

Date : 17/03/25

Intervenant : Cédric Surquin.

Cisco

Travail Dirigé

Sécurisation de base d'un switch Cisco



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

1. Configurer l'accès SSH.
2. Modifiez les paramètres SSH.
3. Vérifiez la configuration SSH.

Topologie :

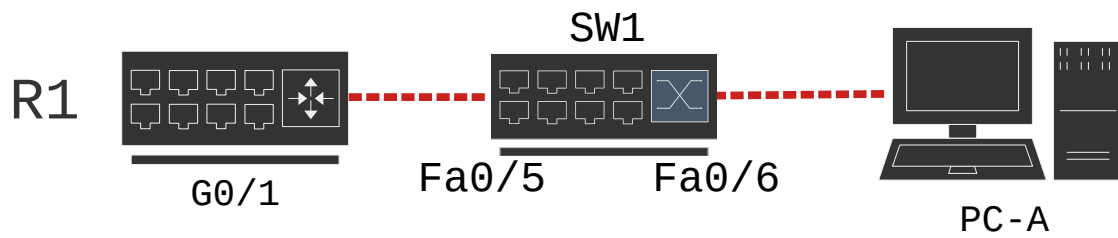


Tableau d'adressage :

Appareils	Interfaces	Adresses IP	Passerelle par défaut
R1	G0/1	172.16.99.1/24	N/A
S1	VLAN99	172.16.99.11/24	172.16.99.1
PC-A	NIC	172.16.99.3/24	172.16.99.1

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 déverrouiller n'importe quel périphérique avec une adresse MAC non reconnue par le commutateur.

Remarque : les routeurs utilisés lors des travaux pratiques CCNA sont des routeurs à services intégrés (ISR) Cisco 1941 équipés de Cisco IOS version 15.2(4)M3 (image universalk9). Les commutateurs utilisés sont des modèles Cisco Catalyst 2960s équipés 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.

Partie 1 : Configuration de la topologie et initialisation des périphériques

Étape 1 :

Câblez le réseau conformément à la topologie

Étape 2 :

Initialisez et redémarrez le routeur et le commutateur.

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 pratique 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 l'accès au port console et lignes vty
- f. Chiffrez les mots de passe en clair dans le fichier de configuration.
- 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 d'administration 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** comme mot de passe pour l'accès au port console et lignes vty
- e. Configurez une passerelle par défaut sur S1 en utilisant l'adresse IP de R1
- f. Chiffrez les mots de passe en clair dans le fichier de configuration.
- 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-if)# name Management
S1(config-if)# exit
```

- i. Attribuez à l'interface VLAN99 l'adresse IP attendue conformément au tableau d'adressage IP

```
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
```

- 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 ?

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

- m. Attribuez les ports F0/5 et F0/6 au VLAN99 sur le commutateur

```
S1(config)# interface f0/5
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# interface fa 0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# end
```

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

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 , 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 ?

c. 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 du SSH

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 pas 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 le module de 1024 bits.

```
S1(config)# crypto key generate rsa general-keys modulus 1024
```

Remarque : Sur Cisco Packet Tracer, il se peut que l'option modulus ne soit pas prise en charge, n'hésitez pas à la retirer de la commande, la longueur de la clé de chiffrement SSH vous sera demandée via le prompt dans tous les cas

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 tentative d'authentification SSH permet-il ? _____

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

Étape 2 : Configurez l'accès SSH sur S1.

Modifiez la configuration de SSH par défaut.

```
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 du client SSH du PC, ouvrez une connexion SSH avec S1. Connectez-vous en utilisant le nom d'utilisateur **admin** et le mot de passe **sshadmin**. La connexion a-t-elle réussi ? _____

Tapez **exit** pour fermer la connexion SSH.

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'adresse MAC, à des attaques d'usurpation d'adresses MAC et à des connexions non autorisées aux ports de 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

- Configurez une bannière MOTD (« message of the day ») sur S1 avec un message d'avertissement de sécurité approprié
- Exécutez une commande **show ip interface brief** sur S1. Quels ports physiques sont à l'état « up » ?
- 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 fa0/7 - 24
S1(config-if-range)# shutdown
S1(config-if-range)# interface range g0/1 - 2
S1(config-if-range)# shutdown
```

- Exécutez la commande **show ip interface brief** sur S1. Quel est l'état des ports f0/1 à f0/4 ? _____

- 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 avec la commande « `no ip http server` »

g. À partir de PC-A, utilisez son 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 ?

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**

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.

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. Arrêtez le port, puis activez la sécurité des ports sur f0/5.

```
S1(config)# interface f0/5
S1(config-if)# shutdown
S1(config-if)# switchport port-security
```

Remarque : l'exécution de la commande `switchport port-security` ne va lier qu'une seule adresse MAC au port, interdisant de ce fait toutes les autres de « passer ». Sa politique par défaut, en cas de MAC étrangère tentant de passer, est « violation »,

qui signifie l'extinction immédiate du port avec signalement d'une erreur. Ces comportements peuvent être ajustés et feront l'objet d'un autre exercice.

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 » fait ici référence à l'adresse MAC réelle de l'interface g0/1 du routeur

Activez le port du switch/commutateur, vérifiez la sécurité des ports sur l'interface f0/5 de S1 en exécutant une commande **show port-security interface**.

```
S1(config-if)# no shutdown
S1(config-if)# end
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 F0/5 ? _____

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

```
R1# ping 172.16.99.3
```

Vous allez maintenant violer la sécurité en modifiant l'adresse MAC sur l'interface du routeur. Passez en mode configuration d'interface pour g0/1 et arrêtez cette interface.

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

e. Configurez une nouvelle adresse MAC pour l'interface, un utilisant aaaa.bbbb.cccc comme adresse.

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

f. 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 de S1 indiquant une violation de sécurité.

R1(config-if)# no shutdown

g. 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.

h. Sur le switch, 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
```

i. Supprimons l'adresse MAC configurée auparavant et activons l'interface à nouveau

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

j. 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 ? _____

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

l. 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 !

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

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

Fin du Travail Dirigé.