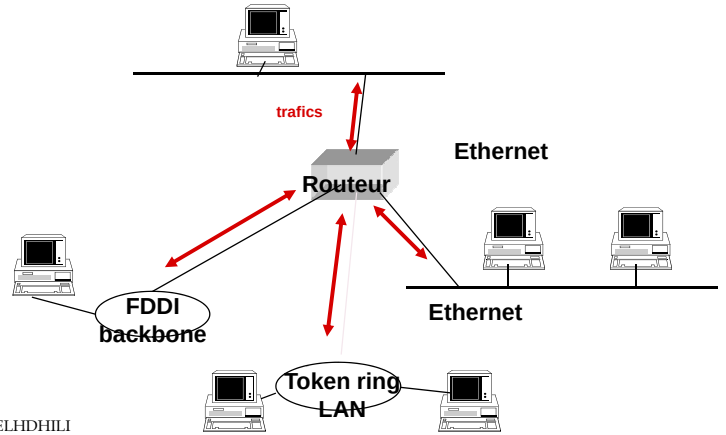
Administration et sécurité des réseaux

Chapitre 2

Le Protocole SNMP
(Simple Network Management Protocol)

SNMP : Motivation

- Nécessité d 'avoir un protocole permettant de remonter des informations sur l 'activité des différentes ressources du réseau (les serveurs, les routeurs, les hubs, etc).



Présentation de SNMP

- Protocole d'administration de machines supportant TCP/IP
  - SNMP Version 1 (SNMPv1) Défini dans la RFC 1157
    - Mécanisme de sécurité basé sur la notion de communauté (mot de passe en clair dans les requêtes et réponses)
  - SNMP Version 2 (SNMPv2) Défini dans les RFC 1905, 1906 et 1907
    - Introduit deux nouveaux types de paquets get-bulk-request et inform-request (communication entre plate-formes)
  - SNMP Version 3 (SNMPv3) Défini dans les RFC 2570, 2571, 2572, 2573, 2574 et 2575
    - Introduit de nouveaux mécanismes de sécurité (authentification forte et confidentialité)

Présentation de SNMP

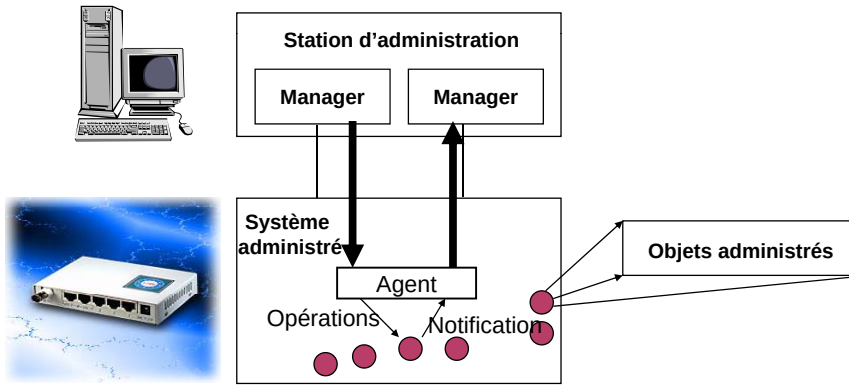
- Répond à un grand nombre de besoins :
  - Administrer à distance des machines indépendamment de leur architecture
  - Disposer d'une cartographie du réseau
  - Fournir un inventaire précis de chaque machine
  - Mesurer la consommation d'une application
  - Signaler les disfonctionnements

Modèle d 'administration SNMP

- Une administration SNMP est composée de trois types d'éléments :
  - des **agents** chargés de superviser un équipement. On parle d'agent SNMP installé sur tout type d'équipement.
  - une ou plusieurs **stations de gestion** capables d'interpréter les données
  - une **MIB** (Management Information Base) décrivant les informations gérées (objets administrés).
- SNMP permet **la supervision, le contrôle et la modification** des paramètres des éléments du réseau.

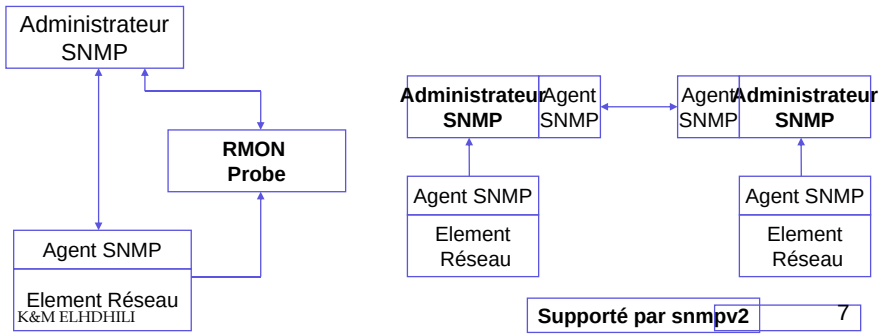
Modèle d 'administration des réseaux

- Le modèle « Manager-Agent » ou modèle deux-tiers.



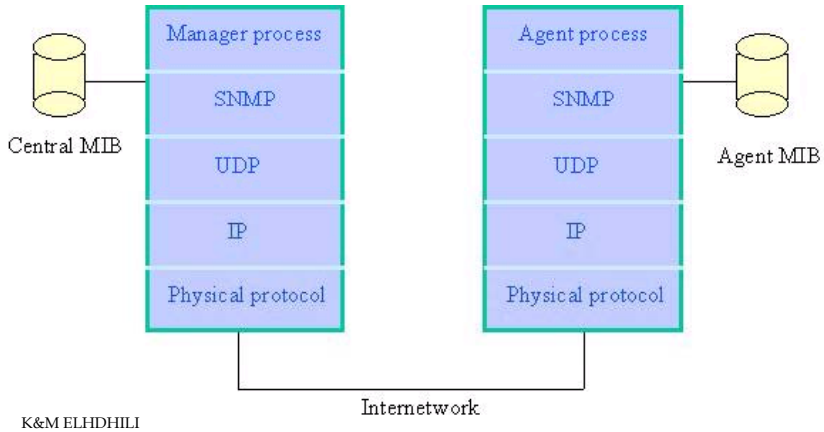
Modèle d 'administration SNMP

- L 'architecture **trois-tiers** insère entre le Manager et l 'agent une sonde RMON ou une autre station d 'administration (modèle SNMPv2).
  - La sonde RMON permet de faire la collecte d 'informations d 'administration et quelques traitements sur le trafic.



L 'architecture de SNMP

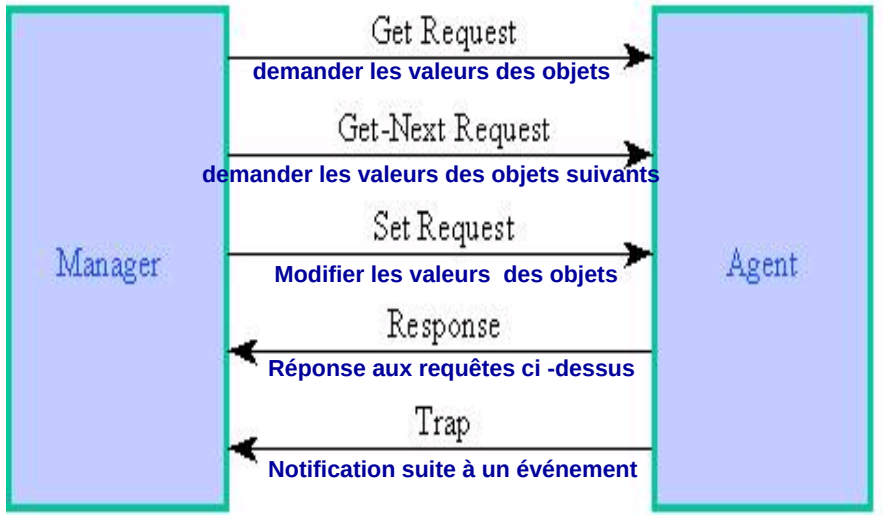
- SNMP fonctionne au dessus de UDP



Les opérations SNMP

- SNMP offre 3 opérations simples :
  - **GET :**
    - ➔ Permet à la station d'administration de retirer les valeurs d'un objet de la station administrée.
  - **SET:**
    - ➔ Permet à la station d'administration d'affecter des valeurs à un objet dans la station administrée.
  - **TRAP:**
    - ➔ Permet à une station administrée d'envoyer des notifications à la station d'administration pour les événements significatifs.

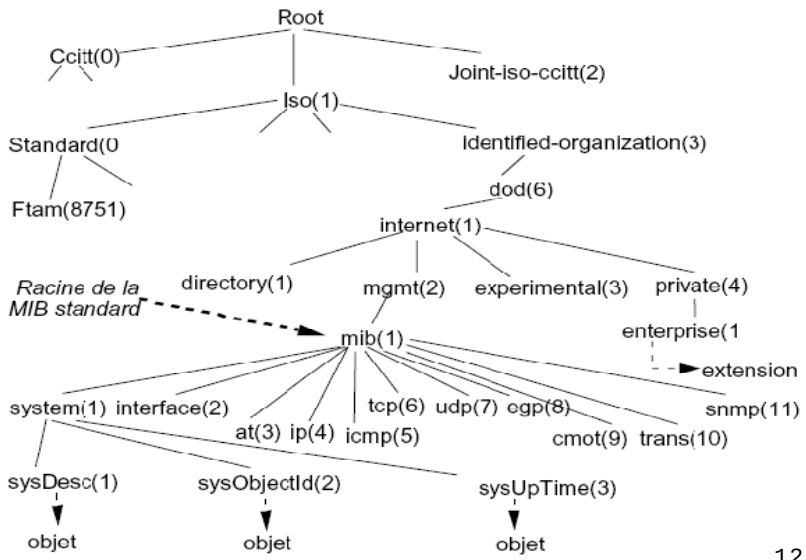
Les PDUs SNMP



La MIB (Management Information Base)

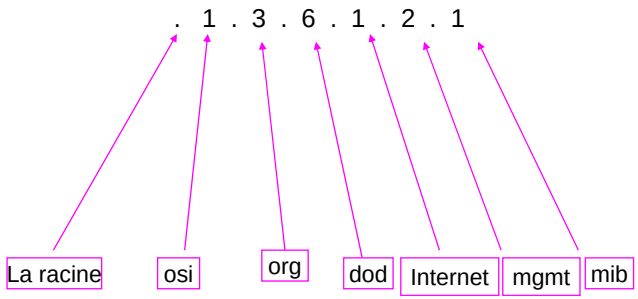
- 1 ressource à gérer = 1 objet
- Les objets administrables sont une abstraction des ressources physiques (interfaces, équipements,etc.) et logiques (connexion TCP, paquets IP, etc.)
- **MIB** : collection structurée d'objets reconnus par les agents
- Chaque nœud dans le système doit maintenir une MIB qui reflète l'état des ressources gérées
  - Une entité d'administration peut accéder aux ressources du nœud en lisant les valeurs de l'objet ou en les modifiant
- **MIB: 2 objectifs**
  - Un schéma commun : SMI (Structure of Management Information)
  - Une définition commune des objets et de leur structure

Arbre des MIB accessibles

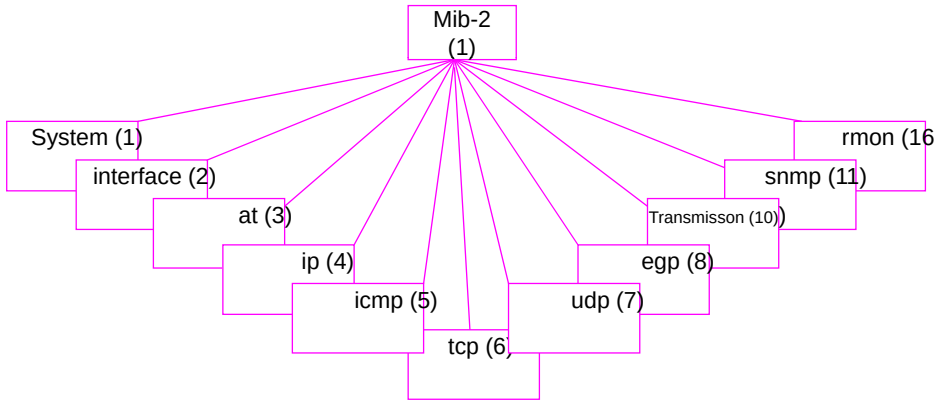


Identificateur d 'un objet de la MIB

- Identificateur d 'un objet:
  - ➔ Identificateur unique = séquence d 'entiers dont chacun représente la position de ces successeurs dans l 'arbre.
  - Exemple**: identificateur de l 'objet MIB** :



Le groupe MIB-2



Le groupe MIB-2

MIB-2

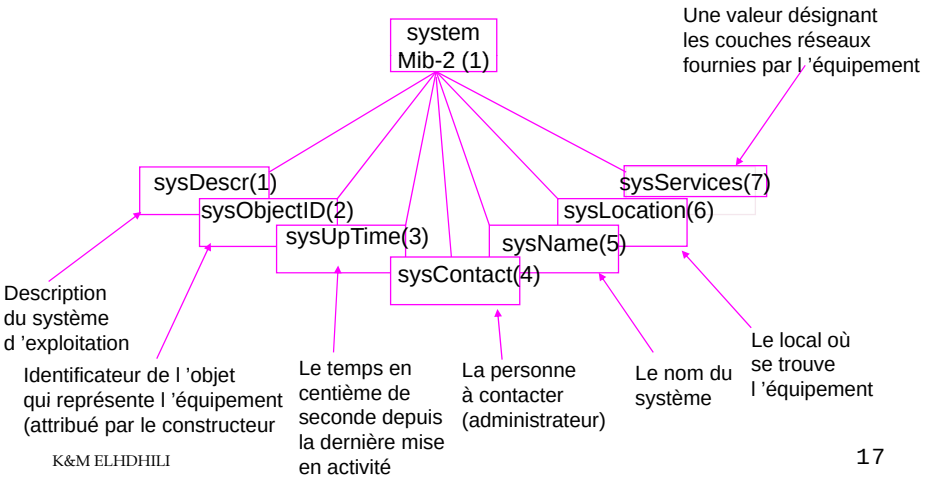
groupe	nbre éléments	commentaire
system	7	nœud dans le réseau
interfaces	25	interfaces réseau
at	5	IP address translation
ip	65	Internet Protocol
icmp	26	Internet Control Message Protocol
tcp	21	Transmission Control Protocol
udp	8	User Datagram Protocol
egp	22	Exterior Gateway Protocol
transmission	114	informations sur la transmission
snmp	28	SNMP
rmon	218	Remote network monitoring

La structure numérique de la MIB-2

system	1.3.6.1.2.1.1
interfaces	1.3.6.1.2.1.2
at	1.3.6.1.2.1.3
ip	1.3.6.1.2.1.4
icmp	1.3.6.1.2.1.5
tcp	1.3.6.1.2.1.6
udp	1.3.6.1.2.1.7
egp	1.3.6.1.2.1.8
rmon	1.3.6.1.2.1.9
transmission	1.3.6.1.2.1.10
snmp	1.3.6.1.2.1.11

Le groupe « System »

- **System** : correspond au nom de l'agent, n° de version, type de la machine, nom du système d'exploitation, etc.



Le groupe « Interface »

ifNumber : le nombre d 'interfaces

ifIndex : Index de l 'interface (son numéro)

ifDescre : Description de l 'interface

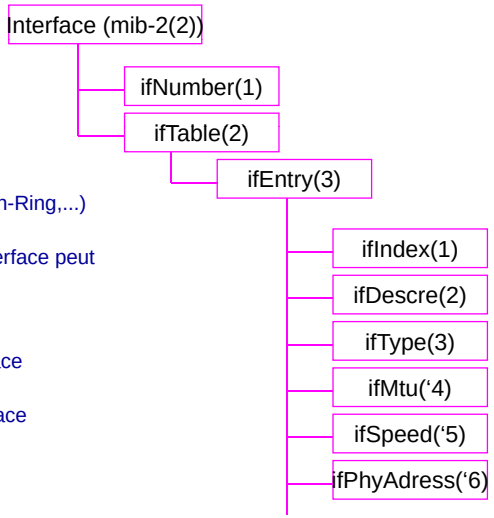
ifType : le type de l 'interface (Ethernet, Token-Ring,...)

ifMtu : le nombre maximum d 'octet que l 'interface peut envoyer ou recevoir

ifSpped : Une estimation du débit de l 'interface

ifPhyAdress : l 'adresse physique de l 'interface

....



Le groupe « IP »

ipForwarding : Agit comme passerelle, ou non

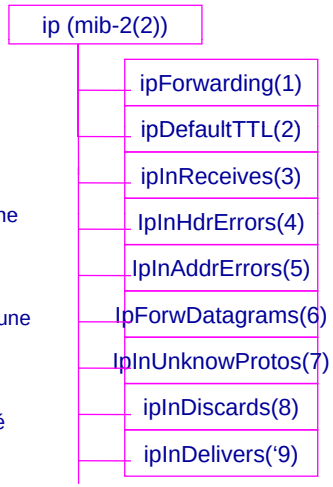
ipDefault TTL : la valeur par défaut du TTL ajouté dans un paquet IP

ipInReceives : Le nombre total de paquets IP reçus

IpInHdrErrors : Le nombre total de paquets écartés dus à une erreur sur l 'en-tête

IpInAddrErrors : Le nombre total de paquets écartés dus à une erreur sur l 'adresse de destination

IpForwDatagrams : Le nombre total de paquets dont l 'entité réceptrice ne représente pas la destination finale.



Les autres groupes

icmp : 26 compteurs

- pour chaque message icmp, 2 compteurs pour compter les messages reçus et émis
- 4 compteurs pour compter le nombre total de messages icmp reçus, reçus par erreur ou non envoyés,

tcp : rend compte des connexions TCP en cours et leurs paramètres

de type nombre max de connexions simultanées permises, nombre d'ouvertures actives, l'état de chaque connexion (écoute, time-wait,...).

udp : - 4 compteurs renseignent sur le nombre de datagramme

UDP envoyés, reçus, en erreur, ...

egp : gère le protocole egp (External gateway protocol)(routage

des paquets entre routeurs). On a le nbre de paquets entrants, sortants, en erreur, la table des routeurs adjacents, des infos sur les routeurs...

snmp : requis pour chaque entité mettant en oeuvre le protocole

SNMP. Contient le nombre de messages SNMP entrants et sortants, le nombre de mauvaises versions reçues ou de nom de communauté invalide, la répartition du type de requêtes reçues et envoyées (get, get_next, set et trap)

Mécanismes de sécurité de SNMP

- SNMP implémente 3 mécanismes de sécurité:
  - L 'authentification,
  - l 'autorisation (politique d 'accès)
  - L 'identification de l 'objet
- L 'authentification se fait par le choix d 'un nom de communauté afin de restreindre l 'accès aux agents que par les administrateurs réseaux.
  - Le nom de communauté est vérifié pour chaque requête SNMP.
  - Il est relié au mode d 'accès aux objets de la MIB (lecture-écriture).
- Chaque communauté définie un mode d 'accès qui peut être soit Read-only, soit read-write.

Mécanismes de sécurité de SNMP

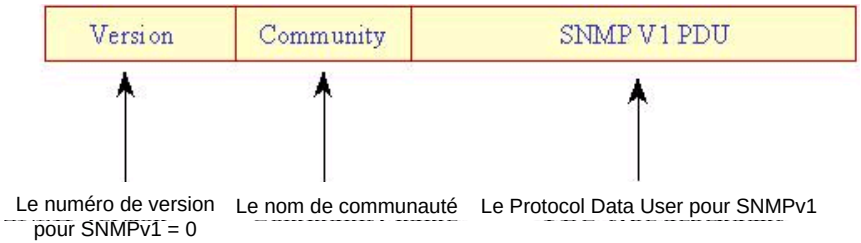
- L 'autorisation est l 'intersection entre le mode d 'accès défini par la communauté et l 'accès à l 'objet défini parmi les caractéristiques de l 'objet.

Mode d'accès	read-only	read-write	write-only	not-accessible
read-only	3	3	1	1
read-write	3	2	4	1

- où les classes sont définies par :

1 no right
2 get, get-next, set, trap
3 get, get-next, trap
4 set, trap

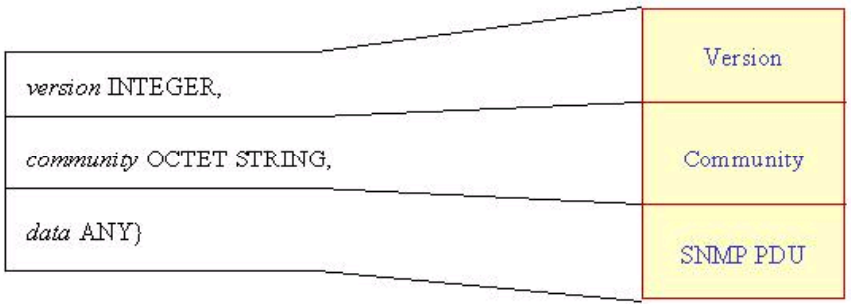
Format général du Message SNMP



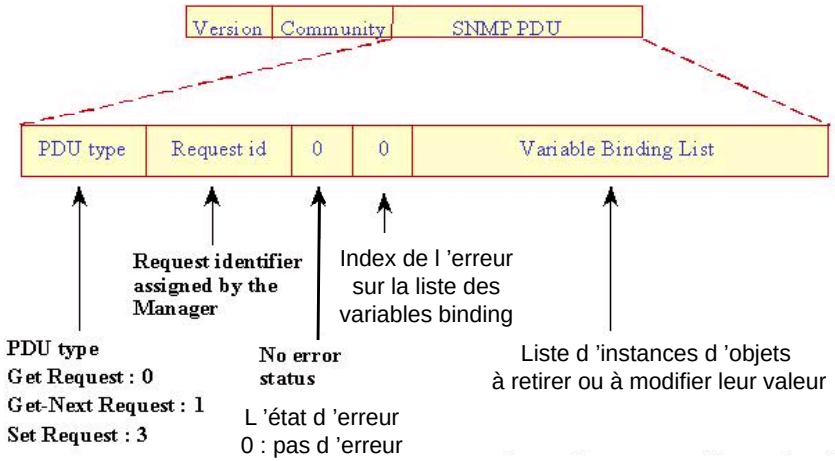
- SNMP community = Un ensemble d'administrateurs autorisés à utiliser l'agent
- Chaque communauté est définie en utilisant un nom unique
- Les administrateurs doivent préciser le nom de la communauté dans les requêtes SNMP

Définition ASN.1 du Message

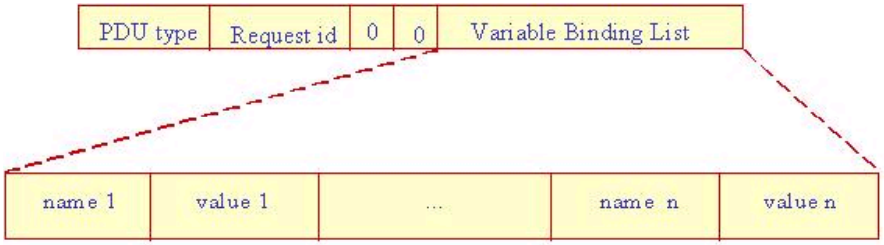
RFC1157-SNMP DEFINITIONS ::= BEGIN
IMPORTS *ObjectName*, *ObjectSyntax*, ... FROM *RFC1155-SMI*;
Message ::= SEQUENCE {



Format des Get, Get-Next et Set

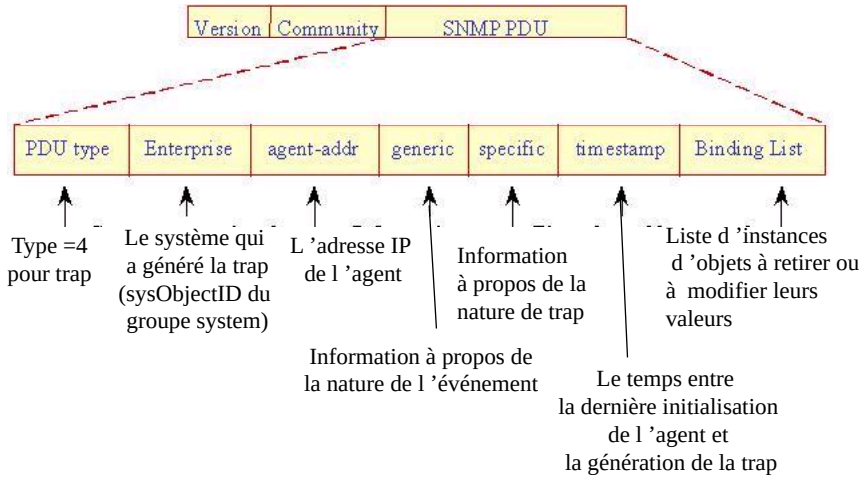


Format de Variable Binding List



VarBind ::= **SEQUENCE** {
name ObjectName,
value ObjectSyntax }
VarBindList ::= **SEQUENCE OF** *VarBind*

Format de Trap



Le champ "Generic"

- Le champ "Generic" peut prendre une des valeurs suivantes :
  - **coldStart (0) :** Une réinitialisation inatendue due à une défaillance.
  - **warmStart (1)** : Une défaillance mineur
  - **linkDown (2)** : Une défaillance survenue sur une interface physique.
  - **linkUp (3)** : Une interface devient active.
  - **authenticationFailure (4) :** L'agent a reçu un message avec une authentification impropre
  - **egpNeighborLoss (5) :** Un routeur voisin utilisant EGP (External Gateway Protocol) est déclaré comme étant non focntionnel
  - **enterpriseSpecific (6) :** L'événement relatif à "enterprise-specific" est survenu

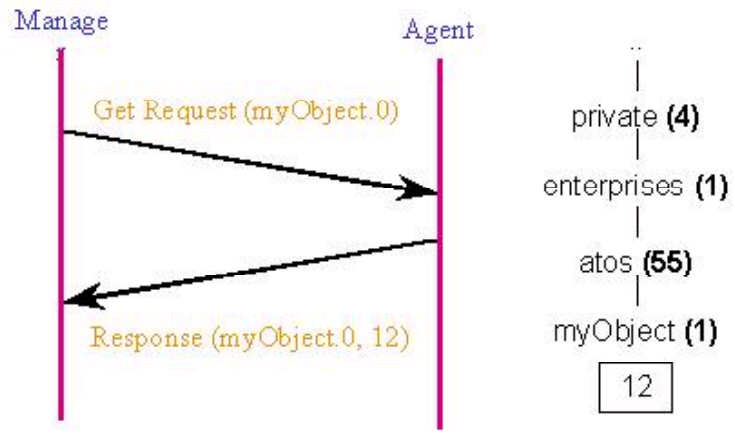
Exemple de Trap

Trap	Enterprise	agent-addr	generic	specific	timestamp
4	1.3.6.1.4.1.20.1	132.18.54.21	3	0	22759400
ipInReceives.0		956340			

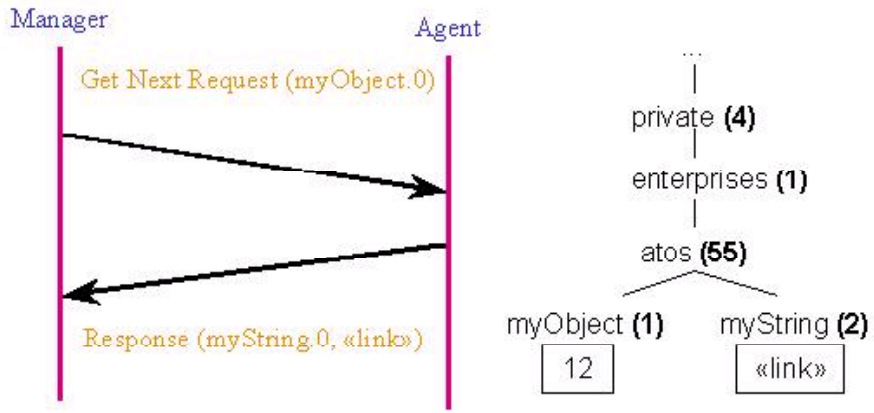
Binding List

- L 'adresse IP de agent émetteur : 132.18.54.21
- L 'objet concerné par la trap est : 1.3.6.1.4.1.20.1 (MIB privée)
- Type de trap : link up (generic=3)
- Indication : le nombre de paquets reçus est 956340
- La dernière réinitialisation de l'agent : 6 heures passées.

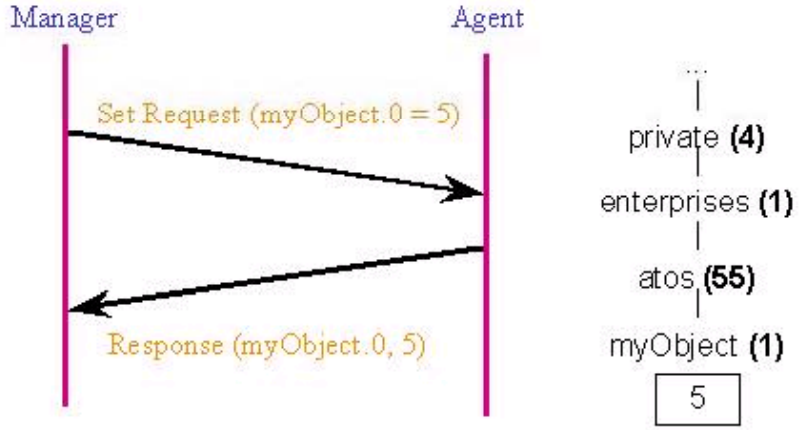
La requête GET



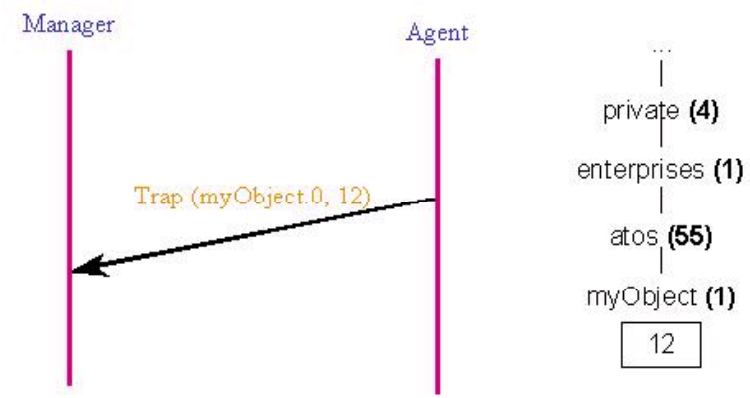
La requête GETNextRequest



La requête Set

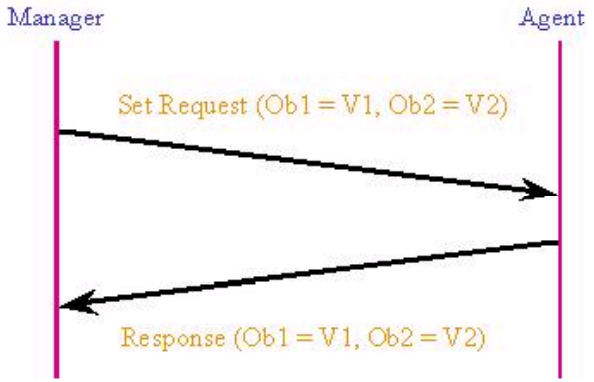


La notification TRAP

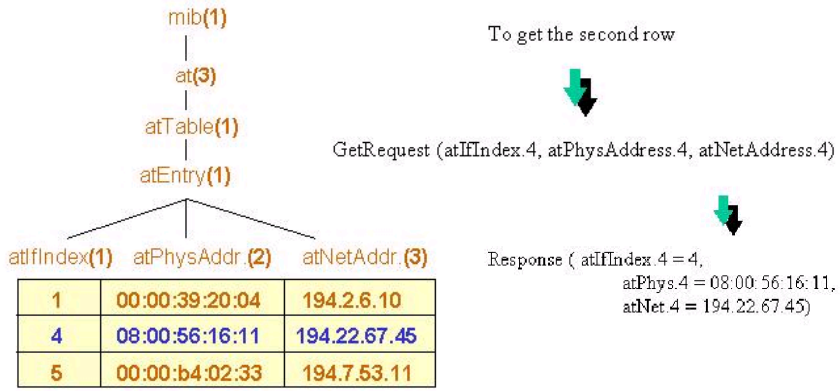


Les requêtes multiples

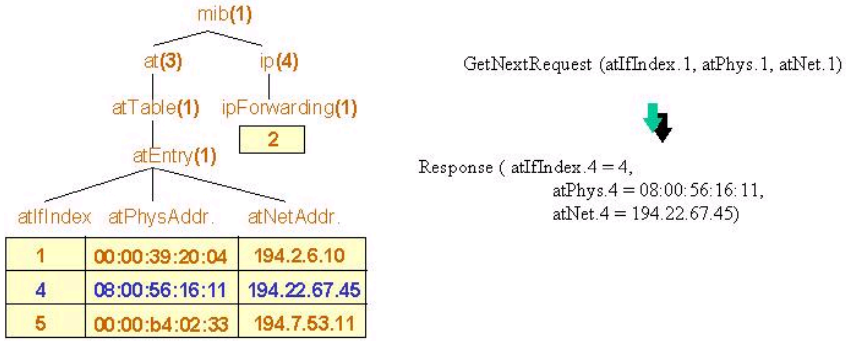
- Les requêtes Get, Get Next and Set Requests peuvent préciser plusieurs objets à lire ou à modifier leurs valeurs.



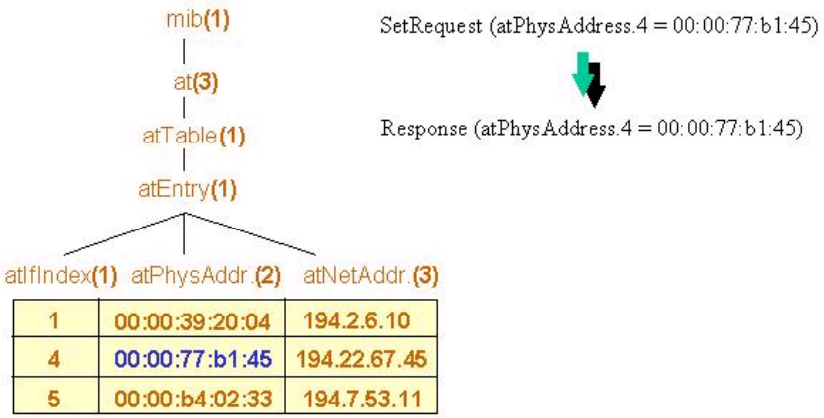
Exemple de Get Request



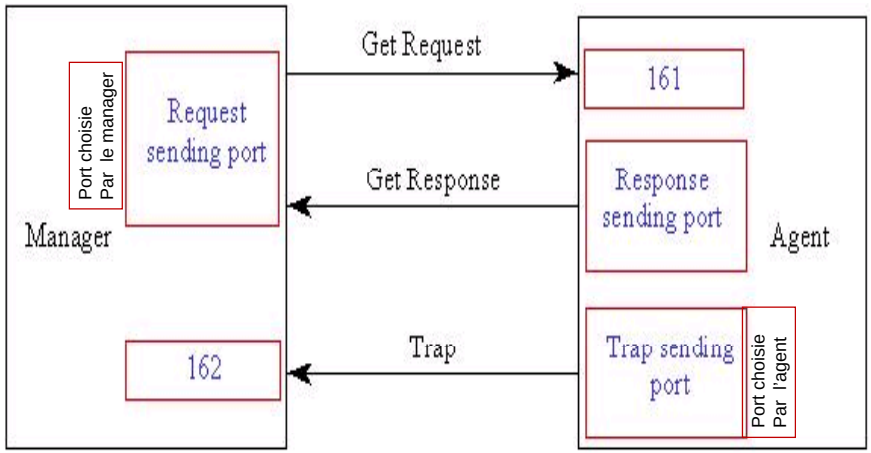
Exemple de GetNext Request



Exemple de Set Request



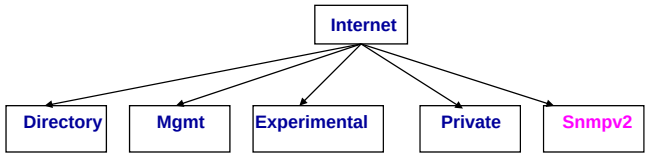
Numéros des Ports de SNMP



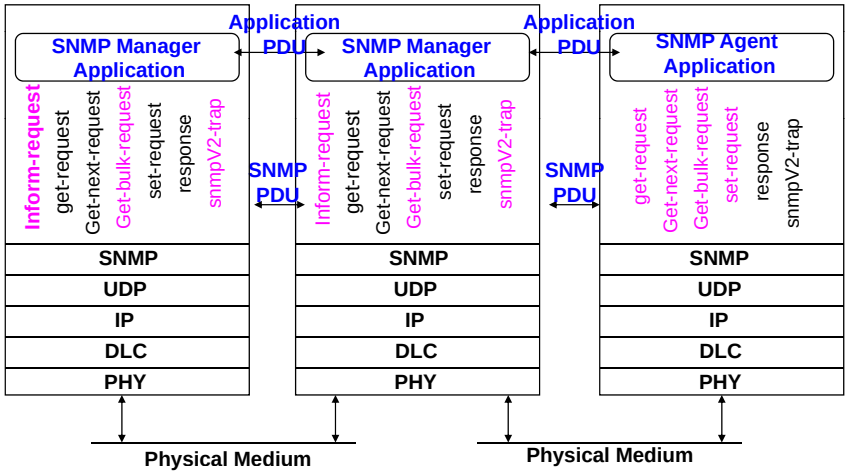
SNMPv2

Introduction

- SNMPv2: mêmes éléments de base que SNMPv1
- Différence significative:
  - ➔ un agent et un manager ont la même fonction.
  - ➔ Deux messages sont ajoutés :
    - **get-bulk**: demander et recevoir un grand volume de données
    - **Inform request**: pour la communication entre deux systèmes d 'administration



L 'architecture de SNMPv2



Les opérations de SNMPv2

- Les messages **get-request, get-next-request, et set-request** sont les mêmes que ceux de SNMPv1 et ils sont générés par l 'application d 'administration.
- Le message **response** est le même aussi que celui de SNMPv1, mais il est généré dans ce cas par l 'agent ou le manager.
- Le message **inform-request** est généré par le manager et envoyé à un autre manager.
- Le message **get-bulk-request** est généré par le manager afin de transférer une grande quantité de données de l 'agent vers le manager.
- L 'événement **SNMPv2-trap (**notification) est généré et transmis quand une situation exceptionnelle apparaît.

Les opérations de SNMPv2

- La structure de données PDU dans SNMPv2 a été uniformisée pour tous les messages (sauf pour le message get-bulk-request) afin d 'améliorer les performances d 'échange.

PDU Type	RequestID	Error Status	Error Index	VarBind 1 name	VarBind 1 value	...	VarBind n name	VarBind n value

  - avec SNMPv1 Les VarBinds ne sont pas toutes retournées dans le cas d 'une erreur (Error Status ≠ 0), avec SNMPv2 uniquement la varBind qui génère l 'erreur est ignorée et le reste sera retournée dans la réponse.
- La structure de données PDU get-bulk-request est :

PDU Type	RequestID	Non-Repeaters	Max Repetitions	VarBind 1 name	VarBind 1 value	...	VarBind n name	VarBind n value

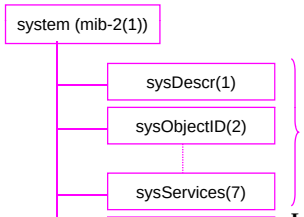
  - non-repeaters : nombre de variables non répétés à retourner (variables atomiques)
  - max-repeaters : nombre de lignes à retourner (variables composées)
- get-next-request ne peut retourner qu'une seule ligne (la ligne qui suit celle précisée par les varBinds)

La MIB de SNMPv2

- La MIB de SNMPv2 est définie dans la RFC 1907
- Trois nouveaux groupes dansSNMP V2 MIB :
  - *system* group :
    - extension du groupe original "MIB-II *system*"
    - le groupe SNMP V1 system + de nouveaux objets
  - *snmp* group :
    - rafinement du groupe original "MIB-II *snmp*"
    - le groupe SNMP V1 snmp + de nouveaux objets
  - *snmpMIBObjects* group : traite les "SNMPv2-Trap PDUs"
    - snmpTrap subgroup : Informations à propos des traps générés par les agents
    - snmpSet subgroup : Utilisé pour résoudre des problèmes qui proviennent des opérations SET.

La MIB

- Le groupe "system"



SNMPv1

La valeur de sysUpTime qui indique le temps d 'un changement majeur sur l 'état ou la valeur d 'une instance du snmpORID

Table dynamique d 'objets décrivant les ressources du système

Index de la table

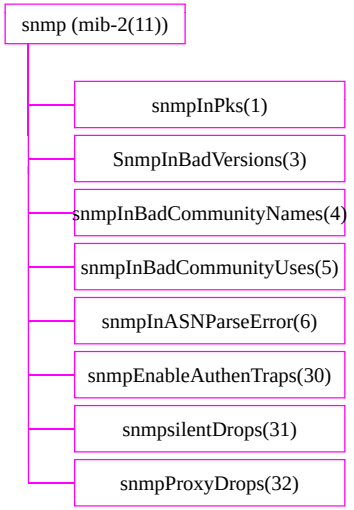
L 'identificateur de l 'OR

Description de l 'OR

La valeur de sysUpTime depuis que l 'objet a été instantié

La MIB

- Le groupe "snmp"



Le nombre total de messages délivrés du service de transport

Le nombre total de messages du service de transport dont la version est invalide

Le nombre total de messages du service de transport dont le nom de communauté est inconnu

Le nombre total de messages du service de transport dont le nom de communauté est non autorisé par l 'opération

Le nombre total d 'erreurs sur ASN.1 et BER

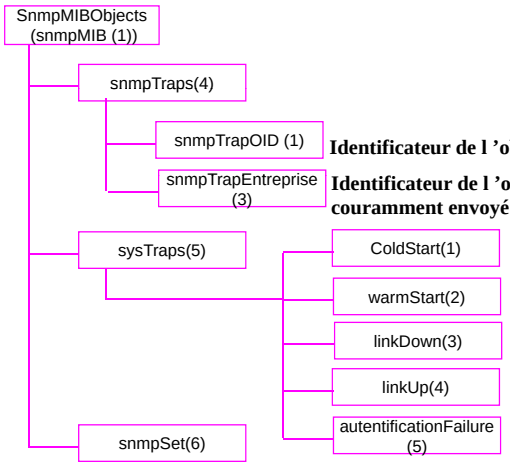
Indique si l 'entité SNMPv2 est autorisée à générer des traps pour un échec sur l ' 'authentification.

Le nombre total de requêtes échouées à cause d 'une réponse qui dépasse la taille maximale ou une exception sur varbinds

Le nombre total de requêtes échouées à cause d 'une inaccessibilité avec un proxy

La MIB

- Le groupe "snmpMIBObjetcs"



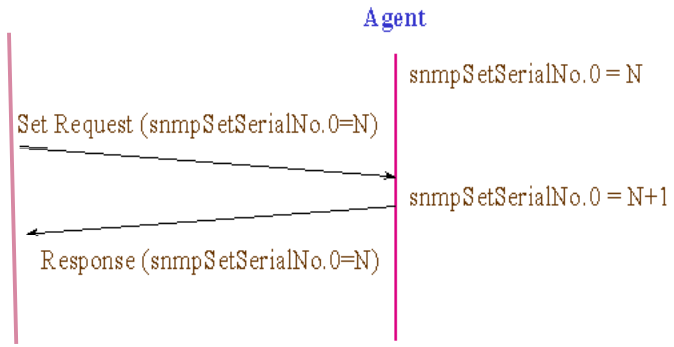
Identificateur de l 'objet du trap couramment envoyé

Identificateur de l 'objet de l 'entreprise associé au trap couramment envoyé

Verrouillage utilisé pour protéger les objets de la MIB contre des accès concurrents de plusieurs Managers avec l 'opération Set

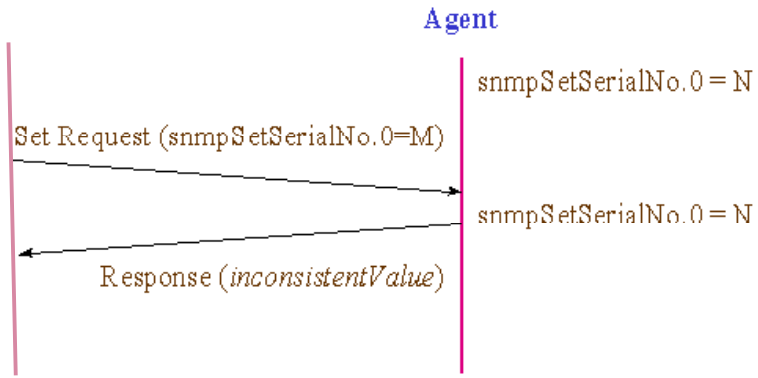
La MIB

- L'agent accepte l'opération SET sur le snmpSetSerialNo si la valeur invoquée est la même que celle de la valeur courante
- la valeur de snmpSetSerialNo est incrémentée de 1

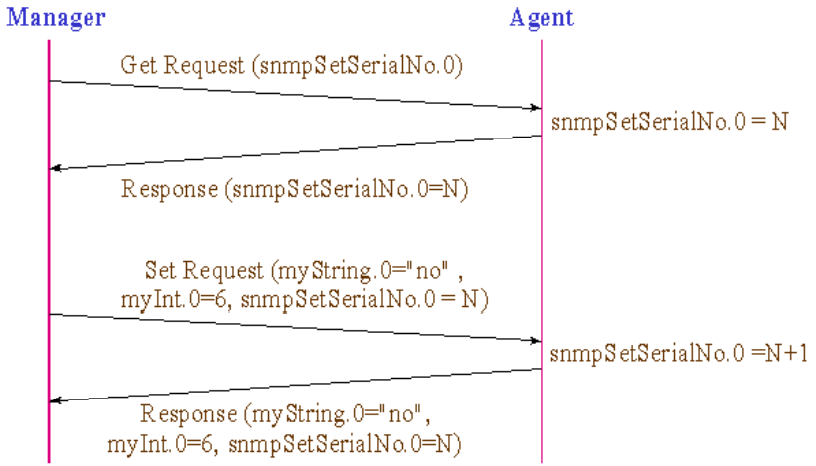


La MIB

- L'agent refuse l'opération SET sur snmpSetSerialNo si la valeur invoquée est différente de la valeur courante



La MIB



TP(SNMP)

Mise en place d'un Agent et d'un Manager SNMP Sous Linux

Mise en place d'un agent SNMP sous Linux

- Implémentation de l'agent SNMP
- **snmpd**
  - démon relatif au service SNMP de base
  - Écoute du port 161
  - Écoute des SET, GET … et génération des Response
- **snmptrapd**
  - Démon responsable de la génération des Trap
  - Gère le port 162

- Agent SNMP activé par activation de ces deux démons
- Configuration possible à travers : **/etc/snmp/snmpd.conf**
- Journalisation et historique : **/var/log/snmpd.log**

Mise en place d'un Manager

- Agent et Manager doivent être dans la même communauté.
- Ensemble d'outils permettant l'exécution de requêtes SNMP

- Exemple : les outils NET-SNMP
  - Intérrogation d'un agent :
    - **snmpget**
    - **snmpgetnext**
    - **snmpwalk**
  - Modification d'attributs de la MIB d'un agent : **snmpset**
  - Outils additionnels : **snmpstat**, **snmptranslate**, **snmpstatus** etc.

  - Manuel d'utilisation, page projet : http://www.net-snmp.org
  - Téléchargement : http://rpm.pbone.net