PORT-SECURITY (SÉCURITÉ SUR LES PORTS)

SWITCHPORT SECURITY

PRÉSENTATION

Cette fonction permet de ***contrôler les adresses MAC autorisées*** sur un port. En cas de "***violation***", c'est-à-dire en cas d'adresses MAC non autorisées sur le port, ***une action est prise***.

Dans les infrastructures LAN modernes, on trouvera un port de commutateur dédié par station de travail.

Dans ce cadre, les ports ne devraient recevoir de trafic que d'**une seule adresse MAC** autorisée.

On y trouvera alors une utilité pour empêcher la connexion de commutateurs pirates par exemple.

SWITCHPORT SECURITY

PRÉSENTATION

Avec les Switchs Cisco, il est possible de faire un contrôle sur les ports en limitant l'accès à certaines adresses MAC, cela permet de sécuriser l'accès. Pour cela, il faut utiliser l'option « **Port-security** ».

Il y a deux méthodes, la première consiste à ***enregistrer manuellement l'adresse MAC autorisée*** et la seconde consiste à ***prendre comme adresse MAC autorisée celle de l'hôte qui va se connecter et envoyer une trame en premier à ce port du Switch Cisco.***

Pour rappel, l'adresse MAC correspond à l'adresse physique de la machine c'est-à-dire de sa carte réseau.

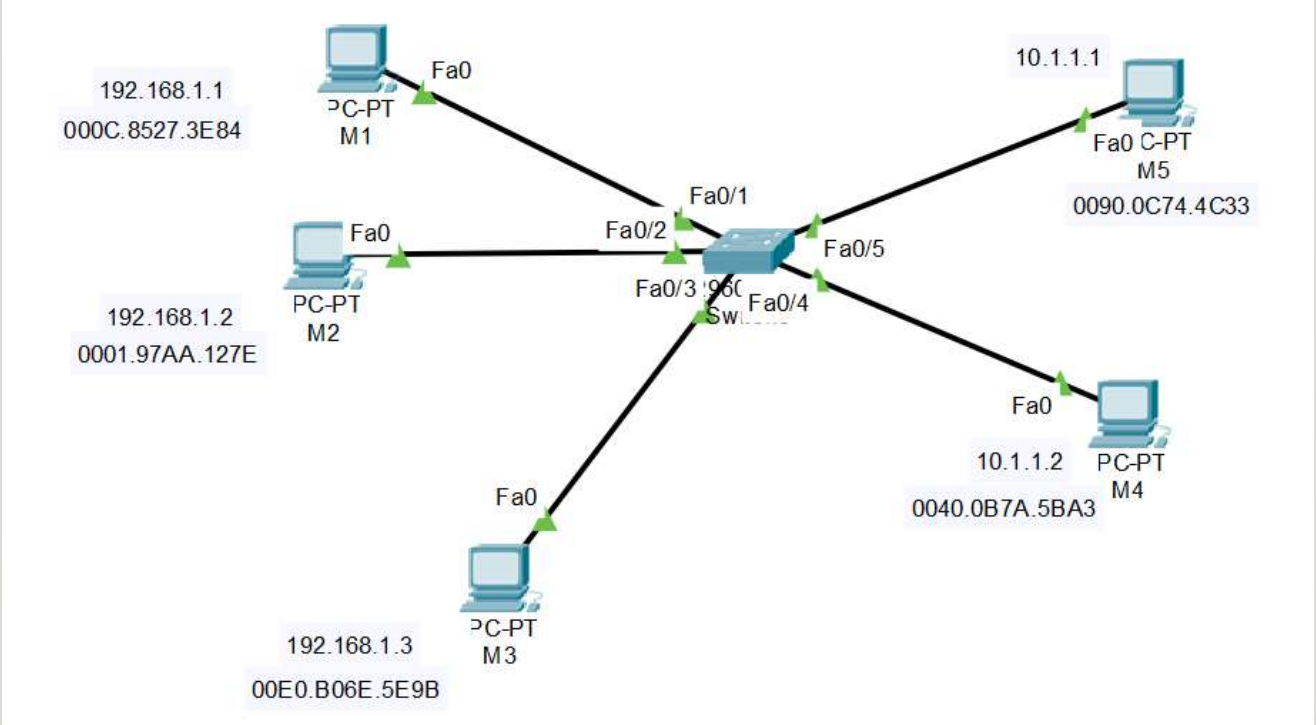
SWITCHPORT SECURITY

Enregistrer manuellement l'adresse MAC autorisée:

En définissant une adresse MAC précise pour un port. Dans le but d'empêcher n'importe quel poste de travail de se connecter.

Sans protection les postes de travail peuvent se connecter sur n'importe quel port du Switch et communiquer entre eux.

SWITCHPORT SECURITY



SWITCHPORT SECURITY

Nous allons autoriser dans un premier temps uniquement le « **M1** » à se connecter au port **F0/1** du Switch, pour éviter que ***les autres machines*** s'y connecte.

Switch>enable

Switch#Configure terminal

Switch(config)#interface FastEthernet 0/1

Switch(config-if)#switchport mode access

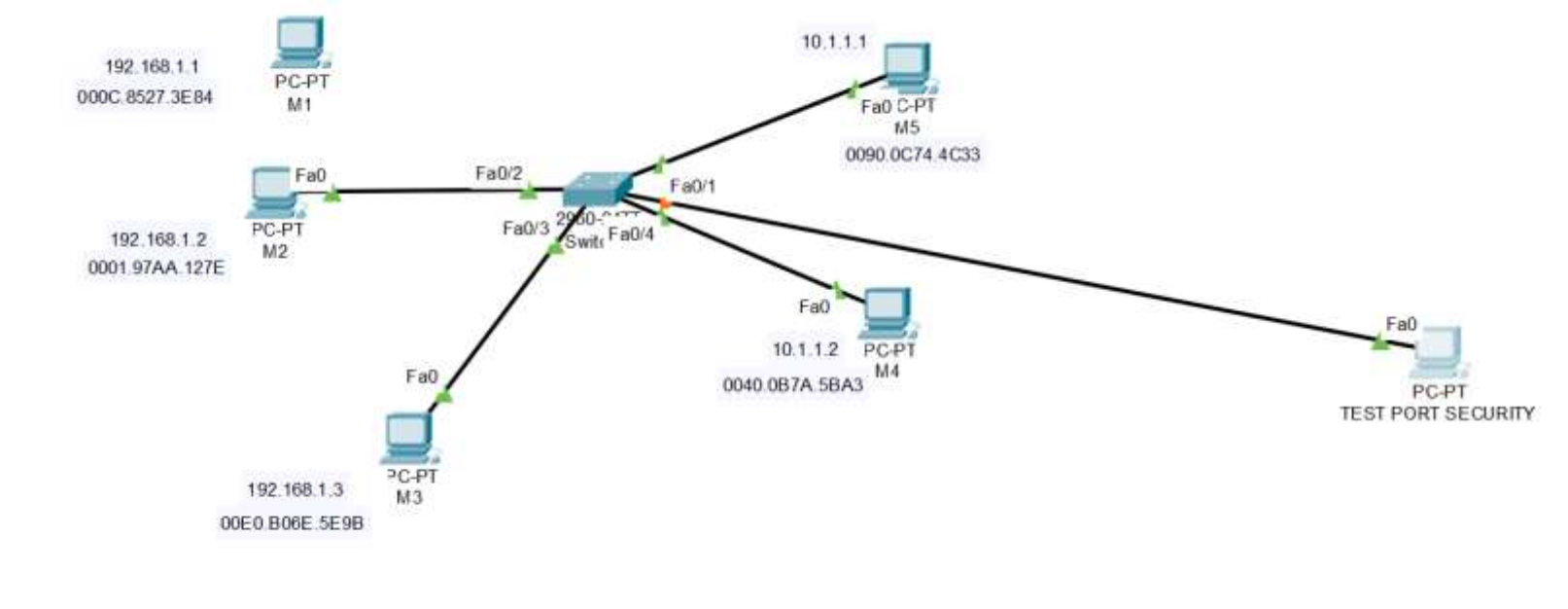
Switch(config-if)#switchport port-security ***« pour activer le service »***

Switch(config-if)#switchport port-security mac-address 000C.8527.3E84

SWITCHPORT SECURITY

Exemple :

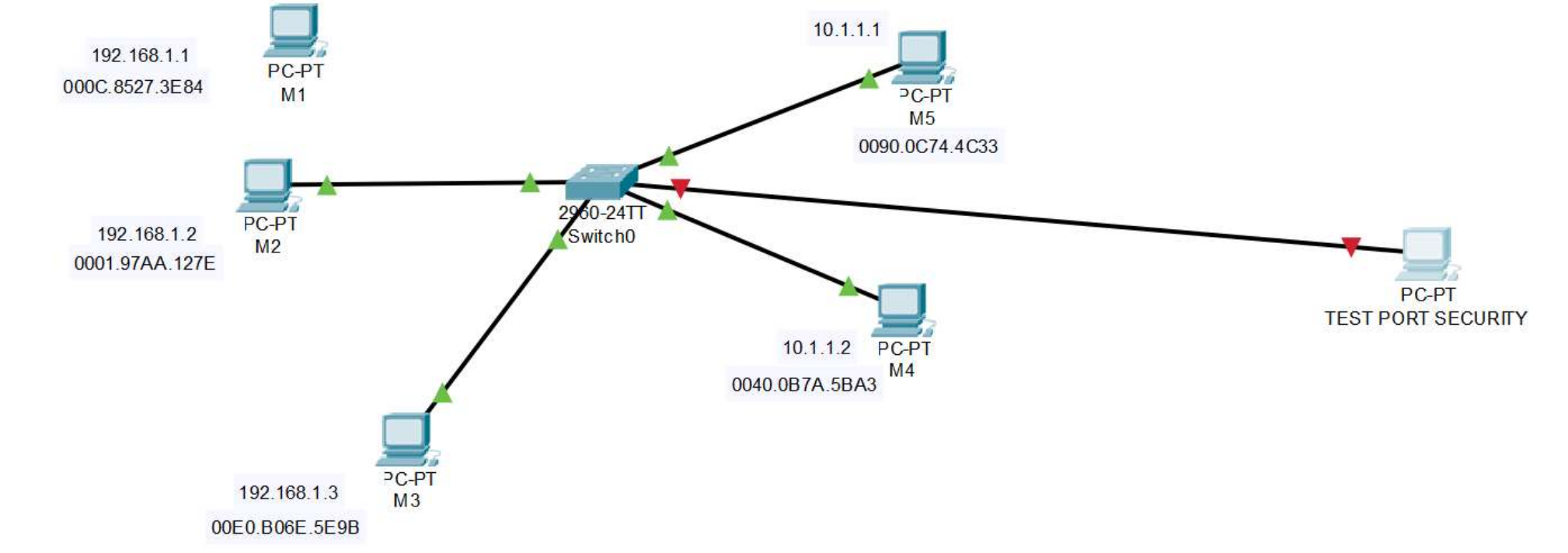
Prenons maintenant une nouvelle machine « NOM = TestPortSecurity »,et essayons de le mettre dans le port F0/1



SWITCHPORT SECURITY

Donner une configuration IP à la machine et essayer d'envoyer un message test à n'importe quelle machine?

SWITCHPORT SECURITY



SWITCHPORT SECURITY

La connexion ne marchera pas, vu que nous avons lié le port f0/1 à l'adresse mac de la machine M1 (Le port en rouge : mais il est NO SHUTDOWN) il est désactivé par le système.

Tapant la commande : ***show interfaces f0/1 status***

```
Switch#sho interfaces f0/1 status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        err-disabled 10         auto    auto  10/100BaseTX
```

SWITCHPORT SECURITY

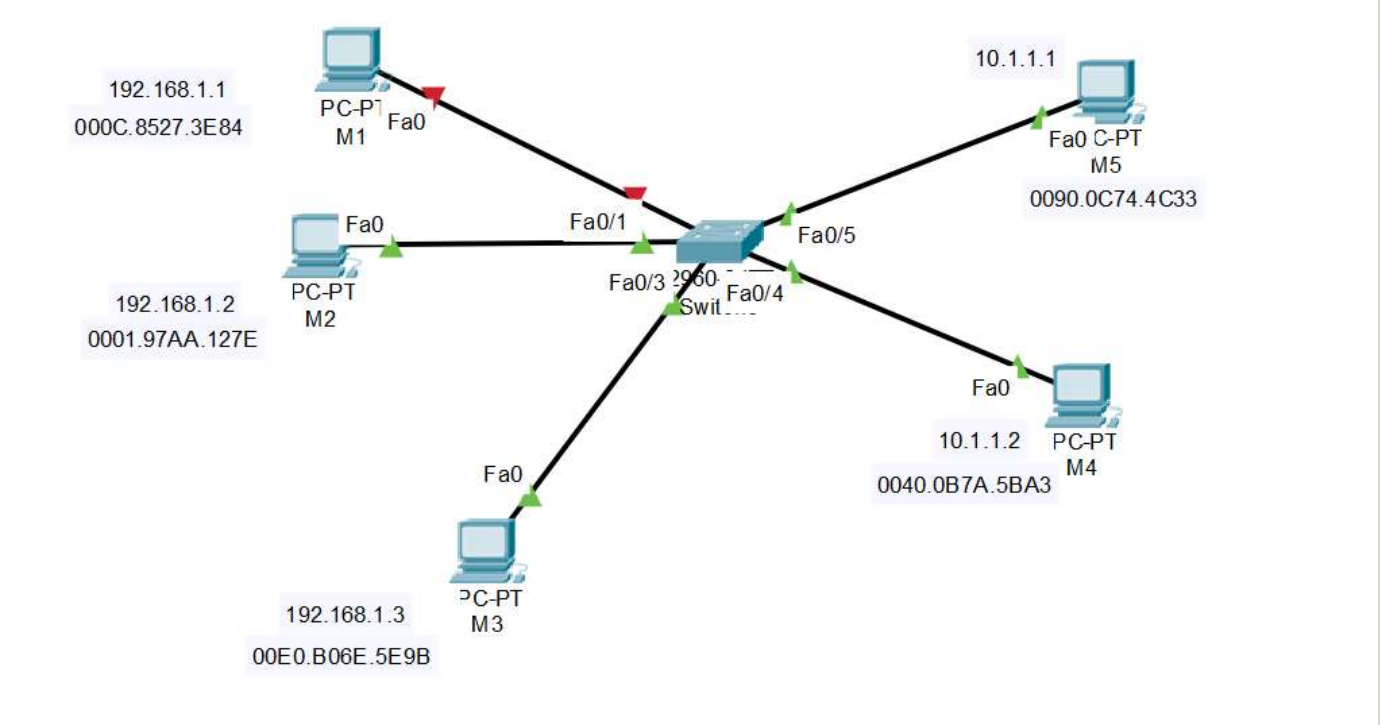
Ca dépend de la configuration, ca peut arriver que même en branchant dans le bon port la bonne machine, le port restera en rouge statut ***ERR-Disabled****,*

Pour débloquer le port il faut :

SHUTDOWN

NO SHUTDOWN

SWITCHPORT SECURITY



Switchport Security

Voir de manière globale où est active la protection et avoir quelques informations :

*** ***show port-security***

Switch#show port-security

Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action

(Count) (Count) (Count)

Fa0/1 1 1 1 Shutdown

SWITCHPORT SECURITY

```
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                (Count)       (Count)         (Count)
------------------------------------------------------------------------
        Fa0/1         1           1                 1          Shutdown
------------------------------------------------------------------------
Switch#
```

SWITCHPORT SECURITY

Ajouter une autre adresse :

De la même façon, on peut ajouter une autre adresse MAC,

Ajoutant l'adresse mac de la machine M3,

Switch(config-if)#switchport port-security mac-address 00E0.B06E.5E9B

```
Switch(config-if)#switchport port-security mac
Switch(config-if)#switchport port-security mac-address 00E0.B06E.5E9B
```

SWITCHPORT SECURITY

Augmenter le nombre d'adresses MAC autorisées sur un port , Par défaut, il est possible d'autoriser une seule adresse MAC sur chacun des ports mais il est possible d'augmenter le nombre d'adresses grâce à la commande

switchport port-security maximum NomBre *(NomBre : le max d'adresses autorisées)*

Exemple :

Lançant la commande

SHOW PORT-SECURITY INTERFACE F0/1

Maximum MAC Addresses : 2 ****** Max Mac autorisés***

Total MAC Addresses : 2 ****** Nombre configurés***

SWITCHPORT SECURITY

Essayons maintenant d'autoriser une autre adresse :

Switch(config-if)#switchport port-security mac-address 0001.97AA.127E

Total secure mac-addresses on interface FastEthernet0/1 has reached maximum limit.

SWITCHPORT SECURITY

Afficher les ***port-security*** par **interface** ou par **adresse** :

Switch#show port-security ?

address Show secure address

interface Show secure interface

SWITCHPORT SECURITY

Configuration automatique

Configuration Automatique : Le premier hôte qui va communiquer en passant par le port sera en quelque sorte le propriétaire.

Tout le temps qu'il n'y a pas de trame, l'adresse MAC du PC connecté n'est pas enregistrée.

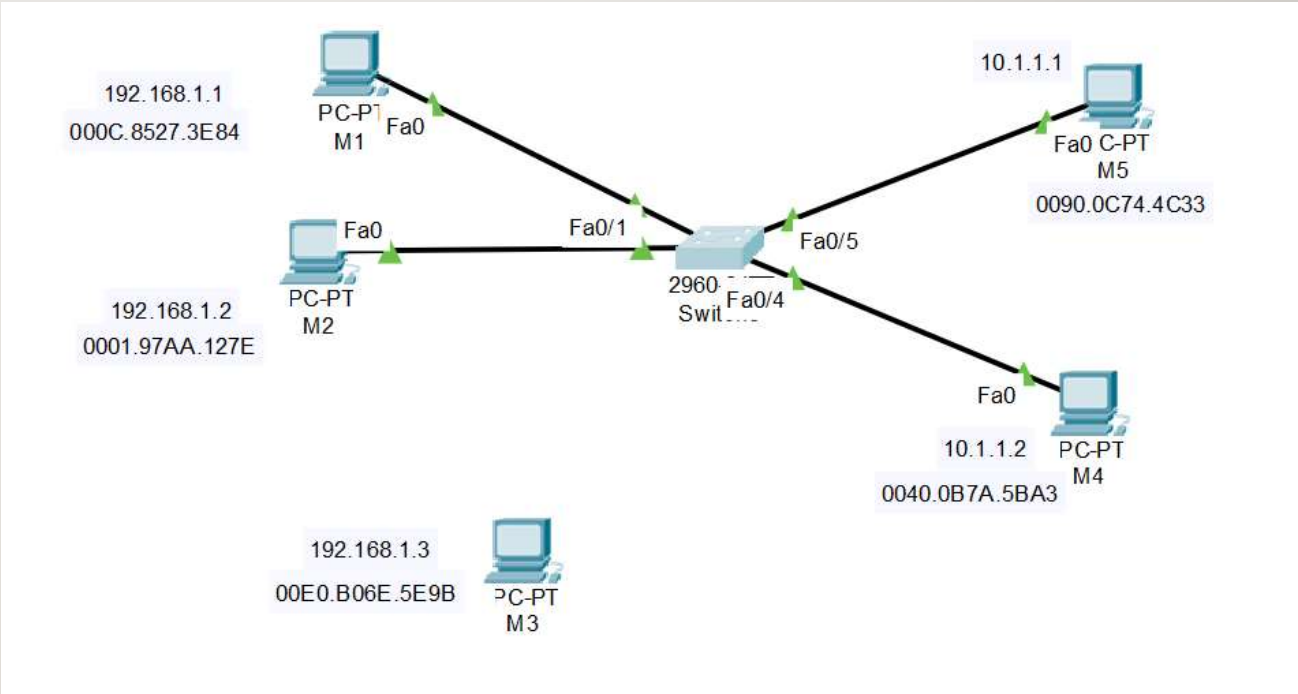
SWITCHPORT SECURITY

Exemple :

- Connectant M3 au port F0/10

Après avoir configuré F0/10

Comme indiqué ci-dessous :



SWITCHPORT SECURITY

Switch>enable

Switch#Configure terminal

Switch(config)#interface FastEthernet 0/10

Switch(config-if)#switchport mode access

Switch(config-if)#switchport port-security

Switch(config-if)#switchport port-security mac-address sticky

SWITCHPORT SECURITY

Affichant maintenant le ***port-sécurity*** sur l'interface F0/10

SWITCHPORT SECURITY

Mode de "violation"

Une "**Violation**" est une action prise en cas de non-respect d'une règle port-security.

Lorsqu'un hôte non autorisé se connecte sur un port sécurisé, le switch se doit de réagir à cette violation de la sécurité. Pour cela il utilise la commande « **switchport port-security violation** » avec 3 options différentes, qui sont :

SWITCHPORT SECURITY

La méthode « shutdown » : Elle désactive l'interface lorsque qu'il y a violation.

Pour la réactiver, il faut désactiver le port manuellement et le réactiver manuellement pour qu'il redevienne actif. Pour cela, allez dans la configuration de l'interface et saisissez la commande « shutdown » pour désactiver puis « no shutdown » pour activer l'interface.

SWITCHPORT SECURITY

La méthode « protect » : Toutes les trames ayant des adresses MAC sources inconnues sont bloquées et les autres autorisées.

La méthode « restrict » :

Alerte SNMP envoyée et le compteur de violation est incrémenté.

SWITCHPORT SECURITY

Exemple si on veut ajouter ce paramètre sur une interface déjà sécurisée :

Switch>enable

Switch#Configure terminal

Switch(config)#interface FastEthernet 0/10

Switch(config-if)#switchport mode access

Switch(config-if)#switchport port-security violation shutdown