Présentation des vlan Mikrotik

WIFI FRANCE
NETWORKING SOLUTIONS

Introduction

Qu’est ce qu’un 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 géres logiquement

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.

La norme 802.1Q
Etiquetage du réseau VLAN

On utilise des étiquettes VLAN pour indiquer l appartenance à tel réseau VLAN d une trame en circulation.

Ces étiquettes sont fixées à la trame au moment où elle fait son entrée dans un port de commutateur appartenant à un réseau VLAN.

Elles sont retirées lorsque la trame quitte un port appartenant à ce réseau VLAN.

Le type du port appartenant au réseau VLAN détermine si l'étiquette VLAN doit ou non rester fixée à la trame. Les deux types de ports possibles au sein d un environnement VLAN sont les ports d'accès et les ports de liaison.

Chaque trame avec une étiquette VLAN comporte des champs indiquant son appartenance à un réseau VLAN. Il existe deux grands formats d étiquettes VLAN :

- le format de liaison inter-commutateur ISL de Cisco
- le format standard 802.1Q.

Tandis que ISL est un format propriétaire de Cisco, 802.1Q est un format IEEE standard. Le format 802.1Q permet aux trames étiquetées de circuler entre les commutateurs de plusieurs constructeurs.

L'étiquette 802.1Q comporte moins de champs que l'étiquette ISL. Elle est insérée dans la trame et non placée en début de trame.

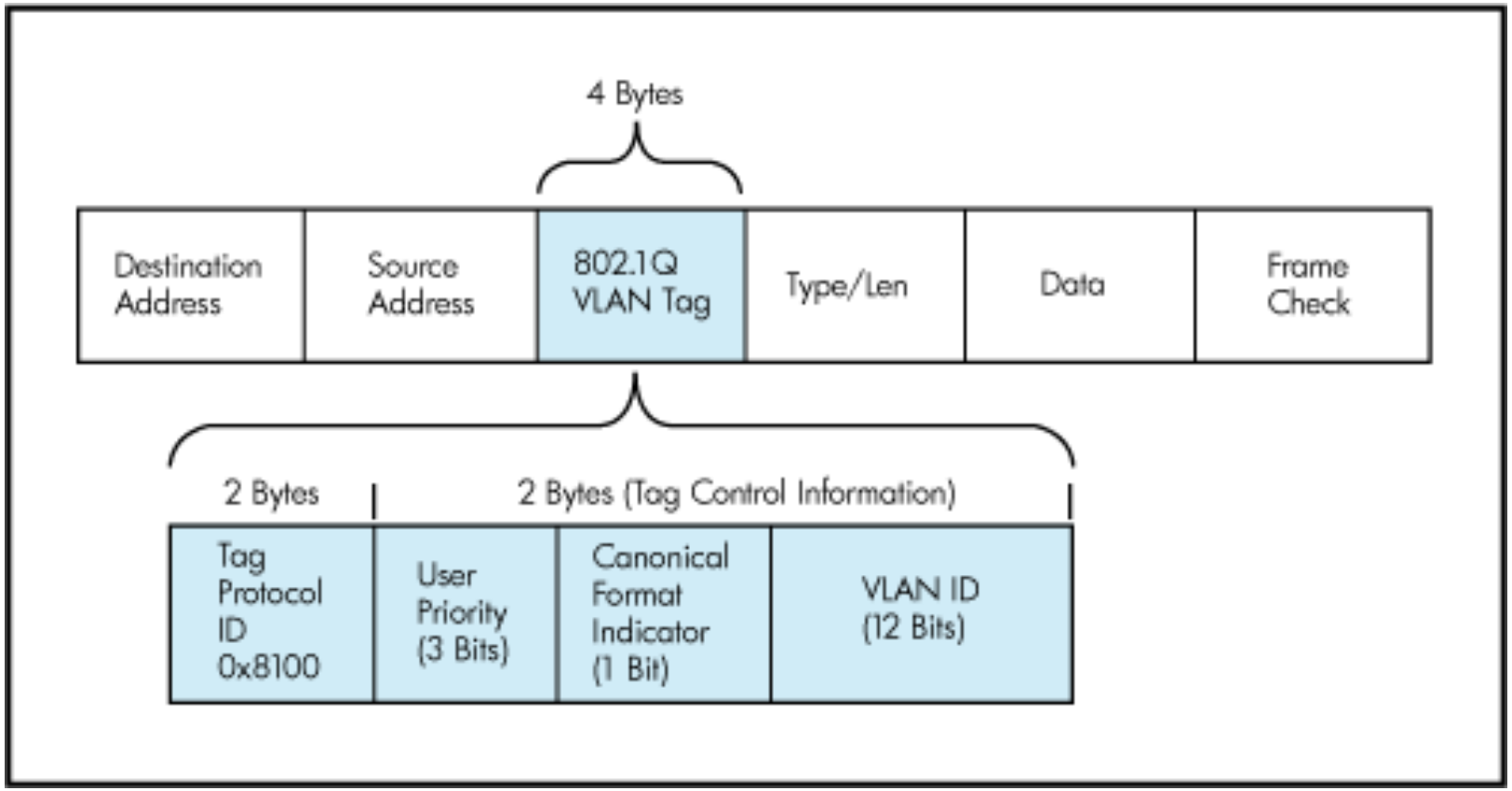
Comme le montre le schéma, le tag dot1q comporte plusieurs informations:

Un identifiant du protocole (2 octets)

3 bits pour indiquer une priorité (utilisés pour des fonctionnalités de QoS au niveau de la trame).

CFI: 1 bit servant à garantir la compatibilité entre les trames ethernet et token-ring (ce bit est toujours à 0 pour une trame ethernet).

L'identifiant du vlan, codé sur 12 bits (valeurs allant de 0 à 4096, certaines n'étant pas utilisées)

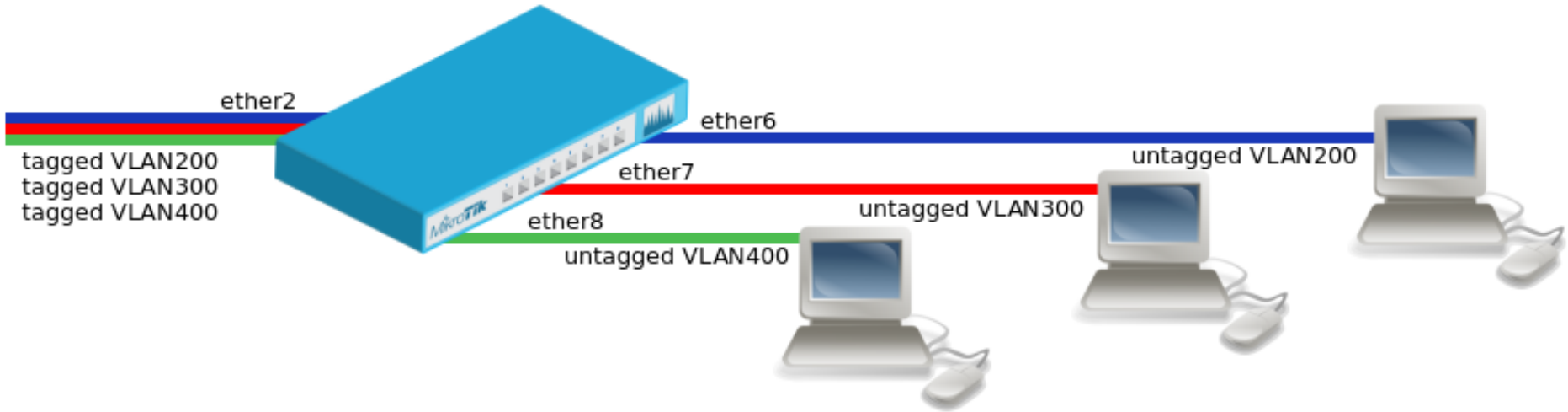


Vlan basé sur les ports

```
/interface vlan
add interface=ether2 name=eth2-vlan200 vlan-id=200
add interface=ether2 name=eth2-vlan300 vlan-id=300
add interface=ether2 name=eth2-vlan400 vlan-id=400

/interface bridge
add name=bridge-vlan200
add name=bridge-vlan300
add name=bridge-vlan400

/interface bridge port
add bridge=bridge-vlan200 interface=eth2-vlan200
add bridge=bridge-vlan200 interface=ether6
add bridge=bridge-vlan300 interface=eth2-vlan300
add bridge=bridge-vlan300 interface=ether7
add bridge=bridge-vlan400 interface=eth2-vlan400
add bridge=bridge-vlan400 interface=ether8
```



Vlan basé sur les adresses MAC

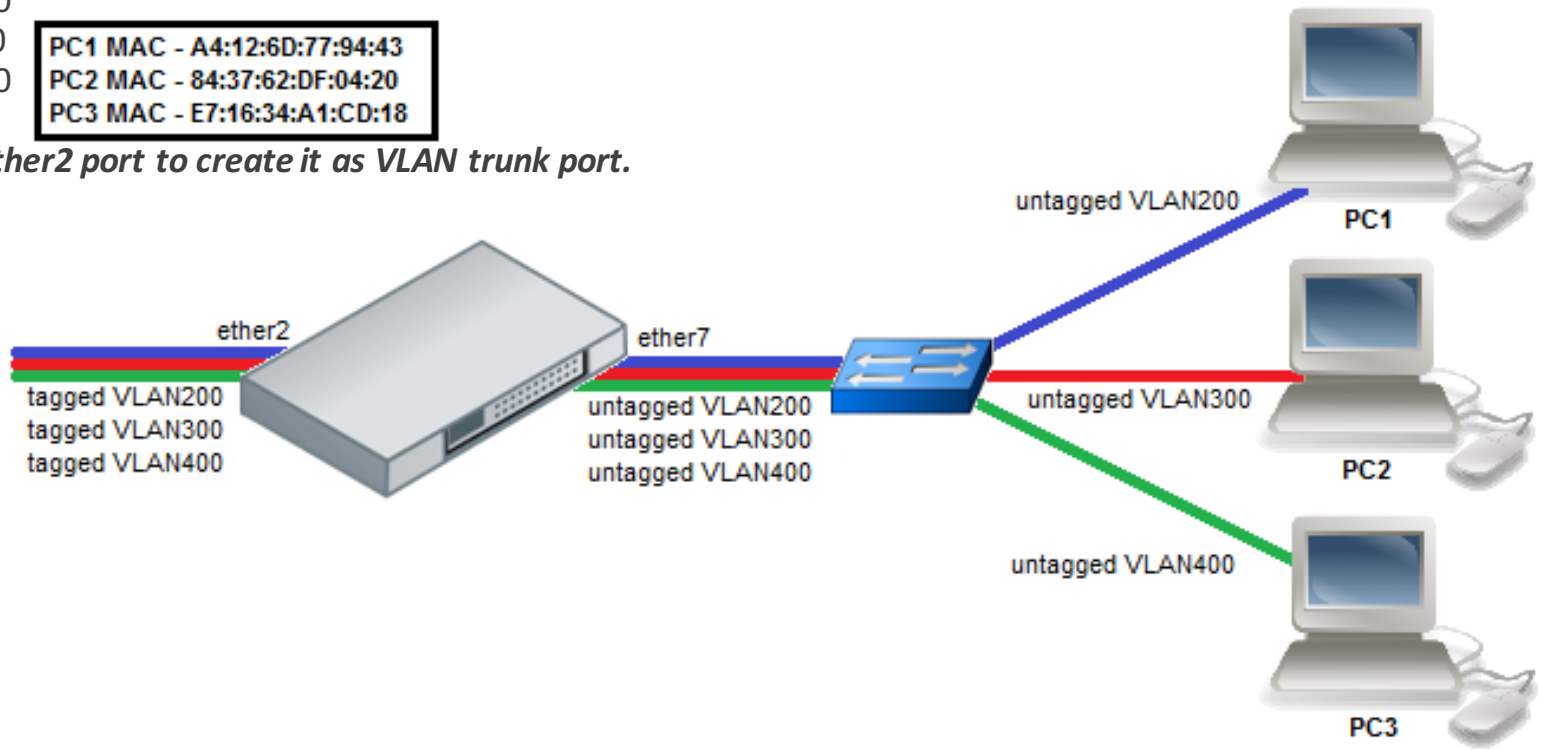
Create a group of switched ports.
/interface ethernet
set ether7 master-port=ether2

Enable MAC based VLAN translation on access port.
/interface ethernet switch port
set ether7 allow-fdb-based-vlan-translate=yes

Add MAC-to-VLAN mapping entries in MAC based VLAN table.
/interface ethernet switch mac-based-vlan
add src-mac=A4:12:6D:77:94:43 new-customer-vid=200
add src-mac=84:37:62:DF:04:20 new-customer-vid=300
add src-mac=E7:16:34:A1:CD:18 new-customer-vid=400

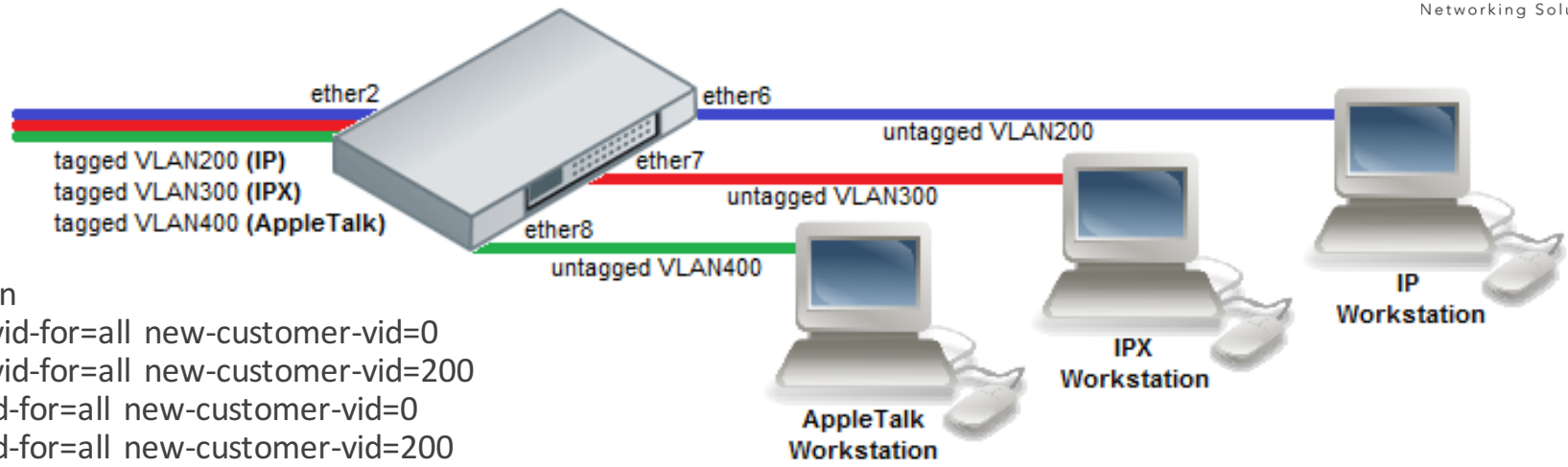
PC1 MAC - A4:12:6D:77:94:43
PC2 MAC - 84:37:62:DF:04:20
PC3 MAC - E7:16:34:A1:CD:18

Add VLAN 200, VLAN 300 and VLAN 400 tagging on ether2 port to create it as VLAN trunk port.
/interface ethernet switch egress-vlan-tag
add tagged-ports=ether2 vlan-id=200
add tagged-ports=ether2 vlan-id=300
add tagged-ports=ether2 vlan-id=400



Vlan basé sur le protocole

Create a group of switched ports.
/interface ethernet
set ether6 master-port=ether2
set ether7 master-port=ether2
set ether8 master-port=ether2



Set VLAN for IP and ARP protocols
/interface ethernet switch protocol-based-vlan
add port=ether2 protocol=arp set-customer-vid-for=all new-customer-vid=0
add port=ether6 protocol=arp set-customer-vid-for=all new-customer-vid=200
add port=ether2 protocol=ip set-customer-vid-for=all new-customer-vid=0
add port=ether6 protocol=ip set-customer-vid-for=all new-customer-vid=200

Set VLAN for IPX protocol
/interface ethernet switch protocol-based-vlan
add port=ether2 protocol=ipx set-customer-vid-for=all new-customer-vid=0
add port=ether7 protocol=ipx set-customer-vid-for=all new-customer-vid=300

Set VLAN for AppleTalk AARP and AppleTalk DDP protocols.
/interface ethernet switch protocol-based-vlan
add port=ether2 protocol=0x80F3 set-customer-vid-for=all new-customer-vid=0
add port=ether8 protocol=0x80F3 set-customer-vid-for=all new-customer-vid=400
add port=ether2 protocol=0x809B set-customer-vid-for=all new-customer-vid=0
add port=ether8 protocol=0x809B set-customer-vid-for=all new-customer-vid=400

Retrouvez toute la gamme MikroTik sur www.wifi-France.com