TP13 – Implémentation sécurité VLAN

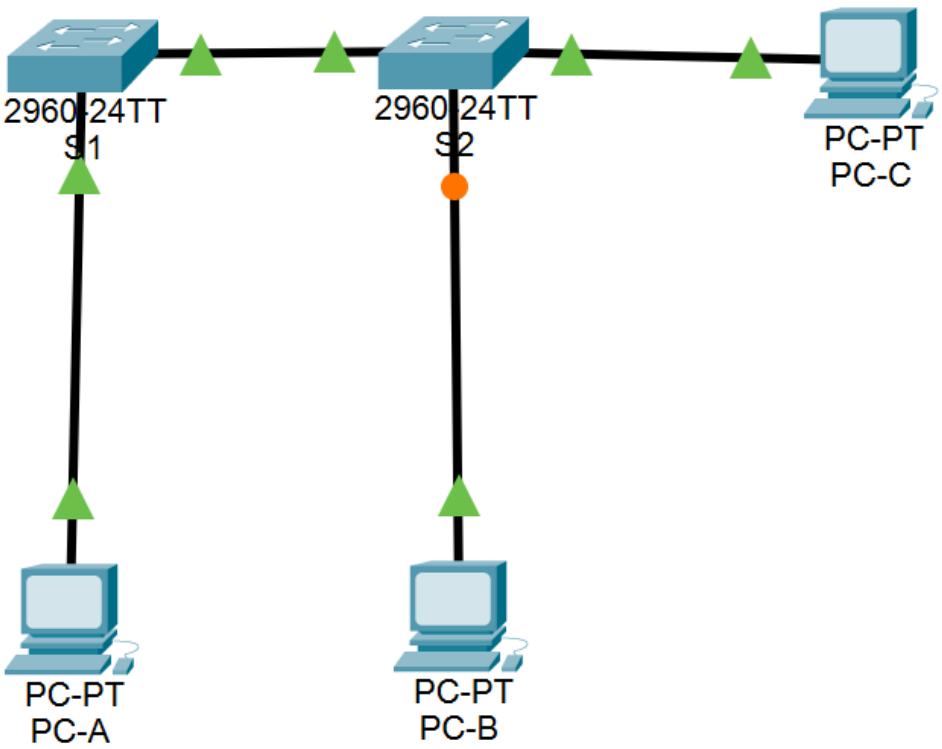
SAOU Rayan

Table des matières

---

1. Respect de la topologie

Nous installons les équipements de la manière suivante :



Nous configurons les adresses IP sur les PC-A, PC-B et PC-C :

```
Device Name: PC-A
Device Model: PC-PT

Port            Link   IP Address         IPv6 Address                              MAC Address
FastEthernet0   Up     172.17.99.3/16     <not set>                                 0004.9A07.7842
Bluetooth       Down   <not set>          <not set>                                 00D0.58C1.E620

Gateway: 172.17.99.1
DNS Server: <not set>
Line Number:  <not set>

Physical Location: Intercity > Home City > Corporate Office > PC0
```

```
Device Name: PC-B
Device Model: PC-PT

Port            Link   IP Address         IPv6 Address                              MAC Address
FastEthernet0   Up     172.17.10.3/16     <not set>                                 000D.BD55.5EB7
Bluetooth       Down   <not set>          <not set>                                 0009.7C62.D05A

Gateway: 172.17.10.1
DNS Server: <not set>
Line Number:  <not set>

Physical Location: Intercity > Home City > Corporate Office > PC1
```

```
Device Name: PC-C
Device Model: PC-PT

Port            Link   IP Address         IPv6 Address                              MAC Address
FastEthernet0   Up     172.17.99.4/16     <not set>                                 0030.F259.B39E
Bluetooth       Down   <not set>          <not set>                                 0001.97D1.136A

Gateway: 172.17.99.1
DNS Server: <not set>
Line Number:  <not set>

Physical Location: Intercity > Home City > Corporate Office > PC2
```

Ensuite, nous respectons cette configuration de base sur chaque switch :

```
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)#logging synchronous
S1(config-line)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#logging synchronous
S1(config-line)#
```

Ensuite, nous configurons pour chaque switch les VLAN :

```
S1(config-line)#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)#
```

Nous attribuons l'addresse IP au VLAN 99 pour les deux switchs :

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

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

Nous configurons F0/6 sur S1 en tant que port d'accès et nous l'attribuons au VLAN 99 :

```
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 99
S1(config-if)#
```

Nous configurons F0/11 sur S2 en tant que port d'accès et nous l'attribuons au VLAN 10 :

```
S2(config-if)#int f0/11
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
```

Nous configurons F0/18 sur S2 en tant que port d'accès et nous l'attribuons au VLAN 99 :

```
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
```

Nous vérifions ensuite les attributions VLAN et des ports de chaque switch :

```
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
999  BlackHole                         active
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    Fa0/1, 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
S2#
```

Tous les autres ports sont attribués au VLAN 1.

Nous désactivons ensuite tous les ports non utilisés de chaque switch :

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

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down
S1(config-if-range)#int range f0/7-24
S1(config-if-range)#shut
```

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

%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)#
```

```
S2(config)#int range f0/2-10
S2(config-if-range)#shut

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
S2(config-if-range)#int range f0/12-17
S2(config-if-range)#shut
```

```
S2(config-if-range)#int range f0/19-24
S2(config-if-range)#shut

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
S2(config-if-range)#int range g0/1-2
S2(config-if-range)#shut
```

Nous vérifions ensuite la connectivité entre les périphériques :

- A partir de PC-A nous tentons un ping à l'adresse IP de gestion 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 = 1ms, Average = 0ms

C:\>
```

Ils sont dans le même réseau, et dans le même VLAN 99

- Ping de S1 à S2 :

```
S1#ping 172.17.99.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Cela ne marche pas car ils ne sont ni dans le même réseau, le port F0/1 entre les deux n'est pas en mode trunk, et que ce ne sont pas les même VLAN

- Ping de PC-B aux adresses de gestion S1 et S2, PC-A, PC-B et PC-C

```
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),

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 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),

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),

C:\>
```

Les requêtes n'aboutissent pas car PC-B est dans un VLAN à part, et qu'aucun périphérique lui permet de router vers les autres VLAN !

- Ping depuis PC-C sur l'adresse de gestion de S1 et S2 :

```
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),

C:\>ping 172.17.99.12

Pinging 172.17.99.12 with 32 bytes of data:

Request timed out.
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 = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Réussite partielle, car le port F0/1 n'est pas en mode trunk et ne permet pas l'accès à S1.

2. Implémentation de la sécurité VLAN sur les commutateurs

Nous configurons le port F0/1 de S1 en mode trunk :

```
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)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

Idem pour S2 :

```
S2(config)#int f0/1
S2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

S2(config-if)#switchport mode trunk
S2(config-if)#
```

Nous vérifions le trunking entre S1 et S2 à l'aide de la commande *sh interface trunk* les deux switchs :

```
S1#sh int 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

S1#
```

```
S2#sh int 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#
```

Nous allons modifier le VLAN natif pour les ports trunk F0/1 de S1 et S2, le natif actuel pour ces interfaces sont le VLAN 1.

Nous modifions le VLAN natif de l'interface F0/1 de S1 à VLAN 99 :

```
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 1 on
FastEthernet0/1 VLAN99.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0099. Inconsistent local vlan.

S1(config-if)#
```

Un message d'erreur apparaît car le VLAN natif de S2 n'a pas été modifié, nous le faisons donc :

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

Nous vérifions que le VLAN natif est désormais le 99 pour les deux switchs :

```
S1#sh int 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#
```

```
S2#sh int 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#
```

Le trunk a été établi, nous réessayons les tests de connectivités :

- 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

C:\>
```

Pas de problème.

- 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
```

La requête réussit grâce au trunking de F0/1 entre les deux switchs

- PC-B vers S1,S2, PC-A et PC-C :

```
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),

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 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),

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),

C:\>
```

Les requêtes n'ont toujours pas abouti pour les mêmes raisons.

- PC-C vers S1,S2 et PC-A

```
C:\>ping 172.17.99.11

Pinging 172.17.99.11 with 32 bytes of data:

Request timed out.
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255
Reply from 172.17.99.11: bytes=32 time=6ms TTL=255
Reply from 172.17.99.11: bytes=32 time=6ms TTL=255

Ping statistics for 172.17.99.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 4ms

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

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=7ms 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 = 7ms, Average = 1ms

C:\>
```

Les requêtes ont abouti car ils sont dans le même VLAN.

Nous allons maintenant empêcher l'utilisation du protocole DTP sur S1 et S2, nous observons le comportement par défaut avec la commande ***sh int f0/1 switchport*** :

```
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)
Trunking Native Mode VLAN: 99 (Management&Native)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
```

Nous désactivons sur S1 la négociation :

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

Idem sur S2 :

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

Et si nous regardons à nouveau :

```
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)
Trunking Native Mode VLAN: 99 (Management&Native)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
```

Nous allons maintenant sécuriser les ports d'accès sur S1 et S2 :

Si nous exécutons la commande ***sh int f0/2 switchport*** :

```
S1#sh int 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
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
```

L'état du trunking est en ***dynamic auto*** et la négociation est ***activée*** :

Nous désactivons le trunking sur les ports d'accès 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)#
```

Et nous faisons de même pour les ports d'accès de S2 :

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

Nous vérifions 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)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
```

Et nous vérifions l'attribution des ports VLAN des deux switches :

```
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
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S2#
```

Nous faisons en sorte que le port F0/1 sur S1 n'autorise que 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)#
```

Et idem 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)#
```

Et nous vérifions l'état du trunk avec 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#
```