LES ATTAQUES ETHERNET

1 – Introduction aux attaques Ethernet

Il ne faut pas sous estimer les attaques provenant de l'intérieur du réseau. Cela représente un réel risque, qu'il soit appliqué par un utilisateur de l'entreprise ou un pirate.

Le fait de se brancher sur le réseau Ethernet de l'entreprise nous ouvre déjà beaucoup de possibilités d'attaques. Le problème d'aujourd'hui des entreprises, c'est qu'elles ne prennent pas souvent conscience du danger interne et n'appliquent pas ou peu de protection LAN. Ainsi, des attaques DOS et d'écoute sont facilement réalisables sans aucune authentification.

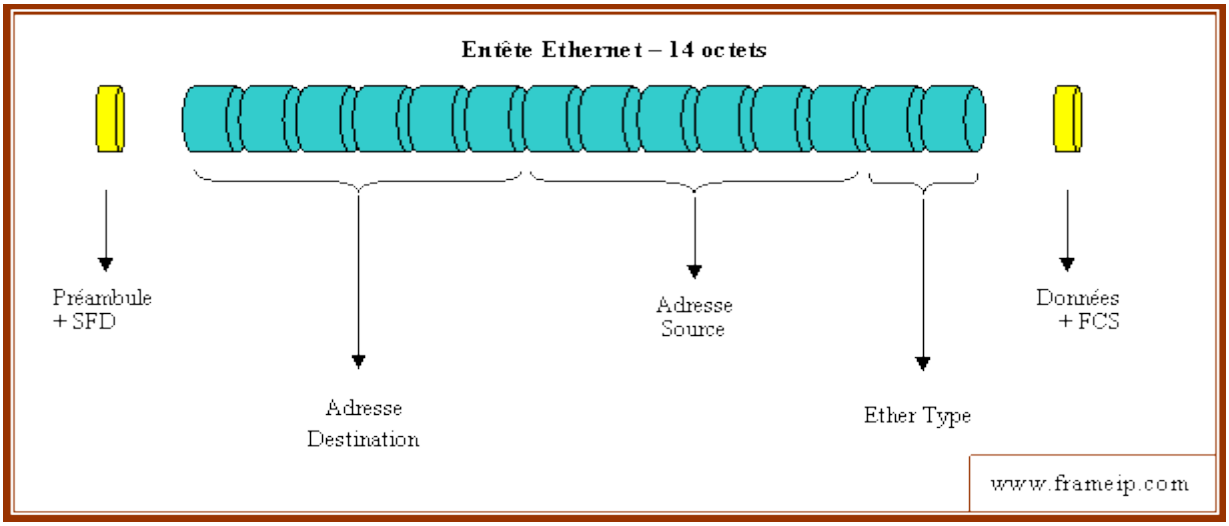
2 – Rappel des terminologies

2.1 – Protocole Ethernet

L'Ethernet est basé sur un principe de dialogue sans connexion et donc sans fiabilité. Le seul contrôle présent est le CRC (Cyclic Redundancy Code) qui valide la conformité reçue, mais pas son intégrité.

Ethernet est un protocole de discussion niveau 2 d'OSI et permet l'interconnexion de nombreux équipements du marché. Au point qu'aujourd'hui, 95% des équipements du marché sont basé sur Ethernet.

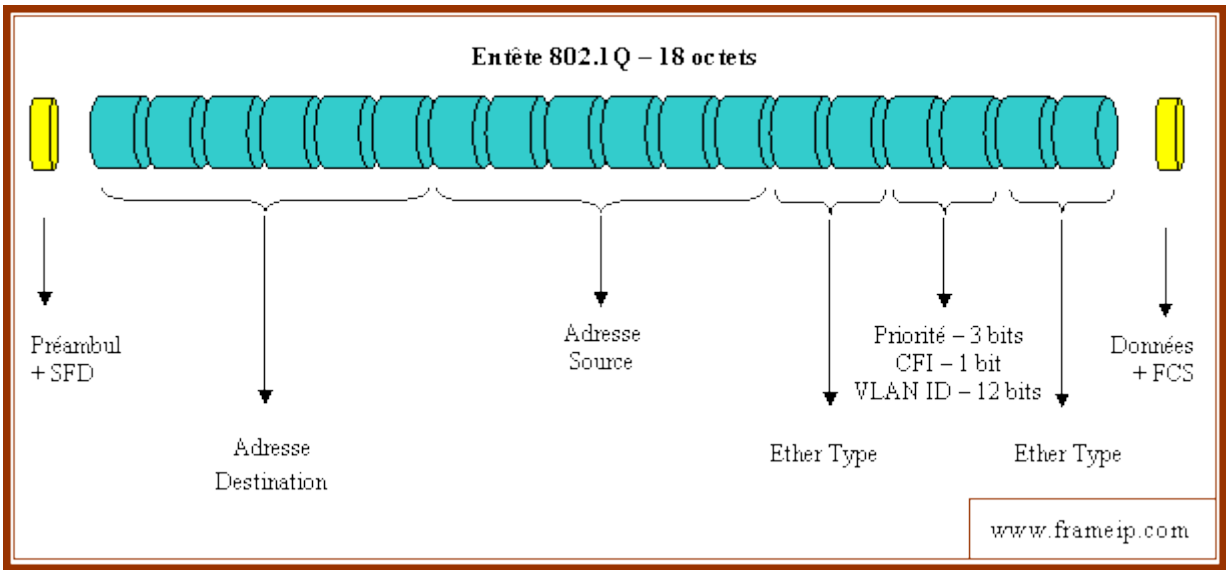
Voici l'entête d'une trame Ethernet :



2.2 – 802.1Q

Le protocole 802.1Q permet de réaliser des réseaux virtuelles sur une architecture Ethernet. Ces réseaux privée sont appelé VLAN. Pour cela, 4 octets sont ajoutés à l'entête Ethernet classique permettant, principalement, d'indiquer le numéro de VLAN et donc l'ID du sous réseau.

Voici l'entête d'une trame 802.Q :



De nouveau, comme pour Ethernet en mode classique, 802.1Q ne possède pas de sécurisation.

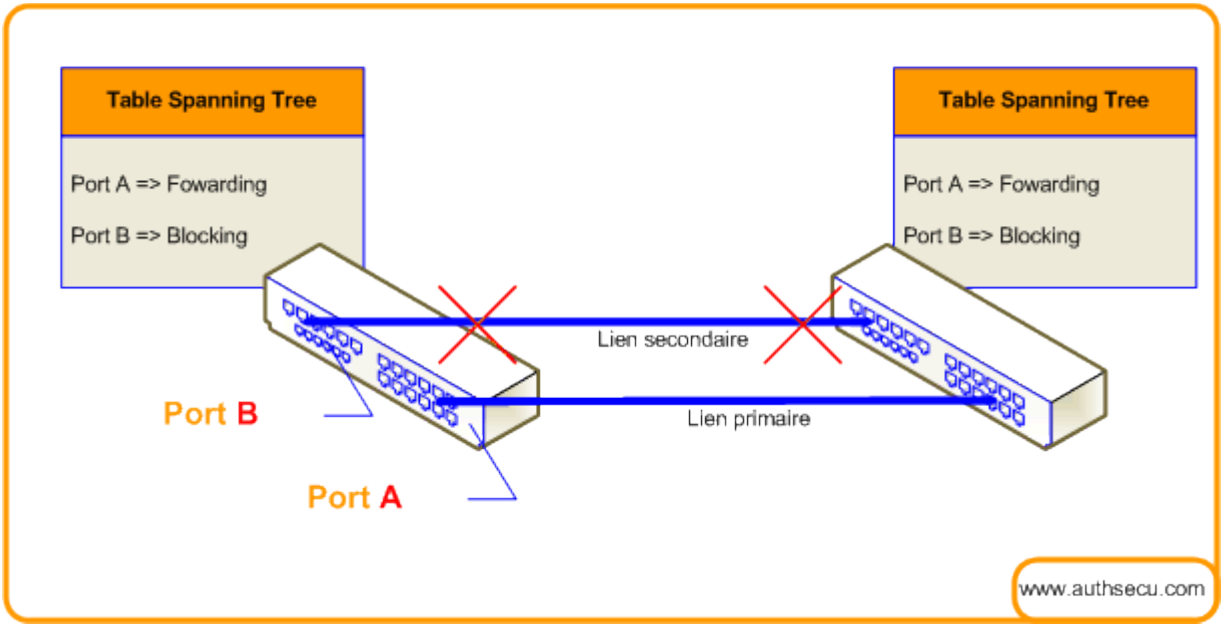
2.3 – Trunk VLAN

Un Trunk VLAN est un des modes de fonctionnement d'un raccordement entre deux Switchs. La fonction de ce lien Trunk est de transporter les VLAN à travers l'ensembre des commutateurs du LAN. Chaque VLAN reste distinct grâce à son taggue 802.1Q.

2.4 – Spanning Tree

Le protocole STP, répondant à l'appellation Spanning Tree Protocol définit dans dans le document IEEE 802.1d. L'algorithme Spanning Tree fournit des chemins redondants en définissant un arbre qui recense tous les commutateurs du réseau étendu LAN. Il permet ainsi de gérer les boucles Ethernet en offrant à chacun le chemin le plus court.

Schématiquement, dans le cadre de deux Switchs interconnectés deux fois, donc en boucle, STP positionnera le port A en mode « Forwarding » et le second en « Blocking ». Lors de la perte du lien primaire, Spanning Tree s'en apercevra et changera le mode du port B en « Fowarding » permettant ainsi au deux commutateurs de continuer à se voir.



3 – L'authentification Ethernet

Comme nous l'avons dit précédemment sur les attaques, Ethernet et 802.1Q ne travaillent pas en session et de possèdent pas nativement d'authentification. Cependant, plusieurs mécanisme et protocole normalisé peuvent être implémenter pour combler se manque. Voici les détails de ces concepts qui sont en réalité très peu déployer dans le monde de l'entreprise.

3.1 – Filtrage par @MAC

Cette méthode est basé sur un filtrage par port physique des Switchs. Pour cela, l'équipement de commutation Ethernet autorisera uniquement les adresses MAC spécifiées à se connecter. L'administrateur réseau obtient alors une sécurisation d'accès contre certaines attaques Ethernet et donc garantie que l'équipement réseau connecté est bien désiré.

Il y a moyen d'adapter cette méthode à 802.1Q en attribuant un VLAN e fonction de l'adresse MAC source. Ainsi, sur le port du Switch, il est possible d'indiquer que tel adresse MAC rentre dans le VLAN A alors qu'une autre adresse MAC appartient au VLAN B.

C'est clairement des fonctionnalités très intéressante et efficaces contre certaines attaques Ethernet, cependant il reste deux faiblesse à cette méthode qui sont :

- Une lourde administration qui est décentralisée. Même si certain constructeur permette un auto apprentissage des adresse MAC, on imagine rapidement l'impact d'un déploiement de 500 nouveau portable, d'un déménagement et etc. Et maîtrise de l'administrateur est purement

relatif dans un contexte qui est mouvant et espacé.

•Une sécurisation partielle car il est simple de changer l'adresse MAC de son PC afin de correspondre à ce que désire le Switch. Cela permet de se protéger facilement contre les utilisateurs, mais pas du tout contre les pirates.

3.2 – Filtrage par @IP

Cette méthode de sécurisation est aussi basé sur un filtrage par port physique des Switchs. Pour cela, l'équipement de commutation Ethernet attribua un VLAN en fonction de l'adresse IP Source. Ainsi, sur le port du Switch, il est possible d'indiquer que tel adresse IP rentre dans le VLAN A alors qu'une autre adresse MAC appartient au VLAN B.

C'est clairement aussi une fonctionnalité très intéressante et efficaces contre certaines attaques Ethernet, cependant il reste les deux mêmes faiblesses qui sont l'administration décentralisée et la sécurité par usurpation d'adresse IP.

3.3 – Filtrage par *

Cette méthode de sécurisation est aussi basé sur un filtrage par port physique des Switchs. Pour cela, l'équipement de commutation Ethernet attribua un VLAN en fonction de n'importe quel champs de la trame. Cela peux très bien être la priorité TOS, le Port TCP demandé, la longueur de trame et tout autres champs.

Ainsi, sur le port du Switch, il est possible d'indiquer que les flux HTTP (TCP 80) rentre dans le VLAN A alors les autres flux appartiennent au VLAN B.

C'est clairement aussi une fonctionnalité très intéressante et modulable contre certaines attaques, cependant il reste les deux mêmes faiblesses qui sont l'administration décentralisée et la sécurité par modification des champs.

3.4 – 802.1X

Cette méthode de sécurisation repose sur le protocole 802.1X normalisée par les RFC 3580 (IEEE 802.1X) et RFC 3748 (EAP). Elle repose sur une authentification contrôlé par le Switch. Pour cela, chaque équipement Ethernet qui désire dialoguer à travers le Switch, devra au préalable s'authentifier auprès d'une base de compte. En fonction du compte employé, il est possible de fournir les droits et fonctionnalités suivantes :

•Autorisation ou pas à dialoguer sur ce port de Switch

•Appartenance à un VLAN Spécifique. Ainsi, peux importe le port physique utilisée, la carte réseau sera toujours dans le même VLAN attribuée dynamiquement

•Un marquage du champs TOS

•Et bien d'autres possibilité tel que le routage, le filtrage firewalling, le chiffrement …

Ce login et mot de passe n'est pas forcement imposé à l'utilisateur et il peut être intégré dans les paramètres du driver pilotant la carte réseau Ethernet. De plus, la base de compte est soit stockée sur chaque Switch, soit centralisée sur un annuaire et requêtée via RADIUS (Protocole le plus courrant du monde industriel).

4 – Les attaques Ethernet

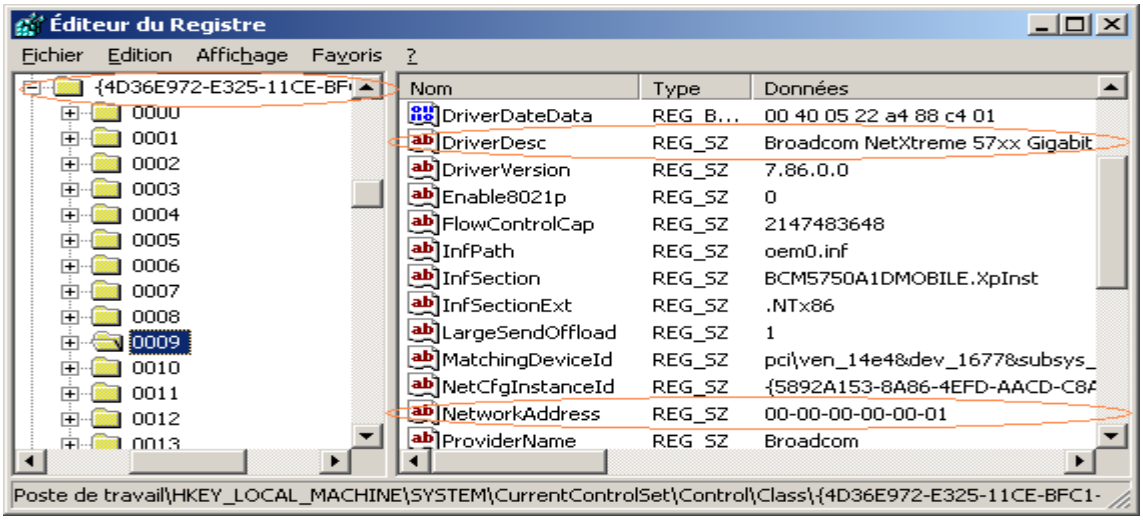
4.1 – Attaque avec usurpation d'identité

Ce n'est pas une attaque en soit, mais un moyen de se cacher. Cela permet d'éviter au maximum d'être repéré et d'être loggué. Pour cela, il ne faut pas utiliser sa réelle adresse MAC, mais une fictive. Deux moyens sont disponibles pour effectuer du MAC Spoofing. Le premier est basé sur l'utilisation d'outil tel que frameip.exe qui permet de forger des paquets avec l'adresse MAC source de votre choix. Le second moyen d'attaque est de changer les paramètres de son driver Ethernet géré par le système d'exploitation. Voici comment cela peux être réalisée :

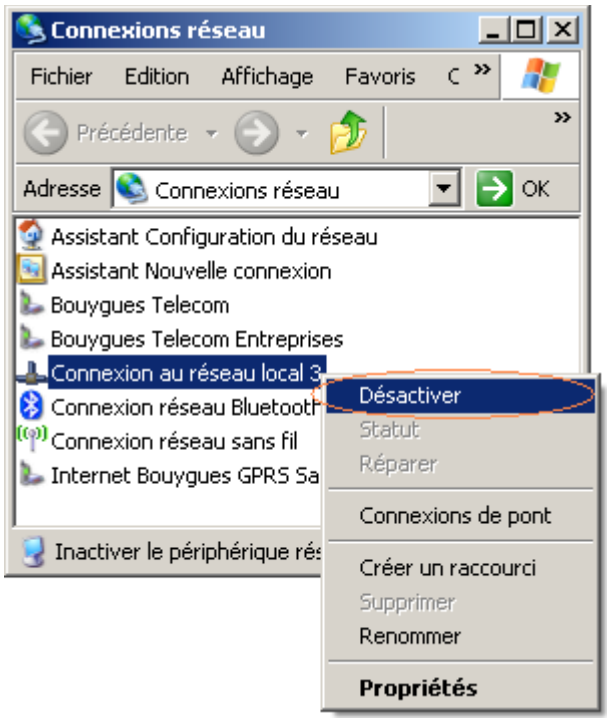
4.1.1 – Sous Windows

Vous devez modifier la base de registre afin d'insérer l'adresse MAC fictive. Voici les différentes étapes à suivre :

- Exécuter l'utilitaire regedit.exe
- Ouvrir la clé HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}\
- Parcourir chaque sous clé 001, 002, … et regarder la valeur de « DriverDesc » afin de trouver le nom de l'interface désirée
- Insérer dans la sous clé précédemment sélectionnée, une valeur de type chaîne nommé « NetworkAddress »
- Appliquer l'adresse MAC à cette valeur de type chaîne avec des traits d'unions de séparation. Voici un exemple 12-34-56-78-90-ab



Après cette insertion, il ne vous reste plus qu'à redémarrer votre interface en effectuant un clique droit dessus – disable puis enable



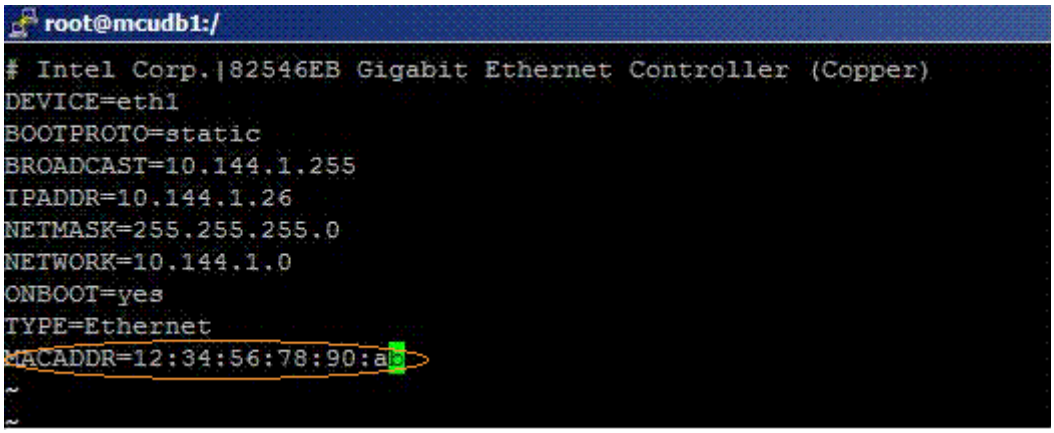
4.1.2 – Sous Linux

Voici les commandes permettant de changer son adresse MAC :

```
/etc/init.d/network stop
ip link set eth0 address 12:34:56:78:90:ab
/etc/init.d/network start
```

Cependant, après un reboot de la station, l'adresse MAC d'origine sera reprise. Pour que cette action soit persistante, il faut alors modifier le fichier ifcfg-eth1 comme cela :

vi /etc/sysconfig/network-script/ifcfg-eth1



/etc/init.d/network restart

4.1.3 – Sous Cisco

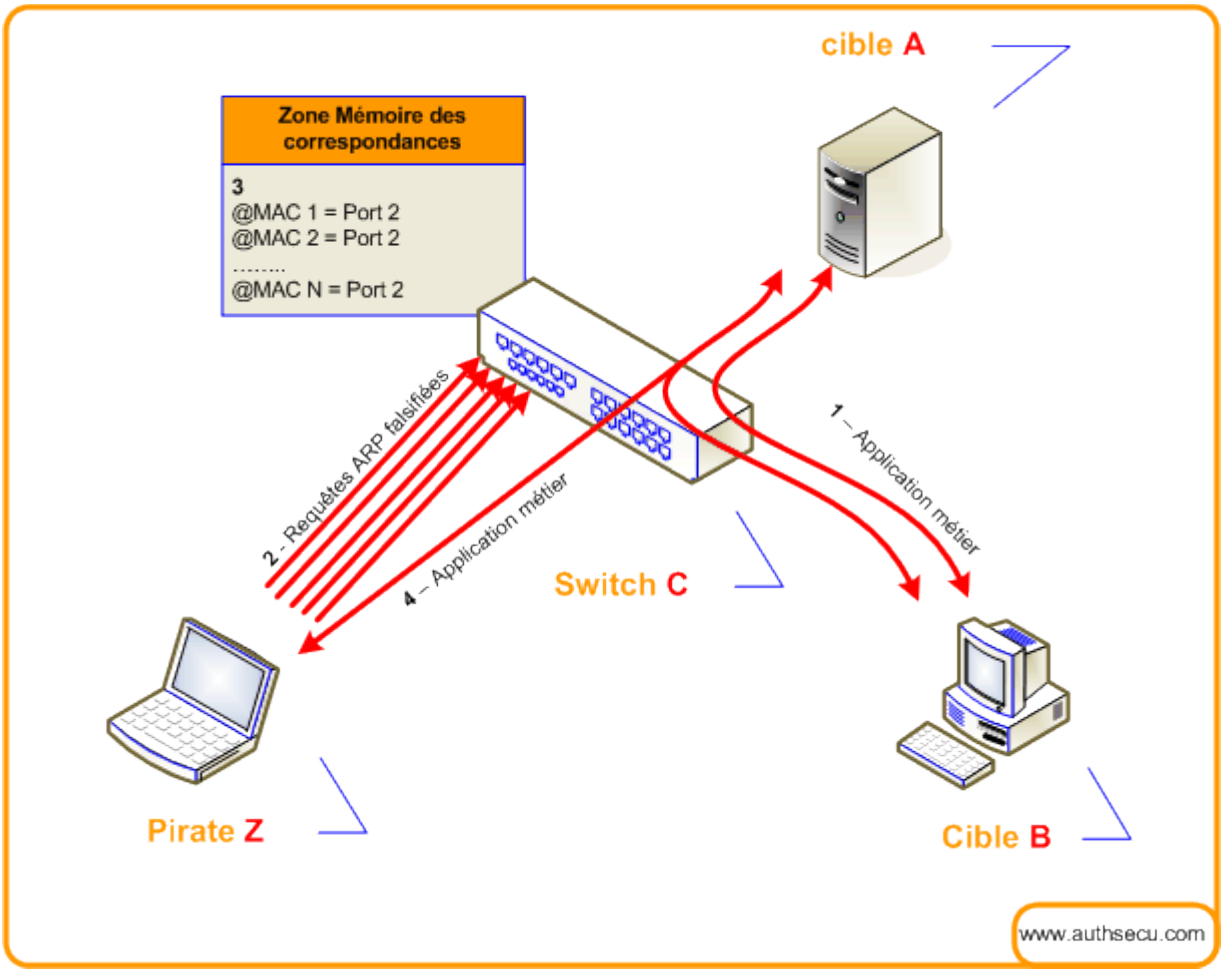
Vous devez insérer l'adresse MAC en config-if grâce à la commande mac-address. Voici un exemple de modification :

mac-address 0000.1111.2222

4.2 – Attaque MAC Flooding

Cette attaque est basée sur l'envoi massif de requête et réponse ARP. Chaque requête doit avoir une adresse MAC différente, ainsi les différents Switchs du LAN vont apprendre cette correspondance entre l'adressa MAC et le port physique. Avec une attaque d'envoi massif, le Switch saturera rapidement sa mémoire qui est limitée. Cela dépend du constructeur, de l'équipement et de la version, mais les conséquences peuvent être multiple comme par exemple :

- Buffers overflow de la mémoire gérant les correspondances (cette conséquence n'est plus réaliste de nos jours)
- Arrêt du fonctionnement du Switch ne pouvant plus commuter de trame
- Passage du Switch en mode HUB permettant ainsi à l'attaquant d'effectuer de l'écoute. Le schéma ci dessous montre le procédé de cette attaque :



1 – Les cibles A et B s'échangent des informations normalement
2 – Le pirate Z envoi plein de requêtes ARP avec des adresses MAC différentes
3 – Le Switch C met à jour sa table de correspondance jusqu'à saturation de la mémoire
4 – Les cibles A et B s'échangent des informations, mais le pirate les reçoit aussi du fait que le Switch fonctionne désormais en HUB

Ils existent plusieurs possibilités afin d'éviter cette attaque. Par exemple, il est possible :

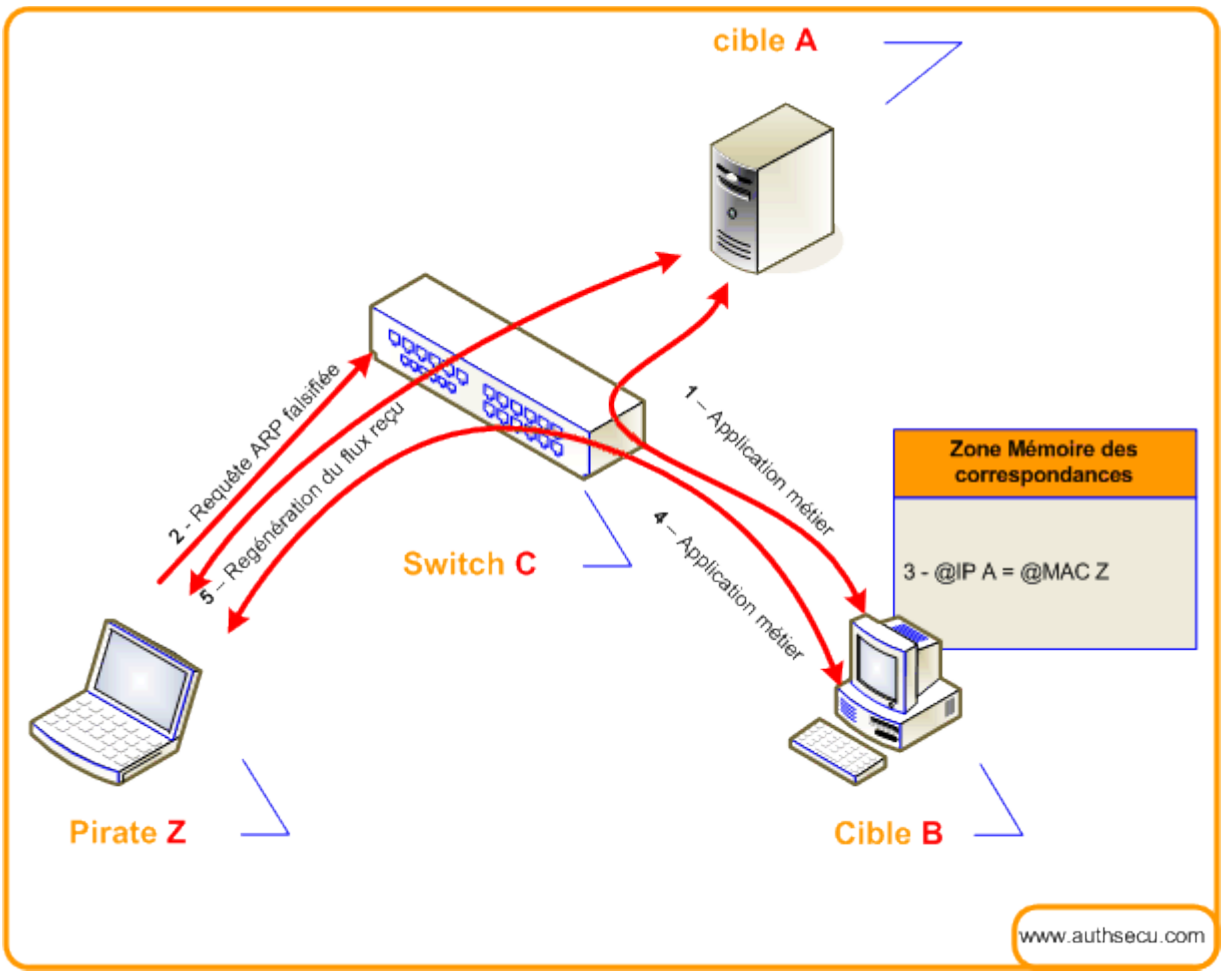
- De n'autoriser qu'une liste d'adresse MAC prédéfinie par port. Cisco propose cela via la commande « switchport port-security mac-address H.H.H »
- D'appliquer un filtre sur le nombre de correspondance maximum par port. 3 modes existent qui sont « protect », « restrict » et « shutdown »
- D'utiliser l'authentification 802.1X

4.3 – Attaque ARP Poisoning

Cette attaque Ethernet se base sur l'envoi d'informations de requêtes ARP falsifiées. L'intérêt ce cette attaque est de faire croire aux autres que l'adresse IP de la cible correspond à une adresse MAC que l'on choisie. Ainsi, les différents équipements du LAN apprennent la mauvaise correspondance.

La conséquences de cette attaque peuvent être multiple tel que :

- La rupture de toutes communications de la cible IP. Les cibles sont souvent les serveurs et les routeurs rendant indisponible les services associés
- L'écoute des flux de la cible. Pour cela, il faut spécifier l'adresse MAC du hackeur dans l'information ARP. Le schéma ci dessous montre le procédé :



1 – Les cibles A et B s'échangent des informations normalement
2 – Le pirate Z envoi une requête ARP empoisonnée
3 – La cible B met à jour sa table de correspondance
4 – La cible B envoi ses donnée au pirate Z en croyant s'adresse à la cible A
5 – La pirate transfert les données reçues vers la cible A en mettant sa réelle adresse MAC source afin de s'assurer de recevoir les réponses

Ils existent plusieurs possibilités afin d'éviter cette attaque. Par exemple, il est possible :

- De n'autoriser qu'une liste d'adresse MAC prédéfinie par port. Cisco propose cela via la commande « switchport port-security mac-address H.H.H »
- D'utiliser une détection IDS sur le Switch
- D'utiliser l'authentification 802.1X

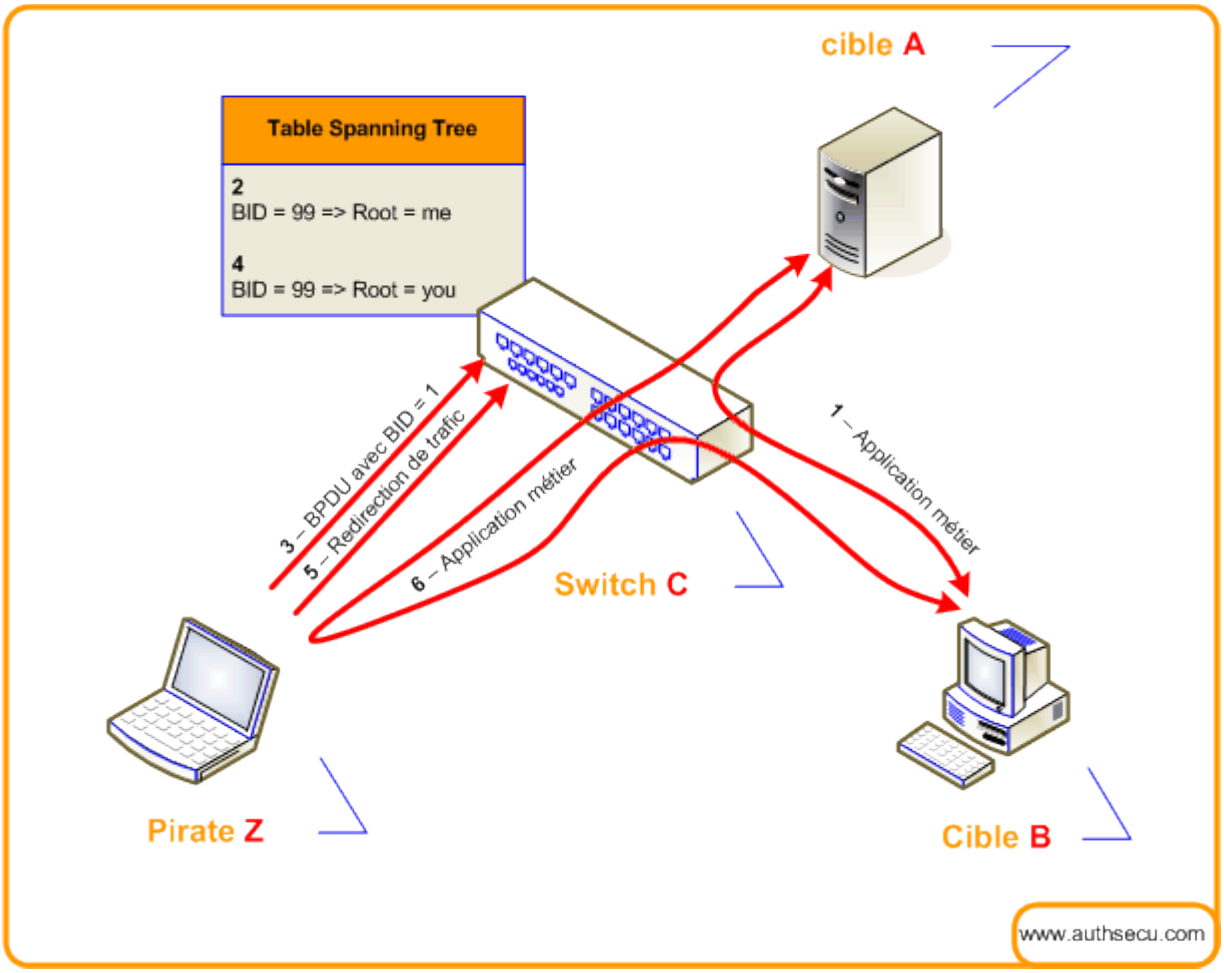
4.4 – Attaque spanning tree

Cette attaque se base sur l'envoi de trames BPDU (bridge protocol data units) à destination du Switch cible. Dans un environnent Sapnning-Tree, il y a un seul Switch qui est élu root (maître) servant de référence pour les coûts et les chemins. Ces trames BPDU émises avec un BID (Bridge ID) très petit, obligera

les commutateurs à recalculer le nouveau root.

Cela dépend du constructeur, de l'équipement et de la version, mais les conséquences peuvent être multiple comme par exemple :

- Suite à la saturation processeur provoquée par les calculs permanents, les commutateurs ne commutent plus ou crash littéralement. Il est même possible que les Switchs basculent alors en mode HUB permettant ainsi à l'attaquant d'effectuer de l'écoute.
- Suite à l'envoi d'un BID plus petit que ceux des Switchs, l'attaquant se retrouvera alors élu comme maître de l'environnement Spanning-Tree. Ainsi, le hackeur pourra redéfinir la topologie à sa guise et ainsi intercepter tous les trafics qu'il désir. Le schéma ci dessous montre le procédé :



1 – Les cibles finales A et B s'échangent des informations normalement
2 – Le Switchs est le maître du contexte Spanning Tree
3 – Le pirate Z envoi une trame BPDU avec un BID très faible
4 – Le commutateur admet que le pirate Z soit devenu le maître du contexte STP
5 – Le hacker redéfinis la topologie afin de rediriger les flux vers lui
6 – Les cibles A et B s'échangent des informations, mais le pirate les reçoit aussi

Ils existent plusieurs possibilités afin d'éviter cette attaque. Par exemple, il est possible :

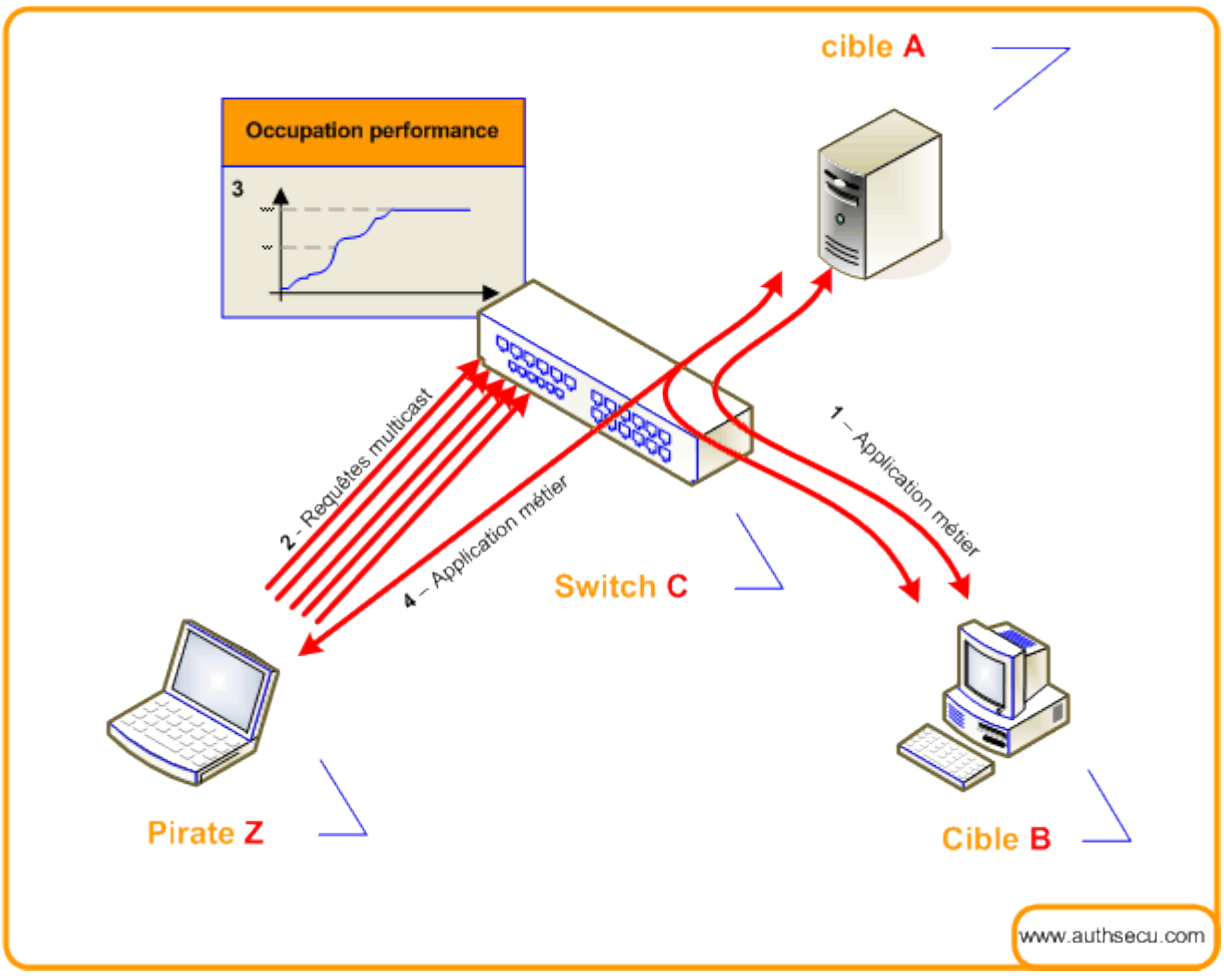
- D'activer STP (Spanning Tree Protocol) uniquement sur les ports interconnecté à un autre commutateur
- D'activer STRG (Spanning Tree Root Guard) sur les commutateurs permettant de laisser passer les BPDU tant que le port en question ne demande pas à devenir maître dans l'instance Spanngin Tree
- D'activer le BPDU Guard sur les Switchs afin de bloquer tous les type de message BPDU du port en question.

4.5 – Attaque saturation processeur via BPDU

Cette attaque se base sur l'envoi massive de datagramme multicast (consommateur de processeur distant) à destination du Switch. L'intérêt est de changer le mode de fonctionnement du Switch afin qu'il travail en HUB. Cela est possible car certain Switch, à l'approche de la saturation processeur, préfère basculer en mode HUB afin de préserver une priorité sur l'exploitation.

Cela dépend du constructeur, de l'équipement et de la version, mais les conséquences peuvent être multiple comme par exemple :

- Buffer over flow du Switch (cette conséquence n'est plus réaliste de nos jours)
- Impossibilité au Switch de commuter la plus part des trames
- Passage du Switch en mode HUB permettant ainsi à l'attaquant d'effectuer de l'écoute. Le schéma ci dessous montre le procédé :



1 – Les cibles finales A et B s'échangent des informations normalement
2 – Le pirate Z flood le Switch avec des requêtes Multicast
3 – Le Switch C voit son occupation processeur monter en flèche et bascule en mode HUB
4 – Les cibles A et B s'échangent des informations, mais le pirate les reçoit aussi

Ils existent plusieurs possibilités afin d'éviter cette attaque. Par exemple, il est possible :

- d'utiliser des Switchs travaillant en mode distribué apportant une gestion processeur décentralisé à chaque port
- d'applique un filtre IP sur chaque port afin d'éviter les requêtes à destination du Switch lui même

4.6 – Attaque VLAN via Cisco DTP

Cette attaque se base sur l'envoi d'une trame forgée avec un tague 802.1Q. L'intérêt est de pouvoir discuter avec des cibles membres d'un VLAN déférent du siens. Pour cela, si le Switch intègre un protocole de type DTP (Dynamic Trunking Protocol), lorsqu'il verra arriver une trame taggé, il changera le port du pirate en mode trunck. Ce qui permet alors au hackeur de pouvoir, en

forgeant ses trames, discuter avec n'importe quel VLAN.

Le moyen de protection contre cette attaque Ethernet est simple, il suffit de ne pas utiliser des protocoles comme DTP.

4.7 – Attaque 802.1Q caché

Cette attaque se base sur l'envoi d'une trame forgée avec deux tagues 802.1Q. L'intérêt est de pouvoir discuter avec des cibles membres d'un VLAN déférent du siens. Pour cela, le pirate doit être positionné sur un port Trunk VLAN natif. Le Switch supprimera le premier tag lorsqu'il verra arriver une trame taggée qui ne devrait pas l'être sur un VLAN natif. L'astuce étant d'avoir caché derrière le premier tag, un second correspondant à la cible.

Le moyen de protection contre cette attaque Ethernet consiste à bien maîtriser les modes de ses ports afin d'éviter des erreurs d'administration. Il est aussi intéressant de ne pas prendre des produit bon marché afin que le Switch soit assez intelligent pour comprendre le double VLAN.

5 – Conclusion

Il est important de prendre conscience des risques lié au réseau LAN d'entreprise. La sécurité informatique Interne est réelle et obligatoire, il est alors bien de commencé déjà par sécuriser l'accès via les commutateurs contre l'ensemble des attaques Ethernet.

De plus, comme sur l'Internet, il faut analyser, consolider et archiver les logs des différents équipements réseaux.