

# Introduction

Dans un domaine de diffusion, c’est le switch qui orchestre la communication. Ce domaine est généralement relié à d’autres domaines de diffusion, grâce à un Router.

Si on s’intéresse à l’aspect de communication à une échelle plus grande, dans une institution ou une entreprise ; on cherche ainsi à minimiser les chances de tomber en un problème de broadcast, et d’éviter de subir des contraintes organisationnelles, avoir la possibilité d’ajouter un élément de sécurité est aussi un point positif et surtout de minimiser le nombre de périphériques réseaux.

Un moyen survient à cet effet, c’est de rassembler les terminaux en des groupements logiques, cette approche permet ainsi de subdiviser même un domaine de broadcast en des domaines plus petits. Une généralisation est possible pour des machines de nature différentes, dans le cas du « VXLAN ». Sans oublier qu’avec les VXLAN on est capable de faire un nombre plus important de groupements.

Ces groupements ne peuvent pas désormais communiquer, Elles auront besoin d’un élément supplémentaire, dans chaque cas de figure.

Par la suite, on va survoler l’approche VLAN qui va servir de référence et aborder les problèmes qui peuvent survenir, après on se penche sur les aspects propres au protocole VXLAN, et les mécanismes mises en place avec cette solution.

# I - VLAN

## A - Cas d’utilisation

### 1 - Plus de flexibilité, par rapport aux solutions non virtuelles

Partant d’une configuration des ports, on peut simplement taguer des ports à des VLAN. Cette configuration est facilement mise à jour, sans intervention. Ainsi la configuration de la structure du réseau est bien plus accessible ; cet aspect est très avantageux pour la collaboration en équipes.

Ainsi le partage d’une grande quantité de données aux appareils les uns des autres, en partageant un même VLAN s’ils travaillent sur des étages séparés ou dans des bâtiments différents.

### 2 - Réduction de la surveillance administrative

Les VLAN permettent aux administrateurs réseau de limiter automatiquement l'accès à un groupe spécifié d'utilisateurs en divisant les postes de travail en différents segments LAN isolés. Lorsque les utilisateurs déplacent leurs postes de travail, les administrateurs n'ont pas besoin de reconfigurer le réseau ou de modifier les groupes VLAN.

Une caractéristique intéressante des VLAN est qu'il est possible de changer la topologie logique sans déplacer aucun câble ni changer d'adresse, alors nous aurons juste besoin de configurer le segment sur le commutateur.

Ces facteurs réduisent le temps et l'énergie que les administrateurs doivent consacrer à la configuration et aux mesures de sécurité.

### 3 - Aspect rentable

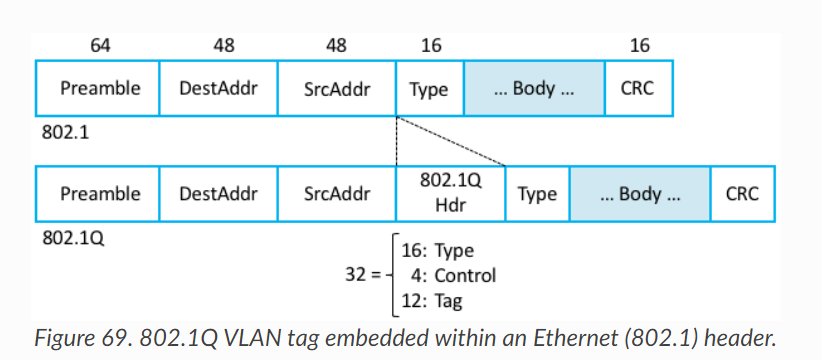
Puisque les hôtes communiquent avec les Switch VLAN et n’ont pas besoins de routeurs uniquement s’ils sont en train d’envoyer les données externes au VLAN, ceci permet au vlan de partage la charge des données (load-balancing) .Si elles étaient partagées via un routeur seront soumis à un goulot d'étranglement et influence ainsi la latence du réseau.

## B - Autres aspects du VLAN

On peut rappeler que le besoin pour les VLAN, est né au préalable à partir des limites de la mise en échelle des commutateurs, et désormais avec cette solution, on est non seulement capable de Contrôler la taille du domaine de diffusion, mais aussi d’employer des protocoles différents, sans avoir à soucier de l’incompatibilité qui pourrait se dérouler sans les VLAN.

### 1 - Structure d’une trame VLAN

Pour expliciter plus en détails les mécanismes de ce protocole, il faut déjà introduire la trame associée :



Partant de la spécification 802.1, on insère alors un header qui s’étend sur 32 bits comportant 16 bits qui permettent la compatibilité , les 4 bits de contrôles servent de définir la priorité et le tag qui est l’identificateur des réseaux virtuels qu’on peut associer , on peut avoir réseaux virtuels dans un seul LAN.

## C - Types de VLAN

##### 1 - VLAN par port

Avec ce mode, une trame peut alors avoir deux états, soit tagué à un VLAN et peut être alors reconnu depuis le commutateur. Dans le cas où la trame ne l’est pas, le commutateur identifiera à partir du port auquel la machine source est liéé et le transmet alors en des trames identifiées dans le même VLAN.

* Des problèmes de sécurité sont susceptibles d’avoir lieu si un pirate se connecte via un port tagué via une machine physique.

##### 2 - VLAN par adresse MAC

La segmentation du réseau selon les adresses MAC, en gardant l’encapsulation 802.1Q sur les segments trunk, permet de regrouper les services des utilisateurs.

* Le pirate doit avoir l’adresse MAC du VLAN pour accéder.

##### 3 - Vlan par sous-réseau

Une affectation automatique à un VLAN suivant une adresse IP. Par conséquent, il suffit de configurer les clients pour joindre les groupes souhaités. Il est aussi possible de séparer les protocoles par VLAN

* Le spoofing IP est possible qui est plus simple comparé au spoofing MAC.

# II - VxLAN

On commence par introduire le concept du VxLAN qui est une technologie overlay

## A - Technologie

### 1 - Avantage pour la virtualisation

Un des aspects à noter , à part le fait de pouvoir connecter des machines de différentes natures , est le fait de pouvoir déplacer les VM connecté dans le data center, étant dans un état de marche ; c’est la migration stateful. Cette possibilité n’est pas possible avec la création de sous réseau.

### 2 - Définition du VxLAN

VxLAN fournit des mécanismes d’agrégation et fait passer des tunnels entre multiples réseau de niveau 2 sur des infrastructures de niveau 3. (Overlay)

De ce fait, on peut alors connecter deux ou plusieurs réseaux de niveau 3 et comme si c’est un réseau de niveau 2 ; et c’est principalement grâce à cela qu’on arrivera à faire communiquer les machines virtuelles comme si elles opèrent sur le niveau 2.

### 2 - Critères d’implémentation

L’architecture initiale du réseau est un élément essentiel à considérer pour les VxLAN

#### Multicast

Dans la version de VxLAN sans contrôle plane, le multicast est nécessaire pour transporter le trafic provenant d’un serveur ; dans le cas d’une adresse mac inconnue pour le transfert des paquets ou même le multicast de trafic.

Le multicast est aussi utilisé dans le cas de découverte de VTEP endpoints, dans le cas où le contrôle plane est existant, on n’a pas besoin de cette fonctionnalité.

* IGMP (Internet Group Management Protocol) limite le trafic de broadcast dans un domaine de broadcast aux récepteurs et aux périphériques de multi broadcast intéressés. Dans un environnement avec un volume important de trafic de multidiffusion, l'utilisation d’IGMP préserve la bande passante car le trafic de multi broadcast n'est transféré que sur les interfaces où se trouvent des récepteurs IGMP.

#### Protocols de Routage

Zerghjkl;:

##### Routage intra Domain

##### Routage inter Domain

## B - Mécanisme

Généralement avec la technologie VxLAN l’objectif est de relié deux agrégation de réseau qui avec un Switch ou un vSwitch lorsqu’on souhaite connecter des machines virtuelles et c’est deux éléments rattachés avec un tunnel qui est l’élément principal du réseau overlay.

Des deux côtés les deux commutateurs encapsulent d’autres machines et permettent ainsi la communication non homogène des deux côtés.

Cette façon de faire permet aussi une meilleure allocation des ressources qui est assurée par l’environnement virtualisé au niveau 2.

Vu qu’avec l’encapsulation, on garde aussi les informations de niveau 2, on est assez certain d’avoir un couple unique entre VNI dans le cas des machines physique mais il faut impérativement éviter les MAC dupliqué au sein du même VNI qui peut apparaître dans les groupements de VM.

Un avantage aussi pour les machines virtuelles est que le mapping des VNI et toutes les encapsulations et les désencapsulations se font automatiquement au niveau de l’hyperviseur.

Les plates-formes de commutation compatibles VxLAN sont également responsables de la

Encapsulation / désencapsulations de la surcharge des périphériques réseau connectés 802.1q. Le VTEP doit être configuré avec la couche 2 ou le sous-réseau IP vers VNI.

Mappages réseau ainsi que VNI vers des groupes de multidiffusion IP. L'ancien mappage permet à VTEPS de créer des tables de transfert pour VNI / MAC.

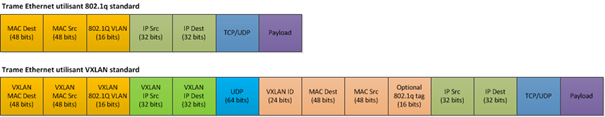
Les flux de trafic et ce dernier permet aux VTEP d'émuler des fonctions de diffusion / multidiffusion sur le réseau de superposition.

* Pouvoir désormais faire ça

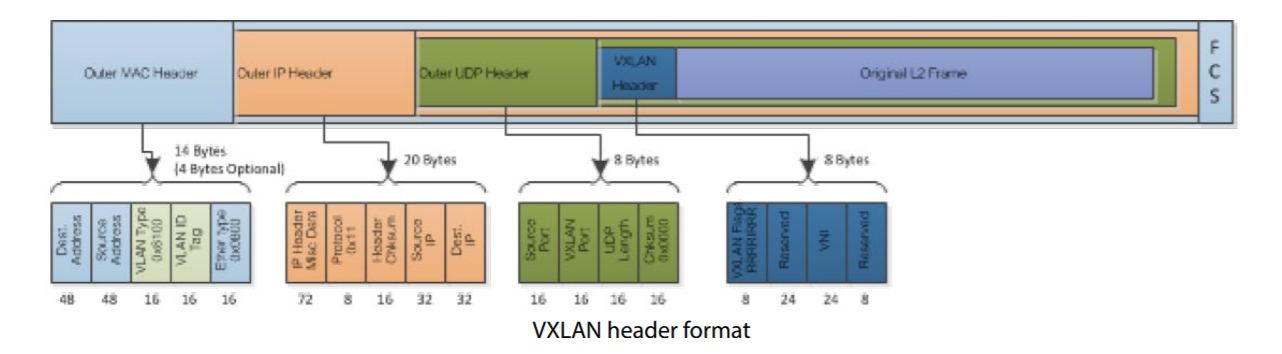
## C - Encapsulation

### 1 - Comparaison avec les VLAN

Si on regarde les deux trames à premier abord on peut remarquer la complexité supplémentaire qui est apportée



### 2 - Les caractéristiques du VxLAN

- Trame VxLAN : Trame UDP sur IP encapsulant la trame L2 provenant du tenant

- Le port UDP source est un hash de l’entête MAC interne à la trame pour permettre la répartition de charge.

- Limitations repoussées : 2^24 VxLAN possibles (VNI)

- Isolation : Seuls les nœuds dans le tenant peuvent communiquer entre eux

- Chaque tenant est indépendant et possède son adressage/MAC propre qu’il peut partager avec d’autres tenants

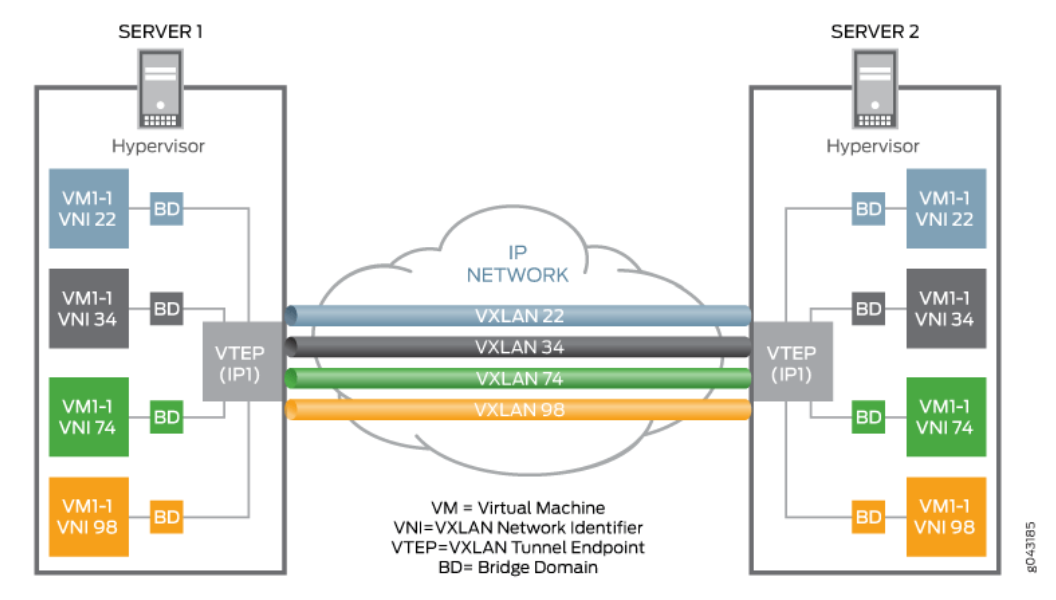
- Tagging (802.1Q) extérieur possible sur la trame VxLAN pour isoler le trafic sur un LAN sous-jacent.

- Notion de VTEP : VxLAN Tunnel End Point qui porte les entrées/sorties du tunnel VxLAN.

- Compatibilité : Les VM ne « voient » pas si elles sont sur un VLAN ou un VxLAN.

### 3 - Notions de Base

Quand on observe une architecture VxLAN plusieurs notions sont abordées, et chacune contribue à la compréhension de la logique.



**VXLAN Gateway**: est un portail qui laisse passer le Traffic entre les éléments VxLAN et non-VXLAN et fait office d’un end point virtuel pour le réseau.

**VXLAN segment**: un segment VXLAN de couche 2 au-dessus duquel les VM communiquent. Seulement les VMs du même segment peuvent communiquer entre eux.

**VNI**: Virtual Network Identifier (VNI), est aussi appelé VXLAN segment ID. cette information est utilisée pour identifier le tunnel.

**VTEP**: The VXLAN Tunnel Endpoint (VTEP) c’est le point qui clôture le Tunnel du VXLAN tunnel. Sachant que la même addresse IP peut être utilisée pour plusieurs tunnels.

**VXLAN header**: En plus de l’entête UDP, les packages encapsulées comporte aussi un header VxLAN qui comporte 24-bit de VNI pour identifier d’une façon unique le segment de niveau 2 dans le réseau qui se superpose à l’infrastructure.

### 4 - Règles de transfert

Avec ces éléments en place, le VTEP exécute ses règles de transfert:

1. Si les adresses MAC source et de destination vivent sur le même hôte, le trafic est commuté localement via le vSwitch et aucune encapsulation VxLAN se produit.

2. Si l'adresse MAC de destination n'est pas activée sur l'hôte ESX, les trames sont encapsulées dans l'entête VxLAN approprié par le source VTEP et sont transmises au VTEP de destination en fonction de sa table locale. Le VTEP de destination dégroupe la trame de l'entête VxLAN et le remet à la VM destinataire.

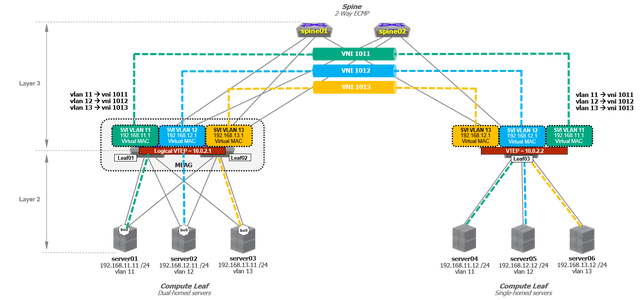
3. Pour le trafic unicast inconnu ou de diffusion / multidiffusion, le VTEP local encapsule la trame dans un entête VxLAN et envoie la trame encapsulée à l'adresse de multidiffusion VNI qui est attribuée au VNI au moment de la création. Cela inclut toutes les requêtes ARP, les requêtes Bootp / DHCP, etc. Les VTEP sur d'autres hôtes reçoivent la trame de multidiffusion et les traitent.

le trafic est (voir note 2 ci-dessus).

L'implémentation de ce schéma de tunneling est relativement simple par rapport à d'autres schémas, tels que MPLS ou OTV, car l'administrateur doit uniquement configurer les mappages VNI ou IP et les adresses de multidiffusion. Le reste est géré par les VTEP.

Voici des détails supplémentaires sur le format du cadre:

### Exemple d’infrastructure



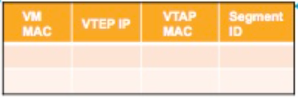
Ce mécanisme de transmission par tunnel permet alors de relier le réseau, et faisant comme si il existe une connexion directe, comme ce qui est mis en couleur dans la figure :

Les messages peuvent alors passer à travers ces tunnel, sans que les Machines virtuelles connectées ne soit conscient de ce chemin de transmission, dans l’illustration on peut remarquer que dans le réseau overllay il 6 sous réseaux sur lequel repose la logique du réseau Overlay.

Ces sous-réseaux sont fortement liés à des switch (leaf01, leaf02, leaf03) qui permettent d’assurer la connectivité. Puisque c’est ces éléments qui assurent l’intégrité et la liaison avec les tunnels.

Les couleurs verts, bleus, jaune permettent de mettre en reliefs les séparations logiques dans le modèle. Et qui détermine le cloisonnement du trafic qui circule dans cette structure, ces uplink permettent alors de relier l’architecture logique avec l’architecture virtuelle. Qui est alors une raison essentielle pour la simplification des tables de commutation.

Avec cette forte liaison entre les encapsulations, on peut raisonner par rapport aux sous-réseaux communicants qui dans notre cas portent la même couleur. Et on peut ainsi ne plus se préoccuper de l’architecture logique.

Pour communiquer, on doit commencer avec les VTEP qui permettent de savoir quel élément, ces endpoints qui dans le réseau peuvent apprendre et permettre de rejoindre les terminaux où les VMs selon le cas en remplissant une table de cette 

Forme qui est mise à jour depuis les deux

Extrémités du tunnel.

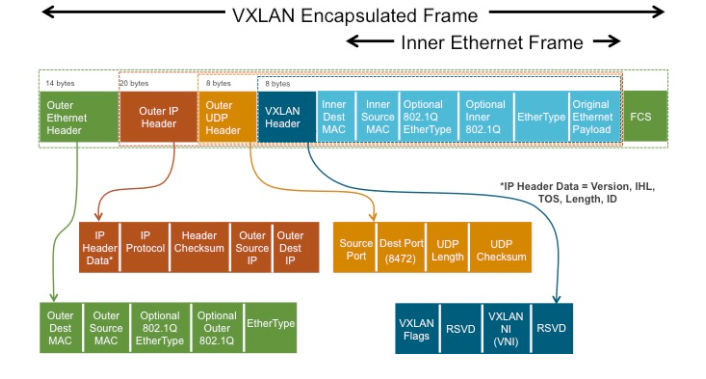
Les machines sont généralement rattachées aux serveurs dans une sorte de Pods

#### ARP broadcast

Dans le cas d’un message ARP broadcast, ce message est encapsulé dans un message multicast pour traverser le réseau. Et enrichit alors la table en retenant les chemins à suivre. Mais ceci aura toujours besoin du mapping MAC et IP par rapport au VTEP.

#### Chemin du paquet

On se basant sur l’apprentissage déjà évoqué dans le petit a ;



Si un terminal lié au serveur 1 cherche à envoyer un message en mettant l’adresse MAC et IP et l’adresse source IP et MAC de la machine relié au serveur 4, ce paquet reçu par le VTEP dans le tunnel de VNI 1011, à ce niveau il est lu et on identifie la source et utilise la table pour identifier la source et le chemin à suivre et encapsule le message avec des header propre au serveur 4 :

TO : 192.168.11.12/24

FROM : 192.168.11.11/24

UDP DST 4789

UPD SRC : Dynamique

VNI : 1011

L’UDP destinataire est réservé pour les opérations de VxLAN.

Le calcul dynamique d’UDP source facilite la tâche et permet l’équilibre de charge (load-balancing)

Le dernier élément est le plus important car c’est à travers cette information qu’on est capable de distinguer le trafic qui permet de joindre la destination.

Au niveau de serveur cette entête est décapsulé et fonctionne ainsi comme un protocole de niveau 2

* Cette opération se déroule identiquement dans l’autre direction de transmission, qui est effectuée grâce à l’encapsulation du VxLAN.

# III - Cloud et VXLAN

Comparé au VxLAN et au VLAN, VxLAN est sans aucun doute une meilleure solution avec des avantages évidents: des liaisons et une capacité suffisante pour gérer un Trafic massif dans un environnement cloud. La technologie VxLAN est destinée à fournir les mêmes services connectés aux systèmes d'extrémité Ethernet que les VLAN aujourd'hui, tout en offrant un moyen d'étendre le réseau L2 sur un réseau L3. VxLAN assure une isolation propre entre les machines virtuelles et l'infrastructure de transport IP physique, et permet une fiabilité et une évolutivité inégalées du réseau. N'oubliez pas que nous avons besoin de la terminaison VxLAN dans les périphériques physiques, tels que les commutateurs, les pare-feu et les équilibres de charge avant de pouvoir commencer à envisager des déploiements à grande échelle.

# Conclusion

Les solutions architecturales basées sur la couche 3 sont dominantes dans les plateformes et pour les communications à grande distance, le cas du VxLAN s’ajoute à cette catégorie d’infrastructure ayant déjà de fortes relations avec le cloud .Ethernet reste assez limitée par rapport à la scalabilité, étant basée sur des design en arborescents et surtout avec les protocoles de découvertes basées sur le broadcast de packets. VLAN permet assez d’avantages par rapport au modèle classique ; grâces l’agrégation de liens. VxLAN quand à lui apporte une solution de même nature qui est plus adaptée pour les Datacenter de son aspect scala blé et surtout en bénéficiant de la faculté de tourné sur des réseaux logique moins complexe en permettant les applications d’accéder à la structure et bénéficiassions de la gestion en masse grâce l’usage des adresse IP.

# Bibliographie

<https://tools.ietf.org/html/rfc7348>

<https://tools.ietf.org/html/rfc3069>

<https://www.ionos.fr/digitalguide/serveur/know-how/quest-ce-que-le-multiprotocol-label-switching-mpls/>

https://france.devoteam.com/devoblog/mettre-en-place-des-tunnels-vxlan-grace-aux-extensions-bgp-evpn/

https://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/white-paper-c11-737022.html

https://therandomsecurityguy.com/posts/vxlan/