TURING 图灵计算机科学丛书

WILEY

Computer Networking

Internet Protocols in Action

计算机网络实验教程

[美] Jeanna Matthews 著
李毅超 曹 跃 王 钰 等译

人民邮电出版社
POSTS & TELECOM PRESS

TURING 图灵计算机科学丛书

Computer Networking
Internet Protocols in Action

计算机网络实验教程

[美] Jeanna Matthews 著

李毅超 曹 跃 王 钰 等译

人民邮电出版社
POSTS & TELECOM PRESS

图书在版编目（CIP）数据

计算机网络实验教程 /（美）马修著；李毅超译. —北京：人民邮电出版社，2006.1
（图灵计算机科学丛书）

ISBN 7-115-14250-5

Ⅰ. 计… Ⅱ. ①马…②李… Ⅲ. 计算机网络—教材 Ⅳ. TP393

中国版本图书馆 CIP 数据核字（2005）第 154864 号

版 权 声 明

图灵计算机科学丛书

计算机网络实验教程

◆ 著 [美] Jeanna Matthews
译 李毅超 曹 跃 王 钰 等
责任编辑 杨海玲

◆ 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 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京鸿佳印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：12.75
字数：301 千字 2006 年 1 月第 1 版
印数：1－5 000 册 2006 年 1 月北京第 1 次印刷

著作权合同登记号 图字：01-2005-5705 号
ISBN 7-115-14250-5/TP・5123

定价：29.00 元

读者服务热线：(010)88593802 印装质量热线：(010)67129223

内 容 提 要

本书运用简洁易懂的描述和生动直观的实例，介绍计算机网络及其协议。书中创造性地使用开源网络协议分析软件 Ethereal 观察应用层、传输层、网络层、链路层和有关网络安全的各种协议的活动，进行实验，使读者能够在不具备网络设备的情况下深入了解计算机网络协议。

本书已经在康奈尔大学等学校本科生和研究生的计算机网络教学中得到成功运用。本书适合作为计算机、通信、电子等相关专业的本科生和研究生的计算机网络课程配套教材，还为自学计算机网络的读者提供非常理想的指导，对于相关技术人员同样是一本不可多得的参考书。

译 者 序

我们有幸翻译了 Jeanna Matthews 博士的这本著作。这是一本通俗、直观、全面介绍计算机网络和 TCP/IP 协议的书籍，是一本优秀的教材和参考书。作者巧妙应用开源网络协议分析软件 Ethereal，以一种创造性的方式教授计算机网络知识。内容从轻/重流量网络的基础知识开始，然后讲到应用层、传输层、网络层、链路层以及有关网络安全的重要知识，涉及了诸多当前的热点研究问题。

借助本书读者在没有真实网络环境的情况下，仍然能够通过实践学习计算机网络协议。同时本书也为教师省去收集教学材料的麻烦，提供了教授网络课程的宝贵课件。这些都已在包括康奈尔大学在内的美国大学的教学实践中得到了验证。本书的创作体现了作者对计算机网络的清晰理解，凝聚了作者计算机网络教学的丰富经验。对于那些没有计算机网络实验设备环境条件的大学生或是自学者，这本书必将是一个“新大陆”。这也是我们愿意花费时间和精力翻译此书的真正动力，谨以此表示对本书作者 Jeanna Matthews 博士的敬佩。我们慎重地将这本书推荐给读者，并深信读者阅读此书定会受益匪浅。

本书是由电子科技大学计算机科学与工程学院李毅超、曹跃、王钰等三位老师共同负责翻译的，最后由李毅超和曹跃统校全稿。参加本书翻译工作的实验室研究生有李晓冬、梁晓、崔甲、何子昂、周梅、刘洋等，在此特别感谢他们为本书大量实验的验证和书稿翻译所做的贡献。本书还得到电子科技大学本科教学实验建设项目基金和电子科技大学精品课程建设项目基金的支持，特此鸣谢！限于水平和经验，译文中欠妥之处，敬请读者批评指正。

前　言

本书简介

本书通过简洁、易懂的描述和生动的实例，将一种积极主动的方式引入计算机网络的教学当中。本书可以作为主教材与课堂材料配套使用，也可以作为辅助教材提供课外实验。同时，本书也是计算机专业人员非常理想的自学指导材料。事实上，这本书可以帮助任何一位对网络有兴趣的读者了解他们每天都在使用的网络的内部秘密，从而成为一名知识丰富的网络使用者。

本书由一系列的实验组成，每个实验都分析了对实际网络活动的跟踪记录。重要的概念都是放到现实场景的实际跟踪（trace）中进行讲解的。读者能够以一种最佳的方式——在实践中观察来学习网络协议的细节。

书中精选的实例能够使读者更加清楚网络协议与现实生活的联系。例如，安全问题在整本书中的地位非常突出。读者将了解到在线浏览网站或购物时，在网络上会传送些什么信息。他们也可以了解到，未使用 WEP 的家庭无线网络会如何暴露给驾车经过的其他人。这些以及更多具体的例子可以帮助读者弄清如何保护他们的网络免受攻击。

对于所有学习计算机网络的人来说，本书将帮助他们通过实践而不是简单地听课来学习网络知识。本书已经在本科生和硕士生的计算机网络课程中得到运用，而且还成功地运用于高中生的短期课程中。同时它还能用作网络课程的配套教材，可以根据计算机科学专业的电子及计算机工程专业以及管理专业学生的不同需要进行调整。学生可以把它作为课程自学的基础，而专业人士则可以通过它来进一步提高计算机网络知识水平。我们真诚地希望这些实验可以使计算机网络知识变得更加生动有趣。

如何使用本书和下载资源

分组跟踪文件

本书基于这样一个前提——学习计算机网络的最好方法是在实践中进行观察。书中每一个实验都附带了一个或几个分组跟踪文件，读者可以借此进行实践。为了更好地理解本书相应内容，读者应当在讨论这些跟踪文件时将它们打开。讨论一个新的跟踪文件时，左边的图标总是会出现在相应段落的左边，相应段落中会给出跟踪文件的名字（如 **exampleFileName.cap**）。

这些跟踪文件可以在下载资源[1] 中找到。从目录中选择当前正在阅读的实验的名字，即可看到在这个实验中涉及的所有跟踪文件的列表。

这些跟踪文件使用的是一种标准的分组捕获格式，读者可以使用不同的网络分析工具来阅读。本书中使用的是 Ethereal 这个开源软件，它具有易操作的图形界面，同时适用于不同的平台，包括 Windows、Linux 和 Solaris。

第 1 章讨论 Ethereal 中捕获分组的基础知识。在开始这一部分之前，我们首先要提醒读者必须先在本地主机上安装 Ethereal。读者可以从 http://www.ethereal.com/download.html 上下载 Ethereal 的最新版本。我们在下载资源中包括了一个运行在 Windows 平台上的 Ethereal 安装软件。

除了我们提供的跟踪记录以外，读者可能还想捕获自己的网络活动的其他跟踪记录。观察自己捕获的跟踪，了解自己所处网络的特性当然有趣。我们鼓励读者这么做，但是熟悉所在网络的管理员对网络规则的设置非常重要。例如，捕获分组通常在共享的校园网中是被禁止的。当做本书上的实验时读者会更加明白这是为什么。

本书结构

本书分成6 章：其中第1 章讲述了使用Ethereal 进行网络跟踪所需的基础知识，中间4 章分别讲述了网络协议栈的每一层（应用层、传输层、网络层和数据链路层），最后一章着重讲解了安全问题。

这些实验是以自顶向下的形式组织的，但是我们做了特殊安排，使它们也适合用于以自底向上的方式介绍协议栈的课程。在图 1 中介绍了两种使用本书的方法。无论使用哪种方法，我们建议读者最好从第 1 章开始，最后讲述第 6 章。同时建议每一章中的实验也能按照顺序完成。

在每个实验开始时首先介绍它所涉及的背景知识，因此本书可以当作一系列独立的实验来使用，也可以用作传统计算机网络课程的配套教材。

“简介”的后面是“配置”部分。在这里将描述在捕获跟踪记录之前应当如何安装相应的硬件和软件。即使读者并没有自己捕获跟踪记录，这里仍然为此提供了足够的信息。这一部分一般都包括一个网络图。

接下来就是“实验”部分。这是实验中内容最多的一部分。在这一部分，将讲解如何进行跟踪，并按步骤地叙述如何对跟踪进行初步分析。在每一个实验中，我们会要求读者从下载资源中打开跟踪记录并一步一步地往下进行。虽然可以只阅读文字而不动手，但是如果能按照指导动手实践，将会学到更多东西。这部分将通过一些使用 Ethereal 的截屏来分析跟踪过程的各个方面。

再后面的部分是一些相关的“问题”。一些问题可以通过阅读实验来回答，一些问题要求从下载资源中打开跟踪记录并进行分析，其他的则要求借助搜索因特网进行研究。需要广泛研究和自由回答的问题被组织到专门的“讨论与研究”部分。

1. 本书原版附有一张配套光盘，其内容可以在 www.turingbook.com 网站本书网页上直接下载。下文中凡是涉及“附带 CD”的地方均已相应改为“下载资源”。——编者注

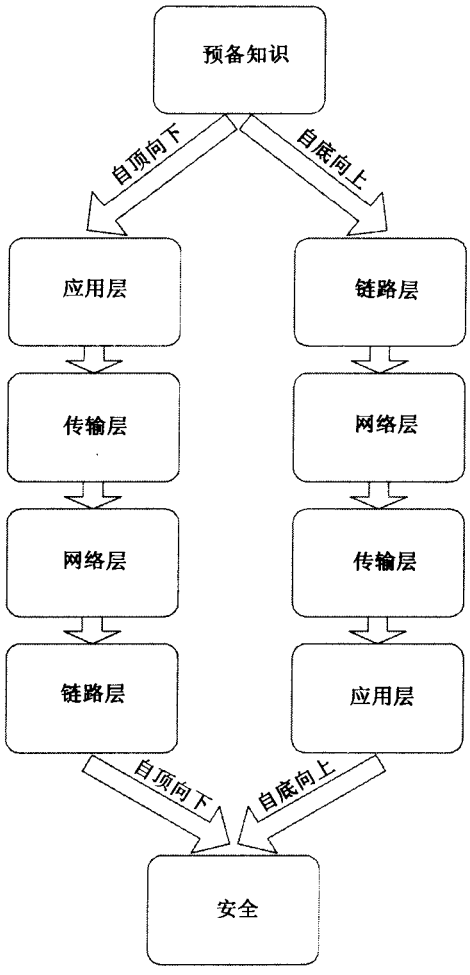

图 1　两种使用方法

每个实验的最后一部分是“参考资源”。它包括一系列的在线资料，这些资料对以后的网络学习将是十分有帮助的。在某些情况下，我们提供了具体的 URL，在有些情况下还详细给出了一系列值得推荐的检索关键词，可以通过搜索引擎进行搜索。我们鼓励大家尽可能多地参考这些资源。读者从本书或任何网络相关课程所获得的最重要的东西，是深刻理解如何使用在线资源来回答并解决所遇到问题。我们当然也鼓励大家从因特网上搜索更多的信息。大量有用的信息可以使读者对计算机网络的学习更加清晰并得到提高。

下载资源包括每个实验的实际跟踪以及 Ethereal 软件的源代码和二进制可执行文件。专为教师提供的教辅材料中还包括了许多问题的答案。

编写本书的原因

作为一名计算机网络教师，我一直在寻找一种高效而易于管理的方式为学生提供动手实验。刚开始，我认为需要一个拥有全套网络设备的实验室，因此着手搜集了大量的路由器、

交换机、网络集线器、PC 机，同时找到一个实验室来安置它们。我能够为少数的学生提供很好的学习环境，但无法适应一般班级的规模。配备一个能够容纳整个班级的实验室过于昂贵，并且负责太多的实验将成为实验室管理员的恶梦。即使是仅仅容纳一个小班级的实验室，它也需要花费大量的时间进行维护、升级和管理。

我发现自己面临极为令人不快的抉择——要么采用一种纯授课方式（没有我和学生喜爱的动手实验）来教授计算机网络，要么继续花费大量时间在实验所需设备的资助和管理上。基于这一点，我又仔细地研究了所有的实验。它们几乎每一个都包括 3 个部分：（1）配置硬件和软件，为网络实验做准备；（2）实验并捕获跟踪记录；（3）分析跟踪记录并弄清所发生事件的细节。我幡然省悟，真正地学习大部分是在第 3 步——分析捕获的跟踪记录。

我决定尝试一种新的方式，即向学生详细地叙述实验的过程，然后将实验中的跟踪进行分类分析。尝试的结果让我感到十分兴奋。我可以只用一套简单的网络设备来进行分组的跟踪记录捕获。在写习题答案提示时可以只用具体分组的编号，因为所有的学生看到的都是相同的跟踪记录。即使是那些对学生搜集分组跟踪非常敏感的校园网的系统管理员同样会很高兴，因为我搜集和交给学生的都是我自己的跟踪记录。

我已经在大规模班级（150 人）和小规模班级（10 人）里测试了这种方法。同时将它运用在规模较小的学校（Clarkson，3000 名学生）和规模较大的学校康奈尔大学（Cornell，20 000名学生）。我已经将它成功地运用在研究生的网络教学以及高中生的短期网络培训课程中。我发现这种方法能够解决 95% 的令人头痛的麻烦。

学生一般都反映：基于网络跟踪的动手实验是网络课中最有趣的部分，帮助他们加深了对课堂内容的理解。他们说这种作业方式激发了自己去做进一步研究，从而帮助理解跟踪记录的每一个细节。学生常常带着他们自己的跟踪记录来问我他们发现的精彩深入的问题。

当我将这种方法运用在网络教学中时，我发现尽管需要做的工作（捕获跟踪记录、描述实验的步骤、列出问题及答案等）比起维护一个实验室要简单得多，但仍然相当花费时间。例如，在实际过程中，当我将结果在线发送给学生时，确定这些跟踪记录中没有捕获任何不能公开的私有数据就可能是件棘手的事。因此我决定写一本书，为其他希望为计算机网络课程增加动手实验的老师扫清障碍。本书及下载资源就是最终成果。

联系作者

希望读者能认识到这本书是一种为计算机网络学习增加有趣的动手实验的简易方法。我们也乐意听到读者在常规课程或自学过程中使用这些实验的感受。非常欢迎读者将对本书的评论和建议发送给作者：

Dr. Jeanna Matthews
8 Clarkson Avenue，MS 5815
Potsdam，NY 13699
jnm@ clarkson. edu

致　谢

我要感激所有对本书的出版做出贡献的人。感谢本书的第一位编辑 Paul Crokett 给予我的信任以及使本书得以出版所给予的帮助。我还要感谢高级编辑助理 Simon Durkin 对本书的贡献。执行编辑 Bill Zobrist 负责本书的最后修改并在介绍性内容方面提出了许多有用的建议。高级编辑助理 Bridget Morrisey 负责下载资源的制作。高级产品编辑 Lisa Wasserman 负责了本书的编辑和校对工作。

我还要感谢我的丈夫 Leonard Matthews 在整个写作过程中给予我的宽容和支持，同时感谢我的孩子 Robert 和 Abigail 给予我大量的时间去工作。

通过多年的计算机网络的教学工作，我开发了一系列的实验从而形成了本书。在我的课堂上许多学生已经完成了同样的实验，并且他们对所有的实验的反馈对于本书的编写是极有价值的。我要感谢提出新的问题、建议新的实验、为问题做出不同正确答案的每一位同学。

我想特别提出一些学生的名字：Niranjan Srinivasan、Chong-Suk Yoon、Dachao Wang、Nidthida Perm-Ajchariyawong 以及 Tingyan Yuan，他们帮我收集整理了本书最初的一部分实验。Eric Kobelski 和 Scott Mead 收集了无线和 FDDI（光纤分布式数据接口）的跟踪记录。Steve Evanchik 收集了 SMTP 和 POP 的跟踪记录。Kandiah Mathavan、Eric Kobelski、Scott Mead、Jason Herne 和 Nate Dudek 帮助我捕获了 EIGRP 和 BGP 跟踪记录。Todd Deshane、Anthony Peltz 和 Tim Fanelli 允许我访问他们管理的几台计算机。Leslie Cherian 帮助我完成了本书的索引。

Clarkson 大学 2004 年春季学期 CS 454/554 课程的学生对本书的 Beta 版提供了极好的反馈。特别是 Patty Jablonski，他进行了详细的记录，对修改许多错误起到了很大的作用。Eli Dow、Dalia Solomon、Corey Girard、Creighton Long 和 Tim Fanelli 也提出了许多有用的建议。

同时还要感谢 Ethereal 的开发者们，是他们为计算机网络探索提供了这样一个理想的工具，还将其作为一个开源软件提供给大家使用。

目　录

第1章 预备知识

引言

贯穿全书，将通过观察网络活动跟踪记录来学习因特网所基于的网络协议。为此我们需要使用 Ethereal 这个开源网络协议分析器。这一章将为读者开始下面的学习做好充分准备。

我们从用 Ethereal 来捕获和观察一个很短的轻流量网络跟踪的实验开始。这个实验会介绍一些 Ethereal 的基本功能。

掌握了 Ethereal 的基础知识后，我们将转移到因特网分层协议栈的概述上来。本书的后几章将主要聚焦在每层的具体细节上。但是本章中的概述对理解每一层所处的大背景仍然是非常必要的。

本章中的第三个实验观察一个涉及多个网络活动的复杂网络。它将告诉你如何使用过滤器来定义和理解每个单独的网络活动。

实验 1.1　用 Ethereal 来观察一个轻流量网络

简介

如果使用 Web 浏览器或电子邮件客户端这样的网络软件，必须有网络连接才可能工作。然而，你知道它们在因特网上传送的是什么类型的信息吗？例如，计算机要对远程 Web 服务器发送什么来获取网页呢？计算机如何将邮件发给指定的人呢？

你可以通过使用网络协议分析器来观察网络会话的细节。网络协议分析器是一个能记录所有网络分组并且以人们可读的形式显示的软件。在重流量网络中，信息量可能是非常大的，因此网络协议分析器能够提供所有分组的统计概要，并且允许用户过滤掉不想要的分组或查找出感兴趣的特定分组。

在这本书里，我们将使用一个叫做 Ethereal 的开源网络协议分析器。在本章里我们将会对 Ethereal 做一个基础的介绍。掌握了 Ethereal 的基础知识之后，我们可以用它作为工具来对网络协议（如 HTTP、SMTP、TCP、UDP、IP 和一些其他协议）的细节进行探讨。

如果能在本机上安装 Ethereal 并且按照指示进行每个实验，你将从每个实验中学到更多知识。Ethereal 可以在多种系统平台上运行，包括 Windows、Mac 和 Unix/Linux。在下载资源中还有一些源代码和二进制代码。你也可以直接从 Ethereal 的网页 http://www. Ethereal. com 下载其最新版本。下载资源的版本中使用的对话框和书中使用的对话框相对应。但如果你使用的是更新的版本，这些对话框可能会略有不同。

在第一个实验中，我们将观察一个从“轻流量网络”捕获的分组跟踪。我们将为你展示如何捕获自己的分组跟踪记录（在你的局域网上允许进行该实验的情况下）。我们还会说明如何在跟踪中观察每个分组的细节，以及如何查看整个跟踪记录的统计概要。

配置

本书的每个实验都会从描述实验运行的网络配置开始。本实验是在私有家庭网络环境中进行的。一台运行 Windows 的 PC 连接到线缆调制解调路由器。在开始实验之前，所有使用网络的应用程序（Web 浏览器、电子邮件客户端）都已关闭。实验配置如图 1. 1. 1 所示。

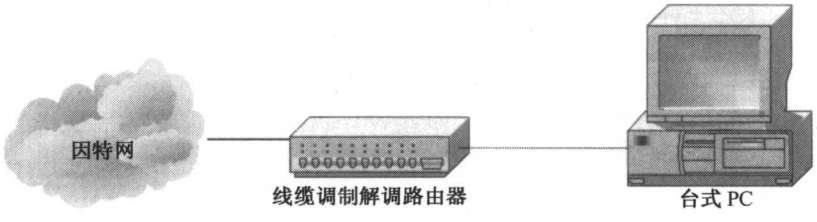

图 1. 1. 1　实验配置

实验

首先启动 Ethereal。要想捕获一个跟踪记录，我们从 Capture（捕获）菜单中选择 Start，并用 Capture Options（捕获选项）对话框来指定跟踪记录的各个方面。图 1.1.2 和图 1.1.3 所示为 Capture 菜单和 Capture Options 对话框。

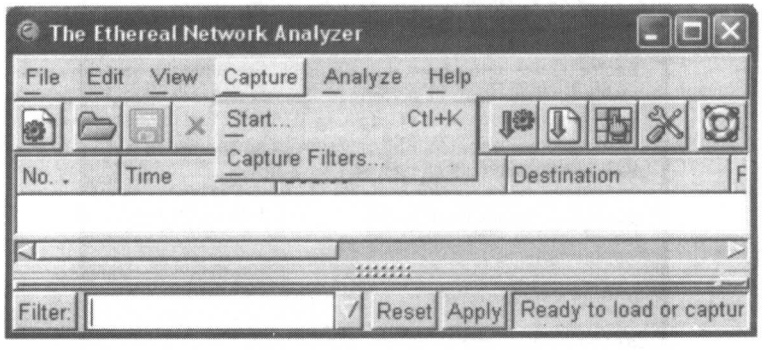

图 1.1.2　Capture 菜单

使用 Capture Options 对话框

在本实验中我们不会用到 Capture Options 对话框中的所有选项，但对它的每个选项我们都给出一个简要的介绍。

1. Interface（接口）和 Link-layer header type（链路层首部）类型

在接口下拉菜单中，可以选择跟踪所用的接口。例如，如果机器同时拥有以太网接口和无线网络接口，你必须选择其中一个进行监测。如果选择以太网接口，将只记录那些通过非无线网络传输的通信。进行捕获时，如果发现没有通信或是所获得的通信不符合期望，那么就可能需要选择另一个网络接口了。

链路层首部类型字段说明了 Ethereal 将如何解释该链路层的帧。这也与接口的类型有关。

2. Limit each packet to *N* bytes（将每个分组限制在 *N* 个字节内）

Ethereal 能够捕获整个分组——数据和首部。典型情况下，数据会占据大多数的空间，但是通常首部包含了最有用的信息（源地址、目的地址、分组的类型等）。如果不打算观察数据，那么可以只捕获首部以节省空间。为此，需要计算出感兴趣的首部的最大字节长度，然后使用该最大长度来捕获每个分组中的这一部分。

3. Capture packets in promiscuous mode（在混杂模式下捕获分组）

如果你的计算机在一个共享网段上，诸如一个无线局域网或者一个以太网集线器上，那么网络接口将能探测到所有的分组，包括那些发到其他机器上的分组。但是，更多的情况是，目的地为其他计算机的分组将被忽略掉。如果你的网络接口设置为“混杂模式”（Promiscuous mode），它将记录下所有的分组，包括那些并非发往你的机器的分组。要想把网络接口设置为混杂模式，需要对这台计算机具有管理员特权。

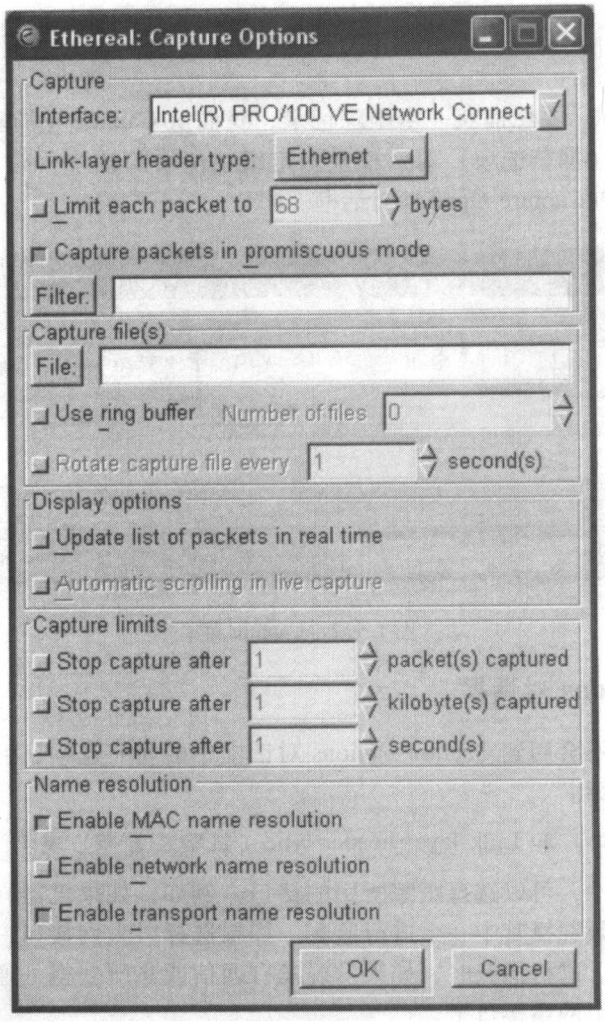

图 1.1.3　Capture Options 对话框

在混杂模式下从一个共享网段上捕获分组的时候，可能会捕获到一些由其他人发送的敏感信息。因此，在混杂模式下，捕获分组之前，必须获得网络管理员的允许或是网络用户的同意。许多公司和大学都严禁对其网络进行跟踪。

在本书的每个实验里，我们都会给出已捕获的跟踪记录以供分析。你可以自由地打开这些跟踪记录而不需要任何特殊权限。

5~6

4. Filter（过滤器）

可以指定一个捕获过滤器（filter）来限制捕获的数据量。只有那些匹配过滤规则的分组才会被记录。例如，你可以用下面的过滤器来捕获那些只从 IP 地址 192.168.0.1 发出和发往它的分组：`host 192.168.0.1`。Ethereal 过滤器功能很强，但是需要学习一种简单的过滤语言。