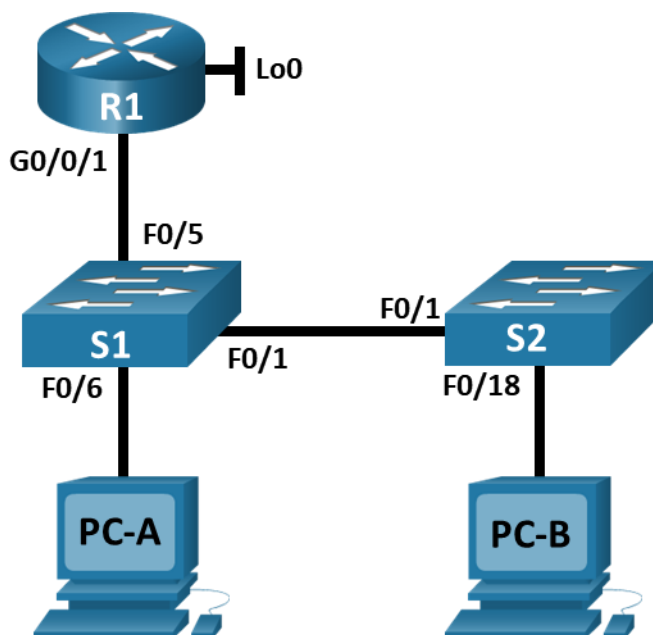


# Travaux pratiques - Configuration de la sécurité du commutateur

## (Version de l'instructeur)

**Remarque de l'instructeur:** le texte en rouge ou surligné en gris apparaît uniquement dans la version de l'instructeur.

### Topologie



### Table d'adressage

Périphérique	Interface /Vlan	Adresse IP	Masque de sous-réseau
R1	G0/0/1	192.168.10.1	255.255.255.0
	Bouclage 0	10.10.1.1	255.255.255.0
S1	VLAN 10	192.168.10.201	255.255.255.0
S2	VLAN 10	192.168.10.202	255.255.255.0
PC – A	Carte réseau (NIC)	DHCP	255.255.255.0
PC – B	Carte réseau (NIC)	DHCP	255.255.255.0

### Objectifs

#### Partie 1: Configurer les périphériques réseau.

- Câblage du réseau.

- Configurer R1.
- Configurer et vérifier les paramètres de base du commutateur.

### Partie 2: Configurer les VLAN sur Les Commutateurs.

- Configurer VLAN 10.
- Configurer le SVI pour VLAN 10.
- Configurer VLAN 333 avec le nom natif sur S1 et S2.
- Configurer VLAN 999 avec le nom ParkingLot sur S1 et S2.

### Partie 3: Configurer la Sécurité du Commutateur.

- Mettre en œuvre le trunc 802.1Q
- Configurer les ports d'accès.
- Sécuriser et désactiver les ports de commutateurs inutilisés.
- Documenter et mettre en œuvre les fonctions de sécurité des ports.
- Mettre en œuvre la sécurité d'espionnage DHCP.
- Mettre en œuvre PortFast et la protection BPDU.
- Vérifier la connectivité de bout en bout.

## Contexte/scénario

Ces travaux pratiques passent en revue les fonctionnalités de sécurité de couche 2 précédemment apprises.

**Remarque:** les routeurs utilisés dans les travaux pratiques CCNA sont Cisco 4221 version 16.9.3 de Cisco IOS XE (image universalk9). Les commutateurs utilisés dans les travaux pratiques sont des modèles Cisco Catalyst 2960s version 15.0(2) de Cisco IOS (image lanbasek9). D'autres routeurs, commutateurs et d'autres 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 ce qui est indiqué dans les travaux pratiques. Reportez-vous au tableau récapitulatif de l'interface du routeur à la fin de ces travaux pratiques pour obtenir les identifiants d'interface corrects.

**Remarque:** vérifiez que les paramètres des commutateurs ont été effacés et qu'ils ne présentent aucune configuration initiale. En cas de doute, contactez votre instructeur.

**Remarque de l'instructeur:** referez au guide de travaux pratiques de l'instructeur pour initialiser et recharger les périphériques.

## Ressources requises

- 1 routeur (Cisco 4221 avec la version 16.9.3 de Cisco IOS XE universelle ou similaire).
- 2 commutateurs (Cisco 2960 avec la version 15.0(2) de Cisco IOS image lanbasek9 ou similaire).
- 2 PC (Windows équipé d'un programme d'émulation de terminal tel que Tera Term).
- Câbles de console pour configurer les appareils Cisco IOS via les ports de console.
- Câbles Ethernet comme la topologie indique.

### Instructions

#### Partie 1: Configurer les périphériques réseau.

##### Étape 1: Câblage du réseau

- a. Connectez le réseau conformément à ce qui est indiqué dans la topologie.
- b. Initialisez les périphériques

##### Étape 2: Configurer R1.

- a. Chargez le script de configuration suivant sur R1.

```
Enable
configure terminal
hostname R1
no ip domain lookup
ip dhcp excluded-address 192.168.10.1 192.168.10.9
ip dhcp excluded-address 192.168.10.201 192.168.10.202
!
ip dhcp pool Students
    network 192.168.10.0 255.255.255.0
    default-router 192.168.10.1
    domain-name CCNA2.Lab-11.6.1
!
interface Loopback0
    ip address 10.10.1.1 255.255.255.0
!
interface GigabitEthernet0/0/1
    Description de Liaison porte 5 à S1
    ip dhcp relay information trusted
    ip address 192.168.10.1 255.255.255.0
    no shutdown
!
line con 0
    logging synchronous
    exec-timeout 0 0
```

- b. Vérifiez la configuration d'exécution sur R1 à l'aide de la commande suivante:

```
R1# show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 unassigned YES unset down down
GigabitEthernet0/0/1 192.168.10.1 YES manual up up
Loopback0 10.10.1.1 YES manual up up
```

- c. Vérifiez que l'adressage IP et les interfaces sont dans l'état up/ up (dépannez si nécessaire).

### Étape 3: Configurer et vérifier les paramètres de base du commutateur.

- a. Configurez le nom d'hôte pour les commutateurs S1 et S2.

```
Switch# config t
Switch(config)# hostname S1
```

```
Switch# config t
Switch(config)# hostname S2
```

- b. Empêchez les recherches DNS indésirables sur les deux commutateurs

```
S1(config)# no ip domain-lookup
S2(config)# no ip domain-lookup
```

- c. Configurez les descriptions d'interface des ports utilisés sur S1 et S2.

```
S1(config)# interface f0/1
S1(config-if)# description Link to S2
S1(config-if)# interface f0/5
S1(config-if)# description Link to R1
S1(config-if)# interface f0/6
S1(config-if)# description Link to PC-A
```

```
S2(config)# interface f0/1
S2(config-if)# description Link to S1
S2(config-if)# interface f0/18
S2(config-if)# description Link to PC-B
```

- d. Déterminez la passerelle par défaut pour le VLAN de gestion d'être 192.168.10.1 sur les deux commutateurs.

```
S1(config)# ip default-gateway 192.168.10.1
S2(config)# ip default-gateway 192.168.10.1
```

## Partie 2: Configurer les VLAN sur les commutateurs.

### Étape 1: Configurer VLAN 10.

Ajoutez VLAN 10 à S1 et S2 et nommez le VLAN **Management**.

```
S1(config)# vlan 10
S1(config-vlan)# name Management
```

```
S2(config)# vlan 10
S2(config-vlan)# name Management
```

### Étape 2: Configurer le SVI pour VLAN 10.

Configurez l'adresse IP selon la table d'adressage de SVI pour VLAN 10 sur S1 et S2. Activez les interfaces SVI et fournissez une description de l'interface.

```
S1(config)# interface vlan 10
S1(config-if)# ip address 192.168.10.201 255.255.255.0
S1(config-if)# description Management SVI
S1(config-if)# no shutdown
```

```
S2(config)# interface vlan 10
S2(config-if)# ip address 192.168.10.202 255.255.255.0
S2(config-if)# description Management SVI
S2(config-if)# no shutdown
```

### Étape 3: Configurer VLAN 333 avec le nom natif sur S1 et S2.

```
S2(config)# vlan 333
S1(config-vlan)# name Native
```

```
S2(config)# vlan 333
S2(config-vlan)# name Native
```

### Étape 4: Configurer VLAN 999 avec le nom ParkingLot sur S1 et S2.

```
S1(config-vlan)# vlan 999
S1(config-vlan)# name ParkingLot
```

```
S2(config-vlan)# vlan 999
S2(config-vlan)# name ParkingLot
```

## Partie 3: Configurer la Sécurité du Commutateur.

### Étape 1: Mettre en œuvre le trunc 802.1Q

- Sur les deux commutateurs, configurez le trunc sur F0/1 pour utiliser le VLAN 333 comme VLAN natif.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 333
```

```
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk native vlan 333
```

- Vérifiez que le trunc est configuré sur les deux commutateurs.

```
S1# show interface trunk
```

```
Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q trunking 333
```

```
Port Vlans allowed on trunk
Fa0/1 1-4094
```

```
Port Vlans allowed and active in management domain
Fa0/1 1,10,333,999
```

```
Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,333,999
```

```
S2# show interface trunk
```

```
Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q trunking 333
```

```
Port Vlans allowed on trunk
Fa0/1 1-4094
```

```
Port Vlans allowed and active in management domain
Fa0/1 1,10,333,999
```

```
Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,333,999
```

- c. Désactivez la négociation DTP sur F0/1 sur S1 et S2.

```
S1(config)# interface f0/1
S1(config-if)# switchport nonegotiate
```

```
S2(config)# interface f0/1
S2(config-if)# switchport nonegotiate
```

- d. Vérifiez en utilisant la commande **show interfaces** .

```
S2# show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
```

```
S2# show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
```

### Étape 2: Configurer les ports d'accès

- a. Sur S1, configurez F0/5 et F0/6 comme des ports d'accès associés au VLAN 10.

```
S1(config)# interface range f0/5 - 6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
```

- b. Sur S2, configurez F0/18 comme un port d'accès associé au VLAN 10.

```
S2(config)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 10
```

### Étape 3: Sécuriser et désactiver les ports de commutateurs inutilisés.

- a. Sur S1 et S2, déplacez les ports inutilisés de VLAN 1 à VLAN 999 et désactivez les ports inutilisés.

```
S1(config)# interface range f0/2-4 , f0/7-24, g0/1-2
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
S1(config-if-range)# shutdown
```

```
S2(config)# interface range f0/2-17 , f0/19-24, g0/1-2
S2(config-if-range)# switchport mode access
```

```
S2(config-if-range)# switchport access vlan 999
```

```
S2(config-if-range)# shutdown
```

- b. Vérifiez que les ports inutilisés sont désactivés et associés au VLAN 999 en exécutant la commande **show**.

```
S1# show interfaces status
```

```
Port Name Status Vlan Duplex Speed Type
Fa0/1 Link to S2 connected trunk a-full a-100 10/100BaseTX
Fa0/2 disabled 999 auto auto 10/100BaseTX
Fa0/3 disabled 999 auto auto 10/100BaseTX
Fa0/4 disabled 999 auto auto 10/100BaseTX
Fa0/5 Link to R1 connected 10 a-full a-100 10/100BaseTX
Fa0/6 Link to PC-A connected 10 a-full a-100 10/100BaseTX
Fa0/7 disabled 999 auto auto 10/100BaseTX
Fa0/8 disabled 999 auto auto 10/100BaseTX
Fa0/9 disabled 999 auto auto 10/100BaseTX
Fa0/10 disabled 999 auto auto 10/100BaseTX
<output omitted>
```

```
S2# show interfaces status
```

```
Port Name Status Vlan Duplex Speed Type
Fa0/1 Link to S1 connected trunk a-full a-100 10/100BaseTX
Fa0/2 disabled 999 auto auto 10/100BaseTX
Fa0/3 disabled 999 auto auto 10/100BaseTX
<output omitted>
Fa0/14 disabled 999 auto auto 10/100BaseTX
Fa0/15 disabled 999 auto auto 10/100BaseTX
Fa0/16 disabled 999 auto auto 10/100BaseTX
Fa0/17 disabled 999 auto auto 10/100BaseTX
Fa0/18 Link to PC-B connected 10 a-full a-100 10/100BaseTX
Fa0/19 disabled 999 auto auto 10/100BaseTX
Fa0/20 disabled 999 auto auto 10/100BaseTX
Fa0/21 disabled 999 auto auto 10/100BaseTX
Fa0/22 disabled 999 auto auto 10/100BaseTX
Fa0/23 disabled 999 auto auto 10/100BaseTX
Fa0/24 disabled 999 auto auto 10/100BaseTX
Gi0/1 disabled 999 auto auto 10/100/1000BaseTX
Gi0/2 disabled 999 auto auto 10/100/1000BaseTX
```

### Étape 4: Documenter et mettre en œuvre les fonctions de sécurité des ports.

Les interfaces F0/6 sur S1 et F0/18 sur S2 sont configurées comme ports d'accès. Dans cette étape, vous allez aussi configurer la sécurité des ports sur ces deux ports d'accès.

- a. Sur S1, exécutez la commande **show port-security interface f0/6** pour afficher les paramètres de sécurité de port par défaut de l'interface F0/6. Notez vos réponses dans le tableau ci-dessous.

```
S1# show port-security interface f0/6
```

```
Port Security : Disabled
```

```
Port Status : Secure-down
```

```

Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 0
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0

```

Configuration de la sécurité des ports par défaut	
Caractéristique	Paramètre par défaut
Sécurité des ports	Désactivé
Nombre maximal des adresses MAC	1
Mode de violation	Arrêter
Délai d'expiration	0 mins
Type d'obsolescence	Absolu
Obsolescence d'adresse statique sécurisé	Désactivé
Adresses MAC rémanentes	0

b. Sur S1, activez la sécurité des ports sur F0/6 avec les paramètres suivants:

- Nombre maximal d'entrées d'adresse : 3
- Mode de violation : **Restrict**
- Temps d'obsolescence : **60 min**
- Type d'obsolescence : **Inactivité**

```

S1(config)# interface f0/6
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 3
S1(config-if)# switchport port-security violation restrict
S1(config-if)# switchport port-security aging time 60
S1(config-if)# switchport port-security aging type inactivity

```

c. Vérifiez la sécurité de port sur S1 F0/6

```

S1# show port-security interface f0/6
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Restrict
Aging Time : 60 mins
Aging Type : Inactivity
SecureStatic Address Aging : Disabled

```



```
Adresses MAC maximales (Maximum MAC Adresses) : 3
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0022.5646.3411:10
Security Violation Count : 0
```

```
S1# show port-security address
```

```
Secure Mac Address Table
```

```
-----
Vlan Mac Address Type Ports Remaining Age
                                           (mins)
-----
 10 0022.5646.3411 SecureDynamic Fa0/6 60 (I)
-----
```

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

- d. Activez la sécurité des ports pour F0/18 sur S2. Configurez le port pour ajouter automatiquement les adresses MAC apprennent sur le port à la configuration courante.

```
S2(config)# interface f0/18
```

```
S2(config-if)# switchport port-security
```

```
S2(config-if)# switchport port-security mac-address sticky
```

- e. Configurez les paramètres de sécurité de port suivant sur S2 F/18:

- o Nombre maximal d'entrées d'adresse: **2**
- o Mode de Violation : **Protect**
- o Temps d'obsolescence : **60 min**

```
S2(config)# interface f0/18
```

```
S2(config-if)# switchport port-security aging time 60
```

```
S2(config-if)# switchport port-security maximum 2
```

```
S2(config-if)# switchport port-security violation protect
```

- f. Vérifiez la sécurité de port sur S2 F0/18

```
S2# show port-security interface f0/18
```

```
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Protect
Aging Time : 60 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Adresses MAC maximales (Maximum MAC Adresses) : 2
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0022.5646.3413:10
Security Violation Count : 0
```

```
S2# show port-security address
```

```
Secure Mac Address Table
-----
Vlan Mac Address Type Ports Remaining Age
                                           (mins)
-----
 10 0022.5646.3413 SecureSticky Fa0/18 -
-----
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

### Étape 5: Mettre en œuvre la sécurité d'espionnage DHCP.

- a. Sur S2, activez et configurez l'espionnage DHCP sur le VLAN 10.

```
S2(config)# ip dhcp snooping
S2(config)# ip dhcp snooping vlan 10
```

- b. Configurez le port trunc sur S2 comme un port approuvé.

```
S2(config)# interface f0/1
S2(config-if)# ip dhcp snooping trust
```

- c. Limitez les ports non approuvés, F18 sur S2 à cinq paquets DHCP par seconde.

```
S2(config)# interface f0/18
S2(config-if)# ip dhcp snooping limit rate 5
```

- d. Vérifiez l'espionnage DHCP sur S2.

```
S2# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
DHCP snooping is operational on following VLANs:
10
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: 0cd9.96d2.3f80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface Trusted Allow option Rate limit (pps)
-----
FastEthernet0/1 yes yes unlimited
  Custom circuit-ids:
FastEthernet0/18 no no 5
  Custom circuit-ids:
```

- e. À partir de l'invite de commande sur PC-B, libérez puis renouvelez l'adresse IP.

```
C:\Users\Student> ipconfig /release
C:\Users\Student> ipconfig /renew
```

- f. Vérifiez la liaison de l'espionnage DHCP en utilisant la commande **show ip dhcp snooping binding** .

```
S2# show ip dhcp snooping
```

```
MacAddress IpAddress Lease(sec) Type VLAN Interface
```

```
-----
```

```
00:50:56:90:D0:8E 192.168.10.11 86213 dhcp-snooping 10 FastEthernet0/18
```

```
Total number of bindings: 1
```

### Étape 6: Mettre en œuvre PortFast et la protection BPDU

- a. Configurez PortFast sur tous les ports d'accès qui sont utilisés sur les deux commutateurs.

```
S1(config)# interface range f0/5 - 6
```

```
S1(config-if)# spanning-tree portfast
```

```
S2(config)# interface f0/18
```

```
S2(config-if)# spanning-tree portfast
```

- b. Activez la protection BPDU sur les ports d'accès S1 et S2 VLAN 10 connectés aux PC-A et PC-B.

```
S1(config)# interface f0/6
```

```
S1(config-if)# spanning-tree bpduguard enable
```

```
S2(config)# interface f0/18
```

```
S2(config-if)# spanning-tree bpduguard enable
```

- c. Vérifiez que la protection BPDU et PortFast sont activés sur les ports appropriés.

```
S1# show spanning-tree interface f0/6 detail
```

```
Port 8 (FastEthernet0/6) of VLAN0010 is designated forwarding
```

```
Port path cost 19, Port priority 128, Port Identifier 128.6.
```

```
<output omitted for brevity>
```

```
Number of transitions to forwarding state: 1
```

```
The port is in the portfast mode
```

```
Link type is point-to-point by default
```

```
Bpdu guard is enabled
```

```
BPDU: sent 128, received 0
```

### Étape 7: Vérifier la connectivité de bout en bout.

Vérifiez la connectivité PING entre tous les périphériques de la table d'adressage IP. Si les pings échouent, vous devrez peut-être désactiver le pare-feu sur les hôtes PC.

### Questions de réflexion

1. En référence à la sécurité des ports sur S2, pourquoi n'y a-t-il pas une valeur de minuterie pour l'obsolescence restant en minutes lorsque l'apprentissage rémanente a été configurée?

**Ce commutateur ne prend pas en charge l'obsolescence de la sécurité des ports des adresses sécurisées rémanentes.**

2. En référence à la sécurité des ports sur S2, si vous chargez le script running-config sur S2, pourquoi PC-B sur le port 18 n'obtiendra-t-il jamais d'adresse IP via DHCP?

**La sécurité des ports est déterminée pour seulement deux adresses MAC et le port 18 a deux adresses MAC «rémanentes» liées au port. En addition, la violation est protégée, qui n'enverra jamais de message console / syslog ni incrémentera le compteur de violation.**

3. En ce qui concerne la sécurité des ports, quelle est la différence entre le type d'obsolescence absolu et le type d'obsolescence inactif ?

**Si le type d'inactivité est déterminé, alors les adresses sécurisées sur le port seront supprimées uniquement s'il n'y a pas de trafic de données provenant des adresses source sécurisées pendant la période du temps spécifiée.**

**Si le type absolu est déterminé, toutes les adresses sécurisées sur ce port expirent exactement après la fin de la durée spécifiée.**

## Configurations des périphériques (finales)

### Commutateur S1

```
S1# show running-config
Building configuration...

Current configuration: 5203 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
no ip domain-lookup
!
spanning-tree mode pvst
!
vlan 10
  name Management
!
vlan 333
  name Native
!
vlan 999
  name ParkingLot
!
interface FastEthernet0/1
  La Description de Liaison à S2
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 333
```

## Travaux pratiques - Configuration de la sécurité du commutateur

---

```
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/2
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/3
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/4
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/5
La Description de Liaison à R1
switchport access vlan 10
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/6
La Description de Liaison à PC-A
switchport access vlan 10
switchport mode access
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security aging time 60
switchport port-security aging type inactivity
switchport port-security
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/7
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/8
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/9
switchport access vlan 999
switchport mode access
```

## Travaux pratiques - Configuration de la sécurité du commutateur

---

```
shutdown
!
interface FastEthernet0/10
  switchport access vlan 999
  switchport mode accessSEP
  shutdown
!
interface FastEthernet0/11
  switchport access vlan 999
  switchport mode accessSEP
  shutdown
!
interface FastEthernet0/12
  switchport access vlan 999
  switchport mode accessSEP
  shutdown
!
interface FastEthernet0/13
  switchport access vlan 999
  switchport mode accessSEP
  shutdown
!
interface FastEthernet0/14
  switchport access vlan 999
  switchport mode accessSEP
  shutdown
!
interface FastEthernet0/15
  switchport access vlan 999
  switchport mode accessSEP
  shutdown
!
interface FastEthernet0/16
  switchport access vlan 999
  switchport mode accessSEP
  shutdown
!
interface FastEthernet0/17
  switchport access vlan 999
  switchport mode accessSEP
  shutdown
!
interface FastEthernet0/18
  switchport access vlan 999
  switchport mode accessSEP
  shutdown
!
interface FastEthernet0/19
```

```
switchport access vlan 999
switchport mode accessSEP
shutdown
!
interface FastEthernet0/20
switchport access vlan 999
switchport mode accessSEP
shutdown
!
interface FastEthernet0/21
switchport access vlan 999
switchport mode accessSEP
shutdown
!
interface FastEthernet0/22
switchport access vlan 999
switchport mode accessSEP
shutdown
!
interface FastEthernet0/23
switchport access vlan 999
switchport mode accessSEP
shutdown
!
interface FastEthernet0/24
switchport access vlan 999
switchport mode accessSEP
shutdown
!
interface GigabitEthernet0/1
switchport access vlan 999
switchport mode accessSEP
shutdown
!
interface GigabitEthernet0/2
switchport access vlan 999
switchport mode accessSEP
shutdown
!
interface Vlan1
no ip address
!
interface Vlan10
description de gestion SVI
ip address 192.168.10.201 255.255.255.0
!
ip default-gateway 192.168.10.1
```

```
line con 0
  exec-timeout 0 0
  logging synchronous
line vty 0 4
  login
line vty 5 15
  login
!
end
```

### Commutateur S2

```
S2# show running-config
Building configuration...

Current configuration : 5303 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S2
!
ip dhcp snooping vlan 10
ip dhcp snooping
no ip domain-lookup
!
spanning-tree mode pvst
!
vlan 10
  name Students
!
vlan 333
  name Native
!
vlan 999
  name ParkingLot
!
interface FastEthernet0/1
  La Description de Liaison à S1
  switchport trunk native vlan 333
  switchport mode trunk
  switchport nonegotiate
  ip dhcp snooping trust
!
interface FastEthernet0/2
  switchport access vlan 999
  switchport mode access
```



## Travaux pratiques - Configuration de la sécurité du commutateur

---

```
shutdown
!
interface FastEthernet0/3
 switchport access vlan 999
 switchport mode accessSEP
 shutdown
!
interface FastEthernet0/4
 switchport access vlan 999
 switchport mode accessSEP
 shutdown
!
interface FastEthernet0/5
 switchport access vlan 999
 switchport mode accessSEP
 shutdown
!
interface FastEthernet0/6
 switchport access vlan 999
 switchport mode accessSEP
 shutdown
!
interface FastEthernet0/7
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/8
 switchport access vlan 999
 switchport mode accessSEP
 shutdown
!
interface FastEthernet0/9
 switchport access vlan 999
 switchport mode accessSEP
 shutdown
!
interface FastEthernet0/10
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/11
 switchport access vlan 999
 switchport mode accessSEP
 shutdown
!
interface FastEthernet0/12
 switchport access vlan 999
```

## Travaux pratiques - Configuration de la sécurité du commutateur

---

```
switchport mode access
shutdown
!
interface FastEthernet0/13
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/14
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/15
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/16
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/17
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/18
La Description de Liaison à PC-B
switchport access vlan 10
switchport mode access
switchport port-security maximum 2
switchport port-security violation protect
switchport port-security mac-address sticky
switchport port-security aging time 60
switchport port-security
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 5
!
interface FastEthernet0/19
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/20
switchport access vlan 999
switchport mode access
```

## Travaux pratiques - Configuration de la sécurité du commutateur

---

```
shutdown
!
interface FastEthernet0/21
 switchport access vlan 999
 switchport mode accessSEP
 shutdown
!
interface FastEthernet0/22
 switchport access vlan 999
 switchport mode accessSEP
 shutdown
!
interface FastEthernet0/23
 switchport access vlan 999
 switchport mode accessSEP
 shutdown
!
interface FastEthernet0/24
 switchport access vlan 999
 switchport mode accessSEP
 shutdown
!
interface GigabitEthernet0/1
 switchport access vlan 999
 switchport mode accessSEP
 shutdown
!
interface GigabitEthernet0/2
 switchport access vlan 999
 switchport mode accessSEP
 shutdown
!
interface Vlan1
 no ip address
!
interface Vlan10
 description de gestion SVI
 ip address 192.168.10.202 255.255.255.0
!
ip default-gateway 192.168.10.1
!
line con 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
 login
line vty 5 15
 login
!
```

end