Cisco Systems

Cisco 职业认证培训系列
CISCO CAREER CERTIFICATIONS

ciscopress.com

CCIE 安全 Lab 实战

CCIE® Self-Study
CCIE Security Practice Labs

Seven comprehensive CCIE security labs to
hone configuration and troubleshooting skills

[美] Yusuf Bhaiji，CCIE #9305 著
胡捷 姚军玲，CCIE #11470 译

人民邮电出版社
POSTS & TELECOM PRESS

Cisco 职业认证培训系列

CCIE 安全 Lab 实战

[美] Yusuf Bhaiji，CCIE #9305 著

胡 捷 姚军玲，CCIE #11470 译

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

CCIE 安全 Lab 实战 /（美）海吉著；胡捷，姚军玲译．—北京：人民邮电出版社，2005.6
（Cisco 职业认证培训系列）

ISBN 7-115-13392-1

Ⅰ．C… Ⅱ．①海…②胡…③姚… 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（2005）第 032727 号

版 权 声 明

Cisco 职业认证培训系列

CCIE 安全 Lab 实战

◆ 著 [美] Yusuf Bhaiji，CCIE #9305
译 胡 捷 姚军玲，CCIE #11470
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：29.5
字数：721 千字 2005 年 6 月第 1 版
印数：1－3 000 册 2005 年 6 月北京第 1 次印刷

著作权合同登记号 图字：01-2004-0563 号

ISBN 7-115-13392-1/TP・4656

定价：85.00 元（附光盘）

本书如有印装质量问题，请与本社联系 电话：（010）67129223

前　言

正如 Vinton G.Cerf 所说的："对于 Internet，最美妙的事是可以连接到其他所有人，最可怕的事是被其他人连接。"

对大量信息的访问伴随着风险，Internet 上的每个人都是潜在的赌金保管者。该风险从信息丢失/讹误到信息偷窃，乃至更多。安全事件的数量也在显著地增加。

所有这些事情的发生，强烈促使全世界每个组织不断改进网络安全以完善目前的安全状况。现代更为复杂的网络，要求全面完整的安全问题解决方案。

对安全认证的需要

安全是网络产业发展最为快速的领域之一。信息安全是所有组织日程安排的重点。公司需要保证信息安全，因此越来越强烈地期盼 IT 专家知道如何做到信息安全。Cisco 公司通过提供 CCIE 安全证书，即建立一个专业的网络互连标准来实现这一点。

IT 业对安全的根本需求是确定无疑的。国际数据公司预测，2004 年全世界信息安全市场将从 55 亿美元增加至 172 亿美元。

SANS 研究所的项目评估说，20 名安全专家中有不到一人掌握了核心的知识和能力以正确应用安全手段。同样，去年有 5 万个 IT 安全职位空缺。

这里有一些安全统计数据（来源于 Cisco Packet Magazine，2003 年季刊第一册）：

- 一个来自实时信息保护公司 Riptech 的最近研究表明：与 2001 下半年相比，2002 年上半年网络安全危险事件上升 28%。
- 一个来自 2002 年美国联邦调查局（FBI）的报告显示：在过去的 12 个月里，85%的商业活动涉及计算机安全危险。

- 2001 年的调查表明：FBI 发现 91%的应述者报告了内部网络滥用问题。

CCIE 认证概述

CCIE 被公认为是业界最高水平 IT 认证项目，通常被称为网络博士。拥有它，在业界意味着拥有最优秀的网络互连技巧。

在 CertCities.com 的年度调查中，CCIE 认证最近被 IT 专业人士选为 **2003 年最热门证书**，这归功于在紧张的职业市场中，证书重要性的不断增长。

而且，在今年早些时候，它还被 CertCities.com 读者授予**最受尊敬证书**头衔。

CCIE 项目的设计是为了帮助个人、公司、组织、产业和国家选拔出顶级的网络互连专家队伍。

本项目通过验证其职业、产业以及继续学习的情况评价出业界精英。在取得认证的过程中，个人必然会获得广泛的产品知识，但产品培训并不是 CCIE 的目的。其着眼点是选拔出在不考虑技术或产品品牌的整个网络中能够明了和应对细微差异、复杂情况和潜在困难的专家。

CCIE 项目与产业的步调一致，其真正使命是着眼于现代技术与实际应用，以便不断地选拔出高水平的网络互连人才。

目前，CCIE 认证分 4 种：

- 路由与交换；
- 安全；
- 通信与服务；
- 语音。

本书着重于 CCIE 安全实验室考试。

关于其他各类信息，请参考以下 URL：

www.cisco.com/go/ccie。

CCIE 安全考试概述

CCIE 安全考试包括 IP 和 IP 路由选择，也包括具体安全组件。

要想成为 CCIE 有两个步骤。第一步是通过由 Cisco 授权考试中心举办的两个小时的资格笔试。第二步是成功完成 Cisco 为测试考生对实际的实验室网络设备进行配置、测试和故障排除而设置的 Lab 实验考试。资格考试是参加实验室考试的先决条件。欲了解更详细的资料，请参考以下 URL：

www.cisco.com/warp/public/625/ccie/security/。

安全资格笔试

由 Cisco 授权考试中心举办的两个小时的多项选择笔试在计算机上完成。本考试闭卷，共 100 个问题，不允许使用任何参考资料。

注意 更多信息请参考 www.cisco.com/warp/public/625/ccie/security/preparing_wr_exam.html 上的 Cisco 安全笔试蓝皮书。

安全实验室考试

安全实验室考试为一天，共计 8 个小时的实验考试。CCIE 考生要在物理层之上完成一个复杂的设计。不要求考生配置终端用户系统，但要负责网络内的各种设备。

每个配置方案和问题都配有相应的分值，考生必须获得至少 80 分（100 分满分）才可以通过。

在 CCIE 实验室考试的准备过程中有 3 个核心要素：

- 你目前的工作经验水平；
- 你的受训水平；
- 你可用的时间和自学的设备选择。

注意　更多关于 CCIE 实验室考试的信息请参考 www.cisco.com/warp/public/625/ccie/security/preparing_lab_exam.html。

设备列表

要完成本书的 Lab 实战，你需要以下设备：

- 8 台路由器——路由器可以是任何型号——2500、2600 或 3600 系列均可，但模块化的路由器最好，这样你可以交换模块，适应不同的实验室拓扑。
- 你需要以下接口/电缆，以适应不同的实验室拓扑。更多细节请参考每章的设备列表。
  - ☐ 以太网/快速以太网模块/端口
  - ☐ 串行模块/端口
  - ☐ ISDN BR/S/T 模块/端口
  - ☐ ATM 模块/端口
  - ☐ 直通电缆
  - ☐ 交叉电缆
  - ☐ DTE-DCE 背对背式电缆的串行端口
  - ☐ ATM 光纤电缆（依赖于模块/GBIC）

注意　本书中的大多数实验要求你配置 ATM。如果你没有 ATM 模块，请用背对背式串行连接代替。

- 两台 Catalyst3550 交换机；
- 1 台 PIX 防火墙（任意型号）；
- 1 台 Cisco 入侵检测系统（IDS）42XX 装置；
- 1 台 VPN-3000 集中器；
- 两台 PC：
  - ☐ 安装 Cisco Secure ACS3.X 和 Microsoft CA 服务器的 Windows 2000 服务器
  - ☐ 使用 Cisco VPN Client 3.0 软件的测试 PC

读者对象

本书是为正在准备参加 CCIE 安全实验室考试的考生而设计的。

有安全专业技能的网络工程师，可以利用本书提供的复杂方案、故障排除技巧和解决方案。

本书的主要目标之一是为准备参加 CCIE 实验室考试的考生提供复杂的实践方案，以便使考生对真正的 CCIE 实验室考试有一个直观的感性认识。

CCIE 考生可以利用本书检测自己对 CCIE 实验室考试的准备程度。

关于本书

在本书的 7 章中共有 7 个 Lab 实战。每章的格式相同，但每章的练习内容不同。本书每章的难易程度和复杂程度相同，涵盖了所有技术。

各章以概述、设备列表、通用规则和建立实验室拓扑指导（包括布线规则）开始，接下来是 10 个练习部分：

节 1.0：基本配置

节 2.0：路由选择配置

节 3.0：ISDN 配置

节 4.0：PIX 配置

节 5.0：VPN（IPSec/GRE/L2TP/PPTP）配置

节 6.0：IOS 防火墙配置

节 7.0：AAA 配置

节 8.0：高级安全

节 9.0：IP 服务和协议无关特性

节 10.0：安全违例

每一节都有子节，子节由于技术问题不同分成若干类型，并各有其分值分配。

各个配置小节也有其各自的分值分配。考生须至少获得 80 分（100 分满分）才可以通过。

接下来的验证、提示和故障排除练习部分是本书的一个重要部分。这部分为你提供了故障排除技巧提示，以辨别问题中隐含的问题或诀窍。你可以利用这部分来验证和比较所采用的故障排除方法。这部分也可以指导你在检测和故障排除过程中使用常用的 show 和 debug 命令。

为了更好地帮助你，与本书配套的整个实验的 CD-ROM 还为你提供了所有设备的配置和 show 与 debug 命令输出。

CCIE 实验室考试的主要挑战之一是利用综合技术完成一个大而复杂的方案。大多数时候，考生在诸如配置个别的单项技术上知识丰富、技术熟练，但是将所有的高水平复杂技术综合成一个方案，却存在着困难。在本书各章中提供了涵盖所有技术的复杂的综合方案，使考生可以自测备考程度，了解自己的优缺点。

本书将帮助每一位参加 CCIE 安全实验室考试的考生取得成功。

注意

一旦你已成功地完成了所有的 Lab 实战，我确信你将坐下来准备参加 CCIE 实验室考试了。记住成功将取决于诸多主要因素，这很重要：

- **时间管理**——通读整个试卷，并且在你未制定计划之前切勿开始配置——记住“分割和战胜”技术。完美的计划是成功的关键。

- **明晰问题**——CCIE 实验室考试的最大挑战之一是问题的释义。你必须学会释义问题，并准确地明白要求是什么。如果问题的含义不清楚，可以让考官澄清。弄清任何不确定的东西，不要做任何假设。
- **清单**——在考试期间，保存两份清单：
  - □ 你认为已正确配置，但需要进一步测试的条目；
  - □ 你暂时不能回答、为避免浪费时间必须略过、但稍后你要再重新思考的条目。
- **分数核查**——这是聪明的态度。不要在无分值的任务上浪费时间，先回答你最有把握的部分。把有挑战性的问题留待考试结束前回答。试着让自己得到最高分值，可以使你始终清楚自己完成的进度。
- **功能测试**——结束前进行功能测试——只有配置正常工作才能获得分值。
- **有效的故障排除**——别把时间浪费在不确定的故障排除上，试着继续，把问题留在以后的阶段，多半，这种着眼点的改变会帮助你找到解决之道。
- **存储图和数据流**——在大脑中存储整个实验室拓扑和数据流。这将有助于你的故障排除和避免你注意力集中在错误的问题和设备上。
- **消除紧张的技巧**——不要让自己的神精紧张。如果你觉得紧张或混乱，就走出实验室到休息室去休整一下。Cisco 提供使人可以得到恢复的休息室——自己休息一下。这将有助于你放松，以便能够以清晰的思维重新开始。

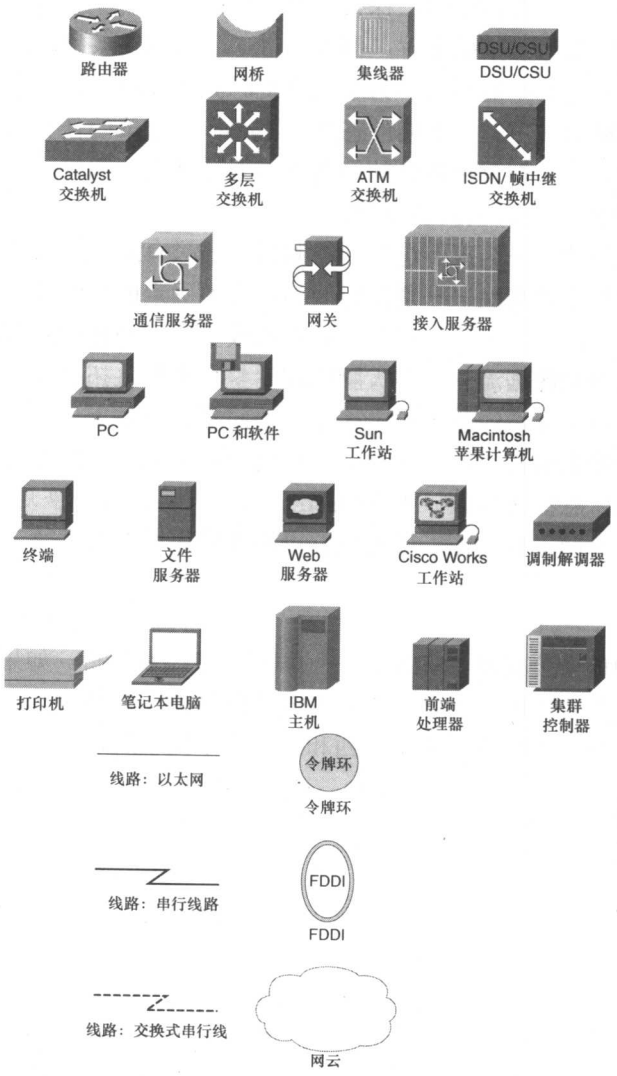
结束语

我成功的秘密公式是“MDC”——积极、专注和坚持。如果你坚持这 3 件事，你肯定会成功。CCIE 考试只是一个测试。如果你没有通过，不要放弃，再试一次！从积极的意义上讲，最初的失败将给你学习更多东西和探索你早先未发现事情的机会。

祝你好运！

Fahim Hussain Yusuf Bhaiji，CCIE #9305
CCIE 考官
悉尼，澳大利亚 Cisco Systems 公司

本书采用的图标



命令语法约定

本书采用与 IOS 命令参考一样的命令约定格式，即：

- **粗体**表明按照显示的文字输入命令及关键字。在配置的范例中及输出（不是一般的命令语法）中，**粗体**表明需要用户手工输入的命令（例如 **Show** 命令）；
- *斜体*表示由用户给出的参数实际值；
- 竖线（|）分隔二选一选项，相互不包含的选项；
- 方括号（[]）表明可选项；
- 大括号（{}）表明必选项；
- 方括号包含大括号（[{}]）表明在可选项中必选其中一个。

目　录

第 1 章

Lab 实战 1

本书中的所有实验都是基于多重协议和多重技术的，用来测试你在诸如路由选择、交换、安全和 VPN 等领域的知识，与在 CCIE 安全蓝图中标注的一样。当你第一次在实验室中阅读考题时，你可能会觉得它们相当容易，但是这些考题经过严谨地编写，具有许多隐含的问题，以提高复杂性。就像真实的 CCIE 实验室考试一样。

为了帮你通过考试，这里提供了完整的实验室考试方案，包括配置以及拓扑图中所有设备的常用 **show** 命令的输出。此外，本书还提供了“验证、提示和故障排除技巧”一节，教授你故障排除方面的技巧和提示，并且帮你指出考题中隐藏问题和狡诈的问题。

这是本书 7 个实验中的第一个。实验满分是 100 分。你必须在 8 个小时内完成，必须获得至少 80 分才能通过。跟所有的实验一样，你必须在 8 个小时内能够回答所有的问题包括初始配置（例如 IP 寻址），这不包括布线的时间。只允许 1 小时的布线时间，按照提供的指示，并观察通常的指导原则。只要你满足图 1-1 中的拓扑需要，你可以使用任何形式的路由器组合。没必要使用同一型号的路由器。

注意 实际CCIE的实验室并不需要你去布线和设定IP地址。

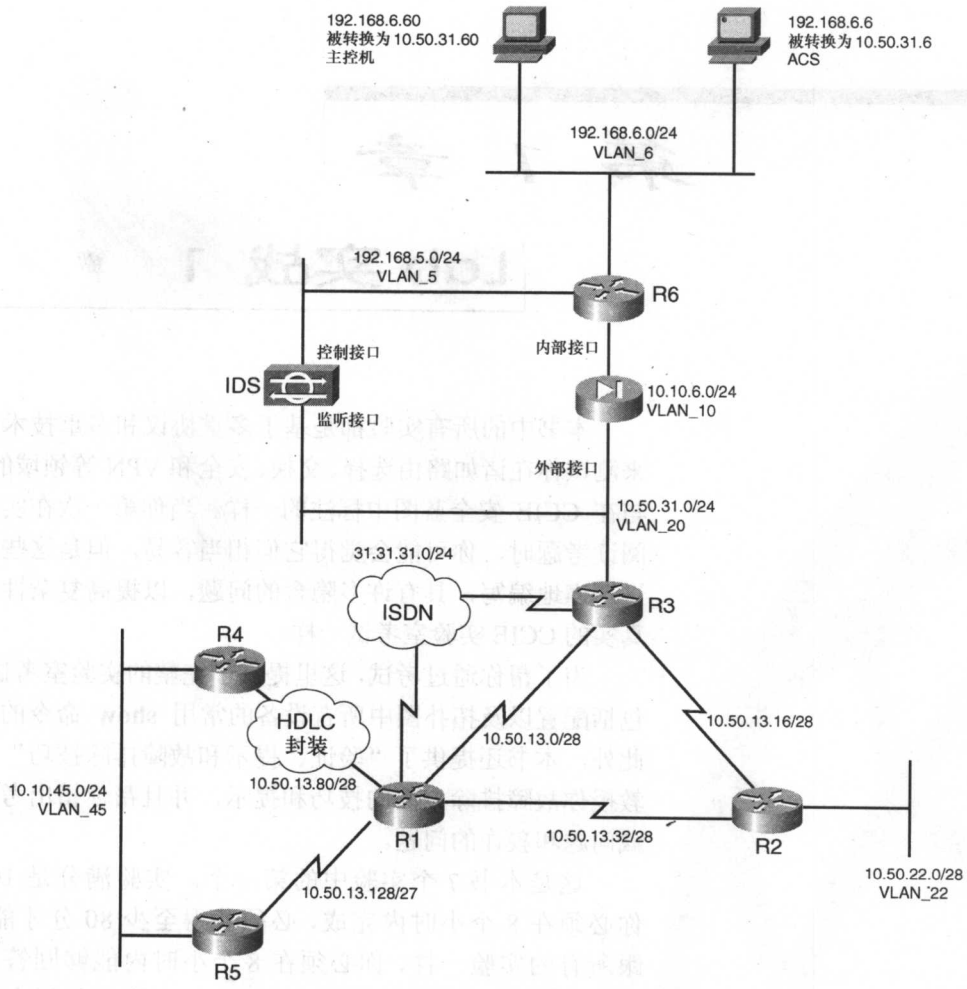


图 1-1 实验拓扑

1.1 设备列表

- 下列标准的 6 台路由器（所有路由器加载的都是最新的 Cisco IOS 版本 12.1[T]）：
  R1——4 个串口，1 个 BRI（具有 IP Plus 镜像）
  R2——2 个串口，1 个以太网接口（具有 IP Plus+Firewall 镜像）
  R3——2 个串口，1 个以太网接口，1 个 BRI（具有 IP Plus + IPSec 56 镜像）
  R4——1 个串口，1 个以太网接口（具有 IP Plus + Firewall+IPSec 56 镜像）
  R5——1 个串口，1 个以太网接口（具有 IP Plus 镜像）
  R6——5 个串口，3 个以太网接口（具有 IP Plus + IPSec 56 镜像）

- 1 台 3550 交换机；
- 1 台 PIX——2 个接口（带 6.x 版软件）；
- 1 台安装了 CiscoSecure ACS 3.x+的 Windows 2000 Server PC；
- 拓扑中的 IDS 设备并不是必需的，放在那里只是帮助你更清晰地配置实验室中其他方面的设备。后续章节确实需要一台网络 IDS 设备。

1.2 通用规则

- 正式开始前阅读全部的实验室规则。
- 除非特别说明或需要，否则不要配置任何静态/默认路由。
- 使用图中提供的 DLCI。
- 使用图中提供的 IP 寻址方案，除非特别说明，否则不要修改任何 IP 地址。在 CCIE 实验中，已装载初始配置，因此不要改变 IP 地址。在本书中，每一章都有一个不同 IP 寻址方案的单独实验拓扑，因此每一章都需要重新规划线缆，所有的 IP 地址需要重新配置，确保和前一章不同。
- 使用 **cisco** 作为认证字符串的密码，这包括使用 enable 密码和 TACACS+/RADIUS 密钥或其他目的。
- 在本实验中，根据需要添加额外的环回。
- 按照图 1-1 所示，在交换机 1 上配置 VLAN。
- 所有的路由器必须使用最优路径 ping 通网络中的任何接口。
- 你必须合理规划时间以在 8 个小时内完成此实验。
- 当进行本实验时，不要使用任何外部资源或本书提供的答案。
- 配置一个回退机制以确保本地数据库 AAA 出现问题时，可以妥善处理。如果你没有这样做，本题将不得分。
- 不要在控制台端口和辅助端口上配置任何认证或授权。

1.3 建立 Lab

只要能够满足图 1-1 的拓扑需要，你可以使用任何路由器的组合。没有必要使用同一型号的路由器来完成本实验。

1.3.1 帧中继 DLCI 信息

只有图 1-2 中的 DLCI 可以映射到路由器。