《计算机网络》实验指导

实验六：SNMP 协议分析

一、实验目的

1、掌握 SNMP 协议基本内容和通信过程；

2、理解 MIB 的工作原理，并熟悉 Windows 操作系统的基本 MIB 信息；

3、理解网络监测的基本原理。

二、实验学时

2 学时

三、实验类型

创新性

四、实验需求

1、硬件

每人配备计算机 1 台，计算机接入实验室局域网，每小组配备二层交换机 1 台。

2、软件

Windows 7 操作系统，安装 Wireshark 软件。

3、网络

支持对互联网的访问。

4、工具

无

五、实验理论

1、应用层的基本理论；

2、UDP 通信的基本理论；

3、SNMP 协议和 MIB 的基本理论和基本内容；

4、对象标识 OID 的基本知识。

六、预备知识

1、网络嗅探工具 Wireshark 的使用方法；

2、Windows 系统上常用的 SNMP OID；

表 6-1 Windows 系统上常用的 SNMP OID

序号	监控点名称	OID	数值	增量单位
1	CPU 使用情况			

		…		
2	物理内存			
		…		
3	虚拟内存			
		…		
4	网络接口			
		…		
5	进程信息			
		…		
…	…	…	…	…

要求：

请查阅相关资料完善表 6-1 的设计，并填写具体内容，将结果填写到实验报告册中。

3、请查阅相关资料，列举三种基于 SNMP 协议的网络管理软件，并填写表 6-2 基于 SNMP 协议的网络管理软件对比分析一览表。

表 6-2 基于 SNMP 协议的网络管理软件对比分析一览表

序号	软件名称	版本号	软件开发商	安装环境
1				
2				
3				

要求：

请查阅资料完成表 6-2 的具体内容，并将结果填写到实验报告册中。

七、实验任务

1、完成 Windows 操作系统下 SNMP 客户端的安装与配置；

2、掌握 SNMP 请求发送的方法，并完成对 SNMP 协议的分析；

3、通过数据报文分析 SNMP 协议的通信过程。

八、实验内容及步骤

说明：本实验指导所使用的二层交换机为神州数码 DCS-3950，所有实验操作和命令都以此为基础。本实验最低需要 1 台 DCN DCS-3950、6 台主机支持。

1、Windows 操作系统下 SNMP 客户端的安装与配置

（1）本部分以 Windows 7 操作系统为例，进行配置。

（2）打开【控制面板】【程序】【打开或关闭 Windows 功能】，如图 6-1 所示。

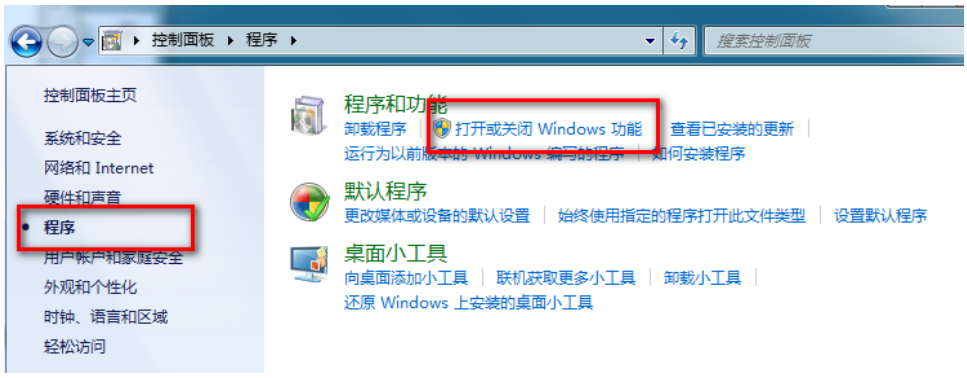

图 6-1 安装 SNMP 的准备

（3）选择【简单网络管理协议（SNMP）】后，点击【确定】按钮，进行安装。如图 6-2 所示。

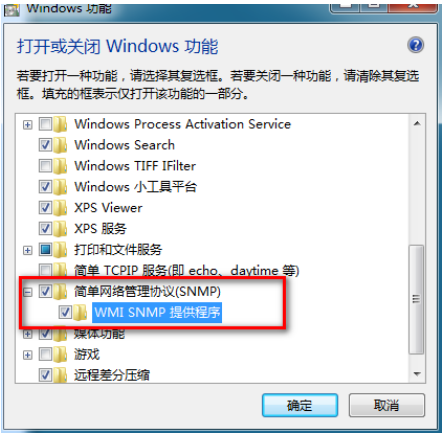

图 6-2 安装 SNMP 客户端

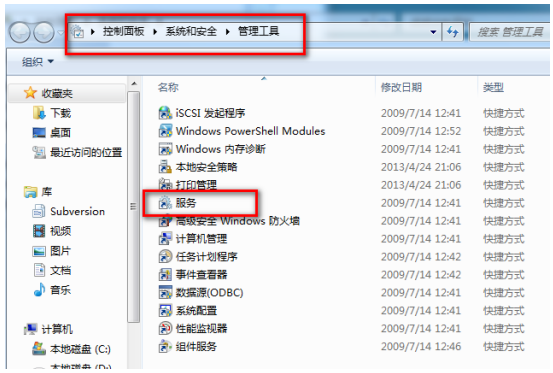

图 6-3 打开服务管理器

（4）打开【控制面板】【系统和安全】【管理工具】，双击打开【服务】。如图 6-3 所示。

（5）在【服务】窗口中，双击【SNMP Service】服务，开始对 SNMP 进行配置。

（6）在【陷阱】选项卡中，填写社区名称为“**NetworkMonitor**”，点击按钮【添加到列表】。

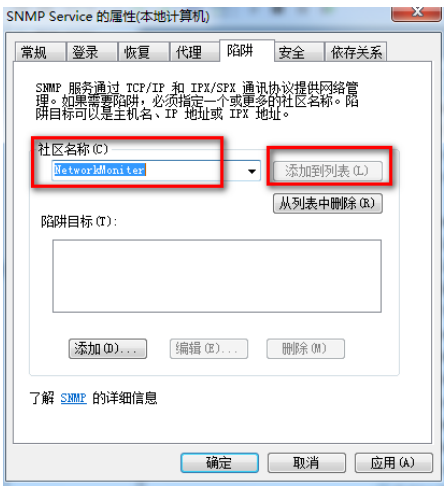

图 6-4 配置 SNMP 的陷阱

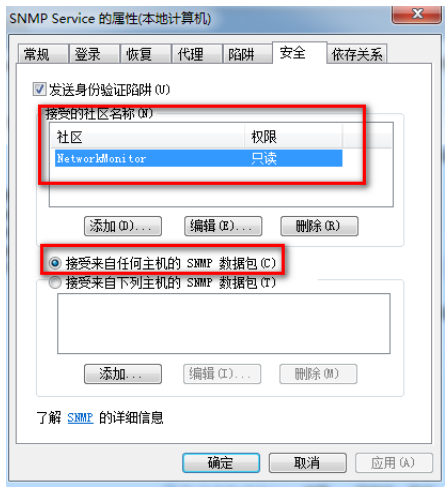

图 6-5 配置 SNMP 的安全

如图 6-4 所示。*（此步骤可以省略，请分析原因。）*

（7）在【安全】选项卡中，选择【添加】按钮，添加一个新的共同体“**NetworkMonitor**”，并选择【接受来自任何主机的 SNMP 数据包】。如图 6-5 所示。

（8）选择【应用】和【确定】按钮，完成配置。

（9）在【服务】窗体中，选择“SNMP Service”服务，点击【重启动此服务】，对 SNMP 服务进行重新启动，使得配置生效。如图 6-6 所示。

图 6-6 重启动 SNMP Service 服务

（10）至此，该 Windows 操作系统可以通过共同体名称响应来自任何主机的 SNMP 请求。

2、安装 Net-SNMP

（1）获得 Net-SNMP 软件

软件可以通过官方网站获得，Net-SNMP 官方网站：http://www.net-snmp.org

上述软件，也可以通过课程网站（http://ke.51xueweb.cn/Network.html）获得。

并按照提示安装 Net-SNMP。

（2）根据提供的资料，掌握 Net-SNMP 的基本功能和命令使用方法。

（3）至此，该操作系统可以通过 Net-SNMP 的 SNMPWALK 工具发送 SNMP 请求报文。

要求：

请查阅相关资料，完成（2）的要求，将答案填写到实验报告册中。

3、使用 Net-SNMP 工具进行数据采集

（1）启动 Windows 命令行工具。

（2）在命令行中输入“**snmpwalk -v 2c -c NetworkMonitor localhost .1.3.6.1.2.1.1**”后回车确认。此命令是通过 Net-SNMP 工具向本地主机发送了一个 SNMP 请求，MIB 的信息为.1.3.6.1.2.1.1。

（3）查看获得的信息，并填写表 6-3 通过 SNMP 请求获得 Windows 系统的基本信息。

表 6-3 通过 SNMP 请求获得 Windows 系统的基本信息

序号	字段名	字段值	字段解释和说明
1			

2			
3			
4			
5			
6			
7			
8			

要求：

请完成表 6-3 的填写，并将结果填写到实验报告册中。

（4）请通过 Net-SNMP 工具得到本机的运行情况，并完成表 6-4 本机设备运行状态一览表。

表 6-4 本机设备运行状态一览表

序号	字段名	字段值	字段解释和说明
1			
2			
3			
…			

要求：

请完成表 6-4 的具体内容，至少应包括本地主机的 CPU、内存、虚拟内存、磁盘、网络接口、进程数信息，并将结果填写到实验报告册中。

5、SNMP 报文分析

（1）启动 Wireshark，在 Filter 中输入“snmp.community=="NetworkMonitor"”，选择【Start】按钮，开始数据报文采集，选择左上角红色按钮停止报文采集。如图 6-7 所示。

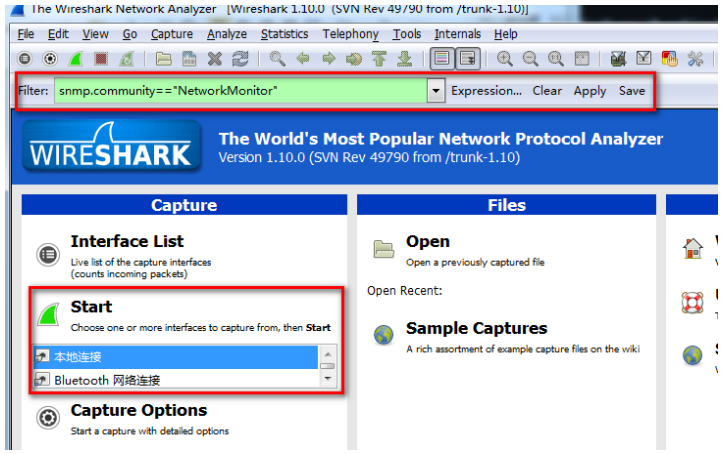

图 6-7 通过 Wireshark 工具进行 SNMP 协议的报文采集

（2）启动 Windows 命令行工具。

（3）在命令行中输入“**snmpwalk -v 2c -c NetworkMonitor localhost .1.3.6.1.2.1.1**”后回车确认。此命令是通过 Net-SNMP 工具向本地主机发送了一个 SNMP 请求，MIB 的信息为.1.3.6.1.2.1.1。

此时通过 SNMP 请求获得了本机信息，但是 Wireshark 却没有采集到任何数据。如图 6-8 所示。

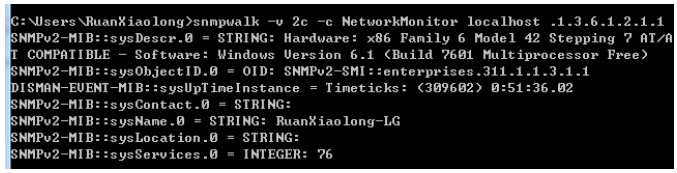

图 6-8 SNMP 请求查看本地主机的基本信息

（4）在命令行中输入“**snmpwalk -v 2c -c NetworkMonitor 172.16.1.* .1.3.6.1.2.1.1**”后回车确认。此命令是通过 Net-SNMP 工具向本小组其他计算机发送了一个 SNMP 请求，MIB 的信息为.1.3.6.1.2.1.1。此时通过 SNMP 请求获得了对方计算机的信息， Wireshark 采集到 SNMP 通信的数据报文。如图 6-9 所示。

要求：

1、使用 SNMPWALK 向本地主机发送 SNMP 请求，为什么 Wireshark 采集不到数据报文？

2、使用 SNMPWALK 向网络内的其他主机发送 SNMP 请求，哪些情况下会无法得到响应？应该如何解决？

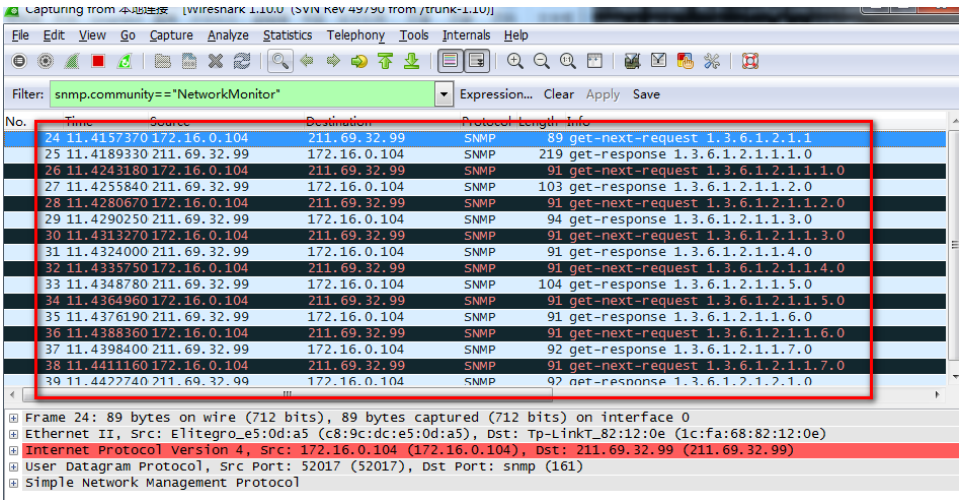

图 6-9 SNMP 数据报文

3、SNMP 协议使用的传输控制协议是什么？端口号是多少？

请查阅相关资料，回答上述 3 个问题，并将答案填写到实验报告册中。

（5）分析步骤（4）中采集到的数据报文，填写表 6-5。

表 6-5 一次 SNMP 解析请求过程

序号	发送时间	来源 IP	目的 IP	报文具体作用和描述
1				
2				

3				
4				
5				
6				
7				
8				
…				

要求：

请根据实验结果完成表 6-5 的具体内容，并将结果填写到实验报告册中。

九、实验分析

1、SNMP v1、v2 和 v3

（1）SNMP 都有哪些版本？这些版本分别有那些差异和不同？

（2）不同版本的 SNMP 协议，其报文结构和通信过程是否一致？

（3）本实验是使用 SNMP 的什么版本进行的？

要求：

1、请按照（1）的要求绘制表格，对比分析 SNMP 各个版本的差异，并将表格填写到实验报告册中。

2、请按照（2）(3）2 个要求，回答上述问题，并将结果填写到实验报告册中。

2、SNMP 的安全性

（1）SNMP 在通信过程中是否安全？有哪些安全风险？

（2）SNMP 协议是如何提高自身安全性的？

（3）SNMP 在局域网和广域网的环境中，通信过程是否有差异？

要求：

请查阅相关资料，回答上述 3 个问题，并将答案填写到实验报告册中。

3、公有 MIB 库与私有 MIB 库

（1）常见公有 MIB 库有哪些？遵循什么标准？

（2）私有 MIB 库与公有 MIB 库的区别是什么？

要求：

请查阅相关资料，回答上述 2 个问题，并将答案填写到实验报告册中。

十、课外自主实验

1、配置交换机 DCS-3950 支持 SNMP

（1）SNMP 是否可以查看交换机、路由器等网络设备的信息？

（2）请使用 DCS-3950 交换机为基础，配置该交换机的 SNMP 服务。

（3）请使用 Net-SNMP 的 SNMPWALK 工具访问交换机的信息，并完成表 6-6。

表 6-6 交换机运行状态一览表

序号	字段名	字段值	字段解释和说明
1			
2			
3			
…			

（4）不同品牌的交换机的 MIB 信息一致么？网络设备的 MIB 信息应该从哪里获得？

要求：

1、请按照（2）的要求，配置 DCS-3950 的 SNMP 服务，并将具体的配置命令填写到实验报告册中。

2、请按照（3）的要求，进行具体实验完成表 6-6 的填写，并将实验结果和实验分析的具体内容填写到实验报告册中。

3、请按照（1）（4）2 个要求，回答上述问题，并将答案填写到实验报告册中。

2、安装 SNMP 网络管理工具：PRTG

（1）获得并安装 PRTG，PRTG 软件可通过官方网站获得；

（2）使用 PRTG 对本机设备进行监控；

（3）使用 PRTG 对自主实验 1 中的交换机设备进行监控。

要求：

1、请按照（1）的要求，自主获取 PRTG 软件进行安装，并将具体的安装步骤填写到实验报告册中。

2、请按照（2）的要求，通过查阅 PRTG 软件使用文档，进行设置，监控 SNMP，并将具体的实验步骤填写到实验报告册中。

十一、实验扩展资源

1、图书

（1）网络协议分析与实现 胡维华 高等教育出版社

（2）简单网络管理协议教程 Sean Harnedy 电子工业出版社

（3）SNMP 简单网络管理协议 李明江 电子工业出版社

（4）精通 SNMP 武孟军 人民邮电出版社

2、文章

（1）基于 SNMP 协议网络设备信息的采集 田雷 《吉林大学》2009 年

（2）简单网络管理协议 SNMP 浅析 尚建贞 逯晖 《计算机时代》2011 年 07 期

（3）基于 SNMP 协议的网络拓扑发现算法的研究 杨凯 马季兰 《电脑开发与应用》

2008 年 03 期

（4）基于 SNMP 协议的 Web 监控系统 师鸿博 《南京邮电大学》2011 年

3、互联网资源

（1）协议分析网：http://www.cnpaf.net/Class/ProtocolAll/

（2）中国网管联盟：www.bitscn.com/network/

（3）Wireshark 官方文档：http://www.wireshark.org/docs/

4、电子资源下载

课程网站：ke.51xueweb.cn/Network.html。