# 精通SNMP

武孟军 编著

37份 RFC文档精华
全面掌握SNMPv1、SNMPv2、SNMPv3、SMIv1、SMIv2、RMON1、RMON2
15项 实验验证
深入理解SNMP、RMON工作机制
12年 网络管理经验的汇集
全面提升网络管理水平

**特色精华**

- ASN.1和ASN.1宏的应用及BER编码
- SMIv1、SMIv2
- MIB文档格式，被管理对象的概念、意义及定义形式
- SNMPv1、SNMPv2通信协议的处理规范
- 实际环境中SNMP通信协议时序、包格式
- SMIv2文本约定、MIB中表之间的关系
- SNMPv3的组成、内部处理逻辑
- SNMPv3的安全机制及其内部处理逻辑
- 实际环境中SNMPv3安全处理机制、抓包分析
- RMON1、RMON2原理及其实际应用演示

人民邮电出版社
POSTS & TELECOM PRESS

# 精通SNMP

武孟军 编著

**37份** RFC文档精华

全面掌握SNMPv1、SNMPv2、SNMPv3、SMIv1、SMIv2、RMON1、RMON2

**15项** 实验验证

深入理解SNMP、RMON工作机制

**12年** 网络管理经验的汇集

全面提升网络管理水平

人 民 邮 电 出 版 社

北 京

**图书在版编目（CIP）数据**

精通SNMP / 武孟军编著. -- 北京 : 人民邮电出版社, 2010.7
ISBN 978-7-115-22912-0

Ⅰ. ①精… Ⅱ. ①武… Ⅲ. ①计算机网络－管理－协议 Ⅳ. ①TP393.07

中国版本图书馆CIP数据核字(2010)第103501号

## 内 容 提 要

本书以RFC文档内容为主线，理论联系实际，全面系统地介绍了SNMP的相关知识，内容包括了ASN.1、SNMPv1、SNMPv2c、SNMPv3、RMON1和RMON2，涵盖了读者学习SNMP从入门到精通所需要的全部知识。通过本书，可以了解SNMP的基本原理，熟练阅读、书写MIB文档，熟练掌握SNMP各个版本的实际应用，全面提高网络管理水平。

本书可以作为网络工程师、网络管理员、网络管理软件开发者和SNMP代理开发者、针对某一产品的MIB制订者学习SNMP的参考资料。

**精通 SNMP**

◆ 编　　著　武孟军
责任编辑　刘　浩
◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街14号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
聚鑫印刷有限责任公司印刷
◆ 开本：787×1092　1/16
印张：25.75
字数：642千字　　2010年7月第1版
印数：1－3 500册　　2010年7月河北第1次印刷

ISBN 978-7-115-22912-0

定价：59.00元

**读者服务热线：(010)67132692　印装质量热线：(010)67129223**
**反盗版热线：(010)67171154**

# 前　言

随着计算机网络的诞生和发展，网络管理也经历了一个从无到有、从初级到高级的发展过程。SNMP 简单网络管理协议，是网络管理人员提高网络管理水平和工作效率必须熟练掌握的知识。

初次接触 SNMP 的人，很容易被它的名字所迷惑，大体上会感觉它是个很简单的协议。介绍网络技术的书中很少提及它，即使有也很简短。但如果真的想深入学习一下，会发现它远不是你所想象的那么简单：SNMP 从 1989 年发布至今，仅版本就有七八个，相关的 RFC 文档多达数百个，且关于 SNMP 的技术仍在发展中，新的建议草案也不断出现。面对困难，许多学习者或半途而废，或囫囵吞枣、了解点皮毛作罢。

其实，真正掌握 SNMP 不仅仅需要读者具备一定的计算机网络知识，还需要了解一些其他方面的基础知识。比如抽象语法标记 ASN.1，编译原理中用到的巴柯斯范式 BNF，SNMPv3 中还涉及密码学和网络安全方面的一些知识。因此，学习 SNMP 不能将它仅仅局限于计算机网络，它已经是一个涉及多学科知识的独立体系。

本书共分 22 章，从读者学习 SNMP 需要的基础知识开始，结合实际，全面、系统地介绍了 SNMP 全部知识，包括 ASN.1、SNMPv1、SNMPv2c、SNMPv3、RMON1 和 RMON2 等内容。整个体系基本上是以 SNMP 不同发展时期的 RFC 知识为主线，介绍关键知识点，结合应用实际，力图向读者讲清楚 SNMP 的前世今生。

第 1～3 章，介绍 SNMP 和 ASN.1 的基础知识。ASN.1 是深入学习 SNMP 的必备知识，不需要精通，但读者至少要了解 ASN.1 是什么，有什么用，在 SNMP 中有哪些应用。该部分要重点掌握 ASN.1 类型定义，宏的概念以及使用，BER 编码规则。

第 4～7 章，介绍 SNMPv1 的内容。该部分应重点掌握 SMI、被管理对象的概念和定义形式、对象标识符的概念和意义、SNMP、MIB 文件的一般格式、被管理对象的组织、概念表、标量对象和列对象、对象类型和对象实例的区别与联系以及标识方法和 MIB-II 中常用的被管理对象等知识。

第 8～12 章，介绍 SNMPv2c 的相关知识。该部分应理解文本约定和一致性陈述宏的意义及使用，重点掌握 SMIv2 的内容，表与表之间的关系，能够读懂遵循 SMIv2 标准的 MIB，并能够根据实际情况，书写简单的 SMIv2 MIB。

第 13～19 章，介绍 SNMPv3 的相关内容。该部分应理解 SNMPv3 实体的体系框架，熟悉消息处理和 PDU 分发过程，重点掌握 USM 和 VACM 的知识。

第 20～22 章，介绍 RMON 的相关知识。该部分应掌握 RMON 的基本工作原理，控制表和数据表的概念和作用，RMON1 的第 1、2、3 和 9 功能组的概念和实际应用，理解其余功能组和 RMON 2 功能组的基本工作原理。

本书可以作为 SNMP 学习者系统的学习教材，或网络工程技术人员的参考资料。读者要求具备基本的网络知识，可以是希望学习掌握 SNMP 全面知识网络工程师、网络管理员、网络管理软

件开发者和 SNMP 代理开发者、针对某一产品的 MIB 制订者等。

作者写作时阅读了大量 SNMP 有关的 RFC 文档和其他相关的资料，并做了许多验证性的实验，全书在阐明 SNMP 基本理论的同时，注重实用性。凡是能够用实验验证的知识点，尽量进行实验。书中所举实例，大部分源自实际的实验环境，少部分从互联网资源中选取。关于 SNMP 的技术术语，除少量不常用的以外，尽量沿用已有的名称。

SNMP 内容繁杂，涉及面十分广泛，由于水平所限，书中的错误在所难免，欢迎读者批评指正（邮箱地址为 book_better@sina.com）。

编者

2010-06-20

# 目　录

# 1 SNMP基础

SNMP是英文Simple Network Management Protocol（简单网络管理协议）的缩写。从狭义上讲，它是一种专门用于网络管理软件和网络设备之间通信的协议；从广义上讲，它是一组为实现网络的自动化管理任务而制订的一系列通行标准，包括了管理信息的表示与命名、通信协议等内容。

SNMP最早是Internet工程任务组（Internet Engineering Task Force，IETF）为解决Internet上的网络设备管理问题而提出的一个临时方案，第一个正式版本在1989年发布，经过二十多年的发展，SNMP日臻完善，目前已经是应用最广泛的一个成熟网络管理标准协议。

## 1.1 网络管理和SNMP

早期的计算机网络规模小，结构简单，因此网络管理活动也相对简单。随着计算机网络技术的迅速发展，网络规模日益庞大，结构也越来越复杂，简单、粗陋的管理方式已经不再适应现代的计算机网络，网络管理必须向高度集中和高度智能化的方向发展。

在此期间，先后出现了多种网络管理标准。最早致力于网络管理标准化工作的是国际标准化组织（International Standards Organization，ISO），它是网络互连协议OSI（Open System Interconnection Reference Model，开放系统互联参考模型）的制订者。ISO制订的第一个网络管理标准为CMIS/CMIP（The Common Management Information Service/Protocol），也是基于OSI模型的，并在当时的网络管理中得到了初步应用。同期出现的其他网络管理协议还有高层实体管理系统HEMS（High Level Entity Management Systems）、简单网关监控协议SGMP（Simple Gateway Monitoring Protocol）等。

随着TCP/IP和Internet的迅速普及，1987年Internet的管理机构IAB（Internet Activities Board）认为有必要为基于TCP/IP技术的网络制订新的网络管理标准。其长期目标是在CMIS/CMIP基础上，制订一套功能完善、适用于TCP/IP协议栈的网络管理协议CMOT（Common Management Information Services and Protocol Over TCP/IP）。然而，业界对基于TCP/IP的网络管理标准的需求是如此迫不及待，已经等不及CMOT的推出了。为了应急，IAB决定将已有的SGMP修订、完善，作为一种临时的网络管理解决方案，这就是后来一统天下的SNMP。

### 1.1.1 什么是网络管理

简单地说，网络管理就是维护一个网络系统的正常运行。“正常运行”的意思是网络系统

能够按照设计的目标，发挥应有功能。网络管理，最直接的原因是组成网络的硬件设备会损坏，通信线路会出现中断故障，过多的网络用户会争用有限的网络资源（线路带宽、设备 CPU 处理能力等）。现代的网络管理，已不仅仅是维护网络的正常运行，还需要收集、分析网络运行数据，展示网络运行状况的性能指标，进而判断、预测网络故障，为网络优化及改造提供基础运行数据支持。

关于网络管理的组成，ISO 在 ISO/IEC 7498 文档第 4 部分，根据功能的不同，将基于 OSI 参考互联模型的网络管理划分为如下五部分：

- 故障管理（fault management）
- 计费管理（accounting management）
- 配置管理（configuration management）
- 性能管理（performance management）
- 安全管理（security management）

故障管理和性能管理是最基本的网络管理，是其他管理活动的基础，也是最常见的网络管理。一个网络系统，无论发生什么故障，都是对网络服务功能的破坏，因此，网络故障是最严重的网络事件，直接导致网络某部分功能的丧失。性能管理则是在网络无故障的基础上，对网络资源进行监视和调度，合理分配网络资源，保障网络功能正常发挥。不适当的性能管理会使得网络堵塞、某一部位产生处理瓶颈甚至导致整个网络瘫痪。性能管理的目的不仅仅是保证网络系统有充裕的资源可用，还要求网络资源达到一定的利用率以避免资源浪费。性能管理的理想目标是网络各个环节资源利用率协调一致，避免存在“短板现象”。

早期的网络管理相对简单，基本上是命令行方式的手工管理。不同的网络设备，命令格式不同，管理方式也不同。例如，网络管理员可能从设备面板指示灯的状态发现异常，也可能是接到用户的报障，才知道网络出现了问题。下一步，可能是登录到网络设备，输入各种命令，检查设备的运行状态，判断哪个部分出现了问题，然后再根据不同情况，进一步采取措施，修复故障。可见，这种管理方式属于“事件驱动”型：网络管理员不能主动发现问题，往往是异常问题发生并产生了影响之后，才察觉网络问题，然后再去检查、解决，具有一定的滞后性。

有的网络设备生产商针对自己的产品，开发了一些专用的、可以实现自动管理网络设备的应用软件，这些软件是最早的网络管理软件。这些管理软件的应用，将网络管理员从手工管理方式上升到自动化智能管理方式。然而，随着网络的发展，特别是出现网络互联的需求后，被管理的网络规模增大、结构复杂程度增加，网络中的设备往往不止来自一家生产商，这样，要想实现自动化智能网络管理，就需要同时运行几套网络管理软件，不仅不能统一管理，而且效率也不高。

### 1.1.2 网络管理的演变

网络管理的实质，是网络管理人员从网络设备获取一些网络运行状态信息，再对这些信

息进行综合分析、判断，从而确定网络运行状态的一个过程。一次典型的网络管理活动可以分为如图 1-1 所示的 3 部分。

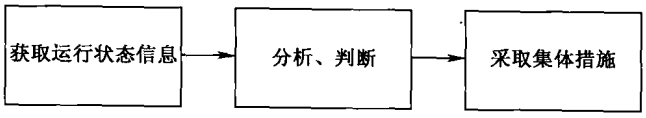


图 1-1 网络管理活动的过程

网络管理活动中首要的一个步骤就是“获取运行状态信息”，例如某个网络接口运行状态，某台设备的 CPU 利用率等。这些信息，网络管理术语中称其为“管理信息”。广义上说，它可以是任何一种网络管理员感兴趣的、与网络运行状态有关的信息。自动化智能网络管理，其实就是将“获取运行状态信息”这一步骤程序化。先进一点的网络管理软件，可以实现管理信息的分析判断，从而在一定程度上隔离出故障范围。一般地，故障恢复措施仍需要管理人员手工完成。

因此，网络管理协议的主要工作，就是为网络管理软件如何从网络设备获取网络运行状态信息，制订一套通用标准。

网络管理协议首先要解决两个问题，一是管理信息的表示与标识，二是网络设备与网络管理软件之间在传递管理信息时使用的通信协议。所有的网络管理协议，基本上都是以这两个主题为中心的。

### 1.1.3 SNMP 的发展

由于 SNMP 具有简单、易实施和容易扩充等优点，一经推出就得到了广泛的应用和支持，显示了强大的生命力。当 CMOT 趋于成熟时，SNMP 在实际应用中早已是今非昔比，已经得到了包括 IBM、HP 等大公司的数百家厂商的支持，早已成为网络管理领域事实上的工业标准。至今，SNMP 前后一共推出了 8 个版本，但实践中真正得到广泛应用的只有 3 个，分别是 SNMPv1、SNMPv2c 和 SNMPv3。

1. SNMPv1

主要由以下 RFC 文档组成：

- RFC 1155　基于 TCP/IP 的网络管理信息结构结构与标识。
- RFC 1157　简单网络管理协议。
- RFC 1212　简明 MIB 定义。
- RFC 1213　基于 TCP/IP 的网络管理信息库（MIB-II）。
- RFC 1215　定义 SNMP 陷阱消息宏。

SNMPv1 简单易于实施，被业界广泛接受并得以实施。但它最致命的一个缺点是安全性差，唯一的安全机制是基于共同体字符串（community strings），类似一个普通的字符串密码。

### 2. SNMPsec

主要由以下 RFC 文档组成：

- RFC 1351　SNMP 管理模型。
- RFC 1352　SNMP 安全协议。
- RFC 1353　用于 SNMP 管理团体的管理对象定义。

这个版本在 SNMPv1 基础上增加了较强的安全措施，其安全机制基于一种“团体（parties）”的结构。只有少数厂商实施过该版本，目前市场上已难觅踪影。

### 3. SNMPv2p

主要由以下 RFC 文档组成：

- RFC 1441　网络管理架构版本 2 介绍。
- RFC 1445　SNMPv2 管理模型。
- RFC 1446　SNMPv2 安全协议。
- RFC 1448　SNMPv2 协议操作。
- RFC 1449　SNMPv2 传输层映射。

这个版本也称为 SNMPv2，即第二版 SNMP。它不仅仅改进了 SNMPv1 安全性（和 SNMPsec 一致），同时在数据定义、协议操作类型等方面也做了较大变动。

### 4. SNMPv2c

主要由以下 RFC 文档组成：

- RFC 1901　介绍基于共同体的 SNMPv2。
- RFC 1905　SNMPv2 协议操作。
- RFC 1906　SNMPv2 传输层映射。

这个版本实际上是将 SNMPv2p 的数据定义和协议操作，与 SNMPv1 安全机制结合起来，形成一种新的简化版本，称为基于共同体的 SNMPv2，简称 SNMPv2c。它在数据定义、协议操作类型等方面也做了较大变动。大部分标称支持 SNMPv2 的设备，实际上实施的就是这个版本。

### 5. SNMPv2u

主要由以下 RFC 文档组成：

- RFC 1905　SNMPv2 协议操作。
- RFC 1906　SNMPv2 传输层映射。
- RFC 1909　SNMPv2 管理架构。
- RFC 1910　SNMPV2 基于用户的安全模型。

该版本是将 SNMPv2c 安全机制加以改进，新的安全特性是基于用户（users）的安全结构。

6. SNMPv2*

该版本将 SNMPv2p 和 SNMPv2u 的优点集合起来，但它还没有形成 RFC 文档便夭折了。

7. SNMPv3

1998 年 IETF 发布了 SNMPv3，SNMPv3 相关 RFC 文档如下：

- RFC 3410　Internet 标准管理架构及适用说明。
- RFC 3411　SNMP 网络管理框架结构。
- RFC 3412　SNMP 消息处理与分发。
- RFC 3413　SNMP 应用。
- RFC 3414　SNMPv3 基于用户的安全模式。
- RFC 3415　SNMPv3 基于视图的访问控制模式。

SNMPv3 有一个显著特点，就是增加了安全性。在提供三对 SNMP 消息的加密和认证措施的同时，也加强了 MIB 的访问控制。

## 1.2 SNMP 概述

作为一种标准的网络管理协议，从功能上，SNMP 的组成可以分为两大部分：管理信息的定义与标识和 SNMP 实体之间的通信协议。

管理信息的定义与标识的核心内容是管理信息结构与标识（Structure and Identification of Management Information，SMI）和许多的管理信息库（Management Information Base，MIB）。SMI 目前有 SMIv1 和 SMIv2 两个版本，它规定如何定义、标识管理信息。MIB 遵循 SMI 规范，定义具体的管理信息。

通信协议主要内容分别在 SNMPv1、SNMPv2 和 SNMPv3 等标准中定义，不同版本中的通信协议操作和通信协议安全机制不同。

### 1.2.1 管理工作站和代理

智能化的网络管理中，网络管理程序代替网络管理员，按照预先设置自动进行网络设备信息的收集、分析和处理。另外，支持 SNMP 功能的网络设备，必须有相应的支撑软件。

运行网络管理程序的计算机称为网络管理工作站（Network Management Station，NMS），代理（Agent）是运行在被管理的网络设备上完成 SNMP 功能的进程。管理工作站通过向代理发起查询操作，获得网络设备的工作状态信息；而代理则负责响应和处理来自管理工作站的服务请求，并向管理工作站报告本地发生的重大网络事件。运行代理的网络设备可以是路由器、交换机、集线器、主机、网络打印机，甚至是一台不间断电源（UPS），这些设备称为

被管理设备，有时候也称这些设备是“可网管的”。图 1-2 所示为部署在一个网络中的网络管理工作站和网络设备示意图。

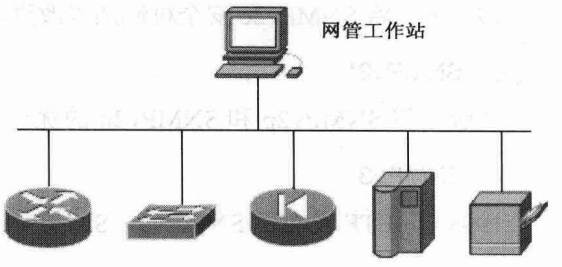


图 1-2 管理工作站和代理

在 SNMPv3 中，没有管理工作站与代理的概念，它们被统一称为 SNMP 应用程序实体。

委托代理（Proxy Agent）是一种特殊的 SNMP 代理。RFC 3413 给出了委托代理的三种用途：

（1）转发 SNMP 请求。委托代理可以透明转发一个 SNMP 请求到另外一个 SNMP 应用程序实体。通常情况下，不同的网络传输域或不同的 SNMP 版本之间，需要委托代理进行请求消息转发。

（2）SNMP 请求翻译。委托代理可以将 SNMP 请求翻译成不支持 SNMP 的另外一种管理协议的操作。

（3）特殊代理结构支持。当代理 A 中的某个管理信息取决于另外一些远程的代理中管理信息的状态时，代理 A 可以称为远程代理的委托代理。这种情况和代理的结构有关，实际情况中较少遇到。

### 1.2.2 SNMP 的组成

SNMP 是应用层协议，通信的参与者不仅仅是不同操作系统的主机，还有各种网络设备。因此，SNMP 定义了一套自己的“抽象语法”，就是通信双方交换数据的标准格式定义。

任何通信协议都具有语义、语法和时序三要素，SNMP 也不例外。语义表示如何解释得到的数据，语法规定了数据的组成格式，而时序则规定了双方交互数据时的先后顺序。协议的语意和语法一般通过 PDU（协议数据单元，Protocol Data Unit）实现。SNMP 中定义了 5 种 PDU。

SNMP 使用抽象语法标记（Abstract Syntax Notation One，ASN.1）定义抽象语法和 PDU。以 SNMPv1 为例，RFC 1155（基于 TCP/IP 的网络管理信息结构结构与标识，SMI）规定了如何定义 SNMP 使用的抽象语法，通俗地说也就是 SNMP 代理和工作站通信时使用的数据类型；RFC 1213（基于 TCP/IP 的网络管理信息库，MIB-II）依据 SMI 定义了一组标准的数据类型，这些数据类型的取值，表示一些对网络管理活动有意义的网络资源，定义这些数据类型的文本，称为 MIB；RFC 1157（简单网络管理协议，SNMP）定义了管理工作站和代理之间的通信协议和 PDU 格式。

SMI、MIB 和 SNMP 构成了 SNMP 协议簇的基石，堪称组成 SNMP 协议簇的“三驾马车”。

遵循 SMI，可以根据实际需要，定义出更多的数据类型（MIB）。一句话，SMI 和 MIB 的作用就是定义 SNMP 应用程序交互数据时使用的数据类型，而 SNMP 则规定了这些数据如何在应用程序之间交互，包括交互数据时使用的 PDU 格式、意义和消息顺序。

SMI、MIB 和 SNMP 三者之间的关系如图 1-3 所示。

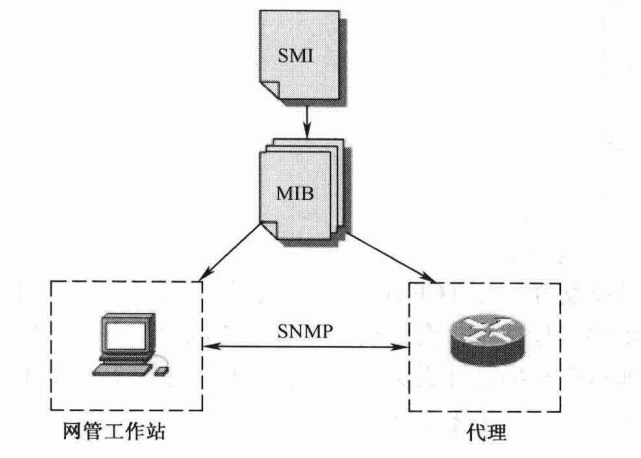


图 1-3 SMI、MIB 和 SNMP 之间的关系

需要注意的是，MIB 和 SMI 关系紧密，依据不同的 SMI 版本定义的 MIB，格式也不尽相同；SNMP 与 MIB 之间的关系相对松散，SNMP 只负责应用之间的数据传递方式，功能是保证 SNMP 应用之间正确、有效地传递数据，至于传递的是什么数据，意思是什么，则由应用程序负责解释。

可以看出，SNMP 中数据类型的定义和通信协议的定义，各自相互独立，互不影响。这一点很重要，当新的需求出现需要升级时，可以单独更改其中之一个而不影响另外一个。之所以如此是因为，IAB 的原意是在 CMOT 替换 SNMP 时，不至于重新定义 MIB，但这实际上却为 SNMP 以后的版本升级带来了极大的便利。

### 1.2.3 SNMP 与 TCP/IP

最初的 SNMPv1 标准是为满足基于 TCP/IP 的网络管理而开发的。及至 SNMPv2，RFC 1906 定义了 SNMP 消息在多种网络层协议上传输的规则，使得 SNMP 演变为一个可以运行在多种网络协议上的网络管理协议。

从 TCP/IP 协议栈的角度看，SNMP 属于应用层协议，与 Telnet、FTP 和 HTTP 等应用层协议层次相同，如图 1-4 所示。

任何应用层协议，都是为某种特定的网络应用而设计的。例如，HTTP 是为了满足浏览器和 Web 服务器站点之间的通信需要而设计的，FTP、TFTP 是为了满足网络文件传输应用而设计的。同样的，SNMP 是为了满足网络管理活动中的通信需要而制订的。

和本地应用程序不同，网络应用层协议面临的一个问题是，网络中参与通信的双方，很有可能存在系统差异。例如，网络中的服务器可能是一台 IBM 小型机，也可能是一台联想服务器，而客户端可能是一台个人电脑；通信双方的操作系统可能是 UNIX、Linux 或 Windows。不同的平台和系统，存储和处理数据的方式也各不相同。