CCSP Securing Cisco IOS Networks Study Guide

CCSP:

思科IOS网络安全全息教程

〔美〕 Todd Lammle 著
Carl Timm, CCIE #7149
王 军 等译

考试号：642-501

全球最优秀的出版社之一
各种SYBEX学习指南书籍
印数已经超过500万册

SYBEX
美迪亚
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

CCSP Securing Cisco IOS Networks Study Guide

考试号
642-501

CCSP：思科IOS网络安全全息教程

〔美〕 Todd Lammle
Carl Timm, CCIE #7149 著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 提 要

本书主要介绍CCSP认证考试涉及的全面内容，并提供了大量的实验题和复习题。

本书首先概括地介绍了网络安全和基本的网络威胁，然后依次介绍了AAA安全、配置CiscoSecure ACS和TACACS+、Cisco边界路由器、基于上下文的访问控制配置、Cisco IOS防火墙认证和入侵检测、Cisco IOS IPSec支持、Cisco IPSec预共享密钥、Cisco Easy VPN和PIX防火墙。另外，因为本书是针对认证考试的，所以书中还提供了大量的模拟试题，通过这些试题，读者可以进一步加深与巩固所学的知识。

本书主要针对那些准备参加CCSP认证考试的人员。不过，任何对网络安全感兴趣的读者都可以从本书中获取大量有用的知识。

版权贸易合同登记号：01-2003-1087

图书在版编目（CIP）数据

CCSP：思科IOS网络安全全息教程/（美）莱默（Lammle, T.）著；王军等译.—北京：电子工业出版社，2003.11

书名原文：CCSP Securing Cisco IOS Networks Study Guide

ISBN 7-5053-9215-8

Ⅰ. C… Ⅱ. ①莱… ②王… Ⅲ. 计算机网络－安全技术－工程技术人员－资格考核－自学参考资料 Ⅳ. TP393.08

中国版本图书馆CIP数据核字（2003）第089230号

责任编辑：陈　宇

印　　刷：北京天竺颖华印刷厂

出版发行：电子工业出版社　http://www.phei.com.cn

北京市海淀区万寿路173信箱　邮编：100036

北京市海淀区翠微东里甲2号　邮编：100036

经　　销：各地新华书店

开　　本：787×1092　1/16　印张：20.5　字数：520千字

版　　次：2003年11月第1版　2003年11月第1次印刷

定　　价：35.00元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换，若书店售缺，请与本社发行部联系。联系电话：010-68279077。质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

译 者 序

Cisco认证是网络领域中最具权威性的认证体系，它包括CCNA、CCNP、CCDA、CCDP、CCIE以及最新的CCSP。本书正是专门针对CCSP认证的最新考试（642-501）而编写的，其中包含CCSP考试的所有考试主题，并提供了大量的练习和模拟试题。本书由经验丰富的Cisco互联网安全专家编写，因此还包括了他们的丰富实践经验。

本书介绍了以下方面的内容：第1章“网络安全概述”，介绍了必须知道的网络安全和基本的网络威胁。第2章“AAA安全”，介绍了Cisco NAS（网络访问服务器）和AAA安全。第3章“配置CiscoSecure ACS和TACACS+”，解释了如何安装、配置和管理Windows 2000和Windows NT服务器上的CiscoSecure ACS。第4章“Cisco边界路由器问题及解决方案”，介绍了Cisco边界路由器以及网络边界路由器可能发生的问题。第5章“基于上下文的访问控制配置”，介绍了Cisco IOS防火墙及其主要组件——基于上下文的访问控制（CBAC）。第6章“Cisco IOS防火墙认证和入侵检测”，讨论了IOS防火墙认证代理（IOS Firewall Authentication Proxy），它允许创建访问控制策略并将其应用到个人而不是地址。第7章“了解Cisco IOS IPSec支持”，介绍了虚拟专用网络（VPN）的概念，并解释了满足公司远程网络访问所需要的解决方案。第8章“Cisco IOS IPSec预共享密钥和认证中心支持”，解释了如何配置IPSec来利用预共享密钥（这是最简单的IPSec实现），以及如何配置站点到站点的IPSec来支持认证中心。第9章“使用Cisco Easy VPN进行远程访问”，讨论了一种非常优秀的VPN技术——Cisco Easy VPN。Cisco Easy VPN是IOS中的新功能，它允许有能力的IOS路由器作为VPN服务器。附录A“PIX防火墙介绍”，描述了Cisco PIX防火墙的功能和基本配置。虽然这不是SECUR考试目标的内容，但是这个附录能够帮助你了解和配置PIX防火墙。词汇表汇集了Cisco术语，它是很好的一个参考工具，可用来了解本书中一些晦涩难懂的术语。

本书主要由王军翻译。译者具有多年的计算机和网络工作经验，而且从事了多年的计算机图书编写与翻译工作。为了把国外优秀的图书介绍给国内的读者，译者做出了自己最大的努力。但是，诸事都不可能完美，书中难免包含不妥之处，恳请读者谅解并提出宝贵的意见。参与翻译工作的还有孙永强、周涛、王珺、王健、何文、陈雪松、张吉祥、吕杰、刘体争、陈旌、方勇、许萍、张雯静等。

最后，要特别感谢我的妻子——刘芳，她在全书的翻译和统稿过程中一直鼓励我、支持我，没有她，我就无法完成这项艰巨的任务。

致　谢

感谢Neil Edde和Maureen Adams从一开始就帮助我，使得本书能够非常出色，这是我最高兴的事情！谢谢，Neil和Maureen！

也要谢谢Heather！O'Connor女士帮助我编排本书的结构，她和Mae Lum在本书的编写过程中一直指导我——这是一个非常艰巨的任务！还要感谢Monica Lammle，他帮助我使得本书能够如期出版，并感谢Carl Timm和Donald Porter给予我技术上的支持——没有你们，我是无法完成这本书的！

此外，还要感谢Sybex的编辑以及其他工作人员：文字校对Sarah Lemaire；排版Judy Fung；校对Laurie O'Connell、Nancy Riddiough和Monique van den Berg；索引编写员Nancy Guenther。

致 读 者

感谢你使用Sybex出版的书籍来准备Cisco认证网络安全专家（CCSP）考试。这个考试由Cisco所开发，用来验证专业人员在设计和实现Cisco安全网络解决方案等方面的能力，CCSP证书是最高级的IT认证之一。

Sybex公司对能够为认证考试者提供在竞争激烈的IT行业中获取成功所需要的知识和技能而深感自豪。Sybex的任务就是教会每个人在现实世界中实际利用这些技术，而不仅仅是提供考试答案。Cisco的目的是建立可测量的标准来认证在互联网高新技术领域工作的专家，Sybex的目标是提供给这些专家满足这些标准所必须获得的技能和知识。

本书作者、编辑和技术人员努力工作，使得书中内容更全面、更有深度和更便于学习。我们确信，本书以及本书选配光碟中一些软件学习工具完全能够满足并超过CCSP认证的要求和标准，而且能够帮助CCSP认证考试者通过考试。

祝你在CCSP认证中好运！

Neil Edde

Sybex公司认证副总编

前　言

欢迎进入Cisco安全认证的精彩世界！你选择了这本书，是因为你想获得更多更好的技术、更多的机遇、更好的工作、更多的工作保证、更高的生活质量。然而，天上不会掉馅饼，我的朋友——你非常聪明！我怎么会知道？因为你做出了聪明的决策——选择了本书，如果你不聪明，就不会这样做。而且，你是正确的——Cisco安全认证能够帮助你得到第一份网络工作，并实现更多薪水、更高声望和工作保证的梦想。实际上，只要你没有怪异的工作习惯，选择Cisco认证，就会获得飞快的提升。而且，如果进入到安全领域并获得安全认证，那就会获得更多！

Cisco安全认证能够给予你另一个重要的优势：突破这些条条框框，并认识到获得这些证书所需要的知识完全可以提高你对安全连网技术的理解，这不仅仅是与Cisco产品相关。你将会完全掌握网络安全的知识，以及多种拓扑如何组合在一起，来形成安全的网络。这一定不会给你带来什么伤害！了解了这些知识，你就完全能够胜任每个网络工作——这也是Cisco安全认证所要求的，即使是在只有少数Cisco设备的公司！

这些新的Cisco安全认证已经超出了普通认证的范围，如CCNA/CCDA和CCNP/CCDP，它提供了在理解当前安全网络时一个必不可少的因素——深入网络互连的Cisco安全领域。

事实上，当你决定要获得Cisco安全认证时，就决定了要成为最出色的——在路由选择和网络安全方面都是最出色的。本书就可以帮你实现这个目标。

你可能会想："为什么网络容易受到安全破坏？为什么操作系统不能够提供保护？"答案非常简单明了：用户想拥有更多功能，而Microsoft会尽可能地提供给用户这些功能，因为这些功能是需要支付费用的。像共享文件和打印机这些功能，和从Internet登录到公司基础设施，这些并不是必要的——它们只是所期望的。新的公司战斗口号是："给予我们完整的Internet访问权限，并使得它更快更容易，但是必须确保它是安全的！"是的，我们正在这样做。

我是否在说Microsoft是问题所在？不是——他们只是问题的一部分，还有很多其他安全问题。如果用户通过单击鼠标就能够执行网络上的几乎所有功能，这当然会导致非常严重的安全问题。而且，如果Windows没有后门，当前也就不会有黑客。然而，所有这些实际上只是开始。要能够真正地保护自己，必须了解很多技术和网络互连设备的弱点。相信我，这些技术和网络互连设备是非常多的。

因此，这里的目标实际上包含两个方面：首先，我们将提供理解所有这些弱点所需要的信息；其次，我们将介绍如何创建一个单一的、网络范围的安全策略。但是，我们要先看看Internet上多数安全问题幕后的两个关键问题：

- 如何保护机密信息并且仍然允许公司用户获得这个信息的访问权限？
- 如何保护网络及其资源不被网络外面的未知用户访问？

如果想保护某些东西，就必须知道它在哪里，对吗？重要的/机密的信息保存在何处对

于网络安全管理员来说是至关重要的。有两个地方可保存信息：物理存储介质（例如硬盘或RAM）和以数据包的形式在网络中传输。本书的重点是有关网络上传输机密信息的网络安全问题。但是，要记住，物理介质和数据包都必须受到保护以防网络内外的入侵者。本书中的所有例子都将使用TCP/IP，因为它是当前最流行的协议并且它有一些固有的安全弱点。

但是，不能停留在这里。除了TCP/IP之外，还需要了解操作系统和网络设备的一些弱点。如果在网络设备上没有设置密码和认证，显然会有麻烦。如果没有理解路由选择协议，特别是不了解它们如何在网络中通告，那么可能就等于半夜不锁大门。此外，你对防火墙了解多少？是否有防火墙？如果有，其弱点在哪里？它是否有漏洞？如果没有考虑这些问题，则设备将是网络的致命弱点。

什么是真正的安全

至此，你有了保护网络安全的想法。要在该游戏中保持竞争力，需要有定期监视和使用的安全策略。好的想法不能够阻止黑客攻击，使自己免于遭难才是有远见的。必须考虑所有可能的问题，写下来，讨论，并提出解决方案和坚固的行动计划。

需要清晰简明地向老板表达你的计划，以便他们做出决策。有了这些知识和详尽的计划之后，就需要平衡安全需求和用户友好访问。需要在可接受的成本下完成这些工作。但是，与许多有价值的东西一样，要获得它并不容易。

第一级安全方案应该允许网络管理者向公司客户提供很好的服务——包括内部客户和外部客户，并且同时为公司节省大笔资金。如果可以这样做，其最好的结果是耗费不多的资金而运行。所有人（不包括黑客）都会满意。很好！

实际上，如果能够了解安全，并且想出了如何有效提供网络服务而且不会花费整个IT预算，则会得到一个长期的、前途光明的IT职业。你必须能够：

- 启用新的网络应用程序和服务。
- 减少实现成本和网络操作。
- 使得因特网成为全局的低成本访问媒体。

能使复杂事情简单化并更易于管理的人会受到尊敬——现实中非常需要这样的人。简化复杂性的一种方法是将大的、多层次的事情划分为易于管理的小块。为此，需要将每个网络归类为以下3种网络安全之一：受信任网络、不受信任网络和未知网络。在开始学习本书之前，应该对这些网络有所了解。

受信任网络 受信任网络（Trusted networks）是想保护的网络，它们位于安全周边（security perimeter）的区域。安全周边通过网络适配器连接到防火墙服务器。虚拟专用网络（Virtual private networks，VPN）也可以认为是受信任的网络，只有它们通过不受信任的网络来发送数据。因此，VPN比较特殊——它们使用特殊的环境并需要特殊的考虑来建立安全策略。VPN上传输的数据包是在受信任网络上建立的，因此防火墙服务器需要认证这些数据包的来源、检查数据完整性并提供其他安全需要。

不受信任网络 不受信任网络（Untrusted networks）是安全周边外的区域并且不受你或管理员控制，例如因特网和公司ISP。实际上，需要在这些网络上保护自己，同时又要允许访问它们。

未知网络　因为不能归类所不知道的东西，所以未知网络（unknown networks）可以是受信任网络也可以是不受信任网络。这种网络没有告诉防火墙它是内部（受信任）网络还是外部（不受信任）网络。你可能不喜欢这些网络来打扰你。

如何使用本书

如果想努力学习并准备通过Securing Cisco IOS Networks（SECUR 642-501）考试，则本书正是你所需要的。本书详细介绍了通过SECUR考试所需要的知识，并且教会你如何在Cisco路由器上配置安全。

本书包含了很多有价值的信息。如果能够理解本书的组织方式，则学习效率会更高。要从本书中获得最大的收益，建议：

1. 立即完成前言后面的评估考试（答案位于考试的末尾，不要作弊）。如果不知道某些答案，非常好——这就是购买本书的原因！但是，需要仔细阅读错误答案的解释，并记录内容来自哪一章。它将有助于规划你的学习策略。而且，如果不知道答案，没有关系——只需要考虑，你将学习这些知识！
2. 认真地学习每一章，确保完全理解了每章开始所列出的信息和考试目标，并且要特别注意与评估考试中答错题相关的一些章节。
3. 花一些时间完成每章后面的书面实验。不要跳过它——它与SECUR考试直接相关，这也是每章的重点。因此，不要忽略它——一定要理解每个问题及其答案。
4. 回答每章中的复习题（答案位于每章的末尾）。在回答问题的同时，记下有疑惑的问题，并复习相关内容。不要丢掉你的学习笔记——在参加考试之前应该再次复习对你来说比较困难的一些问题！确保完全理解了每个问题的答案，因为这些问题能够帮助你在参加SECUR考试之前掌握所必须知道的材料。
5. 完成每章中的动手实验，参照相关章节的材料，以便能够理解每一步。如果手头没有Cisco的设备，则一定要更加认真学习这些例子。可以到www.routersim.com查看路由器模拟器，来帮助获得实践经验。
6. 尽量去做本书选配光碟中的额外考试题。这些问题只位于本书选配光碟中，可用来测试自己，对自己的知识水平有一个大体的了解。
7. 回答本书选配光碟上的所有闪卡问题。闪卡程序能够有助于你准备SECUR考试。

   提示：电子闪卡可用在Windows计算机、Pocket PC或Palm设备上。
8. 确保阅读了每章末尾的考试要点、关键术语和本章中使用的命令，并要非常熟悉这3个部分的信息。

我不会骗你——学习本书中的所有知识不是一天就可以完成的。我要说的是，它是有点难度的。不过这也是值得的。因此，必须做一个好学生，定期学习。每天花一些时间来学习，并选择一个舒适的、安静的环境。不是利用每个晚上熄灯之前躺在床上的15分钟来学习，实际上你不想一遍又一遍地阅读相同的章节，是不是？如果选择一个难于集中精神学习的时间/地点，那么一遇到难题，你就会很快放弃！

本书覆盖了通过SECUR考试所需要知道的所有内容。但是，即使这样，还需要花一些时间来实际使用路由器或路由器模拟软件，这才是打开成功之门的真正钥匙。

如果按照上述8个步骤来认真学习，练习每个复习题、额外考试、电子闪卡、书面实验和动手实验，并利用路由器或路由器模拟程序来实践，要不通过SECUR考试都很困难！

本书包含哪些内容

下面是通过SECUR考试所必须知道的信息——也就是本书中所要介绍的内容。

第1章介绍了必须知道的网络安全和基本的网络威胁。第1章还描述了网络中可能存在的弱点。所有组织都必须有很好的策略，本章解释了如何开发坚固的公司安全策略及其应该包含的大纲指南。

第2章介绍了Cisco NAS（网络访问服务器）和AAA安全。第2章解释了如何配置Cisco NAS路由器以便进行认证、授权和记账。

第3章解释了如何安装、配置和管理Windows 2000和Windows NT服务器上的CiscoSecure ACS（第3章还简单介绍了UNIX服务器上的CiscoSecure ACS）。此外，本章还描述了NAS如何使用TACACS+或RADIUS来向ACS传递用户访问请求。

第4章介绍了Cisco边界路由器以及从黑客到网络边界路由器所可能发生的问题。本章还描述了如何实现这些问题的解决方案。

第5章介绍了Cisco IOS防火墙及其主要组件——基于上下文的访问控制（Context-Based Access Control，CBAC）。该章还解释了在保护网络方面，CBAC如何不同于且优于静态的ACL。

第6章讨论了IOS防火墙认证代理（IOS Firewall Authentication Proxy），它允许创建并可以将访问控制策略应用到个人而不是地址。此外，该章还解释了IOS防火墙入侵检测系统（Firewall Intrusion Detection System，IDS），它允许IOS路由器作为CiscoSecure IDS探测器，对潜在的恶意数据包做出反应。

第7章介绍了虚拟专用网络（virtual private networks，VPN）的概念，并解释了满足公司远程网络访问需要的解决方案。该章还描述了VPN如何使用IP安全（IPSec）来在公共网络上提供安全通信。

第8章解释了配置IPSec利用预共享密钥（这是最简单的IPSec实现），以及如何配置站点到站点的IPSec来支持认证中心。

第9章讨论了一种非常酷的VPN技术——Cisco Easy VPN。Cisco Easy VPN是IOS中的新功能，它允许有能力的IOS路由器作为VPN服务器。

附录描述了Cisco PIX防火墙的功能和基本配置。虽然这不是SECUR考试目标的内容，但是这个附录能够帮助你了解和配置PIX防火墙。

词汇表汇集了Cisco术语，它是很好的一个参考工具，可用来了解本书中一些晦涩难懂的术语。

多数章节包含书面实验、动手实验和大量复习题来帮助你掌握这些内容。不要忽略这些工具——它们对于你成功地通过考试是非常重要的。

本书选配光碟中的内容

为了帮助你通过认证考试，我们尽量地提供一些极好的工具。在针对认证考试进行学

习的时候，你应该试试下面的这些工具。

全新的Sybex考试引擎

由Sybex专家所开发的考试准备软件可以为你通过考试提供一些准备工作。在这个考试引擎中，可以发现本书中的所有复习题和评估考试题，以及只有本书选配光碟上才有的两个额外考试题。可以做这些评估考试，考试每一章，或者做额外的考试题。所得到的分数表示了你在每个SECUR考试目标上的学习效果。

说明：要找到Cisco和Microsoft的所有考试模拟软件，可以查看www.routersim.com上的CertSim链接。

适用于PC和Palm设备的电子闪卡程序

为了准备考试，需要做些什么？我们总结一下。首先可以阅读本书、学习每一章后面的复习题、练习本书和选配光碟中包含的模拟试题等。然后，可以通过选配光碟中提供的闪卡程序来进行自我测试。现在，应该非常有信心，因为你知道，如果掌握了这些困难的问题并了解其答案，则即使最困难的SECUR考试，你都可以通过。

闪卡包含了150多个特别设计的较有难度的问题，确保你能够准备充分。通过复习题、练习题和闪卡的考验，用户将更有把握通过考试！

本书的PDF格式

Sybex在选配光碟中提供了本书的PDF格式。如果在旅途中不想携带书，或者喜欢在计算机屏幕上阅读，则可以在PC或笔记本上阅读本书。本书选配光碟上还提供了带搜索功能的Acrobat Reader 5.1。

Cisco安全认证

现在出现了一些新的Cisco安全认证，但是有关SECUR考试的本书是Cisco安全认证所必要的！所有新的Cisco安全认证都需要有效的CCNA证书。

Cisco认证安全专家（CCSP）

必须通过5门考试才可以成为CCSP。最为关键的是SECUR考试。因此，如果通过了SECUR，才可参加其他4门考试。下面列出了成为CCSP所必须通过的考试项目：

- Securing Cisco IOS Networks（642-501 SECUR）
- Cisco Secure PIX Firewall Advanced（642-521 CSPFA）
- Cisco Secure Intrusion Detection System（642-531 CSIDS）（2003年秋季的新考试）
- Cisco Secure Virtual Networks（642-511 CSVPN）
- Cisco SAFE Implementation（9E0 -131 CSI）

Cisco防火墙专家　Cisco安全认证重点是为了满足对知识丰富的网络专家的需求，他应该能够实现完整的安全解决方案。Cisco防火墙专家（Cisco Firewall Specialists）重点是使用Cisco IOS软件和Cisco PIX防火墙技术来保护网络访问。

要获得Cisco防火墙专家证书必须通过两门考试：Securing Cisco IOS Networks（642-

501 SECUR）和Cisco Secure PIX Firewall Advanced（642-521 CSPFA）。

Cisco IDS专家 Cisco IDS专家（Cisco IDS Specialists）能够操作和监视Cisco IOS软件和IDS技术，来检测和响应入侵活动。

要获得Cisco IDS专家证书必须通过两门考试：Securing Cisco IOS Networks（642-501 SECUR）和Cisco Secure Intrusion Detection System（642-531 CSIDS）（新的考试从2003年秋季开始）。

Cisco VPN专家 Cisco VPN专家（Cisco VPN Specialists）可以使用Cisco IOS软件和Cisco VPN 3000系列的集线器技术来配置VPN，跨越共享的公共网络。

获得Cisco VPN专家认证必须通过两门考试：Securing Cisco IOS Networks（642-501 SECUR）和Cisco Secure Virtual Networks（642-511 CSVPN）。

说明：CCSP考试和考试编号会随时变化。请到Cisco Web站点（www.cisco.com）来查看最新信息。

说明：有关Sybex公司CCSP考试书籍等内容，可访问www.sybex.com。

Cisco网络支持认证

最初，为了获取令人羡慕的CCIE证书，用户只能参加一次考试，然后就要面对极度困难的实验，其成功率是相当低的。为了帮助用户通过CCIE认证，同时也为了评估员工的相应技术水平，Cisco创建了一系列新的认证。用户可以逐步地通过各个认证，最后获得CCIE证书。这样，以前只有很少人通过的CCIE之门被打开了。下面我们来介绍这些认证以及如何帮助你获得CCIE证书。

Cisco认证的网络工程师（CCNA）

CCNA认证位于新的Cisco认证过程的第一个，它是所有当前Cisco认证的开始。通过新的认证程序，Cisco创建了一个通向CCIE的台阶。现在，要成为Cisco认证的网络工程师，可以选择Sybex出版的“CCNA Study Guide”（该书中文版已由电子工业出版社出版，书名为《CCNA学习指南（第三版）》），并花费125美元来参加考试。

然后，可以继续学习并通过更高级别的认证，称为Cisco认证资深网络工程师（CCNP）。拥有CCNP证书的人具有参加CCIE实验室考试所需的所有技术和知识，但是，因为任何书籍都无法代替实际的考试，所以我们将简短地讨论一下准备CCIE实验室考试时还需要哪些知识。

如何成为CCNA

成为CCNA的第一步是通过一个小的测试（不要希望它非常简单）。事实上，它只是一个测试，但是仍然必须具有足够的知识以便理解（和阅读）考试题目的内容。

而且，有Cisco路由器的操作经验是非常重要的。如果有Cisco 2500或2600系列的路由器，则可以尝试设置。但是，如果没有，则Sybex出版的“CCNA Study Guide”中提供了数百个例子来帮助网络管理员（或想成为网络管理员的用户）学习通过CCNA考试所必要的知识。

获得实践路由器经验的另一种方法是，在现实世界中参加Globalnet Training Solutions公司举行的一些研究性会议，这是由我——Todd Lammle所主持的。Globalnet Training研究会议将讲授成为CCNA、CCNP、CCSP和CCIE所需要知道的所有知识！每个学生都可以通过

至少配置两个路由器和一个交换机来获得实践经验，这里不是共享设备！

说明：要联系Todd Lammle进行实践培训，可查看www.globalnettraining.com。

说明：有关Sybex公司的“CCNA：Cisco Certified Network Associate Study Guide”（即前面提到的“CCNA Study Guide”），可以查看www.sybex.com。

Cisco认证资深网络工程师（CCNP）

你会想：“太好了，在通过CCNA之后还需要做什么？”很好，如果你想成为路由和交换领域中的CCIE（最受欢迎的证书），则需要知道存在多种通往CCIE的途径。第一种途径是继续学习并成为Cisco认证资深网络工程师（CCNP），除了CCNA认证之外，这还需要面对4个其他的考试。

CCNP认证程序将帮助用户理解并解决当今网络中出现的问题——但是它不仅仅局限于Cisco世界。在获取CCNP证书的过程中，将会极大地增长用户的网络知识和技能。

虽然为了参加CCIE实验考试并不一定要成为CCNP和CCNA，但是如果已经拥有了这些证书，它们将对你有很大的帮助。

如何成为CCNP

成为CCNA之后，要获得CCNP，还必须参加4个其他的考试：

Exam 643-801：建立可扩展的Cisco互联网络（BSCI）　这个考试继续考核CCNA课程中所学习的基础知识。它的重点是大型的、多协议的互联网络，以及如何通过访问列表、排队、隧道、路由分配、路由映射、BGP、EIGRP、OSPF和路由摘要来管理它们。

Exam 643-811：建立Cisco多层交换网络（BCMSN）　这个考试测试用户的Cisco Catalyst交换机的知识。

Exam 643-821：建立Cisco远程访问网络（BCRAN）　这个考试确定你是否真正了解了如何安装、配置、监视和诊断Cisco ISDN和拨号访问产品。必须了解PPP、ISDN、帧中继和认证等知识。

Exam 643-831：Cisco互联网络调试支持（CIT）　这个考试测试你调试以太网和令牌环局域网、IP、IPX和AppleTalk网络以及ISDN、PPP和帧中继网络的技能。

说明：有关Sybex公司CCNP考试的学习指南的更多信息，参见www.sybex.com。

说明：www.routersim.com站点上具有一个用于所有CCNP考试的完整的Cisco路由器。

如果你讨厌总是考试，那么你可以在通过CCNA考试和CIT考试之后，再参加一个考试，叫做基础考试（640-841）。这样做同样可以获得CCNP证书——不过要注意，这个考试相当长，它把BSCI、BCMSN和BCRAN考试的所有内容集合到了一个考试中。祝你好运！但是，通过参加这个考试，你可以节省125美元（在通过的前提下）。

提示：记住，考试目标和考试本身会在没有通知的前提下随时发生改变，因此，用户最好随时检查Cisco的网站（www.cisco.com）以了解最新的信息。

Cisco认证互联网络专家（CCIE）

你已经成为了一个CCNP，现在你可以向Cisco认证互联网络专家（CCIE）发起冲击。下一步该做什么？Cisco建议在参加CCIE实验之前，至少需要两年的工作经验。在克服这些障碍之后，在参加实际的实验考试之前，必须通过书面的CCIE Exam Qualification。

实际上，有4种CCIE认证，在参加动手实验考试之前必须通过其中一个书面考试。

CCIE Communications and Services（Exams 350-020、350-021、350-022、350-023） CCIE通信和服务书面考试包括IP和IP路由、光学、DSL、拨号、电缆、无线、WAN交换、内容网络和语音。

CCIE Routing and Switching（Exam 350-001） CCIE路由和交换考试包括IP和IP路由、非IP桌面协议（例如IPX）以及有关桥和交换的技术。

CCIE Security（Exam 350-018） CCIE安全考试包括IP和IP路由，以及特定的安全组件。

CCIE Voice（Exam 351-030） CCIE语音考试包括构成Cisco Enterprise VoIP解决方案的所有技术和应用程序。

如何成为CCIE

要成为CCIE，Cisco建议完成下列任务：

1. 参加GlobalNet Training CCIE动手实验程序，其位于www.globalnettraining.com。
2. 通过Drake/Prometric考试（每次考试将花费300美元，因此希望你第一次就能够通过）。有关更详细的信息，可参见下面的“在哪参加考试”。
3. 在Cisco通过一天的动手实验。每个实验将需要1250美元，而且许多人都失败了两次或更多次。一些人根本就没有通过——它太难了！Cisco增减了CCIE实验的考点，因此最好查看Cisco网站来获得最新的信息。考虑一下，除了旅途费用之外，参加该考试还需要1250美元！

Cisco的网络设计认证

除了网络支持认证，Cisco还为网络设计者创建了额外的认证，包括Cisco认证设计工程师和Cisco认证资深设计工程师。如果想成为CCIE，我们建议在参加实验室考试之前先通过CCNP和CCDP认证。

通过这个认证，用户将获得设计路由LAN、路由WAN、交换LAN、交换WAN和ATM LANE网络所需的知识。

Cisco认证设计工程师（CCDA）

要想成为CCDA，用户必须通过Cisco网络互联解决方案考试（640-861 DESGN）。要想通过这个考试，用户必须理解如何完成以下的工作：

- 识别客户商务需求和他们的网络互联要求。
- 访问现有的客户网络，并指出可能的问题。
- 设计符合客户要求的网络解决方案。

- 向客户和网络工程师解释此网络解决方案。
- 计划网络设计的实现。
- 验证网络设计的实现。

提示： “CCDA：Cisco Certified Design Associate Study Guide, 2nd ed”（Sybex, 2003）是帮助用户通过CCDA考试的最好学习材料之一。

Cisco认证资深设计工程师（CCDP）

如果用户已经获得了CCNP证书并且想获得CCDP证书，则可以参加CID 640-025考试。如果用户还没有通过CCNP认证，则必须要参加CCDA、CCNA、BSCI、交换、远程访问和CID考试。

CCDP认证技能包括：

- 设计复杂的路由LAN、路由WAN、交换LAN和ATM LANE网络。
- 掌握基础的CCDA技术知识。

通过CCDP的人能够熟练完成以下工作：

- 在分层环境中进行网络层的寻址
- 使用访问列表管理网络流量
- 分层网络设计
- 使用并传播VLAN
- 性能考虑：需要的硬件和软件；交换引擎；内存、成本和最小化

在哪参加考试

用户可以在全世界范围内的800多个Thomson Prometric Authorized Testing Centers（www.2test.com）参加考试，或者拨打电话800-204-EXAM（3926）。用户还可以在VUE授权中心（www.vue.com）注册并参加考试，或者拨打电话877-404-EXAM（3926）。

要注册Cisco认证考试，具体步骤如下：

1. 确定要参加考试的编号（SECUR考试的编号为642-501）。
2. 在最近的Thomson Prometric注册中心或VUE考试中心进行注册。这时，用户将被要求支付考试费用。在写此书的时候，每门考试需要125美元并且必须在付款后的一年内参加考试。用户可以提前6个星期或者直到考试的同一天再安排考试计划——但是，如果一门考试失败，进行重考时必须要等待72小时。如果临时有事或者想改变考试计划，用户可以提前24小时联系Thomson Prometric或VUE。
3. 当计划参加考试时，用户需要考虑所有可能的事项，包括所需的手续、ID要求以及考试中心的位置等等。

对参加SECUR考试的提示

SECUR考试需要在90分钟内完成大约70道问题，每次考试都有变化。大约答对82%才能够通过该考试，同样，由于每次考试都会有点不同，所以目标应该更高。

考试中的许多问题的答案选项看上去都差不多——特别是语法问题（下面会讨论）！记

住，要非常仔细地阅读答案选项。如果命令顺序出错或者其中的一个字母出错，则整个问题都是错的。因此，需要反复地做每章后面的练习，直到熟练掌握它们。

小心语法

不同于Microsoft或Novell考试，SECUR考试有很多类似答案的选项。虽然有些语法是错误的，但它通常是经过精心设计的错误。有些选项在语法上是正确的，但它们的显示顺序是错误的。Cisco确实过于挑剔，而且他们常常会出一些陷阱问题。例如：

True or False: access-list 101 deny ip any any eq 23 denies Telnet access to all systems.

这个语句看上去是正确的，因为多数人考虑是端口号（23）并认为："是的，这是用于Telnet的端口。"实际上是：你不能过滤端口号上的IP（只有TCP和UDP）。

同时，切记：正确的答案就是Cisco的答案。在许多情况下，可能会有多个合适的答案，但是只有Cisco建议的答案是正确的。

下面给出一些有助于通过考试的提示：

- 提前到达考试中心，这样可以放松一下并可以复习一下学习材料。
- 仔细阅读问题。不要急着下结论，确保确实搞清楚了每一个问题。
- 在做没有把握的多项选择题时，首先使用排除法排除那些明显错误的答案，这样可以极大地增加猜中的机会。
- 在Cisco考试中不能随意前进或后退，所以在单击"Next"时要反复检查答案，因为进入到下一题后，将无法返回前面的问题进行修改。

在完成考试后，将会立即在线得到考试是否通过的结果——一份打印的考试分数报告，它指出用户是否通过考试以及每一部分的结果，考试管理员会将这个报告交给用户。考试成绩将会在考试后的5天内自动传送到Cisco，所以用户不需要再向Cisco传送分数。如果通过了考试，用户将会在2到4星期之内得到Cisco的确认。

如何联系作者

可以通过Globalnet Training Solutions公司（www.globalnettraining.com）联系Todd Lammle，该培训公司位于达拉斯，他的软件公司位于丹佛。

还可以到站点www.globalnettraining.com/forum，联系Todd Lammle和Carl Timm。这里，可以找到有关Cisco认证的信息，并且还可以对他们所编写的书询问一些问题。

评估考试

1. Which of the following commands trace AAA packets and monitor their activities? (Choose all that apply.)
   A. debug aaa authentication
   B. debug aaa authorization

C. debug aaa all

D. debug aaa accounting

2. What is the last header you can read in clear text when a packet has been encrypted using IPSec?

A. Physical

B. Data Link

C. Network

D. Transport

3. Which of the following is an example of a configuration weakness?

A. Old software

B. No written security policy

C. Unsecured user accounts

D. No monitoring of the security

4. Which IOS feature best prevents DoS SYN flood attacks?

A. IPSec

B. TCP Intercept

C. MD5 authentication

D. ACLs

5. RSA digital signatures and _____ are IPSec authentication types supported by the Cisco Easy VPN Server.

A. Pre-shared keys

B. LSA analog signatures

C. DSS

D. DES

E. 3DES

6. Which of the following commands do you use to change the maximum number of half-open TCP connections per minute to 100?

A. ip inspect tcp synwait-time 100

B. ip inspect tcp idle-time 100

C. ip inspect max-incomplete high 100

D. ip inspect one-minute high 100

E. ip inspect tcp max-incomplete host 100

7. IP spoofing, man-in-the-middle, and session replaying are examples of what type of security weakness?

A. Configuration weakness

B. TCP/IP weakness

C. Policy weakness