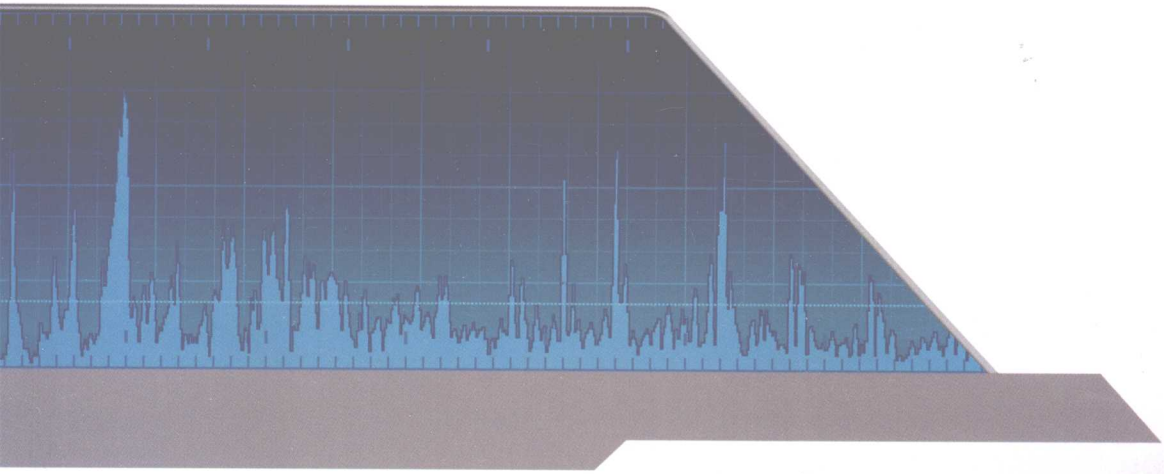
实用网络流量分析技术

高彦刚 编著



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

实用网络流量分析技术

高彦刚　编著

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书对流量分析技术的原理和相应流量分析工具的工作原理进行了详细的阐述，重点说明如何结合网络实际管理工作进行网络流量分析，不但在理论上论述网络流量对网络运行质量的影响，同时结合案例分析，阐述如何快速发现影响网络运行的流量以及分析这些流量产生的原因并解决问题。结合实际案例，使读者能够有效掌握对蠕虫病毒、ARP 攻击、DoS 攻击、路由问题、软件的资源滥用等危害网络正常运行的各种网络行为的分析方法。

书中完全以实用技术为主的技术内容，能够在很大程度上提高网络管理人员的网络分析技术水平，从而在对管理水平要求越来越高的实际网络管理工作中游刃有余。本书适合从事网络管理工作的技术人员和相关专业师生阅读。

图书在版编目（CIP）数据

实用网络流量分析技术/高彦刚编著. —北京：电子工业出版社，2009.7
ISBN 978-7-121-08979-4

Ⅰ. 实… Ⅱ. 高… Ⅲ.计算机网络—流量—分析 Ⅳ.TP393

中国版本图书馆 CIP 数据核字（2009）第 086168 号

责任编辑：高买花 特约编辑：陈宁辉
印　　刷：北京机工印刷厂
装　　订：三河市鹏成印业有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱 邮编 100036
开　　本：720×1000 1/16 印张：12.5 字数：252 千字
印　　次：2009 年 7 月第 1 次印刷
印　　数：4 000 册 定价：36.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前言

网络流量分析技术一直以来都是网络管理技术人员必备的一项技术，掌握网络流量分析技术对更好地了解网络的运行情况、及时有效地发现并分析各种网络和应用问题都有很大的帮助。

很多技术人员认为网络流量分析技术是非常难以掌握的复杂技术，其实并不然。网络流量分析技术本身并不复杂，而且易于掌握，关键在于如何将其同实际的网络分析结合起来，发挥其最佳作用。

《实用网络流量分析技术》涉及网络管理各个层面的实用分析技术。书中包括对流量分析技术原理的阐述和网络流量分析工具的介绍，使技术人员能够更深入地理解网络流量分析技术。本书的重点在于阐述网络运行中的各种关键流量特征、重要网络行为特性的分析原理，结合具体的分析案例，帮助技术人员系统掌握如何在实际网络环境中利用网络流量分析技术提高技术人员的网络分析能力。

《实用网络流量分析技术》是编著者从事了多年网络流量分析技术工作的经验积累和总结，相信能对广大技术人员掌握网络分析技术有所帮助，同时也希望得到您的宝贵意见。

高彦刚

2009 年 5 月

目录

第 1 章

关于网络流量分析

本章主要说明网络流量分析的概念、用途，以及如何将网络流量分析技术融入到网络管理流程中。

1.1 什么是网络流量分析

网络的作用是传输应用数据，应用数据在 OSI 协议模型中的传输过程描述如 图 1-1 所示。

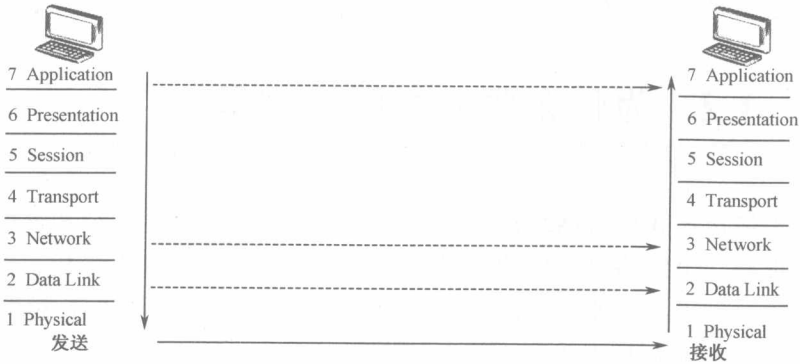


图 1-1 OSI 协议模型

在 OSI 协议模型中，发送方的应用数据由下层协议逐层处理，最后通过物理层传输，接收方则逐层向上处理从物理链路上接收的信号，

最后还原成应用层数据。

一个 Web 应用数据在 OSI 模型中的网络数据传输处理过程如图 1-2 所示。

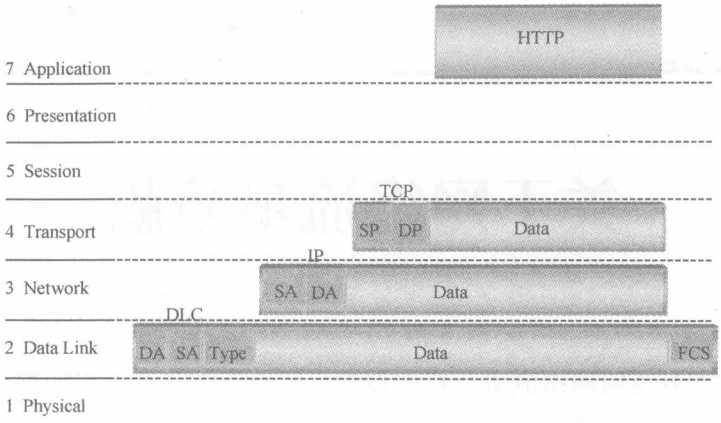


图 1-2　Web 应用的数据传输处理过程

从图 1-2 可以看出，应用数据在应用层采用 HTTP 协议，在传输层被分段，在网络层封包，在数据链路层封帧，由物理层传输，由每一层进行处理，按照相应的协议进行封装。

网络流量的分析就是对在网络中传输的实际数据流进行分析，网络数据流的分析包括从底层的数据流一直到应用层数据的分析，有时我们也称为网络协议分析。

1.2　为什么要分析网络流量

简单地说，我们对网络流量进行分析的目的是了解、发现和证明。

管理好一个网络最重要的就是对网络的了解，了解网络拓扑、设备、配置等是必须的，但要保证网络的服务质量，那是远远不够的，对网络流量的分析能使网络技术人员更深入地了解网络。

（1）网络运行规律的了解。

每个网络都有自身的运行规律，这和网络的结构、应用特点等紧密相关，通过对网络流量的长期分析，能够了解网络系统运行的规律。

（2）网络应用运行规律的了解。

网络上重要的应用在运行时，每一个访问，每一个交易处理，数据都由网络来传输，通过分析应用的流量，能够清楚了解应用运行的规律，访问量、交易处理数量、响应性能等数据，都可以通过流量分析手段获取。

（3）网络用户的网络行为。

每个网络用户的网络行为都是相互影响的，同时会对网络的运行产生影响，伴随每个用户在网络中的每个网络行为都有网络流量产生，通过对网络用户的网络流量进行分析，能够直观地了解网络用户的网络行为。

发现，主要是针对异常的发现，是建立在了解的基础之上的，如果能做到及时地发现网络中的异常，将使网络管理更主动，将为网络的持续高性能运行提供重要的保障。

（1）网络运行异常的发现。

网络中流量的异常，包括利用率、数据包数的异常。

（2）网络应用运行的异常发现。

连接数量、应用响应、应用流量的异常，都可以通过长期主动分析来及时发现。

（3）网络用户的异常网络行为。

异常的网络行为也都有明显的流量特征，如感染的蠕虫病毒、安装了后门程序等，长期的流量分析能及时发现网络用户的这些异常网络行为，及时发现网络用户的异常网络行为是避免其影响网络运行的关键。

网络流量的分析可以为网络和应用问题的分析提供依据，特别是数据包级的分析，而这些依据是真实的，因为它们是实实在在在网络中传输的数据包，这也是流量分析能够大大提高网络和应用问题分析效率的原因。

1.3 网络流量分析的意义

网络流量分析是有助于维护网络持续、高效和安全运行的一种手段，网络流量分析的意义在于取得对网络运行管理、应用运行管理和网络应用问题分析有意义的数据。

这些数据多种多样，像利用率、bps、pps 还是延迟、重传、连接数量

等这些流量分析的数据，都要和我们实际的网络应用运行情况结合起来才有意义，因为不同的网络和不同的应用都有完全不同的流量数据。

网络流量分析的数据的意义是建立在了解的基础上的，只有对你的网络和应用进行深入了解，才能使这些数据的价值得到真正的体现。

举个例子说，血液中白血球数量对分析一个人的身体状态来说是很重要的数据，不管是检查身体还是生病做检查它都是重要数据，但是这数据要和每个人的实际情况结合才有意义，如年龄大小、怀孕与否、身体情况等，另外这个数据的意义是建立在对身体了解的基础上的，只有了解了每种状况下该数据的正常值以及什么原因能引起该数值上升或下降时，我们通过检查得到的分析数值才有意义，才能通过该数值了解我们的身体状态。

网络流量分析在网络管理中具有重要的意义，网络流量分析给技术人员提供的有效技术数据对了解网络、发现问题、确认原因都有重要意义，而这些能够在网管工作的整个进程中提供有效的帮助。

本书将主要通过原理介绍以及实际案例分析来介绍网络流量分析技术在网络管理中的实际应用。

第2章

网络流量分析工具

本章主要说明网络流量分析工具的历史、工作原理，以及网络流量未来的发展方向。本文中的网络流量分析工具主要指针对网络流量进行直接分析的分析工具，不包括通过 RMON 以及 FLOW 取得流量分析结果并进行统计分析展示的软件。

2.1 网络流量分析工具的工作原理

一个网络流量分析工具的完整功能由软件和硬件共同完成。硬件的主要功能是流量的取得，而软件的主要功能则是流量的分析和数据展示。

2.1.1 网络流量的取得

网络流量分析的对象是网络流量，而网络流量的获取是分析的基础和前提。

网络流量分析工具用于获取网络流量的硬件是网络接口卡，不同类型的网卡用来分析不同类型的网络，最早用来做流量分析的网卡是以太网卡和 Token Ring Romom 网卡，而随着网络技术的发展很多厂商开始生产专门用于做流量分析目的的网络接口卡，这些接口卡在流量的处理性能上比普通的网卡有很大的提高。

在获取网络流量时，网络接口卡必须工作在一种称为“混杂模式”（Promiscuous）的状态下。在正常状态下，网络接口卡只将收到流量中的广播包以及发送给本网卡物理地址的流量传送给上层程序进行处理，而在“混杂模式”下工作的网卡会将所有接收到的流量传送给上层程序进行处理。

在最早的共享式以太网网络环境中，每个网卡都能接收到本网络域中所有的流量，因此只需将网络流量分析设备接入到网络中就能分析到该网络中的所有流量。随着交换技术的普及，接入到交换机其中一个端口的流量分析设备无法接收到其他端口的流量，网络流量工具在获取网络流量主要通过以下两种方式。

1. 流量镜像方式

流量镜像（SPAN）是交换机具备的专门为流量分析设计的一种功能，通过镜像，交换机能够将选定端口或 VLAN 中传输的流量复制发送到指定的交换机端口，该端口一般称为流量监控端口，流量分析设备只需接入到该端口就可以分析到其他端口的网络流量。

2. TAP 设备

TAP 设备是一种用于直接复制网络链路上的物理信号设备，包括电信号和光信号两种类型，电信号 TAP 类似于三通，跟在电话线上搭接电话线工作原理类似，有无源和有源之分。光信号 TAP 主要是各种分光器，作用是将光信号通过物理手段分成两路，一路用于网络正常通信，一路用于对链路流量进行分析，在不影响传输的情况下实现监控分析。光 TAP 在网络链路上的部署如图 2-1 所示。

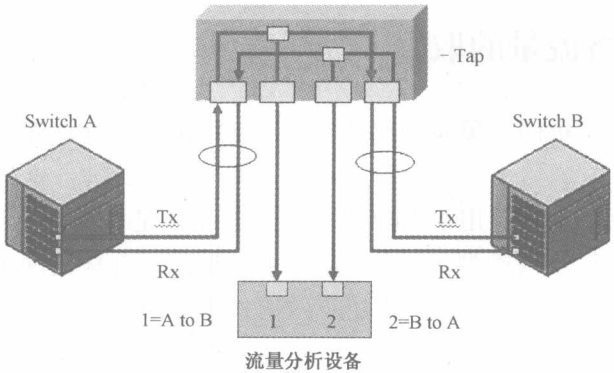


图 2-1　光 TAP 在网络链路上的部署

2.1.2　流量的分析

流量的分析主要靠分析软件实现，一个通用的流量分析工具对流量的主要分析功能包括统计分析、智能分析、捕获和解码分析三类。其分析系统功能意如图 2-2 所示。

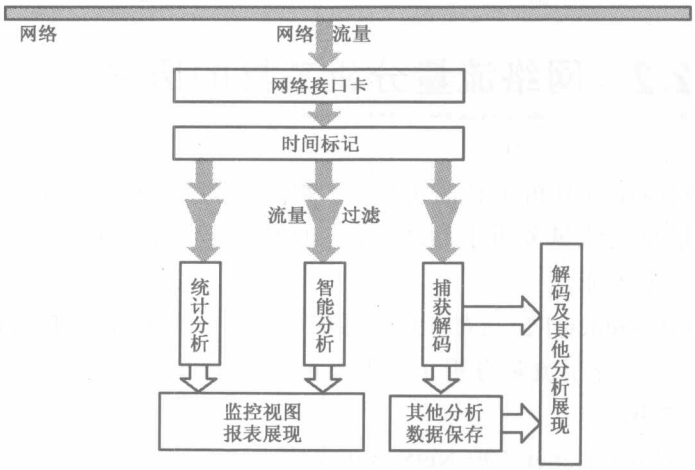


图 2-2　网络流量分析系统功能

如图 2-2 所示，网络流量分析工具通过网络接口卡获取网络中的实际数据包，首先按收到数据包的时间对数据包进行时间标记（有些分析专用的网络接口卡本身具有硬件时间标记功能），然后由软件分析模块进行分析并展现监控、报表、解码等数据分析视图，按分析方法的不同可分为统计分析、智能分析、捕获解码分析三类。

1. 统计分析

统计分析通过统计方法提供流量的统计数据，针对一段时间内（一般最小时间间隔为秒）数据包的统计，包括数据包数、字节数、不同包长包数等链路流量统计，每个 MAC 地址的流量及 MAC 地之间流量信息，IP 层数据包统计，TCP 层数据统计等。

统计的结果以监控视图及报表的形式展现。

2. 智能分析

智能分析指对网络中的数据流特征进行分析，通过一定的方式匹配和

比对，提供针对性的分析结果，如对网络某种问题的流量特征进行匹配，从而在问题出现时自动发现及告警。

3. 捕获和解码分析

捕获和解码分析是最原始的网络流量分析功能，通过将流量捕获，对每一个数据报文分层进行协议解析并展现。

2.2 网络流量分析工具的历史

提起网络流量分析工具的历史，不得不提的是 Sniffer 的历史，Sniffer 产品作为最早的流量分析工具之一，它的发展史是整个网络流量分析工具发展史的一个缩影。

Network General 公司在 1986 年推出了第一款 Sniffer Portable（便携式 Sniffer），拉开了流量分析工具发展的序幕。该产品的发展如下：

☆ 2007 年

Network General 被 NetScout 收购

☆ 2004 年

发布 Sniffer Application Intelligence（应用智能管理）解决方案

☆ 2003 年

发布业界第一款 10-Gigabit probe

发布 multi-Gigabit core platform（s6000）

发布 Gigabit capture/storage product（Infinistream）

☆ 2002 年

发布 enterprise management & reporting solution（nPO）

发布 2G/3G mobile product（Sniffer Mobile）

☆ 2001 年

发布 VoIP probe（Sniffer Voice）

☆ 2000 年

发布业界第一款 Wireless LAN probe

☆ 1999 年

发布 Windows version of Sniffer

☆ 1998 年

发布业界第一款 Gig probe

☆ 1997 年

Network General 与 McAfee Associates 合并成立 Network Associates，Inc.

☆ 1991 年

Network General 发布业界第一款 distributed Sniffer

☆ 1986 年

Network General 发布业界第一款 Sniffer Portable

从 Sniffer 的历史我们可以看到，流量分析工具是一直跟随网络技术向前发展的，第一代流量分析工具是伴随第一代局域网技术产生的（以太网技术、令牌环技术），随着网络技术的发展，流量分析工具的性能和功能也有相应的加强，流量分析技术应用到各种高性能网络环境中。

而从流量分析本身的技术来看，并没有太大的发展，只是根据不同的需要和不同的网络技术在不断地扩展和完善，但在展现形式上有很大的提高，从最初的简单流量捕获的解码分析，到适用于不同用户不同需求的监控和报表展现，以及企业级分布式部署方式等有了很大不同，同时在流量分析数据的进一步处理上有了很大 提高。

流量分析技术也广泛应用于很多不同功能的产品技术中，像 IDS（入侵检测系统）、防火墙、流量控制设备、负载均衡设备等，都和流量分析技术直接相关，采用流量分析技术设计的专用分析系统也越来越多，也是流量分析工具的一个发展方向。

2.3 网络流量分析工具的产品功能

本书中的流量分析案例主要采用 Sniffer Pro 和 Sniffer Infinistream 两个产品，下面对它们的主要功能进行介绍。