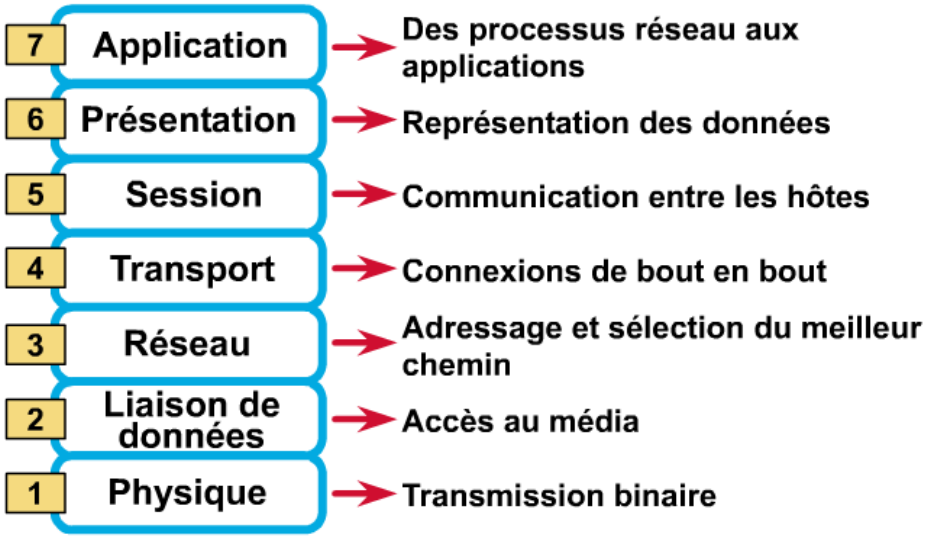
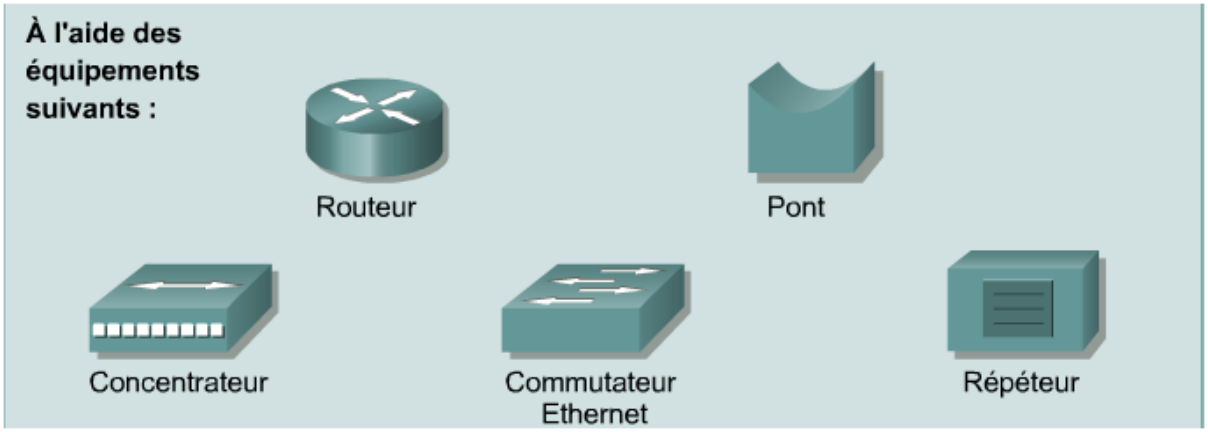
Commutation – VLAN – Spanning Tree

I. GENERALITES

1. Les équipements d'interconnexion de réseaux.

Afin de mieux appréhender les notions présentées dans ce document, il est nécessaire d'identifier les différents éléments d'interconnexion de réseaux et leur positionnement dans le modèle OSI





OSI 1 OSI 3

OSI 2 OSI 2

OSI 1

Au niveau 1 :

- Un répéteur reçoit un signal, le régénère et le transmet sur tous ses ports, sauf celui qui a reçu le signal.

- Les concentrateurs (Hub) sont, en fait, des répéteurs multiports. La différence entre un concentrateur et un répéteur réside dans le nombre de ports respectifs de ces équipements. Un répéteur classique possède généralement deux ports et un concentrateur entre 4 et 24 ports. Les équipements raccordés à un concentrateur reçoivent tout le trafic qui traverse le concentrateur.

Au niveau 2 :

- Un pont doit prendre des décisions intelligentes quant à la transmission ou non des signaux au segment suivant d'un réseau. Lorsqu'un pont reçoit une trame sur le réseau, il recherche l'adresse MAC de destination dans une table spécifique afin de déterminer s'il doit filtrer la trame, la diffuser ou la copier sur un autre segment :
  - Si l'équipement de destination se trouve sur le même segment que la trame, le pont n'envoie pas la trame vers d'autres segments. Ce processus correspond au «filtrage».
  - Si l'équipement de destination se trouve sur un autre segment, le pont transmet la trame au segment approprié.
  - Si le pont ne connaît pas l'adresse de destination, il transmet la trame à tous les segments, excepté à celui par lequel la trame a été reçue. Ce processus correspond à la «diffusion».

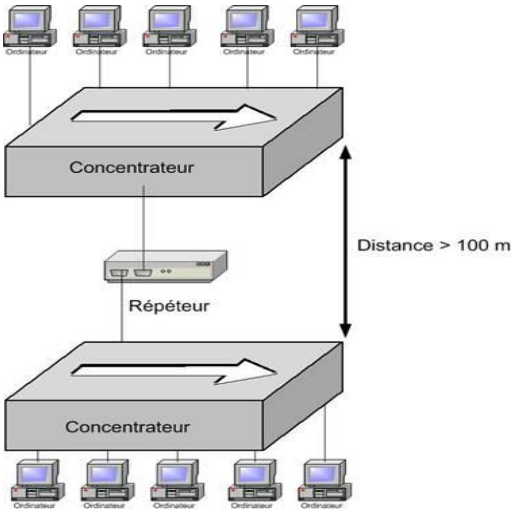
- Les commutateurs sont parfois qualifiés de «ponts multiports». A l'instar des ponts, les commutateurs recherchent des informations sur les trames de données qu'ils reçoivent de la part des ordinateurs du réseau. Ils se servent ensuite de ces informations pour créer des tables et déterminer la destination des données que s'envoient les ordinateurs sur le réseau.

Au niveau 3 :

- Les deux principales fonctions des routeurs sont la sélection des meilleurs chemins pour les paquets de données entrants et la commutation des paquets vers l'interface de sortie appropriée. Pour ce faire, les routeurs créent des tables de routage et échangent des informations sur le réseau avec d'autres routeurs.

2. La segmentation.

2.1. Domaine de collision.

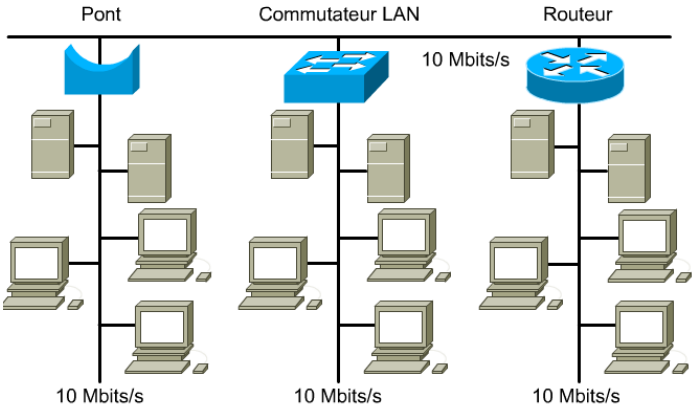


Un domaine de collision est une région du réseau au sein de laquelle les hôtes partagent l'accès au média. Autrement dit, les nœuds (ordinateurs et équipements actifs) utilisent le même tuyau pour transmettre les données. Lorsqu'une station effectue une transmission, tous les autres équipements la reçoivent. De plus, personne ne peut émettre pendant ce temps.

Une collision survient lorsqu'une station cherche à émettre alors qu'une autre est déjà en train d'émettre.

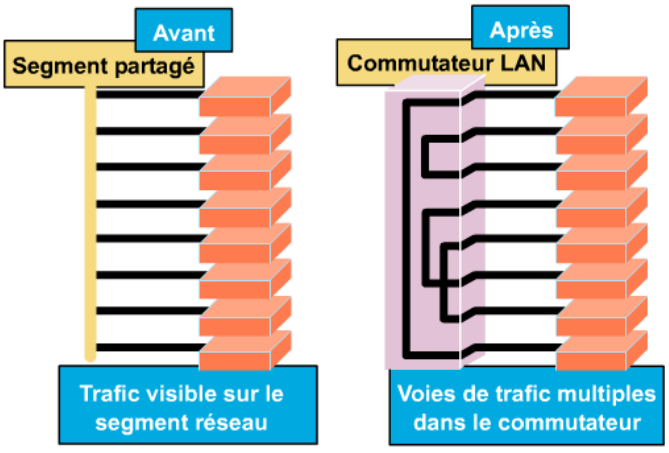
Les équipements de couche 1 (répéteurs et concentrateurs) transmettent la totalité des données qui sont reçues sur un port vers les autres ports, ce qui augmente considérablement le domaine de collision.

2.1. Segmentation du domaine de collision.



Les ponts et les commutateurs (couche n°2) permettent de segmenter un réseau en se basant sur les adresses MAC des hôtes. Ils entretiennent un table de pontage ou de commutation qui va permettre d'assurer la cohésion adresse MAC / port de commutateur ou de pont.

De cette façon, une trame n'est pas retransmise sur tous les ports mais seulement vers celui de destination. Ainsi, un commutateur permet la communication simultanée sans collision, comme présenté dans le schéma ci-dessous.



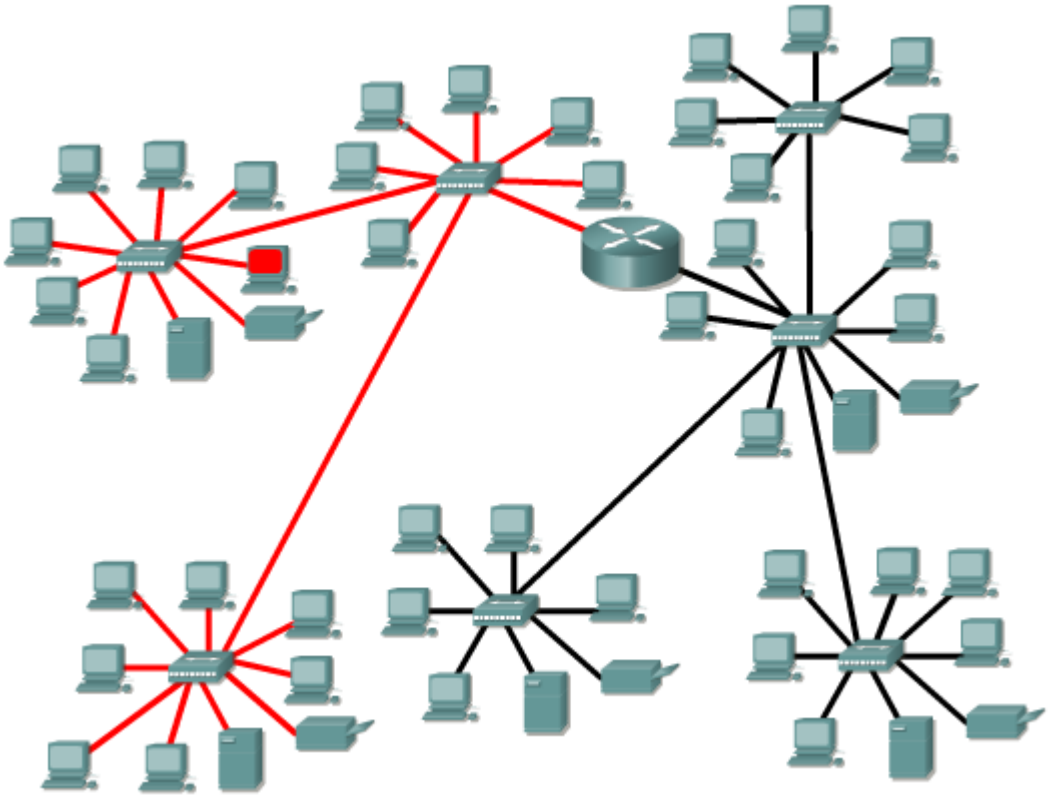
2.1. Domaine de diffusion (broadcast).

Lorsqu'une station doit communiquer avec tous les hôtes du réseau, elle envoie une trame de broadcast avec une adresse MAC de destination 0xFFFFFFFFFFFF. La carte réseau de chaque hôte doit alors envoyer une réponse à cette adresse.

Les équipements de couche 2 doivent diffuser la totalité du trafic de broadcasts et de multicast. L'accumulation du trafic de broadcast de chaque équipement du réseau s'appelle le **rayonnement de diffusion** (*broadcast radiation*). Il arrive alors que le réseau soit saturé au point que les données d'application ne disposent plus d'une bande passante suffisante.

Les résultats démontrent clairement que les broadcasts diffusés sur le réseau peuvent entraîner l'arrêt de la station de travail.

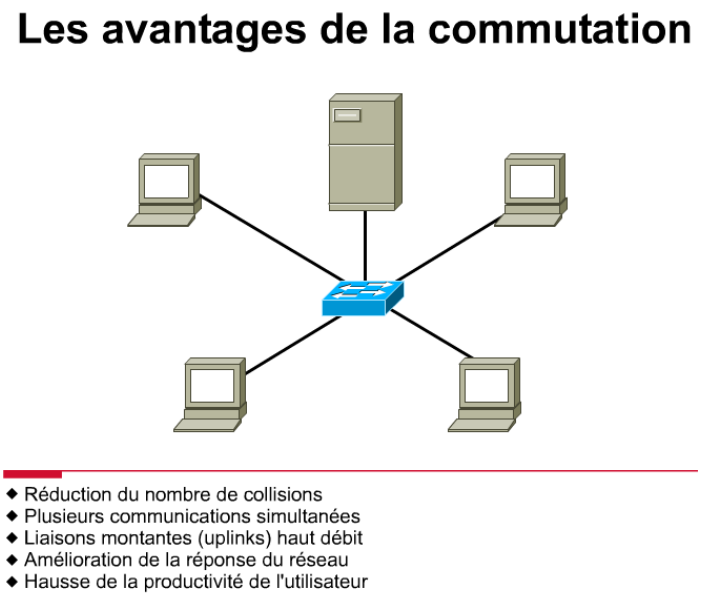
La seule façon de segmenter un domaine de broadcast est d'utiliser des équipements de niveau 3 (routeurs). Ceux-ci vont bloquer ces trames car ils connaissent déjà le chemin à emprunter pour joindre l'hôte recherché (en fonction de son l'adresse IP).



L'utilisation de commutateurs et des VLAN vont permettre de résoudre une partie des problèmes liés aux domaines de diffusion et aux domaines de collision.

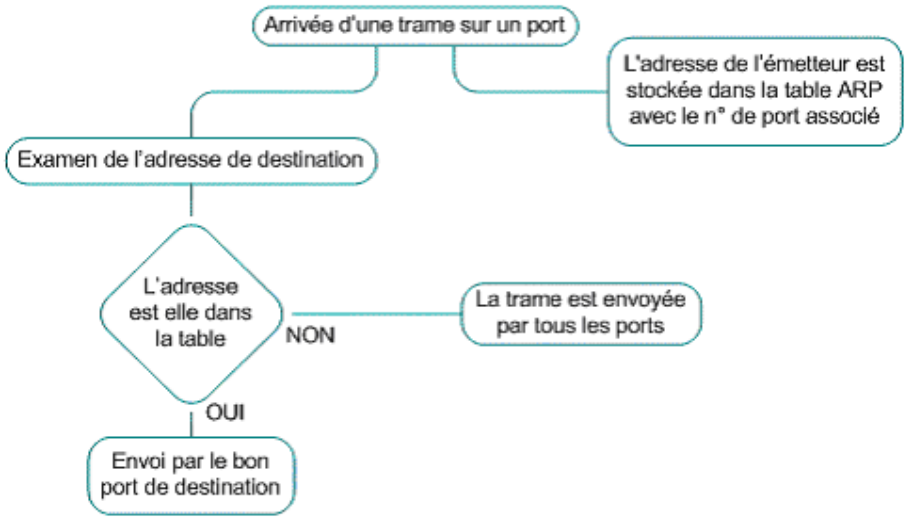
II. LES COMMUTATEURS.

Les commutateurs présentent de nombreux avantages. Un commutateur LAN permet à de nombreux utilisateurs de communiquer en parallèle, grâce à l'utilisation de circuits virtuels et de segments réseau spécialisés, dans un environnement exempt de toute collision. Cela optimise la bande passante disponible sur le média partagé. De plus, passer à un environnement LAN commuté se révèle particulièrement économique, dans la mesure où le matériel informatique et le câblage peuvent être réutilisés. Enfin, la puissance du commutateur alliée au logiciel pour configurer des LAN offrent aux administrateurs réseau une grande souplesse de gestion.



1. Fonctionnement du commutateur.

Les décisions d'acheminement du commutateur sont basées sur les adresses MAC contenues dans les trames circulant sur le réseau :



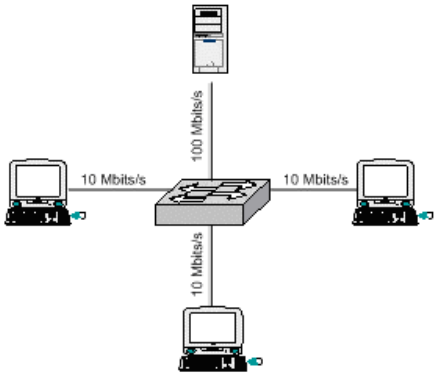
À chaque fois qu'une adresse est stockée, elle est horodatée. Cela permet de stocker les adresses pendant une période déterminée. À chaque fois qu'une adresse est référencée ou trouvée dans la mémoire associative, elle est de nouveau horodatée. Les adresses qui ne sont pas consultées durant une période déterminée sont éliminées de la liste. L'élimination des adresses obsolètes ou périmées permet à la mémoire associative de conserver une base de données d'acheminement précise et fonctionnelle.

Comme présenté au chapitre « Domaine de collision », un commutateur peut assurer la communication simultanée, sans collision entre plusieurs couples de machines. On nomme cette technique la « micro segmentation ».

2. Commutation symétrique / asymétrique.

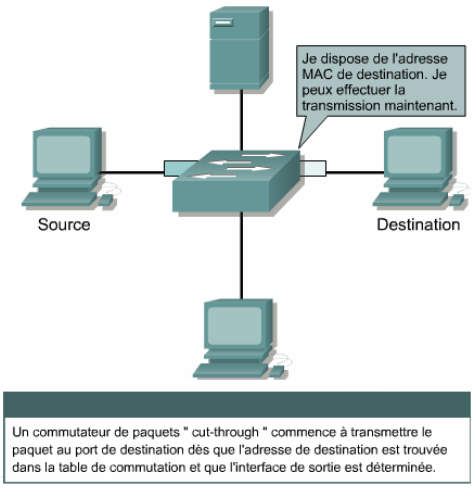
La commutation peut aussi être caractérisée en fonction de la bande passante attribuée à chaque port :

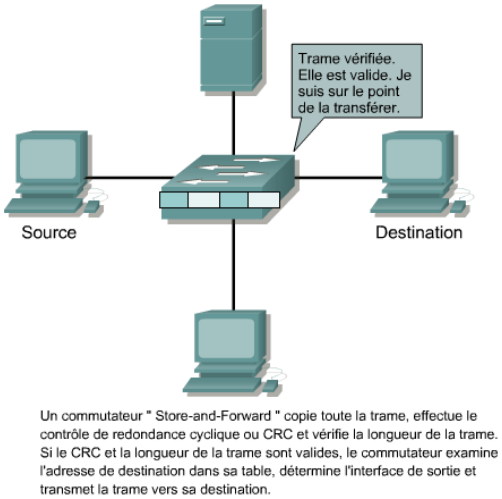
- *Commutation symétrique* : Les connexions commutées offre la même bande passante à chaque port.
- *Commutation asymétrique* : Les connexions commutées offrent des bandes passantes différentes.



3. Deux modes de commutation.

La commutation d'une trame vers un port de destination est fonction du niveau de latence et de fiabilité. Un commutateur peut commencer à transférer la trame dès que l'adresse MAC est reçue. Ce mode de commutation des paquets est appelé «Cut-through» : il se caractérise par un temps de latence très faible. Cependant, la vérification des erreurs n'est pas effectuée.
Un commutateur peut également attendre de recevoir la trame entière avant de la transférer vers le port de destination. Cela permet au logiciel de commutation de vérifier la séquence de contrôle de trame (FCS, *Frame Check Sequence*). Étant donné que la trame entière est stockée avant d'être transmise, ce mode de commutation des paquets est appelé «Store-and-Forward».





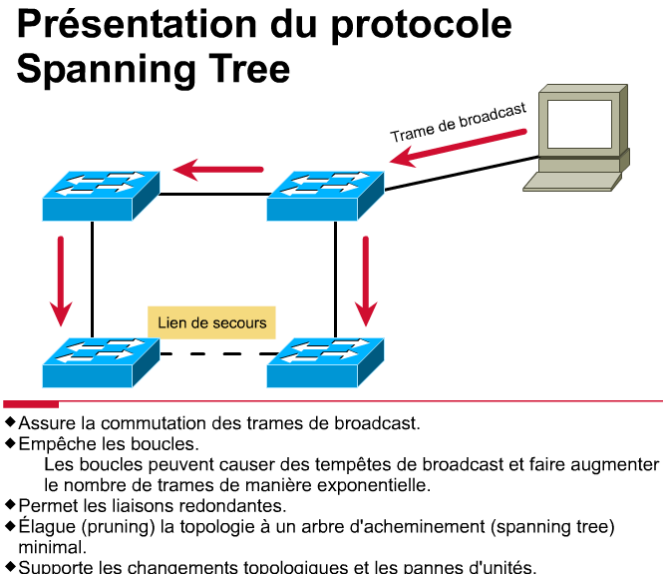
4. Spanning Tree Protocol (SPT).

Dans un réseau où se trouvent plusieurs commutateurs, il est possible, voire souhaitable de réaliser des liens redondants. Bien qu'extrêmement utiles, les chemins redondants peuvent avoir des effets secondaires, tels que les boucles de commutation. Ces boucles de commutation représentent un inconvénient. Elles peuvent survenir intentionnellement ou accidentellement et elles peuvent provoquer des tempêtes de broadcasts qui risquent de submerger rapidement le réseau.

L'algorithme Spanning Tree calcule une topologie « stable » ; c'est-à-dire un réseau exempt de boucle entre tous les noeuds du réseau. En cas de défaillance du lien principal, le commutateur « remet en fonctionnement » le lien de secours.

Les trames Spanning Tree, appelées unités BPDU, sont envoyées et reçues à intervalles réguliers par tous les commutateurs d'un réseau.

La norme associée est référencée 802.1d.

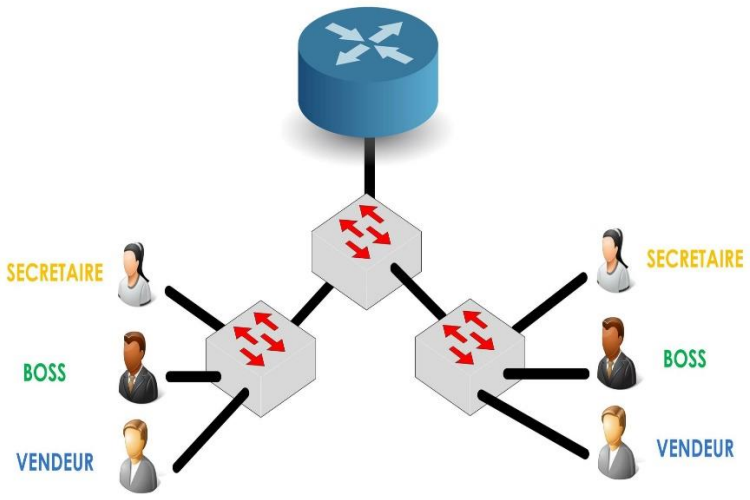


III. VLAN (Virtual LAN)

Mise en situation.

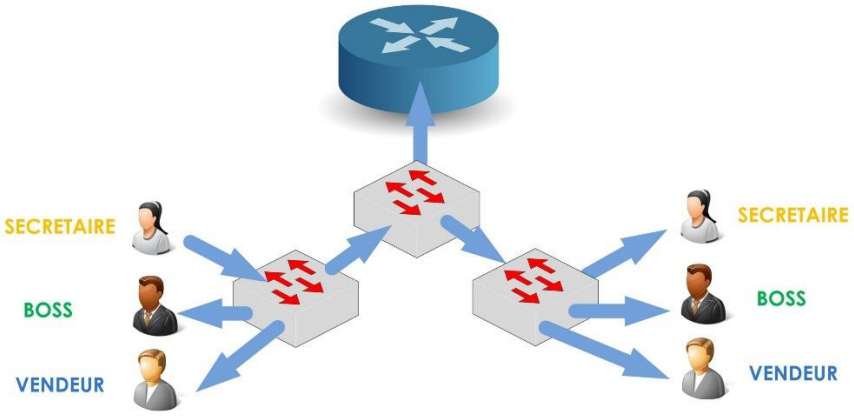
Vous pouvez voir ci-dessous un réseau d'entreprise standard. Ce réseau comprend :

- **10 Boss** *(Plage d'adresse IP : 192.168.10.0 /24)*
- **50 Secrétaires / Comptable** *(Plage d'adresse IP : 192.168.20.0 /24)*
- **200 Vendeurs** *(Plage d'adresse IP : 192.168.30.0 /24)*



Un réseau d'entreprise standard

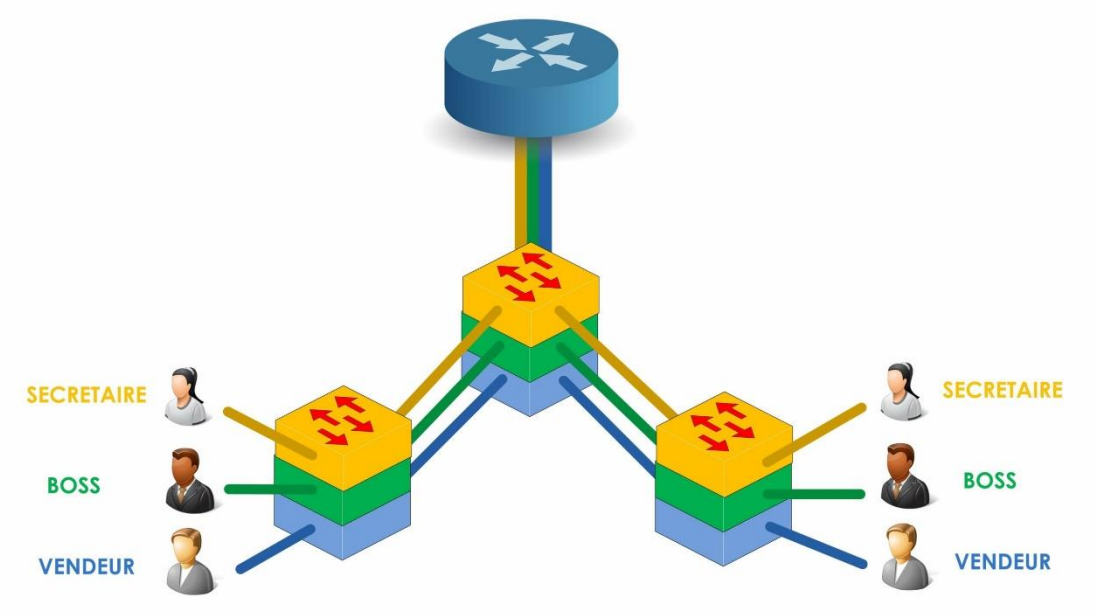
Si un de nos ordinateurs émet un broadcast ARP, il sera diffusé sur TOUS les ports de notre réseau ! Tous nos postes vont émettre des broadcasts pour fonctionner, notre réseau va très vite être pollué !



Un broadcast circule sur tous les ports de l'entreprise

Comment diminuer le nombre de broadcasts qui circule sur le réseau ?

- Enlever des postes ? **Impossible**
- Créer un réseau par groupe de travail ? **Oui**



La solution : créer un réseau par groupe d'utilisateur

Résultat :

- Le réseau **Boss** *(10 users) = Diminution du nombre de broadcasts reçu de* ***96,2%***
- Le réseau **Secrétaire** *(50 users) =Diminution du nombre de broadcasts reçu de* ***80,8%***
- Le réseau **Vendeurs** *(200 users) = Diminution du nombre de broadcasts reçu de* ***23,1%***

Points négatifs :

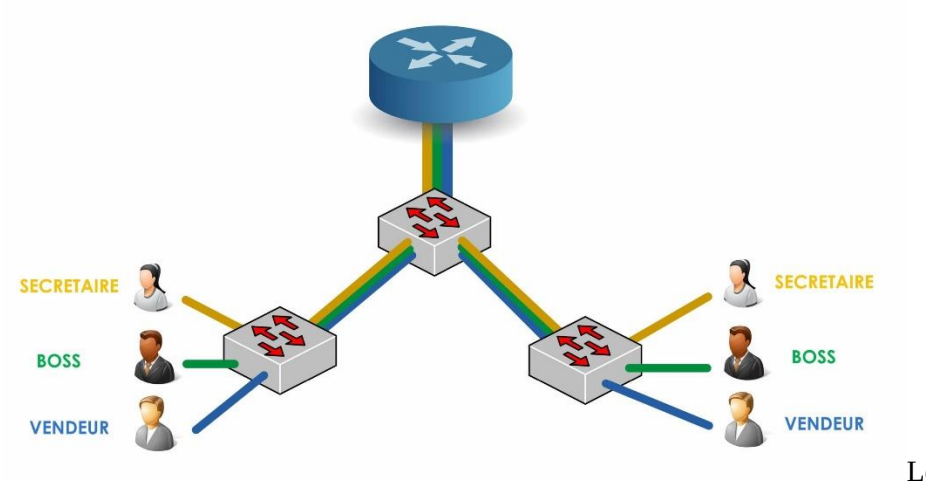
- Ça coûte super cher cette méthode !!!!!!!

Comment faire ?

- Trouver une solution pour créer ce type d'architecture avec peu de matériel !!

La solution trouvée :

- les Virtual LAN *(VLAN)*



Les Virtual LAN

1.1.1. Avantages

Avantage principal :

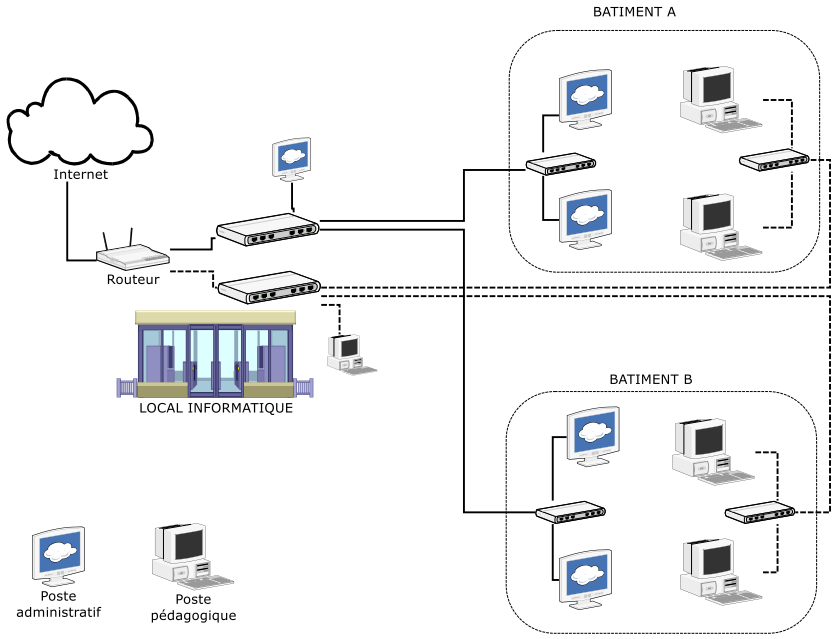
- Réduire le domaine de broadcast.

Avantages secondaires :

- Améliorer la **gestion du réseau**.
- Optimiser la **bande passante**.
- **Séparer les flux**.

Autre exemple :
Dans une entreprise ou une organisation administrative, il n'est pas rare que des machines géographiquement voisines ne fassent pas partie du même service / réseau. Par exemple, dans la salle des professeurs d'un lycée, on pourra trouver un ordinateur connecté au réseau pédagogique (pour la préparation des cours) et un ordinateur connecté au réseau administratif (pour la saisie des notes).

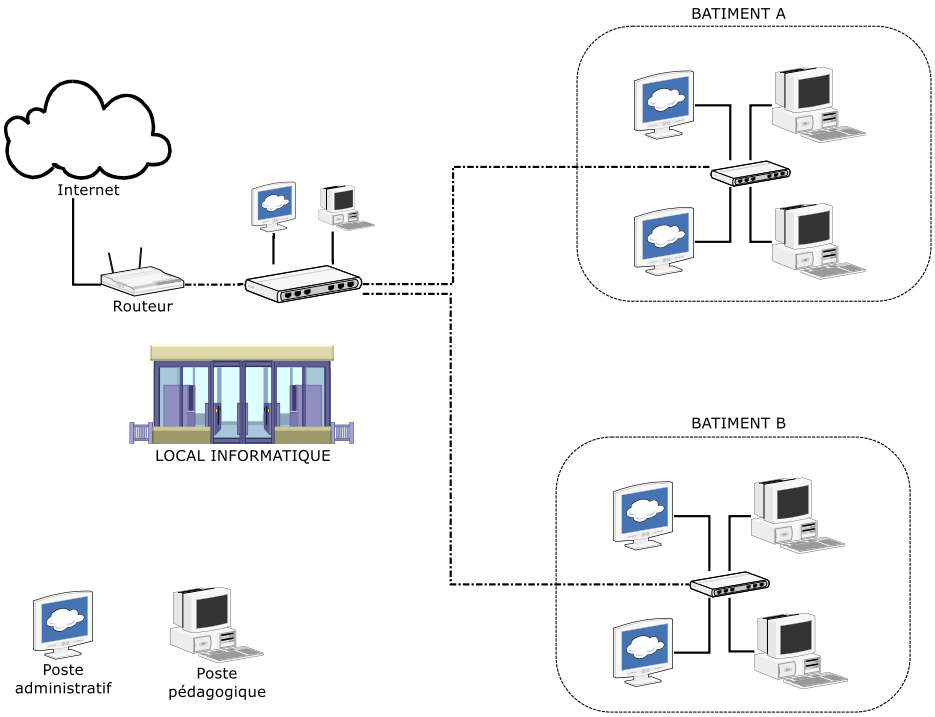
Ces ordinateurs ne doivent pas communiquer pour des questions de sécurité. Pour ce faire, il faut utiliser des matériels distincts : switchs, câbles, fibres. Bref, il faut tout en double, comme l'illustre le schéma ci-dessous.



Remarque : Le routeur représente le point potentiel d'interconnexion entre les deux réseaux. Cependant, les interfaces réseau étant différentes, la communication entre les deux sera impossible, sauf paramétrage spécifique.

Sur ce second schéma, tous les ordinateurs sont reliés aux mêmes équipements et utilisent les mêmes voies de transmission entre bâtiments. Pourtant, les ordinateurs pédagogiques et administratifs ne peuvent communiquer, malgré le fait qu'ils possèdent des IP compatibles.

Ceci est dû au fait que ce réseau utilise les **VLAN ou réseaux virtuels**.



Principe.

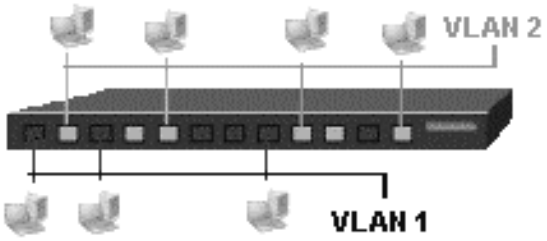
Un VLAN ou réseau virtuel est un regroupement de postes de travail indépendamment de la localisation géographique sur le réseau. Ces stations pourront communiquer comme si elles étaient sur le même segment. **Un VLAN est identifié par son VID** (numéro).

Dans le schéma ci-dessus, les postes du réseau administratif font partie d'un VLAN, les postes du réseau pédagogique font partie d'un autre VLAN, lesquels ne peuvent communiquer, sauf par le biais du routeur, s'il est programmé pour cela.

Différents types de VLAN.

1. VLAN par port.

Un VLAN par port, aussi appelé VLAN de niveau 1 (pour physique), est obtenu en associant chaque port du commutateur à un VLAN particulier. C'est une solution simple, qui a été rapidement mise en œuvre par les constructeurs.

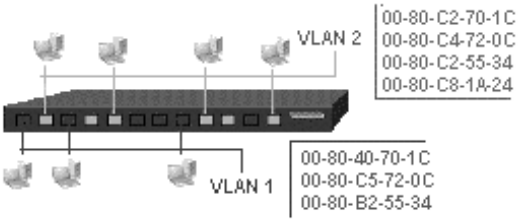


Les VLAN par port manquent de souplesse, tout déplacement d'une station nécessite une reconfiguration des ports. De plus, toutes les stations reliées sur un port par l'intermédiaire d'un même concentrateur, appartiennent au même VLAN.

2. VLAN par adresse MAC.

Un VLAN par adresse MAC, ou VLAN de niveau 2 est constitué en associant les adresses MAC des stations à chaque VLAN.

L'intérêt de ce type de VLAN est surtout l'indépendance de la localisation. La station peut être déplacée, son adresse physique ne changeant pas, il est inutile de reconfigurer le VLAN. Les VLAN configurable avec l'adresse MAC sont bien adaptés à l'utilisation de stations portables.



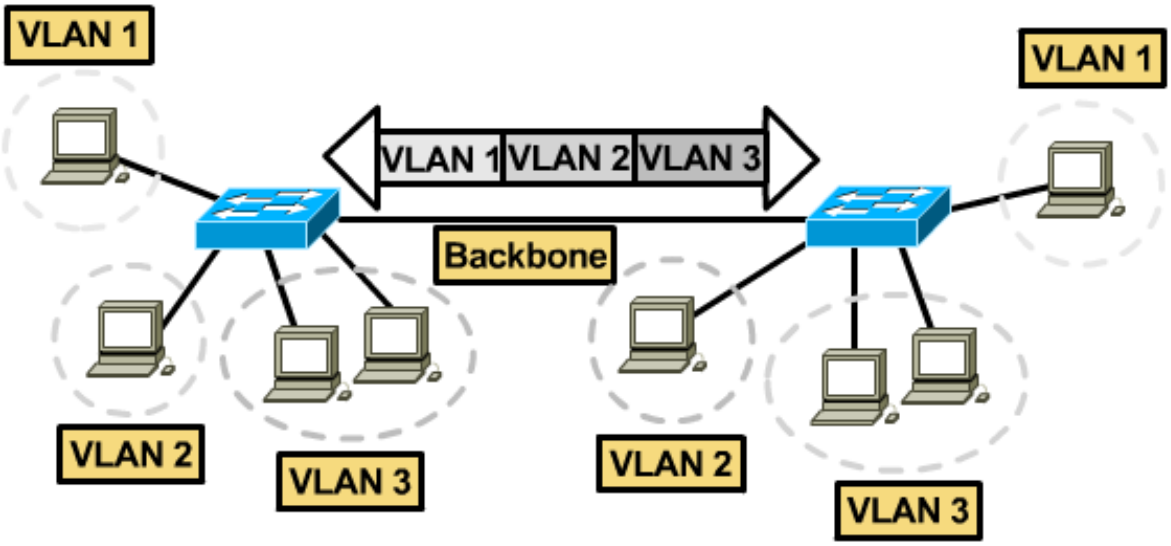
Cependant, la configuration peut s'avérer fastidieuse car elle nécessite de renseigner une table de correspondance avec toutes les adresses MAC et elle doit être partagée par tous les commutateurs.

3. VLAN par sous-réseau.

Également appelé VLAN de niveau 3, un VLAN par sous réseau utilise les adresses IP. Un réseau virtuel est associé à chaque sous réseau IP. Dans ce cas, les commutateurs apprennent la configuration et il est possible de changer une station de place sans reconfigurer le VLAN. Cette solution est l'une des plus intéressantes, malgré une petite dégradation des performances de la commutation due à l'analyse des informations.

Etiquetage des trames (802.1Q).

Comment le commutateur de gauche recevant une trame du commutateur de droite peut-il savoir à quel VLAN elle appartient ?



On utilise pour cela le marquage (tag) des trames. Concrètement, on ajoute un en-tête supplémentaire contenant notamment le n° de VLAN (VID) auquel appartient la trame. La norme 802.1Q définit trois sortes de trames :

- Les trames non étiquetées (untagged frame).
- Les trames étiquetées (tagged frame).
- Les trames étiquetées par une priorité (priority-tagged frame).

Préambule	SFD	@ MAC destination	@ MAC source	TAG	Type donnée	Données	FCS (CRC)	Délai intertrame
7x 10101010	10101011	6 octets	6 octets	4 octets	2 octets	46-1500 octets	4 octets	12 octets

TPID	Priority	CFI	VID
16 bits	3 bits	1 bit	12 bits

Remarque importante : Les switchs doivent être configurés de la même manière, c'est-à-dire utiliser les mêmes numéros de VLAN.

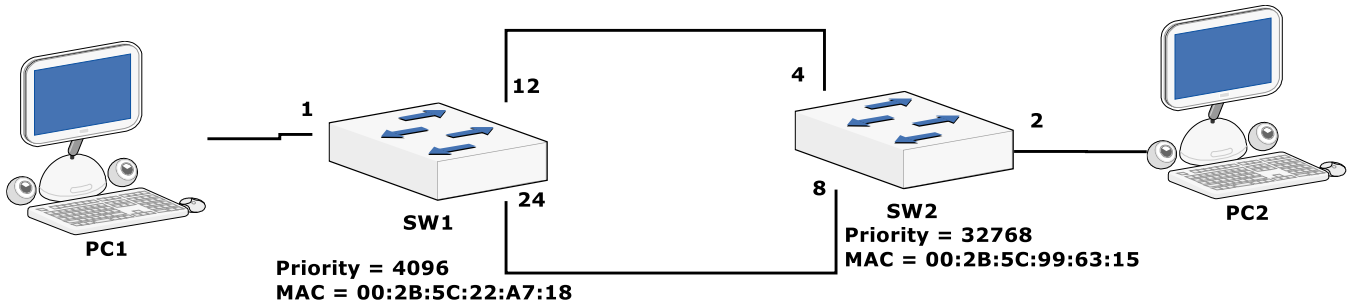
IV. Spanning-Tree

Mise en situation

Dans une architecture informatique, il arrive que le réseau comporte des boucles : plusieurs chemins possibles pour aller d'un point à un autre. Ce système présente un avantage certain **: la redondance** permet de pallier une éventuelle coupure d'un lien (travaux, rongeurs…).

Mais cette redondance, si elle est mal gérée, peut entrainer des problèmes très importants.

1. Tempête de broadcast.



1. PC1 envoie une requête ARP (en broadcast.

2. SW1 reçoit sur le port 1 et diffuse sur les ports 12 et 24

3a. SW2 reçoit sur le port 4 et diffuse vers 2 et 8
3b. En même temps, SW2 reçoit sur le port 8 et diffuse vers 4 et 2.

4a. SW1 reçoit sur le port 24 et diffuse vers 1 et 12.
4b. En même temps, SW1 reçoit sur le port 12 et diffuse sur 1 et 24

5. Répétition de 3a et 3b.

6. Répétition de 4a et 4b

Ce phénomène, appelé ***tempête de broadcast*** (broadcast storm) génère un trafic (inutile) très important.

2. Trames reçues en double

1. PC1 envoie un ping vers PC2.

2. SW1 reçoit sur le port 1 et diffuse (ports 12 et 24) car il ne connait pas la position de PC2

3a. SW2 reçoit sur la demande ping sur le port 4 et envoie PC2.
3b. En même temps, SW2 reçoit sur la demande sur le port 8 et envoie vers PC2.

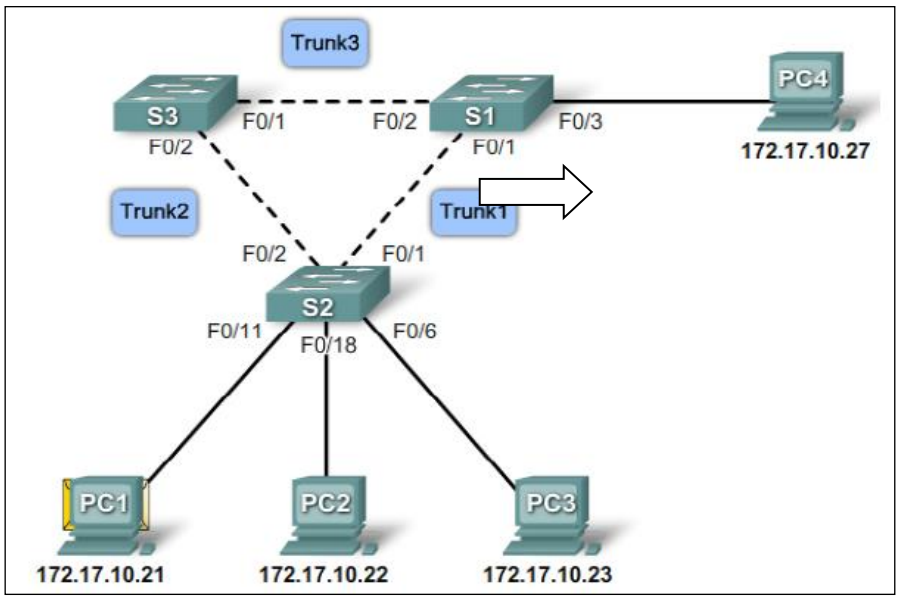
PC2 aura donc reçu deux demandes identiques.

3. Tables d'adresses MAC imparfaites.

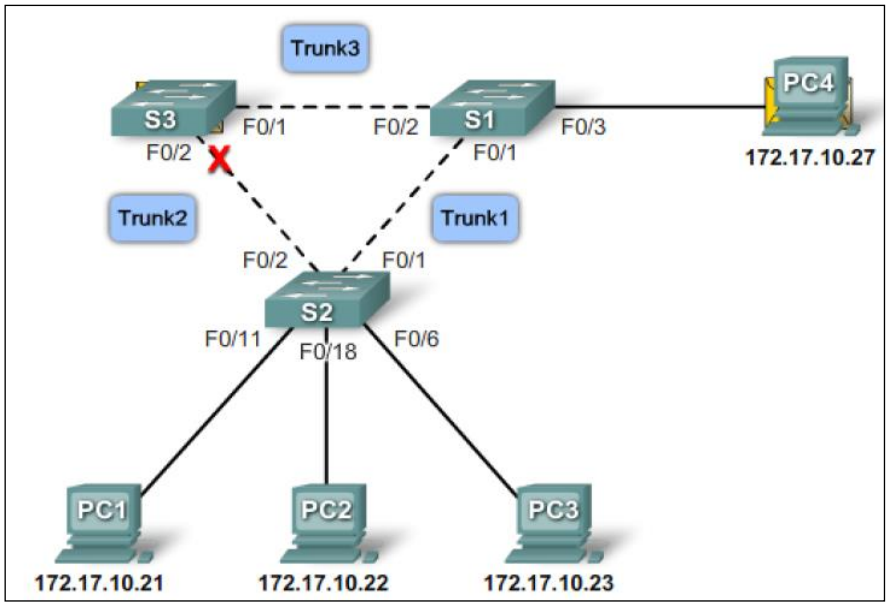
Du fait des diffusions en double, les tables des switchs se remplissent de manière imparfaites ou erronnées. Par exemple, SW2 "pensera" que PC1 est connecté sur son port 4 ou 8 ?. Avec des architectures plus complexes, une trame pourrait ainsi emprunter un chemin plus long que nécessaire.

2) Présentation du Spanning-Tree

Afin d'éviter les problèmes cités plus haut, on utilise un système chargé de détecter les boucles et de désactiver les liens redondants. C'est le protocole ***Spanning-Tree***, ou ***Arbre de Recouvrement***.



Avant



Après : le lien S2-S3 est désactivé

Il existe plusieurs protocoles de Spanning-Tree. Le plus connu est le STP ou 802.1D

3) Résumé du Fonctionnement du protocole STP (802.1D).

1. 1ère étape : Sélection du Root bridge.

Le Root Bridge, ou switch racine, est celui qui a la plus petite Bridge Identity (BID). Il s'agit d'un nombre composé de :

- Une ***priorité***, comprise entre 1 et 655356 (par défaut à 32768).
- ***L'adresse MAC*** du switch, pour départager en cas d'égalité sur la priorité.

2. 2ème étape : Sélection du meilleur chemin.

L'étape suivante consiste à sélectionner le meilleur chemin depuis les switchs vers le Root Bridge. Chaque liaison à un "coût". Le coût le plus faible l'emporte.

Link Speed	Cost (Revised IEEE Specification)	Cost (Previous IEEE Specification)
10 Gb/s	2	1
1 Gb/s	4	1
100 Mb/s	19	10
10 Mb/s	100	100

En cas d'égalité parfaite (coût, puis @MAC), c'est le numéro de port le plus faible qui détermine le "gagnant".

3. 3ème étape : Activation des ports.

En fonction des deux étapes précédentes, les ports sont activés ou désactivés. On dit qu'ils sont :

- ***Actif***, ou ***Forwarding*** : C'est le fonctionnement habituel d'un port de commutateur.

- ***Inactif*** ou ***Blocking*** : Le port est désactivé mais lit/transmet les trames STP pour être informé en cas de défaillance.

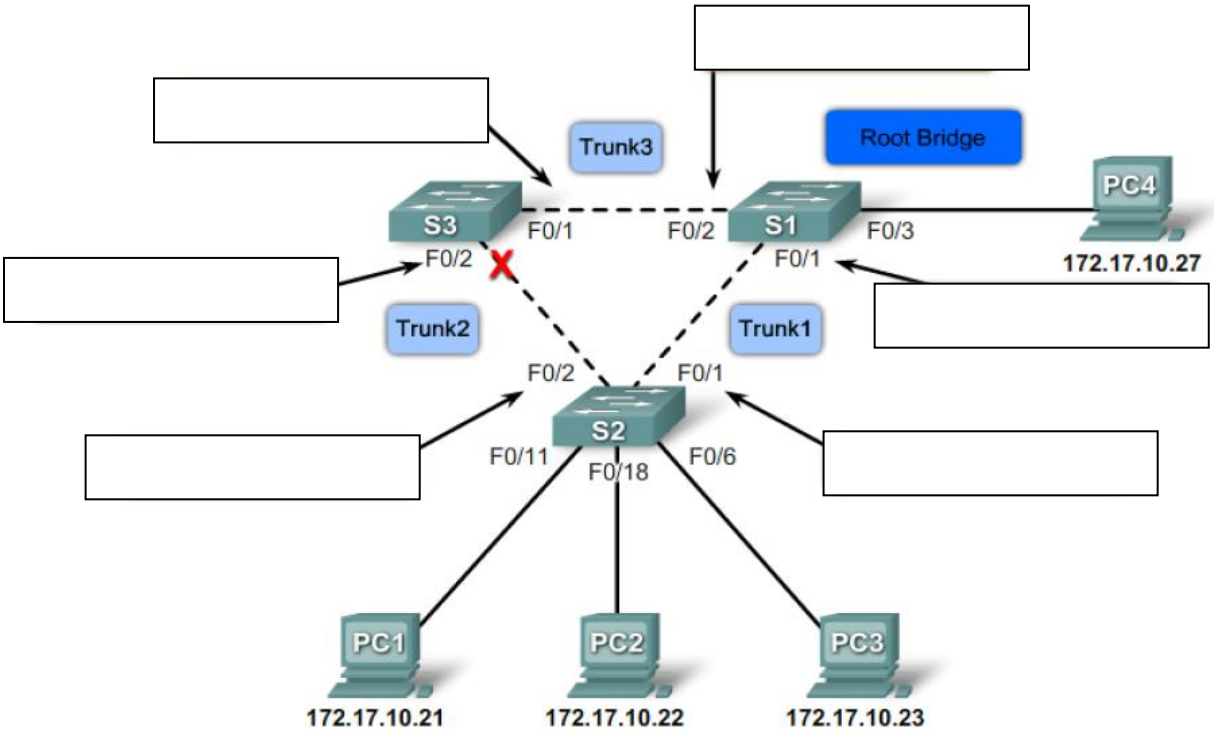
4. Nom des ports.

Chaque port faisant partie de la topologie STP est nommé :

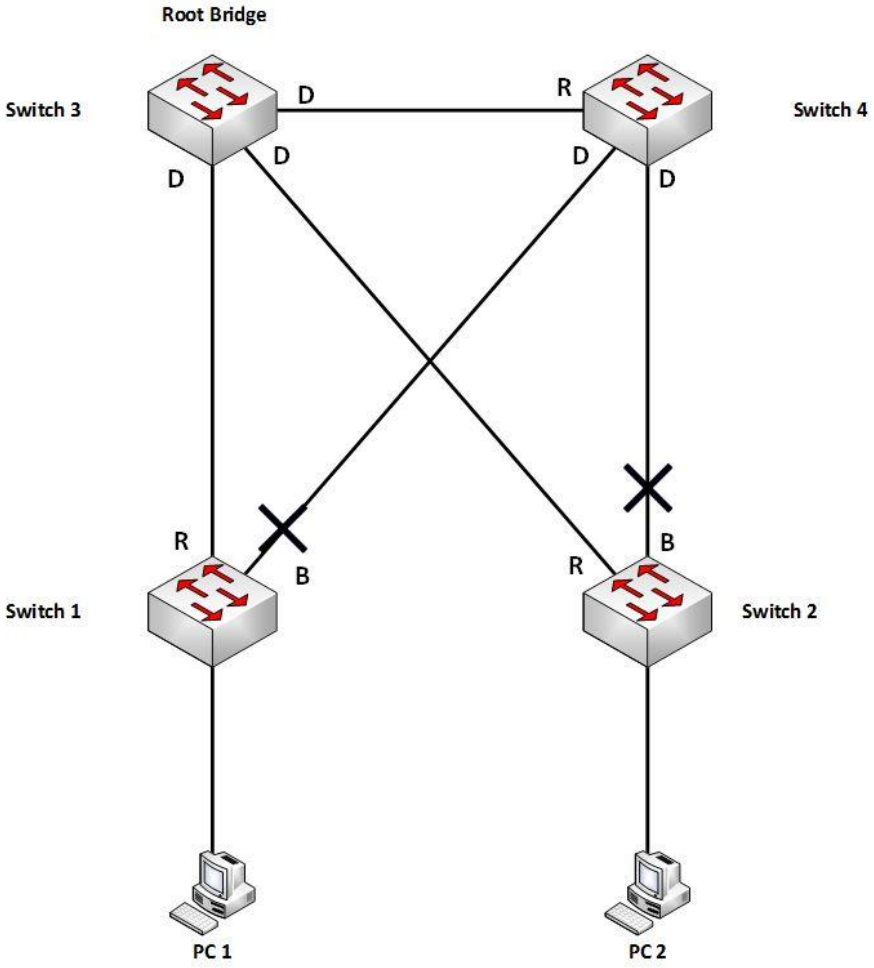
- ***Root Port*** : Ce sont les ports qui mènent au Root Bridge. Le Root Port reçoit les messages émis pas le Root Bridge.

- ***Designated Ports*** : Ce sont les ports qui émettent les trames 802.1D à destination des différents commutateurs.

- ***Non désignated Port*** : Ou Blocking Port, représente les ports qui n'émettent pas de données. Ces ports lisent quand même les messages 802.1D



Voici une autre topologie d'exemple avec les rôles des ports :



4) Trame BPDU.

Afin de détecter les boucles, les switchs émettent des messages appelés **BPDU – Bridge Protocol Data Units**.

Les BPDU vont permettre de découvrir la topologie, et d'élire le Root Bridge.

Le Root Bridge est en quelque sorte le chef de la topologie Spanning Tree.

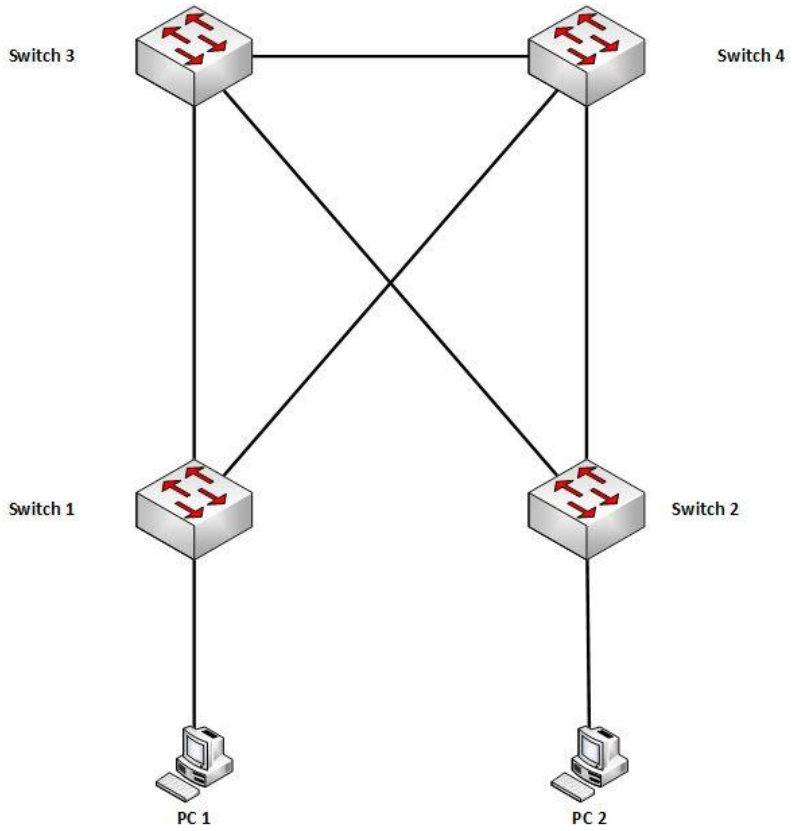
Une fois le Root Bridge élu, les switchs vont rechercher le meilleur chemin vers le Root Bridge.

Les chemins redondants seront désactivés.

En d'autres termes, les switchs vont chercher le port avec la métrique la plus faible vers le Root Bridge, puis ils vont couper les autres ports.

Nous verrons plus tard, que pour trouver le meilleur chemin, les switchs utilisent le coût de chaque lien traversé.

Prenons un exemple :

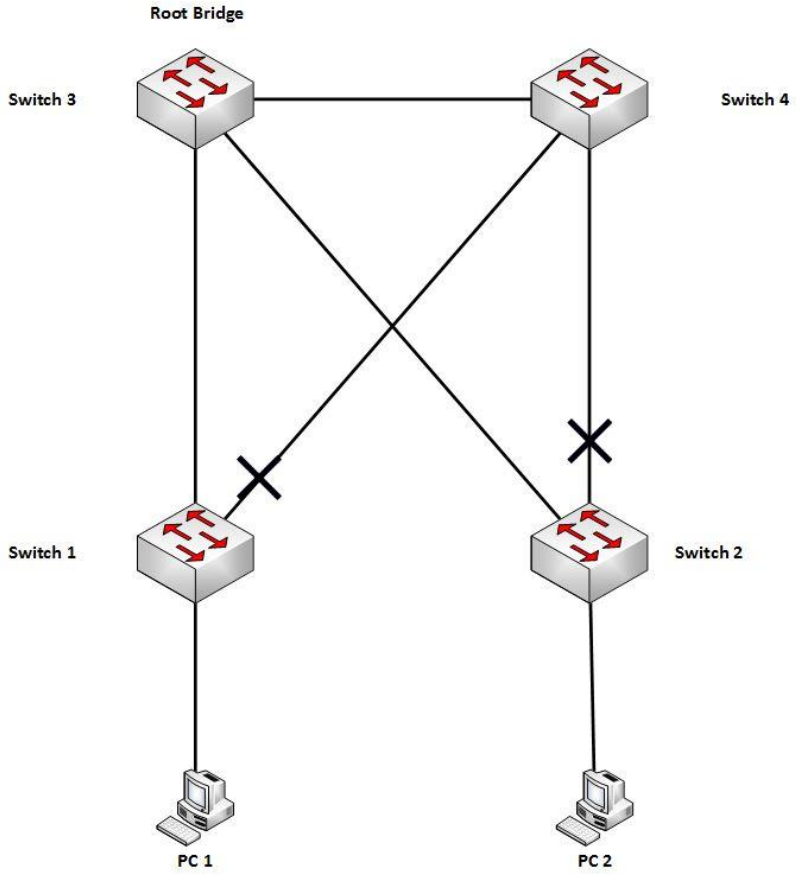


Dans cette topologie, il y a des liens redondants.

Considérons que S3 est élu Root Bridge.
S1, S2 et S4 vont chercher le meilleur chemin vers S3.

En toute logique, ils vont choisir un lien direct vers S3 (nous reviendrons sur ce choix juste après).

Nous obtiendrons alors ceci :

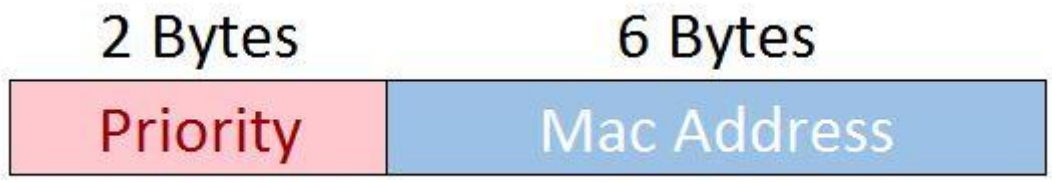


Il n'y a plus de boucle !!!

Revenons sur l'élection du Root Bridge. Comment est-il choisi ?

Les messages BPDU contiennent le Bridge ID.

Le Bridge ID est composé de la priorité du switch + son adresse MAC.



La priorité est de 32768 par défaut. Elle peut être modifiée pour influencer l'élection.
Elle peut aller de 0 à 61440.

Pour gagner l'élection, le switch doit avoir le BID le plus bas.
C'est donc le switch avec la priorité la plus basse qui gagnera.
En cas d'égalité (ou si la priorité est partout à sa valeur par défaut), c'est le switch avec l'adresse MAC la plus basse qui gagnera.
Au final, si nous ne changeons pas la priorité, le Root Bridge sera choisi de manière « arbitraire ».

Il existe 3 types de BPDU :

- BPDU de configuration, utilisé pour le calcul de Spanning Tree
- BPDU de notification de changement (TCN – Topology Change Notification BPDU), utilisé quand la topologie change
- BPDU d'acquittement de changement

Les BPDU sont envoyés en Multicast sur l'adresse 01:80:C2:00:00:00
Les BPDU de configuration contiennent l'ID du switch qui envoie le message, l'ID du port, le coût du lien.

Les BPDU de changement sont envoyés par l'un des switchs lorsque la topologie change. Ensuite, le Root Bridge va envoyer un BPDU de configuration à tout le monde.

Le BPDU d'acquittement se fait en réponse au BPDU de changement.

Détail de la BPDU :

Protocole	Version	Type Msg	Flags	Root ID	Coût	ID Pont	ID Port	Age Msg	Age Max	Hello T	Forward Delai
2	1	1	1	8	4	8	2	2	2	2	2

•Protocole, Version : Valeur toujours à 0

•Type Message (1 octet) :–0 pour un message de configuration,
–128 pour un message de changement de topologie

•Flags :(1 octet) mais seulement 2 bits utilisés
–TC : Topology-Change
–TCA : Topology-Change Acknowledgment, Acquittement en réception d'un message de configuration avec le bit TC à 1.

•Root ID et Port ID : 2 octets pour la priorité et 6 pour l'@ Mac

•Coût du port : alloue un coût à un port, pour privilégier un port par rapport à un autre (1 à 65535)

• Age Max: temps maximum d'attente pour qu'un pont considère la topologie caduque (recalcul de la topologie) (6 à 40 s, 20 s de base)

• Hello Time : intervalle entre chaque envoi de trames (hello) par le pont maître (1 à 10s, 2s de base)

• Forward Delay : durée de l'état écoute et de l'état apprentissage (4 à 30 s, 15 s recommandé)

Suite à la détection d'une panne, la nouvelle configuration met environ **50 secondes** à se mettre en place.
(Age Max + 2 x Forward Delay)

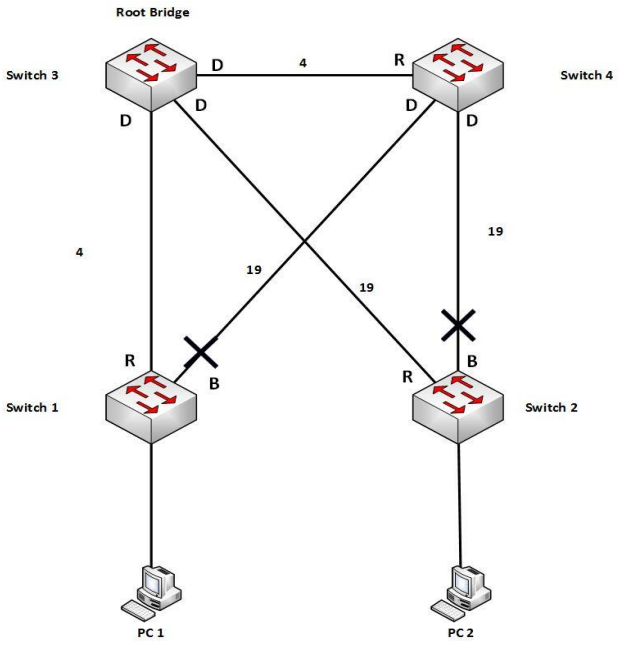
5) Mécanisme de décision des Switchs.

Pour que les switchs trouvent le meilleur chemin vers le Root Bridge, ils se basent sur le coût de chaque lien.
Spanning Tree défini un coût en fonction du type de lien.
Voici le tableau récapitulatif :

Bande Passante du lien	Coût STP	Coût RSTP
4 Mbps	250	5000000
10 Mbps	100	2000000
16 Mbps	62	1250000
100 Mbps	19	200000
1 Gbps	4	20000
10 Gbps	2	2000
100 Gbps	1	200
1 Tbps	1	20
10 Tbps	1	2

Ensuite, les switchs vont **additionner les coûts** de tous les liens jusqu'au Root Bridge, pour en déduire le meilleur chemin, et donc le Root Port.

Voici notre topologie précédente avec les coûts :

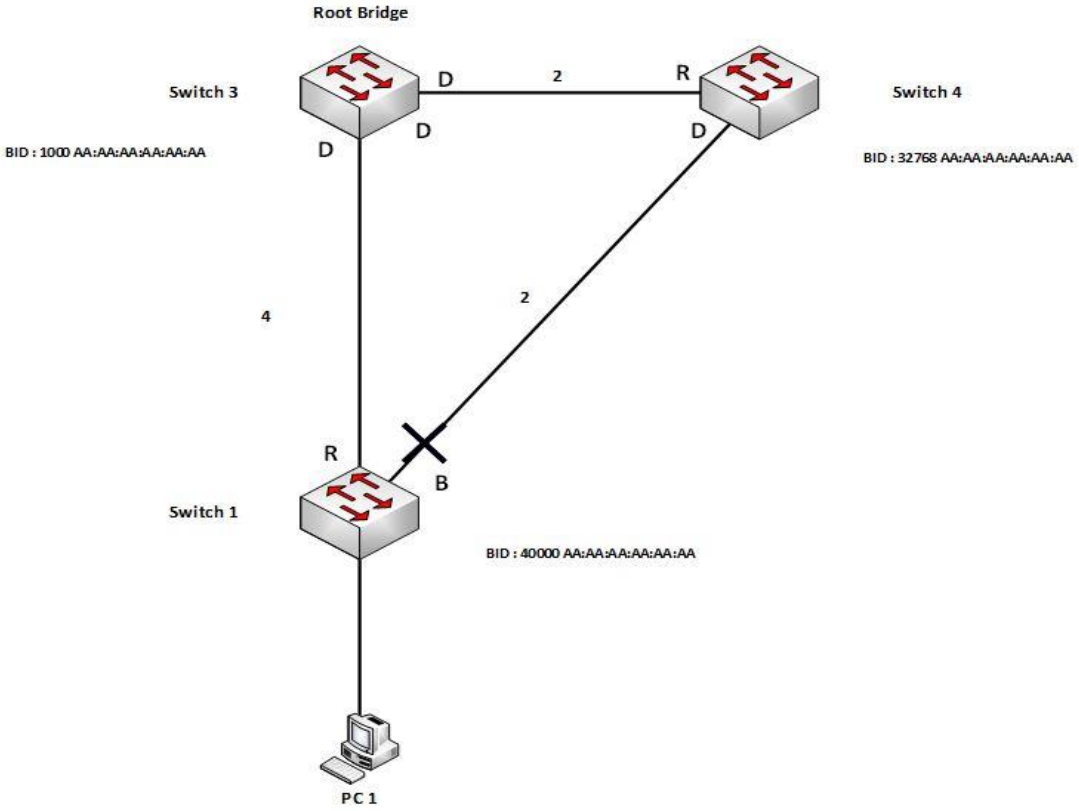


Si le switch a le choix entre deux chemins équivalents, il va les départager grâce au Bridge ID.

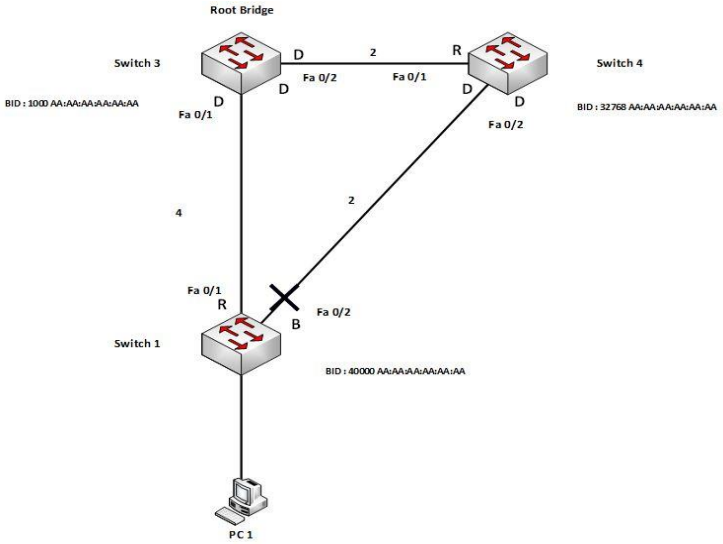
Le voisin avec le plus petit BID gagnera.

S'il y a toujours égalité (deux liens entre deux switch), c'est le **port avec le numéro le plus bas** qui sera privilégié.

Exemple :



Autre question qui se pose, comment choisir le port à bloquer sur un lien ?



Dans ce schéma il y a un lien bloqué entre S1 et S4.

Seul le port Fa 0/2 de S1 est bloqué. Il n'est pas possible de bloquer aussi le port FA 0/2 de S4, car il faut obligatoirement qu'il y ait un port Designated sur chaque lien.

Mais alors pourquoi bloquer le port de S1 et pas celui de S4 ?

S1 ayant le BID le plus haut, c'est lui qui devra passer son port en Blocking.

S4 garde son port en Designated pour la raison précédemment citée.

6) Quelques commandes Cisco

Pour le diagnostic :

#**show spanning-tree** [?]

Désactivation de STP :

(config)#**no spanning-tree vlan** *vlan-id*

Priorité du switch :

(config)#**spanning-tree vlan [***vlan-id***] priority** *priority*

7) Exemple d'architecture réseau de Campus vs Spanning-Tree :