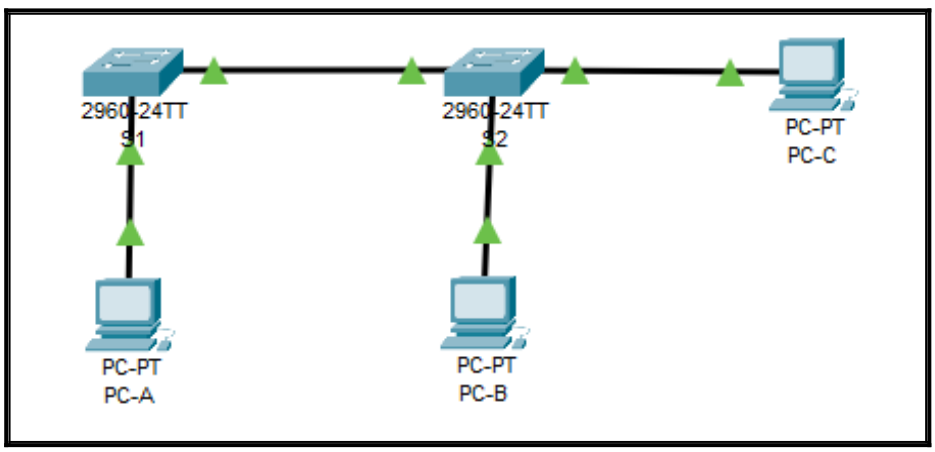
Travaux pratiques : implémentation de la sécurité VLAN (3.3.2.2)

Sommaire :

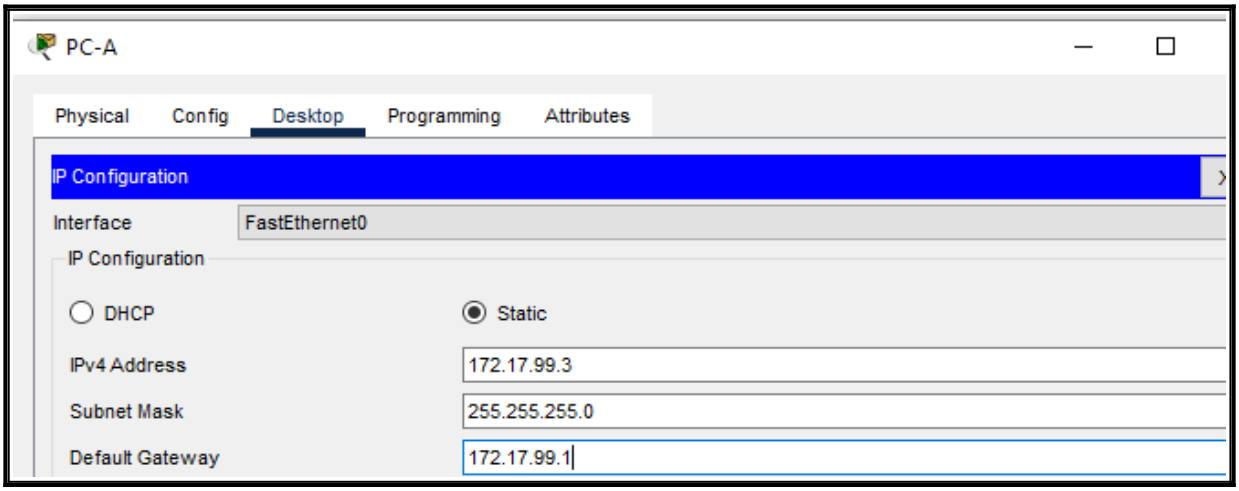
Partie 1 : Création du réseau et configuration des paramètres de base du périphérique :

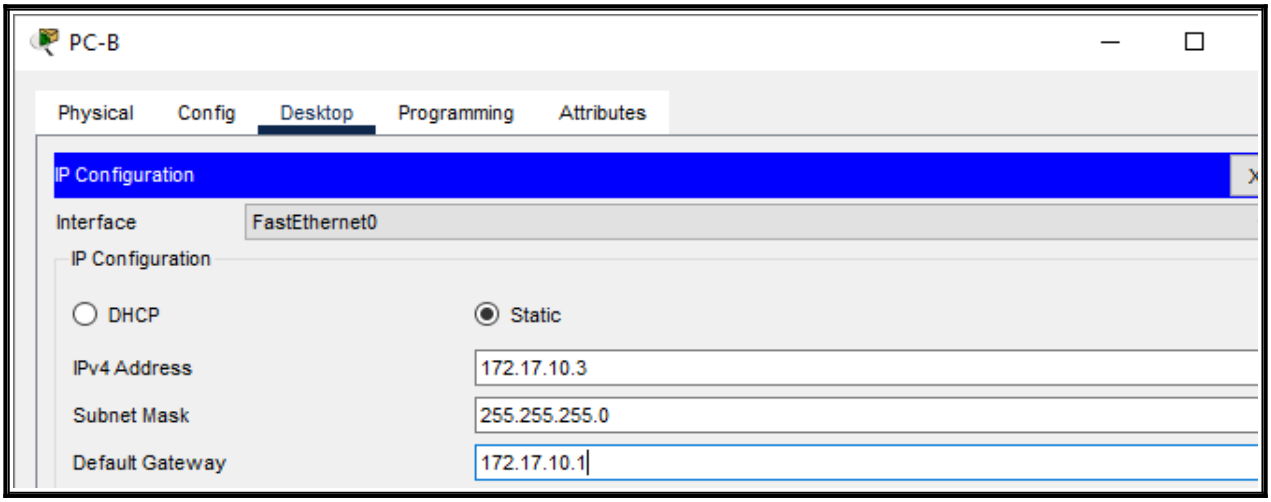
Étape 1 : Câblez le réseau conformément à la topologie.

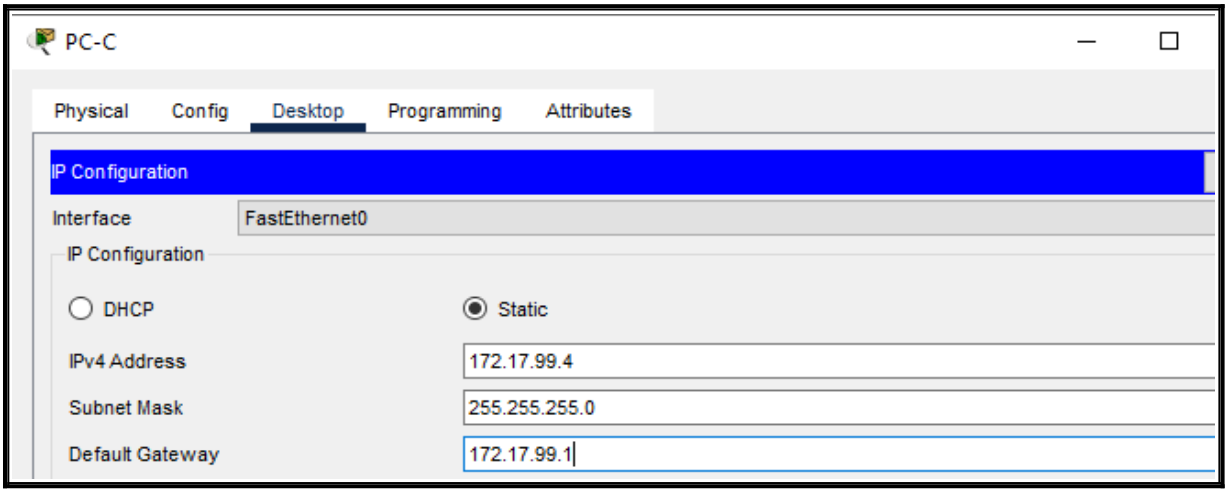


1ère étape : Nous câblons le réseau conformément à la topologie demandé.

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







1ère étape : Nous configurons les interfaces hôtes des pc avec leur **adresses IP**, pour **PC-A**, **PC-B** puis **PC-C**.

Étape 4 : Configurez les paramètres de base pour chaque commutateur.

```
S1#sh run
Building configuration...

Current configuration : 1219 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
no ip domain-lookup
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
```

```
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
 password cisco
 logging synchronous
!
line vty 0 4
 password cisco
 logging synchronous
 login
line vty 5 15
 login
!
!
!
!
end
```

S1

```
S2#sh run
Building configuration...

Current configuration : 1219 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S2
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
no ip domain-lookup
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
```

```
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
 password cisco
 logging synchronous
!
line vty 0 4
 password cisco
 logging synchronous
 login
line vty 5 15
 login
!
!
!
!
end
```

S2

1ère étape : Nous **configurons** les deux **Switchs** (Commutateurs) présent dans la topologie.

Étape 5 : Configurez des VLAN sur chaque commutateur.

```
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   Donnees                          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
```

```
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   Donnees                          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
```

1ère étape : Cette commande permet d'obtenir un aperçu des **Vlan** après les avoir créer mais aussi configurer en attribuant les **interfaces** à leur Vlan correspondant.

Étape 6 : Configurez la sécurité de base du commutateur.

S1

```
interface FastEthernet0/1
!
interface FastEthernet0/2
 shutdown
!
interface FastEthernet0/3
 shutdown
!
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 switchport access vlan 99
 switchport mode access
!
interface FastEthernet0/7
 shutdown
!
interface FastEthernet0/8
 shutdown
!
interface FastEthernet0/9
 shutdown
!
interface FastEthernet0/10
 shutdown
!
interface FastEthernet0/11
!
interface FastEthernet0/12
 shutdown
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
```

```
!
interface FastEthernet0/1
!
interface FastEthernet0/2
 shutdown
!
interface FastEthernet0/3
 shutdown
!
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
!
interface FastEthernet0/7
 shutdown
!
interface FastEthernet0/8
 shutdown
!
interface FastEthernet0/9
 shutdown
!
interface FastEthernet0/10
 shutdown
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/12
 shutdown
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 switchport access vlan 99
 switchport mode access
!
```

S2

1ère étape : Nous désactivons tous les ports physiques non utilisés.

Étape 7 : Vérifiez la connectivité entre les périphériques ainsi que les informations VLAN.

```
C:\>ping 172.17.99.11

Pinging 172.17.99.11 with 32 bytes of data:

Reply from 172.17.99.11: bytes=32 time<1ms TTL=255
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255

Ping statistics for 172.17.99.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

1ère étape : Test de ping depuis PC-A vers l'adresse de gestion de S1.

```
C:\>ping 172.17.99.3

Pinging 172.17.99.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.17.99.3:
    Packets: Sent = 4, Received = 0, Lost =
```

PC-A

```
C:\>ping 172.17.99.11

Pinging 172.17.99.11 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.17.99.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

S1

```
C:\>ping 172.17.99.4

Pinging 172.17.99.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.17.99.4:
    Packets: Sent = 4, Received = 0, Lost =
```

PC-C

```
C:\>ping 172.17.99.12

Pinging 172.17.99.12 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.17.99.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

S2

2ème étape : Depuis PC-B nous effectuons un ping vers PC-A, PC-C, S1 et S2. Ils ne fonctionnent pas puisque les machines ne sont pas dans le même vlan.

```
S1#ping 172.17.99.12

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.12, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

3ème étape : Test de ping depuis S1 vers S2, celui-ci ne fonctionne pas.

Partie 2 : Implémentation de la sécurité VLAN sur les commutateurs :

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

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

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

1ère étape: Nous configurons les **interfaces** en tant que port **trunk**.

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

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

```
S2(config)#int f0/1
S2(config-if)#switchport trunk native vlan 99
```

1ère étape : Nous configurons le **vlan natif 99 sur l'interface trunk**.

```
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
```

2ème étape : Nous vérifions par la suite que les modifications sont correctes.

Étape 3 : Vérifiez que le trafic peut correctement traverser la liaison trunk.

PC-A vers S1

```
C:\>ping 172.17.99.11

Pinging 172.17.99.11 with 32 bytes of data:

Reply from 172.17.99.11: bytes=32 time<1ms TTL=255
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255

Ping statistics for 172.17.99.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

S1 vers S2

```
S1#ping 172.17.99.12

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.12, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

PC-B vers PC-A

```
C:\>ping 172.17.99.3

Pinging 172.17.99.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.17.99.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC-B vers PC-C

```
C:\>ping 172.17.99.4

Pinging 172.17.99.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.17.99.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC-B vers S1

```
C:\>ping 172.17.99.11

Pinging 172.17.99.11 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.17.99.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC-B vers S2

```
C:\>ping 172.17.99.12

Pinging 172.17.99.12 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.17.99.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC-C vers PC-A

```
C:\>ping 172.17.99.3

Pinging 172.17.99.3 with 32 bytes of data:

Reply from 172.17.99.3: bytes=32 time<1ms TTL=128
Reply from 172.17.99.3: bytes=32 time<1ms TTL=128
Reply from 172.17.99.3: bytes=32 time<1ms TTL=128
Reply from 172.17.99.3: bytes=32 time<1ms TTL=128

Ping statistics for 172.17.99.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

PC-C vers S1

```
C:\>ping 172.17.99.11

Pinging 172.17.99.11 with 32 bytes of data:

Reply from 172.17.99.11: bytes=32 time<1ms TTL=255
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255

Ping statistics for 172.17.99.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

PC-C vers S2

```
C:\>ping 172.17.99.12

Pinging 172.17.99.12 with 32 bytes of data:

Reply from 172.17.99.12: bytes=32 time<1ms TTL=255
Reply from 172.17.99.12: bytes=32 time<1ms TTL=255
Reply from 172.17.99.12: bytes=32 time<1ms TTL=255
Reply from 172.17.99.12: bytes=32 time<1ms TTL=255

Ping statistics for 172.17.99.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

1ère étape : Nous effectuons une liste de différentes requêtes de ping afin de vérifier que seul PC-B ne peut pas communiqué avec le reste de la topologie.

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

```
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
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (Management&Native)
Voice VLAN: none
```

1ère étape : Nous observons que la **négociation est activée**.

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

```
S2(config)#int F0/1
S2(config-if)#switchport nonegotiate
```

2ème étape : Depuis les deux switch nous désactivons la négiciation sur l'interface f0/1.

```
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
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (Management&Native)
Voice VLAN: none
```

```
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
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (Management&Native)
Voice VLAN: none
```

3ème étape : Nous vérifions de nouveau que la **négociation à été désactivée**.

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
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

1ère étape : Nous observons le **mode d'administration** et l'**état de la négociation de trunking de l'interface f0/2**.

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

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

2ème étape : Depuis les deux switch nous désactivons le **trunking** sur les ports d'accès **f0/2**.

```
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
Access Mode VLAN: 999 (BlackHole)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

3ème étape : Nous de nouveau le **mode administration** et la **négociation trunk**.

```
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   Donnees                           active
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
```

4ème étape : Nous vérifions que les **attributions des ports VLAN** sont correctes.

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

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

5ème étape : Nous configurons l'interface **f0/1** sur le switch S1 et S2 de manière à **autorisée seulment les VLAN 10 et 99**.

```
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
```

```
S2#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
```

6ème étape : Nous vérifions sur les deux switch que les modifications ont été prises en compte.