

Cours 40 : Simple Network Management Protocol

Dans ce cours nous verrons le fonctionnement de SNMP (Simple Network Management Protocol). Nous verrons tout d'abord le fonctionnement de SNMP, puis les différentes versions disponibles de SNMP, nous verrons ensuite les différents types de messages que SNMP utilise pour fonctionner. Nous verrons comment configurer basiquement SNMP.

SNMP est un protocole de type standard industrie et le protocole a été originellement publié en 1988.

Le RFC 1065 structure et identifie la gestion des informations pour TCP/IP basé sur Internet.

Le RFC 1066 permet la gestion des informations de base pour la gestion de base du réseau pour TCP/IP basé sur Internet.

Le RFC 1067 est un protocole de gestion du réseau simple (Simple Network Management Protocol ou SNMP)

Les 3 RFC précédentes forment la version 1 de SNMP.

Le terme Simple dans le nom du protocole ne signifie pas qu'il s'agit d'un protocole simple, la version 1 est même plus compliqué que la dernière version actuelle qui est la version 3.

SNMP peut être utilisé pour suivre le statut d'appareils, faire des changements de configuration etc...

Il y a deux types d'appareils dans SNMP.

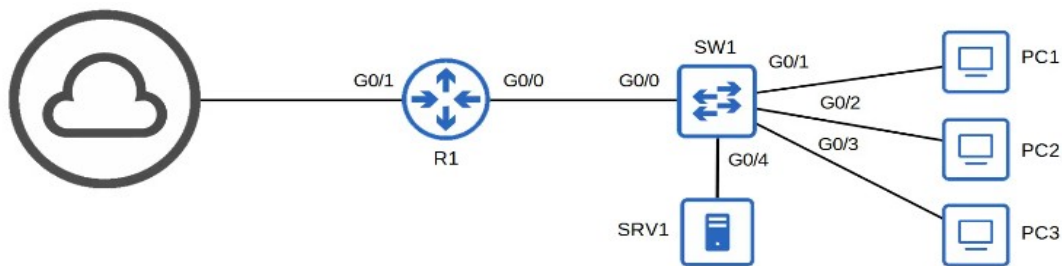
1) Les appareils gérés :

- Ce sont les appareils utilisés gérés en utilisant le protocole SNMP.
- Par exemple, les appareils du réseau comme les routeurs et commutateurs.

2) Network Management Station (NMS) (en français : Les stations de gestion du réseau)

- Ce sont l'appareil ou les appareils qui gèrent d'autres appareils.
- C'est aussi le « serveur SNMP ».

Voyons comment fonctionne SNMP, pour cela nous utiliserons le réseau suivant :



Le serveur 1 est ici le NMS. Les appareils gérés sont ici le commutateur et le routeur.

Il y a 3 principales opérations en utilisant SNMP.

1) les appareils gérés peuvent notifier le NMS des événements.

Par exemple la connexion entre le Switch1 et le PC1 est interrompue, le SW1 enverra un message au NMS lui indiquant que la connexion est interrompue.

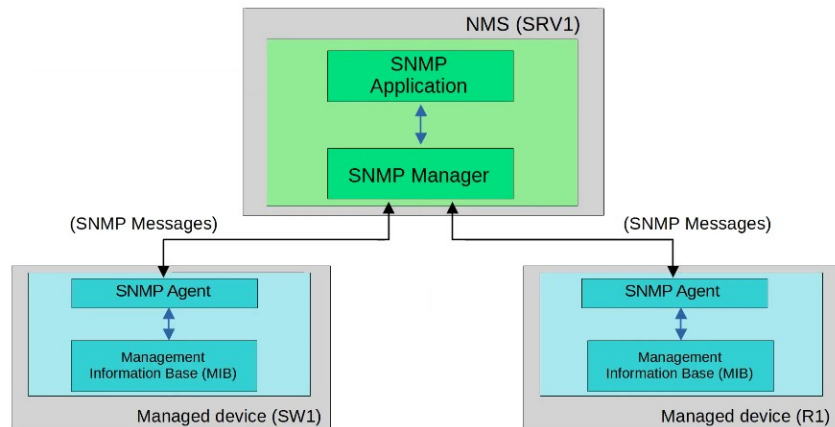
2) Le NMS peut aussi demander aux appareils gérés des informations à propos de leur statut actuel. Par exemple le NMS peut demander au SW1 ainsi qu'au routeur R1 quelle est son utilisation du CPU. R1 répond en lui indiquant son statut d'utilisation.

3) Le NMS peut demander aux appareils gérés de changer leurs configurations.

Par exemple le NMS peut demander au Routeur R1 de changer son adresse IP pour une autre.

Le routeur R1 répond ensuite au NMS et lui indique que l'adresse IP est bien la nouvelle configurée.

Il est possible de résumer le fonctionnement du réseau avec le schéma ci dessous :

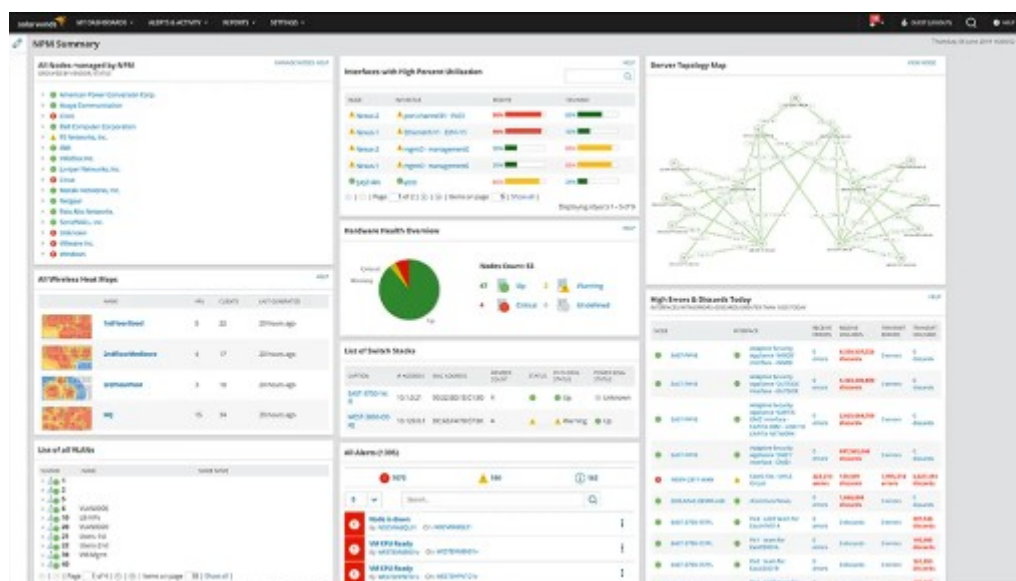


au niveau du NMS ou serveur 1 on peut retrouver le gestionnaire SNMP qui est le logiciel du NMS qui interagit avec l'appareil géré.

Il reçoit des notifications, envoie des requêtes pour des informations, envoie des changements de configuration, etc...

Il y a aussi l'application SNMP qui fournit une interface pour l'administrateur réseau qui interagit avec. Cela affiche des alertes, des statistiques, des chartes, etc...

Une application SNMP ressemble à cela :



Il y a plusieurs choix d'applications disponibles dans l'utilisation du protocole SNMP, l'application ci dessus provient de SolarWind.

Ensuite au second niveau on peut voir différents appareils qui sont les appareils gérés (SW1 et R1)

Il y a plusieurs entités présentes pour chaque appareil, tout d'abord l'agent SNMP, qui est le logiciel qui se lance dans les appareils gérés et qui interagit avec le gestionnaire SNMP du NMS.

Il envoie/receptionne des notifications de messages du NMS.

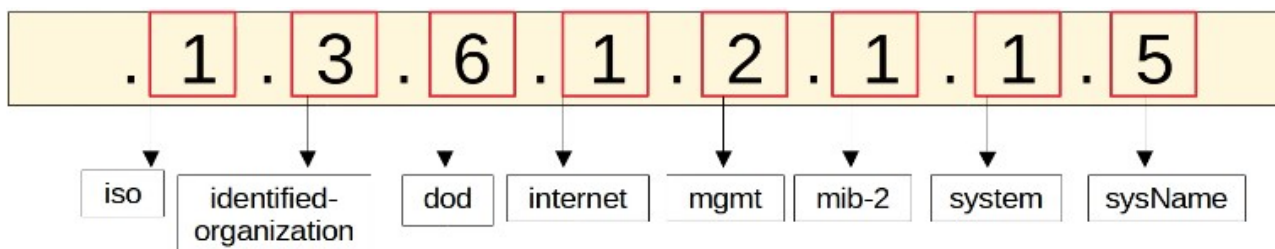
Un autre composant important est le Management Information Base (MIB) c'est la structure qui contient les variables gérés par SNMP.

Chacune de ces variables est identifié avec un ID d'Objet. (OID pour Object ID)

Des exemples de variables sont le statut de l'interface, le trafic, l'utilisation CPU, la température, etc...

Des messages SNMP entre le MIB et le gestionnaire SNMP sont échangés.

Les ID d'objets SNMP sont organisés en une hiérarchie de structure.



Par exemple le NMS peut envoyer un message SNMP à SW1 afin de connaître la valeur de son OID. Le SW1 peut lui répondre que l'OID demandé est SW1.

Il est possible d'avoir plus d'informations concernant l'OID sur le site : oid-info.com

Voyons à présent quelles sont les principales Version qui existent du protocole SNMP.

Plusieurs versions de SNMP ont été proposés ou développé, il existe cependant 3 versions principales qui sont les suivantes :

- SNMPv1 : Il s'agit de la version originale de SNMP

- SNMPv2c : Il permet au NMS de recevoir un grand montant d'informations en une seule requête, donc cela est plus efficace.

La lettre « c » fait référence au « community string » utilisé comme mot de passe dans SNMPv1 (il fallait sélectionner une lettre pour mot de passe), et supprimé de SNMPv2, puis rajouté une nouvelle fois pour SNMPv2c.

- SNMPv3 : Il s'agit de la version la plus sécurisé de SNMP qui supporte des mot de passe crypté et une authentification. Si possible cette version devrait être utilisé.

Voyons à présent le type de messages utilisé :

Classe de message	Description	Messages
Read	Les messages envoyés par le NMS pour lire des informations depuis les appareils gérés. (Pour savoir par exemple l'utilisation CPU)	<i>Get</i> <i>GetNext</i> <i>GetBulk</i>
Write	Les messages envoyés par le NMS pour changer des informations sur les appareils gérés (par exemple l'adresse IP)	<i>Set</i>
Notification	Les messages envoyés par les appareils gérés pour alerter le NMS d'un évènement particulier	<i>Trap</i> <i>Inform</i>
Response	Les messages envoyés en réponse d'un message/requête précédent	<i>Response</i>

Voyons rapidement en détail chacun de ces messages :

- Get : Il s'agit d'une requête envoyé depuis le gestionnaire à l'agent pour récupérer la valeur de la variable de l'OID ou de plusieurs variables. L'agent envoie ensuite un message « Response » avec le valeur actuelle de chaque variable.

Par exemple le NMS demande quelle est le statut de l'interface G0/1 au Switch. Celui ci répond que l'interface est « Up » ou active.

- GetNext : Il s'agit d'une requête envoyé depuis le gestionnaire vers l'agent pour découvrir les variables disponibles dans le MIB.

Par exemple il demande quelle est le prochain OID, donc ce message peut servir à savoir quelles OID sont disponibles.

- GetBulk : Il s'agit d'une version plus efficace des messages GetNext.

- Set : Il s'agit d'une requête envoyé depuis le gestionnaire vers l'agent pour changer la valeur d'une ou de plusieurs variables. L'agent envoie un message de Response avec la nouvelle valeur.

Par exemple le NMS envoie un message au SW1 lui demandant de changer de nom d'hôte pour SW10 et celui ci répond avec son nouveau nom d'hôte.

- Trap : Il s'agit d'une notification envoyé depuis l'agent vers le gestionnaire. Le gestionnaire n'envoie pas de message de réponse qui confirme qu'il a reçu le Trap, donc ces messages sont « peu fiables ».

Par exemple la connexion entre R1 et SW1 est interrompue, le SW1 envoie un message de Trap au NMS pour lui indiquer que la connexion est interrompu.

- Inform : est un message de notification qui confirme avec un message de réponse.

A l'origine utilisé pour la communication entre plusieurs gestionnaire, mais après des mis à jour cela permet aux agents d'envoyer des messages Inform aux gestionnaires aussi.

- Response : Il s'agit de messages envoyés en réponse à d'autres.

Les ports utilisés par SNMP sont :

- Agent SNMP : UDP 161

- Gestionnaire SNMP : UDP 162

Voyons comment configurer le protocole SNMPv2c.

Dans le même réseau qu'auparavant on lance les commandes suivantes depuis le routeur R1 :

```
R1(config)#snmp-server contact jeremy@jeremysitlab.com
R1(config)#snmp-server location Jeremy's House

R1(config)#snmp-server community Jeremy1 ro

R1(config)#snmp-server community Jeremy2 rw

R1(config)#snmp-server host 192.168.1.1 version 2c Jeremy1

R1(config)#snmp-server enable traps snmp linkdown linkup
R1(config)#snmp-server enable traps config
```

On configure tout d'abord l'adresse de contact et la localisation de l'appareil, il s'agit de commandes optionnel : `snmp-server contact` et `snmp-server location`

On configure ensuite le SNMP community string (la lettre qui servira de mot de passe) :

`snmp-server community Jeremy1 ro` signifie read only pour que l'utilisateur Jeremy1 n'envoie pas de messages de type Set.

`snmp-server community Jeremy2 rw` signifie read/write pour que l'utilisateur Jeremy2 utilise des messages de type Set.

On tape ensuite le mot de passe à utiliser.

On spécifie ensuite l'adresse du NMS avec la commande :

```
snmp-server host 192.168.1.1 version 2c jeremy1
```

Ici l'adresse du serveur NMS est 192.168.1.1 on indique la version SNMP à utiliser ici la version 2c et l'utilisateur pouvant se connecter au NMS, ici l'utilisateur Jeremy1.

On configure le type de messages Trap qui seront envoyés au NMS :

```
snmp-server enable traps snmp linkdown linkup
```

```
snmp-server enable traps config
```

Dans cette configuration lorsque qu'un appareil change de statut de « up » à « down » un message Trap est envoyé.

Voyons plus en détail avec Wireshark les messages envoyés lorsque l'interface G0/1 est interrompue.

No.	Time	Source	Destination	Protocol	Length	Info
209	13:55:21.662570	192.168.1.254	192.168.1.1	SNMP	221	snmpV2-trap 1.3.6.1.2.1.
> Frame 209: 221 bytes on wire (1768 bits), 221 bytes captured (1768 bits) on interface -, id 0						
> Ethernet II, Src: 0c:1c:1a:87:fb:00 (0c:1c:1a:87:fb:00), Dst: 0c:1c:1a:50:80:01 (0c:1c:1a:50:80:01)						
> Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.1						
> User Datagram Protocol, Src Port: 65385, Dst Port: 162						
▼ Simple Network Management Protocol						
version: v2c (1)						
community: Jeremy1						
▼ data: snmpV2-trap (7)						
▼ snmpV2-trap						
request-id: 14						
error-status: noError (0)						
error-index: 0						
▼ variable-bindings: 6 items						
> 1.3.6.1.2.1.1.3.0: 104924						
> 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.3 (iso.3.6.1.6.3.1.1.5.3)						
> 1.3.6.1.2.1.2.2.1.1.2: 2						
> 1.3.6.1.2.1.2.2.1.2.2: 4769676162697445746865726e6574302f31						
> 1.3.6.1.2.1.2.2.1.3.2: 6						
> 1.3.6.1.4.1.9.2.2.1.1.20.2: 61646d696e6973747261746976656c7920646f776e						

On peut ici voir les messages OID qui sont envoyés :

Le message OID envoyé est : 1.3.6.1.6.3.1.1.5.3

Si l'on vérifie sur le site : <http://oid-info.com/> on pourra voir que le message correspondant est de type Trap qui permet de notifier le NMS que l'interface est à l'arrêt ou « down » en Anglais.

OID:	{iso(1) identified-organization(3) dod(6) internet(1) snmpV2(6) snmpModules(3) snmpMIB(1) snmpMIBObjects(1) snmpTraps(5) linkDown(3)}
	1.3.6.1.6.3.1.1.5.3
	/ISO/Identified-Organization/6/1/6/3/1/1/5/3

Sur Wireshark on peut aussi observer la version du protocole utilisé ici c'est la version v2c.

Le « community » est ici Jeremy1 le « community string » avec pour règle ro configuré auparavant. Il est à préciser qu'avec les protocole SNMPv1 et SNMPv2c il n'y a pas de cryptage. Le contenu et le community sont envoyés en texte clair. Il n'y a pas de sécurité, les paquets peuvent facilement être capturés et lus.