1) NET-SNMP : Analyse de la MIB d'un agent

- Analyse d'une trame SNMP : En exploitant le client SNMP créé lors du TP1 et d'un observateur de trames réseau (tcpdump), analyser les trames SNMPGET et SNMPRESPONSE en les décomposant : préciser le rôle de chaque octet.
- Insérer le code suivant dans le code client snmp du TP1 et le tester.

```
o=0;
if(recue[o]==marqueur)   {
    if (recue[o+1]>0x80)o=o+1;
    printf("     marqueur+%doctets\n",(unsigned)recue[o+1]);
    o=o+2;
  }
if((recue[o]==integer)&&(o<4)){printf("   SNMPv%d\n",(unsigned)recue[o+2]+1);o=o+3;}
if((recue[o]==string)&&(o<7))   {
    printf("   Communaute=\"");
    tmp = (char *)malloc(sizeof(char)*(recue[o+1]+1));
    for(j=0;j<recue[o+1];j++)tmp[j]=recue[o+2+j];
    tmp[j]=0;
    printf("%s\"\n",tmp);
    free(tmp);
    o=o+2+recue[o+1];
  }
if(recue[o]==response)   {
    if(recue[o+1]>0x80)o=o+1;
    printf("   PDU SNMP-RESPONSE + %d octets\n",(unsigned)recue[o+1]);
    o=o+2;
  }
if((recue[o]==integer))    {
    val=0;
    for(j=0;j<recue[o+1];j++) val = val *256 + (unsigned)recue[o+2+j];
    printf("     ReqID=%d\n",val);
    o=o+2+recue[o+1];
  }
if(recue[o]==integer) {printf("     ES=%d\n",(unsigned)recue[o+2]);o=o+3;}
if(recue[o]==integer) {printf("     EI=%d\n",(unsigned)recue[o+2]);o=o+3;}
if(recue[o]==marqueur)    {
    if (recue[o+1]>0x80)o=o+1;
    printf("     marqueur+%doctets\n",(unsigned)recue[o+1]);
    o=o+2;
  }
do  {
    if(recue[o]==marqueur){
                if (recue[o+1]>0x80)o=o+1;
                printf("     marqueur+%doctets\n",(unsigned)recue[o+1]);
                o=o+2;
              }
    if(recue[o]==oid){
                printf("OID=");
                tmp = (char *)malloc(sizeof(char)*(recue[o+1]+8+6+20));
                j=0;
                do {
                    if(recue[o+2+j]==iso)strcpy(tmp,"iso.org");
                    else sprintf(tmp,"%s.%d",tmp,(unsigned char)recue[o+2+j]);
                    j++;
                  }while(j<recue[o+1]);
                printf("%s\n",tmp);
                free(tmp);
                o=o+2+recue[o+1];
              }
    if(recue[o]==string){
                tmp = (char *)malloc(sizeof(char)*(recue[o+1]+1));
                for(j=0;j<recue[o+1];j++)tmp[j]=recue[o+2+j];
                tmp[j]=0;
                printf("\"%s\"\n",tmp);
                free(tmp);
                o=o+2+recue[o+1];
              }
    if((recue[o]==integer)){
                val=0;
                for(j=0;j<recue[o+1];j++) val = val *256 + (unsigned)recue[o+2+j];
                printf("%d\n",val);
                o=o+2+recue[o+1];
              }
    if((recue[o]==timeticks)){
                val=0;
                for(j=0;j<recue[o+1];j++) val = val *256 + (unsigned)recue[o+2+j];
                printf("timeticks=%d\n",val);
                o=o+2+recue[o+1];
              }
    if((recue[o]==gauge))    {
                val=0;
                for(j=0;j<recue[o+1];j++) val = val *256 + (unsigned)recue[o+2+j];
                printf("Gauge32=%d\n",val);
                o=o+2+recue[o+1];
              }
  }while(o<(nb-1));
```

2) NET-SNMP : Analyse des objets gérés d'un agent

2.1) PDU SNMPGET

- Dans la MIB, localiser l'objet décrivant le système.
  - Après analyse de la commande "**snmpget**" du projet 'NET-SNMP", afficher la description du système à savoir : **system.sysDescr.0** ou 1.3.6.1.2.1.1.1.0
  - Avec cette commande, scruter les objets du noeud ".**system**" de la "**mib-2**"
- Quelles sont les contraintes de cette commande (ou requête SNMP)

2.2) Configuration

- Afin de rendre accessible cet agent sur le LAN,

  - **VERSION 5.4.3** :Si la commande 'snmpstatus -V' retourne la chaîne : 'NET-SNMP version: **5.4.3**' :
    - Modifier le fichier '**/etc/snmp/snmpd.conf**'
      - en plaçant en commentaire la ligne '`agentAddress udp:127.0.0.1`' afin que tout agent puisse accéder à la mib
      - Dans les ACCESS CONTROL,
        - Ajouter la ligne '`view systemonly included .1.3.6.1.2.1.2`' permettant de rendre accessible le noeud 'interfaces'
        - Ajouter la ligne '`view systemonly included .1.3.6.1.2.1.4`' permettant de rendre accessible le noeud 'ip'
    - Modifier le fichier '**/etc/snmp/snmp.conf**'
      - Ajouter la ligne '`mibdirs /usr/share/snmp/mibs/`'
      - Ajouter les lignes '
        - `mibs HOST-RESOURCES-MIB`
        - `mibs +IP-MIB`
    - Décompresser 'philippe.hars.free.fr/**mibs/mibs.zip**' dans le répertoire '**/usr/share/snmp/mibs**' que vous aurez créé
    - Par exemple, rajouter les MIBS cisco sur le manager :
      - site '**ftp://ftp.cisco.com/pub/mibs/**'
      - donc dans le répertoire '`/usr/share/snmp/mibs`'
    - redémarrer snmpd
    - tester snmpget en précisant les noms des nœuds (system.sysDescr.0 par exemple).

2.3) PDU SNMPGETNEXT

- Après analyse de la commande "**snmpgetnext**" du projet 'NET-SNMP", scruter une partie des objets du noeud "**.interfaces**" de la "**mib-2**". Conclusion

- Tester dans une requête plusieurs OIDs.

- Tester : snmpget *agent* -c public -v 2c **-O vq** system.sysDescr.0

- Réaliser une requête produisant une réponse erronée et analyser la trame ainsi obtenue en utilisant l'option -d, exemple : snmpget 127.0.0.1 -d -c public -v 1 system.sysDescr

3) Arborescence de la MIB d'un Agent

- Après analyse de la commande "**snmptranslate**" du projet 'NET-SNMP" avec les options '-Tp' et '-IR', puis scruter les objets du noeud '**ip**' de la "**mib-2**"
- Analyser l'arbre obtenu du noeud '**ip**'.
- On désire connaître les interfaces réseau d'un agent et obtenir les informations sur chacune d'elle. Indiquer les objets de la MIB à scruter ainsi que la méthode pour les obtenir (interfaces.ifNumber.0). Appliquer votre méthode sur un agent. On pourra comparer les résultats avec la commande "**ifconfig**" . On pourra obtenir avec "**snmptranslate**" des informations précises sur chaque objet désiré.

  - Compléter le tableau :

Informations	*OID*	*Interface 0*	*Interface 1*	*Interface 3*
Nombre d'interfaces	interfaces.ifNumber.0			
Index de l'interface	interfaces.ifTable.ifEntry.ifIndex.i	1	2	3
Type d'interface (ifType)				
Nom interface(ifDescr)		lo		
Adresse mac(ifPhysAddress)				
Vitesse de l'interface(ifSpeed)				
État de l'interface(ifOperStatus)				
Nombre d'erreur en sortie (ifOutErrors)				
Paquets reçus (ifInUcastPkts)				
Paquets transmis (ifOutUcastPkts)				
...				

- Que réalise les commandes :
  - snmpgetnext 127.0.0.1 -c public -v 1 **ip.ipAddrTable.ipAddrEntry.ipAdEntAddr**
  - snmpgetnext 127.0.0.1 -c public -v 1 ip.ipAddrTable.ipAddrEntry.ipAdEntAddr**.127.0.0.1**
  - snmpgetnext 127.0.0.1 -c public -v 1 ip.ipAddrTable.ipAddrEntry.**ipAdEntIfIndex**
  - snmpgetnext 127.0.0.1 -c public -v 1 ip.ipAddrTable.ipAddrEntry.ipAdEntIfIndex**.127.0.0.1**
  - snmpgetnext 127.0.0.1 -c public -v 1 ip.ipAddrTable.ipAddrEntry.**ipAdEntNetMask**
  - snmpgetnext 127.0.0.1 -c public -v 1 ip.ipAddrTable.ipAddrEntry.ipAdEntNetMask**.127.0.0.1**
  - snmpgetnext 127.0.0.1 -c public -v 1 ip.ipAddrTable.ipAddrEntry.**ipAdEntBcastAddr**
  - snmpgetnext 127.0.0.1 -c public -v 1 ip.ipAddrTable.ipAddrEntry.ipAdEntBcastAddr**.127.0.0.1**

4) Scripts Shell d'analyse d'une interface

- Analyser le script suivant, le tester et commenter l'affichage qui en résulte :

```
#!/bin/bash
if [ $# -lt 1  ] ; then
    echo "Usage $0 hostname indexinterface. Exemple : $0 192.168.25.1 2 "
else
    debut="interfaces.ifTable.ifEntry"
    if [ $# -gt 0 ] ; then
       hote=$1
    else
       hote=localhost
    fi
# utiliser AltGr 7 pour `
    a=`snmpget -c public -v 1 -Oqv ${hote} interfaces.ifNumber.0`
    echo "Il y a $a interface(s) reseau sur ce materiel."
    interface=1
    if [ $# -gt 1 ] ; then
              if [ $2 -gt 0 -a $2 -le $a ] ; then
                 interface=$2
        fi
    fi
    echo "Voici les caracteristiques de l'interface dont l'index et $interface :"
    for obj in ifIndex ifDescr ifType ifMtu ifSpeed ifPhysAddress ifAdminStatus ifOperStatus ifLastChange
ifInOctets ifInUcastPkts ifInNUcastPkts ifInDiscards ifInErrors ifInUnknownProtos ifOutOctets ifOutUcastPkts
ifOutNUcastPkts ifOutDiscards ifOutErrors ifOutQLen ifSpecific
    do
#A decommenter pour afficher la commande
#             echo "snmpget -c public -v 1 ${hote} ${debut}.${obj}.${interface}"
             a=`snmpget -c public -v 1 -OQs ${hote} ${debut}.${obj}.${interface}`
             echo "$a"
    done
fi
exit 0
```

6)Affectation d'objets d'un agent

- Repérer dans la mib les interfaces à l'aide de la commande : `snmptranslate -Tp -IR interfaces`
- Repérer le nombre d'interfaces réseau d'un agent
- Repérer l'état d'une interface réseau d'un agent ainsi que la demande du changement de son état.
- Peut-on désactiver une interface réseau d'un agent et comment. Il y a-t-il des contraintes à cette affectation?

- Tester la désactivation de l'interface "eth0" puis sa réactivation en utilisant SNMPv2. Interpréter vos observations.

7) Divers

- Que réalise la commande '`snmpstatus -c public -v 1 127.0.0.1`'
- Tester la commande '`snmpwalk agent -c public -v 2c interfaces`'
- Tester la commande '`snmpbulkget`' en listant toutes les données des noeuds '`system`' et '`ifTable`'
- Tester la commande '`snmpbulkwalk`' en listant toutes les données du noeud '`at`'

8) NET-SNMP : Les Traps

- Quel est le rôle de la commande snmptrap ?
- Commenter les paramètres suivants ainsi que le résultat affiché de la commande suivante :

```
snmptrap -v 2c -c <COMMUNAUTE> -d <MANAGER> '' 1.3.6.1.6.3.1.1.5.3 ifIndex i 2 ifAdminStatus i 1
ifOperStatus i 2
OU
snmptrap -v 2c -c public -d 192.168.25.60 ''
snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTraps.linkDown ifIndex i 2 ifAdminStatus i 1
ifOperStatus i 2
```

- Quel est le rôle de `snmptrapd`?
- Pour Ubuntu18
  - Utiliser la commande : `sudo systemctl edit snmptrapd.service`
    OU éditer le fichier /*etc/*`systemd/system/snmptrapd.service.d/override.conf`
  - Y insérer les 3 lignes suivantes :

```
[Service]
ExecStart=
ExecStart=/usr/sbin/snmptrapd -Ln -f -Lf /var/log/snmptrapd.log
```

  - Utiliser la commande :`sudo systemctl daemon-reload`
  - Relancer le service :`sudo systemctl restart snmptrapd.service`
  - Vérifier le service :`systemctl status snmptrapd.service`
  - Éditer le fichier : `/etc/snmp/snmptrapd.conf`
  - Y insérer les 2 lignes suivantes :

```
ignoreAuthFailure yes
disableAuthorization yes
```

  - Autre vérification : ps ax | grep snmp

```
/usr/sbin/snmptrapd -Ln -f -Lf /var/log/snmptrapd.log
```

Tester le script suivant :

```
#!/bin/bash
manager="127.0.0.1"
echo "Usage   : $0 manager (Exemple : $0 $manager)"
if [ $# -ge 1 ]; then
 manager=$1
fi
#1.3.6.1.6.3.1.1.5.3=internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTraps.linkDown
#   manager="x.x.x.x" uptime=''  trap-oid=linkDown
#   OID=ifIndex:Integer:2 => InterfaceDontIndexVaut2
#   OID=ifadminStatus:Integer:1  => Up
#   OID=ifOperStatus:Integer:2   => Down
snmptrap -v 2c -c public -d $manager '' 1.3.6.1.6.3.1.1.5.3 ifIndex i 2 ifadminStatus i 1
ifOperStatus i 2
exit 0
```

  - Vérifier le contenu du fichier log : `more /var/log/snmptrapd.log`
  - Modifier le script afin d'indiquer que l'interface 3 est passée de l'état Down à l'état Up
  - Quel effet a l'ajout de l'option -On dans la ligne ExecStart
  - Changer l'affichage des logs :
    - Éditer le fichier */etc/*`snmp/snmptrapd.conf`
    - En vous aidant du manuel de snmptrapd, ajouter la ligne suivante dûment complétée :
      format2 Trap emis depuis ……\n\tDate heure locale ../../…. .. :.. :..\n\tDate heure systeme ../../…. .. :.. :..\n\tDescription : …….\n\tVariables : ……..\n\n

Sur la documentation d'un switch Dlink type DGS3627, donner les commandes de configuration permettant d'activer les traps snmp et d'émettre un trap à chaque changement d'état d'un des ports de ce switch.

- Analyser `snmptrapfmt` et son fichier de configuration.