TP Gestion de réseaux

Antoine Laguette, Guillaume Tisserand, Juliette Bluem

23 septembre 2022

Partie I : Introduction

Dans ce TP nous sommes invité à découvrir le protocole SNMP ainsi qu'un logiciel NMS. Ces deux technologies vont nous permettre de gérer un réseau et dans sa finalité le superviser comme avec un logiciel de supervision de type Nagios. Durant ce TP nous découvrirons Zabbix. Pour commencer nous mettons en place et configurons une infrastructure réseau :

Matériel requis :

- Deux routeurs
- Un commutateur
- Deux hôtes
- 4 câbles RJ45

Topologie :

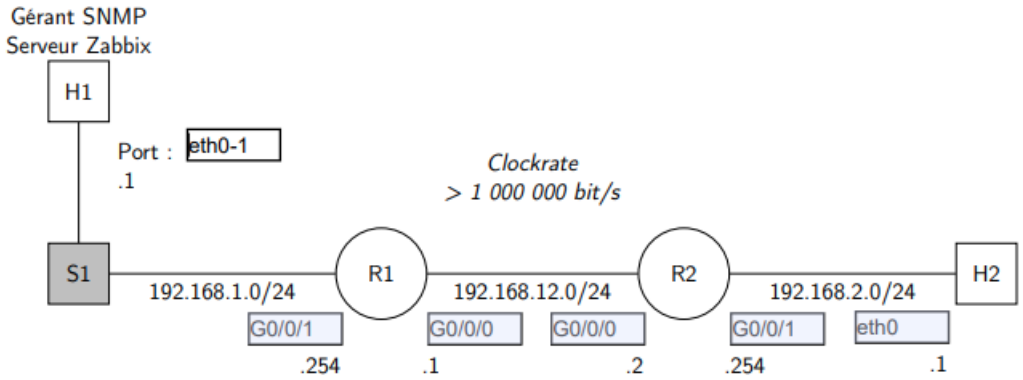

FIGURE 1 – Topologie préliminaire

Après plusieurs mois sans faire manipulations réseaux il nous a fallu un peu de temps pour nous remettre dans le bain ! En effet, nous avons dû passer du temps sur la mise en place de la configuration préliminaire. Mise en place de la topologie physique, adressage des hôtes et des ports des routeurs puis configuration des routes. Nous avons rencontré quelques difficultés au niveau des hôtes car nous utilisions nos ordinateurs personnels sous Windows 11 en tant que tel, nous verrons que la version d'OS a un impact pour la suite du TP. Les pare feux bloque les ping donc il a fallu les désactiver.

Nous vérifions que les hôtes communiques entre eux via des pings, tout fonctionne.

Partie II : SNMP

Pour rappel, SNMP (Simple Network Management Protocol) est un protocole de communication appartenant aux couches 7, 6 et 5 du modèle OSI. Ce protocole va permettre aux administrateurs réseaux de récupérer des informations via UDP sur l'état de leur réseaux, des liens et des équipement qui le composent dans le but d'apporter une supervision globale et un diagnostic rapide en cas de problème. Egalement il va nous permettre d'apporter des configurations (fonction limité) à certains équipements

La première étape de ce TP consiste donc à activer et configurer ce protocole sur notre infrastructure dans le but de le prendre en main d'identifier les informations que nous pouvons en tirer.

Pour se faire nous activons les agents SNMPv2 (il existe deux versions) en effectuant plusieurs opérations sur l'infrastructure :

- Vérification de l'écoute des agents sur les hôtes
- "Adressage" du du VLAN1 du switch
- Activation du service SNMP sur le commutateur et les deux routeurs

Une fois SNMP configuré nous pouvons commencer à récupérer des informations comme par exemple le temps d'activité d'un équipement. Ce temps peut nous permettre de savoir depuis quand l'équipement tourne et, éventuellement, déceler si ce dernier redémarre anormalement ce qui pourrait correspondre à une cyber-attaque ou bien un dysfonctionnement de ce dernier.

La requête se fait de cette manière :

```
┌──(root💀kali)-[~]
└─# snmpget -v 2c -c public  192.168.1.254 1.3.6.1.2.1.1.3.0
iso.3.6.1.2.1.1.3.0 = Timeticks: (1074530) 2:59:05.30
```

FIGURE 2 – Requête faite sur l'hôte 1

Pour aller plus loin nous observons une trame SNMP afin d'observer les informations échanger entre le superviseur et le réseau et identifier les informations qui peuvent circuler en clair. Nous utilisons doinc Wireshark pour effectuer une capture de trame.

FIGURE 3 – Trame SNMP via Wireshark

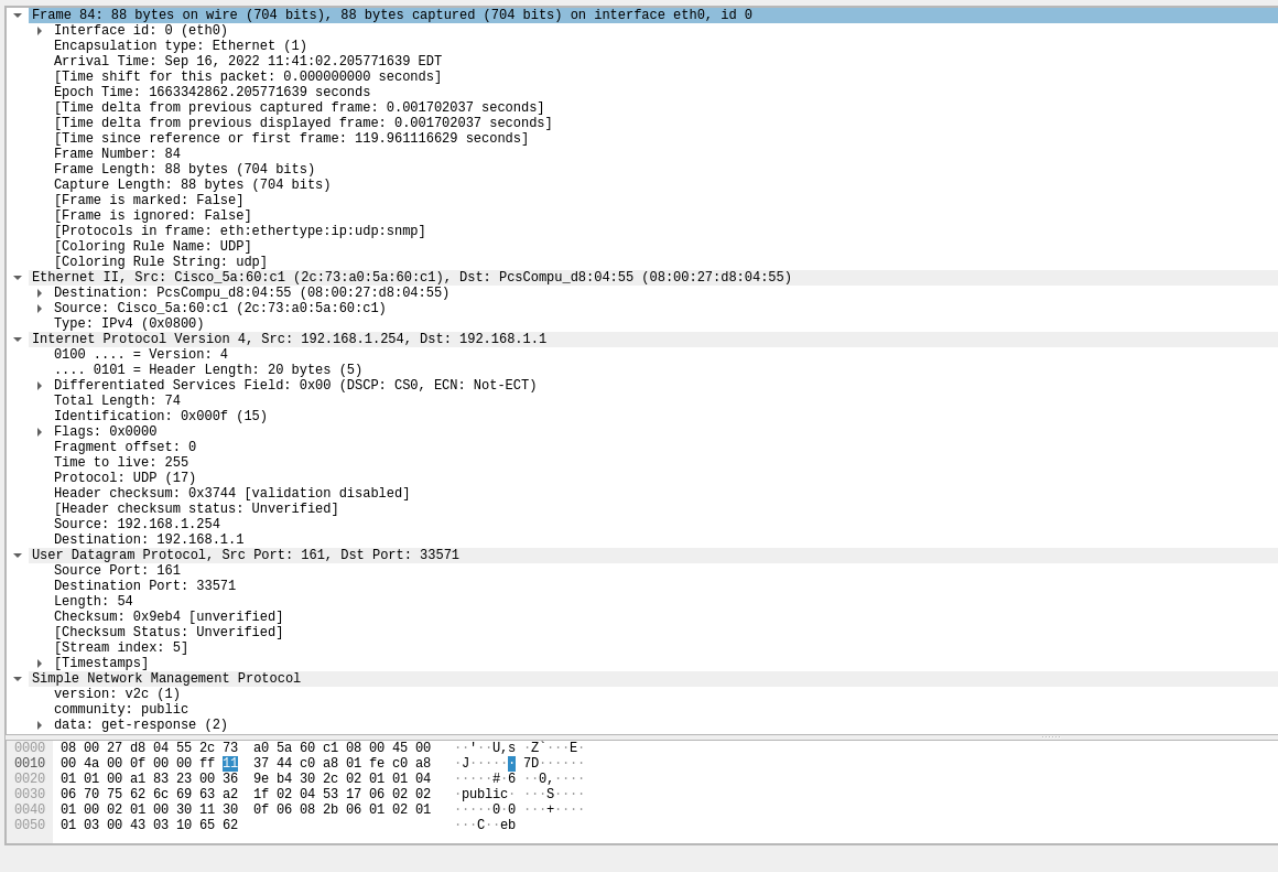

FIGURE 4 – Detail de la Trame SNMP

Le problème est que nous avions vraiment besoin d'une connexion internet en plus de celle sur le réseau que nous avions monté. En effet, plusieurs pluggins SNMP devaient être installés sur les hôtes. Il fallait donc jongler avec les réseaux, ce qui n'était pas des plus pratique. Nous pensons qu'il pourrait être intéressant de consacrer une petite partie sur dans l'installation préliminaire tant qu'une connexion à internet est possible.

Partie III : NMS

Malgrès nos efforts, nous n'avons pas pu atteindre cette partie. Néanmoins nous pouvons affirmer que NMS pour Network Management Station est une solution qui sollicite SNMP dans le but de centraliser les informations collecter sur un réseau.

Pour cette partie, nous n'avons pas eu le temps d'installer Zabbix sur un système linux afin de répondre aux questions et expérimenter la connexion entre Zabbix et un Hôte. Zabbix est un logiciel libre qui sert a des fins de supervision de type NMS, nous aurions utilisé le protocole SNMP afin de communiquer l'utilisation des ressources de l'ordinateur. Zabbix connaît dans sa bibliothèque l'OID de beaucoup de système, ainsi il est capable de chercher automatiquement les ressources qui l'intéresse afin de l'afficher sur une interface plus facile à interpréter.

Partie IV : Conclusion

Malgré les différents problèmes rencontrés de part de l'utilisation de machines non compatibles avec la connexion port COM pour configurer le matériel ou encore les problèmes de compatibilité de Windows 11 sur l'installation de SNMP et de Zabbix. Nous avons tout de même compris le protocole SNMP ainsi que l'arborescence des OID et le principe de fonctionnement d'un NMS sans pour autant l'avoir manipuler.