# 

# SOMMAIRE

[I. Présentation 2](#_Toc159255347)

[II. Méthode de configuration 2](#_Toc159255348)

[III. Sécurisation manuelle de l’accès 3](#_Toc159255349)

[IV. Sécurisation automatique de l’accès 4](#_Toc159255350)

[V. Configurer la réaction lors de la violation de la sécurité 5](#_Toc159255351)

[5](#_Toc159255352)

1. PRESENTATION

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.

II. METHODE DE CONFIGURATION

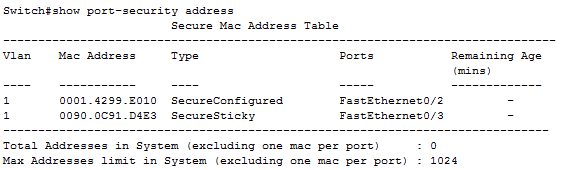
- Pour voir de manière globale où est active la protection et avoir quelques informations :

Show port-security int fa0/1



- Pour voir les adresses MAC autorisées sur chacun des ports sécurisés :

show port-security address



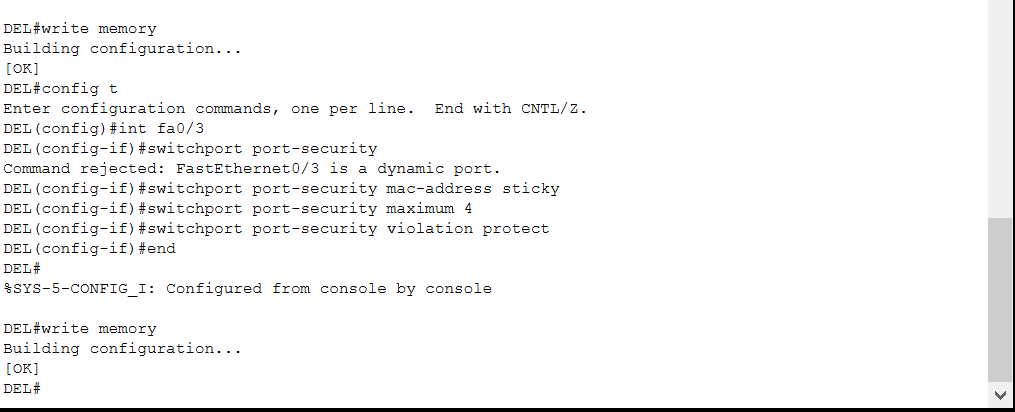
III. SECURISATION MANUELLE DE L’ACCES

Dans un premier temps, on va sécuriser manuellement l’accès en définissant une [adresse MAC](https://www.it-connect.fr/quest-ce-qu-une-adresse-mac/) précise pour un port. Dans le but d’empêcher n’importe quel poste de travail de se connecter.

Pour le moment, il n’y a pas de sécurité, les postes de travail peuvent se connecter sur n’importe quel port du Switch et communiquer entre eux.

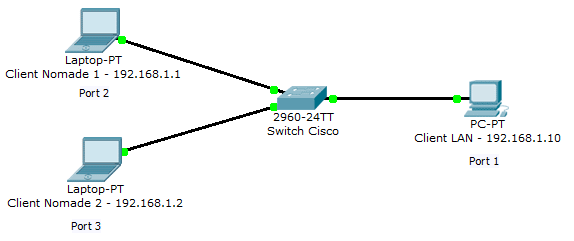
* **Adresse MAC « Client Nomade 1 »** : 00:01:42:99:E0:10
* **Adresse MAC « Client Nomade 2 »** : 00:90:0C:91:D4:E3
* **Adresse MAC « Client LAN »** : 00:D0:58:57:DE:7D

Étant donné qu’il y a des clients nomades (PC Portables) ils pourraient facilement changer de port sur le Switch donc nous allons autoriser uniquement le « **Client Nomade 1** » à se connecter au port 2 du Switch, pour éviter que le « **Client Nomade 2** » s’y connecte.



Ce qui correspond à : Passer en mode privilégié puis en mode de configuration et ensuite dans la configuration de l’interface FE 0/2 (port 2). En passe cette interface en mode « **access** » au lieu de « **dynamic** » puis on active la sécurité du port « **port-security** ». Pour finir, on définit l’adresse MAC autorisée sur cette interface.

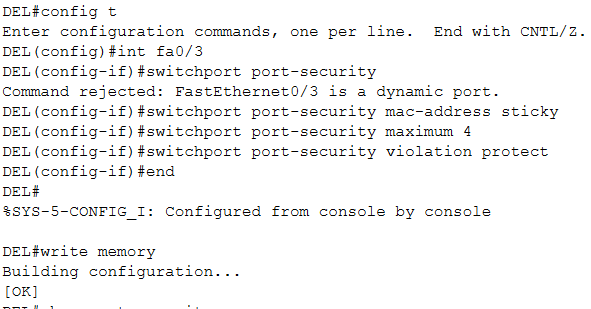
Lorsque l’on débranche le « **Client Nomade 1** » et que l’on branche le « **Client Nomade 2** » on peut voir que la connexion est active (elle peut se désactiver) mais si on effectue un *ping* avec le « **Client LAN** » vers le « **Client Nomade 2** » il n’y a pas de réponse. La protection s’applique bien.



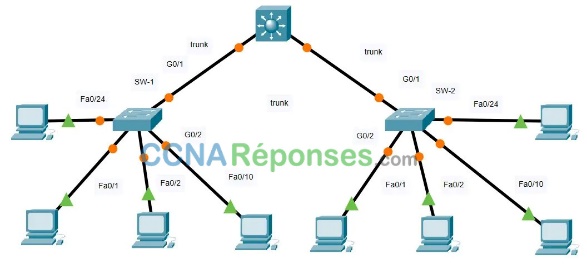
IV. SECURISATION AUTOMATIQUE DE L’ACCES

Il est possible de sécuriser l’accès de manière automatique c'est-à-dire que l’on active le « **port-security** » et c’est le premier hôte qui va se connecter et envoyer une trame qui va en être 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.

Par exemple, paramétrons de cette manière le port 3 (Interface FastEthernet 0/3) :



Le port est actif et le PC connecté, il ne reste plus qu’à envoyer une trame (par exemple pinger le PC « **Client LAN** ») pour que l’adresse MAC du «**Client Nomade 2** » soit enregistrée.



V. CONFIGURATION DE LA REACTION EN CAS DE VIOLATION DE LA SECURITE

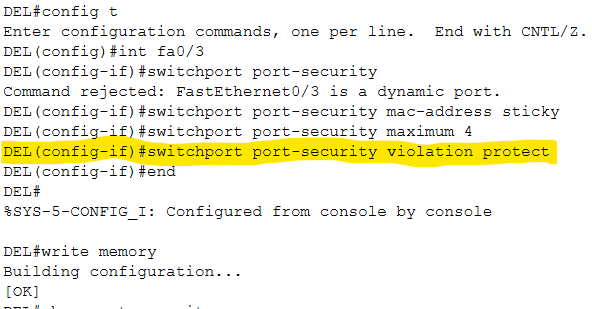
Lorsqu’un hôte non autorisé se connecte sur un port sécurisé, le switch se doit de réagir à cette violation de la sécurité. Pour cela il utilise la commande «**switchport port-security violation** » avec 3 options différentes, qui sont :

* 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.

* 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.

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



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 :

