Visual C++

开发基于SNMP的网络管理软件

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

CD-ROM

Visual C++

Visual C++

开发基于SNMP的网络管理软件

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，徐奘，任相臣编著.
—北京：人民邮电出版社，2007.1
ISBN 978-7-115-15365-4

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（2006）第 118727 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。书中第1章～第6章由介绍ASN.1语言入手，通过分析SNMP相关RFC文档的原始定义，并结合实例，翔实、深入地讲解了SNMP的原理。第7章～第13章通过具体实例，讲述开发基于SNMP网管软件的方法。

本书可作为网络管理人员学习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

◆ 编　　著　武孟军　徐　奘　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
北京鸿佳印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：24
字数：630 千字　　2007 年 1 月第 1 版
印数：4 001 – 5 000 册　　2007 年 8 月北京第 2 次印刷

ISBN 978 7-115-15365-4/TP・5748

定价：49.00 元（附光盘）

读者服务热线：(010)67132692　印装质量热线：(010)67129223

前 言

最初，TCP/IP的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，简称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6章介绍了SNMP的入门知识，这些知识是进行高效的网络管理和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7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。如果你是一名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），就具备了自己编写网络管理软件的能力。自己开发，不仅仅是节省一笔资金的问题，重要的是可以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都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，使得程序更加实用和完美。

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。也欢迎读者就书中内容通过邮件与我交流，电子邮件地址：

book.better@sohu.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、陈克、孔繁京、梅祖欢、刘李安、于辉、陈天全、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，对安信证券的一份祝贺吧。

作者

2006年11月

光盘内容

本书所附光盘中有书中第7章～第13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 2570　第3版互联网标准网络管理框架介绍
- RFC 2571　SNMP网络管理框架结构
- RFC 2572　SNMP消息处理与分发
- RFC 2573　SNMP应用
- RFC 2574　SNMPv3基于用户的安全模式
- RFC 2575　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，简称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、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。

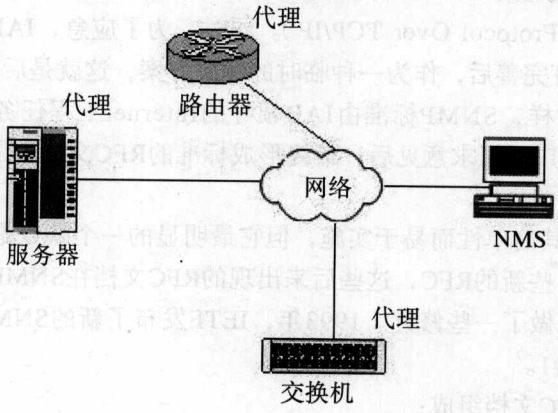

图1-1　网络中的管理工作站和代理

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，简称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，简称SMI）。

注意：MIB分为标准MIB和私有MIB两种。标准MIB指的是RFC1213中定义的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，简称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，简称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（前三种操作的应答消息）、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，简称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缺省设置为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种称为标准Trap，其余的称为扩展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。

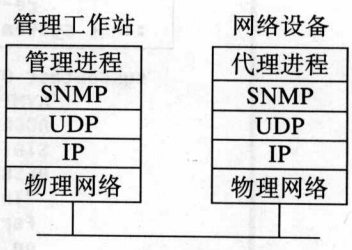

图1-2　SNMP在TCP/IP中的位置

缺省情况下，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。