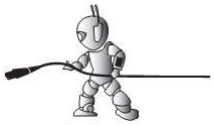
ASR Administration des Services Réseaux

Master RT 1

RT 21
Administration des Services Réseaux



Chapitre II
Le Service SNMP (Simple Network Management Protocol)

Dr. H. Zerrouki
<zerrouki.hadj@gmail.com>

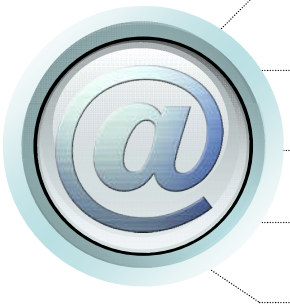
UDL-SBA, Faculté de Génie Electrique

DÉPARTEMENT
Télécommunications

ASR Administration des Services Réseaux

Master RT 2

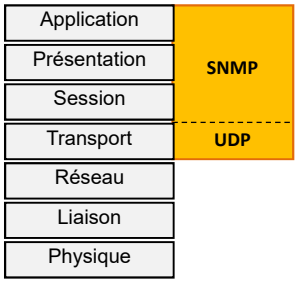
Plan de cours



- Présentation du protocole SNMP
- Les composants de base de SNMP
- La structure de données (MIB) et (SMI)
- Les opérations SNMP
- Description du protocole SNMP

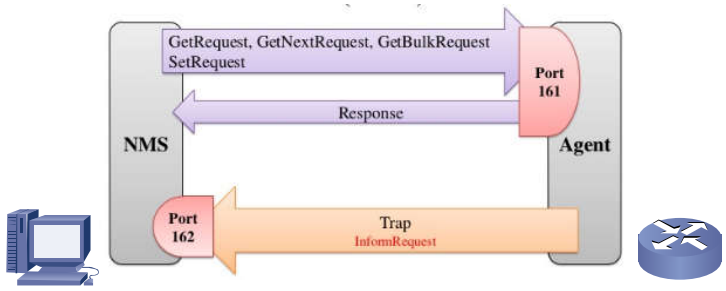
Présentation du protocole SNMP

- **SNMP** (**S**imple **N**etwork **M**anagement **P**rotocol) a été défini en **1989**. Depuis, il est devenu un standard pour la **gestion de réseaux**.
- permet de faciliter l'échange d'information d'administration entre différentes entités d'un réseau pour disposer d'une cartographie du réseau;
- gérer les performances, détecter et résoudre des problèmes.
- SNMP est un protocole de la famille **TCP/IP**, il est compatible à toutes plateformes hétérogènes et est installé sur la plupart des matériels réseaux tels que les **routeurs** et les **commutateurs**.
- Il est utilisé sur tous les réseaux de type Internet.
- Cette technologie se situe entre la couche 4 (Transport) et la couche 7 (Application).



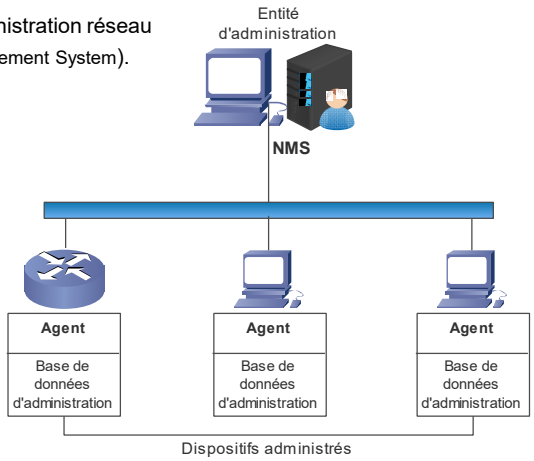
Présentation du protocole SNMP

- Le SNMP exploite les capacités du protocole **UDP**
- Le protocole UDP fonctionne en mode **non connecté**, c'est-à-dire qu'il n'existe pas de lien persistant entre la station d'administration et l'agent.
- Deux ports sont désignés pour l'utilisation de SNMP :
  - Port **161** pour les requêtes à un agent SNMP.
  - Port **162** pour l'écoute des alarmes destinées à la station d'administration.



Les composants de base de SNMP

- Un réseau administré par SNMP dispose de **trois** composants clé :
  - Les dispositifs administrés,
  - Les agents
  - Les systèmes d'administration réseau (NMS, Network Management System).



Les composants de base de SNMP

- **Un dispositif administré** :
  - Un dispositif administré est un nœud réseau qui contient un agent SNMP et qui réside sur un réseau administré.
  - Les dispositifs administrés collectent et conservent des informations d'administration, et rendent ces informations disponibles aux NMS à l'aide de SNMP.
  - Les dispositifs administrés, appelés « éléments réseau », peuvent être :
    - ✓ **des routeurs,**
    - ✓ **des serveurs d'accès,**
    - ✓ **des commutateurs,**
    - ✓ **des hôtes ordinateurs**
    - ✓ **des imprimantes.**

- **Un agent** :
  - Un agent est un module logiciel d'administration réseau qui réside sur un dispositif administré (OS).
  - Un agent possède une connaissance locale des informations d'administration et traduit celle-ci en un format compatible avec SNMP.

Les composants de base de SNMP

- **Un NMS** :
  - NMS : *(Network Management System)* ou systèmes de gestion de réseau :
  - C'est une console au travers de laquelle les administrateurs peuvent réaliser des tâches d'administration,
  - **exp.** : exécutent des applications qui surveillent et contrôlent des dispositifs administrés.
  - Un NMS fournit l'essentiel des ressources de traitement et mémoires nécessaires à l'administration réseau.
  - Il doit y avoir un ou plusieurs NMS sur un réseau administré.

- SNMP est un protocole d'administration distribuée. Un système peut opérer soit comme un NMS, soit comme un agent, ou les deux à la fois.
- Lorsqu'un système fonctionne comme NMS et agent, un autre NMS est susceptible d'exiger que le système interroge des dispositifs administrés qui fournissent un résumé des informations apprises ou rapportent les informations d'administration conservées en local.

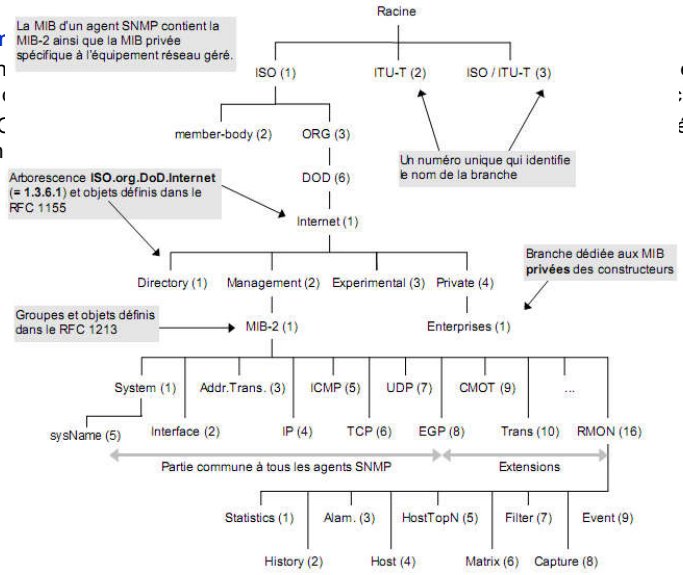
La structure de données (MIB) et (SMI)

- L'élément le plus important dans le protocole SNMP est probablement qu'il a permis de décrire un grand nombre de composants (réseaux ou autres) de façon standard.
- Cette description est faite dans la **MIB** (*Management Information Base*), qui regroupe les informations d'intérêt pour les administrateurs.
- On y retrouve toute l'expérience des spécialistes qui ont établi les modèles concernant les sujets qu'ils maîtrisent, ce qui en fait tout l'intérêt pour les administrateurs réseau.
- Le modèle n'est pas un modèle objet : les entités modélisées ne sont pas des objets au sens informatique du terme, mais plutôt un ensemble de variables typées qui peuvent être lues ou mises à jour.

La structure de données (MIB) et (SMI)

Nomm

- Ch … er) qui le … hique.
- L'O … ésente un …



La structure de données (MIB) et (SMI)

Nommage des objets

- Chaque objet possède un numéro unique qui le situe par rapport au nœud père, ainsi qu'un **nom symbolique**. Le chemin suivi pour aller de la racine à l'objet constitue l'**OID** de celui-ci.
- **Exemple :** sur la figure, l'objet décrivant le nom d'une machine s'appelle **`sysName`** et a un OID défini de la manière suivante :

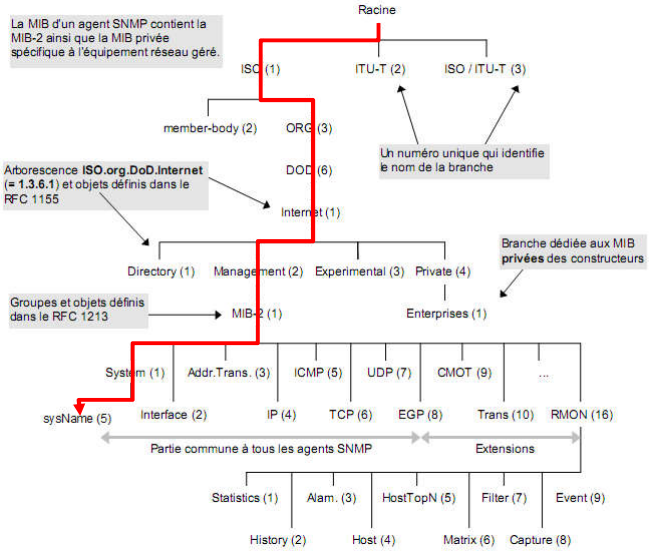
```
sysName OBJECT IDENTIFIER ::= { iso(1) org(3) dod(6)
  internet(1) mgmt(2) mib-2(1) system(1) sysName(5)}
```

ou encore, s'il est défini à partir de son père :

```
sysName OBJECT IDENTIFIER ::= { system 5 }
```

- En abrégé, il est noté **.1.3.6.1.2.1.1.5**
- De fait, l'arbre de nommage est infini. Dans l'espace de nommage, seule la partie située sous 1.3.6 (dod) est utilisée par SNMP.
- La partie supérieure est gérée par l'ISO, qui a prévu un espace de nommage pour le DoD (Département de la Défense américain), organisme à l'origine d'Internet.

La structure de données (MIB) et (SMI)



La structure de données (MIB) et (SMI)

Modules de MIB

- Les objets sont décrits par ensembles qu'on appelle « modules de MIB ». Par abus de langage, on les appelle les MIB.
- Ils sont classés dans l'espace de nommage sous la branche « **`internet`** » :
  - « **`mgmt(2)`** » contient tous les modules de MIB standard établis par l'IETF (Internet Engineering Task Force) Groupe de travail sur l'ingénierie Internet;
  - « **`expérimental(3)`** » contient les modules de MIB établis de manière expérimentale par l'IETF (sachant qu'on les retrouvera sous leur forme définitive dans des sous-arborescences de «**`mgmt`**», plus ou moins modifiés, après aboutissement du standard) ;
  - « **`private(4)`** » contient les modules de MIB développés en dehors des standards IETF, par exemple par des entreprises ou des centres de recherche. Les modules de MIB développés sous cette arborescence sont communément appelés «MIB privées ».

La structure de données (MIB) et (SMI)

❑ **Extension de la MIB**

Au bout d'un moment, les variables choisies pour la MIB (puis la MIB-2) se sont avérées insuffisantes pour plusieurs applications. On va donc trouver deux autres types de MIB que sont les **private MIB** et les **MIB R-MON** (Remote network Monitoring).

- ***Les privates MIB*** : représentées en .1.3.6.1.4 dans la structure SMI, permettent aux entreprises de rajouter des variables pour une implémentation particulière des agents SNMP. Cela leur permet d'ajouter de nouvelles variables en fonctions des applications qu'elles veulent.

- ***Les MIB R-MON*** : permettent par exemple de placer des agents SNMP sur des supports physiques. Sur un câble, on peut connecter une sonde R-MON qui va enregistrer tout ce qui se passe et que l'administrateur pourra interroger pour avoir des informations sur les collisions, les débits à un endroit précis.

La structure de données (MIB) et (SMI)

❑ **DESCRIPTION DES OBJETS : (SMI)**

- La structure **SMI** (*Structure of Management Information*) décrit les règles de description de l'information et permet d'identifier de façon unique un objet de la MIB géré par un agent SNMP.

- SMI s'intéresse aussi à la représentation des données (et leur type) pour chaque objet de la MIB. Un objet de la MIB est déclaré et défini en langage **ASN.1** (Abstract Syntax Notation 1) : langage de représentation de donnée.

- Les objets définis avec ASN.1 peuvent être :
  - ✓ ***des types***, avec des types simples comme INTEGER ou BOOLEAN, et des types construits permettant de définir des listes (SEQUENCE) et des tableaux (SEQUENCE OF) ;
  - ✓ ***des valeurs***, c'est-à-dire des objets ayant un type précédemment défini ;
  - ✓ ***des macros***, qui permettent d'étendre les définitions et définir de nouveaux types.

La structure de données (MIB) et (SMI)

❑ DESCRIPTION DES OBJETS : (SMI)

Par convention :

- les types commencent par une majuscule,
- les valeurs par une minuscule
- les macros sont tout entières en majuscules.
- Les commentaires sont précédés de deux tirets.

SNMP n'utilise qu'une petite partie du langage ASN.1. Au niveau des types, seuls quelques uns sont utilisés comme :

- **Integer** : valeur entière sur **32 bits** en complément à 2.
- **Octet String** : chaîne de caractères.
- **IpAddress** : adresse **IP**.
- **PhysAddress** : adresse MAC (**6 octets** pour un réseau de type Ethernet).
- **Counter** : entier de 32 bits non signé qui s'accroît de 0 à (2^{32} **-1**) puis revient à 0.
- **TimeTicks** : compteur de temps sur 32 bits non signé en **1/100** de s.

La structure de données (MIB) et (SMI)

❑ DESCRIPTION DES OBJETS : (SMI)

❑ Syntaxe des objets

La MIB SNMP est composée de différents objets :

- ***objets partiels***, qui servent à construire l'arborescence de la MIB. Ils n'ont pas de type, mais un OID.
  Par exemple, l'objet `System OBJECT IDENTIFIER ::= { mib-2 1 }` groupe les objets de ma mib-2 qui permettent d'identifier un agent SNMP ;
- ***objets scalaires***, c'est-à-dire qu'ils ont une instance unique. Ils auront un type simple (faisant partie de la syntaxe de base ASN.1), ou un type défini dans SMIv1 ou SMIv2 ;
- ***objets tabulaires*** : une table est décrite comme une séquence de lignes qui sont elles-mêmes une séquence d'objets.

La structure de données (MIB) et (SMI)

❑ **DESCRIPTION DES OBJETS : (SMI)**

Exp :

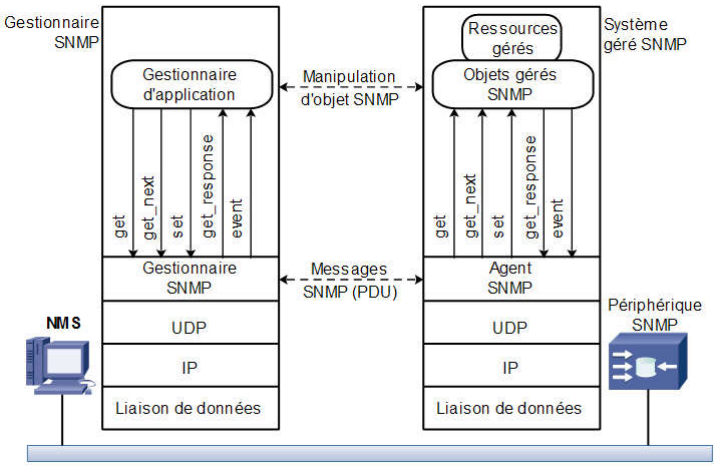
sysDescr OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
ACCESS read-only
STATUS mandatory
DESCRIPTION
"A textual description of the entity. This value should include …."
::= { **system 1** }

---

sysUpTime OBJECT-TYPE
SYNTAX TimeTicks
ACCESS read-only
STATUS mandatory
DESCRIPTION
"The time (in hundredths of a second) since the network management portion of the system was last re-initialized."
::= { **system 3** }

Les opérations SNMP

❑ Le protocole SNMP supporte trois types de requêtes : ***GET***, ***SET*** et ***TRAP***. Il utilise alors les opérations suivantes pour la gestion du réseau :

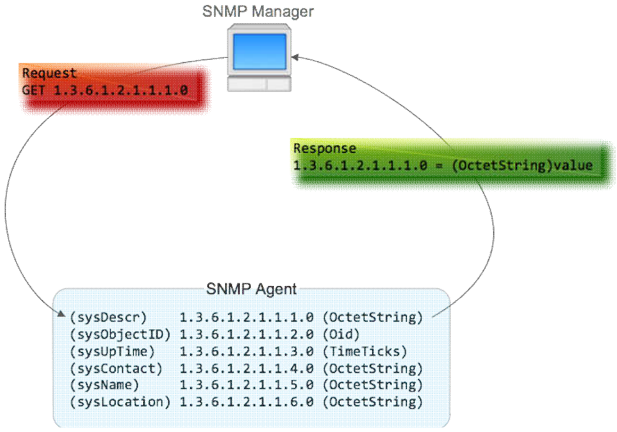


Les opérations SNMP

❑ Lire les informations (GET)

- ***Get Request :*** Cette requête permet aux stations de gestion (manager) d'interroger les objets gérés et les variables de la MIB des agents. La valeur de l'entrée de la MIB (nom) est passée en paramètre. Elle permet d'accéder à une variable précise.

- **Exp.**



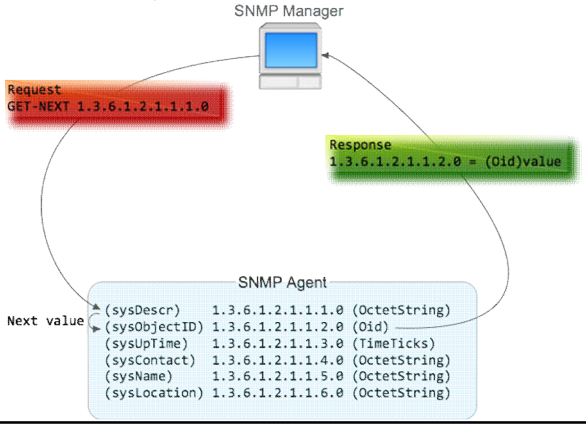
Les opérations SNMP

❑ Lire les informations (GET)

- ***Get-Next Request :*** Cette requête permet aux stations de gestion de recevoir le contenu de l'instance qui suit l'objet nommé (passé en paramètre) dans la MIB.

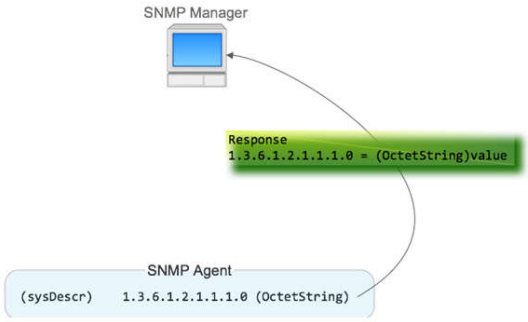
  Cette commande permet en particulier aux stations de gestion de balayer les tables des MIB. Elle permet d'accéder à plusieurs variables simultanément.

- **Exp.**



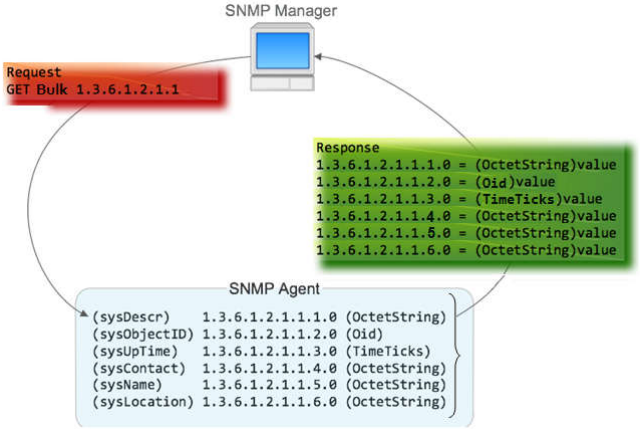
Les opérations SNMP

- **Lire les informations (GET)**
  - ***Get Response :*** A chaque envoie d'un message à l'exception de TRAP, un message de réponse est retourné. L'agent répond toujours par *GetResponse*. Toutefois si la variable demandée n'est pas disponible, le *GetResponse* sera accompagné d'une erreur *noSuchObject*. Ils ont chacun une signification bien distincte :
    - ***GetResponse :*** tout s'est bien passé, l'information est transmise.
    - ***NoSuchObject :*** aucune variable n'a été trouvée.
    - ***NoAccess :*** vous ne disposez pas des bons droits d'accès.
  - **Exp.**



Les opérations SNMP

- **Lire les informations (GET)**
  - ***Get Bulk Request :*** (SNMP v2 et v3) Cette requête est une amélioration du SNMP, elle permet aux managers d'interroger les objets gérés et les variables de la MIB des agents. Il permet à la station de gestion de récupérer efficacement des grandes données.
  - **Exp.**

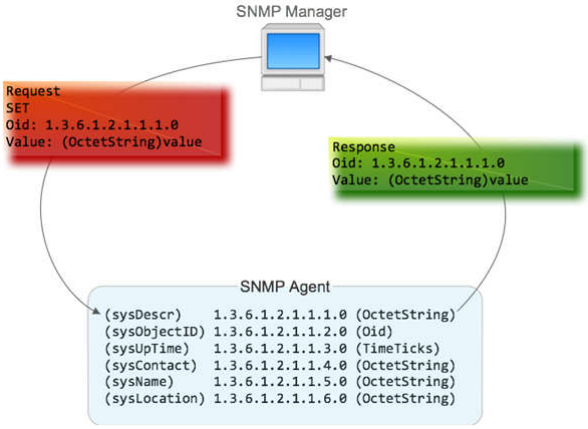


Les opérations SNMP

❑ **Modifier les informations (SET)**

- ***SetRequest :*** Cette requête permet aux stations de gestion de modifier une valeur de la MIB et de lancer des périphériques. Elle permet par exemple à un manager de mettre à jour une table de routage. *SetRequest* provoque aussi le retour de *GetResponse.*

- **Exp.**



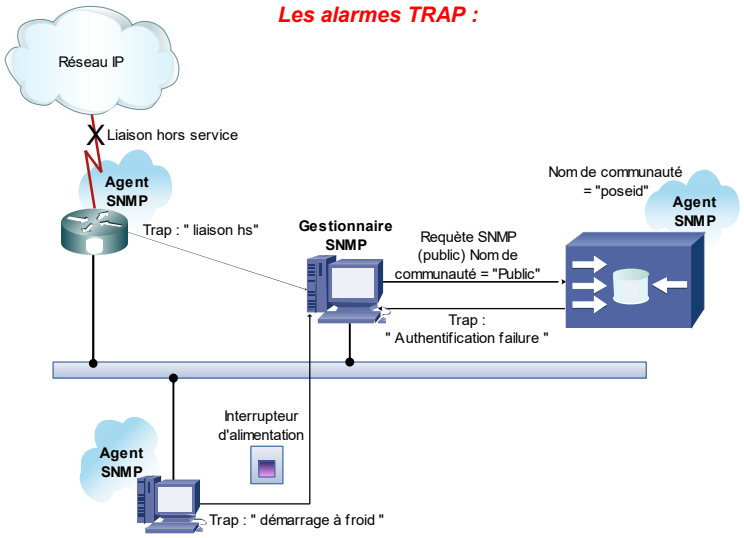
Les opérations SNMP

❑ **Type de non sollicités**

- ***Les alarmes TRAP :*** Lorsqu'un périphérique entre dans un état anormal, l'agent SNMP prévient le gestionnaire SNMP par le biais d'un Trap SNMP. Les Trap peuvent être :
  - ***Link Up* ou *Link Down*** (lorsque l'interface devient active ou au contraire passive),
  - ***Cold start*** (démarrage à froid),
  - ***Warm start*** (démarrage à chaud), réinitialisation de l'agent SNMP,
  - ***Authentication failure*** (échec d'authentification, lorsqu'un nom de communauté incorrect est spécifié dans une requête),
  - ***Loss of EGP Neighbor*** (perte de voisin EGP).

- ***InformRequest :*** (SNMP v2 et v3) Le but de l'I*nformRequest*-PDU est réellement de faciliter la communication d'information entre les stations de gestion de réseau. L'agent SNMP sur un NMS peut choisir d'informer des autres d'une certaine information en envoyant une *InformRequest*-PDU à cet autre l'agent de SNMP.

Les opérations SNMP

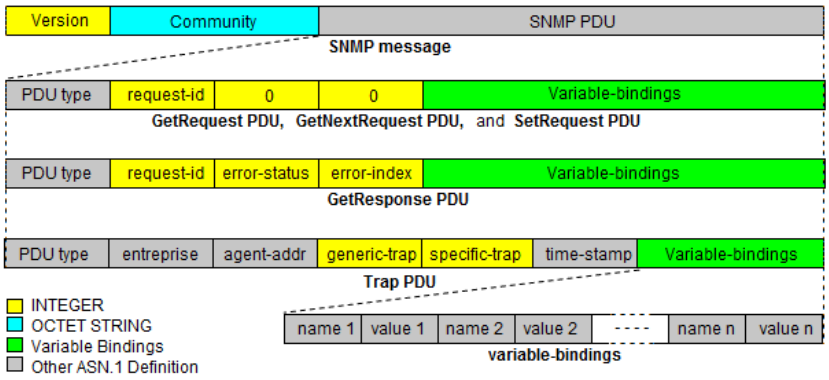


Dr. H. Zerrouki

Description du protocole SNMP

Format des PDUs (messages) SNMP

Une requête SNMP est construite de la façon suivante :



Dr. H. Zerrouki

Description du protocole SNMP

Format des PDUs (messages) SNMP

- **Version :** Version de SNMP.
  - **0** → SNMPv1
  - **1** → SNMPv2
  - **2** → SNMPv3

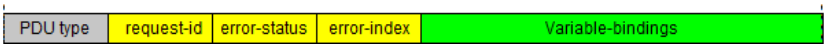
- **Community :** Nom de la communauté (agit comme un mot de passe).

- **PDU type :** Type de PDU (Protocol Data Units)
  - **0** → GetRequest
  - **1** → GetNextRequest
  - **2** → SetRequest
  - **3** → GetResponse
  - **4** → Trap
  - **…**

- **Request-id :** Utilisé pour différencier les messages.
  Le champ *identificateur de la requête* est défini par le manager lors de l'envoi d'une requête et utilisé par l'agent dans sa réponse. cela permet d'associer la réponse à la requête vu que le protocole transport utilisé est UDP.

Description du protocole SNMP

Format des PDUs (messages) SNMP



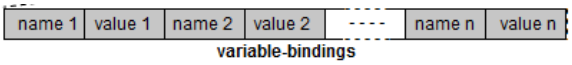
- **Error-status :** Utilisé pour signaler une erreur (0 si pas d'erreur).
  Le *statut d'erreur* est positionné par l'agent. Il est toujours à zéro **0** dans une requête.
  Il prend une valeur qui indique si une réponse *GetResponse* s'est bien passée ou non

Statut d'erreur	Nom	Description
0	*noError*	Pas d'erreurs.
1	*tooBig*	Réponse de taille trop grande.
2	*noSuchName*	Variable inexistante.
3	*badValue*	Ecriture d'une valeur invalide
4	*readOnly*	Essai de modification d'une variable en lecture seule.
5	*genErr*	Autre erreur

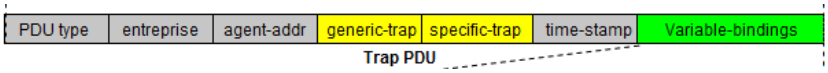
- **Error-index :** Indique la sous-catégorie d'erreur.
  L'*index d'erreur* indique la variable qui a provoqué l'erreur (uniquement dans les cas *noSuchName*, *badValue* et *readOnly*).

Description du protocole SNMP

Format des PDUs (messages) SNMP



- **Variable-bindings :** Nom des variables avec leurs valeurs.
  Il contient une liste d'objets pour lesquels le serveur souhaite obtenir une réponse. Cette liste se présente sous la forme d'une suite de couples (Identifiant :: valeur).



- **Enterprise :** contient l'identificateur de l'équipement ayant généré cette alerte (nom d'une entreprise, par exemple). Sa valeur est issue de la variable sysObjectID du groupe système.
- **Agent-addr :** Adresse de l'émetteur de l'alarme (@ IP).
- **Specific-trap :** Identificateur d'alarme spécifique.
  permet d'identifier un Trap spécifique à une entreprise.

Description du protocole SNMP

Format des PDUs (messages) SNMP

- **Generic-trap :** Identificateur de l'alarme.
  contient un entier qui traduit l'une des sept (**7**) alertes SNMP possibles.

Type de trap	Nom	Description
0	coldStart	Initialisation de l'agent
1	warmStart	Réinitialisation de l'agent
2	linkDown	Passage de l'interface à l'état bas (première variable)
3	linkUp	Passage de l'interface à l'état haut (première variable)
4	authenticationFailure	Emission par le manager d'une communauté invalide
5	egpNeighborLoss	Passage d'un homologue EGP à l'état bas (première variable indiquant l'@ IP de l'homologue)
6	enterpriseSpecific	cf. champ spécifique pour avoir de l'information

- **Time-stamp :** Temps écoulé depuis la dernière réinitialisation de l'entité.
  Ce temps est exprimé en centièmes de secondes. Sa valeur est issue de la variable *sysUptime* du groupe système.

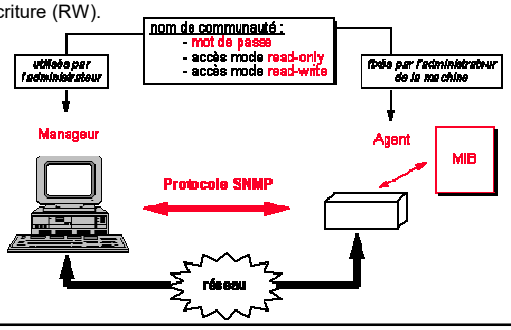
Description du protocole SNMP

Communauté

- Un agent SNMP est plus ou moins finement paramétrable, suivant le système. Il est possible, par exemple de créer des groupes de sécurité qui auront accès en lecture/écriture (**RW** : *Read/Write*), d'autres encore en lecture seule (**RO** : *Read Only*), mais sur certaines branches seulement.

- Chaque groupe devra disposer d'une sorte de mot de passe, appelé "***Community***". Donc il existe deux communautés par défaut :
  - **public :** droit de lecture des informations de la MIB (RO);
  - **private :** droit de lecture et d'écriture (RW).

En général, la communauté "public" est celle qui a le droit de lecture sur les informations non sensibles.



Description du protocole SNMP

Les différentes versions de SNMP

Plusieurs versions du protocole ont vu le jour à savoir :

❑ ***SNMPv1 :***

- Ceci est la première version du protocole, tel que définie dans le RFC 1157.
- La sécurité de cette version est triviale, car la seule vérification qui est faite est basée sur la chaîne de caractères " community ".

❑ **SNMPsec** : Cette version ajoute de la sécurité au protocole SNMPv1.

- La sécurité est basée sur des groupes. Très peu ou aucun manufacturier n'a utilisé
- Cette version est maintenant largement oubliée.

❑ ***SNMPv2p* :**

- Beaucoup de travaux on été exécutés pour faire une mise à jour de SNMPv1.
- Ces travaux ne portaient pas seulement sur la sécurité.
- Le résultat est une mise à jour des opérations du protocole, des nouvelles opérations, des nouveaux types de données.
- La sécurité est basée sur les groupes de SNMPsec.

Description du protocole SNMP

Les différentes versions de SNMP

- ***SNMPv2c*** **:**
- Cette version du protocole est appelé " ***c****ommunity stringbased* SNMPv2 ".
- Une amélioration des opérations de protocole et des types d'opérations de SNMPv2p
- Utilise la sécurité par chaîne de caractères " community " de SNMPv1.

- ***SNMPv2u*** :
- Cette version du protocole utilise les opérations, les types de données de SNMPv2c
- La sécurité basée sur les usagers.

- ***SNMPv2**** **:**
- Cette version combine les meilleures parties de SNMPv2p et SNMPv2u.
- Les documents qui décrivent cette version n'ont jamais été publiés dans les RFC.

Description du protocole SNMP

Les différentes versions de SNMP

- ***SNMPv3*** **:**
- Standard actuel.
- Cette version comprend une combinaison de la sécurité basée sur les usagers et les types et les opérations de SNMPv2p, avec en plus la capacité.
- SNMPv3 introduit des notions de sécurité comme :
  - Authentification / intégrité basé sur du DES et clef secrète
  - Confidentialité des données
  - Contrôle d'accès par la MIB

FIN