普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

教育部高等学校信息安全类专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇

局域网安全管理实践教程

王继龙 安淑梅 邵丹 编著

http://www.tup.com.cn

清华大学出版社

普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

教育部高等学校信息安全类专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇

局域网安全管理实践教程

王继龙 安淑梅 邵丹 编著

LAN Security Management Practice Guide

http://www.tup.com.cn

清华大学出版社
北京

内 容 简 介

本书详细介绍在组建局域网中涉及的多项安全技术，包括路由网安全技术、交换网安全技术和无线局域网安全技术等实验内容。

全书共分为4个模块，按照组网中使用到的安全产品，详细讲述了使用这些网络安全设备，解决遇到的基础网络设施安全、访问控制安全、端口安全、接入安全和无线局域网安全等各种安全问题。全书对所使用到的相关安全产品的基本配置、基本界面、功能配置都做了详细的讲解，以帮助读者熟悉产品的使用，并进一步了解其在工程项目中的实施方法。

本书可作为高等院校计算机、通信工程等相关专业本科生或研究生的实验教材，也可作为网络安全专业认证的培训教材，还可作为网络设计师、网络工程师、系统集成工程师和其他专业技术人员解决网络安全问题的技术参考用书。

图书在版编目（CIP）数据

局域网安全管理实践教程/王继龙，安淑梅，邵丹编著．—北京：清华大学出版社，2009.7
（高等院校信息安全专业系列教材）
ISBN 978-7-302-20193-9

Ⅰ．局…　Ⅱ．①王…　②安…　③邵…　Ⅲ．局部网络－安全技术－高等学校－教材
Ⅳ．TP393.108

中国版本图书馆CIP数据核字(2009)第077857号

责任编辑：谢　琛　赵晓宁
责任校对：焦丽丽
责任印制：李红英

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　　**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：北京密云胶印厂
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：19.75　　**字　数**：454千字
版　　次：2009年7月第1版　　**印　次**：2009年7月第1次印刷
印　　数：1～4000
定　　价：29.50元

创新网络教材编辑委员会

（院校成员名单排名不分先后）

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，共同指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点如下：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教

材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者对本系列教材提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”已于2006年初正式列入普通高等教育“十一五”国家级教材规划（见教高[2006]9号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展将起到重要的指导和推动作用。“高等院校信息安全专业系列教材”将在教育部高等学校信息安全类专业教学指导委员会的组织和指导下，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国信息安全学科的发展不断修订和完善。

我们的E-mail地址是：zhangm@tup.tsinghua.edu.cn；联系人：张民。

清华大学出版社

前言

随着21世纪的到来，人类已步入信息社会，信息产业正成为全球经济发展的主导产业。计算机科学与技术在信息产业中占据了重要的地位，随着互联网技术的普及和推广，网络技术更是信息社会发展的推动力，人们日常学习、生活和工作都越来越依赖于网络，因此关于信息技术、信息安全技术、网络安全技术正发展成为越来越重要的学科。

互联网技术的发展改变了我们的生活，今天信息安全内涵已发生了根本变化。安全已从一般性的安全防卫，变成了一种非常普通的安全防范；从一种研究型的安全学科，变成了无处不在，影响人们学习、生活和工作息息相关的安全技术。技术的普及也推动了社会对人才的需求，因此建立起一套完整的网络安全课程教学体系，提供体系化的安全专业人才培养计划，培养一批精通安全技术的专业人才队伍，对目前高校计算机网络安全方向专业人才培养，显得尤为重要。

1. 关于教材开发的背景

结合国家“十二五”本科计算机专业课程规划体系，以及深入领会教育部计算机科学与技术教学指导委员会编制的《计算机科学与技术专业规范的知识体系和课程大纲》文件精神，为及时反映目前网络安全专业学科发展动态，创新教材编辑委员会组织编写了本书。希望编撰的网络安全知识内容，既重视理论、方法和标准的介绍，又兼顾技术、系统和应用分析，在内容结构和知识点布局上还有所创新。

此外，随着互联网技术的普及和推广，日常学习和工作依赖于网络的比重增加，计算机网络安全的实施和防范技术，成为目前最为瞩目的学习内容。根据上述思路，创新网络教材编辑委员会选择网络安全技术在生活中具体应用作为教材开发主线，规划出面向实际工程案例，可操作、可应用、可实施的网络安全技术教程。希望规划的安全技术直观、形象、具体、可实施，选编和规划的安全知识具有专业化、体系化、全面化特征，能体现和代表当前最新的网络安全技术发展方向。

2. 关于教材开发的指导思想

通过调查目前市场发现，指导计算机网络安全实践教学内容的教材非常缺乏。翻阅市场上现存、数量有限的安全类教材，这些教材品种都偏重于网络安全理论诠释，而针对实际网络安全工程实施、可在课堂中动手实施的安

全类教材甚少。正是基于此，创新网络教材编辑委员会组织国内院校一线教师，联合来自厂商专业工程师开发了这本覆盖基础网络安全技术的专业教程，希望着重培养学生对网络基础安全技术的兴趣。

和同类以网络安全技术为研究方向的专业书籍相比，本书更注重实际安全问题的解决。全书以安全技术应用为主线，以培养学生安全问题解决能力为目标，以加强实际安全应用和技能锻炼为根本，满足学校安全类课程实验教学需要。因此，全书在开发过程中，强化实践教学能力的培养，着重讲授生活中的网络安全问题，诠释安全策略配置，最后依据学校提供的安全实践教学平台，直观、形象地解释安全技术，帮助学生理解抽象的网络安全专业理论。

3. 关于教材开发的内容

本书是针对高等院校计算机、通信工程等相关专业，在学习基础网络安全理论时，配套开发的网络安全实验教程。全书详细地介绍了组建局域网安全过程中使用到的多项安全产品及其相关技术，涉及了路由、交换、无线局域网等多个网络安全实验，以弥补课堂理论学习中实践教学的不足。

本书按照局域网组建过程中应用到的安全产品的类型，详细介绍组网过程中使用到的安全产品，遇到的安全问题，选择的安全技术，包括路由安全、设备安全、访问控制安全、端口安全、接入安全、无线局域网安全等实验操作及实施过程。全书对这些安全产品的基本配置、基本界面、功能配置都给予详细讲解，来帮助读者深入了解网络安全项目的设计与实施。通过对全部内容的学习，帮助读者更牢固地掌握安全技术、实施方法。

全书包括了近四十多个难度不同的网络安全实验内容，适合学生循序渐进地学习。可作为高等院校计算机、通信工程等相关专业本科生和研究生计算机网络工程课程的实验教材。全书的实验设计和安排，以实际工程项目的需求为依据，旨在加深学生对网络安全工程所涉及的基础理论知识的理解，提高学生网络安全工程相关的动手实践能力、分析问题和解决问题的能力。

4. 关于教材使用的方法

通过全书提供的近三十多个安全实验的训练，能够帮助学生熟练掌握网络安全工程师所需要的基本实践技能。所有实验操作都以日常安全需求为主线串接知识，以问题解决过程作为核心，因此教师在使用本书时，可以作为相关安全理论学习完成之后的实验补充，帮助学生加强对抽象安全理论的直观理解。也可以根据教学的实际情况，从中选择部分实验教学内容，要求学生在学完理论之后，完成适当数量和难度的实验以补充理论诠释知识的不足。由于书中全部内容都来自实际工程案例的总结，本书还可作为就业前实习用书，通过对一定数量的安全工程案例学习，积累实际的安全施工经验，以增强安全类工程施工的能力和故障排除的能力。

5. 关于课程的环境安排

本书覆盖计算机网络安全规划、组建和配置中涉及到的主流安全设备配置、管理技术，书中所有项目都来自于多年积累的企业工程案例。经过提炼，按照再现企业工程项目的组织方式进行串接，每个工程项目都详细介绍了工程名称、工程背景、技术原理、工程设

备、工程拓扑、工程规划、工作过程和结果验证等多个环节，循序渐进地展现企业工程项目施工过程，并把这些工程在网络实验室中搭建出来，积累工作中的施工经验。

为顺利实施本教程，除需要对网络技术有学习的热情之外，还需要具备基本的计算机、网络、安全基础知识。这些基础知识为学习者提供一个良好的基础，帮助理解本书中的技术原理，为网络技术的进阶提供良好帮助。为很好地实施这些安全实验，还需要为本课程提供一个可实施交换、路由、无线和安全实验的网络环境，再现企业网络工程项目。这种课程工作环境包括：一个可以容纳 40 人左右的网络实验室，不少于 4 组实验台。每组实验台中包括的组网实验设备有二层交换机、三层交换机、模块化路由器、无线局域网接入设备、无线网卡、网络防火墙、测试计算机和若干根网络连接线（或制作工具）。

虽然本书选择的工程项目来自厂商案例，使用的网络实验设备也是来自厂商，但本课程在规划中，力求全部的知识诠释和技术选择都具有通用性，遵循行业内通用技术标准和行业规范。全书中关于设备的功能描述、接口标准、技术诠释、协议细节分析、命令语法解释、命令格式、操作规程、图标和拓扑图形的绘制方法等，都使用行业内的标准，以加强其通用性。

6. 关于课程的时间安排

本书希望通过加强学生对网络设备的实践操作，积累网络工程一线施工经验，让学生深入理解网络安全设备的配置和运行机制，熟悉网络安全项目发生的场景，掌握施工过程。此外，借助网络安全实验平台，还可以学习网络安全设计、网络攻防和故障性能分析等相关知识，加强学生对网络安全技术的理解和掌握，培养学生的动手实践和设计分析能力，培养创新型人才。

本书可作为高等院校计算机科学与技术、通信工程、计算机网络等相关专业本科生或研究生学习、研究网络安全技术的实验教材。其前导性的课程包括计算机网络、局域网组建、路由和交换技术等基础性网络技术。本课程的安排时间在 36～72 学时不等，根据学校具体教学计划安排来确定，可选择全部的内容作为实验对象，也可选择部分内容。课程时间一般安排在三年级学期段，学生在学完基础网络技术后，作为基础网络技术的提高和补充。此外，本书还可以作为社会上培训机构网络安全专业认证的培训教材，以及网络工程师、系统集成工程师和其他专业技术人员用于解决在实际工作中遇到的网络安全问题的技术参考用书。

7. 关于课程资源

不同的专业课程教学都具有其本身的针对性。强化安全技术专业实践能力、强化安全技术应用和安全技能素养的培养，是本课程区别于传统网络安全专业课程特色之一。即使在目前众多以技能为教学的实验课程中，本课程也具有其他课程不能比拟的个性。无论是前期为保证课程的有效实施，方便学校的管理，在课程实施环境（网络实验室）上投入资金，还是在课程规划思想上的创新、实验手段的多样性上，本课程研发上投入的人力都具有绝对优势。

特别为有效保证课程实验的有效实施，保证课程教学资源的长期提供：安全案例的积累、最新安全技术的更新、新技术的学习、课程学习中的技术交流和讨论等。为此，本课程

的研发队伍还专门投入人力和物力，为本课程建设有专门的实践教学俱乐部资源共享基地，以有效支持课程在实施的过程中资源的更新，疑难问题的解决，课程实施讨论等一系列支持和服务工作。详细内容可以访问和本课程实施配套的网站 http://www.labclub.com.cn，可以获得更多的资源支持。

8. 关于课程开发队伍

本书由创新网络教材编辑委员会组织来自院系教学一线的专家、教师，联合来自厂商专业工程师队伍协作编写完成。这些工作在各行业内的专家，把自己多年来在各自领域中积累网络安全技术及工作经验，以及对网络安全技术的深刻理解，诠释成本书的经验积累。

本书第一作者王继龙博士，毕业于清华大学计算机系，长期在清华大学信息网络工程研究中心从事大规模互联网的规划、建设、运行和研究工作，历任研发部主任、清华大学校园网运行中心主任、第二代中国教育和科研计算机网(CERNET2)运行中心主任，第二代跨欧亚信息网(TEIN2)运行中心主任等职位。其在网络安全领域的技术积累，以及多年在组建局域网络安全体系，维护局域网安全的宝贵经验，为全书规划了安全实验大纲，提供了技术方向引导，形成全书安全知识体系，并承担了部分安全实验编写任务。

本书第二作者安淑梅女士毕业于东北大学，CCIE(＃11720)，高级工程师，熟悉思科网络、华为网络和锐捷网络产品和方案，拥有多家厂商的工作经历，熟悉面对不同的厂商安全设备，针对应用和实施网络安全防范能力。她多年在网络一线从事售前工程师、培训讲师的工作背景，参与过多个网络工程整网安全的规划、实施经历，对全书安全问题需求，再现企业安全工程实验的体例和样式，起到结构形成作用，并承担了部分实验编写任务。

邵丹女士毕业于吉林大学，现为长春大学计算机科学技术学院副教授，学院主管教学主任，主攻网络集成和局域网安全，有多年丰富的教学经验，对全书按照教材风格形成、方便学生学习、方便课堂教学、在实验室中有效实施，以及从一线教师实施角度，提供了全书文字内容形式和语言风格编辑工作，承担了部分实验编写任务。

王继龙负责全书项目立项工作，承担了全书关于局域网安全体系规划以及访问控制安全和网络接入安全章节的编写工作。安淑梅女士负责了全书案例整理和无线局域网安全章节编写任务。邵丹女士承担了端口安全和生成树安全章节编写任务。此外，在本书的编写过程中，还得到了其他一线教师、技术工程师、产品经理汪双顶、李文宇、方洋、张选波、高峡、杨靖、张勇、蔡韡等大力支持。他们积累多年的来自教学和工程一线的工作经验，都为本书的真实性、专业性以及方便在学校教学、方便实施给予了有力的支持。

本书规划、编辑的过程历经近三年多的时间，前后经过多轮的修订，牵涉到很多的人力支持，其改革力度较大，远远超过前期策划的估计，加之课程组文字水平有限，错漏之处在所难免，敬请广大读者指正 labserv@ruijie.com.cn。

创新网络教材编委会
2009 年 4 月

使用说明

为帮助学生全面理解安全技术细节，建立直观的网络安全印象，本书每一个实验开始时，都为读者引入一个来自企业真实网络的安全问题，建立教学、学习环境，让读者深入到网络安全的场景环境中，了解本节安全知识内容，了解对应施工中需要的技术。

在全书关键技术解释和工程方案实施中，会涉及到一些网络专业术语和词汇，为方便大家今后在工作中的应用，全书采用业界标准的技术和图形绘制方案。全书中使用的关于相关的符号以及网络拓扑图形惯有的风格和惯例，本书中使用的命令语法规范约定如下。

- 竖线“|”表示分隔符，用于分开可选择的选项。
- 星号“*”表示可以同时选择多个选项。
- 方括号“[ ]”表示可选项。
- 大括号“{ }”表示必选项。
- 粗体字表示按照显示的文字输入的命令和关键字。在配置的示例和输出中，粗体字表示需要用户手工输入的命令（如 **show** 命令）。
- 斜体字表示需要用户输入的具体值。

以下为本书中所使用的图标示例：


接入交换机


固化汇聚交换机


模块化汇聚交换机


核心交换机


二层堆栈交换机


三层堆栈交换机


中低端路由器


高端路由器


Voice 多业务路由器


SOHO 多业务路由器


IPv6 多业务路由器


服务器

感谢国内网络产品和方案提供者锐捷网络有限公司，为全书提供多个来自不同行业的工程案例。为方便对工程项目的技术细节诠释，本书技术描述主要依托锐捷网络操作系统展开。但在书籍中出现所有命令和术语，同样具有通用性，能兼容目前网络工程施工中应用到的所有主流设备。并且本书中讲述的技术原理，以及针对网络问题提出的解决方案，同样可以适用于所有现实网络工作场景。

目 录

第1章 访问控制安全

1.1 使用标准 IP ACL 进行访问控制

【实验名称】

使用标准 IP ACL 进行访问控制。

【实验目的】

使用标准 IP ACL 实现简单的访问控制。

【背景描述】

某公司网络中，行政部、销售部门和财务部门分别属于不同的三个子网，三个子网之间使用路由器进行互联。行政部所在的子网为 172.16.1.0/24，销售部所在的子网为 172.16.2.0/24，财务部所在的子网为 172.16.4.0/24。考虑到信息安全的问题，要求销售部不能对财务部进行访问，但行政部可以对财务部进行访问。

【需求分析】

标准 IP ACL 可以根据配置的规则对网络中的数据进行过滤。

【实验拓扑】

图 1-1 是某公司部门之间网络拓扑规划图，希望实现各子网之间安全访问控制。

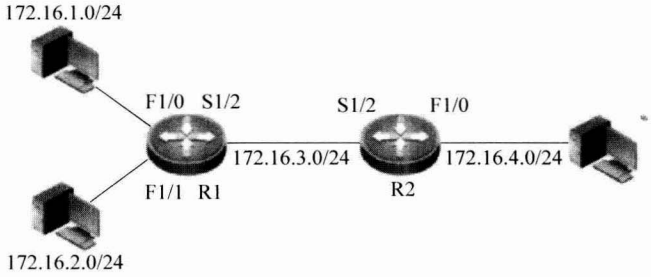

图 1-1 某公司部门之间网络拓扑规划图

【实验设备】

路由器 2 台；PC 3 台。

【预备知识】

- 路由器基本配置。

• 标准 IP ACL 原理及配置。

标准 IP ACL 简单的说法便是数据包过滤。网络管理人员通过对网络互联设备的配置管理，来实施对网络中通过的数据包的过滤，从而实现对网络中的资源进行访问输入和输出的访问控制。配置在网络互联设备中的访问控制列表 ACL 实际上是一张规则检查表，这些表中包含了很多简单的指令规则，告诉交换机或路由器设备，哪些数据包是可以接收的，哪些数据包是需要拒绝的。

交换机或路由器设备按照 ACL 中的指令顺序执行这些规则，处理每一个进入端口的数据包，实现对进入或流出网络互联设备中的数据流过滤。通过在网络互联设备中灵活地增加访问控制列表，可以作为一种网络控制的有力工具，过滤流入和流出数据包，确保网络的安全，因此 ACL 也称为软件防火墙。

根据访问控制标准的不同，ACL 分为多种类型，实现不同的网络安全访问控制权限。常见的 ACL 有两类：标准访问控制列表（Standard IP ACL）和扩展访问控制列表（Extended IP ACL），在规则中使用不同的编号区别，其中标准访问控制列表的编号取值范围为 1～99；扩展访问控制列表的编号取值范围为 100～199。

两种 ACL 的区别是：标准 ACL 只匹配、检查数据包中携带的源地址信息；扩展 ACL 不仅仅匹配检查数据包中的源地址信息，还检查数据包的目的地址，以及检查数据包的特定协议类型、端口号等。

标准访问控制列表检查数据包的源地址信息，数据包在通过网络设备时，设备解析 IP 数据包中的源地址信息，对匹配成功的数据包采取拒绝或允许操作。在编制标准的访问控制列表规则时，使用编号 1～99 值来区别同一设备上配置的不同标准访问控制列表条数。

如果需要在网络设备上配置标准访问控制列表规则，使用以下的语法格式：

```
Access-list listnumber {permit | deny} source-address [ wildcard-mask ]
```

其中，

listnumber 是区别不同 ACL 规则序号，标准访问控制列表的规则序号值的范围是 1～99。

permit 和 deny 表示允许或禁止满足该规则的数据包通过。

source-address 代表受限网络或主机的源 IP 地址。

wildcard-mask 是源 IP 地址的通配符比较位，也称反掩码，用来限定匹配网络范围。

【实验原理】

标准 IP ACL 可以对数据包的源 IP 地址进行检查。当应用了 ACL 的接口接收或发送数据包时，将根据接口配置的 ACL 规则对数据进行检查，并采取相应的措施，允许通过或拒绝通过，从而达到访问控制的目的，提高网络安全性。

【实验步骤】

（1）R1 基本配置。

```
R1#configure terminal
```

```
R1(config)#interface fastEthernet 1/0
R1(config-if)#ip address 172.16.1.1 255.255.255.0
R1(config-if)#exit

R1(config)#interface fastEthernet 1/1
R1(config-if)#ip address 172.16.2.1 255.255.255.0
R1(config-if)#exit

R1(config)#interface serial 1/2
R1(config-if)#ip address 172.16.3.1 255.255.255.0
R1(config-if)#exit
```

(2) R2 基本配置。

```
R2#configure terminal
R2(config)#interface serial 1/2
R2(config-if)#ip address 172.16.3.2 255.255.255.0
R2(config-if)#exit

R2(config)#interface fastEthernet 1/0
R2(config-if)#ip address 172.16.4.1 255.255.255.0
R2(config-if)#exit
```

(3) 查看 R1、R2 接口状态。

```
R1#show ip interface brief
Interface              IP-Address(Pri)      OK?     Status
serial 1/2             172.16.3.1/24        YES     UP
serial 1/3             no address           YES     DOWN
FastEthernet 1/0       172.16.1.1/24        YES     UP
FastEthernet 1/1       172.16.2.1/24        YES     UP
Null 0                 no address           YES     UP

R2#show ip interface brief
Interface              IP-Address(Pri)      OK?     Status
serial 1/2             172.16.3.2/24        YES     UP
serial 1/3             no address           YES     DOWN
FastEthernet 1/0       172.16.4.1/24        YES     UP
FastEthernet 1/1       no address           YES     DOWN
Null 0                 no address           YES     UP
```

(4) 在 R1、R2 上配置静态路由。

```
R1(config)#ip route 172.16.4.0 255.255.255.0 serial 1/2

R2(config)#ip route 172.16.1.0 255.255.255.0 serial 1/2
R2(config)#ip route 172.16.2.0 255.255.255.0 serial 1/2
```