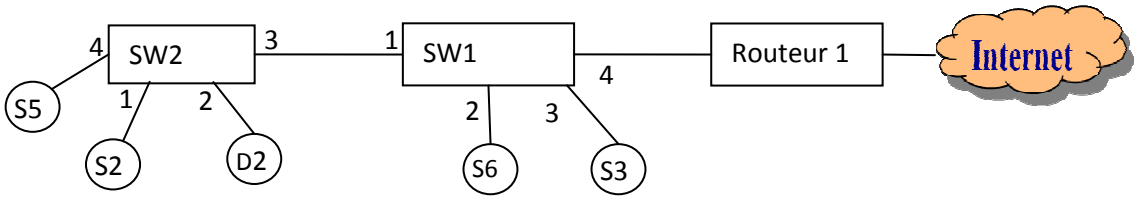
TD1 : attaques réseaux

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 :

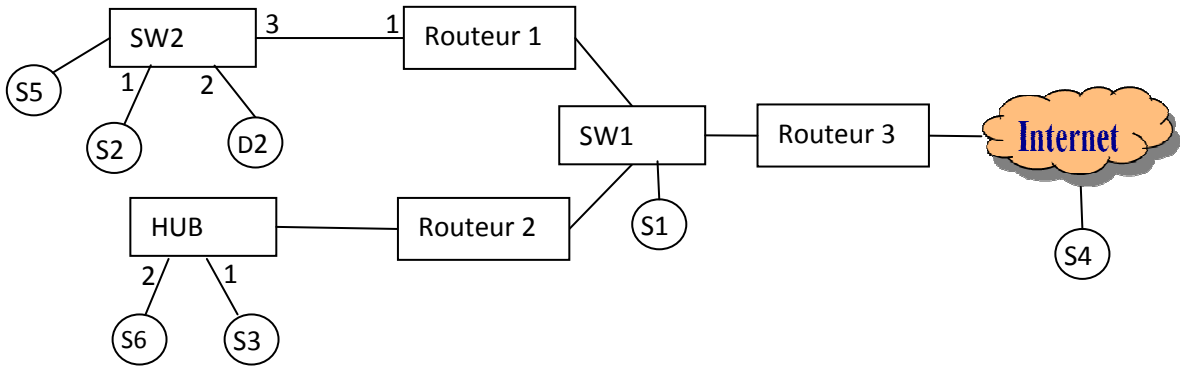
Soit le réseau câblé suivant où les cercles sont des stations de travail :



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 tous 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 station S6. Expliquer comment S5 peut intercepter le trafic de toutes les machines destiné à Internet ?
7) Supposons que le routeur 1 implémente des règles qui rejettent tous les paquets destinés au serveur FTP (TCP/21) implémenté au niveau de la station S3. Expliquer comment un utilisateur sur Internet peut se connecter à 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) 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).
4) S4 peut-il exécuter une attaque TCP syn flooding sur S1 (TCP syn flooding: Etablir plusieurs connexion successives semi-ouvertes afin de saturer la pile TCP de la victime)

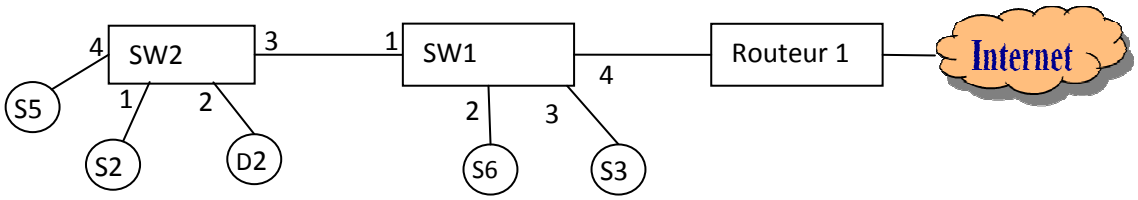
Correction du TD1 : attaques réseaux

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 sur son port P une trame venant d'une source S d'adresse MAC MAC_S, il ajoute dans sa table de commutation le triplet (MAC_S, P, temporisateur)

2) Expliquer le rôle des temporisateurs au niveau des entrées des tables de commutation ?

   ➔ Si le temporisateur expire et que le commutateur n'a pas reçu de trames de la part d'une source S d'adresse MAC MAC_S se trouvant sur son port P, le triplet (MAC_S, P, temporisateur) est supprimé de la table de commutation : la source a quitté le réseau a changé de port ou elle est inactive.

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 ?

   ➔ S2 sera marqué accessible à partir du port 4 et les trames qui lui sont destinées seront véhiculé vers S5 jusqu'au moment où S2 envoie une trame.

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 ?

   ➔ Oui, en inondant la table de commutation de SW2 (avec l'attaque ARP flooding par exemple). SW2 se comportera comme un HUB et les trames échangées entre S2 et D2 seront automatiquement reçu par S5.

5) Sachant qu'il est possible d'envoyer un ARP Reply sans sollicitation au préalable (Gratuious ARP Reply). Expliquer comment S5 peut récupérer tous les messages échangés entre S2 et D2 ?

   ➔Exécuter l'attaque ARP spoofing sur 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 ?

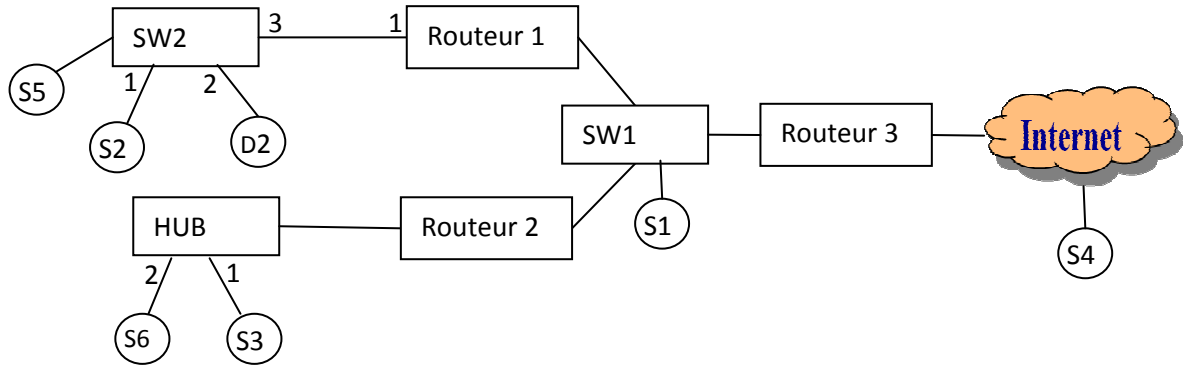
➔ Tuer le serveur légitime (par DHCP starvation). Puis, se transformer en serveur DHCP et préciser aux clients son adresse IP comme passerelle par défaut.

7) Supposons que que le routeur 1 implémente des règles qui rejettent tous les paquets destiné au serveur FTP (TCP/21) implémenté au niveau de la station S3. Expliquer comment un utilisateur sur Internet peut se connecter à ce serveur ?

➔ Utiliser, par exemple, l'attaque tiny fragment en précisant le numéro de port dans le second fragment.

Exercice 2 :

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



5) Quel sont les trames que la station S2 peut sniffer (écouter) ? Expliquer ?

➔ Les trames qui lui sont destiné ou celles envoyées en diffusion car le réseau auquel S2 est connecté est commuté.

6) 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).

➔ Seul les stations reliées à SW2 vu qu'ils sont les seuls qui peuvent recevoir les paquets « ARP Who is », paquets envoyés en diffusion et donc, rejetés par le routeur 1.

7) 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).

➔ Tous les nœuds du réseau puisque les réponses vont être envoyé en unicast à la victime et traverseront donc les routeurs.

8) S4 peut-il exécuter une attaque TCP syn flooding sur S1 (TCP syn flooding: Etablir plusieurs connexions successives semi-ouverte afin de saturer la pile TCP de la victime)

➔ Oui car c'est une attaque externe