

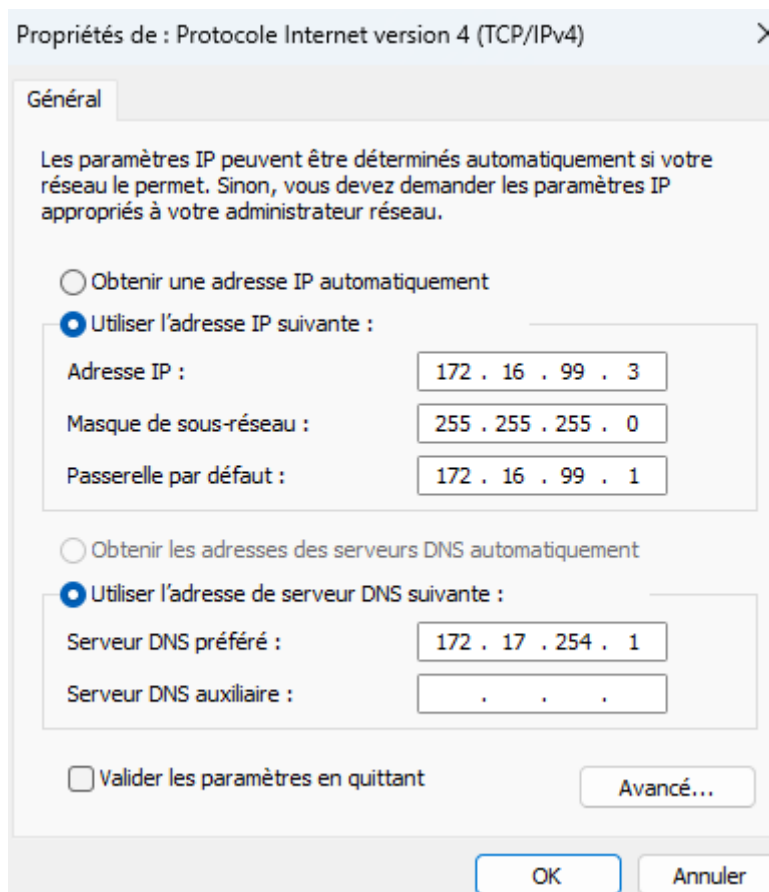
SOMMAIRE

Partie 1 : Configuration de la topologie et initialisation des périphériques.....	1
Partie 2 : configuration des paramètres du périphérique de base et vérification de la connectivé.....	1
Étape 1 : Configurez une adresse IP sur PC-A.....	1
Étape 2 : Configurez les paramètres de base sur R1.....	2
Étape 3 : Configurez les paramètres de base sur S1.....	2
Étape 4 : Vérifiez la connectivité entre les périphériques.....	3
Partie 3 : configuration et vérification de l'accès SSH sur S1.....	4
Étape 1 : Configurez l'accès SSH sur S1.....	4
Étape 3 : Vérifiez la configuration de SSH sur S1.....	5
Partie 4 : configuration et vérification des fonctions de sécurité sur S1.....	5
Étape 1 : Configurez les fonctions de sécurité générales sur S1.....	5
Étape 2 : Configurez et vérifiez la sécurité des ports sur S1.....	6

Partie 1 : Configuration de la topologie et initialisation des périphériques

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

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



Étape 2 : Configurez les paramètres de base sur R1.

c. Reconfiguré l'adresse IP de l'interface comme indiqué dans la table d'adressage. Et enregistre la configuration

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/1
R1(config-if)#ip add 172.16.99.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#^Z
R1#
```

```
R1#sh ip int br
Interface                IP-Address      OK? Method Status
-----
Loopback0                 192.168.1.1    YES NVRAM  up
Embedded-Service-Engine0/0 unassigned     YES NVRAM  administratively down
GigabitEthernet0/0       192.168.1.1    YES NVRAM  down
GigabitEthernet0/1       172.16.99.1    YES manual up
Serial0/0/0               192.168.2.1    YES NVRAM  down
Serial0/0/1               unassigned     YES NVRAM  administratively down
```

Étape 3 : Configurez les paramètres de base sur S1.

a. Configurez le nom d'hôte du périphérique. désactivez la recherche DNS.,attribué **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.configurez une passerelle par défaut pour S1 en utilisant l'adresse IP de R1.chiffrez les mots de passe en clair.

```
switch1(config)#no ip domain lookup
switch1(config)#hostname S1
S1(config)#enable secret class
S1(config)#line con 0
S1(config-line)#pass
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#service pass
S1(config-line)#exi
S1(config)#service pass
S1(config)#service password-enc
S1(config)#service password-encryption
S1(config)#^Z
S1#
```

```
S1(config)#ip default
S1(config)#ip default
S1(config)#ip default-gateway 172.16.99.1
S1(config)#
```

h. Créez le VLAN 99 sur le commutateur nommé **Management**.

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

TP6 - Configuration des fonctions de sécurité du commutateur

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

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

```
S1(config)#int vlan 99
S1(config-if)#ip add 172.16.99.11 255.255.255.0
S1(config-if)#no shut
S1(config-if)#end
S1#
```

```
VLAN Name                Status
-----
1    default                active
99   Management              active
```

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'état est « up » et le protocole est « down ».

```
Vlan99          172.16.99.11    YES manual up        down
FastEthernet0/1 unassigned     YES unset  down        down
FastEthernet0/2 unassigned     YES unset  down        down
```

Pourquoi le protocole est-il down , même si vous avez exécuté la commande **no shutdown** pour l'interface VLAN99 ? Aucun port physique n'a été attribué au VLAN 99 sur le commutateur.

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

```
S1(config)#int f0/5
S1(config-if)#switchp
S1(config-if)#switchport mode acce
S1(config-if)#switchport mode access
S1(config-if)#swit
S1(config-if)#switchport access vlan 99
S1(config-if)#int f0/6
S1(config-if)#switchp mod acce
S1(config-if)#switchp mod access
S1(config-if)#switchp
*Mar  1 00:25:45.567: %LINEPROTO-5-UPDOWN:
% Incomplete command.
S1(config-if)#switchp access vlan 99
```

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

```
S1#sh ip int br
Interface          IP-Address      OK? Method Status  Protocol
Vlan1              19.168.1.101   YES NVRAM  up      down
Vlan99             172.16.99.11  YES manual up       up
```

Étape 4 : Vérifiez la connectivité entre les périphériques.

TP6 - Configuration des fonctions de sécurité du commutateur

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

```
PS C:\Users\Administrateur> ping 172.16.99.1
```

```
Envoi d'une requête 'Ping' 172.16.99.1 avec 32 octets de données :  
Réponse de 172.16.99.1 : octets=32 temps<1ms TTL=255  
Réponse de 172.16.99.1 : octets=32 temps<1ms TTL=255  
Réponse de 172.16.99.1 : octets=32 temps<1ms TTL=255  
Réponse de 172.16.99.1 : octets=32 temps=1 ms TTL=255
```

```
Statistiques Ping pour 172.16.99.1:
```

```
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),  
Durée approximative des boucles en millisecondes :  
Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

```
PS C:\Users\Administrateur> ping 172.16.99.11
```

```
Envoi d'une requête 'Ping' 172.16.99.11 avec 32 octets de données :  
Délai d'attente de la demande dépassé.  
Réponse de 172.16.99.11 : octets=32 temps=2 ms TTL=255  
Réponse de 172.16.99.11 : octets=32 temps=1 ms TTL=255  
Réponse de 172.16.99.11 : octets=32 temps=2 ms TTL=255
```

- 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 ? Oui

```
S1#ping 172.16.99.1  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 172.16.99.1, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/203/1007 ms  
S1#
```

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

Étape 1 : Configurez l'accès SSH sur S1.

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

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

- b. Crée une entrée dans la base de données des utilisateurs locaux à utiliser lors de la connexion au

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

TP6 - Configuration des fonctions de sécurité du commutateur

c. Configurer 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)#transpo
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#exit
S1(config)#
```

d. Générer 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 7 seconds)
S1(config)#
```

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 ? Oui

```
login as: admin
Keyboard-interactive authentication prompts from server
Password:
End of keyboard-interactive prompts from server

S1#
```

Quelle invite était affichée sur S1 ? Pourquoi ?

S1 affiche l'invite en mode d'exécution privilégié, car l'option 15 de privilège a été utilisée lors de la configuration du nom d'utilisateur et du mot de passe.

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

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

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 » ?

```
FastEthernet0/5    unassigned    YES unset    up
FastEthernet0/6    unassigned    YES unset    up
FastEthernet0/7    unassigned    YES unset    down
```

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

```
S1(config)#int ran g0/1 - 2
S1(config-if-range)#shut
S1(config-if-range)#int range f0/1 - 4
S1(config-if-range)#shut
S1(config-if-range)#int ran f0/7 - 24
S1(config-if-range)#shut
```

TP6 - Configuration des fonctions de sécurité du commutateur

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

```
Vlan99          172.16.99.11    YES manual up      up
FastEthernet0/1 unassigned     YES unset  administratively down down
FastEthernet0/2 unassigned     YES unset  administratively down down
FastEthernet0/3 unassigned     YES unset  administratively down down
FastEthernet0/4 unassigned     YES unset  administratively down down
```

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

a. Noté 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

Quelle est l'adresse MAC de l'interface G0/1 de R1 ?
il s'agit de e02f.6dee.f6f1.

```
R1#sh int g0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is e02f.6dee.f6f1 (bia e02f.6dee.f6f1
)
```

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 : e02f.6dee.f6f1 1

Adresse MAC de F0/6 : 40ae;30cl.f4bd

```
99    40ae.30cl.f4bd    DYNAMIC    Fa0/6
99    e02f.6dee.f6f1    DYNAMIC    Fa0/5
```

c. Configuration la sécurité de base des ports

```
S1(config)#int f0/5
S1(config-if)#shut
S1(config-if)#switch port-
S1(config-if)#switch port-security
S1(config-if)#switch
S1(config-if)#switchport port
S1(config-if)#switchport port-security mac
S1(config-if)#switchport port-security mac-address e02f.6dee.f6f1
S1(config-if)#no shut
S1(config-if)#end
S1#
```

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

```
S1#sh port-security int 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
S1#
```

TP6 - Configuration des fonctions de sécurité du commutateur

Quel est l'état des ports de F0/5 ?

L'état est « Secure-up », ce qui signifie que le port est sécurisé, mais que l'état et le protocole sont « up ».

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
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R1#
```

f. ont a 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 configure une nouvelle adresse MAC pour l'interface, en utilisant aaaa.bbbb.cccc comme adresse.

```
R1(config)#int g0/1
R1(config-if)#shut
R1(config-if)#
Feb 11 07:40:43.182: %LINK-5-
```

```
R1#conf t
Enter configuration commands, one per
R1(config)#int g0/1
R1(config-if)#shut
R1(config-if)#
Feb 11 07:40:43.182: %LINK-5-CHANGED:
e to administratively down
```

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.

Non, le port F0/5 sur S1 est arrêté en raison de la violation de sécurité.

```
R1#ping 172.16.99.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

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

```
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int g0/1
S1(config-if)#^Z
S1#sh port
S1#sh 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#sh port-se
S1#sh port-security int 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
```

TP6 - Configuration des fonctions de sécurité du commutateur

```
S1#sh int f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 2401.c767.3b85 (bia 2401.c767.3b85)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
```

- 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)#int g0/1
R1(config-if)#no mac-add
R1(config-if)#no mac-address aaaa.bbbb.cccc
R1(config-if)#no sh
R1(config-if)#end
R1#
```

- 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 ?
Non

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

Le port F0/5 sur S1 est toujours dans un état « Error Disabled ».

```
S1#sh int f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 2401.c767.3b85 (bia 2401.c767.3b85)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec
```

- n. Effacez l'état « Error Disabled » de F0/5 sur S1 et exécutez la commande show interface f0/5 sur S1 afin de vérifier que F0/5 n'est plus en mode « Error Disabled ».

```
R1(config-if)#shut
R1(config-if)#dhut
^
Invalid input detected at '^' marker.

R1(config-if)#
R1(config-if)#
R1(config-if)#no shut
R1(config-if)#^Z
R1#sh int f0/5
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 2401.c767.3b85 (bia 2401.c767.3b85)
```

- 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

```
FastEthernet0/1, changed state to up
R1#ping 172.16.99.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1#
```

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

Afin d'empêcher les périphériques non autorisés d'accéder à votre réseau en cas de connexion à un commutateur de celui-ci

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

Une excellente raison est qu'un utilisateur n'a pas pu connecter un périphérique au commutateur sur un port non utilisé et accéder au LAN.