18. A、D。现场勘测时应将每一个接入点的功率和信道设置记录在案，但不必记录安全设置与 IP 地址。

19. B。在被动人工勘测中，无线接口卡测量接收信号强度(单位：dBm)、噪声电平(单位：dBm)、信噪比(单位：dB)、带宽数据速率等射频数据。但是在勘测过程中，客户端适配器并没有与接入点建立关联。

20. C。预测性覆盖分析软件根据建模算法和衰减值生成射频覆盖蜂窝的可视化模型，从而不必去实际测量射频数据。

第 17 章

1. D。在 IEEE 最初制定的 802.3af 修正案中，PoE 就定义在第 33 条款。一项修正案被整合到修订后的标准中时，条款编号保持不变。

2. A。如果设备无法提供可选的分类签名，它将被自动划分为 0 类设备，PSE 将为该设备分配 15.4 W 的电量。

3. A、C。PoE 标准定义了 PD(受电设备)与 PSE(供电设备)两种设备。

4. D。虽然 PD 的额定电压为 48 V，但它必须接受最高 57 V 的供电。

5. A、B、C。PD 必须能通过数据电缆对或空闲电缆对接受供电，10BaseT 或 100BaseTX 设备使用 1-2、3-6 数据对，而 1000BaseT 设备利用 4-5、7-8 数据对。PD 必须向 PSE 返回检

测签名。此外，PD 必须能通过电源的任意极性接受供电。向 PSE 返回分类签名并非强制要求。

6. D。PD 可以向 PSE 提供分类签名，不过这并非强制要求。如果 PD 无法提供分类签名，它将被划分为 0 类设备，PSE 将为其分配最大的电量(15.4W)。

7. A、B、C。采用备选方案 B 时，端接式 PSE 和中跨式 PSE 将通过空闲电缆对为 PD 输送电量。由于 10BaseT 和 100BaseTX 设备仅使用两对以太网电缆收发数据，因此二者可以通过备选方案 B 接受供电。在 802.3at 标准批准之前，1000BaseT 设备使用全部 4 对以太网电缆收发数据，它只能通过采用备选方案 A 的端接式 PSE 接受供电，但现在也可以用 Alternate B。100BaseFX 设备使用光缆，它与 PoE 并不兼容。

8. D。Class 4 设备在 802.3at 标准中定义，Class 4 PD 需要的功率在 12.95W 到 25.5W 之间。

9. C。每台 PoE 设备可以从 PSE 接受的最大功率为 30W。如果一个 24 口 PoE 交换机的所有端口都与 PD 相连，交换机输出的总功率为 720W(30W×24=720W)。

10. D。PSE 将输送给 PD 的电量划分为 4 个等级：0 类设备需要 15.4W，1 类设备需要 4.0W，2 类设备需要 7.0W，3 类设备需要 15.4W，4 类设备为 30.0W。由于这个接入点的耗电量为 7.5W，PSE 将为其分配 15.4W 的电量。

11. D。PSE 的输出电压范围是 44V～57V，额定电压为 48 V。

12. A。100m 是以太网电缆的最大有效距离，不过这并非 PoE 的限制，长度为 90m 的电缆不存在任何问题。尽管 PoE 标准并未做出明确定义，但是 5e 类线缆可以用于 1000BaseT 通信，因此也可以使用 PoE。由于该以太网交换机属于 1000BaseT 交换机，它只能采用备选方案 A(使用数据电缆对)为 PD 供电。如果 PoE VoIP 电话的数量较多，其耗电量可能超过交换机的负荷，从而影响到接入点的供电。

13. B。交换机为每台 0 类设备分配 15.4W 的电量，为每台 1 类设备分配 4.0W 的电量。10 部 VoIP 电话的耗电量为 40W，10 个接入点的耗电量为 154W，而交换机本身的耗电量为 500W，因此所有设备的总耗电量为 694W(40W+154W+500W)。

14. B。交换机为每台 2 类设备分配 7.0 W 的电量，为每台 3 类设备分配 15.4W 的电量。10 部相机的耗电量为 70W，10 个接入点的耗电量为 154W，而交换机本身的耗电量为 1000W，因此所有设备的总耗电量为 1224W(70W+154W+1000W)。

15. C。PD 第一次连接到 PSE 时，其额定电阻值为 25 kΩ。

16. B。PSE 首先输出 10.1 V 的电压，同时测量数据电路以确认 PD 的检测签名。

17. C。0 类 PD 的最大功耗为 12.95W，PSE 将为该类设备分配 15.4 W 的电量。这是因为考虑到 PSE 与 PD 之间的电缆和接头损耗，PSE 必须为可能存在的电量损失预留空间。1 类 PD 的最大功耗为 3.84W，2 类 PD 的最大功耗为 6.49W。

18. E。用于标识不同设备的电流范围如下：

0 类：0mA～4mA

1 类：9mA～12mA

2 类：17mA～20mA

3 类：26 mA～30mA

4 类：36mA～44mA

19. C。采用模式 A 的 PD 从电源的正极或负极接受供电，使用引脚 1、2、3、6。采用模式 B 的 PD 使用引脚 4、5、7、8。

20. C。Type2 型的设备会进行一次物理层或数据链路层检测，以识别 Type2 型 PD 是连接在 Type1 型还是 Type2 型 PSE 上。如果相互认证无法完成，设备只能按 Type1 型工作。

第 18 章

1. A、C、E。802.11n 标准允许使用最多 4 条射频链的 4×4 MIMO 系统。每条射频链都会耗电，4×4 MIMO 系统的耗电量远远大于 2×2 MIMO 系统。802.3-2005 标准第 33 条款(PoE 标准)定义的最大输出功率为 15.4W，而老一代的 802.11n 双频 3×3 和 4×4 MIMO 接入点的耗电量大于 15.4W，所以不支持 802.3af。新一代的 3×3 系统支持 802.3at。在 802.3at 修正案可以提供 30W 的电力，802.3at PSE 设备也提供更高的电源预算。

2. A、C、D。空间复用同时发送多路独立的数据流。如果 MIMO 接入点向 MIMO 客户端发送两路独立的数据流，且客户端可以成功接收这两路数据流，则吞吐量将增加为原来的两倍。如果 MIMO 接入点向 MIMO 客户端发送 3 路独立的数据流，且客户端可以成功接收这 3 路数据流，则吞吐量将增加为原来的 3 倍。传输波束成形技术利用多径效应提高通信质量，能获得更高的信噪比与更强的接收信号幅度。由于信噪比提高，系统可以采用更为复杂的调制方式来编码更多的数据位，从而提高了吞吐量。40MHz 信道将数据传输的可用带宽增加了一倍，吞吐量随之提高。A-MPDU 与双 CTS 保护机制均属于 MAC 子层增强技术。

3. D。SMPS(空间复用节电)允许 802.11n MIMO 设备仅保留一个无线射频卡，关闭其他无线射频卡。例如，采用 4 条射频链的 4×4 MIMO 设备可以关闭其中 3 个无线射频卡以降低耗电量。SMPS 包括静态与动态两种工作模式。

4. E。可以将保护间隔视为时延扩展的缓冲，符号传输之间的保护间隔通常为 800ns。保护间隔不仅能补偿时延扩展，也有助于避免码间干扰，而保护间隔过短将导致码间干扰。HT 无线接口可以使用更短的 400 ns 保护间隔。

5. A、B、C、D、E。HT 无线接口根据调制方式、空间流数量、信道宽度、保护间隔、平等/非平等调制等多种参数定义数据速率，调制编码方案(MCS)是这些参数的不同组合。20MHz HT 与 40MHz HT 信道一共存在 77 种调制编码方案。

6. A、B、C、E。为减少开销并提高吞吐量，802.11n 修正案定义了两种新的帧聚合方式。帧聚合是一种将多个帧合并到单个帧传输的机制，它包括 A-MSDU(MSDU 聚合)与 A-MPDU (MPDU 聚合)两类。MTBA(多流量 ID 块确认)帧用于确认 A-MPDU，采用块确认能减少开销。RIFS 是一种长度为 2μs 的帧间间隔，HT 绿地网络使用 RIFS 以减少帧突发期间的开销。与普遍使用的 SIFS 相比，长度仅为 2 μs 的 RIFS 产生的开销更少。保护间隔在物理层中使用。

7. C。采用波束成形技术的 802.11n 发射机根据接收机反馈的探空帧调整信号相位。此时，发射机称为波束成形器(beamformer)，接收机称为波束成形接收器(beamformee)，二者相互向对方发送 MIMO 信道的特性信息。

8. A。MIMO 无线接口同时发送多路无线信号，每路无线信号通过独立的无线接口与天线传输给接收机。MIMO 系统实际上利用了多径效应。每路独立的信号称为空间流，不同无线接口发送的空间流包含不同的数据。3×3:2 MIMO 系统可以发送 2 路独立的数据流，其中第一个数字“3”表示发射机的数量，第二个数字“3”表示接收机的数量，第三个数字 2 代表空间流的数量。

9. A。多个 MPDU 可以被聚合到一个帧中，构成 A-MPDU 的所有 MPDU 必须具有相同的接收机地址，且必须属于同一 802.11e QoS 访问类别。

10. A、B、C。当网络中仅存在 HT 无线接口时，应采用模式 0、1、2 定义的保护机制。当网络中同时存在 HT 与 Non-HT 无线接口时，应采用模式 3(HT 混合模式)定义的保护机制。

11. B、C、D。Wi-Fi CERTIFIED n 项目包括以下强制性基准要求：802.11n AP 在发射与接收模式必须支持两路空间流、WPA/WPA2 认证、WMM 认证、在 5GHz UNII 频段支持 40MHz 信道。客户端必须一路或以上空间流。

12. C、D。CSD 是一种 802.11n 标准定义的传输分集技术。与 STBC 不同，使用 CSD 的发送机的传输信号可以被传统的 802.11a 和 802.11g 客户端接收。MRC 属于接收分集。

13. A、B、D。HT(条款 20)无线接口向后兼容 HR-DSSS(条款 18)、OFDM(条款 17)与 ERP(条款 19)无线接口。换句话说，802.11n 无线接口向后兼容 802.11b、802.11a 与 802.11g 无线接口。但是，HT 无线接口并不兼容传统的 FHSS 无线接口。

14. B。传输波束成形利用 MIMO 多天线发射机调整外出信号相位。如果发射机知道接收机的位置，就可以调整多路信号的相位，以期达到当多路信号到达接收机时保持相位同步，此时产生的多径效应就是积极的，而非破坏性的。波束控制和动态波束成形属于智能天线技术范畴，可以创造定向波束。

15. C、D。HT 混合格式属于强制格式，支持 20MHz 通信与 40MHz 通信。HT 绿地格式属于可选格式，支持 20MHz 通信与 40MHz 通信。Non-HT 传统格式属于强制格式，只支持 20MHz 通信。PCO 不是 PPDU 格式。

16. C。多信道架构不支持在 2.4GHz 频段部署 40MHz HT 信道。尽管 2.4GHz ISM 频段包括 14 个信道，但只有 3 个互不重叠的 20MHz 信道。无论采用何种方式在 2.4GHz 频段进行信道绑定，任意两个 40MHz 信道都会相互重叠。换句话说，在 2.4GHz ISM 频段根本无法规划 40MHz 信道复用。

17. C。Non-HT 复制传输在 5GHz 以 802.11a 数据率发送，在 2.4GHz 按 802.11g 数据率发送。图 18-18 中，你可以看到 non-HT 复制传输同时在相邻的两个 20MHz 信道(52 个子载波)发送相同的数据。这会导致在主信道和次信道的客户端都会更新 NAV 并延迟传输。Non-HT 重复模式可以改善错误率，但并未在 WLAN 厂商产品中大范围部署。

18. B、C。传统的 802.11 技术依赖于频段，只能使用一个射频频段进行通信。例如，FHSS(条款 14)、HR-DSSS(条款 18)与 ERP(条款 19)无线接口仅能使用 2.4GHz ISM 频段收发数据，OFDM(条款 17)无线接口仅能使用 5GHz UNII 频段收发数据。而 HT(条款 20)无线接口不依赖于频段，它可以使用 2.4GHz ISM 与 5GHz UNII 两个频段收发数据。

19. B。802.11n 既可以采用 800ns 保护间隔，也可以采用较短的 400ns 保护间隔，后者属于可选设置。采用较短的保护间隔能缩短符号时间，数据速率将因此提高 10%左右。当

802.11n 无线接口采用可选、较短的 400ns 保护间隔时，虽然吞吐量有所提高，但是发生码间干扰的概率也将随之增加，从而增加数据损坏的概率。数据损坏将引发第 2 层重传，后者会导致吞吐量降低。有鉴于此，应仅在射频环境较好时采用 400ns 保护间隔。如果采用较短的保护间隔导致吞吐量下降，则应改用默认的保护间隔设置(800ns)。

20. A、C。随着发射机和接收机之间的距离逐渐增大，接收信号强度将越来越接近本底噪声。MRC 算法被用来优化混合多路接收信号，具体做法是查看每个唯一的信号，并以优化方式组合它们，产生积极作用，而非破坏性作用。MIMO 系统利用交换分集和 MRC 一起来改善接收信号 SNR。传输波束成形能获得更高的信噪比与更强的接收信号幅度，因此接入点可以覆盖更大范围内的客户端。

附录 B

略语表、首字母缩略词及功率管理规定

CWNP 认证

CWAP Certified Wireless Analysis Professional(认证的无线分析专业工程师)
CWDP Certified Wireless Design Professional(认证的无线设计专业工程师)
CWNA Certified Wireless Network Administrator(认证的无线网络管理员)
CWNE Certified Wireless Network Expert(认证的无线网络专家)
CWNP Certified Wireless Network Professional(认证的无线网络专业工程师)
CWNT Certified Wireless Network Trainer(认证的无线网络讲师)
CWSP Certified Wireless Security Professional(认证的无线安全专业工程师)
CWTS Certified Wireless Technology Specialist(认证的无线技术专员)

无线网络机构和规程

ACMA Australian Communications and Media Authority(澳大利亚通信与媒体主管机构)
ARIB Association of Radio Industries and Businesses(Japan) (日本无线工业及商贸联合会)
ATU African Telecommunications Union(非洲通信联盟)
CEPT European Conference of Postal and Telecommunications Administrations(欧洲邮电管理委员会)
CITEL Inter-American Telecommunication Commission(美洲国家电讯委员会)
CTIA Cellular Telecommunications and Internet Association(无线通信与互联网协会)
ERC European Radiocommunications Committee(欧洲无线电通讯委员会)
EWC Enhanced Wireless Consortium(无线增强联盟)
FCC Federal Communications Commission(联邦通信委员会)
FIPS Federal Information Processing Standards(联邦信息处理标准)
GLBA Gramm-Leach-Bliley Act(金融服务现代化法案)
HIPAA Health Insurance Portability and Accountability Act(健康保险流通与责任法案)
IAB Internet Architecture Board(互联网架构委员会)
ICANN Internet Corporation for Assigned Names and Numbers(互联网名称与数字地址分配机构)
IEC International Electrotechnical Commission(国际电工技术委员会)
IEEE Institute of Electrical and Electronics Engineers(电气与电子工程师协会)
IESG Internet Engineering Steering Group(互联网网工程指导组)
IETF Internet Engineering Task Force(互联网工程任务组)
IRTF Internet Research Task Force(互联网研究工作组)
ISO International Organization for Standardization(国际标准化组织)
ISOC Internet Society(互联网协会)
NEMA National Electrical Manufacturers Association(国际电气制造业协会)

NIST National Institute of Standards and Technology(美国国家标准技术研究所)

RCC Regional Commonwealth in the field of Communications(通信领域区域联盟)

SEEMesh Simple, Efficient, and Extensible Mesh(Mesh 标准化机构之一，与 WIMA 一样都是 802.11s 标准前身)

TGn Sync Task Group n Sync(快速 WLAN 标准联盟之一)

WECA Wireless Ethernet Compatibility Alliance(无线以太网兼容性联盟)

WIEN Wireless InterWorking with External Networks(与外网的无线互联)

Wi-Fi Alliance Wi-Fi Alliance(Wi-Fi 联盟)

WiMA Wi-Mesh Alliance(Mesh 标准化机构之一，与 SEE Mesh 一样都是 802.11s 标准前身)

WNN Wi-Fi Net News(无线网络每日新闻)

WWiSE World-Wide Spectrum Efficiency(全球频谱效率联盟)

测量单位

dB decibel(分贝)

dBd decibel referenced to a dipole antenna(以双偶极天线为参照物的分贝值)

dBi decibel referenced to an isotropic radiator(以全向辐射体为参照物的分贝值)

dBm decibel referenced to 1 milliwatt(以毫瓦为参照物的分贝值)

GHz gigahertz(千兆赫)

Hz hertz(赫兹)

KHz kilohertz(千赫)

mA milliampere(毫安)

MHz megahertz(兆赫)

mW milliwatt(毫瓦)

SNR signal-to-noise ratio(信噪比)

V volt(伏特)

VDC voltage direct current(直流电压)

W watt(瓦特)

技术术语

AAA authorization, authentication, and accounting(认证、授权与统计)

AC access category(访问类别)

AC alternating current(交流电)

ACK acknowledgment(确认)

AES Advanced Encryption Standard(高级加密标准)

AGL above ground level(地平面之上)

AID association identifier(关联标示符)

AIFS arbitration interframe space(仲裁帧间间隔)

AKM Authentication and Key Management(认证与密钥管理)

AM amplitude modulation(调幅)

A-MPDU Aggregate MAC Protocol Data Unit(聚合 MAC 协议数据单元)

A-MSDU Aggregate MAC Service Data Unit(聚合 MAC 服务数据单元)

AP access point(接入点)

APSD automatic power save delivery(计划自动节电传输)

ARS adaptive rate selection(自适应速率选择)

ARS automatic rate selection(自动速率选择)

AS authentication server(认证服务器)

ASK Amplitude Shift Keying(幅移键控)

ATEX Atmosphères Explosives(防爆指令)

ATF airtime fairness(通话时间公平)

ATIM announcement traffic indication message(通告流量指示消息)

BA Block Acknowledgment(块确认)

BER bit error rate(比特错误率)

BPSK Binary Phase Shift Keying(二进制相移键控)

BSA basic service area(基础服务区域)

BSS basic service set(基础服务集)

BSSID basic service set identifier(基础服务集标识)

BT Bluetooth(蓝牙)

BVI Bridged Virtual Interface(桥接虚拟接口)

CAD computer-aided design(计算机辅助设计)

CAM content addressable memory(内容可寻址内存)

CAM Continuous Aware mode(持续清醒模式)

CAPWAP Control and Provisioning of Wireless Access Points(无线 AP 控制与配置协议)

CCA clear channel assessment(空闲信道评估)

CC-AP cooperative control access point(协同控制 AP 协议)

CCI co-channel interference(同频干扰)

CCK Complementary Code Keying(补码键控)

CCMP Counter Mode with Cipher Block Chaining Message Authentication Code Protocol(计数器模式密码块链消息认证码协议)

CCX Cisco Compatible Extensions(思科兼容扩展协议)

CF Compact Flash(微型快擦写存储卡)

CF contention free(无竞争机制)

CFP contention-free period(无竞争周期)

CLI command-line interface(命令行)

CP contention period(竞争周期)

CRC cyclic redundancy check(循环冗余校验)

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance(载波侦听多路访问冲突避免)

CSMA/CD Carrier Sense Multiple Access with Collision Detection(载波侦听多路访问冲突检测)

CTS clear to send(清除发送)

CW contention window(竞争窗口)

CWG-RF Converged Wireless Group–RF Profile(融合无线组–射频性能)

DA destination address(目标地址)

DBPSK Differential Binary Phase Shift Keying(差分二进制相移键控)

DC direct current(直流电)

DCF Distributed Coordination Function(分布式协调功能)

DDF distributed data forwarding(分布式数据转发)

DFS dynamic frequency selection(动态频率选择)

DHCP Dynamic Host Configuration Protocol(动态主机分配协议)

DIFS Distributed Coordination Function interframe space(分布式协调功能帧间间隔)

DoS denial of service(拒绝服务攻击)

DQPSK Differential Quadrature Phase Shift Keying(差分正交相移键控)

DRS dynamic rate switching(动态速率交换)

DS distribution system(分布系统)

DSAS distributed spectrum analysis system(分布式频谱分析系统)

DSCP differentiated services code point(差分服务代码点)

DSM distribution system medium(分布式系统媒介)

DSP digital signal processing(数字信号处理)

DSRC Dedicated Short Range Communications(专用短程通信)

DSS distribution system services(分布式系统服务)

DSSS direct sequencing spread spectrum(直序扩频)

DTIM delivery traffic indication message(交付流量指示消息)

EAP Extensible Authentication Protocol(扩展认证协议)

EDCA Enhanced Distributed Channel Access(增强式分布信道访问)

EEG enterprise encryption gateway(企业加密网关)

EIFS extended interframe space(扩展帧间间隔)

EIRP equivalent isotropically radiated power(等效全向辐射功率)

EM electromagnetic(电磁)

EQM equal modulation(平等调制)

ERP Extended Rate Physical(扩展速率物理层)

ERP-CCK Extended Rate Physical–Complementary Code Keying(扩展速率物理层-补码键控)

ERP-DSSS Extended Rate Physical–Direct Sequencing Spread Spectrum(扩展速率物理层-直序扩频)

ERP-OFDM Extended Rate Physical–Orthogonal Frequency Division Multiplexing(扩展速率物理层-正交频分复用)

ERP-PBCC Extended Rate Physical–Packet Binary Convolutional Coding(扩展速率物理层-分组二进制卷积码)

ESA extended service area(扩展服务区域)

ESS extended service set(扩展服务集)

ESSID extended service set identifier(扩展服务集标识)

EUI extended unique identifier(扩展唯一标识符)

EWG enterprise wireless gateway(企业无线网关)

FAST Flexible Authentication via Secure Tunnel(安全隧道灵活认证协议，思科的一种 EAP 认证协议)

FCS frame check sequence(帧校验序列)

FEC forward error correction(前向纠错)

FHSS frequency hopping spread spectrum(跳频扩频)

FM frequency modulation(调频)

FMC fixed mobile convergence(固定与移动融合)

FSK Frequency Shift Keying(频移键控)

FSPL free space path loss(自由空间路径损耗)

FSR fast secure roaming(快速安全漫游)

FT fast BSS transition(快速 BSS 切换)

FZ Fresnel zone(菲尼尔区)

GCMP Galois/Counter Mode Protocol(伽罗瓦计数器模式协议，一种先进的加密协议)

GFSK Gaussian Frequency Shift Keying(高斯频移键控)

GI guard interval(保护间隔)

GMK Group Master Key(组主密钥)

GPS global positioning system(全球定位系统)

GRE Generic Routing Encapsulation(通用路由封装)

GSM Global System for Mobile Communications(全球移动通信系统)

GTC Generic Token Card(通用令牌卡)

GTK Group Temporal Key(组临时密钥)

GUI graphical user interface(图像化界面)

HC hybrid coordinator(混合协调)

HCCA Hybrid Coordination Function Controlled Channel Access(HCF 受控信道访问)

HCF Hybrid Coordination Function(混合协调功能)

HR-DSSS High-Rate Direct Sequencing Spread Spectrum(高速直序扩频)
HSRP Hot Standby Router Protocol(热备份路由协议)
HT High Throughput(高吞吐量)
HT-GF-STF high-throughput Greenfield short training field(HT 绿地模式短训练字段)
HT-LTF high-throughput long training field(HT 长训练字段)
HT-SIG high-throughput SIGNAL field(HT 信号字段)
HT-STF high-throughput short training field(HT 短训练字段)
HTTPS Hypertext Transfer Protocol Secure(超文本传输协议安全)
HWMP Hybrid Wireless Mesh Protocol(混合无线网状网协议)
IAPP Inter-Access Point Protocol(AP 间协议)
IBSS independent basic service set(独立的基础服务集)
ICMP Internet Control Message Protocol(互联网控制消息协议)
ICV Integrity Check Value(完整性校验值)
IDS intrusion detection system(入侵检测系统)
IE Information Element(信息元素)
IFS interframe space(帧间间隔)
IP Internet Protocol(互联网协议)
IP Code Ingress Protection Code(国际防护等级)
IPSec Internet Protocol Security(互联网协议安全)
IR infrared(红外技术)
IR intentional radiator(主动辐射器)
IS integration service(集成服务)
ISI intersymbol interference(码间干扰)
ISM Industrial, Scientific, and Medical(工业科学和医疗)
ITS Intelligent Transportation Systems(智能交通系统)
IV Initialization Vector(初始化向量)
L2TP Layer 2 Tunneling Protocol(第 2 层隧道协议)
LAN local area network(局域网)
LEAP Lightweight Extensible Authentication Protocol(轻量型扩展认证协议)
LLC Logical Link Control(逻辑链路控制)
L-LTF legacy (non-HT) long training field(传统非 HT 长训练字段)
LOS line of sight(视线)
L-SIG legacy (non-HT) signal(传统非 HT 信号)
L-STF legacy (non-HT) short training field(传统非 HT 短训练字段)
LWAPP Lightweight Access Point Protocol(轻量型 AP 协议)
MAC media access control(媒介访问控制)
MAHO Mobile Assisted Hand-Over(移动辅助切换)
MAN metropolitan area network(城域网)

MAP mesh access point(网状接入点)

MCA multiple-channel architecture(多信道架构)

MCS modulation and coding schemes(调制编码计划)

MD5 Message Digest 5(消息摘要协议第 5 版)

MDI media dependent interface(媒介独立接口)

MFP management frame protection(管理帧保护)

MIB Management Information Base(管理信息数据库)

MIC Message Integrity Check(消息完整性校验)

MIMO multiple-input multiple-output(多入多出)

MMPDU MAC Management Protocol Data Unit(MAC 管理协议数据单元)

MP mesh point(网状点)

MPDU MAC Protocol Data Unit(MAC 协议数据单元)

MPP mesh point portal(Mesh 节点门户)

MPPE Microsoft Point-to-Point Encryption(微软点到点加密)

MRC maximal ratio combining(最大比混合)

MSDU MAC Service Data Unit(MAC 服务数据单元)

MSSID Mesh Service Set Identifier(Mesh 服务集标识)

MTBA multiple traffic ID block acknowledgment(多流量 ID 块确认)

MTU maximum transmission unit(最大传输单元)

MU-MIMO Multi-user MIMO(多用户多入多出)

NAT Network Address Translation(网络地址转换)

NAV network allocation vector(网络分配向量)

NEC National electrical code(国家电气规程)

OFDM Orthogonal Frequency Division Multiplexing(正交频分复用)

OS operating system(操作系统)

OSI model Open Systems Interconnection model(开放系统互连)

OUI Organizationally Unique Identifier(组织唯一标示符)

PAN personal area network(个人网络)

PAT Port Address Translation(端口地址转换)

PBCC Packet Binary Convolutional Coding(分组二进制卷积码)

PBX private branch exchange(专用分组交换机)

PC point coordinator(点协调)

PCF Point Coordination Function(点协调功能)

PCI Peripheral Component Interconnect(外部设备互连)

PCMCIA Personal Computer Memory Card International Association (PC Card) (个人计算机存储卡国际协会)

PCO phased coexistence operation(阶段共存模式)

PD powered device(受电设备)

PEAP Protected Extensible Authentication Protocol(受保护的扩展认证协议)
PHY physical layer(物理层)
PIFS Point Coordination Function interframe space(点协调功能帧间间隔)
PLCP Physical Layer Convergence Procedure(物理层汇聚协议)
PMD Physical Medium Dependent(物理媒介相关)
PMK Pairwise Master Key(成对主密钥)
PN pseudo-random number(伪随机数)
PoE Power over Ethernet(以太网供电)
POP Post Office Protocol(邮局协议)
PPDU PLCP Protocol Data Unit(PLCP 协议数据单元)
PPP Point-to-Point Protocol(点到点协议)
PPTP Point-to-Point Tunneling Protocol(点到点隧道协议)
PSE power-sourcing equipment(供电设备)
PSK Phase Shift Keying(相移键控)
PSK preshared key(预共享密钥)
PSMP Power Save Multi-Poll(多点轮询节电机制)
PSPF Public Secure Packet Forwarding(公共安全数据包转发)
PS-Poll power save poll(节点轮询)
PSTN public switched telephone network(公共交换电话网)
PTK Pairwise Transient Key(成对临时密钥)
PtMP point-to-multipoint(点到多点)
PtP point-to-point(点到点)
QAM quadrature amplitude modulation(正交调幅)
QAP quality-of-service access point(服务质量接入点)
QBSS quality-of-service basic service set(服务质量基础服务集)
QoS quality of service(服务质量)
QSTA quality-of-service station(服务质量站)
QPSK Quadrature Phase Shift Keying(正交相移键控)
RA receiver address(接收方地址)
RADIUS Remote Authentication Dial-In User Service(远程认证拨入用户服务)
RBAC role-based access control(基于角色的访问控制)
RF radio frequency(射频)
RFC request for comment(请求注解)
RFSM radio frequency spectrum management(射频频谱管理)
RIFS reduced interframe space(缩减帧间间隔)
RRM radio resource measurement(无线资源管理)
RSL received signal level(接收信号水平)
RSN robust security network(强健安全网络)

RSNA robust security network association(强健安全网络联盟)
RSSI received signal strength indicator(接收信号强度指示)
RTLS real-time location system(实时定位系统)
RTS request to send(请求发送)
RTS/CTS request to send/clear to send(请求发送/清除发送)
RWG residential wireless gateway(家庭无线网关)
RX receive or receiver(接收方)
SA source address(源地址)
S-APSD scheduled automatic power save delivery(计划自动节电交付)
SCA single-channel architecture(单信道架构)
SD Secure Digital(安全数字，一种存储标准)
SDR software defined radio(软件可定义无线接口)
SIFS short interframe space(短帧间间隔)
SISO single-input single-output(单入单出)
SM spatial multiplexing(空间复用)
SMTP Simple Mail Transfer Protocol(简单邮件传输协议)
SNMP Simple Network Management Protocol(简单网络管理协议)
SNR signal-to-noise ratio(信噪比)
SOHO small office/home office(小型办公/家庭办公)
SOM system operating margin(系统操作容限)
SQ signal quality(信号质量)
SSH Secure Shell(安全外壳，一种远程交互式访问协议)
SSID service set identifier(服务集标识)
SSL Secure Sockets Layer(安全套接字层)
STA station(站)
STC Space Time Coding(空时编码技术)
STP Spanning Tree Protocol(生成树)
TA transmitter address(传输方地址)
TBTT target beacon transmission time(目标信标传输时间)
TCP/IP Transmission Control Protocol/Internet Protocol(传输控制协议/互联网协议)
TIM traffic indication map(流量指示图)
TKIP Temporal Key Integrity Protocol(临时密钥集成协议)
TLS Transport Layer Security(传输层安全)
TPC transmit power control(传输功率控制)
TSN transition security network(过渡安全网络)
TTLS Tunneled Transport Layer Security(隧道传输层安全)
TX transmit or transmitter(发送方)
TxBF transmit beamforming(传输波速成形)

TXOP transmit opportunity(传输机会)

U-APSD unscheduled automatic power save delivery(非计划自动节电交付)

UEQM unequal modulation(非等调制)

UNII Unlicensed National Information Infrastructure(不需许可的国家信息基础设施)

UP user priority(用户优先级)

USB Universal Serial Bus(通用串行总线)

VHT Very high throughput(超高吞吐量)

VLAN virtual local area network(虚拟局域网)

VoIP Voice over IP(IP 语音)

VoWiFi Voice over Wi-Fi(WiFi 语音)

VoWIP Voice over Wireless IP(无线 IP 语音)

VPN virtual private network(虚拟专用网络)

VRRP Virtual Router Redundancy Protocol(虚拟路由冗余协议)

VSWR voltage standing wave ratio(电压驻波比)

WAN wide area network(广域网)

WAVE Wireless Access in Vehicular Environments(车载环境下的无线接入)

WDS wireless distribution system(无线分布系统)

WEP Wired Equivalent Privacy(有线等效私密协议)

WGB workgroup bridge(工作组网桥)

WIDS wireless instruction detection system(无线入侵检测系统)

Wi-Fi 有时认为是 *wireless fidelity* 的缩写，没有正式定义；WiFi 通常被认为是定义 802.11 技术的术语

WIGLE Wireless Geographic Logging Engine(无线地理记录引擎)

WiMAX Worldwide Interoperability for Microwave Access(全球微波接入互操作性)

WIPS wireless intrusion prevention system(无线入侵防御系统)

WISP Wireless Internet Service Provider(无线互联网服务提供商)

WLAN wireless local area network(无线局域网)

WLSE Wireless LAN Solution Engine(无线局域网管理引擎，思科旧有的无线管理系统)

WM wireless medium(无线媒介)

WMAN wireless metropolitan area network(无线城域网)

WMM Wi-Fi Multimedia(WiFi 多媒体)

WMM-PS Wi-Fi Multimedia Power Save(WMM 节电)

WMM-SA Wi-Fi Multimedia Scheduled Access(WiFi 多媒体计划访问)

WNMS wireless network management system(无线网络管理系统)

WPA Wi-Fi Protected Access(WiFi 保护接入)

WPAN wireless personal area network(无线个人网络)

WPP Wireless Performance Prediction(无线性能评估)

WWAN wireless wide area network(无线广域网)

WZC Wireless Zero Configuration(无线零配置)

XOR exclusive or(异或)

功率管理规定

FCC(美国联邦通信委员会)负责管理美国境内以及往来美国的通信。其他国家也有类似的监管机构，负责管理主动辐射器(intentional radiator)的输出功率以及 802.11 天线的辐射功率(即 EIRP)。制定输出功率管理规定的目的在于尽可能减小设备对本频段、相邻频段或附近频段的干扰。

监管机构一般负责管理两类通信的输出功率：点对多点(PtMP)通信与点对点(PtP)通信，前者的功率要求通常比后者更为严格。这是因为点对多点信号向所有方向辐射，其覆盖范围较大，因此更容易对其他设备造成干扰。而高增益天线向外辐射的点对点信号较为集中，干扰到其他设备的几率较小。下面将介绍 FCC 制定的功率管理规定。

2.4GHz ISM 频段点对多点(PtMP)通信

点对多点网络由一台中央设备和若干与中央设备通信的设备构成。如果中央设备使用全向天线，FCC 会自动将通信的性质界定为点对多点通信。不过使用全向天线并非点对多点通信的强制要求，许多接入点也使用半指向贴片天线收发数据。

FCC 规定，主动辐射器的最大输出功率为 1W(30dBm)，天线的最大辐射功率(EIRP)为 4W(36dBm)。也就是说，如果主动辐射器的最大输出功率为 30dBm(1W)，由于 EIRP 被限制为 36dBm(4W)，则可用的最大天线增益为 6dBm。请记住，EIRP 是主动辐射器输出功率与天线增益之和。

受 FCC 的输出功率规定所限，无论采用何种方式也无法使 EIRP 超过 36dBm(4W)。换句话说，如果希望使用增益更高的天线，则必须将天线增益从 EIRP 中扣除，以计算主动辐射器的最大可用功率。例如，使用 9dBi 贴片天线时，主动辐射器的最大输出功率为 27dBm(36dBm－9dBi＝27dBm)，即 500mW。如果使用增益超过 6dBi 的天线，则增益每提高 1dB，主动辐射器的输出功率必须相应降低 1dB，这称为 1:1 法则。

5GHz UNII 频段点对多点(PtMP)通信

5GHz UNII 频段点对多点通信与 2.4GHz ISM 点对多点通信的功率管理规定相同。点对多点设备可使用 6dBi 天线而不会违反最大 EIRP 的规定。如果希望继续提高天线增益，则必须相应降低主动辐射器的输出功率。FCC(美国联邦通信委员会)和 ERC(欧洲无线通信委员会)对 5GHz 点对多点通信做了明确规定，图 B-1 和 B-2 分别显示了主动辐射器的最大输出功率与 EIRP 的管理规定。

IEEE 将各频段主动辐射器的最大输出功率定义如下：

UNII-1: 40 mW
UNII-2: 200 mW
UNII-2E: 200 mW
UNII-3: 800 mW

FCC 与 ERC 规定，当 EIRP 超过 500mW 时，系统必须使用 TPC(传输功率控制)。

FCC 与 ERC 规定，5GHz 无线局域网设备必须使用 DFS(动态频率选择)，以免干扰到雷达传输。

图 B-1　5GHz 点对多点通信：主动辐射器功率管理规定

EIRP(等效全向辐射功率)

UNII-1 频段

FCC：主动辐射器的最大输出功率为 50mW，最大天线增益为 6dBi，EIRP 为二者之和

(IEEE 将主动辐射器的最大输出功率限制为 40mW)

UNII-2 与 UNII-2 扩展频段

FCC：主动辐射器的最大输出功率为 250mW，最大天线增益为 6dBi，EIRP 为二者之和

(IEEE 将主动辐射器的最大输出功率限制为 200mW)

UNII-3 频段

FCC：主动辐射器的最大输出功率为 1000mW，最大天线增益为 6dBi，EIRP 为二者之和

(IEEE 将主动辐射器的最大输出功率限制为 800mW)

图 B-2　5GHz 点对多点通信：EIRP 管理规定

2.4GHz ISM 频段点对点(PtP)通信

在点对点网络中，两台设备使用定向天线相互通信。2.4GHz ISM 频段点对点通信与该频段点对多点通信的功率管理规定相同，即主动辐射器的最大输出功率为 1W，采用 6dBi 天线，最大 EIRP 为 4W。尽管主动辐射器的最大输出功率仍然被限制为 1W，不过由于设备使用定向天线且仅与一台设备进行通信，FCC 放宽了对天线增益和 EIRP 的限制。如果使用增益超

过 6dBi 的天线，则增益每提高 3dB，主动辐射器的输出功率必须相应降低 1dB，这称为 3:1 法则。

由于 EIRP 是主动辐射器输出功率与天线增益之和，如果天线增益提高 3dB 且主动辐射器的输出功率降低 1dB，则 EIRP 将提高 2dB。为便于理解，可将 3:1 法则简单记忆为 3-2-1。即天线增益提高 3dB，EIRP 增加 2dB，主动辐射器的输出功率降低 1dB。3:1 法则如表 B-1 所示。

表 B-1 3:1 法则

主动辐射器输出功率	天 线 增 益	最大 EIRP
30dBm(1W)	6dBi	+36dBm(4W)
29dBm	9dBi	+38dBm(6.3W)
28dBm	12dBi	+40dBm(10W)
27dBm	15dBi	+42dBm(16W)
26dBm	18dBi	+44dBm(25W)
25dBm	21dBi	+46dBm(39.8W)
24dBm	24dBi	+48dBm(63W)
23dBm	27dBi	+50dBm(100W)
22dBm	30dBi	+52dBm(158W)

5GHz UNII 频段点对点(PtP)通信

FCC 针对 5GHz UNII-1 和 UNII-2 频段点对点通信与这两个频段点对多点通信的功率管理规定相同。由于 UNII-3 频段通常用于远距离点对点通信，因此 FCC 对该频段的功率管理规定有所不同。如果固定点对点发射机输出的最大功率为 30dBm(1W)，那么可以采用增益最高为 23dBi 的天线而不必对主动辐射器做出任何调整。此时，最大 EIRP 为 53dBm(200W)。如果使用增益超过 23dBi 的天线，则增益每提高 1dBi，主动辐射器的输出功率必须相应降低 1dB，即必须遵守 1:1 法则。

附录 C 关于本书附加学习工具

本附录中包含：

- √ 附加学习工具
- √ 系统要求
- √ 如何使用学习工具
- √ 故障排除

附加学习工具

以下各节按类别排列并汇总了可在本书网站上找到的软件和其他工具。如果你需要安装方面的帮助，请参阅本附录的“如何使用学习工具”部分中的安装说明。

本书附加学习工具可在 www.sybex.com/go/cwna3e 下载，你可以看到如何将文件下载到电脑硬盘的说明。

Sybex 测试引擎

本文件包含了 Sybex 测试引擎，其中包括附赠三个考试练习、评估测试以及章节复习题(已被本书收录)。

电子抽认卡

这些便利的电子抽认卡一面是问题，另一面是答案。

术语表(pdf 格式)

包括了 pdf 格式的电子版术语表，可用 Adobe Reader 打开阅览。

Adobe Reader

我们还包括了 Adobe Reader 的安装文件，以便你查看 pdf 文件。如果要了解关于 Adobe Reader 的更多信息或者更新的软件版本，可访问 Adobe 的官方网站：www.adobe.com/products/reader/。

系统需求

确保你的计算机满足如下的系统最低需求：

- 运行微软 Windows 98/Windows 2000/windows NT(SP4 或更新)/Windows Me/Windows XP/Wndows Vista 或 Windows 7
- 互联网连接

如果你的计算机无法满足大部分需求，在使用软件和文件的时候可能会遇到问题，请参阅本书网站上的 Readme 文件。

如何使用学习工具

请按如下步骤安装软件：

(1) 将 ZIP 文件下载到本地电脑硬盘，解压缩。下载方法请参考 www.sybex.com/go/cwna3e 上的指南文件。

(2) 单击 Start.exe。

(3) 如果希望使用学习工具，请阅读许可协议后，单击 Accept 按钮。

这时会出现学习工具界面，你可以轻易访问希望查看的内容。

故障排除

Wiley 提供的程序可以在大多数满足最低系统要求的计算机上工作。但是你的计算机可能因为某些原因无法正确运行。

可能有两个主要的原因：计算机内存不足或与正在运行的程序冲突。如果你看到出现“内存不足”或者“无法继续安装”提示，请尝试按下面的步骤操作。

- 关闭杀毒软件。安装程序可能有时看起来与病毒程序相似，使杀毒软件误报。
- 关闭所有正在运行的程序。运行的程序越多，可供其他程序使用的内存越少。安装程序通常会更新文件和程序；如果让其他程序一直运行，将可能无法安装。
- 安装更多的内存。这样做可能会比较昂贵。但增加内存确实可以帮助提高计算机运行速度，并可以同时运行更多的程序。

用户关怀

如果对本书附加学习工具仍有疑问，请联系 Wiley 产品技术支持。电话：(800) 762-2974.74，或在 http://sybex.custhelp.com/发送邮件咨询。