Université de Caen Normandie 2019/2020
U.F.R des sciences
2ème année Licence – informatique

Réseaux 1 – TP4
Découverte du matériel LAN

Objectifs :

- Appréhender les bases de la configuration d'un commutateur (switch);
- Thèmes abordés :
  - configuration de base (liaison série, préparer le vlan par défaut);
  - analyse de trafic (sniffer Tcpdump ou Wireshark);
- Documents complémentaires :
  - Toutes les documentations sur le CISCO : https://www.cisco.com/c/en/us/support/switches/index.html

Organisation de la séance :

Les étudiants seront divisés en groupes (Selon le nombre des commutateurs disponibles). Chaque groupe est doté au minimum du matériel suivant :

- 1 commutateur (CISCO),
- 1 câble port-série,
- 2 adaptateurs USB-Ethernet,
- 2 câbles RJ45 (chaque groupe doit avoir une couleur unique) et
- 2 ordinateurs de la salle.

Le TP se déroule sur 2 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 du prochain TP.

Commutation ethernet :

Principes de base :

Un commutateur Ethernet est un équipement, pour l’instant, 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 concentrateur "hub". Un concentrateur 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 au début 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 concentrateur ou commutateur est un nœud, 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, voir le CM6) 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), voir le CM5.
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'auto-négociation (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.

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:

- Associer à chaque port une liste d'adresses MAC (ethernet) autorisées. C'est l'approche généralement retenue pour empêcher 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.
- 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.

Un (VLAN, Virtual Local Area Network) 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.

Réalisations

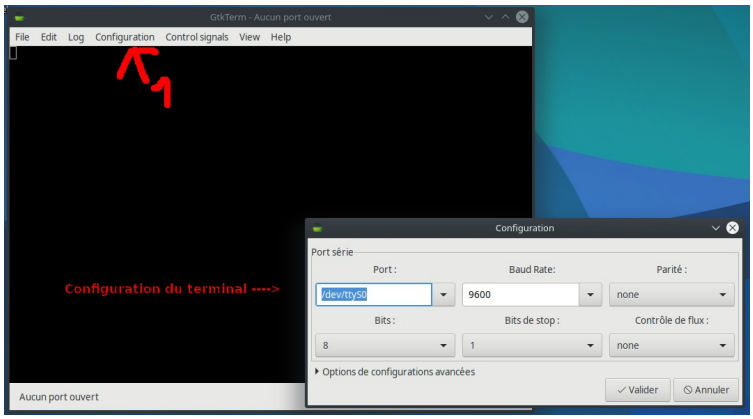
La figure au tableau décrit la configuration de base du réseau à construire sur la salle.

1. Configuration de base

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

1. Connectez un ordinateur au commutateur via le câble série fourni (qui se branche sur la face arrière du
commutateur). Attention de confondre l'extrémité avec les autres ports RJ45 du commutateur.

2. Lancez un émulateur d'un terminal port série (gtkterm sous linux, ou HyperTerminal sous Windows); configurez le programme en respectant la figure suivante, validez les paramètres, et enfin tapez entrer :



3. Débranchez le commutateur et rebranchez le en appuyant sur le bouton "Mode", vous allez voir les LEDs clignotent en vert, gardez le bouton appuyé jusqu'à la LED système passera à l'orange un court instant avant de virer au vert, cette fois sans clignoter. C'est à ce moment, et à ce moment seulement, qu'il faut relâcher la pression du bouton Mode. La pression prend environ 10 secondes.

Si dans la console vous avez les ':' après le nom du commutateur, saisissez :

switch : flash_init
switch : boot

Ces deux commandes permettent d'initialiser le flash et de lancer le firmware du commutateur (un petit système d'exploitation dédié à un type de matériel).

4. Réinitialisez la configuration avec la suite des commandes suivantes :

switch> enable
switch# erase startup-config (ou parfois, switch#erase nvram:)
switch# delete flash:vlan.dat
switch# del flash:config.text

- *enable* permet de passer en mode privilégié pour pouvoir exécuter certaines commandes d'administration, remarquer le changement du curseur terminal en #.
- *erase startup-config* permet de supprimer l'espace nvram (mémoire RAM non volatile) contenant la configuration du démarrage (appelé, startup-config). Par conséquent, le commutateur doit être configuré dans le prochain démarrage.
- La précédente commande permet de restaurer le commutateur en paramètre usine avec une seule exception. La base de données VLAN (qui sera explorée dans le TP5) ne fait pas partie de la configuration du démarrage. En effet, elle fait partie de l'espace flash où elle est enregistrée. Par conséquent, la base de données VLAN doit être aussi supprimée avec la commande *delete flash:vlan.dat.*
- La dernière commande, *del flash:config.text*, est optionnelle, elle permet de supprimer une configuration enregistrée avec la commande write pour des raisons de restauration.

Note: le commutateur utilise un système de fichiers en mémoire flash, on peut afficher son contenu en utilisant la commande 'dir' :
switch#dir flash:

5. Rechargez le système:
switch#reload

Comme il n'y a plus de fichier de configuration de démarrage, le système vous propose de lancer le dialogue de configuration initial :
Continue with the configuration dialog? [yes/no]:
Répondez par non: **'no'**

6. Nous allons configurer manuellement le commutateur :
   a) Passez en mode utilisateur privilégié.
   b) Passez en mode configuration globale en utilisant la commande **#configure terminal**, que remarquez-vous ?
   c) Donnez au commutateur un nom en utilisant la commande **#hostname nom_de_votre_choix**, que remarquez-vous ?
   d) Passez au vlan 1 en utilisant la commande **#interface vlan 1**, quelle est la particularité de ce val1 ? et que remarquez-vous sur le terminal après l'exécution de cette commande ?
   e) Donnez une adresse IP à ce vlan en utilisant la commande **#ip address une_adresse_ip son_masque** tout en notation pointée (e.g. 192.168.0.1/24). Si on veut que le commutateur soit accessible à distance, on peut utiliser la commande suivante dans le mode « configuration globale, question b» pour spécifier l'adresse du routeur qui lie le commutateur avec le reste du monde, **#ip default-gateway ip_du_routeur**. Vous pouvez ignorer cette dernière commande puisque le commutateur n'est pas lié à un routeur.
   f) Enfin, retournez au mode initial d'utilisateur privilégié en utilisant la commande **#end**, et sauvegardez la configuration en utilisant la commande **#copy running-config startup-config**, qui permet de mettre la configuration, actuellement dans la RAM, dans l'espace mémoire non volatil NVRAM, vérifiez si le fichier existe ?

7. Si on veut vérifier que la configuration est effectivement une configuration de démarrage, utilisez la commande suivante **#show startup-config**, que remarquez-vous ?

8. En se basant sur votre manipulation des commandes précédentes, quelle est la version de votre commutateur ? Note : Tapez « **?** » pour avoir de l'aide.

9. On peut utiliser la commande suivante **#show interfaces FastEthernet 0/1**, si on s'intéresse à avoir des informations sur l'interface FastEthernet 0/1 du commutateur. Essayez la commande sur une interface choisie, puis analyser la sortie.

2. Configurer le réseau

1. Quels sont les câbles Ethernet nécessaires ? Si on dispose d'un équipement ancien, indiquez le type de chaque câble (droit ou croisé) et justifier le choix.

2. Lancez le programme *virtualbox* sur les deux ordinateurs de la salle. Si vous ne disposez pas dans votre liste une machine *vbox* préconfigurée, fermez le programme *virtualbox* et utilisez la commande suivante dans un terminal pour en créer une :

>**virtualbox-createtp --create Réseaux1 2019-10-03_buster_reseau_router**

Relancez le programme *virtualbox* et démarrez la machine virtuelle créée sur les deux ordinateurs de la salle. Pour ouvrir votre session, utilisez le compte suivant qui vous donnera des droits d'un utilisateur privilégié :

login : **root**
password : **root**

3. Connectez les deux ordinateurs de la salle avec le commutateur via l'adaptateur USB-Ethernet, et configurez les adresses IP associées en utilisant les commandes ci-dessous.

Nous utilisons une machine virtuelle qui crée un pont pour associer l'interface virtuelle avec l'adaptateur USB-Ethernet, et ainsi la machine virtuelle sera considérée par le commutateur comme une machine physique. Utilisez les commandes suivantes pour configurer l'adresse IP de chaque interface virtuelle, ces commandes permettent d'avoir une configuration temporaire jusqu'au prochain redémarrage :

- Vérifier le nom de l'interface associée à l'adaptateur en regardant le fichier avec la commande >**nano /etc/network/interfaces**. Cliquez sur **ctrl+x** pour sortir. Le nom de l'interface virtuelle liée à l'adaptateur USB-Ethernet est appelée **enp0s8**.
- **ip link set dev enp0s8 down**
- **ip addr add dev enp0s8 192.168.1.**<donnez un id=[1,…,254] différent pour chaque interface virtuelle>**/24**
- **ip link set dev enp0s8 up**

3. À l'aide des commandes **ifconfig**, **ping** et **arp** , déterminez et notez les adresses MAC des deux ordinateurs et celle du commutateur. Le commutateur a-t-il une ou plusieurs adresses MAC ? (expliquez les mesures effectuées)

4. Affichez la table d'adressage dynamique utilisée par le commutateur (adresses MAC – ports). Toutes les machines liées sont-elles visibles ? Commenter.

5. Analysez le trafic en utilisant le programme **tcpdump**. Lancez un ping de la 1er machine à la 2ème machine, tout en observant le trafic sur la 2ème machine. Qu'observe-t-on ? Répétez l'expérience plusieurs fois et que peut-on conclure ?