Réseaux
VLAN

Sommaire

1. Généralités

2. Fonctionnement

3. Interconnexion inter-VLAN

4. MRP (ex. GARP)

5. Implémentation

6. Cas pratique

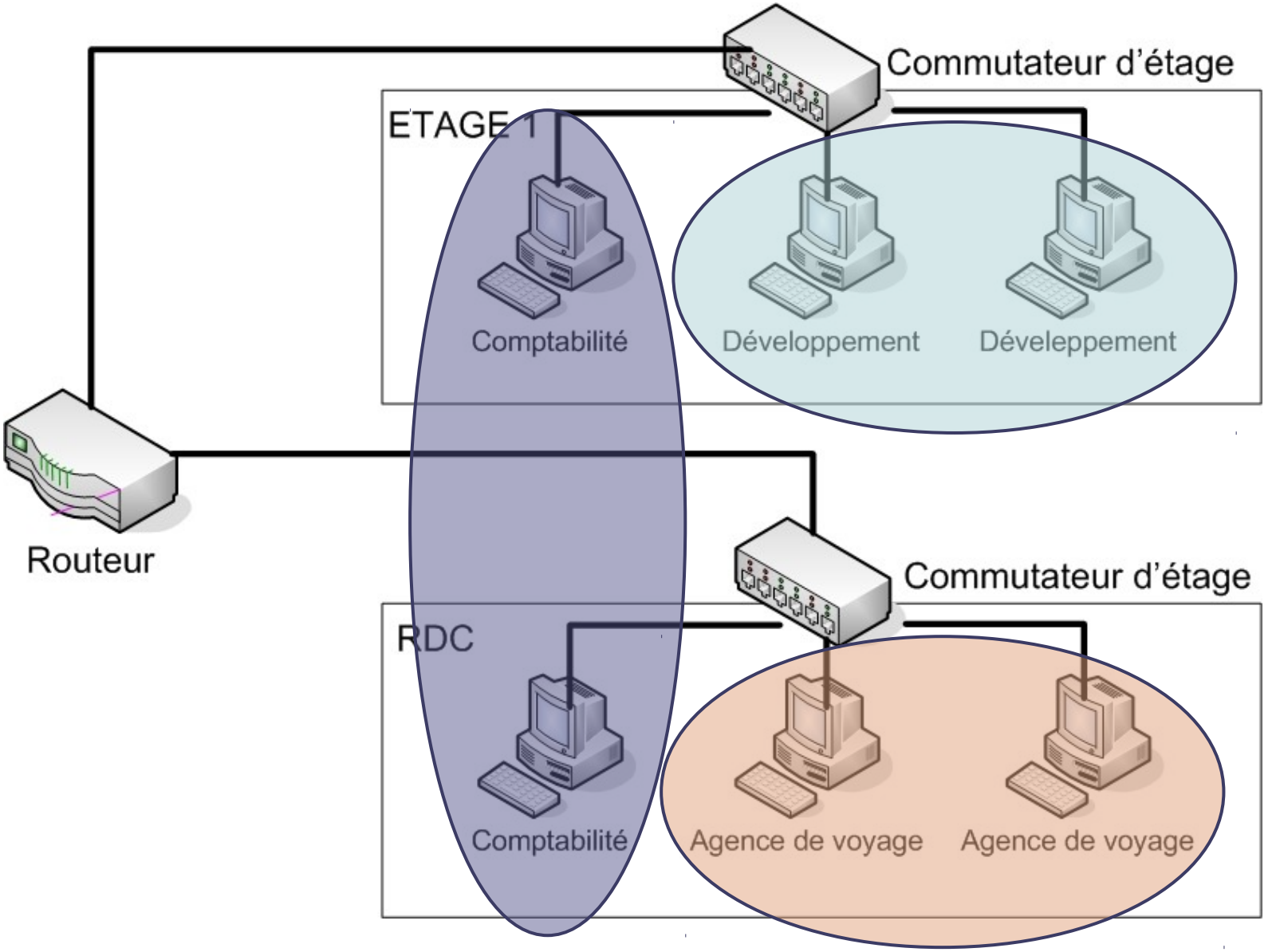
- Originellement ISL (Cisco), introduit les notions de base des VLAN comme l'étiquetage, le routage inter-VLAN, … ;

- Par la suite la norme IEEE 802.1q (1998) reprend principalement les notions de l'ISL ;

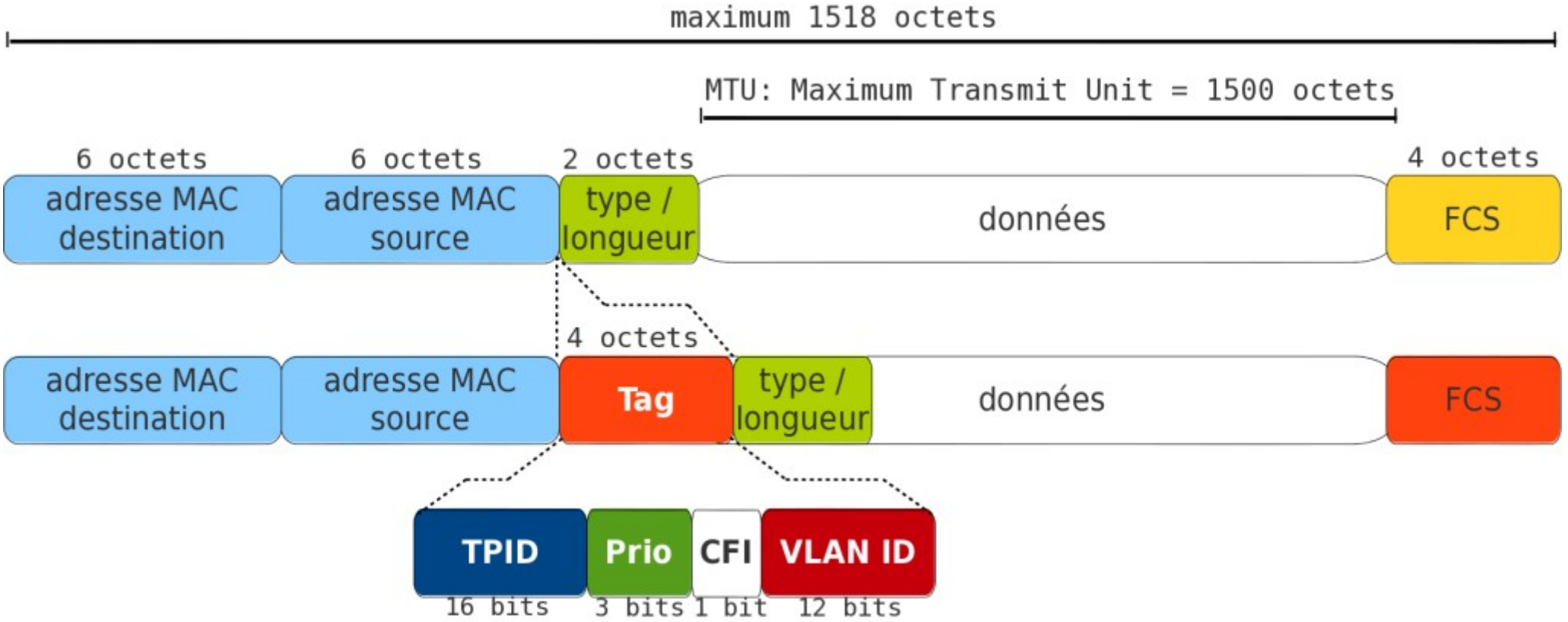
- Enfin, la norme IEEE 802.1q (2003) évolue pour supporter l'enregistrement dynamique des VLANs (GVRP) et la transmission de trames sur plusieurs instances de ***Spanning Tree***

- Les VLANS agissent au niveau 2 du modèle OSI ;
- Ils permettent la segmentation d'un support physique en segments logiques ;
- Ils apportent les avantages suivant:
  - limite la diffusion des broadcastes ;
  - plus grande flexibilité de la segmentation du réseau ; (indépendance géographique)
  - amélioration de la sécurité ;
  - priorisation des flux.

Fonctionnement



Voici la trame Ethernet 802.1q :



- TPID : type de tag, 0x8100 pour 802.1q ;
- Priorité : niveau de priorité définit par l'IEEE 802.1p ;
- CFI : Ethernet ou Token-ring ;
- VID : Vlan identifier, jusqu'à 4096 vlans.

Il faut noter que le champ FCS est recalculé après l'insertion de la balise de VLAN.

Voici un extrait de capture, réalisée avec ***Wireshark***, qui illustre les champs de la balise IEEE 802.1q :

```
Frame 103 (1518 bytes on wire, 1518 bytes captured)
Ethernet II, Src: 00:14:f2:75:ed:72, Dst: 00:10:5a:de:9d:d7
    Destination: 3com_de:9d:d7 (00:10:5a:de:9d:d7)
    Source: Cisco_75:ed:72 (00:14:f2:75:ed:72)
    Type: 802.1Q Virtual LAN (0x8100) (1)
802.1Q Virtual LAN
    000. .... .... .... = Priority: 0 (2)
    ...0 .... .... .... = CFI: 0 (3)
    .... 0000 0110 0100 = ID: 100 (4)
    Type: IP (0x0800)
Internet Protocol, Src: 172.17.0.2 (172.17.0.2), Dst: 172.16.80.19 (172.16.80.19)
Transmission Control Protocol, Src Port: www (80), Dst Port: 1548 (1548)
```

1. Tag protocol identifier, TPID, EtherType : ce champ de 16 bits identifie le protocole véhiculé dans la trame.
   La valeur 0x8100 désigne une balise IEEE 802.1Q / 802.1P.

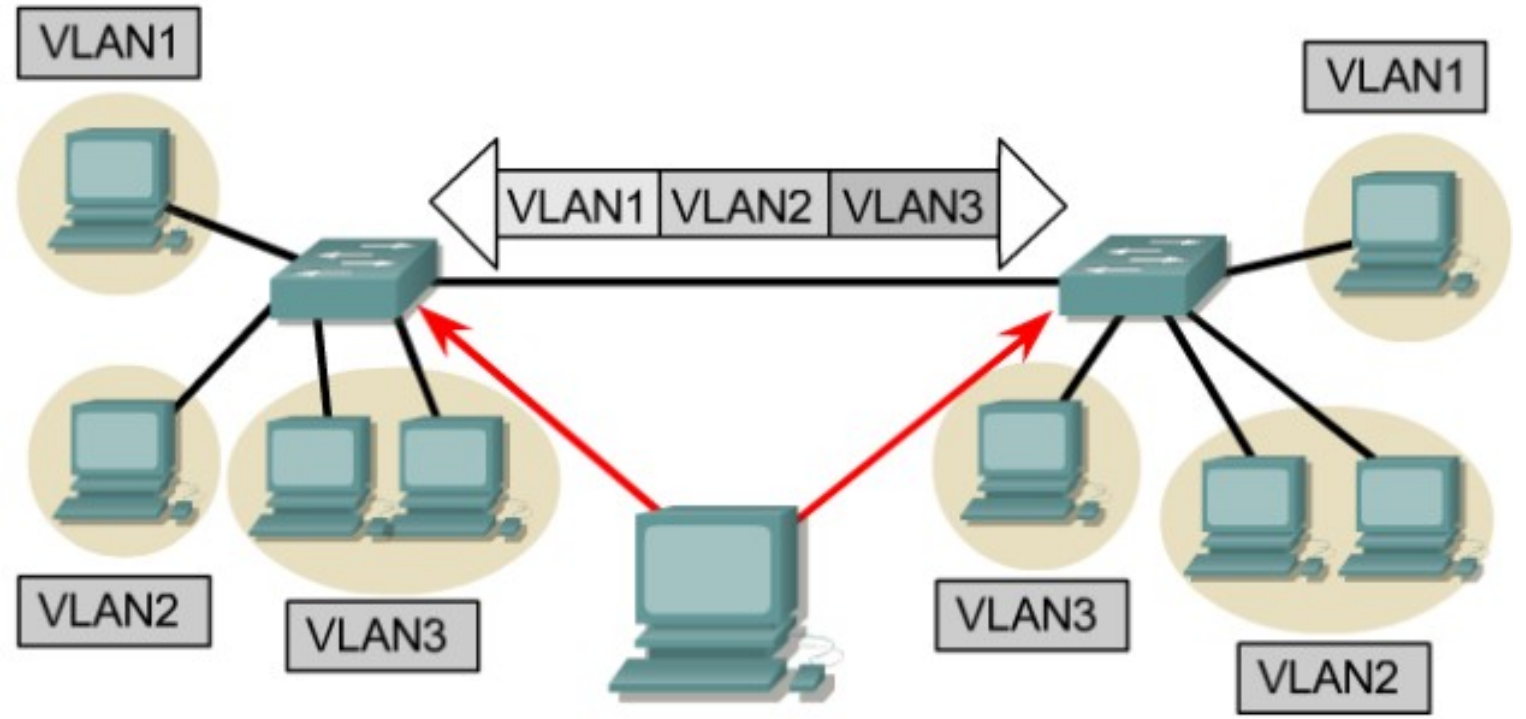
2. Priority : ce champ de 3 bits fait référence au standard IEEE 802.1P. Sur 3 bits on peut coder 8 niveaux de priorités de 0 à 7.
   La notion de priorité dans les VLANs est sans rapport avec les mécanismes de priorité IP au niveau réseau.
   Ces 8 niveaux sont utilisés pour fixer une priorité aux trames d'un VLAN relativement aux autres VLANs.

3 Canonical Format Identifier : ce champ codé sur 1 bit 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).

4 VLAN Identifier, vlan id, VID : ce champ de 12 bits sert à identifier le réseau local virtuel auquel appartient la trame.
Il est possible de coder 4096 réseaux virtuels avec ce champ.

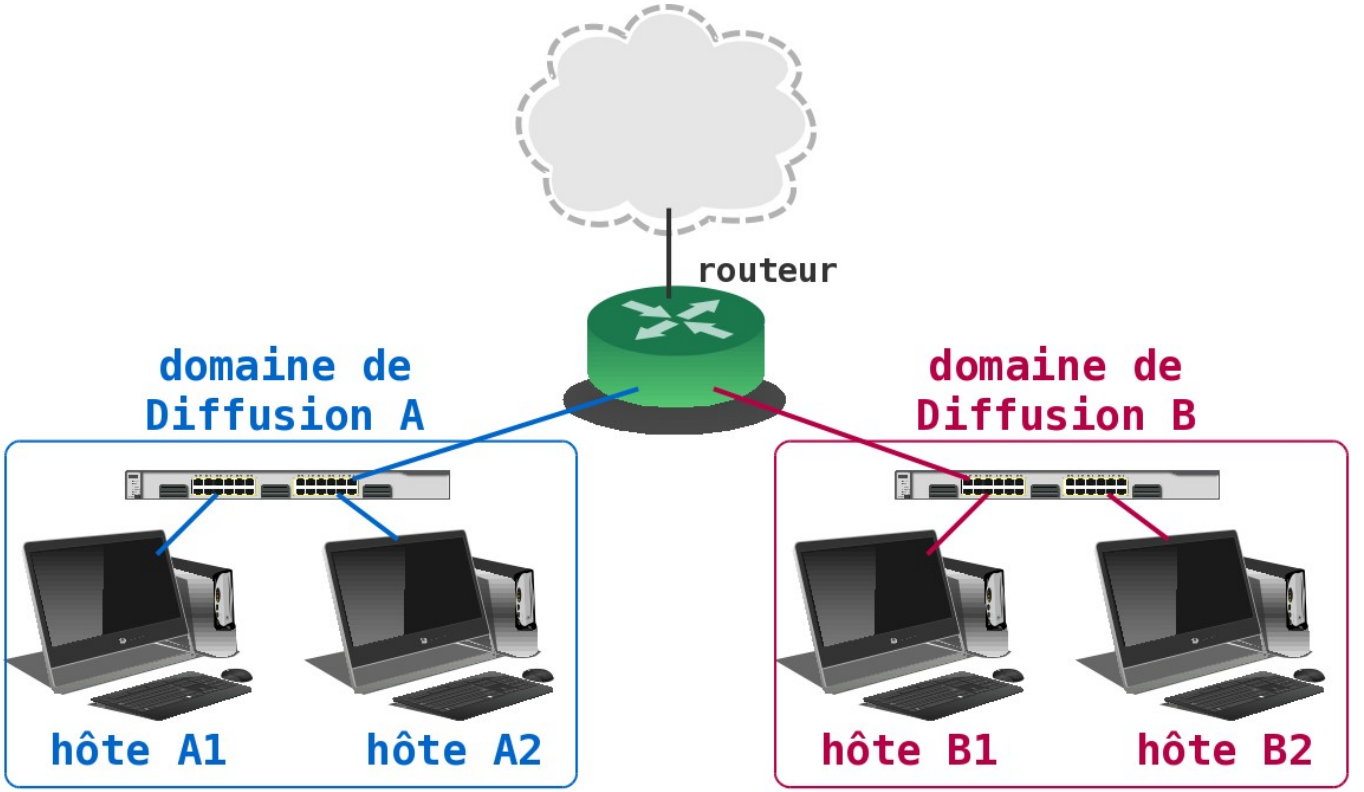
Il existe différents types de VLAN :

- Par port ;
- Par adresse MAC ;
- Par adresse IP ;
- Par protocole de niveau 3.



- La communication entres VLANS se fait au niveau 3 du modèle OSI ;

- Le routage entres interfaces virtuelles ne peut être réalisé que par un routeur, seul apte à modifier le VID associé à une trame.



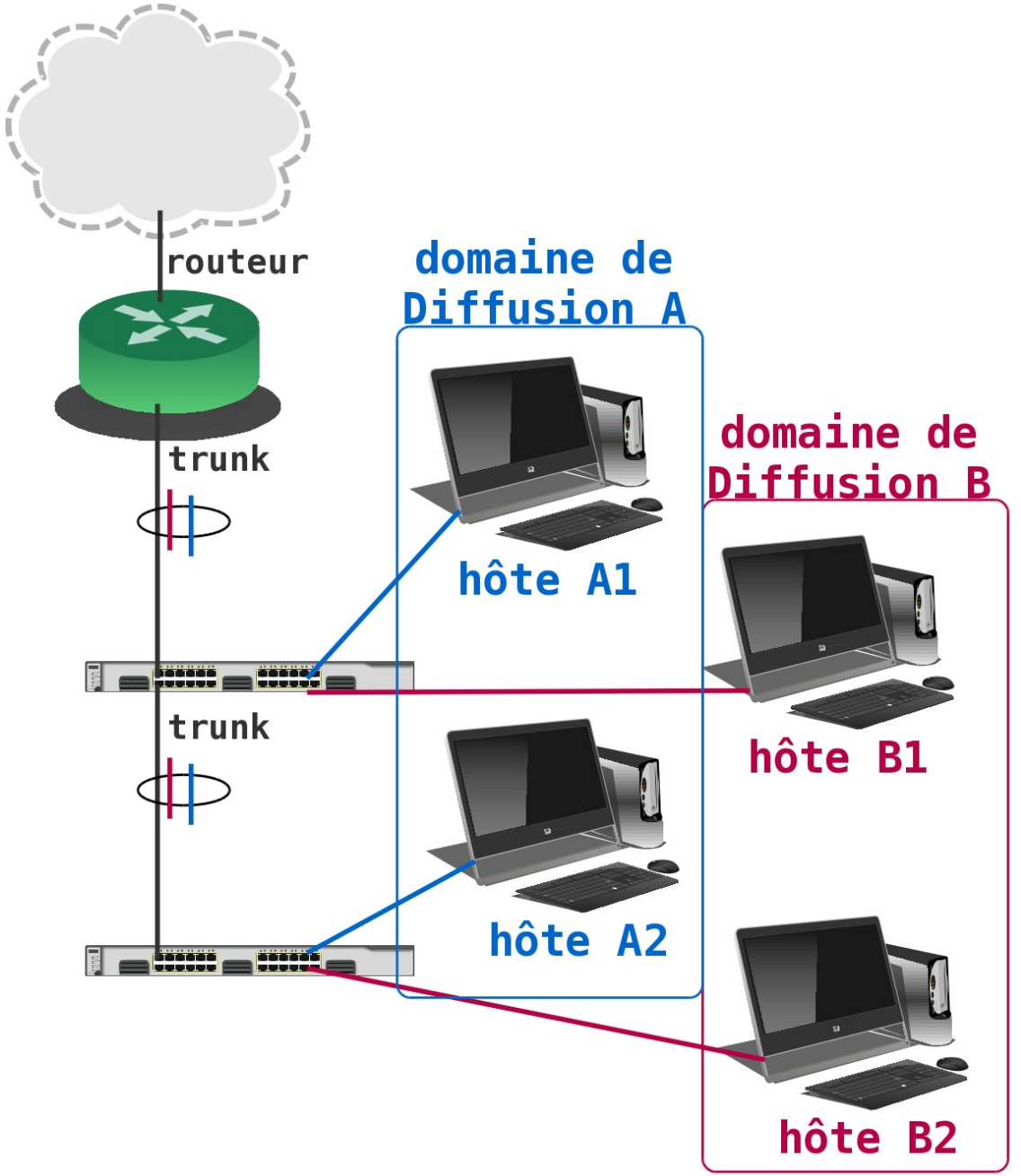
- Si on programme le commutateur A avec 2 VLANs distincts pour chacun des PCs A1 et A2, alors toute communication entre A1 et A2 sera impossible.

- Ces deux PCs ne pourront communiquer avec d'autres réseaux que si l'interface du routeur RA appartient aux deux VLANs.

- Cette situation peut présenter des avantages du point de vue exploitation mais elle dépend beaucoup de la gestion des interfaces physiques : **le coût d'administration devient très important dès que le nombre de réseaux virtuels augmente.**

- Si l'utilisateur du PC A1 déménage dans un lieu ou seul le domaine de diffusion B est distribué, il est nécessaire d'étendre le domaine de diffusion A jusqu'à ce nouveau lieu.
  En conséquence, il faudra installer un nouveau commutateur et câbler de nouvelles prises entre le point de brassage principal du domaine A et ce lieu.

- Sur une même infrastructure, on se retrouve rapidement avec des commutateurs saturés pour lesquels tous les ports disponibles sont utilisés et d'autres commutateurs pour lesquels seuls quelques ports sont utilisés.



Dissocions les notions d'interface physique et d'interface de routage : on n'associe plus une interface physique à chaque domaine de diffusion mais une **interface «virtuelle»**

- Le contrôle d'accès est centralisé au niveau du routeur. Il n'existe plus de «mélange des genres» entre la programmation des commutateurs et le contrôle d'accès au niveau réseau.

- Les communications entre les hôtes d'un même domaine de diffusion ou entre plusieurs domaines de diffusion sont gérées de la même façon.

- On obtient de véritables réseaux locaux distribués sur la totalité de l'infrastructure (équipements de niveau 2 + équipements de niveau 3).

- La gestion du parc des ports de commutation est optimisée.
- Comme les domaines de diffusion sont partagés entre tous les équipements, la gestion des évolutions est beaucoup plus souple.
- Les déménagements n'entraînent aucun recâblage tant que l'évolution du nombre des hôtes n'implique pas une augmentation du nombre de ports.
- Il est donc possible de concentrer l'administration sur un nombre d'équipements plus faible que dans une architecture sans routage inter-VLAN.

On peut noter sur le schéma précédent un nouveau type de lien, ***Trunk***. Ce type de lien peut être placer entre :

- deux commutateurs : c'est le mode de distribution des réseaux locaux le plus courant.
- un commutateur et un hôte : c'est le mode de fonctionnement à surveiller étroitement. Un hôte qui supporte le ***trunking*** a la possibilité d'analyser le trafic de tous les réseaux locaux virtuels.
- un commutateur et un routeur : c'est le mode fonctionnement qui permet d'accéder aux fonctions de routage, donc à l'interconnexion des réseaux virtuels par routage inter-VLAN.

Enfin, il ne faut pas oublier que tous les VLANs véhiculés dans le même ***trunk*** partagent la bande passante du média utilisé.

Le *trunk* peut donc constituer un goulot d'étranglement si sa capacité est insuffisante.

MRP

- ***Multiple Registration Protocol*** (MRP), autrefois connu sous les noms ***Generic Attribute Registration Protocol*** (GARP) et ***GARP VLAN Registration Protocol*** (GVRP) est un protocole standard de niveau 2 pour la configuration automatique des VLANs dans un réseau commuté ;

- Il est défini par la norme IEEE 802.1ak ;

- Il permet d'enregistrer ou dés-enregistrer des attributs et leur valeur, comme les identifiants de VLAN ou l'appartenance à des groupes multicasts.

- GARP définit une architecture, des règles d'opérations, les machines à états et les variables pour l'enregistrement et le dés-enregistrement des valeurs d'attributs.

- GARP est utilisé pour l'enregistrement de VLAN, le ***trunking*** entre des commutateurs réseaux et par ***GARP Multicast Registration Protocol*** (GMRP).

Implémentation: création de VLAN

Sous linux, la commande ***ip*** permet de créer des VLANs :

*# ip link add link eth**X** name eth**X.VLAN_ID** type vlan id **VLAN_ID***

- ***X*** représente le numéro d'interface utilisé ;
- ***VLAN_ID*** représente l'identifiant du VLAN ;

Elle permet également de les supprimer :

*# ip link del eth**X.VLAN_ID***

Une fois le VLAN créé, il faut lui assigner une adresse IP (si besoin) :

ip addr add dev eth***X***.***VLAN_ID*** 192.168.100.1/24

Enfin, il faut allumer l'interface :

ip link set dev eth***X***.***VLAN_ID*** up

Malheureusement cette configuration est éphémère et ne résistera pas au redémarrage de la machine...

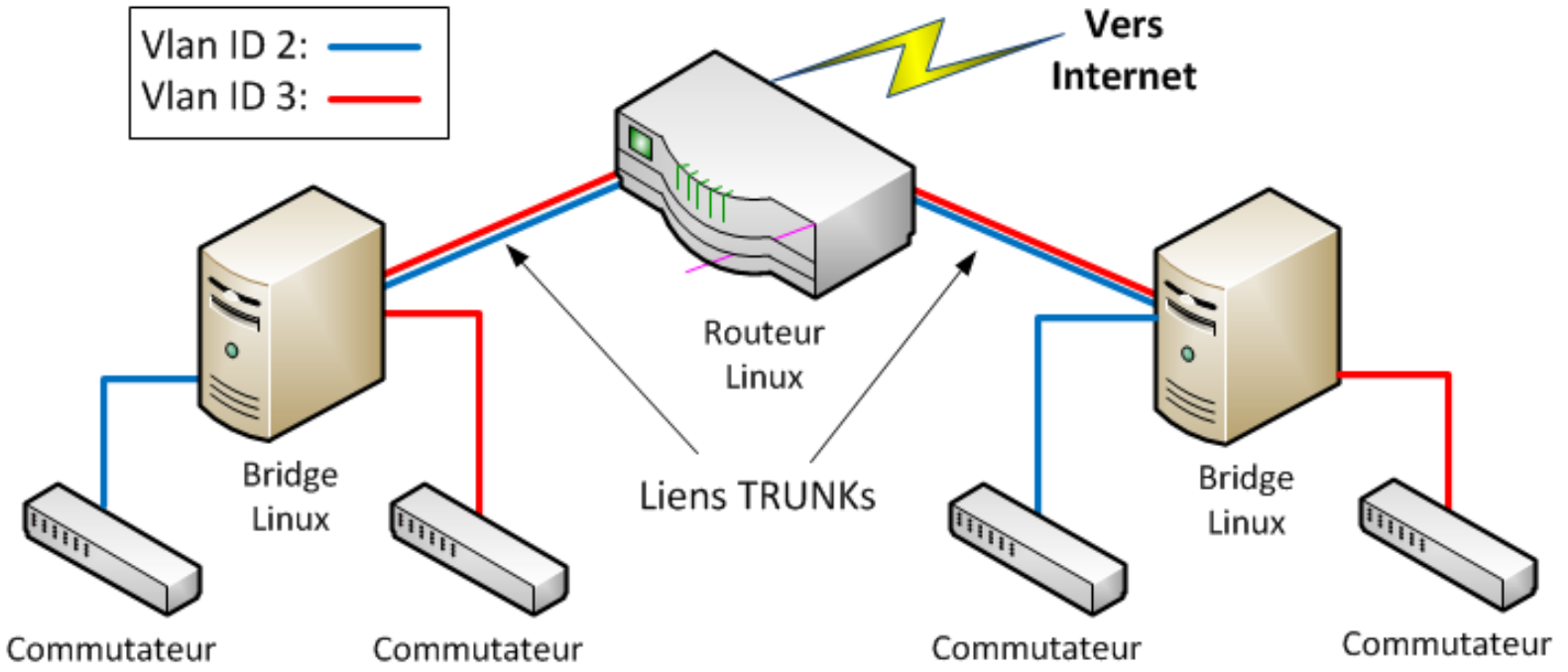
Pour configurer de manière permanente un VLAN, il faut créer le fichier adapter dans le répertoire ***/etc/sysconfig/network-scripts*** :

- Pour l'interface eth0 et le vlan id 2, le fichier portera le nom ***ifcfg-eth0.2***
- Il contiendra les lignes suivantes :

```
DEVICE="eth0.2"
VLAN=yes
BOOTPROTO="static"
ONBOOT="yes"
TYPE="Ethernet"
IPADDR=192.168.50.254
NETMASK=255.255.255.0
```

Maintenant tous les paquets sortant de l'interface ***eth0*** seront tagués et tous ceux entrant sur l'interface ***eth0.2*** seront dé-tagués !

Grâce aux commandes ***brctl*** et ***ip*** essayez de reproduire le schéma réseau ci-dessous :



Vous pouvez :

- vous aidez d'***iptables*** pour réaliser l'interconnexion entre les deux VLANs ;
- utilisez le service ***dhcpd*** pour distribuer dynamiquement les adresses sur ces deux VLANs.

- Tout d'abord raccordons le routeur à Internet en branchant une es cartes réseau et en la configurant correctement ;

- Activons le forwarding ip dans le fichier ***/etc/sysctl.conf*** puis rechargez les paramètres du noyau avec ***sysctl -p*** ;

- Supprimez le filtrage de la chaîne FORWARD (***iptables -F FORWARD***) ;

- Activez le camouflage pour les réseaux du ***VLAN*** 2 et 3
  # iptables -t nat -A POSTROUTING -s @res_vlan2 -j MASQUERADE
  # iptables -t nat -A POSTROUTING -s @res_vlan3 -j MASQUERADE

  A ce stade le routeur devrait 'pinger' Internet (essayez 8.8.8.8)

- Configurons maintenant les deux interfaces qui sont reliées aux bridges (ex. eth1 et eth2) de manière à ce quelle n'ai aucune configuration de niveau 3 (dans le répertoire ***/etc/sysconfig/network-scripts***)

ifcfg-eth1

```
DEVICE="eth1"
BOOTPROTO="none"
ONBOOT="yes"
TYPE="Ethernet"
```

ifcfg-eth2

```
DEVICE="eth2"
BOOTPROTO="none"
ONBOOT="yes"
TYPE="Ethernet"
```

- Maintenant que les interfaces vont démarrer, il faut configurer les vlan 2 et 3 dessus (ici exemple uniquement pour eth1) :

Ifcfg-eth1.2

```
DEVICE="eth1.2"
VLAN=yes
BOOTPROTO="none"
ONBOOT="yes"
TYPE="Ethernet"
BRIDGE=vlan2
```

Ifcfg-eth1.3

```
DEVICE="eth1.3"
VLAN=yes
BOOTPROTO="none"
ONBOOT="yes"
TYPE="Ethernet"
BRIDGE=vlan3
```

- N'oubliez pas les fichiers ***ifcfg-eth2.2*** et ***ifcfg-eth2.3*** !

- Vous aurez certainement remarquez la dernière ligne de chacun des fichiers de configuration des ***VLAN*** : BRIDGE=vlan***X***

  Cette ligne permet de dire que cette interface fait partie du bridge vlan***X***

- Créons les fichiers de configuration de ces deux bridges (toujours dans le répertoire ***/etc/sysconfig/network-scripts***) :

vlan2

```
DEVICE="vlan2"
VLAN=yes
BOOTPROTO="static"
ONBOOT="yes"
TYPE="Bridge"
IPADDR=192.168.2.254
NETMASK=255.255.255.0
```

vlan3

```
DEVICE="vlan3"
VLAN=yes
BOOTPROTO="static"
ONBOOT="yes"
TYPE="Bridge"
IPADDR=192.168.3.254
NETMASK=255.255.255.0
```

- N'oubliez pas de rechargez la configuration réseau :

```
# service network restart
```

- L'activation du service DHCP se fait une fois le service installé :

  # yum install dhcp

- Une fois le service installé, il faut configurer ses interfaces d'écoute dans le fichier ***/etc/sysconfig/dhcpd*** :

  DHCPDARGS="eth1.2 eth1.3 eth2.2 eth2.3"

- Il ne vous reste plus qu'à configurer les deux sous-réseaux dans le fichier ***/etc/dhcp/dhcpd.conf*** :

```
subnet 192.168.2.0 netmask 255.255.255.0 {
        option routers 192.168.2.254;
        option domain-name-servers 8.8.8.8;
        range 192.168.2.10 192.168.2.20;
}

subnet 192.168.3.0 netmask 255.255.255.0 {
        option routers 192.168.3.254;
        option domain-name-servers 8.8.8.8;
        range 192.168.3.10 192.168.3.20;
}
```

- La configuration des bridge commence par le choix d'une interface qui va servir de port ***TRUNK*** (ex. eth0):

ifcfg-eth0

```
DEVICE="eth0"
BOOTPROTO="none"
ONBOOT="yes"
TYPE="Ethernet"
```

Ifcfg-eth0.2

```
DEVICE="eth0.2"
VLAN=yes
BOOTPROTO="none"
ONBOOT="yes"
TYPE="Ethernet"
BRIDGE=vlan2
```

Ifcfg-eth0.3

```
DEVICE="eth0.3"
VLAN=yes
BOOTPROTO="none"
ONBOOT="yes"
TYPE="Ethernet"
BRIDGE=vlan3
```

- Puis se termine par la rassemblement des interfaces dans les bridges (ex. ***eth1*** et ***eth2***) :

Ifcfg-eth1

```
DEVICE="eth1"
BOOTPROTO="none"
ONBOOT="yes"
TYPE="Ethernet"
BRIDGE=vlan2
```

Ifcfg-eth2

```
DEVICE="eth2"
BOOTPROTO="none"
ONBOOT="yes"
TYPE="Ethernet"
BRIDGE=vlan3
```

- Si on branche un commutateur sur eth1, on devrait recevoir une adresse en 192.168.2.0/24 et sur eth2 en 192.168.3.0/24