Laboratoire de gestion des réseaux informatiques (GRX)

SNMP

**Auteur** : Sébastien Henrioud (modifié par Bastian Gardel)

**Professeur** : Stephan Robert

**Version** : 2.0/16.11.2016

**Groupe No**: \_\_\_\_\_\_\_\_\_

**Etudiants** : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Contenu

Délai 3

1 Introduction 3

2 Matériel 3

3 Topologie 4

4 Table d’adressage 4

5 Laboratoire 5

Objectif 1 : Construire le réseau et réaliser la configuration de base des équipements. 5

Objectif 2 : Configurer un « SNMP Manager » 5

Objectif 3 : Configurer différents agents SNMP 5

6 Exercices avancés 7

**Objectifs**

1. Construire le réseau et réaliser la configuration de base des équipements.
2. Configurer un « SNMP Manager ».
3. Configurer différents « SNMP Agents ».

##

## Délai et Consignes

Le fichier PDF du rapport contenant les réponses aux questions et la configuration des équipements doit être envoyé au professeur et à l’assistant **avant le début du prochain laboratoire**. Le rapport doit être rédigé de telle sorte à ce qu'un ingénieur qui ne connait pas la gestion des réseaux puisse refaire les expériences que vous avez menées sans autre documentation que celle de votre rapport. **Veuillez illustrer toutes vos manipulations avec des screenshots et des explications claires. Ajouter en annexe les configurations Cisco.**

# Introduction

Dans ce laboratoire, vous allez découvrir un deuxième protocole standard utilisé dans le cadre de la gestion et de la surveillance des équipements réseaux, le protocole SNMP qui est supporté par une grande majorité des équipements (switchs, routeurs, serveurs, modems, imprimantes, PCs). SNMP se présente sous la forme d’une collection de variables qui représentent la configuration du système de l’agent. Chaque variable peut être lue et même parfois écrite par le « SNMP Manager »

# Matériel

Chaque poste de travail est composé des éléments suivants :

* 1 poste de travail Dell 9010 avec :
	+ Win7 + Wireshark
* 1 Poste de travail Dell 9020
* 1 routeur Cisco
* 1 switch Cisco

# Topologie



# Table d’adressage

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Equipement | OS | Interface | Adresse IP | Masque de sous-réseau | Passerelle par défaut |
| R1 |  | G0/0 |  |  |  |
|  |  | G0/1 |  |  |  |
| S1 |  |  |  |  |  |
| Dell 9010 | Win7 | NIC |  |  |  |
| Dell 9020 | Win7 | NIC |  |  |  |

# Laboratoire

## Objectif 1 : Construire le réseau et réaliser la configuration de base des équipements.

* Câbler le réseau comme noté selon la topologie ci-dessus.
* Configurer les PCs.
* Réinitialiser le switch et le routeur si nécessaire
* Réaliser la configuration par défaut pour le routeur et le switch de sorte à ce que chaque équipement puisse pinguer n’importe quel autre élément (vérification de la connectivité). On peut relier le Dell 9010 à internet avec une carte réseau libre.
1. (1 pt) Remplir la table d’adressage (à joindre au rapport)

## Objectif 2 : Configurer un « SNMP Manager »

* (1 pt) Depuis le Dell 9010 avec Win7, télécharger et installer la console SNMPB depuis l’url suivante : <http://sourceforge.net/projects/snmpb/>
* Lancer le programme
* (1 pt) Contrôler que le host localhost existe déjà (vérifier que le community string est bien public)

## Objectif 3 : Configurer différents agents SNMP

Après l’installation de la partie serveur, il est temps d’installer 2-3 clients pour voir comment le protocole fonctionne.

* Activer l’agent SNMP Windows 7 sur le Dell 9010. C’est un service déjà disponible sur Win7, il suffit de l’activer et de le paramétrer correctement. Laissez le « community string » en mode RO avec la valeur par défaut public.
1. (1 pt) Montrer à l’aide de captures d’écran les changements de configuration que vous avez réalisés
* A l’aide du browser snmpb, interrogez le localhost.
1. (1 pt) Donnez 5 objets SNMP.
* Activer et configurez l’agent SNMP sur le Dell 9020 Laissez le « community string » en mode RO mais changez sa valeur « public » pour « publicD9020 ».
1. (1 pt) Que faut-il changer sur le Dell 9010 pour que ce dernier soit capable d’interroger l’agent SNMP du Dell 9020 ? (2 éléments)
2. (1 pt) A l’aide du browser SNMP (snmpb), interrogez le Dell 9020 et déterminez le nom de l’équipement, le nom du responsable de l’équipement, le modèle de l’équipement, son nombre d’interfaces et le trafic sur chacune des interfaces.
3. (1 pt) A l’aide de Wireshark, capturez et présentez de manière lisible les trames lorsque le Dell 9010 demande le nom de l’équipement du Dell 9020 (les champs concernant SNMP doivent être visibles et commentés)
* (1 pt) Configurez le routeur cisco de manière à pouvoir le gérer via SNMPv2. (choisissez « cisco » pour community string RO et « ciscorw » pour community string RW). Configuer le également pour qu’il envoie ses traps snmp au manager. N’oubliez pas de modifier la machine Win7 sur laquelle est installée snmpb pour que celui-ci connaisse aussi les nouveaux community string.
* (1 pt) Créez un nouveau profil dans snmpb pour le routeur en spécifiant notamment son adresse ip et ses deux « communities string ».
* Testez que le « manager SNMP » (snmpb) est capable d’interroger l’agent SNMP du routeur cisco.
* (1 pt) Trouvez un moyen de changer le nom du routeur depuis le PC Dell 9010 à l’aide du protocole SNMP.
* Changez le nom du routeur R1 pour « Router-<Your name> », capturez les trames échangées et analysez-les.
1. (1 pt) Que pouvez-vous dire sur la sécurité du protocole SNMPv2 ? Citez deux moyens d’améliorer la sécurité de notre infrastructure.
* Tout en capturant le trafic réseau, faites un « copy run start » sur le routeur. Vérifiez que vous récupérez bien la « SNMP trap » sur le manager snmpb.
1. (1 pt) Analysez les trames de la capture précédente et décodez la signification des différentes trames SNMP en recherchant la signification du « OID code » à l’aide de la MIB Cisco en cliquant sur le lien SNMP Object Navigator de la page suivante : <http://tools.cisco.com/ITDIT/MIBS/servlet/index>
2. (1 pt) Quelles commandes supplémentaires faut-il mettre en œuvre sur le routeur Cisco si vous voulez restreindre l’accès des requêtes à certains hosts (sur lesquels sont en général installés les managers) seulement (identifiés par leurs adresses IP) ? Configurer le routeur. (Pour illustrer que la nouvelle configuration fonctionne, vous pouvez installer le manager sur le Dell 9020)

* (1 pt) Configurez le deuxième équipement Cisco de manière à pouvoir l’interroger sur votre SNMP Manager et récupérer ses trap.

## Exercices avancés

* Vous pouvez essayer un autre outil : PowerSNMP (Manager gratuit).
1. (1 pt) Est-ce que le routeur ou le switch sont capables de faire du SNMPv3 ? Si oui, configurez-le sur un des deux équipements. Sinon expliquez pourquoi.