



N° d'ordre : .....

**UNIVERSITE DE M'SILA**  
**FACULTE DES MATHÉMATIQUES ET DE L'INFORMATIQUE**  
**Département TIC**

**MEMOIRE de fin d'étude**

**Présenté pour l'obtention du diplôme de MASTER**

**Domaine : Mathématiques et Informatique**

**Filière : Informatique**

**Spécialité : Technologie de l'Information et de la Communication (TIC)**

**Par : BENAISSA ADIL**

**SUJET**

**ETUDE ET SIMULATION DU ROUTAGE INTER-VLAN**

**Soutenu publiquement le : 16 / 06 /2015 devant le jury composé de :**

**Mr. GUERNA**

**Université de M'sila Président**

**Mr. HEMMAK ALLAUA**

**Université de M'sila Rapporteur**

**Mr. KHETTAF**

**Université de M'sila Examineur**

**Promotion : 2014/2015**

## *DEDICACES*

*Je dédie le fruit de mes efforts, comme symbole de gratitude.*

*A mes parents qui m'entourent et m'encouragent toujours par leur tendresse et leur affection.*

*A mes sœurs, à toute la famille, qui m'ont aidée par leur soutien moral.*

*A tous mes amis, pour leur amitié et leur conseil.*

*Qu'Allah soit leur guide*

*Adil*

## Remerciements

Je tiens tout d'abord à *Allah* le tout puissant, qui m'a donné la force et la patience pour l'accomplissement de ce travail.

Je tiens à remercier chaleureusement mon encadreur, *Monsieur HEMMAK ALLAUA*, pour m'avoir proposé ce projet, en me faisant confiance, ainsi pour avoir dirigé ce travail avec ses orientations, ses précieux conseils et remarques. Je vous remercie infiniment *Monsieur* pour le temps que vous avez consacré à ce travail, pour votre entière disponibilité. J'ai eu le grand plaisir de travailler sous votre direction. Mes remerciements s'adressent également aux membres du jury pour l'immense honneur qu'ils m'ont fait en acceptant d'évaluer ce travail.

Enfin, je remercie tous ceux qui ont contribué de près ou de loin, par leurs encouragements et conseils à l'accomplissement de ce modeste travail.

# Table des matières

<b>Remerciements</b>	<b>iii</b>
<b>Table des matières</b>	<b>iv</b>
<b>Liste des Figures</b>	<b>vii</b>
<b>Liste des Tableaux</b>	<b>ix</b>
<b>INTRODUCTION GENERALE</b>	<b>10</b>
 <b>CHAPITRE 1 : GENERALITÉ SUR LES RÉSEAUX</b>	
<b>1 Introduction</b>	<b>12</b>
<b>2 Définition</b>	<b>12</b>
<b>3 Les différents types de réseaux</b>	<b>12</b>
3.1 Le réseau personnel (PAN)	12
3.2 Le réseau local (LAN)	13
3.3 Le réseau métropolitain (MAN)	13
3.4 Le réseau étendu (WAN)	13
<b>4 Les réseaux locaux</b>	<b>13</b>
4.1 Les catégories des réseaux	13
4.1.1 Le réseau (peer to peer ou pair à pair)	14
4.1.2 Le réseau Server/Client	14
4.2 Topologie de réseau	14
4.2.1 Topologie physique	14
4.2.2 Les topologies logiques	15
4.3 Les réseaux locaux Ethernet	15
<b>5 Les architectures de réseaux</b>	<b>16</b>
5.1 Le modèle OSI	16
5.2 Le modèle TCP/IP	17
5.3 Les unités de données et les équipements réseau	19
5.4 Modélisation OSI et standard Ethernet	20
5.5 Types d'adresses MAC	22
<b>6 Le routage</b>	<b>23</b>
<b>7 Conclusion</b>	<b>24</b>

## **CHAPITRE 2 RESAUX LOCAUX VIRTUELS**

<b>1 Introduction</b>	25
<b>2 Définition</b>	25
<b>3 Type de VLAN</b>	26
3.1 Les VLAN statique	26
3.2 Les VLAN dynamiques	26
<b>4 Gestion de Vlan</b>	28
<b>5 Agrégation de Vlan (Trunking) et normes</b>	29
5.1 Vlan standard ou IEEE 802.10	29
5.2 La norme 802.1Q	29
5.1.1 La Balise 802.1Q	29
5.1.2 Le protocole ISL (Inter-Switch Link)	31
5.3 Le protocole VTP (Vlan trunk Protocol)	31
5.3.1 Trunking méthode	31
5.3.2 Le protocole VTP	32
5.4 L'IEEE 802.1p	32
<b>6 Avantage VLAN</b>	33
<b>7 Conclusion</b>	33

## **CHAPITRE 3 : ROUTAGE INTER-VLAN**

<b>1 Introduction</b>	35
<b>2 Fonctionnement du routage inter-vlan</b>	35
2.1 Qu'est ce que le routage inter-vlan ?	35
2.2 Situation avant routage inter-VLAN	36
2.3 Situation après routage inter-VLAN	37
2.4 Bande passante et trunks	38
2.5 Les Méthodes du routage inter-vlan.	38
2.6 Routage inter-vlan physique	38
2.6.1 Routage inter-vlan logique (Router on a stick)	40
2.7 Routage inter-vlan des commutateurs multicouche	42
<b>3 Dépannage du routage inter-VLAN</b>	42
3.1 Problèmes de configuration inter-VLAN	42
3.1.1 Problème lie aux ports de commutateur	42

3.2 Problèmes d'adressage IP	44
<b>4 Conclusion</b>	<b>45</b>

## **CHAPITRE 4**

### **ETUDE PAR LA SIMULATION ROUTAGE INTER-VLAN**

<b>1 Introduction</b>	<b>46</b>
<b>2 Le logiciel Packet Tracer</b>	<b>46</b>
2.1 Fonctionnement du logiciel Packet Tracer	47
2.1.1 L'espace de travail logique (Logical work space)	47
2.1.2 L'espace de travail physique (Physical work space)	49
2.1.3 Mode temps réel	52
2.1.4 Mode simulation	53
2.2 Simulation Routage inter-vlan	54
2.2.1 Architecture	55
2.2.2 OSPF	56
2.2.2.1 Configuration	56
2.2.3 Déroulement de la simulation	58
2.2.4 Mise en place d'un routage inter-VLAN	59
2.2.4.1 Déroulement de la simulation	62
<b>3 Résultat de la simulation et discussion</b>	<b>63</b>
<b>4 OPNET Modeler</b>	<b>63</b>
4.1 Présentation l'OPNET	64
4.2 L'éditeur de projets	64
4.3 Simulation	68
4.3.1 Simulation de Réseau local virtuel	68
4.4 Réseau sans VLAN	68
4.5 Réseau avec des VLAN	69
4.6 Résultats des Analyses	
<b>5 Conclusion</b>	<b>70</b>
<b>CONCLUSION &amp; PERSPECTIVES</b>	<b>71</b>
<b>BIBLIOGRAPHIE</b>	<b>72</b>

## Liste des figures

Figure 1.1 : les différents types des réseaux.....	13
Figure 1.2 : les différents types des réseaux.....	14
Figure 1.3 : Le model OSI.....	16
Figure1.4: Le model OSI en détail.....	16
Figure 1.5 : Le model TCP/IP et le model OSI.....	18
Figure 1.6 : La couche application.....	18
Figure 1.7 : La couche transport.....	18
Figure 1.8 : La couche transport.....	18
Figure 1.9 : La couche Internet.....	19
Figure1.10 : La couche réseau.....	19
Figure1.11 : couche OSI et les équipements .....	19
Figure1.12 : OSI et Ethernet.....	21
Figure1.13 : L'octet de poids le plus fort d'une Adresse MAC.....	22
Figure1.14 : eui-48 et eui-64.....	23
Figure2.1 : définition des groupes des VLANs .....	25
Figure 2.2 : Vlan axés au port.....	26
Figure 2.3 : Format de l'entête Ethernet V2.....	27
Figure 2.4 : Trame encapsulée 802.1q.....	29
Figure 2.5 : <i>Trame ISL</i> .....	30
Figure 2.6: Liaison en mode Trunk.....	31
Figure 2.7 : Subdivision d'une liaison physique en liaison logique (Trunking) .....	32
Figure3.1 Routage inter-vlan.....	35
Figure 3.2 Domaine de diffusion et collision .....	36
Figure3.3 Scénario avant routage inter-vlan.....	36
Figure3.4 Scénario après le routage inter vlan.....	37
Figure3.5 le Routage inter-vlan physique.....	39
Figure 3.6 : Division d'un port physique en port logique au sein d'un routeur.....	40
Figure 3.7 Le routage inter-vlan Router on a stick.....	41

Figure 3.8 Le routage inter-vlan des commutateurs de multicouche.....	42
Figure 3.9 topologie avec problème de configuration dans le Switch.....	43
Figure 3.10 problèmes de lien tombe en panne.....	43
Figure 3.11 Topologie avec Adresse ip de routeur 1 mal configuré.....	44
Figure 3.12 Topologie avec Adresse de PC1 mal configuré.....	45
Figure 4.1 : Démarrage de Packet Tracer 6.2.0.....	46
Figure 4.2 : Espace de travail logique.....	47
Figure 4.3 : Ajout et suppression d'un module.....	48
Figure 4.4 : Interface de commande.....	49
Figure 4.5 : Packet Tracer : zone Interurbain (M'sila - Alger) .....	50
Figure 4.6 : Plan d'une ville (M'sila) avec les bâtiments.....	50
Figure 4.7 : Plan d'un Bâtiment avec les différents cabinets.....	51
Figure 4.8 : les équipements dans les cabinets de câblage.....	51
Figure 4.9 : Présentation du réseau en mode temps réel.....	52
Figure 4.10 : Ping de PC1 vers PC0.....	53
Figure 4.11 : Packet Tracer : mode simulation.....	53
Figure 4.12 : Détail d'une trame : Ethernet II, IP, ICMP pour un simple PDU (Ping).....	54
Figure 4.13 : Scénario réseaux LAN.....	55
Figure 4.14 show ip ospf.....	57
Figure 4.15 show ip ospf Neighbor.....	57
Figure 4.16 : Initialisation de la configuration.....	57
Figure 4.17 : Envoie de PDU de configuration.....	58
Figure 4.18 : Envoie l'enveloppe de l'ospf.....	58
Figure 4.19 paquet ospf inclut dans le format PDU.....	59
Figure 4.20 : Scénario avec Vlan et Routage inter vlan.....	60
Figure 4.21 : Initialisation de la configuration.....	62
Figure 4.22 Démarrage OPNET.....	63
Figure 4.23 Espace de simulation OPNET.....	64
Figure 4.24 Crée un nouveau projet .....	65
Figure 4.25 Au court de crée un projet .....	65
Figure 4.26 Réseau sans VLAN OPNET.....	67
Figure 4.27 Réseau commuté avec VLAN.....	67
Figure 4.28 Attribue les VLANS sous OPNET .....	68



Figure 4.29 Trafic reçue de demande par le serveur d'administration (packet / sec).....	68
Figure 4.30 Trafic reçue demande par la faculté Serveur (packet / sec).....	69
Figure 4.31 Trafic demande reçue par les étudiants Server (packet / sec).....	66

## Liste des tableaux

Table 2.1: Quelques valeurs du champ Ethertype.....	27
Table 2.2: Valeur du champ Type pour ISL.....	31
Table 4.1: Table D'adressage.....	55
Table 4.1: VLAN : regroupement fonctionnel.....	60
Table 4.3 distribution des stations dans département .....	66

# INTRODUCTION GÉNÉRALE

Le rôle des réseaux a sensiblement évolué ces dernières années, il ne se limite pas au transfert de l'information en toute sécurité mais aujourd'hui il contribue largement à la rationalisation des utilisateurs et à l'optimisation des performances applicatives. De ce fait on a besoin d'un ensemble des moyens et techniques permettant la diffusion d'un message auprès d'un groupe plus ou moins vaste et hétérogène.

Aujourd'hui, il est plus que fréquent de voir l'utilisation de VLAN au sein d'un réseau d'entreprise. Les VLAN Ethernet (réseau local virtuel) offrent de nouvelles solutions et opportunités en matière de gestion des réseaux informatiques des entreprises. L'évolution rapide de la connectivité Internet a poussé de nombreuses organisations à étendre leur installation informatique.

Ce nouveau mode de segmentation des réseaux locaux modifie radicalement la manière dont les réseaux sont conçus, administrés et maintenus. La technologie de VLAN comporte ainsi de nombreux avantages et permet de nombreuses applications intéressantes.

L'usage des réseaux locaux virtuels (VLANs) et du routage entre ces mêmes réseaux locaux est devenu systématique dans les infrastructures d'interconnexion contemporaines. Ce routage inter-VLAN présente de nombreux intérêts tant du point de vue conception que du point de vue exploitation.

Notre projet consiste à étudier et simuler les VLANs et le routage entre les VLAN, conçu pour les réseaux locaux Ethernet dans le but de le rendre plus performant grâce aux nombreuses solutions que nous offre la technologie VLAN.

Le présent travail est organisé en quatre chapitres.

Dans le premier chapitre, nous présentons un aperçu général sur les réseaux Ethernet. Ainsi, la définition de réseau et des explications pour tous ces caractéristiques en introduisent les différents types de réseaux et les architectures de réseaux.

Dans le deuxième chapitre, nous présentons le réseau local virtuel (VLAN) en donnant son principe de fonctionnement à savoir l'Agrégation de Vlan (Trunking) et normes et les différents types de vlan et leur avantage.

Dans le troisième chapitre, nous présentons le routage inter vlan en désignons leur fonctionnement et les différentes méthodes de routage inter vlan enfin on a défini le contrôle d'accès.

Dans le quatrième chapitre, il est composé de deux parties ; dans le 1er partie nous présentons l'environnement de simulation Packet Tracer, la simulation et mis en place d'un réseau LAN avant de crée les VLANs et après d'utiliser les VLANs et le routage entre eux. Le 2eme partie conçu a utilisé le simulateur OPNET MODLER qui permet de faire une étude comparative entre les LAN et les VLAN dans le contexte les métrique de performance comme le trafic envoyés, le trafic reçus, le retard et le nombre de collision sont mesurés et analysés.

# CHAPITRE 1

## GENERALITÉ SUR LES RÉSEAUX

---

### 1 Introduction

Dans le monde d'aujourd'hui, la plupart des entreprises, quelle que soit leur taille et leur fonctionnalité a besoin d'un système d'information qu'est un ensemble des méthodes et des moyens pour traiter et stocker les informations nécessaires, mais le problème qu'elle se pose comment faire échanger l'information entre les différents services qu'elle appartient et pour qu'elle puisse fournir à ses partenaires l'accès à ces informations à distance ? .

Un réseau informatique est la seule solution pratique pour résoudre ce problème posé, l'utilisation d'ordinateurs par une plus grande partie des entreprises a facilité la création d'un réseau interne et un autre externe. Les services qu'ils offrent font partie de la vie courante des entreprises et administrations (banques, gestion, commerce, recherche, etc....), et des particuliers (messageries, loisirs, services d'informatique par minitel et Internet, ...).

Dans ce chapitre nous allons présenter un aperçu général sur les réseaux informatiques, ainsi, la définition de réseau et des explications pour toutes ces caractéristiques.

### 2 Définition

Le mot réseau est très souvent employé dans un sens qui le lie aux communications. Ainsi tout un chacun connaît le réseau téléphonique, le réseau électrique, le réseau routier on parlera aussi, d'un réseau d'amis.

En informatique, un réseau est un ensemble d'objets interconnectés les uns avec les autres. Il permet de faire circuler des éléments entre chacun de ces objets selon des règles bien définies. Dans le cas où les objets sont des ordinateurs on parle d'un réseau informatique. [1]

### 3 Les différents types de réseaux

On peut dire que le réseau informatique est distingué par quatre types différents selon (la taille de réseau, sa vitesse de transfert des données et aussi leur étendue) :

#### 3.1 Le réseau personnel (PAN) :

Le PAN (Personnel Area Network), c'est le plus petite étendue de réseau, il désigne une interconnexion d'équipement informatique dans un espace de dizaine de Mètre. Il peut être appelé réseau individuel ou réseau domestique. [2]

### 3.2 Le réseau local (LAN) :

La LAN (Local Area Network), c'est des ordinateurs qui se connectent les uns très proches des autres. L'interconnexion sera dans un même immeuble ou deux bâtiments raccordés par une liaison rapide (un câble). Sa longueur varie de quelques centaines Mètre.

### 3.3 Le réseau métropolitain (MAN) :

Le MAN (Métropolitain area network) Interconnecte plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer comme si ils faisaient partie d'un même réseau local. Un MAN est formée de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique). [2]

### 3.4 Le réseau étendu (WAN)

Interconnecte plusieurs LANs à travers de grandes distances géographiques.

Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles.

Les WAN fonctionnent grâce à des routeurs qui permettent de "choisir" le trajet le plus approprié pour atteindre un nœud du réseau. Le plus connu des WAN est Internet [2].

La figure 1.1 suivante représente les différents types des réseaux.

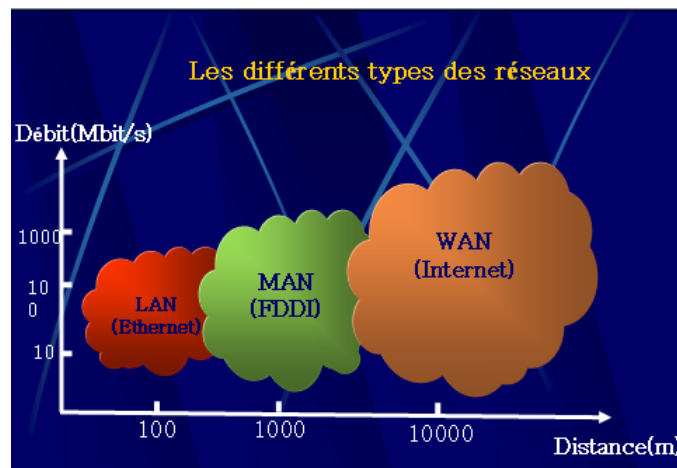


Figure 1.1 : les différents types des réseaux [2]

## 4 Les réseaux locaux

### 4.1 Les catégories des réseaux

On distingue également deux catégories de réseaux :

- Réseaux poste à poste (peer to peer= P2P).
- Réseaux avec serveur dédié (Server/client).

#### 4.1.1 Le réseau (peer to peer ou pair à pair)

Chaque poste ou station fait office de serveur et les données ne sont pas centralisées, l'avantage majeur d'une telle installation est son faible coût en matériel (les postes de travail et une carte réseau par poste). En revanche, si le réseau commence à comporter plusieurs machines (>10 postes) il devient impossible à gérer [2].

#### 4.1.2 Le réseau Server/Client

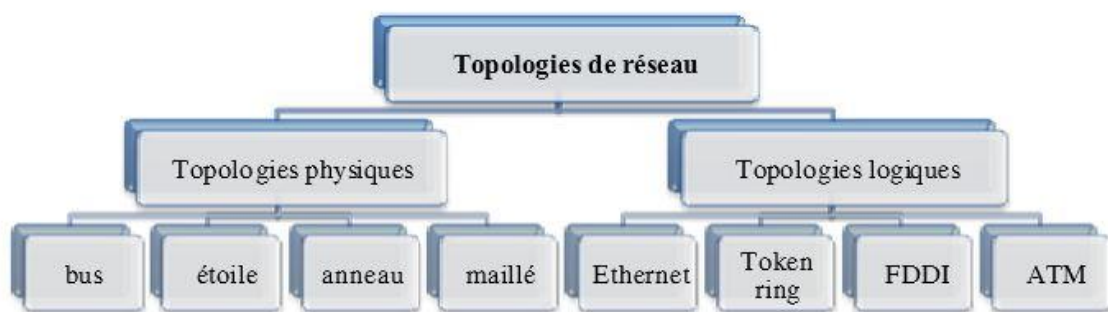
Il ressemble un peu au réseau poste à poste mais cette fois-ci, on y rajoute un poste plus puissant, dédié à des tâches bien précises.

Cette nouvelle station s'appelle serveur. Le serveur Centralise les données relatives au bon fonctionnement du réseau [2].

### 4.2 Topologie de réseau

Il existe plusieurs organisations de réseaux, qui ont chacune des capacités et des contraintes déferentes. On choisira donc une topologie plus qu'une autre en fonction du réseau à mettre en place.

Il existe deux types de topologie de réseau comme la figure 2 présente



**Figure 1.2** : les différents types des réseaux

#### 4.2.1 Topologie physique

Une topologie physique correspond à la disposition physique d'un réseau, mais ne spécifie pas les types de périphérique, les méthodes de connectivité ou les adresses d'un réseau.

Les topologies physiques sont disposées selon trois principaux groupes de formes géométriques : le bus, l'anneau et l'étoile.

### 4.2.2 Les topologies logiques

Une topologie logique s'appelle aussi un système de transport réseau. La topologie logique d'un réseau décrit la manière par laquelle les données sont mises en trames et comment les impulsions électriques sont envoyées sur le support physique du réseau. Les éléments d'une topologie logique appartiennent à la fois aux couches liaison et réseau du modèle OSI<sup>1</sup>.

Chaque topologie logique possède son propre ensemble de principes de signalisation de données, mais impose aussi des exigences particulières au niveau du média de transmission et de la topologie physique. Ethernet et Token Ring sont les deux systèmes de transport réseau (topologie logique) les plus courants. [3]

### 4.3 Les réseaux locaux Ethernet

Aujourd'hui, un réseau local repose presque systématiquement sur la technologie Ethernet. Il hérite donc des caractéristiques de cette technologie. Les deux notions clés dans ce contexte sont collision et diffusion.

#### ➤ Domaine de collision

Une collision intervient lorsque deux hôtes d'un réseau émettent simultanément sur un média partagé. Le domaine de collision est un sous-ensemble du réseau à l'intérieur duquel les hôtes sont en compétition pour accéder à un même média ou canal de communication. Plus le nombre d'hôtes présents dans un même domaine de collision est important, plus la fréquence des collisions augmente et plus les performances se dégradent. Pour garantir les meilleures conditions de communication, on cherche donc à réduire au maximum l'étendue du domaine de collision [4].

#### ➤ Domaine de diffusion

La diffusion est un mécanisme d'annonce générale qui assure que tous les hôtes d'un réseau local reçoivent les trames de diffusion émises par n'importe quel autre hôte de ce même réseau. Le domaine de diffusion est un réseau à l'intérieur duquel tous les hôtes peuvent émettre et doivent recevoir des trames de diffusion. Comme dans le cas précédent, plus le nombre d'hôtes présents dans le domaine de diffusion est important, plus les performances se dégradent. Là encore, pour garantir les meilleures conditions de communication, on cherche à réduire «raisonnablement» l'étendue du domaine de diffusion. [4]

---

<sup>1</sup> OSI : Open Systems Interconnection



## 5 Les architectures de réseaux

### 5.1 Le modèle OSI

Au début des années 70, chaque constructeur a développé sa propre solution réseau autour d'architecture et de protocole privés et il s'est vite avéré qu'il serait impossible d'interconnecter ces différents réseaux si une norme internationale n'était pas établie. Cette norme établie par l'internationale standard organisation (ISO) est la norme open system interconnexion (OSI, interconnexion de systèmes ouverts). [6]

Un système ouvert est un ordinateur, un terminal, un réseau, n'importe quel équipement respectant cette norme et donc apte à échanger des l'information avec d'autres équipement hétérogènes et issus de constructeurs différents.

La première objectif de la norme OSI a été de définir un modèle de toute architecture de réseau base sur découpage en sept couches chacun de ces couches correspondant à une fonctionnalité particulière d'un réseau.

Les couches 1, 2,3 et 4 sont dites basses et les couches 5,6 et 7 sont dites hautes. [2]

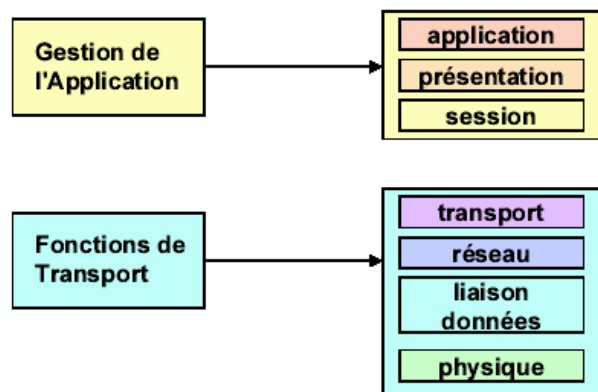


Figure 1.3 : Le model OSI

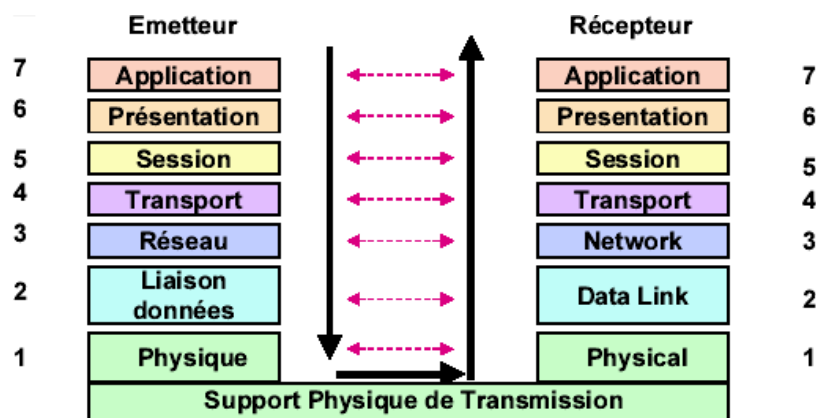


Figure1.4: Le model OSI en détail

❖ **La couche physique**

Cette couche définit les caractéristiques techniques, électriques, fonctionnelles et procédure les nécessaires à l'activation et à la désactivation des connexions physiques destinées à la transmission de bits entre deux entités de la couche liaisons de données.

❖ **La couche liaison**

Cette couche définit les moyens fonctionnels et procéduraux nécessaires à l'activation et à l'établissement ainsi qu'au maintien et à la libération des connexions de liaisons de données entre les entités du réseau.

Cette couche détecte et corrige, quand cela est possible, les erreurs de la couche physique et signale à la couche réseau les erreurs irrécupérables.

❖ **La couche réseau**

Cette couche assure toutes les fonctionnalités de services entre les entités du réseau, c'est à dire : l'adressage, le routage, le contrôle de flux, la détection et la correction d'erreurs non résolues par la couche liaison pour préparer le travail de la couche transport.

❖ **La couche transport**

Cette couche définit un transfert de données entre les entités en les déchargeant des détails d'exécution (contrôle entre l'OSI et le support de transmission).

Son rôle est d'optimiser l'utilisation des services de réseau disponibles afin d'assurer à moindre coût les performances requise par la couche session.

❖ **La couche session**

Cette couche fournit aux entités de la couche présentation les moyens d'organiser et de synchroniser les dialogues et les échanges de données. Il s'agit de la gestion d'accès, de sécurité et d'identification des services.

❖ **La couche présentation**

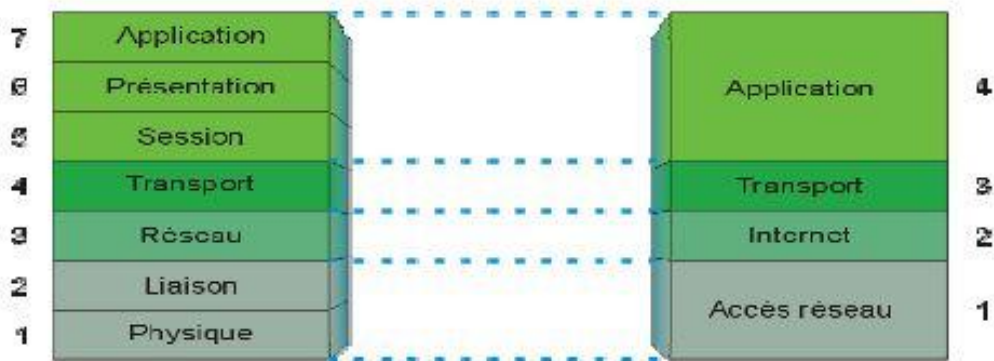
Cette couche assure la transparence du format des données à la couche application.

❖ **La couche application**

Cette couche assure aux processus d'application le moyen d'accès à l'environnement OSI et fournit tout les services directement utilisables par l'application (transfert de données, allocation de ressources, intégrité et cohérence des informations, synchronisation des applications). [6]

## 5.2 Le modèle TCP/IP

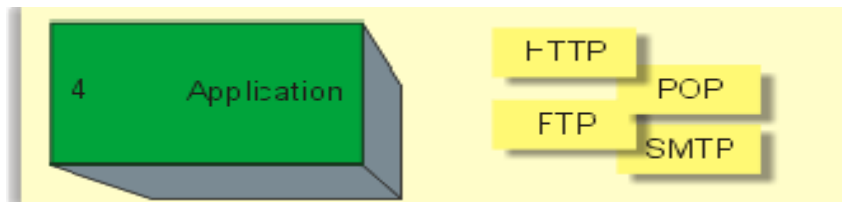
Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches :



**Figure 1.5 :** Le model TCP/IP et le model OSI

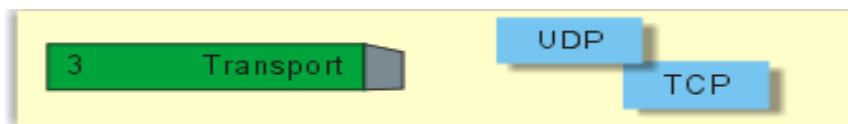
Le modèle OSI a été mis à côté pour faciliter la comparaison entre les deux modèles. Il y a 4 couches principales dans l'environnement TCP/IP :

- ❖ **couche application** : les applications interagissent avec les protocoles de la couche Transport pour envoyer ou recevoir des données.



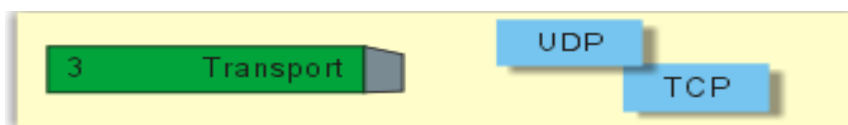
**Figure 1.6 :** La couche application

- ❖ **La couche transport** : chargé de fournir un moyen de communication de bout en bout entre 2 programmes d'application. Agi en mode connecté et en mode non connecté. Elle divise le flux de données venant des applications en paquets, transmis avec l'adresse destination IP au niveau IP.



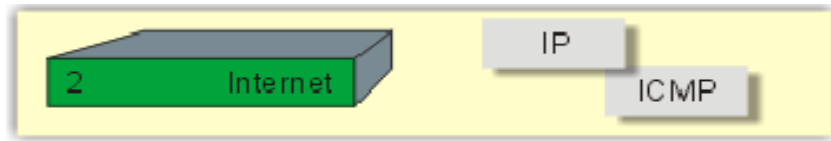
**Figure 1.7 :** La couche transport

- ❖ **La couche transport** : chargé de fournir un moyen de communication de bout en bout entre 2 programmes d'application. Agi en mode connecté et en mode non connecté. Elle divise le flux de données venant des applications en paquets, transmis avec l'adresse destination IP au niveau IP.



**Figure 1.8 :** La couche transport

- ❖ **La couche Internet** : encapsule les paquets reçus de la couche Transport dans des datagrammes IP. Mode non connecté et non fiable.



**Figure 1.9** : La couche Internet

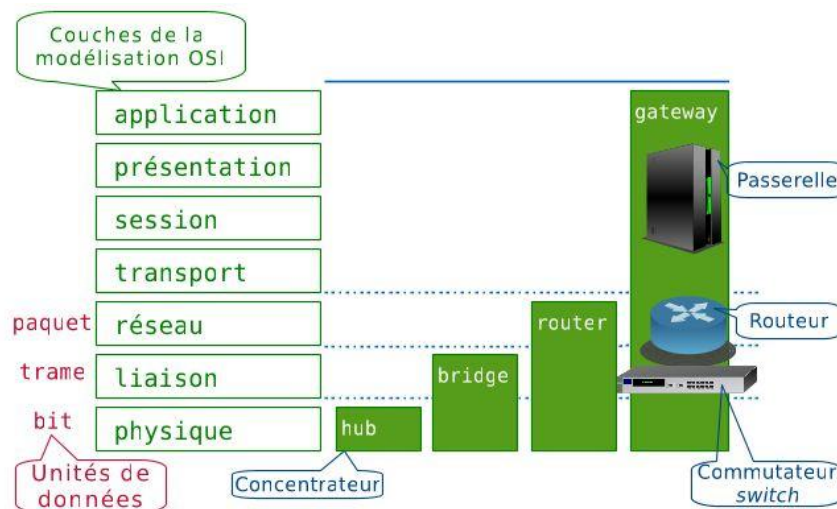
- ❖ **La couche Hôte Réseau** : assure la transmission d'un datagramme venant de la couche IP en l'encapsulant dans une trame physique et en transmettant cette dernière sur un réseau physique. [6]



**Figure1.10** : La couche réseau

### 5.3 Les unités de données et les équipements réseau

Les unités de données sont spécifiques à chaque couche du modèle, il est plus aisé de concevoir des équipements spécialisés dans le traitement de ces unités des données. On aboutit ainsi à la représentation suivante.



**Figure1.11** : couche OSI et les équipements

#### ➤ **Concentrateur :**

La capacité de traitement d'un concentrateur se limite à la couche physique et l'unité de données manipulée est le bit. Comme cet équipement est incapable de distinguer le début ou la fin d'un flot de bits, il n'a aucun impact sur la délimitation des domaines de collision ou de diffusion.

- **Pont :**

Ils servent à relier entre eux deux réseaux différents d'un point de vue physique. De plus ils filtrent les informations et ne laissent passer que celles qui doivent effectivement aller d'un réseau vers l'autre. Ils peuvent être utilisés pour augmenter les distances de câblage en cas d'affaiblissement prématuré du signal.

La capacité de traitement d'un pont couvre les couches liaison et physique. L'unité de données manipulée est la trame.

- **Commutateur :**

Un commutateur est un pont avec une électronique spécialisée qui garantit la bande passante par port.

Les bénéfices apportés par l'utilisation des commutateurs Ethernet sont nombreux. Un commutateur crée un domaine de collision distinct par port. Les connexions sur chaque port utilisent le mode full-duplex, ce qui offre des garanties sur les temps de transmission des trames. Enfin, on peut considérer qu'un commutateur multiplie la quantité totale de bande passante disponible sur un réseau local.

- **Routeur :**

La capacité de traitement d'un routeur couvre les trois couches basses du modèle OSI : physique, liaison et réseau. Les traitements du niveau réseau permettent de délimiter un domaine de diffusion par interface sur un routeur. Comme la gestion du sous-réseau inclut la couche liaison, une interface de routeur délimite aussi un domaine de collision.

Un routeur réalise des traitements plus complexes au niveau liaison. La prise de décision sur l'acheminement des paquets, c'est à dire le routage, est alimentée par un ou plusieurs protocoles de routage dynamique.

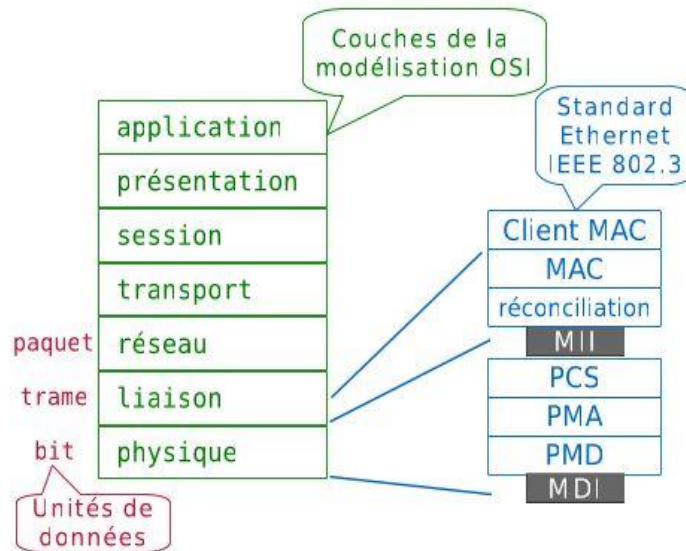
- **Passerelle :**

La capacité de traitement d'une passerelle couvre toutes les couches du modèle OSI de la couche application à la couche physique.

Parmi les traitements réalisés par une passerelle, on trouve les fonctions de cache de filtrage et de redirection. On peut citer les exemples des services mandataires avec filtrage d'URLs ou les services de routage d'appels en téléphonie sur IP.

## 5.4 Modélisation OSI et standard Ethernet

On fait correspondre le modèle OSI et le standard Ethernet, ce sont les couches physiques et une moitié de la couche liaison qui nous intéressent. [5]



**Figure1.12 : OSI et Ethernet**

- **MAC** : Media Access Control
- **Réconciliation** : La sous-couche *réconciliation* traduit les commandes de la sous-couche MAC sous une forme électrique appropriée pour les éléments de la couche physique.
- **MI** : *Media Independent Interface*. Cette interface isole la sous-couche MAC de la couche physique de façon à ce que plusieurs implémentations différentes soient utilisables au niveau de la couche physique.
- **PCS** : (Physical **C**oding **S**ublayer) Encodage/décodage des flux de données depuis et vers la sous-couche MAC. Les techniques de codage varient suivant les générations des variantes d'Ethernet et les débits.
- **PMA** : *Physical Medium Attachment*. Transformation et synchronisation des groupes de code en flux de bits adaptés à des composants de transmission série et vice versa
- **PMD** : (*Physical Medium Dependent*) Transmission du signal à l'aide des fonctions d'amplification, de modulation et de changement de forme d'onde. Ces fonctions varient suivant les variantes d'Ethernet et les débits.
- **MDI** : *Medium Dependent Interface*. Définitions des différents types de connecteurs suivant les médias utilisés : paires torsadées cuivre ou fibres optiques.

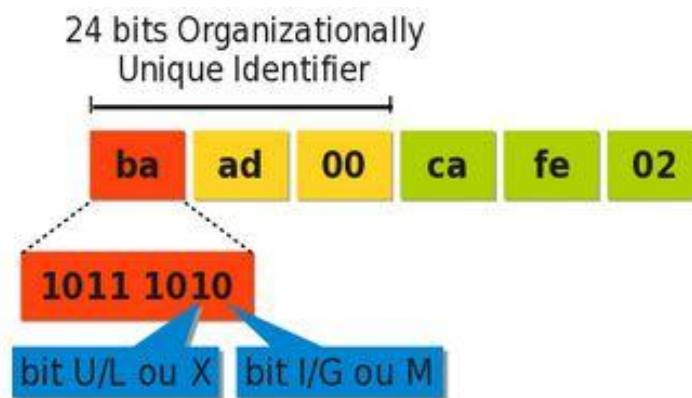
## 5.5 Types d'adresses MAC

Les adresses utilisées dans les trames Ethernet sont appelées adresses MAC ; acronyme issu du nom de la sous-couche consacrée à la méthode d'accès. Ces adresses sont représentées sur 48 bits ou 64 bits soit 6 ou 8 octets.

- **EUI-48 : (48-bit Extended Unique Identifier)**

La représentation sur 48 bits a été retenue par le comité *IEEE 802* et est utilisée dans plusieurs technologies réseau dont Ethernet.

Dans les spécifications de l'*IEEE*, l'espace d'adressage est découpé en deux parties. Les trois octets ou les 24 bits de poids fort sont réservés à l'identification du constructeur de l'interface réseau. C'est la partie **Organizationally Unique Identifier (OUI)** de l'adresse ; attribuée et enregistrée directement par l'*IEEE* ou l'*IANA*. Les trois octets ou les 24 bits de poids faible sont attribués par le constructeur comme numéro de série.[5]



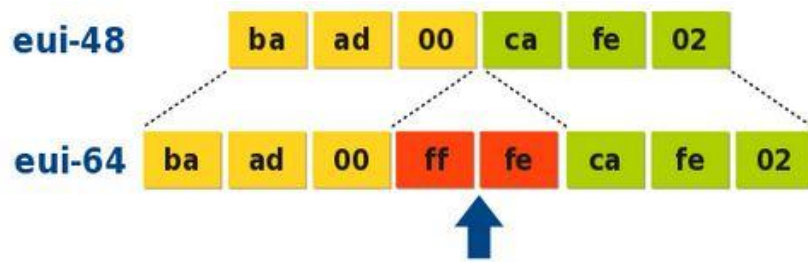
**Figure1.13 :** L'octet de poids le plus fort d'une Adresse MAC

La figure1.13 illustre les deux bits de poids faible l'octet de poids le plus fort servent à identifier les usages d'une adresse MAC.

- Le bit de rang 0 (de poids le plus faible) sert à distinguer une adresse individuelle (I) ou *unicast* (bit = 0) d'une adresse de groupe (G) ou *multicast* (M) (bit = 1).
- Le bit de rang 1 ou **Universal/Local** sert à distinguer une adresse universelle pour laquelle la partie *Organizationally Unique Identifier* a été attribuée par l'*IEEE* (bit = 0) d'une adresse pour laquelle la même partie est administrée localement (bit = 1).

➤ **EUI-64, 64-bit Extended Unique Identifier**

La représentation sur 64 bits des adresses MAC est apparue plus récemment dans les réseaux Ethernet. C'est encore l'*IEEE* qui publie les spécifications liées à l'utilisation de ces adresses sur 8 octets.[5]

**Figure1.14 : eui-48 et eui-64**

Les adresses au format EUI-64 sont de plus en plus répandues avec le déploiement du protocole IPv6 qui compose automatiquement les adresses de lien local avec l'adresse MAC sur 48 bits de l'interface dans laquelle deux octets supplémentaires insérés entre la partie OUI et la partie numéro de série.

**Exemple :** une interface ayant l'adresse MAC EUI-48 00:3f:1c:54:5e:65 aura pour adresse de lien local IPv6 :fe80:: 23f:1cff:fe54:5e65/64. On reconnaît ici l'insertion des deux octets ff:fe

Après cette présentation des différents formats et usages des adresses véhiculées dans les trames Ethernet, il est facile d'admettre que la constitution de groupes d'adresses sur une base logique ou hiérarchisée n'est pas possible. Il faut donc recourir à une modification des champs de la trame pour introduire cette notion de groupe logique. C'est justement l'objet des réseaux locaux virtuels ou VLANs.

## 6 Le routage

Le rôle fondamental de la couche réseau (niveau 3 de modèle OSI) est de déterminer la route que doivent propager les paquets qui fait référence à la fonction principale d'un routeur. Il distingue les différents protocoles de la couche réseau qui permet prendre des décisions plus sophistiquées de propagation.[1]

La fonction de routage construit la table de routage indiquant un chemin pour une destination désire, Ces tables sont mises à jour dynamiquement grâce aux protocoles de routage.



## **7 Conclusion**

Pour satisfaire notre besoins dans un réseau il faut tout d'abord bien choisir : une topologie adéquat, un bon système de câblage, les meilleur techniques de transmission et son oublier choisir une architecture conforme aux organismes de normalisation pour les réseaux.

Dans ce chapitre nous avons abordé la généralité sur les réseaux, et présenté différents types de réseau avec les architectures de réseaux. On a présenté les notions des réseaux locaux.

Aujourd'hui, il est plus que fréquent de voir l'utilisation de VLAN au sein d'un réseau d'entreprise. Le prochain chapitre portera sur les réseaux locaux virtuels (VLANs).

# CHAPITRE 2

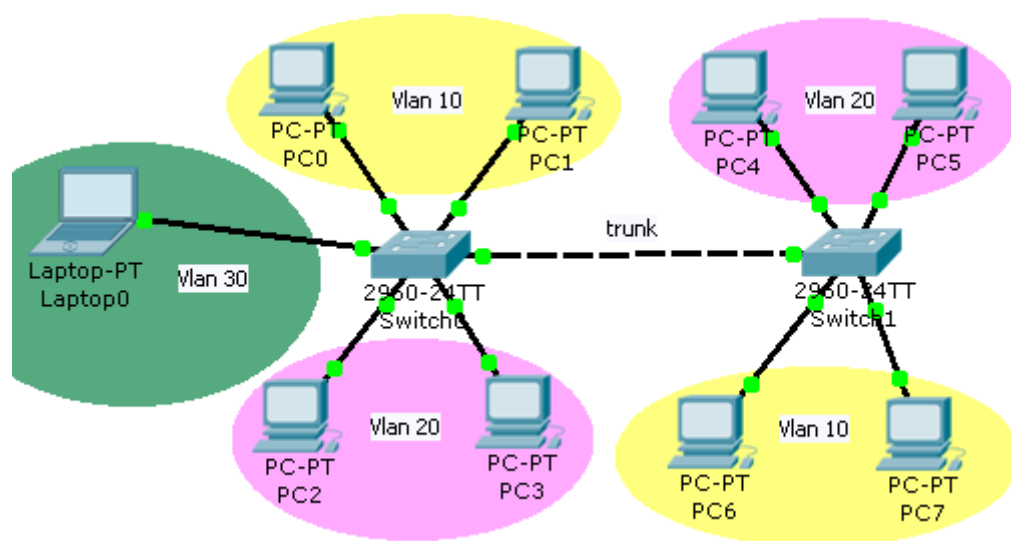
## RESAUX LOCAUX VIRTUELS

### 1 Introduction

De nombreuses techniques cherchent à améliorer la qualité d'un réseau du point de vue interconnexion. La mobilité des utilisateurs constitue une certaines limites pour le réseau local habituel, d'où la création des réseaux locaux virtuels ou VLANs. L'idée de base est de segmenter un réseau local non plus physiquement mais aussi logiquement, on réorganise ainsi les utilisateurs selon leurs emplacement, leurs fonctions, leurs travaux, et même par les applications ou protocoles qu'ils utilisent. Les Vlan sont en effet devenus depuis peu un facteur important pour la gestion des réseaux qu'on ne peut négliger, surtout si on considère le gain de sécurité qu'ils apportent.

### 2 Définition

Un LAN virtuel est un ensemble logique d'unités ou d'utilisateurs qui peuvent être regroupés par fonction, par service ou par application, quel que soit l'emplacement de leur segment physique. La configuration d'un LAN virtuel est effectuée au niveau du commutateur par un logiciel. Les LAN virtuels ne sont pas normalisés et nécessitent un logiciel spécial fourni par le fabricant du commutateur. Par la création d'un LAN virtuel on est capable de créer un petit domaine de diffusion dans les commutateurs et d'assigner différents ports du commutateur à différents sous réseaux.[7]



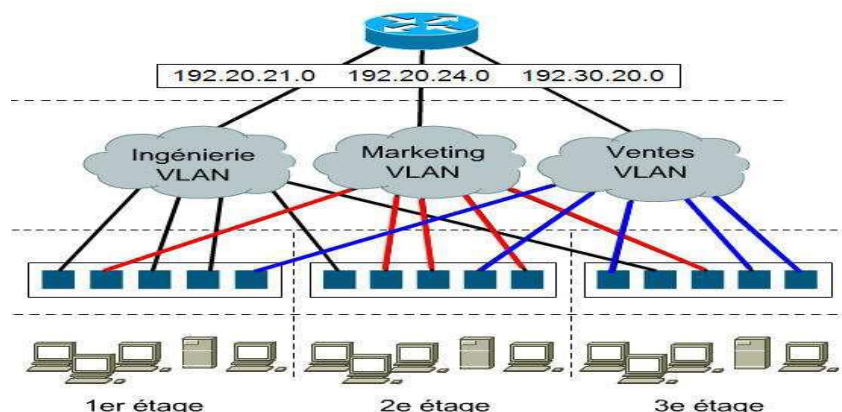
**Figure2.1 :** définition des groupes des VLANs

### 3 Type de VLAN

#### 3.1 Les VLAN statique

Les VLAN statique constituent la manière typique pour créer un LAN virtuel, mais aussi le plus sécurisant. Les ports du commutateur assignés manuellement à un VLAN est maintenu jusqu'à ce que l'administrateur du réseau change la configuration du VLAN ou l'association à un VLAN. Ce type de configuration est simple et facile à maintenir.

Une configuration le plus répandu est le vlan axés au port (ou vlan par port). Dans ce type de configuration on affecte à des ports le même type de LAN virtuel, donc ces ports reçoivent le même code d'identification VLAN.[8]



**Figure 2.2 :** Vlan axés au port

Dans ce schéma on voit que les ports du commutateur (Switch) sont affectés à différents LAN virtuels.

#### 3.2 Les VLAN dynamiques

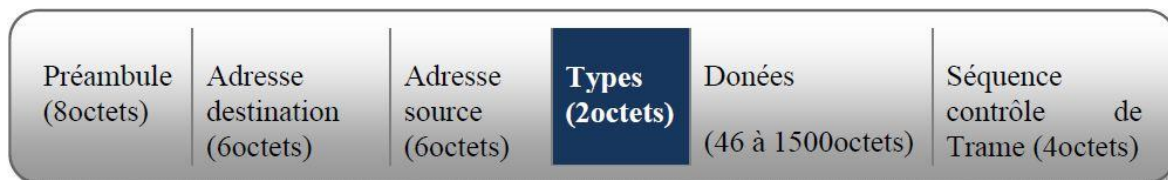
Les LAN virtuels dynamiques sont des ports de commutateur qui peuvent automatiquement déterminer les LAN virtuels auxquels ils sont affectés. Les fonctions de LAN virtuel dynamique sont basées sur les adresses MAC (VLAN par adresse MAC), l'adressage logique ou le type de protocole des paquets de données (VLAN de niveau 3). Lorsqu'une station est connectée pour la première fois à un port de commutateur non affecté, le commutateur approprié vérifie l'adresse MAC dans la base de données de gestion VLAN et configure dynamiquement le port selon la configuration VLAN correspondante.[13]

Les VLAN de niveau 3 consistent à utiliser des informations de niveau 3 comme critère d'appartenance à un Vlan. Le but est en effet de pouvoir identifier les individus d'un Vlan pour savoir où envoyer les informations, et en fait délimiter les différents domaines de diffusion. Ainsi on utilise les informations de niveau 3. [8]

On distingue deux types de LAN virtuel de niveau 3 :

❖ Les VLANs par protocoles :

On utilise les informations dans l'entête de la trame niveau 2 de l'utilisateur (pour identifier le protocole de niveau 3 utilisé). La seule lecture de cette information permet donc de déterminer dans quel domaine de broadcast doit être diffusée la trame. Exemple de l'entête Ethernet V2 :



**Figure 2.3 :** Format de l'entête Ethernet V2

On analyse le champ type pour déterminer le type de protocole. Voici quelques types courants.

Valeurs(en Hexa)	Protocoles
0x0800	Internet Protocol, Version 4 (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x080b	AppleTalk (Ethertalk)
0x8100	IEEE 802.1Q-tagged frame
0x86DD	Internet Protocol, Version 6 (IPv6)
0x8848	MPLS multicast

**Table 2.1:** Quelques valeurs du champ Ethertype

❖ Les VLANs par adresse de niveau 3 :

Comme dans le cas précédent, on utilise les informations de niveau 3 du modèle OSI. Pour les VLANs par adresse de niveau 3, les informations à étudier ne seront plus dans l'entête de la trame de niveau 2 mais dans le paquet de niveau 3 de l'utilisateur. Ce type de VLAN est donc applicable pour les protocoles routables (nécessite une adresse de niveau 3). Prenons comme exemple un réseau IP. On crée les différents VLANs à partir des sous réseaux.

➤ **Exemple de configuration de VLAN :**

Considérons un commutateur nommé Switch1

```
Switch1>enable
Switch1#configure terminal
Switch1 (config) #vlan 2
Switch1 (config-vlan) #name vlan Marketing
Switch1 (config)#interface FastEthernet0/1
Switch1 (config-if) #switchport mode access vlan 2
```

La première ligne permet d'entrer en mode privilège dans le matériel. La ligne suivante permet de configurer le Switch, en suite on à la base de données du matériel (Switch) et d'entrer le numéro et le nom du VLAN (vlan 2, vlan Marketing). Puis on accède le port concerné par le commande « interface *TypePort* ». Enfin on définit le mode d'accès au port concerné, dans notre cas « *access* » qui veut dire accès directe au port.

On définit deux types de mode d'accès au port. Un port access-link n'est associé qu'à un seul VLAN, un port trunk-link est associé à tous les VLAN.

## 4 Gestion de Vlan

Il existe plusieurs mécanismes de gestion des VLANs. Certains sont propriétaires et ne fonctionnent que sur les équipements d'une seule marque.

✓ **VLANs par ports**

Cette technique fournit une méthode de division d'un équipement de niveau 2 (commutateur) en plusieurs domaines de diffusion. La configuration de cette division est spécifique à chaque plateforme.

Bien que le coût d'administration de ce genre de configuration soit important puisqu'il faut gérer manuellement sur chaque équipement la distribution des réseaux locaux, cette technique est indépendante des plateformes et de leurs systèmes d'exploitation. C'est la raison principale pour laquelle elle est très répandue. Le commutateur assure une isolation complète entre l'hôte et le VLAN auquel il appartient. [5]

✓ **VLANs du type Cisco Inter-Switch Link, ISL VLANs**

Cette technique propriétaire a été développée spécifiquement pour les équipements Cisco™. Elle complète les en-têtes de trames avec 30 octets répartis en 13 champs. Ce type d'encapsulation n'est plus beaucoup utilisé du fait de son incompatibilité avec le standard IEEE 802.1Q.

## ✓ VLANs IEEE 802.1Q

Le standard IEEE 802.1Q fournit un mécanisme d'encapsulation très répandu et implanté dans de nombreux équipements de marques différentes. C'est sur ce standard que s'appuie ce document. L'en-tête de trame est complété par une balise de quatre octets. Les champs contenus dans ces quatre octets sont présentés dans la section suivante.[5]

## 5 Agrégation de Vlan et normes

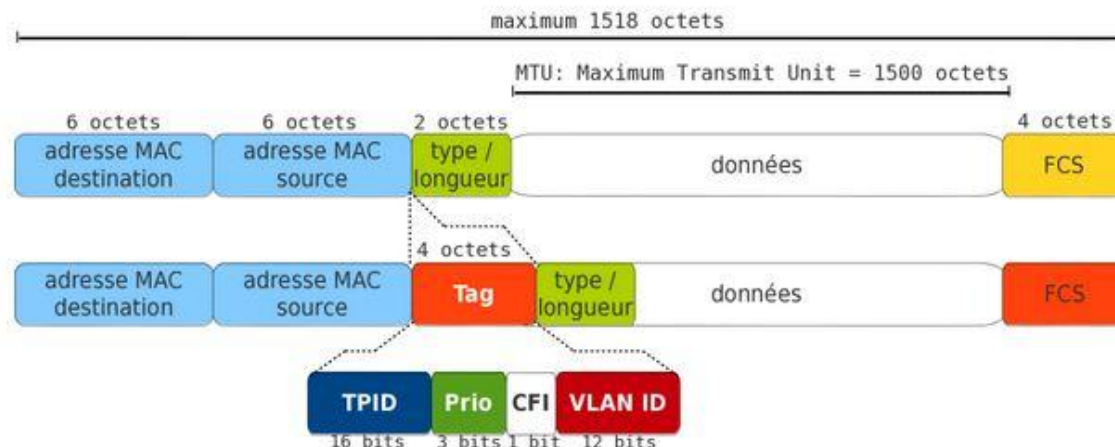
### 5.1 Vlan standard ou IEEE 802.10

Cette norme propriétaire CISCO dans un réseau FDDI (Fiber Data Distribution Interface). Cette compagnie a utilisé la norme 802.10, qui est originellement destiné à des spécifications de sécurités, pour implémenter la notion de Trame étiquetée (Frame Tagging).[9]

### 5.2 La norme 802.1Q

#### 5.2.1 La Balise 802.1Q

Le standard IEEE 802.1Q définit le contenu de la balise de VLAN (*VLAN tag*) avec laquelle on complète l'en-tête de trame Ethernet. Le format de la trame Ethernet modifiée avec les 4 octets supplémentaires est présenté dans la Figure 2.3 :[10]



**Figure 2.4 :** Trame encapsulée 802.1q

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

#### ❖ Tag protocol identifier, *TPID*, *EtherType*

Ce champ de 16 bits identifie le protocole véhiculé dans la trame. La valeur  $0 \times 8100$  désigne une balise IEEE 802.1Q / 802.1P.

#### ❖ *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.

❖ **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*).

❖ **VLAN Identifier, vlan id, VID**

Ce champ de 12 bits sert à identifier le réseau local virtuel auquel appartient la trame.

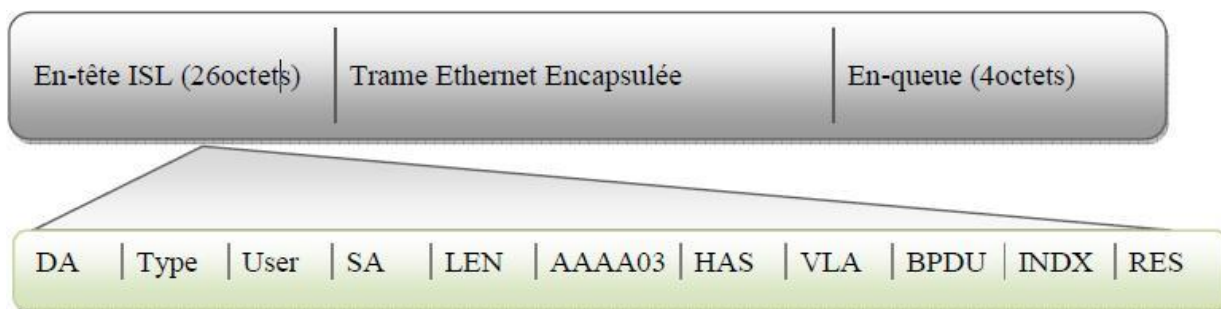
### 5.2.2 Le protocole ISL (Inter-Switch Link)

Ce type de protocole est propriétaire au commutateur CISCO, comme le 802.1q qui est un protocole standard pour l'encapsulation des trames inter, l'ISL est utilisé pour taguer les liaisons FastEthernet ou Gigabit Ethernet dans les équipements CISCO. [12]

La trame ISL ajoute un en-tête de 26 octets et une en-queue de 4 octets. ISL travail au dessus des protocoles existant c'est-à-dire il supporte de multiples protocoles de niveau 2 (Ethernet, Token Ring, ATM, FDDI).

Le seul problème avec ce protocole est de l'incompatibilité avec les standards IEEE, mais propose une qualité de transmission des trames assez intéressantes pour les équipements CISCO.

Voici le format d'une trame ISL



**Figure 2.5 : Trame ISL**

DA : (40 bits) adresse de destination. L'adresse multicast 0x01-00-0C-00-00 ou 0x03-00-0C-00-00 pour indiquer que c'est une trame ISL.

Champ Type :

Valeurs	Types
0000	Ethernet
0001	Token Ring
0010	FDDI
0011	ATM

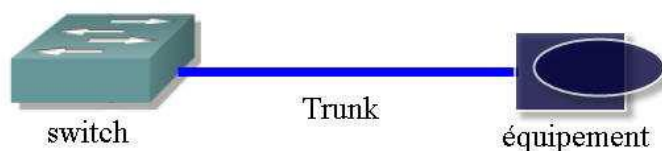
**Table 2.2:** Valeur du champ Type pour ISL

- ❖ **User** :(4bits) définit la priorité Ethernet, 0 minimum et 3 maximums.
- ❖ **SA** :(48bits) adresse MAC source
- ❖ **LEN ou length** :(16bits) indique la longueur des champs DA, Type, User, SA, LEN et CRC
- ❖ **AAAA03** : définit le SNAP (Standard subNetwork Access Protocole) et le LLC (logical link header).
- ❖ **HSA** :(3bits) les trois bits de l'adresse source.
- ❖ **VLA** :(15 bits) pour numéroté les VLAN, on utilise les 10 derniers bits donc on a  $10^{10}=1024$  VLANs.
- ❖ **BPDU** :(1bit) indique si la trame est une trame BPDU du spanning Tree (arbre couvrant) ou si la trame encapsulée est du CDP (Cisco Discovery Protocol), du VTP (Virtual Trunking Protocol).
- ❖ **INDEX** : (16bits) indique l'index du port source du paquet sur le Switch.
- ❖ **RES** : (16bits) réservé pour Token Ring et FDDI.

### 5.3 Le protocole VTP (Vlan trunk Protocol)

#### 5.3.1 Trunking méthode

La liaison en mode Trunk (ou Tronc) est une liaison point à point. On l'utilise souvent dans les liaisons peuvent atteindre une vitesse de 100 Mbps ou 1000Mbps entre deux Switch (commutateurs), ou un Switch et un routeur, ou un Switch et un serveur.



**Figure 2.6:** Liaison en mode Trunk



Le Trunking (Tronc) permet à une liaison (à un port) d'être subdivisée de façon logique pour pouvoir transporter plusieurs VLAN en même temps. Dans ce cas il est possible d'avoir un domaine de diffusion en même temps mais dans différentes liaisons logiques.



**Figure 2.7 :** Subdivision d'une liaison physique en liaison logique (Trunking)

L'avantage de l'utilisation d'une liaison en mode Trunk est qu'il est possible de transmettre quelques informations concernant tous les VLANs dans la liaison physique. Pour les matériels CISCO par exemple, ils utilisent le protocole DTP (Dynamic Trunking Protocol) pour transmettre les informations pour une trame étiquetée avec le 802.1q.

### 5.3.2 Le protocole VTP

Le protocole VTP (Vlan Trunk protocol), utilisé dans les équipements CISCO, permet de gérer dynamiquement les Vlan au même titre que le GVRP. Ce protocole permet à un segment en mode Trunk entre les ponts (il n'est jamais utilisé entre les hôtes). Il est aussi utilisé pour maintenir la base de données entre les ponts (paramètres du vlan, protocole d'étiquette, nom du vlan,...). En d'autre terme le VTP protocole est utilisé pour configurer et d'administrer les VLANs sur les matériels. [11]

On peut distinguer trois modes de fonctionnements :

- VTP mode server assure la configuration du réseau et déploiement.
- VTP mode client pour déterminer la configuration du réseau.
- VTP mode transparent configure le réseau localement c'est-à-dire pas via VTP (n'accepte pas les mis à jour de la base de données), par contre on peut propager les messages via le segment en mode trunk.

Le VTP permet de maintenir l'uniformité dans tout le réseau, c'est-à-dire que chaque équipement possède les informations concernant la configuration du réseau.

### 5.4 L'IEEE 802.1p

Ce protocole normalisé par l'IEEE permet de faciliter les performances des commutateurs et des ponts, le 802.1p introduit la notion de classe de service permettant de déterminer la priorité entre les trafics sur les réseaux en cas des congestions de la liaison. Donc une file d'attente est gérée pour réorganiser les flux et afin de déterminer qui est la priorité rapide et qui est considérée priorité normale. [12]

## 6 Avantage VLAN

La productivité des utilisateurs et l'adaptabilité du réseau sont importantes pour la croissance et la réussite de l'entreprise. Les VLAN permettent d'adapter un réseau selon les objectifs de l'entreprise. Les principaux avantages des VLAN sont les suivants : [14]

- **Sécurité** : les groupes contenant des données sensibles sont séparés du reste du réseau, ce qui diminue les risques de violation de confidentialité.
- **Réduction des coûts** : des économies sont réalisées grâce à une diminution des mises à niveau onéreuses du réseau et à l'utilisation plus efficace de la bande passante et des liaisons montantes existantes.
- **Meilleures performances** : le fait de diviser des réseaux linéaires de couche 2 en plusieurs groupes de travail logiques (domaines de diffusion) réduit la quantité de trafic inutile sur le réseau et augmente les performances.
- **Réduction des domaines de diffusion** : la division d'un réseau en VLAN réduit le nombre de périphériques dans le domaine de diffusion.
- **Efficacité accrue du personnel informatique** : les VLAN facilitent la gestion du réseau, car les utilisateurs ayant des besoins réseau similaires partagent le même VLAN. Lorsque vous configurez un nouveau commutateur, toutes les stratégies et procédures déjà configurées pour le VLAN correspondant sont implémentées lorsque les ports sont affectés. Le personnel informatique peut aussi identifier facilement la fonction d'un VLAN en lui donnant un nom approprié.
- **Gestion simplifiée de projets et d'applications** : les VLAN rassemblent des utilisateurs et des périphériques réseau pour prendre en charge des impératifs commerciaux ou géographiques. La séparation des fonctions facilite la gestion d'un projet ou l'utilisation d'une application spécialisée.

## 7 Conclusion

Les VLANs, Virtual Local Area Networks, introduisent donc un nouveau concept à l'intérieur des entreprises. En effet, cette technologie a le potentiel pour répondre au besoin de mouvement en interne des entreprises. Ainsi, une entreprise peut réorganiser l'ensemble de ces services ou de ces groupes de travail sans que le responsable Télécom ne soit à passer de longues heures à reconfigurer l'ensemble des machines du parc. Les VLANs apportent donc une très grande flexibilité dans la gestion du réseau. Les VLANs vont ainsi permettre à l'entreprise de songer à des réorganisations futures sans se soucier de la

situation physique de l'existant informatique. Ainsi, le déploiement de réseaux virtuels est un choix stratégique pour l'entreprise pour ainsi diminuer les coûts de déplacement des utilisateurs entre les services.

# CHAPITRE 3

## ROUTAGE INTER-VLAN

---

### 1 Introduction

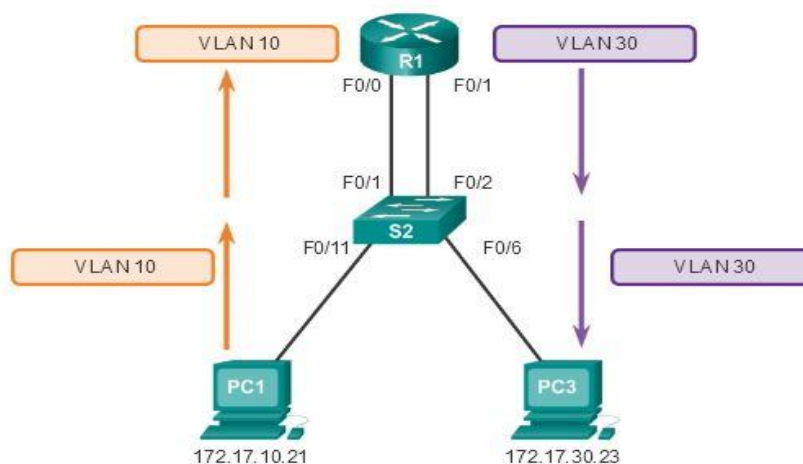
L'utilisation des VLAN pour segmenter un réseau commuté permet d'améliorer les performances, la facilité de gestion et la sécurité. Les trunks servent à faire circuler des informations entre les périphériques depuis des VLAN multiples. Cependant, étant donné que ces VLAN ont segmenté le réseau, un processus de couche 3 est requis pour permettre au trafic de se déplacer d'un segment du réseau à un autre.

Ce chapitre porte sur les méthodes utilisées pour l'implémentation du routage inter-VLAN. Il inclut des configurations aussi bien pour l'utilisation d'un routeur que celle d'un commutateur de couche 3. Il décrit également des problèmes rencontrés lors de l'implémentation du routage inter-VLAN et les techniques de dépannage standard.

### 2 Fonctionnement du routage inter-vlan

#### 2.1 Qu'est ce que le routage inter-vlan ?

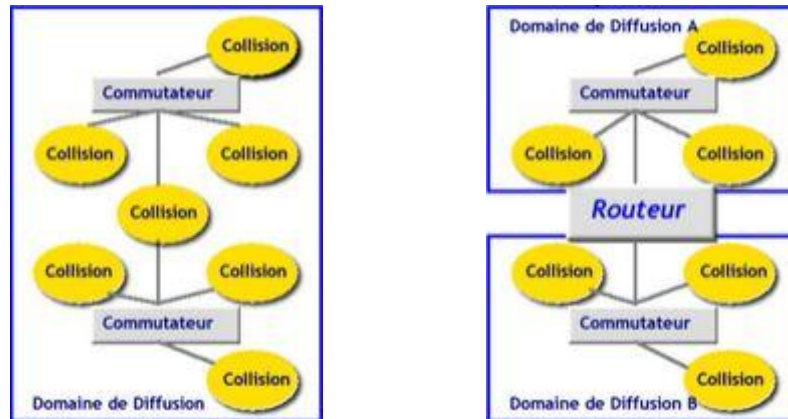
Un VLAN est un domaine de diffusion : les ordinateurs se trouvant sur des VLAN différents ne peuvent donc pas communiquer sans l'intervention d'un dispositif de routage. Un périphérique qui prend en charge le routage de couche 3, tel qu'un routeur ou un commutateur multicouche, permet d'exécuter les fonctions de routage nécessaires. Quel que soit le périphérique utilisé, le processus de transfert du trafic réseau d'un VLAN à un autre à l'aide du routage est appelé routage inter-VLAN.[14]



**Figure3.1** Routage inter-vlan

A partir de la Segmentation des réseaux locaux, on déduit deux règles de base :

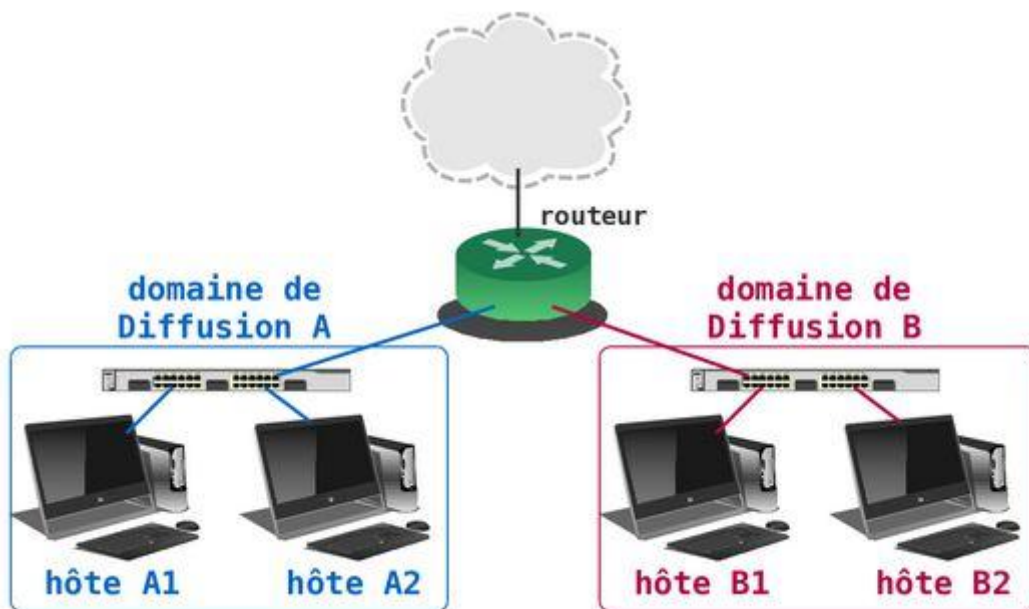
- ✓ Une interface de commutateur délimite un domaine de collision.
- ✓ Une interface de routeur délimite à la fois un domaine de collision et un domaine de diffusion.



**Figure 3.2** Domaine de diffusion et collision

## 2.2 Situation avant routage inter-VLAN

Du point de vue conception, le respect de ces deux règles impose que l'on ajoute une interface de routeur pour chaque nouveau domaine de diffusion ou périmètre de contrôle. De plus, les commutateurs appartenant à un domaine de diffusion sont dédiés à ce domaine. Il n'est pas possible de distribuer plusieurs réseaux locaux virtuels entre plusieurs domaines de diffusion «isolés» par un routeur.



**Figure3.3** Scénario avant routage inter-vlan

La figure3.3 représente une conception sans routage inter-vlan, donc on déduit quelque points sure cette conception sont :

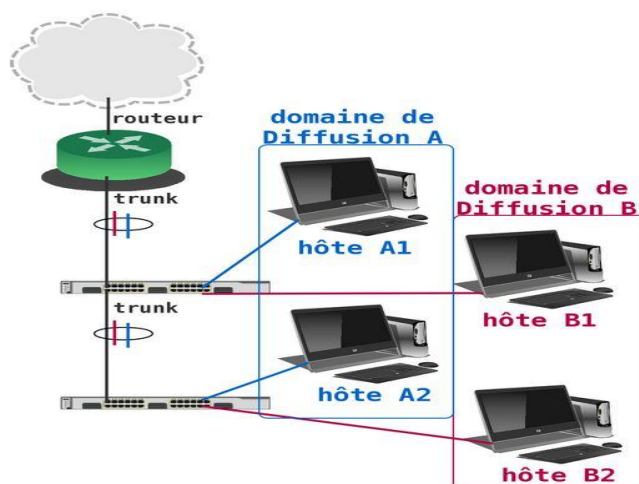
- Si on programme le commutateur A avec 2 VLANs distincts pour chacun des PCs A1 et A2, alors toute communication entre A1 et A2 sera impossible. De plus, ces deux PCs ne pourront communiquer avec d'autres réseaux que si l'interface du routeur RA appartient aux deux VLANs programmés.
- Cette situation peut présenter des avantages du point de vue exploitation mais elle dépend beaucoup de la gestion des interfaces physiques. Ce que ne montre pas le diagramme simplifié ci-dessus, c'est que le coût d'administration devient très important dès que le nombre de réseaux virtuels augmente.
- Si l'utilisateur «associé» au PC A1 déménage dans un lieu où 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.

Ce scénario montre qu'il est excessivement difficile d'optimiser le parc des ports de commutateurs avec ce type d'architecture. Le coût de l'infrastructure augmente donc fortement puisqu'il faut passer par des réinvestissements lourds en câblage et en équipements à chaque modification des périmètres.

### 2.3 Situation après routage inter-VLAN

Les deux règles de base énoncées ci-dessus ne sont pas remises en question. Il s'agit maintenant de dissocier 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».[5]



**Figure3.4** Scénario après le routage inter vlan

Des remarques sur ce type de conception relativement à la situation sans routage inter-VLAN :

- 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 donc 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.

#### **2.4 Bande passante et trunks**

En reprenant la remarque sur le partage des débits entre les VLANs à l'intérieur des trunks, il devient intéressant de partager le débit disponible en fond de panier dans des châssis de commutateurs. Le critère de choix d'un équipement, commutateur ou routeur, s'articule de plus en plus autour du rapport entre la capacité de commutation en millions de paquets par seconde (mpps) et le prix d'achat.

L'augmentation régulière des débits utiles par port favorise l'adoption d'architectures à base de routage inter-VLAN. Les évolutions techniques des routeurs conduisent à diminuer le nombre de leurs interfaces alors que les évolutions des commutateurs conduisent à augmenter considérablement le nombre de leurs ports. [5]

#### **2.5 Les Méthodes du routage inter-vlan**

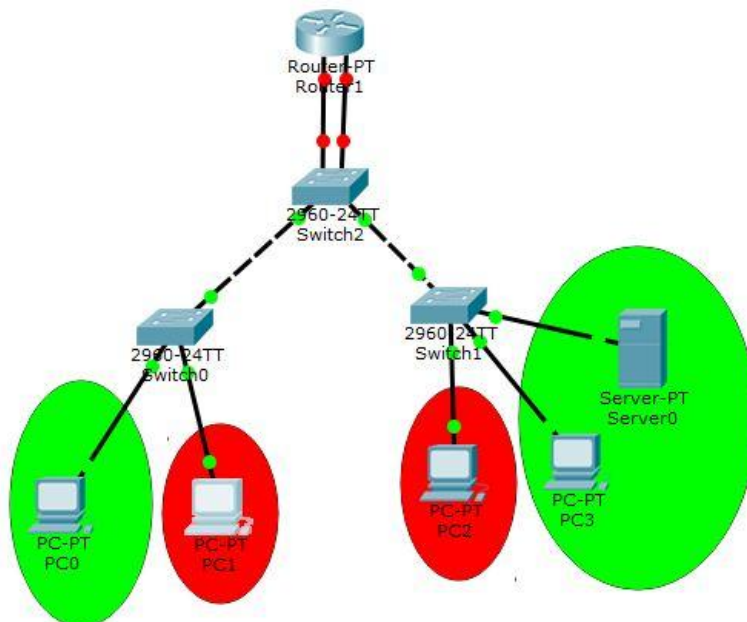
IL existe trois moyens pour configurer le routage inter-VLAN, de façon physique, de façon logique (Router on a stick) et avec des commutateurs multicouche.

#### **2.6 Routage inter-vlan physique**

La première méthode de routage inter-VLAN reposait sur des routeurs utilise plusieurs liens physiques pour permettre aux différents VLAN de communiquer entre eux. Chaque interface ou bien lien physique devait être connectée à un VLAN distinct et configurée pour un sous-réseau différent.[14]

Le routage inter-VLAN s'effectue par la connexion de différentes interfaces de routeur physiques à différents ports de commutateur physiques. Les ports de commutateur connectés

au routeur sont placés en mode d'accès et chaque interface physique est affectée à un VLAN distinct. Chaque interface de routeur peut alors accepter le trafic du VLAN associé à l'interface de commutateur à laquelle elle est connectée, et le trafic peut être acheminé vers les autres VLAN connectés aux autres interfaces.



**Figure3.5** le Routage inter-vlan physique

Dans la Figure3.5 illustre le routage inter-VLAN physique, on a deux VLANs donc deux liens physiques.

- **Configuration**

Pour configurer notre routage inter-VLAN physique il faut :

- d'abord configurer notre Switch 2 pour que l'interface Fa0/3 soit dans le VLAN 10

```
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

- Ensuite il nous faut configurer les adresses IP de nos interfaces du routeur pour qu'ils correspondent au bon sous réseau.



```

Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 10.1.10.5 255.255.255.0
Router(config-if)#no shutdown
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip address 10.1.20.5 255.255.255.0
Router(config-if)#no shutdown

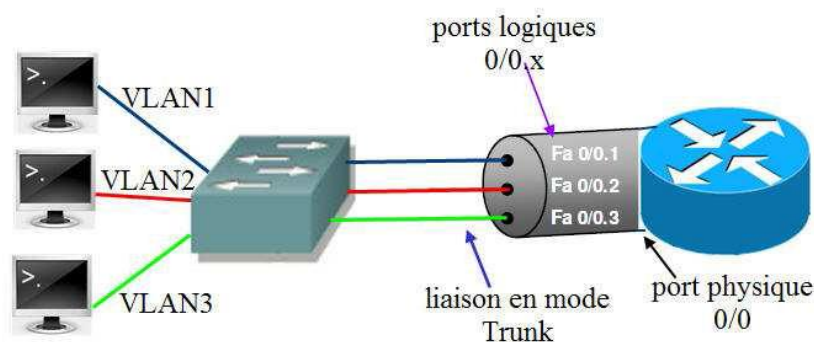
```

Alors le routage inter-VLAN est configurée il est maintenant possible de communiquer entre les VLAN à condition de désigner comme passerelle par défaut de nos ordinateurs l'adresse IP de l'interface du routeur correspondant au VLAN auquel appartient l'ordinateur.

### 2.6.1 Routage inter-vlan logique (Router on a stick)

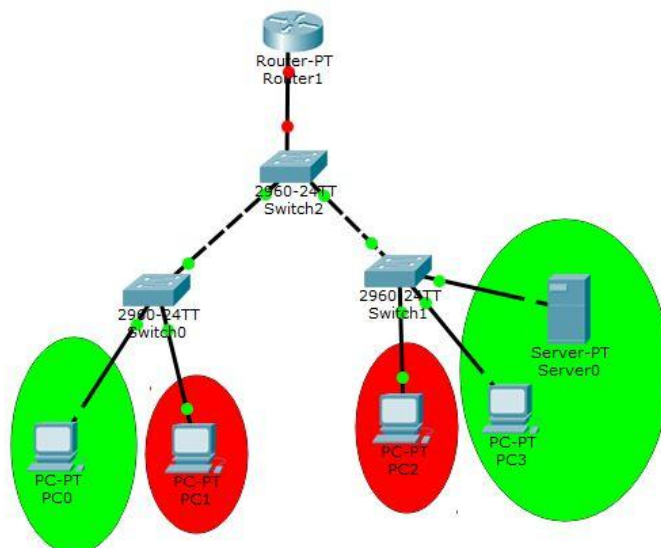
La méthode « router-on-a-stick » est un type de configuration de routeur dans laquelle une seule interface physique achemine le trafic entre plusieurs VLAN d'un réseau. Comme vous pouvez le voir dans la figure, le routeur est connecté au commutateur S1 à l'aide d'une seule connexion réseau physique (un trunk).

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 VLAN à l'aide de 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.



**Figure 3.6 :** Division d'un port physique en port logique au sein d'un routeur

La figure suivante présente l'architecture de routage inter-vlan, comme elle est montrée la figure 3.7 le routeur utilise un seul lien pour propager les deux VLANs



**Figure 3.7** Le routage inter-vlan Router on a stick

- **Configuration**

Pour configurer le routage inter-VLAN « Router on a stick » il faut :

- d'abord configurer un trunk sur l'interface FA0/3 du Switch 2

```
Switch (config-if)#interface fastEthernet 0/3
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport native vlan 99
Switch(config-if)#no shutdown
```

- Puis il faut configurer notre routeur. Pour cela nous allons créer des sous interfaces.

```
Router(config)#interface fastEthernet 0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 10.1.10.5 255.255.255.0
Router(config-subif)#interface Fa0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 10.1.20.5 255.255.255.0
Router(config)#interface fastEthernet 0/0
Router(config-if)#no shutdown
```

- Nous avons donc créé deux sous interface Fa0/0.10 et Fa0/0.20 l'une pour le VLAN 10 et l'autre pour le VLAN 20. Notez que l'interface physique doit être allumée avec que le routage inter-VLAN fonctionne.

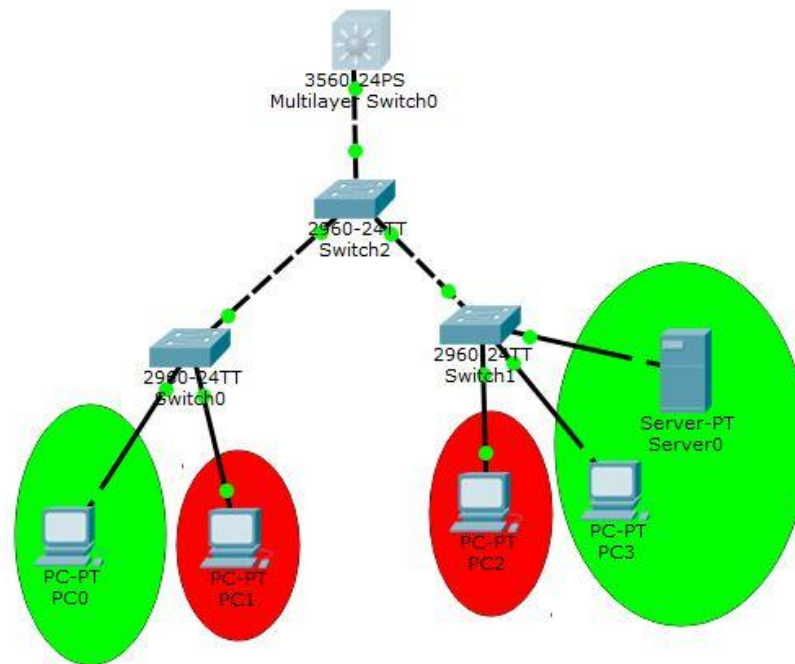
Le routage inter-VLAN logique est configuré, les VLAN peuvent maintenant communiquer entre eux à condition de désigner comme passerelle par défaut de nos

ordinateurs l'adresse IP de l'interface du routeur correspondant au VLAN auquel appartient l'ordinateur.

## 2.7 Routage inter-vlan des commutateurs multicouche

Les commutateurs multicouches peuvent effectuer des fonctions de couche 2 et 3, ce qui évite aux routeurs dédiés d'effectuer du routage de base sur un réseau. Les commutateurs multicouches prennent en charge le routage dynamique et le routage inter-VLAN.

La figure 3.8 suivante



**Figure 3.8** Le routage inter-vlan des commutateurs de multicouche

## 3 Dépannage du routage inter-VLAN

### 3.1 Problèmes de configuration inter-VLAN

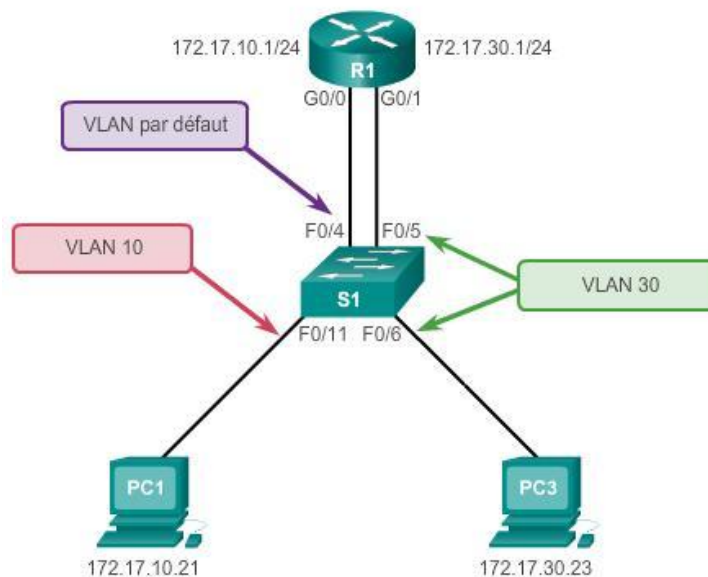
Il n'est pas rare que certaines erreurs surviennent lors de la configuration du routage entre plusieurs VLAN. On cite quelques problèmes réputés

#### 3.1.1 Problème lié aux ports de commutateur

Lors de l'utilisation du modèle de routage existant pour le routage inter-VLAN, assurez-vous que les ports de commutateur se connectant aux interfaces de routeur sont configurés sur les VLAN corrects. Si un port de commutateur n'est pas configuré pour le bon VLAN, les périphériques configurés sur ce VLAN ne peuvent pas se connecter à l'interface du routeur et sont donc incapables d'envoyer des données à d'autres VLAN.[11]

Comme présenté dans la topologie de la Figure 3.9, le PC1 et l'interface G0/0 du routeur R1 sont configurés pour se trouver sur le même sous-réseau logique, comme indiqué par leur

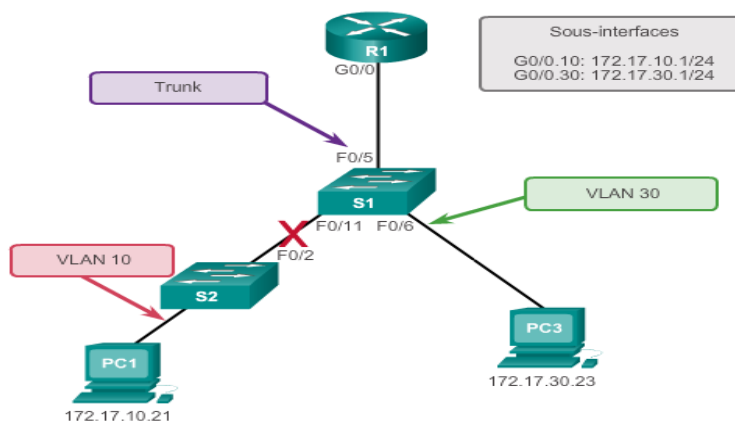
affectation d'adresse IP. Cependant, le port de commutateur F0/4 qui se connecte à l'interface G0/0 du routeur R1 n'a pas été configuré et reste dans le VLAN par défaut. Le routeur R1 se trouvant sur un autre VLAN que PC1, ils ne sont pas en mesure de communiquer.



**Figure 3.9** topologie avec problème de configuration dans le Switch

Pour corriger ce problème, exécutez la commande de mode de configuration d'interface **switchport access vlan 10** sur le port de commutateur F0/4 du commutateur S1. Lorsque le port de commutateur est configuré pour le VLAN correct, PC1 peut communiquer avec l'interface G0/0 du routeur R1, qui lui permet d'accéder aux autres VLAN connectés au routeur R1.

La topologie de la Figure 3.10 montre que la liaison trunk entre S1 et S2 est interrompue. Comme il n'existe aucun chemin ni connexion redondante entre les périphériques, tous les périphériques connectés à S2 sont incapables d'atteindre R1. Par conséquent, tous les périphériques connectés à S2 sont incapables d'assurer le routage vers d'autres VLAN via R1.



**Figure 3.10** problèmes de lien tombe en panne

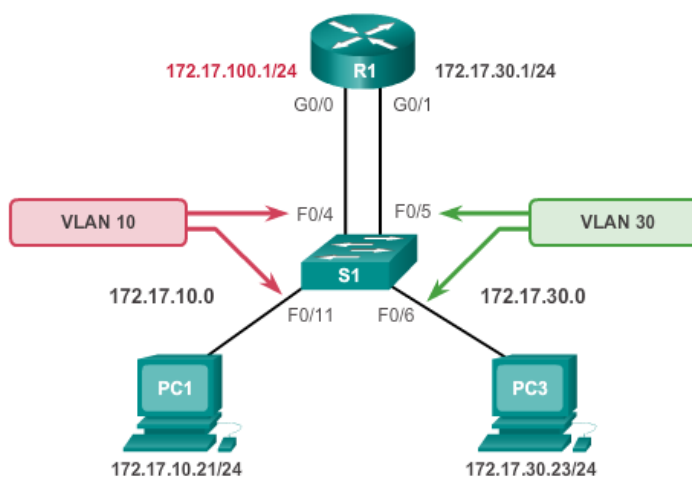
Pour réduire les risques de liaison défectueuse entre commutateurs interrompant le routage inter-VLAN, les liaisons redondantes et les chemins de substitution doivent être pris en compte dans la conception du réseau.

### 3.2 Problèmes d'adressage IP

Les VLAN correspondent à des sous-réseaux uniques sur le réseau. Pour que le routage inter-VLAN fonctionne, un routeur doit être connecté à tous les VLAN, par des interfaces physiques distinctes ou des sous-interfaces. Une adresse IP correspondant au sous-réseau pour lequel elle est connectée doit être affectée à chaque interface ou sous-interface. Ceci permet aux périphériques du VLAN de communiquer avec l'interface de routeur et d'activer le routage de trafic vers d'autres VLAN connectés au routeur. [14]

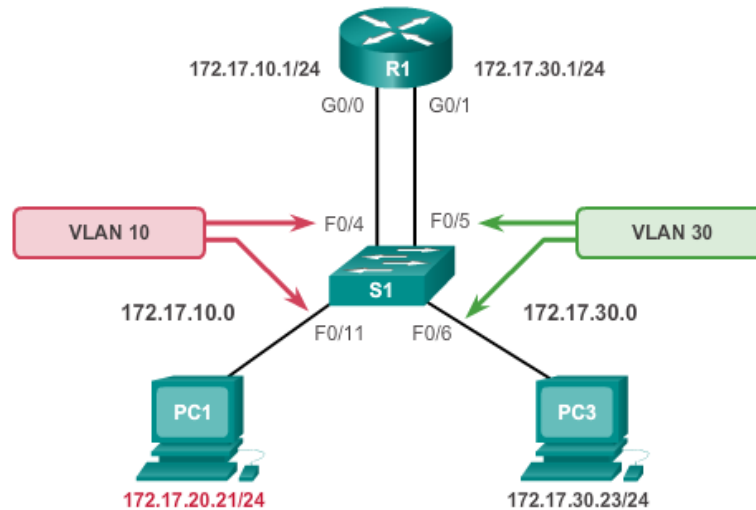
Voici quelques erreurs courantes d'adressage IP :

- Comme l'illustre la Figure 3.11, le routeur R1 a été configuré avec une adresse IP incorrecte sur l'interface G0/0, ce qui empêche le PC1 de communiquer avec le routeur R1 sur le VLAN 10. Pour corriger ce problème, affectez l'adresse IP correcte à l'interface G0/0 du routeur R1 à l'aide de la commande `ip address 172.17.10.1 255.255.255.0`. Une fois l'adresse IP correcte affectée à l'interface du routeur, le PC1 peut utiliser cette dernière comme passerelle par défaut pour accéder à d'autres VLAN.



**Figure 3.11** Topologie avec Adresse ip de routeur 1 mal configuré

- Dans la Figure 2, le PC1 a été configuré avec une adresse IP incorrecte pour le sous-réseau associé au VLAN 10. Ceci empêche PC1 de communiquer avec le routeur R1 sur le VLAN 10. Pour corriger ce problème, affectez l'adresse IP correcte à PC1. Selon le type de PC utilisé, les détails de configuration peuvent être différents.



**Figure 3.12** Topologie avec Adresse de PC1 mal configuré

## 4 Conclusion

Le routage inter-VLAN est le processus de routage de trafic entre différents VLAN, en utilisant un routeur dédié ou un commutateur multicouche. Le routage inter-VLAN facilite la communication entre des périphériques isolés par des limites de VLAN.

Après l'étude de routage inter-vlan et les VLANs nous pouvons conclure que les VLANs sont très utiles dans un réseau car ils permettent de séparer en plusieurs segments logique un réseau. En outre les VLANs permettent d'améliorer la gestion du réseau, d'optimiser la bande passante, et de segmenter un domaine de broadcast. Puisqu'ils seront indispensables dans l'étape suivante, qui consiste à la réalisation de notre travail, qu'on va présenter dans le chapitre suivant.

# CHAPITRE 4

## ETUDE PAR LA SIMULATION ROUTAGE INTER-VLAN

---

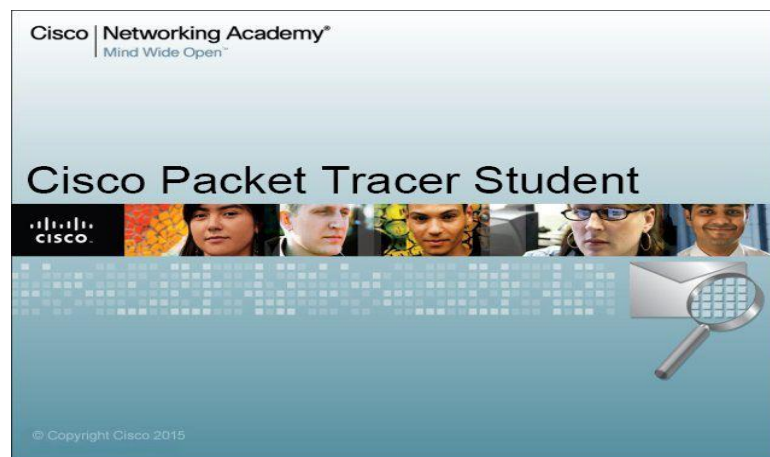
### 1 Introduction

Avant de déployer et de mettre en place un réseau, il est nécessaire de voir son fonctionnement afin d'éviter tout risque de perte. Pour évaluer les performances du Routage inter-vlan présenté dans le chapitre précédent, nous avons effectué des simulations, d'abord nous allons présenter les outils de simulation utilisés, Il s'agit le simulateur Packet Tracer 6.2.0, on a simulé la conception des VLANs et le routage entre eux, en suite, on a utilisé le Opnet simulateur pour faire une étude comparative entre architecteur de réseaux utilise le vlan et sans VLANs (LAN). En fin, nous allons étudier la performance des réseaux avec VLAN et routage inter vlan et sans utiliser les VLANs dans l'aspect transfert des packets.

### 2 Le logiciel Packet Tracer

Le logiciel Packet Tracer est un logiciel fourni par l'entreprise CISCO. Il fournit une interface souple et permet de visualiser le réseau dans son aspect logique et physique. Dans Packet Tracer la simulation est basée sur l'étude de la conception et la forme du réseau, la configuration et la réparation des réseaux informatiques. Ainsi la simulation se situe à travers une configuration des différents dispositifs dans le logiciel.[15]

Packet Tracer se fonde sur un modèle simplifié des dispositifs et des protocoles de gestion de réseau. Les vrais réseaux informatiques demeurent le repère des qualifications pour comprendre le comportement du réseau et de développer une gestion du réseau.



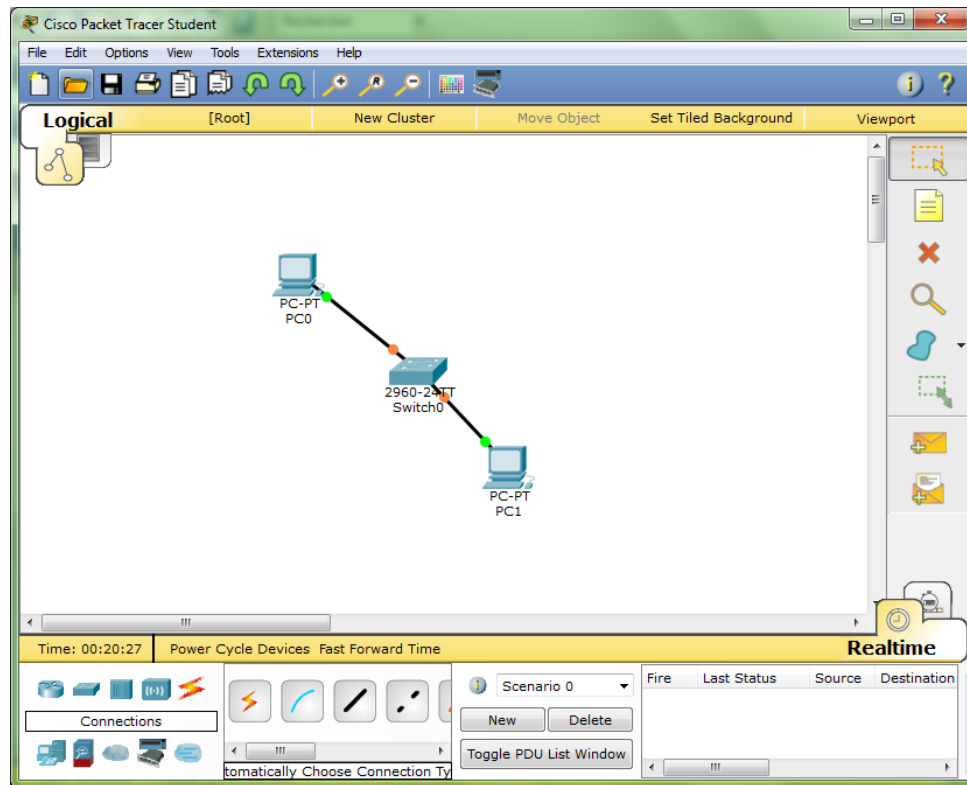
**Figure 4.1 : Démarrage de Packet Tracer 6.2.0**

## 2.1 Fonctionnement du logiciel Packet Tracer

Le logiciel fonctionne sous deux différents aspects. Il permet ainsi de visualiser l'état du réseau en deux points de vue distincts.

### 2.1.1 L'espace de travail logique (Logical workspace)

C'est dans cette partie du logiciel qu'on passe beaucoup du temps, car il permet de créer et de configurer le réseau qu'on étudie.

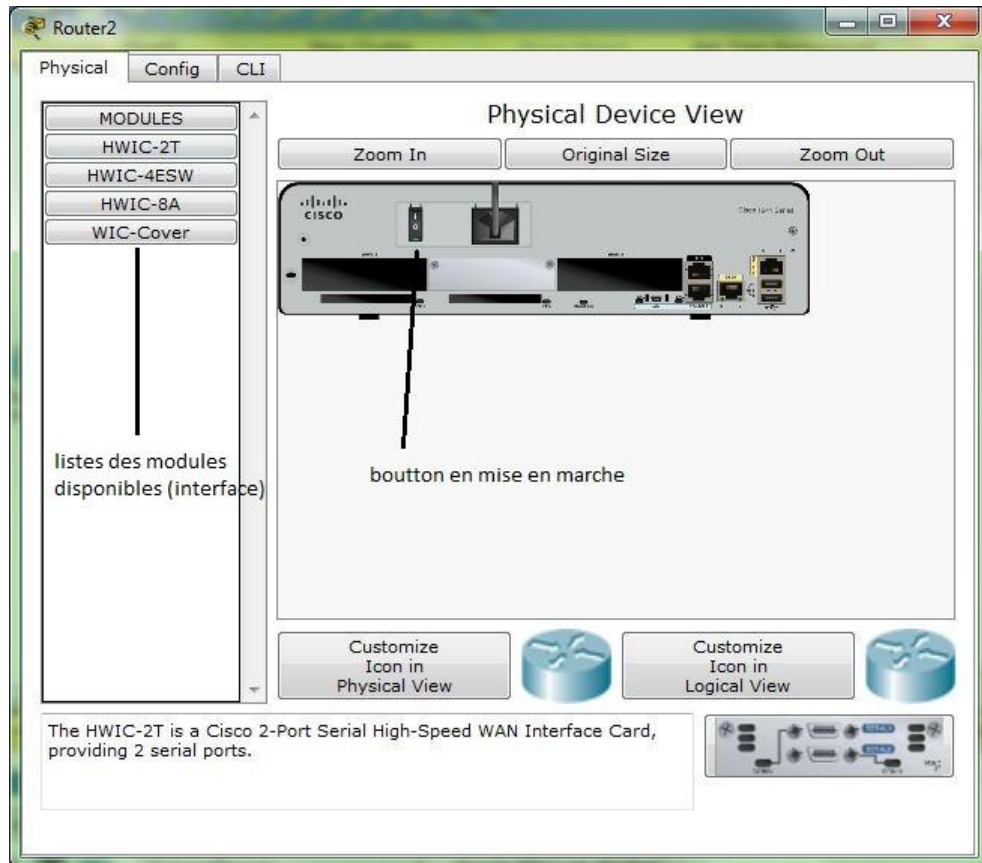


**Figure 4.2 :** Espace de travail logique

Dans un premier temps on doit choisir les dispositifs nécessaires dans le champ où se trouvent les icones des équipements, ensuite les placés dans l'espace de travail. Après le logiciel nous permet de faire les actions suivantes pour pouvoir manipuler les dispositifs.

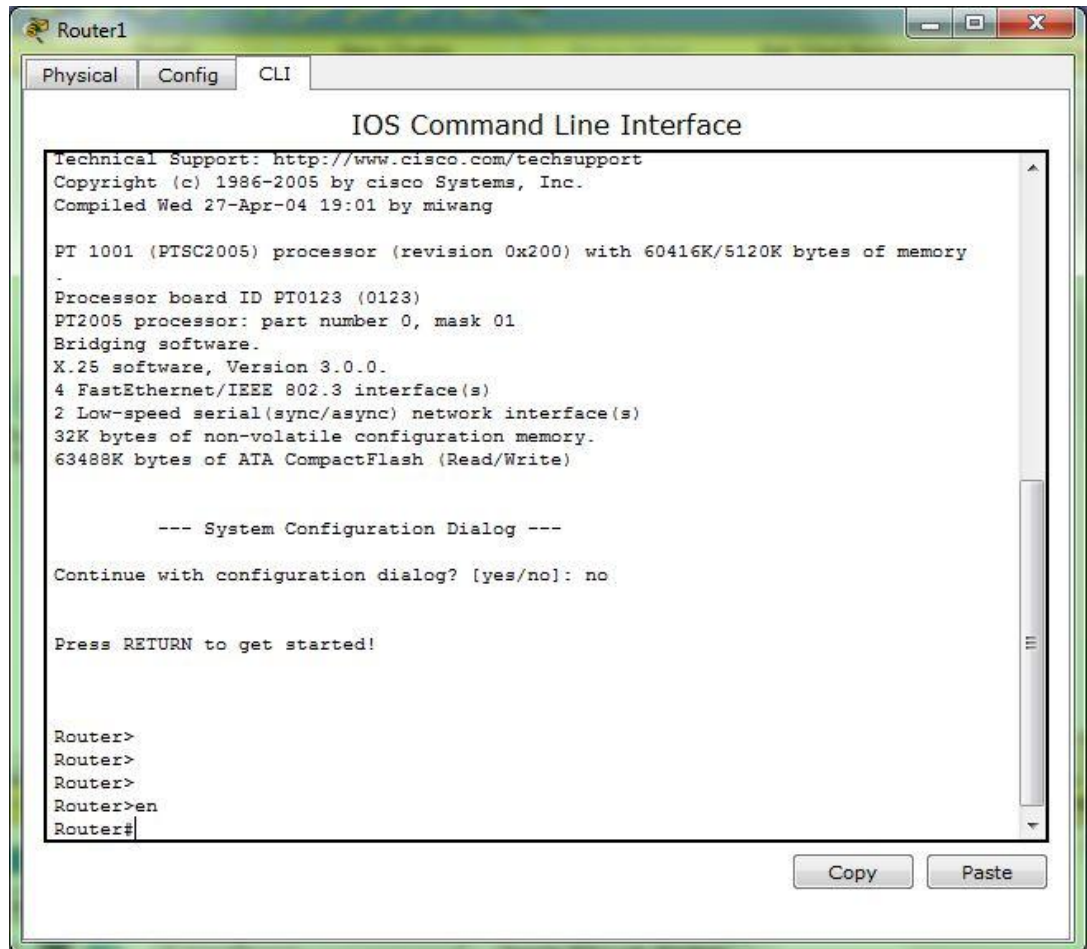
- ✓ Ajout des modules dans les dispositifs pour installer les interfaces nécessaire au fonctionnement du réseau (le dispositif concerné doit être mis hors tension). De même on peut aussi enlever un module.





**Figure 4.3 :** Ajout et suppression d'un module

- ✓ Connecter les dispositifs avec les câbles appropriés (dans la figure 5.01 les deux ordinateurs sont connectés avec le commutateur par un câble droit).
- ✓ Configurer les paramètres des dispositifs (comme les noms des dispositifs, les adresses IP...) dans des boîtes de dialogues suite à un clic sur un dispositif.
- ✓ Dans les cas d'un routeur ou un commutateur, le logiciel permet de faire une configuration avancée à partir d'une interface de commande ou CLI (IOS Command Line Interface).



**Figure 4.4 :** Interface de commande

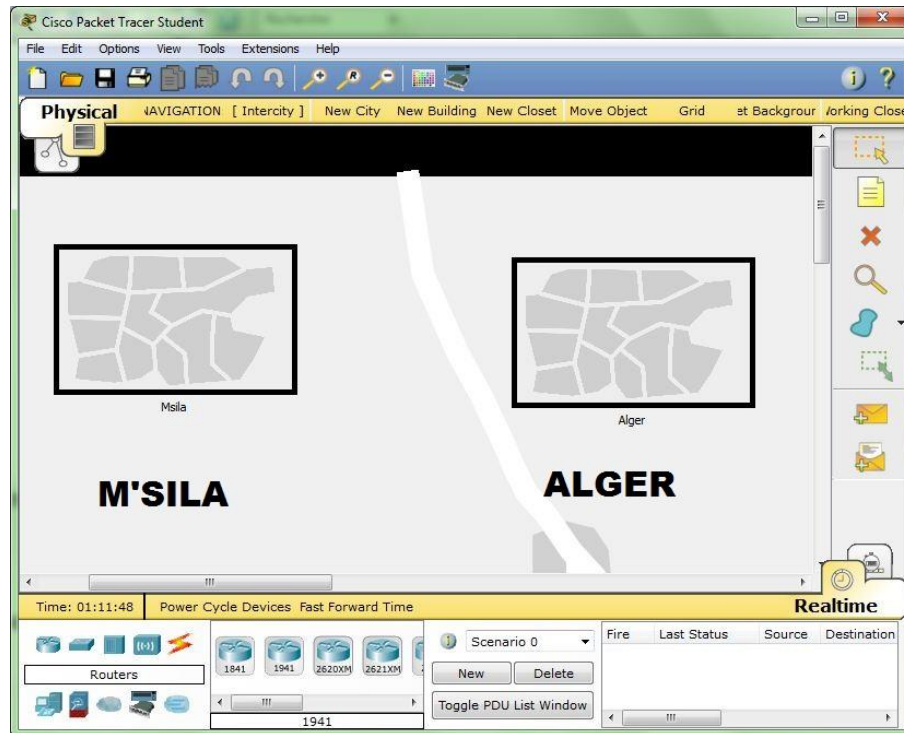
La boîte de dialogue de la figure 5.03 permet de configurer un équipement par l'interface de commande et de le visualiser dans son aspect physique.

### 2.1.2 L'espace de travail physique (Physical work space)

Le but de la zone de travail physique est de donner une dimension physique de la topologie logique du réseau. Cette espace de travail est divisée en 4 couches pour illustrer 4 environnements dans le cas réel.

#### ✓ L'Interurbain

L'espace interurbain permet de visualiser les connexions à longue distance, c'est-à-dire dans une superficie plus vaste.

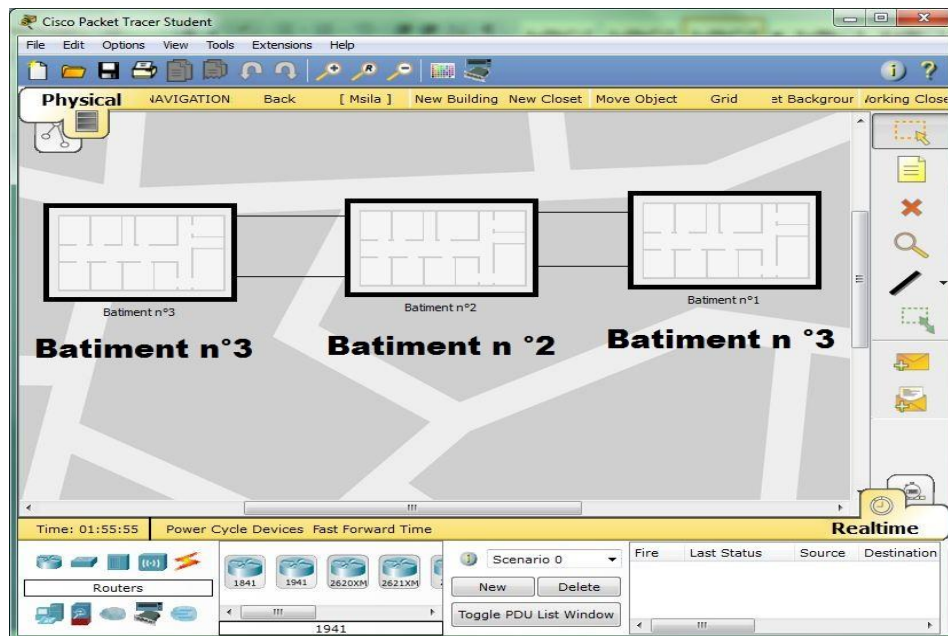


**Figure 4.5 :** Packet Tracer : zone Interurbain (M'sila - Alger)

Une zone Interurbain peut contenir plusieurs villes.

✓ Ville.

Chaque ville peut contenir plusieurs bâtiments.



**Figure 4.6 :** Plan d'une ville (M'sila) avec les bâtiments

Les bâtiments sont représentés par les icônes en rectangles.

✓ Bâtiment

Dans Chaque bâtiment on trouve les étages où sont rangés les différents compartiments pour placer les cabinets.

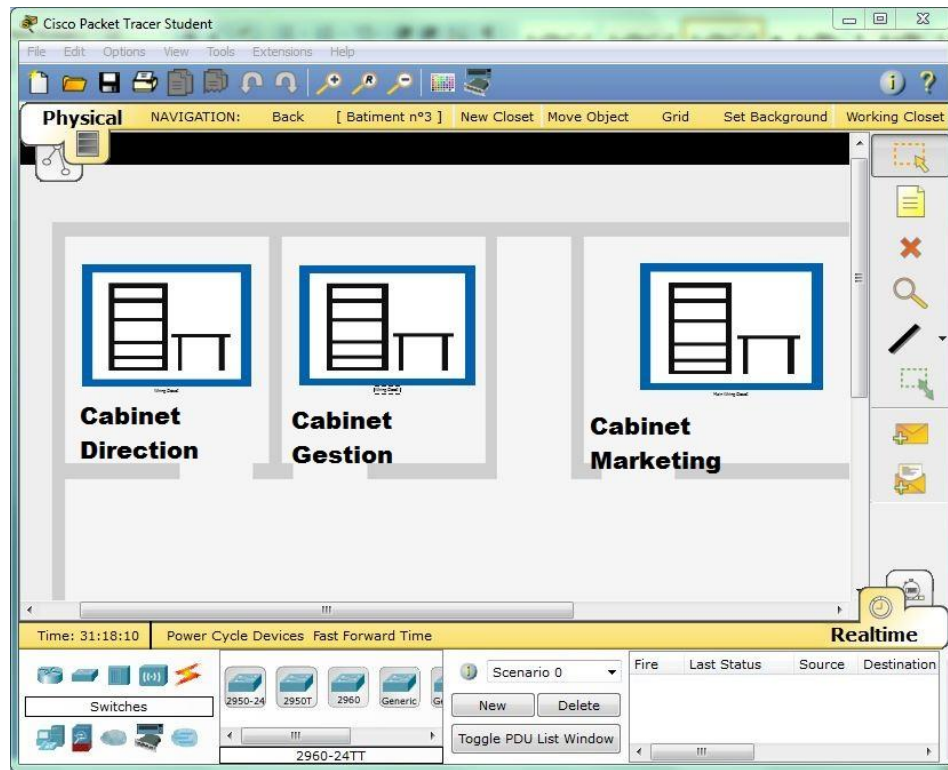


Figure 4.7 : Plan d'un Bâtiment avec les différents cabinets

Les cabinets sont représentés par l'existence d'une étagère pour le rangement des équipements.

✓ Cabinet de câblage

Le cabinet de câblage contient les dispositifs permettant de ranger les équipements et de les interconnectés.

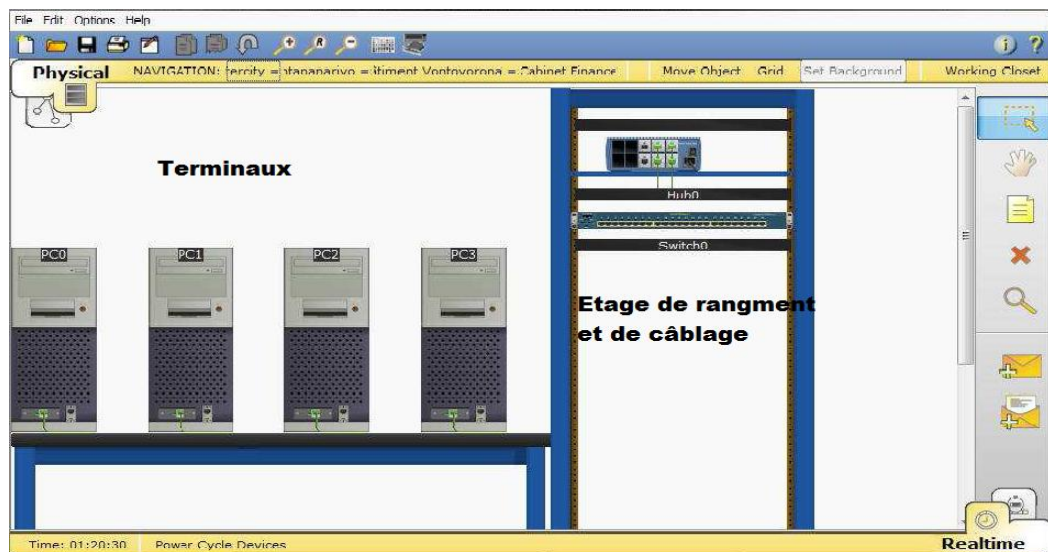


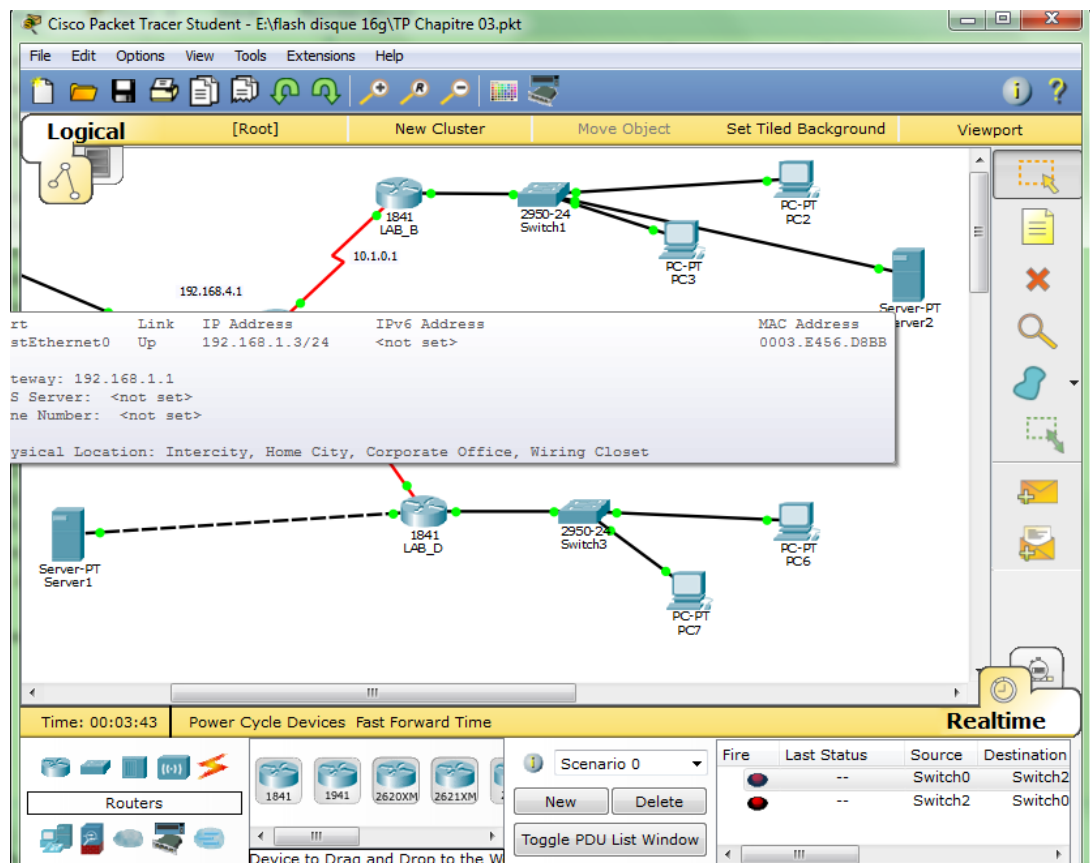
Figure 4.8 : les équipements dans les cabinets de câblage

Le logiciel propose aussi deux modes de fonctionnements, et qui reflètent l'arrangement en temps du réseau. On peut voir ainsi le fonctionnement direct d'une simulation et les étapes de transmission des informations dans le réseau.

### 2.1.3 Mode temps réel

Dans ce mode le réseau fonctionne dans un modèle à temps réel. Le réseau répond immédiatement aux actions qu'on lui exerce et fonctionne exactement comme dans un vrai réseau (en tenant compte les notions de temps).

Exemple :



**Figure 4.9 :** Présentation du réseau en mode temps réel

Dans ce mode de fonctionnement l'administrateur peut voir directement les différents paramétrages d'un composant en plaçant le pointeur de la souris au dessus. L'utilisateur peut envoyer ou créer graphiquement un PDU simple ou complexe sur les boutons en forme d'enveloppe.



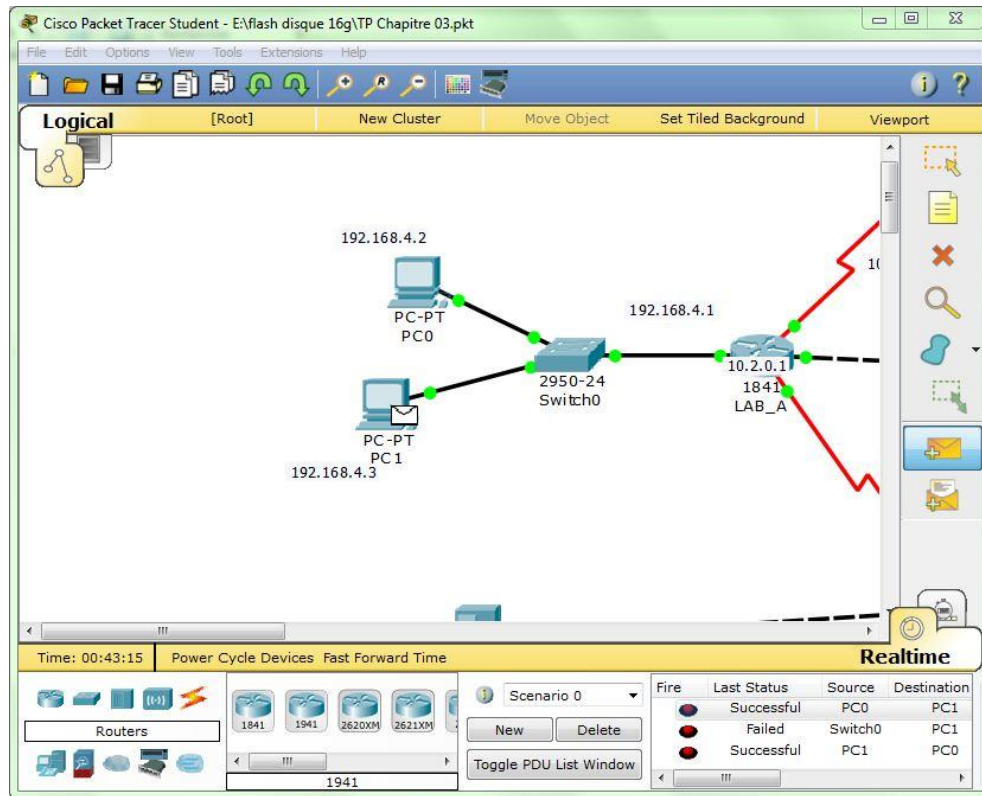


Figure 4.10 : Ping de PC1 vers PC0

## 2.1.4 Mode simulation

Dans ce mode on peut voir le réseau fonctionnant à un rythme lent, c'est-à-dire l'administrateur peut visualiser les chemins que les trames prennent et il peut les analysés en détail.

Exemple :

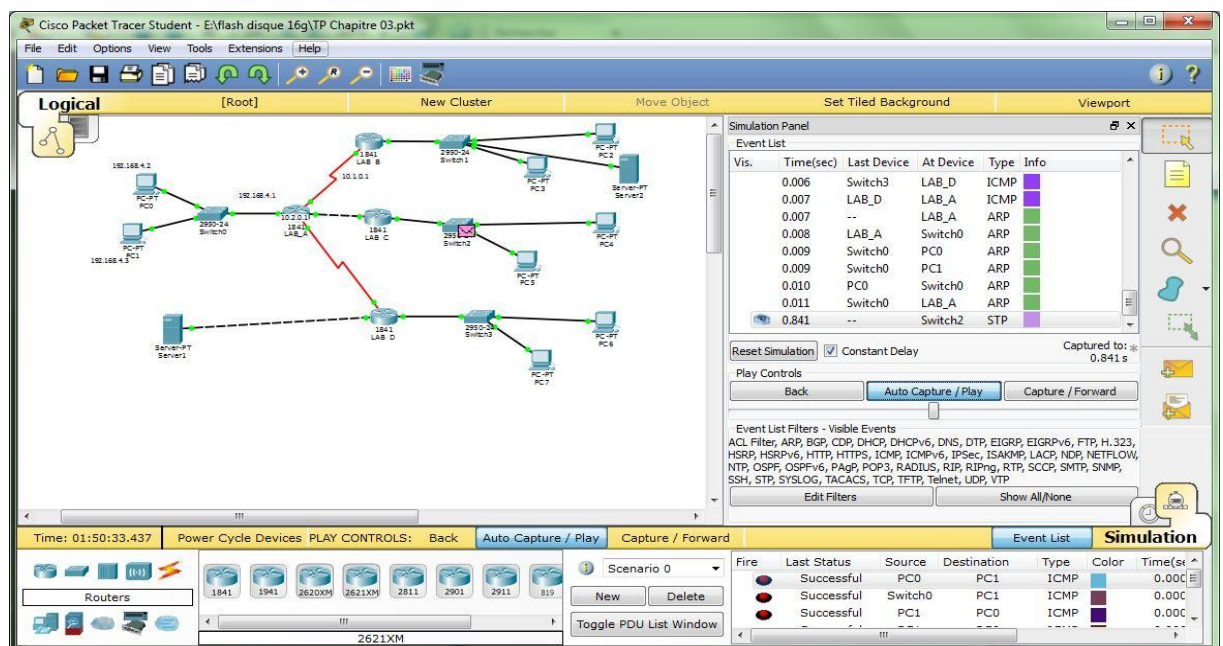
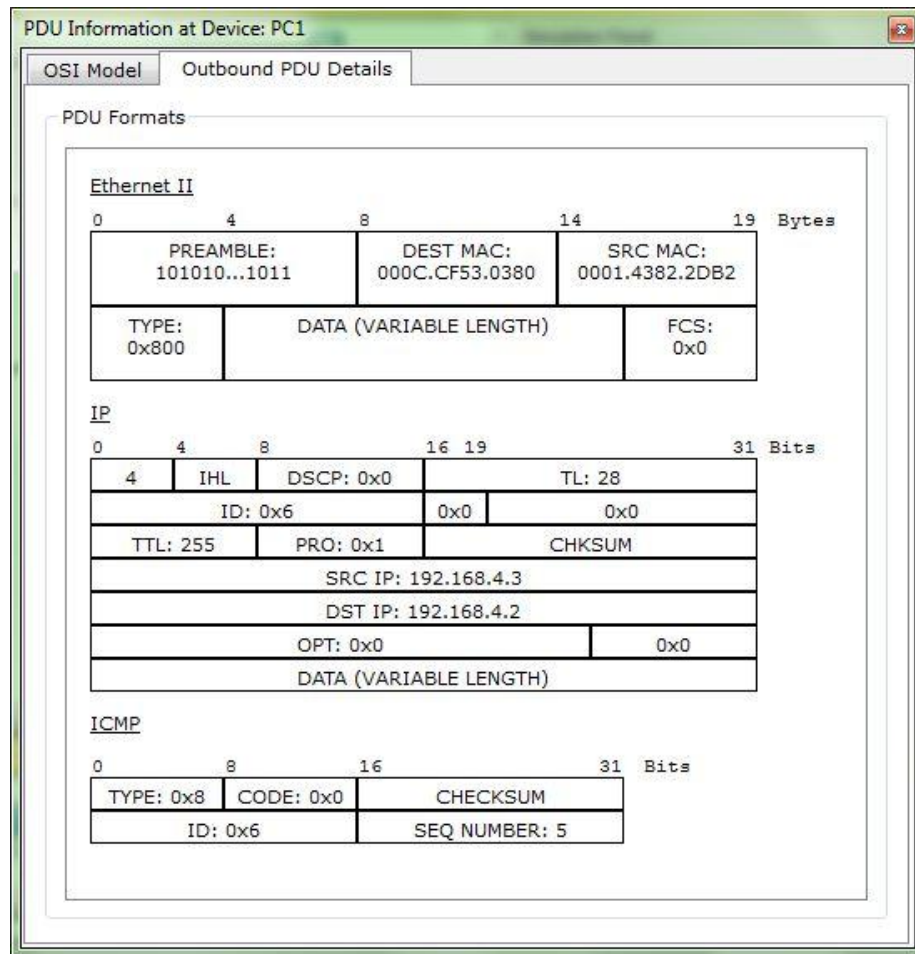


Figure 4.11 : Packet Tracer : mode simulation

En cliquant sur l'enveloppe, on peut voir les détails des trames c'est-à-dire les valeurs des champs d'une trame



**Figure 4.12 :** Détail d'une trame : Ethernet II, IP, ICMP pour un simple PDU (Ping)

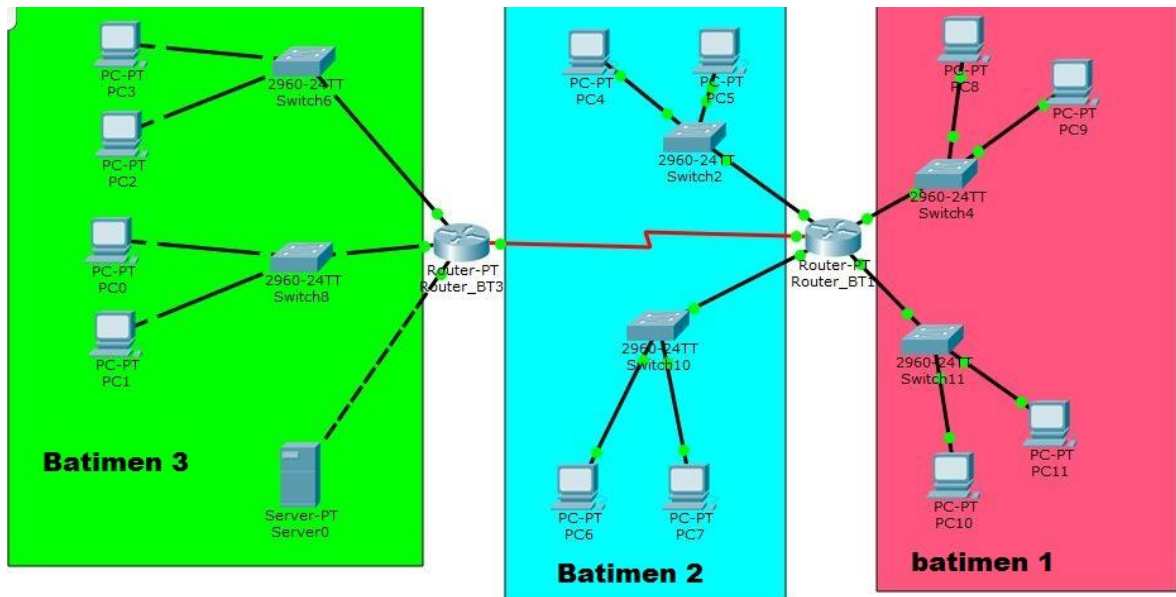
## 2.2 Simulation Routage inter-vlan

Nous allons voir maintenant une simulation d'un routage inter-vlan. Tout d'abord on va présenter un réseau avec une segmentation vlan sans utiliser le routage vlan, Le réseau proposé comprendra des VLANs qui représenteront les groupes de travaux. Le but est de faire une simulation d'un scénario avec segmentation LAN comparé avec la segmentation VLAN en utilisant le routage inter-vlan comparative.

D'abord on a proposé un scénario sans Vlan, quant nous allons prendre en conscience la méthodologie pour la segmentation d'un réseau LAN qui on a cité dans le 1<sup>er</sup> chapitre.

### 2.2.1 Architecture

La conception du 1<sup>er</sup> scénario fonctionne selon la hiérarchie suivante :



**Figure 4.13 : Scénario réseaux LAN**

On a proposé ce scénario d'une petite entreprise avec l'adressage dans la table suivante :

L'équipement	L'interface	Adresse de Réseau	Masque de réseau
Router_Bt3	Fa 0/0	192.168.1.0	255.255.255.0
	Fa 1/0	192.168.2.0	255.255.255.0
	Eth 6/0	172.128.16.0	255.255.255.252
	Se 2/0	10.10.0.0	255.255.255.252
Router_Bt1	Fa 0/0	192.168.3.0	255.255.255.0
	Fa 1/0	192.168.4.0	255.255.255.0
	Eth7/0	192.168.5.0	255.255.255.0
	Eth 8/0	192.168.6.0	255.255.255.0
	Se 2/0	10.10.0.0	255.255.255.252

**Table4.1** Tableau d'adressage de notre scénario

1.1 On a choisit le Protocole OSPF come Protocole de routage de réseau ; donc le routage il est dynamique.

1.2 Pour configurer le routage OSPF dans le routeur in faut d'abord configurer les interfaces et attribue chaque interface une adresse IP distincte comme suivant :

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.1.0 255.255.255.0
Router(config-if)#no shutdown
Router(config)#interface fastEthernet 1/0
Router(config-if)#ip address 172.128.16.1 255.255.255.252
Router(config-if)#no shutdown
```



Donc il faut taper la commande ***no shutdown*** pour activer l'interface

Avant d'avoir la configuration de la Protocole OSPF, d'abord on prend quelque notion.

### 2.2.2 OSPF

OSPF est un protocole de routage d'état de lien, il est développé par l'IETF à la fin des années 1980, pour les réseaux filaires.

Il utilise l'algorithme SPF pour *Shortest Path First*, plus connu sous le nom d'algorithme de Dijkstra, afin d'élire la meilleure route vers une destination donnée [16].

Le protocole OSPF utilise 5 types de paquets, ils se sont :

Paquet de Hello : permet de découvrir ses voisins et d'avertir son entourage de sa présence.

Paquet de Database Description: (DBD) – contient un résumé de la base de données de chaque routeur dont les noms des routeurs connus.

Link-state request packets (LSR) – pour faire une demande d'informations complémentaire par rapport à sa DBD.

Link-state updates packets (LSU) – décrivent les changements de topologie et contient 7 types différents de LSA.

Link-state avertissements (LSA) qui contient le sous-réseau, le masque, la métrique et d'autres informations sur les sous-réseaux.

Link-state Acknowledgement packets (LSAck) – pour accuser réception des paquets OSPF reçus.

Nous avons choisis deux types de paquet essentiels parmi les 5 paquets pour simuler le protocole OSPF sont :

1. Le paquet Hello.
2. Le paquet de description de base.

#### 2.2.2.1 Configuration

Maintenant on peut configurer le routage dynamique OSPF pour chaque routeur :

Il faut pour chaque routeur attribuer un ID de OSPF et le Route ID :

```
Router (config)#router ospf 1
Router (config-router)#router-id 1.1.1.1
Router (config-router) #network 10.10.2.0 0.0.0.3 area 0
Router (config-router) #network 10.10.0.0 0.0.0.3 area 0
Router (config-router) #network 192.168.5.0 0.0.0.255 area 0
Router (config-router) #network 192.168.6.0 0.0.0.255 area 0
Router (config-router) #network 192.168.7.0 0.0.0.255 area 0
Router (config-router) #network 192.168.8.0 0.0.0.255 area 0
```

Alors le protocole OSPF est le protocole de routage de notre réseau, pour vérifier l'état de protocole on utilise la commande **SHOW IP OSPF**, la figure suivant illustre les résultat de la commande

```

Router4
Physical Config CLI
IOS Command Line Interface

Router#show
Router#show i
Router#show ip
Router#show ip o
Router#show ip ospf
Routing Process "ospf 1" with ID 1.1.1.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 5
    Area has no authentication
    SPF algorithm executed 2 times
    Area ranges are
    Number of LSA 1. Checksum Sum 0x009a64
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
Router#
Copy Paste

```

**Figure 4.14** show ip ospf

Et pour avoir la table des voisins on va taper la commande **show ip ospf neighbor**

```

Router>en
Router#show ip o
Router#show ip ospf ne
Router#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address      Interface
1.1.1.1          0    FULL/ -         00:00:31   10.10.0.1    Serial2/0
3.3.3.3          0    FULL/ -         00:00:37   10.10.2.2    Serial3/0
Router#
Copy Paste

```

**Figure 4.15** show ip ospf neighbor

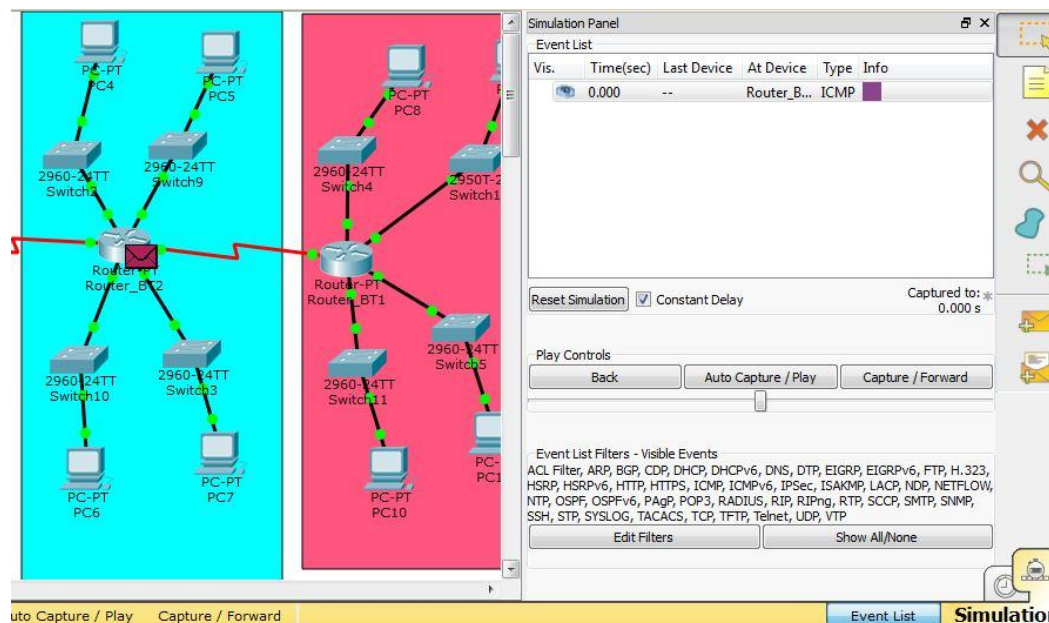
### 2.2.3 Déroutement de la simulation

Pour voir plus en détail nous allons passer en mode simulation dans le logiciel, et en activant le bouton capture on peut visualiser les différents paquets échanger dans le réseau.

Le réseau est maintenant configure avec le routage dynamique et nous allons segmenter de façon classique LAN

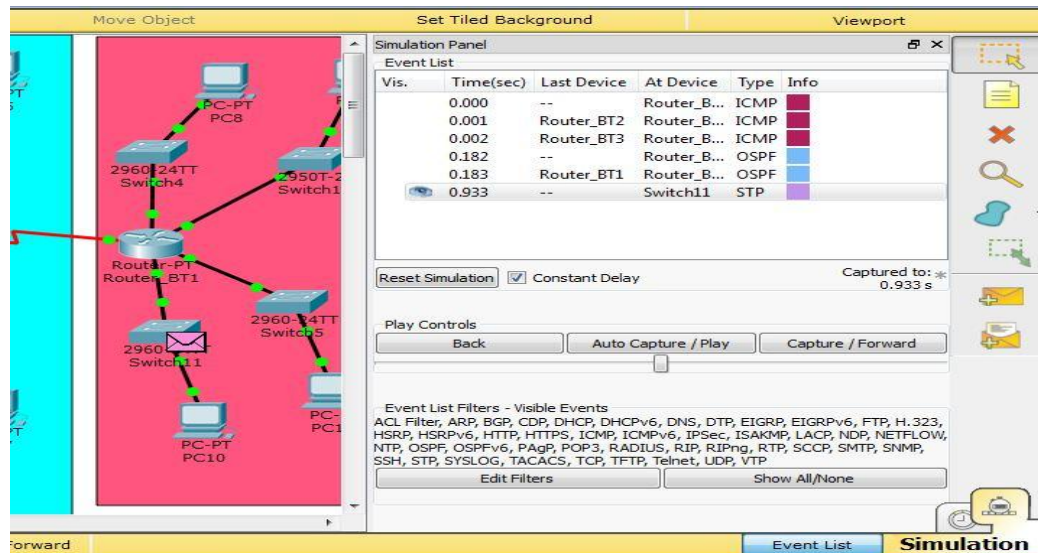
Après lancement de l'application et en chargeant le fichier (.pkt) qui contient les configurations et l'architecture du réseau à simuler, les dispositifs sont à l'état d'initialisation. Les commutateurs charge leurs base de données. Cet état est marqué par les points orange sur les liens.

Initialement chaque Routeur envoie un PDU (enveloppe rouge dans la figure 5.14) de configuration au routeur qui lui est proche.



**Figure 4.16 : Envoie de PDU de configuration**

Les routeurs échangent le PDU entre eux pour vérifier l'état et la connectivité entre les routeurs, puis le protocole OSPF inclus dans le format PDU pour faire le routage. Comme la figure suivante montre l'enveloppe bleue pour le protocole OSPF



**Figure 4.17 :** Envoie l'enveloppe de l'ospf

Lorsque que le routeur sont bien connecté entre eux le protocole OSPF envoi le message HELLO après chaque 10 s .et la figure suivante présent le paquet OSPF

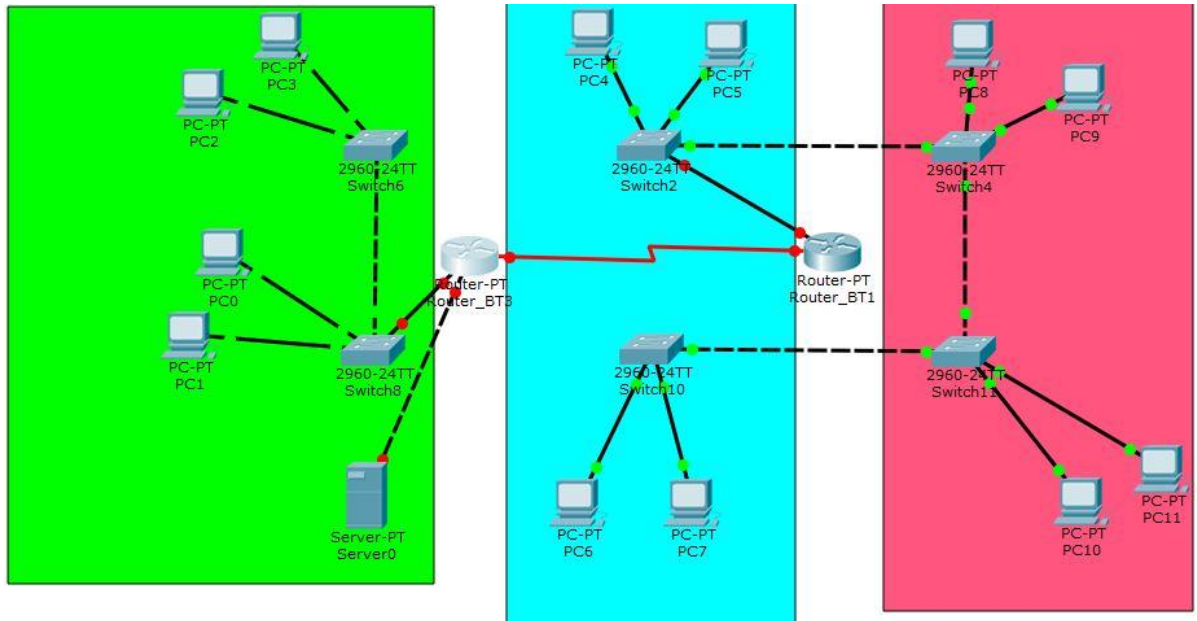
OSPF Hello		
0	2	Bytes
VERSION NUM: 2	TYPE: 1	PACKET LEN: 48
ROUTER ID: 3.3.3.3		
AREA ID: 0.0.0.0		
CHECK SUM: 0	AUTH TYPE: 0	
AUTHENTICATION:		
NETWORK MASK: 255.255.255.252		
HELLO INTERVAL: 10	OPTIONS: 0	RP: 0
ROUTER DEAD INTERVAL: 40		
DESIGNATED ROUTER: 0.0.0.0		
BACKUP DESIGNATED ROUTER: 0.0.0.0		
NEIGHBOR COUNT: 1		

**Figure 4.18** paquet ospf inclut dans le format PDU

## 2.2.4 Mise en place d'un routage inter-VLAN

Dans une entreprise, on veut séparer logiquement les différents services dans un souci de confidentialité des services et pour améliorer la gestion du réseau.

Alors, on va utiliser les VLANs et le routage inter-vlan, pour ce la l'architecture de réseaux va être modifié, la figure suivant présente la nouvelle architecture



**Figure 4.19 :** scénario avec VLAN et routage inter VLAN

Nous allons prendre les départements situant dans une entreprise pour illustrer les groupes de travaux. On va donc classifier ces groupes de travaux par des réseaux virtuels donnés par le tableau 5.01.

Département	Nom Vlan	Numéro Vlan	Adresse IP (réseau)
Marketing	VLAN_MRKT	10	192.168.10.0
Ventes	VLAN_VNT	20	192.168.20.0
Finance	VLAN_FNC	30	192.168.30.0
Comptable	VLAN_COMT	40	192.168.40.0
Engineering	VLAN_ENG	50	192.168.50.0
Production	VLAN_PRDCT	60	192.168.60.0
Trunks	VLAN_NATIVE	99	N/A

**Table 4.2:** VLAN : regroupement fonctionnel

Chaque commutateur dans le réseau doit avoir les mêmes bases données. Les informations concernant les VLANs doivent être inclus dans la mémoire de chaque commutateur.

Nous avons besoins aussi d'un routeur qui sert à router les paquets venant d'un autre segment ou domaine de broadcast.

Après avoir mis en place les différents équipements, d'abord on configure tout les commutateurs et les routeurs et attribuer des adresse IP pour chaque sous\_interface dans le réseau,

- **Configuration**

Nous configurerons des VLANs de niveau 1, en attribuant les VLANs aux ports du Switch.  
Pour configurer le Switch,

Nous commencerons par déclarer les VLANs sur les commutateurs :

```
Switch(config)#Vlan 10
Switch(config-vlan)#name VLAN_MRKT
Switch(config)#Vlan 20
Switch(config-vlan)#name VLAN_VNT
Switch(config)#Vlan 30
Switch(config-vlan)#name VLAN _FNC
Switch(config)#Vlan 40
Switch(config-vlan)#name VLAN_COMT
Switch(config)#Vlan 50
Switch(config-vlan)#name VLAN_ENG
Switch(config)#Vlan 60
Switch(config-vlan)#name VLAN _PRDCT
Switch(config)#Vlan 99
Switch(config-vlan)#name VLAN _NATIVE
```

En suite on va crée les sous interface dans les deux routeur

Router 1 :

```
Router1(config)#interface fastEthernet 0/0.10
Router1(config-subif)#encapsulation dot1Q 10
Router1(config-subif)#ip address 192.168.10.1 255.255.255.0
Router1(config)#interface fastEthernet 0/0.20
Router1(config-subif)#encapsulation dot1Q 20
Router1(config-subif)#ip address 192.168.20.1 255.255.255.0
```

Routeur 2 :

```
Router2(config)#interface fastEthernet 0/0.30
Router2(config-subif)#encapsulation dot1Q 40
Router2(config-subif)#ip address 192.168.40.1 255.255.255.0
Router2(config)#interface fastEthernet 0/0.50
Router2(config-subif)#encapsulation dot1Q 50
Router2(config-subif)#ip address 192.168.50.1 255.255.255.0
Router2(config)#interface fastEthernet 0/0.60
Router2(config-subif)#encapsulation dot1Q 60
Router2(config-subif)#ip address 192.168.60.1 255.255.255.0
```

Maintenant on va créer les liens Trunk entre les Switch et les Switch et routeur, et les interfaces qui ont un lien entre les Switch et les Hôte sont en mode Access

```
Switch(config)#interface range fastEthernet 0/2-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
```

Les trunk maintenant

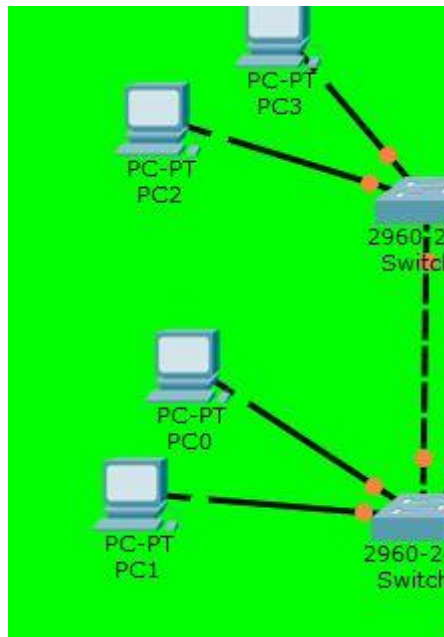
```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10
```

Et on va continuer la configuration avec tous les équipements.

#### 2.2.4.1 Déroulement de la simulation

Pour voir plus en détail nous allons passer en mode simulation dans le logiciel, et en activant le bouton capture on peut visualiser les différents paquets échangés dans le réseau.

Après lancement de l'application et en chargeant le fichier (.pkt) qui contient les configurations et l'architecture du réseau à simuler, les dispositifs sont à l'état d'initialisation. Les commutateurs chargent leur base de données. Cet état est marqué par les points orange sur les liens.



**Figure 4.20 :** Initialisation de la configuration

Alors le lien étiqueté c'est le plus important dans le routage inter-vlan qui joue le rôle d'une passerelle de couche 2 à couche 3.



### 3 Résultat de la simulation et discussion PACKET TRACER

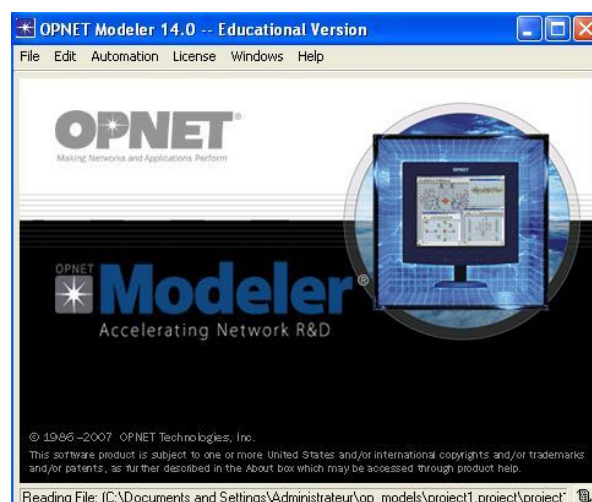
On a choisit Packet tracer pour la mise en place du routage inter-vlan pour présenter le changement topologique avec les vlan et le routage inter vlan et pour mieux éclaircir la configuration de routage inter-vlan dans le réel. On conclure des point d'après cette simulation

- ✓ Après qu'on a changé la segmentation avec des VLANs on constate que le domaine de diffusion a diminué et a amélioré la gestion du réseau.
- ✓ Les VLAN sont très utiles dans un réseau car ils permettent de séparer en plusieurs segments logique un réseau.
- ✓ Le routage inter-vlan a permet d'optimiser la bande passante, et de segmenter un domaine de broadcast.
- ✓ Donc le seul inconvénient est la configuration des vlans qui prend beaucoup de temps pour les administrateurs.

Et pour analyser les performances des vlan on va utiliser le simulateur OPNET qui présenter dans la section suivante.

### 4 Simulation avec l'OPNET Modeler

Les aspects de performance comme l'envoi de trafic, reçus de trafic, le retard et le nombre de collision sont mesurés et analysés. La simulation a été réalisée en utilisant des OPNET Modeler Edition 14.5. OPNET Fournit un environnement de développement complet pour la spécification, la simulation et l'analyse de la performance des réseaux de communication. La méthode de simulation est choisie parce qu'elle peut nous aider à concevoir la structure du réseau, fournir des renseignements sur la structure de la circulation et nous sauver du coût d'achat des équipements et la construction de l'ensemble de la structure de réseau physique.



**Figure 4.21** Démarrage OPNET



## 4.1 Présenter L'OPNET

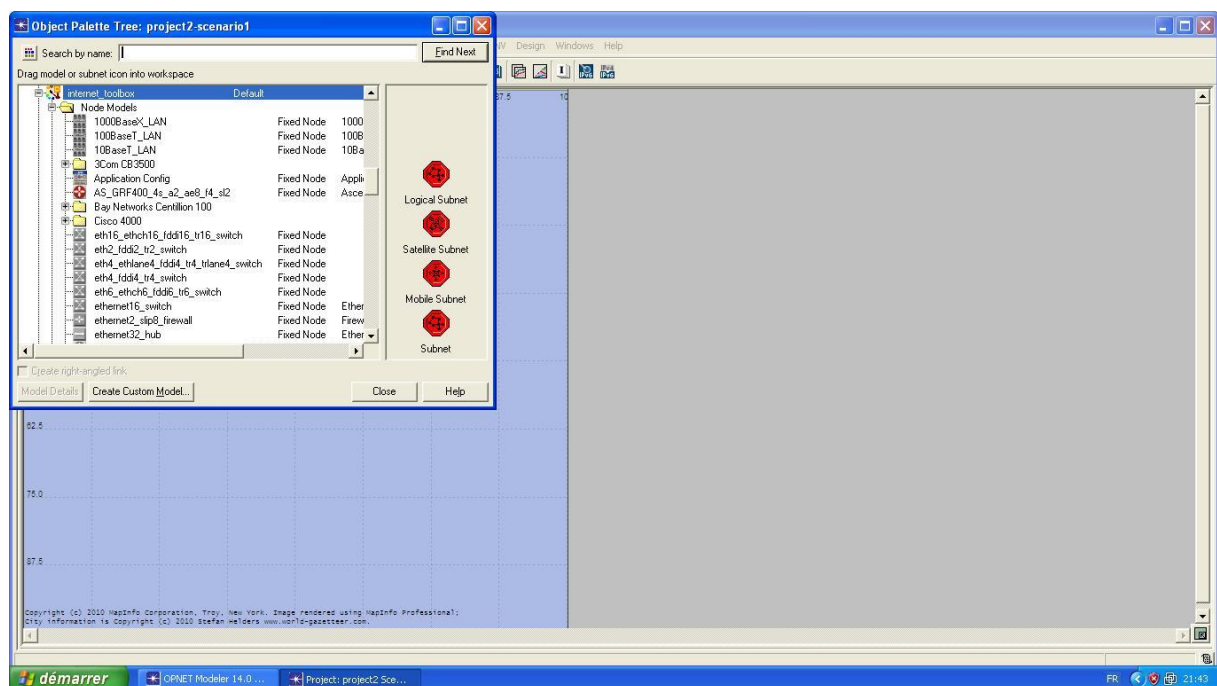
### 4.1.1 L'éditeur de projets

L'éditeur de projets représente un graphique de la topologie des communications du réseau. Ce dernier est constitué d'objets équipements et liens configurables via des boîtes de dialogues.

Les méthodes de copier collé des équipements et des liens à partir des palettes d'objets de l'éditeur permettent de réaliser le réseau. Il est également possible d'utiliser la fonction d'importation rapide de l'ensemble de la configuration. Il est possible d'utiliser la librairie OPNET ou de réaliser votre propre palette intégrant vos propres équipements et liens.

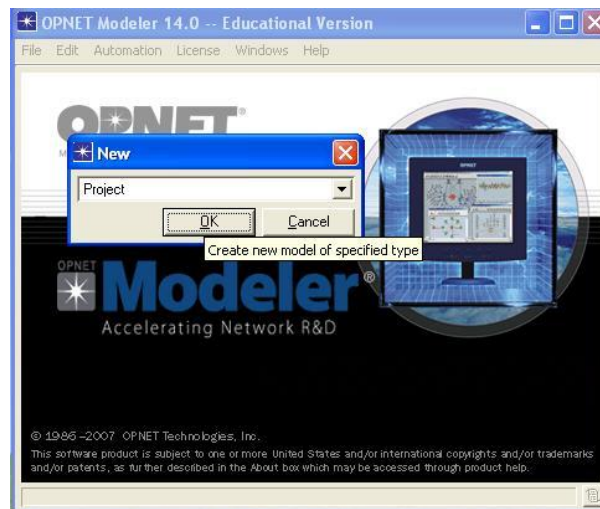
L'éditeur de projets intègre également un environnement géographique avec des caractéristiques dimensionnelles reprenant les composants utiles pour la modélisation de réseaux câblés ou sans fils.

L'utilisation du menu Protocoles permet de configurer rapidement les protocoles et d'activer des paramètres particuliers.[17]



**Figure 4.22** Espace de simulation OPNET

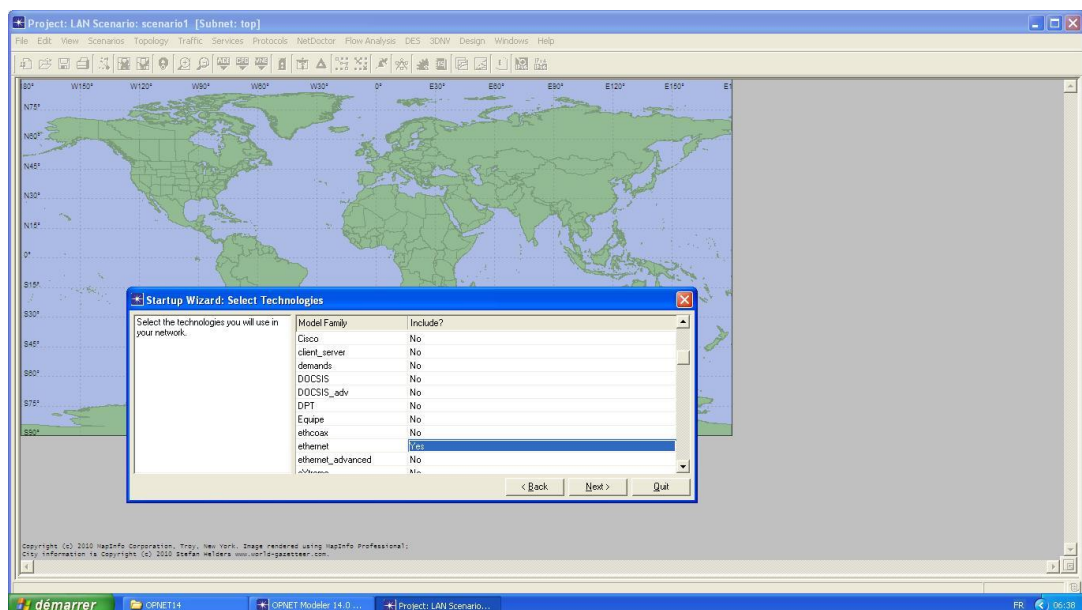
### 4.1.2 Crée un projet dans L'OPNET



**Figure 2.23** Crée un nouveau projet

On suivre les étapes suivante :

1. Démarrez OPNET MODLER · Choisissez Nouveau dans le menu Fichier.
2. Sélectionnez Projet et cliquez sur OK · Nommez le projet <votre initiales> \_VLAN, et Cliquez sur OK.
3. Dans l'assistant de démarrage: boîte de dialogue de la topologie initiale, assurez-vous que l'option Créer Scénario vide est sélectionné · Cliquez sur Suivant · Choisir Campus de la liste à l'échelle du réseau · Dans l'assistant de démarrage: boîte de dialogue Taille Spécifiez, affectez les suivantes: Taille? Kilomètres, X Span? 1, et Y Span? 1 puis Cliquez sur Suivant deux fois puis Cliquez sur OK.



**Figure 4.24** Au court de crée un projet

## 4.2 Simulation

### 4.2.1 Simulation de Réseau local virtuel

Dans cette section, le scénario LAN virtuel est expliqué et détaillé. Deux scénarios ont été construits pour comparer le comportement d'un réseau avec des VLAN et un autre sans VLAN comme indiqué dans la figure 25 et 24. Ce scénario est considéré être mis en place dans un environnement de bureau avec trois groupes logiques d'utilisateurs qui sont répartis autour de deux bâtiments, l'administration, les professeurs et étudiants départements. Ces services sont logiquement séparés en utilisant un réseau local virtuel différent pour chacun d'entre eux pour des raisons de sécurité, et de réduire la demande de trafic vers les serveurs.

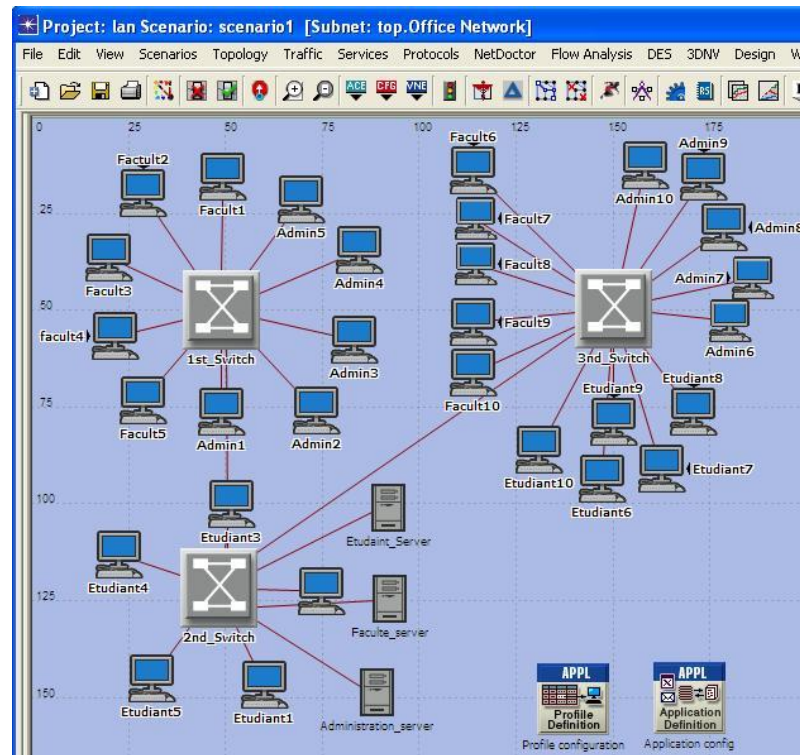
Le tableau 4.2 montre comment les nœuds et les serveurs sont répartis et regroupés en trois ministères différents.

Département	Serveur	Station	Nom de VLAN	ID de VLAN
Administration Département	Admin Serveur	Admin1 Admin10	VLAN10	10
Faculté Département	Faculté Serveur	faculté1 faculté10	VLAN20	20
Département des étudiants	Étudiant serveur	étudaint10 étudiant 10	VLAN30	30

**Table4.3** distribution des stations dans département

### 4.3 Réseau sans VLAN

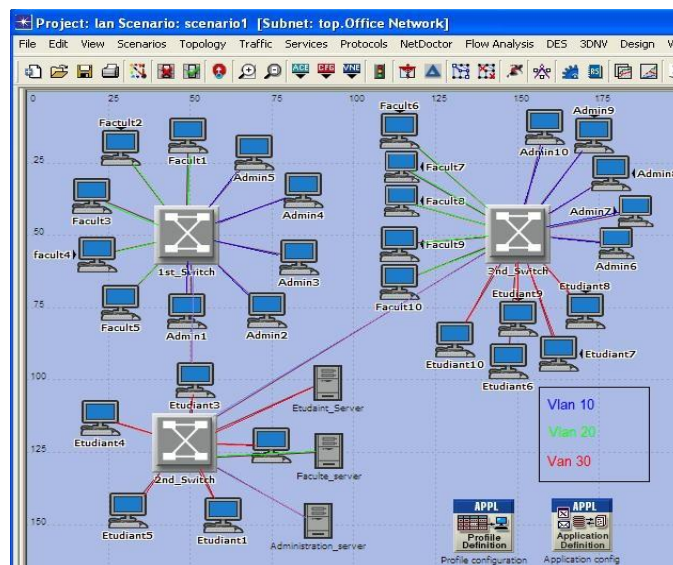
Figure4.25 représente réseau commuté Office sans VLAN. Dans ce scénario, il n'y a pas de séparation entre les utilisateurs, par conséquent, chaque connexion est autorisée et il est possible pour tout utilisateur d'avoir accès à des serveurs de gestion confidentiels, tous les nœuds sont dans un seul et même réseau, et ils peuvent communiquer et partager ressources sans restrictions, les étudiants peuvent d'administration d'Access Server, de sorte que le serveur d'administration devenir chargé, et enfin se congestionné en raison des demandes de trafic élève.



**Figure 4.25** Réseau sans VLAN OPNET

#### 4.4 Réseau avec des VLAN

Figure 4.26 représente un réseau à commutation de bureau avec des VLAN. Il est un réseau composé de trois départements. Ces services sont logiquement séparés en utilisant un réseau local virtuel différent pour chacun d'eux. Les flèches bleues indiquent les postes de travail du réseau d'administration et le serveur, les flèches vertes représentent les postes de travail du réseau de la faculté et le serveur, et les flèches rouges sont les postes de travail du réseau des étudiants et des serveurs.



**Figure 4.26** Réseau avec VLAN

On va attribuer les vlan de façon qui montre dans la Figure 4.23 suivante

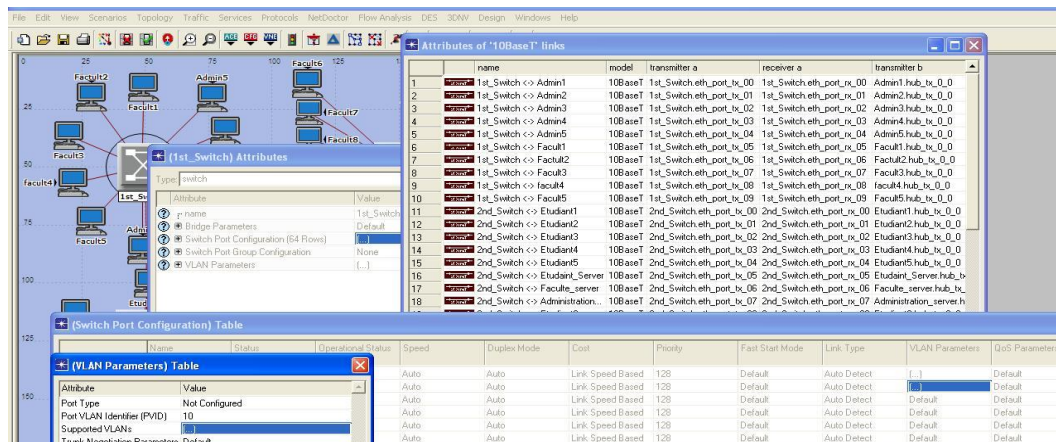


Figure 4.27 Attribue les VLANs

## 4.5 Résultats des Analyses

Différentes simulations ont été exécutées en utilisant un logiciel OPNET pour tous les dispositifs de réseau à l'aide différents scénarios.

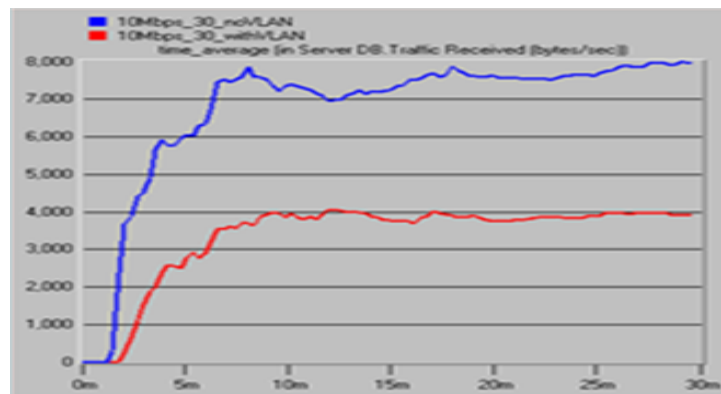
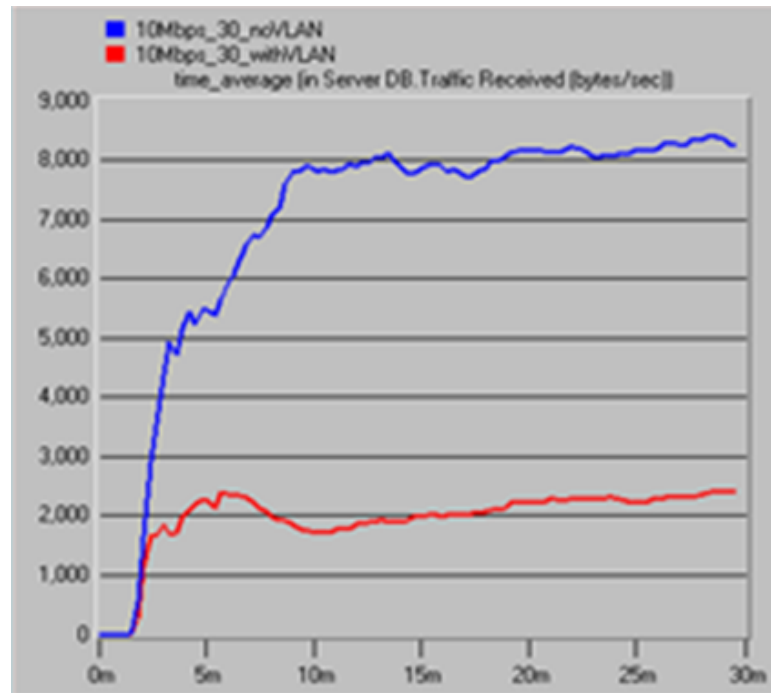
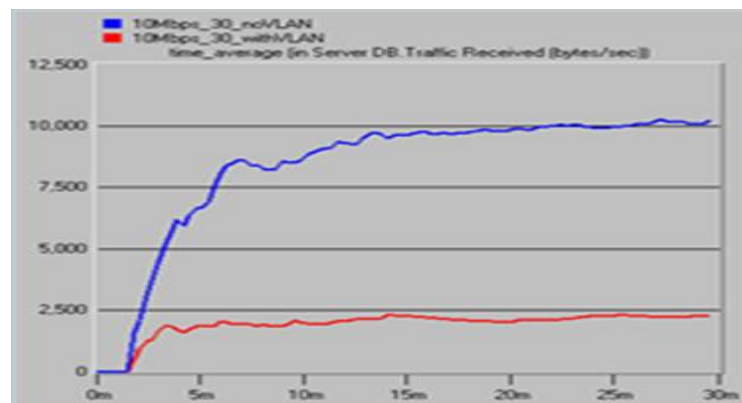


Figure 4.28 Trafic reçue de demande par le serveur d'administration (octets / sec)



**Figure 4.29** Trafic reçue demande par le Serveur de faculté (Packet / sec)



**Figure 4.30** Trafic demande reçue par le Serveur d'étudiants (Packet / sec)

Comme le montre la figure 4. 10 et 11, le graphique bleu est le scénario Aucun VLAN, et le graphe rouge est le réseau avec le scénario de VLAN, le trafic reçu dans le scénario sans VLAN est plus élevé avec VLAN

Le premier scénario est un seul domaine de diffusion. Si l'on considère la figure 4.9, dans le pas de VLAN Scénario un total de vingt postes de travail transmettent accès à la base de la demande du trafic lourd pour le serveur d'administration de administration et étudiants postes de travail. Alors que le réseau avec VLAN seul scénario d'administration 10 postes de travail envoient accès à la base de la demande du trafic lourd pour le serveur d'administration, en vertu de ce réseau les étudiants en design sont empêchés d'accéder au serveur d'administration, et l'ensemble du réseau est séparé en trois réseaux logiques, et ceci est l'un des avantages de l'utilisation de VLAN.



## 5 Conclusion

Le logiciel PACKET TRACER présente une très grande souplesse pour un avant goût d'un réseau à déployer. Ce que nous avons dans ce chapitre est une simulation du routage inter-vlan, l'utilisation des VLANs et la mise en place du routage inter vlan. On a vu qu'avec la simulation on peut prévoir tout le changement susceptible de se présenter dans la réalité.

Dans cette étude, différents déploiements de réseaux ont été envisagés d'utiliser OPNET. Dans les deux premiers LAN réseau déploiements des paquets reçus, les paquets envoyés, les retards et les collisions ont été inspectés. Nous avons comparé la performance et de l'effet des deux réseaux dans le cas de l'envoi et la réception de trames. Delay, trafic Évier, sources de trafic, Collision et Taille de l'image sont les paramètres de performance. Les résultats de la simulation par rapport montrer une bonne approximation du trafic de données analysées dans l'environnement Ethernet et les recherches démontré que plus la taille de paquet Ethernet mieux certains de métrique de performance de réseau comme l'utilisation moyenne, nombre de collisions et de retard, mais dans certains cas, la taille de paquet n'a pas d'impact significatif sur la performance du réseau. Les résultats de la simulation montre que la performance du réseau améliore dans les réseaux locaux, dans lequel les commutateurs, sont installés, parce que le commutateur LAN crée isolées domaines de collision. En distribuant des utilisateurs sur plusieurs domaines de collision, collisions sont évitées et la performance améliore Plus de trafic existe dans le réseau sans VLAN, puisque toute communication entre les départements est permis, lors de l'utilisation de VLAN; il n'est pas plus possible d'envoyer du trafic ou accéder à certaines ressources sans authentification, il améliore l'utilisation de la bande passante, la sécurité et l'administration en soutenant une virtuelle organisation.

## CONCLUSION & PERSPECTIVES

Pour satisfaire notre besoins dans un réseau il faut tout d'abord bien choisir : une topologie adéquat, un bon système de câblage, les meilleur techniques de transmission et son oublier choisir une architecture conforme aux organismes de normalisation pour les réseaux.

Les VLANs, Virtual Local Area Networks, introduisent donc un nouveau concept à l'intérieur des entreprises. En effet, cette technologie a le potentiel pour répondre au besoin de mouvement en interne des entreprises. Ainsi, une entreprise peut réorganiser l'ensemble de ces services ou de ces groupes de travail sans que le responsable Télécom ne soit à passer de longues heures à reconfigurer l'ensemble des machines du parc. Les VLANs apportent donc une très grande flexibilité dans la gestion du réseau. Les VLANs vont ainsi permettre à l'entreprise de songer à des réorganisations futures sans se soucier de la situation physique de l'existant informatique. Ainsi, le déploiement de réseaux virtuels est un choix stratégique pour l'entreprise pour ainsi diminuer les coûts de déplacement des utilisateurs entre les services.

La limite que présente LAN standard nous permet de parler dans le troisième chapitre les LAN virtuels qui offrent beaucoup plus d'avantages dans la mise en place d'un réseau au sein d'une entreprise. Avec le VLAN les utilisateurs peuvent être classés selon leur domaine de travail, selon le protocole qu'ils utilisent. L'interconnexion des dispositifs ne dépend plus des emplacements physiques. Le VLAN permet donc de segmenter le réseau en des domaines de collision plus petite.

Dans ce travail, nous avons simulé le Routage inter vlan (VLANs), et dans la raison de mesurer les performances de VLAN et routage inter vlan, pour faire la comparaison entre la segmentation LAN et VLAN et montré que VLAN et routage inter vlan est optimal que LAN en terme de nombre d'envoi et le reçoit de packets.

Nous avons proposés un scénario pour faire une étude comparative entre LAN et VLAN, nous suggérons l'utilisation la segmentation VLAN et routage inter vlan mieux que LAN pour la conception d'un réseau plus performant, sécurisé et faible.

Ce travail nous a permis d'apprendre comment utilisé la segmentation des VLAN et routage inter VLAN dans les réseaux d'entreprise grâce aux simulateurs PACKET TRACER et OPNET MODLER.

Nous envisageons, dans un futur travail, d'implémenter notre travail dans un autre environnement comme le NS2, nous allons aussi étendre notre travaille pour améliorer les segmentations des réseaux en utilisant les VLANs avec la redondance des liens pour éviter la panne de réseaux.



# BIBLIOGRAPHIE

- [1] J. P. Arnaud, RÉSEAUX ET TÉLÉCOMS, Dunod, Paris, 2003.
- [2] ABED Amine et GUENOUNA Abdelwahab, (2005). La voix sur IP. Mémoire de fin d'étude pour l'optimisation de diplôme d'ingénieur d'état spécialité télécommunication, institut de la télécommunication Abdelhafid boussouf –ORAN.
- [3] Andrew .G. (2002).TCP/IP JumpStart-Internet Protocol Basics. Edition
- [4] Dean .T .Réseaux Informatique. Edition RYNALD GOULET. 2001.
- [5] inetdoc.net. <http://www.inetdoc.net/articles/inter-vlan-routing/> consulté le 15/04/2015.
- [6] Philippe A., José D., « Réseaux informatiques », Notions fondamentales, Architecture, Modélisation OSI, TCP/IP, Wi-Fi, 2009.
- [7] Blanc J., « les réseaux locaux virtuels », T MRIM-MOTAUBAN, Technologie, Décembre 2007.
- [8] Sanchez R., « les réseaux locaux virtuels », CERTA, [www.reseaucerta.org](http://www.reseaucerta.org), v1.0 janvier 2006.
- [9] Todd L., « CCNA Cisco Certified Network Associate », Study Guide, 4e édition , 2009.
- [10] D. McPherson. B. Dykes, “VLAN Aggregation for Efficient IP Address Allocation” Request for Comments RFC 3069, Onesecure, Inc. February 2001.
- [11] Gyan Prakash Pal, Sadhana Pal “Virtual Local Area Network” International Journal of Scientific Research Engineering & Technology (IJSRET), Volume 1, Issue 10 pp 006-010 January 2013.
- [12] Lammle T., Barkl A., « CCDA Cisco Certified Design Associate », Study Guide, 2e edition 2003.

- [13] Velaga Pavani, Immadisetty L V Chandrika, A.Rama Krishna “Local Area Network (LAN) Technologies” International Journal of Innovative Technology and Exploring Engineering (IJITEE) Volume 1, Issue 6, November 2012.
- [14] Learn Network Academy [www.netacad.com](http://www.netacad.com) consulté le 12/02/2015 (Student Cisco)
- [15] cisco [www.cisco.com](http://www.cisco.com) consulter le 24/05/2015
- [16] J. Moy, “Open Shortes path first” (OSPF version 2) Request for Comments RFC 2328, April 1998
- [17] OPET [www.opnet.com](http://www.opnet.com) consulté les 31/05/2015

## ملخص

أصبح استخدام الشبكات المحلية الظاهرية (شبكة محلية ظاهرية)، والتوجيه بين تلك الشبكات المحلية نفسها منهجي في البنية التحتية الربط المعاصرة. هذا التوجيه بين VLAN لديها مصالح كثيرة من كلا جهة نظر تصميم من الناحية التشغيلية جوانب الأداء مثل إرسال المرور تلقت يتم قياس حركة المرور، وتأخير وعدد من الاصطدام وتحليلها. تم إجراء المحاكاة باستخدام OPNET صانع التماثيل الطبعة 14.5. لدراسة أداء شبكات LAN و VLAN

**الكلمات المفتاحية:** شبكة محلية (LAN) الشبكات المحلية الظاهرية، التوجيه بين VLAN، الأداء، المحاكاة، OPNET، إرسال حركة المرور.

## Abstract

The use of virtual LANs (VLANs) and routing between those same LANs became systematic in contemporary interconnection infrastructure. This inter-VLAN routing has many interests of both the design point of view of operating standpoint. Performance aspects such as sending traffic received traffic are measured and analyzed. The simulation was performed using OPNET Modeler Edition 14.5. To study the performance of LAN and VLAN networks and inter vlan routing

**Keywords:** Local Network (LAN), VLANs, inter-VLAN routing, performance, simulation, OPNET, sending traffic.

## Résumé

L'usage des réseaux locaux virtuels (VLANs) et du routage entre ces mêmes réseaux locaux est devenu systématique dans les infrastructures d'interconnexion contemporaines. Ce routage inter-VLAN présente de nombreux intérêts tant du point de vue conception que du point de vue exploitation. Les aspects de performance comme l'envoi de trafic, reçus de trafic, sont mesurés et analysés. La simulation a été réalisée en utilisant des OPNET Modeler Edition 14.5. Pour étudier la performance des réseaux LAN et VLAN. Et le routage inter vlan

**Mots-clés:** Réseau locaux (LAN), VLAN, Routage inter-vlan, Performance, la simulation, OPNET, l'envoi de trafic.