# Réseaux

# Simple Network Management Protocol

## Sommaire

# Genèse

- Comment connaître l'état d'un équipement réseau, d'un système ou d'une application ?

- Comment configurer à distance ?

- Comment faire de la gestion / supervision de masse ?

- Comment centraliser ces informations ?
(Security Information Management)

La gestion et la surveillance du reseau et des services sont primordiaux.

Complexité et hétérogénéite imposent des standards pour réduire les coûts

Les methodes ad-hoc ne suffisent pas à assurer le suivi:

- ping ;
- traceroute ;
- netstat ;
- telnet ;
- interface web sur les matériels ;
- whois ;
- ...

```
[root@fw ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=146 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=14.1 ms
```

```
[root@fw ~]# netstat -atnp
Connexions Internet actives (serveurs et établies)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 127.0.0.1:199               0.0.0.0:*                   LISTEN      1236/snmpd
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN      1248/sshd
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN      1353/master
tcp        0     52 192.168.100.200:22          192.168.100.1:49484         ESTABLISHED 1420/sshd
tcp        0      0 :::22                       :::*                        LISTEN      1248/sshd
tcp        0      0 ::1:25                      :::*                        LISTEN      1353/master
```

Les différents éléments à prendre en compte :

•Gestion des fautes : récupérer, isoler, réparer les fautes ;

•Gestion de l'utilisation : suivi de l'utilisation des ressources ;

•Gestion des configurations : déploiement et maintenance de la configuration des ressources ;

•Gestion de la performance : repose sur la surveillance et le contrôle des ressources ;

•Gestion de la sécurité : protection des informations et contrôle des accès

Un système d'exploitation enregistre des informations sur son fonctionnement:

- /var/log → pour les journaux
- /proc → pour des indicateurs sur le matériel
- /dev → pour des indications sur les périphériques connectés

Comment récupérer ces informations ?

Un équipement enregistre des informations sur son fonctionnement:

- nombre de connexions ;
- nombre de paquets reçus / transmis / jetés ;
- utilisation CPU / mémoire ;
- quantité de toner / papier disponible ;
- température de fonctionnement ;
- ...

Comment récupérer ces informations ?

Une application enregistre des informations sur son fonctionnement:

- bugs / erreurs ;
- logs ;
- nombre de threads / processus ;
- temps de réponse ;
- …

Comment récupérer ces informations ?

Il y a des informations qui intéressent les administrateurs système,comme par exemple:

- la température du processeur;
- la vitesse de rotation des ventilateurs;
- le fait qu'une machine ait été ouverte (interrupteur boîtier);
- …

Comment récupérer ces informations ?

# Généralités

La première version de SNMP (SNMPv1) a été conçue fin 1980.

Sa conception permettait de gérer la plupart des contraintes que nous avons définies dans la partie précédente.

Elle possède les problèmes suivants :

- manque de hiérarchie;
- peu de codes d'erreur et de notifications;
- faibles performances;
- sécurité laxiste;
- etc…

Les limitations de SNMPv1 déclenche le développement de SNMPv2:

- SNMPv2p (historique):
  améliorations sur les opérations du protocole existantes, ajout de nouvelles opérations, de nouveaux types de données.

- SNMPv2c (community):
  Appelée « community string based SNMPv2 »
  Amélioration des opérations et types de SNMPv2p
  Utilise la sécurité par chaîne de caractères "community".

- SNMPv2u (expérimental):
  Utilise les opérations et types de SNMPv2c
  Sécurité basée sur les usagers

La version la plus utilisée est SNMPv2c,

Inversion de la tendance avec l'introduction en 1997 de SNMPv3.

Avantages de SNMPv3:
- sécurité plus importante
- gestion hiérarchisée

Inconvénients de SNMPv3:
- complexité énorme
- difficultés d'implémentation
- mise en œuvre délicate

SNMP est un protocole de la famille TCP/IP (Internet protocol), et peut donc être utilisé sur tous les réseaux de type Internet.

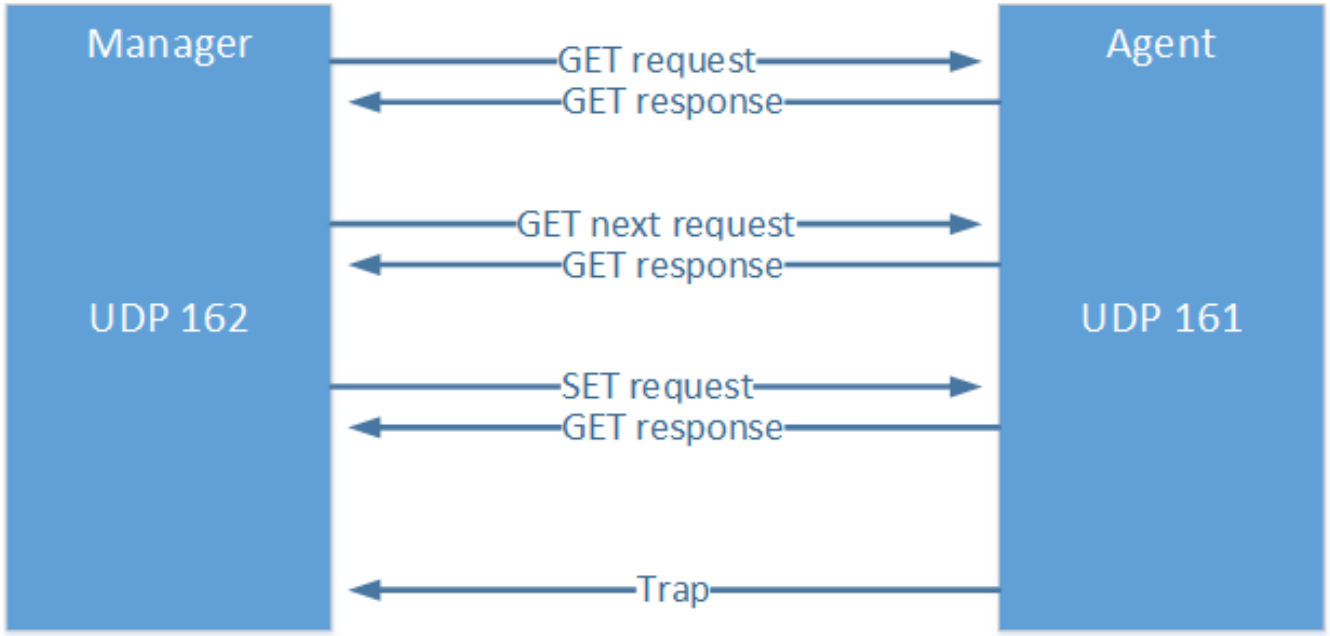
Il exploite les capacités du protocole de transport UDP :

- Chaque trame possède une adresse source et une adresse destination
- Un checksum optionnel qui couvre l'entête et les données de la trame.
- 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.

# Principes de fonctionnement

Le protocole SNMP se base sur le fait qu'il existe une station de gestion réseau, le manager, dont le rôle est de contrôler le réseau et de communiquer via ce protocole avec un agent.

L'agent est de manière générale une interface SNMP embarquée sur le matériel destiné à être administré à distance.



| Commande | Action |
|---|---|
| get request | Le Manager SNMP demande une information à un agent SNMP |
| get next request | Le Manager SNMP demande l'information suivante à l'agent SNMP |
| set request | Le Manager SNMP met à jour une information sur un agent SNMP |
| get response | L'agent SNMP répond à un get-request ou a un set-request |
| trap | L'agent SNMP envoie une alarme au Manager |

Commandes:

Les commandes suivantes sont émises par le manager à destination d'un agent :
- *get-request*
- *get-next-request*
- *set-request*

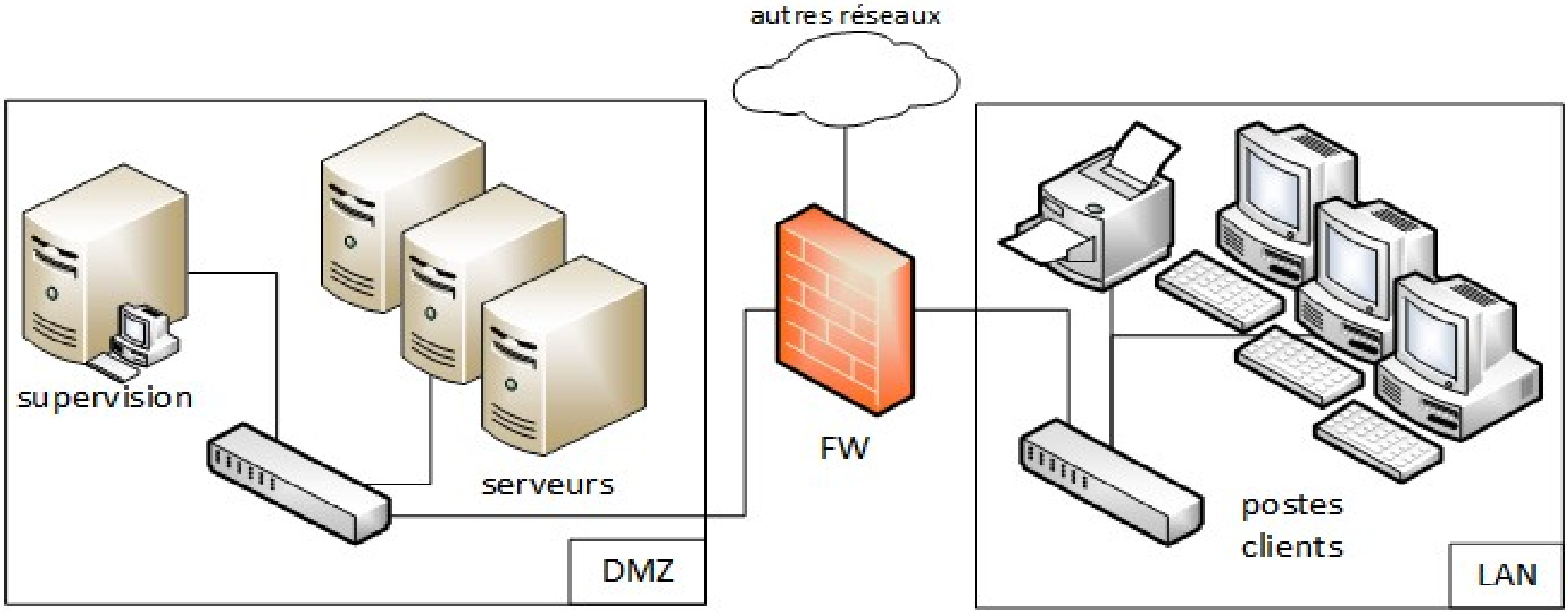
Elles attendent toutes une réponse *get-response* de la part de l'agent.

Traps:

Les traps sont des alertes.

Elle sont toujours émises par l'agent à destination du manager, et n'attendent pas de réponse.

## Exemple d'intégration dans un réseau:



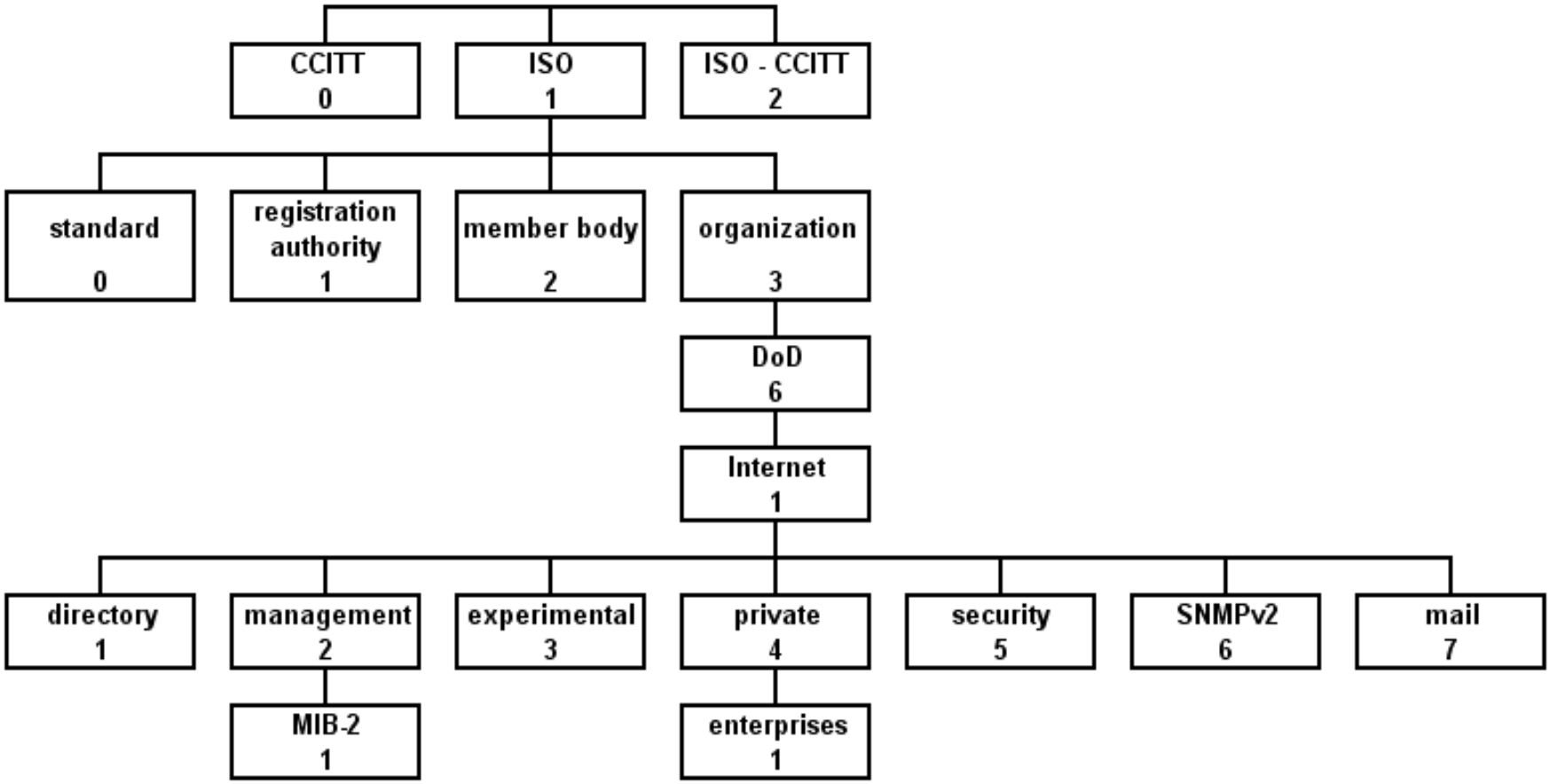
# La *Management Information Base*

# (MIB)

## La ***M**anagement **I**nformation **B**ase* (*MIB*)

La MIB est l'ensemble des informations structurées sur une entité réseau qui peuvent être récupérées et / ou modifiées.

Elle est structurée de la sorte:



## Structure de la MIB

Elle est organisée hiérarchiquement, de la même façon que l'arborescence des domaines Internet.

Elle contient une partie:
- commune à tous les agents SNMP en général;
- commune à tous les agents SNMP de même type;
- spécifique à chaque constructeur.

Elle peut contenir des scalaires (valeurs uniques) ou des tableaux de scalaires.

La structure est normalisée ainsi que les appellations des diverses rubriques.

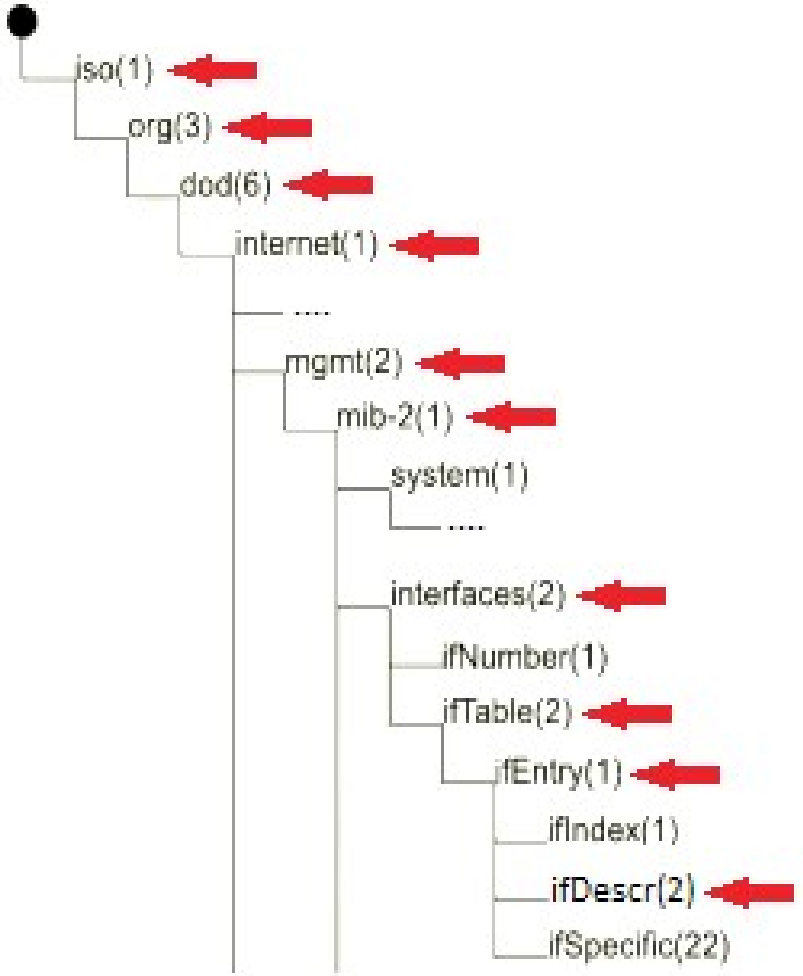
## Accès à un élément

La structure de la MIB est hiérarchique : les informations sont regroupées en arbre.

Chaque information a un **O**bject **Id**entifier (*OID*):
- une suite de chiffres séparés par des points (identifiant unique);
- un nom indiqué dans le document qui décrit la MIB.

## Accès à un élément

Exemple, 1.3.6.1.2.1.2.2.1.2 est l'object identifier ifDescr qui est la chaîne de caractères décrivant une interface réseau:



# Installation et utilisation

# Go to → The Linux Craftsman