目录

一、 网络管理前言

二、 传统局域网管理

三、 网络管理功能

四、 网络管理协议

五、 网络管理模型

六、 简单网络管理协议（SNMP v1）

七、 简单网络管理协议（SNMP v2）

八、 简单网络管理协议（SNMP v3）

九、 RMON

十、 网络管理系统

十一、 网络管理和维护

十二、 网络管理现状和发展

网络协议是网络管理的基础知识
网络管理服务器：一个稳定的网络离不开良好的服务器管理
网络管理软件：用好软件工具将让你的工作事半功倍
网络管理技巧进阶：网络知识的灵活运用都能成为网络管理的高级技巧
网络管理经验谈：将每次解决问题的过程全部记录下来就是你最好的管理经验

网络管理前言

随着网络技术与应用的不断发展，计算机网络在我们的日常生活中已经变得越来越普遍。特别是 20 世纪 90 年代以来，随着 Internet 在世界范围的普及，计算机网络逐渐成为人们获取信息、发布信息的重要途径，与此同时，基于计算机网络的应用也越来越多，许多人们生活中的重要环节都可以利用网络方便、快捷地实现。例如：网络商店的出现，使得人们在家里就可以选购到自己满意的商品；金融网络的发展，使得货币完全电子化，人们 再也不用在钱包中塞满纸币；还有邮电网络、各种专业大型网络等等。这些网络的发展使得大到国家经济命脉小到个人日常生活严重依赖于计算机网络，因此网络运行的稳定性、 可靠性就显得至关重要，于是网络管理就应运而生。

实际上，网络管理并不是一个什么新概念。从广义上讲，任何一个系统都需要管理，只是根据系统的大小、复杂性的高低，管理在整个系统中的重要性也就有重有轻。网络也是一个系统。追溯到 19 世纪末的电信网络，就已经有了自己相应的管理“系统”，这就是整个电话网络系统的管理员，尽管他能管理的内容非常有限。而计算机网络的管理可以说伴随着 1969 年世界上第一个计算机网络——ARPANET的产生便产生了，当时，ARPANET就有一个相应的管理系统。随后的一些网络结构，如IBM的SNA、DEC的DNA、SUN的AppleTalk等，也都有相应的管理系统。网络管理是计算机网络发展的必然产物，它随着计算机网络的发展而发展。不过，虽然网络管理很早就有，却一直没有得到应有的重视。这是因为当时的网络一是规模较小，二来复杂性不高，一个简单的网络管理系统就可以满足网络正常管理的需要，因而对其研究较少。早期的计算机网络主要是局域网，在一定范围内连接数百台计算机，因此最早的网络管理是局域网

管理。由于局域网管理主要保证在局域网内的所有计算机能够顺利传递和共享文件，因此早期的局域网管理系统与网络操作系统密不可分。但随着网络的发展，规模逐渐增大，复杂性增加，以前的网络管理技术已不能适应网络的迅速发展。而Internet的出现打破了网络的地域限制，跨地域的广域网络得到飞速发展，这时的网络管理不再局限于保证文件的传输，而是保障连接网络的网络对象(路由器、交换机、线路等)的正常运转，同时监测网络的运行 性能，优化网络的拓扑结构。网络管理系统也因此越来越独立，越来越复杂，功能也越来越完备，网络管理也发展成为计算机网络中的一个重要分支，国际上各种网络管理的标准也相继制定，网络管理逐步变得规范化、制度化。

网络系统规模的日益扩大和网络应用水平的不断提高，一方面使得网络的维护成为网络管理的重要问题之一，例如排除网络故障更加困难、维护成本上升等；另一方面，如何提高网络性能也成为网络系统应用的主要问题。虽然可以通过增强或改善网络的静态措施来提高网络的性能，比如增强网络服务器的处理能力、采用网络交换等新技术来拓宽网络的带宽等，但是网络运行过程中负载平衡等动态措施也是提高网络性能的重要方面。通过静态或动态措施提高的网络性能分别称为网络的静态性能和动态性能。而网络的动态性能的提高是通过网络管理系统即“网管系统”来加以解决的。

一般说来，网络管理就是通过某种方式对网络状态进行调整，使网络能正常、高效地运行。其目的很明确，就是使网络中的各种资源得到更加高效的利用，当网络出现故障时能及时作出报告和处理，并协调、保持网络的高效运行等。一般而言，网络管理有五大功能，它们是：网络的失效管理、网络的配置管理、网络的性能管理、网络的安全管理、网络的计费管理。这五大功能包括了保证一个网络系统正常运行的基本功能。

传统局域网管理

传统的局域网管理主要针对一定范围的局域网络，在这样的局域网络中包括的主要管理对象有：服务器、客户机、各种网络线路与集线器以及各种网络操作系统。由于在这样规模的局域网中，网络管理的对象有限，网络管理一般包括三个方面：了解网络，网络运行以及网络维护。

1．了解网络

要管好一个局域网，就必须对该局域网有清楚的了解。对该网络的清晰了解以及对各种网络信息的资料化管理记录，是保证网络正常运转以及进行各种网络维护的前提与基础。

(1)识别网络对象的硬件情况：局域网是由各种节点组成，这样的节点主要是服务器和客户机，因此首先需要识别这些节点的硬件组成。硬件识别包括了解服务器和客户机的品牌、它们的芯片速率、网卡品牌与配置情况，以及集线器的型号与品牌，这样就可以了解局域网中硬件设备的提供商并对硬件设备所能达到的性能有大体的了解。另外，对服务器的硬件还必须有进一步的了解，包括服务器的外设配置情况、硬盘驱动器的容量以及内存大小等。

(2)判别局域网的拓扑结构：了解了网络中的关键部件之后需要进一步了解它们是如何连接运行的，即网络结构下的实际布线系统。常见的三种布线的拓扑结构是星形、总线和环型拓扑结构，另外也有无线和点对点的拓扑结构，但不常用。在了解局域网的布线结构后，针对每种结构各自的优缺点，应注意其将导致的性能与故障差异。然后需要了解的是实现网络传输方式是 Ethernet，它是一种支持广泛的传输协议以及多种布线形式的成熟标准。Ethernet 是非确定型的，网络传送任务越重，越有可能发生冲突，而冲突将导致影响响应时间。所以网络上有大量活动节点时性能就会大大降低，如果 Ethernet 集线器上总是出现冲突信号的话，在熟悉网络布局后可能就得重新考虑分布网络上的用户。Ethernet 的缆线包括：粗缆 Ethernet，或叫 10Base5 Ethernet，使用大号的同轴电缆；细缆 Ethernet，也叫 10Base2 Ethernet，使用小口径的 RG-58 同轴电缆；10BaseT Ethernet，在星形结构中使用非屏蔽双绞线。对于采用 Ethernet 方式的局域网，网络管理员不仅要清楚 Ethernet 的原理，还必须了解组网所用的 Ethernet 缆线和插头以及它们的特点，这样在网络出现故障时可以帮助故障点的寻找与排除。除了 Ethernet 之外，其他的网络传输方式还有标记环(Token Ring)、光纤分布数据接口(FDDl)以及 ARCNet 等。了解局域网使用的传输方式是局域网管理的基本条件之一。

(3)确定网络的互联：首先需要确定网络连接的设备和接入网络的方式。这些设备与接入方式包括：使用调制解调器(Modem)，使用网络插座，使用 CSU／DSU 连接，使用网桥工作，使用路由器，使用网关。这些接入设备对于保证网络节点的连通以及该局域网与主干网连通有着重要作用，同时也是网络故障多发的故障点和影响网络性能的可能瓶颈所在。另一方面，还需要在网络服务器或其他网络设备上确定该局域网的所有子网和各客户机都能连通，并记录下网络中各子网以及客户机的 IP 地址分配。

(4)确定用户负载和定位：网络负载最重要的方面是用户的分布，因为每一网络和服务器上的用户数量是影响网络性能的关键因素，因此确定网络上有多少用户以及他们各自的定位尤其重要。首先，查看文件服务器上的负载，了解文件服务器正常运行的时间，查看服务器 CPU 的使用率，以及服务器上网络连接的数目，这些数据提供了网络负载的直接数据；然后，利用这些数据分析众多服务器中哪个使用率最高，哪些网络的负担最重，最后对网络用户以及负载

分布情况有个大致的了解。

2．网络运行

要使一个局域网顺利运转必须完成很多工作，这些工作包括：配置网络，即选择网络操作系统，选择网络连接协议，并根据选择的网络协议配置客户机的网络软件；然后配置网络服务器及网络的外围设备，做好网络意外预防处理；最后还有网络安全管理、网络用户权限分配以及病毒的预防与处理。

(1)配置网络；配置网络就要选择网络操作系统。传统的网络操作系统包括 UNIX， Windows NT，NetWare，VINES，Windows for Workgroups，LANtastic，PersonaI Net- Ware 等，这些网络操作系统有各自的特点，相对而言，在局域两中 Windows NT 和 Net-Ware 比较普遍。NT 最大的优势在于价格和支撑其发展的巨头 Microsoft。NT 支持 IPX 和 TCP／IP，因此在大多数网络环境中受到欢迎，另外，其安全性和网络管理功能也不错在硬件完全兼容时安装也比较方便。在现有网络中，大约 70％的网络操作系统采用了 Novell 公司的 NetWare 系列。NetWare 是一种快速而可靠的操作系统，十分类似于 DOS，它对多种网络协议和多种客户机操作系统有着完善的支持，其兼容性和模块化设计也使它领先于其它系统。

选择网络协议也是配置网络的重要组成部分。现在流行的局域网网络协议包括 IPX／SPX、TCP／IP、NETBIOS、NetBEUI 和 AppleTalk 等。比较普遍的协议是 IPX／SPX 和 TCP／IP，其中 IPX／SPX 是 NetWare 所采用的数据传输方式，在局域网中使用非常普遍；TCP／IP 是面向 Internet 所使用的网络协议，具有广泛的影响力。

在确定了网络操作系统和网络协议之后，需要配置该网络中每台客户机的网络软件。在 DOS 平台上，一般是安装相应网络协议的网络驱动软件，然后修改一些配置文件中的参数；在 GUI 的操作系统(例如 Windows 系列、Macintosh 和 OS2)中，则选择相应的对话框窗口配置网络参数；在 UNIX 系统中，主要靠修改系统配置文件来配置网络。

(2)配置网络服务器：在局域网中，服务器往往具有重要作用，一个配置良好的服务器可以顺利保障网络的运行。首先是在服务器上用磁盘和卷根据内容的性质与空间大小分配来划分工作，这样可以把不同的程序和数据按照一种顺序存放在磁盘中，而卷的使用不仅可以按一定的层次存放数据，而且可以控制用户的访问权，然后在服务器上启动网络服务进程，监测网络用户的访问。还有一些外围设备，比如共享打印机、共享外接磁盘或驱动器等，这些设备在服务器上都应正确配置。

最后还应该注意的是预防网络意外发生，首先是保证电源(特别是网络服务器的电源)，一般的方式是配置 UPS 应急电源；然后是保证服务器的环境状况(比如维持机房的温度与湿度在一定的范围)；最后是做好重要数据和系统的备份工作。备份的硬件设备包括硬盘阵列和磁带、光盘驱动器等，备份的方法很多，常用的是磁盘镜像、磁盘双工或磁盘阵列等。在进行备份时一定要做好详细记录，对备份内容进行分类并做标记。

(3)网络安全控制：网络安全控制的首要任务是管理用户注册和访问权限。在局域网上，网络操作系统一般都提供用户管理和权限分配的工具。对于局域网内，部用户，利用这些工具可以检查和设置用户信息、进行账号限制，例如改变账号密码、设置组、确定组中的账号、修改组或账号的权限、设定账号有效时间等等。定时对网络当前访问情况进行检查并做好记录，及时发现异常情况。另外，管理局域网外部权限和连接也很重要，一般局域网外部用户可能会访问该局域网，如查看已有文件、传递他们的文件或使用其他网络资源，因此对这种用户也需要建立账号，但应根据其使用网络的目的详细控制其访问权限，然后定期检查哪些用户最近没有注册，对一些不再需要的账号及时注销。

查找并消除病毒也是局域网管理的一项重要任务。病毒对局域网的危害非常严重，一种网络病毒可以通过网络迅速地传染到局域网的每一台客户机，因此及时发现并杀死病毒至关重要。有多种不同的方法可以识别病毒：在文件级上，用 CRC 技术可以将预期的文件大小或其他特征与文件被打开之前所看到的实际特征进行比较；最常用的方法是对文件进行扫描，发现已知病毒的标志、代码，从而辨认出每一种病毒的变形。一旦发现病毒，当然就要清除它。利用一些杀毒软件可以杀死病毒恢复原来的文件。另一种方法是删除有病毒的文件，然后用备份的无病毒文件替代。另外还必须对受病毒感染的服务器上的各卷进行扫描，如果在网络服务器之间或客户机之间存在通信联络，还必须去扫描其他系统。确定适当的持续的病毒防护是避免病毒侵害的最有效方法，这样的防护包括：建立和增强反病毒规则和程序；在客户机上安装和更新反病毒软件；安装基于网络的反病毒软件。

3．网络维护

网络维护是保障网络正常运行的重要方面，主要包括故障检测与排除、网络日常检查及网络升级。

(1)常见网络的故障和修复：在局域网中，最重要的故障检测工作是文件服务器的维护。只要服务器正常工作，集中存储的数据就是安全的，用户可以在需要时访问这些数据。当然，网络连接设备应保证用户能持续工作，而客户机本身也应能正常工作。

故障处理过程有四个主要部分：发现故障迹象，追踪故障的根源，排除故障，记录故障的解决方法。网络故障处理经常需要进行大量的调查研究，但相对而言只有很少的问题是真正比较复杂的。常见的情况是，故障的解决方法是很简单的，只不过被其他问题或不完全的信息掩盖了。在处理故障期间，可以参考图 1 中的流程图，以确保能对网络

故障进行逻辑的和有条理的分析。

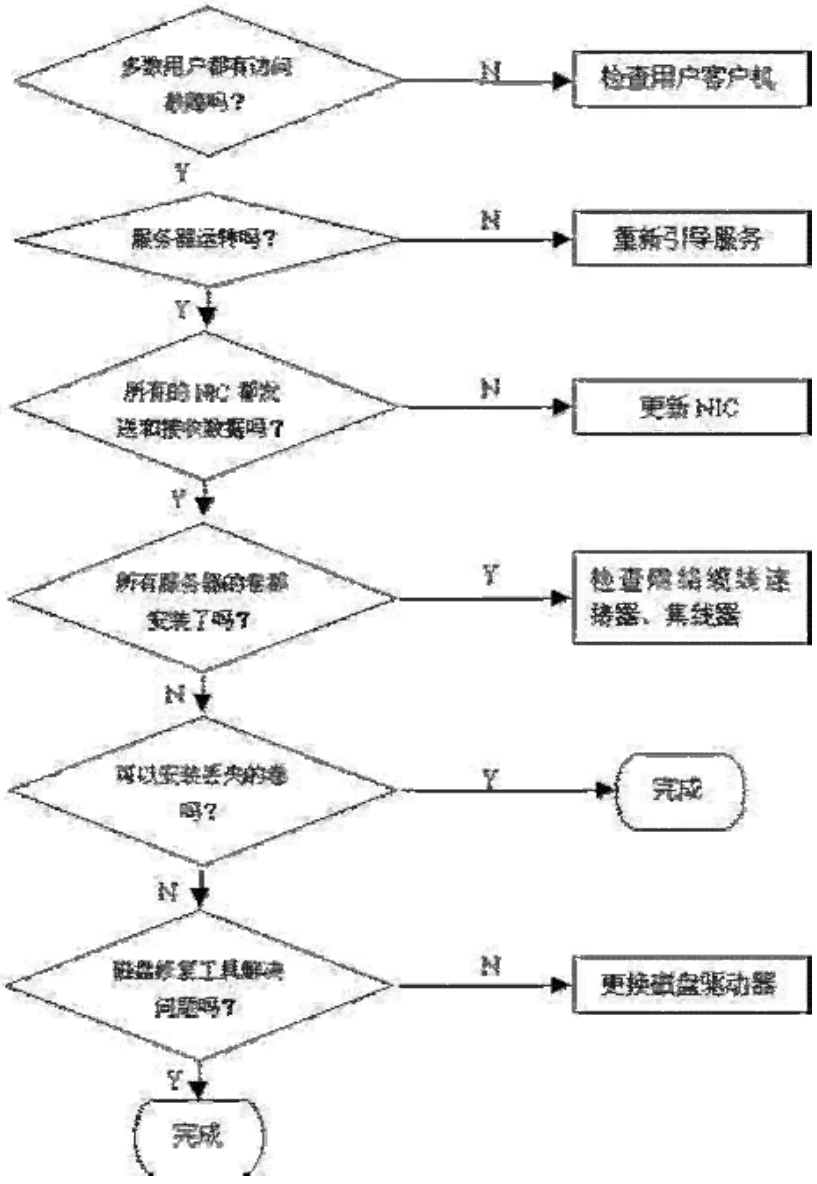
当网络管理人员收到故障报告时，首先应该检查别的用户是否也遇到同一问题，如果有多个用户报告了同类问题，那么很可能是出现了服务器或缆线故障，而不是用户客户机所引起的故障。

排除文件服务器上的错误非常关键，因为它通常会影响到很多用户，因此首先要对服务器进行认真检查：服务器是否在运行?监视器是否显示信息?服务器是否响应键盘输入？服务器控制台是否显示异常终止或其他信息?服务器NIC(网络适配器)是否发送和接收数据？服务器的卷是否已安装?

文件服务器通常是十分稳定的，但它们也特别容易出现三种类型的故障：第一类故障并不是网络操作系统本身的错误，而是由于配置的更改造成的，因此无论何时改变网络操作系统的配置都必须备份以前的配置并记录更改日期；第二类故障是部件失效，虽然 NIC 和磁盘失效是最为常见的，但从键盘端口到 SIMM 的任何部件都可能会发生故障，甚至在高品质服务器上也无法避免；第三类故障是服务器的软件模块引发的系统冲突故障，比如磁盘驱动程序或 LAN 驱动程序引发的内存故障等。

当服务器故障检查各方面都没有问题时，引起大量用户访问故障的问题很可能出现在网络缆线系统上。如果故障网络采用的是总线拓扑结构，那么故障检测工作可能会比较繁重；对于星形结构，则应检查集线器或 MAU 是否通电并能正常运行。如果连接设备本身运行良好，可检查它们与服务器的物理连接。一般而言，对于物理网络，电缆和按插件老化、电磁干扰、电缆长度限制是最常见的物理网络故障源；连接设备，如接插板、集线器和路由器也是故障多发点。

(2)网络检查：网络检查是在网络正常运转情况下对服务器状态和网络运行情况的动态信息收集和分析的过程。有些数据最好每天检查一次，而有些数据则较长时间检查一次即可。下面列出一些需要定期检查的网络关键信息：



故障检测流程图

频率	活 动	频率	活 动
每日	检查各服务器的卷空间	每日	去除旧用户
每日	列出前一天创建的文体	每月	检查用户账号安全性
每日	找出可被存档 / 删除的旧文件	每月	确保备份的完整性
每日	检查备份的执行情况	每月	更服务器模块
每日	检查服务器错误记录文件	每月	更新客户文件

(3)网络升级：网络升级是一个持续的过程，它需要考虑一些财务和预算因素。一般在网络管理中需要考虑的是必须进行的升级，这些升级能够保证网络正常运转。虽然网络操作系统的升级通常是最迫切的，但硬件和软件也可能需要升级。

服务器升级是最重要的。必须的服务器升级有三种：最简单的是用户许可证升级，如果网络服务器的能力已达到最大限度，并需要容纳更多的用户，就需要进行许可证升级；另二种服务器升级是网络操作系统的升级，如果使用的是过时的或有故障的网络操作系统，就应该升级为最新的版本；第三种服务器升级所指的范围相对来说要广泛一些，主要指硬件升级，硬件升级可能包括增加磁盘空间、改进容错措施或系统升级。另外，客户软件的升级有时也是很必要的，因为旧客户软件对于网络操作系统可能是一种沉重的负担。

在确定了最重要的升级之后，应决定需要购买的产品，并对升级费用进行评估，然后制定实施升级的工作步骤，最后应从成本和效益两方面总结新配置的优点。

网络管理功能

在实际网络管理过程中，网络管理应具有的功能非常广泛，包括了很多方面。在()SI 网络管理标准中定义了网络管理的 5 大功能：

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

这 5 大功能是网络管理最基本的功能。

事实上，网络管理还应该包括其他一些功能，比如网络规划、网络操作人员的管理等。不过除了基本的网络管理 5。大功能，其他的网络管理功能实现都与具体的网络实际条件有关，因此我们只需要关注 OSI 网络管理标准中的 5 大功能，其中：

(1)配置管理：最基本的网络管理功能。主要负责：自动发现网络拓扑结构，构造和维护网络系统的配置。监测网络被管对象的状态，完成网络关键设备配置的语法检查，配置自动生成和自动配置备份系统，对于配置的一致性进行严格的检验。

(2)故障管理；网络管理的核心。过滤、归并网络事件，有效地发现、定位网络故障，给出排错建议与排错工具，形成整套的故障发现、告警与处理机制。

(3)性能管理：采集、分析网络对象的性能数据，监测网络对象的性能，对网络线路质量进行分析。同时，统计网络运行状态信息，对网络的使用发展作出评测、估计，为网络进一步规划与调整提供依据。

(4)安全管理：结合使用用户认证、访问控制、数据传输、存储的保密与完整性机制，以保障网络管理系统本身的安全。维护系统日志，使系统的使用和网络对象的修改有据可查。控制对网络资源的访问。

5)计费管理：对网际互联设备按 IP 地址的双向流量统计，产生多种信息统计报告及流量对比，并提供网络计费工具，以便用户根据自定义的要求实施网络计费。

下面我们将针对 5 大功能中每个部分的功能进行具体的描述。

1．配置管理

(1)配置信息的自动获取：在一个大型网络中，需要管理的设备是比较多的，如果每个设备的配置信息都完全依靠管理人员的手工输入，工作量是相当大的，而且还存在出错的可能性。对于不熟悉网络结构的人员来说，这项工作甚至无法完成‘因此，一个先进的网络管理系统应该具有配置信息自动获取功能。即使在管理人员不是很熟悉网络结构和配置状况的情况下，也能通过有关的技术手段来完成对网络的配置和管理。在网络设备的配置信息中，根据获取手段大

致可以分为三类：一类是网络管理协议标准的 MIB 中定义的配置信息(包括 SNMP；和 CMIP 协议)；二类是不在网络管理协议标准中有定义，但是对设备运行比较重要的配置信息；三类就是用于管理的一些辅助信息。

(2)自动配置、自动备份及相关技术：配置信息自动获取功能相当于从网络设备中“读”信息，相应的，在网络管理应用中还有大量“写”信息的需求。同样根据设置手段对网络配置信息进行分类：一类是可以通过网络管理协议标准中定义的方法(如 SNMP 中的 set 服务)进行设置的配置信息；二类是可以通过自动登录到设备进行配置的信息；三类就是需要修改的管理性配置信息。

(3)配置一致性检查：在一个大型网络中，由于网络设备众多，而且由于管理的原因，这些设备很可能不是由同一个管理人员进行配置的。实际上‘即使是同一个管理员对设备进行的配置，也会由于各种原因导致配置一致性问题。因此，对整个网络的配置情况进行一致性检查是必需的。在网络的配置中，对网络正常运行影响最大的主要是路由器端口配置和路由信息配置，因此，要进行、致性检查的也主要是这两类信息。

(4)用户操作记录功能：配置系统的安全性是整个网络管理系统安全的核心，因此，必须对用户进行的每一配置操作进行记录。在配置管理中，需要对用户操作进行记录，并保存下来。管理人员可以随时查看特定用户在特定时间内进行的特定配置操作。

2．性能管理

(1)性能监控：由用户定义被管对象及其属性。被管对象类型包括线路和路由器；被管对象属性包括流量、延迟、丢包率、CPU 利用率、温度、内存余量。对于每个被管对象，定时采集性能数据，自动生成性能报告。

(2)阈值控制：可对每一个被管对象的每一条属性设置阈值，对于特定被管对象的特定属性，可以针对不同的时间段和性能指标进行阈值设置。可通过设置阈值检查开关控制阂值检查和告警，提供相应的阈值管理和溢出告警机制。

(3)性能分桥：对历史数据进行分析，统计和整理，计算性能指标，对性能状况作出判断，为网络规划提供参考。

(4)可视化的性能报告：对数据进行扫描和处理，生成性能趋势曲线，以直观的图形反映性能分析的结果。

(5)实时性能监控：提供了一系列实时数据采集；分析和可视化工具，用以对流量、负载、丢包、温度、内存、延迟等网络设备和线路的性能指标进行实时检测，可任意设置数据采集间隔。

(6)网络对象性能查询：可通过列表或按关键字检索被管网络对象及其属性的性能记录。

3．故障管理

(1)故障监测：主动探测或被动接收网络上的各种事件信息，并识别出其中与网络和系统故障相关的内容，对其中的关键部分保持跟踪，生成网络故障事件记录。

(2)故障报警：接收故障监测模块传来的报警信息，根据报警策略驱动不同的报警程序，以报警窗口／振铃(通知一线网络管理人员)或电子邮件(通知决策管理人员)发出网络严重故障警报。

(3)故障信息管理：依靠对事件记录的分析，定义网络故障并生成故障卡片，记录排除故障的步骤和与故障相关的值班员日志，构造排错行动记录，将事件-故障-日志构成逻辑上相互关联的整体，以反映故障产生、变化、消除的整个过程的各个方面。

(4)排错支持工具：向管理人员提供一系列的实时检测工具，对被管设备的状况进行测试并记录下测试结果以供技术人员分析和排错；根据已有的徘错经验和管理员对故障状态的描述给出对徘错行动的提示。

(5)检索／分析故障信息：浏阅并且以关键字检索查询故障管理系统中所有的数据库记录，定期收集故障记录数据，在此基础上给出被管网络系统、被管线路设备的可靠性参数。

4．安全管理

安全管理的功能分为两部分，首先是网络管理本身的安全，其次是被管网络对象的安全。

网络管理过程中，存储和传输的管理和控制信息对网络的运行和管理至关重要，一旦泄密、被篡改和伪造，将给网络造成灾难性的破坏。网络管理本身的安全由以下机制来保证：

(1)管理员身份认证，采用基于公开密钥的证书认证机制；为提高系统效率，对于信任域内(如局域网)的用户，可以使用简单口令认证。

(2)管理信息存储和传输的加密与完整性，Web 浏览器和网络管理服务器之间采用安全套接字层(SSL)传输协议，对管理信息加密传输并保证其完整性；内部存储的机密信息，如登录口令等，也是经过加密的。

(3)网络管理用户分组管理与访问控制，网络管理系统的用户(即管理员)按任务的不同分成若干用户组，不同的用户组中有不同的权限范围，对用户的操作由访问控制检查，保证用户不能越权使用网络管理系统。

(4)系统日志分析，记录用户所有的操作，使系统的操作和对网络对象的修改有据可查，同时也有助于故障的跟踪与恢复。

网络对象的安全管理有以下功能：

(1)网络资源的访问控制，通过管理路由器的访问控制链表，完成防火墙的管理功能，即从网络层(1P)和传输层(TCP)

控制对网络资源的访问，保护网络内部的设备和应用服务，防止外来的攻击。

(2)告警事件分析，接收网络对象所发出的告警事件，分析员安全相关的信息(如路由器登录信息、SNMP 认证失败信息)，实时地向管理员告警，并提供历史安全事件的检索与分析机制，及时地发现正在进行的攻击或可疑的攻击迹象。

(3)主机系统的安全漏洞检测，实时的监测主机系统的重要服务(如 WWW，DNS 等)的状态，提供安全监测工具，以搜索系统可能存在的安全漏洞或安全隐患，并给出弥补的措施。

总之，网络管理通过网关(即边界路由器)控制外来用户对网络资源的访问，以防止外来的攻击；通过告警事件的分析处理，以发现正在进行的可能的攻击；通过安全漏洞检擒来发现存在的安全隐患，以防患于未然。

5．计费管理

(1)计费数据采集：计费数据采集是整个计费系统的基础，但计费数据采集往往受到采集设备硬件与软件的制约，而且也与进行计费的网络资源有关。

(2)数据管理与数据维护：计费管理人工交互性很强，虽然有很多数据维护系统自动完成，但仍然需要人为管理，包括交纳费用的输入、联网单位信息维护，以及账单样式决定等。

(3)计费政策制定；由于计费政策经常灵活变化，因此实现用户自由制定输入计费政策尤其重要。这样需要一个制定计费政策的友好人机界面和完善的实现计费政策的数据模型。

(4)政策比较与决策支持：计费管理应该提供多套计费政策的数据比较，为政策制订提供决策依据。

(5)数据分析与费用计算：利用采集的网络资源使用数据，联网用户的详细信息以及计费政策计算网络用户资源的使用情况，并计算出应交纳的费用。

(6)数据查询：提供给每个网络用户关于自身使用网络资源情况的详细信息，网络用户根据这些信息可以计算、核对自己的收费情况

网络管理协议

随着网络的不断发展，规模增大，复杂性增加，简单的网络管理技术已不能适应网络迅速发展的要求。以往的网络管理系统往往是厂商在自己的网络系统中开发的专用系统，很难对其他厂商的网络系统、通信设备软件等进行管理，这种状况很不适应网络异构互联的发展趋势。20 世纪 80 年代初期 Internet 的出现和发展使人们进一步意识到了这一点。研究开发者们迅速展开了对网络管理的研究，并提出了多种网络管理方案，包括 HEMS、SGMP、CMIS／CMIP 等。

IAB最初制订的关于Internet管理的发展策略，其初衷是采用跳MP作为暂时的Internet管理解决方案，并在适当的时候转向CMIS／CMIP。SGMP是在NYSERNET和SURANET上开发应用的网络管理工具，而CMIS/CMIP是 20 世纪 80 年代中期国际标准化组织(ISO)和CCITT联合制订的网络管理标准。同时，IAB还分别成立了相应的工作组，对这些方案进行适当的修改，使它们更适于Internet的管理。这些工作组随后相应推出了SNMP(Simple NetWork Management Protoc011988)和CMOT(CMIP／CMIS Over TCP／IPl989)等网络管理协议，下面进行简单介绍。目前有影响的网络管理协议是SNMP（Simple Network Management Protocol）和CMIS/CMIP（the Common Management Information Service/Protocol）。它们代表了目前两大网络管理解决方案。其中，SNMP流传最广，应用最多，获得支持也最广泛，已经成为事实上的工业标准

1．SNMP

简单网络管理协议(SNMP)的前身是 1987 年发布的简单网关监控协议(SGMP)。 SGMP 给出了监控网关(OSI 第三层路由器)的直接手段，SNMP 则是在其基础上发展而来。最初，SNMP 是作为一种可提供最小网络管理功能的临时方法开发的，它具有以下两个优点：

(1)与 SNMP 相关的管理信息结构(SMI)以及管理信息库(MIB)非常简单，从而能够迅速、简便地实现；

(2)SNMP 是建立在 SGMP 基础上的，而对于 SGMP，人们积累了大量的操作经验。

SNMP 经历了两次版本升级，现在的最新版本是 SNMPv3。在前两个版本中 SNMP 功能都得到了极大的增强，而在最新的版本中，SNMP 在安全性方面有了很大的改善，SNMP 缺乏安全性的弱点正逐渐得到克服。

2．CMIS／CMIP

公共管理信息服务／公共管理信息协议(CMIS／CMIP)是哦 OSI 提供的网络管理协议簇。CMIS 定义了每个网络组成部分提供的网络管理服务，这些服务在本质上是很普通的，CMIP 则是实现 CMIS 服务的协议。

OSI 网络协议旨在为所有设备在 ISO 参考模型的每一层提供一个公共网络结构，而 CMIS／CMIP 正是这样一个用于所有网络设备的完整网络管理协议簇。

出于通用性的考虑，CMlS/CMIP 的功能与结构跟别 MP 很不相同，SNMP 是按照简单和易于实现的原则设计的，而 CMIS／CMIP 则能够提供支持一个完整网络管理方案所需的功能。

CMIS/CMIP 的整体结构是建立在使用 ISO 网络参考模型的基础上的，网络管理应用进程使用 ISO 参考模型中的应用层。也在这层上，公共管理信息服务单元(CMISE)提供了应用程序使用 CMIP 协议的接口。同时该层还包括了两个 ISO 应用协议：联系控制服务元素(ACSE)和远程操作服务元素(RpSE)，其中 ACSE 在应用程序之间建立和关闭联系，而 ROSE 则处理应用之间的请求／响应交互。另外，值得注意的是 OSI 没有在应用层之下特别为网络管理定义协议。

3．CMOT

公共管理信息服务与协议(CMOT)是在 TCP／IP 协议簇上实现 CMIS 服务，这是一种过渡性的解决方案，直到 OSI 网络管理协议被广泛采用。

CMIS 使用的应用协议并没有根据 CMOT 而修改，CMOT 仍然依赖于 CMISE、ACSE 和 ROSE 协议，这和 CMIS／CMIP 是一样的。但是，CMOT 并没有直接使用参考模型中表示层实现，而是要求在表示层中使用另外一个协议--轻量表示协议(LPP)，该协提供了目前最普通的两种传输层协议--TCP 和 UDP 的接口。

CMOT 的一个致命弱点在于它是一个过渡性的方案，而没有人会把注意力集中在一个短期方案上。相反，许多重要厂商都加入了 SNMP 潮流并在其中投入了大量资源。事实上，虽然存在 CMOT 的定义，但该协议已经很长时间没有得到任何发展了。

4．LMMP

局域网个人管理协议(LMMP)试图为 LAN 环境提供一个网络管理方案。LMMP 以前被称为 IEEE802 逻辑链路控制上的公共管理信息服务与协议(CMOL)。由于该协议直接位于 IEEE802 逻辑链路层(LLC)上，它可以不依赖于任何特定的网络层协议进行网络传输。

由于不要求任何网络层协议，LMMP 比 CMIS/CMIP 或 CMOT 都易于实现，然而没有网络层提供路由信息，LMMP 信息不能跨越路由器，从而限制了它只能在局域网中发展。但是，跨越局域网传输局限的 LMMP 信息转换代理可能会克服这一问题。

5、SNMP 与 CMIP 的比较

SNMP 与 CMIP 是网络界最主要的两种网络管理协议。在未来的网络管理中,究竟哪一种将占据优势,一直是业界争论的话题。

总的来说,SNMP 和 CMIP 两种协议是同大于异。两者的管理目标、基本组成部分都基本相同。在 MIB 库的结构方面,很多厂商将 SNMP 的 MIB 扩展成与 CMIP 的 MIB 结构相类似,而且两种协议的定义都采用相同的抽象语法符号(ASN.1)。

不同之处,首先,SNMP 面向单项信息检索,而 CMIP 则面向组合项信息检索。其次,在信息获得方面,SNMP 主要基于轮询方式,而 CMIP 主要采用报告方式。再次,在传送层支持方面,SNMP 基于无连接的 UDP,而 CMIP 倾向于有连接的数据传送。此外,两者在功能、协议规模、性能、标准化、产品化方面还有相当多的不同点

网络管理模型

SNMP 是英文“Simple Network Management Protocol”的缩写，中文意思是“简单网络管理协议”。SNMP 首先是由 Internet 工程任务组织(Internet Engineering Task Force)(IETF)的研究小组为了解决 Internet 上的路由器管理问题而提出的。

SNMP 是目前最常用的环境管理协议。SNMP 被设计成与协议无关，所以它可以在 IP，IPX，AppleTalk，OSI 以及其他用到的传输协议上被使用。SNMP 是一系列协议组和规范（见下表），

名字	说明
MIB	管理信息库
SMI	管理信息的结构和标识
SNMP	简单网络管理协议

它们提供了一种从网络上的设备中收集网络管理信息的方法。SNMP 也为设备向网络管理工作站报告问题和错误提供了一种方法。

现代计算机网络管理系统主要由四个要素组成：若干被管的代理（Managed Agents）；至少一个网络管理器（Network Manager）；一种公共网络管理协议（Network Management Protocol）；一种或多种管理信息库（MIB,Management Information Base）。其中网络管理协议是最重要的部分，它定义了网络管理器与被管代理间的通信方法，规定了管理信息库的存储结构、信息库中关键字的含义以及各种事件的处理方法。

被管代理可以是主机、路由器、网桥、打印机以及任何可以与外界交流状态信息的硬件设备。为了便于SNMP直接

管理，节点必须能运行SNMP进程，即SNMP代理（SNMP Agent）。每个代理都要维护一个本地数据库，存放它的状态、历史并影响它的运行。所有的计算机以及越来越多的网桥、路由器和外部设备都能够满足这个要求。

网络管理由管理工作站完成，它实际上是一台运行特殊管理软件的计算机。管理站运行一个或多个管理进程，它（或它们）通过SNMP协议在网络上与代理通信，发送命令以及接收应答。该协议允许管理进程查询代理的本地对象的状态，必要时对其进行修改。许多管理站都具有图形用户界面，允许网络管理者检查网络状态并在需要时采取行动。管理进程和代理之间的信息交换以SNMP信息的形式进行，SNMP信息的负载可以是SNMPv1 或SNMPv2 的协议数据单元（PDU）。PDU表示某一类管理操作（例如取得和设置管理对象）和与该操作有关的变量名称。SNMPv3 规定了可以使用信息头的用户安全模块（USM），与安全有关的处理在信息一级完成。

大多数实际网络都采用了多个制造商的设备，为了使管理站能够与所有这些不同设备进行通信，由这些设备所保持的信息必须严格定义。如果一个路由器根本不记录其分组丢失率，那么管理站向它询问时就得不到任何信息。所以SNMP极为详细地规定了每种代理应该维护的确切信息以及提供信息的确切格式。SNMP模型的最大部分就是定义谁应该记录什么信息以及该信息如何进行通信。总之，每个设备都具有一个或多个变量来描述其状态。在SNMP文字中，这些变量叫做对象（Object）。网络的所有对象都存放在一个叫做管理信息库（MIB）的数据结构中。

简单网络管理协议（SNMP v1）

简单网络管理协议(SNMP)是最早提出的网络管理协议之一，它一推出就得到了广泛的应用和支持，特别是很快得到了数百家厂商的支持，其中包括 IBM，HP，SUN 等大公司和厂商。目前 SNMP 已成为网络管理领域中事实上的工业标准，并被广泛支持和应用，大多数网络管理系统和平台都是基于 SNMP 的。

一、 SNMP 概述

SNMP 的前身是简单网关监控协议(SGMP)，用来对通信线路进行管理。随后，人们对 SGMP 进行了很大的修改，特别是加入了符合 Internet 定义的 SMI 和 MIB：体系结构，改进后的协议就是著名的 SNMP。SNMP 的目标是管理互联网 Internet 上众多厂家生产的软硬件平台，因此 SNMP 受 Internet 标准网络管理框架的影响也很大。现在 SNMP 已经出到第三个版本的协议，其功能较以前已经大大地加强和改进了。

SNMP 的体系结构是围绕着以下四个概念和目标进行设计的：保持管理代理(agent)的软件成本尽可能低；最大限度地保持远程管理的功能，以便充分利用 Internet 的网络资源；体系结构必须有扩充的余地；保持 SNMP 的独立性，不依赖于具体的计算机、网关和网络传输协议。在最近的改进中，又加入了保证 SNMP 体系本身安全性的目标。

另外，SNMP 中提供了四类管理操作：get 操作用来提取特定的网络管理信息；get-next 操作通过遍历活动来提供强大的管理信息提取能力；set 操作用来对管理信息进行控制(修改、设置)；trap 操作用来报告重要的事件。

二、 SNMF 管理控制框架与实现

1．SNMP 管理控制框架

SNMP 定义了管理进程(manager)和管理代理(agent)之间的关系，这个关系称为共同体(community)。描述共同体的语义是非常复杂的，但其句法却很简单。位于网络管理工作站(运行管理进程)上和各网络元素上利用 SNMP 相互通信对网络进行管理的软件统统称为 SNMP 应用实体。若干个应用实体和 SNMP 组合起来形成一个共同体，不同的共同体之间用名字来区分，共同体的名字则必须符合 Internet 的层次结构命名规则，由无保留意义的字符串组成。此外，一个 SNMP 应用实体可以加入多个共同体。

SNMP 的应用实体对 Internet 管理信息库中的管理对象进行操作。一个 SNMP 应用实体可操作的管理对象子集称为 SNMP MIB 授权范围。SNMP 应用实体对授权范围内管理对象的访问仍然还有进一步的访问控制限制，比如只读、可读写等。SNMP 体系结构中要求对每个共同体都规定其授权范围及其对每个对象的访问方式。记录这些定义的文件称为“共同体定义文件”。

SNMP 的报文总是源自每个应用实体，报文中包括该应用实体所在的共同体的名字。这种报文在 SNMP 中称为“有身份标志的报文”，共同体名字是在管理进程和管理代理之间交换管理信息报文时使用的。管理信息报文中包括以下两部分内容：

(1)共同体名，加上发送方的一些标识信息(附加信息)，用以验证发送方确实是共同体中的成员，共同体实际上就是用来实现管理应用实体之间身份鉴别的；

(2)数据，这是两个管理应用实体之间真正需要交换的信息。

在第三版本前的 SNMP 中只是实现了简单的身份鉴别，接收方仅凭共同体名来判定收发双方是否在同一个共同体中，而前面提到的附加倍息尚未应用。接收方在验明发送报文的管理代理或管理进程的身份后要对其访问权限进行检查。访问权限检查涉及到以下因素：

(1)一个共同体内各成员可以对哪些对象进行读写等管理操作，这些可读写对象称为该共同体的“授权对象”(在授权范围内)；

(2)共同体成员对授权范围内每个对象定义了访问模式：只读或可读写；

(3)规定授权范围内每个管理对象(类)可进行的操作(包括 get，get-next，set 和 trap)；

(4)管理信息库(MIB)对每个对象的访问方式限制(如 MIB 中可以规定哪些对象只能读而不能写等)。

管理代理通过上述预先定义的访问模式和权限来决定共同体中其他成员要求的管理对象访问(操作)是否允许。共同体概念同样适用于转换代理(Proxy agent)，只不过转换代理中包含的对象主要是其他设备的内容。

2．SNMP 实现方式为了提供遍历管理信息库的手段，SNMP 在其 MIB 中采用了树状命名方法对每个管理对象实例命名。每个对象实例的名字都由对象类名字加上一个后缀构成。对象类的名字是不会相互重复的，因而不同对象类的对象实例之间也少有重名的危险。

在共同体的定义中一般要规定该共同体授权的管理对象范围，相应地也就规定了哪些对象实例是该共同体的“管辖范围”，据此，共同体的定义可以想象为一个多叉树，以词典序提供了遍历所有管理对象实例的手段。有了这个手段，SNMP 就可以使用 get-next 操作符，顺序地从一个对象找到下一个对象。get-next(object-instance)操作返回的结果是一个对象实例标识符及其相关信息，该对象实例在上面的多叉树中紧排在指定标识符；bject-instance 对象的后面。这种手段的优点在于，即使不知道管理对象实例的具体名字，管理系统也能逐个地找到它，并提取到它的有关信息。遍历所有管理对象的过程可以从第一个对象实例开始(这个实例一定要给出)，然后逐次使用 get-next，直到返回一个差错(表示不存在的管理对象实例)结束(完成遍历)。

由于信息是以表格形式(一种数据结构)存放的，在 SNMP 的管理概念中，把所有表格都视为子树，其中一张表格(及其名字)是相应子树的根节点，每个列是根下面的子节点，一列中的每个行则是该列节点下面的子节点，并且是子树的叶节点，如下图所示。因此，按照前面的子树遍历思路，对表格的遍历是先访问第一列的所有元素，再访问第二列的所有元素……，直到最后一个元素。若试图得到最后一个元素的“下一个”元素，则返回差错标记。

三、SNMP 管理信息库 MIB

1、不得不说的：MIB 和 SMI

前面已经提到，为了实现 SNMP 协议的与设备和传输协议无关，必然要设定一种中间的传输方式，来实现信息的传递。在 RPC 中采用了 XDR 表示方法，在 SNMP 中则设定了一种 SMI(Structure of Management Information)结构来传递 SNMP 信息，而 SMI 的具体表现就是 SNMP 的设计核心:MIB (Manage Information Base)管理信息库。

MIB 在表现形式上，是一组属性的集合与详细描述，每一组属性都称为一个对象。每一个对象都有以下四个属性：

- 对象类型（Object Type）
- 语法（Syntax）
- 访问（Access）
- 状态（Status）

对象类型(Object Type)定义了一个特定对象的名字，例如 sysUpTime。这个名字只是一个标示符。MIB 对象既可以用这个标示符来表示，也可以用相应的 MIB 号码来表示。

例如定义 internet OBJECT IDENTIFIER : : = { iso org(3) dod(6) 1 } 那么既可以用 internet 也可以用字串 .1.3.6.1 来表示这个对象。

语法(Syntax)这个属性指定了数据类型，例如整数、8 位组串数字（字符串；范围为 0 至 255）、对象标识符(预先定义的数据类型别名）或 NULL。NULL 是留待的后使用的空位。

访问(Access)表明了这个特定对象的访问级别。合法的值有：只读、读写、只写和不可存取。

状态(Status)定义了这个对象的实现需要：必备的(被管理节点必须实现该对象);可选的(被管理对象可能实现该对象):或者已废弃的（被管理设备不需要再实现该对象）

2、MIB 结构

管理信息库MIB指明了网络元素所维持的变量（即能够被管理进程查询和设置的信息）。MIB给出了一个网络中所有可能的被管理对象的集合的数据结构。SNMP的管理信息库采用和域名系统DNS相似的树型结构，它的根在最上面，根没有名字。图 3 画的是管理信息库的一部分，它又称为对象命名（objectnamingtree）。

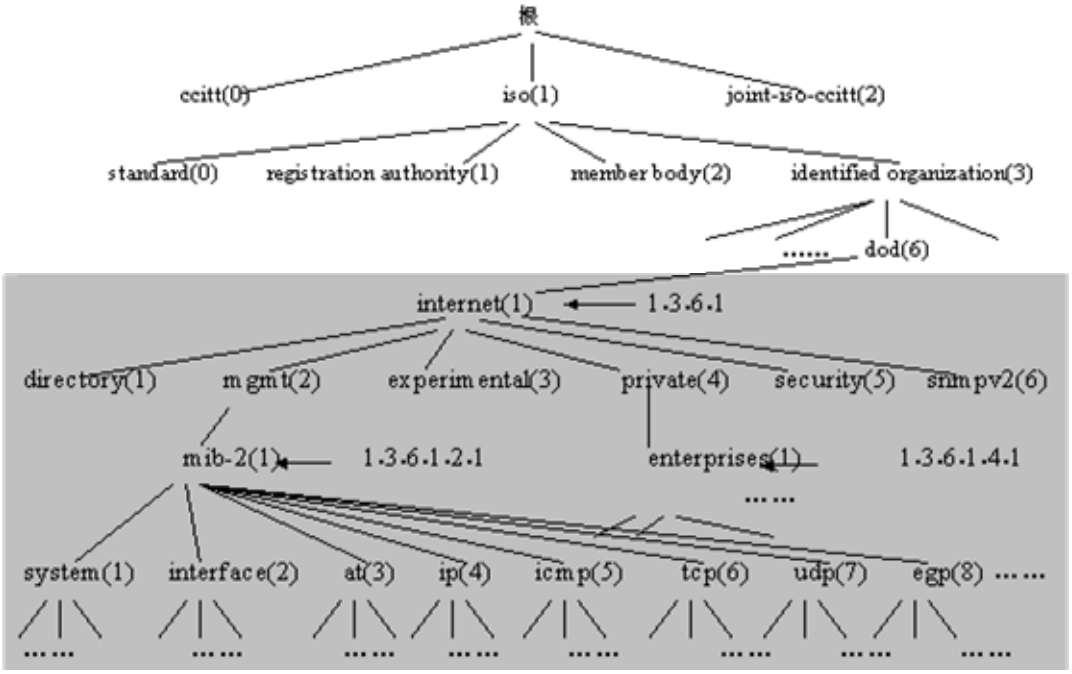


图 3 管理信息库的对象命名举例

对象命名树的顶级对象有三个，即 ISO、ITU-T 和这两个组织的联合体。在 ISO 的下面有 4 个结点，其中的一个（标号 3）是被标识的组织。在其下面有一个美国国防部（Department of Defense）的子树（标号是 6），再下面就是 Internet（标号是 1）。在只讨论 Internet 中的对象时，可只画出 Internet 以下的子树(图中带阴影的虚线方框)，并在 Internet 结点旁边标注上{1.3.6.1}即可。

在 Internet 结点下面的第二个结点是 mgmt（管理），标号是 2。再下面是管理信息库，原先的结点名是 mib。1991 年定义了新的版本 MIB-II，故结点名现改为 mib-2，其标识为{1.3.6.1.2.1}，或{Internet(1) .2.1}。这种标识为对象标识符。

最初的结点 mib 将其所管理的信息分为 8 个类别，见表 1。现在 de mib-2 所包含的信息类别已超过 40 个。

表 1 最初的结点 mib 管理的信息类别

类别	标号	所包含的信息
system	(1)	主机或路由器的操作系统
interfaces	(2)	各种网络接口及它们的测定通信量
address translation	(3)	地址转换（例如 ARP 映射）
ip	(4)	Internet 软件（IP 分组统计）
icmp	(5)	

tcp udp egp	(6) (7) (8)	ICMP 软件（已收到 ICMP 消息的统计） TCP软件（算法、参数和统计） UDP软件（UDP通信量统计） EGP软件（外部网关协议通信量统计）

应当指出，MIB的定义与具体的网络管理协议无关，这对于厂商和用户都有利。厂商可以在产品（如路由器）中包含SNMP代理软件，并保证在定义新的MIB项目后该软件仍遵守标准。用户可以使用同一网络管理客户软件来管理具有不同版本的MIB的多个路由器。当然，一个没有新的MIB项目的路由器不能提供这些项目的信息。
这里要提一下MIB中的对象{1.3.6.1.4.1}，即enterprises（企业），其所属结点数已超过 3000。例如IBM为11.3.6.1.4.1.2}，Cisco为{1.3.6.1.4.1.9}，Novell为{1.3.6.1.4.1.23}等。世界上任何一个公司、学校只要用电子邮件发往iana-mib@isi.edu进行申请即可获得一个结点名。这样各厂家就可以定义自己的产品的被管理对象名，使它能用SNMP进行管理。

SNMP 的实现机制

SNMP 规定了 5 种协议数据单元 PDU（也就是 SNMP 报文），用来在管理进程和代理之间的交换。这 5 种协议数据单元被称为 SNMP 的请求响应原语。

- get-request 操作：从代理进程处提取一个或多个参数值
- get-next-request 操作：从代理进程处提取紧跟当前参数值的下一个参数值
- set-request 操作：设置代理进程的一个或多个参数值
- get-response 操作：返回的一个或多个参数值。这个操作是由代理进程发出的，它是前面三种操作的响应操作。
- trap 操作：代理进程主动发出的报文，通知管理进程有某些事情发生。

前面的 3 种操作是由管理进程向代理进程发出的，后面的 2 个操作是代理进程发给管理进程的，为了简化起见，前面 3 个操作今后叫做 get、get-next 和 set 操作。图 4 描述了 SNMP 的这 5 种报文操作。

SNMP 中各种管理信息大多以表格形式存在，一个表格对应一个对象类，每个元素对应于该类的一个对象实例。那么，管理信息表对象中单个元素(对象实例)的操作可以用前面提到的 get-next 方法，也可以用后面将介绍的 get / set 等操作。下面主要介绍表格内一行信息的整体操作。
(1)增加一行：通过 SNMP 只用一次 set 操作就可在一个表格中增加一行。操作中的每个变量都对应于待增加行中的一个列元素，包括对象实例标识符。如果一个表格中有 8 列，则 set 操作中必须给出 8 个操作数，分别对应 8 个列中的相应元素。
(2)删除一行：删除一行也可以通过 SNMP 调用一次 set 操作完成，并且比增加一行还简单。删除一行只需要用 set 操作将该行中的任意一个元素(对象实例)设置成“非法”即可。但该操作有一个例外：地址翻译组对象中有一个特殊的表(地址变换表)，该表中未定义一个元素的“非法”条件。因此，SNMP 中采用的办法是将该表中的地址设置成空串，而空字符串将被视为非法元素。

至于删除一行时，表中的一行元素是否真的在表中消失，则与每个设备(管理代理)的具体实现有关。因此，网络管理操作中，运行管理进程可能从管理代理中得到“非法”数据，即已经删除的不再使用的元素的内容，因此管理进程必须能通过各数据字段的内容来判断数据的合法性

注意：在代理进程端是用熟知端口 161 俩接收 get 或 set 报文，而在管理进程端是用熟知端口 162 来接收 trap 报文。

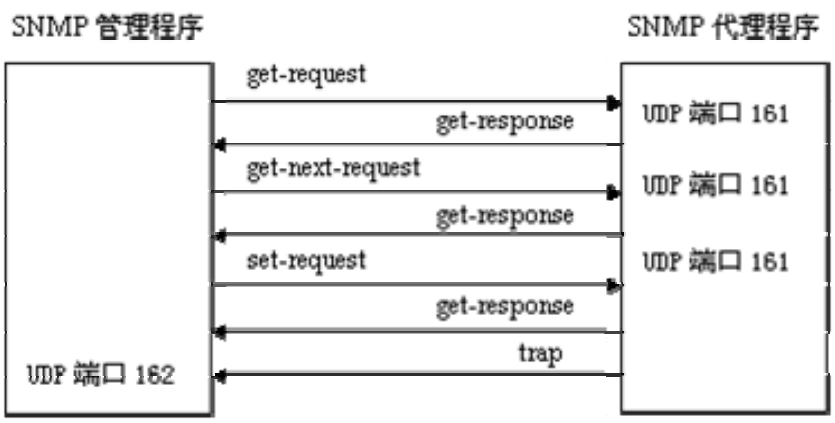
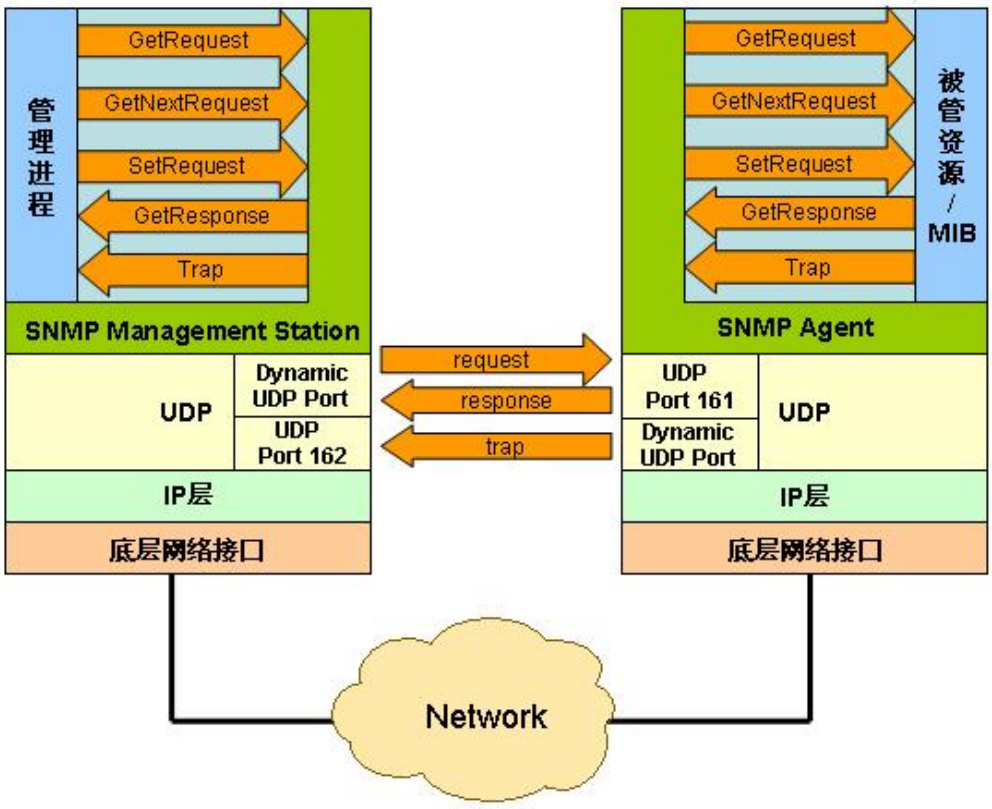


图 4 SNMP 的 5 种报文操作



SNMPv1模型示意图

四、SNMP 数据类型

SNMP 中，数据类型并不多。这里我们就讨论这些数据类型，而不关心这些数据类型在实际中是如何编码的。

- INTEGER 一个变量虽然定义为整型，但也有多种形式。有些整型变量没有范围限制，有些整型变量定义为特定的数值（例如，IP 的转发标志就只有允许转发时的或者不允许转发时的这两种），有些整型变量定义一个特定的范围（例如，UDP 和 TCP 的端口号就从 0 到 65535）。
- OCTERSTRING 0 或多个 8bit 字节，每个字节值在 0～255 之间。对于这种数据类型和下一种数据类型的 BER 编码，字符串的字节个数要超过字符串本身的长度。这些字符串不是以 NULL 结尾的字符串。
- DisplayString 0 或多个 8bit 字节，但是每个字节必须是 ASCII 码。在 MIB-II 中，所有该类型的变量不能超过 255 个字符（0 个字符是可以的）。
- OBJECTIDENTIFIER
  - NULL 代表相关的变量没有值。例如，在 get 或 get-next 操作中，变量的值就是 NULL，因为这些值还有待到代理进程处去取。
  - IpAddress 4 字节长度的 OCTERSTRING，以网络序表示的 IP 地址。每个字节代表 IP 地址的一个字段。
  - PhysAddress OCTERSTRING 类型，代表物理地址（例如以太网物理地址为 6 个字节长度）。
  - Counter 非负的整数，可从 0 递增到 232—1（4294976295）。达到最大值后归 0。
  - Gauge 非负的整数，取值范围为从 0 到 4294976295(或增或减)。达到最大值后锁定直到复位。例如，MIB中的tcpCurrEstab就是这种类型的变量的一个例子，它代表目前在ESTABLISHED或CLOSE_WAIT状态的TCP连接数。
  - TimeTicks 时间计数器，以 0.01 秒为单位递增，但是不同的变量可以有不同的递增幅度。所以在定义这种类型的变量的时候，必须指定递增幅度。例如，MIB 中的 sysUpTime 变量就是这种类型的变量，代表代理进程从启动开始的时间长度，以多少个百分之一秒的数目来表示。
  - SEQUENCE 这一数据类型与 C 程序设计语言中的“structure”类似。一个 SEQUENCE 包括 0 个或多个元素，每一个元素又是另一个 ASN.1 数据类型。例如，MIB 中的 UdpEntry 就是这种类型的变量。它代表在代理进程侧目前“激活”的 UDP 数量（“激活”表示目前被应用程序所用）。在这个变量中包含两个元素：
  - IpAddress 类型中的 udpLocalAddress，表示 IP 地址。
  - INTEGER 类型中的 udpLocalPort，从 0 到 65535，表示端口号。
  - SEQUENDEOF 这是一个向量的定义，其所有元素具有相同的类型。如果每一个元素都具有简单的数据类型，例如是整数类型，那么我们就得到一个简单的向量（一个一维向量）。但是我们将看到，SNMP 在使用这个数据类型时，其向量中的每一个元素是一个 SEQUENCE（结构）。因而可以将它看成为一个二维数组或表。

五、SNMP 报文格式

图 5 是封装成 UDP 数据报的 5 种操作的 SNMP 报文格式。可见一个 SNMP 报文共有三个部分组成，即公共 SNMP 首部、get/set 首部 trap 首部、变量绑定。

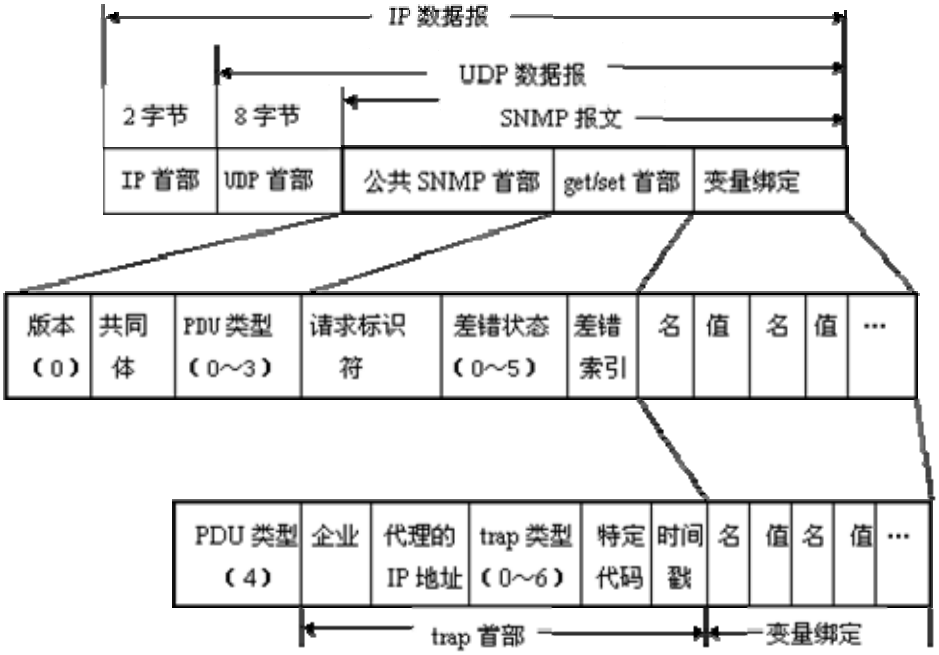


图 5 SNMP 报文格式

（1）公共 SNMP 首部
共三个字段：

- 版本
  写入版本字段的是版本号减 1，对于 SNMP（即 SNMPV1）则应写入 0。
- 共同体（community）
  共同体的概念：SNMP 网络管理是一种分布式应用，这种应用的特点是管理站和被管理 站之间的关系可以是一对多的关系，即一个管理站可以管理多个代理，从而管理多个被 管理设备。只有属于同一团体的管理站和被管理站才能互相作用，发送给不同团体的报 文被忽略。SNMP 的团体是一个代理和多个管理站之间的认证和访问控制关系。共同体就是一个字符串，作为管理进程和代理进程之间的明文口令，常用的是 6 个字符“public”。
- PDU 类型
  根据 PDU 的类型，填入 0～4 中的一个数字，其对应关系如表 2 所示意图。

表 2 PDU 类型

PDU 类型	名称
0	get-request
1	get-next-request
2	get-response
3	set-request
4	trap

2）get/set 首部

- 请求标识符(request ID)

这是由管理进程设置的一个整数值。代理进程在发送 get-response 报文时也要返回此请求标识符。管理进程可同时向许多代理发出 get 报文，这些报文都使用 UDP 传送，先发送的有可能后到达。设置了请求标识符可使管理进程能够识别返回的响应报文对于哪一个请求报文

- 差错状态（error　status）
  由代理进程回答时填入 0～5 中的一个数字，见表 3 的描述

表 3 差错状态描述

差错状态	名字	说明
0	noError	一切正常
1	tooBig	代理无法将回答装入到一个SNMP报文之中
2	noSuchName	操作指明了一个不存在的变量
3	badValue	一个 set 操作指明了一个无效值或无效语法
4	readOnly	管理进程试图修改一个只读变量
5	genErr	某些其他的差错

- 差错索引(error　index)
  当出现 noSuchName、badValue 或 readOnly 的差错时，由代理进程在回答时设置的一个整数，它指明有差错的变量在变量列表中的偏移。

（3）trap 首部

- 企业（enterprise）。填入 trap 报文的网络设备的对象标识符。此对象标识符肯定是在图 3 的对象命名树上的 enterprise 结点{1.3.6.1.4.1}下面的一棵子树上。
- trap 类型。此字段正式的名称是 generic-trap，共分为表 4 中的 7 种。

trap 类型	名字	说明
0	coldStart	代理进行了初始化
1	warmStart	代理进行了重新初始化
2	linkDown	一个接口从工作状态变为故障状态
3	linkUp	一个接口从故障状态变为工作状态
4	authenticationFailure	从SNMP管理进程接收到具有一个无效共同体的报文
5	egpNeighborLoss	一个 EGP 相邻路由器变为故障状态
6	enterpriseSpecific	代理自定义的事件，需要用后面的“特定代码”来指明

当使用上述类型 2、3、5 时，在报文后面变量部分的第一个变量应标识响应的接口。

- 特定代码(specific-code)。指明代理自定义的时间（若 trap 类型为 6），否则为 0。
- 时间戳(timestamp)。指明自代理进程初始化到 trap 报告的事件发生所经历的时间，单位为 10ms。例如时间戳为 1908 表明在代理初始化后 1908ms 发生了该时间。

（4）变量绑定(variable-bindings)
指明一个或多个变量的名和对应的值。在 get 或 get-next 报文中，变量的值应忽略

六、SNMP 网络管理工作站数据收集方法

在网络管理中有两种方法实现信息的传递，一种是轮询，只有当管理工作站发出请求时代理端才反馈回信息；另一种是中断(或称为自陷 Trap)，当代理端发现有事件触发时，就主动反馈一条信息给管理工作站。

在 SNMP 协议中 get 集指令用来获取对象信息，set 指令用来设置对象属性，trap 指令用来实现中端消息的传递。

在 SNMP 协议工作时，如果采用轮询方式，Agent 端设备监听 UDP 端口 161 进行通讯；如果采用中断方式，ManagerWorkstation 端监听 UDP 端口 162 进行通讯。
过程如下：

轮询模式
管理工作站 ==> Network ==> Agent(Listen:UDP 161) <== Device get 指令 转换成 snmp 消息格式 验证权限，处理请求并反馈管理工作站 <== Network <== Agent <== Device

如果你只使用只轮询的方法，那么网络管理工作站总是在控制之下。而这种方法的缺陷在于信息的实时性，尤其是错误的实时性。

自陷模式
管理工作站(Listen:UDP 162) <== Network <== Agent <== Device 监听 UCP 162 转换成 snmp 消息格式 当设备事件发生时主动反馈信息

基于中断的方法可以在出现异常事件时，立即通知网络管理工作站。但产生错误或自陷需要系统资源

七、SNMP 的风险及防范

接入 Internet 的网络面临许多风险，Web 服务器可能面临攻击，邮件服务器的安全也令人担忧。但除 此之外，网络上可能还存在一些隐性的漏洞。大多数网络总有一些设备运行着 SNMP 服务，许多时候这些 SNMP 服务是不必要的，但却没有引起网络管理员的重视。

根据 SANS 协会（http://www.sans.org）的报告，对于接入 Internet 的主机，SNMP 是威胁安全的十大首要因素之一；同时，SNMP 还是 Internet 主机上最常见的服务之一。特别地，SNMP 服务通常在位于网络边缘的设备（防火墙保护圈之外的设备）上运行，进一步加剧了 SNMP 带来的风险。这一切听起来出人意料，但其实事情不应该是这样的。

一、背景知识

SNMP 开发于九十年代早期，其目的是简化大型网络中设备的管理和数据的获取。许多与网络有关的软件包，如 HP 的 OpenView 和 Nortel Networks 的 Optivity Network Management System，还有 Multi Router Traffic Grapher（MRTG）之类的免费软件，都用 SNMP 服务来简化网络的管理和维护。

由于 SNMP 的效果实在太好了，所以网络硬件厂商开始把 SNMP 加入到它们制造的每一台设备。今天，各种网络设备上都可以看到默认启用的 SNMP 服务，从交换机到路由器，从防火墙到网络打印机，无一例外。

仅仅是分布广泛还不足以造成威胁，问题是许多厂商安装的 SNMP 都采用了默认的通信字符串（例如密码），这些通信字符串是程序获取设备信息和修改配置必不可少的。采用默认通信字符串的好处是网络上的软件可以直接访问设备，无需经过复杂的配置。

通信字符串主要包含两类命令：GET 命令，SET 命令。GET 命令从设备读取数据，这些数据通常是操作参数，例如连接状态、接口名称等。SET 命令允许设置设备的某些参数，这类功能一般有限制，例如关闭某个网络接口、修改路由器参数等功能。但很显然，GET、SET 命令都可能被用于拒绝服务攻击（DoS）和恶意修改网络参数。

最常见的默认通信字符串是 public（只读）和 private（读/写），除此之外还有许多厂商私有的默认通信字符串。几乎所有运行 SNMP 的网络设备上，都可以找到某种形式的默认通信字符串。

SNMP 2.0 和 SNMP 1.0 的安全机制比较脆弱，通信不加密，所有通信字符串和数据都以明文形式发送。攻击者一旦捕获了网络通信，就可以利用各种嗅探工具直接获取通信字符串，即使用户改变了通信字符串的默认值也无济于事。

近几年才出现的 SNMP 3.0 解决了一部分问题。为保护通信字符串，SNMP 3.0 使用 DES（Data Encryption Standard）算法加密数据通信；另外，SNMP 3.0 还能够用 MD5 和 SHA（Secure Hash Algorithm）技术验证节点的标识符，从而防止攻击者冒充管理节点的身份操作网络。

虽然 SNMP 3.0 出现已经有一段时间了，但目前还没有广泛应用。如果设备是 2、3 年前的产品，很可能根本不支持 SNMP 3.0；甚至有些较新的设备也只有 SNMP 2.0 或 SNMP 1.0。

即使设备已经支持 SNMP 3.0，许多厂商使用的还是标准的通信字符串，这些字符串对黑客组织来说根本不是秘密。因此，虽然 SNMP 3.0 比以前的版本提供了更多的安全特性，如果配置不当，其实际效果仍旧有限。

二、禁用 SNMP

要避免 SNMP 服务带来的安全风险，最彻底的办法是禁用 SNMP。如果你没有用 SNMP 来管理网络，那就没有必要运行它；如果你不清楚是否有必要运行 SNMP，很可能实际上不需要。即使你打算以后使用 SNMP，只要现在没有用，也应该先禁用 SNMP，直到确实需要使用 SNMP 时才启用它。

下面列出了如何在常见的平台上禁用 SNMP 服务。

■ Windows XP 和 Windows 2000

在 XP 和 Win 2K 中，右击“我的电脑”，选择“管理”。展开“服务和应用程序”、“服务”，从服务的清单中选择 SNMP 服务，停止该服务。然后打开服务的“属性”对话框，将启动类型该为“禁用”（按照微软的默认设置，Win 2K/XP 默认不安装 SNMP 服务，但许多软件会自动安装该服务）。

■ Windows NT 4.0

选择“开始”→“设置”，打开服务设置程序，在服务清单中选择 SNMP 服务，停止该服务，然后将它的启动类型该为禁用。

■ Windows 9x

打开控制面板的网络设置程序，在“配置”页中，从已安装的组件清单中选择“Microsoft SNMP 代理”，点击“删除”。检查 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices 和 HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\Windows\CurrentVersion\Run 注册键，确认不存在 snmp.exe。

■ Cisco Systems 硬件

对于 Cisco 的网络硬件，执行“no SNMP-server”命令禁用 SNMP 服务。如果要检查 SNMP 是否关闭，可执行“show SNMP”命令。这些命令只适用于运行 Cisco IOS 的平台；对于非 IOS 的 Cisco 设备，请参考随机文档。

■ HP 硬件

对于所有使用 JetDirect 卡（绝大部分 HP 网络打印机都使用它）的 HP 网络设备，用 telnet 连接到 JetDirect 卡的 IP 地址，然后执行下面的命令：

```
SNMP-config: 0
quit
```

这些命令将关闭设备的 SNMP 服务。但必须注意的是，禁用 SNMP 服务会影响服务的发现操作以及利用 SNMP 获取设备状态的端口监视机制。

■ Red Hat Linux

对于 Red Hat Linux，可以用 Linuxconf 工具从自动启动的服务清单中删除 SNMP，或者直接从/etc/services 文件删除启动 SNMP 的行。对于其他 Linux 系统，操作方法应该也相似。

三、保障 SNMP 的安全

如果某些设备确实有必要运行 SNMP,则必须保障这些设备的安全。首先要做的是确定哪些设备正在运行 SNMP 服务。除非定期对整个网络进行端口扫描，全面掌握各台机器、设备上运行的服务，否则的话，很有可能遗漏一、二个 SNMP 服务。特别需要注意的是，网络交换机、打印机之类的设备同样也会运行 SNMP 服务。确定 SNMP 服务的运行情况后，再采取下面的措施保障服务安全。

■ 加载 SNMP 服务的补丁

安装 SNMP 服务的补丁，将 SNMP 服务升级到 2.0 或更高的版本。联系设备的制造商，了解有关安全漏洞和升级补丁的情况。

■ 保护 SNMP 通信字符串

一个很重要的保护措施是修改所有默认的通信字符串。根据设备文档的说明，逐一检查、修改各个标准的、非标准的通信字符串，不要遗漏任何一项，必要时可以联系制造商获取详细的说明。

■ 过滤 SNMP

另一个可以采用的保护措施是在网络边界上过滤 SNMP 通信和请求，即在防火墙或边界路由器上，阻塞 SNMP 请求使用的端口。标准的 SNMP 服务使用 161 和 162 端口，厂商私有的实现一般使用 199、391、705 和 1993 端口。禁用这些端口通信后，外部网络访问内部网络的能力就受到了限制；另外，在内部网络的路由器上，应该编写一个 ACL，只允许某个特定的可信任的 SNMP 管理系统操作 SNMP。例如，下面的 ACL 只允许来自（或者走向）SNMP 管理系统的 SNMP 通信，限制网络上的所有其他 SNMP 通信：

```
access-list 100 permit ip host w.x.y any
access-list 100 deny udp any any eq snmp
access-list 100 deny udp any any eq snmptrap
access-list 100 permit ip any any
```

这个 ACL 的第一行定义了可信任管理系统（w.x.y）。利用下面的命令可以将上述 ACL 应用到所有网络接口：

```
interface serial 0
ip access-group 100 in
```

总之，SNMP 的发明代表着网络管理的一大进步，现在它仍是高效管理大型网络的有力工具。然而，SNMP 的早期版本天生缺乏安全性，即使最新的版本同样也存在问题。就象网络上运行的其他服务一样，SNMP 服务的安全性也是不可忽视的。不要盲目地肯定网络上没有运行 SNMP 服务，也许它就躲藏在某个设备上。那些必不可少的网络服务已经有太多让人担忧的安全问题，所以最好关闭 SNMP 之类并非必需的服务——至少尽量设法保障其安全。

简单网络管理协议（SNMP-v2）

一、 概述

简单性是SNMP标准取得成功的主要原因。因为在大型的、多厂商产品构成的复杂网络中,管理协议的明晰是至关重要的，但同时这又是SNMP的缺陷所在——为了使协议简单易行,SNMP简化了不少功能，如：
没有提供成批存取机制，对大块数据进行存取效率很低；

- 没有提供足够的安全机制，安全性很差；
- 只在TCP/IP协议上运行，不支持别的网络协议；
- 没有提供 manager 与 manager 之间通信的机制，只适合集中式管理，而不利于进行分布式管理；
- 只适于监测网络设备,不适于监测网络本身。

针对这些问题,对它的改进工作一直在进行。如 1991 年 11 月,推出了 RMON(RemoteNetworkMonitoring)MIB,加强 SNMP 对网络本身的管理能力。它使得 SNMP 不仅可管理网络设备,还能收集局域网和互联网上的数据流量等信息。

SNMP 如同 TCP/IP 协议簇的其他协议一样,并没有考虑安全问题,因此许多用户和厂商提出了修改初版 SNMP、增加安全模块的要求。于是,IETF 于 1992 年雄心勃勃地开始了 SNMPv2 的开发工作。它宣布计划中的第二版将有以下改进:
· 提供验证、加密和时间同步机制,提高安全性;
· GETBULK 操作提供一次取回大量数据的能力,用更有效的方式传递管理信息;
· 建立一个层次化的管理体系。增加 Manager-to-Manager 之间的信息交换机制,从而支持分布式的管理体系;增加中级(子)管理者(Middle-Level Manager or Sub-Manager),分担主管理者的任务,增加远程站点的局部自主性。

1993 年,SNMP v2 成为提案标准(proposed standard),即 RFC14xx 系列,此时有多个研究小组开始建造 SNMP v2 原型系统的项目。在实施过程中,他们发现 SNMP v2 比人们原先的预想复杂多了,失去了 Simple 的特点。1994 年,当一个问题摆在 IETF 面前,即是否有足够多的支持使 SNMP v2 升级成为草案标准(Draft Standard)时,一场关于 SNMP v2 复杂性的大讨论轰轰烈烈地开始了。讨论的焦点集中在所谓的可管理的模型上面,即实现 SNMP v2 安全模型的数据应该怎样被管理。在这个模型中,引入了"Parties"和"Context"的概念,它们标识了在每个要发送的报文中应该包括的内容。在如何实现这个模型的问题上,出现了两种不同意见,即通常所说的 SNMP v2*和 SNMP usec(SNMP v2u)。双方各持已见,任何一方都没有足够的支持成为下一版标准,当开发计划的结束时间到来时,IETF 只好把几乎所有与安全相关的内容从 SNMP v2 中去掉,从而形成现在看到的最终的 SNMP v2 草案标准,即 RFC 19xx 系列。SNMP v2 中最初没有报文的定义,后来又出现了 SNMP v2C (Community-based SNMP v2)作为 SNMP v2 的补充,它增加了 v2 的报文定义,但与 v1 的报文非常类似。SNMP v2 的开发最终还是失败了,IETF 解散 SNMP v2 工作组,决定把统一 SNMP v2*和 SNMP v2u 的工作留给 SNMPng (next generation)即现在的 SNMP v3 去做

SNM-Pv2 包容了以前对SNMP所做的各项改进工作,并在保持了SNMP清晰性和易于实现的特点以外,功能更强,安全性更好,具体表现为:

- 供了验证机制、加密机制、时间同步机制等，安全性大大提高，
- 提供了一次取回大量数据的能力，效率大大提高；
- 增加了 manager 和 manager 之间的信息交换机制,从而支持分布式管理结构。由中间(intermediate)manager 来分担主 manager 的任务,增加了远地站点的局部自主性。
- 可在多种网络协议上运行,如OSI、Appletalk和IPX等,适用多协议网络环境(但它的缺省网络协议仍是UDP)。

根据Carnegie-Mellin大学(SNMPv2 标准的制定者之一)的StevenWaldbusser测试结果,SNMPv2 的处理能力明显强于SNMPv1,大约是SNMPv1 的 15 倍。

SNMPv2 一共由 12 份协议文本组成(RFC1441-RFC1452),已被作为Internet的推荐标准予以公布。看出它支持分布式管

理。一些站点可以既充当manager又充当agent,同时扮演两个角色。作为agent,它们接受更高一级管理站的请求命令,这些请求命令中一部分与agent本地的数据有关,这时直接应答即可;另一部分则与远地agent上的数据有关。这时agent就以manager的身份向远地agent请求数据,再将应答传给更高一级的管理站。在后一种情况下,它们起的是proxy(代理)的作用。

二、SNMPv2 标准中的安全机制

SNMPv2 对SNMPv1 的一个大的改进,就是增强了安全机制。对管理系统安全的威胁主要有下面几种:

(1)信息篡改(modification)

SNMPv2 标准中,允许管理站(manager)修改agent上的一些被管理对象的值。破坏者可能会将传输中的报文加以改变,改成非法值,进行破坏。因此,协议应该能够验证收到的报文是否在传输过程中被修改过。

(2)冒充(masquerade)

SNMPv2 标准中虽然有访问控制能力,但这主要是从报文的发送者来判断的。那些没有访问权的用户可能会冒充别的合法用户进行破坏活动。因此,协议应该能够验证报文发送者的真实性,判断是否有人冒充。

(3)报文流的改变(messagestreammodification)

由于SNMPv2 标准是基于无连接传输服务的,报文的延迟、重发以及报文流顺序的改变都是可能发生的。某些破坏者可能会故意将报文延迟、重发,或改变报文流的顺序,以达到破坏的目的。因此,协议应该能够防止报文的传输时间过长,以给破坏者留下机会。

(4)报文内容的窃取(disclosure)

破坏者可能会截获传输中的报文,窃取它的内容。特别在创建新的SNMPv2Party时,必须保证它的内容不被窃取,因为以后关于这个Party的所有操作都依赖于它。因此,协议应该能够对报文的内容进行加密,保证它不被窃听者获取。

针对上述安全性问题,SNMPv2 中增加了验证(Authentication)机制、加密(Privacy)机制,以及时间同步机制来保证通信的安全

三、SNMPv2 Party

SNMPv2 标准中增加了一种叫做Party的实体。Party是具有网络管理功能的最小实体,它的功能是一个SNMPv2entity(管理实体)所能完成的全部功能的一个子集。每个manager和agent上都分别有多个Par-ty,每个站点上的各个Party彼此是平等的关系,各自完成自己的功能。实际的信息交换都发生在Party与Party之间(在每个发送的报文里,都要指定发送方和接收方的Par-ty)。每个Party都有一个唯一的标识符(partyidentity)、一个验证算法和参数以及一个加密算法和参数。Party的引入增加了系统的灵活性和安全性,可以赋予不同的人员以不同的管理权限。SNMPv2 中有三种安全性机制:验证(authentication)机制、加密(privacy)机制和访问控制(accesscontrol)机制。这些机制都工作在Party一级,而不是manager/agent一级。

四、SNMPv2 协议操作

SNMPv2 标准的核心就是通信协议———它是一个请求/应答式的协议。这个协议提供了在manager与agent、manager与manager之间交换管理信息的直观、基本的方法。

1、 SNMPv2 提供了 3 种访问管理信息的方法

Ø 管理站和代理之间的请求/响应通信

Ø 管理站和管理站之间的请求/响应通信

Ø 代理系统到管理站的非确认通信

2、 SNMPv2 报文结构和交换序列

SNMPv2 报文的结构分为 3 部分：版本号、团体名和作为数据传送的 PDU。SNMPv2 版本号为 1 SNMPv1 版本号为 0

Ø SNMPv2 发送序列：

n 根据协议需要构造 PDU

n 把 PDU、源和目标端口地址以及团体名传送给认证服务，认证服务产生认证码或对象数 据进行加密。

n 加入版本号、团体名构造报文。

n 进行 BER 编码，产生 0/1 比特流，发送出去

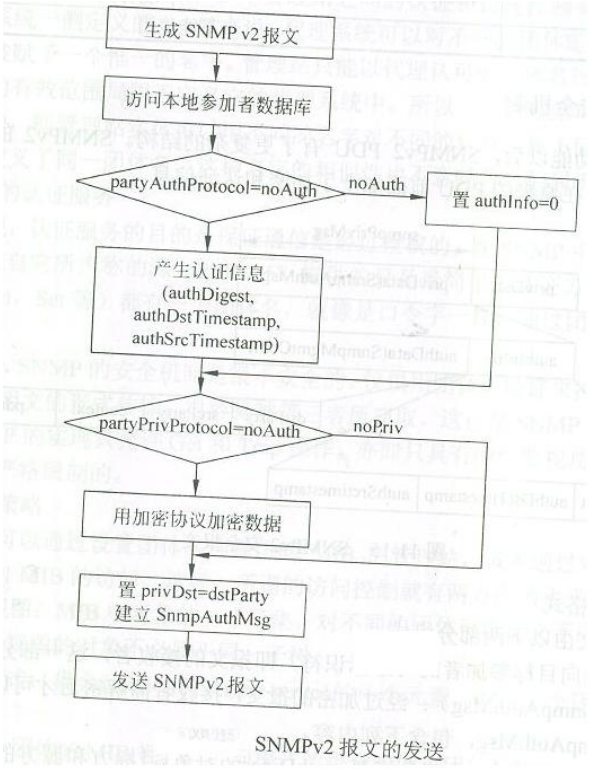
Ø 接收序列

n 对报文进行语法检查，丢弃出错报文

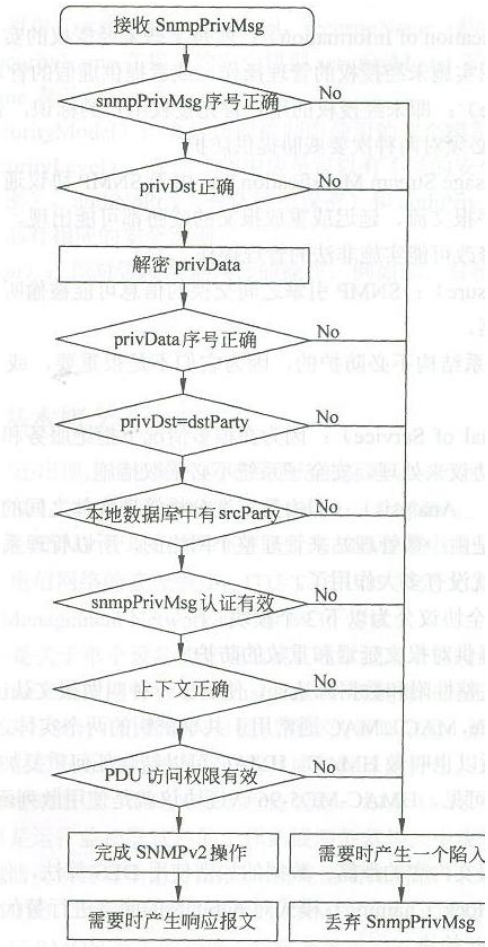
n 把 PDU 部分、源和目标端口教给认证服务。如果失效，发送一个陷入，丢弃报文。

n 认证通过，把 PDU 转换成 asn.1 的形式

n 协议实体对 PDU 作句法检查，如果通过，根据团体名和适当的访问策略作相应的处理



SNMPv2 报文的发送



SNMPv2 安全报文的接收

每条SNMPv2 的报文都由一些域构成:如果发送方、接收方的两个Party都采用了验证(authentication)机制,它就包含与验证有关的信息;否则它为空(取NULL)。

验证的过程如下:发送方和接收方的 Party 都分别有一个验证用的密钥(secretkey)和一个验证用的算法。报文发送前,发送方先将密钥值填入图中 digest 域,作为报文的前缀。然后根据验证算法,对报文中 digest 域以后(包括 digest 域)的报文数据进行计算,计算出一个摘要值(digest),再用摘要值取代密钥,填入报文中的 digest 域。接收方收到报文后,先将报文中的摘要值取出来,暂存在一个位置,然后用发送方的密钥放入报文中的 digest。将这两个摘要值进行比较,如果一样,就证明发送方确实是 srcParty 域中所指明的那个 Party,报文是合法的;如果不一样,接收方断定发送方非法。验证机制可以防止非法用户"冒充"某个合法 Party 来进行破坏。authInfo 域中还包含两个时间戳(timestamp),用于发送方与接收方之间的同步,以防止报文被截获和重发。

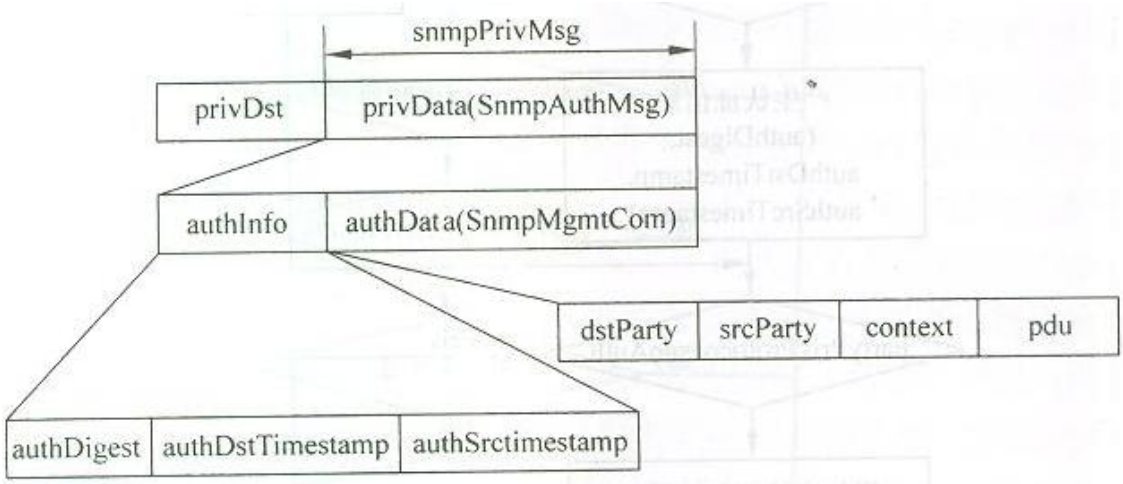


图 11-15　SNMPv2 安全报文

SNMPv2 的另一大改进是可以对通信报文进行加密,以防止监听者窃取报文内容。除了privDst域外,报文的其余部分可以被加密。发送方与接收方采用同样的加密算法(如DES)。
通信报文可以不加任何安全保护,或只进行验证,也可以二者都进行。

简单网络管理协议（SNMP-v3）

1、SNMP v3 现状

尽管 SNMP v2 的开发结束了,但人们对安全的需求仍然存在。1997 年 4 月,IETF 成立了 SNMP v3 工作组,决心完成 v2 未完成的事业。v3 将统一 v2*和 v2u 中的概念和技术思想,并不考虑增加新的功能,而是回到 SNMP v1 Simple 的老路上,他们的目标是:

- 尽量利用现有的成果,尤其是 v2*和 v2u;
- 达到 SET 安全标准的要求;
- 尽可能简单;
- 支持大规模的网络;
- 定义一个可以长久使用的框架;
- 尽量使之沿着标准化的大道前进。

SNMP v3 工作组的工作重点是安全、可管理的体系结构和远程配置。他们计划于 1998 年 4 月提交所有的说明书给 IESG 以成为提案标准(proposed standard)。

与前两种版本相比， SNMPV3 中增加了安全管理方式及远程控制。 SNMPV3 结构引入了基于用户的安全模型用于保证消息安全及基于视图的访问控制模型用于访问控制（USM）。这种安全管理方式支持不同安全性，访问控制及消息处理等模式的并发使用，其具体说明如下：

- 安全性
- 认证和隐私
- 授权和访问控制
- 管理框架
- 实体命名
- 人员和政策
- 用户名及密钥管理
- 通知目标文件
- 代理关系
- SNMP 中的远程配置

SNMPV3 使用 SNMP SET 命令配置 MIB 对象，使之能动态配置 SNMP 代理。这种动态配置方式支持本地或远程地配置实体的添加、删除及修改。

SNMPv3 信息格式：

<table>
<tr><td colspan="6">Msg Processed by MPM (Msg Processing Model)</td></tr>
<tr><td>Version</td><td>ID</td><td>Msg Size</td><td>Msg Flag</td><td colspan="2">Security Model</td></tr>
<tr><td colspan="6">Msg Processed by USM (User Security Module)</td></tr>
<tr><td>Authoritative Engin ID</td><td>Authoritative Boots</td><td>Authoritative Engine Time</td><td>User name</td><td>Authentication parameters</td><td>Privacy Parameter</td></tr>
<tr><td colspan="6">Scoped PDU</td></tr>
<tr><td>Context engine ID</td><td>Context name</td><td colspan="4">PDU</td></tr>
</table>

- Version：SNMPv3（3）。
- ID：用作两个 SNMP 实体间的唯一标识，以调整请求和响应信息。
- Msg Size：信息发送端所支持的八位信息最大值
- Msg Flags：八位的串，包含三个最不重要的标记位：ReportableFlag、PrivFlag、AuthFlag。
- Security Model：标识发送端使用的安全模式，接收端使用该安全模式处理该信息。
- AuthoritativeEngineID：SNMP 的 SnmpEngineID 值包括信息交换。因此，该值涉及 Trap 资源、响应或报告，通过 Get、GetNext、GetBulk、Set 或 Inform 发送至目的地。
- AuthoritativeEngineBoots：SNMP 的 snmpEngineBoots 值包括信息交换。
- AuthoritativeEngineTime：SNMP 的 SnmpEngineTime 值包括信息交换。
- User Name：发生信息交换的用户。
- AuthenticationParameters：如果交换没有被认证，则为空。否则它就是一个认证参数。
- PrivacyParameters：不允许私有交换，则为空。否则它就是一个私有参数。
- PDU（Protocol Data Unit）：SNMPv3 中的 PDU 类型与 SNMPv2 中的相同。

2、SNMP v3 的框架结构

RFC 2271 定义的 SNMPv3 体系结构，体现了模块化的设计思想，可以简单地实现功能的增加和修改。其特点：
* 适应性强：适用于多种操作环境，既可以管理最简单的网络，实现基本的管理功能，又能够提供强大的网络管理功能，满足复杂网络的管理需求。
* 扩充性好：可以根据需要增加模块。
* 安全性好：具有多种安全处理模块。

SNMPv3 主要有三个模块：信息处理和控制模块、本地处理模块和用户安全模块。

信息处理和控制模块

信息处理和控制模块（Message Processing And Control Model）在 RFC 2272 中定义，它负责信息的产生和分析，并判断信息在传输过程中是否要经过代理服务器等。在信息产生过程中，该模块接收来自调度器（Dispatcher）的 PDU，然后由用户安全模块在信息头中加入安全参数。在分析接收的信息时，先由用户安全模块处理信息头中的安全参数，然后将解包后的 PDU 送给调度器处理。

本地处理模块

本地处理模块（Local Processing Model）的功能主要是进行访问控制，处理打包的数据和中断。访问控制是指通过设置代理的有关信息使不同的管理站的管理进程在访问代理时具有不同的权限，它在 PDU 这一级完成。常用的控制策略有

两种：限定管理站可以向代理发出的命令或确定管理站可以访问代理的 MIB 的具体部分。访问控制的策略必须预先设定。SNMPv3 通过使用带有不同参数的原语使用来灵活地确定访问控制方式。

用户安全模块

与 SNMPv1 和 SNMPv2 相比，SNMPv3 增加了三个新的安全机制：身份验证，加密和访问控制。其中，本地处理模块完成访问控制功能，而用户安全模块（User Security Model）则提供身份验证和数据保密服务。身份验证是指代理（管理站）接到信息时首先必须确认信息是否来自有权的管理站（代理）并且信息在传输过程中未被改变的过程。实现这个功能要求管理站和代理必须共享同一密钥。管理站使用密钥计算验证码（它是信息的函数），然后将其加入信息中，而代理则使用同一密钥从接收的信息中提取出验证码，从而得到信息。加密的过程与身份验证类似，也需要管理站和代理共享同一密钥来实现信息的加密和解密。

SNMPv3 使用私钥（privKey）和验证密钥（authKey）来实现这两种功能。

身份验证：RFC2104 中定义了 HMAC，这是一种使用安全哈希函数和密钥来产生信息验证码的有效工具，在互联网中得到了广泛的应用。SNMP 使用的 HMAC 可以分为两种：HMAC-MD5-96 和 HMAC-SHA-96。前者的哈希函数是 MD5，使用 128 位 authKey 作为输入。后者的哈希函数是 SHA-1，使用 160 位 authKey 作为输入。

加密：采用数据加密标准（DES）的密码组链接（CBC）码，使用 128 位的 privKey 作为输入。

3.SNMP v3 与安全管理

SNMP v3 相对于 v2(RFC 19xx 系列)主要增加了安全特性。在网络管理系统中,常见的安全威胁有如下几种类型:

- 修改信息(Modification of Information):某些非授权的 SNMP 实体可以对传输过程中的由合法的 SNMP 实体产生的报文进行修改,用这样的方法来进行非授权的管理操作(如修改某个对象的值),因此,协议应该能够验证收到的报文是否在传输过程中被修改过。
- 伪装(Masquerade):没有授权的用户可能冒充别的合法用户的身份识别(identity)来取得授权,因此,协议应该能够验证报文发送者的真实性。
- 报文流的改变(Message Stream Modification):由于 SNMP 是基于无连接的 UDP 之上的,报文的延迟、重发以及顺序的改变都是可能的。某些破坏者可能会故意将报文延迟,重发以及改变报文流的顺序以达到破坏目的。
- 泄密(Disclosure):破坏者可能会截获传输中的报文,窃取其中的保密内容。

要对付以上的安全威胁,实现安全的管理,通常经由以下两个阶段:

· 传送/接收报文的过程

· 在处理报文内容的过程

这两个阶段分别对应于报文处理和 PDU 处理模块,因此在 SNMP v3 中的安全是指在报文级别实现的安全,而访问控制则对应于在协议操作级别实现的安全。由两者共同实现安全的管理框架

RFC 2574 定义了 USM，USM 负责鉴别、加密、解密 SNMP 报文。

USM 利用多用户的概念，要求每个用户均提供密钥进行身份验证、信息加密，最终使得 SNMPv3 可以解决如上四种典型安全问题。它指定使用 HMAC-MD5 和 HMAC-SHA 进行身份

验证，指定使用 CBC-DES 进行信息加密。在提交 RFC 2574(USM)时，这三种安全协议被认为是(可接受的)安全的。同时，这个模型允许将来需要时使用新的验证、加密协议。

利用 USM 的密钥管理，用户的口令可以转化为针对单个 SNMP 实体的唯一密钥，这样如果该密钥被泄露或盗取，只有与之相配的单个设备才有被侵入的风险。USM 使用的是 MD5 算法，SHA 或其他散列算法也适用于 SNMPv3。作为一种预防措施，口令不通过线路传送，PDU 使用该密钥衍生出的两个密钥被散列计算两次。然后，前面的 12 个字节被用作消息验证代码（MAC），并被添加到信息中。同样的操作过程会在对端反向发生一次。这种复杂的密钥管理很快将被更为简便的 Diffie-Hillman 密钥交换方法取代。

RFC 2575 定义了 VACM，VACM 负责管理 MIB 数据访问权限。VACM 引入的概念相当复杂、混乱。SNMPv1 和 SNMPv2c 采用 communitystring 来划分 MIB 范围、确定访问权限等等。而 VACM 允许更加严谨的动态的访问控制模型，易于管理员配置。

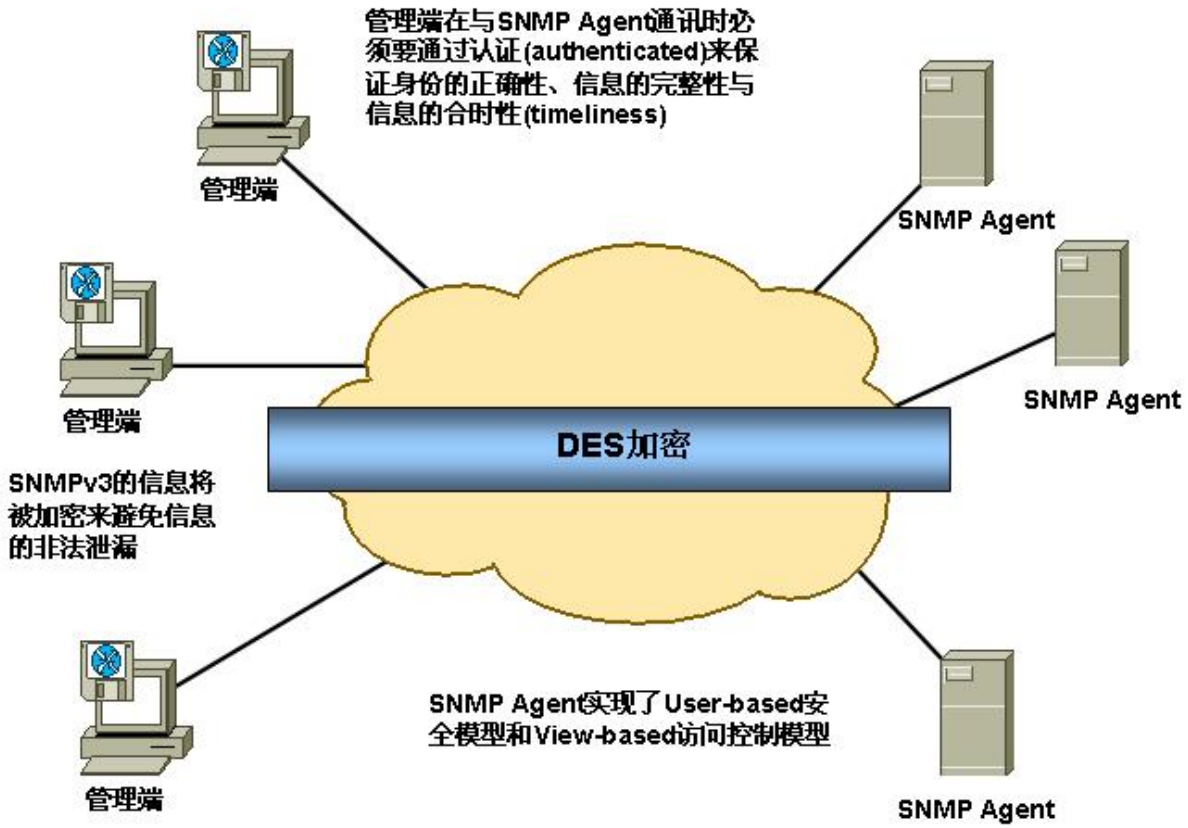
配置每个 VACM 表时应该特别小心。一点微小的错误配置可能导致一个巨大的安全漏洞，比如潜在允许对敏感数据进行非法访问。应该先在一个测试用网络环境中测试你的配置，确认无误后再应用到实际网络环境中去。

SNMPv3 规定了三个安全级别（验证和隐私层次）。第一层是无隐私，即“noAuthnoPriv”。该层类似 SNMPv1 和 v2 的明文共用字符串，适用于调试，或当 SNMP 网络实体处于一个可信赖的环境中时使用。第二层是无隐私验证，即“authNoPriv”。许多管理厂商都认为其客户会在首次实施 SNMPv3 时选择这种比较简单的安全层次。第三层是“authPriv”，

它不仅要进行验证，而且要对 SNMP 数据进行加密，但许多厂商和企业都认为这一层的过程会消耗太多的网络设备资源。

SNMPv3 框架确保了安全子系统和访问控制子系统的模块化，虽然目前 USM 与 VACM 分别被用做安全模块以及访问控制模块，但你可以实现自己的安全模块以及访问控制模块。

将来 IETF 可能会更新这些模块。无论如何，SNMPv3 框架确保新旧模块之间可以平滑过渡。



SNMPv3的安全性

4、结束语

SNMPv3 保持了 SNMPv1 和 SNMPv2 易于理解和实现的特性，同时还增强了网络管理的安全性能，提供了前两个版本欠缺的保密、验证和访问控制等安全管理特性。SNMPv3 正在逐渐扩充和发展，新的管理信息库还在不断增加，能够支持更多的网络应用。所以，它是建立网络管理系统的有力工具，也将推动互联网不断发展。

RMON

简介

为支持新的分布式结构，更高性能的应用和更多的用户而逐步发展的网络对网络管理解决方案的有效性产生巨大的影响，它还要求网络标准必须与联网技术的发展保持同步。目前有一种有效的低成本的网络管理解决方案正得到广泛的接受，那就是远程监控(RMON)标准。RMON（Remote Network Monitoring，远程网络监控）为网络管理员从一个中心点监视、分析、检修一组分布式局域网（LAN）及互连的T-1/E-1 和T-2/E-3 线提供了标准的信息。RMON特别定义了任何网络监控系统必须能够提供的信息。它作为简单网络管理协议（SNMP）的一个扩展，是请求评注RFC1757 中管理信息库（MIB）的一部分。最新的级别是RMON版本 2（有时写作“RMON 2”或“RMON2”）。

为何要RMON?

SNMP(简单网络管理协议)是一种广为执行的网络协议，它使用嵌入到网络设施中的代理软件来收集网络通信信息和

有关网络设备的统计数据。代理不断地收集统计数据，如所收到的字节数，并把这些数据记录到一个管理信息库(MIB)中。网管员通过向代理的MIB发出查询信号可以得到这些信息，这个过程叫轮询(polling)。

虽然MIB计数器将统计数据的总和记录下来了，但它无法对日常通信量进行历史分析。为了能全面地查看一天的通信流量和变化率，管理人员必须不断地轮询SNMP代理，一天中每分钟就轮询一次。这样，网管员可以使用SNMP来评价网络的运行状况，并揭示出通信的趋势，如哪一个网段接近通信负载的最大能力或不必要地正使通信出错。先进的SNMP网管站甚至可以进行编程来自动关闭端口或采取其它矫正措施来处理历史的网络数据。 RMON MIB也可以用于记录网络性能数据和故障历史，可以在任何时候访问故障历史数据以有利于进行有效的故障诊断。使用这种方法减少了管理者同代理间的通信流量，使简单而有力地管理大型互联网络成为可能。

RMON收集九种信息，包括发送的包、发送的字节、丢失的包、主机的数据、两个地址集合间的会话、以及发生的特定类型的事件等。网络管理员可以查出每个用户施加于网络多大的带宽或通信量，还有哪些网址被访问了。可以设置警钟来警惕迫近问题。

然而SNMP轮询有两个明显的弱点：

它没有伸缩性。在大型的网络中，轮询会产生巨大的网络管理通信量，因而导致通信拥挤情况的发生。

它将收集数据的负担加在网络管理控制台上。管理站也许能轻松地收集 8 个网段的信息，当它们监控 48 个网段时，恐怕就应付不下来。RMON标准可以对数据网进行防范管理，它使SNMP更有效、更积极主动地监测远程设备，网络管理员可以更快地跟踪网络、网段或设备出现的故障，然后采取防范措施，防止网络资源的失效。RMON MIB的实现可以记录某些网络事件，即使在网络管理站没有与监控设备主动进行联接（脱机）的情况下，也同样可以完成记录。

RMON 的目标

一、远程网络监视的目标：

RMON 定义了远程监视的管理信息库，以及 SNMP 管理站和远程监 视器之间的接口，一般 RMON 的目标只是监视子网范围内的通信，从而减少管理站和被管 理站系统间的通信负担。具体 RMON 具有下列目标：

1. 离线操作：必要时管理站可以停止对监视器的轮询，从而减少通信提高带宽利用率。 即使不受管理站查询，监视器也能不断收集子网故障、性能和配置方面信息，统计和积 累数据，以便管理站查询时及时提供管理信息。另外，在网络出现异常时间使其能及时 向管理站报告。
2. 主动监视：如监视器有足够资源，通信负载允许，监视器可以连续地或周期的运行诊 断程序，获得并记录网络性能参数。
3. 问题检测和报告：监视器也可被动地获得网络数据，并在出现异常时向管理站报告。
4. 提供增值数据：监视器可以分析收集到的子网数据。
5. 多管理站操作：一个网络可以由多个管理站，或者分布的实现不同的网络管理功能。

二、 表管理操作原理：

在 RMON 规范中增加了两种新的数据类型：

1. OwnerString ：：=DisplayString
2. EntryStatus ：：=INTRGER{valid(1)，createRequest(2)，underCreation(3)，invalid(4)}

在每一个可读写的 RMON 表中都有一个对象，其类型为 OwnerString，气滞为标行所有人或创建者；

RMON 表中还一对象，类型为 EntryStatue，其值表示行的状态，对象名义 Statue 结尾。

RMON 规范中的表结构由表控制和数据表两部分组成，控制表定义数据表的结构，数据表

用于存储数据。控制表包含：rmlControlIndex、rmlControlParameter、 rmlControlOwner, rmlControlStatue。数据表由 rmlDataControlIndex 和 rmlDataIndex 共同索引。

增加行：管理占用 Set 命令在 RMON 表中增加行，并遵循下列规则：

3. 管理站用 SetRequest 生成一个新行，如果新行的索引值不冲突，则代理产生一个新行 ，其状态值为 creatRequest(2)；
4. 新行产生后，由代理把状态对象值置为 underCreation(3)。对与管理站没有设置新值 得列对象，代理可以置为默

认值，或者让新行维持这种不完整、不一致的状态。

5. 新行的状态值保持为 underCreation(3)，直到管理站产生了所要生成的新行。这时由 管理站置每一信行状态的值为 valid(1)

6. 如果管理站要生成的新行已经存在，则返回一个错误值。

删除行：只有行的所有者才能发出 SetRequest PDU，把行状态值置为 invalid(4)。

修改行：首先置行状态对象的值为 invalid(4)，然后用 SetRequest PDU 改变行中其它对 象的值。

三、 多管理站访问中出现的问题及解决办法：

RMON 监视器允许多个管理站并发的访问，当多个管理站访问时可能出现下列问题：

Ø 多个管理站对资源的并发访问可能超过监视器的能力；

Ø 一个管理站可能长时间占用监视器资源，使得其它站得不到访问；

Ø 占用监视器资源的管理站可能出现崩溃，而没有释放资源。RMON 控制表中列对象 Owner 规定了表的所属关系；

Ø 管理站能认得自己所属的资源，也知道自己不再需要的资源；

Ø 网络操作员可以直到管理站占有的资源，并决定是否释放这些资源；

Ø 一个被授权的网络操作员可以单方面决定是否释放其它操作员的资源；

Ø 如果管理站重新启动它应该是方不再使用的资源。

RMONMIB

Internet工程特别小组(IETF)于 1991 年 11 月公布RMONMIB来解决SNMP在日益扩大的分布式网络中所面临的局限性。RMONMIB的目的在于使SNMP更为有效更为积极主动地监控远程设备。

RMON监视器可用两种方法收集数据：一种是通过专用的RMON探测仪（Probe），网管站直接从探测仪获取管理信息并控制网络资源，这种方式可以获取RMON MIB的全部信息；另一种方法是将RMON代理直接植入网络设备（路由器、交换机、Hub等）使它们成为带RMON Probe功能的网络设施，网管站用SNMP的基本命令与其交换数据信息，收集网络管理信息，但这种方式受设备资源限制，一般不能获取RMON MIB的所有数据，大多数只收集四个组的信息。

RMON可以用硬件监视设备（称作“探测器”）或通过软件或一些组合来支持。例如，思科的LAN交换机就包括了当通信量流过时可以中断信息并将其记入它的MIB中的软件。软件代理能够用图形用户接口收集信息并传给网络管理员。许多商家都提供带不同种类RMON支持的产品。

RMONMIB由一组统计数据、分析数据和诊断数据构成，利用许多供应商生产的标准工具都可以显示出这些数据，因而它具有独立于供应商的远程网络分析功能。RMON探测器和RMON客户机软件结合在一起在网络环境中实施RMON。RMON的监控功能是否有效，关键在于其探测器要具有存储统计数据历史的能力，这样就不需要不停地轮询才能生成一个有关网络运行状况趋势的视图。“RMONMIB功能组”功能框可以对通过RMOMMIB收集的网络管理信息类型进行描述。

遍布在LAN网段之中的RMON探测器不会干扰网络。它能自动地工作，无论何时出现意外的网络事件，它都能上报。探测器的过滤功能使它根据用户定义的参数来捕获特定类型的数据。当一个探测器发现一个网段处于一种不正常状态时，它会主动与在中心的网络管理控制台的RMON客户应用程序联系，并将描述不正常状况的捕获信息转发。客户应用程序对RMON数据从结构上进行分析来诊断问题之所在。对于 3Com公司产品，TranscendManagement控制台执行RMON客户应用程序。

通过追踪谁与谁交谈，RMON可以帮助网管员确定如何最佳给他们的网络分段。网管员通过报告意外事，可以识别出占有最大带宽的用户；这些用户然后放置于各自的网段之中来尽可能减少他们对其它用户的影响。

RMON实现了对异构环境进行一致的远程管理，它为通过端口远程监视网段提供了合适的解决方案。作为IETF定义的管理信息库，RMON是对SNMP标准的扩展，它定义了标准功能以及在基于SNMP管理站和远程监控者之间的接口，主要实现对一个网段乃至整个网络的数据流量的监视功能，目前已成为成功的网络管理标准之一。 RMON MIB的使用意味着首次把网络管理扩展到物理层，使独立地收集设备的数据成为可能，内置的监控工具提供了不占用宝贵网络资源（带宽）而对整个流量进行有限度的分析能力，RMON产品已经可以使用，而且其数量在今后会平稳增长

RMON的一个重要的优点还在于它与现存的SNMP框架相兼容，不需对该协议进行任何修改。

据战略网络咨询公司(SNC)称，网络预算的 67%都花费在日常操作活动上。事实上，这意味着网管员的时间有 3/4 是放在只对网络进行日常操作上面，根本没有时间进行主动管理。

而RMON自主性的操作和分布式的管理体系可以大幅提高网络管理效率，因而节省了金钱和时间。事实上，SNC预测RMON可以将一个网络管理小组的效率提高两倍以上，使小组在不增加人员的情况下所支持的用户和网络数量都翻一番，如左图所示。要是网络预算的效率也能像这些个人生产率一样可以翻一番的话，那么无疑可以节省大量开支。SNC估算，管理一个桌面机的年平均费用为 1500 美元，RMOM和RMONⅡ标准可以将这一费用减少到每年 600 美元。

RMON MIB

RMON MIB由一组统计数据、分析数据和诊断数据组成，不象标准MIB仅提供被管对象大量的关于端口的原始数据，它提供的是一个网段的统计数据和计算结果。RMON MIB对网段数据的采集和控制通过控制表和数据表完成。RMON MIB的使用意味着首次把网络管理扩展到物理层，使独立地收集设备数据成为可能，内置的监控工具提供了不占用宝贵网络资源（带宽）而对整个流量进行有限度的分析的能力。

RMON MIB 按功能分成九个组。每个组有自己的控制表和数据表。其中，控制表可读写，数据表只读，控制表用于描述数据表所存放数据的格式。配置的时候，由管理站设置数据收集的要求，存入控制表。开始工作后，RMON 监控端根据控制表的配置，把收集到的数据存放到数据表。RMON 在监控元素的 9 个 RMON 组中传递信息，各个组通过提供不同的数据来满足网络监控的需要。每个组都是可选项，所以，销售商不必在 MIB 中支持所有的组。

RMON MIB 包含以下数据：

RMON 1 MIB 组

RMON 1 MIB 组	功能	元素
统计量	包括探测器为该设备每个监控的接口测量的统计值。	数据包丢弃、数据包发送、广播数据包、CRC 错误、大小块、冲突以及计数器的数据包。范围从 64~128、128~256、256~512、512~1024 以及 1024~1518 字节。
历史	定期地收集统计网络值地记录并存储起来以便日后提取。	取样周期、样品数目和项目。提供有关网段流量、错误包、广播包、利用率以及碰撞次数等其他统计信息的历史数据。
告警	定期从探测器的变量选取统计例子。并与前面配的阈值相比较。	告警类型、间隔、阈值上限、阈值下限
主机	包括网络上发现的与每个主机相关的统计值。	主机地址、数据包、接收字节、传输字节、广播传送等。
HostTopN	准备描述主机的表，根据一个统计值排序列表。	统计值、主机、周期的开始和结束、速率基值、持续时间。
矩阵组	记录关于子网上两个主机之间流量的信息，该信息以矩阵形式存储起来。	源地址和目的地址对、数据包、字节和每一对的错误。
过滤器	允许监视器观测与一过滤	字节过滤器类型、过滤器表达式等。

	器相匹配的数据包。	
捕获包	数据包在流过一个信道之后被捕获。	捕获所有通过过滤器的数据包或简单地记下基于这些数据包的统计。
事件	控制在此处事件的产生和报告.	事件类型、描述、事件最后一个发送的时间
令牌环	支持令牌环	不常使用

RMON II 浮出水面

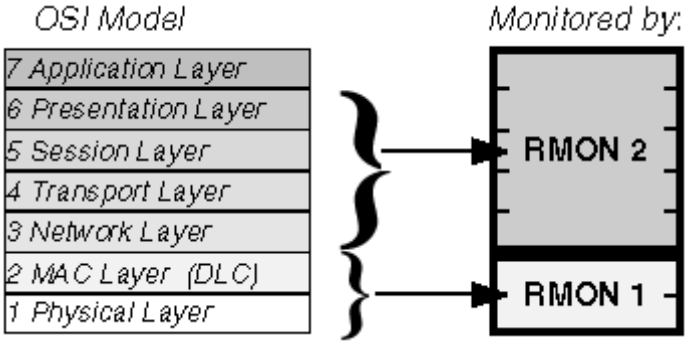
在RMON基础上产生的RMON II标准能将网管员对网络的监控层次提高到网络协议栈的应用层。因而除了能监控网络通信与容量外，RMONⅡ还提供有关各应用所使用的网络带宽量的信息，这也是在客户机/服务器环境中进行故障排除的重要因素。

RMON 在网络中查找物理故障，RMON II 进行的则是更高层次的观察，它监控实际的网络使用模式。RMON 探测器观察的是由一个路由器流向另一个路由器的数据包，而 RNOM II 则深入到内部，它观察的是哪一个服务器发送数据包，哪一个用户预定要接受这一数据包，这一数据包表示何种应用。网管员能够使用这种信息，按照应用带宽和响应时间要求来区分用户，就像过去他们使用网络地址生成工作组一样。

RMON II 没有取代 RMON，而是它的补充技术，是 RMON 的扩展。RMON v2 专注于 MAC 层以上更高的流量层，它主要强调 IP 流量和应用程序层流量。RMON v2 允许网络管理应用程序监控所有网络层的信息包，这与 RMONv1 不同，后者只允许监控 MAC 及其以下层的信息包。

RMON II 在 RMON 标准基础上提供一种新层次的诊断和监控功能。事实上，RMON II 能够监控执行 RMON 标准的设备所发出的意外事件报警信号。

在客户机/服务器网络中，安放妥当的 RMON II 探测器能够观察整个网络中的应用层对话。最好将 RMON II 探测器放在数据中心或工作组交换机或服务器集群中的高性能服务器之中。原因很简单，因为大部分应用层通信都经过这些地方。



RMON 2 MIB 组

RMON 2 MIB 组	功能
协议目录	协议目录是一种简单的便于共同建立 RMON2 应用程序、实现 RMON 代理的途径。这对于应用程序和代理出自不同的提供商的情况尤其重要。
协议分布	将探测器收集的数据转换为正确的协议名，从而可以显示给网络管理者。
地址映像	MAC 层的地址与网络层的地址之间的转换使得读和记忆变得容易。地址转换不仅为网络管理者提供了帮助，而且它支持 SNMP 管理平台并引入了改进的拓扑布局转换。

网络层主机	网络层主机(IP 层)统计值。
网络层矩阵表	在两个地址之间存储并重新获取网络层主机(IP 层)统计值。
应用层主机	应用层主机统计值。
应用层矩阵表	在两个地址之间存储并重新获取应用层主机(IP 层)统计值。
用户历史	这一特性使网络管理者能够配置系统中的任何历史记录，例如在指定文件服务器或路由器对路由器的连接上的特殊历史。
探测器配置	RMON2 的这一特性使某提供商的 RMON 应用程序能够配置其他提供商的 RMON 探测器。

RMON MIB 的使用意味着首次把网络管理扩展到物理层，使独立地收集设备的数据成为可能，内置的监控工具提供了不占用宝贵网络资源（带宽）而对整个流量进行有限度的分析能力，RMON 产品已经可以使用，而且其数量在今后会平稳增长。

目前大部分 RMON Agent 只支持统计、历史、告警、事件四个组，如 Cisco、3COM、华为的路由器或交换机都已实现这些功能，不但支持网管工作站为 Agent 记录的任何计数和整数类对象设置采样间隔和报警阈值，而且允许网管工作站根据需要以表达式形式对多个变量的组合进行设置。

网络管理系统

由于网络管理已经有了一系列的标准，以及 OSI 定义的网络管理五大功能，使得具有配置管理、性能管理、故障管理、安全管理和计费管理五大功能的管理系统成为可能。同时，也正是得益于这样的网络管理系统，我们才能对网络进行充分、完备和有序的管理。但是由于涉及到众多的网络管理协议和五个方面所要求的功能以及不同网络的实际情况，使得网络管理系统在技术上具有很强的挑战性。

一、网管软件的分类

网络管理系统是对以上几个基本要素的组合。我们大致可以将网络管理系统划分为三代。

第一代网管就是最常用的命令行方式，并结合一些简单的网络监测工具，它不仅要求使用者精通网络的原理及概念，还要求使用者了解不同厂商的不同网络设备的配置方法。这种方式的优点是具有很大的灵活性，缺点是风险系数增大，容易引发误操作，而且不具备图形化和直观性,比如网络探测工具 NetXray 可以运行在多种协议之下，包括 TCP/IP，SPX/IPX 等，工作在网络环境的底层，拦截所有正在网络上传输的数据并进行筛选处理，实时分析网络状态和设备布局，但第一代网管工具只能统计和分析网络的数据，并不能监控设备的状态，因此需要配合一系列 CLI 命令直接在设备上查看系统和端口信息。

第二代网管有着良好的图形化界面，用户无须过多了解设备的配置方法，就能图形化地对多台设备同时进行配置和监控，大大提高了工作效率，但仍然存在由于人为因素造成的设备功能使用不全面或不正确的问题，比如 CiscoView 是一个基于 GUI 的设备管理软件应用程序，可以图形的方式显示 Cisco 的物理视图。另外，它还提供配置和监视功能以及基本的故障排除功能。借助 CiscoView 可以更容易地理解设备提供的大量管理数据，网络管理员无需对远程站点上的每台设备进行物理检测就能够全面查看 Cisco 产品。

第三代网管相对来说比较智能，是真正将网络和管理进行有机结合的软件系统，具有“自动配置”和“自动调整”功能，对网管人员来说，只要把用户情况、设备情况以及用户与网络资源之间的分配关系输入网管系统，系统就能自动地建立图形化的人员与网络的配置关系，并自动鉴别用户身份，分配用户所需的资源(如电子邮件、Web、文档服务等)，同时，整个企业的网络安全得以保证；因此第三代网管系统是企业级的管理平台，由多个软件包构成，涉及到 OSI 全

部七层协议集。目前第三代系统可选的范围比较广，例如 CA Unicenter TNG、CiscoWorks2000、HP OpenView、IBM Tivoli、APRISMA Spectrum 等。这些网管软件通常包括一系列的子系统，有些子系统具有第二代系统的功能，如 CiscoWorks 中的 CiscoView。有些系统集成了其他系统的一些子系统以增强功能。

虽然网管系统发展到了第三代，但并不等于前二代系统已经淘汰，如何选择在于用户具体的网络管理需求，这三代系统分别适应不同的网络规模和网络应用，系统结构越是趋同，所需要的网管系统就越简单。而复杂的异构环境则需要完全成熟的企业管理软件。

国内网管软件近几年也取得一定的发展，但总体来说较大型的成熟的软件不多，国产软件的优势在于本地化，用户对界面的可操作感强，但大部分软件只相当于国外第三代网管系统中的某个子系统功能，网络的监控功能比较强，缺乏自动解决问题和管理用户资源的能力，而且软件更新和售后服务连贯性不强。总体来说，目前国内网管软件比较适用于中等规模企业或作为大型网管系统的辅助工具。

选择一款合适的网管软件

用户在选购网管软件时，必须结合具体的网络条件，网管软件用于辅助日常网络管理，提高管理效率，所以选择的软件应该体现有效管理原则。目前市场销售的网络管理软件可以按功能划分为：网元管理（主机系统和网络设备）、网络层管理（网络协议的使用、LAN 和 WAN 技术的应用以及数据链路的选择）、应用层管理（应用软件）三个层次，其中最基础的是网元管理，最上层的是应用层管理。

二、网管软件介绍

现在市场上号称是网络管理系统的软件不少，但真正具有网络管理五大功能的网络管理系统却不多。我们下面将介绍四种网络管理系统，并给出它们的优缺点比较。这四种网络管理系统是：惠普(HP)公司的 0pen-View，国际商用公司(IBM)的 NetView，SUN 公司的 SunNet 以及近年来代表未来智能网络管理方向的 Cabletron 公司的 SPECTRUM。

一、 HP 的 0penView

HP 的 OpenView 有争议地成为了第一个真正兼容的、跨平台的网络管理系统，因此也得到了广泛的市场应用。但是，虽然 0penView 被认为是一个企业级的网络管理系统，但它跟大多数别的网络管理系统一样，不能提供 NetWare，SNA，DECnet，x．25，无线通信交换机以及其他非 SNMP 设备的管理功能。另一方面，HP 努力使 OpenView 由最初的提供给第三方应用厂商的开发系统，转变为一个跨平台的最终用户产品。它的最大特点是被第三方应用开发厂商所广泛接受。比如 IBM 就把 OpenView 增强功能并扩展成为自己的 NetView 产品系列，从而与 OpenView 展开竞争。特别在最近几年，OpenView 已经成为网络管理市场的领导者，与其他网络管理系统相比，OPenView 拥有更多的第三方应用开发厂商。在近期，OpenView 看上去更像一个工业标准的网络管理系统。

1、网络监管特性

()penView 不能处理因为某一网络对象故障而误导致的其他对象的故障。具体说来就是，它不具备理解所有网络对象在网络中相互关系的能力，因此一旦这些网络对象中的一个发生故障，导致其他正常的网络对象停止响应网络管理系统，它会把这些正常网络对象当作故障对象对待。同时，OpenView 也不能把服务的故障与设备的故障区分开来，比如是服务器上的进程出了问题还是该服务器出了问题，它不能区分。这些是 OpenView 的最大弱点。

另外，在 OpenView 中，性能的轮询与状态的轮询是截然分开的，这样导致一个网络对象响应性能轮询失败但不触发一个报警，仅仅只有当该对象不响应状态的轮询才进行故障报警。这将导致故障响应时间的延长，当然两种轮询的分开将带来灵活性上的好处，第三方的开发商可以对不同轮询的事件分别处理。

OpenView 还使用了商业化的关系数据库，这使得利用 OpenView 采集来的数据开发扩展应用变得相对容易。但第三方应用开发厂商需要自己找地方存放自己的数据，这又限制了这些数据的共享。

2．管理特性

OpenView 的 MIB 变量浏览器相对而言是最完善的，而且正常情况下使用该 MIB 变量浏览器只会产生很少的流量开销。但 OpenView 仍然需要更多、更简洁的故障工具以对付各种各样的故障与问题。

3．可用性

OpenView 的用户界面显得干净以及相对的灵活，但在功能引导上显得笨拙。同时 OpenView 还在简单、易用的 Motif 的图形用户界面上提供状态信息和网络拓扑结构图形，虽然这些信息和图形在大多数网络管理系统中都提供。但是一

个问题是 OpenVjew 的所有操作(至少现在)都在 X-W1ndows 界面上进行，它还缺乏一些其他的手段，比如 WWW 界面和字符界面，同时它还缺乏开发基于其他界面应用的 API。

4. 总结

OpenV5ew 是一个昂贵的，但相对够用的网络管理系统，它提供了基本层次上的功能需求。它的最大优势在于它被第三方开发厂商所广泛接受。但得到了 NetView 许可证的 IBM 已经加强并扩展了 OpenView 的功能，以此形成了 IBM 自己的 NetView／6000 产品系列，该产品可以在很大程度上视为 OpenView 的一种替代选择。

二、 IBM 的 NetView

IBM 的 NetView 是一个相对比较新，同时又具有兼容性的网络管理系统。NetView 既可以作为一个跨平台的、即插即用的系统提供给最终用户，也可以作为一个开发平台，在上面开发新的网络管理应用。IBM 从 HP 得到 OpenView3．1 的许可证，并在此基础上大大扩展了它的功能，并将与其他软件产品集成起来，从而形成了自己的 NetV5ew 产品系列。跟 OpenView 一样，NetView 作为企业级的网络管理系统，但它也不能提供 Net-Ware，SNA，DECnet，X．25，无线通信交换机以及其他非 SNMF 设备的管理功能。在网络管理产品市场上，NetView 在过去几年得到广泛的关注。NetView 的市场人员宣称尽管 IBM 是从 HP 那里得到了 OpenView 的最初许可证，但 IBM 在此基础上自己增加了 70％的代码，并修正了很多 OpenView 的 bugs,因此 NewView 应该被认为是一种新的产品。NetView 产品系列包括一个故障卡片系统，一些新的故障诊断工具，以及一些 OpenView 所不具备的其他特性。虽然目前 NewView 在吸引第三方应用开发厂商方面还不如 open-View，但这种差距正在缩小。

1．网络监管特性

NetView 不能对故障事件进行归并，它不能找出相关故障卡片的内在关系，因此对一个失效设备，即使是一个重要的路由器，将导致大量的故障卡片和一系列类似的告警，这是难以接受的。更糟的是，第三方开发的应用似乎也不能确定这样的从属关系，比如一个针对 CISCO 产品的插件不能区分线路故障和 CSU／DSU 故障。因此，NetView 不具备在掌握整个网络结构情况下管理分散对象的能力。在一个大型、异构网络中，这意味着服务的开销不能轻易地从网络开销中区分出来。

同样的，在 NetView 中，性能轮询与状态轮询也是彻底分开的，这也将导致故障响应的延迟。但对第三方而言，NetView 提供了一些某种程度上的灵活性，在系统告警和事件中允许调用用户自定义的程序。NetView 也使用了商业化的关系数据库，这使得利用 NetView 采集来的数据开发扩展应用变得相对容易。但第三方应用开发厂商需要自己找地方存放自己的数据，这又限制了这些数据的共享。

IBM 在 OS／2 Intel 平台上利用 proxy 代理可以管理内部设备，并通过 SNMP 与 NetView 的管理进程通信。IBM 宣称 NetView 的管理进程具备理解并展示 Novell 的 NetWare 局域网的能力。

2．管理特性 IBM 极大地简化了 NetView 的安装过程，使得安装 NetView 比安装 OpenView 简单许多，它也是大多数网络管理软件中最容易安装的。

3．可用性

NetView 用户界面显得干净和相对的灵活，它比 OpenView 更容易使用。它的 Motif 的图形用户界面也像大多数网络管理软件一样用图形方式显示对象的状态和网络拓扑结构。IBM 还增加了一种事件卡片机制，并在一个单独的窗口中按照一定的索引显示最近发生的事件。但同样一个问题是 NetView 的所有操作(至少现在)都在 X-Windows 界面上进行，它还缺乏一些其他的手段，比如 WWW 界面和字符界面，同时它也缺乏开发基于其他界面应用的 API。

4．小结

IBM 在 HP 的 OpenView 上进行了很多改进，在他们的 NetView 产品系列中提供了更全面的网络管理功能。同时 NetView 还以更便宜的价格、更多的性能和更强的灵活性提供给用户，但它仍然存在着一些令人烦恼的限制。缺乏相关。性的处理使 NetView 对进行自动管理感到困难，不过它针对一些告警还是有某种程度上的过滤与归并机制。

总之，NetView 在 openView 的基础上进行了一系列的改进，我们期待 NetView 的新开发版本能够加入更多的改进，包括处理相关性的能力以及适应不同网络环境的能力等。

三、 SUN 的 SUNNet Manager

SunNet Manager(SNM)是第一个重要的基于 Unix 的网络管理系统。SNM 一直主要作为开发平台而存在，它仅仅提供很有限的应用功能。为了实用化，还必须附加很多第三方开发的针对具体硬件平台的网络管理应用。SNM 的开发似乎已经减慢甚至停止，不过 SUN 已经签署一份许可证给 NetLabs DiMONS 3G 公司，授权该公司以 SNM 为基础开发一个名叫 Encompass 的新网络管理系统。对于 SNM，该系统跟其他大多数网络管理系统一样，它也不能提供 NetWare，SNA，DECnet，X．25，无线通信交换机以及其他非 SNMP 设备的管理功能。SNM 只能运行在 SUN 平台上，它需要 32MB 内存和 400MB 硬盘。

作为广泛使用的最早的网络管理平台，SNM 曾经一度占据了市场的领导地位。但后来 SNM 在市场的地位被 HP 的

OpenView 所取代，现在 SNM 在市场中所占的份额越来越少，不过 SNM 仍然具有很多第三方开发的应用。

1．网络监管特性

SNM 有两个有趣的特性：Proxy 管理代理和集成控制核心。SNM 是第一个提供分布式网络管理的产品，它的数据采集代理可以通过 RPC(远程过程调用)与管理进程通信。这样 Proxy 管理代理就可以像管理进程的子进程一样分布在整个网络；而集成控制核心可以在不同的 SNM 的管理进程之间分享网络状态信息，这种特性在异构网络中显得特别有效。然而，SNM 不支持相关性处理抵消了 Proxy 管理代理的优势，使得 SNM 的 Proxy 管理代理把网络结构并行化的努力得不到有力的支持。

SNM 的 Proxy 管理代理不仅可以在 SUN 平台上，也可以在 HP／UX 以及 AIX 平台上。一个 Proxy 管理代理可以对一个子网进行轮询，以减少单点的故障、使轮询分布化、以及减少网络的流量开销。同时，Proxy 管理代理也能把不可靠的 SNMP traps 转变为可靠的告警，这些 SNMP trap 被送到本地的管理代理，然后送给管理进程。

2．管理特性

集成控制核心允许多个 SNM 共享网络状态信息，这样在一个子网可以拥有一个自己的 SNM 以监控该子网的状态，然后集成控制核心在不同 SNM 之间共享信息，这样即使是异构的复杂网络也能很好地收集和发布网络信息。

新的 SNM 2．2 版本在易安装性、易配置性以及提供缺省配置选项方面有了很大进步，但在这方面，它还赶不上 IBM 的 NetView。

3．可用性

SNM 更多的是作为一个平台而不是一个网络管理产品出现，它提供了一系列的 API 可供第三方厂、商在，其上开发自己的应用，因此如果希望使用针对 SNM 的友好的用户界面，则必须购买第三方提供的软件。在某种意义上说，如果购买了 SNM 而不购买第三方的应用软件，那么 SNM 将没有什么用处。另外，SNM 使用一种嵌入式的文件系统来保存数据，但在某些 SNM 的版本中也可以使用关系数据库系统，不过用户得另行付费。

4．小结

SNM 提供一种集成的网络管理，这是一种介于集中式的网络管理和分散的、非共享的对象管理之间的网络管理方式。集成网络管理特别在管理不同独立部门的网络所组成的统一网络时非常有用，而分布式的轮询机制也在一定程度上补偿了缺乏相关性处理的缺陷。

SNM 是处于开发周期最末端的产品，SUN 公司坚持用一种简洁的、使用 NetIJabs DiMoNS3G 技术的产品来淘汰 SNM。虽然 SNM 是一个广泛使用的，同时被很多第三方厂商支持的软件，但它似乎将不再具有未来的发展前景。

四、 Cabletron 的 SPECTRUM

Cabletron 的 SPECTRUM 是一个可扩展的、智能的网络管理系统，它使用了面向对象的方法和 C1ient／Server 体系结构。SPECTRUM 构筑在一个人工智能的引擎之上，该引擎叫 Inductive Modeling Technology(IMT)，同时 SPECTRUM 借助于面向对象的设计，可以管理多种对象实体；该网络管理系统还提供针对 Novell 的 NetWare 和 Banyan 的 VINES 这些局域网操作系统的网关支持。另外，一些本地的协议支持(比如 AppleTalk，IPX 等)都可以利用外部协议 API 加入到 SPECTRUM 中，当然这样需要进一步的开发。

虽然 SPECTRUM 是一个优秀的网络管理软件，但它却只有很低的市场占有率。同时与前面三种网络管理系统相比，SPECTRUM 只得到少数第三方开发厂商的支持。而缺乏一种第三方厂商的支持，将损害 SPECTRUM 的长期发展前景，虽然它现在拥有很多先进的特性。

1．网络的监视特性

SPECTRUM 是所有四种网络管理软件中唯一具备处理网络对象相关性能力的系统。SPECTRUM 采用的归纳模型可以使它检查不同的网络对象与事件，从而找到其中的共同点，以归纳出同一本质的事件或故障。比如，许多同时发生的故障实际上都可最终归结为一个同一路由器的故障，这种能力减少了故障卡片的数量，也减少了网络的开销。

SPECTRUM 服务器提供两种类型的轮询：自动轮询与手动轮询；在每次自动轮询中，服务器都要检查设备的状态并收集特定的 MIB 变量值。与其他网络管理系统一样，SPECTRUM 也可设定哪些设备需要轮询，哪些 MIB 变量需要采集数据，但不同之处在于，对同一设备对象 SPECTRUM 中没有冗余监听。

SPECTRUM 提供多种形式的告警手段，包括弹出报警窗口、发出报警声响、发报警电子邮件以及自动寻呼等。在一个附加产品中，甚至允许 SPECTRUM 提供一种语音响应支持。

SPECTRUM 的自动拓扑发现非常灵活，但相对比较慢。它提供交互式发现的功能，即用户指定要发现的于网去进行自动发现，或用户可以指定特定的 IP 地址范围、路由器以及设备等。单一网络和异构网络它都支持自动发现。SFECTRUM 使用一种集成的关系数据库系统来保存数据，但它不支持直接对该数据库的 SQL 语言操作。SPECTRUM 的 数据网关提供类似 SAS 的访问接口，用户可以用 SAS 语言来访问数据库，同时它还提供针对其他数据库系统的 SQL 接口。

2．管理特性

在 SPECTRUM 中，管理员可以控制网络操作人员访问系统的界面，以控制系统的使用权限，同时严格控制一个域的操作人员只能控制自己的这一个管理域。但是在管理员的这一层次上只有一级控制，因此一个部门的管理员可以访问其他部门的用户文件。SPECTRUM 的 MIB 浏览器，叫做 attribute walk，非常的复杂与笨拙，甚至要求用户给出 MIB 变量的标识才能查询，当然也存在很出色的第三方 MIB 浏览器。

3．可用性

通过 SPECTRUM 的图形用户界面，用户可以定义自己的操作环境并设置自己的快捷方式。不过在 SPECTRUM 中没有在线帮助。另外，SPECTRUM 提供了 X-Windows 和行命令两种方式来查询和操作数据库中的数据。

4．小结

SPECTRUM 是一个性能强大同时非常灵活的网络管理系统。它被一些用户使用并给予很高的评价。SPECTRUM 还提供；些独特的功能，比如相关性的分析和错误告警的控制等。SPECTRUM 也是四种网络管理系统中最复杂的产品，这种复杂性是它的灵活性带来的，而这种灵活性是必要的。但这种灵活性，或者说是复杂性，限制了 SPECTRUM 的第三方开发厂商的数量。

网络管理和维护

网络管理和维护是一项非常复杂的任务，虽然现在关于网络管理既制订了国际标准，又存在众多网络管理的平台与系统，但要真正做好网络管理的工作不是一件简单的事情。做好这项工作需要广泛的背景知识与大量的实际操作经验，下面我们将介绍网络技术发展下一些新形式的网络管理，以及在长期网络管理实践基础上总结出来的一些网络管理经验。

一、 VLAN 管理

VLAN(虚拟局域网)就是一个计算机网络，其中的计算机好像是被同一网线连接在一起，而实际上它们可能分处于局域网的不同区域。VLAN 更多的是通过软件而非硬件来实现，因此这使得它具有很高的灵活性。VlAN 的一个主要特性就是提供了更多的管理控制，减少了相对日常管理开销，提供了更大的配置灵活性。

VLAN 的这些特性包括：①当用户从一个地点移动到另一个地点时，简化了配置操作和过程修改；②当网络阻塞时，可以重新调节流量分布；②提供流量与广播行为的详细报告，同时统计 VLAN 逻辑区域的规模与组成；④提供根据实际情况在 VLAN 中增加和减少用户的灵活性。

上面的这些操作必须透明地执行，同时需要不用具备太多实际网络复杂连接情况的了解，或者不用知道如何重新配置协议。虽然用户可以直接地通过设置或重置 VLAN 的端口来配置 VLAN，但缺乏智能网络管理工具的帮助；而保证 VLAN 在若干部门之间正常通信是很困难的。

CISCO 公司提供了一组 VLAN 的管理工具：VLANView 和 TrafficView，我们通过这两个工具来介绍 VLAN 管理所应具有的功能。这些工具都基于 SNMP，完全支持 SNMP 的“get”和“set”操作，而且可以无缝地集成常用的网络管理平台，比如 openView，NetView 和 SunNet Manager 等。这些工具还用可视化的图形用户界面来简化 VLAN 的设计、配置和管理，同时还可管理从小型局域网到具有多层交换的复杂大型网络。

1．VLANView

VLANView 具有图形用户界面，它的核心应用是通过图形界面上的拖放操作模式来为 VLAN 创建的逻辑组分配端口。在这种功能中，以图形方式自动画出每个交换机在网络中拓扑位置，并提供交换机每个端口的状态显示，然后允许用户拖放一个或多个端口给一个 VLAN。这种图形界面下的拖放操作方式减少了配置时间，同时使得操作简单易用。

VLANView 不仅减少了给 VLAN 配置端口的时间，而且还提供了在主干网不同交换机间配置 VLAN 的功能。该功能在相连的路由器与交换机之间传递一系列的配置选项以优化 VL 久 N 的流量、首先、提供一种简单操作模式、该模式可以色动启动交换机之间的主干线路，而这些交换机都配置有 VLAN 或处于连接 VLAN 的链路之上。其次，网络管理员可以通过在冗余线路上分配 VLAN，或在一特定区域内分离 VLAN，以方便地调优它们。最后，网络管理员可以方便地通过主干网查看 VIAN 的配置情况，以及每个 VLAN 的详细连接信息，包括交换机、线路的连接配置以及端口的分配情况。

VLANView 还将具备一些扩展功能，包括通过发现终端主机的 MAC / IP 地址给 VLAN 动态分配交换机的端口，给端口添加安全功能以识别非授权用户以及基于应用层和网络层协议对第三层 VLAN 进行动态分组。

2．TrafficView

TrafficView 是一个基于 RMON 的流量监听与分析应用，该应用可以提供给端口和每个局城网段的流量信息。同时，该应用不仅可以为每个局域网的故障诊断与排除提供帮助，而且流量趋势分析以发现主要的网络变化。这些趋势信息在网络规划阶段、网络实施阶段以及计划审批阶段都非常有用，同时利用这些趋势信息还能很快发现网络发生的故障。

另一方面，TrafficView 的管理代理具有通用性，这些管理代理不仅可以给 Traffic View 提供数据，还可以给任何具有 RMON 的应用提供数据。这为网络管理功能的集成提供了保障。

二、 WAN 接入管理

在网络管理的解决方案中，我们知道一个大型网络，一般是 WAN，是通过分层进行管理的。比如在一个全国性的网络中心之下有许多地区性的网络中心，一般全国性的网络中心主要保证这个 WAN 的主干网正常运转，而地区性网络中心则主要负责各个网络用户的接入管理。

对于每个想入网的用户而言，首先要考虑在网络连接上怎么接人这个网络。一般用户需要找到主管自己这片地区的地区性网络中心，然后提出申请，最后该地区性网络中心再进行用户的接入操作。这些操作一般包括：

(1)联网用户必须租用一条网络线路，连接用户与地区性网络中心。该线路可以是已经存在的，属于某个商业网络公司或电信公司，也可以是单独为该用户铺设的一条线路。 线路既可能是使用光纤的 DDN 专线，也可能是使用电话线的 DDR 线路。联网用户租用了网络线路就要向线路的经营者交纳租金，而线路的经营者可能不是提供接入服务的地 区性网络中心。

(2)联网用户需要向地区网络中心申请一段属于自己的 IP 地址，然后在全国网络中心注册域名。

(3)对于接入的联网用户，一般都要向地区性网络中心一次性交纳一笔接入费用，然后地区网络中心再对该用户进行网络接入的相关配置。

(4)在联网用户端也需要进行相应的配置，然后开通该用户的网络连接，最后联网用户需要根据其使用网络资源的流量交纳网络费用。

在上面的操作中可以看到，地区网络中心对新联网用户的接人需要进行相应的配置， 这些配置操作一般包括：

(1)在接入路由器上，选择一个空闲端口，在该端口上进行相应的配置，然后再根据接人的拓扑关系，配置该端口的路由信息。

(2)在接入路由器上，根据用户的 IP 地址范围建立一个 access-1ist 组，一旦用户要求或其他情况(如用户没有按规定交纳费用等)发生时，可以立即断掉该用户的网络连接。

(3)把该路由器端口和连接联网用户的线路加入网络管理监视对象集，以保障提供给用户可靠、稳定的网络接人服务。

三、 网络故障诊断和排除

网络中可能出现的故障多种多样，往往解决一个复杂的网络故障需要广泛的网络知识与丰富的工作经验。这也是为什么一个成熟的网络管理机构制订有一整套完备的故障管理日志记录机制，同时人们也率先把专家系统和人工智能技术引进到网络故障管理中来的原因。另一方面，由于网络故障的多样性和复杂性，网络故陈分类方法也不尽相同。我们可以根据网络故障的性质把故障分为物理故障与逻辑故障,也可以根据网络故障的对象把故障分为线路故障、路由器故障和主机故障。

我们首先介绍按：照网络故障不同性质而划分的物理故障与逻辑故障。

1．物理故障

物理故障，是指设备或线路损坏、插头松动、线路受到严重电磁干扰等情况。比如说，网络中某条线路突然中断，这时网络管理人员从监控界面上发现该线路流量突然掉下来或系统弹出报警界面，这时首先用 ping 检查线路在网络管理中心这端的端口是否连通，如果不连通，则检查端口插头是否松动，如果松动则插紧，再用 ping 检查，如果连通如故障解决。这时须把故障的特征及其解决步骤详细记录下来。也有可能是线路远离网络管理中心的那端插头松动，则需要通知对方进行解决。另一种常见的物理故障就是网络插头误接。这种情况经常是没有搞清网络插头规范或没有弄清网络拓扑规划的情况下导致的。比如说网络插头都有一些规范，只有搞清网线中每根线的颜色和意义，才能做出符合规范的插头，否则就会导致网络连接出错。另一种情况，比如两个路由器直接连接，这时应该让一台路由器的出口连接另一路由器的入口，而这台路由器的入口连接另一路由器的出口才行，这时制作的网线就应该满足这一特性，否则也会导致网络误解。不过像这种网络连接故障显得很隐蔽，要诊断这种故障没有什么特别好的工具，只有依靠经验丰富的网络管理人员了。

2. 逻辑故障

逻辑故障中的一种常见情况就是配置错误，就是指因为网络设备的配置原因而导致的网络异常或故障。配置错误可能是路由器端口参数设定有误，或路由器路由配置错误以致于路由循环或找不到远端地址，或者是网络掩码设置错误等。比如，同样是网络中某条线路故障，发现该线路没有流量，但又可以 Ping 通线路两端的端口，这时很可能就是路由配置错误导致循环了。诊断该故障可以用 traceroute 工具，可以发现在 traceroute 的结果中某一段之后，两个 IP 地址循环出现。这时，一般就是线路远端把端口路由又指向了线路的近端，导致 IP 包在该线路上来回反复传递。这时需要更改远端路由器端口配置，把路由设置为正确配置，就能恢复线路了。当然处理该故障的所有动作都要记录在日志中。逻辑故障中另一类故障就是一些重要进程或端口关闭，以及系统的负载过高。比如，路由器的 SNMP 进程意外关闭或

死掉，这时网络管理系统将不能从路由器中采集到任何数据，因此网络管理系统失去了对该路由器的控制。还有，也是线路中断，没有流量，这时用 ping 发现线路近端的端口 ping 不通，这时检查发现该端口处于 down 的状态，就是说该端口已经给关闭了，因此导致故障。这时只需重新启动该端口，就可以恢复线路的连通了。另一种常见情况是路由器的负载过高，表现为路由器 CPU 温度太高、CPU 利用率太高，以及内存余量太小等，虽然这种故障不能直接影响网络的连通，但却影响到网络提供服务的质量，而且也容易导致硬件设备的损害。

网络故障根据故、障的不同对象也可划分为：线路故障、路由器故障和主机故障。

1．线路故障

线路故障最常见的情况就是线路不通，诊断这种故障可用 ping 检查线路远端的路由器端口是否还能响应，或检测该线路上的流量是否还存在。一旦发现远端路由器端口不通，或该线路没有流量，则该线路可能出现了故障。这时有几种处理方法。首先是 ping 线路两端路由器端口，检查两端的端口是否关闭了。如果其中一端端口没有响应则可能是路由器端口故障。如果是近端端口关闭，则可检查端口插头是否松动，路由器端口是否处于 down 的状态；如果是远端端口关闭，则要通知线路对方进行检查。进行这些故障处理之后，线路往往就通畅了。如果线路仍然不通，一种可能就得通知线路的提供商检查线路本身的情况，看是否线路中间被切断，等等；另一种可能就是路由器配置出错，比如路由循环了。就是远端端口路由又指向了线路的近端，这样线路远端连接的网络用户就不通了，这种故障可以用 traceroute 来诊断。解决路由循环的方法就是重新配置路由器端口的静态路由或动态路由。

2．路由器故障

事实上，线路故障中很多情况都涉及到路由器，因此也可以把一些线路故障归结为路由器故障。但线路涉及到两端的路由器，因此在考虑线路故障是要涉及到多个路由器。厢有些路由器故障仅仅涉及到它本身，这些故障比较典型的就是路由器 CPU 温度过高、CPU 利用率过高和路由器内存余量太小。其中最危险的是路由器 CPU 温度过高，因为这可能导致路由器烧毁。而路由器 CPU 利用率过高和路由器内存余量太小都将直接影响到网络服务的质量，比如路由器上丢包率就会随内存余量的下降而上升。检测这种类型的故障，需要利用 MIB 变量浏览器这种工具，从路由器 MIB 变量中读出有关的数据，通常情况下网络管理系统有专门的管理进程不断地检测路由器的关键数据，并及时给出报警。而解决这种故障，只有对路由器进行升级、扩内存等，或者重新规划网络的拓扑结构。另一种路由器故障就是自身的配置错误。比如配置的协议类型不对，配置的端口不对等。这种故障比较少见，但没有什么特别的发现方法，排除故障就与网络管理人员的经验有关了。

3．主机故障

主机故障常见的现象就是主机的配置不当。比如，主机配置的 IP 地址与其他主机冲突，或 IP 地址根本就不，在子网范围内，这将导致该主机不能连通。还有一些服务的设置故障。比如 E-Mail 服务器设置不当导致不能收发 E-Mail，或者域名服务器设置不当将导致不能解析域名。主机故障的另一种可能是主机安全故障。比如，主机没有控制其上的 finger，rpc，rlogin 等多余服务。而恶意攻击者可以通过这些多余进程的正常服务或 bug 攻击该主机，甚至得到该主机的超级用户权限等。另外，还有一些主机的其他故障，比如不当共享本机硬盘等，将导致恶意攻击者非法利用该主机的资源。发现主机故障是一件困难的事情，特别是别人恶意的攻击。一般可以通过监视主机的流量、或扫描主机端口和服务来防止可能的漏洞。当发现主机受到攻击之后，应立即分析可能的漏洞，并加以预防，同时通知网络管理人员注意。

四、 网络管理工具

目前网络管理的工具很多，但很多网络管理工具都集成到网络管理系统中，单独的网络管理工具不多。但仍然存在一些简单、实用的网络管理工具，这些工具包括：连通性测试程序(ping)、路由跟踪程序(traceroute)和 MIB 变量浏览器。

1．连通性测试程序

连通性测试程序就是 ping，是一种员常见的网络工具。用这种工具可以测试端到端的连通性，即检查源端到目的端网络是否通畅。ping 的原理很简单，就是从源端向目的端发出一定数量的网络包，然后从目的端返回这些包的响应，如果在一定的时间内收到响应，则程序返回从包发出到收到的时间间隔，这样根据时间间隔就可以统计网络的延迟。如果网络包的响应在一定时间间隔内没有收到，则程序认为包丢失，返回请求超时的结果。这样如果让 ping 一次发一定数量的包，然后检查收到相应的包的数量，则可统计出端到端网络的丢包率，而丢包率是检验网络质量的重要参数。

在广域网中，线路一般是网络的重要对象，因此监测线路的通断，统计线路的延迟与丢包率是发现网络故障、检查网络质量的重要手段。而网络中线路两端一般是路由器的两个端口，所以通常的监测手段就是登录到线路一端的路由器端口上 ping 线路另一端路由器的端口地址，从而掌握该线路的通断情况和网络延迟等参数。同时，由于登录是可以远程进行的，所以即使网络管理者在北京，如果他有足够的权限，他甚至能监测广州到上海线路的情况。

ping 这种工具有一个局限性，它一般一次只能检测一端到另二端的连通性，而不能一次检测一端到多端的连通性。因此 ping 有一种衍生工具就是 fping，fping 与 ping 基本类似，唯一的差别就是 fping 一次可以 ping 多个 IP 地址，比如

C 类的整个网段地址等。网络管理员经常发现有人依次扫描本网的大量 IP 地址，其实就是 fping 做到的。

2，路由跟踪程序

路由跟踪程序就是 traceroute，在 WIN95 中是 tracert 命令。由于 ping 工具存在一些固有的缺陷，比如从网络的一台主机 ping 另一台主机，我们可以知道端到端之间的通断和延迟，但这个端到端之间可能有多条网络线路组成，中间经过多个路由器。用 ping 检查端到端的连通情况，如果不通则无法知道是网络中哪一条线路不通，即使端到端通畅也无法了解线路中四条线路延迟大，哪条线路质量不好，因此这就需要 traceroute 工具了。traceroute 在某种方面与 ping 类似，它也是向目的端发出一些网络包，返回这些包的响应结果，如果有响应也返回响应的延迟。但 traceroute 与 ping 的员大区别在于 traceroute 是把端到端的线路按线路所经过的路由器分成多段，然后以每段返回响应与延迟。如果端到端不通，则用该工具可以检查到哪个路由器之前都能正常鸡应，到哪个路由器就不能响应了，这样就很容易知道如果线路出现故障，则故障源可能出在哪里。另一方面，如果在线路中某个路由器的路由配置不当，导致路由循环，用 traceroute 工具可以方便地发现问题。即 traceroute 一端到另一端时，发现到某一路由器之后，出现的下一个路由器正是上一个路由器，结果出现循环，两个路由器返回的结果中间来回交替出现，这时往往是那个路由器的路由配置指向了前一个路由器导致路由循环了。

3．MIB 变量浏览器

MIB 变量浏览器是另一种重要的网络管理工具。在 SNMP 中，MIB 变量包含了路由器的几乎所有重要参数，对路由器进行管理很大程度上是利用 MIB 变量来实现的。比如，路由器的路由表、路由器的端口流量数据、路由器中的计费数据、路由器 CPU 的温度、负载以及路由器的内存余量等，所有这些数据都是从路由器的 MIB 变量中采集到的。虽然对 MIB 变量的定时采集与分析大部分都是程序进行的，但一种图形界面下的 MIB 变量浏览器也是需要的。一般 MIB 变量浏览器，都按照 MIB 变量的树形命名结构进行设计， 这样就可以自顶向下，根据所要浏览的 MIB 变量的类别逐步找到该变量，而无需记住该变量复杂的名字。网络管理人员可以利用 MIB 变量韧览器取出路由器当前的配置信息、 性能参数以及统计数据等，对网络情况进行监视。

网络管理现状

现在，各大电信运营商的要求网络系统，已经从建设阶段进入了运行维护阶段。在维护阶段，在服务效率和服务质量方面提出了更高的要求。前期网络管理系统存在的不足也逐渐暴露出来，造成在使用和推广方面的障碍。

前期网络管理系统建设存在的主要问题包括：

◇ 网管系统缺乏整体规划。由于没有建立整个网络管理系统的整体规划，造成网络管理产品的重复采购，各厂商的管理界面不统一，缺乏互操作性。

◇ 网络管理需求不明确。前期的网络管理产品大多数与网络应用同步建设，此阶段建设人员更多的精力投入到网络应用的建设中，因此对网络管理需求提出较少，造成建设与实际应用要求的脱节。

◇ 网络管理产品缺乏易用性。国外网管产品具备较严密的体系结构、产品线丰富、成熟度高，为网络管理建立了初期的网管模型。但是，其全英文的界面造成了使用不便。前期的网络管理产品，一般仅支持集中部署模式，造成管理人员在日常监控中的不便。此外，由于产品本身技术问题已经及实施问题，运维人员往往被大量的告警信息所淹没，难以迅速判断故障源。种种不便，造成网络管理系统在建设完成后，运维人员不愿意使用的状况。

◇ 缺乏对于业务的监控。在运行维护阶段，运维人员维护的重点是业务应用。国外网管产品普遍无法提供对应用的监控，造成了网管运维人员认为"网管无用"的错觉。

◇ 对网络安全缺乏足够认识。在网络建设初期，往往忽视网络安全建设。随着网络应用的逐步发展，来自外部的黑客攻击、病毒入侵，以及来自内部的恶意破坏、误操作，造成网络风险日益加剧；在认识到安全的重要性后，又往往对安全进行独立考虑，网络管理与安全管理各自为战，造成管理手段的割裂，同样带来了安全隐患。

◇ 缺乏对运维人员进行管理和监督的技术手段。传统的网管产品，较重视系统本身对故障的监控能力，而缺乏对人员和工作流程的监控和管理。缺乏对故障处理过程的监督，将会影响到故障处理的效率；缺乏对变更过程的评估，将会给网络正常运营带来巨大的风险；缺乏故障处理后的回顾和考核，无法进行企业内部的知识积累，无法推动运维人员使用网络管理系统来处理问题并解决问题。对于人员的管理光靠规章和制度还是不够的，应辅助以足够的技术手段和考核手段。缺乏足够的技术手段的监督，也是造成网管系统推广困难的主要原因。

各运营商及国内的网络管理建设人员，均认识到这些问题，已经开始制定适应企业需要的网络管理方案，并开始研制适应国内电信企业运营的自主的网络管理产品。可以看到国内的网络管理已经开始进入成熟期。

首先理论方面经过不断的实践和修改，已经趋于成熟；网络运维人员对网络管理的认识日趋成熟，对网络管理系统建设的要求更加具体、合理；国内自主知识产权的网络管理产品日趋成熟和专业，国内网络管理厂商根据多年的网

络管理经验、参考电信相关的行业规范，开始制作更加符合国内电信行业运营维护的网络管理系统，且已经开始积累实施经验；经过多年的网络管理系统建设，网络管理系统技术服务人员日趋专业化。

在这一阶段，企业对网络管理提出的要求具有一下特点：

◇ 强调对于业务的管理。随着对网络管理认识的深入和业务的发展，运维人员已经将管理重点转移到业务的监控方面，提出了业务展示的需求，以及需要监控的具体业务指标。

◇ 强调了系统的互操作性。中国移动和中国联通纷纷开始制定网络管理和运营维护规范，提出网络管理系统的整体架构，使得网络管理系统的建设更加规范化，网络管理系统之间具备了互操作性。

◇ 强调系统的易用性。通过总结前期的问题，对网络管理产品的易用性提出了很高的要求。

◇ 强调系统的安全性。强调对于整体业务的安全性的保证，同时将安全设备的报警管理等也纳入到统一的网络管理框架中，防止了管理上的分裂。

◇ 强调管理工作的流程化。通过先进的管理理论 ITIL 与公司管理规章、人员结构相结合，提出了具有企业特点的事件管理、问题管理、配置管理、变更管理流程，并提出绩效管理的具体模式。

◇ 建立完整的网络管理体系架构。通过先进的网络监控手段、安全保障手段与最优化的管理手段的融合，建立了网络和业务系统的安全保障、故障防范、系统监控、故障处理、问题解决的完整的网络管理体系架构。

为了满足 IP 网管在新时期的新要求，国内的网络管理系统建设厂商，开始研发可满足国内电信企业要求的具有自主知识产权的网络管理系统。经过多年的探索和实践，国内的网络管理产品日趋成熟，基本上可以满足现阶段的 IP 网管的需要。国内的网络**管理系统的主要特点是：**

◇ 整体的网络管理架构。通过先进的网管技术、安全技术、IT 服务管理技术的高度融合，建立整体网络管理架构，实现对安全、性能、故障、配置和资产的统一管理；通过建立事件管理、问题管理、配置管理和变更管理的最佳服务管理流程，保证 IT 服务效率和服务质量；通过建立绩效管理，保证对服务质量有效管理和监控。整体网络管理架构的建立，改变了以往管理监控产品分散、工作流程与监控系统脱节的局面。如果说前期的网络管理是对于设备运行状况的一次设备层的梳理的话，整体网络管理架构的建设是同时对设备、工作流和人员进行了一次梳理，使得运维工作更加顺畅。

◇ 具备较好的集成性。由于目前的网络设备、存储设备等对网络管理系统的开放程度不一，有的仅支持其自身的管理软件，企业往往需要采购不同的管理软件，造成管理分散，管理界面不统一，使管理工作变得更加复杂。因此，需要具备集成性的网络管理平台，将不同厂商的网络和应用管理产品在界面级、消息级和数据级集成起来。

◇ 具备针对系统、业务的监控能力。包括对系统、业务应用的拓朴展示、关键文件和进程的监控、实时的性能监控、故障告警、故障分析、定位和处理等。网络管理系统对业务的监控和管理能力的增强，提高了企业的服务能力和服务质量，从而提高了企业的市场竞争能力。因此，越来越多的业务将进入网络管理的监控范围。对于业务的监控的细化，将成为今后的网络管理系统完善的重点。

◇ 具备安全管理能力。通过对入侵监测、漏洞扫描、防病毒、防火墙、数字认证技术、授权访问技术的综合利用，为业务系统的正常运营提供安全环境，并将安全设备管理纳入网络管理范围，进行统一告警和处理，以保证安全事件的发生"事前有监控，事后有响应"。

◇ 易于使用和部署。采用中文界面，并支持集中式、分布式和集中分布式等多种部署方式。运维人员除可以在一个集中的管理界面上，对整体网络系统进行监控和故障外，还可支持根据业务内容，对管理对象进行管理区域划分，并指定相关运维人员进行管理。系统支持个性化，支持权限管理和 B/S 模式。运维人员可以方便地通过浏览器进入自己的管理界面，进行对相关业务和系统的监控。

◇ 增强系统分析和处理能力。简化管理界面，使之更适于运维人员的使用。同时，增强系统分析和处理能力。通过事件压制、事件合并、事件过滤以及事件关联等多种技术手段，屏蔽不重要的告警信息，减少告警干扰。帮助运维人员能够将精力集中关键问题上，准确定位故障源，并协助提出问题的解决方案。

◇ 增强的系统的性能管理能力。网络系统管理已经从被动的管理进入主动的管理阶段，因此可以看到系统的侧重点从故障管理开始转移到对系统性能的管理。通过对网络设备、安全设备、系统平台、数据库、中间件以及业务系统性能的实时监控，对监控对象之间关联性的分析，迅速定位性能瓶颈，对性能瓶颈设备进行改造，可以有效的做到对系统运行状况的控制，减少突发事件发生的频率。此外，历史性能数据的分析，为系统和设备的升级提供了参考依据，增强了网络和应用系统的经济性和实用性。

◇ 具备可扩展性。电信运营商的网络设备和业务系统，在近几年来呈几何级数增长。因此，网络管理系统应具备可扩展性，以便将新的网络设备和业务系统方便地纳入网络管理范围。网络管理系统只有具备良好的可扩展性，才能适应电信行业业务发展的需要。

网络管理发展趋势

毫无疑问，伴随着新的网络技术的发展，网络管理必将融入先进技术和管理手段，以适应网络的发展。目前，这些新的技术和管理模式已经呈萌芽态势：

◇ 网络管理范围将扩展到无线网络、VoIP、VPN 领域，同时网络管理系统中，也必将融入这些新技术。

◇ 网络管理系统智能化。系统将提供智能模拟、故障自动诊断和排除、系统自动恢复等人工智能技术，帮助运维人员更好的完成运维工作。

◇ 网络管理系统将为企业高层决策提供支持。网络管理系统将不仅仅是运维人员的管理和服务工具，同时也将成为高层对企业的业务运行状况的观察工具，并为企业的决策支持提供业务数据。

◇ 网络管理将更加侧重于服务。从当今的网络管理系统上可以看出，企业已经将注意力从设备转移到了服务支持。在未来的网络管理系统的建设中，网络管理的服务化将更加受到企业的支持。

总之，随着网络技术的不断发展，网络管理技术将成为企业不可豁却的管理手段，将直接影响到企业的服务质量、管理水平，影响到企业的市场地位。