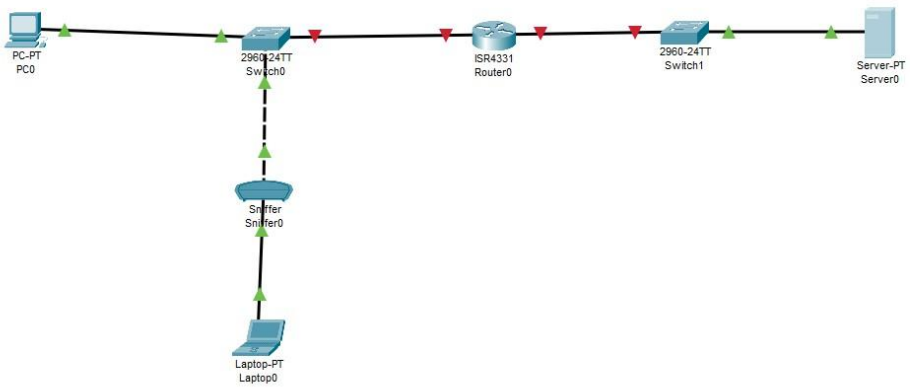
Lebeau Mathéo TP ARP POISONNING BTS SIO 2

Intro :

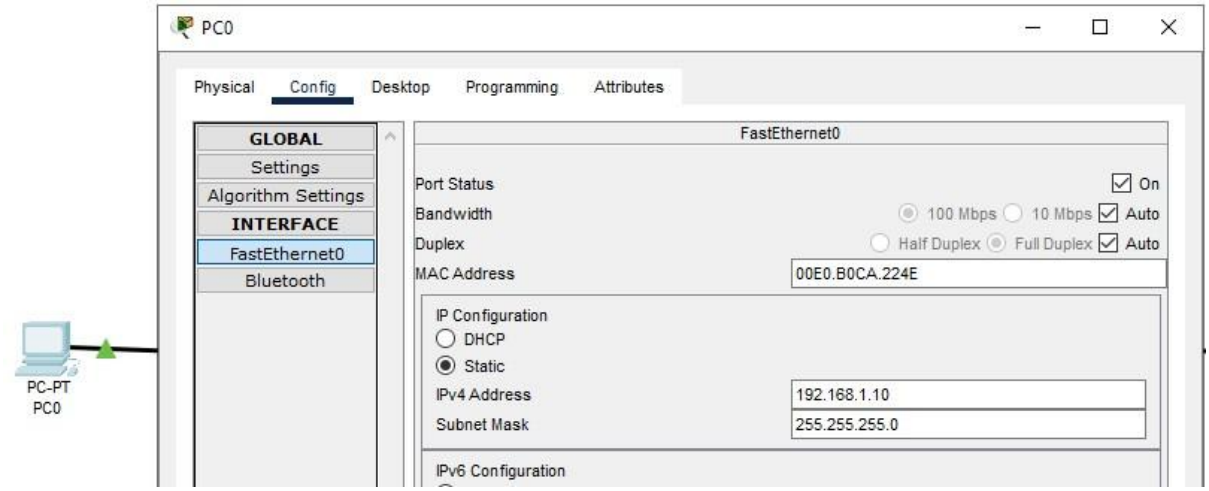
Nous allons aujourd'hui utiliser le logiciel cisco packet tracer pour simuler une usurpation d'adresse mac et réaliser une attaque de type man in the middle pour voir toutes les informations transitant par la fausse passerelle.

Pour commencer une fois l'application installée on va ajouter les différents composants nécessaires dans la barre de menu se trouvant en bas et on les lie entre eux avec des cables.

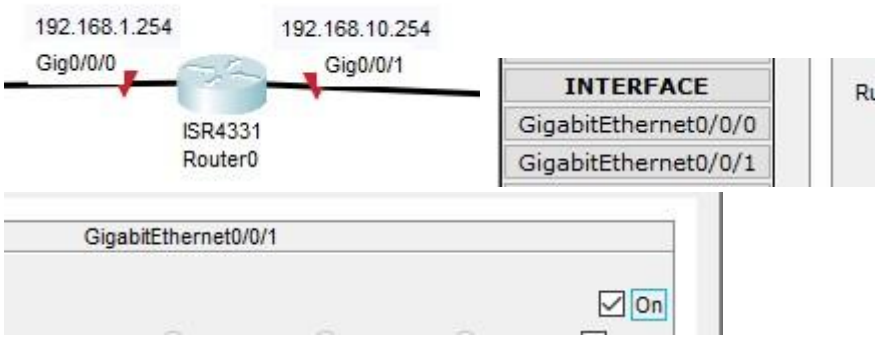
On obtient alors ceci sans configuration.



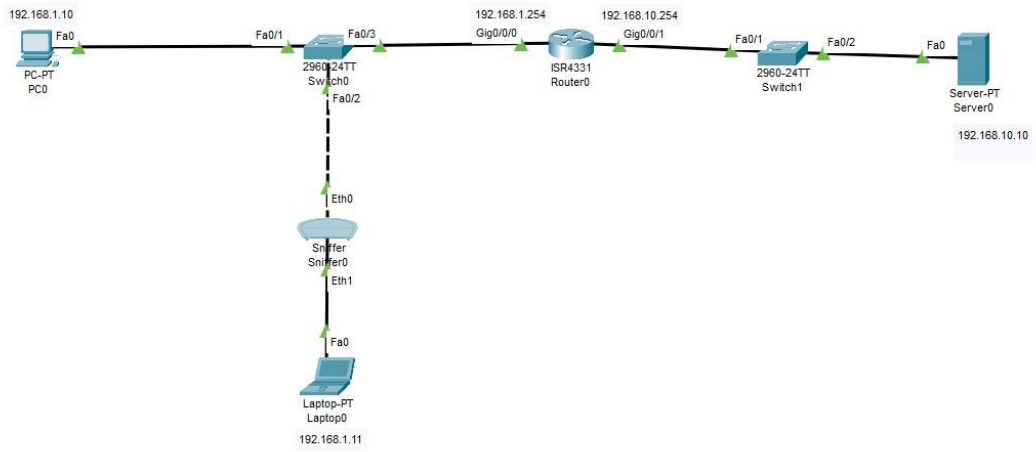
Puis on va attribuer des ip aux deux machines et au server pour commencer en double cliquant dessus et dans fastethernet on fera de même pour les deux autres.



Puis on attribuera au routeur principal deux ip pour les deux “côtés” de notre réseau de la même façon que pour les PC seulement il faudra le faire dans deux onglets différents et ne pas oublier d’activer les ports.



Tous nos voyants passent alors au vert.



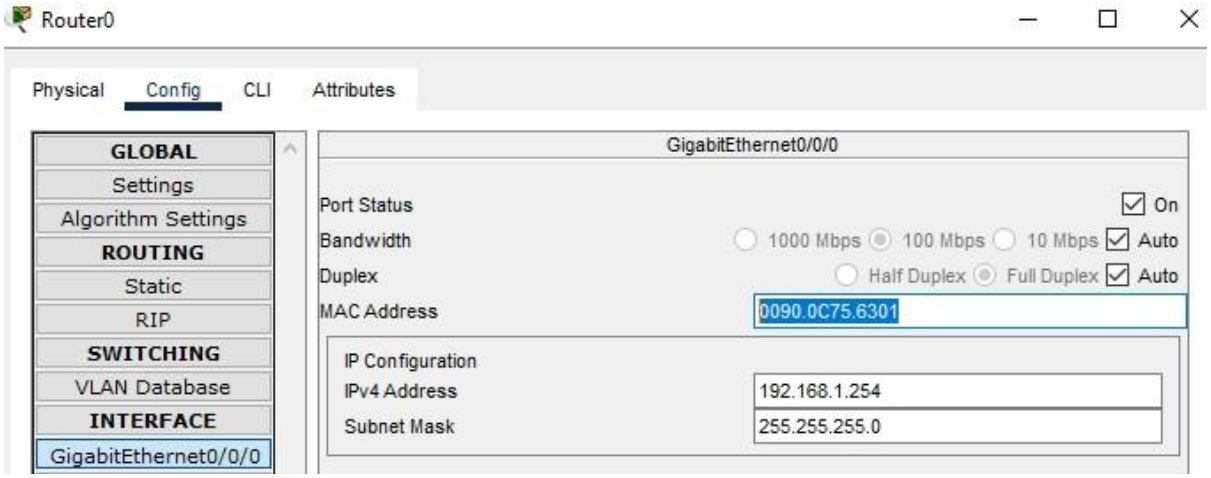
On a maintenant fini notre infrastructure et on va pouvoir commencer les manipulations qui vont se dérouler en plusieurs étapes.

-Tout d'abord on va vouloir récupérer l'adresse mac de la passerelle du réseau en question, pour ce faire on va préparer notre attaque avec quelque dernier test.

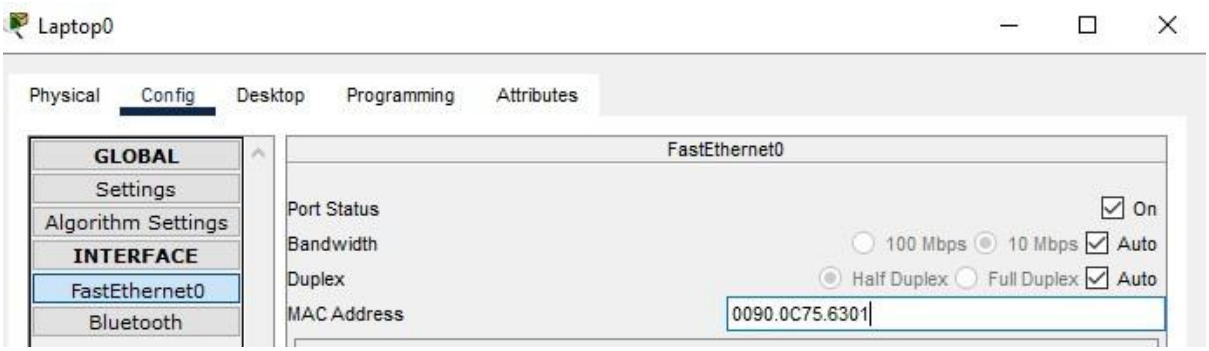
Aussi on va entrer la passerelle dans le pc client pour qu'il puisse accéder au server web.

Et inversement avec 192.168.10.254 sur le server pour qu'il puisse rejoindre l'autre réseau et on vérifie avec un ping et un test en se connectant à la page web.

Tout est bon on va pouvoir simuler que l'attaquant obtient l'adresse mac de la passerelle on va la récupérer sur le routeur et la rentrer dans le pc de l'attaquant.



Et on la rentre dans le pc attaquant.



-On va ensuite faire plein de ping sur le pc client depuis le pc attaquant pour faire correspondre sa passerelle sur le pc de l'attaquant et non pas le routeur, c'est le début de l'attaque. Pour ce faire on utilisera : ping 192.168.1.10 -a

On a l'ip du pc client et le –a fera des requêtes en continu et on va choisir de faire ça pendant toute la durée de l'attaque pour que le routeur ne reprenne pas le dessus on ira ensuite

vérifier si dans la table arp du pc client on a bien l'ip du pc attaquant et on verra enfin si on capte le packet avec le pc attaquant.

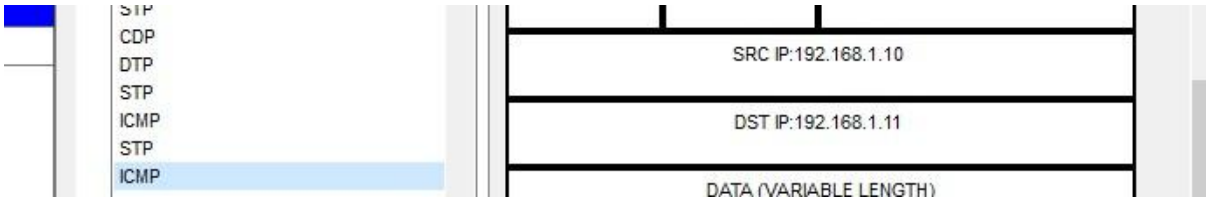
Une fois le ping lancé on voit dans la table arp du switch que on passe par un chemin différent de l'habituel

```
Switch>show mac-address-table
          Mac Address Table
-------------------------------------------

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

   1    0090.0c75.6301    DYNAMIC     Fa0/2
   1    00e0.b0ca.224e    DYNAMIC     Fa0/1
Switch>
```

Et on voit bien le packet sur le sniffer qui va sdu pc client jusqu'au server et le pc attaquant intercepte bien les packets



Et le pc client ne peut plus accéder à la page web

Et une fois le ping arrêté tout revient à la normale et le routeur redevient la passerelle et on peut à nouveau accéder à la page web.

Conclusion :

Ce type d'attaque à comme principal faiblesse le fait qu'il faille accéder au réseau aussi bloquer les ports non utilisés des switches et n'autoriser que quelques adresses mac par ports ou encore avoir une table arp statique. Ces méthodes vont empêcher l'attaque il existe encore plein de méthodes comme un IPS ect.