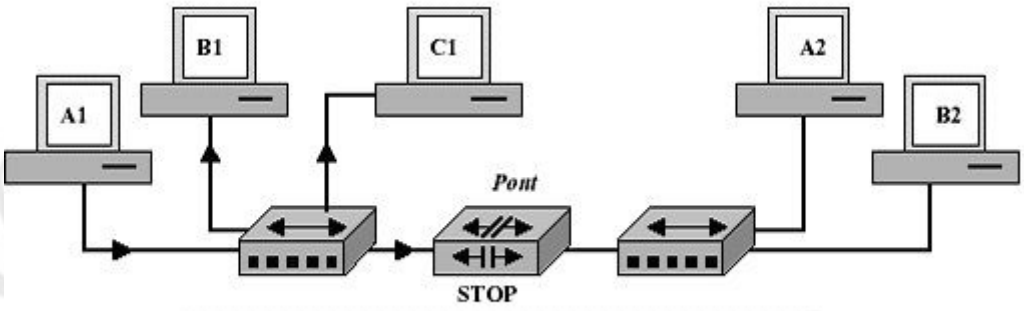
Le ponts, les switchs

1. Les ponts

Le pont est un dispositif permettant de filtrer les trames. Le filtrage consiste à laisser passer d'un segment de réseau à l'autre seules les trames qui lui sont destinées. Pour réaliser le filtrage, le pont décode et analyse les trames. Il extrait l'adresses MAC de l'émetteur afin de renseigner une table qui contient des couples adresse MAC, numéro de port. Il n'analyse pas les autres champs de la trame, sauf le champ FCS (rejet de la trame en cas d'erreur de FCS). A la mise sous tension du pont, la table *MAC-port* est vide.
Le pont agit au niveau de la couche 2 (liaison) du modèle OSI. Il permet donc aussi être utilisé pour interfacer un réseau Ethernet avec un réseau Token Ring.



Un message émis par A1 à destination de B1 est filtré par le pont

1.1. Technologie des ponts

Lorsque le pont reçoit une trame, il extrait l'adresse MAC de l'émetteur et enregistre une entrée (si elle n'existe pas déjà) dans sa table *MAC-port*. Pour réexpédier la trame, le pont examine les champs sources et destination. Plusieurs cas se présentent :

- L'adresse de destination figure dans sa table et correspond au port qui a reçu la trame. Cela signifie que l'émetteur et le destinataire se situe sur le même segment de réseau. Le pont ne transmet pas.
- L'adresse de destination figure dans sa table et ne correspond pas au port qui a reçu la trame. Cela signifie que l'émetteur et le destinataire ne se situent pas sur le même segment de réseau. Le pont transmet la trame.
- L'adresse de destination ne figure pas dans la table du pont . Le destinataire n'a jusqu'à présent émis aucune trame et le pont ne peut le localiser. Dans ce cas, le pont la transmet la trame.

A chaque entrée est associée une durée de vie, lorsque ce temps est atteint, l'entrée est supprimée de la table. Ceci permet de gérer l'arrêt ou le déplacement de stations dans le réseau.
Il existe des exceptions au filtrage : lorsque la trame est du type *broadcast* ou *multicast*, le pont laisse passer la trame.

1.2. Exemple

Sur un nouveau pont n'ayant jamais fonctionné sont branchés les stations suivantes :

Port N°0	Port N°1
S1, S2, S3	S4, S5, S6

La station S1 envoie une trame à S2
[1] Ecrire le contenu de la table
[2] Déterminez quelles sont les stations qui perçoivent la trame

La station S4 envoie une trame à S1
[3] Ecrire le contenu de la table
[4] Déterminez quelles sont les stations qui perçoivent la trame

La station S3 envoie une trame à S1
[5] Ecrire le contenu de la table
[6] Déterminez quelles sont les stations qui perçoivent la trame

1.3. L'offre du marché.

Les ponts présentaient une solution économique pour baisser la charge du réseau, mais aujourd'hui avec l'apparition des switchs à faible coût, il devient exceptionnel d'acheter un pont, sauf pour réaliser une liaison entre réseaux ethernet et token-ring.

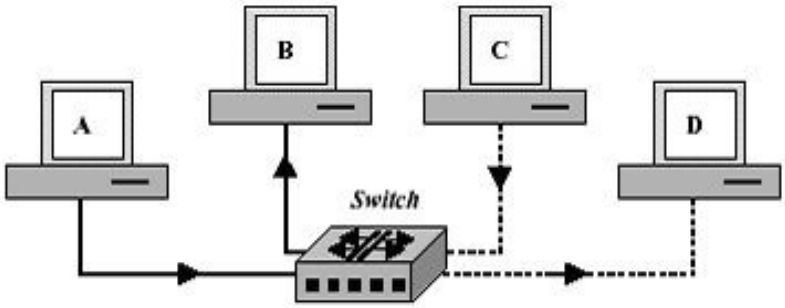
2. Spanning tree (802.1d) ou (802.1w).

- Pour éviter d'éventuelles pannes, il peut être intéressant de construire une **architecture redondante** qui repose d'une part sur un système de câblage qui offre plusieurs cheminements (une boucle), d'autre part sur la mise en place d'équipements de secours. Cette redondance est possible avec les ponts car ils s'échangent des informations sur la topologie du réseau et déterminent les routes actives de celles qui ne le sont pas.
- Le *spanning tree* est un protocole de niveau 2 associé à un algorithme qui permet d'éviter qu'une trame boucle sans fin dans le réseau. Les ponts s'échangent des trames *spanning tree* et calculent une route en invalidant les chemins multiples susceptibles de créer des boucles.
- La première étape du processus consiste à élire un pont racine en fonction de l'adresse MAC du pont et d'un indice de priorité paramétrable par l'administrateur réseau.
- La deuxième étape consiste à déterminer pour chaque pont son port racine.
- La troisième étape consiste à invalider les chemins redondants.
- Le pont racine émet régulièrement des BPDU pour maintenir l'état du "spanning tree". Le processus de création du "spanning tree" peut durer plusieurs dizaines de seconde. Pendant cette phase, aucun pont ne traite de trames. Le réseau s'arrête donc de fonctionner chaque fois qu'un pont est allumé ou éteint quelque part dans le réseau.
- **Attention** : réaliser une boucle sans mettre en place le protocole *spanning tree* est une faute grave qui à pour conséquence de bloquer totalement le réseau !.

3. Les commutateurs (switch)

Le commutateur est un pont multi-ports rapide. Le commutateur est un équipement qui offre une bande passante dédiée pour chaque port (contrairement au concentrateur qui partage la bande passante entre tous ses ports).

Important : chaque port du commutateur délimite un domaine de collision.



Un message émis par A à destination de B est seulement transmis à B
En même temps, C peut transmettre un message à D

3.1. Modes de fonctionnement

- **Store and forward** : le commutateur mémorise entièrement une trame avant de la transmètre vers le port destinataire. Ce mode de fonctionnement permet au commutateur de gérer des débits différents sur ses ports, et de vérifier la validité des trames grâce au champ FCS, mais ceci est très gourmand en temps et en mémoire.
- **On the fly** : dès le décodage de l'adresse Mac du destinataire, la trame est transférée vers le port correspondant. On ne perd donc quasiment plus de temps à traverser le switch. Par contre, il n'y a plus de contrôles ce qui entraîne la propagation des trames erronées sur le réseau.

3.2. Règle 5-4-3

La règle 5-4-3 n'est plus applicable pour les switchs puisqu'ils ne sont pas sujet aux mécanisme de détection de collision. Toutefois les règles de câblages préconisent de ne pas avoir plus de 3 niveau de répartition (répartiteur, sous-répartiteur, sous-sous-répartiteur), ce qui implique qu'une trame ne peut traverser que 5 switchs au maximum.

3.3. Autres caractéristiques des commutateurs

- Contrairement aux ponts, le commutateur effectue un filtrage positif, c'est à dire, qu'une station doit avoir émis une trame avant de pouvoir en recevoir une. Ceci a pour avantage d'éviter l'inondation sur de gros réseaux mais a pour inconvénient de bloquer la communication dans certains cas.
- Les switch *auto-configuration* sont capable de choisir s'il faut utilis le mode *half-duplex* ou le mode *full-duplex* sur chacun de leurs ports. La technique *full-duplex* est normalisée 802.3x.
- Le *port trunking* est la faculté d'associer plusieurs liens (jusqu'à 4) entre 2 switchs en une sorte de congrégation de liens. Les différents liens constituant ce trunk seront alors utilisés simultanément, permettant ainsi d'augmenter le débit inter-switch. Du point de vue du switch, la connexion à un trunk est vue comme un seul port.
- Les switchs *auto-sense* sont capables de détecter automatiquement la vitesse du réseau a plus approprié pour chacun de leurs ports.
- Les switch *auto-uplink* ou *auto-MDI/MDIX* sont capable de croiser automatiquement les paires de câbles pour réaliser automatiquement un port upink.
- Sur certains switch il est possible d'utiliser un port pour "écouter" à des fin d'analyse le trafic réseau qui se transite par un autre port. On appelle cette technologie le *mirroring*.

3.4. L'offre du marché.

- On trouve des switchs basiques (10/100 mbps, autonome, non administrable, *on the fly*) avec 4+1 ports pour moins de 30 €.
- Un switch professionnel (10/100, *rackable*, *stackable*, administrable, VLAN niveau 2) avec 24 ports + 1 port uplink combo 1 Gbps (cable catégorie 6 ou fibre optique) pour 500 €.
- Un switch professionnel (10/100/1000, *rackable*, *stackable*, administrable, VLAN niveau 3, *store and forward*) avec 24 ports + 2 ports fibre optique 1 Gbps pour 2000 €.

4. VLAN.

Certains commutateurs paramétrables permettent de mettre en oeuvre des **VLAN** (Virtual LAN), c'est à dire de construire plusieurs réseaux logiques sur un même réseau physique.
Un VLAN regroupe les communications concernant un groupe de stations indépendamment de leur localisation. Les messages entre stations d'un même réseau virtuel ne sont pas diffusés sur les autres réseaux virtuels. Les utilisateurs peuvent facilement être changés de groupe par simple reconfiguration des commutateurs auxquels les stations sont connectées.

4.1. Utilité d'un VLAN

La plus grande utilité des VLAN est d'apporter de la modularité, on passe facilement de 3 VLAN à 8 ports à par exemple 4 VLAN de 6 ports sur un même switch 24 ports. Un switch 24 ports découpé en 3 VLAN de 8 ports peut être comparé à un ensemble de 3 mini-switch 8 ports autonome. Un switch 24 ports découpé en 4 VLAN de 6 ports peut être comparé à un ensemble de 4 mini-switch 6 ports autonome.

4.2. Les méthodes pour mettre en place des VLAN.

4.2.1. Par numéro de port (VLAN niveau 1).

On définit les ports appartenant à chaque réseau virtuel, un même réseau virtuel peut être constitué de ports appartenant à des commutateurs différents. Lorsque l'on change le brassage, il faut reconfigurer le commutateur.

4.2.2. Par adresse MAC (VLAN niveau 2).

On associe les adresses MAC à un VLAN. L'adresse MAC étant spécifique pour chaque station, le déplacement d'une station ne nécessite pas la reconfiguration du commutateur. Attention, cette méthode de gestion des VLAN est très lourde à administrer !

4.2.3. Par adresse IP (VLAN niveau 3).

On peut utiliser le type de protocole ou l'adresse réseau (IP) pour définir l'appartenance
à un réseau virtuel. Quoique que basé sur des informations de la couche 3 du modèle OSI cela ne constitue pas une fonction de routage (ces informations servent à déterminer l'appartenance à un réseau virtuel, mais pas à acheminer les paquets en fonction de l'adresse réseau). Les performances du VLAN de niveau 3 sont moindres par rapport aux VLAN de niveaux 1 et 2, car il faut analyser les paquets jusqu'au niveau 3 du modèle OSI.

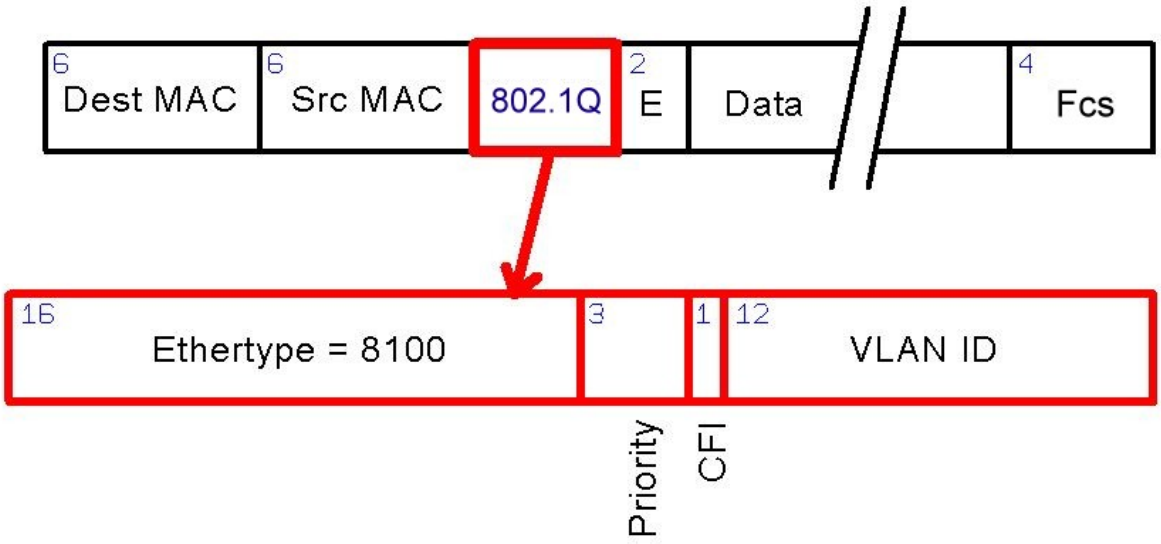
4.3. Le protocole 802.1Q .

4.3.1. Si on ne met pas en place le protocole 802.1Q :

Les VLAN ne sont connus que par un seul switch. Il est impossible de faire communiquer un poste du VLAN N°2 situé sur le switch S1 avec un autre poste déclaré sur le VLAN n°2 situé sur un autre switch (S2). Le VLAN n°2 se S1 est considéré comme un VLAN différent du VLAN n°2 de S2. De plus une machine ne pourra pas appartenir à plusieurs VLAN.

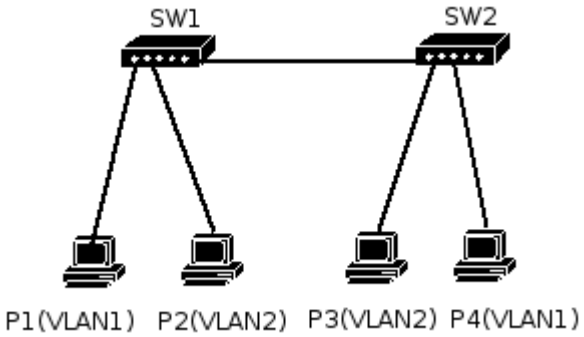
Si **on met en place** le protocole 802.1Q :
Les ports compatibles 802.1Q des switchs ajoutent un *tag* de 4 octets qui précise l'identifiant du VLAN émetteur. La modification de l'entête implique que l'émetteur et le récepteur d'une trame taguée soient capable d'implémenter le protocole 802.1Q. Il est possible de faire communiquer un poste du VLAN n°2 situé sur un swicth S1 avec un autre poste déclaré sur le VLAN n°2, mais situé sur un autre switch (S2). Le VLAN n°2 sera commun aux switchs S1 et S2.
Remarque 1 : Certaines cartes réseaux sont compatible 802.1Q. Les postes clients équipés de ces cartes peuvent donc faire partie de plusieurs VLAN.
Remarque 2 : On appelle *trunk* les câbles de liaisons entre switchs utilisant le protocole 802.1Q.

4.3.2. Schéma d'une trame Ethernet II taguée.



4.3.3. Exemple

Il faut taguer les ports qui relient les switchs pour partager les VLAN.



(u)=untaged
(t)=taged

Table Port-Vlan de SW1
port1 --> vlan1 (u)
port2 --> vlan2(u)
port 5 -> vlan1 (t) et vlan2(t)

Table Port-Vlan de SW2
port 1 -> vlan1(t) et vlan2(t)
port2 --> vlan2(u)
port3 --> vlan1(u)