Conception des Infrastructures Réseaux

SISR 2

BTS Services Informatiques aux Organisations
1ère année

Chapitre 2 :
Les réseaux locaux virtuels

Objectifs :

Comprendre l'utilité, les protocoles et les techniques associées à la technologie des VLANs.

Plan :

TD associés :
   TD1 : Découverte des VLANs
   TD2 : Maîtrise des protocoles 802.1d et 802.1q

1. Historique.

Les premiers réseaux Ethernet (on se situe donc en couche 2) étaient conçus à base de câbles coaxiaux raccordés entre eux et connectés aux ordinateurs, si bien que tout signal électrique émis par l'un d'eux était reçu par tous les autres. L'ensemble des machines ainsi reliées entre elles s'appellait un domaine de collision (puisque ces machines partageaient le même médium physique).

Dans le cas de grands réseaux locaux, il était impossible d'avoir un seul domaine de collision (pour des raisons d'éloignement géographique, de longueur de câbles, de temps de propagation ou à cause du nombre trop important d'ordinateurs) et il fallait donc concevoir des domaines de collision de taille raisonnable, reliés entre eux par des routeurs. Des ponts Ethernet n'auraient pas suffi car ils augmentent le temps de propagation des signaux électriques, d'où la nécessité de remonter en couche 3. Chacun de ces domaines de collision était également appelé segment Ethernet.

À chaque segment Ethernet correspondait donc un sous-réseau IP. Au bout du compte, on aboutissait à un découpage logique calqué très exactement sur le découpage physique du réseau. Cela imposait une proximité géographique des machines si l'on voulait qu'elles appartiennent au même segment Ethernet, ce qui n'est pas nécessairement pratique. Par ailleurs, ceci limitait grandement la mobilité des ordinateurs.

Après l'arrivée des premiers commutateurs, de nouvelles possibilités sont apparues. Compte tenu de l'électronique interne des commutateurs, plus complexe que celles des répéteurs, il devenait possible de disposer de plusieurs segments Ethernet au sein d'un même commutateur. Mais, en ajoutant quelques en-têtes supplémentaires aux trames Ethernet, il devenait possible d'étendre la taille de ces segments Ethernet à l'ensemble d'un réseau de commutateurs interconnectés. Les réseaux virtuels (virtual LAN, VLAN) étaient nés.

2. Le principe de fonctionnement.

Les VLAN sont une évolution du concept de réseau local sur une topologie en étoile construite autour de commutateurs. Il s'agit de découper virtuellement les équipements de commutation pour construire plusieurs sous-réseaux indépendants, le câblage restant inchangé.
Les réseaux virtuels permettent de réaliser des réseaux axés sur l'organisation de l'entreprise en s'affranchissant de certaines contraintes techniques comme la localisation géographique. On peut ainsi définir des domaines de diffusion (domaines de broadcast) indépendamment de l'endroit où se situent les systèmes.

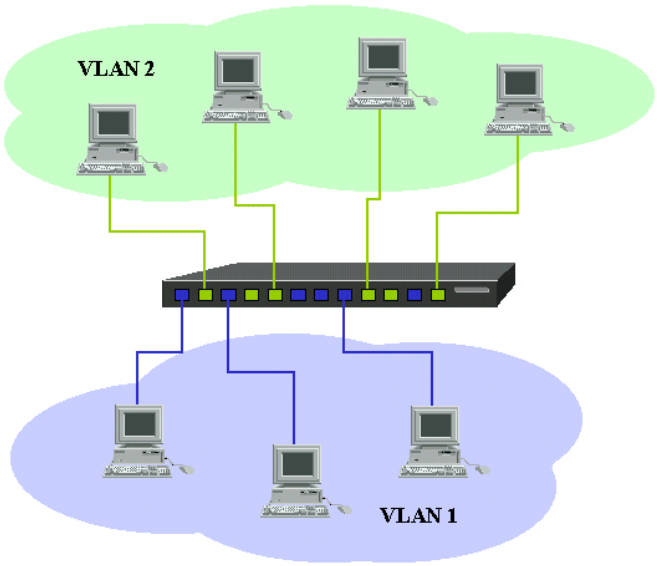
Un VLAN est l'équivalent moderne des segments Ethernet de l'ancien temps. Tous les ordinateurs faisant partie d'un même VLAN sont capables de communiquer entre eux directement sans avoir à passer par un routeur. On ne parle plus de domaine de collision, étant donné qu'il n'y a pas de collisions avec des commutateurs, mais de **domaine de diffusion**, puisqu'une trame de diffusion émise par un ordinateur sera reçue par toutes les machines faisant partie du même VLAN. A contrario, deux machine n'appartenant pas au même VLAN ne peuvent plus communiquer bien qu'elles soient physiquement connectées au même réseau.

3. Les différents types de VLANs.

Il existe plusieurs méthodes de construction des VLAN : par port, par adresse MAC, par protocole, par sous-réseau, par règles.

3.1. 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.

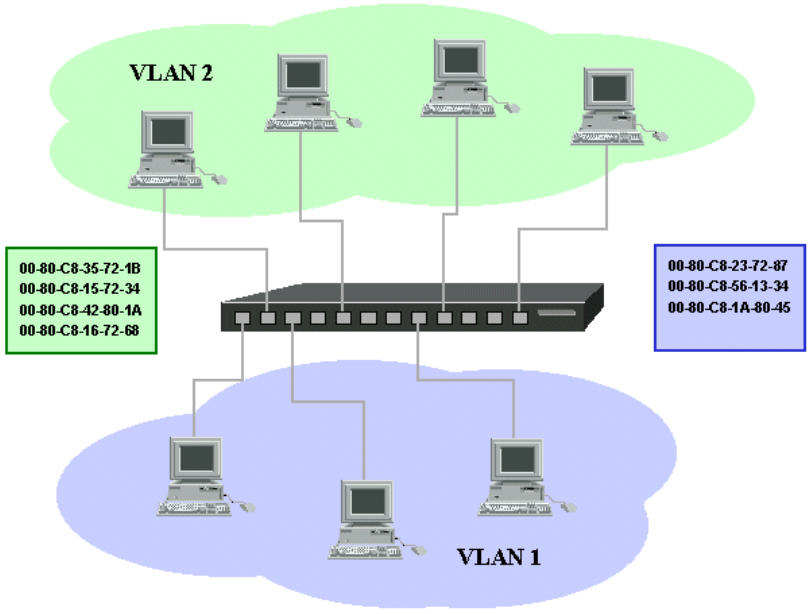


Les premières implémentations ne permettaient pas de créer un même VLAN sur plusieurs commutateurs. Depuis une nouvelle génération de commutateurs permet de réaliser d'un tel VLAN, grâce à l'échange d'informations entre les commutateurs et au marquage des trames.

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 concentrateur, appartiennent au même VLAN. Le VLAN port est impossible à mettre en œuvre dans le cas d'ordinateurs portables pouvant se connecter à des emplacements banalisés dans l'entreprise.

3.2. 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 vis à vis de la localisation. La station peut être déplacée sur le réseau physique, son adresse physique ne changeant pas, il est inutile de reconfigurer le VLAN. Les VLAN par adresse MAC sont très adaptés à l'utilisation de stations portables.

La configuration peut s'avérer rapidement fastidieuse puisqu'elle nécessite de renseigner une table de correspondance avec toutes les adresses du réseau. Cette table doit aussi être partagée par tous les commutateurs, ce qui peut engendrer un trafic supplémentaire sur le réseau.
Il est possible de coupler un serveur RADIUS à ce genre de solution pour gérer les adresses MAC.

3.3. VLAN par protocole.

Un VLAN par protocole, ou **VLAN de niveau 3**, est obtenu en associant un réseau virtuel par type de protocole rencontré sur le réseau. On peut ainsi constituer un réseau virtuel pour les stations communiquant avec le protocole TCP/IP, un réseau virtuel pour les stations communiquant avec le protocole IPX, ...

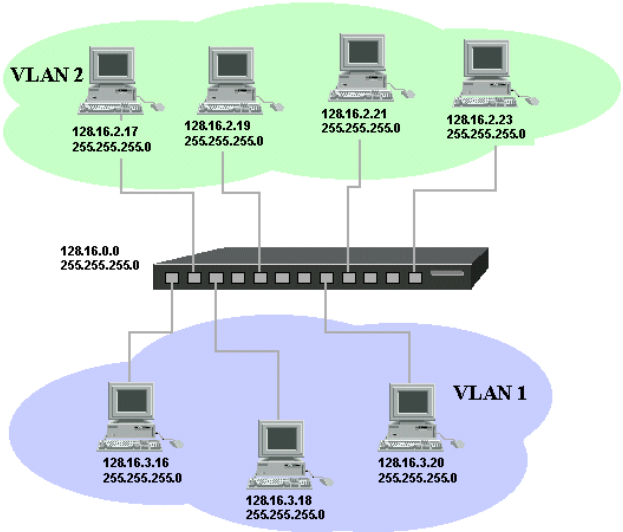
Dans ce type de VLAN, les commutateurs apprennent automatiquement la configuration des VLAN. Par contre, elle est légèrement moins performante puisque les commutateurs sont obligés d'analyser des informations de niveau 3 pour fonctionner.

Les VLAN par protocole sont surtout intéressant dans des environnements hétérogènes multi-protocoles (Novell Netware avec IPX, Unix avec TCP/IP, Macintosh avec Appletalk...). La généralisation de TCP/IP leur a fait toutefois perdre de l'intérêt.

3.4. VLAN par sous-réseau.

Egalement appelé VLAN de niveau 3 et variante des précédents, un VLAN par sous-réseau utilise les adresses IP sources des datagrammes émis. Un réseau virtuel est associé à chaque sous-réseau IP.

Dans ce cas, les commutateurs apprennent automatiquement la configuration des VLAN et il est possible de changer une station de place sans reconfiguration des VLAN.
Il suffit également de changer une station de travail de sous réseau pour la changer de VLAN.



Cette solution est l'une des plus intéressantes, malgré une légère dégradation des performances de la commutation due à l'analyse des informations de niveau réseau (niveau 3).

3.5. VLAN par règles.

Plus récemment est apparue une nouvelle méthode de définition de réseaux virtuels basée sur la possibilité des commutateurs d'analyser le contenu des trames. Les possibilités sont multiples, allant des réseaux virtuels par type de service (ports TCP) aux réseaux virtuels par adresse multicast IP.

4. Les avantages.

- réduction des messages de diffusion, par exemple les requêtes ARP (Address Resolution Protocol) liées au protocole IP (Internet Protocol) qui peuvent occuper une part non négligeable du trafic quand le réseau devient important. Les messages de diffusion (broadcast) sont limités à l'intérieur de chaque VLAN. Ainsi les broadcasts d'un serveur peuvent être limités aux clients de ce serveur.

- création de groupes de travail indépendamment de l'infrastructure physique. Des groupes de stations peuvent être réalisés sans remettre en cause l'architecture physique du réseau. De plus, un membre de ce groupe peut se déplacer sans changer de réseau virtuel. Dans le cas de VLAN par adresse MAC ou par sous-réseau IP, il n'y a même pas de reconfiguration des commutateurs.

- augmentation de la sécurité par le contrôle des échanges inter-VLAN. Les échanges inter-VLAN se réalisent tout comme des échanges inter-réseaux, c'est-à-dire au travers de routeurs. Il est par conséquent possible de mettre en œuvre un filtrage du trafic échangé entre les VLAN.

5. Le marquage des trames IEEE 802.1q.

La plupart des commutateurs administrables sont compatibles avec le protocole IEEE 802.1q. Cela signifie qu'ils savent gérer le marquage des trames.

5.1. Qu'est-ce que le marquage ?

Un VLAN peut être local à un commutateur ou s'étendre à un ensemble de commutateurs reliés entre eux. On a donc la possibilité d'organiser la structure logique de son réseau sans avoir à se soucier de sa structure physique, ce qui apporte une souplesse fort appréciable.

Dans le cas où une trame Ethernet doit être transportée d'un commutateur à un autre, il est nécessaire de connaître le VLAN auquel elle appartient. C'est ce qu'on appelle le marquage. Le marquage permet de reconnaître le VLAN d'origine d'une trame. Il peut être implicite, c'est-à-dire que l'appartenance à tel ou tel VLAN peut être déduite des informations contenues dans la trame (adresse MAC, protocole, sous-réseau IP) ou par son origine (port). Il peut être explicite, dans ce cas une information (souvent un numéro de VLAN) est insérée dans la trame. Tout dépend du type de VLAN.

- Dans le cas d'un VLAN par port, le transfert d'une trame vers un autre commutateur ne conserve pas d'information sur l'appartenance à tel ou tel VLAN. Il est nécessaire de mettre en œuvre un marquage explicite des trames.

- Dans le cas d'un VLAN par adresse MAC, il est possible d'envisager que la table de correspondance entre les adresses MAC et les numéros de VLAN soit distribuée sur tous les commutateurs. C'est une solution lourde à laquelle on peut préférer un marquage explicite.

- Dans le cas d'un VLAN de niveau 3, il fut utiliser un marquage implicite. Il n'est pas nécessaire de marquer les trames sur les liaisons inter-commutateurs. L'analyse des trames dégradant les performances, il est là aussi préférable de marquer explicitement les trames.

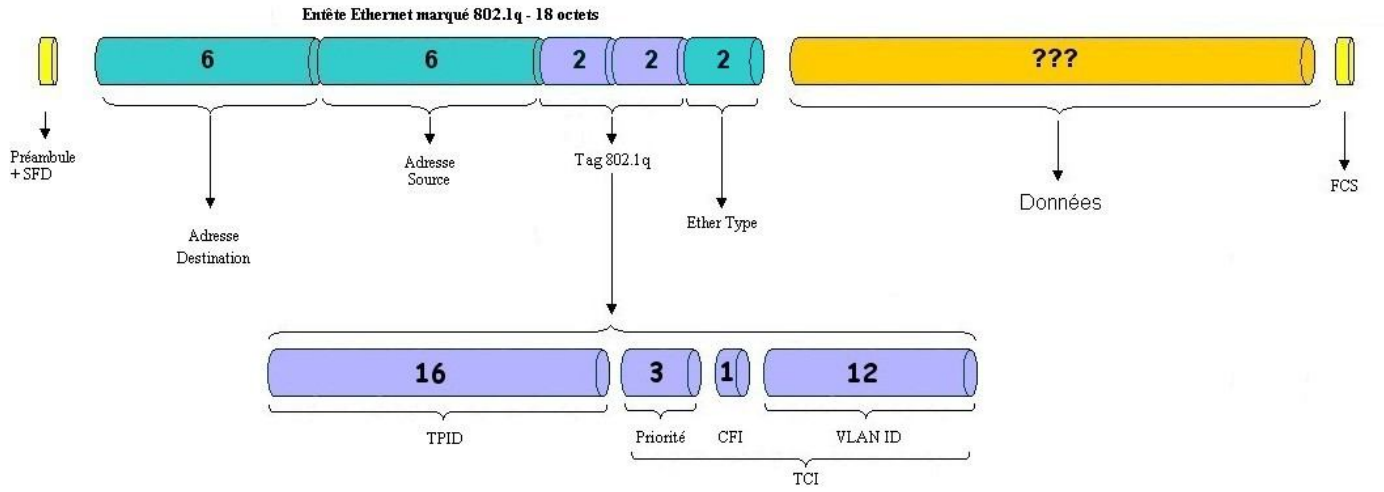
Plusieurs solutions de marquages ont été proposées par des constructeurs telles Virtual Tag Trunking de 3Com ou encore ISL (InterSwitch Link Protocol) de Cisco, toutes incompatibles entre elles. Pour cette raison, l'IEEE a défini une norme de définition des VLAN sous la référence 802.1q.

5.2. Marquage, Tag, Trunk.

En français, on parle de marquage, encore que les termes étiquette ou tag sont couramment admis. Il est également possible, dans la terminologie Cisco, de parler de trunk.

L'idée serait d'arriver à ce que certains ports du switch puissent être assignés à plusieurs VLANs, ce qui fera économiser du câble et des ports sur le commutateur.

Le principe consiste à ajouter dans l'en-tête Ethernet ou MAC, un marqueur (Tag) qui permet d'identifier le VLAN.
Attention : toutes les solutions propriétaires ne répondent pas nécessairement à cette norme.

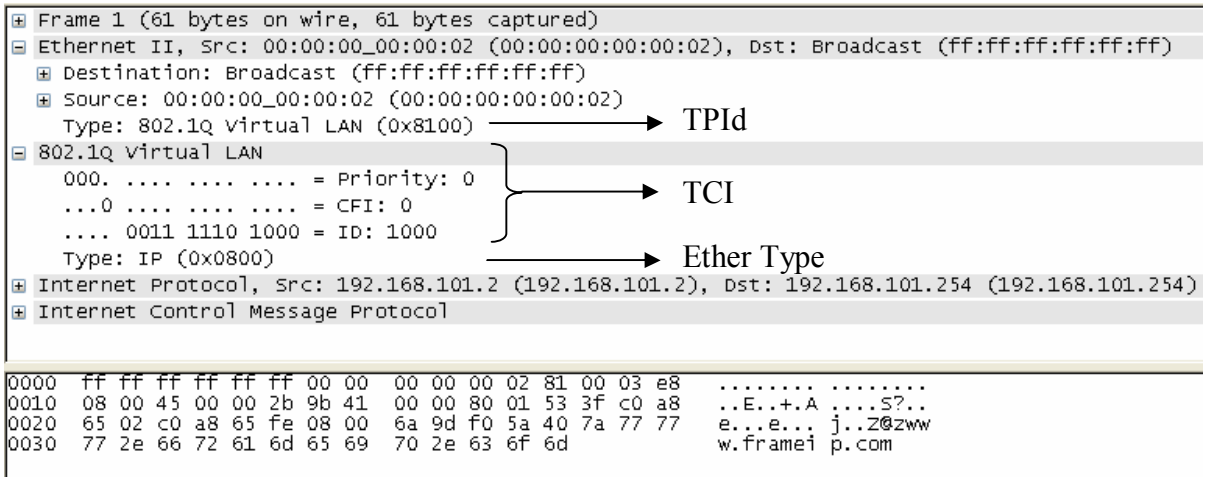


Un champ **Tag 802.1q** de 4 octets est inséré avant le champ **Ether Type**.
Ce dernier servait et sert toujours à identifier le type de protocole utilisé en couche réseau. Il contient toujours 0800 ou 0x0800 qui signifient IPv4.
0x permet de rappeler que le champ est exprimé en hexadécimal.

Le champ Tag 802.1q est composé de deux champs, de deux octets chacun :

		Taille *bits*	Nom	Description
Tag 802.1q	TPID	16	**T**ag **P**rotocol **Id**entifier	Désigne le type de tag. Il permet par exemple au commutateur d'identifier la trame comme comportant un tag 802.1Q pour celle ayant un format Ethernet II / 802.3. Dans ce cas, cette valeur est égale à la constante hexadécimale 0x8100. Également appelé VPID (VLAN Protocole Identifier).
	TCI **T**ag **C**ontrol **I**nformation	3	Priorité	Sur 3 bits on peut coder 8 niveaux de priorités de 0 à 7. Ces 8 niveaux sont utilisés pour fixer une priorité aux trames d'un VLAN relativement aux autres VLANs.
		1	CFI	Canonical Format Identifier. Ce champ est utilisé pour des raisons de compatibilité entre les réseaux Ethernet et les réseaux de type Token ring. Il doit être marqué à 0.
		12	VLAN ID VID	Ce champ est codé sur 12 bits et représente le numéro du VLAN. Il est donc possible d'intégrer la trame dans 1 VLAN parmi 4096 possibilités. La valeur 0 indique qu'il n'y a pas de VLAN.

Ci-dessous, une présentation de la capture d'une trame ICMP étiquetée réalisée avec WireShark.



5.3. Les ports des commutateurs.

Les ports d'un commutateur peuvent être dans l'un des trois états suivants : *untagged*, *tagged* ou *no*.

Untagged : le port n'est associé qu'à un seul VLAN. C'est à dire que tout équipement raccordé à ce port fera partie du VLAN.

Tagged : signifie que les trames qui arrivent et sortent sur le port sont marquées par une en-tête 802.1q supplémentaire dans le champs Ethernet.
Un même port peut être "tagged" sur plusieurs VLAN différents.

No : aucune configuration dans le VLAN. Le port est inactif.

Chez Cisco, la terminologie est un peu différente : ***untagged*** devient ***ACCESS***, ***tagged*** devient ***Trunk***.
Le tout, c'est de le savoir.

Le marquage est implémenté pour la gestion des VLANs répartis sur plusieurs commutateurs. Les trames voyagent alors au format Ethernet sur les ports *untagged* ou *no* et au format IEEE802.1q sur les ports *tagged* dans les commutateurs.
Lorsqu'une trame arrive sur un port tagged, son entête Ethernet est complété pour recevoir le tag, et le FCS est recalculé.

5.4. Usages et limites du marquage.

Le premier intérêt du protocole IEEE802.1q est de permettre la création de VLAN répartis sur plusieurs commutateurs.
On peut ainsi mettre dans un même VLAN les prises destinées aux imprimantes, à l'administration réseau, à la comptabilité, même si pour des raisons diverses les bureaux ne sont pas regroupés.

Il peut être également possible, grâce aux ports *tagged*, de partager un même port entre plusieurs VLANs, pour accéder à un serveur, …

Si le serveur est directement relié à ce port, il faut que sa carte réseau soit compatible 802.1q.

5.5. Interconnexion des VLANs.

Pour interconnecter les VLANs, même s'ils sont dans le même sous réseau IP, ce qui est à éviter, il faut mettre ne œuvre un routeur, qui aura une interface dans chaque VLAN.

Cette technique est nommée routage inter VLAN.

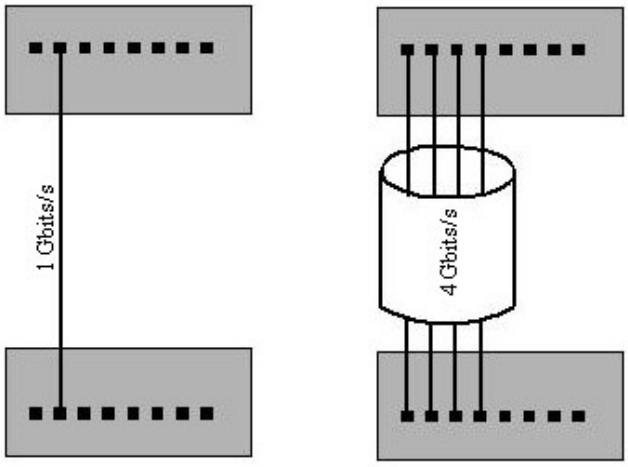
Remarque : 802.1q est basé sur un protocole propriétaire CISCO ISL (Inter Switch Linking) et permet également de gérer la qualité de service (QoS) par la même technique de marquage de la trame.

6. Les plus des commutateurs administrables.

Bien que n'ayant rien à voir directement avec les VLANs, les commutateurs administrables sont également capables de faire d'autres choses : intégration d'un agent SNMP, d'un serveur HTTP destiné uniquement à son administration, intégration de la gestion de redondance de liens, de l'agrégation de ports, de mécanismes d'authentification, …

6.1. L'agrégation de liens.

Il s'agit d'une technique proposée par de nombreux constructeurs, sur des matériels haut de gamme :
Au lieu d'établir une liaison simple entre deux commutateurs, il est possible de les agréer c'est-à-dire d'utiliser plusieurs liaisons en parallèle, ce qui augmente d'autant le débit "virtuel" de la liaison :



Cette agrégation porte également le nom de … trunk.

6.2. Les mécanismes d'authentification dans les VLANs.

La sécurité des VLANs repose sur les mécanismes mis en œuvre pour l'authentification des machines se connectant aux ports des switchs.
Ci-dessous sont détaillées les principales méthodes utilisables pour l'authentification :

- **Fixer une adresse MAC à un port physique :** cette méthode, certes efficace, pose le problème de l'administration qui devient très lourde à gérer notamment lors des déplacements de machines dans le réseau. Ainsi chaque port physique fait partie d'un seul VLAN et seule l'interface réseau paramétrée peut se connecter au port.

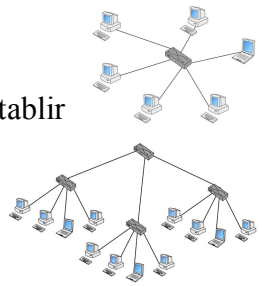
- **802.1x (RFC 2284) :** cette norme d'authentification est également employée dans la récente norme de réseaux WIFI 802.11i. On distingue 3 rôles dans le schéma d'authentification :
  - « l'authentificateur » qui met en œuvre l'authentification et route le trafic vers le réseau si l'authentification a marché.
  - le « demandeur » qui demande l'accès au réseau. Dans notre cas, il s'agit de la machine cliente.
  - le « serveur d'authentification » qui effectue l'authentification du demandeur en vérifiant les données qu'il a transmises. La plupart du temps il s'agit d'un serveur radius.

  Le concept de « Controlled/Uncontrolled Port » :
  l'Uncontrolled Port (UP) et le Controlled Port (CP) sont 2 abstractions fonctionnelles qui sont physiquement sur la même connexion réseau. Une trame du client est routée par l'AP (Access Point qui est dans notre cas le switch) vers l'UP ou le CP en fonction de l'état de l'authentification.
  Le résultat de cette abstraction logique est que si le client n'est pas authentifié il aura seulement accès au serveur d'authentification. Une fois l'authentification réussie il pourra accéder aux services du réseau.
  Un point important est que cette authentification doit être mutuelle ce qui rend quasi impossible toute attaque de type « man in the middle ».

- **Port security (propriétaire cisco) :** Cette technologie permet d'implémenter de façon plus souple les règles ci-dessus en indiquant des règles sur les adresses mac permettant de se connecter : une liste de macs autorisés, des conditions de connections (horaires, …).

- **Dynamics Vlans (VQP et VMPS) (propriétaire cisco)** : VQP (Vlan Query Protocol) est un protocole qui permet au switch client d'interroger un serveur VMPS (VLAN Membership Policy Server) avec des informations sur les stations enregistrées et leur VLAN associé. Ainsi le switch client pourra associer le port avec le bon VLAN. Le serveur VMPS peut être un switch (ex : cisco catalyst) ou un serveur windows 2000 avec active directory server.

6.3. La redondance de liens.



Imaginons un réseau Ethernet mettant en œuvre plusieurs commutateurs. Au lieu d'établir une structure en étoile, ou en arbre si elle est plus complexe, il devient possible de rajouter des liaisons entre les commutateurs qui n'étaient pas interconnectés.

Cette redondance de lien a pour but de créer des chemins alternatifs en cas de rupture d'un chemin inter commutateur.

Cela a aussi une incidence : le domaine de diffusion offre des boucles dans lesquelles les trames de diffusion (broadcast) risquent de tourner en rond, provoquant une tempête de diffusion (broadcast storm) qui paralyse le réseau et des problèmes d'identification des trames : une même trame risque d'apparaître plusieurs fois en suivant des chemins différents, ce que les éléments du réseau ne sauront pas gérer.

L'idée est donc bonne, mais pas aussi simple que cela. Il faut mettre en œuvre les chemins redondants, mais s'arranger pour qu'ils ne s'activent que lorsque ce sera nécessaire.

Tous les appareils compatibles IEEE 802.1d utilise le STP (Spanning Tree Protocol) : un algorithme permet de déterminer les liaisons à conserver (chemins courants) et les liaisons à désactiver (chemin invalidés), en fonction d'un coefficient fixé pour chacune par l'administrateur réseau et basé sur la qualité de la liaison, les volumes passants par la liaison, …

La représentation du réseau devient un arbre et plus un réseau, d'où le nom.