

Les VLANs

Virtual LAN

Sondes Kallel

1

Plan

- Rappel
- Principe des VLANs
- Intérêts
- Appartenance à un VLAN
- Identification des VLAN (IEEE 802.1Q)

2

Définition

Virtual Local Area Network

3

Pourquoi les VLANs ?

- Dans les réseaux locaux partagés
 - les sous-réseaux sont liés aux hubs
 - les utilisateurs sont groupés géographiquement
 - pas de sécurité sur un segment : n'importe quelle station du segment peut capturer l'ensemble du trafic réseau
 - la mobilité entraîne un changement d'adresse et/ou un re-câblage

4

Pourquoi les VLANs ?

- Trois nécessités auxquelles un LAN commuté ne répond pas
 - Limitation des domaines de diffusion
 - Garantir la sécurité par isolement de certains trafics (Souvent, il n'est pas nécessaire que les paquets broadcast de tous les appareils soient envoyés à l'ensemble du réseau, ils existent des groupes de machines qui ont besoin de recevoir les paquets broadcast les unes des autres, mais pas de l'extérieur du groupe)
 - Permettre la mobilité des utilisateurs

5

Pourquoi les VLANs ?

- Isoler les domaines de collision et de diffusion
- C'est quoi un domaine de collision et de diffusion ??
 - Rappel

6

DOMAINE DE DIFFUSION / DOMAINE DE COLLISION

□ DOMAINE DE DIFFUSION

- Un domaine de diffusion (broadcast domain) est une zone logique d'un réseau informatique où un ordinateur quelconque connecté au réseau peut directement transmettre à tous les autres ordinateurs du même domaine, sans devoir passer par un routeur.

- Plus spécifiquement, c'est une zone du réseau informatique composée de tous les ordinateurs et équipements de communication qui peuvent être contactés en envoyant une trame à l'adresse de diffusion de la couche liaison.

7

DOMAINE DE DIFFUSION / DOMAINE DE COLLISION

□ DOMAINE DE COLLISION

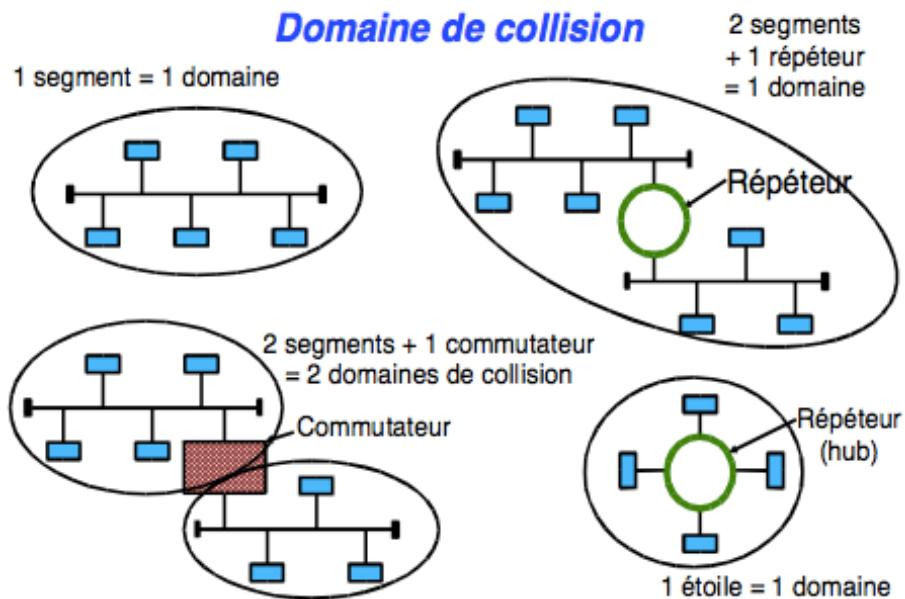
- Un domaine de collision est une zone logique d'un réseau informatique où les paquets de données peuvent entrer en collision entre eux, dans un réseau Ethernet.

- Un domaine de collision peut être un seul segment de câble Ethernet, un seul concentrateur ou même un réseau complet de concentrateurs et de répéteurs.
 - Un concentrateur forme un seul domaine de collision alors qu'un commutateur ou un routeur en crée un par port, ce qui réduit les risques de collision.

 - Lorsque l'Ethernet est utilisé en mode duplex (full-duplex), il n'y a plus de domaine de collision, car aucune collision n'est possible.

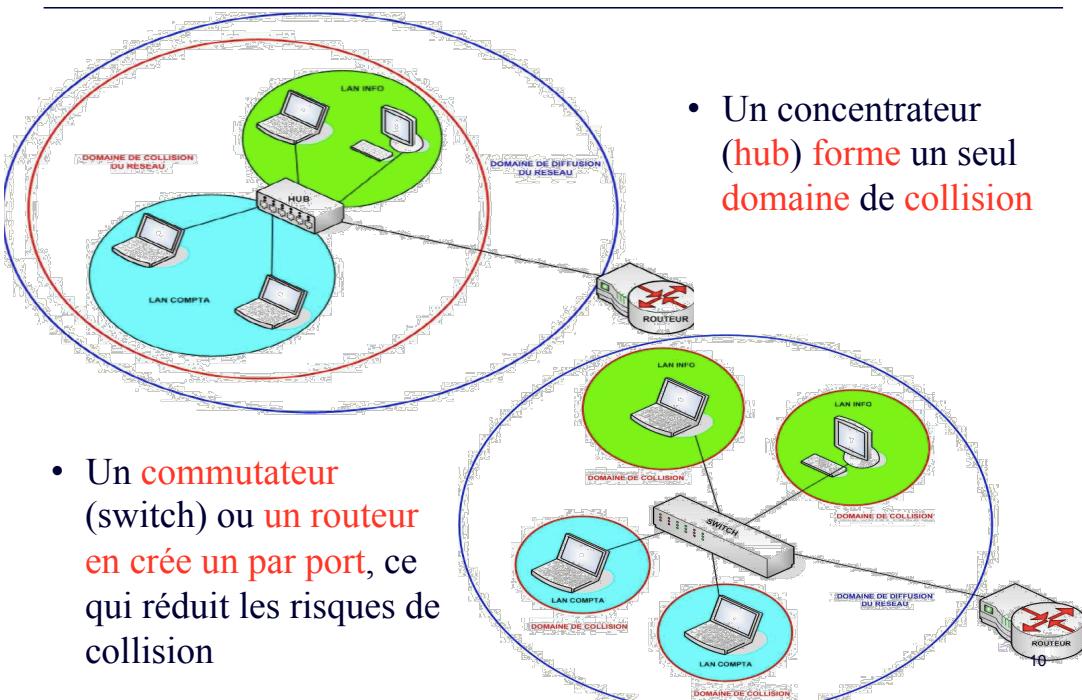
8

DOMAINE DE COLLISION



9

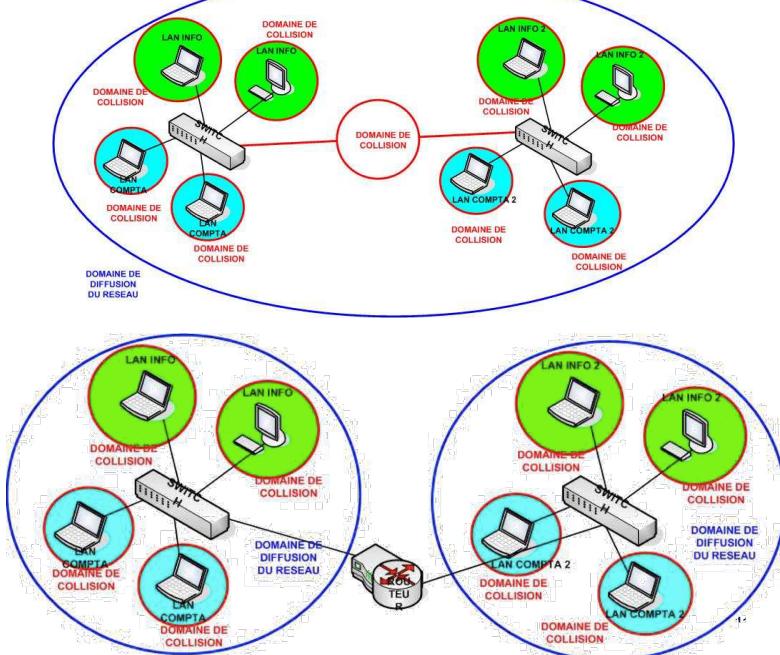
DOMAINE DE DIFFUSION / DOMAINE DE COLLISION



10

DOMAINE DE DIFFUSION / DOMAINE DE COLLISION

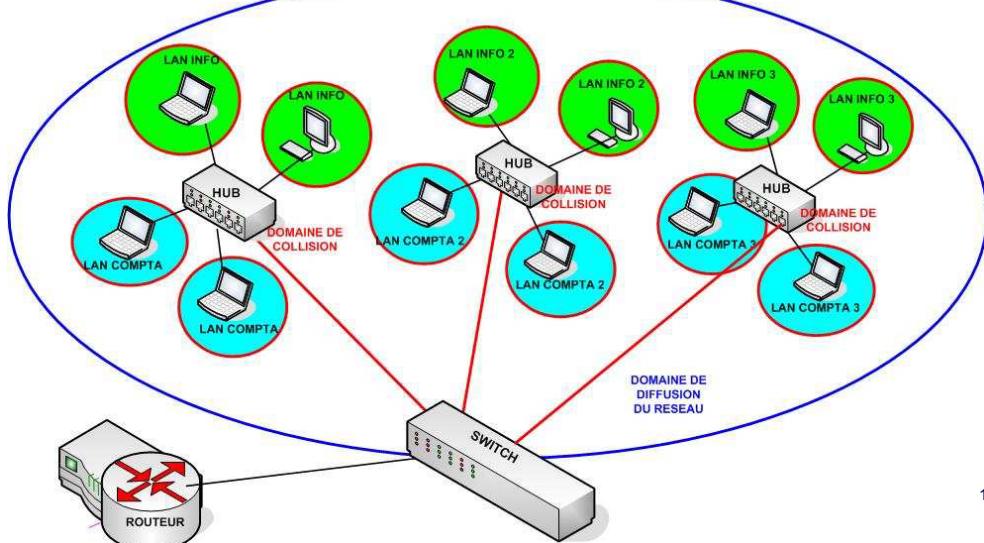
- Les concentrateurs / Hub et commutateurs conservent le même domaine de diffusion



- Les routeurs les divisent

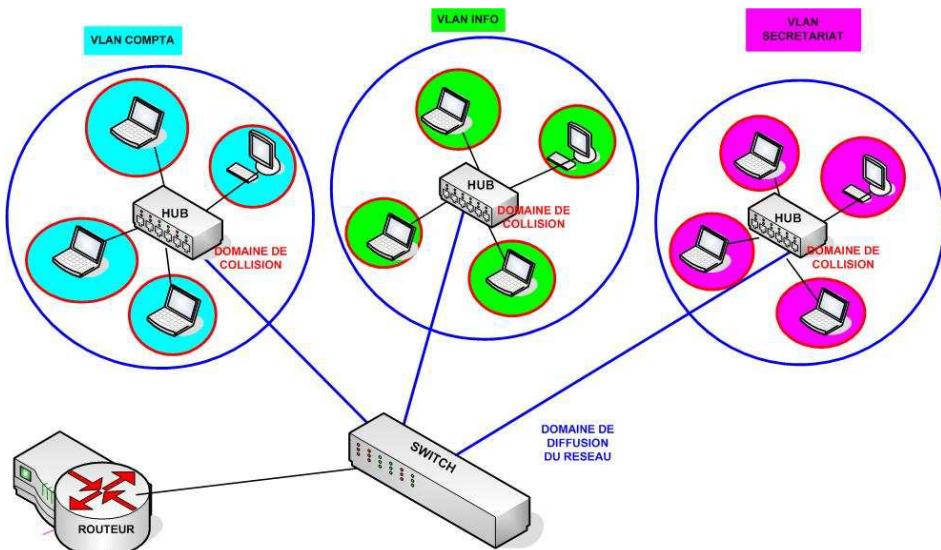
DOMAINE DE DIFFUSION / DOMAINE DE COLLISION

- Hub et commutateurs conservent le même domaine de diffusion
- **MAIS** Il existe une solution pour séparer virtuellement un hub/commutateur en plusieurs domaines de diffusion : Les VLANs



VLANS ET DOMAINE DE DIFFUSION / COLLISION

- L'utilisation de réseaux virtuels VLANs permet de séparer virtuellement un concentrateur/commutateur en plusieurs domaines de diffusion.



13

Solution => Les VLANs

14

VLAN (Virtual Area Network)

- Plusieurs réseaux logiques indépendant sur le même réseau physique
- La communication n'est autorisée qu'entre machines d'un même VLAN
- Les communications inter-VLAN doivent transiter par un routeur

15

VLAN (Virtual Area Network)

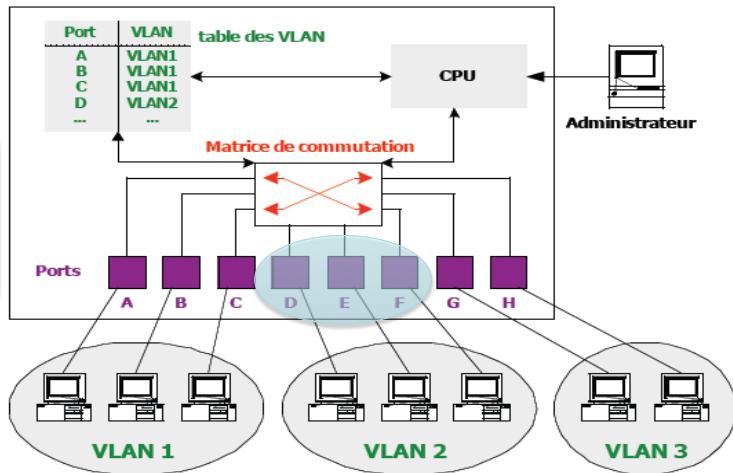
- L'appartenance à un VLAN étant définie logiquement et non géographiquement
- Les VLAN permettent d'assurer la mobilité des postes de travail
- Plusieurs niveaux de VLAN

16

Principe des VLAN (1)

- Il s'agit de diviser le LAN en unité logique appelés LAN virtuels; cela revient à avoir différent LAN à l'intérieur d'un même LAN physique
- Chaque LAN est identifié par un numéro unique
- Les appareils d'un même VLAN peuvent tous communiquer entre eux, mais pas avec ceux-en-dehors.(L'appartenance à un VLAN étant définie logiquement et non géographiquement)

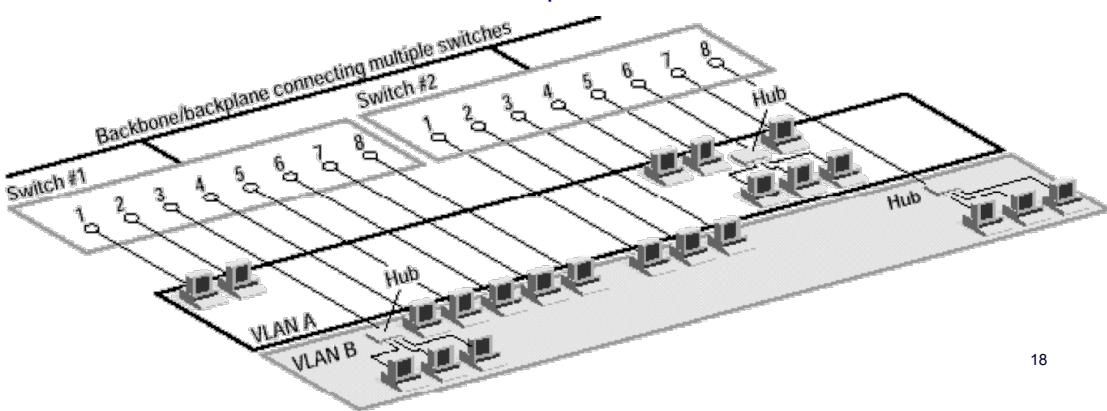
Une diffusion provenant d'une station du VLAN2 ne sera répercutée que sur les ports D, E, F



Principe des VLAN (2)

- L'administrateur configure statiquement la table des VLAN
- Les communications inter-VLAN ne sont possibles qu'à travers un routeur
- L'appartenance à un VLAN est indépendante de la localisation géographique - un VLAN peut s'étendre sur plusieurs commutateurs
- Un segment Ethernet est un domaine de collision
- Un VLAN est un domaine de diffusion

Exemple

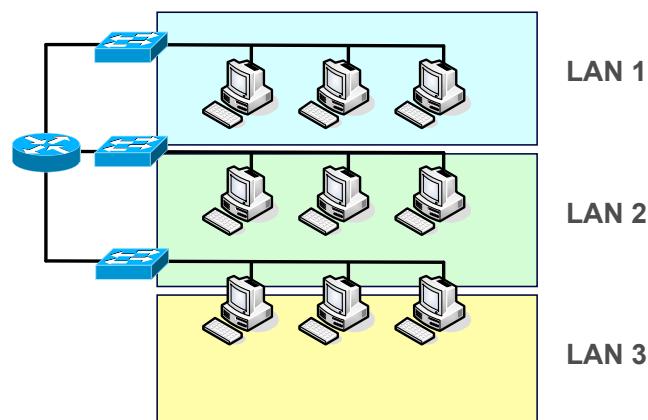


Intérêts des VLANs

- Confidentialité et sécurité
 - le trafic entre les réseaux virtuels est isolé
 - permet de limiter l'accès à certains équipements ou services (VLAN des machines en libre service, VLAN des accès à Internet, ...)
- Performance
 - limite la portée des broadcast
 - répartition de la charge du réseau
- Facilité de mise en oeuvre et souplesse
 - logiciel d'administration du commutateur
 - on peut retirer ou donner l'accès à un VLAN sans modifier le câblage dans les armoires de brassage, voire sans déplacer la station
 - une station peut appartenir à plusieurs VLANs

19

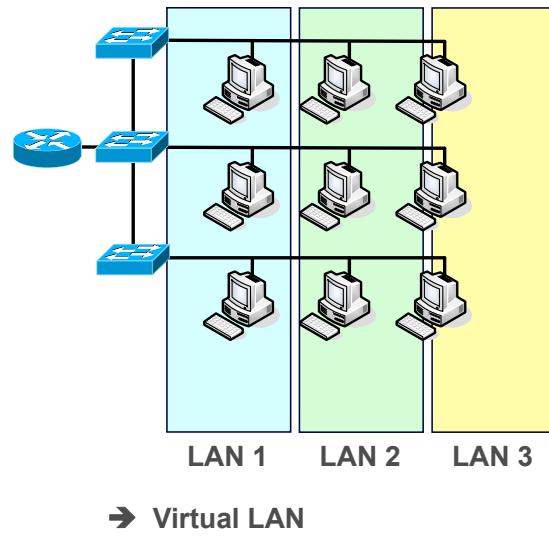
Intérêt



→ Classic Segmentation

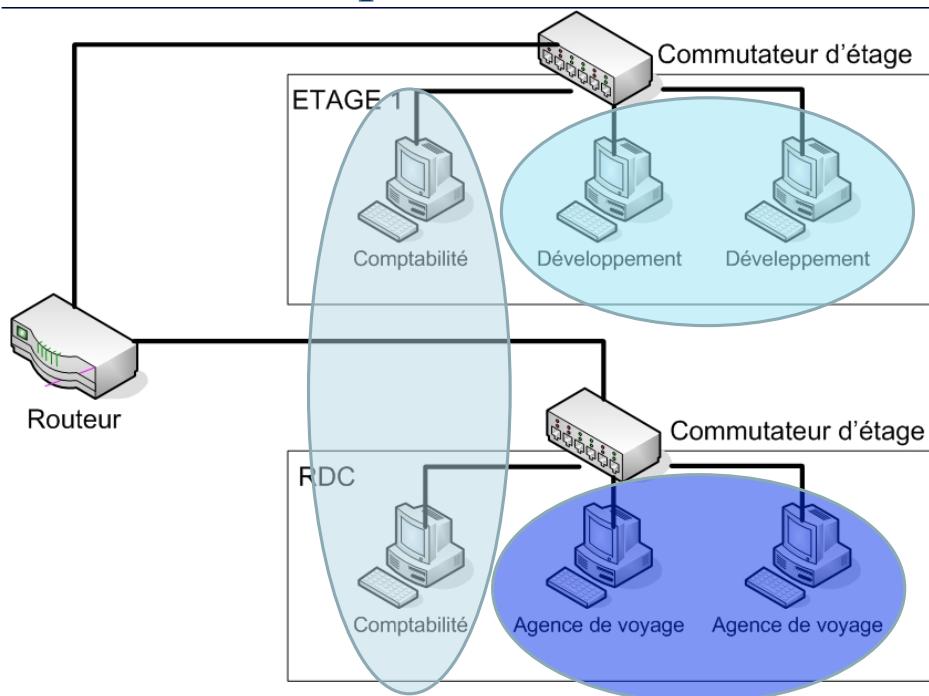
20

Intérêt



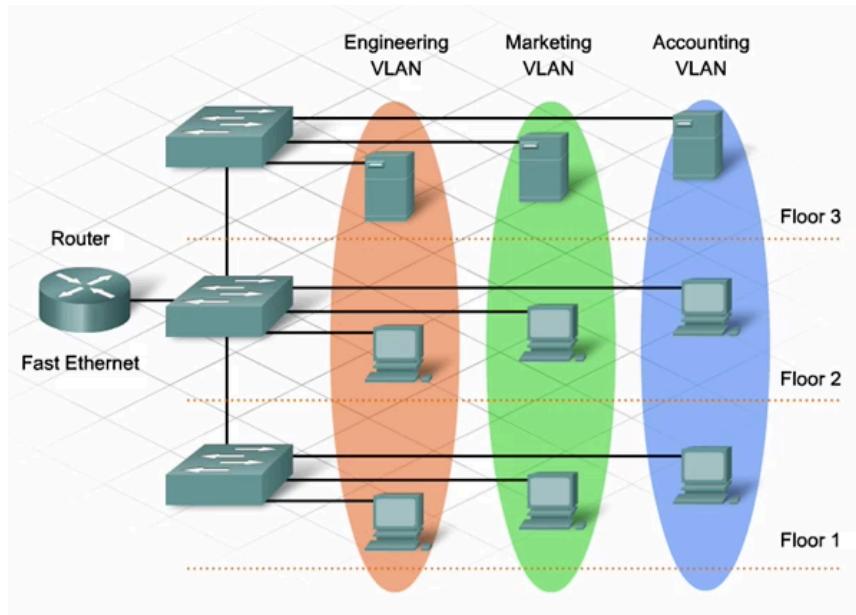
21

Intérêt : exemple



22

Intérêt : exemple



23

Types de VLAN

- Statique
- dynamique

24

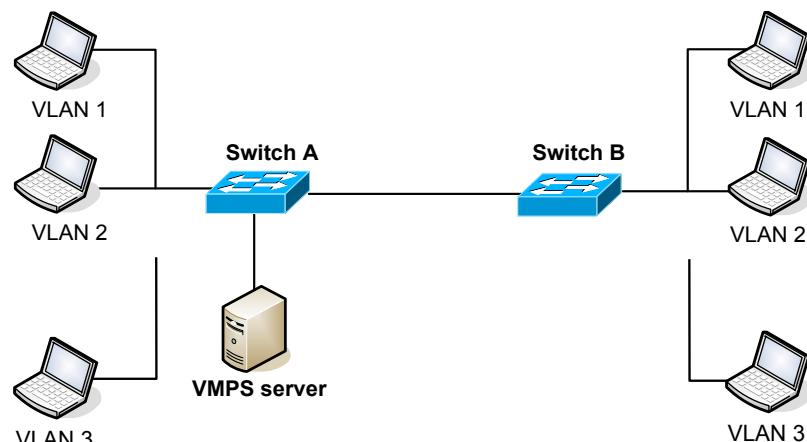
Statique

- Un port physique correspond à un seul VLAN
- La table de commutation est remplie manuellement
- Avantage
 - Rapidité et simplicité d'installation
- Inconvénient
 - Le port n'est pas sécurisé
 - Difficile à gérer

25

Dynamique

- L'appartenance à un VLAN selon @ MAC
- Administration logicielle

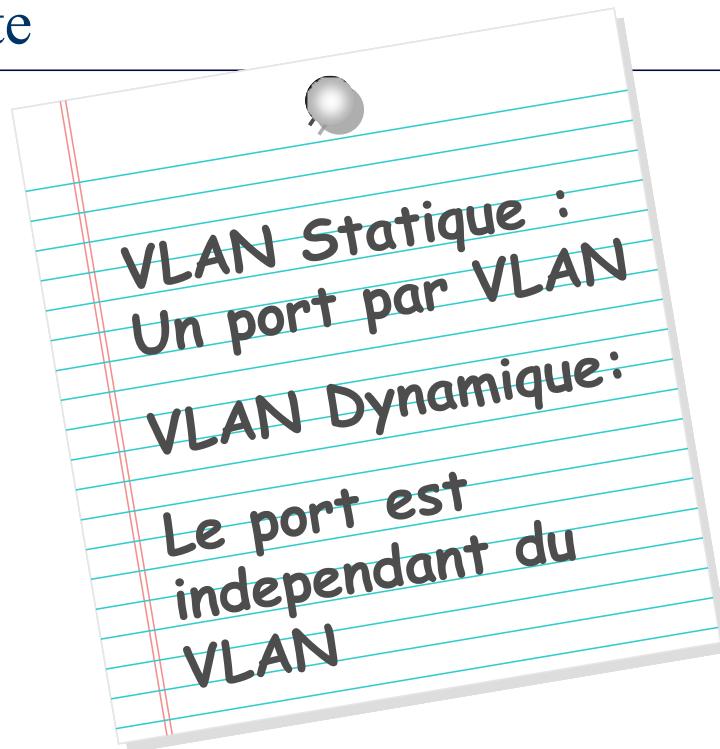


- VLAN Management Policy Server : permet d'affecter dynamiquement les ports d'un commutateur à un Vlan en fonction de l'adresse MAC du périphérique réseau.
- Il est chargé de faire correspondre un Vlan à une ou plusieurs adresses MAC.

26



Note



Types de VLAN

- Par port
- Par adresse MAC
- Par adresse IP
- Par Protocole de niveau 3

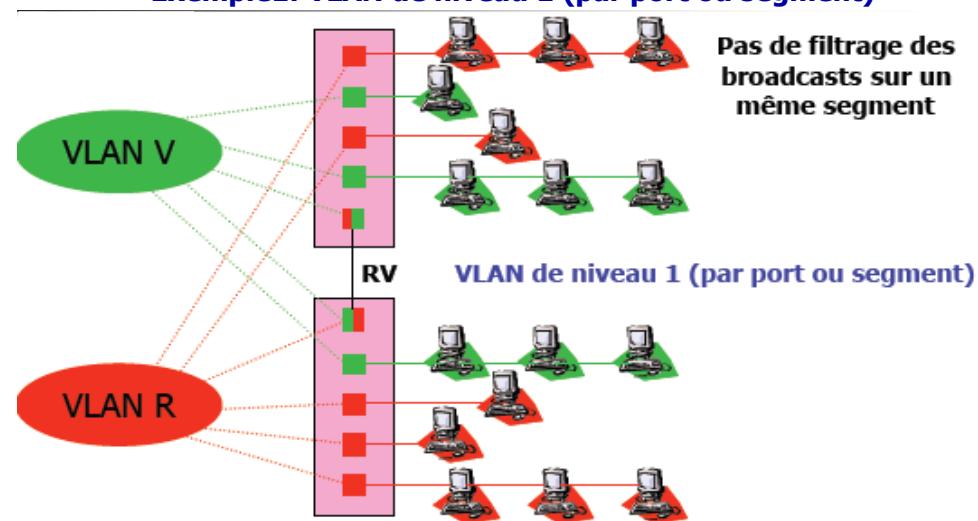
VLAN Niveau 1

- VLAN niveau 1 ou VLAN par port (Port-Based VLAN)
 - Les stations regroupées à un même port du commutateur
 - Configuration statique, le déplacement d'une station implique son changement de VLAN
 - configuration statique fixée par l'administrateur

29

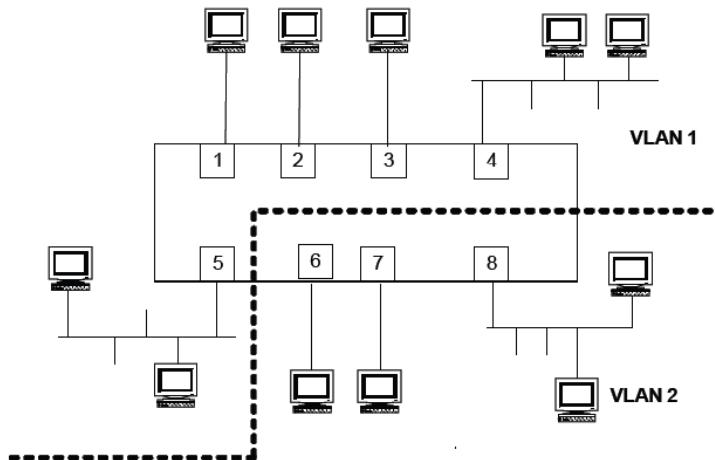
VLAN Niveau 1

Exemple1: VLAN de niveau 1 (par port ou segment)



30

VLAN Niveau 1



31

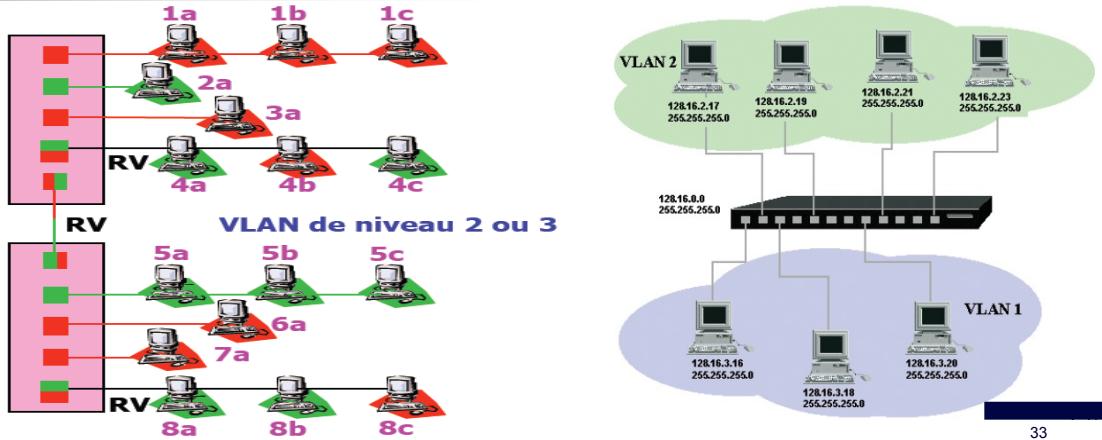
VLAN Niveau 2

- VLAN niveau 2 (MAC Address-Based VLAN)
 - Association des stations par leurs adresses MAC
 - Les tables d'adresse sont introduites par l'administrateur ou par apprentissage automatique
 - Une station peut appartenir à plusieurs VLAN
 - Une indépendance des protocoles supérieurs
 - Plus souple : permet la mobilité des machines sans reconfigurer les VLAN
 - l'administrateur doit connaître les @ MAC...
 - deux stations du même segment Ethernet peuvent appartenir à des VLAN distincts

32

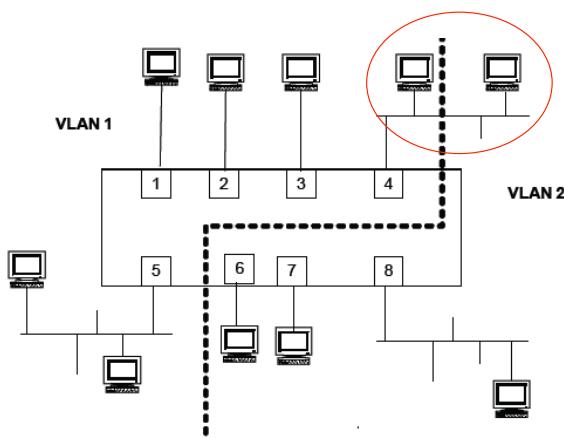
VLAN Niveau 2

- Une adresse MAC ne peut appartenir qu'à un seul VLAN
- Plusieurs VLAN par port autorisés
- Nécessite une analyse de chaque trame
- Echange des tables de correspondances @MAC/VLAN entre les commutateurs ou étiquetage des trames nécessaires



33

VLAN Niveau 2



+ Grande souplesse car permet d'avoir des stations sur un même port du switch et pourtant appartenant à des VLAN différents

34

VLAN Niveau 3

□ VLAN niveau 3 (Network Address-Based VLAN)

- Les stations sont définies par leur adresse réseau
 - On associera un VLAN à une plage d'adresse
- Les utilisateurs d'un VLAN sont affectés dynamiquement à un VLAN
- Une station peut appartenir à plusieurs VLAN par affectation statique
- Le commutateur doit accéder à l'adresse de niveau 3 pour définir le VLAN
- l'adresse de niveau 3 est utilisée comme étiquette pour une commutation (pas de routage)

35

VLAN Niveau 3

□ Avantages et inconvénients

- très souple : association d'un préfixe IP (@ de sous-réseau ou plages d'@) et d'un numéro de VLAN
- un routeur permet de passer d'un VLAN à l'autre
- perte de performance : il faut analyser les trames au niveau 3 pour déterminer l'appartenance à un VLAN
- non sécurisé : l'utilisateur peut facilement changer son @ IP

36

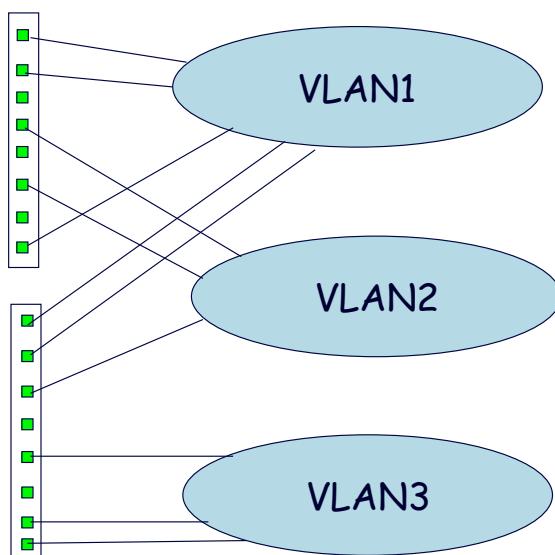
VLAN

- Les VLAN peuvent être réalisé par
 - Protocole (IP,IPX*...), la commutation ne pouvant s'établir qu'entre stations utilisant le même protocole
 - Par application (N° de port TCP), la constitution des VLAN est alors dynamique, un utilisateur pouvant successivement appartenir à des VLAN différents selon l'application utilisée
 - Par mot de passe (constitution dynamique des VLAN au login de l'utilisateur)

37

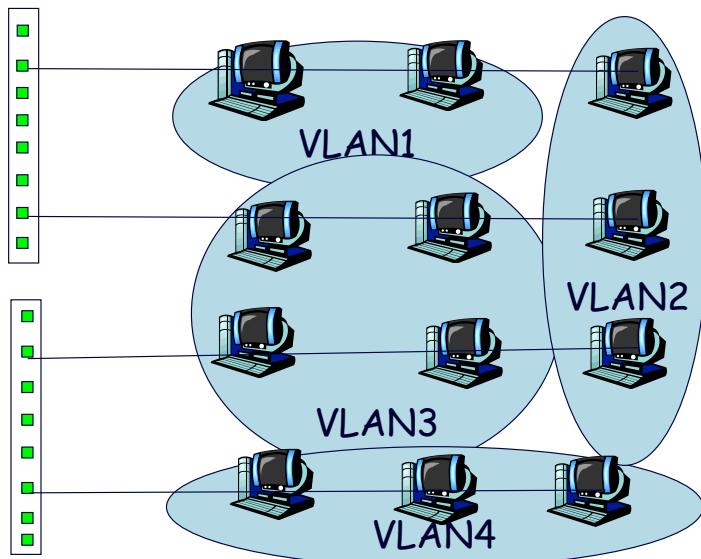
*IPX : Internetwork Packet Exchange (datagramme mode non connecté protocole de niveau 3)

VLAN niveau1, par port ou segment



38

VLAN (niveau2(@MAC) ou (N3@IP))



39

Comment ça marche

- Comment une machine fait elle pour savoir à quel VLAN elle appartient?
 - La machine peut ne pas le savoir, ou ne pas pouvoir l'exprimer
 - L'administrateur le spécifie au niveau des switchs
- Les switchs ajoutent des « étiquettes » (tags) aux trames, et masquent leur présence aux machines
 - Ces tags permettent d'aiguiller les trames entre switchs
 - Ils sont retirés de la trame avant qu'elle soit délivrée aux machines qui ne savent pas les interpréter.

40

VLAN: la norme IEEE 802.1Q

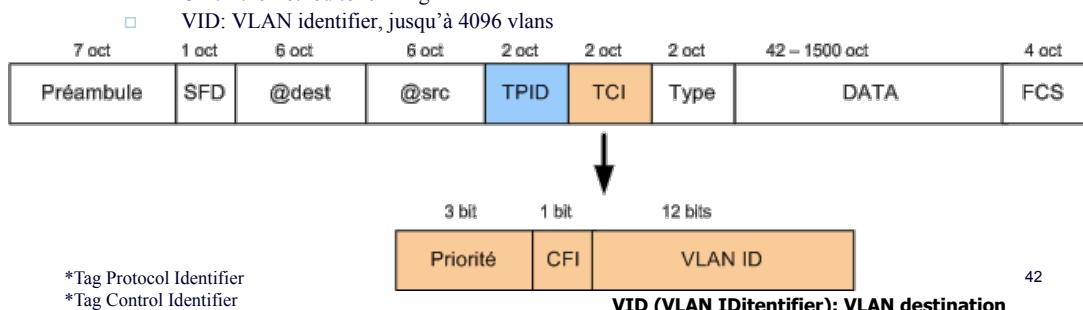
Identification des VLAN

- Il faut transporter l'information d'appartenance à un VLAN (chaque commutateur doit connaître le VLAN associé à la source et au destinataire)
- Deux possibilités
 - chargement des tables de VLAN dans tous les équipements (problème de facteur d'échelle)
 - ajout d'une étiquette aux trames transportées entre les commutateurs uniquement (côté émetteur)
 - l'étiquette identifie le VLAN de la station source
 - norme IEEE 802.1p/Q : format des étiquettes indépendant du constructeur de l'équipement

41

Trame Ethernet 802.1Q

- Modification transparente de l'en-tête MAC (compatibilité avec les anciens équipements)
 - un niveau d'encapsulation 802.1p/Q identifié par 0x8100=TPID
 - la trame 802.3 est allongée de 4 octets (nécessite de recalculer le FCS)
 - champ priorité sur 3 bits : files d'attente plus ou moins prioritaires dans les commutateurs (QoS - voix par ex.)
 - bit CFI (canonical Format Identifier) pour le routage par la source
 - TPID: type du tag, 0x8100 pour 802.1Q
 - Priorité: niveaux de priorité définis par l'IEEE 802.1P
 - CFI: Ethernet ou token-ring
 - VID: VLAN identifier, jusqu'à 4096 vlans



42

Champs IEEE 802.1p et 802.1q

- TPID (*Tag Protocol Identifier*). 2 octets
 - Pour identifier le protocole de la balise insérée
 - 0x**8100** pour les trames « taggées » si 802.1q
- TCI (*Tag Control Information*). 2 octets
 - 3 premiers bits: *user priority* (802.1p) de 0 à 7
 - 1 bit CFI (*Canonical Format Indicator*).
 - Assure la compatibilité entre les adresses
 - Ethernet:0 / token ring :1
 - 12 bits: VID (*VLAN Identifier*)
 - 0 => l'en-tête ne contient que des infos de priorité
 - 1 => valeur par défaut d'identificateur de VLAN
 - FFF => réservé (implémentation)

43

Trois types de trames VLANs

- Pouvant traverser un switch « *VLAN-aware* »
 - Trame non taggée
 - absence d'en-tête (TIPD+TCI) après adresse MAC source
 - Trame taggée de priorité
 - VID=0 => Pas signifiant. Ne transporte que des infos de priorité. Du point de vue du processus de transmission, elle est considérée comme une trame non taggée
 - Trame taggée de VLAN
 - TIPD=0x8100, CFI=0 et VID entre 1 et 4094.
- Switch « *vlan informé* » (*Vlan-aware*) : reconnaît les trames étiquetées ; (*Vlan-unaware*) c'est dans le cas contraire.

44

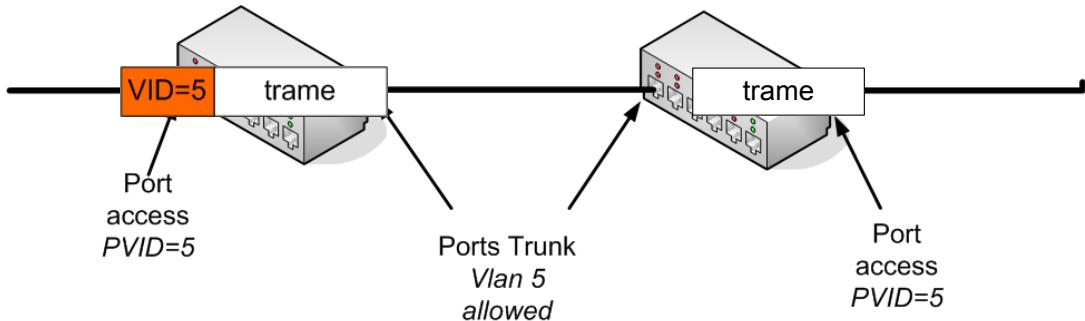
Terminologie

- VID : Vlan ID
- PVID : Port Vlan ID
- Mode d'accès
 - Port Access ou untagged (non étiqueté)
 - Port trunk ou tagged (étiquetté)
 - Matériel Aware (Vlan-informé)
- VLANs de base
 - VLAN natif (trame non étiquetée)
 - VLAN par défaut généralement VLAN 1
 - VLAN utilisateur
 - VLAN de management

Politique de transmission

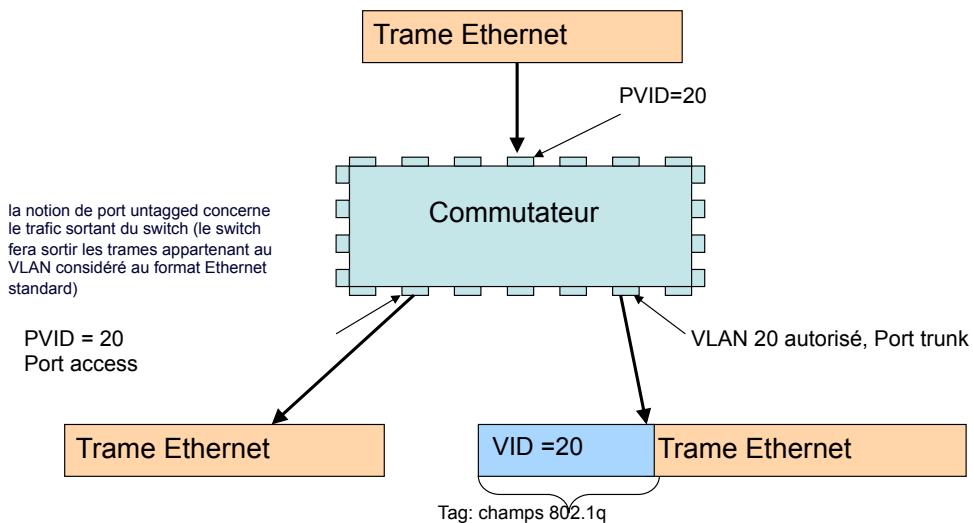
- 802.1Q (1998) a choisi de considérer:
 - Switchs *VLAN-aware* utilisent par défaut le tag
 - Si une trame est taggée de VLAN, on utilise son VID
 - Sinon (trame taggée de priorité ou non taggée), on peut utiliser d'autres moyens pour déterminer le VLAN d'appartenance, en inspectant les données comme l'adresse MAC ou le champ type (solutions propriétaires).
 - En l'absence d'un autre moyen, c'est le port de réception qui donnera l'appartenance de la trame à un VLAN: son PVID (*Port VLAN IDentifier*)

Exemple

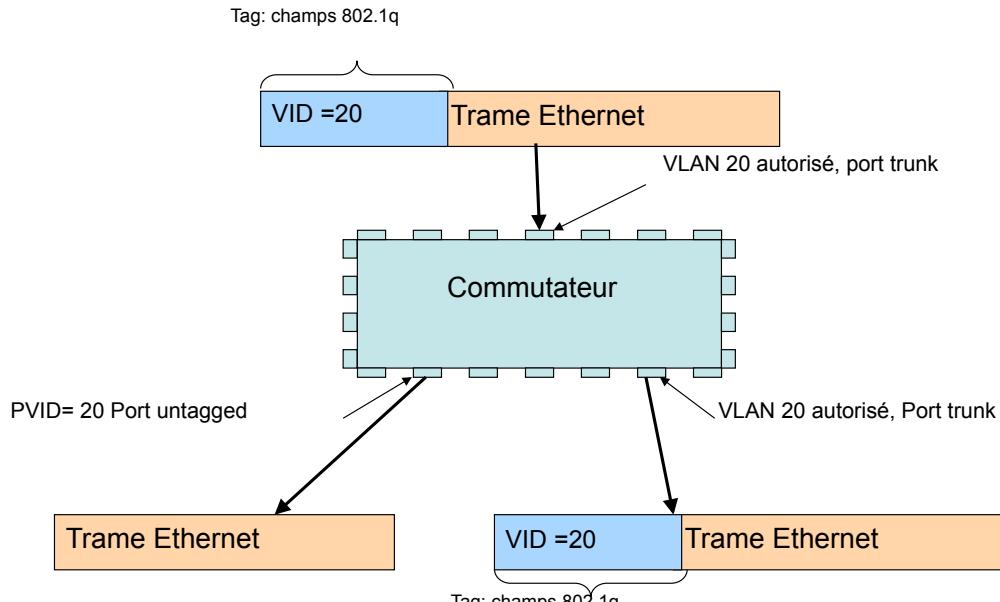


segmenter les ports : une trame Ethernet classique (non tagguée) arrive sur un port donné. On associe un VLAN (un VID) à ce port, c'est à dire que le switch va ajouter le **tag** à la trame. Cette trame ne sera ensuite émise que sur les ports qui acceptent le même VID. Dans l'autre sens, si un paquet arrive dans le switch à destination du VLAN associé à ce port, il sera émis par le switch après retrait du tag. Ainsi, l'équipement connecté au port émettra et recevra des trames Ethernet normales, sans tag. Il ne saura pas qu'il est sur un VLAN. ⁴⁷

Exemple



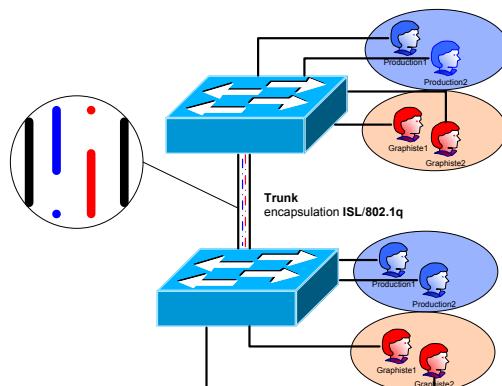
Exemple



Mettre un port sur plusieurs VLAN : dans ce cas, le port est configuré pour accepter des trames déjà tagguées. L'équipement connecté au port doit donc savoir émettre des trames Ethernet 802.1q. Cela lui permet d'envoyer et recevoir des trames Ethernet vers ou depuis plusieurs VLAN.
Dans ce cas, on dit que le port est ajouté au VLAN "VID" en mode tagged. Un port peut être *tagged* sur autant de VLAN que nécessaire : il générera les trames Ethernet pour tous les VLAN concernés.

Principe du Trunking

- Utilisé dans un réseau avec plusieurs commutateurs
- Transmet le trafic VLAN sur plusieurs équipements
- Une seul lien physique, plusieurs liens logiques



Interconnexion inter-VLAN

- Se fait au niveau 3 du modèle OSI,
- Donc routage, entre interfaces virtuelles
- Seul un routeur peut réaliser l'interconnexion entre deux VLANs et modifier ainsi le VID associé à une trame.

51

Commandes VLAN

52



Commandes

Création de VLAN

■ **vlan {vlan-id}**

- Mode de configuration Global
- Crée le VLAN et entre son mode de configuration

■ **name {vlan_name}**

- Mode de configuration Global
- Nomme le VLAN

```
Mon-switch(config)#vlan 36
Mon-switch(config-vlan)#name My_VLAN
```



Commandes

Configure un port dans un VLAN

■ **switchport mode {access | dynamic {auto | desirable} | trunk}**

- Mode de configuration de l'Interface
- Configure une interface d'un VLAN ou un trunking

■ **switchport access vlan {n°vlan}**

- Mode de configuration de l'Interface
- Configure un VLAN statique dans une interface



Commandes

Effacer VLANs

- Les Vlans sont enregistrés dans un flash
 - **Delete flash: vlan.dat**
 - Mode Privilegié
 - Après reboot, ça s'efface



Commandes

Debug commands

- **show interfaces [interface-id | vlan {vlan-id}] [switchport | trunk]**
 - Mode Privilegié
 - Montre l'état de l'interface
- **show vlan [brief | {vlan-id} | name {vlan-name} | summary]**
 - Mode Privilegié
 - Liste les informations de ou des VLAN(s) spécifié(s)



Commandes

Commandes de Debug

■ show flash :

- Mode Privilegié
- Montre les informations sur vlan.dat

Commandes Trunking



Commandes

Configure un port en mode trunk

- **switchport mode trunk**
 - Mode de configuration Interface
 - Permet d'assurer le trunking
- **switchport trunk [allowed | encapsulation | native | pruning]**
 - Mode de configuration Interface
 - Liste le VLAN authorized
 - Type d'encapsulation (ISL, 802.1q)
 - Native VLAN configuration
 - Liste non-transmitted VLAN (pruning)



Commandes

Commandes de Debug

- **show port capabilities [if/sub-if]**
 - Montre les capacités du port
- **show interface trunk**
 - Montre la configuration du trunking