UNIVERSITÉ CAEN NORMANDIE

La supervision : *Monitoring* 23.02.2023

Je n'ai que 2 yeux ☹

It is the responsibility of the NOC to notify staff and customers if there are any problems on the network....

Auteur : Pascal Fougeray

source : **http://indianatelephonenetwork.com/support/network-outages/**

---

1 Introduction

La supervision ou monitoring des réseaux, un vaste programme...

L'objectif de la supervision des réseaux est d'avoir un réseau opérationnel sans rupture de service, ce qui définit une certaine Qualité de Service (**QoS**) offerte par l'opérateur, l'administrateur à l'abonné, l'utilisateur.

2 Définitions

- Administrer, Superviser ou Exploiter ?
  - **Administrer** : c'est se connecter sur une machine, lancer des commandes, modifier des droits, lancer un processus, des logs via un protocole tel *syslog* etc...,
  - **Superviser** : c'est
    - collecter en **temps réel** des informations sur l'utilisation, sur les évènements etc...
    - interroger périodiquement (le ***polling***)

    les éléments **actifs** du réseau, un serveur, un *switch*, un routeur, un DSLAM ADSL etc...
  - **Exploiter** : c'est traiter les problèmes opérationnels sur le réseau, ce qui recouvre la **supervision**, mais aussi la **maintenance**, le **support** et l'**assistance technique**.

On doit pouvoir localiser le plus rapidement possible toute défaillance.

Si on se réfère l'ISO (***International Standard Organization***), 5 axes de gestion existent

1. La gestion des **anomalies** ou des **fautes** : ***Fault Management*** ou ***monitoring***.
   => gérer les **alarmes** émises par le réseau, on localise un incident par un diagnostic des alarmes, on "***journalise***" les problèmes. . .
   — Garder une trace des changements
   - Consigner tous les changements
   - Identifier plus facilement les problèmes liés aux mises à niveau et modifications de configuration
   — Conserver l'historique des opérations réseau
   – Un système de tickets permet de garder l'historique des évènements
   – L'historique permet de vous défendre et de vérifier ce qui s'est passé.
2. La gestion de la **configuration réseau** : ***Configuration Management***
   => gérer les configurations **matérielle** et/ou **logicielle** du réseau pour en **optimiser l'utilisation**.
   Chaque équipement est identifié à l'aide d'un nom ou identificateur d'objet unique **OID :** ***Object Identifier*** .
3. La gestion des **performances** : ***Performance Management***
   => gérer en **temps réel** le réseau, afin de vérifier s'il peut **écouler** le **trafic** demandé.
   — Être informé des problèmes
   — Avoir une longueur d'avance sur les utilisateurs est bon pour l'image du FAI.
   — Des logiciels de surveillance peuvent générer des tickets et informer automatiquement les gestionnaires (administrateurs réseau ou système) des problèmes.
4. La gestion de la **sécurité** : ***Security Management***
   => gérer les contrôles d'accès au réseau, la **confidentialité** , l'**intégrité** et l'**authentification** des données qui y transitent.
   — Difficile de savoir si un problème est une panne ou attaque en cours
   — Différence entre un Déni de Services ***DoS*** et une panne de réseau ?
   — Tendances et automatisation permettent de savoir si une attaque est en cours !
   — Les outils utilisés peuvent aider à mitiger le succès d'une attaque :
   — Les flux sur un interface,
   — Une charge anormale sur des serveurs,
   — Des pannes de service.
   — etc...
5. La gestion de la **comptabilité** : ***Accounting Management***
   => gérer la consommation réseau par abonné dans un but de **facturation**.
   — Suivi de l'utilisation des ressources
   — Facturation des clients en fonction de l'utilisation

Un administrateur système/réseau d'un réseau local d'une entreprise administre le système d'exploitation et le réseau.

Cette administration est facile, mais les difficultés s'amoncèlent proportionnellement à la taille du réseau.

La solution est alors de rationaliser, de normaliser les méthodes.

Des **normes** ont été alors proposées pour la supervision des réseaux.

— L'**ISO** a proposé dans les années 80 la norme **CMIS/CMIP**, ***Common Management Information Service*** ISO 9595, ***Common Management Information Protocol*** ISO 9596 comme protocole d'administration des réseaux.
— L'**IAB**, ***Internet Activities Board*** ,approuve, dans un premier temps, le protocole **SNMP** (*Simple Network Management Protocol*) et par la suite CMOT (*CMIP Over TCP*).

3 Network Operations Center

Un centre d'opérations d'un réseau, ***Network operations center*** : **NOC**, est un service, dans le sens administratif et non informatique, chargé

— du contrôle des transactions,
— de la surveillance des incidents,
— de la charge d'un réseau LAN ou WAN,

— L'administration du réseau, les tâches courantes de tous les jours avec une astreinte **24/24 7/7 365/an** de façon à avoir une **GTR** (*Garantie de Temps de Rétablissement*) ou **RCS** (Rétablissement de la Continuité de Service) en moins de x heures. Dans les milieux Anglo-Saxon, on parle de GRS *Guaranteed Return to Service* ou bien de **MTTR** *Mean Time To Repair* ou bien de **MDT** Mean Down Time
— La mise en place de nouveaux services pour les clients,
— L'administration des accès et la gestion en temps réel de la bande passante, en modifiant par exemple le TE, ***Traffic-Engeniering***.
— etc...

source : **http://commons.wikimedia.org/wiki/File:Batelco_Network_Operations_Centre_%28NOC%29.JPG**

4 Les protocoles de supervision

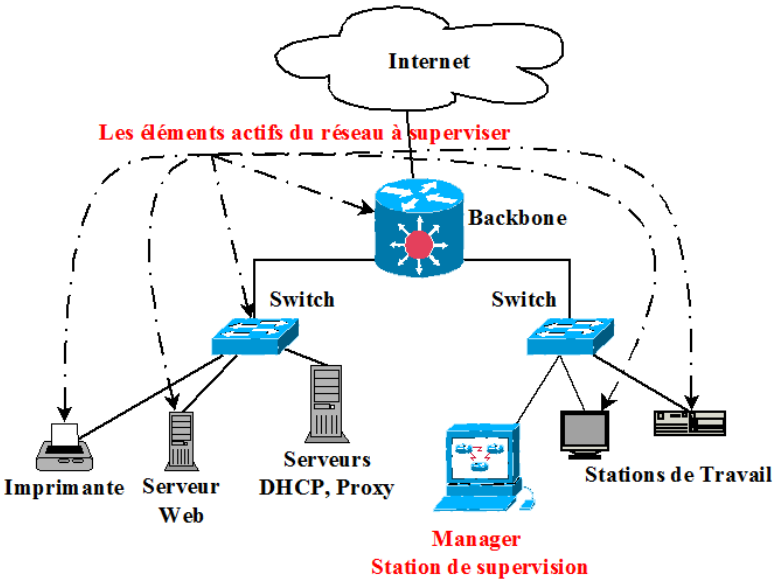
Les protocoles de gestion de réseaux sont nombreux, mais seuls 2 d'entres eux sont standardisés :

1. **CMIP – Common Management Information Protocol**
   Il fonctionne avec la pile de communication OSI.
   Il fonctionne sous UDP/IP avec les ports 163 et 164.
   Remarque : Comme le temps, nous est compté, si vous désirez plus de renseignements sur ce protocole, je vous invite à aller sur le site : http://www.faqs.org/rfcs/rfc1189.html
2. **SNMP – Simple Network Management Protocol**
   Il fonctionne nativement sous UDP/IP avec les ports 161 et 162, mais pas seulement, voir plus loin.
   C'est ce protocole que nous allons étudier et utiliser en TD/TP.
3. **WMI - Windows Management Instrumentation**
   Exemple, si vous devez administrer un réseau ne contenant que des machines Windows©, clients et serveurs, alors rien ne vous empêche d'utiliser cette technologie WMI.
   Le principe est proche de SNMP, les agents sont déjà installés sur les postes clients et la machine de supervision n'a plus qu'à les interroger.
   Pour plus d'informations, voir l'URL : http://msdn.microsoft.com/en-us/library/aa394582%28v=vs.85%29.aspx

5 Le principe et les entités

L'environnement de gestion SNMP est constitué de 4 entités :

1. La **station de supervision**, ***manager*** exécute les applications de gestion qui contrôlent les éléments réseaux, c'est un ordinateur "quelconque",
2. Les **éléments actifs** du réseau, ***agents SNMP*** : les équipements actifs ou les logiciels que l'on désire superviser.
3. Le **protocole SNMP**, ***Simple Network Management Protocol*** : de couche 7, il permet à la station de supervision de récupérer des informations sur les éléments actifs du réseau et de recevoir des alertes ou alarmes, les ***traps*** provenant de ces éléments actifs.
4. Les variables **MIB**, *Management Information Base* est un ensemble d'objets résidant dans une base d'information virtuelle.



5.1 Le *manager*

L'administrateur système doit alors disposer sur sa machine de supervision d'un outil appelé ***manager***.

C'est un **client** qui envoie les requêtes aux divers agents SNMP du réseau.

Il devra disposer aussi d'une **fonction serveur**, car il reste à l'écoute des alertes, signaux d'alarmes, que les divers équipements actifs du réseau peuvent émettre à tout instant.

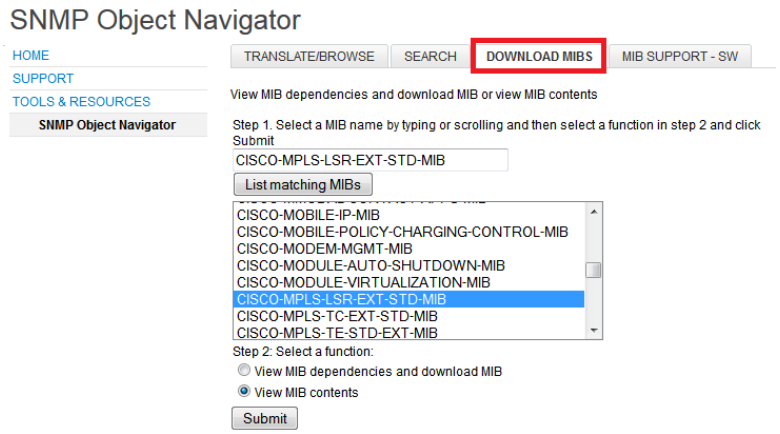
Cette écoute se fait nativement sur le port **UDP 162** mais pas obligatoirement, elle peut-être fait sur un autre port selon la configuration choisie.

5.1.1 Sa constitution

La station de gestion du réseau contient :

— Le protocole de communication, la pile IP avec le protocole SNMP,

— Des bases de données, **MIB**, identiques à celles déployées dans les éléments actifs du réseau et ainsi tous les ***objets*** connus des systèmes à administrer.
Si le manager ne possède pas cette base de données, il ne pourra pas interroger les différents éléments actifs du réseau à surveiller.
Il est possible de récupérer ces MIB chez les fabricants de ces éléments actifs.
Par exemple pour Cisco, il suffit d'aller sur le site :
http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2, comme le montre la figure suivante



Un autre site : ***Circitor*** http://www.circitor.fr/Mibs/Mibs.php

— La MIB des routeurs Mikrotik : http://www.circitor.fr/Mibs/Html/M/MIKROTIK-MIB.php

— Les applications de gestion des bases de données, **MIB**, donc un **serveur de base de données** tels *mysql*, *OracleDB* etc...

— Une interface graphique pour visualiser les cartes, souvent Web, donc **un serveur Web** tels *nginx* ou *Apache2*.

5.1.2 Des exemples de manager

Il en existe plein pour des usages bien différents et selon que l'on soit peu ou prou copyleft ou copyright.

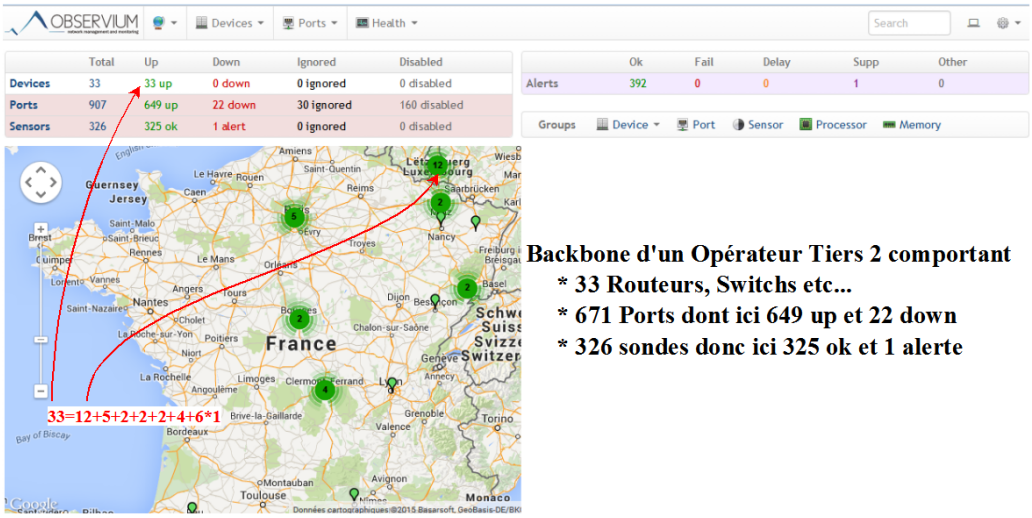
- Des **libres** :
  - ***Nagios*** : http://www.nagios.orgNagios™ (Netsaint) C'est un logiciel libre sous licence GPL. C'est un programme modulaire découpé en 3 parties :
    1. Le moteur de l'application qui vient ordonnancer les tâches de supervision,
    2. L'interface web, qui permet d'avoir une vue d'ensemble du système d'information et des possibles anomalies,
    3. Les *plugins*, plus d'une centaine (http://nagiosplugins.org/man) modifiables en fonction de ses besoins afin de superviser les services ou ressources disponibles des équipements réseaux.
  - ***Zabbix*** : http//www.zabbix.com
  - ***openNMS*** : http//www.opennms.org
  - ***Shinken*** : http://www.shinken-monitoring.org
  - ***Centreon*** : http://www.centreon.fr/
- Une liste plus exhaustive
  - http://www.simpleweb.org/software/
  - Le panorama de la supervision : http://wiki.monitoring-fr.org/supervision/links
- Des **non libres** : les offres des éditeurs
  - **HP** : Openview (NNM, OVO, ...) : Système développé par HP permettant d'administrer un réseau décentralisé.
    https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-10{}36657_4000_100&jumpid=h
  - **IBM** : Tivoli : voir l'url http://www-01.ibm.com/software/fr/tivoli/
  - ***WhatsUpGold d'Ipswitch*** : http://www.whatsupgold.com/fr/
  - ***Network Performance Monitor*** de Soladwinds : http://www.solarwinds.com/network-performance-monitor.aspx
  - ***Observium*** : http://www.observium.org/
    Ils ont une démo live excellente ! ! ! http://demo.observium.org/ **A VOIR ! ! !**

5.1.2.1 Un exemple d'exemples L'image suivante représente l'utilisation réelle ! ! ! d'un backbone Réel d'un tiers 2

Comme c'est une interface Web, on utilise le protocole HTTPs donc pas de filtrage !

Avec cet outil on peut :

- Tout connaitre en **temps réel,** le **présent**
- **analyser** tout ce qui s'est passé**,** le **passé**
- intervenir à distance ou bien envoyer des équipes d'interventions
- prévenir des futurs pannes, le **futur**



5.1.3 GPL vs Other...

Non, je ne vais pas vous dire que l'un est mieux que l'autre, je laisse cela à ceux qui n'ont pas grand chose à faire...

En TP nous utiliserons une version disons payante en démo, pourquoi, car c'est beaucoup plus rapide à installer et que nous n'avons pas le temps d'administrer une solution telle que Nagios ou Centreon.

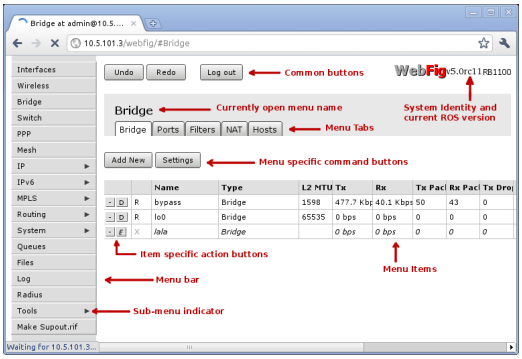
Vous ferez cela avec mon collègue durant la seconde partie de ce module M3108c.

5.1.4 Le management Web

Il est possible de gérer un équipement actif directement par son interface Web.

En effet sur chaque équipement, il y a un serveur web qui tourne, il suffit de configurer le routeur pour qu'il accepte.

Nous l'vons vu sur lors du TP NAT2 !



5.2 Les agents

Chaque équipement, ordinateurs, routeurs, ponts, commutateurs... que l'on voudra **superviser** doit disposer d'un **agent SNMP**.

Cet agent est un **serveur**, qui est en permanence à l'écoute du port **UDP 161** mais pas obligatoirement, il peut-être fait sur un autre port selon la configuration choisie.

— Lorsqu'il recevra une requête, il y répondra, mais seulement si la requête est émise par une **entité autorisée,** voir configuration ***acl*** un peu plus loin.

— L'agent peut agir sur l'environnement local, si l'administrateur souhaite modifier un paramètre

— L'agent peut aussi émettre des alarmes, il doit être configuré pour cela.
Exemple : si le débit sur une interface réseau atteint une valeur considérée par l'administrateur comme critique, si une de ses interfaces passe en "*down*" pour un "*switch*".
Il existe une multitude d'alarmes possibles, suivant la complexité de l'agent. La température du processeur, le taux d'occupation des disques durs et du CPU, la charge du serveur Web etc...

Il est indispensable que ces **informations remontées par les agents soient de bonne qualité et en premier lieu fiables**

Il y a 2 solutions pour cela :

1. La solution logicielle, c'est souvent le cas, le processeur partage son temps entre sa tâche principale qui peut être pour un *switch* le transfert de paquets et celle du traitement des alarmes et du comptage des statistiques.
2. La solution matérielle : plus performante, c'est d'ajouter une sonde **RMON**

5.3 Les sondes ou agents RMON

Pour cette partie on se rapproche du cours l'analyse de ***logs*** et la supervision de la sécurité d'un réseau.

Le standard **RMON** (***Remote network Monitoring***) est fondé sur l'utilisation du protocole de gestion SNMP et met en jeu 2 composants :

1. un gestionnaire SNMP
2. des agents SNMP prenant RMON en charge.
   L'association des 2 composants correspond à **un système d'analyseurs réseaux distribués**.

Une sonde **RMON** a pour fonction principale de **capturer** ou d'**analyser** les flux de paquets de données d'un réseau sans incidence sur son débit.
Les sondes RMON sont disponibles sous plusieurs formes.

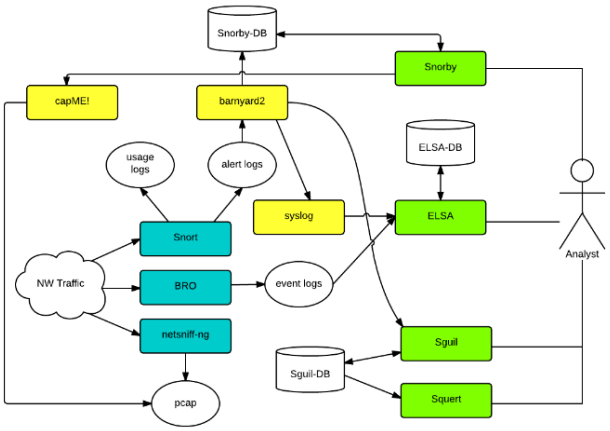
— Les équipements dédiés (***appliance*** : produit, matériel et logiciel permettant de répondre à un besoin par une solution clef en main.) à cette fonction, tel :

Netscout http://www.netscout.com/Pages/default.aspx

— Les équipements non dédiés incluant des agents RMON pour certains commutateurs Ethernet.
— Sous forme de logiciel à installer sur des systèmes d'exploitation Windows ou Gnu/Linux (Sonde Network Instruments, Distributed Sniffer, RMONster32, Netscout Probe).

La solution sur le Campus3,solution à l'aide d'un serveur, donc un ordinateur avec un système d'exploitation d'installé.

1. ***Security Onion*** http://blog.securityonion.net/p/securityonion.html : une distribution gnu/linux pour la détection d'intrusion, la supervision du réseau et la gestion des journaux de bords (***logs***). Elle est basé sur Ubuntu et contient les logiciels suivants :



Snort système de détection d'intrusion (IDS) et de prévention d'intrusion (IPS)

Suricata un IDS Detection d'Intrusion / IPS Prévention d'Intrusion Open Source https://suricata.io/

OSSEC Agent détecteur d'intrusion sur machine hôte https://www.ossec.net

Sguil Une interface open source de surveillance de la sécurité réseau clients lourds http://sguil.sourceforge.net/

Squert, Interface PHP à la base de donnée Sguil http://www.squertproject.org/

Snorby, Web 2.0, Ajax, Ruby-on-Rails (Interface « Cool ») http://ww1.snorby.org/

ELSA, **E**nterprise **L**og **S**earch and **A**rchive

NetworkMiner, Analysez le réseau pour obtenir des informations détaillées sur les hôtes disponibles https ://sourceforge.net/projects/networkminer/

et beaucoup d'autres outils de sécurité...

L'assistant de configuration simple à utiliser permet de construire une armée de capteurs distribués assez rapidement

5.4 MIB [1] I & II

La **MIB** (***Management Information Base***) ou **Base de données d'informations de gestion pour la gestion de réseaux**, est une base de données d'informations, elle est propre à chaque équipement et chaque type de réseau. Par exemple, la MIB *Ethernet* est différente de la MIB d'*ATM*.

Elle est définie par les RFC

— 1213 https://tools.ietf.org/html/rfc1213 *Management Information Base for Network Management of TCP/IP-based internets : MIB-II*
— 4113 **https://tools.ietf.org/html/rfc4113** *Management Information Base for the User Datagram Protocol (UDP)*

Un fichier MIB est un document texte écrit en langage **ASN**.1 (*Abstract Syntax Notation 1*).

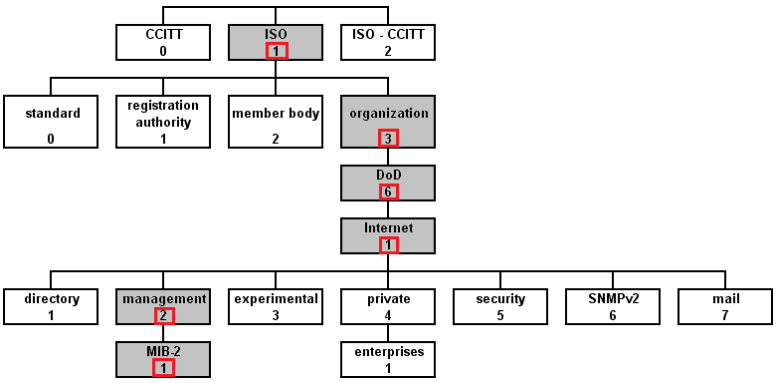
Il décrit les variables, les tables et les alarmes gérées au sein d'une MIB.

Un extrait du fichier *HOST-RESOURCES-MIB* que l'on peut trouver dans le répertoire */usr/share/snmp/-mibs* sous les systèmes de type UNIX.

1. Non cela n'a rien à voir avec le célèbre film : Men In Black :)

5.4.1 Détails de la MIB : Hiérarchie des objets, MIB privées et extensions

Hiérarchie des objets, nommage et OID
Pour identifier chaque objet, l'IETF y a associé un code unique dans la MIB 2.
Voici le début de la structure hiérarchisée de la MIB I

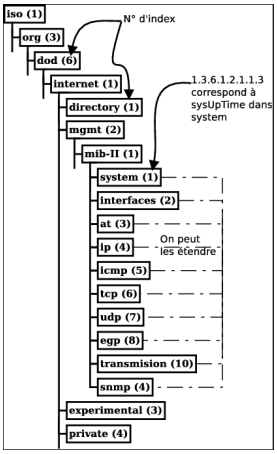


5.4.2 La structure

Elle est organisée hiérarchiquement, à la manière de l'arborescence des domaines Internet.
Elle contient 3 parties :

1. une partie commune à tous les agents SNMP en général,
2. une partie commune à tous les agents SNMP d'un même type de matériel,
3. une partie spécifique à chaque constructeur.

— Sa structure et ses appellations des diverses rubriques sont normalisées.
— Ces appellations ne servent qu'à rendre les choses plus lisibles.
— Chaque niveau de la hiérarchie est repéré par un index numérique par exemple ***1.3.6.1.2.1.1.3*** qui correspond à ***SNMPv2-MIB : :sysUpTime***
— SNMP n'utilise que cet index pour récupérer les informations.



5.4.3 La consultation de la MIB

Le protocole SNMP permet de lire et d'écrire dans cette MIB. Il existe pour cela, un ensemble de commandes[2]. Voir plus loin le chapitre intitulé le protocole SNMP.

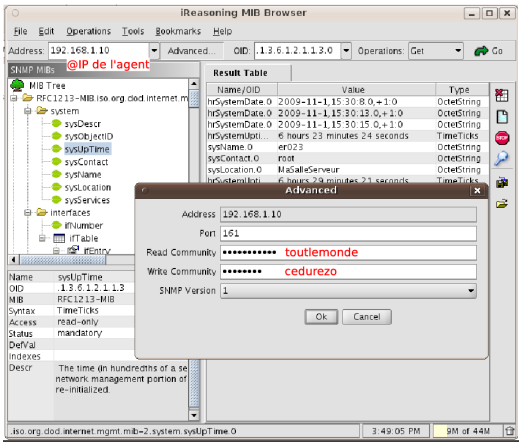
Comme nous pouvons lire et écrire, il y a une notion de droits à respecter. On parle alors de communauté.

5.4.4 Les lecteurs de MIB ou MIB browser

Nous verrons plus loin que les commandes SNMP pour consulter la MIB sont assez "indigestes". Heureusement, il existe des outils pour lire les MIBs. Certains sont gratuits et d'autres payants...

— ***tkmib*** : juste pour information... , fonctionne sous Linux et Mac OS X
— ***mibbrowser*** de *ireasoning* : http://www.ireasoning.com/, nous allons l'utiliser en TP.
Il fonctionne sous les 3 principaux systèmes d'exploitation.
Pour le télécharger, voir l'url suivante : http://www.ireasoning.com/downloadmibbrowserlicense.shtml
Pour l'utiliser, je vous invite à consulter l'aide en ligne : http://www.ireasoning.com/browser/help.shtml
L'image suivante donne un aperçu de son utilisation.

2. Assez indigestes :)



— ***loriotpro*** que l'on peut télécharger et tester facilement : http://www.loriotpro.com/index_FR.php, il fonctionne sous Windows.

5.4.5 Les extensions de la MIB

Au bout d'un moment, les variables choisies pour la MIB (puis la MIB2) se sont avérées insuffisantes pour plusieurs applications. On trouve ainsi 2 autres types de MIB :

1. les Private MIB, représentées en 1.3.6.1.4 dans la classification SMI, elles permettent aux entreprises de rajouter des variables pour une implémentation particulière des agents SNMP. Cela leur permet d'ajouter de nouvelles variables en fonction des applications qu'elles veulent développer.
2. les MIB R-MON ***Remote network MONitoring,*** elles permettent par exemple de placer des agents SNMP sur le trafic. L'administrateur pourra l'interroger pour avoir des informations sur les collisions, les débits à un endroit précis.

5.5 Le protocole SNMP

SNMP pour Simple Network Manager Protocol ou Protocole simple de gestion de réseau

Au début des années 90, le protocole SNMP (*Simple Network Management Protocol*), par sa "simplicité", devient le **standard** et est adopté par les différents constructeurs.

C'est actuellement LE protocole de supervision des réseaux IP, et aussi des réseaux d'opérateurs tel MPLS.

SNMP est donc désormais un standard ! ! !

Ce protocole permet d'interroger la base d'informations, MIB d'un équipement capable de traiter les messages SNMP.

Ce protocole dispose d'un ensemble de commandes qui permettent d'interroger la MIB.

5.5.1 Les versions de SNMP

SNMP se décline en différentes versions : v1, v2, v2c, v3...

v1 RFC 1157 : Sécurité problématique, la seule vérification qui est faite est basée sur les chaines de caractères "*community*" (*public* et *private*...).

sec RFC 1351, 1352 et 1353, elle ajoute de la sécurité à SNMP v1, elle est très peu utilisée.

v2p amélioration du protocole SNMP et intégration de la sécurité de SNMP sec.

v2c RFC 1901, 1905 et 1906 amélioration du protocole mais avec la sécurité de SNMP v1.

v2u RFC 1905, 1906, 1909 et 1910, v2c avec la sécurité basée sur les usagers **USM**, ***User-based Security Model***.

v3 : Reprend le meilleur en protocole et en sécurité de v2p et v2u : Messages type v2 et sécurité basée sur USM et **VACM**.

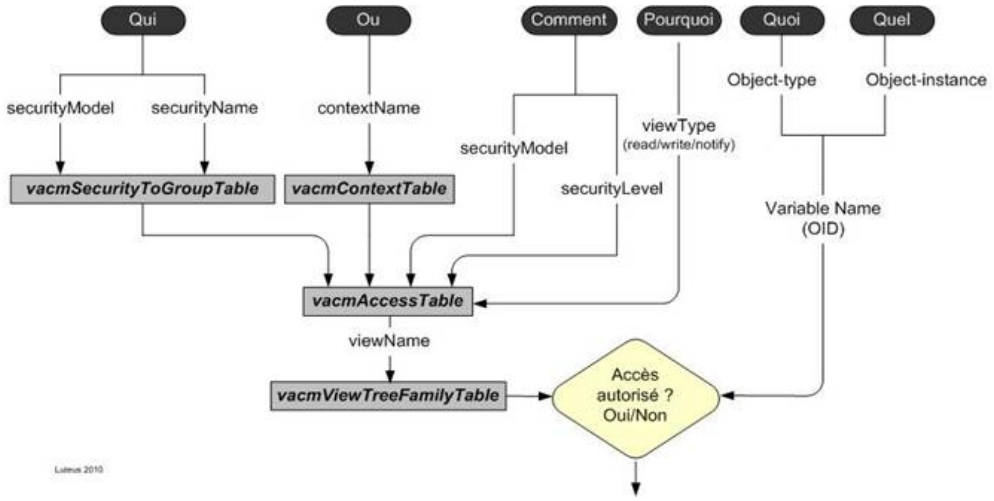
USM : 3 mécanismes différents ayant pour seul but d'empêcher un type d'attaque :

1. **L'authentification** : Empêche quelqu'un de changer le message SNMPv3 en cours de route et de valider le mot de passe de la personne qui transmet la requête. Basé sur HMAC-MD5-96 ou HMAC-SHA-96

2. Le **chiffrement** : Empêche quiconque de lire les informations de gestions contenues dans un message SNMPv3. Basé sur DES.
3. **L'estampillage du temps** ou **horodatage** : Empêche la réutilisation d'un message SNMPv3 valide et déjà transmis par quelqu'un.

VACM : Permet le contrôle d'accès au MIB. Ainsi on a la possibilité de restreindre l'accès en lecture et/ou écriture pour un groupe ou par utilisateur

Plus d'informations : **http://www.frameip.com/snmp/#VACM_%28View_Access_Control_Model%29**



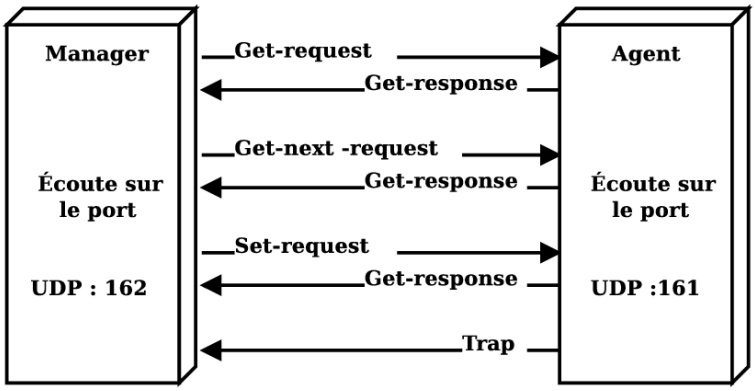
Source :

http://www.loriotpro.com/Products/AgentSNMP-NuDesign/Agent-SNMP-NuDesign_fichiers/image004.jpg

Plus d'informations ici :
http://www.frameip.com/snmp/#User_Security_Module_%28USM%29

5.5.2 Les ports et le dialogue SNMP

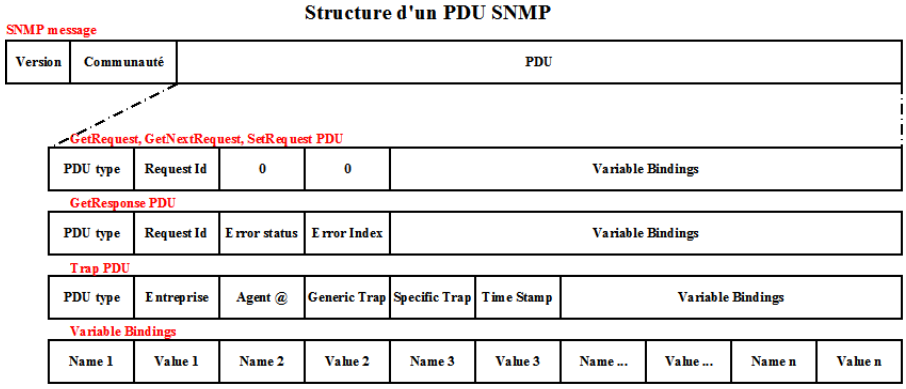
Le dialogue SNMP se fait nativement sur les ports 161 et 162 en **UDP**.
Pourquoi 2 ports ?
— Le port 161 pour l'agent et ne concerne que les demandes du manager à l'agent.
— Le port 162 pour le manager et ne concerne que les alarmes (***trap***s) envoyées par l'agent au manager pour informer qu'il y a un souci...
La figure suivante illustre ce principe.



Il est possible d'utiliser d'autres ports tels :
— **161/tcp** pour SNMP classique
— **162/tcp** pour SNMP classique
— **199/tcp** pour SNMP Unix Multiplexer : SMUX
— **199/udp** pour SNMP Unix Multiplexer : SMUX
— **391/tcp** synoptics-relay pour SynOptics SNMP Relay Port

— **391/udp** synoptics-relay pour SynOptics SNMP Relay Port
— **705/tcp** agentx pour AgentX
— **1993/tcp** snmp-tcp-port pour cisco SNMP TCP port
— **1993/udp** snmp-udp-port pour cisco SNMP TCP port

5.5.3 Format de la trame SNMP



— **Version** : numéro de version SNMP. Le manager et l'agent doivent utiliser le même !
— **Communauté** : ce champ sert à identifier auprès du manager l'agent avant de lui accorder un accès.
— **PDU** : il y a 5 types de PDU,

1. *GetRequest*,
2. *GetNextRequest*,
3. *GetResponse*,
4. *SetRequest*,
5. TRAP

et 3 formats de PDU

1. Un format pour *GetRequest*, *GetNextRequest* et *SetRequest*,
2. Un format pour *GetResponse*,
3. Un format pour TRAP.

— Format utilisé pour les PDU du genre GET, ou SET :

request-id : Utilisé pour différencier les messages.

error-status : Utilisé pour signaler une erreur (0 si pas d'erreur).

error-index : Indique la sous-catégorie d'erreur.

variablebindings : Nom des variables avec leurs valeurs, NULL lors d'une opération Get

enterprise : Type de l'objet générant l'alarme.

agent-addr : Adresse de l'émetteur de l'alarme.

generic-trap : Identificateur de l'alarme.

specific-trap : Identificateur d'alarme spécifique.

time-stamp : Temps écoulé depuis la dernière réinitialisation de l'entité.

— **error-status** et **error-index** : renvoie les éventuelles erreurs

AuthorisationErreur : erreur d'autorisation de lecture de la MIB

NoAccess : Accès à la MIB interdit

NoCreation : Objet non créé

NoWritable : Pas de permission d'écrire

ReadOnly : Pas de permission de lire

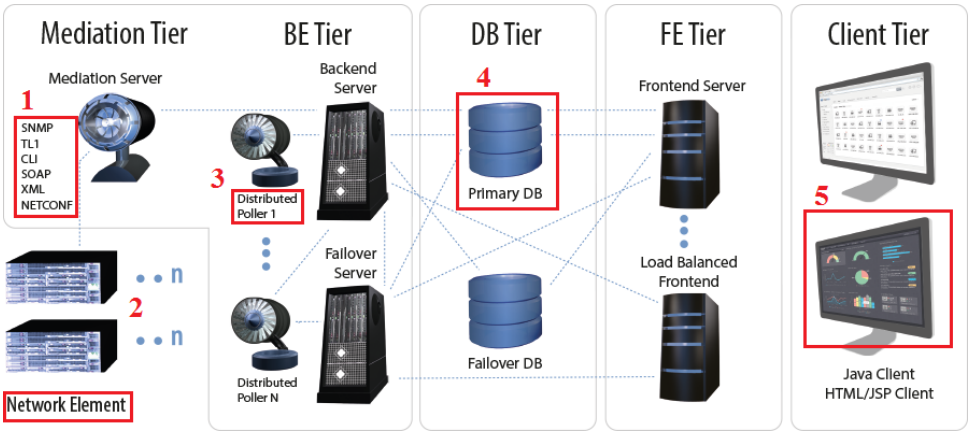
WrongEncoding : Erreur d'encodage

WrongLength : erreur de longueur de la requête

WrongType : Type de donnée erronée
WrongValue : Valeur de donnée erronée

Voilà ce que toutes ces entités peuvent donner

1. Les **protocoles**
2. Les **Agents**
3. Les **sondes**
4. La **BDD**
5. **L'interface**
   (a) **Graphique**
   ou
   (a) **Web**



Source : **http://www.webnms.com/webnms/index.html**

5.6 Les communautés

La communauté permet de créer **des domaines d'administration**, elle est décrite par une chaine de caractères.

Il y a 2 communautés :

1. **RO** : pour Read Only, on ne peut que lire les valeurs des OID
2. **RW** : pour Read Write, on peut lire et écrire, dans le sens modifier, les valeurs des OID

Par défaut, la communauté est PUBLIC.

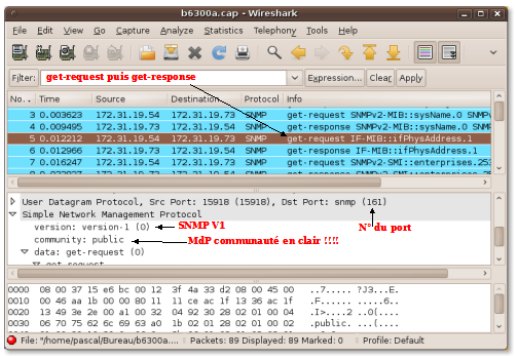
On peut paramétrer un agent SNMP afin de créer des groupes de sécurité qui auront accès pour certains en lecture seule, d'autres en lecture/écriture, d'autres encore en lecture seule, mais sur certaines branches de la MIB.

Chaque groupe devra disposer d'un mot de passe, appelé *community*.

Exemple :

snmpget -v 1 ***-c toutlemonde*** *192.168.1.10 .iso.org.dod.internet.mgmt.mib-2.system.sysContact.0*

L'inconvénient est qu'avec SNMP v1, version vraiment stabilisée et reconnue par tous, ce mot de passe circule en clair sur le réseau, ce qui rend SNMP dangereux...



On verra tout cela plus en détails en TP.

6 Le "marché" de la supervision

Nous avons vu jusqu'à présent comment superviser un réseau en utilisant des commandes. Il existe des outils beaucoup plus performants proposés par les éditeurs et par le monde libre.

Voici un site Web qui les recense : http://wwwsnmp.cs.utwente.nl/software/

6.1 Les offres des éditeurs

— **Ciscoworks** : voir l'url
http://www.cisco.com/web/FR/documents/pdfs/datasheet/ios/NETWORK_CONNECTIVITY.pdf
— **HP** : Openview (NNM, OVO, ...) : Système développé par HP permettant d'administrer un réseau décentralisé., voir l'url :
https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-10{^}{}36657_4000_100&jumpid=hpr_R1002_USEN
— **IBM** : Tivoli : voir l'url http://www-01.ibm.com/software/fr/tivoli/
— etc ...

6.2 Les offres du monde libre

plus à notre porté :)
— **cacti** : http://www.cacti.net/index.php il s'appuie sur RRDTools
  — RRDTools : http://oss.oetiker.ch/rrdtool/ base de données tournante (Round-Robin Database) dédiée à la supervision. C'est donc un outil qui permet de faire des bases de données et aussi des graphes.
— **nagios** : http://www.nagios.org Nagios™ (Netsaint) C'est un logiciel libre sous licence GPL.
C'est un programme modulaire découpé en 3 parties :

1. Le moteur de l'application qui vient ordonnancer les tâches de supervision,
2. L'interface web, qui permet d'avoir une vue d'ensemble du système d'information et des possibles anomalies,
3. Les *plugins*, plus d'une centaine (http://nagiosplugins.org/man) modifiables en fonction de ses besoins afin de superviser les services ou ressources disponibles des équipements réseaux.

— **mrtg** : (Multi Router Traffic Grapher)
Il est très facile à installer et à utiliser. Il suffit d'avoir
  — un serveur Web tel *Apache*,
  — de lancer 2 ou 3 commandes et le tour est joué :)
  Les données sont stockées dans le répertoire */var/www/mrtg*
  — On lance un navigateur et on utilise l'url http ://@IP/mrtg
  — On obtient des graphes donnant par exemple : *charge moyenne de "hostname" x 100*, *Nombre de connexion TCP simu* etc...
— **zabbix** : http://www.zabbix.com

7 La pratique

7.1 Mikrotik

Les routeurs Mikrotik comme tous les autres routeurs des autres fabricants permettent qu'on les supervise. Que cela soit en SNMP v1, V2c ou V3

Tout est indiqué ici
https://wiki.mikrotik.com/wiki/Manual:SNMP
Voici une conf de base en SNMPv3, rien de trop compliqué et nous verrons cela en TP.

```
/snmp community
add addresses=0.0.0.0/0 authentication-password=toto encryption-password=titi \
    name=v3R2-SNMP security=authorized write-access=yes
/ip address
add address=172.31.1.2/24 interface=ether1 network=172.31.1.0
/snmp
set contact=leprof@thebest.fr enabled=yes location=icietpasailleurs \
    src-address=172.31.1.2 trap-community=v3R2-SNMP trap-generators=\
    interfaces trap-interfaces=ether2,ether3 trap-target=172.31.1.254 \
    trap-version=3
/system identity
set name=R2-SNMP
```

Ici nous avons donc les résultats suivants spour un routeur

```
[admin@R2-SNMP] /snmp> print
          enabled: yes
          contact: leprof@thebest.fr
         location: icietpasailleurs
        engine-id:
      src-address: 172.31.1.2
     trap-target: 172.31.1.254
   trap-community: v3R2-SNMP
     trap-version: 3
  trap-generators: interfaces
  trap-interfaces: ether2,ether3
[admin@R2-SNMP] /snmp> community
[admin@R2-SNMP] /snmp community> print value-list
                        name: public v3R2-SNMP
                   addresses: ::/0   0.0.0.0/0
                    security: none   authorized
                 read-access: yes    yes
                write-access: no     yes
    authentication-protocol: MD5    MD5
        encryption-protocol: DES    DES
    authentication-password:        toto
        encryption-password:        titi
[admin@R2-SNMP] /snmp community> ..
[admin@R2-SNMP] /snmp> export
# may/22/2019 17:36:53 by RouterOS 6.43.8
# software id =
#
#
#
/snmp community
add addresses=0.0.0.0/0 authentication-password=toto encryption-password=titi \
    name=v3R2-SNMP security=authorized write-access=yes
/snmp
set contact=leprof@thebest.fr enabled=yes location=icietpasailleurs \
    src-address=172.31.1.2 trap-community=v3R2-SNMP trap-generators=\
    interfaces trap-interfaces=ether2,ether3 trap-target=172.31.1.254 \
    trap-version=3
[admin@R2-SNMP] /snmp>
```

7.2 Linux : Agent & Manager !

On ne fera pas en TP, c'est trop long mais pour ceux que ça interesse, pourquoi pas ☺
On peut et on doit superviser des serveurs de type Gnu/Linux !

7.2.1 L'agent

Il suffit :

1. **Installer** l'agent **snmpd** (le serveur ou ***daemon*** ! ! !) : ***apt-get install snmpd***
   Il comprend entre autres que 2 commandes dans le répertoire ***/usr/sbin*** qui sont :
   (a) ***snmpd*** : *is an SNMP **agent** which binds to a port and awaits requests from SNMP management software.*
   Upon receiving a request, it processes the request(s), collects the requested information and/or performs the requested operation(s) and returns the information to the sender.
   (b) ***snmptrapd*** : *is an SNMP application (**daemon** ! ! !) that receives and logs SNMP TRAP and INFORM messages*
2. **Configurer** en modifiant le fichier ***/etc/snmp/snmpd.conf***
   Voir documentation : http://www.net-snmp.org/docs/man/snmp.conf.html

7.2.2 Le Manager

Il faut l'installer...
— Voir avec mon collègue si vous voulez Nagios 3 ou 4, Centreon etc...
— Sinon on peut utiliser le paquet Net-SNMP : **http://www.net-snmp.org**
Il suffit :

1. **Installer** le manager **snmp** : ***apt-get install snmp***
   Il comprend entre autres de nombreuses (plus de 20) commandes (plus de 20) dans le répertoire ***/usr/bin*** dont voici la définition des principales que l'on pourra utiliser en TD/TP
   (a) ***snmpconf*** : pour créer et/ou modifier les fichiers de conf de ***snmp*** et ***snmpd***, via des menus ***cli***.
   (b) ***snmpget*** : pour obtenir une information sur un OID précis.
   (c) ***snmpgetnext*** : pour obtenir une information sur l'OID suivant sans passer quoi que ce soit en paramètre
   (d) ***snmpinform*** : lien symbolique vers ***snmptrap***

(e) ***snmpset*** : pour position une valeur sur un OID précis.

(f) ***snmpstatus, snmptable, snmptest,***

(g) ***snmptranslate*** : pour convertir un objet d'une MIB représenté sous sa forme décimale OID en sa forme symbolique et réciproquement

(h) ***snmptrap*** : pour générer un paquet Trap vers un manager, donc port 162 ! ! !

(i) ***snmpusm*** : pour modifier la table des utilisateurs SNMP v3

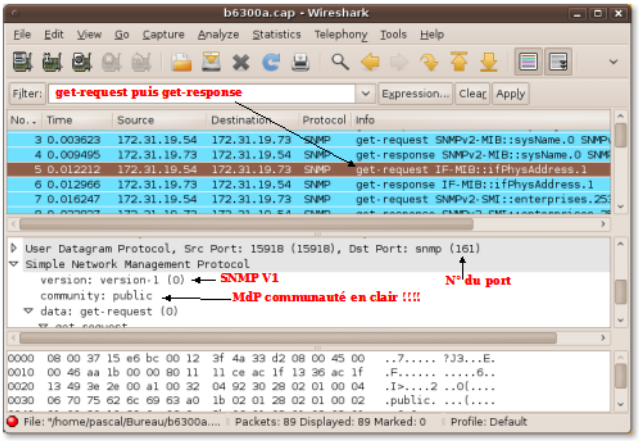
(j) ***snmpvacm*** : pour modifier la table des droits d'accès SNMP v3

(k) ***snmpwalk*** : pour obtenir des informations par lots.

2. **Configurer** en modifiant les fichiers ***/etc/snmp/snmpd.conf*** et ***/etc/snmp/snmptrapd.conf***
   Voir documentations :
   http://www.net-snmp.org/docs/man/snmpd.conf.html et **http://www.net-snmp.org/docs/man/snmptrapd.conf.html**
3. Fini

Dont toute la documentation est ici : **http ://www.net-snmp.org/docs/man/**

7.2.3 Quelques utilisations de ces commandes snmp



— **snmptranslate** : traduire un OID sous une forme vers une autre (Texte->Num ...)
  — ***snmptranslate 1.3.6.1.2.1.1.3*** renvoie : *SNMPv2-MIB : :sysUpTime*
  — ***snmptranslate 1.3.6.1.2.1*** renvoie : *SNMPv2-SMI : :mib-2*
  — ***snmptranslate -Tp -IR system***
  renvoie :

```
+--system(1)
   |
   +-- -R-- String      sysDescr(1)
   |        Textual Convention: DisplayString
   |        Size: 0..255
   +-- -R-- ObjID       sysObjectID(2)
   +-- -R-- TimeTicks   sysUpTime(3)
   |  |
   |  +--sysUpTimeInstance(0)
   |
   +-- -RW- String      sysContact(4)
   |        Textual Convention: DisplayString
   |        Size: 0..255
   +-- -RW- String      sysName(5)
   |        Textual Convention: DisplayString
   |        Size: 0..255
   +-- -RW- String      sysLocation(6)
   |        Textual Convention: DisplayString
   |        Size: 0..255
   +-- -R-- INTEGER     sysServices(7)
   |        Range: 0..127
   +-- -R-- TimeTicks   sysORLastChange(8)
   |        Textual Convention: TimeStamp
   |
   +--sysORTable(9)
      |
      +--sysOREntry(1)
         |  Index: sysORIndex
         |
         +-- ---- INTEGER     sysORIndex(1)
```

```
|          Range: 1..2147483647
+-- -R-- ObjID       sysORID(2)
+-- -R-- String      sysORDescr(3)
|          Textual Convention: DisplayString
|          Size: 0..255
+-- -R-- TimeTicks sysORUpTime(4)
           Textual Convention: TimeStamp
```

- **snmpget** : lire des informations
  - ***snmpget -v 1 -c toutlemonde 192.168.1.10 .iso.org.dod.internet.mgmt.mib-2.system.sysContact.0***
    renvoie : SNMPv2-MIB : :sysContact.0 = STRING : "c'est moi :)"
    Ce qui donne le nom de "l'administrateur" du réseau.
- **snmpset** : écriture d'informations
  - ***snmpset -v 1 -c cedurezo 192.168.1.10 .iso.org.dod.internet.mgmt.mib-2.system.sysContact.0 s plusroot***
    renvoie : SNMPv2-MIB : :sysContact.0 = STRING : plusroot
    Ce qui positionne le champ *sysContact* avec la chaine de caractères (**s** comme *string*) à *plusroot*.

Remarque 1 : comme on désire écrire, on a ***changé*** le nom de la ***communauté*** en passant de ***toutlemonde*** à ***cedurezo*** ! ! !
Remarque 2 : on peut contracter l'écriture : ***snmpset -v 1 -c cedurezo 192.168.1.10 sysContact.0 s plusroot***

- **snmpgetnext** : recevoir des informations dont on ne connait pas l'index
  - ***snmpgetnext -v 1 -c cedurezo 192.168.1.10 .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0***
    renvoie : SNMPv2-MIB : :sysContact.0 = STRING : root
    ce qui correspond au champ *sysContact* qui est le champ suivant *sysUpTime*.
- **snmpwalk** : plusieurs informations à la fois
  - ***snmpwalk -c toutlemonde -v 1 192.168.1.10 system***
    renvoie :

```
SNMPv2-MIB::sysDescr.0 = STRING: Linux er023 2.6.31-14-generic #48-Ubuntu SMP Fri Oct 16 14:04:26 UTC 2009 i686
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (2437504) 6:46:15.04
SNMPv2-MIB::sysContact.0 = STRING: plusroot
SNMPv2-MIB::sysName.0 = STRING: er023
SNMPv2-MIB::sysLocation.0 = STRING: MaSalleServeur
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORID.1 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.2 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.6 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.7 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.8 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORDescr.1 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.2 = STRING: The MIB for Message Processing and Dispatching.
SNMPv2-MIB::sysORDescr.3 = STRING: The management information definitions for the SNMP User-based Security Model.
SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for SNMPv2 entities
SNMPv2-MIB::sysORDescr.5 = STRING: The MIB module for managing TCP implementations
SNMPv2-MIB::sysORDescr.6 = STRING: The MIB module for managing IP and ICMP implementations
SNMPv2-MIB::sysORDescr.7 = STRING: The MIB module for managing UDP implementations
SNMPv2-MIB::sysORDescr.8 = STRING: View-based Access Control Model for SNMP.
SNMPv2-MIB::sysORUpTime.1 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.2 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.3 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.4 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.5 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.6 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.7 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.8 = Timeticks: (0) 0:00:00.00
```

- **snmptrap** : envoi/réception de traps (alertes)

Plus d'informations ici : http://www.systemx.fr/linux/supervision/snmpserver.html

8 Conclusion

La supervision des réseaux est un métier à part entière qui demande beaucoup de connaissances dans le domaine et de rigueur

Les outils pour la mise en place sont nombreux et l'on a l'embarras du choix. Leur mise en application peut s'avérer lourde et complexe.

Attention à ne pas utiliser une pioche pour ouvrir un pot de cornichons ☺

Des fois, un simple ***Packet Internet Network Gopher***[3] est suffisant pour savoir s'il y a "quelque chose" à l'autre bout ☺

3. ***ping*** ☺