Champ	Détails
Projet	**Sécurisation des ports du commutateur (Port Security)**
Objectif	Empêcher les intrusions réseau physiques via l'apprentissage dynamique d'adresses MAC (Sticky) et la gestion des violations.
Environnement	Cisco Packet Tracer (Simulateur Réseau)
Auteur	**Chadhouli EL-Anrif**
Date	30/11/2025

1. Contexte et Justification Technique

Par défaut, un port de switch est vulnérable. N'importe qui peut s'y connecter (intrusion physique) ou lancer une attaque par saturation de table MAC (MAC Flooding), transformant le switch en hub passif. **Objectif du TP :** Verrouiller l'accès au port **FastEthernet0/1** pour qu'il n'accepte qu'une seule adresse MAC spécifique apprise dynamiquement.

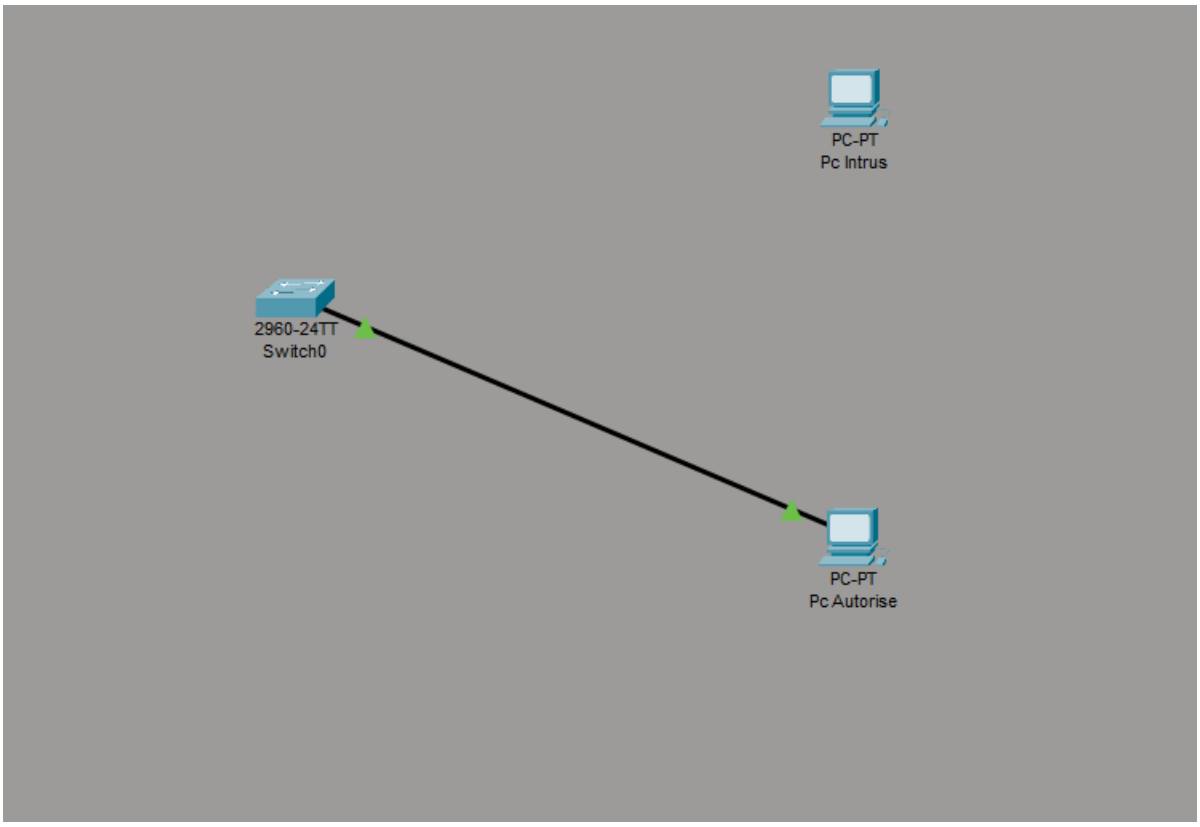
---

2. Procédure de configuration

Étape 1 : Mise en place de la topologie

Action :

1. Dans Packet Tracer, déployer un Switch 2960 et deux PCs.
2. Configurer les IP :
    - **PC_Autorise** : 192.168.1.10 /24
    - **PC_Intrus** : 192.168.1.20 /24
3. Câbler uniquement **PC_Autorise** sur le port **Fa0/1** du switch.



Étape 2 : Configuration du Port Security (Mode Sticky)

Action : Sur le Switch, entrer les commandes suivantes pour activer la sécurité et l'apprentissage dynamique :

```
SW1> enable
SW1# configure terminal
SW1(config)# interface FastEthernet0/1
! C'est une bonne pratique de définir le port en mode access
SW1(config-if)# switchport mode access

! Activer la fonctionnalité Port Security sur l'interface
SW1(config-if)# switchport port-security

! Définir le nombre maximum d'adresses MAC autorisées (ici, 1 seule)
SW1(config-if)# switchport port-security maximum 1

! Activer l'apprentissage "collant" (sticky)
SW1(config-if)# switchport port-security mac-address sticky
SW1(config-if)# end
SW1# write memory
```

Critique : À ce stade, la table MAC est vide. Le switch n'a rien appris. **Action obligatoire :** Depuis **PC_Autorise**, lancer un Ping vers une fausse adresse (ex : 192.168.1.50) pour générer une trame sortante.

Vérification : Vous devriez voir que Port Security est Enabled et que le Total MAC Addresses est à 1.

```
SW1#show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Étape 3 : Simulation d'intrusion (Violation Shutdown)

Action :

1. Débrancher le câble de **PC_Autorise**.
2. Brancher **PC_Intrus** sur le même port **Fa0/1**.
3. Attendre que le lien passe au vert (utiliser le bouton "Fast Forward Time" de Packet Tracer).
4. Depuis **PC_Intrus**, tenter un Ping.

Résultat : Le lien doit immédiatement passer au **ROUGE** (shutdown).

[INSÉRER CAPTURE D'ÉCRAN ICI] *Légende : Constat de la violation. Le lien vers le PC_Intrus est coupé (triangle rouge).*