Université
De Boumerdes

Université
De Limoges

Vlans

Réalisé par : Dr RIAHLA
Dr à l'université de limoge (France)

2016/2017

Plan

- Segmentation d'un VLAN
  - Définition, Problématique
  - Avantage,
  - Type de VLAN
  - Etiquetage des trames Ethernet)
- Protocole DTP (Dynamic Trunking Protocol)
- Sécurité et conception VLAN
- Routage inter-VLAN

Introduction Vlans

PROBLEMATIQUE

Problématique

- Durant ma formation à la Direction Mud-Logging, division forage de SONATRACH, j'ai constaté certaines lacunes dans l'exploitation des ressources existantes, ce qui nuit à l'efficacité et au rendement des employés.

- Dans l'entreprise : Les hôtes et serveurs connectés à des commutateurs de la couche 2 font partie du même segment de réseau. Cette configuration présente deux problèmes considérables.

Problématique

1_Sous l'impulsion des commutateurs, des diffusions inondent tous les ports, ce qui consomme de la bande passante de façon inutile. Plus le nombre de périphériques connectés à un commutateur est important, plus le trafic de diffusion généré est volumineux et plus la quantité de bande passante gaspillée augmente.

2_Chaque périphérique connecté à un commutateur peut transférer et recevoir des trames à partir de chaque autre périphérique du commutateur.

Objectif du travail

Objectif du travail

Pour répondre à cette problématique, j'ai présenté une solution qui est développé autour des VLANS

- **Vlan?**
- **Pourquoi les réseaux locaux virtuels ?**

Pourquoi les réseaux locaux virtuels ?

1_ Les réseaux locaux virtuels assurent la connectivité et la **sécurité**, tout en contrant les diffusions et les domaines défaillants.

2_ Les réseaux locaux virtuels segmentent de façon **logique** les réseaux et contiennent des diffusions afin d'améliorer la sécurité et les performances du réseau.

3_Les commutateurs sur lesquels **l'agrégation** est activée permettent aux réseaux locaux virtuels de s'étendre sur de nombreux sites géographiques.

4_Le protocole **VTP** (vlan trunking Protocol) est utilisé pour simplifier la configuration et la gestion des réseaux locaux virtuels au sein d'un réseau complexe d'entreprise commuté.

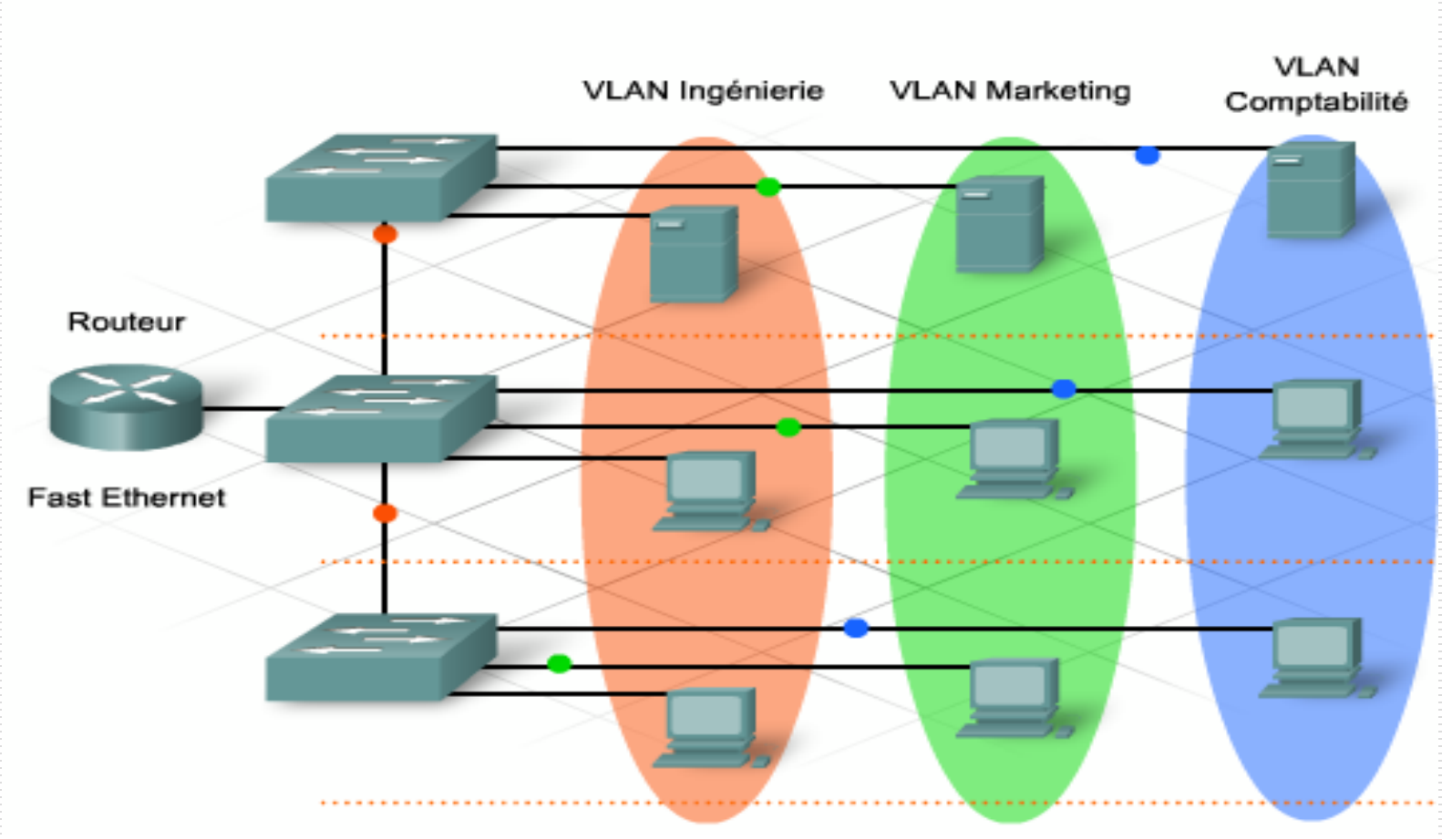
Les réseaux locaux virtuels

En raison de ce regroupent logique, une diffusion est transmise uniquement aux machines du même VLAN. Même si les deux machines se trouvent physiquement dans le même commutateur.

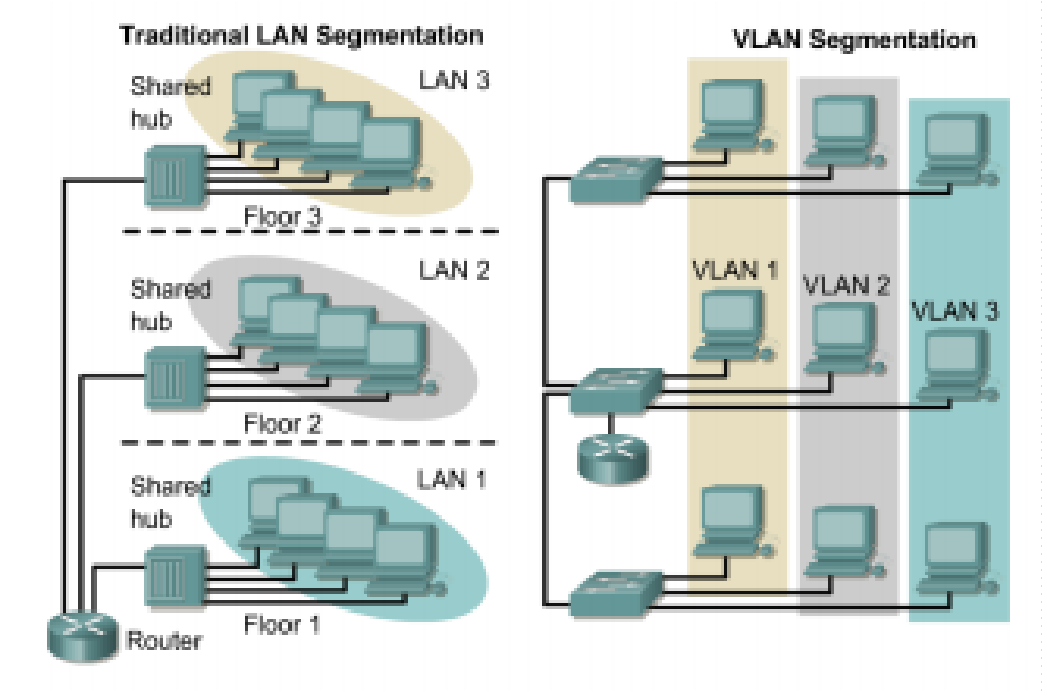
Chaque réseau local virtuel fonctionne donc comme un réseau local distinct.

Un réseau local virtuel détend sur un ou plusieurs commutateurs.

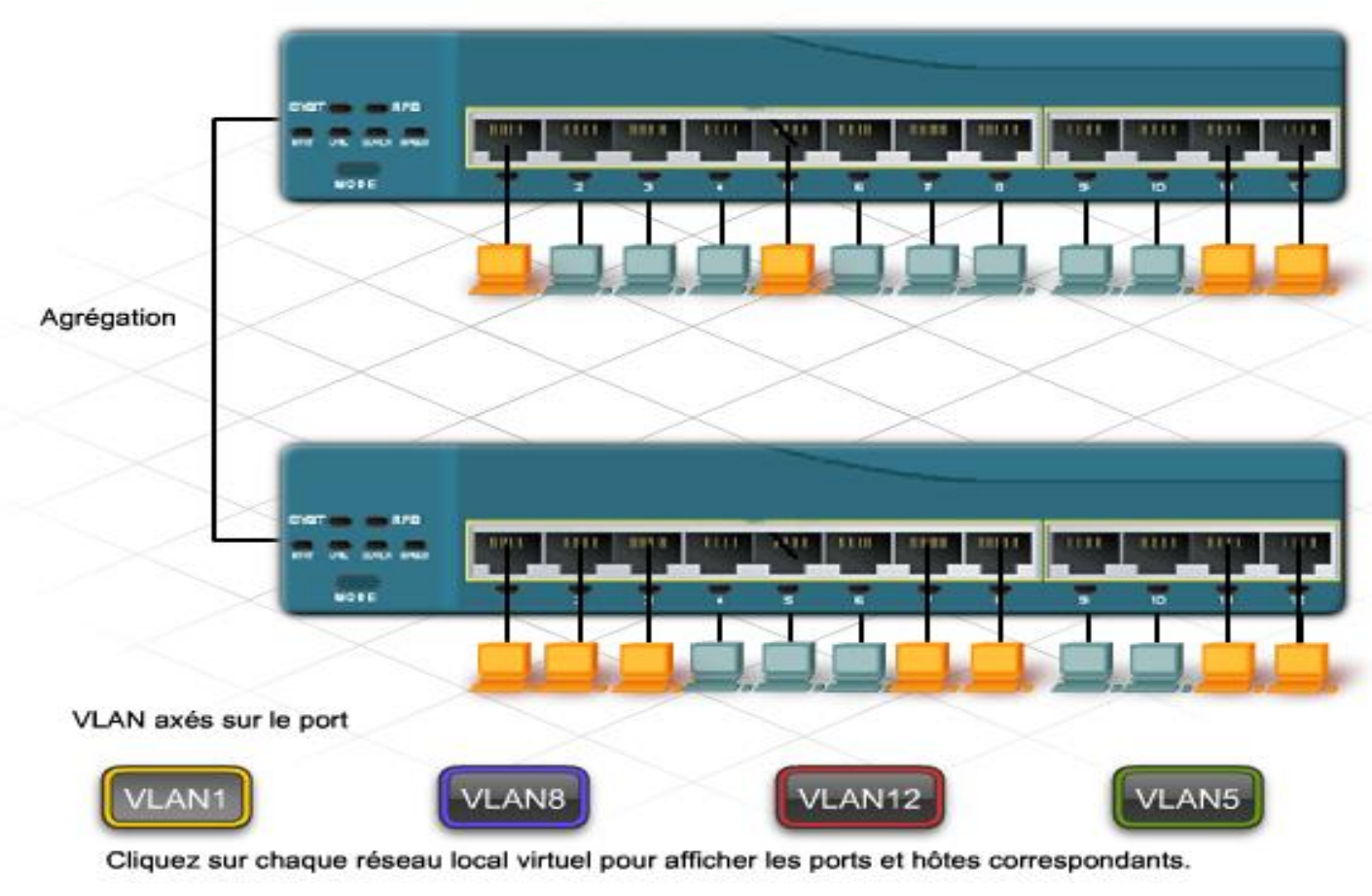
Les réseaux locaux virtuels exemple



Les réseaux locaux virtuels exemple



Les réseaux locaux virtuels



Les réseaux locaux virtuels avantages

Dans un réseau commuté, les réseaux locaux virtuels (vlan) sont créés pour contenir des diffusions et rassembler des hôtes au sein de communautés d'intérêt.

Un réseau local virtuel est un domaine de diffusion logique qui peut s'étendre sur plusieurs segments de réseau local physique.

Il permet à un administrateur de regrouper des stations par fonction logique ,par équipe de projet ou par application, quel que soit l'emplacement physique des utilisateurs.

Les réseaux locaux virtuels avantages

Les avantages principaux de la segmentation par vlan sont la **réduction des domaines de broadcast** et **l'accroissement de la sécurité** (si des **filtres** sont mis en place pour la communication entre les réseaux).

Types des réseaux locaux virtuels

Dans un réseau local virtuel, l'appartenance d'une machine à un réseau local virtuel est affectée de façon **statique** (vlan N1) ou **dynamique** (vlan N2).

L'appartenance statique nécessite qu'un administrateur affecte manuellement chaque port de commutateur à un vlan spécifique.

Ce type d'appartenance est le plus simple à configurer et le plus répandu, mais il est le plus exigeant en termes d'administration pour gérer les ajouts, les déplacements et les modifications.

Types des réseaux locaux virtuels

L'appartenance dynamique à un vlan nécessite un serveur de stratégies de gestion des réseaux locaux virtuels (VMPS). Le VMPS comprend une base de données qui associe des adresses MAC à des affectations de réseau local virtuel.

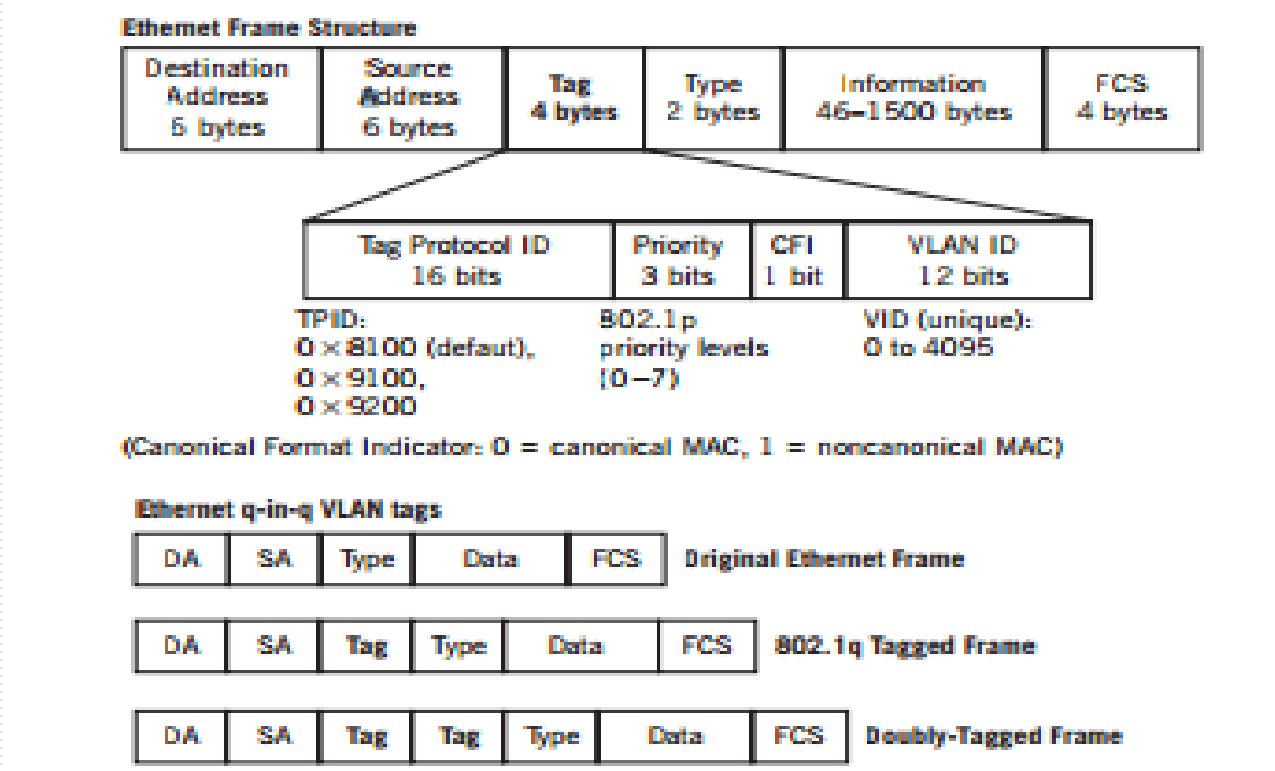
Dans un réseau local virtuel dynamique, les déplacements, ajouts et modifications sont automatisés, et ne requièrent aucune intervention de l'administrateur.

Les trames de VLAN

Lorsque plusieurs switchs doivent être reliés afin de créer les différents VLANs, il est nécessaire d'échanger entre ces switchs des trames appartenant à différents VLANs, il est nécessaire de savoir à quel VLAN appartient une trame.

- On doit «noter» à quel VLAN chaque trame appartient ;
- On utilise la norme IEEE 802.1Q, qui étend la trame 802.3 :
  - Elle utilise le «frame tagging», c-à-d de l'étiquetage de trame ;
  - Les étiquettes permettent de savoir à quel domaine de diffusion appartient la trame ;
  - Il est possible de mettre plusieurs tags dans une trame

Les VLANs et le trunking
La norme 802.1Q (dot1Q**)**



Les VLANs et le trunking
La norme 802.1Q

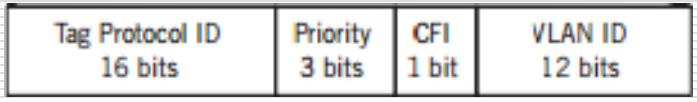
Elle ajoute :

- **4 octets** au format de la trame, entre l'@MAC source et le champs type contenu dans la trame ;
- La taille maximale de la trame passe de 1518 octets à 1522 octets.
- Un identifiant de VLAN qui peut aller de 0 à 4095.

Il est possible d'utiliser un **double étiquetage**, appelé «q in q» pour permettre à un FAI d'avoir ses propres VLANs en plus de ceux du client (dans le cas ou les sites du client sont dispersés et doivent communiquer entre eux par l'intermédiaire du FAI).

norme 802.1p intègre des **notions de priorités** pour favoriser le trafic d'un VLAN et faire de la QoS.

Les VLANs et le trunking
La norme 802.1Q



- le **TPID**, «Tag Protocol Identifier» : prend la place du type dans une trame 802.3 et identifie la trame comme étant une trame de VLAN (valeur 0x8100)

- **PCP**, «Priority Code Point» : champ sur 3 bits allant de la priorité 1 la plus faible à 7 la plus forte (la valeur 0 indique pas de priorité) Ces priorités peuvent être associées à des classes de trafic : voix, vidéo, données… ;

- **CFI**, «Canonical Format Indicator» : compatibilité avec les Token Ring : une trame dont le CFI est à 1, c-à-d non canonical, alors la trame ne doit pas être relayée vers un port non tagé, non associé à un VLAN ;

- **VID**, «VLAN Identifier» : identifie le VLAN, le numéro 1 est associé à un VLAN de gestion administrative, et la valeur 0 indique que la trame n'appartient à aucun VLAN.

Les réseaux locaux virtuels

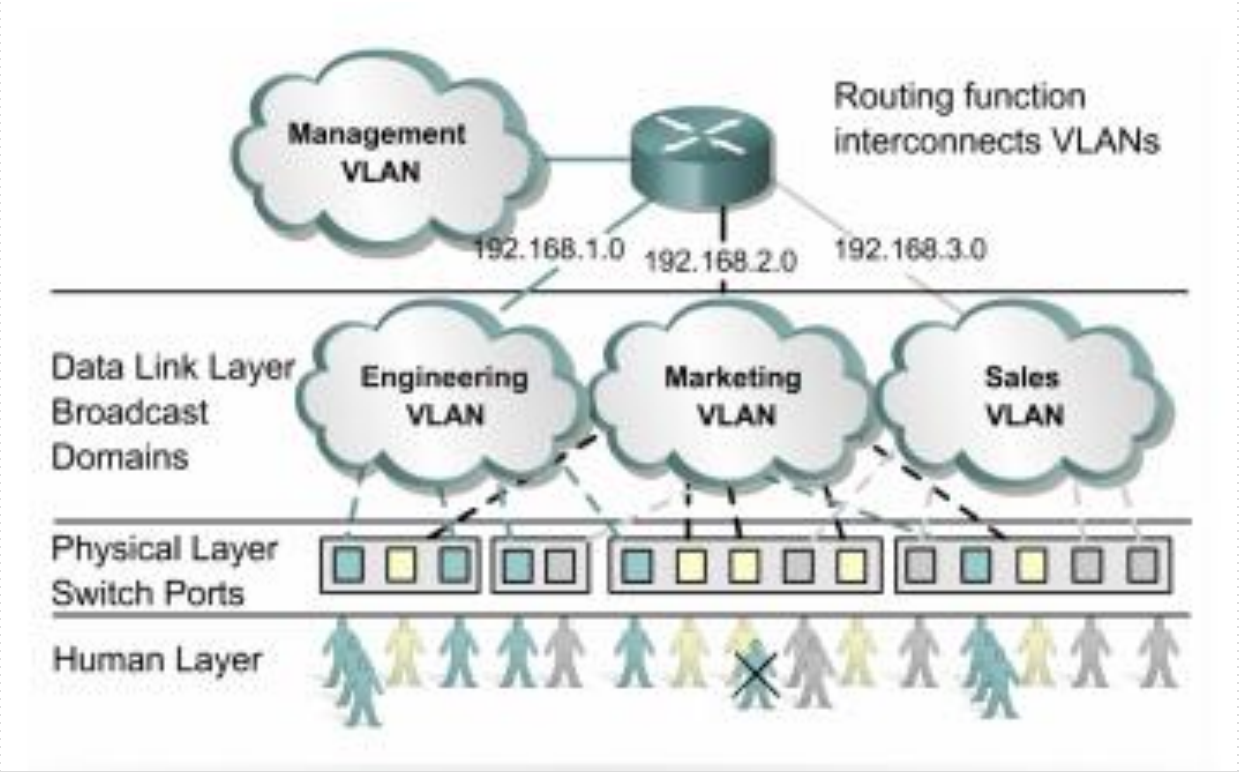
Une approche «traditionnelle» :

- Différents LAN utilisant des ponts, switch ou répéteurs ;
- Un routeur interconnectant ces différents LANs ;

Une approche «VLAN» :

- Un ou plusieurs switch en mode VLAN ;
- Un routeur interconnectant ces différents VLANs

Les réseaux locaux virtuels



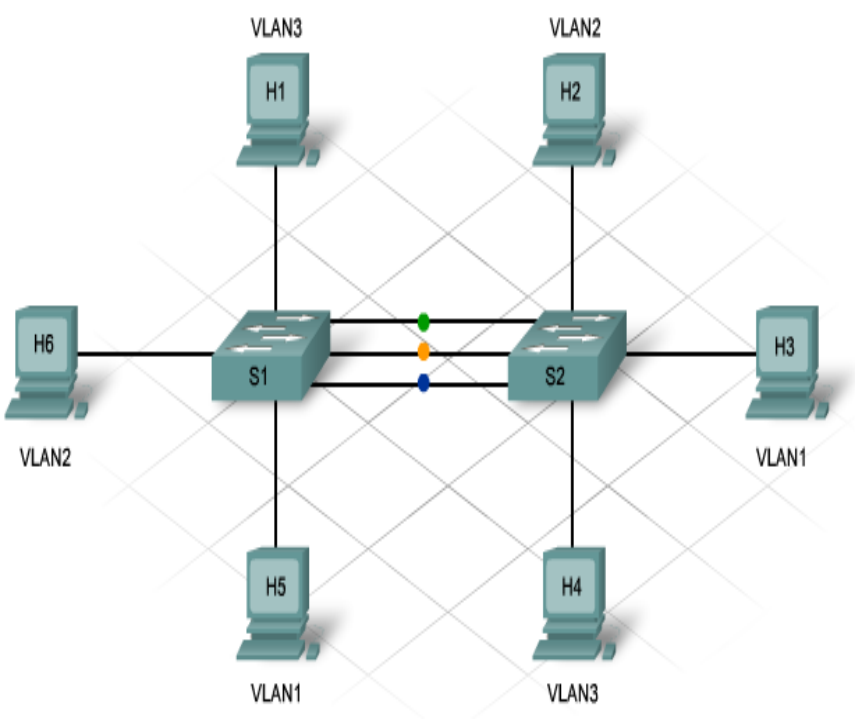
Agrégation et Routage entre les réseaux locaux virtuels

Les agrégations transportent le trafic provenant de plusieurs vlans via une liaison unique et permettent à chaque vlan d'atteindre l'intégralité d'un réseau.

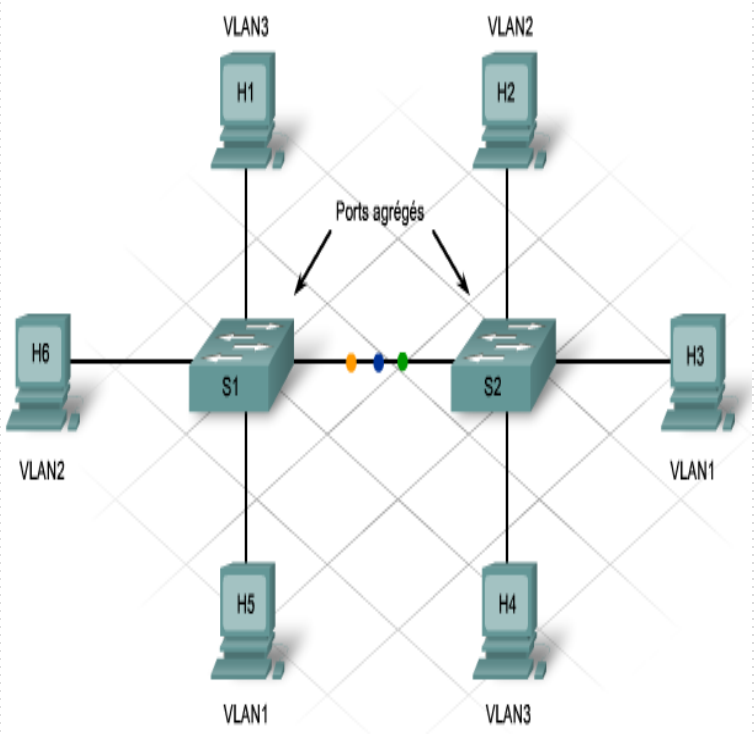
Les ports agrégés sont nécessaires à l'acheminement entre des périphériques de trafic provenant de plusieurs vlans, lors de la connexion de deux commutateurs, d'un commutateur et d'un routeur, ou d'une carte réseau hôte prenant en charge l'agrégation 802.1Q.

Port agrège et port non agrège

1_port non agrège



2_port agrège



Configuration d’un réseau local virtuel

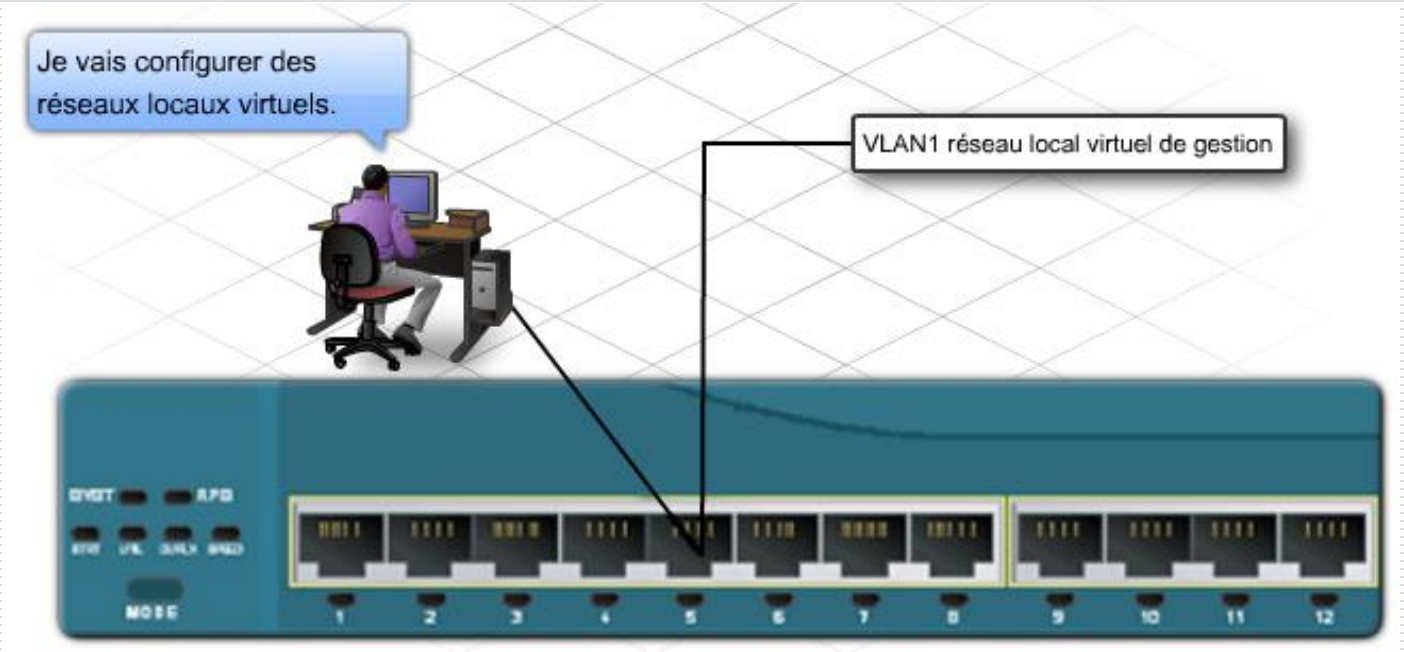
Configuration d'un réseau local virtuel

Qu'ils soient crées de façon statique ou dynamique, le nombre maximal de réseaux locaux virtuels dépend du type de commutateur et du logiciel **Ios** (CISCO) utilisés.

Par défaut, Vlan1 est appelé réseau local virtuel de gestion.

Configuration d'un réseau local virtuel

- Le vlan de gestion



Configuration d’un réseau local virtuel

Le port est configuré en mode ***access*** ou en mode ***trunk***.

Le mode *access* est utilisé pour la connexion terminale d'un périphérique (pc, imprimante, serveur, ...) appartenant à un seul vlan.

Le mode *trunk* est utilisé dans le cas ou plusieurs vlans doivent circuler sur un même lien.

C'est par exemple le cas de la liaison entre deux switchs ou bien le cas d'un serveur ayant une interface appartenant à plusieurs vlans.

Configuration d’un réseau local virtuel

Dans le cas de l'utilisation d'un ordinateur connecté à un téléphone IP (ce dernier étant connecté à un port du switch), le port aura deux vlans (un vlan dédié au réseau donnée et un vlan dédié au réseau voix).

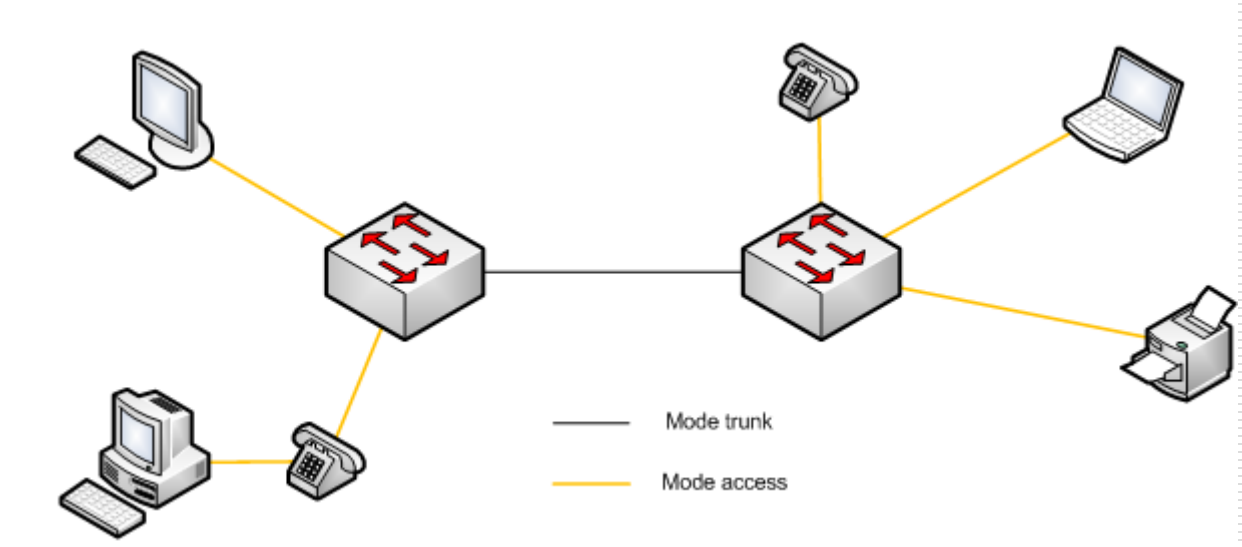
Le port sera configuré en général en mode *access*, une commande sera ajoutée pour la configuration du vlan voix (*voice vlan*).

La communication entre les vlans est possible en passant par un routeur ou un switch de niveau 3 (switch-routeur).

Selon l'utilisation, il peut être conseillé de filtrer les réseaux au minimum au moyen d'ACLs (access control list).

Configuration d'un Vlan EN résumé

- La liaison entre les switchs est en mode *trunk*.
- Les autres ports des switchs sont en mode *access*.
- Le vlan dédié aux téléphones sera également configuré sur tous les ports en plus de leur vlan data respectif.
  Un vlan dédié à l'administration et à la supervision du switch sera créé.
  L'adresse IP de supervision du switch sera associée à ce vlan.



Configuration d'un Vlan
Ajout et suppression

Création du vlan 2 puis des vlans 3 à 5

2960-RG(config)#**vlan 2**
2960-RG(config-vlan)#**name administration**
2960-RG(config-vlan)#**ex**
2960-RG(config)#**vlan 3,4,5**
2960-RG(config-vlan)#**ex**
2960-RG(config)#

Configuration d'un Vlan

Affichage des vlans ainsi que des affectations de port

```
2960-RG#show vlan

VLAN Name Status Ports
---- -------------------------------- --------- -------------
------------------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Gi0/1
2 administration active
3 VLAN0003 active
4 VLAN0004 active Fa0/5, Fa0/6, Fa0/7, Fa0/8
5 VLAN0005 active
10 VLAN0010 active Fa0/1
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
```

Configuration d’un Vlan

Affectation d'un port à un vlan

Dans l'exemple ci-dessous le port est configuré en mode access puis il est placé dans le vlan 3.

Pour un switch série 2950, 2960, 3750

```
2960-RG(config)#interface fastEthernet 0/1
2960-RG(config-if)#switchport mode access
2960-RG(config-if)#switchport access vlan 3
2960-RG(config-if)#ex
2960-RG(config)#
```

L'exemple suivant présente la configuration des ports 5 à 8 en mode access, puis configurés avec le vlan 4

```
2960-RG(config)#interface range fastEthernet 0/5-8
2960-RG(config-if-range)#switchport mode access
2960-RG(config-if-range)#switchport access vlan 4
2960-RG(config-if-range)#end
2960-RG#
```

Configuration d’un Vlan

Affectation d'un port à un vlan

Pour un switch série 6500

```
6500(config)#interface gi 0/2
6500(config-if-range)#switchport
6500(config-if-range)#switchport mode access
6500(config-if-range)#switchport access vlan 4
6500(config-if-range)#end
6500#
```

Configuration d'un port en mode trunk

Pour un switch série 2960

```
2960-RG(config)#interface gigabitEthernet 1/0/1
2960-RG(config-if)#switchport mode trunk
2960-RG(config-if)#
```

Pour un switch série 2950 et 3750

```
3750(config)#interface gigabitEthernet 1/0/1
3750(config)#switchport trunk encapsulation dot1q
3750(config-if)#switchport mode trunk
3750(config-if)#
```

Pour un switch série 2960

```
2960-RG(config)#interface gigabitEthernet 1/0/1
2960-RG(config-if)#switchport mode trunk
2960-RG(config-if)#
```

Filtrage des vlans sur un port uplink

Pour les swiths série 2950, 2960, 3750, 6500 (dans l'exemple, on autorise les vlans 2,3 et 10 a être transportés sur le lien).

```
2960-RG(config)#interface gigabitEthernet 1/0/1
2960-RG(config-if)#switchport trunk allowed vlan add 2,3,10
2960-RG(config-if)#
```

Pour interdire un vlan de passer par le lien trunk (dans l'exemple, le vlan3):

```
2960-RG(config-if)#switchport trunk allowed vlan remove 3
2960-RG(config-if)#
```

Pour supprimer la commande de filtrage:

```
2960-RG(config-if)#no switchport trunk allowed vlan
2960-RG(config-if)#
```

Configuration d'un vlan dédié à la téléphonie

Le protocole cdp doit préalablement être activé.

```
2960-RG(config)#vlan 10
2960-RG(config-vlan)#name voip
2960-RG(config-vlan)#ex
2960-RG(config)#int fastEthernet 0/1
2960-RG(config)#switchport voice vlan 10
```

Suppression de la configuration d'un port

Comme d'habitude, il suffit de mettre la commande no devant les commandes entrées précédemment.

Par exemple:

```
2960-RG(config)#int fastEthernet 0/1
2960-RG(config-if)#no switchport access vlan
2960-RG(config-if)#no switchport mode acc
2960-RG(config-if)#end
```

Le rôle des commandes show

Pour vérifier, gérer ou dépanner des réseaux locaux virtuels, il est important de connaître les principales commandes show disponibles dans le logiciel IOS Cisco.

Les commandes suivantes permettent de vérifier et de gérer des réseaux locaux virtuels :

Le rôle des commandes show

1_Show vlan Affiche une liste détaillée de tous les numéros et noms des réseaux locaux virtuels actifs sur le commutateur, ainsi que les ports associés à chacun d'eux.

2_ show vlan brief Affiche une liste résumée indiquant uniquement les réseaux locaux virtuels actifs et les ports associés à chacun d'eux.

3_ show vlan numéro _ id Affiche des informations relatives à un réseau local virtuel spécifique, en fonction du numéro d'ID.

4_ show vlan Name nom _ vlan Affiche des informations relatives à un réseau local virtuel spécifique, en fonction du nom.

Suite Cours 2 sur les vlan
Le Protocol vtp (vlan turking Protocol)

Le protocole VTP (VLAN Trunking Protocol)

Présentation du Protocol (VTP)

VTP est un protocole de messagerie client/serveur qui ajoute, supprime et renomme des vlans dans un domaine VTP unique.

Tous les commutateurs soumis à la même gestion font partie d'un domaine (échangeront leurs informations sur les VLAN).

Chaque domaine possède un nom unique. Les commutateurs VTP partagent uniquement des messages VTP avec d'autres commutateurs du même domaine.

Pourquoi le Protocole VTP?

Si un réseau d'entreprise comportant des centaines de Vlans n'est pas géré automatiquement, chaque réseau local virtuel doit être configuré manuellement sur chaque commutateur.

Toute modification apportée à la structure de réseau local virtuel requiert une configuration manuelle supplémentaire.

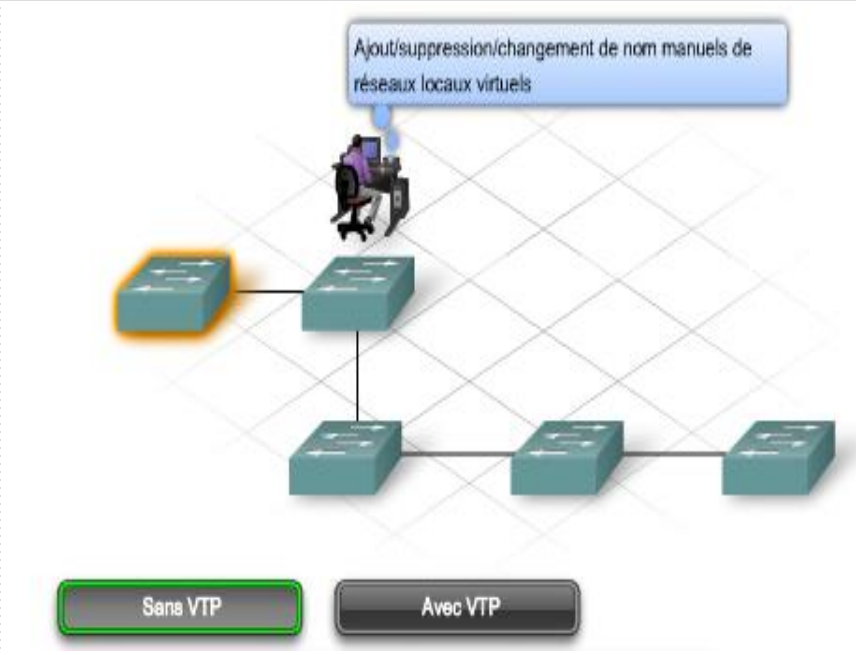
Si un nombre n'est pas tapé correctement, des incohérences de connectivité peuvent se produire sur l'ensemble du réseau.

Pourquoi le Protocole VTP?

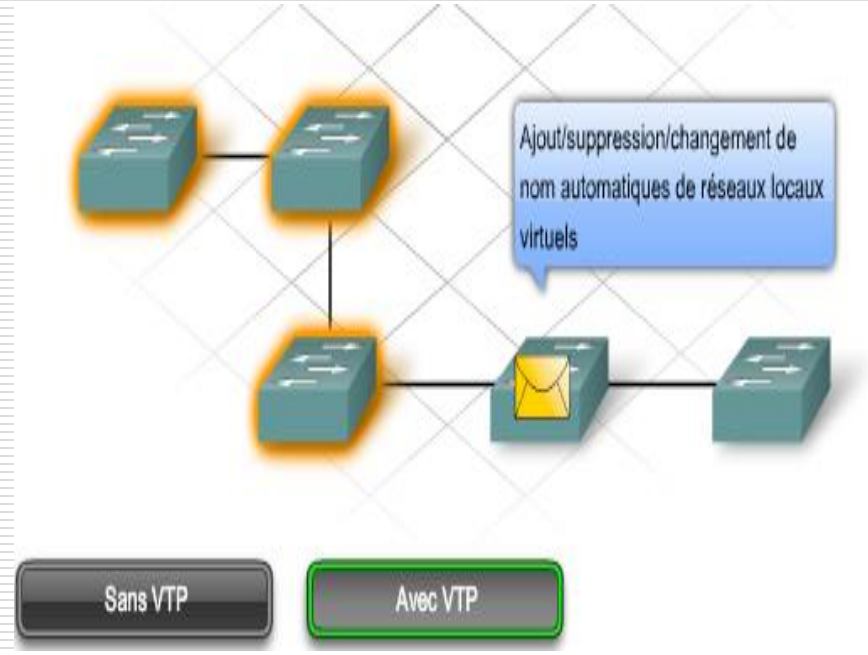
Pour résoudre ce problème, Cisco a créé le protocole VTP qui permet d'automatiser de nombreuses fonctions de configuration des réseaux locaux virtuels.

Ce protocole garantit que la configuration est gérée de manière cohérente sur tout le réseau, et il réduit la tâche de gestion et de surveillance des réseaux locaux virtuels.

Pourquoi le Protocole VTP?



Sans VTP



Avec VTP

Pourquoi le Protocole VTP?

- la manipulation peut être faite sur un seul switch
- La modification sera diffusée sur les autres via le protocole VTP : VLAN Trunking Protocol
- Nous distinguons dans ce cas, des switchs VTP server et des VTP client
- La VTP server va diffuser la modification vers les autres switchs VTP client

le Protocole VTP et les modes?

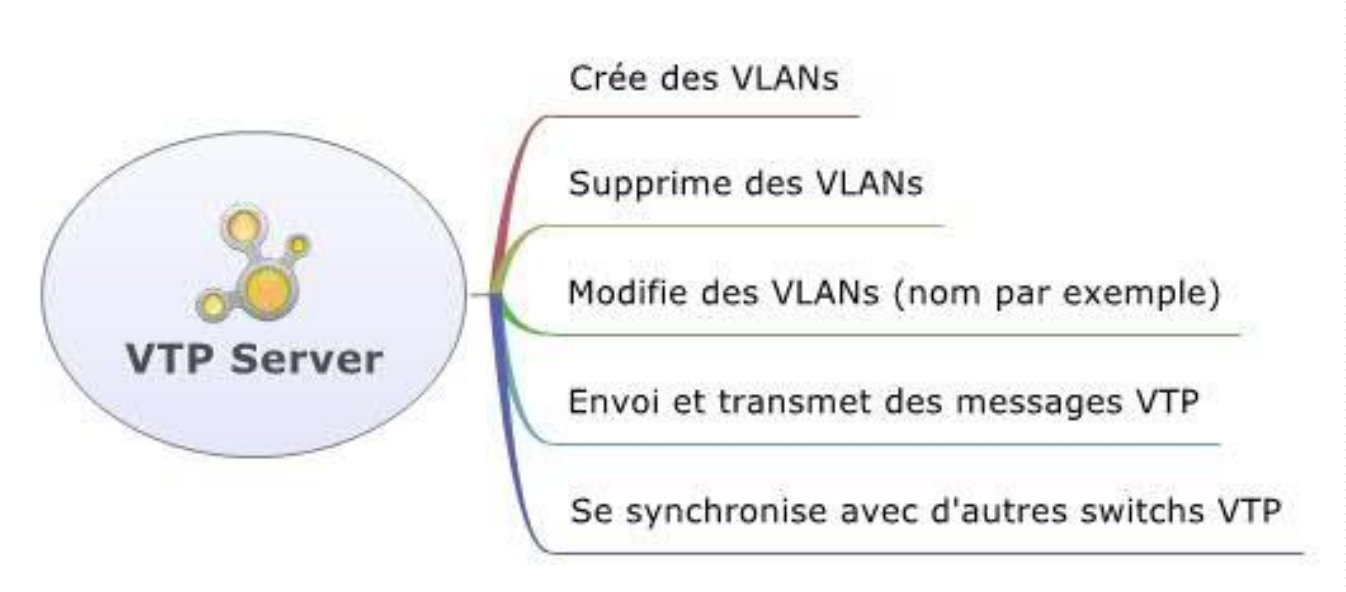
- **Mode server**
  - il diffuse ses informations sur les VLAN à tous les autres switchs appartement au même VTP domain
  - ces informations sont stockées en NVRAM et sur un tel switch, il est possible de créer, modifier ou détruire un VLAN du VTP domain
- **Mode client**
  - Il stocke uniquement les informations sur les VLAN, transmises par le switch en mode VTP server sur le même domaine
- **Mode transparent**
  - Il transmet les informations VTP aux autres switchs mais ne les traitent pas. Ces switchs sont autonomes et ne participent pas aux VTP

le Protocole VTP et les modes?

- **Le VTP Pruning**
  - Supprime la propagation des messages de broadcast, multicast et autres messages inconnu unicast sur les liens trunks afin d'optimiser la bande passante

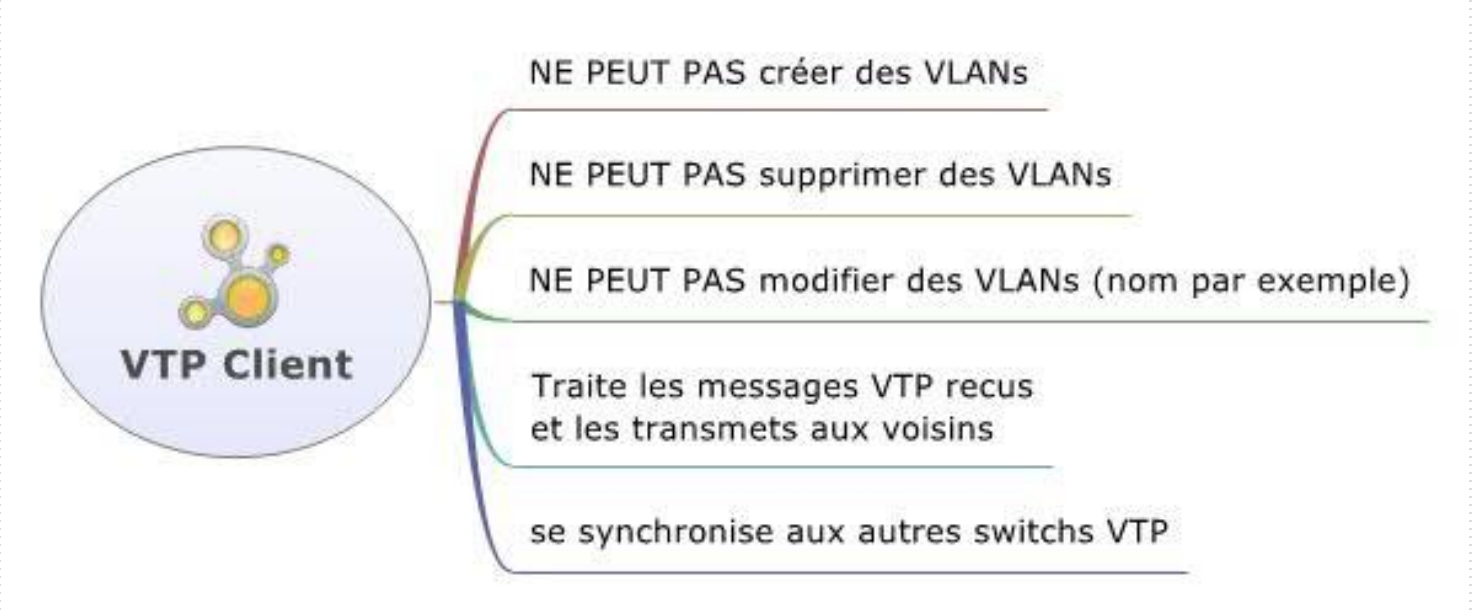
Switch en mode VTP Server

- Le switch en mode Server permet à l'administrateur de faire toute modification sur les VLANs et de propager automatiquement ses modifications vers tous les switchs du réseau.



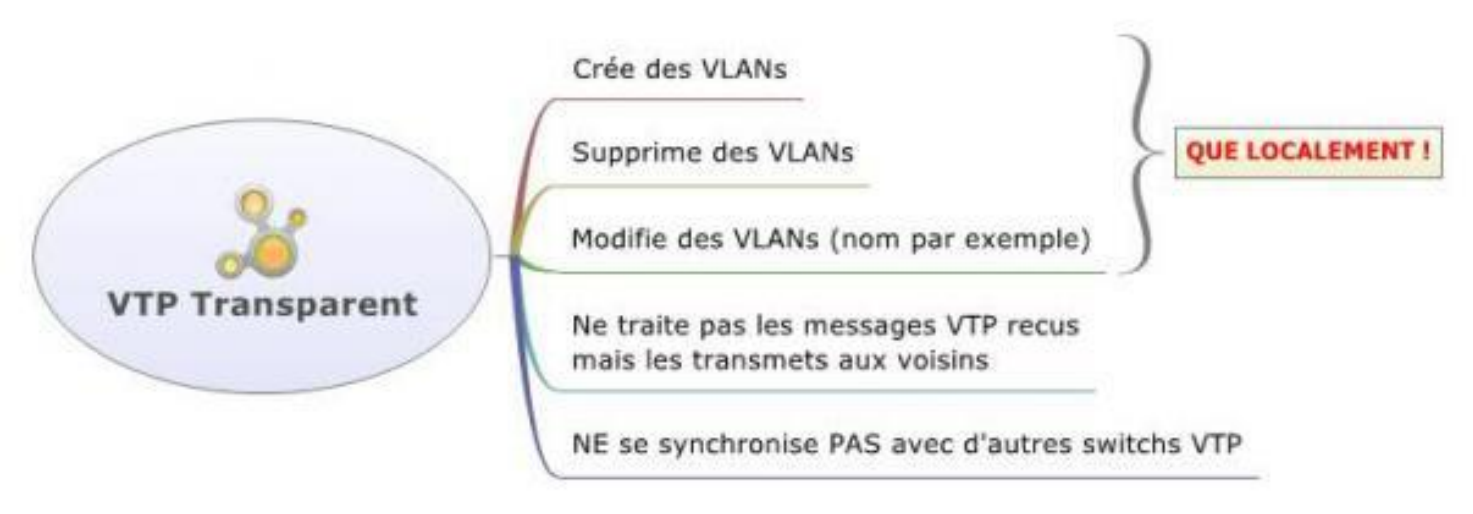
Switch en mode VTP Client

- Le switch en mode Client ne permet pas à l'administrateur de faire des modifications sur les VLANs. Vous recevez un message d'erreur quand vous essayez de créer un VLAN.



Switch en mode VTP Transparent

- Le switch en mode Transparent permet à l'administrateur de faire toute modification sur les VLANs en **local uniquement** et donc ne propage pas ses modifications vers tous les switchs du réseau.

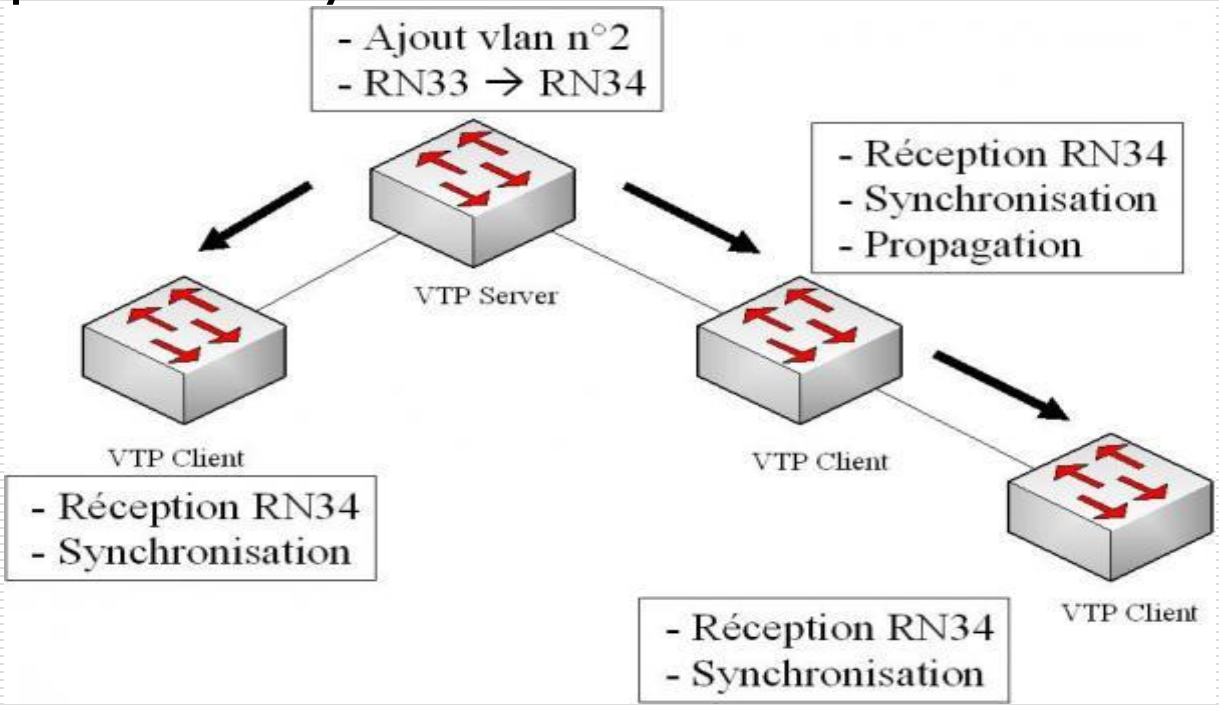


Synchronisation

- A chaque création/suppression/modification de VLAN, une variable appelée RN – Revision Number – s'incrémente.
- A chaque création/suppression/modification de VLAN, le switch Server envoi un message VTP avec la nouvelle valeur du RN.
- Les autres switchs compare le RN reçu du switch Server avec le RN qu'ils stocke en local, si ce dernier est plus petit (logiquement) alors les switchs se synchronisent avec le Server et récupère la nouvelle base de données des VLANs.

Synchronisation

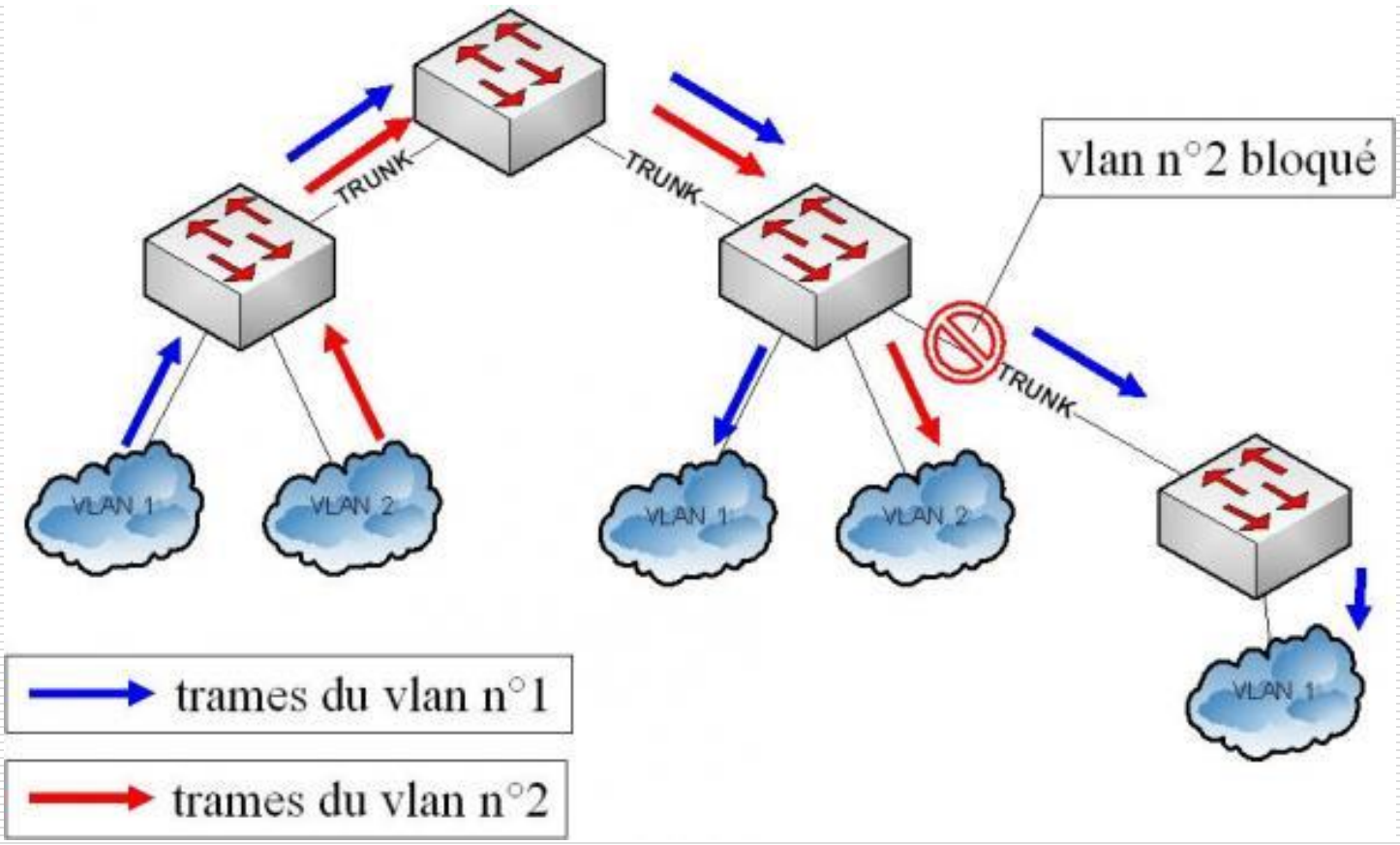
- Par défaut, le RN est envoyé automatiquement dès une création/suppression/modification de VLAN puis envoyé toutes les 5 minutes.



VTP Pruning

- Cette commande optionnelle permet de faire des économies de bande passante.
- Explication: imaginons qu'un switch reçoit les VLANs 1 et 2 mais qu'aucunes de ses interfaces appartiennent au VLAN 2. Lorsque le switch voisin lui enverra des trames du VLAN 2, ce switch les supprimera car aucune de ses interfaces appartiennent à ce VLAN. Il est donc inutile que le switch voisin lui envoi du trafic pour le VLAN 2.
- On active alors la fonction VTP pruning pour avertir le switch voisin de ne pas lui envoyer de trafic pour ce VLAN. La fonction s'active à partir du switch Server.

VTP Pruning


TRUNK
TRUNK
vlan n°2 bloqué
TRUNK
VLAN 1
VLAN 2
VLAN 1
VLAN 2
VLAN 1
trames du vlan n°1
trames du vlan n°2

Remarques importantes

- Les messages VTP se propagent sur les liens configurés en Trunk (norme 802.1Q) et pas en Access
- VTP ne gère que la plage de VLAN comprise entre 1 et 1005. La plage étendue 1006 à 4096 n'est pas supportée. Pour cela, il faut basculer en mode Transparent sur tous les switchs et créer ses VLANS étendus à la mano
- Il existe 3 versions de VTP, bien vérifier qu'une et une seule version est active sur son réseau pour éviter les surprises (v1 et v2 incompatibles entre elles)

Remarques importantes

- La configuration VTP n’est pas visualisable dans la running-config mais est stockée dans le fichier vlan.dat situé dans la flash (faites un show flash: pour voir le fichier)

Configuration du protocole VTP ?

Switch(config) # vtp domain domain_name
Switch(config) # vtp mode { serveur | client | transparent}
Switch(config) # vtp password password
Switch(config) # end
Switch#copy running-config startup-config

La configuration par défaut d'un switch

- mode server
- le VTP domain name est égal à null
- Tous les ports sont dans le VLAN 1
- Le numéro de révision de la configuration VTP est 1
- La version du protocole VTP est 1
  - Il existe 3 versions. Pour un VTP domain, tous les switchs doivent être dans la même version
- La commande show vtp status permet de visualiser la configuration d'un switch

La configuration étapes

1. **obligatoire**: configurer un domaine VTP qui permet à tous les switchs d'être dans le même "groupe d'amis"
2. **obligatoire**: configurer le mode de votre switch (client, transparent ou server)
3. **optionnel**: activer la fonction pruning

4. **optionnel**: configurer un mot de passe pour sécuriser les messages VTP
5. **optionnel**: activer la version 2 ou 3 de VTP (version 1 active par défaut)

La configuration étapes

1, configuration domaine VTP qu'on appelle TEST:

Switch>enable
Switch#configure terminal
Switch(config)#vtp domain TEST
Changing VTP domain name from NULL to TEST

2. configuration du mode Server:

Switch(config)#vtp mode server

Device mode already VTP SERVER.

3. activation de la fonction pruning (à partir du switch Server):

Switch(config)#vtp pruning

Pruning switched on

La configuration étapes

4. configuration d'un mot de passe VTP cisco123):

Switch(config)#vtp password cisco123

Setting device VLAN database password to cisco123

5. activation de la version 2 de VTP (à faire sur tous les switchs!):

Switch(config)#vtp version 2

Vérifications

- visualiser si le mot de passe a bien été tapé

Switch#show vtp password

- vérifier si on envoi et on reçoit bien des messages VTP avec les switchs voisins

Switch#show vtp counters

- vérifier la configuration globale du VTP (commande la plus utilisée)

Switch#show vtp status

Vérifications

Switch#show vtp status

```
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : TEST
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xCD 0x24 0x5F 0xE3 0xF2 0x01 0xFF 0x6B
Configuration last modified by 0.0.0.0 at 3-1-11 00:15:36
```

Exercice

- activer le mode Server sur switch_A et le mode client sur switch_B
- activer la version 2 sur switch_A et switch_B
- définir le domaine VTP = TEST
- créer les VLAN 3 et 4 sur switch_A
- vérifier que tout est bon

VMPS

- Le Vmps est un service, crée par Cisco, chargé de faire correspondre un Vlan à une (ou plusieurs) adresse Mac et s'impose donc comme la solution.
- La gestion dynamique des Vlans passe tout d'abord par la compréhension d'une architecture réseau basé sur les Vlans de **niveau 2**, du protocole **VTP** (Vlan Trunking Protocol), puis par l'étude du protocole **VQP** (Vlan Query Protocol).
- L'utilisation du protocole VTP est obligatoire sur le réseau sur lequel on veut déployer une solution VMPS utilisera le nom de domaine VTP lors de l'échange de paquets entre le serveur VMPS et les commutateurs clients.

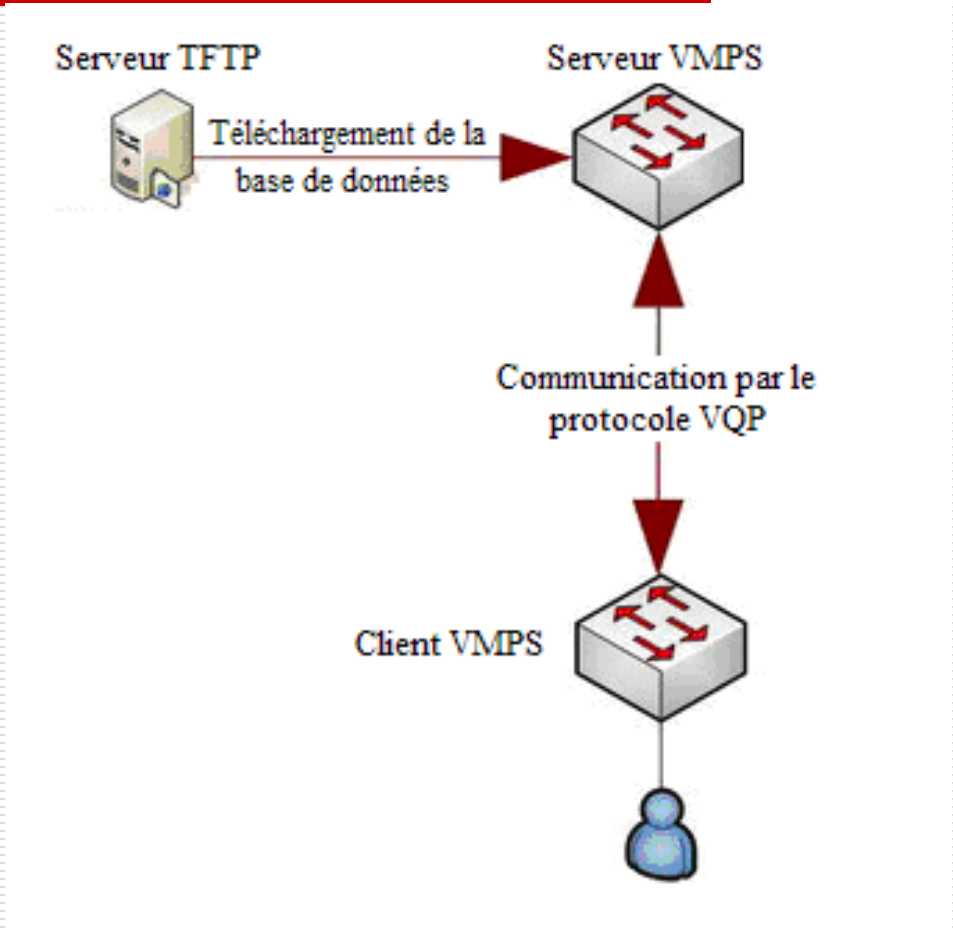
Le protocole VQP

- Un protocole qui permet au switch client d'interroger un serveur VMPS avec des informations sur les stations enregistrées et leur Vlan associé.
- Ainsi le switch client pourra associer le port avec le bon VLAN.
- Le serveur VMPS est le plus souvent un switch ou un routeur Cisco, mais il existe également des serveurs " libres " (dont le code source est consultable et modifiable) destiné aux machines Unix (Linux et Solaris).
- Le Vmps est donc basé sur une architecture client/serveur et permet de gérer dynamiquement les assignations de Vlan en fonction d'adresses MAC (Media Access Control).

Le protocole VQP

- Lorsqu'une machine se connecte à un port, le switch récupère son adresse MAC et se connecte au serveur VMPS afin de vérifier le droit d'accès de cette machine.
- Lorsque celle-ci est autorisée, le serveur envoie au client le Vlan dans lequel cette machine doit se connecter.
- Le switch place donc le port dans le bon Vlan et la machine a donc accès au réseau.

Le protocole VQP



Le serveur VMPS

- Le serveur VMPS peut être accompagné de serveur secondaire pour prendre le relai en cas de panne ou pour simplement équilibrer la charge (load-balancing).
- Le serveur utilise une base de données contenant les adresses MAC des clients, le Vlan correspondant et d'autres règles permettant de donner le droit à un utilisateur de se connecter.
- Normalement cette base de données est téléchargée par le serveur VMPS à partir d'un serveur TFTP (Trivial File Transfert Protocol), qui peut être situé n'importe où sur le réseau.
- Cette base de données est chargée dans le serveur à chaque démarrage/redémarrage de celui-ci.

Le serveur VMPS

- A partir de ce moment le serveur est prêt à répondre aux requêtes des clients.
- A chaque démarrage ou redémarrage du serveur, cette base de données est à nouveau téléchargée.
- Le VMPS ouvre un socket, le protocole UDP est utilisé.
- Lorsque le serveur reçoit une requête valide d'un client, il recherche dans sa base de données, l'adresse MAC correspondante et le numéro de Vlan associé.
- Si le Vlan choisi est autorisé sur le port, le nom du Vlan est envoyé au client (le switch).
- Si le Vlan n'est pas autorité sur le port, il y a 2 solutions:
  - le serveur VMPS est en mode open, il renvoie un message avertissant que l'accès au réseau est refusé,
  - le VMPS est en mode secure, le port du switch est alors refermé.

Le serveur VMPS
Les options disponibles

- Il est possible de configurer un Vlan par défaut, appelé Vlan Fallback. Ainsi lorsqu'une requête contenant une adresse MAC ne se trouvant pas dans la base de données arrive au serveur, ce dernier renvoie le nom de ce Vlan par défaut et le switch ouvre l'accès au réseau. Si la configuration d'un Vlan par défaut n'a pas été faite et que l'adresse MAC n'est pas trouvée, le serveur envoie un message annonçant que l'accès est refusé ou referme le port si le serveur est en mode secure.
- Dans la configuration du serveur, une option permet de filtrer les adresses MAC auxquelles on ne souhaite pas donner l'accès en ne spécifiant aucun Vlan. Dans ce cas, selon le mode de configuration du serveur, le port est fermé (mode secure) ou un message de refus de connexion est envoyé.

Configuration du serveur openVMPS

- Le serveur openVMPS respecte le protocole décrit précédemment de façon à rester compatible avec les commutateurs Cisco.
- La différence principale se situe au niveau de la base de données. Elle n'est pas stockée sur un serveur TFTP mais directement sur le serveur.
- On peut la trouver dans le fichier de configuration, avec les options générales du serveur.
- La syntaxe est la même que pour les commutateurs serveur VMPS.
- Par défaut, le fichier utilisé est vmpsd.conf, il se trouve dans le répertoire /etc. Cependant il est possible d'utiliser un autre fichier lors du lancement du serveur en utilisant l'option " -c ".

Configuration du serveur openVMPS

```
!Choix du mode secure ou open
vmps mode open

!Nom du domaine VTP
vmps domain DOMAIN_NAME

!Action par défaut lorsqu'une requête sans nom de domaine arrive au serveur,
!ici on refuse le traitement
vmps no-domain-req deny

!Vlan par défaut si l'adresse MAC n'est pas trouvée
vmps fallback VMPSRogue


!
! --- Mac Address Section ---           Bloc équivalent à la base de données
!

vmps-mac-addrs                          !Début de liste des adresses MAC


!
! --- VLAN Admin ---                    !Nom du Vlan concerné
!

!Cette ligne contient le mot clé address suivi de l'adresse MAC de la machine concernée,
!puis le mot clé vlan-name suivi du nom du Vlan dans laquelle cette machine doit être placée.
!En fin de ligne on trouve un commentaire avec le nom de la machine.
address 0000.0000.0001 vlan-name Admin ! machine1
                                                                    !


!
! --- VLAN Compta ---
!
address  0000.0000.0002 vlan-name Compta ! machine2

...

!
! --- VLAN Serveur ---
!
address 0000.0000.0003 vlan-name Serveur ! machine3
```

Configuration des commutateurs clients

- La configuration des commutateurs clients se fait en 2 étapes: la configuration générale du Vmps et celle des ports concernés.
- **Configuration générale**

adresse IP du serveur VMPS principal

switch(conf)# vmps server 192.168.0.1 primary

adresse IP du serveur VMPS secondaire

switch(conf)# vmps server 192.168.0.2

choisir le temps entre deux requêtes au serveur :

switch(conf)# vmps reconfirm 120

spécifier le nombre de requêtes à effectuer sur le serveur principal avant de passer au serveur secondaire

switch(conf)# vmps retry 3

Configuration des commutateurs clients

- **Configuration générale**

il est possible de vérifier les paramètres VMPS précédemment

```
switch# show vmps
```

- **Configuration des ports des commutateurs**

la commande est la même que pour assigner un Vlan à un port

il suffit d'écrire le mot dynamic à la place du numéro du Vlan

```
switch(conf)# interface GigabitEthernet 0/1
switch(conf-if)# switchport access vlan dynamic
```

observer la configuration de l'interface

```
switch# sh ru int gi 0/1
```

Le protocole DTP (Dynamic Trunking Protocol)

- Le protocole DTP (Dynamic Trunking Protocol) permet à deux commutateurs qui sont connectés ensemble de monter un lien trunk automatiquement sous certaines conditions,

- Par exemple la connexion d'un port configuré par défaut en **dynamic auto** vers un port **trunk**.

Le protocole DTP (Dynamic Trunking Protocol)

- Le principe est très simple, lorsqu'un port monte, des annonces DTP sont envoyées;
  - si le port est connecté à un switch voisin, ce dernier va recevoir l'annonce DTP et y répondre. Des deux côtés, l'activation du Trunk s'effectue;
  - si le port est connecté à un pc, ce dernier ne répondra pas à l'annonce car il comprend pas le protocole. Sur le port du switch, le Trunk n'est pas activé et donc reste en mode Access.

Le protocole DTP (Modes des ports physiques)

SW1(config-if)#switchport mode <mode de fonctionnement>

- **access**: typiquement le mode d'un port prévu pour recevoir la connexion d'un PC, d'un serveur, …désactivation du trunk et informer le voisin
- **trunk**: force le mode de fonctionnement en trunk (le sw se met automatiquement en trunk et informe son voisin)
- **dynamic auto**: autorise la négociation (attend une sollicitation du voisin, il n'envoie pas de requête mais il répond aux requêtes DTP)
- **dynamic desirable**: autorise la négociation avec une préférence pour le passage en trunk si possible.
- **Nonegociate** le sw se met en trunk sans informer le voisin
- **Off** désativation du trunk,

Le protocole DTP (Dynamic Trunking Protocol)

SW1	SW2	Résultat
access	n'importe quel mode	non-trunk
trunk	trunk	trunk
trunk	dynamic desirable	trunk
trunk	dynamic auto	trunk
dynamic auto	dynamic auto	non-trunk
dynamic auto	dynamic desirable	trunk
dynamic desirable	dynamic desirable	trunk

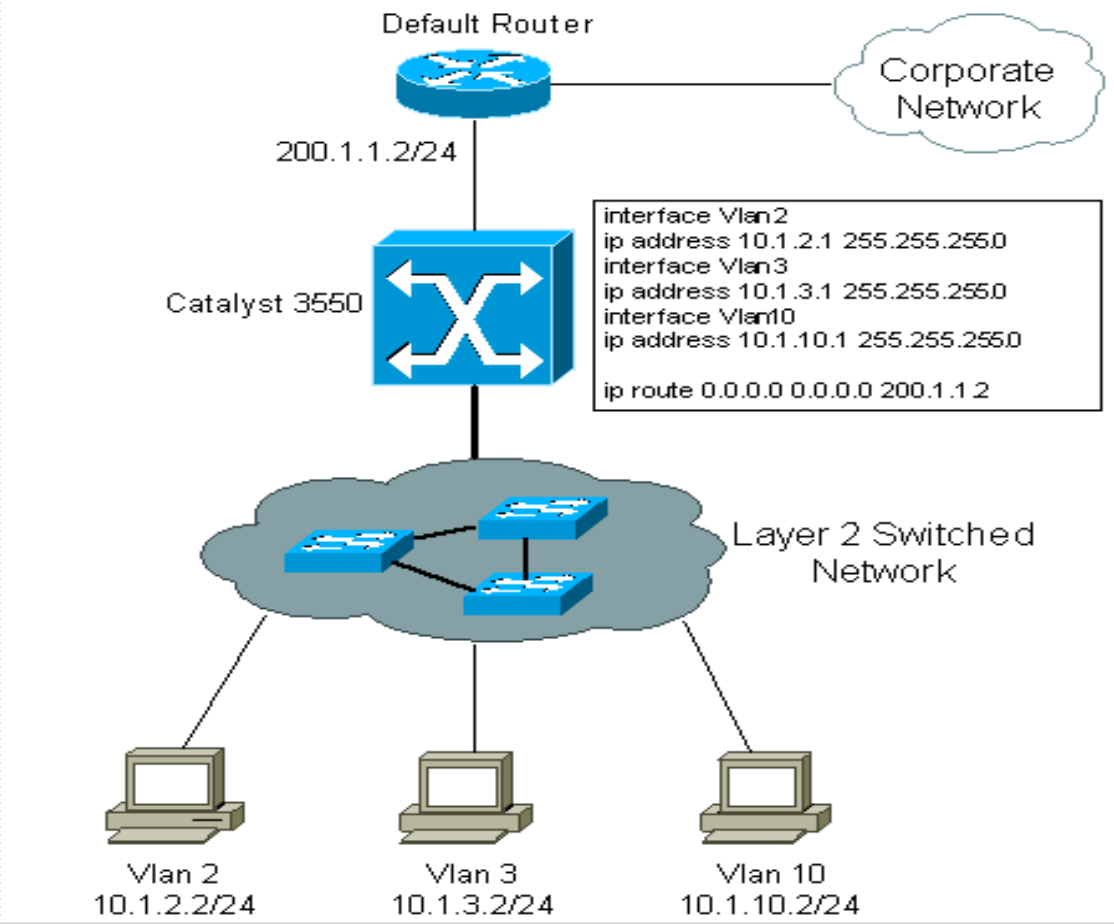
Le protocole DTP (Important)

- Comme dans tout protocole, le bug ou le plantage existe, ce qui a pour conséquence qu'un lien entre 2 switchs peut ne pas monter en Trunk et donc basculer en mode Access.
- La conséquence est que les trames utilisateurs taguées avec leur VLAN ne peuvent plus passer par ce lien. Grosso modo, on coupe la communication réseau.
- Il est donc fortement conseillé de désactiver le DTP et de forcer le lien Trunk entre 2 switchs.
- Mon conseil reste le forcage en statique d'une configuration Trunk entre 2 switchs dont voici la configuration:
- **Switch_1(config)# interface fastethernet 0/1**
- **Switch_1(config-if)# shutdown**
- **Switch_1(config-if)# switchport mode trunk**
- **Switch_1(config-if)# switchport nonegociate**
- **Switch_1(config-if)# no shutdown**

Le protocole DTP (Important)

- Idem sur le switch 2. Avec ces commandes, vous forcez le trunk (mode trunk) de par et d'autre et vous désactivez l'envoi d'invitation au voisin (**nonegociate**), donc vous désactivez le DTP. Au moins, vous maitrisez votre réseau et son comportement!

Routage intervlan (VLAN niveau 3)



VLAN niveau 3

- les Vlans de niveau 3 permettent de regrouper plusieurs machines suivant le sous réseau auquel elles appartiennent.
- La mise en place de Vlan de niveau 3 est conditionné par l'utilisation d'un protocole routable (IP, autres protocoles propriétaires ...).
- L'attribution des Vlans se fait de manière automatique en décapsulant le paquet jusqu'a l'adresse source. Cette adresse va déterminer à quel Vlan appartient la machine.

Les avantages

1. permet une affectation automatique à un Vlan suivant une adresse IP
2. Il est aussi possible de séparer les protocoles par Vlan

Les inconvénients

1. lenteur par rapport aux Vlans de niveau 1 et 2 le switch est obligé de décapsuler le paquet jusqu'à l'adresse IP
2. le spoofing IP est beaucoup plus simple à réaliser que le spoofing MAC.
3. Les Vlans de niveau 3 nécessite l'utilisation d'un protocole de routage

Routage intervlan sur un switch de niveau 3

1. Activez le routage sur le commutateur à l'aide de la commande ip routing===➔ **Switch(config)#ip routing** puis **show ip route**
2. Création et configuration des vlans

Déterminez **les adresses IP** que vous voulez assigner à l'interface VLAN sur le commutateur.
Pour que le commutateur puisse effectuer le routage entre les VLAN, les interfaces VLAN doivent être configurées avec une adresse IP.

a. Quand le commutateur reçoit un paquet destiné à un autre sous-réseau/VLAN, le commutateur regarde **la table de routage** pour déterminer où il doit expédier le paquet.
b. Le paquet est alors passé à l'interface VLAN de la destination.
c. Il est ensuite envoyé au port où le périphérique est relié.

Routage intervlan sur un switch de niveau 3

3. Configurez les interfaces VLAN avec l'adresse IP

Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface Vlan2
Switch(config-if)#ip address 10.1.2.1 255.255.255.0
Switch(config-if)#no shutdown
Répétez ce processus pour tous les VLAN.

4. Configurez l'interface sur le routeur par défaut. Dans ce scénario, vous avez un port FastEthernet de couche 3.

Switch(config)#interface FastEthernet 0/1
Switch(config-if)#no switchport
Switch(config-if)#ip address 200.1.1.1 255.255.255.0
Switch(config-if)#no shutdown

La commande no switchport donne à l'interface les capacités de couche 3. L'adresse IP est dans le même sous-réseau que le routeur par défaut.

Routage intervlan sur un switch de niveau 3

5. Configurez la route par défaut pour le commutateur.
Switch(config)#ip route 0.0.0.0 0.0.0.0 200.1.1.2

- Si le commutateur reçoit un paquet pour un réseau qui n'est pas la table de routage, il l'envoie à la passerelle par défaut pour être traité.
- À partir du commutateur, vérifiez que vous pouvez envoyer un ping au routeur par défaut.
- La commande **ip default-gateway** est utilisée pour spécifier la passerelle par défaut quand le routage n'est pas activé.

Routage intervlan sur un switch de niveau 3

6. Configurez vos périphériques pour qu'ils utilisent l'interface VLAN respective de Catalyst 3550 en tant que leur passerelle par défaut.
   Par exemple, les périphériques dans le VLAN 2 devraient utiliser l'adresse IP d'interface du VLAN 2 en tant que sa passerelle par défaut.
7. Quand vous mettez en œuvre le routage inter-VLAN, vous pouvez également isoler quelques VLAN de l'acheminement.

Routage intervlan sur un switch de niveau 3

```
Cat3550#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2,
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, * - candidate default, U - per-user static route,
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 200.1.1.2 to network 0.0.0.0

     200.1.1.0/30 is subnetted, 1 subnets
C       200.1.1.0 is directly connected, FastEthernet0/48
     10.0.0.0/24 is subnetted, 3 subnets
C       10.1.10.0 is directly connected, Vlan10
C       10.1.3.0 is directly connected, Vlan3
C       10.1.2.0 is directly connected, Vlan2
S*   0.0.0.0/0 [1/0] via 200.1.1.2
```

Le 802.1x et les Vlans

- Assigner un Vlan à un utilisateur lors d'une authentification par 802.1x. Couplé au **GVRP(Diffusion dynamique des VLANs)**, nous avons donc une solution automatisée et sécurisée.
- 802.1X est un standard lié à la sécurité des réseaux informatiques,
- Il permet de contrôler l'accès aux équipements d'infrastructures réseau
- En s'appuyant sur le protocole EAP pour le transport des informations d'identification en mode client/serveur, et sur un serveur d'authentification (tel que RADIUS, TACACS, CAS, etc.)
- le déploiement de l'IEEE 802.1X fournit une couche de sécurité pour l'utilisation des réseaux câblés et sans fil.

Le 802.1x et les Vlans

- Si un équipement réseau actif, tel qu'un commutateur réseau ou une borne Wi-Fi est compatible avec la norme IEEE 802.1X, il est possible de contrôler l'accès à chacun de ses ports (PAE).

Le 802.1p et les Vlans

- Le 802.1p est une extention du 802.1q permettant d'offrir un mecanisme de prioritisation des trâmes au niveau LAN.
- Il s'appuie sur le champ priorité de la trame 802.1q définit sur 3 bits.
- Il existe deux utilisations du 802.1p, la première dans le cadre du GMRP et le deuxième dans un mécanisme de classe de service.
- Le **GMRP** est un protocole de multicast équivalent à l'IGMP mais au niveau 2.
- **Le mécanisme de classe de service:**

consiste à buffeuriser les trames et à emettre des plus prioritaires aux moins prioritaires. Cette solution est très basique pluisqu'elle ne garanti aucun débit et n'assure aucun contrôle de flux.

Le 802.1p et les Vlans

- **Le mécanisme de classe de service:**

7 Contrôle du réseau (network critical)
6 Voix interactive
5 Multimédia interactif
4 Application à charge controlé (streaming)
3 Service maximum (Business critical)
0 Service au mieux (Best effort)
2 Service économique (standard)
1 Arrière plan (background)

Résumé

VLAN de niveau 1 (ou VLAN par port) : on y définit les ports du commutateur (switch) qui appartiendront à tel ou tel VLAN.
VLAN de niveau 2 (ou VLAN par adresse MAC) : on indique directement les adresses MAC des cartes réseaux contenues dans les machines que l'on souhaite voir appartenir à un VLAN, si la base de données contenant les adresses MAC tombe en panne, tout le réseau est alors affecté). De plus, il est possible de tricher sur son adresse MAC (spoofing).
VLAN de niveau 3 (ou VLAN par adresse IP) : même principe que pour les VLAN de niveau 2 sauf que l'on indique les adresses IP (ou une plage d'IP) qui appartiendront à tel ou tel VLAN.
VLAN par protocole un VLAN pour IP, un autre VLAN pour le trafic Appletalk

Résumé

Déploiement et transport des Vlans

- Le protocole 802.1q
- Le VTP (Vlan Trunking Protocol)

Contrôle d'accès

- Le VMPS (VLAN Membership Policy Server)
- 802.1x

Les contrôles de flux

- Le 802.1p

Sécurité et conception VLAN