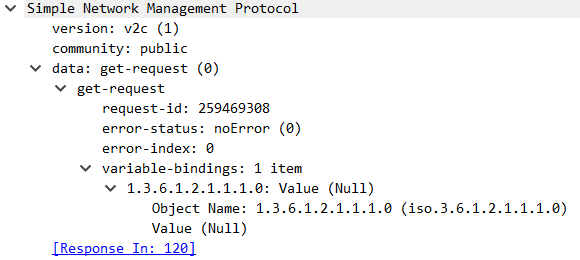
**实验九 网络管理实验**

1. 打开截获的报文，选中一条get报文，回答下面问题：

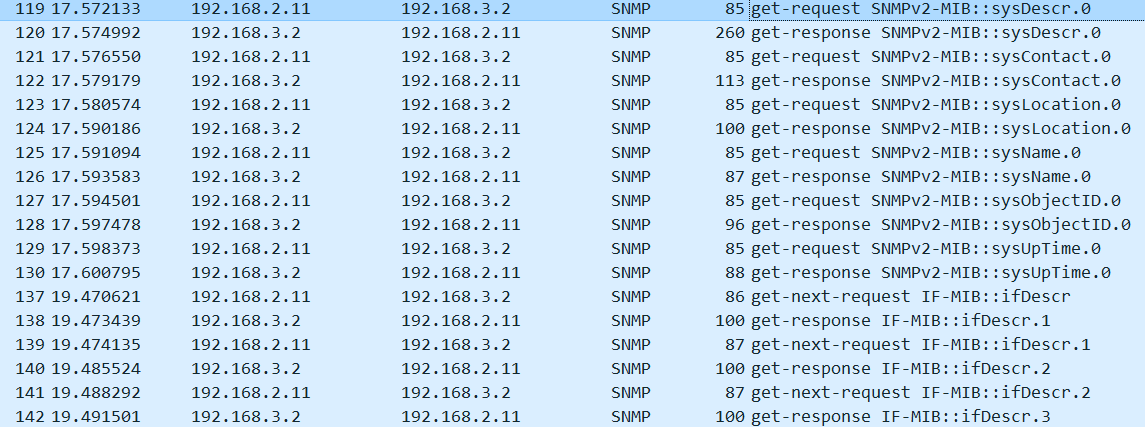
此报文的类型字段值是 0 ，它表示此报文属于snmp定义的哪种协议数据单get-request。

此报文的请求标识符字段的值为 259469308 ，请说明它的作用 由管理进程设置的一个整数值，让响应报文发送回来做标识符，显示对应于哪一个请求报文 。并找到与其对应的相应报文，其报文编号为 120 。



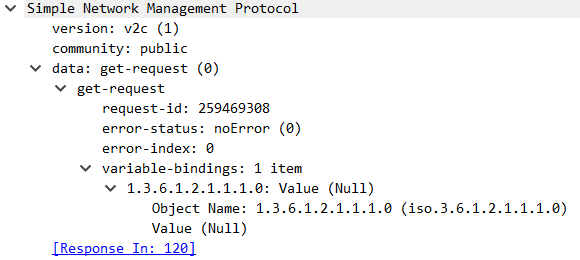
1. 简要分析网管程序读取被管设备信息的过程。

**答：网管程序通过不断向被管设备发送SNMP报文，报文类型是get-request和get-next-request，在SNMP报文中设置需要的知道的变量字段名，在被管设备收到请求报文之后，根据自己情况发送get-response报文回复相应的变量值。**



1. 观察在实验中截获的报文，请分析，网管程序向被管设备所请求的第一个参数是什么？它在MIB中的标识符识什么？

**答：第一个参数是SNMPv2-MIB::sysDescr.0，在MIB中的标识符是1.3.6.1.2.1.1.1.0。**



1. 找到第二个get报文和与其对应的response报文，并根据其内容填写下表：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 报文类型 | 类型代 码 | Request ID | Object identifer 1 | | Object identifer 2 | | Object identifer 3 | |
| 标识符 | 值 | 标识符 | 值 | 标识符 | 值 |
| Get | 0 | 259469310 | SNMPv2-MIB::sysContact.0 | NULL | 无 | 无 | 无 | 无 |
| Response | 2 | 259469310 | SNMPv2-MIB::sysContact.0 | Hangzhou H3C Tech. Co., Ltd. | 无 | 无 | 无 | 无 |

1. 在所截的报文中，找到对象ifindex，回答它在MIB中的对象标识符为1.3.6.1.2.1.2.2.1.1。
2. 分别找到SNMP定义的各PDU类型，进行详细的分析。并补全下表：

|  |  |  |
| --- | --- | --- |
| PDU类型编号 | PDU类型名称 | 作用 |
| 0 | get-request | 从代理进程处提取一个或多个参数值 |
| 1 | get-next-request | 从代理进程处提取一个或多个参数值的下一个参数值 |
| 2 | get-response | 从代理进程处返回的一个或多个参数值 |
| 3 | set-request | 设置代理进程的一个或多个参数值 |
| 4 | trap | 代理进程通知管理进程有某些事情发生 |

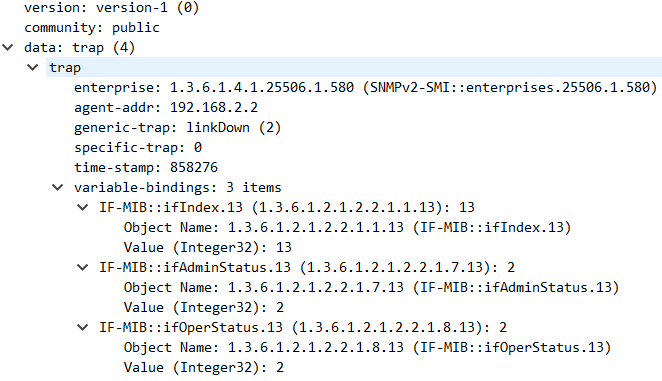
7. 找到trap报文，并对其首部进行分析，填写下表：

|  |  |  |
| --- | --- | --- |
| 字段名 | 字段长度 | 字段表达信息 |
| enterprise | 11 | 企业:(SNMPv2SMI::enterprises.25506.1.580) |
| agent\_addr | 192.168.2.2 | 代理企业IP地址：192.168.3.2 |
| generic\_trap | 1 | 陷阱类型代码：LinkDown(2) |
| specific\_trap | 1 | 0 |
| time\_stamp | 3 | 时间戳：858276 |

请写出trap报文中企业字段的值是SNMPv2SMI::enterprises.25506.1.580。它的作用是什么？

**答；作用是为了表示产生陷阱报文的网络设备的对象标识符。**

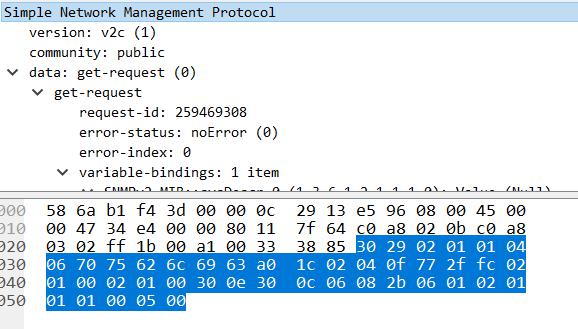
请写出H3C公司在MIB中的结点为\_1.3.6.1.4.1.25506\_\_。



8.找到“打开设备”时，RouterManager（网管程序）向路由器（被管设备）请求信息的报文，这些报文是在MIB树上检索信息的过程，此过程使用最多的PDU类型是什么？在检索过程中起了什么作用？

答：使用最多的是get-next-request类型的PDU，在检索过程从代理进程处提取一个或多个参数值的下一个参数值。（原因：因为MIB中的参数值多以表格的储存，所以get-next-request相对较多）

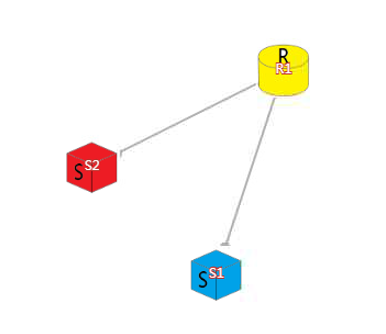
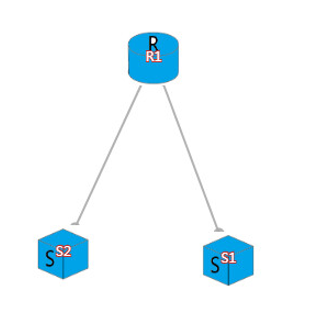
9. ASN.1基本编码规则的分析，以第一条get报文为例，选中此报文用TLV方法进行编码，并填写下表：



|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| SNMP报文的TLV编码 | | | | | | | | | |
| 字段 | 字段表达信息 | | | | | | 编码 | | |
| Message-T | 通用类 构造类型 SEQUENCE | | | | | | 00 1 10000 | | |
| Message-L | V字段长度为41字节 | | | | | | 0 0101001 | | |
| Message-V | SNMP | | | | | | … | | |
| Message-V字段 | | | | | | | | | | |
| Version | 字段 | | 字段表达信息 | | | | | 编码 | | |
| T | | 通用类 简单类型 INTEGER | | | | | 00 0 00010 | | |
| L | | 1字节 | | | | | 0 0000001 | | |
| V | | version: v2 | | | | | 0x01 | | |
| Community | T | | 通用类 简单类型 OCTET STRING | | | | | 00 0 00100 | | |
| L | | 6字节 | | | | | 0 0000110 | | |
| V | | public | | | | | 0x 70 75 62 6c 69 63 | | |
| Get PDU | T | | 上下文类 构造类型 | | | | | 10 1 00000 | | |
| L | | 28字节 | | | | | 0 0011100 | | |
| Get-PDU-V | | get-request | | | | | … | | |
| Get-PDU-V字段 | | | | | | | | | | |
| Request-id | | 字段 | | | 字段表达信息 | | | | 编码 | |
| T | | | 通用类 简单类型 INTEGER | | | | 00 0 00010 | |
| L | | | 4字节 | | | | 0 0000100 | |
| V | | | request\_id:259469308 | | | | 0x 0f 77 2f fc | |
| Error-status | | T | | | 通用类 简单类型 INTEGER | | | | 00 0 00010 | |
| L | | | 1字节 | | | | 0 0000001 | |
| V | | | error-status: noError | | | | 0x 00 | |
| Error-index | | T | | | 通用类 简单类型 INTEGER | | | | 00 0 00010 | |
| L | | | 1字节 | | | | 0 0000001 | |
| V | | | error-index: 0 | | | | 0x 00 | |
| Variable-bindings | | T | | | 通用类 构造类型 SEQUENCE-OF | | | | 00 1 10000 | |
| L | | | 14字节 | | | | 0 0001110 | |
| VarBind | | T | 通用类 构造类型 SEQUENCE | | | | 00 1 10000 | |
| L | 12字节 | | | | 0 0001100 | |
| Name | T | 通用 简单OBJECT IDENTIFIER | | | 00 0 00110 | |
| L | 8字节 | | | 0 0001000 | |
| V | SNMPv2-MIB::sysDescr.0 | | | 0x2b06010201010100 | |
| Value | T | 通用 简单 NULL | | | 00 0 00101 | |
| L | 0字节 | | | 0x 00 | |

10 网络拓扑发现实验中，断开一台交换机，重新发现网络拓扑看有何变化？网管软件有何变化？设备管理中查看此交换机的接口列表，看有什么变化。

**答：网络未断开之前🡪网络断开之后**



**网管软件发现交换机断开之后，网管软件中显示交换机为断开状态，对应交换机的接口列表状态变为shutdown状态。**

**Ps:要查看网管软件的变化需要在四台机器上安装网管软件，而实验过程中假如只在其中一台电脑安装网管软件这里是看不到变化的，然后断开交换机S1，再去其他机器上面查看端口变化。**