République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU

FACULTE DU GENIE ELECTRIQUE ET D' INFORMATIQUE
DEPARTEMENT D' ELECTRONIQUE

Mémoire de Fin d'Etudes
De MASTER ACADEMIQUE

Domaine : **Sciences et Technologies**
Filière : **Génie électrique**
Spécialité : **Télécommunication et réseaux**

Présenté par :
CHERIFI Hanane
CHERIFI Lydia

Mémoire dirigé par Mr SEHAD et co-dirigé par Mr BAGHDAD

Thème :

La configuration et l'interconnexion de deux réseaux distants

Mémoire soutenu publiquement Juiliet 2017 devant le jury composé de :

Président	M^{r} **LAZRI**	Maitre de de conférence (UMMTO)
Promoteur	M^{r} **SEHAD**	Maitre de de conférence (UMMTO)
Examinateur	M^{r} **OUALOUCHE**	Maitre de de conférence (UMMTO)

Année universitaire 2016/2017

Remerciement

On tient à exprimer nos vifs remerciements et nos sincères reconnaissances à notre encadreur MR BAGHDAD qui nous a fait profiter de salarge expérience tout au long de ce projet de fin d'étude ainsi qu'à notre promoteur MR SAHAD pour sa disponibilité et MR OUALOUCH ET LAZRI pour Leurs aides.

Nous remercions les membres du jury qui nous on fait l'honneur de participer au jugement de ce travail.

Un grand merci à notre famille respective en particulier à nos parents pour nous avoir soutenues et aidées tout au long de nos études.

Nous tenons aussi à remercier vivement tous ceux qui nous ont aidées de prés ou de loin à élaborer ce projet , et tous nos amis.

Glossaire

A

ATS : Algérie Télécom Satellite.

ATI : Algérie Télécom Internet.

AT : Algérie Télécom.

ACL : Liste de contrôle D'accès.

ACE : Access Control Entry.

B

BOOTP : Booststrop Protocole.

Bit :Binary Digit

Bps : Bits par seconde.

C

CSMA /CD : Carrier Sense Multiple Access/Collision Detection.

CE :Customer Edge (router)

CME : Circuit Multiplication Equipement.

CISCO : Société de matériel informatique.

CLI : Command-line interface.

CMRR :Centres Mémoire de Ressources et de Recherche.

CRMT :Organisme de recherches scientifiques et techniques.

CRE : Commission de régulation de l'énergie.

CGIR : conception et gestion d'infrastructures réseau.

D

DECN : Digital Equipment corporations.

DLCI : Data Link Connection Identifier.

DHCP : Dynamic Host Configuration Protocol.

DNS : Domain Name Server.

DTP : Dynamic Trunk Protocol.

DSL : Digital Subscriber Line.

E

EIA / TIA : Electronic industriel Association / Télécommunication Industries Association .

ERA :Access Network Establishment

ERMS : ETUDES REALISATIONS EN METALLERIE

F

FDDI : Fiber Distributed Data Interface.

FTP : File Transfert Protocol.

FH : Fiber Hertizienne.

H

Hub :Host Unit Broadest

Host ID : Host Identification.

HDLC :High Level Data Link Control.

I

ISO : International Standard Organisation.

IP : Internet Protocol.

IPv4 : Internet Protocol version 4.

IPv6 : Internet Protocol version 6.

IANA : Internet Assigned Numbers Authority.

IBM :International Business Machines

IPSec :IP Security Protocols.

L

LLC : Layer link control.

LSR :Label Switch Router.

LS :Location Server.

L2TP :Layer 2 Tunneling Protocol.

LET :Laboratoire Des Equipements De Télécommunications.

LAN :Local Area Network.

M

MAN :Metropolitan Area Network.

MAC :Médium Access Control.

MAU : Multi station Access Unit.

MPLS :Multi Protocol Label Switching.

O

OSI :Open Systems Interconnection.

P

Ping : Send Echo Messages

PPP :Point To Point Protocol.

PAP : PasswordAuthentication Protocol.

PDU : Unité De Donnée De Protocole.

Q

QOS : Quality of Service

R

RNIS : Réseau Numérique à Intégration De Service.

S

STP : Shielded Twisted-Pair

SNA : Système Network Architecture

SSL :Secure Socket Layer

T

TCP :Transmission Control Protocol.

TLS :Transport Layer Security.

U

UDP : User Detagram Protocol.

UTP :User Datagram Protocol.

V :

VOIP : Voice Over IP.

VLAN : Réseau Local Virtuel.

VTP : Virtual Trunck Protocol.

VPN :Virtual Private Network.

VPS : Serveur Virtuel Privé.

W :

WAN : Wide Area Network.

WIFI : Wireless Fidehty (Ensemble Des Protocoles De Communication Sans Fil).

WINS : Windows Internet Naming Service.

Liste des figures

Liste des figures

Liste des figures

Liste des Tableaux

Sommaire

Sommaire

Sommaire

Chapitre II : Notions sur les réseaux locaux virtuels (Vlan) et les protocoles

Sommaire

Chapitre III : Conception de l'architecture d'interconnections

Sommaire

Chapitre IV : Simulation

Sommaire

INTRODUCTION GENERALE

Introduction

Le rôle des réseaux a sensiblement évolué ces dernières années, il ne se limite plus au transfert de l'information 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 sécurisé auprès d'un groupe plus ou moins vaste et hétérogène.

L'interconnexion des réseaux est devenue un sujet aussi important que les réseaux eux-mêmes. Il faut interconnecter les réseaux pour qu'ils puissent s'échanger des informations. Aucun domaine n'échappe à cette révolution technologique, qui au fil des jours s'affiche comme un outil indispensable de travail.

Le besoin de répartition et de disponibilité de l'information à tous les postes des entreprises a entraîné l'émergence des réseaux locaux. Un nouveau challenge s'offre aux professionnels de l'informatique. Celui d'interconnecter les réseaux locaux entre eux afin que l'emplacement géographique ne soit plus un handicap pour l'accès aux informations [1].

C'est dans ce contexte que nous allons traiter la problématique « configuration et interconnexion de deux réseaux distants » pour qu'on dispose d'un réseau d'entreprise permettant de partager des ressources communes, d'échanger des informations et des communications téléphoniques sur IP.

Afin de connecter deux sites distants, nous disposons de plusieurs solutions [2]. Notre choix s'est porté sur l'utilisation de lignes spécialisées qui convient particulièrement aux moyennes et grandes entreprises.

Algérie télécom est le fournisseur de ces lignes pour les entreprises algériennes ayant Des besoins de communiquer de façon permanente et en toute sécurité avec ses différents sites.

Effectivement Nous avons effectué notre stage au sein d'Algérie Télécom qui a pour objectif l'étude et conception d'interconnexions de deux réseaux distants par des solutions fiables et moins couteuses.

Nous avons structuré le présent mémoire en quatre chapitres :

dans le premier chapitre, nous présentons les généralités sur les réseaux informatiques.

Le deuxième chapitre est consacré aux notions sur les réseaux locaux virtuels (VLAN) et les protocoles. Le troisième chapitre dédie à concevoir l'architecture d'interconnexion.

Le quatrième chapitre est consacré à la simulation de l'architecture avec le logiciel Cisco « paquet Tracer», ainsi le teste et la validation de la configuration.

Enfin nous terminons notre travail par une conclusion générale.

I. Préambule

Avant l'existence des réseaux, les personnes qui souhaitaient partager des informations devaient les échanger oralement, les copier sur une disquette et la remettre à une autre personne qui devait recopier son contenu sur son ordinateur.

La nécessité de communication et du partage des informations en temps réel, impose aujourd'hui aux entreprises la mise en réseau de leurs équipements informatiques en vue d'améliorer leurs rendements [1].

Avant de nous attaquer aux infrastructures réseaux, reprenons quelques notions théoriques de base sur les réseaux informatiques en général.

I .1 Définition des réseaux informatiques

Un réseau informatique est un ensemble d'ordinateurs et de terminaux interconnecter entre eux au moyen des médias de communication pour objectif de réaliser le partage des différentes ressources matérielles et/ou logicielles.

I.2 Fonctionnalité d un réseau informatique

Un ordinateur est une machine permettant de manipuler des données. L'utilisateur, en étant qu'être communiquant, a rapidement compris l'intérêt qu'il pouvait y avoir à relier ces ordinateurs entre eux afin de pouvoir échanger des informations.

Un réseau informatique peut servir plusieurs buts distincts :

- **Partage de fichier :** selon le niveau de sécurité et d'administration centralisée souhaités. Permet à plusieurs utilisateurs de lire, de modifier un fichier simultanément; verrouiller des parties d'un fichier à quelques utilisateurs …etc.

- **Application centrale :** dans des applications de gestion au sens large, on fait appel à un programme gérant une ou plusieurs bases de données, ces logiciels nécessitent généralement un serveur avec un système d'exploitation dédié. Ceci permet à plusieurs PC de travailler sur la même base de données simultanément.

- **Le partage de connexion internet :** permet de connecter plusieurs ordinateurs simultanément sur internet via une seule liaison (passerelle), le partage utilise les fonctionnalités de Windows.
- **Le partage de périphérique :** partage des ressources matérielles, (d'imprimante, de disque, graveur…etc.).
- **La communication entre personne :** courrier électronique, discussion en direct…etc.
- **La communication entre processus :** entre les ordinateurs industriels…etc.

I.3 Les Différents types des réseaux :

On peut distinguer différent types des réseaux selon plusieurs critère tel que (la taille de réseau, sa vitesse de transfère des données et aussi leur entendu) telle que :

- LAN (Local Area Network)
- MAN (Métropolitain Area Network)
- WAN (Wide Area Network)

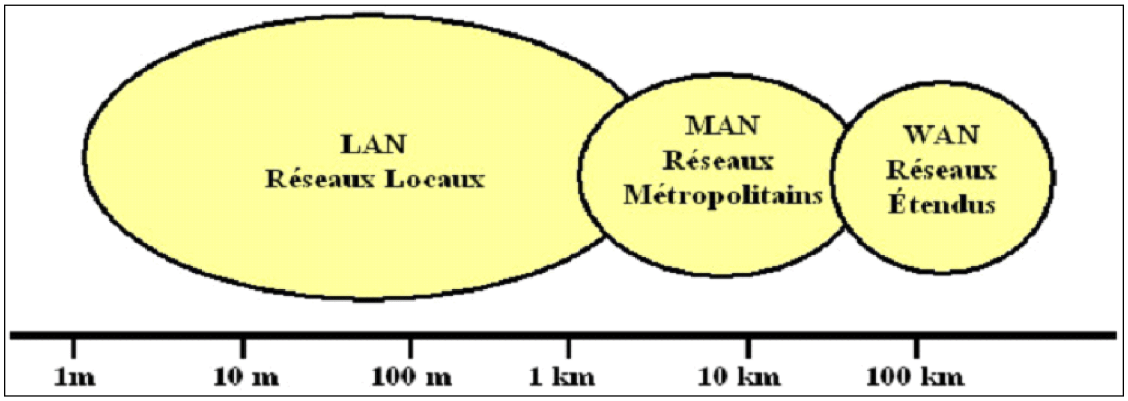


Figure I.1 : Différents types des réseaux

I .3.1 Les réseaux locaux LAN

LAN (réseau local), il s'agit d'un ensemble d'ordinateurs appartenant à une organisation, reliés entre eux sur une échelle géographique relativement restreinte, souvent à l'aide d'une même technologie. Exemple : cyber café. Un réseau local est donc un réseau sous sa forme la plus simple.

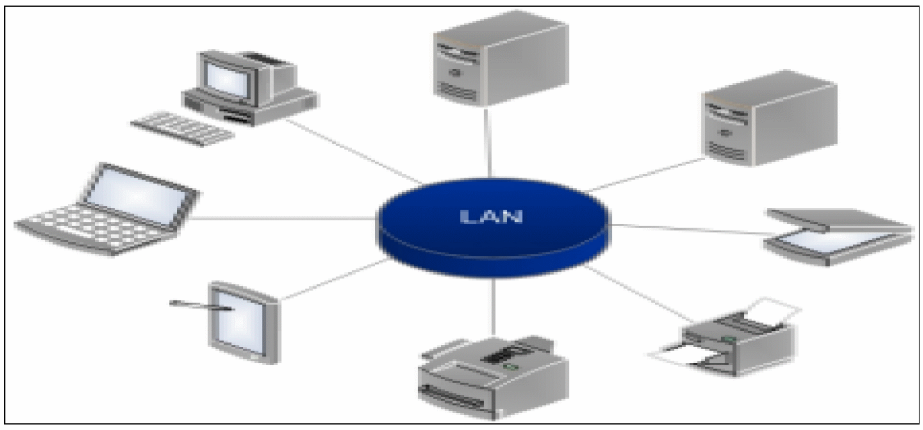


Figure I.2 : Exemple réseau LAN

I.3.2 Les réseaux métropolitains MAN

Les MAN (Métropolitaine Area Network) interconnectent 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 s'ils faisaient partie d'un même réseau local. Il peut regrouper un petit nombre de réseau locaux au niveau d'une ville ou d'une région.

Un MAN est formée de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

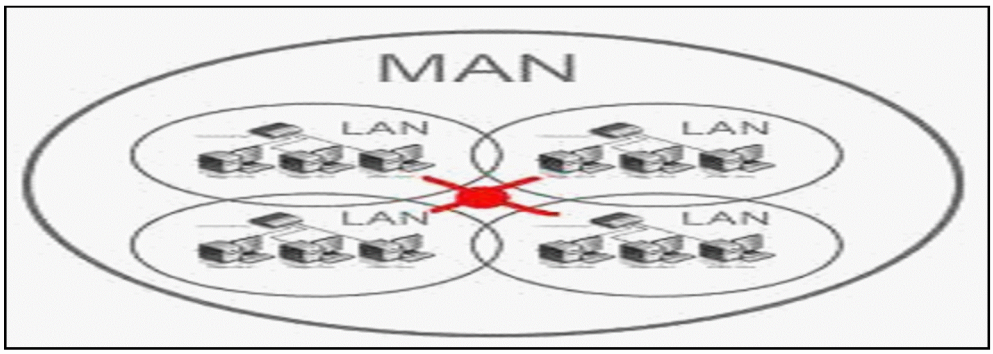


Figure I. 3 : Exemple d'un réseau MAN

I.3.3 Les réseaux étendus WAN

Réseau étendu à longue distance constitué par l'interconnexion des plusieurs réseaux et qui se distingue des réseaux locaux et métropolitains. Il relie plusieurs ordinateurs notamment

à travers une ville, un pays, continent ou encore toute la planète, la communication s'effectue grâce aux réseaux privées et ou publiques [1].

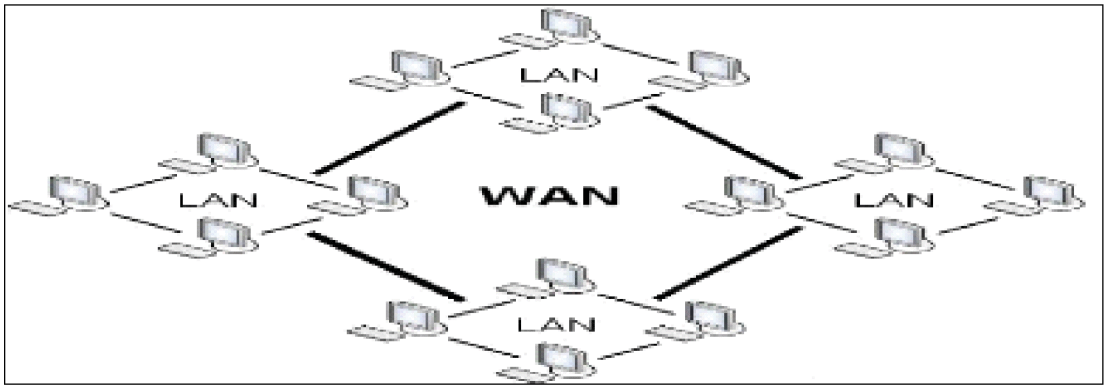


Figure I. 4: Exemple d'un réseau WAN

I.4 Les réseaux locaux d entreprise

Nous allons mettre le point sur les réseaux locaux d'entreprise, leurs caractéristiques ainsi que les éléments utilisés.

I.4.1 Caractéristiques d'un réseau local :

Les réseaux locaux sont des infrastructures complexes et pas seulement des câbles entre stations de travail. Si l'on énumère la liste des composants d'un réseau local, on sera surpris d'en trouver une quantité plus grande que prévu :

- **Le câblage :** constitue l'infrastructure physique, avec le choix entre paires téléphoniques, câble coaxial ou fibre optique. Il détermine le type de concentrateurs (Switch, Hub, Point d'accès WIFI…). Ces équipements constituent les nœuds dans le cas des réseaux en étoile.
- **La méthode d'accès :** décrit la façon dont le réseau arbitre les communications de différentes stations sur le câble : ordre, temps de parole, organisation des messages. La méthode d'accès est essentiellement matérialisée dans les cartes d'interfaces, qui connectent les stations au câble.
- **Les protocoles de réseaux** sont des logiciels qui ''tournent'' à la fois les différentes stations et leurs cartes d'interface réseaux. C'est le langage de communication. Pour que deux structures connectées sur le réseau, ils doivent ''parler'' le même protocole.

- **Le système d'exploitation** du serveur réseau, souvent nommé gestionnaire du réseau, est installé sur les serveurs. Il gère les partages, droits d'accès,…pour Microsoft, on retrouve Windows NT serveur, Windows 2003, 2008. Ce sont des versions spécifiques.
- **Le système de sauvegarde** est un élément indispensable qui fonctionne de diverses manières soit en recopiant systématiquement tous les fichiers des serveurs, soit en faisant des sauvegarde régulières, éventuellement automatisées.
- **Un pont, un routeur ou passerelle** constituent les moyens de communication qui permettent à un de ses utilisateurs de ''sortir'' du réseau local pour atteindre d'autres réseaux ou des serveurs distants, internet.
- **Le système de gestion et d'administration** du réseau envoie des alarmes en cas d'incidents, comptabilise le trafic, mémorise l'activité du réseau et aide à superviser son réseau. Cette partie est typiquement software.

I.4.2 Architecture des réseaux locaux :

Dans les réseaux locaux, il existe deux architectures applicatives qui sont :

I.4.2.1 Architectures du réseau poste à poste

Le réseau post à post appelé (peer to peer ou point à point ou égal à égal) est un réseau ou chaque poste gère ses propres ressources, chaque utilisateur est administrateur de sa propre machine. Avec cette architecture, chaque poste est à la fois serveur et client. Il n'y a pas d'hiérarchie entre les machines ni de statut privilégié pour certains utilisateurs, ils ne sont pas dotés d'un serveur central pour stocker les fichiers (données). Cela signifie que l'ordinateur joue le rôle du client serveur à la fois.

L'avantage du réseau poste à poste est qu'il est facile à mettre en place avec un coût faible. Les inconvénients sont qu'il ne supporte pas plusieurs machines, qu'il peut devenir difficile à administrer et qu'il n'est pas aussi sécurisé.

Cette architecture est beaucoup plus efficace aux petites structures où la sécurité n'est pas nécessaire et ne dépassant plus d'une dizaine d'ordinateurs.

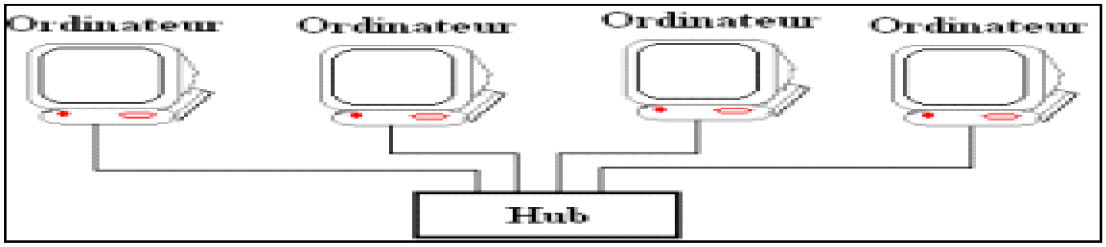


Figure I. 5 : Architecture poste à poste

I.4.2.2 Architecture du réseau client/ serveur

Le réseau client/serveur est un réseau dans le lequel une ou plusieurs machines jouent le rôle du serveur (ou des serveurs). Les autres machines sont des machines clientes. Le serveur est chargé de fournir des services aux clients. Quand une machine cliente veut un service, il envoie une requête au serveur. Ce dernier analyse la requête et satisfait la machine cliente en lui envoyant le service voulu. Un serveur est une machine souvent si puissante plus une application serveur. C'est pour cela d'ailleurs qu'en pratique, une machine peut jouer le rôle de plusieurs serveurs en même temps.

Les avantages d'un réseau client/serveur sont que le réseau peut supporter plusieurs machines, qu'on peut ajouter ou retirer un poste client sans perturber le réseau, qu'il y a la sécurité du réseau, qu'il y a une centralisation des ressources et que l'administration se fait au niveau serveur.

Les inconvénients sont que le prix est élevé, que le disfonctionnement du serveur entraine le disfonctionnement du réseau et qu'il y a un risque d'avoir un encombrement si plusieurs machines émettent au même moment [1].

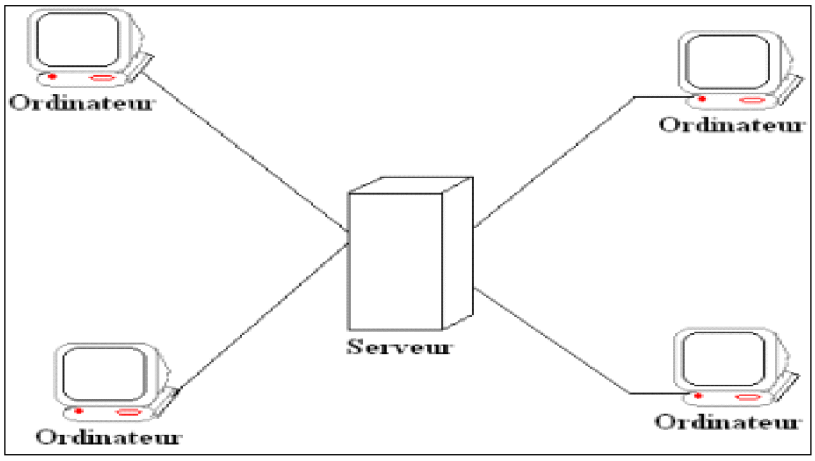


Figure I.6 : Architecture client / serveur

I.5 Topologies

C'est l'ensemble des méthodes physiques et standards qui orientent ou facilite la circulation des données entre ordinateurs dans un réseau.

Il existe deux types de topologie à savoir : la topologie physique et la topologie logique.

I.5.1 Topologie Physique

La topologie physique désigne la manière dont les équipements sont interconnectés en réseau. Dans cette topologie nous avons trois grandes topologies qui sont :

I.5.1.1 Topologie en Bus

Dans une topologie en bus, tous les ordinateurs sont connectés à un seul câble continu ou segment.

Les avantages de ce réseau : coût faible, faciliter de la mise en place et la distance maximale de 500m pour les câbles de 10 base 5 et 200m pour les câbles de 10 base 2. La panne d'une machine ne cause pas une panne au réseau, le signal n'est jamais régénère, ce qui limite la longueur des câbles. Il faut mettre un répéteur au-delà de 185m. Ce réseau utilise la technologie Ethernet 10 base 2.

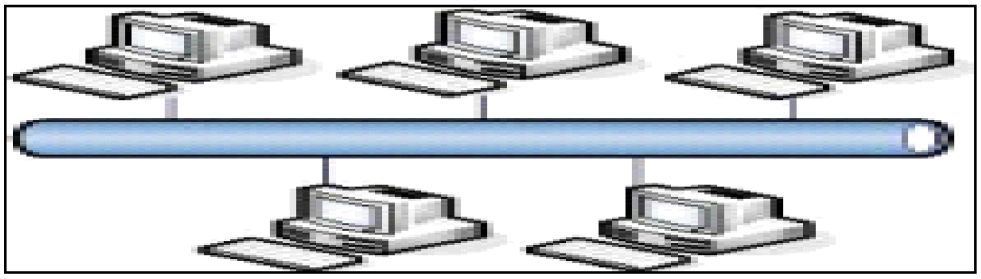


Figure I. 7 : topologie en bus

I.5.1. 2 Topologie en Etoile

La topologie en étoile est la plus utilisée. Dans la topologie en étoile, tous les ordinateurs sont reliés à un seul équipement central, qui peut être un concentrateur (Hub), un commutateur (Switch), ou un Routeur.

Les avantages de ce réseau est que la panne d'une station ne cause pas la panne du réseau et qu'on peut retirer ou ajouter facilement une station sans perturber le réseau.

Il est aussi très facile à mettre en place mais les inconvénients sont : que le coût est un peu élevé, la panne du concentrateur centrale entraine le disfonctionnement du réseau.

La technologie utilisée est l'Ethernet 10 base T, 100 base T.

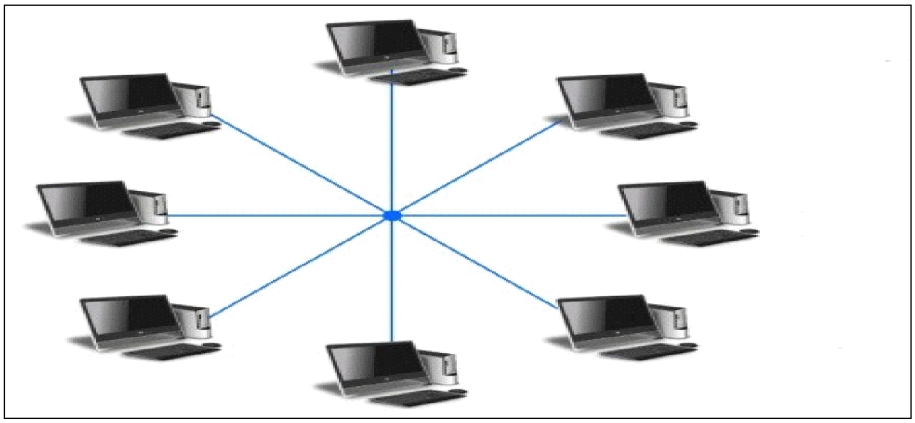


Figure I.8 : Topologie en étoile

I.5.1. 3 Topologie en Anneau

Dans un réseau possédant une topologie en anneau, les stations sont reliées en boucle et communiquent entre elles. Avec la méthode « chacun à son tour de communiquer». Elle est utilisée pour le réseau Token ring ou FDDI

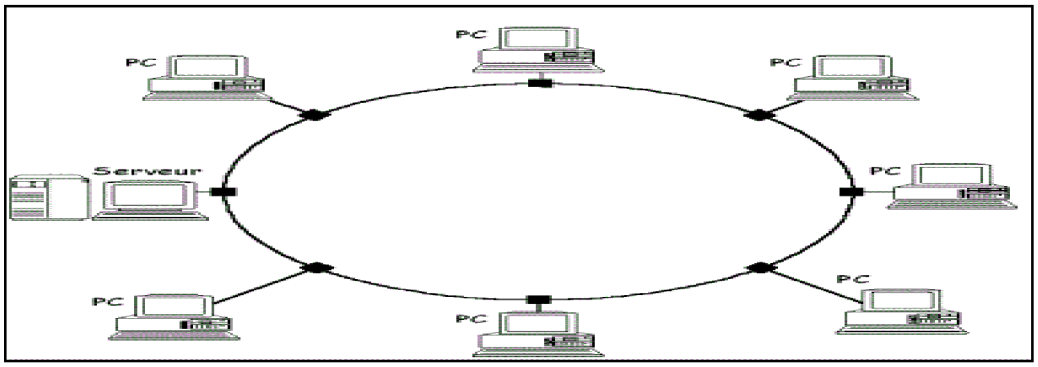


Figure I.9 : topologie en Anneau

I.5.2 Topologie logique

La topologie logique désigne la manière dont les équipements communiquent en réseau. Dans cette topologie les plus courantes sont les suivantes :

I.5.2.1 Topologie Ethernet

Ethernet est aujourd'hui l'un des réseaux les plus utilisées en local. Il repose sur une topologie physique en étoile.

Dans un réseau Ethernet, la communication se fait à l'aide d'un protocole appelé CSMA/CD, ce qui fait qu'il aura une très grande surveillance des données à transmettre pour éviter toute sorte de collision. Par conséquent un poste qui veut émettre doit vérifier si le canal est libre avant d'y émettre.

I.5.2.2 Topologie Token ring

Elle repose sur une topologie physique en Anneau (ring), il utilise la méthode d'accès par jeton (token). Dans cette technologie, seul le poste ayant le jeton a le droit de transmettre si un poste veut émettre, il doit attendre jusqu'à ce qu'il ait le jeton ; dans un réseau token ring, chaque noeud du réseau comprend un MAU (Multi Station Access Unit) qui peut recevoir les connexions des postes. Le signal qui circule est régénéré par chaque MAU.

Mettre en place un réseau token ring coûte chers, malgré la panne d'une station MAU provoque le disfonctionnement du réseau.

I.5.2.3 Topologie FDDI

La technologie LAN FDDI (Fiber Distributed Data Interface) est une technologie d'accès réseau utilisant des câbles fibre optiques.

Le FDDI est constitué de deux anneaux : un anneau primaire et anneau secondaire. L'anneau secondaire sert à rattraper les erreurs de l'anneau primaire, le FDDI utilise un anneau à jeton qui sert à détecter et à corriger les erreurs. Ce qui fait que si une station MAU tombe en panne, le réseau continuera de fonctionner [1].

I.6 Supports de transmission

Pour relier les diverses entités d'un réseau, plusieurs supports physiques de transmission de données peuvent être utilisés. Une de ses possibilités est l'utilisation de câbles.

Il existe de nombreux types de câbles, mais on distingue généralement :

- Le câble de type coaxial.
- Le câble de type pair torsadé.
- La fibre optique.

En plus des liaisons physiques, actuellement il y'a des réseaux qui utilisent la liaison sans fil comme support de transmission.

I.6.1 Le Câble coaxial :

Le câble coaxial (en Anglais coaxial câble) a longtemps été le câblage de prédilection, pour la simple raison qu'il soit peu coûteux et facilement manipulable (poids, flexibilité, …).

Un câble coaxial est constitué d'une partie centrale (appelée âme), c'est-à-dire un fil de cuivre, enveloppé dans un isolant, puis d'un blindage métallique tressé et enfin d'une gaine extérieure.

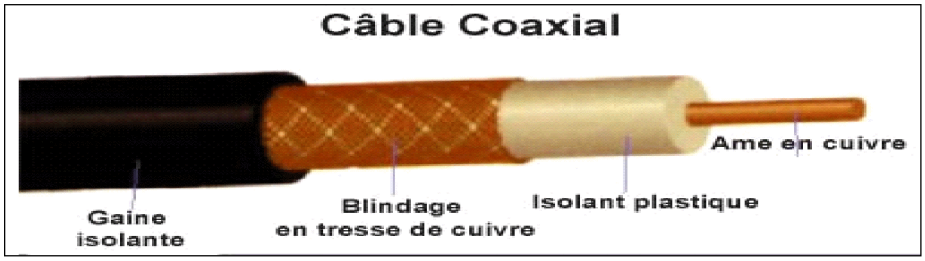


Figure I .10 : Câble coaxial

- **gaine** permet de protéger le câble de l'environnement extérieur. Elle est habituellement en caoutchouc (parfois en chlorure de polyvinyle (PVC), éventuellement en téflon).
- **Le blindage** (enveloppe métallique) entourant les câbles permet de protéger les données transmises sur le support des parasites (autrement appelés, bruit) pouvant causer une distorsion de données.
- **L'isolant** entourant la partie centrale est constitué d'un matériau diélectrique permettant d'éviter tout contact avec le blindage, provoquant des interactions électriques (court-circuit).
- **L'âme** accomplissant la tâche de transport des données, est généralement composée d'un seul brin en cuivre ou de plusieurs brins torsadés.

Grace à son blindage, le câblage coaxial peut être utilisé sur des longues distances et à haut débit (contrairement à un câble de type pair torsadé), on le réserve toutefois pour des installations de base.

Il existe des câbles coaxiaux possédant un blindage double (une couche isolante, une couche de blindage) ainsi que des câbles coaxiaux à quadruple blindage (deux couches isolantes, deux couches de blindage).

➢ On distingue habituellement deux types de câbles coaxiaux :

- **Le 10Base2 (câble coaxial fin) :** est un câble de fin diamètre (6mm), de couleur blanche (ou grisâtre) par convention. Très flexible il peut être utilisé dans la majorité

des réseaux, en le connectant directement sur la carte réseau. Il permet le transport d'un signal sur une distance d'environs 185 mètres sans affaiblissement.

- **Le 10Base5 (câble coaxial épais):** est un câble blindé de plus gros diamètre (12mm) et de 50 ohms d'impédance. Il y'as longtemps été utilisé dans les réseaux Ethernet, ce qui lui a voulu l'appellation de «Câble Ethernet Standard ». Etant donné que son âme a un plus gros diamètre, la distance susceptible d'être parcourue par les signaux est grande, cela lui permet de transmettre sans affaiblissement des signaux sur une distance atteignant 500 mètre (sans ré amplification du signal). Sa bande passante est de 10Mbps il est donc employé très souvent comme câble principal (back one) pour relier des petits réseaux dont les ordinateurs sont connectés avec du Thinnet. Toutefois, étant donné son diamètre il est moins flexible que le Thinnet.

I.6.2 La paire torsadée :

Dans sa forme la plus simple, le câble à paire torsadée est constitué de deux brins de cuivre entrelacés en torsade et recouverts d'isolants.

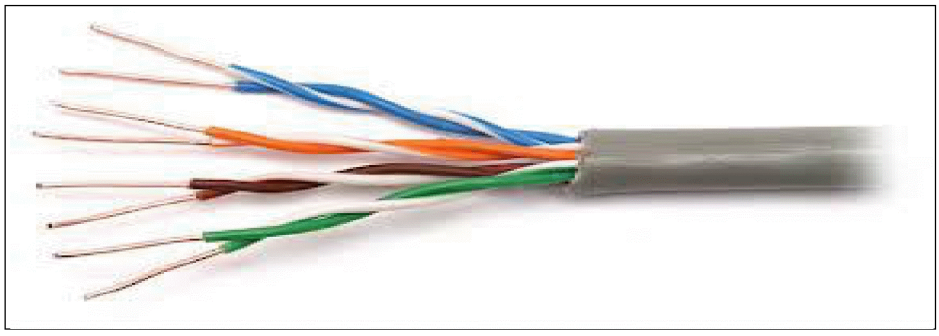


Figure I.11: Câble a paire torsadées

➢ On distingue généralement deux types de paires torsadées :

- Les paires blindées (STP : Shielded Twisted-Pair).
- Les paires non blindées (UTP : Unshielded Twisted-Pair).

La paire torsadée est donc adaptée à la mise en réseau local d'un faible parc avec un budget limité, et une connectique simple. Toutefois, sur de longues distances avec des débits élevés elle ne permet pas de garantir l'intégrité des données.

I.6.2 .1 La paire torsadée non blindées (UTP) :

Le câble UTP obéit à la spécification 10BaseT. C'est le type de paire torsadée le plus utilisé et le plus répandu pour les réseaux locaux. Voici quelques caractéristiques :

- Longueur maximale d'un segment : 100 mètres
- Composition : 2 fils de cuivre recouverts d'isolant
- Norme UTP : conditionnent le nombre de torsions par pied (33cm) de câble en fonction de l'utilisation prévue.

UTP : répertorié dans la norme commerciale Building Wiring Standard 568 de l'EIA/TIA (Electronic industries association/ télécommunication Industries Association). La norme EIA/TIA 568 a utilisé UTP pour créer des normes applicables à toutes sortes de locaux et de contextes de câblage qui garantissent au public l'homogénéité des produits. Ces normes incluent cinq catégories de câbles UTP :

- **Catégorie 1 :** câble téléphonique traditionnel (transfert de voix mais pas de données).
- **Catégorie 2 :** transmission des données à 4 Mbit/s maximum (RNIS). Ce type de câble est composé de 4 paires torsadées.
- **Catégorie 3 :** 10 Mbit/s maximum. Ce type est composé de 4 paires torsadées et de 3 torsions par pied.
- **Catégorie 4 :** 16 Mbit/s maximum. Ce type de câble est composé de 4 paires torsadées en cuivre.
- **Catégorie 5 :** 100 Mbit/s maximum. Ce type de câble est composé de 4 paires torsadées en cuivre.

La plupart des installations téléphoniques utilisent un câble UTP. Si la paire torsadée préinstallé est de bonne qualité, il est possible de transférer des données et donc l'utiliser en réseau informatique. Il faut faire attention cependant aux nombres de torsades et aux autres caractéristiques électriques requises pour une transmissions de données de qualité.

Le majeur problème provient du fais que le câble UTP est particulièrement sujet aux interfaces (signaux d'une ligne se mélangeant à ceux d'une autre ligne). La seule solution réside dans le blindage.

I.6.2.2 La paire torsadée blindée (STP) :

Le câble STP (Shleded Twisted Pair) utilise une gaine de cuivre de meilleure qualité et plus protectrice que la gaine utilisée par le câble UTP. Il contient une enveloppe de protection entre les paires et autour des paires. Dans le câble STP les fils de cuivre d'une paire sont eux-mêmes torsadés, ce qui fournit au câble STP un excellent blindage, c'est-à-dire une meilleure protection contre les interférences. D'autre part il permet une transmission plus rapide et sur une plus longue distance.

Figure I.12 : Câble UTP et FTP

I.6.2.3 les connecteurs pour paire torsadé :

La paire torsadée se branche à l'aide d'un connecteur RJ-45. Ce connecteur est similaire au RJ-11.de plus, le RJ-45 se compose de huit broches alors que RJ-11 n'en possède que six, voir quatre généralement.

I.6.3 La fibre optique :

Le câblage optique est particulièrement adapté à la liaison entre répartiteurs (liaison centrale entre plusieurs bâtiments, appelé back one, ou en français épine dorsale) car elle permet des connexions sur de longues distances (de quelques kilomètres à 60 km dans le cas fibre monomode) sans nécessiter de mise à la masse. De plus ce type de câble est très dur car il est extrêmement difficile de mettre un tel câble sur écoute.

Toutefois, malgré sa flexibilité mécanique, ce type de câble ne convient pas pour des connexions dans un réseau local car son installation est problématique et sont cout est élevé. C'est la raison pour laquelle on opte pour la paire torsadée ou le câble coaxial pour de petites liaisons.

La fibre optique est constituée d'un cylindre de verre ou de plastique très mince entouré d'une gaine généralement de même matériau mais présentant un indice de réfraction optique lus faible. Le tout est protégé par une gaine extérieure.

✓ La fibre optique est un câble possédant de nombreux avantages :

- Légèreté
- Immunité au bruit
- Faible atténuation
- Tolère des débits de l'ordre de 100 Mbps
- Largeur de bande de quelques dizaines de mégahertz à plusieurs gigahertz (fibre monomode).
- Le câblage optique permet des connexions sur de longues distances de quelques kilomètres à 60km dans le cas de fibre monomode sans nécessiter de mise à la masse.

De plus ce type de câble est très sur car il est extrêmement difficile de mettre un tel câble sur écoute.

Figure 1. 13 : Fibre optique

I.6.4 Les ondes radios :

Les liaisons par infrarouges sont utilisées dans les réseaux locaux d'entreprise pour éviter un câblage encombrant. Les liaisons par faisceaux hertziens peuvent être terrestres ou satellitaires. Les débits sont très élevés mais les transmissions sont sensibles aux perturbations et les possibilités d'écoute sont nombreuses [1].

I.7 Les équipements du réseau :

1.7.1 Modem

Le Modem (pour modulation-démodulation), est un périphérique servant à communiquer avec des utilisateurs distants par l'intermédiaire d'une ligne téléphonique. Il permet par exemple d'échanger (envoi/réception) des fichiers, de se connecter à Internet…

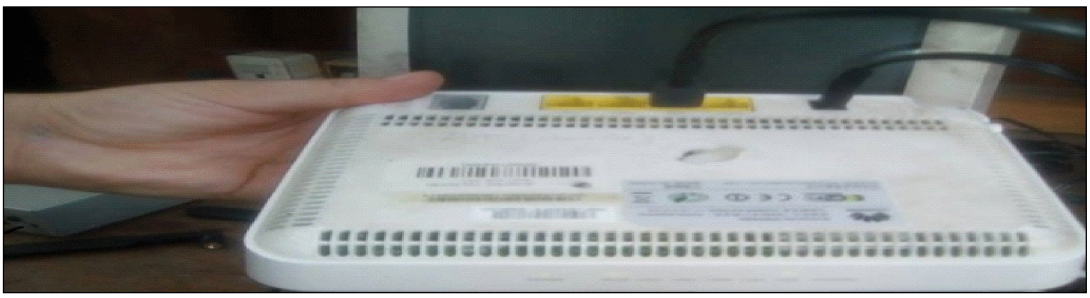


Figure I.14: Modem

I.7.2 Répéteurs (répéter) :

Un répéteur est un dispositif électronique combinant un récepteur et un émetteur, qui compense les pertes de transmission d'un média (ligne, fibre, radio) en amplifiant et traitant éventuellement le signal, sans modifier son contenu.

Figure I. 15: Répéteur

I.7.3 Routeur (router) :

Un routeur est un équipement d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter.

Figure I.16: Routeur

I.7.4. Hub (Host Unit Broadest) :

Un Hub est un élément matériel permettant de connecter le trafic réseau provenant de plusieurs hôtes, et de régénérer le signal. Le hub est ainsi une entité possédant un certain nombre de ports (généralement 4, 8,16 ou 32). Son unique but est de récupérer les données binaires parvenant sur un port et de les diffuser sur l'ensemble des ports.

Le hub permet de connecter plusieurs machines entre elles, parfois disposées en étoile, ce qui lui vaut le nom de Hub, pour illustrer le fait qu'il s'agit du point de passage des communications des différentes machines.

Figure I .17: Hub

I.7.5 Switch (switchers) :

Un Switch est un pont multiport, c'est-à-dire qu'il s'agit d'un élément actif agissant un niveau 2 du modèle OSI.

Le Switch analyse les trames arrivant sur ses ports d'entrée et filtre les données afin de les aiguiller uniquement sur les ports adéquats. Si bien que le Switch permet d'allier les propriétés du pont en matière de filtrage et du concentrateur en matière de connectivité.

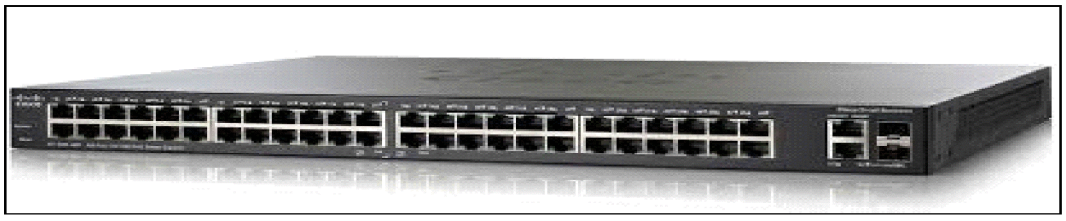


Figure I.18 : Switch

I.7.5 Carte réseau (Network Unterface Card) :

Une carte réseau est matérialisée par un ensemble de composants électroniques soudés sur un circuit imprimé. L'ensemble constitué par le circuit imprimé et les composants soudés s'appelle une carte électronique, d'où le nom de carte réseau.

La carte réseau ou NIC (Network Interface Card) est une carte qui sert d'interface entre la machine et le support de transmission. Elle possède généralement deux témoins lumineux (LED). La fonction d'une carte réseau est de préparer, d'envoyer et de contrôler les données sur le réseau.

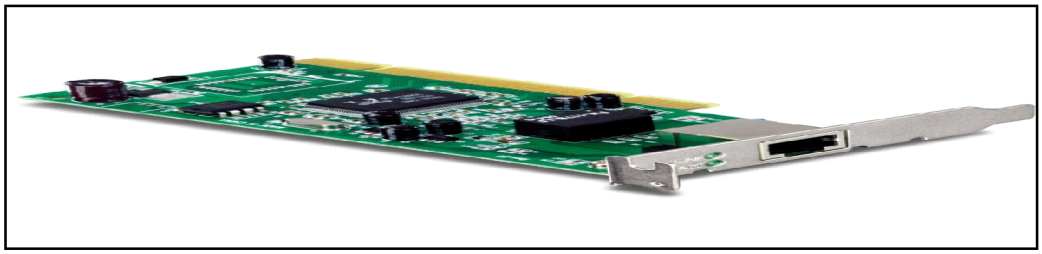


Figure I.19 : Carte réseau

I.7.6 Scalance :

Les points d'accès SCALANCE sont utilisés pour construire le réseau sans fil et fournir à ses clients l'accès à la radio, par exemple, SCALANCE clients, les appareils sans fil ou les ordinateurs portables. Pour les grandes infrastructures, plusieurs

Points d'accès couvrent le réseau sans fil et aussi soutenir la transition en douceur des clients entre les points d'accès. Selon la version du produit (plage de température ambiante est de -20 °C à +60 °C) la résistance contre la condensation permet également une utilisation en extérieur [1].

Figure I.20 : Scalance

I.8 Architecture des réseaux informatiques

Pour que les données transmises de l'émetteur vers le récepteur et arrivent correctement avec la qualité de service exigée, il faut une architecture logicielle.

- Deux grandes architectures :
  - Le modèle OSI
  - Le modèle TCP/IP

I.8.1 Modèle OSI

La première évolution des réseaux informatiques a été des plus anarchiques, chaque constructeur développant sa propre technologie. Le résultat fut une quasi-impossibilité de connecter différents réseaux entre eux.

Pour palier à ce problème d'interconnections, l'ISO (International Standards Organisation) décida de mettre en place un modèle de référence théorique décrivant le fonctionnement des communications réseaux. Ainsi fût créé le modèle OSI, à partir des structures réseau prédominantes de l'époque : DECN (Digital Equipment Corporations Networking développé par digital) et SNA (System Network Architecture développé par IBM).Ce modèle a permis aux différents constructeurs de concevoir des réseaux interconnectables.

Le modèle OSI est un modèle conceptuel. Il a pour but d'analyser la communication en découpant les différentes étapes en 7 couches, chacune de ces couches remplissant une tâche bien spécifique.

I.8.1.1 Les 7 couches du modèle OSI sont les suivantes :

- **Couche 1** : **Couche physique**

La couche physique définit les spécifications du média (câblage, connecteur, voltage, bande passante…).

- **Couche 2 : Couche liaison de donnée**

La couche liaison de donnée s'occupe de l'envoi de la donnée sur le média. Cette couche est divisée en deux sous-couches :

La sous-couche MAC (Média Access Control) est chargée du contrôle de l'accès au média. C'est au niveau de cette couche que l'on retrouve les adresses de liaison de donnée (MAC, DLCI).

La sous-couche LLC (Layer Link Control) s'occupe de la gestion des communications entre les stations et interagit avec la couche réseau.

- **Couche 3** : **Couche réseau**

Cette couche gère l'adressage de niveau trois, la sélection du chemin et l'acheminement des paquets au travers du réseau.

- **Couche 4 : Couche transport**

La couche transport assure la qualité de la transmission en permettant la retransmission des segments en cas d'erreurs éventuelles de transmission. Elle assure également le contrôle du flux d'envoi des données.

- **Couche 5 : Couche session**

La couche session établit, gère et ferme les sessions de communications entre les applications.

- **Couche 6 : Couche présentation**

La couche présentation spécifie les formats des données des applications (encodage MIME, compression, encryptions).

- **Couche 7 : Couche application**

Cette couche assure l'interface avec les applications, c'est la couche la plus proche de l'utilisateur.

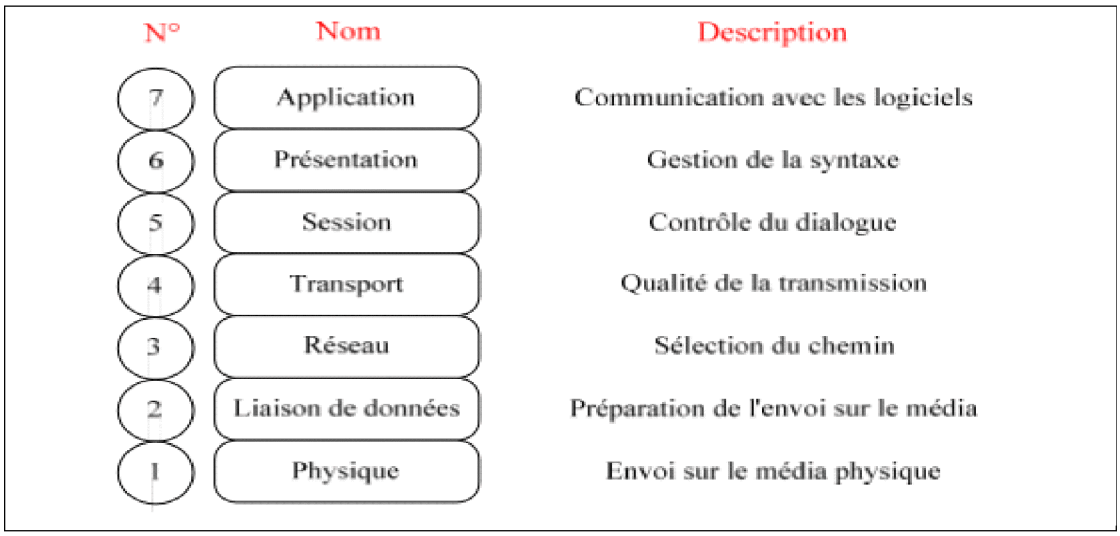


Figure I.21 : Les 7 couches du modèle OSI

I.8.1.2 Les Avantages du modèle OSI :

Une division de la communication réseau en éléments plus petits et plus simples pour une meilleure compréhension

- L'uniformisation des éléments afin de permettre le développement multi constructeur
- La possibilité de modifier un aspect de la communication réseau sans modifier le reste (Exemple : un nouveau média)

Pour communiquer entre les couches et entre les hôtes d'un réseau, OSI a recourt au principe d'encapsulation.

Encapsulation : processus de conditionnement des données consistant à ajouter un en-tête de protocole déterminé avant que les données ne soient transmises à la couche inférieure

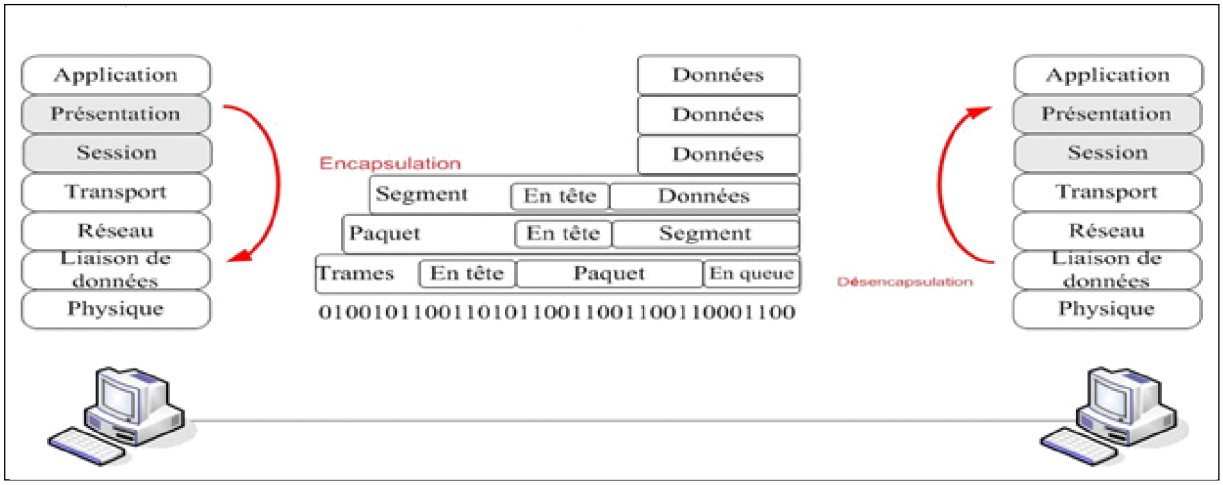


Figure I.22 : Principe de l'encapsulation

Lorsque 2 hôtes communiquent, on parle de communication d'égal à égal, c'est-à-dire que la couche N de la source communique avec la couche N du destinataire. Lorsqu'une couche de l'émetteur construit des données, elle encapsule ces dernières avec ses informations puis les passe à la couche inférieure. Le mécanisme inverse a lieu au niveau du destinataire ou une couche réceptionne les données de la couche inférieure, enlève les informations la concernant, puis transmet les informations restantes à la couche supérieure. Les données transitant à la couche N de la source sont donc les mêmes que les données transitant à la couche N du destinataire.

✓ Pour identifier les données lors de leur passage au travers d'une couche, l'appellation PDU (Unité de données de protocole) est utilisée.

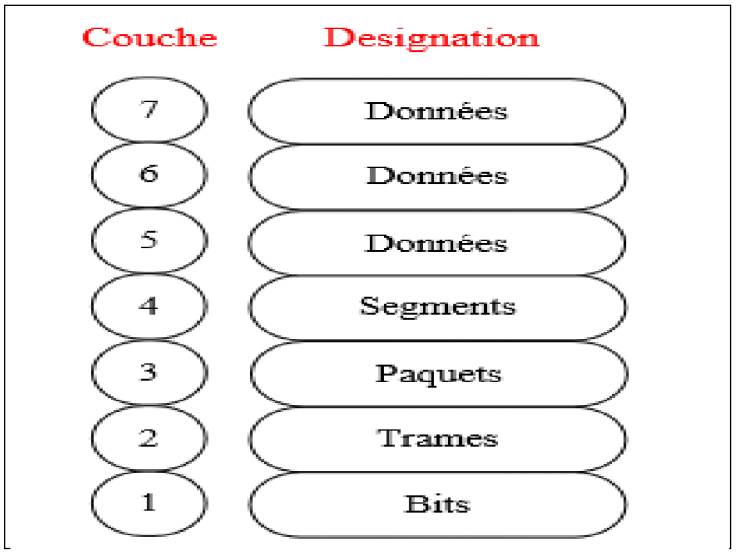


Figure I.23 : Identification des données

I.8.2 Modèle TCP/IP

I.8.2.1 Présentation de TCP/IP

Même si le modèle de référence OSI est universellement reconnu, historiquement et techniquement, la norme ouverte d'Internet est le protocole TCP/IP (pour Transmission Control Protocol/Internet Protocol). Le modèle de référence TCP/IP et la pile de protocoles TCP/IP rendent possible l'échange de données entre deux Mise en place de VLAN au sein du Réseau du Groupe ITA-Ingénierie SA : Cas du Site ITA-Marcory 29 ordinateurs, partout dans le monde, à une vitesse quasi équivalente à celle de la lumière.

TCP/IP est un modèle comprenant 4 couches :

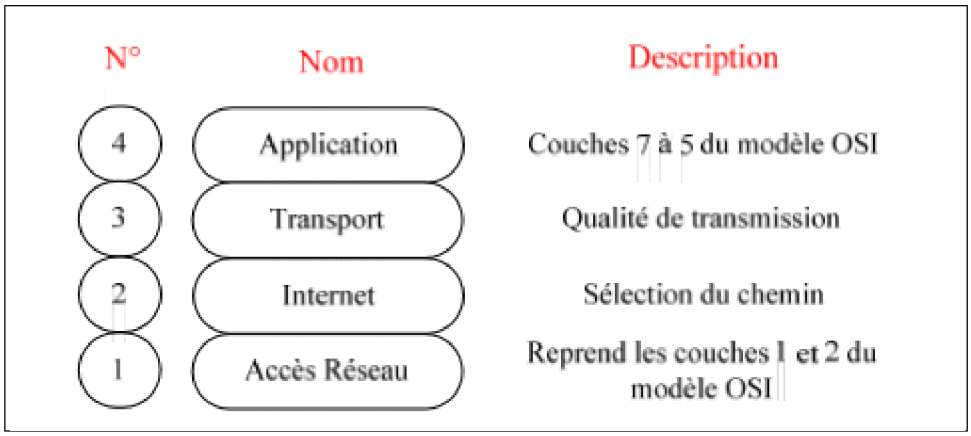


Figure I.24 : Les 4 couche TCP/IP

➢ Les rôles des différentes couches sont les suivants :

- **Couche Accès réseau** : elle spécifie la forme sous laquelle les données doivent être acheminées quelque soit le type de réseau utilisé
- **Couche Internet** : elle est chargée de fournir le paquet de données (datagramme).
- **Couche Transport** : elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaître l'état de la transmission.
- **Couche Application** : elle englobe les applications standard du réseau.

I.8.3 Comparaison entre le modèle TCP/IP et le modèle OSI

Ces deux modèles sont très similaires, dans la mesure où les 2 sont des modèles de communication à couche et utilisent l'encapsulation de données.

On remarque cependant deux différences majeures :

• TCP/IP regroupe certaines couches du modèle OSI dans des couches plus générales

• TCP/IP est plus qu'un modèle de conception théorique, c'est sur lui que repose le réseau

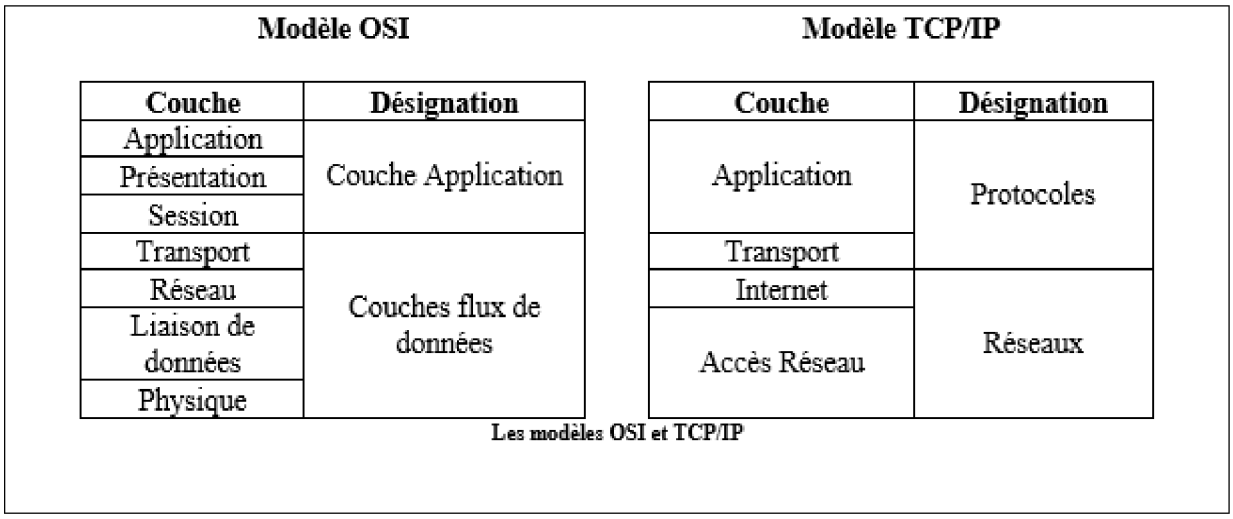


Figure I.25 : Les modèles OSI et TCP/IP

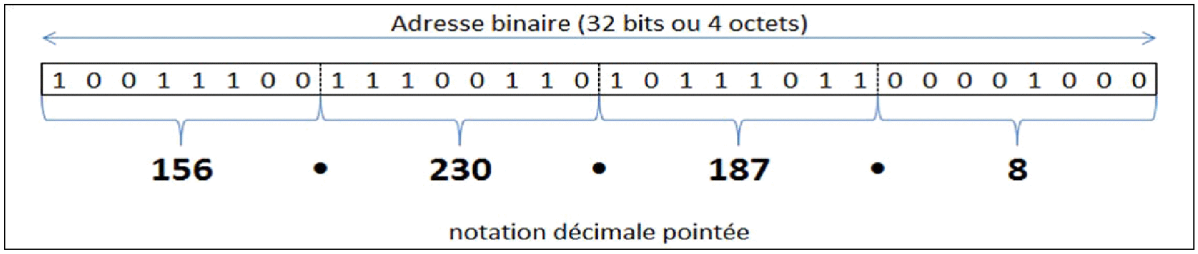
I.9 Protocole UDP (User Datagram Protocol)

UDP est un protocole de transport (couche 4 du modèle OSI) sans connexion qui fonctionne au dessus du protocole de réseau IP (couche 3 du modèle OSI). C'est un protocole simple a mettre en ouvre, cependant il n'est pas fiable (perte de messages, messages non ordonnes, . . .) Les messages qu'envoi UDP son appelés datagrammes [3].

I.10 Format de l'adresse IP

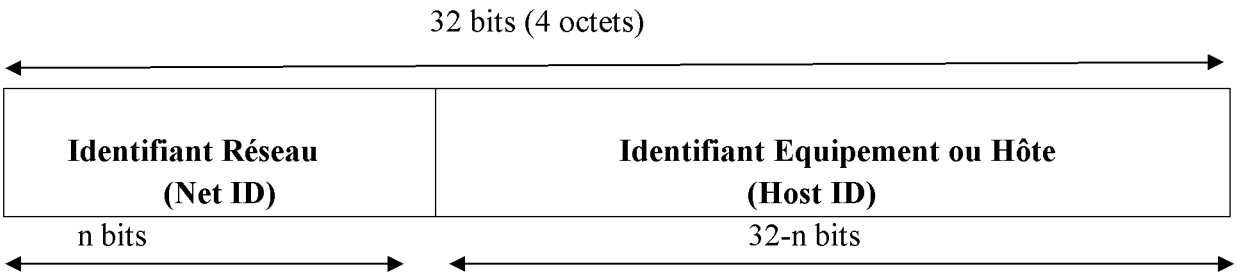
I.10.1 Notation

Une adresse IP (Internet Protocol) est constituée d'un nombre binaire de 32 bits. Pour faciliter la lecture et la manipulation de cette adresse on la représente plutôt en notation décimale pointée, par exemple :



I.10.2 Structure

Une adresse IP d'un équipement, codée sur 4 octets, contient à la fois un identifiant réseau (Net ID) et un identifiant équipement (Host ID)



Dans le cas des réseaux « standards » (sans sous-réseaux) la partie Identifiant Réseau peut être codée sur 1, 2 ou 3 octets. Le nombre de bits restants pour la partie HostID détermine le nombre d'équipements pouvant être connectés sur le réseau.

I.9.3 Classes d'adresses IP

En fonction du nombre d'équipements pouvant être connectés à un réseau, les adresses IP appartiennent à la **classe A, B ou C**.

- **Le format d'une adresse IP selon sa classe est le suivant :**

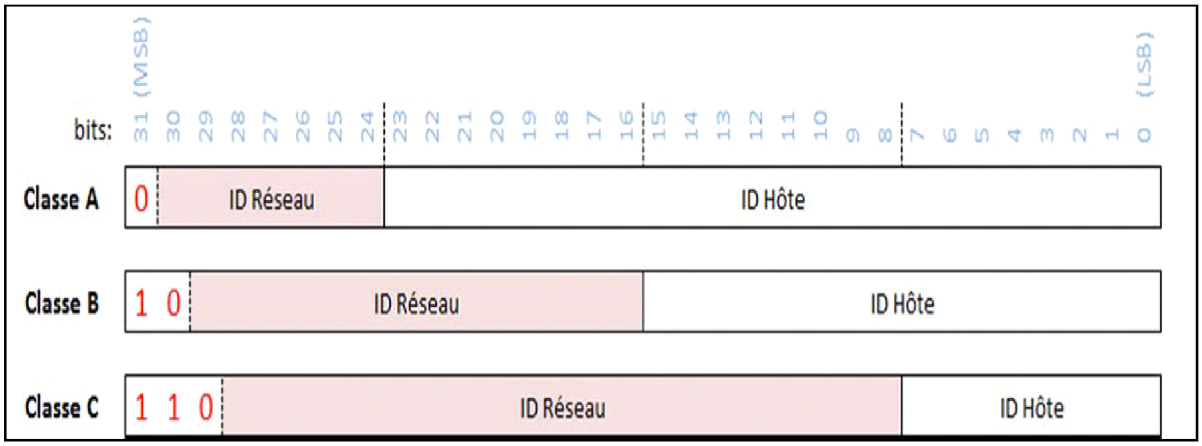


Figure I.26 : Les classes d'adresse IP

L'adresse IP du réseau est une adresse IP avec tous les bits de la partie « ID Hôte » à 0. C'est donc une Adresse réservée et non attribuable à un équipement.

Une autre combinaison est réservée. C'est celle où tous les bits de la partie « ID Hôte » sont à1. Cette adresse est l'adresse de diffusion (broadcaste) et sert à désigner tous les hôtes du réseau.

I.10.4 Masques de sous réseaux

I.10.4.1 Format

Une adresse IP est toujours associée à un « masque de sous-réseau », c'est grâce à celui-ci que l'on peut extraire de l'adresse IP, le N° de la machine et le réseau / sous réseau auquel il appartient.

Par défaut, lorsqu'il n'y a pas de sous réseaux, les masques sont :

@ En classe A : 255.0.0.0
@ En classe B : 255.255.0.0
@ En classe C : 255.255.255.0

I.10.5 Adresses Public / Adresses Privée

Sont celles qu'il est possible d'utiliser pour une connexion à l'Internet. Elles sont attribuées par l'IANA (Internet Assigned Numbers Authority) auprès de qui il faut s'enregistrer.

Tout ordinateur d'un réseau local voulant se connecter à Internet doit disposer de sa propre adresse IP.

I.10.5.1 Adresse public

Une adresse IP dite "publique" est une adresse qui est unique au niveau mondial et qui est attribuée à une seule entité.

- **Par exemple** l'adresse IP : 198.133.219.25 est celle du constructeur Cisco et que seul Cisco a le droit de l'utiliser.

I.10.5.2 Adresse privée

Une adresse IP dite "privée" est une adresse qui n'est pas unique au niveau mondial et donc qui peut être attribuée à plusieurs entités en même temps. La restriction pour que cela

soit autorisé est qu'une adresse IP privée ne peut pas sortir vers l'extérieur ou plus simplement ne peut pas sortir sur Internet [4].

Classe d'adresses privées	Plage d'adresses privées
Réseau privé de classe A	De 10.0.0.1 à 10.255.255.254
Réseau privé de classe B	De 172.16.0.1 à 172.31.255.254
Réseau privé de classe C	De 192.168.0.1 à 192.168.255.254

Tableau I.1: Classe et plage des adresses privée

Conclusion

L'initiation aux réseaux informatique nous a permis de comprendre le monde et l'intérêt des réseaux informatiques, notamment fonctionnalités, architecture et transmission de données

II. Préambule

Aujourd'hui, une entreprise peut occuper tout un immeuble et avoir plusieurs secteurs répartis dans chaque niveau de l'immeuble utilisant les mêmes ressources. On peut retrouver par exemple, le service finance au premier niveau, au troisième niveau et au dernier niveau de l'immeuble.

Étant dans le même réseau ses activités sont dispersées, pour pallier à cela, il y a la naissance des VLAN une technologie récente permettent d'appliquer plusieurs optimisations sur les réseaux locaux et ainsi faciliter le travail de l'administrateur. En premier lieu, nous allons voir quelques définitions des différents éléments qui feront l'objet de ce travail.

II.1 Définition

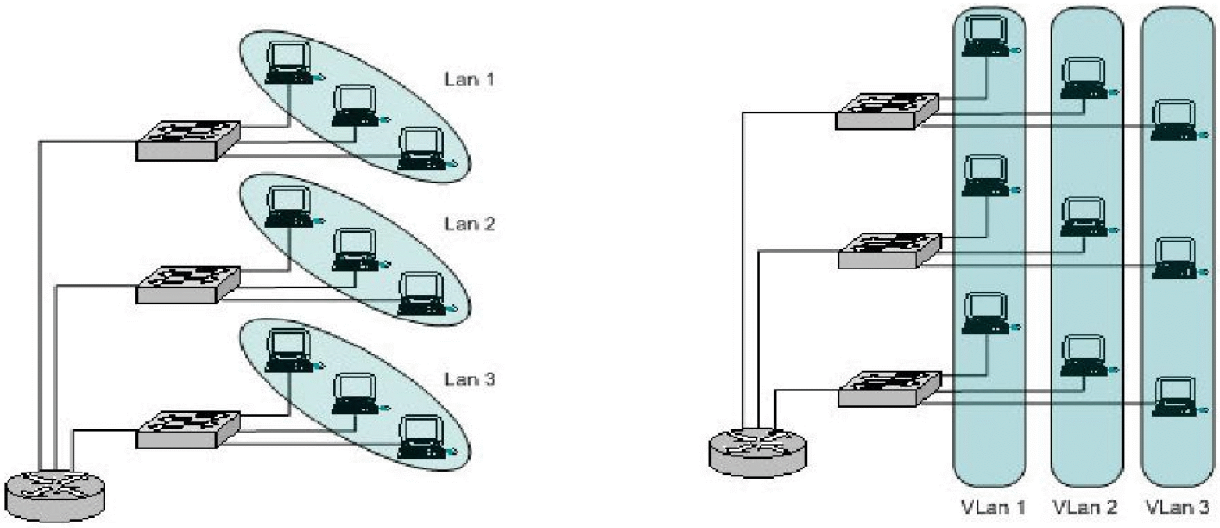
Un VLAN (Virtual Local Area Network) est un réseau local virtuel utilisant la technologie Ethernet pour regrouper les éléments du réseau (utilisateurs, périphériques, etc.) selon des critères logiques (fonction, partage de ressources, appartenance à un département, etc.), sans se heurter à des contraintes physiques (dispersion des ordinateurs, câblage informatique inapproprié, etc.)

- Les propriétés offertes par le VLAN sont :
  - support des transferts de données allant jusqu'à 1Gb/ .
  - peut couvrir un bâtiment, relier plusieurs bâtiments ou encore s'étendre au niveau d'un réseau plus large (WAN).
  - apporte des outils supplémentaires pour le renforcement de la sécurité.
  - une station peut appartenir a plusieurs VLAN simultanément. C'est un sous réseau de niveau 2 construit à partir d'une technologie permettant de cloisonner des réseaux par usage de filtres de sécurité. Cette technologie balise le domaine de broadcast auquel ces machines appartiennent de telle sorte que le trafic intra-domaine ne puisse pas être vu par des tiers n'appartenant pas à ce domaine de broadcast [5].

II.2 Principe

Le principe des VLAN consiste à regrouper des machines dans un ou plusieurs segments quelque sois leur emplacement physique. En fait, cette technologie permet de créer des segments Ethernet logiques, indépendamment de l'implantation géographique.

La mise en place des vlan nécessite l'utilisation d'équipement supportant cette technologie.



Segmentation traditionnelle **segmentation par VLAN**

Figure II.1 : Segmentation traditionnelle /par VLAN

Les principales différences entre la commutation traditionnelle et les VLAN sont :

- Les VLAN fonctionne au niveau des couche 2 et 3 du modèle OSI
- La commutation inter VLAN est assurée par le routage de couche 3
- Les VLAN fournissent une méthode de contrôle des broadcastas
- Les VLAN permettent d'effectuer une segmentation selon certains critères
    - Des collègues travaillant dans le même service
    - Une équipe partageant le même applicatif
- Les VLAN peuvent assure la sécurité des réseaux en définissant quels nœuds réseaux peuvent communiquer entre eux.
- Il est possible alors de segmenter le réseau en plusieurs domaines de broadcaste afin d'en améliore les performances.
- La communication inter VLAN est assure par des routeurs [6].

II.3 Création DES VLAN :

Il existe deux méthodes d'appartenance au VLAN

II.3.1 statiques:

Dans un VLAN statique, l'administrateur réseau crée un VLAN puis attribue des ports de commutation au VLAN. Les VLAN statiques sont également appelés VLAN basés sur les ports. L'association avec le VLAN ne change pas jusqu'à ce que l'administrateur modifie l'affectation des ports et Les périphériques utilisateurs finaux deviennent les membres du VLAN en fonction du port de commutateur physique auquel ils sont connectés.

Les ports sur un seul commutateur peuvent recevoir plusieurs VLAN. Bien que deux périphériques soient connectés à différents ports sur un même commutateur, le trafic ne passera pas entre eux si les ports connectés se trouvent sur des VLAN différents donc nous avons besoin d'un périphérique de couche 3 (généralement un routeur) pour permettre la communication entre deux VLAN.

II.3.2 dynamiques:

Dans un VLAN dynamique, le commutateur attribue automatiquement le port à un VLAN en utilisant des informations du périphérique utilisateur comme adresse MAC, adresse IP, etc. Lorsqu'un périphérique est connecté à un port de commutateur, le commutateur interroge une base de données pour établir l'appartenance au VLAN. Un administrateur réseau doit configurer la base de données VLAN d'un serveur de stratégie d'appartenance VLAN (VMPS).

Les VLAN dynamiques supportent la mobilité instantanée des périphériques finaux. Lorsque nous déplaçons un périphérique d'un port sur un commutateur vers un port sur un autre commutateur, les VLAN dynamiques configureront automatiquement l'appartenance au VLAN [5].

II.4 Classification des ports de commutateur

Les ports de commutateur peuvent être configurés pour jouer deux rôles différents. Un port est classé comme port d'accès ou comme port agrégé.

II.4.1 Port d'accès :

Un port d'accès appartient à un seul réseau local virtuel. En général, des périphériques uniques tels que des PC ou des serveurs se connectent à ce type de port. Si un concentrateur

connecte plusieurs PC à un port d'accès unique, chaque périphérique connecté au concentrateur est un membre du même réseau local virtuel.

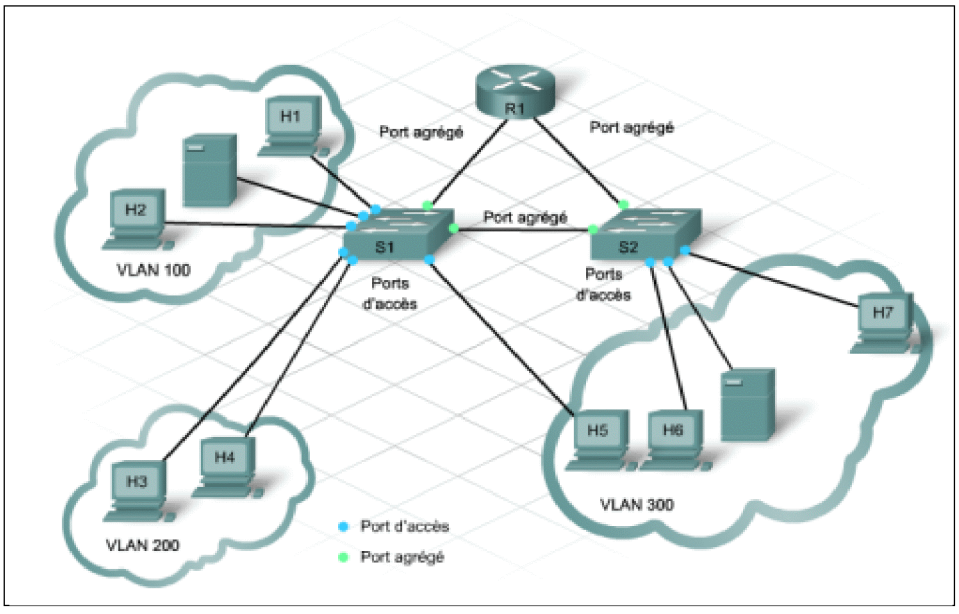
II.4.2 Port agrégé :

Un port agrégé est une liaison point à point entre le commutateur et un autre périphérique réseau. Les agrégations transportent le trafic provenant de plusieurs réseaux locaux virtuels via une liaison unique et permettent à chaque réseau local virtuel d'atteindre l'intégralité d'un réseau.

Les ports agrégés sont nécessaires à l'acheminement entre des périphériques de trafic provenant de plusieurs réseaux locaux virtuels, lors de la connexion de deux commutateurs, d'un commutateur et d'un routeur, ou d'une carte réseau hôte prenant en charge l'agrégation

En l'absence de port agrégé, chaque réseau local virtuel requiert une connexion distincte entre les commutateurs. Par exemple, une entreprise qui possède 100 réseaux locaux virtuels requiert 100 liaisons de connexion. Ce type de configuration n'est pas très évolutif et coûte très cher.

✓ Les liaisons agrégées offre une solution à ce problème en transportant du trafic provenant de plusieurs réseaux locaux virtuels sur la même liaison [7] .



Figeur II.2 : port d'acces / port agrégé

II.5 Typologie des VLAN

Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue :

II.5.1 Un VLAN de niveau 1 (aussi appelés VLAN par port, en anglais Port-Based VLAN)

Définit un réseau virtuel en fonction des ports de raccordement sur le commutateur. Les ports des Switch sont associés à des VLAN.

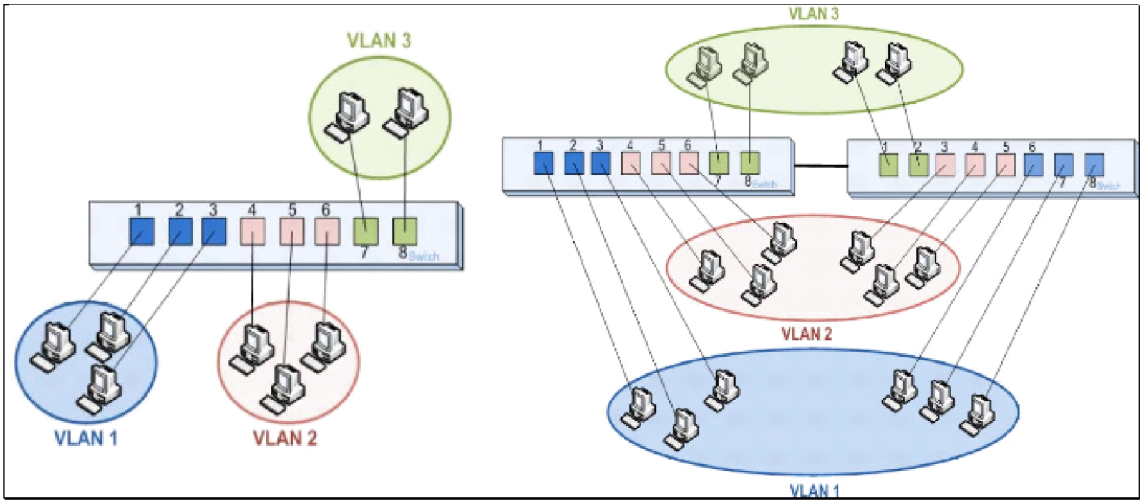


Figure II.3 : VLAN par ports.

II.5.2 Un VLAN de niveau 2 (également appelé VLAN MAC, ou en anglais MAC Address-Based VLAN)

Consiste à définir un réseau virtuel en fonction des adresses MAC des stations. Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station.

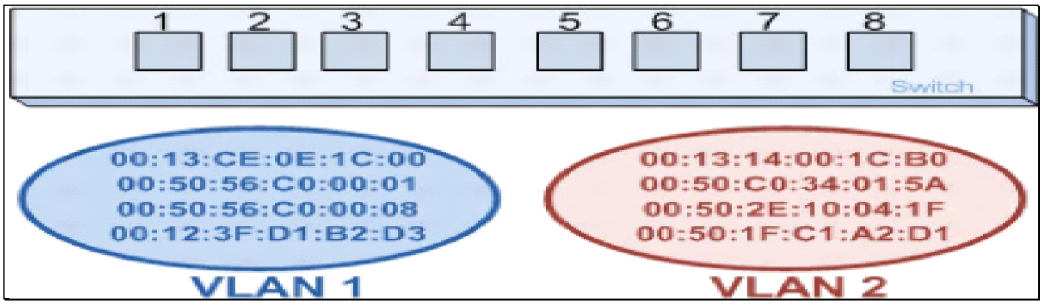


Figure II.4 : Les VLAN par adresse MAC

II.5.3 Un VLAN de niveau 3

On distingue plusieurs types de VLAN de niveau 3 :

II.5.3.1 Le VLAN par sous-réseau (en anglais Network Adresse-Based VLAN)

Associe des sous-réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de déplacement d'une station. En contre partie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.

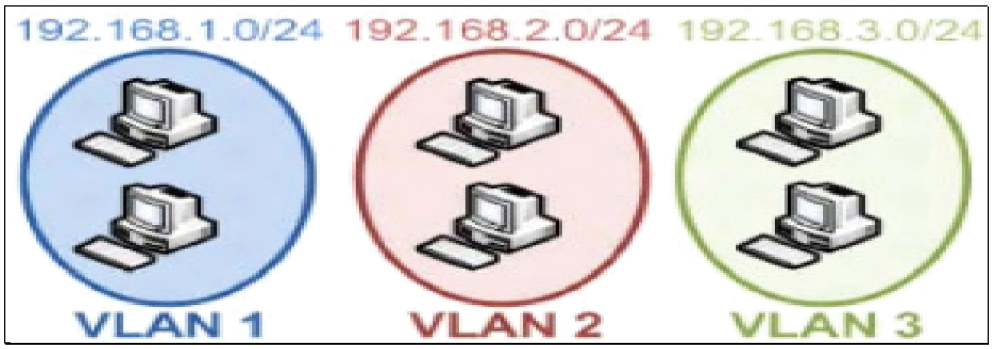


Figure II.5 : VLAN par sous réseau

II.5.3.2 Le VLAN par protocole (en anglais Protocol-Based VLAN)

Permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau [5].

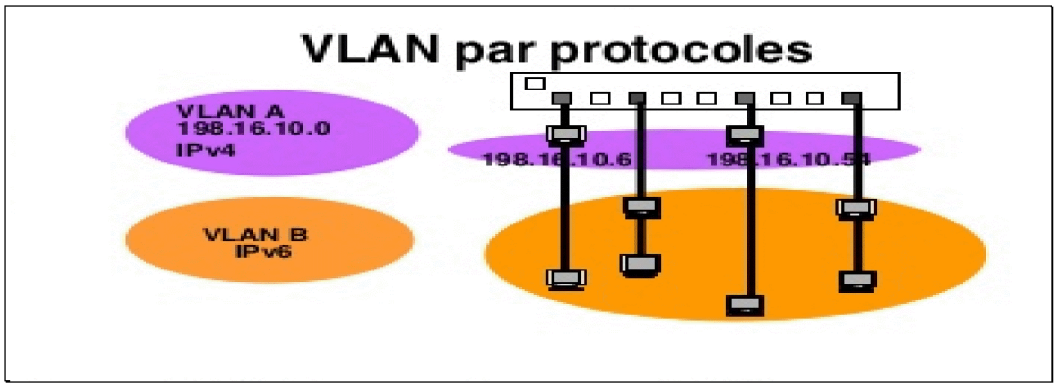


Figure II.6 : VLAN par protocole

II.6 Avantages des VLAN

Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants :

• **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 :** 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.

• **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 [8].

II.7 Interconnections entre VLAN

Les VLAN étant au niveau 2 du modèle OSI, l'interconnexion entre deux VLAN ne peut s'effectuer que par l'intermédiaire d'une passerelle de niveau trois. Il est donc nécessaire de réaliser du routage entre deux VLAN au même titre qu'entre deux réseaux Ethernet. Ce routage est réalisé entre des interfaces virtuelles (une par VLAN) de la même manière qu'il serait réalisé entre des interfaces physiques.

Pour router les trames entre deux VLAN, les routeurs doivent pouvoir les dé taggues puis les tagguer à nouveau avec le bon VID.

Généralement les routeurs d'aujourd'hui permettent d'associer un même VLAN à plusieurs interfaces physique. Les routeurs réalisent alors une commutation entre leurs interfaces appartenant au même réseau virtuel (dans le cadre d'un même VLAN il n'y a à priori pas de routage).

II.8 Routage

Le routage est la tâche consistant à trouver un chemin d'un émetteur à une destination souhaitée. Il se réduit essentiellement à trouver des routeurs entre des réseaux, Aussi longtemps qu'un message reste sur un réseau ou sous-réseau unique, tout problème de routage est résolu par une technologie qui est spécifique au réseau. Le routage IP entre en jeu essentiellement quand les messages doivent aller d'un émetteur sur un tel réseau vers une destination située sur un autre réseau. Dans ce cas, le message doit traverser des routeurs connectant les réseaux. Si les réseaux ne sont pas adjacents, le message peut traverser plusieurs réseaux intermédiaires, et les routeurs les connectant. Une fois que le message arrive sur un routeur situé sur le même réseau que la destination, la technologie propre de ce réseau est utilisée pour atteindre la destination.

II.8.1 Types de Routage :

II.8.1.1 Routage Statique

L'administrateur réseau spécifie manuellement la table de routage

– **Inconvénients :** l'administrateur doit faire les mises à jour en cas de changement de la topologie du réseau

– **Avantages :** réduction de la charge du système, car aucune mise à jour de routage n'est envoyée.

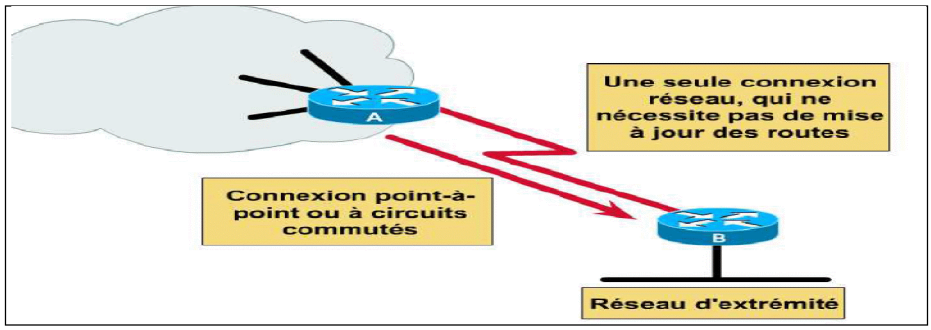


Figure II.7 : Routage statique

II.8.1.2 Routage dynamique

Le routage dynamique est assuré par les routeurs eux- même en s'échangeant des informations sur leurs tables de routage (nécessité d'un protocole de routage).

– **Inconvénients :** augmentation de la charge du système, car des mises à jour de routage doivent êtres envoyées

- **Avantages :** prise en compte automatique d'un changement de la topologie du réseau, Simplicité de la configuration.

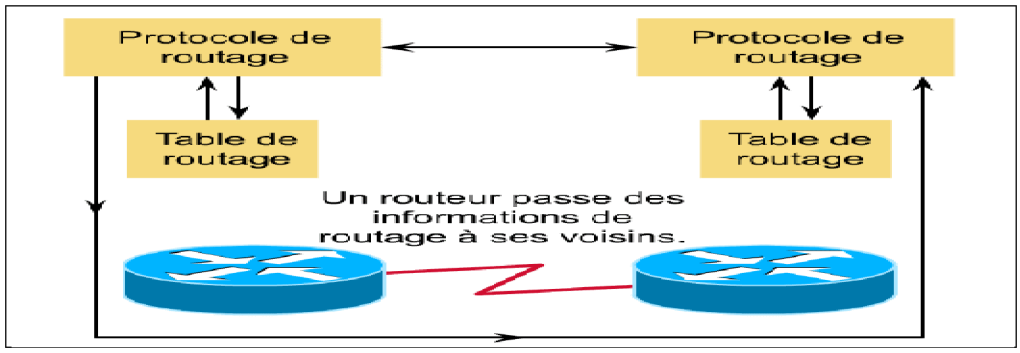


Figure II.8: routage dynamique

II.9 Routage inter-VLAN

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.

Le routage inter-VLAN existant (routage traditionnels) dépendait généralement de la disponibilité d'un port de routeur physique pour chaque VLAN configuré. Le routeur doit posséder plusieurs interfaces physiques et chaque interface est connectée à un VLAN déférent.

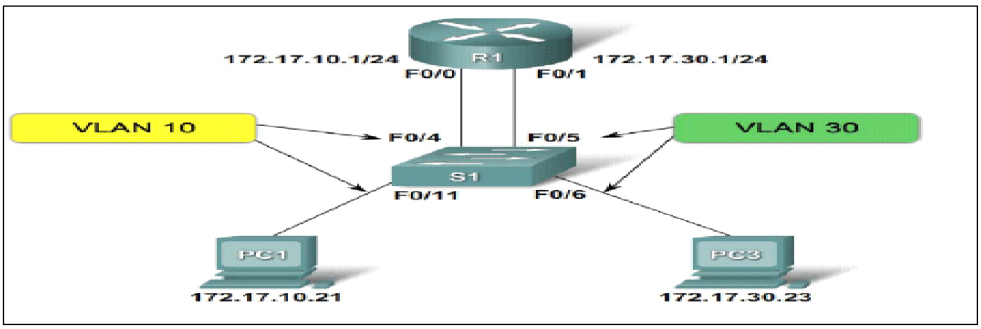


Figure II.9 : Le routage inter-VLAN traditionnel

Il a été remplacé par la topologie router-on-a-stick (une seule interface physique, plusieurs sous-interfaces logiques). Qui repose sur un routeur externe avec des sous-interfaces en trunk avec un commutateur de couche 2.Avec l'option router-on-a-stick, l'adressage IP et les informations VLAN appropriés doivent être configurés sur chaque sous-interface logique et une encapsulation de trunk doit être configurée pour correspondre à celle

de l'interface de trunking du commutateur. Le routeur posséder donc d'autant d'interface logique qu'il existe de vlan a interconnecter.

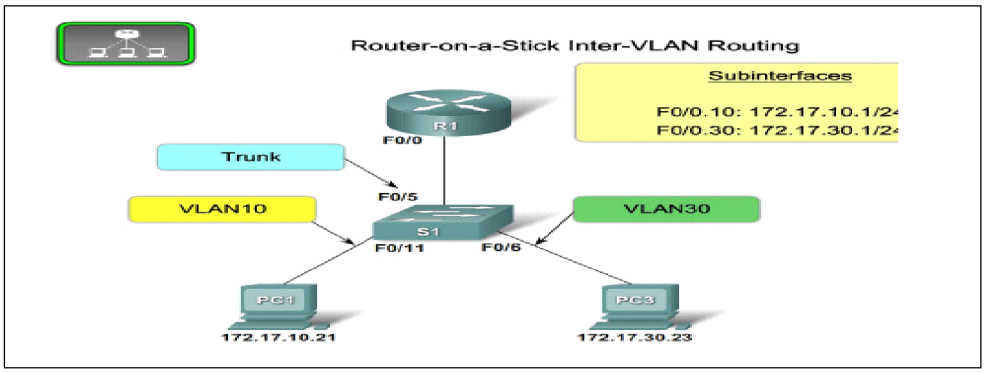


Figure II.10 : Le routage inter-VLAN (Router-on –sticks)

- **Avantages et Inconvénients des deux techniques du routage inter-vlan**

Routage inter-VLAN traditionnel	**Routage inter-VLAN (Router-on -sticks)**
Une interface physique par vlan	une interface physique pour de nombreux vlan
Aucun conflit de bande passante	Conflit de bande passante
Connectée au port de commutateur en mode d'accès	Connectée au port de commutateur en mode d'agrégation
Plus couteuse en termes de port	Moins couteuse en termes de port
Configuration de connexion plus complexe	Configuration de connexion moins complexe

Tableau II.1 : Avantage et Inconvénient de Routage inter-VLAN

Une autre possibilité consiste en une option inter-VLAN multicouche utilisant la commutation de couche 3. La commutation de couche 3 englobe les interfaces SVI et les ports routés. La commutation de couche 3 est généralement configurée au niveau de la couche de distribution et de la couche cœur de réseau du modèle de conception hiérarchique. La commutation de couche 3 avec des interfaces SVI est une forme de routage inter-VLAN. Un port routé est un port physique qui fait office d'interface sur un routeur. Contrairement à un port d'accès, un port routé n'est pas associé à un VLAN spécifique [5].

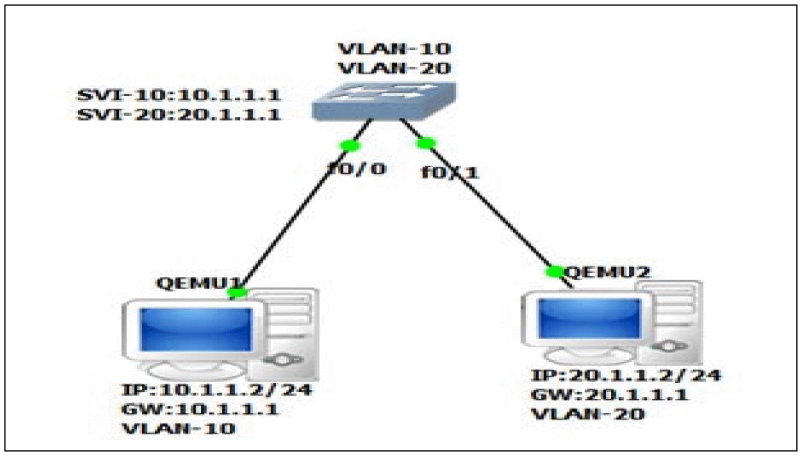


Figure II.11 : Le routage inter-VLAN avec SVI

II.10 DTP (Dynamique trunk protocol)

DTP (Dynamic trunk protocole) est un protocole réseau propriétaire de Cisco Systèmes donc ne fonctionne qu'entre Switch Cisco, permettant de gérer dynamiquement l'activation/désactivation du mode trunk d'un port sur un commutateur réseau.

Le principe est très simple, lorsqu'un port monte, des annonces DTP sont envoyées :

- si le port est connecté à un Switch voisin, ce dernier va recevoir l'annonce DTP et y répondre. Des deux côtés, l'activation du Trunk s'effectue.
- si le port est connecté à un PC, ce dernier ne répondra pas à l'annonce car il ne comprend pas le protocole. Sur le port du Switch, le Trunk n'est pas activé et donc reste en mode Access.

II.10.1 Fonctionnement

Un port physique d'un Switch peut avoir plusieurs état (ou mode) concernant le DTP. Ces états sont très importants à connaitre car selon le modèle de switch , l'état par défaut n'est pas le même.

Mode	Fonction
Dynamic Desirable	Annonce sa volonté de monter en trunk (négociation)
Dynamic Auto	Attends une sollicitation du voisin. Il n'envoie pas de requêtes mais répond aux requêtes d'en face
Trunk (on)	Le switch se met en mode trunk automatiquement et en informe le switch voisin
Nonegotiate	Le switch se met en mode trunk automatiquement sans en informer le switch voisin
Off	Désactivation du Trunk
Access	Désactivation du Trunk et prévient le voisin

Tableau II.2 : les déférents modes de port physique

le port "souhaite, "impose" ou "interdit" de monter un trunk , tout est une question de négociation avec son voisin. les différentes possibilités sont présenter dans (le tableau II.2).

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	?
Access	Access	Access	?	Access

Tableau II.3 : les déférentes négociations entre les ports

"?" Sont les cas où le comportement des 2 Switch est incertain car la configuration est incohérente: d'un côté on configure le port en Access et de l'autre en Trunk donc ça ne fonctionnera pas [7].

II.11 VTP (VLAN Trunking protocol)

Le protocole de jonction VLAN (VTP) réduit la gestion dans un réseau commuté. Quand vous configurez un nouveau VLAN sur un serveur VTP, le VLAN est distribué par tous les commutateurs dans le domaine. Ceci réduit la nécessité de configurer le même VLAN partout. VTP est un protocole propriétaire de Cisco qui est disponible sur la plupart des produits de la gamme Cisco Catalyst. Il fonctionne avec une architecture client/ serveur.

II.11.1 Le mode de fonctionnement

Le serveur tient à jour une table de VLAN déclarés. Cette table est diffusée à l'ensemble des clients étant sur le même domaine VTP. De ce fait chaque modification de la table est répercutée à l'ensemble des clients. Ainsi tous les VLAN définis sur le serveur pourront transiter par l'ensemble des ports trunk des switchs clients (sauf configuration contraire sur les interfaces).

II.11.2 Les modes de VTP (vlan trunk protocole)

Les dispositifs de VTP peuvent être configurés pour fonctionner suivant les trois modes suivants :

1) le mode serveur :

- Il défini le nom de domaine VTP.
- Il peut ajouter, modifier ou supprimer un Vlan.
- Il tient à jour la liste des VLAN déclarés et la diffuse à l'ensemble des clients.

2) le mode client VTP :

- Il possède un nom de domaine,
- Il reçoit la liste des VLAN il la propage aux autres clients auxquels il est connecté et met à jour sa propre liste.

3) le mode transparent :

- Ill ne participe pas aux domaines VTP du réseau.
- Il transmet les paquets VTP via ses liens trunk.
- Il possède sa propre liste de Vlan qu'il est possible de modifier.

Si une des conditions suivantes n'est pas respectée, le domaine de VTP ne sera pas valide et l'information ne se propagera pas:

- Il faut donc assigner le même nom de domaine de VTP à chaque commutateur.
- l'option trunk pour l'interconnexion des commutateurs doit être activée [9].

II. 12 ACL (Acess control List)

Une ACL (Access Control List) est une listes de règle permettant de filtrer les paquets en fonction de critères définis par l'utilisateur comme l'adresse IP source ,IP destination, port source, port destination . Ces ACL peuvent êtres appliquées en entrée ou en sortie d'une interface de routeur, de manière à filtrer les paquets entrants et/ou sortants.

L'ACL est composée d'une liste d'ACE (Access Control Entry), ces ACE vont être interprétées de manières séquentielles c'est-à-dire, lorsqu'un paquet arrivera sur l'interface du routeur où nous avons configuré notre ACL celui-ci va regarder la première ACE si celle-ci correspond au trafic qu'il analyse, il va appliquer ce qui est décrit dans l'ACE, si la première ACE ne correspond pas au trafic il va regarder la seconde et ainsi de suite jusqu'à trouver une correspondance. S'il ne trouve aucune correspondance le paquet sera supprimée, en effet lors de la création d'une ACL tout ceux qui n'est pas directement autorisés dans l'ACL est interdit.

II.12.1 Les Type D'ACL :

On distingue deux types d'ACL parmi lesquelles :

II.12.1.1 Les ACL standards : Les ACL standards sont numérotées de 1-99, elles se basent sur les adresses IP de source pour savoir quel paquet filtrer, elles doivent être placées au plus près de la destination.

II.12.1.2 Les ACL étendues : Contrairement au ACL standard les ACL étendues ne se reposent pas uniquement sur l'adresse IP source, mais sur plusieurs champs de l'en-tête IP et les protocoles utilisés. Les ACL étendues se placent au plus proche de la source (afin d'éviter de gaspiller de la bande passante en envoyant sur le réseau des paquets qui seront supprimées une fois arriver à destination.). Les ACL étendues sont numérotées de 100 à 199[7].

II. 13 Protocole DHCP (Dynamic Host Configuration Protocol)

Le protocole DHCP (Dynamics Host Configuration Protocol) est une extension de protocoles BOOTP qui as été conçu pour assurer la configuration des stations de travail sans disque .Le protocole DHCP fournit une configuration dynamique des adresses IP et des informations associées aux ordinateurs configurés pour l'utiliser (clients DHCP). Ainsi chaque hôte du réseau obtient une configuration IP dynamiquement au moment du démarrage, auprès du serveur DHCP. Le serveur DHCP lui attribuera notamment une adresse IP, un masque et éventuellement l'adresse d'une passerelle par défaut. Il peut attribuer beaucoup d'autres paramètres IP notamment en matière de noms (l'adresse des serveurs DNS, l'adresse des serveurs WINS).

II.13.1 Les mécanismes d'allocation d'adresses IP par DHCP

Le protocole DHCP comprend trois mécanismes d'allocation d'adresses, offrant ainsi de la souplesse lors de l'attribution d'adresses IP :

II.13.1.1 Allocation manuelle : l'administrateur attribue une adresse IP pré allouée au client et le protocole DHCP communique uniquement l'adresse IP au périphérique.

II.13.1.2 Allocation automatique : Le protocole DHCP attribue de façon automatique et permanente une adresse IP statique à un périphérique en sélectionnant cette adresse dans un pool d'adresses disponibles. Il n'y a pas de bail et l'adresse est attribuée de façon permanente au périphérique.

II.13.1.3 Allocation dynamique : le protocole DHCP attribue, ou loue, de façon automatique et dynamique une adresse IP à partir d'un pool d'adresses pour une durée limitée définie par le serveur ou jusqu'à ce que le client indique au serveur DHCP qu'il n'a plus besoin de cette adresse.

II.13.2 Rôle d'un service DHCP

Un serveur DHCP ou (service DHCP) (Dynamic Host Configuration Protocol) est un serveur ou (service) a pour rôle de distribuer des adresses IP à des clients pour une durée déterminée.

Au lieu d'affecter manuellement à chaque hôte une adresse statique, ainsi que tous les paramètres tels que (serveur de noms, passerelle par défaut, nom du réseau), un serveur DHCP alloue à un client, un bail d'accès au réseau, pour une durée déterminée (durée du bail). Le serveur passe en paramètres au client toutes les informations dont il a besoin [5].

II.13.3 Les requêtes et les messages DHCP

On pourrait croire qu'un seul aller-retour peut suffire à la bonne marche du protocole. En fait, il existe plusieurs messages DHCP qui permettent de compléter une configuration, la renouveler... Ces messages sont susceptibles d'être émis soit par le client pour le ou les serveurs, soit par le serveur vers un client (Tableau II.3):

Nom de requête	Description
DHCPDISCOVER (1)	Pour localiser les serveurs DHCP disponibles et demander une première configuration
DHCPOFFER (2)	réponse du serveur a un message DHCPDISCOVER, qui contient les premiers paramètres
DHCPREQUEST (3)	requête diverse du client pour par exemple prolonger son bail
DHCPDECLINE (4)	Le client annonce au serveur que l'adresse est déjà utilisée
DHCPPACK (5)	réponse du serveur qui contient des paramètres et l'adresse IP du client
DHCPNAK (6)	Réponse du serveur pour signaler au le client que son bail est échu ou si le client annonce une mauvaise configuration réseau
DHCPRELEASE (7)	Le client libère son adresse IP
DHCPINFORM (8)	Le client demande des paramètres locaux, il a déjà son adresse IP

Tableau II.4 les différents messages utilisé entre serveur et le client

II.13.4 Fonctionnement de DHCP

Lorsqu'un client DHCP (ordinateur demande une adresse IP à un serveur) initialise un accès à un réseau TCP/IP, le processus d'obtention du bail IP se déroule en 4 phases.

1 - Le client émet un message de demande de bail IP DHCPDISCOVER (qui est envoyé sous forme d'une diffusion sur le réseau avec adresse IP source 0.0.0.0 et adresse IP destination 255.255.255.255 et adresse MAC).

2 - Les serveurs DHCP répondent en proposant une adresse IP avec une durée de bail et l'adresse IP du serveur DHCP (DHCOFFER)

3 - Le client sélectionne la première adresse IP (s'il y a plusieurs serveurs DHCP) reçue et envoie une demande d'utilisation de cette adresse au serveur DHCP (DHCPREQUEST). Son message envoyé par diffusion comporte l'identification du serveur sélectionné qui est informé que son offre a été retenue ; tous les autres serveurs DHCP retirent leur offre et les adresses proposée redeviennent disponibles.

4 - Le serveur qui reçoit la demande DHCPREQUEST officialise la configuration en envoyant un accusé de réception en unicast, le (DHCPACK) . Il est possible, mais hautement improbable, que le serveur n'envoie pas le DHCPACK. Ceci peut se produire si le serveur a concédé ces informations à un autre client entre temps. Dès qu'il reçoit le message (DHCPACK), le client peut commencer à utiliser l'adresse attribuée.

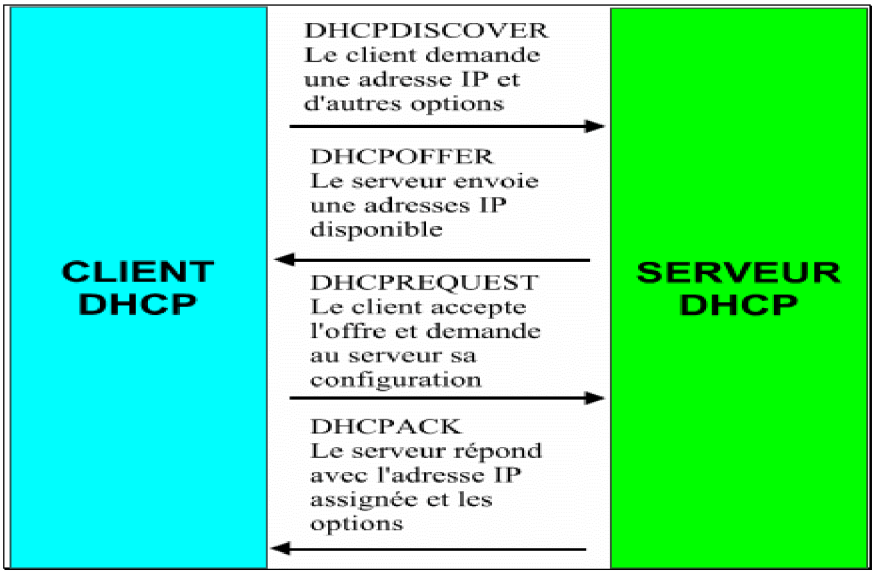


Figure II.12 : Schéma résume le fonctionnement de DHCP

- Si le client détecte que l'adresse est en cours d'utilisation sur le segment local, il envoie un message DHCPDECLINE et le processus recommence. Si le client a reçu un DHCPNACK du serveur après avoir envoyé le DHCPREQUEST, il recommence tout le processus.
- Si le client n'a plus besoin de l'adresse IP, il envoie un message DHCPRELEASE au serveur.

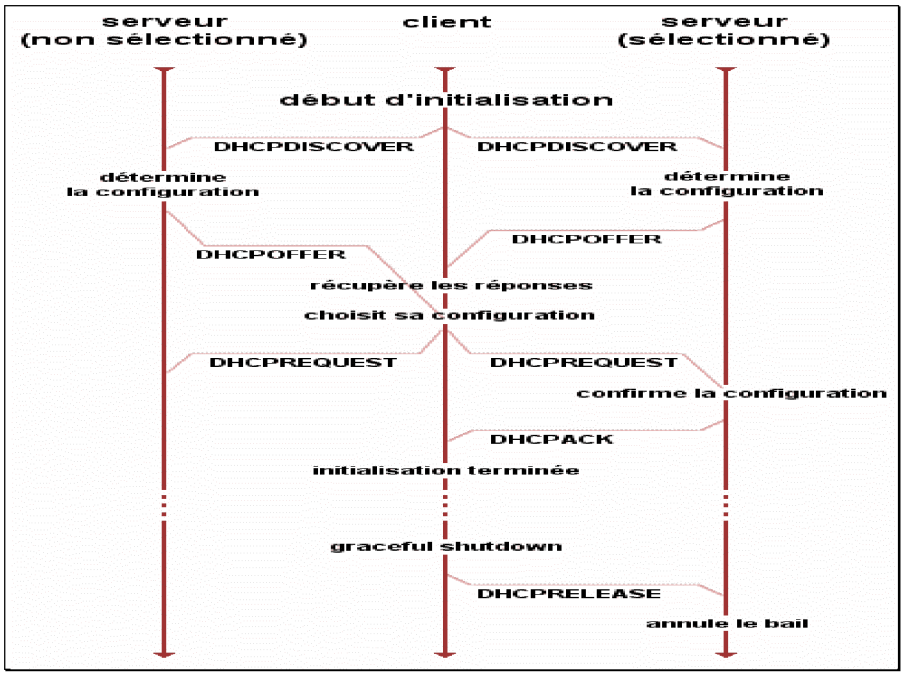


Figure II.13: Chronogramme résume la communication client /serveur

II.13.5 Avantages de DHCP dans l'administration d'un réseau

- Le protocole DHCP offre une configuration de réseau TCP/IP fiable et simple, empêche les conflits d'adresses et permet de contrôler l'utilisation des adresses IP de façon centralisée. Ainsi, si un paramètre change au niveau du réseau, comme, par exemple l'adresse de la passerelle par défaut, il suffit de changer la valeur du paramètre au niveau du serveur DHCP, pour que toutes les stations aient une prise en compte du nouveau paramètre dès que le bail sera renouvelé. Dans le cas de l'adressage statique, il faudrait manuellement reconfigurer toutes les machines.
- économie d'adresse : ce protocole est presque toujours utilisé par les fournisseurs d'accès Internet qui disposent d'un nombre d'adresses limité. Ainsi grâce à DHCP, seules les machines connectées en ligne ont une adresse IP. En effet, imaginons un fournisseur d'accès qui a plus de 1000 clients. Il lui faudrait 5 réseaux de classe C, s'il voulait donner à

chaque client une adresse IP particulière. S'il se dit que chaque client utilise en moyenne un temps de connexion de 10 mn par jour, il peut s'en sortir avec une seule classe C, en attribuant, ce que l'on pourrait appeler des "jetons d'accès" en fonction des besoins des clients.

- Les postes itinérants sont plus faciles à gérer.
- Le changement de plan d'adressage se trouve facilité par le dynamisme d'attribution [10].

Conclusions

A travers ce chapitre on a présenté des Notions sur les réseaux locaux virtuels (VLAN) et les protocoles. Les VLAN sont des configurations essentielles dans un réseau d'entreprise.

La technologie VLAN offre de nombreux avantages aux administrateurs réseaux. Les VLAN permettent notamment de contrôler les broadcasts de couche 3 ; ils améliorent la sécurité du réseau et facilitent le regroupement logique des utilisateurs du réseau.

La configuration et la mise à jour manuelle du protocole VTP (VLANTrunking Protocol) sur de nombreux commutateurs est un vrai défi. VTP présente un avantage, une fois qu'un réseau a été configuré avec VTP, la plupart des tâches de configuration VLAN sont automatiques [8]. Le prochain chapitre sera consacré à concevoir notre architecture d'interconnexion.

III. Préambule :

La conception est l'une des étapes essentielles permettant d'assurer la rapidité et la stabilité d'un réseau. Si un réseau n'est pas conçu adéquatement, de nombreux problèmes imprévus peuvent survenir, ce qui peut entraver son fonctionnement. La conception est véritablement un processus en profondeur. Dans ce chapitre nous allons concevoir l'architecteur d'interconnexion de l'entreprise.

III.1 Présentation du modèle :

Le but de notre travail est de simuler et configurer un réseau d'entreprise constitué de deux sites. Un site à Tizi-Ouzou et un autre site se trouve à Alger.

Chaque sites dispose de :

- Départements FINANCE
- Départements COMPTABILITE
- Départements LOGISTIQUE
- Voix IP (propose a l'entreprise)
- Connections internet sécuriser

Notre réseau est segmenté de telle sorte à avoir un département par Vlan. Chaque département se trouvera sur un Vlan différent afin de segmenter au mieux notre réseau, d'en faciliter l'administration, gérer la bande passante et d'augmenter la sécurité.

Chaque départements sera brancher sur un switch et ainsi tous les Switchers seront branche sur le même multi layer Switch et Routeur (de même pour le site d'ALG).

III.2 Présentation Des équipements Utilisés

Les équipements réseaux utilisés sont présentés dans, le tableau III.1.

Equipement	Types	Nombre
Router	2811	2 (site TZO, sites ALG)
Multilayer Switch	3560-24PS	2 (site TZO, sites ALG)
Switch	2950-24	8 (4 site TZO, 4 site ALG)

Téléphone	IP- Telephone	16 (8 site TZO ,8 site ALG)
PC	PC-PT	4 (2 site TZO, 2 site ALG)
Laptot	Laptot-PT	12 (6 site TZO, 6 site ALG)

Tableau III.1 : Liste des équipements utilise dans les deux sites

III.3 Nomination Des VLAN et Adressage

Les VLAN sur le Routeur de site TZO seront nommées dans la configuration comme suite

Nom de VLAN	ID VLAN	Adresse Réseau	Masque Réseau	Passerelle
Finance	10	10.10.10.0	255.255.255.0	10.10.10.1
Comptabilite	20	20.20.20.0	255.255.255.0	20.20.20.1
Logistique	30	30.30.30.0	255.255.255.0	30.30.30.1
VoIP	11	11.11.11.0	255.255.255.0	11.11.11.1

Tableau III.2 : Les VLAN du site TZO

Les VLAN sur Routeur de site ALG seront nommées dans la configuration comme suite :

Nom de VLAN	ID VLAN	Adresse Réseau	Masque Réseau	Passerelle
finance	110	110.110.110.0	255.255.255.0	110.110.110.1
comptabilite	120	120.120.120.0	255.255.255.0	120.120.120.1
logistique	130	130.130.130.0	255.255.255.0	130.130.130.1
VoIP	111	111.111.111.0	255.255.255.0	111.111.111.1

Tableau III.3 : Les VLAN du site ALG

III.4 Nomination Des équipements

III.4.1 Nomination Des équipements d'interconnections

Les équipements d'interconnections dans les sites distants seront nommées comme suit (Tableau III.4)

Sites distants	
Site TZO	Site ALG
Router (TZO)	Router (ALG)
Multilayer Switch (DSL_Tizi)	Multiayer Switch (DSL_ALG)
Switch (FINANCE_Tizi)	Switch (FINANCE_ALG)
Switch (COPMT_Tizi)	Switch (COMPT_ALG)
Switch (LOG_Tizi)	Switch (LOG_ALG)
Switch(MAGASIN)	Switch (MAGASIN LOG_ALG)

Tableau III.4 : Les équipements d'interconnections

III.4.2 Nomination d'Hôte

Les hôtes dans les sites distants seront nommées comme suite (Tableau III.5)

Sites distant			
Site TZO		Sites ALG	
Nom d'hôtes	Vlan ID	Nom d'hôtes	Vlan ID
Laptop0	10	LAPTOP0	110
Laptop1	10	LAPTOP1	110
Laptop2	20	LAPTOP2	120
Laptop3	20	LAPTOP3	120

Laptop4	30	LAPTOP4	130
Laptop5	30	LAPTOP5	130
PC0	30	PC2	130
PC1	30	PC3	130

Tableau III.5 : Listes D'hôtes

III.4.3 Nomination des Téléphones IP

Le téléphone IP également appelée téléphonie Internet, est un mode de téléphonie utilisant le protocole de télécommunications crée pour Internet. Les téléphones IP dans les deux sites distants seront nommés comme suite (Tableau III.6).

Sites distant	
Sites TZO	Sites ALG
TEL:1501	TEL:1601
TEL:1502	TEL:1602
TEL:1503	TEL:1603
TEL:1504	TEL:1604
TEL:1505	TEL:1605
TEL:1506	TEL:1606

Tableau III.6 : Listes des téléphones IP

III.5 Configuration des ports trunk et accès

Les interfaces entre tous les Switch et routeurs sont configures en mode trunk pour qu'elles puissent transporter les informations des différentes Vlan. Les interfaces qui seront connectés à des postes de travail seront configurées en mode accès.

III.6 VTP

Le VTP est un protocole propriétaire Cisco permet de circuler les informations des VLAN Sur les différentes Switch sans avoir besoins de configurer les Vlan sur chaque Switch.

Nous allons configurer les Routeurs et Switch de deux sites distant en mode VTP client et serveur. Le tableau III.7 ci-dessous montre comment le VTP sera configuré dans les deux sites :

Site TZO			Site ALG		
VTP	Name	Mode	VTP	Name	Mode
Router	TZO	Server	Router	ALG	Server
Switch	DSL_Tizi	Client	Switch	DSL_ALG	Client
Switch	FINANCE_Tizi	Client	Switch	FINANCE_ALG	Client
Switch	COMPT_Tizi	Client	Switch	COMPT_ALG	Client
Switch	LOG_Tizi	Client	Switch	LOG_ALG	Client
Switch	MAGASIN	Client	Switch	MAGASIN LOG_ALG	Client

Tableau III.7 : VTP

III.7 Sécurité (ACL)

On va sécuriser notre réseau, en autorisant ou non (permit, deny) la connexion entre les d'efférents VLAN de deux sites distant. Pour cela, on va créer des règles que l'on va dicter au routeur (car c'est lui qui décide ou non de transmettre les paquets).

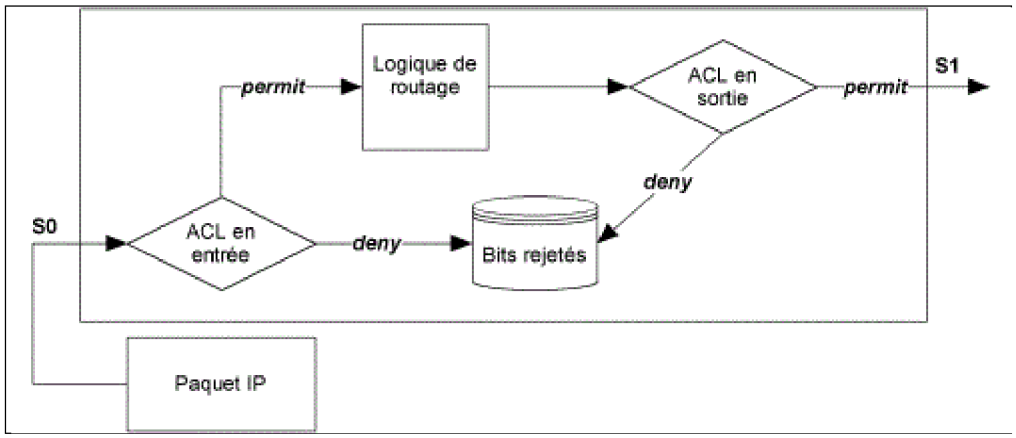


Figure III.1 : Règle de filtrage

Voici comment les Vlan auront le droit de se voir :

Site TZO / Site ALG	Finance	Comptabilite	Logistique	VoIP
Finance	OUI	NON	NON	OUI
Comptabilite	NON	OUI	NON	OUI
Logistique	NON	NON	OUI	OUI
VoIP	OUI	OUI	OUI	OUI

Tableau III.8 : Droit d'accès

III.8 Connectivité des sites distants

Les déférentes solutions que nous proposons pour interconnecter les deux sites distants de l'entreprise sont :

III.8.1 Liaisons spécialisées (ligne louée)

La Liaison spécialisée est une liaison permanente réservée à l'usage exclusif d'un utilisateur. Elle offre la possibilité de transmission entre deux points de terminaison déterminés du réseau public. Sa mise en place et son exploitation sont assurées par un opérateur de télécommunication (Algérie Telecom).

Les lignes louées ou spécialisées permettent la transmission de données de moyens a hauts débits (64 Kbps à 155Mbps).Algérie télécom propose généralement un débit de 2Mbit/s.

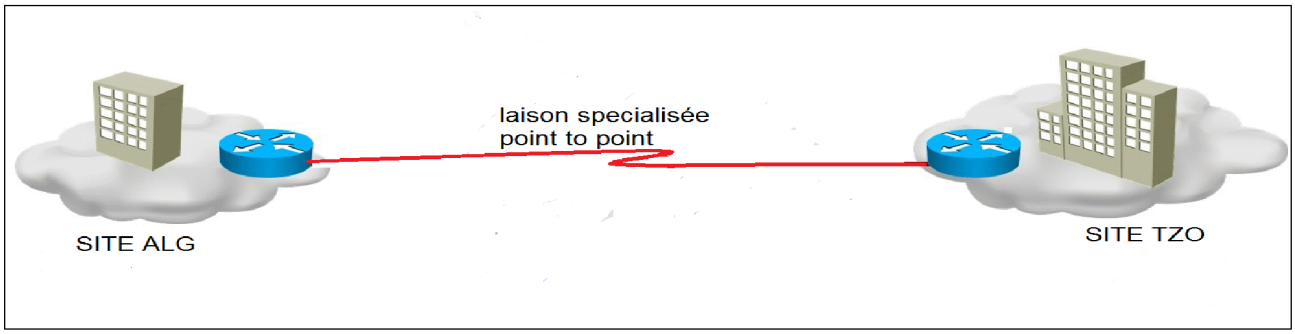


Figure III.2 : Interconnections par liaison spécialisée

❖ Les Avantages

- Un transfert rapide de données.
- Une plus grande sécurité dans les émissions/réceptions de données.
- Une communication fiable et de qualité
- La disposition d'une liaison permanente de manière exclusive évitant ainsi la saturation du réseau

❖ Les inconvénients

- Le coût des liaisons spécialisées peut être très élevé lorsqu'elles servent à connecter plusieurs sites [11]

III.8.2 La Fibre optique

La fibre optique est un support physique permettant la transmission de données à haut débit sous forme d'impulsions lumineuses modulées. Il existe deux catégories de fibre optique, la fibre optique monomode qui permet d'atteindre Un débit de100 Gb/s et la fibre optique multimode dont le débit est compris entre 20 et 500Mb/s. (pour interconnectés nos deux sites on utilise la fibre optique monomode) .

❖ Les Avantages

Les avantages de la fibre optique sont:

- Débit très élevé
- Transmission longue distance (dizaines voir centaines de km)
- Sécurité élevée
- Perte de signal sur une grande distance bien plus faible que lors d'une transmission

Électrique dans un conducteur métallique;

- Insensibilité aux interférences extérieures (proximité d'un câble à Haute tension par exemple).

❖ **Les Inconvénients**

Comme inconvénients, nous avons:

- Coût de déploiement élevé (prix du mètre et installation nécessitant des spécialistes dans le domaine)
- Maintenance difficile [12].

III.8.3 VPN (VIRTUAL PRIVATE NETWORK)

Le VPN est l'abréviation de Virtual Private Network ou Réseau Privé Virtuel. Le VPN dispose de la même fonctionnalité qu'un réseau prive (utilisant des lignes spécialisées) mais utilise Internet pour créer des lignes louées virtuelles qui passent par le réseau public. Un VPN permet le raccordement de travailleurs mobiles, l'interconnexion de sites distants. Il

est constitué de liaisons virtuelles sur Internet entre des sites distants appartenant à une même société ou à un même organisme. Les informations sont transmises à travers un « tunnel» crypté sur internet.

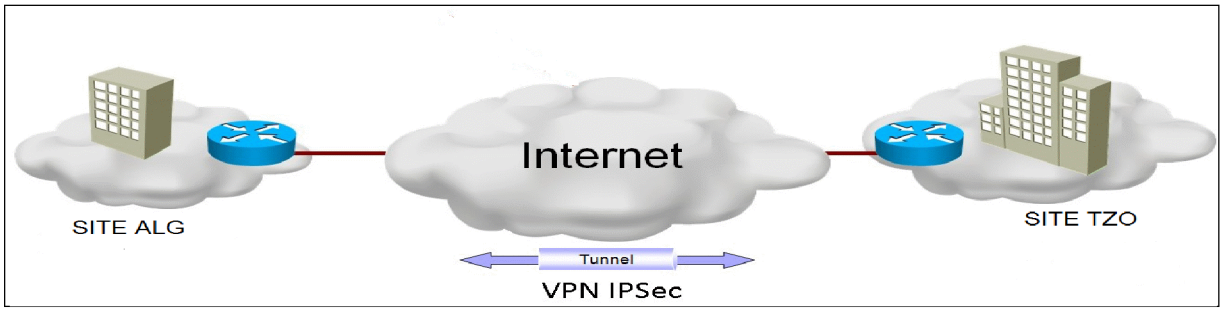


Figure III.3 : Interconnections par VPN

❖ Les Avantages

- La possibilité de réaliser des réseaux privés à moindre coût;
- La mise en œuvre d'un intranet étendu permettant à tous les utilisateurs d'accéder à distance à des ressources partagées, quelle que soit leur localisation géographique.

❖ Les Inconvénients

- Le Problème de sécurité lié au risque de piratage des données;
- La Disponibilité du réseau est liée à internet.

- Le VPN doit être établit entre chaque station. En effet une station ne possédant pas l'application VPN ne pourra pas communiquer avec les autres, et la sécurisation entre cette station et l'entrée du VPN ne sera pas activée. Pour les clients nomades, il faut installer un logiciel sur les pc portable et maintenir le parc à niveau de régulière. Il faut savoir plus le nombre de sites est important, plus la stabilité de la solution s'amoindrie et plus le VPN est lourd à déployer [12].

III.8.4 MPLS

La technologie MPLS consiste à doter les trames circulant sur le réseau d'une étiquette (label) servant à indiquer aux routeurs le chemin que la donnée doit emprunter.

Ces chemins peuvent être établis de façon manuelle (par un administrateur) ou de façon automatique (par un protocole de signalisation).

MPLS combine donc les principes du routage (IP) avec les principes de la commutation. Le routage du paquet se fait à l'entrée du nuage et la commutation se fait à l'intérieur du nuage.

Dans un réseau MPLS on définit 3 types de routeurs :

- **CE :** Customer Edge => routeur client

- **PE / LER :** Provider Edge / Label Edge Router => point d'entrée sur le réseau MPLS

- **LSR :** Label Switching Router => routeur de coeur de réseau

- **Nuage :** réseau MPLS

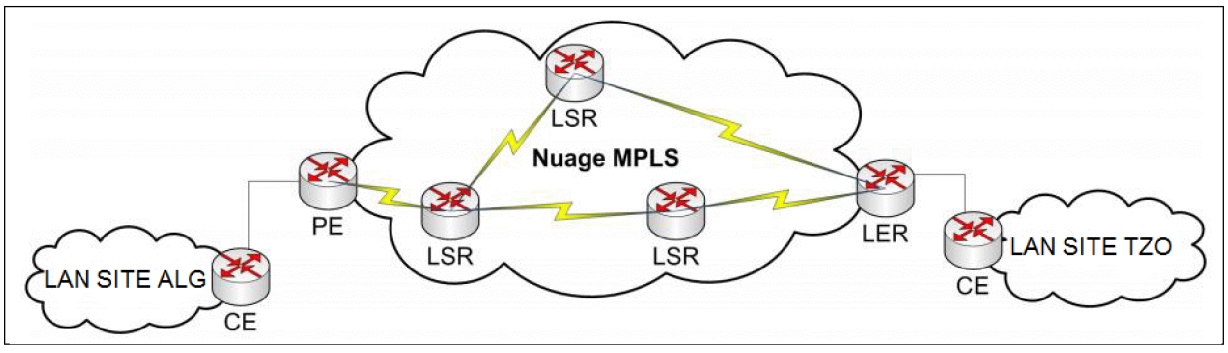


Figure III.4 : Interconnections par MPLS (RMS)

Le routeur d'entrée reçoit le paquet labellisé, il identifie le prochain saut (LSR suivant), il met à jour le label et l'envoie au nœud suivant.

❖ Avantages

- Production de profit
- Suivi de l'´evolution d'IP
- Souplesse
- Neutralité vis à vis des couches adjacentes
- Utilisation de l'existant
- Evolutivité
- Possibilité de mesures précises

❖ Les Inconvénients

- Manque d'homogénéité des équipements
- Sous dimensionnement des routeurs MPLS
- Difficulté à remplacer les réseaux existants
- Manque de fiabilité [12]

III.9 Tableau Comparatif des Solutions

Solution	**Fibre Optique**	**LS**	**VPN**	**MPLS**
Autonomie	Oui	NON	NON	NON
Débit	Jusqu'à 100 Gb/s pour la fibre monomode entre 20 et 500Mb/s pour la fibre Multimode	(64kbit/s, 155 Mbit/s)	Jusqu'à 50Mbits/s	(512 Kbits/s à 100 Mbits/s)
Sécurité	Sécurité élevée	Sécurité élevée	Selon les besoins, les protocoles L2TP, IPsec, SSL/TLS, et OpenVPN sont bien sécurisés	Sécurité garantie
Implémentation	Complexe	Facile	Facile	Facile
Durée d'implémentation	Très élevé	Peu élevée	Peu élevée	Peu élevée
Cout	Très élevé	Moyen	Moyen	Moyen

Tableau III.9 : Comparaison entre les déférentes solutions

Apres l'étude comparative notre choix s'est porter sur la Solution Liaison Spécialisée point à point.

III.10 Inter connexion LS

Les tableaux III.10 et III.11 indiquent la désignation des interfaces et l'adressage de LS.

Routeur	Interface série	Routeur	Interface série
Routeur Site TZO	Se0/0/0	Router Site ALG	Se0/0/0

Tableaux III.10 : Désignation de LS sur les interfaces de routeurs

Routeur	Interface	Adresse IP	Masque
Router Site TZO	Se 0/0/0	172.16.15.1	255.255.255.252
Router Site ALG	Se 0/0/0	172.16.15.2	255.255.255.252

Tableaux III.11: Adressage de LS

- **La table de routage**

Routeur	@ destination	Masque	Passerelle
Routeur Site TZO	0.0.0.0	0.0.0.0	172.16.15.2
Routeur Site ALG	0.0.0.0	0.0.0.0	172.16.15.1

Tableau III.12 : Table de routage

III.11 Protocole PPP :

Le protocole PPP fournit les connexions routeur à routeur et hôte à réseau sur les réseaux synchrones et asynchrones. Ce protocole PPP fonctionne avec différents protocoles de couche réseau, par exemple les protocoles IPv4 et IPv6. Le protocole PPP utilise le processus d'encapsulation HDLC, mais comporte également des mécanismes de sécurité intégrés, tels que PAP et CHAP.

Le protocole PPP établit la connexion directe à l'aide de câbles série, de lignes de téléphone, de lignes de raccordement, de téléphones cellulaires, de liaisons radio spécialisées ou de liaison fibre optique [7].

III.12 VoIP (Voice over Internet Protocol):

Est un nom générique définissant le transport de trafic Vocal au moyen de la transmission par paquets sur le protocole Internet, Le trafic VoIP peut être acheminé sur un réseau privé contrôlé ou le réseau Internet public Ou une combinaison des deux. Aussi VOIP peut définir comme une technologie de Communication vocale en pleine émergence. [7]

III.13 Discussion

Apres une étude des différentes solutions proposes, Notre choix s'est porté sur la Liaison Spécialisée point à point vu le nombre d'avantage qu'elle offre a l'entreprise telle que des débits de connexion symétriques, garantis en émission et en réception de données allant de 64 Kbps jusqu'à des dizaines de Mbps , la possibilité d'échanger de tous types de données et Toutes les communications sont sécurisées et offrent ainsi une fiabilité et une confidentialité totales.

IV. Préambule

Dans ce chapitre on va configurée notre architecture réseau en utilisant le simulateur « Cisco Packet Tracer Intructor », faire aussi les différentes tests et la validation de la configuration.

IV.1 Présentation de simulateur « Cisco Packet Tracer »

Le « Cisco Packet Tracer » est un programme puissant de simulation qui permet d'expérimenter le comportement du réseau. En effet, Packet Tracer fournit la simulation, la visualisation, la création, l'évaluation et les capacités de collaboration et facilite l'enseignement et l'apprentissage des technologies complexes.

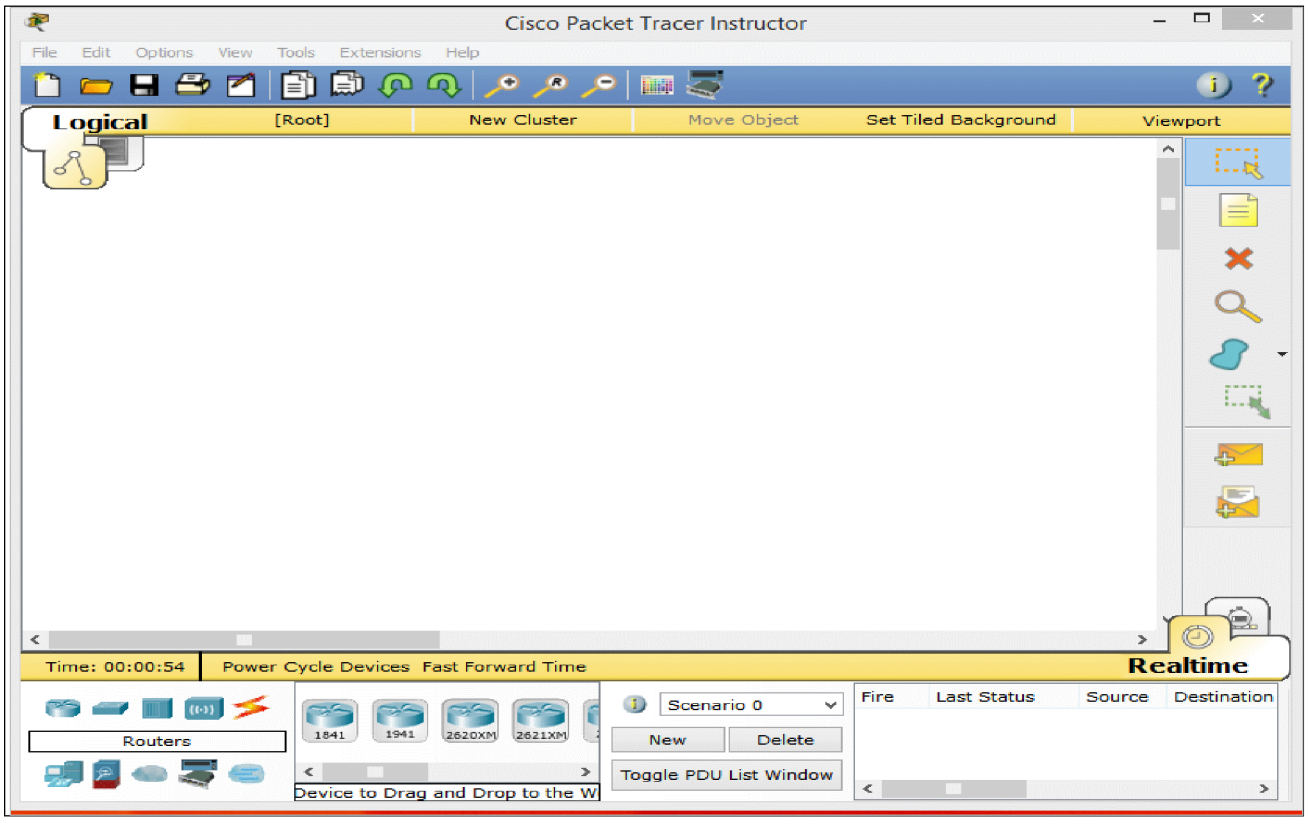


Figure IV.1 : le logiciel Packet Tracer

IV.2 Architecture d'interconnections de l'entreprise.

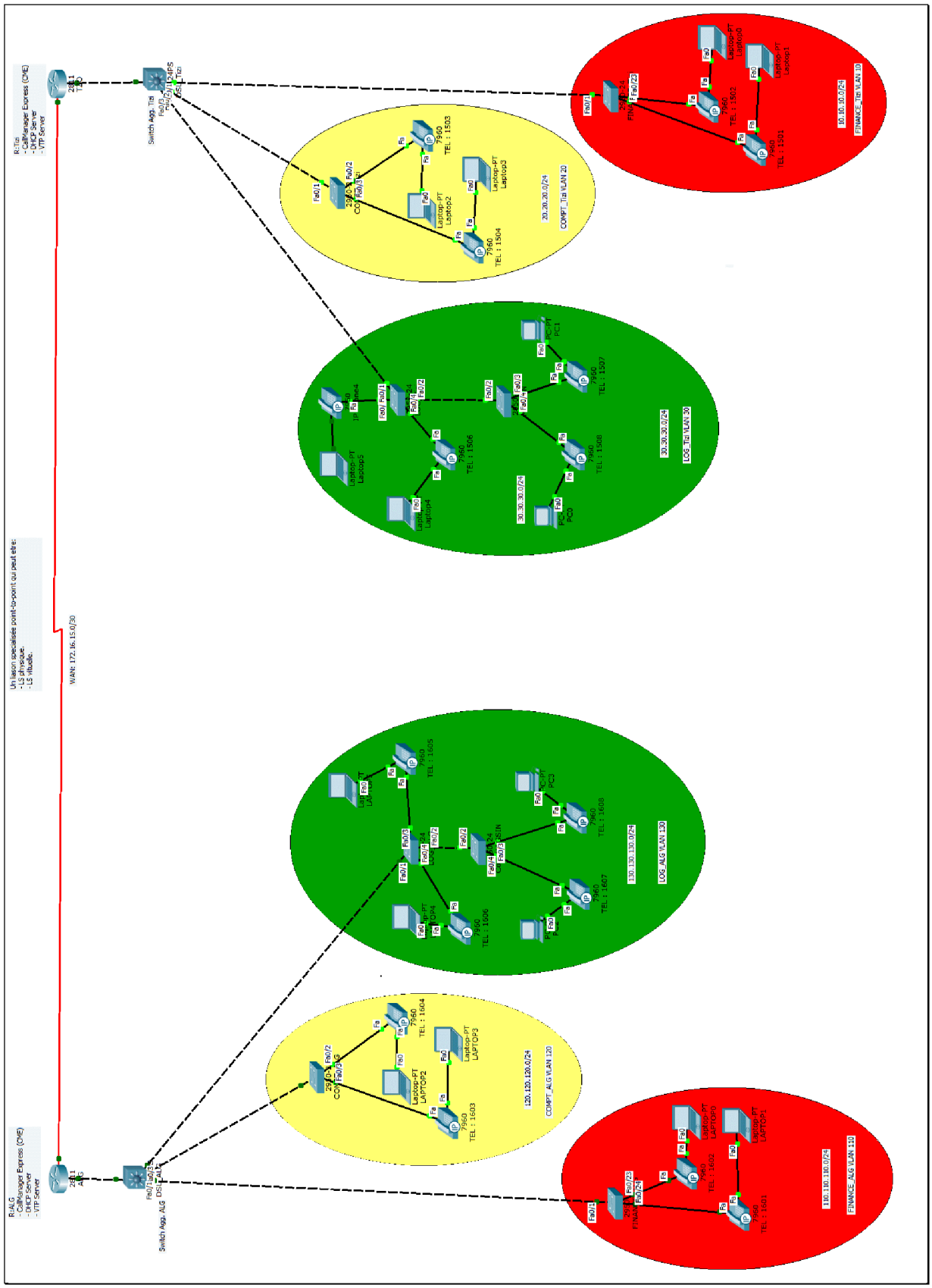


Figure IV.2 : Architecture de l' entreprise

IV.3 Méthode configuration des équipements :

Pour configurer les équipements du modèle on utilise le CLI (Command Line Interface)

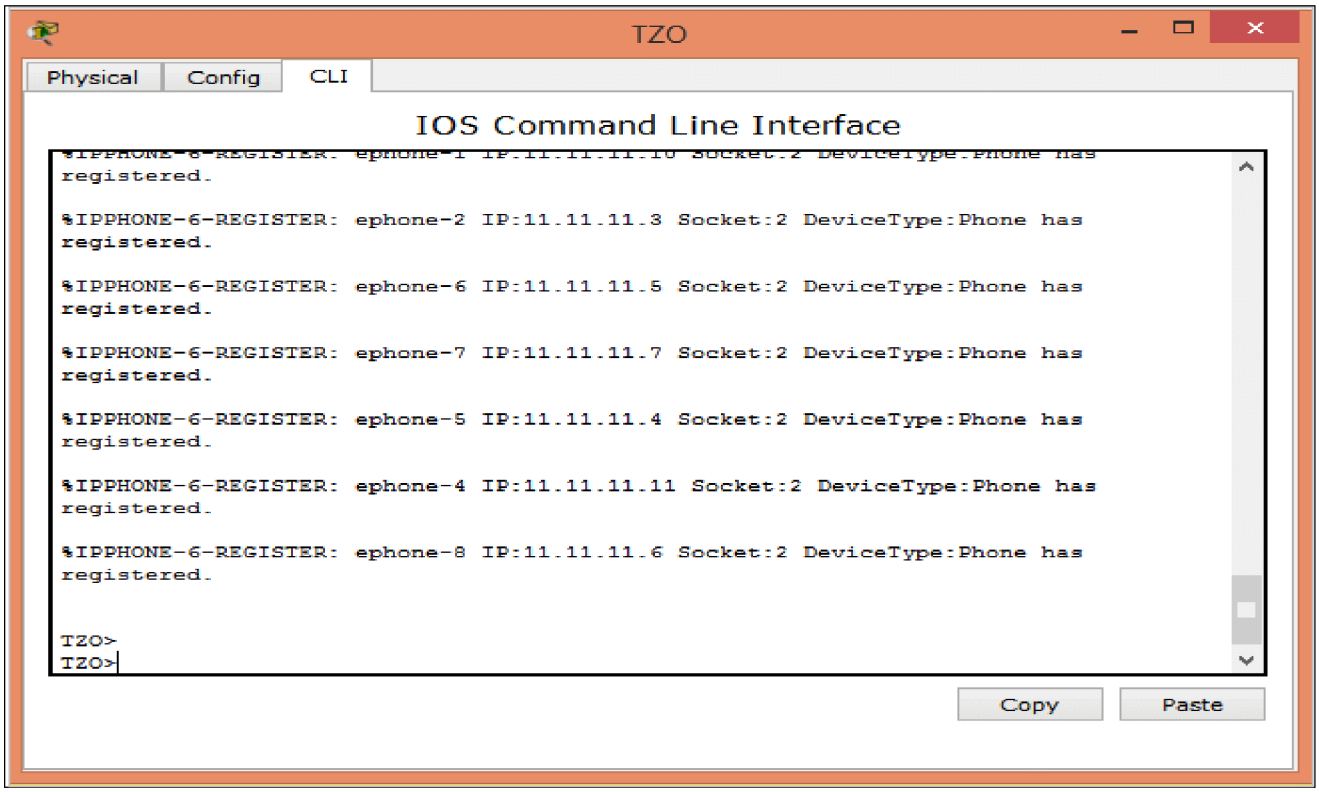


Figure IV.3 : Interface CLI

IV.4 Configuration des équipements

On va lancer des séries des configurations sur tous les équipements du réseau. Dans ce qui suit on va présenter la configuration en générale de tous les équipements avec un exemple configurée.

Notre architecture réseau dispose de deux sites (TZO, ALG) donc on configure les équipements de site TZO et on refait les mêmes procédures de configuration pour le site d'ALG.

IV.4.1 Configuration des équipements (SITE DE TZO)

IV.4.1.1. Configuration de routeur

Les étapes de configurations sont présentées comme suit :

1. Configuration de Hostname.
2. Configuration de VTP.
3. Créations des VLAN.
4. Configuration de pool DHCP pour Finance, Comptabilité, Logistique et la VoIP.
5. Création et Configuration des sous interfaces du routeur :

   5.1 Configuration de l'interface FastEthernet0/0.

   5.2 Création et Configuration de l'interface virtuelle FastEthernet 0/0.10

   5.3 Création et Configuration de l'interface virtuelle FastEthernet 0/0.20.

   5.4 Création et Configuration de l'interface virtuelle FastEthernet 0/0.30.

   5.5 Création Configuration de l'interface virtuelle FastEthernet 0/0.11.

6. Configuration d'ACL (Access Contrôle List)

   6.1 Création et application de la liste d'accès 1 sur l'interface Fa0/0.10

   6.2 Création et application de la liste d'accès 2 sur l'interface Fa0/0.20

   6.3 Création et application de la liste d'accès 3sur l'interface Fa0/0.30

7. Configuration de l'interface série et l'activation de ppp
8. Configuration de routage statique.
9. Configuration de téléphone IP et l'affichage des caractéristique (Call Manager Express).
10. Configuration de la passerelle du CME TZO pour joindre le CME ALG.

1. Configuration de Hostname .

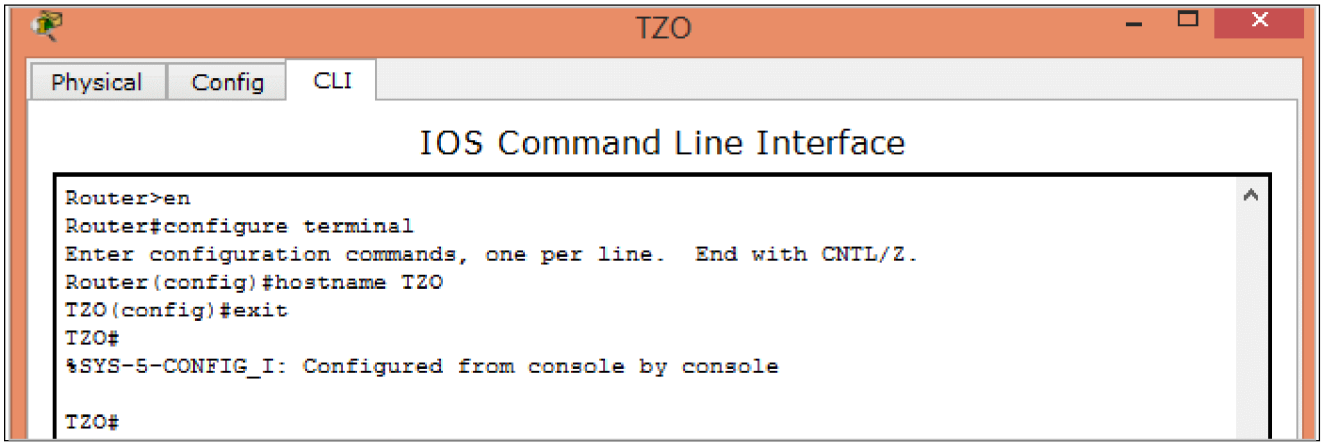


Figure VI.4 : Routeur nommé TZO

2. Configuration de VTP (Vlan trunk protocole)

On configure le Routeur comme VTP Server et on lui attribut le nom de Domain et le Password.

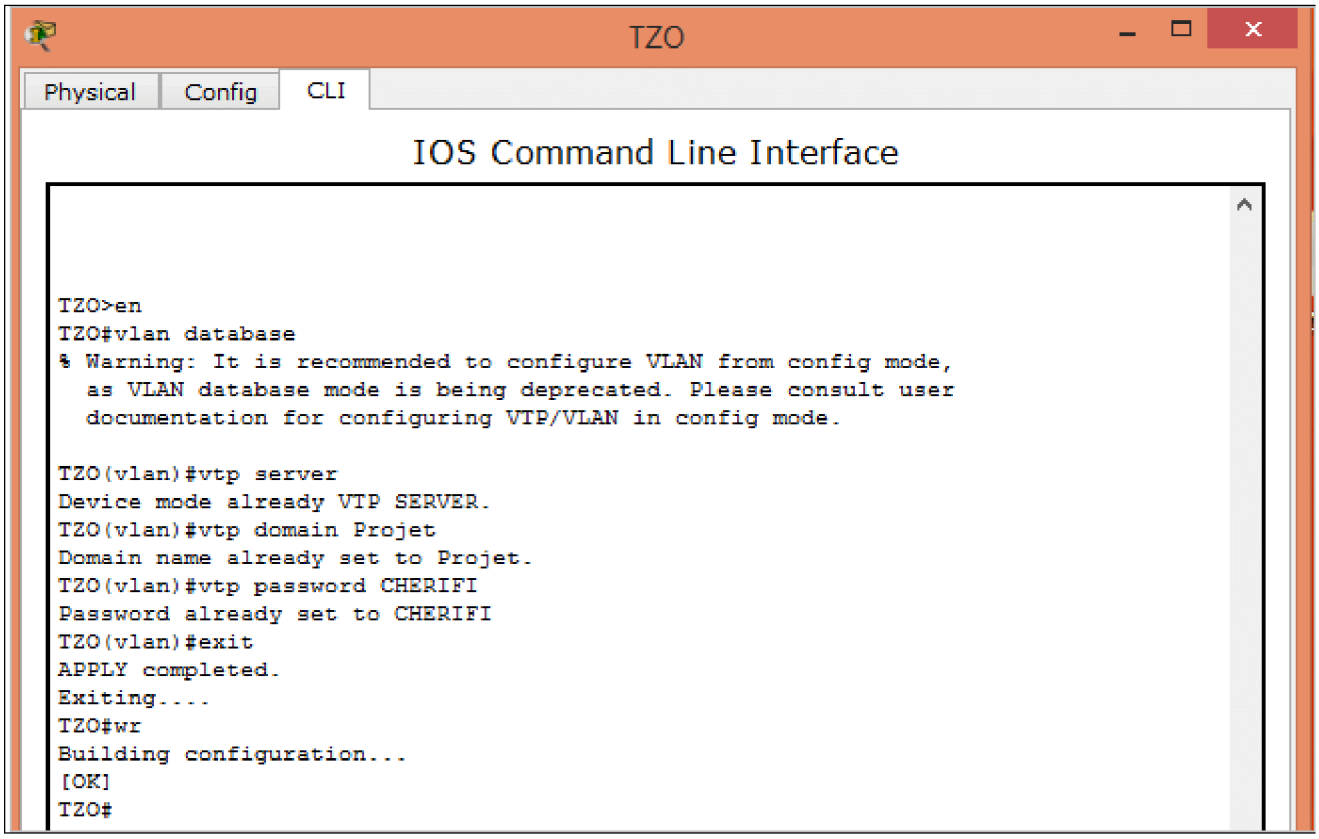


Figure VI.5: Configuration de VTP (Routeur TZO)

On utilise la commande < show vtp status> pour affiches le statut de VTP

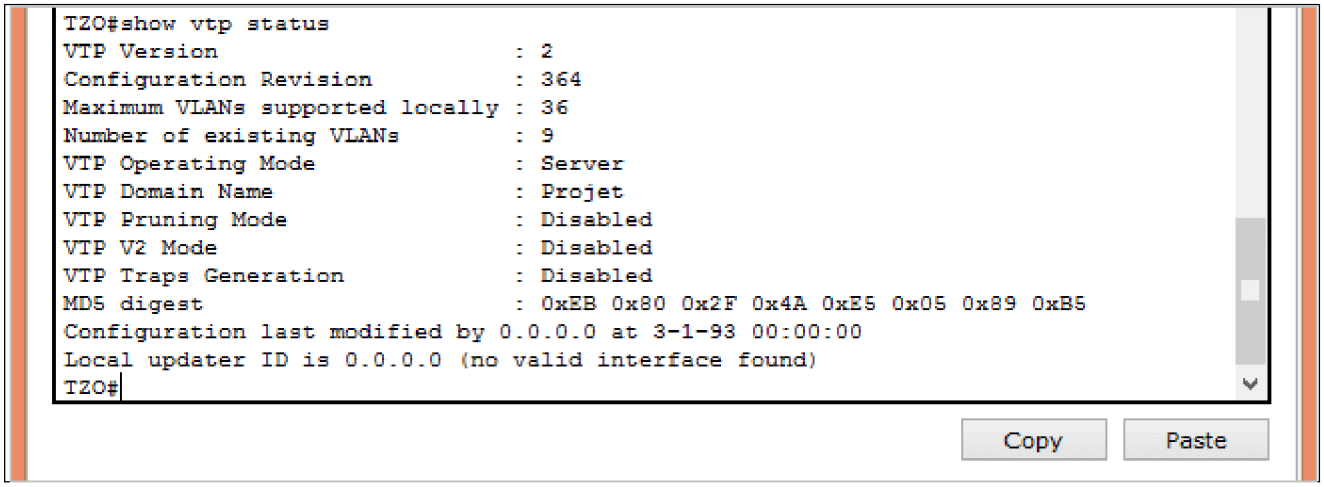


Figure IV.6 : Le statut de VTP

3. Créations des VLAN

On utilise la commande « vlan database » pour créer les VLAN sur le routeur .On va créer 4 VLAN (vlan10.vlan 20 .vlan 30.vlan 11)

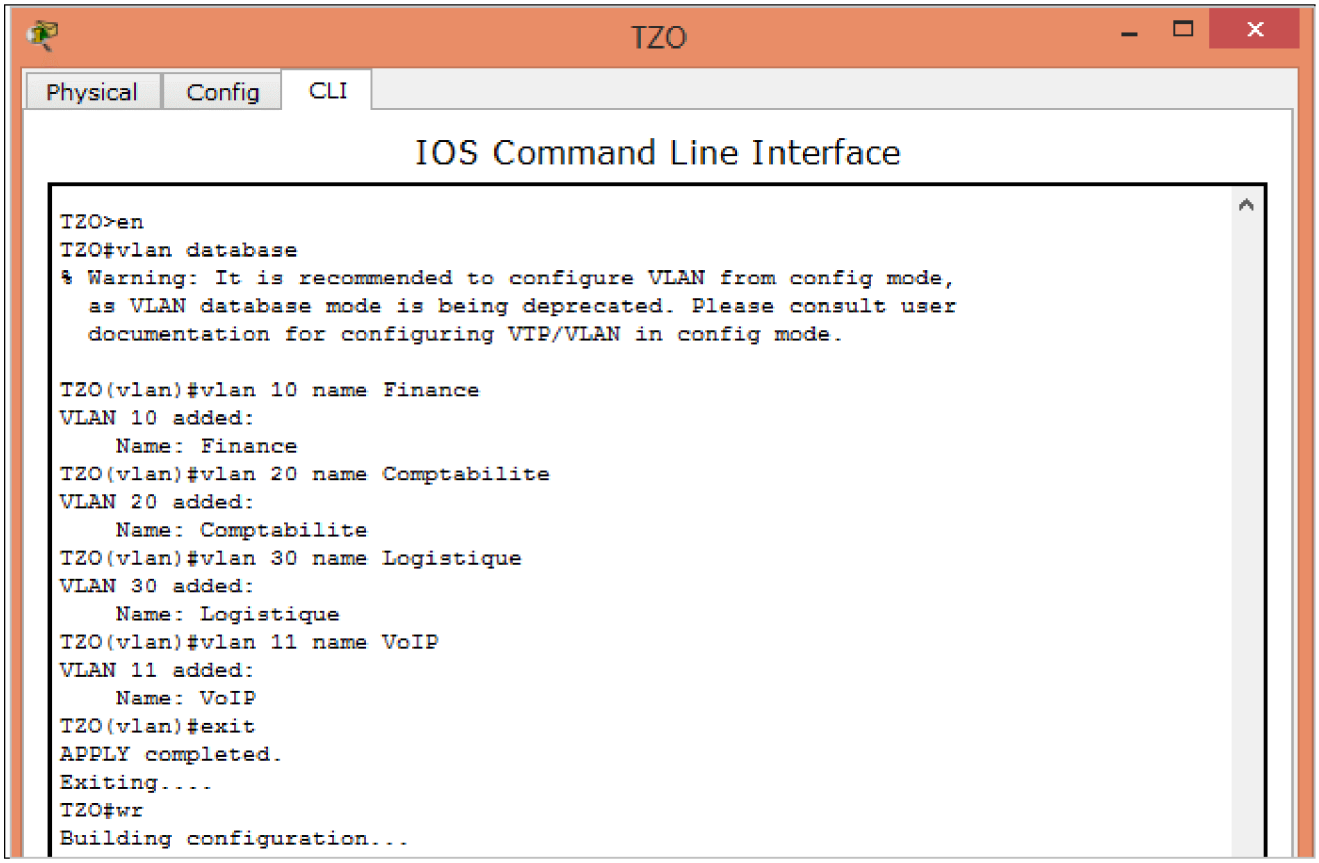


Figure IV.7: Création des VLAN

On utilise la commande « show vlan brief » pour afficher les VLAN

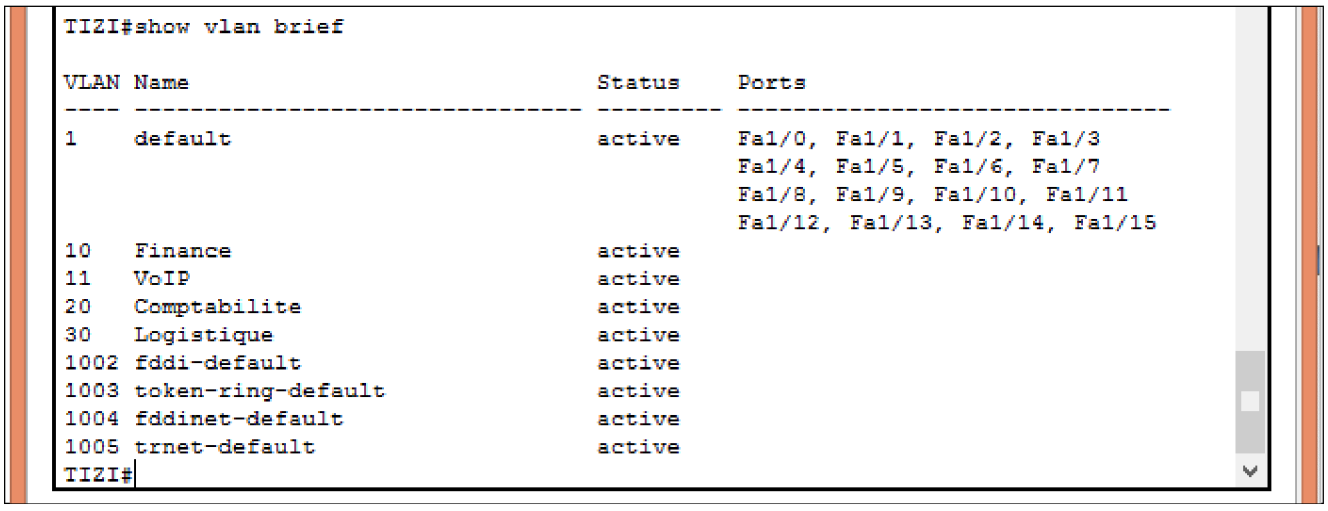


Figure IV.8 : Affichage des VLAN

4. Configuration de pool DHCP

On configure le pool DHCP correspond au déférent VLAN (Finance, Comptabilite, Logistique, VoIP)

```
TZO>
TZO>en
TZO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
TZO(config)#ip dhcp pool Finance
TZO(dhcp-config)#network 10.10.10.0 255.255.255.0
TZO(dhcp-config)# default-router 10.10.10.1
TZO(dhcp-config)#exit
TZO(config)#ip dhcp pool Comptabilite
TZO(dhcp-config)#network 20.20.20.0 255.255.255.0
TZO(dhcp-config)# default-router 20.20.20.1
TZO(dhcp-config)#exit
TZO(config)#ip dhcp pool Logistique
TZO(dhcp-config)#network 30.30.30.0 255.255.255.0
TZO(dhcp-config)# default-router 30.30.30.1
TZO(dhcp-config)#exit
TZO(config)#ip dhcp pool VoIP
TZO(dhcp-config)# network 11.11.11.0 255.255.255.0
TZO(dhcp-config)# default-router 11.11.11.1
TZO(dhcp-config)# option 150 ip 11.11.11.1
TZO(dhcp-config)#exit
TZO(config)#do wr
Building configuration...
[OK]
```

Figure IV.9 : Configuration de pool DHCP pour les déférents VLAN.

5. Création et Configuration des sous interfaces du Routeur

Pour pouvoir router nos Vlan, il faut 4 interfaces. Le problème est que si l'on doit router 10.15ou 20 vlan, ça va coûter cher ! Donc la solution, c'est de créer des sous interfaces virtuelles afin de faire transiter nos VLAN par ceux-ci. On peut créer des sous interfaces virtuelles vu que tous nos réseaux vont passer dans la seule interface physique du routeur Fa0/0.

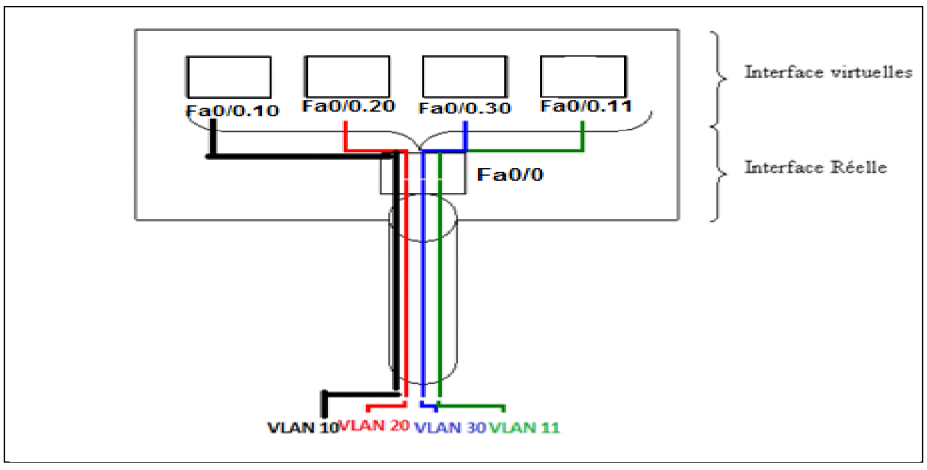


Figure IV.10: Interface virtuelle

Comme on peut le voir sur la Figure IV.10, tous nos VLAN passeront dans l'interface réelle du routeur Fa0/0 qui sera alors découpé en interface virtuelle. Nous allons en créer 4, une pour chaque VLAN.

Par contre, comme nous allons utiliser des sous interfaces, il ne faut pas que l'interface physique Fa0/0 est une adresse IP. Sinon cela va "cacher" les adresses IP de nos sous réseau virtuel que nous allons mettre dans nos sous interfaces. Il faut laisser l'interface Fa0/0 vierge.

Tout d'abord on s'assure que notre interface réelle Fa0/0 soit bien vierge puis on va criée et Configure les sous interfaces virtuel.

5.1 Configuration de l'interface Fa0/0.

```
TZO>en
TZO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
TZO(config)#interface FastEthernet0/0
TZO(config-if)#no ip address
TZO(config-if)#no shut

TZO(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

Figure IV.11 : Configuration de Fa0/0

5.2 Création et Configuration de l'interface virtuelle FastEthernet 0/0.10

```
TZO(config)#interface FastEthernet0/0.10
TZO(config-subif)# encapsulation dot1Q 10
TZO(config-subif)# ip address 10.10.10.1 255.255.255.0
TZO(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed state
to up

TZO(config-subif)#exit
```

Figure IV.12 : Création et configuration de Fa0/0.10

5.3 Création et Configuration de l'interface virtuelle FastEthernet 0/0.20

```
TZO(config)#interface FastEthernet0/0.20
TZO(config-subif)# encapsulation dot1Q 20
TZO(config-subif)# ip address 20.20.20.1 255.255.255.0
TZO(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20, changed state
to up

TZO(config-subif)#exit
```

Figure IV.13 : Création et configuration de Fa0/0.20.

5.4 Création et Configuration de l'interface virtuelle FastEthernet 0/0.30

```
TZO(config)#interface FastEthernet0/0.30
TZO(config-subif)# encapsulation dot1Q 30
TZO(config-subif)# ip address 30.30.30.1 255.255.255.0
TZO(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state
to up

TZO(config-subif)#exit
```

Figure IV.14 : Création et configuration de Fa0/0.30

5.5 Création et Configuration de l'interface virtuelle FastEthernet 0/0.11

```
TZO(config)#interface FastEthernet0/0.11
TZO(config-subif)# encapsulation dot1Q 11
TZO(config-subif)# ip address 11.11.11.1 255.255.255.0
%LINK-5-CHANGED: Interface FastEthernet0/0.11, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.11, changed state
to up

TZO(config-subif)#exit
TZO(config)#do wr
```

Figure IV.15 : Création et configuration de Fa0/0.11

6. Configuration d'ACL (Access Contrôle List)

On configure les ACL sur le routeur de site TZO on refait la même procédure sur le routeur de site ALG. On utilise les ACL standards

6.1 Création et Application de la liste d'accès 1 sur l'interface Fa0/0.10

```
TZO>en
TZO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
TZO(config)#access-list 1 permit 111.111.111.0 0.0.0.255
TZO(config)#access-list 1 permit 110.110.110.0 0.0.0.255
TZO(config)#access-list 1 deny any
TZO(config)#interface FastEthernet0/0.10
TZO(config-subif)#ip access-group 1 out
TZO(config-subif)#exit
```

Figure IV.16 : Configuration d'ACL 1 sur l'interface Fa0/0.10

6.2 Création et Application de la liste d'accès 2 sur l'interface Fa0/0.20

```
TZO(config)#access-list 2 permit 111.111.111.0 0.0.0.255
TZO(config)#access-list 2 permit 120.120.120.0 0.0.0.255
TZO(config)#access-list 2 deny any
TZO(config)#interface FastEthernet0/0.20
TZO(config-subif)#ip access-group 2 out
TZO(config-subif)#exit
```

Figure IV.17 : Configuration d'ACL 2 sur l'interface Fa0/0.20

6.3 Création et Application de la liste d'accès 3 sur l'interface Fa0/0.30

```
TZO(config)#access-list 3 permit 111.111.111.0 0.0.0.255
TZO(config)#access-list 3 permit 130.130.130.0 0.0.0.255
TZO(config)#access-list 3 deny any
TZO(config)#interface FastEthernet0/0.30
TZO(config-subif)#ip access-group 3 out
TZO(config-subif)#exit
TZO(config)#exit
TZO#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure IV.18 : Configuration d'ACL 3 sur l'interface Fa0/0.30

6. Configuration de l'interface série et l'encapsulation ppp.

Pour interconnecter les deux sites de l'entreprise par la liaison spécialisée point as point On configure l'interface serial0/0/0 WAN de R TZO connectée au R ALG et on active le ppp ainsi le clock rate pour synchroniser le réseau .on refait les mêmes procédures sur le R ALG.

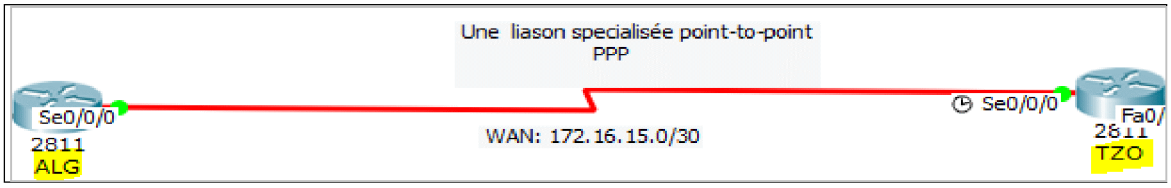


Figure IV.19 : L'interconnexion de deux sites par la liaison spécialisée point a point

```
TZO>en
TZO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
TZO(config)#interface Serial0/0/0
TZO(config-if)# bandwidth 10000
TZO(config-if)# ip address 172.16.15.1 255.255.255.252
TZO(config-if)# encapsulation ppp
TZO(config-if)# clock rate 64000
TZO(config-if)#no shut
```

Figure IV.20 : Configuration de l'interface série de routeur TZO et l'activation de PPP

```
ALG>en
ALG#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ALG(config)#interface Serial0/0/0
ALG(config-if)# bandwidth 10000
ALG(config-if)# ip address 172.16.15.2 255.255.255.252
ALG(config-if)# encapsulation ppp
ALG(config-if)#exit
ALG(config)#do wr
Building configuration...
[OK]
```

Figure IV.21 : Configuration de l'interface série de routeur ALG et l'activation de PPP

8. Configuration de Routage statique

- On configure la route par default sur le Routeur de site TZO en utilisant l'interface série 0/0/0 de Routeur de site ALG comme passerelle de dernier recours Gateway of last resort

```
TZO>en
TZO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
TZO(config)#ip route 0.0.0.0 0.0.0.0 172.16.15.2
TZO(config)#do wr
Building configuration...
[OK]
```

Figure IV.22 : Configuration de la route par default sur le routeur de site TZO

Nous utilisons la commande<< show IP route >> pour afficher la table de routage

```
TZO#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.16.15.2 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, FastEthernet0/0.10
     11.0.0.0/24 is subnetted, 1 subnets
C       11.11.11.0 is directly connected, FastEthernet0/0.11
     20.0.0.0/24 is subnetted, 1 subnets
C       20.20.20.0 is directly connected, FastEthernet0/0.20
     30.0.0.0/24 is subnetted, 1 subnets
C       30.30.30.0 is directly connected, FastEthernet0/0.30
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.15.0/30 is directly connected, Serial0/0/0
C       172.16.15.2/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 172.16.15.2
```

Figure IV.23 : La Table de routage de routeur TZO

- On configure la route par default sur le Router de site ALG en utilisant l'interface série 0/0/0 de Router de site TZO comme passerelle de dernier recours (Gateway of last resort)

```
ALG>en
ALG#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ALG(config)#ip route 0.0.0.0 0.0.0.0 172.16.15.1
ALG(config)#do wr
Building configuration...
[OK]
ALG(config)#
```

Figure IV.24 : Configuration de la route par default sur le routeur de site ALG

9. Configuration de téléphone IP et l'affichage des caractéristiques

On configurons le Call Manager Express (CME TZO)

- On utilise la commande « telephony-service »pour entre dans le mode de la config de téléphone IP

```
TZO>en
TZO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
TZO(config)#telephony-service
TZO(config-telephony)# max-ephones 40
TZO(config-telephony)# max-dn 40
TZO(config-telephony)# ip source-address 11.11.11.1 port 2000
TZO(config-telephony)# auto assign 1 to 40
TZO(config-telephony)#exit
TZO(config)#ephone-dn 1
TZO(config-ephone-dn)# number 1501%LINK-3-UPDOWN: Interface ephone_dsp DN 1.1,
changed state to up

TZO(config-ephone-dn)#exit
TZO(config)#ephone-dn 2
TZO(config-ephone-dn)# number 1502%LINK-3-UPDOWN: Interface ephone_dsp DN 2.1,
changed state to up

TZO(config-ephone-dn)#exit
TZO(config)#ephone-dn 3
TZO(config-ephone-dn)# number 1503%LINK-3-UPDOWN: Interface ephone_dsp DN 3.1,
changed state to up
```

.
.

```
TZO(config)#ephone-dn 40
TZO(config-ephone-dn)# number 1540%LINK-3-UPDOWN: Interface ephone_dsp DN 40.1,
changed state to up

TZO(config-ephone-dn)#exit
TZO(config)#do wr
Building configuration...
[OK]
TZO(config)#
```

Figure IV.25 : Configuration de téléphone IP de 1 a 40

- On affiche les caractéristiques des téléphones IP numérotes de 1a 8.

```
TZO(config)#ephone 1
TZO(config-ephone)#type 7960
TZO(config-ephone)#button 1:1
Need to configure ephone mac address or VM station-id
TZO(config-ephone)#exit
TZO(config)#ephone 2
TZO(config-ephone)#type 7960
TZO(config-ephone)#button 1:2
Need to configure ephone mac address or VM station-id
TZO(config-ephone)#exit
TZO(config)#ephone 3
TZO(config-ephone)#type 7960
TZO(config-ephone)#button 1:3
Need to configure ephone mac address or VM station-id
TZO(config-ephone)#exit
```

-
-

```
TZO(config)#ephone 7
TZO(config-ephone)#type 7960
TZO(config-ephone)#button 1:7
Need to configure ephone mac address or VM station-id
TZO(config-ephone)#exit
TZO(config)#ephone 8
TZO(config-ephone)#type 7960
TZO(config-ephone)#button 1:8
Need to configure ephone mac address or VM station-id
TZO(config-ephone)#exit
TZO(config)#do wr
Building configuration...
[OK]
TZO(config)#exit
TZO#
```

Figure IV.26 : Affichages des caractéristiques des 8 téléphones IP

10. Configuration de la passerelle du CME TZO pour joindre le CME ALG

On refait les mêmes procédures pour le Routeur de site ALG.

On utilise la commande « dial-Peer Voice » pour entre dans le mode de la config

```
TZO>en
TZO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
TZO(config)#dial-peer voice 2 voip
TZO(config-dial-peer)# destination-pattern 1...
TZO(config-dial-peer)# session target ipv4:172.16.15.2
TZO(config-dial-peer)#exit
TZO(config)#do wr
Building configuration...
[OK]
```

Figure IV.27: Configuration de la passerelle du CME TZO

Les téléphones des deux sites peuvent dès à présent s'appeler.

IV.4.1.2. Configuration des commutateurs

On refait les mêmes procédures de configuration pour les commutateurs de site ALG.

IV.4.1.2.1. configuration de Multilayer switch (DSL_Tizi)

Les étapes de configuration sont présentées comme suit :

1. Configuration de Hostname (DSL_TIZ).
2. Configuration de VTP en mode client .
3. Configuration des interfaces en mode trunk

1. Configuration de Hostname

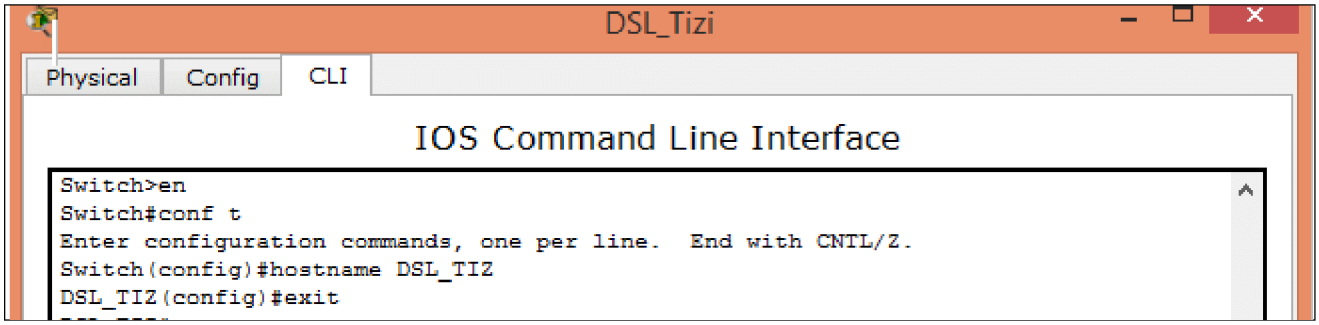


Figure IV.28: Switch nommé DSL_TIZ

2. Configuration de VTP (Vlan trunk Protocol)

On configure le Switch DSL_TIZ comme VTP client on lui attribut le nom de Domain et le password.

```
DSL_TIZ>en
DSL_TIZ#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DSL_TIZ(config)#vtp mode clien
Setting device to VTP CLIENT mode.
DSL_TIZ(config)#vtp domain Projet
Changing VTP domain name from NULL to Projet
DSL_TIZ(config)#vtp password CHERIFI
Setting device VLAN database password to CHERIFI
DSL_TIZ(config)#exit
DSL_TIZ#
%SYS-5-CONFIG_I: Configured from console by console

DSL_TIZ#wr
Building configuration...
[OK]
```

Figure IV.29: Configuration de VTP (Switch DSL_TIZ)

On utilise la commande « show vtp status » pour afficher le Statut de VTP.

```
DSL_TIZ#show vtp status
VTP Version                     : 2
Configuration Revision          : 100
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 9
VTP Operating Mode              : Client
VTP Domain Name                 : Projet
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x2B 0xD3 0x03 0x15 0x54 0x30 0xB0 0xF5
Configuration last modified by 10.10.10.1 at 3-1-93 00:00:00
DSL_TIZ#
```

Figure IV.30: le Statut de VTP

3. Configurations des Interfaces en mode trunk.

- On configure l'interface GigabitEthernet0/1 qui reliée le Switch et le Routeur en mode trunk

```
DSL_TIZ>en
DSL_TIZ#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DSL_TIZ(config)#interface GigabitEthernet0/1
DSL_TIZ(config-if)# switchport trunk encapsulation dot1q
DSL_TIZ(config-if)# switchport mode trunk
```

Figure IV.31 : Configuration de l'interface GigabitEthernet0/1

- On configure l'interface FastEthernet0/1 en mode trunk

```
DSL_TIZ(config)#interface FastEthernet0/1
DSL_TIZ(config-if)# switchport trunk encapsulation dot1q
DSL_TIZ(config-if)# switchport mode trunk

DSL_TIZ(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
```

Figure IV.32 : Configuration de l'interface FastEthernet0/1(Switch DSL_TIZ)

- On configure l'interface FastEthernet0/2 en mode trunk

```
DSL_TIZ(config)#interface FastEthernet0/2
DSL_TIZ(config-if)# switchport trunk encapsulation dot1q
DSL_TIZ(config-if)# switchport mode trunk

DSL_TIZ(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to
```

Figure IV.33 : Configuration de l'interface FastEthernet0/2(Switch DSL_TIZ)

- On configure l'interface FastEthernet0/3 en mode trunk

```
DSL_TIZ(config)#interface FastEthernet0/3
DSL_TIZ(config-if)# switchport trunk encapsulation dot1q
DSL_TIZ(config-if)# switchport mode trunk

DSL_TIZ(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to
down

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

DSL_TIZ(config-if)#exit
DSL_TIZ(config)#do wr
Building configuration...
[OK]
```

Figure IV.34: Configuration de l'interface FastEthernet0/3 (Switch DSL_TIZ)

On utilise la commande « show vlan brief » pour afficher les VLAN et les interfaces affectées.

```
DSL_TIZ#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig0/2
10   Finance                           active
11   VoIP                              active
20   Comptabilite                      active
30   Logistique                        active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
DSL_TIZ#
```

Figure IV.35 : Affichage des VLAN

IV.4.1.2.2. configuration de Switch FINANCE_Tizi

Les étapes de configuration sont présentées comme suit :

1. Configuration de VTP
2. Configuration de l'interface FastEthernet0/1
3. Configuration est Affectations des interfaces aux VLAN

1. Configuration de VTP (Vlan trunk protocole)

On configure le Switch Finance_Tizi comme VTP client on lui attribuant le nom de Domain et le password.

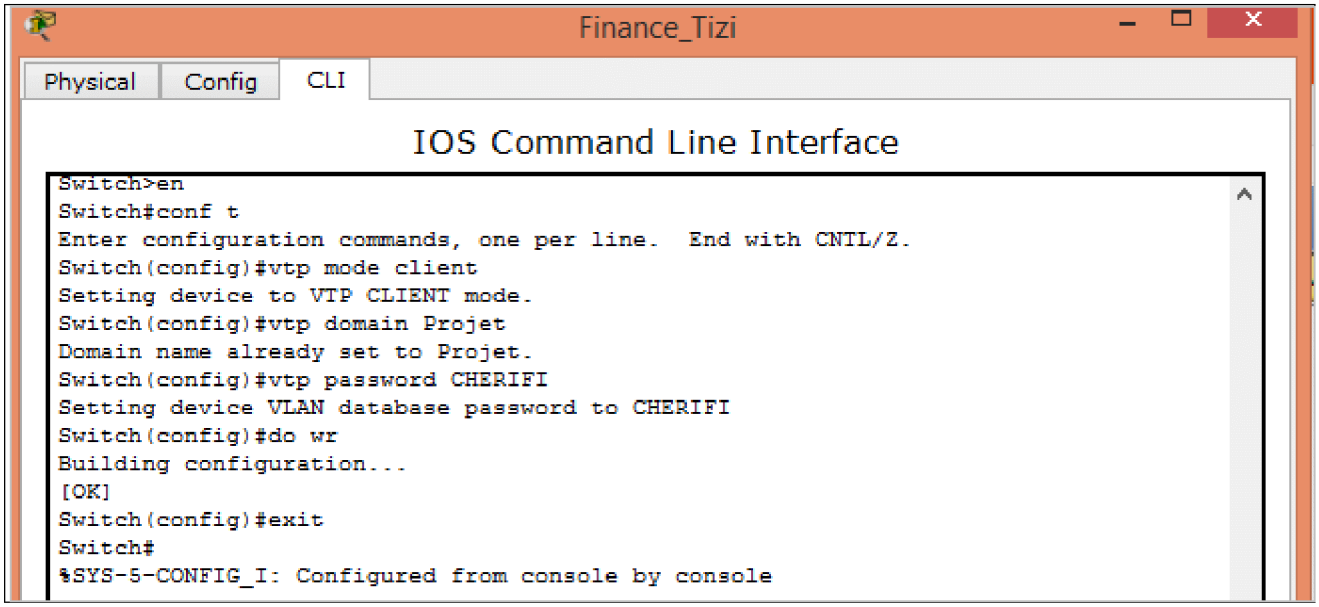


Figure IV.36 : Configuration de VTP (Switch Finance_Tizi)

2. Configuration de l'interface FastEthernet0/1

On configure l'interface FastEthernet0/1 qui relier le Switch Finance_Tizi et le Switch DSL_Tizi en mode trunk.

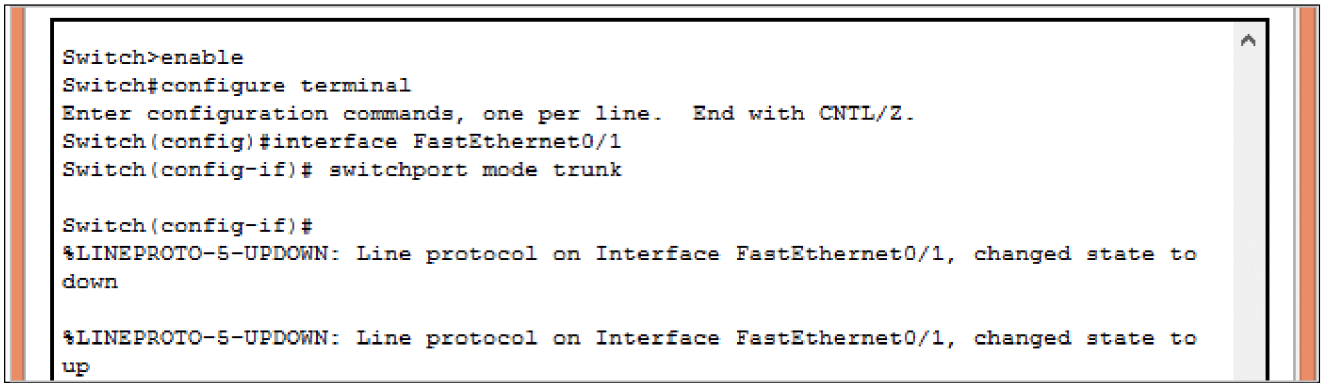


Figure IV.37: Configuration de l'interface FastEthernet0/1(Switch Finance_Tizi)

3. Configuration et Affectation des interfaces aux VLAN

On configure les interfaces de Switch en mode Access et on les places dans les VLAN (10 ,11)

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet0/23
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 11
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/24
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 11
Switch(config-if)#exit
Switch(config)#do wr
Building configuration...
[OK]
```

Figure IV.38 : Configuration et Affectation des interfaces aux VLAN

On utilise la commande « show vlan brief » pour afficher les VLAN et les interfaces affecter

```
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22
10   Finance                           active    Fa0/23, Fa0/24
11   VoIP                              active
20   Comptabilite                      active
30   Logistique                        active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

Figure IV.39 : Affichage des VLAN

Nous utilisons les mêmes étapes pour configure le Switch COMPT_Tizi, Switch LOG_Tizi, Switch MAGASIN.

IV.4.1.2.3 Configuration de Switch COMPT_Tizi

1. Configuration de VTP (Vlan trunk protocole)

On configure le Switch COMPT_Tizi comme VTP client on lui attribut le nom de Domain et le password.

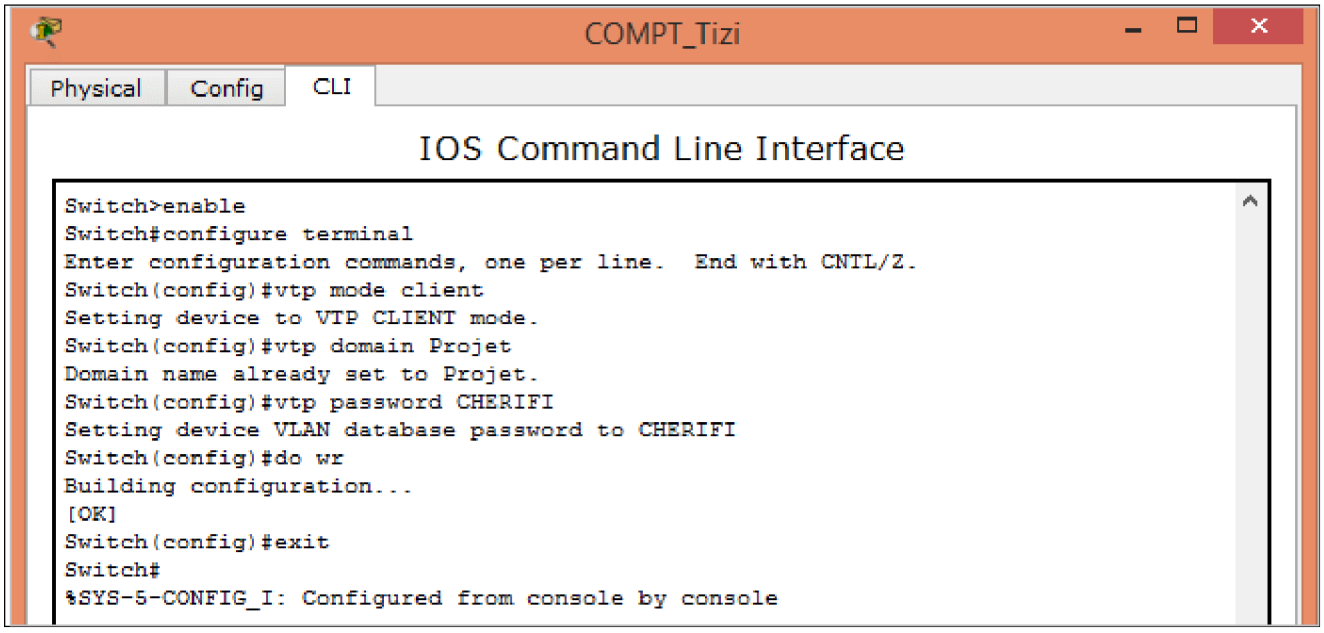


Figure IV.40 : Configuration de VTP (Switch COMPT_Tizi)

2. Configuration de l'interface FastEthernet0/1

On configure l'interface FastEthernet0/1 qui relier le Switch COMPT_Tizi et le Switch DSL_Tizi en mode trunk.

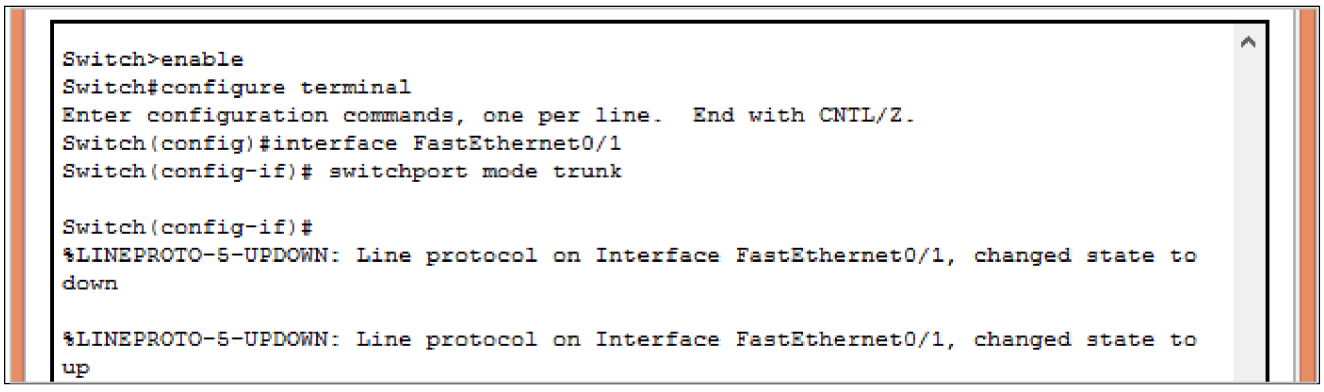


Figure IV.41 : Configuration de l'interface Fa0/1(Switch COMPT_Tizi)

3. Configuration et Affectation des interfaces aux VLAN

On configure les interfaces de Switch en mode Access et on les places dans les vlan (20 ,11)

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet0/2
Switch(config-if)# switchport access vlan 20
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 11
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/3
Switch(config-if)# switchport access vlan 20
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 11
Switch(config-if)#exit
Switch(config)#do wr
Building configuration...
[OK]
Switch(config)#exit
Switch#
```

Figure IV.42 : Configuration et Affectation des interfaces aux VLAN

IV.4.1.2.4. Configuration de Switch LOG_Tizi

1. Configuration de VTP (Vlan trunk protocole)

On configure le Switch LOG_Tizi comme VTP client on lui attribuant le nom de Domain et le password.

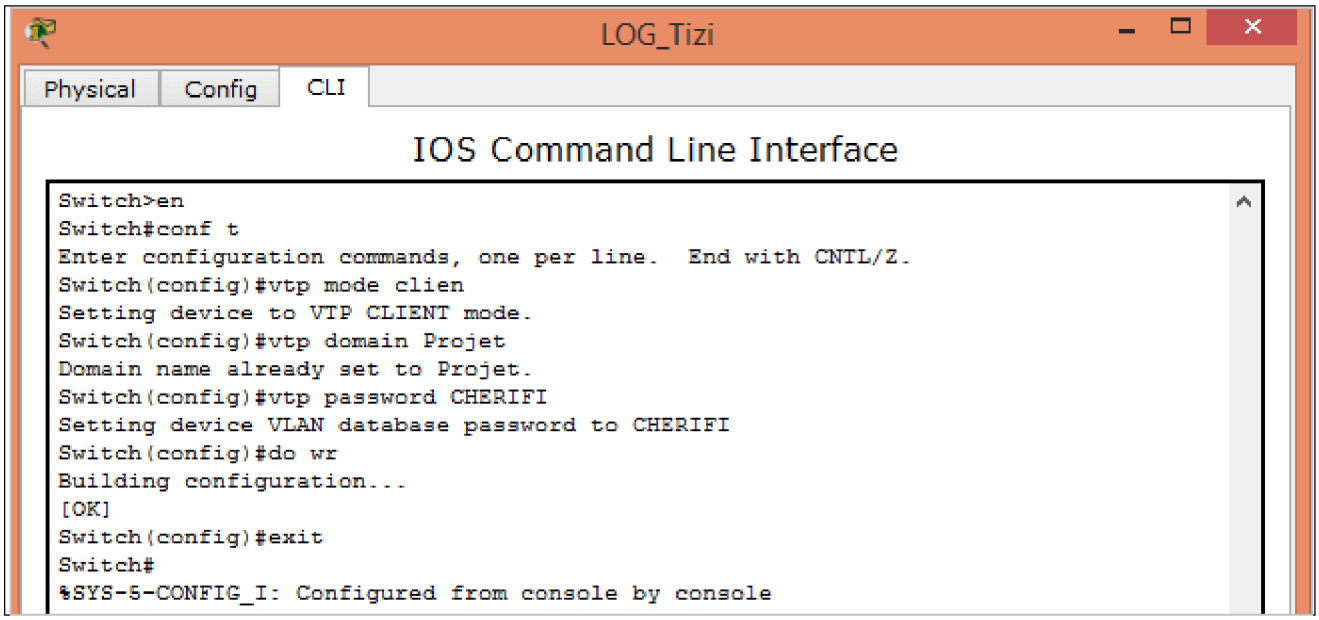


Figure IV.43 : Configuration de VTP (Switch LOG_Tizi)

2. Configuration des interfaces en mode Trunk.

2. 1 Configuration de l'interface FastEthernet0/1

On configure l'interface FastEthernet0/1 qui relier le Switch LOG_Tizi et le Switch DSL_Tizi en mode trunk.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet0/1
Switch(config-if)# switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
down

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

Figure IV.44 : Configuration de l'interface FastEthernet0/1(Switch LOG_Tizi)

2. 2 Configuration de l'interface FastEthernet0/2

On configure l'interface FastEthernet0/2 qui relier le Switch LOG_Tizi et le Switch MAGASIN en mode trunk.

```
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#no shut

Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

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

Figure IV.45 : Configuration de l'interface FastEthernet0/2 (Switch LOG_Tizi)

3. Configuration et affectation des interfaces aux VLAN

On configure les interfaces en mode Access puis on les places dans le vlan 30 et vlan 11

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet0/3
Switch(config-if)# switchport access vlan 30
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 11
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/4
Switch(config-if)# switchport access vlan 30
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 11
Switch(config-if)#exit
Switch(config)#do wr
Building configuration...
[OK]
Switch(config)#exit
Switch#
```

Figure IV. 46 : Configuration et affectation des interfaces aux VLAN

IV.4.1.2.5. Configuration de Switch MAGASIN

1. Configuration de VTP (Vlan trunk protocole)

On configure le Switch MAGASIN comme VTP client on lui attribuant le nom de Domain et le password.

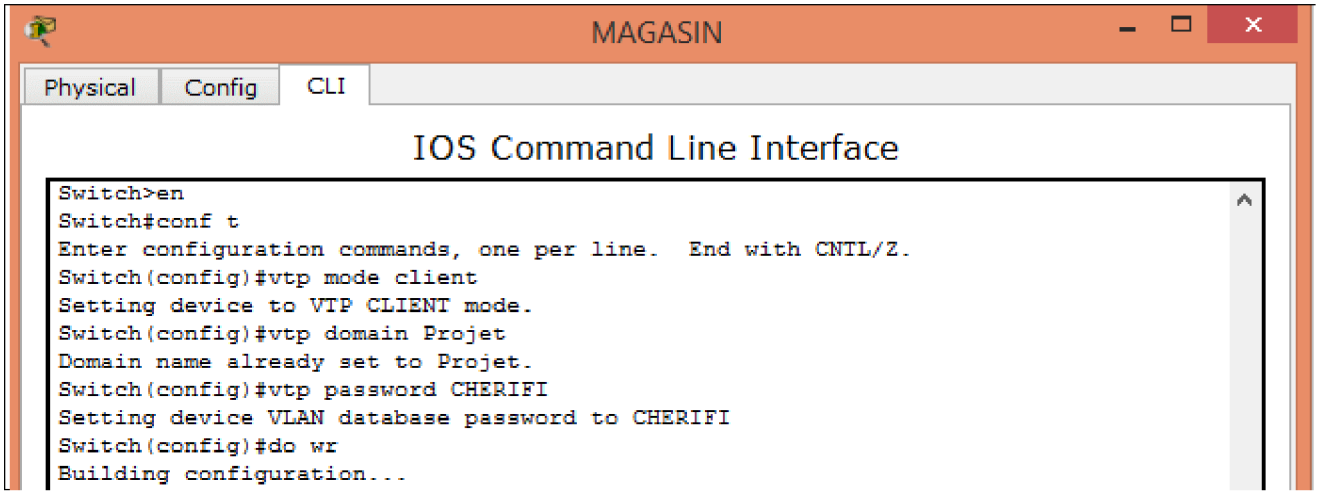


Figure IV. 47 : Configuration de VTP (Switch MAGASIN)

2. Configuration de l'interface FastEthernet0/2

On configure l'interface FastEthernet0/2 qui relier le Switch MAGASIN et le Switch LOG_Tizi en mode trunk

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)#exit
Switch(config)#exit
Switch#
```

Figure IV. 48 : Configuration de l'interface Fa0/2 (Switch MAGASIN)

3. Configuration et Affectation des interfaces aux VLAN

On configure les interfaces de Switch Magasin en mode Access et on les places dans le vlan 30 et vlan 11

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport access vlan 30
Switch(config-if)#switchport mode access
Switch(config-if)#switchport voice vlan 11
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/4
Switch(config-if)# switchport access vlan 30
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 11
Switch(config-if)#do wr
Building configuration...
[OK]
```

Figure IV. 49 : Configuration et affectation des interfaces Fa0/3 et Fa0/4 aux VLAN

IV.5 Attribution d'adresse IP pour Pc à partir de DHCP :

On dispose dans notre architecteur de 12 laptop et 4 PC chaque un aura son adresse IP, masque, la passerelle automatiquement as partir de serveur DHCP. (Figure III.50) montre un exemple de laptop0

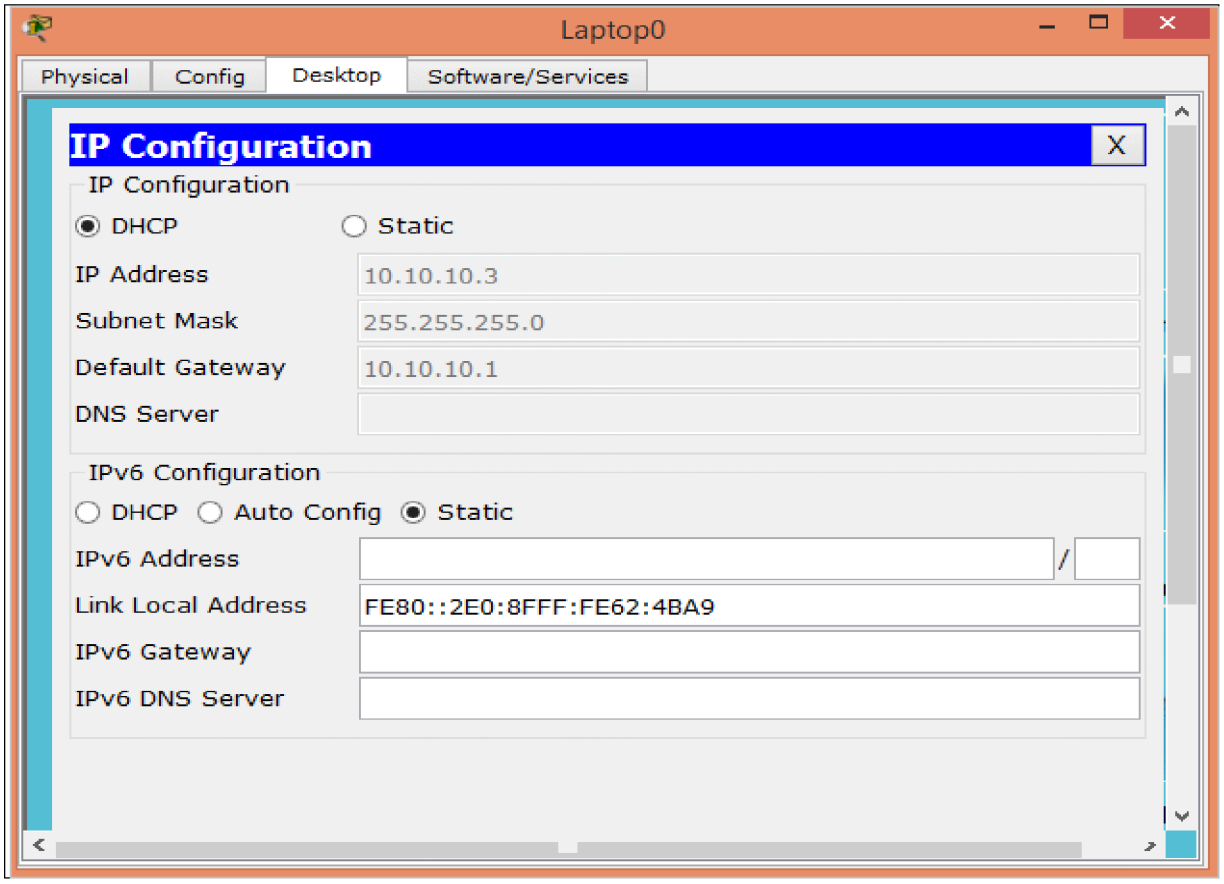


Figure IV.50: Attribution l'adresse IP, masque, passerelle de laptop0 par le server DHCP

IV.6 Test et validation de configuration

On test dans cette partie les communications entre tous les équipements en utilisant la commande Ping et en effectuant des appels. Ces tests sont faits entre équipements (Switch et routeurs, PCs, téléphone IP), inter-Vlan, entre Vlan et entre les sites. Il est à noter que la commande Ping est très utile pour tester la réponse d'un ordinateur sur un réseau. Cette commande envoie des paquets avec le protocole ICMP.

IV.6.1Test inter-Vlan

Nous testons la communication par exemple entre laptop6 et PC0 de VLAN LOG_Tizi, C'est deux postes sont dans le même sous-réseau, ils devraient pouvoir communiquer.

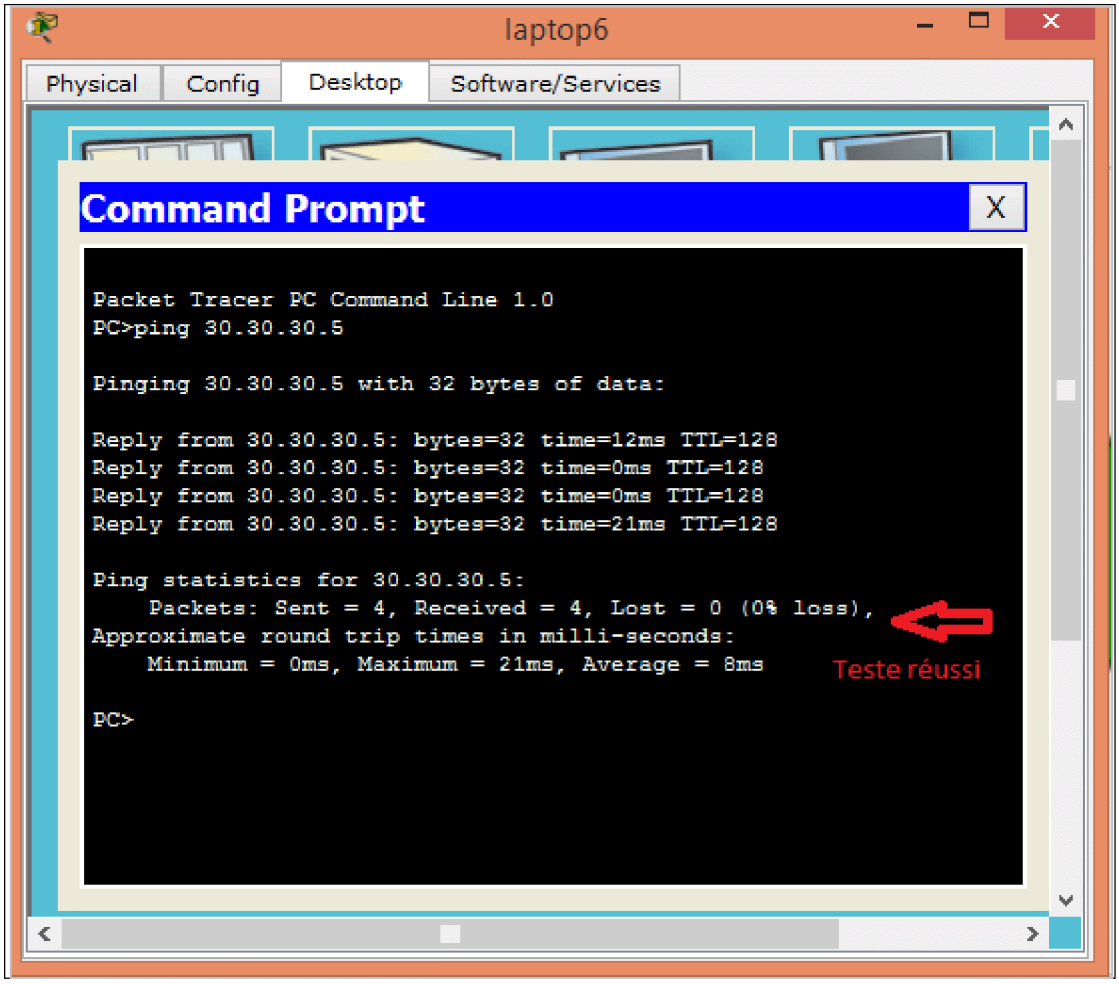


Figure IV.51: Teste entre laptop6 et PC0

IV.6.2 Test entre VLAN

1. On teste la communication entre Laptop1 de vlan 10 (FIN_Tizi) d'adresse IP 10.10.10.2 et Laptop6 de vlan 30 (LOG_Tizi) d'adresse IP 30.30.30.4. C'est deux postes ne sont pas dans le même sous-réseau, ils ne devraient pas communiquer.

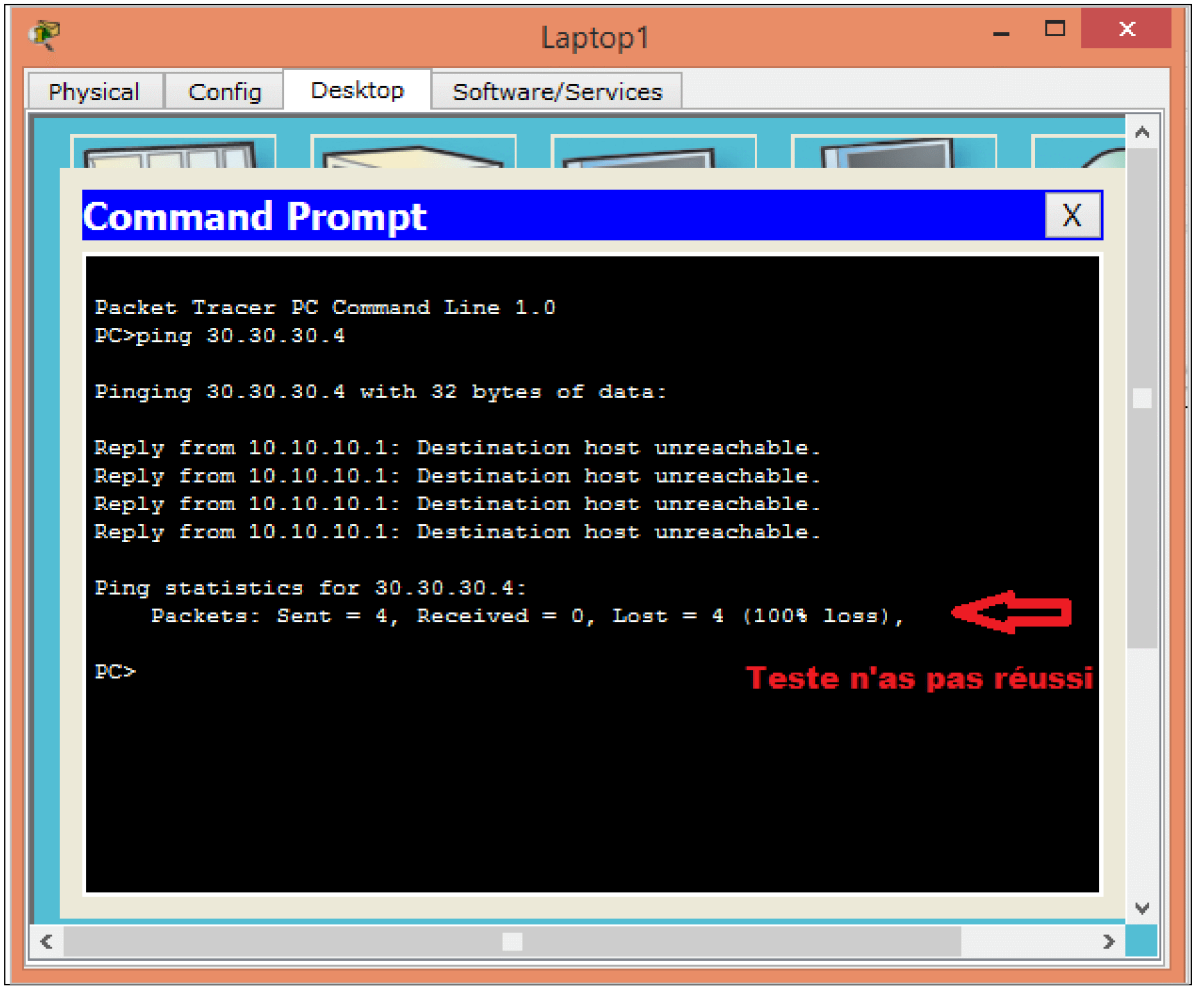


Figure IV.52: Teste entre laptop1 et laptop6

2. Nous testons la communication entre les téléphones IP on lançon des appelles vers les différents numéros de téléphone. on prend par exemple un appelle de TEL : 1508 appartenant au vlan LOG-Tizi vers le TEL : 1501 appartenant au vlan FINANCE_Tizi.

Figure IV.53 : Composition de numéro de correspondent 1501

Figure IV.53: Recevoir l'appelle (Suite)

IV.6.3 Teste de connectivite entre l'interface série de routeur TZO et celle de routeur ALG.

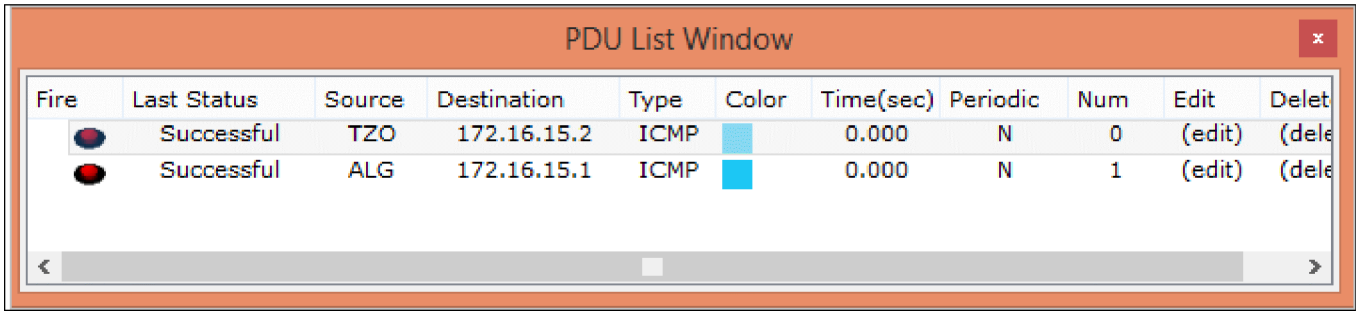


Figure IV.55: Teste de connectivite entre les interfaces série de deux sites.

IV.6.4 Teste d'ACL entre les deux sites distants (TZO, ALG)

1. Nous testons la communication entre les téléphones IP de deux sites distant (ALG et TZO) on lançon des appelles. on prend par exemple le TEL : 1502 appartenant au vlan Finance_Tizi vers le TEL : 1605 appartenant au vlan LOG_ALG

Figure IV.56: Composition de numéro de correspondent 1605

Figure IV.57: Recevoir l'appelle (suit)

.

2. Teste d' ACL entre les VLAN des deux sites distants (TZO,ALG)

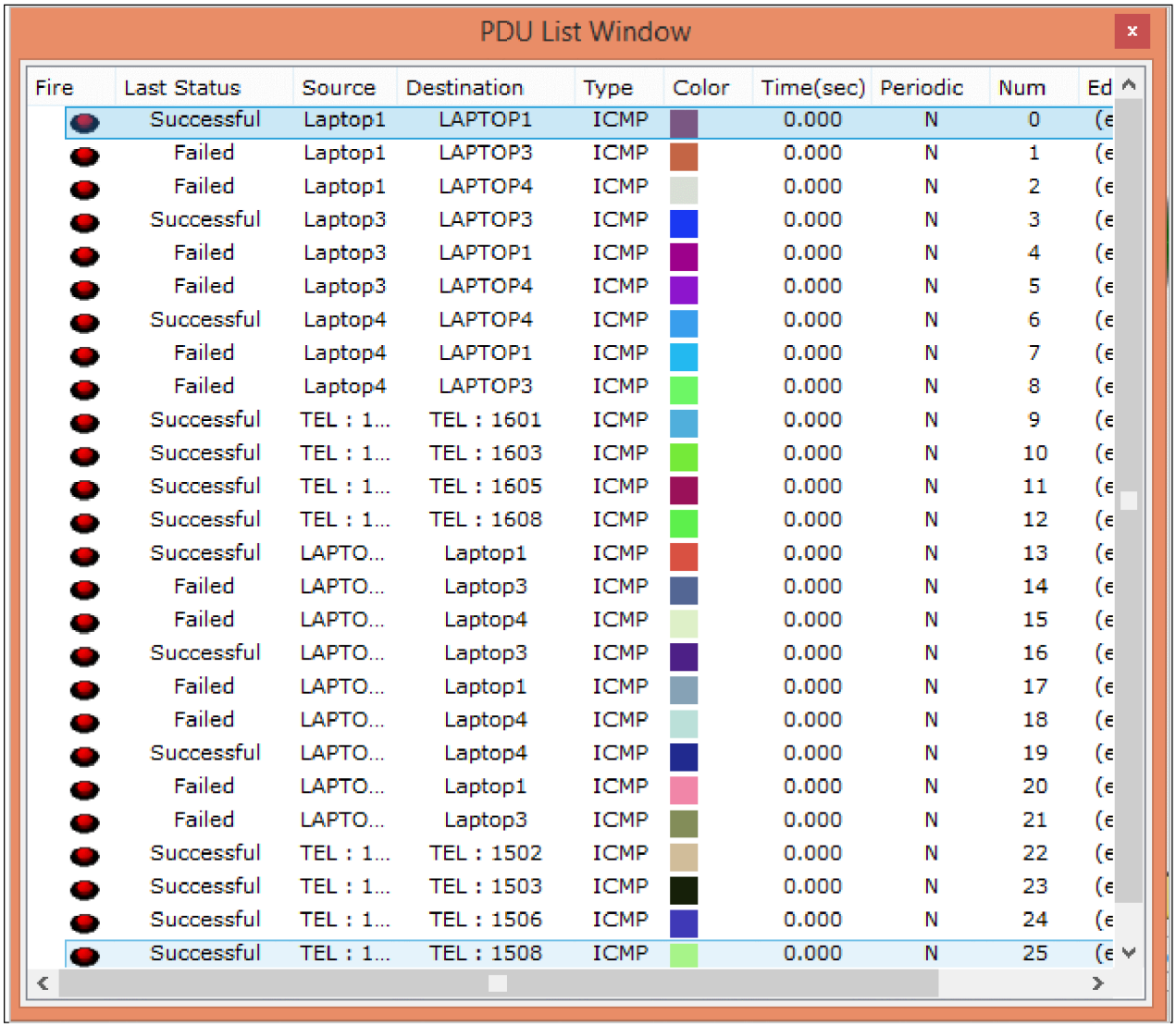


Figure IV.58 : Test entre les hôtes et téléphone IP de deux site distants

IV.7 Discutions :

Dans ce chapitre nous avons simulé notre architecture d'interconnexion basée sur la liaison spécialisée point à point avec le simulateur « Cisco Packet Tracer Intructor » comme nous avons configuré chaque équipement appartenant à ce réseau d'entreprise, avec des tests de validation . En effet les différents tests de connectivités que nous avons effectués entres les équipements des deux sites distants sont bien réussies, donc notre architecture d'interconnexion de l'entreprise basée sur la ligne spécialisée est bien conçu et fonctionne parfaitement.

Conclusion générale

Aujourd'hui, avec l'évolution de la technologie, les réseaux sont omniprésents et nous pouvons partager des applications, échanger des informations, consulter des bases de données et effectuer des transferts de fichiers entre plusieurs postes à distance.

Notre stage pratique au sein de services exploitation de la direction opérationnelle des Télécommunications d'Algérie télécom consistait à faire une étude et conception d'interconnexion de deux réseaux distants par des solutions fiables et moins couteuses. Le présent travail nous a permis de nous familiariser avec les équipements CISCO. Nous avons au passage maîtrisé la configuration des routeurs CISCO aussi bien pour la VoIP que pour le routage, le routage inter vlan la sécurité des réseaux IP, la configuration des Switchs CISCO aussi bien de la commutation que du VLAN.

En effet Dans notre projet, nous avons fait au premier lieu une conception de l'architecture d'interconnexion de l'entreprise. Notre choix s'est porté sur l'utilisation d'une ligne spécialisée qui est à la fois économique et performante pour l'entreprise. Puis, nous avons effectués la simulation réalisée à l'aide du logiciel « paquet tracer ». À cet effet, nous avons tout d'abord implémenté la topologie réseau de l'entreprise. Ensuite, nous avons effectué les configurations nécessaires et les tests de validation de la configuration.

La technologie de ligne spécialisée est fréquemment utilisée dans les entreprises souhaitant interconnecter leur site distant, vu le nombre davantage quelle offre, un transfert rapide de données, une plus grande sécurité dans les émissions/réceptions de données ainsi une communication fiable et de qualité.

Enfin, on espère que notre travail apportera une validation pratique et donnera, une bonne cause pour mieux explorer ce domaine et maitres en œuvre les possibilités réseautiques au profit des nouveaux besoins en matière de communication humaine.

Bibliographie

Bibliographie

[1] Dean, Villeneuve, Bessens, Piette etSimond.Réseaux informatique ,2e édition, Québec,Reynald Goulet Inc., 2002, 972pages.

[2] Jean-Luc Montagnier .construire son réseau d'entreprise, éditions Eyrolles. 2001.

[3] Cisco CCNA Module 1. École supérieure privée d'informatiqueSUPINFO, 2008, 68 p.

[4] Belgacem Jarray . Réseaux informatiques, adresseIP, modèle OSI, Ethernet, vlan, EditionsTechnosup, Ellipses, septembre 2014.

[5] Laurent SCHALKWIJK, André VAUCAMPS .Cisco Routage et Commutation, Réf. ENI : CE2M2CIS, octobre 2015, 622 pages.

[6] Philippe Lacurie .chapitre -10 les vlan, lycée COLLEGE RAYMONDE PONCARE, bar le duc ,2016 .

[7] Cisco Systems, CCNA 3 and 4 compagnion guide, volumes 3et 4,2003, 997 pages.

[8] Cours VLAN- SlideShare EL AMERI EL HASSAN ,2017 .

[9] Cours VTP- SlideShare EL AMERI EL HASSAN, 2017.

[10] Claude Servin .Réseau et Télécoms ,4éme édition, Dunod, paris, 2013, 800pages.

[11] Catalogue d'interconnexion d'Algérie télécoms Année 2016.

[12]Guy PUJOLLE. Les réseaux ,3ème édition Eyrolles, 2003.

❖ Sites

- http://www.cisco.com/warp/public/473/21.html http://www.cisco.com/univercd/cc/td/doc/ pro duct/lan/cat5000/rel_4_2/config/vlans.htm :Documents techniques CISCO sur le VLAN Trunking Protocol.
- http://Les Réseaux Privés Virtuels - Vpn.mht :Aperçu sur les VPN
- http://www.judoclubfirminy.fr/_CV/cisco : Tutoriel sur Cisco Paquet Tracer
- https://isrdoc.wordpress.com/category/documents-pdf-doc/ : duc et note sur les Systèmes et les réseaux.
- http://www.touslesreseaux.com : Un aperçu sur les réseaux.

ANNEXES

1. Présentation d'Algérie télécom :

1.1 Historique de l'entreprise :

Régie par la loi 2000/03 du 5 aout 2000. Algérie Télécom est née pour relever le défi de l'ouverture du marché des télécommunications annoncées par des réformes engagées par le pays. Algérie Télécom jouit d'un statut d'entreprise publique économique. Ce statut établit la forme juridique d'une société par action SPA.

Compte tenu du rôle que jouent les Télécommunications dans le développementEconomique, social, culturel, et en adéquation avec les objectifs assignés pour remplir les retards marqué dans ce domaine.Algérie Télécom a inscrit des actions multiples qu'elle doit réaliser avec succès pour répondre aux besoins de sa clientèle et assure une présentation des services et la qualité. Le challenge d'Algérie Télécom en sa qualité d'opérateur historique est d'être leader dans son domaine et nourri des ambitions de devenir un busines partenaire incontournable à l'échelle régionale et nationale.

Algérie Télécom s'est engagée comme acteur principal dans la mise en œuvre de programme de développement de société de l'information en Algérie. Compte tenu des besoins de la clientèle dans les différents segmentes des services des Télécommunications.

Algérie Télécom se propose de construire des relations d'affaires a longue terme avec les opérateurs économique intéressés par le secteur des Télécommunications et des multimédias.

1.2 Missions d'Algérie télécom :

L'activité majeur d'Algérie Télécom est de :

- ✓ Fournir les services de Télécommunication permettant le transport et l'échange de la voix, message écrit, données numériques d'information audiovisuelle… etc.
- ✓ Développer, exploiter et gérer les réseaux publics et privés des Télécommunications.
- ✓ Etablir, exploiter et gérer les interconnexions avec les opérateurs des réseaux.

1.3Objectifs d'Algérie télécom :

Algérie Télécom est engagée dans le monde des technologies de l'information et de la communication avec les objectifs suivantes :

- ✓ L'offre de service téléphonique et facilité d'accès aux services de télécommunication au plus grand nombre d'usages, en particulier en zones rurales ;
- ✓ Accroitre la qualité des services offerts de la gamme et rendre les services de Télécommunications plus compétitifs;
- ✓ Développer un réseau national de Télécommunication fiable et connecter aux autoroutes de l'information.

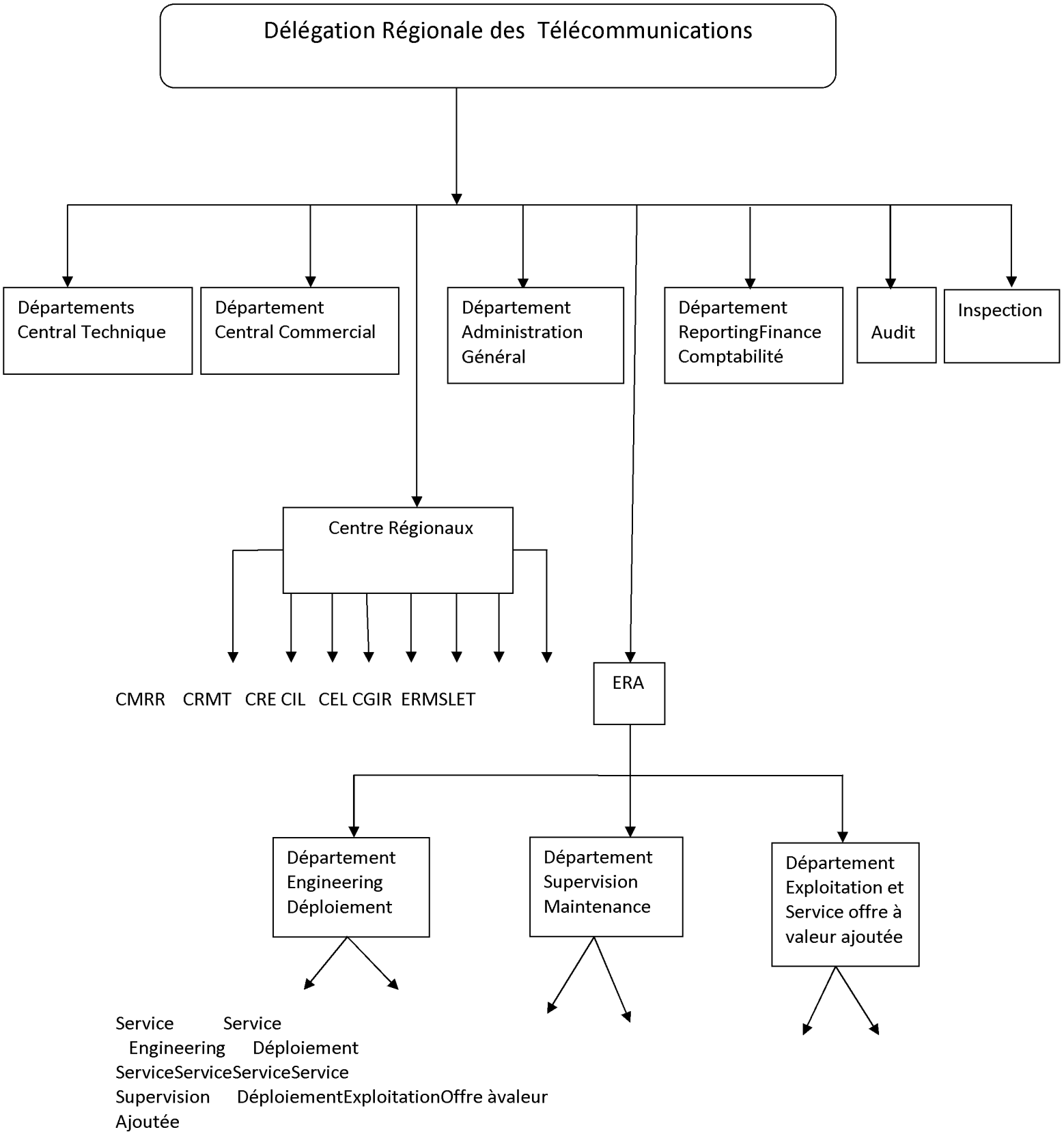
1.4 Organisation d'Algérietélécom :

Algérie Télécom est organisée en direction centrales, régionale et directions opérationnelles de wilaya auteur de ses métiers fixes et services, et d'autre part des fonctions supports réseaux. A cette structure s'ajoutent trois filiales spécialisées et de dimension nationales.

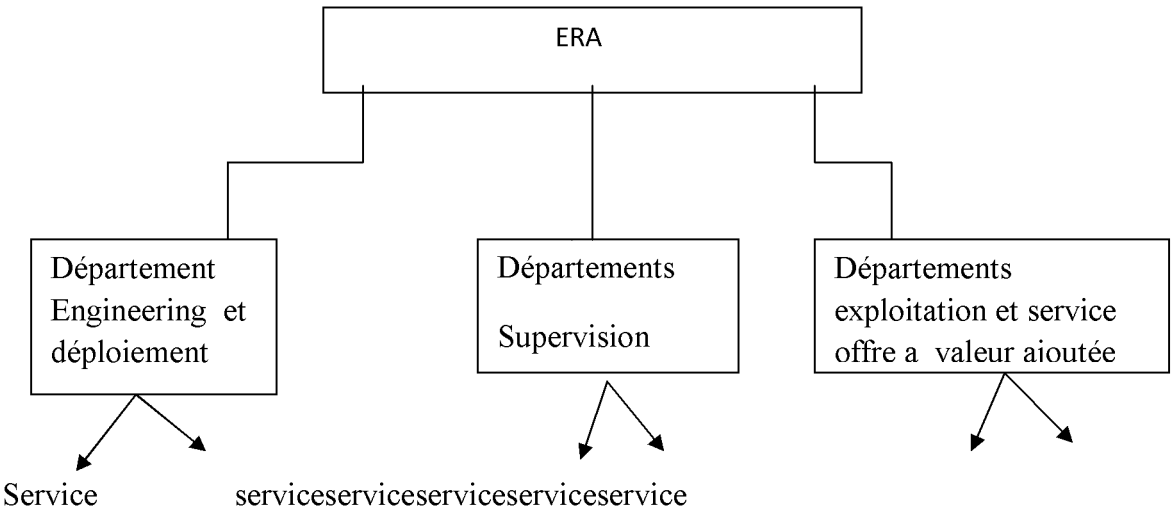
- La filiale de téléphonie mobile « Algérie Télécom mobile : Mobilis »
- La filiale des télécommunications par satellite « Algérie Télécom Satellite : ATS »
- La filiale des services internet « Algérie Télécom Internet DJAWEB : ATI »

Algérie Télécom s'implique dans le développement socio-économique du pays à travers la fourniture des services de Télécommunication. En outre, elle met en œuvre des moyens importants pour rattacher les localités isolées

2. Organigramme de la structure d'accueil (Délégation Régionale des Télécommunications) **:**



2.1Organigramme de département d'accueil (ERA) :



2.1.1.Mission des différents services de département d'accueil :

a. Service engineering

- Suivi de l'étude des sites destinée a l'implantation des équipements.
- suivi de la préparation de l'environnement (l'énergie, abri, transport FH)
- suivi de l'installation et mise en service de l'équipement

b. Service déploiement

- Etude et définition des besoins des dots en termes d'accès.
- Réception des équipements et leur dispatching sur site.
- Préparation et suivi des installations des équipements.
- configuration et mise en service des équipements réseaux.

c. Service maintenance

- Intervention et maintenance de niveau 1&2.
- Elaboration et prise en charge d'un programme périodique pour une maintenance préventive de tous équipements.
- Relever des dérangements et traitement des anomalies soft et hardware

d. Service supervision

- Supervision des équipements et des liaisons.
- Analyse, interprétation et prise en charge des alarmes observées sur les outils de supervision.
- Support et assistance aux structures régionales.
- signalisation des alarmes, en temps réel, aux différents acteurs concerner soit pour intervention et/ou pour information sur le dysfonctionnement.

e. Service exploitation

- Assistance permanente aux départements haut débit.
- Traitement et suivi des réclamations.
- Suivi de la situation des raccordements.

f. Service offre à valeur ajoutée

- Etude d'éligibilité et intégration des réseaux professionnels (intranet, VPN….)
- prise en charge, en collaboration avec les entités d'AT, tout dysfonctionnement des sites réaliser.