LES RESEAUX VIRTUELS – VLAN

PLAN

I. INTRODUCTION

Les réseaux virtuels (Virtual LAN) sont apparus comme une nouvelle fonctionnalité dans l'administration réseau avec le développement des commutateurs.
La notion de VLAN est un concept qui permet de réaliser des réseaux de façon indépendante du système de câblage. Ces réseaux permettent de définir des domaines de diffusions restreints, cela signifie qu'un message émis par une station du VLAN ne pourra être reçu que par les stations de ce même VLAN.

Un VLAN, est donc, un regroupement logique, et non physique, de plusieurs stations. Pour réaliser ce regroupement, on intervient directement, par voie logicielle, sur le ou les éléments actifs que sont les commutateurs VLAN.

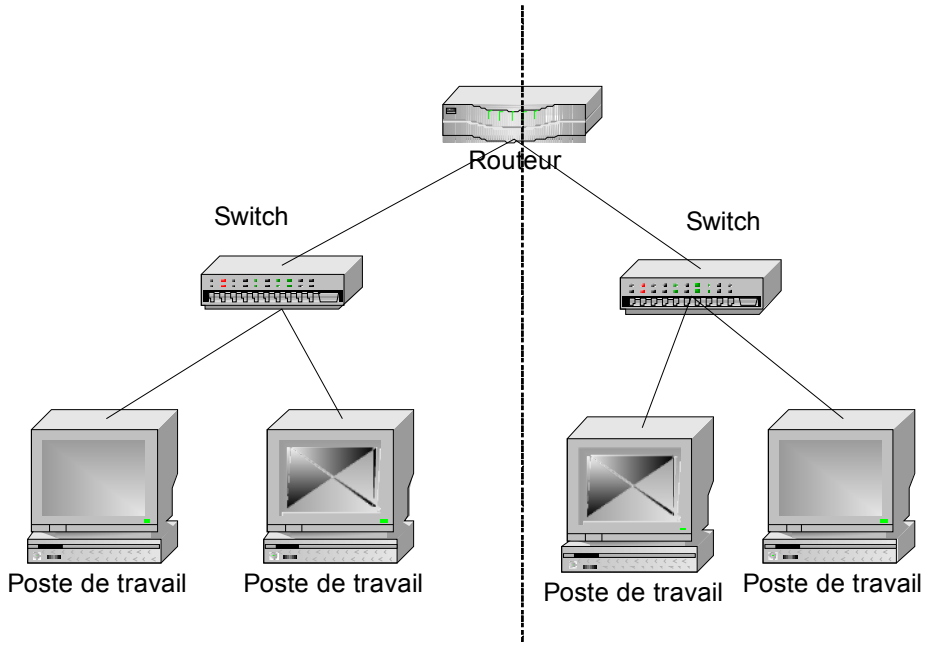
II. LES AVANTAGES D'un VLAN

- Ils permettent de supporter les organisations virtuelles, en rendant l'appartenance à un groupe indépendant de sa position géographique.
- Ils optimisent la bande passante, en réalisant des réseaux disjoints, donc en réalisant des domaines de collision disjoints.
- Ils simplifient l'administration, en utilisant des commandes centralisées pour gérer un réseau plutôt que des interventions dans les armoires de brassage.
- Ils améliorent la sécurité, en créant des règles de communication inter-VLAN.

III. LE PARTIONNEMENT DU RESEAU SANS LES VLAN

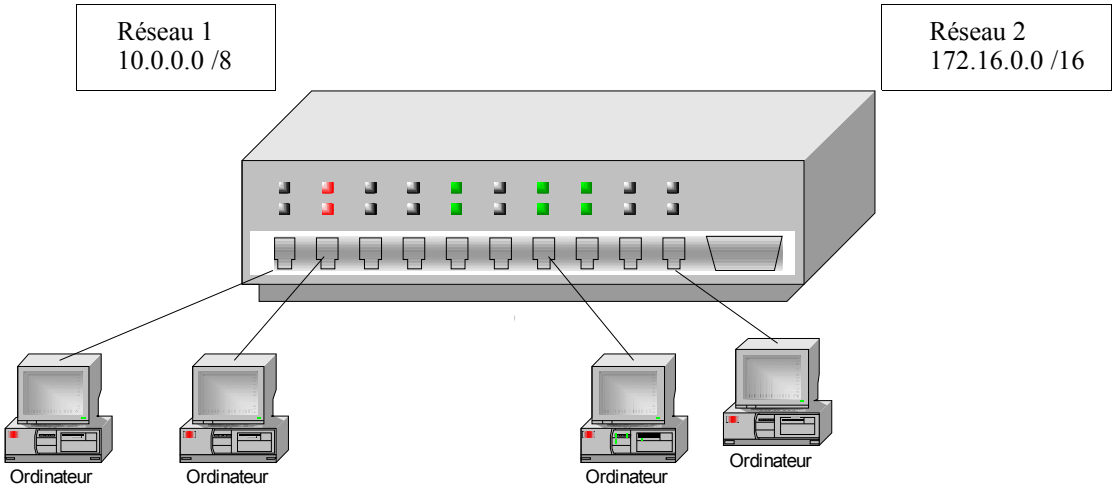
1. Réseaux physiquement disjoints

La première technique consiste à séparer un réseau en deux sous réseaux en utilisant un routeur. C'est la technique employée lorsque l'on met en place des réseaux sous IP.



2. Séparer les réseaux par un switch

La seconde technique consiste à séparer les réseaux par un switch, les paquets d'un réseau IP ne voyant pas les paquets des autres réseaux IP. En utilisant, deux ou plusieurs lans avec des adresses IP réseaux différentes, le commutateur est tout à fait capable de séparer les réseaux.



Cette technique pourrait être satisfaisante dans une architecture réseau simple, mais peu recommandable dans une architecture complexe, car ne disposant d'aucun outil pour une gestion centralisée du réseau.

IV. LA TECHNIQUE DES VLAN

Pour réaliser des VLANs, il faut tout d'abord des commutateurs spéciaux qui supportent le VLAN.

Ces produits combinent tous les avantages des solutions précédentes :

- Partitionnement en plusieurs domaines de broadcast
- Affectation d'un ou plusieurs ports à un VLAN depuis une console centrale
- Amélioration de la bande passante par la fonction de commutation
- Adaptation de la vitesse du switch à la capacité du réseau
- Regroupement des VLAN sur un même segment backbone (réseaux distants avec des Vlan commun de bout en bout)
- Gestion d'une bonne étanchéité entre VLAN

1. Les types de VLAN

Il existe plusieurs types de VLAN, en fonction de leurs méthodes de travail, nous pouvons les associer à une couche particulière du modèle OSI.

- **VLAN de niveau 1** associé à la couche physique
- **VLAN de niveau 2** associé à la couche liaison
- **VLAN de niveau 3** associé à la couche réseau

V. VLAN DE NIVEAU 1

Le VLAN de niveau 1 correspond à une configuration physique du réseau, il s'agit d'associer chaque port du switch à un VLAN.

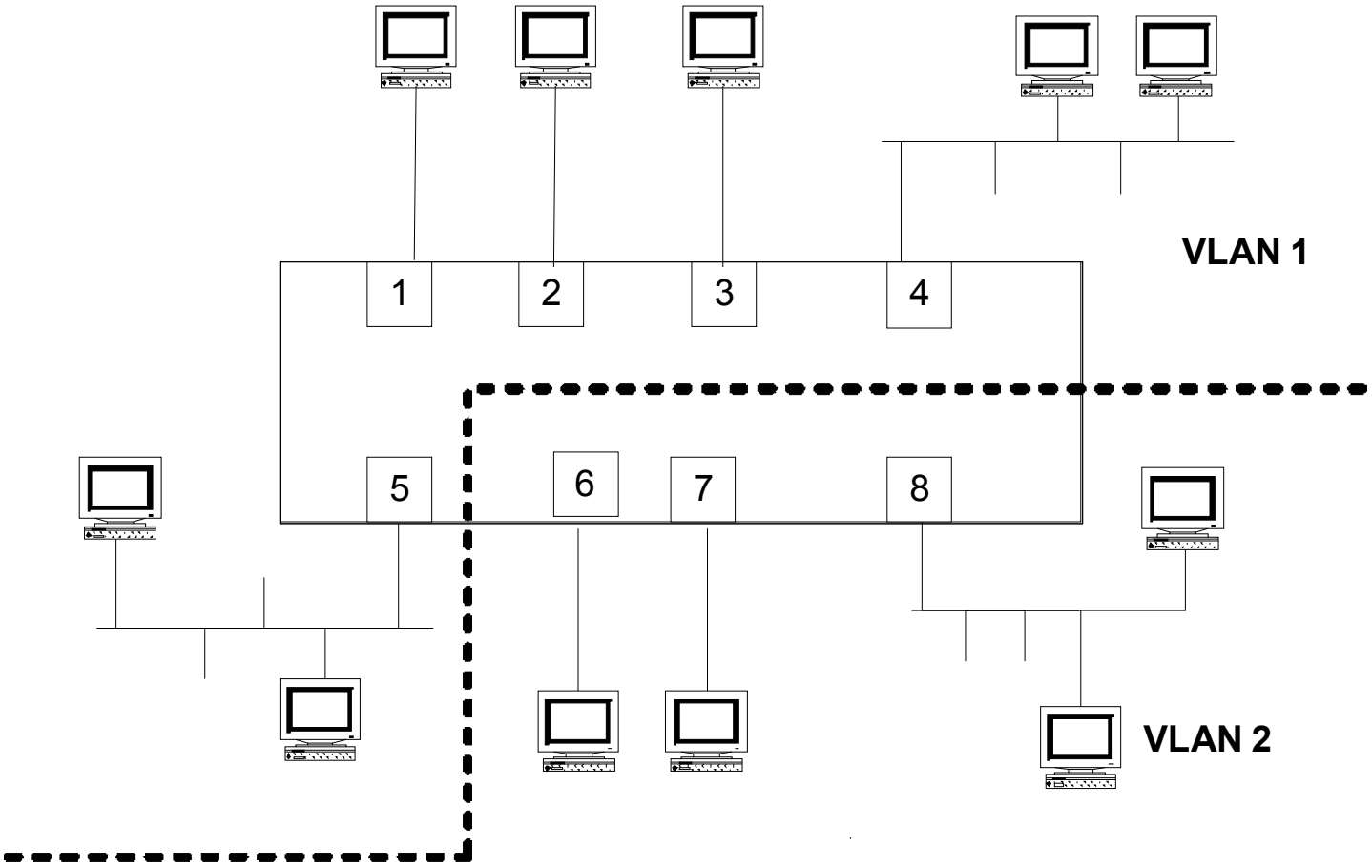
Dans ce type de VLAN :

- **C'est le port qui détermine le VLAN auquel appartient les stations associées**
- Il n'y a pas de traitement lourd pour chaque trame dans le processus de routage

Toutefois, ce type de VLAN comporte quelques inconvénients important :

- Un brassage est nécessaire en cas de déménagement géographique des stations
- Nécessite de modifier les VLAN en cas d'ajout ou de retrait d'utilisateurs
- Ne permet pas de traiter les switchs cascadés

Avec ce type de VALN, on ne dispose pas d'une souplesse très importante, et c'est pourquoi ils sont peu utilisés.



A titre d'exemple, voici le genre de commandes d'assignation à insérer dans le switch

- assign port 1,2,3,4,5 to VLAN 1
- assign port 6,7,8 to VLAN2

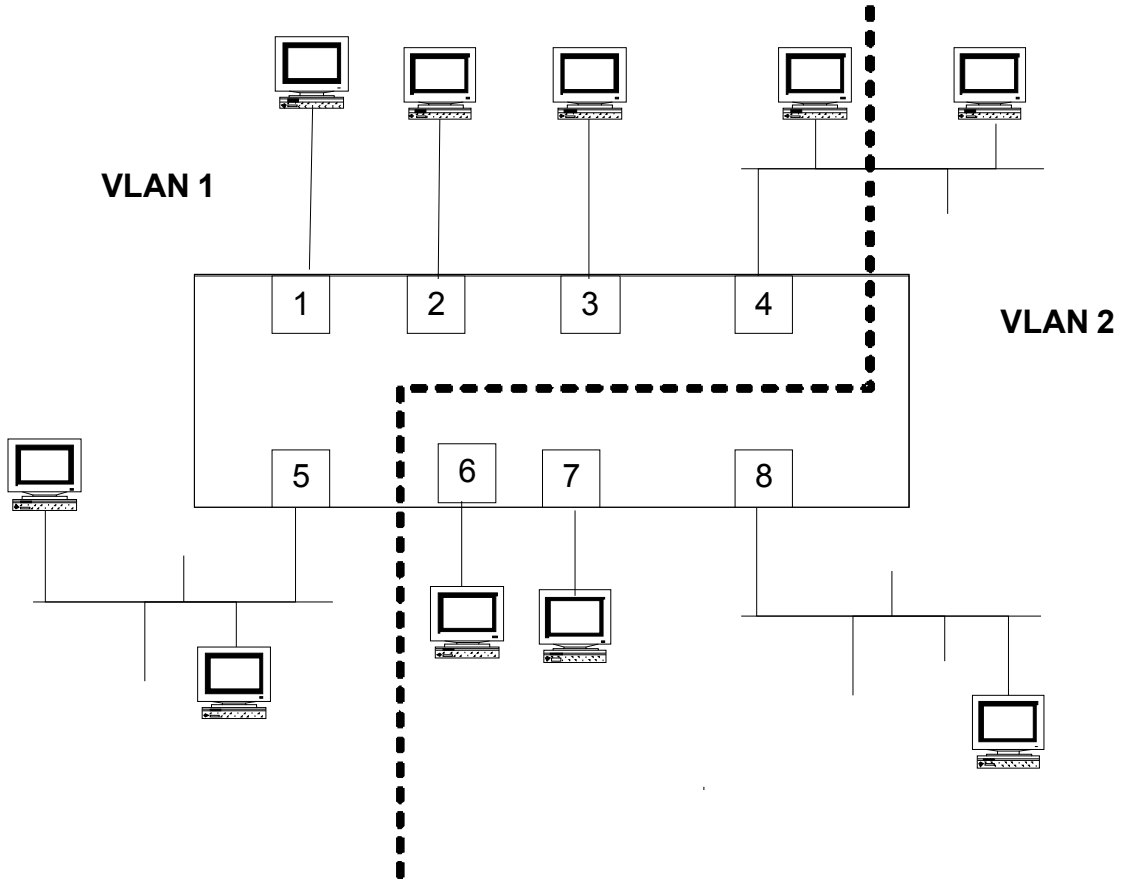
VI.VLAN DE NIVEAU 2

Dans ce type de VLAN, c'est l'adresse MAC de la carte réseau de la station, qui détermine le VLAN auquel elle appartient

Cela offre une grande souplesse et permet d'avoir des stations sur un même port du switch et pourtant appartenant à des VLAN différents.
Ce point est très important car il permet alors, d'autoriser des switchs en cascades sur le switch configuré en VLAN. Le switch VLAN, placé en tête de pont, fera alors le routage sans difficultés, puisque la lecture de l'adresse MAC de la trame lui indiquera le numéro de VLAN associé.

La souplesse qui en découle donne la pleine puissance des VLAN, car en cas de mouvement de postes, toute reconfiguration est inutile, le switch VLAN saura toujours associé l'adresse MAC de la carte réseau au bon VLAN.

Le seul bémol à ce type de VLAN est la nécessité de maintenir un fichier de correspondance entre adresse_mac et VLAN, le switch l'ayant créer lors de sa configuration, il suffit de l'exporter. Bien entendu, tout changement de carte réseau sur un poste nécessite un changement similaire sur son association VLAN.

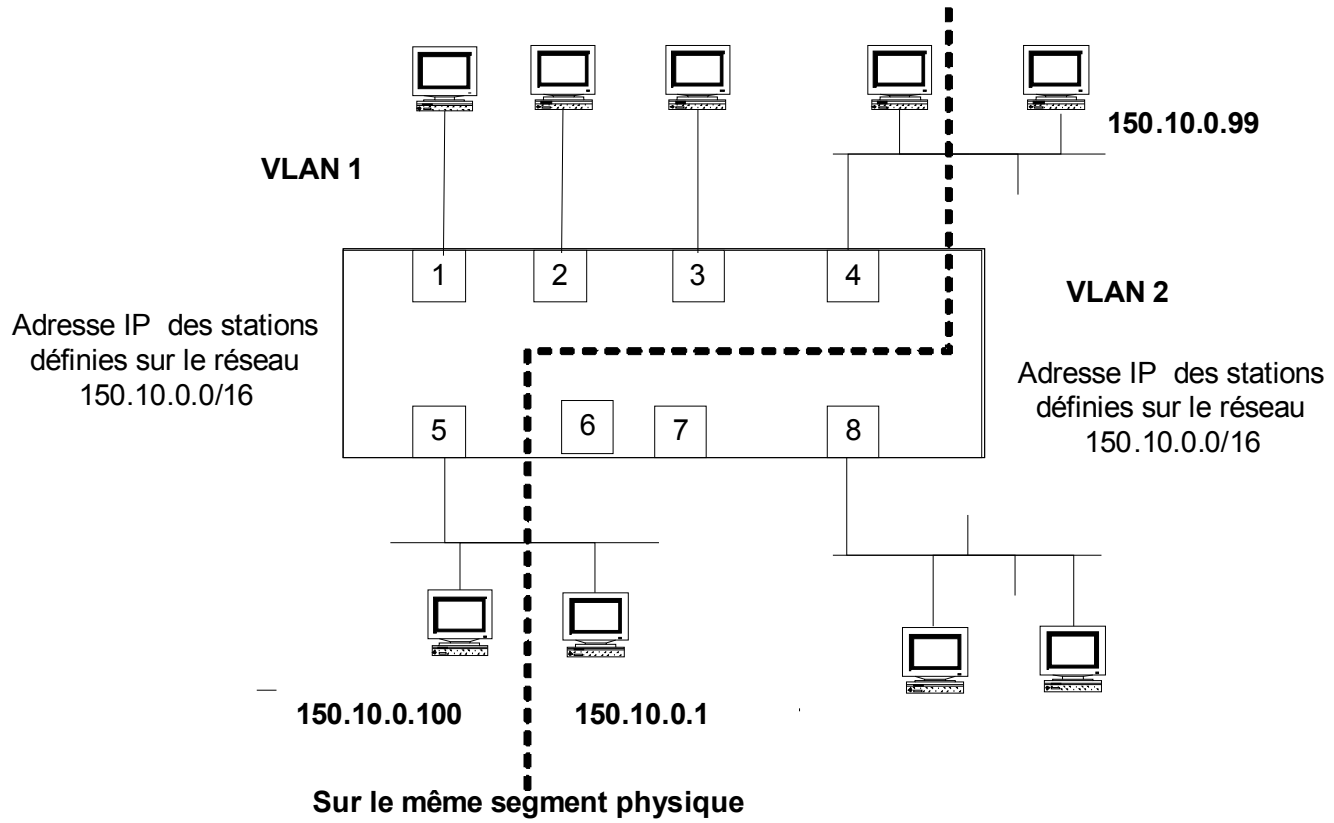


VII. VLAN DE NIVEAU 3

On peut considérer que c'est le niveau de VLAN par défaut, en effet, au niveau 3, c'est l'adresse IP de la station qui détermine le VLAN auquel elle appartient. Plus précisément, on associera un VLAN à une plage d'adresse.

Avec les VLAN de niveau 3, la configuration est aisée car on se trouve au niveau IP, donc loin de toute configuration matérielle tels que ports ou adresses MAC. On retrouve bien entendu, la puissance des VLAN, c'est-à-dire que des stations sur un même port du switch peuvent appartenir à des VLAN différents.
Le niveau 3 est adapté au réseau complexe et aux entreprises possédant de nombreux portables avec ou sans fils.

La puissance des OS intégrés dans les switch VLAN leur permet de traiter rapidement des milliers de trames en parallèle. En effet, si nous rentrons plus en détails dans le traitement de la trame, nous trouvons une trame Ethernet classique avec un champ de données contenant un paquet IP. Le commutateur devra avant tout routage de la trame, extraire le paquet IP de la trame Ethernet, et ensuite extraire de ce paquet IP, l'adresse IP destination de la trame et le masque de sous réseau associé.



On peut, au sein d'un même réseau IP définir des groupes de stations appartenant à des différents VLAN et cela de manière totalement transparente, sans multiplier le nombre de sous réseaux à gérer.

VIII. LE FONCTIONNEMENT INTERNE DES SWITCHS VLAN

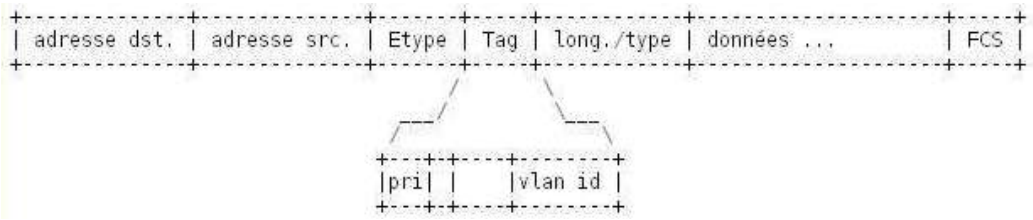
A présent que nous avons vu le principe des VLAN, attardons nous sur le fonctionnement interne du VLAN, et étudions la problématique suivante :

Comment transporter et reconnaître à l'arrivée sur un même segment physique, des trames issues de plusieurs VLAN?

1. Le marquage des trames

Pour réaliser cette opération, les systèmes d'exploitation des switchs VLAN réalisent le marquage des trames. À l'aide du marquage de trame, un champ de quatre octets est rattaché à toutes trames traversant le réseau. Ce champ (tag) identifie le VLAN auquel appartient la trame, il est ajouté à la trame par la station émettrice ou par un périphérique en réseau, par exemple, un commutateur. Outre les informations VLAN, la priorité relative de la trame sur le réseau peut être spécifiée par l'étiquette.

La trame Ethernet ci-dessous, présent le point où sera inséré le tag VLAN.



Les différents champs de la trame sont :

- ***adresse MAC destination*** (6octets)
  Permet de connaître la destination de la trame
- ***adresse MAC source*** (6 octets)
  Permet en cas de problèmes sur la trame, d'avertir la station émettrice que sa trame n'a pu être livrée, et de redemander une retransmission
- ***Etype*** (2 octets)
  Champ défini avec le code 0800
- ***Tag Vlan*** (4 octets)
  Définit l'identifiant VLAN et sa priorité – Nous l'étudierons plus en détails avec la norme IEEE 802.1Q
- ***Long/type***: (2 octets)
  Définit la taille des données utiles dans le champ données, sachant que ce champ doit faire au minimum 46 octets et maximum 1500. Si la trame ne contient que 10 octets utiles, 36 octets de bourrage seront insérés dans le champ données. La valeur du champ Long/type sera alors définie à 10.
- ***FCS*** (4 octets)
  Ce Frame Control Sequence est un contrôle basé sur une division polynomiale des en têtes de la trame, sans le champ données. Ce FCS correspond au reste obtenu en divisant la trame par un polynôme normalisé CRCx. Ce contrôle est également appelé Contrôle à Redondance Cyclique.

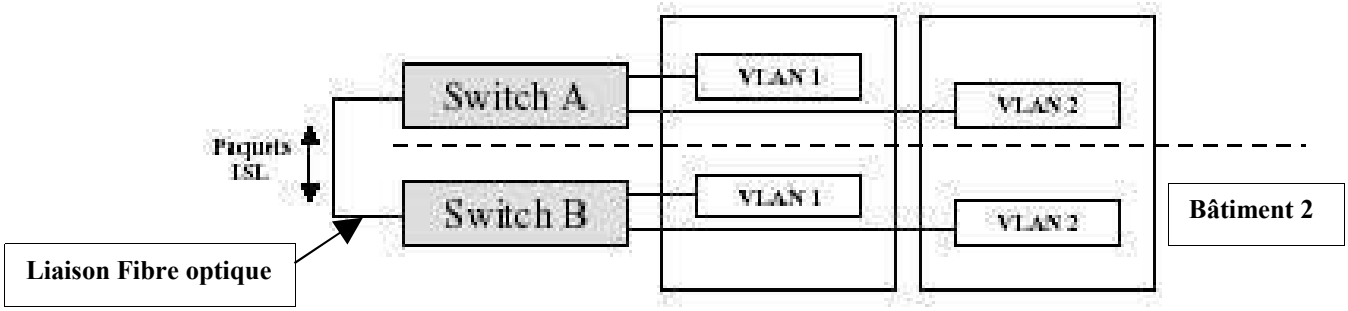
Deuxième problématique :

Comment étendre un même VLAN sur plusieurs commutateurs ?

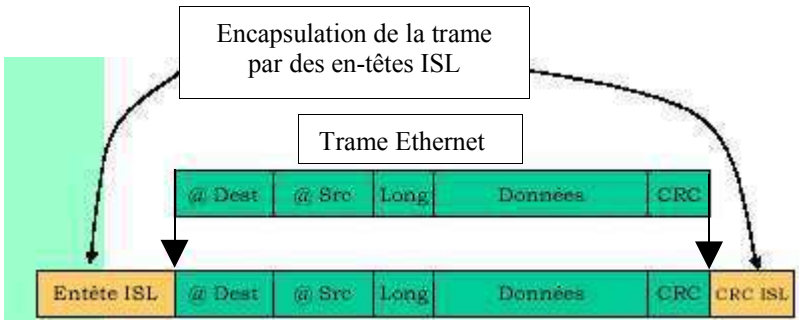
Pour résoudre ce problème, les constructeurs proposent des solutions, en particulier CISCO qui propose le protocole ISL (InterSwitch Link).Et de façon plus ouverte, il a été défini la norme IEEE 802.1Q

2. Le protocole ISL

ISL est un protocole propriétaire CISCO, il a pour objectif de permettre un marquage des trames afin d'en effectuer un routage correct sur des liens communs à plusieurs VLAN, typiquement un backbone en fibre optique.



Voici un schéma représentant l'encapsulation de la trame Ethernet
par des en-têtes spécifiques ISL



Voici une définition succincte des champs composant ces deux en têtes

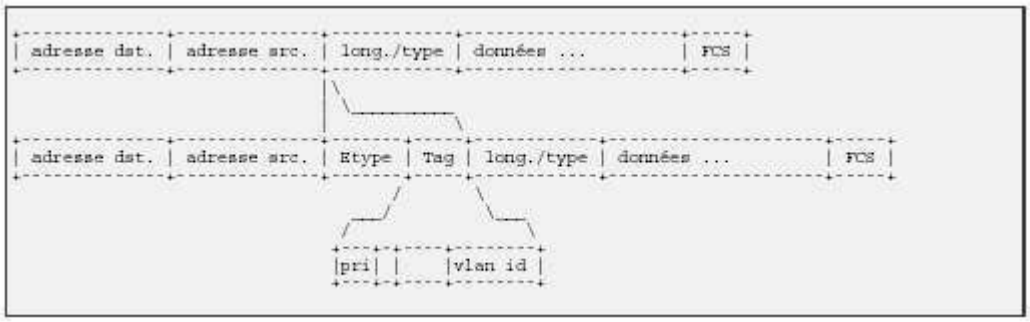
- **• Entête ISL**
  - Adresse destination (40 bits)
  - Type (Ethernet, Token Ring, ATM, FDDI, …) (4 bits)
  - Utilisateur (Priorité) (4 bits)
  - Adresse émetteur (@ MAC du port émetteur) (48 bits)
  - Longueur (16 bits)
  - Constante (AA AA 03) (24 bits)
  - Bits de poids forts de l'adresse source (24 bits) – Réseau virtuel (16 bits)
  - BPDU : 1 si paquet de gestion du protocole Spanning tree (1 bit)
  - Index (utilisé en maintenance) (16 bits)
- **CRC ISL**
  - CRC (32 bits) (Contrôle à Redondance Cyclique ⍁Division polynomiale)

3. La norme IEEE 802.1Q

Le standard IEEE 802.1Q fournit un mécanisme d'encapsulation très répandu et implanté dans de nombreux équipements de marques différentes. Comme dans le cas de l'encapsulation ISL précédente, l'en-tête de trame est complété par une balise de 4 octets.

Le standard IEEE 802.1Q définit le contenu de la balise de VLAN (**VLAN tag**) avec laquelle on complète l'en-tête de trame Ethernet.

Ce VLAN tag est placé à la suite du champ Ethertype de la trame Ethernet, qui lui même est juste derrière l'adresse MAC Source.



Structure du VLAN Tag

Priority (3bits)	Canonical Format Identifier (1bit)	VLAN Identifier (12 bits)

Le champ Priority

- Ce champ de 3 bits fait référence au standard IEEE 802.1P. Sur 3 bits on peut coder 8 niveaux de priorités de 0 à 7.
- La notion de priorité dans les VLANs est sans rapport avec les mécanismes de priorité IP.
- Ces 8 niveaux sont utilisés pour fixer une priorité aux trames d'un VLAN relativement aux autres VLAN. La priorité du routage d'un VLAN par rapport à l'autre est définie lors de la définition des VLANS.

Le champ Canonical Format Identifier

- Ce champ codé sur 1 bit assure la compatibilité entre les adresses MAC Ethernet et Token Ring dans le cas d'architecture réseau mixte, plutôt rare à présent.
- Un commutateur Ethernet fixera toujours cette valeur à 0. Si un port Ethernet reçoit une valeur 1 pour ce champ, alors la trame ne sera pas propagée puisqu'elle est destinée à un port «sans balise» (untagged port).

Le champ VLAN Identifier, vlan id, VID

- Ce champ de 12 bits sert à identifier le VLAN auquel appartient la trame.
- Il est possible de coder 4094 VLANs avec ce champ.

IX. Pour aller plus loin – Les liens TRUNK – Les liens MESH

1. Le Trunking

Un *trunk* est une connexion physique unique sur laquelle on transmet le trafic de plusieurs réseaux virtuels. 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 La distribution du trafic sur chacun des liens du trunk est effectuée sur la base d'une résolution d'adresse source et/ou destination, voir d'une négociation . Les trames qui traversent le *trunk* sont complétées avec un identificateur de réseau local virtuel (VLAN id). Grâce à cette identification, les trames sont conservées dans un même VLAN (ou domaine de diffusion).

Les *trunks* peuvent être utilisés :

- **Entre deux commutateurs**

  C'est le mode de distribution des réseaux locaux le plus courant.

- **Entre un commutateur et un hôte**

  C'est le mode de fonctionnement à surveiller étroitement. Un hôte qui supporte le *trunking* a la possibilité d'analyser le trafic de tous les réseaux locaux virtuels.

- **Entre un commutateur et un routeur**

  C'est le mode fonctionnement qui permet d'accéder aux fonctions de routage ; donc à l'interconnexion des réseaux virtuels par routage inter-VLAN.

Tous les VLAN véhiculés dans le même *trunk* partagent la bande passante du média utilisé. Si un *trunk* utilise un lien 100Mbps, la bande passante de tous les VLAN associés est limitée à ces 100Mbps.

1. Le Meshing

Une autre manière d'agréger plusieurs liens est le meshing. Cette technique ne se limite pas à des liaisons point à point entre deux switchs puisqu'elle peut regrouper tout un maillage de switchs (plusieurs switchs reliés entre eux de façon redondante).

À l'intérieur d'un même mesh, le trafic est distribué dynamiquement vers les liens offrant l'accès le plus rapide, l'objectif ici est de partager la charge réseau sur plusieurs liens, évitant ainsi toute saturation et assurant un Qos de qualité0

Un ensemble de switchs reliés (de manière redondante) par des liens paramétrés comme mesh constitue un meshed domain. Ce dernier détermine régulièrement les "meilleurs" chemins à l'intérieur de ce domaine selon plusieurs critères: en fonction de la taille de la file d'attente des buffers associés aux ports du switch, de leur configuration en vitesse et de la quantité de paquets jetés qui illustre l'occupation du port.

Un chemin déterminé comme "meilleur" entre deux adresses MAC reste valable tant que l'entrée de ces adresses MAC n'expire pas dans la table d'adressage. La différence principale avec le trunk

est que tous les liens restent actifs et qu'ils peuvent rapidement être sollicités pour répondre à une augmentation du trafic.

X. QUELQUES ÉQUIPEMENTS POUR LA RÉALISATION DE VLAN

Commutateur Procurve HP 2524 pour réseaux d'entreprises –503 €

- 24 ports 10/100Base-TX auto-sensing, auto MDI/MDI-X (sur RJ-45)
- Commutation Ethernet : Commutation non bloquante sur tous les ports Ethernet, auto-négociation Full / Half Duplex, authentification 802.1x, **support des VLAN 802.1Q** (x30, configuration dynamique), gestion des priorités 802.1p, Rapid et Fast Convergence Spanning Tree (802.1D et 802.1w)

D-Link DGS-3312SR –1369 €
Commutateur de tête de réseaux

- 4 ports SFP (Small Form Pluggable) 10/100/1000Base-TX auto-sensing, auto MDI/MDI-X sur RJ-45
- Commutation Ethernet : Commutation non bloquante sur tous les ports Ethernet, auto-négociation Full / Half Duplex, contrôle de flux 802.3x, **support des VLAN 802.1Q**, gestion des priorités 802.1p, authentification 802.1x, Rapid Spanning Tree, gestion QoS, contrôle de la bande passante, limitation des broadcasts, IGMP snooping
- Table des adresses MAC : 16 000 entrées (8 000 dans une pile)

NetGear FS750T-530 €

- L'interface du navigateur permet une gestion simple, permettant d'évaluer la performance du switch, de configurer des ports, de mettre en place des agrégats de ports, des VLAN ou de la priorité de trafic. Livré prêt à l'emploi, il est facile à paramétrer et à utiliser

- Commutation Ethernet : Commutation non bloquante sur tous les ports Ethernet, auto-négociation Full / Half Duplex, contrôle de flux 802.3x, **support des VLAN 802.1Q** (64 groupes), agrégation de liens IEEE 802.3ad, gestion des priorités 802.1p, gestion QoS par port,

Documents de référence

WEBOGRAPHIE

- Documentation Cisco:
  InterSwitch Link and IEEE 802.1Q Frame Format
- Documentation Cisco décrivant une configuration simple sur le routage inter-VLAN
  Configuring InterVLANRouting and ISL/802.1Q Trunking.
- Exemple pédagogique de configuration de VLAN sur DELL power connect 5212
  http://docs.us.dell.com/support/edocs/network/pc5212/fr/UG/pc5212ce.htm
- Exemple d'application de VLAN
  http://www.awt.be/web/sec/index.aspx?page=sec,fr,100,010,003
- Exemple de commande de configuration d'un vlan sur INTEL Switch 6000
  http://support.intel.com/support/express/switches/6000/sb/CS-012323.htm
- Exemple de configuration de VLAN sur matériel Cisco
  http://www.cisco.com/en/US/products/hw/switches/ps646/products_command_reference_chapter09186a00801cdf03.html
- Présentation des réseaux virtuels installés sur le campus de Jussieu
  http://web.ccr.jussieu.fr/ccr/services/reseau/Presentation.htm

BIBLIOGRAPHIE

Les réseaux locaux virtuels
de Gilbert Held

InterÉditions
1998
2-2258-3156-4
240 pages - 39,50 €

Cisco
Interconnexion des réseaux à l'aide des routeurs et commutateurs
de Djillali Seba

Eni
novembre 2003
2-7460-2144-7
500 pages - 27,14 €

J'ai pu constater que la littérature est assez pauvre concernant les Vlan, en fait, de nombreux constructeurs fournissent des formations et des supports par le biais d'achat de matériel. Toutefois, ceci est compensé par le nombre de sites traitant de la technique des VLAN.