TP2 LAN

Objectifs

Maîtriser certains des concepts, des protocoles et des technologies rencontrés sur les réseaux locaux (LAN) et en particulier :

- commutation et sécurisation des interfaces ethernet
- spanning tree
- bridges virtuels
- VLAN
- port mirroring
- agrégation de liens
- SNMP

Consignes

Pour ce TP et les suivants, vous répondrez aux questions en indiquant, autant que possible, le raisonnement qui vous a mené à la solution, et vous noterez la procédure mise en place (liste de commandes, schémas, etc.) lors de vos manipulations.

Ne restez jamais bloqué plus de 10 minutes avant de demander de l'aide à votre enseignant.

Lorsqu'il s'agira de modifier la configuration d'un équipement réseau, il ne faudra **en aucun cas lancer les commandes « copy running-config startup-config » ou « write memory »**.

Répartissez-vous en trinômes. Chaque trinôme doit disposer de 3 postes de travail, si possible connectés à la même baie de brassage.
S'il n'y a pas suffisamment de postes fixes dans la salle, certains trinômes utiliseront 2 postes fixes + 1 ordinateur portable.

1 Commutation

Avant toute manipulation, désactivez le protocole spanning-tree (qui sera traité plus loin) sur les switches que vous utiliserez :

```
Switch(config)#no spanning-tree vlan 1
```

1) - Affectez une adresse IP à l'une des interfaces ethernet de 3 postes A, B et C et connectez-les à un même commutateur.
- Échangez des données entre ces 3 postes (ping).
- Consultez la table d'acheminement (appelée aussi table de commutation ou table d'adresses MAC) (*show mac-address-table*) et vérifiez qu'elle s'est dynamiquement alimentée.
- Envoyez en continu des requêtes d'écho ICMP (ping) uniquement de A vers B.
- Lancez une capture de trames sur C avec *wireshark*. C reçoit-il les messages ICMP envoyés en unicast de A vers B ?
- Laissez tourner les pings de A vers B et la capture sur C. Affichez la table d'acheminement du switch juste après avoir déconnecté B. Que constatez-vous ?
- Analysez la capture de trames. C reçoit-il les messages ICMP envoyés en unicast de A vers B ? Déduisez-en le comportement d'un commutateur lorsqu'il reçoit une trame destinée à une adresse

qui ne figure pas dans sa table de commutation.

2) - Notez l'adresse MAC de C et remplacez-là par celle de B, de manière à ce que B et C aient la même adresse matérielle (utilisez la commande *ifconfig* ou *ip link*).
- Si elle est encore présente, ôtez du cache ARP de A l'entrée correspondant à l'ancienne adresse MAC de C en utilisant la commande *ip neighbor* ou *arp*).
- Lancez simultanément des échanges de pings entre A et B et entre A et C.
- Affichez la table de commutation (aussi appelée table CAM sur les switches Cisco, pour Content Addressable Memory). Que constatez-vous ?
- Tentez ensuite d'y ajouter 2 entrées statiques pour cette adresse MAC (uniquement si votre switch n'est pas un 3500XL). Que constatez-vous ?
- Reconfigurez l'ancienne adresse MAC de C.

3) - Connectez C à un 2ème switch et interconnectez les 2 switches.
- Lancez des pings entre A et C et entre B et C.
- Affichez les tables de commutation des deux switches.
- Que constatez-vous au niveau du port du 2ème switch connecté au 1er ?
- Reconnectez de nouveau les postes sur le même switch.

2 Sécurisation des ports

Imaginez ce qui peut se produire si un poste envoie en permanence des trames dont l'adresse MAC source est à chaque fois différente.

1) Pour parer à ce type de problème, il existe des mécanismes de sécurité.
Utilisez les options des commandes « port security » et/ou « switchport port-security » pour limiter à 1 le nombre maximum d'adresses MAC associées au port relié à A.
Lancez un ping vers A et affichez la table d'acheminement.
Aidez-vous de la commande *show port security* (3500XL) ou *show port-security* (2550 et 2560) pour les questions qui suivent.
Connectez A sur un autre port et tentez de le pinguer. Que se passe-t-il ?
Connectez B au port sécurisé et tentez de le pinguer depuis C. Que se passe-t-il ?
Si vous disposez d'un switch 2950 et 2960, essayez également le mode *sticky* (collant).

2) Utilisez la commande *ifconfig* ou *ip link* pour remplacer l'adresse MAC de B par celle de A.
Tentez de nouveau de pinguer B. Qu'en déduisez-vous quant à la capacité de cette technique à sélectionner les postes autorisés à se connecter au réseau ?
Comparez avec les groupes voisins le comportement des switches selon qu'ils sont plus anciens (3500xl) ou plus récents (2550 et 2560).
Désactivez la sécurisation par limite d'adresses MAC et supprimer les adresses de type "secure" de la table de commutation.

3) Comment sécuriser une série (*range*) de ports sans relancer les commandes pour chaque port individuellement (uniquement sur les switches 2550 ou 2960).

3 Boucles de commutation

Si ce n'est pas déjà fait (*show spanning-tree*), désactivez STP sur vos 2 switches (qu'on appellera S1

et S2) par la commande :
```
Switch(config)#no spanning-tree [vlan 1]
```

1) Connectez un poste A au switch S1.
Connectez le switch S1 au switch S2 par deux câbles.
Sur le poste A, lancez une capture de trames et envoyez une unique requête d'écho ICMP (option -c de ping) en diffusion générale.
Quel phénomène constatez-vous ? Quelle en est la cause.

2) Hormis le broadcast, quels types de trafic peuvent, selon vous, conduire à des boucles de commutation ?

3) Déconnectez l'une des interfaces, arrêtez la capture et affichez les statistiques pour noter le nombre de paquets/s capturés.
Configurez la fonctionnalité de contrôle de tempête (*storm control*) de manière à limiter le trafic de broadcast à 1000 paquets/s.
Appliquez le filtre sur l'une des 4 interfaces impliquées dans la boucle suffit-il pour l'interrompre totalement ? Pourquoi ? Pour répondre, consultez la table de commutation.
Quelles sont, au minimum, les interfaces à filtrer pour interrompre la tempête ?

4) Quel problème peut poser le *storm control* sur un réseau de production ?

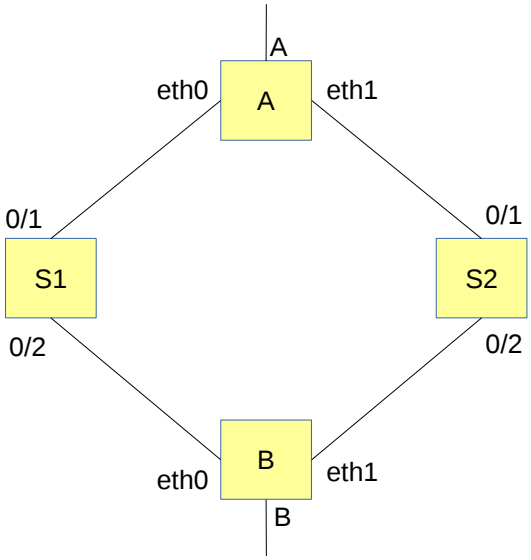
Désactivez les filtres et connectez les 2 switches par un unique lien.

4 Bridge Linux

Il sera utile par la suite de transformer un poste de travail en un commutateur (ou un pont, c'est-à-dire un commutateur à 2 ports).
Utilisez la commande *brctl* sur A pour :
- créer un bridge que vous nommerez A
- associer 2 des interfaces ethernet de votre poste à ce bridge, après avoir déconfiguré leur adresse IP

Attribuez une adresse IP à l'interface A (qui est une interface virtuelle connectée au pont A).
Connectez B et C sur A (attention au type de câble…) et vérifiez que A, B et C peuvent communiquer entre eux.
Déconnectez B et C et connectez S1 et S2 à A.

Transformez également B en pont et connectez-le à S1 et S2, comme sur la figure qui suit.



5 Arbre recouvrant

Il existe un moyen de résoudre intelligemment le problème de la tempête de diffusion (*broadcast storm*).

- Lancez des captures de trames sur les interfaces eth0 et eth1 de A et B.
- Activez STP sur A, B, S1 et S2.
- Utilisez la commande *brctl showstp* avec la commande *watch* pour afficher l'évolution de la configuration STP sur A et B.
- Lancez la commande *debug spanning-tree events* sur les commutateurs Cisco Catalyst.

1) Comme tout arbre, notre arbre recouvrant (spanning tree) a une racine. D'après les commandes *brctl showstp* (Linux) et *show spanning*-tree (Cisco), quel pont a été désigné "racine" de l'arbre ?

2) Environ 30 secondes après avoir activé STP sur tous les ponts, la topologie est stabilisée. Les messages du protocole Spanning Tree émis par les commutateurs sont appelés BPDU (Bridge Protocol Data Unit). Quelle est la fréquence de transmission de ces messages (*hello time*) ?

3) Quelles sont les adresses sources des trames qui véhiculent ces BPDU. Déduisez-en les ports qui émettent et les ports qui reçoivent les BPDU.
Les ports qui émettent les BPDU sont appelés *ports désignés*.
Les ports désignés sont dans l'état *forwarding*. Autrement dit ces ports sont actifs.

4) Quelle est l'adresse de destination des trames qui transportent les BPDU ? Quelle est la particularité de cette adresse ? Ces trames sont-elles diffusées sur l'ensemble du domaine de diffusion ethernet ?

5.1 Choix du pont racine

1) Augmentez la valeur de priorité du pont racine et observez l'évolution du contenu des BPDU et des valeurs reportées par les ponts (*flags*, *timers*, *port state*). Un autre pont est devenu la racine de l'arbre.

2) Si tous les ponts ont la même priorité, comment le pont racine est-il désigné ?

3) Utilisez la méthode précédente pour faire en sorte que le pont S1 soit forcé à devenir la racine. Pourquoi un administrateur réseau voudrait-il définir lui-même la racine de l'arbre recouvrant ?

Lorsqu'un pont détecte une modification de topologie, il envoie vers la racine un BPDU de type "*topology change notification*". Le pont racine ajoute alors un drapeau "*topology change advertisement*" à tous les BPDU qu'il envoie pendant un certain délai. Ces BPDU sont propagés de nœud en nœud sur les branches de l'arbre.

5.2 Choix des ports racines

1) Diminuez légèrement la valeur de la priorité du pont connecté au port qui est dans l'état bloqué (la priorité de ce pont doit rester supérieure à celle du pont racine). Quels sont les différents états pris par ce port pendant les secondes qui suivent le changement de topologie ? Au bout de 30 secondes environ, quel est le résultat du changement de topologie ?

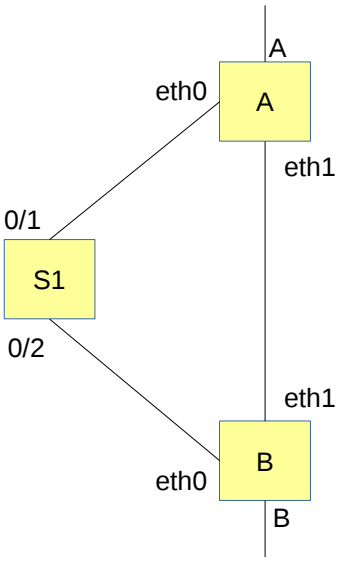
2) Sur S2, diminuez la vitesse (*speed*) de ce port. Que ce passe-t-il au bout de 30 secondes ?

Une fois le pont racine élu, chaque pont non racine détermine quel est le port qui permet d'atteindre la racine de la façon la plus rapide. Ce port est appelé "port racine" et placé dans l'état *forwarding*.

3) Comparez les BPDU envoyées à S2 par A et celles envoyées à S2 par B. Quels éléments de ces BPDU permettent-ils de choisir le port racine ? Ces éléments sont-ils les seuls à être pris en compte par S2 lors du choix du port racine ? Quel élément a le plus de poids lors du processus de choix du port racine ?

5.3 Choix des ports désignés

1) Désactivez STP sur S2.
Sur A, quelle est l'adresse source des trames contenant les BPDU reçus sur eth1 ?
Sur B, quelle est l'adresse source des trames contenant les BPDU reçus sur eth1 ?
Vous pouvez constater que S2 ne participe plus au protocole Spanning Tree.
S2 émet-il des BPDU ?
Que fait S2 des BPDU provenant de A et de B ?



2) Affectez au pont B une priorité d'une valeur supérieure à celle de A et de S1 et comparez les BPDU envoyés de A vers B et de B vers A au moment de cette modification.
Quel est l'état des ports eth1 sur A et B après un délai de 30 secondes ?

Sur chaque liaison, le port désigné est celui qui permet d'atteindre la racine de la façon la plus rapide.

3) Diminuez la vitesse du lien S1-A et analyser les BPDU envoyé par S1, A et B au moment du changement. Quel est l'état des ports eth1 sur A et B après un délai de 30 secondes ?

4) Quelle est la nouvelle valeur du coût du chemin vers la racine (*root path cost*) annoncé par A ? Quel paramètre a le plus de poids lors du processus de choix du port désigné ? Quel autre paramètre est utilisé an cas d'égalité du premier ?

5) Chaque pont non racine compare les BPDU qu'il envoie avec ceux qu'il reçoit sur chaque port non racine.
Si les BPDU qu'il envoie sont "meilleures" que celles qu'il reçoit, alors le port est dit "désigné" et il est placé dans l'état *forwarding*.
Si les BPDU qu'il reçoit sont "meilleures" que celles qu'il envoie, alors le port est mis dans l'état *blocking*.

6) Quel est l'intérêt et/ou l'inconvénient d'activer STP sur les liens connectés à des postes de travail ?

7) Quel peut être l'utilité de maintenir volontairement des boucles physiques sur un réseau où STP est actif ?

8) Pour conclure sur STP, quels sont les 2 gros avantages qu'offre ce protocole en bloquant automatiquement les boucles ?

6 Isolation des échanges

1) Connectez A au port 1, B au port 2 et C au port 3 d'un switch.

Appliquez la commande « port protected » ou « switchport protected » aux ports 1 et 2.
Envoyez une requête d'écho ICMP de A vers B, puis de A vers C. Que constatez-vous ?
Lancez une requête d'écho ICMP en diffusion générale (broadcast) à partir de A. Que constatez-vous ?
Quel est l'intérêt des ports « protégés » ?

2) Connectez maintenant B sur le port 2 d'un autre switch, « protégez » ce port et pinguez de nouveau B depuis A. Que constatez-vous ?

7 VLAN

Avant de commencer cette partie, exécutez la commande suivante sur les 2 switches que vous utiliserez :
`delete flash:vlan.dat`

A et B sont les postes de simples employés qui doivent être isolés des postes C et D, ceux du grand chef et de sa secrétaire.
A est connecté au port 1, B au port 2, C au port 3 et D au port 4 d'un commutateur.
Tous les postes ont des adresses du réseau 10.0.0.0/8.

1) Utilisez la commande *switchport access ...* pour associer A et B au VLAN 2 et C et D au VLAN 3. Nommez le VLAN2 « atelier » et le VLAN3 « direction ».
Qui reçoit un ping en diffusion générale émis par A ?
Qui reçoit un ping en diffusion générale émis par C ?

2) Affichez la table de commutation. Quel est l'intérêt d'associer les entrées de cette table à des numéros de VLAN ?

3) Les bureaux de l'entreprise sont répartis de manière à ce que :
- A et C sont reliés sur les ports 1 et 2 du switch S1
- B et D sont reliés sur les ports 1 et 2 du switch S2
Proposez et mettez en place une solution basique (avec 2 câbles) pour que les employés puissent communiquer ensemble, et le patron avec sa secrétaire.

8 Trunk

1) Les deux switches de l'entreprise se trouvent dans deux bâtiments différents et sont reliés par un unique lien en fibre optique. De plus, le service compta, le service commercial, le service après-vente, etc. souhaiteront eux aussi, par la suite, être dans leur propre réseau isolé.
Configurez un *trunk* entre les deux switches avec la commande *switchport mode*.

2) Intercalez un hub (concentrateur) entre S1 et S2 et connectez une sonde sur ce hub, c'est-à-dire un poste sur lequel vous lancez une capture de trames en mode *promiscuous*.
Echangez des messages ICMP entre A et B et entre C et D. Comparez les paquets capturés sur le trunk et les paquets envoyés ou reçus par les postes. Déduisez-en la manière dont les switches différencient les trames du VLAN 2 et les trames du VLAN 3 qui circulent sur le trunk.

3) Quelle est la taille du champ *identifiant de VLAN* ? Déduisez-en le nombre maximum de VLAN configurables (en théorie) sur un réseau.

4) Le protocole ISL est un protocole désuet et propriétaire Cisco. Remplacez le protocole ISL (utilisé par défaut sur le trunk des switches les moins récents) par le standard actuel (IEEE 802.1Q) en utilisant la commande *switchport trunk*.
Que se passe-t-il si les protocoles configurés aux extrémités du trunk sont différents ?

5) Utilisez la commande *switchport trunk* pour indiquer aux switches S1 et S2 que le VLAN 2 est le VLAN *natif*. Capturez de nouveau quelques échanges entre A et B. Que constatez-vous ?
Lancez des pings en broadcast. Les VLAN 1 et 2 sont-ils toujours isolés l'un de l'autre ?
Peut-on avoir plusieurs VLAN natifs sur le même trunk ?
Le VLAN natif est utilisé par certains protocoles de signalisation, comme CDP (Cisco Discovery Protocol) ou DTP (Dynamic Trunking Protocol).

6) Le bureau de la secrétaire a changé de bâtiment. Déconnectez D de S2 et remettez le port 2 de S2 dans le VLAN par défaut (le VLAN 1).
Depuis C, lancez un ping en diffusion générale après avoir lancé une capture sur la sonde.
Que constatez-vous ? Le trunk transmet-il les trames envoyées sur le VLAN 3 ? Quel problème ce comportement peut-il poser sur un grand réseau ? Vous verrez dans le chapitre qui suit qu'un mécanisme lié au protocole VTP peut résoudre ce problème.

7) Les switches récents (2550 et 2560) offrent la possibilité de négocier avec l'équipement distant le mode dans lequel se trouve un port (*trunk* ou *access*). Cette possibilité repose sur le protocole DTP (Dynamic Trunking Protocol), activé avec la commande *switchport mode dynamic*. Quel est l'intérêt de ce protocole ?
En matière de sécurité informatique, et quelles que soient les circonstances, on ne peut pas faire confiance aux postes de travail des utilisateurs. Dans ces conditions, quel problème peut poser le protocole DTP ?

9 Surveillance de port

Les commutateurs Cisco offrent une fonctionnalité appelée Switch Port Analyzer (SPAN).
Si vous avez accès à un switch Cisco Catalyst 2950 ou 2960, utilisez la commande *port monitor* ou *monitor session* pour recopier tout le trafic circulant sur le trunk vers un port sur lequel vous connecterez votre sonde. L'entête 802.1Q des paquets doit être conservée lors de leur recopie vers la sonde. Le SPAN rend ainsi le hub inutile.

Si vous utilisez des switches Cisco Catalyst 3500xl, alors utilisez la commande *port monitor* pour recopier tout le trafic circulant sur le vlan 2 vers un port sur lequel vous connecterez votre sonde.

10 VTP

VTP (VLAN Trunking Protocol) est un protocole propriétaire Cisco qui permet de faciliter l'administration des VLAN.

1) Configurez S1 en mode serveur et S2 en mode client.
Affichez la liste des VLAN sur S1 et de nouveau, depuis C, lancez un ping en diffusion générale après avoir lancé une capture sur la sonde.
Que constatez-vous ? Le trunk transmet-il les trames envoyées sur le VLAN3 ? Pourquoi ?
Que transportent les paquets VTP ? Sur quel lien sont transmis ces paquets ?

Tentez de créer un VLAN sur S2. Que se passe-t-il ? Est-ce normal ?

2) Ajoutez un VLAN sur S1 et observez la modification du numéro de séquence des annonces VTP.
Mettez maintenant S2 en mode *server* et ajoutez un autre VLAN. Que se passe-t-il ?
Réfléchissez au problème de sécurité que pose ce protocole.

3) Quel problème pose le fait que VTP soit un protocole propriétaire ?

Lorsque VTP est actif (mode *client* ou *server*), seuls les VLAN 1 à 1005 peuvent être utilisés.

11 Routage inter-vlan

Utilisez un routeur pour réaliser le routage entre les VLAN 2 et 3.
Pour cela, connectez un lien trunk entre l'un des deux switches et le routeur, et sur le routeur, configurez des interfaces virtuelles associées aux VLAN.

Les trames 802.1Q peuvent-elles passer « à travers » les routeurs (d'un réseau à un autre) ?

12 Trunk et serveur

1) Scénario : un hyperviseur héberge des serveurs virtuels qui doivent être connectés à des réseaux différents. Votre poste de travail symbolise l'hyperviseur.
Aidez-vous de la commande *vconfig* pour configurer un *trunk* entre S2 et votre poste, sur lequel une interface virtuelle sera connectée au VLAN 2 et une autre interface sera connectée au VLAN 3.
Le module du noyau Linux qui gère le protocole 802.1Q, nommé « 8021q », est préchargé sur vos postes.
Vérifiez que vous pouvez joindre votre voisin, lui aussi connecté au VLAN 2 et 3 via un *trunk*.

3) L'administrateur du réseau ne souhaite pas, pour des raisons évidentes de sécurité, que les serveurs puissent accéder à tous les VLAN du réseau.
Limitez leur accès au seul VLAN2 en utilisant la commande *switchport trunk*.

4) Les annonces VTP sont-elles reçues par votre poste ?
Configurez S2 en mode transparent. Transmet-il toujours les annonces à votre poste ?
Ajoutez un VLAN sur S1. Est-il pris en compte par S2 ?
Ajoutez un VLAN sur S2 et affichez la configuration courante (running-config). Que constatez-vous ?
Supprimez maintenant le fichier *flash:vlan.dat* sur S2. Affichez la liste des VLAN (*show vlan brief*). Que constatez-vous ?
Où se trouvent stockés les VLAN appris par VTP ?
Où se trouvent stockés les VLAN configurés lorsque VTP est désactivé ?

13 Agrégation de liens

13.1 Etherchannel

1) Le lien trunk entre S1 et S2 constitue un goulet d'étranglement, car son débit est identique au débit des liens utilisés par les postes (liens d'accès).
Réalisez une interface virtuelle (appelée *port-channel* ou *port group*) agrégeant 3 des interfaces de S1 et de S2. Mettez ensuite cette interface en mode *trunk*.

2) Utilisez iperf pour charger le lien entre A et B, connectés respectivement à S1 et S2, sur le VLAN2.
Affichez les statistiques des interfaces. La charge est-elle répartie sur les trois liens de l'Etherchannel ?
Lancez maintenant 2 transferts simultanés depuis un poste vers 2 postes différents. La charge est-elle répartie sur les trois liens de l'Etherchannel ?
Lancez maintenant 2 transferts simultanés vers le même poste. La charge est-elle répartie sur les trois liens de l'Etherchannel ?
Sur quel critère le switch se base-t-il pour répartir les trames sur les interfaces de l'Etherchannel ?

13.2 Bonding Linux

Sous Linux, l'agrégation de liens se nomme « bonding ». Le module du noyau Linux qui gère le bonding, nommé également « bonding », est préchargé sur vos postes.

1) La charge réseau vers un serveur peut parfois être importante. Pour augmenter la bande passante totale et la fiabilité de la liaison avec le serveur, agrégez 2 liens entre votre poste et le commutateur en utilisant la commande *ifenslave*.

2) Réitérez les transferts réalisés dans le chapitre précédent. Que constatez-vous ?

Une fois ce chapitre terminé, lancez la commande suivante sur tous les switches que vous avez utilisés :
```
delete flash:vlan.dat
```

14 Supervision

La supervision d'un réseau consiste à obtenir des informations utiles pour sa gestion (prévision des évolutions éventuelles, détection des anomalies, etc.).

La supervision d'un réseau repose notamment sur le protocole SNMP (*Simple Network Management Protocol*).
Ce protocole permet à un logiciel de gestion (le NMS, *Network Management System*) d'interroger un serveur (appelé *agent SNMP*) localisé sur l'équipement à surveiller.
L'agent peut également envoyer un message d'alerte, appelé *trap SNMP*, au NMS lors d'un événement particulier.

Les informations auxquelles SNMP accède sont structurées sous la forme d'un arbre d'objets, appelé MIB (*Management Information Base*). La MIB varie en fonction des équipements. Par exemple, un serveur Linux n'a pas la même MIB qu'un commutateur Cisco.

Pour référencer un objet de la MIB, on utilise un OID (Object Identifier). Par exemple, l'OID de l'*uptime* d'une machine, c'est-à-dire depuis combien de temps une machine est allumée, est 1.3.6.1.2.1.1.3.
Les premières valeurs (1.3.6.1), que l'on peut voir comme le tronc de l'arbre, sont toujours les mêmes.

1) L'identifiant de communauté (community string) joue le rôle de mot de passe d'accès à l'agent SNMP. La version 1 de SNMP est utilisée par l'agent. Utilisez la commande *snmpwalk* pour lire l'*uptime* de votre poste (*localhost*).

2) Connectez votre NMS à un commutateur et configurez ce dernier de manière à ce qu'il envoie un *trap* SNMP à chaque fois qu'une adresse MAC associée au port 10 est ajoutée ou supprimée de la table de commutation.
Sur votre NMS, utilisez le programme /usr/sbin/snmptrapd pour qu'il reçoive les *traps* SNMP et les affiche sur la console.