Sécurité physique des équipements

Assurer l'intégrité physique du matériel est la priorité avant d'envisager toute autre action.

Volumes techniques protégés

Pour protéger un équipement d'une intervention indésirable, on peut :

- L'enfermer dans un volume technique protégé (armoire métallique fermée à clé, ventilée);
- L'enfermer dans un local technique protégé (parois coupe-feu, porte pare-flamme, fermée à clé);
- L'enfermer dans un local protégé par contrôle d'accès (badge, lecture biométrique, clé électronique, etc...).

Ainsi on interdit l'accès au port console de l'équipement.

Accès depuis la console

Toutefois il n'est pas exclu qu'un individu mal intentionné accède au commutateur (double des clés, badge d'accès perdu non invalidé, etc.). Nous allons donc rajouter plusieurs protections:

Sécurisation du mode enable

```
Press RETURN to get started.
SW1>enable
SW1#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#enable password agriotes
SW1(config)#
```

Résultat:

```
Press RETURN to get started.
SW1>enable
Password:
```

Mais si on oublie de sortir du mode enable, d'autres pourraient voir le mot de passe en clair ...

```
SW1#show run
Building configuration...
[...]
hostname SW1
!
enable password agriotes
[...]
```

On va donc **chiffrer ce mot de passe** :

```
SW1>en
Password:
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#service password-encryption
```

Résultat :

```
SW1#show run
Building configuration...
hostname Switch
```

```
!
enable password 7 08204B5C0016111201
!
```

La commande *service password-encryption* permet de chiffrer tous les mots de passe attribués sur le commutateur mais ils sont déchiffrables aisément[1)]. Nous préférerons la commande suivante pour chiffrer le mot de passe enable en MD5:

```
SW1(config)#enable secret agriotes
```

Résultat:

```
SW1#show run
Building configuration...
hostname SW1
!
enable secret 5 $1$mERr$ZttMyXJHEB0w.GJNsoF3R0
```

Sécurisation du port console

Malgré tout, on peut voir une partie de la **configuration sans entrer dans le mode enable**. Exemple:

```
SW1>show ip dhcp snooping
Switch DHCP snooping is disabled
```

On va donc sécuriser l'accès au port console :

```
SW1>en
Password:
SW1#conf t
SW1(config)#line console 0
SW1(config-line)#password motdepasse
SW1(config-line)#login
```

nous avons tapé le mot de passe en clair mais il apparaîtra chiffré dans la configuration car nous avons activé précédemment le service password-encryption.

Résultat au branchement du câble console :

```
Press RETURN to get started.
User Access Verification
Password:
```

Sécurisation de la configuration

En appuyant 10 secondes sur le bouton MODE du commutateur (valable par exemple sur un commutateur Cisco 2960), on remet la configuration à zéro! Pour désactiver cette fonctionnalité il

suffit de taper la commande suivante :

```
SWITCH(config)#no setup express
```

Pour résumer

`service password-encryption` pour chiffrer l'ensemble des mots de passe du commutateur.
`enable secret motdepasse` pour chiffrer solidement le mot de passe du mode enable.
Et on interdit l'accès physique au commutateur.

Si un accès au commutateur est possible à distance, on sécurisera la ligne de la même manière que pour la console.

Connexion entre commutateurs

Nous devons prévoir les cas où les commutateurs seraient reliés entre eux par un câble droit et protéger le commutateur des branchements réalisant une boucle.

Auto MDIX

Ayant affaire à des équipements de même nature, nous utilisons des câbles croisés pour brancher les commutateurs entre eux. Or c'est n'est pas une évidence pour tout le monde… Nous allons donc nous prémunir d'un branchement hasardeux en rendant le commutateur indépendant du support utilisé :

```
SW1(config)#interface range fastEthernet 0/1-24
SW1(config-if-range)#mdix auto
SW1(config-if-range)#interface range gigabitEthernet 0/1-2
SW1(config-if-range)#mdix auto
```

Les commutateurs récents ne sont généralement plus dépendants du médium utilisé.

Spanning Tree Protocol

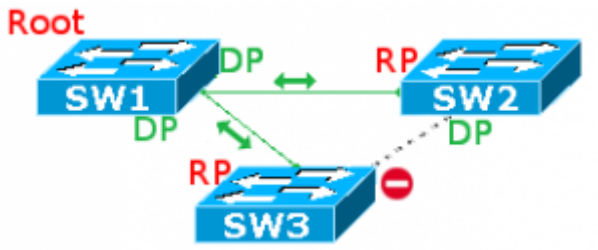
Comme on peut le voir sur le schéma initial, trois commutateurs sont reliés entre eux, créant une boucle:

Pour éviter que les signaux se répètent indéfiniment entre commutateurs (tempête de diffusion), nous avons mis en place le protocole STP [2)]
Nous avons décidé que le commutateur SW1 sera le commutateur **racine** (au plus proche du coeur

du réseau) en lui affectant le plus faible identifiant:

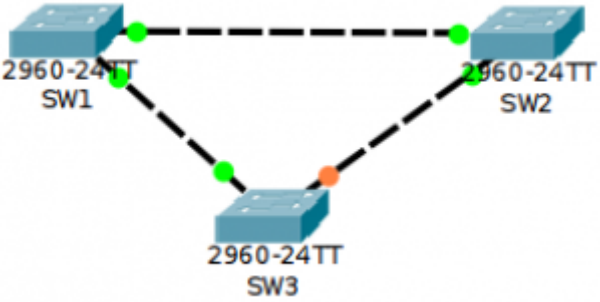
```
SW1(config)#spanning-tree vlan 1 priority 4096
SW1(config)#
```

Les débits et distances étant les mêmes entre les 3 commutateurs, la liaison de données se fait ainsi :



Les ports racines (*RP pour root port*) des commutateurs SW2 et SW3 sont au plus près du commutateur racine et les ports désignés entre chaque commutateur (*DP pour designed port*) sont placés de telle sorte que le port de SW3 relié au port de SW2 n'est ni RP ni DP : il est donc bloqué et la liaison directe est interrompue entre les commutateurs SW2 et SW3.

Vérification de notre configuration avec PacketTracer:



Conclusion

Nous avons vu :

- Comment protéger un commutateur physiquement;
- Comment s'affranchir des branchements douteux;
- Comment sécuriser la connexion au commutateur.

Voilà des commutateurs Bretons bien protégés!

Il est temps de regarder de plus près le fonctionnement du transfert de données sur la couche 2 dans le chapitre suivant.

[1)]

http://sio.pqd.fr/ciscocrack.html

[2)]

Spécifications : http://standards.ieee.org/getieee802/download/802.1D-2004.pdf