TP SNMP

Remarque : Ceci est un TP en évolution. Veuillez signaler les erreurs/ambiguïtés trouvées ou les améliorations possibles. Merci

Introduction – Construction et configuration de la plateforme

Le TP a pour but de collecter des informations par SNMP, et de découvrir le logiciel open source OpenNMS. Le TP a lieu sur une plateforme de 4 PC (spécialisés) et un Hub – Il y a au plus 6 plates-formes, de nom ***i*** = a à ***i*** = f, qui comprennent

- Un PC, tp-visu-i qui sert de station de supervision.
- Deux PC, tp-gena-i et tp-genb-i qui servent à créer du trafic
- Un PC, tp-rmon-i qui sert de sonde RMON-1 (Ethernet) grâce au logiciel Beholder
- Un HUB Allied Telesyn 36xxTR (agent SNMP, MIB HUB) –Attention : il a une adresse IP (tp-hub-i), et connait l'adresse de tp-visu-i. Son nom **définit** la plateforme. On utilise ce HUB pour que la sonde puisse voir tout le trafic, et pour étudier la MIB HUB.
- Vous avez aussi une copie papier des MIB II, REPEATER et BTNG. Elles sont à rendre en fin de TP.
  - Les MIBs pour le HUB sont la MIB HUB (SNMP-REPEATER-MIB) ET la MIB II.
  - Les MIBs pour la station sonde sont MIB RMON (BTNG) ET **une partie de** MIB II (l'implantation dans Beholder de MIB II est incomplète).
  - La MIB pour les trois autres stations est la MIB II.

Remarque : en fait les PC implantent aussi des MIB plus récentes; mais la MIB II est toujours supportée (compatibilité ascendante), et on l'utilise ici car elle est plus simple.

A noter :

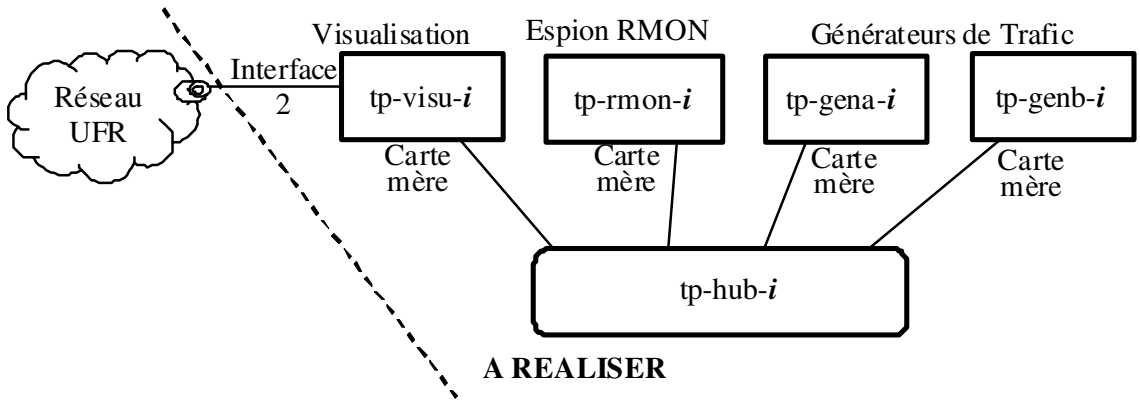
- Les communautés sont « `public` » pour les accès lecture et « `private` » pour les accès en RW.
- Les adresses IP sur la plateforme sont 192.168.C.D avec :
  - C=5 (resp. 6, 7, 8, 9, 10) pour la plateforme a (resp. b, c, d, e, f)
  - D=1 (resp. 2, 3, 4, 5) pour tp-visu-i (resp. tp-rmon-i, tp-gena-i, tp-genb-i, tp-hub-i).
  - **Ces adresses sont dans** l'/etc/hosts de vos machines, par exemple :

192.168.5.1 tp-visu-a
192.168.5.5 tp-hub-a
192.168.7.3 tp-gena-c
192.168.8.4 tp-genb-d

Remarque : les plateformes sont indépendantes et lors d'un TP ***il peut y en avoir plusieurs*** en avec le même nom. Le nom **est fixé** par celui du hub, qui est prédéfini.

Préliminaire
Mise en place de la plateforme

Réalisez le câblage suivant pour obtenir le réseau présenté ci-dessous pour la plateforme i :



PLATEFORME i

Montez la plateforme, allumez le HUB. Vérifiez le nom des machines (prompt login).

- il y a 4 machines/plateforme, soit 4 noms différents, **avec la même dernière lettre, la même que celle le hub**.
- Le PC tp-visu-i a sa deuxième interface (carte supplémentaire) configurée pour accéder au réseau UFR (www vers les docs), mais pas les autres PC.

Vérifiez la connectivité par les LED du HUB et par de pings.

Note : les Pc sont déjà configurés – S'il faut les reconfigurer, connectez vous en root et taper « `tp-snmp` *nom-de-la-machine* » (tp-visu-a, tp-genb-c, …)
En fin de TP : La configuration des PC est très spécifique. A la fin de la séance, il **faudra penser à exécuter la commande** « `/var/backups/BackToNormal` » pour remettre les PC dans un mode plus normal

A faire tout de suite après la construction de la plateforme :

La collecte de statistiques de opennms étant lente, il faut la lancer dès que possible :
Après avoir configuré les machines et **avant toute autre manipulation**, faire les 1 et 2 de la 2ème manipulation. Passez ensuite à la 1ère manipulation.
Il est aussi prudent de vérifier que tout c'est bien passé. Pour cela, 5 à 10 minutes après la configuration ci-dessus (point 2 de la 2ème manipulation), retournez dans opennms, aller dans le menu 'Node list' et vérifiez que les 5 machines de votre plateforme sont connues.

1ère Manipulation
Interrogation de matériel supportant la MIB II

Le but de cette manipulation est d'utiliser les possibilités de NET-SNMP pour montrer les différents objets de la MIB II. NET-SNMP est un des paquetages le plus courants pour consulter ***en commande mode ligne*** des matériels SNMP. Il existe plusieurs commandes (cf. les « man », et « man snmpcmd », « man variables » pour les options communes) :

- Récupérer des informations ; une seule requête (snmpget, snmpgetnext), ou requêtes multiples (snmpwalk, snmptable, snmpdelta).
- Modifier des variables SNMP (snmpset).
- Récupérer des informations pré-formatées (snmpdf, snmpnetstat, snmpstatus).
- Convertir des OID ou afficher des MIB (snmptranslate).
- Browser graphique Tk/perl (tkmib)

Options à connaitre : -v1 : utiliser SNMPv1 ; -c mycom : utiliser la communauté SNMPv1 'mycom' ; -Ou : format d'affichage des OID classique ; -On : OID numérique, -Os : format OID compact. Utiliser –Ou **est fortement conseillé**.
Pour snmpdelta –CT imprime les args en multi-colonne.
Défaut des commandes snmp* lors du TP : -v1 –c public
Par exemple : « `snmpwalk -Ou 127.0.01 ip`» liste les valeurs sous le nœud mib-2.ip de la machine locale.
Utilisez surtout les commandes ligne, sur tp-visu-i (mais vous pouvez tester tkmib).

Remarque : la commande « script TRACEX » lance un shell avec copie de tout l'affichage dans le fichier TRACEX, jusque l'exit du shell - cela peut remplacer avantageusement des copies d'écran. (Mais Attention : 1/ TRACEX est écrasé si on relance script. 2/ la copie de l'écran est complète, y compris les caractères de contrôle => ne faites pas de vi sous script !)

1. Récupération du contenu d'une variable ou d'une table de variables.
   - Lisez les variables du groupe "system" d'une entité réseau MIB II (Utiliser la commande snmpwalk). Quel type d'information récupérez-vous ? - Comparer avec ce que dit la MIB II (les OID, types, description ...)
   - Lisez la variable sysUpTime en utilisant snmpget puis snmpgetnext. Comparer les arguments et les résultats. Essayer aussi l'option -On – OID numérique.
   - Visualisez la table établissant la correspondance adresse IP - adresse MAC (Utiliser snmptable). Commentez.
   - Idem pour les configurations d'interface IP, ou les tables de routages IP. Comparer le résultat de snmptable, snmpnetstat et le netstat sur la machine
2. Récupérer de compteurs de trafic.
   - Trouvez plusieurs manières de lire le compteur de nombre d'octets IP reçus par tp-gena-i. Note : Il n'y a pas de solution exacte, choisissez celle qui semble la meilleure.
   - Surveillez ce compteur (utiliser snmpdelta) tout en générant du trafic tcp (cf. la description de ttcp/netperf en fin de ce document). Que constatez-vous ?
   - Afficher les compteurs octets IP reçus et émis pour tp-gena-i (utiliser snmpdelta avec option -CT). Comparer les valeurs. Est-ce que cela correspond à ce que vous savez de TCP ?
3. Snmpset permet de modifier des variables. Modifiez plusieurs variables du groupe système de tp-gena-i ou tp-genb-i. Effectuez une lecture, modifiez et enfin relisez. Trouvez les conditions pour que le set marche.

2ème Manipulation
Utilisation d'un système de gestion intégré

Note : Il existe peu de logiciels de gestion SNMP généraliste, surtout open source. On a choisit de montrer OpenNMS. Ce logiciel permet de détecter et de surveiller un parc sur différents réseaux, à long terme. Pour pouvoir faire un TP en quelques heures, il a fallu modifier la configuration et le programme pour réduire des périodes. De plus ceci est la première version du TP. Donc le document ou les choix peuvent être incorrects.

Note : La doc en ligne est sur www.opennms.org (attention on utilise une vieille version)

1. Sur tp-visu-i, vérifier que opennms est actif (sh /usr/local/etc/rc.d/opennms status). Puis lancer l'environnement graphique, firefox et connectez vous à la console sur http://localhost:8980/opennms ; login : admin ; password : admin
2. Il faut que la station connaisse les matériels à surveiller. Normalement on déclare les plages IP à surveiller (menu Admin/Discovery), et opennms les scanne. Mais comme le scan est à bas débit, nous allons déclarer les machines à la main : pour les 5 **adresses IP** de la plateforme, allez dans Admin/Nodes/Add Interface et ajoutez l'adresse IP.
3. Vérifiez la « Node list », regardez quelles informations ont été détectées (cela peut prendre un peu de temps). Vous pouvez surveiller l'avancement dans 'Events'.
4. Regardez les menus principaux, imaginez comment les infos peuvent servir à connaitre l'état du site.
   Note : Je vous serais très reconnaissant si vous me suggériez des questions de TP plus ciblées !
5. Essayez de tracer des rapports de trafic. Note : La durée entre deux interrogations est très longue par défaut, et la période minimale de 1 jour. Le logiciel de vos plateformes à été modifié pour interroger SNMP toutes les secondes et de proposer des graphes de durée 5 ou 15 minutes.

Note : Pour faire des copies d'écran d'OpenNMS, xfce propose un outil de copie d'écran. On peut aussi utiliser un menu interne de Firefox : taper Maj-F2, puis « screenshot *fichier* » (cf help screenshot). Il existe aussi des plugins de capture dans le catalogue Firefox (non installés), par exemple Abduction, Screengrab, … qui créent des images, souvent de .png (visibles en les ouvrant directement dans Firefox) - attention beaucoup de plugins sont incompatibles avec votre Firefox/FreeBSD. On peut aussi utiliser un téléphone portable si on préfère ☺

3ème Manipulation
Interrogation de matériel supportant la MIB HUB

Le but de cette manipulation est de montrer les possibilités offertes par un matériel supportant cette MIB (cf. document MIB HUB fourni).

1. Découvrez la structure de votre HUB (Nombre de ports RJ45, Nombre de cartes présentes sur le HUB, Nombre de Ports Actifs, ...), en utilisant la mib HUB et les commandes snmp*.

2. Note : Pour cette question l'idéal serait de faire des graphes mais je n'ai pas trouvé de logiciel simple – ou le bon menu de openNMS.. Donc utilisez snmpdelta.

   Réalisez un même affichage permettant d'observer pour chaque entité raccordée sur ce HUB, le nombre d'octets reçus ou émis (groupe RptrMonitorPortTable)
   Générez maintenant du trafic entre les différents éléments de la plateforme. Que constatez-vous ? (granularité des mises à jour, variables disponibles …)

   Ajouter un tracé regroupant le nombre de collision pour les mêmes entités.

3. La MIB HUB possède des possibilités d'invalidation par logiciel des ports du HUB.

   Choisissez une des machines générateurs de trafic et repérer son numéro de port sur le HUB. Coupez de manière logicielle ce port et vérifier que cette station est bien isolée du reste de la plateforme.

   Revalidez le port pour la suite du TP et **vérifiez** le bon fonctionnement du port.

Remarque : Il convient de ne pas invalider l'ensemble des ports du HUB, sinon celui ci ne sera plus accessible via le réseau, donc non reconfigurable par SNMP.

4. Il est possible de programmer le HUB pour que des TRAPS soient émis vers la station d'administration. Ceci a déjà été effectué lors de la configuration du hub 36xxTR.

   Cherchez dans la MIB HUB un trap que vous pouvez générer, provoquez en et observez les "Traps Reports" récupérés par OpenNMS (dans la liste des events du node : ce n'est pas forcément classé comme alarme pour OpenNMS). On peut aussi observer un trap coldStart (ou warmStart), qui n'est pas spécifique au hub en rallumant le hub.

4ème Manipulation (optionnelle, pas pour les TP de 3h)
Vers une analyse réseau plus fine - RMON MIB

Remarque : cette partie est pour mémoire, pas encore modifiée pour le TP version 2010.

Le but de cette manipulation est d'illustrer quelques unes des nombreuses possibilités offertes par les agents supportant la MIB RMON.

1. Interprétation de tracés

- Réalisez deux tracés simultanés :
  - l'un représentant le nombre d'octets collectés par l'agent RMON,
  - l'autre le nombre d'octets reçus et émis par l'agent MIB II du générateur1.
- Générez du trafic à partir du générateur 2 vers le générateur 1.
- Générez ensuite du trafic du générateur 1 vers le générateur 2.

Que constatez-vous ?

2. Détection d'un réseau encombré

- Gardez le tracé nombre d'octets collectés par l'agent RMON
- Créez un nouveau tracé représentant le nombre de collisions détectées par l'agent RMON.
- Générez du trafic du générateur 1 vers le générateur 2, et simultanément du générateur 2 vers le générateur 1.

  Que remarquez-vous ? Faites un rapprochement avec les informations affichées et/ou collectées par SNMP sur le HUB ?

3. La RMON MIB permet d'obtenir la distribution des paquets présents sur le câble en fonction de leur taille.

- Réalisez un tracé regroupant cette distribution.
- Générer à l'aide de l'utilitaire ping des paquets ICMP de taille variable entre les deux stations générateurs.
- Vérifier l'impact de ce trafic sur les différents compteurs.
- Quelle analyse peut-on faire selon vous suivant la taille de paquets et des applications TCP/IP que vous connaissez (telnet, ftp, nfs, ...) ? Pour affiner votre analyse, générez du trafic ftp en transférant quelques gros fichiers via la commande ftp entre gena-i et genb-i, et du trafic telnet en vous connectant de gena-i vers genb-i.

4. En utilisant le contenu des tables Host et Matrix nous pouvons quantifier le trafic par machine et le dialogue entre les couples de machine. Pour observer cette possibilité, générer du trafic de la station visu-i vers la station gena-i, et la station genb-i vers la même station gena-i.

5. En utilisant le groupe HostTopN, qu'il convient d'activer sur l'agent RMON, réaliser les mêmes opérations que ci-dessus, et réaliser un classement des machines les plus bavardes en émission (respectivement en réception) sur le réseau de votre plateforme.

6. En utilisant, les possibilités de l'agent RMON, réalisez une mesure du degré d'utilisation de la bande passante du réseau et comparer la avec les indications fournies par NetPerf.

Outils utilisés lors du TP SNMP

`ttcp` est un générateur de trafic qui permet de calculer le débit en TCP. Il faut 2 appels, un en mode serveur (réception) sur une machine, l'autre en mode émission sur une autre machine.

- Mode réception : *ttcp –rs* (attente d'une connexion) ou
  sh –c "while :; do ttcp –rs ; done" (boucle infinie)
- Mode émission : *ttcp –ts [-n 1000000] [-l 4096]* machine
  -n 100000 envoie 100000 buffers (défaut 2048)
  -l 4096 utilise un buffer de 2ko (défaut 8ko)
- help : *ttcp*

`netperf` est un utilitaire qui permet de calculer le débit utile d'une communication (en flux TCP unidirectionnel par défaut, mais aussi UDP ou transactionnel). netperf a beaucoup d'options, utiliser *netperf –h* pour les voir.
Il faut 2 programmes, serveur (récepteur) sur une machine, client (émetteur) sur les autres machines.

- serveur : *netserver* (boucle infinie, attente de clients)
- client : *netperf [-l 300] –H* machine
  -l 300 envoie pendant 300 secondes
- help : *netperf -h*

`tcpmt/tcptarget/udpmt/udptarget` est un ensemble d'utilitaires qui permet de calculer le débit utile d'une communication. tcptarget/udptarget sont les récepteurs, tcpmt/udpmt les émetteurs.

- serveur : *tcptarget* (attente d'une connexion)
  sh –c "while :; do tcptarget ; done" (boucle infinie)
- client : *tcpmt [-d 300]* machine
  -d 300 envoie pendant 300 secondes
- help : *tcptarget -h* ET *tcpmt -h*

Ipmt/$ tcptarget

```
IPv6 (and IPv4) protocol
Using port 13000
    1.000 2882924.6
    2.000 2637552.7
    3.000 2636768.7
```

....

Ipmt/$ udpmt localhost

```
IPv4 protocol
Time         Packets    Total       | Kbit/s     Avg 10     Avg
41605.879     246664  246664        | 2881036    2881036    2881036
41606.879     225815  472479        | 2637474    2759254    2759254
41607.879     225758  698237        | 2636896    2718468    2718468
41608.879     225766  924003        | 2636907    2698078    2698078
```

....