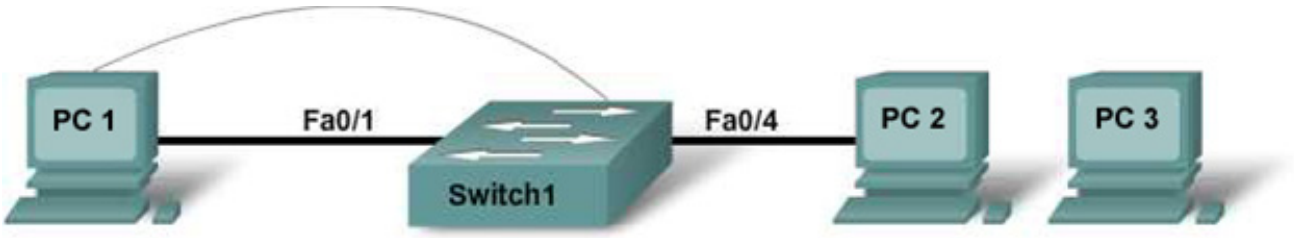
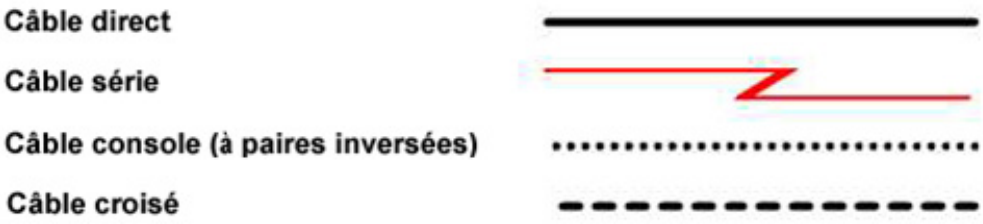
Travaux pratiques 3.1.4 : Application des mesures de sécurité de base pour les commutateurs





Désignation du périphérique	Adresse IP	Masque de sous-réseau	Passerelle par défaut	Mot de passe secret actif	Mot de passe vty et mot de passe de console
PC1	192.168.1.3	255.255.255.0	192.168.1.1		
PC2	192.168.1.4	255.255.255.0	192.168.1.1		
PC3	192.168.1.5	255.255.255.0	192.168.1.1		
Switch1	192.168.1.2	255.255.255.0	192.168.1.1	class	cisco

Objectifs

- Configurer des mots de passe pour sécuriser l'accès à l'interface de ligne de commande (ILC)
- Configurer un commutateur pour désactiver le serveur http à des fins de sécurité
- Configurer la sécurité des ports
- Désactiver les ports inutilisés
- Tester la configuration de la sécurité en connectant des hôtes non spécifiés à des ports sécurisés

Contexte / Préparation

Installez un réseau similaire à celui du schéma de topologie.

Ressources requises :

- Un commutateur Cisco 2960 ou comparable
- Trois PC Windows, dont un au moins équipé d'un programme d'émulation de terminal
- Au moins un câble console, avec connecteur RJ-45 vers DB-9
- Deux câbles droits Ethernet (PC1 et PC2 à commutateur)
- Accès à l'invite de commandes du PC
- Accès à la configuration réseau TCP/IP du PC

REMARQUE : assurez-vous que le commutateur a été effacé et vérifiez l'absence de configurations initiales. Pour plus d'informations sur l'effacement des commutateurs et des routeurs, reportez-vous au Manuel des travaux pratiques, disponible dans la section Tools (Outils) du site Academy Connection.

Étape 1 : connexion du PC1 au commutateur

a. Connectez le PC1 au port de commutation Fast Ethernet Fa0/1. Configurez PC1 pour l'utilisation de l'adresse IP, du masque et de la passerelle spécifiés dans le tableau.

b. Établissez une session d'émulation de terminal du commutateur à partir de PC1.

Étape 2 : connexion du PC2 au commutateur

a. Connectez le PC2 au port de commutation Fast Ethernet Fa0/4.

b. Configurez le PC2 pour utiliser l'adresse IP, le masque et la passerelle spécifiés dans le tableau.

Étape 3 : configuration de PC3, sans connexion

Un troisième hôte est nécessaire au bon fonctionnement de ces travaux pratiques.

a. Configurez PC3 à l'aide de l'adresse IP 192.168.1.5. Le masque de sous-réseau est 255.255.255.0 et la passerelle par défaut est 192.168.1.1.

b. Ne connectez pas encore ce PC au commutateur. Il sera utilisé pour tester le système de sécurité.

Étape 4 : configuration initiale sur le commutateur

a. Définissez **Switch1** en tant que nom d'hôte du commutateur

```
Switch>enable
Switch#config terminal
Switch(config)#hostname Switch1
```

b. Définissez **cisco** en tant que mot de passe du mode d'exécution privilégié.

```
Switch1(config)#enable password cisco
```

c. Définissez **class** en tant que mot de passe secret du mode d'exécution privilégié.

```
Switch1(config)#enable secret class
```

d. Configurez les lignes de console et de terminal virtuel pour utiliser et demander un mot de passe de connexion.

```
Switch1(config)#line console 0
Switch1(config-line)#password cisco
Switch1(config-line)#login
Switch1(config-line)#line vty 0 15
Switch1(config-line)#password cisco
Switch1(config-line)#login
Switch1(config-line)#end
```

e. Quittez la session en mode console et ouvrez une nouvelle session.

Quel est le mot de passe requis pour passer en mode d'exécution privilégié ?

_____

Pourquoi ? _____

Étape 5 : configuration de l'interface de gestion de commutateur sur le réseau local virtuel VLAN 1

a. Passez en mode de configuration d'interface pour le réseau local virtuel VLAN 1.

```
Switch1(config)#interface vlan 1
```

b. Configurez l'adresse IP, le masque de sous-réseau et la passerelle par défaut pour l'interface de gestion.

```
Switch1(config-if)#ip address 192.168.1.2 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config-if)#exit
Switch1(config)#ip default-gateway 192.168.1.1
Switch1(config)#end
```

Pourquoi l'interface VLAN 1 requiert-elle une adresse IP sur ce réseau local ?

_____

Quel est l'objectif d'une passerelle par défaut ?

_____

Étape 6 : vérification des paramètres de gestion des réseaux locaux

a. Vérifiez que l'adresse IP de l'interface de gestion du réseau local virtuel VLAN 1 et l'adresse IP de PC1 et de PC2 se trouvent sur le même réseau local. Utilisez la commande **show running-config** pour vérifier la configuration de l'adresse IP du commutateur.

b. Vérifiez les paramètres d'interface sur le réseau local virtuel VLAN 1.

```
Switch1#show interface vlan 1
```

Quelle est la bande passante définie sur cette interface ?

_____

Quels sont les spécifications du réseau local virtuel ?

Le réseau local virtuel VLAN 1 est _____, le protocole de ligne est _____.

Étape 7 : désactivation du commutateur en tant que serveur http

Désactivez la fonctionnalité permettant au commutateur d'être utilisé en tant que serveur http.

```
Switch1(config)#no ip http server
```

Étape 8 : vérification de la connectivité

a. Pour vérifier que les hôtes et les commutateurs sont correctement configurés, envoyez une requête ping à l'adresse IP du commutateur à partir des hôtes.

La requête ping a-t-elle abouti ? _____

Si la requête ping échoue, vérifiez à nouveau les connexions et les configurations. Vérifiez si les câbles ne sont pas défectueux et si les connexions sont stables. Vérifiez les configurations de l'hôte et du commutateur.

b. Enregistrez la configuration.

Étape 9 : enregistrement des adresses MAC de l'hôte

Définissez et enregistrez les adresses de couche 2 des cartes d'interface réseau des PC. À l'invite de commandes de chaque PC, tapez **ipconfig /all**.

PC1 _____

PC2 _____

PC3 _____

Étape 10 : définition des adresses MAC acquises par le commutateur

Déterminez les adresses MAC que le commutateur a acquises en tapant la commande **show mac-address-table** à l'invite du mode d'exécution privilégié.

```
Switch1#show mac-address-table
```

Combien y a-t-il d'adresses dynamiques ? _____

Combien y a-t-il d'adresses MAC au total ? _____

Les adresses MAC correspondent-elles aux adresses MAC de l'hôte ? _____

Étape 11 : affichage des options show mac-address-table

Affichez les options disponibles de la commande **show mac-address-table**.

```
Switch1(config)#show mac-address-table ?
```

Quelles sont les options disponibles ? _____

_____

Étape 12 : configuration d'une adresse MAC statique

Configurez une adresse MAC statique sur l'interface Fast Ethernet 0/4. Utilisez l'adresse qui a été enregistrée pour PC2 à l'étape 9. L'adresse MAC 00e0.2917.1884 n'est utilisée que dans cet exemple d'instruction.

```
Switch1(config)#mac-address-table static 00e0.2917.1884 vlan 1
interface fastethernet 0/4
```

Étape 13 : vérification des résultats

a. Vérifiez les entrées de la table d'adresses MAC.

```
Switch1#show mac-address-table
```

À présent, quel est le nombre total d'adresses MAC ? _____

À présent, quel est le nombre d'adresses MAC statiques ? _____

b. Supprimez l'entrée statique de la table d'adressage MAC.

```
Switch1(config)#no mac-address-table static 00e0.2917.1884 vlan 1
interface fastethernet 0/4
```

Étape 14 : liste des options de sécurité des ports

a. Définissez les options permettant de définir la sécurité des ports sur l'interface FastEthernet 0/4.

```
Switch1(config)#interface fastethernet 0/4
Switch1(config-if)#switchport port-security ?
```

Quelles sont les options disponibles ? _____

b. Afin que le port de commutation FastEthernet 0/4 n'accepte qu'un périphérique, configurez la sécurité des ports comme suit :

```
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport port-security
Switch1(config-if)#switchport port-security mac-address sticky
```

c. Quittez le mode de configuration et vérifiez les paramètres de sécurité des ports.

```
Switch1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
-------------------------------------------------------------------------
      Fa0/4        1            0                0            Shutdown
-------------------------------------------------------------------------
```

Si un hôte différent de PC2 tente de se connecter à Fa0/4, que se passe-t-il ?

_____

Étape 15 : limite du nombre d'hôtes par port

a. Sur l'interface FastEthernet 0/4, définissez sur 1 le nombre maximum d'adresses MAC pour la sécurité des ports.

```
Switch1(config-if)#switchport port-security maximum 1.
```

b. Déconnectez le PC connecté à FastEthernet 0/4. Connectez le PC3 à FastEthernet 0/4. L'adresse IP 192.168.1.5. a été attribuée au PC3, et PC3 n'a pas encore été attaché au commutateur. Il peut être nécessaire d'envoyer une requête ping à l'adresse 192.168.1.2 du commutateur pour générer du trafic.

Consignez toute observation utile. _____

_____

Étape 16 : configuration du port pour la désactivation en cas de violation de la sécurité

a. L'interface doit être désactivée en cas de violation de la sécurité. Entrez la commande suivante pour que le paramètre de sécurité de port soit défini sur la désactivation :

```
Switch1(config-if)#switchport port-security violation shutdown
```

Quelles autres actions sont disponibles avec la sécurité des ports ? _____

_____

b. Si nécessaire, envoyez une requête ping à l'adresse de commutateur 192.168.1.2 à partir du PC3 192.168.1.5. Ce PC est à présent connecté à l'interface FastEthernet 0/4. Cela garantit la présence de trafic entre le PC et le commutateur.

c. Consignez toute observation utile.

_____

_____

d. Vérifiez les paramètres de sécurité des ports.

```
Switch1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
-------------------------------------------------------------------------
      Fa0/4        1            1                0            Shutdown
-------------------------------------------------------------------------
```

Étape 17 : affichage des informations de configuration du port 0/4

Pour afficher uniquement les informations de configuration du port FastEthernet 0/4, tapez **show interface fastethernet 0/4** à l'invite du mode d'exécution privilégié.

```
Switch1#show interface fastethernet 0/4
```

Quel est l'état de cette interface ?

FastEthernet0/4 est _____ et le protocole de ligne est _____

Étape 18 : réactivation du port

a. Si le port est désactivé à la suite d'une violation de la sécurité, utilisez les commandes **shutdown / no shutdown** pour le réactiver.

b. Essayez de réactiver ce port plusieurs fois en basculant entre l'hôte d'origine du port 0/4 et le nouveau. Connectez l'hôte d'origine, tapez la commande **no shutdown** dans l'interface et envoyez une requête ping à l'invite de commandes.

Vous devez utiliser la requête ping plusieurs fois ou utiliser la commande **ping 192.168.1.2 -n 200**. Cette dernière définit sur 200 le nombre de paquets de requêtes ping plutôt que sur 4. Changez ensuite d'hôte et réessayez.

Étape 19 : désactivation des ports inutilisés

Désactivez tous les ports non utilisés par le commutateur.

```
Switch1(config)#interface range Fa0/2 – 3
Switch1(config-if-range)#shutdown
Switch1(config-if-range)#exit
Switch1(config)#interface range Fa0/5 – 24
Switch1(config-if-range)#shutdown

Switch1(config)#interface range gigabitethernet0/1 - 2
Switch1(config-if-range)#shutdown
```

Étape 20 : remarques générales

a. Pourquoi la sécurité de port doit-elle être activée sur un commutateur ? _____

_____

b. Pourquoi les ports non utilisés sur un commutateur doivent-ils être désactivés ? _____

_____