实验九：SNMP 协议分析

一、实验目的

1、理解 SNMP 协议基本内容和通信过程；

2、掌握 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

综合型

四、实验需求

1、硬件

每人配备计算机 1 台。

2、软件

Windows 7 以上操作系统，安装 Wireshark 网络嗅探软件，安装 Net-SNMP 软件。

3、网络

实验室局域网支持，能够访问校园网，能够访问互联网。

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；

4、对象标识 OID 的基本知识。

六、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。

七、实验内容及步骤

1、Windows 操作系统下 SNMP 客户端的安装与配置

（1）本实验以 Windows 7 操作系统为例，进行 SNMP 的安装与配置。

（2）打开【控制面板】【程序】【打开或关闭 Windows 功能】，如图 9-1 所示。

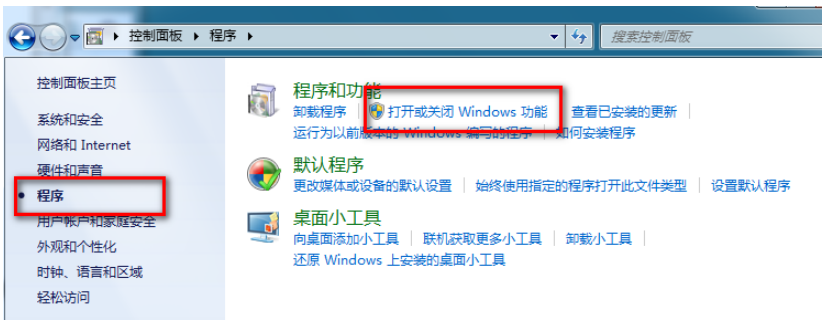

图 9-1 安装 SNMP 的准备

（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 9-2 所示。

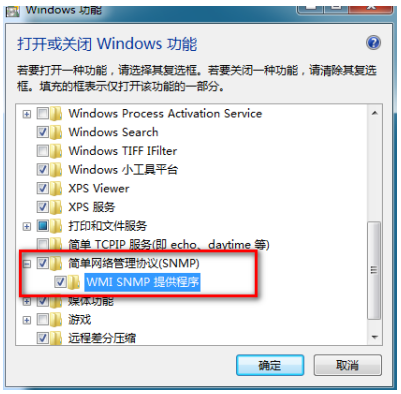

图 9-2 安装 SNMP 客户端

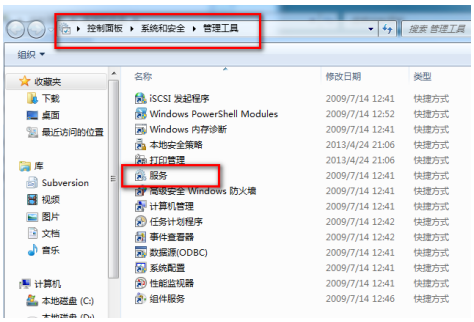

图 9-3 打开服务管理器

（4）打开【控制面板】【系统和安全】【管理工具】，双击打开【服务】，如图 9-3 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】，如图 9-4 所示。

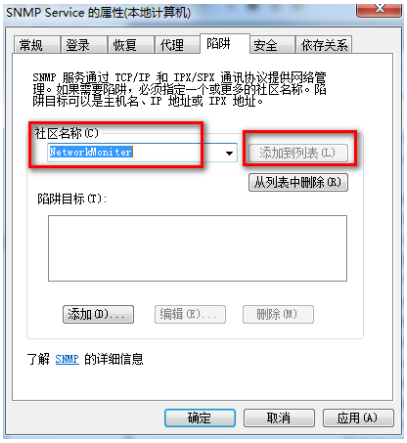

图 9-4 配置 SNMP 的陷阱

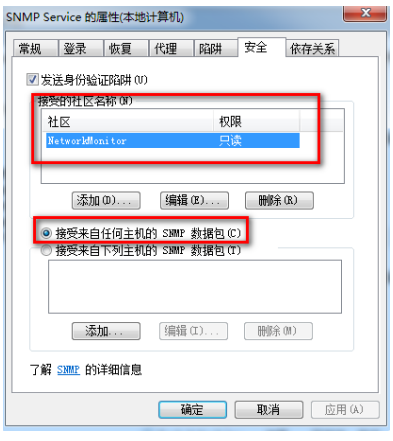

图 9-5 配置 SNMP 的安全

（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 9-5 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 9-6 所示。

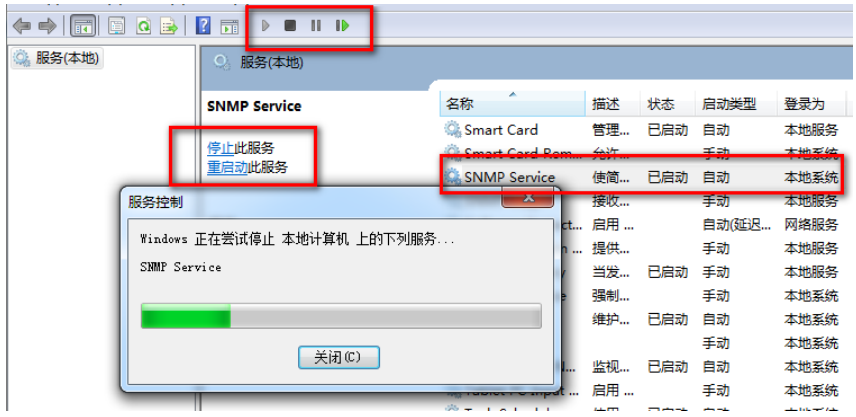

图 9-6 重启动 SNMP Service 服务

（10）至此，该 Windows 操作系统可以响应来自其他主机的 SNMP 请求。

2、安装 Net-SNMP

（1）下载安装包

可通过官方网站（http://www.net-snmp.org）获得 Net-SNMP 软件安装程序；

可通过本课程网站（http://network.ke.51xueweb.cn）下载本教程所使用的软件版本。

（2）安装 Net-SNMP。

a、双击 Net-SNMP 安装程序，进入如图 9-7 所示的 Net-SNMP 安装界面，点击【Next >】开始进行安装。点击【I accept …】，同意安装，如图 9-8 所示。点击【Next >】，选择默认安装组件，如图 9-9 所示。

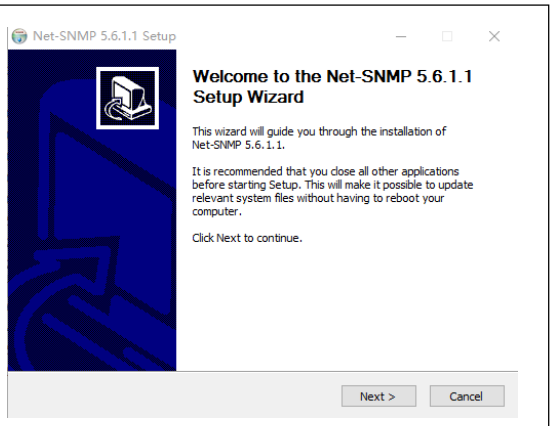

图 9-7 安装提示

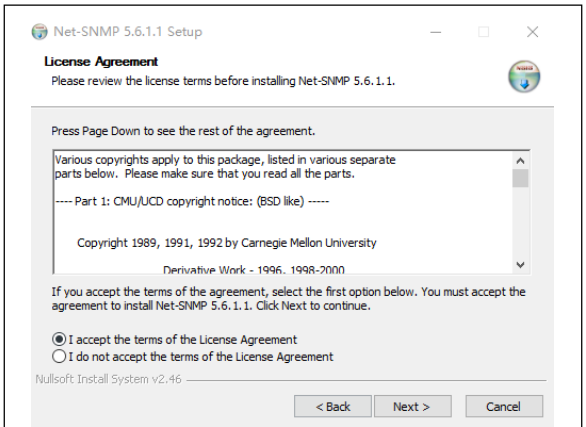

图 9-8 同意安装

b、用户可使用默认的 Net-SNMP 安装目录，也可自行修改默认路径，如图 9-10 所示。

c、Net-SNMP 软件安装过程，如图 9-11 所示，安装完成后如图 9-12 所示。

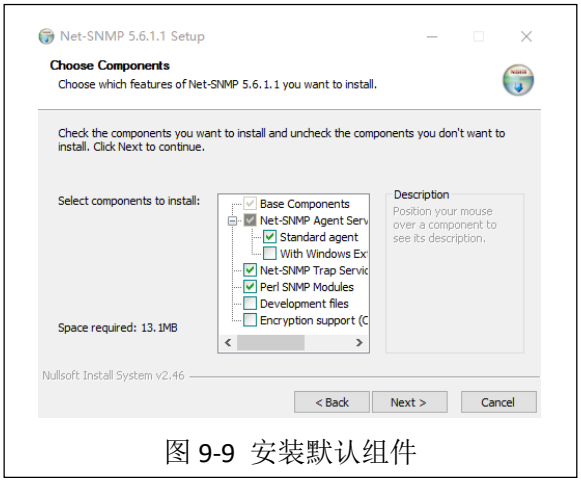

图 9-9 安装默认组件

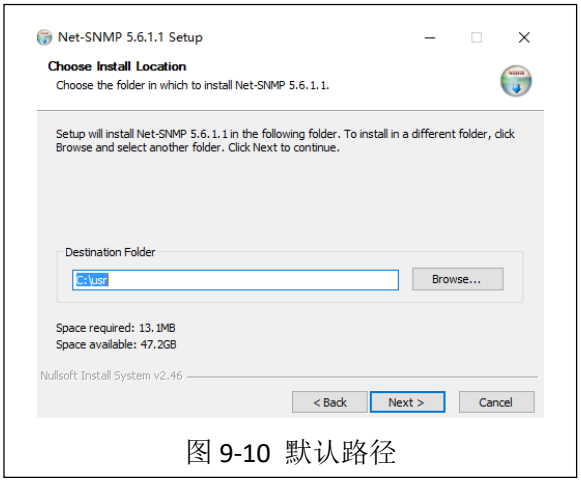

图 9-10 默认路径

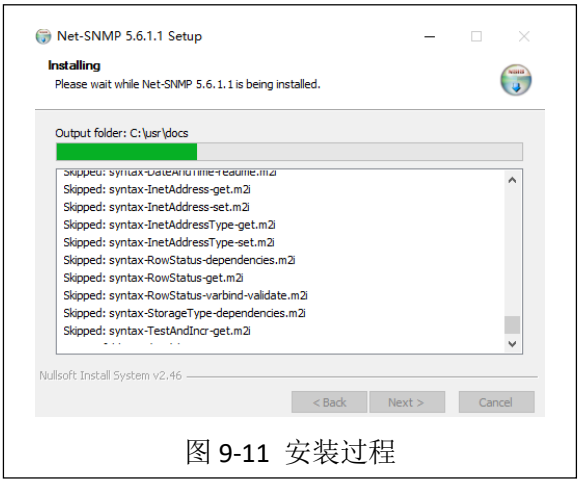

图 9-11 安装过程

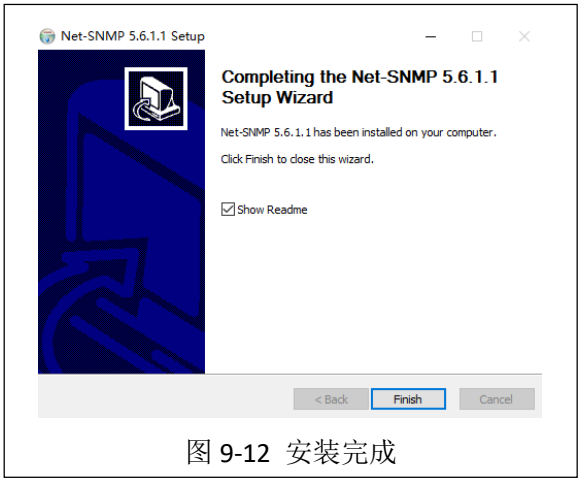

图 9-12 安装完成

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 9-1 通过 SNMP 请求获得 Windows 系统的基本信息。

表 9-1 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			

（4）通过指定 OID 的方式进行 Windows 系统基本信息的采集。

例如，“snmpget -v 2c -c NetworkMonitor localhost {系统名的 OID}”可以采集 Windows 系统的系统名信息；查看采集的信息，并将 SNMP 请求获得的 Windows 操作系统的信息填写到表 9-2 中。

表 9-2 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	系统描述		
2	系统的私有 OID		
3	系统运行时间		
4	系统联系人		
5	系统名称		
6	系统位置		
7	系统服务数		
8	系统时间		
9	系统用户数		
10	系统进程		
11	系统最大进行数		
12	硬盘总大小		
13	硬盘使用情况		
14	物理内存大小		
15	物理内存使用情况		

4、SNMP 报文分析

（1）启动 Wireshark，在【Filter】中输入

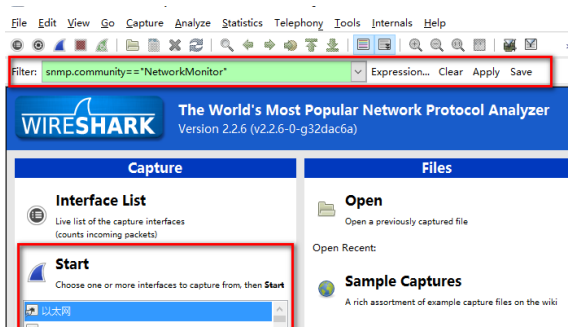

图 9-13 通过 Wireshark 工具进行 SNMP 协议的报文采集

“snmp.community=="NetworkMonitor"”，选择【Start】按钮，开始数据报文采集。如图 9-13 所示。

（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 9-14，9-15 所示。

```
C:\Users\helulu>snmpwalk -v 2c -c NetworkMonitor localhost .1.3.6.1.2.1.1
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: Intel64 Family 6 Model 78 Stepping 3 AT/A
T COMPATIBLE - Software: Windows Version 6.3 (Build 10586 Multiprocessor Free)
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.311.1.1.3.1.1
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1955927) 5:25:59.27
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: helulu
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 76
```

图 9-14 SNMP 请求查看本地主机的基本信息

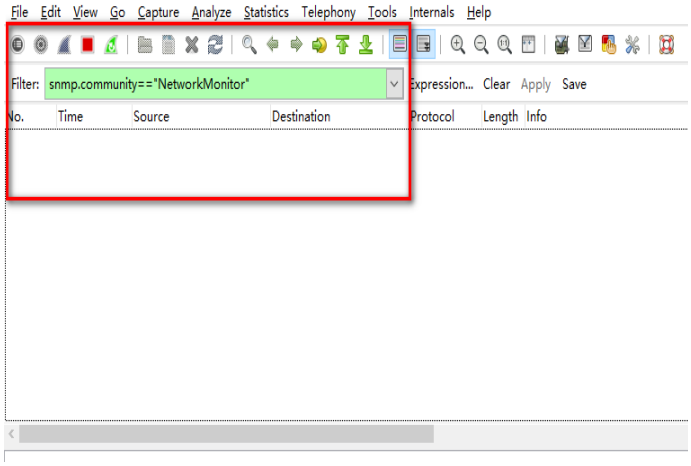

图 9-15 SNMP 数据报文

（4）在命令行中输入“**snmpwalk -v 2c -c NetworkMonitor 192.168.157.194 .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 通信数据报文，如图 9-16 所示。

（5）从获取的 UDP 数据报文中任意选择其中一条数据报文，对该数据报文进行详细分析，填写表 9-3，9-4。

表 9-3 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				
…				

表 9-4 一次 SNMP 解析响应过程

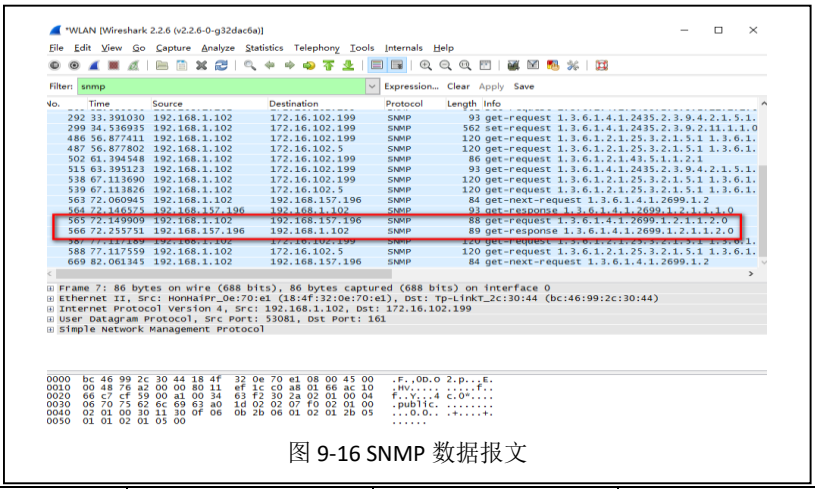

图 9-16 SNMP 数据报文

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				
…				

八、实验分析

1、为什么使用 Net-SNMP 能够采集到本机信息，但无法通过 Wireshark 获取到数据报文？

2、SNMP v1、v2 和 v3

（1）SNMP 都有哪些版本？这些版本分别有那些差异？

（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？

3、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？

4、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？