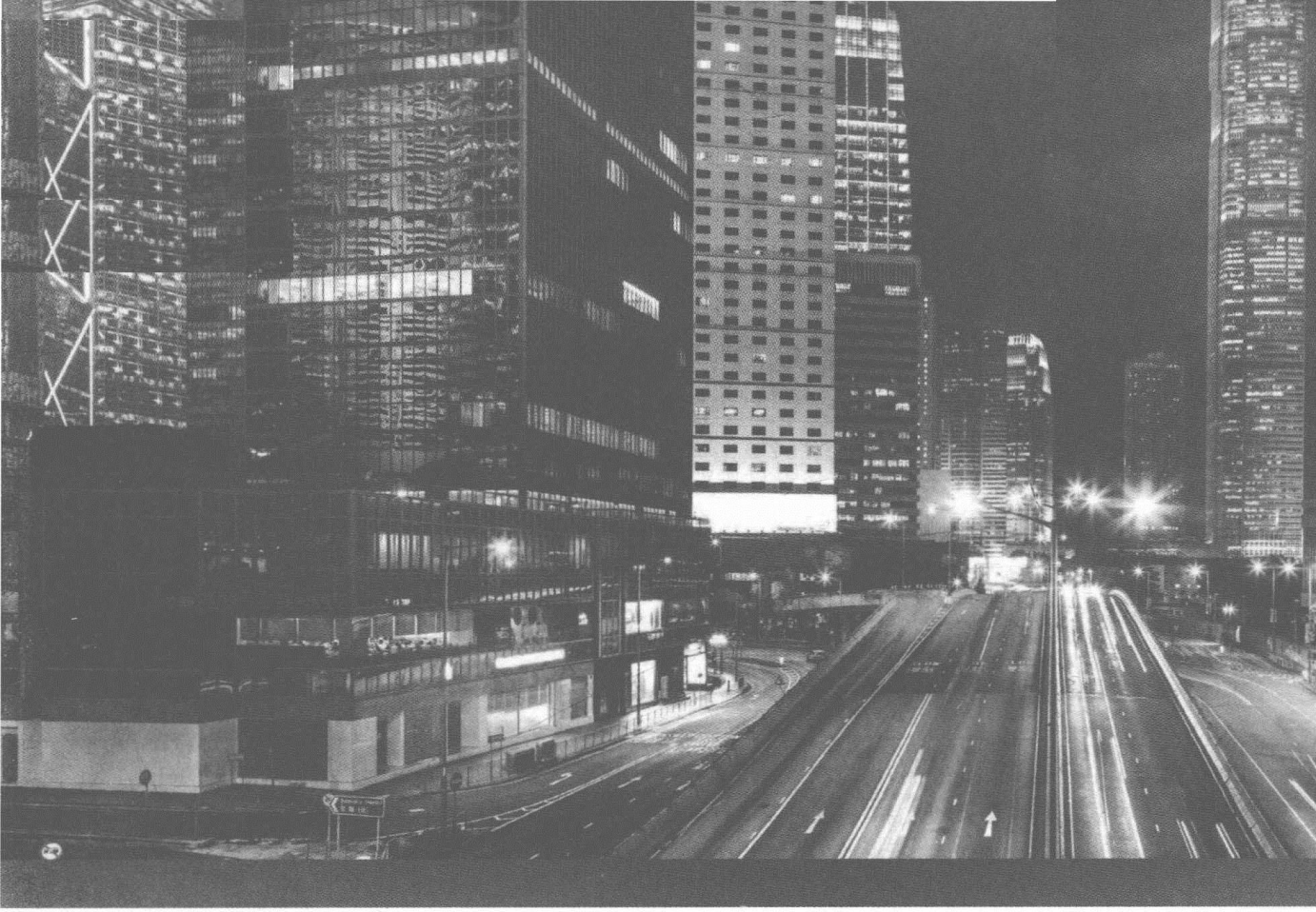
精通Wireshark

Mastering Wireshark

[印度] Charit Mishra 著
YESLAB工作室 译

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS



精通Wireshark

[印度] Charit Mishra 著
YESLAB工作室 译

人民邮电出版社
北京

图书在版编目（CIP）数据

精通Wireshark / (印) 夏里特·米什拉
(Charit Mishra) 著 ; YESLAB工作译. -- 北京 : 人民
邮电出版社, 2017.5
ISBN 978-7-115-44969-6

Ⅰ. ①精… Ⅱ. ①夏… ②Y… Ⅲ. ①计算机网络－通
信协议 Ⅳ. ①TN915.04

中国版本图书馆CIP数据核字(2017)第041412号

版权声明

◆ 著　[印度] Charit Mishra
译　YESLAB 工作室
责任编辑　傅道坤
责任印制　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
北京天宇星印刷厂印刷

◆ 开本：800×1000　1/16
印张：17.5
字数：247 千字　2017 年 5 月第 1 版
印数：1－2 500 册　2017 年 5 月北京第 1 次印刷

著作权合同登记号　图字：01-2016-6530 号

定价：69.00 元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广字第 8052 号

内容提要

本书按照由浅至深的次序，从网络的基本概念和 Wireshark 的基本界面说起，介绍了在不同环境中使用 Wireshark 解决各类网络中常见问题的方法与技巧。

本书共分为 9 章，涵盖了 Wireshark 数据包分析简介，Wireshark 提供的过滤数据的不同方式，Wireshark 中的高级特性，用 Wireshark 监控应用层协议并分析传输层协议的工作机制，用 Wireshark 分析无线流量，用 Wireshark 分析与网络安全相关的问题，配置 Wireshark 以进行网络排错，Wireshark v2 版本的新增特性等内容。

本书内容实用详尽，贴近真实的网络排错、运维需求，适合网络管理人员、技术支持人员、安全从业人员阅读，还适合高校计算机网络、信息安全专业的师生阅读。

关于作者

Charit Mishra 是一位技术顾问与渗透测试专家，供职于全球顶尖的咨询公司 Protiviti。他的工作职责是帮助客户找出网络中的安全漏洞，他无比热爱自己的这份工作。他凭借自己在安全方面的实践经验考取了大量顶级行业认证，如 OSCP、CEH、CompTIA Security+和 CCNA R&S。此外，他也拥有计算机科学领域的硕士学位。他曾经在各类学术会议和民间组织中就信息安全与渗透测试发表过专业演讲。读者可以通过 LinkedIn（https://ae.linkedin.com/in/charitmishra）和 Twitter（@charit0819）来与他取得联系。

首先，我要对挚爱的双亲和姐姐 Ayushi 表达自己最深的谢意。他们对我无条件的支持、他们在我人生重大抉择时期为我提供的专业指导意见，以及他们给予我的理解与鼓励，成就了我的一切。若没有他们的智慧与建议，我如今的一切成就皆为梦呓。

我也要感谢我的挚友和导师 Piyush Verma 先生，感谢他给予我的信任，以及在我迷茫时给予我的引导。我还要感谢我的好友们，尤其要感谢 Siddarth Pandey 先生、Arham Husain 先生、Bharath Methari 先生、Dileep Mishra 先生和我在巴基斯坦的至交 Haider Ali Chughtai 先生。我的一切成就离不开他们共同的帮助与激励。如果我忘记提到哪位朋友，在此表示歉意。

最后，我要感谢 Packt Publishing 这个卓越的团队，他们对本书出版所提供的支持从未间断。感谢所有参与了本书审校的同仁，你们提升了这本书的质量。

恰如一代宗师斯瓦米·维帷卡南达所言：“如有一日，你顺风顺水，即可断言，前路必为歧途。”

关于审稿人

Anish Nath 经常在 YouTube 上传关于安全技术、黑客技术以及其他云相关技术的视频，读者可以访问 https://goo.gl/sbJkuX 来浏览这些内容。

前言

在我们周围，几乎每台设备都已经与其他设备通过网络连接在了一起。连接的目的或为共享信息，或为给其他设备提供支持。如果头脑中拥有了这样一幅图景，你认为网络中最重要的环节是哪一部分呢？显然，一定不是设备之间的物理连接。

本书的着眼点是如何使用 Wireshark 来理解网络中最常见的异常情况，并对这些情况进行排错。本书有可能是你网络/流量/数据包分析的起点，但你有可能最终会称为这一代人的“救世主”，成为你所在团队的超级英雄，你可以轻松帮助人们解决在网络连接、网络管理和计算机取证等方面遇到的疑难。如果你的日常工作就需要和计算机网络打交道，那么本书可以成为好的开始。本书会从最基本的概念开始说起，循序渐进带领读者进入最有深度的概念。

在本书中，我尽可能涵盖了大家在排错中最有可能会遇到的问题，同时提供了一些上手练习的案例，以便帮助读者更好地掌握这些概念。如果能够掌握数据包分析的方法，读者就可以学会如何一路从应用排错到网络的线缆。本书会告诉读者，如何让网络中流动的数据变得更加容易为我们所理解。在本书中，读者一定会读到一些很有意思的章节，包括如何对缓慢的网络进行排错，如何通过 WiFi 执行数据包分析，如何对恶意软件进行分析。也不要忘记本书在介绍 Wireshark 2.0 时提到的那些特性。祝你排错愉快！

本书组织架构

第 1 章，欢迎来到 Wireshark 数据包分析的世界，会向读者介绍 TCP/IP 模型的基本概念，帮助读者熟悉 Wireshark 的 GUI 界面，以及抓包的示例。在这一章中，读者会学习到如何设置网络分析软件来对网络进行分析。

第 2 章，用 Wireshark 过滤出我们需要的数据，会介绍 Wireshark 提供的两种不同过滤方式，这两种方式分别称为抓包过滤器和显示过滤器。我们在这一章中会介绍如何创建和使用不同的配置文件。读者应该熟悉 Wireshark 提供的丰富界面，并且能够开始抓取自己想要抓到的数据包。

第 3 章，掌握 Wireshark 的高级特性，会帮助读者了解 Wireshark 的 Statistics（统计数据）菜单背后的内容，并且掌握 Wireshark 携带的各种命令行工具的使用方法。读者在这一章中会学习到如何准备各种图标和数据流拓扑，最重要的是，如何成为一名命令行专家。

第 4 章，监控应用层协议，会帮助读者理解并分析各种应用层协议的正常行为和异常行为。在这一章中，我们会简单探讨管理员可以用来理解这些协议行为的方法。我们都已经掌握了一些基本的概念，但是你想过应用层协议出现问题的几率有多大吗？在本章中，你会了解到如何处理应用层协议的问题。

第 5 章，分析传输层协议，会介绍 TCP 和 UDP 协议工作原理，解释它们如何进行通信，它们分别面临着怎样的问题，以及如何使用 Wireshark 来对它们进行分析。读者在这一章要成为传输层的诊断专家，能够轻松找出网络中的常见故障，证明自己的价值。

第 6 章，分析无线流量，会介绍如何对无线流量进行分析，如何找到无线流量中的问题。我会带领读者进入无线协议分析的世界，让读者成为 WiFi“忍者”。

第 7 章，网络安全分析，会向读者展示如何使用 Wireshark 来分析与网络

安全相关的问题，比如恶意软件流量、网络入侵、踩点攻击等。在这一章中，读者会学到如何找出网络安全的异常状态，当场抓住入侵网络的黑客，搞得他们痛哭流涕，体验一把如何解决 CTF 的难题。

第 8 章，排错，会向读者传授如何配置和使用 Wireshark 来对网络进行排错。在这一章中，读者会掌握给各种网络问题（比如网速过慢）进行排错的艺术。读者还会通过最常见的日常案例，学习到如何对网络问题进行排错。

第 9 章，Wireshark v2 简介，会通过一些实践案例，向读者展示 Wireshark 最新版本的一些强大的特性，比如 USBPcap、智能滚动条、图形提升等。

阅读本书的先决条件

你只需要一个可以正常使用的 Wireshark 安装程序，以及对一些网络协议的基本理解。能够大致熟悉一些网络协议会对阅读本书很有帮助，不熟悉也并不影响阅读。

本书的读者对象

你对网络中发生的一切感到好奇吗？在你无法解决网络中发生的故障时，你会感到懊恼吗？如果你对这类问题的答案是肯定的，你就是本书的目标读者。

本书是写给那些对网络和安全技术抱有热情的读者的，这些人应该有兴趣深入理解网络的内部工作方式，希望能够掌握 Wireshark 使用方法，但并不了解这款软件的全部功能。

目录

第 1 章
欢迎来到 Wireshark 数据包分析的世界

在这一章里，我们会介绍 TCP/IP 模型的基本概念，并在帮助读者熟悉 Wireshark GUI 界面的同时，向读者展示一个抓包的实例。在这一章中，读者会学到下列内容：

- 什么是 Wireshark；
- Wireshark 是怎么工作的；
- TCP/IP 模型概述；
- 数据包分析简介；
- 为什么要使用 Wireshark；
- 理解 Wireshark 的 GUI 界面；
- 第一次抓包。

1.1 Wireshark 简介

Wireshark 是最强大的抓包软件之一，这款软件不仅能让系统/网络管理员的工作变得简单轻松，而且可以让传播安全福音的技术群体从中获益。

Wireshark 也称为协议分析软件，它可以帮助 IT 从业者分析网络级别的故障。这种工具在优化网络性能方面也可以发挥重要的作用。

Wireshark 可以对网络数据包进行细致入微地分析，显示出数据包的详细内容，并由技术人员判断这些信息是否满足相关用户的需求。如果你也是每天都要和包交换网络打交道的芸芸众生之一，那么 Wireshark 就是为你量身订制的工具，它可以在你进行各类排错工作时大显身手。

1.2　TCP/IP 模型概述

下面，我们来讨论一下网络领域最重要的话题。要想理解这些技术之间是如何关联起来的，读者就必须理解 TCP/IP 模型的基本概念。即使是计算机世界也需要通过一系列的规则和规范才能完成通信，这就是网络协议的作用之所在了。网络协议的作用正是管理数据包/数据分段/数据帧如何通过主机之间的一条专用通道进行传输。

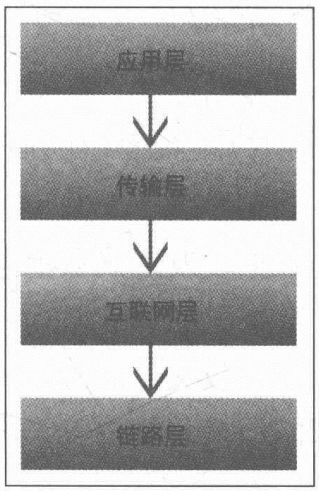
TCP/IP 模型最初称为 DoD 模型，因为这个项目当初是由美国国防部（United States Department of Defense）负责统筹的。TCP/IP 模型涉及当前数据包生命周期的方方面面，它涵盖了数据包在始发节点创建、封装一系列信息（PDU）、逐层进行处理、在网络中准备进行发送、通过中间节点向目的设备路由、通过解封装剔除添加的信息还原为最初的数据包等全部的操作过程。

如果读者对于网络协议的基本概念还感到有些模棱两可，推荐读者先复习一下这些概念，然后再阅读后面的内容，因为阅读本书需要读者对 TCP/UDP 协议相对比较熟悉。在复习之后，读者自己就应该能够想象出上面我们提供的数据包处理过程了。

1.3　TCP/IP 模型的分层

如下所示，TCP/IP 模型中包含了 4 层，每一层均包含了一系列对应的协

议。每个协议都自己的作用，这些协议也都是通过这个模型来对接业界标准的。



第一层是**应用层**，这一层直接和用户及其他网络层协议进行互动；这一层的重点在于将数据通过用户可以理解的方式呈现给用户。应用层也会追踪用户连接的 Web 会话，并且使用一系列的协议帮助应用层连接到 TCP/IP 模型中的其他各层。在本书当中，我们会介绍下面几种非常常用的应用层协议：

- **超文本传输协议（HTTP）；**
- **文件传输协议（FTP）；**
- **简单网络管理协议（SNMP）；**
- **简单邮件传输协议（SMTP）。**

第二次是**传输层**。这一层唯一的作用是创建两台主机通信时使用的套接字（读者应该已经意识到网络套接字对于通信的重要性了），这是在两台设备之间创建出一条独立连接的关键。

两台主机对于同一个通信实例可以建立多条连接，这是将 IP 地址和端口号结合起来实现的。在广域网通信中需要使用 IP 地址（而在局域网通信中，数据传输实际上是通过 MAC 地址来实现的），而一台设备之所以可以与多台设备通过多条信道进行通信，这完全是借助端口号来实现的。除了某些限制

使用的端口号之外，每个系统都可以在通信的过程中使用一个随机的端口号。

这一层也会充当两台主机之间通信的骨干。这一层中最常用的协议是 TCP 和 UDP，它们的概念分别如下所示。

- **TCP：**这是一种面向连接的协议，常常称为可靠协议。首先，这种协议会在两台主机之间创建一条专用的通信信道，然后再开始传输数据。接下来，发送方会通过这条信道发送等分的数据段，而接收方则会针对每个接收到的数据段发送确认消息。一般来说，发送方会等待一段时间，然后再次发送同一个数据段，以确保接收方能够接收这个数据段。比如，在用户下载文件的时候，就是由 TCP 进行管理，并且确保每个比特位都能成功传输的。
- **UDP：**这是一种无连接的协议，术语中常常称之为不可靠通信协议。不过这种协议十分简单，因为它不会创建专用的信道，发送方只负责向目的设备发送数据段，但并不关心接收方是不是接收到了数据。这种通信的形式其实并不会影响通信的质量；因为这种通信形式都满足了发送方向接收方传输数据的需求。比如，当用户在玩局域网游戏时，有几个比特位丢失其实并不会影响用户的游戏体验，因此用户体验也不会因此而降低。

第三层是**互联网层**，这一层关注的重点是数据的往返传输。这一层最主要的协议就是 IP（互联网协议），它同时也是这一层最重要的协议。IP 可以给数据提供路由功能，正是因为 IP 协议提供的路由功能，很多数据包才能最终到达自己的目的地。这一层还包括一些其他的协议，如 ICMP 和 IGMP。

最后一层是**链路层**（这一层常常被人们称为网络接口层），这一层与网络硬件相连。虽然 TCP/IP 协议栈中并没有在这一层定义任何协议，但这一层其实实施了很多协议，如**地址解析协议（ARP）**和**点到点协议（PPP）**。这一层关注的是信息的比特数据如何在物理线缆中进行传输。这一层会建立并终结连接，会将信号由模拟信号转化为数字信号，反之亦然。网桥和交换机这类