<<网络流量监测与控制>>

图书基本信息

书名：<<网络流量监测与控制>>

13位ISBN编号：9787563520985

10位ISBN编号：7563520988

出版时间：2009-9

出版时间：北京邮电大学出版社

作者：刘芳 编

页数：216

<<网络流量监测与控制>>

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、UDO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 Strearn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。

<<网络流量监测与控制>>

内容概要

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。

<<网络流量监测与控制>>

书籍目录

章节摘录

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1P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。

<<网络流量监测与控制>>

版权说明