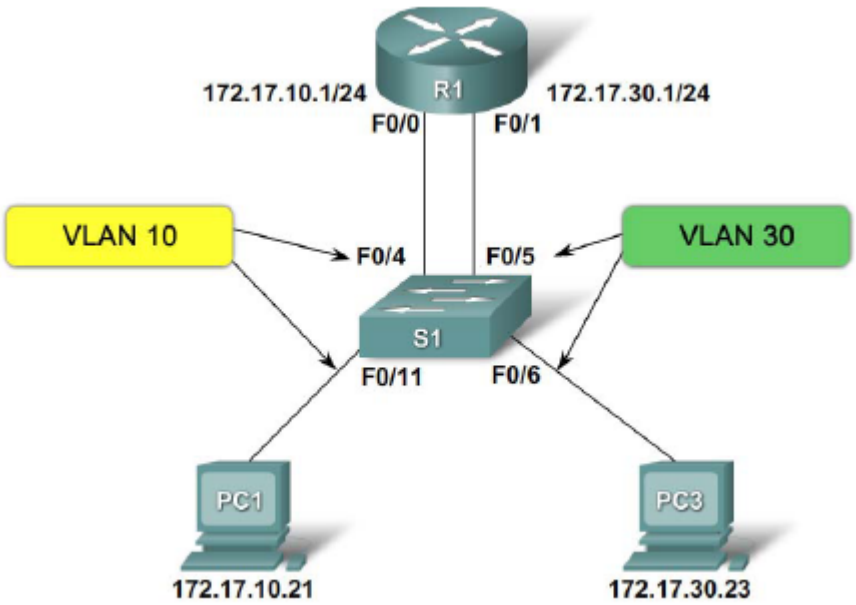
ROUTAGE INTER-VLAN

Le routage INTER-VLAN permet de router l'information entre les VLAN et donc de faire communiquer (sous conditions) les VLAN.

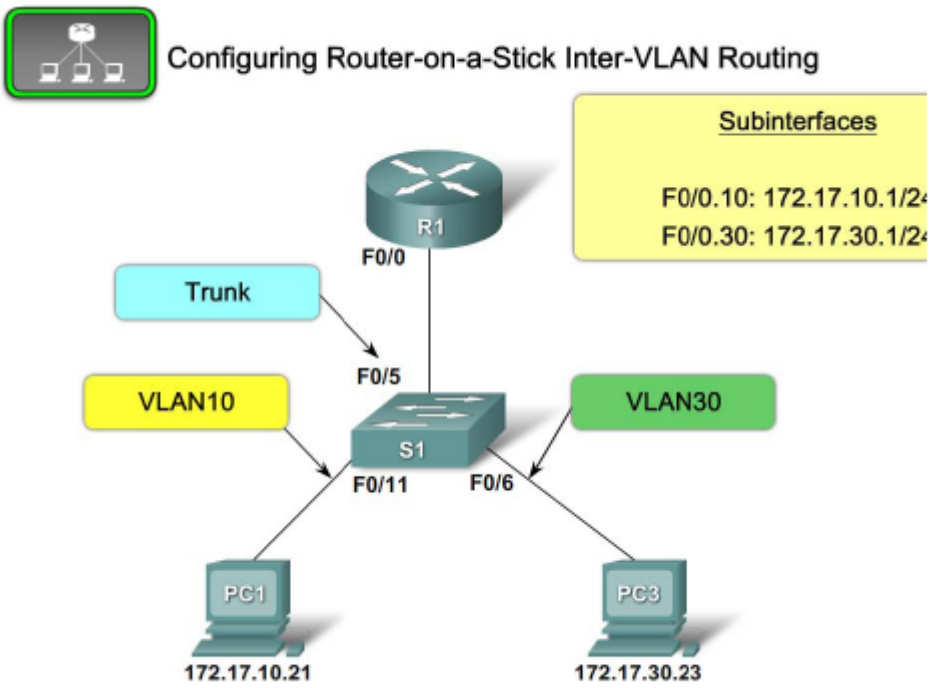
Le routage inter-VLAN nécessite un routeur ou un commutateur de niveau 3 (switch L3).

1 - Le routage inter-VLAN traditionnel (une interface physique par VLAN)

Le routeur doit posséder plusieurs interfaces physiques et chaque interface est connectée à un VLAN différent.



Configuration avec sous-interface du routage inter-VLAN (ROUTER ON THE STICK) : Une seule interface physique, plusieurs sous-interfaces logiques (une par VLAN)



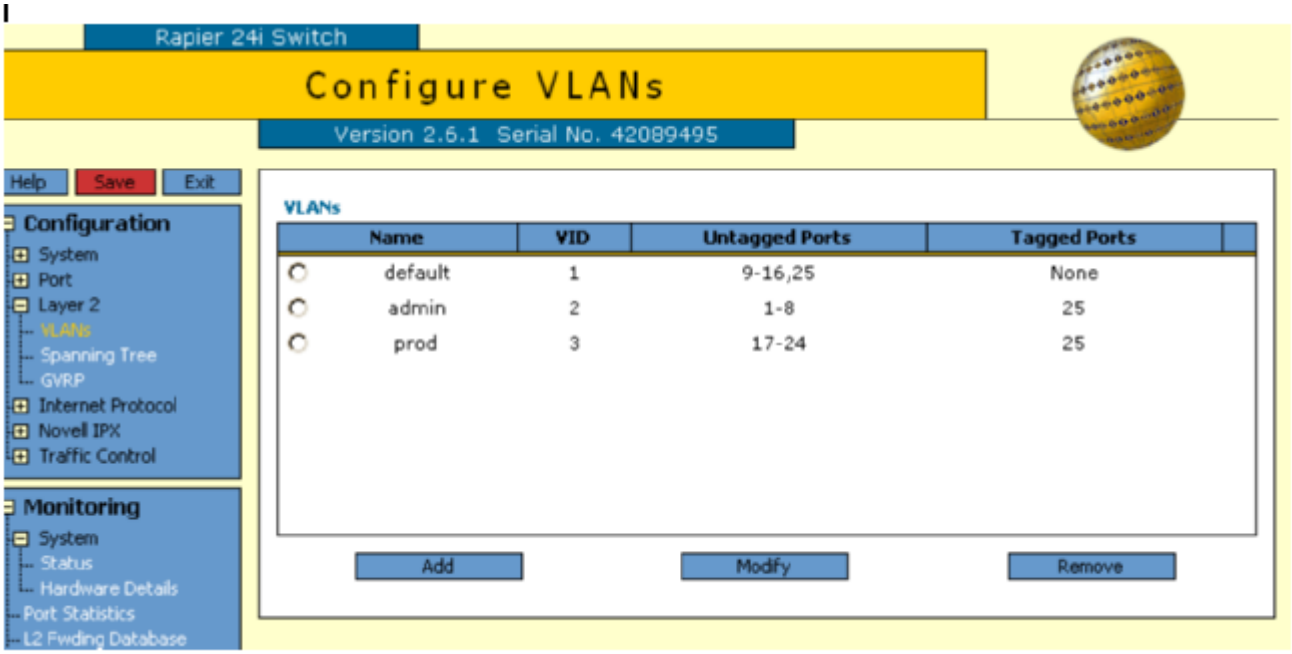
Rappel : le mode Trunk (appellation Cisco) est un lien 802.1q. Ici F0/0 et F0/5 sont des ports étiquetés 802.1q.

Interfaces ou sous-interfaces ? Avantages et désavantages.

- **Limite de quantité de ports :** les sous-interfaces permettent au routeur d'accommoder plus de VLANs que le nombre d'interfaces physiques disponibles.
- **Performance :** avec des interfaces, toute la bande passante est allouée au VLAN. Avec les sous-interfaces, le trafic de chacun des VLANs doit compétitionner pour la bande passante : goulot d'étranglement.
- **Coût :** un routeur possédant plusieurs interfaces est plus dispendieux. Chaque interface est connectée à un port différent sur le commutateur, donc le commutateur utilise plus de ports.
- **Complexité :** sous-interface, moins complexe physiquement, mais plus complexe au niveau de la configuration.

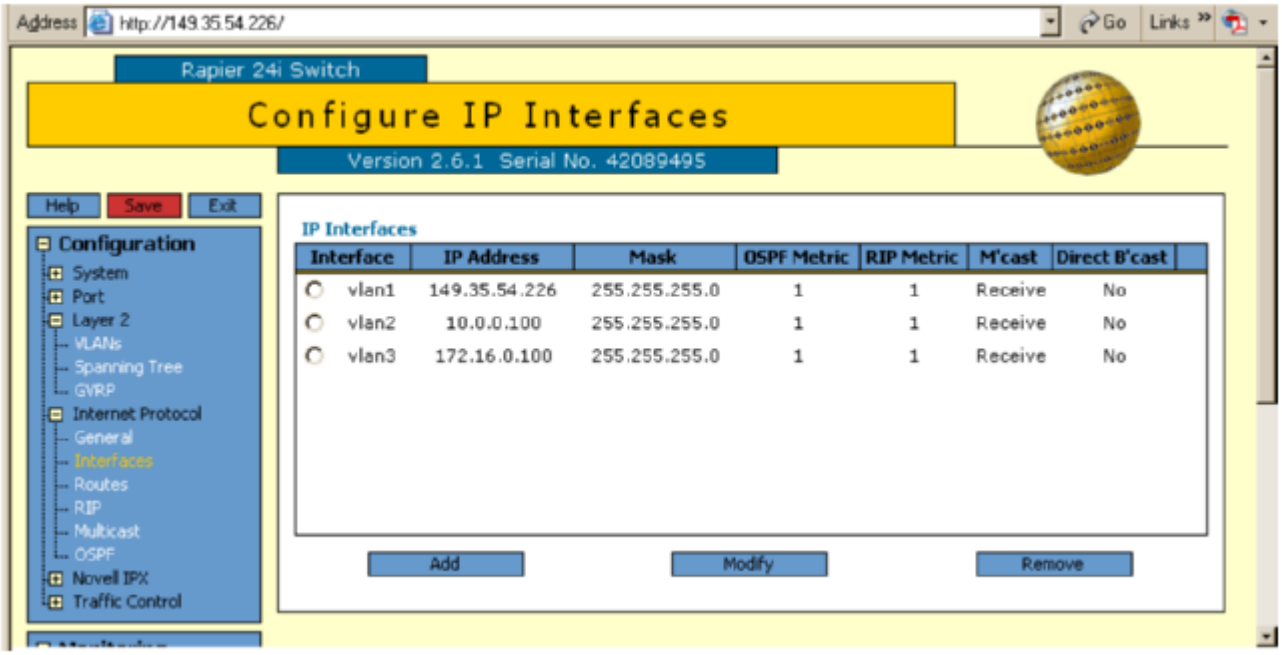
Solution « moderne » : utiliser un switch L3 !

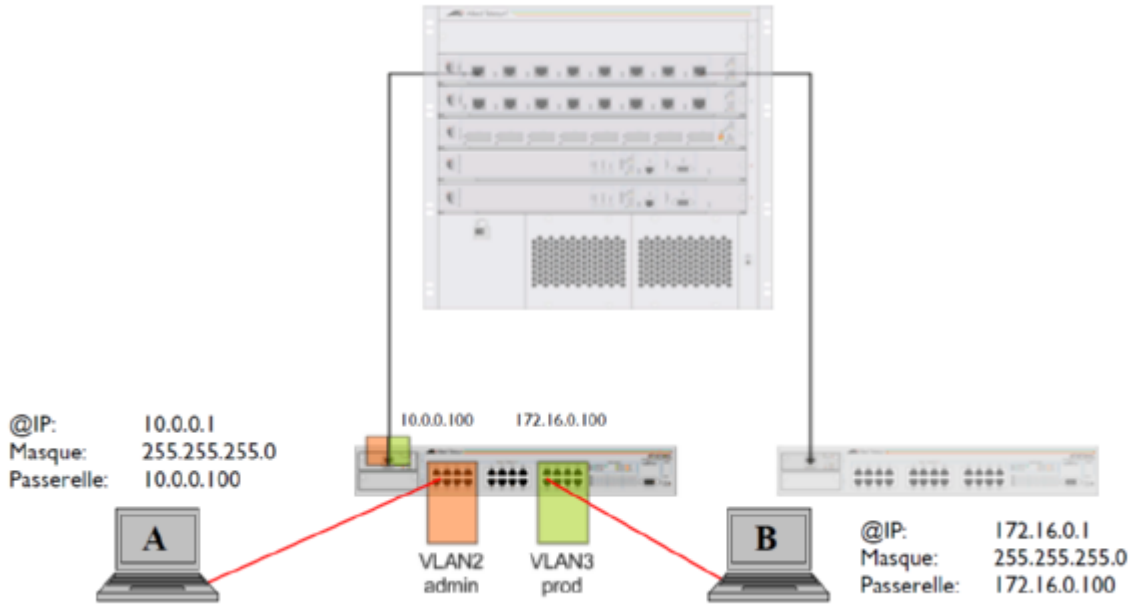
Etape 1 : configurer les VLAN



Suite à cela, vous avez donc trois VLANs (défault, admin, prod) qui ne peuvent communiquer ensemble.

Etape 2 : configurer les interfaces IP des VLAN





Une fois cette étape de configuration réalisée, toutes les communications sont possibles entre les VLANs si les stations sont correctement configurées. Une station appartenant au VLAN 2 devra avoir une adresse dans le même réseau IP que l'adresse affectée à l'interface VLAN 2 et l'adresse de sa passerelle par défaut est égale à l'adresse attribuée à l'interface VLAN 2. La même logique s'applique bien sûr aux stations de VLAN 1 et VLAN 3.

Etape 3 : Contrôler les communications inter-VLAN (via des ACL)

Il est fréquent de vouloir mettre en place des restrictions de trafic entre stations et/ou serveurs. Il est alors nécessaire de mettre en place un contrôle des communications, ou **A**ccess **C**ontrol **L**ists (**AC**Ls).

Dans l'exemple suivant, on peut souhaiter que, concernant les communications inter-VLAN, seules soient possibles les communications entre les stations A et B et ce uniquement en http.

La mise en place des ACLs se fait en deux étapes :

- L'**identification** des flux
- Une **action** sur les flux identifiés (**rejet** ou **acceptation**)

IDENTIFICATION DES FLUX

1. Les flux venant de VLAN 1 et allant vers VLAN 2
2. Les flux venant de VLAN 1 et allant vers VLAN 3
3. Les flux venant de VLAN 2 et allant vers VLAN 1
4. Les flux venant de VLAN 2 et allant vers VLAN 3
5. Les flux venant de VLAN 3 et allant vers VLAN 1
6. Les flux venant de VLAN 3 et allant vers VLAN 2
7. Les requêtes HTTP venant de A et allant vers B
8. Les requêtes HTTP venant de B et allant vers A
9. Les réponses HTTP venant de B et allant vers A
10. Les réponses HTTP venant de B et allant vers A

On se servira des adresses des équipements source et destination ainsi que du port applicatif (HTTP = 80) pour identifier ces 2 flux.

La gestion des ACL sera étudiée en détail dans le module SISR5

From:
https://siocours.lycees.nouvelle-aquitaine.pro/ - **Les cours du BTS SIO**

Permanent link:
https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/sisr2/r.inter-vlan

Last update: **2014/01/03 21:31**