信息安全技术丛书

WIRESHARK

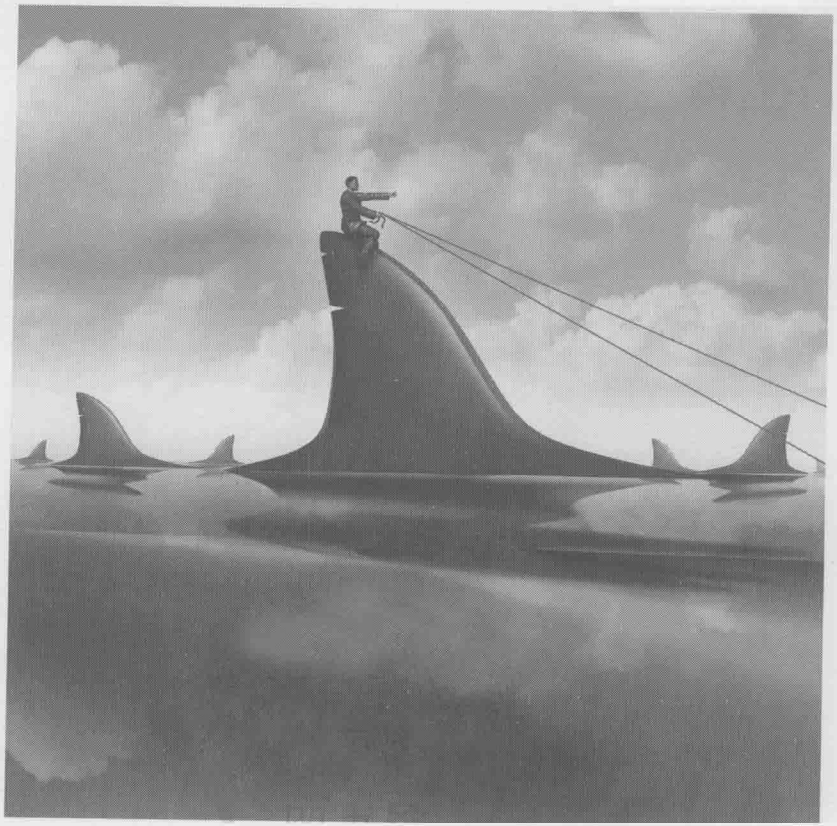
Life is tough,
But wireshark makes it easy.

Wireshark
网络分析就这么简单

林沛满 著

人民邮电出版社
POSTS & TELECOM PRESS

信息安全技术丛书



Wireshark
网络分析就这么简单

林沛满 著

人民邮电出版社

图书在版编目（CIP）数据

Wireshark 网络分析就这么简单 / 林沛满著. -- 北京 : 人民邮电出版社, 2014.12
ISBN 978-7-115-36661-0

Ⅰ. ①W… Ⅱ. ①林… Ⅲ. ①计算机网络－网络分析－应用软件 Ⅳ. ①TP393.02

中国版本图书馆CIP数据核字(2014)第226824号

◆ 著　　林沛满
责任编辑　傅道坤
责任印制　彭志环　焦志炜
◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京艺辉印刷有限公司印刷
◆ 开本：800×1000　1/16
印张：12
字数：218 千字　　2014 年 12 月第 1 版
印数：1－4 000 册　　2014 年 12 月北京第 1 次印刷

定价：39.00 元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315

内容提要

Wireshark 可能是世界上最好的开源网络包分析器，能在多种平台上（比如 Windows、Linux 和 Mac）抓取和分析网络包，在 IT 业界有着广泛的应用。

本书采用诙谐风趣的手法，由浅入深地用 Wireshark 分析了常见的网络协议，读者在学习 Wireshark 的同时，也会在不知不觉中理解这些协议。作者还通过身边发生的一些真实案例，分享了 Wireshark 的实战技巧。

本书不务虚，不注水，几乎页页干货，篇篇精华，力求为读者提供最佳阅读体验，使读者在一个轻松愉悦的阅读氛围中，潜移默化地掌握 Wireshark 的使用技巧和网络知识，为你的工程师生涯加油助力。

无论你是技术支持工程师、系统管理员、现场工程师、公司 IT 部门的老好人，还是高校网络相关专业的教师，无论你是 CCNA、CCNP、CCIE，还是 MCSE，本书都是迅速了解、掌握 Wireshark 技巧的绝佳读物。

关于作者

林沛满，2005 年毕业于上海交通大学，现任 EMC 网络存储部门的主任工程师。多年来为多个产品团队提供过技术咨询，范围包括网络、操作系统、文件系统和域等，这就是本书所涵盖的协议如此五花八门的原因。每年临近加薪的日子，他也会组织一些技术培训来提醒上司。本书的部分内容就来自这些培训资料。

平时他也写一些技术博客，你或许还能在 IT168 或者 ChinaUnix 技术社区看到它们。本书也有少数内容来自这些博客。

当林先生不在工作时，大部分时间都花在了园艺花卉上，尤其是欧洲月季。

致　谢

感谢很多人对本书的付出。

历城路幼儿园的林小满同学几乎每次邀请爸爸捉迷藏时都失望而归，因为写作本书的时间都被安排在下班后。爸爸会一直记得你期待的眼神和失望时撅起的小嘴。

来自摩根的曹若沈女士帮我弥补了所有的亲子时间，并且在百忙之中检查了每篇草稿。我就算包揽下一年的洗碗工作也难以回报。

来自 EMC、微软和思科等单位的多位朋友审阅了本书的大多数内容，尤其是我的同事赖苏成一个人完成了所有关于 TCP 的部分的审阅。赖先生是一位精通外文的网络专家，在削球技术上也造诣颇深，有意结识这位青年才俊的妹子可以向我索取手机号码。

最后，要感谢 EMC 公司提供了最顶级的网络、VMware 和存储空间，使我能够快速地搭建本书所需要的实验环境。

前　言

几个月前和老同学聚餐，席间有位经理说，“最近招了个不错的工程师，居然懂Wireshark。”我刚想科普一下 Wireshark 是什么，就听见另一位表示羡慕，说自己也在寻觅这样的人才。这时候我才意识到，原来 Wireshark 的市场需求已经这么大了。

当然，对我这样的 Wireshark 老粉丝来说，也不会感到很意外。随着互联网的井喷式发展，现代人的生活越来越依赖于网络，很多人开玩笑说 WiFi 也要列入马斯洛需求模型的最底层了。从事网络工作的技术人员自然也承受着从未有过的压力，比如每次促销对于电商都是极大的考验。而 Wireshark 正好是解决网络问题的利器，当我们透过它来看网络时，看到的不再是没有意义的“0”和“1”，而是人人都能理解的语句；由于它支持成百上千的协议，所以我们几乎可以看到网络上的一切，解决起问题自然也更得心应手。不久前我为一家电商做过系统调优，就是基于 Wireshark 的分析结果。

这便是我决定写作本书的原因，这么好的工具应该为更多人所用。本书先带你认识 Wireshark，学会使用它的技巧；然后利用 Wireshark 剖析一些常用的网络协议，相信有一些是你所需要的；最后分享了我用 Wireshark 处理过的几个经典案例，希望对你的工作有所帮助，能起到举一反三的效果。

本书组织结构

有别于网络教材，本书并不从 TCP/IP 的底层讲到顶层，而是采用了从简单到复杂的顺序。全书共分为 3 部分。

第 1 部分“初试锋芒”，先从一道经典的面试题讲起，带你体验 Wireshark 的魅力。接下来两篇是简单的应用实例，分析了服务器失去连接的原因，以及 Excel 程序保存文件的过程。再往下就是该部分最有价值的文章——“你一定会喜欢的技巧”，分享了很多实用窍门。最后的两篇小文章无关技术，分别讲述了 Wireshark 的前世今

生和一位网络高手的故事。这一部分内容相对简单，可以较快阅读。

第 2 部分“庖丁解牛”，用 Wireshark 剖析了很多协议，比如 DNS、TCP、FTP、HTTP 和 NFS 等。有些协议非常复杂，比如用于身份认证的 Kerberos，建议读者学习此类内容时放慢阅读速度，仔细领略其分析技巧。好在应用层协议相对独立，所以当你遇到一个不感兴趣的协议时，直接跳过也无妨。也有些协议相对简单，比如 DNS，可能书中的内容你本来就懂了。不过再简单的协议也有值得研究之处，比如你之前可能没有意识到，DNS 查询在基于 TCP 时效率有多低。这一部分还介绍了 Linux 和 Windows 上的一些小 bug，它们居然在最流行的操作系统上存在了多年而没有被发现。总体而言，这一部分的内容庞杂繁复，需要读者花费最多的时间来阅读。

第 3 部分“举重若轻”，分享了一些用 Wireshark 解决的真实案例，其中大部分是关于性能的，因为性能问题最为棘手。研究这些案例不一定对工作有直接帮助，因为遇到相同症状的概率不高，但是用 Wireshark 解决问题的思路都是相通的，相信读者可以起到触类旁通的效果。我们也许可以在几个小时里学会使用 Wireshark 软件，在几天里学会一个协议，但是思路的养成却需要经年累月的锻炼。最隐蔽的问题往往在网络包中看不到蛛丝马迹，我们不得不用推理、联想甚至发散的思维来寻找原因。希望通过这些案例，有助于读者们形成这种思维习惯。

本书每部分的结尾都有一篇非技术文章，它或者是行业趣闻，或者是本人的工作感触，希望能增加读者的阅读乐趣。

你想知道的一些问题

1. Wireshark 是什么？

Wireshark 是最流行的网络嗅探器之一，能在多种平台上抓取和分析网络包，比如 Windows、Linux 和 Mac 等。它的图形界面非常友好，但如果你觉得鼠标操作不够有腔调，也可以使用它的命令行形式——TShark。

2. 学习 Wireshark 有何意义？

很显然，Wireshark 并不能帮我们变成网络新贵，但它对技术上有所追求的工

程师来说，有着金钱难以衡量的价值。用它来辅助学习，可以更深入地理解网络协议；用它来排查故障，可以更快地发现问题。假如你是团队中唯一掌握 Wireshark 的网络工程师，这个看家本领非常有助于你保持大牛地位。在同事们手足无措时，你可以用最快的速度摆平，然后平静地说一句："问题解决了，我先去泡杯咖啡。"接下来就可以离开座位，让他们一脸崇拜地研究你满是 TShark 命令的屏幕了。

3. 为什么要写作本书？

Wireshark 本身是免费的，在我们心存感激的同时，也注意到一些需要花大钱的地方——Wireshark University 的 5 天培训费为 3395 美金，而且没有在中国开课。对于大多数中国工程师来说，唯一的途径就是自学，这便是我写作本书的原因。

与其他网络图书不同，本书舍弃了公式和协议的条条框框，借助 Wireshark 直观地显示网络细节，让原本拒人千里的协议鲜活地呈现出来。你只需稍加思考，相信很多原来的难点都可以迎刃而解。书中用 Wireshark 解决的几个问题，也全部源于真实案例，很可能会在工作中遇到。

4. 本书适合哪些读者？

如果你是公司 IT 门部的老好人，常常有同事咨询各种疑难杂症，那你适合阅读本书。从 ping 不通主机到访问不了共享目录，都有活生生的例子，比如第 1 部分的《从一道面试题开始说起》和《初试牛刀：一个简单的应用实例》。

如果你是技术支持工程师，每天被客户当作出气筒，本书简直就是为你而作。下次就发个 Wireshark 截屏给客户，"看，明明是你们自己的 VLAN 配错了，当然连不上！"

如果你是数据中心的管理员，不时要跟习惯推卸责任的网管吵架，也请阅读本书。它将演示如何通过抓到的包推出网络状况，甚至算出 TCP 拥塞窗口。如果那些网管员问你是怎么算的，你只需低调地掏出本书，让他们看到发黄的纸张和印着咖啡渍的封面即可。

如果你在现场实施项目，常被好客的甲方挽留到深夜，请携带本书。本出第 3 部

分的几篇现场调优案例，说不定会给你带来共鸣。

如果你是高校网络相关专业的一名伟大的人民教师，常因准备课件而发愁，也建议参考本书。上课时打开 Wireshark，也许比精美的课件更受学生欢迎。

其他职业的读者请酌情参考上面内容。但如果你是一名神秘的黑客，我不得不直言相告：虽然 Wireshark 能解析网络包，却不能帮你在肉鸡上抓包，所以本书作用有限。虽然《首席信息安全官必须知道的五大黑客工具》之类的高大上文章会把 Wireshark 列进黑客软件，但是众所周知，头衔上包含“首席”二字的人已经不会亲自使用这些工具。

5. 阅读本书需要什么基础？

要想阅读本书，你需要具备基本的网络知识，比如在学校里上过网络课，或者学习过 CCNA 的培训资料。对于缺乏网络基础的 Wireshark 用户，建议先阅读一本较成系统的教材，个人推荐 Richard Stevens 的《TCP/IP 详解卷 1：协议》。搭上《颈椎病防治一本通》也许还能免运费，前一本有助于你更快地学会 Wireshark，后一本则能在学会 Wireshark 之后治疗职业病。

由于本书涵盖了很多协议，所以每位读者都可能会遇到完全陌生的内容。好在大多协议都相对独立，所以实在看不懂的部分也可以跳过。举个例子，假如你的工作与 Kerberos 毫无关系，那么看不懂也没必要强求，毕竟学起来颇费心血。

6. 对阅读本书有何建议？

本书有别于大部头的网络百科全书，所以无论你在车上还是如厕时皆可轻松阅读。但有部分内容可能需要你放慢速度，甚至多读几遍才能理解。有个实验环境是最好的，可以自己抓些网络包对照学习。技术类知识就是这样，如果你从最简单的地方开始动手操作，接下来就如鱼得水；如果从一开始只依靠冥想，到后面就会走火入魔。

7. 还有什么要对读者说的？

我心目中一本好的技术图书应该是内容准确，表达通俗，容易理解的，本书也尽

量追求这几点（相信本书也做到了）。

为了保证内容的准确性，我邀请了一位 Windows 技术支持、一位网络存储工程师、两位经验丰富的 CCIE 审阅了初稿的大部分文章。如此兴师动众，是因为同时精通 NFS、Kerberos 和 TCP 等协议的工程师并不多见。即便这样，本书仍可能存在纰漏。如果你在阅读过程中发现了任何问题，欢迎反馈到本人邮箱 linpeiman@hotmail.com。

在通俗与精确之间，本书选择了前者。比如“抓包（packet）”一词本身就不够精确，Wireshark 抓到的应该是帧（frame）。但是出于表达习惯，我并没有改成“抓帧”。又比如对同一个网络分层的称呼，工程师们也有不同的习惯，希望读者能够接受这些“混乱”。

容易理解是最难做到的一点。传说白居易写完一首诗，必定先请不识字的老太婆品鉴，一直要修改到老太婆听懂为止。本书的初稿也邀请了我家的“老太婆”进行试读，基本上她看懂后才敢交稿。当然我家这位“老太婆”在本科阶段学习过网络课程。我有时会在书中用图表、类比和 Wireshark 等方式来反复解释同一知识点，就是为了辅助理解。如果让部分读者感到啰嗦，先在此表示歉意。

目　录

目　录

初试锋芒

1

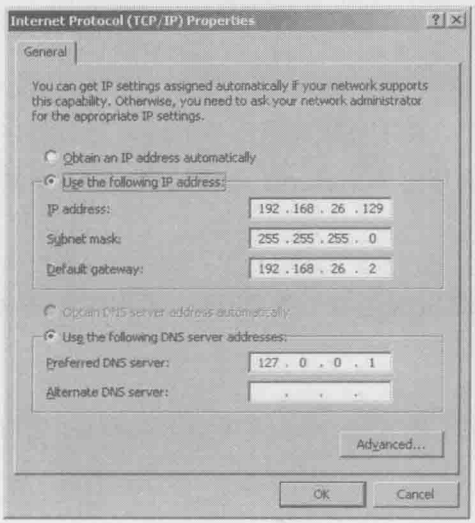
从一道面试题开始说起

我每次当面试官，都要伪装成无所不知的大牛。

这当然是无奈的选择——现在每封简历都那么耀眼，不装一下简直镇不住场面。比如尚未毕业的本科生，早就拿下 CCIE 认证；留欧两年的海归，已然精通英、法、德三门外语；最厉害的一位应聘者，研究生阶段就在国际上首次提出了计算机和生物学的跨界理论……可怜我这个老实人在一开场还能装装，到了技术环节就忍不住提问基础知识，一下子把气氛从学术殿堂拉到建筑工地。不过就是这些最基础的问题，却常常把简历精英们难住。本文要介绍的便是其中的一道。

问题：两台服务器 A 和 B 的网络配置如下（见图 1），B 的子网掩码本应该是 255.255.255.0，被不小心配成了 255.255.255.224。它们还能正常通信吗？

服务器 A：



服务器 B：

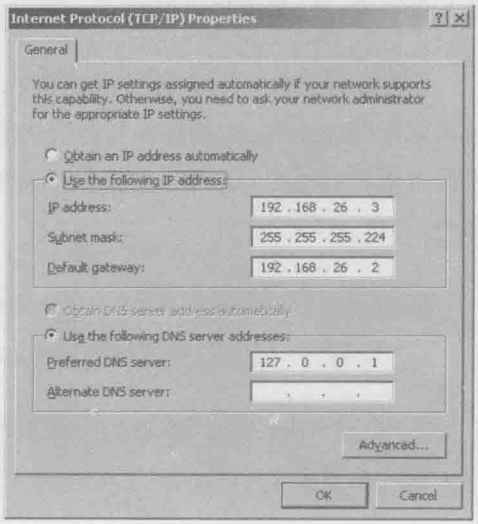


图 1

很多应聘者都会沉思良久（他们一定在心里把我骂了很多遍了），然后给出下面这些形形色色的答案。

答案 1：“A 和 B 不能通信，因为……如果这样都行的话，子网掩码还有什么用？”（这位的反证法听上去很有道理！）

答案 2：“A 和 B 能通信，因为它们可以通过 ARP 广播获得对方的 MAC 地址。”（那子网掩码还有什么用？楼上的反证法用来反驳这位正好。）

答案 3：“A 和 B 能通信，但所有包都要通过默认网关 192.168.26.2 转发。”（请问这么复杂的结果你是怎么想到的？）

答案 4：“A 和 B 不能通信，因为 ARP 不能跨子网。”（这个答案听上去真像是经过认真思考的。）

以上哪个答案是正确的？还是都不正确？如果这是你第一次听到这道题，不妨停下来思考一下。

真相只有一个，应聘者的答案却是五花八门。可见对网络概念的理解不容含糊，否则差之毫厘，谬以千里。要知道，这还只是基本的路由交换知识，假如涉及复杂概念，结果就更不用说了。

问题是即便我们对着教材咬文嚼字，也不一定能悟出正确答案。这个时候，就可以借助 Wireshark 的抓包与分析功能了。我手头就有两台 Windows 服务器，已经按照面试题配好网络。如果你以前没有用过 Wireshark，就开始第一次亲密接触吧。

1. 从 http://www.wireshark.org/download.html 免费下载安装包，并在服务器 B 上装好（把所有可选项都装上）。

2. 启动 Wireshark 软件，单击菜单栏上的 Capture，再单击 Interfaces 按钮（见图 2）。