L3 informatique TP n°4 : Administration et supervision réseau

Sovanna Tan

Octobre 2009, rev. septembre 2017

Plan

1. Introduction
2. Simple Network Management Protocol (SNMP)
3. Les outils

1 Introduction

2 Simple Network Management Protocol (SNMP)

3 Les outils

Terminologie

Administration réseau

L'ISO distingue cinq domaines de l'administration réseau :

- Gestion de la configuration : configuration des routeurs, commutateurs (switches), points d'accès Wi-FI, etc.
- Gestion de la performance : mesure, analyse, contrôle de paramètres tels le taux d'utilisation et le débit.
- Gestion des pannes : détection et réparation.
- Gestion de la comptabilité : enregistrement de l'accès et de la durée d'utilisation des ressources par les utilisateurs en vue d'une facturation par exemple.
- Gestion de la sécurité : contrôle d'accès aux ressources, détection d'intrusion.

Objet du TP

Supervision réseau

Analyse et vérification du fonctionnement des équipements et des services, gestion de la performance et des pannes.

1 Introduction

2 Simple Network Management Protocol (SNMP)

3 Les outils

Simple Network Management Protocol (SNMP)

Principe de fonctionnement de SNMP

Une console de supervision (*manager*) envoie des requêtes en utilisant le protocole SNMP aux équipements (*nodes*) administrés par ce moyen.

- Sur les équipements, des agents collectent les informations et les transmettent à la console de supervision.
- En cas d'anomalie, les équipements peuvent envoyer des alarmes ou *traps*.
- Le protocole permet également à la console de modifier des paramètres de configuration sur les équipements.

Console de supervision SNMP

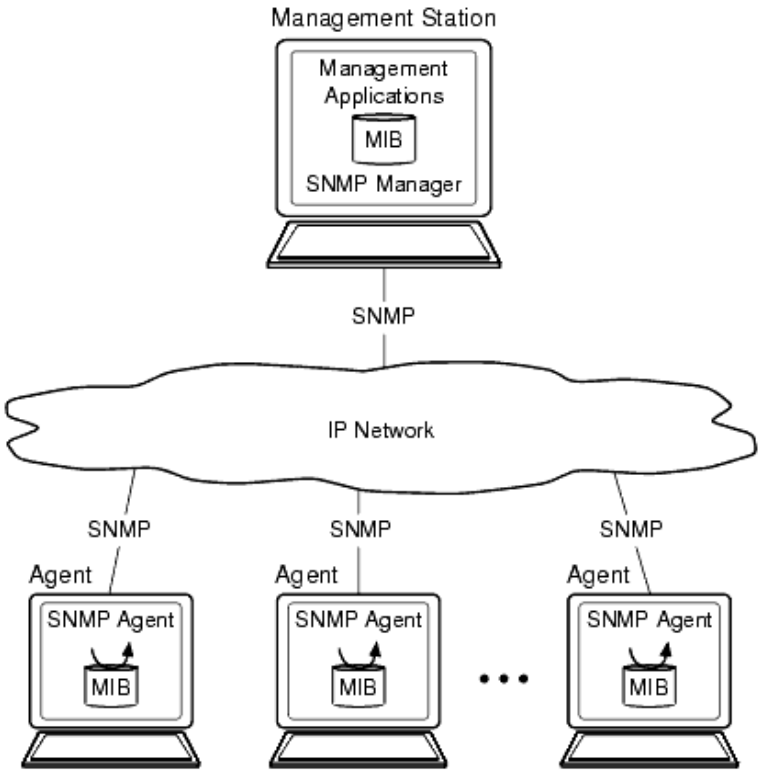

Image extraite de `http://docs.hp.com/en/5991-5856/ar01s02.html`

Informations échangées avec SNMP

Management Information Base (MIB)

- Ensemble d'informations structuré et normalisé géré par un agent SNMP écrit en ASN.1 (Abstract Syntax Notation One).
- Système arborescent similaire au DNS.
- Les données contenues sont de type scalaire ou tableau de scalaires.
- Une MIB se compose de
  - une partie commune à tous les agents SNMP ;
  - une partie commune aux agents SNMP d'un même type de matériel ;
  - et une partie spécifique à chaque constructeur.

Extrait de MIB

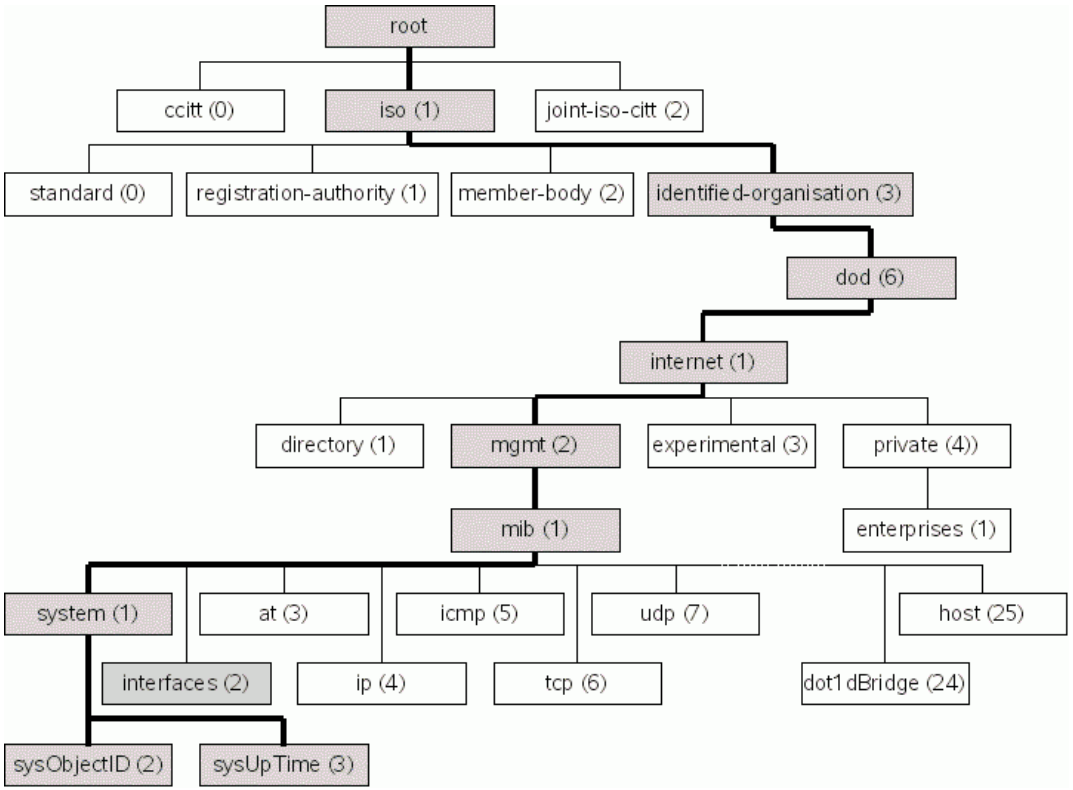

Image extraite de

`https://www-rp.lip6.fr/trac/pfres/wiki/observations_snmp_getrequest`

Elément d'une mib

Object IDentifier (OID)

Type de données normalisé par l'ISO, utilisé pour représenter les données d'une MIB.

- Exemple : iso.org.dod.internet.mgmt.mib.system.sysDescr.0 ou 1.3.6.1.2.1.1.1.0
- Le protocole SNMP permet aux équipements de communiquer à la console de supervision, la valeur des paramètres identifiés par les OIDs, regroupés dans les MIBs.
- Les OIDs sont également utilisés pour représenter les entrées d'un annuaire LDAP (Lightweight Directory Access Protocol).

Identification

Communauté SNMP (*community*)

Les équipements et les consoles de supervision sont regroupés dans des communautés. Le nom de la communauté sert à identifier le groupe.

- Il existe deux communautés par défaut :
  - `public` : droit de lecture des informations de la MIB ;
  - `private` : droit de lecture et d'écriture.
- Le nom de communauté sert de mot de passe. Il est prudent de ne pas utiliser les noms de communauté par défaut.
- Dans SNMP version 1, le nom de la communauté circule en clair sur le réseau.

1 Introduction

2 Simple Network Management Protocol (SNMP)

3 Les outils

Les outils

- `Net-SNMP` : suite d'outils qui implémentent SNMP.
- `Nagios` : surveille les équipements et les services.
- `Network TOP (ntop)` : collecte les informations sur le trafic réseau.
- `Cacti` : représente graphiquement des données collectées avec SNMP entre autre.