

Ministère de l'enseignement supérieur et de la recherche scientifique  
Institut Supérieur des Études Technologiques de Zaghuan  
Département Technologies de l'Informatique



Module  
**Réseaux Locaux d'Entreprises  
& Architecture TCP/IP**  
Chapitre 4  
Les VLANs

Elaboré par  
**RimBRAHMI**

Public cible  
**2<sup>ème</sup> année Licence Appliquée en Réseaux et Services  
Informatiques**

Année universitaire 2019-2020

**Table de matières**

Chapitre 4 : Les VLANs.....	4
Leçon 1 :Les VLANs .....	5
Introduction .....	6
I. Les VLANs .....	6
I.1. Les limites des LANs .....	6
I.2. Présentation des VLANs .....	6
I.3. Importance .....	7
I.4. Les avantages .....	8
I.5. Les types des VLANs.....	8
I.5.1. VLAN par défaut (VLAN 1).....	8
I.5.2. VLAN natif .....	9
I.5.3. VLAN de gestion .....	9
I.5.4. VLAN de données.....	9
I.5.5. VLAN voix.....	9
I.6. Les techniques des VLANs.....	9
I.6.1. VLAN de niveau 1(par port) .....	9
I.6.2. VLAN de niveau 2 (MAC) .....	10
I.6.3. VLAN de niveau 3 (adresses réseaux) .....	10
II. Les types des liaisons.....	12
II.1. Liaison d'accès .....	12
II.2. Liaison trunk.....	12
III. Les types de ports .....	12
III.1. Port accès.....	12
III.3. Port trunk.....	13
IV. Trunk des VLANs .....	13
IV.1. Principe .....	13
IV.2. VLAN native et étiquetage 802.11Q.....	13
III. Les attaques sur les VLANs .....	15
III.1. Attaque double tagging.....	15
III.2. Attaque usurpation du commutateur .....	15
III.3. Périphérie PVLAN .....	15
IV. Bonne pratique pour la conception d'un VLAN .....	15

V. Activité .....	16
Conclusion.....	16
Leçon 2 : Routage inter VLAN .....	17
Introduction .....	18
I. Fonctionnement du routage inter-VLAN .....	18
II. Les méthodes du routage inter-VLAN.....	18
II.1. Les méthodes de routage inter-VLAN au niveau du routeur .....	18
II.1.1. Ancienne méthode de routage inter-VLAN (Legacy inter-VLAN).....	18
II.1.2. La méthode « router on a stick ».....	19
II.2. Les techniques de routage au niveau des commutateurs niveau 3 .....	21
II.2.1. Interface SVI.....	21
II.2.2. Ports routés .....	22
Conclusion.....	23
Leçon 3 : Agrégation des liens .....	24
Introduction .....	25
I. Agrégation des liens .....	25
I.1. Présentation.....	25
I.2. Avantages de l'Ether Channel.....	26
II. Fonctionnement de l'EtherChannel .....	26
II.1. Restrictions d'implémentation .....	26
II.2. Protocoles d'agrégation des Liens .....	26
II.2.1. LACP (Link Aggregation Control Protocol) .....	26
II.2.2. PAgP : Port Aggregation Protocol propriétaire Cisco .....	27
III. Configuration du protocole EtherChannel.....	27
Conclusion.....	30

## Chapitre 4 : Les VLANs

### Vue d'ensemble

Ce chapitre donne une présentation générale sur les réseaux locaux virtuels (VLAN), les types des liaisons et ports, les techniques des VLANs, le routage inter-VLAN ainsi que l'agrégation des liens.

### Objectifs

- Comprendre les VLANs et leurs types
- Identifier les types des liaisons et des ports.
- Comprendre la norme 802.1Q
- Connaitre les diverses méthodes de routage inter-VLAN
- Comprendre l'agrégation des liens

### Prérequis

U.E Fondement réseaux, U.E Architecture et système I

### Durée de déroulement

- 4.5h de cours
- 1 séance de TD

### Elements de contenu

- Les VLANs
- Le routage inter-VLAN
- L'agrégation des liens

**Leçon 1 : Les VLANs**

▪ <b>Objectif Général</b>	<ul style="list-style-type: none"><li>• Connaître les diverses caractéristiques des réseaux locaux virtuels des réseaux locaux d'entreprises.</li><li>• Comprendre la fonction des VLAN dans un réseau commuté.</li></ul>
▪ <b>Objectifs Spécifiques</b>	<ul style="list-style-type: none"><li>• Identifier les diverses techniques des VLANs.</li><li>• Comprendre les diverses attaques sur un VLAN.</li><li>• Identifier les meilleures pratiques de sécurité pour un environnement segmenté.</li><li>• Comprendre les liaisons trunk entre les VLANs.</li></ul>
▪ <b>Volume horaire</b>	<ul style="list-style-type: none"><li>• Cours : 1.30h</li></ul>
▪ <b>Mots clés</b>	<ul style="list-style-type: none"><li>• VLAN, VLAN1, VLAN natif, VLAN de données, VLAN voix, Liaison trunk, IEEE 802.1Q, VLAN niveau 1, niveau 2, niveau 3...</li></ul>

## Introduction

Les réseaux Ethernet présentent des problèmes qui affectent les performances des réseaux **locaux** qui constituent un facteur important dans la productivité d'une entreprise, à savoir les collisions et la latence des équipements réseaux. L'une des solutions permettant de les améliorer consiste à **diviser de vastes domaines de diffusion en domaines plus petits**.

Un réseau local virtuel (VLAN) peut être **créé sur un commutateur de couche 2 pour réduire la taille des domaines de diffusion**, de sorte qu'elle **soit équivalente à celle d'un périphérique de couche 3**. Les VLANs sont généralement intégrés à la conception du réseau, ce qui permet à ce dernier de **s'adapter aux objectifs d'une entreprise**. Alors que **les VLAN sont principalement utilisés dans des réseaux locaux commutés**, les implémentations modernes leur permettent d'accéder aux réseaux métropolitains et étendus.

## I. Les VLANs

### I.1. Les limites des LANs

Au fur et à mesure les réseaux locaux se développent, le trafic échangé entre les stations augmente. Il n'y a pas de réelle frontière dans un réseau en expansion, ce qui provoque des interruptions et une utilisation croissante de trafic. **La solution Classique consiste à implémenter un routeur au sein du réseau local pour générer des domaines de diffusion** et cela entraîne des charges supplémentaires et aussi l'équipement de couche 3 (routeur) **ne fournit pas un débit efficace que celui fourni par les commutateurs**, ce qui entraîne des **goulots d'étranglement** aux points de transit entre les domaines de diffusions.

### I.2. Présentation des VLANs

Ce n'est pas une nouvelle norme de réseau local, mais une **méthode pour gérer les réseaux locaux**. Il s'agit plus de **superviser le réseau**. Les VLAN (Virtual Local Area Network) constituent une **étape importante dans la gestion d'un grand réseau**. Beaucoup de temps est passé pour séparer physiquement les réseaux dans les panneaux de brassage.

En général, **un grand réseau n'est pas un réseau tout à plat, mais une série de réseaux croisés physiquement et interconnectés par des routeurs**. **Lorsqu'un utilisateur se déplace ou un bureau change d'affectation, il faut se déplacer pour modifier le panneau de brassage, de manière à mettre ce bureau sur un autre hub**.

Avec les VLANs, qui prennent tous leurs poids avec les commutateurs et leur généralisation. Il est possible, à partir d'une station de supervision, de grouper les utilisateurs entre eux sans se déplacer. Le résultat est identique à une séparation physique. Un utilisateur ne pourra pas faire partager d'information avec un collègue d'un autre service.

Un VLAN (Virtual Local Area Network) est un réseau local regroupant un ensemble de machines de façon logique et non physique. Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage), en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole).

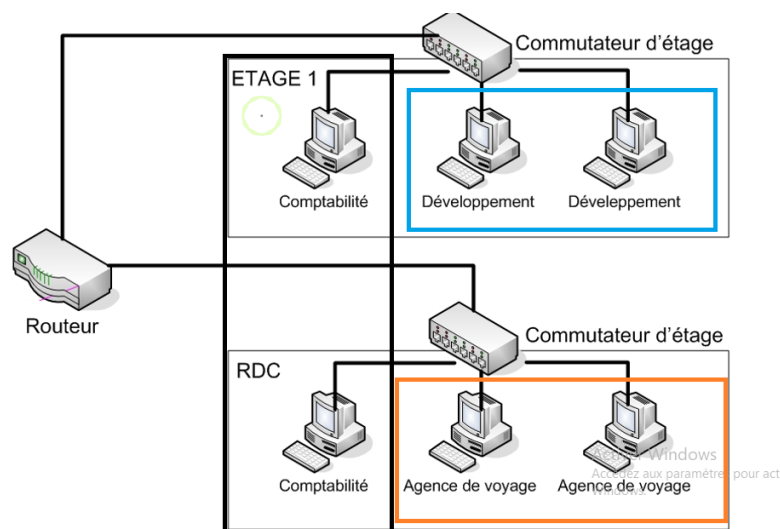


Figure 4.1. 1 : Exemple de VLAN

### I.3. Importance

Dans un réseau commuté, les VLAN assurent la segmentation et favorisent la flexibilité de l'entreprise en offrant des groupes des périphériques dans un LAN. Ces groupes des appareils communiquent comme s'ils étaient reliés au même câble. Les VLANs reposent sur des connexions logiques, et non des connexions physiques.

La mise en place des VLANs permet de segmenter le réseau local d'une entreprise en fonction en se basant sur des facteurs citant la fonction, l'équipe de projet ou l'application quel que soit l'emplacement du périphérique. Les équipements d'un VLAN, qui est considéré comme un réseau logique distinct, se comportent comme s'ils partagent une infrastructure commune avec d'autres VLANs. Les trames de monodiffusion, de diffusion et de multidiffusion se sont transférées que vers les équipements font partie au VLAN d'où elles proviennent.

#### I.4. Les avantages

La mise en place des VLANs au sein d'une entreprise offre des atouts considérables afin d'accroître la réussite et la croissance de l'entreprise citant :

- **La sécurité** : les équipements contenant des données critiques sont groupés dans un VLAN. Cela diminue le risque de violation de confidentialité.
- **Meilleures performances** :
- **Reduction des couts** : minimisation de mise a niveau du reseau et une utilisation efficace de la bande passante.
- **Reduction de la taille des domaines de diffusion** : la mise en place des VLANs au sein d'un reseau local diminue le nombre des équipements dans le domaine de diffusion.
- **Facilite de gestion de reseau** : une gestion facile de reseau est garantie par des équipements ayant des besoins similaires partagent le même VLAN et lors de l'ajout d'un nouveau commutateur, toutes les stratégies déjà configurées pour le VLAN sont implémentées lorsque les ports sont places.
- **Gestion simplifie des applications et des projets** : La séparation des fonctions facilite la gestion d'un projet ou l'utilisation d'une application spécialisée.

#### I.5. Les types des VLANs

Nous distinguons des divers types de VLANs utilisés dans les locaux modernes. Certains types de VLANs sont déterminés par les classes de trafic et d'autres par leur fonction spécifique

##### I.5.1. VLAN par défaut (VLAN 1)

Tous les ports de commutateur font partie du VLAN par défaut après le démarrage initial d'un commutateur chargeant la configuration par défaut. Les ports de commutateur qui participent au VLAN par défaut appartiennent au même domaine de diffusion.

Le VLAN 1 dispose de toutes les fonctions de n'importe quel VLAN, à l'exception du fait qu'il ne peut pas être renommé ni supprimé. Par défaut, tout le trafic de contrôle de couche 2 est associé au VLAN 1.



### **I.5.2. VLAN natif**

Un VLAN natif est affecté à un port d'agrégation 802.1Q. Les ports d'agrégation sont les liaisons entre les commutateurs qui prennent en charge la transmission du trafic associée à plusieurs VLAN. Un port d'agrégation prend en charge le trafic provenant de nombreux VLAN (trafic étiqueté), ainsi que le trafic qui ne provient pas d'un VLAN (trafic non étiqueté). Le port d'agrégation place le trafic non étiqueté sur le VLAN natif, qui par défaut est le VLAN 1.

### **I.5.3. VLAN de gestion**

Un VLAN de gestion est configuré pour accéder aux fonctionnalités de gestion d'un commutateur. Le VLAN 1 est le VLAN de gestion par défaut. Pour créer le VLAN de gestion, l'interface virtuelle du commutateur (SVI) de ce VLAN se voit attribuer une adresse IP et un masque de sous-réseau, ce qui permet de gérer le commutateur via HTTP, Telnet, SSH ou SNMP.

### **I.5.4. VLAN de données**

Un VLAN de données est un VLAN configuré pour transmettre le trafic généré par l'utilisateur. Les VLANs de données sont utilisés pour diviser un réseau local en groupes d'utilisateurs.

### **I.5.5. VLAN voix**

La fonction VLAN voix permet aux ports du commutateur d'acheminer le trafic VoIP (voix sur IP) provenant d'un téléphone IP. Puisque la qualité audio de la téléphonie IP peut se détériorer si la transmission des données est inégale, le commutateur prend en charge la qualité de service (QS).

## **I.6. Les techniques des VLANs**

Il existe trois types des VLANs

### **I.6.1. VLAN de niveau 1(par port)**

Nous affectons chaque port des commutateurs à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminée par sa connexion à un port du commutateur. Les ports sont donc affectés statiquement à un VLAN. Les ports des commutateurs sont associés à des VLANs.

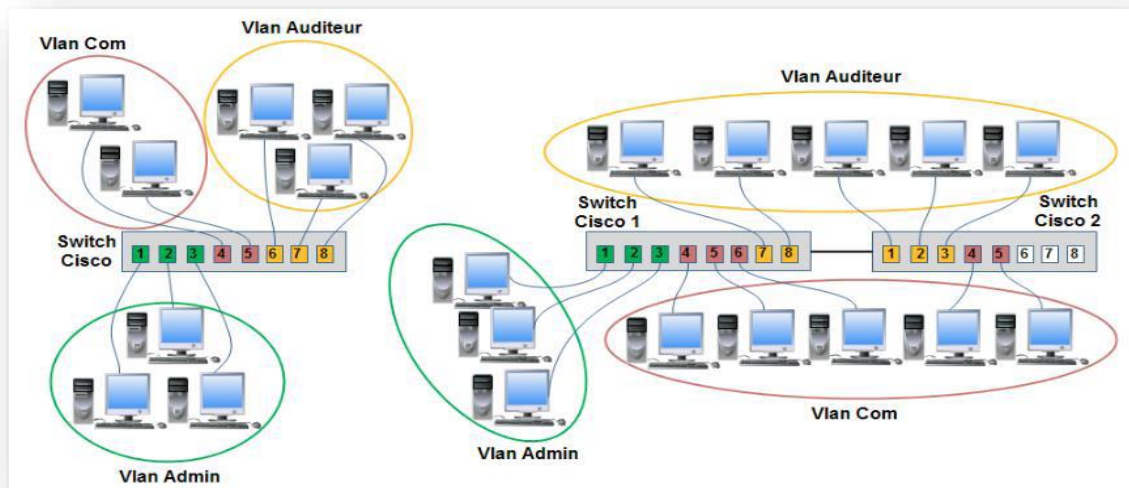


Figure 4.1. 2: VLAN par port

### I.6.2. VLAN de niveau 2 (MAC)

Nous affectons chaque adresse MAC à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminée par son adresse MAC. En fait il s'agit à partir de l'association MAC/VLAN d'affecter dynamiquement les ports des commutateurs à chacun des VLAN.

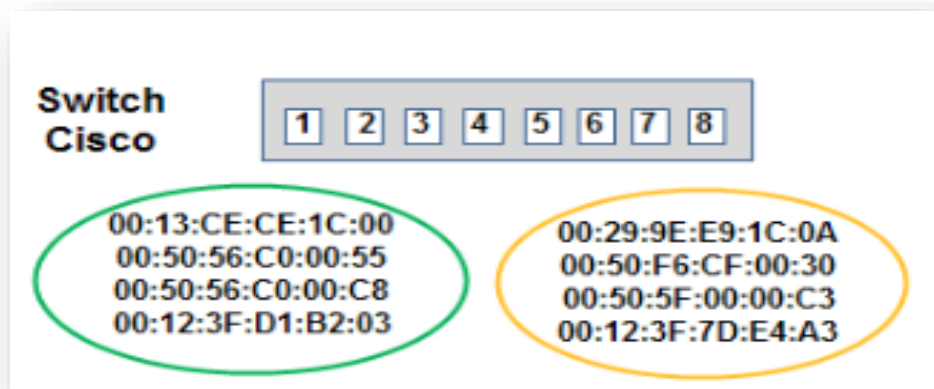


Figure 4.1. 3: VLAN par adresse MAC

### I.6.3. VLAN de niveau 3 (adresses réseaux)

Nous affectons un protocole de niveau 3 ou de niveau supérieur à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminée par le protocole de niveau 3 ou supérieur qu'elle

utilise. En fait, il s'agit à partir de l'association protocole/VLAN d'affecter dynamiquement les ports des commutateurs à chacun des VLAN.

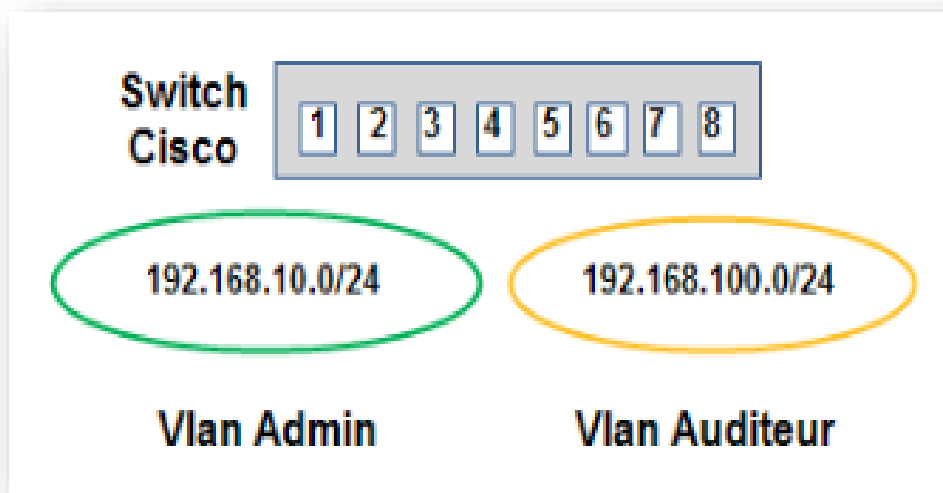


Figure 4.1. 4 : VLAN par adresse IP

#### Tableau comparatif des types de VLANS

Types de VLANS	Description
VLAN niveau 1 basé sur le port	<ul style="list-style-type: none"> <li>• Configuration la plus courante</li> <li>• Ports affectés individuellement à un ou plusieurs VLANs,</li> <li>• Mise en place facile</li> <li>• Couplé à DHCP,</li> </ul> <p>Les VLAN par ports offrent une bonne flexibilité</p> <ul style="list-style-type: none"> <li>• Les interfaces de gestion des commutateurs permettent une configuration facile</li> </ul>
VLAN niveau 2 basé sur l'adresse MAC	<ul style="list-style-type: none"> <li>• Rarement utilisé</li> <li>• L'adresse MAC détermine l'appartenance à un VLAN</li> <li>• Les commutateurs s'échangent leurs tables d'adresses MAC ce qui peut ralentir les performances</li> <li>• Difficile à administrer,</li> <li>• Difficile à dépanner</li> </ul>

VLAN niveau 3 basé sur le protocole	<ul style="list-style-type: none"> <li>• Pas utilisé aujourd'hui à cause de la présence de DHCP</li> <li>• L'adresse IP (sous-réseau) détermine l'appartenance à un VLAN</li> </ul>
-------------------------------------	---

## II. Les types des liaisons

Les liaisons peuvent être classées en deux, des liaisons d'accès et des liaisons trunk.

### II.1. Liaison d'accès

Une liaison d'accès permet de relier un système d'extrémité et un commutateur participant à un VLAN. Les liaisons entre les équipements terminaux et les commutateurs sont toutes des liens d'accès.

### II.2. Liaison trunk

Une liaison trunk est un lien sur lequel les trames étiquetées de VLAN sont susceptibles d'être transmises. Les liaisons entre les commutateurs sont généralement des liaisons trunk.

## III. Les types de ports

### III.1. Port accès

Les ports d'accès sont ceux par lesquels une trame entre et ressort d'un réseau VLAN. Lorsqu'un port d'accès reçoit une trame, celle-ci ne comporte pas d'étiquette VLAN. C'est au moment où la trame rentre dans le port d'accès que l'étiquette VLAN est fixée à la trame. Pendant que la trame transite par le commutateur, elle transporte l'étiquette VLAN qui lui a été attribuée au moment d'entrer dans le port d'accès. L'étiquette VLAN est supprimée lorsque la trame quitte le commutateur via le port d'accès de destination. Les périphériques d'émission et de réception ignorent qu'une étiquette VLAN n'a jamais été utilisée. Ports d'accès :



### III.2. Port sécurité

Le port sécurité permet de contrôler les adresses MAC autorisées sur un port. En cas d'adresses MAC non autorisées sur le port, une action est prise.

Dans les réseaux locaux modernes, nous trouverons un port de commutateur dédié par station de travail. Dans ce cadre, les ports ne devraient recevoir de trafic que d'une seule adresse MAC autorisée. Cela nous permet à empêcher la connexion de commutateurs pirates par exemple.

### III.3. Port trunk

Dans les réseaux comportant plusieurs commutateurs, il est indispensable de pouvoir envoyer des trames avec étiquette VLAN d'un commutateur à un autre. La différence entre les ports d'accès et ports trunk est que les ports trunk ne retirent pas l'étiquette VLAN de la trame lorsqu'ils l'envoient. La présence de l'étiquette VLAN permet au commutateur de réception de connaître l'appartenance de la trame en transit. La trame peut ainsi être renvoyée aux ports appropriés du commutateur de réception.

## IV. Trunk des VLANs

### IV.1. Principe

Lorsqu'un réseau comporte plusieurs commutateurs, chaque commutateur doit pouvoir localiser toutes les stations à l'aide de la table de commutation et connaître le VLAN d'appartenance de la source et du destinataire. Lorsque la taille du réseau est importante, les tables deviennent très grandes et pénaliser les performances. Il est plus efficace d'étiqueter les trames. L'étiquète identifie le VLAN de la station source, le commutateur n'a plus alors qu'à connaître les VLANs d'appartenance des stations qui lui sont raccordées. Un trunk des VLANs permet d'acheminer le trafic de plusieurs VLANs. Généralement, il est établi entre des commutateurs pour permettre aux périphériques du même VLAN de communiquer même s'ils sont physiquement connectés à des commutateurs différents. Un trunk de VLAN n'est associé à aucun VLAN, non plus les ports trunk qui n'appartiennent à aucun VLAN.

### IV.2. VLAN native et étiquetage 802.11Q

Un VLAN correspond à un domaine de diffusion. Cependant, lorsque plusieurs VLANs sont définis sur un même segment, cette définition est mise en défaut. Il est surement possible d'imaginer que le commutateur transforme la diffusion en une rafale d'unicast. La solution optée par l'IEEE est toute différente : un seul VLAN peut être déclaré par port (interface), sauf

pour les liaisons inter-commutateur supportant le trafic de VLAN différents, ces liens dits **Trunk Link**.

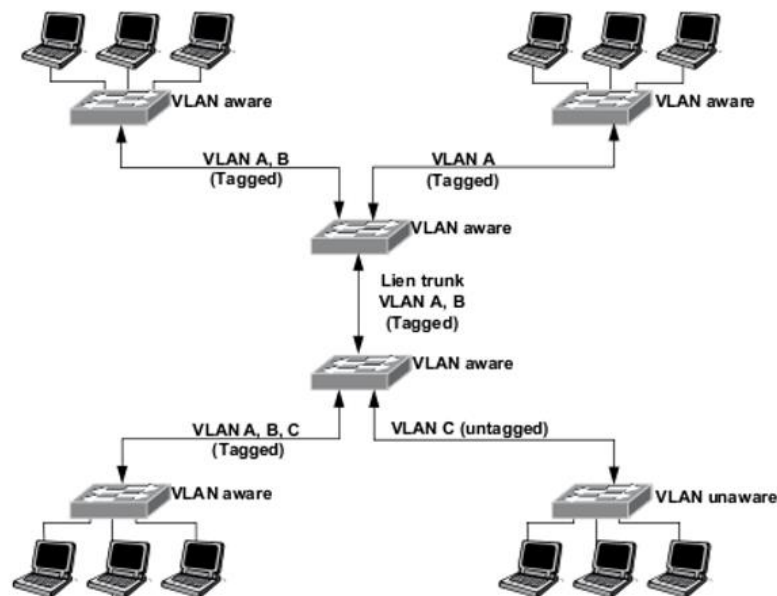


Figure 4.1. 5 : Le principe de l'étiquetage des trames dans les VLANs

Les VLANs sont définis dans les normes IEEE 802.1Q (concerne l'étiquetage) et 802.1P (la qualité de service) qui introduisent quatre octets supplémentaires dans la trame MAC. Ces quatre octets permettent d'identifier les VLANs (VLAN tagging) et de gérer huit niveaux de priorité (qualité de service),

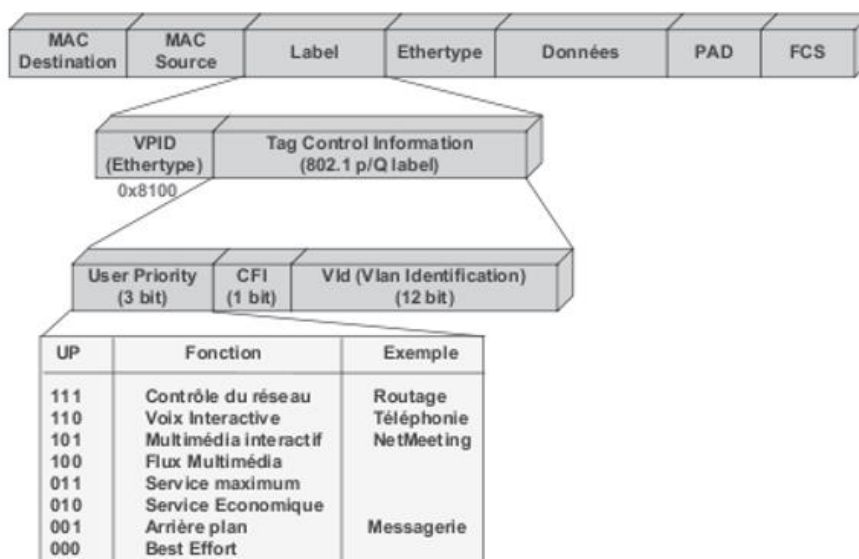


Figure 4.1. 6 : La trame 802.1P/Q

### III. Les attaques sur les VLANs

#### III.1. Attaque double tagging

Après que les commutateurs désencapsulent la trame et enlèvent le champ 802.1Q. Le pirate incorpore un deuxième entête dans la trame qui est non autorisé. Par la suite, le commutateur transmet la trame vers le VLAN spécifié dans le faux entête 802.1Q ajouté par le pirate. La meilleure façon de parer ces attaques consiste à vérifier que le VLAN natif des ports trunk est différent de celui de tous les autres ports.

#### III.2. Attaque usurpation du commutateur

Par défaut, le port du commutateur est configuré en mode dynamique automatique. En configurant un hôte pour qu'il fasse office de commutateur et forme un trunk, le pirate peut accéder à n'importe quel VLAN du réseau. Il peut ensuite accéder aux autres VLAN. Pour éviter une attaque de base, nous désactivons le trunking sur tous les ports, sauf sur ceux qui l'utilisent.

#### III.3. Périphérie PVLAN

La fonction PVLAN (VLAN privé), ou « ports protégés », garantit qu'il n'y a aucun échange de trafic de monodiffusion, de diffusion ou de multidiffusion entre les ports protégés du commutateur. Cette protection n'est pertinente qu'en local. En général, un port protégé échange du trafic uniquement avec les ports non protégés.

### IV. Bonne pratique pour la conception d'un VLAN

Il existe des meilleures pratiques pour concevoir un VLAN, citant :

- Déplacer tous les ports du VLAN1 et attribuer-les à un VLAN qui n'est pas utilisé.
- Arrêter tous les ports non utilisés du commutateur.
- Séparer le trafic de gestion et le trafic des données des utilisateurs.
- Remplacer le VLAN de gestion par un VLAN autre que VLAN1. Faire de même pour le VLAN natif.
- Assurer que seuls les périphériques du VLAN de gestion peuvent se connecter aux commutateurs.
- Le commutateur doit accepter uniquement les connexions SSH.
- Désactiver l'autonégociation sur les ports trunk.
- Ne pas utiliser les modes « auto » ni « désirable » pour les ports des commutateurs

## **V. Activité**

1. Donnez un exemple d'utilisation d'un VLAN.
2. C'est quoi la liaison Trunk ?
3. Une école d'informatique a deux VLANs : un VLAN enseignant et un VLAN étudiants. Comment est-il possible qu'un étudiant envoie un message à un enseignant ?

## **Conclusion**

Dans ce chapitre, nous avons appris les divers types des VLANs, la connexion entre les VLANs (liaison Trunk), les diverses attaques sur les VLANs ainsi que les meilleures pratiques pour concevoir un VLAN. Nous détaillerons dans la prochaine leçon le routage inter VLAN.



**Leçon 2 : Routage inter VLAN**

▪ <b>Objectif Général</b>	<ul style="list-style-type: none"><li>• Comprendre la fonction routage entre les VLANs.</li></ul>
▪ <b>Objectifs Spécifiques</b>	<ul style="list-style-type: none"><li>• Identifier les diverses techniques de routage inter-VLAN.</li><li>• Comprendre la méthode ancienne de routage Legacy.</li><li>• Comprendre la méthode router on a stick.</li><li>• Comprendre les interfaces SVI.</li><li>• Comprendre les ports routes.</li></ul>
▪ <b>Volume horaire</b>	<ul style="list-style-type: none"><li>• Cours : 1.30h</li></ul>
▪ <b>Mots clés</b>	<ul style="list-style-type: none"><li>• Routage inter-VLAN, Router on a stick, interface SVI, ports routés, commutateur multicouche ; routeur ...</li></ul>

## Introduction

Nous avons mis en place des VLANs afin de définir un domaine de diffusion et un cloisonnement logique au-dessus d'une topologie réseau connue ainsi qu'isoler le trafic. Cependant, les VLANs posent des problèmes à savoir d'isoler des parties du réseau que nous ne voulons pas l'isoler aussi empêcher certains services afin de communiquer. D'où un équipement de couche 3 est nécessaire pour parer surtout le problème de communication.

## I. Fonctionnement du routage inter-VLAN

Le routage inter VLAN assure la communication entre tous les VLANs qui existent dans un réseau local à travers un équipement de couche 3 (un routeur/un commutateur multicouches).

Il existe trois façons de router le trafic entre les stations du réseau :

- Routage par un commutateur niveau 3.
- Routeur avec un lien par VLAN
- Routeur avec un seul lien pour tous les VLANs

## II. Les méthodes du routage inter-VLAN

Pour transmettre le trafic entre les VLANs, Deux solutions s'offrent à nous, utiliser un routeur, ou utiliser un commutateur de niveau 3.

### II.1. Les méthodes de routage inter-VLAN au niveau du routeur

#### II.1.1. Ancienne méthode de routage inter-VLAN (Legacy inter-VLAN)

Le routage est effectué en connectant différentes interfaces physiques du routeur sur différentes interfaces physiques du commutateur.

Les ports du commutateur connectés au routeur sont en mode accès. Chaque interface physique est assignée à un VLAN différent. Cette méthode devient gênante dans un réseau où le nombre de VLANs est élevé.

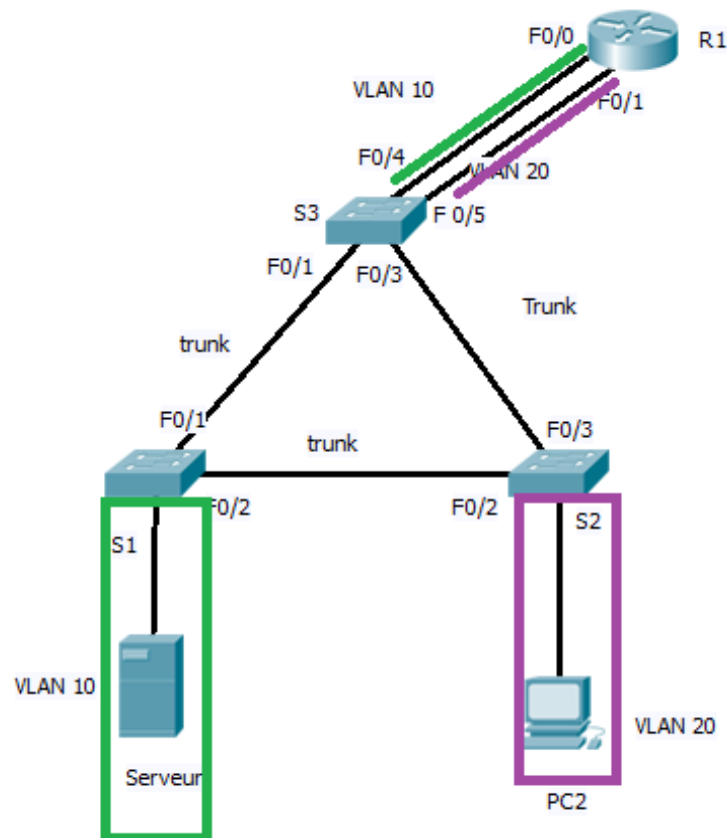


Figure 4.2. 1: Le routage inter-VLAN classique

Nous constatons que cette topologie comporte deux VLANs, VLAN 10 et VLAN 20, chaque VLAN dispose sa propre liaison dédiée entre le routeur et le commutateur. Les commutateurs sont interconnectés par des liaisons trunk.

## II.1.2. La méthode « router on a stick »

### II.1.2.1. Principe

Cette méthode moderne remplace la méthode classique en évitant les interfaces physiques sur le routeur et sur le commutateur. Une seule interface physique est requise sur le routeur et le commutateur pour acheminer les trames entre les différents VLANs. Cette interface est configurée comme une liaison trunk.

Nous appelons cette méthode « router on a stick », elle sert à configurer une seule interface physique comme une liaison trunk qui achemine le trafic entre plusieurs VLANs.

Le routeur effectue le routage inter-VLAN en acceptant le trafic étiqueté VLAN sur l'interface trunk provenant du commutateur adjacent. Il procède ensuite au routage en interne entre les VLANs à l'aide des sous-interfaces. Le routeur transfère alors le trafic acheminé, étiqueté

VLAN vers le VLAN de destination, depuis la même interface physique utilisée pour recevoir le trafic.

Les sous-interfaces sont configurées sur le routeur. Chaque sous-interface est configurée indépendamment avec une adresse IP et une affectation à un VLAN. Les sous-interfaces configurées pour différents sous-réseaux correspondant à leur affectation VLAN sont utilisées afin de faciliter le routage logique. Dès que le routeur a pris la décision de routage, les trames étiquetées seront renvoyées depuis l'interface physique.

#### II.1.2.1. Exemple

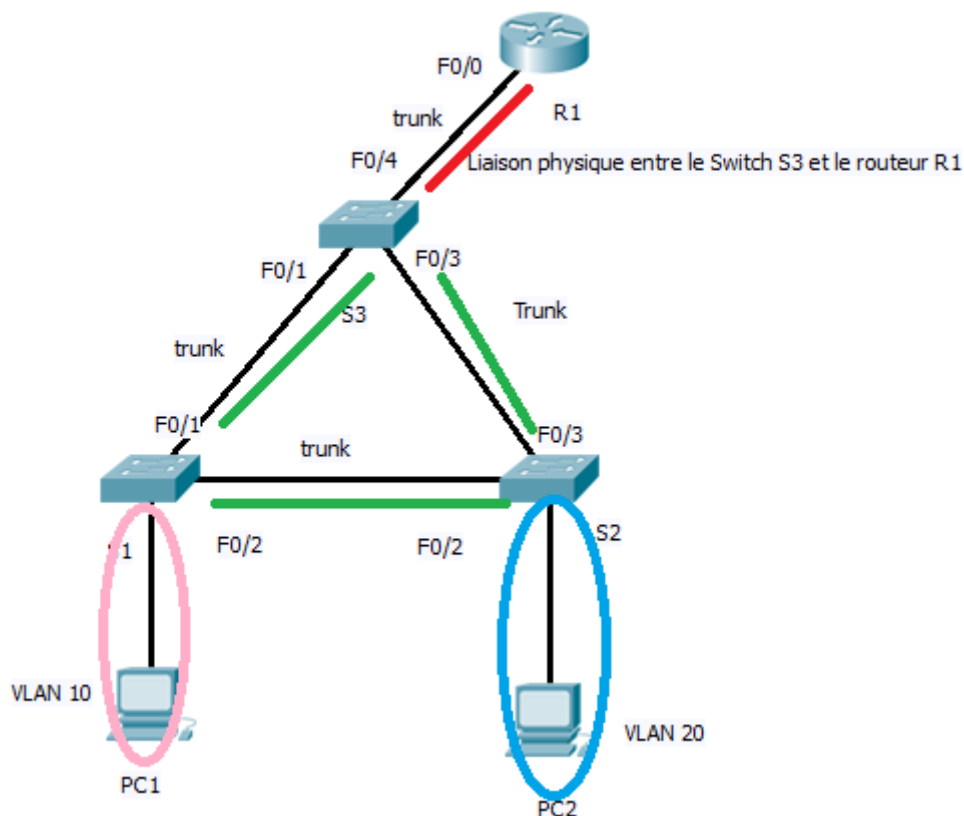


Figure 4.2. 2 : routage inter-VLAN router on a stick

Sous interface	adresse
F0/0.10	192.168.10.1
F 0/0.20	192.168.20.1

La figure suivante montre le parcours suivi par le trafic monodiffusion envoyé par le PC1 du VLAN 10 vers le PC2 du VLAN 20.

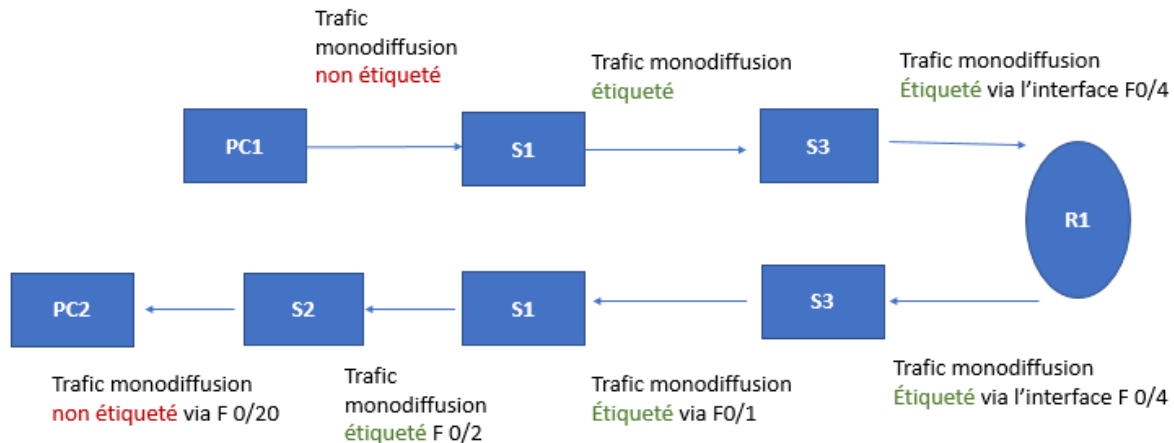


Figure 4.2. 3 : Communication entre PC1 et PC2

## II.2. Les techniques de routage au niveau des commutateurs niveau 3

La mise en place de routage inter-VLAN avec une architecture qui n'utilise pas de routeur pour effectuer le routage. La tâche de routage est assurée par un commutateur de niveau 3 avec des fonctions de niveau 3 comme le routage.

### II.2.1. Interface SVI

Une interface SVI (Switch Virtual Interface) est une interface virtuelle configurée sur un commutateur multicouche. Une interface SVI est créée pour chaque VLAN existant sur le commutateur. Elle assure les mêmes fonctions pour le VLAN qu'une interface de routeur. Une interface physique existe entre les commutateurs et le commutateur multicouche. L'interface SVI est configurée en mode trunk.

L'interface SVI présente des avantages suivants

- Ils sont beaucoup plus rapides que les routeurs sur une clé USB parce que tout est matériel commuté et routé.
- Aucune liaison externe n'est nécessaire entre le commutateur et le routeur pour le routage.
- Ils ne se limitent pas à un seul lien. Les canaux EtherChannels de couche 2 peuvent être utilisés entre les commutateurs pour obtenir plus de bande passante.
- La latence est beaucoup plus faible parce qu'il n'a pas besoin de quitter le commutateur.

Avec la méthode Router On A Stick, tout le trafic passera par le lien entre le switch et le routeur. Cela peut éventuellement créer un goulot d'étranglement et donc une congestion du lien.

Avec la méthode Switch de niveau 3, le routage se fera en local sur le switch, ce qui diminue grandement le risque de congestion.

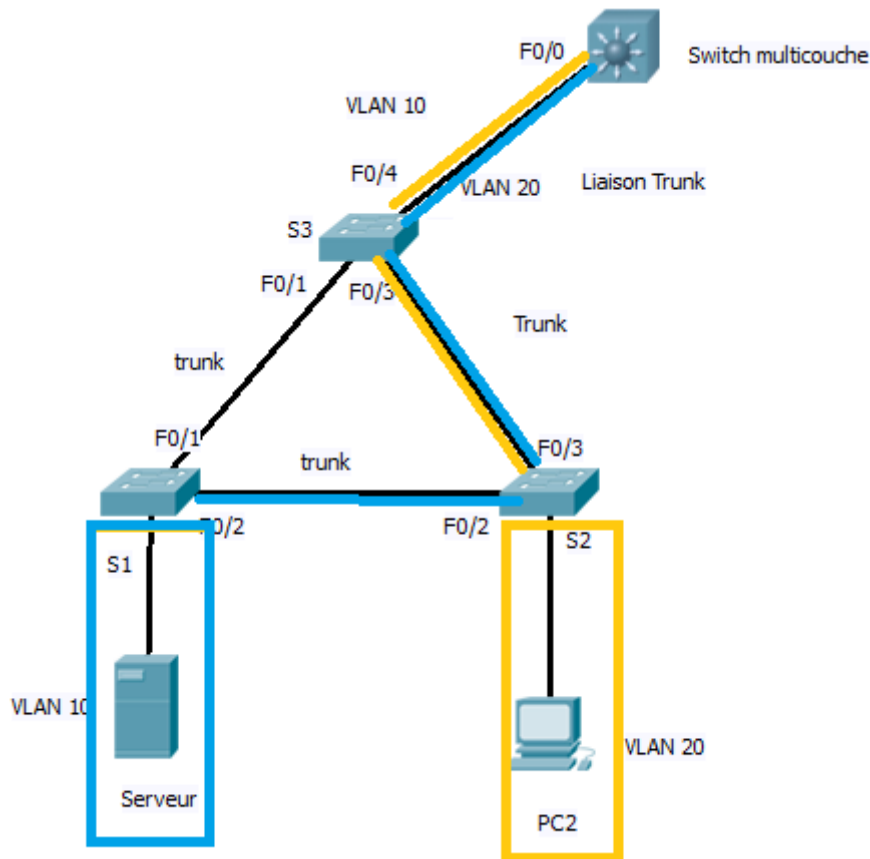


Figure 4.2. 4 : Interface SVI

### II.2.2. Ports routés

Un port routé de commutateur est configuré en tant que port routé de couche 3 : ce port se comporte comme une interface physique de routeur. Les caractéristiques des ports routés sont les suivantes :

- Ils ne sont associés à aucun réseau local virtuel spécifique.
- Ils peuvent être configurés avec un protocole de routage de couche 3.

- Ils constituent des interfaces de couche 3 uniquement et ne prennent pas en charge les protocoles de couche 2.

### **Conclusion**

Dans ce chapitre, nous avons découvert les différentes méthodes de routage inter-VLAN à savoir les méthodes router on a stick et la méthode ancienne en utilisant un routeur comme équipement de couche 3 ainsi que les méthodes reposées sur les ports routes et les interfaces SVI dans le cas où nous avons utilisé un commutateur multicouche. Nous verrons dans la prochaine leçon une technique qui nous permettra d'améliorer les performances de notre réseau local.

**Leçon 3 : Agrégation des liens**

▪ <b>Objectif Général</b>	<ul style="list-style-type: none"><li>• Comprendre l'intérêt de l'agrégation des liens.</li></ul>
▪ <b>Objectifs Spécifiques</b>	<ul style="list-style-type: none"><li>• Identifier les divers statuts des protocoles LACP et PAgP.</li><li>• Comprendre les diverses restrictions de l'agrégation des liens : le nombre maximal de groupe et le nombre maximal d'interfaces par groupe.</li><li>• Comprendre le fonctionnement de l'EtherChannel</li></ul>
▪ <b>Volume horaire</b>	<ul style="list-style-type: none"><li>• Cours : 30mn</li></ul>
▪ <b>Mots clés</b>	<ul style="list-style-type: none"><li>• Agrégation des liens, EtherChannel, LACP, PAgP...</li></ul>



## Introduction

Au sein d'un réseau local d'entreprise moderne, une liaison trunk entre les commutateurs est défectueuse. L'administrateur réseau opte quelle solution pour réparer ce problème. Des solutions possibles sont de changer le câble, connecter un second câble entre les commutateurs et reconfigurer la trunk ou bien connecter des câbles entre les commutateurs, les regrouper et configurer comme une liaison trunk. La dernière solution proposée est la meilleure parlant d'un réseau moderne entièrement redondant dont tous liens sont tous actifs et on bénéficie d'une bande passante plus large, c'est l'agrégation des liens.

## I. Agrégation des liens

### I.1. Présentation

Dans les réseaux modernes entièrement redondant, nous regroupons plusieurs interfaces physiques en un seul lien logique afin d'optimiser le débit des données. Ceci introduit efficacement des solutions pour fournir une utilisation plus importante de liens disponibles, ainsi que la résilience étendue en cas d'échec de des liens individuels devaient se produire. Nous appelons cette forme d'agrégation d'Ether Channel qui est utilisée dans les réseaux commutés.

Lorsqu'un Etherchannel est configuré, l'interface virtuelle résultante est appelée un canal de port (port-Channel abrégé Po)

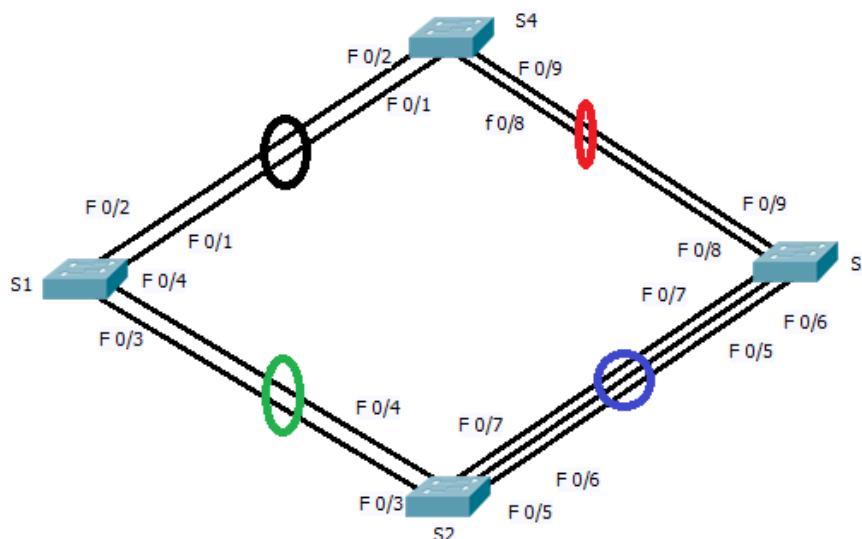


Figure 4.3. 1 : Agrégation des liens entre des commutateurs

Cette topologie contient quatre EtherChannel. Chaque commutateur comporte deux EtherChannel.

## I.2. Avantages de l'Ether Channel

La technologie Ether Channel présente des avantages importants

- Une utilisation plus importante de la bande passante
- Prévention de panne
- Assurer l'équilibrage de charge
- Assure la cohérence de la configuration sur toutes les liaisons.

## II. Fonctionnement de l'EtherChannel

### II.1. Restrictions d'implémentation

EtherChannel peut être implémenté en regroupant plusieurs ports physiques sur une ou plusieurs liaisons logiques EtherChannel. Les types d'interface ne peuvent pas être associés. L'EtherChannel offre une bande passante bidirectionnelle simultanée jusqu'à 800 Mb/s (Fast EtherChannel) ou 8 Gb/s (Gigabit EtherChannel) autrement dit nous regroupons 8 ports de chaque commutateur au maximum donc EtherChannel peut se regrouper jusqu'à 16 ports Ethernet compatible-configurés. Les commutateurs peuvent supporter six Ether Channel. Des EtherChannel peuvent être formés par négociation en utilisant le protocole LACP (Link Aggregation Control Protocol).

### II.2. Protocoles d'agrégation des Liens

Il existe deux protocoles d'agrégation de lien suivant les quels nous pourrions configurer un Etherchannel.

#### II.2.1. LACP (Link Aggregation Control Protocol)

Ce protocole permet de créer la liaison EtherChannel en détectant les configurations de chacun des côtés et en assurant leur compatibilité, afin que la liaison EtherChannel puisse être activée au besoin. Ce protocole utilise également 3 statuts dans sa configuration :

- **On** : Sert à déclarer une agrégation active
- **Active** : C'est un mode qui fait la demande avec le switch d'en face pour créer l'agrégation
- **Passive** : C'est un mode qui attend la négociation pour devenir une agrégation

### II.2.2. PAgP : Port Aggregation Protocol propriétaire Cisco

- S'il est activé, PAgP gère également l'EtherChannel. Les paquets PAgP sont envoyés toutes les 30 secondes.
- PAgP vérifie la cohérence de la configuration et gère les ajouts de liaison et les défaillances entre deux commutateurs.
- Il garantit que tous les ports ont le même type de configuration quand un EtherChannel est créé.
- Dans un EtherChannel, tous les ports doivent obligatoirement avoir une vitesse, un paramètre de bidirectionnalité et des informations VLAN identiques.
- Toute modification d'un port après la création du canal modifie également tous les autres ports du canal.

Il est également possible de configurer un EtherChannel statique ou inconditionnel sans PAgP ou LACP.

Protocole	Mode	Description
<b>PAgP</b>	<b>Desirable</b>	Ce mode place l'interface en mode active, elle initialisera les négociations en voyant des paquets PAgP.
	<b>Auto</b>	Ce mode met l'interface en négociation passive, autrement dit l'interface n'initialise pas la négociation et répond aux paquets (PAgP/LACP) reçus.
<b>LACP</b>	<b>Active</b>	Ce mode place le port dans un état de négociation actif. Dans cet état, le port entame des négociations avec d'autres ports en envoyant des paquets LACP.
	<b>Passive</b>	Ce mode place un port dans un état de négociation passif. Le port répond aux paquets LACP qu'il reçoit, mais n'entame pas de négociation par paquet LACP.
<b>--</b>	<b>On</b>	Ce mode force l'interface en Etherchannel sans négociation, sans négociation, sans échange de paquets PAgP ou LACP.
	<b>Off</b>	Désactive l'EtherChannel

### III. Configuration du protocole EtherChannel

Il y a deux façons de configurer EtherChannel. La première est de procéder manuellement en saisissant une commande sur chaque port à agréger, des deux côtés de la liaison, la seconde est de laisser la configuration automatique, à l'aide de l'un des deux protocoles PAgP et LACP.



Figure 4.3. 2 : Exemple de configuration

C'est les différentes commandes exécutées sur le commutateur S1 et a les retaper sur le commutateur S2.

```
Switch>enable
```

```
Switch#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch(config)#interface range f 0/1-3
```

```
Switch(config-if-range)#channel-group 1 mode desirable
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
```

```
Switch(config-if-range)#interface port-channel 1
```

```
Switch(config-if)#switchport mode trunk
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

```
Switch(config-if)#switchport trunk allowed vlan 10,20,99
```

```
Switch(config-if)#end
```

```
Switch#
```

%SYS-5-CONFIG\_I: Configured from console by console

Après la configuration de l'EtherChannel, nous la vérifions par plusieurs commandes

- **Show interface port-Channel** : affiche l'état général de l'interface de port-Channel
- **Show EtherChannel summary** : affiche une ligne d'informations unique par canal de port
- **Show EtherChannel port-Channel** : affiche des informations concernant une interface port-Channel spécifique

```
Switch#show etherchannel summary
```

Flags: D - down      P - in port-channel

I - stand-alone s - suspended

H - Hot-standby (LACP only)

R - Layer3      S - Layer2

U - in use      f - failed to allocate aggregator

u - unsuitable for bundling

w - waiting to be aggregated

d - default port

Number of channel-groups in use: 1

Number of aggregators:      1

Group Port-channel Protocol Ports

```
-----+-----+-----+-----
```

```
1   Po1(SD)      PAgP   Fa0/1(I) Fa0/2(I) Fa0/3(I)
```

```
Switch#
```

**Conclusion**

L'EtherChannel est une technologie qui permet d'améliorer les performances du réseau d'entreprise. De plus cette technologie est simple à mettre en place et ne nécessite généralement pas d'investissement. Le nombre de lien regroupable limité à huit ports qui doit être de même type.