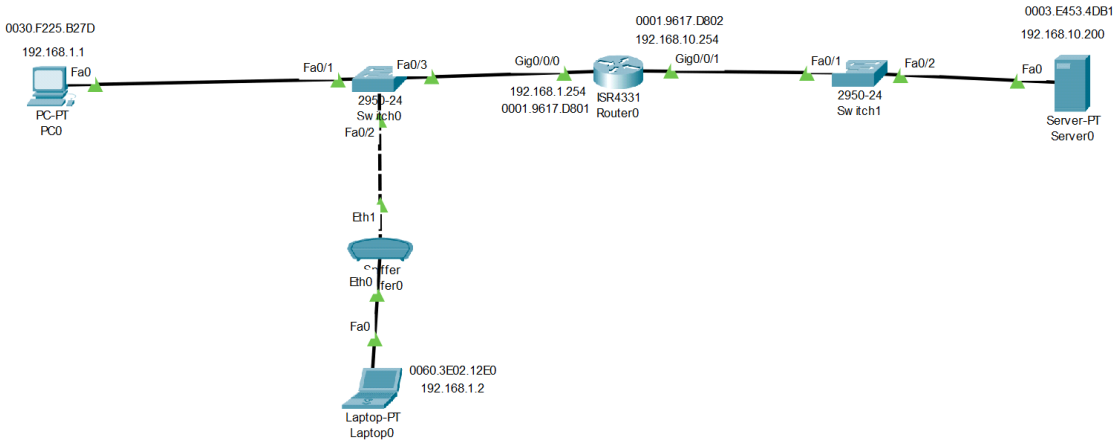
Man In The Middle

Introduction : Dans ce TP nous allons voir une attaque « Man In The Middle » en empoisonnant un cache ARP, nous allons réaliser celui-ci sur Cisco Packet Tracer en créant un petit réseau normal pour ce test et en y installant un sniffeur et un pc d'attaquant, voici le schéma du réseau :

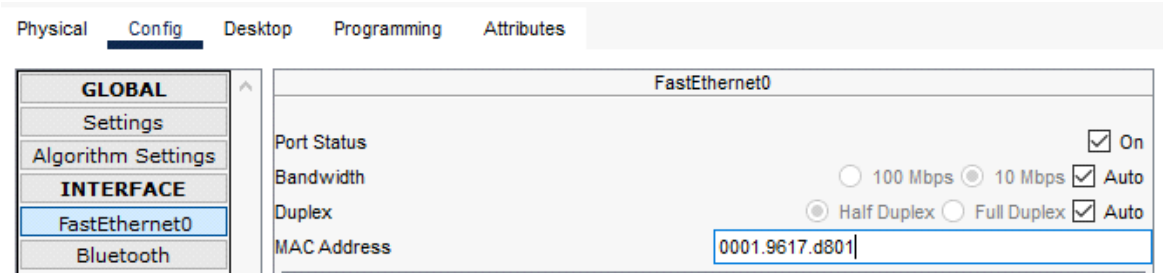


- Le pc user : 192.168.1.1
- Le pc attaquant : 192.168.1.2

-
```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.1           0030.f225.b27d        dynamic
  192.168.1.254         0001.9617.d801        dynamic
```
Sur le pc de l'attaquant « arp –a » nous permet de récupérer l'adresse ip et la mac adresse de la passerelle et d'un autre pc connecté au switch :

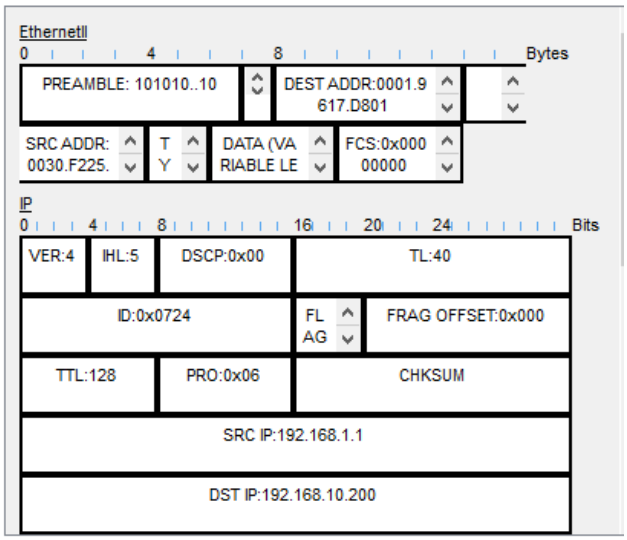
```
Switch#show mac-address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.9617.d801    DYNAMIC      Fa0/3
   1    0030.f225.b27d    DYNAMIC      Fa0/1
   1    0060.3e02.12e0    DYNAMIC      Fa0/2
```

- Chaque pc ping la passerelle, avec la commande « show mac-address-table » sur le switch nous permet de récupérer les adresses mac et le port de chaque appareil qui envoi ou reçoit une trame :

- 

Changement de l'adresse mac afin de se faire passer pour le routeur et de recevoir les trames passantes :

Nous voyons dans le sniffeur que les trames sont interceptées, et donc si des informations importantes et personnelles aller être envoyé au même moment, les informations seront interceptées par l'attaquant.



Conclusion : Dans ce TP nous avons vu la facilité à intercepter des informations si le réseau n'est pas sécurisé, cependant il existe des façons pour sécuriser le réseau, comme par exemple le chiffrage des échanges qui permet que même si les paquets sont interceptés ils seront chiffrés et donc pas lisible. Il y a aussi la limitation d'adresse mac par port qui permet que le port soit bloqué s'il obtient une autre adresse mac. Enfin la prévention, c'est-à-dire qu'avoir des équipements à jour, un Wi-Fi sécurisé…

Cela permettrai de limiter les failles dans le réseau.