SNMP,

SNMP v2,

SNMP v3,

RMON 1，2

SNMP 网络管理

William Stallings／著　　胡成松 汪凯／译

Addison-Wesley

中国电力出版社
www.infopower.com.cn

SNMP,

SNMP v2,

SNMP v3,

RMON 1，2

SNMP 网络管理

William Stallings／著　　胡成松 汪凯／译

中国电力出版社

内 容 提 要

这是一本全面介绍 SNMP 的经典书籍。SNMP 是在网络技术和规模高速发展的今天，业界的网络管理和维护的标准化标准。

本书详细论述了基于 SNMP 的网络管理技术，包括网络管理概念、SNMP 的功能和发展、SNMP 管理信息结构和管理信息库、网络安全常识和 SNMP 各版本的协同工作问题。

本书结构严谨、内容丰富，适合网络管理、设计人员阅读，也可作为数据处理和数据通信专业的教程和参考书。

图书在版编目（CIP）数据

SNMP 网络管理/（美）斯大林编著；健莲科技译. - 北京：中国电力出版社，2001

ISBN 7-5083-0646-5

Ⅰ.S… Ⅱ.①斯…②健… Ⅲ.计算机网络 - 管理 Ⅳ.TP393.07

中国版本图书馆 CIP 数据核字（2001）第 034206 号

中国电力出版社出版、发行

（北京三里河路 6 号 100044 http://www.infopower.com.cn）

三河市实验小学印刷厂印刷

各地新华书店经售

*

2001 年 9 月第一版 2001 年 9 月北京第一次印刷

787 毫米×1092 毫米 16 开本 29 印张 658 千字

定价 49.00 元

前　言

随着计算机和数据网络技术的迅猛发展，以及供应商提供的设备和网络多样性的爆炸性增长，组织机构对信息处理的需求也日益增长起来。组织机构仅仅依赖于单个供应商和相对简单的结构来满足需求的日子已经一去不复返了。这个世界不再被分为纯基于大型机、与 IBM 兼容的集中式环境和基于 PC 机、单 LAN（Local Area Network，局域网）类型的分布式环境。今天典型的组织拥有一个大型可扩展的但无固定形式的结构，由网桥和路由器支持着各种各样的 LAN、WAN（Wide Area Network，广域网）和各种各样的分布式计算服务和设备，包括 PC 机、工作站和服务器组成。另外，尽管有二十多年的溢美之词，该大型机也应用于众多的分布式配置和一些集中式配置中。

为管理这些规模和多样性继续增长的系统和网络，需要有一套自动化的网络管理工具和程序。在多供应商环境下，这些工具和程序的操作基础是与网络管理相关的信息表达和交换的标准化技术。

为和这些需求相适应，管理员和用户都需要求助于一个标准：SNMP（Simple Network Management Protocol，简单网络管理协议）和相关的 RMON（Remote Network Monitoring，远程网络监视）规范。SNMP 最初于 80 年代末期制定并很快成为多供应商环境下网络管理的标准方法。然而，由于限制太多，SNMP 不能胜任所有的关键性网络管理的需要。作为必不可少的网络管理工具，SNMP 已经做了三次改进并完善了其功能。

首先，基于 SNMP 的 RMON 规范发布于 1991 年。RMON 于 1995 进行了修订，RMON 的增强版发布于 1997 年，称作 RMON2。RMON 定义了管理远程 LAN 的算法和数据库。其次，被称作 SNMPv2 的 SNMP 增强版，发布于 1993 年并于 1995 年进行了修订，SNMPv2 比原来的 SNMP 版本功能更多、效率更高。最后，SNMPv3 发布于 1998 年。SNMPv3 为当前及以后的 SNMP 版本定义了整体的框架结构，并为 SNMP 增加了安全特性。本书讲述 SNMPv1、SNMPv2，以及 RMON1 和 RMON2 的最新版本，同时也讲述新的 SNMPv3，这些版本都正在被使用。

目标

为有效管理现有的系统和明智地规划将来要使用的网络管理系统，系统管理员需要理解网络管理技术并深入理解现有的和发展中的标准的细节，本书的目的正是如此。

本书详细介绍了基于 SNMP 的网络和互连网络的管理知识。本书的第一部分为网络管理技术概论，使读者能够把各种供应商的产品放到需要的环境中去。第二部分讲述现在仍被广泛使用的一系列 SNMP 标准。第三部分讲述 RMON1 的修订版和功能扩充的增强版 RMON2。第四部分讲述 SNMPv3。SNMPv3 提供了和 SNMPv1、SNMPv2 一起使用时的安全特性。与这些标准应用相关的实际问题和基于这些标准的产品也在各部分一起讲述。

适合读者

本书是为对网络管理感兴趣的广大读者编写的，这些读者包括：

● 数据处理和数据通信专业的学生以及专业人士：本书可以作为该领域的基础教程和参考书。

● 网络管理设计以及实现人员：本书讨论关键性的设计内容并探索满足通信要求的一些方法。

● 网络系统管理员以及用户：本书试图帮助读者理解在网络管理工具中需要什么样的特性和结构，并讲述了关于现有的以及发展中的标准信息，从而使读者能够评价某一供应商产品的具体性能。

致　　谢

在此感谢 IBM 的 Uri Blumenthal，他提供了许多真知灼见并解答了一些关于 SNMPv3 的问题。

在这里我还要感谢以下各位审阅者，他们慷慨地对本书第二版部分章节甚至是整本书提出了宝贵的反馈意见：AT&T 公司的 K. K Ramakrishnan、Technically Elite Concepts 的 Russell Dietz、FTP 软件公司的 Ravi Prakash、Cisco 公司的 Ole Jacobsen、Research Libraries Group 公司的 Cliff Baker、Cisco 公司的 Sandra Durham，以及 Cygnus 公司的 Ian Taylor。另外，RMON2 的两位主要作者，Bierman Consulting 公司的 Andy Bierman 和 AXON 网络公司的 Robin Iddon，也提供了对 RMON 的详细述评。

除此之外，非常感谢下面各位阅读了本书的原始提纲和早期的手稿：BBN 公司的 Lyman Chapin、Novell 公司的 Radia Perlman、Midnight 网络公司的 Glen Glater、Christopher Heigham 和 Peter Schmidt。

译　者　序

随着 Internet 的出现和发展，网络技术的迅猛发展已经使得网络规模更加庞大、结构更加复杂、支持的用户更多，同时也提供更多的服务，人们越来越意识到网络管理的重要性。但是，只有通过适当的网络管理，功能强大的网络才能得到充分利用，因此有效的网络管理性能已经成为评价网络的一个重要指标。如何用经济有效的办法把来自多个供应商和运营者的网络部件装配成一个完整的网络，并使所有的网络部件不仅能协同工作，还必须便于作为一个统一整体资源来操作和维护，这已经成网络拥有者面临的巨大挑战。要迎接这种挑战，就要使用一种集成管理方式，并使之标准化，这是一条必经之路。当前被业界普遍接受的是 SNMP，到目前为止，SNMP 实际上已经成为一个标准。

本书分五部分详细论述了基于 SNMP 的网络管理技术。第一部分是网络管理技术概论，对当前网络管理技术作了一般性的介绍，从而使读者能够把各种现有产品和自己所在的环境对应起来。第二部分讲述了现在仍被广泛使用的 SNMP 最初标准，也就是 SNMPv1。第三部分讲述 RMON1 的改进版以及扩充了 RMON1 功能的 RMON2。第四部分讲述 SNMPv2，详细介绍了 SNMPv2 协议及其最新的管理信息结构和管理信息库。第五部分介绍了网络的安全常识和 SNMPv3，后者和 SNMPv1 和 SNMPv2 一起使用，为 SNMP 提供了全新的安全特性，也为将来 SNMP 的发展创建了一个整体框架。本书最后有两个附录，介绍了 TCP/IP 协议组和 ASN.1（第一抽象语法表示）。同时全书 17 章中还包含有 13 个章后附录，介绍了各章中所涉及到的一些相关知识或协议规范。

作为一名网络顾问或网络管理员，在安装完网络并且设置了用户账号与应用程序之后，你的工作并没有结束，您的下一个任务就是网络管理，它就好像是一场永远也不会结束的战斗。本书就是为这样的网络管理员所准备的，同时，那些协议设计和实施人员以及所有对网络管理感兴趣的读者都会受益匪浅，我相信本书将是每一位读者的必备参考书。

由于书中所介绍的最新 SNMPv3 发表于 1998 年，国内介绍得不多，有些术语没有统一的翻译，我尽量参考了一些流行的译法，并且都附上了对应的英文，便于读者阅读参考。同时，虽然该书已经是第三版，堪称是该类书籍中的经典之作，但仍然有一些小错误，译者都一一给出了注解，便于有条件的读者与该书原版进行对照阅读。由于译者水平有限，书中错误在所难免，希望读者能够提出自己宝贵的意见，您可以通过 snmp@eyou.com 直接和我联系。

目　录

第一部分　网络管理基础

第二部分　SNMPv1

第三部分 RMON

第四部分 SNMPv2

第五部分 SNMPv3

附　录

第1章 概 论

网络和分布式处理系统变得日益重要，事实上已经成为商业领域中的主要部分。在特定的组织机构内部，愈来愈大、愈来愈复杂的网络用于支持更多的应用程序和更多的用户。由于网络规模上的增长，有两点已经变得很明显：

- 网络与它相关的资源和分布式应用程序对该组织机构来说必不可少。
- 更多可能出错的情况使得网络或网络的一部分不能工作，或是把网络的性能降低到不可忍受的程度。

一个大型的网络不可能放到一起并仅由一个人进行管理。这种系统的复杂度说明需要自动化的网络管理工具。如果网络里包含有多个供应商提供的设备，需要这种工具的迫切性便随之增加，同时提供这种工具的难度也随之增加。

由于网络装置变得愈来愈大、愈来愈复杂、愈来愈富于变化，使得网络的管理费用随之增加。为了控制费用，需要使用标准工具，使其能够应用于更多的产品类型，包括终端系统、网桥、路由器和电信设备以及可用于多供应商环境中的设备。正是为了满足这种需要，SNMP（Simple Network Management Protocol，简单网络管理协议）发展起来，它提供了一种对多供应商、可协同操作的网络管理工具。

SNMP 实际上是指网络管理的一系列标准，包括协议、数据库结构定义和一系列数据对象。SNMP 在 1989 年作为基于 TCP/IP 互联网的标准而被采用并受到广大用户的欢迎。1991 年发布了 SNMP 的一个补充：RMON（Remote Network Monitoring，远程网络管理）。RMON 扩充了 SNMP 的功能，包括对 LAN（Local Area Network，局域网）的管理以及对依附于这些网络的设备的管理。1993 年，SNMP 的升级版，也被称作为 SNMPv2（SNMP 第二版）被提了出来，SNMPv2 在 1995 年发布。SNMPv2 增强了 SNMP 的功能，并规定在基于 OSI 的网络中使用 SNMP。同在 1995 年，RMON 扩展成为 RMON2。最后，在 1998 年发布了 SNMPv3。这一系列文档定义了 SNMP 的安全性，并定义了将来改进的总体结构。SNMPv3 预定与 SNMPv2 的功能一起使用，但也可以和 SNMPv1（SNMP 的最初版本）一起使用。

本书致力于研究 SNMP、RMON 1、RMON 2、SNMPv2、SNMPv3 和与每一个协议相关的实际问题。本章的其余部分和以下两章，从总体上对网络管理进行了概述。

1.1 网 络 管 理 须 知

表 1-1 列出了 ISO（International Organization for Standardization，国际标准化组织）定义的网络管理的关键功能。尽管这种功能划分是为 OSI 环境开发的，但已被标准和非标准的网络管理系统所广泛接受。这种分类为我们对必要条件的讨论提供了一种有用的方法。

表 1-1　OSI 管理功能分类

故障管理
探测、隔离和修正 OSI 环境下的不正常操作功能
计费管理
建立对被管理对象的使用计费并识别使用被管理对象的功能
配置和名称管理
为辅助提供互连服务的连续操作，执行控制、识别、从被管理对象采集数据以及向被管理对象提供数据的功能
性能管理
对被管理对象的行为和通信活动的效率进行评价所需要的功能
安全管理
正确操作 OSI 网络管理和保护管理对象等基本的 OSI 安全方面的功能

1.1.1　故障管理

1．综述

为维持一个复杂网络的正常操作，必须把该系统作为一个整体来处理，每一个重要的组件都要能正常工作。当故障（fault）出现时，有必要尽快：

- 精确确定故障发生的位置。
- 把其余的网络同故障部分隔离开来，使其余的网络不受干扰继续工作。
- 不使用该组件，重新配置或修改网络，尽量减少该操作的影响。
- 修复或替换故障组件，恢复网络到初始状态。

故障管理定义的核心是故障的定义。故障有别于错误（error）。故障是指需要管理关注（或操作）来修复的不正常状态，而错误是一个简单的事件。故障通常由不能正常操作或过多的错误来表示。例如，如果通信线路被割断了，任何信号也不能通过；或是电缆里的皱痕使得信号失真而出现持续的高位错误率。一些错误（例如，通信链路的单个位错误）会不时地发生，一般不认为它们是故障。在通常情况下，用各种协议的错误控制机制来补偿错误。

2．用户要求

终端用户期望快速而可靠的问题解决方案。大多数用户能忍受偶尔发生的故障，但如果故障经常出现，终端用户一般会希望能马上收到通知并希望能立即解决问题。提供这种级别的故障解决方案需要非常快速而且可靠的故障探测和诊断管理功能。可以通过使用冗余组件和备用通信路由，给予网络一定程度上的“故障容错”能力，从而使故障的影响和持续时间减到最小。为增加网络的可靠性，故障管理能力本身就应该是冗余的。

用户希望获知他们网络状态，包括预定和非预定的维护工作。通过置信度测试或转存对象、日志、警告或统计数据的分析等机制，用户希望对网络的正确运行放心。在修正故障和完全恢复网络到运行状态之后，故障管理服务必须确保该问题已经真正解决，不会产生新的问题。这种需求称作问题跟踪和控制。同网络管理的其他领域一样，故障管理应该

对网络的性能产生最小的影响。

1.1.2 计费管理

1. 综述

在许多企业网络中，一个部门或成本中心，甚至一个项目账号都因为使用网络服务而需要计费。这些是内部计费程序，而不是真正的现金交易，但对分享网络资源的终端用户来说是非常重要的。进一步来说，即使不使用这些内部计费程序，网络管理员也需要跟踪终端用户对网络资源的使用，一般包含以下几方面的原因：

- 终端用户或终端用户组可能滥用他们的访问权限并以其他终端用户为代价而加重网络的负担。
- 终端用户可能不知道如何有效地使用网络，网络管理员可以通过改变程序来提高网络性能。
- 如果对终端用户活动充分了解，网络管理员便处于一个较为有利的位置来计划网络的发展。

2. 用户要求

网络管理员要能设定在各种各样的节点上记录计费信息的种类、向上一级管理结点发送信息的时间间隔和在计算费用时所用的算法。计费报表应该在网络管理控制下生成。

为了限定计费信息的访问权限，计费工具必须提供验证终端用户访问权限的功能并能对计费信息进行操作。

1.1.3 配置和名称管理

1. 综述

现代数据通信网络由单个的组件和可配置成执行许多不同应用程序的逻辑子系统（例如在操作系统中的设备驱动程序）所组成。例如，同样的设备可以配置成路由器或者终端系统，或者兼而有之。一但确定了如何使用某一设备，配置管理员便可以选择合适的软件并为该设备设定属性和一些参数（例如传输层重发计时器）。

配置管理是和初始化网络以及正常关闭网络或网络的一部分联系在一起的，它也和维护、添加、更新组件之间的关系以及网络操作中组件本身的状态有关。

2. 用户要求

对网络的启动和关闭操作是配置管理的具体职责，通常，希望能在无人管理的情况下执行对某些组件的这种操作（例如启动或关闭网络接口单元）。网络管理员需要能够确定最初网络所应包含的组件并定义这些组件之间既定的连接关系。如果经常用同样或相似的资源属性来配置网络，就需要一种方法来定义或修改默认的属性以及把这些预定义的属性装载到具体的网络组件中去。当终端用户要求改变时，网络管理员需要能够改变网络组件之间的连接关系。在响应性能评价或者为支持网络升级、故障恢复或者安全检查时，经常需

要对网络进行重新配置。

终端用户通常需要或者想要知道他们的网络资源和组件的状态，因此，当配置改变时，应将这些改变通知终端用户。配置报表可以由程序周期性地或者按这种报表的请求而产生。在重新配置之前，终端用户通常想知道新的资源状态和它们的属性，而网络管理员通常只希望授权终端用户（操作员）来管理和控制网络操作（例如软件分发和升级）。

1.1.4 性能管理

1. 综述

现代数据通信网络由许多各种各样的组件组成，这些组件必须相互通信并且共享数据及资源。在某些情况下，对一个应用程序的效率来说，关键是将网络通信限定在某一特定性能之内。

计算机网络性能管理在功能上包含两大类——监视和控制。监视功能是指跟踪网络活动，控制功能是使性能管理可以为提高网络性能而做一些调节。与网络管理员相关的性能管理方面问题是：

- 什么是容量利用等级？
- 流量是否过大？
- 输出输入总和是否减少到不可接受的程度？
- 是否有瓶颈？
- 响应时间是否在增加？

要处理这些问题，网络管理员必须集中监视一些初始的资源集合以便评估网络性能等级，这包含把恰当的方法和数值与相关的网络资源关联起来作为不同性能等级的指标，例如，在传输连接中重发次数就认为是需要关注的性能问题。因此，性能管理必须监视许多资源来提供确定网络操作等级的信息。通过采集、分析这些信息，然后使用合成分析作为预设值的反馈，这样网络管理员便愈来愈熟练地识别指示当前或即将出现的性能下降时的状态。

2. 用户要求

在一个特定的应用程序应用到网络中之前，终端用户希望知道平均和最慢响应时间以及网络服务的可靠性等信息。因此必须有足够的性能信息来评估终端用户的请求。终端用户希望通过管理网络服务为他们的应用程序连续提供理想的响应时间。

网络管理员需要性能统计数据来帮助他们计划、管理和维护大型的网络。性能统计数据在给终端用户带来问题之前就能辨别出潜在的瓶颈，这样就可以采取合适的修正动作。这种动作可以根据在高峰期或通过某一区域的负载快速增加而确认有瓶颈时改变路由表来平衡流量或重新分布流量负载的形式。从长期来看，基于这种性能信息功能的计划可以用来帮助作出正确的决定，例如关于为该区域增加线路。

1.1.5 安全管理

1. 综述

安全管理包括管理信息保护和访问控制工具，其中包含密钥的生成、分发和存储。必须维护并分发密码和其他一些授权或访问控制信息。安全管理同样也关心监视和控制计算机网络访问以及从网络节点上对网络管理信息的访问。日志记录是一种很重要的安全工具，因此，安全管理基本上包含采集、存储并检查审计记录和安全日志记录，以及打开或关闭这些日志记录的工具。

2. 用户要求

安全管理提供工具来保护网络资源和终端用户信息。网络安全工具应该只对授权用户有效。终端用户希望知道适当的安全措施是有效的而且安全工具的管理本身也是安全的。

1.2 网 络 管 理 系 统

网络管理系统是网络监视和控制工具的集合，一般包含有以下一些观点：

- 为执行大多数或全部的管理任务，有一个单一操作接口，这个接口拥有功能强大但用户界面友好的命令集。
- 使用最少数量的专用设备。也就是说，网络管理所需要的大多数软件和硬件都被组合到现有的用户设备中。

网络管理系统由在现有网络组件中所添加的硬件和软件组成。执行网络管理任务的软件存在于主机或通信处理器中（例如，前端处理器、终端簇控制器、网桥、路由器）。网络管理系统设计成把整个网络看作一个统一结构来处理，每个节点都有为系统所知的地址和标签以及每个元素和链接的具体属性。网络的活动元素定期反馈统计信息到网络控制中心。

1.2.1 网络管理配置

图 1-1 显示了网络管理系统的结构。每个网络节点都包含一系列用于执行网络管理任务的软件，在图中被称为 NME（Network Management Entity，网络管理实体）。每个 NME 都执行以下的任务：

- 采集与通信和网络相关活动的统计信息。
- 在本地存储统计信息。
- 响应从网络控制中心传来的命令，包括：

* 把采集到的统计信息传输到网络控制中心

* 改变参数（例如传输协议中使用的一个计时器）

* 提供状态信息（例如参数值、活动连接）

* 产生人工流量来测试网络

- 当本地条件发生显著变化时向网络控制中心发送消息。

网络中至少应有一台主机被设计成网络控制主机或者管理站。除 NME 软件之外，网络

控制主机还包含一系列被称作 NMA（Network Management Application，网络管理应用程序）的软件。NMA 包含一个操作界面，允许授权用户来管理网络，通过显示信息和/或通过发送命令到全网络中的 NME 来响应用户命令。这种通信通过应用程序级别的网络管理协议来执行，该协议以与其他分布式应用程序一样的方式来使用通信结构。

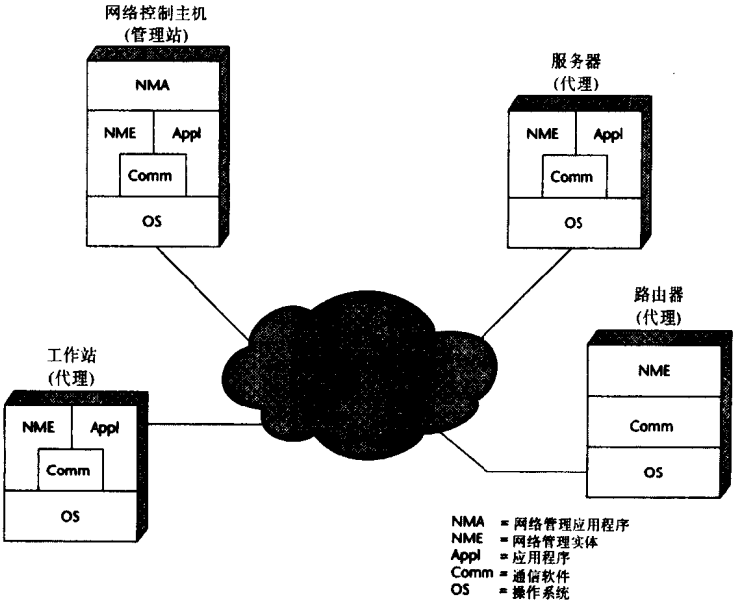

图 1-1 网络管理系统的元素

作为网络管理系统一部分的其他网络节点包含一个用于响应管理站系统请求的 NME，一般被管理系统中的 NME 认为是代理模块（agent module），或简称代理（agent）。代理在终端系统上实现，该终端系统支持终端用户应用程序，也支持提供通信服务的节点，例如前端控制器、簇控制器、网桥和路由器。

下面按顺序观察一下。

- 由于网络管理软件依赖于主机操作系统和通信结构，到现在为止，大多数这类软件都设计为在单一供应商的设备上使用。而近年来，已经出现了为管理多供应商网络而设计的标准化网络管理系统。
- 如在图 1-1 中所描述的，网络控制主机和其他系统中的 NME 通信并控制 NME。
- 为维持网络管理功能的高度可用性，通常要使用两到三台网络控制主机。在普通操作中，一台机器空闲或者只是简单地采集统计信息，而其余的用于控制．如果主要的控制主机出现故障，即可启用备用系统。

1.2.2 网络管理软件结构

管理站或者代理中的网络管理软件的真正结构各不相同，这取决于具体的平台功能和网络管理能力。图 1-2 展示了一种普通的结构。软件可以被分为三大类：

* 用户表示软件