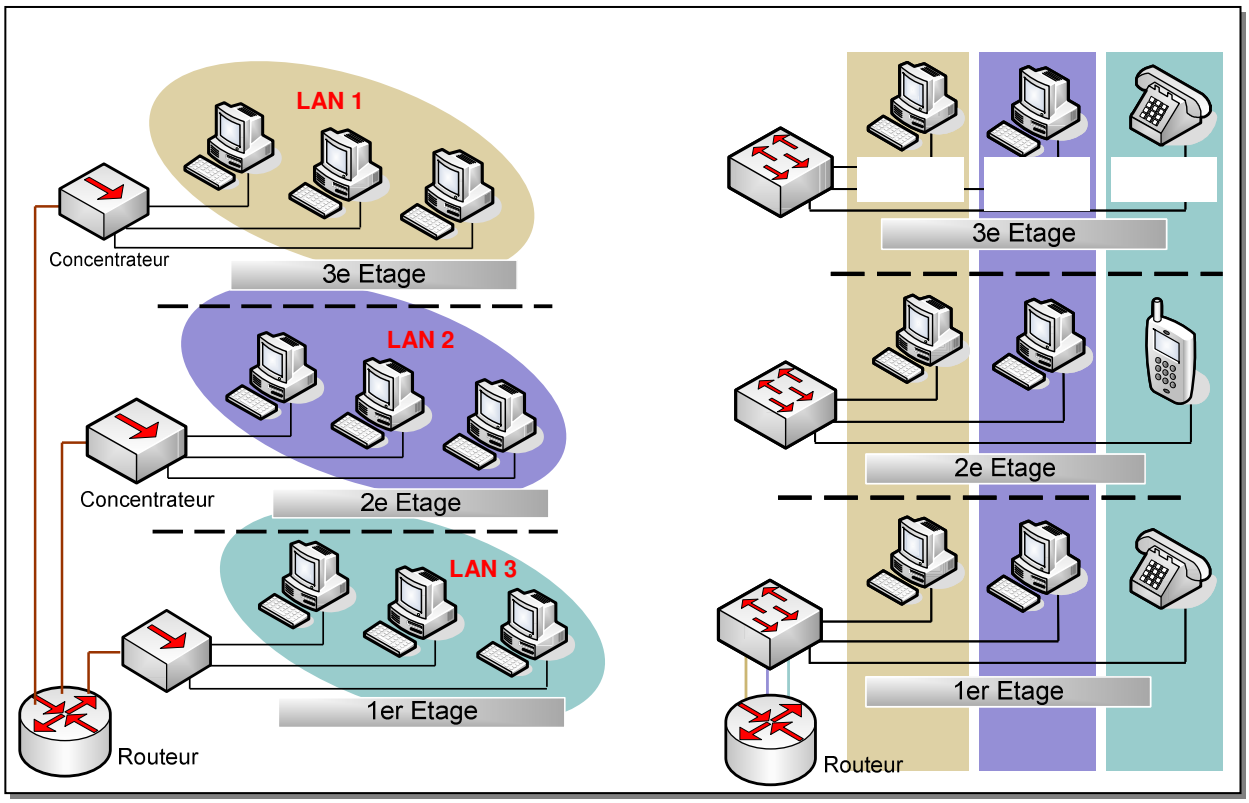
Les réseaux locaux virtuels (Vlan)

1. Le concept des réseaux privés virtuels (vlan) :

1.1 Présentation :



Segmentation traditionnelle :

- *Constat* : topologie physique et topologie logique sont étroitement liées, c'est-à-dire que les postes informatiques sont regroupés vers un seul et même équipement.
- *Idée* : rajouter de l'informatique de telle sorte à obtenir des topologies physique et logique indépendantes tout en conservant des domaines de broadcast suffisamment petits afin de garantir la bande passante.

Segmentation avec des Vlans :

- _____
  _____
  _____
  _____
- De plus les VLAN participent à l'utilisation efficace de la bande passante, car ils partagent le même domaine de broadcast.

1.2 Vlan et modèle OSI :

Le transport des données est surtout gérer par les 3 couches basses du modèles OSI. L'expérience a montré que la mise en œuvre des réseaux privés virtuels doit être faite à travers ces 3 niveaux du modèle.

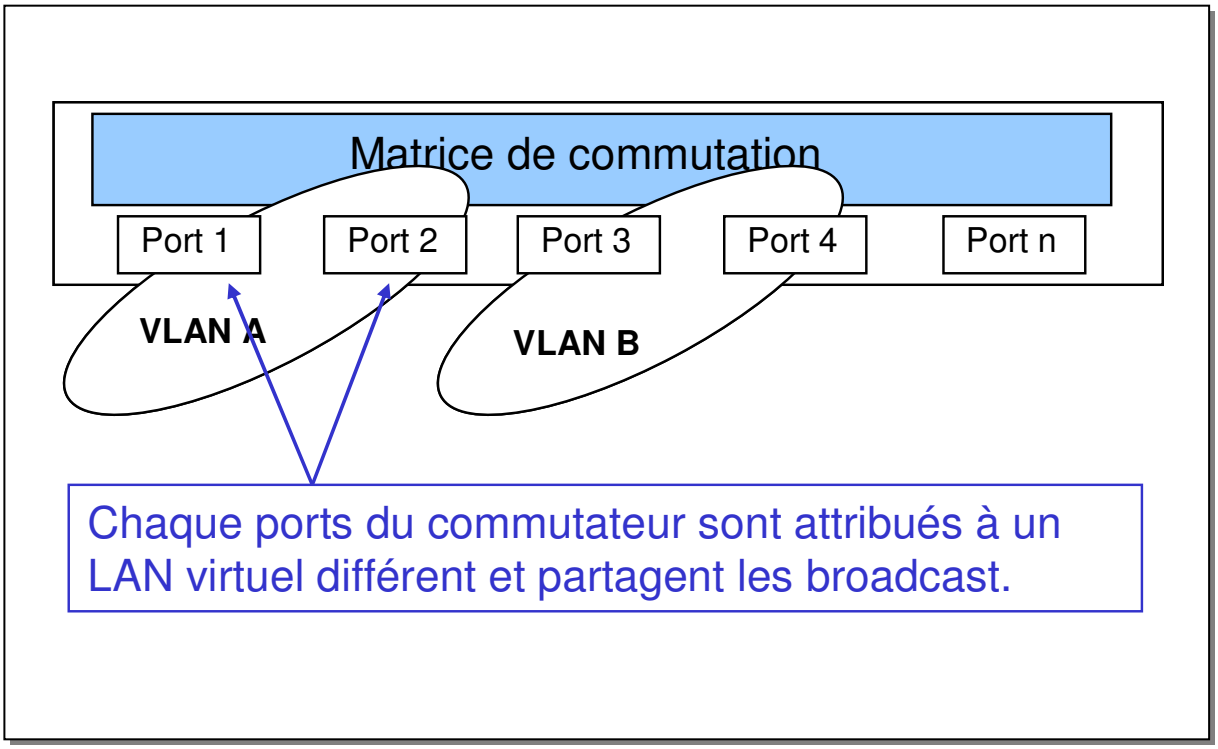
Acheminement des paquets → Réseau / Liaison de données / Physique

On parle _____

2. Les réseaux Locaux Virtuels de niveau 1 et 2 :

2.1 Vlan statiques ou vlan de niveau 1 :

2.1.1 Principe



Les Vlan statiques sont _____

2.1.2 Fonctionnement :

```
EC-PRE1R0#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                                Gig1/2
401  W-PU-401                         active    Fa0/16, Fa0/17
402  T-PU-402                         active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15
405  D-PU-405                         active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10
499  A-PU-499                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
EC-PRE1R0#
```

Liste des ports affectés au vlan « D-PU-405 »

On construit une table des réseaux privés virtuels qui sera alors consultée par le commutateur durant son fonctionnement.

Que fait alors le commutateur lorsqu'il reçoit une trame sur un de ses ports ?

-

-

-

-

Avantages :

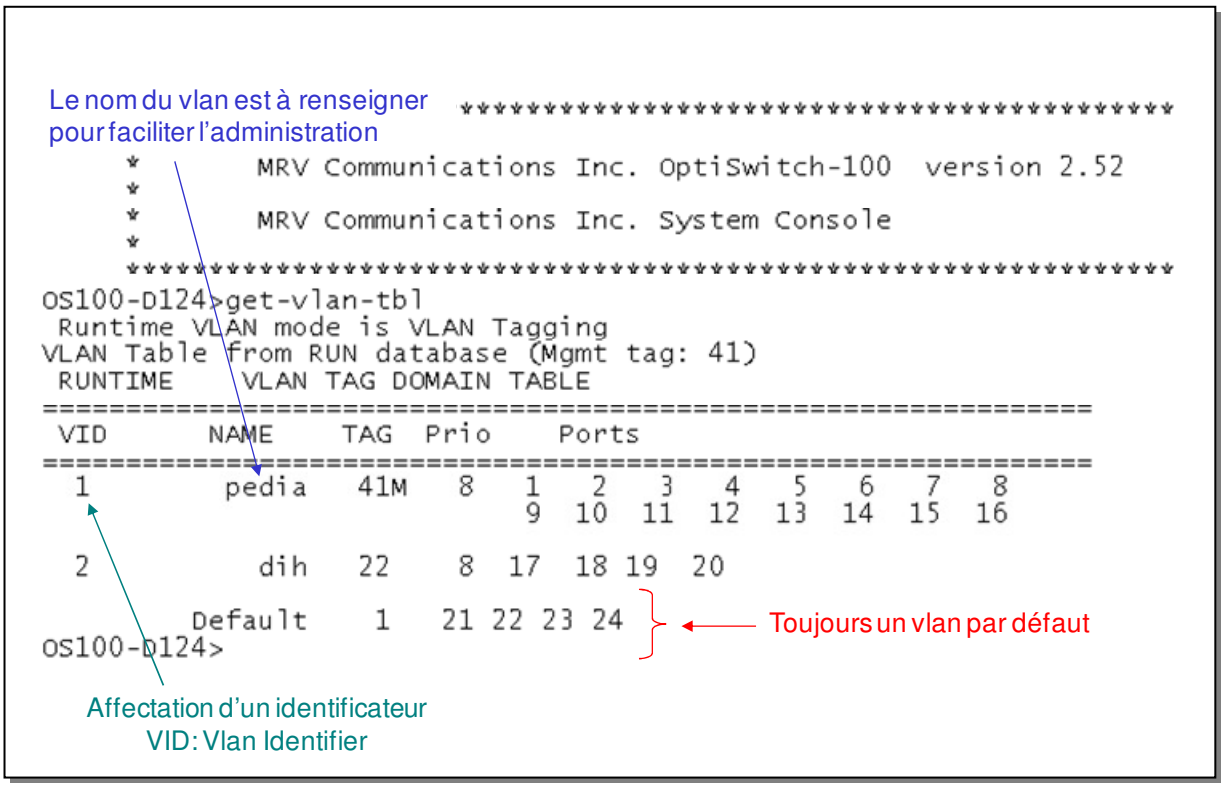
- Les Vlan limitent les flux de trafic aux ports des membres du Vlan,
- **Sécurité** : chaque groupe d'utilisateur est isolé et facile à surveiller,
- **Réduction** du domaine de broadcast (limitation des broadcast),
- Ce principe est le plus utilisé.

Inconvénients :

- Bien que l'on puisse administrer à distance cela nécessite un brassage et un repérage des ports sur commutateur (statique).

La mise en œuvre et les tests des vlans statiques sont abordés durant le TP.

2.1.3 Autre exemple d'une table :



Exemple de configuration chez Cisco :

Deux étapes:

1. Création des vlans
   - En entrant dans la base des Vlans:

```
Switch# vlan database
Switch(vlan)#vlan <ViD:numéro du vlan>
Switch(vlan)#vlan <ViD> name <nom administratif>
```

   - En mode de configuration globale:

```
Switch#conf t
Switch(config)#vlan <ViD:numéro du vlan>
Switch(config-vlan)#name <nom administratif>
```

2. Affectation des interfaces

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan <ViD>
```

It is recommended to configure VLAN from config mode, as VLAN database mode is being deprecated.

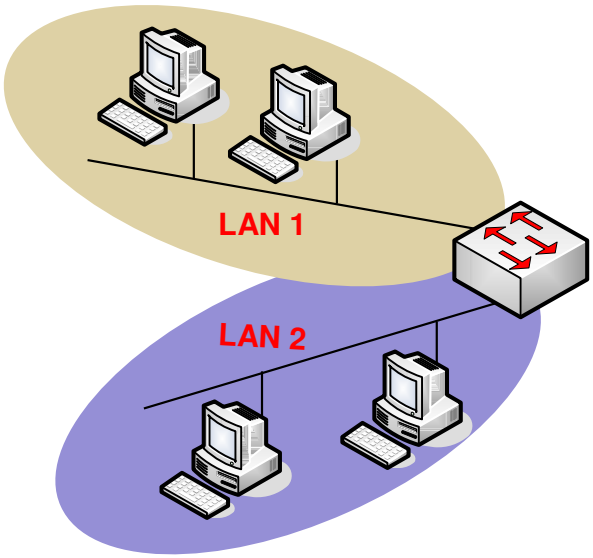
Comme dit plus haut ce mode est plus approprié d'après Cisco

Mode d'affectation

Vlan statique et de Niveau 1

2.2 Vlan dynamiques ou vlan de niveau 2 :

Appartenance par adresse MAC



Base de données

Vlan 1
00-B0-c2-17-f3-bf
00-07-cb-17-d4-c2
00-07-c3-24-53-b2

Vlan 2
00-07-1A-17-f3-ff
00-20-cb-57-d4-ba
00-04-76-24-53-b6

Quand un appareil arrive sur un réseau, le commutateur auquel il est connecté questionne une base de données sur le serveur de configuration de VLAN pour déterminer son appartenance à un VLAN.

Avantages :

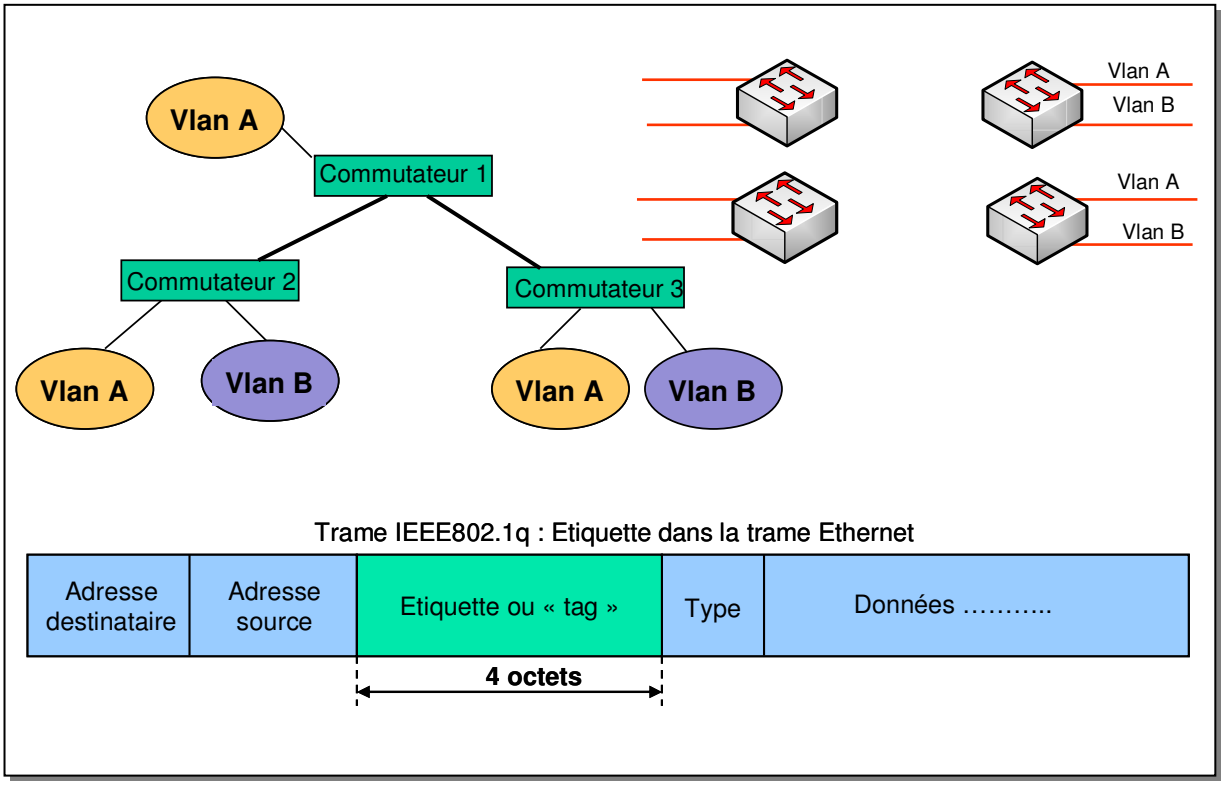
-
- Pas de brassage et changement dynamiques,
- Notification en cas d'utilisateur non reconnu,
-

Inconvénients :

- Base de données à maintenir,
- Charges supplémentaires sur les commutateurs et le réseau lors des échanges d'informations.

2.3 Agrégation de Vlan ou trunking :

2.3.1 Principe :



L'apparition de l'agrégation (trunking) remonte aux origines des technologies radio et de téléphonie. Dans les technologies radio, une agrégation est une ligne de communication simple qui transporte plusieurs canaux de signaux radio.

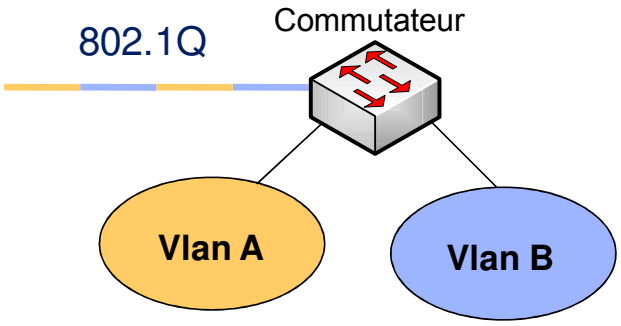
Pour les réseaux locaux, une **agrégation** est une connexion **physique** et **logique** entre deux commutateurs par lesquels le trafic réseau est acheminé. Cela consiste à mettre en œuvre un marquage dans la trame Ethernet.

Le standard IEEE 802.1P/Q définit la manière d'inscrire une étiquette dans la trame Ethernet de manière à reconnaître l'appartenance de celle-ci à un réseau local virtuel au niveau du port d'un commutateur.

2.3.1 Structure de la trame :

Champ	Fonction
Tag protocol identifier, TPID, EtherType : 12 bits	Utilisés pour identifier le protocole de la balise insérée. Dans le cas de la balise 802.1Q la valeur de ce champ est fixée à 0x8100.
Priority : 3 bits	Ce champ fait référence au standard IEEE 802.1P. Sur 3 bits on peut coder 8 niveaux de priorités de 0 à 7. La notion de priorité dans les VLANs est sans rapport avec les mécanismes de priorité IP. Ces 8 niveaux sont utilisés pour fixer une priorité aux trames d'un VLAN relativement aux autres VLANs.
Canonical Format Identifier : 1 bit	Ce champ assure la compatibilité entre les adresses MAC Ethernet et Token Ring. Un commutateur Ethernet fixera toujours cette valeur à 0. Si un port Ethernet reçoit une valeur 1 pour ce champ, alors la trame ne sera pas propagée puisqu'elle est destinée à un port «sans balise» (*untagged port*).
VLAN Identifier, vlan id, VID : 12 bits	Identifier le réseau local virtuel auquel appartient la trame.

2.3.1 Mise en œuvre :



Quelque soit l'équipement et son système d'exploitation :

1 : _____

2 : _____

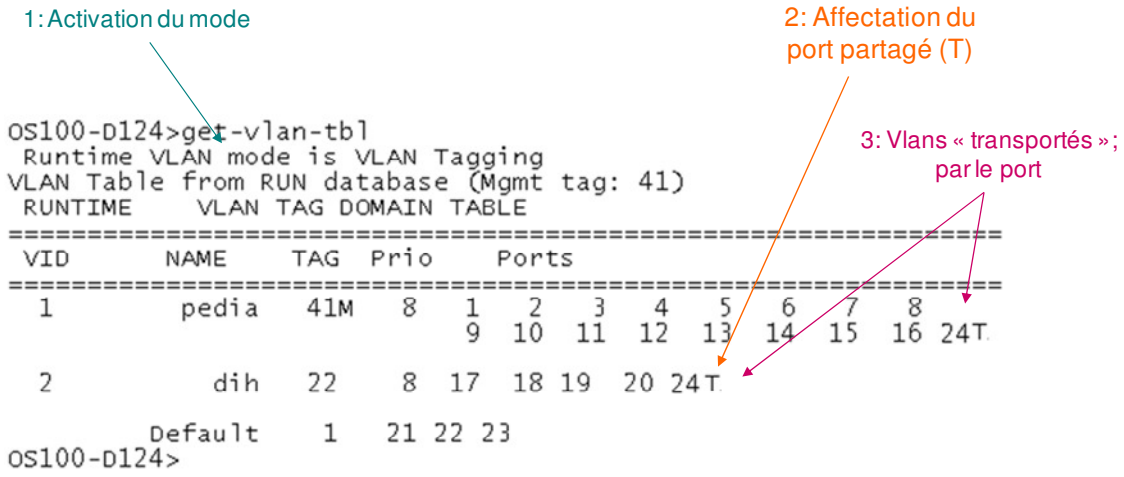
3 : _____

Attention : Le port du commutateur sur lequel est effectué l'agrégation devient alors un port partagé sur tous les vlan mais il ne transporte aucun Vlan tant que l'étape 3 n'est pas effectuée.

Chez Cisco :

```
Switch(config)#interface fa <num_int>
Switch(config-if)#description <lien vers....>
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan <ViD>
```

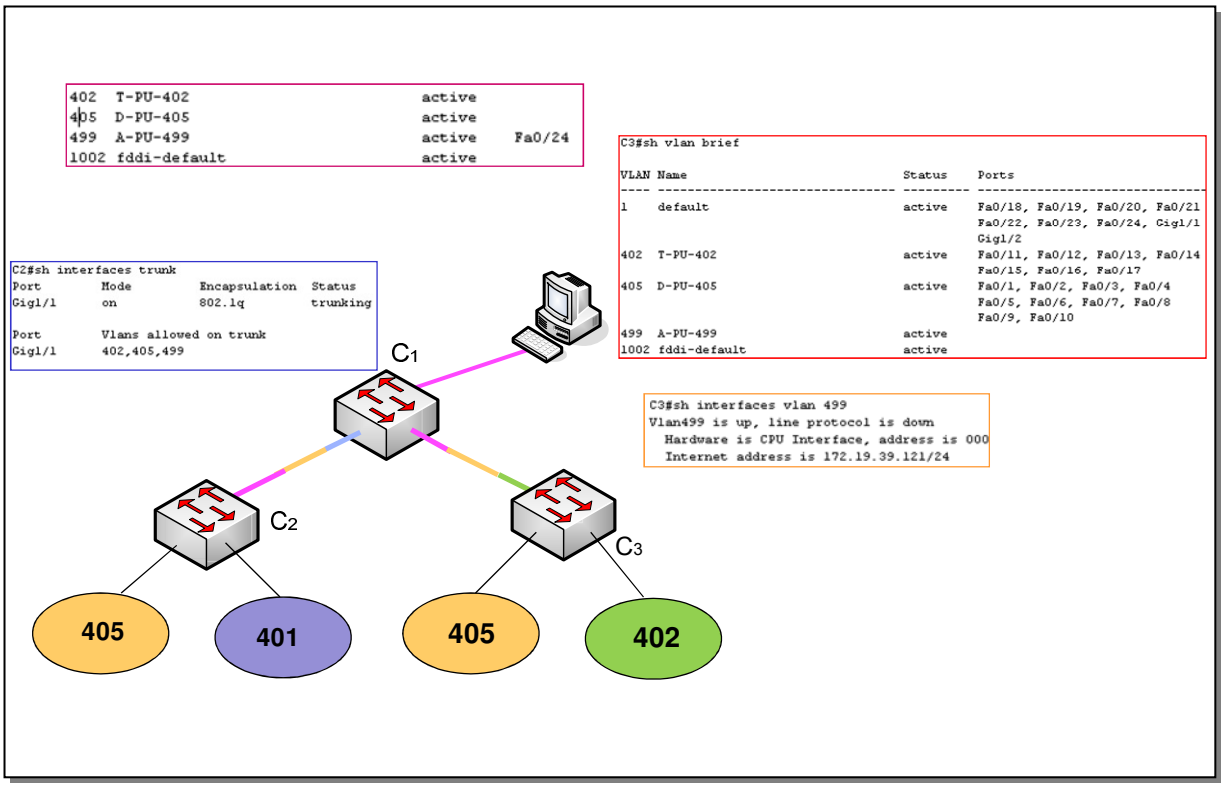
Chez un autre par exemple:



La mise en œuvre et les tests de l'agrégation de port sont abordés durant le TP.

2.4 Le réseau d'administration :

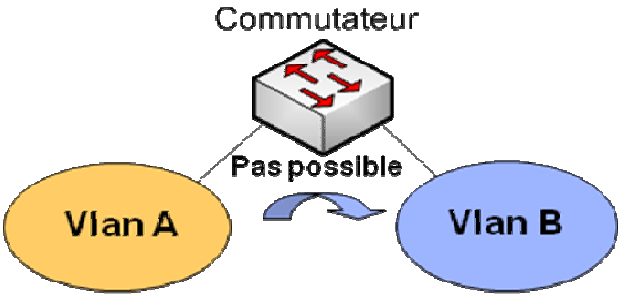
Un réseau d'administration est créée afin d'effectuer des opérations de maintenance ou de surveillance sur l'infrastructure de réseau. Il suffit ensuite de disposer d'une station de supervision et d'administration.



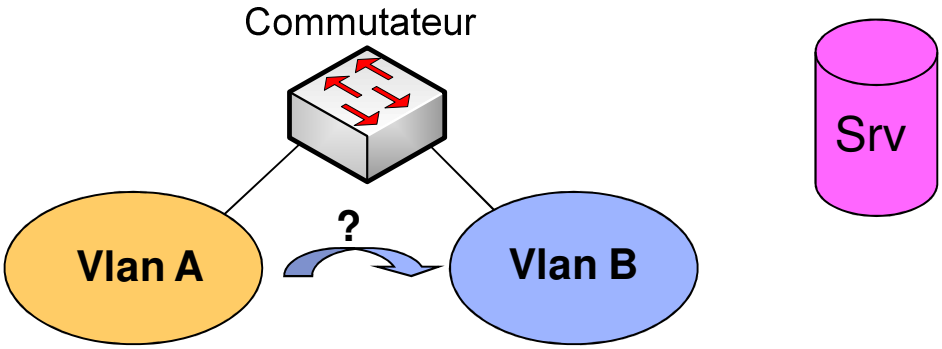
3. Le routage entre Vlan :

3.1 Quelle est la problématique ?

- Par le principe mise en œuvre nous n'avons aucune communication possible entre les vlan :



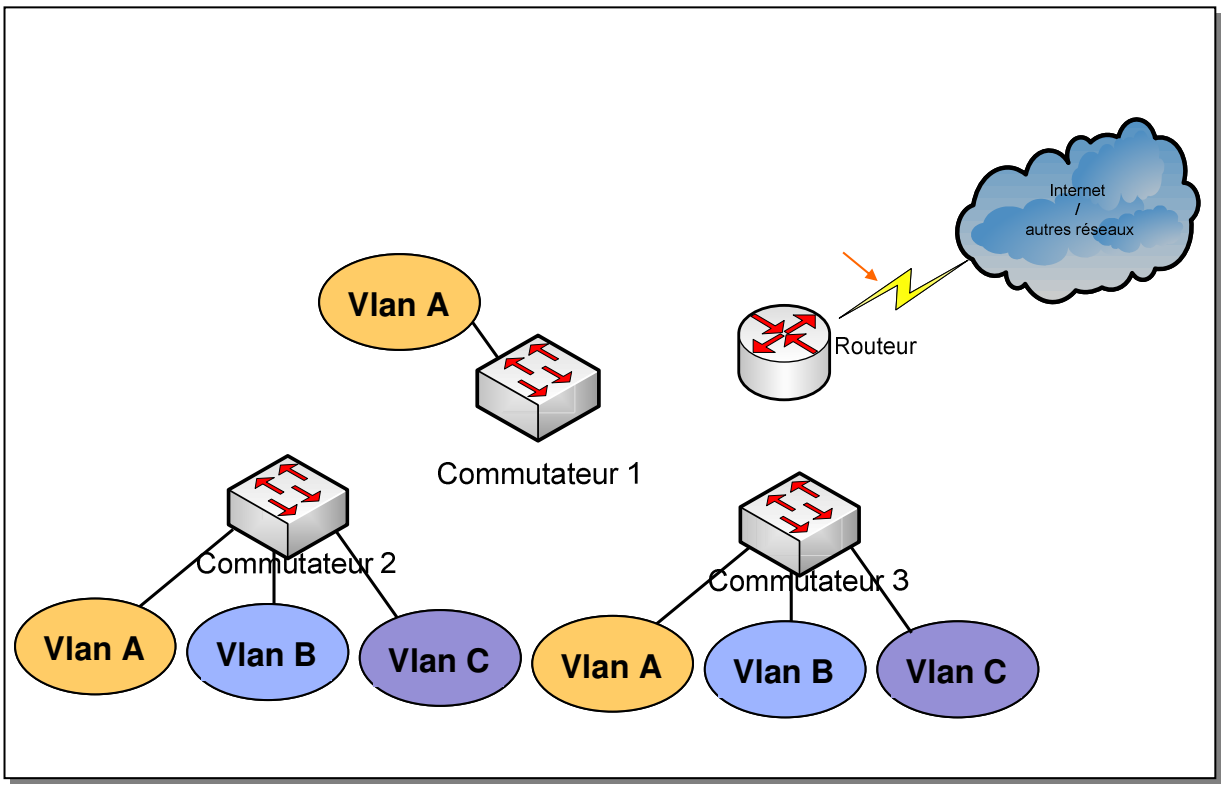
- Petit souci car dans un réseau nous avons des ressources commune entre les utilisateurs : accès internet, des serveurs ...



Cela reste une solution d'appoint car la communication entre Vlan reste impossible. C'est encore moins pratique pour les « gros » réseaux comme les réseaux de Campus.

- La solution ?
  -

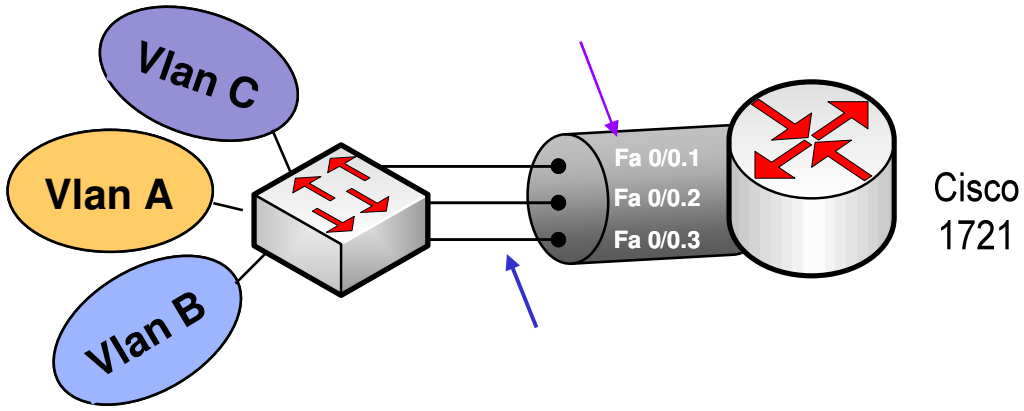
3.2 Routage des Vlan avec un routeur ou vlan de niveau 3 :



Attention tous les routeurs ne prennent pas en charge le standard IEEE 802.1Q. Avec les routeurs Cisco il faut être muni au minimum de la version 12.X et avoir suffisamment de mémoire vive !

On réalise alors des Vlan axés sur le protocole IP ou le sous réseau ou l'adressage que l'on appelle aussi Vlan de Niveau 3.

Exemple de configuration avec un routeur Cisco :



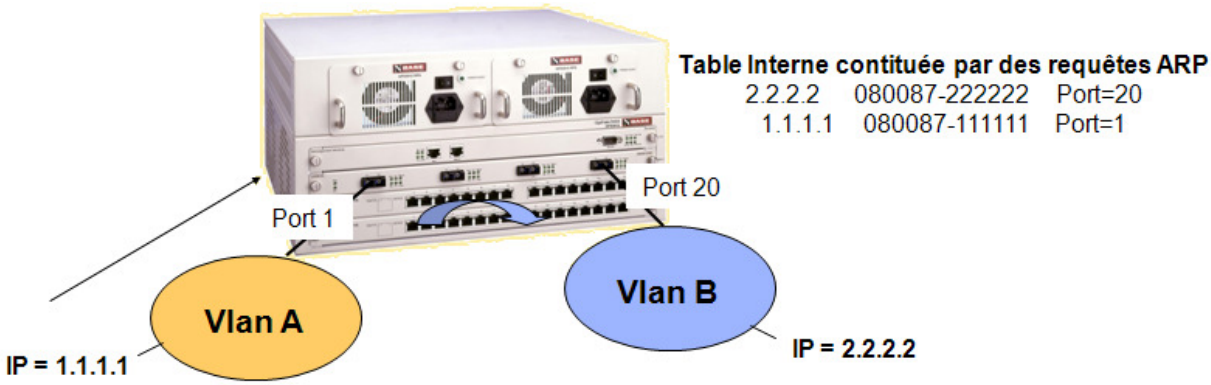

```
router#conf t

router(config)#interface FaEthernet 0/0
router(config-if)#no shutdown

router(config-subif)#
router(config-subif)#description vlan A TAG 10
router(config-subif)#
router(config-subif)#ip address <adresse_IP> <mask>
router(config-subif)#end
...
router#
```

3.3 Les commutateurs de Niveau 3:

La solution d'associer un routeur logiciel ou matériel à l'infrastructure reste chère et lente. Actuellement la solution est le mise en place des commutateurs de N3.

- Issus de la technologie des routeurs,
- Le routage est effectué par des Asics dédiés,
- Limitent les broadcasts aux sous-réseaux constitués (Vlan),
- Accélèrent le routage IP entre les sous-réseaux,
- Assurent la commutation Niveau 2 pour les autres protocoles,
- Assurent la conversion 10/100/1000 Mbps,

3.3.1 Cas N°1 : Solution propriétaire



- Une table interne associe : les adresses IP + les adresses Mac + le port concerné,
- Une trame entrante déclenche la consultation de la table IP,
- La trame est ensuite commutée vers le port associé,
- **Bénéfice : Rapidité car PAS de Routage Intra-Subnet !!!**

Exemple de configuration avec un commutateur Cisco :

Trois étapes:

1. Création des Vlans comme avec les commutateurs de N2
2. Affectation des Adresses IP au Vlan <ViD>

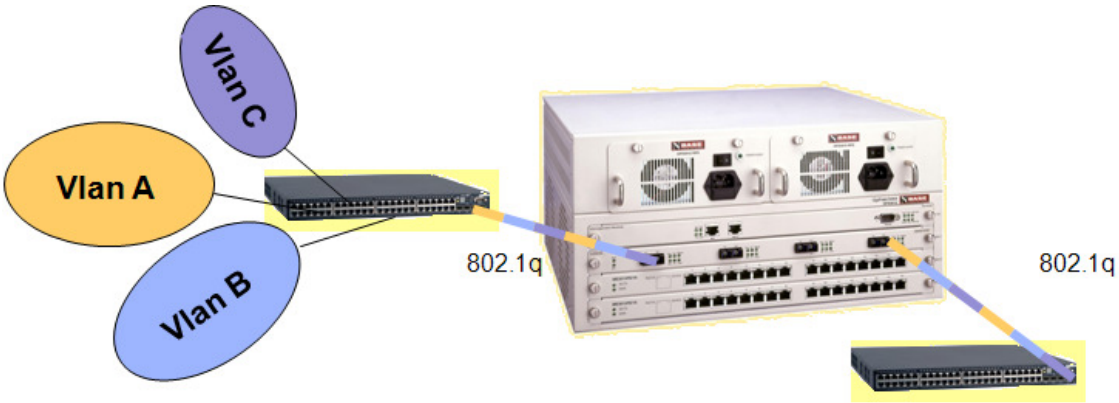
```
Switch(config)#interface vlan <Vid>
Switch(config-if)#ip address <addr> <mask>
Switch(config-if)#no shutdown
```

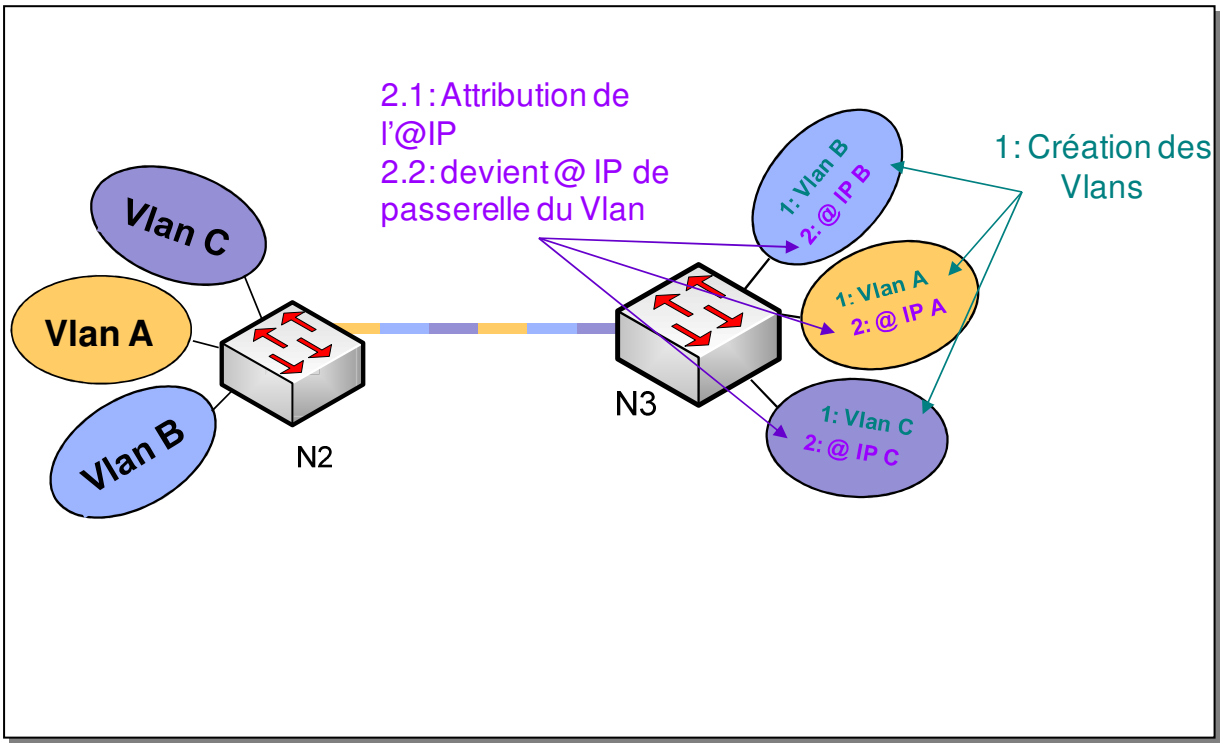
…….

```
Switch(config-if)#sh ip route
```

3.3.2 Cas N°2 : Solution 802.1q

- Le commutateur Niveau 3 doit savoir lire le champ de 4 octets.





Trois étapes:

1. Création des Vlans comme avec les commutateurs de N2
2. Affectation des Adresses IP au Vlan <ViD>
3. Sur l'interface du port trunck

```
Switch(config)#interface Ga <num_int>
Switch(config-if)#description <lien vers....>
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan <ViD>
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#end
```

3.3.3 Cas N°3 : Solution dynamique

- Le commutateur Niveau 3 utilise des protocoles de routage dynamique RIPv1-v2/OSPF,
- Les Vlan IP sont automatiquement constitués en lisant l'adresse source IP,
- Les tables de routage hardware sont constituées automatiquement,
- Le routage s'effectue comme dans un routeur traditionnel.

3.4 Listes d'accès de contrôle d'accès :

Par définition un routeur route. Donc il va transmettre tous les paquets échangés entre les Vlan. Chaque groupe d'utilisateur n'est plus isolé la sécurité n'est plus assurée.

Le réseau d'administration n'est lui aussi plus isolé. La solution ?

Les listes de contrôle d'accès (ACL : Access Control List) qui établissent des règles de pare feu au sein des commutateurs de N3. *L'analyse d'une ACL est abordée durant le TP.*

4. Les Protocoles VRRP ou HSRP :

4.1 Etats des lieux dans les réseaux ?

Dans les réseaux actuels nous avons beaucoup de Vlans N3 :

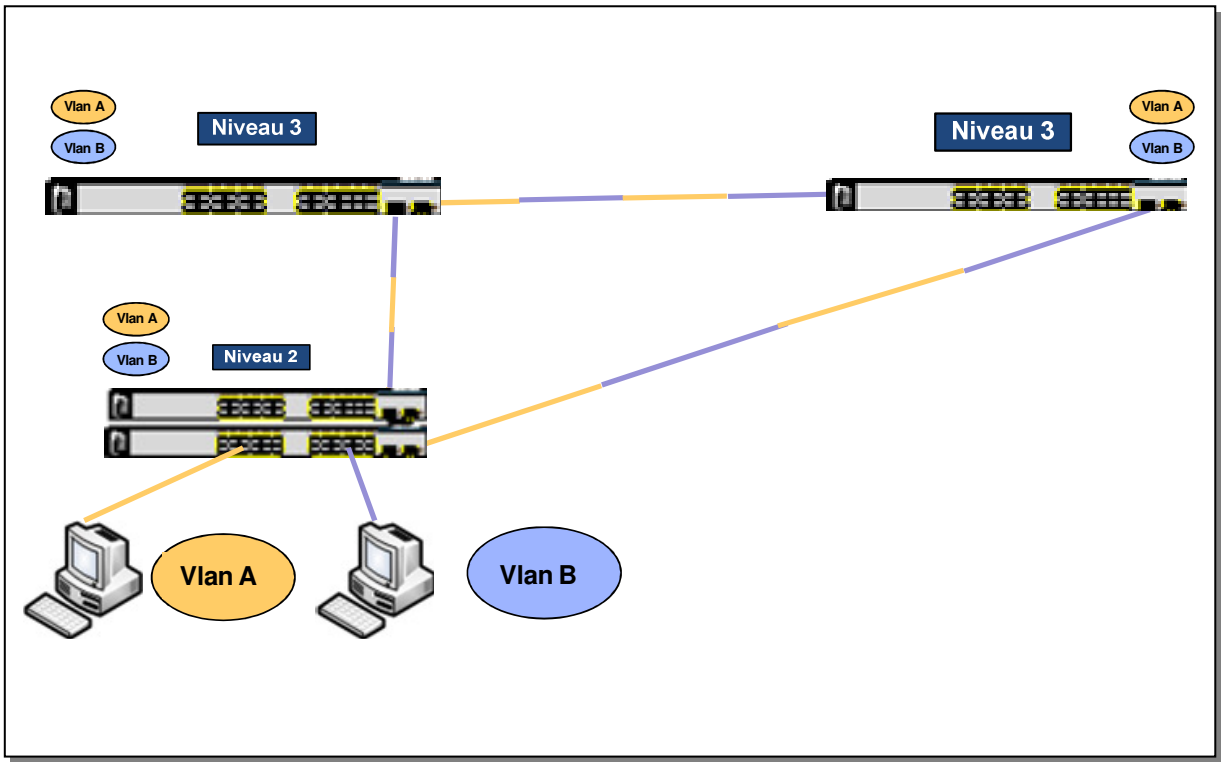
- Mais pourquoi?
  -
  -
  -
- En aucun cas, un client ne doit pas être en mesure de ne pas sortir de son domaine de broadcast pour atteindre une ressource
- Mise à part l'adresse IP de destination, quels sont les 2 paramètres réseau que doit avoir un client pour communiquer avec une ressource d'un réseau étendu?
  -
  -

Les réseaux actuels c'est aussi de la haute disponibilité avec de la redondance :

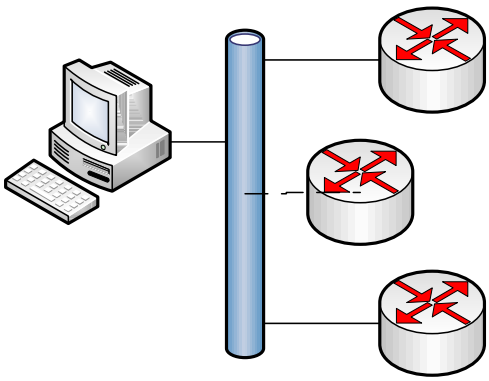
- De liens,
- D'alimentations,
- D'équipements de N2,
- D'équipements de N3.
  - Pb sur un même réseau possibilité d'avoir 2 routeurs!!!!!
  -

4.2 Présentation des protocoles :

Pour répondre à ce besoin le standard Virtual Router Redundancy Protocol est né suite au développement du protocole propriétaire Cisco Hot Standby Router Protocol. En effet ils permettent la mise en place d'un système de redondance des routeurs afin que le trafic soit toujours assuré même en cas de panne d'un routeur.



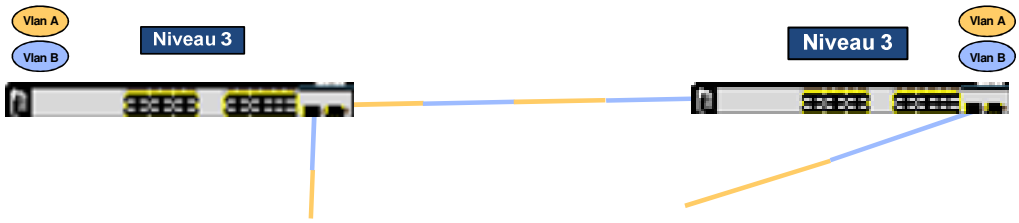
Le schéma ci-dessous peut être équivalent à la représentation logique :



Combien d'adresses IP faudra t-il avoir de disponibles dans le réseau pour adresser correctement ces passerelles ?

_____

4.3 Fonctionnement :

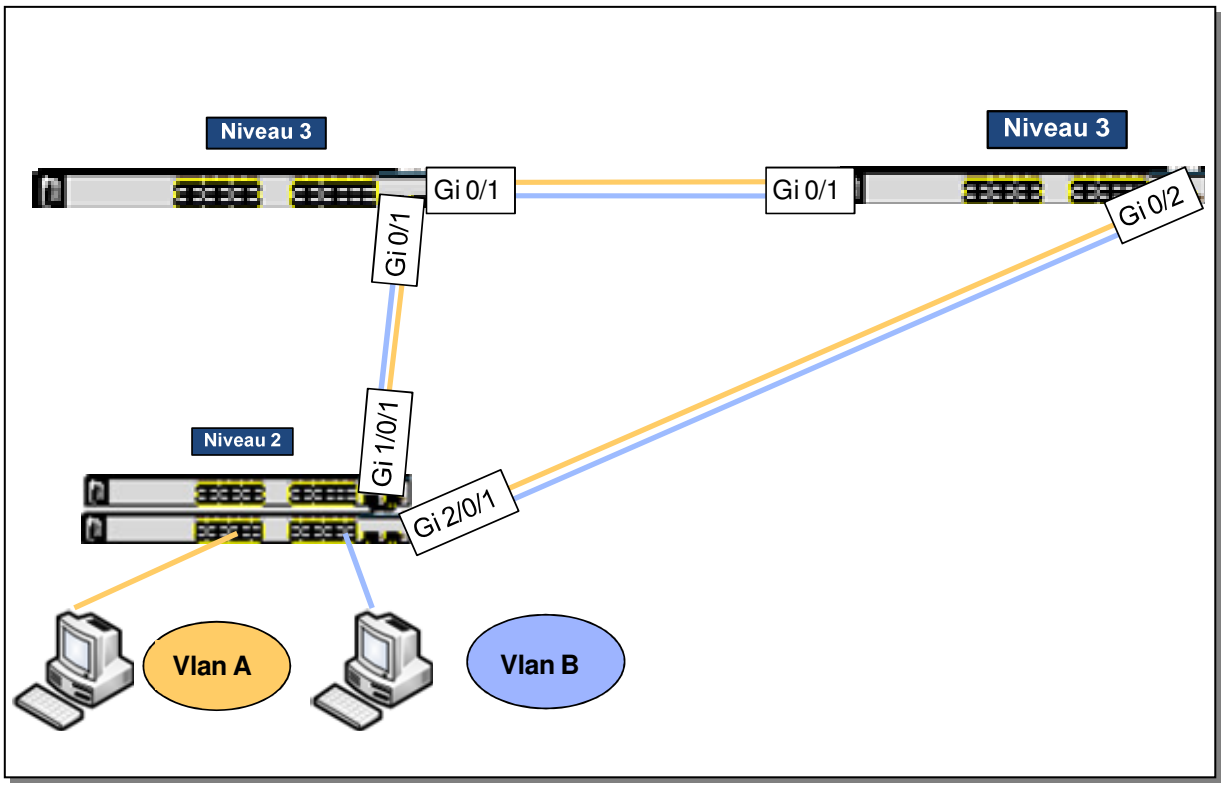


Group = 0 est une valeur réservée,

Group = 255 est pour le cas particulier ou il ne reste que deux adresses IP disponibles sur le sous réseau. L'adresse IP virtuelle est alors aussi une adresse IP réelle.

Une fois configurés les deux routeurs s'échangent des paquets « HELLO » à intervalles de temps réguliers (Hellotime pour HSRP). C'est-à-dire que le routeur en standby envoie ces paquets et tant que le routeur Master répond dans un délai imparti (Holdtime pour HSRP) il reste inactif.

4.4 Répartition de charge :



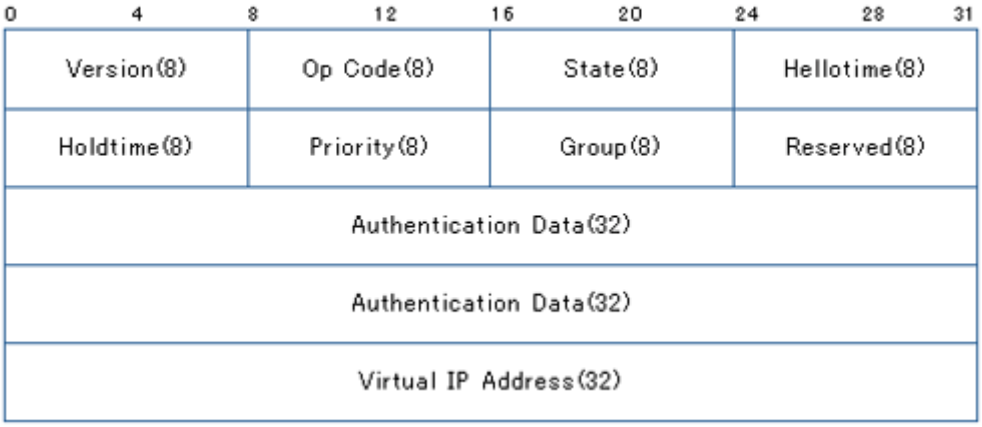
4.5 Paramétrage HSRP :

```
switch #
switch#conf t
switch(config)#interface vlan <ViD>
switch(config-if)#standby ?
  <0-255>          group number
  authentication   Authentication
  delay            HSRP initialisation delay
  ip               Enable HSRP and set the virtual IP address
  name             Redundancy name string
  preempt          Overthrow lower priority Active routers
  priority         Priority level
  redirect         Configure sending of ICMP Redirect messages with an
                   HSRP virtual IP address as the gateway IP address
  timers           Hello and hold timers
  track            Priority tracking
  version          HSRP versionswitch(config-if)#standby

switch(config-if)#standby ?
```

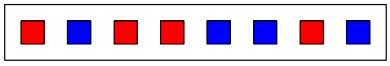
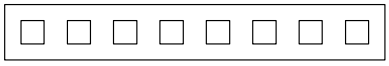
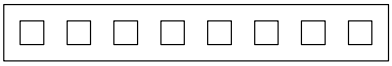
4.6 Structure des paquets HSRP :

Les routeurs appartenant à un même groupe HSRP communiquent via le port 1985 en UDP par multicast (224.0.0.2), ils échangent des paquets ayant pour adresse source leurs adresses physiques.

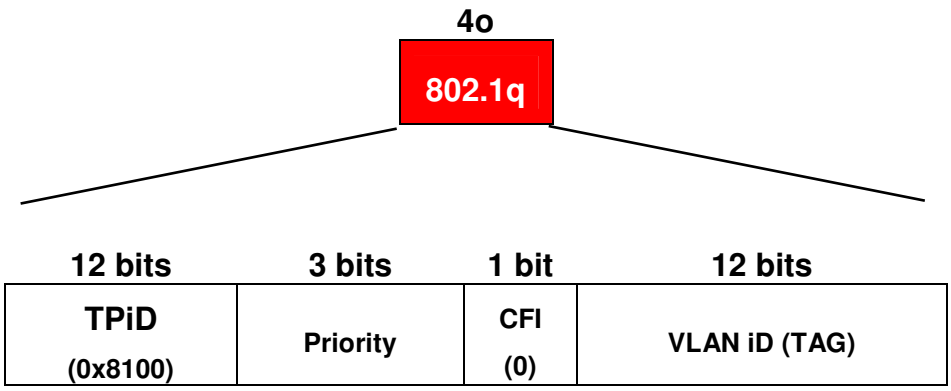
RFC : 2281



5. En Résumé :

VLAN de niveau 1	VLAN de niveau 2	VLAN de niveau 3
Groupement de segments ou groupement de ports	Groupement selon les adresses MAC	Groupement de selon des informations de niveau 3 (adresses IP, protocoles)
 VLAN 2 : ports 1, 3, 4, 7 VLAN 3 : ports 2, 5, 6, 8	 VLAN 2 : 02:25:DE:78:AD:2C 08:00:23:CB:23:47 03:24:55:ABCE:A7 VLAN 3 : 00:15:00:37:9A:DA 00:15:F2:38:2C:DC 02:BC:2D:AB:02:3E	 VLAN 2 : sous-réseau 134.157.4.0 VLAN 3 : sous-réseau 134.157.8.0

et :



Le principal avantage :

Ils permettent à l'administrateur réseau d'organiser le LAN de manière logique et non physique. Cela signifie qu'un administrateur peut effectuer toutes les opérations suivantes:

-
-
-
-
-