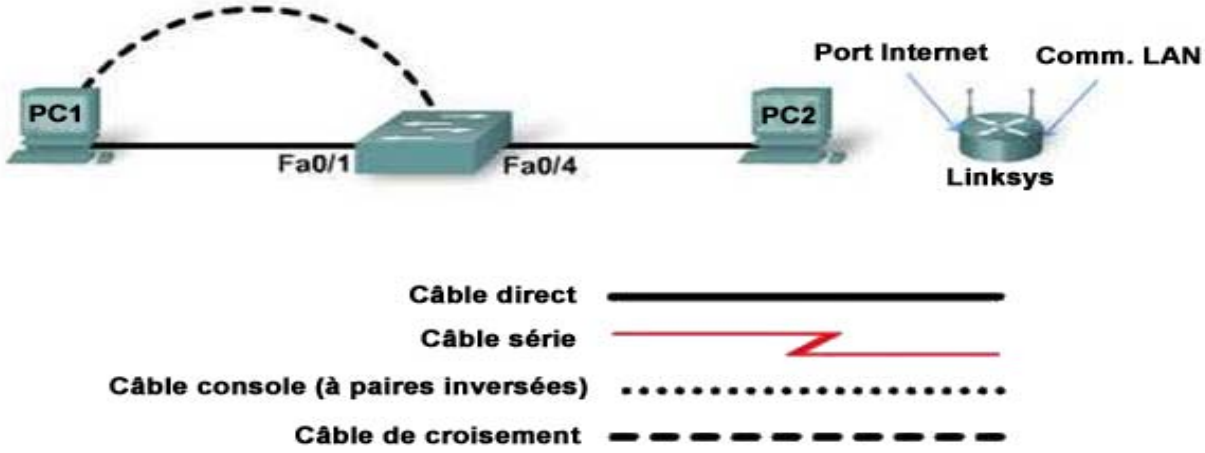
Travaux pratiques 1.4.6B Mise en œuvre de la sécurité des ports



Désignation du périphérique	Nom du périphérique	Adresse du VLAN 1	Masque de sous-réseau
Comm1	FC-ASW-1	10.0.0.2	255.255.255.0
PC1	Hôte 1	10.0.0.254	255.255.255.0
PC2	Hôte 2	10.0.0.253	255.255.255.0
Port Internet du Linksys	Intrus	10.0.0.252	255.255.255.0

Objectifs

- Configurer la sécurité de ports FastEthernet individuels d'un commutateur
- Tester et confirmer la sécurité des ports de commutation qui ont été configurés

Objectifs de l'examen CCNA 640-802

Ces travaux pratiques font appel à des compétences qui se rapportent aux objectifs d'examen CCNA suivants :

- Effectuer et vérifier les tâches initiales de configuration du commutateur, notamment la gestion de l'accès à distance
- Vérifier l'état du réseau et le fonctionnement du commutateur au moyen des utilitaires de base (comprenant ping, traceroute, Telnet, SSH, arp et ipconfig) et les commandes **show** et **debug**
- Mettre en œuvre la sécurité de base du commutateur (comprenant la sécurité des ports, l'accès au réseau, le réseau local virtuel de gestion autre que VLAN 1 etc.)

Résultats attendus et critères de réussite

Avant de commencer ces travaux pratiques, lisez les tâches que vous devez effectuer. Selon vous, quel sera le résultat de l'exécution de ces tâches ?

_____

_____

_____

Selon vous, pour quelle raison les administrateurs réseau mettent-ils en œuvre la sécurité de ports sur le réseau ?

_____

_____

_____

Comment un administrateur réseau sait-il si la sécurité de ports fonctionne correctement ?

_____

_____

_____

Contexte / Préparation

Une des importantes responsabilités des administrateurs et concepteurs de réseau est la sécurité du réseau. Les ports de commutation de la couche d'accès sont accessibles via le câblage structuré au niveau des prises murales disponibles. N'importe qui peut brancher un PC, ordinateur portable ou point d'accès sans fil à l'une de ces prises. Elles représentent donc des accès possibles au réseau pour les utilisateurs non autorisés.

Les commutateurs offrent une fonction appelée *sécurité des ports*. Celle-ci permet de limiter le nombre d'adresses MAC pouvant être acquises dans une interface. Le commutateur peut être configuré pour entreprendre une action [arrêter] dans le cas où ce nombre serait dépassé. Le nombre d'adresses MAC par port peut être limité, généralement à 1. La première adresse acquise par le commutateur de façon dynamique pour ce port devient l'adresse sécurisée.

En utilisant la topologie donnée, ces travaux pratiques configurent un commutateur fournissant un accès au réseau à uniquement deux PC et en testent la sécurité en tentant de connecter un périphérique « intrus », le routeur sans fil Linksys, au port sécurisé.

Tâche 1 : configuration et test de la connectivité du commutateur

Étape 1 : préparation du commutateur à la configuration

REMARQUE : si les PC utilisés dans ces travaux pratiques sont également connectés au réseau local de votre établissement ou à Internet, assurez-vous de bien noter les raccordements de câbles et les paramètres TCP/IP afin que ceux-ci puissent être rétablis à la fin des travaux pratiques.

a. En vous référant au schéma de la topologie, connectez le câble console (à paires inversées) au port console du commutateur et l'autre extrémité au port COM 1 de l'ordinateur hôte à l'aide d'un adaptateur DB-9 ou DB-25. Assurez-vous que l'ordinateur hôte et le commutateur sont tous les deux sous tension.

b. Établissez une session en mode console de PC1 au commutateur Comm1.

c. Préparez le commutateur pour la configuration des travaux pratiques en veillant à ce que toutes les configurations VLAN et générales soient supprimées.

1) Supprimez le fichier de configuration de démarrage du commutateur de la mémoire NVRAM.

```
Switch#erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

2) Appuyez sur **Entrée** pour confirmer.

La réponse suivante devrait s'afficher :

```
Erase of nvram: complete
```

d. Mettez hors tension puis sous tension le commutateur puis quittez le mode de configuration initiale lorsque le commutateur redémarre.

Étape 2 : configuration du commutateur

Configurez le nom d'hôte et l'adresse IP de l'interface VLAN 1 comme indiqué dans le tableau.

Étape 3 : configuration des hôtes reliés au commutateur

a. Configurez les deux PC afin qu'ils utilisent le même sous-réseau IP pour l'adresse et le masque comme indiqué dans le tableau.

b. Connectez PC1 au port de commutation Fa0/1 et PC2 à Fa0/4. Le périphérique Linksys n'est pas connecté à ce stade des travaux pratiques.

Étape 4 : vérification de la connectivité de l'hôte

Envoyez une requête ping de chaque PC vers le commutateur pour vérifier que la configuration est correcte. Si l'une des requêtes échoue, dépannez les configurations des hôtes et du commutateur.

Étape 5 : enregistrement des adresses MAC

Déterminez et enregistrez les adresses de couche 2 des cartes d'interface réseau PC.

(Pour Windows 2000, XP ou Vista, vérifiez à l'aide de **`Démarrer > Exécuter > cmd > ipconfig /all`**.)

Adresse MAC de PC1 : _____

Adresse MAC de PC2 : _____

Étape 6 : détermination des adresses MAC acquises par le commutateur

a. À l'invite du mode d'exécution privilégié, lancez la commande **show mac-address-table** pour afficher les adresses MAC du PC acquises par le commutateur.

```
FC-ASW-1#show mac-address-table
```

Reportez les informations affichées dans le tableau.

_____

_____

b. Notez les adresses MAC indiquées et leurs ports de commutation associés. Confirmez que ces adresses et ports correspondent aux PC connectés.

Comment ces associations d'adresses MAC et de ports ont-elles été acquises ?

_____

_____

Tâche 2 : configuration et test de la sécurité de ports dynamiques du commutateur

Étape 1 : activation des options de sécurité de ports

a. Déconnectez tous les câbles Ethernet allant aux PC des ports de commutation.

b. Assurez-vous que la table d'adresses MAC est bien vide. Pour ce faire, lancez les commandes **clear mac-address-table dynamic** et **show mac-address-table**.

c. Effacez les entrées de la table d'adresses MAC.

```
FC-ASW-1#clear mac-address-table dynamic
```

d. Lancez la commande **show mac-address-table**.

Reportez les entrées de la table.

_____

_____

_____

_____

e. Déterminez les options permettant de définir la sécurité des ports sur l'interface FastEthernet 0/4. Dans le mode de configuration globale, entrez **interface fastethernet 0/4**.

```
FC-ASW-1(config)#interface fa 0/4
```

L'activation de la sécurité des ports de commutation comporte plusieurs options, par exemple elle permet de définir ce qu'il se passe si un paramètre de sécurité n'est pas respecté.

f. Pour configurer le port de commutation FastEthernet 0/4 de façon à ce qu'il n'accepte que le premier périphérique connecté, lancez les commandes suivantes dans le mode de configuration :

```
FC-ASW-1(config-if)#switchport mode access
FC-ASW-1(config-if)#switchport port-security
```

g. L'interface doit être désactivée en cas de violation de la sécurité. Attribuez la valeur **shutdown** à la mesure de sécurité de port :

```
FC-ASW-1(config-if)#switchport port-security violation shutdown
FC-ASW-1(config-if)#switchport port-security mac-address sticky
```

Quelles autres actions sont disponibles dans la sécurité des ports ?

_____

h. Quittez le mode de configuration.

Étape 2 : vérification de la configuration

a. Affichez la configuration courante.

Quelles instructions dans cette configuration reflètent directement la mise en œuvre de la sécurité ?

_____

_____

_____

_____

b. Affichez les paramètres de sécurité des ports.

```
FC-ASW-1#show port-security interface fastethernet 0/4
```

Reportez les informations affichées dans le tableau.

_____

_____

_____

_____

_____

_____

_____

_____

Étape 3 : vérification de la sécurité des ports

a. Connectez PC1 au port de commutation Fa0/1 et PC2 au port Fa0/4.

b. À l'invite de commande, envoyez une requête ping de PC1 à PC2.

A-t-elle abouti ? _____

c. À l'invite de commande, envoyez une requête ping de PC2 à PC1.

A-t-elle abouti ? _____

d. Dans la session en mode console, lancez la commande **show mac-address-table**.

Reportez les informations affichées dans le tableau.

_____

_____

e. Affichez les paramètres de sécurité des ports.

```
FC-ASW-1#show port-security interface fastethernet 0/4
```

Reportez les informations affichées dans le tableau.

_____

_____

_____

_____

_____

_____

_____

_____

Notez les différences par rapport aux entrées reportées à l'étape 2 b.

_____

_____

_____

f. Confirmez l'état du port de commutation.

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

Quel est l'état de cette interface ?

FastEthernet0/4 est _____ le protocole de ligne est _____

Étape 4 : test de la sécurité des ports

a. Déconnectez PC2 de Fa0/4.

b. Connectez PC2 au Linksys sur l'un des ports du commutateur du réseau local Linksys.

c. Utilisez l'onglet Basic Setup pour régler l'adresse IP Internet de l'appareil Linksys sur l'adresse et le masque, comme illustré dans le tableau.

d. Configurez PC2 afin qu'il obtienne une adresse IP au moyen de DHCP. Vérifiez que PC2 reçoive une adresse IP de l'appareil Linksys.

e. Connectez le port Internet du Linksys à Fa0/4.

f. Envoyez une commande ping de PC1 à PC2.

A-t-elle abouti ? _____

g. Envoyez une commande ping de PC2 à PC1.

A-t-elle abouti ? _____

Reportez le résultat affiché sur l'écran de console à la ligne de commande du commutateur.

_____

_____

_____

h. Lancez la commande **show mac-address-table**.

Reportez les informations affichées dans le tableau.

_____

_____

i. Affichez les paramètres de sécurité des ports.

```
FC-ASW-1#show port-security interface fastethernet 0/4
```

Reportez les informations affichées dans le tableau.

_____

_____

_____

_____

_____

_____

_____

_____

Notez les différences par rapport aux entrées reportées à l'étape 3 e.

_____

_____

_____

j. Confirmez l'état du port de commutation.

```
FC-ASW-1#show interface fastethernet 0/4
```

Quel est l'état de cette interface ?

FastEthernet0/4 est _____ le protocole de ligne est _____

Étape 5 : réactivation du port

a. Si une violation de la sécurité a lieu et que le port est désactivé, passez en mode de configuration de l'interface Fa0/4, déconnectez le périphérique à la source du problème et utilisez la commande **shutdown** pour désactiver temporairement le port.

b. Déconnectez le Linksys et reconnectez PC2 au port Fa0/4. Lancez la commande **no shutdown** dans l'interface.

c. Envoyez une commande ping de PC1 à PC2. Il est possible qu'il faille répéter plusieurs fois cette commande avant qu'elle réussisse.

Donnez les raisons pour lesquelles plusieurs tentatives d'envoi de requête ping peuvent être nécessaires avant que l'une d'entre elles réussisse.

_____

_____

_____

Étape 6 : discussion de la sécurité de ports de commutation au moyen de l'attribution dynamique d'adresses MAC

Avantages :

_____

_____

_____

_____

Inconvénients :

_____

_____

_____

_____

Étape 7 : remise en état

Effacez les configurations et redémarrez les commutateurs. Déconnectez et rangez le câblage. Pour les PC hôtes habituellement connectés à d'autres réseaux (comme le réseau local de l'établissement ou Internet), reconnectez le câblage approprié et restaurez les paramètres TCP/IP.

Tâche 3 : remarques générales

Lors de l'analyse de la phase de conception d'un réseau d'entreprise type, il est nécessaire de considérer les questions de vulnérabilité en matière de sécurité au niveau de la couche d'accès. Exposez lesquels des commutateurs de la couche d'accès doivent être dotés de la sécurité de ports et ceux pour lesquels elle n'est éventuellement pas appropriée. Incluez les éventuels problèmes futurs concernant les accès sans fil et les accès en mode invité au réseau.