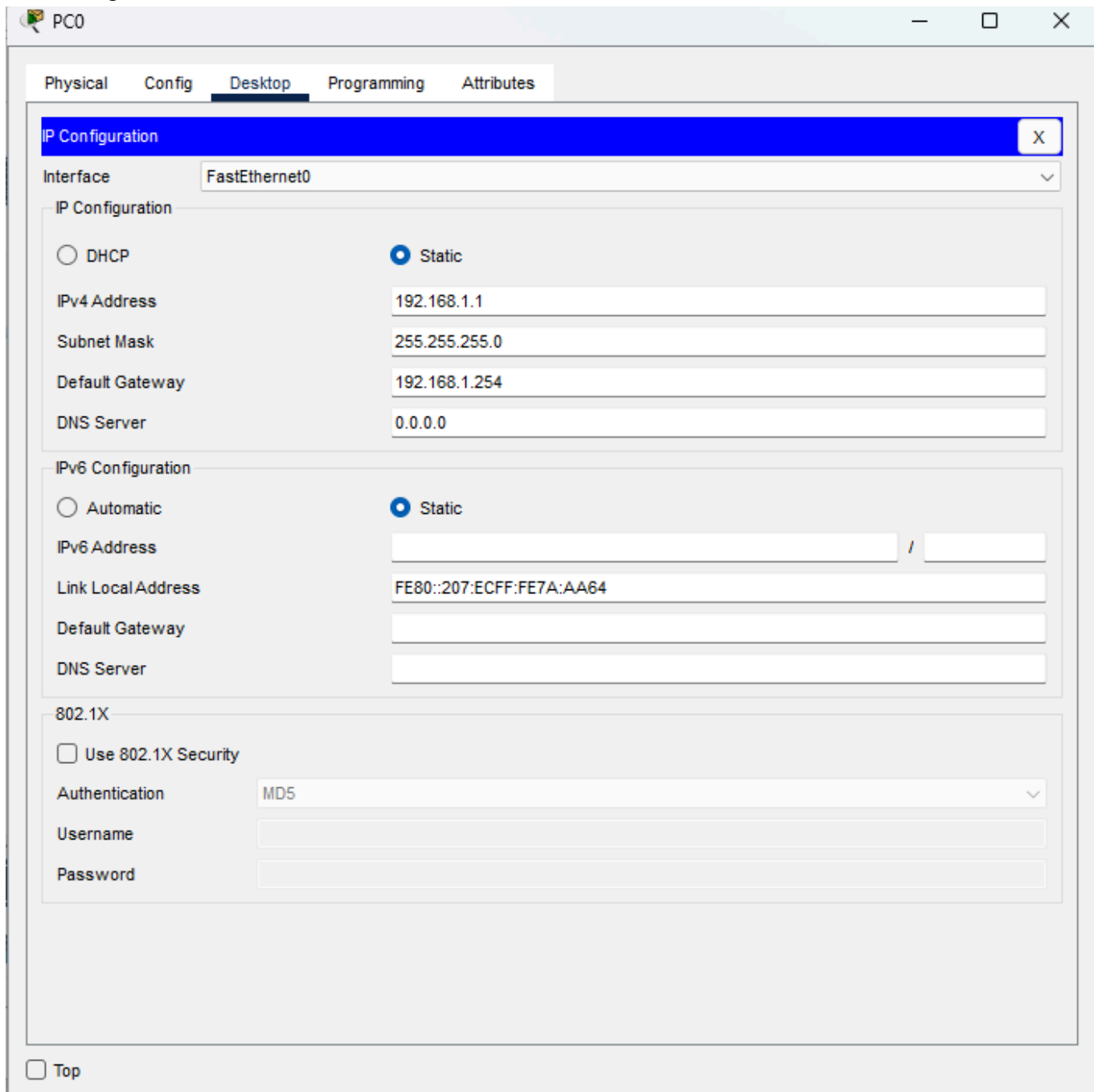


Attaque spoofing ARP

Cas Pratique PacketTracer :

--->Configurer PC Client :



The screenshot shows the 'PC0' configuration window in Packet Tracer, with the 'Desktop' tab selected. The 'IP Configuration' section is expanded, showing the 'FastEthernet0' interface. The 'Static' radio button is selected for both IPv4 and IPv6 configurations. The IPv4 settings are: IP Address 192.168.1.1, Subnet Mask 255.255.255.0, Default Gateway 192.168.1.254, and DNS Server 0.0.0.0. The IPv6 settings are: Automatic radio button selected, IPv6 Address field empty, Link Local Address FE80::207:ECFF:FE7A:AA64, Default Gateway field empty, and DNS Server field empty. The '802.1X' section is also visible, with 'Use 802.1X Security' unchecked, Authentication set to MD5, and Username and Password fields empty.

PC0

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.1.1

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.254

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::207:ECFF:FE7A:AA64

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

☐ Top

-->Configurer le pc attaquant (supposons qu'il a obtenu une adresse du réseau grâce au DHCP)

```

C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2E0:F9FF:FEEB:23C
    IPv6 Address . . . . .: ::
    IPv4 Address. . . . .: 192.168.1.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                192.168.1.254

Bluetooth Connection:

```

-->Configurer le serveur web

Server0

Physical Config Services **Desktop** Programming Attributes

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.10.200

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

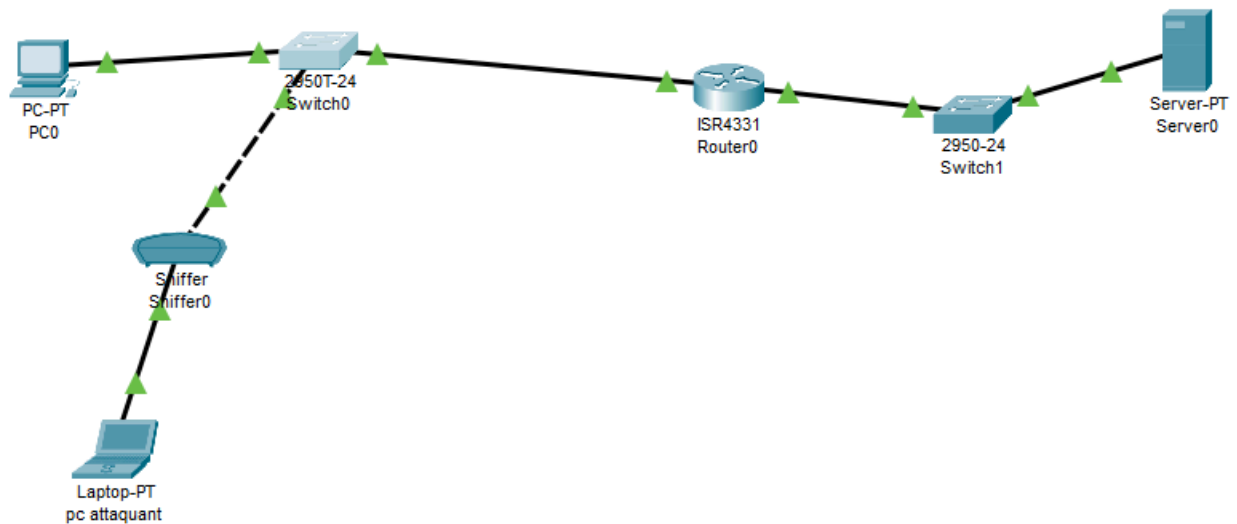
☐ Automatic ☒ Static

-->Configurer le routeur

Device Name: Router0
Device Model: ISR4331
Hostname: Router

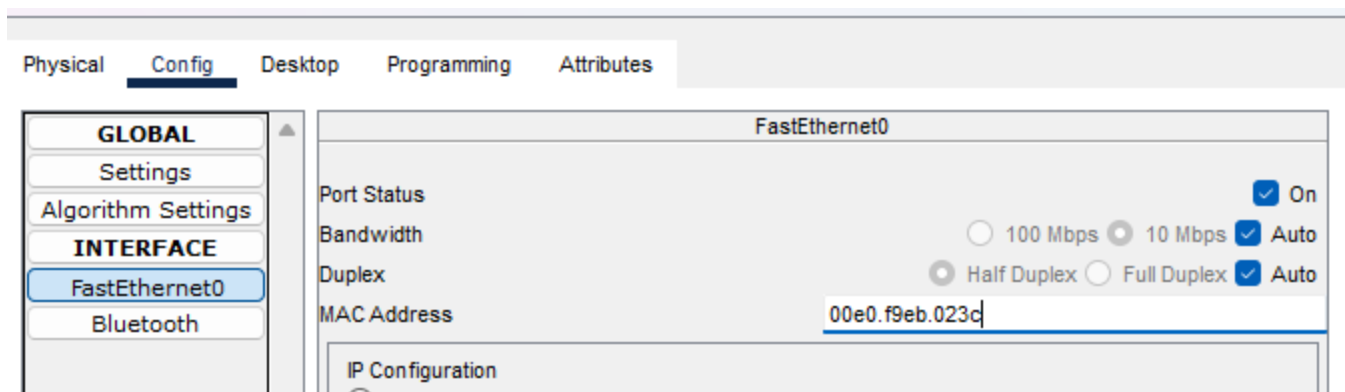
Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet0/0/0	Up	--	192.168.1.254/24	<not set>	00D0.FF47.5B01
GigabitEthernet0/0/1	Up	--	192.168.10.254/24	<not set>	00D0.FF47.5B02
GigabitEthernet0/0/2	Down	--	<not set>	<not set>	00D0.FF47.5B03

-->Réseau après la mise en place



-->DEBUT DU SPOOFING

-->Récupérer depuis le pc attaquant l'adresse MAC du routeur et la mettre à notre pc



--> Ouvrir le switch et vérifier sur la table des adresses MAC que le port de l'adresse MAC attaquant a changé.

-->Avant

Vlan	Mac Address	Type	Ports
1	0007.ec7a.aa64	DYNAMIC	Fa0/1
1	00d0.ff47.5b01	DYNAMIC	Fa0/3
1	00e0.f9eb.023c	DYNAMIC	Fa0/2

Switch#

-->Après

Vlan	Mac Address	Type	Ports
1	0007.ec7a.aa64	DYNAMIC	Fa0/1
1	00d0.ff47.5b01	DYNAMIC	Fa0/2
1	00e0.f9eb.023c	DYNAMIC	Fa0/2

Switch#

-->Après avoir scanné le réseau et avoir découvert l'IP du pc client

-->On va empoisser le réseau en envoyant un ping continue

```
C:\>  
C:\>  
C:\>ping -t 192.168.1.2
```

-->Et depuis le pc client on va essayer d'accéder au service web qui ne fonctionnera pas a cause du Ping.

--> ouvrir le Sniffeur(machine KALI en réel) et vérifier le trafic et les paquets interceptés par celui-ci

-->Chercher le Protocol TCP et le lire et on pourra apercevoir dessus l'adresse src Dest, MDP si ils ne sont pas chiffrés,...

