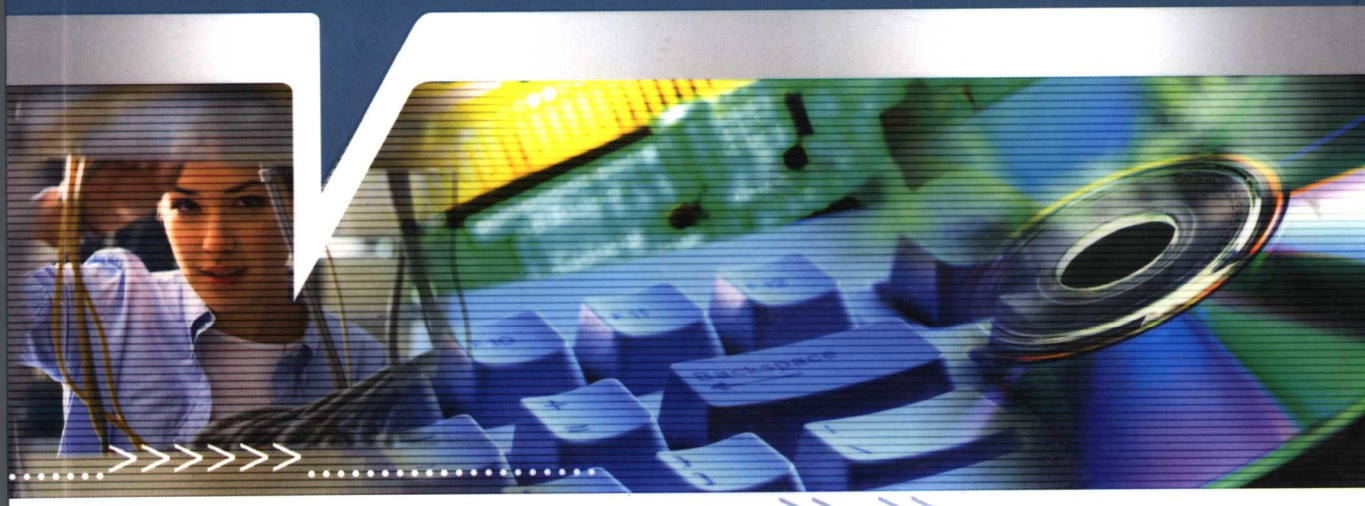
模块化网络实验指导丛书
Series of Modular Network Experiment Guides

网络安全与管理项目实验指导书

Network Security and Management Project Experiment Guide

◎ 姚 羽　宋真君　李文宇　等编著



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

模块化网络实验指导丛书

网络安全与管理项目实验指导书

姚　羽　宋真君　李文宇　等编著

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

模块化网络实验指导丛书之《网络安全与管理实验项目指导书》主要介绍了防火墙的初始配置、防火墙网桥模式、防火墙路由模式和防火墙 NAT 功能等防火墙产品的基本操作技术；在 VPN 私有专用网络部分介绍了 VPN 设备的基本操作技术、VPN 通信实验、Access VPN、Intranet VPN 通信、IPSec VPN 穿越 NAT 的通信、Access VPN 用户授权、Intranet VPN 桥模式等基本操作技术模块。在身份认证部分中，介绍了 802.1x 交换机的配置、RG-SAM 的安装与配置、接入身份认证、在线用户管理、DHCP Option82 等基础网络安全技术内容。在网络管理部分的实验操作中，编排了 StarView 二层拓扑发现、StarView 三层拓扑发现、StarView 节点性能监控和 StarView 事件告警的网络实验、实训基础和操作。在 IDS 部分安排了 IDS 操作技术中的策略管理实验、IIS 服务漏洞攻击检测实验、RG-IDS 与 RG-WALL 防火墙联动实验、Windows PnP 远程执行代码漏洞攻击检测实验、端口扫描攻击检测实验。

网络安全与管理实验指导书主要面向大、中专院校计算机网络专业的教师和学生，为开展实验、实训教学提供可选择的指导教程，也可为其他专业的学生和相关认证提供实验指导。

图书在版编目（CIP）数据

网络安全与管理项目实验指导书/姚羽等编著. —北京：电子工业出版社，2007.12
（模块化网络实验指导丛书）
ISBN 978-7-121-05440-2

Ⅰ. 网… Ⅱ. 姚… Ⅲ. 计算机网络—安全技术 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2007）第 180706 号

责任编辑：周宏敏
印　　刷：北京天宇星印刷厂
装　　订：三河市鹏成印业有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1 092　1/16　印张：20　字数：512 千字
印　　次：2007 年 12 月第 1 次印刷
印　　数：4 000 册　　定价：35.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

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。

服务热线：（010）88258888。

创新网络技术教材编委会

《模块化网络实验指导丛书》编写小组成员

姚　羽	博士	东北大学信息科学与工程学院
王　玲	教授	四川师范大学计算机科学学院
沈　岳	副教授	湖南农业大学信息科学技术学院
贺　平	教授	广东番禺职业技术学院
宋真君	副教授	辽宁省交通高等专科学校
张国清	副教授	辽宁省交通高等专科学校
安淑梅	工程师	福建星网锐捷网络有限公司
刘　亮	工程师	福建星网锐捷网络有限公司
汪双顶	工程师	福建星网锐捷网络有限公司
方　洋	工程师	福建星网锐捷网络有限公司
杨　靖	工程师	福建星网锐捷网络有限公司
石　林	工程师	福建星网锐捷网络有限公司
李文宇	工程师	福建星网锐捷网络有限公司
叶　榕	产品经理	福建星网锐捷网络有限公司
刘　鹏	产品经理	福建星网锐捷网络有限公司
刘学斌	产品经理	福建星网锐捷网络有限公司
李海全	产品经理	福建星网锐捷网络有限公司
朱继明	产品经理	福建星网锐捷网络有限公司
陈　俊	产品经理	福建星网锐捷网络有限公司
季　翔	产品经理	福建星网锐捷网络有限公司
张　勇	产品经理	福建星网锐捷网络有限公司
谷会波	产品经理	福建星网锐捷网络有限公司

序

进入21世纪，随着信息技术的快速发展和普及，计算机网络的地位越来越重要，人们在日常生活、工作和学习中越来越依赖于网络。培养一大批熟练掌握网络技术并具有综合应用能力的人才，已成为当前我国社会发展的迫切需要。网络技术学习和网络人才培养在各级、各类教育中也占据了重要的地位。在当前课程和教学改革如火如荼的大环境下，各院校都在努力对传统的计算机网络专业教学进行发展和完善，以满足不同专业和不同层次教学的需求，这也对新型的课程和教材提出了新的要求。

学会工作，将所学知识和技能快速应用于现实工作中并圆满完成实际工作任务，是现代教育的特点和灵魂。毕业生完成综合性工作的质量的高低，是衡量各类教育、教学质量的重要标志。如何有效地把理论知识、实践技能与实际应用有机结合在一起，是整个教学活动的核心。由于计算机网络是一门理论性和实践性都很强的技术，因此，要想真正掌握网络技术并创造性地解决实际技术问题，达到融会贯通、学以致用的目的，仅仅学习书本上的知识是远远不够的。只有在特定的网络实训环境中，通过大量的、综合性的工作与学习任务的学习，理论联系实际，才能取得较好的学习效果。

如何针对传统课程的缺点进行课程模式和教学方法的改革？专业教学如何适应飞速发展的网络技术的日新月异的技术标准？如何使毕业生尽快适应企业的工作需求？这些都是目前网络技术教育工作者思考和探索的问题。创新网络技术教材编委会编写的这套《模块化网络实验指导丛书》，正是针对这一思考和探索的反应。这套由一线教师、国内著名网络设备和方案解决厂商共同编写的网络实验、实训指导丛书，以网络实用技术为脉络，将当前网络行业发展的最新实用技术传递到教学第一线，把企业在实际工程项目中积累的丰富经验带到了教学第一线。丛书中的所有内容都来自于企业的实际工程项目，并通过一线教师验证和审阅。在网络实验室中搭建出工程项目，知识的展示和诠释上按照企业实际工作情境和工作过程循序渐进地进行，体现了从实际出发、帮助学习者积累项目经验、以尽快具备企业所需要的实际工作能力的教学指导思想。

我真诚地希望这套丛书能够帮助相关院校更快、更好和更容易地培养出社会所需要的网络技术人才，为我国网络技术教育送上一股不断创新的改革东风，为网络技术教育的发展锦上添花。

北京师范大学技术与职业教育研究所

2007-11-15

出 版 说 明

纵观网络技术的发展历史，新知识、新技术、新标准层出不穷，日新月异，技术的更新远远超过其他专业，导致学校网络专业教学一直处于一个尴尬的境地，教材的更新远远慢于技术的换代，教学内容的陈旧给网络技术人才培养及网络专业教学提出了极大挑战，新教材的编写和更新也显得日益迫切。正是在这样的背景下，创新网络技术教材编委会联合院校、锐捷网络厂商、出版社编写了这套网络实验、实训指导丛书。丛书以网络实用技术为脉络，将目前网络行业的最实用、最新的技术传递到教学一线，把厂商积累的工程项目带到教学一线，以期为网络技术教学和学习提供更多的实验、实践教学参考与借鉴。

本套丛书在一年前推出了电子版，深受大中专院校教师的喜爱，纷纷给出反馈，希望能印刷出版。经过精心筹划推出的《模块化网络实验指导丛书》，包括交换技术、路由技术、无线技术、防火墙技术、VPN 技术、网络管理技术、IPv6 技术、存储技术、VoIP 技术、综合案例、身份认证、融合通信共 12 个网络知识模块。在成书之际，又进行了精心修改和补充，使内容更符合大中专院校网络专业的教学需求，因此具有与其他类型的教材不同的体系架构和风格，具有突出的特点。

（1）理念的创新。采用模块抽取的结构组织知识体系。首先，对于技术内容的抽取，每个学校可以根据课程设置、课时安排，灵活地从丛书提供的各类实验指导模块中选取与理论教材配套的实验指导模块，组成适合于各学校教学需要的实验内容。其次，对于实验内容的数量抽取，丛书为每项技术都设计了一定数量的实验，教师可以根据学生的能力及课时安排，针对每种技术讲授，选择开展哪些实验模块内容。

（2）形式的创新。从设计开始就考虑到实验更新的及时性、灵活性，采用模块化的结构方式，把网络专业知识教学体系中涉及的知识内容，按照知识体系编成几个大的知识模块，以便于教师从中遴选实验，同时根据教学需要将自己设计的实验加入所属类别的模块中。每个子模块又细分成几个小的模块，读者可以根据自己的知识基础，按照目前掌握知识的程度，选择自己需要的内容，抽取出来改编成册，以有效地配合网络专业技术的理论教学需求，强化对网络原理的更深入的理解。

（3）内容的创新。将网络技术按照技术分门别类。所有技术都是当今网络界流行的主流技术，将这些先进的网络技术融入传统课堂中，本身就是一项教学创新。同时，每个实验都附有实验目的、背景描述、实验设备、实验拓扑、实验步骤等内容。

本套丛书在规划过程中，希望选编的网络知识专业化、体系化、全面化，能体现和代表最新的网络技术发展方向，因此在内容选择上和传统教材有很大的区别，实际上是弥补传统教材在知识更新方面的不足。同时，为满足各级包括本科类院校、高职类院校、职业类院校等不同层次的教学要求，本套丛书在知识体系的编排上采用模块化的结构方式，把网络专业知识教学体系中涉及的知识内容，按照知识体系结编成几个大的知识模块，每个子模块又细分成几个小的模块，读者可以根据自己的知识基础，按照目前掌握知识的程度，选择自己需要的内容，抽取出来结编成册，开展实验、实训教学，以有效地配合网络专业技术的理论教

学需求，培养学生的网络实践能力，强化对网络原理的更深入的理解。

本套丛书中的所有知识模块都来自于企业多年积累的工程项目，在知识的诠释上按照再现企业工程项目的组织方式进行串接，每个实验或实训都详细介绍了实验名称、实验背景、技术原理、实验功能、实验目的、实验设备、实验拓扑、实验规划、实验步骤、结果验证等多个环境，循序渐进地展现企业工程项目，并把这些工程项目在网络实验室中搭建出来。真正做到了从实际出发，强化实际应用，积累学习者的项目经验，尽快适应企业工作岗位能力的教学指导思想。

本套丛书可作为计算机网络基础或者计算机网络原理等理论课程的实验课程补充，也可以作为计算机网络专业学生在学习完全部理论课程之后，为适应就业岗位的需要，单独开展的基于企业工作过程的独立技能训练课程，同时也可以作为独立的职业资格认证课程的教材。

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和网络基础知识，以帮助理解实验指导书中的网络技术原理。更重要的是应具有可以为本套丛书开展项目的网络实验室，即一个可以再现企业网络项目工程和实施网络项目的工作环境。

这种网络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 组的工作台，至少配备 1 台/2 人的 PC。每组还需要可以用来组建网络的实验设备：三层交换机设备（2 台）、二层交换机设备（2 台）、模块化路由器设备（4 台）、测试计算机 4 台（每组）和若干根网络连接线，这些都是组建基础网络必需的基本设备。

此外，如果需要开展网络安全技术原理和网络安全操作技能的学习，则应为每组实验台配置网络防火墙、VPN 等安全设备若干；如果需要开展无线网络技术原理和无线局域网络操作技能的学习，则应为每组实验台配置无线接入设备 AP、无线网卡、无线网桥等无线设备若干；如果需要开展网络存储技术原理和网络存储设备操作技能的学习，则应为每组实验台配置网络存储设备若干；如果需要开展网络管理原理和网络管理操作技能的学习，则应为每组实验台配置网络管理软件包等。学习者可以根据自己的需要合理进行模块化组合和安排。

本套丛书对关键技术解释和方案实施中涉及到一些网络专业术语和词汇，参考实际工作中惯有的风格和惯例，使用下述约定。

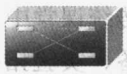
¦（虚线）：表示在几个选项中选择一个，并且这些选项是互相排斥的。

[]（方括号）：表示可选择的参数。

{}（大括号）：表示一个必需的选择参数。

!（感叹号）：表示对该行命令的解释和说明。

 ：路由器。

 ：二层交换机。

 ：三层交换机。

 ：核心交换机。

 ：PC。

 ：服务器。

 ：Internet。

 ：防火墙。

 ：无线接入设备 AP。

 ：IDS 安全设备。

虽然本书的实验、实践内容主要针对锐捷网络开发的 RGNOS 系统，但书中出现的基本命令和术语同样具有通用性，能兼容目前网络工程中的所有主流设备。并且，书中讲述的技术原理和针对网络问题提出的解决方案，同样适用于所有现实网络的工作场景。

尽管得到了众多一线授课教师及业内专家的建议，但面对如此繁杂的编撰工作，我们深知仍然难免错漏，还望读者批评指正。同时也欢迎读者多提宝贵意见，邮件请发至 labserv@ruijie.com.cn，不胜感激！

创新网络技术教材编委会

2007 年 11 月

前言

随着网络技术的不断发展，社会经济建设与发展越来越依赖于计算机网络，与此同时，网络安全对国民经济、甚至对国家和地区的重要性也日益突显。加快培养网络安全方面的应用型人才、广泛普及网络安全知识和掌握网络安全技术迫在眉睫。

目前市场上关于网络安全与管理技术理论的教材很多，大多着眼于网络安全与管理的原理和安全算法等纯技术层面的内容，而关于网络安全与管理技术在实践中如何应用以及如何与工程项目有机结合的内容很少，因此读者在学习的过程中，接触到的大都是纯理论的知识，网络安全与管理的应用技能很差，学到的知识基础很难扎实，时间一长必然遗忘。

模块化网络实验指导丛书之《网络安全与管理项目实验指导书》是一本全面的、面向结果计算机的网络安全实验指导书，旨在提供关于计算机网络安全领域所涉及的主要知识体系和知识内容，作为读者在学习抽象的网络安全理论知识之后的实验、实践知识的补充。通过全书提供的多个实验知识模块体系，使读者全面感受网络安全知识和实际应用内容的有机结合，把知识和实际应用建立起对应关系，使学习更具针对性。同时，通过本书提供的多个实验实践项目，可以有效帮助读者对课堂教学中学到的抽象理论的理解，加深印象。

《网络安全与管理项目实验指导书》是在广泛调研和充分论证的基础上，结合当前应用最为广泛的操作平台和网络安全规范，并通过研究实践而形成的满足社会广泛需求、适合高等院校计算机教育改革和发展特点的专著。与国内同类书籍相比，本书更注重以能力为中心，以培养应用和技能为根本，通过认识、实践、总结和提高这样一个认知过程，精心组织，图文并茂，深入浅出，具有独创性、层次性、先进性和实用性。

《网络安全与管理项目实验指导书》主要介绍网络安全知识体系中涉及的网络防火墙技术、VPN 私有专用网络技术、网络身份认证技术和 IDS 网络安全管理 4 个和网络安全防范有关的实验内容模块以及一个网络管理知识模块。其中在网络防火墙技术实验模块中，按照实际工作过程中网络安全技能的需要，共安排了防火墙的初始配置、防火墙网桥模式、防火墙路由模式和防火墙 NAT 功能等基本操作技术。在 VPN 私有专用网络部分的实验模块中，共安排了 VPN 设备的基本操作技术、VPN 通信实验、Access VPN、Intranet VPN 通信、IPSec VPN 穿越 NAT 的通信、Access VPN 用户授权、Intranet VPN 桥模式等基本操作技术。在身份认证部分的实训技术中，安排了 802.1x 交换机的配置、RG-SAM 的安装与配置、接入身份认证、在线用户管理、DHCP Option82 等基础实验技术。在 IDS 网络安全实验模块中，共安排了 IDS 设备的基本操作技术、策略管理实验、RG-IDS 与 RG-WALL 防火墙联动实验、IIS 服务漏洞攻击检测实验、Windows PnP 远程执行代码漏洞攻击检测实验、端口扫描攻击检测实验等。在网络管理部分的实验操作中，安排 StarView 二层拓扑发现、StarView 三层拓扑发现、StarView 节点性能监控和 StarView 事件告警的网络实训基础和操作。

东北大学信息科学与工程学院姚羽博士、辽宁交通高等专科学校宋真君教授联合锐捷网

络的资深网络工程师李文宇和汪双顶进行了全书所有项目的开发和整理工作，此外来自锐捷网络的工程师安淑梅、刘亮、叶榕、刘鹏、刘学斌、李海全、朱继明、陈俊、季翔、张勇、谷会波等也为书中项目资料的来源提供了资料和整理工作。本书中的所有知识模块都来自于企业多年积累的工程项目，在知识的诠释上按照再现企业工程项目的组织方式进行串接，希望选编的网络知识专业化、体系化、全面化，能体现和代表最新的网络技术发展方向，因此在内容的选择上和传统教材有很大的区别，从而弥补了传统教材知识更新方面的不足。

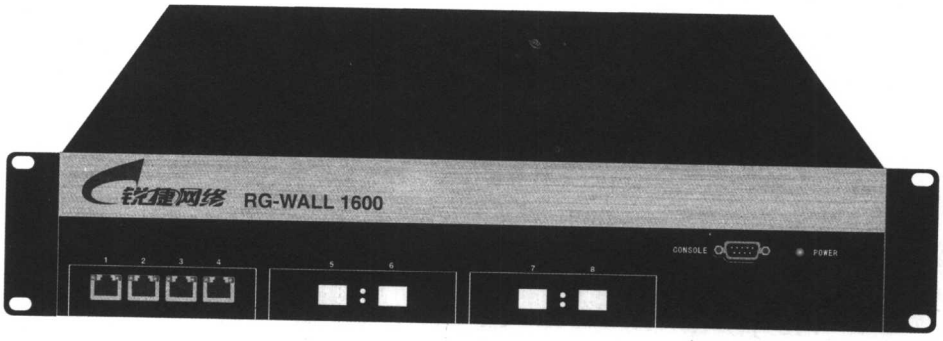
本书规划、编辑的过程历经近一年半的时间，前后经过近 6 轮的修订，改革力度之大，远远超过我们原先的估计，加之作者水平有限，错漏之处在所难免，敬请广大读者指正。

创新网络技术教材编委会

2007 年 11 月

目　录

第一篇　防火墙技术模块



实验一　防火墙的初始配置

【实验名称】

防火墙的初始配置。

【实验目的】

通过对防火墙进行初始配置，使管理人员以后可以通过 Web 方式对防火墙进行远程配置和管理。

【背景描述】

作为公司的网络管理员，一定希望在机房对防火墙进行初始配置后，以后可以通过 Web 方式对防火墙进行远程配置和管理，因此需要对其进行初始的基本设置。

本实验中 PC 通过串口 Com1 用控制线连接到防火墙的控制口（Console），通过一根交叉网线连接到防火墙的以太网口 F0，并事先在 PC 上安装了 Java 程序（j2re-1_4_0-win-i 或更高版本）。

【实现功能】

实现通过 Web 方式对防火墙进行远程配置和管理。

【实验拓扑】

如图 1-1-1 所示的网络拓扑是某公司网络中心的拓扑结构，希望在机房对防火墙进行初始配置后，以后可以通过 Web 方式对防火墙进行远程配置和管理。

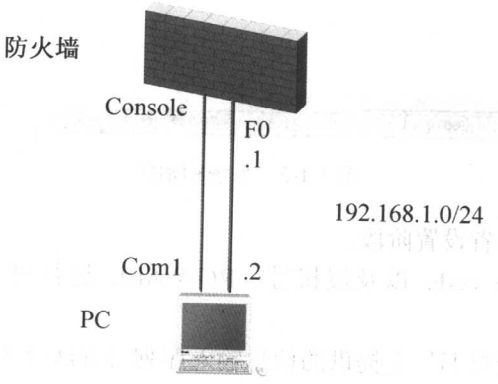


图 1-1-1　某公司网络中心的拓扑结构

【实验设备】

防火墙设备 1 台，测试 PC 1 台，网线 1 条，配置线 1 条。

【实验步骤】

第一步：登录防火墙。

```
**********************************************
** RG-OS V1.0      http://www.red-giant.com.cn **
**********************************************
RG-Wall-150 login: root
Password: rg-wall123
```

以上是系统登录的缺省 ID 和口令值。

```
/ >si                    ！进入系统初始化设置
```

RG-WALL 缺省登录的提示或者重新设置时的提示内容如图 1-1-2 所示。

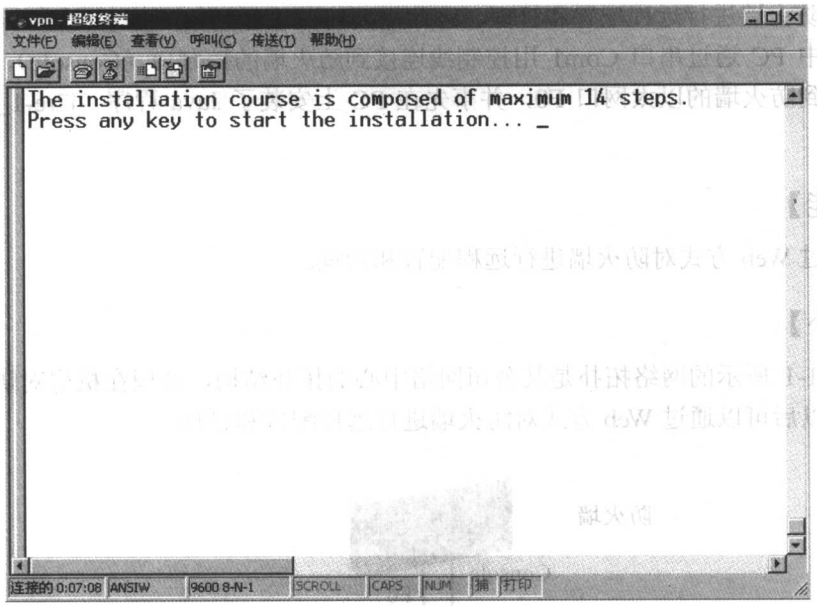


图 1-1-2　系统初始化

在此按任意键进入缺省设置阶段。

输入序列号、feature code 以及授权号：RG-WALL 运行时系统将提示输入序列号、feature code 以及授权号。

请按照“产品使用授权书”上提供的信息输入序列号并区分大小写。

序列号的格式为 SW-xx-xxxxx 以及 SK-xx-xxxxx。

```
SW-03-91004 ↵
```

输入完序列号再输入 feature code，如图 1-1-3 所示。

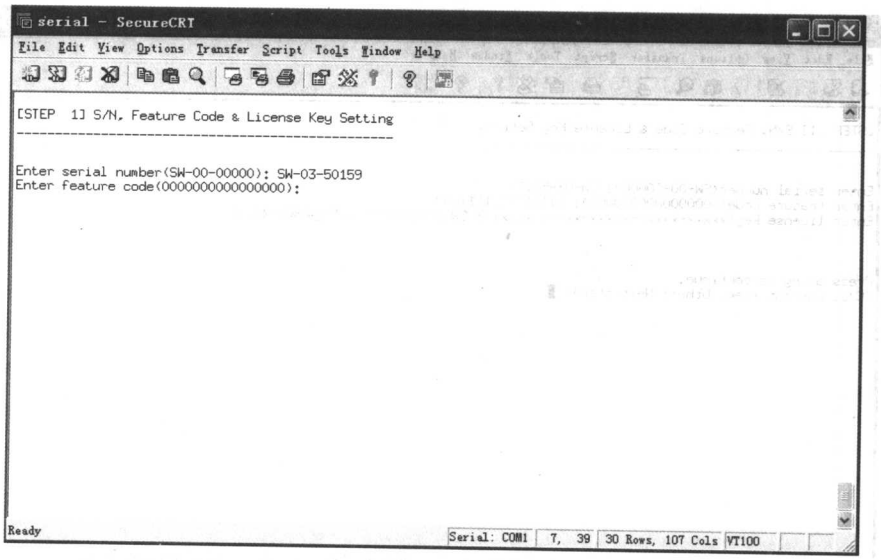


图 1-1-3 输入序列号和 feature code

feature code 是设置 RG-WALL 可使用功能的编码，是根据与公司签订的合同提供的 16 位编码。输入完 feature code 后会出现授权号输入提示，如图 1-1-4 所示。

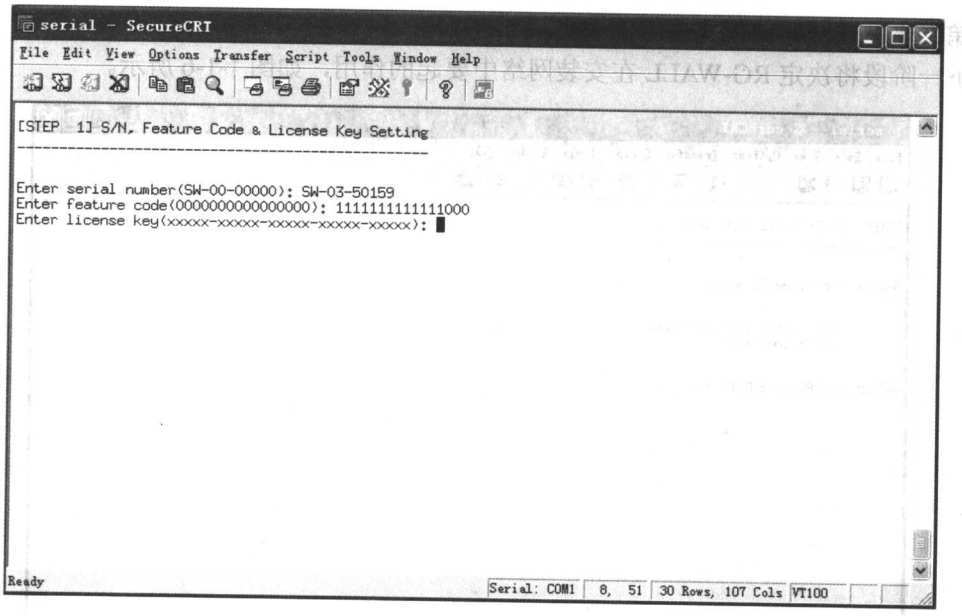


图 1-1-4 输入授权号与序列号

授权号和序列号与 feature code 相同，是公司赋予的编号。授权号输入错误时也同样不能继续安装。产品授权号输入正确后，将出现如图 1-1-5 所示的界面，从而进入下一步设置阶段。