

Configuration de Port-security

Introduction

Nous allons voir comment implémenter de la sécurité sur nos switchs

Configuration du Port security

Il faut tout d'abord configurer le port en mode access

```
switch(config)#int fa0/1
switch(config-if)#switchport mode access
```

Puis activer le port security

```
switch(config-if)#switchport port-security
```

Pour n'autoriser qu'une seule adresse MAC à se connecter au switch

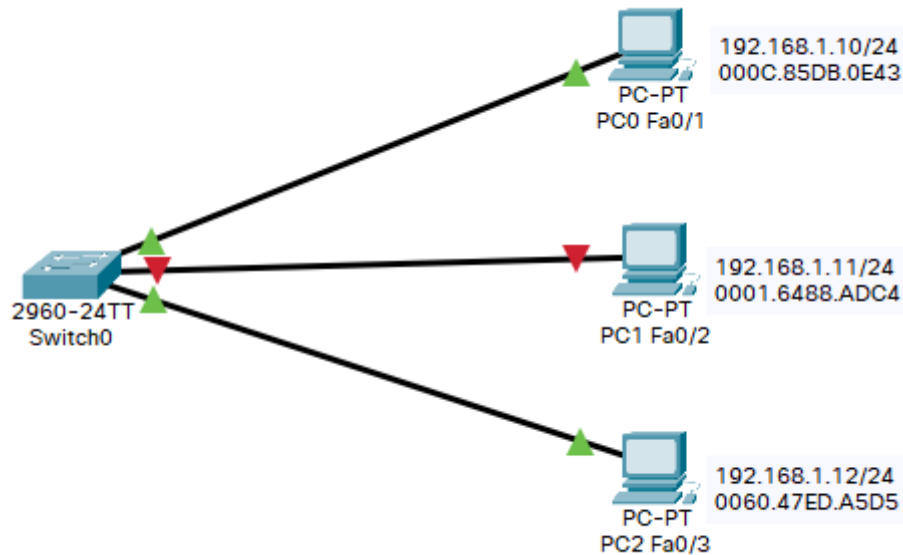
```
switch(config-if)#switchport port-security maximum 1
```

Evidement, s'il y a un téléphone IP + un PC, il faudra mettre le paramètre sur 2

Il existe 3 options pour la gestion des adresses MAC :

1. Dynamic : Le switch apprend les adresses MAC automatiquement
2. Static : Nous devons configurer l'adresse MAC manuellement
3. Sticky : Le switch apprend les adresses MAC automatiquement et les ajoute à la conf

Pour la suite, je vais me baser sur cette topologie :



Configuration de fastEthernet 0/1

```
switch(config)#interface FastEthernet0/1
switch(config-if)#switchport mode access
switch(config-if)#switchport port-security
switch(config-if)#switchport port-security mac-address 000C.85DB.0E43
```

Configuration de fastEthernet 0/2

```
switch(config)#interface FastEthernet0/1
switch(config-if)#switchport mode access
switch(config-if)#switchport port-security
switch(config-if)#switchport port-security mac-address 000C.85DB.0E42
```

Configuration de fastEthernet 0/3

```
switch(config)#interface FastEthernet0/1
switch(config-if)#switchport mode access
switch(config-if)#switchport port-security
switch(config-if)#switchport port-security mac-address sticky
```

Il faut ensuite configurer la violation

Dès qu'une des règles ci-dessus n'est pas respectées, nous avons plusieurs solutions.

1. Mode shutdown : Va désactiver le port
2. Mode protect : les trames des adresses mac non renseignées sont ignorées par le switch

3. Mode restrict : fonctionne comme le mode protect mais en plus, un message snmp est envoyé et peut aussi être récupéré par un serveur syslog

Sur mon exemple, les ports fastEthernet 0/1 et 0/2 ont été configurés en mode shutdown

```
switch(config-if)#switchport port-security violation shutdown
```

le port fastEthernet 0/3 en mode restrict

```
switch(config-if)#switchport port-security violation restrict
```

PC0 : L'adresse MAC est entrée en mode statique dans le switch, et elle correspond à l'adresse MAC du pc, donc rien ne se passe

PC1 : L'adresse MAC est entrée en mode statique dans le switch, mais ne correspond à l'adresse MAC du pc, le port est shutdown

PC2 : L'adresse MAC est apprise par le switch est correspond à l'adresse MAC du pc, rien ne se passe. Si toutefois nous branchons un autre pc, le port bloquera tout le trafic et enverra des trames d'erreur.

Revision #3

Created 14 March 2024 12:00:10 by Dunnload

Updated 19 March 2024 06:56:38 by Dunnload