TP 1/5: Découverte du matériel LAN

Objectifs

- Appréhender les bases de la configuration d'un commutateur (switch);
- Thèmes abordés:
  - configuration de base (liaison série, applet http);
  - configuration des ports: auto-négociation, débits en 10 et en 100Mbps;
  - analyse de trafic (*sniffer Ethereal*);
- Documents complémentaires:
  - Toutes les documentations sur le CISCO 2950: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2950

Organisation de la séance

Les étudiants (environ 14) seront divisés en 7 groupes de 2 personnes. Chaque groupe est doté au minimum du matériel suivant:

- 2 PC, dotés 2 cartes Ethernet;
- accès à un commutateur (switch CISCO 2950-12);

Le TP se déroule sur 2,5 heures. Le texte ci-dessous décrit une série de réalisations à effectuer en se répartissant les tâches.

Compte Rendu

Aucun compte rendu n'est demandé pour ce TP. Toutefois, la prise de notes sur ces actions de base est plus que recommandée pour la suite des TPs.

Commutation ethernet : rappels des bases

Principes de base

Un commutateur ethernet est un équipement de niveau 2 : il manie des trames ethernet (adresses MAC) sans regarder leur contenu (par exemple un datagramme IP). Avant l'apparition des commutateurs, on utilisait des *ponts* pour segmenter les réseaux Ethernet.

Un commutateur Ethernet (*switch*) s'installe comme un "*hub*". Un hub répète les trames qu'il reçoit sur tous ses ports. Un commutateur essaie de minimiser les envois inutiles qui gaspillent de la bande passante et génèrent des collisions. Pour cela, il utilise une table de commutation qui associe à chaque adresse MAC connue le port par lequel on peut l'atteindre.

Afin de simplifier la mise en place du commutateur et son administration, cette table est *apprise* automatiquement durant le fonctionnement. Lorsque l'adresse de destination d'une trame n'est pas dans la table, le commutateur l'envoie sur tous ses ports, sauf celui par lequel elle est arrivée (il se comporte alors comme un hub). Cependant, il note au passage l'adresse *source* de la trame dans sa table. De cette façon, les futurs envois vers cette station pourront être optimisés.

Un mécanisme de *vieillissement* (aging) des associations permet de résoudre le problème des déplacements de station d'un port à l'autre.

Normalement, la topologie physique d'un réseau Ethernet est un arbre (chaque hub ou commutateur est un noeud, les stations sont des feuilles). Il peut arriver que l'on crée des boucles: soit par inadvertance, soit pour obtenir des redondances augmentant la robustesse du réseau. Les commutateurs utilisent un algorithme distribué pour construire un *arbre recouvrant* (spanning tree) afin d'éviter les bouclages infinis. Pour cela, ils échangent les BPDU du protocole STP.

Débits, duplex et autonégociation

Les réseaux Ethernet filaires offrent différents débits et différents modes: half duplex (HD), full duplex (FD).

Le support utilisé est soit des paires torsadées (TX) soit de la fibre optique (FX).

Actuellement, les plus communs sont:

- 10Mbps HD (hub, anciennes cartes réseaux);
- 10Mbps FD (plus rarement utilisé);
- 100Mbps HD (typiquement hubs 10/100)
- 100Mbps FD ("fast ethernet", souvent commuté)
- 100Mbps FD / Fibre (liaison + longues)
- 1000Mbps FD (TX ou FX)

Deux équipements connectés ne peuvent communiquer que s'ils utilisent le même mode. Certaines erreurs de configuration se traduisent par une communication possible mais avec de

forts taux d'erreurs ou de collisions (exemple: carte half-duplex connecté à commutateur full-duplex).

En général, on peut soit fixer le mode (débit et duplex) sur chaque équipement, soit utiliser un mécanisme d'*autonégociation* (dans ce cas, il faut le spécifier aux deux extrémités).

Sur les cartes réseau, le choix du mode est normalement un paramètre du pilote (*driver*). Sous Linux, les commandes `mii-tool` et/ou `ethtool` permettent d'afficher ou de modifier le mode.

Configuration et administration du commutateur

La configuration d'un commutateur professionnel (il existe des modèle meilleur marché offrant moins de fonctionnalités) peut s'effectuer de différentes façons:

- console sur liaison série RS232;
- console telnet ou ssh sur IP;
- serveur HTTP embarqué (interface graphique);
- protocole SNMP.

Autres fonctionnalités

Enfin, les commutateurs offrent de nombreuses autres fonctionnalités que nous n'avons pas le temps d'étudier ici. Parmi les plus importantes, citons:

- Sécurisation des ports

  Deux approches:

  1- associer à chaque port une liste d'adresses MAC (ethernet) autorisées. C'est l'approche généralement retenue pour empecher les connexions de visiteurs indésirables sur de petits réseaux.

  Inconvénients: administration qui devient lourde sur de grands réseaux, sécurité très relative car les stations peuvent facilement changer d'adresse MAC.

  2- 802.1x et serveur d'authentification RADIUS.

  Avantage: gestion centralisée des autorisations (annuaire).

  Inconvénient: mise en place plus complexe. Va se répandre, surtout avec l'arrivée des réseaux sans fils pour lesquels cette approche devient incontournable.

- VLAN (Virtual Local Area Network) Un VLAN est un sous-réseau de niveau 2, qui peut partager le même réseau avec d'autres VLANs. Les commutateurs sont chargés d'isoler chaque VLAN, ce qui est utile pour sécuriser les échanges. Le protocole 802.1q est utilisé pour marquer les trames Ethernet et indiquer le VLAN auquel elles appartiennent.

  Les VLAN peuvent être définis par port ou par adresse MAC.

Pour communiquer entre eux, deux VLANs doivent être reliés par un routeur (niveau 3). Le niveau de sécurité n'est cependant pas idéal, certaines attaques permettent de passer d'un VLAN à l'autre (voir les documents cités ci-dessous).

Réalisations

La figure au tableau décrit la configuration de base de du réseau à construire sur la salle.

1. Configuration du switch

On va reconfigurer le switch comme s'il était neuf: pour cela, suivre les étapes suivantes:

1. Connecter un PC au switch via un cable série (qui se branche sur la face arrière du switch);
2. Lancer un émulateur de terminal (minicom sous linux, ou HyperTerminal sous Windows); Le configurer en 9600 8N1.
3. Eteindre le switch (le débrancher) et le rebrancher en appuyant sur le bouton "Mode" (garder le bouton appuyé jusqu'à affichage d'un message dans la console:

```
  The system has been interrupted prior to initializing the flash
  file system. These commands will initialize the flash file system, and
  finish loading the operating system software:
```

7. Initialiser le système avec les commandes:

```
  switch# flash_init
  switch# load_helper
```

   Puis supprimer l'ancienne configuration:

```
switch# del flash:config.text
```

   Note: le switch utilise un système de fichiers en mémoire flash, on peut afficher son contenu:

```
switch# dir flash:
```

   Démarrer le système:

```
switch# boot
```

   Comme il n'y a plus de fichier de configuration, le système vous propose de lancer le dialogue de configuration initial:

```
Continue with the configuration dialog? [yes/no]: Y
```

   Répondez oui: "Y"

10. Configuration de base:

- entrer les mots de passe telnet (utiliser toujours "pouzin") et enable (« cisco »)
- spécifier l'adresse IP du switch (192.168.X.100/24).
- indiquer "vlan1" pour que l'on puisse administrer le switch à partir du VLAN par défaut.

Après cette première configuration, le switch est fonctionnel et on peut le connecter au réseau ethernet.

2. Configurer le réseau

2.1. Quels sont les câbles ethernet nécessaires ? Indiquer le type de chaque câble (droit ou croisé) et justifier le choix.

2.2. Configurer les interfaces IP (ipconfig ou `ifconfig`) sur chaque PC.

2.3. A l'aide des commandes `ifconfig`, `ping` et `arp`, déterminer et noter les adresses MAC des PC et celle du switch. Le switch a-t-il une ou plusieurs adresses MAC ? (expliquez les mesures effectuées)

2.4. A l'aide de la commande `mii-tool` (ou suivant votre matériel `ethtool`), déterminez sur chaque PC l'état de la carte réseau utilisée (half-duplex ou full-duplex, 10 ou 100Mbps). Expliquez les résultats observés.

3. ARP (Address resolution Protocol)

3.1. Faire afficher la table ARP du switch. Débrancher le port d'un PC. Au bout de combien de temps la table est-elle mise à jour ?

3.2. Afficher la table d'association ports <-> adresses MAC. Tous les PC sont-ils visibles ? Commenter.

4. Analyse de trafic

4.1. Lancer `etherreal` sur le PC et capturer le trafic pendant 20 secondes. Donner la liste des trames observées et leur signification.

4.2. Lancer un ping de PC à PC, tout en observant le trafic sur PC2. Qu'observe-t-on ? Répéter l'expérience plusieurs fois et conclure.