Introduction à SNMP

RANDRIANARIVONY Nirinarisantatra

Administrateur Système
i RENALA - Fiadanana

May 22, 2014

Présentation Générale

- Qu'entend-on par SNMP?
- OID
- MIB
- Interrogations et invitations à émetttre
- Déroutements

R. Nirinarisantatra, 2014

Qu'entend-on par SNMP?

- SNMP – Simple Network Management Protocol
  - Un standard de l'industrie avec des centaines d'outils pour l'exploiter
  - Supporté par tout équipement réseau digne de ce nom
- Basé sur des interrogations–réponses: **GET / SET**
  - GET sert principalement à la surveillance
- OID (Object Identifiers)
  - Clés pour identifier des morceaux d'information (organisées de manière hiérarchique)
- Concept de bases d'informations de gestion (MIB)
  - standard et propriétaire (entreprise)

R. Nirinarisantatra, 2014

Qu'entend-on par SNMP? (suite)

- Terminologie
  - Le "manager" ("client" superviseur)
  - L'agent (opérant sur l'équipement/le serveur)
- Interrogations (requêtes) types
  - Octets en entrée/sortie sur une interface, erreurs
  - Charge de l'UC
  - Temps d'utilisation (uptime)
  - Température ou autres OID propres aux constructeurs
- Pour les hôtes (serveurs ou postes de travail)
  - Espace disque
  - Logiciels installés
  - Processus en cours d'exécution
  - ...
- Windows et UNIX disposent d'agents SNMP

R. Nirinarisantatra, 2014

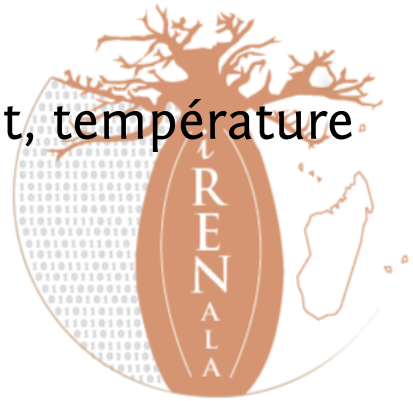
Qu'entend-on par SNMP? (suite)

- Protocole UDP, port 161
- Différentes versions
  - v1 (1988) – RFC1155, RFC1156, RFC1157
    - Spécification d'origine
  - v2 – RFC1901 ... RFC1908 + RFC2578
    - Etend la v1, nouveaux types de données, méthodes de recherche améliorées (GETBULK)
    - Nous utilisons la version v2c (sans modèle de sécurité)
  - v3 – RFC3411 ... RFC3418 (avec sécurité)
- Nous utilisons généralement SNMPv2 (v2c)

R. Nirinarisantatra, 2014

Principes de fonctionnement

- GET (manager -> agent)
  - Demande une valeur
- GET-NEXT (manager -> agent)
  - Récupère la valeur suivante (liste de valeurs d'une table)
- GET-RESPONSE (agent -> manager)
  - Répond à GET/SET ou erreur
- SET (manager -> agent)
  - Définit une valeur ou réalise une action
- TRAP (agent -> manager)
  - Notification spontanée (alerte) de l'équipement (arrêt, température au-dessus du seuil, ...)



R. Nirinarisantatra, 2014

OIDs et MIBs

OID: Object Identifier – Identificateur Objet

- Une clé unique pour désigner un élément de données particulier dans l'équipement
- Le même élément de données est toujours trouvé au même OID – c'est simple!
- Un OID est une chaîne de chiffres à longeur variable, par ex.: 1.3.6.1.2.1.1.3
- Allouée de manière hiérarchique pour assurer l'unicité (comme le DNS)

R. Nirinarisantatra, 2014

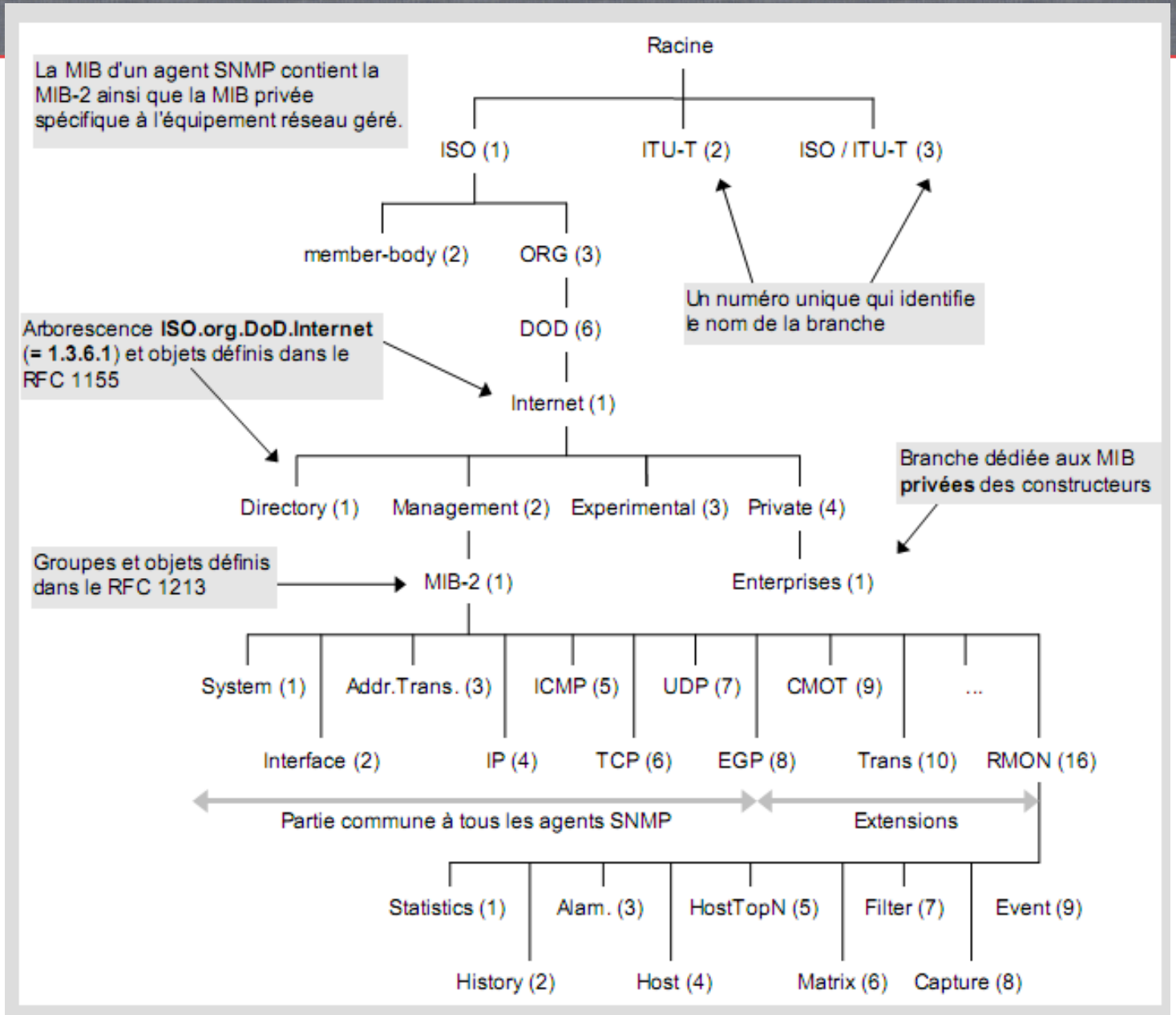
OIDs et MIBs (suite)

MIB: Management Information Base – Base Informationnelle de Gestion

- Une collection d'OID qui sont apparentés
- Une association entre OID numériques et des noms symboliques lisibles par des humains

R. Nirinarisantatra, 2014

L'arborescence MIB



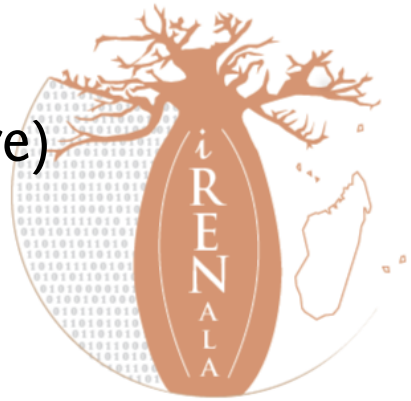
R. Nirinarisantatra, 2014

La MIB internet

- **directory** (1): répertoire OSI
- **mgmt** (2): objets RFC standard (*)
- **experimental** (3): expérimentations sur internet
- **private** (4): propriétaire (*)
- **security** (5): sécurité
- **snmpV2** (6): SNMP interne

(*) En réalité, il n'y a que 2 branches qui nous intéressent:

- 1.3.6.1.**2**.1 = MIB standard
- 1.3.6.1.**4**.1 = MIB spécifique à un fabricant (propriétaire)



R. Nirinarisantatra, 2014

OID et MIB

- Navigation descendante dans l'arborescence
- OID séparés par '.'
  - 1.3.6.1.4.1.9. ...
- Un OID correspond à une étiquette
  - .1.3.6.1.2.1.1.5 => sysName
- Le chemin complet:
  - .iso.org.dod.internet.mgmt.mib-2.system.sysName
- Comment passer des OID à des étiquettes (et inversement?)
  - Utilisation des fichiers MIB !

R. Nirinarisantatra, 2014

MIB

- Les MIB sont des fichiers définissant des objets pouvant faire l'objet d'interrogations; ces fichiers intègrent:
  - Le nom de l'objet
  - La description de l'objet
  - Le type de données (entiers, textes, listes)
- Les MIB revêtent la forme de texte structuré en notation ASN.1
- Les MIB types incluent:
  - MIB-II – (RFC1213) – groupe de sous-MIB
  - HOST-RESOURCES-MIB (RFC2790)
- Les MIB permettent également d'interpréter une valeur retournée par un agent

R. Nirinarisantatra, 2014

Interrogation d'un agent SNMP

- Commandes de requête classiques:
  - snmpget
  - snmpwalk
  - snmpstatus
  - snmptable
- Syntaxes
  - snmpXXX -c community -v1 host [oid]
  - snmpXXX -c community -v2c host [oid]
- Exemples
  - snmpstatus -c NetManage -v2c 192.168.56.254
  - snmpget -c NetManage -v2c 192.168.56.254 .iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber.0
  - snmpwalk -c NetManage -v2c 192.168.56.254 ifDescr

R. Nirinarisantatra, 2014

Interrogation d'un agent SNMP (suite)

- Communauté:
  - Chaîne de "sécurité" (mot de passe) définissant le niveau d'accès du manager - RO (lecture uniquement) ou RW (lecture-écriture)
  - Forme d'authentification la plus simple dans SNMP
- OID
  - Une valeur, .1.3.6.1.2.1.1.5.0, par exemple, le nom correspondant
  - .iso.org.dod.internet.mgmt.mib-2.system.sysName.0
- Demandons le nom du système (avec l'OID ci-dessus)
  - À quoi correspond le .0? Que remarquez-vous?

R. Nirinarisantatra, 2014

Panne SNMP ... pas de réponse?

- L'équipement peut être éteint/déconnecté ou injoignable
- L'équipement ne fait peut être même pas tourner un agent SNMP
- L'équipement a peut-être une communauté SNMP différente
- L'équipement est peut-être configuré pour refuser les requêtes depuis votre adresse
- Dans tous les cas ci-dessus, vous n'obtiendrez pas de réponse!

R. Nirinarisantatra, 2014

Prochains exercices ...

- Utilisation de snmpwalk, snmpget
  - Fichier de configuration: /etc/snmp/**snmp**.conf
- Configuration de l'agent SNMPD
  - Fichier de configuration: /etc/snmp/**snmpd**.conf
- Chargement des MIB

R. Nirinarisantatra, 2014