**实战演练之报文格式分析**

    Trap报文格式和上述图5所展示的结构有些差别，这里我们只分析SNMPv1和SNMPv2的Trap报文格式。trap报文前面的部分都一样，区别在PDU协议数据单元部分。

**SNMPv1 Trap报文**

SNMPv1的Trap报文格式如下所示：

注意：除了PDU类型和PDU长度字段外，后面的每个字段都是BER编码方式。

    trap类型”可以取以下值，其中0~6是已定义的特定trap，7及其以后的类型由供应商自定义。

表2 trap类型、名称及描述信息

|  |  |  |
| --- | --- | --- |
| trap类型 | 名称 | 描述信息 |
| 0 | coldStart | 代理进程对自己初始化 |
| 1 | warmStart | 代理进程对自己重新初始化 |
| 2 | linkDown | 一个接口已从工作状态变为故障状态(报文中的第一个变量标识此接口) |
| 3 | linkUp | 一个接口已从故障状态变为工作状态(报文中的第一个变量标识此接口) |
| 4 | authenticationFailure | 从SNMP管理进程收到无效共同体的报文 |
| 5 | egpNeighborLoss | 一个EGP邻站已变为故障状态(报文中的第一个变量包含邻站IP地址) |
| 6 | enterpriseSpecific | 在这个特定的代码段中查找trap信息 |

通过wireshark抓包工具，捕获一条如下的SNMP报文，接下来对其进行仔细分析。

SNMPv1原始报文内容：

00 23 5a 9e 58b9 00 4c 41 49 50 55 08 00 45 00 00 48 00 00 40 00 40 11 a5 4e c0 a80a 01 c0 a8  0a05 0c 00 00 a200 34 ff e0 30 2a 02 01 00 04 06 70 75 62 6c 69 63a4 1d 06 0a 2b 06 01 04 01 bf 08 03 02 0a 40 04 c0 a8 0a01 02 01 00 02 01 00 43 01 0e 30 00

目的MAC：00 23 5a 9e 58 b9

源MAC：00 4c 41 49 50 55

协议类型：08 00 ，为IP数据报

IP头：45 00 00 48 00 00 40 00 40 11 a5 4e c0 a80a 01 c0 a80a 05 0c

UDP头：0c 00 00 a2 00 34 ff e0

其余部分都为SNMP报文，接下来我们对照前面的报文结构体来逐个分析一下。

n  30 表示SNMP消息是ASN.1的SEQUENCE类型；

n  2a 表示该SNMP报文的总长度是42(0x2a)个字节，该字段所表示的报文长度起始于它后面的第一个字节直到报文结束；

n  02 01 00 表示版本号，可见其确实为BER编码方式。02表示该字段是INTEGER类型；01表示该字段占1个字节；00表示版本号，该值为“版本号-1”；

n  04 06 70 75 62 6c 69 63 表示团体名，04表示该字段为OCTETSTRING类型；06表示该字段占6个字节；70 75 62 6c 69 63表示团体名的ANSII码的十六进制形式，这里是“public”；

n  a4 1d 其中a4中的“4”表示这是一个trap报文，a4又叫报文的标签标记；1d表示后面还有29(0x1d)个字节的数据；

n  06 0a 2b 06 01 04 01 bf 08 03 02 0a 企业OID标识。06表示该字段是个对象标识符，OBJECTIDENTIFIER；0a表示该字段占10(0x0a)个字节；关于SNMP的OID的编码方式有些奇特：例如1.3.6.1.2…. 取前两个数字分别记为x和y。编码时40\*x+y，这里x=1，y=3，因此结果为40\*1+3=43，即表示十六进制的2b。因此，这里的企业OID编码即为1.3.6.1.4.1.8072.3.2.10；

n  40 04 c0 a80a 01 同样40表示该字段为OCTET STRING 类型；04表示IP地址占4个字节；IP地址为192.168.10.1；

n  02 01 00 其中00表示trap类型为coldStart；

n  02 01 00 其中00表示我们指定的trap即specific-trap也为coldStart类型；

n  43 01 0e 43表示为TimeTicks类型；01表示该字段占1个字节；0e即十进制的14表示时间标签为0.14秒，这里时间计数器以0.01秒递增；

n  30 00 30表示“键-值”值对的编码类型为SEQUENCE；00表示该字段占0个字节，即没有该字段。

**SNMPv2 Trap报文**SNMPv2的Trap报文格式如图8所示：

同样的，这里除了trap类型和报文长度是标准网络字节序之外，其余协议字段也均为BER编码方式。可以看到v2版的trap报文正在向统一的报文格式发展，已经非常类似普通的SNMP请求、响应报文了。

SNMPv2原始报文内容：

00 23 5a 9e 58b9 00 4c 41 49 50 55 08 00 45 00 00 7b 00 00 40 00 40 11 a5 1b c0 a8 0a01 c0 a8 0a05 0c 01 00 a2 0067 04 bb 305d 02 01 01 04 06 70 75 62 6c 69 63a7 50 02 04 1773 2c fb 02 01 00 02 01 00 30 42 30 0d 06 08 2b 06 01 02 01 01 03 00 43 01 0e 30 17 060a 2b 06 01 06 03 01 01 04 01 00 06 09 2b 06 01 0603 01 01 05 01 3018 06 0a2b 06 01 06 03 01 01 04 0300 06 0a2b 06 01 04 01 bf 08 03 02 0a

目的MAC：00 23 5a 9e 58 b9

源MAC：00 4c 41 49 50 55

协议类型：08 00，IP报文

IP头：45 00 00 7b 00 00 40 00 40 11 a5 1b c0 a80a 01 c0 a80a 05

UDP头：0c 01 00 a2 00 67 04 bb

余下部分全为SNMP报文内容，这里我们做一下简单的约定：

xx 标注类型；xx 标注长度；xx 标注真正的数据。

这样一来上面这串原始数据就好分析多了J

n  30 5d 整个SNMP报文的编码方式为30，即SEQUENCE类型，报文长度93(0x5d)字节；

n  02 01 01 版本号01即v2版本；

n  04 06 70 75 62 6c 69 63 团体名70 75 62 6c69 63  即英文的“public”；

n  a7 50 a7表示trap类型为7，即厂商自定义trap；50表示PDU区段占80(0x50)字节；

n  02 04 17 73 2c fb 请求ID为17 73 2c fb 十进制的393424123；

n  02 01 00 错误状态0；

n  02 01 00 错误索引0；

n  30 42 “变量名-值”对编码类型30 即SEQUENCE类型；“变量名-值”所占总字节0x42，即66字节；

n  30 0d 06 08 2b 06 01 02 01 01 03 00 43 01 0e 第一个“名-值”对区段编码方式30 即SEQUENCE类型；第一个“名-值”对总长度0x0d，13字节；第一个变量名的编码类型0x06，时间标签；第一个变量名占0x08个字节；第一个变量名2b 06 01 02 01 01 03 00，为1.3.6.1.2.1.1.3.0；第一个变量值为0x0e，即14；

n  30 17 06 0a2b 06 01 06 03 01 01 04 0100 06 09 2b 06 01 06 03 01 01 05 01 第二个“名-值”对；变量名1.3.6.1.6.3.1.1.4.1.0；变量值1.3.6.1.6.3.1.1.5.1；

n  30 18 06 0a2b 06 01 06 03 01 01 04 0300 06 0a2b 06 01 04 01 bf 08 03 02 0a 第三个“名-值”对；变量名1.3.6.1.6.3.1.1.4.3.0；变量值1.3.6.1.4.1.8072.3.2.10；