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：

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：
装 订 者：
经　　销：全国新华书店
开　　本：185mm×260mm　　印　　张：36.25　　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：

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)。

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。

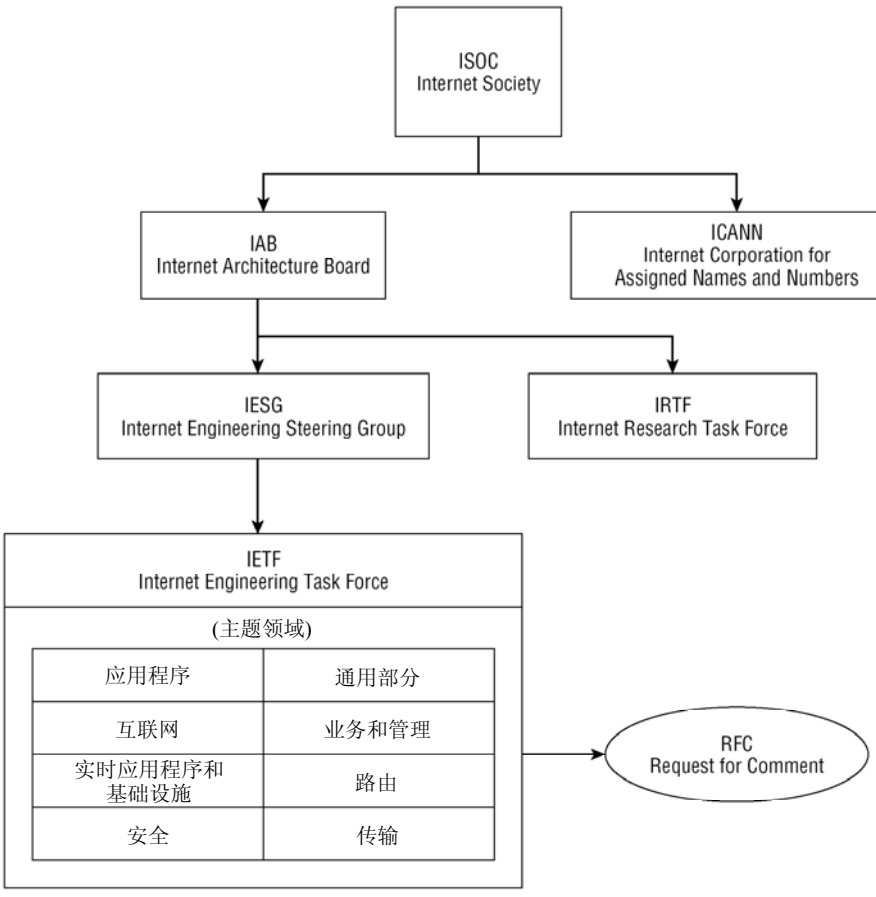

图 1-1　ISOC 层级架构

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。

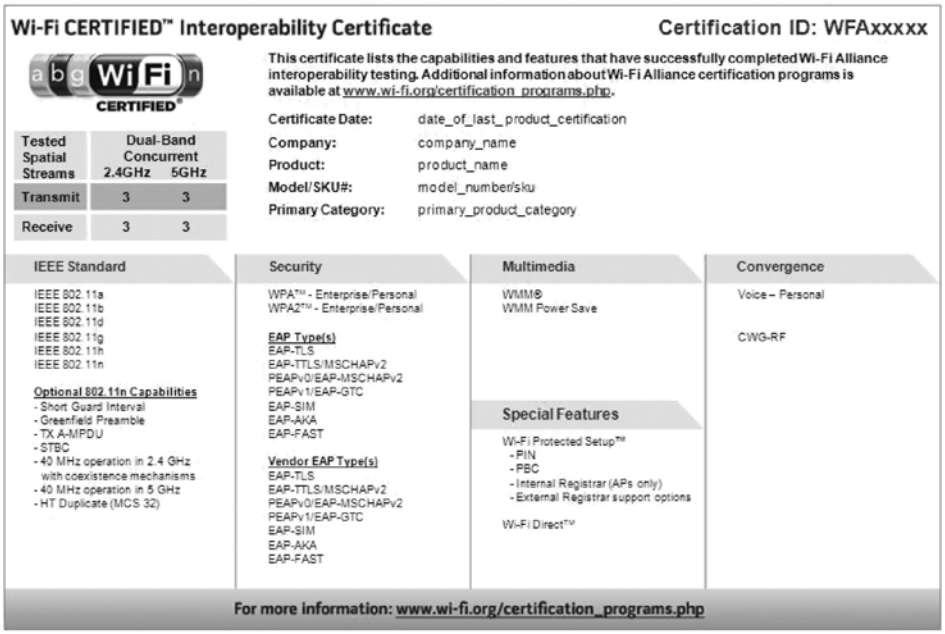

图 1-3　Wi-Fi 互操作性证书

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。

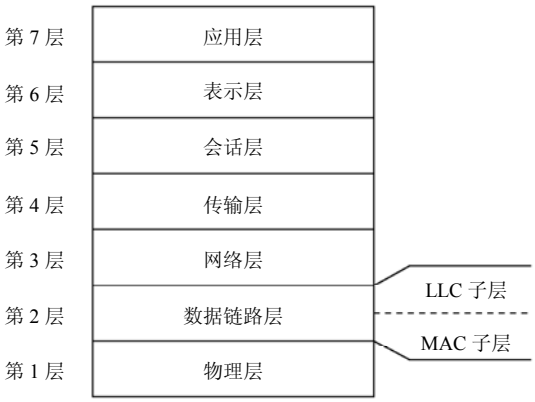

图 1-4　OSI 模型

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。

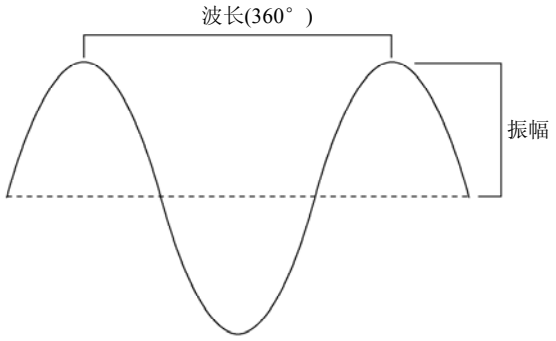

图 1-5　波的波长与振幅

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。

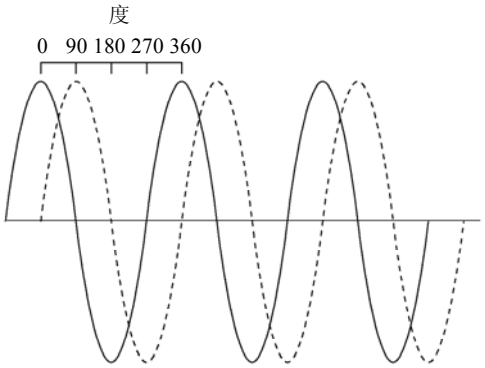

图 1-6　两个相同的波，不过它们彼此 90° 异相

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。

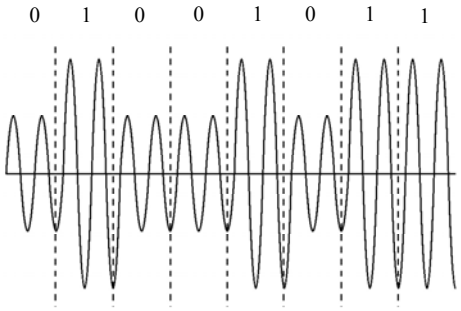

图 1-7 幅移键控示例(ASCII 大写字母 K)

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。

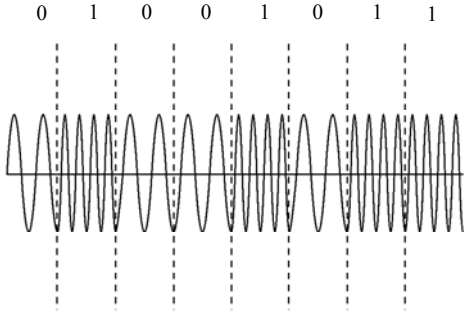

图 1-8　频移键控示例(ASCII 大写字母 K)

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。

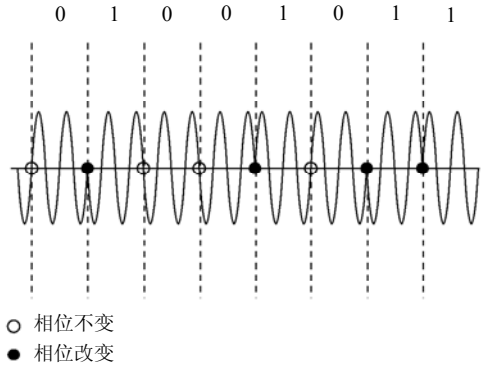

图 1-9　相移键控示例(ASCII 大写字母 K)

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。

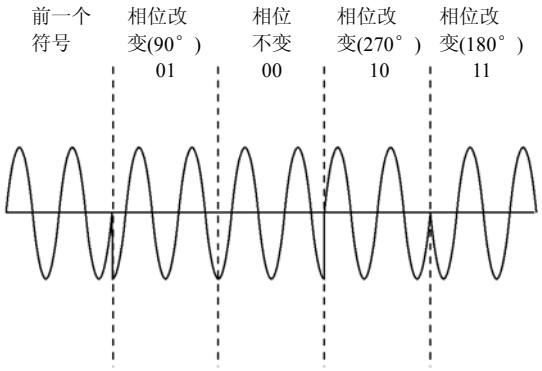

图 1-10　多进制相移键控示例(ASCII 大写字母 K)

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 技术大有裨益。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。

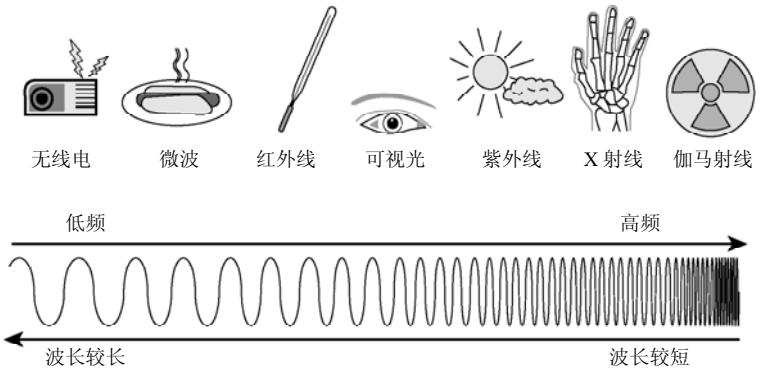

图 2-1　电磁频谱

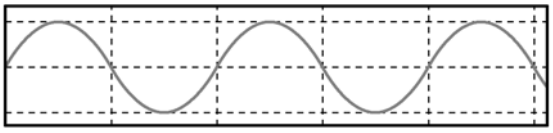

图 2-2　正弦波

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。

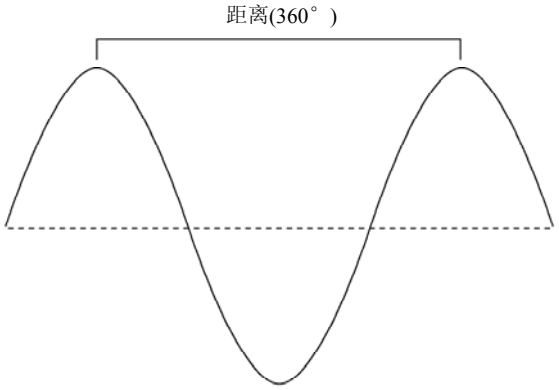

图 2-3 波长

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

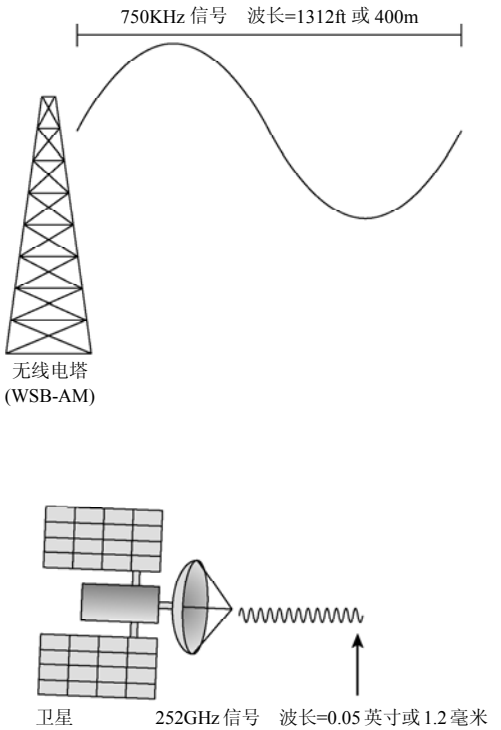

图 2-4 频率 750KHz 信号与频率 252GHz 信号的波长比较

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。

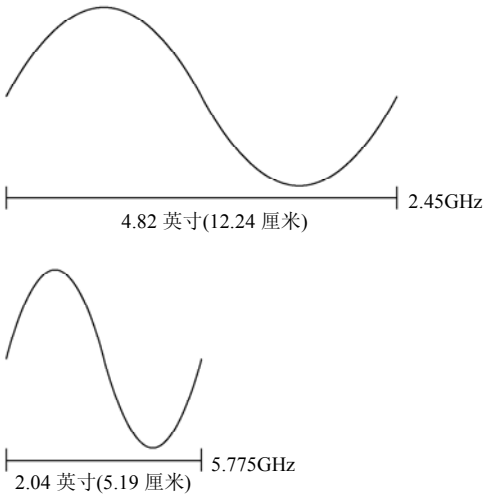

图 2-5　2.45GHz 波长与 5.775GHz 波长

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

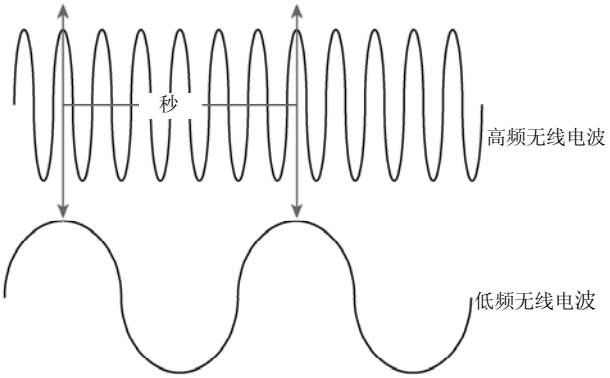

图 2-7　频率

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：

λ=c/f 或 f=c/λ，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。

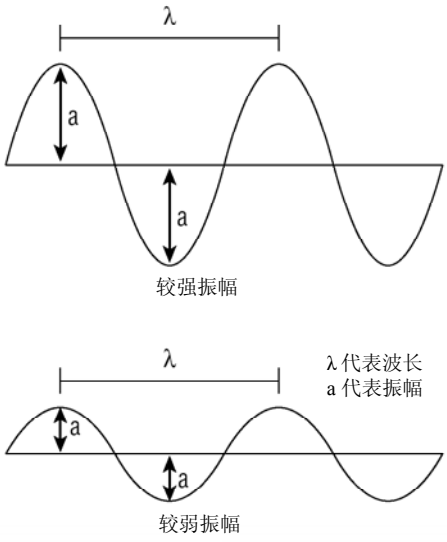

图 2-8　振幅

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。

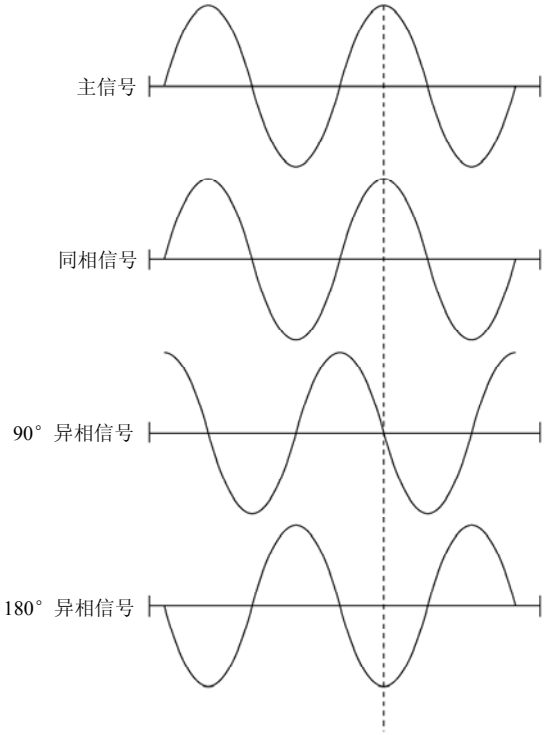

图 2-9 相位关系

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)。

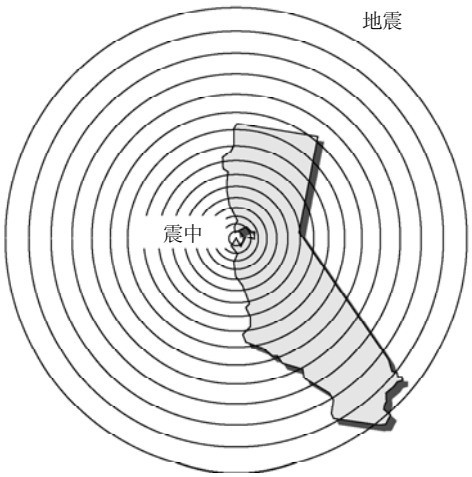

图 2-10　传播模拟

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。

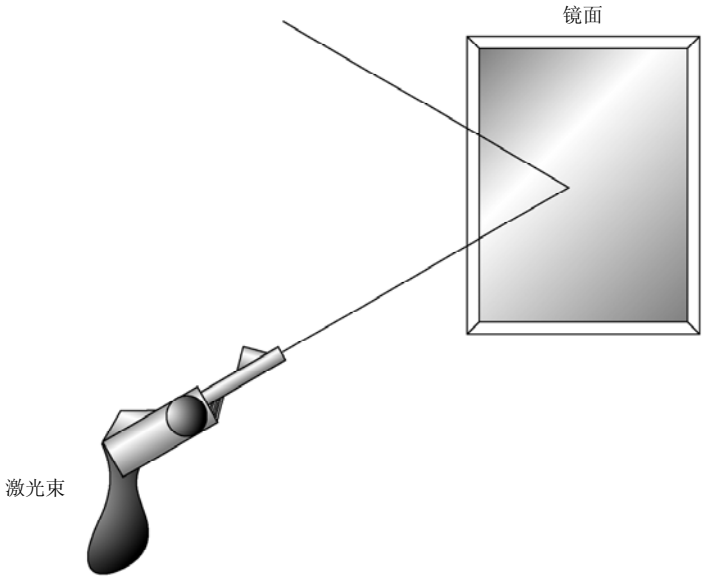

图 2-11　反射模拟

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。

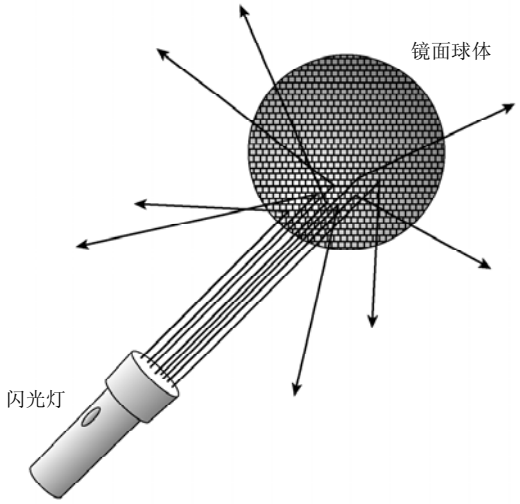

图 2-12　散射模拟

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。

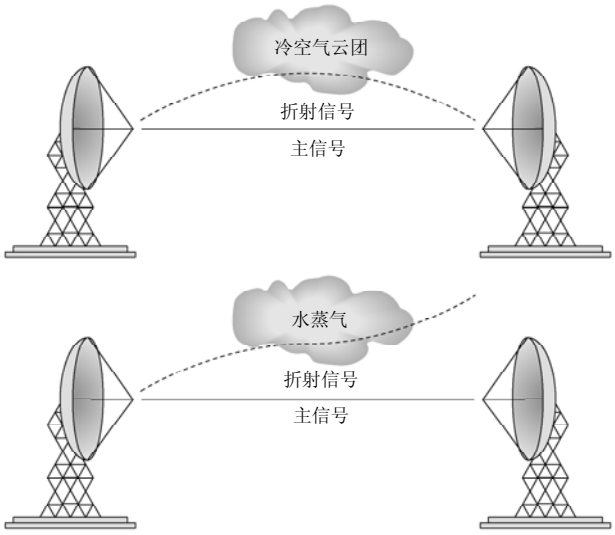

图 2-13　折射

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。

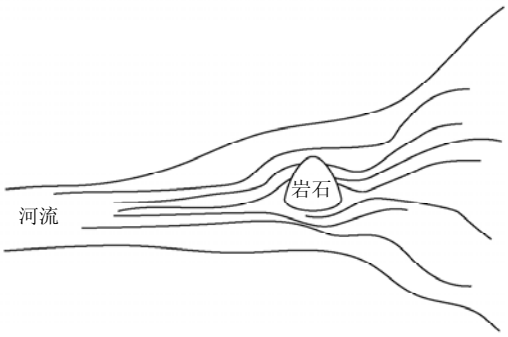

图 2-14　衍射模拟

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。

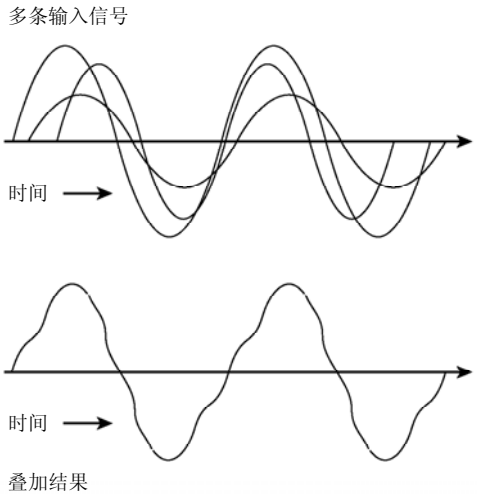

图 2-16 数据损坏 ISI

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。

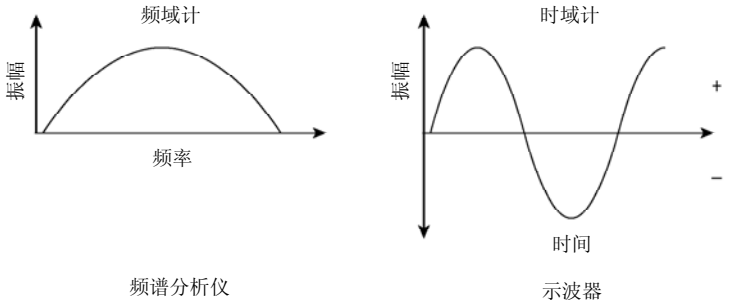

图 2-17　射频信号测量工具

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