Introduction au routage inter-VLAN

Philippe Latu
philippe.latu(at)inetdoc.net

https://www.inetdoc.net

Résumé

L'usage des réseaux locaux virtuels (VLANs) et du routage entre ces même réseaux locaux est devenu systématique dans les infrastructures d'interconnexion contemporaines. Ce routage inter-VLAN présente de nombreux intérêts tant du point de vue conception que du point de vue exploitation. La même question revient sans fin : quelle est la meilleure solution entre une interconnexion de niveau 2 (couche liaison de données) et une interconnexion de niveau 3 (couche réseau) ? Loin de prétendre répondre à une telle interrogation, cet article présente les concepts élémentaires sur les réseaux locaux virtuels et le routage associé.

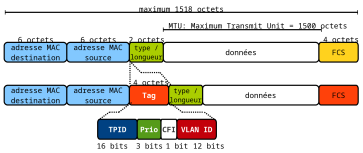


Table des matières

1. Copyright et Licence

1.1. Méta-information

Cet article est écrit avec *DocBook* XML sur un système *Debian GNU/Linux*. Il est disponible en version imprimable au format PDF : `inter-vlan-routing.pdf`.

2. Quelques notions sur les réseaux locaux Ethernet

Aujourd'hui, un réseau local repose systématiquement sur la technologie Ethernet. Il hérite donc des caractéristiques de cette technologie et les notions de ***collision*** et de ***diffusion*** sont les deux points clés.

Une collision intervient lorsque deux hôtes d'un réseau émettent simultanément sur un média partagé. On appelle ***domaine de collision*** un sous-ensemble du réseau à l'intérieur duquel les hôtes sont en compétition pour accéder à un même média ou canal de communication. Plus le nombre d'hôtes présents dans un même domaine de collision est important, plus la fréquence des collisions augmente et plus les performances se dégradent. Pour garantir les meilleures conditions de communication, on cherche donc à réduire au maximum l'étendue du domaine de collision. Sur les réseaux filaires actuels, les domaines de collision ne posent plus aucun problème depuis que l'on utilise des commutateurs. La vocation d'un commutateur est de constituer un circuit de communication unique entre deux hôtes. Une fois le circuit constitué, toute collision est impossible.

La diffusion est un mécanisme d'annonce générale qui assure que tous les hôtes d'un réseau local reçoivent les trames de diffusion émises par n'importe quel autre hôte de ce même réseau. On appelle ***domaine de diffusion*** un réseau à l'intérieur duquel tous les hôtes peuvent émettre et doivent recevoir des trames de diffusion. Comme dans le cas précédent, plus le nombre d'hôtes présents dans le domaine de diffusion est important, plus les performances se dégradent. Là encore, pour garantir les meilleures conditions de communication, on cherche à réduire «raisonnablement» l'étendue du domaine de diffusion. C'est précisément sur le dimensionnement des domaines de diffusion que le débat sur le choix du niveau d'interconnexion entre réseaux locaux intervient. Le document *Segmentation des réseaux locaux* apporte un premier niveau d'éclairage.

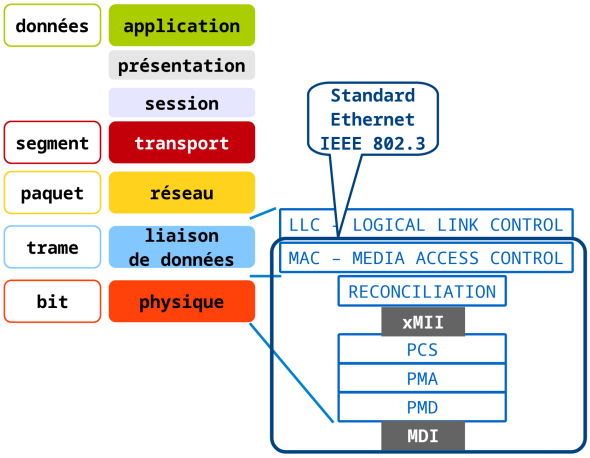
Voyons comment on délimite les domaines de collision et de diffusion en faisant la correspondance entre les définitions données par la modélisation OSI et le standard Ethernet. Une fois cette correspondance faite, les unités de données manipulées par les équipements d'interconnexion permettent de définir l'étendue des domaines de collision et de diffusion.

2.1. Correspondance entre modélisation OSI et standard Ethernet

Depuis fort longtemps, la modélisation OSI sert de référence à la description des couches orientées transmission de l'information. Cette modélisation est présentée de façon plus détaillée dans le support *Modélisations réseau*.

Les spécifications des réseaux Ethernet ont été publiées à la même époque et ont été développées par l'***Institute of Electrical and Electronics Engineers***. Elles sont accessibles à la page *IEEE 802.3™: ETHERNET*.

Si on fait correspondre le modèle OSI et le standard Ethernet, ce sont les couches physique et une moitié de la couche liaison qui nous intéressent.



La représentation graphique fait apparaître un grand nombre d'acronymes. Même si le propos de ce document n'est pas de traduire le standard IEEE 802.3, voici quelques éléments d'explication pour chaque sous-couche du standard Ethernet représentée.

*Logical Link Control*LLC

Cette sous-couche ne fait pas partie du standard Ethernet proprement dit. Il s'agit d'une sous couche de services qui occupe la moitié supérieure de la couche liaison de données du modèle OSI. Elle est définie par le standard IEEE 802.2 pour les réseaux locaux. Les services offerts sont relatifs au traitement d'erreurs et au contrôle de flux.

*Media Access Control*MAC

Cette sous-couche joue un rôle très important dans les réseaux Ethernet. Elle est responsable des mécanismes de contrôle d'accès au canal de transmission sur le réseau de diffusion multi-accès. Ce rôle

d'arbitrage des accès entre les différents hôtes présents dans le réseau de diffusion suppose que ces hôtes soient identifiés par une adresse. Les formats de ces adresses sont présentés en détail dans la Section 2.3, « Types d'adresses MAC ».

*Reconciliation Sublayer*RECONCILIATION

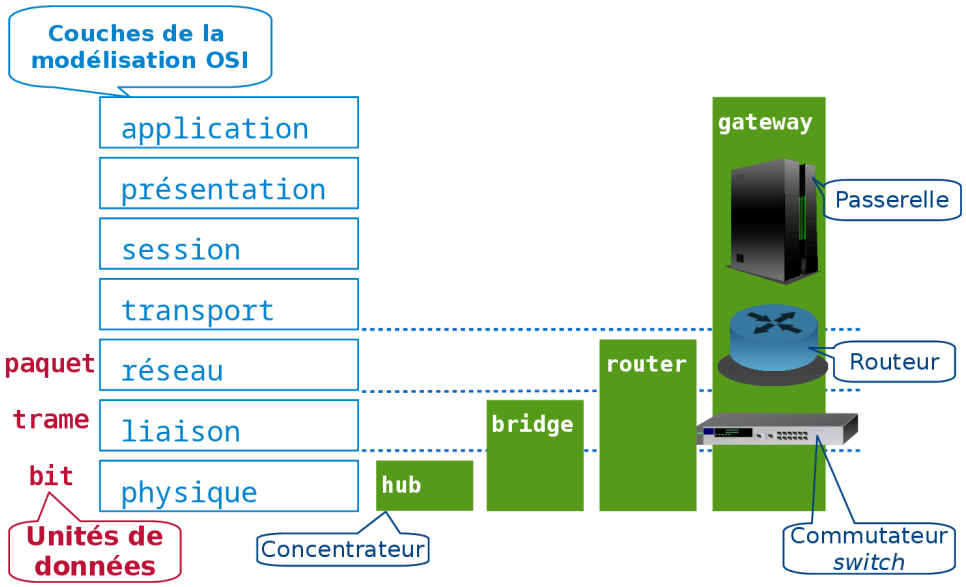
Cette sous-couche est chargée de faire la correspondance entre les signaux fournis au niveau xMII et les instructions de contrôle de la couche physique (PLS).

- MII : *Media Independent Interface*. Cette interface isole la sous-couche MAC de la couche physique de façon à ce que plusieurs implémentations différentes soient utilisables au niveau de la couche physique.
- PCS : *Physical Coding Sublayer*. Encodage/décodage des flux de données depuis et vers la sous-couche MAC. Les techniques de codage varient suivant les générations des variantes d'Ethernet et les débits.
- PMA : *Physical Medium Attachment*. Transformation et synchronisation des groupes de code en flux de bits adaptés à des composants de transmission série et vice versa.
- PMD : *Physical Medium Dependent*. Transmission du signal à l'aide des fonctions d'amplification, de modulation et de changement de forme d'onde. Ces fonctions varient suivant les variantes d'Ethernet et les débits.
- MDI : *Medium Dependent Interface*. Définitions des différents types de connecteurs suivant les médias utilisés : paires torsadées cuivre ou fibres optiques.

2.2. Correspondance entre unités de données et équipements réseau

Le modèle OSI a introduit un acronyme particulier pour caractériser les unités de données manipulées au niveau de chaque couche : PDU pour *Protocol Data Unit*. L'*Encapsulation* est la notion clé pour isoler les traitements effectués sur les unités de données. Le principe de l'encapsulation veut que les unités de données utilisées à chaque niveau soient indépendantes. Par conséquent, les champs de la trame sont traités au niveau liaison et ne devraient avoir aucune relation avec les champs du paquet au niveau réseau et ainsi de suite.

Si les unités de données sont spécifiques à chaque couche du modèle, il est plus aisé de concevoir des équipements spécialisés dans le traitement de ces unités des données. On aboutit ainsi à la représentation suivante.



ConcentrateurHub

La capacité de traitement d'un concentrateur se limite à la couche physique et l'unité de données manipulée est le bit. Comme cet équipement est incapable de distinguer le début ou la fin d'un flot de bits, il n'a aucun impact sur la délimitation des domaines de collision ou de diffusion.

On peut considérer que les *Hubs* sont des équipements obsolètes qui n'ont plus leur place dans les réseaux locaux contemporains.

PontBridge

La capacité de traitement d'un pont couvre les couches liaison et physique. L'unité de données manipulée est la trame. La couche liaison constitue le niveau le plus bas de délimitation des bornes du flot de bits reçus

ou émis sur une interface réseau. C'est aussi dans la couche liaison que l'on définit la méthode d'accès aux différents médias de transmission.

C'est la capacité à reconnaître les champs d'une trame qui est déterminante dans la détection d'une collision lorsque deux hôtes ou plus émettent simultanément dans un même réseau local. De plus, comme les trames contiennent les adresses source et destination, il est possible de prendre une première décision sur l'acheminement. Pour réaliser ce traitement sur l'acheminement des trames entre ses différents ports, un pont maintient une table de correspondance entre les adresses source des hôtes qui émettent du trafic et le numéro du port sur lequel les trames sont reçues. En conséquence, peut donc dire qu'*une interface de pont délimite un domaine de collision*.

Si un réseau local comprend plusieurs segments et donc plusieurs ponts, ceux-ci utilisent le ***Spanning Tree Protocol*** (STP) dans le but de constituer une topologie réseau sans boucle. Ce protocole est basé sur l'échange de trames dédiées appelées ***Bridge Protocol Data Unit*** (BPDU). La description du fonctionnement de ce protocole sort du cadre de cet article. Il est possible de consulter la page ***Wikipedia*** correspondante : *Spanning Tree Protocol*.

Si les ponts, en tant qu'équipement d'interconnexion réseau ont quasiment disparu, toutes leurs fonctionnalités ont été intégralement conservées dans les commutateurs présentés ci-après.

CommutateurSwitch

En première approximation, un commutateur est un pont avec une électronique spécialisée qui garantit la bande passante par port. On retrouve les fonctions essentielles.

1. Transmission ou non des trames en fonction des adresses MAC destination.
2. Apprentissage des adresses MAC source en examinant chaque trame reçue sur un port.
3. Construction d'une topologie réseau sans boucle entre équipements d'interconnexion de niveau liaison à l'aide du protocole STP.

Relativement aux équipements des générations précédentes, les bénéfices apportés par l'utilisation des commutateurs Ethernet sont nombreux. Un commutateur créé un domaine de collision distinct par port. Les connexions sur chaque port utilisent le mode ***full-duplex***, ce qui offre des garanties sur les temps de transmission des trames. Enfin, on peut considérer qu'un commutateur multiplie la quantité totale de bande passante disponible sur un réseau local.

RouteurRouter

La capacité de traitement d'un routeur couvre les trois couches basses du modèle OSI : physique, liaison et réseau. Les traitements du niveau réseau permettent de délimiter un *domaine de diffusion* par interface sur un routeur. Comme la gestion du sous-réseau inclut la couche liaison, une interface de routeur délimite aussi une *domaine de collision*.

Dans la quasi totalité des réseaux, le protocole routé utilisé est IP. Il est basé sur le principe de la commutation de paquets et son format d'adressage permet de construire un découpage en groupes logiques d'hôtes à la différence du format des adresses Ethernet. C'est justement cette absence de capacité à découper l'espace d'adressage en groupes logiques au niveau liaison qui a conduit au développement des réseaux locaux virtuels présentés ci-après.

Il faut ajouter qu'un routeur réalise des traitements plus complexes qu'un commutateur au niveau liaison. La prise de décision sur l'acheminement des paquets, c'est à dire le routage, est alimentée par un ou plusieurs protocoles de routage dynamique. Ces protocoles de routage sont des processus qui s'exécutent dans l'espace utilisateur d'un système d'exploitation complet. On voit donc que la première prise de décision sur le routage d'un nouveau paquet vers une destination non connue, passe par un traitement 100% logiciel. Ce n'est que dans un second temps qu'il est possible de déléguer la transmission des paquets vers des destinations mémorisées à une électronique spécialisée.

Pour distinguer les traitements, on peut dire que le routage de paquets est une opération logicielle tandis que la commutation de paquets peut être une opération matérielle sur un équipement disposant de composants spécialisés.

*PasserelleGatewayApplication Level Gateway*ALG

La capacité de traitement d'une passerelle couvre toutes les couches du modèle OSI de la couche application à la couche physique. La gestion du sous-réseau est donc incluse et une interface de passerelle délimite à la fois un *domaine de diffusion* et un *domaine de collision*.

Parmi les traitements réalisés par une passerelle, on trouve les fonctions de cache de filtrage et de redirection. On peut citer les exemples des services mandataires avec filtrage d'URLs ou les services de routage d'appels en téléphonie sur IP.

2.3. Types d'adresses MAC

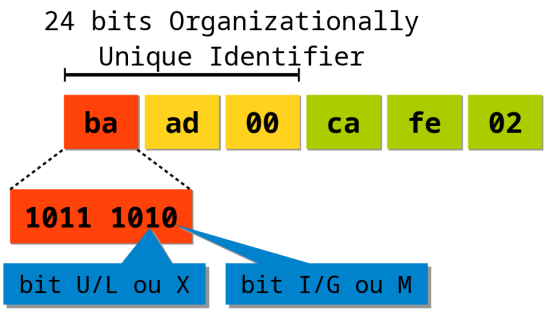
Les adresses utilisées dans les trames Ethernet sont appelées adresses MAC ; acronyme issu du nom de la sous-couche consacrée à la méthode d'accès. Ces adresses sont représentées sur 48 bits ou 64 bits soit 6 ou 8 octets. Le terme d'*adressage matériel* est généralement utilisé dans la mesure où les adresses MAC sont directement gravées dans les composants d'interface réseau.

Même si ce format d'adressage est non hiérarchisé et ne prévoit aucune possibilité de découpage en groupes logiques, on distingue différents types d'adresses MAC.

EUI-48*48-bit Extended Unique Identifier*

À l'origine, la représentation sur 48 bits a été retenue par le comité *IEEE 802* et est utilisée dans plusieurs technologies réseau dont Ethernet.

Dans les spécifications de l'*IEEE*, l'espace d'adressage est découpé en deux parties. Les trois octets ou les 24 bits de poids fort sont réservés à l'identification du constructeur de l'interface réseau. C'est la partie *Organizationally Unique Identifier* (OUI) de l'adresse ; attribuée et enregistrée directement par l'*IEEE* ou l'*IANA*. Les trois octets ou les 24 bits de poids faible sont attribués par le constructeur comme numéro de série.



Les deux bits de poids faible l'octet de poids le plus fort servent à identifier les usages d'une adresse MAC.

- Le bit de rang 0 (de poids le plus faible) sert à distinguer une adresse individuelle (I) ou *unicast* (bit = 0) d'une adresse de groupe (G) ou *multicast* (M) (bit = 1).

  Une trame avec une adresse MAC source *unicast* est émise à destination des hôtes du domaine de collision. Dans notre cas, le domaine de collision se limite au port du commutateur sur lequel l'hôte émetteur est connecté. Une trame avec une adresse MAC destination *unicast* est traitée après réception uniquement par l'hôte pour lequel il y a correspondance exacte entre cette adresse destination et l'adresse de son interface.

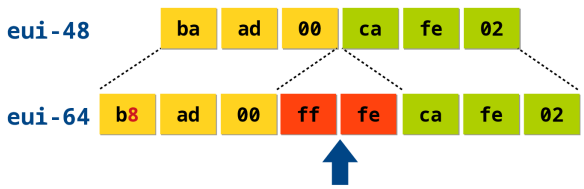
  Une trame *multicast* est émise à partir d'une source unique à destination de tous les hôtes abonnés à un flux particulier. La notion d'abonnement est gérée par les couches supérieures. Suivant l'électronique d'un commutateur, il est possible de filtrer (*IGMP snooping*) la transmission des trames vers les seuls hôtes abonnés au flux. Si cette fonction n'est pas présente sur le commutateur, les trames sont recopiées sur tous les ports indistinctement.

- Le bit de rang 1 ou *Universal/Local* sert à distinguer une adresse universelle pour laquelle la partie *Organizationally Unique Identifier* a été attribuée par l'*IEEE* (bit = 0) d'une adresse pour laquelle la même partie est administrée localement (bit = 1).

Pour plus de détails, voir le document *Standard Group MAC Addresses: A Tutorial Guide*.

EUI-64*64-bit Extended Unique Identifier*

La représentation sur 64 bits des adresses MAC est apparue plus récemment dans les réseaux Ethernet. C'est encore l'*IEEE* qui publie les spécifications liées à l'utilisation de ces adresses sur 8 octets.



Les adresses au format EUI-64 sont de plus en plus répandues avec le déploiement du protocole IPv6 qui compose automatiquement les adresses de lien local avec l'adresse MAC sur 48 bits de l'interface dans laquelle deux octets supplémentaires insérés entre la partie OUI et la partie numéro de série.

Par exemple, une interface ayant l'adresse MAC EUI-48 `00:3f:1c:54:5e:65` aura pour adresse de lien local IPv6 : `fe80::23f:1cff:fe54:5e65/64`. On reconnaît ici l'insertion des deux octets `ff:fe`.

Pour plus de détails, voir le document *Guidelines for 64-bit Global Identifier (EUI-64™) Registration Authority*.

Après cette présentation succincte des différents formats et usages des adresses véhiculées dans les trames Ethernet, il est facile d'admettre que la constitution de groupes d'adresses sur une base logique ou hiérarchisée n'est pas possible. Il faut donc recourir à une modification des champs de la trame pour introduire cette notion de groupe logique. C'est justement l'objet des réseaux locaux virtuels ou VLANs.

3. Réseaux locaux virtuels : VLANs

3.1. Définitions

On a vu qu'un réseau local (LAN) est défini par un domaine de diffusion dans lequel tous les hôtes reçoivent les messages de diffusion émis par n'importe quel autre hôte du réseau. Par définition, un réseau local est délimité par une interface d'équipement de niveau 3 du modèle OSI (couche réseau).

Un réseau local virtuel (VLAN) est un réseau local (LAN) distribué sur des équipements de niveau 2 du modèle OSI (couche liaison). Le domaine de diffusion se retrouve ainsi réparti sur ces mêmes équipements de niveau 2. Ainsi, tous les hôtes appartenant au même réseau local (domaine de diffusion) constituent un groupe logique indépendant de la topologie physique du réseau.

La définition de base étant posée, deux problèmes restent à résoudre.

- Comment communiquer entre plusieurs réseaux locaux virtuels ?
- Comment assurer la répartition de plusieurs réseaux locaux virtuels sur plusieurs équipements de niveau liaison ?

Pour traiter le premier problème, il faut rappeler qu'il est absolument nécessaire de passer par un routeur (niveau réseau du modèle OSI) pour interconnecter plusieurs réseaux locaux. On aboutit ainsi au second problème à une différence près. Le routeur doit avoir connaissance des mêmes informations que les commutateurs au niveau liaison.

Pour traiter le premier et le second problème, il est donc nécessaire d'élaborer une technique de partage des réseaux locaux entre équipements. Cette technique consiste à étiqueter les trames pour identifier le trafic des différents réseaux locaux sur un même canal physique.

Ainsi, les réseaux locaux sont distribués sur les différents équipements via des liaisons logiques dédiées appelées ***trunks***. Le ***trunk*** est une connexion physique unique sur laquelle on transmet le trafic de plusieurs réseaux virtuels. 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. C'est la solution du second problème énoncé ci-dessus.

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. C'est la solution du premier problème énoncé ci-dessus.

Enfin, il ne faut pas oublier que tous les VLANs véhiculés dans le même ***trunk*** partagent la bande passante du média utilisé. Le ***trunk*** peut donc constituer un goulot d'étranglement si sa capacité est insuffisante.

3.2. Réseaux locaux virtuels standards

Il existe plusieurs mécanismes de gestion des VLANs. Certains sont propriétaires et ne fonctionnent que sur les équipements d'une seule marque.

VLANs par ports

Cette technique fournit une méthode de division d'un équipement de niveau 2 (commutateur) en plusieurs domaines de diffusion. La configuration de cette division est spécifique à chaque plateforme.

Bien que le coût d'administration de ce genre de configuration soit important puisqu'il faut gérer manuellement sur chaque équipement la distribution des réseaux locaux, cette technique est indépendante des plateformes et de leurs systèmes d'exploitation. C'est la raison principale pour laquelle elle est très répandue. Le commutateur assure une isolation complète entre l'hôte et le VLAN auquel il appartient.

VLANs du type Cisco Inter-Switch LinkISL VLANs

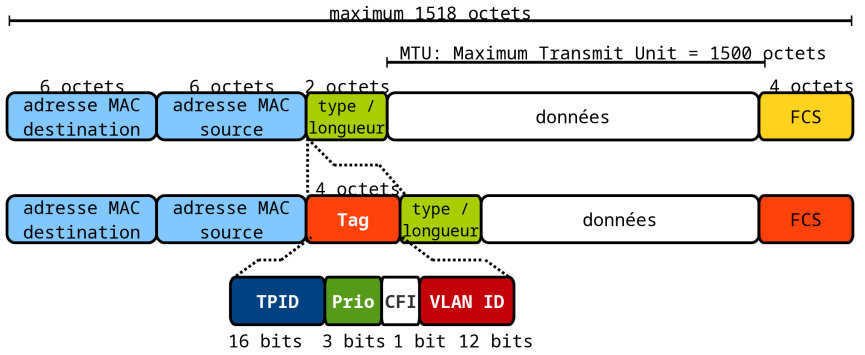
Cette technique propriétaire a été développée spécifiquement pour les équipements Cisco™. Elle complète les en-têtes de trames avec 30 octets répartis en 13 champs. Ce type d'encapsulation n'est plus beaucoup utilisé du fait de son incompatibilité avec le standard IEEE 802.1Q. La documentation Cisco™ est à l'adresse *InterSwitch Link and IEEE 802.1Q Frame Format*

VLANs IEEE 802.1Q

Le standard IEEE 802.1Q fournit un mécanisme d'encapsulation très répandu et implanté dans de nombreux équipements de marques différentes. C'est sur ce standard que s'appuie ce document. L'en-tête de trame est complété par une balise de quatre octets. Les champs contenus dans ces quatre octets sont présentés dans la section suivante. Les spécifications sont accessibles à l'adresse *IEEE 802.1Q Standard*

3.3. Balise IEEE 802.1Q

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. Le format de la trame Ethernet modifiée avec les 4 octets supplémentaires est présenté ci-dessous :



Il faut noter que le champ `FCS` est recalculé après l'insertion de la balise de VLAN.

Voici un extrait de capture, réalisée avec Wireshark, qui illustre les champs de la balise IEEE 802.1Q.

```
Frame 103 (1518 bytes on wire, 1518 bytes captured)
Ethernet II, Src: 00:14:f2:75:ed:72, Dst: 00:10:5a:de:9d:d7
    Destination: 3com_de:9d:d7 (00:10:5a:de:9d:d7)
    Source: Cisco_75:ed:72 (00:14:f2:75:ed:72)
    Type: 802.1Q Virtual LAN (0x8100) ❶
802.1Q Virtual LAN
    000. .... .... .... = Priority: 0 ❷
    ...0 .... .... .... = CFI: 0      ❸
    .... 0000 0110 0100 = ID: 100     ❹
    Type: IP (0x0800)
Internet Protocol, Src: 172.17.0.2 (172.17.0.2), Dst: 172.16.80.19 (172.16.80.19)
Transmission Control Protocol, Src Port: www (80), Dst Port: 1548 (1548)
```

❶ *Tag protocol identifier*TPIDEtherType

Ce champ de 16 bits identifie le protocole véhiculé dans la trame. La valeur `0x8100` désigne une balise IEEE 802.1Q / 802.1P.

❷ *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 au niveau réseau. Ces 8 niveaux sont utilisés pour fixer une priorité aux trames d'un VLAN relativement aux autres VLANs.

❸ *Canonical Format Identifier*

Ce champ codé sur 1 bit assure la compatibilité entre les adresses MAC Ethernet et Token Ring. 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*).

❹ *VLAN Identifier*vlan idVID

Ce champ de 12 bits sert à identifier le réseau local virtuel auquel appartient la trame. Il est possible de coder 4094 (2^12-2) réseaux virtuels (VLANs) avec ce champ.

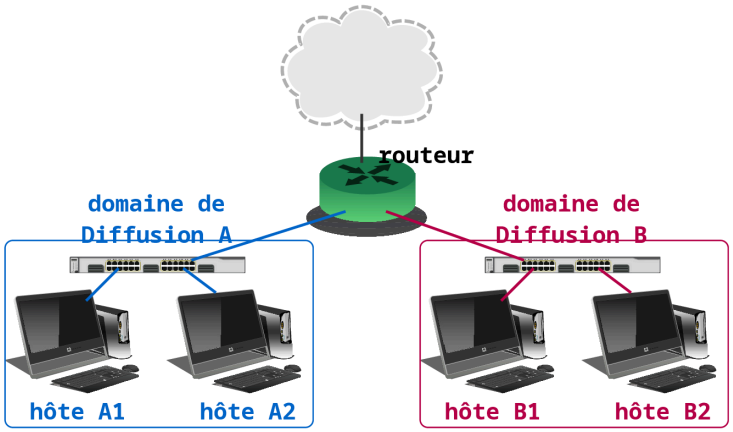
4. Routage inter-VLAN

A partir de l'argumentation développée précédemment et dans l'article *Segmentation des réseaux locaux*, on dispose de deux règles de base. Sans aucune programmation particulière des équipements :

- Une interface de ***commutateur*** délimite un domaine de ***collision***.
- Une interface de ***routeur*** délimite à la fois un domaine de ***collision*** et un domaine de ***diffusion***.

4.1. Situation avant routage inter-VLAN

Du point de vue conception, le respect de ces deux règles impose que l'on ajoute une interface de routeur pour chaque nouveau domaine de diffusion ou périmètre de contrôle. De plus, les commutateurs appartenant à un domaine de diffusion sont dédiés à ce domaine. Il n'est pas possible de distribuer plusieurs réseaux locaux virtuels entre plusieurs domaines de diffusion «isolés» par un routeur.



Remarques sur ce type de conception :

- Si on programme le commutateur A avec 2 VLANs distincts pour chacun des PCs A1 et A2, alors toute communication entre A1 et A2 sera impossible. De plus, ces deux PCs ne pourront communiquer avec d'autres réseaux que si l'interface du routeur RA appartient aux deux VLANs programmés.

  Cette situation peut présenter des avantages du point de vue exploitation mais elle dépend beaucoup de la gestion des interfaces physiques. Ce que ne montre pas le diagramme simplifié ci-dessus, c'est que le coût d'administration devient très important dès que le nombre de réseaux virtuels augmente.

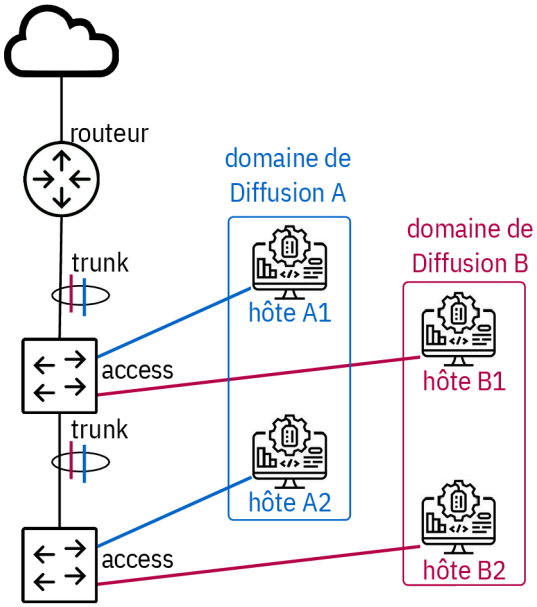
- Si l'utilisateur «associé» au PC A1 déménage dans un lieu ou seul le domaine de diffusion B est distribué, il est nécessaire d'étendre le domaine de diffusion A jusqu'à ce nouveau lieu. En conséquence, il faudra installer un nouveau commutateur et câbler de nouvelles prises entre le point de brassage principal du domaine A et ce lieu.

  Sur une même infrastructure, on se retrouve rapidement avec des commutateurs saturés pour lesquels tous les ports disponibles sont utilisés et d'autres commutateurs pour lesquels seuls quelques ports sont utilisés.

  Ce scénario montre qu'il est excessivement difficile d'optimiser le parc des ports de commutateurs avec ce type d'architecture. Le coût de l'infrastructure augmente donc fortement puisqu'il faut passer par des réinvestissements lourds en câblage et en équipements à chaque modification des périmètres.

4.2. Situation après routage inter-VLAN

Les deux règles de base énoncées ci-dessus ne sont pas remises en question. Il s'agit maintenant de dissocier les notions d'interface physique et d'interface de routage. On n'associe plus une interface physique à chaque domaine de diffusion mais une interface «virtuelle» (encore du virtuel !).



Remarques sur ce type de conception relativement à la situation sans routage inter-VLAN :

- Le contrôle d'accès est centralisé au niveau du routeur. Il n'existe plus de «mélange des genres» entre la programmation des commutateurs et le contrôle d'accès au niveau réseau. Les communications entre les hôtes d'un même domaine de diffusion ou entre plusieurs domaines de diffusion sont gérées de la même façon.

  On obtient donc de véritables réseaux locaux distribués sur la totalité de l'infrastructure (équipements de niveau 2 + équipements de niveau 3).

- La gestion du parc des ports de commutation est optimisée. Comme les domaines de diffusion sont partagés entre tous les équipements, la gestion des évolutions est beaucoup plus souple. Les déménagements n'entraînent aucun recâblage tant que l'évolution du nombre des hôtes n'implique pas une augmentation du nombre de ports. Il est donc possible de ***concentrer*** l'administration sur un nombre d'équipements plus faible que dans une architecture sans routage inter-VLAN.

4.3. Bande passante et trunks

En reprenant la remarque sur le partage des débits entre les VLANs à l'intérieur des ***trunks*** (voir à la fin de la Section 3.1, « Définitions »), il devient intéressant de partager le débit disponible en fond de panier dans des châssis de commutateurs. Le critère de choix d'un équipement, commutateur ou routeur, s'articule de plus en plus autour du rapport entre la capacité de commutation en millions de paquets par seconde (mpps) et le prix d'achat.

L'augmentation régulière des débits utiles par port favorise l'adoption d'architectures à base de routage inter-VLAN. Les évolutions techniques des routeurs conduisent à diminuer le nombre de leurs interfaces alors que les évolutions des commutateurs conduisent à augmenter considérablement le nombre de leurs ports.

Lors de la conception de la topologie physique d'une architecture, la densité de ports dans un rayon de 90m dans les réseaux filaires cuivre devient un point sensible. Si cette densité est importante, il faudra recourir à des équipements de type châssis qui permettent d'associer un module de routage à plusieurs modules de commutation. Tous ces modules disposent de composants spécialisés interconnectés en fond de panier sur différents bus eux aussi spécialisés. Si au contraire, la topologie physique est géographiquement plus étalée, on aura recours à l'agrégation de canaux. Cette technique permet d'augmenter la capacité utile d'un ***trunk*** en distribuant le trafic sur plusieurs canaux physiques vus comme un seul et unique lien.

5. Applications pratiques

Le routage inter-VLAN est utilisé plusieurs niveaux dans les documents présentés sur ce site.

Introduction au routage inter-VLAN

Le support de travaux pratiques *Routage inter-VLAN dans un contexte IaaS* est une introduction aux opérations de configuration. Il est basé sur une séparation entre la fonction de routage au niveau réseau assurée par un système GNU/Linux et la fonction de commutation des trames au niveau liaison assurée par un commutateur Cisco.

Introduction au routage dynamique avec OSPF

Le support de travaux pratique *Routage dynamique avec OSPF (Bird)* est une excellente occasion de caractériser l'indépendance entre topologie logique et topologie physique. En effet, la topologie physique est

de type étoile puisque l'on utilise des connexions filaires cuivre Ethernet alors que la topologie logique est de type triangle grâce à l'utilisation des VLANs.