信息通信专业教材系列

网络流量监测与控制

Wangluoliuliang Jiance Yu Kongzhi

刘　芳　主编
窦伊男　陈陆颖　于　华　雷振明　参编

北京邮电大学出版社
www.buptpress.com

信息通信专业教材系列

网络流量监测与控制

刘　芳　主编

窦伊罗　陈陆颖　参编

于　华　雷振明　参编

北京邮电大学出版社

·北京·

内 容 介 绍

本书分为12章，系统介绍了网络流量的监测和控制的相关基础知识，首先是网络流量的监测意义和方法、异常流量的特点。然后介绍了几个软件的功能、原理和使用方法(包括主机内嵌流量监测软件Wireshark、监测运行SNMP协议的网络设备的软件MRTG、开放源代码的网络数据包截获和分析软件WinPcap)。最后讲解了流的概念、方法，常用的流技术，IP设备输出流量信息标准IPFIX参考模型和格式，流量监控硬件的结构、功能和相关硬件技术，业务分析的关键问题和业务识别的主要方法，用户行为的分析过程和常用的分析方法，各种流量控制技术的原理等。

本书可以作为信息工程、通信工程及计算机科学技术等本科专业的教材和教学参考书，也可以作为专业技术人员的参考和培训资料。

图书在版编目(CIP)数据

网络流量监测与控制/刘芳主编．—北京：北京邮电大学出版社，2009
ISBN 978-7-5635-2098-5

Ⅰ．网… Ⅱ．刘… Ⅲ．①计算机网络—流量—监测②计算机网络—流量—控制 Ⅳ．TP393

中国版本图书馆CIP数据核字(2009)第177995号

书　　名：网络流量监测与控制
作　　者：刘　芳
责任编辑：刘　颖
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路10号(邮编：100876)
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京源海印刷有限责任公司
开　　本：787 mm×960 mm　1/16
印　　张：14.25
字　　数：292千字
印　　数：1—3 000册
版　　次：2009年9月第1版　2009年9月第1次印刷

ISBN 978-7-5635-2098-5　　定　价：25.00元

前　言

随着宽带互联网在中国的迅速发展，全国各大网络运营商的网络规模都在不断扩张，网络结构日渐复杂，网络业务日趋丰富，网络流量高速增长。网络运营商需要对网络流量进行可靠、有效的监测与控制，并对网络以及网络所承载的各类业务进行及时、准确的分析，挖掘网络资源潜力，控制网络互联成本，并为网络规划、优化调整和业务发展提供基础依据。

本书作者长期在网络流量监测与控制领域进行研究工作，深感缺少一本这个领域中介绍常用知识的书籍，作者在多年的研究及实践基础上，参阅了大量有关知识的书籍和资料，进行整理，完成了本书的编写。

本书分为12章。第1章为概论，介绍网络流量监测的意义和价值、宽带网络中的主要设备、网络流量监测的手段和内容。第2章介绍了因特网基本知识，第3章讨论网络异常流量，包括链路流量及其异常、针对路由协议的攻击、针对设备转发表的攻击、与各种协议(IP、ICMP、TCP、UDP以及应用层协议)相关的异常、端口扫描、DoS与DDoS攻击、蠕虫攻击等。第4～6章介绍了几个常用监测软件的功能、原理和使用方法。首先是主机内嵌流量监测软件，以Wireshark为例讲解报文捕获、解码分析、报文统计的方法，介绍Wireshark中Follow TCP Stream的功能以及Wireshark的Pcap文件保存格式；其次对于监测运行SNMP协议的网络设备的软件MRTG，介绍了MRTG监测的内容、数据处理的方法、主要组成部分、配置使用方法，最后介绍了基于Win32平台的网络数据包截获和分析软件WinPcap的功能、结构、安装使用方法，并介绍主要函数及其使用方法。第7章讨论流技术，给出了流的定义、开始和结束标记方法、流记录信息输出内容、流的统计、采样、分类和汇聚方法，详细分析NetFlow和sFlow两个主流技术。第8章介绍网络流量监测相关的标准RTFM、IPPM、IPFIX、PSAMP的内容，讲解了IPFIX主要任务和5种备选协议，详细介绍了与IPFIX最相似的NetFlow V9数据包的格式，描述了

IPFIX 流定义、参考模型、推/拉模式、传输层协议的选择、IPFIX 的信息模型和输出格式。第 9 章介绍了流量监控硬件的结构和功能，讨论了硬件监控采用的主要硬件技术，包括网络处理器、现场可编程门阵列 FPGA、内容可寻址存储器 CAM、哈希等。第 10 章介绍了 IP 网络对业务的支持、网络业务模式、典型业务的工作原理、业务分析的关键问题和业务识别的主要方法。第 11 章介绍了用户行为分析的概念、特点、难点、意义和发展现状，讲解了网络用户行为分析的过程，介绍了用户数据分析的常用的统计方法和数据挖掘方法，简单描述了用户行为分析的常用工具，最后用一个案例说明用户行为分析的过程和方法。第 12 章说明了网络流量控制的必要性，讲解了几种流量控制的方法：TCP 流量控制、IntServ 综合服务、DiffServ 区分服务、路由器的流量控制策略，最后介绍了目前实用的流量控制措施。

本书由刘芳担任主编，窦伊男、陈陆颖、于华、雷振明参加编写。其中，第 1 章由雷振明教授编写，第 7 章和第 8 章由陈陆颖编写，第 9 章由于华编写，第 10 章和第 11 章由窦伊男编写，其余由刘芳编写，全书由刘芳统稿。刘鹏、苗卉、曹晓光、宋莎莎、胡亮、王新良等人做了部分资料整理工作。

本书的出版得到了国家科技支撑计划课题“可信任互联网——新一代可信任互联网安全和网络服务”(2008BAH37B00)和北京邮电大学信息与通信工程学院 2009 年本科教育教学改革与研究项目的支持，北京邮电大学出版社为本书的出版做了大量的工作，在此一并表示感谢。

由于网络监测与控制技术发展迅速，加上作者水平有限，书中难免存在一些缺点和错误，希望广大读者批评指正。

编 者

2009 年 8 月

目　　录

第1章 概 论

目前网络已经非常普及，网络的应用也越来越多，从浏览网页和收发电邮，到打游戏、聊天、看电影、听音乐、打电话包罗万象。电视网和电话网能够做的事情，宽带网也都能够做了。同时，宽带网还能够做电视网、电话网以外的许多其他的事情。而这一切，都是靠信息在网络上的流动来实现的。汽车在马路上跑，常常会引出交通堵塞以及不遵守交通规则等现象，因此需要交通部门来实时检测道路情况和处理突发事件。同样，网络流量也需要监测和控制。

首先，对网络流量监测与控制涉及的名词予以定义。

网络：本书所说的网络，指的是宽带因特网。

流量：来自英文 traffic，这个翻译不够准确，traffic 原指交通，马路上车堵了叫做“traffic jam”就是一例。而网络中的 traffic 乃是指网络上传输的数据信息，不只是其大小的一个量。流字很贴切，量字的定义则太窄了。因为流量是一个约定俗成的说法，但这里说的流量，是指网络上传输的数据信息，不只是表示其大小的一个量。

监测：指对网络流量进行长期不间断的监视和测量，叫做网络流量监测。大致和英文的 monitoring 对应。

控制：指对网络流量的控制，对网络某些流量的限制或限速。网络流量控制的基本目的之一是使各种信息在网络上的流动最大限度的畅通。

1.1 网络流量监测的意义和价值

1. 科学规划和扩容

在没有有效的流量监测情况下，如果流量长期过大，最简单的办法是扩容。但是一

味地扩容，不仅投资巨大，而且不一定能解决问题并获得相应的收益。在对网络进行有效的流量监测情况下，可以通过流量历史数据的趋势分析来对一些低附加值流量进行控制，从而减少扩容的次数。网络流量监测还能提前预测到何时流量会增加到需要扩容的地步，从而提前采取措施。通过对流量的分析，还可预测某处扩容后对于其他各处的影响等，为提出一个具有全网动态实时监测与自校正能力的拓扑的优化设计与管理方案奠定基础。

2. 公平分配资源和计费

目前少量用户占用了大部分网络资源，而大量用户占用的资源却很少，有时还需要等待一个页面缓慢地打开，这样的资源分配显然是不公平的。通过网络流量监测手段发现：即使同一类付费用户，其流量也可能有十倍、百倍的差别。网络流量监测手段不仅能够发现这种不公平性，而且能够对如何使资源比较公平地分配给出提示。

按流量收费的固有障碍产生于计算机动作的自动化和与用户的愿望的不一致。即计算机接收的信息可能不是用户想要的，甚至可能是有害的，例如病毒，因此不能按照接收信息付费；计算机发送的信息也可能不是用户想发的，而是计算机自动产生的，甚至是因为受到网络入侵以后自动发送的，因此完全按流量付费的合理性也同样受到质疑。

通过对客户的流量进行监测分析，可以统计出业务类型、服务等级、通信时间和时长、通信数据量等参数，为基于 IP 的计费应用和服务等级协议(SLA)的校验服务提供数据依据。

3. 网络的运行维护

如果网络中的哪个部分出现问题，一般会有相应的流量异常。因此，流量异常的显示也就可以成为网络故障分析的一个辅助手段。但是，为了能够有一个流量异常的判断依据，首先需要确定什么是正常的流量。这个正常的流量通常是靠逐日积累得到一个滑动平均值。这个值一般叫做基线(Base Line)。

目前可以看到的，在汇聚了一定量主机的网络出口，以一天为一个周期，每天的时间流量曲线具有很好的相似性。工作日和周末、节假日有显著的不同。通过对网络中一些特定流量的长期监控，有助于网管人员了解网络的流量模型，所形成的基准数据可供网管人员正确分析网络使用状况，并可及时发布异常警讯，在故障事件爆发或扩大前实施防范措施，进而提升网络的整体质量及效能。

4. 提高网络资源的利用效率

通过流量监测可以发现信息流动的路由不合理：某些链路很忙而其他链路可能很闲，或者有便宜的路线没有用却用了贵的，等等。因此可以通过修改配置或者网络连接来减少支出，增加收入。通过流量分析，可以为多出口的流量负载均衡、重要链路的带宽设置、路由选择和设定 QoS 等网络优化措施提供数据依据。

通过对与其他网络互联流量的监控，分析网络内部用户访问其他外部网络的业务特

点和主要流量的去向，准确掌握内部用户对外网的兴趣点，找到应用最多的热点信息内容，发现其他的网络资源浪费现象。例如某一地区的用户大量地访问位置很远的某个服务器，意味着该服务器的位置放置不当。根据分析结果进行相应网络内容的建设，将用户感兴趣的热点信息内容放到内部网络，减轻互联链路的压力。

5. 发现和防止网络中的“坏”行为

对网络中的主机、网络业务、使用网络的用户以及网络本身造成损害的行为，统统称其为网络中的“坏”行为。这些行为主要包括攻击、病毒、僵尸网络、垃圾邮件、间谍软件和流氓软件等。网络中的“坏”行为有逐年变化和有增无减的趋势。

发现这些“坏”行为有正面和反面的两种办法。目前专用设备，例如防火墙、杀毒软件和入侵检测设备(IDS)，是通过发现“坏”行为特征的信息流来完成检测。而一般的流量监测设备则通常是通过建立正常流量的基线，从而发现流量的某种异常来确定“坏”行为的出现。这种做法往往能够发现那些最新出现，其特征尚不清楚的“坏”行为，但是往往不能确定是哪种具体的“坏”行为。通过与网络通信正常基线的比对，管理员对出现的异常通信可以快速定性是否为网络安全攻击，确定安全攻击的类型，评估本次攻击的危险程度及可能造成的影响范围，并采用相应技术手段实施事故应急处理。

6. 用户行为分析

针对性营销是目前商界推崇的商业手法，其核心在于了解用户。通过对网络流量数据的积累、分析、挖掘，如用户上网时间习惯、关注的热点内容等，可以了解用户的真正需求，分析出用户的价值和增值点，然后利用网络资源，制定相应的市场营销策略，提升用户对网络的依赖性和忠诚度，进而构建更好的盈利模式。

7. 网络业务分析

目前网络上已经有多种盈利的和非盈利的业务。例如，搜索、门户、游戏、影视、购物、聊天、邮件、电话等。

通过对网络业务的监测，可以了解该业务的主要受众、该业务的最受欢迎部分和最具价值部分等等，根据这些监测结果，可以有针对性地开发有吸引力的业务。

虽然以上列举并不全面，但是已经足够说明网络流量监测的重要价值和意义。

1.2 网络七层协议模型与因特网

本节概述因特网的协议分层结构，简述网络流量监测在因特网协议各层的意义和内容。

网络七层协议模型是指国际标准化组织(International Standards Organization，ISO)制定的一组计算机通过网络互连的开放标准(Open System Interconnection，OSI)。网络七层协议模型如下：

(1) 物理层:定义通过网络设备发送数据的物理方式,作为网络媒介和设备间的接口。

(2) 数据链路层:定义操作通信连接的程序,封装数据包为数据帧、监测和纠正数据包传输错误。

(3) 网络层:定义网络设备间如何传输数据,根据唯一的网络设备地址转发数据包,提供流和拥塞控制以防止网络资源的损耗。

(4) 传输层:管理网络中端到端的信息传送,通过错误纠正和流控制机制提供可靠且有序的数据包传送,提供面向连接的数据包的传送,也提供无连接的数据包传送。

(5) 会话层:管理用户会话和对话,控制用户间逻辑连接的建立和挂断,报告上一层发生的错误。

(6) 表示层:掩盖不同系统间的数据格式的不同性;指定独立结构的数据传输格式;数据的编码和解码、加密和解密、压缩和解压缩。

(7) 应用层:定义了用于在网络中进行通信和数据传输的接口-用户程序,提供标准服务,比如虚拟终端、文件以及任务的传输和处理。

OSI 的七层协议体系结构的概念清楚,理论细致完整,也许就是因为太细致、太完备了,世界上没有几个网络通信协议完全满足这个体系标准。作为目前世界上使用最广泛的因特网上的 TCP/IP 协议,只能和七层协议大致对应,如图 1-1 所示。目前七层协议结构的主要用途是作为一种网络协议分层功能模型的概念标准,方便对于实际存在的网络协议进行分析说明。TCP/IP 协议分为四层网络结构:物理层、网络层、传输层和应用层,不同层次完成不同功能,每一层由众多协议组成。

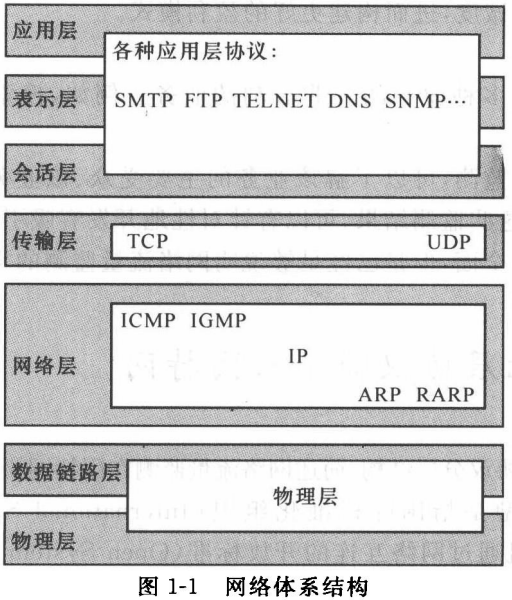

图 1-1 网络体系结构

1. 物理层

用于传送 IP 报文的底层网络，在因特网中被称为物理层。因此它的功能相当于七层协议模型的物理层和数据链路层。

但是，因特网没有定义自己的物理层协议，只是对于起到物理层作用的各种物理网络都定义了承载 IP 报文的方法。其中最为重要的几个包括：以太网、ATM 网、帧中继网以及各种编码格式的物理链路(HDLC、SDH 等)。

数据链路层协议只提供链路传输能力，而网络层协议则具备路由能力。可以看到，因特网物理层不仅包括了各种不同的物理链路，还包括了各种著名的物理网络。这些网络本身都已经提供了网络层功能，而在承载 IP 报文时，却只是作为提供数据链路层能力的网络(简称二层网络)来用，即第 3 层的路由能力往往只是作为灵活调配逻辑链路的手段而已。

目前在骨干网络中使用 MPLS 有越来越普遍的趋势，骨干网中使用 MPLS 都是在 IP 层之上的。但是从其作用来讲，MPLS 仍应归于物理层的范围。这是因为 MPLS 仍然只起到承载 IP 报文的作用，虽然它是在 IP 层上承载。

目前流量监测主要针对 IP 层以上进行。但是，二层网络中除了 IP 报文之外，必然存在二层网络中特有的其他报文，而这些报文必然也占用带宽资源；同时，也存在二层网络中特有的故障和恶意攻击等。因此，对于二层网络的流量监测也同样是必要的。事实上，目前主要作为二层网络使用的以太网、ATM 网、帧中继网以及 MPLS 网，都是网络协议非常复杂的网络。

2. 网络层和传输层

因特网协议网络层包括 IP 协议和其他几个相关协议(ICMP、IGMP、ARP 等)，因特网的名字就来自 IP 协议(Internet Protocol)。因特网协议传输层是指 TCP 协议和 UDP 协议。IP 协议定义了一种不可靠的尽力而为的报文传输机制。TCP 协议在这种机制上提供面向连接的可靠传输能力，UDP 协议在这种机制上提供无连接的不可靠传输能力。同时，这两种协议都在 IP 层之上增加了区分不同会话的能力。这些会话目前往往表示了网络中的不同业务。不同的业务有不同的端口号，一些端口号被定义为周知端口号(Well-known Port Number)，每个号码对应于一种特别的业务。例如，端口 80 被定义为 HTTP 专用端口号码。

传统的流量监测的主要工作全部是在这两个协议层面。在原有的体系框架下面，在这两个协议层面，已经能够得出网络流量监测最关心的一些量。这就是：谁，在网中使用什么业务，流量多大。谁可以用 IP 地址来区分，业务可以用协议类型和端口号码来区分。但是随着网络技术和应用的发展，目前已经有越来越多的应用不再使用端口号码作为区分的依据。

3. 应用层

因特网不对七层协议模型中的会话层、表示层、应用层予以区分。建筑在 TCP 和

UDP 之上的应用层协议同时具备了这三层的功能。大量的应用层协议是因特网的特有优势，是它迅速普及发展的重要因素。例如目前耳熟能详的 HTTP、SMTP、FTP 等，都是著名的应用层协议的例子。

事实上只有应用层流量分析才能得到许多关于网络业务的重要信息。因此应当在这个层面上进行多方面多角度的流量监测。

1.3 宽带网络的构成

经过大约十几年的建设，国内的宽带网络体系结构已经基本定型。几大运营商差别不大，和国际上也基本一致。

每个运营商网络都会使用一个基本的分级结构。包括国家骨干网、省骨干网、城域网、接入网这样 4 个层级，并且基本和行政区划相重合。

1. 国家骨干网

在最高的层级，是国家骨干网，采用全连接的网状网或者部分连接的网状网。它连接了各个省网，并且连接到国际出口和到其他运营商的网络出口。

目前国家骨干网的节点设备都是采用高速路由器。节点间互连一般使用 10 G 或者 2.5 G 速率的 SDH 通道。由国际标准化组织 ITU-T 定义的在 SDH 通道上承载 IP 报文的方法叫做 POS(Packet Over SDH)。

国家骨干网上很少直接使用光纤传送 POS 信号。一般会使用波分复用技术来在一条光纤上传送多路高速 SDH 信号，多条光纤使用环网技术或者交叉连接设备构成 SDH 传输网络，同时向电话网、IP 网和其他各种专用网提供基于 SDH 的数字传输能力。

各个省网到骨干网的连接通常总是多于一条，并且总会连接到不同的城市。目的不只是要增加容量，而且为了保证安全。万一哪一条路断了，仍有其他的路径连接。

同样国际出口和运营商互连接口也都多于一个，并且连到不同的地点，原因和上面一样。这种技术一般叫做双归或者多归。

在国家骨干网上的流量监测主要服务于网络的运行维护和资源调配。例如，各个网络设备和链路的流量负担是否合理；是否有异常的流量现象出现，等等。

2. 省骨干网(省网)

省网就是低一个层级的国家骨干网，省网与国家骨干网不同的地方很少。不过现在有些人在提倡减少网络层级，其中的一个具体做法就是合并省网和国家骨干网。但是这样的话骨干网节点可能太多了一点(如达到 50 个左右)，因此可能还是要分层，例如采用如下方法分层：若干核心节点全互连，其他则有选择地连接到一些核心节点上。

中国的省规模相差太大。发达地区的一个城域网的规模可能大于甚至几倍于一个

一般的省网，因此省网的概念值得推敲。运营商可以根据具体情况采取一些变通的措施，例如一些大型城域网直接接入国家骨干网，甚至一些大型的IDC也可能直接接入国家骨干网。

运营商之间在省级一般没有互连，这使得省网的构造会比国家骨干网简单。但是这对于用户和资源利用来讲不是很好，比如天津网通的一个用户连到天津电信的一个服务器，需要从天津到北京再到天津兜一个大圈子，而这个服务器也许就在隔壁。

单纯就省网来说，流量监测的目的和国家骨干网应当是一样的。但是由于内部管理体制的关系，省网的流量监测可能会涉及更复杂的内容，特别是经营分析需要的一些内容。

3. 城域网

城域网很复杂，不像国家骨干网和省骨干网只使用路由器作为节点设备，城域网设备种类很多。同时，一个城域网内往往可能连接几十万甚至上百万用户，而一个骨干网的外连线路最多不会超过百这个数量级。因此，城域网内往往还要再分级。因此把城域网中的接入网分出去，另外作为一段。而城域网中除了接入网之外的部分，就叫做城域骨干网。但是这样分了以后，城域骨干网就成为了一个纯路由器网络，和省网也就大同小异了。

城域网和骨干网的一个重要不同是：一个运营商非常可能建设几个不同的宽带骨干网，用来提供不同的业务质量等级服务；但是建设几个宽带城域网的可能性是极小的。因此，下一代城域网必须能够区分不同的业务、提供不同的质量等级，这导致它的复杂性。

4. 接入网

所谓接入网是指骨干网到用户终端之间的所有设备。其长度一般为几百米到几千米，因而被形象地称为“最后一公里”。由于骨干网一般采用光纤结构，传输速度快，因此，接入网便成为了整个网络系统的瓶颈。目前宽带网络的接入方式主要有DSL、LAN、Cable Modem三种。

美国的Cable Modem用户很多。但是在中国，DSL占据大部分。以ADSL为例，从家里的PC开始，它经过一个ADSL Modem连接到电话线，许多条电话线在运营商的端局连接到一个集中器设备，该设备叫做数字用户线路接入复用器(Digital Subscriber Line Access Multiplexer，DSLAM)。可能有数百条线路连接到DSLAM，而它使用100 M或者GE LAN连接到它的上一个设备，这个设备通常叫做接入服务器(BAS或者BRAS，Broadband Access Server或者Broadband Remote Access Server)，BAS通常连到一台三层交换机，至此接入层结束。BAS也可以用其他方式连接到网络，这里不再赘述。

上面讲的是家庭用户的宽带网络接入方式。企业或者单位，内部有一个计算机网络的，通常是使用专线接入，因此不需要DSLAM和BAS。

和骨干网不同，接入网总是采用双归的树形结构。各个DSLAM之间的通信量总是