第38章　SNMP：简单网络管理协议

作者：Tim Parker

本章内容包括：

- 什么是SNMP
- 管理信息基(MIB)
- 使用SNMP
- UNIX与SNMP
- Windows与SNMP

本章讲述简单网络管理协议（SNMP)。SNMP通常用来管理网络设备并获取设备信息。SNMP使网络管理变得简单，因此通常用在 TCP/IP网络，尤其是大规模网络，。SNMP同样可用来将自身的状态发送给特殊的SNMP服务器软件，显示错误隐患及其他可能出现的问题。网络管理员使用SNMP可以在一个地方获取所有支持SNMP的网络节点的信息，并且可对其进行远程配置。

38.1　什么是SNMP

简单网络管理协议最初是为处理网络上路由器而设计的。虽然 SNMP是TCP/IP协议族中的一员，但它并不依赖于IP。目前大部分SNMP都使用IP协议，但SNMP是独立的协议(因此，它也用于Novell公司SPX/IPX的IPX协议之上)。

SNMP并不是单个协议，它由三个协议组成，这三个协议用于网络管理。组成 SNMP协议的三个协议及功能如下所示：

- 管理信息基(MIB)　　包含状态信息的数据库。
- 管理信息的结构与标识(SMI)　　定义MIB的入口。
- 简单网络管理协议(SNMP)　　受管理的对象与服务器间的通信方法。

拥有SNMP能力的管理代理软件包要么在系统启动时加载，要么嵌入到设备的硬件中。拥有SNMP代理的设备由于不同的厂商而有各种不同的名称，但总的可分为 SNMP管理设备和受SNMP管理的设备两种。SNMP相容设备也拥有将SNMP集成到其软件或硬件上的代码。当设备中包含SNMP时，我们称之为可管理的设备。

受SNMP管理的设备可与位于网络某处的 SNMP服务器通信。设备与服务器有两种通信方式：投票及中断。接受投票的设备由服务器询问当前的状态或统计信息。投票通常在一定时间间隔执行，由网络服务器与受管理的设备进行通信。投票的问题是：信息不总是实时的，同时由于受管理的设备数量增多及投票频率过高的影响容易造成网络拥塞。

在基于中断的SNMP系统中，当受管理的设备出现异常时，向服务器发送消息，在这种方式下，服务器可以及时知道问题 —— 除非设备崩溃，此时，只有其他设备与已崩溃的设备进行连接时，系统才可能发现问题。基于中断的设备也存在自己的问题，最主要的是设备需要组织发送给服务器的消息，这将消耗掉系统时钟周期，从而降低系统的工作效率。同时也可

能导致性能“瓶颈”从而引发其他问题。如果消息数据量较大，包含很多统计数据，组织和传输消息将导致网络性能下降。

如果网络上出现较严重的问题，如电源掉电或电压过高，每个受管理的 SNMP设备都设法向服务器发送中断消息以报告问题。这将导致网络拥塞从而使服务器接收到错误的消息。

通常，将投票与中断结合使用以弥补各自的缺陷，我们称这种组合方式为直接自陷投票(trap-directed polling)，服务器定时统计或在管理员指导下统计设备信息。同时，每个受管理的设备在某种条件发生时产生中断消息，中断发生的条件比纯粹的中断驱动系统要严格。例如，如果用户使用中断SNMP，路由器负载每增长10%都向服务器报告。如果使用直接自陷投票SNMP，用户可从投票中获得路由器的负载，并且当路由器负载增加很快时，将向服务器发送中断消息。当服务器接收到此中断消息后，如果需要的话，可进一步查询设备的详细信息。

SNMP服务器软件包可与SNMP代理通信、传输或请求一系列不同类型的信息。通常由服务器向代理请求统计信息，包括处理的包数量、设备的状态与设备类型相关的特殊信息等 (如modem失效连接的次数)及处理器的负载。

服务器也可向代理发送指令以修改数据库 (MIB)中的项。服务器也可设置代理方的阈值或条件，当代理超过阈值或满足条件时向服务器发送中断消息，如 CPU负载达到90%。

虽然服务器与代理间的通信内容趋向于抽象，但通信本身以非常直接简单的方式完成。如：服务器发送“当前负载”，代理返回75%。代理从不向服务器发送数据，除非产生中断消息或收到服务器请求，这意味着在没有进行投票或产生中断消息时，系统可能存在潜伏的问题。

38.2 管理信息基(MIB)

每个受管理的SNMP设备均维护包含统计信息及其他数据的数据库。我们称之为管理信息基或MIB。MIB的每一项包含一种信息：对象类型、语法、访问字段及状态字段等。 MIB的项通常由协议规定，并且严格遵守抽象语法规则 1(ASN.1)的格式。

对象类型为项的名称，通常为简单的名字。语法是一个值字段，通常为字符串或整型，并不是所有的MIB的项均包含值字段。访问字段用于定义项的访问权限，通常有以下四类：只读、可读/写、只可写或不可访问。状态字段包含指示值，标明MIB项是否为命令、可选或作废。命令表示受管理的设备必须执行该项。可选表示受管理的设备可以选择执行该项，作废表示不执行。

目前执行的MIB有两种， MIB-1和MIB-2。两者结构不同， MIB-1创建于1988年，其表中包含114项，分为两组，支持MIB-1的受管理的设备必须支持所有的适用于该设备的组。例如：受管理的打印机不能执行处理外部网关协议的项，与外部网关协议 (EGP)相关的项用于路由器或类似的设备。打印机需要指明它可处理的项。

MIB-2是MIB-1的扩展，于1990年提出。它包含171项共分为10组。除了扩展了原有的组外，又新增加了组。与MIB-1类似，支持MIB-2的设备必须执行所有适用于该类型的组。用户将会发现许多设备仅支持MIB-1而不支持MIB-2。

除了MIB-1和MIB-2外，还有许多正在测试的MIB，它们包含许多不同的组和项。但它们并未被广泛使用。某些公司开发 MIB以供自己使用，某些厂商也提供对这些 MIB的支持，如HP(惠普)公司自己开发的MIB得到了许多可管理设备及服务器软件包的支持。

38.3 使用SNMP

简单网络管理协议有许多不同的版本，其中最通用的为 SNMP v1。一般情况下， SNMP被

用于非同步客户/服务器应用，受管理的设备或SNMP服务器软件都可产生消息，根据需要等待响应。这些消息或响应由具体的网络软件(如IP)打包并处理。SNMP在TCP/IP中使用UDP协议作为其消息传输协议。UDP端口161可接受除自陷外的所有消息，自陷消息由162号端口接收。代理通过UDP161号端口接收来自服务器的消息。

SNMP的第一个主要版本SNMP v1仅包含较为简单的操作，它很容易被设备制造商实现并得到操作系统的支持。SNMP v1支持以下五种服务器与代理间的操作：

- get —— 用于获取MIB项的值。
- get-next —— 用于遍历MIB项。
- get-response —— get的响应。
- set —— 用于修改MIB的项。
- trap —— 用于设置中断条件。

当发送请求时SNMP项的某些字段为空，以便客户填充并返回给服务器。这是一种在一个块内传送问题或答案的有效方法。避免了通过复杂的查询算法寻找与请求对应的结果。

例如：在get命令中，类型和值字段为空，客户方填充这两个字段后(除非请求失败，否则返回错误消息)将消息返回给服务器。

SNMP v2在SNMP v1的基础上增加了一些新的功能。对于服务器来说，最方便的命令为get-bulk操作，它使客户方在一条消息中发送大量MIB项的信息(SNMP v1需要多条get-next操作才可完成相同功能)。此外，SNMP v2比SNMP v1有更强的安全性，可防止入侵者监视受管理的设备的状态。SNMP v2既支持加密也支持认证。因此，SNMP v2远比SNMP v1复杂，也没有SNMP v1应用广泛。

SNMP支持代理管理，即包含SNMP代理和MIB的设备可与有不完全的SNMP代理软件的设备进行通信。基于代理的管理可以将设备的MIB放在客户方的内存中，通过连接远程机器对设备进行管理。例如：可以通过代理管理打印机，将打印机的客户方SNMP软件及MIB放在代理工作站中，通过代理工作站对打印机进行管理。基于代理的管理可以减轻负载过重的设备的工作量。

尽管SNMP已得到了广泛的应用，但它仍有一些不足之处。最主要的是UDP的可靠性。因为UDP是无连接协议，服务器与代理间的消息传送没有可靠的保障。另外，SNMP仅提供简单的消息传送机制。因此，不能对消息进行过滤，这有可能导致接收消息的软件负载过重。最后一点不足是，SNMP从某种程度上说仍然使用投票方式，这将消耗大量带宽。

网络管理的将来属于OSI网络管理标准：通用管理信息服务(CMIS)及通用管理信息协议(CMIP)，它们建立在TCP/IP之上。IAB发布了基于TCP/IP的通用管理信息服务与协议CMOT作为TCP/IP及OSI管理的标准。

SNMP及CMOT都使用网络管理者与网络设备(如工作站、网桥、路由器等)交换信息。主管理工作站与不同的管理进程通信获取网络的状态信息。SNMP及CMOT的体系结构都将收集的信息以某种方式存储以便供其他协议读取。

SNMP管理者处理所有使用SNMP的设备间的通信和软件。支持软件提供用户接口，使网络管理员可观察整个系统的状态及单个设备的状态，并可监视特定的网络设备。

38.4 UNIX与SNMP

当大多数网络和系统管理员考虑使用SNMP时，都会想到UNIX，因为基于UNIX的SNMP

已得到了广泛的使用。当网络规模较大时，SNMP几乎是管理员的惟一选择，因为它可使管理员获得整个网络中设备的信息并及时得到问题警报。SNMP几乎已与任何版本的UNIX捆绑，且安装过程简便。经过短暂的学习，管理员可使用它有效地管理含有上千个设备的网络。对于Linux也是如此。

本节讲述如何在UNIX系统中配置安装SNMP，正如用户想到的，基于GUI的SNMP管理软件包远比基于字符的系统友好，因而许多UNIX厂商都提供特殊的SNMP管理应用的软件。

38.4.1 在UNIX和Linux上安装SNMP

大多数UNIX系统本身包含客户和服务器软件。客户软件通过snmpd守护进程执行，当在网络上使用SNMP时，客户方软件就始终执行。通常snmpd守护进程在程序启动时运行。这主要决定于rc系列启动文件。当SNMP启动时，守护进程读取配置文件。对于大多数SNMP代理，snmpd读取文件如下：

```
/etc/inet/snmpd.conf
/etc/inet/snmpd.comm
/etc/inet/snmpd.trap
```

文件所处的目录根据UNIX版本的不同而不同，用户需要检查文件系统以得到正确的位置。

snmpd.conf文件中包含四个系统MIB对象。在大部分情况下，这些对象在安装时设置，但用户也可修改对象的内容。snmpd.conf文件的示例如下：

```
#       @(#)snmpd.conf    6.3 8/21/93 - STREAMware TCP/IP  source
#
# Copyrighted as an unpublished work.
#  © Copyright 1987-1993 Lachman Technology, Inc.
# All rights reserved.
descr=SCO TCP/IP Runtime Release 2.0.0
objid=SCO.1.2.0.0
contact=Tim Parker  tparker@tpci.com
location=TPCI Int'l HQ, Richmond
```

在许多snmpd.conf文件中，用户需要填入用户及位置字段(它说明系统的用户及位置)，但descr及objid字段不需作修改。snmpd.conf文件定义的变量及相应的MIB变量如下：

```
descr          sysDescr
objid          sysObjectID
contact        sysContact
location       sysLocation
```

snmpd.comm(community)文件提供认证信息及可访问本地数据库的主机列表。远程主机访问本地SNMP数据的权限由snmpd.comm文件指定。snmpd.comm文件示例如下：

```
#       @(#)snmpd.comm    6.5 9/9/93 - STREAMware TCP/IP  source
accnting    0.0.0.0         READ
r_n_d     147.120.0.1       WRITE
public    0.0.0.0         read
interop   0.0.0.0         read
```

snmpd.comm文件的每一行包含三个字段：组织名称、远程主机的 IP地址及组织的访问权限，权限可以是READ(只读)、WRITE(可读写)及NONE(禁止访问)三种形式，可读写表示可修改MIB数据而不是文件系统。

snmpd.trap文件为当发生自陷时，需向那些主机发送消息。 snmpd.trap文件的示例如下：

```
#       @(#)snmpd.trap     6.4 9/9/93 - STREAMware TCP/IP  source
superduck 147.120.0.23    162
```

snmpd.trap文件的每一行包含三个字段：组织名称、 IP地址及发送自陷消息的UDP端口。

38.4.2 SNMP命令

UNIX提供一组基于SNMP的命令，使网络管理员可获得 MIB的信息或SNMP设备的信息。确切命令依赖于具体的实现，但大多数 SNMP系统都支持表38-1所示的命令。

表38-1 SNMP命令

命 令	描 述
getone	使用SNMP get命令获取变量的值
getnext	使用SNMP getnext命令获取下一个变量的值
getid	获取sysDescr, sysObjectID及sysUpTime的值
getmany	获取一组MIB变量的值
snmpstat	获取SNMP数据结构
getroute	获取路由信息
setany	使用SNMP set命令设置变量的值

大多数SNMP命令都需要参数指明设置或读取变量。下面列出了表 38-1所示命令的输出：

```
$ getone merlin udpInDatagrams.0
Name: udpInDatagrams.0
Value: 6
$ getid merlin public
Name: sysDescr.0
Value: UNIX System V Release 4.3
Name: sysObjectID.0
Value: Lachman.1.4.1
Name: sysUpTime.0
Value: 62521
```

没有SNMP命令被认为对用户友好，因为其响应过于简洁以致于难以理解。因此，许多基于GUI的SNMP网络管理工具渐渐流行。它提供更有效的管理手段并提供易于理解的输出方式。

基于图形界面的SNMP工具充分利用彩色显示器显示网络实时统计数据。这些工具通常比较复杂且昂贵。但是，一旦建立，它们将在网络监视及设备管理中发挥重要作用。

SNMP的重要特性之一是它及时报告网络设备故障。使用 GUI管理工作站可以在网络拓扑图中显示各设备的状态。

38.5 Windows与SNMP

Windows NT、Windows 95及Windows 98都在不同程度上支持SNMP。每个操作系统都有

可用的驱动程序可使它成为SNMP代理，某些操作系统如Windows NT和Windows 95/98还支持管理方代理。下面将介绍每个操作系统如何设置 SNMP应用。

38.5.1 Windows NT

Windows NT提供一组SNMP监视服务，它们可像标准服务一样安装。首先双击 Control Panel(控制面板)当中的Network(网络)项，选择Services(服务)页。如果列表中没有 SNMP Services，点击Add(添加)按钮，从服务列表中选中SNMP Services添加到系统中。从系统文件中读取一组驱动程序后，弹出含有三个标签页的窗体，用户可在窗体中添加配置信息。

窗体的第一页为SNMP Agent页，如图38-1所示，用来填入SNMP管理员的联系信息。在页上部的两个字段填入管理员的位置及姓名。用户也可以不填，但为了网络用户方便与管理员联系最好填写。页的下半部分显示需使用的SNMP服务。缺省设置对大多数网络均是最优设置。

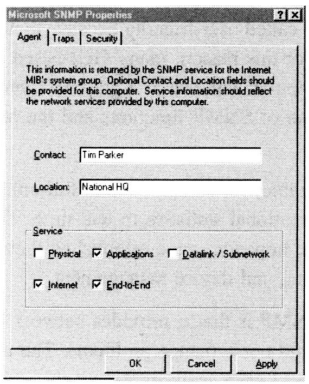

图38-1 SNMP Agent页

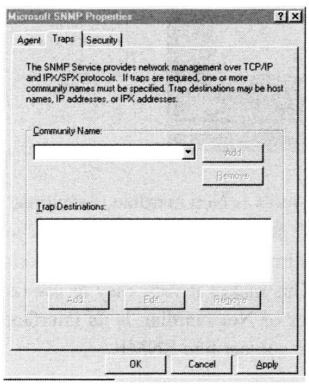

图38-2 SNMP Traps页

Traps页如图38-2所示，用来填入监视的组织名。任何列出的组织均可作为错误自陷组织。通常，所有的机器均在 Public组织下。如果用户敲入新的组织名，需要指出 SNMP监视设备的IP地址。例如，用户可将 SNMP自陷从“ research ”组织路由到“ research ” SNMP管理者。

SNMP服务窗体的最后一个标签页为 Security页(见图38-3)。该页可对SNMP服务基于组织进行严格的访问控制。页的下半部分的两个按钮可使用户仅从指定的设备接收消息。

设置完成后， Windows NT重启并激活SNMP服务。

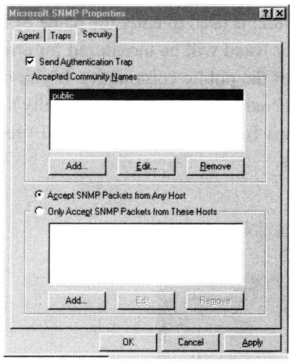

图38-3 SNMP Security页

38.5.2 Windows 95、Windows 98和Windows 3.x

大多数Windows 3.x 、Windows 95及Windows 98 SNMP代理基于public域或共享域，并可通过Web搜索引擎找到。 Windows SNMP代理都可使用户监视网络，一部分可报告网络故障，少数允许用户基于Windows平台对网络进行管理。

NetGuardian是基于Windows 95的流行工具，由lisbon大学开发。NetGuardian需要TCP/IP栈Trumpet WinSock，通常以.ZIP文件发布。解压缩后，不需要与 Windows内核连接或加载特

定的驱动程序，这使它非常容易安装使用。 NetGuardian的最显著特点是其界面，它可能是用户看到的最简洁的工具。

NetGuardian的主窗体如图38-4所示，图中显示NetGuardian存储的某个网络的拓扑图。机器上的“ X ”表示NetGuardian无法与该机器建立连接 (因为缺省的图为欧洲某网络图。因此，第一次启动时，机器上都是“ X ”)。为使NetGuardian查询用户自己的网络，需从 Net菜单上选择Discover选项。它将弹出询问需查找的地址范围的窗口，如图 38-5所示。

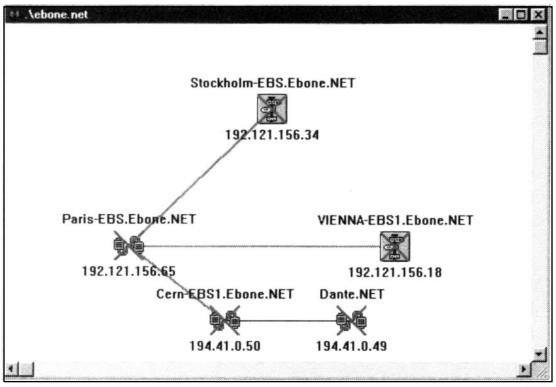

图38-4 NetGuardian窗体显示网络拓扑图

当搜索完成后，NetGuardian在新的网络图中显示结果。图38-6显示仅有三台机器的简单网络。 NetGuardian通过Ping网络中的用户指定范围内的每个 IP地址搜索机器。

使用NetGuardian简洁的界面，管理员可以检查网络中所有活跃的机器，可从添加或删除网络图中主机，重新组织网络图的结构。 NetGuardian非常容易学习和使用，并且拥有许多SNMP包缺少的特殊功能 (如图形方式显示网络性能，如图38-7所示)。

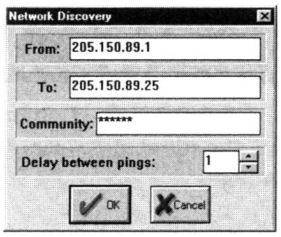

图38-5 当搜索网络时，NetGuardian询问IP地址的范围

注意 用户可从网络的许多站点下载 NetGuardian，如匿名服务器ftp.fc.ul.pt，路径为/pub/networking/snmp/netgXXXzip，其中“ XXX ”表示版本号。

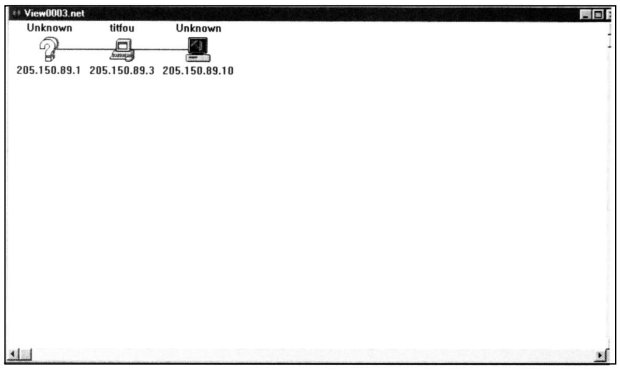

图38-6 包含三台机器的NetGuardian网络图报告网络的活跃状况

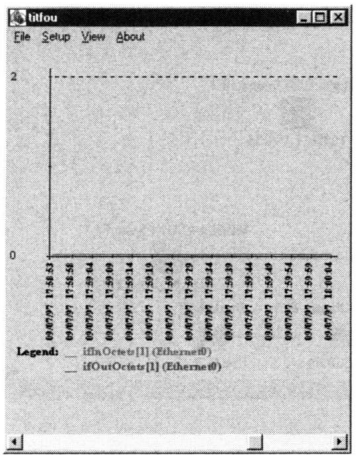

图38-7 NetGuardian以图形方式显示网络性能

38.6 小结

SNMP是管理网络设备简单有效的方法。自从1988年提出后，不断地复杂化，并且将会被CMOT所取代。但目前，SNMP仍然是管理系统的选择。SNMP的简单性是它最大的优点，厂商可花费很小的力气使其产品支持SNMP。对于网络管理员，SNMP几乎是一个完美的工具。