Travaux pratiques : configuration des fonctions de sécurité des commutateurs

Topologie

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/1	172.16.99.1	255.255.255.0	N/A
S1	VLAN 99	172.16.99.11	255.255.255.0	172.16.99.1
PC-A	NIC	172.16.99.3	255.255.255.0	172.16.99.1

Objectifs

Partie 1 : configuration de la topologie et initialisation des périphériques

Partie 2 : configuration des paramètres du périphérique de base et vérification de la connectivité

Partie 3 : configuration et vérification de l'accès SSH sur S1

- Configurez l'accès SSH.
- Modifiez les paramètres SSH.
- Vérifiez la configuration SSH.

Partie 4 : configuration et vérification des fonctions de sécurité sur S1

- Configurez et vérifiez les fonctions de sécurité générales.
- Configurez et vérifiez la sécurité des ports.

Contexte/scénario

Il est assez courant de verrouiller l'accès aux PC et aux serveurs, et d'y installer des fonctions de sécurité correctes. Il est important que les périphériques de votre infrastructure réseau, tels que les commutateurs et les routeurs, soient également configurés avec des fonctions de sécurité.

Au cours de ces travaux pratiques, vous appliquerez quelques-unes des méthodes recommandées visant à configurer des fonctions de sécurité sur des commutateurs LAN. Vous activerez exclusivement des sessions SSH et HTTPS sécurisées. Vous configurerez et vérifierez également la sécurité des ports en vue de verrouiller n'importe quel périphérique avec une adresse MAC non reconnue par le commutateur.

Remarque : le routeur utilisé lors des travaux pratiques CCNA est un routeur à services intégrés (ISR) Cisco 1941 équipé de Cisco IOS version 15.2(4)M3 (image universalk9). Le commutateur utilisé est un modèle Cisco Catalyst 2960 équipé de Cisco IOS version 15.0(2) (image lanbasek9). D'autres routeurs, commutateurs et versions de Cisco IOS peuvent être utilisés. Selon le modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent varier de ceux indiqués dans les travaux pratiques.

Reportez-vous au tableau récapitulatif des interfaces de routeur à la fin de ces travaux pratiques pour obtenir les identifiants d'interface corrects.

Remarque : assurez-vous que le routeur et le commutateur ont été réinitialisés et ne possèdent aucune configuration initiale. En cas de doute, contactez votre instructeur ou reportez-vous aux travaux pratiques précédents afin de connaître les procédures d'initialisation et de redémarrage des périphériques.

Ressources requises

- 1 routeur (Cisco 1941 équipé de Cisco IOS version 15.2(4)M3 image universelle ou similaire)
- 1 commutateur (Cisco 2960 équipé de Cisco IOS version 15.0(2) image lanbasek9 ou similaire)
- 1 PC (Windows 7, Vista ou XP, équipé d'un programme d'émulation du terminal tel que Tera Term)
- Câbles de console pour configurer les périphériques Cisco IOS via les ports de console
- Câbles Ethernet conformément à la topologie

Partie 1 : Configuration de la topologie et initialisation des périphériques

Dans la Partie 1, vous allez configurer la topologie du réseau et effacer toutes les configurations, le cas échéant.

Étape 1 : Câblez le réseau conformément à la topologie.

Étape 2 : Initialisez et redémarrez le routeur et le commutateur.

Si des fichiers de configuration ont été préalablement enregistrés sur le routeur ou le commutateur, initialisez et redémarrez ces périphériques à leurs configurations de base.

Partie 2 : Configuration des paramètres du périphérique de base et vérification de la connectivité

Dans la Partie 2, vous allez configurer des paramètres de base sur le routeur, le commutateur et le PC. Reportez-vous à la topologie et à la table d'adressage au début de ces travaux pratiques pour le nom des périphériques et les informations d'adressage.

Étape 1 : Configurez une adresse IP sur PC-A.

Étape 2 : Configurez les paramètres de base sur R1.

a. Configurez le nom d'hôte du périphérique.

b. Désactivez la recherche DNS.

c. Configurez l'adresse IP de l'interface comme indiqué dans la table d'adressage.

d. Attribuez **class** comme mot de passe du mode d'exécution privilégié.

e. Attribuez **cisco** comme mot de passe pour la console et vty et activez la connexion.

f. Chiffrez les mots de passe en clair.

g. Enregistrez la configuration en cours en tant que configuration initiale.

Étape 3 : Configurez les paramètres de base sur S1.

Une bonne pratique de sécurité consiste à attribuer l'adresse IP de gestion du commutateur à un autre VLAN que le VLAN 1 (ou à tout autre VLAN de données avec des utilisateurs finaux). Au cours de cette étape, vous allez créer le VLAN 99 sur le commutateur et lui attribuer une adresse IP.

a. Configurez le nom d'hôte du périphérique.

b. Désactivez la recherche DNS.

c. Attribuez **class** comme mot de passe du mode d'exécution privilégié**.**

d. Attribuez **cisco** en tant que mots de passe de console et vty, puis activez la connexion.

e. Configurez une passerelle par défaut pour S1 en utilisant l'adresse IP de R1.

f. Chiffrez les mots de passe en clair.

g. Enregistrez la configuration en cours en tant que configuration initiale.

h. Créez le VLAN 99 sur le commutateur et nommez-le **Management**.

```
S1(config)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# exit
S1(config)#
```

i. Configurez l'adresse IP de l'interface de gestion du VLAN 99, comme indiqué dans la table d'adressage, puis activez l'interface.

```
S1(config)# interface vlan 99
S1(config-if)# ip address 172.16.99.11 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
S1#
```

j. Exécutez la commande **show vlan** sur S1. Quel est l'état du VLAN 99 ?

k. Exécutez la commande **show ip interface brief** sur S1. Quel est l'état et quel est le protocole de l'interface de gestion du VLAN 99 ?

Pourquoi le protocole est-il « down », même si vous avez exécuté la commande **no shutdown** pour l'interface VLAN 99 ?

l. Attribuez les ports F0/5 et F0/6 au VLAN 99 sur le commutateur.

```
S1# config t
S1(config)# interface f0/5
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# end
```

m. Exécutez la commande **show ip interface brief** sur S1. Quels sont l'état et le protocole affichés de l'interface VLAN 99 ?

Remarque : il existe un délai lorsque les états des ports convergent.

Étape 4 : Vérifiez la connectivité entre les périphériques.

a. À partir de PC-A, envoyez une requête ping à l'adresse de la passerelle par défaut sur R1 ? Les requêtes ping ont-elles abouti ?

b. À partir de PC-A, envoyez une requête ping à l'adresse de gestion de S1. Les requêtes ping ont-elles abouti ?

c. À partir de S1, envoyez une requête ping à l'adresse de la passerelle par défaut sur R1 ? Les requêtes ping ont-elles abouti ?

d. À partir de PC-A, ouvrez un navigateur Web et accédez à http://172.16.99.11. Si le système vous invite à saisir un nom d'utilisateur et un mot de passe, laissez le champ du nom d'utilisateur vide et entrez **class** comme mot de passe. Si le système vous demande si vous voulez une connexion sécurisée, répondez **Non.** Avez-vous pu accéder à l'interface Web sur S1 ?

e. Fermez la session du navigateur sur PC-A.

Remarque : l'interface Web non sécurisée (serveur HTTP) sur un commutateur Cisco 2960 est activée par défaut. Une mesure de sécurité courante consiste à désactiver ce service, comme décrit à la Partie 4.

Partie 3 : Configuration et vérification de l'accès SSH sur S1

Étape 1 : Configurez l'accès SSH sur S1.

a. Activez SSH sur S1. À partir du mode de configuration globale, créez un nom de domaine **CCNA-Lab.com**.

```
S1(config)# ip domain-name CCNA-Lab.com
```

b. Créez une entrée dans la base de données des utilisateurs locaux à utiliser lors de la connexion au commutateur par le biais de SSH. L'utilisateur doit posséder un accès de niveau administrateur.

Remarque : le mot de passe utilisé ici N'est PAS un mot de passe fort. Il est uniquement utilisé pour les besoins de ces travaux pratiques.

```
S1(config)# username admin privilege 15 secret sshadmin
```

c. Configurez l'entrée de transport de telle sorte que les lignes vty permettent uniquement les connexions SSH et utilisez la base de données locale pour l'authentification.

```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
```

d. Générez une clé de chiffrement RSA utilisant un module de 1 024 bits.

```
S1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: S1.CCNA-Lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 3 seconds)

S1(config)#
S1(config)# end
```

e. Vérifiez la configuration SSH et répondez aux questions ci-dessous.

```
S1# show ip ssh
```

Quelle version de SSH le commutateur utilise-t-il ?

Combien de tentatives d'authentification SSH permet-il ?

Quelle est la valeur par défaut du délai d'attente de SSH ?

Étape 2 : Modifiez la configuration de SSH sur S1.

Modifiez la configuration de SSH par défaut.

```
S1# config t
S1(config)# ip ssh time-out 75
S1(config)# ip ssh authentication-retries 2
```

Combien de tentatives d'authentification SSH permet-il ?

Quelle est la valeur du délai d'attente de SSH ?

Étape 3 : Vérifiez la configuration de SSH sur S1.

a. À l'aide d'un logiciel client SSH sur PC-A (par exemple Tera Term), ouvrez une connexion SSH avec S1. Si vous recevez un message sur votre client SSH concernant la clé d'hôte, acceptez-le. Connectez-vous en utilisant le nom d'utilisateur **admin** et le mot de passe **cisco**.

La connexion a-t-elle réussi ?

Quelle invite était affichée sur S1 ? Pourquoi ?

b. Tapez **exit** pour terminer la session SSH sur S1.

Partie 4 : Configuration et vérification des fonctions de sécurité sur S1

Dans la Partie 4, vous allez arrêter les ports inutilisés, désactiver certains services en cours d'exécution sur le commutateur et configurer la sécurité des ports sur la base des adresses MAC. Les commutateurs peuvent être soumis à des attaques de saturation de la table d'adresses MAC, à des attaques d'usurpation d'adresses MAC et à des connexions non autorisées aux ports des commutateurs. Vous allez configurer la sécurité des ports de manière à limiter le nombre d'adresses MAC pouvant être apprises sur un port de commutateur et désactiver le port si ce nombre est dépassé.

Étape 1 : Configurez les fonctions de sécurité générales sur S1.

a. Configurez une bannière MOTD (« message of the day » ou message du jour) sur S1 avec un message d'avertissement de sécurité approprié.

b. Exécutez une commande **show ip interface brief** sur S1. Quels ports physiques sont à l'état « up » ?

c. Arrêtez tous les ports physiques non utilisés sur le commutateur. Utilisez la commande **interface range**.

```
S1(config)# interface range f0/1 – 4
S1(config-if-range)# shutdown
S1(config-if-range)# interface range f0/7 – 24
S1(config-if-range)# shutdown
```

```
S1(config-if-range)# interface range g0/1 – 2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

d. Exécutez la commande **show ip interface brief** sur S1. Quel est l'état des ports F0/1 à F0/4 ?

e. Exécutez la commande **show ip http server status**.

Quel est l'état du serveur HTTP ?

Quel port de serveur utilise-t-il ?

Quel est l'état du serveur sécurisé HTTP ?

Quel port de serveur sécurisé utilise-t-il ?

f. Les sessions HTTP envoient toutes leurs données en texte clair. Vous allez désactiver le service HTTP en cours d'exécution sur S1.

```
S1(config)# no ip http server
```

g. À partir de PC-A, ouvrez une session de votre navigateur Web et accédez à http://172.16.99.11. Quel était votre résultat ?

h. À partir de PC-A, ouvrez une session sécurisée de votre navigateur Web et accédez à https://172.16.99.11. Acceptez le certificat. Connectez-vous sans utiliser de nom d'utilisateur et avec le mot de passe **class**. Quel était votre résultat ?

i. Fermez la session Web sur PC-A.

Étape 2 : Configurez et vérifiez la sécurité des ports sur S1.

a. Notez l'adresse MAC de G0/1 sur R1. À partir de l'interface en ligne de commande de R1, exécutez la commande **show interface g0/1** et notez l'adresse MAC de l'interface.

```
R1# show interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is 30f7.0da3.1821 (bia
3047.0da3.1821)
```

Quelle est l'adresse MAC de l'interface G0/1 de R1 ?

b. À partir de l'interface en ligne de commande de S1, exécutez une commande **show mac address-table** en mode d'exécution privilégié. Recherchez les entrées dynamiques des ports F0/5 et F0/6. Notez-les ci-dessous.

Adresse MAC de F0/5 :

Adresse MAC de F0/6 :

c. Configurez la sécurité de base des ports.

Remarque : cette procédure est généralement exécutée sur tous les ports d'accès du commutateur. Le port F0/5 est affiché ici à titre d'exemple.

1) À partir de l'interface en ligne de commande de S1, passez en mode de configuration d'interface pour le port qui se connecte à R1.

```
S1(config)# interface f0/5
```

2) Arrêtez le port.

```
S1(config-if)# shutdown
```

3) Activez la sécurité des ports sur F0/5.

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

Remarque : l'exécution de la commande **switchport port-security** définit le nombre maximal d'adresses MAC à 1 ainsi que l'action de violation à « shutdown ». Les commandes **switchport port-security maximum** et **switchport port-security violation** peuvent être utilisées pour modifier le comportement par défaut.

4) Configurez une entrée statique pour l'adresse MAC de l'interface G0/1 de R1 notée à l'étape 2a.

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

(xxxx.xxxx.xxxx est l'adresse MAC réelle de l'interface G0/1 du routeur.)

Remarque : vous pouvez également utiliser la commande **switchport port-security mac-address sticky** pour ajouter toutes les adresses MAC sécurisées apprises dynamiquement sur un port (jusqu'au maximum défini) à la configuration en cours du commutateur.

5) Activez le port du commutateur.

```
S1(config-if)# no shutdown
S1(config-if)# end
```

d. Vérifiez la sécurité des ports sur l'interface F0/5 de S1 en exécutant une commande **show port-security interface**.

```
S1# show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-up
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   : 0000.0000.0000:0
Security Violation Count   : 0
```

Quel est l'état des ports de F0/5 ?

e. À l'invite de commande de R1, envoyez une requête ping à PC-A pour vérifier la connectivité.

```
R1# ping 172.16.99.3
```

f. Vous allez maintenant violer la sécurité en modifiant l'adresse MAC sur l'interface du routeur. Passez en mode de configuration d'interface pour G0/1 et arrêtez cette interface.

```
R1# config t
R1(config)# interface g0/1
R1(config-if)# shutdown
```

g. Configurez une nouvelle adresse MAC pour l'interface, en utilisant **aaaa.bbbb.cccc** comme adresse.

```
R1(config-if)# mac-address aaaa.bbbb.cccc
```

h. Si possible, ayez une connexion console ouverte sur S1 en même temps que vous réalisez cette étape. Vous verrez divers messages s'afficher sur la connexion console à S1 indiquant une violation de sécurité. Activez l'interface G0/1 sur R1.

```
R1(config-if)# no shutdown
```

i. À partir du mode d'exécution privilégié sur R1, envoyez une requête ping à PC-A. La requête ping a-t-elle abouti ? Justifiez votre réponse.

j. Sur le commutateur, vérifiez la sécurité des ports à l'aide des commandes indiquées ci-dessous.

```
S1# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
---------------------------------------------------------------------
      Fa0/5            1           1                1         Shutdown
---------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :0
Max Addresses limit in System (excluding one mac per port) :8192

S1# show port-security interface f0/5
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   : aaaa.bbbb.cccc:99
Security Violation Count   : 1

S1# show interface f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
<Résultat omis>

S1# show port-security address
                Secure Mac Address Table
------------------------------------------------------------------------
Vlan     Mac Address       Type                  Ports      Remaining Age
                                                             (mins)
----     -----------       ----                  -----   -------------
  99     30f7.0da3.1821    SecureConfigured      Fa0/5         -
```

```
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :0
Max Addresses limit in System (excluding one mac per port) :8192
```

k. Sur le routeur, arrêtez l'interface G0/1, supprimez l'adresse MAC codée en dur du routeur, puis réactivez l'interface G0/1.

```
R1(config-if)# shutdown
R1(config-if)# no mac-address aaaa.bbbb.cccc
R1(config-if)# no shutdown
R1(config-if)# end
```

l. À partir de R1, envoyez à nouveau une requête ping à PC-A à l'adresse 172.16.99.3. La requête ping a-t-elle abouti ?

m. Exécutez la commande **show interface f0/5** afin de déterminer la cause de l'échec de la requête ping. Notez vos résultats.

n. Effacez l'état « Error Disabled » de F0/5 sur S1.

```
S1# config t
S1(config)# interface f0/5
S1(config-if)# shutdown
S1(config-if)# no shutdown
```

Remarque : il existe un délai lorsque les états des ports convergent.

o. Exécutez la commande **show interface f0/5** sur S1 afin de vérifier que F0/5 n'est plus en mode « Error Disabled ».

```
S1# show interface f0/5
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

p. À partir de l'invite de commande de R1, envoyez à nouveau une requête ping à PC-A. Cette nouvelle requête ping devrait aboutir.

Remarques générales

1. Pourquoi activer la sécurité des ports sur un commutateur ?

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

Tableau récapitulatif des interfaces de routeur

Résumé des interfaces de routeur				
Modèle du routeur	**Interface Ethernet 1**	**Interface Ethernet 2**	**Interface série 1**	**Interface série 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Remarque : pour savoir comment le routeur est configuré, observez les interfaces afin d'identifier le type de routeur ainsi que le nombre d'interfaces qu'il comporte. Il n'est pas possible de répertorier de façon exhaustive toutes les combinaisons de configurations pour chaque type de routeur. Ce tableau inclut les identifiants des combinaisons possibles des interfaces Ethernet et série dans le périphérique. Ce tableau ne comporte aucun autre type d'interface, même si un routeur particulier peut en contenir un. L'exemple de l'interface RNIS BRI peut illustrer ceci. La chaîne de caractères entre parenthèses est l'abréviation normalisée qui permet de représenter l'interface dans les commandes de Cisco IOS.