网络监测基础与实战

颜东成　韩玉宁　等编著

深入介绍网络监测和管理所涉及的基础知识和概念

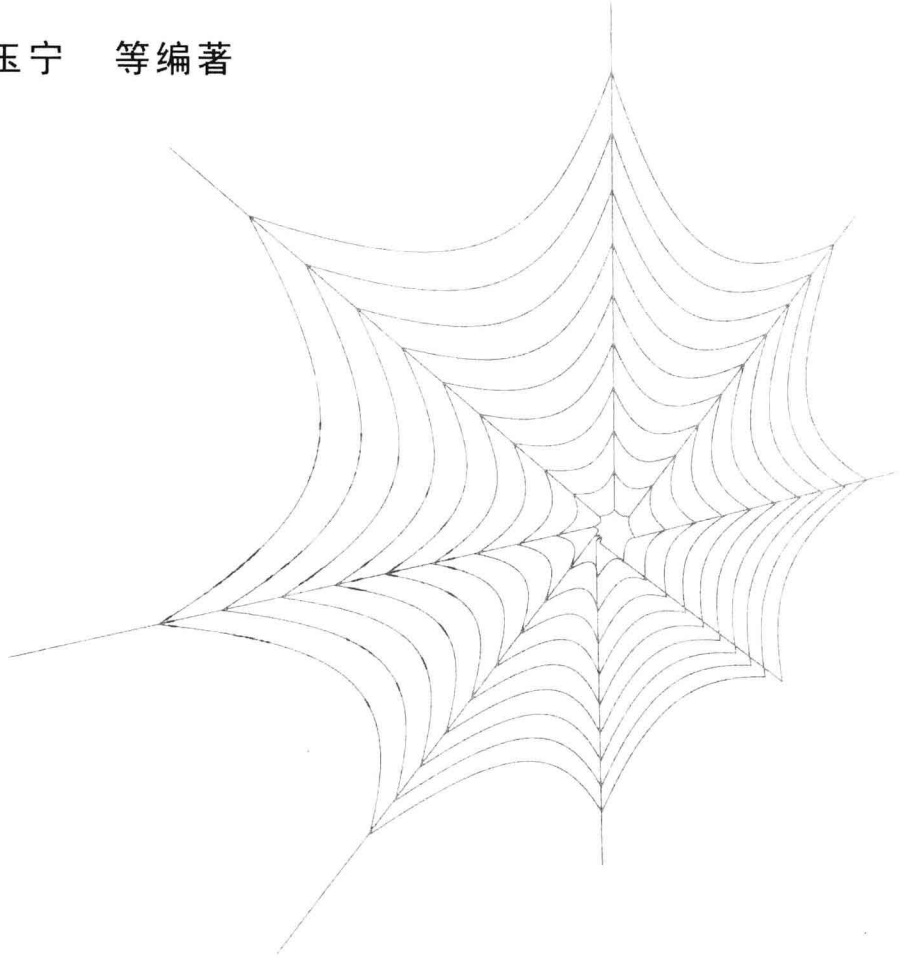
详细介绍WhatsUp Gold、PRTG、Wiki Syslog三款监测软件的使用

实现网络设备级监控、网络出入口流量监测及网络运行日志管理和分析

清华大学出版社

网络监测基础与实战

颜东成　韩玉宁　等编著



清华大学出版社
北　京

内 容 简 介

本书介绍了网络监控技术的基础知识，并且以三款主流软件为平台重点介绍了网络管理和监测中的设备级监控、网络整体流量监控、运行日志分析和管理三个层面的应用。

本书第1～4章主要介绍网络监测和管理所涉及的基础知识，包括各类网络接口、交换机和Vlan知识、路由器和配置模式、防火墙和DMZ结构、网络协议和管理应用等。这些内容大多都是以实际应用和具体操作进行介绍的，为读者后续的学习打好基础；第5～12章以IpSwitch WhatsUp Gold、PRTG、Wikis Syslog三款网络管理软件为平台讲解网络设备级监控、网络整体流量监控、运行日志分析和管理等内容。这三款软件广受好评，使用广泛，功能齐全，能够实现对网络的全面监控并保障网络稳定、健康地运行。

本书内容全面、讲解详细，从基础知识到实际应用大多都配合实例讲解，本书适合所有网络维护人员和管理人员阅读；可作为了解网络监测技术和熟悉网络监测工具的教材，对于从事网络安全工作和网络管理软件开发的人员，本书也具备较高的参考价值。

图书在版编目（CIP）数据

网络监测基础与实战 / 颜东成，韩玉宁等编著. —北京：清华大学出版社，2011.9
ISBN 978-7-302-26160-5

Ⅰ.①网…　Ⅱ.①颜…　②韩…　Ⅲ.①网络管理软件　Ⅳ.①TP393.07

中国版本图书馆CIP数据核字（2011）第136038号

责任编辑：夏兆彦
责任校对：徐俊伟
责任印制：杨　艳
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62795954，jsjjc@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：三河市李旗庄少明装订厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：26.25　**字　数**：659千字
版　　次：2011年9月第1版　　**印　　次**：2011年9月第1次印刷
印　　数：1～3000
定　　价：49.50元

产品编号：040704-01

前　言

随着网络和计算机技术的不断发展，各行各业都越来越多地依赖于网络和计算机。人们使用网络和计算机办公、交易、娱乐、通信、商业应用等，这对网络及其设备提出了更高的稳定性和高效性要求。另外，随着网络和计算机设备中承载的业务越来越多，网络日益庞大，结构也趋复杂，网络设备种类也越来越繁多，非法攻击和入侵也日益增多……这些都是网络管理中所要面临的问题。这就要求在监测和管理好网络的前提下，还需要分析和优化网络，发现网络中存在的隐患，把握网络运行的趋势，确保网络运行的持续和健康。

想要管理好网络和设备，必要的监测技术和手段不可或缺。然而国内图书市场上还找不到一本专门介绍网络监测的书籍，特别是对于设备状态监测工具 WhatsUp Gold 和网络流量分析工具 PRTG 的介绍更是鲜见。本书便是基于这个原因而写作，以填补这方面的空白，为网络管理和维护、网络安全等从业人员提供帮助。

本书内容可以分为两篇。具体介绍如下：

第 1 篇包括第 1～4 章，主要介绍网络维护和监测的基础知识。具体内容包括物理层硬件接口和 IP 地址、常见的网络设备的维护和管理、常用的网络协议的概念及应用、网络管理的基础架构和原理等知识。本篇内容都较为注重具体应用的介绍，可以为网络维护和监测技术的学习奠定良好的基础。

第 2 篇包括第 5～12 章，主要介绍 IpSwitch WhatsUp Gold、PRTG、Wiki Syslog 这 3 款广受好评、使用广泛、功能齐全的网络维护和监测软件，以实现对网络中不同层面、不同对象、不同系统的管理和监测。具体内容包括 WhatsUp Gold 安装和快速上手、设备发现及报警设置和属性详解、信息采集和网络状态监测实例、Web 界面及报表应用详解、PRTG 安装及配置流量监测、PRTG 功能及设置项详解、Kiwi Syslog 安装及设备配置、Kiwi Syslog 功能与程序配置等。通过这 3 款软件，可以实现网络的管理和架构，更为重要的是可以实现网络的各方面监控、重要信息的采集、流量的监控和统计、日志信息的收集和分析等，帮助您管理好网络，迅速发现和处理故障，让您的网络处于健康的运行状态。

本书涉及的 3 款网络管理和监测软件简单介绍如下：

IpSwitch WhatsUp Gold：网络设备监控程序。该软件为网络设备及主机监控的领导品牌。IpSwitch 的分销网络遍及世界 44 个国家和地区，全球有超过 100 000 个网络在使用该系统。在中国，IpSwitch 网络管理软件在政府、制造、电信、金融、能源、医疗、教育及其他行业也拥有近万个用户。该系统功能丰富，易用性强，响应及时，广泛地支持各类网络设备，提供强大的网络监控、网络拓扑管理、多种方式的故障报警及全面的数据报表，帮助您实时掌握网络状态，保障设备的正常运行。

PRTG（Paessler Router Traffic Grapher）：流量监控软件。该软件是德国软件公司 Paessler

的主打产品，是一款用于获取流量资讯并产生图形化报表的软件。其功能强大，已成为流量监控的代表软件。通过 PRTG 能够打造专业的网管平台，为网络管理员提供带宽使用情况和网络设备的当前和长期使用趋势信息，帮助管理员查找网络故障，分析网络的升级方向。

Wiki Syslog Deamon：日志管理程序。改软件采用目前较为通用的 Unix/Linux Syslog 日志格式进行日志信息管理和记录，通过配置 Windows、Linux 操作系统和各类网络设备，它能够广泛收集各类日志信息，实现日志信息的集中管理。Wiki Syslog Deamon 还能够按照日志信息的产生来源、重要级别等进行分类管理，从而帮助网络管理员从海量的日志信息中甄别出实用和有效的日志记录，用于分析网络运行状态和故障原因，辅助调整和优化网络结构。

本书中介绍的 3 款软件面向的对象不同，分工也不同，可以配合一起使用，也可以根据网络实际情况使用其中之一。通过掌握这 3 款软件的使用，能协助网络管理员轻松管理好网络。书中除了对 3 款软件的介绍外，还介绍了网络协议及常用服务等基础知识，例如 SNMP 协议、传输协议、Exchange Server 服务、SQL Server 服务、WMI 等，以帮助网络管理员了解和熟悉网络管理及监测技术。

本书主要由颜东成、韩玉宁编写，其他参与编写的人员有李甘、甘昕艳、唐景丽、王焕如、梁宁、陈兴龙、唐晓年、兰天莹、余兰、甄翠明、陈中全、朱寿华、潘龙江、陈晓莹、唐志、张小宁、潘元真、邝燕、麦品芝、龙丽坤。在此对他们的辛勤工作表示感谢！

感谢家人对本书写作的大力支持！感谢公司领导和同事给予的关注！也感谢清华大学出版社的领导和编辑对本书出版的大力支持！没有你们的支持，本书不可能顺利出版。

本书作者

目　录

第 1 篇　网络监测必备基础知识

第 2 篇 网络监测实战

第 1 篇　网络监测必备基础知识

第 1 章　网络接口及 IP 地址介绍

本书所介绍的网络管理和监测方式，包括网络接口状态、硬件设备运行情况、端口流量统计、协议及服务状态等，其中将涉及很多物理层的基础知识，包括传输介质、各类硬件设备接口、常用的端口、网络协议等，在前三章中将一一对这些网络管理员应知应会的基础概念进行介绍。

尽管这些网络基础概念非常普遍，但仍有一些较模糊的概念和值得注意的细节需要网络管理员明确。本章主要介绍网络传输介质、常见接口以及 IP 地址相关知识，通过对本章内容的学习，网络管理员应认识和熟悉各种常见物理层组件，理解 IP 地址的相关概念和应用。

1.1 物理层传输介质介绍

最常用的网络传输介质包括双绞线、同轴电缆、光纤等。以下将介绍这三大类传输介质的概念、属性、分类等情况，以加深对这三类传输介质的认识。首先介绍双绞线。

1.1.1 双绞线

双绞线电缆最早在 1881 年被用于贝尔发明的电话系统中。由于其价格低廉、布线方便、抗干扰性强以及传输距离远等特性，双绞线得到很大的发展，目前已经成为应用最为广泛的网络传输介质，主要应用于局域网网络连接和电话线路连接。

双绞线可分为 STP（Shielded Twisted Pair，屏蔽双绞线）与 UTP（Unshielded Twisted Pair，非屏蔽双绞线）两大类型。屏蔽双绞线在传输线和外层绝缘保护套之间增加了一层金属网屏蔽层，比非屏蔽双绞线有更高的传输性能和抗干扰性。在百米范围内，屏蔽五类线传输速率可达 155Mbps，而普通五类线最高速率约 100Mbps。

一般地，在楼宇内布线，通常使用较为柔软的普通非屏蔽双绞线即可。而在户外、需防止信号外泄、对信号有更高速率等场合才使用屏蔽双绞线。

屏蔽双绞线和非屏蔽双绞线的结构如图 1-1 所示。

图 1-1　屏蔽双绞线和非屏蔽双绞线

1. 双绞线的分类

双绞线按照不同的技术标准可分为一类、二类、三类、四类、五类、超五类、六类、七类双绞线。一类和二类双绞线最早用于电话语音传输，由于电气性能差、传输速率低已被淘汰。目前较为常用的是超五类和六类线。以下介绍三类以上的双绞线。

三类线：网线外层标识为 Cat3，可提供最高 10Mbps 的速率，曾普遍应用于 10M 以太网中。目前除了传统的语音系统仍然使用三类双绞线以外，其他地方已不再使用。

四类线：标识 Cat4，相比于三类线，四类双绞线在传输性能上有所改进，在距离和速率方面均有所提高。百米的距离内最高支持 16Mbps 的传输速率，主要用在以前旧的 10M 或 100M 以太网中。

五类线：标识是 Cat5，主要用于语音传输和最高速率 100Mbps 的数据传输，广泛应用于百兆或千兆速率以太网。五类线由四对绝缘的铜导线绞在一起构成，但实际的传输中，五类线只使用了其中的两对线，分别是第 1、2、3、6 四根线，剩余的四根线一般不用。

注意： 在双绞线中，一般线序 1、2 用于发送数据，3、6 用于接收数据，4、5 用于传输语音，7、8 用于传输电源。

超五类线：标识为 Cat5e，是目前市场的主流产品。超五类线在传输性能上有更大幅度的提高，具有更高抗干扰性、更小时延误差和串扰低等优势。在百米范围内，其最高传输速率可达 155Mbps，主要用于千兆位以太网中。超五类线在外形和结构上与五类线非常类似。不同的是，超五类线中同时使用四对铜导线，以全双工模式传输。而五类线仅使用两对线，以半双工模式传输。因此，超五类线能够应用于千兆高速网络。

六类线：标识是 Cat6，与五类线最大的区别在于带宽和传输速率的不同。百米范围内，六类线能够提供高达 1000Mbps 的传输速率，适用于千兆高速网络。六类线在外形和结构上与五类线也有所区别，六类线增加了绝缘的十字塑料骨架，将四对导线分别卡入十字骨架的四个凹槽内，使线对之间保持一定空间和相对位置，以降低串扰，大幅提高综合性能。六类线已成为中高端市场中的主流代表产品。普通非屏蔽五类线和六类线如图 1-2 所示。

图 1-2　非屏蔽五类线和六类线

七类线：七类线是一种屏蔽类双绞线，其每一对导线都有单独的屏蔽层，导线之外还

包含整体屏蔽层，其传输速率最高可达 10Gbps，主要是为了适应万兆以太网的发展要求，其接口与目前的 RJ-45 接口并不兼容。

注意：在描述双绞线性能参数时，常用到两个容易混淆的概念，即传输频率和传输速率。传输频率即带宽（单位为 MHz）是描述单位时间内信号振荡的次数；而传输速率（单位为 Mbps）表示的是单位时间内传输的二进制的数量。这两个单位为截然不同的概念，如六类线传输频率为 250 MHz，最大传输速率达到 1000 Mbps。

2. 直通线、交叉线和反转线

双绞线按照两端线序的不同，可分为直通线和交叉线。直通线两端遵循相同的标准线序（586A 或 586B 标准）。而交叉线两端线序不同，一端是 586B，另一端是 586A。两种线序标准排列如下：

- 568B 线序从左到右为 1 橙白、2 橙、3 绿白、4 蓝、5 蓝白、6 绿、7 棕白、8 棕；
- 568A 线序从左到右为 1 绿白、2 绿、3 橙白、4 蓝、5 蓝白、6 橙、7 棕白、8 棕。

一般地，同种类型设备之间使用交叉线连接，不同类型设备之间使用直通线连接。例如交换机与交换机之间使用交叉线连接，计算机与交换机之间使用直通线连接。但随着交换技术的发展，目前大多计算机网卡和交换机、路由器设备端口均支持端口自动翻转技术（Auto MDI/MDIX），能够自适应两种线序。也就是说，局域网任意设备之间互联，均使用同一标准线序可以正常连接，通常使用 586B 线序。

注意：在端口不支持 Auto MDI/MDIX 时，或者一些需要特殊设备，如 VPN、防火墙等，就应该注意在同类型设备互联时应采用交叉线连接。

1.1.2 同轴电缆

同轴电缆以硬铜线为芯，外包一层绝缘材料。这层绝缘材料用密织的网状导体环绕，网外又覆盖一层保护性材料，其结构如图 1-3 所示。

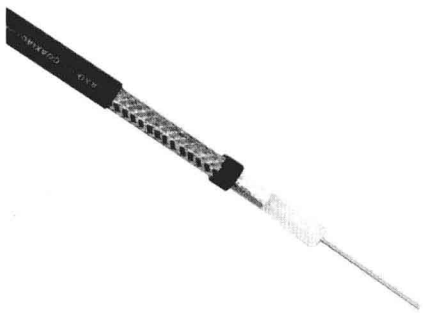


图 1-3 同轴电缆线结构

同轴电缆从用途上分可分为 50Ω基带同轴电缆（即网络同轴电缆，用于传送数字信号）和 75Ω宽带同轴电缆（即视频同轴电缆，可用于模拟和数字信号传输），分类如图 1-4 所示。

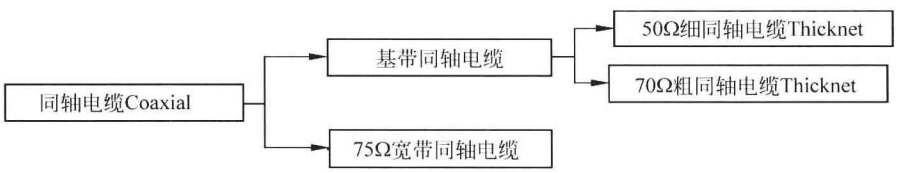


图 1-4 同轴电缆的大致分类方式