SWITCHING : Port-Security

Concept:

Sécurisation des ports d'un switch basée sur l'adresse MAC source de la trame Ethernet entrant sur un port:

- Nombre d'adresses MAC différentes autorisées pour un port donné (nombre d'entrée dans la table d'adresses MAC).
- Mode de fonctionnement lors d'une violation de sécurité.
- Apprentissage dynamique des adresses MAC autorisées (ajoutées à la running-config par l'IOS).

Modes de fonctionnement

Mode / Fonctionnalité	*Bloquer la trame*	*Compteur de violations*	*Fermeture du port*
Protect	**Oui**	Non	Non
Restrict	**Oui**	**Oui**	Non
Shutdown	**Oui**	**Oui**	**Oui**

Configuration

```
switch> enable
switch# configure terminal
switch(config)# interface <NOM> <NUM>

! Port-security requiert un port d'accès (défaut: dynamic auto)
switch(config-if)# switchport mode access

! Définir le nombre maximum d'adresses MAC source différentes (défaut: 1)
switch(config-if)# switchport port-security maximum <N>

! Définir le mode de réaction en cas de violation (défaut: shutdown)
switch(config-if)# switchport port-security violation <MODE>

! Configurer une adresse MAC statique ou apprentissage dynamique
switch(config-if)# switchport port-security mac-addres <MAC|sticky>

! Activer le port-security
switch(config-if)# switchport port-security
```

SWITCHING : Port-Security

Vérifiation

```
switch# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
-----------------------------------------------------------------------------
      Fa0/1             10            0                  0          Shutdown
      Fa0/2              5            1                  0          Shutdown
      Fa0/3              5            0                  0          Shutdown
      Fa0/4              5            0                  0          Shutdown
      Fa0/5              5            0                  0          Shutdown
      Fa0/6              5            0                  0          Shutdown
      Fa0/7              5            0                  0          Shutdown
      Fa0/8              5            0                  0          Shutdown
      Fa0/9              5            0                  0          Shutdown
     Fa0/10              5            0                  0          Shutdown
     Fa0/11              5            0                  0          Shutdown
     Fa0/12              5            0                  0          Shutdown
     Fa0/13              5            0                  0          Shutdown
     Fa0/14              5            0                  0          Shutdown
     Fa0/15              5            0                  0          Shutdown
     Fa0/16              5            0                  0          Shutdown
     Fa0/17              5            0                  0          Shutdown
     Fa0/18              5            0                  0          Shutdown
     Fa0/19              5            0                  0          Shutdown
     Fa0/20              5            0                  0          Shutdown
     Fa0/21              5            0                  0          Shutdown
     Fa0/22              5            0                  0          Shutdown
     Fa0/23              5            1                  0          Shutdown
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

Nombre de MAC Autorisées

Nombre de MAC déjà connues

Nombre de violations

Action en cas de violation

Remarques:

- Seuls les ports pour lesquels la commande "switchport port-security" a été entrée utiliseront cette fonctionnalité, et apparaîtront dans la liste affichée via "show port-security". Donc, un port n'apparaissant pas dans cette liste n'a pas de sécurité active.
- Un port désactivé par port-security (mode shutdown) sera dans un état particulier: DOWN/DOWN (err-disabled).
- Pour réactiver un port en "err-disabled", il faut effectuer un "shutdown, no shutdown" sur le port en question.