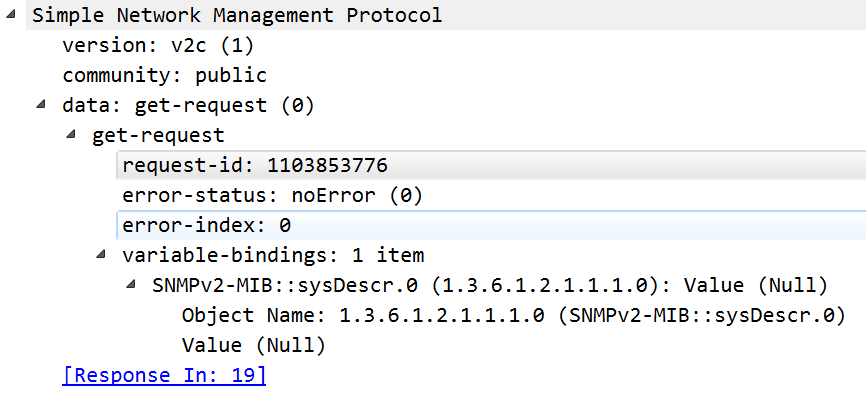
**实验九 网络管理实验**

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 1103853776 ，请说明它的作用 由管理进程设置的一个整数值，用来识别返回的响应报文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 19 。



1. 简要分析网管程序读取被管设备信息的过程。

答：

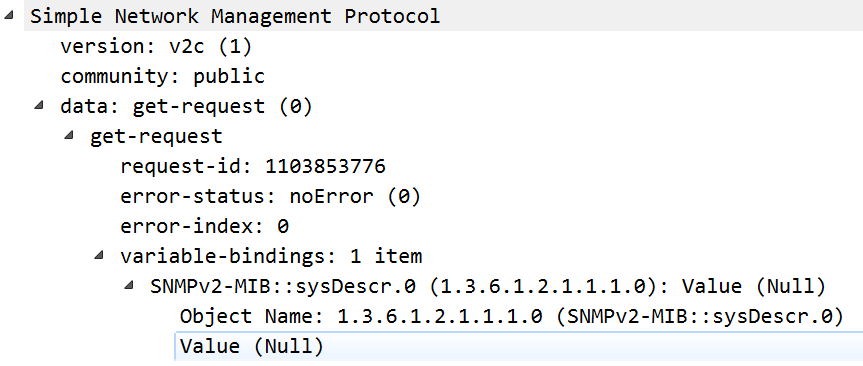
网关程序通过不断向被管设备发送get-request和get-next-request报文，请求各种变量的信息，被管设备收到请求报文后，发送get-response报文回复相应的变量信息。



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中的标识符识是什么？

答：

请求的第一个参数是SNMPv2-MIB::sysDescr.0，它在MIB中的标识符识是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 | 1103853778 | SNMPv2-MIB::sysContact.0 | Null | 无 | 无 | 无 | 无 |
| Response | 2 | 1103853778 | 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 |

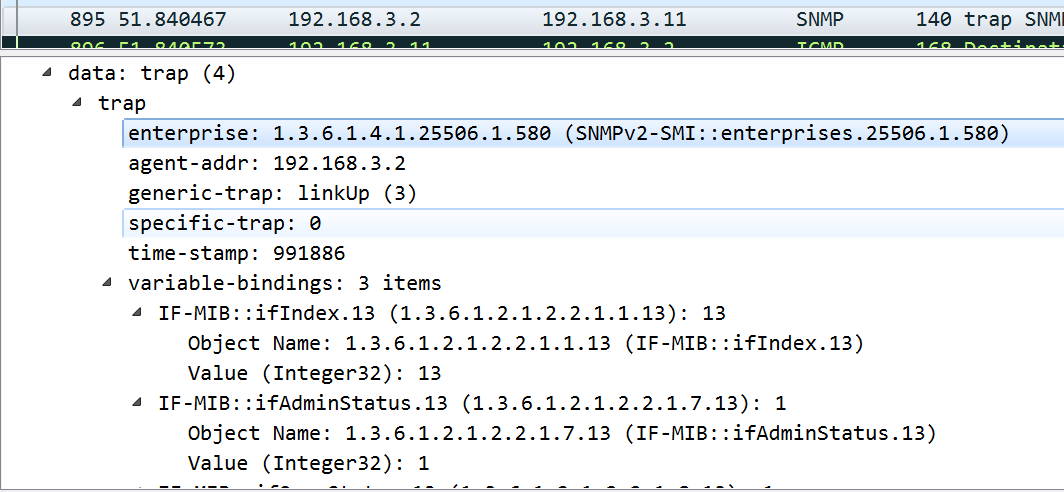
1. 分别找到SNMP定义的各PDU类型，进行详细的分析。并补全下表：找到trap报文，并对其首部进行分析，填写下表：

|  |  |  |
| --- | --- | --- |
| 字段名 | 字段长度 | 字段表达信息 |
| enterprise | 11 | 企业： SNMPv2-SMI::enterprise.25506.1.580 |
| agent\_addr | 4 | 代理的IP地址： 192.168.3.2 |
| generic\_trap | 1 | Trap类型： linkUp(3) |
| specific\_trap | 1 | 特定代码： 0 |
| time\_stamp | 3 | 时间戳： 991886 |

请写出trap报文中企业字段的值是 SNMPv2-SMI::enterprise.25506.1.580 。它的作用是什么？

**答：企业字段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 。



1. 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PDU类型是get-next-request，用来从代理进程处提取一个或多个参数值的下一个参数值。（p.s.题目的意思是不是：问网管程序为发送者的报文中使用最多的？）

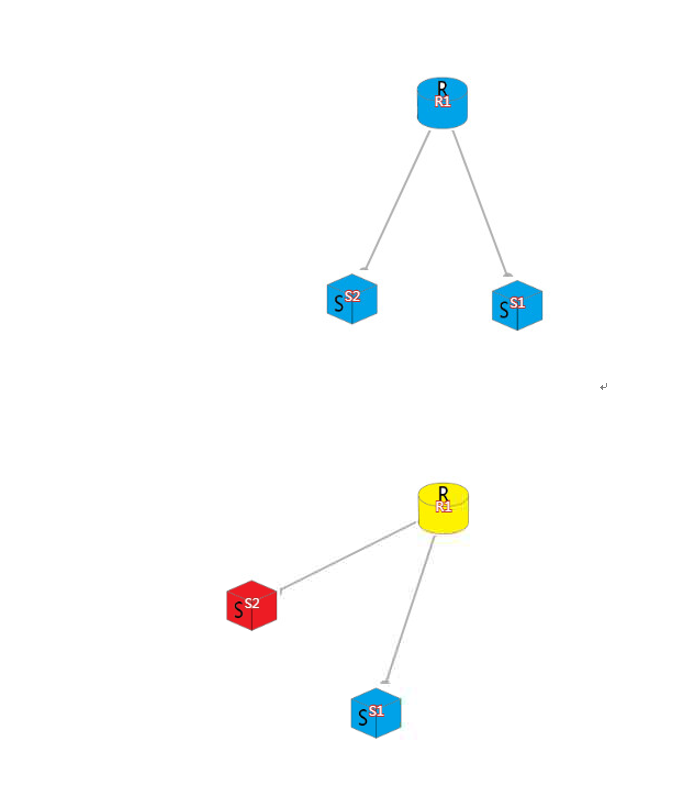
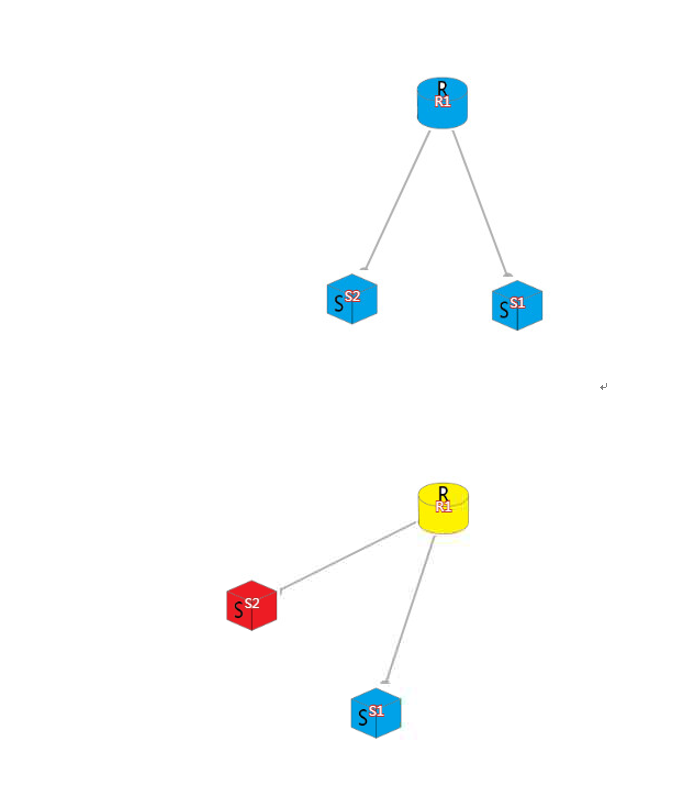
1. ASN.1基本编码规则的分析，以第一条get报文为例，选中此报文用TLV方法进行编码，并填写下表：

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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: v2c | | | | 0x 01 | | |
| 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: 1103853776 | | | | 0x 41 cb 78 d0 | |
| 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 | |

1. 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：

断开交换机S2前： 断开交换机S2后：

断开交换机后，S2变成红色断开状态，R1变成黄色状态（设备有端口变为down状态但设备还连在网络中）。

网管软件显示交换机为断开。

交换机的接口列表为shutdown状态。