

实验九：SNMP 协议分析

一、实验目的

- 1、了解 SNMP 协议；
- 2、熟悉 SNMP 的报文结构与通信过程；
- 3、了解 MIB 结构和工作原理；
- 4、掌握通过 SNMP 获取设备运行指标数据。

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，不低于双核 CPU、8G 内存、500GB 硬盘。

2、软件

推荐 Ubuntu Desktop 操作系统，安装 GNS 3 仿真软件，安装 Wireshark 抓包工具。
支持 Windows 操作系统，安装 GNS 3 仿真软件，安装 Wireshark 抓包工具。
安装 Net-SNMP 工具。

3、网络

计算机使用固定 IP 地址接入局域网，并支持对互联网的访问。

4、工具

无。

五、实验任务

- 1、完成 SNMP 报文结构分析；
- 2、完成 SNMP 通信过程分析；
- 3、完成使用 SNMP 获取交换机数据；
- 4、完成使用 SNMP 获取路由器数据。

六、实验内容及步骤

任务 1：实验准备

步骤 01：实验拓扑设计

网络拓扑结构，如图 9-1 所示。拓扑图中的设备选取 RouteSwitch-3600，可以右键单击相应的设备，选取：**change symbol** 项，在 **Classic** 里面选择需要的图标。

步骤 02：实验网络设计

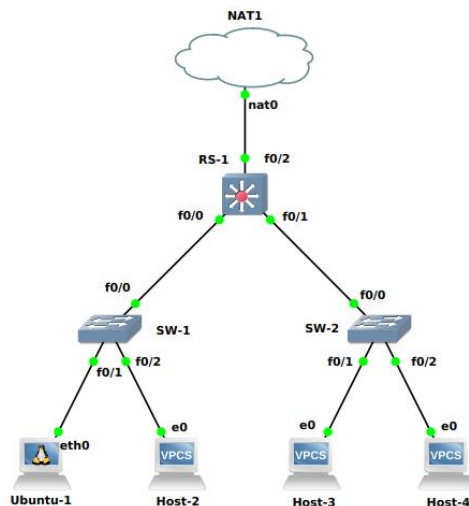


图 9-1 拓扑结构

① 本实验涉及的设备说明，如表 9-1 所示。

表 9-1 设备表

设备	设备类型	规格型号	备注
Host-1~Host-4	终端主机	--	Host-1 为 Ubuntu DockerGuest-1
SW-1~SW-2	路由交换机	CISCO C3600 (二层模块)	--
RS-1	路由交换机	CISCO C3600	--
NAT1	NAT 网络	--	--

② 交换机接口与 VLAN 规划，如表 9-2 所示。

表 9-2 交换机接口与 VLAN 规划表

交换机	接口	VLANID	连接设备	接口类型
SW-1	f0/1	11	Host-1	Access
SW-1	f0/2	12	Host-2	Access
SW-1	f0/0	--	RS-1	Trunk
SW-2	f0/1	11	Host-3	Access
SW-2	f0/2	12	Host-4	Access
SW-2	f0/0	--	RS-1	Trunk
RS-1	f0/0	--	SW-1	Trunk
RS-1	f0/1	--	SW-2	Trunk

RS-1	f0/2	200	NAT1	Access
------	------	-----	------	--------

③ 地址规划，如表 9-3 所示。

表 9-3 主机地址规划表

主机	IP 地址/子网掩码	网关	接入位置	所属 VLANID
Host-1	172.16.64.1 /24	172.16.64.254	SW-1 f0/1	11
Host-2	172.16.65.1 /24	172.16.65.254	SW-1 f0/2	12
Host-3	172.16.64.2 /24	172.16.64.254	SW-2 f0/1	11
Host-4	172.16.65.2 /24	172.16.65.254	SW-2 f0/2	12

④ 交换机接口地址，如表 9-4 所示。

表 9-4 交换机接口地址规划表

交换机	接口	VLANID	地址	接口类型
SW-1	f0/1	11	172.16.64.101/24	Access
SW-1	f0/2	12	172.16.65.101/24	Access
SW-2	f0/1	11	172.16.64.102/24	Access
SW-2	f0/2	12	172.16.65.102/24	Access

⑤ 路由接口地址，如表 9-5 所示。

表 9-5 路由接口地址规划表

设备名称	接口名称	接口地址	备注
RS-1	VLAN11	172.16.64.254 /24	--
RS-1	VLAN12	172.16.65.254 /24	--
RS-1	VLAN200	192.168.122.2/24	

⑥ 路由规划，如表 9-6 所示。

表 9-6 路由规划表

路由设备	目的网络	下一跳地址	路由类型
RS-1	172.16.64.0 /24	172.16.64.254	直连路由
RS-1	172.16.65.0 /24	172.16.65.254	直连路由
RS-1	0.0.0.0	192.168.122.1	静态路由

步骤 03: 在 GNS3 中实现网络

(1) 在 GNS3 中，按实验拓扑设计和实验网络设计实现网络，如图 9-1 所示。
在 GNS3 中连接互联网的参考配置命令如下。

参考命令:

```
//创建 VLAN200
RS-1#vlan database
RS-1(vlan)#vlan 200
//退出 VLAN 数据库模式，至特权模式
RS-1(vlan)#exit
RS-1#
//进入配置模式
```

```
RS-1#configure terminal
//将接口 f0/2 配置为 Access 模式，属于 VLAN200
RS-1(config)#interface f0/2
RS-1(config-if)#switchport mode access
RS-1(config-if)#switchport access vlan 200
RS-1(config-if)#no shutdown
RS-1(config-if)#exit
RS-1(config)#
RS-1(config)#ip routing
//配置静态路由
//去往目的网络 0.0.0.0/0 的报文，下一跳地址为 192.168.122.1
RS-1(config)# ip route 0.0.0.0 0.0.0.0 192.168.122.1
//配置 NAT
RS-1(config)#interface vlan 200
RS-1(config-if)#ip nat outside
RS-1(config-if)#interface vlan 11
RS-1(config-if)#ip nat inside
RS-1(config-if)#ip nat inside source list 1 interface vlan 200 overload
RS-1(config)#access-list 1 permit 172.16.0.0 0.0.255.255
RS-1(config)#exit
RS-1#write
```

（2）配置 Ubuntu-1 网络地址

Ubuntu-1 的网络配置如图 9-2 所示。

（3）通过在线方式为 Ubuntu-1 安装 SNMP 工具

```
#
# This is a sample network config uncomment lines to configure the network
#

# Static config for eth0
auto eth0
iface eth0 inet static
    address 172.16.64.1
    netmask 255.255.255.0
    gateway 172.16.64.254
    up echo nameserver 8.8.8.8 >/etc/resolv.conf

# DHCP config for eth0
# auto eth0
# iface eth0 inet dhcp
```

图 9-2 Ubuntu 网络配置

参考命令：

```
//修改仓库源
root@Ubuntu-1:~# sed -i s@/archive.ubuntu.com/@/mirrors.aliyun.com/@g /etc/apt/sources.list
//更新软件列表
root@Ubuntu-1:~# apt-get update
//安装 SNMP 请求命令
root@Ubuntu-1:~# apt-get install snmp
```

任务 2：通过 SNMP 监控交换机

步骤 01：配置 SW-1 开启 SNMP 服务

在 SW-1 上配置开启 SNMP 服务，参考配置命令如下。

参考命令：

```
SW-1#configure terminal
// 配置一个只读的团体名
SW-1(config)#snmp-server community monitor ro
SW-1(config)#
SW-1(config)#exit
SW-1# write
```

步骤 02：设置抓包点，启动 Wireshark 进行抓包

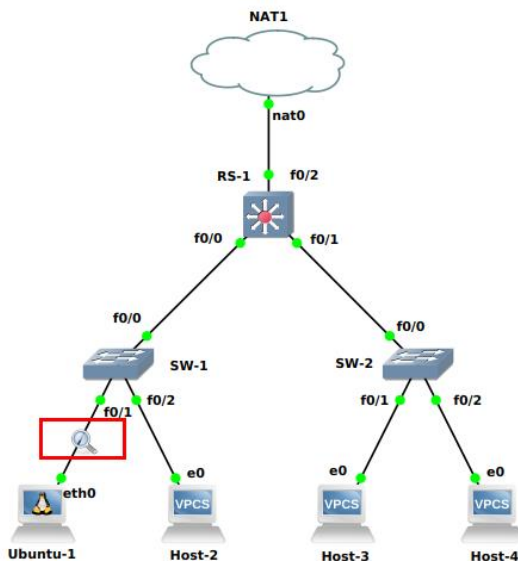


图 9-3 设置抓包点

在 Ubuntu-1 与 SW-1 之间设置抓包点，并启动 Wireshark 进行抓包，如图 9-3 所示。

步骤 03：执行 SNMP 请求命令

打开 Ubuntu-1 终端，使用 snmpget 命令获取 SW-1 的系统描述信息，如下所示。

参考命令：

```
root@Ubuntu-1:~# snmpget -v 2c -c monitor 172.16.64.101 1.3.6.1.2.1.1.1.0
```

步骤 04：分析 SNMP 报文结构

在 Wireshark 窗体中查看抓到的 SNMP 报文，截图一张。

(1) 分析 SNMP 请求报文结构，并填写表 9-7。

表 9-7 SNMP v2 Get-Request 报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Version		第 位		
2	Community		第 位		
3	PDUType		第 位		
4	RequestID		第 位		
5	ErrorStatus		第 位		

6	ErrorIndex		第 位		
7	VarBindList		第 位	--	
8	Variable-bindings（按照变量-值格式填写）				

（2）分析 SNMP 响应报文结构，并填写表 9-8。

表 9-8 SNMP v2 Get-Response 报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Version		第 位		
2	Community		第 位		
3	PDUType		第 位		
4	RequestID		第 位		
5	ErrorStatus		第 位		
6	ErrorIndex		第 位		
7	VarBindList		第 位	--	
8	Variable-bindings（按照变量-值格式填写）				

任务 3：通过 SNMP 监控交换机更多运行指标

步骤 01：配置 SW-2 开启 SNMP 服务

参照 SW-1 配置方法，配置 SW-2 开启 SNMP 服务。

步骤 02：使用 SNMP 获取 SW-2 数据

依据表 9-9 中的 OID 信息，通过 snmpwalk 命令获取 SW-2 的数据。

参考命令：

```
root@Ubuntu-1:~# snmpwalk -v 2c -c monitor 172.16.64.102 1.3.6.1.2.1.1.3
```

表 9-9 SW-2 的 OID 信息表

OID	描述	采集时间（年月日时分秒毫秒）	值
1.3.6.1.2.1.1.3	系统持续运行时长		
1.3.6.1.2.1.2.2.1.10	接收网络包数		
1.3.6.1.2.1.2.2.1.16	发送网络包数		

1.3.6.1.2.1.2.2.1.14	接收网络包错误数		
1.3.6.1.2.1.2.2.1.20	发送网络包错误数		
1.3.6.1.2.1.2.2.1.13	接收网络包丢弃数		
1.3.6.1.2.1.2.2.1.19	发送网络包丢弃数		

任务 4：使用自动化脚本持续监控路由器监控指标

步骤 01：配置 RS-1 开启 SNMP 服务

配置 RS-1 开启 SNMP 服务。

```
RS-1#configure terminal
// 配置一个只读的团体名
RS-1 (config)#snmp-server community public ro
RS-1 (config)#
RS-1 (config)#exit
```

步骤 02：撰写 Shell 脚本，使用 SNMP 定时采集 RS-1 的运行数据

撰写 Shell 脚本，将获取的数据格式化输出并写入文本文件，脚本内容如下所示。

为简化实验操作，建议：可将脚本内容复制到文本文件当中，清除到不需要的格式。然后在 Ubuntu-1 中打开终端，输入：nano snmp.sh,在打开的脚本文件当中把脚本文件粘贴进去，然后 ctrl+o 保存，ctrl+x 退出。接着在 Ubuntu-1 的终端中输入：sh snmp.sh 运行该脚本。

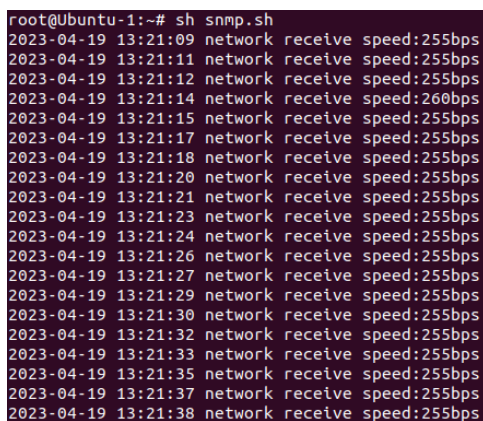
脚本内容：

```
#!/bin/bash
sum1=0
data=`snmpwalk -v 2c -c public 172.16.64.254 .1.3.6.1.2.1.2.2.1.10`
i=1
for element in $data
do
    j=`expr $i % 4`
    if [ $j -eq 0 ]
    then
        sum1=`expr $sum1 + $element`
    fi
    i=`expr $i + 1`
done
while :
do
    sum2=0
    sleep 1
    data=`snmpwalk -v 2c -c public 172.16.64.254 .1.3.6.1.2.1.2.2.1.10`
    i=1
    for element in $data
    do
        j=`expr $i % 4`
        if [ $j -eq 0 ]
        then
            sum2=`expr $sum2 + $element`
        fi
        i=`expr $i + 1`
    done
    diff=`expr $sum2 - $sum1`
    bitDiff=`expr $diff \* 8`
```



扫码看脚本

```
average=`expr $bitDiff / 60`  
time=`date +%s`  
echo `date -d "1970-01-01 UTC -8 ${time} seconds" +"%Y-%m-%d %H:%M:%S" network  
receive speed: ${average}bps`  
echo "${time} ${average}" >> if.txt  
sum1=$sum2  
done
```



```
root@Ubuntu-1:~# sh snmp.sh  
2023-04-19 13:21:09 network receive speed:255bps  
2023-04-19 13:21:11 network receive speed:255bps  
2023-04-19 13:21:12 network receive speed:255bps  
2023-04-19 13:21:14 network receive speed:260bps  
2023-04-19 13:21:15 network receive speed:255bps  
2023-04-19 13:21:17 network receive speed:255bps  
2023-04-19 13:21:18 network receive speed:255bps  
2023-04-19 13:21:20 network receive speed:255bps  
2023-04-19 13:21:21 network receive speed:255bps  
2023-04-19 13:21:23 network receive speed:255bps  
2023-04-19 13:21:24 network receive speed:255bps  
2023-04-19 13:21:26 network receive speed:255bps  
2023-04-19 13:21:27 network receive speed:255bps  
2023-04-19 13:21:29 network receive speed:255bps  
2023-04-19 13:21:30 network receive speed:255bps  
2023-04-19 13:21:32 network receive speed:255bps  
2023-04-19 13:21:33 network receive speed:255bps  
2023-04-19 13:21:35 network receive speed:255bps  
2023-04-19 13:21:37 network receive speed:255bps  
2023-04-19 13:21:38 network receive speed:255bps
```

图 9-4 运行脚本

在 Ubuntu-1 的终端中执行 Shell 脚本，如图 9-4 所示。

步骤 03：通过数据分析工具进行数据分析

将监控数据存储文件 if.txt 拷贝并存储到计算机中。

使用数据分析工具，例如 Excel、PowerBI 等工具，进行数据分析，绘制网络接收速率的折线图。

七、实验考核

1、任务说明

使用 Wireshark 分析 SNMP 报文结构；

使用 SNMP 监控交换机、路由器。

2、任务要求

要求 1：完成 SNMP 报文结构分析；

要求 2：完成 SNMP 通信过程分析；

要求 3：完成使用 SNMP 获取交换机数据；

要求 4：完成使用 SNMP 获取路由器数据。

3、考核要求

题目 1：使用 Wireshark 分析 SNMP 报文结构，请提交【SNMP 报文数据】截图和表 9-7 和 9-8 截图，共三张图。

题目 2：分析【SNMP 监控交换机更多运行指标】，填写表 9-9，并截图提交。

题目 3：使用自动化脚本持续监控路由器监控指标，建议提交脚本运行结果截图一张即可。