信息安全
技术大讲堂

从实践中学习
Wireshark
数据分析

大学霸IT达人◎编著

从理论、应用和实践三个维度讲解Wireshark数据分析的相关知识
通过201个操作实例手把手带领读者从实践中学习Wireshark数据分析技术
涵盖环境搭建、数据捕获、数据处理、数据呈现、数据分析、协议分析……

机械工业出版社
China Machine Press

信息安全
技术大讲堂

从实践中学习
Wireshark
数据分析

大学霸IT达人◎编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

从实践中学习Wireshark数据分析 / 大学霸IT达人编著. —北京：机械工业出版社，2020.1
（信息安全技术大讲堂）

ISBN 978-7-111-64354-8

Ⅰ. 从… Ⅱ. 大… Ⅲ. 计算机网络－网络分析 Ⅳ. TP393.02

中国版本图书馆CIP数据核字（2019）第296877号

从实践中学习 Wireshark 数据分析

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）
责任编辑：欧振旭 李华君 责任校对：姚志娟
印 刷：中国电影出版社印刷厂 版 次：2020 年 1 月第 1 版第 1 次印刷
开 本：186mm × 240mm 1/16 印 张：28.75
书 号：ISBN 978-7-111-64354-8 定 价：129.00 元

客服电话：（010）88361066 88379833 68326294 投稿热线：（010）88379604
华章网站：www.hzbook.com 读者信箱：hzit@hzbook.com

前言

网络日益普及的今天，每秒钟都有海量的数据在网络中进行传输。为了保证数据正确地从源地址发送到目标地址，不同人群为之努力工作。网络程序开发人员分析数据，确认数据正确生成和被处理；网络维护人员分析数据，确保数据的正确传输；网络安全人员分析数据，确保数据没有被截取或伪造。

Wireshark 是一款业界知名的数据捕获和分析工具。它不仅支持几百种网络协议的解析，还提供了大量的分析功能，能满足不同用户的数据分析需求。同时，它提供了丰富的用户接口，允许用户以图形化和命令行等多种方式使用。

本书基于 Wireshark 3，详细讲解了数据抓包和分析的相关技术。书中首先介绍了环境搭建、数据捕获、数据处理和数据呈现；然后详细介绍了数据分析的各种功能和应用技巧，如显示过滤器、分组分析和着色规则等；最后详细介绍了常见网络协议的数据分析方式，包含网络基础协议（ARP、DNS、DHCP）、数据传输协议（TCP、UDP）和高级应用协议（HTTP、SMTP/POP3、SMB）等。

本书有何特色

1. 涵盖Wireshark常用分析功能

由于协议形式众多，使得数据分析是一项复杂度非常高的工作。为了方便用户分析，Wiresahrk 提供了众多的分析功能。本书涵盖了其中常见的各种功能，如捕获过滤器、显示过滤器、专家意见、名称解析、分组标记、数据导出和分组跳转等。

2. 内容实用，可操作性强

Wireshark 提供的每个功能都来源于众多用户的建议，都具有极强的代表性和可操作性。为了方便读者学习和理解，书中介绍了约 200 个操作实例，用于辅助讲解各个知识点。

3. 涵盖重要协议的数据分析

Wireshark 数据分析的最终落脚点是协议，所以本书挑选了最为常见的网络协议数据包进行分析，如 802.11、ARP、DHCP、DNS、TCP、UDP、HTTP、SMTP/POP3、SMB、

TFTP、SCTP 和 FTP 等协议的数据包。

4．环环相扣，逐步讲解

Wireshark 数据分析是一个连贯和完整的过程，从环境准备、数据的获取和保存，到分析手段和具体协议分析，每个阶段环环相扣，逐步推进。本书按照这个顺序，逐层讲解了 Wireshark 数据分析的方式和技巧，以帮助读者最终掌握数据分析的技巧。

5．提供完善的技术支持和售后服务

本书提供了对应的 QQ 群（343867787）供大家交流和讨论学习中遇到的各种问题。同时，本书还提供了专门的售后服务邮箱 hzbook2017@163.com。读者在阅读本书的过程中若有疑问，可以通过该邮箱获得帮助。

本书内容

第 1 章网络数据分析概述，主要介绍了网络数据的传输方式、OSI 模型、TCP/IP 协议族和 Wireshark 软件的获取和安装。

第 2~4 章为网络数据分析的基础，主要介绍了捕获数据、使用过滤器、存储数据、快速分析和数据呈现等内容。

第 5、6 章主要介绍了使用显示过滤器、名称解析、协议解析、数据包分组、分组注释、跳转分析和着色规则等各种数据分析技术。

第 7、8 章主要介绍了无线网络抓包和分析、WEP/WPA 握手包数据分析、无线数据解密及 ARP/DHCP/DNS 数据分析。

第 9~12 章为网络应用协议分析，主要介绍了 TCP 数据分析、UDP 数据分析、HTTP 数据分析和 SMTP/POP3/SMB/TFTP/SCTP/FTP 数据分析。

附录 A 主要介绍了 Wireshark 自带的各种命令行工具，如文件查看工具 capinfos、捕获工具 dumpcap、编辑工具 editcap，以及分析工具 tshark 与 rawshark。

本书配套资源获取方式

本书涉及的工具和软件需要读者自行下载。下载途径有以下几种：

- 根据书中对应章节给出的网址自行下载；
- 加入技术讨论 QQ 群（343867787）获取；
- 登录华章公司网站 www.hzbook.com，在该网站上搜索到本书，然后单击“资料下载”按钮，即可在页面上找到“配书资源”下载链接。

本书内容更新文档获取方式

为了让本书内容紧跟技术的发展和软件更新，我们会对书中的相关内容进行不定期更新，并发布对应的电子文档。需要的读者可以加入 QQ 交流群（343867787）获取，也可以通过华章公司网站上的本书配套资源链接下载。

本书读者对象

- 网络安全和维护人员；
- 渗透测试技术人员；
- 信息安全技术爱好者；
- 网络应用程序开发人员；
- 计算机安全技术自学者；
- 高校相关专业的学生；
- 专业培训机构的学员。

本书阅读建议

- Wireshark 可以自动解析几百种网络协议。为了深入理解和学习网络协议，阅读本书时可以参考丛书中的《从实践中学习 TCP/IP 协议》分册。
- 学习阶段可在不同的网络环境下进行操作与练习，以了解各种网络环境下的数据传输特点和协议包构成的不同之处。
- 由于 Wireshark 会经常更新、增补不同的功能，所以学习时要定期更新工具，以获取更加稳定和强大的功能。

本书作者

本书由大学霸 IT 达人团队编写。感谢在本书编写和出版过程中给予笔者大量帮助的各位编辑！由于作者水平所限，加之写作时间较为仓促，书中可能还存在一些疏漏和不足之处，敬请各位读者批评指正。

编著者

目录

前言

第 1 章　网络数据分析概述 ····· 1

1.1　网络数据传输 ····· 1

1.1.1　网络构成 ····· 1

1.1.2　数据传输 ····· 2

1.1.3　网络类型 ····· 3

1.2　网络协议 ····· 6

1.2.1　OSI 模型 ····· 6

1.2.2　TCP/IP 协议族 ····· 7

1.3　Wireshark 概述 ····· 9

1.3.1　Wireshark 的历史 ····· 9

1.3.2　获取 Wireshark 软件 ····· 10

1.3.3　Windows 系统安装 Wireshark ····· 11

1.3.4　Mac OS 系统安装 Wireshark ····· 16

1.3.5　Linux 系统安装 Wireshark ····· 21

第 2 章　捕获数据包 ····· 22

2.1　指定网络接口 ····· 22

2.1.1　接口种类 ····· 22

2.1.2　选择接口 ····· 24

2.1.3　捕获 USB 设备包 ····· 29

2.2　使用管道接口 ····· 32

2.2.1　添加管道接口 ····· 32

2.2.2　捕获管道接口数据 ····· 34

2.3　远程捕获数据包 ····· 35

2.3.1　管理远程接口 ····· 36

2.3.2　Windows 下配置 rpcapd 服务 ····· 36

2.3.3　Linux 下配置 rpcapd 服务 ····· 41

2.3.4　添加远程接口 ····· 42

2.3.5　实施远程捕获数据包 ····· 44

2.4　使用捕获过滤器 ····· 46

2.4.1　指定捕获过滤器 ····· 46

2.4.2　基于类型过滤 ····· 49

2.4.3　基于传输方向过滤 ····· 51

2.4.4 基于协议过滤……54
2.4.5 基于数据过滤……56
2.4.6 使用多个捕获过滤器……57
2.4.7 使用预置表达式……57
第 3 章 数据处理……60
3.1 保存文件……60
3.1.1 自动保存文件……60
3.1.2 手动保存文件……68
3.2 打开文件……72
3.2.1 打开抓包文件……73
3.2.2 文件属性……76
3.2.3 合并抓包文件……79
3.2.4 导入转储文件……82
3.3 快速分析……86
3.3.1 关联地址……86
3.3.2 协议构成……88
3.3.3 数据包长度……89
3.3.4 数据流量……90
3.3.5 发包统计……95
第 4 章 数据呈现……98
4.1 分组列表……98
4.1.1 默认列……98
4.1.2 编辑现有列……100
4.1.3 添加/删除列……104
4.1.4 隐藏/移动/重排列……112
4.2 分组详情……117
4.2.1 查看方式……117
4.2.2 操作树形结构……118
4.2.3 专家信息……123
4.3 分组字节流……125
4.3.1 数值形式……126
4.3.2 文本形式……129
4.3.3 分析分组字节……131
第 5 章 显示过滤器……133
5.1 基础使用……133
5.1.1 使用显示过滤器……133
5.1.2 获取显示过滤器表达式……136
5.1.3 使用单一显示过滤器……143
5.1.4 使用多个显示过滤器……150

5.1.5 高级过滤器 …… 150
5.2 使用技巧 …… 152
5.2.1 使用显示过滤器按钮 …… 152
5.2.2 使用对话过滤器 …… 157
5.2.3 基于显示过滤器保存 …… 158
5.2.4 使用预置表达式 …… 160
5.2.5 使用宏 …… 162
第 6 章 分析手段 …… 165
6.1 分析分组 …… 165
6.1.1 查找信息 …… 165
6.1.2 复制信息 …… 167
6.2 基于时间分析 …… 173
6.2.1 时间格式 …… 173
6.2.2 设置时间参考 …… 174
6.2.3 修正显示的时间 …… 177
6.3 名称解析 …… 179
6.3.1 MAC 地址解析 …… 179
6.3.2 端口自动解析 …… 182
6.3.3 IP 地址解析 …… 185
6.4 协议解析 …… 186
6.4.1 启用协议 …… 186
6.4.2 指定解析的协议 …… 188
6.5 数据包分组 …… 190
6.5.1 标记分组 …… 191
6.5.2 导出分组结果 …… 194
6.5.3 忽略分组 …… 197
6.6 分组注释 …… 199
6.7 跳转分析 …… 202
6.7.1 顺序跳转 …… 202
6.7.2 指定跳转分组 …… 205
6.7.3 对话内跳转 …… 207
6.7.4 历史记录跳转 …… 208
6.8 着色规则 …… 209
6.8.1 启用着色规则 …… 209
6.8.2 设置着色规则 …… 210
6.8.3 对话着色 …… 214
第 7 章 无线网络抓包和分析 …… 216
7.1 软硬件需求 …… 216
7.1.1 Wireshark 组件需求 …… 216

7.1.2 硬件需求 …… 217
7.2 捕获数据 …… 218
7.2.1 捕获数据包 …… 218
7.2.2 流量基本分析 …… 223
7.2.3 捕获过滤 …… 226
7.3 分析数据 …… 227
7.3.1 常用显示过滤器 …… 227
7.3.2 分析认证方式 …… 229
7.3.3 分析 WEP 握手包 …… 231
7.3.4 分析 WPA 握手包 …… 236
7.4 数据解密 …… 241
7.4.1 WEP 解密 …… 242
7.4.2 WPA 解密 …… 244
7.4.3 永久解密 …… 247
第 8 章 网络基础协议数据包分析 …… 250
8.1 ARP 分析 …… 250
8.1.1 过滤 ARP 包 …… 250
8.1.2 分析 ARP 会话 …… 251
8.1.3 发现 ARP 攻击 …… 254
8.2 DHCP 分析 …… 258
8.2.1 过滤 DHCP 包 …… 258
8.2.2 分析 DHCP 会话 …… 259
8.2.3 数据统计 …… 266
8.3 DNS 分析 …… 267
8.3.1 过滤 DNS 包 …… 268
8.3.2 分析 DNS 会话 …… 269
8.3.3 数据统计 …… 271
第 9 章 TCP 协议数据分析 …… 273
9.1 捕获 TCP 数据包 …… 273
9.1.1 捕获过滤 …… 273
9.1.2 端点分析 …… 274
9.1.3 端口过滤 …… 277
9.2 会话分析 …… 281
9.2.1 会话统计 …… 281
9.2.2 建立连接 …… 285
9.2.3 断开连接 …… 293
9.2.4 防火墙过滤 …… 301
9.3 传输数据分析 …… 303
9.3.1 跟踪流 …… 303

9.3.2 保存流 …… 308
9.3.3 TCP 流图形 …… 309
第 10 章 UDP 协议数据分析 …… 315
10.1 基础分析 …… 315
10.1.1 捕获过滤 …… 315
10.1.2 端点分析 …… 318
10.1.3 会话分析 …… 319
10.2 传输数据分析 …… 323
10.2.1 跟踪流 …… 323
10.2.2 保存流 …… 327
10.2.3 UDP 多播流 …… 328
第 11 章 HTTP 协议数据包分析 …… 332
11.1 过滤数据包 …… 332
11.1.1 捕获过滤 …… 332
11.1.2 显示过滤 …… 335
11.2 IP 地址分析 …… 337
11.2.1 结合 DNS 数据包分析 …… 337
11.2.2 结合 DNS 缓存 …… 338
11.2.3 自动解析 …… 341
11.2.4 地址位置信息 …… 344
11.2.5 网站汇总 …… 348
11.2.6 编辑解析的名称 …… 349
11.3 请求分析 …… 351
11.3.1 请求概要 …… 351
11.3.2 请求目标 …… 353
11.3.3 URL 数据传递 …… 355
11.3.4 表单数据传递 …… 357
11.3.5 Cookie 数据传递 …… 359
11.3.6 请求端类型 …… 362
11.4 响应分析 …… 363
11.4.1 请求和响应对应关系 …… 364
11.4.2 响应状态码 …… 366
11.4.3 查看网页内容 …… 368
11.4.4 跟踪流 …… 370
11.4.5 保存流 …… 374
11.4.6 导出 HTTP 对象 …… 375
11.5 HTTPS 分析 …… 377
11.5.1 TLS 流 …… 377
11.5.2 导出 TLS 会话密钥 …… 380

11.5.3 HTTPS 统计分析 …… 381
11.5.4 解密 HTTPS 数据 …… 381
第 12 章 其他应用协议数据包分析 …… 388
12.1 SMTP/POP3 分析 …… 388
12.1.1 过滤 SMTP/POP 数据包 …… 388
12.1.2 分析 SMTP 会话 …… 389
12.1.3 导出 IMF 对象 …… 392
12.2 SMB 分析 …… 393
12.2.1 过滤 SMB 数据包 …… 394
12.2.2 导出 SMB 对象 …… 395
12.3 TFTP 分析 …… 396
12.3.1 过滤 TFTP 数据包 …… 396
12.3.2 导出 TFTP 对象 …… 397
12.4 SCTP 分析 …… 398
12.4.1 过滤 SCTP 数据包 …… 398
12.4.2 SCTP 分析 …… 399
12.5 FTP 分析 …… 401
12.5.1 过滤 FTP 数据包 …… 401
12.5.2 重组 FTP 数据 …… 406
附录 A Wireshark 命令行工具 …… 409
A.1 捕获文件信息查看工具 capinfos …… 409
A.1.1 基本使用 …… 409
A.1.2 报告形式 …… 410
A.1.3 信息种类 …… 414
A.1.4 杂项 …… 415
A.2 数据包捕获保存工具 dumpcap …… 416
A.2.1 捕获数据 …… 416
A.2.2 远程捕获 …… 419
A.2.3 自动停止捕获 …… 420
A.2.4 保存文件 …… 421
A.3 编辑捕获文件 editcap …… 422
A.3.1 基本语法 …… 422
A.3.2 移除指定的数据包 …… 424
A.3.3 去除重复的数据包 …… 424
A.3.4 修正时间 …… 425
A.3.5 截断存储 …… 425
A.3.6 随机修改 …… 426
A.3.7 合并文件 …… 426
A.3.8 修改注释 …… 426

A.3.9 文件集合 …… 426
A.3.10 修改密钥 …… 427
A.3.11 杂项 …… 427
A.4 数据包分析工具 tshark …… 428
A.4.1 捕获数据 …… 428
A.4.2 自动停止捕获 …… 430
A.4.3 远程捕获 …… 431
A.4.4 处理方式 …… 431
A.4.5 保存文件 …… 433
A.4.6 输出信息 …… 434
A.4.7 杂项 …… 439
A.5 简易数据文件分析工具 rawshark …… 439
A.6 其他工具 …… 440
A.6.1 显示过滤器字节码查看工具 dftest …… 441
A.6.2 合并捕获文件 mergecap …… 441
A.6.3 解析 IP 地理信息工具 mmdbresolve …… 442
A.6.4 数据包排序工具 reordercap …… 443
A.6.5 十六进制文本数据转化工具 text2pcap …… 443

第 1 章　网络数据分析概述

网络中的不同设备为了实现通信，会不断发送数据。这些数据被称为网络数据。网络数据根据特定的协议，按照指定格式封包，然后进行传输。如果要对网络数据进行分析，则需要了解网络数据传输方式及使用的网络协议。在此基础上，用户借助 Wireshark 工具，可以快速捕获并分析网络数据包。本章将介绍网络数据分析的相关概念及 Wireshark 工具的安装方法。

1.1　网络数据传输

如果要分析网络数据，则需要先了解网络数据传输的基础知识，如网络构成、数据传输及网络类型。本节将介绍网络数据传输的基础知识。

1.1.1　网络构成

如果要了解网络数据传输，则必须先对网络的构成有所了解。通常情况下，一个网络包括三部分，分别是网络主机、网络线路和网络设备。下面分别介绍这三部分。

1．网络主机

网络主机是指具有网络接口设备（网卡）的主机，如计算机和手机等。通常情况下，计算机又分为云服务器、虚拟主机和物理主机。

2．网络线路

网络线路就是指传输数据的方式。通常情况下，人们使用的网络线路有有线和无线两种。其中，有线就是指通过使用网线的方式连接网络，这种方式限制了设备之间的距离，但是数据传输比较稳定；无线是指通过无线协议实现数据传输和网络连接。例如，对于普通家用 Wi-Fi 网络，一般室内 50 米范围内可以全方位传输数据。但是，无线传输方式容易被电磁波干扰，尤其是墙壁等障碍物对无线信号影响较大。

3. 网络设备

如果要连接网络，则肯定离不开网络设备。网络设备是指使用网线将网络主机连接到一起的设备，如集线器、交换机和路由器。

1.1.2 数据传输

数据传输是指数据从网络主机上通过网络线路传输到另外一台网络主机上。当用户了解数据传输的方式后，就知道在哪里可以捕获需要的数据包。通常情况下，用户无法捕获到某主机数据包，往往是抓包的位置不对，数据没有经过捕获的位置。所以，如果要捕获数据包，则必须确定数据是从哪条线路传输，然后将 Wireshark 放置在该数据传输所经过的设备上。例如，在一个有线局域网中，用户访问百度网站的数据传输线路如图 1.1 所示。

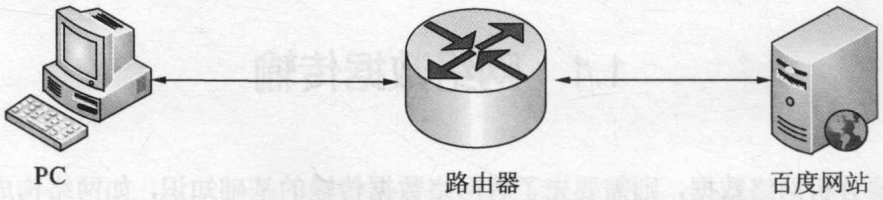

图 1.1 局域网访问百度网站

在该网络中，用户访问百度网站中间就经过一个路由器设备，所有的数据都将由路由器进行转发。所以，此时用户直接在该客户端上启动 Wireshark 即可捕获到访问百度网站的所有数据包。

例如，在一个城域网中，用户访问百度网站的数据传输线路如图 1.2 所示。

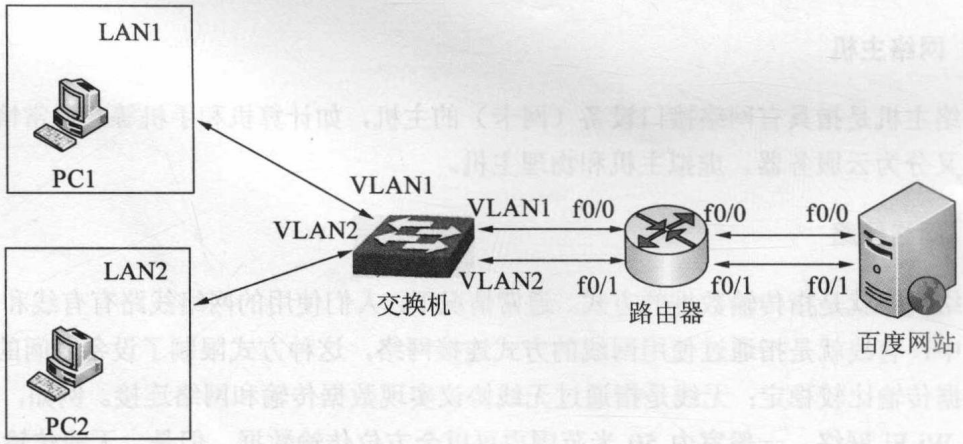

图 1.2 城域网访问百度网站

在该网络中访问百度网站时，主机 PC1 和 PC2 分别位于两个不同城市的局域网内。当主机 PC1 访问百度网站时，经过交换机的 VLAN1 接口和路由器的 f0/0 接口到达目的地；主机 PC2 访问百度网站时，经过交换机的 VLAN2 接口和路由器的 f0/1 接口到达目的地。由此可以说明，这两个主机通过两条不同的路线到达目的地。所以，用户在主机 PC1 上只能捕获到自己访问百度网站的所有数据包，但是无法捕获到主机 PC2 访问百度网站的数据包。

1.1.3　网络类型

依据不同标准，网络有不同的分类方法。根据地理位置分类，网络可以分为局域网、城域网、广域网和个人网 4 种。其中，网络类型不同，数据传输模式不同，数据传输的复杂程度也不同。下面将分别介绍这 4 种类型网络的数据传输方式。

1．局域网

局域网（Local Area Netwok，LAN）是指在某一区域内由多台计算机互联成的计算机组。局域网是最常见、应用最广泛的一种网络。所谓局域网，就是在局部地区范围内使用的网络，它所覆盖的地区范围比较小。在局域网中，PC 通常是通过路由器连接到网络中的，如图 1.3 所示。

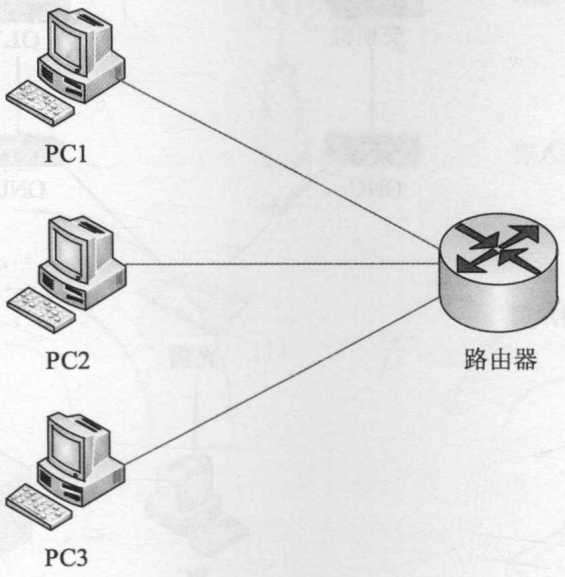

图 1.3　局域网数据传输方式

2. 城域网

城域网（Metropolitan Area Network，MAN）是在一个城市范围内所建立的计算机通信网，属于宽带局域网。这种网络的连接距离为 10 千米到 100 千米，它采用的是 IEEE 802.6 标准。其中，城域网数据传输方式如图 1.4 所示。

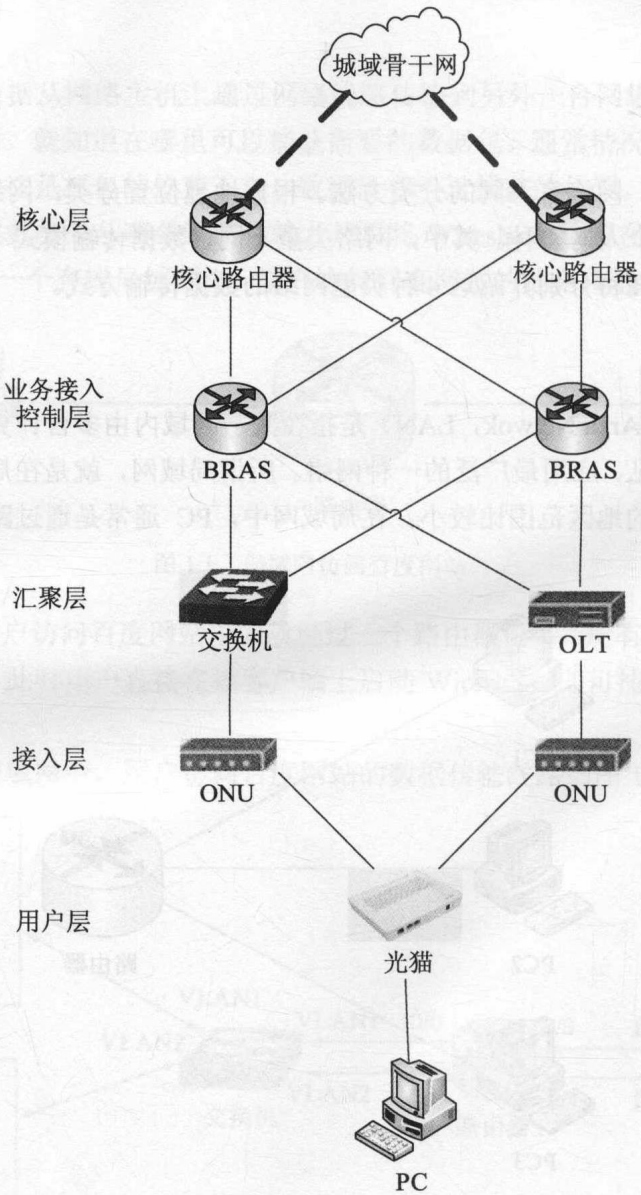

图 1.4　城域网数据传输方式