Exercice Packet Tracer 2.4.7 : Configuration de la sécurité des commutateurs

Schéma de topologie

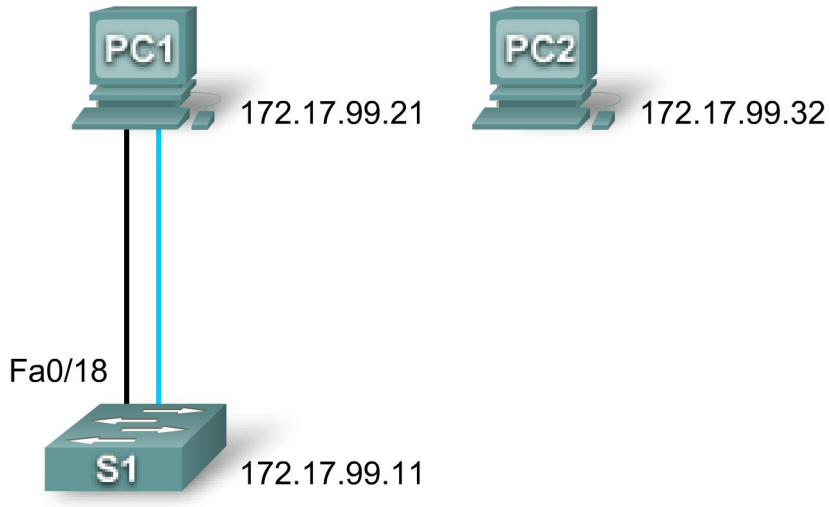

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
S1	**VLAN99**	172.17.99.11	255.255.255.0
PC1	**Carte réseau**	172.17.99.21	255.255.255.0
PC2	**Carte réseau**	172.17.99.32	255.255.255.0

Objectifs pédagogiques

- Configurer la gestion de base du commutateur
- Configurer la sécurité du port dynamique
- Tester la sécurité du port dynamique
- Sécuriser les ports inutilisés

Tâche 1 : configuration de la gestion de base du commutateur

Étape 1 : sur PC1, accédez à la connexion de console au commutateur S1

- Cliquez sur PC1 puis sélectionnez l'onglet **Desktop**. Sélectionnez **Terminal** dans l'onglet **Desktop**.
- Conservez ces paramètres par défaut pour la **configuration du terminal** puis cliquez sur OK :

  Bits par seconde = 9600
  Bits de données = 8
  Parité = Aucune
  Bits d'arrêt = 1
  Contrôle de flux = Aucun
- Vous êtes désormais connecté au commutateur S1. Appuyez sur Entrée pour afficher l'invite du commutateur.

Étape 2 : passage au mode d'exécution privilégié

Pour accéder au mode d'exécution privilégié, tapez la commande **enable**. L'invite passe de **>** à **#**.

```
S1>enable
S1#
```

Vous remarquerez que vous êtes passé au mode d'exécution privilégié sans préciser de mot de passe. Pourquoi l'absence d'un mot de passe en mode d'exécution privilégié compromet-elle la sécurité ?

_____

_____

_____

Étape 3 : passage au mode de configuration globale et configuration du mot de passe du mode privilégié

- Tant que vous êtes en mode d'exécution privilégié, vous pouvez accéder au mode de configuration globale en utilisant la commande **configure terminal**.
- Utilisez la commande **enable secret** pour définir le mot de passe. Dans le cadre de cet exercice, définissez le mot de passe sur la valeur **class**.

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#enable secret class
S1(config)#
```

Remarque : PT n'évalue pas la commande **enable secret**.

Étape 4 : configuration du terminal virtuel et des mots de passe de console, obligation de connexion pour les utilisateurs

Un mot de passe doit être obligatoire pour accéder à la ligne de console. Un utilisateur malveillant peut obtenir des informations cruciales même en mode d'exécution utilisateur de base. En outre, les lignes vty doivent être protégées par un mot de passe avant d'envisager un accès à distance des utilisateurs au commutateur.

- Accédez à l'invite de console à l'aide de la commande **line console 0**.
- Utilisez la commande **password** pour configurer les lignes de console et vty à l'aide du mot de passe **cisco**. Remarque : dans ce cas de figure, PT n'évalue pas la commande **password cisco**.

- Entrez la commande **login**, qui nécessite la saisie d'un mot de passe avant d'accéder au mode d'exécution utilisateur.
- Répétez le processus avec les lignes vty. Utilisez la commande **line vty 0 15** pour accéder à l'invite appropriée.
- Tapez la commande **exit** pour retourner à l'invite de configuration globale.

```
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```

Étape 5 : configuration du chiffrement de mot de passe

Le mot de passe du mode privilégié est déjà chiffré. Pour chiffrer les mots de passe de ligne que vous venez de configurer, entrez la commande **service password-encryption** en mode de configuration globale.

```
S1(config)#service password-encryption
S1(config)#
```

Étape 6 : configuration et test de la bannière MOTD

Configurez le message du jour (MOTD) avec **Authorized Access Only** comme texte. Le texte de la bannière tient compte des majuscules. Assurez-vous de ne pas ajouter d'espaces avant ou après ce texte. Utilisez un séparateur avant et après le texte de la bannière pour en spécifier le début et la fin. Le séparateur **&** est utilisé dans l'exemple suivant. Ceci dit, vous pouvez utiliser tout autre caractère à condition qu'il ne figure pas dans le texte de la bannière. Après la configuration du MOTD, déconnectez-vous du commutateur pour vérifier l'affichage de la bannière à votre reconnexion.

```
S1(config)#banner motd &Authorized Access Only&
S1(config)#end [or exit]
S1#exit

S1 con0 is now available

Press RETURN to get started.

[Entrée]

Authorized Access Only

User Access Verification

Password:
```

- L'invite exige désormais un mot de passe pour passer en mode d'exécution utilisateur. Entrez le mot de passe **cisco**.
- Passez en mode d'exécution privilégié en utilisant le mot de passe **class** et retournez au mode de configuration globale à l'aide de la commande **configure terminal**.

```
Password: [cisco] !Remarque : le mot de passe ne s'affiche pas à la frappe.

S1>enable
Password: [class] !Remarque : le mot de passe ne s'affiche pas à la frappe.
```

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#
```

Étape 7 : vérification des résultats

Votre taux de réalisation doit être de 40 %. Si tel n'est pas le cas, cliquez sur **Check Results** pour vérifier quels composants obligatoires n'ont pas encore été terminés.

Tâche 2 : configuration de la sécurité du port dynamique

Étape 1 : activation de VLAN99

Packet Tracer s'ouvre avec l'interface VLAN 99 désactivée. Cet état ne correspond pas au fonctionnement réel d'un commutateur. Vous devez activer VLAN 99 avec la commande **no shutdown** avant que l'interface ne soit activée dans Packet Tracer.

```
S1(config)#interface vlan 99
S1(config-if)#no shutdown
```

Étape 2 : passage au mode de configuration d'interface pour FastEthernet 0/18 et activation de la sécurité du port

Avant de configurer toute autre commande de sécurité du port sur l'interface, vous devez activer la sécurité du port.

```
S1(config-if)#interface fa0/18
S1(config-if)#switchport port-security
```

Sachez que retourner au mode de configuration globale avant de passer au mode de configuration d'interface pour fa0/18 n'est pas une nécessité.

Étape 3 : configuration du nombre maximum d'adresses MAC

Pour configurer le port afin d'apprendre une seule adresse MAC, définissez **maximum** sur **1** :

```
S1(config-if)#switchport port-security maximum 1
```

Remarque : PT n'évalue pas la commande **switchport port-security maximum 1**. Ceci dit, cette commande est essentielle pour configurer la sécurité du port.

Étape 4 : configuration du port pour ajouter l'adresse MAC à la configuration en cours

Vous pouvez ajouter l'adresse MAC apprise sur le port à la configuration en cours de ce dernier.

```
S1(config-if)#switchport port-security mac-address sticky
```

Remarque : PT n'évalue pas la commande **switchport port-security mac-address sticky**. Ceci dit, cette commande est essentielle pour configurer la sécurité du port.

Étape 5 : configuration du port pour un arrêt automatique si sa sécurité est compromise

Si vous ne configurez pas la commande suivante, le commutateur S1 enregistre uniquement la violation dans les statistiques de sécurité sans pour autant l'arrêter.

```
S1(config-if)#switchport port-security violation shutdown
```

Remarque : PT n'évalue pas la commande **switchport port-security violation shutdown**. Ceci dit, cette commande est essentielle pour configurer la sécurité du port.

Étape 6 : confirmation de l'apprentissage par le commutateur S1 de l'adresse MAC pour PC1

Envoyez une requête ping au commutateur S1 depuis PC1.

Confirmez que le commutateur S1 a désormais une entrée d'adresse MAC statique pour PC1 dans la table MAC :

```
S1#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  99    0060.5c5b.cd23    STATIC      Fa0/18
```

L'adresse MAC est désormais ajoutée à la configuration en cours.

```
S1#show running-config
<résultat omis>
interface FastEthernet0/18
 switchport access vlan 99
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0060.5C5B.CD23
<résultat omis>
S1#
```

Étape 7 : vérification des résultats

Votre taux de réalisation doit être de 70 %. Si tel n'est pas le cas, cliquez sur **Check Results** pour vérifier quels composants obligatoires n'ont pas encore été terminés.

Tâche 3 : test de la sécurité du port dynamique

Étape 1 : déconnexion entre PC1 et le commutateur S1 et connexion de PC2 au commutateur S1

- Pour tester la sécurité du port, supprimez la connexion Ethernet entre PC 1 et le commutateur S1. Si vous déconnectez les câbles de console par mégarde, il vous suffit de les reconnecter.
- Connectez PC2 à Fa0/18 sur le commutateur S1. Attendez que le voyant de liaison orange passe au vert, puis envoyez la requête ping au commutateur S1 depuis PC1. Le port doit s'arrêter automatiquement.

Étape 2 : vérification du rôle du problème de sécurité du port dans son arrêt

Pour vérifier que le port a effectivement été arrêté pour des raisons de sécurité, entrez la commande **show interface fa0/18**.

```
S1#show interface fa0/18
FastEthernet0/18 is down, line protocol is down (err-disabled)
  Hardware is Lance, address is 0090.213e.5712 (bia 0090.213e.5712)
<résultat omis>
```

Le protocole de ligne est désactivé à cause d'une erreur (**err**) liée à l'acceptation d'une trame avec une adresse MAC différente de l'adresse MAC apprise. Cette erreur explique pourquoi le logiciel Cisco IOS a arrêté le port (**disabled**).

Vous pouvez également contrôler si la sécurité a été compromise à l'aide de la commande **show port-security interface fa0/18**.

```
S1#show port-security interface fa0/18
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        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 00E0.F7B0.086E:99
Security Violation Count   : 1
```

Remarquez que l'état du port est **secure-shutdown** et que le nombre de violations de sécurité est **1**.

Étape 3 : restauration de la connexion entre PC1 et le commutateur S1 et réinitialisation de la sécurité du port

Procédez à une déconnexion entre PC2 et le commutateur S1. Reconnectez PC1 au port Fa0/18 sur le commutateur S1.

Remarquez que le port est toujours désactivé bien que vous ayez reconnecté l'ordinateur autorisé sur le port. Vous devez réactiver manuellement un port désactivé suite à une violation de sécurité. Arrêtez le port puis réactivez-le à l'aide de la commande **no shutdown**.

```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface fa0/18
S1(config-if)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to
administratively down
S1(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
S1(config-if)#exit
S1(config)#
```

Étape 4 : test de la connectivité en envoyant une requête ping au commutateur S1 depuis PC1

La requête ping au commutateur S1 depuis PC1 doit aboutir.

À la fin de cette tâche, votre taux de réalisation reste à 70 %.

Tâche 4 : sécurisation des ports inutilisés

La désactivation de tous les ports inutilisés sur un commutateur de réseau est une méthode simple que de nombreux administrateurs choisissent pour protéger leur réseau contre tout accès non autorisé.

Étape 1 : désactivation de l'interface Fa0/17 sur le commutateur S1

Passez en mode de configuration d'interface pour FastEthernet 0/17 et arrêtez le port.

```
S1(config)#interface fa0/17
S1(config-if)#shutdown
```

Étape 2 : test du port en connectant PC2 à Fa0/17 sur le commutateur S1

Connectez PC2 à l'interface Fa0/17 sur le commutateur S1. Remarquez que les voyants de liaison sont rouges. PC2 ne peut pas accéder au réseau.

Étape 3 : vérification des résultats

Votre taux de réalisation doit être de 100 %. Si tel n'est pas le cas, cliquez sur **Check Results** pour vérifier quels composants obligatoires n'ont pas encore été terminés.