《网络运维管理》—— 实验指导书

实验四：通过 SNMP 监控网络设备信息

一、实验简介

在前面实验的基础上，在园区网内部的服务器、网络设备上安装并配置 SNMP，然后园区网内添加一台管理机（可用实体计算机代替），安装 net-snmp 软件，通过 SNMP 监控园区网内部的服务器或网络设备的相关信息。

二、实验目的

1、掌握 SNMP 的工作原理；

2、掌握 SNMP 监控的搭建配置；

三、实验理论

1、SNMP

四、实验规划

1、网络拓扑规划

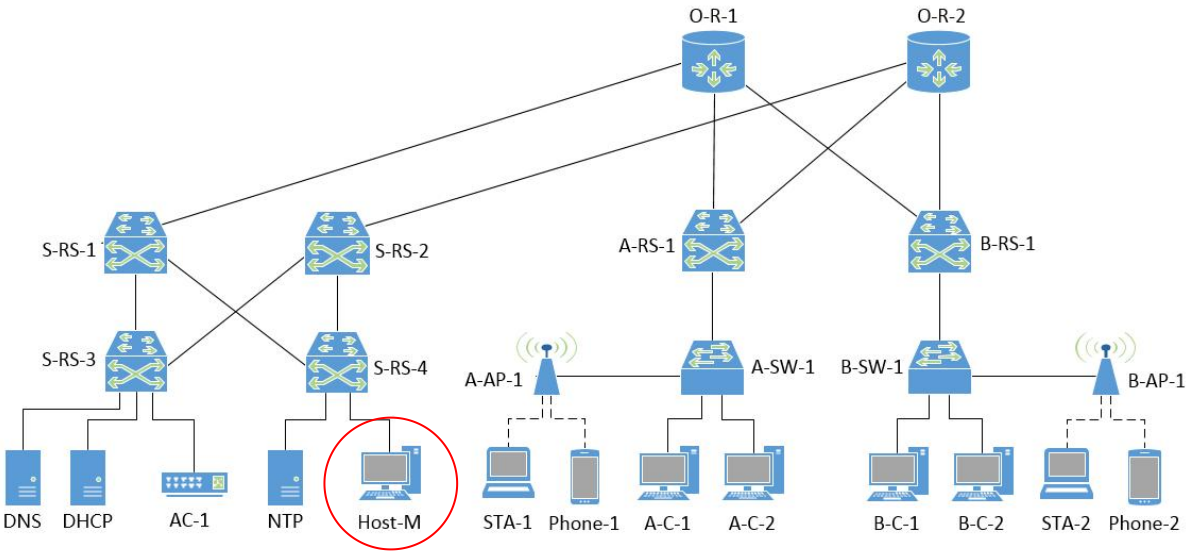

图 1 实验四的网络拓扑规划

表 1 网络设备说明

序号	设备线路	设备类型	规格型号	备注
1	A-C-1、A-C-2	用户主机	PC	A 区用户
2	B-C-1、B-C-2	用户主机	PC	B 区用户
3	STA-1、STA-2	移动终端	STA	移动用户
4	Phone-1、Phone-2	移动终端	Cellphone	移动用户
5	A-SW-1、B-SW-1	二层交换机	S3700	用户区域接入交换机

6	A-RS-1、B-RS-1	三层交换机	S5700	用户区域汇聚交换机
7	O-R-1、O-R-2	核心路由器	AR2220	核心区域路由器
8	S-RS-1、S-RS-2	三层交换机	S5700	数据中心汇聚交换机
9	S-RS-3、S-RS-4	三层交换机	S5700	数据中心接入交换机
10	A-AP-1、B-AP-1	无线接入点（AP）	AP3030	接入移动终端
11	AC-1	无线控制器	AC6605	用于 AP 的管理和配置
12	DNS Master	DNS 服务器	虚拟机接入	主 DNS 服务器
13	DNS Slave	DNS 服务器	虚拟机接入	辅 DNS 服务器
14	NTP-1	时间服务器	虚拟机接入	主时间服务器
15	NTP-2	时间服务器	虚拟机接入	辅时间服务器
16	Host-M	管理机	本地实体计算机	

【说明】

（1）由于需要在管理机上安装 net-snmp 软件，因此 Host-M 使用本地实体计算机或者 VirtualBox 虚拟机。

（2）本地实体计算机通过 Cloud 接入 eNSP 的仿真网络。

2、交换机 VLAN 设计

设计要求：

（1）本实验采用基于端口划分 VLAN。

（2）用户主机（有线）VLAN 设计：第一个 VLAN ID 用自己的学号后两位+1 来定义。例如 2021181001，其第 1 个 VLAN 的 ID 是 2，后面的 VLAN 依次加 1，即 VLAN3、VLAN 4……

（3）移动终端（无线）VLAN 设计：第一个 VLAN ID 用自己的学号后两位+200 来定义。例如 2021181001，其第 1 个 VLAN 的 ID 是 201，后面的 VLAN 依次加 1，即 VLAN 202、VLAN203……

（4）无线用户终端采用 2.4GHz 和 5GHz 两个频段接入网络，分别属于不同 VLAN；

（5）其他 VLAN 设计：三层虚拟接口的 VLAN，AP 所属的 VLAN 等，由学生自行设计。

3、IP 地址设计

设计要求：

（1）用户主机（含无线终端）IP 地址设计：格式是 192.A.B.*，其中，A 等于学号的最后两位，B 必须大于等于学号的后两位且小于等于学号后两位+5，*表示该位数值由考生自定。例如张三（2021181002）可以使用的 IP 地址范围是：192.2.2.0～192.2.7.255。**设计用户主机 IP 地址时要考虑路由聚合**。

注意：各网段的默认网关地址，使用本网段最后一个单播地址。

（2）服务器 IP 地址设计：格式是 172.16.A.*，其中，A 等于学号的最后两位，*表示该位数值由考生自定。**Host-M 的 IP 地址属于服务器 IP 地址范围。**

（3）路由接口 IP 地址设计：路由接口 IP 地址格式是 10.0.A.*。其中，A 等于学号的最后两位，*表示该位数值由考生自定。

（4）所有网络设备（此处指路由器、三层交换机等）的管理 IP，采用 10.10.A.*/24 网段中的 IP 地址，A 为学生本人学号的后两位；

（5）其他 IP 地址设计由学生自定。

4、路由表规划

本实验采用 OSPF 协议。

五、实验内容及打分

本实验共包含 3 个任务，由学生独立完成。教师在实验课上检查实验完成情况并提出相应问题，将根据各任务的完成情况及回答问题情况进行打分。

1、任务一：在园区网中接入管理机并实现全网通信（5 分）

（1）根据实验拓扑在 eNSP 中部署园区网；
（2）通过 VirtualBox 创建虚拟网卡，并接入实体计算机，作为 Host-M；
（3）实现全网互通；

【提示】本实验是在前面实验的基础上完成的。

2、任务二：配置园区网中各网络设备的管理 IP 并实现路由可达（5 分）

（1）给路由器、三层交换机配置管理 IP 地址；
（2）配置 OSPF，使得管理机（Host-M）可以 ping 通各网络设备的管理 IP 地址；

3、任务三：在被监控的服务器上配置 SNMP 服务（30 分）

被监控主机必须配置好 SNMP 服务，方可被监控到。本任务是在被监控的服务器（例如 DNS Master，安装 CentOS8 操作系统）上安装并配置 SNMP 服务，主要步骤包括：

（1）确认被监控的服务器可以在线安装 SNMP 组件

配置 SNMP 服务时，需要在线安装 SNMP 组件，因此此处要确保两点，一是被监控的服务器（例如 DNS Master）能够访问互联网，二是被监控服务器上配置有本地 DNS 地址（可以实现域名查询）。

【提示】CentOS 系统的 DNS 配置信息是在/etc/resolv.conf 文件中。

```
#vi /etc/resolv.conf        （使用 vi 命令编辑 resolv.conf 文件）

# Generated by NetworkManager
# No nameservers found; try putting DNS servers into your
# ifcfg files in /etc/sysconfig/network-scripts like so:
nameserver 114.114.114.114          // 此处添加 DNS 信息
nameserver 8.8.8.8                  //添加第 2 台 DNS 服务器信息
```

其他具体操作略

（2）安装 SNMP 服务组件

使用 SNMP 服务时，需要先安装 SNMP 服务的相关组件。

CentOS 及其它 RedHat 系列产品提供了 net-snmp 的二进制包。我们可以直接从源里安装。需要安装的组件除了 net-snmp 之外，还有 net-snmp-utils，net-snmp-libs 等。命令如下：

```
# yum –y install net-snmp-libs net-snmp net-snmp-utils net-snmp-devel
net-snmp-perl
```

注意：

1. net-snmp-devel 是为了使用 net-snmp-config，net-snmp-utils 是为了使用 snmpwalk。

输入上述的命令后，可看到安装加载过程，见图 2，安装完成后可看到“Complete”字符。

```
[root@localhost etc]# yum -y install net-snmp net-snmp-libs net-snmp-utils net-snmp-dev
el net-snmp-perl
已加载插件：fastestmirror
base                                                     | 3.6 kB  00:00:00
extras                                                   | 3.4 kB  00:00:00
updates                                                  | 3.4 kB  00:00:00
```

图 2 安装 SNMP 服务组件

（3）配置被监控机的 SNMP 配置文件

SNMP 服务的配置信息存放在/etc/snmp/snmpd.conf 文件中，需要对此文件进行修改，包括设置共同体名称，添加可访问信息的节点等操作。

①编辑打开 snmpd.conf 文件

```
# vi /etc/snmp/snmpd.conf
```

②配置 SNMP 服务的共同体名称

在配置文件中找到图 3 中的内容。

```
# First, map the community name "public" into a "security name"

#         sec.name  source          community
com2sec notConfigUser  default       public
```

图 3 查看并配置共同体名字

说明：Linux vi 中查找字符内容的方法

使用 vi 编辑器编辑长文件时，常常是头昏眼花，也找不到需要更改的内容。这时，使用查找功能尤为重要。方法如下：

1、命令模式下输入“/字符串”，例如/community 表示查找“community”。

2、如果查找下一个，按“n”即可。

“community”字段名即表示 SNMP 共同体，其下为字段值，默认值是“public”，表示本机的 SNMP 共同体名称是 public。

“source”表示采集数据请求的来源，即允许谁从本机采集监控数据，其默认值是“default”，表示允许任何主机进行数据采集。

注意：

1. 在 SNMP v1 版本中，引入了共同体的概念。在进行监控数据采集时，必须知道被监控设备的共同体名称，因此，将共同体名称修改为你自己才知道的字符串，是一种安全措施。例如，将“community”字段下面的 public 改为 xuchenggang，则管理机在通过 snmp 采集被监控设备的信息时，必须知道该共同体的值；
2. 修改“source”的值，只允许指定的设备进行监控数据的采集，也是一种安全措施。例如，将“source”字段下面的 default 改为 192.168.31.100，表示只允许来自该 IP 地址的 snmp 请求，才能被允许访问被监控设备；
3. SNMP v2 版本使用共同体名称。v1 没有安全措施，v3 使用认证和加密的机制实现安全。

③ 添加可访问信息的节点

继续在 snmpd.conf 文件中找到图 4 所示内容，其下添加“.1”的访问节点，表示可访问到 OID 值为.1.*的对应信息，从而增加可访问信息的节点。

完成上述配置后，点击【Esc】键退出编辑状态，然后在配置文件中输入“：wq”，点击回车，

```
# Make at least  snmpwalk -v 1 localhost -c public system fast again.
#        name           incl/excl     subtree         mask(optional)
view    systemview    included   .1.3.6.1.2.1.1
view    systemview    included   .1.3.6.1.2.1.25.1.1
view    systemview    included   .1     // 添加此行
```

保存配置文件并退出。

图 4 添加可访问信息的节点

注意：SNMP 中，MIB（管理信息库）是树形目录，此处的“subtree”字段值，用来定义可以访问到（即监控到）的设备信息节点，例如定义为.1.3.6，就表示只能够访问 1.3.6.*的 OID 对应的信息。

（4）安装并配置防火墙

SNMP 的访问是使用 UDP 协议，并通过 161 端口，CentOS 系统中默认安装的防火墙为 Firewall 防火墙，默认情况下，防火墙禁止 SNMP 的访问。因此，要想实现 SNMP 的访问，需要在防火墙上设置允许规则。

由于 firewall 防火墙操作复杂，因此，本实验中使用 IPTables 防火墙，其具体操作步骤如下。

①禁用 Firewall 防火墙。

由于在 CentOS 系统中默认安装的防火墙为 Firewall 防火墙，为避免防火墙冲突，需要禁止系统自带防火墙，主要的命令如下。

```
# systemctl stop firewalld
  //禁止 Firewall 防火墙
# systemctl disable firewalld.service
  //禁止开机启动 Firewall 防火墙
# systemctl status firewalld
  //查看 Firewall 防火墙状态
```

可通过查看防火墙的状态，判断该防火墙是否被禁用，如图 5 所示。

```
[root@localhost ~]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since 日 2018-01-21 16:15:23 CST; 4s ago
  Process: 602 ExecStart=/usr/sbin/firewalld --nofork --nopid $FIREWALLD_ARGS (code=exited, status=
CESS)
 Main PID: 602 (code=exited, status=0/SUCCESS)

1月 21 16:14:02 localhost.localdomain systemd[1]: Starting firewalld - dynamic firewall daemon...
1月 21 16:14:05 localhost.localdomain systemd[1]: Started firewalld - dynamic firewall daemon.
1月 21 16:15:23 localhost.localdomain systemd[1]: Stopping firewalld - dynamic firewall daemon...
1月 21 16:15:23 localhost.localdomain systemd[1]: Stopped firewalld - dynamic firewall daemon.
[root@localhost ~]#
```

图 5 查看 Firewall 防火墙状态

②安装 IPTables 防火墙

下载并安装 IPTables 防火墙及防火墙服务，主要命令如下。

```
# yum install   iptables iptables-services
  //下载并安装 IPTables 防火墙及服务
```

安装成功后，系统会给出提示，见图 6。

```
Running transaction
  Updating   : iptables-1.4.21-18.2.el7_4.x86_64                          1/3
  Installing : iptables-services-1.4.21-18.2.el7_4.x86_64                 2/3
  Cleanup    : iptables-1.4.21-13.el7.x86_64                              3/3
  Verifying  : iptables-1.4.21-18.2.el7_4.x86_64                          1/3
  Verifying  : iptables-services-1.4.21-18.2.el7_4.x86_64                 2/3
  Verifying  : iptables-1.4.21-13.el7.x86_64                              3/3

Installed:
  iptables-services.x86_64 0:1.4.21-18.2.el7_4

Updated:
  iptables.x86_64 0:1.4.21-18.2.el7_4

Complete!
[root@localhost sysconfig]#
```

图 6 成功安装 iptables 防火墙

③配置防火墙，添加防火墙规则

安装成功 iptables 后，在 /etc/sysconfig 目录中会生成 iptables 文件，编辑该文件，设置 iptables 防火墙规则。主要配置如下所示。

```
# vi /etc/sysconfig/iptables
  //打开 IPTables 防火墙的配置文件
-A INPUT –p udp -m state --state NEW –m udp --dport 161 –j ACCEPT
  //添加 161 端口通过防火墙的规则
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
  //添加允许 80 端口通过防火墙的规则
```

修改的配置文件结果如图 7 所示。添加规则完成后，在配置文件中输入“：wq”，点击回车，保存规则并退出。

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p udp -m state --state NEW -m udp --dport 161 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

图 7 在 iptables 防火墙配置文件中添加规则

注意：防火墙规则的顺序，顺序不对，规则不起作用。

（5）重启相关服务

经过上述的配置之后，需要重启相关服务，使 SNMP 客户端的配置生效，具体命令如下。

```
# systemctl restart snmpd.service          //重启 SNMP 服务
# systemctl enable snmpd.service           //配置 SNMP 服务开机启动
# systemctl restart iptables.service       //重启 IPTables 防火墙
# systemctl enable iptables.service        //配置 IPTables 防火墙开机启动
```

经过上述的步骤，完成对 CentOS 8 系统虚拟主机的 SNMP 服务配置。

4、任务四：在管理机 Host-M 上监控（采集）服务器信息（20 分）

本任务需要在管理机 Host-M（此处用实体计算机代替，安装 Windows10）上安装 NET-SNMP 软件，通过该软件进行 SNMP 数据采集，从而获取被监控服务器中的信息，主要步骤包括：

（1）下载并安装 Net-SNMP

可通过 Net-SNMP 官方网站 http://www.net-snmp.org（见图 8）下载获得安装软件

net-snmp-5.6.1.1-1.x86。也可从本课程网站上下载。

图 8 从 net-snmp 官网上下载软件

根据提示，在本地实体机上完成安装 Net-SNMP 软件，见图 9、10。

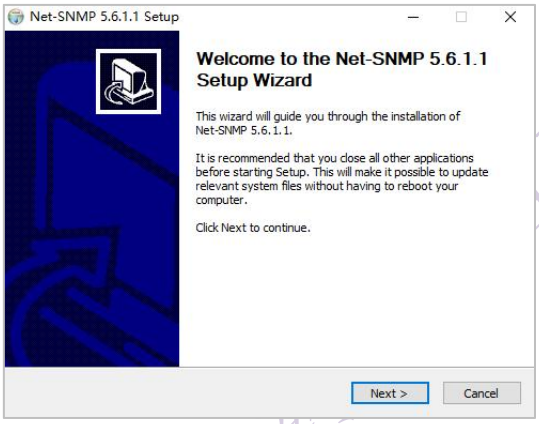

图 9 开始安装 net-snmp

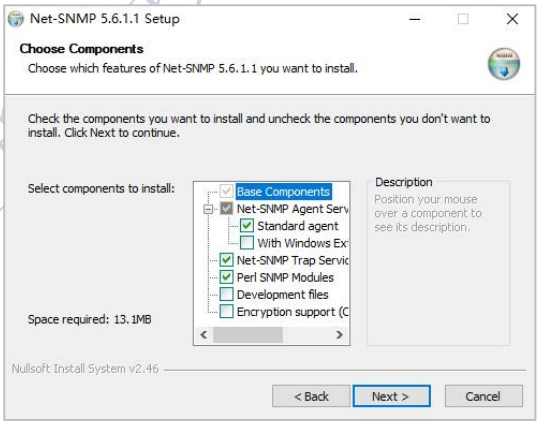

图 10 选择 net-snmp 组件

（2）使用 Net-SNMP 软件进行数据采集

通过 Windows 的命令行方式，对 CentOS 系统进行数据采集，具体操作步骤如下。

第一步：打开本地实体主机的【运行】程序，输入“cmd”，回车运行，打开本地主机的命令行界面。

第二步：在命令行中输入如下命令

snmpwalk -v 2c -c [共同体名] [IP 地址] [OID]

此命令是通过 Net-SNMP 工具向被监控主机发送了一个 SNMP 请求，其中，

- ✓ Snmpwalk：为命令动词，表示请求获取被监控设备中 OID 值所对应的信息。
- ✓ -v 2c：表示使用 SNMP v2 版本。
- ✓ [共同体]：表示被监控主机的共同体名称；
- ✓ [IP 地址]：表示被监控主机的 IP 地址；
- ✓ [OID]：表示要获取的信息对应的 OID 值。

例如，输入命令 **snmpwalk -v 2c -c My_Cacti 192.168.31.50 .1.3.6.1.4.1.2021.4**

其中：“My_Cacti”表示被监控设备的共同体名称，其 IP 地址是 192.168.31.50，管理机要获取的是 OID 值为“.1.3.6.1.4.1.2021.4”的信息，即获取内存相关信息。其结果见图 11。

```
C:\Users>snmpwalk -v 2c -c My_Cacti 192.168.31.50 .1.3.6.1.4.1.2021.4
UCD-SNMP-MIB::memIndex.0 = INTEGER: 0
UCD-SNMP-MIB::memErrorName.0 = STRING: swap
UCD-SNMP-MIB::memTotalSwap.0 = INTEGER: 839676 kB
UCD-SNMP-MIB::memAvailSwap.0 = INTEGER: 839676 kB
UCD-SNMP-MIB::memTotalReal.0 = INTEGER: 501080 kB
UCD-SNMP-MIB::memAvailReal.0 = INTEGER: 241792 kB
UCD-SNMP-MIB::memTotalFree.0 = INTEGER: 1081468 kB
UCD-SNMP-MIB::memMinimumSwap.0 = INTEGER: 16000 kB
UCD-SNMP-MIB::memShared.0 = INTEGER: 4464 kB
UCD-SNMP-MIB::memBuffer.0 = INTEGER: 764 kB
UCD-SNMP-MIB::memCached.0 = INTEGER: 167456 kB
UCD-SNMP-MIB::memSwapError.0 = INTEGER: noError(0)
UCD-SNMP-MIB::memSwapErrorMsg.0 = STRING:
```

图 11 通过 net-snmp 获取被监控主机的内存相关信息

还可以使用 snmpget 命令获取指定的信息，例如获取内存总大小，见图 12。

```
C:\Users>snmpget -v 2c -c My_Cacti 192.168.31.50 .1.3.6.1.4.1.2021.4.5.0
UCD-SNMP-MIB::memTotalReal.0 = INTEGER: 501080 kB
```

图 12 通过 net-snmp 获取被监控主机的内存大小

注意：

1. 命令中的 OID 值可以互联网上查询；
2. Windows 操作系统和 Linux 操作系统针对相同对象的 OID 值可能并不相同，查询时要注意；
3. snmpwalk 是对 OID 值的遍历，例如某个 OID 值下面有 N 个节点，则依次遍历出这 N 个节点的值；snmpget 是取具体的 OID 的值，适用于 OID 值是一个叶子节点的情况。例如，将图 12-2-15 中的命令动词换成 snmpget，则结果出现错误，见图 13。

```
C:\Users>snmpget -v 2c -c My_Cacti 192.168.31.50 .1.3.6.1.4.1.2021.4
UCD-SNMP-MIB::memory = No Such Object available on this agent at this OID
```

图 13 使用 snmpget 命令访问非叶子节点的结果

表 2 OID 值举例

OID 值	描述	适用操作系统
.1.3.6.1.2.1.1.1.0	获取系统基本信息	Linux / Windows
.1.3.6.1.2.1.1.3.0	监控时间	Linux / Windows
.1.3.6.1.2.1.2.1.0	网络接口的数目	Linux / Windows
.1.3.6.1.2.1.2.2.1.3	网络接口类型	Linux / Windows
.1.3.6.1.2.1.2.2.1.6	接口的物理地址	Linux / Windows
.1.3.6.1.2.1.2.2.1.10	接口收到的字节数	Linux / Windows
.1.3.6.1.2.1.25.2.3.1.4	硬盘簇的大小	Linux / Windows
.1.3.6.1.2.1.25.2.3.1.5	硬盘簇的的数目	Linux / Windows
.1.3.6.1.2.1.25.2.3.1.6	使用多少，跟总容量相除就是占用率	Linux / Windows
. 1.3.6.1.4.1.2021.11.10.0	系统 CPU 百分比	Linux
. 1.3.6.1.4.1.2021.11.11.0	空闲 CPU 百分比	Linux

5、任务五：在被监控的网络设备上配置 SNMP 并实现信息数据采集（10 分）

本任务在园区网内部的各路由器、交换机上配置 SNMP，使得管理机可以 SNMP 从这些设备上获取信息。

提示：

1. 华为设备 SNMP 配置步骤

第一步：使用 system-view 命令进入系统视图模式。

第二步： snmp-agent community read public

//设置一个 SNMP Community，使用该 Community 连接交换机时，只可以读取其 SNMP 信息。此处的 public 为用户配置的共同体名称，可更改为其他字符串。

第三步：snmp-agent community write private

//设置一个 SNMP Community，使用该 Community 连接交换机时，不仅可以读取其 SNMP 信息，还可以将值写入 SNMP 的 MIB 对象，实现对设备进行配置。此处的 public 为用户配置的共同体名称，可更改为其他字符串。

第四步： snmp-agent sys-info version all

//设置交换机支持的 SNMP 协议，有 v1,v2c,v3 这 3 个版本，如果不确定，可设为 all，将会同时支持这 3 个协议。

第五步：使用 display current-configuration 命令显示并检查配置。

第六步：使用 save 命令保存配置。

2. OID 值举例

表 3 交换机 OID 值举例

OID 值	描述	适用操作系统
.1.3.6.1.2.1.1.1.0	获取系统基本信息	路由器/交换机
.1.3.6.1.2.1.1.3.0	监控时间	路由器/交换机

6、回答问题（30 分）

教师在实验课上检查实验完成情况并提出相应问题，将根据各任务的完成情况及回答问题情况进行打分。

六、实验拓展及分析

1、简述 OID 的含义

2、通过查询 MIB RFC 1213，获得更多、更全面的 OID 值，从而获取更多的设备参数信息。除了实验指导书中所列出的 OID 值之外，找出 10 个 OID 值，自行验证，并将验证结果写入下面的表格：

序号	OID 值	中文描述其含义	对应设备
	.1.3.6.1.2.1.1.1.0	获取系统基本信息	路由器/交换机
	.1.3.6.1.2.1.1.3.0	监控时间	路由器/交换机