Dersim Besiktas

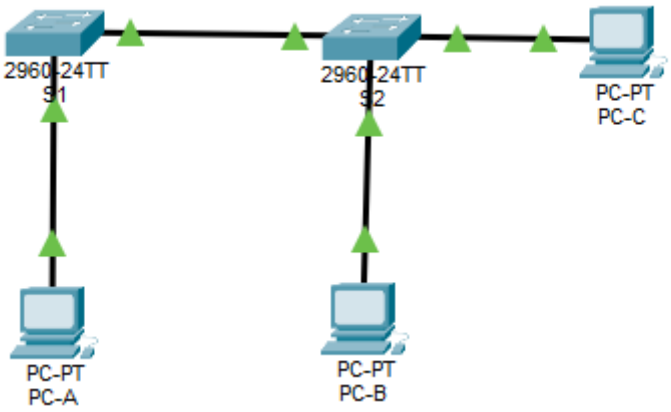
implémentation de la sécurité VLAN

SOMMAIRE

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

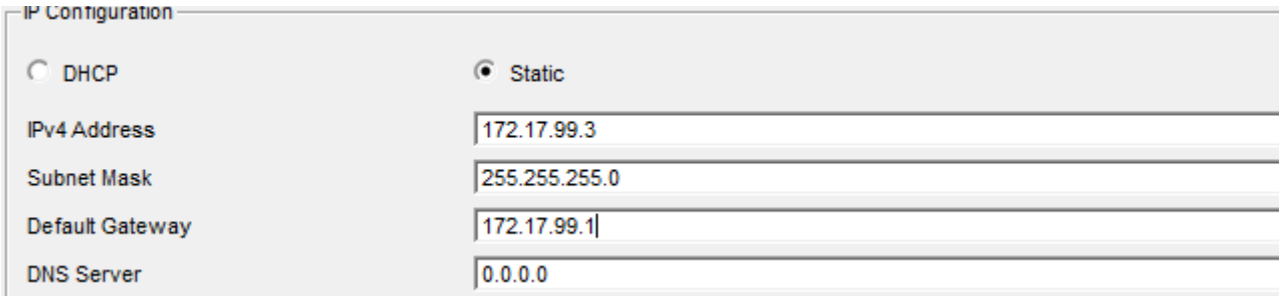
Étape 1 : Câblez le réseau conformément à la topologie

Je câble le réseau conformément à la topologie

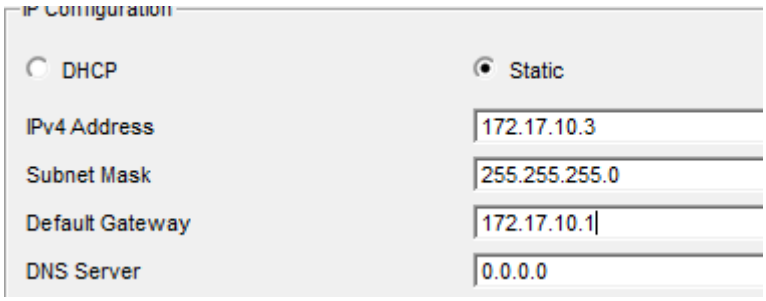


Étape 2 : Configurez les adresses IP sur PC-A, PC-B et PC-C

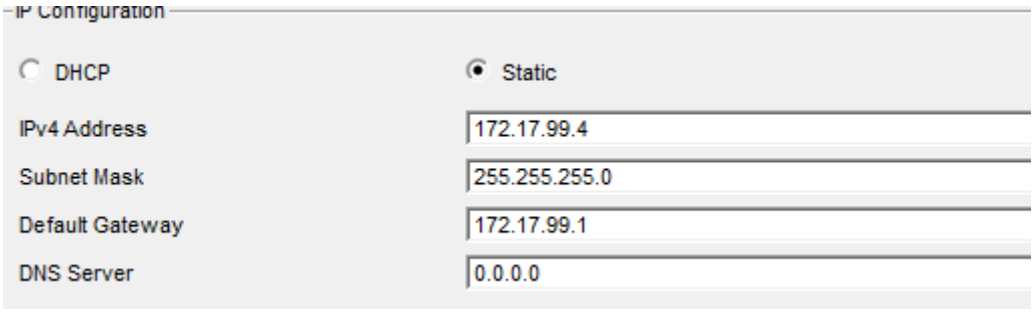
Je configure l'IP de PC-A



Je configure l’IP de PC-B



Je configure l’IP de PC-C



Étape 3 : Configurez les paramètres de base pour chaque commutateur

Configuration de S1

Je désactive la recherche DNS

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#
```

Je change le nom du commutateur

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

J’attribue classe comme mot de passe pour le mode privilégié

```
S1(config)#enable secret class
S1(config)#
```

J’attribue cisco comme mot de passe console et vty

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#enable secret class
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#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)#
```

Configuration de S2

Je désactive la recherche DNS

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-l
Switch(config)#no ip domain-lookup
Switch(config)#
```

Je change le nom du commutateur

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

J’attribue class comme mot de passe pour le mode privilégié

```
S2(config)#enable secret class
S2(config)#
```

J’attribue cisco comme mot de passe console et vty

```
S2(config)#line con 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#logging synchronous
S2(config-line)#line vty 0 4
S2(config-line)#password cisco
S2(config-line)#login

S2(config-line)#exec-timeout 5 0
S2(config-line)#logging synchronous
S2(config-line)#
```

Étape 4 : Configurez des VLAN sur chaque commutateur

Je créer les VLAN sur S1

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

Je mets une adresse IP au VLAN 99

```
S1(config-vlan)#int vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#
```

Je mets l’interface F0/6 en tant que port access et je l’attribue au VLAN 99

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 99
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

Je créer les VLAN sur S2

```
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#vlan 10
S2(config-vlan)#name Donnees
S2(config-vlan)#vlan 99
S2(config-vlan)#name Management&Native
S2(config-vlan)#vlan 999
S2(config-vlan)#name BlackHole
S2(config-vlan)#
```

Je mets une adresse IP au VLAN 99

```
S2(config)#int vlan 99
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#
```

Je configure les interfaces F0/11 et F0/18 en tant que port d'accès et je les attribues au VLAN 10 et 99

```
S2(config)#int f0/11
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#int f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 99
S2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S2(config-if)#
```

Je tape la commande show vlan brief sur les deux switchs

```
S1#sh vlan br

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
```

```
S2#sh vlan br

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
```

Étape 5 : Configurez la sécurité de base du commutateur

Je désactive les interfaces non utilisées sur S1

```
S1(config-if-range)#int range f0/2 - 5
S1(config-if-range)#shut
```

```
S1(config-if-range)#int range f0/7 - 24
S1(config-if-range)#shutdown
```

```
S1(config-if-range)#int range g0/1 - 2
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
S1(config-if-range)#
```

Je désactive les interfaces non utilisées sur S2

```
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int range f0/2 - 10
S2(config-if-range)#shut
S2(config-if-range)#
```

```
S2(config-if-range)#int range f0/12 - 17
S2(config-if-range)#shutdown
```

Étape 6 : Vérifiez la connectivité entre les périphériques ainsi que les informations VLAN

Je ping S1 depuis PC-A

```
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

C:\>
```

Ping S2 depuis S1

```
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)

S1#
```

Ping S2 depuis PC-B

```
C:\>ping 172.17.99.11

Pinging 172.17.99.11 with 32 bytes of data:

Request timed out.
```

Ping S1 depuis PC-B

```
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),

C:\>
```

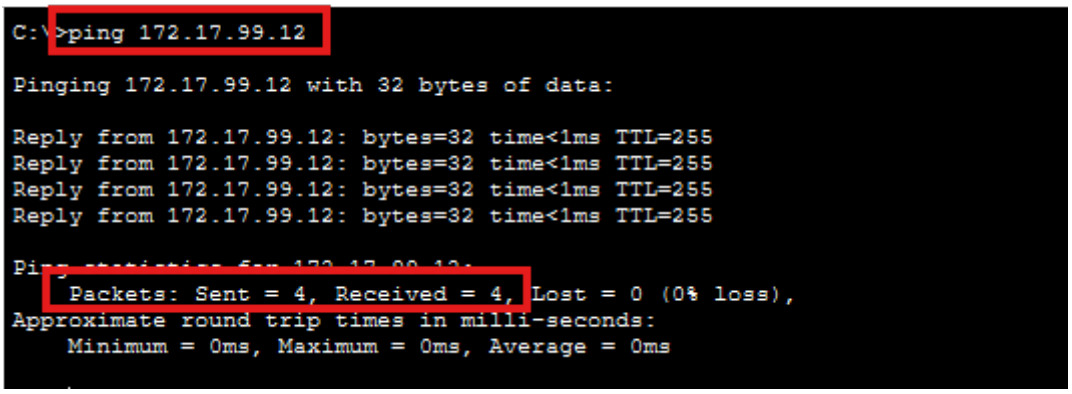
Ping PC-A depuis PC-B

```
C:\>ping 172.17.99.3

Pinging 172.17.99.3 with 32 bytes of data:

Request timed out.

Ping statistics for 172.17.99.3:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
```

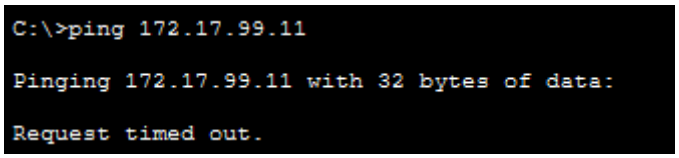
Ping PC-C depuis PC-B

```
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 S2 depuis PC-C



Ping S1 depuis PC-C



Partie 2 : Implémentation de la sécurité VLAN sur les commutateurs

Étape 1 : Configurez les ports trunk sur S1 et S2

Je configure les ports trunk sur S1 et S2

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int f0/1
S1(config-if)#switchport mode trunk
S1(config-if)#
```

```
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int f0/1
S2(config-if)#switchport mode trunk
S2(config-if)#
```

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

Je configure le vlan natif sur S1 et S2

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int f0/1
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#
```

```
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int f0/1
S2(config-if)#switchport trunk native vlan 99
S2(config-if)#
```

Sur S1 je tape la commande show interface trunk

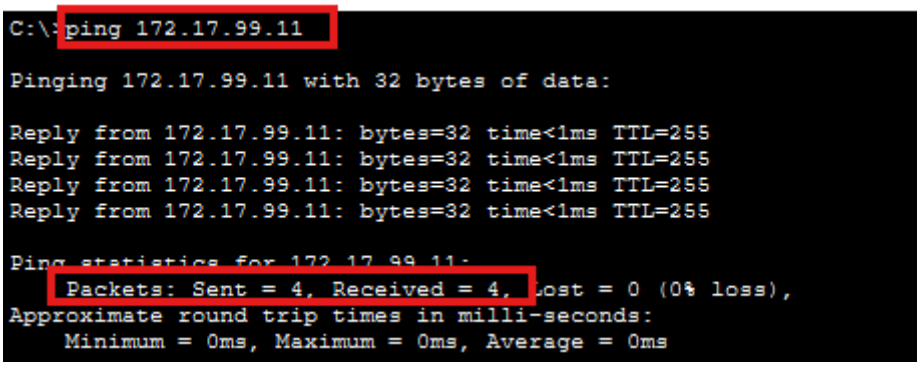
```
S1>en
Password:
S1#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

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

S1#
```

Sur S2 je tape la commande show interface trunk

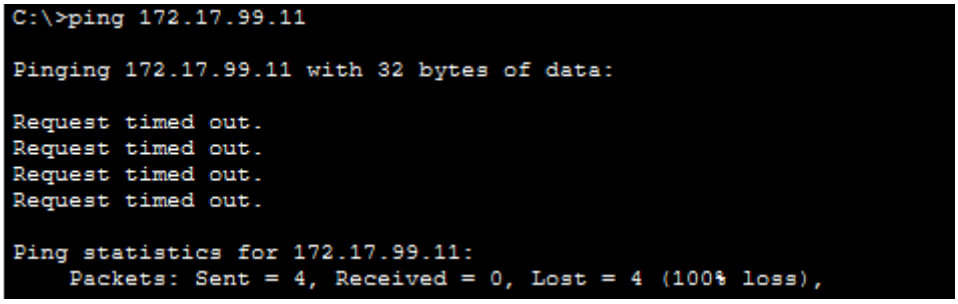
```
S2>en
Password:
S2#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

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

S2#
```

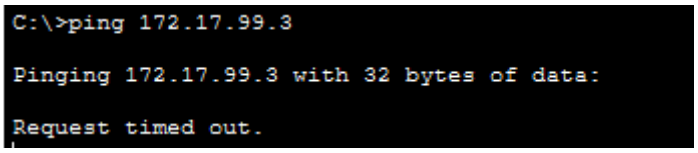
Étape 3 : Vérifiez que le trafic peut correctement traverser la liaison trunk

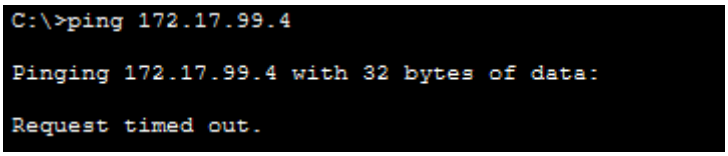
Je ping S1 depuis PC-A



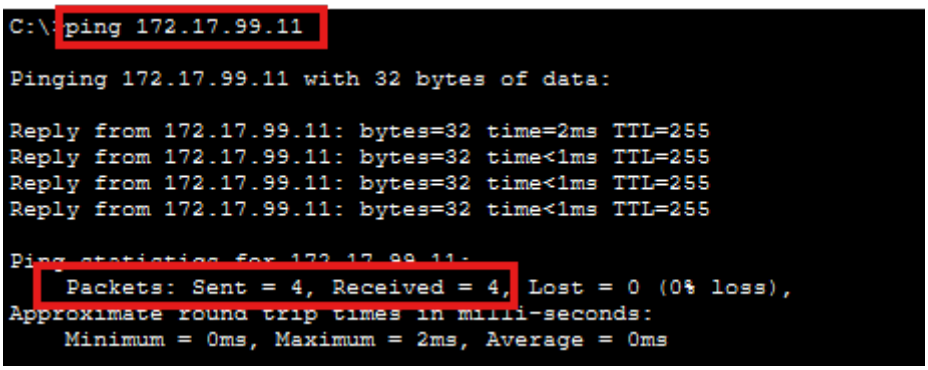
Je ping S1,PC-A et PC-C depuis PC-B

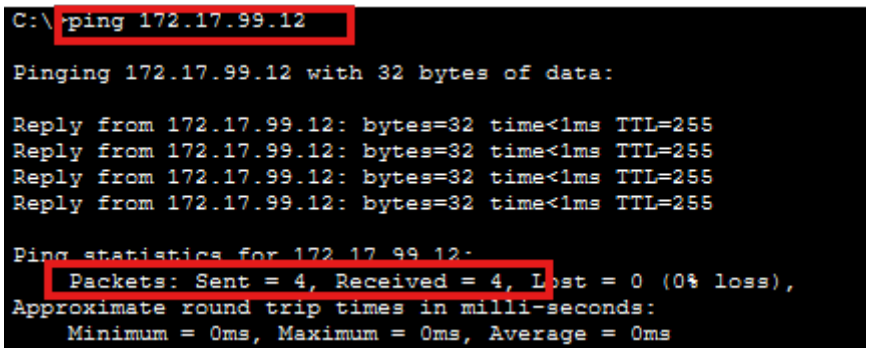


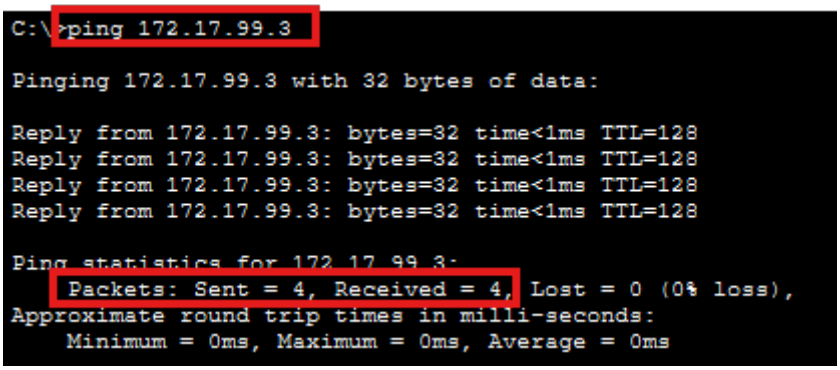




Je ping S1,S2 et PC-A depuis PC-C







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

```
S1#sh int 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)
```

Je désactive la négociation sur S1

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int f0/1
S1(config-if)#switchport nonegotiate
S1(config-if)#
```

Je désactive également sur S2

```
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int f0/1
S2(config-if)#switchport nonegotiate
S2(config-if)#
```

Je vérifie qu'il est bien désactiver sur S1 et S2

```
S1#sh int 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)

S2#sh int 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)
```

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
```

```
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)
```

Je désactive le trunking sur les port d'accès de S1

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int range f0/2 - 5
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 999
S1(config-if-range)#
```

Je désactive également sur S2

```
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int range f0/2 - 5
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 999
S2(config-if-range)#
```

Je vérifie que le port F0/2 est configuré pour accéder à S1

```
S1#sh int 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)
```

Je vérifie les attributions des ports VLAN sur les deux switchs

```
S1#sh vlan br

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
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#
```

```
S2#sh vlan br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    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    Fa0/2, Fa0/3, Fa0/4, Fa0/5
1002 fddi-default                      active
```

Je fais en sorte que le port trunk F0/1 sur S1 autorise seulement les VLAN 10 et 99

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int f0/1
S1(config-if)#switchport trunk allowed vlan 10,99
S1(config-if)#
```

Je fais la même chose sur S2

```
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int f0/1
S2(config-if)#switchport trunk allowed vlan 10,99
S2(config-if)#
```

Sur S1 et S2 je vérifie les VLAN autorisés

```
S1#sh int 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

S1#
```

```
S2#sh int 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#
```