Structure d'une trame SNMP-GET

Analyse de trame $IP\left(UDP\left(SNMP\right)\right)$ résultant d'une requête SNMPGET

```
0x0000   4500 0047 0000 4000 4011 8722 c0a8 1914      voir tcpdump -tXS -i eth0 udp port 161
0x0010   c0a8 191f 801f 00a1 0033 b801 3029 0201
0x0020   0004 0670 7562 6c69 63a0 1c02 045f 3935
0x0030   0d02 0100 0201 0030 0e30 0c06 082b 0601
0x0040   0201 0106 0005 00
```

Décomposition de cette trame :
Début en-tête IP :

4500 0047: IPV4, 5*32 bits d'en-tête=20octets, ,Longueur paquet =0x0047=71octets
0000 4000 : numéro du fragment = 0, 4:DF=1 alors ne pas fragmenter, offset du fragment =0
4011 8722 : 0x40*saut de durée de vie, protocole = 0x11 = 17 = UDP , checksum en-tête = 0x8722
c0a8 1914 : adr IP source = 192.168.25.20
c0a8 191f : adr IP cible = 192.168.25.31
Pas de padding dans cette trame et donc les octets suivants sont des octets de données

Début en-tête UDP :

801f 00a1 : Début en-tête UDP avec port d'émission=0x801f, port de réception = 0xA1=161=SNMP
0033 b801 : 0x33=51 octets de données UDP après l'en-tête IP, checksum = 0xb801

Début des données UDP : requête SNMP

3029 :

02 01 00:

04 06 70 7562 6c69 63 :

a0 1c :

02 04 5f39350d :

02 01 00 :

02 01 00 :

30 0e :

30 0c :

06 08 2b 06 01 02 01 01 06 00 :

05 00 :

Structure d'une trame SNMP-RESPONSE

Début des données UDP :

```
30 70
02 01 00

04 06 70 7562 6c 69 63

a2 63

02 04 1d b0 2f df
02 01 00
02 01 00
30 55
30 53

06 08 2b 06 01 02 01 01 01 00

04 47

   4c 69 6e 75 78 20 6c 61 6e 66 65 75 73 74 2e 68 61 72 73 70
   20 32 2e 34 2e 31 39 2d 31 36 6d 64 6b 20 23 31 20 46 72 69
   20 53 65 70 20 32 30 20 31 38 3a 31 35 3a 30 35 20 43 45 53
   54 20 32 30 30 32 20 69 36 38 36
```

- Remarque sur l'indication de la longueur :

si taille<=0x80 alors la longueur est sur 1 octet. Exemple : 0x3029 indique qu'il reste 0x29 octets à interpréter
si 0x80<taille<=0xff alors la longueur est sur 1 octets=> 0x81,0xLL. Exemple : 0x308189 indique qu'il reste 0x89 octets à interpréter
si taille>0xff alors la longueur est sur 2 octets => 0x82,0xHH,0xLL. Exemple : 0x30820189 indique qu'il reste 0x0129 octets à interpréter