Les Réseaux Locaux virtuels (Vlan)

J BLANC

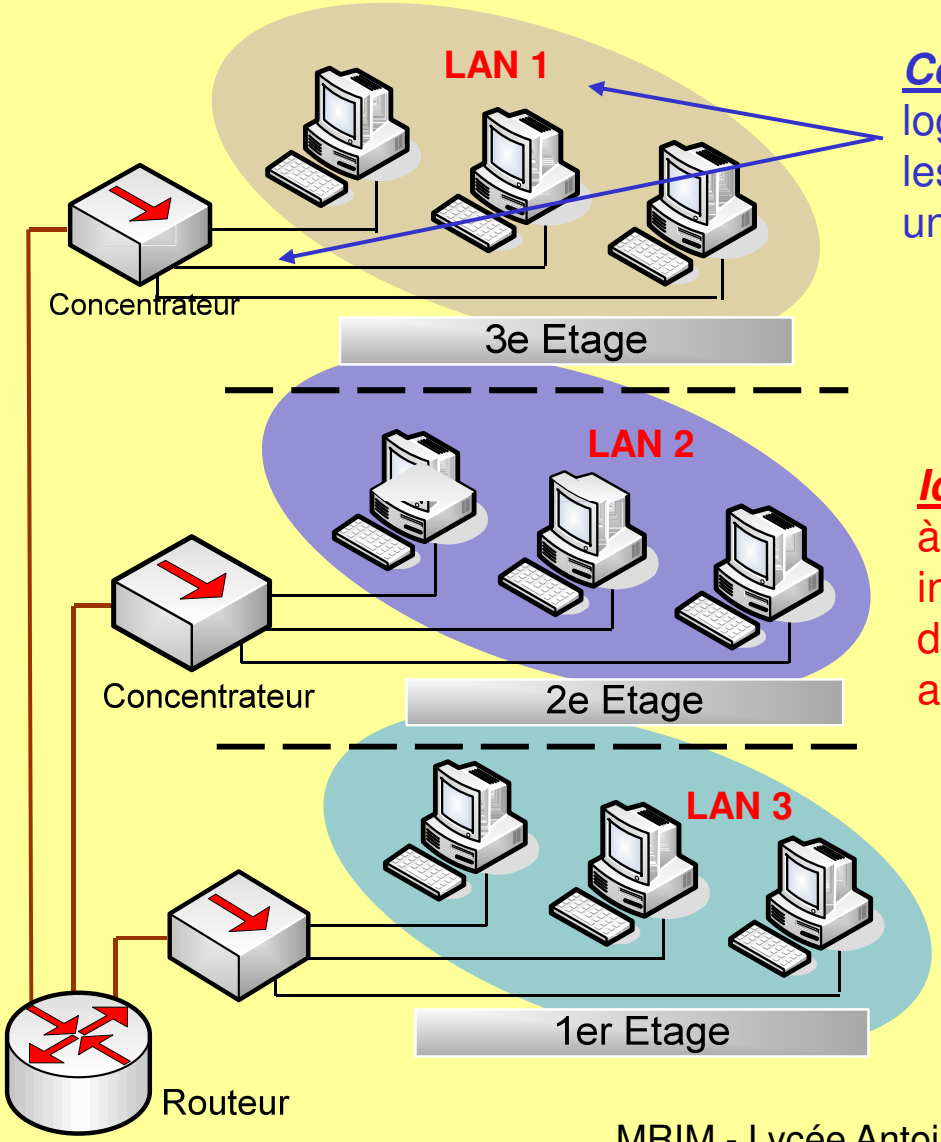
But:

- Comprendre le fonctionnement des Vlans afin d'intervenir sur le réseau du CHU pour assurer la mise en service ou la maintenance.
- Bibliographie:
  - CCNA Cisco,
  - http://computer.howstuffworks.com/lan-switch17.htm
  - Documentations constructeurs
- Merci à:
  - T.Calmont Technicien mise en œuvre pour son support technique et la relecture,
  - F.Beunier (MRV.com) et D.Nogueira (dynetcom) pour leur support technique.

Plan

- Le concept des Vlans
- Les Vlans de Niveau 1 et 2
  - Les vlan statiques,
  - Les vlan dynamiques,
  - L'agrégation de Vlan,
  - Le réseau d'administration,
- Le routage des vlan.
  - Le tout avec:
    - 2 TP
    - 1 ou 2 TD

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.

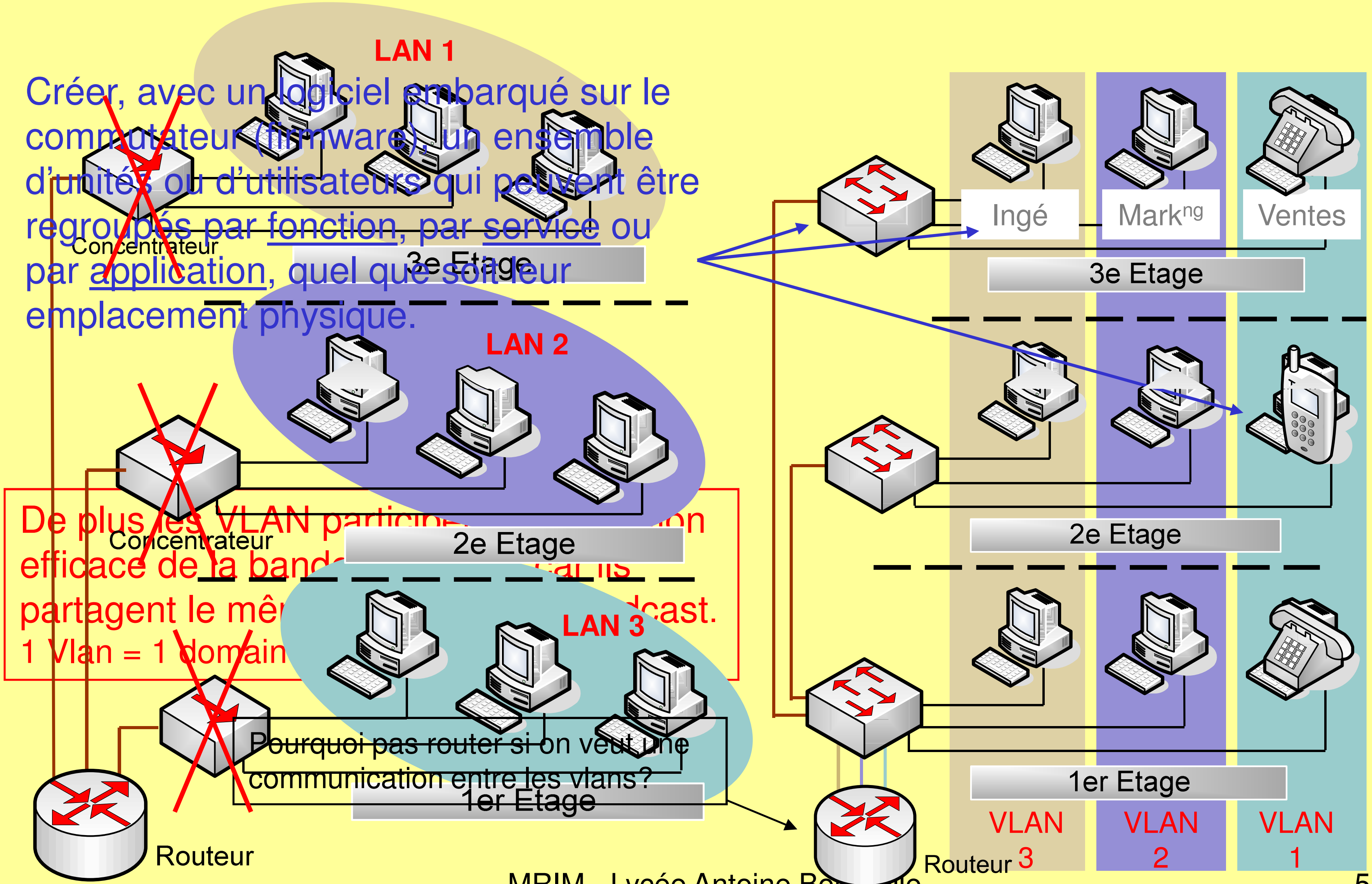
Idée **:** rajouter de l'informatique de telle sorte à obtenir des topologies physique et logique indépendantes tout en conservant des domaines de broadcast suffisamment petits afin de garantir la bande passante.

Segmentation avec des Vlans

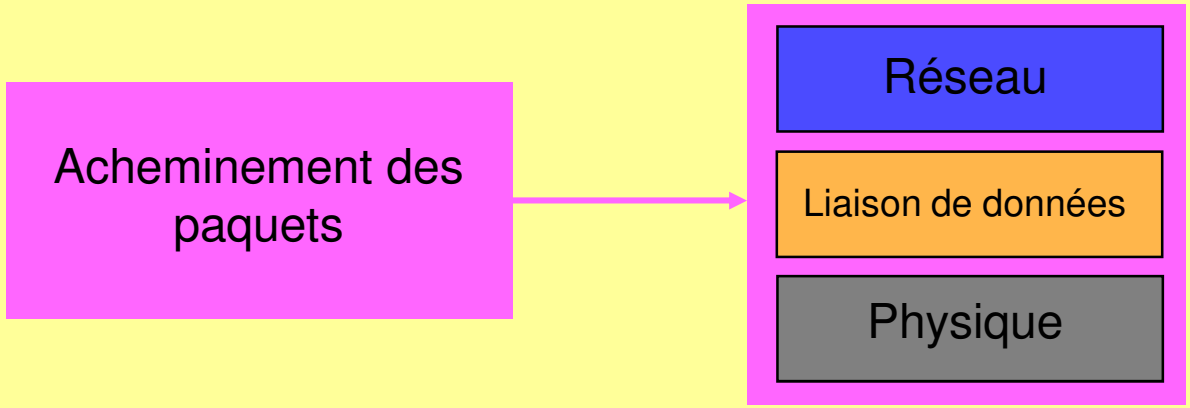
Créer, avec un logiciel embarqué sur le commutateur (firmware), un ensemble d'unités ou d'utilisateurs qui peuvent être regroupés par fonction, par service ou par application, quel que soit leur emplacement physique.

De plus les VLAN particip ... ion
efficace de la band ... car ils
partagent le mê ... dcast.
1 Vlan = 1 domain

Pourquoi pas router si on veut une communication entre les vlans?

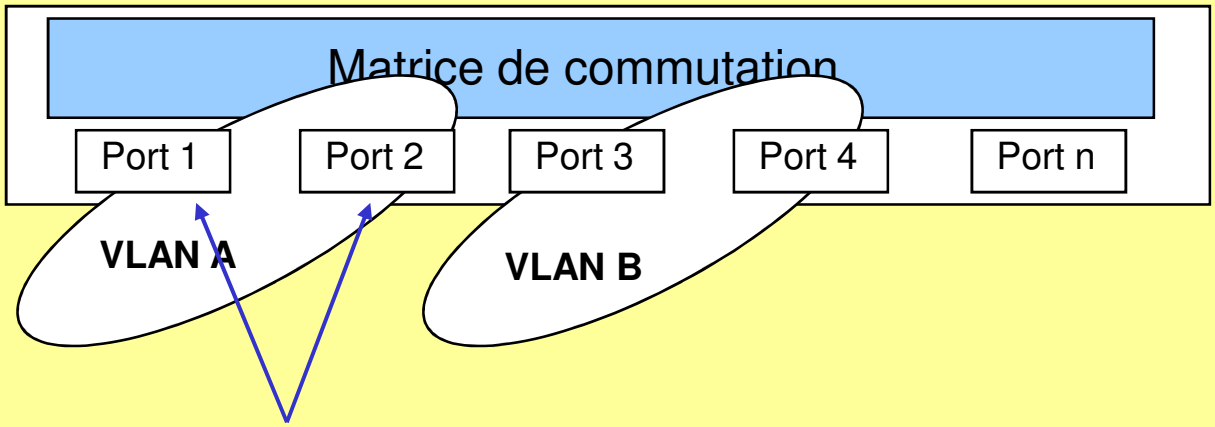


Modèle OSI



- 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 locaux virtuels doit être faite à travers ces 3 niveaux du modèle.
- On parle alors de Vlan de Niveau 1, 2 ou 3.
- Avant tout? 1 rappel sur le principe de fonctionnement d'un commutateur et ses caractéristiques.

Vlan Statiques

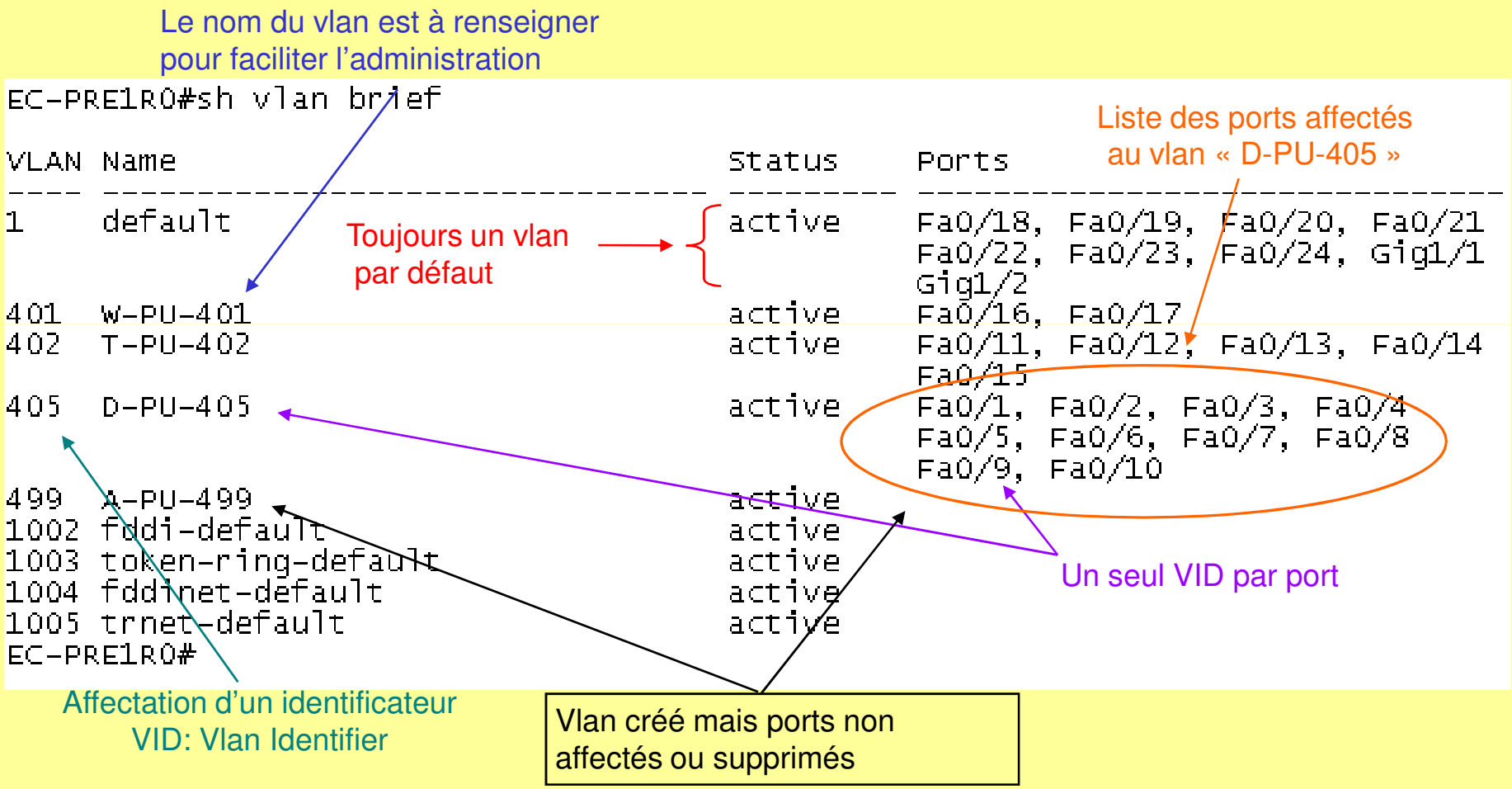


Chaque port du commutateur est attribué à un LAN virtuel différent et partagent les broadcasts.

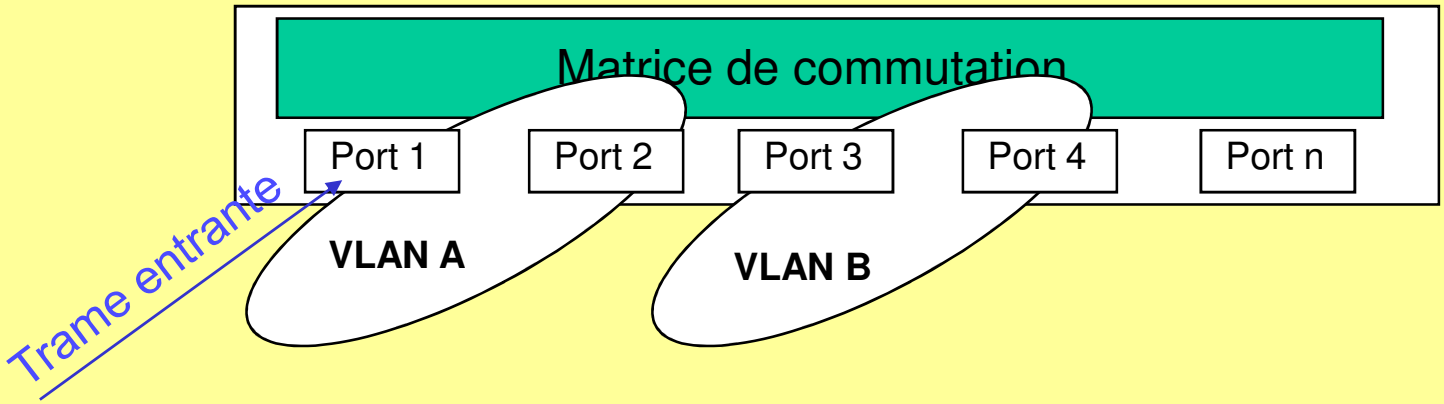
- Les Vlan statiques sont axés sur une segmentation par ports, on parle alors de vlan de niveau 1.

Fonctionnement 1/2:

Principe de la construction d'une table:



Fonctionnement 2/2:

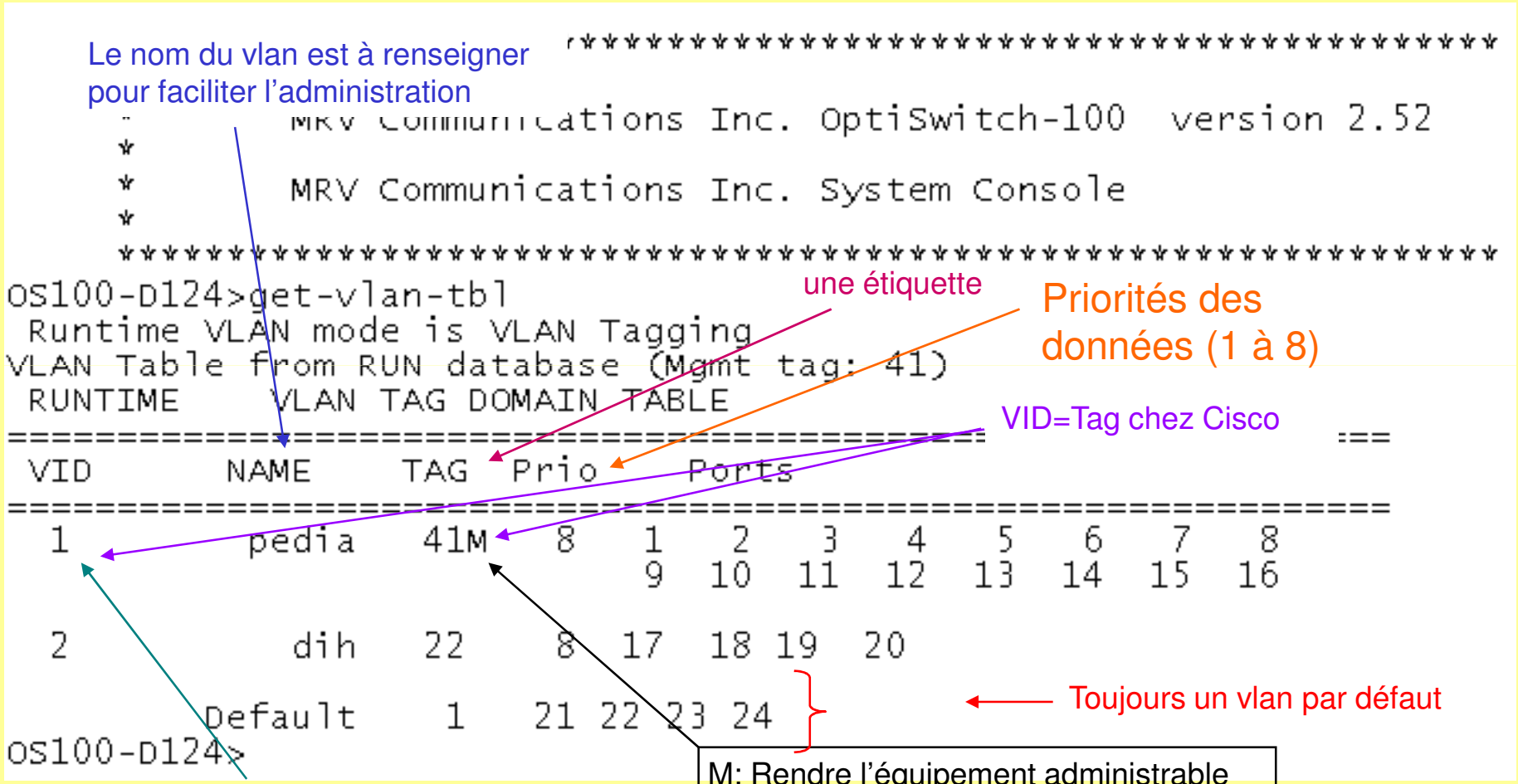


- ***Que fait alors le commutateur lorsqu'il reçoit une trame sur un de ses ports ?***
  - Le commutateur analyse le VID du port sur lequel il reçoit la trame,
  - Il analyse ensuite la trame et détermine grâce à l'adresse MAC destination sur quel port il doit envoyer la trame,
  - Il analyse ensuite le VID du port destination et le compare au premier VID,
  - Si les VID sont identiques ainsi que le nom, la trame circule librement sinon elle est détruite.

Avantages / Inconvénients

- **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).
- **Inconvénients** *:*
  - Bien que l'on puisse administrer à distance cela nécessite un brassage et un repérage des ports sur le commutateur (statique).
- ***La mise en œuvre et les tests des vlans statiques seront abordés durant le TP.***

Autre exemple :



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.

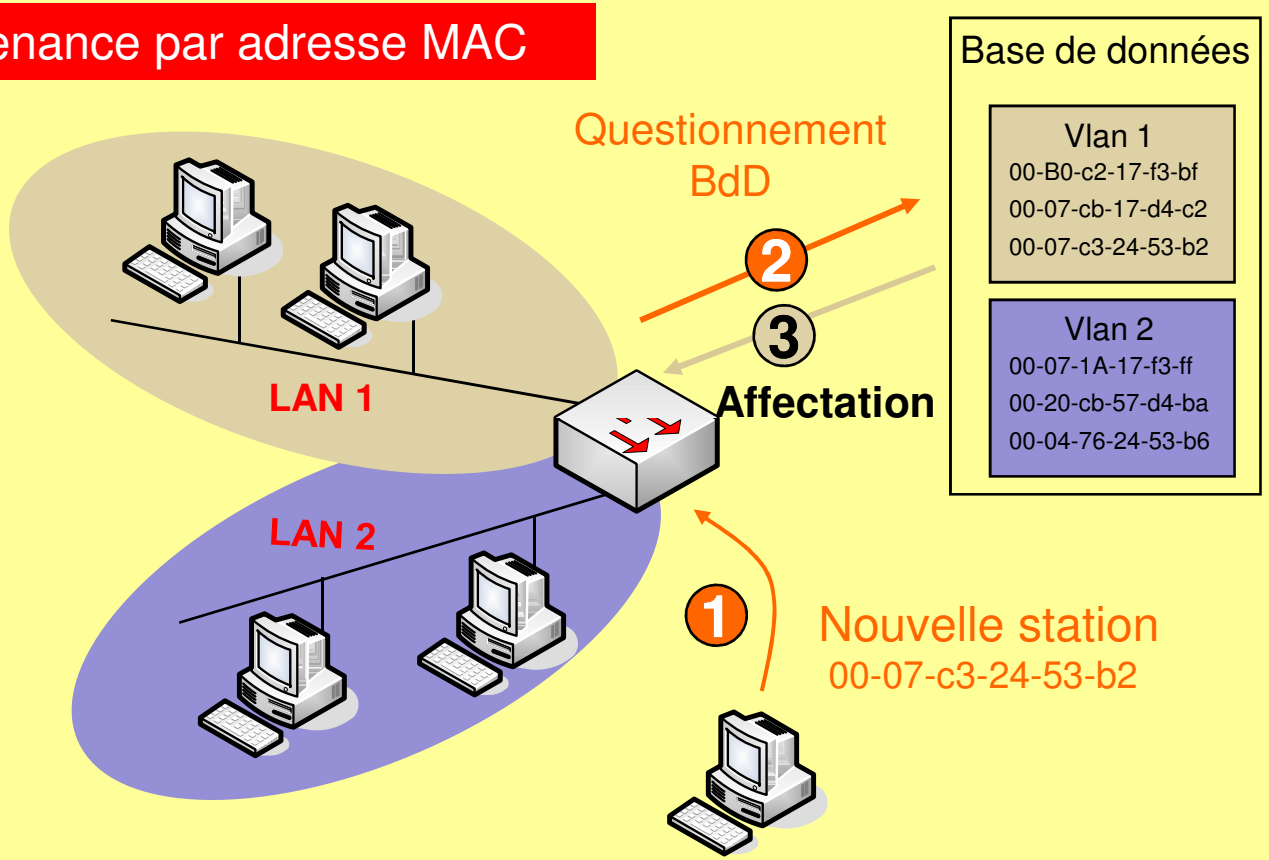
Comme dit plus haut ce mode est plus approprié d'après Cisco

Mode d'affectation

Vlan statique et de Niveau 1

Vlan dynamiques :

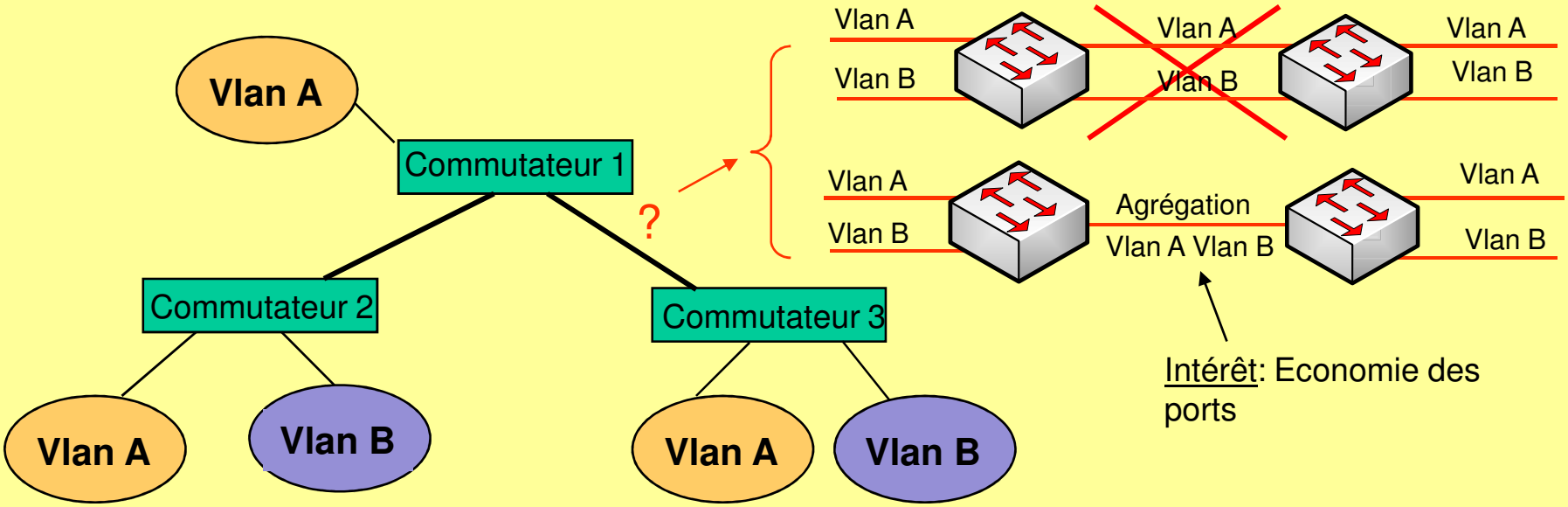
Appartenance par adresse MAC



Vlan dynamique

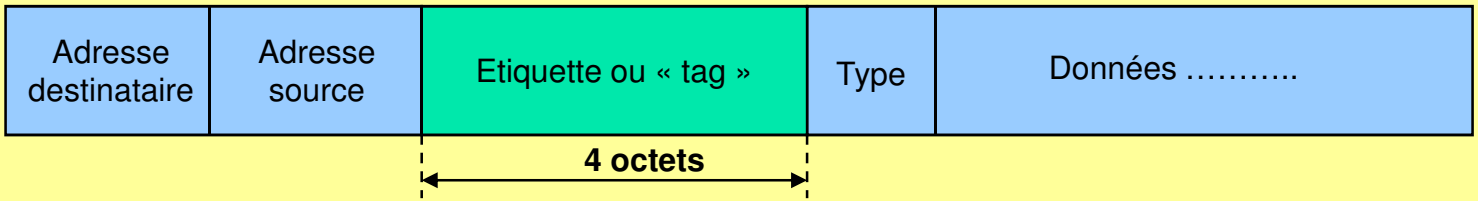
- ***Avantages :***
  - Administration centralisée,
  - Pas de brassage et changements dynamiques,
  - Notification en cas d'utilisateur non reconnu,
  - Prise en charge facile des utilisateurs mobiles.
- ***Inconvénients :***
  - Base de données importantes à maintenir,
  - Charges supplémentaires sur les commutateurs et le réseau lors des échanges d'informations.

Agrégation de vlan ou trunking :



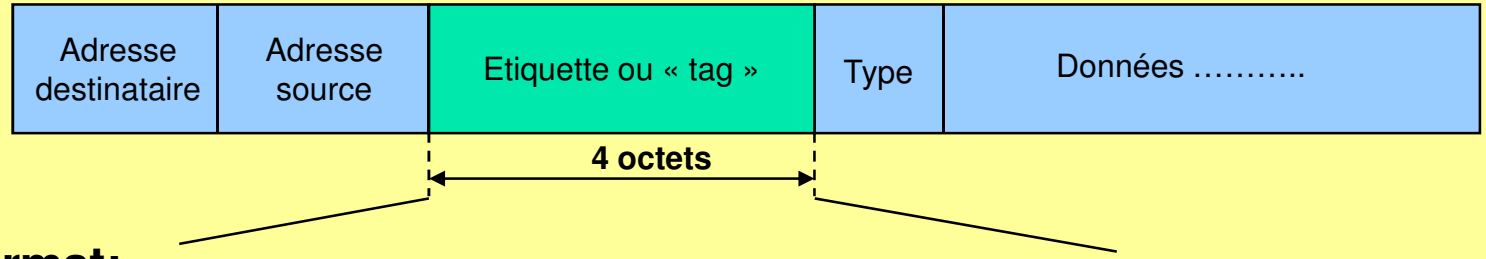
- ***Comment?***

Trame IEEE 802.1q : Etiquette dans la trame Ethernet



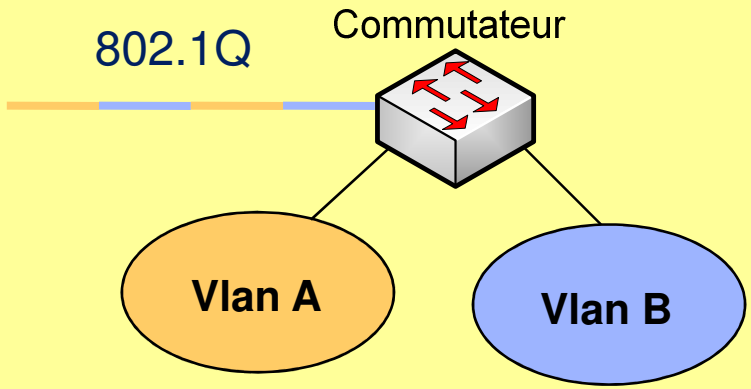
- ***Ce standard définit la manière d'inscrire une étiquette dans la trame Ethernet de manière à reconnaître l'appartenance de celle-ci à un réseau local virtuel au niveau du port d 'un commutateur***

Le standard I.E.E.E 802.1 q



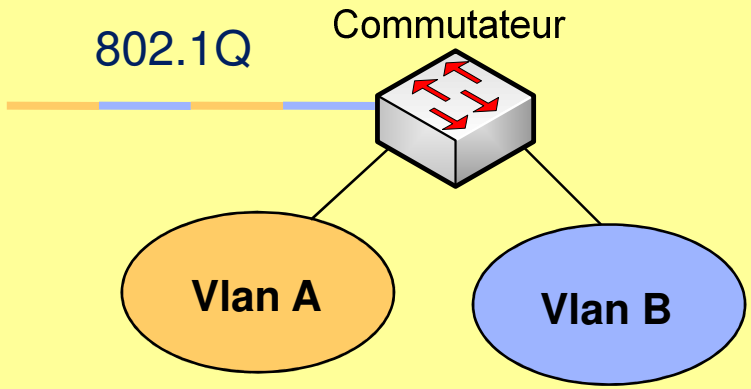
- **Format:**
  - **Tag protocol identifier, TPID, EtherType** : 12 bits
    - Utilisés pour identifier le protocole de la balise insérée. Dans le cas de la balise 802.1Q la valeur de ce champ est fixée à 0x8100.
  - **Priority : 3 bits**
    - Ce champ fait référence au standard IEEE 802.1P. Sur 3 bits 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.
- **Attention** : Le port du commutateur sur lequel est effectué l'agrégation devient alors un port partagé sur tous les vlan. Sur certain commutateur il faut le **spécifier**.

Mise en Pratique de l'agrégation:



- Quelque soit l'équipement et son système d'exploitation :
  1. Il faut activer le mode 802.1q,
  2. Affecter un port commun
  3. Annoncer les vlans transportés par le port commun.
- **Attention** : Le port du commutateur sur lequel est effectué l'agrégation devient alors un port partagé sur tous les vlans, mais il ne transporte aucun Vlan tant que l'étape 3 n'est pas effectuée.

Mise en Pratique de l'agrégation:



Mode d'affectation

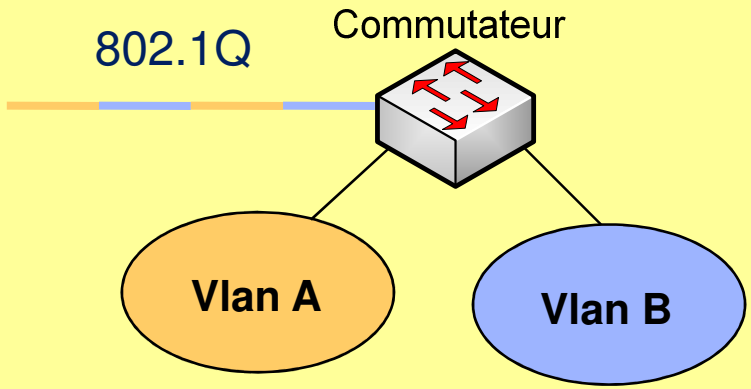
Attention danger!!!!
Transporte tous les Vlans par défaut

Vlans « transportés »; pour une série: 305-310 (305 à 310 par ex)

- Chez Cisco:
  - Configuration basique

```
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>
```

Mise en Pratique de l'agrégation:



- Chez MRV:

1: Activation du mode

2: Affectation du port partagé (T)

3: Vlans « transportés »; par le port

```
OS100-D124>get-vlan-tbl
 Runtime VLAN mode is VLAN Tagging
VLAN Table from RUN database (Mgmt tag: 41)
 RUNTIME     VLAN TAG DOMAIN TABLE
=============================================================
 VID       NAME     TAG  Prio     Ports
=============================================================
  1          pedia    41M    8    1   2   3   4   5   6   7   8
                                   9  10  11  12  13  14  15  16 24T

  2            dih    22     8   17  18 19  20 24T

           Default     1    21 22 23
OS100-D124>
```

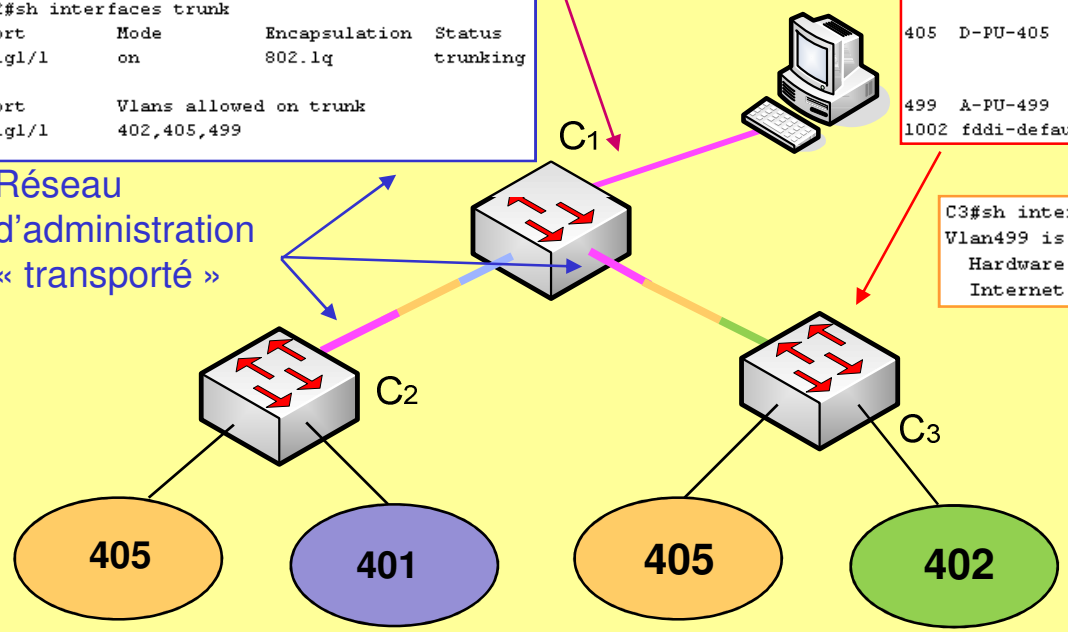
Un réseau d'administration

```
402   T-PU-402                         active
405   D-PU-405                         active
499   A-PU-499                         active     Fa0/24
1002  fddi-default                     active
```

Un port sur l'infrastructure dédié à l'administration

```
C2#sh interfaces trunk
Port        Mode         Encapsulation  Status
Gig1/1      on           802.1q         trunking

Port        Vlans allowed on trunk
Gig1/1      402,405,499
```

Réseau d'administration « transporté »



La table des vlans

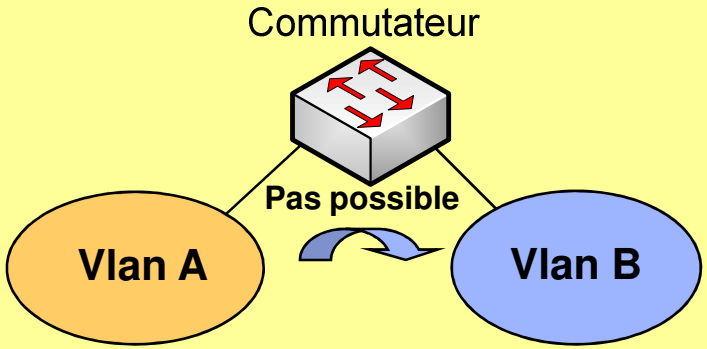
```
C3#sh vlan brief

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
402  T-PU-402                         active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17
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
```

```
C3#sh interfaces vlan 499
Vlan499 is up, line protocol is down
  Hardware is CPU Interface, address is 000
  Internet address is 172.19.39.121/24
```

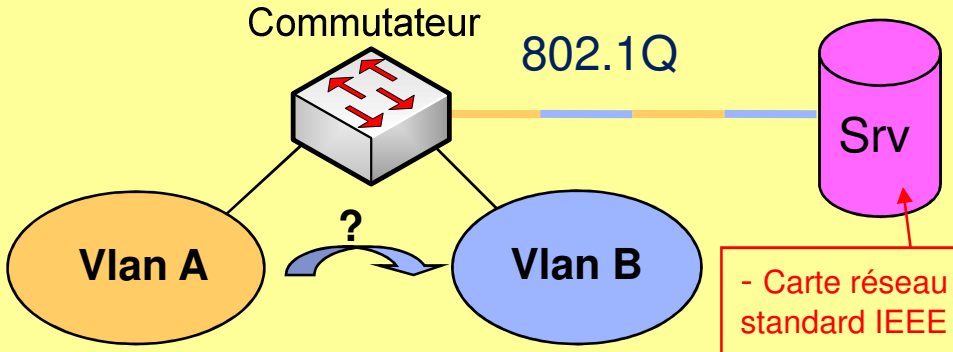
Pas de port mais une adresse IP sur l'interface logicielle « vlan 499 » pour dialoguer

Le routage entre les Vlans : quelle est la problématique?

- Par le principe mise en œuvre aucune communication n'est possible entre les Vlan



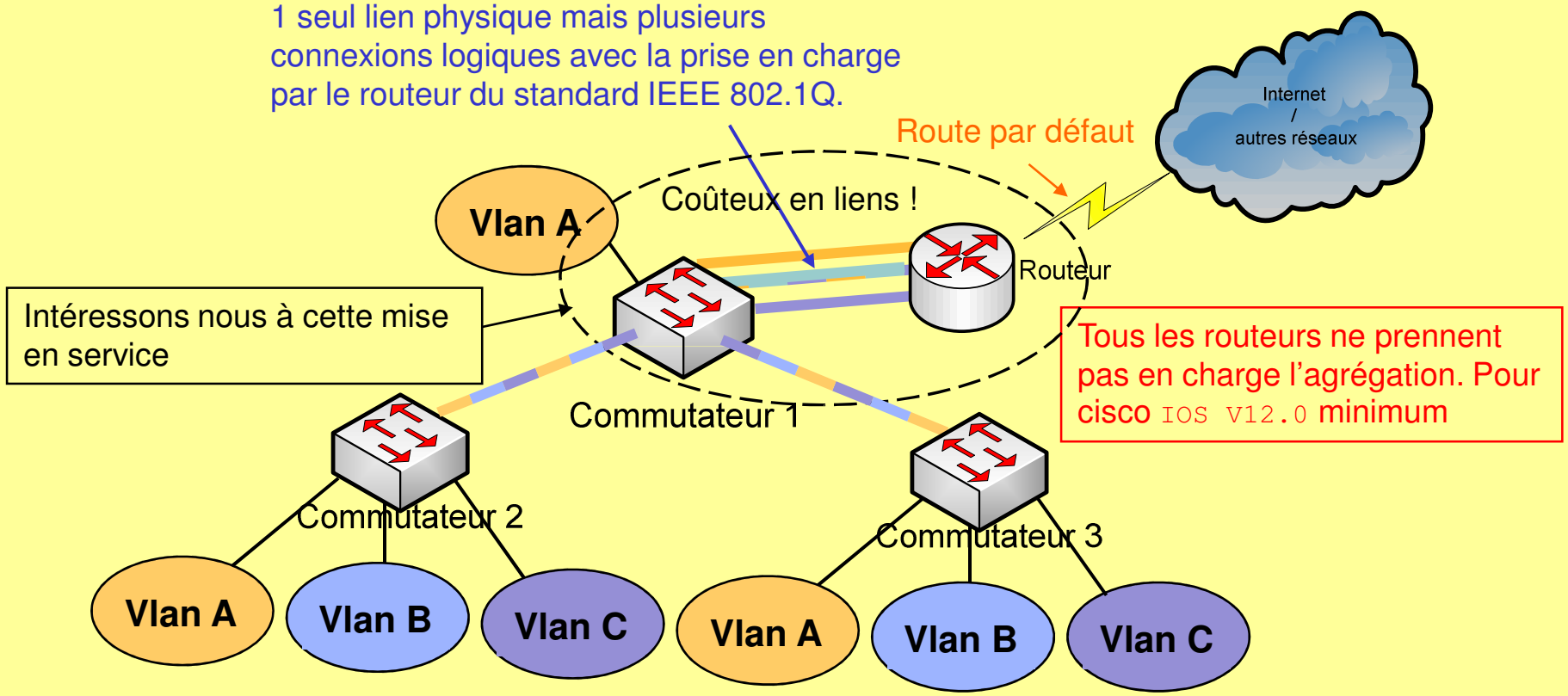
- Ressources communes? Ex: Accès Internet, serveurs....



- Carte réseau prenant en charge le standard IEEE 802.1Q
- Définir plusieurs adresses IP si plan d'adressage différent d'un vlan à l'autre

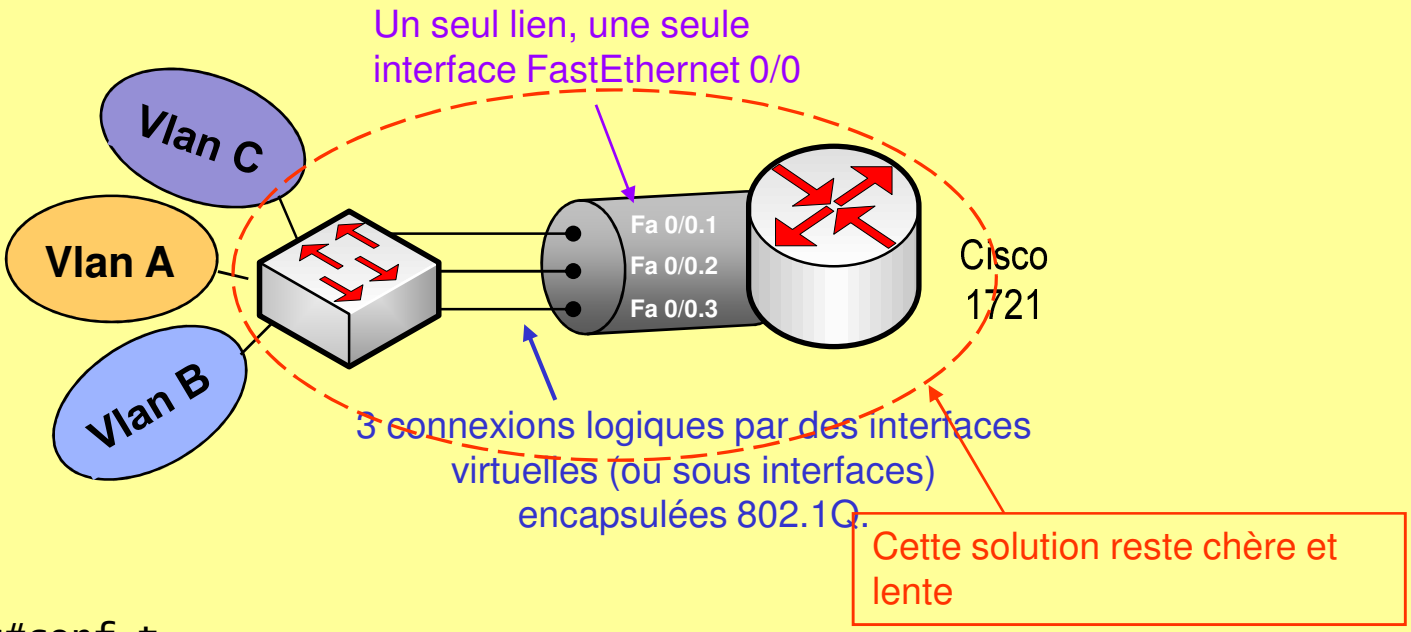
- La solution? ☞ Router les Vlan!!!

Le Routage des Vlans



On réalise des Vlan axés sur le protocole, le sous réseau ou l'adressage (ou vlan de niveau 3).

Le routage des Vlans



- Exemple:
  - `router#conf t`
  - `router(config)#interface FaEthernet 0/0`
  - `router(config-if)#no shutdown`

  - `router(config-if)#interface FastEthernet 0/0.1`
  - `router(config-subif)#description vlan A TAG 10`
  - `router(config-subif)#encapsulation dot1q <tag_vlan>`
  - `router(config-subif)#ip address <adresse_IP> <mask>`
  - `router(config-subif)#end`
  - `...`

  - `router#show ip route`

Commutateur N3 :

- La solution : Le commutateur de N3

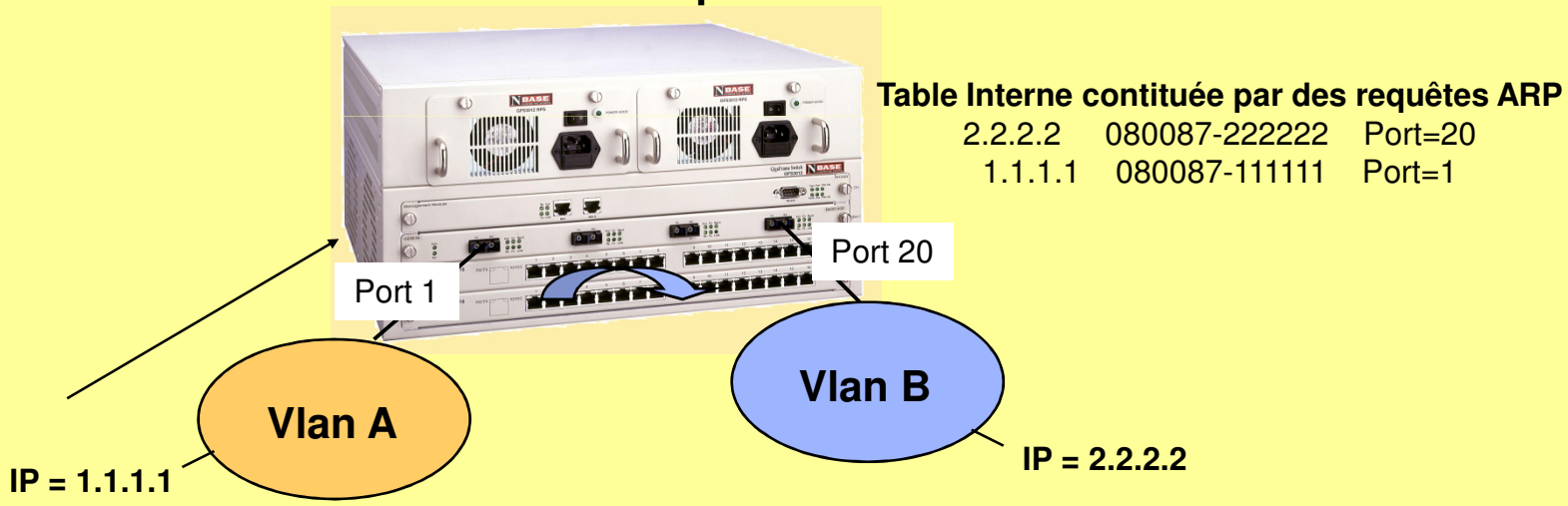
- **Issus de la technologie des routeurs,**
- **Le routage est effectué par des Asics dédiés,**
- **Limitent les broadcasts aux sous-réseaux constitués (Vlan),**
- **Accélèrent le routage IP entre les sous-réseaux,**
- **Assurent la commutation Niveau 2 pour les autres protocoles,**
- **Assurent la conversion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

L'analyse et l'optimisation de la configuration d'un commutateur de N3 sont abordés durant le TP.

Vlan Niveau 3
Fonctionnement

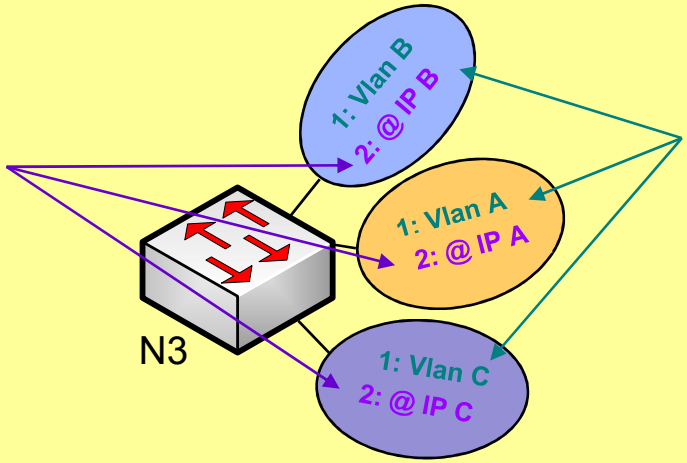
Cas N°1 : Direct IP

- **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 !!!

Mise en pratique chez Cisco



Deux étapes:

1. Création des Vlans comme avec les commutateurs de N2
2. Affectation des Adresses IP

```
Switch(config)#interface Vlan <ViD>
Switch(config-if)# ip address <addr> <masque>
Switch(config-if)#no shutdown
….
Switch#sh ip route
```

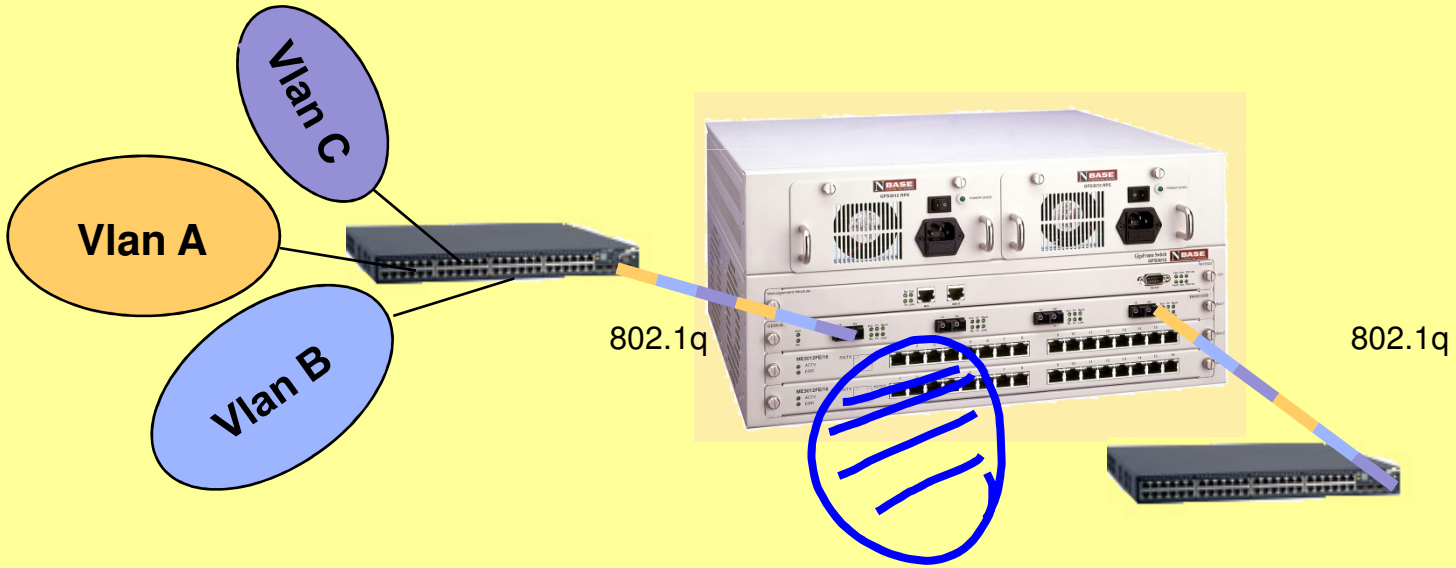
L'adresse IP attribuée devient l'adresse de passerelle du Vlan

Affichage des route mais elles sont à définir.

Vlan Niveau 3
Fonctionnement

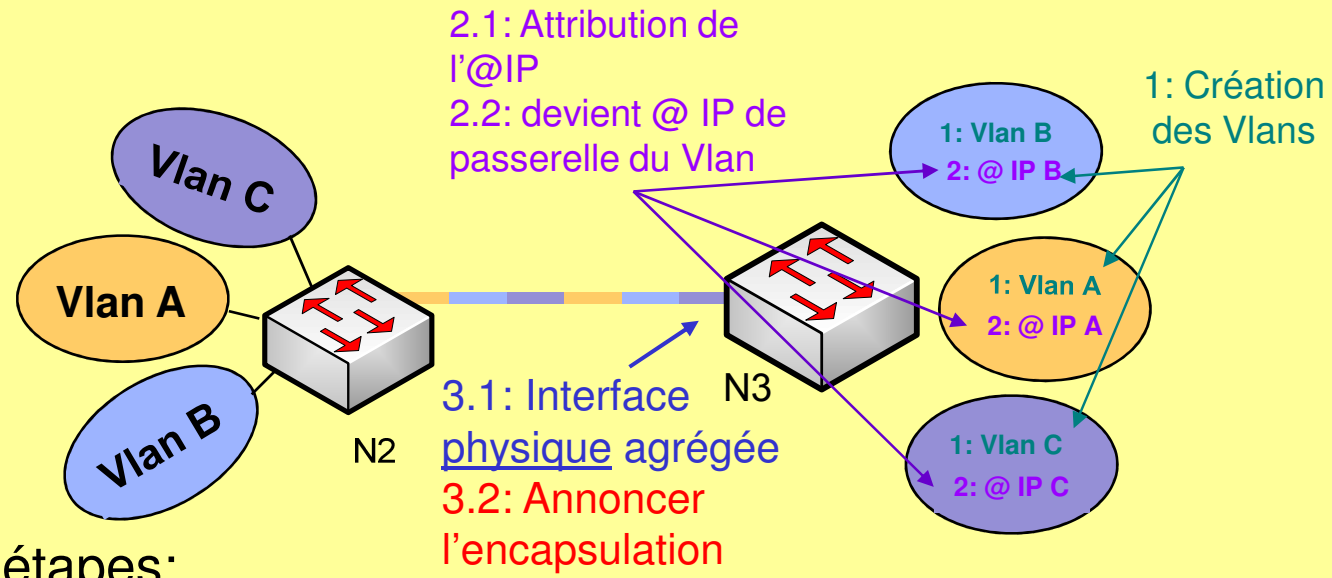
Cas N°2 : Solution 802.1q

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



L'analyse et la mise à jour d'une configuration d'un commutateur de N3 sont abordés durant le TP.

Mise en pratique chez Cisco



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

3 ViD à autoriser dans ce cas

Conf port trunk comme N2

```
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
```

Annoncer pour le N3 l'encapsulation 802.1q

Vlan Niveau 3
Fonctionnement

Cas N°3 : Solution dynamique

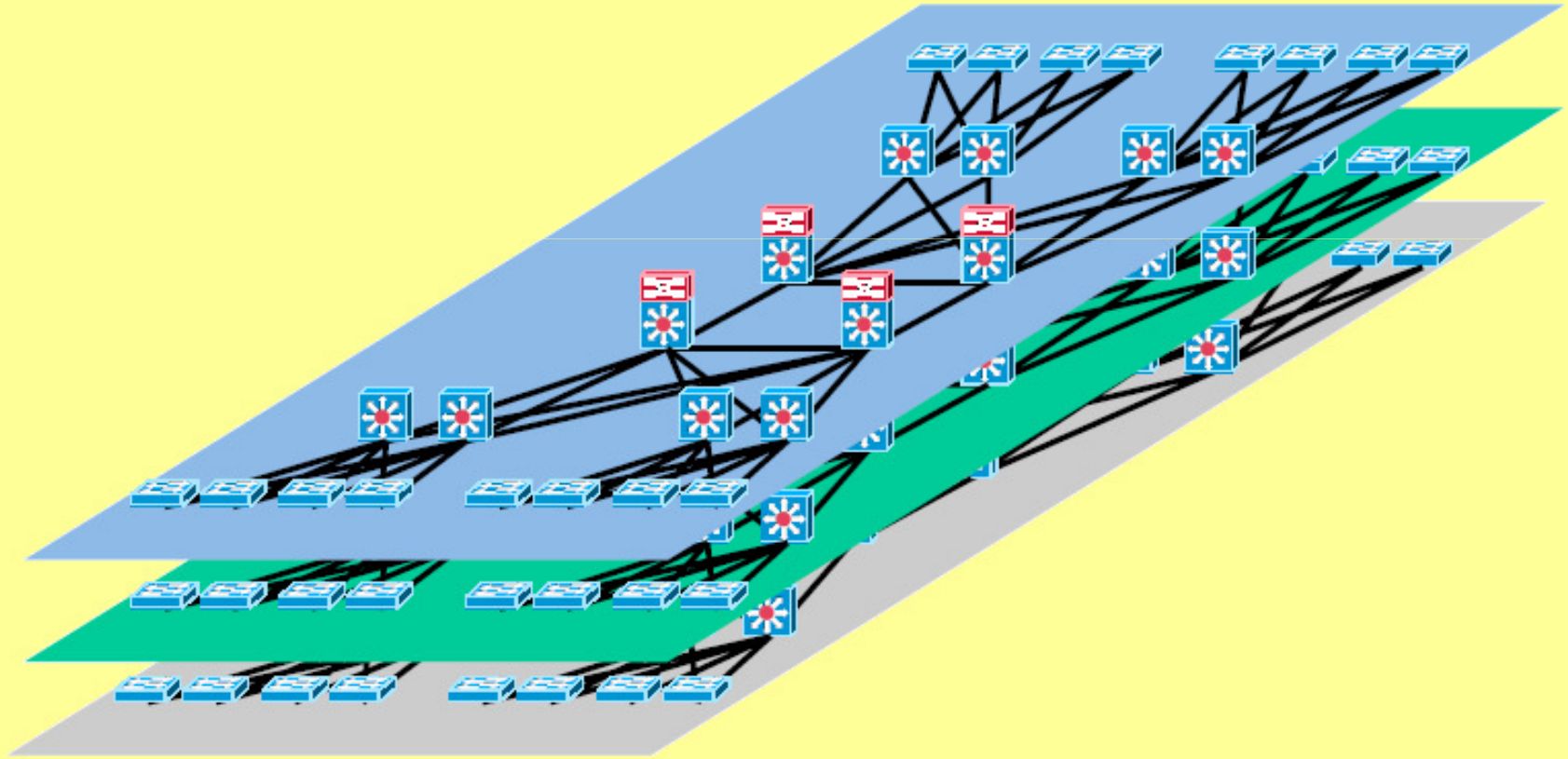
- **Le commutateur Niveau 3 utilise des protocoles de routage dynamique RIPv1-v2/OSPF**
- **Les Vlan IP sont automatiquement constitués en lisant l 'adresse source IP**
- **Les tables de routage hardware sont constituées automatiquement**
- **Le routage s 'effectue comme dans un routeur traditionnel**

Bilan des Vlan de N3 :

- **Les Vlan sont routés puisque par définition un routeur route!!!,**
- **Pb de sécurité puisque chaque groupe d'utilisateurs n'est plus isolé,**
- **Plus de réseau d'administration isolé également!!!!!**
- **La solution:**
  - **Les liste de contrôle d'accès (ACL : Access Control List)**
  - **Des règles de pare feu au sein des commutateurs de N3.**
- ***L'analyse d'une ACL est abordée durant le TP.***

Conséquence: Nouvelle infrastructure

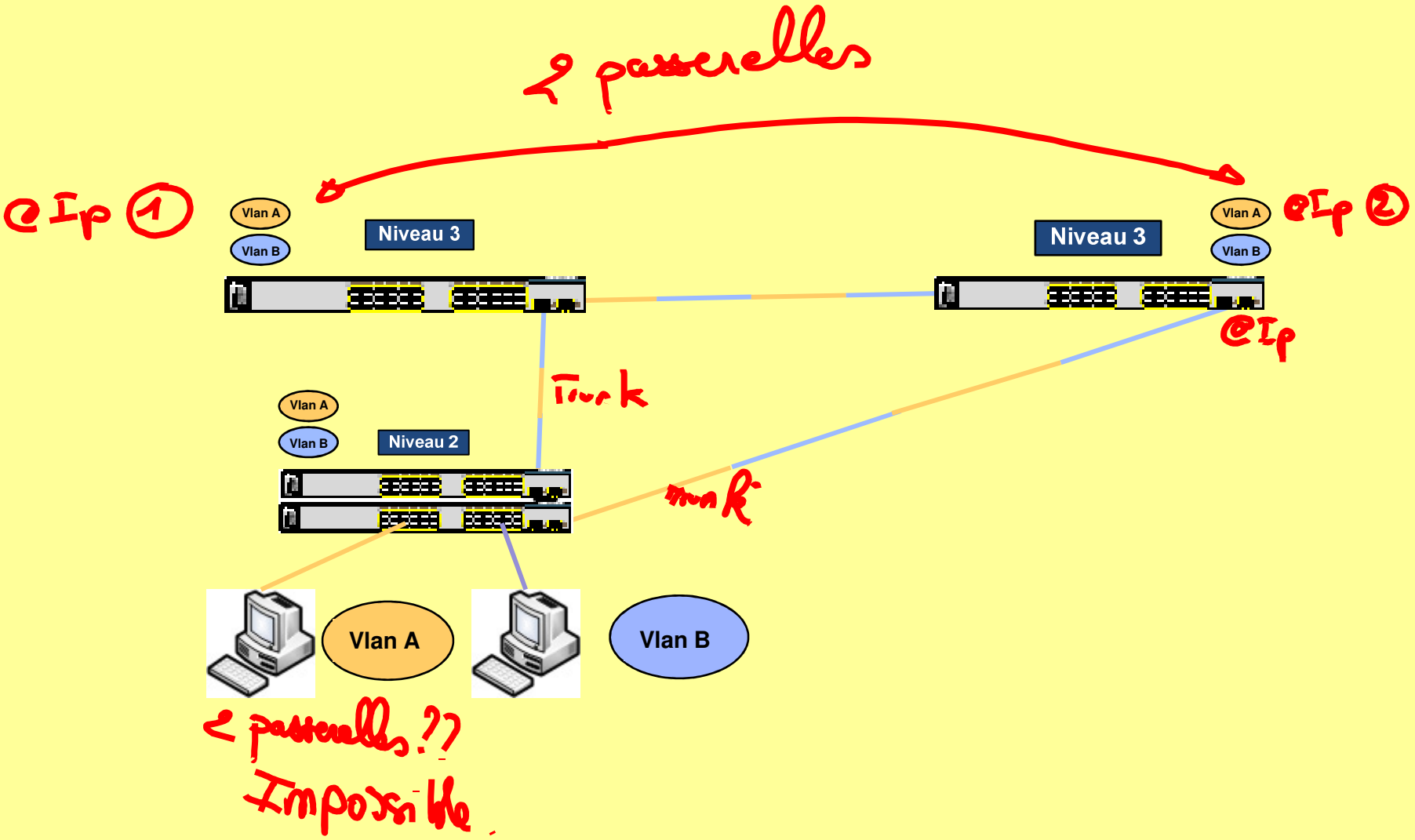
- « Virtualisation » de l'infrastructure,

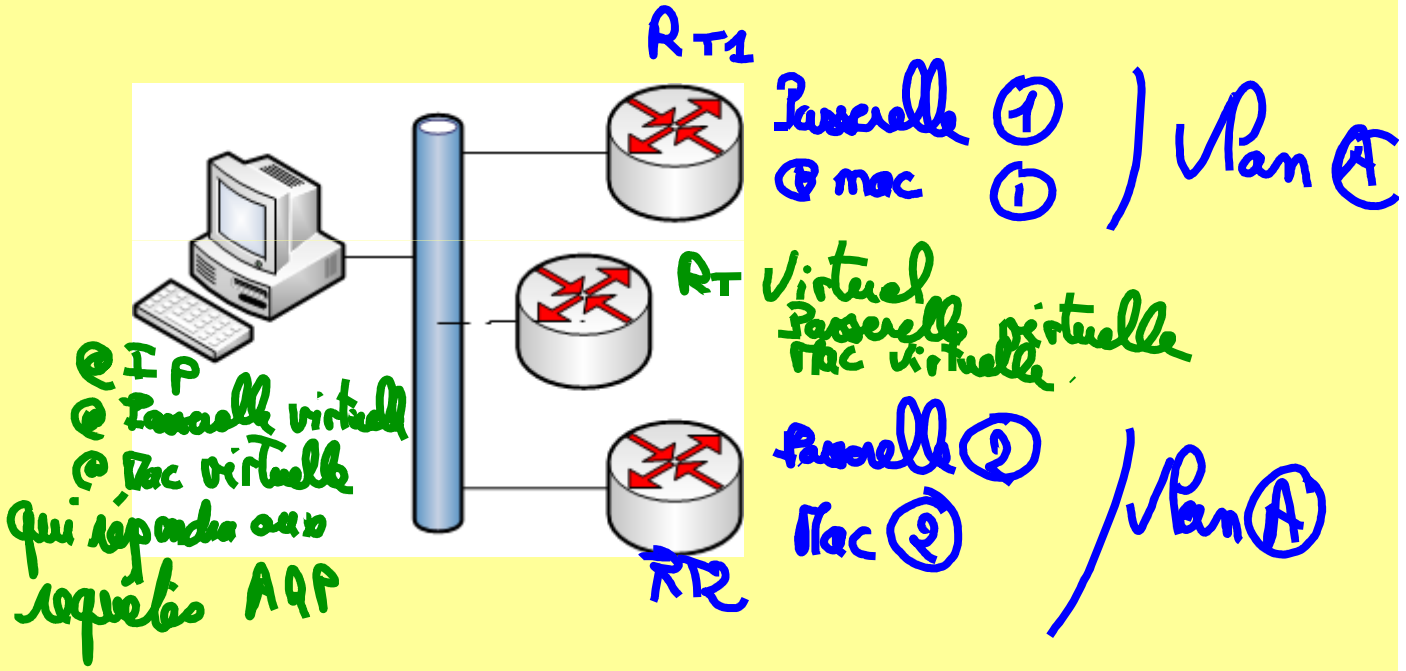


Les protocole VRRP et HSRP

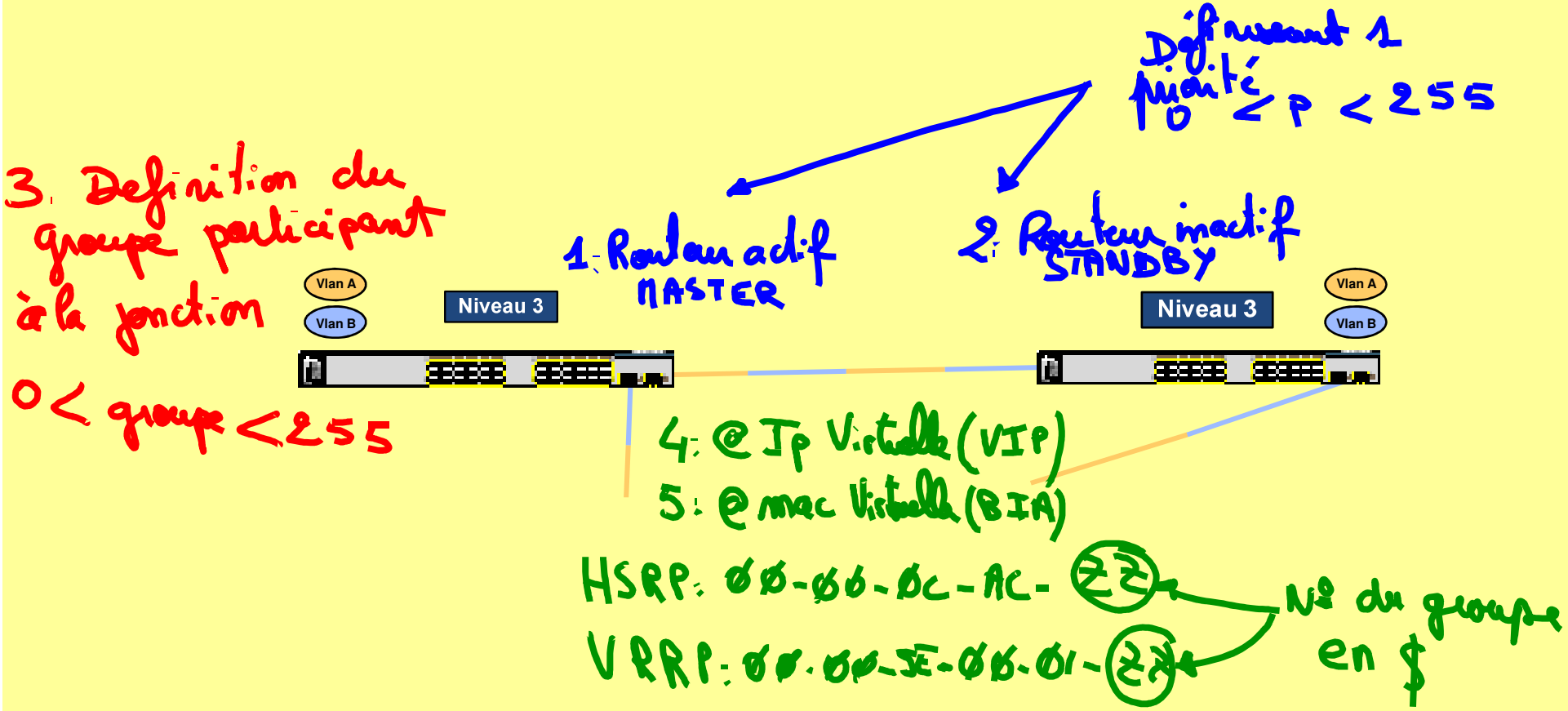
- Réseaux Actuels beaucoup de Vlans N3:
  - Mais pourquoi?
    - Séparer les domaines de Broadcast,
    - Bien séparer les applications
    - Mieux Déployer les ressources
  - En aucun cas, un client ne doit pas être en mesure de ne pas sortir de son domaine de broadcast pour atteindre une ressource
  - 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?
    - Une adresse IP de passerelle,
    - L'adresse MAC de la passerelle
- Réseau actuels c'est aussi 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!!!!!
    - Un Client n'a qu'une seule adresse de passerelle!!!!

Les protocole VRRP et HSRP

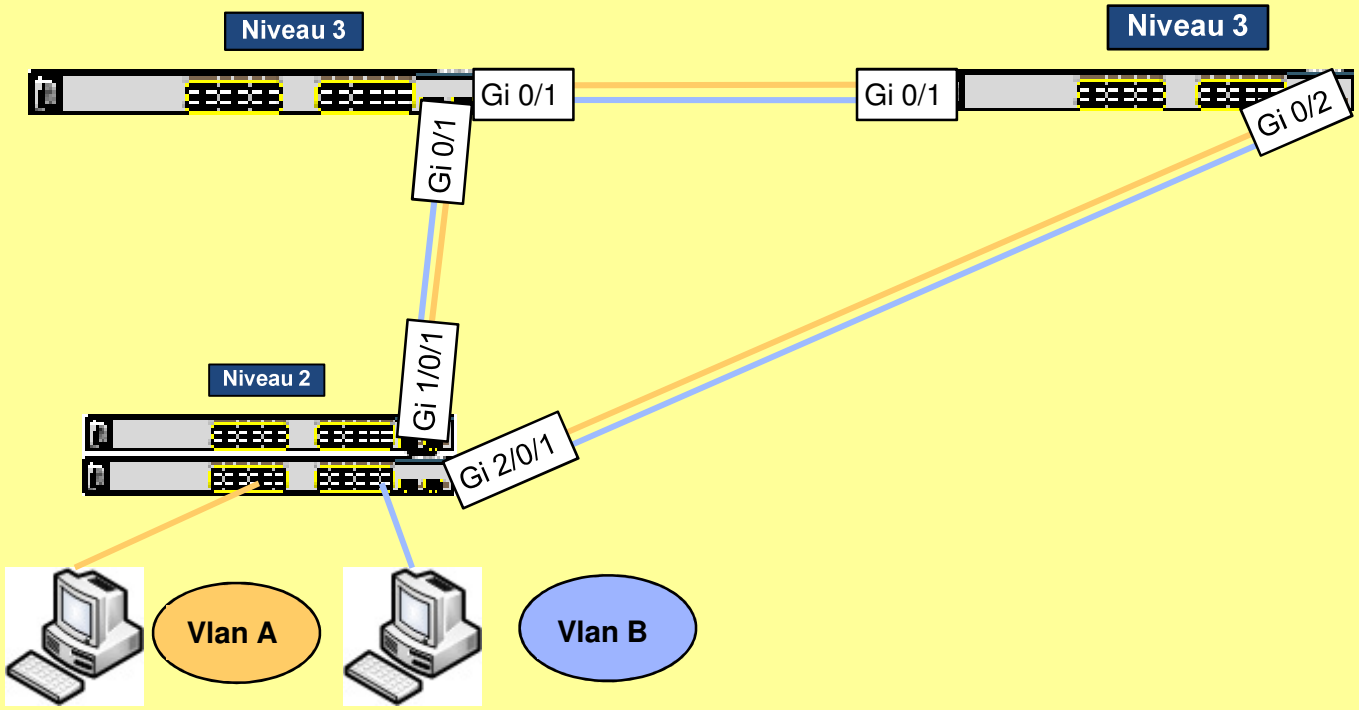



RT1
Passerelle 1
@ mac 1
Vlan A
RT
Virtuel
Passerelle virtuelle
Mac virtuelle
@IP
@ Passerelle virtuelle
@ Mac virtuelle
qui répondra aux
requêtes ARP
Passerelle 2
Mac 2
Vlan A
RT2

Fonctionnement VRRP et HSRP



La répartition de Charge



Paramétrage HSRP

3 paramètres cités précédemment

Ajustable mais par défaut 3*3s Hellotime et 10s holdtime

- 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 version
```

- switch(config-if)#standby

2 conditions pour qu'un routeur soit actif:

a) Plus grande priorité

b) Mode preempt

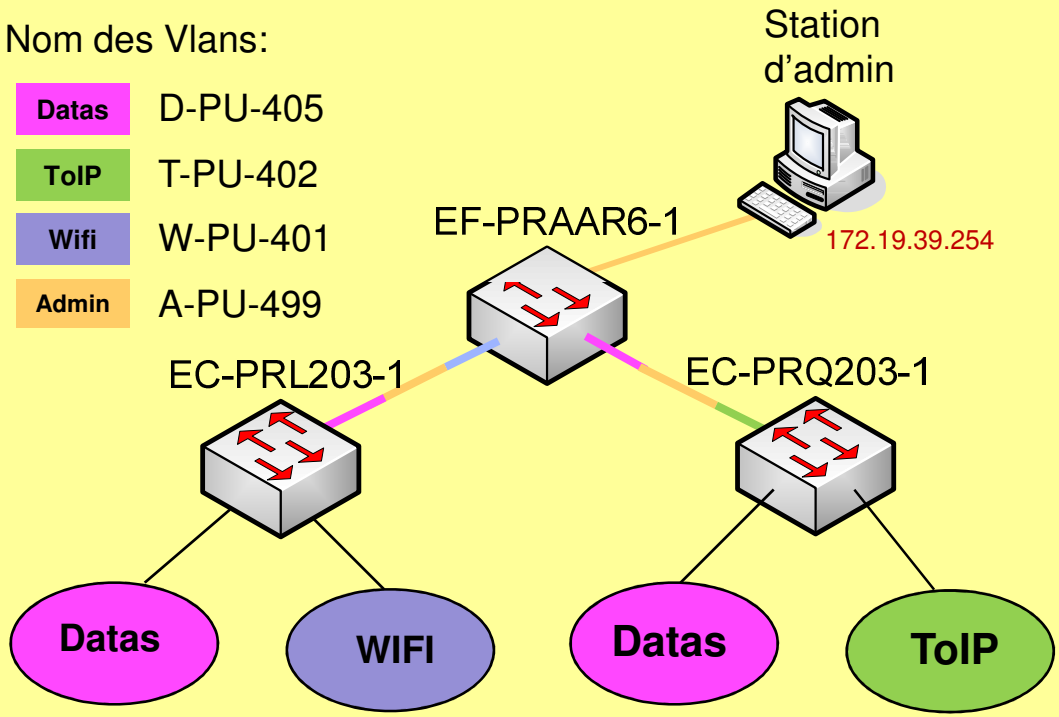
Très utile si le routeur définit actif venait à être défectueux et redevienne actif après dépannage

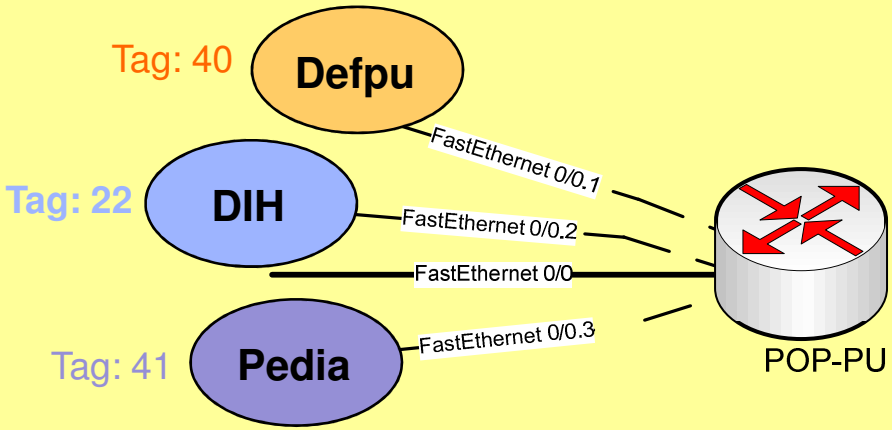
Le principal avantage

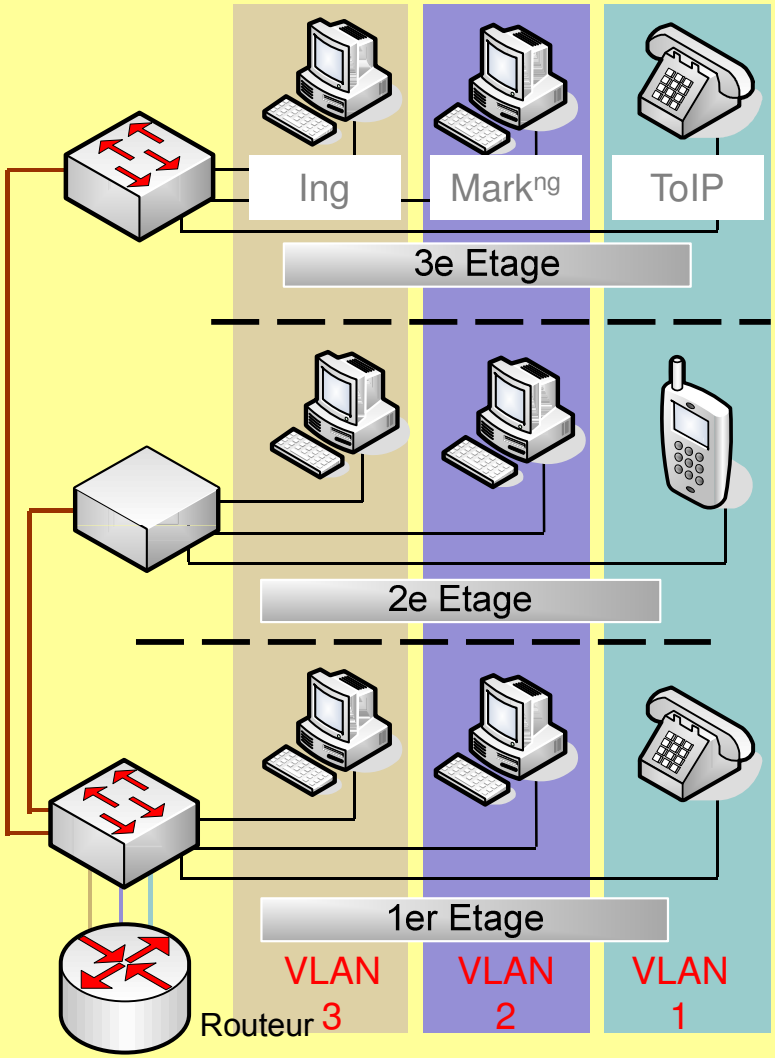
- Ils permettent à l'administrateur réseau d'organiser le LAN de manière logique et non physique. Cela signifie qu'un administrateur peut effectuer toutes les opérations suivantes:
- Déplacer facilement des stations de travail sur le LAN
- Ajouter facilement des stations de travail au LAN
- Modifier facilement la configuration LAN
- Contrôler facilement le trafic réseau
- Améliorer la sécurité

Dialogue

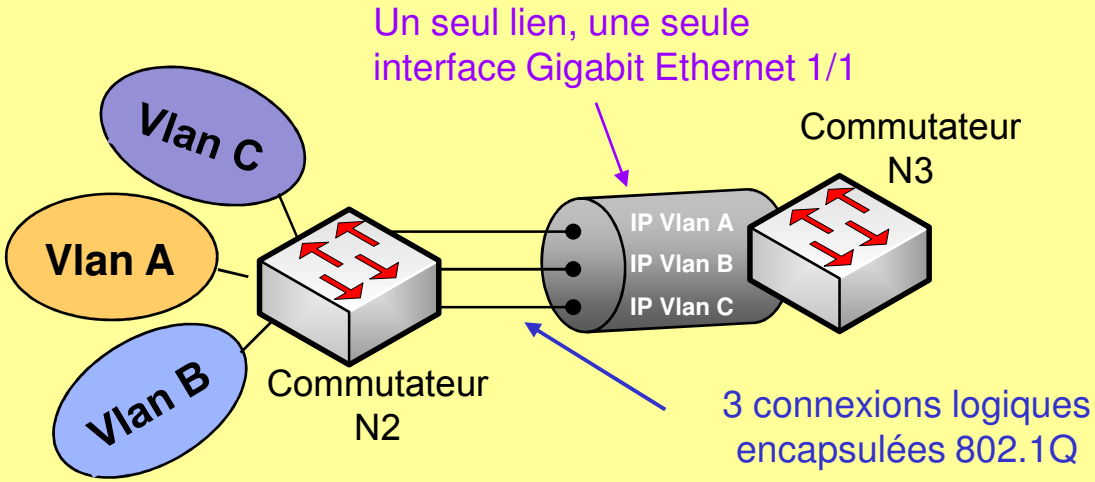
Un réseau d'administration




Tag: 40
Defpu
FastEthernet 0/0.1
Tag: 22
DIH
FastEthernet 0/0.2
FastEthernet 0/0
Tag: 41
Pedia
FastEthernet 0/0.3
POP-PU


Ing
Mark^ng
ToIP
3e Etage
2e Etage
1er Etage
VLAN 3
VLAN 2
VLAN 1
Routeur

Mise en pratique chez Cisco



Trois étapes:

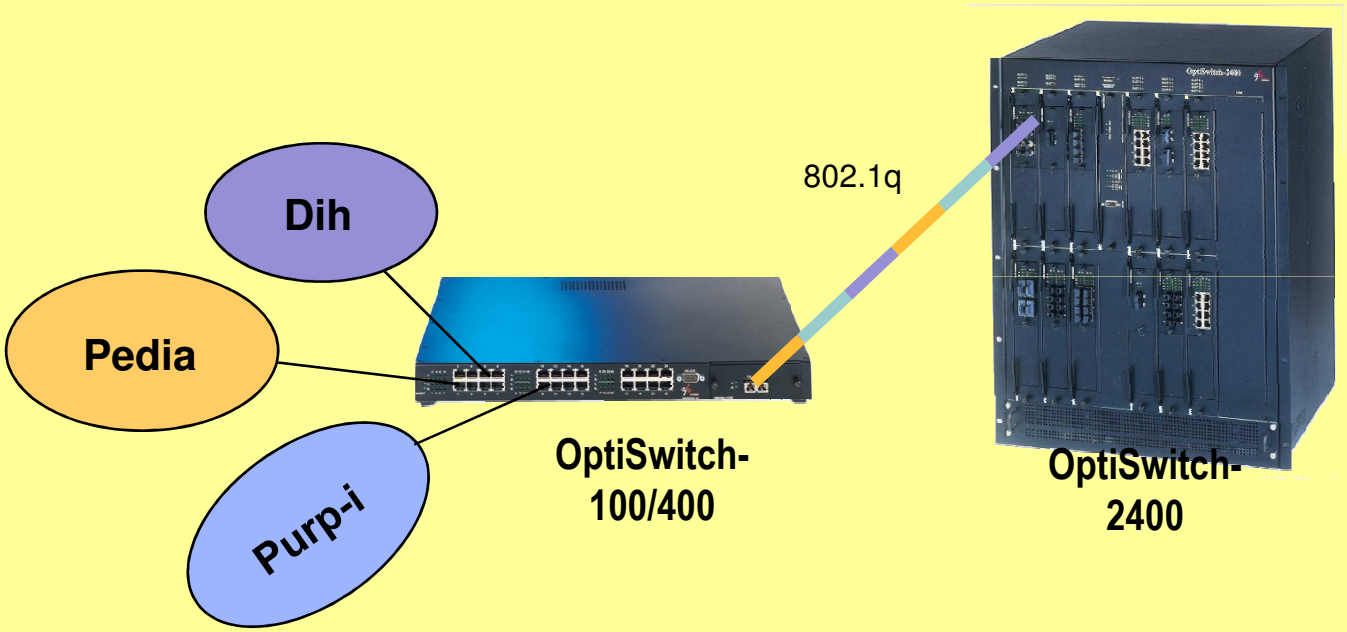
1. Création des Vlans comme avec les commutateurs de N2
2. Affectation des Adresses IP au Vlan <ViD>
3. Sur l'interface du port trunck

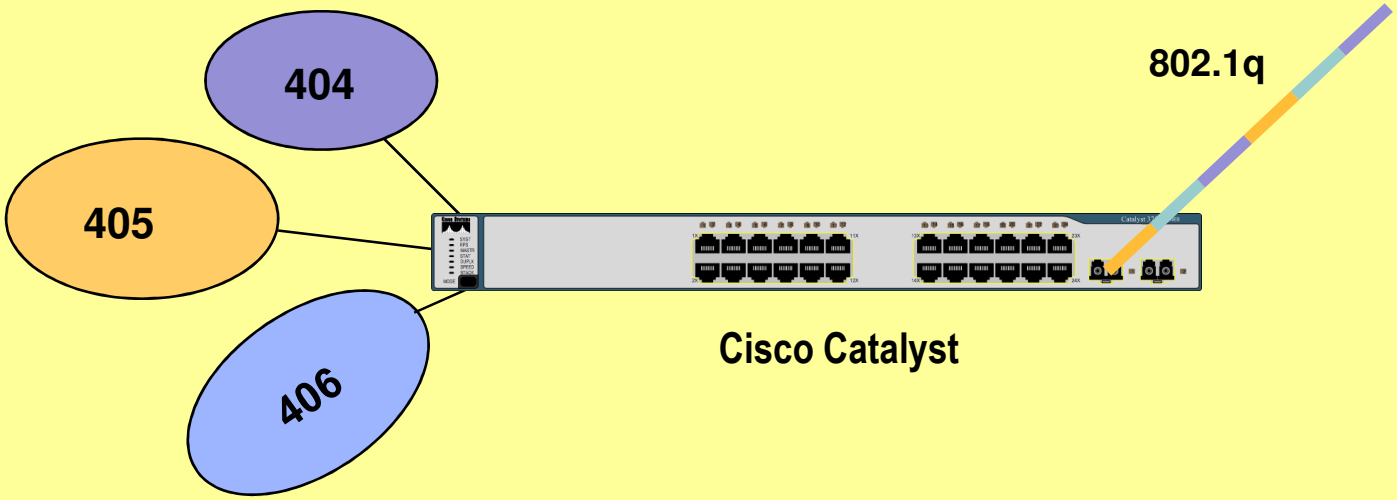
3 ViD à autoriser dans ce cas

Conf port trunk comme N2

```
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
```

Annoncer pour le N3 l'encapsulation 802.1q


Dih
Pedia
Purp-i
802.1q
OptiSwitch-
100/400
OptiSwitch-
2400


404
405
406
802.1q
Cisco Catalyst

Segmentation avec des Vlans

Créer, avec un logiciel embarqué sur le commutateur (firmware) un ensemble d'unités ou d'utilisateurs qui peuvent être regroupés par fonction, par service ou par application, quel que soit leur emplacement physique.

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