[Titre du document]

[Sous-titre du document]

[École]

[Titre du cours]

# 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 ainsi à assurer la 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 la contraintes organisationnelles, la possibilité d’ajoute un élément de sécurité est aussi une point positive et surtout de minimiser le nombre périphériques réseaux.

Un moyen survient à cet effet, c’est de rassembler les terminaux en des groupements logique, cette approche permet ainsi de subdiviser même un broadcast domaine en des domaines plus petits. Cette approche peut être généralisée pour des machines de nature différente, dans le cas du « VXLAN ».sans oublier qu’avec les VXLAN on est capable de faire un nombre plus important de groupement.

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 de sécurité qui peuvent survenir, après on se penche sur les aspects propre au protocole VXLAN, et les mécanismes mises en avant avec cette solution.

# VLAN

## Cas d’utilisation

### 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.

### 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 aurions 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.

### Aspect rentable

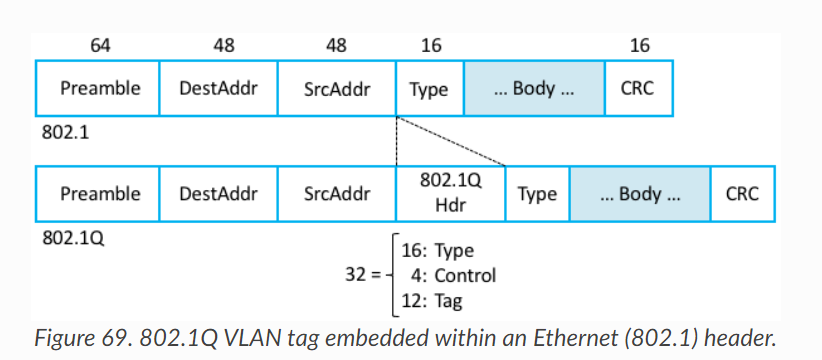
Puisque les hôtes communiquent avec les switches VLAN et n’ont pas besoins de routeurs uniquement s’ils sont en train d’envoyer les données externe au VLAN, ceci permet au vlan de partage la charge des données (load balencing) .Si elles étaient partagées via un routeur seront soumis à un goulot d'étranglement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

## Autres aspect VLAN

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

### Structure d’une trame VLAN

Pour expliciter plus en détails les mécanismes de se protocoles de niveau 2, il faut déjà commencer par introduire la trame associé :



Partant de la spécification 802.1, on insère alors un header qui s’étend sur 32 bits comportant 16 bites qui permettent la compatibilité , les 4 bits de contrôles servent de définir la priorité et les tag qui est l’équivalent des réseaux virtuelle qu’on peut associé qui permet d’avoir réseau virtuel partant d’un seul LAN physique.

#### VLAN par port

Avec ce mode, une trame peut alors deux états, soit taggué ou associé à un VLAN et peu alors reconnu depuis le Switch, dans le cas où la trame ne l’est pas, le switch identifiera à partir du port au quel est lié la machine et le transmet alors au trames identifiés dans le même VLAN.

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

#### 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.

#### 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.

# VXLAN

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

### Avantage pour la virtualisation

Un des aspects à noter , à part le fait de pouvoir connecté des machines de différentes nature , 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.

### Définition du VXLAN

VXLAN fournit des mécanismes d’agrégation et faire passer des tunnels entre multiples réseau de niveau 2 sur des infrastructures de niveau 3.

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

### Critères d’implémentation

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

#### Multicast: IGMP and PIM

#### Protocols de Routage: OSPF, BGP, IS-IS

# 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 élément rattaché avec un tunnel qui est l’élément principale du réseau overlay.

Des deux coté les deux Switchs 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 apparaitre dans les groupements de VM.

Un avantage aussi pour les machines virtuelles est que le mapping des VNI et toutes les Encapsulation 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.

=>

=>

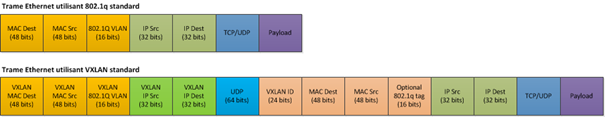
=>

=>

# Encapsulation

## Comparaison avec les VLAN

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



# 

A Chaque segment VXLAN on associe un identificateur de 24 bits VXLAN Network Identifier nommé VNI est c’est avec cet élément qu’on arrivé à avoir plus de sous réseau que dans le cas des VLAN

# Conclusion

# Bibliographie

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

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

<https://www.arista.com/assets/data/pdf/Whitepapers/Arista_Networks_VXLAN_White_Paper.pdf>

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

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