TP réseaux « TCP/IP »:
Utilisation d'un simulateur de réseaux

Préparation :

- **Lire, comprendre et réfléchir aux questions posées dans le sujet de TP**
- **Faire éventuellement une petite recherche**

Après avoir activé le lien :

- **Installer le logiciel sur votre poste**
- **Lire la documentation du logiciel**

Manipulations/Simulations :

Points importants :

- **Autonomie**
- **Réflexion**
- **Logique**

Un CR sera à me rendre sous format informatique en PDF à mon adresse mail universitaire, bruno.deresme@univ-valenciennes.fr **ou papier dans mon casier à l'ISTV3**

Bon courage,

Introduction
Le simulateur de réseaux que nous allons utiliser au cours de ce TP a été développé par Pierre Loisel et est disponible gratuitement ici :
http://archives.reseaucerta.org/outils/outils.php?num=236
ou http://archives.reseaucerta.org/outils/simulateur/
ou http://www.reseaucerta.org/outils/simulateur/.
Il permet de créer un réseau et de simuler son comportement au niveau Liaison de données, IP, et Transport. On peut sauvegarder le réseau réalisé sous la forme d'un fichier xml, et le charger ultérieurement. Il permet aussi d'exporter l'image représentant le réseau.

Il s'utilise selon les 4 modes suivants (accessibles depuis le menu *Mode*):

Conception réseau
(F2) permet d'ajouter des stations, câbles, hubs, switch, etc. Dans ce mode, on peut modifier le nombre de cartes réseaux des stations, leur ajouter une carte d'accès distant (modem), modifier le nombre de ports des hubs, switch, etc. C'est donc principalement un mode qui s'occupe du matériel ;

Ethernet
(F3) permet d'émettre une trame à partir d'une carte à destination d'une autre carte (ou en broadcast), éteindre un matériel, etc.

IP
(F4) permet de configurer les matériels au niveau IP, notamment les adresses IP et les tables de routage, activer le routage sur du matériel possédant plusieurs cartes. Permet aussi d'observer l'émission et le traitement de requêtes/réponses ARP et ping.

Transport
(F5) permet d'envoyer des messages. Dans ce mode, on peut aussi faire du NAT/PAT et filtrer des trames (fonction firewall).

TP-manip :

a. En mode conception (F2), créer un réseau composé de 2 ordinateurs reliés par un câble croisé (figure 1). On accède à un menu permettant de modifier le type de câble en effectuant un clic droit sur une des cartes qu'il relie. En effectuant un clic droit sur une station, on accède à un menu permettant de modifier son nom, son nombre de cartes réseau, et la présence d'une carte d'accès distant (modem). Le modem permettra de se connecter à (un fournisseur d'accès à) Internet via une ligne téléphonique.

Figure1 : 2 ordinateurs reliés par un câble

b. En mode Ethernet (F3), choisir la simulation pas à pas et lire les différentes étapes tout au long des manips du TP. Cocher aussi "Message réception" de façon à avoir une popup lorsqu'un message arrive correctement à destination. Emettre une trame depuis st1 vers st2. L'émission d'une trame se demande en faisant un clic droit sur la carte émettrice.

c. Ajouter une carte réseau à st1 et la relier à un hub, lui-même connecté à une autre station (st3) et un autre hub sur lequel est reliée encore une autre station (st4) comme ceci :

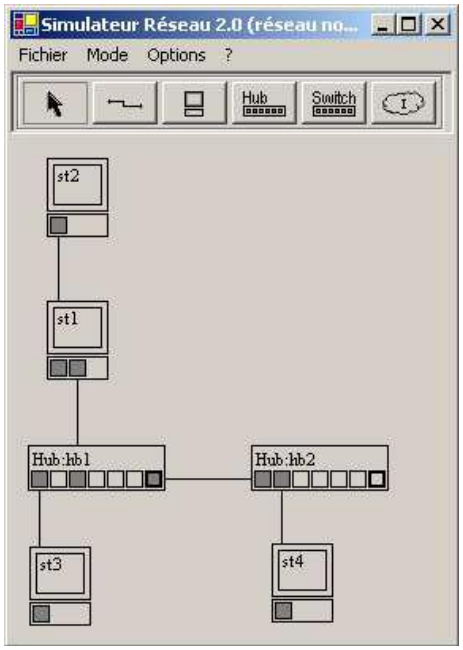

Figure 2

d. En mode Ethernet, vérifier que st4 peut envoyer une trame à st1. De même avec une trame broadcast. Quelle(s) différence(s) y a-t-il entre les deux envois ?

e. En mode IP, configurer les stations st1, st3 et st4 pour qu'elles fassent partie du même réseau 192.168.0.0/24 (le /24 veut dire que l'adresse du réseau (ou du sous-réseau) est sur 24 bits : son masque est donc 255.255.255.0). Attribuer une adresse IP à une carte réseau se fait en effectuant un clic droit sur la carte. Pour st3 et st4, utiliser st1 comme passerelle. Avant d'indiquer une passerelle, il faut d'abord attribuer une adresse IP à la station.

f. En effectuant un clic droit sur la station st3, envoyer une requête ping depuis st3 vers st4. Elle doit correctement arriver, ainsi que la réponse. Remarquez que l'émission de la requête d'écho ICMP (ping) provoque au préalable l'envoi d'une requête et d'une réponse ARP.
g. Activer le routage sur st1, st1 et st2 font parties du réseau 192.168.1.0/24.
h. Faire ce qu'il faut pour qu'une requête ping depuis st4 vers st2 soit satisfaite.
i. En mode Transport (F5), faire écouter le port TCP 22 (ssh) par st3.
j. Envoyer une requête depuis st2 vers st3 sur le port TCP 22.
k. Faire répondre st3.
l. Envoyer une requête depuis st2 vers st3 sur le port UDP 22.
m. Créer le réseau 192.168.2.0/24 composé de 2 switchs et de 2 stations par switch (st5 et st6 sur l'un, st7 et st8 sur l'autre, comme sur la figure 3 ci-après). Le switch sur lequel sont connectés st5 et st6 ne doit avoir qu'un seul port de cascade (uplink), alors que celui sur lequel sont connectés st7 et st8 ne doit en avoir aucun. Utiliser le port uplink du premier switch pour le connecter au second. Configurer le réseau de telle sorte que st5 soit la passerelle.
n. Faire écouter st8 sur le port 21 (ftp).
o. Emettre une requête depuis st6 sur le port 21 de st8. Celle-ci ainsi que la réponse ne doivent pas poser de problèmes.
p. Supprimer le câble reliant les deux switch et supprimer le port uplink. Faire en sorte de relier les switch sans utiliser de câble uplink, comme ci-dessous:

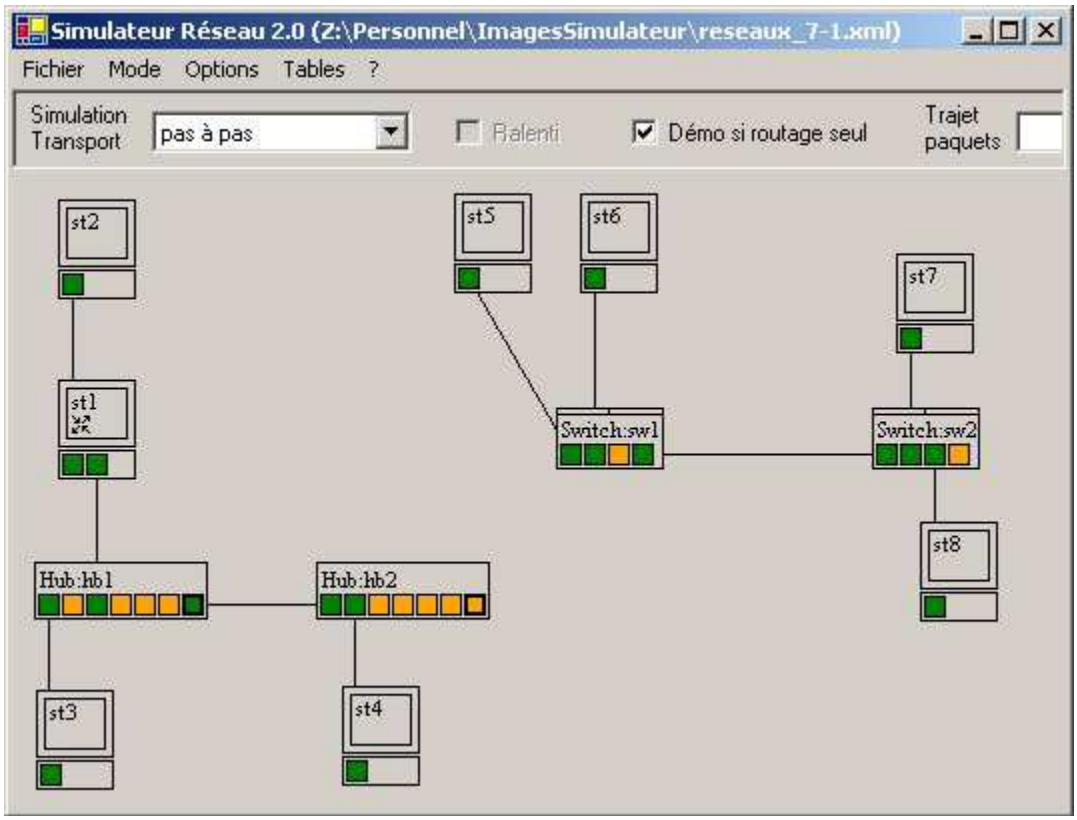

Figure 3

q. Emettre une requête depuis st5 sur le port 21 de st8. Celle-ci ainsi que la réponse ne doivent toujours pas poser de problèmes.
r. Ajouter Internet.
s. Ajouter une carte d'accès distant à st1 et à st5. Relier cette carte à un Fournisseur d'Accès Internet en utilisant un câble de type ligne téléphonique. De même pour st5.
t. st1 et st5 se sont vus attribuer par leur FAI une adresse supplémentaire. Il faut ainsi renseigner leurs passerelles.
u. Envoyer une requête depuis st1 vers st5. Cela devrait marcher.
v. En revanche, toutes les autres adresses ne sont pas connues des FAI. Envoyer une requête ping depuis st1 vers st8. Celle-ci est bloquée par le FAI.
w. Activer le routage ainsi que le NAT/PAT sur la machine st5 (interface officielle) : les datagrammes à destination du port TCP 50 doivent être acheminés vers le port TCP 21 de st8.

x. Envoyer une requête depuis st1 vers le port TCP 50 de st5 (utiliser l'IP de son interface officielle). Celle-ci devrait être routée vers le port TCP 21 de st8, et st8 devrait pouvoir répondre.
y. En principe, il devrait être possible d'envoyer une requête ping depuis st7 vers st1 et la réponse devrait parvenir. Or dans ce simulateur, le NAT ne fonctionne qu'en mode transport. Ainsi, ici la translation d'adresse ne fonctionne pas juste au niveau IP et la réponse ne peut pas parvenir à l'émetteur. Essayer quand même et observez l'adresse source du datagramme en sortie de st5.
z. Faire écouter st1 sur le port UDP 5000. Depuis st7, envoyer une requête vers le port UDP 5000 de st1. Cette fois, en sortie de st5 on a bien comme adresse source, celle de st5 et non de st7 ! La réponse devrait donc être possible.
aa. Activer le NAT/PAT sur st1 (interface officielle) : les datagrammes à destination du port TCP 1024 doivent être routés vers le port TCP 22 de st3.
ab. Envoyer une requête depuis st7 vers le port TCP 1024 de st1. Elle devrait arriver correctement, et la réponse devrait être possible.
ac. Essayer de faire la requête de st1 vers le serveur ftp de st8 en mode manuelle. Essayer ensuite de faire la requête de st7 vers le serveur SSH de st3.

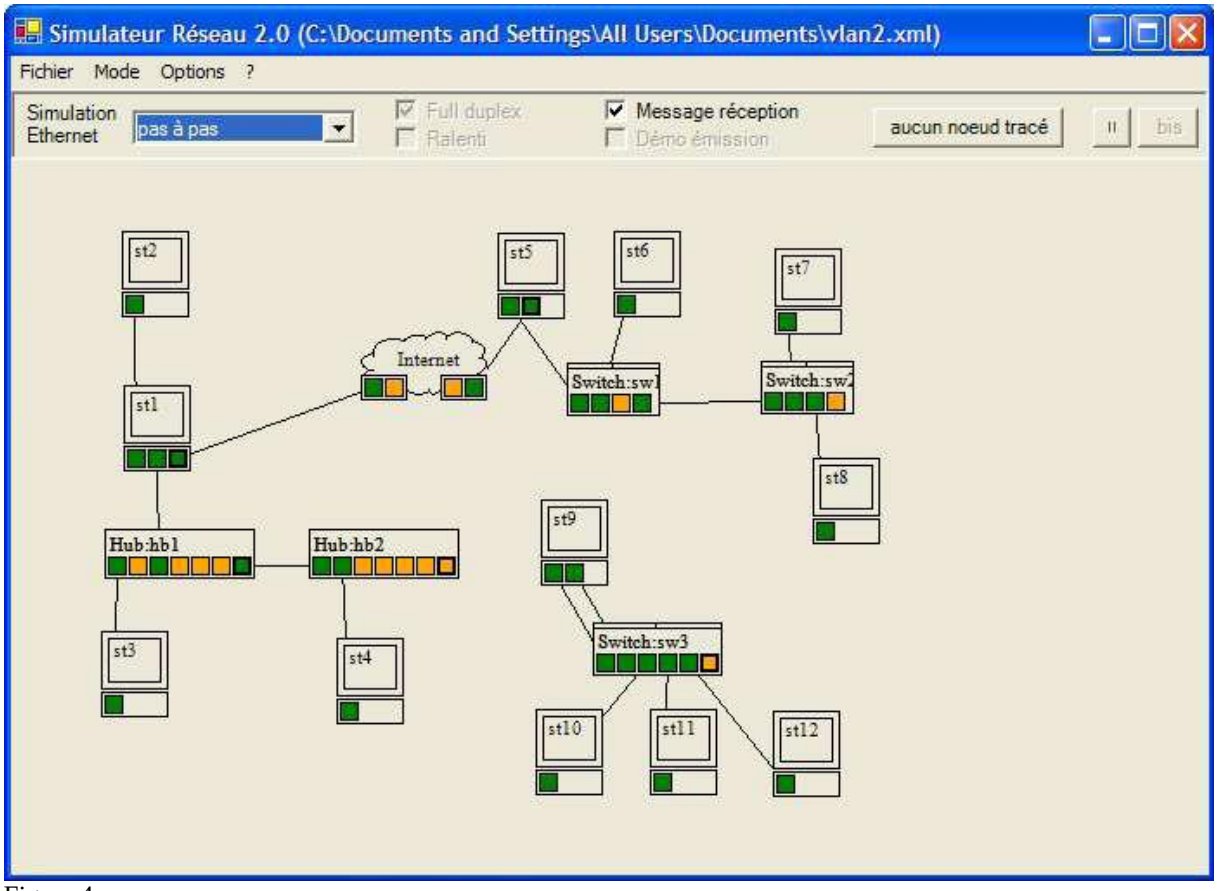

Figure 4

ad. Ajouter un troisième réseau constitué pour l'instant d'un switch et de 4 postes. Ce switch gérera les Vlan, st9 servira de passerelles d'un vlan vers l'autre. Utiliser des Vlans de niveau 1, st9 fait partie des 2 vlans, st10 et st11 du vlan 2, st2 du vlan 3. Tester en mode Ethernet d'émettre une trame en broadcast depuis chaque machine.
ae. Ajouter un switch (sans vlan) avec 2 postes connectés au sw3 par le port uplink. Mettre le port uplink du switch 3 dans le vlan 3. Tester une trame en broadcast depuis st11 puis depuis st12.
af. Tester une trame en broadcast depuis st13.
ag. Ajouter la gestion de vlan sur le dernier switch (sw4). Tester les trames depuis st11, st12 et st13.
ah. Sur sw4, gérer les vlans en mettant st13 dans le vlan 2 et st14 dans le vlan 3. Le port de liaison sera dans le vlan 2. Tester les trames depuis st11, st12, st13 et enfin st14.
ai. Ajouter un port 802.1q sur chaque switch et faire la liaison entre eux par ce port. Tester les trames depuis st11, st12, st13 et enfin st14.
aj. Configurer le vlan 2 avec l'adresse réseau 10.0.0.0 / 16 et le vlan 3 avec l'adresse 172.16.21.0 /24, st9 sera la passerelle. Faire ce qu'il faut pour que st14 puisse faire un ping vers st13 (en conservant évidement les vlans).
ak. Tester le ping de st14 vers st13.

al. Que faut-il faire pour pouvoir brancher st13 sur le switch 3 tout en pouvant continuer à faire un ping de st14 vers st13 ? (ne faites pas la modification ou bien juste temporairement pour vérifier votre réponse)
am. Passer la gestion des vlans en niveau 2 sur sw3. Configurer le switch sw3 pour que st10 et st11 soit dans le vlan 5 et st12 dans le vlan 10, st9 est toujours la passerelle, déconnecter sw3 de sw4. Consulter la table port/vlan. Tester les trames depuis st11 et st12.
an. Reconnecter le sw3 au sw4 par le port 802.1q. Tester les trames depuis st11, st12 et st13.
ao. Mettre le port de st13 dans le Vlan 5, celui de st14 dans le vlan 10. Tester les trames depuis st11, st12, st13 et st14.
ap. Passer sw4 avec un Vlan de niveau 2. Configurer dans sw4 les adresses macs de st13 dans le Vlan 5 et de st14 dans le Vlan 10. Tester les trames depuis st11, st12, st13 et st14.
aq. Débrancher st13 de sw4 et le rebrancher sur sw3. Tester les différentes trames.
ar. Faire ce qu'il faut pour que l'on puisse brancher st9 à st14 sur sw3 ou sw4 sans que cela ne change rien.
as. Vérifier que st9 est toujours bien la passerelle.
at. Connecter st9 à internet. Le vlan 5 sera un réseau sécurisé qui accueille un serveur SSH sur st13. Le Vlan 10 sera la DMZ qui accueille un serveur Web sur st12 et un serveur ftp sur st13. Ecouter les ports qui conviennent, activer le NAT sur st9 et configurer les bonnes redirections.
au. Tester l'accès au serveur Web et au serveur FTP depuis les autres réseaux.
av. Ajouter un poste sur Internet pour obtenir la configuration suivante :

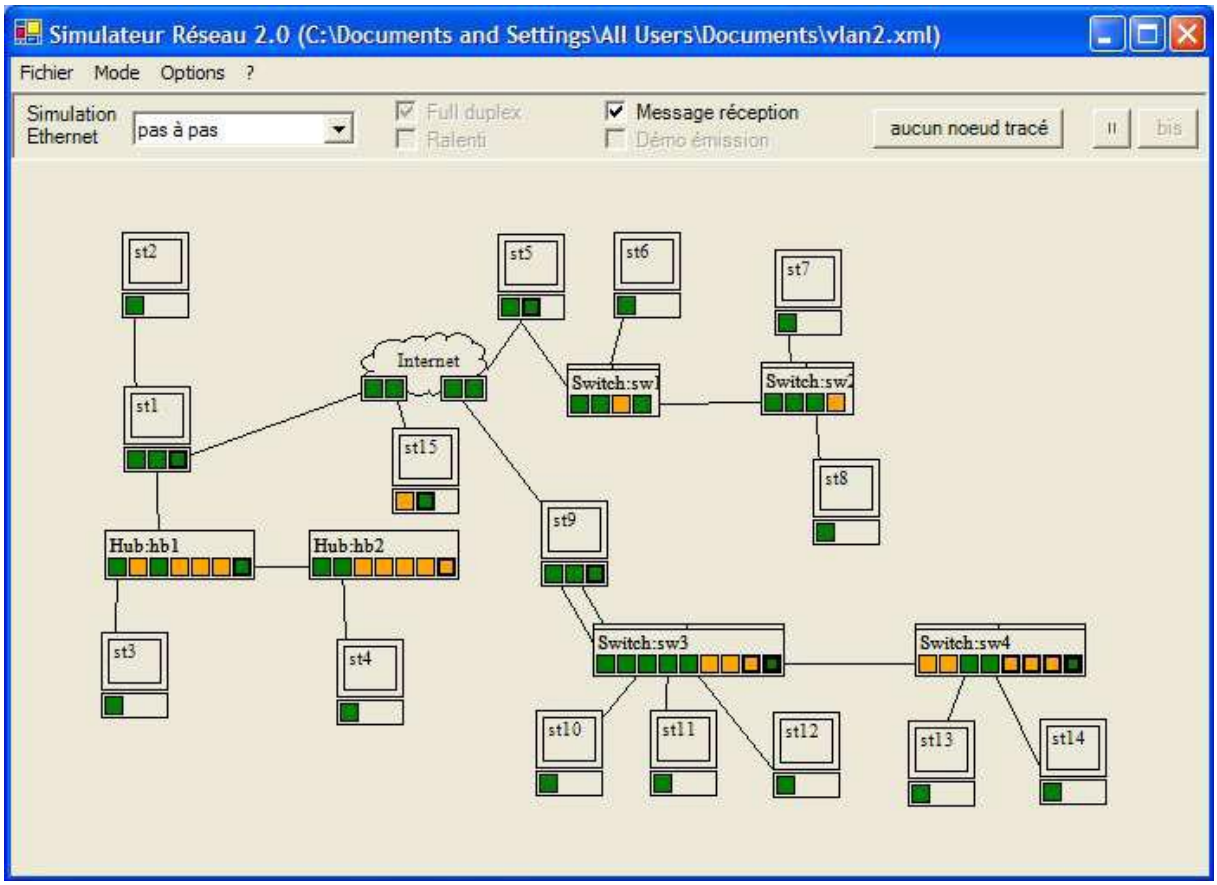

Figure 5

aw. Configurer le fichier host de st15 pour SAS corresponde à st9.
ax. Configurer le firewall (règles de filtrage) de st9 pour que tout le monde puisse atteindre un serveur web ou FTP dans la DMZ mais que seul st15 puisse atteindre le serveur SSH. Bloquer tout autre type de trafic. Tester depuis st7 le serveur Web, FTP et SSH de st9. Tester depuis st5 le serveur Web, FTP et SSH de SAS.
ay. Tester de st13 et st14 le serveur FTP de st8. Tester de st13 et st14 le serveur Web de st8 (qui n'existe pas).
az. Corriger les règles de filtrage pour les messages ICMP soit reçu correctement par st13 et st14 en cas d'erreur d'adresse IP ou de numéro de port.

NB : Si vous arrivez à faire toutes ces requêtes en mode manuelle, vous avez correctement assimilé les principes de base du routage IP

Quelques mots techniques :

ARP : protocole de résolution d'adresses, protocole effectuant la traduction d'une adresse de protocole de couche réseau (typiquement une adresse IPv4) en une adresse MAC (typiquement une adresse ethernet), ou même de tout matériel de couche de liaison
Broadcast : le broadcasting désigne une méthode de transmission de données à l'ensemble des machines d'un réseau.
DMZ : sous-réseau isolé par un pare-feu
FAI : fournisseurs accès internet
Firewall : ou pare-feu, logiciel et/ou un matériel, permettant de faire respecter la politique de sécurité du réseau
FTP : protocole de transfert de fichiers
HUB : ou concentrateur, appareil permettant d'interconnecter électriquement plusieurs appareils, typiquement des ordinateurs (connexions réseau Ethernet via hub Ethernet) ou encore des périphériques (hub USB, Firewire,...), mais aussi parfois un commutateur ou un routeur
ICMP : protocole qui permet le contrôle des erreurs de transmission
IP : famille de protocoles de communication de réseau informatique conçus pour et utilisés par Internet.
NAT : « traduction d'adresse réseau » lorsqu'il fait correspondre les adresses IP internes non-uniques et souvent non routables d'un intranet à un ensemble d'adresses externes uniques et routables. Ce mécanisme permet notamment de faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé, et pallie ainsi l'épuisement des adresses IPv4
PAT : Effectue une translation des ports IP entre l'intérieur d'un réseau privé et une Adresse IP sur internet
PING : nom d'une commande informatique permettant de tester l'accessibilité d'une autre machine à travers un réseau IP. La commande mesure également le temps mis pour recevoir une réponse, appelé round-trip time (temps aller-retour)
POPUP : fenêtre secondaire
port TCP : N° du port (22 : SSH, 23 : telnet, 1863 : MSN …)
requête : demande
SSH : protocole de communication sécurisé
SWITCH : commutateur réseau qui permet l'interconnexion d'entités réseau appartenant à un même réseau physique. Contrairement au concentrateur (ou hub), il fractionne le réseau en domaines de collision indépendants.
UPLINK : un port uplink permet de cascader (empiler) des hubs ou des switchs. Un switch sans uplink est un switch "stand-alone".
Vlan : Réseau local virtuel