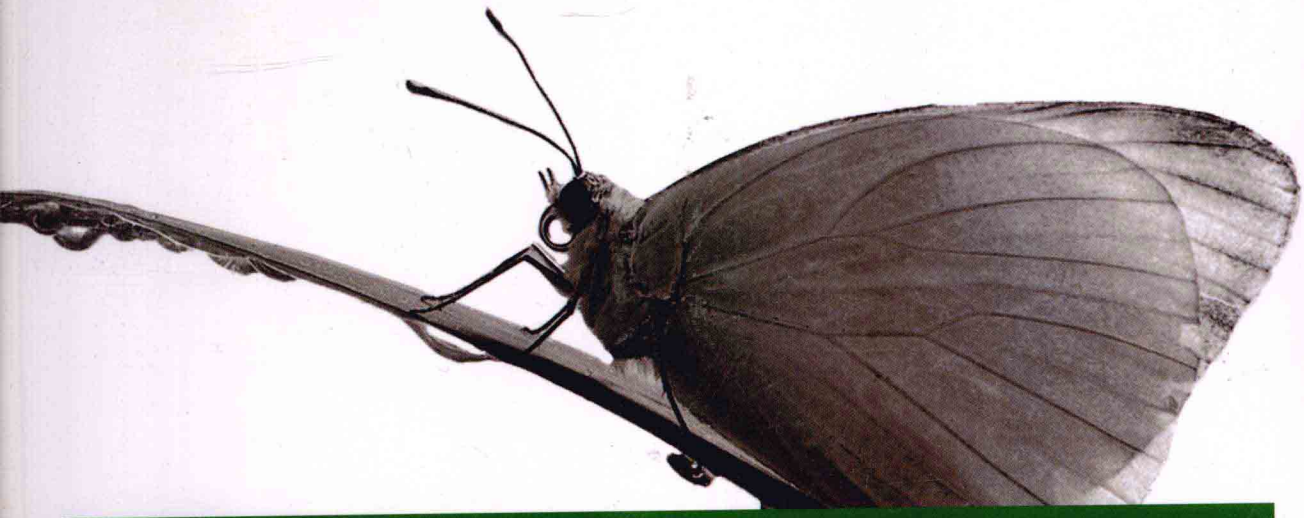
Broadview
www.broadview.com.cn

仅仅通过一台电脑，完成一整套的网络解决方案！



Router OS 全攻略

崔北亮（CCIE） 编著

Router OS是目前功能最强、应用最广的软路由，全书围绕着热门应用和网络管理的实际需求展开，通过近百个实验，介绍了网络架设、访问控制、认证计费、VPN部署、限速与QoS、无线部署和网络监控的实现等。

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

Router OS 全攻略

崔北亮（CCIE） 编著

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

内 容 简 介

本书针对当前网络的突出问题（譬如带宽控制、服务优先、BT 下载、QQ 聊天、认证计费、网络安全、异地互联和无线接入等），从网络管理工作的实际需要出发，给出各种解决方案。书中全面、系统地介绍了 Router OS 在网络建设和管理中的各种应用。全书共十七章，内容包括 Router OS 安装、命令行介绍、NAT 配置、路由原理和配置、交换机的 VLAN 划分和 Trunk 路由、PPPoE 服务器架设和计费管理、VPN 架设和用途、速率控制和 QoS 的实现、防火墙配置及应用、用户访问日志记录、多出口的冗余和负载均衡、无线网络的配置、用户的管理、多种协议介绍和应用（包括 VRRP、EoIP、RIP、OSPF、ARP、NTP、SNMP）、带宽测试、网络监控和网络安全等。第 17 章补充介绍了 SolarWinds 网管软件在大型网络中的部署和应用，使复杂的网络管理变得一目了然，直观高效。

本书适用于所有网络管理人员，尤其适用于中小企事业单位、网吧、宾馆和运营商的网络管理人员；更是那些想掌握网络技术、提高动手能力、并能应用于实践的网络爱好者，是一本难得一见的实验指导用书。

图书在版编目（CIP）数据

Router OS 全攻略 / 崔北亮编著. —北京：电子工业出版社，2010.5
ISBN 978-7-121-10688-0

Ⅰ. ①R… Ⅱ. ①崔… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2010）第 065087 号

责任编辑：李 冰
印 刷：北京智力达印刷有限公司
装 订：北京中新伟业印刷有限公司
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：787×980 1/16 印张：20 字数：431 千字
印 次：2010 年 5 月第 1 次印刷
印 数：4000 册 定价：50.00 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。

前　言

我在大学的网络中心工作十多年，面对的是充满好奇与逆反、极具表现的大学生，可以说大学的网络算是社会上最难管理的网络了。为了限制用户的疯狂下载，学校投资了近40万，购买了专业的流控；为了对用户的网络行为进行约束，学校投资近40万购买了专业的认证系统，对用户的身份进行审核，记录用户的网络行为；为了实现共享上网，学校投资了近50万购置了专业的防火墙；为了校外的合法用户可以使用校内的资源，学校投资了近20万，购置了VPN接入设备。有了这些专业设备的投入，网管终于可以稍做喘息了，可主干上串接的任何设备故障，包括防火墙、流控设备、计费设备等都会导致网络瘫痪。

近十年来，我代表江苏省电教馆培训了全省近3000名中小学网管人员，同时也给各类企业培训了上千名网络技术骨干，很多单位和企业的环境与大学大体相仿，同样面临着很多网络方面的棘手问题，可我校的成功管理经验却不足以被他们借鉴，原因在于很多中小企业和中小学校没有高校这么多的资金投入，也缺乏能同时驾驭这么多厂商设备的网络管理人员。

这里我很荣幸地向大家推荐一款软路由产品——Router OS。Router OS是一种路由操作系统，通过该软件可以将标准的PC电脑变成专业路由器，在软件的开发和应用上可以不断地更新和发展，使其功能不断增强和完善，几乎可以满足网络管理者的所有需求。Router OS的功能包括：NAT、PPPoE、VPN、速率控制和QoS实现、防火墙配置、用户访问控制和访问记录、多出口的冗余和负载均衡、无线网络配置、策略路由、带宽控制、脚本编写、认证与计费、VRRP、RIP和OSPF、EoIP、NTP、网络监控和带宽测试等，几乎是一套整体的网络解决方案。很多学员向我提出的难题都在Router OS中找到了解决方案。Router OS强大的功能、低廉的价格、极高的性价比和可扩展性足以让所有的硬件路由望尘莫及。

本书全面介绍了Router OS的各项功能，很多章节更是加入了本人的心得和体会，为了便于读者的学习和使用，软件包中提供了本人编写的所有源程序和代码。限于本人水平有限，一些小的错误在所难免，不足之处敬请谅解，对已发现的错误都会在“http://blcui.njut.edu.cn/bbs”论坛及时更新。

致谢

首先要特别感谢电子工业出版社的李冰等编辑，他们在我写作的过程中给了很多无私的帮助和鞭策。感谢中国路由论坛“http://bbs.router.net.cn/”和软件路由论坛“http://bbs.routerclub.com/”上的各位版主和版友，我从论坛中得到了很多启发和提高。

本书写作目的

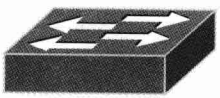
Router OS 功能强大却鲜为人知；市面上虽有一些厂商说明手册，但多繁琐并且功利性强；网络上虽有一些介绍，但多支离破碎，系统性不强。本书从实际需求出发，针对目前网络中的焦点问题和热门应用展开，系统地讲解满足各种需求的配置步骤，解决用户没有硬件设备和资金不足的苦恼。仅仅通过一台电脑，完成一整套的网络解决方案。

资源下载

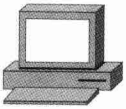
为了节省读者的开支，本书涉及的所有应用软件、程序和代码均可从作者的个人主页“http://blcui.njut.edu.cn/ros.rar”处下载。为了便于读者能更好地阅读此书，相互交流，作者个人主页上开通了“http://blcui.njut.edu.cn/bbs”讨论版。

图标示例

在本书中使用的图标如下：

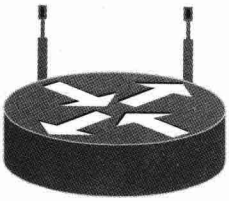


二层交换机

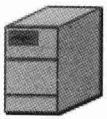


PC 机

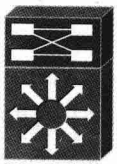
路由器



无线路由器



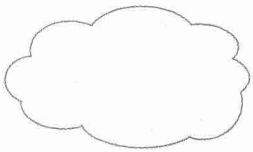
服务器



路由交换机

无线和虚电路

双绞线



网云

目　录

第 1 章　安装 Router OS ····· 1

1.1　ROS 概述基础 ····· 1

1.2　安装 ROS ····· 2

1.2.1　安装 VMware 虚拟机软件 ····· 2

1.2.2　虚拟机的基本设置 ····· 3

1.2.3　安装 ROS 操作系统 ····· 7

1.2.4　获取授权文件 ····· 10

第 2 章　ROS 基础 ····· 11

2.1　ROS 命令行 ····· 11

2.2　使用 Winbox ····· 13

2.2.1　配置 Winbox ····· 13

2.2.2　更新授权 ····· 17

2.2.3　删除及添加模块 ····· 18

2.2.4　升级 ROS ····· 19

2.3　接口管理 ····· 20

2.4　实验拓扑 ····· 22

2.4.1　ROS 配置 ····· 22

2.4.2　配置 Windows Server ····· 25

2.5　Setup 命令 ····· 28

2.6　DHCP ····· 32

2.7　ADSL 接入 ····· 36

第 3 章　NAT 和路由 ····· 38

3.1　动态 NAT ····· 39

3.2　静态 NAT ····· 41

3.3　构建思科路由和交换机架 ····· 44

3.3.1 拓扑 45
3.3.2 安装 Dynamips 46
3.3.3 Dynamips 的使用方法 49
3.3.4 设计 Dynamips 的拓扑 50
3.4 路由 51
3.4.1 直连路由 51
3.4.2 静态路由 51
3.4.3 默认路由 60
3.4.4 单臂路由 60
3.4.5 动态路由 64
3.4.6 恢复 ROS 配置 64
第 4 章 PPPoE 65
4.1 PPPoE 服务 65
4.2 RADIUS 计费 72
4.3 搭建用户自助平台 78
4.3.1 安装 IIS 78
4.3.2 配置 Web 站点 79
第 5 章 VPN 83
5.1 VPN 基础知识 83
5.1.1 VPN 优点 83
5.1.2 VPN 分类 84
5.1.3 实验拓扑 84
5.2 站点到站点 VPN 86
5.2.1 PPTP VPN 87
5.2.2 IPSec VPN 89
5.3 远程访问 VPN 92
5.3.1 配置远程访问 VPN 92
5.3.2 使用 RADIUS 计费 99
5.3.3 VPN 借道访问 99
第 6 章 速率控制 101
6.1 队列类型 101

6.2 简单队列 102
6.2.1 单个 IP 限速 102
6.2.2 网段限速 106
6.2.3 队列执行顺序 106
6.2.4 配置突发 107
6.2.5 连续多个 IP 限速 108
6.2.6 PCQ 动态限速 110
6.3 队列树配置 114
6.4 网吧应用示例 116
第 7 章 脚本生成器 120
第 8 章 路由器的安全 125
8.1 防止外部访问路由器 125
8.2 管理路由器配置文件 126
8.3 导出和导入命令 127
第 9 章 防火墙配置 129
9.1 设置专业防火墙规则 129
9.2 防火墙过滤规则详述 130
9.3 防火墙应用示例 135
9.3.1 防止二级代理 135
9.3.2 限制 TCP 连接数 143
9.3.3 七层协议过滤 144
9.3.4 内部用户上网管理 146
第 10 章 热点服务 148
10.1 热点服务详述 148
10.2 配置热点服务 150
第 11 章 日志 162
11.1 ROS 系统日志 162
11.2 ROS 用户访问日志 165
第 12 章 多出口应用 171
12.1 搭建环境 171

12.2 根据目的 IP 地址双线分流 …… 174
12.3 根据建立连接双线分流 …… 182
12.4 根据源 IP 地址双线分流 …… 188
第 13 章 无线配置 …… 192
13.1 配置无线路由 …… 192
13.2 无线漫游 …… 201
13.3 桥接有线和无线网卡 …… 203
13.4 增强无线网卡的功率 …… 204
13.5 无线远距离传输 …… 208
第 14 章 用户管理 …… 213
14.1 User Manager …… 213
14.2 认证计费 …… 220
第 15 章 高级协议 …… 222
15.1 VRRP …… 222
15.1.1 VRRP 介绍 …… 222
15.1.2 VRRP 实验 …… 226
15.2 EoIP …… 231
15.2.1 互联远程网络 …… 231
15.2.2 桥接远程网络 …… 235
15.3 动态路由协议 …… 237
15.3.1 静态路由与动态路由 …… 237
15.3.2 管理距离 …… 238
15.3.3 路由选路原则 …… 238
15.3.4 距离矢量和链路状态路由协议 …… 239
15.4 RIP …… 240
15.5 OSPF …… 247
15.6 MPLS …… 250
第 16 章 小型应用 …… 257
16.1 ARP 的攻、判、防 …… 257
16.2 NTP …… 270
16.2.1 NTP 客户端 …… 270

16.2.2 NTP 服务端 ····· 272
16.3 SNMP ····· 274
16.4 带宽测试 ····· 275
16.5 破解 ROS 密码 ····· 278
16.6 网络监控 ····· 279
16.6.1 Torch ····· 279
16.6.2 Tracking ····· 280
16.6.3 Packet Sniffer ····· 281
16.7 防端口扫描 ····· 285
16.8 计划任务 ····· 286
16.9 Netwatch ····· 287
第 17 章 SolarWinds 网管系统 ····· 291
17.1 功能简介 ····· 291
17.2 安装 SolarWinds ····· 295
17.3 配置 SolarWinds ····· 297

第 1 章 CHAPTER 安装 Router OS

本章介绍 Router OS（简称“ROS”）特点、VMware 虚拟机的使用及安装 ROS 等。

1.1 ROS 概述基础

ROS 是一种路由操作系统，可通过它将标准的 PC 变为专业的路由器，在软件的开发和应用上不断地更新和发展，经过多次升级和改进，其功能也在不断增强和完善。ROS 除具备普通路由器的基本功能外，在无线、认证、策略路由、带宽控制和防火墙过滤等方面上也有非常突出的表现，其极高的性价比受到越来越多网络专业人员的青睐。

ROS 可安装在普通的 PC 中，一台 586 PC 安装 ROS 后就可以实现路由功能，达到提高网络访问速度和吞吐量的效果，成为一套低成本且高性能的路由器系统。ROS 的主要特点如下。

（1）价格优势

一般普通的路由器动辄上万元，而一台淘汰的 PC 就可以满足 ROS 的安装条件，性能方面也绝不亚于一般的硬件路由器。

（2）功能强大

ROS 除具备目前路由系统的大部分功能外，还具备很多专业硬件路由器无法实现的功能，正开始走向系统化、专业化和多元化，可以实现防火墙、路由器、流量控制、网桥、无线 AP（Access Point，接入点）、认证系统、VPN（Virtual Private Network，虚拟专用网）、网络监控和日志记录的功能，几乎是一套完整的网络解决方案。

笔者是思科 CCIE 认证取得者，了解多数厂家的网络设备，ROS 的很多功能在多数硬件路由器上无法实现，而这些功能却是网络管理者迫切需要的，本书将对这些特殊功能进行介绍。

（3）系统稳定

ROS 采用 Linux 内核，系统安全稳定，不像 Windows 系统的漏洞层出不穷，安全时刻

受到威胁。

（4）速度快

Linux 系统经过实践考验，在并发处理和内存管理方面具有较高的效率。ROS 对 Linux 系统进行了一定的封装，使效率更高。

（5）零维护

由于 Linux 系统的稳定性，ROS 在配置完成后，一般可以做到零维护，减少用户在网络方面的维护开销。

（6）增减服务方便

这是所有软路由的优势，可以很容易地增加和减少一个功能，并可以根据当前网络存在的突出问题下载安装新的功能包。

（7）添加删除模块方便

添加和删除模块即添加和删除一块网卡，价格便宜且操作方便。

（8）可编程

ROS 支持脚本，可编程，进而可以实现更复杂的任务。

（9）适用面广

ROS 能适应网吧、企业、小型 ISP（Internet Server Provider，Internet 服务提供商）接入商及社区等场合。

1.2 安装 ROS

本书中的大多数实验都可以在同一台计算机上完成，为了不影响正常工作，将 ROS 安装在一台虚拟的计算机中。借助 VMware 软件，可以在一台物理计算机上安装多台虚拟计算机。这些虚拟计算机可以被安装不同或相同的操作系统，它们之间协同工作，用来模拟真实的网络环境。

1.2.1 安装 VMware 虚拟机软件

VMware 软件可以从 ros.rar 压缩包中找到，本书中涉及的所有软件和脚本均可以在该压缩包的相应章节的文件夹中找到，也可以从笔者的个人主页“http://blcui.njut.edu.cn/ros.rar”中下载该软件包，或者在笔者的个人论坛“http://blcui.njut.edu.cn/bbs”中交流和讨论。

把 ros.rar 压缩包解压到计算机的硬盘中，双击 1\VMware-workstation\VMware-workstation-5.5.1-19175.exe 文件开始安装。安装过程比较简单，安装完成后真实计算机的网络连接如图 1-1 所示。多出两块网卡简称为“VMnet1”和“VMnet8”，本书所

有实验用不到 VMnet8 网卡，建议永久禁用。

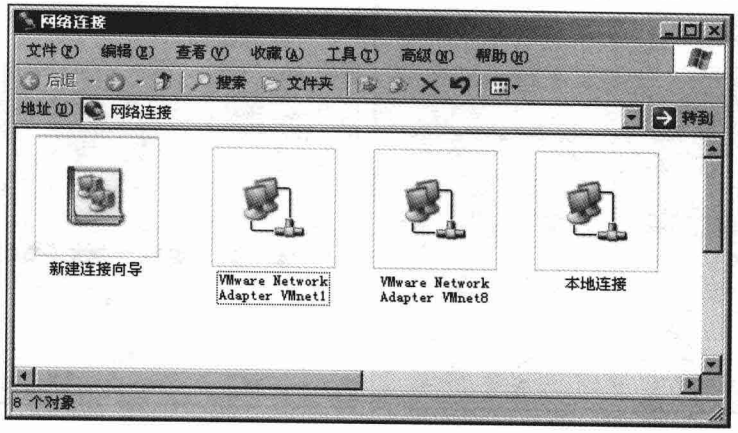


图 1-1　VMware 安装完成后的网络连接

1.2.2　虚拟机的基本设置

1．虚拟机的初始设置如下

（1）运行 VMware 软件，单击“File”→“New”→“Virtual Machine”选项，如图 1-2 所示。

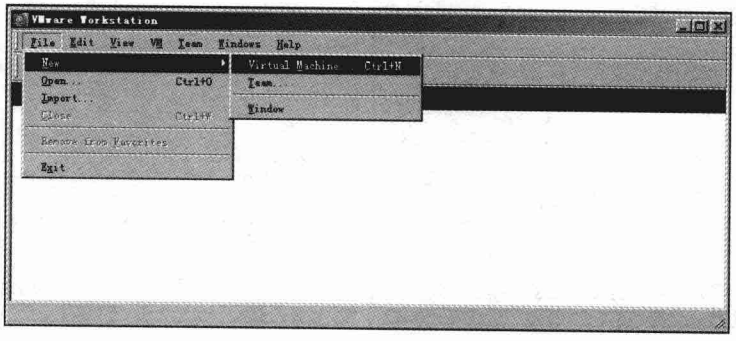
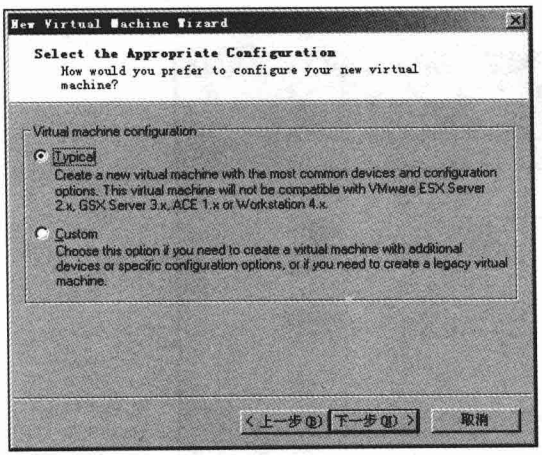


图 1-2　“Virtual Machine”选项

（2）弹出“New Virtual Machine Wizard”窗口，单击“下一步”按钮，弹出“Select the Appropriate Configuration”对话框，如图 1-3 所示。

（3）单击“下一步”按钮，弹出“Select a Guest Operating System”对话框，如图 1-4 所示。选择“Other”单选按钮。



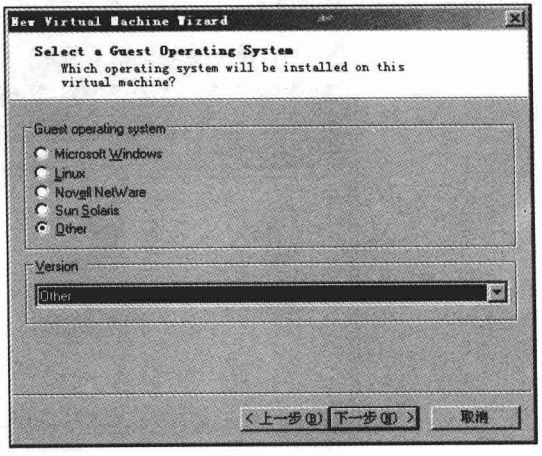
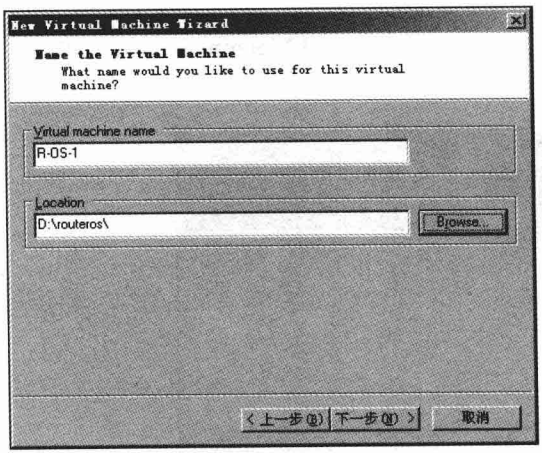


图 1-3 “Select the Appropriate Configuration”对话框　图 1-4 “Select a Guest Operating System”对话框

（4）单击“下一步”按钮，弹出“Name the Virtual Machine”对话框，如图1-5所示。注意“Location”文本框用于设置ROS的安装路径，ROS需要的硬盘空间很少，一般64 MB已够。

（5）单击“下一步”按钮，弹出“Network Type”对话框，如图 1-6 所示。



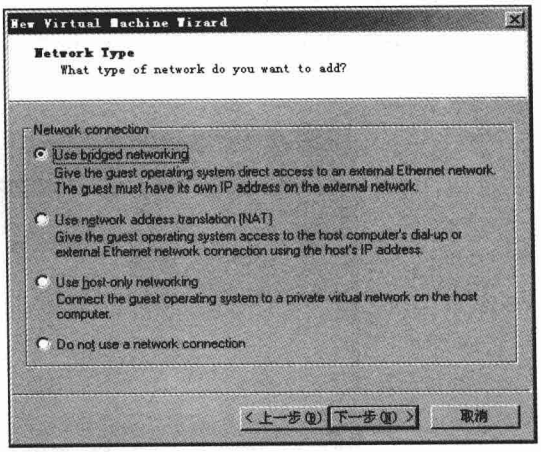


图 1-5 “Name the Virtual Machine”对话框　图 1-6 “Network Type”对话框

其中的 4 个单选按钮如下。

- Usebridge networking（桥接）：选择该单选按钮，直接将虚拟网卡桥接到真实机的物理网卡上，相当于在真实机的前面连接一台交换机。虚拟机和真实计算机都接在交换机上，二者处于同等的地位，在网络关系上是平等的，使用这种方式的前提是需要得

到多个 IP 地址。网卡类型可以随时改变，即使虚拟机启动后也可实时改变并立即生效。

- Network Address Translation（NAT，网络地址转换）：安装 VMware 后可以通过单击真实计算机的“开始”→“程序”→“管理工具”→“服务”选项找到“VMware DHCP Service”服务，该服务自动为配置成 NAT 和 Host-only 类型的虚拟机分配 IP 地址，这样虚拟机就可以使用 DHCP 服务。配置为 NAT 类型的虚拟机可以借助真实计算机的合法 IP 访问外部网络，提供了从虚拟机私有 IP 到真实计算机合法 IP 之间的地址转换。相当于有一个 NAT 服务器在运行，只不过这个 NAT 配置集成到 VMware 中了，不需要用户配置。如果只有一个外网地址，这种方式很合适，本书中的实例不需要使用这种网卡类型。
- Use host-only networking（主机模式）：选择该单选按钮，没有地址转换服务。因此，默认情况下，虚拟机只能访问真实计算机，这也是 Host-only 的名字的意义。并且也会有一个 DHCP 服务加载到 VMnet1 上，这样连接到 VMnet1 上的虚拟机仍然可以设置为 DHCP，方便系统的配置。这种方式更为灵活，用户可以手工配置 NAT。

提示

Host-only 需要借助真实计算机的 VMnet1 网卡，因此不能将其禁用。

- Do not use a networking connection：选择该单选按钮，不使用网络，虚拟计算机是一台单机。

每种网络类型都有其优势和特点，可以根据实际需要选择。

（6）单击“下一步”按钮，弹出“Specify Disk Capacity”对话框，如图 1-7 所示。

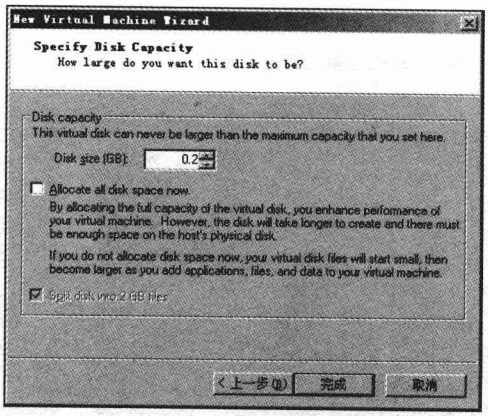


图 1-7 “Specify Disk Capacity”对话框

设置虚拟机硬盘为 0.2 GB。选择“Allocate all disk space now”复选框，立即从物理硬盘中划出虚拟机使用的硬盘空间；否则虚拟机的硬盘大小是动态变化的。选择“Split disk into 2 GB files”复选框把虚拟机硬盘文件分成 2 GB 的多个文件。

（7）单击“完成”按钮，完成虚拟机的初始设置。

2．更改虚拟机的配置

虚拟机初始设置后相当于购置了一台新的计算机，不过是裸机（即只有硬件，还没有安装操作系统的计算机）。如不满意虚拟机的默认硬件的设置，可以单击图 1-8 中的“Edit virtual machine settings”选项修改内存大小、网卡数量及类型，以及光盘来源（如果没有系统光盘，可以用 ISO 代替）等，这里删除不使用的“Audio”（声卡）。

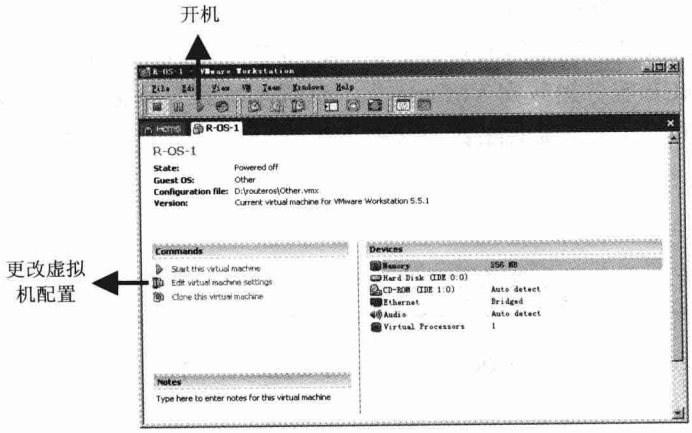


图 1-8　更改虚拟机配置

启动后也可动态更改网卡类型。单击“VM”→“Removable Devices”→“Ethernet”→“Edit”选项，如图 1-9 所示。

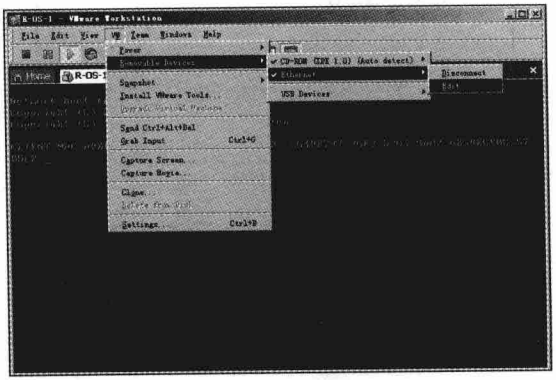


图 1-9　“Edit”选项