HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD

Laboratoire de gestion des réseaux informatiques (GRX)

SNMP

Professeur : Alain Bron

Assistant : Rémi Poulard

Version : 3.0

Objectifs

1. Configurer l'adressage des équipements.
2. Configurer un « SNMP Manager ».
3. Configurer différents « SNMP Agents ».
4. Récupérer des informations sur les équipements
5. Récupérer des alarmes
6. Observer le trafic
7.

Délai et Consignes

Le fichier PDF du rapport être envoyé au professeur et à l'assistant en principe **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.**

Notation

Le laboratoire compte au total 20 points
Note du laboratoire = (Nb points obtenus / 5) + 2
(1 de base + 1 de présence aux labos = 2)
Exemples :
20 points obtenus → +4 → note = 6
15 points obtenus → +3 → note = 5

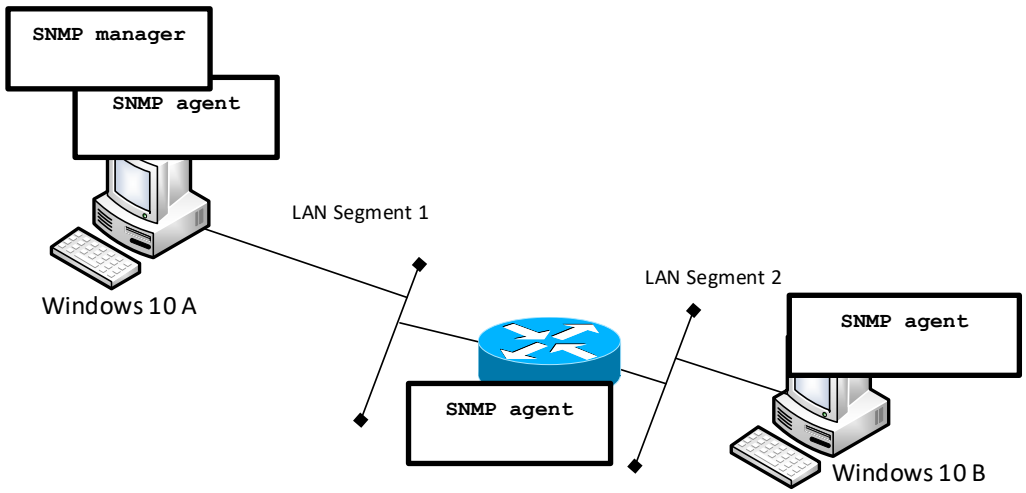
1 Introduction

Ce laboratoire permet la mise en œuvre du 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 d'objets/attributs constitutifs du système cible géré par un agent SNMP. Chaque objet peut être lu et/ou écrit par le « SNMP Manager » ou console SNMP.

2 Matériel

- L'infrastructure virtuelle est la même que celle utilisée pour le labo syslog. La VM Linux n'est pas utilisée dans le cadre de ce labo.

3 Topologie logique



4 Laboratoire (20 pts)

Objectif 1 : Configurer le réseau virtuel

- Configurez les PCs sous Windows 10
- Réinitialisez le routeur si nécessaire
- Réalisez 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).

Objectif 2 : Configurer un « SNMP Manager »

1. (1 pt) Installez et exécutez le manager /console SNMPb (http://sourceforge.net/projects/snmpb) sur la machine Windows 10 A
2. (1 pt) Contrôlez que le profile host localhost existe déjà (vérifiez que le community string est bien *public*) dans la liste des profils de l'application SNMPb

Objectif 3 : Configurer les agents SNMP en mode v2

Installer/configurer les agents SNMP.

- Activez l'agent SNMP sur la machine Windows 10 A. Le paramétrage s'effectue au niveau du service correspondant. Laissez le « community string » en mode RO avec la valeur par défaut *public*.

3. (1 pt) Montrez à l'aide de captures d'écran les changements de configuration que vous avez réalisés

- A l'aide du browser SNMPb, interrogez le localhost.

4. (1 pt) Donnez 5 objets SNMP de votre choix

- Activer et configurez l'agent SNMP sur la machine Windows 10 B en conservant le « community string » en mode RO mais en mettant sa valeur à « *not-public* ».

5. (1 pt) Que faut-il changer sur la machine Windows 10 A pour qu'elle soit capable d'interroger l'agent SNMP de la machine Windows 10 B ? (2 éléments)
6. (1 pt) A l'aide du browser SNMPb interrogez la machine Windows 10 B 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.
7. (1 pt) A l'aide de Wireshark, capturez et présentez de manière lisible les trames lorsque la machine Windows 10 A interroge la machine Windows 10 B pour obtenir le nom de l'équipement (les champs concernant SNMP doivent être visibles et commentés).

- Activer et configurez l'agent SNMP sur le routeur Cisco

8. (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). Configurez également le routeur pour qu'il envoie ses traps snmp au manager.

9. (1 pt) Créez un nouveau profil dans l'application SNMPb pour pouvoir gérer votre routeur.

10. (1 pt) Changez le nom du routeur à l'aide de l'application SNMPb (nouveau nom : *router-<votre-nom>*) tout en capturant/analysant les messages échangés à l'aide de Wireshark.

11. (1 pt) Que pouvez-vous dire sur la sécurité du protocole SNMPv2 ? Citez deux moyens d'améliorer la sécurité de notre infrastructure.

12. (1 pt) Générez une trap SNMP en déclenchant un événement sur votre routeur (un peu d'imagination...) et vérifiez que vous récupérez bien la « SNMP trap » sur l'application SNMPb.

13. (1 pt) Analysez les trames de la capture précédente et décodez la signification des différents messages SNMP en recherchant la signification du « OID code » à l'aide du *SNMP Object Navigator* Cisco https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index (compte Cisco à créer si nécessaire)

- Windows Powershell permet de créer des scripts, utiles pour récupérer des informations de manière régulière et automatisée par exemple.

  Installez sur la machine Windows 10 B le module `NetCmdlets`, qui contient des commandes SNMP permettant d'effectuer des requêtes SNMP :

  ```
  PS>Install-Module -Name NetCmdlets
  ```

14. (1 pt) Récupérez le nom de votre routeur à l'aide de la *cmdlet* adéquate.
15. (1 pt) Configurez le routeur de manière à ce qu'il n'accepte des requêtes SNMP que de la part de votre machine Windows 10 A uniquement. Validez votre configuration en vérifiant que votre machine Windows 10 B n'y a plus accès.

Objectif 4 : MIBs privées

- Afin d'interroger des objets spécifiques à votre équipement, vous avez besoin d'intégrer à votre manager SNMP (l'application SNMPb) les MIB privées nécessaires.

  Vous désirez obtenir des informations sur la mémoire flash embarquée sur votre routeur : chargez les MIBs privées nécessaires

16. (1 pt) donnez la liste des MIBs que vous avez chargé.
17. (1 pt) montrez le résultat obtenu en effectuant un requête depuis l'application SNMPb

Objectif 5 : Configurer les agents SNMP en mode v3

18. (1 pt) Modifiez la configuration de votre router afin qu'il n'accepte plus que des requête SNMPv3.
19. (1 pt) Configurez votre application SNMPb en conséquence et montrer le résultat d'une requête sur la valeur *SysUpTime* (MIB-2)
20. (1 pt) Capturez/analysez les messages lors d'une requête SNMP v3.