Travaux pratiques : implémentation de la sécurité VLAN

TP13

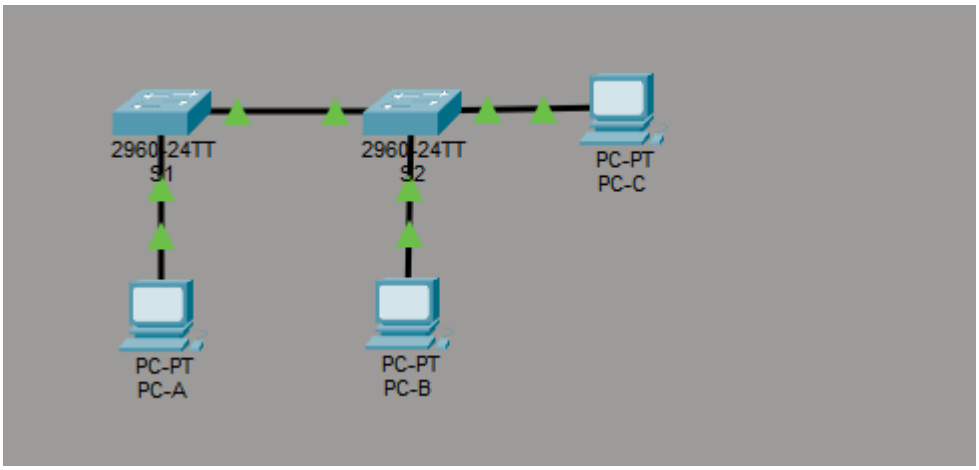
Sgolmin Raphael

Table des matières

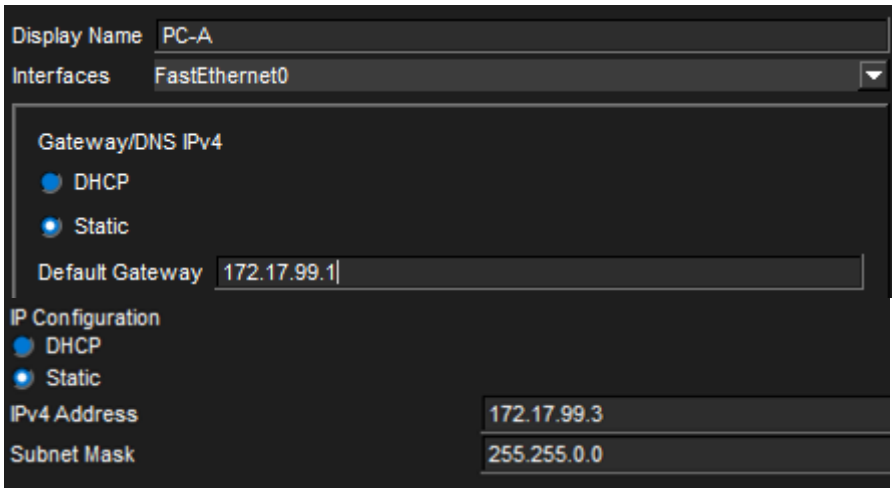
Partie 1 : Création du réseau et configuration des paramètres de base du périphérique 3
Étape 1 : Câblez le réseau conformément à la topologie. 3
Étape 3 : Configurez les adresses IP sur PC-A, PC-B et PC-C. 3
Étape 4 : Configurez les paramètres de base pour chaque commutateur 5
Configuration réalisée sur S1 et S2 Étape 5 : Configurez des VLAN sur chaque commutateur. ... 5
Étape 6 : Configurez la sécurité de base du commutateur 7
Partie 2 : Implémentation de la sécurité VLAN sur les commutateurs 7
Étape 1 : Configurez les ports trunk sur S1 et S2. 7
Étape 2 : Modifiez le VLAN natif pour les ports trunk de S1 et S2. 8
Étape 4 : Empêchez l'utilisation du protocole DTP sur S1 et S2. 9
Étape 5 : Sécurisez les ports d'accès sur S1 et S2. 10

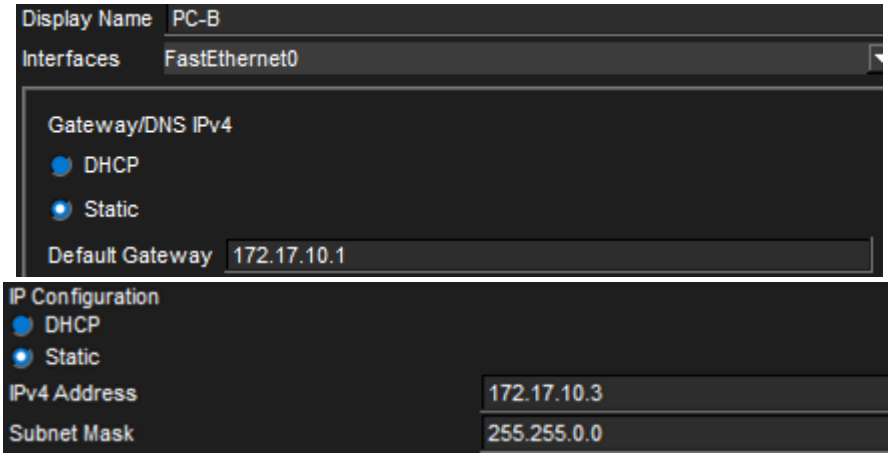
Partie 1 : Création du réseau et configuration des paramètres de base du périphérique

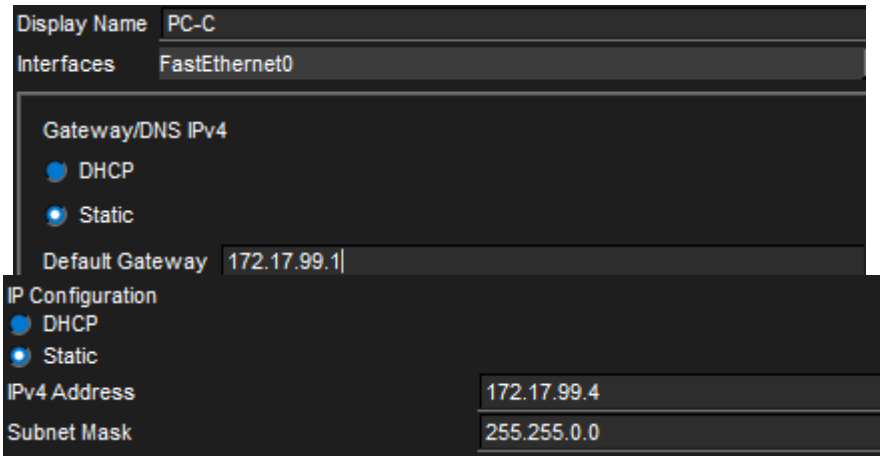
Étape 1 : Câblez le réseau conformément à la topologie.



Étape 3 : Configurez les adresses IP sur PC-A, PC-B et PC-C.




Display Name
PC-B
Interfaces
FastEthernet0
Gateway/DNS IPv4
DHCP
Static
Default Gateway
172.17.10.1
IP Configuration
DHCP
Static
IPv4 Address
172.17.10.3
Subnet Mask
255.255.0.0


Display Name
PC-C
Interfaces
FastEthernet0
Gateway/DNS IPv4
DHCP
Static
Default Gateway
172.17.99.1
IP Configuration
DHCP
Static
IPv4 Address
172.17.99.4
Subnet Mask
255.255.0.0

Étape 4 : Configurez les paramètres de base pour chaque commutateur

Configuration réalisée sur S1 et S2

```
S1(config)#no ip domain-lookup
S1(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#logging synchronous
S1(config-line)#exit
S1(config)#
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#logging synchronous
S1(config-line)#exit
```

```
S2(config)#no ip domain-lookup
S2(config)#hostname S2
S2(config)#enable secret class
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#logging synchronous
S2(config-line)#exit
S2(config)#
S2(config)#line vty 0 15
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#logging synchronous
S2(config-line)#exit
```

Étape 5 : Configurez des VLAN sur chaque commutateur.

```
S1(config)#vlan 10
S1(config-vlan)#name Data
S1(config-vlan)#exit
S1(config)#
S1(config)#vlan 99
S1(config-vlan)#name Management&Native
S1(config-vlan)#exit
S1(config)#
S1(config)#vlan 999
S1(config-vlan)#name BlackHole
S1(config-vlan)#exit
```

```
S2(config)#vlan 10
S2(config-vlan)#name Data
S2(config-vlan)#exit
S2(config)#
S2(config)#vlan 99
S2(config-vlan)#name Management&Native
S2(config-vlan)#exit
S2(config)#
S2(config)#vlan 999
S2(config-vlan)#name BlackHole
S2(config-vlan)#exit
```

```
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Vlan99, changed state to up

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

```
S2(config)#interface vlan 99
S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S2(config-if)#no shutdown
```

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

```
S2(config)#interface f0/11
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#ex
S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 99
S2(config-if)#
```

J’ai créé les VLAN suivants sur les deux commutateurs :

- VLAN 10 : Data

- VLAN 99 : Management & Native

- VLAN 999 : BlackHole

Puis j’ai configuré l’interface VLAN 99 pour la gestion :

- S1 : 172.17.99.11

- S2 : 172.17.99.12

J’ai vérifié avec show interface trunk :

```
S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
10   Data                             active
99   Management&Native                active    Fa0/6
999  BlackHole                        active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S1#
```

```
S2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   Data                             active    Fa0/11
99   Management&Native                active    Fa0/18
999  BlackHole                        active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S2#
```

J’ai observé que les ports non configurés appartiennent par défaut au VLAN 1.

Étape 6 : Configurez la sécurité de base du commutateur

```
S1(config)#banner motd # Accs non autoris interdit #
S1(config)#service password-encryption
S1(config)#interface range f0/2-5
S1(config-if-range)#shutdown
```

Partie 2 : Implémentation de la sécurité VLAN sur les commutateurs

Étape 1 : Configurez les ports trunk sur S1 et S2.

J'ai configuré le port F0/1 des deux commutateurs en mode trunk afin de permettre le passage de plusieurs VLAN entre S1 et S2.

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

S1(config-if)#
```

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

```
S1#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99,999
```

```
S2#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99,999
```

Après vérification, le trunk était actif avec le VLAN natif par défaut (VLAN 1).

Étape 2 : Modifiez le VLAN natif pour les ports trunk de S1 et S2.

Pour améliorer la sécurité, j'ai modifié le VLAN natif en VLAN 99.
Un message CDP indiquait un mismatch temporaire jusqu'à ce que la configuration soit identique sur les deux commutateurs.

```
S1(config)#interface f0/1
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#
```

```
S2(config)#interface f0/1
S2(config-if)#switchport trunk native vlan 99
S2(config-if)#%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0099.
Port consistency restored.
```

```
S1# show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99,999
```

```
S2#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99,999
```

Étape 4 : Empêchez l'utilisation du protocole DTP sur S1 et S2.

J’ai désactivé la négociation automatique du trunking (DTP) sur S1 et S2 afin d’éviter la création automatique de trunks non souhaités.

```
S1# show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
```

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

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

```
S1#show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
```

```
S2#show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
```

Étape 5 : Sécurisez les ports d'accès sur S1 et S2.

```
S1# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
```

Les ports inutilisés de S1 et S2 ont été configurés en mode access et placés dans le VLAN 999 (BlackHole

```
S1(config)#interface range f0/2-5
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 999
S1(config-if-range)#
```

```
S2(config)#interface range f0/2-5
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 999
S2(config-if-range)#
```

```
S1#show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
```

```
S1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   Data                              active
99   Management&Native                 active    Fa0/6
999  BlackHole                         active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S1#
```

Cela empêche toute connexion non autorisée.

J’ai limité les VLAN autorisés sur S1 et S2 sur la liaison trunk aux VLAN 10 et 99 uniquement afin d’améliorer la sécurité du réseau.

```
S1(config)#interface f0/1
S1(config-if)#switchport trunk allowed vlan 10,99
S1(config-if)#
```

```
S2(config)#interface f0/1
S2(config-if)#switchport trunk allowed vlan 10,99
S2(config-if)#
```

La commande **show interface trunk** confirme que seuls ces VLAN sont autorisés.

```
S1#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,99

Port        Vlans allowed and active in management domain
Fa0/1       10,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,99
```