Cisco Systems

Cisco 职业认证培训系列
CISCO CAREER CERTIFICATIONS

ciscopress.com

CCIE Security 认证考试指南

CCIE® Self-Study
CCIE Security
Exam Certification Guide

Official self-study test preparation guide
for the CCIE Security written exam

内附光盘

Henry Benjamin, CCIE #4695 著
卓林, CCIE #8867 译

人民邮电出版社
POSTS & TELECOM PRESS

Cisco 职业认证培训系列

CCIE Security认证考试指南

Henry Benjamin, CCIE #4695著

卓林，CCIE #8867 译

人 民 邮 电 出 版 社

图书在版编目(CIP)数据

CCIE Security 认证考试指南/（美）本杰明（Benjamin, H.）著；卓林译.
—北京：人民邮电出版社，2004.6
（Cisco 职业认证培训系列）
ISBN 7-115-12225-3

Ⅰ.C... Ⅱ.①本...②卓... Ⅲ.计算机网络—工程技术人员—资格考核—自学参考资料
Ⅳ.TP393
中国版本图书馆 CIP 数据核字（2004）第 047697 号

Cisco 职业认证培训系列
CCIE Security 认证考试指南

◆ 著 Henry Benjamin,CCIE #4695
译 卓 林，CCIE #8867
责任编辑 李 际

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 ciscobooks@ptpress.com.cn
网址 http://www. ptpress.com.cn
读者热线 010-67132705
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：28
字数：679 千字 2004 年 6 月第 1 版
印数：1-3 500 册 2004 年 6 月北京第 1 次印刷

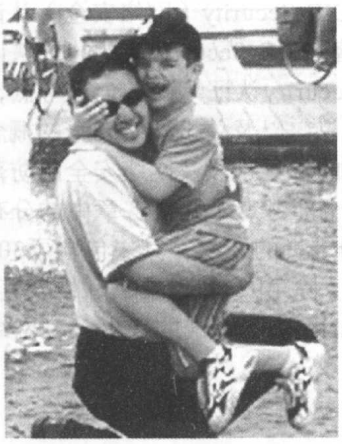
著作权合同登记 图字：01 - 2003 - 0660 号
ISBN 7-115-12225-3/TP • 3942
定价：65.00 元（附光盘）
本书如有印装质量问题，请与本社联系 电话：（010）67129223

内容提要

本书的目的是帮助读者准备CCIE Security（网络安全）认证的笔试（考试号#350-018），同时也有助于准备CCIE Security认证的重认证考试（考试号#350-009）。本书涵盖了CCIE Security认证笔试的全部考点，内容涉及一些基础性的常用网络概念、应用协议，以及关于网络安全的概念和协议，更深入的内容包括因特网上黑客攻击的常见手段及网络安全的防范技术。本书第1章对CCIE Security认证笔试的全部考点及其在各章中的分布情况做了清晰的介绍。随书所附的光盘是一份宝贵的礼物，其中包含了300多道模拟试题、示例配置、本书的英文电子版（除第9章和附录C），以及其他更多资料。

本书主要针对参加CCIE Security认证考试的考生，对网络安全技术人员也是一本难得的参考书。

作者简介



Henry Benjamin, CCIE #4695, 拥有3项CCIE证书，分别是1999年5月获得的路由与交换认证证书、2001年6月获得的ISP Dial认证证书以及2002年5月获得的通信与服务认证证书。其超过10年的Cisco网络工作经验包括了大型IGRP、EIGRP、BGP和OSPF等IP网络的规划、设计以及实施。目前，Henry在澳大利亚悉尼的一家大型IP组织里面担任首席网络设计师，为全澳大利亚和亚洲的网络设计和实施提供服务。而在过去的两年里，Henry则是悉尼的CCIE全球性组织中的主力。作为该组织的一名高级核心成员，其工作包括为著名的CCIE R/S、CCIE网络安全和CCIE C/S认证考试的实验部分以及CCIE重认证考试出题。此外，Henry曾经写了两本著作：*CCNP Practical Studies: Routing*（Cisco Press）和*CCIE R&S Exam Cram*。1991年，Henry在悉尼大学获得了航空工程专业的学士学位。

特约作者简介

Gert De Laet，CCIE #2657，拥有CCIE网络安全认证证书和路由与交换认证证书。他在互联网络领域工作超过9年。Gert目前在比利时布鲁塞尔Cisco的CCIE小组中担任CCIE协议/内容工程师以及EMEA的项目经理。此外，他还拥有电子专业的工程学位。Gert是本书第9章的作者，也是整本书主要的技术审稿人。

技术审稿人简介

Anand Deveriya，CCIE #10401，是网络安全的CCIE以及MCSE，具有5年以上在LAN/WAN以及Cisco产品网络安全方面的经验。目前他是Summerville Senior Living的网络经理，负责全国性VoIP帧中继WAN网络的设计和部署，同时也参与LAN/WAN网络安全的监控、入侵试验的测试以及OS的强化工作。而此前，他在NEC担任一名网络工程师，其工作是利用路由器、交换机、PIX以及VPN设备，部署可扩展的、安全的、具有冗余的主干网络和园区网。

Charles Resch，CCIE #6582，目前在Nuclio担任高级网络工程师，负责管理设备的安装与配置，实现对客户网络的监控。他所做过的项目包括配置双Cisco PIX防火墙的电子商务站点、Cisco内容交换机（CSS）的负载均衡系统、Intel和SonicWall SSL的下载系统、Cisco交换机（HSRP-VLAN）以及Cisco安全入侵检测系统（CSIDS）。此外，他还在西北商业学院的信息技术院中担任过高级讲师以及Globalcom 公司高级互联网工程师。他在Cisco硬件产品、Cisco IOS软件、众多的可路由和路由选择协议以及操作系统方面有着极其丰富的经验。

Gert Schauwers，CCIE #6924，拥有网络安全、路由与交换以及通信与服务3项CCIE证书，在互联网络方面有着4年以上的工作经验，目前在布鲁塞尔CCIE小组担任一名CCIE内容工程师，拥有电子专业的工程学位。

原书致谢

我必须感谢Cisco Press的诸位人士，感谢你们将此极具挑战性的工作交付给我，感谢你们给予我的支持与帮助。

Brett Bartow是一位了不起的人士，我衷心地感谢你无与伦比的洞察力和对我完全的信任。Andrew Cupp，或者是像大家称呼你的那样，Drew，你是那样的了不起，你的编辑与技术方面的能力真是让我惊讶，没有你的努力，这本书无法达到现在的水平。目前市面上的书是没有办法和这本书相比较的。谢谢你们以优秀的笔触完成了所有的章节。你们的付出使该书得到了进一步的完善。Cisco Press是一个由诸位这样勤奋用功的员工们组成的大家庭。受邀请撰写此书实在是一件令人愉快的事情。任何有灵感的作者能够选择的出版社只有一个，那就是Cisco Press。此外，我也要感谢Tammi Ross、Tracy Hughes和Ginny Bess，感谢你们给予我的所有帮助，感谢San Dee Phillips和Patrick Kanouse精彩的笔墨为读者今天所看到的本书而做出的贡献。

各位技术编辑们，Gert De Laet、Gert Schauwers、Anand Deveriya和Charles Resch，为本书奉献了大量宝贵的技术知识，事实表明，他们有一天也能从事自己的写作，而且我深信这一天不会太远。其中特别要感谢Gert De Laet，谢谢你帮我撰写第9章网络安全部分的内容，这真是令人愉快和让我感到荣幸的一件事情。感谢Gert Schauwers在过去的12个月里给我的鼓励，我真的很怀念在San Jose一起打高尔夫球的日子。

非常感谢Gert D.和Gert S.所给予我的真挚友谊。

最后，我还要感谢一个人，那就是我亲爱的妻子Sharon以及我们惟一的儿子Simon（我们的小蜘蛛侠）。我非常感谢你们在我需要时间完成此书的时候对我的理解和体谅。我非常珍惜和家人在一起的时间，我那个正在长大的小家伙让我觉得作为他的爸爸是一件很自豪的事情。Simon，我愿意永远的陪着你走来走去，陪你去看新的蜘蛛侠系列片。我也要感谢我的爸爸和妈妈，感谢你们以自身的伟大把我抚养成人，感谢我的岳父岳母（Nana和Mate以及Princess），感谢你们在过去的6个月里对我的鼓励，感谢Albert舅舅做的那些美妙的油炸面圈和你对我的勉励，感谢动人的Melanie姐姐在我有生之年对我的爱护，今年姐姐以优异的成绩通过了考试成为了一名注册护士，你真是一位伟大的姐姐，我真的为你骄傲，Mel。感谢我在世界上最美丽的城市罗马学习物理时的朋友Mello Yello. Massimo Piccinini，感谢你在那5年里给与我的友谊和爱护；你真是一位很棒的朋友（amico（意）朋友）。

此外，我还要感谢我亲爱的姑妈，她们在和我呆在一起的日子里给了我难以忘怀的勉励和爱护，谢谢你们，Lyda姑妈和Alice姑妈。

原书序

CCIE考试的目的是挑选出优秀的互联网络人才，以帮助个人、公司、行业乃至国家在网络世界中获得成功。其中，CCIE网络安全认证考试是为了挑选网络安全领域的优秀人才。

CCIE网络安全认证的第一步是极具挑战性的笔试，该考试将考查较大范围内的技术知识。如果成绩达到专家水平，考生就能够进一步参加考查实际技能的CCIE网络安全实验认证考试。

为什么要参加网络安全认证?

网络安全是网络行业中增长速度最快的领域之一。互联网的广泛发展、电子商务的快速增长以及公共网络和专用网络所面临日益增加的威胁，都使得网络安全和信息保护成为各种组织最为关心的问题。因此，对具备此类知识和技能的人才的需求也日益增长。所以，受过专门培训的网络安全人才在未来的日子里是非常受欢迎的。

为什么要参加CCIE网络安全认证?

CCIE网络安全认证的目的就是选拔优秀的网络安全专家，通过该考试的考生将名列世界优秀网络安全专家的行列，这对大家的职业生涯、发展机会以及薪水来说都是大有裨益的。

CCIE网络安全认证使公司无需花费培训成本就可以获得优秀的网络安全专家，保护他们重要的信息资产。

这本书对那些想要参加CCIE网络安全认证考试的考生来说是一份宝贵的财富。通过本书的学习，为CCIE网络安全认证笔试做准备的考生们能够获得大量深入的网络安全知识。这本书主要深入地描述了网络安全各个方面的特性，让读者能够领会并且可以驾驭网络安全方面的一些细节知识、复杂内容以及潜在的网络安全隐患。本书及所附光盘包含的大量内容是大家在准备CCIE网络安全认证考试时强大的补充工具。

祝大家好运！

Gert De Laet
Cisco Systems公司
CCIE网络安全认证产品经理

前　言

CCIE网络安全认证是越来越为人们所接受的一门互联网络认证考试，也是目前世界上最为流行的网络安全认证考试之一。尽管CCIE认证考试是以CCNA和CCNP的知识为基础的，但并不是说参加CCIE考试之前一定要先参加这两门考试。然而，参加CCNA和CCNP认证过程有助于我们理解Cisco考试的主题以及考试的技巧。

本书编写的目的就是帮助大家为CCIE网络安全认证笔试（考试号#350-018）做准备，同时也有助于大家准备CCIE网络安全认证的重认证考试（考试号#350-009）。

Cisco在2001年推出CCIE网络安全认证，目前该项认证已经成为Cisco认证考试系列中最受欢迎的考试，因此，Cisco加大了对此项考试的投入。

CCIE网络安全认证包括笔试和为期一天的实验考试。要获得该认证，考生首先要通过的就是笔试。两项考试都很难，本书主要就是为了帮助大家通过笔试。第9章包括1个CCIE网络安全认证考试的自学实验，帮助大家进行综合的笔试准备，这让你初步了解实验考试中可能遇到的各种挑战。

Cisco特意加大CCIE网络安全认证考试的难度，没有任何一本书能够完全涵盖此考试所有的内容。考生们必须要具备广泛的实践经验并且查阅大量的资料。这样才能让大家对CCIE网络安全认证考试所涉及的内容（请见第1章）有一个全面的认识。利用本书以及光盘中的练习，大家可以评估一下自己对这些内容的准备情况。

CCIE网络安全认证笔试时间为两个小时，包含多项选择题，其中涉及数量庞大的Cisco IOS软件配置和实践练习问题。一些问题答案惟一，而另外一些则有多个答案。

CCIE网络安全认证笔试只是获取CCIE网络安全认证的第一步。

本书就为大家准备CCIE网络安全认证笔试提供了大量的技术和实践知识，让读者在通往当前最为流行的一门认证考试的途中全面地获取所需的知识内容与技能。

通过笔试意味着大家已然掌握了网络的概念性知识和网络安全的基础性知识，以此为基础我们就能够利用Cisco路由器建立起复杂安全的可路由IP网络。这是非常有用的一项技能，它向雇人单位表明我们已然能够胜任工作中可能遇到的任何挑战。

注意　CCIE网络安全认证的笔试是机考形式的多项选择题，可以在任何的VUE考点（www.VUE.com/cisco）或者是Prometric考试中心

（www.prometric.com.cn）进行。考试共2个小时，100道题。关于考试的确切时间长度信息，大家可以直接和VUE或Prometric联系，认证考试一直处于改变中，因此大家一定要从Cisco获取最新的信息：
www.cisco.com/en/US/learning/le3/le2/le23/le476/learning_certification_type_home.html。

注意 关于如何使用本书以及如何为CCIE网络安全认证考试做准备，大家可以参考第1章“利用本书准备CCIE网络安全认证笔试”以及附录B“CCIE网络安全考试的学习技巧”等内容。

本书的目的

本书最主要的目的就是确保各位CCIE网络安全认证考生能够获得所需的知识和技能。大多数的Cisco认证考试都需要考查实践技能，而向大家提供这些技能训练的惟一办法就是将这些技能融合在采用Cisco技术的工作环境当中。

本书全面涉及了CCIE网络安全认证考试的考查内容，另外也包括少量不在考查范围之内的基础性知识，其最终目的就是让大家能够自信地通过CCIE网络安全认证笔试。因此，正如后面将要介绍的那样，这本书所有的特点就是帮助大家理解考试中IP路由选择和网络安全相关的各种问题，帮助大家发现以前知识中所匮乏的部分，帮助大家掌握所有需要掌握的内容。

随书所附的光盘是一份宝贵的财富，它是实际考试的一次模拟仿真，包含了300道样题。光盘的使用有两种模式，学习模式中，大家可以集中在具体的几个内容上，其中也包括本书电子版的链接，而考试模式则为大家提供模拟考试的机会。

本书的组织

每章开始的时候都有一个“我已经知道这些了吗”的小测试，考查大家当前的知识水平，其目的是帮助大家确定是否需要学习本章全部的内容，或者只需要阅读该章的某一部分，或者是可以跳过这一章。大家可以查看第1章和每章“我已经知道这些了吗”部分的介绍，以了解更多信息。

每章接下来的内容就是基础知识内容部分，它介绍了该章所包含的CCIE网络安全认证考试所涉及的内容。每章的最后有基础知识总结，这里更为精炼地列出了本章所涉及的知识内容，是用作复习的好材料。每章结束的时候都有Q & A以及实践练习，用于评估大家对该章内容的掌握程度。

第1章，“利用本书准备CCIE网络安全认证笔试”

第1章详细列出了CCIE网络安全认证考试的考查内容以及如何使用本书，此外也讨论了CCIE网络安全认证考试的考点。

第2章，“常用网络概念”

第2章讲述的是常用的一些网络技术概念，包括OSI参考模型的概述、交换的概念和路由选择协议。本章讲述了TCP/IP模型在当前IP网络中常用的应用。为了确保大家能够深刻理解Cisco IOS如何路由IP数据报，我们在本章中还给出了路由选择协议的概念及其配置实例。本章结束的时候对当前广为采用的WAN协议(如PPP、ISDN和帧中继)进行了讨论。请大家记住，CCIE网络安全考试既包括路由和交换的内容，也包括网络安全的内容。这些都在第1章中详细地列出。

第3章，“应用协议”

第3章讲述的是域名系统和TFTP文件传输的问题，其中包括一些最常用的应用，如FTP

和HTTP，此外还包括一些更安全的从万维网上下载信息的方法，如Secure Shell和SSL。本章还给出了一个具有挑战性的实验内容，要求大家利用所学的IOS技巧对DNS、TFTP、NTP和SNMP进行配置。

第4章，“Cisco IOS的细节问题以及网络安全性”

第4章讨论Cisco IOS路由器一些更为深入和高级的特性，包括Cisco路由器的详细硬件构成以及如何管理Cisco路由器。这一章中以当前大型IP网络为例，列出了常用的Cisco设备操作命令及Cisco IOS管理范例，详细介绍了Cisco的密码恢复技术以及基本的密码安全措施，以便大家能够牢固掌握Cisco设备的操作方式。此外，本章还描述了标准访问控制列表和扩展访问控制列表及其应用实例。

第5章，“网络安全协议”

第5章侧重于讨论由Cisco开发和支持，并在RFC中定义的一些网络安全协议，如TACACS+、RADIUS和Kerberos。除了一些配置实例之外，本章还介绍了一些加密技术及其在当前脆弱的IP网络中的应用。

第6章，“操作系统与Cisco安全应用程序”

第6章讨论了目前最为普及的操作系统：Windows和UNIX，也详细介绍了运行于这些平台上的一些应用程序，此外还讨论了Cisco安全与Cisco策略管理。

第7章，“网络安全技术”

第7章讲述基本的网络安全技术以及最近出现的新型安全网络技术，包括分组过滤和代理技术。IPv4的IP地址快速消耗的事实已然使得NAT/PAT的应用越来越普遍。这一章讨论的就是这类问题及其相关的IOS配置实例。

Cisco PIX是Cisco的专利网络安全设备，本章也将向大家介绍该设备的体系结构及此特殊安全设备的配置方法。本章最后是IOS特性集以及VPN的相关内容。

第8章，“网络安全策略、漏洞及保护措施”

第8章回顾了目前互联网用于对抗电子攻击最为常用的一些Cisco网络安全策略与机制，同时也介绍了标准网络安全组织CERT/CC，以及基于Cisco IOS生成所受攻击报表并据此采取相应措施的一些网络安全技术。此外，作为CCIE网络安全认证笔试所需掌握的基础性知识，本章还讨论了一些Cisco网络安全应用，如入侵检测系统。

第9章，“CCIE网络安全认证自学实验”

第9章是大家准备CCIE网络安全认证考试的最后一步。本章的CCIE网络安全实验由前任悉尼CCIE实验考官和现任布鲁塞尔CCIE实验考官共同设计的，旨在帮助考生们通过真正的实际动手实验为最后冲刺CCIE实验考试做好准备。这一试验主要是为了考查大家通过本书所掌握的实际应用能力，考生们利用此实验能够明确自己在准备实验考试的时候应该注意的内容。

附录A，“练习题答案”

附录A是前面各章中“我已经知道这些了吗”小测试和Q & A 练习题的答案以及相应的解释。

附录B，“CCIE网络安全认证考试的学习技巧”

附录B是一些大家在开始准备CCIE网络安全认证考试的漫漫长征之前应该了解并考虑的学习技巧和准备步骤。

附录C，“CCIE路由与交换实验实例”

附录C其实是额外增加的附录，旨在给大家的CCIE路由与交换实验考试提供帮助，并且也可以让大家了解CCIE实验考试的难度。

随书光盘

随书附带的光盘包含考试模拟测试引擎，有300道以上的试题。通过练习，考生能够评估自己考试准备的成效究竟如何。

这个强大的测试引擎能够将我们的精力集中在特定的内容上，这些内容完整的计时测试题考查了书中各章所涉及的内容。只有认真做一做这些测试题并仔细参考其后的答案，大家才能算是真正地为CCIE网络安全认证考试做好了准备。

此外，光盘中还有书中的URL链接和配置实例。作为赠送，我的第一本书*CCIE Exam Cram*包含在光盘里面，帮助各位考生准备路由与交换认证考试或CCIE网络安全认证考试。请大家享受这些知识吧!

命令语法约定

本书中的命令语法参照如下约定：

- 命令、关键字和参数的实际值采用黑体表示。
- 参数（还需要赋实际值的）用斜体表示。
- 可选的关键字和参数放在中括号 [ ] 里面。
- 必选的关键字和参数放在大括号{}里面。

大家要注意的是，这些约定只是针对命令语法而言。

结束语

本人拥有多项Cisco认证证书，获取这些证书的喜悦和成功都极大地影响了我的生活和我的家庭。网络工程师总是会遭遇到各种挑战的，无可否认，成为一名Cisco认证专业人士的过程将使我们努力去获取和掌握那些曾经认为是遥不可及的知识和技能。

我衷心期望大家在学习这本书的时候能够真正享受书中的知识，它是我们6个月日夜辛劳的结晶，为的就是使之成为大家在获取CCIE认证长征路上的一位佳朋良伴。

如果大家成功地通过认证考试，欢迎大家随时和我联系（hbenjamin@optusnet.com.au），让我也能分享大家的成功与喜悦。

目　录