1

《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 | | |
|---|------|------|--|
| 2 | | | |
| 2 | 虚拟内存 | | |
| 5 | | | |
| 4 | 网络接口 | | |
| 4 | | | |
| F | 进程信息 | | |
| 5 | | | |
| | | | |

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

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



(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





- (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"<u>NetworkMonitor</u>",点击按钮【添加到列表】。

| SNMP Service 的雇性(本地计算机) | SNMP Service 的雇性(本地计算机) |
|--|---|
| 常规 登录 恢复 代理 陷阱 安全 依存关系 | 常规 登录 恢复 代理 陷阱 安全 依存关系 |
| SWAP 服务通过 TCP/IP 和 IPX/SPX 通讯协议提供网络管理。如果需要PGH,必须指定一个或更多的社区名称。陷阱目标可以是主机名、IP 地址或 IPX 地址。 | ☑ 发送身份验证和讲(0) 接受的社区名称(0) 社区 和限 |
| 社区名称 (C) Networkdoniter | Networkflonitor 只读 |
| 从列表中聯係 (B) 路明目标 (T): | 添加 (0) 編編 (2) 剛除(3) ● 接受来自任何主机的 SMMP 数据包 (2) ● 接受来自任何主机的 SMMP 数据包 (2) |
| <mark>添加 @)</mark> 編輯 (E) 前除 M) 了解 SMME 的详细信息 | |
| | · · · · · · · · · · · · · · · · · · · |
| 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。

| | 0 | 2 🖬 🕨 🗖 1 | 1 10 | | | | | | |
|----------|----------|--------------|------------|---------------------|----|-----|-----|---------|------|
| 🔍 服务(本地) | | 0。服务(本地) | _ | | | | | | |
| | | SNMP Service | | 名称 | | 描述 | 状态 | 启动类型 | 登录为 |
| | | 停止此服务 | | Smart Card | | 管理 | 已启动 | 自动 | 本地服务 |
| | | 重启动此服务 | | SNMP Service | | 使简 | 已启动 | 自动 | 本地系统 |
| | 服务控制 | | | × | | 接收 | | 手动 | 本地服务 |
| | | | | | ct | 启用 | | 自动(延迟 | 网络服务 |
| | Windows | 止在宏试得止 本地10 | +算机 上的下列服务 | ř | n | 提供 | | 手动 | 本地服务 |
| | SNMP Ser | vice | | | 1 | 当发 | 已启动 | 手动 | 本地服务 |
| | | | | | e | 强制 | | 手动 | 本地系统 |
| | | | | | | 维护 | 已启动 | 自动 | 本地系统 |
| | | | | | | | | 手动 | 本地系统 |
| | | | 关闭(C) | | 1 | 监视 | 已启动 | 自动 | 本地系统 |
| | | | | ing rabiet i e inpe | at | 启用 | | 手动 | 本地系统 |
| | | | | | | 4-m | | <u></u> | |
| | | 图 6-6 | 5 重启动 SN | MP 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

2、安装 Net-SNMP

求。

(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 "<u>snmpwalk -v 2c -c NetworkMonitor localhost .1.3.6.1.2.1.1</u>"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 | | | |

4

| 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。

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

表 6-4 本机设备运行状态一览表

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"<u>snmp.community=="NetworkMonitor</u>"",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。

| 🔷 🚡 🖳 🗐 🕞 I C, Q, 🔍 🔛 📓 🖾 I | 8 % | | | | | | | |
|---|--|--|--|--|--|--|--|--|
| Expression Clear Apply Save | | | | | | | | |
| WIRESHARK The World's Most Popular Network Protocol Analyzer Version 1.10.0 (SVN Rev 49790 from /trunk-1.10) | | | | | | | | |
| Files | | | | | | | | |
| Open Open a previously captured file | | | | | | | | |
| Sample Captures | | | | | | | | |
| A rich assortment of example capture files on the wiki | | | | | | | | |
| Capture Options Start a capture with detailed options | | | | | | | | |
| | Expression Clear Apply Save Expression Clear Apply Save Set Popular Network Protocol Analyzer Rev 49790 from /trunk-1.10) Files Open Open a previously captured file Open Recent: Sample Captures A rich assortment of example capture files on the wiki | | | | | | | |

(2) 启动 Windows 命令行工具。

6

(3)在命令行中输入"<u>snmpwalk -v 2c -c NetworkMonitor localhost .1.3.6.1.2.1.1</u>"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

| | C:\Users\RuanXiaolong>snmpwalk −v 2c −c NetworkMonitor localhost .1.3.6.1.2.1.1 |
|---|--|
| | SNMPv2-MIB::sysDescr.0 = STRING: Hardware: x86 Family 6 Model 42 Stepping 7 AT/A |
| | T COMPATIBLE - Software: Windows Version 6.1 (Build 7601 Multiprocessor Free) |
| | SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.311.1.1.3.1.1 |
| | DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (309602) 0:51:36.02 |
| | SNMPv2-MIB::sysContact.0 = STRING: |
| | SNMPv2-MIB::sysName.0 = STRING: RuanXiaolong-LG |
| | SNMPv2-MIB::sysLocation.0 = STRING: |
| | SNMPv2-MIB::sysServices.0 = INTEGER: 76 |
| ľ | |
| | 图 6-8 SNMP 请求查看本地主机的基本信息 |

所示。

(4) 在命令行中输入"<u>snmpwalk -v 2c -c NetworkMonitor 172.16.1.* .1.3.6.1.2.1.1</u>"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?

| | 💿 🔏 🔳 🙋 📄 🛅 💥 🤔 er: snmp.community=="NetworkMonito | 🔍 🔃 幹 📦 🚡 👱 or" | Expressio | l Q @ ∰ ⊠ 18 % ∰ n Clear Apply Save | |
|-----|---|----------------------|-------------|---|---|
| lo. | Time Source | Destination | Protocol | Length Info | |
| _ | 24 11.4157370 172.16.0.104 | 211.69.32.99 | SNMP | 89 get-next-request 1.3.6.1.2.1.1 | |
| | 25 11.4189330 211.69.32.99 | 172.16.0.104 | SNMP | 219 get-response 1.3.6.1.2.1.1.1.0 | |
| _ | 26 11.4243180 172.16.0.104 | 211.69.32.99 | SNMP | 91 get-next-request 1.3.6.1.2.1.1.1.0 | |
| | 27 11.4255840 211.69.32.99 | 1/2.16.0.104 | SNMP | 103 get-response 1.3.6.1.2.1.1.2.0 | |
| | 28 11.42806/01/2.16.0.104 | 172 16 0 104 | SNMP | 91 get-next-request 1.3.6.1.2.1.1.2.0 | |
| | 30 11.4313270 172.16.0.104 | 211.69.32.99 | SNMP | 91 get-next-request 1.3.6.1.2.1.1.3.0 | |
| | 31 11,4324000 211,69,32,99 | 172.16.0.104 | SNMP | 91 get-response 1, 3, 6, 1, 2, 1, 1, 4, 0 | |
| | 32 11.4335750 172.16.0.104 | 211.69.32.99 | SNMP | 91 get-next-request 1.3.6.1.2.1.1.4.0 | |
| | 33 11.4348780 211.69.32.99 | 172.16.0.104 | SNMP | 104 get-response 1.3.6.1.2.1.1.5.0 | |
| | 34 11.4364960 172.16.0.104 | 211.69.32.99 | SNMP | 91 get-next-request 1.3.6.1.2.1.1.5.0 | ľ |
| | 35 11.4376190 211.69.32.99 | 172.16.0.104 | SNMP | 91 get-response 1.3.6.1.2.1.1.6.0 | |
| | 36 11.4388360 172.16.0.104 | 211.69.32.99 | SNMP | 91 get-next-request 1.3.6.1.2.1.1.6.0 | |
| | 37 11.4398400 211.69.32.99 | 211 60 22 00 | SNMP | 92 get-response 1.3.6.1.2.1.1.7.0 | |
| | 39 11 4422740 211 69 32 99 | 172 16 0 104 | SNMP | 92 get_response 1 3 6 1 2 1 2 1 0 | |
| | 19 11.4477740711.09.37.99 | III | SINNE | 57 OFFFFFF50003F 1. 3. 0. 1. 7. 1. 7. 1. 0 | • |
| F | rame 24: 89 bytes on wire (71 | 2 bits), 89 bytes ca | ntured (712 | bits) on interface 0 | |
| E | thernet II, Src: Elitegro_e5: | 0d:a5 (c8:9c:dc:e5:0 | d:a5), Dst: | Tp-LinkT_82:12:0e (1c:fa:68:82:12:0e) | |
| I | nternet Protocol Version 4, S | rc: 172.16.0.104 (17 | 2.16.0.104) | , Dst: 211.69.32.99 (211.69.32.99) | |
| U | ser Datagram Protocol, Src Po | rt: 52017 (52017), D | st Port: sr | mp (161) | |
| S | imple Network Management Prot | locol | | | |
| | | | | | |
| | | 图 6-9 | SNMP 巻 | 女据报文 | |
| | | Пох | | | |

(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。

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

表 6-6 交换机运行状态一览表

(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》

9

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。