

# Cybersécurité Spanning-Tree mise en place



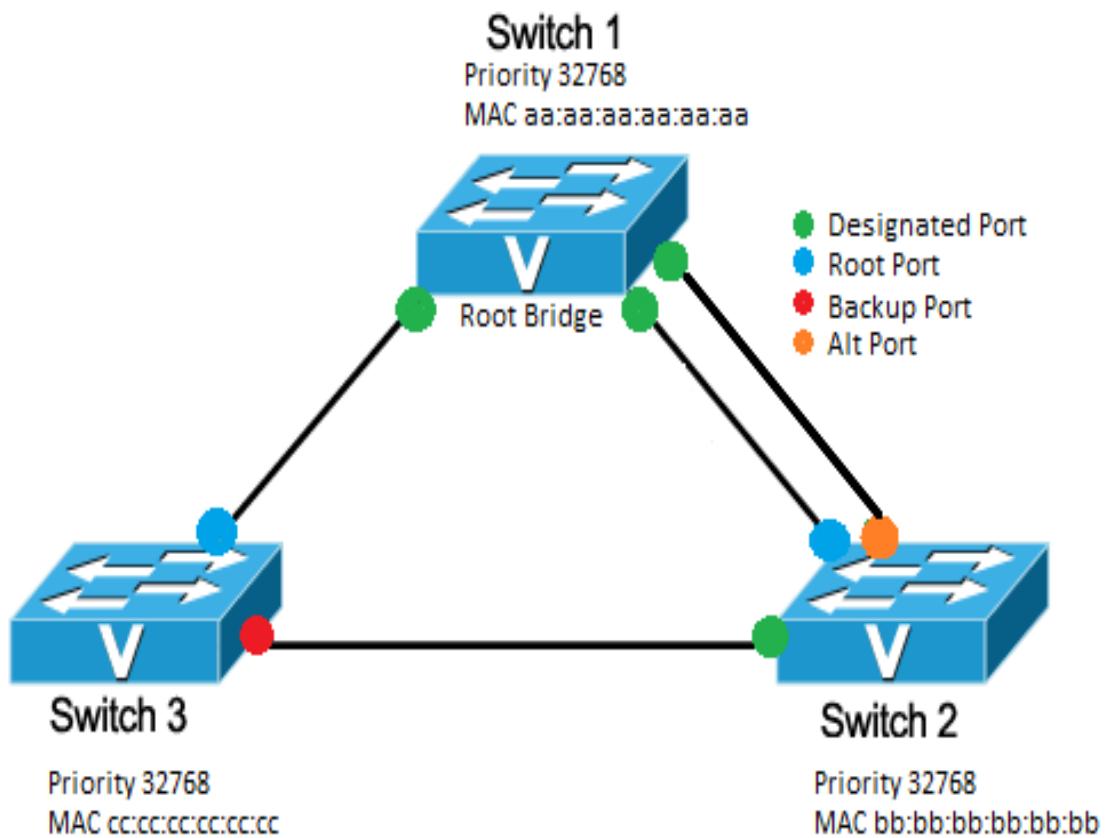
## Définition du Spanning-tree :

	2
• <u>Partie 1 Mise en place du protocole STP</u>	3
Schéma Réseau du Spanning-Tree	3
Mise en place d'un spanning tree	3
Afficher les informations d'interface vlan 1	5
Mise en place et compréhension du Spanning-tree	6
• <u>Partie 2 : Mise en place de la propagation des VLAN protocole</u>	10
Création des VLAN	10
Création d'un serveur VTP	11
Propagation des VLAN sur le Switch B	12
Mise en place du serveur VTP sur le Switch B	13

## Définition du Spanning-tree

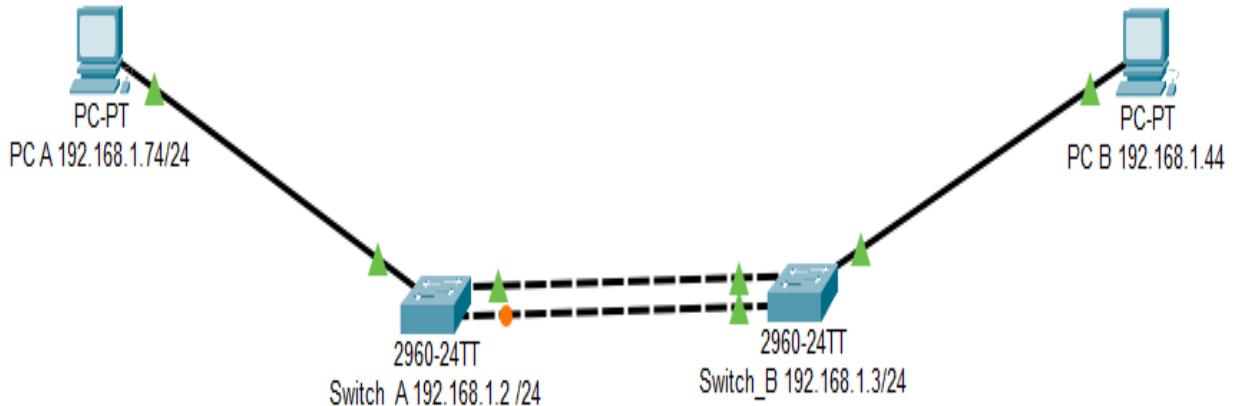
Le Spanning-tree organise les connexions entre les ordinateurs pour éviter les problèmes de boucles et garantir un réseau qui fonctionne bien. Il permet de connecter des ordinateurs ensemble de manière intelligente pour éviter que les données se perdent ou tournent en rond comme exemple de boucle infini qui peut se produire dans un réseau sans la présence du Spanning-tree entre deux switch et le broadcast entre les différents postes. Cela va alors provoquer un envoi de trames infini sur la bande passante

En utilisant des termes plus techniques nous pouvons alors dire que le Spanning-tree est une structure arborescente utilisée dans les réseaux informatiques pour éliminer les boucles potentielles, assurant ainsi un fonctionnement stable et efficace du réseau.



## Partie 1 Mise en place du protocole STP

### Schéma Réseau du Spanning-Tree



### Mise en place d'un spanning tree

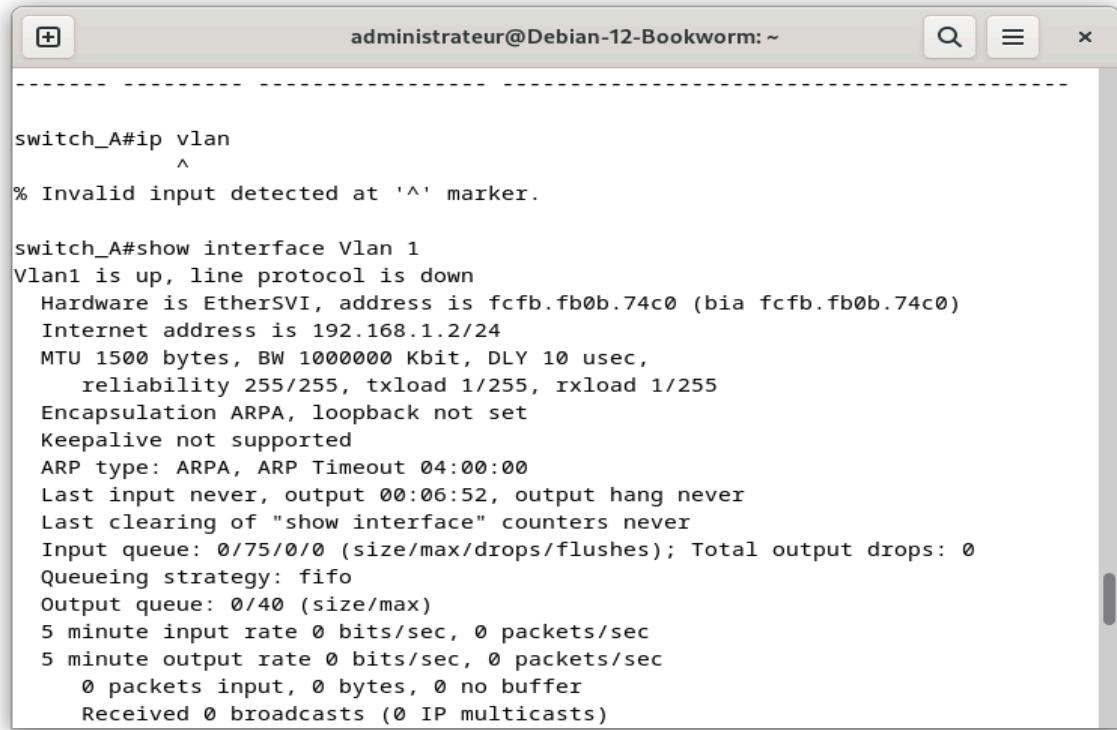
On retrouve ci-dessous la configuration des deux commutateurs avec la modification des mots de passe des commutateurs A et B avec la mise en place d'un mot de passe "class" et d'un nouveau nom d'hôte nommé Switch\_A et Switch\_B.

```
+ administrateur@Debian-12-Bookworm: ~
switch_A#config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch_A(config)#enable secret class
switch_A(config)#config t
^
% Invalid input detected at '^' marker.

switch_A(config)#interface VLAN 1
switch_A(config-if)#ip address 192.168.1.2 255.255.255.0
switch_A(config-if)#no shutdown
switch_A(config-if)#exit
switch_A(config)#interface VLAN 1
switch_A(config-if)#ip address 192.168.1.2 255.255.255.0
switch_A(config-if)#no shutdown
switch_A(config-if)#exit
switch_A(config)#ip default-gateway 192.168.1.1
switch_A(config)#exit
switch_A#
*Mar 1 00:27:20.585: %SYS-5-CONFIG_I: Configured from console by console
switch_A#show vlan

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

Nous configurons ensuite les deux commutateurs en mettant leurs adresses IP et leurs masques avec la passerelle par défaut pour pouvoir communiquer avec les Hôtes ou clients.

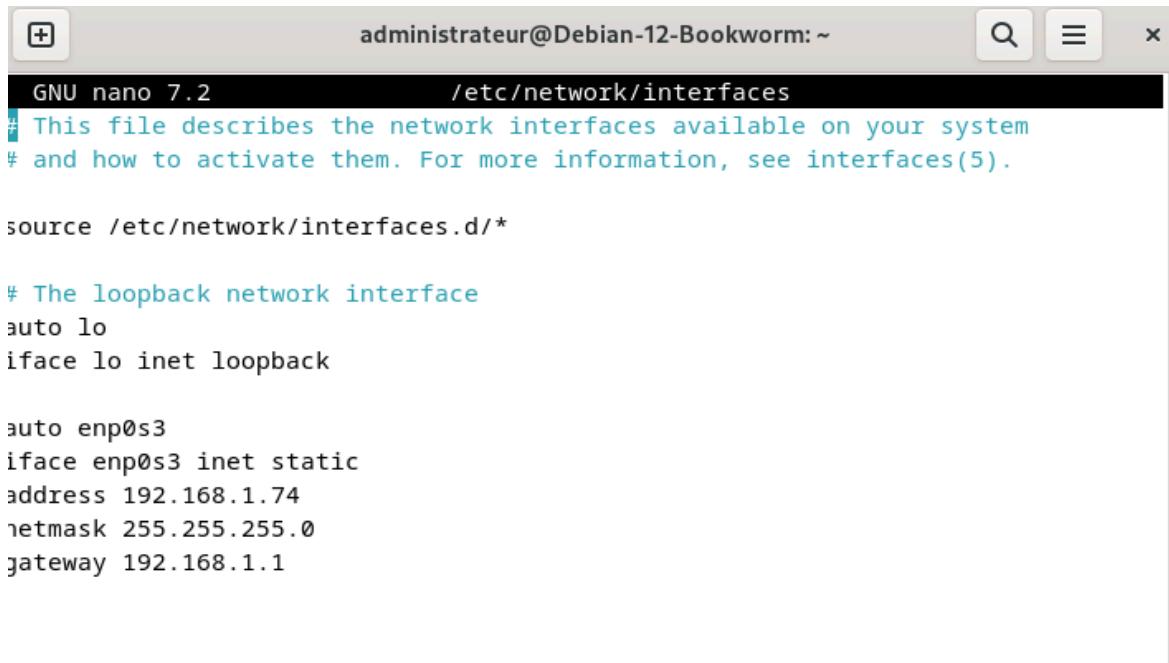


```
switch_A#ip vlan
^
% Invalid input detected at '^' marker.

switch_A#show interface Vlan 1
Vlan1 is up, line protocol is down
  Hardware is EtherSVI, address is fcfc.fb0b.74c0 (bia fcfc.fb0b.74c0)
  Internet address is 192.168.1.2/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:06:52, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
```

### configuration des postes

Nous configurons à la suite les postes clients à l'aide la commande “nano/etc/network/interfaces” pour pouvoir configurer les postes d'hôtes.



```
GNU nano 7.2          /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.*

# The loopback network interface
auto lo
iface lo inet loopback

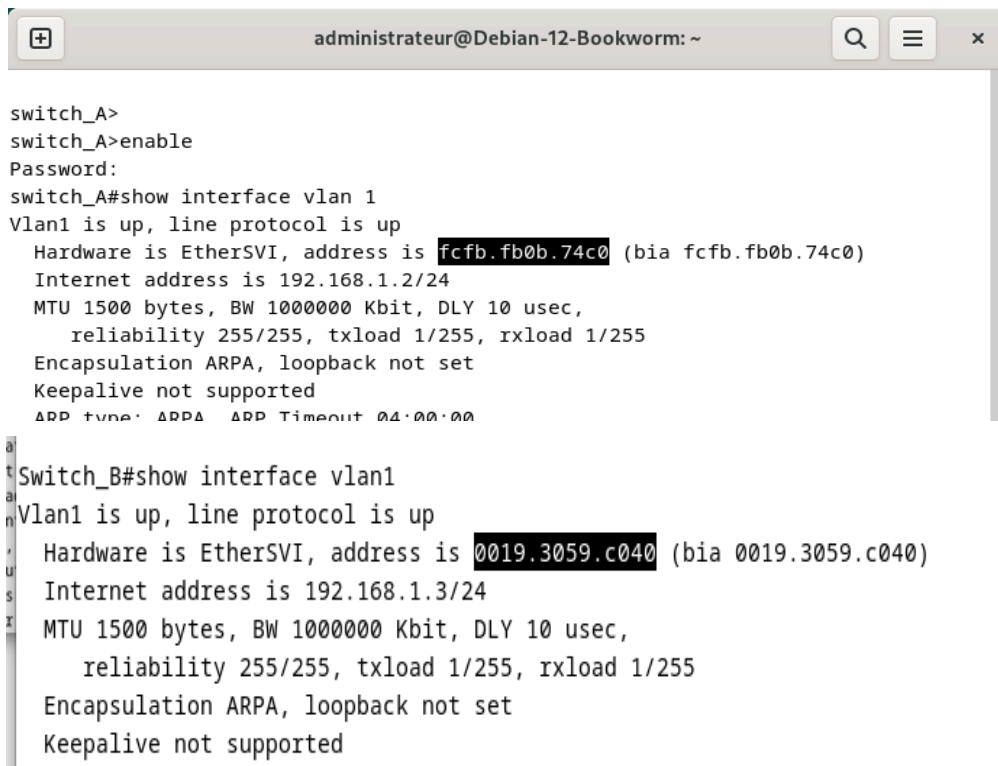
auto enp0s3
iface enp0s3 inet static
  address 192.168.1.74
  netmask 255.255.255.0
  gateway 192.168.1.1
```

Du poste j'ai pu alors effectué les vérifications des différents ping j'ai pu ping le Switch A avec le poste A , le switch B avec ce même poste et aussi le poste B.

```
root@Debian-12-Bookworm:/home/administrateur# nano /etc/network/interfaces
root@Debian-12-Bookworm:/home/administrateur# /etc/init.d/networking stop
Stopping networking (via systemctl): networking.service.
root@Debian-12-Bookworm:/home/administrateur# /etc/init.d/networking start
Starting networking (via systemctl): networking.service.
root@Debian-12-Bookworm:/home/administrateur# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=2 ttl=255 time=1.26 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=255 time=1.29 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=255 time=1.01 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=255 time=1.16 ms
64 bytes from 192.168.1.2: icmp_seq=6 ttl=255 time=1.31 ms
root@Debian-12-Bookworm:/home/administrateur# ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_seq=1 ttl=255 time=2.71 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=255 time=2.47 ms
64 bytes from 192.168.1.3: icmp_seq=3 ttl=255 time=0.832 ms
64 bytes from 192.168.1.3: icmp_seq=4 ttl=255 time=2.32 ms
64 bytes from 192.168.1.3: icmp_seq=5 ttl=255 time=1.35 ms
64 bytes from 192.168.1.3: icmp_seq=6 ttl=255 time=0.918 ms
```

### Afficher les informations d'interface vlan 1

Les informations de l'interface Vlan nous permettent de savoir l'Adresse Mac du Switch A et du Switch B..



```
switch_A>
switch_A>enable
Password:
switch_A#show interface vlan 1
Vlan1 is up, line protocol is up
    Hardware is EtherSVI, address is fcfb.fb0b.74c0 (bia fcfb.fb0b.74c0)
    Internet address is 192.168.1.2/24
    MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
        reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive not supported
    ARP type: ARPA ARP Timeout 04:00:00

Switch_B#show interface vlan1
Vlan1 is up, line protocol is up
    Hardware is EtherSVI, address is 0019.3059.c040 (bia 0019.3059.c040)
    Internet address is 192.168.1.3/24
    MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
        reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive not supported
```

## Mise en place et compréhension du Spanning-tree

Nous affichons la table de Spanning tree sur chaque commutateur.

The image shows two separate windows, each representing a different switch. Both windows have a title bar with the switch name (Switch\_A and Switch\_B) and a tab bar with 'Physical', 'Config', 'CLI' (which is highlighted in blue), and 'Attributes'. Below the tabs is the 'IOS Command Line Interface' prompt. The main area of each window displays the output of the 'show spanning-tree' command. The output includes information about the spanning tree protocol (IEEE 802.1D), the root bridge (Switch\_B), port details (Root ID, Priority, Address, Cost, Hello Time, Max Age, Forward Delay), and interface roles (Desg, FWD, Root, Altn) and costs. Both windows also show a 'Ctrl+F6 to exit CLI focus' message at the bottom and 'Copy' and 'Paste' buttons.

Le commutateur B sera alors la racine car on sélectionne la racine en fonction de l'adresse MAC la plus petite Switch B est en 0019.3059.c040.

- Le commutateur racine est switch B on le remarque avec la présence de son adresse MAC 0019.3059.c040.
- La priorité du commutateur racine est 32769
- Les ports assurent la transmission sont Fa 0/1, 0/2, 0/3.
- Aucun port n'assure le blocage sur le commutateur racine.
- la priorité du commutateur non racine est 32769
- l'ID du pont commutateur est 0040.0BCD.BB47.
- Les ports qui assurent la communication sont Fa 0/1 et Fa 0/2 .
- Le port qui bloque la transmission BLK est le Fa 0/3 .
- Le voyant est orange.

Étape 6 : Mon Switch A est passé en pont racine car il est stipulé que le premier choix par défaut du spanning tree n'est pas forcément le choix le plus optimisé donc nous passons le switch A en Racine au lieu du B.

Mise en place de Spanning tree sur le switch A qui devient alors racine :

```

Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority 4097
              Address 0040.0BCD.BB47
              This bridge is the root
              Hello Time 2 sec Max Age 20 sec Forward Delay 15
sec

  Bridge ID  Priority 4097 (priority 4096 sys-id-ext 1)
              Address 0040.0BCD.BB47
              Hello Time 2 sec Max Age 20 sec Forward Delay 15
sec
              Aging Time 20

  Interface      Role Sts Cost      Prio.Nbr Type
  -----  -----
  Fa0/1          Desg FWD 19      128.1      P2p
  Fa0/2          Desg FWD 19      128.2      P2p
  Fa0/3          Desg FWD 19      128.3      P2p

Switch#

```

Ctrl+F6 to exit CLI focus      Copy      Paste

On remarque alors que sur le Switch B un port est alors bloqué comparé à avant la mise en place du protocole priority 4096 sur le switch A. Donc lors de l'examen de la nouvelle table du Spanning-tree on remarque que les ports qui bloquent les transmissions sont inversés donc le switch B se retrouve avec le port Fa 0/3 bloqué donc orange à la place du Switch\_A.

```

Switch>enable
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority 4097
              Address 0040.0BCD.BB47
              Cost 19
              Port 1(FastEthernet0/1)
              Hello Time 2 sec Max Age 20 sec Forward Delay 15
sec

  Bridge ID  Priority 32769 (priority 32768 sys-id-ext 1)
              Address 0009.7CBA.3176
              Hello Time 2 sec Max Age 20 sec Forward Delay 15
sec
              Aging Time 20

  Interface      Role Sts Cost      Prio.Nbr Type
  -----  -----
  Fa0/3          Altn BLK 19      128.3      P2p
  Fa0/1          Root FWD 19      128.1      P2p
  Fa0/2          Desg FWD 19      128.2      P2p

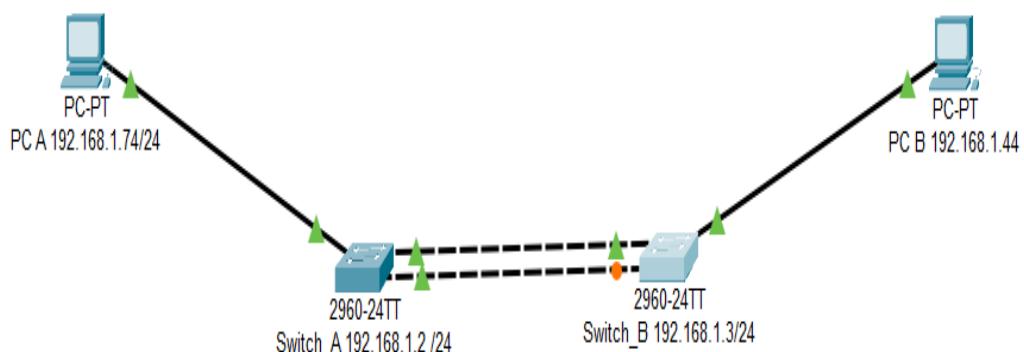
Switch#

```

Ctrl+F6 to exit CLI focus      Copy      Paste

Top

On remarque mieux ce changement à l'aide de la simulation Packet tracer :



Après la mise en place du Spanning tree sur le SWITCH A nous pouvons alors observer la présence d'un fichier dans la commande "show running-config". Qui met en avant l'entrée elle se nomme " spanning mode pvst" et "spanning-tree extend system-id". Cette entrée permet d'indiquer l'existence du protocole spanning tree et la présence de la racine sur ce switch.

```

Switch>enable
Switch#show running-config
Building configuration...

Current configuration : 1161 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 4096
!

```

Retirer un câble du commutateur pour voir la réaction du spanning-tree on remarque alors que sans boucle le spanning tree disparaît pour permettre au poste client de pouvoir communiquer entre eux sans le problème de boucle infini en cas de Broadcast.

Switch_A	PORTS	Switch B
Allumé vert	1	Allumé vert
Allumé vert	2	Allumé vert
Allumé vert	3	Allumé Orange
éteint	4	éteint
éteint	5	éteint
éteint	6	éteint
éteint	7	éteint

éteint	8	éteint
éteint	9	éteint
éteint	10	éteint
éteint	11	éteint
éteint	12	éteint

Retirer un câble du commutateur pour voir la réaction du spanning-tree on remarque alors que sans boucle le spanning tree disparaît pour permettre au poste client de pouvoir communiquer entre eux sans le problème de boucle infini en cas de Broadcast. Après avoir retiré le câble nous pouvons remarquer que la LED passe à la couleur verte et n'a plus orange donc plus aucun port bloquer.

```

Switch_A 192.168.1.2/24
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID  Priority  4097
            Address  0040.0BCD.BB47
            This bridge is the root
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec

  Bridge ID  Priority  4097 (priority 4096 sys-id-ext 1)
            Address  0040.0BCD.BB47
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec
            Aging Time 20

  Interface      Role Sts Cost      Prio.Nbr Type
  -----  -----  -----  -----  -----
  Fa0/1        Desg FWD 19        128.1    P2p
  Fa0/2        Desg FWD 19        128.2    P2p
  Fa0/3        Desg FWD 19        128.3    P2p

Switch#
$LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to down
Ctrl+F6 to exit CLI focus

```

```

Switch_B 192.168.1.3/24
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID  Priority  4097
            Address  0040.0BCD.BB47
            Cost      19
            Port     1(FastEthernet0/1)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec

  Bridge ID  Priority  32769 (priority 32768 sys-id-ext 1)
            Address  0009.7CBA.3176
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec
            Aging Time 20

  Interface      Role Sts Cost      Prio.Nbr Type
  -----  -----  -----  -----  -----
  Fa0/1        Root FWD 19        128.1    P2p
  Fa0/2        Desg FWD 19        128.2    P2p

Switch#
Ctrl+F6 to exit CLI focus

```

On remarque sur la table de spanning tree après avoir retiré le cable que plus aucun port est bloquer pourtant le switch A est toujours racine.

Donc lorsqu'on replace le câble sur le switch on peut remarquer le retour d'un port orange et sur la table du spanning-tree nous avons le retour du port 3 en mode BLK. Pour empêcher la mise en place d'une boucle.

## **Partie 2 : Mise en place de la propagation des VLAN protocole VTP.**

Durant cette deuxième partie nous avons pour mission de mettre en place à l'aide de deux commutateur et deux poste client de mettre en place des vlan sur le switch A et de transmettre ainsi de faire connaître de manière automatique les différents ports et les Vlan mise en place sur le Switch\_A vers le Switch\_B.

Nous avons donc créé des VLAN au sein du Switch\_A que nous observons grâce à la commande "show vlan" on retrouve en effet le VLAN 10 , 20, 30.

```
switch_A#show vlan

/LAN 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, Fa0/11, 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
                           Gi0/1, Gi0/2
1002 fddi-default   act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default   act/unsup
1005 trnet-default   act/unsup
```

### **Création des VLAN**

```
switch_A(vlan)#Vlan 10 name comptabilite
VLAN 10 added:
  Name: comptabilite
switch_A(vlan)#Vlan 20 name Marketing
VLAN 20 added:
  Name: Marketing
switch_A(vlan)#Vlan 30 name ingenierie
VLAN 30 added:
  Name: ingenierie
switch_A(vlan)#exit
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gi0/1, Gi0/2
10	comptabilite	active	Fa0/4, Fa0/5, Fa0/6
20	marketing	active	Fa0/7, Fa0/8, Fa0/9
30	ingenerie	active	Fa0/10, Fa0/11, Fa0/12
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdtnet-default	act/unsup	
1005	trnet-default	act/unsup	
VLAN	Type	SAID	MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
1	enet	100001	1500 - - - - 0 0
10	enet	100010	1500 - - - - 0 0
20	enet	100020	1500 - - - - 0 0
30	enet	100030	1500 - - - - 0 0
1002	fddi	101002	1500 - - - - 0 0
1003	tr	101003	1500 - - - srb 0 0

### Création d'un serveur VTP

```

switch_A#vlan database
% Warning: It is recommended to configure VLAN from config mode,
as VLAN database mode is being deprecated. Please consult user
documentation for configuring VTP/VLAN in config mode.

switch_A(vlan)#vtp domain cisco
Changing VTP domain name from NULL to cisco
switch_A(vlan)#
*Mar  8 00:08:15.268: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed
% Incomplete command.

switch_A(vlan)#vtp server
Device mode already VTP SERVER.
switch_A(vlan)#exit

```

Un serveur VTP est un appareil dans un réseau informatique qui gère les informations relatives aux VLAN (Virtual LANs ou Réseaux Locaux Virtuels). Pour comprendre le rôle d'un serveur VTP dans un réseau informatique avec de nombreux commutateurs, imaginez que chaque commutateur puisse avoir plusieurs VLAN configurés, qui sont comme des groupes virtuels d'ordinateurs pouvant communiquer entre eux. Le serveur VTP apparaît comme le chef des commutateurs et permet donc, lors de sa configuration, de transmettre de manière intelligente les différents ports et VLAN créés et attribués à chaque commutateur du réseau.

Affectation au port Fa 0/1 et du mode trunk :

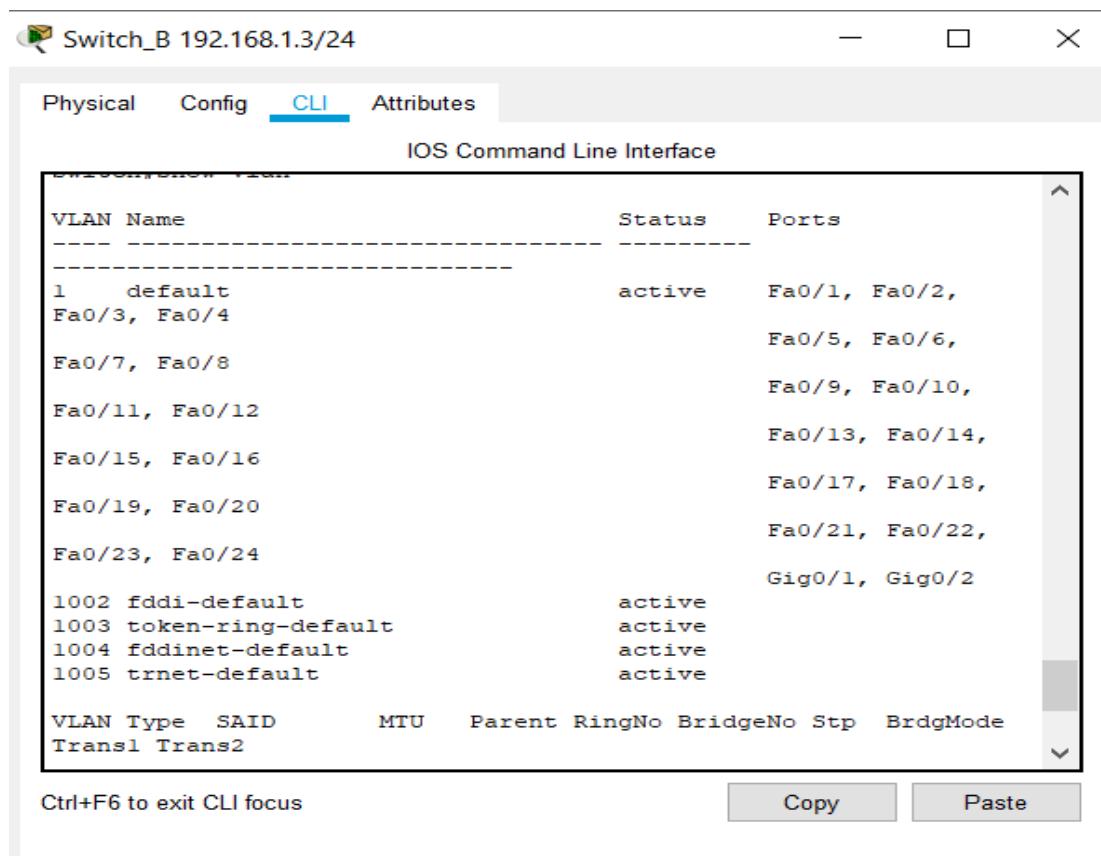
Rappel le mode Trunk permet alors de permettre au sein d'un réseau que les différents VLAN qui le compose puissent communiquer ensemble sans aucune difficulté il permet de faire acheminer la totalité des informations.

```
switch_A#config t
Enter configuration commands, one per line. End with CNTL/Z.
switch_A(config)#interface fastethernet 0/1
switch_A(config-if)#switchport mode trunk
switch_A(config-if)#

```

### Propagation des VLAN sur le Switch B

On remarque avec SHOW vlan que actuellement le Switch B ne possède pas de port attribué au vlan configuré et que les Vlan n'apparaissent pas non plus.



## Mise en place du serveur VTP sur le Switch B

```
% Invalid input detected at '^' marker.  
Switch(vlan)#no vtp  
% Incomplete command.  
Switch(vlan)#vtp domain cisco  
Domain name already set to cisco.  
Switch(vlan)#vtp client  
Setting device to VTP CLIENT mode.  
Switch(vlan)#exit  
APPLY completed.  
Exiting....
```

On remarque alors à la suite de l'implantation du serveur VTP que le Switch B dispose de l'accès à la totalité des VLAN et malheureusement les ports ne sont pas attribués aussi automatiquement. Il est ainsi impossible de pouvoir effectuer les différents ping entre les Vlans sans l'attribution automatique des ports par VTP.

```
Exiting....  
Switch#show vlan  
  
VLAN Name Status Ports  
---- -- ----  
-----  
1 default active Fa0/2, Fa0/3,  
Fa0/4, Fa0/5  
Fa0/6, 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 comptabilite active  
20 Marketing active  
30 Ingenierie active  
1002 fddi-default active  
1003 token-ring-default active  
1004 fddinet-default active
```