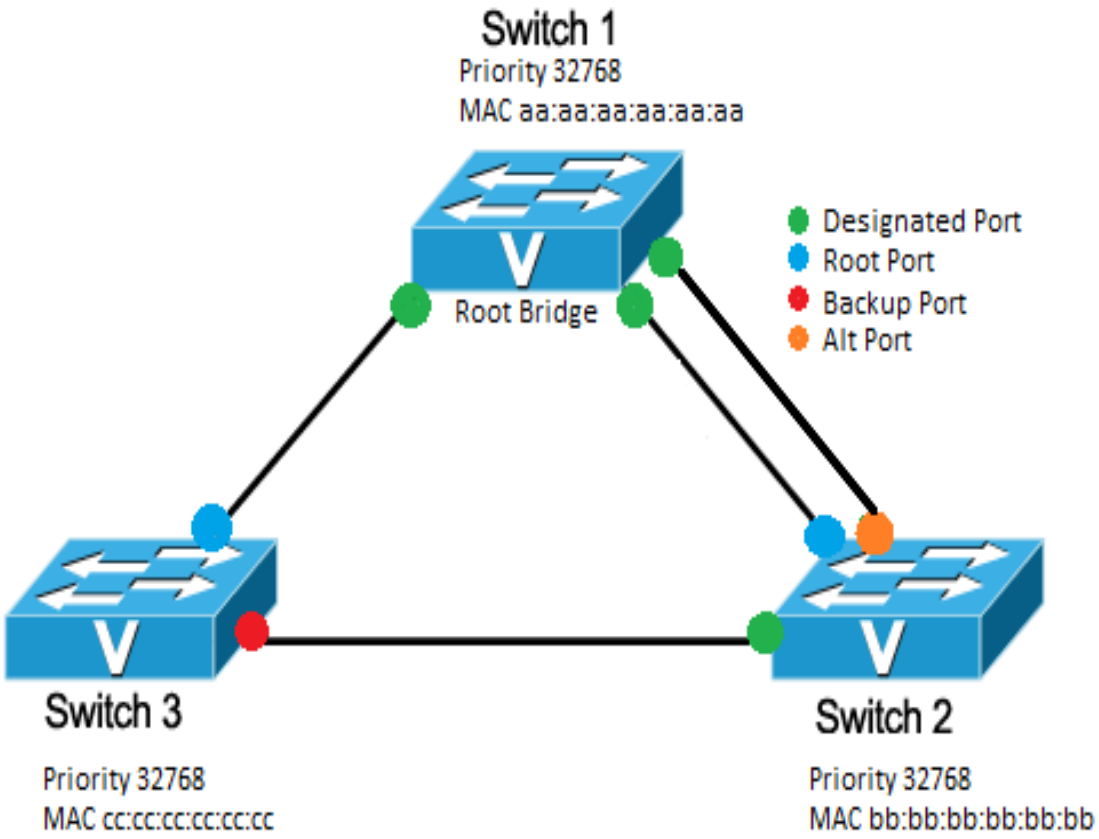
Cybersécurité Spanning-Tree mise en place

Définition du Spanning-tree :

Définition du Spanning-tree

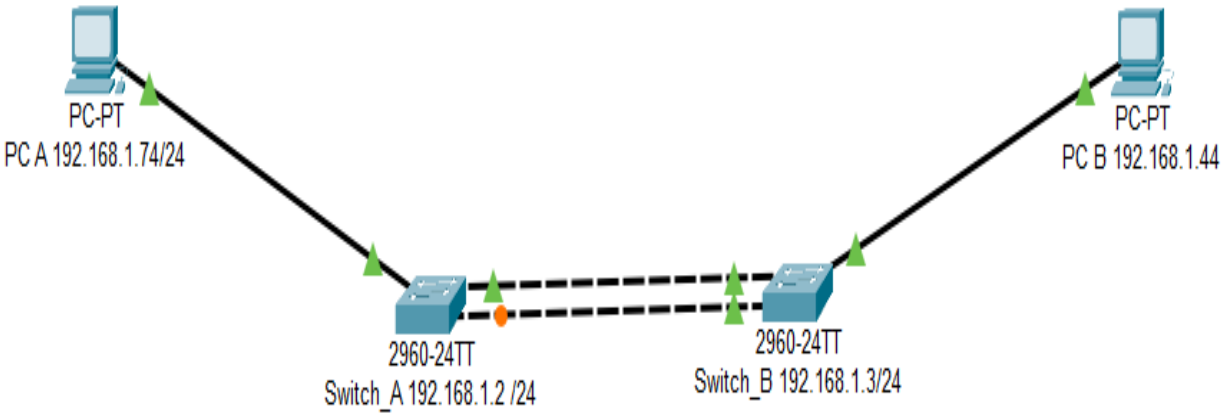
Le Spanning-tree organise les connexions entre les ordinateurs pour éviter les problèmes de boucles et garantir un réseau qui fonctionne bien. Il permet de connecter des ordinateurs ensemble de manière intelligente pour éviter que les données se perdent ou tournent en rond comme exemple de boucle infini 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 envoie 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.



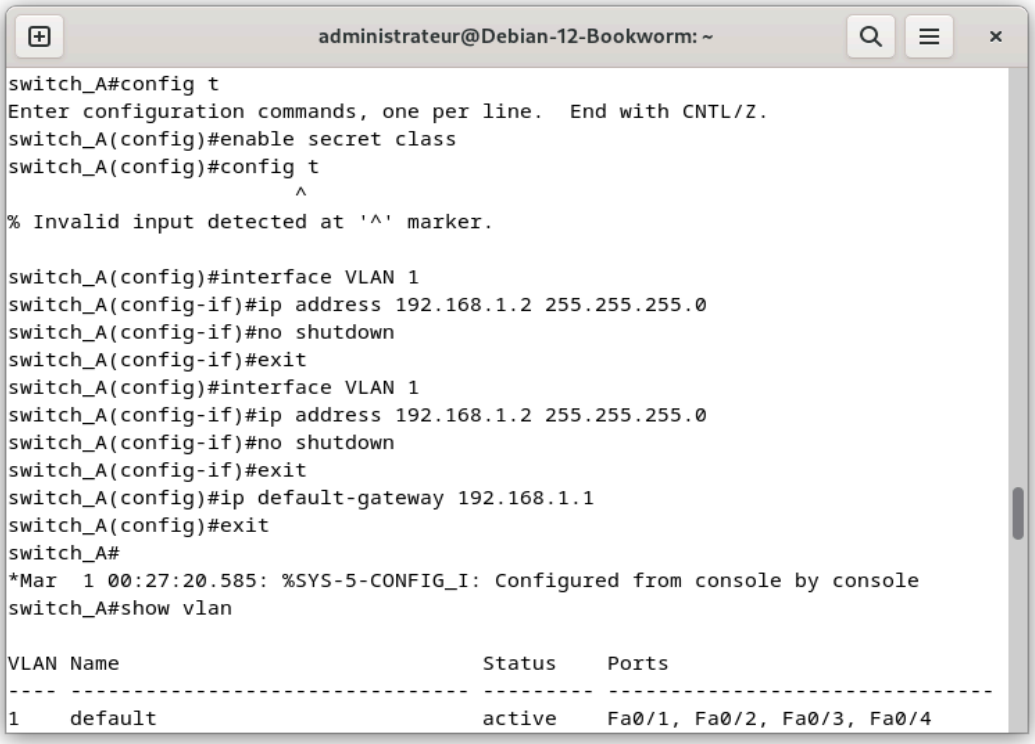
Partie 1 Mise en place du protocole STP

Schéma Réseau du Spanning-Tree

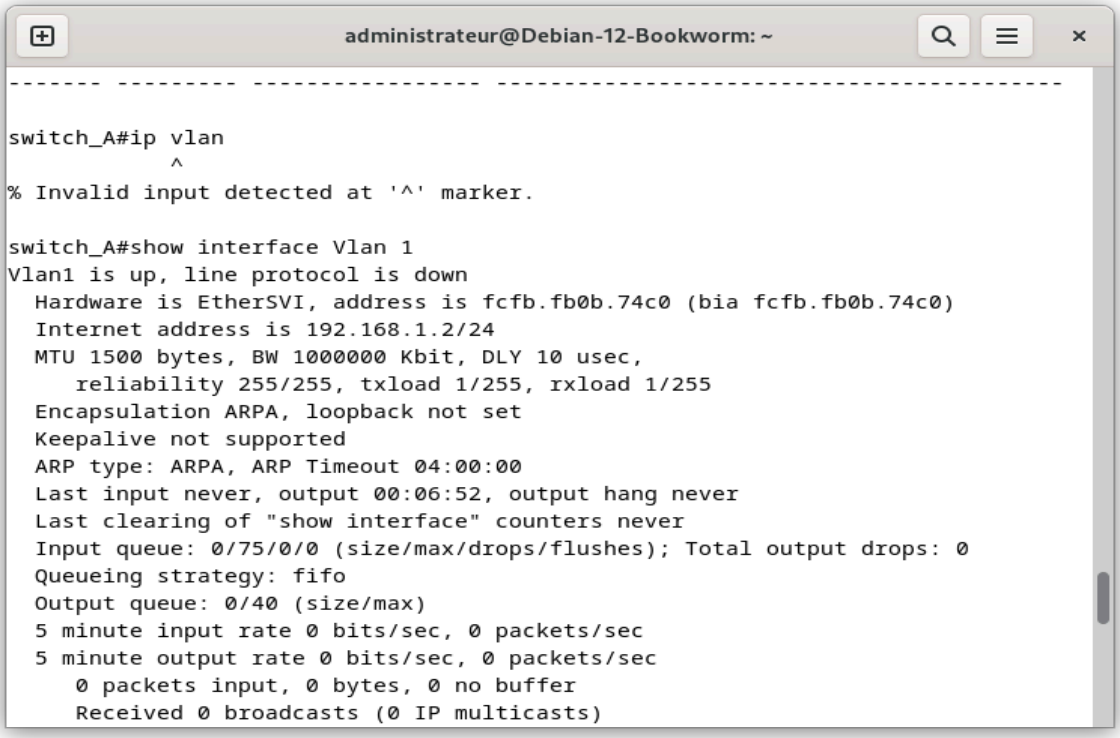


Mise en place d'un spanning tree

On retrouve ci-dessous la configuration des deux commutateurs avec la modification des mots de passes 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.

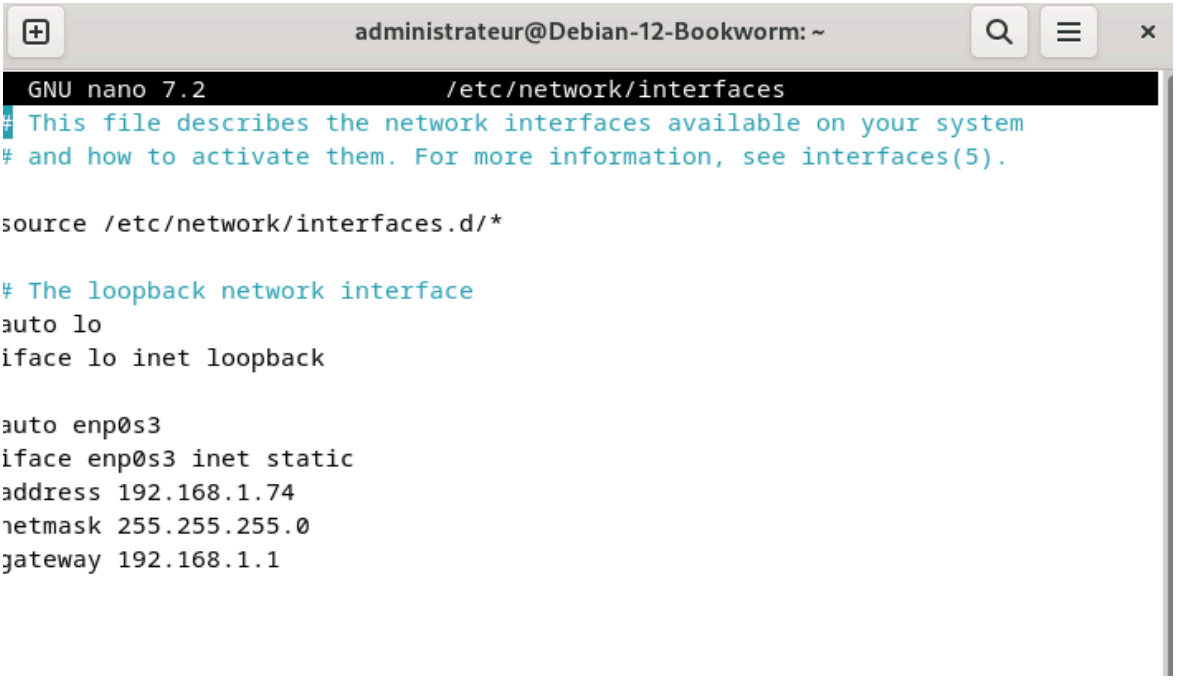


Nous configurons ensuite les deux commutateurs en mettant leurs adresses IP et leurs masques avec la passerelle par défaut pour pouvoir communiquer avec les Hôtes ou clients.



configuration des postes

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



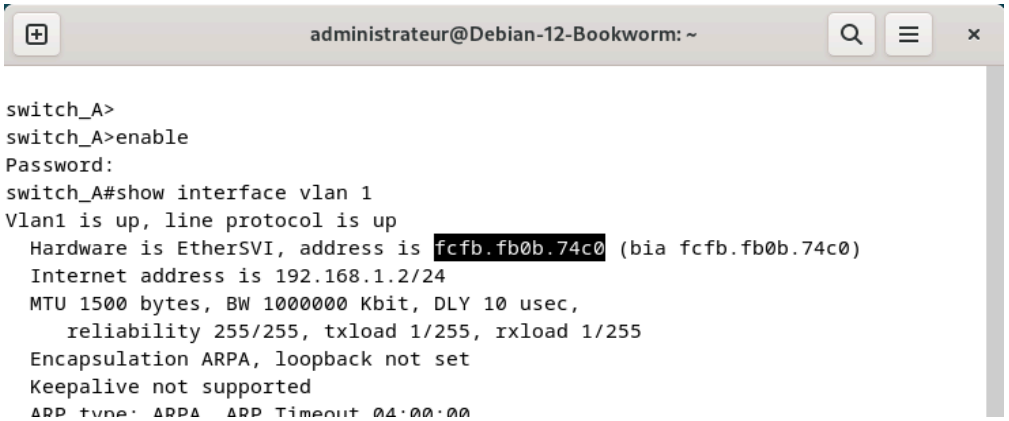
Du poste j'ai pu alors effectué les vérifications des différents ping j'ai pu ping le Switch A avec le poste A , le switch B avec ce même poste et aussi le poste B.

```
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

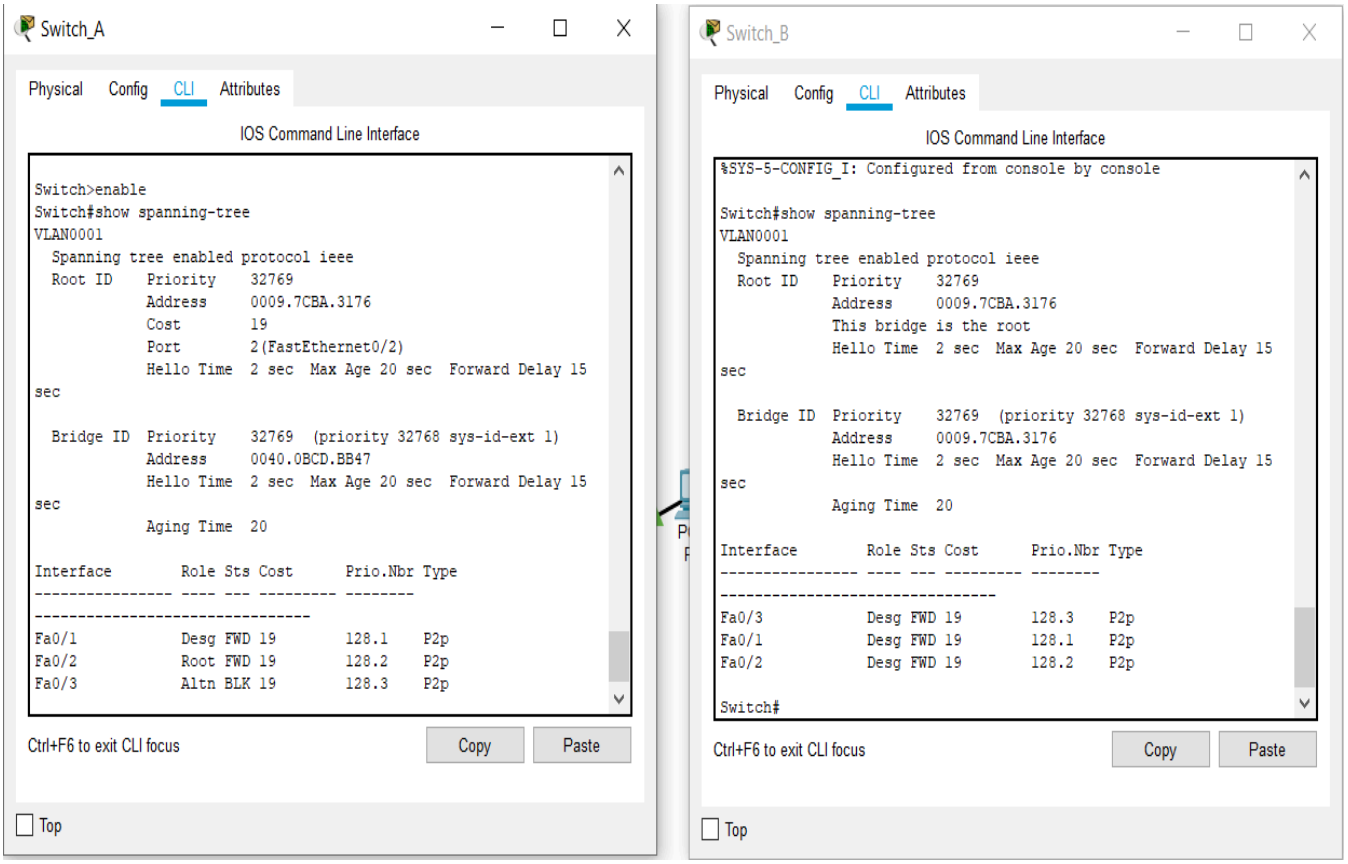
Les informations de l'interface Vlan nous permettent de savoir l'Adresse Mac du Switch A et du Switch B..




```
Switch_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.

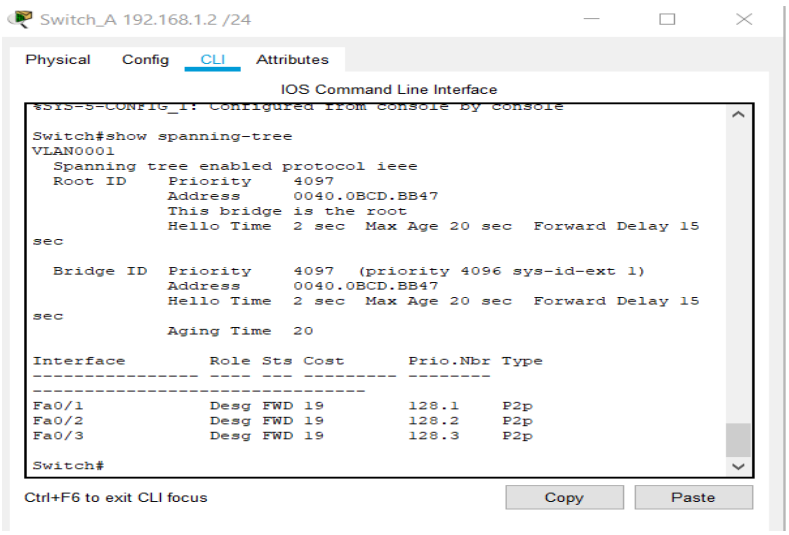


Le commutateur B sera alors la racine car on sélectionne la racine en fonction de l'adresse MAC la plus petite Switch B est en 0019.3059.c040.

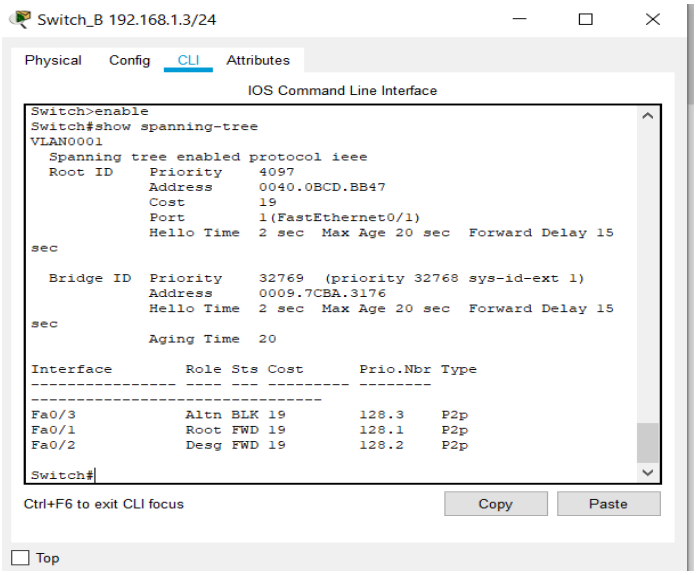
- Le commutateur racine est switch B on le remarque avec la présence de son adresse MAC 0019.3059.c040.
- La priorité du commutateur racine est 32769
- Les ports assurent la transmission sont Fa 0/1, 0/2, 0/3.
- Aucun port n'assure le blocage sur le commutateur racine.
- la priorité du commutateur non 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.

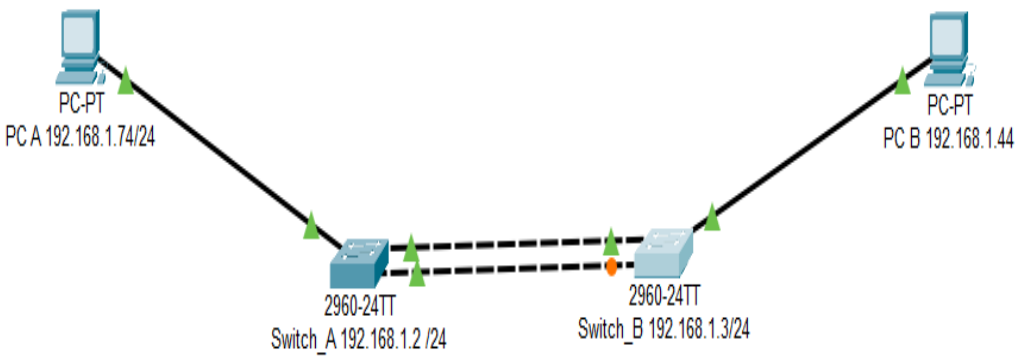
Mise en place de Spanning tree sur le switch A qui devient alors racine :



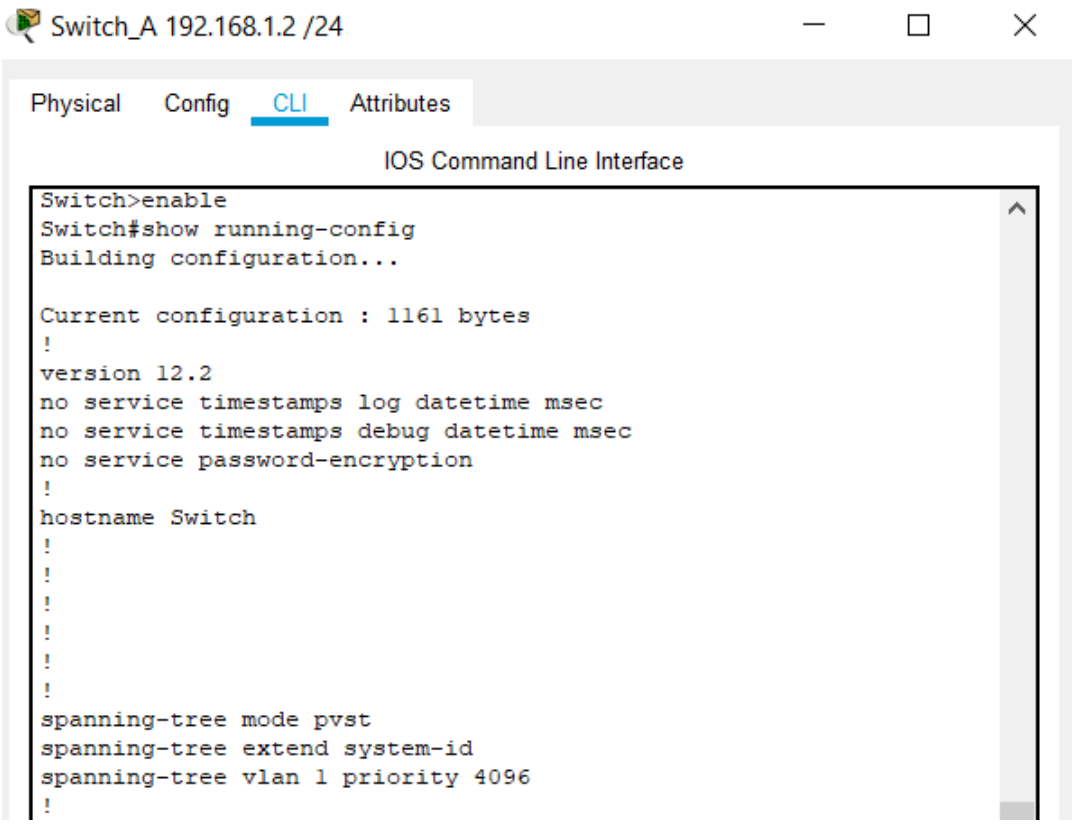
On remarque alors que sur le Switch B un port est alors bloqué comparé à avant la mise en place du protocole priority 4096 sur le switch A. Donc lors de l'examination de la nouvelle table du Spanning-tree on remarque que les ports qui bloquent les transmissions sont inversés donc le switch B se retrouve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



On remarque mieux ce changement a 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.

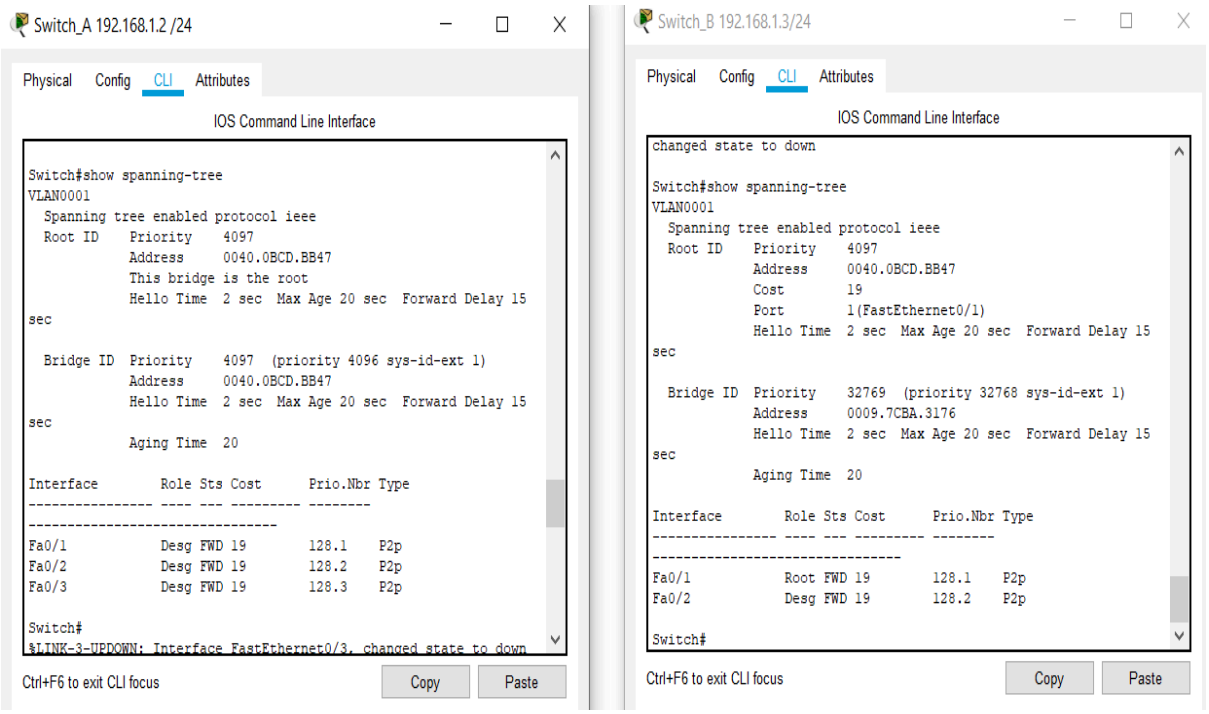


Retirer un câble du commutateur pour voir la réaction du spanning-tree on remarque alors que sans boucle le spanning tree disparaît pour permettre au poste client de pouvoir communiquer entre eux sans le problème de boucle infini en cas de Broadcast.

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'ai plus orange donc plus aucun port bloquer.



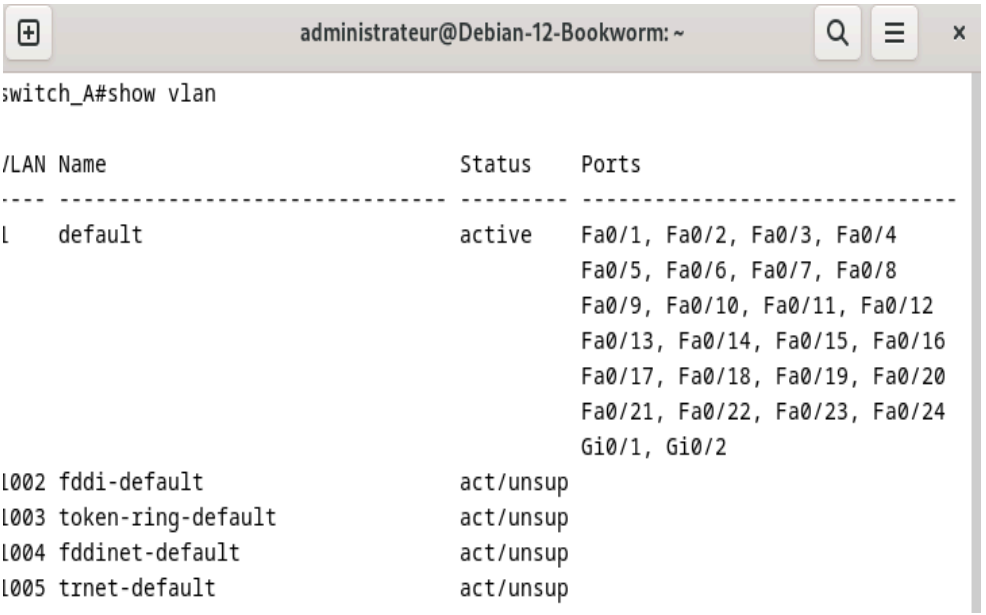
On remarque sur la table de spanning tree après avoir retiré le cable que plus aucun port et bloquer pourtant le switch A est toujours racine.

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.

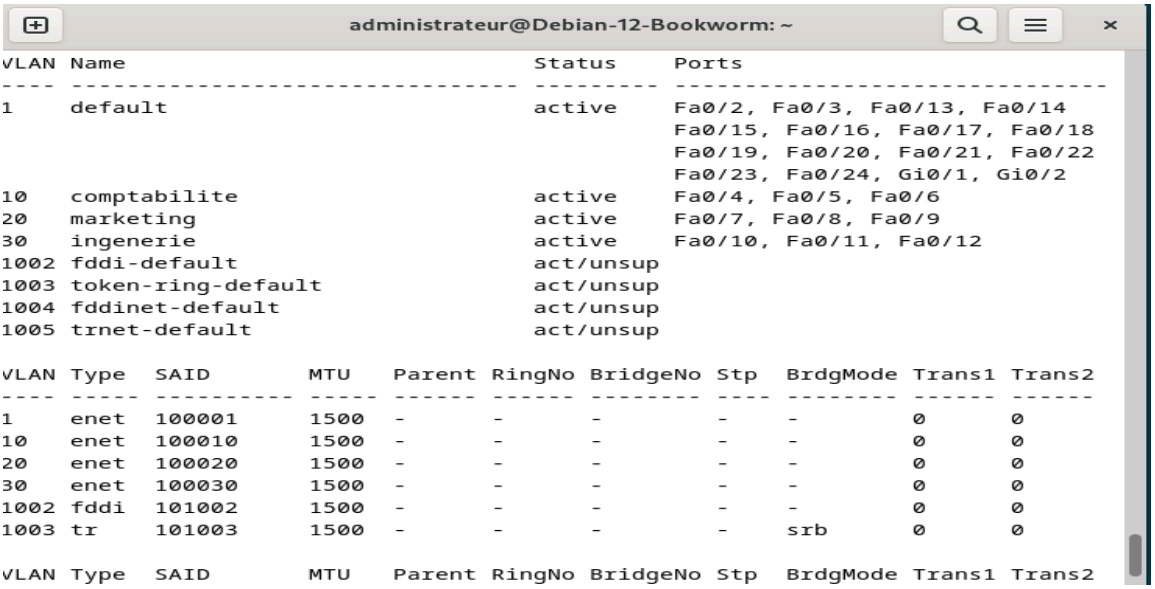
Durant cette deuxième partie nous avons pour mission de mettre en place à l'aide de deux commutateur et deux poste client de mettre en place des vlan sur le switch A et de transmettre ainsi de faire connaître de manière automatique les différents ports et les Vlan mise en place sur le Switch_A vers le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



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
```



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.

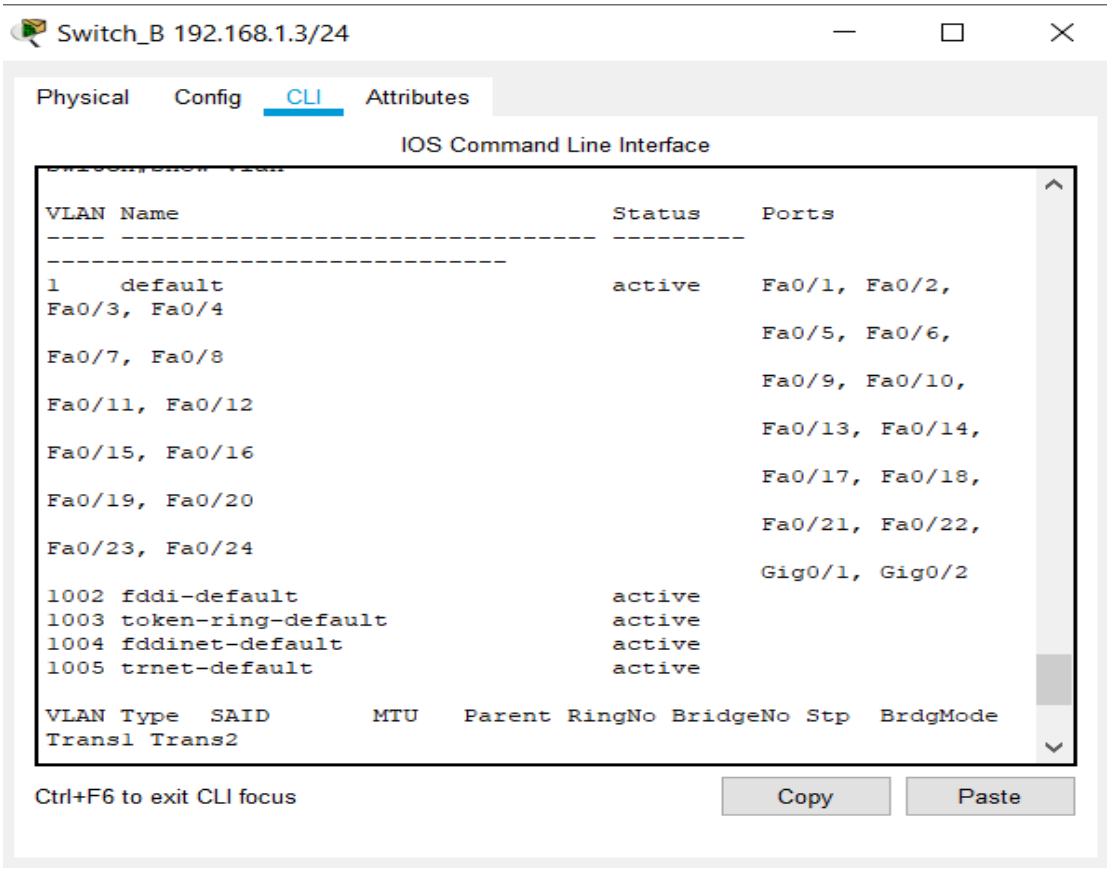
Affectation au port Fa 0/1 et du mode trunk :

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.

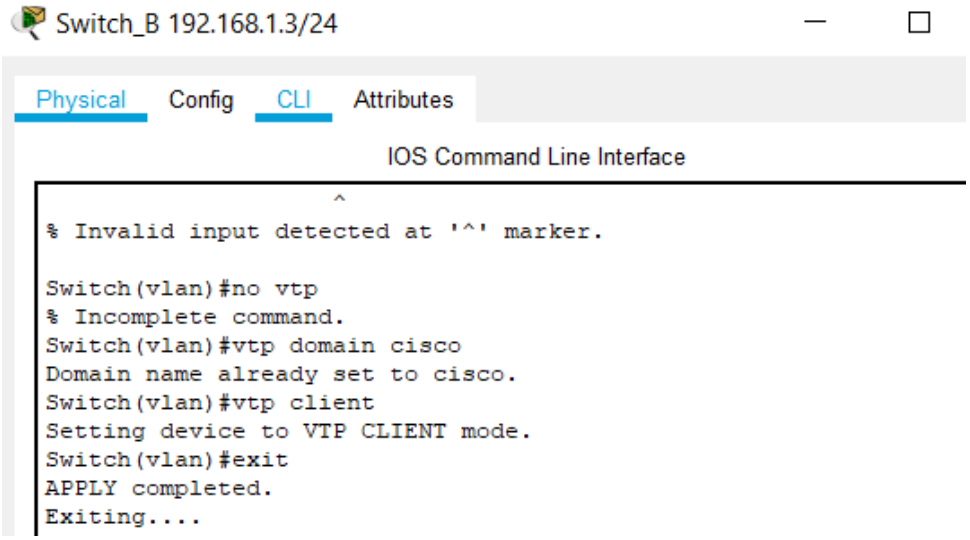
```
switch_A#config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch_A(config)#interface fastethernet 0/1
switch_A(config-if)#switchport mode trunk
switch_A(config-if)#
```

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



On remarque alors a 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.