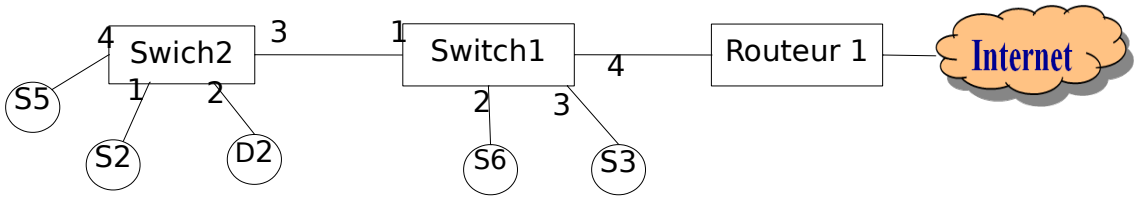
TD1 : attaques réseaux

Données :

- Par défaut, les routeurs rejettent les messages envoyés en diffusion.
- Les commutateurs diffusent les messages s'ils ne peuvent pas déterminer le port de sortie.

Exercice 1 :

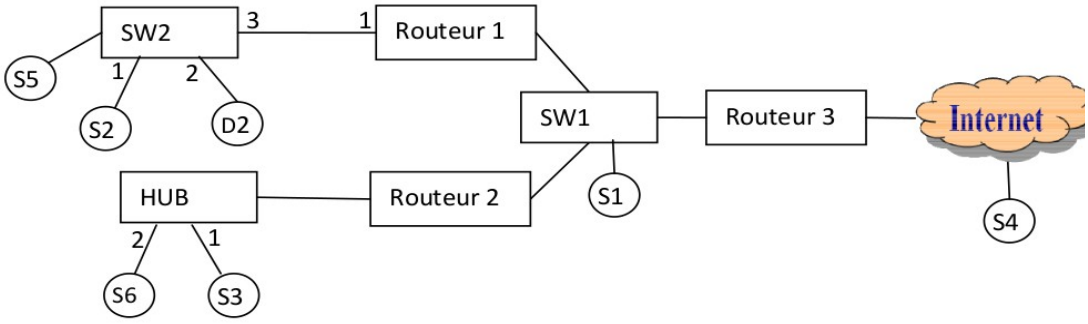
Soit le réseau câblé suivant où les cercles sont des stations de travail :



1) Expliquer comment se fait l'apprentissage par les commutateurs de l'appartenance d'une station à un réseau local (relié à un port du commutateur) afin de faire correctement l'acheminement des trames ?
2) Expliquer le rôle des temporisateurs au niveau des entrées des tables de commutation ?
3) Supposons que la table de commutation (CAM) de SW2 contient les entrées S2, D2 et S5. Si S5 envoie une trame en spécifiant comme adresse MAC source celle de S2, quel problème peut surgir ?
4) Supposons que la table de commutation (CAM) de SW2 contient les entrées S2, D2 et S5. Si S2 se connecte à D2 en envoyant un mot de passe en clair? S5 peut-il récupérer ce mot de passe ? Si oui, comment ?
5) Sachant qu'il est possible d'envoyer un ARP Reply sans sollicitation au préalable (Gratuious ARP Reply). Expliquer comment S5 peut récupérer tout les messages échangés entre S2 et D2 ?
6) Supposons que toutes les machines obtiennent leurs configurations IP à partir d'un serveur DHCP installé au niveau de la sation S6. Expliquer comment S5 peut intercepter le trafic de toutes les machines destiné à Internet ?
7) Supposons que que le routeur 1 implémente des règles qui rejettent tout les paquets destiné au serveur FTP (TCP/21) implémenté au niveau de la station S3. Expliquer comment un utilisateur sur Internet peut se connecter sur ce serveur ?

Exercice 2 :

Soit le réseau câblé suivant où les cercles sont des stations de travail et les « SW » sont des commutateurs.



1) Quel sont les trames que la station S2 peut sniffer (écouter) ? Expliquer ?
2) Quel sont les stations qui peuvent lancer une attaque ARP spoofing sur le réseau relié à l'interface 1 du routeur1? Expliquer ? (ARP spoofing: Répondre à une trame ARP who is? par une trame ARP reply avec une adresse MAC qui ne correspond pas à l'adresse IP donnée).
3) S4 peut-il exécuter une attaque TCP syn flooding sur S1 (TCP syn flooding: Etablir plusieurs connexion successives semi-ouverte afin de saturer la pile TCP de la victime)