Les réseaux locaux virtuels (VLAN)

Objectif : Présenter la norme 802.1Q et les implémentations des constructeurs

Auteur : Roger SANCHEZ

Sommaire

Introduction : le retour de la couche 2

La technologie Ethernet s'est imposée ces dernières années face à ses concurrents, en offrant des débits de 100 Mb/s, 1 Gb/s et 10 Gb/s. Aujourd'hui seul ATM paraît en mesure encore de résister. Mais ceux qui prédisaient le tout ATM semblent s'être trompés, le marché des réseaux locaux se fonde, certainement durablement, sur Ethernet.
Cependant, l'accroissement du débit s'est accompagné d'un changement sur les structures d'interconnexion.

Ce n'est pas la première fois. L'histoire d'Ethernet est riche en versions: ALOHA, 10base5, 10base2, 10 BaseT, etc... Ces changements n'ont jamais affecté ni la structure de la trame (Ethernet II ou 802.3) ni la méthode d'accès (CSMA / CD).

Par contre l'évolution en cours remet en cause pour la première fois ces piliers technologiques d'Ethernet. En effet le « tout commuté » remplace ce qui était à la base la gestion d'une liaison multipoint par un ensemble de liaisons point à point. Cette modification profonde n'est pas sans conséquence sur la méthode d'accès, sur la notion de segment mais aussi sur la structure de la trame.

Mais la force d'Ethernet c'est d'avoir toujours su évoluer de façon cohérente, c'est à dire en préservant systématiquement la compatibilité ascendante, permettant ainsi de faire communiquer des structures de réseaux correspondant à des périodes historiques différentes. C'est peut-être cela qui crée quelquefois temporairement, des difficultés supplémentaires d'apprentissage.

L'objet de ce document est de présenter les réseaux locaux virtuels (Virtual Local Area Network – VLAN). C'est à dire la segmentation des réseaux permise par les commutateurs, une segmentation qui n'est plus physique mais uniquement logique. Ce document propose aussi une démarche d'apprentissage.

La plupart des ouvrages et des articles confondent la définition des principes d'un Vlan et leur méthode de construction (Vlan de niveau 1 2 3 .etc.). Cette approche rend plus difficile la compréhension et à fortiori l'explication de cette technologie en masquant les mécanismes mis en œuvre.

Créer et administrer des réseaux basés sur les Vlan nécessite d'aller au-delà de cette liste de niveaux. Il faut présenter la norme 802.1q qui définit les principaux concepts mis en œuvre, et montrer (comme pour le modèle OSI) comment elle se décline dans l'industrie.

Enfin il faut mesurer « l'intelligence » de plus en plus importante qui est associée aux éléments actifs de la couche 2 (carte réseau et commutateurs). En effet ce niveau du modèle OSI était essentiellement associé aux problèmes d'adressage en liaison avec la couche 3 où la majorité des traitements étaient détaillées. Aujourd'hui les technologies Vlan, qualité de service, authentification, Wi-Fi, (on peut même déclarer des « triggers » pour déclencher des scripts en fonction d'évènements sur un port) routage à la source, obligent à une redistribution des séquences d'enseignement.

Ce document respectera le plan suivant :

On rappellera dans un premier temps le principe de la commutation. On exposera la présentation classique de la notion de VLAN. Puis on approfondira la norme 802.1q en montrant ses écarts par rapport à la présentation classique. Enfin nous verrons quelques implémentations chez les constructeurs pour finir par des questionnements pédagogiques, et une suite de TP et d'exercices.

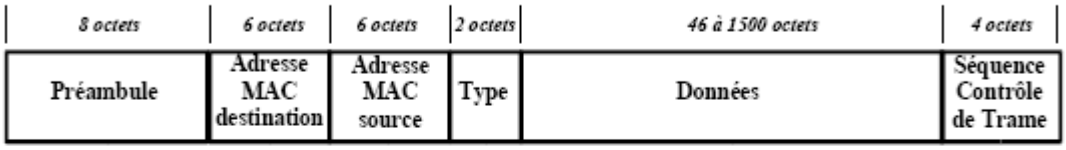
Les Vlan : approche usuelle

Rappels sur la commutation

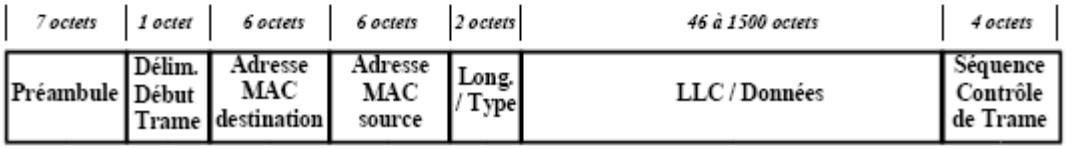
Contrairement à un concentrateur, un commutateur ne diffuse pas les trames. Il met en relation les seuls postes concernés par l'échange. Avant de réémettre les trames le commutateur vérifie que le support de communication est libre. Un commutateur évite donc les collisions au contraire d'un concentrateur.

A chaque fois qu'un message lui parvient, le commutateur associe le port par lequel arrive la trame à l'adresse matérielle (adresse MAC) de l'émetteur de la trame. Ainsi après un certain nombres de trames, le commutateur connaît « l'emplacement » (c'est à dire le port de rattachement) des postes sur le réseau et peut les mettre en relation deux à deux.

- Version Ethernet II (consortium DIX)



- Version IEEE 802.3



Cette association adresse MAC / port est gérée dans des tables d'association présentes dans chaque commutateur. Cette table est construite progressivement par apprentissage.

Si une trame contient une adresse de destination qui n'est pas présente dans la table, cette trame est transmise sur tous les ports du commutateur à l'exception du port émetteur de la trame. C'est aussi ainsi que sont traités les trames de diffusion.

Il y a d'un point de vue transversalité un algorithme intéressant proposé par l'exonet suivant :
www.reseaucerta.org/exonets/exonet52.htm

On distingue deux modes de fonctionnement du commutateur :

Store and forward : il stocke les trames entièrement avant de les réémettre. Il ne réémet donc pas les trames erronées (CRC "*Control Redundancy Check*" innatendu) ou en collision. Par contre ces commutateurs sont plus lents et nécessitent des mémoires tampons importantes

On the fly (appelé aussi *cut through* chez CISCO) : à la volée, les commutateurs réémettent immédiatement après lecture de l'adresse MAC destinataire, c'est plus rapide mais on propage les trames erronées - notamment les trames en collision et celles dont le CRC indique une erreur de transmission.

Le commutateur permet de garantir la bande passante d'un réseau. La bande passante c'est le débit d'un réseau. En ne diffusant pas à tous les postes mais aux seuls postes concernés par l'échange, le commutateur optimise l'utilisation de la bande passante. Ainsi un commutateur 100 mb/s de 12 ports garantira 100 mb/s par port alors qu'un concentrateur 100 mb/s de 12 ports divisera cette bande passante entre tous ses ports.

Ethernet commuté

L'actualité des architectures réseau est l'Ethernet entièrement commuté et donc la disparition progressive des concentrateurs. En utilisant uniquement des commutateurs, il n'y a plus de collision possible. Chaque port forme un mini-segment composé du commutateur et d'une carte ou aucune collision ne peut se produire.

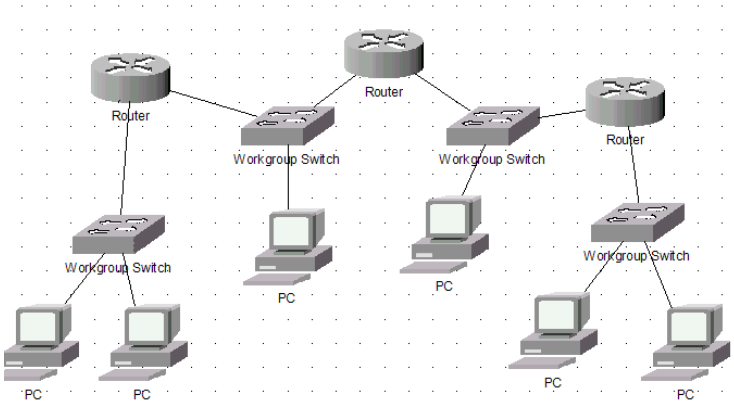
Dans ce cas, pendant l'émission d'une trame, la paire de réception n'est plus monopolisée par la détection de collision et on peut recevoir en même temps, c'est à dire travailler en mode bidirectionnel (*full duplex*).

Il faut souligner aussi que l'absence de collision supprime les limitations de distance que leur détection impliquait.

Dans une architecture entièrement commutée on met généralement en œuvre des interconnexions redondantes entre commutateurs pour garantir une plus grande tolérance aux pannes. Les liaisons redondantes doivent être invalidées quand elles ne sont pas utiles et validées en cas de rupture d'une liaison. Cette gestion de la redondance est prise en charge par le protocole 802.1d (arbre de recouvrement, en anglais *spanning tree*). voir le document : http://www.reseaucerta.org/cotecours/cotecours.php?num=259

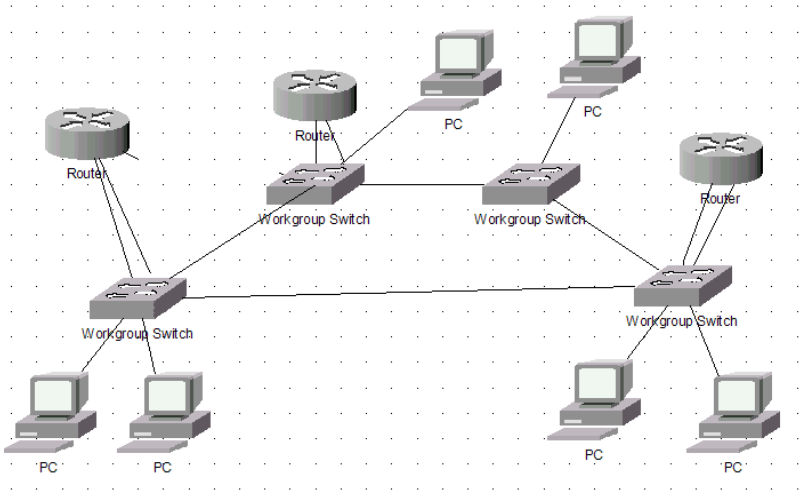
L'accroissement des domaines de diffusion

Avec les concentrateurs et les commutateurs de première génération, la séparation des flux gérés par la couche 2 ne peut se faire qu'en regroupant géographiquement les groupes de travail. En effet, si le commutateur segmente les domaines de collision, il maintient cependant un seul domaine de diffusion.



Segmentation des domaines de diffusion par les routeurs

Si l'interconnexion du réseau repose sur les commutateurs et non sur les routeurs (ce qui est de plus en plus le cas) cela pose deux problèmes :
les trames de diffusion sont propagées sur tout le réseau, or ces trames sont nombreuses (ARP, DHCP, Netbios, .etc.).
en mettant une carte réseau en mode 'promiscus' on peut capturer ces trames

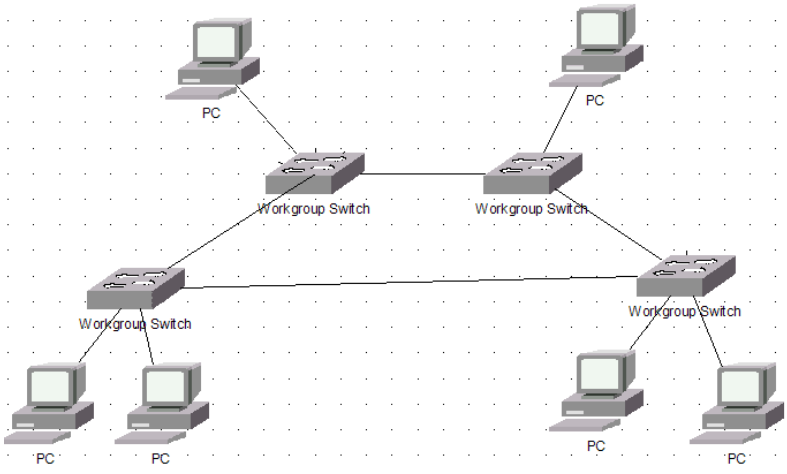


Un seul domaine de diffusion (avec liaison redondante)

La séparation et la sécurité des domaines de diffusion exigeaient, avant l'apparition des Vlans, une séparation géographique des domaines de diffusion et une interconnexion par routeur

Première définition des Vlan

Un VLAN permet de créer des domaines de diffusion (domaines de *broadcast*) gérés par les commutateurs indépendamment de l'emplacement où se situent les nœuds, ce sont des domaines de diffusion gérés logiquement



Domaines de diffusion logique et commutateurs/routeurs

Les avantages des VLANs sont les suivants :

La réduction des messages de diffusion (notamment les requêtes ARP) limités à l'intérieur d'un VLAN. Ainsi les diffusions d'un serveur peuvent être limités aux clients de ce serveur.
La création de groupes de travail indépendants de l'infrastructure physique ; possibilité de déplacer la station sans changer de réseau virtuel.
L'augmentation de la sécurité par le contrôle des échanges inter-VLAN utilisant des routeurs (filtrage possible du trafic échangé entre les VLANs).

L'indépendance entre infrastructure physique et groupe de travail implique qu'un commutateur puisse gérer plusieurs Vlan et qu'un même Vlan puisse être réparti sur plusieurs commutateurs. En conséquence, une trame qui circule dans un commutateur et entre les commutateurs doit pouvoir être associée à un Vlan.

Pour répondre aux objectifs des Vlan la règle suivante doit être impérativement respectée : une trame doit être associée à un Vlan et un seul et ne peut pas sortir du Vlan, sinon l'étanchéité du niveau 2 n'est plus respectée.

Les méthodes de construction d'un Vlan doivent donc déterminer la façon dont le commutateur va associer la trame à un Vlan. Usuellement on présente trois méthodes pour créer des VLAN : les vlan par port (niveau 1), les Vlan par adresses MAC (niveau 2), les Vlan par adresses IP (niveau 3) ainsi que des méthodes dérivées.

Les Vlan par port (Vlan de niveau 1)

On affecte chaque port des commutateurs à un VLAN.

L'appartenance d'une trame à un VLAN est alors déterminée par la connexion de la carte réseau à un port du commutateur.
Les ports sont donc affectés statiquement à un VLAN.

Si on déplace physiquement une station il faut désaffecter son port du Vlan puis affecter le nouveau port de connexion de la station au bon Vlan. Si on déplace logiquement une station (on veut la changer de Vlan) il faut modifier l'affectation du port au Vlan.

Les Vlan par adresse MAC (Vlan de niveau 2)

On affecte chaque adresse MAC à un VLAN.

L'appartenance d'une trame à un VLAN est déterminée par son adresse MAC. En fait il s'agit, à partir de l'association Mac/VLAN, d'affecter dynamiquement les ports des commutateurs à chacun des VLAN en fonction de l'adresse MAC de l'hôte qui émet sur ce port.

L'intérêt principal de ce type de VLAN est l'indépendance vis-à-vis de la localisation géographique. Si une station est déplacée sur le réseau physique, son adresse physique ne changeant pas, elle continue d'appartenir au même VLAN (ce fonctionnement est bien adapté à l'utilisation de machines portables).

Si on veut changer de Vlan il faut modifier l'association Mac / Vlan.

Les Vlan par adresse de Niveau 3 (VLAN de niveau 3)

On affecte une adresse de niveau 3 à un VLAN.

L'appartenance d'une trame à un VLAN est alors déterminée par l'adresse de niveau 3 ou supérieur qu'elle contient (le commutateur doit donc accéder à ces informations).
En fait, il s'agit à partir de l'association adresse niveau 3/VLAN d'affecter dynamiquement les ports des commutateurs à chacun des VLAN.

Dans ce type de VLAN, les commutateurs apprennent automatiquement la configuration des VLAN en accédant aux informations de couche 3. Ceci est un fonctionnement moins rapide que le Vlan de niveau 2.

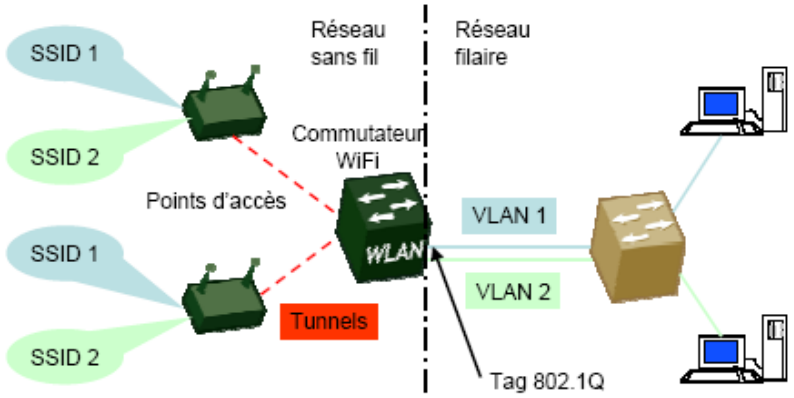
Quand on utilise le protocole IP on parle souvent de Vlan par sous-réseau.

Les autres méthodes pour définir des Vlan

On trouve dans la littérature des références au Vlan par protocoles
C'est à dire qu'on associe une trame à un Vlan en fonction du protocole qu'elle transporte. Ce protocole peut être un protocole de niveau 3 pour isoler les flux IP, IPX, Appletalk .etc…

Mais on peut trouver aussi des Vlan construits à partir de protocole supérieur (notamment H320). On parle quelquefois de Vlan par règles ou par types de service.

Enfin l'apparition du Wi-fi pose des problèmes de sécurité que les Vlan peuvent résoudre. Ainsi une solution basée sur des Vlan par SSID est envisageable.



Ce schéma est tiré d'un présentation faite par Sylvie Dupuis et Catherine Grenet le 13 Octobre 2004 à l'ENSAM (*www.cru.fr/nomadisme-**sans-fil**/J1310/cg-sd.pdf*)

Les questions qu'on est en droit de se poser

Peut-on associer une trame à plusieurs Vlan ?

En fonction de la règle énoncée plus haut, la réponse est toujours non. En effet une trame associée à un VLAN quelle que soit la méthode d'association ne peut être adressée qu'a une carte réseau associée à ce VLAN. Une trame de diffusion émise par une carte réseau associée à un VLAN sera transmise à toutes les cartes réseaux composant ce VLAN et uniquement à celles-ci.

Cela implique-t-il qu'un port de commutateur ne doit être associée qu'à un seul Vlan ?

Car si un port est associé à plusieurs Vlan, à quel Vlan associe-t-il la trame qu'il reçoit ?
Et s'il n'est associé qu'à un seul Vlan comment répartir un Vlan sur plusieurs commutateurs, car les ports d'interconnexion doivent pouvoir faire transiter des trames en provenance de différents Vlan ? Une réponse serait de mettre en place des Vlan de niveau 2 mais alors qu'en est-il pour les Vlan de niveau 1 ?

La carte réseau d'un poste peut-elle être associée à plusieurs Vlan ?

Si oui comment savoir à quel Vlan appartient une trame émise par une telle carte réseau ? Si non comment partager l'accès à des ressources communes entre différentes Vlan ? Une réponse serait des Vlan de niveau 3 mais alors qu'en est-il pour le niveau 1 et le niveau 2 ?

Comment communiquer entre les Vlan ?

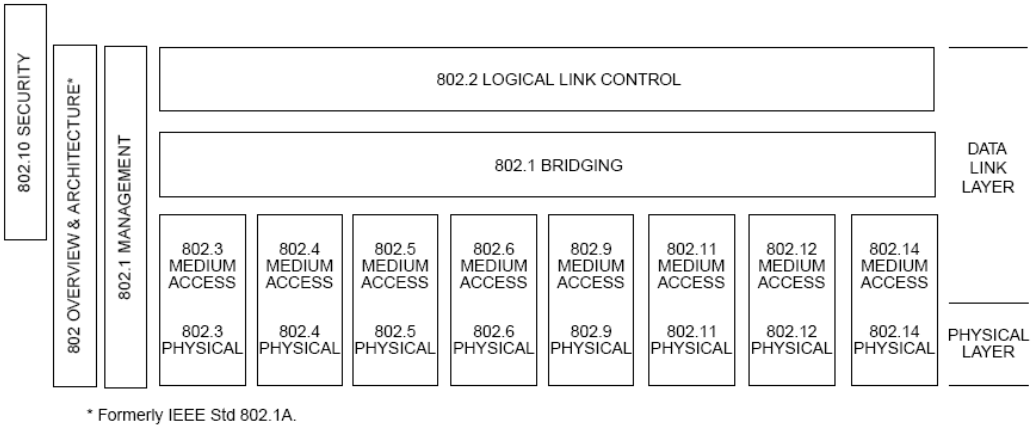
L'étanchéité de la couche 2 implique de remonter jusqu'à la couche 3 pour l'échange entre Vlan. Cet échange peut donc être entièrement contrôlé.

La norme 802.1Q

Les schémas de ce paragraphe sont issus de la norme 802.1Q publiée par l'IEEE.

Introduction

La norme 802.1q date de décembre 1998, c'est donc une norme récente. Une amélioration a été proposée en octobre 2003 pour réduire le trafic du protocole GVRP (Compact-GVRP). La norme 802.1Q dépend de la norme ISO/IEC 15802-3 qui définit les principaux concepts utilisés par la norme. Elle reprend « l'étiquette » définit par la norme 802.3ac en spécifiant l'utilisation des champs.
Où s'insère la norme ?



Les types de trames

La norme définit trois types de trames :
les trames non étiquetées (untagged frame)
les trames étiquetées (tagged frame)
les trames étiquetées par une priorité (priority-tagged frame)

Une trame non étiquetées est une trame qui ne contient aucune information sur son appartenance à un Vlan.
Une trame étiquetées est une trame qui contient une entête supplémentaire. Cette entête modifie le format standard d'une trame, notamment de la trame 802.3.

Le format d'une trame étiquetée 802.1Q est le suivant :

Adresse destination : 6 octets
Adresse Source : 6 octets
VPID (Vlan Protocol Identifier) : 2 octets. Fixé à 0x8100 . Attention à ne pas confondre avec l'identifiant d'un VLAN. Ici il s'agit d'identifier une trame de type 802.1q
UP (User priority) : 3 bits. Permet de définir 8 niveaux de priorités. Utilisé par le protocole 802.1p.
CFI (Canonical Format Identifier) : 1bit. indique que le format est standard (utilisé par le routage par la source)
VID (Vlan Identifier) : 12 bits. Indique sur quel Vlan circule la trame.
Longueur/type : 2 octets. En 802.3 donne la longueur de la trame. En Ethernet II ou DIX(Digital Intel Xerox) indique le type de données transporté.
Données : 46 à 1500 octets
FCS : 4 octets. Frame Check Sequence.

La modification de l'entête implique que les éléments recevant la trame étiquetée (taggée) disposent du protocole 802.1q. Ce n'est généralement pas le cas de la majorité des cartes réseaux aujourd'hui.

Une trame étiquetée par une priorité est une trame dont l'entête 802.1Q contient le champ priorité (UP) renseigné mais dont l'identifiant de Vlan (VID) est à zéro. ***Remarque : la gestion des priorités est plutôt définie par la norme 802.1p.***

Remarque : dans cette présentation il n'est pas fait mention du « routage à la source de niveau 2 » champ « E-RIF » (Embedded Route Information Field) défini par la norme. La présence de ce champ est indiquée par le CFI (Canonical Format Identifier). Il est situé après la longueur (ou type) de la trame. Il se décompose en un champ RC (Route contrôle Field) de 2 octets (indiquant sa longueur LT (length)) et au maximum de 28 octets

Définitions dépendant du type de trame

Un Vlan est un sous-ensemble d'une topologie active d'un réseau local commuté. Ce sous-ensemble est identifié par un VID (Vlan Identifier).

Un élément actif d'un réseau est dit « vlan informé » (Vlan-aware) s'il reconnaît les trames étiquetées. Il est dit « Vlan non-informé » (Vlan-unaware) dans le cas contraire.

Un réseau local virtuel est un réseau où l'existence d'éléments actifs « Vlan informé » (Vlan-aware) permet la création, la modification et la maintenance de Vlan.

L'architecture logique d'un commutateur « vlan informé » est la suivante :

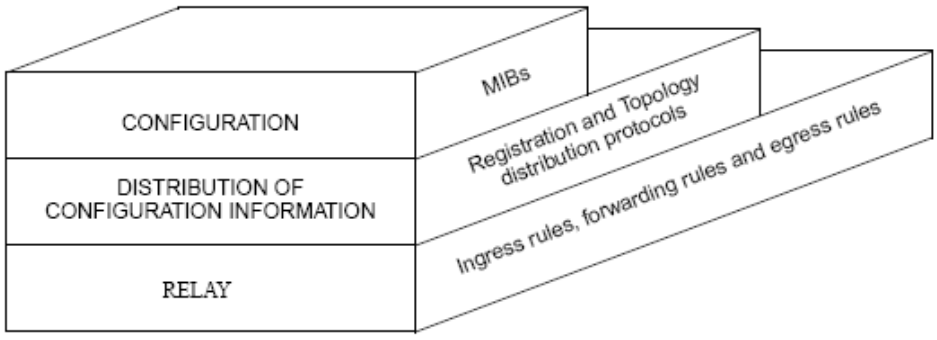


Figure 6-1—VLAN architectural framework

La partie configuration définit les éléments de la Mib (Management Information Base) liés au VLAN qui seront utilisés par le protocole SNMP (Single Network Management Protocol). Elle définit aussi les commandes administratives nécessaires à la gestion des Vlan.

La partie « distribution » se préoccupe des éléments liés à la définition automatique des Vlan et leur propagation dans un réseau. Cette partie dans la norme est prise en charge par le protocole GVRP (GARP Vlan Registration Protocol).

La partie « relay » définit le processus de traitement d'une trame par un commutateur « Vlan informé ».

La commutation de trames dans un commutateur « Vlan informé »

Le processus de commutation (relay) se décompose en trois opérations :

Les opérations liées au traitement d'une trame en entrée d'un port « vlan informé ». Elles sont contrôlées par des règles d'entrée (ingress rules)

Les opérations liées à la décision de commutation (forwarding process) d'une trame prise par un commutateur « vlan informé ». Elles sont contrôlées par des tables de filtrage (filtering database) qui répertorient les associations entre ports et adresses Mac et entre port et Vlan. On associe à ces opérations les opérations de gestion de priorité si celles-ci sont actives. Dans ce cas il y a une table des priorités qui associe une file d'attente à chaque niveau de priorité (8 maximum).

Les opérations liées au traitement d'une trame en sortie d'un port « vlan informé ». Elles sont contrôlées par des règles de sorties (egress rules). Il faut éventuellement ajouter ou retirer une étiquette à la trame et recalculer le FCS.

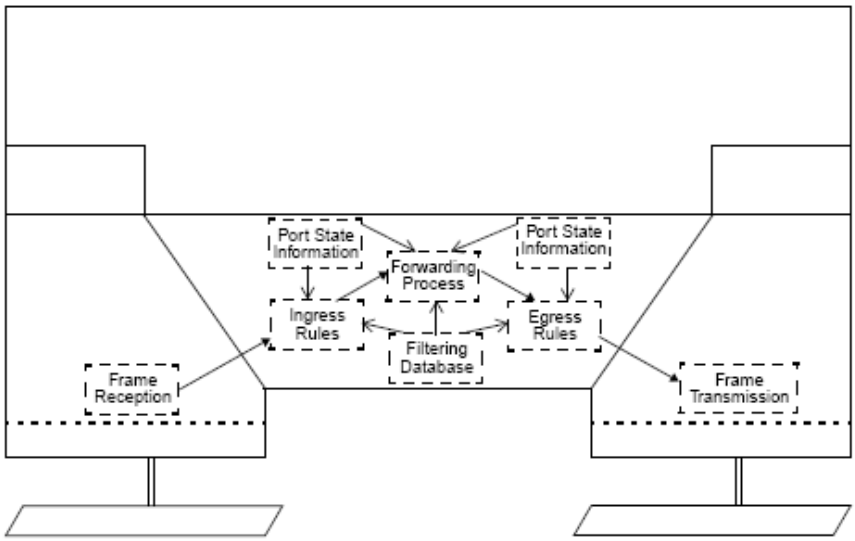


Figure 8-4—Relaying MAC frames

Les règles d'entrée permettent de classer les trames reçues dans un et un seul Vlan. Si cela n'est pas possible la trame est détruite.

La table de filtrage permet de définir les ports sur lesquels la trame doit être transmise.

Les règles de sortie permettent d'éliminer les trames qui ne correspondent pas aux Vlan associés au port et de déterminer le format dans laquelle la trame doit être transmise.

Remarque : on ne détaille pas ici la notion d'IVL (Independant Vlan) et SVL (Shared Vlan) au niveau des tables de filtrage. Schématiquement, les commutateurs de type SVL connaissent l'ensemble des associations mac/vlan réparties sur chaque commutateur (ce qui suppose des échanges importants) et les commutateurs de type IVL n'ont connaissance que de la table mac/vlan associée à leurs ports.

Les types de port dans un commutateur « Vlan informé »

Les paramètres associés à un port (Port State Information) sont entre autres son type (tagged, untagged, priority tagged) et les Vlans auxquels il participe (les PVID, Port Vlan Identifier).

Une trame en entrée ne comportant pas de VID ou bien un VID nul sera associée à un Vlan soit en fonction des paramètres du port de réception soit en fonction d'extensions propriétaires non définies par le protocole 802.1Q. Une trame en entrée doit toujours être associée à un VID. Un port peut admettre toutes les trames ou seulement les trames « étiquetées ». Si la trame n'est pas étiquetée et que le port n'est pas étiqueté, la trame sera associée au PVID du port (qui doit alors être unique) sinon elle est détruite.

Une trame en sortie dont l'association avec un Vlan ne correspond pas au(x) PVID du port en sortie sera détruite.

Un port « étiqueté » transmet des trames étiquetées mais peut traiter des trames non étiquetées.
Un port « non étiqueté » transmet des trames non étiquetées mais peut traiter des trames étiquetées (en enlevant notamment l'étiquette).
Enfin un port « étiqueté par une priorité » transmet des trames « étiqueté par une priorité » mais peut traiter les autres types de trames.

Un commutateur peut avoir des ports de différents types en même temps.

Déclaration des Vlan et affectation des ports à un Vlan

Un port sur un commutateur ne peut participer qu'aux Vlan déclarés sur ce commutateur. La déclaration des Vlan est donc préalable ou conjointe à l'affectation des ports aux Vlan.

La déclaration de Vlan consiste à créer un VID sur un commutateur. Cette création peut être statique (Static Vlan) ou dynamique (Dynamic Vlan).

Un Vlan statique est un Vlan créé manuellement sur le commutateur.

Un Vlan dynamique est un Vlan dont la création sur le commutateur résulte d'un échange avec un autre commutateur.

La création dynamique des Vlan permet de contrôler celle-ci à partir de un ou plusieurs commutateurs et d'éviter ainsi les erreurs sur les identifiants (VID) quand un Vlan est réparti sur plusieurs commutateurs (voir exemples plus bas).

L'affectation d'un port à un Vlan peut être statique ou dynamique. Cela donne les cas de figure suivants :

Ports/Vlan	Statique	Dynamique
Statique	X	X
Dynamique	X	X

A l'état initial un commutateur comporte un Vlan statique, le Vlan par défaut et tous les ports sont affectés à ce Vlan

La création statique des Vlan et l'affectation statique des ports se fait via les commandes d'administration du commutateur.

La création dynamique des Vlan et l'affectation dynamique des ports se fait via le protocole GVRP qui doit être activé sur le commutateur.

Le protocole GVRP (norme 802.1Q)

Présentation

Le protocole GVRP est basé sur un échange de BPDU (Bridge Protocol Data Unit) entre les commutateurs. L'adresse MAC associée est « 01-80-C2-00-00-21 ».

Si le GVRP est actif sur un commutateur, le protocole GVRP est alors actif au niveau de chaque port du commutateur. Mais le protocole GVRP peut être actif aussi au niveau d'une carte réseau. Il est composé d'une partie applicative (GVRP application), des messages échangés (GID GARP Information Déclaration) entre ports de commutateurs différents ou avec les cartes réseaux et des messages échangés entre ports sur un même commutateur (GIP GARP Information Propagation).

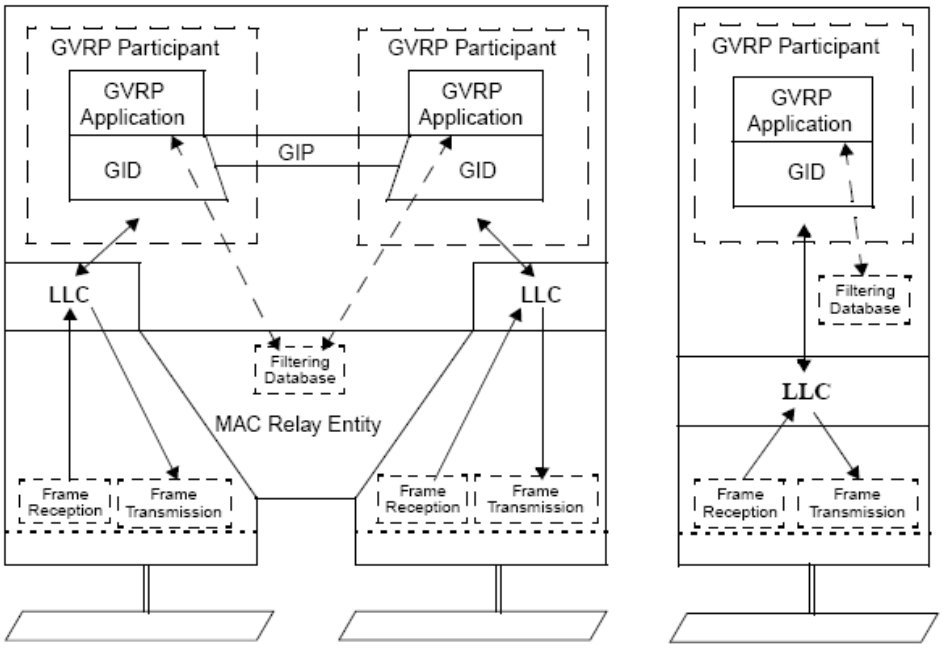


Figure 11-1—Operation of GVRP

Schéma issu de la norme 802.1Q

GVRP doit permettre à un membre participant (GVRP-enabled et GVRP-aware) à l'échange GVRP de déclarer l'ensemble des Vlan auxquels il participe ce qui veut dire qu'il doit recevoir aussi le trafic associé à ces Vlan (s'il lui est adressé bien sûr). Cette opération est un enregistrement (Register).

Un participant doit aussi pouvoir se désaffecter d'un Vlan, c'est une opération de dé-enregistrement (De-register).

A la réception d'un enregistrement GVRP, un port participant au GVRP enregistre dans la table de filtrage du commutateur une association entre lui et les Vlan déclarés dans le GID (affectation dynamique). Attention il faut que la limite de la table de filtrage n'ai pas été atteinte. Le port va ensuite propager (GIP) l'information aux autres ports du commutateur. Ceux-ci vont transmettre l'information sans s'affecter dynamiquement au Vlan. Le comportement d'un port est donc différent selon que l'information GVRP lui parvient à travers un GID ou un GIP.

Un port affecté dynamiquement est implicitement un port « étiqueté ».

Premier exemple

Double propagation d'information GVRP avec affectation des ports

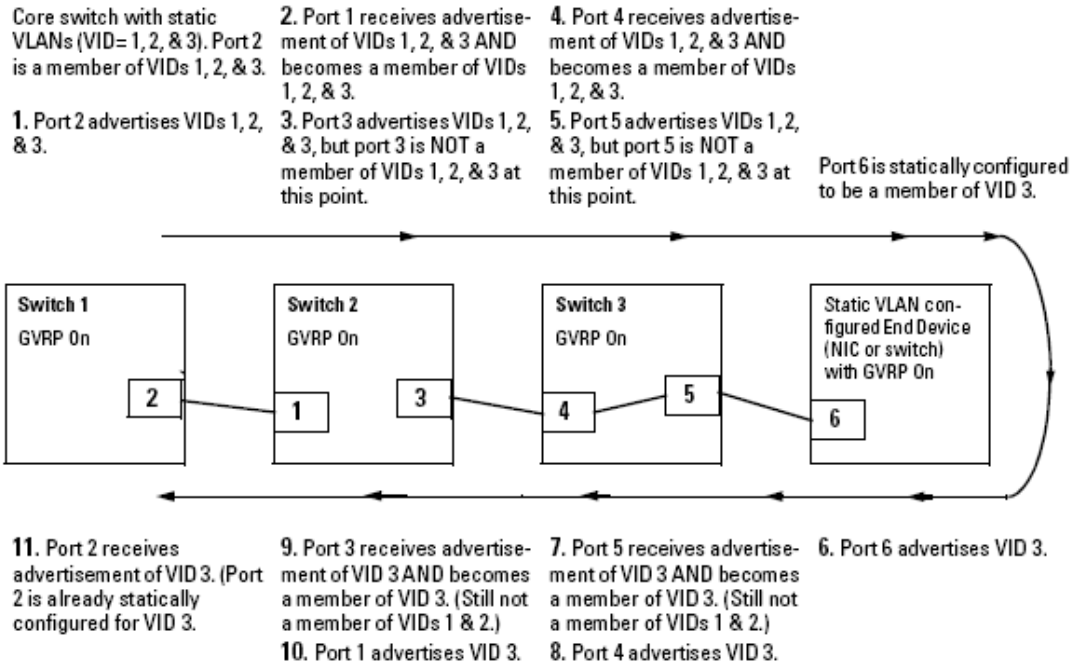


Figure 9-57. Example of Forwarding Advertisements and Dynamic Joining

schéma issu du hp2524mgmnt&config guide.pdf

Deuxième exemple

Propagation de la déclaration des VID à partir d'un serveur source puis affectation des ports.

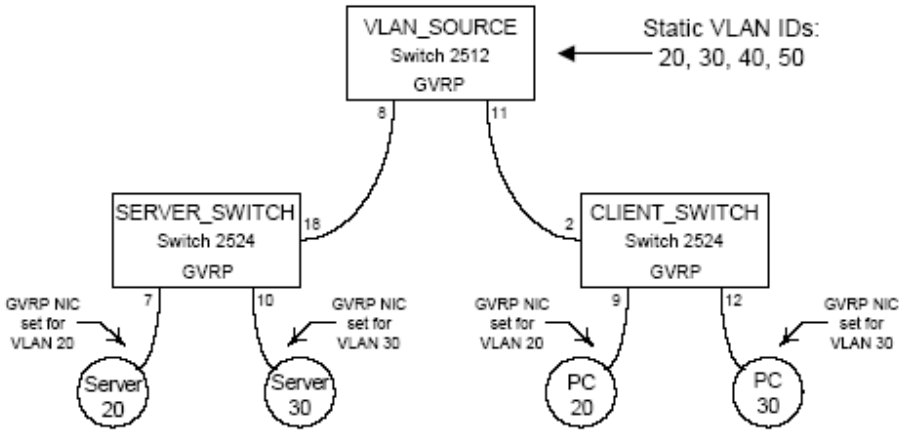


schéma issu du document gvrp_use.pdf du site Hewlett Packard

Paramétrage des ports associés à l'affectation dynamique de Vlan

Par rapport au protocole GVRP un port peut être dans trois états :

Apprentissage (learn)
Bloqué (block)
Non actif (disable)

Un port qui reçoit un GID annonçant (advertisement) un Vlan non déclaré sur le commutateur (Unknown Vlan) réagira en fonction de son état :
apprentissage : il crée le Vlan, s'associe à lui et propage le GIP
bloqué : il ne s'associe pas au Vlan mais propage le GIP
non actif : il ne s'associe pas au Vlan et ne propage pas le GIP

Un port qui reçoit un GID annonçant (advertisement) un Vlan déclaré sur le commutateur (static Vlan) réagira en fonction de son état :
apprentissage : il s'associe à lui et propage le GIP
bloqué : il s'associe au Vlan et propage le GIP
non actif : il ne s'associe pas au Vlan et ne propage pas le GIP

Si un Vlan statique est déclaré sur le commutateur et que les ports sont déjà affectés à ce Vlan, le comportement sera le suivant (HP procurve 2512 et 2524) :

Table 9-9. Controlling VLAN Behavior on Ports with Static VLANs

Per-Port "Unknown VLAN" (GVRP) Configuration	Per-Port Static VLAN Options [1]		
	Tagged or Untagged[2]	Auto[2]	Forbid[2]
Learn (the Default)	Generate advertisements. Forward advertisements for other VLANs. Receive advertisements and dynamically join any advertised VLAN.	Receive advertisements and dynamically join any advertised VLAN that has the same VID as the static VLAN.	Do not allow the port to become a member of this VLAN.
Block	Generate advertisements. Forward advertisements received from other ports for other VLANs. Do not dynamically join any advertised VLAN.	Receive advertisements and dynamically join any advertised VLAN that has the same VID.	Do not allow the VLAN on this port.
Disable	Ignore GVRP and drop all GVRP advertisements.	Ignore GVRP and drop all GVRP advertisements.	Do not allow the VLAN on this port.

[1] Each port of a Series 2500 switch must be a Tagged or Untagged member of at least one VLAN. Thus, any port configured for GVRP to Learn or Block will generate and forward advertisements for the static VLAN(s) for which it has been configured as Tagged or Untagged . By default, all ports are Untagged members of the default VLAN (VID = 1). See the "Note" on page page 9-78.

[2] To configure tagging, **Auto**, or **Forbid**, see "Configuring Static VLAN Name and Per-Port Settings" on page 9-67 (for the CLI) or "Adding or Changing a VLAN Port Assignment" on page 9-60 (for the menu).

Les questions auxquelles on va maintenant répondre

Une trame peut-elle appartenir à plusieurs Vlan ?

Non. Rien de changé, mais là c'est définitif, en effet l'entête 802.1Q n'admet qu'un seul identifiant VLAN (VID) pour une trame

Un port peut-il appartenir à plusieurs Vlan ?

Oui. Mais si une trame non étiquetée arrive sur ce port il doit pouvoir l'associer sans ambiguïté avec un VID. Dans la pratique les ports seront affectés à un seul Vlan et les ports d'interconnexion entre commutateurs à plusieurs Vlan. En fait un port qui reçoit une trame non étiquetée en réception ne doit avoir qu'un seul PVID actif ou bien doit disposer d'un moyen pour associer cette trame à un VLAN. Ce moyen est forcément un champ quelconque de la trame, et ce moyen n'étant pas spécifié par la norme sera forcément propriétaire.

Un poste peut-il appartenir à plusieurs Vlan ?

Oui. Mais alors la carte réseau du poste doit être « vlan informé » et toutes les trames émises et reçues par ce poste seront étiquetées. Le port de raccordement au commutateur sera lui aussi étiqueté. *Voir le TP sous Linux.*

L'exemple suivant est donné dans la documentation de l'Allied 8800.

Figure 14: VLANs with tagged ports.

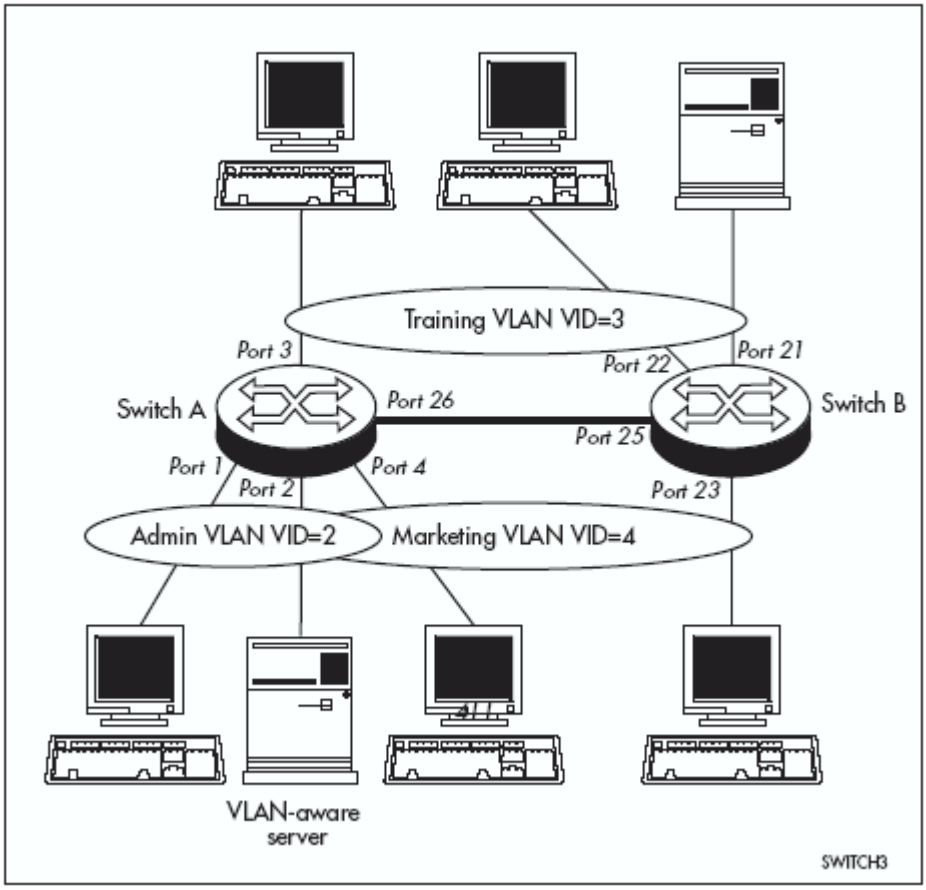


Table 12: VLAN membership of example of a network using tagged ports.

VLAN	Member ports
Training	3, 26 on Switch A
	21, 22, 25 on Switch B
Marketing	2, 4, 26 on Switch A
	23, 25 on Switch B
Admin	1, 2 on Switch A

Où sont les Vlan de niveau 1 2 3 .etc. dans la norme 802.1Q?

La norme ne fait référence explicitement qu'aux Vlan par port (*port-based Vlan*). Dans ce type de Vlan, l'association d'une trame à un Vlan est déterminée par l'appartenance du port à un Vlan. *Seuls les ports d'interconnexion ou les ports où sont connectés des machines « vlan informées » devraient donc avoir plusieurs Vlan associés*.

La norme ne fait aucune référence à d'autres catégories, mais elle ne s'y oppose pas. Le mécanisme d'association d'une trame non étiquetée à un Vlan n'est alors pas défini. Les constructeurs ont donc toute liberté pour proposer une solution.

Cette solution doit bien sûr être compatible avec la norme.

Remarque : si tous les éléments actifs sont « Vlan aware » (y compris les postes de travail) l'association de la trame à un Vlan se fera par celui qui émet la trame, et là tout est envisageable. Cependant la sécurité devra être redéfinie car il serait très simple d'associer un poste à un Vlan *(Voir TP sous Llinux).* La norme 802.1x spécifie des solutions d'authentification au niveau de la couche 2.

Quelques implémentations des Vlan par les équipementiers et les didacticiens ☺

Introduction

Cette partie ne prétend pas à l'exhaustivité mais veut présenter l'approche retenue par quelques constructeurs pour la mise en œuvre de Vlan. On présentera aussi ici l'approche du « simulateur réseau » comme un constructeur parmi d'autres mais qui a le mérite d'être immédiatement disponible et surtout de montrer visuellement les concepts.. Enfin on parlera de l'implémentation Linux qui permet à ce système d'être Vlan-informé (Vlan Aware).

La plupart des commutateurs disposent d'un langage de commande utilisable à partir d'un port console ou de « telnet », ou bien encore d'une interface Web.

Commutateur CISCO 2950 (un best seller CISCO)

CISCO leader du marché a contribué activement à l'élaboration des normes.
Un commutateur CISCO utilise différents protocoles associés au VLAN : ISL, CDP, VTP, 802.1Q et VMPS. Seul 802.1Q n'est pas propriétaire.

ISL (Inter-switch Link) est un protocole d'étiquetage de trames au même titre que 802.1Q mais l'étiquette est placé en en-tête de trame et ne comporte pas les mêmes informations (30 octets répartis sur treize champs).

CDP (Cisco Discovery Protocol) est un protocole qui permet aux commutateurs de propager des informations sur leurs caractéristiques.

VTP (Vlan Trunk protocol) est un protocole qui permet de gérer dynamiquement les Vlan au même titre que GVRP.

VMPS (VLAN Management Protocol Server) est un protocole client/serveur (le 2950 est un client) qui permet à un port d'interroger un serveur VMPS pour associer une trame à un Vlan. Ce serveur VMPS peut être situé sur un autre commutateur ou sur un serveur Windows 200x. Il est intéressant ici de constater qu'on ne se préoccupe pas de niveau 2 3 4 .etc. Ce qui est important c'est d'associer la trame à un VLAN peu importe le critère d'association choisi. En procédant avec un modèle client/serveur CISCO répond à tous les besoins, en effet du point de vue du commutateur client il faut

envoyer les critères de décision (tous les éléments de la trame sont candidats à l'être) à un programme chargé de prendre le décision et de la renvoyer.

Un 2950 distingue deux types de liens : les liens « access-link » et les liens « trunk link ». Un lien access link est un lien où la trame qui circule n'a pas d'étiquette. Un lien trunk link est un lien où la trame qui circule comporte une étiquette ISL ou 802.1Q.

Un port access-link n'est associé qu'à un seul Vlan. Un port trunk link est associé à tous les Vlan (sur ce point on s'éloigne de la norme)

L'association entre trame et Vlan se fait soit par le port, soit par une réponse à une requête VQP (Vlan Query Protocol) adressée à un serveur VMPS. Dans ce cas le port est affecté dynamiquement au Vlan et reste affecté à ce Vlan tant que le port est actif.

Un port miroir est attaché à un Vlan.

Un « Private port » isole le trafic entre ports appartenant à un même Vlan. Ces ports doivent passer par un port maître (l'exemple classique est la chambre d'hôtel, on met toutes les chambres dans le même Vlan pour offrir un accès Internet mais on empêche une chambre d'avoir accès au flux d'une autre chambre. Certains « hébergeurs » l'utilisent pour dissocier leur client tout en les gérant dans un même Vlan).

Remarque : dans la terminologie CISCO un lien trunk correspond à un lien étiquetée alors que pour la plupart des autres constructeurs un lien trunk correspond à une agrégation de liens (notamment chez Allied-Telesyn et HP) Une agrégation de liens chez CISCO est un Etherchannel.

Allied-Telesyn AT- S68

Ce commutateur permet de créer des Port based VLAN uniquement. Il n'y a pas de fonction de routage prise en charge.

Les ports ne sont pas « vlan-informé » et ne mettent donc pas d'étiquettes 802.1Q dans la trame. Si on veut relier les commutateurs entre eux et que les Vlan sont répartis il faudra donc prévoir autant de liens que de Vlan car chaque port d'interconnexion ne sera affecté qu'à un seul Vlan.

Le AT-FS7016 et AT-FS7024 permettent a priori d'affecter un port à plusieurs Vlan pour gérer l'interconnexion. Cependant il n'est pas précisé si ce port est « vlan informé » ou pas. Mais l'exemple donné laisse supposer qu'il s'agit de partager une ressource non « vlan informé » dans ce cas le port est forcément « non étiqueté ».

Un port miroir peut « mirrorer » 23 autres ports qui doivent être sur le même commutateur mais pas forcément sur le même Vlan.

Un lien trunk correspond à une agrégation de liens.

Ce commutateur gère la qualité de service, donc a priori les trames « étiquetées par une priorité » le VID reste nul (on gère 802.1P et non 802.1Q).

Allied-Telesyn 8800 (commutateur / routeur)

Ce commutateur associe des fonctions de routage et de commutation.

Il y a une fonction de limitation du nombre de trames par port par secondes (Packet storm) qui permet de limiter les flux.

On a aussi la possibilité d'autoriser ou non des adresses mac sur un port (256 maximum), cette fonction est appelée « port security ».

Le port miroir est le seul port non affecté à un Vlan, on peut donc « mirrorer » tous les ports du commutateur quel que soit leur Vlan d'appartenance.

Enfin les ports « trunk » sont des ports d'agrégat.

Ce commutateur accepte les trames étiquetées et non étiquetées et dispose donc de ports étiquetés et non étiquetés. Chaque trame traitée par le commutateur est associée à un VID.

Si une trame arrive sur un port étiqueté, elle est associée au Vlan correspondant au VID de la trame.
Si une trame arrive sur un port non étiqueté elle est associée au VID du port.
Remarque : ce n'est pas tout à fait conforme à la norme.

Un port peut appartenir à plusieurs Vlan si et seulement si, ce port est un port étiqueté. Les ports d'interconnexion doivent être étiquetés.

Ce commutateur gère le protocole GVRP.

Les règles à respecter sont les suivantes :
Chaque port doit appartenir a au moins un Vlan statique (sauf le port miroir)
Un port non étiqueté appartient à zéro (défaut) ou un Vlan. Ce port transmet des trames non étiquetées pour ce Vlan
Un port étiqueté peut l'être pour zéro (défaut) ou plusieurs Vlan. Ce port ne transmet que des trames pour ces Vlan et ces trames sont étiquetées, (l'étiquette a été mise à la réception de la trame par un port ou à l'envoi de celle-ci)
Pour un même Vlan un port ne peut pas être étiqueté et non étiqueté
Le port miroir n'est affecté à aucun Vlan

Le commutateur associe des fonctions de routage et de commutation.

On associe le VID d'un Vlan à une interface. L'interface est en fait purement virtuelle. Puis on associe à cette interface une adresse IP et un masque, éventuellement le protocole de routage RIP.

Allied Telesyn 4400 (un routeur / commutateur)

Un routeur dans la liste cela peut surprendre mais…il s'agit d'un routeur Vlan informé.

Dans ce routeur, les interfaces Ethernet sont considérées comme des ports de switch appartenant à un Vlan. Chaque Vlan est associé à une interface virtuelle. Le routage se fait entre deux Vlan (mécanisme assez proche de l'AT 8800).

A voir en pratique.

HP procurve 2524 *(best seller HP)*

Ce commutateur HP respecte assez bien la norme 802.1Q.
Il gère des ports "tagged", "untagged" et "priority tagged".
Et il implémente le protocole GVRP.

Simulateur réseau (constructeur CERTA ☺)

Le simulateur s'est inspiré de CISCO et de fait respecte l'approche vlan « port based » définie par la norme 802.1Q.

On utilise des ports « non vlan informés » (untagged) pour connecter les stations et des ports 802.1Q (« vlan informé » ou « tagged ») pour l'interconnexion des commutateurs.

Il y a deux niveaux de Vlan traités, le Vlan par port et le Vlan par adresses Mac.

La gestion des Vlan par adresses MAC est gérée par l'intermédiaire d'une table Mac/Vlan configurée sur chaque commutateur. Une fois l'association faite on affecte dynamiquement le port au VLAN et cette association reste tant que le port est actif (comme avec VMPS sur CISCO).

Indépendamment d'une utilisation en démonstration ou en TP, on peut aussi ici montrer une implémentation algorithmique associée à un commutateur

Linux

Linux implémente la prise en charge du protocole 802.1Q, et permet donc à la carte réseau d'être « vlan informé » (Vlan aware).

La version de noyau doit être supérieure à 2.4.14.
Sur une distribution Debian, la commande "grep VLAN /usr/src/linux" doit répondre "CONFIG_VLAN_8021Q=y"

La suite de commandes suivantes teste la présence du module 802.1Q, inhibe l'interface « réelle » puis l'associe au vlan 2 avec une adresse IP.

```
modprobe 8021q
ifconfig eth0 0.0.0.0 up
vconfig add eth0 200
ifconfig eth0.200 192.168.50.1 up
```

Travaux pratiques et exercices

Travaux pratiques sur commutateur

La progression des TP est la suivante avec des commutateurs :

Configurer deux vlan sur un commutateur et les faire communiquer par un routeur
Configurer deux vlan sur deux commutateurs et les faire communiquer par un routeur connecté à un seul commutateur
Configurer deux vlan répartis sur deux commutateurs et les faire communiquer par un routeur connecté à un seul commutateur

Ces TPs ne détaillent que les objectifs. Il n'y a pas de mode opératoire associé. Il faut consulter la documentation des commutateurs et trouver les commandes suivantes :

Création d'un Vlan
Affectation d'un port « non-étiqueté » (untagged) à un Vlan
Création d'un port miroir
Création d'un port « étiqueté » (tagged) ou d'un port trunk (cisco) pour l'interconnexion (dans le cas d'un commutateur qui ne dispose pas de cette fonctionnalité, il faut autant de liaisons entre commutateurs que de Vlan à transporter, c'est le cas du AT S68)

Si on dispose de commutateur / routeur, il faut consulter les commandes qui permettent le routage entre Vlan (voir plus haut AT 8800).

Si on dispose de routeur les commandes sont supposées connues.

La mise en œuvre peut être simple et avec un mode opératoire bien rédigé on peut faire monter des architectures complexes à un étudiant qui ignore ce qu'est une adresse Mac. Ce n'est pas le but de ces Travaux pratiques.

Le premier objectif est de bien dissocier les logiques couche 2 et couche 3. On montre notamment que deux postes sur un même réseau IP et sur un même commutateur ne peuvent pas communiquer s'ils sont sur des Vlan différents. On montre aussi que deux postes sur des réseaux IP différents non reliés par un routeur et qui sont sur un même Vlan, communiquent cependant par la couche 2.

Le deuxième objectif est de dissocier l'organisation physique de l'interconnexion de l'organisation logique de la communication. On montrera l'interconnexion de commutateurs et la répartition des Vlan.

L'utilisation d'un analyseur de trames est indispensable.

Travaux pratiques avec le simulateur Boson

Merci à Pierre-Alain Goupille pour avoir été le premier à explorer ce produit.

Le simulateur boson (*www.boson.com*) payant, permet de simuler partiellement le comportement d'un commutateur 2950 (et d'autres produits CISCO).

BOSON est un produit destiné à l'origine à la préparation des certifications CISCO. Il est d'ailleurs livré avec une série de « labs » préparatoires aux examens.

BOSON est composé de deux modules :

Network designer qui permet de dessiner des architectures réseaux
Network sim qui simule le comportement des architectures

Les architectures intègrent des routeurs, des commutateurs et des PC.

Avec le simulateur on travaille en mode console (simulation telnet).
On choisit l'élément sur lequel on travaille, une console s'ouvre et on peut utiliser une grande partie des commandes IOS associées à cet élément pour le paramétrer.
Une fois la configuration terminée on peut la tester (commande *ping* sur les PC).

On ne peut pas cependant créer de port miroir ni faire de l'analyse de trames. Attention, dans la version testée, Boson fait communiquer deux postes si ils sont sur le même réseau IP mais pas sur le même Vlan (bug ?), c'est à dire que la diffusion ARP n'est pas limitée au VLAN.

Donc, plutôt pour les amateurs de CISCO (qui ont des moyens financiers limités ;-)), c'est extrêmement pratique pour enseigner le langage de commandes Cisco .

Remarque : Freddy Didier a exploré le logiciel de simulation Packet Tracer 3.2.

Travaux pratiques avec le simulateur réseau du CERTA

Rappelons que Pierre Loisel est l'auteur de ce chef d'œuvre.

Avec le simulateur réseau la progression des TP VLAN est la suivante:

Fiche 5 : les Vlan par port
Fiche 6 : les Vlan par adresses MAC
Fiche 10 : Routage inter-Vlan

Bien sûr la lecture des fiches intermédiaires peut s'avérer nécessaire.

Le grand intérêt ici est la visualisation des opérations et la décomposition algorithmique des opérations effectuées par les commutateurs et les routeurs.

Mais c'est aussi le seul produit présenté ici qui permet de montrer simplement le comportement d'un Vlan par adresses Mac.

Travaux pratiques sur Linux

Ce TP a été réalisé avec un poste sous Fedora core 1 qui intègre le module 8021Q.

L'avantage ici c'est d'avoir une chaîne de liaison entièrement « Vlan informé ».

Le TP configure un serveur de ressources et un serveur DHCP accessible sur un seul poste équipé d'une seule carte réseau mais appartenant cependant à 2 vlans. Deux autres postes appartenant chacun à un VLAN se voient servir une adresse IP par le serveur DHCP.

Le poste LINUX est connecté à un port forcément « étiqueté » appartenant aux deux VLAN. Les autres postes sont connectés à des ports « non étiquetés » appartenant bien sûr à un seul VLAN.

Le fait d'être Vlan informé, permet à un poste Linux équipé d'un analyseur de trames comme Ethereal de capturer des trames 802.1Q.

Mais on peut aussi à partir d'Ethereal sous XP capturer des trames 802.1Q. On le fera ici en mettant en place un poste miroir pour capturer le flux du port multi-VLAN.

Exercices

Les exercices sont encore peu nombreux mais cela devrait s'enrichir sous peu ;-) .

Les Exonets 78 et 79 portent sur les Vlan :

78 : Mise en place d'un Vlan sans 802.1Q
79 : Mise en place d'un Vlan avec 802.1Q

Conclusion: Enseigner l'architecture commutée

L'architecture tout commutée annule les collisions et tout ce qui est associé, c'est à dire les limitations en distance (règles de 5 4 3, round trip delay .etc.) et la méthode CSMA/CD. Elle rend possible de nombreux traitements sur la couche 2.

Le Vlan est certainement la nouvelle base de structuration organisationnelle des réseaux complexes. Son enseignement est donc incontournable.

L'approche usuelle des Vlan n'est pas satisfaisante car elle ne permet pas d'appréhender correctement la diversité des solutions existantes.

Il est plus simple de présenter la norme 802.1q (en partie bien sûr et sans GVRP) aux étudiants. En effet il suffit pour eux de comprendre qu'une trame doit être associée à un VLAN par un port en entrée quelle que soit la méthode utilisée pour cela et que cette trame en sortie ne sera prise en compte que par les ports associés à ce Vlan ..

Finalement tout ça pour ça !!! (dur constat du prof réseau qui met des heures à décortiquer un sujet qu'il présentera en 2 minutes à ses étudiants) ;-)