第37章 网 络 管 理

作者：Bernard McCargo

本章内容包括：

- 制定网络监控方案
- 网络问题及网络问题解决方案
- 网络管理工具
- 配置SNMP
- SNMP 工具和命令
- RMON及相关的MIB模型
- 建立网管需求

当网络来源于一个厂商，则由该厂商负责网络的维护。因此，在美国， AT&T和本地电话公司负责电话网， IBM管理计算部分的大型机， DEC管理工程部门的微机。网络管理者只需简单区分问题的来源，由对应的厂商来解决具体的问题。

当前，互联网络难于管理的原因主要有以下三点：

- 分布式数据处理系统取代了集中式数据处理系统。
- AT&T于1984年的解体极大地改变了 (美国)用户电话线路的管理方式。目前互联网络管理者必须与LEC(本地交换提供者)、IXC(远程交换局)及其他服务提供商接触，如：包交换公共数据网(PSPDN)。
- 电子工业的发展、数据通信技术的进步，使得电子行业的厂商如雨后春笋，层出不穷。

所有的这些发展促使厂商间的技术日益相近。厂商和标准化组织都致力于迎接上述挑战。目前占主导地位的标准ISO7498-4定义了五个不同的管理领域。

- 错误管理 —— 检查、测试和纠正网络上的错误。
- 计费管理 —— 在不同实体间分配网络费用。
- 性能管理 —— 收集和记录与性能相关的统计信息。
- 安全管理 —— 保护网络资源及对网络实施访问控制。

各种标准化组织都已开发出相应的协议支持这些标准，然而最流行的网络管理协议是简单网络管理协议(SMTP)。它由Internet(TCP/IP)组织开发，其流行主要归功于简单性：它仅定义了5种命令/响应。因此，使网络管理尽可能简单，并且减少网络成员与管理实体间管理数据的流量。

数据通信领域的厂商开发出了许多基于标准协议如 SNMP的网络管理系统，它们均采用适当的体系结构。在这一市场大的厂商有 AT&T(统一网络管理体系结构， UNMA)、DEC(管理控制中心 —— DECmcc)， Hewlett-Packard(OpenView网络管理)、Bay网络公司 (Optivity)、Cisco公司(Cisco Works)及IBM(NetView)。这一领域随着网络复杂性的增长而不断发展。

37.1 制定网络监控方案

所有这些因素：集中与分布计算体系结构、宽带传输应用、特殊的工作站、多协议、新

的局域网、城域网互连方法及完全不同的网络管理系统 —— 构成一个有趣的集合。互联网中使用了多种线缆，包括双绞线、同轴电缆和光纤。广域网硬件可以包括不相容访问部件，如CSMA/CD(IEEE 802.3)及令牌环(IEEE 802.5)。互联设备如网桥可以使用不同的算法如spanning树(IEEE 802.3)或源路由(IEEE 802.5)。从某网络操作系统发出的电子邮件包不能与其竞争者的电子邮件通信。那么用户如何分析互联网络以确保其网络工作正常呢？

首先，用户需明确网络“工作正常”的含义。这个问题可能有多种答案，对于最终用户这意味着较快的响应速度。对于管理者(非系统管理员)，意味着以较低的价格获得足够的设备。对于管理员，这意味着网络不需要花太多的精力维护其运转。对于网络工程师，答案在于带宽、转发速度、延迟等等诸如此类的因素。

设计一个运作良好的网络监控系统，必需以用户的期望和公司的限制作为考虑的出发点。设计者的任务是在一系列矛盾中权衡以满足合理的期望。“链条总是以最薄弱的地方为准”也适用于网络。所有的方面都必须平衡以获取最优性能。

有一些问题直接影响到网络性能，设计者必须加以考虑：如网络带宽、硬件容量及应用等。这些方面是构造一个网络基准的关键。网络基准是网络健壮性的写照，当发出问题时，它们可以用来进行分析比较，查找并解决问题。

37.2 网络问题及其解决方案

互联网络不断地分布化，提供更高的带宽，支持更多的协议，网络管理员必须随时准备调整网络结构并且购买新的分析工具。

分布式网络需要公司改变其原有的集中式MIS部门。独立的部门需要它们自己的网络管理职员处理与用户相关的问题。而重要的部门需要配备更好的工具和人员以处理网络上出现的问题。

高带宽互连设备的发展大大减少了已有的网络分析工具和管理设备的寿命。新技术如光纤局域网、高速城域网等变得越来越普遍，因此网络管理者需要不断地更新其诊断设备。当广域网间采用模拟线路连接时，网络管理者怀疑线路有问题，需要测试线路是否损坏应模拟传输参数如脉冲信号、延迟扭曲及脉冲过滤等。但今天的数字线路完全由高带宽光纤组成，需要采用完全不同的技术测试和分析传输指标。例如对于T1/T3线路需要测试正确的数据帧、不正确的产生信号(如BPV)、特定的数据编码(如B8ZS)。如果传输介质是光纤，而不是双绞线或同轴电缆，分析员需要光纤接口而不是电子接口。

下面是一些帮助用户解决网络问题的建议：

- 弄清问题　用户不能清楚地描述问题，就不可能有效地解决问题。
- 开发解决方案　在解决过程中需要小心谨慎并采用一些有效的方法。
- 将工作归档　用户可以不断地积累经验。
- 发布结果　其他用户可以从中获得知识。

37.3 网络管理工具

网络管理工具非常复杂，并且随着需要监控的协议数量增多，而变得更加复杂。多协议网络需要更加复杂和更智能的分析工具。分析员处理单个协议包，如SNA时，必须掌握更多的协议如SNA、DECNet和TCP/IP。为了理解这一趋势，用户必须对分析工具的工作方式有一

定了解，并且知道它的发展方向。

37.3.1 使用协议分析器

协议分析器工作如下。分析器以被动模式依附于互联网络，并且捕获在各种设备间传输的信息。这些信息可分为两类：

- 数据——数据来源于最终用户进程，如电子邮件消息。
- 控制——控制信息确保数据传输服从协议规则。

因此，控制信息通常被称为协议控制信息 (PCI)，它对于每一个协议都是惟一的。因此，如果七种协议联合实现某种网络功能，必须有七种不同的 PCI元素。这些元素通常称为头(header)，随数据一起封装入数据链接层的帧中。需要传输的数据在应用层组织，因此又称做应用层数据(AD)。应用层头(AH)被添加在AD之前，并且(AH+AD)被传送到下一层(表示层)。表示层将AH+AD看作它的数据，添加它的头 (表示层头， PH)，结果数据变为 PH+AH+AD，整个过程一直持续到整个帧中添加了每个层次的 PCI。

协议分析器的工作是将帧中的 PCI以用户可理解的格式显示出来。随着协议的不断发展这一看似简单的工作也变得越来越复杂。

协议分析器的可用性随时间变化而变迁。第一代分析器仅分析数据流并将结果以数字形式显示在CRT上，这一代分析器用户不友好。第二代分析器可以分析到 OSI第三层。它们可以面向位分析协议，用户可编程测试获得解决问题的参数。这些测试可能要求捕获到特定工作站或基于特定协议的数据如 IP协议。目前第三代协议分析工具可以解码和处理到 OSI第七层，并为用户提供编程和测试的友好界面。

第四代协议分析工具将会有什么样的功能？它们是否胜任分析 LAN、MAN及WAN的混合网络？这个问题非常关键。因为 LAN、MAN和WAN所使用的协议复杂程度不相同。虽然更高层次的信息如：信号和网络管理数据有时也使用，但 MANS和WAN一般使用OSI 1～3层。LAN覆盖了OSI 1～7层(见图37-1)，一个WAN/WAN分析器必须能在物理层、数据链路层及网络层解码获取PCI。这样，分析工具可以测试数据包所经过的通信子网，但不需要解码获得包中的信息。只有在局域网中的最终用户对包中的内容感兴趣。运行网络操作系统的工作站如Windows NT或Novell公司的NetWare，它们包含协议层1～7层。

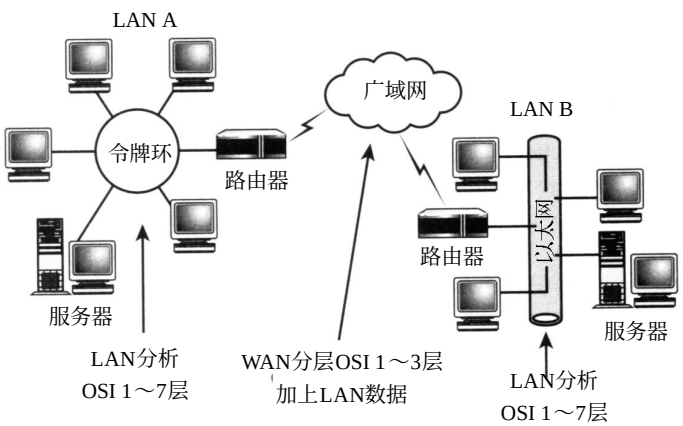

图37-1 局域网与广域网分析

为了正确地诊断在LAN A中的工作站与LAN B中的服务器通过广域网互联的问题， LAN分析器必须解码到高层。

LAN和WAN的测试要求也随着经常出现的问题类型不同而不同。 LAN的失效具有重复性而广域网的问题可能是一次性事件。 LAN与MAN或WAN的分析器的差异最终体现在空间上，MAN/WAN分析器通常使用在机房或中心办公室等空间有限的地方 (因此，它们通常设计既可为水平也可垂直使用)。LAN分析器应用于桌面上。

37.3.2 专家系统

为了保持复杂网络良好的性能，网络分析工具必须智能化。所有的分析工具都包含一些嵌入的知识如特征标识、协议、协议间交互等等。它们通过这些知识为用户提供帮助、产生测试序列或展开某端口的协议信息并使用这些信息展开其他协议信息。但是更智能的分析工具是那些包含专家系统的分析工具。

真正的专家系统能够使用一组规则结合网络和操作的知识诊断并解决网络问题。专家系统的知识来自于多种渠道，包括原理数据库 (例如：IEEE制定的网络操作标准)；特定的网络数据库(网络节点的拓扑信息)；用户的经验等。所有这些信息产生问题起因的假设和解决问题的一系列措施。例如：由以太网中过高的冲突发生率推断需对骨干线路及终结器做进一步测试并最终获得结论。

Hewlett-Packard(惠普)的LAN分析器符合专家系统的标准。 Network General分析工具包含一个称之为Expert Sniffer的专家系统，它实时自动标识问题并根据专家知识提出解决方案。其他的LAN厂商正计划开发包含专家系统的分析工具，如： Bytex和Wandel & Goltermann。

惠普的专家系统称之为 Fault Findert(错误发现者)。用户或分析员将错误症状传送给错误发现者，分析工具将基于目前的网络状况和 /或分析工具的产生测试推断出错误假设，这一过程一直持续到得到结论为止。如果没有得到结论，分析工具将显示一系列可能的错误及网络症状以便用户进一步分析。因为专家系统不断地产生假设 /测试假设，所以它对网络的影响较小。

因为WAN协议本身的复杂性，如ISDN和七号信令(SS7)，第三代WAN分析工具提供非常强大的分析功能。例如，第三代分析工具可对进入的数据流作统计分析，基于帧 (OSI第二层)或报文(OSI第三层)的统计结论可对WAN链接状况作快速诊断。较少的 CRC校验错误的帧或较少的拒绝报文表明链接状态良好。如果发生错误， WAN协议分析器将通过有选择地测试信息给出错误产生的原因，这些信息通过称之为过滤的过程从高速链接上获得。例如，只有某台工作站发生错误，分析器将设置过滤以便只捕获来自该工作站的报文。

37.3.3 基于PC的分析器

Intel 80386和80486微处理器使得微处理器在 80年代到90年代发生了巨大飞跃。随着处理能力的提高，它们日益成为建立测试环境的理想平台。便携式电脑允许用户将分析器带到远程节点。标准的总线(ISA、EISA及PCI)允许用户方便地添加其他设备，如 modem，以便进行远程访问。因此，许多分析器厂商选择 PC做为它们产品的硬件平台。 LAN分析器本身与网络操作系统类似，因此LAN分析器厂商一直都使其产品支持 PC系统。WAN分析器也逐渐转向支持PC。

当检测建立在PC平台上的分析器时，用户首先要回答以下问题：厂商是怎样定义“适用于PC”的含义及用户如何实现这些功能？首先，使用PC作分析器平台与集成了PC能力的分析器两者间存在差异。大多数厂商如CXR/Digilog和ProTools将其分析器建立在膝上电脑或桌面电脑上，而Cabletron System公司将其分析器建立在苹果机上。因此，用户可以使用这些设备作其他用途如：字处理、表单处理等。其他厂商如Wandel & Goltermann使用多处理器：一个用于PC应用，另一个用于分析器。另一种选择是GN Navtel公司开发的软件，它允许任何PC分析分析器捕获的数据。其他产品允许用户使用标准的DOS磁盘驱动器存储数据或输出到CRT或打印机。因此，用户首先必须明确“适用于PC”的具体含义。

第二个问题是实现：用户如何将PC改造为分析器？同样有三种选择。FTP软件公司的分析器是独立的软件产品，用户可以将它安装在自己的含有网卡的PC上。FTP提供支持各种网卡的版本如3Com Etherlink, Proteon ProNET等等。第二种选择是购买硬件/软件包，并将它安装在PC上。WAN分析器如Frederick Engineering公司和Progressive Computing公司的产品一般都采用这种方法。第三种选择是购买完整的系统，很多厂商都采用此种方式，如CXR/Digilog公司、惠普公司、Network General公司和TTC/LP COM公司等。因为只有一个厂商负责整个系统，因而此种选择将会受到最完善的技术支持。

37.3.4 网络管理协议支持

已有大量的文档讨论对复杂网络的集中管理需要一个统一的网络管理标准这一问题。目前，已有两种协议支持这一任务：SNMP，它在TCP/IP领域已得到广泛的应用，另一种是OSI网络管理协议：通用管理信息协议(CMIP)。根据分析器支持的协议来看，SNMP目前占有较大市场，已成为公认的标准。虽然有些分析器支持CMIP——Tekelec的WAN分析器支持CMIP，AR/Telenex支持IBM的NetView，但没有协议分析器经过它们的矩阵交换——SNMP已得到广泛的支持。

SNMP支持多种目的的网络管理。SNMP的代理开发人员或管理者可以通过捕获代理管理者的信息精确测试它们的编码。分析器也能确定代理与相应的管理者间的响应延迟时间。因为管理数据花费网络带宽，分析器也能测试网络管理网络管理信息流量与用户网络流量的比值。

Micro Technology、Novell的局域网、Kamputech、Wandel & Goltermann和Network General等均支持SNMP。Spider Systems也计划将SNMP集成到它们的产品中。

Novell将SNTP集成到其网络探针LANtern中。LANtern适用于以太网/IEEE 802.3网络及使用SNMP与SNMP网络管理节点通信。网络为LANtern探针与管理节点提供通信路径。因为LANtern是以太网监听器而不是协议分析器，它只收集网络统计信息如碰撞冲突、CRC校验错或帧差错，而不对帧进行解码。

另一个LAN分析器厂商，FTP软件公司提供一种非常有趣的产品：SNMP工具，它基于FTP的著名产品PC/TCP。SNMP工具可运行于任何DOS PC上，并且支持绝大多数网卡。同时它为专业SNMP应用提供一个开发包。

37.3.5 集成网络仿真/模型工具

当网络的主机比较集中或在同一个位置时，计算响应时间、延迟及网络增长非常容易。

网络资源的分布化使得预测这些性能参数日益困难。对当前网络的分析将有助于用户预测这些指标。

分析器在数据搜集方面性能卓越。但用户如何处理这些信息？早期的分析器仅提供捕获数据的ASCII码输出。后来，分析器将数据转化为表单或数据库文件以便进一步分析。例如：以局域网源端IP地址排列的流量表单适用于对不同部门的计费应用。

目前，大部分LAN分析器都集成了LAN仿真或建模软件工具如BONeS(ComDisco Systems公司，或LANSIM(InternetiX公司)。Quintessential是广域网仿真与建模工具的开发商，它提供接收广域网分析器的输出作为数据源的工具。典型的应用为建模测试 SNA线路的响应时间。给出从分析器获得的采样或响应延迟时间， QSI软件可以预测流量增加、应用增长而导致的网络变化。

仿真/建模软件在许多领域都非常有用，其中包括：网络最初的设计、网络重新配置或重新设计、稳定性检测等。大量的可变因素 (就目前网络研究而言已超过 100个可变的因素)用来标明工作站、服务器及使用的协议的种类和数量、流量负载等等，这些因素都必须输入模型。它们的值将会影响到仿真的结果。如：网络响应时间为服务器的数量与每个服务器的用户的函数。如果响应时间增加，管理员应考虑重新分布用户或增加服务器。使用网络分析工具获得的实际数据仿真得到的网络特征的描述比用管理员的估计值得到的仿真结果要精确得多。这一功能可应用于网络设计、增长及重新设计等过程。

Bytex、 Network General和Spider Systems的LAN分析器均支持上述仿真/建模工具中的一种，在将来，仿真/建模工具将直接集成到LAN分析器中。

37.4 配置SNMP

SNMP使网络管理员可远程解决问题，监控 Hub、路由器及其他设备。使用 SNMP，用户不需要接近设备就可获得关于设备的信息。

SNMP如果理解和使用恰当，就可成为非常有用的工具。用户可以获得大量各种设备的信息。下面是可以通过SNMP获得的信息的实例：

- 路由器的IP地址
- 打开的文件数量
- 硬件设备的空间利用率
- 运行在主机上的软件版本信息

SNMP使用分布式体系结构实现这些功能，这表示 SNMP的各部分分布在网络上完成信息收集和数据处理以提供远程管理。

因为SNMP是分布式系统，用户的管理可以在不同位置多个系统或单个系统上对网络进行管理。

微软提供的SNMP使Windows NT将其当前的状态信息发送给运行 SNMP管理系统的机器。但是这只是SNMP代理方，而不是管理工具。

以下可作为SNMP管理实用工具，其中不包括Windows NT：

- IBM NetView
- Sun NetManager
- Hewlett-Packard OpenView

37.4.1 配置Windows SNMP

下面是安装SNMP服务的理由：

• 用户需要用性能监视器监视TCP/IP。

• 用户需要用第三方应用监视基于Windows NT的系统。

假设用户已安装了TCP/IP并且具有安装使用SNMP的权限，则安装SNMP的步骤如下。

1. 安装SNMP服务

安装SNMP服务的步骤如下：

1) 打开“网络”对话框，在“服务”页中点击“添加”按钮，弹出“选择网络服务”对话框。

2) 选择SNMP服务并点击“确定”。

3) 指出Microsoft Windows NT系统文件的位置。

4) 文件拷贝完成后，弹出Microsoft SNMP属性对话框，键入公司名称和地址信息。

5) 点击“确定”关闭SNMP属性对话框，点击“关闭”退出“网络”对话框。完成后点击“确定”重启系统。

2. 安装协议

使用SNMP的第一步是安装协议，过程如下：

1) 打开“网络”对话框，点击“服务”页。

2) 选择“添加”按钮，选中“SNMP 代理”，点击“确定”按钮并敲入资源目录。

3) 关闭“网络设置”对话框并重启系统。

3. 使用SNMPUTIL测试SNMP

为了进行测试，用户首先要获得SNMPUTIL的拷贝，它可从Windows NT Resource Kit中获得。如果用户没有 Resource Kit，可在Internet上查找(但是推荐使用 Resource Kit) SNMPUTIL。

在测试前，用户需增加命令的显示行数：点击窗口控制菜单的左上角，选择“属性”。在LayOut页中，修改高度值如300。

测试步骤如下：

1) 打开DOS命令窗口。

2) 敲入以下命令：

```
SNMPUTIL get 127.0.0.1 public
.1.3.6.1.4.1.77.1.2.2.0
SNMPUTIL get 127.0.0.1 public
.1.3.6.1.4.1.77.1.2.24.0
```

3) 检查接收到的数字，要检查第一个数字，点击“控制面板”上的“服务”图标，并计算服务的数目(或使用NET STAT命令计算服务的数目)。

4) 检查第二个参数，打开域用户管理器计算用户的数量。

5) 在域用户管理器中增加用户 test。切换到命令窗口，再次敲入 SNMPUTIL命令(使用向上的方向键)。

6) 检查数字是否增加，然后敲入以下命令：

```
SNMPUTIL walk 127.0.0.1 public
.1.3.6.1.4.1.77.1.2.25
```

7) 再次点击控制面板上Services图标。停止Server服务。将出现停止Computer Browser服务的警告。

8) 再次敲入以下命令：

```
SNMPUTIL get 127.0.0.1 public
.1.3.6.1.4.1.77.1.2.2
```

9) 确认服务器没有运行，然后敲入以下命令：

```
SNMPUTIL walk 127.0.0.1 public
.1.3.6.1.4.1.77.1.2.3.1.1
```

除了Server和Computer Browser服务不列出外，所有运行的服务都列出。

注意 即使Server服务已经停止，仍然可以使用Socket访问这些信息，Server服务是一种NetBIOS服务器，因为用户可直接使用Socket，所以也可以使用SNMP代理，它使用161号UDP端口。

10) 重启Server和Computer Browser服务。

11) 如果用户想获得LAN Manager MIB的所有信息，可使用以下命令：

```
SNMPUTIL walk 127.0.0.1 public
.1.3.6.1.4.1.77
```

37.4.2 配置UNIX SNMP

在Unix系统中，协议可表述为启用、不启用并且可设置协议属性。其中协议包括 SNMP、RIP、Hello、ICMP Redirect、EGP和BGP等等。协议表述的结构可分为两类：内部协议和外部协议，但SNMP协议表述例外，采用独特的表达结构：

```
snmp  yes | no | on | off
```

这个命令控制gated是否注册SNMP守护进程的信息。SNMP不是一种路由信息，不能通过上述命令激活，用户必须单独运行 SNMP软件。上述语句仅控制 gated是否管理软件的状态。通过设置yes或on(任何一个均可)使Reporting激活，设置为no或off使之不激活。

37.4.3 SNMP安全属性

SNMP包含多个影响SNMP代理安全性的属性。在缺省情况下，代理使用组织名 (public)响应任何一个管理者。因为代理可能在用户的网络内部，也可能在网络之外，因此，用户最好修改组织名以区分机器的位置。

下面列出了所有可用的安全属性：

1) 发送认证请求(trap)。

如果SNMP访问不是来自于同一个组织或不在可接收的管理者列表内，则 SNMP代理发送认证请求。

2) 可接受的组织名。

列出代理响应的组织名列表。当管理者发送查询信息时，必须包含组织名。

3) 接受来自任何主机的SNMP报文。

响应来自任何组织的任意管理系统的所有查询。

4) 仅接受特定主机的SNMP访问报文。

仅响应列出主机的查询。

37.4.4 SNMP代理与管理

SNMP主要包括两部分：管理者与代理。

- 管理者为一个集中的工作站，用户可以管理 SNMP。
- 代理位于任何用户想要获取数据的设备。

下面章节将对两部分做详细讨论。

1. SNMP管理系统

管理系统是从客户方获取信息的关键组件。用户必须至少拥有一个管理系统才可以使用SNMP服务，管理系统负责提出问题。正如上面提到的，管理系统根据设备的类型询问相应的信息。实际上，管理系统为运行上面提到的某个软件包的计算机 (见图37-2)。

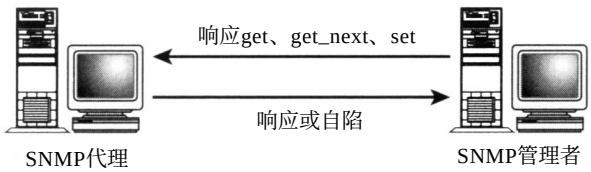

图37-2 大部分代理与管理者的通信都从管理者开始

下面是一些管理系统的命令，这些是通用命令，不针对任何特定的设备：

- get —— 获取特定的值，例如查询打开了多少活跃的会话。
- get-next —— 获取下一个对象的值。例如，用户可以查询客户方 ARP缓存然后查询每个子序列的值。
- set —— 改变可读写属性对象的值。出于安全性的考虑，该命令并不经常使用，实际上大部分对象都是只读属性。

通常一组主机中仅有一台运行 SNMP服务的管理系统。这一组主机称为一个组织。有时，用户可能需要多个管理系统。以下是需要多个管理系统的原因。

- 用户可能需要多个管理系统监视相同代理的不同方面。
- 同一个组织有不同的管理站点。
- 随着网络的扩大和复杂性，用户网络需要区分的不同领域。

2. 基于Windows的SNMP代理

我们已经了解了SNMP管理方的职责及命令。总的来说管理方是获取信息的活跃组件。

另一方面SNMP代理负责响应管理者的请求。通常代理可以是路由器、服务器或 Hub。代理通常都只被动地响应查询。

在某些特定的情况下，代理也可以是通信的发起者，比如自陷 (trap)。自陷由管理方在代理上进行设置。但是管理系统不需要查询代理是否发生自陷。当事件发生时，代理将主动向管理者发送警告信息。

在某些情况下，用户需要配置 SNMP代理的其他方面，这些方面决定设备的类型及谁将负责该系统。

这些可用的属性列举如下：

• 联系 —— 当主机的情况异常时需要通知的人名，通常是主机的用户。
• 位置 —— 这个描述性字段有助于在发送警告时获取路径信息。
• 服务 —— 该列表框中的项标识代理将监视的设备和连接的类型，它包括以下几方面：
a. 物理层　用于系统管理物理设备如中继器或 hub。
b. 应用　用于Windows NT使用基于TCP/IP的应用，通常始终被选中。
c. 数据链路/子网　表明系统管理网桥。
d. Internet　当Windows NT作为IP路由器时选中该选项。
e. 端到端　如果Windows NT使用TCP/IP时，需选此项。显然，它也始终被选中。

SNMP的任何错误都将存储在系统日志中，它记录任何 SNMP的活动。使用事件查看器可以发现问题并找到可能的解决办法。

37.5 SNMP工具及命令

现在我们已经学习了管理系统及代理。用户可以使用 SNMP命令查询不同的数据库。

管理系统向代理发送的查询信息存放在管理信息基 (MIB)中。其中是一系列可供管理系统查询的值(具体的值依赖于设备的类型)。MIB实际上是可供查询的信息数据库。

MIB数据库多种多样。存储在代理中的 MIB类似于Windows NT的注册表，也采用层次结构。MIB即可供代理也可供管理系统查询使用。

SNMP服务是Windows NT TCP/IP软件的附加组件。它支持四种 MIB，每一种都是动态链接库，可根据需要加载或卸载。它为任何运行 SNMP管理软件的TCP/IP主机提供SNMP代理服务。同时也执行以下操作：

• 向多个主机报告特殊情况如自陷。
• 响应来自多个主机的查询请求。
• 使用主机名和IP地址辨别接收信息或发送请求的主机。

SNMP应用并非来自 Windows NT，它包含在Unix系统中。对于Windows NT，需要安装 Windows NT Resource Kit。它是基于命令行方式的管理系统应用。它检查 SNMP是否安装且工作正常，用户也可使用它做命令调用。但仅依靠它进行 SNMP管理是不够的，而且用户可能因为其语法过于复杂而放弃使用。

语法结构与命令

下面是SNMP应用的通用语法结构：

```
snmputil command agent community object_identifier_(OID)
```

下面是用户可使用的命令：

• WAIK —— 遍历MIB分支，标识出在object_identifier中指出的对象。
• GET —— 返回由object_identifier指定的项的值。
• GETNEXT —— 返回由Get命令指令的对象的下一个对象对应的值。

例如：查询Wins服务器的启动时间 (假设WINS已安装且运行 SNMP代理)，可用下述命令查询WINS MIB：

```
C:\>snmputil getnext localhost public
.1.3.6.1.4.1.311.1.1.1.1
```

在上例中，第一部分指明 Microsoft分支：.1.3.6.4.1.311(或iso. org. dod. internet. private.

enterprise.microsoft)。后一部分指明特定的 MIB及需要查询的对象 :.1.1.1.1 (或. software.Wins.Par.ParWinsStartTime)。返回值如下：

Value=OCTET STRING - 01:17:22 on 11:23:1997.<0xa)

37.6 RMON及相关的MIB模型

RMON使用的对象及事件包含5种MIB模型(见表37-1)。

表37-1 与RMON相关的RFC文档

MIB模型	描 述
RMON-MIB	RFC1757：远程网络监视管理信息基(又称如RMON1，定义了203种对象和两个事件)
TOKEN-RING-RMON-MIB	RFC1513：令牌环扩展远程网络监视 MIB(又称为RMON1，令牌环扩展，定义了181种对象)
RMON2-MIB	RFC2021：远程网络监视管理信息基版本 2(又称为RMON2，也是RMON1的扩展，定义了268种对象)
HC-RMON-MIB	Internet-draft：高容量网络远程网络监视 MIB(又称为HC-RMON，包括RMON1及RMON2的定义，定义了184种对象)
SMON-MIB	Internet-draft：交换网络远程网络监视 MIB(又称为SMON或SWITCH-ROM，定义了52种对象)

5种RMON MIB模型总共定义了900多种对象。这个数字非常大，例如：仅有 56种对象用于透明网桥，110种对象用于以太网中继器。此外，除了 RMON MIB模型，远程网络监视MIB协议标识(RFC 2074)文档包含协议标识语言的定义及第一版的协议列表。用户在使用 RMON时，并不需要理解所有的对象。

37.7 建立网管需求

下面是建立网络管理组件及功能需求的一般步骤：

1. 列出信息的详细列表

首先，用户需要列出需要从每个管理对象获得的信息。详细描述每一条信息，如数据类型是什么，是平均值、计数器、无符号整数，还是文本信息。

2. 列出技术支持的组织名单

列出负责设备功能的组织名单，查询它们所能提供的服务。获得这些信息可使用户以比较简单的方式完成工作。

3. 构画报告策略

构画出设备报告的方式、方法。

4. 确定报警所需的信息(实时)

那些信息是报警(实时)所必须的：

- 建立阀值，如每一个小时三次。
- 建立报警优先级，将阀值与报警的优先级关联。
- 建立可自动运行的诊断程序或帮助信息以简化工作。
- 建立可接受的定期查询频率(如每5分钟、10分钟、1小时等)。

5. 确定建立月报表所需的信息

那些元素是建立月报表所必需的：

• 设备或服务的可用性。

• 使用频率及负载。

6. 确定调整性能所需的信息

那些信息元素与调整网络网络组件与功能相关？

查看组成数据元素的方式或对数据进行处理的方式将有助于性能调整。

7. Interview管理

它确保网络管理系统渗透到公司的所有角落。

8. 解释NMS的角色和客观性

• 解释网络管理系统的角色及其客观性。

• 提高支持组织的工作效率。

• 减小纠正错误的平均时间。

• 与支持组织和站点建立联系，交流信息。

9. 收集管理需求

• 收集公司每个单元对于网络管理的重要功能需求。

• 不要将功能局限在可管理的SNMP设备上。

• 如果设备的功能没有智能化，建议升级或更换设备。

10. 实现需求

实现需求，当集成整个系统时，注意每个需求的实现。

11. 改变监视的技术支持组织

当实现了上述步骤后，改变与管理对象或系统相关的支持组织。

12. 重新了解需求

• 经过一定时期后，重新了解各部门的需求。

• 若有必要，重新建立需求。

• 修改报告的格式及数据类型，以提高报告的易用性。

13. 提供有效的在线帮助

在实现过程中，注意帮助信息。它是任何MIS组织的重要组成。使网络管理系统可提供友好的实时帮助。

14. 测试警报

对警报进行测试是检查系统解决问题能力快速而有效的方法。如果有技术支持组织适当的参与，所有的诊断步骤都应做适当测试。不要遗漏任何必须的管理标识。

15. 训练Help Desk解决问题

训练Help Desk将问题解决的过程输入到其诊断表的恰当位置，这可使用户使用任何应用(如MS word)填写特定的设备。

16. 存档诊断过程

与一个支持组织相关的技巧在一个管理功能域中 (Management Functional Domain，MFD)，它与其他管理功能域不同。将诊断过程存档可以在整个企业共享这些知识技能。诊断过程包括问题的症状信息、解决问题的技巧及步骤等。当用户有 Desktop Support、Unix System Support、Network Support等技术资料在手边，就可以提高其处理突发问题的能力。网络管理

系统做为一个集成度很高的系统必须有较强的灵活性，并能根据公司变化而改变。

17. 简化元素管理系统(EMS)

元素管理系统如第三方的产品： SunNet Manager、HP OpenView, NetView 6000、NetView、NetMaster、3M TOPAZ、Larsecom的Integra-T必需能很方便地集成到整个系统。由于体系结构上的原因，没有EMS能意识到其他EMS的存在。EMS在更高层次实现管理，因此EMS仅在其MFD内管理它们的领域。

18. 依靠人工智能

Alarm Correlation、Diagnostics的功能都可以通过相关数据库用人工智能 (AI)原理实现。几乎所有的管理产品都采用了人工智能引擎计算组件故障的可能性。 AI引擎所得到的结论日益精确。如果将AI更全面地集成到商业应用中将发挥更大作用。

AI应用仍然需要人的干预，但这将处在更高的层次。 Network General 公司的Distributed Sniffer Server是一个优秀的人工智能应用。通过分析协议、流量、连接及 LAN控制机制的关系，DSS使用AI在问题潜伏时就作相应的处理，避免其形成较大的危害如性能下降、服务崩溃等。

此外，人工智能还可用于捕获可疑的网络行为，以帮助网络诊断。同时， AI有自学习能力，可以从过去发生的问题中获得知识，从而避免类似问题发生，或加速同类问题的解决速度。

37.8 小结

本章主要讲述了简单网络管理协议，因为它与网络管理密切相关。正如读者看到的，SNMP是一种非常简单的协议，它可以用来查询存储在管理信息基 (MIB)中的信息。这使得管理软件(如HP的OpenView)可以读取Windows NT或Unix系统中的信息。

如果用户想要使用 SNMP，必须购买 SNMP管理软件。 SNMP可直接安装，当使用Windows NT时，它允许性能查看器检测它的功能。

下面是本章讲述内容的要点：

- 用户必须理解SNMP代理仅仅是一个代理，它仅是SNMP Manager API的提供方。
- 用户需要理解管理者向代理发送的三种命令： set、get和get-next。
- 用户需要了解什么是自陷，它是由代理发送的。
- 用户需要了解代理可以监视的 5个领域并且知道所对应的含义：物理层、应用、数据链路/子网、Internet及端到端。
- 用户需要知道怎样安装代理。
- 用户需要了解如何配置认证自陷。
- 用户需要了解如何配置管理者的组织名及地址。
- 用户需要理解 MIB的结构及 Windows NT所使用的四种 MIB：LAN Manager MIBII、Internet MIBII、DHCP MIB和WINS MIB。
- 用户需要知道只有安装SNMP代理才可能激活性能监视器。

目前市场上有许多功能强大的产品不但能管理硬件，而且可管理服务和应用。系统的实现方式也非常关键，因为每个安装的管理能力必须符合整个系统的要求。此外，分散的系统必须集成并且由同一个组织管理以获得最佳性能。