《网络运维管理》—— 实验指导书

实验三：对园区网的监控

一、实验简介

本实验在前面实验二的基础上进行，包括两项内容：一是通过 SNMP 监控园区网内的网络设备和服务器的信息（例如系统信息、CPU 的使用率等）；二是在园区网中搭建 Cacti 服务器，以图形化方式监控整个园区网中各网络设备、服务器的运行情况。

二、实验目的

1、理解 SNMP 的工作原理；
2、掌握 SNMP 监控的搭建配置；
3、掌握通过 SNMP 采集设备信息的方法；
4、理解 Cacti 工作原理；
5、掌握 Cacti 服务的部署；
6、掌握通过 Cacti 监控整个园区网中各网络设备（含服务器）的运行情况

三、实验理论

1、SNMP
2、Cacti

四、实验规划

1、网络拓扑规划

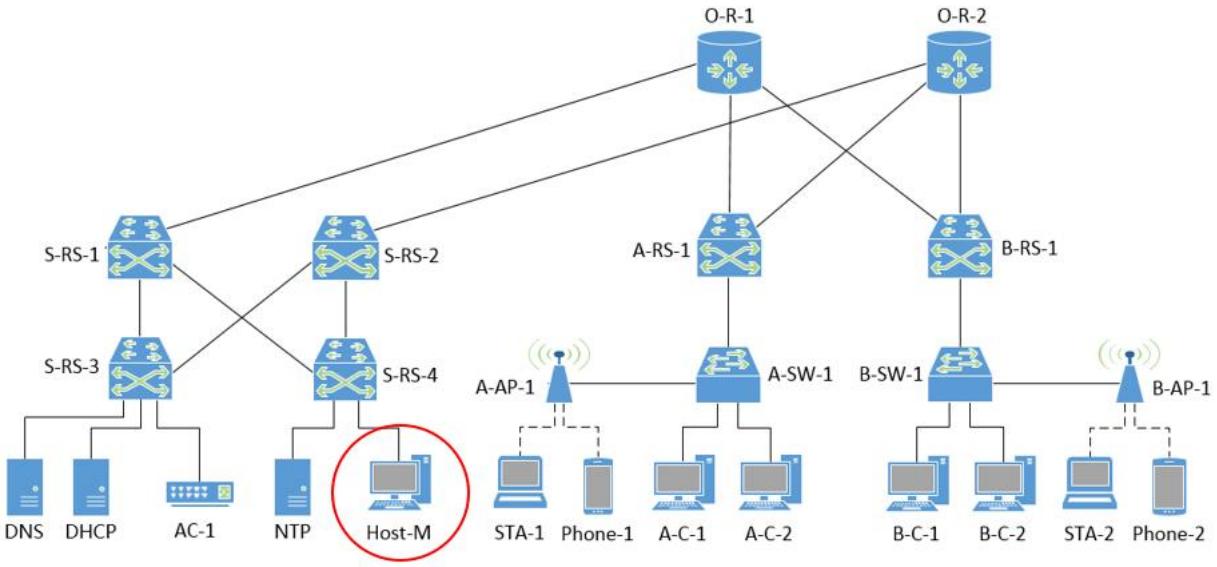

图 1 实验三网络拓扑规划

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
711	AC-1	无线控制器	AC6605	用于 AP 的管理和配置
12	DNS	服务器	虚拟机接入	DNS 服务器
13	DHCP	服务器	虚拟机接入	DHCP 服务器
14	NTP	服务器	虚拟机接入	NTP 服务器
15	Host-M	管理机	实体计算机	通过 Cloud 接入 eNSP

【说明】

（1）此处园区网中的服务器（DNS、NTP、DHCP），学生可参考教材中相关章节，自行添加；

（2）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。

（3）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、实验任务及要求

本实验共包含 6 个任务，由学生独立完成。

任务 1：在园区网中部署服务器（10 分）

任务说明：**在前面实验二所创建的园区网基础上**，在园区网内部署服务器（例如 DNS/DHCP/NTP 等），作为后期被 Cacti 监控的设备

本任务具体操作参看教材“项目四：提供本地 DNS”、“项目五：提供 NTP 时间同步服务”、“项目六：使用 DHCP 进行地址管理”。

任务 2：在被监控的服务器上配置 SNMP 服务（10 分）

被监控的服务器必须配置好 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：

步骤 01：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

步骤 02：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

步骤 03：配置被监控主机的 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，保存配置文件并退出。

```
# 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
```

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。

步骤 04：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。

步骤 05：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。

任务 3：在被监控的网络设备上配置 SNMP（10 分）

本任务在园区网内部的各路由器、交换机上配置 SNMP，使得管理机可以通过 SNMP 从这些

设备上获取信息。

配置提示： 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。

//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。

第二步： snmp-agent community read public

//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。

第三步：snmp-agent community write private

//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

第四步： snmp-agent sys-info version all

（完毕）

任务 4：在管理机 Host-M 上监控（采集）设备信息（10 分）

任务说明：本任务需要创建一台管理机 Host-M（此处用实体计算机代替，安装 Windows10）并将其接入到园区网指定位置。在该管理机上安装 NET-SNMP 软件，通过该软件进行 SNMP 数据采集，即管理机可以通过 SNMP 方式获取被监控服务器或网络设备中的运行信息（例如硬盘使用率、CPU 工作情况等）。主要步骤包括：

步骤 01：在园区网中设置管理机，使之可以访问各网络设备

通过 VirtualBox 创建虚拟网卡，并接入实体计算机，作为 Host-M，将 Host-M 接入在园区网数据中心区域的 S-RS-4 下面。

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；

【提示】本实验是在前面实验的基础上完成的，在实验二中，已经完成了各网络设备管理 IP 地址的配置。

步骤 02：在管理机上安装 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。

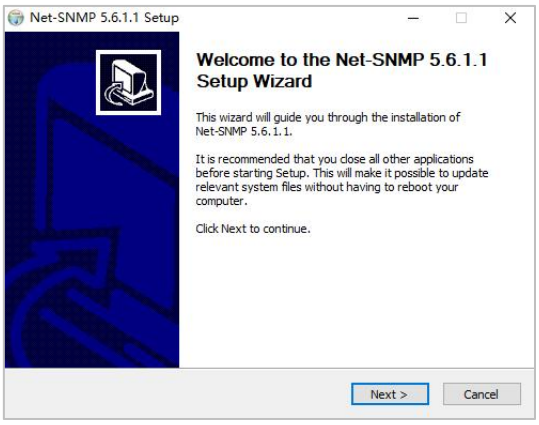

图 9 开始安装 net-snmp

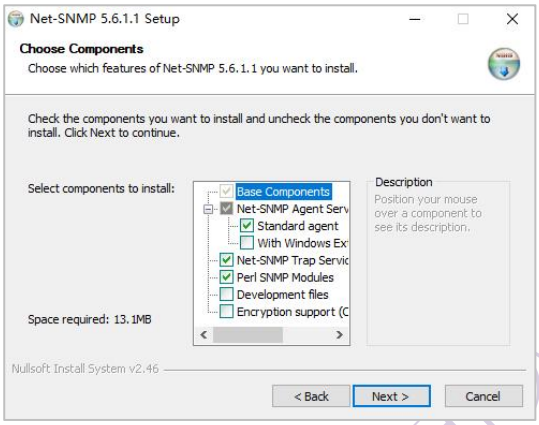

图 10 选择 net-snmp 组件

步骤 03：通过管理机（以 SNMP 方式）采集园区网内设备的运行数据

具体操作步骤如下：

（1）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。

（2）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 服务器 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

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

任务 5：创建 Cacti 服务器并进行相关配置（30）

任务说明：在前面任务 4 中，通过在管理机上输入具体的 SNMP 命令，采集被监控设备的某一个信息。本任务中，在园区网内部署一台安装 Cacti 系统的服务器，用来作为监控机，定期自动监控园区网内部各服务器（例如 DNS/DHCP 等）和网络设备的运行情况，并将获取到的监控结果数据以 Web 方式展示。具体步骤如下：

【提示】任务 5 的具体操作，可参考教材或课程网站

步骤 1：创建 Cacti 服务器虚拟机

在 VirtualBox 中创建 CentOS8 虚拟机，为了便于后面的操作中在线安装 Cacti 软件，此处可保持虚拟机网卡为缺省设置。具体操作略。

步骤 2：在线安装 Cacti 依赖包

具体操作参看教材“项目七：建设覆盖全网的运维监控系统”的任务 1 步骤 2。

步骤 3：获取并安装 Cacti 软件

Cacti 官方的安装教程：https://docs.cacti.net/Install-Under-CentOS_LAMP.md。

（1）安装wget软件包

wget是Linux中的一个下载文件的工具，支持通过 HTTP、HTTPS、FTP 三个最常见的TCP/IP协议下载，并可以使用 HTTP 代理。

```
[root@VM-CentOS ~]# yum install -y wget
```

（2）下载Cacti软件包

通过wget工具从课程网站中下载Cacti软件包。

```
[root@VM-CentOS ~]# wget https://internet.hactcm.edu.cn/software/cacti/cacti-1.2.x.zip
```

提醒

1. 本步骤为在线安装Cacti，后续可能因为Cacti版本升级或其他原因致使下载路径变动而导致下载失败。读者可从github中获取Cacti最新软件包，上传Cacti服务器上进行系统安装。

（3）安装unzip软件包

unzip是Unix和类Unix系统上的解压缩工具，用于解压缩由ZIP压缩算法创建的压缩文件。

```
[root@VM-CentOS ~]# yum install -y unzip
```

（4）解压Cacti软件包

使用unzip将获取的Cacti软件包解压至/var/www目录，并将其重命名为cacti。

```
[root@VM-CentOS ~]# unzip cacti-1.2.x.zip -d /var/www/
[root@VM-CentOS ~]# mv /var/www/cacti-1.2.x /var/www/cacti
```

（5）设置 cacti 目录权限

将 cacti 目录/var/www/cacti 及其所有子文件的属主与属组设置为 apache。并将 cacti 目录及其所有子文件的权限设置为 755，即属主有读、写、执行权限，属组和其它用户有读、写权限。确保 Cacti 能够正常运行。

```
[root@VM-CentOS ~]# chown -R apache:apache /var/www/cacti
[root@VM-CentOS ~]# chmod -R 755 /var/www/cacti
```

步骤 4：配置 Cacti 运行环境

具体操作参考“项目七：建设覆盖全网的运维监控系统”的任务 1 步骤 4。

（1）为 PHP 设置时区

（2）配置 MariaDB

（3）启动 MariaDB 并设置开机自启

（4）设置数据库 root 用户的密码

（5）设置数据库的时区

（6）创建 Cacti 所需数据库，并导入初始数据表

（7）配置 Apache HTTP Server

（8）启动 HTTPD 并设置开机自启

（9）配置 Cacti

（10）创建监控数据采集的任务计划

步骤 5：配置防火墙并关闭 SELinux

具体操作参考“项目七：建设覆盖全网的运维监控系统”的任务 1 步骤 5

（1）配置防火墙

（2）关闭 SELinux

步骤 6：将 Cacti 服务器部署到园区网

将 Cacti 服务器（虚拟机）接入到 eNSP 中园区网数据中心的交换机上，如图 14 所示。注意网卡的连接方式。

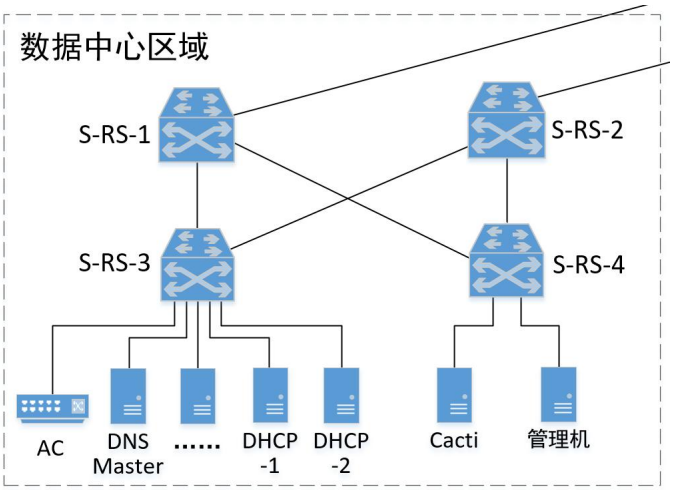

图 14　Cacti 服务器的部署拓扑（只显示部分拓扑）

配置 Cacti 服务器接入园区网的网卡 IP 地址，学生自行设计。

配置数据中心交换机 S-RS-4 连接 Cacti 服务器的三层虚拟接口 IP 地址，学生自行设计。

配置数据中心交换机 S-RS-4 的路由（OSPF），实现 Cacti 服务器与园区网的内部的设备的通信。学生自行设计。

步骤 7：将管理机接入园区网交换机 S-RS-4

此处需要将管理机（用本地实体主机代替）接入园区网，并实现管理机对 Cacti 的访问。

将管理机接入园区网以后，为了实现对 Cacti 的访问，需要在管理机（即本地实体主机）上配置静态路由。学生自行设计。

【提示】此处接入管理机的目的，是为了通过管理机的 Windows 操作系统（例如用自己的笔记本电脑作为管理机），以 Web 方式登录 Cacti 服务器，从而查看 Cacti 的监控结果（图形化方式展示）。

步骤 8：Cacti Web 安装

接下来需要以 Web 方式登录 Cacti 服务器，并进行最后的安装配置。

具体操作参考“项目七：建设覆盖全网的运维监控系统”的任务 1 步骤 6。

安装完成后出现【开始使用】，开始使用 Cacti 监控系统。

步骤 9：在 Cacti 添加 DNS 服务器监控

接下来，需要将被监控的设备添加入 Cacti 服务器。

具体操作参考“项目七：建设覆盖全网的运维监控系统”的任务 2 步骤 6。

步骤 10：在 Cacti 添加其他服务器监控

参照本任务的步骤 9，完成添加其他服务器，并放到默认图形树上，此处略。服务器添加完成后如图 15 所示。

图 15 服务器监控列表

步骤 11：在 Cacti 添加网络设备监控

Cacti 添加网络设备监控与添加服务器监控的步骤一致，所用模板也一致。添加监控时，使用网络设备的 loopback 地址。

参照本任务的步骤 9，完成添加其他网络设备监控，此处略。

所有设备监控添加完成后的图形树如图 16 所示。

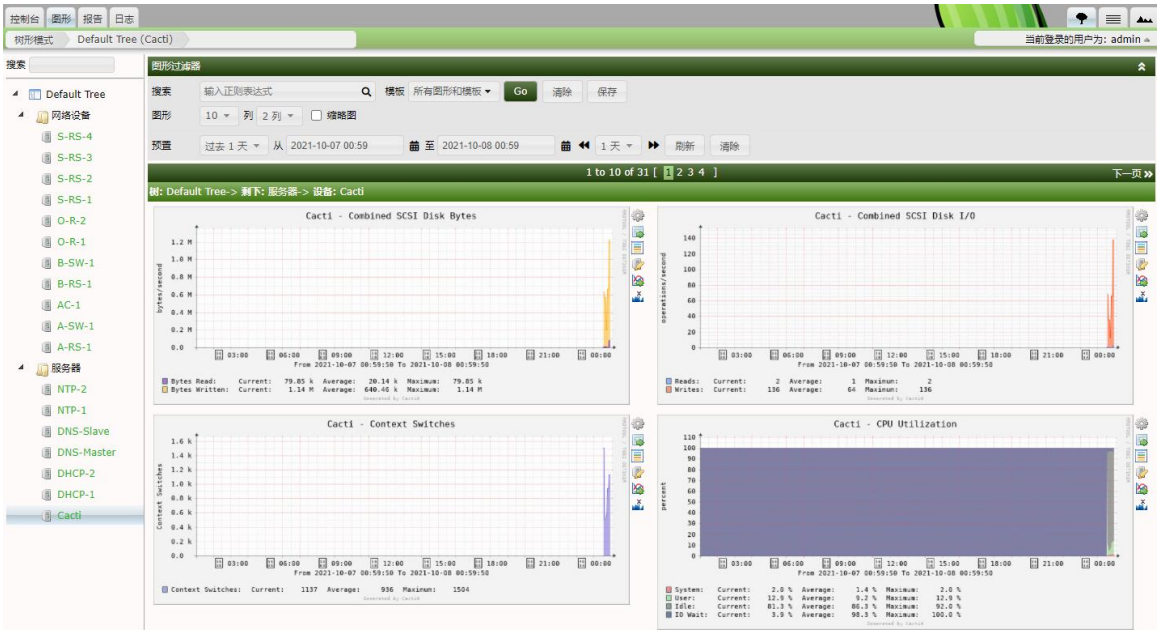

图 16 全部监控对象的图形树

至此，实现对全网设备的监控。管理员可从图 16 中左侧的列表里面选择想要查看（监控）的设备，在右侧即可显示出该设备的运行状态信息。

六、实验考核

实验考核从【完成维度】和【时间维度】两个维度进行评分。

1、【完成维度】考核

本维度主要考核学生完成实验的程度以及对实验内容的理解程度，包括【任务完成度】和【回答问题】两个部分。具体如下：

（1）任务完成度（70 分）

学生在完成实验后，要当面提交教师检查实验结果。教师检查每个实验任务的完成情况，并根据实验指导书中每个任务的分值，给出任务完成度的分数。本项目满分 70 分。

（2）回答问题（30 分）

学生在完成实验后，要当面提交教师检查实验结果，并回答教师提问。教师根据学生回答情况评分。本项目满分 30 分。

【注意】：教师提问时，可参考“七、思考与讨论”中的问题，从中随机选取 2-3 个问题进行提问。

2、【时间维度】考核

本维度主要考核学生完成实验的时间，具体如下：

（1）当堂提交（100 分起评）

本实验的实验课当堂提交并通过【完成维度】考核的，从 100 分起评。

（2）一周内提交（90 分起评）

本实验的实验课结束一周内提交并通过【完成维度】考核的，从 90 分起评，即本次实验考核最高 90 分。

（3）一周后提交（80 分起评）

本实验的实验课结束一周后提交并通过【完成维度】考核的，从 80 分起评，即本次实验考核最高 80 分。

（4）未提交（0 分）

本学期教学工作结束时，仍未提交的，本次实验考核 0 分。

七、思考与讨论

学生在做实验时，要结合实验内容和过程，讨论分析以下问题，以备教师提问

1. 什么是 SNMP？有什么功能？根据你的理解，谈谈 SNMP 有什么现实应用。
2. SNMP 有几个版本？各自特点是什么？
3. 请解释管理站、管理程序、被管设备、被管对象、代理这些名词的含义，结合自己在本实验中的实例操作，说说这些名词在 SNMP 通信中（例如通过 SNMP 获取某个设备的信息），各自起的作用是什么？
4. 本实验任务 2 的步骤 03 中，设置了“团体名”，在 SNMP 通信中，团体名有什么作用？你中此处配置的团体名是什么？
5. 本实验任务 4 的步骤 03 中，执行了 snmpget 命令，该命令的作用是什么？此处指导书所给出

的参考命令中，每一个参数代表什么意思？

6. 本实验任务 4 的步骤 03 中，行了 snmpwalk 命令，该命令的作用是什么？此处指导书所给出的参考命令中，每一个命令参数代表什么意思？结合 snmpwalk 命令的结果，谈谈 snmpwalk 与 snmpget 的区别。

7. OID 是什么意思？结合本实验的操作，举例说明：在通过 SNMP 获取某网络设备的信息过程中，哪个地方用到了 OID？这个 OID 代表的具体含义是什么？除了实验指导书中给出的 OID 之外，请自行查询资料，再举出 3 个 OID 的实例值并说明其含义。

8. 结合本实验的整体实施，举例说明通过 SNMP 获取到网络设备参数的步骤，并汇报给老师。

9. 结合本实验的整体实施，举例说明通过 Cacti 对园区网进行监控的步骤，即需要完成哪些配置？

10. 结合本实施的实施，谈谈 Cacti 的工作原理。