420-S0R-TT

Surveillance et optimisation des réseaux

Simple Network Management Protocol (SNMP)

ÉTÉ 2024

Table des matières

1 Introduction

SNMP (*Simple Network Management Protocol*) a été défini pour servir de standard aux échanges d'informations concernant l'état de santé et la configuration des périphériques d'un réseau. C'est un protocole, mais comme d'autres protocoles (par exemple DNS) il repose aussi sur un modèle.

Il existe plusieurs versions de **SNMP** :

SNMPv1 est simple, mais a des lacunes en sécurité : il ne définit aucun mécanisme d'authentification ni de chiffrement.

SNMPv2 vise à corriger ce problème, mais ceux qui ont participé au développement de cette version ne se sont jamais vraiment entendus; il existe donc plusieurs sous-versions de SNMPv2.

SNMPv3 est le standard officiel, le plus récent. Mais en réalité, les 3 versions sont utilisées.

Dans ce cours, nous allons voir deux versions du protocole : la ***2c*** et la ***3***.

2 Une petite chronologie des versions

1988 : SNMPv1

1992 : SNMPsec (n'a jamais été adopté)

1992 : SNMPv2, (n'a jamais fait l'unanimité)

1996 : SNMPv2c (« Community-based SNMP v2 »)

1996 : SNMPv2u (« User-based SNMP v2 »)

1998 : SNMPv3

3 Les références

SNMPv1 : RFC1155, RFC1156, RFC1157, RFC1213

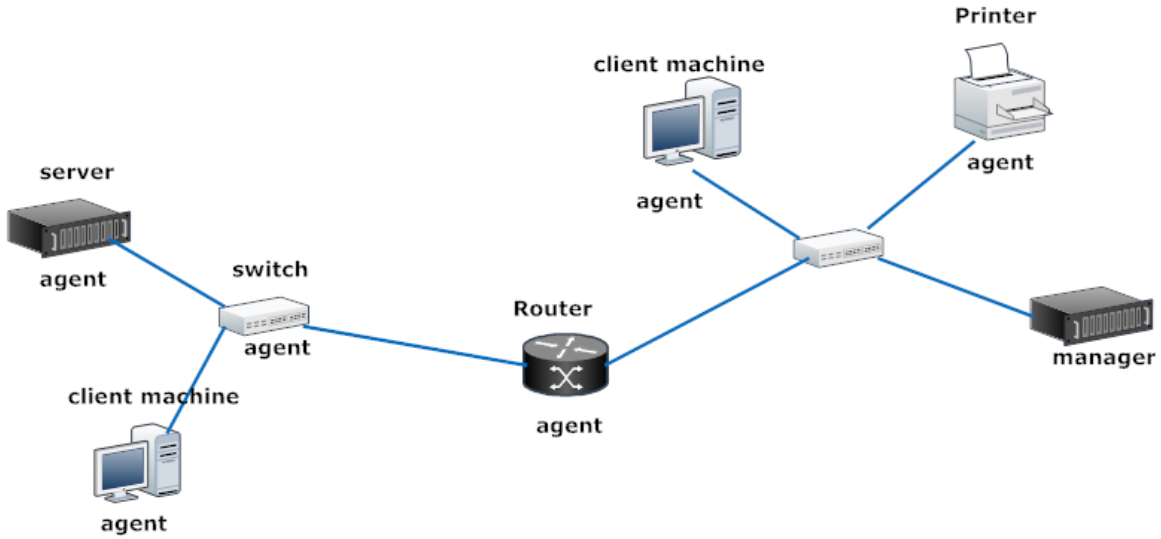
SNMPv2 : RFC1441, RFC1452; RFC1901, RFC1908, RFC1909, RFC1910

SNMPv3 : RFC3411, RFC3412 et RFC3418

4 Architecture du protocole SNMP

Le modèle SNMP suit un modèle entité association qui définit deux types d'entités :

- Les entités gérées (hôtes, commutateurs, routeurs)
- Les entités de gestion (les hôtes qui reçoivent les informations provenant des entités gérées)



En SNMP, on ne parle pas de client ou de serveur, mais plutôt ***d'agent*** et de ***gestionnaire*** (manager).

5 MIB

Les informations qui caractérisent les hôtes et périphériques sont contenues dans des ***MIB*** (*Management Information Base*), elles sont aussi définies dans un standard.

Les MIB sont composés d'un ensemble de variables ayant un nom et une valeur; ces valeurs peuvent être lues ou écrites à partir d'un gestionnaire SNMP. Certaines variables sont en lecture seule.

Chaque objet MIB a les 6 propriétés suivantes (au minimum)

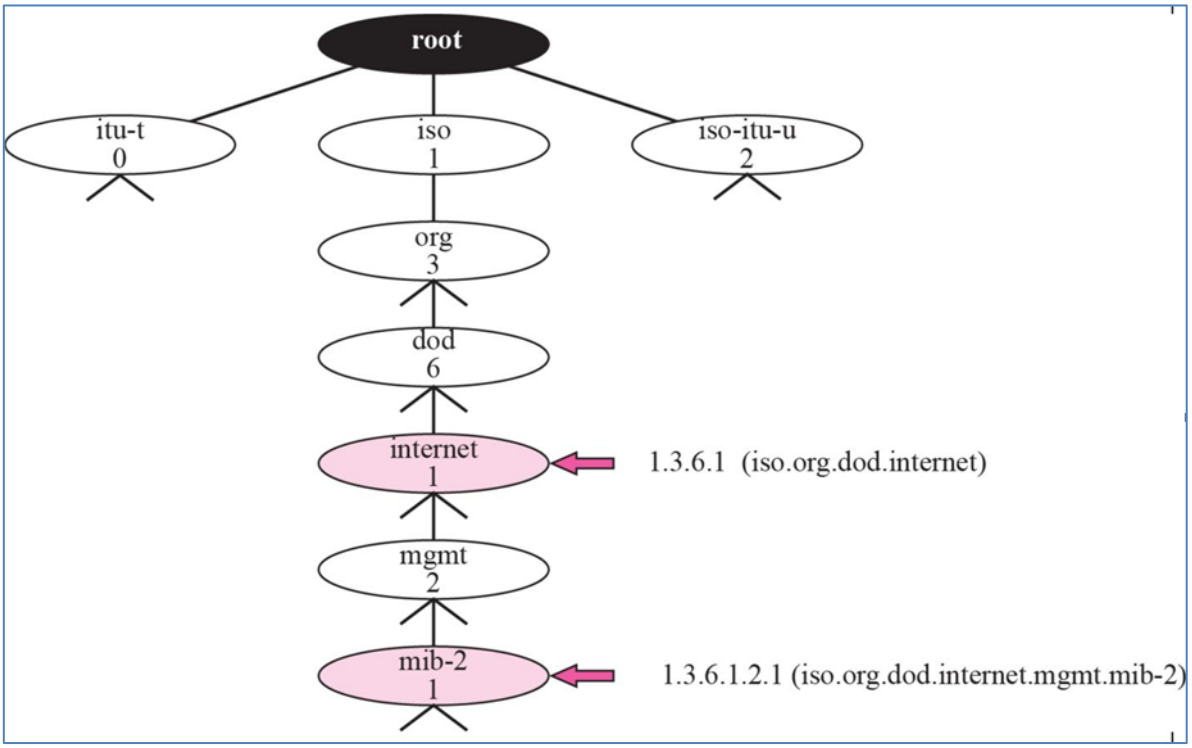
- ***OID :*** Un identifiant unique
- ***Nom :*** Désignation de l'objet
- ***Syntaxe :*** Type de donnée et structure, par exemple un tableau de *chaines de caractères*, nombre entier unique, etc.
- ***Statut :*** Définis si l'objet est conforme au standard actuel ou non
- ***Description :*** Texte descriptif
- ***Accès :*** Lecture seule, lecture-écriture, etc.

Des attributs optionnels sont possibles.

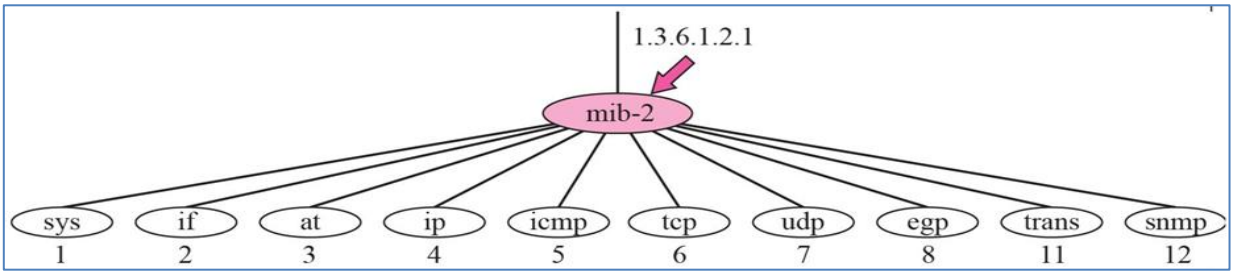
Les **MIBs** sont organisés selon une hiérarchie, et chaque nœud de cette hiérarchie est désigné par un nombre.

Donc n'importe quel objet dans une MIB est désigné par une séquence de nombres : c'est ce nombre qu'on nomme « OID ».

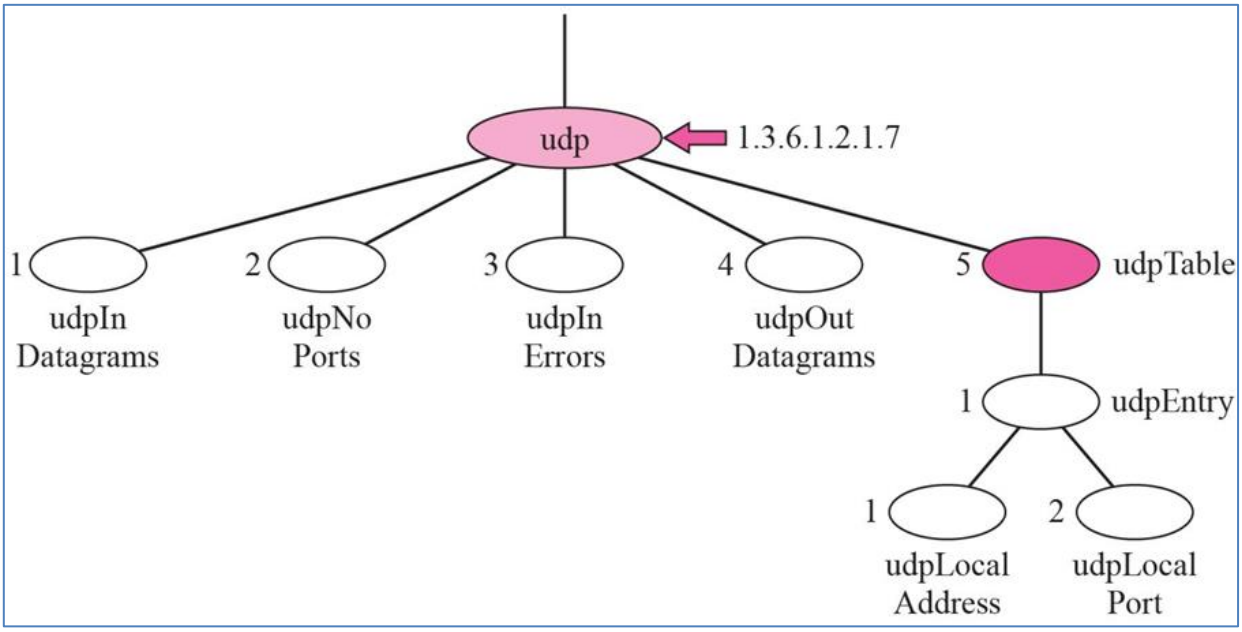
Par exemple, les adresses IP d'un hôte sont contenues dans une table nommée ***IpAddrTable*** dont **l'OID** est ***1.3.6.1.2.1.4.20***.



La plupart des objets utilisés couramment sont dans la branche **1.3.6.1**, plus particulièrement **1.3.6.1.2.1** (les objets communs ou **MIB-2**, qui forment la grande majorité des objets utilisés, voire la description détaillée ici) et **1.3.6.1.4.1** (les objets définis par des entreprises privées, voir la liste des entreprises ayant obtenu un **OID** par **IANA**ici).



Beaucoup d'informations ne font pas partie de la hiérarchie « de base », mais sont plutôt définies dans des modules.



6 SMI

SMI (*Structure of Management Information*) définit la structure des MIB (hiérarchie, *datatypes*, nomenclature, etc.). Les objets MIB sont regroupés en modules MIB, et chaque entité SNMP peut être définie par plusieurs modules.

Pour conclure:

SMI	définition de la structure, datatypes, etc. des MIBs
MIB	liste des objets (définis par la SMI) qui sont supportés par un appareil
SNMP	protocole définissant l'échange de messages entre agents et gestionnaires

7 Messages SNMP

Le protocole SNMP permet 2 types de communication :

- Un gestionnaire interroge les agents (« polling »)
- Les agents envoient des alertes (« trap ») au gestionnaire

Le « **polling** » ou sondage est utile pour collecter des statistiques d'usage ou des informations de configuration, mais quand on veut être prévenu des problèmes dès qu'ils surviennent, un mécanisme d'alerte est nécessaire.

UDP est utilisé comme protocole de transport; le port ***161*** est le port d'écoute sur les agents (requêtes)et le port ***162*** est le port d'écoute sur les gestionnaires (alertes).

Les classes de messages:

Lecture	• *GetRequest,* • *GetNextRequest,* • *GetBulkRequest*
Écriture	• *SetRequest*
Réponse	• *Response*
Alertes	• *Trapv2,* • *InformRequest*

GetRequest : Le gestionnaire envoie une requête à l'agent, qui répond avec un message ***Response***

GetNextRequest : similaire à un ***GetRequest***, mais le gestionnaire demande d'envoyer l'objet suivant celui qui est spécifié dans la requête.

GetBulkRequest : similaire à un ***GetRequest***, mais ***Response*** contient un ensemble d'objets.

SetRequest : Le gestionnaire envoie une requête à l'agent, qui retourne un message ***Response*** après avoir fait les modifications (si possible/permis)

Trapv2 : L'agent envoie une alerte au gestionnaire; le gestionnaire peut retransmettre cette alerte en envoyant un message ***InformRequest*** à un autre gestionnaire, qui doit lui retourner une confirmation avec un message ***Response***.

À noter : un agent qui envoie un message *Trapv2* ne reçoit jamais de confirmation.

8 Sécurité

Dans SNMPv1 et v2, il n'existe pas de méthode uniforme pour assurer l'authentification et la confidentialité.

Dans SNMPv2c, on utilise les « communautés » pour définir l'appartenance à un groupe d'hôtes surveillés. Il y a deux types de communautés : celles qui sont en lecture seule (***rocommunity***) et celles qui sont en lecture/écriture (***rwcommunity***).

Dans SNMPv3, la sécurité est basée sur un système d'utilisateurs. Il y a trois niveaux de sécurité, qui peuvent être différents entre les utilisateurs :

- Pas d'authentification, pas de chiffrement des communications
- Authentification sans chiffrement des communications
- Authentification et chiffrement des communications

L'authentification par mot de passe peut utiliser les algorithmes de hachage MD5 ou SHA, et le chiffrement peut utiliser DES ou AES.

Il n'y a pas de mécanismes de sécurité centralisée : chaque agent définit ses propres utilisateurs et leurs paramètres.

Pour sonder un agent, le gestionnaire doit utiliser les paramètres d'authentification de cet agent, et ces paramètres peuvent être différents pour un autre agent.

Inversement, un agent qui veut envoyer une alerte à un gestionnaire devra s'authentifier conformément aux paramètres définis dans le gestionnaire.

En somme, chaque entité SNMP, qu'elle soit un gestionnaire ou un agent, a ses propres paramètres de sécurité, et ceux-ci doivent être utilisés par n'importe quelle autre entité qui désire lui envoyer un message.

9 Browser SNMP

À télécharger en suivant le lien :

http://www.ireasoning.com/