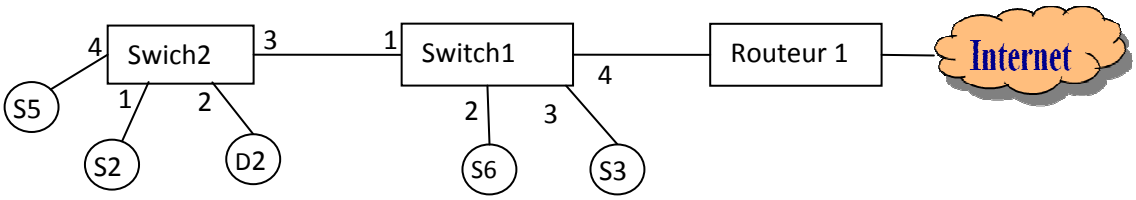
TD1 : attaques réseaux

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 :



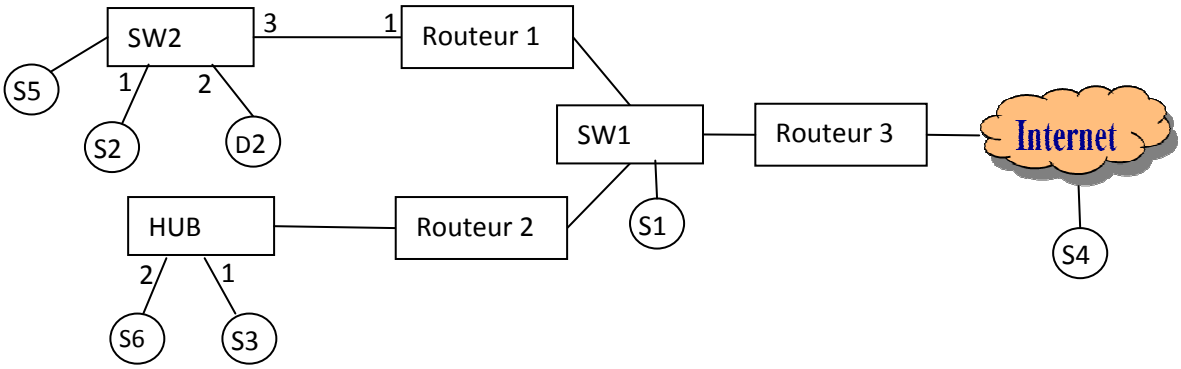
1) Expliquer comment se fait l'apprentissage par les commutateurs de l'appartenance d'une station à un réseau local (relié à un port du commutateur) afin de faire correctement l'acheminement des trames ? ➔ lorsqu'un commutateur reçoit une trame à partir d'un nœud **src** sur son port **p**, il ajoute dans sa table une ligne (src, p, temporisateur)
2) Expliquer le rôle des temporisateurs au niveau des entrées des tables de commutation ? ➔pour supprimer les lignes correspondant aux nœuds qui n'ont pas envoyé de trames jusqu'à l'expiration de leurs temporisateurs (exemple : un nœud peut quitter le réseau. C'est donc inutile de garder la ligne correspondante).
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 ? ➔le switch va modifier sa table en mettant que S2 est accessible par le port 4 et non plus 1 : les trames à destination de S2 vont aller vers S5
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 ? ➔ une solution est de transformer le switch en un hub en inondant sa table de commutation : S5 recevra tout les message qui passe par le switch2
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 ? ➔ envoyer à D2 un message ARP (@IP de S2, @MAC de S5) et envoyer à S2 un message ARP (@IP de SD, @MAC de S5)
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 ? ➔ consommer toute la plage d'adresse du serveur DHCP légitime. Puis, se transformer en serveur DHCP et fournir

aux clients des configurations IP en leur indiquant son adresse comme passerelle par défaut

7) Supposons 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 ? ➔ tiny fragment attack ou overlapping attack

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 ? ➔ les trames qui lui sont destinées ou celles en diffusion (**dans le cas du sniffing passif**)
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). ➔ les trois stations relié à SW2 car ce sont les seules qui peuvent recevoir les trames who is correspondantes (le routeur 1 rejette les trames en diffusion)
3) Quel sont les nœuds qui peuvent être victimes de l'attaque smurf générée par le nœud S2? (smurf : inondation du réseau avec des ping ayant des adresses de broadcast et une adresse source fausse ou d'une victime). ➔ Les nœuds S5 et D2 pour la même raison que la question précédente
4) 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)➔ oui car ce sont des paquets en unicast et peuvent donc traverser le routeur1.