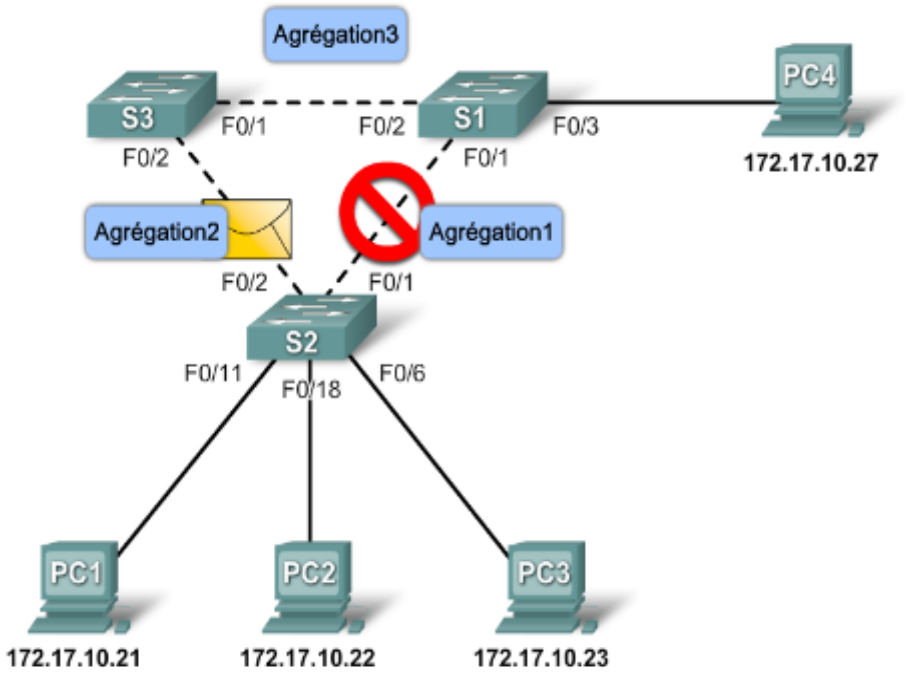
Chapitre 04	Implémenter la redondance LAN

1. Redondance dans un réseau hiérarchique

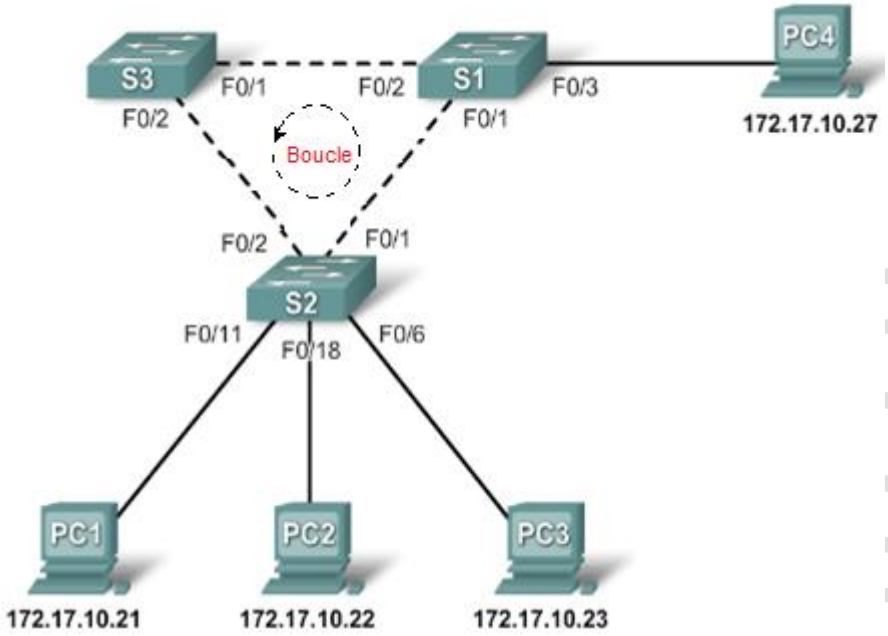
1.1 Redondance sur les liens

- La redondance permet d'avoir plusieurs chemins en cas d'une défaillance d'un lien.
- La multiplication des liens physiques entre les périphériques offre des chemins d'accès redondants. Le réseau peut ainsi continuer à fonctionner, même lorsqu'un port ou un lien donné est défaillant.
- **Exemple :** S2 détecte la connexion interrompue vers S1 et il modifie son chemin d'acheminement pour qu'il passe par le commutateur S3. La boucle entre les trois commutateurs permet d'assurer une liaison de secours (tolérance à la panne) en cas de panne d'un lien.



1.1 Problèmes des liaisons redondantes (sans STP)

- Des tempêtes de diffusion (broadcast) : lorsque des trames de diffusion ou de multicast sont envoyées (FF-FF-FF-FF-FF-FF en destination), les commutateurs les renvoient par tous les ports. Les trames circulent en boucles et sont multipliées. Les trames n'ayant pas de durée de vie (TTL comme les paquets IP), elles peuvent tourner indéfiniment.
- Une instabilité des tables MAC : quand une trame, même unicast, parvient aux commutateurs connectés en redondance, le port du commutateur associé à l'origine risque d'être erroné. Une boucle est susceptible d'être créée.



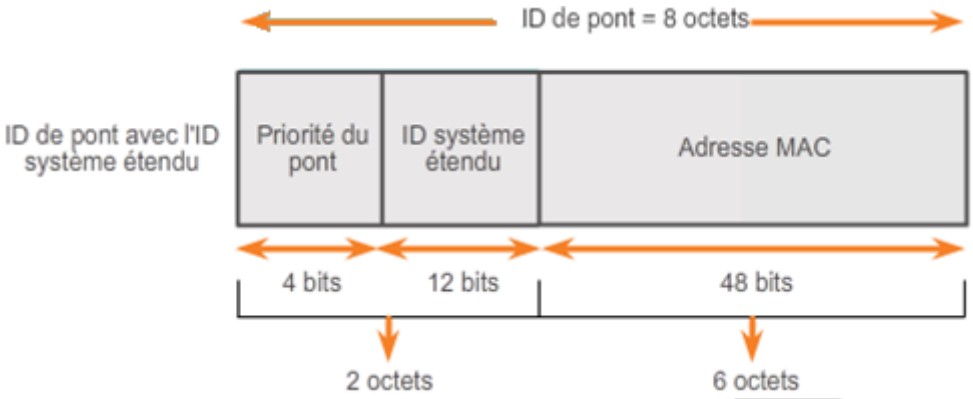
2. Fonctionnement du protocole Spanning-Tree

2.1 Algorithme Spanning Tree

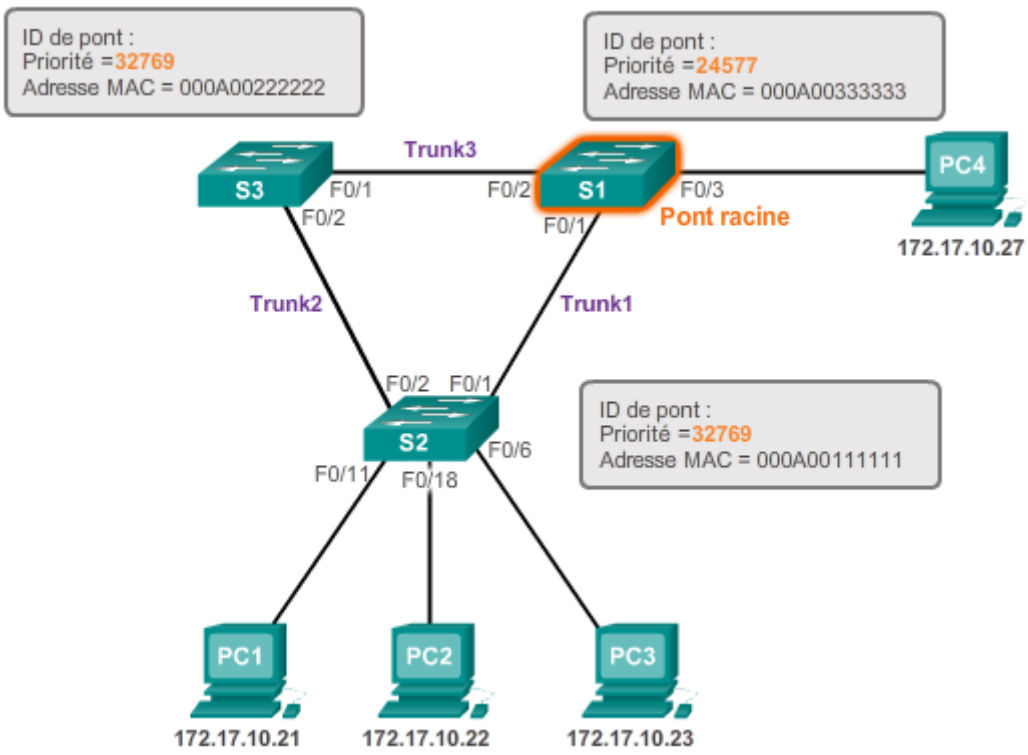
- STP (Spanning-Tree Protocol) repose sur un algorithme appelé STA (Spanning-Tree Algorithm) et qui est inventé par **Radia Perlman**.
- STA crée une topologie sans boucle en sélectionnant un **pont racine** unique où tous les autres commutateurs déterminent un seul chemin **moins coûteux**.
- À l'aide de l'algorithme STA, le protocole STP crée une **topologie sans boucle** en quatre étapes :
  1. Choisir le **pont racine**
  2. Déterminer les **ports racines**
  3. Déterminer les **ports désignés**
  4. Déterminer les **ports alternatifs**.

2.2 Choisir le pont racine

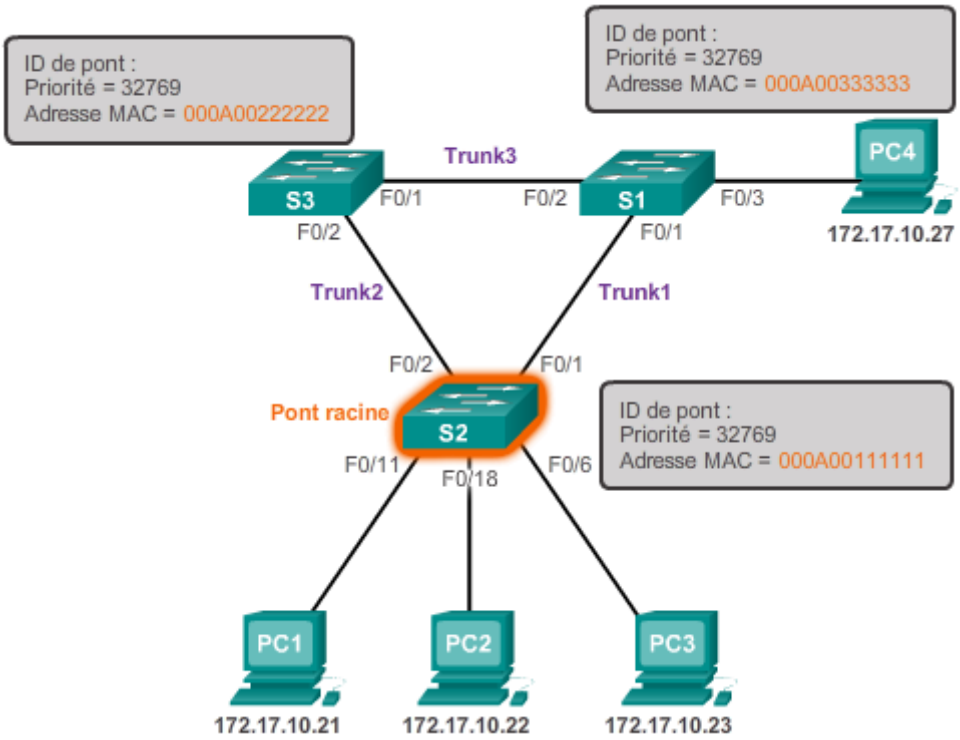
- Pont racine = Commutateur racine = **Root Bridge** (en anglais).
- Le **pont racine** sert de point de référence pour tous les calculs de l'algorithme STA afin de déterminer les chemins d'accès redondants devant être bloqués.
- Un processus d'élection détermine le commutateur qui devient le pont racine.
- Le commutateur qui présente l'**ID de pont (BID = Bridge ID) le plus bas devient le pont racine**.
- Le BID est composé d'une **valeur de priorité de pont**, d'un **ID système étendu** et de **l'adresse MAC du commutateur**.



- La valeur de priorité peut aller **de 0 à 61440**, par **incrément de 4096**, avec une valeur par défaut de **32768**.
- Tous les commutateurs du domaine de diffusion participent au processus d'élection du pont racine en envoyant des **trames BPDU** (Bridge Protocol Data Unit).
- **Remarque :** Les BPDU sont échangées régulièrement (toutes les 02 secondes) et permettent aux commutateurs de garder une trace des changements sur le réseau afin d'activer ou désactiver les ports requis.
- Depuis l'existence des VLAN, la priorité est codée sur **4 bits** (Avant l'apparition des VLAN, la priorité était codée sur 16 bits) auquel on ajoute **12 bits** pour l'identifiant du VLAN sur lequel se construit le Spanning Tree (la priorité ne peut donc prendre que des valeurs multiples de 2^{12}=4096).
- Exemple 01 **:** sélection du pont racine reposant sur la priorité



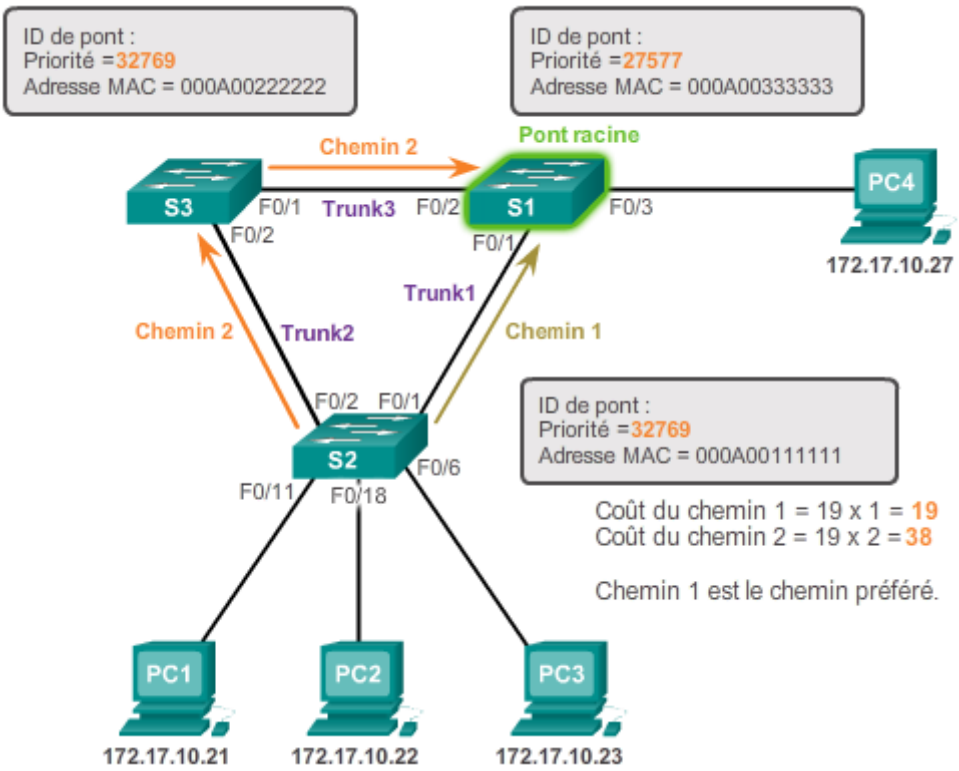
- Exemple 02 : sélection du pont racine reposant sur l'adresse MAC



2.3 Déterminer les ports racines

- Lorsque le pont racine a été choisi, l'algorithme STA lance le processus de détermination des meilleurs chemins possibles vers le pont racine, depuis l'ensemble des destinations du domaine de diffusion.
- Les commutateurs non-root vont sélectionner **un seul port racine** (**Root Port**) qui aura **le chemin le plus court vers le commutateur racine (c'est-à-dire le coût le moins élevé)**.
- Un port racine est en état **Forwarding** (**FWD**).
- Voici les coûts par défaut des ports du commutateur selon l'algorithme STA :

Vitesse de liaison	Coût par défaut
10 Gbps	2
1 Gbps	4
100 Mbps	19
16 Mbps	62
10 Mbps	100
4 Mbps	250



- Il est ainsi possible de modifier les couts par défaut des ports :

Si le port F0/1 est configuré en mode Access (qui connecte un périphérique terminal).	S1(config) # **int F0/1** S1(config-if) # **spanning-tree cost** *valeur*
Si le port F0/1 est configuré en mode Trunk (qui connecte un autre commutateur).	S1(config) # **int F0/1** S1(config-if) # **spanning-tree vlan** *vlan-id* **cost** *valeur*

- **Remarque :** Sur un commutateur non-Root, pour des interfaces STP en cas de coûts égaux vers le commutateur Root, c'est leur priorité la plus faible (d'une valeur de 0 à 255) qui emporte le choix du port Root (elle est de 128 par défaut) en déterminant l'ID du port composé de deux octets (priorité + numéro STP du port) :

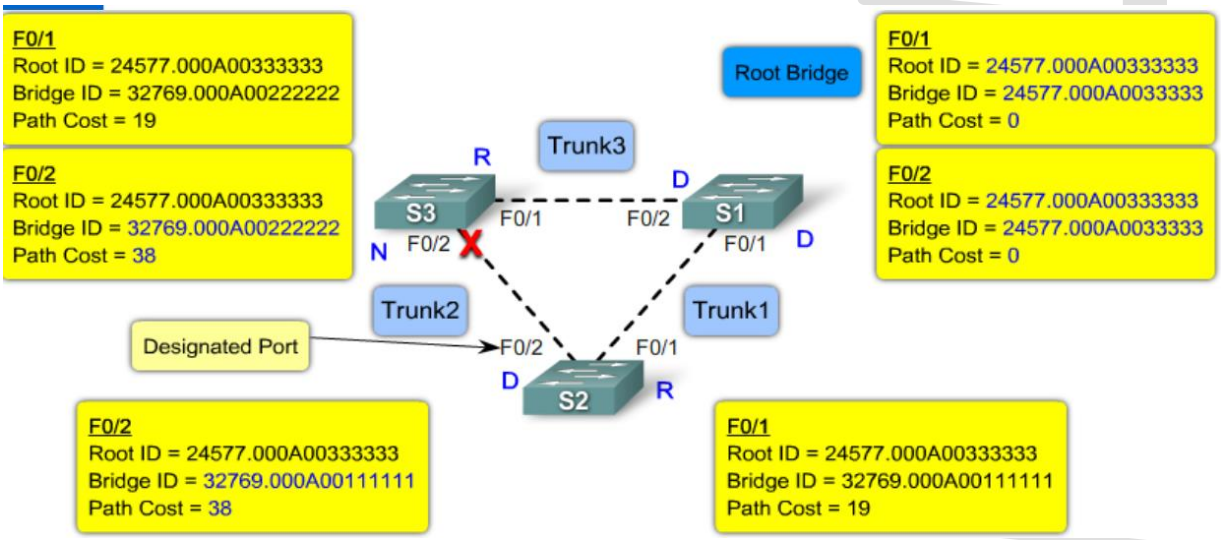
Sur un port en mode Access	S1(config-if) # **spanning-tree port-priority** *priority*
Si un port en mode Trunk	S1(config-if) # **spanning-tree vlan** *vlan-id* **port-priority** *priority*

2.4 Déterminer les ports désignés

- Pour chaque segment physique, domaine de collision ou lien, il y a un **port Désigné** (Designated Port).
- Un port désigné est en état **Forwarding** (**FWD**).
- Le port désigné est le port qui a le chemin le plus court (c'est-à-dire le **coût faible**) vers le pont root.

2.5 Déterminer les ports alternatifs

- Tous les autres ports (autres que les ports racines et les ports désignés) sont des ports alternatifs.
- Un port alternatif est en état **blocking** (**BLK**) ; c'est-à-dire **bloquant tout trafic de données mais restant à l'écoute des BPDU**.
- Dans l'exemple suivant, le port F0/2 de S3 est un port alternatif.



2.6 Etats des ports sur les commutateurs en STP

- Pendant le processus de fabrication de l'arbre recouvrant via le protocole STP, un port du commutateur passe par plusieurs états.
- Un port démarre en état **Blocking** et peut atteindre l'état **Forwarding** en fonction des BPDUs reçus.
- L'état **Disabled** est une désactivation administrative du port ou fait suite à une erreur de sécurité.

Blocking	- Le port est un port alternatif (non-designated). - Le port ne participe pas au réacheminement des trames de données. - Le port reçoit des trames BPDU - Reste dans cet état pendant **20 secondes max**.
Listening	- Le port participe au réacheminement des trames, en fonction des trames BPDU reçues. - Le port reçoit non seulement les trames BPDU, mais transmet également ses propres trames BPDU et informe les commutateurs adjacents qu'il se prépare à participer à la topologie active. - Reste dans cet état pendant **15 secondes max**.
Learning	- Le port ne réachemine toujours pas les trames mais apprend les @MAC sources contenues dans celles-ci pour remplir sa table d'@MAC.
Forwarding	- Le port est considéré comme faisant partie intégrante de la topologie active. - Le port réachemine les trames de données, et envoie et reçoit les trames BPDU.

3. Versions du protocole Spanning-Tree

3.1. Variantes STP

- Plusieurs protocoles Spanning Tree sont apparus depuis sa première création :

STP	Ancienne norme du Spannning Tree.
PVST+	Version améliorée du STP proposée par Cisco.
802.1D	Version mise à jour du protocole STP standard, intégrant IEEE 802.1w
RSTP	Version évoluée du protocole STP, qui offre une convergence plus rapide.
Rapid PVST+	Version améliorée du protocole RSTP proposée par Cisco et utilisant PVST+.
MSTP	Mappe plusieurs VLAN dans une même instance Spanning Tree.

- Voici une comparaison entre les différentes variantes STP :

Protocole	Norme	Ressources nécessaires	Convergence	Calcul d'arborescence
STP	802.1D	Faible	Lente	Tous les VLAN
PVST+	Cisco	Élevée	Lente	Par VLAN
RSTP	802.1w	Moyenne	Rapide	Tous les VLAN
Rapid PVST+	Cisco	Très élevée	Rapide	Par VLAN
MSTP	802.1s, Cisco	Moyenne ou élevée	Rapide	Par instance

3.2. Configuration STP par défaut sur les commutateurs Cisco

Fonctionnalité	Paramètre par défaut
État activé	Activé sur VLAN 1
Protocole du spanning-tree	PVST+ (Rapid PVST+ et MSTP sont désactivés)
Priorité du commutateur	32768
Priorité des ports en Spanning Tree	128
Coût des ports en Spanning Tree	1 Gbps : 4 100 Mbps : 19 10 Mbps : 100

2.7 Vérification des paramètres STP sur les commutateurs Cisco

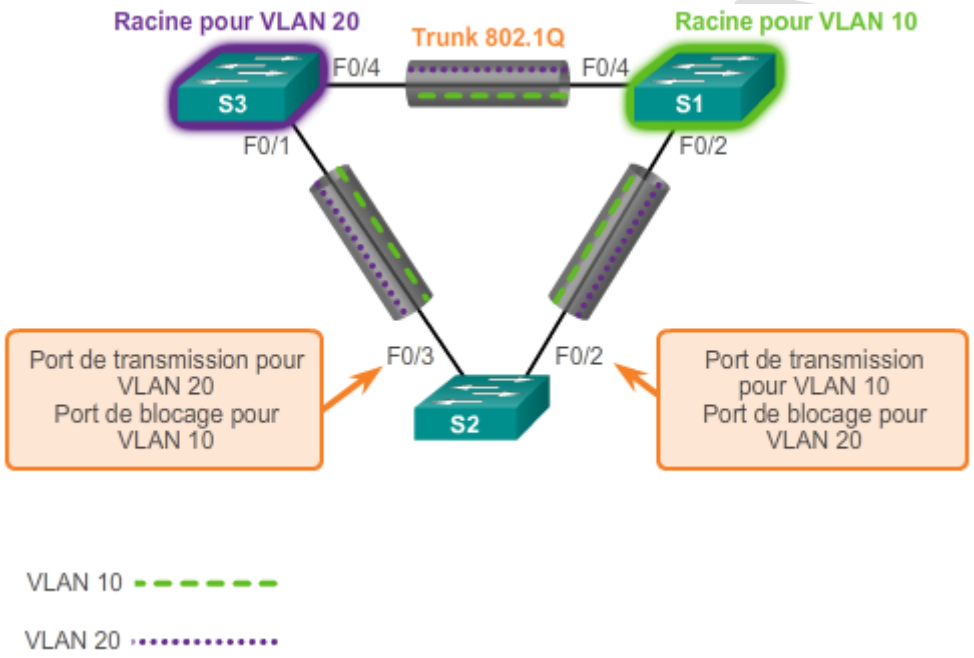
Vérifier les paramètres STP pour l'ensemble des VLAN	**show spanning-tree**
Vérifier les paramètres STP pour un VLAN en particulier (exemple VLAN1)	**show spanning-tree vlan1**

4. Protocole PVST+

4.1. Présentation de PVST+

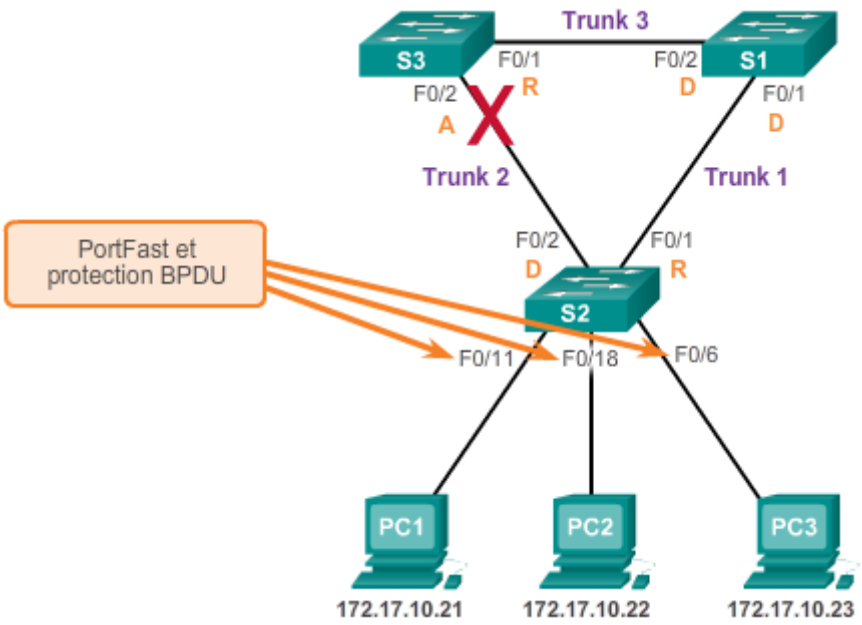
- Protocole propriétaire Cisco.
- Un port trunk peut être en état **blocking** pour un VLAN donné et en **Forwarding** pour les autres VLAN.
- Un commutateur donné peut même être un **pont racine** (Root Bridge) pour un VLAN alors qu'un autre commutateur peut l'être pour un autre VLAN.
- Un équilibrage optimal de la charge de couche 2 peut être atteint.
- Le BID sur le PVST+ intègre le système étendu (c'est-à-dire le numéro de VLAN).
- Pour choisir le mode STP (PVST ou Rapid PVST) sur un commutateur Cisco :

```
S1(config)#spanning-tree mode pvst
```



4.2. PortFast et protection BPDU

- **PortFast** est une fonction Cisco destinée aux environnements PVST+.
- La fonction PortFast permet à un port de passer de l'état de blocage à l'état de réacheminement immédiatement, sans passer par les autres états STP habituels (écoute et apprentissage). Donc, minimiser le temps d'attente des ports d'accès avant la convergence Spanning Tree.
- **Remarque :** la fonction PortFast doit être utilisée uniquement sur les ports d'accès. Si PortFast est activée sur un port connecté à un autre commutateur (port trunk), une boucle Spanning Tree risque d'être créé.
- **Remarque :** Dans une configuration PortFast valide, les trames BPDU ne doivent jamais être reçues, car cela indiquerait qu'un autre pont ou commutateur est connecté au port, avec pour conséquence potentielle une boucle Spanning Tree.



- Voici les commandes de configuration et vérification de PortFast et de Protection BPDU :

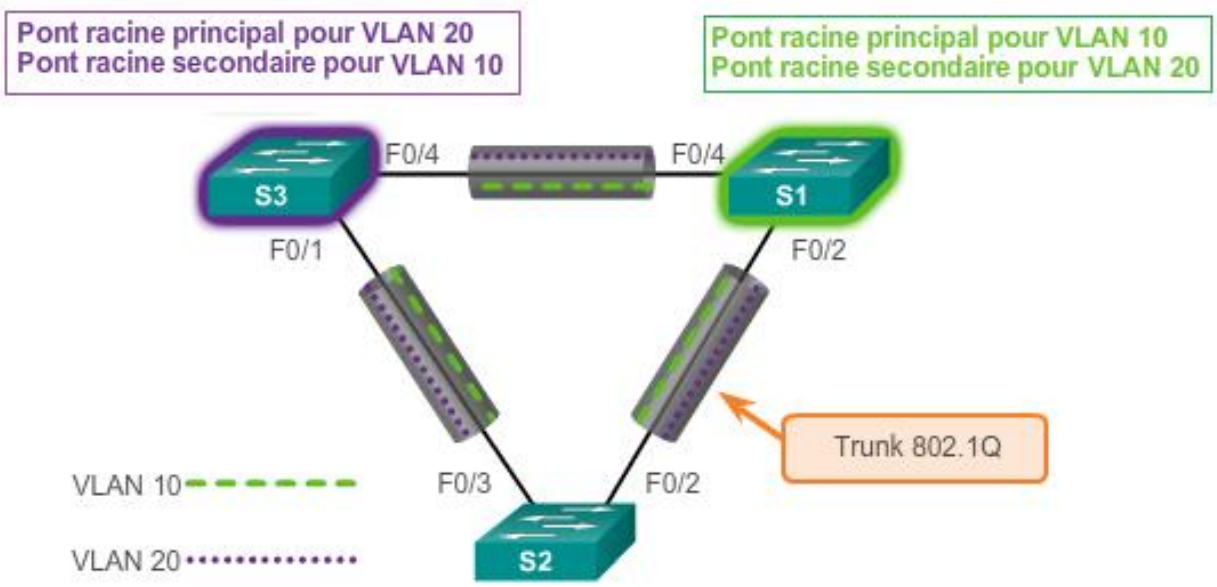
Activer PortFast sur un port de commutation.	S1(config-if) # **spanning-tree portfast**
Désactiver PortFast sur un port.	S1(config-if) # **spanning-tree portfast disable**
Activer PortFast sur toutes les interfaces de non-agrégation.	S1(config-if) # **spanning-tree portfast default**
Activer la protection BPDU sur un port d'accès.	S1(config-if) # **spanning-tree bpduguard enable**
Désactiver la protection BPDU sur un port d'accès.	S1(config-if) # **spanning-tree bpduguard disable**
Activer la protection BPDU sur tous les ports où PortFast est activée.	S1(config-if) # **spanning-tree bpduguard enable**
Vérifier la configuration de PortFast et de protection BPDU.	S1# **show running-conf**

4.3. Equilibrage de charge et tolérance de panne sous PVST+

- Il est possible de configurer un pont racine secondaire autre que le pont racine principal.
- **Pont racine secondaire** = un commutateur qui peut devenir un pont racine d'un VLAN en cas de défaillance du pont racine principal.
- Étapes de configuration de ponts racines principal et secondaire :

Étape 1 : identifier les commutateurs qui seront des pont racine principal et secondaire pour chaque VLAN.
Étape 2 : configurer le pont racine principal pour le VLAN avec **spanning-tree vlan** *num* **root primary**
Étape 3 : configurer le pont racine secondaire pour le VLAN avec **spanning-tree vlan** *num* **root secondary**

- Exemple de configuration des ponts racines principale et secondaire :



S3(config)# **spanning-tree vlan 20 root primary** S3(config)# **spanning-tree vlan 10 root secondary**	S1(config)# **spanning-tree vlan 10 root primary** S1(config)# **spanning-tree vlan 20 root secondary**

- **Remarque :** Une autre méthode pour définir le pont racine consiste à configurer la priorité Spanning Tree de chaque commutateur, en spécifiant la valeur la plus basse, de manière à ce que le commutateur soit sélectionné en tant que pont principal pour le VLAN associé.

Définir la priorité de S3 avec la plus basse valeur possible pour le VLAN 20. Le commutateur S3 sera donc le pont racine principal pour VLAN 20.	S3(config)# **spanning-tree vlan 20 priority 4096**
Définir la priorité de S1 avec la plus basse valeur possible pour le VLAN 10. Le commutateur S1 sera donc le pont racine principale pour VLAN 10.	S1(config)# **spanning-tree vlan 10 priority 4096**

5. Rapid PVST+

5.1. Présentation de Rapid PVST+

- **Rapid PVST+** est l'implémentation Cisco du protocole RSTP.
- Le protocole Rapid PVST+ est une version améliorée du protocole PVST+.
- Rapid PVST+ permet d'accélérer les calculs de l'algorithme STA et la convergence en réponse à des modifications de la topologie de couche 2.
- Rapid PVST+ fournit de multiples améliorations pour optimiser les performances réseau.

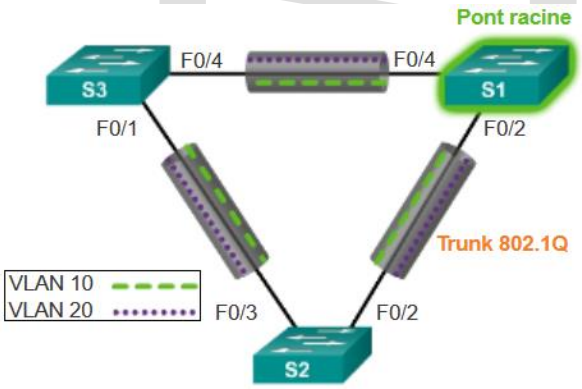
5.2. Configuration de Rapid PVST+

- Voici les commandes de configuration du protocole Rapid PVST+ :

Choisir le mode Rapid PVST+	**spanning-tree mode rapid-pvst**
Spécifier une interface à configurer. Les interfaces autorisées comprennent les ports physiques, les VLAN et les canaux de port. La plage d'ID de VLAN s'étend de 1 à 4094 lorsque l'image logicielle améliorée est installée, et de 1 à 1005 avec l'image logicielle standard. La plage port-channel est comprise entre 1 et 6.	**Interface** *interface-id*
Spécifier que le type de liaison pour ce port est point à point.	**spanning-tree link-type point-to-point**
Désactiver tous protocoles STP détectés.	**Clear spanning-tree detected-protocols**

- Exemple de configuration de Rapid PVST+ sur le commutateur S1 :

```
S1# configure terminal
S1(config)# spanning-tree mode rapid-pvst
S1(config)# interface f0/2
S1(config-if)# spanning-tree link-type point-to-point
S1(config-if)# end
S1# clear spanning-tree detected-protocols
```



- **Remarque** : en général, il n'est pas nécessaire de configurer le paramètre de **type de liaison point à point** pour Rapid PVST+, car il est rare d'avoir un **type de lien partagé**. Dans la plupart des cas, la seule différence entre la configuration de PVST+ et celle de Rapid PVST+ est la commande **spanning-tree mode rapid-pvst**.