内 容 简 介

本书是为《网络管理与维护》课程配套编写的实验指导书。配合计算机网络原理、网络管理与维护的教学体系及方法，通过实验循序渐进地使学生了解网络管理的主要功能，及业界流行的专业网管工具的使用和主要功能，提高学生的理解能力与动手能力。

本书编排了 10 个实验，包括基本网络测试工具的使用、抽象语法记法 1 分析、SNMP 网管配置、SNMP MIB 信息的访问、SNMP 协议工作原理验证与分析、RMON 原理与配置以及网络监视器、性能监视器等。每个实验包括实验目的、实验性质、实验内容和步骤等，其中，验证性实验给出了相关理论，设计性实验给出了设计过程中的思路，启发和引导学生的思考和动手能力。

本书可供网络工程专业开设《网络管理与维护》课程用作实验教材。

本书 2009 年 2 月首次使用，于 2010 年 2 月进行了修订第一次修订，并于 2012 年 1 月再次进行增加了新的内容和新的实验。由于计算机应用技术发展迅速，网络设备与软件版本日益更新，书中疏漏之处在所难免，敬请读者批评指正。

实验要求

《网络管理与维护》课程实验的目的是为了使学生在课程学习的同时，通过在计算机网络环境中的实际操作，对现代计算机网络管理与维护中广泛使用的技术有一个初步的了解；通过实验环节，使学生加深了解和更好地掌握《网络管理与维护》课程教学大纲要求的内容。

在《网络管理与维护》的课程实验过程中，要求学生做到：

⑴ 预习实验指导书有关部分，认真做好实验内容的准备，就实验可能出现的情况提前作出思考和分析。

⑵ 仔细观察上机和上网操作时出现的各种现象，记录主要情况，作出必要说明和分析。

⑶ 认真书写实验报告。实验报告包括实验目的和要求，实验情况及其分析。对需编程的实验，写出程序设计说明，给出源程序框图和清单。

⑷ 遵守机房纪律，服从辅导教师指挥，爱护实验设备。

⑸ 实验课程不迟到。如有事不能出席，所缺实验一般不补。

实验的验收将分为两个部分。第一部分是上机操作，包括检查程序运行和即时提问。第二部分是提交书面的实验报告。此外，针对以前教学中出现的问题，网络实验将采用阶段检查方式，每个实验都将应当在规定的时间内完成并检查通过，过期视为未完成该实验，不计成绩。以避免期末集中检查方式产生的诸多不良问题，希望同学们抓紧时间，合理安排，认真完成。

限于编者实践环节与水平，缺点与不足在所难免，敬请读者批评指正。

目 录

实验 1 基本网络测试工具的使用

1.1 实验目的

⑴ 熟悉常用网络测试命令的语法及其功能；

⑵ 掌握常用的网络故障分析及排除的方法。

1.2 实验类型

验证型实验

1.3 实验环境

可以接入 Internet 的 PC 机。

1.4 实验内容与步骤

1 实验内容

⑴ 阅读后面附录部分相关参考资料，学习常用网络测试命令知识；

⑵ 运行常用网络测试命令，学习网络故障排除的方法，对运行结果进行分析；

⑶ 通过百度等搜索引擎搜索其他的一些网络测试命令或专用的网络测试工具软件，例如 Qcheck 等，通过运行观察其结果。

2 实验步骤

⑴ 在 MS-DOS 窗口中输入“ping 127.0.0.1”来测试本机网卡是否工作正常。

（问题思考：127.0.0.1 这个 ip 地址有什么特殊含义，只能在此处输入 ip 地址吗？）

⑵ 用 ipconfig 命令查看本机的配置信息及其含义。

⑶ 用 ping 命令测试本机是否可和默认网关连通。

⑷ 使用 ping 命令的前后分别运行 arp 命令。记录前后的结果。

（问题思考：前后结果相同吗，为什么？）

⑸ 执行 tracert 命令，记录数据包到达目标主机所经过的路径及到达每个节点的时间。

命令格式：tracert www.163.com（外网）或：tracert www.xust.edu.cn（校园网）。

⑹ 尝试其它的网络测试命令。

1.5 思考题

⑴ 如何判断网络是否连通？

⑵ 如何查看计算机的 MAC 地址、IP 地址？

⑶ 运行 tracert 59.64.182.1，结合结果描述数据从本机到目的主机之间所经过的路由。

附录：参考资料及实验说明

1 网络系统故障

现实使用过程中，计算机网络系统出现问题的情况并不少见，这些问题有的是用户使用不当造成的，也有的是网络系统出现了各种故障，为此我们必须掌握网络系统故障分析和排除的基本方法。

计算机网络系统出现的故障主要分以下几类：

① 网卡故障；

② 计算机网络软件和协议配置问题；

③ LAN 网络连线故障；

④ 网关故障；

⑤ DNS 故障；

⑥ 骨干网故障；

⑦ 网络服务器故障；

⑧ 网络病毒等。

2 网络测试的常用工具和命令

⑴ 利用 ipconfig 显示用户所在主机内部的 IP 协议的配置信息

使用格式：ipconfig [/?] [/all]

参数介绍：

/?　显示 ipconfig 的格式和参数的英文说明。

/all　显示有关 IP 地址的所有配置信息。

主要功能：显示用户所在主机内部的 IP 协议的配置信息。

详细介绍：ipconfig 程序采用 Windows 窗口的形式来显示 IP 协议的具体配置信息。如果 ipconfig 命令后面不跟任何参数直接运行，程序将会在窗口中显示网络适配器的物理地址、主机的 IP 地址、子网掩码以及默认网关等。还可以通过此程序查

看主机的相关信息如：主机名、DNS 服务器、节点类型等。其中网络适配器的物理地址在检测网络错误时非常有用。在命令提示符下键入 ipconfig / ？可获得 ipconfig 的使用帮助，键入 ipconfig / all 可获得 IP 配置的所有属性。

举例说明：如果我们想很快地了解某一台主机的 IP 协议的具体配置情况，可以使用 ipconfig 命令来检测。其具体操作步骤如下：首先单击“开始”菜单，从弹出的菜单中找到“运行”命令，接着程序会打开一个标题为“运行”的对话框，在该对话框中，我们可以直接输入 ipconfig 命令，接着再单击一下回车键。

⑵ 利用 ping 测试网络联通性

使用格式：ping [x] [-t] [-a] [-n count] [-l size]

参数介绍：

-t　让用户所在的主机不断向目标主机发送数据。

-a　以 IP 地址格式来显示目标主机的网络地址。

-n count　指定要 ping 多少次，具体次数由后面的 count 来指定。

-l size　指定发送到目标主机的数据包的大小。

主要功能：用来测试一帧数据从一台主机传输到另一台主机所需的时间，从而判断主响应时间。

详细介绍：该命令主要是用来检查路由是否能够到达某站点。由于该命令的包长常小，所以在网上传递的速度非常快，可以快速检测要去的站点是否可达。如果执行 ping 不成功，则可以预测故障出现在以下几个方面：网线是否连通，网络适配器配置是否正确，IP 地址是否可用等。如果执行 ping 成功而网络仍无法使用，那么问题很可能出在网络系统的软件配置方面，ping 成功只能保证当前主机与目的主机间存在一条连通的物理路径。它的使用格式是在命令提示符下键入：ping IP 地址或主机名，执行结果显示响应时间。重复执行这个命令，你可以发现 ping 报告的响应时间是不同的。具体的 ping 命令后还可跟好多参数，你可以键入 ping 后回车，以得到详细说明。

举例说明：当我们 ping 一个站点时，得到的回答是 Request time out 信息，意味着网址没有在 1 秒内响应，这表明服务器没有对 ping 做出响应的配置或者网址反应极慢。如果你看到 4 个“请求暂停”信息，说明网址拒绝 ping 请求。因为过多的 ping 测试本身会产生瓶颈，因此，许多 Web 管理员不让服务器接受此测试。如果网址很忙或者出于其他原因运行速度很慢，如硬件动力不足，数据信道比较狭窄，可以过

一段时间再试一次，以确定网址是不是真的有故障。如果多次测试都存在问题，则可以认为是用户的主机和该站点没有联接上，用户应该及时与因特网服务商或网络管理员联系。

⑶ 利用 tracert 判定数据包到达目的主机所经过的路径

使用格式：tracert [-d] [-h maximum_hops] [-j host_list] [- w timeout]

参数介绍：

-d　不解析目标主机的名称。

-h maximum_hops　指定搜索到目标地址的最大跳跃数。

-j host_list　按照主机列表中的地址释放源路由。

-w timeout　指定超时时间间隔，程序默认的时间单位是毫秒。

主要功能：判定数据包到达目的主机所经过的路径、显示数据包经过的中继节点清单和到达时间。

详细介绍：这个应用程序主要用来显示数据包到达目的主机所经过的路径。该命令的使用格式是在 DOS 命令提示符下或者直接在运行对话框中键入如下命令：tracert 主机 IP 地址或主机名。执行结果返回数据包到达目的主机前所经历的中断站清单，并显示到达每个继站的时间。该功能同 ping 命令类似，但它所看到的信息要比 ping 命令详细得多，它把你送出的到某一站点的请求包，所走的全部路由均告诉你，并且告诉你通过该路由的 IP 是多少，通过该 IP 的时延是多少。具体的 tracert 命令后还可跟好多参数，大家可以键入 tracert 后回车，其中会有很详细的说明。

举例说明：要是大家想要详细了解自己的计算机与目标主机之间的传输路径信息，可以使用 tracert 命令来检测一下。其具体操作步骤如下：首先单击“开始”菜单按钮，从弹出的菜单中找到“运行”命令，接着程序会打开一个标题为“运行”的对话框，在该对话框中，直接输入 tracert 目标网址命令，单击回车。

⑷ 利用 netstat 了解到主机与因特网的连接

使用格式：netstat [-r] [-s] [-n] [-a]

参数介绍：

-r　显示本机路由标的内容。

-s　显示每个协议的使用状态（包括 TCP、UDP、IP）。

-n　以数字表格形式显示地址和端口。

-a　显示所有主机的端口号。

主要功能：该命令可以让用户了解到自己的主机是怎样与因特网相连接的。

详细介绍：netstat 程序有助于我们了解网络的整体使用情况。它可以显示当前正在活动的网络连接的详细信息，例如显示网络连接、路由表和网络接口信息，可以让用户得知目前总共有哪些网络连接正在运行。我们可以使用 netstat / ？ 命令来查看一下该命令的使用格式以及详细的参数说明。该命令的使用格式是在 DOS 命令提示符下或者直接在“运行”对话框中键入如下命令：netstat[参数]，利用该程序提供的参数功能，我们可以了解该命令的其他功能信息，例如显示以太网的统计信息、显示所有协议的使用状态，这些协议包括 TCP 协议、UDP 协议以及 IP 协议等。另外还可以选择特定的协议并查看其具体使用信息，还能显示所有主机的端口号以及当前主机的详细路由信息。

举例说明：如果要了解盐城市信息网络中心节点的出口地址、网关地址、机地址等信息，可以使用 netstat 命令来查询。具体操作方法如下：首先单击“开始”菜单按钮，从弹出的菜单中找到“运行”命令，接着程序会打开一个标题为“运行”的对话框，在该对话框中，直接输入 netstat 命令，单击回车键即可，也可以在 MS-DOS 方式下，输入 netstat 命令。

⑸ 其它工具和命令

① ROUTE.EXE

该工具显示了您的机器 IP 的路由表，主要显示这几个方面的信息：目标地址、网络掩码、网关、本地 IP 地址和 Metric。

显示全部信息的用法为：ROUTE print 回车

② ARP.EXE

该工具用于查看和处理 ARP 缓存，ARP 是名字解析协议的意思，负责把一个 IP 地址解析成一个物理性的 MAC 地址。

显示全部信息的用法为：ARP -a 回车

③ NBTSTAT.EXE

该工具主要用于查看当前基于 NETBIOS 的 TCP/IP 连接状态，通过该工具你可以获得远程或本地机器的组名和机器名。

用法为：NBTSTAT -a 域名 或 NBTSTAT -A IP 地址 回车

上述程序的使用注意要点主要有以下两点:

① 以上程序最好先打开 MS-DOS 方式再运行;

② 命令用法可用命令/? （如 ping/?）显示命令的详细帮助信息。

3 网络故障分析和排除的基本步骤

产生网络故障原因是很复杂的，同样故障可能导致不同表现。但是，查找故障的基本方法应从最简单的错误入手，先检查网络线、网卡配置、网络连接设备 HUB/交换机的连接；然后是软件设置；最后是其他一些网络硬件故障，因为无论是网卡，HUB 或交换机在正确使用下都是没有那么快就坏的。为了有效地解决故障，我们需要有网络的文档。最好要装备合理工具软件来帮助我们了解在网络正常工作时的参数，通过分析找出网络的故障，具体运用时可参照下图提供的步骤来操作。

Qcheck 是 NetIQ 公司推出的网络应用与硬件测试软件包 Chariot suite 的一部份，是一个免费公版程序。主要功能是向 TCP、UDP、IPX、SPX 网络发送数据流从而来测试网络的吞吐率、回应时间等。下面我们就择其重点介绍一下：

TCP 响应时间（TCP Response Time）

这项测试可以测得完成 TCP 通讯的最短、平均与最长时间。这个测试和「ping」很像，目的在于让你知道收到另一台机器所需的时间。这个测量一般称为「延缓」或「延迟」（latency）。

TCP 传输率（TCP Throughput）

这项测试可以测量出两个节点间使用 TCP 协议时，每秒钟成功送出的数据量。通过这项测试可以得出网络的带宽。

UDP 串流传输率（UDP Streaming Throughput）

和多媒体应用一样，串流测试会在不知会的状况下传送数据。在 Qcheck 中，使用无连结协议的 IPX（Internetwork Packet Exchange，网络交换协议）或 UDP。Qcheck 的串流测试是评估应用程序使用串流格式时的表现，例如 IP 线上语音以及视频广播。此测试显示多媒体流通需要多少的频宽，以方便网络硬件速度和网络所能达到真正数据传输率间的比较。

另外也可以测得封包遗失（packet loss）情况以及处理中的 CPU 占用率（CPU utilization）。

实验 2 Windows SNMP 服务配置

2.1 实验目的

⑴ 掌握 SNMP 服务在主机上的启动与配置。

⑵ 掌握用 MIB 浏览器访问主机上 SNMP MIB 对象的值，测试 Windows SNMP 服务。

2.2 实验类型

验证型实验

2.3 实验环境

⑴ 运行 WIN2000/2003/XP 操作系统的 PC 一台；

⑵ 已安装 MG－SOFT MIB Browser 程序。

2.4 实验原理

1 SNMP 网络管理模型

SNMP 网络管理模型由网络管理站（Manager）、被管设备(Agent)、管理信息数据库（MIB）、管理协议（SNMP）四大部分组成。SNMP 管理模型具备典型的 C/S 体系结构。网络管理站可以是一般的计算机，它运行复杂的管理器软件，对网络设备进行监控。管理器软件一般是图形界面，以图表、曲线方式显示各种网络数据；某些产品还具有相当程度的智能，它能自动分析收集到的网络数据，必要时可以向网络管理员报告错误并指出错误的原因。被管的网络设备可以多种多样，如主机、路由器、网桥、终端服务器等。被管设备上的代理一般以守护进程形式在后台运行。

代理和管理系统都使用 SNMP 消息来检查和交换主机信息。使用 UDP 发送 SNMP 消息。管理系统所需的信息包含在管理信息库 MIB 中。MIB 是一个数据库，此数据库包含关于网络计算机的各种类型的信息。

2 Snmputil 工具的使用

Snmputil 是一个命令行下的软件，使用语法如下：

usage: snmputil get|getnext|walk agent community oid [oid ...]

snmputil trap

其中 snmputil 是程序名；get，获取一个信息；getnext，获取下一个信息；walk，获取指定子树/子目录的全部信息)；agent 表示代理进程的 IP 地址，community 表示团体名，oid 表示 MIB 对象 ID，可以理解成 MIB 管理信息库中各种信息分类存放树资源的一个数字标识。举例说明：

⑴ 查看本地计算机（IP 地址为 192.168.0.3）的系统信息

通过对系统组的 MIB 对象的查阅，我们知道系统信息所对应的 MIB 对象为.1.3.6.1.2.1.1.1（参看系统组对象），我们使用 get 参数来查询：

C:>snmputil get 192.168.0.3 public .1.3.6.1.2.1.1.1.0

Variable = system.sysDescr.0

Value = String Hardware: x86 Family 15 Model 2 Stepping 7 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free)

其中 public 是 192.168.0.3 计算机上的团体名，.1.3.6.1.2.1.1.1.0 是对象实例，注意对象 ID 前面有个“.”，后面还要加一个“0”。如果不在对象 ID 末尾加上一个 0，那么用 get 参数查询就会出错。从查询结果中我们能够看出操作系统版本和 CPU 类型。

⑵ 查询计算机连续开机多长时间

C:>snmputil get 192.168.0.3 public .1.3.6.1.2.1.1.3.0

Variable = system.sysUpTime.0

Value = TimeTicks 447614

如果我们在对象 ID 后面不加 0，使用 getnext 参数能得到同样的效果：

C:>snmputil getnext 192.168.0.3 public .1.3.6.1.2.1.1.3

Variable = system.sysUpTime.0

Value = TimeTicks 476123

⑶ 查询计算机的联系人

C:>snmputil get 192.168.0.3 public .1.3.6.1.2.1.1.4.0

Variable = system.sysContact.0

Value = String administrator

以上简单介绍了用 snmputil 查询代理进程的方法，由于在命令行下使用，可能大家感到颇为不方便，但命令行的一个好处就是可以促进大家主动查阅 MIB 对象，加深对 SNMP 网络管理的认识。

⑷ 使用 walk 查询设备上所有正在运行的进程：

C:>snmputil walk 192.168.0.3 public .1.3.6.1.2.1.25.4.2.1.2

Variable = host.hrSWRun.hrSWRunTable.hrSWRunEntry. hrSWRunName.1

Value = String System Idle Process

Variable = host.hrSWRun.hrSWRunTable.hrSWRunEntry. hrSWRunName.4

Value = String System

Variable = host.hrSWRun.hrSWRunTable.hrSWRunEntry. hrSWRunName.292

Value = String snmputil.exe

Variable = host.hr

SWRun.hrSWRunTable.hrSWRunEntry. hrSWRunName.308

限于篇幅不把所有进程列出来，大家可以在自己的计算机上面实验，以加强感性认识。

⑸ 查询计算机上面的用户列表

C:>snmputil walk 192.168.0.3 public .1.3.6.1.4.1.77.1.2.25.1.1

Variable = .iso.org.dod.internet.private.enterprises. lanmanager.lanmgr-2.server.

svUserTable.svUserEntry.svUserName.4.117.115.101.114

Value = String user

Variable = .iso.org.dod.internet.private.enterprises. lanmanager.lanmgr-2.server.

svUserTable.svUserEntry.svUserName.5.71.117.101.115.116

Value = String Guest

Variable = .iso.org.dod.internet.private.enterprises.

lanmanager.lanmgr-2.server.svUserTable.svUserEntry.

svUserName.13.65.100.109.105.110. 105.115.116.114.97.116.111.114

Value = String Administrator

从中我们可以得知该计算机共有三个用户，它们分别为 user、guest 和 administrator。

Snmputil 还有一个 trap 的参数，主要用来陷阱捕捉，它可以接受代理进程上主动发来的信息。如果我们在命令行下面输入 snmputil trap 后回车，然后用错误的团体名来访问代理进程，这时候就能收到代理进程主动发回的报告。

在 MIBII 中总共有 175 个对象，每个对象均有其不同的含义，我们只有通过查阅 MIB 才能知道它们各自的作用。MIB 对象是 SNMP 网络管理中的核心内容，只有深入了解 MIB 对象的含义我们才有可能知道如何去驾驭 SNMP 网络管理。

2.5 实验内容与步骤

1Windows 的 SNMP 服务的安装

将 Windows 的安装关盘放入驱动器，然后点击“开始”，指向“设置”，单击“控制面板”，双击“添加/删除程序”，然后单击“添加/删除 Windows 组件”，打开 Windows 组件向导。在“组件”中，单击“管理和监视工具”，然后单击“下一步”。安装后 SNMP 将自动启动。

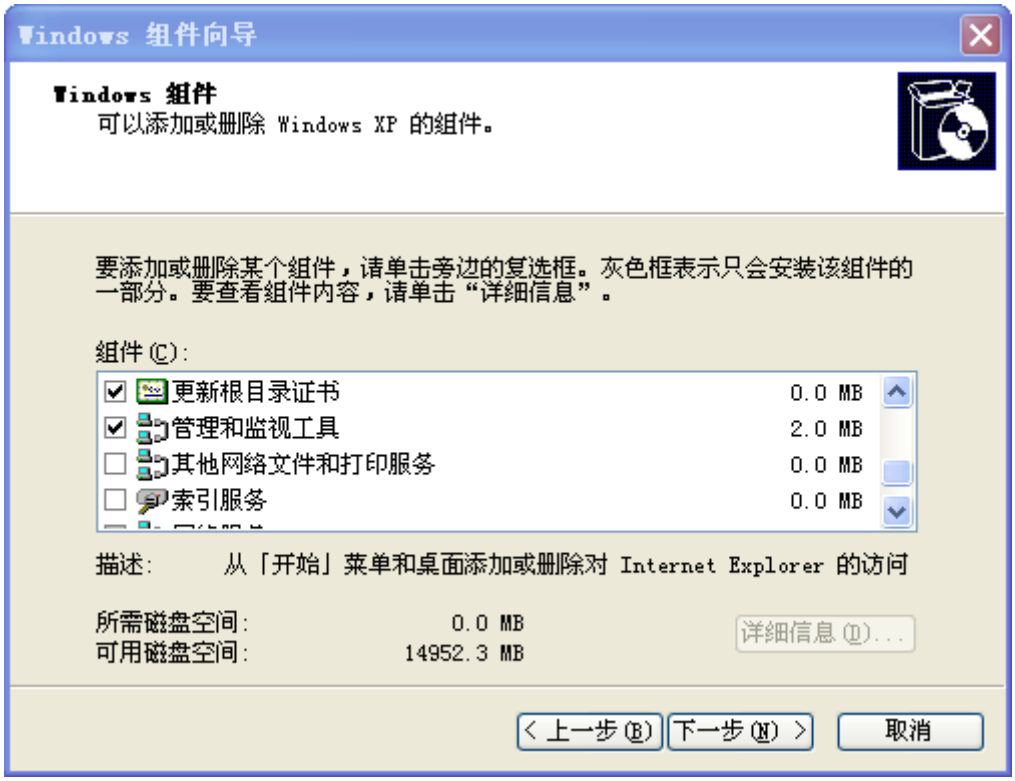

图 2-1 Windows 组件向导

2 在本地主机上启动 SNMP 服务

实验中上述步骤 1 应该已经完成，SNMP 服务应该已经启动。如果 SNMP 服务还未启动则可以通过控制面板—>管理工具—>服务，找到 SNMP service 和 SNMP

trap service（若列表中不存在此服务，则进行步骤 1）并将其启动（右键列表中或双击打开的对话框中）。

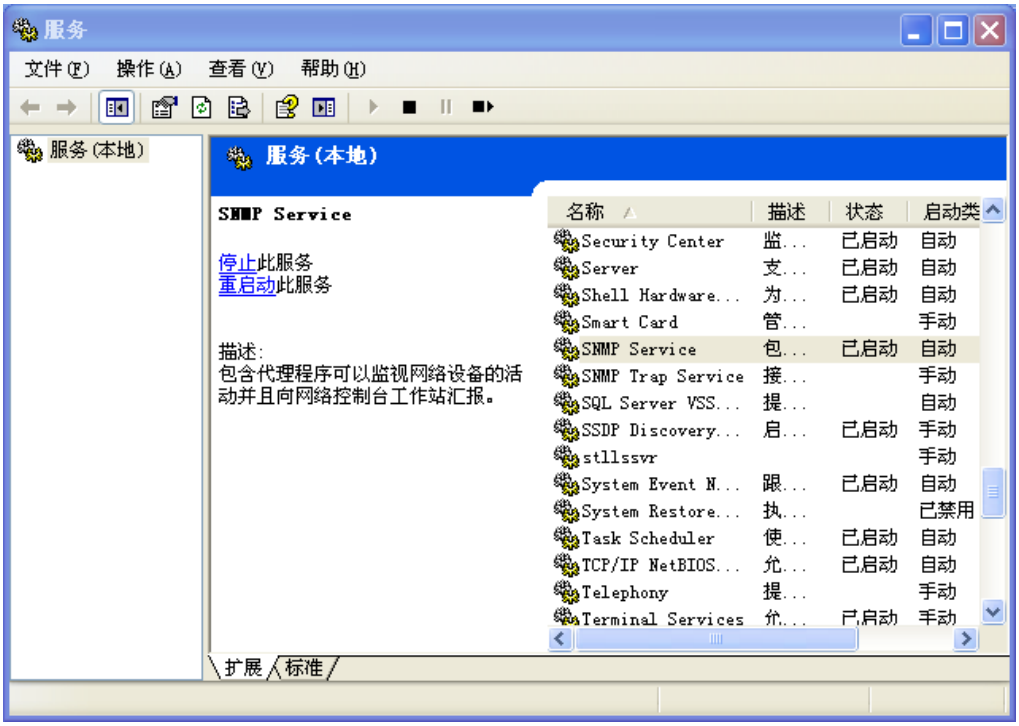

图 2-2 启动 SNMP 服务

3 配置 SNMP 代理属性

通过控制面板—>管理工具—>服务，找到 SNMP service；在右键快捷菜单中单击“属性”。

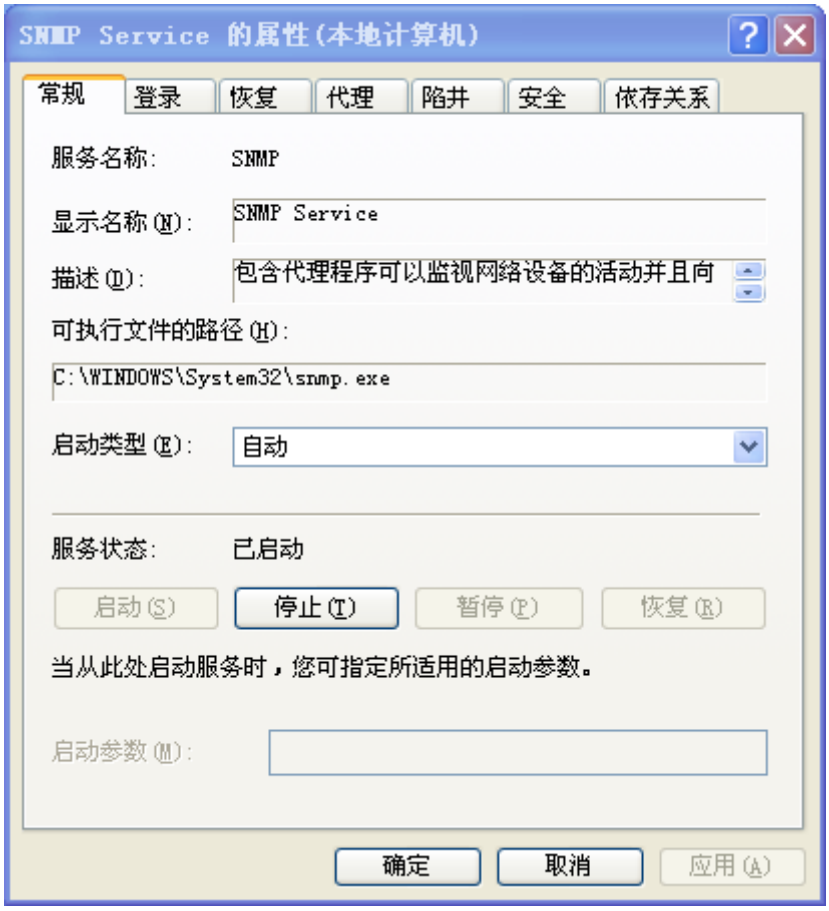

图 2-3 SNMP 服务属性

在“代理”选项卡上的“联系人”中，键入此计算机的用户或管理员的名字（如 Administator）。

在“位置”中，键入计算机或联系人的物理位置，如计算机的 MAC 地址 (00-26-18-A2-47-8A)。

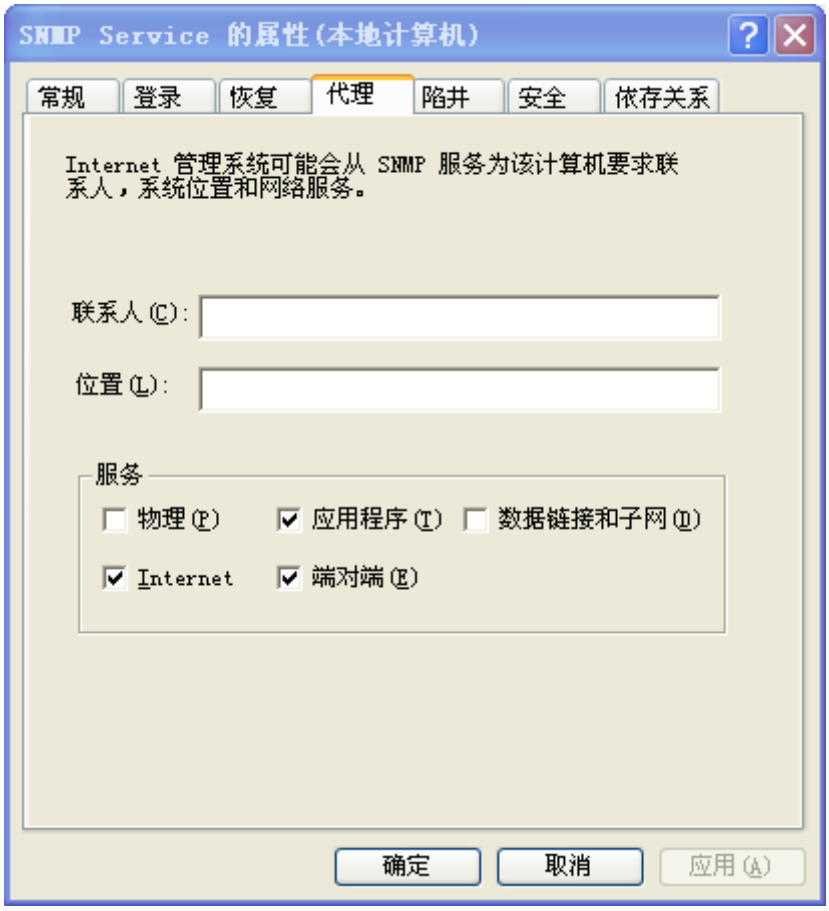

图 2-4 SNMP 代理属性配置

4 配置 SNMP 陷阱属性

在“陷阱”选项卡上的“团体名称”下，键入此计算机发送的陷阱消息的目标团体名称（区分大小写）（public）,然后单击“添加到列表”。

在“陷阱目标”中，单击“添加”。

在“主机名，IP 或 IPX 地址”中，请键入主机信息，然后单击“添加”（例如 192.168.0.100，即本机的 IP 地址）。

重复上述步骤，直到所需的全部团体名和陷阱目标添加完成。

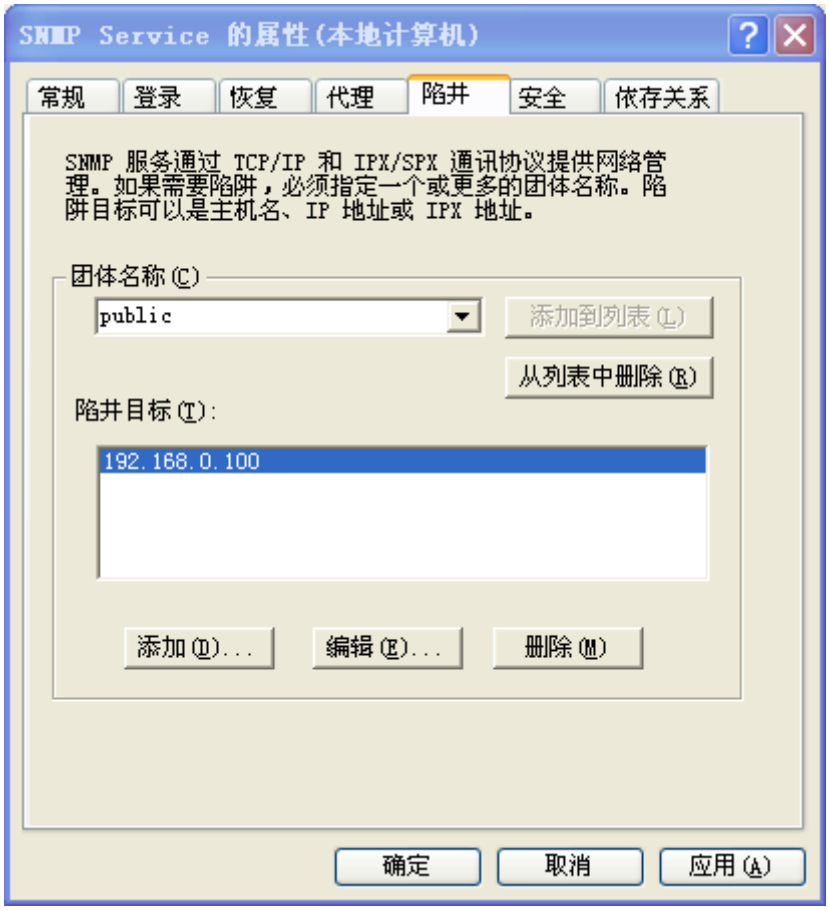

图 2-5 SNMP 陷阱属性配置

5 配置 SNMP 安全属性

打开计算机管理-服务-SNMP 服务-属性。

如果系统在身份验证失败时发送陷阱消息，那么请在“安全”选项卡上选中“发送身份验证陷阱”。

在“接受团体名称”下，单击“添加”。在“团体名称”中，键入团体名称（区分大小写）（public），然后单击“添加”。

指定是否接受来自某个主机的 SNMP 数据包：

要接受来自网络上任何主机的 SNMP 请求而不考虑其身份，请单击“接受来自任何主机的 SNMP 数据包”；

要有限制地接受 SNMP 数据包，请单击“接受来自这些主机的 SNMP 数据包”，然后单击“添加”，键入适当的主机名、IP 地址或 IPX 地址，然后再次单击“添加”。

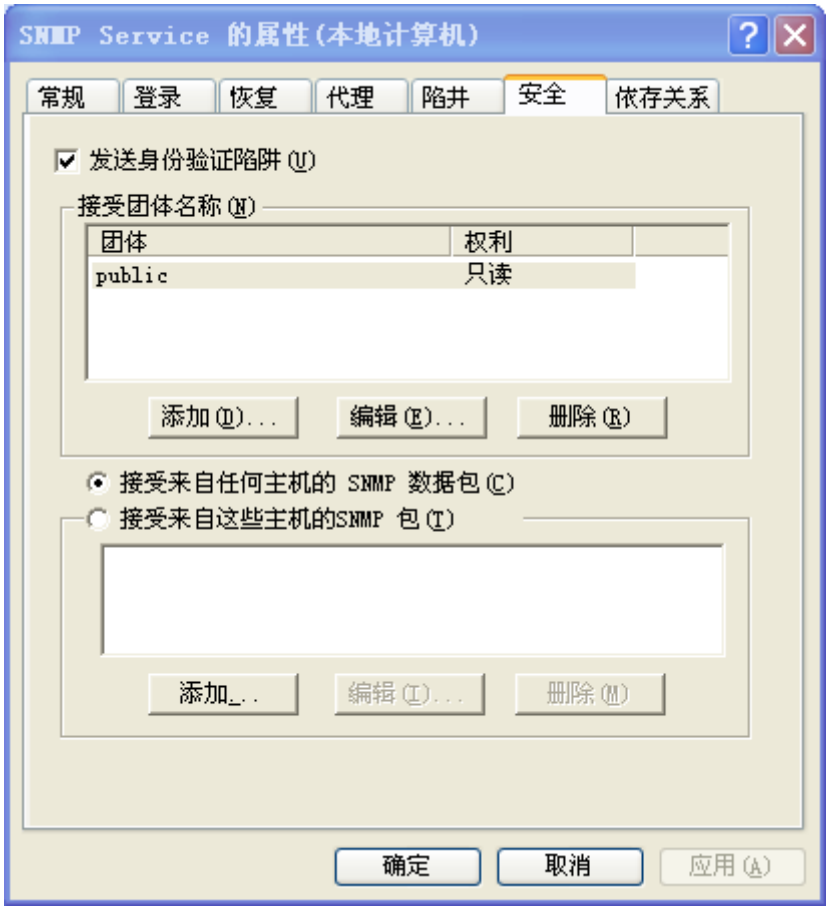

图 2-5 SNMP 安全属性配置

6 测试 Windows SNMP 服务

用 Microsoft 提供的一个实用程序 SNMPUTIL 测试。将 snmputil.exe 拷贝到一个目录下，例如 C 盘根目录下。测试前确定本机 IP 地址（例如 192.168.0.100），有效团体名称为 public。

⑴ 用 get request 查询变量 SYSDESC

Snmputil get 192.168.0.100 public 1.1.0

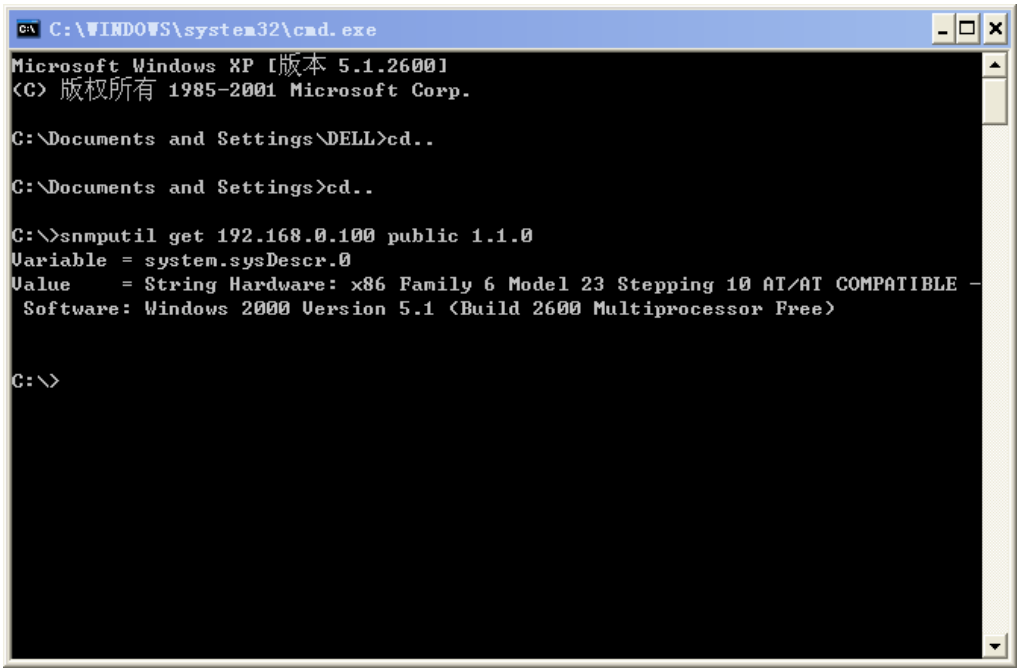

图 2-6 get 命令查询结果

⑵用 get next request 查询变量 SYSDESC

Snmputil getnext 192.168.0.100 public 1.1

得到和⑴一样的结果。

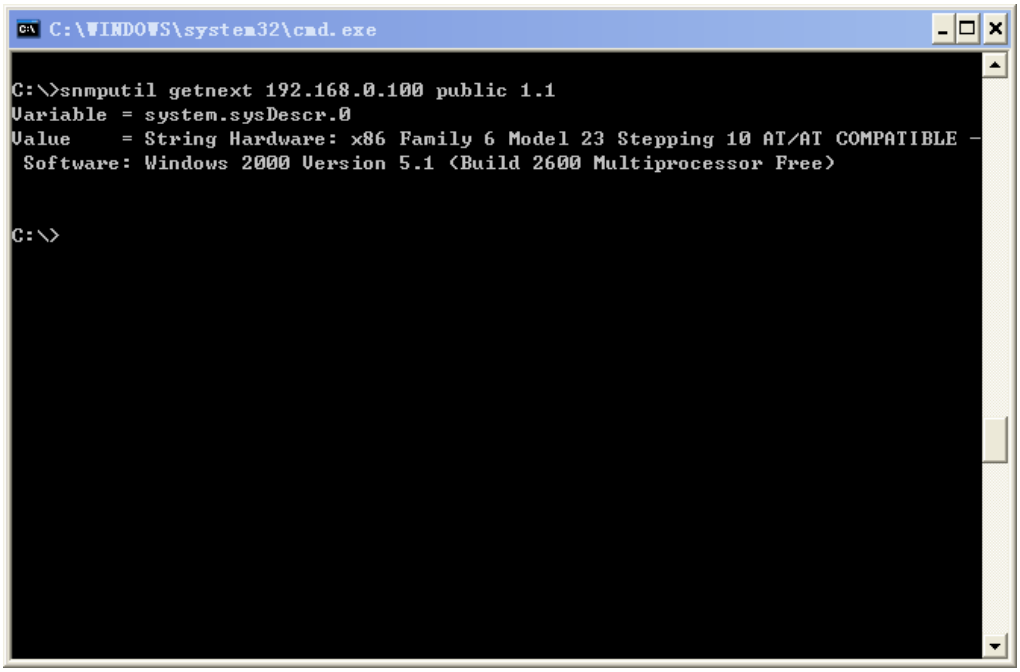

图 2-7 getnext 命令查询结果

⑶ 用 getnext 查询一个非 MIB-2 变量

Snmputil getnext 192.168.0.100 public 1.3.6.1.4.1.77.1.3

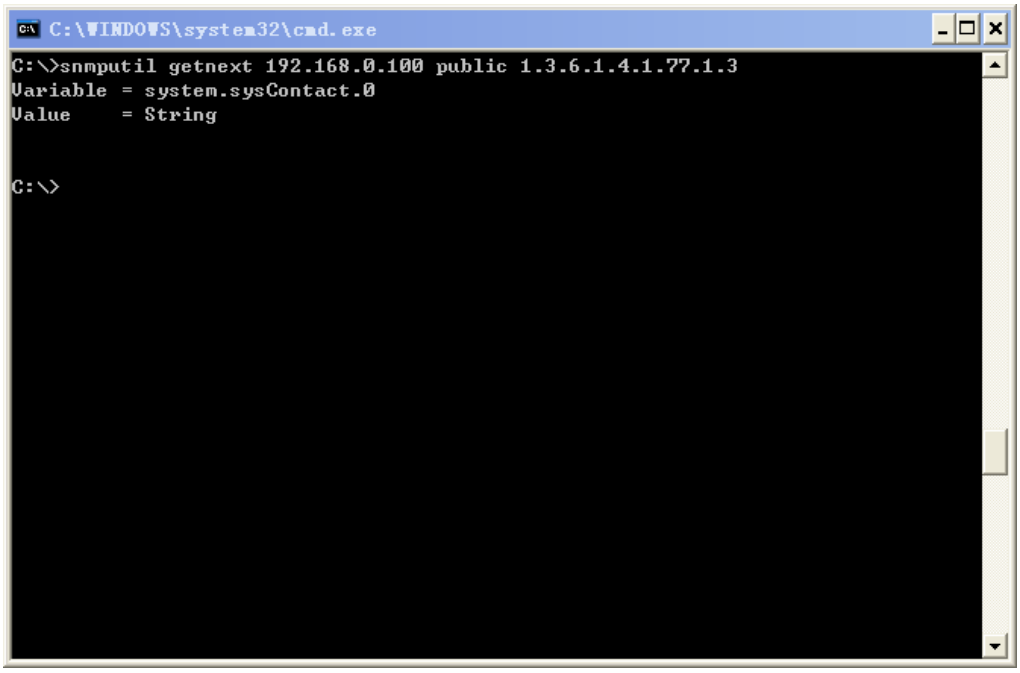

图 2-8 get 命令查询错误结果

⑷ 用 walk 遍历整个 MIB-2 的系统组变量

Snmputil walk 192.168.0.100 public .1.3.6.1.2.1.1

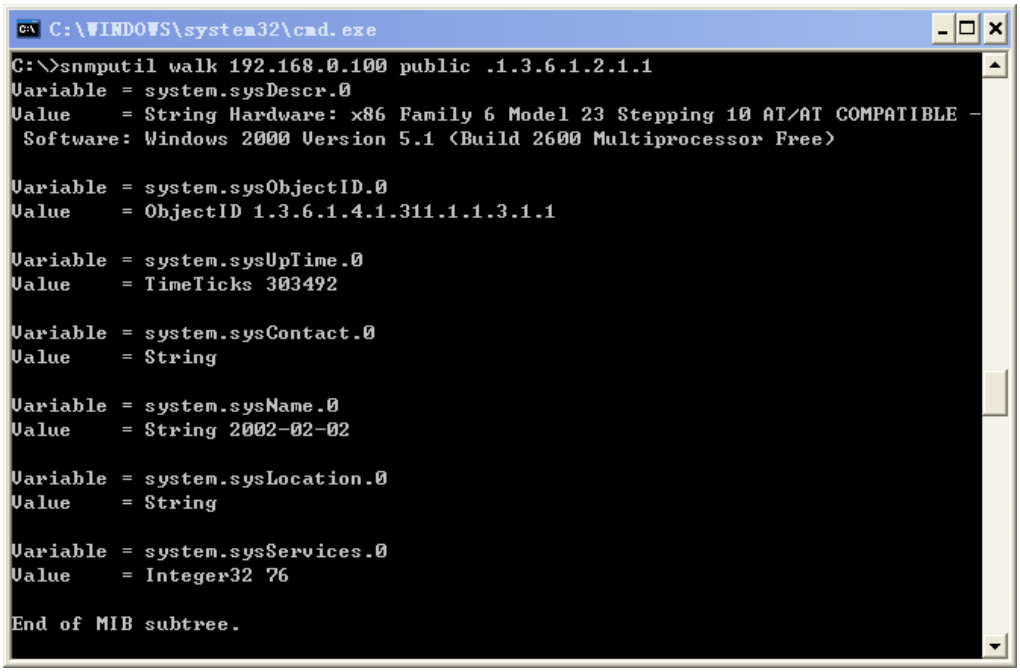

图 2-9 walk 命令遍历系统组

⑸用 walk 遍历整个 MIB-2 子树

Snmputil walk 192.168.0.100 public .1.3.6.1.2.1

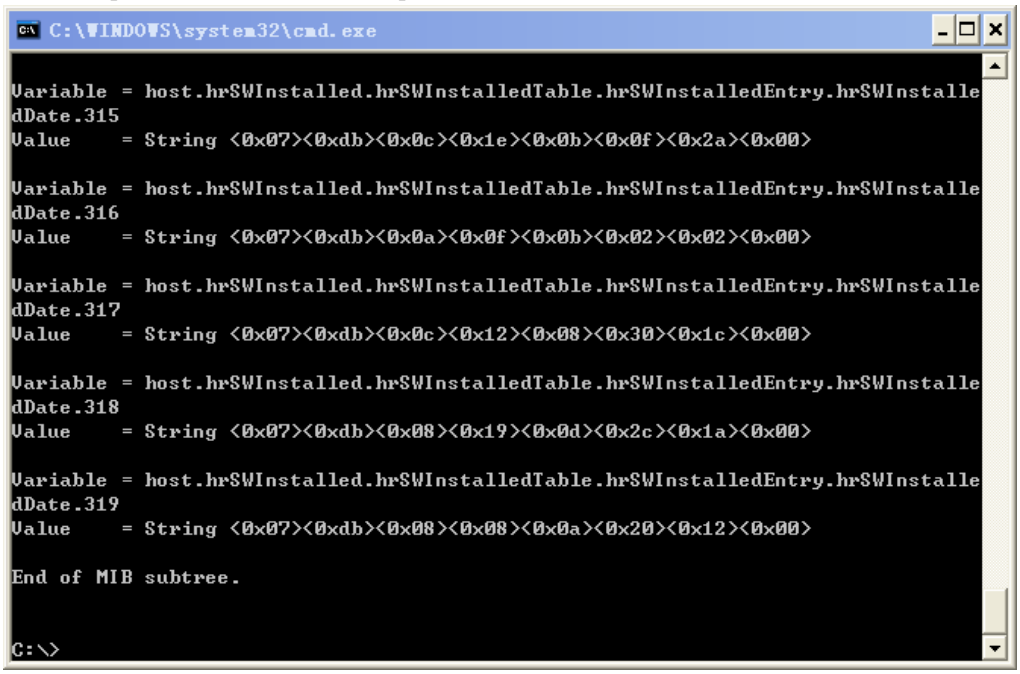

图 2-10 walk 命令遍历 MIB-2

⑹ 测试 SNMP 陷入服务

同时打开两个 DOS 窗口，其中一个启动监听陷入，另一个发送 SNMP 请求。

例如，第一个窗口启动监听陷入：snmputil trap；第二个窗口发送请求，使用一个无效的团体名(test)，snmputil getnext 192.168.0.100 test 1.1. ，由于团体名出错，所以认证出错，消息重发几次后，返回。

请求窗口：

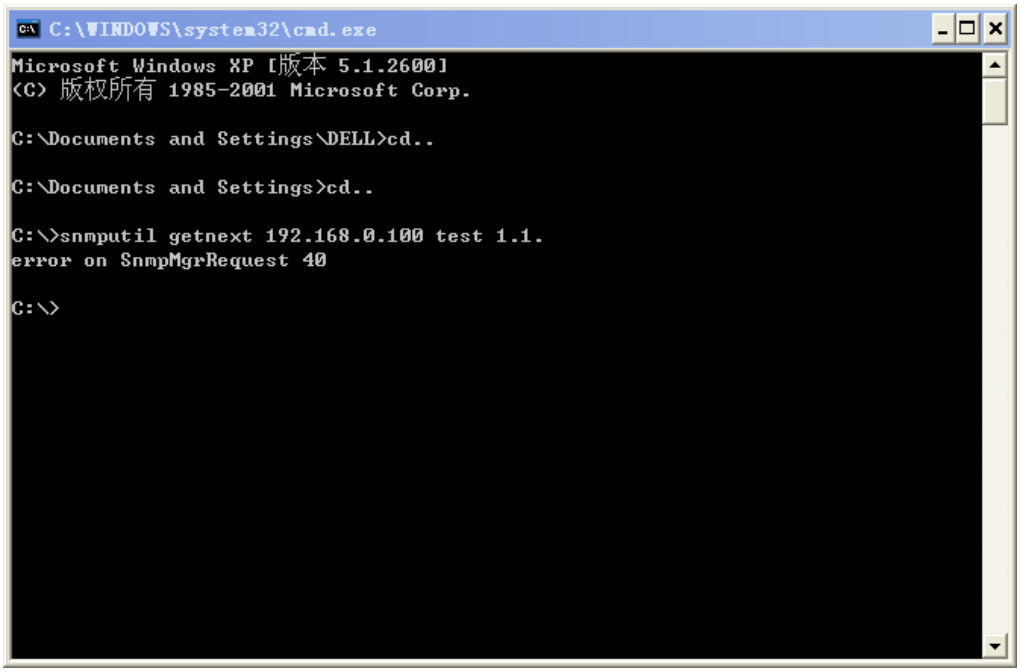

图 2-11 测试陷入服务请求窗口

监听窗口：

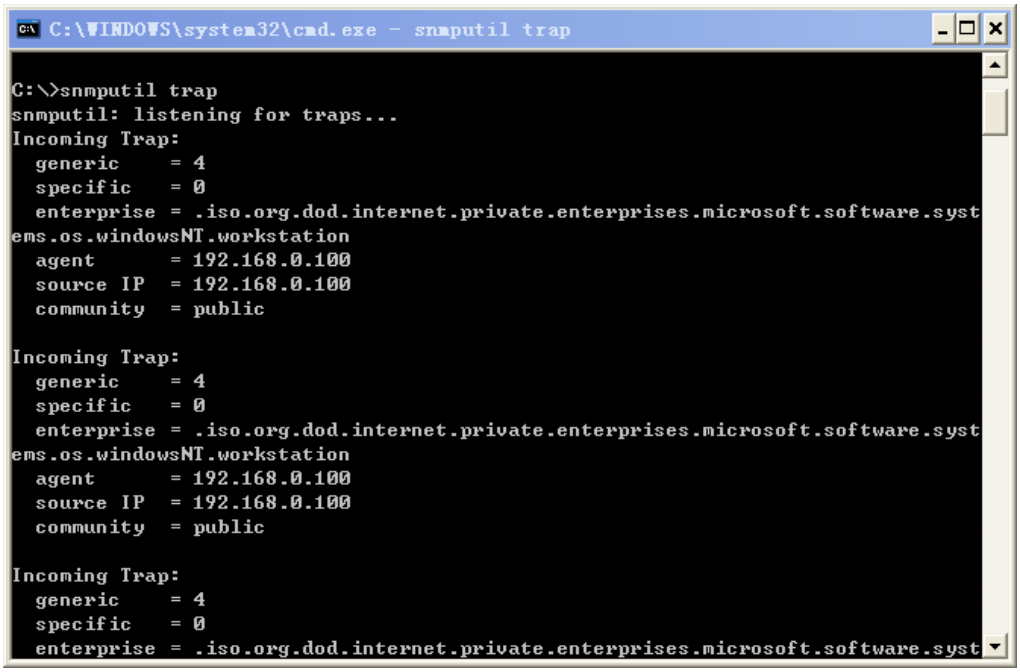

图 2-12 测试陷入服务监听窗口

⑺ 测试冷启动陷入

保持监听窗口继续监听陷入，然后停止 SNMP 服务，再重新启动 SNMP 服务，在陷入窗口会收到扩展代理发送的冷启动陷入。

Incoming trap:

Generic=0

Specific=0

Agent=192.168.0.100

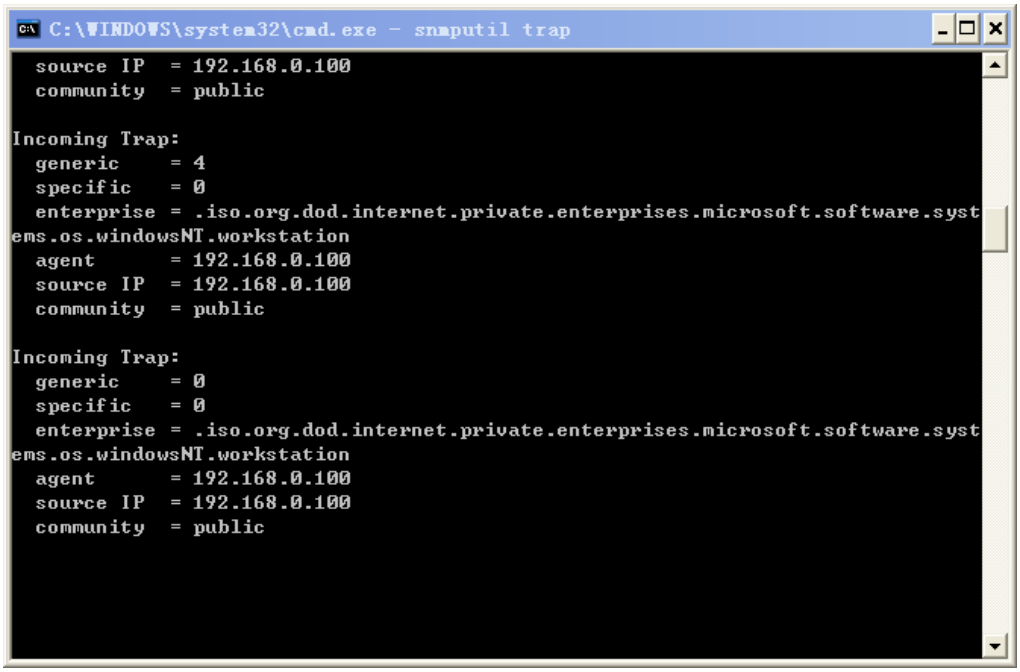

图 2-13 测试冷启动陷入

7 要求：

⑴ 依次访问 system 组的各个对象，写出访问命令及结果。

⑵ 使用 getnext 和 walk 命令分别访问对象 ipRouteTable，记录访问过程和结果。

2.6 思考题

⑴ snmputil 有几种访问 MIB 对象的方法？这些方法有什么不同？

⑵ Windows 下的 SNMP 服务配置有哪些是必须配的？有什么用途？

实验 3 SNMP MIB 信息的访问

3.1 实验目的

⑴ 掌握 SNMP 服务在主机上的启动与配置。

⑵ 掌握用 MIB 浏览器访问 SNMP MIB 对象的值，并通过直观的 MIB-2 树图加深对 MIB 被管对象的了解。

3.2 实验类型

验证型实验

3.3 实验环境

⑴ 运行 WIN2000/2003Server/XP 操作系统的 PC 一台；

⑵ 已安装 MG－SOFT MIB Browser 程序。

3.4 实验原理

管理信息数据库（MIB）是一个信息存储库，它包含了管理代理中有关配置和性能的数据包，有一个组织体系和公共结构，其中包含分属不同组的许多个数据对象。MIB 数据对象以一种树状分层结构进行组织，这个树状结构中的每个分校都有一个专用的名字和一个数字形式的标识符。使用这个树状分层结构，MIB 浏览器能够以一种方便而且简洁的方式访问整个交换机、路由器等，并支持 SNMP（简单网络管理协议）的 MIB 数据库。

MIB Browser 使用 IPv4、IPv6 或 IPX 网络上的标准 SNMPvl、SNMPv2 或 SNMPv3 协议，方便用户监视和管理任何支持标准 SNMPvl、SNMPv2 和 SNMPv3 协议的网络上的 SNMP 设备。例如，文件（file）或数据库服务器（Database Servers）、调制解调器（Modems）、打印机（Printers）、路由器（Routers）和交换机（Switches），等等。同时，通过标准的 SNMPv3 USM 安全模型（SNMPv3 USM security model），MIB Browser 还支持 Diffie－Hell－man 密钥交换模型（iffie-Hellman key exchange model），因此，可以无缝链接并管理基于 DOCSIS 的 SNMPv3 代理（DOCSIS－basedSNMPv3 agents）。例如，cable modem、cable modem 终端系统（termination systems）、机顶盒（set－top boxes）等。MIB Browser 允许用户执行 SNMP Get、SNMP GetNext、SNMP GetBulk 和 SNMP Set 操作。另外，用户还能够利用 MIB Browser

捕捉到由任何网络设备或网络上的应用发出的 SNMP Trap 和 SNMP Inform 包。MIB Browser 能够同时监视多个 SNMP 设备，并包括 SNMP 表格浏览器(SNMP Table viewer)。SNMP 表格编辑器、日志功能、对于查询数值的实时图形表达、扫描代理中使用的 MIB、SNMP 代理快照比较和管理远程 SNMP 代理上的 SNMP v3 USM 用户等特性。

通用的 SNMP Trace window 显示 MIB Browser 和 SNMP agents 间交换的 SNMP 消息。该信息既可以通过原始十六进制方式的 dump 格式显示，也可以通过经过解码的可读格式显示。因此，在开发 SNMP 代理或 SNMP 代理无法正确响应 MIB Browser 请求时，通用的 SNMP Trace window 特别有用。MIB Browser 还包括 MIB Compiler。MIB Compiler 能够编译任何供应商指定的 MIB 文件。编译好的 MIB 文件能够被装人到 MIB Browser。MIB Browser 能够下载并使用编译的 MIB 文件。MIB 文件通常由 SNMP 可管理的设备供应商提供，包含对 SNMP 设备的对象层次和对象属性的描述。换言之，MIB 文件为相应设备的管理提供路标。

常用的 SNMP MIB 浏览器有很多，这里主要介绍 MG－SOFT MIB Browser。

MG－SOFT MIB Browser Professional Edition 是一个极其方便的、功能强大的、用户界面友好的 SNMP Browser（SNMP 浏览器）。软件可以运行在 Microsoft Windows 之上，包括 Windows95／98／ME／NT／2000／XP 和 Windowsserver2003。该测览器还含有 Linux 版本。

3.5 实验内容与步骤

1 在本地主机上启动 SNMP 服务并配置共同体

控制面板－>管理工具－>服务，找到 SNMP service 和 SNMP trap service（若列表中不存在此服务，则用系统盘安装）并将其启动（右键列表中或双击打开的对话框中）；在 SNMP service 属性对话框中配置共同体（默认为 public）；

2 MG－SOFT MIB Browser Professional Edition 的安装及 GET 指令

⑴ 双击运行 MG－SOFT MIB Browser Professional Edition 的安装文件，启动其安装向导，进人安装界面，然后根据安装向导的引导完成安装。

注意：MG－SOFT MIB Browser Pro 的用户端和服务器端应该分别安装在两台计算机上。但如果条件不具备，也可以把它们同时安装在一台计算机上。

⑵ 确定已经安装了 SNMP 应用程序“MIB browser Professional for Windows”，并已启动，使用界面如图 2-1 所示。打开程序的路径为依次单击“开始”－“所有程序”－“MG－SOFT MIB Browser”－“MIB Browser”命令。

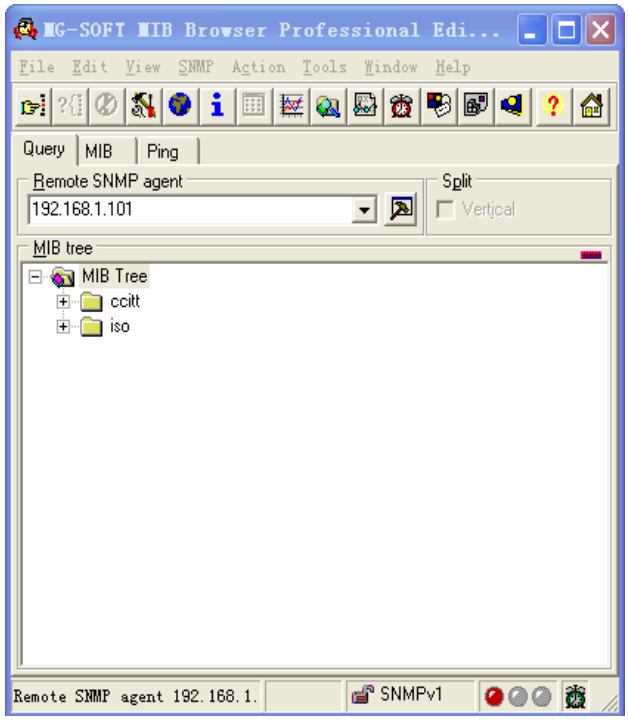

图 3-1 MIB browser Pro 界面

⑶ 在 host 框设置被监测主机的 IP 地址（默认为 localhost）、在 community 框设置被检测主机所配置的 SNMP 服务的共同体（如 public）；

⑷ 观察左侧结构面板中 MIB 树图结构；

⑸ 访问 MIB 对象。在左侧结构面板中选择要访问的 MIB 对象，单击使其凸显，然后用鼠标单击工具栏中的 get 按钮和 getNext 按钮（或菜单栏中 Operations 下的 Get 和 GetNext，或快捷键 Ctrl＋G 和 Ctrl＋N）。

⑹ 观察右侧面板中的显示信息。

3 要求：

⑴ 根据软件左侧 MIB 导航图画出 MIB-2 树图（到组），并画出 UDP 子树（到基本被管对象）。

⑵ 依次访问 system 组的各个对象，考察各个被管对象的物理意义，并写出被管对象 sysDescr 的值。

⑶ 访问对象 ipRouteTable，观察对象值，同时参照工具栏中的 SNMP data table（用此工具打开 SNMP table 窗口，点击 start 获得路由表信息）记录表中其中一行，分析 ipRouteDest、ipRouteNextHop 及 ipRouteType 的含义。

3.6 思考题

⑴ 有几类 MIB 对象？对它们的访问方法有什么不同？

实验 4 抽象语法记法 1（ASN.1）分析

4.1 实验目的

⑴ 理解 ASN.1 的编码规则。

⑵ 掌握 MIB 定义和编译的方法。

4.2 实验类型

设计型实验

4.3 实验环境

⑴ 运行 WIN2000/2003Server/XP 操作系统的 PC 一台；

⑵ 每台 PC 具有一块以太网卡，通过双绞线与局域网相连；

⑶ MG－SOFT MIB Browser 程序。

4.4 实验原理

OSI 定义抽象对象的方法称为 ASN.1(Abstract Syntax Notation One，X.208)，把这些对象转换成“0”和“1”的比特流的一套规则称为 BER(Basic Encoding Rules，X.209)。ASN.1 是一套灵活的记号，它允许定义多种数据类型，从 integer、bit string 一类的简单类型到结构化类型，如 set 和 sequence，还可以使用这些类型构建复杂类型。BER 说明了如何把每种 ASN.1 类型的值编码为 8bit 的 octet 流。通常每个值有不止一种的 BER 编码方法。一般使用另外一套编码规则 DER，它是 BER 的一个子集，对每个 ASN.1 值只有唯一一种编码方法。

4.5 实验内容与步骤

⑴ 确定已经安装了 SNMP 应用程序“MIB browser Professional for Windows”，并已启动，使用界面如图 4-1 所示。打开程序的路径为依次单击“开始”－“所有程序”－“MG－SOFT MIB Browser”－“MIB Browser”命令。

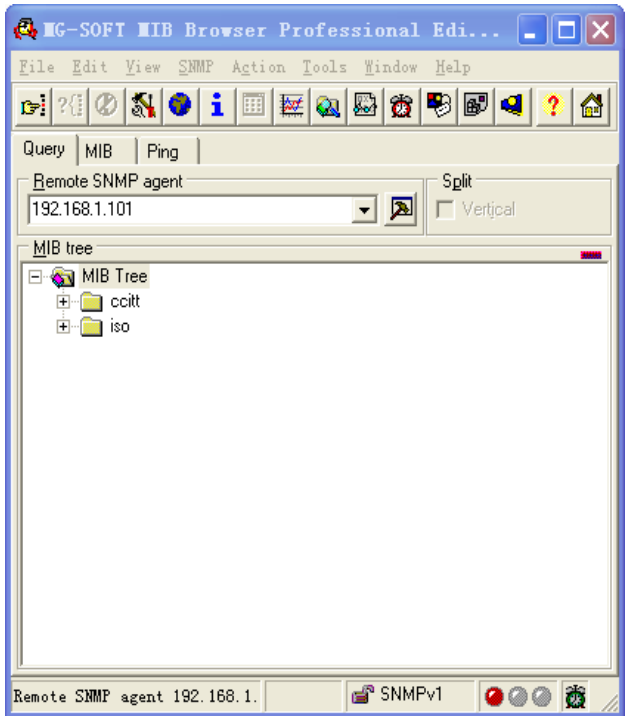

图 4-1 MIB browser Pro 界面

⑵ 启动 MIB Compiler，使用界面如图 4-2 所示。打开程序的路径为依次单击“Action”－“Run MIB Compiler”。

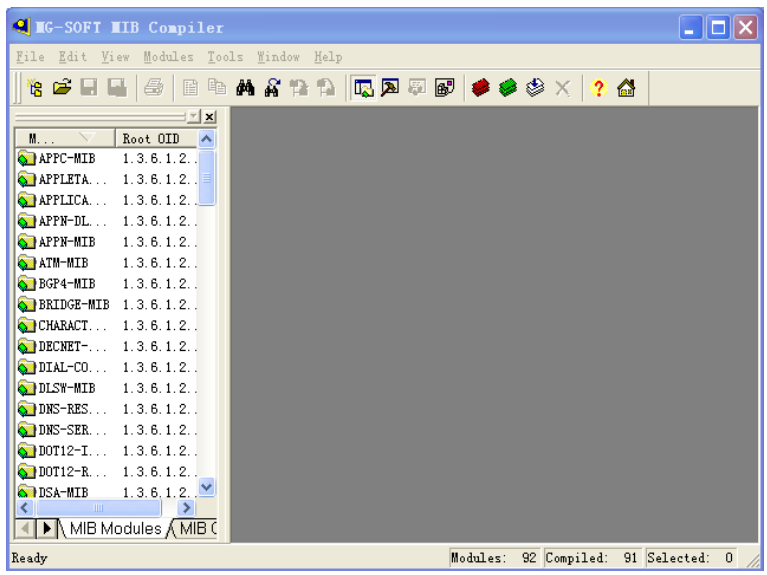

图 4-2 MIB Compiler

⑶ 在 Module 中选中 RFC1213-MIB，单击，查看右侧的 Module 信息。

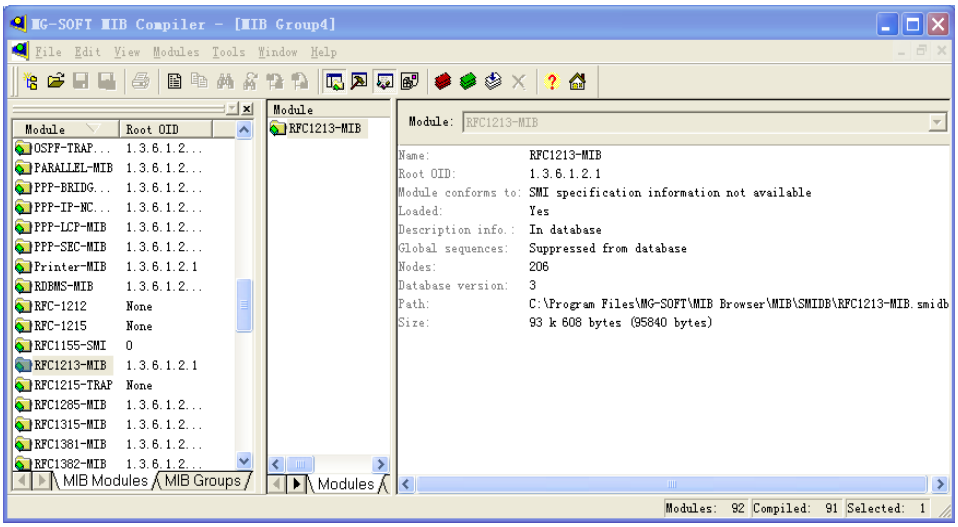

图 4-3 查看 Module 信息

⑷ 在 Module 中选中 RFC1213-MIB，单击右键，在下拉菜单中选择 Edit，右侧出现 RFC1213-MIB 的 ASN.1 源代码。查看 MIB2 中 system group 中所有项的定义方法。可参照 RFC1213。

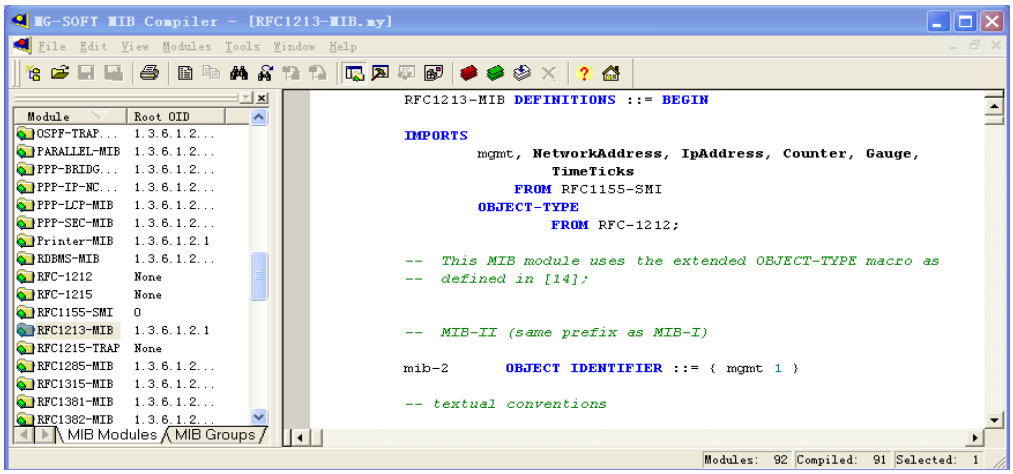

图 3-4 查看 ASN.1 源代码

⑸ 在 RFC1213-MIB 的 ASN.1 源代码中增加一个自定义 MIB，编译并查看。体会 ASN.1 的语法规则和 MIB 的定义方法。

4.6 思考题

⑴ 如果需要自定义一个新的变量类型应该怎么做？举例说明。

⑵ RFC1213 中的 MIB 包含哪些分组？

实验 5 SNMP 网管配置

5.1 实验目的

⑴ 掌握基于 H3C 交换机的 SNMP 协议的配置和管理方法；

⑵ 掌握 SNMP 网管软件的配置和使用方法。

5.2 实验类型

验证型实验

5.3 实验环境

1 组网需求

运行 WIN2000/2003Server/XP 操作系统的 PC 一台作为网络工作站（NMS）；网管工作站与 H3C 交换机 Switch A（SNMP Agent）通过以太网相连，网管工作站 IP 地址为 10.10.10.1，Switch A 的 VLAN 接口 IP 地址为 10.10.10.2。

2 组网图

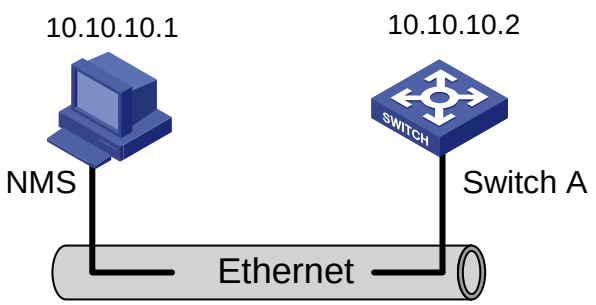

图 5-1 SNMP 配置组网图

5.4 实验原理

1 SNMP 简介

SNMP（Simple Network Management Protocol，简单网络管理协议），用于保证管理信息在网络中任意两点间传送，便于网络管理员在网络上的任何节点检索信息、修改信息、定位故障、完成故障诊断、进行容量规划和生成报告。

SNMP 采用轮询机制，提供最基本的功能集，特别适合在小型、快速和低价格的

环境中使用。SNMP 的实现基于无连接的传输层协议 UDP，因此可以实现和众多产品的无障碍连接。

2 SNMP 的工作机制

SNMP 分为 NMS 和 Agent 两部分：

- NMS（Network Management Station，网络管理站）是运行客户端程序的工作站，目前常用的网管平台有 QuidView、Sun NetManager 和 IBM NetView。
- Agent 是运行在网络设备（如交换机）上的服务器端软件。

NMS 可以向 Agent 发出 GetRequest、GetNextRequest 和 SetRequest 报文，Agent 接收到 NMS 的这些请求报文后，根据报文类型对管理对象（MIB，Management Information Base，管理信息库）进行 Read 或 Write 操作，生成 Response 报文，并将报文返回给 NMS。

Agent 在设备发生异常情况或状态改变时（如设备重新启动），也会主动向 NMS 发送 Trap 报文，向 NMS 汇报所发生的事件。

3 SNMP 的版本

目前，交换机中的 SNMP Agent 支持 SNMP v3 版本，兼容 SNMP v1 版本、SNMP v2c 版本。

SNMP v3 采用用户名和密码认证方式。

SNMP v1、SNMP v2c 采用团体名（Community Name）认证，非交换机认可团体名的 SNMP 报文将被丢弃。SNMP 团体名用来定义 SNMP NMS 和 SNMP Agent 的关系。团体名起到了类似于密码的作用，可以限制 SNMP NMS 访问交换机上的 SNMP Agent。用户可以选择指定以下一个或者多个与团体名相关的特性：

- 定义团体名可以访问的 MIB 视图。
- 设置团体名对 MIB 对象的访问权限为读写权限（write）或者只读权限（read）。具有只读权限的团体名只能对交换机信息进行查询，而具有读写权限的团体名还可以对交换机进行配置。
- 设置团体名指定的基本访问控制列表。

4 交换机支持的 MIB

在 SNMP 报文中用管理变量来描述交换机中的管理对象。为了唯一标识交换机中的管理对象，SNMP 用层次结构命名方案来识别管理对象。整个层次结构就像一棵树，树的节点表示管理对象，如下图 5-2 所示。每一个节点，都可以用从根开始的一条

路径唯一地标识。

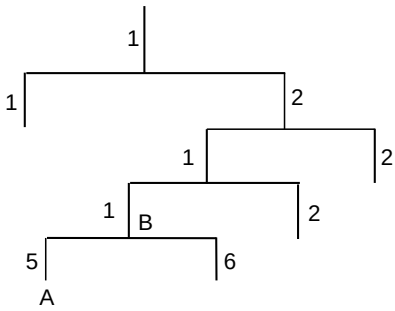

图 5-2 MIB 树结构

MIB（Management Information Base，管理信息库）的作用就是用来描述树的层次结构，它是所监控网络设备的标准变量定义的集合。在图 5-2 中，管理对象 B 可以用一串数字{1.2.1.1}唯一确定，这串数字是管理对象的对象标识符（Object Identifier，OID）。

交换机支持的常见 MIB 如下表 5-1 所示。

表 5-1 常见 MIB

MIB 属性	MIB 内容	参考资料
公有 MIB	基于 TCP/IP 网络设备的 MIB II	RFC1213
	BRIDGE MIB	RFC1493
		RFC2675
	RIP MIB	RFC1724
	RMON MIB	RFC2819
	以太网 MIB	RFC2665
	OSPF MIB	RFC1253
	IF MIB	RFC1573
私有 MIB	DHCP MIB	-
	QACL MIB	-
	MSTP MIB	-
	VLAN MIB	-
	IPV6 ADRDRESS MIB	-
	MIRRORGROUP MIB	-
	QINQ MIB	-

MIB 属性	MIB 内容	参考资料
	802.x MIB	-
	HGMP MIB	-
	NTP MIB	-
	设备管理	-
	接口管理	-

5 配置 SNMP 基本功能

SNMP v3 版本和 SNMP v1 版本、SNMP v2c 版本的配置有较大区别，在配置 SNMP 的基本功能时分为两种情况进行介绍。

SNMP 的具体配置见表 5-2、表 5-3。

表 5-2 配置 SNMP 基本功能（SNMP v1 版本、SNMP v2c 版本）

操作			命令	说明
进入系统视图			**system-view**	-
启动 SNMP Agent 服务			**snmp-agent**	可选 缺省情况下，SNMP Agent 服务处于关闭状态 执行此命令或执行 snmp-agent 的任何一条配置命令，都可以启动 SNMP Agent
设置系统信息，并设置交换机启用 SNMP v1/SNMP v2c 版本			**snmp-agent sys-info** { **contact** *sys-contact* | **location** *sys-location* | **version** { { **v1** | **v2c** | **v3** }* | **all** } }	必选 缺省情况下，系统维护联系信息为“R&D Hangzhou,H3C Technology Co.,Ltd.”；物理位置信息为“Hangzhou China”；版本为 SNMPv3
设置团体名及访问权限	直接设置	设置团体名	**snmp-agent community** { **read** | **write** } *community-name* [**acl** *acl-number* | **mib-view** *view-name*]*	必选 直接设置是以 SNMP v1 版本、SNMP v2c 版本的团体名概念进行设置 间接设置采用与 SNMP v3 版本一致的命令形式，添加的用户即相当于 SNMPv1 版本、SNMPv2c 版本的团体名概念 根据用户习惯，二者任选其一
	间接设置	设置一个 SNMP 组	**snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]	

操作			命令	说明
		为一个 SNMP 组添加一个新用户	**snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number*]	
设置 Agent 能接收/发送的 SNMP 消息包的大小			**snmp-agent packet max-size** *byte-count*	可选 缺省情况下，Agent 能接收/发送的 SNMP 消息包长度的最大值为 1500 字节
设置设备的引擎 ID			**snmp-agent local-engineid** *engineid*	可选 缺省情况下，设备引擎 ID 为公司的“企业号＋设备信息”
创建或更新视图的信息			**snmp-agent mib-view** { **included** | **excluded** } *view-name oid-tree* [**mask** *mask-value*]	可选 缺省情况下，视图名为 ViewDefault，OID 为 1

表 5-3 配置 SNMP 基本功能（SNMP v3 版本）

操作	命令	说明
进入系统视图	**system-view**	-
启动 SNMP Agent 服务	**snmp-agent**	可选 缺省情况下，SNMP Agent 服务处于关闭状态 执行此命令或执行 snmp-agent 的任何一条配置命令，都可以启动 SNMP Agent
设置系统信息,并设置交换机启用 SNMP v3 版本	**snmp-agent sys-info** { **contact** *sys-contact* | **location** *sys-location* | **version** { { **v1** | **v2c** | **v3** }* | **all** } }	必选 缺省情况下，系统维护联系信息为“R&D Hangzhou,H3C Technology Co.,Ltd.”； 物理位置信息为“Hangzhou China”； 版本为 SNMPv3
设置一个 SNMP 组	**snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]	必选

操作	命令	说明
计算明文密码的密文形式	**snmp-agent calculate-password** *plain-password* **mode** { **md5** | **sha** } { **local-engineid | specified-engineid** *engineid* }	可选 若添加新用户时，需要采用密文形式密码则需要计算出相应密码，并保存以便使用
为一个 SNMP 组添加一个新用户	**snmp-agent usm-user v3** *user-name group-name* [**cipher**] [**authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **des56** | **aes128** } *priv-password*]] [**acl** *acl-number*]	必选 S3100 系列以太网交换机中仅 S3100-SI 系列 Release 2106 版本及 S3100-EI 系列交换机支持参数 **aes128**。
设置 Agent 能接收/发送的 SNMP 消息包的大小	**snmp-agent packet max-size** *byte-count*	可选 缺省情况下，Agent 能接收/发送的 SNMP 消息包长度的最大值为 1500 字节
设置设备的引擎 ID	**snmp-agent local-engineid** *engineid*	可选 缺省情况下，设备引擎 ID 为公司的“企业号＋设备信息”
创建或更新视图的信息	**snmp-agent mib-view** { **included** | **excluded** } *view-name oid-tree* [**mask** *mask-value*]	可选 缺省情况下，视图名为 ViewDefault，OID 为 1

📖 **说明：**

S3100 以太网交换机为防止恶意用户对未使用 UDP 端口的攻击，提高交换机的安全性，提供了如下功能：

- 执行 **snmp-agent** 命令或执行 **snmp-agent** 的任何一条配置命令，都可以启动 SNMP Agent，同时打开 SNMP Agent 使用的 UDP 161 端口和 SNMP TRAP Client 使用的 UDP 1024 端口。
- 应用 **undo snmp-agent** 命令的同时即可关闭 UDP 161 端口和 UDP 1024 端口。

6 配置 Trap 基本功能

Trap 是被管理设备不经请求，主动向 NMS 发送的信息，用于报告一些紧急的重要事件（如被管理设备重新启动等）。

需要注意的是，在配置 Trap 基本功能前必须完成 SNMP 基本配置。

表 5-4 配置 Trap

操作		命令	说明
进入系统视图		**system-view**	-
配置允许向 NMS 发送交换机 Trap 信息		**snmp-agent trap enable** [**configuration** | **flash** | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]* | **system** |]	可选 缺省情况下，允许发送 Trap 报文
允许发送端口 Trap 信息	进入端口或者接口视图	**interface** *interface-type interface-number*	
	允许发送端口或者接口的 Trap	**enable snmp trap updown**	
	退回到系统视图	**quit**	
设置 Trap 目标主机地址		**snmp-agent target-host trap address udp-domain** { *ip-address* } [**udp-port** *port-number*] **params securityname** *security-string* [**v1** | **v2c** | **v3** {**authentication** | **privacy** }]	必选
设置发送 Trap 的源地址		**snmp-agent trap source** *interface-type interface-number*	可选
设置发往目的主机的 Trap 报文的消息队列的长度		**snmp-agent trap queue-size** *size*	可选 缺省情况下，发往目的主机的 Trap 报文消息队列长度为 100
设置 Trap 报文的老化时间		**snmp-agent trap life** *seconds*	可选 缺省情况下，Trap 报文的老化时间为 120 秒

📖 **说明：**

用户只需要在当前设备上使用 **display logbuffer** 命令，就可查看网管发送过来的 get 和 set 操作的日志信息。

7 SNMP 配置显示

在完成上述配置后，在任意视图下执行 display 命令，可显示配置后 SNMP 的运行情况，通过查看显示信息，来验证配置的效果。

表 5-5 SNMP 配置显示

配置	命令	说明
显示当前 SNMP 设备的系统信息	**display snmp-agent sys-info** [**contact** | **location** | **version**]*	**display** 命令可以在任意视图执行
显示 SNMP 报文统计信息	**display snmp-agent statistics**	
显示当前设备的引擎 ID	**display snmp-agent** { **local-engineid** | **remote-engineid** }	
显示设备的组信息	**display snmp-agent group** [*group-name*]	
显示 SNMP 用户信息	**display snmp-agent usm-user** [**engineid** *engineid* | **username** *user-name* | **group** *group-name*]	
显示 Trap 列表信息	**display snmp-agent trap-list**	
显示当前配置的团体名	**display snmp-agent community** [**read** | **write**]	
显示当前配置的 MIB 视图	**display snmp-agent mib-view** [**exclude** | **include** | **viewname** *view-name*]	

5.5 实验内容与步骤

1 先进行交换机的 SNMP 配置

启用 SNMP Agent 服务，并设置 SNMP v1、v2c 版本的团体名。

```
<H3C> system-view
[H3C] snmp-agent
[H3C] snmp-agent sys-info version all
[H3C] snmp-agent community read public
[H3C] snmp-agent community write private
```

设置 NMS 访问 SNMP Agent 的 MIB 访问权限。

```
[H3C] snmp-agent mib-view include internet 1.3.6.1
```

设置 SNMP v3 版本的群组和用户，安全级别为需要认证和加密，指定认证协议为 HMAC-MD5、认证密码为 passmd5，指定加密协议为 des、加密密码为 cfb128cfb128。

```
[H3C] snmp-agent group v3 managev3group privacy
write-view internet
[H3C] snmp-agent usm-user v3 managev3user
managev3group authentication-mode md5 passmd5
privacy-mode des56 cfb128cfb128
```

设置网管使用的 VLAN 接口为 VLAN 2 接口，将用于网管的端口 Ethernet1/0/2 加入到 VLAN2 中，配置 VLAN2 的接口 IP 地址 10.10.10.2。

```
[H3C] vlan 2
[H3C-vlan2] port Ethernet 1/0/2
[H3C-vlan2] quit
[H3C] management-vlan 2
[H3C] interface Vlan-interface 2
[H3C-Vlan-interface2]    ip    address    10.10.10.2
255.255.255.0
[H3C-Vlan-interface2] quit
```

允许交换机向网管工作站 10.10.10.1 发送 Trap 报文，使用的团体名为 public。

```
[H3C] snmp-agent trap enable standard authentication
[H3C] snmp-agent trap enable standard coldstart
[H3C] snmp-agent trap enable standard linkup
[H3C] snmp-agent trap enable standard linkdown
[H3C] snmp-agent target-host trap address udp-domain
10.10.10.1 udp-port 5000 params securityname public
```

2 配置 NMS

⑴ 安装 MG－SOFT MIB Browser Pro 软件。

⑵ 确定已经安装了 SNMP 应用程序“MIB browser Professional for Windows”，并已启动，使用界面如图 5-3 所示。打开程序的路径为依次单击“开始”－“所有程序”－“MG－SOFT MIB Browser”－“MIB Browser”命令。

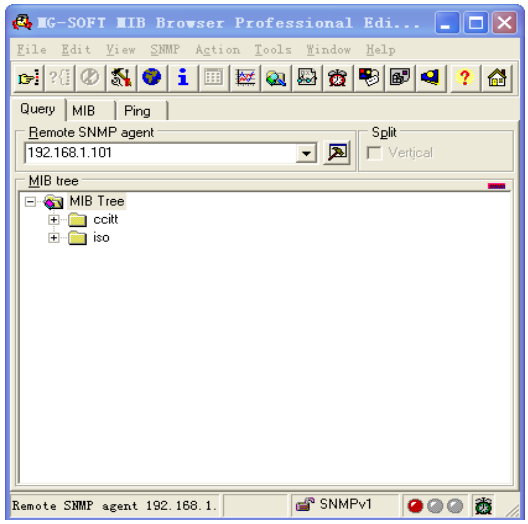

图 5-3 MIB Browser 启动界面

⑶ 设定“MIB Browser”。将 SNMP 服务器的 IP 地址输人“Remote SNMP agent”，并单击“Contact Remote SNMP agent”按钮。例如，在“Remote SNMP agent”文本框中输人 192.168.1.101，然后单击“Contact Remote SNMP agent”按钮  。在“Query results”栏目中，可以看到用户自己的 IP 地址发送出一个要求到 SNMP 服务器所在的 192.168.1.101。在传送要求后，用户会接收到一个由服务器回传的信息。

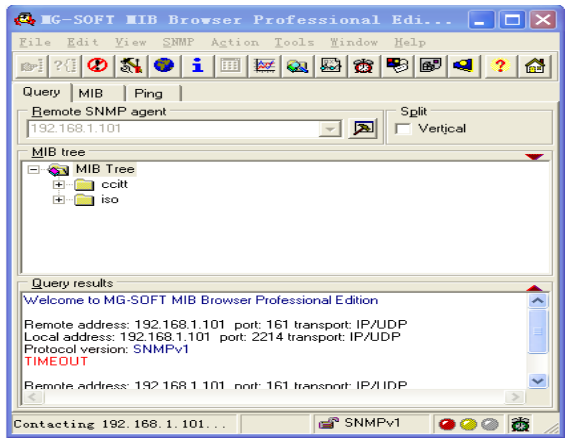

图 5-4 连接远程代理

⑷ 在安装好的 MIB Browser 中看到已经安装了三个 MIB 库 RFC1155-SMI、RFC1213－MIB 和 SNMPv2－TC 如图 5－5 所示。还可以在下面的 Module identity 中选择安装更多的 MIB 库。

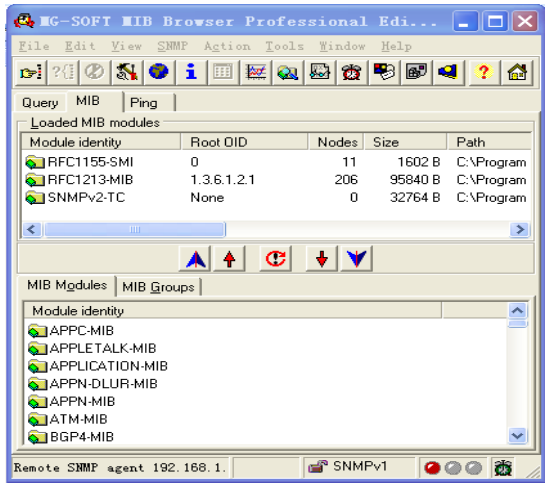

图 5-5 装载 MIB 库

⑸ 接下来将“MIB Tree”菜单里的 MIB 树依次展开，

-iso（国际标准化组织）1

-org（国际组织）3

-dod（美国国防部）6

-internet（互联网）1

-mgmt（管理组织机构）2

-mib2（管理信息库）1

得到 mib2 节点：1.3.6.1.2.1，查看节点 mib2 下的 8 个组：

-system（系统）1

-interface（接口）2

-at（地址翻译）3

-ip（IP 信息）4

-icmp（ICMP 信息）5

-tcp（TCP 信息）6

-udp（UDP 信息）7

-egp（外部网关协议信息）8

单击获取按钮在右侧信息框中会有相应的变量信息；然后找到要查询的节点——system（它的 OID 是 1. 3. 6. 1. 2. 1. 1）。点击 system 组节点；会列出该组节点下的 7 个变量；如图 5－6 所示。

- sysDescr ；系统的文字描述
- sysObjectID ；在子树 1.3.6.1.2.1.1.2 中的厂商标识
- sysUpTime ；从系统的网管部分启动以来运行的时间（百分之一秒为单位）
- sysContact ；联系人的名字及联系方式
- sysName ；节点的完全合格的名称
- sysLocation ；节点的物理位置
- sysServices ；指示节点提供的服务的值。

点击 sysName 变量，在右边的窗口出现该变量的值。

记录 system 组下的变量的对象标识都是多少？点击其他的组节点，查看相应的变量。

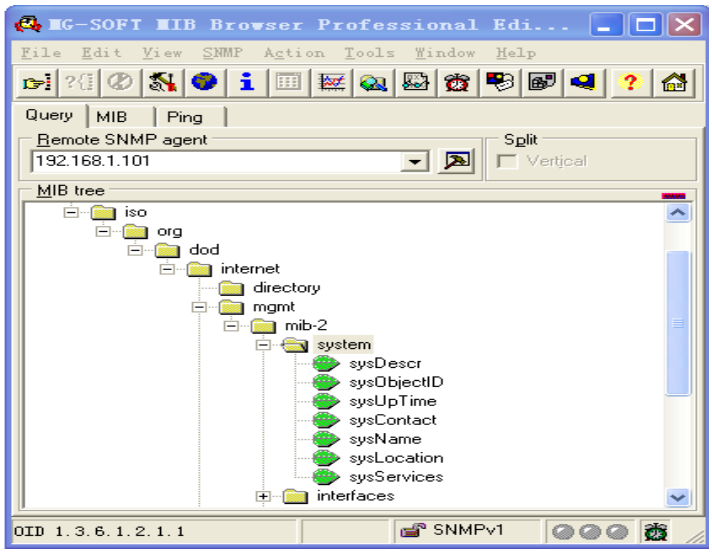

图 5-6 查询 system 节点

⑹ 在该节点—system，可以找到一个叫“sysName”的项目，选取该项目并单击鼠标右键打开快捷菜单，如图 5-7 所示。然后选择“Get”指令。

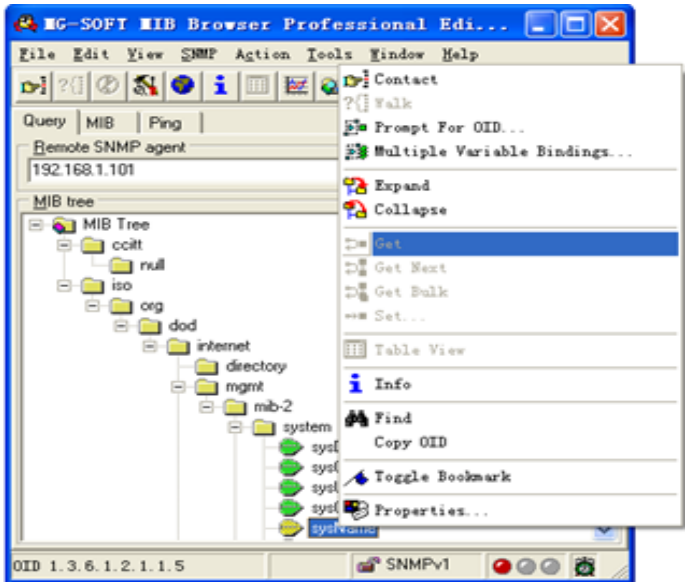

图 5-7 获得变量值

⑺ 用户可以从“Query result”窗口中看到结果。

举例 1：

OID 1.3.6.1.2.1.1.1.0 (sysDescr.0)

结果如下：

Request : Get .1.3.6.1.2.1.1.1.0

Creating Session..

Displaying results...

Oid : 1.3.6.1.2.1.1.1.0 (sysDescr.0)

value : Huawei Versatile Routing Platform Software

VRP(R) Software, Version 3.10(NSSA), RELEASE 5331SP01

Copyright (c) 2001-2004 HUAWEI TECH CO., LTD.

Quidway S8016

由此可以知道该设备是华为的路由设备。

举例 2：

OID：1.3.6.1.2.1.1.3.0 (sysUpTime.0)

结果如下：

Request : Get .1.3.6.1.2.1.1.3.0

Creating Session..

Displaying results...

Oid : 1.3.6.1.2.1.1.3.0 (sysUpTime.0)

value : 411 days 2:56:49

由此可以知道该设备自上一此重启后的使用时间。

首先使用 get next 获得一系列的 IpAdEntAddr 值，如下所示：

Oid : 1.3.6.1.2.1.4.20.1.1.127.0.0.1 (ipAdEntAddr.127.0.0.1)

value : 127.0.0.1

Oid : 1.3.6.1.2.1.4.20.1.1.172.20.60.30 (ipAdEntAddr.172.20.60.30)

value : 172.20.60.30

Oid : 1.3.6.1.2.1.4.20.1.1.172.20.60.62 (ipAdEntAddr.172.20.60.62)

value : 172.20.60.62

Oid : 1.3.6.1.2.1.4.20.1.1.172.20.60.94 (ipAdEntAddr.172.20.60.94)

value : 172.20.60.94

Oid : 1.3.6.1.2.1.4.20.1.1.172.20.60.126 (ipAdEntAddr.172.20.60.126)

value : 172.20.60.126

Oid : 1.3.6.1.2.1.4.20.1.1.172.20.60.158 (ipAdEntAddr.172.20.60.158)

value : 172.20.60.158

.....

而后选择一个感兴趣的 IP 地址，例如 172.20.60.158，查询其对应的 IpAdEntNetMask：

OID：Oid : 1.3.6.1.2.1.4.20.1.3.172.20.60.158

结果如下：

Request : Get .1.3.6.1.2.1.4.20.1.3.172.20.60.158

Creating Session..

Displaying results...

Oid : 1.3.6.1.2.1.4.20.1.3.172.20.60.158 (ipAdEntNetMask.172.20.60.158)

value : 255.255.255.224

可见其 mask 为 255.255.255.224

同时还可以查询其对应的 Interface 的 IfIndex，这可以通过查询 IpAdEntIfIndex 得到：

OID：Oid : 1.3.6.1.2.1.4.20.1.2.172.20.60.158

结果如下：

Request : Get .1.3.6.1.2.1.4.20.1.2.172.20.60.158

Creating Session..

Displaying results...

Oid : 1.3.6.1.2.1.4.20.1.2.172.20.60.158 (ipAdEntIfIndex.172.20.60.158)

value : 1799

知道了 IfIndex，可以在 Interfaces Group 里获取进一步的信息了，如获取接口描述：

Oid : 1.3.6.1.2.1.2.2.1.2.1799

结果如下：

Request : Get .1.3.6.1.2.1.2.2.1.2.1799

Creating Session..

Displaying results...

Oid : 1.3.6.1.2.1.2.2.1.2.1799 (ifDescr.1799)

value : Vlanif6

练习：使用“Get” 指令，取得拥有 SNMP 服务的设备上预设的 TTL 值（默认 TTL）。

📖 **说明：**

网管系统的认证参数配置必须和设备上保持一致，否则网管系统无法管理设备。

5.6 思考题

⑴ 常用的 SNMP MIB 浏览器有哪些？请下载一款使用。

⑵ 使用哪个命令可以一次取得多个 SNMP MIB 值？

实验 6 SNMP 协议工作原理验证与分析

6.1 实验目的

⑴ 通过捕获 SNMP 数据包，学习 SNMP 协议的格式；

⑵ 理解 SNMP 协议的工作原理；

⑶ 理解 SNMP 协议的作用。

6.2 实验类型

验证型实验

6.3 实验环境

1 组网需求

运行 WIN2000/2003Server/XP 操作系统的 PC 一台作为网络工作站（NMS）；网管工作站与 H3C 交换机 Switch A（SNMP Agent）通过以太网相连，网管工作站 IP 地址为 10.10.10.1，Switch A 的 VLAN 接口 IP 地址为 10.10.10.2。

2 组网图

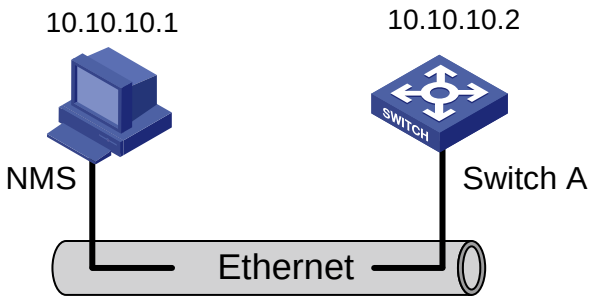

图 6-1 SNMP 配置组网图

6.4 实验原理

SNMP 是用于网络管理站与被管设备的网管代理之间交互管理信息的协议。管理信息的结构使用一种概念树。树叶表示各种对象，帮助用户了解互连网络的结构。网络管理站通过 SNMP 协议向被管设备的网管代理发出各种请求报文，网管代理则接收这些请求后完成相应的操作。SNMP 为应用层协议，是 TCP/IP 协议簇的一部分，它是通过 UDP 用户数据报协议来操作的。

网络管理员对网络及其设备的管理有三种方式：本地终端方式、远程 Telnet 命令方式和基于 SNMP 的代理/服务器方式。

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。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。请注意，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。

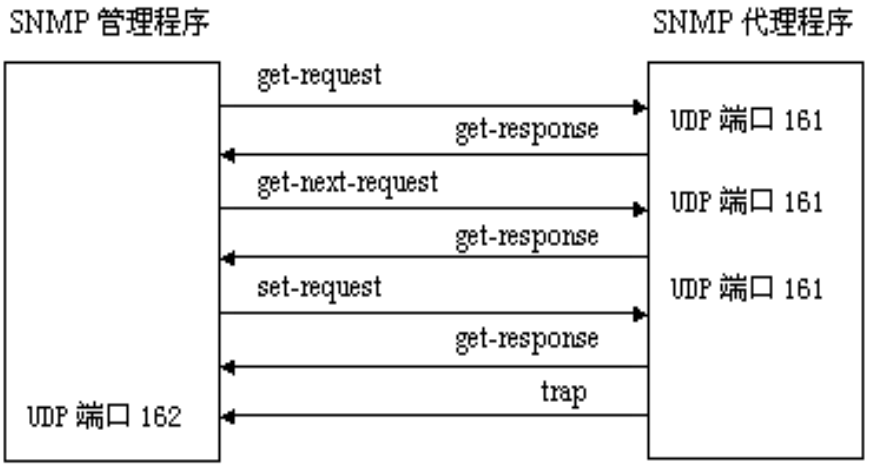

图 6-2 SNMP 的 5 种报文操作

图 6-3 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。

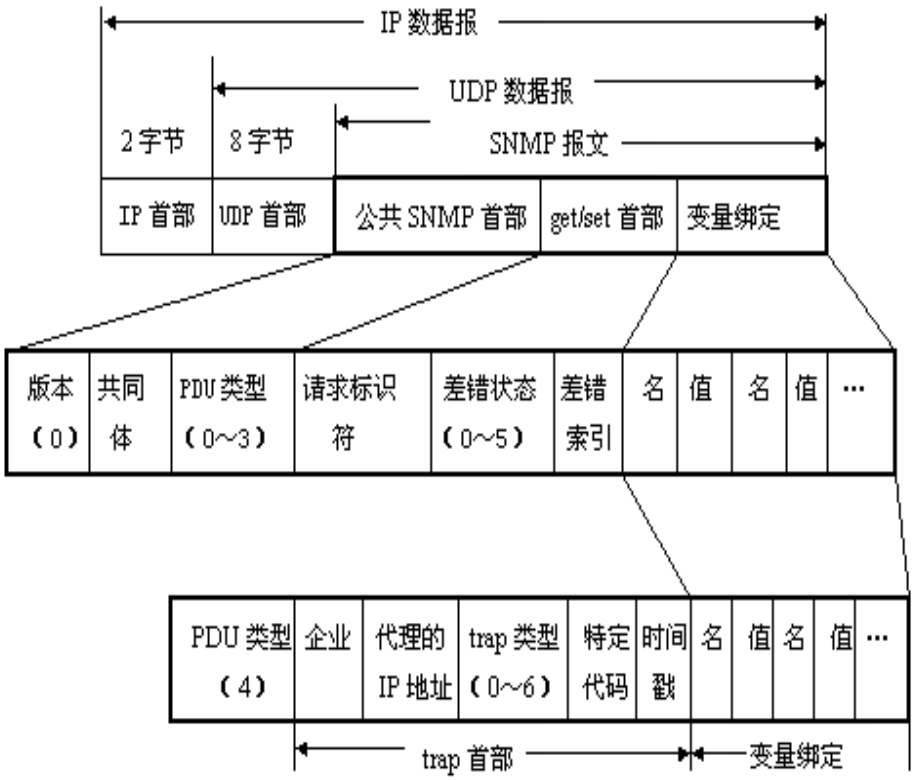

图 6-3 SNMP 报文格式

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 5-1 所示意图。

表 6-1 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 6-2 的描述。

表 6-2 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。此对象标识符是在对象命名树上的 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 5－3 中的 7 种。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。

表 6-3 trap 类型

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

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。

6.5 实验内容与步骤

⑴ 安装网络协议分析仪 Ethereal 和 MG－SOFT MIB Browser Pro。

⑵ 启动并配置 H3C 交换机，启动并配置 MIB browser，使其能执行 Trap 功能。（具体细节见实验四）

⑶ 使用 Ethereal 分析协议捕获数据包

① 启动系统。点击“Ethereal 程序组的图标”将出现如图 6-4 操作界面。

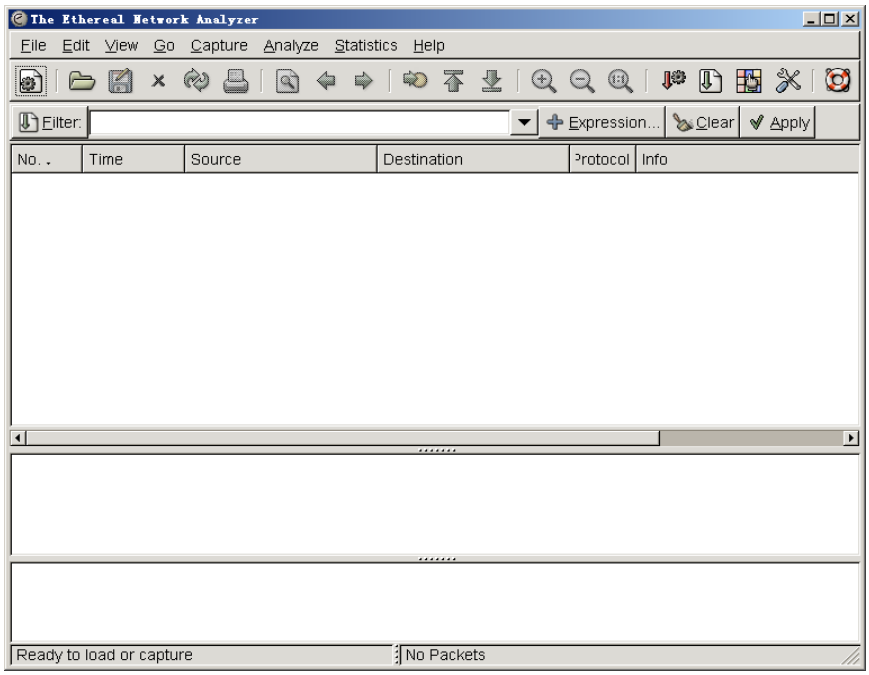

图 6-4 Ethereal 操作界面

② 分组俘获。打开“Capture/Option”菜单，出现如图 6-5 的界面。在“Interface”接口框的下拉列表中选择一个适当的接口项，以及过滤器项。

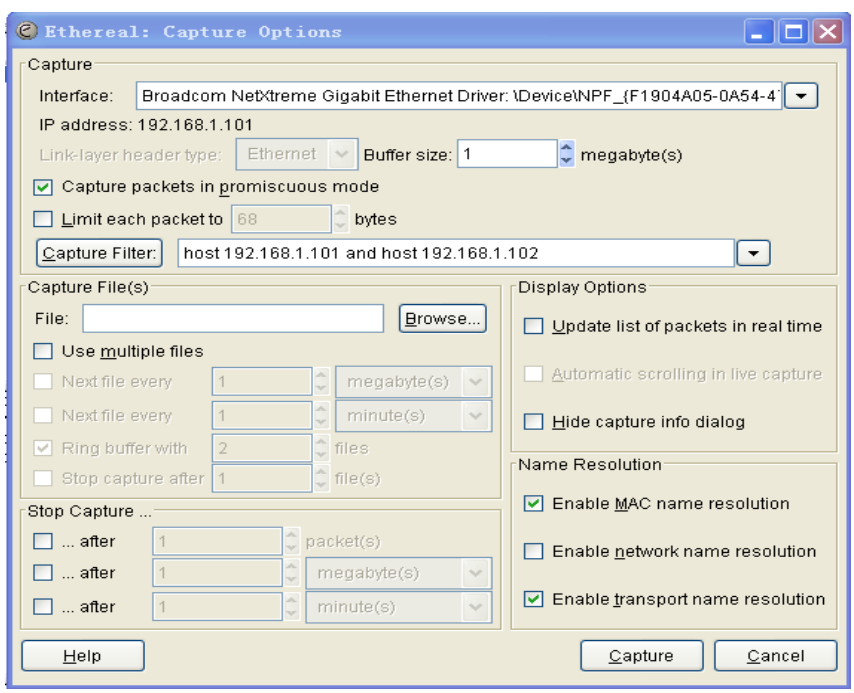

图 6-5　Capture 选项界面

设置 Capture Filter，如图 6-6 所示。

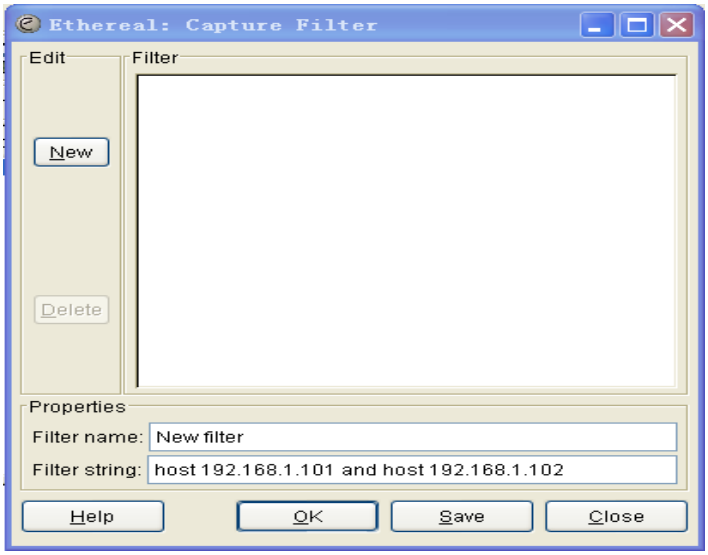

图 6-6 设置过滤器

点击“Captrue”按钮，开始捕获数据。

③ 在 MIB Browser 中执行多个“Get”指令，如图 6-7 所示。

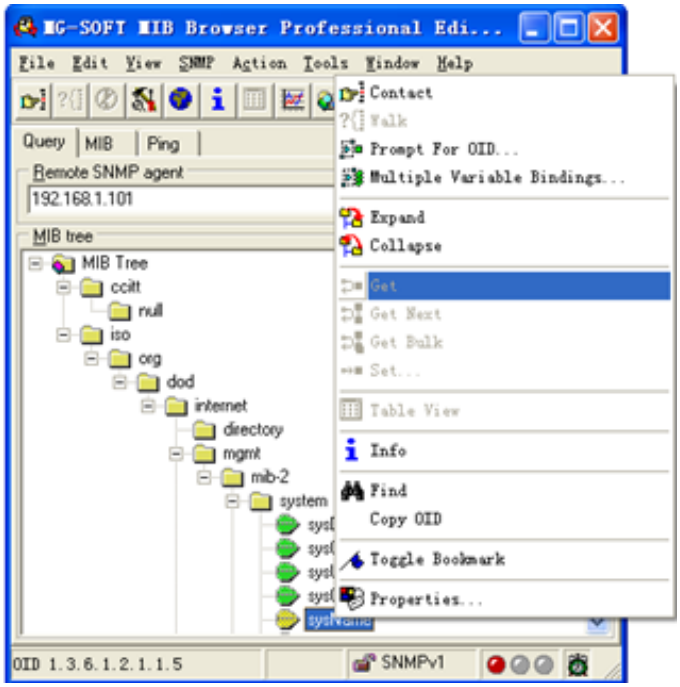

图 6-7 执行 get 命令

④ 根据需要俘获相应的数据包后，可以按“STOP”，出现如图 6-8 所示。

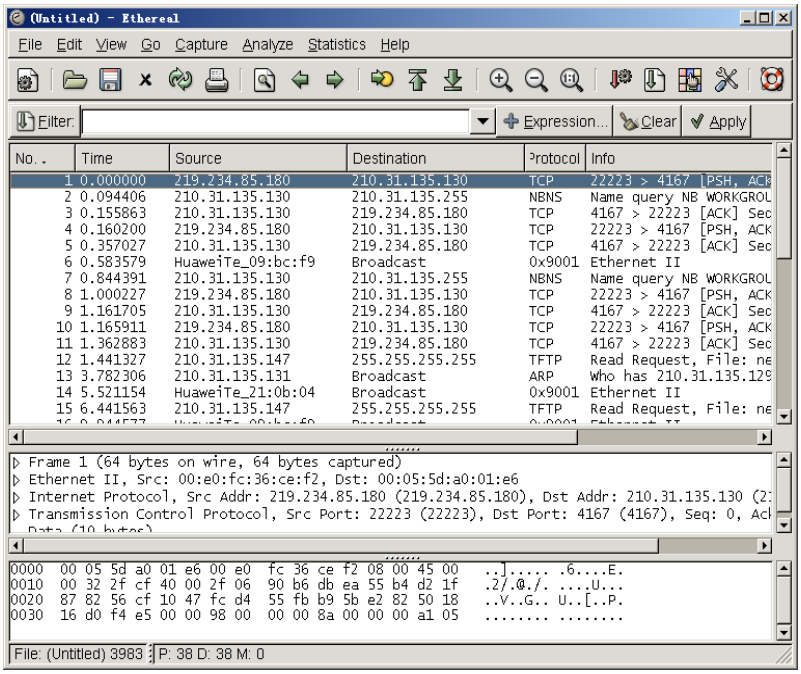

图 6-8 俘获的数据包

⑤ 分组分析。打开“Analyze/Display Filters”菜单，出现如下图的界面。

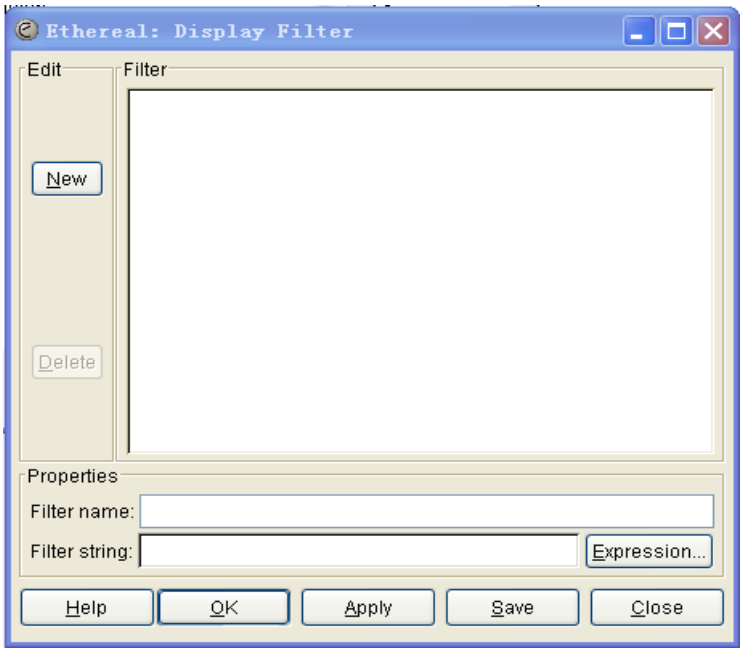

图 6-9 显示过滤器

在点选图 6-9 中的 Expression...的按钮，会出现下图，这是一个封包搜寻器辅助工具，也就是可以辅助我们输入正确的关建字。

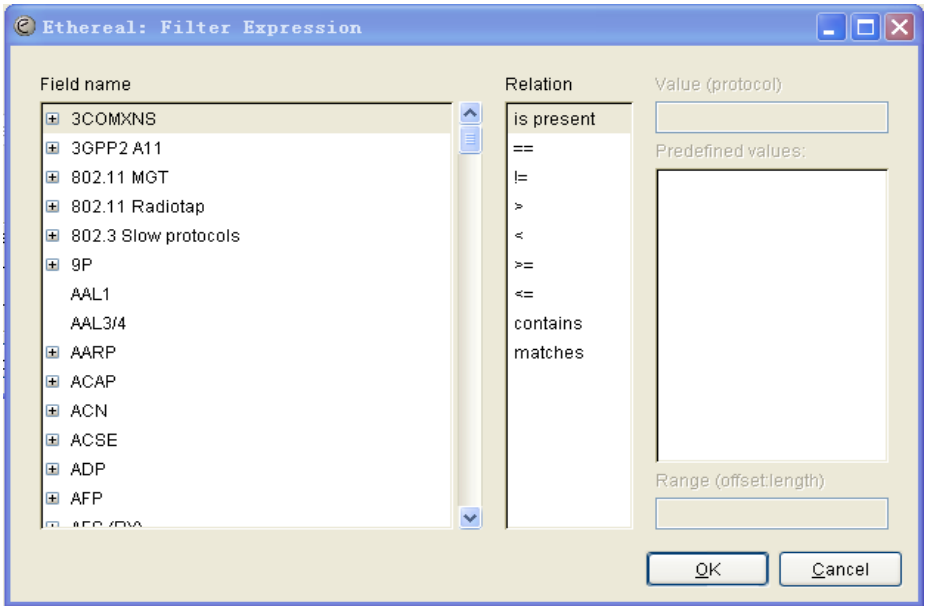

图 6-10 显示过滤器的设置(一)

在左边选出我们要的协定或关键的字串，这里选择比较 SNMP 协议包的版本号，如图 6-11 所示。

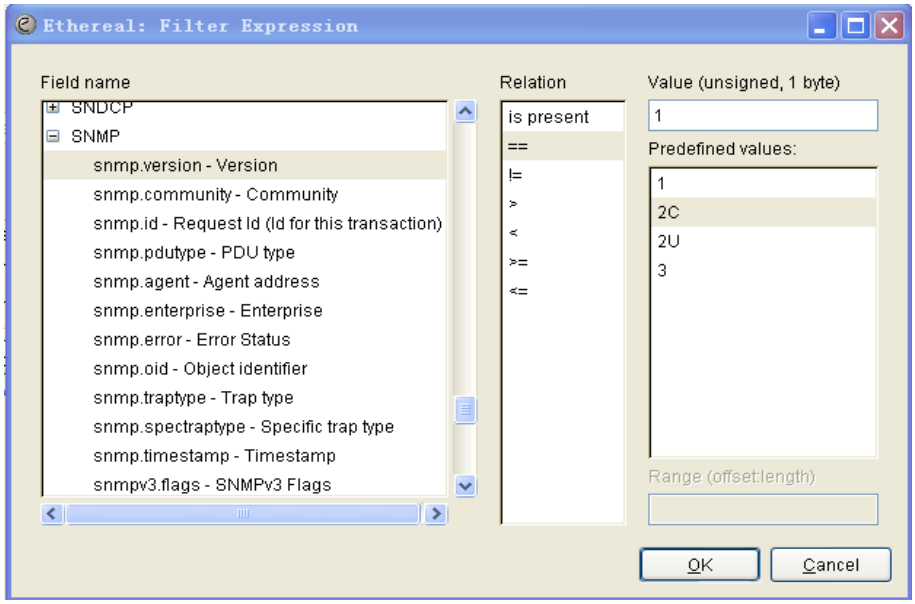

图 6-11 显示过滤器的设置(二)

如果设置好后 Filter 的背景是绿色，则该设置是有效的，否则设定的 Filter 是不合法的。设置合法后点击“apply”，就可以找到这一次所收集的版本号为 1 的 SNMP 包。

⑷ 协议包分析

① 将捕获到的数据包按照 SNMP 包格式进行分析。

② 注意体会 SNMP 协议的工作流程。

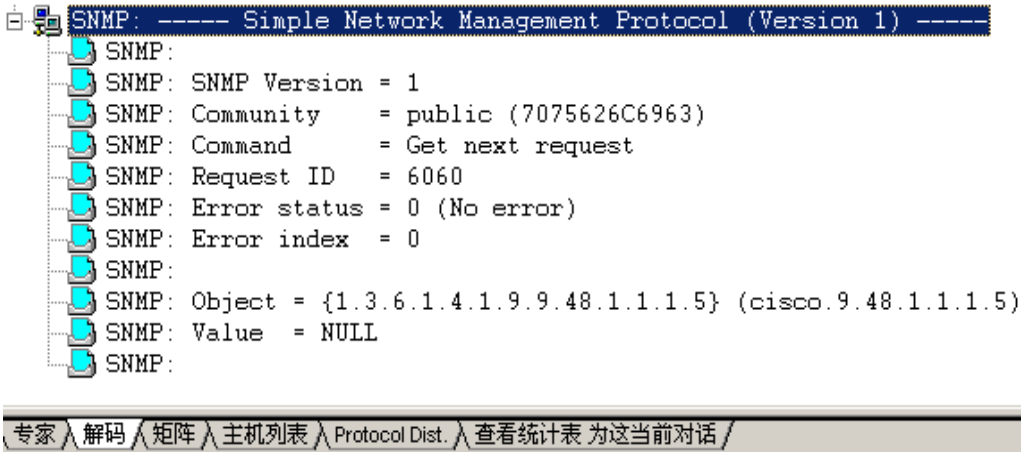

图 6-12 SNMP 协议数据包解析

6.6 思考题

① SNMP 和 SMTP 协议都采用客户/服务器工作方式，其中谁是客户，谁是服务器？

② 为什么 SNMP 的管理进程使用探询（request）掌握全网状态属于正常情况，而代理进程使用陷阱（trap）向管理进程报告属于较少发生的异常情况？

附录：实验指导材料

用 Ethereal 分析协议数据包

Ethereal 是一个图形用户接口（GUI）的网络嗅探器，能够完成与 Tcpdump 相同的功能,但操作界面要友好很多。Ehtereal 和 Tcpdump 都依赖于 pcap 库(libpcap)，因此两者在许多方面非常相似（如都使用相同的过滤规则和关键字）。Ethereal 和其它图形化的网络嗅探器都使用相同的界面模式，如果能熟练地使用 Ethereal，那么其它图形用户界面的嗅探器基本都可以操作。

1 设置 Ethereal 的过滤规则

当编译并安装好 Ethereal 后，就可以执行“ethereal”命令来启动 Ethereal。在用 Ethereal 截获数据包之前，应该为其设置相应的过滤规则，可以只捕获感兴趣的数据包。Ethereal 使用与 Tcpdump 相似的过滤规则，并且可以很方便地存储已经设置好的过滤规则。

2 tcpdump 的表达式介绍

tcpdump 的表达式就是前面提到的 Ethereal 过滤规则。表达式是一个正则表达式，tcpdump 利用它作为过滤报文的条件，如果一个报文满足表达式的条件，则这个报文将会被捕获。如果没有给出任何条件，则网络上所有的信息包将会被截获。

在表达式中一般如下几种类型的关键字，一种是关于类型的关键字，主要包括 host，net，port，例如 host 210.27.48.2，指明 210.27.48.2 是一台主机，net 202.0.0.0 指明 202.0.0.0 是一个网络地址，port 23 指明端口号是 23。如果没有指定类型，缺省的类型是 host.

第二种是确定传输方向的关键字，主要包括 src , dst ,dst or src, dst and src，这些关键字指明了传输的方向。举例说明，src 210.27.48.2，指明 ip 包中源地址是 210.27.48.2，dst net 202.0.0.0 指明目的网络地址是 202.0.0.0。如果没有指明方向关键字，则缺省是 src or dst 关键字。

第三种是协议的关键字，主要包括：**ether**, **fddi**, **tr**, **ip**, **ip6**, **arp**, **rarp**, **decnet**, **tcp, udp**。Fddi 指明是在 FDDI(分布式光纤数据接口网络)上的特定的网络协议，实际上它是“ether”的别名，fddi 和 ether 具有类似的源地址和目的地址，所以可以将 fddi 协议包当作 ether 的包进行处理和分析。

其他的几个关键字就是指明了监听的包的协议内容。如果没有指定任何协议，则 tcpdump 将会监听所有协议的信息包。

除了这三种类型的关键字之外，其他重要的关键字如下：gateway, broadcast, less, greater,还有三种逻辑运算，取非运算是 'not' '!', 与运算是'and','&&'；或运算是'or' ,'||'；这些关键字可以组合起来构成强大的组合条件来满足人们的需要，下面举几个例子来：

① 想要截获所有 210.27.48.1 的主机收到的和发出的所有的数据包：

```
#tcpdump host 210.27.48.1
```

② 想要截获主机 210.27.48.1 和主机 210.27.48.2 或 210.27.48.3 的通信，使用命令：（在命令行中适用括号时，一定要：

#tcpdump host 210.27.48.1 and \ (210.27.48.2 or 210.27.48.3 \)

③ 如果想要获取主机210.27.48.1除了和主机210.27.48.2之外所有主机通信的ip包，使用命令：

ip host 210.27.48.1 and ! 210.27.48.2

④ 如果想要获取主机210.27.48.1接收或发出的telnet包，使用如下命令：

tcp port 23 host 210.27.48.1

3 过滤规则实例

- 捕捉主机10.14.26.53和www服务器www.zju.edu.cn之间的通信(这里主机 10.14.26.53 可以是自身，也可以是通过普通 HUB（而不是交换机）与本机相连的LAN上的其它主机或路由器,下同),Ethereal的capture filter 的filter string设置为：

host 10.14.26.53 and www.zju.edu.cn

- 捕捉局域网上的所有ARP包,Ethereal的capture filter 的filter string设置为：

arp

- 捕捉局域网上主机 10.14.26.53 发出或接受的所有 ARP 包，Ethereal 的capture filter的filter string设置为：arp host 10.14.26.53

或者等价地设置为：arp and host 10.12.105.27

- 捕捉局域网上主机10.14.26.53发出或接受的所有POP包（即src or dst port＝110），Ethereal的capture filter的filter string设置为：

tcp port 110 and host 10.14.26.53

或者等价地设置为：tcp and port 110 and host 10.14.26.53

- 捕捉局域网上主机10.14.26.53发出或接受的所有FTP包（即src or dst port＝21），Ethereal的capture filter 的filter string设置为：

tcp port 21 and host 10.14.26.53

① 在主机10.14.26.53上用FTP客户端软件访问FTP server。

② 观察并分析 10.14.26.53 和 FTP server 之间传输的 Ethernet II(即 DIX Ethernet v2)帧结构，IP数据报结构，TCP segment结构。

③ 观察并分析FTP PDU名称和结构。注意10.14.26.53发出的FTP request PDU中以USER开头、以PASS开头的两个PDU,他们包含了什么信息？对INTERNET的FTP

协议的安全性作出评价。

- 捕捉局域网上的所有 icmp 包，Ethereal 的 capture filter 的 filter string 设置为：icmp
- 捕捉局域网上的所有 ethernet broadcast 帧，Ethereal 的 capture filter 的 filter string 设置为：ether broadcast
- 捕捉局域网上的所有 IP 广播包，Ethereal 的 capture filter 的 filter string 设置为：ip broadcast
- 捕捉局域网上的所有 ethernet multicast 帧，Ethereal 的 capture filter 的 filter string 设置为：ether multicast
- 捕捉局域网上的所有 IP 广播包，Ethereal 的 capture filter 的 filter string 设置为： ip multicast
- 捕捉局域网上的所有 ethernet multicast 或 broadcast 帧，Ethereal 的 capture filter 的 filter string 设置为：ether[0] & 1 != 0
- 要以 MAC address 00:00:11:11:22:22 为抓封包条件，Filter string 设置为：ether host 00:00:11:11:22:22

实验 7 RMON 原理和配置

7.1 实验目的

① 了解 RMON 协议的工作机制；

② 掌握基于 H3C 交换机的 RMON 协议的配置和管理方法。

7.2 实验类型

验证型实验

7.3 实验环境

1 组网需求

运行 WIN2000/2003Server/XP 操作系统的 PC 一台作为网络工作站（NMS）；网管工作站与 H3C 交换机 Switch A（SNMP Agent）通过以太网相连，网管工作站 IP 地址为 10.10.10.1，Switch A 的 VLAN 接口 IP 地址为 10.10.10.2。

2 组网图

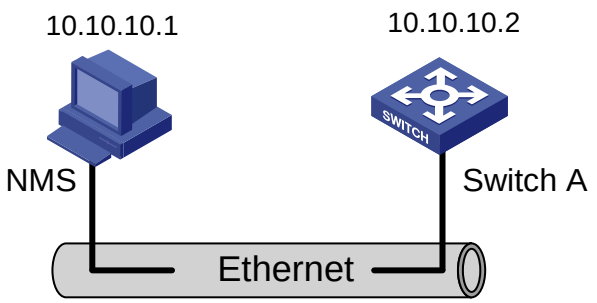

图 7-1 SNMP 配置组网图

7.4 实验原理

1 RMON 简介

RMON（Remote Monitoring，远程网络监视）是 IETF（Internet Engineering Task Force，Internet 工程任务组）定义的一种 MIB（Management Information Base，管理信息库），是对 MIB II 标准重要的增强。RMON 主要用于对一个网段乃至整个网络中数据流量的监视，是目前应用相当广泛的网络管理标准之一。

RMON 包括 NMS（Network Management Station，网络管理站）和运行在各网络

设备上的 Agent 两部分。RMON Agent 运行在网络监视器或网络探测器上，跟踪统计其端口所连接的网段上的各种流量信息（如某段时间内某网段上的报文总数，或发往某台主机的正确报文总数等）。

- RMON 的实现完全基于 SNMP 体系结构，它与现存的 SNMP 框架相兼容。
- RMON 使 SNMP 更有效、更积极主动地监测远程网络设备，为监控子网的运行提供了一种高效的手段。
- RMON 能够减少 NMS 与代理（SNMP Agent）间的通讯流量，从而可以简便而有效地管理大型互连网络。

2 RMON 工作机制

RMON 允许有多个监控者，它可用两种方法收集数据：

- 利用专用的 RMON probe（探测仪）收集数据，NMS 直接从 RMON probe 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；
- 将 RMON Agent 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。RMON NMS 使用 SNMP 的基本命令与 SNMP Agent 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。这四个组是告警组、事件组、历史组和统计组。

H3C 系列以太网交换机以第二种方法实现 RMON。以太网交换机里直接植入 RMON Agent，成为带 RMON probe 功能的网络设施。通过运行在以太网交换机上支持 RMON 的 SNMP Agent，网管站可以获得与以太网交换机端口相连的网段上的整体流量、错误统计和性能统计等信息，实现对网络的管理。

3 几个常用的 RMON 组

⑴ 事件组

事件组用来定义事件号及事件的处理方式。事件组定义的事件主要用在告警组配置项和扩展告警组配置项中告警触发产生的事件。

事件有如下几种处理方式：

① 将事件记录在日志表中；

② 向网管站发 Trap 消息；

③ 将事件记录在日志表中并向网管站发 Trap 消息；

④ 不作任何处理。

⑵ 告警组

RMON 告警管理可对指定的告警变量（如端口的统计数据）进行监视，当被监视数据的值在相应的方向上越过定义的阈值时会产生告警事件，然后按照事件定义的处理方式进行相应的处理。事件的定义在事件组中实现。

用户定义了告警表项后，系统对告警表项的处理如下：

① 对所定义的告警变量 alarm-variable 按照定义的时间间隔 sampling-time 进行采样；

② 将采样值和设定的阈值进行比较，一旦超过该阈值，即触发相应事件。

⑶ 扩展告警组

扩展告警表项可以对告警变量的采样值进行运算，然后将运算结果和设置的阈值比较，实现更为丰富的告警功能。

用户定义了扩展告警表项后，系统对扩展告警表项的处理如下：

① 对定义的扩展告警公式中的告警变量按照定义的时间间隔进行采样；

② 将采样值按照定义的运算公式进行计算；

③ 将计算结果和与设定的阈值进行比较，一旦超过该阈值，即触发相应事件。

⑷ 历史组

配置了 RMON 历史组以后，以太网交换机会周期性地收集网络统计信息，为了便于处理，这些统计信息被暂时存储起来，提供有关网段流量、错误包、广播包、带宽利用率等统计信息的历史数据。

利用历史数据管理功能，可以对设备进行设置。设置的任务包括：采集历史数据、定期采集并保存指定端口的数据。

⑸ 统计组

统计组信息反映交换机上每个监控接口的统计值。统计组统计的是从该统计组创建的时间开始的累计信息。

统计信息包括网络冲突数、CRC 校验错误报文数、过小（或超大）的数据报文数、广播、多播的报文数以及接收字节数、接收报文数等。

利用 RMON 统计管理功能，可以监视端口的使用情况、统计端口使用中发生的错误。

4 配置 RMON

在配置 RMON 功能之前，必须保证 SNMP Agent 已经正确配置。SNMP Agent

的配置请参见实验三。

表 7-1 RMON 配置过程

操作	命令	说明
进入系统视图	**system-view**	-
添加事件表的一个表项	**rmon event** *event-entry* [**description** *string*] { **log** | **trap** *trap-community* | **log-trap** *log-trapcommunity* | **none** } [**owner** *text*]	可选
添加告警表的一个表项	**rmon alarm** *entry-number alarm-variable sampling-time* { **delta** | **absolute** } **rising_threshold** *threshold-value1 event-entry1* **falling_threshold** *threshold-value2 event-entry2* [**owner** *text*]	可选 在添加告警表项之前，需要通过 **rmon event** 命令定义告警表项中引用的事件
添加扩展告警表的一个表项	**rmon prialarm** *entry-number prialarm-formula prialarm-des sampling-timer* { **delta** | **absolute** | **changeratio** } **rising_threshold** *threshold-value1 event-entry1* **falling_threshold** *threshold-value2 event-entry2* **entrytype** { **forever** | **cycle** *cycle-period* } [**owner** *text*]	可选 在添加扩展告警表项之前，需要通过 **rmon event** 命令定义扩展告警表项中引用的事件
进入以太网端口视图	**interface** *interface-type interface-number*	-
添加历史表的一个表项	**rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text*]	可选
添加统计表的一个表项	**rmon statistics** *entry-number* [**owner** *text*]	可选

📖 **说明：**

- 使用 **rmon alarm** 命令和 **rmon prialarm** 命令对节点进行监控时，要求被监控的节点必需存在，否则配置无效。
- 使用 **rmon statistics** 命令添加统计表项时，一个端口下只能创建一个 rmon 统计表项。即如果在一个端口下已经创建了一个统计表项，再在该端口下创建一个其他索引号的统计表项则不能成功。

5 RMON 配置显示

在完成上述配置后，在任意视图下执行 display 命令可以显示配置后 RMON 的

运行情况，通过查看显示信息验证配置的效果。

表 7－2 RMON 显示和维护

配置	命令	说明
显示 RMON 统计消息	**display rmon statistics** [*interface-type interface-number* | **unit** *unit-number*]	**display** 命令可以在任意视图执行
显示 RMON 历史信息	**display rmon history** [*interface-type interface-number* | **unit** *unit-number*]	
显示 RMON 告警信息	**display rmon alarm** [*entry-number*]	
显示扩展 RMON 告警信息	**display rmon prialarm** [*prialarm-entry-number*]	
显示 RMON 事件	**display rmon event** [*event-entry*]	
显示 RMON 事件日志	**display rmon eventlog** [*event-entry*]	

7.5 实验内容与步骤

1 配置 H3C 交换机上的 RMON 功能

创建索引号为 1 的统计表项，记录以太网口 Ethernet1/0/1 的统计信息。

```
<H3C> system-view
[H3C] interface Ethernet 1/0/1
[H3C-Ethernet1/0/1] rmon statistics 1
[H3C-Ethernet1/0/1] quit
```

创建扩展告警触发的事件。

```
[H3C] rmon event 1 log
[H3C] rmon event 2 trap 10.21.30.55
```

在扩展告警表中添加索引号为 2 的表项，对相应告警变量以公式（.1.3.6.1.2.1.16.1.1.1.9.1+.1.3.6.1.2.1.16.1.1.1.10.1）运算，得出以太网口 Ethernet 1/0/1 接收到的所有数据格式正确的过小包和过大包的数量，对该运算结果以 10 秒的采样间隔进行监视，当变化率大于等于上限阈值 50 时触发事件 1，小于等于下限阈值 5 时触发事件 2，设置告警实例采样类型为 forever，创建者为 user1。

```
[H3C] rmon prialarm 2 (.1.3.6.1.2.1.16.1.1.1.9.1+.1.3.6.1.2.1.16.1.1.1.10.1) test 10 changeratio rising_threshold 50 1 falling_threshold 5 2 entrytype forever owner user1
```

```
# 查看索引号为 2 的 RMON 扩展告警表项的配置
[H3C] display rmon prialarm 2
Prialarm table 2 owned by user1 is VALID.
  Samples type            : changeratio
  Variable                          formula                          :
(.1.3.6.1.2.1.16.1.1.1.9.1+.1.3.6.1.2.1.16.1.1.1.10.1)
          Description             : test
          Sampling interval       : 10(sec)
          Rising threshold        : 100(linked with event 1)
          Falling threshold       : 10(linked with event 2)
          When startup enables    : risingOrFallingAlarm
          This entry will exist   : forever.
          Latest value            : 0
```

2 配置 NMS

我们使用 MG－SOFT 软件完成对以太网交换机的 RMON 功能的查询操作。配置方法参照实验 4。

📖 **说明：**

网管系统的认证参数配置必须和设备上保持一致，否则网管系统无法管理设备。

7.6 思考题

⑴ RMON 和 SNMP 有什么不同？着重解决了什么问题？

⑵ 目前的 RMON MIB 中包含哪些组？分成几部分？

实验 8 网络监视器、性能监视器

8.1 实验目的

⑴ 了解事件查看器、性能监视器的运用。

⑵ 掌握网络监视器 Network monitor 的安装和使用方法。

⑶ 理解网络层次结构中各层数据的包装关系。

8.2 实验类型

验证型实验

8.3 实验环境

具备 IIS 的 Windows 2000 Server 计算机、局域网、Windows 2000 Server 安装光盘。

8.4 实验内容与步骤

1 监视事件

IIS 中的网站是靠 IIS 服务来实现的，例如 Web 站点依赖于 WWW 服务，故服务启动失败这样的事件往往暗示着站点不能正常工作的原因。此外，象 TCP/IP 错误，网络硬件设备错误这样的事件往往也是导致服务器不能正常工作的罪魁祸首。当系统提示出错或者 IIS 出现某种异常情况时，有经验的管理员通常先检查事件查看器所记录的事件。

单击“开始”、“控制面板”、“管理工具”、“事件查看器”打开如图 7-1 所示的事件查看器。全部事件分别保存在三个事件日志中：应用程序日志、安全日志和系统日志。

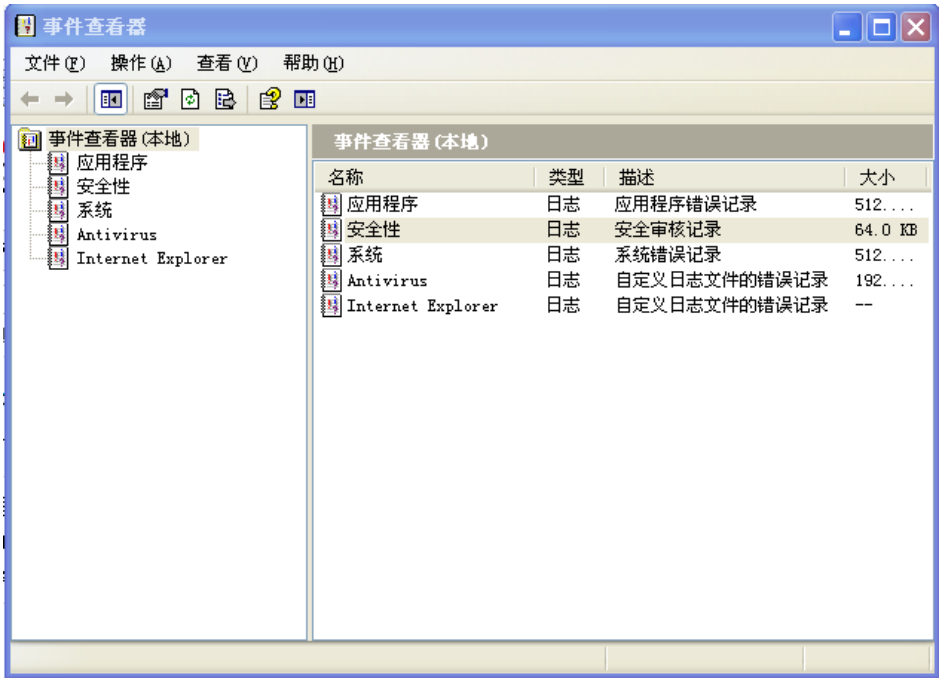

图 8-1 事件查看器

对于 IIS 服务器而言，系统日志中记录的事件显得更加重要。在事件查看器控制树中选择系统日志，则右侧窗格列出已经被记录的全部事件，事件分为：错误、警告、信息等不同类型。

事件列表中仅显示有关事件发生的时间、来源、分类和用户等有限信息，为了详细查看某一事件的描述或信息代码，应双击列表中的事件，查阅事件属性对话框。如右图所示，在事件属性对话框中详细描述事件发生的情况和可能的原因，典型的事件还给出了数据代码供程序员调试使用。单击事件属性对话框中的上下箭头可以继续查看上一个或下一个事件的详细信息。

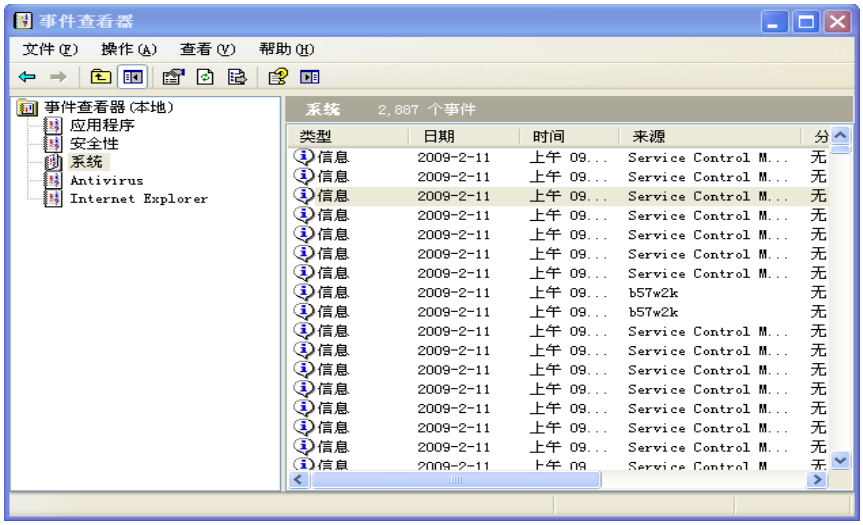

图 8-2 查看事件信息

2 性能监视

通过日志文件的方式对服务器进行长期监视，得到系统对象的平均特性。

利用日志文件进行及监视的方法如下：

⑴ 打开性能监视器：“开始”—“设置”—“控制面板”—“管理工具”—“性能”，如图 8-3 所示。

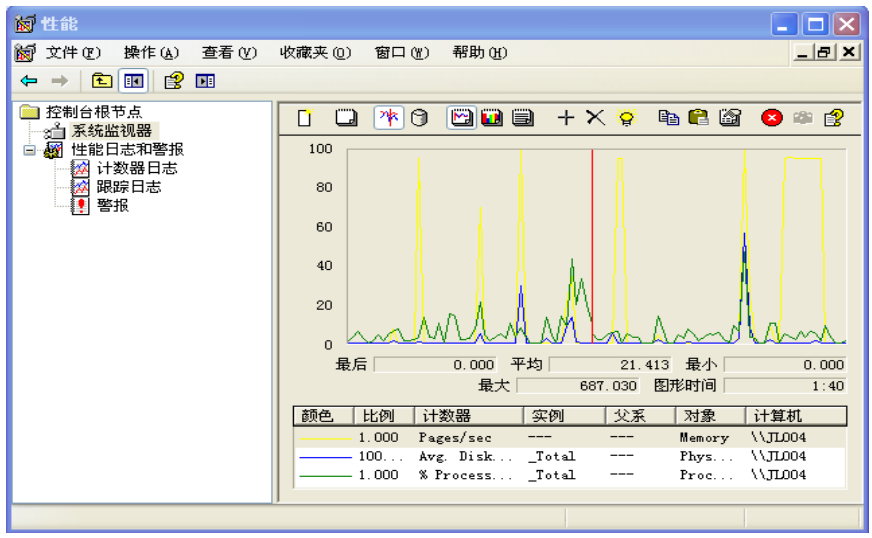

图 8-3 性能查看器

⑵ 展开“性能日志和警报”节点，右击“计数器日志”，选择“新建日志设置…”。在“新建日志设置…”对话框中输入新日志名称，单击“确定”。

⑶ 如图 8-4 所示在新日志属性对话框的“常规”选项卡中单击“添加计数器…”打开计数器对话框，指定该日志文件记录的计数器，单击“确定”返回。

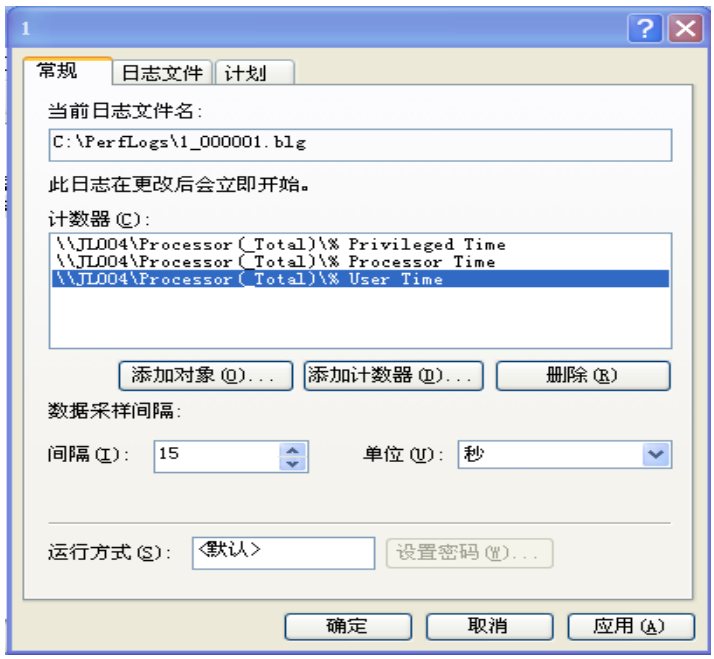

图 8-4 添加计数器

⑷ 在“数据采样间隔”栏中指定计数器数据多久被采集一次，注意，过密的采集间隔会影响系统的正常工作并造成巨大的日志文件。

⑸ 在“计划”选项卡中指定日志启止时间，可选的方式有：手动、指定起止时间或者指定记录时间。

⑹ 如图 8-5 所示，如果选择手动启止日志，则在日志列表中右击日志，选择“启动”，日志图标变为绿色。

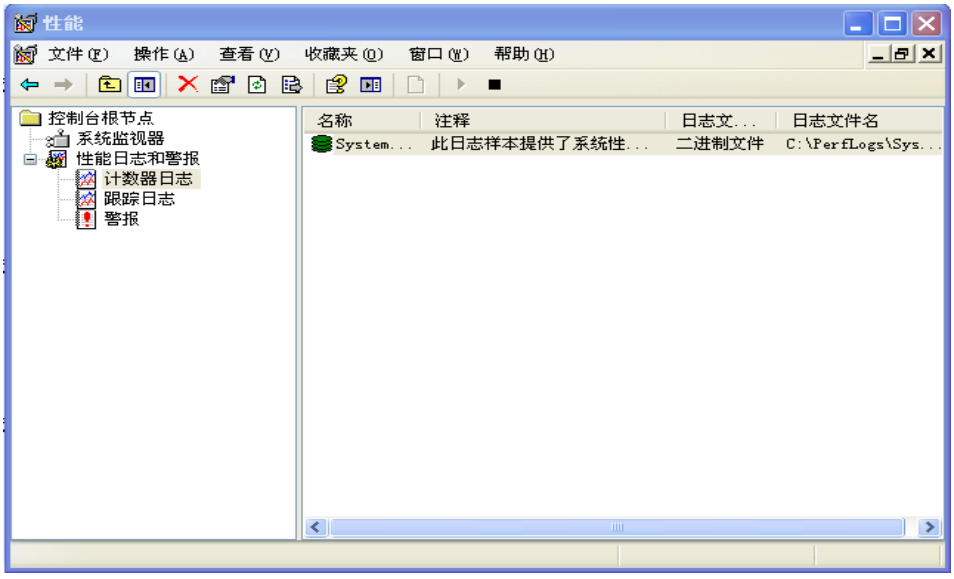

图 8-5 启动日志

添加以下计数器，观察图表变化。

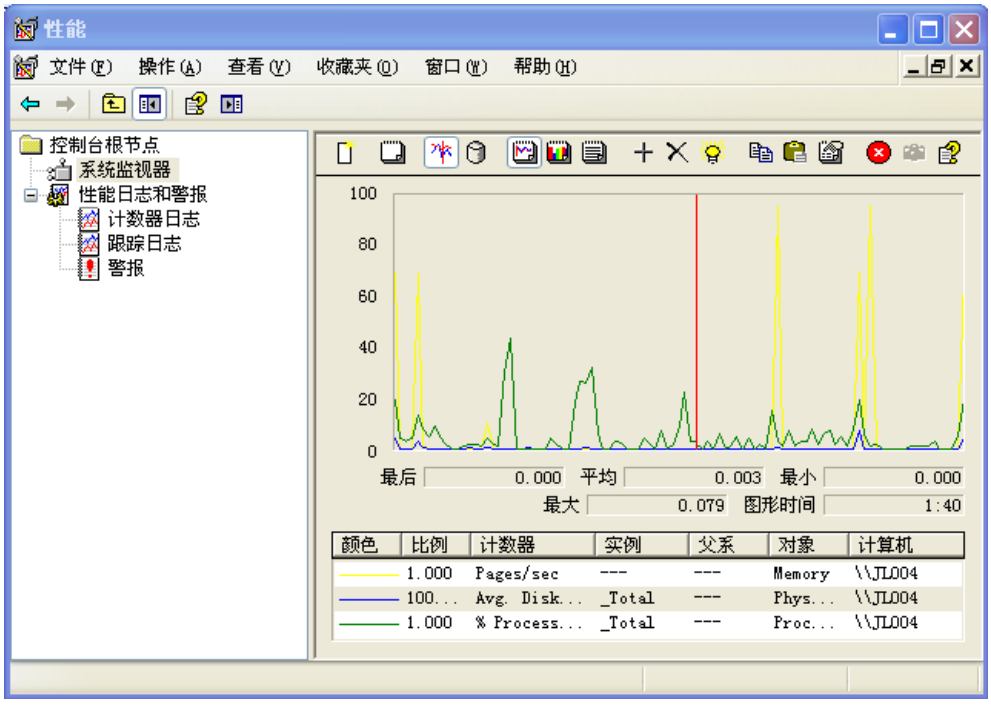

图 8-6 系统监视器性能图

查找内存瓶颈

在性能工具中使用下列计数器标识出现瓶颈的内存资源：

- System Processor Queue Length
- Memory Pages/sec

查找磁盘瓶颈

在性能工具中使用下列计数器标识出现瓶颈的磁盘资源：

- PhysicalDisk % Disk Time 和 % Idle Time
- PhysicalDisk Disk Reads/sec 和 Disk Writes/sec
- PhysicalDisk Avg.Disk Queue Length
- LogicalDisk % Free Space

还要监视内存计数器，以确定是否有过多的内存分页使磁盘使用紧张。

注意：与物理磁盘计数器的数据不同，逻辑磁盘计数器的数据默认情况下不是由操作系统搜集。要获得逻辑驱动器或存储卷的性能计数器数据，必须在命令提示符下键入 diskperf -yv。这会导致用于搜集磁盘性能数据的磁盘性能统计驱动程序报告逻辑驱动器和存储卷的数据。默认情况下，操作系统使用 diskperf -yd 命令包含物理驱动器数据。有关使用 diskperf 命令的详细信息，请在命令提示符下键入 diskperf -?。

查找处理器瓶颈

在性能工具中使用下列计数器标识出现瓶颈的处理器资源：

- Processor Interrupts/sec
- Processor % Processor Time
- Process(process) % Processor Time
- System Processor Queue Length

查找网络瓶颈

在性能工具中使用下列计数器标识出现瓶颈的网络资源

- Network Interface Bytes Total/sec、Bytes Sent/sec 和 Bytes Received/sec
- Protocol_layer_object Segments Received/sec、Segments Sent/sec、Frames Sent/sec 和 Frames Received/sec 对于 NWLink 性能对象，与帧有关的计数器只报告零。对这些对象使用基于数据报的计数器。
- Server Bytes Total/sec、Bytes Received/sec 和 Bytes Sent/sec
- Network Segment % Network Utilization

系统监视器将计数器数据以 blg 文件的形式保存起来（缺省位置是系统分

区的\PerfLogs 目录下）。一旦开始记录，计数器数据被定期（按照采样间隔时间）加入日志文件，直到到达计划的日志结束时间或者手工停止日志记录。

3 建立性能警报

系统监视器能够持续的记录某个计数器的值，但是在某些情况下，我们仅需要及时的获知某一计数器的值是否超过特定的上限或者下限，这就要用到性能警报。在系统监视器中创建警报的方法如下：

⑴ 展开系统监视器的“性能日志与警报”，右击“警报”，选择“新建警报设置…”。指定新警报的名称，单击“确定”。

⑵ 如图 8-7 所示的警报属性对话框中，单击“添加…”，打开添加计数器对话框。

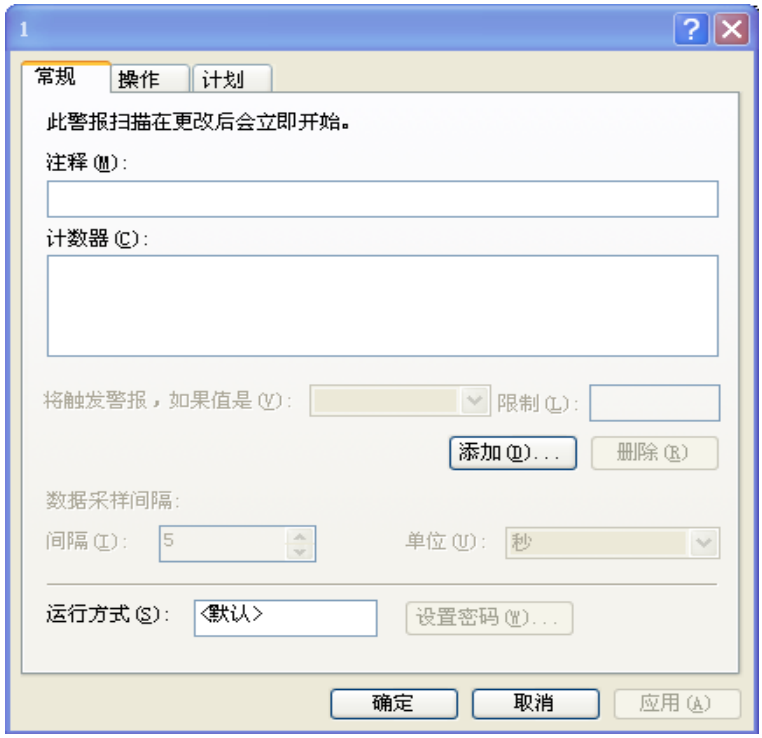

图 8-7 设置警报

⑶ 指定需要创建警报的对象和计数器，以及计数器实例，然后单击“添加”。

⑷ 在“计数器”列表中选择计数器，指定警报范围，即被选中计数器的值一旦超过或者低于限制值，即启动警报。从下拉列表中指定限制方式为“超过”或“低于”，并在“限制”栏中指定限制值。

⑸ 在“常规”选项卡下部指定计数器数据采样的间隔，对于实时数据类型，监

视器以指定的采样间隔为基准作数据平均值，并用该平均值与限制作比较确定是否发送警报。

⑹ 单击“计划”选项卡，指定警报服务工作的有效时间段，可选的方式有：指定起止时间、指定连续工作时间、手工启动。对于连续的警报需求，应当采用手工方式启动警报，直到不需要警报时再手工停止。

⑺ 单击“操作”选项卡，如右图 8-8 所示，指定计数器超过限制时将警报发往何处。一般应选择“计入应用程序事件日志”复选框以保留警报事件备份。选择“发送网络信息到”复选框并指定将警报发送到网络管理员所在的计算机。亦可选择“执行这个程序”并指定发出警报后自动执行的程序，或者单击“命令行参数”指定发出警报后自动执行的系统命令。单击“确定”关闭对话框。

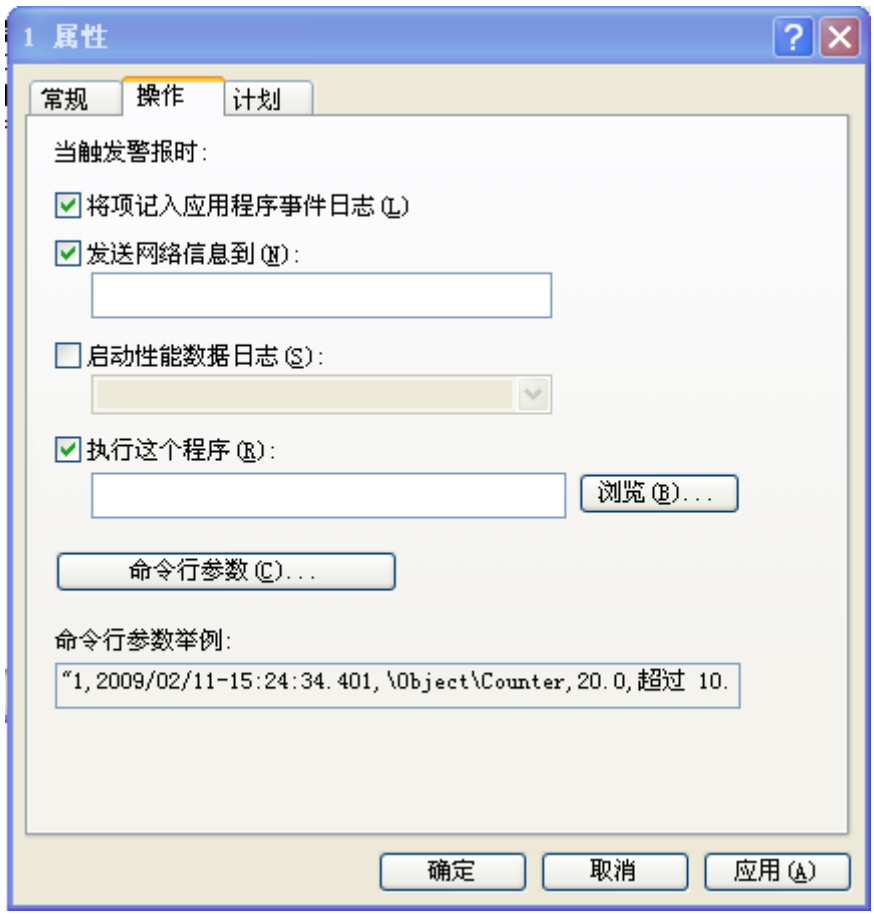

图 8-8 设置警报

⑻ 根据需要手工启动警报服务。右击列表中的警报，选择“开始”启动警报。一旦启动警报，系统监视器将持续的监视警报计数器，发现其值超过限制时立

即将警报信息发送到指定的网络位置或执行预定应用程序，同时在应用程序日志中记录一个警报事件。最常见的警报是监视服务器可用磁盘空间警报，它及时的向管理员发出磁盘空间不足的信息，避免了由此带来的损失。

4 监视网络

⑴ 安装网络监视器

① 依次击点“开始”“设置”，然后选定控制面板；

② 打开“添加/删除程序”对话框；

③ 选定“添加/删除 Windows 组件”；

④ 在 Windows 组件向导中，选定管理和监视工具，然后单击“详细资料”；

⑤ 选定“网络监视工具”复选框，然后单击“确定”按钮；

⑥ 如果系统提示输入其他文件，插入 Windows2000 Server 的光盘，或者键入网络上的文件位置路径。

⑵ 熟悉软件界面

① 抓取窗口：分析网络的总体性能，并且可以启动和停止网络抓取功能，保存抓取的网络信息。设置视图和抓取过滤器及抓取触发器。抓取窗口的 4 个区域：

- 图形窗格：用图形显示网络活动。
- 会话统计数据窗格：汇总两个主机之间传输的信息，指明哪个主机正在发送广播或组播信息。
- 合计数据窗格：显示所有抓取到的信息的统计数据，被抓取的数据帧的统计数据，每秒钟的网络利用率及网络适配卡的统计数据。
- 工作站统计数据窗格：汇总主机发送的数据帧的合计数量、接收数量、接收和发送的数据帧和字节的数量以及发送的广播帧和组播帧的数量

② 抓取汇总信息窗口：抓取信息后查看抓取内容。

⑶ 抓取和显示网络信息

注意显示感兴趣的信息和设置抓取过滤器的方法。

ARP（Ping 命令涉及的一个地址转换协议）信息的抓取和显示实例：

① 依次击点“开始”“程序”“管理工具”，并选定“网络监视工具”。

② 如果这是第一次访问“网络监视工具”，系统将提示你选定一个网络。“捕获”“网络”中选择你的服务器连接的网卡。

③ 这时出现“网络监视工具”抓取窗口，在“捕获”菜单上，单击“开始”。

④ 在命令窗口将 ping 命令发送给本地子网的一个计算机。

⑤ 在“捕获”菜单上选定“停止并查看”。出现网络监视器的抓取汇总信息窗口。

⑥ 在“显示”菜单上，单击“颜色”，选定“ARP_RARP”，选择一个背景颜色，单击“确定”，所有的 ARP 数据帧都使用该颜色来显示。

⑦ 双击 ARP 数据帧查看内容。

⑧ 使用控件按钮控制显示的内容和形式。

⑨ 同样方法显示 ARP 应答帧内容，查看转换结果。

⑩ 使用“文件”菜单保存抓取的信息。

⑷ 抓取文件默认目录 winnt\system32\netmon\captures

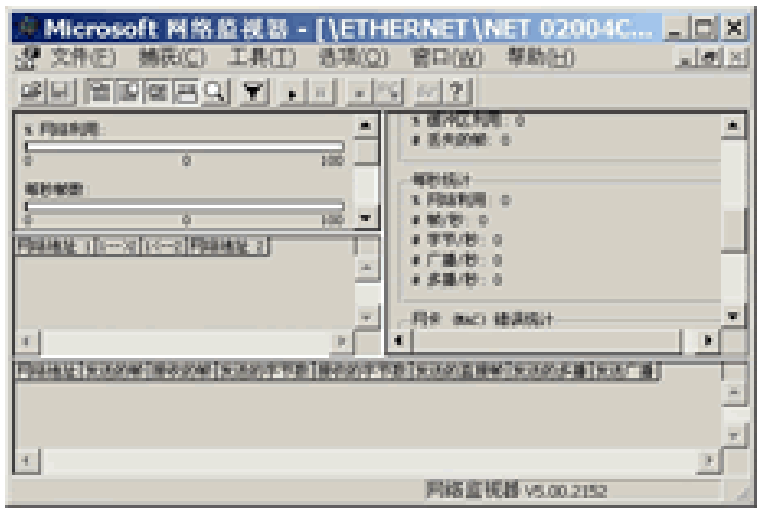

图 8-9 网络监视器

单击“开始”、“程序”、“管理工具”、“网络监视器”，打开如图 8-9 所示的为了监视器窗口。单击“捕获”菜单，选择“开始”，启动网络监视器捕获功能。

查看左上侧窗格显示网络利用率和每秒帧数等有关网络物理特性的信息。这些信息是判断网络的繁忙程度是关键数据。经常处于高利用率的网络显然应该进行升级。

右侧窗格显示网络监视器的统计信息，包括网络统计、每秒统计、捕获统计和错误统计。

网络监视器下部的窗格提供了针对每台网络主机的监视工具，从中可以获知其他计算机的工作状态，也可以查找未经授权的计算机。

查看网络监视器的捕获筛选功能，如图 8-10 所示。主要的筛选方式是主机地址，双击“捕获筛选程序”对话框中的“地址对”，如下图所示，指定捕获特殊主机之间的数据包。

图 8-10 捕获筛选功能

8.5 思考题

⑴ Windows 系统提供的这些监控功能全面吗？还需要提供哪些功能？

⑵ 你还试用了哪些专用网络监控工具软件？它们的主要特点和用途是什么？

实验 9 用 SolarWinds 监控网络

9.1 实验目的

⑴ 掌握网络管理工具组 SolarWinds 的使用方法。

⑵ 理解网络管理软件在网络管理、配置与维护中的作用和功能。

9.2 实验类型

验证型实验

9.3 实验环境

安装了 Windows 2000/xp/2003 系统的主机、局域网、交换机。SolarWinds 软件。

9.4 实验内容与步骤

1 SolarWinds 的 Discovery[网络发现工具栏]具体应用

用网络发现工具能够帮助我们发现网络上很多的 DNS 错误，它的发现引擎是快速、最彻底的引擎之一。在网络发现工具中有以下几项功能：

⑴ IP Network Browse(IP 网络浏览器)

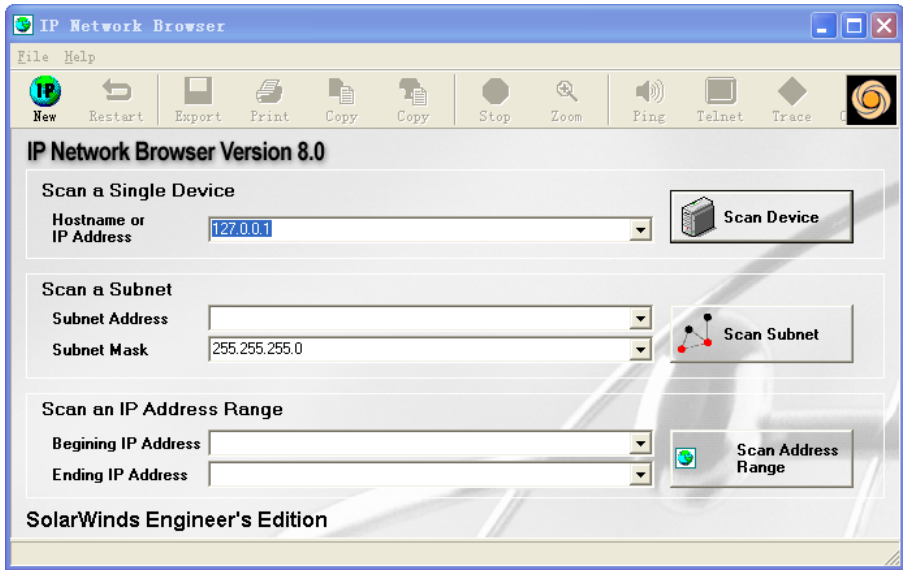

图 9-1 IP 网络浏览器

① 输入 IP 地址如 192.168.12.254 ，单击“Scan device”，扫描到 Cisco s3550-24 交换机设备，如图示。

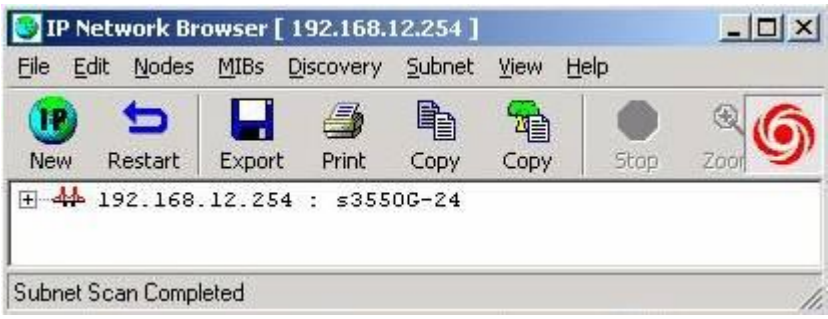

图 9-2 发现新设备

② 输入子网地址和子网掩码，如 192.168.12.0 和 255.255.255.0 ，单击“ Scan Subnet ”，扫描到下列如图示各设备。

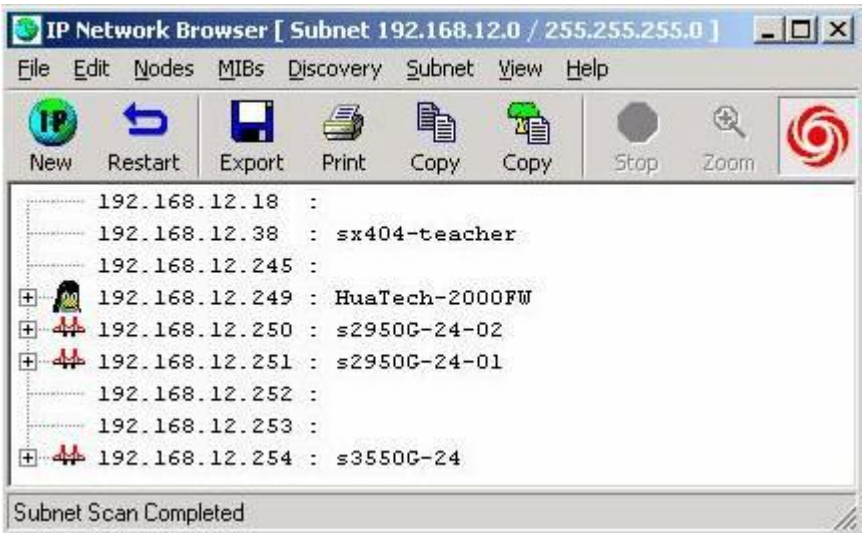

图 9-3 扫描子网

③ 输入起始 IP 地址和终止 IP 地址，如 192.168.12.1 和 192.168.12.254，单击“ScanAddress Range”，扫描到下列如图示各设备。

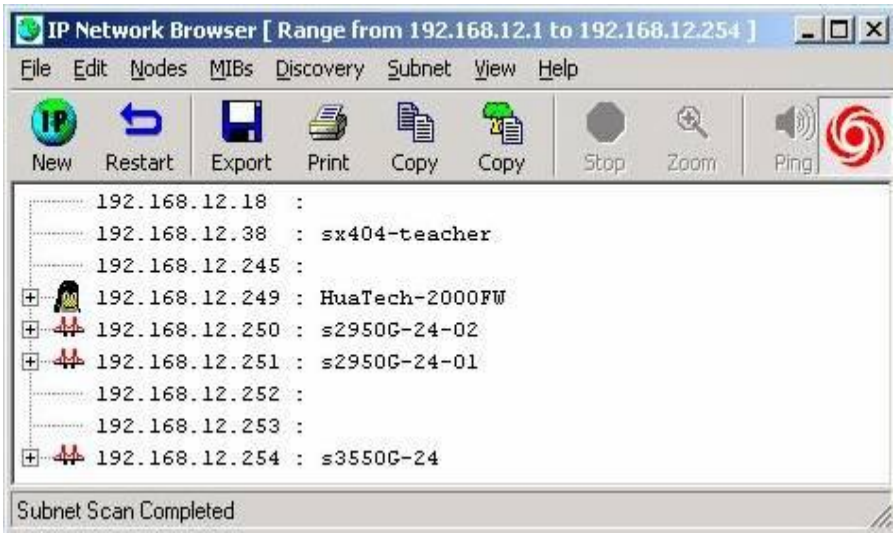

图 9-4 根据 IP 地址扫描设备

⑵ Ping Sweep (Ping 扫描)

输入起始 IP 地址和终止 IP 地址， 如 192.168.12.1 和 192.168.12.50 ，单击“ Scan ”，扫描到下列 IP 地址正在使用，即该设备已开机。

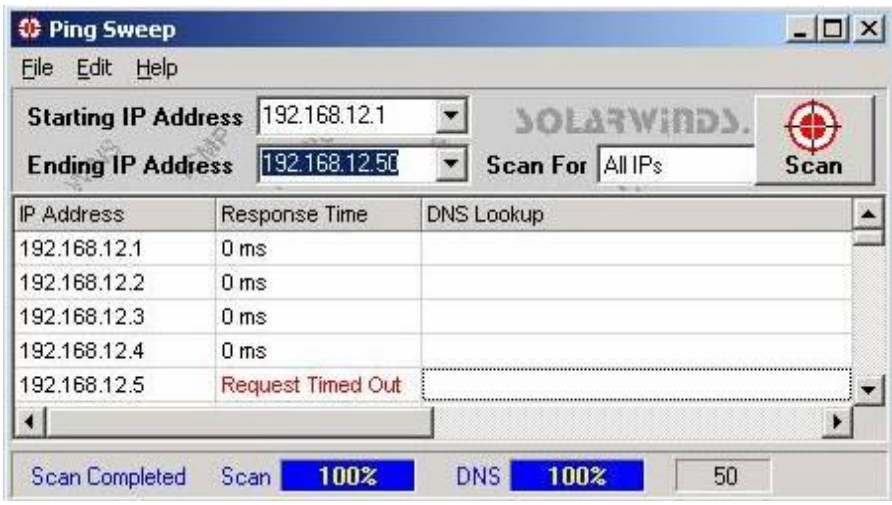

图 9-5 Ping 扫描

⑶ Subnet List（子网地址清单）

输入主机的 IP 地址，如 192.168.12.254 ， SNMPCommunity String 为“ public ”，单击“ Retrieve Subnets ”，扫描到下列如图示的二个网段 192.168.12.0 和 192.168.13.0 。

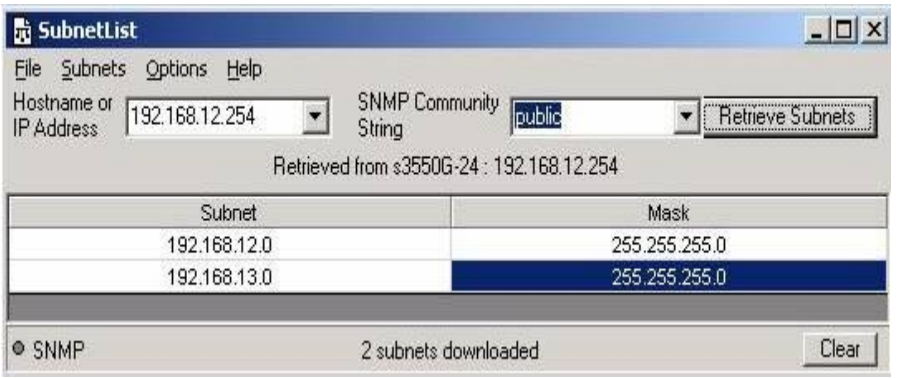

图 9-6 子网清单

⑷ SNMP Sweep(SNMP 扫描)

输入起始 IP 地址和终止 IP 地址， 如 192.168.12.1 和 192.168.12.254 ， 单击“ Scan ”，对网段扫描后可以扫描到如下设备的详细资料，如设备名称、型号、设备描述、厂商、 厂商的网址等资料。

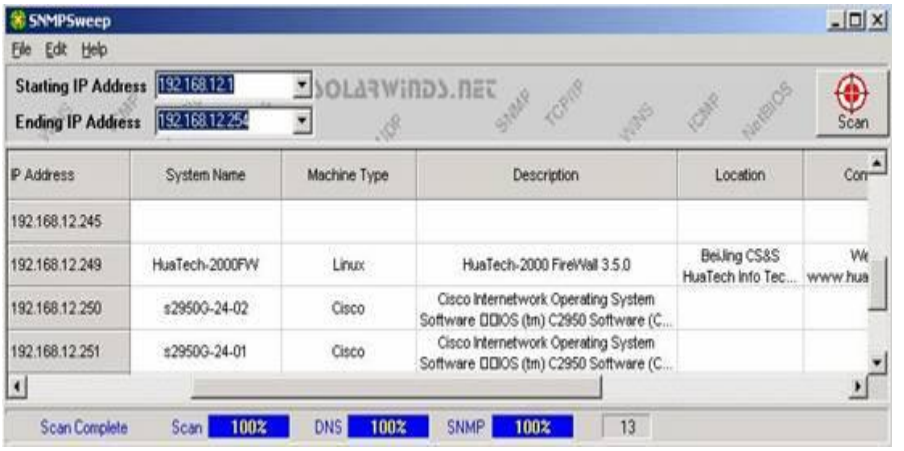

图 9-7 SNMP 扫描

⑸ Network Sonar（网络声纳）

① 网络声纳可以对 TCP/IP 网络设备的搜索结果建立一个 Micosoft 数据库。搜索可以随时暂停或停止。当搜索再次开始的时候，它会接着上次搜索的的结果继续进行扫描。

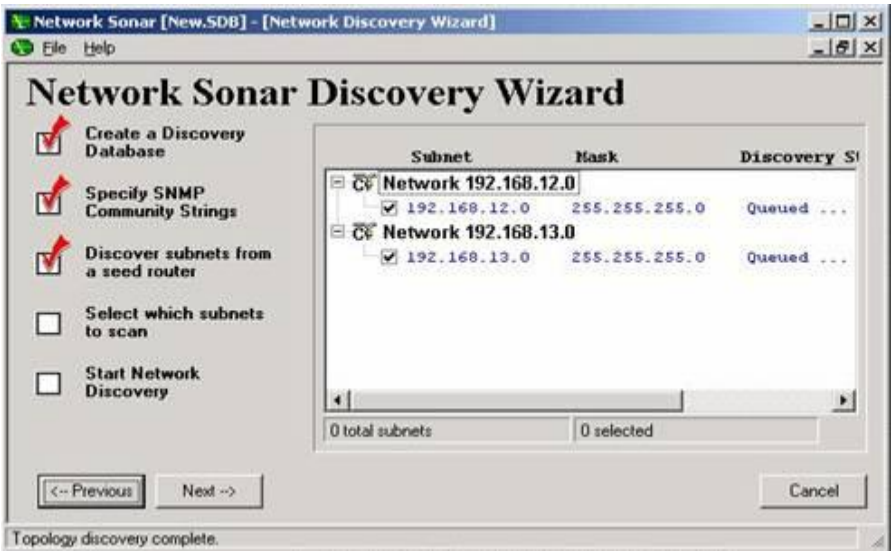

图 9-8 网络声纳

② ICMP，SNMP 以及 DNS 发现引擎能够在你的网络中创建一个详细的发现数据库，可以说是最快最广泛的 TCP/IP 发现工具之一。

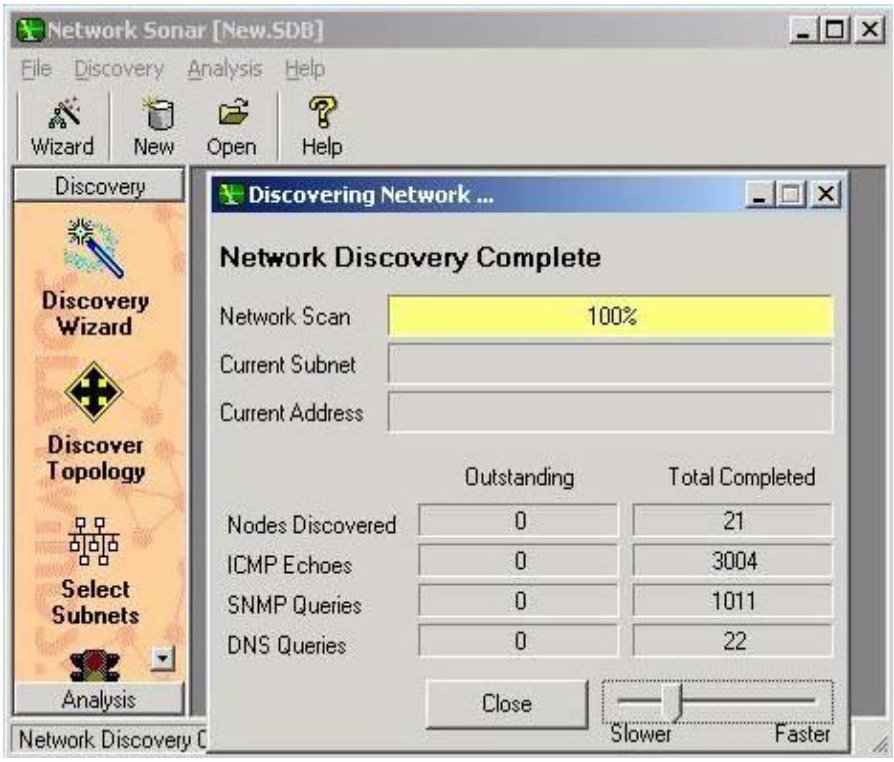

图 9-9 发现引擎

③ 对 TCP/IP 网络设备的搜索结果的分析如下：

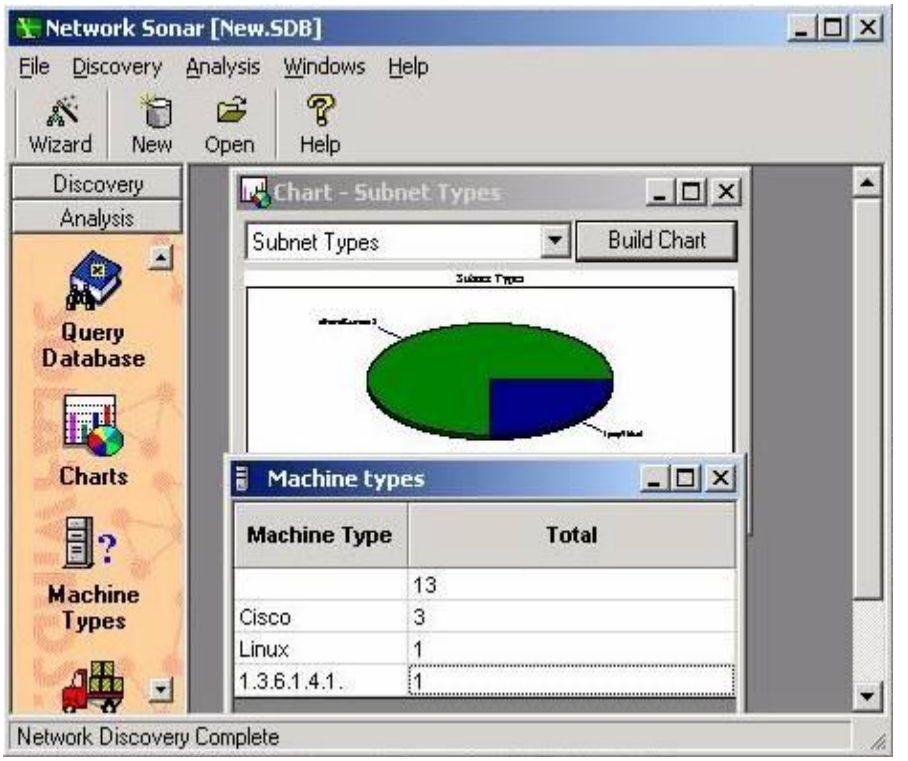

图 9-10 搜索结果

⑹ DNS Audit (域名系统检查)

DNS 检查能够扫描到某一范围的 IP 地址并且能够做出正向和反向的检查，因此 DNS 的错 误就能够被快速识别，并且 DNS 检查能够同时支持 DNS 和 WINS 。输入起始 IP 地址和终止 IP 地址， 如 192.168.12.1 和 192.168.12.254 ，单击“ Scan ”，搜索到下列一个 DNS 服务器。

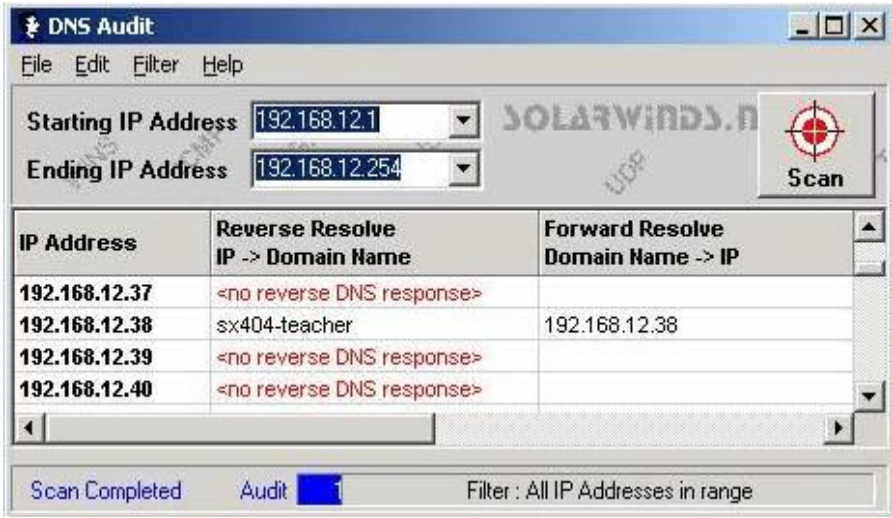

图 9-11 域名系统检查

⑺MAC Address Discovery (MAC 地址发现工具)

MAC 地址发现工具能够找到与之相关联的 IP 地址和物理地址。输入本地子网，如 192.168.12.0 ，单击“ Discover MAC Addresses ”，就发现下列本地正在使用的 MAC 地址及其网卡的制造厂商。

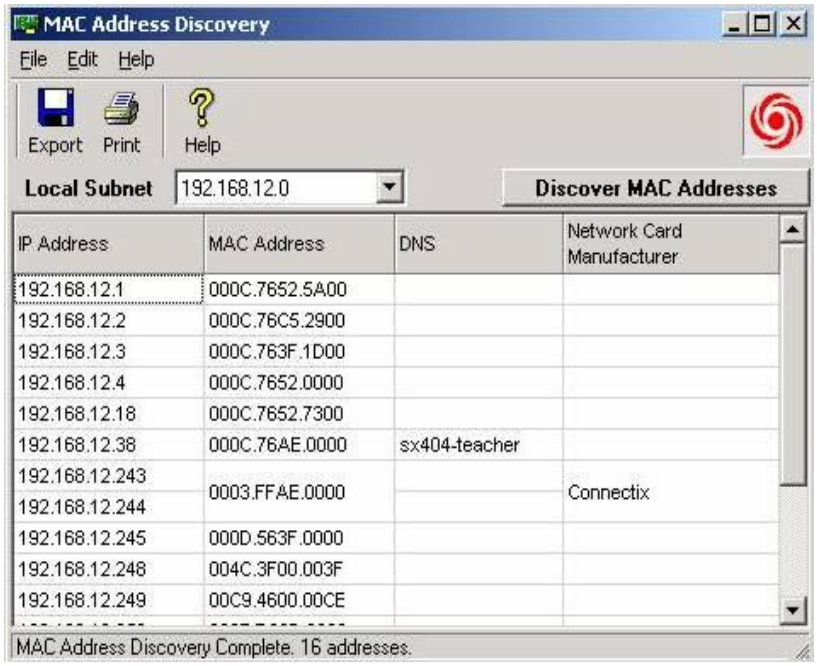

图 9-12 MAC 地址发现

2 用 SolarWinds 监控网络

（1）网络监控

① 打开监控菜单

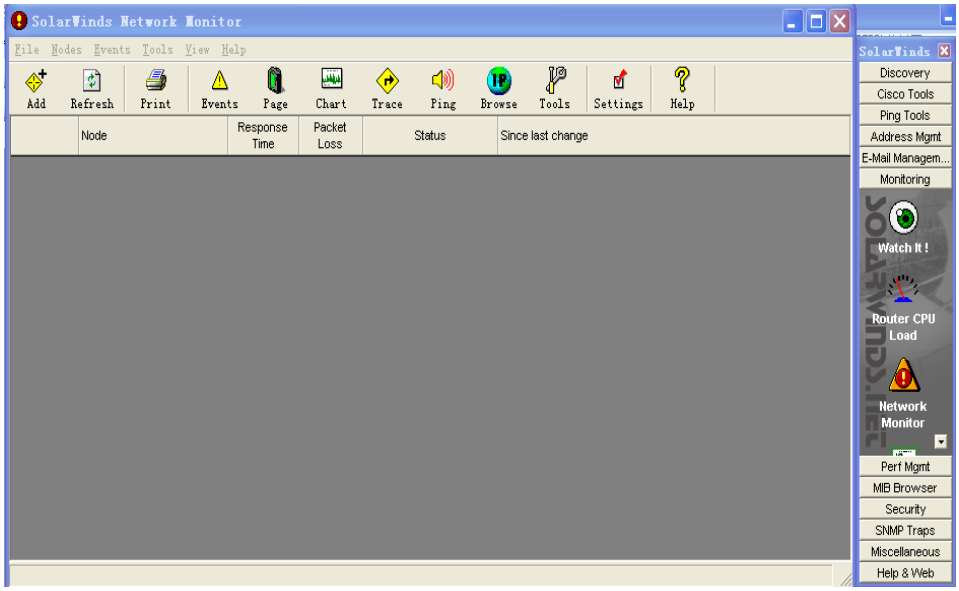

图 9-13 监控菜单

② 点击“add”后输入一个需要监控的 ip 地址，比如 169.254.1.150

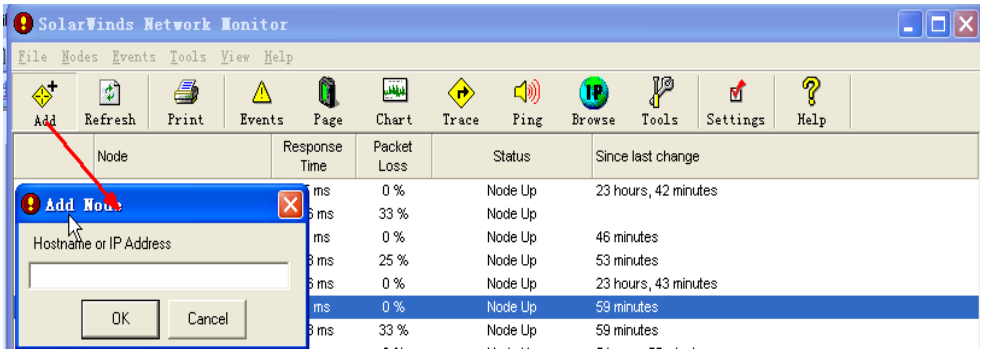

图 9-14 增加需要监控的 IP

③ 这个地方可以设置相应标示，如果 ip 地址比较多的话，可以把不好区分的 ip 地址标示一下，注意：这个地方需要点击“apply changes”保持设置

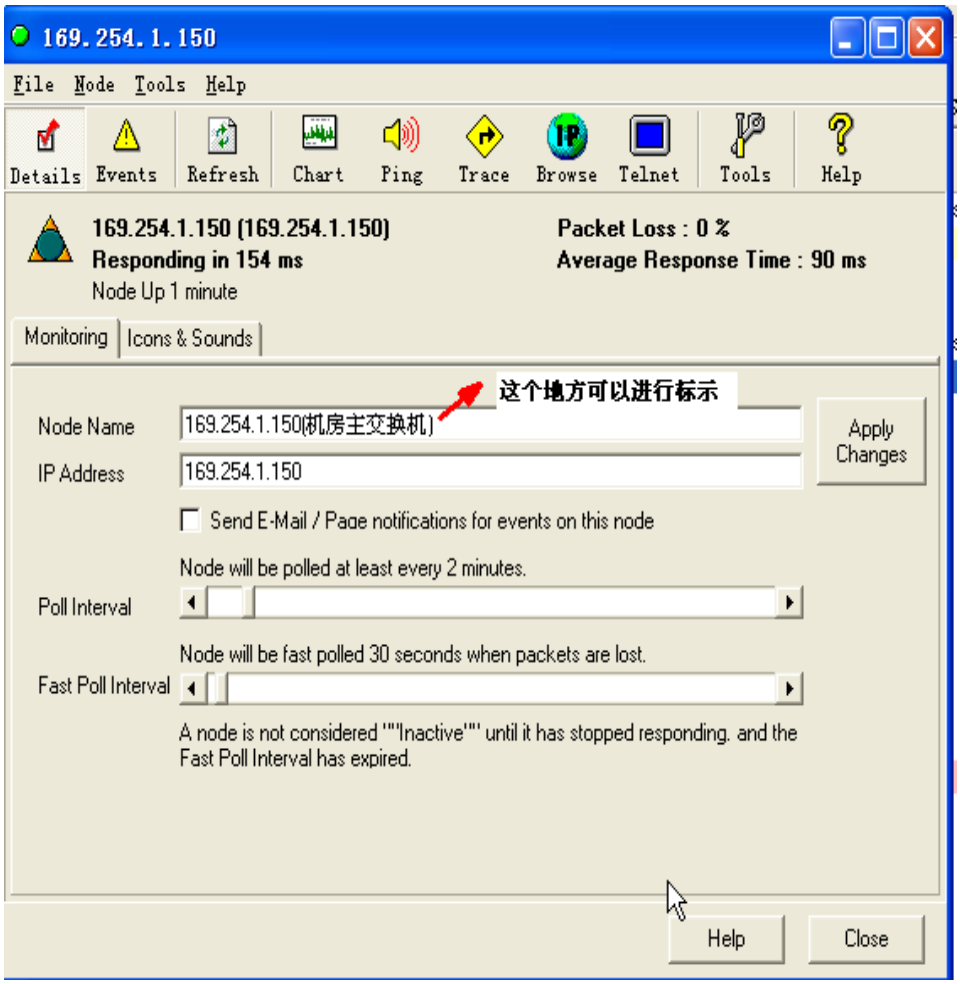

图 9-15 标注特定机器

④ 在“icon”选项可以根据自己的爱好选择相应的图标

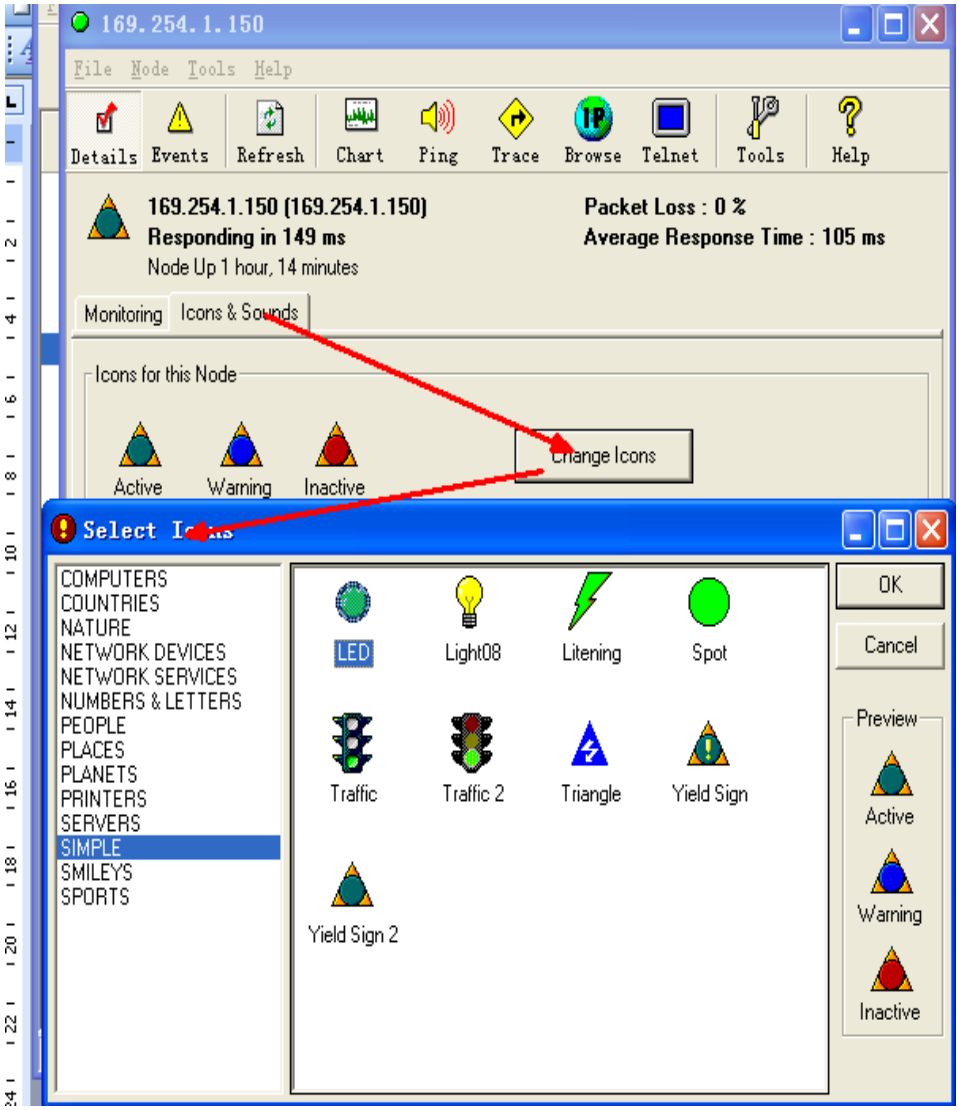

图 9-16 选择图标

⑤ 点击 ok 确定即可

⑥ 如果需要删除监控的 ip 的话，选中相应 ip，然后右键删除 note 即可

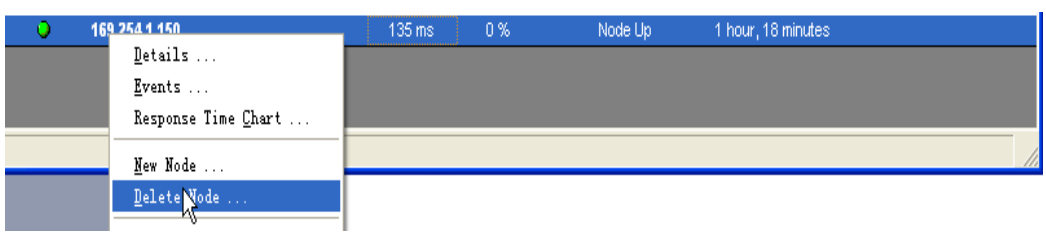

图 9-17 删除监控 IP

⑵ 用 SolarWinds 监控流量

① 首先要在路由器上面开启流量统计功能；这样经过路由器的流量就被记录下来

② 然后打开 SolarWinds 的 Mib Browser—SNMP MIB Browser

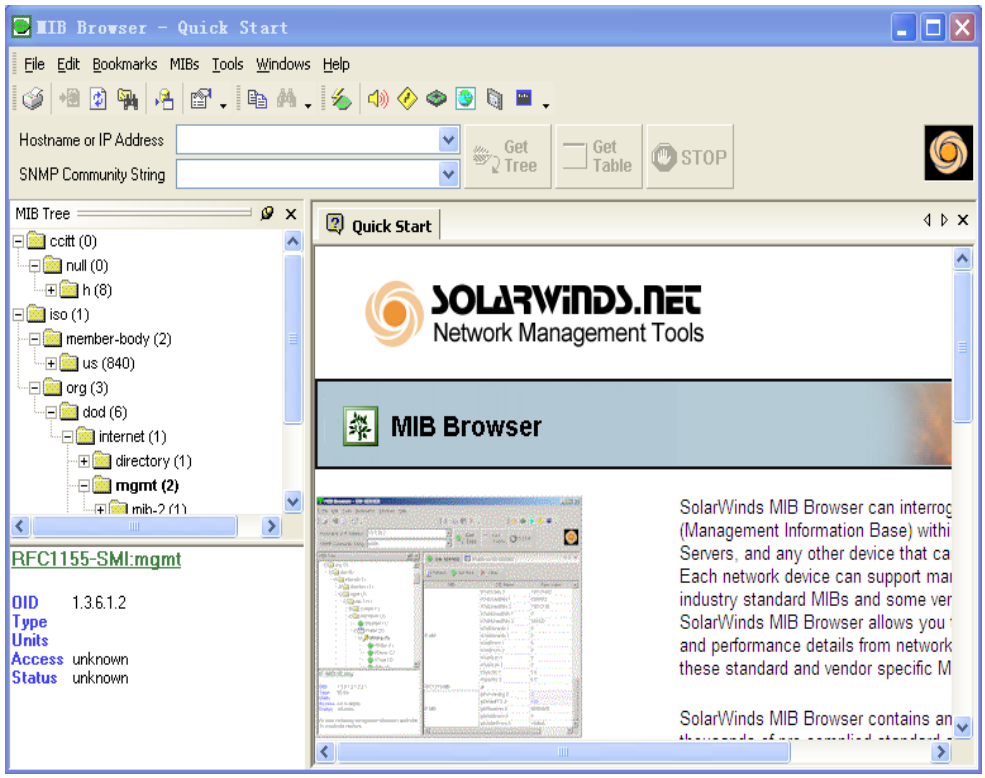

图 9-18 SolarWinds 的 Mib Browser

③ 输入网关的 ip 地址和路由器的 snmp community string（snmp 在路由器上的设置不再描述），然后点击 get tree

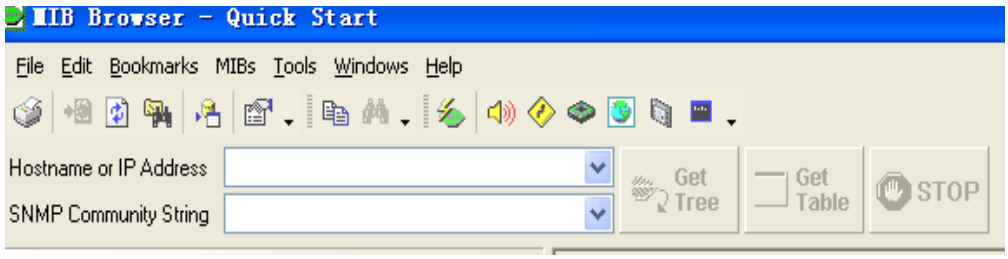

图 9-19 设置 SolarWinds 的 Mib Browser

④ 点击 iso-org-private-enterprise-cisco-local-lip-lipAccountingTable，然后右键-get table，就可以显示每个 ip 地址的流量了。actByts 显示的就是 ip 地址的流量

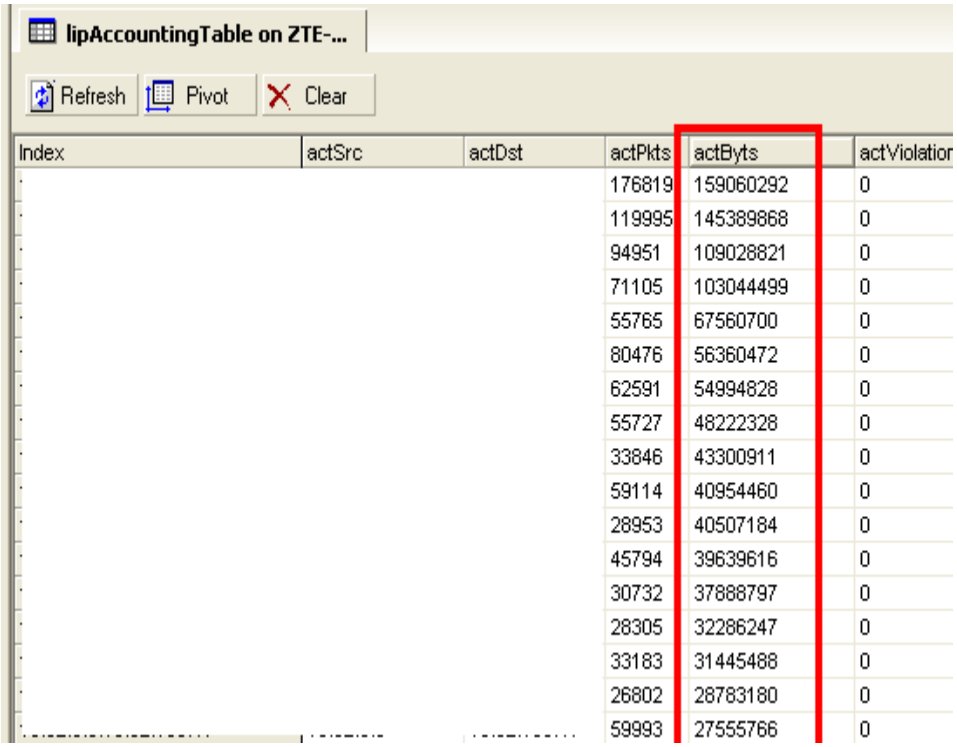

图 9-20 显示流量

如果发现网络比较慢，怀疑某个 ip 地址非法下载的时候，可以先到路由器上面清除流量然后重新计数，然后找到流量最大的 ip 进行处理。

9.5 思考题

⑴ SolarWinds 提供的这些监控功能和 Windows 系统相比全面吗？还需要提供哪些功能？

⑵ 请说出一种你认为最有用的功能，或者说出一种 SolarWinds 还不具备的功能。

附录：实验指导材料

Solarwinds 的简单说明

SolarWinds 是一款功能专业的网络管理工具组，适合专业的网管工程师使用。它的用途十分广泛，涵盖了从简单、变化的 ping 监控器及子网计算器（Subnet calculators）到更为复杂的性能监控器和地址管理功能，大幅的简化网管工程师对于网络的管理工作负担与提升效率，支持在线下载单个升级文件。

Discovery 栏

IP Network Browser 用于扫描于与设定的 SNMP 字符串相同的路由器

Ping Sweep 用于扫描一段 IP 中有哪些正在被使用，并显示出其 DNS 名字

Subnet List 用于扫描路由下的分支网络，并给出了子网掩码

SNMP Sweep 用于在一段 IP 下扫描哪些提供 SNMP 服务

Network Sonar 用于建立和查看 TCP/IP 网络构成数据库

DNS Audit 用于扫描定位本地 DNS 数据库错误

MAC Address Discovery 用于扫描一段 IP 内存在机器的 MAC 地址

Cisco Tools 栏

Config Editor/Viewer 用于下载、查看、比较、备份 Cisco 路由和交换机配置

Upload Config 用于上传 Cisco 路由和交换机配置，可用于修改配置

Download Config 用于下载 Cisco 路由和交换机配置

Running Vs Startup Configs 用于比较正在运行的和开机的配置文件

Router Password Decryption 用于解密 Cisco 的 type 7 型密码

Proxy Ping 用于测试 Cisco 路由器是否具有代理 ping 的能力

Advanced CPU Load 用于建立、查看 Cisco 路由器或交换机 CPU 工作状态数据库

CPU Gauge 用于监控 win2k、Cisco 路由器或交换机 CPU 工作

Router CPU Load 用于及时监控 Cisco 路由器的 cpu 工作

IP Network Browser 用于扫描于设定的 SNMP 团体字符串相同的路由器

Ping Tools 栏

Ping 用于 ping 主机

Trace Route 用于跟踪路由，查看经过的路由地址

Proxy Ping 用于测试 Cisco 路由器是否具有代理 ping 的能力

Ping Sweep 用于扫描一段 IP 中有哪些正在被使用，并显示出其 DNS 名字

Enhanced Ping 用于及时监视一定数量服务器、路由器等的相应能力

Address Mgmt 栏

Subnet Calculator 可以计算网络中的子网个数并显示其配置

IP Address Management 用于及时监控一段网络中 IP 的使用情况

DNS/Whois 用于获取一 IP 或域名的详细 DNS 信息

DNS Analyzer 用于显示 DNS 资源记录的等级结构

Ping Sweep 用于扫描一段 IP 中有哪些正在被使用，并显示出其 DNS 名字

DNS Audit 用于扫描定位本地 DNS 数据库错误

DHCP Scope Monitor 用于监控具有 DHCP 功能主机的子网络

Monitoring 栏

Watch It！用于 telnet、web 管理多个路由设备的工具条

Router CPU Load 用于及时监控 Cisco 路由器的 cpu 工作

Network Monitor 用于监控多个路由设备的多种工作状态参数

Network Performance Monitor 用于监控多个路由设备的各种详尽网络状态

Enhanced Ping 用于及时监视一定数量服务器、路由器等的相应能力

SysLog Server 用于察看、修改 514 UDP 端口接收到的系统 log

SNMP Trap Receiver 用于接收和显示 SNMP Trap 消息

Perf Mgmt 栏

Network Performance Monitor 用于监控多个路由设备的各种详尽网络状态

SNMP Graph 用于在 MIB 中及时的收集设定的 OID 的详细数据

Real-Time Interface Monitor 可以显示路由器和交换机接口的统计数据

Bandwidth Gauges 用仪表的形式监视远程设备的通路与带宽情况

Advanced CPU Load 用于建立、查看 Cisco 路由器或交换机 CPU 工作状态数据库

CPU Gauge 用于监控 win2k、Cisco 路由器或交换机 CPU 工作

MIB Browser 栏

MIB Browser 用于查看、编辑各种 MIB 数据资源

Update System MIB 用于改变各种 SNMP 设备的系统信息

SNMP Graph 用于在 MIB 中及时的收集设定的 OID 的详细数据

MIB Walk 用于收集指定 OID 的详细信息

MIB Viewer 用于查看各种 MIB 数据资源

Security 栏

Port Scanner 用于远程发现设备上 IP 端口的状态

Router Password Decrypt 用于解密 Cisco 的 type 7 型密码

Remote TCP Session Reset 用于显示各设备上的已激活连接

SNMP Brute Force Attack 用于暴力猜解路由器的登陆口令

SNMP Dictionary Attack 用于字典猜解路由器的登陆口令

SNMP traps 栏

SNMP Trap Receiver 用于接收和显示 SNMP Trap 消息

Trap Editor 用于修改 SNMP Trap 模版

Miscellaneous 栏

TFTP Server 用于建立 TFTP 服务器以接收、发送数据

WAN Killer 用于发送特定信息包

Send Page 用于发送 E-Mail 或 Page

Wake-On-LAN 用于远程激活网络功能

实验 10 用 H3C 智能管理中心管理网络

10.1 实验目的

⑴ 了解 H3C 智能管理中心软件的使用方法。

⑵ 理解 H3C 智能管理中心软件在网络管理、配置与维护中的作用和功能。

10.2 实验类型

验证型实验

10.3 实验环境

安装了 H3C 智能管理中心软件的 Windows 2000 系统，局域网、交换机。

10.4 实验内容与步骤

1 登陆 H3C 智能管理中心界面

直接运行 Web 浏览器，在地址栏中输入 http://192.168.4.112:8080/imc 或 https://192.168.4.112:8443/imc（IP 地址和端口号应与实际安装环境保持一致）。

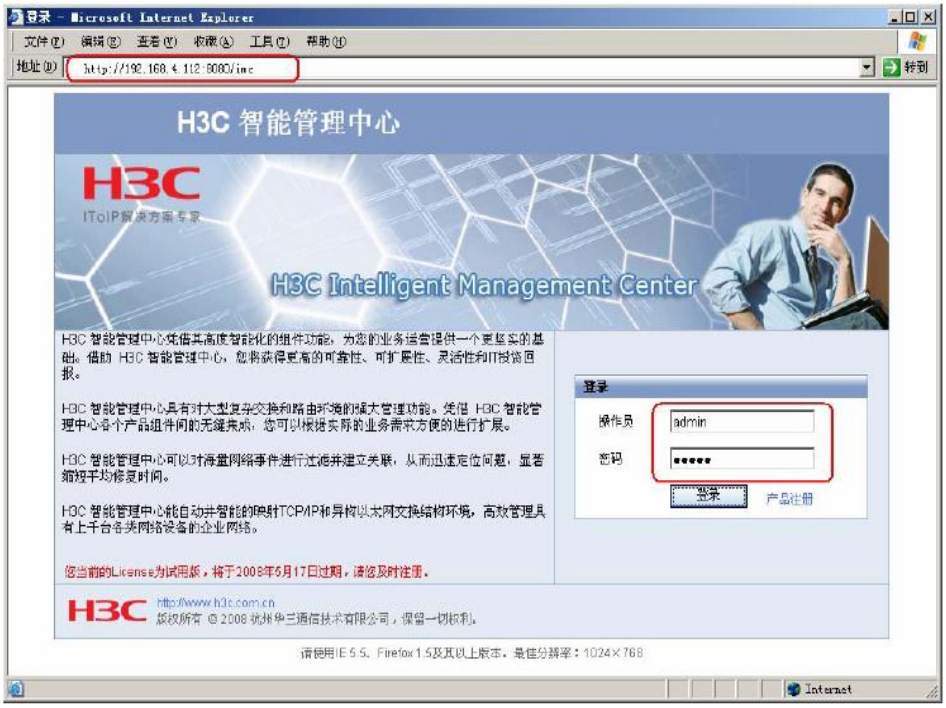

图 10-1 H3C 智能管理中心登陆界面

在登录页面中，输入正确的操作员和密码（例如，首次使用默认用户名和密码，都是 Admin）后单击<登录>按钮，即可进入系统首页。

2 发现网络中的设备

作为网络业务的承载者，网络设备是整个网络的“骨骼”，因此网络管理首先从向系统添加被管理设备开始。单击页面左侧“功能导航”栏中的<自动发现>按钮，进入自动发现简易模式页面，如图 10-2 所示。

图 10-2 自动发现简易模式页面

只需要输入种子设备 IP（可以输入一个或多个），即可查找到以种子设备为中心的三跳以内的设备。

3 熟悉 iMC 的管理界面

iMC 的配置界面如下图所示（以首页为例）。

图 10-3 iMC 配置界面

以自上而下从左到右的顺序，iMC 配置界面分为如下 5 个部分。

表 10-1 配置界面

序号	名称	说明
(1)	管理链接	显示了当前登录的操作员信息以及相关的功能链接。
(2)	功能页签	以不同的角度提供了各类管理功能的配置入口，方便管理员根据实际需要进行切换。
(3)	搜索栏	实现了对用户、设备、接口的搜索，同时支持多条件查询的高级搜索功能。
(4)	导航树	列出了当前功能页签对应的操作链接。首页中列出的是常用链接。
(5)	操作区	该区域主要用于信息展示以及相关功能的操作。

从图 10-3 中我们可以看到如下信息：

- 当前登录的操作员是 admin（鼠标移动到该名称之上可以查看当前操作员的登录时间和登录 IP 地址）；

- 自定义视图、设备视图的图标颜色与视图中严重级别最高的设备图标颜色一致。自定义视图快照中信息部所包含的设备运行正常（图标为绿色）；测试部、开发部、生产部视图下的某些设备产生了严重级别的告警（图标为红色）；财务部视图下的某些设备产生了重要级别的告警（图标为橙色）；
- 设备视图快照下按照类别列出了网络中各类设备的数量以及设备当前的严重级别；
- 设备状态快照中列出了处于不同严重级别的设备数量。
- 界面中的视图、设备类型图标或饼图均为链接，点击后在操作区中将显示其中包含的设备信息列表。如点击饼图中的绿色部分将显示所有状态正常的设备信息列表。

4 查看拓扑

单击页面左侧“网络拓扑”栏中的<网络拓扑>，将在新建窗口中打开用户自定义视图的拓扑。如图 10-4 所示。

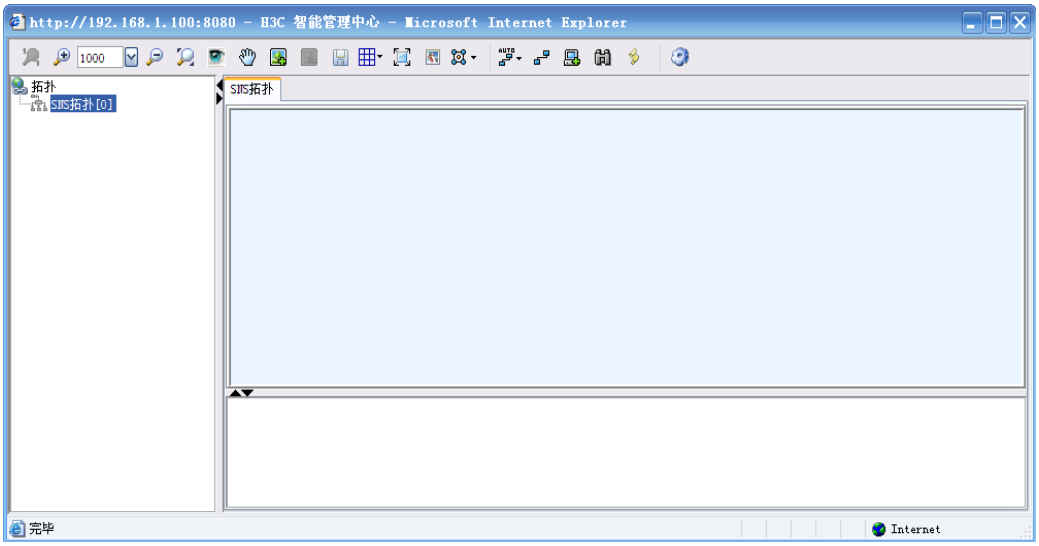

图 10-4 拓扑管理页面

5 在拓扑图中进行设备定位

点击导航树中的[所有设备]节点，打开路由器设备视图（其他视图类似），如下图所示。

图 10-5 路由器设备视图

点击图中的“操作”链接，在弹出菜单中选择[查看拓扑]菜单项，在选择拓扑显示的视图后，系统自动定位到该设备所在的位置。如下图所示。

图 10-6 设备拓扑定位

6 设备性能监控数据以及告警查询

点击图 10-6 中的任意一个设备标签链接，即可打开设备详细信息页面，如下图所示。


设备详细信息
设备标签 1.2.3.67 [修改]
系统名称 3com4400 [修改]
设备状态 严重
sysOID 1.3.6.1.4.1.43.10.27.4.1.2.4
IP地址 1.2.3.67
掩码 255.255.255.0
联系人
位置 beijing
运行时间 0天23小时47分钟31秒210毫秒
设备型号 3Com S4400
类型 交换机
硬件版本 05.07.00
产品号 3C17205
序列号 L6LV4GB837B20
最后轮询时间 2008-10-08 17:54:47
系统描述 3Com SuperStack 3
接口数量 33 接口列表
100 %
今天的不可达比例 7 30
7.5
5.0
2.5
0.0
未恢复告警
紧急 重要 次要 警告
动作
同步
刷新
取消管理
删除
Telnet
Web网管
Ping
路由跟踪
拓扑定位
配置接入设备
SSH
打开设备面板
配置
修改设备标签
修改系统组属性
修改SNMP参数
修改Telnet参数
修改轮询时间
修改Ping参数
性能监视
基础性能数据一览表
更改基础性能监视项
取消基础性能监视
监视指标阈值设置
设备基本信息
地址转换表
IP地址表
TCP连接表
IP路由表
监控信息
定制
服务监控
共有0条记录。
最近10条未恢复告警
更多
级别 告警信息 告警时间
次要 性能任务（设备不可达性比例，性能指标：设备不可达性比例(%)）中设备（1.2.3.67）实例（[.0]）超过阈值10，当前值为100。 2008-10-14 08:51:46
次要 性能任务（设备不可达性比例，性能指标：设备不可达性比例(%)）中设备（1.2.3.67）实例（[.0]）超过阈值10，当前值为100。 2008-10-13 08:49:47
重要 性能任务（设备不可达性比例，性能指标：设备不可达性比例(%)）中设备（1.2.3.67）实例（[.0]）超过阈值50，当前值为100。 2008-10-10 08:47:37
次要 性能任务（设备不可达性比例，性能指标：设备不可达性比例(%)）中设备（1.2.3.67）实例（[.0]）超过阈值10，当前值为100。 2008-10-10 08:47:37
重要 性能任务（设备不可达性比例，性能指标：设备不可达性比例(%)）中设备（1.2.3.67）实例（[.0]）超过阈值50，当前值为100。 2008-10-09 14:50:01
次要 性能任务（设备不可达性比例，性能指标：设备不可达性比例(%)）中设备（1.2.3.67）实例（[.0]）超过阈值10，当前值为100。 2008-10-09 14:50:01
重要 性能任务（设备不可达性比例，性能指标：设备不可达性比例(%)）中设备（1.2.3.67）实例（[.0]）超过阈值50，当前值为100。 2008-10-08 18:06:20
次要 性能任务（设备不可达性比例，性能指标：设备不可达性比例(%)）中设备（1.2.3.67）实例（[.0]）超过阈值10，当前值为100。 2008-10-08 18:06:20
紧急 设备1.2.3.67不可达。 2008-10-08 17:56:54
重要 性能任务（设备不可达性比例，性能指标：设备不可达性比例(%)）中设备（1.2.3.67）实例（[.0]）超过阈值50，当前值为100。 2008-10-07 18:11:40
基础性能监视
更详细数据
监视指标 监视值 操作
设备今天不可达比例 100.000% 停止监视
设备当前响应时间 无响应 停止监视
最近一小时接收IP报文速率平均值 -- 启动监视
最近一小时转发IP报文速率平均值 -- 启动监视
最近一小时输入IP报文丢弃率平均值 -- 启动监视
最近一小时输出IP报文丢弃率平均值 -- 启动监视

图 10-7 设备详细信息

(1) 设备告警信息

对于设备是否正常运行的关键告警，系统通过图形、列表两种形式展示给用户。点击上图中的柱状图，页面将自动跳转到“告警”页签中该设备的相关等级的全部告警信息，方便管理员及时查看相关告警信息。

(2) 性能监控信息

此外，可以查看该设备关键的监视数据。性能数据位于该页面的最下方。同时，可以通过点击右上角的“更详细数据”链接查看该设备的所有性能数据。

(3) 攻击告警信息

可以选择“业务”页签，点击导航树中[实时攻击告警监控]进入业务监控中心，查看来自整个网络的攻击告警信息，并制定相应处理策略。

7 iMC 的操作员管理

点击“系统管理”中的操作员功能节点，点击其中的增加按钮，如下图所示。也可以删除操作员。

图 10-8 增加操作员

10.5 思考题

(1) H3C 智能管理中心使用了哪些核心技术进行网络的管理？

(2) 和 SolarWinds 这样的通用网管平台相比，它有什么优点和缺点？

实验 11 网络通信流量监视

11.1 实验目的

⑴ 理解网络通信流量监视的基本方法。

⑵ 使用多种工具实现本地网内的主机间通信矩阵、主机通信流量统计、协议统计。

11.2 实验类型

验证型实验

11.3 实验环境

安装了 Windows 2000/xp/2003 系统的主机、局域网、交换机。Sniffer Pro 软件。

11.4 实验内容与步骤

1 运行 Sniffer Pro，选择相应网卡；

2 选择 Monitor → Matrix，点击 IP 标签，在左边竖边条中选择 Map，观察当前网络中主机通信矩阵；

3 选择 Monitor → Matrix，点击 IP 标签,左边竖边条中选择 Outline，观察主机间流量；

4 选择 Monitor → Protocol Distribution，在左边竖边条中选择相应的查看方式观察协议分布。

11.5 实验结果

1 观察主机间通信，并完成通信矩阵，填入表 11-1。

表 11-1 路由器设备视图

	主机一	主机二	主机三	主机四	主机五
主机一	——	Bytes	Bytes	Bytes	Bytes
主机二	Bytes	——	Bytes	Bytes	Bytes
主机三	Bytes	Bytes	——	Bytes	Bytes
主机四	Bytes	Bytes	Bytes	——	Bytes
主机五	Bytes	Bytes	Bytes	Bytes	——

A、在主机下方的空格中填上主机的 IP

B、如果某两台主机之间存在通信，请在交叉处的第一个方格中打勾

C、在交叉处第二个方格出填入观察时的通信流量

2 主机间流量统计，完成流量统计表格，完成表 11-1。

3 观察并统计各个协议分布，统计当前流量最大的五种协议，及各种协议所占比重，完成表 11-2。

表 11-2 协议分布

网络中存在的协议有					
各种协议的比重					

参考文献

[1] 《网络管理》（第 3 版），郭军主编，2008 年，北京邮电大学出版社

[2] 《计算机网络与Internet实验教程》，郭银章主编，2008年，机械工业出版社