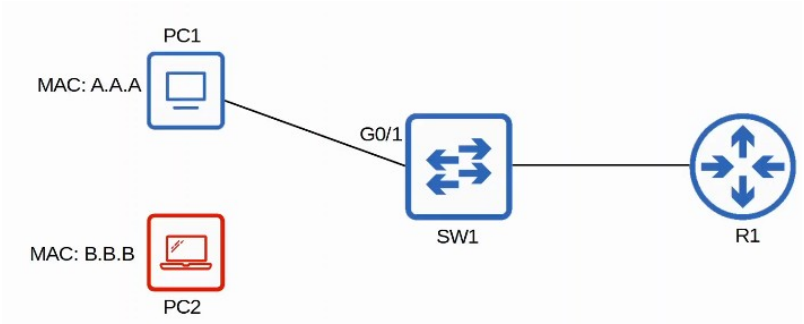
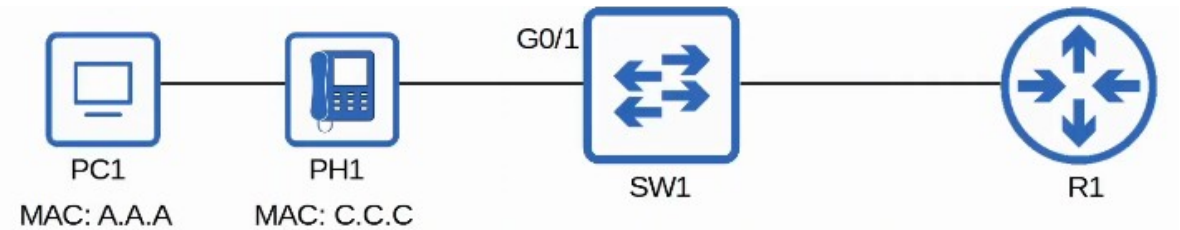
Cours 49 : Port Security

Dans ce cours nous verrons le fonctionnement de Port Security qui est une fonctionnalité des Switch Cisco qui permet de contrôler quelle adresse MAC source sont autorisé dans un port Switch. Nous ferons d'abord une introduction de ce qu'est port security, nous verrons ensuite pourquoi utiliser port security quelle est l'intérêt de l'utiliser, puis nous verrons comment configurer port security.

Port security est don une fonctionnalité intégré dans les switch Cisco qui permet de contrôler quelle adresse MAC source est permise pour entrer dans un port switch. Par exemple si une adresse MAC source non autorisé entre par le port, une action sera prise par le switch.
L'action par défaut est de placer l'interface en état : « err-disabled »
Par exemple sur le réseau suivant :

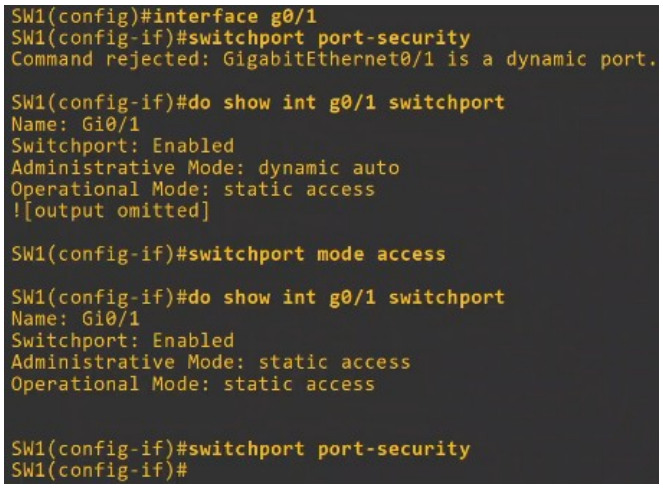


Le switch est configuré pour qu'il n'accepte que les adresses MAC du PC1 : A.A.A qui entrent dans l'interface G0/1
A présent imaginons que le câble du PC1 soit déconnecté et que ce soit le PC2 qui soit connecté à cette même interface, le SW1 va bloquer l'interface en « err-disabled » puisqu'il se rend compte que l'adresse MAC n'est pas celle du PC1.
Il faudra réactiver l'interface pour que celle soit à nouveau active.
Lorsque l'on active port security sur une interface avec les paramètres par défaut, une adresse MAC est autorisé. Il est possible de configurer l'adresse MAC autorisé manuellement.
Si l'on ne configure pas l'interface manuellement le switch va permettre la première source adresse MAC qui entre l'interface. Les adresses MAC peuvent être apprises de manière dynamique ou bien manuellement.
Il est possible de changer le nombre maximal d'adresses MAC autorisés.
Dans le réseau suivant par exemple, il faut autoriser plus d'adresses MAC puisque les deux appareils (le téléphone et le PC) ne pourront pas communiquer sinon car ils sont connectés à une seule interface.



Port security permet au réseau admin de contrôler quelles appareils sont autorisés à accéder le réseau.
Le changement d'adresse MAC est une chose simple, il est facile de configurer un appareil pour envoyer une trame avec une adresse MAC source différente.
Au lieu de spécifier manuellement l'adresse MAC à autoriser sur chaque port, port security a l'habilité de limiter le nombre d'adresses MAC autorisés sur une interface.
Par exemple dans le cas d'une attaque DHCP starvation, l'attaquant va faire du spoofing sur de fausses adresses MAC. Le serveur DHCP va assigner des adresses IP à ces fausses adresses MAC ce qui va limiter le pool DHCP.
Les tables d'adresses MAC des switch peuvent aussi devenir pleines à cause de ce genre d'attaques.
En limitant le nombre d'adresses MAC sur une interface peut protéger de ce genre d'attaques.

Voici à présent les commandes à utiliser pour activer port security :




```
SW1(config)#interface g0/1
SW1(config-if)#switchport port-security
```

Pour afficher la configuration de l'interface on lance la commande :
SW1(config-if)#do show int g0/1 switchport

Port security peut être activé uniquement en mode access port ou en port trunk il doit être configuré de manière statique comme access ou trunk avec les statut :
`switchport mode access` ou `switchport mode trunk`
Les statut : `switchport mode dynamic auto` et `switchport dynamic desirable` ne permettent pas la configuration statique avec port security.

Pour activer le mode statique on lance la commandes :
SW1(config-if)#switchport mode access

Le statut de l'interface a à présent changé en statique, il est donc possible d'activer port security.
On lance donc la commande :
`SW1(config-if)#switchport port-security`

La commande `show port-security interface` suivi du nom d'interface, est très utile on peut voir qu'est indiqué si port security est activé sur l'interface le violation mode permet de dire si l'interface doit être désactivé si une adresse MAC externe entre.
On peut aussi voir affiché le nombre maximal d'adresses MAC.

```
SW1#show port-security interface g0/1
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
```

Lorsque l'on fait un ping entre deux appareils le résultat de la commande est différent :

```
SW1#show port-security interface g0/1
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        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000a.000a.000a:1
Security Violation Count   : 0
```

A présent lorsque l'on tente de connecter un PC avec une autre adresse MAC à l'interface, le statut de l'interface est à présent différend en secure-shutdown :

```
SW1#show port-security interface g0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
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   : 000b.000b.000b:1
Security Violation Count   : 1
```

```
SW1#show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi0/0                        connected    1            auto   auto unknown
Gi0/1                        err-disabled 1            auto   auto unknown
```

L’interface est en statut « err-disabled », pour réactiver cette interface il faudra retirer l’appareil qui cause cela puis lancer les commandes :

```
SW1(config)#interface g0/1
SW1(config-if)#shutdown
SW1(config-if)#no shutdown
```

On peut voir que l’interface est à nouveau activé :

```
SW1#show port-security interface g0/1
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
```

Il existe une autre manière de réactiver une interface, c’est avec « errDisable Recovery »
Cela permet à une interface de se réactiver automatiquement après un certain temps.

```
SW1#show errdisable recovery
ErrDisable Reason            Timer Status
-----------------            --------------
arp-inspection               Disabled
bpduguard                    Disabled
channel-misconfig (STP)      Disabled
dhcp-rate-limit              Disabled
dtp-flap                     Disabled
![output omitted due to length]
psecure-violation            Disabled
security-violation           Disabled
sfp-config-mismatch          Disabled
storm-control                Disabled
udld                         Disabled
unicast-flood                Disabled
vmps                         Disabled
psp                          Disabled
dual-active-recovery         Disabled
evc-lite input mapping fa    Disabled
Recovery command: "clear     Disabled

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:
```

Ici toute les 5 minutes (ou 300 secondes) toutes les interfaces err-disabled sont réactivés automatiquement, mais pour activer cela il faut que la fonction psecure-violation soit activé on lance pour cela la commande :

```
SW1(config)#errdisable recovery cause psecure-violation
```

Pour modifier le temps d’intervalle d’activation entre chaque interface on lance la commande :

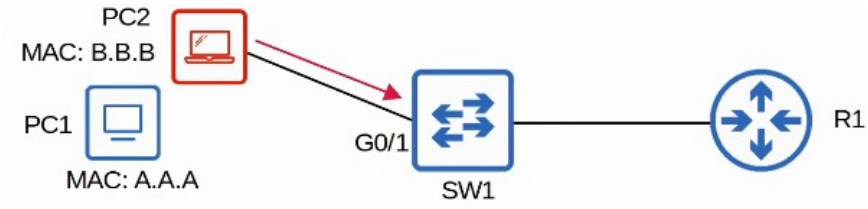
```
SW1(config)#errdisable recovery interval 180
```

Lorsque l'on lance show errdisable recovery on peut voir à présent que la fonctionnalité psecure-violation est à présent bien activé :

```
SW1#show errdisable recovery
ErrDisable Reason            Timer Status
-----------------            --------------
![output omitted due to length]
psecure-violation            Enabled
![output omitted due to length]

Timer interval: 180 seconds

Interfaces that will be enabled at the next timeout:

Interface       Errdisable reason       Time left(sec)
---------       -----------------       --------------
Gi0/1          psecure-violation          149
```

Il y a trois différents modes qui déterminent ce que le switch fais si une trame non autorisé entre dans l'interface configuré avec port security :
- Shutdown : cela éteint l'interface en le plaçant en statut « err-disabled », cela génère aussi un message SNMP lorsque l'interface est désactivé. Le compteur de violation est placé à 1 lorsque l'interface est désactivé.
- Restrict : Le switch va bloquer le trafique des adresses MAC non autorisés, l'interface n'est pas désactivé. Le switch génère un message Syslog ou SNMP chaque fois qu'une adresse MAC non autorisé est détecté. Le compteur de violation s'incrémente à 1 pour chaque trame non autorisé.
- Protect : Le switch bloque le trafique des adresses MAC non autorisés, l'interface n'est pas désactivé dans ce mode. Cela ne génère pas de messages Syslog ou SNMP et cela n'incrémente pas le compteur de violation.

On utilisera le réseau suivant :



Voici les commandes pour configurer le Violation mode restrict :

```
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security mac-address 000a.000a.000a
SW1(config-if)#switchport port-security violation restrict

*May 23 22:54:09.951: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC
address 000b.000b.000b on port GigabitEthernet0/1.

SW1#show port-security interface g0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000b.000b.000b:1
Security Violation Count   : 12
```

Voici les commandes pour configurer le Violation mode protect :

```
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security mac-address 000a.000a.000a
SW1(config-if)#switchport port-security violation protect


SW1#show port-security interface g0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Protect
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000b.000b.000b:1
Security Violation Count   : 0
```

Le mode Shutdown est le mode par défaut.

Voyons plus en détail la configuration de port security avec le MAC Adress Aging.

```
SW1#show port-security interface g0/1
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        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000a.000a.000a:1
Security Violation Count   : 0
```

Par défaut l'adresse MAC n'expire pas et est permanente (Aging Time : 0 mins), il est possible de changer le temps avec la commande : `switchport port-security aging time` suivi du temps en minutes. Le aging time par défaut est « absolute » c'est à dire que après que l'adresse MAC est apprise, le aging time commence et l'adresse MAC est supprimé après le temps expire, même si le switch continue de recevoir des trames de cette adresse MAC source.
Le aging time est en inactivity après que l'adresse MAC sécurisé est apprise, le aging time commence mais est réinitialisé chaque fois qu'une trame de cette adresse MAC source est réceptionné sur cette interface.
Il est possible de changer le type d'aging time avec la commande :
`switchport port-security aging time {absolute | inactivity}`

l'aging Secure Static MAC (les adresses configurés avec `switchport port-security mac-address x.x.x`) est désactivé par défaut.
Cela peut être activé avec `switchport port-security aging static`

Par exemple on configure l'aging de Secure MAC address avec les commandes suivantes :

```
SW1(config-if)#switchport port-security aging time 30
SW1(config-if)#switchport port-security aging type inactivity
SW1(config-if)#switchport port-security aging static


SW1#show port-security interface g0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 30 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Enabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000a.000a.000a:1
Security Violation Count   : 0
```

La commande : `show port-security` affiche quelles interfaces ont port-security activé et plusieurs autres informations :

```
SW1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Gi0/1              1            1                  0         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

L'apprentissage des « sticky » secure Mac address peut être activé avec les commandes suivantes :
`SW1(config-if)#switchport port-security mac-address sticky`

Lorsque activé et les adresses MAC dynamiquement apprises sont ajoutés à la running-config comme ceci :
`switchport port-security mac-address sticky` suivi de l'adresse MAC
Ces adresses MAC « sticky » n'expire jamais.
Il est nécessaire de lancer la running-config vers le startup-config pour les rendre totalement permanent sinon elles ne seront pas gardés lorsque le switch redémarre.
Lorsque l'on lance la commande : `switchport port-security mac-address sticky` toutes les adresses MAC apprises dynamiquement sont convertis en secure MAC Address sticky.
Lorsque l'on lance la commande : `no switchport port-security mac-address sticky` toutes les adresses MAC sticky apprises sont convertis en secure MAC apprises dynamiquement.

Voici les commandes que l'on lance pour la configuration en mode sticky :

```
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security mac-address sticky
SW1(config-if)#do show running-config interface g0/1
!
interface GigabitEthernet0/1
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 000a.000a.000a
 switchport port-security
 negotiation auto
```

Les adresses MAC secure sont ajoutés à la table d'adresse MAC comme toutes les autres adresses MAC. Les adresses Sticky et statique secure MAC address ont pour statut STATIC
Les adresses MAC secure dynamiquement apprises ont pour statut DYNAMIC
Il est possible de voir toutes les adresses MAC secure avec la commande :
`show mac address-table secure`

```
SW1#show mac address-table secure
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    000a.000a.000a    STATIC      Gi0/1
Total Mac Addresses for this criterion: 1
```