UNIVERSITÉ Grenoble Alpes

Master 1 Informatique

TP commutateur administrable - VLAN

Martin Heusse, Pascal Sicard

4 mars 2022

On dispose de commutateurs Allied Telesyn administrable. Ces commutateurs peuvent se configurer de diverses façons :

— par un terminal via un port série ou une interface réseau Ethernet et en utilisant l'application `Telnet`

— par un programme d'administration à l'aide du protocole SNMP (Simple Network Management Protocol)

— En utilisant un serveur HTTP interne au commutateur

On utilisera au départ un PC pris comme une console via un port série. On pourra ensuite utiliser le serveur WEB du commutateur (voir dernier paragraphe).

1 Connexion et lancement

1. Connecter à l'aide d'un câble approprié (câble série) le commutateur à un PC (port série **COM1)**.
2. Dans une fenêtre de commandes sous Free BSD lancer la commande **minicom**. On sort par la commande **Ctrl-A puis Z puis Q**.

Sur la ligne série, deux interfaces sont à votre disposition, soit des menus graphiques, soit en ligne de commande à la manière de ce qui existe sur les routeurs. Le ***login*** administrateur est `manager`, avec comme mot de passe `friend` (ne pas changer ce mot de passe).

Important : *Afin de partir sur de bonnes bases, donnez aux commutateurs une configuration "minimale". Cela peut se faire simplement dans le menu System Config par Reset to Factory Defaults*

2 VLAN

2.1 VLAN sans marqueur

On peut très simplement créer deux commutateurs virtuels en utilisant des VLANs. Dans un premier temps, on n'utilise pas des VLANs avec *tag*.
Remarque : Ces commutateurs ne sont configurables que par association par l'utilisateur (Port, VLAN).

Créer deux VLANs sur un commutateur et vérifier leur isolation.
Voir dans `Menu Vlan` puis `Create Vlan`, puis `Vlan Name`, puis `Untagged Port`, il faut alors donner la liste des numéros de ports non marqués appartenant au VLAN créé (exemple `1,3,4` ou `1-4`). Ne pas oublier de faire `save`.

2.2 VLAN avec marqueurs

Dans le cas où l'on utilise plusieurs commutateurs et que l'on ait besoin d'associer des ports à plusieurs VLANs, il est intéressant de pouvoir marquer les paquets (norme 802.1q) afin de connaître leur appartenance à un VLAN donné. Cela permet par exemple de transporter plusieurs VLANs sur un unique lien entre deux commutateurs.

Les systèmes d'exploitation des machines de TP sont compilées pour supporter les VLANs. On peut donc utiliser les interfaces virtuelles pour fabriquer et recevoir des trames marquées.
Pour cela, il suffit de :

- Créer une telle interface : `ifconfig vlan0 create`, où *vlan0* est le nom de l'interface virtuelle.
- Puis de lui attribuer un numéro de VLAN : `ifconfig vlan0 vlan NoVLAN` où `NoVLAN` est le numéro de VLAN.
- Sans oublier de spécifier l'interface réelle sur laquelle circulera le trafic : `ifconfig vlan0 vlandev NomInterface` où `NomInterface` est le nom de l'interface réelle.
  Exemple : `ifconfig vlan0 vlan NoVlan vlandev xl0` (cf. `man ifconfig`).
- Et enfin de lui attribuer une adresse IP d la même manière qu'une interface réelle.

On peut bien sûr faire tout cela en une seule commande `ifconfig`.
A savoir : la création d'une interface virtuelle associée à un Vlan implique que les trames envoyées et reçues seront marquées par le numéro de Vlan.

Important et IMPERATIF (pour ne pas s'emmêler les pinceaux) : On prendra soin de noter sur la figure du réseau les numéros de ports, les numéros

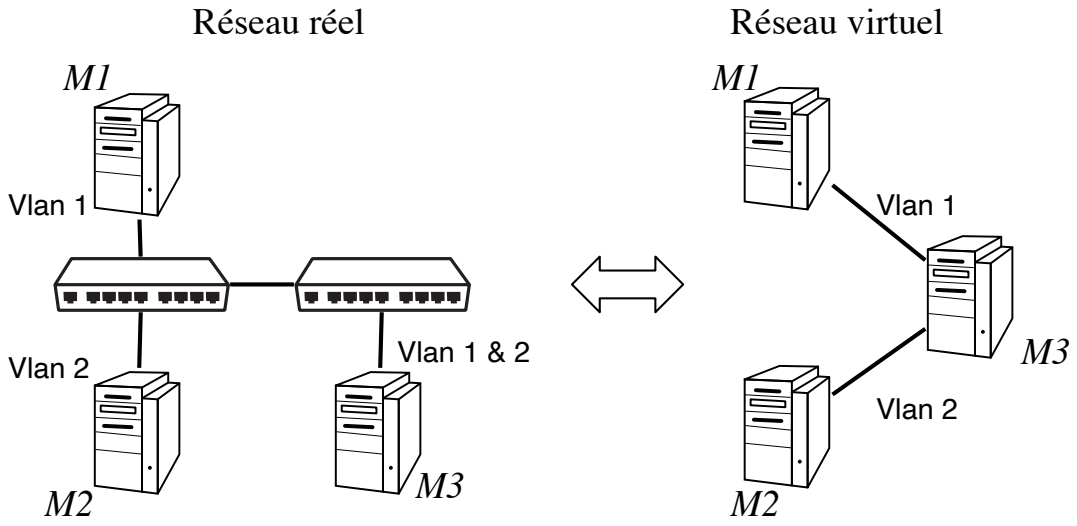

FIGURE 1 – Exemple de topologie : VLANs

de VLAN, et les adresses IP utilisés.

Créer la topologie de la figure 1 sans étiqueter les trames sur les machines n'appartenant qu'à un seul VLAN (M1 et M2).

— Sur chacun des commutateurs créer les deux VLANS et associer les ports à ces VLANS. On précisera les ports sur lesquels les trames doivent être étiquetées (*Tagged*) et ceux non étiquetés (*Untagged*).

— Sur M3 créer une interface virtuelle pour chacun des deux VLANs.

ATTENTION : l'utilisation de l'interface *bge0* semble poser des problèmes d'observations avec Wireshark pour des trames étiquettées. Il est impératif d'utiliser ***em0***.

— Observer l'état de ces deux interfaces (*ifconfig*). Observer la table de routage (*netstat -rn*). Attention c'est le numéro de VLAN (VID :Vlan IDentifiant) qui définit un VLAN et sert d'étiquette dans les trames.

— Peut on associer la même adresse de réseau IP aux deux interfaces ? Pourquoi ?

— Ne pas oublier de rendre M3 routeur (*sysctl net.inet.ip...*)

— Faites sur M3 un ping vers M1. Cela fonctionne-t-il ? Pourquoi ? Les paquets sont-ils "marqués" sur M3 ? et sur M1 ?

— Faites sur M1 un ping vers M2. Cela fonctionne-t-il ? Pourquoi ?

— Capturez les paquets circulant sur le réseau sur la machine M3 lors du Ping.

— Observez et détaillez les entêtes Ethernet des paquets. Vérifiez que les marquages sont faits.

— Résumez sur un chronogramme la circulation des paquets entre les machines et dans les switchs (ainsi que le marquage des Vlans dans les paquets observés) lors de ce ping.

ATTENTION : Si on veut observer les marquage 802.1Q dans les paquets, il faut les capturer sur l'interface physique associées aux interfaces virtuelles.

3 Restriction de l'accès MAC

Il est possible de réduire le nombre d'adresses ethernet tolérées derrière un port. Ainsi par exemple, une seule station peut être connectée à chaque port, et on ne peut plus en changer.

Il faut pour cela passer le port en mode `limité` ou `verrouillé` (voir du côté du `port menu` sur le commutateur).

1. En mode limité on décide du nombre d'adresses MAC pouvant apparaître sur un port donné
2. En mode verrouillé, le commutateur fait la sourde oreille à tout paquet ne portant pas une adresse source physique connue au moment du verrouillage [1] (voir le menu *Mac Address Table* pour avoir la liste des adresses associées à chaque port). Donc pour verrouiller une adresse sur un port il faut tout d'abord que le commutateur l'apprenne (au moins un paquet entrant sur le port), puis verrouiller. [2].

— Proposer un manipulation qui mette en évidence ces deux modes de restriction.
— Observer la table adresse MAC/port du switch lors des échanges des expérimentations.
A quel moment une adresse MAC est associée à un port et donc apparaît dans cette table ?
Que veut dire *static/dynamic* dans cette table ?
— Préciser le fonctionnement du commutateur dans chaque mode.

Attention : La verrouillage sur adresse MAC n'augmente qu'assez peu la sécurité du réseau, car de plus en plus de systèmes permettent de changer les adresses MAC des équipements.

1. Désolé pour cet anthropomorphisme.
2. Il est aussi possible de rentrer l'adresse MAC en statique

4 Port Miroir

Créer un port Miroir sur un commutateur. Vérifier que tous les paquets des ports "mirorés" passent par ce port.

5 Groupement d'interfaces

Les commutateurs dont on dispose en TP permettent de grouper plusieurs interfaces de façon à créer un lien de débit plus important. (*Port trunking*). Les seules conditions à respecter sont que les ports doivent appartenir au même VLAN, et que les liens formant le *trunk* doivent relier des ports ordonnés de la même manière sur les deux commutateurs en jeu.

— Proposer un test de cette fonction.
— Comment se repartit le trafic sur les liens mis en parallèle ?
— On pourra s'aider de l'observation des statistiques du trafic sur les ports (menu *Ethernet Statistics/ Port Statistic* dans le commutateur.
— Quelle différence entre le mode SA (Source Address) et SA/DA (Source Address / Destination Address) ?

6 Observation du contrôle de congestion

Le contrôle de flux est indispensable dans les réseaux ethernet commutés Full-Duplex. On peut parler dans ce cas plutôt de contrôle de congestion du réseau (du switch en l'occurence). En l'absence de collision sur le réseau, l'envoi de paquets explicites est nécessaire pour éviter la saturation des files d'attente des commutateurs et la perte de paquets en grand nombre. Ce contrôle des émetteurs par un élément du réseau est appelé contrôle de congestion. Pour que cela fonctionne il faut que le *contrôle de flux* soit activé sur les ports du commutateur.

Proposer un réseau et une charge de celui-ci qui provoque une saturation d'un segment Il est très simple d'observer les paquets PAUSE (faisant désormais partie de la norme Ethernet) en chargeant le réseau à l'aide de `udpmt` par exemple.
Remarque : Dans le cas de la génération de plusieurs flux à l'aide de `udpmt`, on prendra soin lancer un `udptarget` pour chaque `udpmt`.

Capturer ces paquets (ils sont moins nombreux que ce à quoi on pourrait s'attendre) et expliquer quel impact visible ils ont sur le trafic. L'intérêt de cette manipulation est aussi de se persuader qu'il arrive qu'un commutateur «détruise» beaucoup de trames. Pour cela on peut regarder les différences de nombre de pertes sur

une machine réceptrice de flux UDP avec ou sans contrôle de flux. On observera aussi les débits du côté émetteur(s).

7 Multicast et spanning tree

En cherchant dans les différents menus du commutateur, vérifiez si il peut prendre en compte :
— la gestion des groupes multicast ?
— le spanning tree ?

8 Configuration à travers un navigateur web

La plupart des équipements de réseau récents peuvent être configurés par l'intermédiaire d'une interface web. C'est plus convivial que la ligne série ou le telnet, mais il est alors moins aisé d'avoir une vision d'ensemble de la configuration.

1. Donner une adresse IP au commutateur (menu 4). Ne pas oublier de préciser le Netmask.
2. Brancher un ordinateur sur un port qui n'appartient à aucun VLAN.
3. Attribuer une adresse IP à cet ordinateur.
4. Se connecter à l'adresse IP du switch par `http` (le navigateur sur les machines est *opera* ou *firefox*).

Remarque : les routeurs du commerce ont aussi un serveur *http*. Que l'on peut également aller interroger.

Remarque : A la suite de ces manipulation, veillez à effacer la configuration des commutateurs, cela évitera à d'autres étudiants qui voudraient utiliser ces commutateurs d'avoir des surprises. (*System Config* puis *Reset to Factory Defaults)*

9 Annexe : Particularités des switch AT-8000S

La configuration de la ligne série est différente :

1. Vitesse de la ligne 115200 bauds
2. Pas de contrôle de flux

Il faut donc modifier les paramètres de minicom. Pour cela taper Ctr A puis Z. Puis choisir le menu de configuration O, puis dans *Serial Port Setup* choisir *Hardware flow control : no* et *Bps/Par/Bits* : 115200 bauds, 8 bits de donnée, 1 bit de stop.