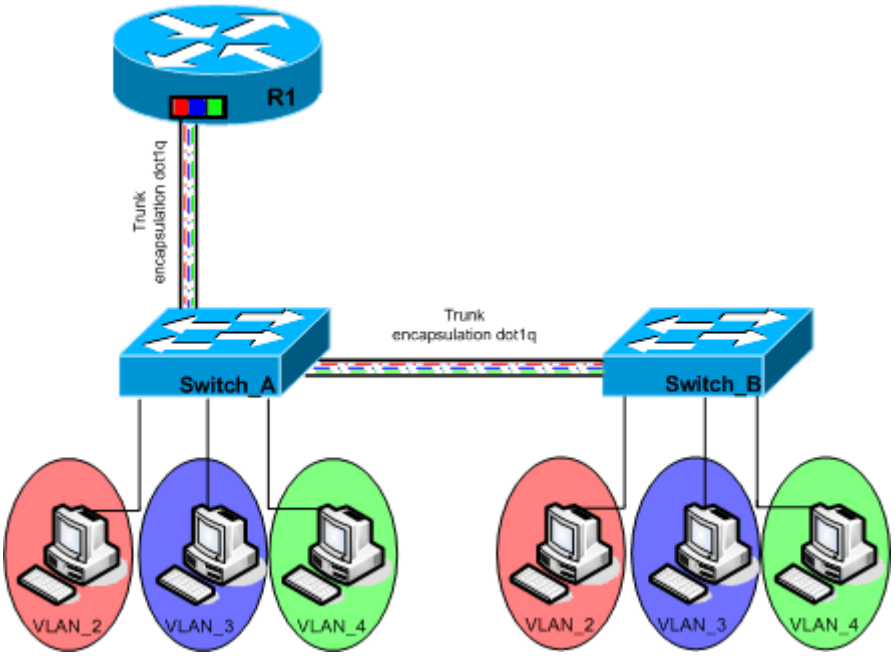
Article	: **VLAN**
de	: **Matthieu Vernerie**
Résumé	: Configuration d'un routage inter-VLAN

Introduction et rappels

Cet article a pour but d'expliquer et d'établir une configuration de routage inter-VLAN.



Bref rappel sur les VLANs et le VTP

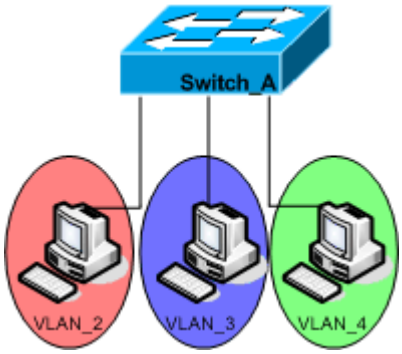
Un VLAN peut être assimilé à un domaine de broadcast. Typiquement, dans une configuration de VLAN, chaque VLAN comprend son propre sous-réseau. Sans équipement de couche 3, il est donc impossible pour les terminaux d'un VLAN de communiquer avec les terminaux d'un autre VLAN.

Le VLAN Trunking Protocol (VTP) est nécessaire si l'on veut étendre une configuration de VLAN sur plusieurs commutateurs. Un trunk est nécessaire pour une connexion entre deux commutateurs traitant des VLANs. Ce trunk représente un canal par lequel transitent les trames des différents VLANs d'un commutateur à un autre. Pour que les commutateurs "sachent" à quel VLAN appartient une trame, un étiquetage est nécessaire. C'est pourquoi on utilise un protocole d'étiquetage : ISL (Cisco) ou 802.1q (IEEE). Nous utiliserons ici le 802.1q qui est le protocole utilisé par défaut.

1. Configuration des VLANs

Pour l'exemple, les VLANs statiques seront utilisés. Chaque port de chaque commutateur va donc être attribué à un VLAN.

Pour la description des commandes, les accolades indiquent un paramètre (obligatoire), les crochets une option.



1.1 Création des VLANs

Pour créer un VLAN, il faut se trouver dans le mode de configuration correspondant, accessible par la commande :

Switch_A# **vlan database**

A partir de ce mode, la création d'un VLAN se fait par la commande :

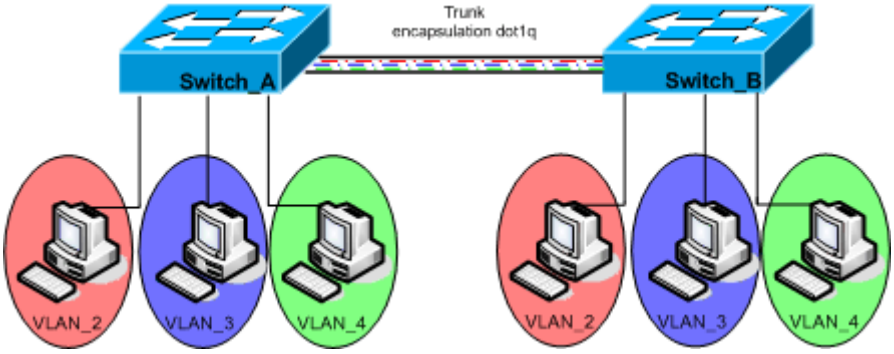
Switch_A(vlan)# **vlan {numéro} [name {nom}]**
Switch_A(vlan)# **exit**

Cette dernière commande permet d'enregistrer la configuration des VLANs, qui se trouve dans le fichier vlan.dat dans la mémoire Flash.
Dans une configuration de VLAN statique, les ports du commutateur doivent être attribués à un VLAN. Ceci se fait dans le mode de configuration de l'interface spécifiée :

Switch_A(config)#**interface fastEthernet {numéro_interface}**
on passe dans le mode de configuration de l'interface spécifiée
Switch_A(config-if)#**switchport mode access**
spécification du mode de l'interface
Switch_A(config-if)#**switchport access vlan {numéro}**
attribution du vlan spécifié à l'interface

La configuration est maintenant faite sur le commutateur Switch_A.

1.2 Configuration d'un domaine VTP



Pour propager cette configuration à un deuxième commutateur, ceux-ci doivent appartenir à un domaine commun : le domaine VTP. Ce domaine est organisé hiérarchiquement : le serveur VTP diffuse ses configurations VLAN, tandis que le client VTP met à jour sa configuration VLAN en fonction des informations reçues du serveur.
Considérons le commutateur Switch_A comme le serveur du domaine VTP, et le commutateur Switch_B comme le client. Les commandes nécessaires sont :

Switch_A# **vlan database**
Switch_A(vlan)# **vtp domain {nom_domaine}**
Switch_A(vlan)# **vtp server**
Switch_A(vlan)# **exit**

Switch_B# **vlan database**
Switch_B(vlan)# **vtp domain {nom_domaine}**
Switch_B(vlan)# **vtp client**
Switch_B(vlan)# **exit**

Enfin, un trunk est nécessaire entre ces deux équipements. C'est en effet par celui-ci que les trames étiquetées transitent. Entre deux commutateurs, un câble croisé doit être utilisé.
Un trunk est une connexion physique regroupant plusieurs connexions logiques. *Dans le schéma, un câble physique laisse transiter 3 trafics logiques différents. Ceux-ci représentent les trafics propres à chaque VLAN.*
L'encapsulation utilisée doit également être spécifiée, à moins que le commutateur utilisé n'accepte qu'un seul protocole. Chaque commutateur doit donc configurer une des ses interfaces pour accueillir un trunk :

Switch_A(config)# **interface fastEthernet {numéro_interface}**
Switch_A(config-if)# **switchport mode trunk**
Switch_A(config-if)# **switchport trunk encapsulation {dot1q | isl}**

Switch_B(config)# **interface fastEthernet {numéro_interface}**
Switch_B(config-if)# **switchport mode trunk**
Switch_A(config-if)# **switchport trunk encapsulation {dot1q | isl}**

A ce stade, la configuration VLAN du commutateur serveur est transmise au client. Il faut cependant assigner les ports du commutateur client aux VLANs spécifiés (la configuration transmise énumère seulement les VLANs crées et leurs noms) :

Switch_B(config)# **interface fastEthernet {numéro_interface}**
Switch_B(config-if)# **switchport mode access**
Switch_B(config-if)# **switchport access vlan {numéro}**

Désormais, chaque hôte peut communiquer avec un hôte du même VLAN, connecté sur un commutateur différent.

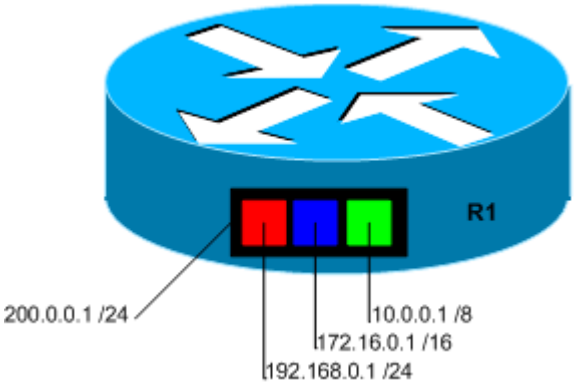
2. Configuration spécifique au routage inter VLAN

2.1 Sur le commutateur

Lorsque deux utilisateurs se trouvent sur des VLANS différents, ils se trouvent - en général - sur des sous-réseaux différents. Pour communiquer, ils doivent donc passer par une passerelle commune : l'interface du routeur connectée au commutateur. Pour spécifier au commutateur la passerelle utilisée pour "passer" d'un VLAN à un autre (ou plus généralement d'un sous-réseau à un autre), on utilise la commande :

Switch_A(config)# **ip default-gateway {adresse_ip}**

2.2 Sur le routeur La liaison routeur-commutateur constitue également un trunk. Cette connexion regroupe en effet plusieurs liens logiques : un trafic VLAN par sous-interface, sur une liaison physique : un câble droit connectant une interface du routeur à une interface d'un commutateur.



Chaque trafic de VLAN est supporté par une sous-interface du routeur. Il faut donc, pour chaque sous-interface, attribuer une adresse IP appartenant au sous-réseau du VLAN et spécifier l'encapsulation (étiquetage) utilisée:

R1(config)# **interface fastEthernet {sous-interface}**
R1(config-sub)# **encapsulation {dot1q | isl} {numéro_vlan}**
R1(config-sub)# **ip address {adresse_ip} {masque_sous_réseau}**

Chaque hôte peut désormais communiquer avec un hôte sur un VLAN différent. Lorsque le premier envoi une trame avec pour destination un sous-réseau différent du sous-réseau source, le commutateur l'encapsule et l'envoi à la passerelle par défaut. Après avoir traversé le trunk, la trame est traitée au niveau du routeur. Celui-ci la désencapsule, la réencapsule pour le VLAN de destination avant de l'envoyer sur la sous-interface correspondante.

3. Configuration complète

3.1 Configuration du switch_A

Création des VLANs

Switch_A# **vlan database**
Switch_A(vlan)# **vlan 2 name VLAN_2**
Switch_A(vlan)# **vlan 3 name VLAN_3**
Switch_A(vlan)# **vlan 4 name VLAN_4**
Switch_A(vlan)# **vtp domain cisco**
Switch_A(vlan)# **vtp server**
Switch_A(vlan)# **exit**

Création des trunk

Switch_A(config)# **interface fastEthernet 0/1**
Switch_A(config-if)# **switchport mode trunk**
Switch_A(config-if)# **switchport trunk encapsulation dot1q**
Switch_A(config-if)# **exit**

Switch_A(config)# **interface fastEthernet 0/8**
Switch_A(config-if)# **switchport mode trunk**
Switch_A(config-if)# **switchport trunk encapsulation dot1q**
Switch_A(config-if)# **exit**

Attribution des VLANs aux ports

Switch_A(config)# **interface fastEthernet 0/2**
Switch_A(config-if)# **switchport mode access**
Switch_A(config-if)# **switchport access vlan 2**
Switch_A(config-if)# **exit**
Switch_A(config)# **interface fastEthernet 0/3**
Switch_A(config-if)# **switchport mode access**
Switch_A(config-if)# **switchport access vlan 3**
Switch_A(config-if)# **exit**
Switch_A(config)# **interface fastEthernet 0/4**
Switch_A(config-if)# **switchport mode access**
Switch_A(config-if)# **switchport access vlan 4**
Switch_A(config-if)# **exit**

3.2 Configuration du switch_B

Adhésion au domaine cisco

Switch_B# **vlan database**
Switch_B(vlan)# **vtp domain cisco**
Switch_B(vlan)# **vtp client**
Switch_B(vlan)# **exit**

Création du trunk

Switch_B(config)# **interface fastEthernet 0/1**
Switch_B(config-if)# **switchport mode trunk**
Switch_B(config-if)# **switchport trunk encapsulation dot1q**
Switch_B(config-if)# **exit**

Attribution des VLANs aux ports
Switch_B(config)# **interface fastEthernet 0/2**
Switch_B(config-if)# **switchport mode access**
Switch_B(config-if)# **switchport access vlan 2**
Switch_B(config-if)# **exit**
Switch_B(config)# **interface fastEthernet 0/3**
Switch_B(config-if)# **switchport mode access**
Switch_B(config-if)# **switchport access vlan 3**
Switch_B(config-if)# **exit**
Switch_B(config)# **interface fastEthernet 0/4**
Switch_B(config-if)# **switchport mode access**
Switch_B(config-if)# **switchport access vlan 4**
Switch_B(config-if)# **exit**

3.3 Configuration du Routeur R1

R1(config)# **interface fastEthernet 0/0**
R1(config-if)# **ip address 200.0.0.1 255.255.255.0**
R1(config-if)# **exit**

R1(config)# **interface fastEthernet 0/0.2**
R1(config-subif)# **encapsulation dot1q 2**
R1(config-subif)# **ip address 10.0.0.1 255.255.255.0**
R1(config-subif)# **exit**

R1(config)# **interface fastEthernet 0/0.3**
R1(config-subif)# **encapsulation dot1q 3**
R1(config-subif)# **ip address 172.16.0.1 255.255.255.0**
R1(config-subif)# **exit**

R1(config)# **interface fastEthernet 0/0.4**
R1(config-subif)# **encapsulation dot1q 4**
R1(config-subif)# **ip address 192.168.0.1 255.255.255.0**
R1(config-subif)# **exit**

Conclusion Vous avez pu voir que pour réaliser un routage entre VLANs, il ne suffit pas de brancher un routeur sur un commutateur... Bien que la configuration paraisse longue, 15 min seront assez pour l'exécuter.
En espérant que cet article vous aura été utile.

Travaux Pratiques

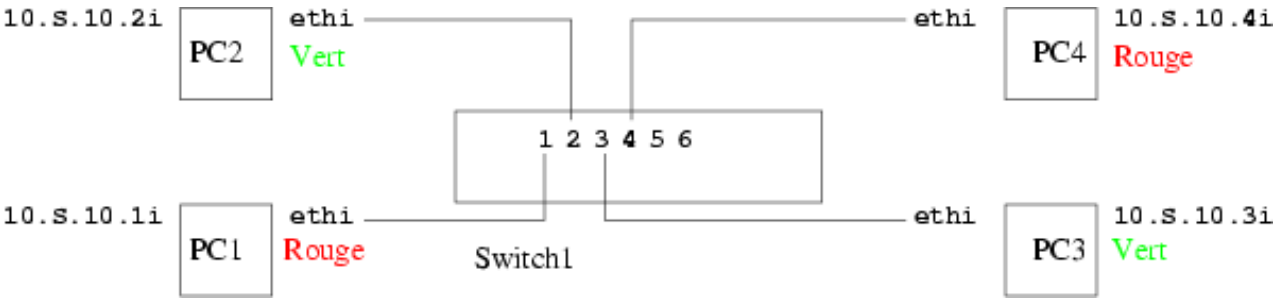
Commutation sur Ethernet - II

Fonctions avancées: VLAN, Trunk

Ce TP a pour but de mettre en oeuvre et observer quelques fonctionnalités avancées de la commutation sur Ethernet avec un ou plusieurs commutateurs (switchs). Nous utiliserons ici des switchs de type HP ProCurve.

Exercice 1 - Domaines de diffusion

En prenant un switch pour quatre PC, réaliser le montage suivant.



1. Donner une adresse IP aux interfaces ethernet des PC de sorte qu'ils puissent communiquer entre eux (utilisez les adresses IP données dans la figure avec un masque d'adresse de `255.255.255.0`, sachant que `S` représente le numéro de votre salle, `65` ou `69`, et que le *i* de `ethi` représente le numéro de l'interface réseau que vous utilisez pour vous connecter au switch, différente de celle qui vous permet d'accéder au réseau extérieur).
2. Vérifier l'état de la table d'adressage du switch et regarder le trafic sur chacune des interfaces des PC (avec `tcpdump` ou `ethereal`), en particulier lors de ping entre les différents PC.
3. En l'absence de toute information dans la table d'adressage du switch, vérifier que tous les PC voient les messages ICMP générés par un ping, y compris les trames unicast.
4. Vérifiez que lorsque le switch dispose de l'association, seules les deux machines concernées par le ping voient le trafic. Que se passe-t-il alors si la machine réalisant le ping n'a plus rien dans sa table ARP ?

Exercice 2 - VLANs non taggés

On désire maintenant que le trafic entre PC1 et PC4 soit complètement différencié du trafic entre PC2 et PC3, c'est à dire qu'aucun échange ni observation ne puisse avoir lieu entre ces deux *réseaux locaux virtuels*. Pour cela, on peut créer deux VLANs distincts: le VLAN *rouge* pour PC1 et PC4 et le VLAN *vert* pour PC2 et PC3. Ce sont des VLANs *par port*, compatibles avec la norme IEEE 802.1Q. En l'absence de toute configuration, les switchs considèrent que tous les ports font partie du même VLAN par défaut.

1. Autoriser les VLANs

Dans le menu principal d'administration du switch, aller dans `Switch Configuration`, éventuellement `Advanced Features` pour les anciens modèles, puis `VLAN Menu` et finalement `VLAN Support`. Pour les anciens modèles, choisir `Yes` dans le champ `Activate VLANs` et sauvegarder (le nombre de VLAN de 8 par défaut peut être modifié). L'astérisque qui apparaît indique alors qu'il faut rebooter le switch pour prendre en compte cette configuration. Donc, rebooter le switch (à partir du menu principal).

2. Définir les VLANs

Ensuite, dans le menu VLAN, faire `VLAN Names` et ajouter les deux VLANs, le rouge et le vert. Par défaut, tous les ports du switch appartiennent au `DEFAULT_VLAN` qui a `1` pour numéro (`VLAN ID`). Il est important de **ne pas modifier ce VLAN par défaut**. Donner des VLAN ID différents pour les VLAN créés. Par exemple, `20` pour le VLAN **rouge** et `30` pour le VLAN **vert**.

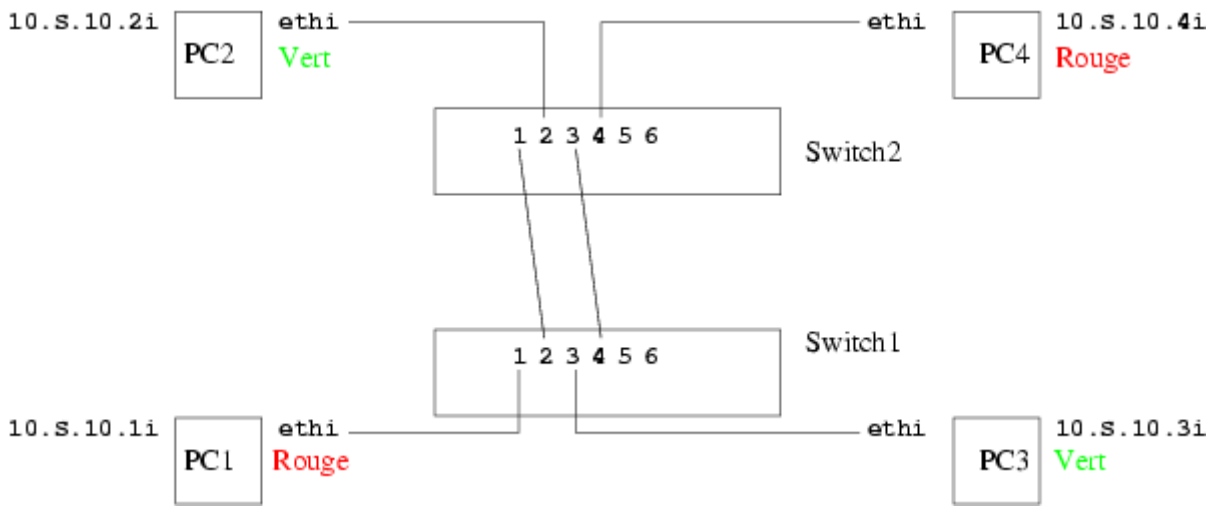
3. Assigner les ports aux VLANs

Dans le menu VLAN, faire `VLAN Port Assignment`. Chaque port est alors proposé pour chaque VLAN (défaut, rouge, vert), et *taggé* ou non. Dans un premier temps, utiliser les VLAN rouge et vert *sans les tagger*. Associer le rouge aux ports reliant le PC1 et le PC4 et le vert aux ports reliant le PC2 et le PC3.

4. Tester alors la communication entre les différents PC et regarder l'activité du trafic sur les différentes interfaces, comme dans l'exercice 1. Expliquer ce qui se passe.
5. Vérifier en particulier si les broadcasts ARP générés par un ping d'une machine sur un VLAN atteignent ou non les machines de l'autre VLAN.

Exercice 3 - VLANs non taggés entre deux switchs

On désire maintenant ajouter un second switch et répartir les machines comme indiqué dans la figure suivante. On désire toujours n'utiliser que des VLANs non taggés.



1. Pourquoi placer deux liens entre les switchs ?
2. Comment configurer les switchs et quelles sont les modifications à apporter aux associations ports/VLAN?
3. Configurer correctement ce montage. Vérifier quelles communications sont possibles entre chaque PC et les trafics visibles sur chaque interface (unicast et broadcast).

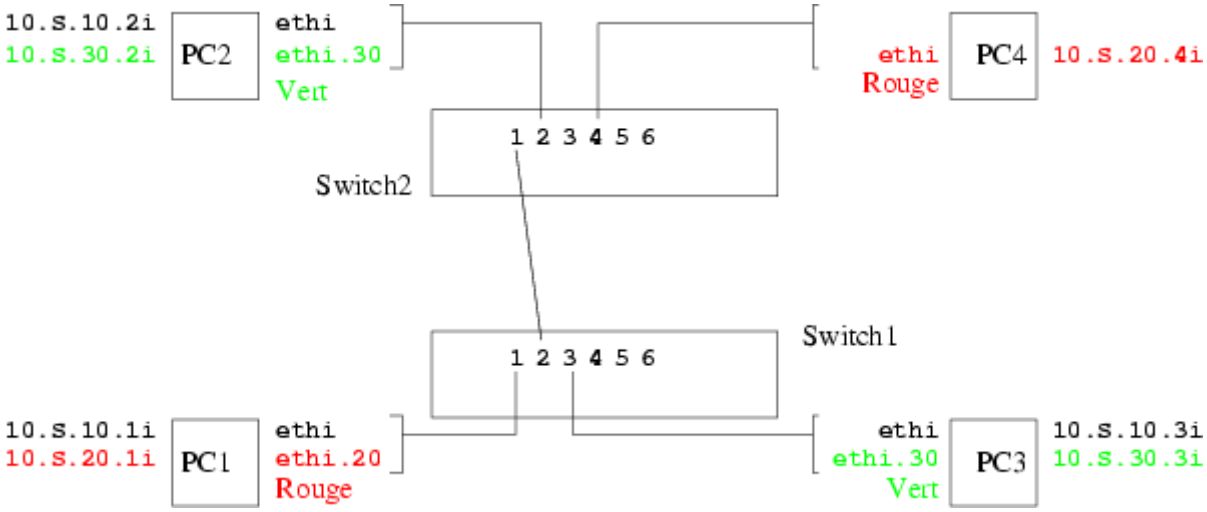
Exercice 4 - VLANs et Spanning Tree

Y a t il une boucle dans cette configuration et un risque d'inondation par les switchs eux-mêmes. Pourrait il y en avoir avec d'autres interfaces raccordées à ces switchs. Que se passerait-il dans la configuration actuelle si on mettait en oeuvre le STA ?

Exercice 5 - VLANs taggés

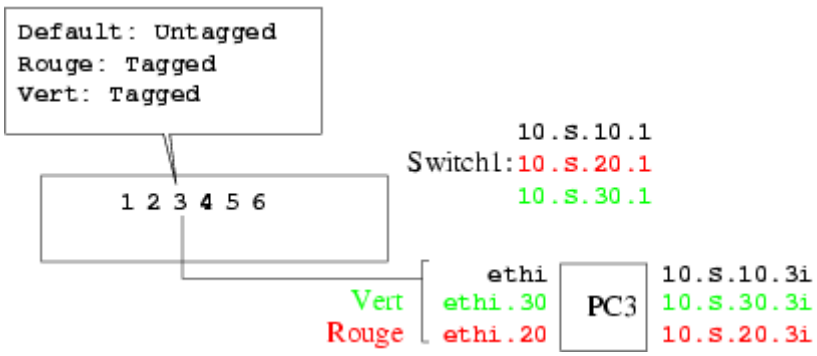
Supposons maintenant que l'on veuille un seul lien entre les deux switchs. Cela nécessite que les trafics des VLANs rouge et vert passent par ce même lien, et donc que ses deux ports soient associés à la fois au VLAN rouge et au VLAN vert. Cela n'est pas possible si les 2 VLANs sont non taggés. **Note:** Un port peut appartenir à plusieurs VLANs, mais un seul (au plus) de ces VLANs peut être non taggé.

1. Modifier les associations entre les VLANs et les ports de sorte que les VLANs rouge et vert soient *taggés* tous les deux entre les deux switchs. Vérifier quelles communications sont possibles entre les PC et quels trafics (unicast et broadcast) sont visibles.
2. Vérifiez que si le port reliant un switch à un PC est taggé, alors le switch ne laisse pas entrer les trames (non taggées) émises par ce PC.
3. Pour configurer une interface de PC de sorte qu'elle émette et accepte les VLAN taggés, il faut créer une nouvelle interface logique. Du point de vue des systèmes, il faut disposer d'un noyau linux compatible avec la norme 820.1Q sur les VLANs qui fournit les utilitaires nécessaires. Vous aurez besoin de la commande `vconfig` (`apt-get install vlan`) et de charger le module `8021q` (`modprobe 8021q`). Par exemple, pour le PC4 :
    - Ajout d'une nouvelle interface logique `ethi.20`, correspondant au VLAN rouge (dont le VLAN ID est 20), sur l'interface physique `ethi`: `vconfig add ethi 20`. Tant que l'interface n'est pas montée, elle n'est pas visible par la commande `ifconfig`.Pour la voir, il faut donc faire `ifconfig -a`.
    - Le montage de cette interface logique se fait alors classiquement: `ifconfig ethi.20 ... up`
4. Vérifier qu'un PC « VLAN aware » qui émet des trames taggées peut communiquer avec un PC « legacy » à travers les switchs. Faire attention aux routes et aux adresses de chaque interface des PC. Décrire alors la configuration que vous avez utilisée en expliquant quels sont les problèmes liés aux adresses IP et aux routes.
5. Vérifier que deux PC « VLAN aware » peuvent communiquer. Décrire la configuration que vous avez utilisée.
6. Réaliser la configuration décrite par la figure suivante, et vérifier quelles sont les communications possibles, dans quels mode (taggé, non taggé...) et quels trafics sont visibles par quels PC (unicast, broadcast).



Exercice 6 - VLANs et serveur

On suppose maintenant que le PC3 est un serveur qui doit pouvoir communiquer avec les deux VLANs. Néanmoins, on veut conserver les deux VLANs avec des trafics distincts. Pour cela, on peut associer une deuxième interface logique de VLAN (rouge) au PC3 (sur la même interface physique ou sur une autre). Réaliser l'exemple de configuration ci-dessous, et vérifier qu'il est possible, à partir du PC3, de communiquer avec le VLAN rouge, le VLAN vert et le VLAN par défaut.
Note: dans certains cas (désormais rares) de multiples interfaces logiques sur une même interface physique, on peut être amené à donner "à la main" des routes au PC (commande `route`).



Exercice 7 - Port Trunking

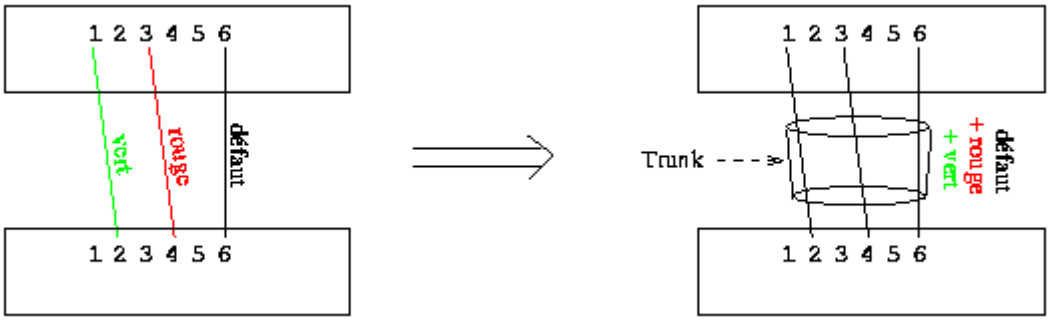
Le *port trunking* est la faculté d'*associer* plusieurs liens (jusqu'à 4) entre 2 switchs en une sorte de congrégation de liens. Les différents liens constituant ce trunk seront alors utilisés simultanément, permettant ainsi d'augmenter le débit inter-switch. La distribution du trafic sur chacun des liens du trunk est effectuée sur la base d'une résolution d'adresse source et/ou destination, voir d'une négociation. Au pire des cas, même si c'est rare, il se peut donc qu'un lien du trunk soit saturé tandis que les autres sont inutilisés.

Du point de vue du switch, la connexion à un trunk est vue comme un seul port. Par exemple, le STA décide soit de transmettre sur tous les liens du trunk, soit de bloquer tous les liens. De même, tous les ports des liens d'un même trunk doivent appartenir aux mêmes VLANs.

La figure suivante illustre une utilisation du trunk: dans la configuration de l'exercice 3 (voir figure), nous avions des liens entre 2 switchs. VLAN rouge uniquement du port 1 au port 2 et VLAN vert uniquement du port 3 au port 4. On peut imaginer qu'il aurait été utile (pour l'administration des switchs, par exemple) d'avoir un lien du port 6 au port 6 pour le VLAN par défaut.

Placer ces trois liens dans un seul trunk permet d'éviter d'avoir des boucles entre les switchs (sans utiliser le STA qui n'est pas adapté ici), tout en conservant les trois liens disponibles. Le seul pré-requis est de créer un trunk dont les caractéristiques regroupent toutes celles des liens qui le constituent: il doit appartenir au VLAN rouge, au VLAN vert et au VLAN par défaut. C'est possible puisque seul le VLAN par défaut est non taggé.

Réaliser ce montage et tester les communications et le trafic.



Etienne.Duris[at]univ-mlv.fr -