Les VLAN

Présentation

Un vlan permet de segmenter un domaine de diffusion en plusieurs domaines et indépendamment de l'emplacement où se situent les nœuds, ce sont des domaines de diffusion logiques.

Les vlan permettent de :

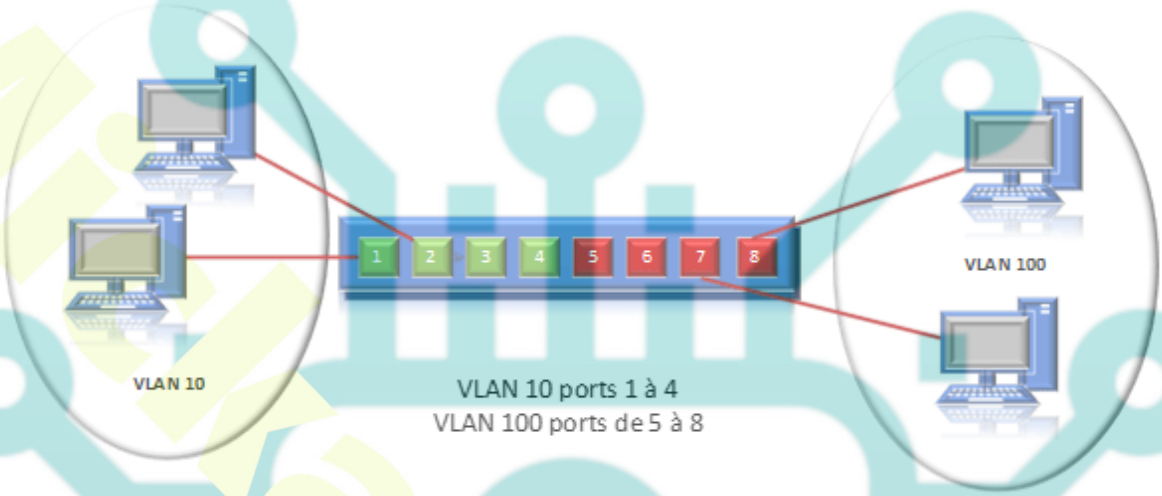
Réduire les messages de diffusion (notamment les requêtes ARP) en les limitant à l'intérieur d'un vlan.
Créer des groupes de travail indépendants de l'infrastructure physique.
Augmenter la sécurité par le contrôle des échanges inter-vlan en utilisant des routeurs filtrants ou des options propriétaires au constructeur.

https://www.youtube.com/watch?v=nsv28gyZozU

Explication vlan

Les différents niveau

VLAN PAR PORT (VLAN de niveau 1)



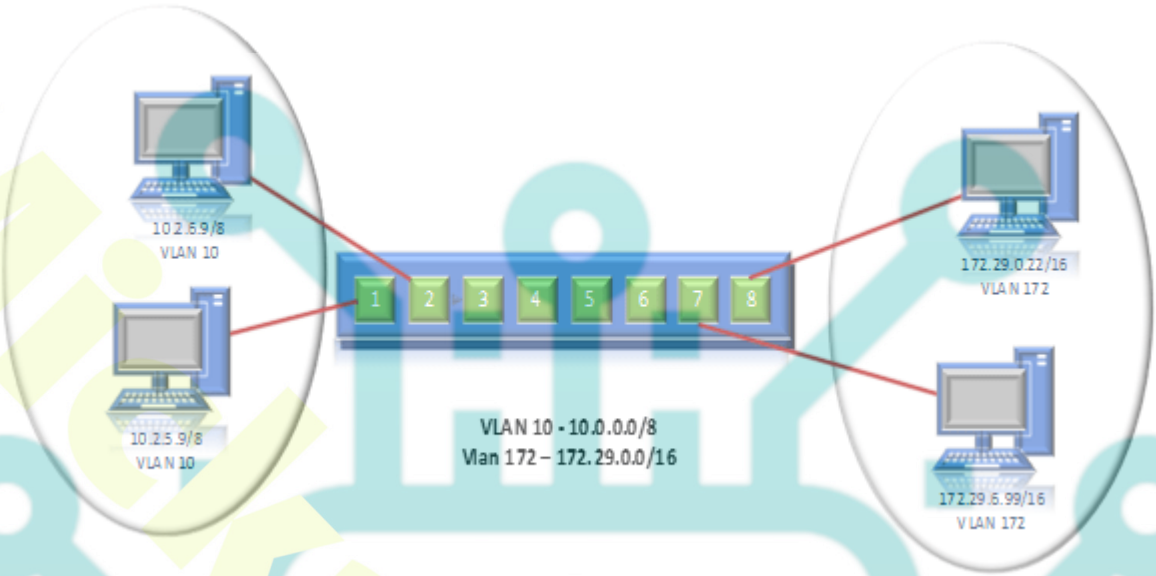
Vlan par port

- 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

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
- On affecte dynamiquement les ports des commutateurs à chacun des vlan en fonction de l'adresse MAC de l'hôte qui émet sur ce port

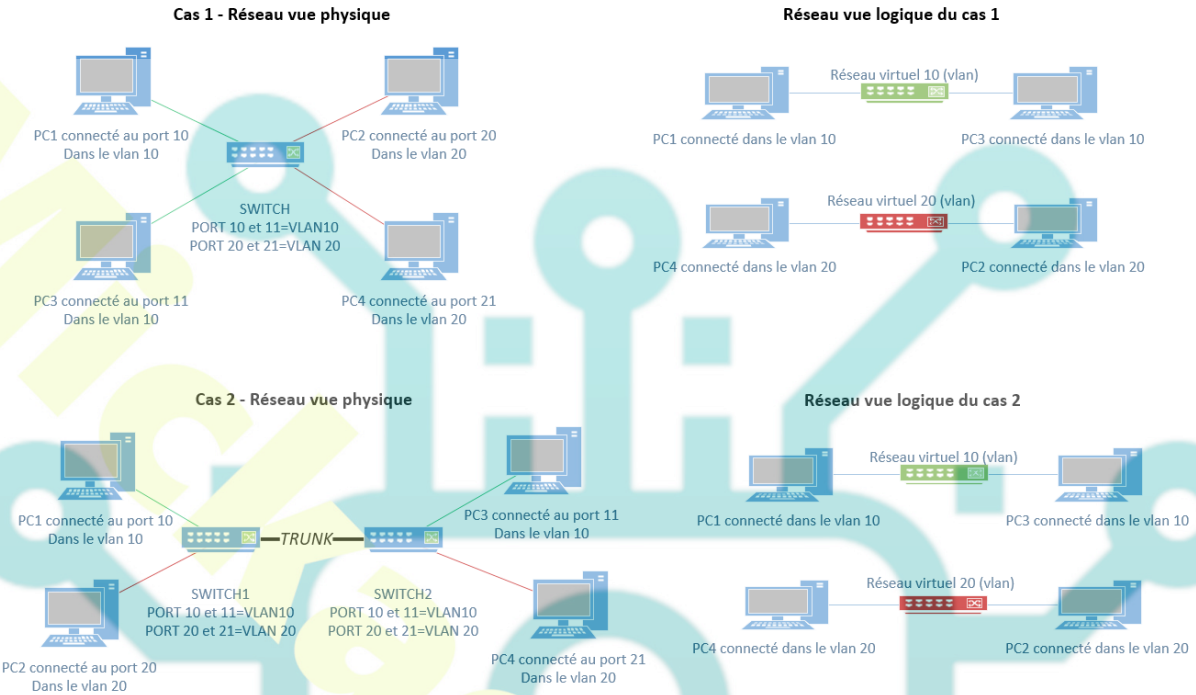
VLAN par adresse IP (VLAN de niveau 3)



Vlan par IP

- 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 qu'elle contient (le commutateur doit donc accéder à ces informations)
- On affecte dynamiquement les ports des commutateurs à chacun des vlan en fonction des adresses réseau

Vue VLAN physique et logique



La norme 802.1q (vlan taggé ou étiqueté)

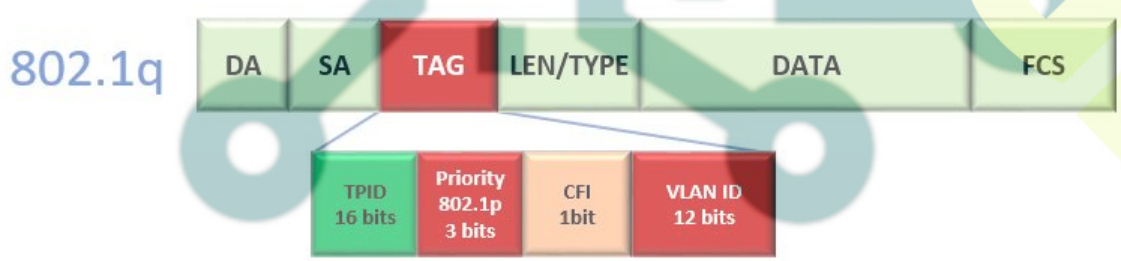
Cette norme permet d'ajouter des informations à la trame Ethernet standard.

La norme définit trois types de trames :

Trames **non étiquetées** – trames qui ne contiennent aucune information sur l'appartenance à un Vlan

Trames **étiquetées** – trames qui contiennent un en-tête supplémentaire.

Trames **étiquetées par une priorité** – définie par la norme 802.1p



TPID – Identificateur de protocole de tag qui permet d'identifier les trames étiquetées des trames non étiquetées.

PCP – Point de code de priorité, classe de service IEEE 802.1p (*voir plus bas dans le cours*)
CFI – indique si la trame est Ethernet ou Token Ring
VLAN ID – Spécifie le vlan auquel appartient la trame

Les trames sont contrôlées par des règles d'entrée (ingress rules)
Les opérations liées à la décision de commutation sont contrôlées par des tables de filtrage (filtering database)
Les opérations liées au traitement d'une trame en sortie sont contrôlées par des règles de sorties (egress rules)
Les paramètres associés à un port peuvent être (tagged, untagged, forbidden, priority tagged)

Gestion du TAG

création peut être **statique** ou **dynamique**. Un vlan statique est un vlan créé manuellement sur le commutateur, alors qu'un vlan dynamique est un vlan dont la création sur le commutateur résulte d'un échange avec un autre élément (serveur d'authentification, switch)

VLAN CAS 1

Ports non tagué en règle de sortie (EGRESS) *mode ACCESS (Cisco)*

Seul le switch connait l'existence des vlan

PC1 connecté au port 10
Carte réseau non taguée

PC2 connecté au port 20
Carte réseau non taguée

SWITCH
PORT 10=VLAN10
PORT 20=VLAN 10

Règle interne au switch (INGRESS)

Si trame Ethernet arrive sur le port 10, elle est taguée VID10

Si trame Ethernet arrive sur le port 20, elle est taguée VID10

Règle externe au switch (EGRESS)

Si trame Ethernet sort sur le port 10, ***«on enlève l'étiquette (TAG) VID10"***

Si trame Ethernet sort sur le port 20, ***«on enlève l'étiquette (TAG) VID10"***

1) Trame Ethernet X partant de PC 1

@MAC SOURCE PC1	@MAC DESTINATION PC2

2) Trame Ethernet X entrante sur port 10 traitée par le switch règle INGRESS

@MAC SOURCE PC1	@MAC DESTINATION PC2	VLAN VID=10

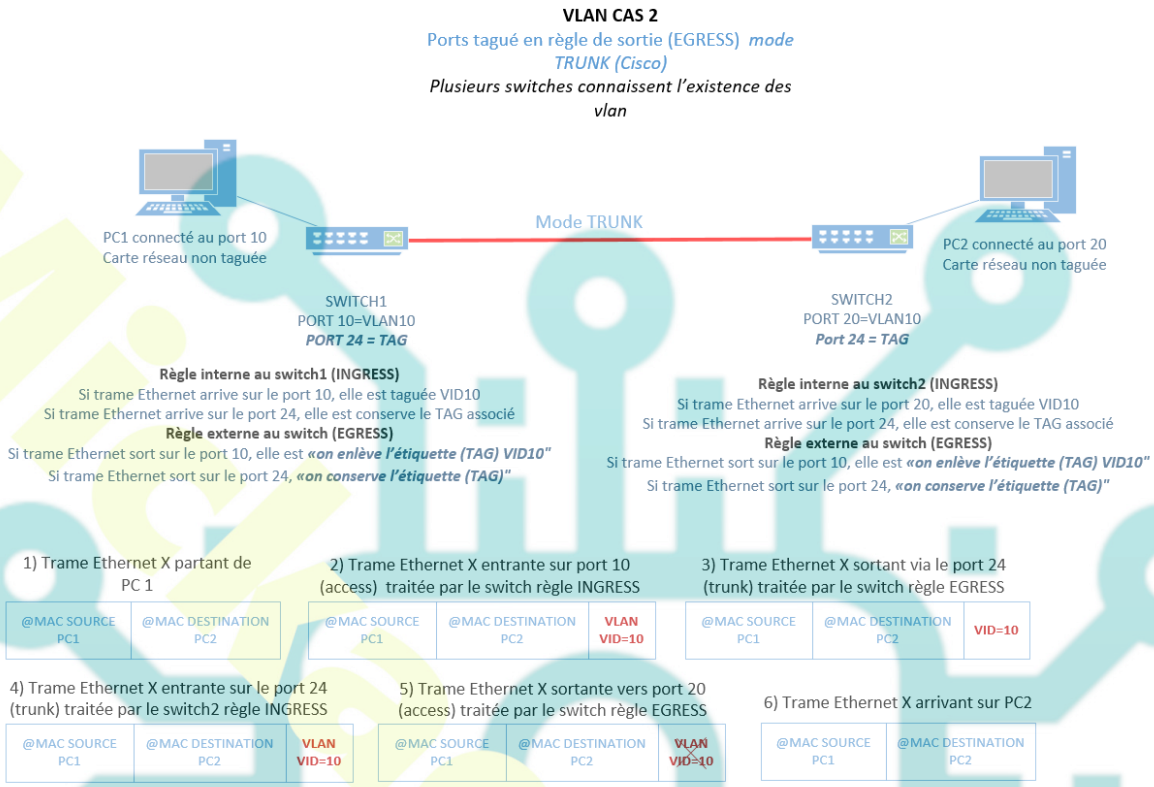
3) Trame Ethernet X sortante port 20 traitée par le switch règle EGRESS

@MAC SOURCE PC1	@MAC DESTINATION PC2	~~VID=10~~

4) Trame Ethernet X arrivant sur PC2

@MAC SOURCE PC1	@MAC DESTINATION PC2

Tag de la trame au sein d'un switch



Tag de la trame multi switch

Norme 802.1p

C'est un mécanisme de qualité de service pour différencier les flux.
802.1p définit 8 classes de service différentes. La manière dont le trafic sera ensuite géré en fonction de la classe à laquelle il sera affecté, n'est pas défini et reste du ressort des constructeurs.

Norme 802.1p

C'est un mécanisme de qualité de service pour différencier les flux.
802.1p définit 8 classes de service différentes. La manière dont le trafic sera ensuite géré en fonction de la classe à laquelle il sera affecté, n'est pas défini et reste du ressort des constructeurs.

User priority	Traffic Type
0	Best Effo rt (au mieux)
1	Background (arrière plan)
2	Spare (économie)
3	Excellent effort
4	Controlled Load (charge contrôlée)
5	Video
6	Voice
7	Network Control (administration)

Classe de trafic

Transmettre les informations de vlan entre switches

Le protocole MVRP (anciennement GVRP)

La création dynamique des vlan et l'affectation dynamique des ports se fait via le protocole MVRP (Multiple VLAN Registration Protocol – 802.1ak). Si le protocole est activé, tous les ports participent.

Le protocole MVRP est fourni spécifiquement pour la diffusion automatique des informations relatives à l'appartenance aux VLAN entre les switches compatibles VLAN.

Le protocole MVRP permet aux switches compatibles VLAN d'apprendre automatiquement l'adressage des ports VLAN sans avoir à configurer individuellement chaque switches et à enregistrer l'appartenance à un VLAN.

Le protocole VTP (Cisco)

C'est un protocole propriétaire Cisco de niveau 2 qui permet l'envoi de messages VTP pour annoncer la création, la suppression ou la modification de vlan.

Le switch possède 3 modes VTP : client, transparent ou server (actif par défaut) :

> VTP **Server** : le switch en mode Server permet à l'administrateur de faire toute modification sur les vlan, ces modifications sont propagées automatiquement vers tous les switches du réseau.
> VTP **Client** : Le switch en mode Client ne permet pas à l'administrateur de faire des modifications sur les vlan.
> VTP **Transparent** : le switch en mode Transparent permet à l'administrateur de faire toute modification sur les vlan en local uniquement et donc ces modifications ne sont pas propagées vers les autres switches du réseau.

Les vlan spécifiques

Vlan VoIP

Ce vlan permet d'isoler les flux de voix des flux de données. Il est proposé par les switches pour gérer la ToIP (téléphonie sur IP)

Vlan par règle ou par type de service

Une solution basée sur des vlan par SSID est possible pour isoler les réseaux Wifi.

Vlan QinQ

Véhicule des informations de vlan dans d'autres vlan (voir cours réseaux étendus)

Vlan 802.1x

Permet l'accès au vlan via authentification.

Principe de fonctionnement
Le client peut envoyer son identité dans un paquet EAP au commutateur.
Le serveur RADIUS reçoit le paquet du commutateur et interroge sa base de données.
Il renvoie le résultat de cette interrogation au commutateur sous forme d'un commandement d'ouverture du port, assorti d'un numéro de VLAN dans lequel placer le client.
A partir de ce moment seulement, il peut y avoir d'autres trames échangées entre le client final et le reste du réseau, comme une trame de requête DHCP par exemple.

PRIVATE VLAN

Depuis quelques années les entreprises ont recours à l'utilisation de vlan pour segmenter leurs réseaux. Elles attribuent à ces vlan un sous-réseau IP qui est routé via des équipements de Niveau 3 (routeur, pare-feu, switch niveau 3)

Cependant, il y a une surabondance de sous-réseaux afin d'apporter une sécurité suffisante entre les différentes machines.

Le Private VLAN est là pour pallier cet excès de découpage et amène une sécurité de niveau 2 supplémentaire. Par exemple, l'utilisation de zone WIFI invité pour interdire à quelqu'un de sniffer les communications (le wifi utilisant la diffusion) ou pour les DMZ, afin d'éviter la multiplication de ces zones sur les pares-feux.

VLAN PRIMARY

Simplement le vlan d'origine. Ce vlan est utilisé pour envoyer les trames « descendantes » vers tous les vlan secondaires.

VLAN PROMISCUOUS

Un nœud attaché à ce vlan peut envoyer et recevoir des paquets avec n'importe quel autre nœud résidant sur des PVLAN secondaires. On y attache un routeur par exemple.

LES VLAN SECONDAIRES

Ils possèdent un numéro de vlan et appartiennent à un des types suivants :

Vlan isolé / isolated vlan : il a des propriétés de communication plus limitées.
Il ne peut communiquer que vers et depuis son PVLAN promiscuité. Il ne peut pas communiquer avec d'autres vlan, en outre, les nœuds au sein d'un PVLAN isolé ne peuvent pas communiquer entre eux non plus.
Les pvlan isolés sont généralement utilisés pour le WIFI.

Vlan communauté / community vlan : Les hôtes étant dans un même vlan communautaire peuvent communiquer entre eux et également avec le vlan promiscous. Cependant, ils ne peuvent pas communiquer avec les autres vlan.
Il peut y avoir plusieurs vlan communautaires au sein d'un vlan privé.

VLan Trunk : Ce vlan fait l'agrégation des autres vlan vers un lien physique

Dans l'exemple, les pvlans Community (203) et isolated (204) sont configurés pour parler par l'intermédiaire du pvlan promiscous(103). Ils appartiennent au même vlan primaire

Primary VLAN ID	Secondary VLAN ID	VLAN Type
103	103	Promiscuous
103	203	Community
103	204	Isolated

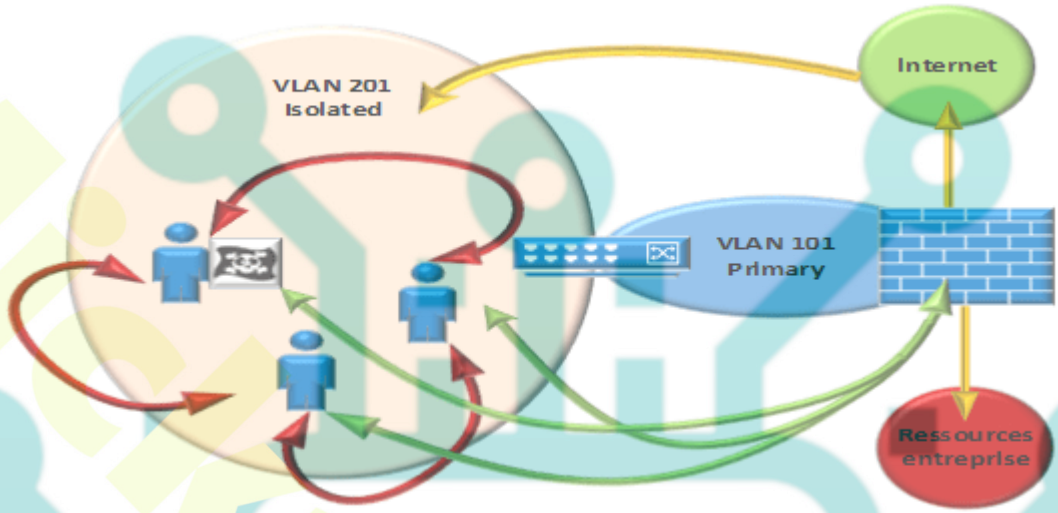
Exemple d'utilisation

Zone "WIFI invité"

Dans le cas des zones invitées, l'isolation des clients est un besoin, car les utilisateurs de l'entreprise sont adeptes du BYOD.

Pour réaliser cette isolation, il faut mettre les clients dans un vlan « isolated », et mettre le Pare-Feu dans un vlan « Primary »

Dans l'exemple ci-dessous, les utilisateurs situés dans l'isolated vlan ne peuvent communiquer entre eux mais ils peuvent utiliser internet via le vlan primaire.

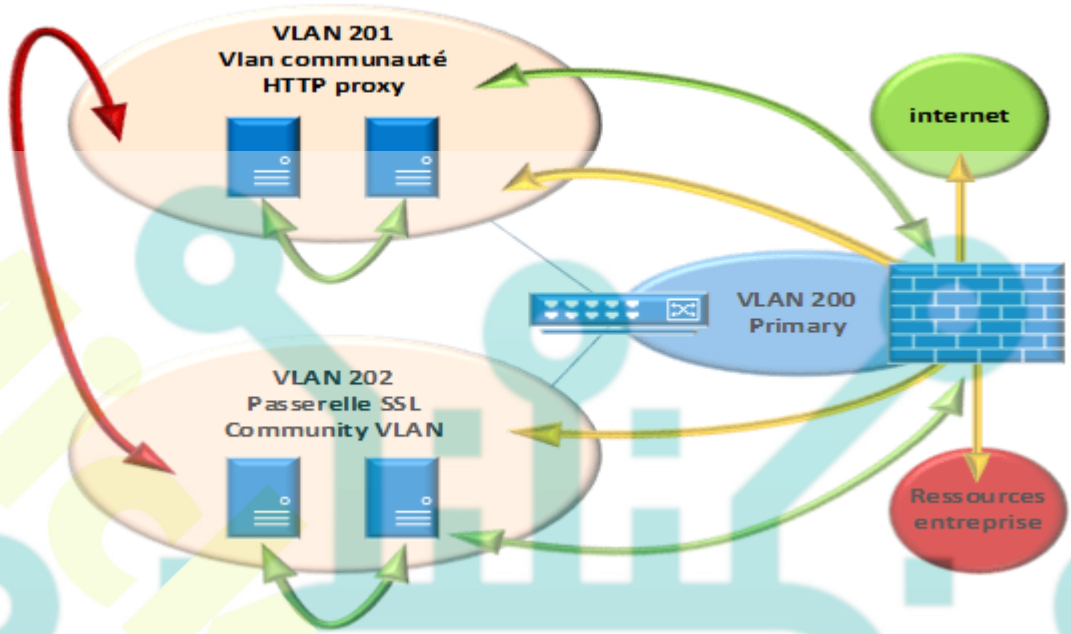


Zone "DMZ"

L'objectif est d'éviter les multiples zones avec interfaces supplémentaires sur les Pare-Feu. Pour réaliser cette isolation, on met les serveurs Proxy et les Passerelles SSL dans des vlan « Community » séparés et le Pare-Feu dans un vlan « Primary ».

Les serveurs peuvent communiquer directement au sein de leur communauté, mais pas directement avec les autres communautés.

Ils ont cependant une ressource commune, le Pare-Feu qui contrôle les accès vers le reste du réseau : Lan, Wan.

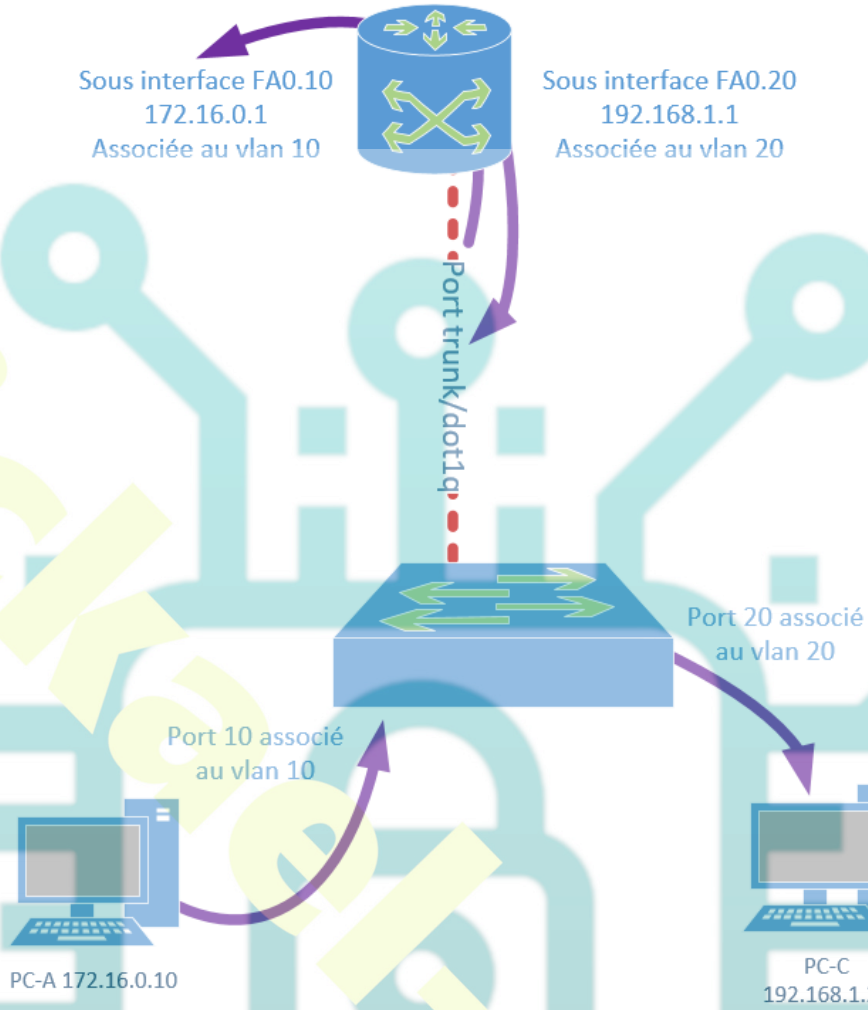


LE ROUTAGE INTERVLAN

Le routage intervlan permet d'interconnecter les messages entre plusieurs réseaux IP situés dans des vlan différents.
Ce routage peut être effectué par un routeur traditionnel ou par un switch de niveau 3 intégrant le service de routage.

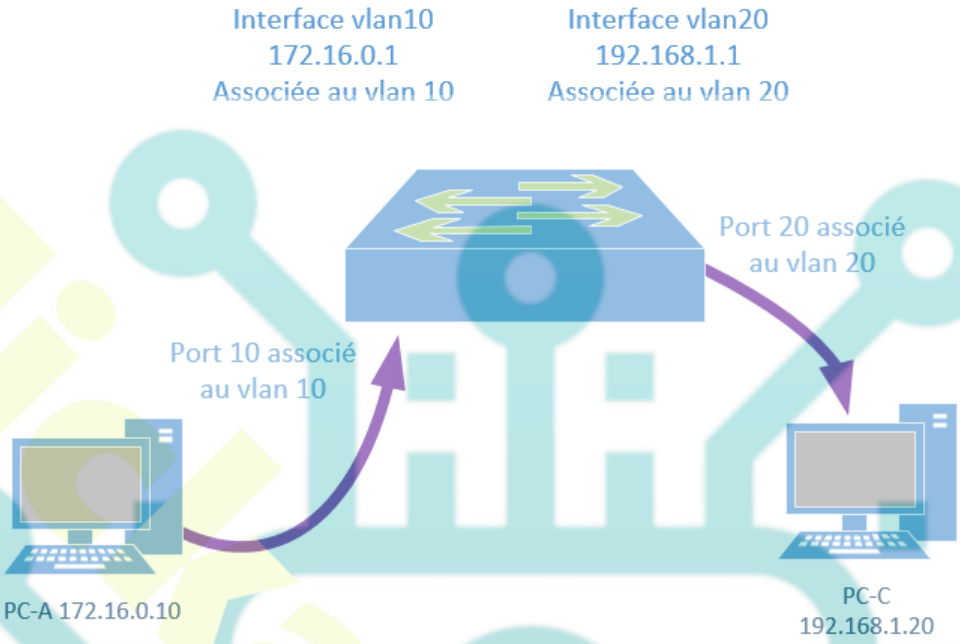
Plusieurs techniques sont possibles

- Un routeur avec une interface réseau dans chaque vlan. Cependant, cette technique n'est plus possible lorsqu'il y a de nombreux vlan.
- Un routeur supportant le tag (802.1q) Dans ce cas une seule interface physique est nécessaire, on utilisera la notion d'interface logique (1 par vlan)



VIA ROUTEUR

- Un switch intégrant le routage. Cette solution est la plus efficace, cependant, ce type de commutateur est plus onéreux qu'un commutateur standard.



Routage sur switch de niveau 3