esprit
Ecole Supérieure Privée
d'Ingénierie et de Technologies

TP : Administration des réseaux : SNMP

I. Introduction au protocole SNMP :

Le protocole SNMP (Simple Network Management Protocol) est très utilisé dans le milieu de l'administration réseau.

En effet, il permet de simplifier grandement la maintenance des réseaux en fournissant aux administrateurs la possibilité d'obtenir de nombreuses informations sur des équipements présents sur le réseau tels que des serveurs, des routeurs ou encore des commutateurs.

Le recueil de ces informations permet d'être informé à tout moment de ce qui se passe sur le réseau et permet de réagir rapidement en cas de problème sur celui-ci, notamment en permettant le management à distance des différents équipements réseaux utilisant le protocole SNMP.

De plus, ce protocole fonctionne suivant un mode « client / serveur » ce qui permet à un administrateur de n'obtenir les informations recueillies par les équipements réseaux que lorsqu'il en fait la demande ou lorsqu'une alerte aura été déclenchée.

Afin d'éviter tout détournement d'information ou contrôle non autorisé sur ces divers équipements, il est également possible d'instaurer des mesures de sécurité permettant de s'assurer que seules des personnes autorisées puissent consulter ces bases d'informations et interagir avec ces équipements.

II. Principe et concept de SNMP :

2.1 Le protocole SNMP définit des échanges entre un client et un serveur afin de :

- Connaître l'état d'un appareil.
- Gérer les évènements exceptionnels.

- Mesurer le trafic et les erreurs à distance.
- Configurer les appareils à distance.

2.2 Le protocole SNMP a 4 principaux avantages :

- Il est simple et facile d'utilisation.
- Il implémente la gestion à distance.
- Il est indépendant des architectures.
- Il est très performant au niveau de gestion et de la surveillance des machines.

III. Configuration et règles de filtrage :

Il est possible d'affecter des règles de filtrage (Access-List) aux consultations SNMP. Ce filtrage offre un complément de sécurité car il permet d'autoriser une adresse IP ou un rang d'adresses IP à communiquer avec l'agent.

Voici un exemple de ce filtrage :

access-list	**1**	**permit**		**192.168.1.10**
access-list	**2**	**permit**		**192.168.1.20**
snmp-server	**community**	**public**	**RO**	**1**
snmp-server	**community**	**private**	**RW**	**2**

Le paramètre « snmp-server » défini et active le serveur SNMP. Après validation de cette commande, les informations SNMP sont accessibles.

La liste 1 définie les adresses IP ayant accès en lecture seule (Read Only - RO) aux informations diffusées sous le paramètre communauté « Publique ».

La liste 2 définie les adresses IP ayant accès en lecture / Ecriture (Read/Write - RW) à ces mêmes informations

IV. Commandes générique à SNMP :

- Activation du protocole SNMP

```
snmp enable
```

- Configuration du manager avec un délais d'expiration

```
snmp-server manager
snmp-server manager session-timeout 10000
```

- Création d'une communauté publique

```
snmp-server community name ro
```

- Création d'une communauté privée

```
snmp-server community name rw
```

- Désactivation de l'agent SNMP

```
no snmp-server
```

- Configuration de l'extinction d'équipement

```
snmp-server system-shutdown
```

- Configuration d'une requête trap :

```
snmp-server host host [traps | informs][version {1 | 2c | 3 [auth | noauth | priv]}
] community-string [udp-port port] [notification-type]
```

Exemple : snmp-server host 192.168.1.30 snmpv1 public bay-controller environment module

- Configuration d'un nouvel utilisateur

```
snmp-server user username [groupname remote ip-address [udp-port port] {v1 | v2c |
v3 [encrypted] [auth {md5 | sha} auth-password [priv des56 priv password]] [access
access-list]
```

Exemple : snmp-server user userone groupone v1

Exemple de commandes de configuration SNMP :

L'exemple suivant autorise l'adresse IP 192.168.1.1, puis active le protocole SNMP. Il autorise ensuite la lecture seule sur la communauté 1, et la lecture/écriture sur la communauté2, il nous spécifie que Mme. Hana est la personne à contacter en cas de problème et le localise à ESPRIT. Enfin il active la capture des requêtes SNMP, et la configuration de l'interface à capturer (loopback).

```
Lab-Snmp (config)#access-list 7 permit 192.168.1.1
Lab-Snmp (config)#snmp enable
Lab-Snmp (config)#snmp-server community community1 ro 7
Lab-Snmp (config)#snmp-server community community2 rw 7
Lab-Snmp (config)#snmp-server contact Hana (98 709 ***)
Lab-Snmp (config)#snmp-server location ESPRIT Tunis
Lab-Snmp (config)#snmp enable traps
Lab-Snmp (config)#snmp trap-source lo0
```

V. Utilité de SNMP au niveau du monitoring:

Grâce à toutes les alertes, nous pouvons nous rendre compte de la congestion réseaux, des saturations de bande passante, etc... Nous pouvons de plus modéré une trop forte utilisation du réseau, vérifier les états de fonctionnement des différents équipements ou serveurs ainsi que

toutes les autres entités du réseau et pour cela de nombreux logiciel comme Nagios, Cacti, nous propose une interface graphique très complète.

Exemple : Imaginons le cas d'une entreprise commerciale dont les revenus dépendent des activités de leur site Web. Une panne du serveur Web signifierait une perte de bénéfice pour l'entreprise, surtout si cette panne dure longtemps. Grâce au protocole SNMP et à son système d'alertes, l'administrateur réseau pourra accroître sa réactivité en cas de problème et réparer les serveurs ou équipements réseaux tombés en panne au plus vite. En effet, le SNMP pourra lui permettre de connaître pratiquement en temps réel l'état du réseau et lui permettre de le surveiller de la manière la plus efficiente possible.