TCP/IP

TCP/IP

数据包分析程序篇

〔日〕小高知宏 著

- TCP/IP 实际应用解析
- TCP/IP 案例 + 基本概念
- 网络与计算机知识技能的结合

科学出版社
www.sciencep.com

TCP/IP

TCP/IP

数据包分析程序篇

〔日〕小高知宏 著
叶 明 译

科学出版社
北京

图字：01-2003-1377 号

Original Japanese language edition
Kiso kara Wakaru TCP/IP Anaraiza Sakusei to Paketto Kaiseki
By Tomohiro Odaka

Published by Ohmsha, Ltd.
This Chinese version published by Science Press, Beijing
Under license from Ohmsha, Ltd.

基礎からわかるTCP/IP
アナライザ作成とパケット解析
小高知宏　オーム社　2002　第1版5刷

图书在版编目(CIP)数据

TCP/IP 数据包分析程序篇/(日)小高知宏著;叶明译. —北京:科学出版社,2003
ISBN 7-03-011208-3

Ⅰ. T…　Ⅱ. ①小…②叶…　Ⅲ. ①计算机网络-通信协议-程序设计　Ⅳ. TN-915. 04

中国版本图书馆 CIP 数据核字(2003)第 013299 号

责任编辑　杨　凯　崔炳哲　　**责任制作**　魏　谨
责任印制　刘士平　　**封面设计**　李　力

科学出版社　出版
北京东黄城根北街 16 号　邮政编码:100717
http://www.sciencep.com

源海印刷有限责任公司 印刷
北京东方科龙图文有限公司　制作
http://www.okbook.com.cn
科学出版社发行　各地新华书店经销

2003 年 4 月第　一　版　开本:16(787×1092)
2003 年 4 月第一次印刷　印张:14
印数:1—5 000　　字数:236 000

定　价:25.00 元
(如有印装质量问题,我社负责调换〈新欣〉)

前　言

本书介绍了直接观察网络上传输数据的程序——数据包分析程序。

书中的数据包分析程序具有以下功能：

(1) 分析网络上出现哪一类数据。

(2) 分析数据从哪里来传输到哪里去。

(3) 分析数据的大小。

(4) 分析数据中的信息。

利用述的功能可以完成下列事件：

• 以曲线形式表示网络的利用情况(拥挤程度和数据传输量等)。

• 用图形用户界面(GUI)实时表示发送数据的计算机名称和地址以及接收数据的计算机名称和地址。

• 用 GUI 实时表示与数据相关的网络应用程序的种类和数据量。

• 表示出数据内部的信息，并分析出以何种方式进行通讯。

• 分析网络安全。

本书对具有以上功能的数据包分析程序的编写方法及其运行进行了介绍。可帮助对数据包分析程序的编写方法感兴趣的读者深入理解程序的组成和各程序块的功能。而对于只需要观察网络的读者，则可以略过程序说明部分。

书中还介绍了网络的基础知识、数据包分析程序的安装方法和使用方法。

本书内容可供以下读者参考：

- 使用因特网或家庭局域网等网络的读者。
- 在公司或学校等组织中使用和管理局域网的读者。
- 想对网络进行具体深入理解的读者。
- 进行网络学习的读者。

在此，对实现范例程序的福井大学研究生院系统设计工程专业的久保长德先生表示感谢。范例程序中的亮点及创意均应归功于久保先生。并且，对为丰富本书内容和在日常的教育研究上提供多种帮助的福井大学研究生院智能系统工学科的小仓久和先生、西野顺二先生及技术部的白井治彦先生深表感谢。还要对在技术内容上提供详细注释的福井大学研究生院系统设计工学专业的舩上赖光先生、福井大学研究生院系统设计工学专业所属的管理工学研究所(株)的广岛恭一先生、福井大学研究生院系统设计工学专业的森下卓哉先生、福井大学研究生院信息工学专业的大原智明先生和平塚纮一郎先生表示感谢。同时，对为出版本书而鼎力相助的OHM社开发部的各位表示感谢。

最后，还要感谢支持我编写本书的家庭成员们(洋子、研太郎、桃子)。

小高知宏

目　　录

第 1 章　以太网和 TCP/IP

1.1　以太网的结构 …… 2

1.1.1　基于网络架构的以太网的定义　2

1.1.2　以太网的物理层协议　3

1.1.3　以太网上的数据交换　7

1.2　以太网帧的构成 …… 10

1.3　IP 的结构 …… 14

1.3.1　作为网络层协议的 IP　14

1.3.2　IP 地址　16

1.3.3　路由　18

1.3.4　IP 的实际通信　20

1.3.5　域名系统　21

1.4　IP 数据报的构成 …… 23

1.4.1　IP 数据报的构成　23

1.4.2　地址解析协议　26

1.4.3　Internet 控制信息协议　28

1.5　TCP/UDP 的作用 …… 29

1.5.1　TCP 和 UDP　29

1.5.2　TCP　31

1.5.3 UDP 33

第 2 章 数据包分析程序的运行和安装

2.1 数据包流量的时间变化 …… 36

2.1.1 以太网帧的流量观察 36

2.1.2 对特定端口的观察 43

2.2 IP 地址和数据包流量的表示 …… 45

2.3 域名和各种协议的表示 …… 49

2.3.1 报头信息的简要表示 49

2.3.2 报头信息的详细表示 51

2.3.3 数据包的连续监视 54

2.4 TCP 数据的表示 …… 56

2.5 在 FreeBSD 中进行安装的说明 …… 58

2.5.1 在 RedHat Linux 中进行安装的不同点 58

2.5.2 具体的变更点 58

第 3 章 数据包监视程序的设计

3.1 以太网帧的监视 …… 62

3.1.1 基本的数据包监视程序 62

3.1.2 数据包取得能力的评价 68

3.1.3 数据包大小的表示 74

3.1.4 获得 MAC 地址 77

3.1.5 时间的表示 83

3.1.6 数据包类型的判断 86

3.2 IP 数据报的监视 …… 88

3.2.1 IP 数据报的取出 88
3.2.2 IP 地址的表示 91
3.2.3 TTL 94
3.2.4 上层协议的表示 97
3.2.5 arp 和 rarp 98
3.2.6 ICMP 101
3.2.7 域名的表示 103
3.3 TCP 和 UDP …… 110
3.3.1 上层协议的表示 110
3.3.2 TCP 消息段的监视 115
3.3.3 UDP 数据报的监视 120

第 4 章 数据包分析程序的构成

4.1 数据包流量的时间变化 …… 124
4.1.1 以太网帧的流量观察 124
4.1.2 对特定端口的相关观察 134
4.2 IP 地址和数据包流量的表示 …… 140
4.3 域名和各种协议的表示 …… 150
4.3.1 报头信息的简要表示 150
4.3.2 报头信息的详细表示 155
4.3.3 数据包的连续监视 163
4.4 TCP 数据的表示 …… 169

第5章　利用数据包分析程序监视网络

5.1　网络负载的监视 …… 178
5.1.1　网络负载随时间的变化　178
5.1.2　网络利用状况的监视　180
5.2　协议的监视 …… 182
5.2.1　对使用协议的检查　182
5.2.2　与问题协议相关的计算机的指定　184
5.3　网络安全和障碍对策 …… 185
5.3.1　对参与通信的计算机的监视　185
5.3.2　收集更详细的信息　188
5.3.3　追查网络应用程序故障的原因　190
5.4　应用程序类别的监视 …… 192
5.4.1　telnet　192
5.4.2　pop3　194
5.4.3　SMTP　202
5.4.4　网络新闻传输协议　209
5.4.5　WWW(服务器的情况、客户端的连接处)　210

参考文献 …… 213

第1章 以太网和TCP/IP

本章主要介绍以太网上层协议中IP、TCP/UDP等通信协议的功能及特点。

1.1 以太网的结构

1.1.1 基于网络架构的以太网的定义

在思考计算机网络构成技术时，一般都推行使用协议进行层与层之间的通信。本书是按照国际标准化组织(ISO：International Standard Organization)提出的 OSI 参考模型(open system interconnect reference model) 展开讲解的。

在 OSI 中，把协议等级分为七层。

第一层是物理层，处理关于硬件上的网络协议。第七层为应用层，处理关于应用程序的协议。第二层到第六层按照其间的顺序被依次设置。

表 1.1　OSI 参考模型

层		名　称	规定的内容
高层	第七层	应用层	关于邮件、新闻等应用程序的协议
	第六层	表示层	数据语法协议
	第五层	会话层	基于网络的管理对话协议
低层	第四层	传输层	补充第三层的功能，可靠地在两台计算机间传输数据
	第三层	网络层	从网络上多台计算机中选择作为通信对象的计算机
	第二层	数据链路层	在两台计算机上进行一对一数据通信
	第一层	物理层	电气信号、连接器规格等关于硬件的协议

另一方面，以太网(Ethernet)是 20 世纪 70 年代，施乐(Xerox)公司的 Palo Alto 研究所设计的，其后在 80 年代由施乐、英特尔、DEC(后被康柏收购)三家公司总结了面向局域网(LAN)的协议的集合。给予以太网的定义是 OSI 参考模型中关于第一层与第二层的协议。

以太网的规格是由美国电气和电子工程师协会(Institute of Electrical and Electronics Engineers)中专门讨论规格的 802 委员会，从 1980 年开始标准化讨论的。并把 IEEE802.3 作为标准规格，其后 ISO 把它作为 ISO802.3 标准。随着技术的发展，为了适应网络高速化，IEEE802 委员会正在讨论新的以太网标准。

但是，以太网的规格与 IEEE802 委员会的规定存在一定的差异。本书分别在必

要的地方进行了介绍。

作为题外话，谈谈802委员会的名字的由来，最初的委员会是在1980年2月召开的，所以名字也就由此而来。

下面对以太网的第一层与第二层协议依次进行介绍。

1.1.2 以太网的物理层协议

在以太网中使用同轴电缆、光纤电缆和双绞线等作为传送媒体。表1.2中记述了以太网的规格名称和传送媒体的种类。

表1.2 以太网使用的传送媒体

媒体名称	规格名称
同轴电缆	10base-5　10base-2
双绞线	10base-T　100base-TX　1 000base-T
光纤电缆	100base-FX　1 000base-SX　1 000base-LX

现在广为使用的传送媒体为双绞线。双绞线是为了提高高频率特性和排除信号干扰将两根细铜线相绞成一组的线。以太网使用的是4组8根绞成的双绞线，本来该种双绞线是被使用在ISDN电话线上的。

双绞线中根据频率特性等的不同又分成若干种，现在经常使用的是被称为第五类的双绞线。以太网的通信(传输)速度如表1.3所示。其中第五类的双绞线具有100Mbit/s的通信速度，规格对应为100base-TX，并且有一部分对应更高的规格(1 000base-T)。

要进行说明的是，所谓10base-T和100base-TX的规格名称中，头部的数值部分表示的是以Mbit/s(Mega bits pre second)为单位的通信速度。尾部的base表示的是基于基本频带的通信。在基本频带通信中，无需对信号调制就可以直接在通信线路上进行信号传输。

表1.3 以太网的通信速度

通信速度	规格名称
10Mbit/s	10base-5　10base-2　10base-T
100 Mbit/s	100base-TX
1Gbit/s(1 000 Mbit/s)	1 000base-SX　1 000base-LX　1 000base-T

使用 100Mbit/s 以下的双绞线的以太网，其实只使用了 4 组 8 根电线中的两组进行信号交换。在以太网的本来的规格中规定一组用来发送数据，另一组用来接收数据。

以太网中，当网络上连接多台计算机时，某瞬间只能有一台计算机可以传送数据。在基本频带方式下，两台计算机同时发送信号会发生冲突，不能进行通信。为了控制数据传送，常使用发送用和接收用两组信号线。

在用双绞线连接时要使用被称为网络集线器的设备。它是为实现多台计算机的连接，把多根双绞线相互连接起来的设备。在使用网络集线器的网络中，计算机以网络集线器为中心呈放射状连接，这样的网络被称为星型网络。

这种网络集线器可分为两大类。一类是转发网络集线器，另一类是开关网络集线器。使用转发网络集线器时，能够将向某一台连接装置发出的输入信号全部传送到其他连接装置。如图 1.1 所示，从计算机 A 发出的信号无论发送到计算机 B、C、D 中的哪一台，都将全部发送到所有的计算机中。以太网中只有被指定为接收信息的计算机才能读取数据，而其他的计算机将把收到的信号删除。

与此相对，在开关网络集线器中网络集线器需要分析数据传送目的地，从而只向关联的计算机发送信号。

如图 1.2 所示，从计算机 A 向计算机 D 发送数据时，开关网络集线器不向计算机 B、C 发送信号。这样，开关网络集线器就像开关一样能切换信号传送的路径。

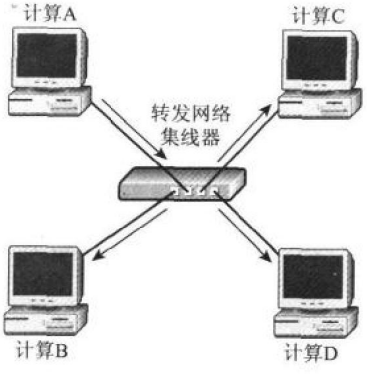


图 1.1　转发网络集线器的功能

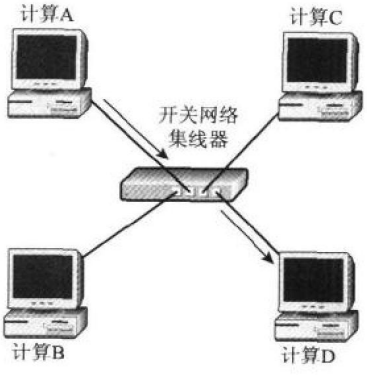


图 1.2　开关网络集线器的功能

使用开关网络集线器时，只能在有通信关系的计算机之间进行通信，所以提高了全体网络的通信效率。

具有 1Gbit/s 通信速度的以太网，被称为千兆以太网。使用双绞线来实现千兆以太网的时候需要第五类以上且具有良好通信的双绞线。这种作为第六类或第七类的双绞线，现在正在进行规范化。

同时，利用两条第五类双绞线中的 8 组 16 根通信线路，也能实现 1Gbit/s 的通信。把这种方法使用在 1 000base-T 中，只要改变一下信号的形式和电线的使用方法，就能实现 1Gbit/s 的通信。

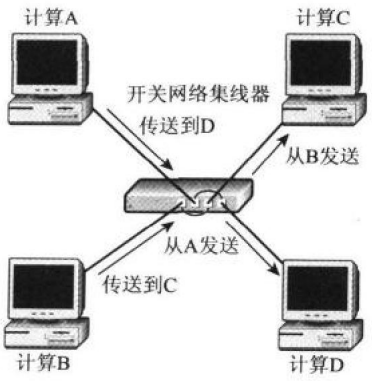
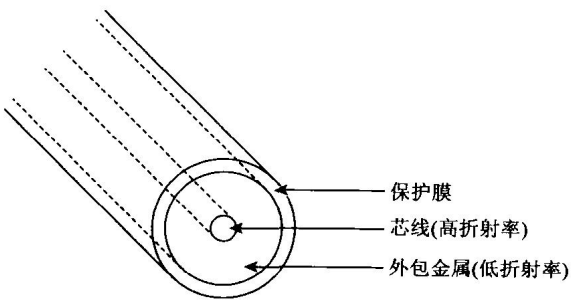


图 1.3 开关网络集线器的并联通信

在具有高速传送速度的以太网中，经常使用光纤电缆。光纤电缆是在细的玻璃纤维中通过光波的形式进行通信的电缆。但是，通过玻璃纤维时，在纤维弯曲的部分会使光折射掉。因此，要在光纤电缆中使用不同折射率的玻璃并对电缆中光的封闭性加以研究。

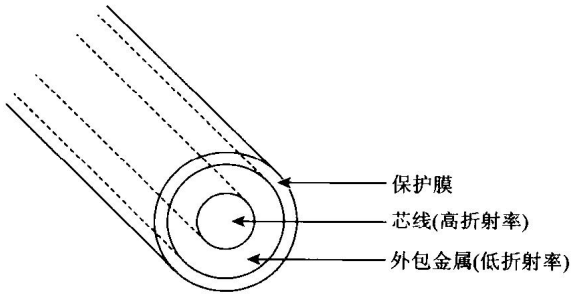
光纤电缆大致可以分为单模和多模两种。单模与多模相比，因为芯线直径小，所以可传送的频率带宽，但连接等操作困难。因此，单模光纤电缆常被用于远距离通信，而多模光纤电缆则被用于局域网内。

一般以光为介质的通信，与双绞线等用铜的情况相比，具有高速通信的优点。因此在千兆以太网的规格中，1 000base-SX 和 1 000base-LX 是用光纤电缆来实现的。即使使用光纤电缆，设备之间的连接同样需要网络集线器，并且接收和发送需要两根光纤电缆，这一点与使用双绞线的以太网很相似。

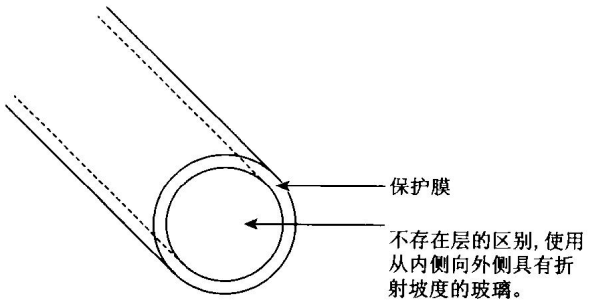


(1) 单模光纤电缆

图 1.4 光纤电缆的构造



(2) 步层多模光纤电缆



(3) 分级多模光纤电缆

图 1.4 (续)

旧的以太网设备是用同轴电缆作为传送媒体的。同轴电缆如图 1.5 所示,构造的中心有一根铜线,该铜线的规格本来是为了传送高频率信号而开发的。

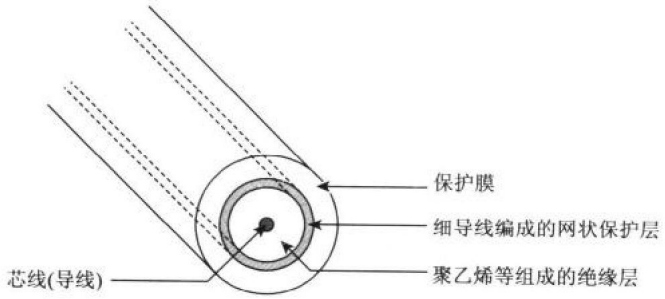


图 1.5 以太网中使用的同轴电缆构造

使用同轴电缆的以太网,设备之间的连接不需要网络集线器。但是,必须在同轴电缆上将设备连接起来,使同轴电缆成为多台设备间共享信号的总线(bus)。与星型

连接方式相对，这样的网络连接形式被称为总线型。

同轴电缆连接的以太网有 10bsae-5 和 10base-2 等规格。虽然哪一种都能达到 10Mbit/s 的传送速度，但使用的同轴电缆有粗细和连接形式的区别。10base-5 在本来的以太网规格中使用在被称为黄缆的粗缆上。

如图 1.6 所示，这种 10base-5 与被称为收发器的连接装置安装在一起，以从收发器经过收发器电缆到计算机的布线方式构成网络。

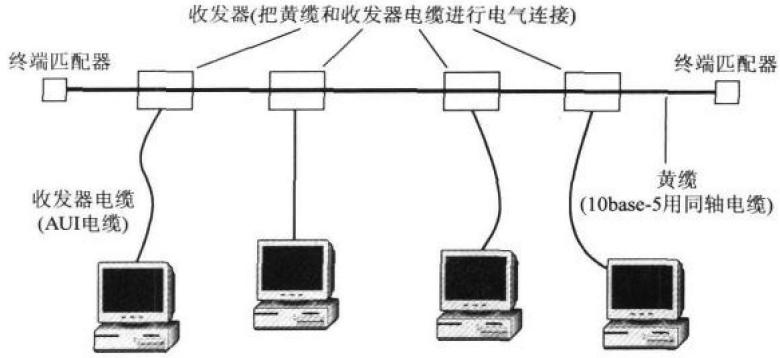


图 1.6 基于 10base-5 的电缆连接

在 10base-2 中使用的电缆比 10base-5 中使用的要细一些。如图 1.7 所示，在设备的连接中使用 T 型连接器，如佛珠一样将计算机连接起来。

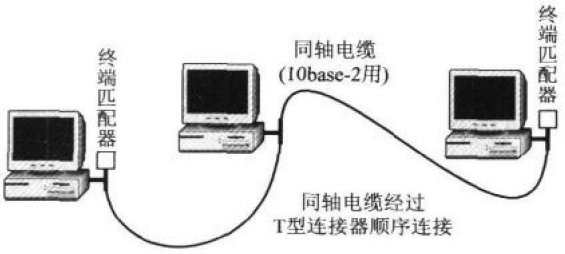


图 1.7 基于 10base-2 的电缆连接

1.1.3 以太网上的数据交换

在以太网中，数据是以被称为帧的数据结构体为单位进行交换的。通常，在计算

机网络上交换的数据结构体的单位是数据包，而在以太网中把使用的数据包称为帧。

这种数据包如图 1.8 所示，是由记录着数据包发送给对方所必需信息的报头部分和记录着传送给接收端信息内容的报文部分组成的。

报头包含接收端的地址、发送端的地址、数据错误检查和改正所必需的错误检验和修正码。数据包被传送到网络上，通过网络中继装置传送到接收端。

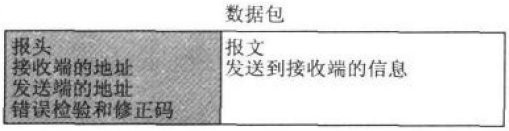


图 1.8　数据包的一般结构

下面讲解一下以太网上的帧是如何被发送出去的。在以太网上，帧是被称为带碰撞检测的载波侦听多址访问(CSMA/CD: Carrier Sense Multiple Access with Collision Detection)发送的。

在 CSMA/CD 技术中，如果网络上没有数据，则任何时候都可以将数据传送出去。因此，传送数据的网络设备，首先要确认网络上是否有数据在传送。如果没有数据则可以将数据发送到网络上。如果网络被使用，那就要等到网络空闲后发送。上面的工作相当于 CSMA/CD 的 CSMA 部分。

在这种方法中，同时发送数据的网络设备会同时认为网络是空闲的，这样就会产生发送冲突。因此，在 CSMA/CD 技术中会经常一边检测数据冲突(collision)，一边发送数据。

在使用同轴电缆的以太网中，冲突就是字符信号发生碰撞从而导致数据包的损坏。

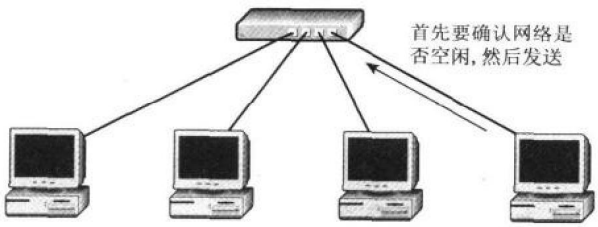


图 1.9　在 CSMA/CD 技术上的数据发送