Visual C++

开发基于SNMP的网络管理软件（第2版）

武孟军 徐奘 任相臣 编著

SNMP基础 —— 透彻分析报文结构　深入理解ASN.1　熟练读懂MIB

HP SNMP++软件包 —— VC++下使用详解

网管软件开发实例：

MIB浏览器

监视广域网线路

测量线路流量

自动绘制网络拓扑图

VLAN管理

人民邮电出版社
POSTS & TELECOM PRESS

Visual C++

开发基于SNMP的网络管理软件（第2版）

武孟军 徐奘 任相臣 编著

人民邮电出版社
北京

图书在版编目（CIP）数据

Visual C++开发基于SNMP的网络管理软件 / 武孟军，徐粪，任相臣编著. —2版. —北京：人民邮电出版社，2009.4
ISBN 978-7-115-20431-8

Ⅰ. V… Ⅱ. ①武…②徐…③任… Ⅲ. C语言—程序设计 Ⅳ. TP312

中国版本图书馆CIP数据核字（2009）第018585号

内 容 提 要

本书讲述了SNMP基础知识和使用Visual C++开发实用网络管理软件的方法与技巧。前几章由ASN.1语言入手，通过分析SNMP相关RFC文档的原始定义，结合实例，详实、深入地讲解了SNMP的原理。后面几章通过几个实例，讲述开发基于SNMP网管软件的方法和必备的网络知识。

本书是网络管理人员学习SNMP，提高网络管理水平的参考资料，也可供网管软件开发人员参考使用。

Visual C++开发基于SNMP的网络管理软件（第2版）

◆ 编　　著　武孟军　徐 粪　任相臣
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
三河市海波印务有限公司印刷

◆ 开本：787×1092　1/16
印张：22.25
字数：540千字　　2009年4月第2版
印数：5 001 – 8 500册　　2009年4月河北第1次印刷

ISBN 978-7-115-20431-8/TP

定价：49.00元

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

第 2 版前言

《Visual C++开发基于 SNMP 的网络管理软件》一书出版后，深受广大读者的关注和好评，他们也提出了不少宝贵意见和建议。

一般说来，开发网络管理软件，不仅需要熟悉相关的网络知识，还要熟悉 SNMP 的基本架构和基础知识。特别地，需要熟练掌握 MIB（尤其是遵循 SMIv2 的 MIB）的阅读理解能力。

相信国内读者学习 SNMP 的经历大都一样：从半山腰开始，越攀登越困难，最后举步维艰，越学越糊涂。为什么呢？因为国外介绍 SNMP 的原版书，很少系统地介绍关于 SNMP 的 RFC 文档，而是偏重于 SNMP 在网络管理中的实际应用。这大概是因为 RFC 都是公开技术文档，对英语国家的读者来说，这些都是应该掌握的基础知识。国内的 SNMP 书籍大都是翻译或参考国外的，而国内读者很少直接阅读过英文 RFC 文档，因此造成了国内读者学习 SNMP 过程中的“舍本逐末”现象只知其然，不知其所以然。

针对这个问题，本书第 1 版花了大量篇幅，向读者全面介绍描述 SNMPv1 基本的 RFC 文档，使读者首先对 SNMP 有一个整体的概念，夯实 SNMP 基础知识。读者掌握了这些基础知识后，就完全有能力通过阅读 SNMP 的 RFC 文档，进一步学习、掌握 SNMP 的其他内容。

第 1 版中 SMIv2 内容章节安排不尽合理，且关于如何阅读 MIB 的内容偏少。同时讲解 ASN.1 内容有不当之处，一是介绍宏定义时混淆了“类型”和类型的“符号形式”，二是介绍 Tag 直接方式定义类型的内容有误。因此本书第 2 版做了如下修订：

- 对内容进行了勘误；
- 扩展了 SMIv2 方面的内容；
- 增加了如何阅读理解 MIB 和介绍 MIB-Ⅱ的内容；
- 程序介绍章节删除了部分不重要的代码。

第 2 版的侧重点仍然是循序渐进向读者介绍 SNMP 的基础知识，熟练阅读理解 MIB。在掌握了 SNMP 的基础知识后，指导读者使用第三方软件包 HP SNMP++，在 VC 环境下，结合实际情况，自己动手，开发一些简单实用的网络管理软件。如网络流量测试、监控通信线路工作状态、绘制网络拓扑和局域网管理等常用管理工具。示例程序注重关键性功能的实现细节，读者可以修改、优化源代码，使其功能更趋完善。

作者

2009-1-15

前　言

最初，TCP/IP 设计者没有太多考虑网络管理方面的事情，而是将大部分的精力放在了实现网络连通性方面。随着智能化网络管理的需求，制订一种网络管理协议变得十分迫切。简单网络管理协议（Simple Network Management Protocol，SNMP），是当时出现的几个网络管理标准中的一个。SNMP 一经发布，就受到了广泛的欢迎，取得了意想不到的成功，并获得了广泛的支持和发展。以后，基于 SNMP 的各种网络管理软件也应运而生。

学习 SNMP，无论是对于网络管理员还是网络管理程序开发者，都是十分必要的。然而，目前介绍 SNMP 的书籍少之又少，结合开发实例的更是凤毛麟角。为帮助读者学习掌握 SNMP 相关知识，并能熟练地在工作实践需要中加以运用，笔者编写了本书。

本书前面几章介绍了 SNMP 的入门知识，这些知识是进行高效的网络管理，开发网络管理软件的必备知识，同时也是进一步学习 SNMP 的基础。后面几章结合实例讲述如何用 Visual C++ 6.0，结合免费的第三方软件，在 Windows 2000 操作系统下，开发一些实用的网络管理工具。这些管理工具可用于：

- 监视物理通信线路的通、断；
- 测量线路通信数据流量、线路带宽利用率；
- 监视网络设备（包括服务器、CPU、内存）使用情况；
- 自动绘制校园网拓扑图；
- 管理局域网。

这些软件，是笔者在长期的网络管理实践中，结合实际需要而开发的。

让读者熟练掌握 SNMP，降低门槛，将看似神秘的网络管理软件设计“平民化”，是本书的一个主要目的。如果你是一个网络工程师或系统管理员，只要会使用 C++语言进行一般的编程（不需要精通），那就具备了自己编写网络管理软件的基础。自己去做，不仅仅是节省一笔金钱的问题，重要的是了解网络管理的精髓，学习更广泛的知识和提升自己的能力。更重要的一点是，没有人比你更清楚你自己最需要什么样的管理工具。

如果你是一位有志于开发网络管理软件的程序员，本书不仅是一本 SNMP 入门书籍，还能让你学习到你亟需掌握的网络知识。书中每章介绍的程序力图向读者说明其编程实现的思路以及解决问题的方法。源程序的具体实现代码不一定是最优的，读者可以根据自己的实际情况，修改、优化源代码，使得程序更加实用、完美。

由于本人水平有限，书中错误与不足之处，在所难免，欢迎读者批评指正。如读者就书中内容有什么问题，欢迎通过 MSN 或邮件与我交流，电子邮件：

book_better@sina.com

致谢：

感谢我的妻子张利民在本书的写作过程中对我的鼓励与支持；感谢原广东证券信息技术

中心刘震总经理和我的同事们对我的支持！参加资料整理的还有张一平、汪进峰、范明明、孙淑华、黄海杰、冼颖升、陈科、孔凡京、梅祖欢、刘李安、玉辉、陈天全、吴戈、贾凤波、杨树青、杨玉顺、王焕君、张婷、马俊丽、鄢丹、田敏，在此深表谢意！

在本书出版之际，广东证券被重组为安信证券，我权且将此书作为对原广东证券的一份怀念，安信证券的一份祝贺吧。

作者

2006 年 11 月

下载代码说明

本书代码可从 http://www.ptpress.com.cn 下载，在输入书号后弹出的页面中单击“素材”即可。下载代码有第 8～14 章示例程序的所有工程文件和已经编译好的 SNMP++静态链接库。

SNMP++静态链接库分为 Debug 和 Release 两个版本，使用时，读者可以将它们直接复制到 Visual C++的链接库目录中。

每章的程序放在单独的目录中，每个目录中的 Debug（或 Release）目录中有编译好的可执行文件，这些可执行文件可以直接作为网络管理工具使用。使用时，被管理的网络设备需要配置启用 SNMP。

调试源代码时，请注意根据情况使用不同版本的 SNMP++静态链接库。工程文件中的编译参数都是配置好的，如果不是太熟悉 VC++的编译环境，最好不要修改。所有程序代码在 Windows 2000、Visual C++ 6.0 环境下调试通过。

目　录

第 1 章　SNMP 概述

自从简单网络管理协议（Simple Network Management Protocol，SNMP）1989 年正式发布第一个版本以来，经过短短十几年时间的完善和发展，它已经成为目前使用最广泛的网络管理标准协议。

SNMP 之所以成功，得益于它的两个主要特点：

（1）简单性。正如它的名字一样，也许是出于一个临时性解决方案的考虑，SNMP 力求简单，最初的版本涉及的操作只有 5 个。这使得 SNMP 的实施很容易进行，成本较低。

（2）扩展性。由于计算机技术经常是“出人意料”地发展，“扩展性”也成了计算机技术领域的一大特色。SNMP 制订时充分考虑了这一点，通信协议与管理信息库互相独立，使得 SNMP 很容易扩展。一项新的网络技术出现，实现者只需自己定义针对该技术的 MIB 文件，就可以将这项新技术纳入到 SNMP 的管理范围；SNMP 版本升级，也只是通信协议的报文格式的改进，和 MIB 无关。

1.1　历史背景

最早致力于网络管理标准化工作的是国际标准化组织（ISO），它是网络互连协议 OSI（开放系统互连）协议的制订者，因此它开发的网络管理标准（CMIS/CMIP，The Common Management Information Service/Protocol）也是基于 OSI 的，并在当时的网络管理中得到了应用。

由于 TCP/IP 技术的应用越来越普及，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。长期的目标是在 CMIS/CMIP 基础上，制订基于 TCP/IP 协议栈的网络管理协议 CMOT（Common Management Information Services and Protocol Over TCP/IP）。同时，为了应急，IAB 决定将已存在的 SGMP（简单网关监控协议）修订完善后，作为一种临时的解决方案，这就是后来的 SNMP。

和其他的网络协议一样，SNMP 标准由 IAB 领导的 Internet 工程任务组（IETF）负责制订。IETF 首先发布 RFC 草案，广泛征求意见后，最终形成标准的 RFC 文档。因此，SNMP 标准由一系列的 RFC 文档定义。

最初，SNMP 虽然因其简单性而易于实施，但它最明显的一个缺点是安全性差。为解决这个问题，IETF 陆续发布了一些新的 RFC，这些后来出现的 RFC 文档在 SNMP 的安全性方面做了很多工作，同时在其他方面也做了一些修订。1993 年，IETF 发布了新的 SNMP 标准，称为 SNMPv2，而以前的标准称为 SNMPv1。

SNMPv2 由下面的 RFC 文档组成：

- RFC 1901　基于共同体的 SNMPv2 介绍
- RFC 1902　SNMPv2 使用的 SMI

- RFC 1903　SNMPv2 使用的文本约定
- RFC 1904　SNMPv2 的一致性陈述
- RFC 1905　SNMPv2 协议操作
- RFC 1906　SNMPv2 传输层映射
- RFC 1907　SNMPv2 使用的 MIB
- RFC 1908　SNMPv1 与 SNMPv2 的共存

SNMP 标准在安全性增强的同时也增加了实施的复杂性，而且当时人们对安全性并不十分重视，因此，后来真正被采用的是称为 SNMPv2c 的简化版本，这个版本中并没有改进 SNMPv1 的安全性，仍然沿用了 SNMPv1 中的安全机制。

真正在安全方面得到加强的是 1998 年发布的版本 SNMPv3，这和近年来人们越来越重视网络安全有很大关系。SNMPv3 由下面的 RFC 文档组成：

- RFC 3410　第 3 版互联网标准网络管理框架介绍
- 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

SNMP 版本是向下兼容的，设备运行的版本是 SNMPv3 时，它可以处理接收到的 SNMP 任何版本的消息。

1.2　基础知识

SNMP 是基于管理工作站/代理模式的，如图 1-1 所示。运行网络管理程序的计算机称为网络管理工作站（Network Manage Station，NMS），代理是运行在网络设备上的进程。管理工作站通过向代理问询获得网络设备的工作状态信息，代理则负责处理和响应来自管理工作站的请求，并向管理工作站报告本地发生的重大事件。运行代理的网络设备可以是路由器、交换机、代理集线器、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。

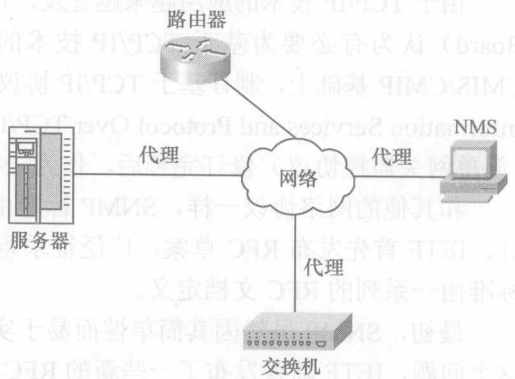

图 1-1　网络中的管理工作站和代理

网络中的代理与管理工作站之间的搭配不是固定的。任意一台启用了 SNMP 的网络设备，就是标准的 SNMP 代理。只要配置了正确权限，任意一台网络管理工作站，都可以对网络中的代理进行管理。

注意：委托代理是一种特殊的代理。当被管理设备由于某种原因（比如低层传输协议不同）不能直接被管理工作站管理时，则可以通过委托代理来管理该设备。委托代理运行在被管理设备以外的平台上，在管理工作站和被管理设备之间起“中介”作用。

网络管理活动是一个网络管理者不断地从被管理设备获取有用的信息，进行分析处理的过程。管理信息库（Management Information Base，MIB）是一个标准文档，它描述了代理能够为管理工作站提供哪些信息，以及管理工作站对这些信息的操作权限（查询或设置）。一台支持 SNMP 的网络设备，应该指明本设备支持哪些 MIB，并提供详细的 MIB 文件。管理工作站只有根据这些 MIB 文件，确定被管理设备中哪些信息能通过 SNMP 被查询，才能进行正确的管理操作。

在 MIB 中，定义的管理信息称为被管理对象。描述被管理对象，即如何标识、表示某一特定管理信息，必须遵循严格的标准。这个标准称为管理信息结构（Structure of Management Information，SMI）。

注意：MIB 分为标准 MIB 和私有 MIB 两种。标准 MIB 指的是由 IETF 主导发布 MIB，例如 RFC1213 定义的 MIB-II，MIB-II 不断有新的内容补充进去，任何支持 SNMP 的设备必须支持 MIB-II。私有 MIB 由网络设备生产商制订，定义该设备支持的特有管理信息描述。

抽象语法标记（Abstract Syntax Notation One，ASN.1）是一种功能强大的数据定义语言。它通常被用来定义异种系统之间通信使用的数据类型，或者定义协议数据单元（Protocol Data Unit，PDU）。

SNMP 中，管理工作站与代理之间频繁传递的管理数据，就属于典型的异种系统之间通信使用的数据。SMI 规定，使用 ASN.1 语言描述 MIB（定义管理工作站与代理之间通信时使用的数据类型）。考虑到简单性，定义 MIB 时，只允许使用 ASN.1 数据类型中的一部分类型，这些类型被定义在 SMI 中。

SNMP 的核心部分是 RFC1157，它使用 ASN.1 语言定义了管理工作站与代理之间交互的报文格式（PDU），这个协议称为简单网络管理协议（SNMP）。平时所说的 SNMP，是指包括了 RFC1157 在内的一系列相关标准组成的网络管理协议。SNMP 不同版本之间的差异，主要就是这部分的不同。它定义了管理工作站与代理之间的 5 种基本操作，每种操作都对应一个协议数据单元的定义：get（获取指定管理信息的操作）、get-next（获取 MIB 中按字典序紧邻指定管理信息的下一个管理信息的操作）、set（设置指定管理信息的操作）、get-response（前 3 种操作的应答消息）、trap（代理向管理工作站发送的报告事件消息）。

概括地说，MIB 是代理提供给管理工作站的标准文档，管理工作站可以向代理查询（设置）MIB 中定义的管理信息，代理使用 Trap 消息向管理工作站报告本地发生的网络事件，SNMP 是管理工作站与代理之间的通信协议。

1.2.1　SNMPv1 的组成

SNMP 首先要解决的是管理工作站与代理之间的通信协议问题，其次是解决管理信息如何表示和描述的问题。因此概括起来，SNMP 标准包括 3 个基本的组成部分。

（1）管理信息结构。在 RFC1155、RFC1212、RFC1215 中定义。RFC1155 和 RFC1212 描述了 MIB 中管理信息如何被定义以及使用什么语言进行定义。RFC1215 则描述了在 MIB 中如何定义 Trap 的方法。

（2）管理信息库，用来描述、定义管理信息。MIB-II 是所有支持 SNMP 的设备必须实现的标准管理信息库，在 RFC1213 中定义。

（3）简单网络管理协议。在 RFC1157 中定义，它规定了进行网络管理活动时允许的操作，

通信双方报文格式、顺序以及 SNMP 的大致体系结构。

SNMP 和 MIB，这两者构成了 SNMP 标准的核心内容。SMI 虽然是一个十分重要的基础标准，但其最终目的是如何更合理有效地制订 MIB 服务。

注意：作为 SNMP 功能上的一个重要补充，远程监视（Remote Monitoring，RMON）是后来出现的一组管理规范。它其实是通过定义特殊的 MIB，进行局域网的远程监控。本书不涉及这方面的内容，有兴趣的读者可以参考其他资料。

1.2.2 SNMP 系统框架与安全机制

管理工作站和被管理设备中使用 SNMP 进行通信的程序实体，称为 SNMP 应用程序实体。向应用程序实体提供 SNMP 协议原语服务的进程，称为 SNMP 的协议实体。

一个 SNMP 代理和任意的 SNMP 应用程序实体（网络管理程序）一起，组成为一个 SNMP 共同体（Community）。每个共同体都有一个以字符串形式表示的名字。

SNMP 程序实体发送或接收的 SNMP 消息中，必须附有共同体名字。只有消息中的共同体名和发送该消息的程序实体所处的共同体名相同时，这个消息才是有效的。

在任意的可网管设备中，MIB 定义的被管理对象的子集，称为 SNMP MIB 视图。同一个视图中的被管理对象，可以来自不同的 MIB 文档。集合{READ-ONLY，READ-WRITE}中的元素被称为 SNMP 访问模式。

一个 SNMP MIB 视图和其对应的 SNMP 访问模式，组成 SNMP 共同体访问环境（SNMP community profile）。SNMP 共同体访问环境表示了对 SNMP MIB 视图中被管理对象特定的访问权限，它作用于视图中的每一个被管理对象。下面是访问控制规则：

（1）如果被管理对象在 MIB 中的访问权限为 read-write 或 write-only，访问环境中的访问模式是 READ-WRITE，那么该对象可以接受 set、get 操作，可以被 Trap 使用。

（2）如果访问环境中的访问模式是 READ-ONLY，则视图中所有对象除访问权限为 not-accessable 的外，只可以接受 get 操作，也可以被 Trap 使用。

（3）当 get、trap 操作用于访问权限为 WRITE-ONLY 的对象时，返回值根据具体的代理实现而不同。

一个 SNMP 共同体和其对应的 SNMP 共同体访问环境一起，组成一个访问策略。

在实际应用中，一个代理可以配置几个具有不同访问策略的共同体。任意的网络管理工作站，只要知道共同体的名字，使用正确的共同体名字访问代理的消息，就被认为是合法的。

例如，在 CISCO 路由器中配置如下命令：

```
snmp-server community public RO
```

这样，代理中就定义了一个名为 public 的共同体，RO 是访问模式 READ-ONLY，因为命令中没有定义和它联系在一起的视图，所以缺省的视图就是该代理支持的所有 MIB 中定义的被管理对象。

注意：在 CISCO 路由器中配置 MIB 视图的方法参见附录 B。

因此，在 SNMP 中，共同体名相当于口令。SNMPv1、SNMPv2 都使用它作为安全认证机制。有 3 种级别的共同体名：只读、读写和 Trap。只读共同体名用来向代理查询数据时提交，读写共同体名既可以读数据又可以设置数据值，Trap 共同体名在管理工作站接收代理发

送的 Trap 时使用。

大部分设备将只读共同体字符串默认设置为 public，读写设置为 private。虽然本书中的例子也使用了 public 作为只读共同体串，但出于安全方面的考虑，建议大家还是按照设置其他密码一样的规则来设置它，并严格管理具有写权限的共同体名。

1.2.3　Trap 消息

管理工作站向代理获取管理信息的途径有两种：一是查询，由管理工作站向代理发出查询消息，代理处理后回送应答消息；二是接收代理发送的 Trap 消息，Trap 消息是当代理探测到本地有和网络运行状态有重要关系的事件发生时，向工作站发送的事件报告消息。

因为网络事件随时都可能发生，因此 Trap 的发送也是随机的。发送给哪个管理工作站，也就是 Trap 的目的地，是事先在代理中指定的。接收到 Trap 后，管理工作站不需要给代理发送确认消息。因此，在较差的网络环境中，Trap 的传输是不可靠的。具体如何处理接收到的 Trap，视具体网络管理应用程序的实现而不同。一般情况下，首先解析 Trap 包含的信息，再进一步判断 Trap 的具体意义，进而确定是否需要做出反应动作。

RFC1157 中，定义了代理向管理工作站传递 Trap 的 PDU 格式，并定义了 6 种不同类型的标准 Trap，这 6 种 Trap 包括了最常见的网络事件（比如某个网络接口工作状态的改变）。同时，还提供了定义其他 Trap 的扩展机制。

定义新 Trap 的需求来源于新技术的应用以及设备生产商，他们希望自己的产品能提供更丰富的 Trap 支持，以方便用户管理网络。这样，很多生产商在自己的 SNMP 代理中，实现了各种不同的扩展 Trap 支持。

为了方便，RFC1215 中专门描述了如何在 MIB 中定义 Trap，并给出一种统一的格式。同时，使用新的格式重新定义了 RFC1157 中的 6 种标准 Trap。

RFC1157 中定义的 6 种标准 Trap 以外的，称为扩展 Trap。

1.2.4　SNMP 与 UDP

从 TCP/IP 协议栈模型看，SNMP 处于应用层协议的位置，使用 UDP 传输服务。

管理工作站不仅向代理发起检索请求，还要能接收代理发送来的 Trap 消息。同样，代理除了接收处理管理工作站发来的请求，还要能够随时向管理工作站发送 Trap 消息，如图 1-2 所示。因此，网络管理程序和代理，本身既是客户端程序，又是服务器程序。

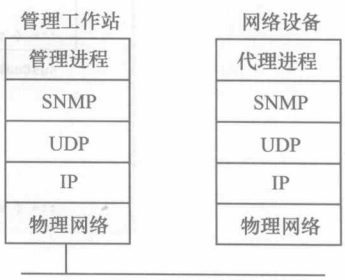

图 1-2　SNMP 在 TCP/IP 中的位置

默认情况下，SNMP 代理监听 UDP 端口 162。任何一个向代理发送检索请求的 NMS，必须向 162 端口发出请求。网络管理程序则通过监视 UDP 端口 161 接收代理发送的 Trap。在实际应用中，这两个端口通过配置是可以更改的。

在 TCP/IP 中，UDP 是不可靠的传输服务，数据的可靠性由应用程序解决。正常情况下，对于管理工作站发出的每个请求，代理都会返回应答，管理工作站可以根据是否有应答包来判断请求数据包是否顺利到达。在设定的时限内，如果收不到应答，NMS 认为以前发送的请

求丢失，可以重新发送请求或者放弃。另外，管理工作站与代理之间的通信可以有异步模式（非阻塞）或同步模式（阻塞）两种。异步模式下，给每个请求分配一个随机正整数作为标识。代理应答时，无论采用何种通信模式，都必须保证应答报文中标识和请求报文中的一致。在同步模式下，虽然每个报文也有标识，但不起作用。

对于代理发出的 Trap，设计者认为重传和确认包会浪费网络资源并增加 SNMP 的复杂性，因此 SNMP 中没有确保 Trap 顺利到达目的地的机制。代理只是在需要的时候简单地发送 Trap，但不保证管理工作站是否收到。

1.3 管理信息库和管理信息结构

在 MIB 中定义被管理对象，可以将网络设备中所能支持的管理信息种类、标识方式等统一起来。这样，就避免了不同的系统使用不同的方式造成的混乱。MIB 其实是代理对外提供的一种访问管理信息的“接口定义”，SMI 则规定了如何定义和描述这个接口。

1.3.1 管理信息库

MIB 不是数据库，其中也没有可用的值。MIB 是“标准”，设备代理必须根据 MIB 中的定义，逐一实现其中描述的被管理对象。“实现”是指，当有查询 MIB 中定义的某个被管理对象的请求到来时，代理必须为其返回一个合适的值。至于代理如何获取这个值，则视代理实现的方法而定。图 1-3 所示为一个普通的 MIB 文件。

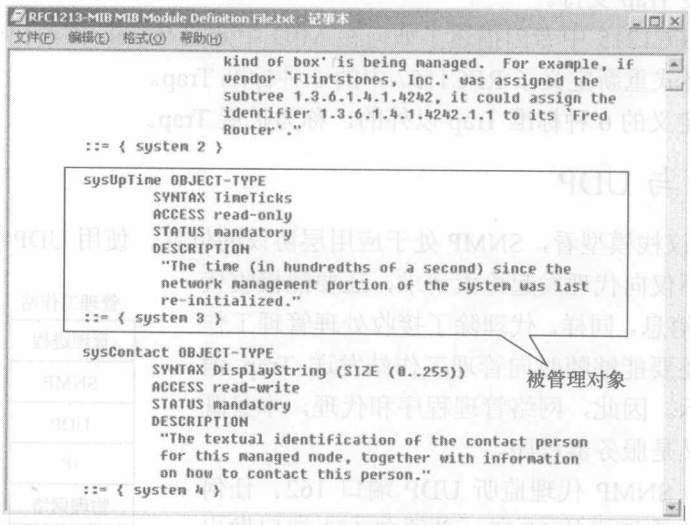

图 1-3 MIB 文件和被管理对象

对网络管理者来说，如果要通过 SNMP 查询某种管理信息，就必须查阅设备的 MIB，确定是否有对应的被管理对象定义。从 MIB 文件中可以知道：

- 使用 SNMP 是否可以向某个代理查询某种感兴趣的管理信息？
- 如可以查询，如何标识这种信息？
- 如查询成功，返回的值表示什么物理意义？