

## Travaux pratiques : configuration des fonctions de sécurité des commutateurs (2.2.4.11)

### Sommaire :

#### 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.
- Étape 3 : Configurez les paramètres de base sur S1.
- Étape 4 : Vérifiez la connectivité entre les périphériques.

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

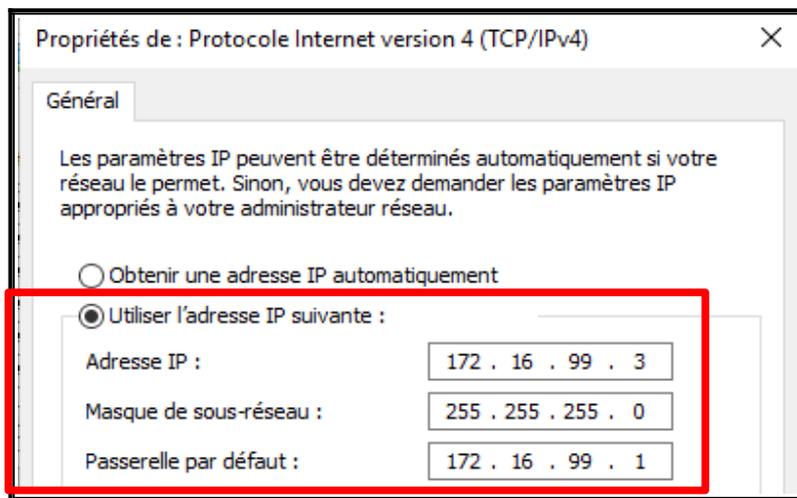
- Étape 1 : Configurez l'accès SSH sur S1.
- Étape 2 : Modifiez la configuration de SSH sur S1.
- Étape 3 : Vérifiez la configuration de SSH sur S1.

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

- Étape 1 : Configurez les fonctions de sécurité générales sur S1.
- Étape 2 : Configurez et vérifiez la sécurité des ports sur S1.

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

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



1ère étape : Nous configurons l'interface IPv4 du PC-A.

### Étape 2 : Configurez les paramètres de base sur R1.

```
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#int g0/1
R1(config-if)#ip address 172.16.99.1 255.255.255.0
R1(config-if)#no shutdown
```

```
R1(config-if)#enable secret class
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exec-timeout 5 0
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exec-timeout 5 0
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#service password-encryption
```

**Configuration complète du routeur R1.**

### Étape 3: Configurez les paramètres de base sur S1.

```
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#enable secret class
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exec-timeout 5 0
S1(config-line)#logging synchronous
S1(config-line)#exit
S1(config)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exec-timeout 5 0
S1(config-line)#logging synchronous
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#ip default-gateway 172.16.99.1
```

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

```
S1(config)#interface vlan 99
S1(config-if)#ip
*Mar 1 00:23:33.228: %LINEPROTO-5-UPDOWN: Line protocol
anged state to down
S1(config-if)#ip address 172.16.99.11 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#end
```

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
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
*Mar 1 00:25:42.144: %LINEPROTO-5-UPDOWN: Line protocol on I
anged state to up
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 99
S1(config-if)#end
```

**Configuration complète du switch S1 ainsi que la création d'un Vlan.**

#### Étape 4 : Vérifiez la connectivité entre les périphériques.

```
C:\Users\jruggeri>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=1 ms 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
```

**1ère étape** : Nous effectuons un premier ping depuis PC-A à la passerelle par défaut sur R1. Celui-ci fonctionne correctement.

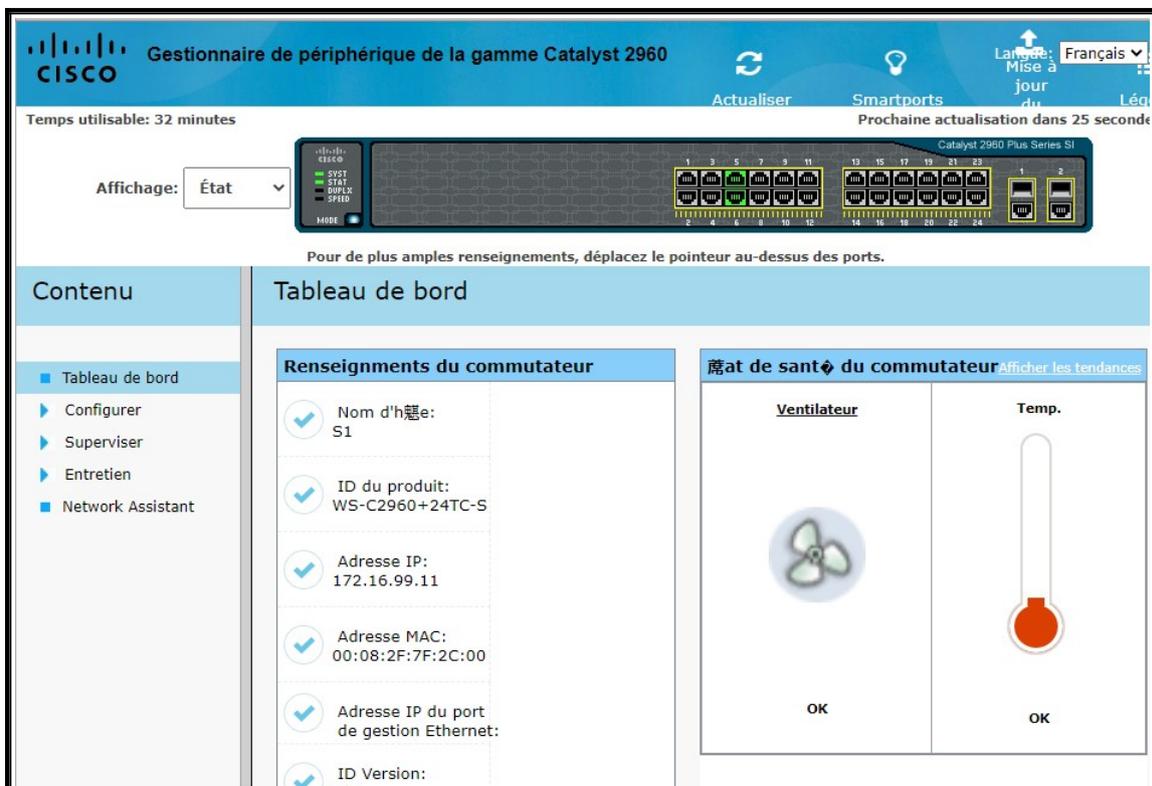
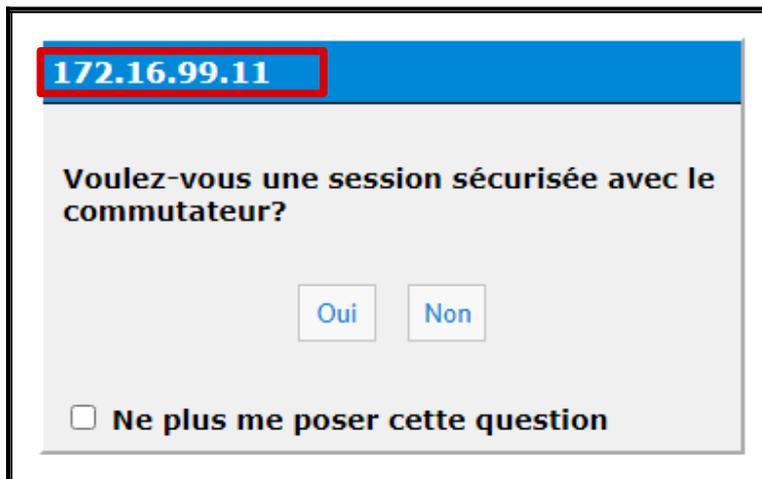
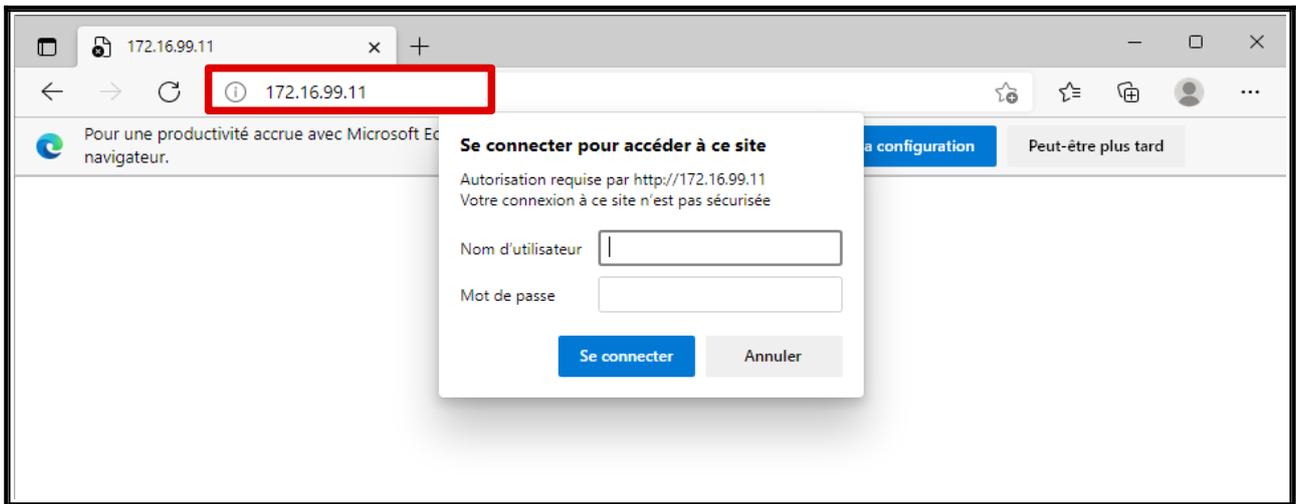
```
C:\Users\jruggeri>ping 172.16.99.11
Envoi d'une requête 'Ping' 172.16.99.11 avec 32 octets de données :
Réponse de 172.16.99.11 : octets=32 temps=2 ms TTL=255
Réponse de 172.16.99.11 : octets=32 temps=1 ms TTL=255
Réponse de 172.16.99.11 : octets=32 temps=1 ms TTL=255
Réponse de 172.16.99.11 : octets=32 temps=2 ms TTL=255

Statistiques Ping pour 172.16.99.11:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
```

**2ème étape** : Cette fois-ci nous envoyons un ping depuis PC-A à l'adresse de gestion de S1. Celui-ci fonctionne correctement.

```
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
```

**3ème étape** : Cette fois-ci depuis S1 nous envoyons un ping à la passerelle par défaut sur R1. Celui-ci fonctionne correctement.



**4ème étape :** Pour terminer depuis le navigateur de PC-A nous accédons à l'interface web du switch S1.

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

Étape 1 : Configurez l'accès SSH sur S1.

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

1ère étape : Nous activons **SSH** sur S1 et créons un nom de domaine **CCNA-Lab.com** .

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

2ème étape : Création d'une **entrée** dans la base de données des utilisateurs locaux à utiliser lors de la connexion au commutateur par le biais de **SSH**.

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

3ème étape : Nous configurons l'entrée de transport afin que les lignes **vty** permettent uniquement les connexions **SSH**.

```
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 6 seconds)

S1(config)#end
S1#
```

4ème étape : Génération d'une **clé** de chiffrement **RSA avec un modulus de 1 024 bits**.

```

S1#show ip ssh
SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc
MAC Algorithms:hmac-shal,hmac-shal-96
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): TP-self-signed-796863488
ssh-rsa AAAAB3NzaClyc2EAAAADAQABAAQgQDM4b55+Wj52+BF0112D+yv9RRMgBD/nSbmPTw/Ji10
3lqTfGfNI9E/QVgSr6tMBQuD+GcocQPnIUXFMSEoYadBUVeNYyLITIY5/t7S3dHeH7SNaxeZq33KtQZi
lvDCKYrLzDS5NBtp4nBRVrf6PTmLEWGxSkeIFk5xVaxDhKJIrw==

```

**5ème étape :** Nous vérifions la configuration SS.

**Étape 2 :** Modifiez la configuration de SSH sur S1.

```

S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#ip ssh time-out 75
S1(config)#ip ssh authentication-retries 2

```

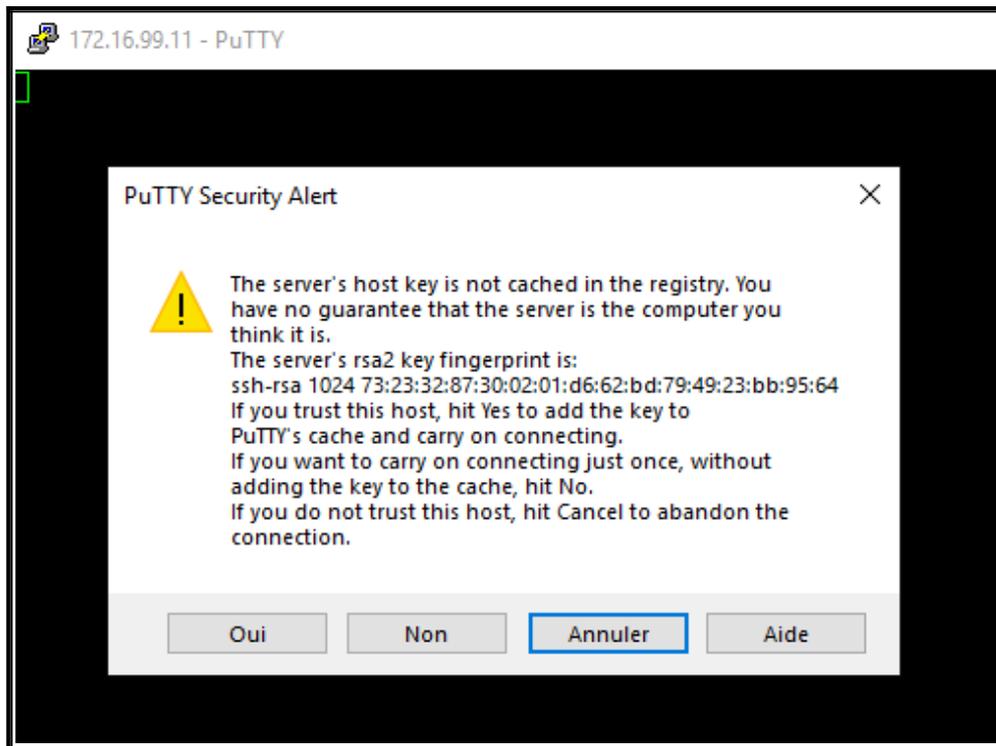
```

S1#show ip ssh
SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc
MAC Algorithms:hmac-shal,hmac-shal-96
Authentication timeout: 75 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): TP-self-signed-796863488
ssh-rsa AAAAB3NzaClyc2EAAAADAQABAAQgQDM4b55+Wj52+BF0112D+yv9RRMgBD/nSbmPTw/Ji10
3lqTfGfNI9E/QVgSr6tMBQuD+GcocQPnIUXFMSEoYadBUVeNYyLITIY5/t7S3dHeH7SNaxeZq33KtQZi
lvDCKYrLzDS5NBtp4nBRVrf6PTmLEWGxSkeIFk5xVaxDhKJIrw==

```

**1ère étape :** Nous modifions la configuration de SSH par défaut.

**Étape 3 :** Vérifiez la configuration de SSH sur S1.



Via le logiciel Putty depuis PC-A, nous ouvrons une connexion SSH avec S1, nous recevons ce message et l'acceptons pour par la suite se connecter avec l'utilisateur admin et sont mot de passe cisco.

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

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

```
S1(config)#banner motd #Securite approprie#  
S1(config)#
```

1ère étape : Configuration d'une **bannière MOTD** sur **S1** avec un message d'avertissement de **sécurité approprié**.

```
S1#show ip interface brief  
Interface IP-Address OK? Method Status Protocol  
Vlan1 unassigned YES NVRAM up down  
Vlan99 172.16.99.11 YES NVRAM up up  
FastEthernet0/1 unassigned YES unset down down  
FastEthernet0/2 unassigned YES unset down down  
FastEthernet0/3 unassigned YES unset down down  
FastEthernet0/4 unassigned YES unset down down  
FastEthernet0/5 unassigned YES unset up up  
FastEthernet0/6 unassigned YES unset up up  
FastEthernet0/7 unassigned YES unset down down
```

2ème étape : Cette commande permet d'observer les ports physiques sur l'état « up », nous remarquons par exemple « FastEthernet0/5 » ou encore « FastEthernet0/6 ».

```

S1(config)#interface range f0/1 - 4
S1(config-if-range)#shutdown
S1(config-if-range)#interface
*Mar 1 00:20:04.402: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state
to administratively down
*Mar 1 00:20:04.411: %LINK-5-CHANGED: Interface FastEthernet0/2, changed state
to administratively down
*Mar 1 00:20:04.419: %LINK-5-CHANGED: Interface FastEthernet0/3, changed state
to administratively down
*Mar 1 00:20:04.419: %LINK-5-CHANGED: Interface FastEthernet0/4, changed state
to administratively down
S1(config-if-range)#interface range f0/7 - 24
S1(config-if-range)#shutdown
S1(config-if-range)#
*Mar 1 00:20:27.412: %LINK-5-CHANGED: Interface FastEthernet0/7, changed state
to administratively down
*Mar 1 00:20:27.412: %LINK-5-CHANGED: Interface FastEthernet0/8, changed state
to administratively down
*Mar 1 00:20:27.421: %LINK-5-CHANGED: Interface FastEthernet0/9, changed state
to administratively down
*Mar 1 00:20:27.421: %LINK-5-CHANGED: Interface FastEthernet0/10, changed state
to administratively down
*Mar 1 00:20:27.429: %LINK-5-CHANGED: Interface FastEthernet0/11, changed state
to
S1(config-if-range)#intadministratively down
*Mar 1 00:20:27.429: %LINK-5-CHANGED: Interface FastEthernet0/12, changed state
to administratively down
*Mar 1 00:20:27.437: %LINK-5-CHANGED: Interface FastEthernet0/13, changed state
to administratively down
*Mar 1 00:20:27.437: %LINK-5-CHANGED: Interface FastEthernet0/14, changed state
to administratively down
*Mar 1 00:20:27.446: %LINK-5-CHANGED: Interface FastEthernet0/15, changed state
to administratively down
*Mar 1 00:20:27.446: %LINK-5-CHANGED: Interface FastEtherne
S1(config-if-range)#interf
S1(config-if-range)#interfct0/16, changed state to administratively down
*Mar 1 00:20:27.463: %LINK-5-CHANGED: Interface FastEthernet0/17, changed state
to administratively down
*Mar 1 00:20:27.463: %LINK-5-CHANGED: Interface FastEthernet0/18, changed state
to administratively down
*Mar 1 00:20:27.471: %LINK-5-CHANGED: Interface FastEthernet0/19, changed state
to administratively down
*Mar 1 00:20:27.471: %LINK-5-CHANGED: Interface FastEthernet0/20, changed state
to administratively down
*Mar 1 00:20:27.479: %LINK-5-CHANGE
S1(config-if-range)#interfcd: Interface FastEthernet0/21, changed state to admin
istratively down
*Mar 1 00:20:27.479: %LINK-5-CHANGED: Interface FastEthernet0/22, changed state
to administratively down
*Mar 1 00:20:27.488: %LINK-5-CHANGED: Interface FastEthernet0/23, changed state
to administratively down
*Mar 1 00:20:27.488: %LINK-5-CHANGED: Interface FastEthernet0/24, changed state
to administratively down
S1(config-if-range)#interface range g0/1 - 2
S1(config-if-range)#shutdown
S1(config-if-range)#end
S1#
*Mar 1 00:21:58.034: %SYS-5-CONFIG_I: Configured from console by console
*Mar 1 00:21:58.361: %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed sta
te to administratively down
*Mar 1 00:21:58.370: %LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
S1#

```

**3ème étape :** Nous arrêtons tous les ports physiques non utilisés sur le commutateur.

```
Sl#show ip interface brief
Interface          IP-Address      OK? Method Status      Protoco
Vlan1              unassigned     YES NVRAM  up          down
Vlan99            172.16.99.11   YES NVRAM  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
FastEthernet0/5   unassigned     YES unset  up          up
FastEthernet0/6   unassigned     YES unset  up          up
FastEthernet0/7   unassigned     YES unset  administratively down down
FastEthernet0/8   unassigned     YES unset  administratively down down
FastEthernet0/9   unassigned     YES unset  administratively down down
FastEthernet0/10  unassigned     YES unset  administratively down down
FastEthernet0/11  unassigned     YES unset  administratively down down
FastEthernet0/12  unassigned     YES unset  administratively down down
FastEthernet0/13  unassigned     YES unset  administratively down down
FastEthernet0/14  unassigned     YES unset  administratively down down
FastEthernet0/15  unassigned     YES unset  administratively down down
FastEthernet0/16  unassigned     YES unset  administratively down down
FastEthernet0/17  unassigned     YES unset  administratively down down
FastEthernet0/18  unassigned     YES unset  administratively down down
FastEthernet0/19  unassigned     YES unset  administratively down down
FastEthernet0/20  unassigned     YES unset  administratively down down
FastEthernet0/21  unassigned     YES unset  administratively down down
FastEthernet0/22  unassigned     YES unset  administratively down down
FastEthernet0/23  unassigned     YES unset  administratively down down
FastEthernet0/24  unassigned     YES unset  administratively down down
GigabitEthernet0/1 unassigned     YES unset  administratively down down
GigabitEthernet0/2 unassigned     YES unset  administratively down down
Sl#
```

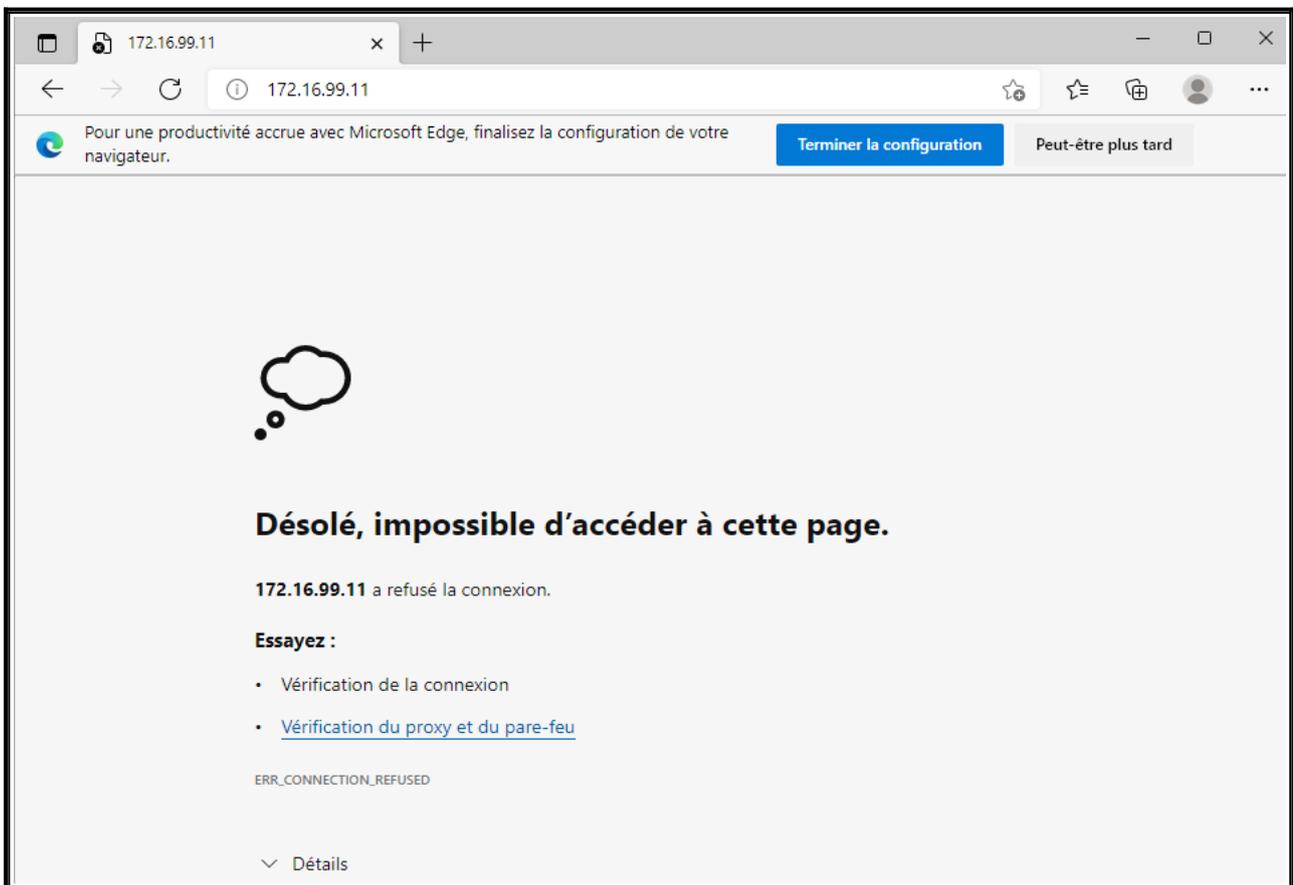
**4ème étape :** Nous saisissons cette commande afin d'observer l'état des ports, on remarque que tous les ports non utilisés sont désormais administrativement éteints.

```
Sl#show ip http server status
HTTP server status: Enabled
HTTP server port: 80
HTTP server authentication method: enable
HTTP server access class: 0
HTTP server base path: flash:/c2960-lanlitek9-mz.152-4.E/html
HTTP server help root:
Maximum number of concurrent server connections allowed: 16
Maximum number of secondary server connections allowed: 5
Server idle time-out: 180 seconds
Server life time-out: 180 seconds
Server session idle time-out: 180 seconds
Maximum number of requests allowed on a connection: 25
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5
rc4-128-sha aes-128-cbc-sha aes-256-cbc-sha dhe-aes-128-cbc-sha
dhe-aes-256-cbc-sha
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:
HTTP secure server active session modules: ALL
```

**5ème étape :** Cette commande permet d'afficher différentes informations sur le statut du serveur http.

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

**6ème étape :** Nous désactivons par la suite le **service http**.



**7ème étape :** Nous tentons d'ouvrir depuis **PC-A** l'interface web du commutateur avec **http**. Celle-ci ne fonctionne pas puisque nous avons désactivé le service.

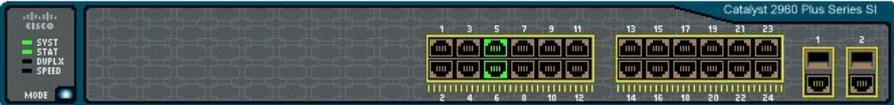
172.16.99.11 : Cisco Device Man... x +

Non sécurisé | <https://172.16.99.11>

Pour une productivité accrue avec Microsoft Edge, finalisez la configuration de votre navigateur. [Terminer la configuration](#) [Peut-être plus tard](#)

**CISCO** Gestionnaire de périphérique de la gamme Catalyst 2960 Actualiser Smartports Lancez la mise à jour du jour Français

Temps utilisable: 26 minutes Prochaine actualisation dans 49 secondes

Affichage: État 

Pour de plus amples renseignements, déplacez le pointeur au-dessus des ports.

### Contenu

- Tableau de bord
- Configurer
- Superviser
- Entretien
- Network Assistant

### Tableau de bord

#### Renseignements du commutateur

- Nom d'hôte: S1
- ID du produit: WS-C2960+24TC-S
- Adresse IP: 172.16.99.11
- Adresse MAC: 00:08:2F:7F:2C:00
- Adresse IP du port de gestion Ethernet:
- ID Version: V01
- Numéro de série: FOC1823Z3AF
- Logiciel: 15.2(4)E
- Personne-ressource:

#### État de santé du commutateur [Afficher les tendances](#)

##### Ventilateur



OK

##### Temp.



OK

**8ème étape :** Nouvelle tentative de connexion à l'interface web du commutateur mais cette fois-ci avec le service https. Donc celui-ci fonctionne puisque le **service https** n'est pas désactivé.

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

```
R1#show interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is e02f.6d9f.cf61 (bia e02f.6d9f.cf61
)
```

**1ère étape :** Nous notons l'adresse MAC de l'interface.

99	503e.aa03.670e	DYNAMIC	Fa0/6
99	e02f.6d9f.cf61	DYNAMIC	Fa0/5

**2ème étape :** Nous notons les adresses **MAC** de ces deux interface à l'aide de la commande « **show mac address-table** ».

```
S1(config)#interface f0/5
S1(config-if)#shutdown
S1(config-if)#switch
*Mar  1 00:34:15.427: %LINK-5-CHANGED: Interface FastEthernet0/5, changed state
to administratively down
*Mar  1 00:34:16.433: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/5, changed state to down
S1(config-if)#switchport port-security
```

```
S1(config-if)#switchport port-security mac-address e02f.6d9f.cf61
```

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

**3ème étape :** Nous configurons la **sécurité** de base des ports, ici la procédure ce fait pour l'interface **f0/5**.

```
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
```

**4ème étape :** Nous vérifions la sécurité sur l'interface **f0/5** de **S1**.

```
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
```

**5ème étape :** Depuis R1 nous envoyons un ping à PC-A afin de vérifier la connectivité. Celui-ci fonctionne.

```
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface g0/1
R1(config-if)#shutdown
```

**6ème étape :** Nous arrêtons l'interface g0/1.

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

**7ème étape :** Configuration d'une nouvelle adresse MAC pour l'interface g0/1.

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

**8ème étape :** Nous réactivons l'interface g0/1.

```
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)
```

**9ème étape :** Depuis **R1** nous envoyons un ping à **PC-A**.

```
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)
```

```
S1#show port-security address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
(mins)
-----
99      e02f.6d9f.cf61   SecureConfigured    Fa0/5    -
-----
Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

**10ème étape :** Nous vérifions la sécurité de l'interface **f0/5**.

```

R1(config)#int g0/1
R1(config-if)#shutdown
R1(config-if)#no mac
Jan 26 12:46:26.875: %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
R1(config-if)#no mac-address aaaa.bbbb.cccc
R1(config-if)#no shutdown
R1(config-if)#end
R1#
Jan 26 12:46:44.671: %SYS-5-CONFIG_I: Configured from console by console
R1#
Jan 26 12:46:45.371: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down

```

**11ème étape :** Nous arrêtons de nouveau l'interface g0/1 et effaçons l'adresse MAC.

```

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)

```

**12ème étape :** Nous effectuons un nouveau ping sur **PC-A** depuis **R1**. Celui-ci ne fonctionne pas.

```

S1#show interface f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
Hardware is Fast Ethernet, address is 0008.2f7f.2c05 (bia 0008.2f7f.2c05)
MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255

```

**13ème étape :** Nous saisissons cette commande pour déterminer la cause de l'échec du ping. Le port **f0/5** est toujours en « **err-disabled** ».

```

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

```

**14ème étape :** Nous supprimons donc l'état de f0/5.

```
S1#show interface f0/5
FastEthernet0/5 is up, line protocol is up (connected)
```

**15ème étape :** Nous vérifions par la suite le nouvel état de **f0/5** celui-ci est en « **connected** ».

```
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
```

**16ème étape :** Nouvelle tentative de ping sur **PC-A** depuis **R1** après avoir modifier l'état de f0/5. Celui-ci fonctionne correctement.