République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane Mira BEJAIA

Faculté des Sciences exactes

Département Informatique

En vue de l'obtention du diplôme Master en Informatique

Option : Administration et sécurité des réseaux

Mémoire de fin de cycle

Thème :

Proposition et mise en œuvre d'une solution de segmentation et de routage du réseau LAN étendu de la RTC Bejaia (Région Transport Centre) Sonatrach BEJAIA.

Réalisé par:

OUSSALAH Billal

REDOUANE Salim

Devant le jury composé de:

Président: M^{r} KHIRDINE Abdelkrim

Examinateurs: M^{r} LARBI Ali

M^{me} BENSAID Samia

Promoteur: M^{r} TOUAZI Djoudi

Co-Promoteur: M^{r} FELLFOUL Allaoua

Année universitaire: 2011-2012

Dédicace

Au nom d'ALLAH le tout puissant, miséricordieux, qu'avec son aide que les choses s'accomplissent.

Je dédie ce modeste travail

A mon cher père : Smail, qui a veillé sur moi durant toute étape de ma vie, qui m'a offert toute chose, seulement pour que je sois bien et heureux et qui m'a fait apprendre les bons principes.

A la personne, que j'aurais aimé qu'elle soit présente, qu'ALLAH l'accueille dans son vaste paradis. Ma chère mère.

A ma belle mère : Zineb, qu'ALLAH lui donne de la force et du courage.

A tous mes frères: Ali, Mamou et Rafik. Toutes mes sœurs : Sonia, Hakima et Kahina. Mes demi-sœurs. Ainsi qu'à mes neveux et mes nièces.

A ma grande mère : Houria, qu'ALLAH lui donne de la santé et du bonheur.

A ma tante : Zaoua, qui m'a offert de l'amour et du soutien, qu'ALLAH la protège.

A ma grande tante : Takhlit, qui j'aime vraiment et fortement, qu'ALLAH lui offre sa paix et sa tranquillité.

A ma tante : Zorha, qui était et est toujours comme une mère pour moi, et qui m'a fait sentir l'amour et la sérénité, qu'ALLAH nous la laisse saine et sauve.

A tous mes oncles, mes tantes, mes cousins et cousines.

A tous mes amis et mes camarades, ainsi, que tous les gens que je connaisse ou qui me connaissent.

Billal.

Dédicaces

Je dédie ce modeste travail et ma profonde gratitude à toute ma grande famille et à mes proches amis, Qu'ils trouvent ici l'expression de ma reconnaissance :

À mes très chers grands-parents.

À mes très chers parents, pour leurs amour et sacrifices.

Je le dédie aussi à tous mes oncles et tantes.

À mes adorables frères, sœur pour leur patience.

À chaque cousins et cousines.

Je le dédie particulièrement à la mémoire de mon oncle Omar, et qu'Allah t'ouvre les portes du paradis.

À mes meilleurs amis.

A mon binôme Billal et sa famille.

À tous les étudiants de la promotion informatique de l'université de Béjaïa.

Enfin je le dédie à tous mes amis et à tous ceux qui me connaissent.

J'exprime mes sentiments les plus profonds et leur dédie mon humble travail.

Salim.

Remerciements

En premier lieu et avant tout, nous remercions ALLAH Tout-puissant de nous avoir donné la force et le courage pour la réalisation de ce travail et qui nous a procuré ce succès.

Un chaleureux merci pour notre cher promoteur Mr D.TOUAZI qui est d'ailleurs notre enseignant, d'avoir accepté de nous encadrer tout au long du semestre, et de travailler avec nous pour la réalisation de ce projet.

Un grand merci pour l'organisme d'accueil SONATRACH, qui nous a accepté comme stagiaires et qui nous a donné une chance pour découvrir le domaine professionnel. Ainsi, que pour tous les travailleurs qui nous ont aidés de prés ou de loin durant notre période du stage.

Nos vifs et particuliers remerciements du plus profonds de nos cœurs, vont droit vers Mr A.FELFOUL chef service du centre informatique de SONATRACH, d'un premier lieu pour son chaleureux accueil et son acceptation de nous encadrer même si la surcharge de son travail ne l'avait pas permise. D'un second lieu, pour son suivi, ses conseils prodigués et ses bonnes orientations qui ont été vraiment une voie éclairée durant notre projet, et qui a su nous faire profiter de sa vaste expérience.

Nos sincères gratitudes, aux membres du jury pour leur accord à faire participer de la commission d'examinateurs.

Nos sincères reconnaissances pour tous nos enseignants, qui nous ont transmis fidèlement leur savoir et qui nous ont appris le vrai sens de: étudier.

Enfin, nous tenons à exprimer nos meilleurs remerciements à nos parents, nos frères et sœurs, ainsi, que toute personne qui nous a soutenus et encouragés

Billal & Salim

Table des matières

Table des matières i

Liste des Figures v

Liste des Tableaux vii

Liste des Abréviations viii

Introduction Générale……1

Chapitre I : ETAT DE L'ART SUR LES RESEAUX INFORMATIQUES.

Introduction 3
1. Définition d'un réseau 3
2. Modèle OSI (Open System Interconnection) 3
3. L'adressage IP 5
3.1. Le protocole IP 5
3.2. Définition d'une adresse IP 5
3.3. Le masque réseau 6
3.4. Les classes des adresses IP 6
3.4.1. Classe A 6
3.4.2. Classe B 6
3.4.3. Classe C 7
3.4.4. Classe D 7
3.4.5. Classe E 7
3.5. Les adresses Spécifiques 8
3.5.1. Adresse privée 8
3.5.2. Adresse de diffusion 8
4. Le routage 8
4.1. Définition d'une route 9
4.2. Les types de routes 9

4.3. La table de routage 9
4.4. Les types de routage 9
4.4.1. Routage statique 10
4.4.2. Routage dynamique 10
4.5. Les protocoles de routage 10
4.5.1. Les protocoles de routage à vecteur distance 11
4.5.2. Les protocoles de routage à état des liens 13
5. Le modèle hiérarchique en trois couches de Cisco 15
5.1. La couche cœur « Core layer » 16
5.2. La couche Distribution « Distribution layer » 16
5.3. La couche Accès« Access layer » 17
Conclusion 18

Chapitre II: ETAT DES LIEUX DE L4ORGANISME D'ACCUEIL.

Introduction 19
1. Présentation de l'organisme d'accueil 19
1.1. Objectifs et évolution 19
1.2. Activités de la SONATRACH 20
1.3. L'organigramme de la SONATRACH 20
1.4. Présentation de la DRGB (Direction Régionale de Bejaia) 21
1.4.1. Les activités 21
1.4.2. Les différents départements 22
1.4. 3. Les stations de pompage et de compression 23
2. Présentation du réseau informatique de la RTC Bejaia 24
3. Design d'un LAN type d'une station 26
5. Problématique 27
6. Solutions proposées 27
Conclusion 28

Chapitre III: ETUDE DES SOLUTIONS PROPOSEES.

Introduction 29
1. Segmentation VLAN 29
1.1. Les avantages VLAN 29

1.2. Critères de regroupement dans un VLAN 30
1.3. Méthode d'implémentation des VLANs 35
2. Interconnexion du réseau 38
2.1. Choix du protocole de routage 40
Conclusion 41

Chapitre IV: PLANIFICATION DES SOLUTIONS.

Introduction 42
1. Présentation de l'architecture réseau 42
2. Présentation des équipements utilisés 43
3. Segmentation VLAN 43
4. Plan de nommage 44
4.1. Nominations des équipements 45
4.2. Désignations des interfaces 45
4.3. Nomination des VLANs 46
5. Protocole VTP (VLAN Trunking Protocol) 46
6. Trafic Entre-VLAN 47
7. Plan d'adressage 48
7.1. Adressage des VLANs 49
7.2. Administration des équipements 50
7.3. Adressage des PCs et serveurs 50
8. Plan de Routage 51
Conclusion 53

Chapitre V: MISE EN ŒUVRE ET REALISATION.

Introduction 54
1. Présentation du simulateur Cisco « Packet Tracer » 54
2. Interface commande de Packet Tracer 55
3. Configuration des équipements 56
3.1. Configuration des commutateurs 56
3.1.1. Configuration du Hostname 57
3.1.2. Configuration des VLANs 58
3.1.3. Configuration du protocole VTP 58

3.1.4. Configuration des interfaces VLAN 60
3.1.5. Configuration des interfaces 60
3.1.6. Attribution des ports des commutateurs aux VLANS 61
4. Configuration des routeurs 63
4.1. Subdivision de l'interface routeur-commutateur Distribution 63
4.2. Configuration des interfaces du routeur 64
4.3. Configuration du routage 66
5. Configuration des PCs et des serveurs 69
6. Les tests de validation 71
6.1. Vérifier la communication entre les équipements d'interconnexion 71
6.2. Vérifier la communication entre les PCs 74
Conclusion 76

Conclusion Générale et perspectives 77

Bibliographie 79

A1 Annexe A1 i
A1.1. Principe de fonctionnement des VLANs i

A2 Annexe A2 ii
A2.1. Description de la norme ii
A2.2. La norme 802.1Q ii

A3 Annexe A3 iv
A3.1. Le protocole VTP (Virtual Trunking Protocol) iv
A3.2. Les modes VTP iv
A3.3. Configuration des modes VTP iv

Liste Des Figures

Figure I.1 : Le modèle OSI. 4
Figure I.2 : Caractéristiques des classes des adresses IP. 7
Figure I.3 : Envoi périodique de copies d'une table de routage aux routeurs voisins et cumul des vecteurs distance. 11
Figure I.4 : Diffusion d'informations de routage entre les routeurs 13
Figure I.5 : Modèle hiérarchique Cisco en trois couches. 15
Figure I.6 : Couche Cœur « Core Layer » 16
Figure I.7 : Couche Distribution « Distribution Layer ». 17
Figure I.8 : Couche Accès « Access Layer » 18
Figure II.1 : Organigramme de SONATRACH. 20
Figure II.2 : Architecture physique du réseau de la RTC. 24
Figure II.3 : Architecture logique point-multipoints du réseau de la RTC. 25
Figure II.4 : Architecture de la station SP3. 26
Figure II.1 : VLANs par services. 31
Figure II.2 : VLANs par emplacement géographique. 34
Figure II.3 : VLAN niveau 1. 35
Figure II.4 : VLAN niveau 2. 36
Figure II.5 : VLAN niveau 3. 37
Figure IV.1 : Architecture de la station SP3. 42
Figure IV.2 : Les différents VLANs du réseau SP3. 44
Figure IV.3 : Les liens du Trunk. 48
Figure IV.4 : Les routeurs du Backbone de la RTC Bejaia. 52
Figure V.1 : Cisco Packet Tracer. 55
Figure V.2 : Interface CLI. 56
Figure V.3 : Nommer le Switch Distribution. 57
Figure V.4 : Création des VLANs. 58
Figure V.5 : Configuration des VTP-Server. 59
Figure V.6 : Configuration Client-VTP. 59
Figure V.7 : Configuration des interfaces VLANs. 60
Figure V.8 : Configuration des liens trunk. 61
Figure V.9 : Attribution des ports aux VLANs. 62

Figure V.10 : Attribution des ports au VLAN Server. 63
Figure V.11 : Subdivision de l'interface routeur. 64
Figure V.12 : Configuration des interfaces routeur. 65
Figure V.13 : Routage au niveau du routeur DRGB. 66
Figure V.14 : Routage au niveau du routeur SP3. 66
Figure V.15 : Routage au niveau du routeur SP1 Bis. 67
Figure V.16 : Routage au niveau du routeur SP2. 67
Figure V.17 : Routage au niveau du routeur SBM. 68
Figure V.18 : Routage au niveau du routeur SC3. 68
Figure V.19 : Routage au niveau du routeur GG1. 69
Figure V.20 : Attribution d'adresse IP aux PCs. 70
Figure V.21 : Attribution d'adresse aux serveurs. 70
Figure V.22 : Test entre le Switch Accès et le Switch Distribution. 71
Figure V.23 : Test entre les Switchs Accès. 72
Figure V.24 : Test entre routeur et Switch Distribution. 72
Figure V.25 : Test entre routeur et Switch Accès. 73
Figure V.26 : Test des routeurs distants. 73
Figure V.27 : Test entre PC d'un même LAN et VLAN. 74
Figure V.28 : Test entre machines des VLANs distincts. 75
Figure V.29 : Test entre PC de même VLAN mais différent LAN. 75
Figure V.30 : Test entre PC de VLAN et LAN différents 76
Figure A2.1 : Extension de la trame Ethernet modifiée par la norme 802.1Q. ii

Liste Des Tableaux

Tableau I.1 :Comparaison entre RIPv1 et RIPv2. 12
Tableau II.1: Ouvrages de la DRGB / SONATRACH. 21
Tableau II.2: Les bâtiments de SP3 26
Tableau III.3 : Les différentes techniques d'implémentation VLAN. 38
Tableau IV.1: Liste des équipements utilisés. 43
Tableau IV.2 : Nom des équipements de la station SP3. 45
Tableau IV.3: Liste des interfaces.. 45
Tableau IV.4: Liste des noms de interfaces.. 46
Tableau IV.5: Désignation VTP.. 47
Tableau IV.6 : Plan d'adressage des VLANs. 49
Tableau IV.7 : Plan d'adressage du VLAN natif. 50
Tableau IV.8 : Plan d'adressage des PCs et serveurs 50
Tableau IV.9 : Réseaux interconnectés directement aux routeurs. 52

Les abréviations

ACL: Access Control List.

AS: System Autonomous (Système Autonome).

CBAC: Context Based Access Control.

CFI : Canonical Format Identifier

C F PA: Compagnie Française des Pétroles Algérie.

CLI: Command Line Interface.

DML: Direction Maintenace Laghouat.

DRGB: Direction Régionale de Bejaia.

EIGRP: Exterior Gateway Routing Protocol.

GEM: Gazoduc Enrico Mattei (Italie)

GNL: Gaz Naturel Liquéfié.

GPDF: Gazoduc Pedro Farel (Espagne)

GPL: Gaz Pétrole Liquide.

Host-ID: Host Identification.

IETF: Internet Engineering Task Force.

IGRP: Interior Gateway Routing Protocol.

IP: Internet Protocol.

ISO: International Standards Organization.

LAN: Local Area Network.

LSA: Link-State Advertisement.

Mbps: Mega Bits Par Second.

Net-ID: Network Identification.

OSI: Open System Interconnexion.

OSPF: Open Shortest Path First.

RIPv1: Routing Information Protocol Version1.

RIPv2: Routing Information Protocol Version2.

RTC: Region Transport Centre (Bejaia).

RTE: Region Transport Est (Skikda).

RTH: Region TransportHoud-El-Hamra.

RTI: Region Transport In Amenas

RTO: Region Transport Ouest (Arzew).

S N R E P AL: Société Nationale de Recherche et Exploitation des Pétroles en Algérie.

SONATRACH: Société Nationale de Transport et Commercialisation des Hydrocarbures.

SOPEG : Société Pétrolière de Gérance.

SubNet: Subdivision Network.

TEP : Tonne équivalent pétrole.

VID: VLAN IDentificateur.

VLAN: Virtual Local Area Network.

VLSM: Variable Length Subnet Masque.

VTP: Vlan Trunking Protocol.

WAN: Wide Area Network.

Introduction Générale

Un réseau informatique peut être vu comme un ensemble de ressources mises en place pour offrir un ensemble de services. Pour parvenir à une meilleure gestion de leurs ressources et informations, nombreuses sont les entreprises qui se sont dotées d'un réseau. Bien que la croissance d'une entreprise soit généralement souhaitée, elle s'accompagne d'un certain nombre de contraintes, telle que l'augmentation rapide du nombre d'utilisateurs, résultant ainsi, un volume accru du trafic généré par ces derniers. Par conséquent, problèmes de baisse des performances du réseau. Donc, une bonne organisation du réseau remédiera à ces problèmes.

Conscient de ces problèmes que rencontrent bon nombre d'entreprises. C'est ainsi que dans le cadre de projet «PROPOSITION ET MISE EN ŒUVRE D'UNE SOLUTION DE SEGMENTATION ET DE ROUTAGE DU RESEAU LAN ETENDU DE LA RTC (REGION TRANSPORT CENTRE) SONATRACH BEJAIA», pouvant apporter des solutions efficaces pour une bonne organisation du réseau de l'entreprise.

La région RTC Bejaia (Région Transport Centre) de SONATRACH, est une région qui gère des pipe-lines (canalisation) de Gaz et de Pétrole provenant du sud algérien. Elle dispose de deux pipe-lines de Pétrole et un pipe-line de Gaz. Tel que, tout au long de ses canalisations, des stations de pompage et de compression équipées d'un personnel veillant à la continuité du travail, sont reliées à RTC Bejaia. Pour acheminer le trafic entre la direction et les stations, la notion du réseau informatique est adaptée. Chaque station dispose d'un LAN et l'interconnexion de tous ses LANs, constitue le réseau informatique de la région RTC.

L'objectif de notre travail, est d'organiser les réseaux locaux des stations, en proposant une solution pour cette dernière et en adoptant un plan d'adressage pour chacun d'eux, afin que la communication au niveau d'une station aura lieu. En outre, Proposer une solution qui permettra la communication entre les différentes stations entre elles et entre la direction de Bejaia. A vrai dire, c'est de proposer une solution de routage entre les sites distants.

Le présent document est composé de cinq chapitres:

Le premier, définit quelques notions théoriques de base, qui aideront et seront utiles pour la compréhension de la problématique posée, à savoir la définition d'un réseau, l'adressage IP et le routage. Le deuxième, porte sur la présentation de l'organisme d'accueil, en indiquant quelques informations nécessaires, comme les départements qui existent, ainsi que la présentation du réseau informatique. Le troisième, fera l'objet de l'étude des solutions proposées, et les critères qui ont poussés à les adopter. Le quatrième chapitre, c'est la partie planification, qui constitue les différents plans pour mettre en œuvre les solutions. Enfin, le dernier chapitre, qui est la partie mise en œuvre et réalisation, contenant toutes les configurations appliquées pour les solutions, ainsi que des tests de validation pour vérifier si vraiment les objectifs ont été atteints.

En fin, le travail se clôturera par une conclusion générale, décrivant les points essentiels développés dans ce projet, ainsi, de donner quelques perspectives pour une prochaine version.

CHAPITRE I

ETAT DE L'ART SUR LES RESEAUX INFORMATIQUES

Introduction

Pour bien mener son projet sur l'organisation et l'interconnexion des réseaux, comprendre les notions de bases sur les réseaux informatiques est très important, afin de bien maitriser son sujet.

L'objectif de ce chapitre est de présenter quelques concepts de bases sur les réseaux informatiques, pour bien aider à mieux assimiler le fonctionnement des réseaux. Donc, toutes les notions nécessaires seront présentées, tirant exemple de l'adressage IP avec les classes d'adresses, le routage et les protocoles de routage, ainsi qu'une description du modèle Cisco hiérarchique.

1. Définition d'un réseau :

Un réseau (network) est un ensemble des moyens matériels et immatériels mis en œuvre pour assurer les communications entre ordinateurs, stations de travail et terminaux informatiques.

Les réseaux informatiques permettent aux utilisateurs de communiquer entre eux et de transférer des informations. Ces transmissions de données peuvent concernées l'échange de messages entre utilisateurs, l'accès a distance aux bases de données ou encore le partage de fichiers.

Un réseau local (Local Area Network) est un réseau informatique a une échelle géographique relativement restreinte, il est utilisé pour relier entre eux les ordinateurs : par exemple d'une habitation particulière, d'une entreprise, d'une salle informatique et d'un bâtiment. L'infrastructure est privée et est gérée localement.

Les LANs classiques offrent des débits de l'ordre de Mbps sur de courtes distances, les plus évolués permettent d'atteindre 100Mbps, les réseaux à 1Gbpas sont même annoncés aujourd'hui.

2. Modèle OSI (Open System Interconnection):

Pour faciliter l'interconnexion des systèmes, un modèle dit d'interconnexion des systèmes ouverts, appelé encore OSI (Open System Interconnection) a été défini par ISO (International Standards Organization).

Le modèle OSI décrit un ensemble de spécifications pour une architecture réseau permettant la connexion d'équipements hétérogènes. Le modèle OSI normalise la manière

dont les matériels et les logiciels coopèrent pour assurer la communication réseau. Ce modèle est organisé en sept couches successives, comme l'indique la figure I.1 :

Figure I.1 : Le modèle OSI.

- ✓ Couche physique : Cette couche gère la transmission des bits sur un support physique.
- ✓ Couche liaison de données : Cette couche assure le contrôle de la transmission des données, elle gère la fiabilité du transfert de bits d'un nœud à un autre du réseau, comprenant entre autres les dispositifs de détection et correction d'erreurs, ainsi que les systèmes de partage des supports. L'unité de données à ce niveau est appelée trames.
- ✓ Couche réseau : Cette couche assure la transmission des données sur les réseaux. C'est ici que la notion de routage intervient, permettant l'interconnexion de différents réseaux. En plus du *routage*[1], cette couche assure la gestion des *congestions*[2]. L'unité de données a ce niveau est appelée paquet.
- ✓ Couche transport : Cette couche gère le transport fiable des paquets de bout en bout.

[1] Le routage est la fonction qui s'occupe de diriger les données réseaux à travers différents segments.
[2] La congestion d'un réseau informatique est la condition dans laquelle une augmentation du trafic provoque un ralentissement global de celui-ci.

- ✓ Couche session : Cette couche assure l'établissement, maintien et la terminaison des sessions de communication.
- ✓ Couche présentation : conversion de données en un format standard. A ce niveau il y a la *compression*[3] et *cryptage*[4] de données.
- ✓ Couche application : Cette couche est source et destination de toutes les informations à transporter, elle rassemble toutes les applications qui ont besoin de communiquer par les réseaux : messagerie électronique, transfert de fichiers, gestionnaire de base de données, etc.

3. L'adressage IP :

L'adressage IP est un adressage logique réseau et non plus physique, c'est-à-dire un adressage non de la couche 2 mais, un adressage de couche 3. Il comporte les adresses IP, les classes d'adresses ainsi les masques réseaux.

3.1. Le protocole IP :

Le protocole IP (Internet Protocol) s'agit d'un protocole réseau (niveau 3 dans le modèle OSI). Le protocole IP permet d'émettre des paquets d'informations à travers le réseau, il est utilisé pour dialoguer les machines entre elles, ainsi, il offre un service d'adressage unique pour l'ensemble des machines.

3.2. Définition d'une adresse IP :

L'adresse IP est une adresse de 32 bits, répartie en 4 fois 8 bits (octet). Cette adresse est un identifiant réseau. On peut ensuite, la diviser en 2 portions : la portion du réseau et la portion hôte. La première identifie le réseau sur lequel est la machine et la deuxième identifie les machines en elles-mêmes. Pour identifier ces deux parties chaque adresse est liée à un masque de sous-réseau ce qui permet de définir sur quel réseau elle se trouve. [A]

Le format binaire d'une adresse IP est comme suit :

xxxxxxxx . xxxxxxxx .xxxxxxxx. xxxxxxxx (tel que x=0 ou x=1).

[3] C'est l'opération informatique qui consiste à transformer une suite de bits A en une suite de bits B plus courte, contenant les mêmes informations, en utilisant un algorithme particulier.
[4] Processus consistant à convertir des données de texte simple en texte crypté compréhensible seulement par les disposants de la clé de cryptage.

3.3. Le masque réseau :

Le masque de réseau sert à séparer les parties réseau et hôtes d'une adresse. On retrouve l'adresse du réseau on effectuant un ET logique bit à bit entre une adresse complète et le masque du réseau.

3.4. Les classes des adresses IP :

Le but de la division des adresses IP en classes, est de facilité la recherche d'un ordinateur sur le réseau. En effet, avec cette notation il est possible de rechercher dans un premier temps le réseau à atteindre puis de chercher un ordinateur sur celui-ci. Ainsi, l'attribution des adresses IP se fait selon la taille du réseau.

En effet, il existe 5 classes des adresses IP, à savoir : classe A, classe B, classe C, classe D et classe E, telle que, chaque classe a un format spécial de son adresse IP. « Adresse réseau et adresse machine ».

3.4.1. Classe A :

Le premier octet est utilisé pour l'adresse *Net-ID*[5], il varie de 1 à 126. Les deuxième, troisième et quatrième octets sont utilisés pour le *Host-ID*[6].

Une adresse de classe A à la forme : R1 .m1 .m2 .m3 (R : Net-ID, m : Host-ID)

Bits de R1 : 0xxxxxxx ou X=0 ou X=1 00000000<=R1<= 01111111

0<=R1<=127 0<=mi<=255

3.4.2. Classe B :

Les premiers et deuxièmes octets sont utilisés pour l'adresse Net-ID, ils varient de 128.0 à 191.255. Les troisièmes et quatrièmes octets sont utilisés pour les adresses Host-ID.

L'adresse de cette classe est comme suit : R1 .R2 .m1 .m2

Bits de R1 : 10xxxxxx ou X=0 ou X=1 10000000<=R1<= 10111111

128<=R1<=191 0<=mi<=255

[5] C'est la partie identificateur du réseau.
[6] C'est la partie identificateur de la machine ou host.

3.4.3. Classe C :

Les premiers, deuxièmes et troisièmes octets sont utilisés pour l'adresse Net-ID, ils varient de 192.0.0 à 223.255.255. Le quatrième est utilisé pour l'adresse Host-ID.

L'adresse IP de classe C a le format : R1 .R2 .R3 .m1

Bits de R1 : 110xxxxx ou X=0 ou X=1 11000000<=R1<= 11011111

192<=R1<=223 0<=m1<=255

3.4.4. Classe D :

La classe D est ce qu'on appelle Multicast, c'est-à-dire qu'elle est destinée à faire de la diffusion d'information sur plusieurs Hôtes (groupe d'Hôtes) simultanément. Le premier octet a une valeur comprise entre :

224= (11100000) et 239=(11101111).

3.4.5. Classe E :

La classe E n'est pas utilisée pour adresser des hôtes ou des groupes d'Hôtes. Le premier octet a une valeur comprise entre :

240= (11110000) et 255=(11111111).

La figure I.2 éclaircie les différentes caractéristiques des classes d'adresses IP :

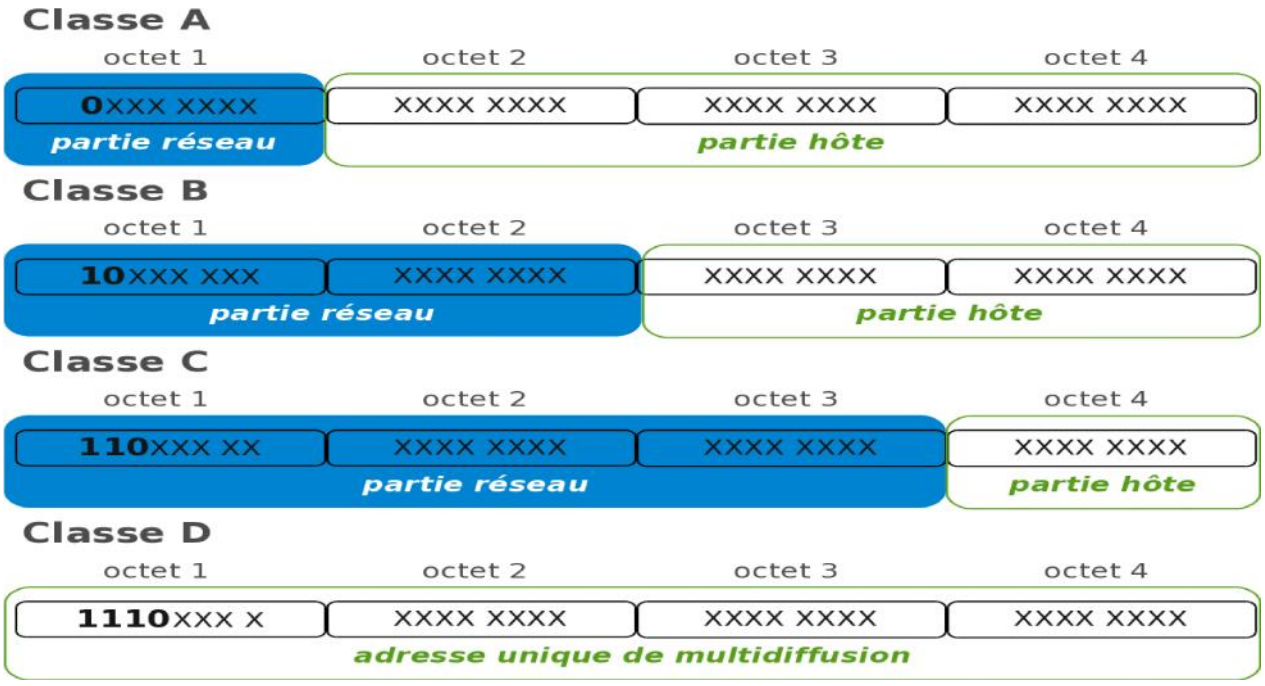

Figure I.2 : Caractéristiques des classes des adresses IP.

3.5. Les adresses Spécifiques :

Dans l'ensemble des adresses IP, il existe certaines adresses qui sont spécifiques, c'est-à-dire, qu'elles ont un usage particulier. Parmi ces adresses, citant : Les adresses privées et les adresses de diffusion.

3.5.1. Adresse privée :

Il existe des adresses privées, dans chaque classe :

- ✓ A --> 10.0.0.0 à 10.255.255.255
- ✓ B --> 172.16.0.0 à 172.31.255.255
- ✓ C --> 192.168.0.0 à 192.168.255.255

Une adresse IP privée n'est pas visible sur internet, au contraire d'une IP publique. On emploie les adresses privées à l'intérieur du réseau et les adresses publiques sont des adresses internet. En interne, il y aura donc un routeur qui va dire ou aller pour rejoindre une adresse publique. On peut accéder à une adresse publique depuis n'importe ou dans le monde alors qu'on ne pourra jamais arriver sur une adresse privée sans être dans le même réseau qu'elle ou à moins de réussir à pirater le réseau. [A]

3.5.2. Adresse de diffusion :

L'adresse de diffusion est utilisée pour envoyer un message à toutes les machines d'un réseau. Elle est obtenue en mettant tous les bits de l'host-id à 1. Il existe aussi l'adresse de Broadcast " générale ", cette adresse permet l'envoi d'un message vers toutes les machines de tous les réseaux connectés. Le routeur quand il reçoit une adresse de Broadcast, va envoyer le message dans tous les périphériques du réseau concerné.

4. Le routage :

Le routage est la fonction qui s'occupe de diriger les données réseaux à travers différents segments. Il va les diriger jusqu'au prochain point de route. Cette fonction emploie des algorithmes de routages et des tables de routage (carte routière en quelque sorte). Le

principal périphérique de routage est le routeur. Il utilise les adresses IP pour diriger correctement les paquets d'un réseau ou segment à un autre. Il doit maintenir sa table de routage à jour et connaître les changements effectués sur les autres appareils par lequel il pourrait faire transiter le paquet.

Pour remplir et mettre à jour la table de routage, il y a deux manières de faire, on peut le faire soit manuellement soit de manière dynamique, en employant des processus tournant sur le réseau. [A]

4.1. Définition d'une route :

Une route c'est le chemin existant entre deux extrémités (source et destination) à travers laquelle les paquets sont envoyés.

4.2. Les types de routes :

Il existe trois types de routes :

- ✓ Route statique : Les routes statiques sont programmées manuellement par l'administrateur du réseau qui les enregistre dans la configuration d'un routeur;
- ✓ Route dynamique : les routes dynamiques, sont apprises d'un protocole de routage dynamique dont le rôle est de diffuser les informations concernant les réseaux disponibles; [B]
- ✓ Route par défaut : La route par défaut est la route qui sera utilisée lorsqu'aucune route spécifique pour aller vers la destination spécifiée n'aura été trouvée.

4.3. La table de routage :

La table de routage est un regroupement d'informations permettant de déterminer le prochain routeur à utiliser pour accéder à un réseau précis sur lequel se trouvera la machine avec laquelle nous souhaitons dialoguer. [D]

4.4. Les types de routage :

La notion de routage dynamique ou statique illustre la manière dont une table de routage d'un routeur est construite. Il existe deux grandes méthodes :

4.4.1. **Routage statique** :

Le routage statique est un principe de routage programmé par l'administrateur de réseau, afin de déterminer le chemin que doit emprunter un paquet pour atteindre sa destination. L'administrateur doit faire la gestion des routes de chaque unité de routage de réseau, les chemins statiques ne s'adaptent pas aux modifications des environnements réseau, l'administrateur doit mettre a jour manuellement les entrées de routes statique chaque fois qu'une modification de la topologie du réseau le nécessite. Les routes statiques sont utilisées le plus souvent pour des raisons de sécurité.

4.4.2. **Routage dynamique** :

Lorsqu'un réseau atteint une taille assez importante, il est très lourd de devoir ajouter les entrées dans les tables de routage à la main. La solution est le routage dynamique. Cela permet de mettre à jour les entrées dans les différentes tables de routage de façon dynamique.

Dans le routage dynamique, les tables sont remplies automatiquement. Un protocole configuré va se charger d'établir la topologie et de remplir les tables de routage. Le routage dynamique permet une modification automatique des tables de routage en cas de rupture d'un lien sur un routeur, il permet également de choisir la meilleure route disponible Pour aller d'un réseau à un autre.

4.5. Les protocoles de routage :

Tous les protocoles de routage ont pour objectif de maintenir les tables de routage du réseau dans un état intègre et cohérent. Pour y parvenir, les protocoles diffusent des informations de routage aux autres systèmes du réseau afin de transmettre les modifications des tables de routage. Ces protocoles réceptionnent en contrepartie les informations de routage d'autres systèmes du réseau afin de mettre à jour les tables de routage. [2]

Un protocole de routage sert à améliorer la vitesse de routage, à gagner du temps en évitant de devoir configurer manuellement toutes les routes sur chaque routeur, à améliorer la stabilité du réseau en choisissant chaque fois la meilleure route.

Les protocoles de routage peuvent être classés dans deux catégories :

- ✓ Les protocoles à vecteur de distance (Distance Vector) ;
- ✓ Les protocoles à état de lien (Link State).

4.5.1. Les protocoles de routage à vecteur distance :

Un routeur mettant en jeu un protocole à vecteur-distance se contente d'avertir les autres routeurs directement connectés sur ses interfaces, de la totalité des réseaux qu'il sait atteindre, ainsi que de la distance à laquelle ils se trouvent. Chacun des routeurs qui reçoit cette information la stocke dans sa table de routage, et ajoute aux distances fournies celle qui le sépare du routeur qui lui fait l'annonce. Ainsi, chaque routeur commence par annoncer les réseaux qui lui sont directement connectés, et, de proche en proche, chaque route se retrouve annoncée sur tous les routeurs. [1]

Ce type de méthode compte le nombre de sauts qu'il y a entre deux endroits. Et c'est en fonction de ce nombre de sauts, qu'il va choisir le chemin le plus court.

La figure I.3, montre comment les routeurs s'échangent et envoient les informations entre eux.

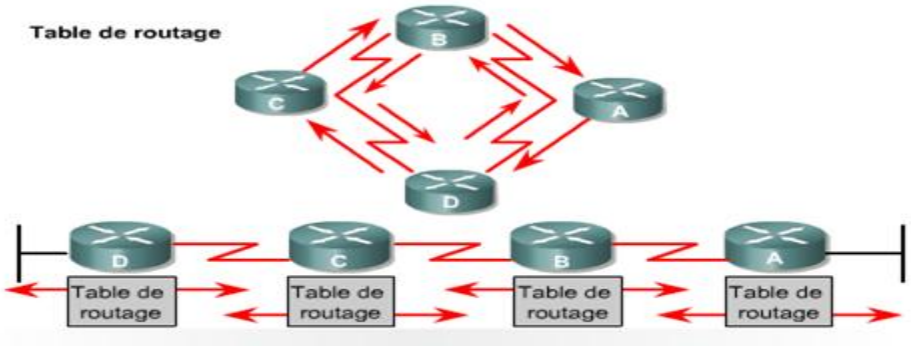

Figure I.3 : Envoi périodique de copies d'une table de routage aux routeurs voisins et cumul des vecteurs distance.

Parmi les protocoles de routage à vecteur distance, figurent les protocoles RIP, IGRP et EIGRP :

- ✓ RIPv1 (Routing Information Protocol) C'est le protocole (distance vector protocol) le plus vieux mais qui est toujours implanté sur beaucoup de sites. C'est un protocole de type IGP (Interior Gateway Protocol) qui utilise un algorithme permettant de trouver le chemin le plus court. Il supporte un maximum de 15 nœuds traversés (il n'est pas adapté au réseau de grande taille). Il fonctionne par envoi de messages toutes les 30 secondes. Les messages RIP permettent de dresser une table de routage. [C]

  Lors de l'initialisation du routeur, celui-ci détermine l'adresse réseau de ses interfaces puis envoie sur chacune, une demande d'informations (table RIP complète) aux

routeurs voisins. Lors de la réception d'une demande, un routeur envoie sa table complète ou partielle suivant la nature de cette demande. Lors de la réception d'une réponse, il met à jour sa table si besoin. Deux cas peuvent se présenter :

- pour une nouvelle route, il incrémente la distance, vérifie que celle-ci est strictement inférieure à 15 et diffuse immédiatement le vecteur de distance correspondant ;
- pour une route existante mais avec une distance plus faible, la table est mise à jour. La nouvelle distance et, éventuellement, l'adresse du routeur si elles se diffèrent, elles sont intégrées à la table.

Bien sûr, si l'appareil reçoit une route dont la distance est supérieure à celle déjà connue, RIP l'ignore. Ensuite, à intervalles réguliers (les cycles durent 30 secondes environ), la table RIP est diffusée qu'il y ait ou non des modifications.

✓ RIPv2 (Routing Information Protocol) C'est une version améliorée pour ajouter le support des sous-réseaux (subnets), des liaisons multipoints et de l'authentification. [C]

Le tableau I.1 montre quelques différences entre RIPv1 et RIPv2 :

RIPv1	RIPv2
Facile à configurer	Facile à configurer
Prend en charge uniquement un protocole de routage par classe (Classfull)	Prend en charge l'utilisation du routage CIDR (Classless).
La mise à jour de routage ne contient aucune information de sous-réseau.	Envoie des informations sur les masques de sous-réseau avec mises à jour des routes.
Ne supporte pas le routage CIDR ce qui oblige tous les équipements d'un même réseau à utiliser le même masque de sous-réseau	Supporte le routage CIDR ce qui permet a des équipements d'un même réseau à utiliser des différents masque de sous-réseau
Aucune authentification dans les mises à jour.	Permet authentification dans les mises à jour de routage.
Envoie les broadcasts sur 255.255.255.255	Envoie les mises à jour de routage en multicast sur 224.0.0.9 ce qui est efficace.

Tableau I.1 : Comparaison entre RIPv1 et RIPv2.

- ✓ IGRP (Interior Gateway Routing Protocol) est un protocole propriétaire développé par Cisco Systems, plus robuste que RIP et possédant moins de limitations. EIGRP (Extended Interior Gateway Routing Protocol) est une version évoluée.

4.5.2. Les protocoles de routage à état des liens :

Algorithmes de routage d'état des liens : Ils testent régulièrement l'état des liens avec leurs voisins et diffusent périodiquement ces états à tous les autres routeurs du domaine. L'algorithme du plus court chemin est généralement fondé sur l'algorithme de Dijkstra, qui calcule le plus court chemin vers chaque destination. Les avantages de tels algorithmes sont d'offrir une convergence rapide sans boucle et à chemins multiples. De plus, chaque passerelle calcule ses propres routes indépendamment des autres, et les métriques sont généralement précises et couvrent plusieurs besoins. En revanche, ces algorithmes sont souvent plus complexes à mettre en œuvre et consommateurs de ressources. [2]

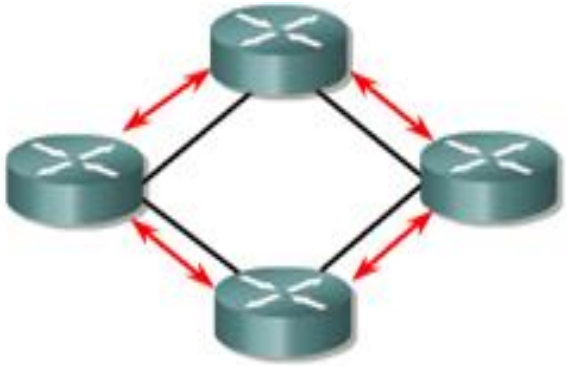

Figure I.4 : Diffusion d'informations de routage entre les routeurs

Le protocole OSPF (Open Shortest Path First) est un protocole de routage à état de liens, il a été développé par l'*IETF*[7] (Internet Engineering Task Force) pour succéder à RIP.

OSPF fait partie de la deuxième génération de protocoles de routage. Beaucoup plus complexe que RIP, mais au prix de performances supérieures, il utilise une base de données distribuée, qui garde en mémoire l'état des liens. Ces informations forment une description de la topologie du réseau et de l'état des nœuds, qui permet de définir l'algorithme de routage par un calcul des chemins les plus courts. [3]

[7] Comité de réflexion concernant les normes à utiliser pour les échanges sur Internet.

L'envoi de la table ne se fait pas de manière régulière, donc une meilleure utilisation de la bande passante. En plus de se baser sur l'état des liens, il se base aussi sur le cout de tel ou tel chemin. Il est calculé en fonction de la bande passante, plus la bande passante, plus le coût est faible. Si deux chemins ont le même cout, il se basera sur le nombre de sauts.

Le fonctionnement d'OSPF au sein d'une seule zone et de la manière dont la table topologie ou la link-state database est construite. La table de routage est constituée à partir de cette base de données. Ce résultat est obtenu grâce à l'application de l'algorithme de routage SPF. En voici les différentes étapes :

- ✓ D'abord, un routeur doit trouver ses voisins. Pour se faire, il utilise des paquets Hello dès son initialisation (activation), qui sont envoyés sur chaque interface dont le routage dynamique est activé, chaque routeur recevant ce paquet, intègre l'adresse IP de l'émetteur dans une base de données appelée base d'adjacence, et répond au routeur émetteur par un paquet IP unicast, le routeur émetteur intègre ainsi son adresse IP. Un routeur va générer un paquet *LSA*[8] (Link-State Advertisement). Cette annonce va représenter la collection de tous les états de liens de voisinage du routeur;
- ✓ Tous les routeurs vont s'échanger ces états de liens par inondation (*flooding*). Chaque routeur qui reçoit des mises à jour d'état de lien (*link-state update*) en gardera une copie dans sa *link-state database* et propagera la mise à jour auprès des autres routeurs;
- ✓ Après que la base de données de chaque routeur soit complétée, le routeur va calculer l'arbre du chemin le plus court (*Shortest Path Tree*) vers toutes les destinations avec l'algorithme Dijkstra. Il construira alors la table de routage (*routing table*), en choisissant les meilleures routes;
- ✓ S'il n'y a pas de modification topologique, OSPF sera très discret. Par contre, cv en cas de changement, il y aura échange d'informations par des paquets d'état de lien et l'algorithme Dijkstra recalculera les chemins les plus courts.

[8] C'est un paquet d'informations de routage qui est transmis entre les routeurs

5. **Le modèle hiérarchique en trois couches de Cisco :**

Cisco a développé un modèle à trois pour la conception des réseaux couches (Three Layer Hierarchical Internetworking Design/Model). Le modèle hiérarchique permet de concevoir des réseaux en couches, pour simplifier l'interconnexion des réseaux, ainsi pour faciliter la maintenance et la modification de l'architecture.

En effet, Grâce à une conception de réseau de ce type, vous créez des éléments que vous pouvez reproduire au rythme de la croissance du réseau. De plus, vous limitez les coûts et la complexité des mises à niveau nécessaires du réseau en les appliquant à un petit sous-ensemble plutôt qu'à l'ensemble du réseau. Dans les grandes architectures réseau, les modifications concernent généralement un grand nombre de systèmes. Vous pouvez également faciliter l'identification des points de défaillance dans un réseau en structurant ce dernier en une série de petits éléments faciles à comprendre. Donc, les points de défaillance seront facilement et rapidement repérés.

Un modèle de réseau hiérarchique comprend les trois couches suivantes :

- ✓ Couche Cœur (Core Layer) : assure l'optimisation du transport entre les sites ;
- ✓ Couche Distribution (Distribution Layer) : assure une connectivité fondée sur les politiques ;
- ✓ Couche Accès (Access Layer) : donne aux utilisateurs l'accès aux réseaux.

La figure I.5 présente les trois couches du modèle Cisco hiérarchique:

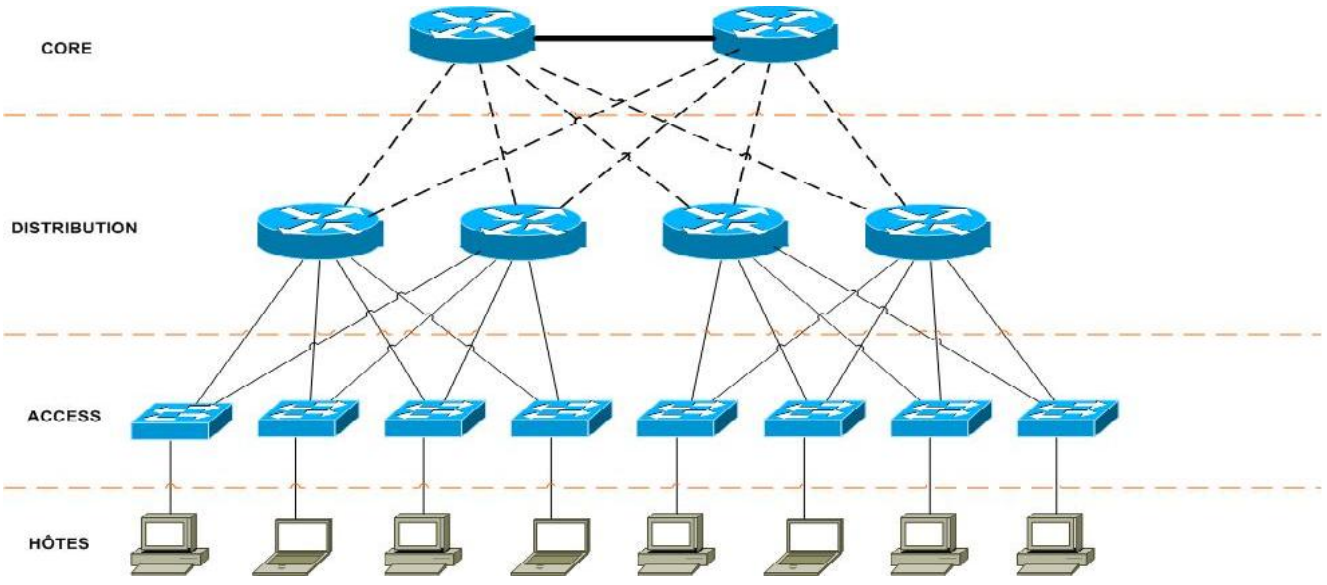

Figure I.5 : Modèle hiérarchique Cisco en trois couches.

5.1. La couche cœur « Core layer » :

C'est la couche supérieure. Son rôle est simple : relier entre eux les différents segments du réseau, par exemple les sites distants, les LANs ou les étages d'une société. [F]

Comme le volume du trafic est élevé, la couche cœur doit le transporté d'une manière fiable et rapide. Au niveau de cette couche, les routeurs sont généralement les plus utilisés. Si l'entreprise est vraiment grande, ce modèle peut s'imbriquer. Le design d'implémentation des routeurs correspond à ce modèle, mais le design des switchs pourra être adapté et reprendra la même hiérarchisation et les mêmes rôles. La Figure I.6, montre la couche Coeur du modèle hiérarchique:

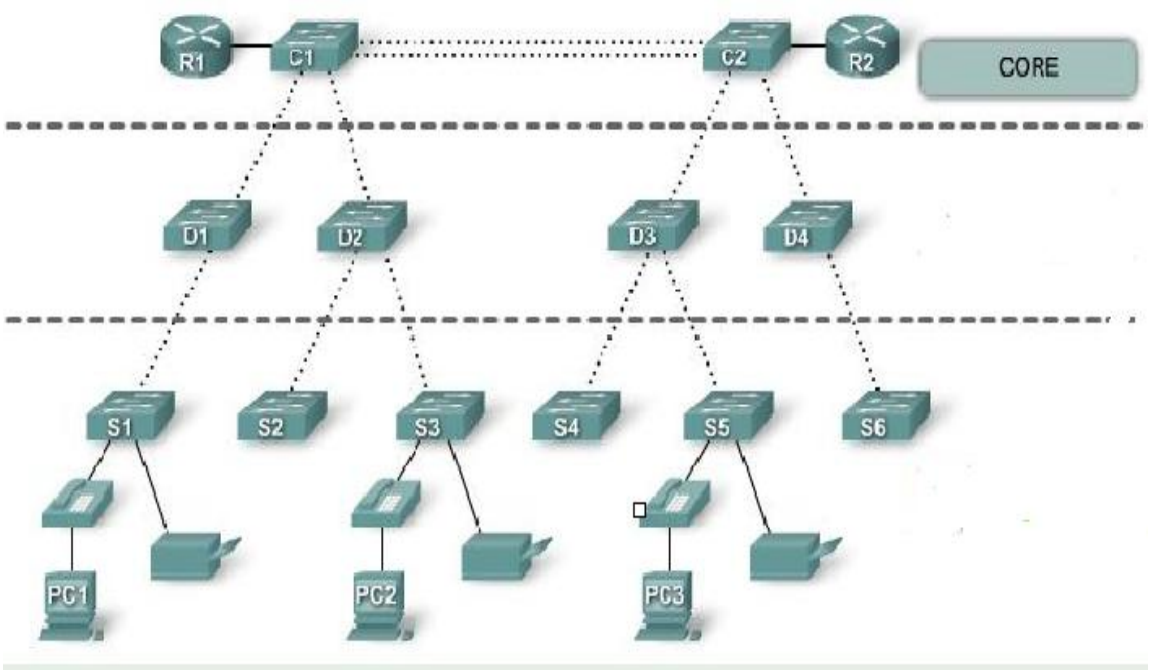

Figure I.6 : Couche Cœur « Core Layer ».

5.2. La couche Distribution « Distribution layer » :

La couche de répartition agit comme une interface entre la couche d'accès et la couche centrale. La fonction principale de la couche de distribution est de fournir le routage, le filtrage et l'accès au *WAN*[9] (Wide Area Network) et de déterminer comment les paquets peuvent accéder à la base, si nécessaire.

[9] Est un réseau couvrant une grande zone géographique, typiquement à l'échelle d'un pays, continent voire de la planète entière.

La couche de distribution s'agit d'un point de regroupement pour tous les commutateurs de couche d'accès et participe également à la conception de routage de base. Cette couche comprend LAN à base de routeurs et commutateurs de couche 3 (modèle OSI). Elle garantit que les paquets sont correctement acheminés entre les sous-réseaux et *VLAN*[10] (Virtual Local Area Network), elle peut comprendre aussi plusieurs fonctions, notamment :

- ✓ Routage VLAN ;
- ✓ Réseau et la mise en œuvre de la politique de sécurité, tels que les pare-feu et de traduction d'adresse ;
- ✓ Les définitions des domaines broadcast et de diffusion multipoints.

La Figure I.7, montre la couche Distribution du modèle hiérarchique:

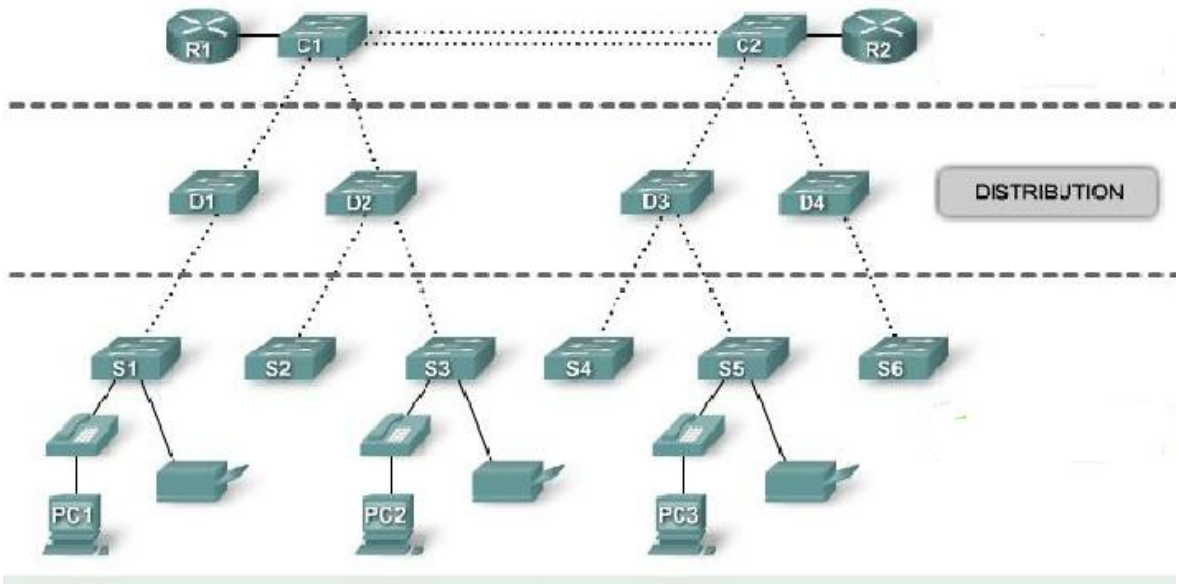

Figure I.7 : Couche Distribution « Distribution Layer ».

5.2. La couche Accès« Access layer » :

Le rôle principal de cette couche est de permettre aux utilisateurs de se connecter au réseau, elle assure un accès de première ligne aux services réseau. C'est au niveau de cette couche que la plupart des hôtes, y compris tous les serveurs et les stations de travail des utilisateurs, sont reliées au réseau.

[10] Voir chapitre 3.

La couche accès assure les fonctions suivantes :

- ✓ Politique et contrôle d'accès suite de la couche de distribution;
- ✓ La micro-segmentation;
- ✓ Le partage de la bande passante.

La Figure I.8, montre la couche Accès du modèle hiérarchique:

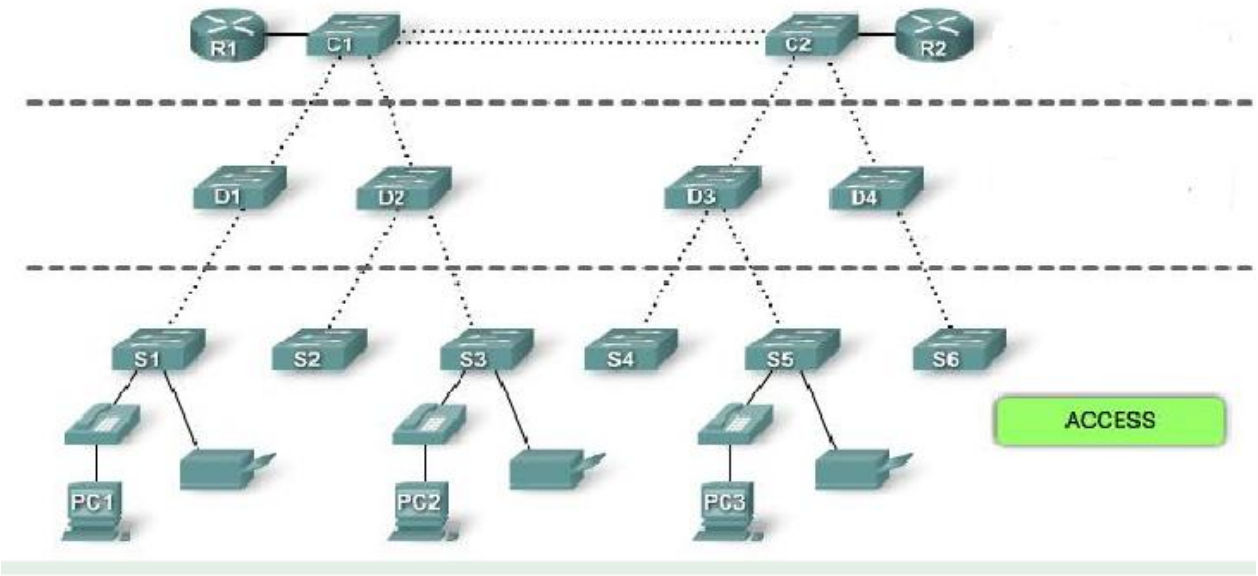

Figure I.8 : Couche Accès « Access Layer ».

Conclusion :

Une bonne compréhension de l'ensemble de concepts de bases de son sujet, permettra d'avoir une idée claire sur les réseaux informatiques et d'aborder son thème, en s'appuyant ainsi, sur une étude d'état des lieux. Le chapitre suivant, donnera une présentation sur l'organisme d'accueil.

CHAPITRE II

ETAT DES LIEUX DE L'ORGANISME D'ACCUEIL

Introduction:

L'étude de l'existant, est un point clé. Car, c'est une étape essentielle qui vise à représenter les contraintes sous lesquelles le projet se réalisera. Le présent chapitre, consistera à présenter brièvement l'organisme d'accueil, qui est SONATRACH, en donnant quelques informations nécessaires qui seront utiles durant le travail, tout en posant la problématique et en donnant une vue brève les solutions à implémenter.

1. Présentation de l'organisme d'accueil:

SONATRACH, avant d'avoir ce nom, elle était la société pétrolière de gérance (SOPEG) fondée le 12 mars 1956 par la compagnie française des pétroles Algérie (C F PA) et la société nationale de recherche et exploitation des pétroles en Algérie (S N R E P AL). Apres l'indépendance, et garce au décret n°63/491 de la nationalisation des hydrocarbures, la SOPEG est devenue SONATRACH.

SONATRACH est une abréviation de « Société Nationale de Transport et Commercialisation des Hydrocarbures» c'est une société Algérienne crée le 31/12/1963. Ses activités principales étaient le transport et la commercialisation des hydrocarbures, et à partir de 1966, son champ d'action s'élargit et englobe la recherche et la transformation des hydrocarbures.

SONATRACH est la première entreprise du continent africain. En 2006, elle est classée 12ème parmi les compagnies pétrolières mondiales, 2ème exportateur de GNL et de GPL et 3ème exportateur de gaz naturel. Elle emploie 120 000 personnes dans l'ensemble du Groupe.

1.1. Objectifs et évolution :

Pour les 25 années à venir, SONATRACH projette de doubler le rythme de la production pour atteindre annuellement 100 TEP (tonne équivalent pétrole), ce qui donnera une production cumulée prévisionnelle de 2.5 milliards de TEP à la fin de l'année 2020.

Le développement de SONATRACH doit être assuré par une volonté de défi qui s'appuie sur :

- ✓ La compétence technologique;
- ✓ L'amélioration de la qualité de l'environnement social;
- ✓ La satisfaction du client et le marketing;
- ✓ Le transfert du savoir-faire.

1.2. Activités de la SONATRACH :

Les activités de base de la SONATRACH ont été fixées en 1992 afin d'atteindre ses objectifs en :

- ✓ La recherche et l'exploitation des gisements;
- ✓ La liquéfaction et la transformation du gaz;
- ✓ La commercialisation;
- ✓ Le transport par canalisation.

1.3. L'organigramme de la SONATRACH :

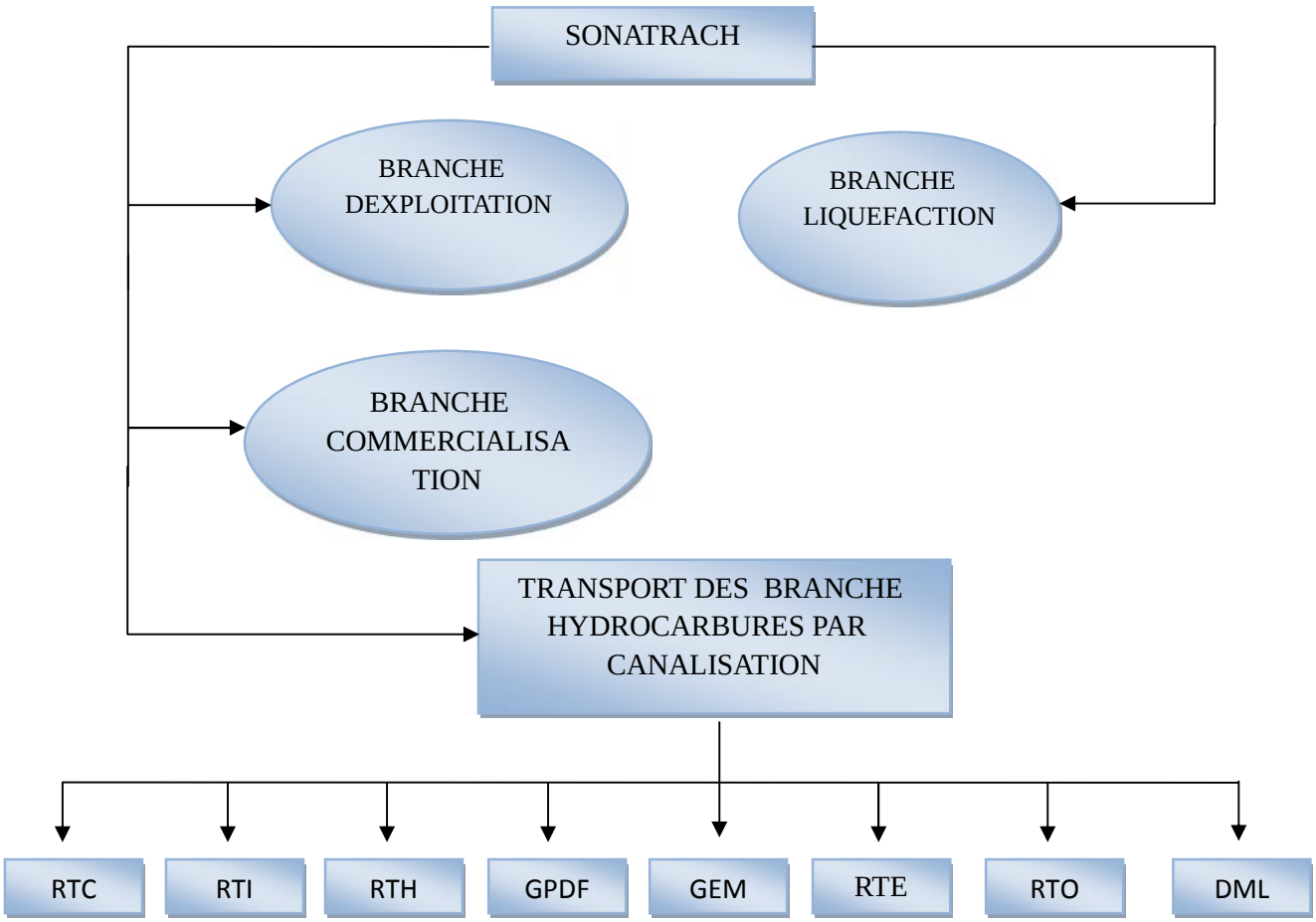

Figure II.1 : Organigramme de SONATRACH.

RTC : Région **T**ransport **C**entre (Bejaia).

RTO : Région **T**ransport **O**uest (Arzew).

RTI : Région **T**ransport **I**n Amenas.

DML : Direction **M**aintenance (Laghouat).

RTH : Région **T**ransport **H**aoud-El-Hamra.

GEM : **G**azoduc **E**nrico **M**attei.

RTE : Région Transport **E**st (Skikda).

GPDF : **G**azoduc **P**edro **F**arel(Espagne).

1.4. Présentation de la DRGB (Direction Régionale de Bejaia) :

La direction régionale de transport de Bejaia **(**DRGB) est l'une des cinq directions régionales de transport des hydrocarbures de la SONATRACH (TRC) couvrant l'activité de la branche transport par canalisation. Elle est chargée de l'exploitation de deux oléoducs, d'un gazoduc et d'un port pétrolier.

1.4.1. Les activités :

la DRGB est l'une des régions de l'entreprise SONATRACH ayant pour mission le transport des hydrocarbures par canalisations, Elle a pour mission de transporter, stocker et livrer les hydrocarbures liquides et gazeux. Elle est chargée de l'exploitation des ouvrages suivants :

Ouvrages	Origine	Destination	Longueur (km)	Diamètre (pouces)	Capacité
Gazoduc	Hassi-R'mel	Bordj Menail	437	42	7 milliards de m^3/ an
Oléoduc	Béni Mensour	Alger	130	16	2.88 millions de tonnes/an
Oléoduc	Haoud El Hamra	Bejaïa	668	24	15 millions de tonnes/an

Source : DRGB/SONATRACH.

Tableau II.1: Ouvrages de la DRGB / SONATRACH.

Un Ouvrage est une canalisation avec tout ce qui lui est raccordé, comme les stations, les canalisations sans les bacs par exemple.

1.4.2. Les différents départements:

La DRGB est divisée en sous direction, telle chaque sous direction est constituée de différents départements, à savoir :

- **La sous direction exploitation:** Charger de l'exploitation des installations de la région, et de maintenir le fonctionnement des trois ouvrages en effectuant des réparations en cas de fuite, de sabotage ou de panne pour les stations. Elle est composée de deux départements qui sont chargés de l'exploitation des trois ouvrages (1 Gazoduc et 2 oléoducs).
  - ✓ Département exploitation liquide;
  - ✓ Département exploitation Gaz.

- **La sous direction technique:** Assurer la maintenance et la protection des ouvrages, ainsi que l'étude et le suivi de projets de réalisation des travaux. Elle est composée de quatre départements :
  - ✓ Département maintenance;
  - ✓ Département protection des ouvrages;
  - ✓ Département approvisionnement et transport;
  - ✓ Département Travaux.

- **La sous direction finances/juridique:** Effectuer la gestion financière, le budget et le contrôle des affaires juridiques. Elle est composée de trois départements :
  - ✓ Département Budget/Contrôle Gestion;
  - ✓ Département Finance;
  - ✓ Département juridique.

- **La sous direction Administrative:** Gérer les ressources humaines et les moyens généraux. Elle est composée de trois départements :
  - ✓ Département Ressources Humaines;
  - ✓ Département Administratif et Social;
  - ✓ Département Moyens Généraux.

- **Autres structures** :
  - ✓ Assistant Sureté : Protéger et sauvegarder le patrimoine humain et matériel de la DRGB;
  - ✓ Département HSE;
  - ✓ Centre Informatique : Regroupe un ensemble des moyens d'exploitation et de développement des applications pour l'ensemble des structures de la DRGB, ainsi que la gestion du réseau informatique interne.

1.4. 3. Les stations de pompage et de compression:

La RTC (Région Transport Centre) est constituée du siège sis à Bejaia qui gère deux oléoducs et un Gazoduc. Tout au long de ces pipelines des stations de pompage et de compression sont installées afin d'acheminer les liquides et les gaz à leur destination dans les conditions contractuelles à savoir débit et pression. Il existe 7 stations de pompage ou de compression, genre d'une chaine dont la destination finale est la DRGB Bejaia, qui sont situées dans des régions différentes :

- ✓ Station SP1 Bis : située à Djamaa (El-Oued) station de pompage du Pétrole;
- ✓ Station SP2 : située à Biskra, station de pompage du Pétrole;
- ✓ Station SP3 : située à M'sila, station de pompage du Pétrole;
- ✓ Station SC3 : située à Moudjbara (Djelfa), station de compression du Gaz;
- ✓ Station SBM : située à Beni-Mansour, station de pompage du Pétrole;
- ✓ Station GG1 : située à Bordj-Ménaïl , station de compression du Gaz;
- ✓ TRA: Terminal Arrivée d'Alger.

Chaque station parmi les stations précédentes, est gérée par un chef de station, qui a sous ses ordres un ensemble de sections qui sont des divisions plus petites qu'un service. Ces sections sont citées la dessous :

- ✓ Section Maintenance;
- ✓ Section Exploitation;
- ✓ Section Administration;
- ✓ Section HSE;
- ✓ Section Transport.

2. Présentation du réseau informatique de la RTC Bejaia :

Le siège de la RTC est un LAN important intégrant des serveurs de base de données métier et des serveurs de communication (Exchange, Active Directory).

Au niveau de chaque station, un réseau LAN est réalisé, pour faciliter la communication entre les acteurs de chaque station et l'utilisation des ressources centralisées au niveau du siège, telles que les bases de données et la connexion internet. Chaque station dispose d'une réplication de l'annuaire Active Directory et d'un serveur de fichiers au niveau local.

Le raccordement des stations au siège est réalisé à travers une boucle fibre optique propriété de la SONATRACH. Cette fibre est gérée par les services de télécommunication. Dans les installations de télécommunication, une carte SAGEM ADR 155C avec une interface FastEthernet prévue pour l'interconnexion des réseaux de données.

L'architecture physique du réseau de la RTC Bejaia est représentée dans la figure II.2:

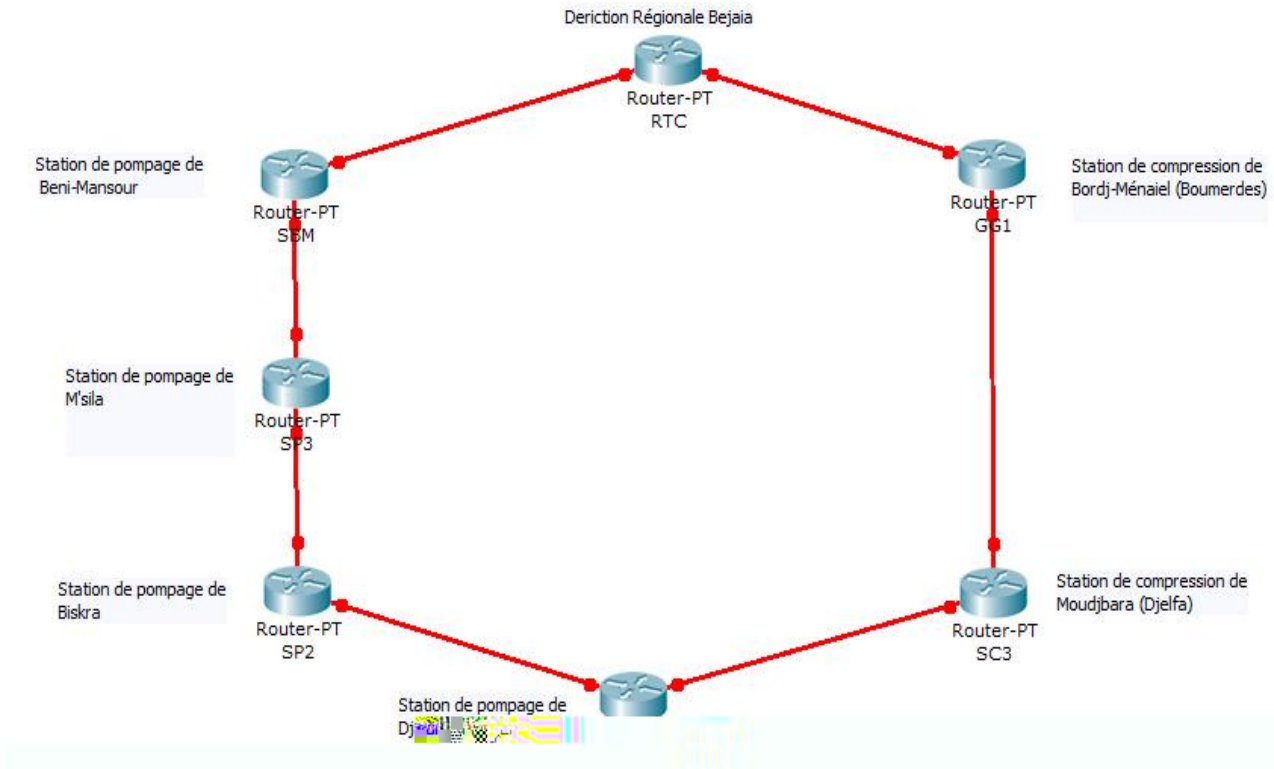

Figure II.2: Architecture physique du réseau de la RTC.

Pour augmenter la disponibilité, une liaison de redondance en ligne spécialisée empruntant un itinéraire différent a été prévue à cet effet.

Les équipements actifs des réseaux des stations sont de marque Cisco et tous sont de niveau 3.

L'architecture synoptique du réseau de la RTC est sous forme d'une topologie point-multipoints, comme le montre figure II.3 :

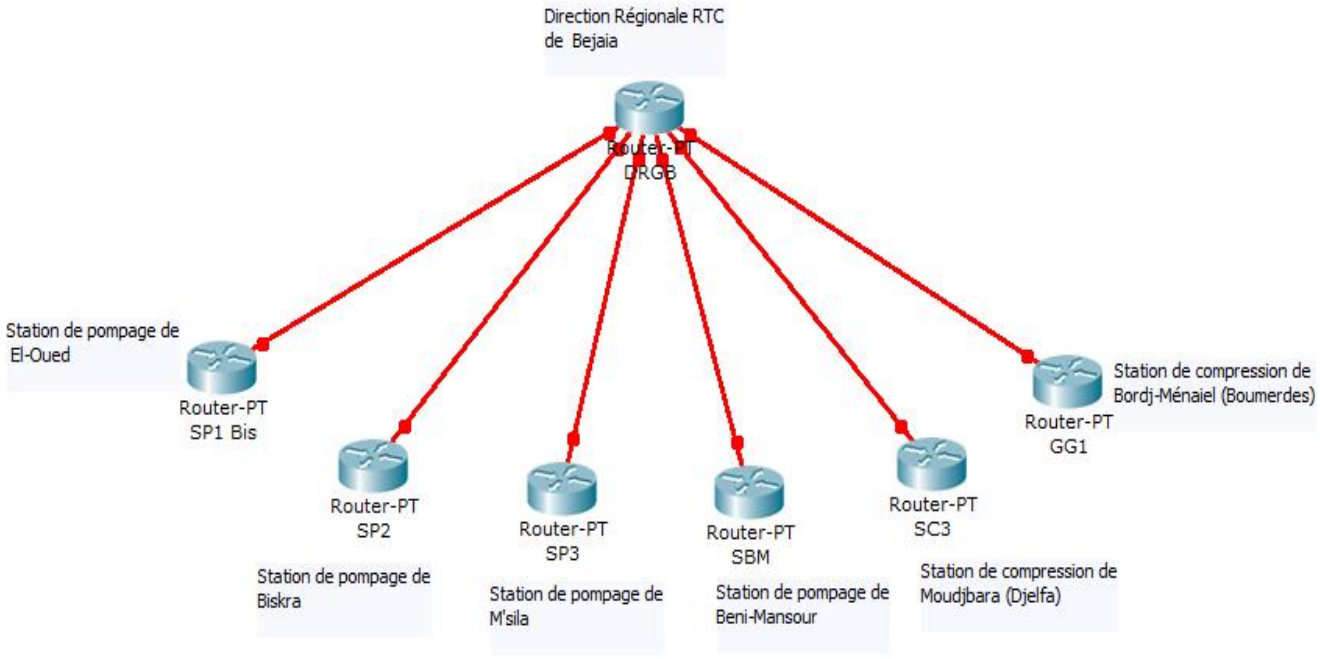

Figure II.3: Architecture logique point-multipoints du réseau de la RTC.

L'architecture réseau de chaque station est hiérarchique, elle est organisée en deux couches : couche Accès et couche Distribution. L'interconnexion des différentes stations au cœur du réseau siège de la RTC, constitue le Backbone. Distinguant ainsi trois couches :

- ✓ Couche Cœur (Backbone): transport optimum entre les différents sites;
- ✓ Couche Distribution : fournit une connectivité basée sur des politique;
- ✓ Couche Accès : fournit un accès réseau pour les groupes du travail et les utilisateurs.

3. Design d'un LAN type d'une station:

Parmi les stations importantes de la RTC Bejaia, la station SP3 qui est une grande station de pompage située à M'sila. Cette station va être prise comme échantillon sur laquelle le travail s'effectuera.

Voici une Figure illustrant l'architecture de la station SP3:

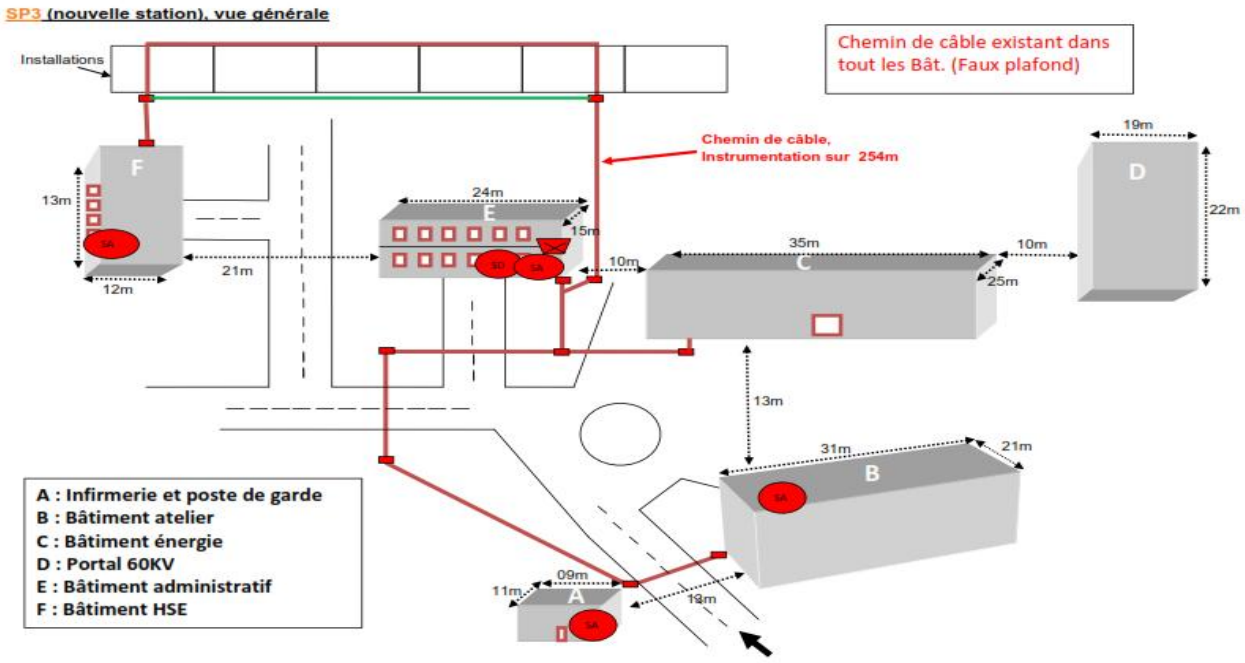

Figure II.4: Architecture de la station SP3.

Les batiments de SP3 à connecter :

Bâtiment		Nbre ports	
Nouvelle station	A	04	Switch d'accès
	E	06 28	Switch de distribution Switch d'accès Routeur
	B	06	Switch d'accès
	F	08	Switch d'accès

Tableau II.2: Les bâtiments de SP3.

5. Problématique :

Les réseaux informatiques sont de plus en plus répandus et complexes. En effet, l'organisation d'un réseau devient plus difficile et complexe. Un plan d'organisation soigné permettra de palier aux problèmes liés à la croissance de l'environnement réseau et aux problèmes affectant ses performances en termes d'optimisation de la bande passante et d'amélioration de la sécurité.

Conscient de ces problèmes que rencontrent bon nombre d'entreprises, ainsi que dans le cadre de projet «PROPOSITION ET MISE EN ŒUVRE D'UNE SOLUTION DE SEGMENTATION ET DE ROUTAGE DU RESEAU LAN ETENDU DE LA RTC BEJAIA (REGION TRANSPORT CENTRE) » pouvant apporter une solution efficace au bon fonctionnement du réseau et faciliter la préparation et la réalisation des projets de la société.

Le réseau de la RTC Bejaia est constitué de plusieurs réseaux locaux distants, telle que chaque station dispose d'un réseau local, donc une interconnexion de toutes les stations sur le plan informatique est nécessaire, à vrai dire, une interconnexion de tous les réseaux locaux.

L'objectif de ce projet, est la mise en place d'un modèle d'organisation et de configuration d'un réseau, sur les différents plans d'adressage et de routage. En effet, proposer une segmentation sous laquelle les différents réseaux locaux des stations vont être organisés, ainsi, de permettre la communication et l'interconnexion entre elles en exploitant le routage. Et tout cela, a fin de permettre une haute disponibilité du réseau.

Dans un premier lieu, organisant chaque station en segmentant son réseau local, dans le second, interconnectant les différentes stations en s'appuyant sur le routage.

6. Solutions proposées :

Organiser son réseau local d'une bonne manière, est important, et adopter un bon modèle de segmentation aussi, est très important. En effet, une bonne organisation permettra une optimisation du réseau en termes d'efficacité et de performance. En outre, opter pour une

solution de routage en choisissant la manière dont laquelle les données seront transitées à travers les réseaux, doit être faite en étudiant très bien le cas.

L'organisation des réseaux locaux de stations de la RTC Bejaia, se fera en les segmentant à l'aide des VLANs. En effet, cette solution est la meilleure et l'adéquate, en vue des avantages qu'elle offre.

L'interconnexion de tous les réseaux locaux des stations de la RTC Bejaia, en adoptant un routage dynamique est plus efficace par rapport à un routage statique, et cela vu la taille considérable du réseau.

Conclusion :

Une bonne étude de l'existant et de l'état des lieux, permettra de mieux s'approfondir dans son projet et de bien étudier sa problématique exacte, en prenant compte l'étude des solutions qui porteront vraiment un plus au cas présenté.

CHAPITRE III

ETUDE DES SOLUTIONS PROPOSEES

Introduction :

Poser les critères de choix des solutions est important, afin de voir si vraiment ces dernières ont été choisies selon de bonnes bases et si elles apportent surement des réponses aux problèmes posés.

Dans ce chapitre, une étude descriptive des solutions proposées, ainsi qu'une argumentation du choix de ces dernières, seront implantées, en illustrant les avantages et les atouts de chaque solution, qui ont poussés à les choisir.

1. Segmentation VLAN :

Un VLAN (Virtual Local Area Network) est une technologie permettant de créer des segments logiques, indépendamment de l'implantation géographique par une configuration logique à l'aide de matériels et logiciels spécifiques. Elle consiste à regrouper les éléments du réseau (utilisateurs, périphériques, etc.) selon des critères logiques (fonction, partage de ressources, appartenances à un département, etc.) sans se heurter à des contraintes physiques (dispersion des ordinateurs, emplacement physique, etc.).

Indépendamment de l'emplacement où se situent les nœuds, les stations peuvent communiquer comme si elles étaient dans le même segment. Un VLAN est assimilable à un domaine de broadcast. Ceci signifie que les messages de diffusion émis par une station d'un VLAN ne sont reçu que par les stations de ce VLAN). La communication entre VLANs n'est possible que par l'intermédiaire d'un périphérique de la couche 3 en assure le routage. Il peut s'agir d'un routeur traditionnel ou d'un commutateur de couche 3.

1.1. Les avantages VLAN :

Les VLANs ont beaucoup d'avantages qui permettent une meilleure organisation d'un réseau local, ainsi d'améliorer son fonctionnement en termes de performances et d'efficacité. Ces avantages sont les suivants :

- ✓ Limiter la propagation du trafic au seul VLAN concerné : un flux originaire d'un VLAN donné n'est transmis qu'aux ports qui appartiennent à ce même VLAN. Chacun des VLANs constitue ainsi un domaine de diffusion propre.

C'est pourquoi le trafic doit être routé pour être acheminé entre différents VLANs. C'est-à-dire que la communication entre-VLAN doit se faire par le passage par un routeur, pour acheminer le trafic entre les équipements appartenant à des VLANs différents (Voir Annexe A1).

- ✓ Meilleures performances : la création de domaine de diffusion plus petit, amène à une diminution de la quantité de trafic inutile sur le réseau, qui résulte une augmentation des performances.
- ✓ Flexibilité de segmentation de réseau : les utilisateurs et les ressources peuvent être regroupées sans devoir prendre en considération leur localisation physique. C'est-à-dire de se faire connecter à un groupe logique des stations du travail, même si ces dernières ne sont pas géographiquement proches les une des autres.
- ✓ Simplicité de l'administration du réseau **:** Les postes du travail appartenant à un même VLAN peuvent être déplacés d'un lieu à l'autre ou d'une zone à une autre, sans devoir à modifier les connexions physique. Ainsi que de nouveaux segments ou utilisateurs peuvent être ajoutés grâce à une simple configuration des commutateurs, soit par la création de nouveaux VLANs, soit par l'affectation de nouveaux utilisateurs à un VLAN.
- ✓ Organisation du réseau : les VLANs permettent de constituer autant de réseaux logiques que l'on désire sur une seule infrastructure physique, donc, cela conduit à une organisation efficace du réseau (mieux organiser son réseau).
- ✓ Augmentation de la sécurité : grâce à la notion des groupes, qui conduit à l'isolement de certains d'eux, certaines ressources seront alors protégées, ainsi il y aura un renforcement considérable de la sécurité du réseau.

1.2. Critères de regroupement dans un VLAN :

Les réseaux locaux virtuels permettent une segmentation et un regroupement dans un même VLAN selon certains critères :

- ✓ Dispositifs de regroupement par fonction : Une façon simple et classique pour la segmentation et le regroupement dans un même VLAN, consiste à regrouper les équipements appartenant à un même département, service ou bien exécutant une même tache. Les équipements sont regroupés sur la base des fonctions, des équipes de projet ou des applications de l'entreprise, sans devoir prendre en

considération la contrainte de l'emplacement géographique ou bien si les équipements appartiennent à un même commutateur ou non. Cette méthode est très adaptable, car elle règle un grand problème de la segmentation, qui est l'indépendance de l'emplacement géographique. Donc, pour l'exemple d'une entreprise, même si un service donné englobe deux unités situées dans des zones distinctes, et même si les équipements font partie de deux commutateurs différents, cela ne pose aucun problème pour les assembler dans un seul VLAN et d'échanger un trafic de données entre ces unités, donc, ce genre de regroupement, facilite grandement l'accomplissement des tâches, ainsi un meilleur fonctionnement de l'entreprise. Par contre, cette méthode pose un problème lors d'échange de données entres les équipements d'un VLAN, qui nécessite un temps de réponse beaucoup plus lent par rapport s'ils faisaient partie d'un même Switch

La Figure III.1, montre un exemple de regroupement de VLAN par fonction :

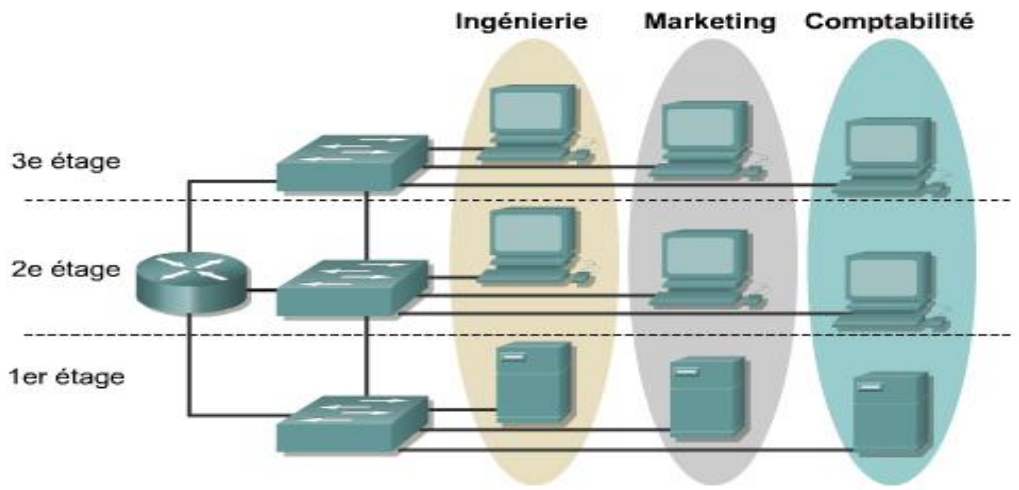

Figure III.1 : VLANs par services.

- ✓ Dispositifs de regroupement par volume du trafic **:** appareils qui communiquent largement entre eux, sont de bons candidats pour être regroupés dans un commun VLAN. Dans la mesure du possible, il convient de placer sur le même réseau VLAN chaque périphérique et les ressources dont il a besoin.

Le périphérique client accède ainsi à la ressource voulue directement, via le réseau commuté, sans devoir passer par un routeur. La pratique de la segmentation selon les modèles (volumes) de trafic gagne en popularité, et il est maintenant reconnu comme l'une des meilleurs pratiques. En effet, les appareils qui envoient et reçoivent des informations entre eux ont souvent des niveaux élevés de trafic, et de les répartir individuellement à différents groupes, il est plus difficile pour les données à passer à travers. Le regroupement des appareils entre eux, cependant, maintient la circulation à l'intérieur d'un segment, la réduction de congestion et les retards de temps. L'inconvénient de cette méthode réside dans la difficulté de regrouper les utilisateurs avec les ressources dont ils ont besoin, puisque presque toutes les ressources (imprimantes, courrier électronique, gestion des fichiers, … etc.) sont utilisées par la majorité des utilisateurs.

- ✓ Dispositifs de regroupement par types de trafic : Les différents types de trafic peuvent être justifiés de leur propre VLAN. Types de trafic comprennent la gestion du trafic réseau, les services vidéo, les fichiers et l'impression, le courrier électronique, navigation sur Internet, etc.

  Donc, un regroupement de chaque service dans un VLAN. Pour les utilisateurs, le regroupement se fait par le type d'application réseau partagée qu'ils utilisent. Cette solution eest avantageuse en terme de qualité de service, car il y a une indépendance VLAN pour chaque service. En effet, pour le cas d'une solution de Voix IP (VoIP), la mise en œuvre de réseaux VLAN se justifierait par la volonté de distinguer le trafic vocal des trames de données en les mettant sur des réseaux VLAN distincts. Lorsque ces deux types de trafic sont séparés, il est possible d'appliquer la qualité de service au trafic voix pour réduire le temps et la perte de trames.

  Comme il est fréquent que les serveurs soient tous regroupés sur le même réseau VLAN. Malheureusement, tous les clients doivent impérativement passer par un routeur au moins pour accéder aux serveurs. Si la gestion des adresses IP s'en trouve facilitée, une telle configuration augmente la latence et produit des goulots d'étranglement.

- ✓ Dispositifs de regroupement par sécurité **:** Segmenter selon les exigences de sécurité est couramment utilisée. Il arrive qu'une entreprise ait besoin de restreindre l'accès à un ou plusieurs périphériques de son réseau local ou bien rendre transparent certains trafics à certains utilisateurs en vue de la sensibilité des données échangées. En effet, c'est suivant des stratégies de sécurité que l'appartenance à un même VLAN est réalisée selon des droits de l'utilisateur. Si tous les périphériques de cette entreprise sont sur le même domaine de broadcast, il devient très difficile d'appliquer des stratégies de sécurité pour certains. Par contre, il sera facile si les périphériques seront situés dans des domaines de broadcast différents. Exemple, regrouper dans un premier VLAN, les utilisateurs ayant droit de consulter les fichiers de base de données. Dans un deuxième VLAN, ceux qui ont le droit d'accéder à un serveur donné.
  Malheureusement, cette solution n'est pas vraiment fiable pour renforcer la sécurité du réseau, puisque, un utilisateur peut toujours y accéder aux VLANs voulus centralisés, si d'autres mesures de sécurité seront pas appliquées.

- ✓ Dispositifs de regroupement géographique : Combiner les dispositifs dans chaque emplacement dans leur propre VLAN d'un même commutateur, peut être avantageux. En effet, Certains réseaux ont limité les capacités trunking, et la nécessité de transférer des données sur de grandes distances physiques réduit la vitesse et l'efficacité du système. Les réseaux d'entreprise ayant centralisé leurs ressources, les utilisateurs sont amenés à utiliser de nombreuses ressources différentes qui, pour la plupart, ne sont plus associées à leur VLAN. En raison de ces changements de localisation et d'utilisation des ressources, les VLANs sont à présent créés plus fréquemment autour de frontières géographiques plutôt que de frontières de standardisation. Cette localisation géographique peut s'étendre à un bâtiment complet ou bien à une surface qui se limite à un seul commutateur dans un réseau local. L'avantage de cette méthode est que le temps de *latence*[1] est réduit. En effet, acheminer une trame entre deux équipements d'un même VLAN situés dans différents commutateurs avec une redondance de liens, doit d'abord sélectionner le

[1] Parfois appelée délai, c'est le temps nécessaire a une trame ou paquet pour circuler entre sa station d'origine et sa destination finale.

chemin le plus court entre les deux extrémités par le *protocole STP*[2] classique (Spanning-Tree) qui met un temps dans les alentours de 50s pour la détermination du plus court chemin. Ce temps soulève une problématique pour les machines qui nécessitent une communication réseau rapide (cas d'une communication à temps réel) et met en évidence l'efficacité du réseau, par rapport si les deux équipements étaient dans un seul commutateur où la notion de redondance est absente. Groupement selon la localisation géographique est la plus ancienne solution à ce problème, et l'une des meilleures pratiques originales dans la segmentation. Les dispositifs dans un emplacement spécifique sont regroupés dans un VLAN, ce qui contribue à accroître et améliorer l'efficacité du réseau en terme de vitesse de transfert de données. En contre partie, l'inconvénient majeur de cette méthode, est que la contrainte de l'emplacement physique des équipements est toujours à respecter, or que le but primordial des VLANs est de s'affranchir aux limitations de l'architecture physique.

La Figure III.2, donne une image sur les VLANs suivant l'emplacement géographique :

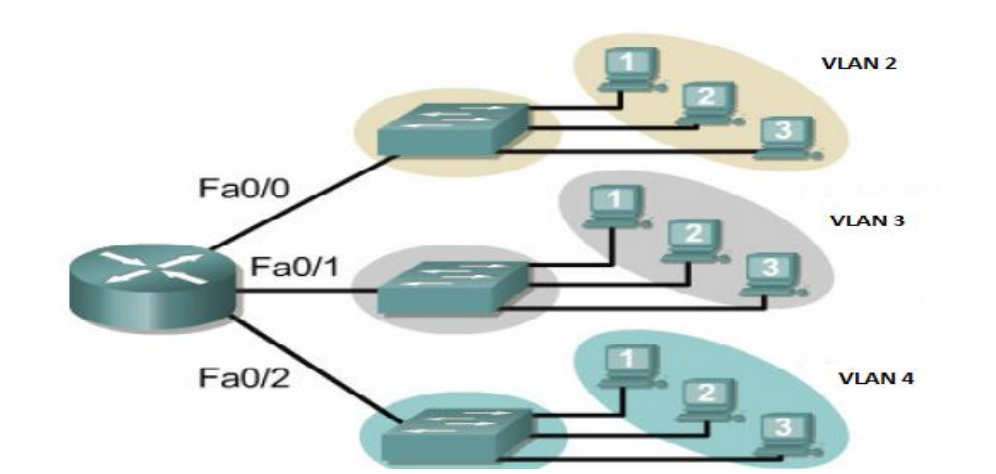

Figure III.2 : VLANs par emplacement géographique.

[2] Est un protocole propriétaire à Cisco, il est de couche 2 et il permet le contrôle de boucles lors de la redondance des chemins.

Une meilleure solution pour l'organisation des LANs des stations de la RTC Bejaia, est la segmentation VLAN en combinant entre les différentes méthodes de regroupement dans un même VLAN. Le mixage des solutions est efficace, vu que chaque méthode apporte un avantage précis. Par conséquent, regrouper les serveurs dans un VLAN pour des besoins de sécurité, ainsi, regrouper les postes des utilisateurs par fonction pour l'accomplissement efficace de leur tâches, et s'il y a lieu de regrouper par raison géographique cela permettra d'augmenter les performances réseau, tout en prenant compte du critère de regroupement par volume de trafic pour les ressources fréquemment utilisées.

1.3. Méthode d'implémentation des VLANs:

L'attribution des VLANs dans un commutateur est faite selon trois techniques, telle que, chaque technique est associée à un niveau donné du modèle OSI. Cette attribution est faite soit par le numéro de port, l'adresse mac ou le sous-réseau.

- ✓ VLAN par port (VLAN niveau 1) : chaque port du commutateur est affecté a un VLAN donné. L'affectation des ports est statique, donc l'administrateur peut savoir directement le VLAN d'appartenance d'un équipement. Cette technique est efficace dans les réseaux où les déplacements sont rares et contrôlés. En effet, une source externe ne peut y accéder au réseau, sauf si elle se branche sur le port appartenant au VLAN voulu à accéder, donc, un renforcement de la sécurité. Par contre, son inconvénient est sa lourdeur d'administration. En effet, si un matériel est déplacé et que l'on désire qu'il soit toujours dans le même VLAN, il faudra alors configurer le nouveau port.
  La Figure III.3 est un exemple de VLAN par port :

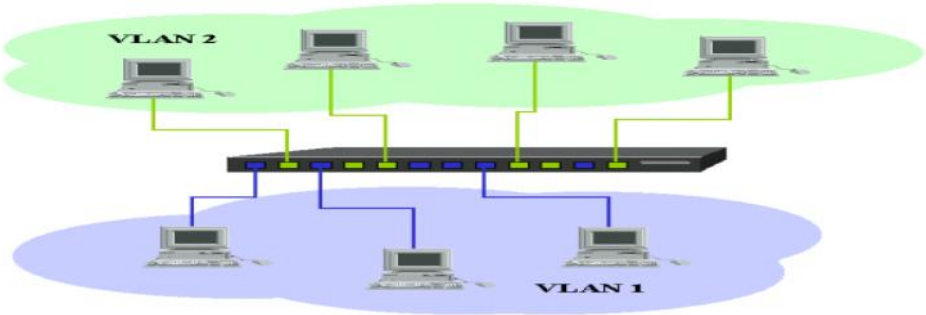

Figure III.3 : VLAN niveau 1.

- ✓ VALN par adresse MAC (VLAN niveau 2) : chaque adresse MAC est affectée à un VLAN. En effet, une table (adresse MAC/VLAN) sur le commutateur doit être remplie, et l'affectation (Port/VLAN) s'effectue à l'aide des premiers paquets portant l'adresse MAC source. L'avantage de cette technique est que le déplacement d'une station, se fait sans devoir à reconfigurer les commutateurs et la station continuera toujours à appartenir au même VLAN. Par contre, l'inconvénient majeur de ce type de VLAN, est que l'administration est complexe pour la configuration et la mise en place de la base de données (adresse MAC/VLAN). En effet, lorsque le nombre d'éléments devient important, le maintien de la base de données devient plus difficile lors de l'ajout de nouveaux équipements ou lors de la réaffectation d'une adresse MAC à un autre VLAN.

  La Figure III.4 est un exemple de VLAN par adresse MAC :

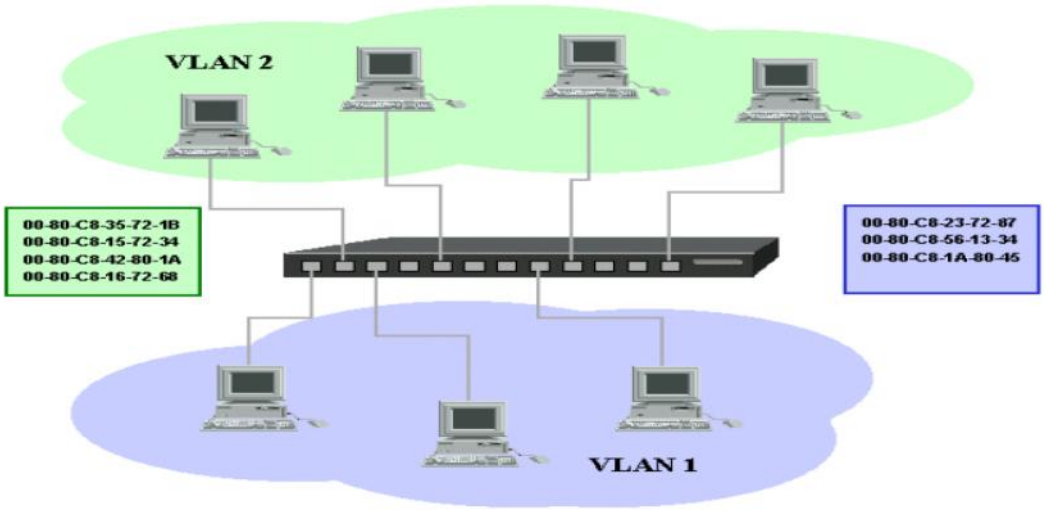

Figure III.4: VLAN niveau 2.

- ✓ VLAN par adresse IP (VLAN niveau 3) : chaque station est affectée à un VLAN en fonction de son adresse IP. Dans ce cas, une table (adresse IP/VLAN) est construite sur le commutateur. L'association (Port/VLAN) est faite d'une manière automatique, en décapsulant le paquet jusqu'à l'adresse

source. Dans ce type de VLAN, les commutateurs apprennent automatiquement la configuration des VLANs en accédant aux informations de couche 3. L'avantage de cette solution, est que le déplacement des équipements est sans reconfiguration, car, l'affectation à un Vlan est automatique suivant une adresse IP. Par contre, une légère dégradation des performances aura lieu, et cela est dû à une analyse plus profonde des informations contenues dans les paquets lors de la décapsulation afin de déterminer le VLAN d'appartenance, d'où, l'obligation d'utiliser un équipement plus couteux pouvant décapsuler le niveau3.

La figure III.5 est un exemple de VLAN par adresse IP :

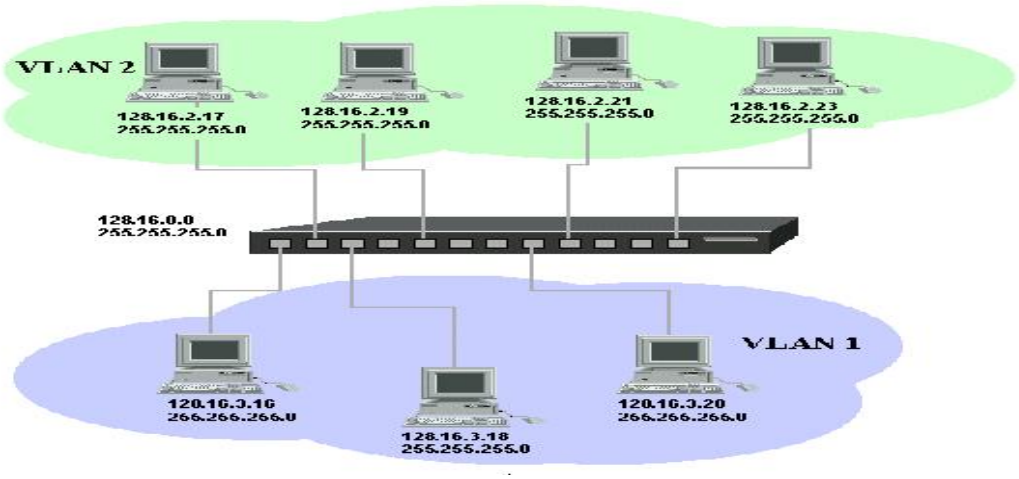

Figure III.5 : VLAN niveau 3.

Le Tableau III.1 montre quelques différances existantes entre les trois techniques d'implémentation VLAN :

Type de VLAN	Description
VLAN par port	• Méthode de configuration la plus courante. • Ports affectés individuellement à un ou plusieurs VLANs. • Facile à mettre en place.
VLAN par adresse MAC	• Rarement utilisé. • Chaque adresse doit être saisie dans le commutateur et configurée individuellement. • Difficile à administrer et à gérer.
VLAN par adresse IP	• une légère dégradation de performances peut se faire sentir dans la mesure de décapsulation des paquets. • Utilisation d'un équipement supportant la décapsulation du niveau3.

Tableau III.1: Les différentes techniques d'implémentation VLAN.

La meilleure technique d'implémentation des VLANs au sein des réseaux locaux des stations de la RTC Bejaia, est celle par port. Le choix a été influencé par le faite qu'il n y pas de mobilité de postes utilisateurs au sein de l'entreprise. En effet, le nombre peu important des utilisateurs du réseau dans chaque station et la vocation technique de ce personnel qui est affecté dans des ateliers spécialisés réduisant ainsi leur mobilité, ce qui favorise le choix de VLAN statique (VLAN par port). En outre, cette technique, offre une administration réseau plus sécurisée par rapport aux VLANs niveau 2 et 3, pas de dégradation des performances du réseau pour l'absence de la décapsulation. De plus, elle a une implémentation simple et facile qui ne nécessite pas une table d'association (Adresse MAC/VLAN) ou (Adresse IP/VLAN).

2. Interconnexion du réseau :

A fin que la communication entre les différents LANs de la RTC Bejaia aura lieu, une interconnexion réseau est nécessaire. Cette interconnexion se réalisera en adoptant le routage dynamique par ce qu'il est le mieux adéquat et le plus efficace.

Le routage statique contrairement au routage dynamique, possède quelques limitations qui influencent négativement sur le bon fonctionnement du réseau. En effet, dans le routage statique, la table de routage est introduite manuellement par l'administrateur, donc, une station ne peut atteindre que les réseaux indiqués dans cette table. En plus, lorsque le réseau

est assez important en terme de taille, les configurations deviennent trop lourdes et il y aura risque de ne pas déclarer des chemins entre les différents réseaux.

Le choix s'est déroulé sur le routage dynamique, en se basant sur quelques critères et avantages qui le privilège par rapport à son opposé, le routage statique, tels que :

- ✓ Taille du réseau : Pour un réseau de grande taille il semblerait plus judicieux de mettre en place un routage dynamique qui évite de devoir initialiser les tables de routage de chaque routeur. L'avantage est surtout que si le réseau change de topologie (suppression, déplacement ou ajout de sites ou réseaux IP), il ne sera pas nécessaire de remanier toutes les tables de routage. [E]
- ✓ Minimiser la bande passante : Il est également possible de minimiser la bande passante utilisée pour rien. En effet, avec un routage dynamique, si un site devient inaccessible, l'information est remontée dans le réseau vers tous les autres sites. Ceux-ci n'émettront plus de paquets vers ce site jusqu'à ce qu'ils reçoivent une information selon laquelle le site est de nouveau opérationnel. Dans un routage statique, l'information n'étant pas remontée, les sites continuent d'émettre pour le site hors service, les paquets utilisent la bande passante du réseau pour ne finalement pas aboutir. [E]

  Mais, les protocoles de routage aussi génèrent eux-mêmes du trafic. En effet pour construire leurs tables de routage, ils émettent des mises à jour (updates).
- ✓ Performances du routeur : Ce dernier point peut influer sur le choix du routage. En effet, dans les réseaux de grande taille il y a beaucoup de réseaux IP déclarés. Un réseau IP correspond à une destination et donc à une entrée dans une table de routage. Dans le cas d'un routage dynamique, la table est construite sur les informations reçues par le routeur dans les "updates" émis par d'autres routeurs. À la réception de ces mises à jour, le routeur compile et interprète les informations, calcule les routes, crée une base de données interne et en extrait une table de routage. Ces opérations mobilisent donc des ressources mémoires et CPU dans le routeur. Plus le réseau est grand plus il faudra de ressources à chaque routeur. Mais, même si le routage dynamique consomme beaucoup de ressources, il est recommandé dans le cas des routeurs performants.

2.1. Choix du protocole de routage :

Les protocoles de routage dynamique interne, sont des protocoles qui fonctionnent à l'intérieur d'un *système autonome*[3] (AS). Ces protocoles sont appelés intra-autonomous system routing protocol ou protocole de routage intra-AS.

L'ensemble de réseaux interconnectés des stations de RTC de Bejaia est considéré comme un seul système autonome, car il regroupe des routeurs dépendants d'une même responsabilité administrative du point de vue du routage et appliquant une politique du routage unique.

Le protocole OSPF est le plus efficace pour interconnecter les LANs de la RTC Bejaia. En effet, OSPF est plus performant que RIP et commence donc à le remplacer petit à petit. Il s'agit d'un protocole de type protocole « route-link » (Protocole d'état des liens), ce qui signifie que, contrairement aux protocoles vecteur de distance, ce protocole n'envoie pas aux routeurs adjacents le nombre de sauts qui les sépare, mais l'état de la liaison qui les sépare, en terme de bande passante, de cette façon, chaque routeur est capable de dresser une carte de l'état du réseau et peut par conséquent choisir à tout moment la route la plus appropriée pour un message donné.

Finalement, le protocole OSPF intègre la notion de zone (area). Un système autonome géré par le protocole OSPF peut être divisé en plusieurs zones de routages qui contiennent des routeurs et des hôtes. Cette division du système autonome en plusieurs zones introduit un routage hiérarchique. Chaque zone possède sa propre topologie et ne connaît pas les topologies des autres zones du système autonome. L'intérêt de définir des zones est de limiter le trafic de routage, de réduire la fréquence des calculs du plus court chemin par l'algorithme SPF et d'avoir une table de routage plus petite, ce qui accélère la convergence de celle-ci.

Le réseau de la RTC Bejaia est considéré comme une seule zone (Area 0), vue le nombre peu important des routeurs et cela pour que chaque routeur ait une vue générale sur l'état du réseau.

[3] C'est un ensemble de réseaux gérés par un administrateur commun et partageant une stratégie de routage commune.

Le protocole OSPF offre :

- ✓ Une meilleure convergence que RIP parce que les changements de routage sont propagés instantanément et non périodiquement de manière incrémentielle grâce aux relations de voisinage entretenues;
- ✓ Etant un protocole de routage à état de lien, chaque routeur possède une connaissance complète des réseaux au sein d'une zone (*area*). Aussi, le danger de boucles de routage n'étant a priori plus présent, la limite du nombre de sauts n'est plus nécessaire;
- ✓ Supporte entièrement les masques a longueur variable (*VLSM* [4] : Variable Length Subnet Masque);
- ✓ Le choix du meilleur chemin est basé sur le coût (la bande passante inversée).

Conclusion:

L'étude des solutions a pour objectif, de permettre une bonne planification. En effet, détailler les solutions, pour mieux planifier sa solution sur son domaine, pour mieux organiser les réseaux locaux des stations de la RTC Bejaia, ainsi que de déployer les protocoles nécessaires pour un meilleur fonctionnement du LAN étendu de la RTC.

[4] C'est une technique qui permet de diviser l'espace d'adresse IP en sous-réseau de différente taille.

CHAPITRE IV

PLANIFICATION DES SOLUTIONS

Introduction

Après avoir bien étudié les solutions proposées du coté théorique, vient le tour de planification. En effet, bien planifier sa solution, conduira à une bonne réalisation de son projet. La planification est l'ensemble des moyens mis en œuvre pour prévoir une bonne implémentation. Elle consiste à organiser les réseaux LANs des stations sur les différents plans (nommage, adressage et routage) et déployer les protocoles nécessaires. Une mauvaise planification implique un non-bon fonctionnement réseau.

1. Présentation de l'architecture réseau :

L'architecture réseau de chaque station est organisée en 2 couches: accès et distribution. L'interconnexion au cœur du réseau du siège de la RTC. Bejaïa se fera via une boucle en fibre optique de la SONATRACH.

Une solution de redondance composée de routeurs, sera ajoutée pour l'interconnexion des sites de la RTC via des liaisons spécialisées.

Comme il a été déjà précisé, c'est la station SP3 qui est prise comme échantillon, et le schéma IV.1 est un schéma synoptique de cette station :

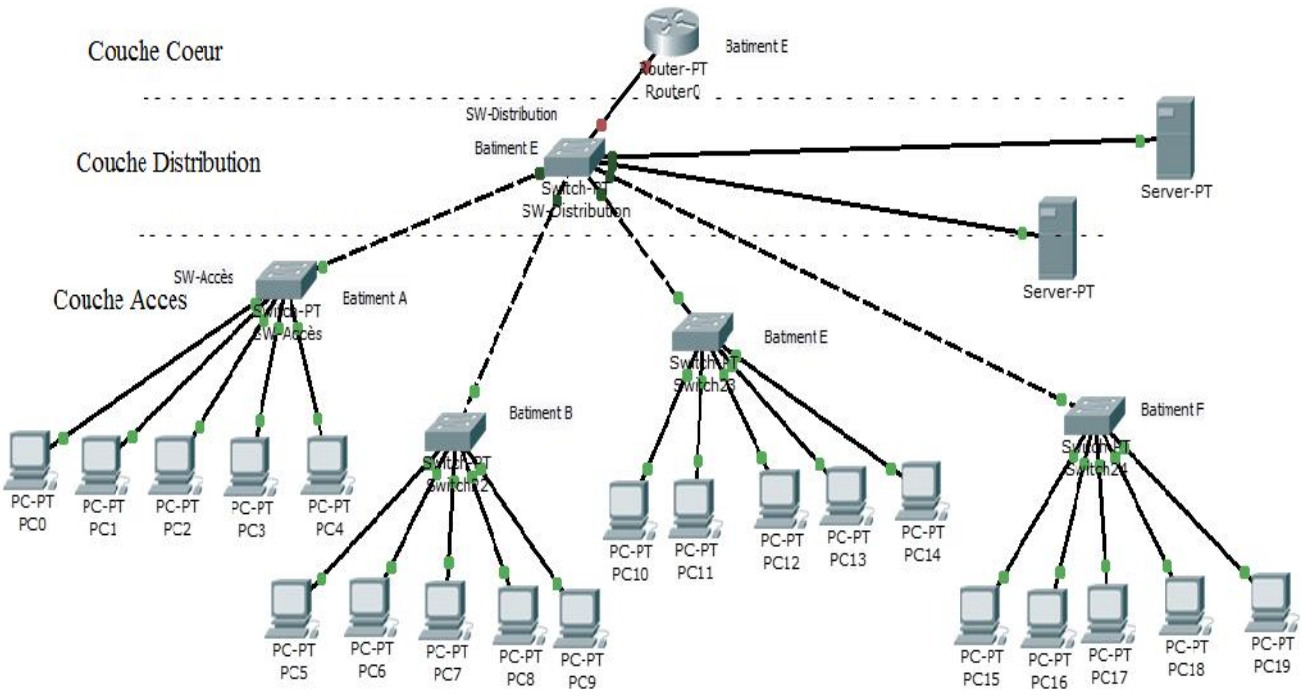

Figure IV.1 : Architecture de la station SP3.

- Couche Distribution : elle est composée d'un Switch de Distribution connecté au routeur, et qu'il lui est connecté les différents Switch d'Accès. Ce Switch permet la connectivité de couche Accès et la couche Cœur, et le filtrage.
- Couche Accès : elle est composée de 4 Switchs d'Accès situés dans divers bâtiments, qui sont attachés au Switch Distribution, tel que, chaque Switch d'Accès relie un ensemble de machines. Cette couche permet l'accès au réseau pour les utilisateurs rattachés aux segments locaux.

2. Présentation des équipements utilisés :

Tous les équipements utilisés au niveau de la SONATRACH, sont tous de même marque (Cisco) puisque ce sont des équipements fiables qui ont fait leur preuve. Comme tout le matériel utilisé est de même marque, ce qui évite tout problème de compatibilité entre les protocoles propriétaires. De plus, cela permet d'exploiter pleinement les protocoles développés par le constructeur.

Les équipements réseau utilisées sont présentés dans le tableau IV.1:

Equipments de modèle type	Nombre	Type et marque de Switch
Routeur	01	Cisco ISR 2811
Switch Distribution	01	WS-C3750G-12S-E Catalyst 3750 12 SFP + IPS Image
Switch d'Accès	04	WS-C3560G-48PS-S Catalyst 3560 48 10/100/1000T PoE + 4 SFP + IPB Image

Tableau IV.1: Liste des équipements utilisés.

3. Segmentation VLAN :

L'organisation réseau des stations de la RTC Bejaia et plus particulièrement le réseau la station SP3, se fera en le segmentant à l'aide des VLANs. Tels que, les différents VLANs qui existeront dans cette station, dépendent des différentes sections sur cette dernière, ainsi que les serveurs existants. Par conséquent, il y aura naissance de 6 VLANs, à savoir :

- ✓ VLAN Maintenance;
- ✓ VLAN Exploitation;
- ✓ VLAN HSE;
- ✓ VLAN Transport ;
- ✓ VLAN Administration;
- ✓ VLAN Serveur.

La figure IV.2 montre les différents VLANs de la station SP3 :

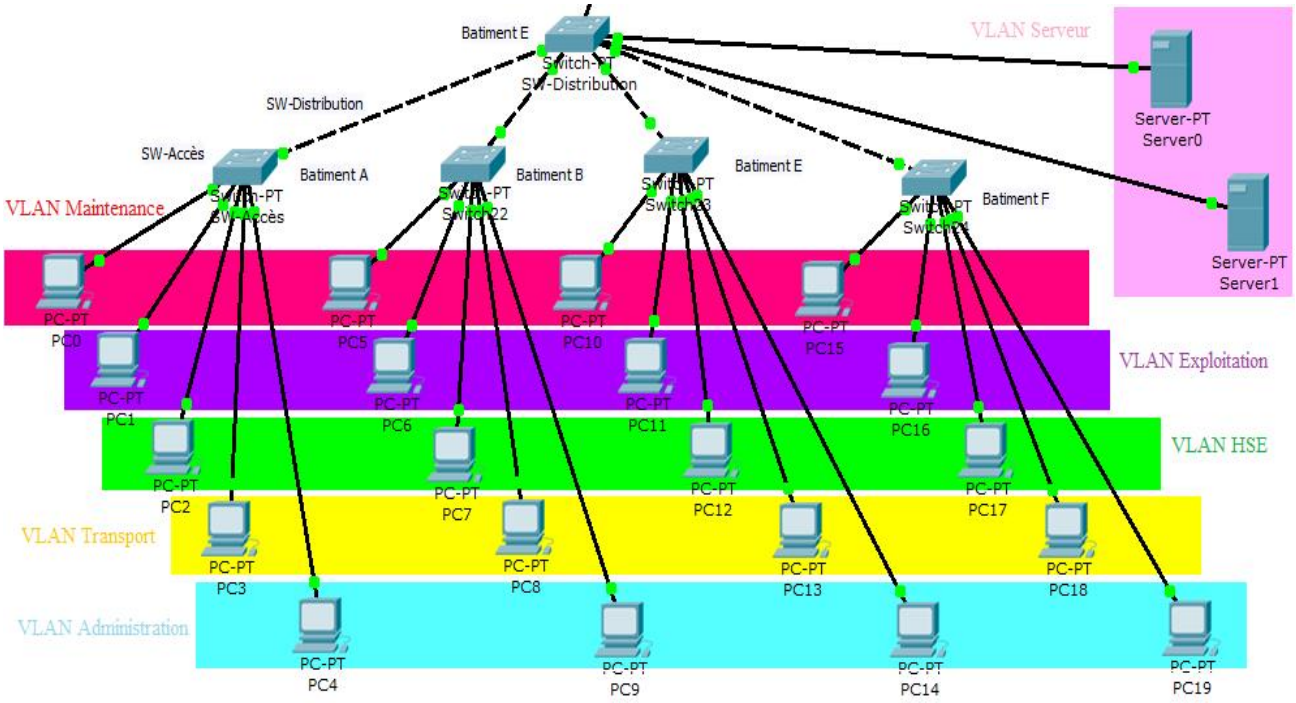

Figure IV.2: Les différents VLANs du réseau SP3.

4. Plan de nommage :

Le plan de nommage consiste à attribuer des noms bien particuliers à chaque équipement. Son objectif est de connaitre le type de l'équipement, s'il s'agit bien d'un serveur, Switch, routeur ou bien d'un PC. En plus, il permet de pouvoir localiser rapidement un équipement. En effet, grâce à ce nom, la zone au quelle appartient cette équipement peut être déduite.

4.1. Nominations des équipements :

Les équipements sont nommés par des noms significatifs pour faciliter l'administration et la gestion du réseau. Le tableau IV.2 présente les noms des différents équipements de la station SP3 :

Station SP3				
Couche Cœur	Couche Distribution	Couche Accès	Serveur	PCs
RT-Cœur	SW-Dist	SW-Acces-A SW-Acces-E SW-Acces-F SW-Acces-B	Sever –Active-D Server-Exchange	PC0, PC1, PC2, PC3, PC4.…PC18, PC19.

Tableau IV.2: Nom des équipements de la station SP3.

4.2. Désignations des interfaces :

Chaque équipement s'interconnecte à un autre équipement via une interface précise. Le Tableau IV.3 désignera la liste des interfaces qui participeront à l'interconnexion des différents équipements :

Equipement 1	Equipement 2	Interface Equipement1	Interface Equipement2
SW-Dist	SW-Acces-A	Fa0/1	Fa0/1
SW-Dist	SW-Acces-B	Fa1/1	Fa0/1
SW-Dist	SW-Acces-E	Fa2/1	Fa0/1
SW-Dist	SW-Acces-F	Fa3/1	Fa0/1
SW-Dist	Sever –Active-D	Fa4/1	Fa0/1
SW-Dist	Server-Exchange	Fa5/1	Fa0/1
SW-Dist	RT-Cœur	Fa6/1	Fa0/0
SW-Acces-A	PC0	Fa1/1	
SW-Acces-A	PC1	Fa2/1	
SW-Acces-A	PC2	Fa3/1	
SW-Acces-A	PC3	Fa4/1	
SW-Acces-A	PC4	Fa5/1	
SW-Acces-B	PC5	Fa1/1	
SW-Acces-B	PC6	Fa2/1	
SW-Acces-B	PC7	Fa3/1	
SW-Acces-B	PC8	Fa4/1	

SW-Acces-B	PC9	Fa5/1	
SW-Acces-E	PC10	Fa1/1	
SW-Acces-E	PC11	Fa2/1	
SW-Acces-E	PC12	Fa3/1	
SW-Acces-E	PC13	Fa4/1	
SW-Acces-E	PC14	Fa5/1	
SW-Acces-F	PC15	Fa1/1	
SW-Acces-F	PC16	Fa2/1	
SW-Acces-F	PC17	Fa3/1	
SW-Acces-F	PC18	Fa4/1	
SW-Acces-F	PC19	Fa5/1	

Tableau IV.3: Liste des interfaces.

4.3. Nomination des VLANs :

Les noms et identificateurs des VLANs à implémenter serons répartis comme suit :

Nom du VLAN	VLAN-ID	Description
Vlan_Defaut	1	Vlan par défaut
Vlan_Maint	10	Vlan pour Section Maintenance
Vlan_Expl	20	Vlan pour Section Exploitation
Vlan_HSE	30	Vlan pour Section HSE
Vlan_Trans	40	Vlan pour Section Transport
Vlan_Admin	50	Vlan pour Section Administration
Vlan_Server	60	Vlan pour les différents serveurs

Tableau IV.4: Liste des noms de VLANs.

5. Protocole VTP (VLAN Trunking Protocol):

Le protocole VTP (VLAN Trunking Protocol) est un protocole de la couche 2 propriétaire à Cisco, conçu pour palier aux problèmes opérationnels au sein des réseaux commutés comportants des VLANs.

VTP règle le problème de la configuration manuelle des VLANs. En effet, si le réseau a une taille considérable, la déclaration de tous les VLANs crées dans tous les commutateurs sera vraiment très difficile à réaliser, et cela est pareil lors de l'ajout d'un nouveau VLAN ou lors de la modification. Donc, la mise à jour des VLANs d'une façon manuelle est très difficile. Le protocole VTP, autorise les changements centralisés (ajout, suppression et modification) qui seront communiqués par les VTP-SEVER à tous les autres commutateurs VTP-CLIENT du réseau ou VTP-TRASPARENT (Voir Annexe A3). VTP permet ainsi d'éviter toute incohérence de configuration des VLANs.

Dans le réseau de la station SP3, c'est le commutateur Distribution (SW-Dist) qui est configuré comme serveur VTP (SERVER-VTP), par contre le reste des commutateurs seront considérés comme client VTP (CLIENT-VTP). Donc, toutes les modifications seront transmises à partir du SERVER-VTP vers tous les CLINET-VTP.

Le Tableau IV.5 désigne le SERVER-VTP et les CLIENT-VTP :

Equipement	Nom Domaine	Mode
SW-Dist	SP3	SEVER
SW-Acces-A	SP3	CLIENT
SW-Acces-B	SP3	CLIENT
SW-Acces-E	SP3	CLIENT
SW-Acces-F	SP3	CLIENT

Tableau IV.5 : Désignation VTP.

6. Trafic Entre-VLAN:

Le trafic entre-VLAN est assuré par un équipement de niveau 3. En effet pour que les machines puissent communiquer d'un VLAN à un autre, il est nécessaire de passer par un routeur en subdivisant logiquement l'interface liée au commutateur en sous-interfaces virtuelles, telle que, chaque sous-interface est attribuée à un VLAN donné. Le nombre des sous-interfaces à créer, est lié au nombre de VLANs existants. Ces sous-interfaces fournissent une solution pour le routage entre les différents VLANs.

Le concept d'agrégation ou bien le Trunk qui utilise la norme IEEE. 802.1Q pour l'identification des trames (Voir Annexe2), est indispensable, il consiste à regrouper plusieurs

liaisons virtuelles sur une liaison physique unique, la fonction d'un Trunk est de transporter les informations des VLANs entre plusieurs commutateurs interconnectés et donc d'étendre la portée des VLANs à un ensemble de commutateurs.

Les interfaces entre le commutateur Distribution (SW-Dist) et tous les commutateurs Accès (SW-Acces), ainsi l'interface entre le SW-Dist et le Roteur, doivent être toutes configurées en mode Trunk, afin qu'elles puissent transporter les informations des différents VLANs.

La Figure IV.3, donne une vue sur les liens Trunk :

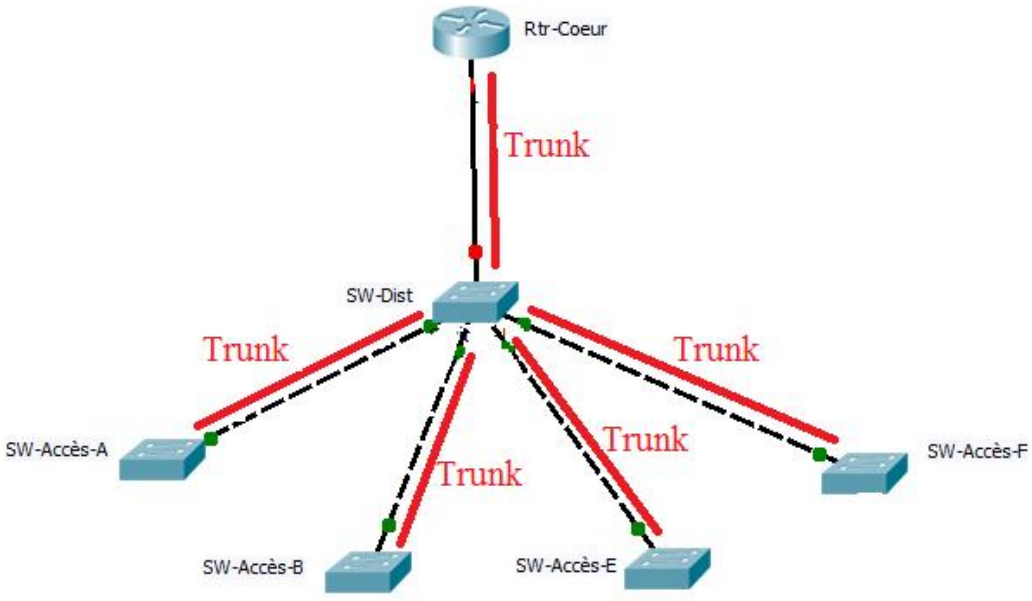

Figure IV.3 : Les liens du Trunk.

7. Plan d'adressage :

Un réseau ne peut bien fonctionner sans une attribution et une configuration correcte de différentes adresses. Le plan d'adressage est la stratégie qui s'applique afin de permettre l'accessibilité des différentes entités d'un réseau de la manière la plus optimale.

L'objectif premier du plan d'adressage, est d'éviter la duplication accidentelle des adresses, c'est-à-dire, il permet de désigner un équipement sans ambigüité, car une adresse IP affectée ne doit être réutilisée.

L'élaboration d'un plan d'adressage nécessite la prise en considération de certaines règles, telle que, la classe d'adressage, la définition de sous-réseau, l'attribution statique et/ou dynamique des adresses. De plus, le plan d'adressage élaboré doit comprendre la notion d'évolutivité. En effet, il doit pouvoir s'adapter à la croissance de l'entreprise, permettre un éventuel aménagement avenir et pouvoir accueillir de nouveaux segments VLANs, et tout cela afin de palier aux pénuries d'adresses et sans devoir changer carrément le plan existant.

7.1. Adressage des VLANs :

L'adressage du réseau de la RTC Bejaia doit respecter l'adresse réseau attribuée par la société SONATRACH à cette région, c'est-à-dire à la Région Transport Centre (RTC Bejaia). Cette adresse est : 10.136.0.0/16, avec une possibilité de création de 255 sous-réseaux, c'est-à-dire, étendre l'adresse réseau de 8 bits à droite pour supporter les 255 sous-réseaux, avec un masque : 255.255.255.0

Donc, l'adressage de tous les réseaux locaux de toutes les stations, se basera sur des adresses privées, et à partir de ces adresses, que l'affectation des adresse IP pour l'ensemble des équipements et des VLANs, va être accomplie.

À partir de l'adresse réseau 10.136.0.0/16, que les sous-réseaux pour l'ensemble des VLANs, vont être crées en affectant ainsi, des adresses pour leurs équipements. Les machines affiliées à un VLAN, vont prendre toutes des adresse IP d'une même adresse sous-réseau.

Le Tableau IV.6, illustre les différentes adresses des VLANs :

Nom VLAN	VLAN-ID	Adresse sous-réseau
Vlan Défaut	1	10.136.1.0/24
Vlan Maint	10	10.136.10.0/24
Vlan Expl	20	10.136.20.0/24
Vlan HSE	30	10.136.30.0/24
Vlan Trans	40	10.136.40.0/24
Vlan Admin	50	10.136.50.0/24
Vlan Server	60	10.136.60.0/24

Tableau IV.6: Plan d'adressage des VLANs.

7.2. Administration des équipements :

Le VLAN par défaut (VLAN 1) sera utilisé pour l'administration des équipements.

Les adresses IP pour le VLAN natif de la station SP3, seront attribuées à partir de l'adresse 10.136.1.0/24 comme le montre le Tableau IV.7 :

Nom équipement	VLAN-ID	Adresse IP VLAN
SW-Dist	1	10.136.1.2/24
SW-Acces-A	1	10.136.1.3/24
SW-Acces-B	1	10.136.1.4/24
SW-Acces-E	1	10.136.1.5/24
SW-Acces-F	1	10.136.1.6/24

Tableau IV.7: Plan d'adressage du VLAN natif.

7.3. Adressage des PCs et serveurs :

Chaque équipement numérique a besoin d'une adresse pour qu'il soit accessible et qu'il puisse communiquer avec les autres équipements du réseau.

Le Tableau IV.8 montre l'attribution des adresses IP aux PCs :

PC /serveurs	Switch	N° port	VLAN-ID	Adresse IP	Passerelle par défaut
PC0	SW-Acces-A	Fa 1/1	10	10.136.10.2/24	10.136.10.1/24
PC1	SW-Acces-A	Fa 2 /1	20	10.136.20.2/24	10.136.20.1/24
PC2	SW-Acces-A	Fa 3 /1	30	10.136.30.2/24	10.136.30.1/24
PC3	SW-Acces-A	Fa 4 /1	40	10.136.40.2/24	10.136.40.1/24
PC4	SW-Acces-A	Fa 5/1	50	10.136.50.2/24	10.136.50.1/24
PC5	SW-Acces-B	Fa 1/1	10	10.136.10.3/24	10.136.10.1/24
PC6	SW-Acces-B	Fa 2 /1	20	10.136.20.3/24	10.136.20.1/24
PC7	SW-Acces-B	Fa 3 /1	30	10.136.30.3/24	10.136.30.1/24
PC8	SW-Acces-B	Fa 4 /1	40	10.136.40.3/24	10.136.40.1/24
PC9	SW-Acces-B	Fa 5/1	50	10.136.50.3/24	10.136.50.1/24

PC10	SW-Acces-E	Fa 1/1	10	10.136.10.4/24	10.136.10.1/24
PC11	SW-Acces-E	Fa 2 /1	20	10.136.20.4/24	10.136.20.1/24
PC12	SW-Acces-E	Fa 3 /1	30	10.136.30.4/24	10.136.30.1/24
PC13	SW-Acces-E	Fa 4 /1	40	10.136.40.4/24	10.136.40.1/24
PC14	SW-Acces-E	Fa 5/1	50	10.136.50.4/24	10.136.50.1/24
PC15	SW-Acces-F	Fa 1/1	10	10.136.10.5/24	10.136.10.1/24
PC16	SW-Acces-F	Fa 2 /1	20	10.136.20.5/24	10.136.20.1/24
PC17	SW-Acces-F	Fa 3 /1	30	10.136.30.5/24	10.136.30.1/24
PC18	SW-Acces-F	Fa 4 /1	40	10.136.40.5/24	10.136.40.1/24
PC19	SW-Acces-F	Fa 5/1	50	10.136.50.5/24	10.136.50.1/24
Sever – Active-D	SW-Dist	Fa 4/1	60	10.136.60.2/24	10.136.60.1/24
Server-Exchange	SW-Dist	Fa 5/1	60	10.136.60.3/24	10.136.60.1/24

Tableau IV.8 : Plan d’adressage des PCs et seveurs.

8. Plan de Routage :

Un bon plan de routage vise à faciliter la gestion d’un système autonome, en automatisant au maximum la construction des tables de routage. Les routeurs vont échanger les informations concernant leurs voisins du réseau par l’intermédiaire du protocole du routage OSPF.

L’implémentation du protocole OSPF se fera au niveau de tous les routeurs des stations constituants le Backbone de la RTC. En effet, toutes les adresses réseaux directement connectées à un routeur, doivent être déclarées, pour que le routage fonctionne correctement.

La figure IV.4 montre les différents routeurs du Backbone de la RTC Bejaia, ainsi que les adresses de leurs interfaces et/ou sous-interfaces :

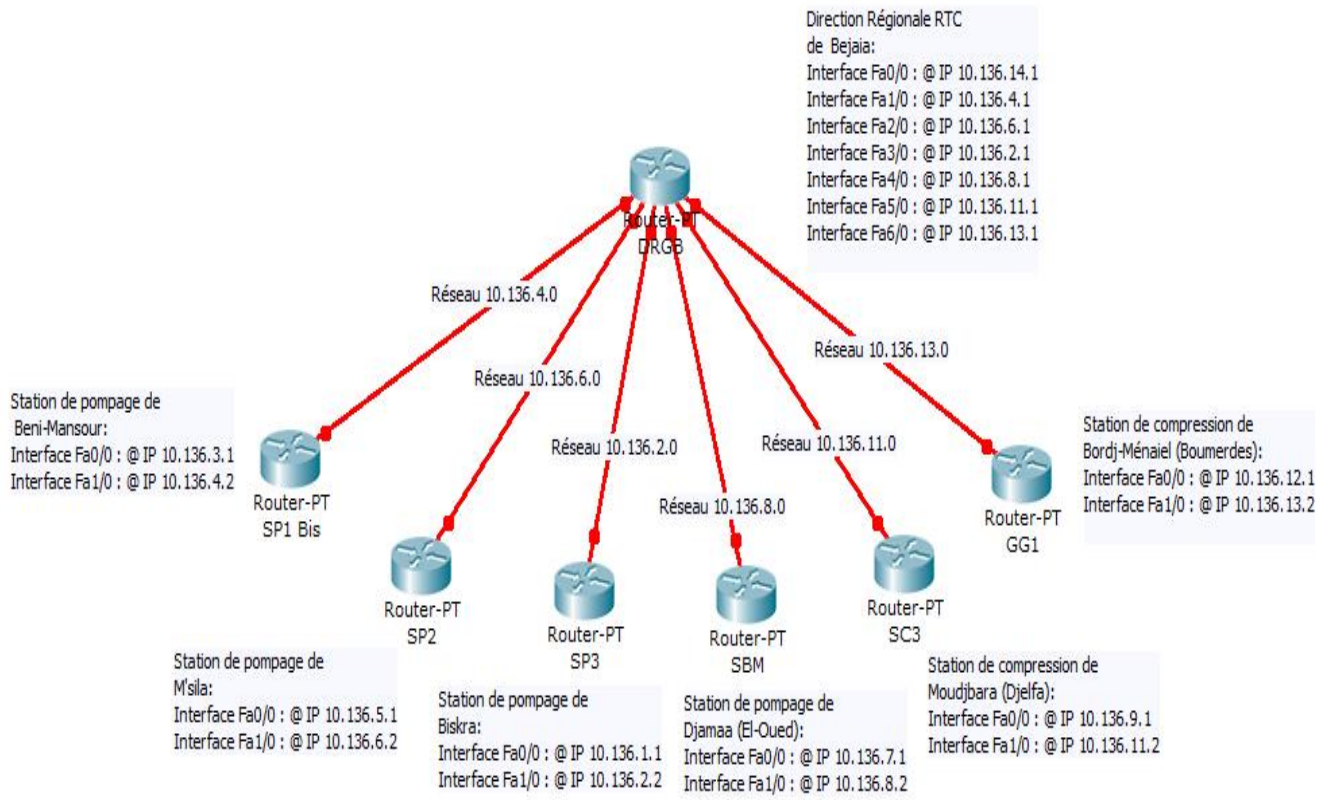

Figure IV.4 : Les routeurs du Backbone de la RTC Bejaia.

Le Tableau IV.9 donne une image de chaque routeur avec les réseaux qui lui y sont directement connectés :

Routeurs	Interface	Adresse IP	Réseau directement connectés
Routeur SP3	Fa 0/0	10.136.1.1	10.136.1.0/24
	Fa 1/0	10.136.2.2	10.136.2.0/24
Routeur SP1 Bis	Fa 0/0	10.136.3.1	10.136.3.0/24
	Fa 1/0	10.136.4.2	10.136.4.0/24
Routeur SP2	Fa 0/0	10.136.5.1	10.136.5.0/24
	Fa 1/0	10.136.6.2	10.136.6.0/24
Routeur SBM	Fa 0/0	10.136.7.1	10.136.7.0/24
	Fa 1/0	10.136.8.2	10.136.8.0/24
Routeur GG1	Fa 0/0	10.136.12.1	10.136.12.0/24
	Fa 1/0	10.136.13.2	10.136.13.0/24
Routeur SC3	Fa 0/0	10.136.9.1	10.136.9.0/24
	Fa 1/0	10.136.11.2	10.136.11.0/24

Routeur RTC	Fa 0/0	10.136.14.1	10.136.14.0/24
	Fa 1/0	10.136.4.2	10.136.4.0/24
	Fa 2/0	10.136.6.2	10.136.6.0/24
	Fa 3/0	10.136.2.2	10.136.2.0/24
	Fa 4/0	10.136.8.2	10.136.8.0/24
	Fa 5/0	10.136.11.2	10.136.11.0/24
	Fa 6/0	10.136.13.2	10.136.13.0/24

Tableau IV.9: Réseaux interconnectés directement aux routeurs.

Conclusion :

La phase planification du projet à été réalisée dans le but de permettre le commencement de la phase finale. Pratiquement parlant, c'est la phase mise en œuvre. Le chapitre suivant, contiendra la partie réalisation et mise en œuvre, c'est-à-dire, appliquer les solutions proposées au niveau du réseau de la RTC Bejaia.

CHAPITRE V

MISE EN ŒUVRE ET REALISATION

Introduction :

Chaque projet ou travail, commence généralement par une étude théorique, et se termine par une étude pratique qui est la mise en œuvre de la solution ou bien la réalisation du projet.

Ce présent chapitre, consistera à mettre en œuvre les solutions proposées pour la réalisation de son projet, avec l'ensemble des configurations nécessaires à implémenter sur les LANs de la RTC Bejaia. Ces configurations entourent entre la configuration des VLANs, l'adressage et le routage, en se basant sur le simulateur Cisco Packet Tracer pour y réaliser. Enfin, des tests de validation pour confirmer le bon fonctionnement du réseau, seront réalisés.

1. Présentation du simulateur Cisco « Packet Tracer » :

Packet Tracer est un simulateur de réseau puissant développé par Cisco Systems pour faire des plans d'infrastructure de réseau en temps réel. Il offre la possibilité de créer, visualiser et de simuler les réseaux informatiques. L'objectif principal de simulateur, est de schématiser, configurer et de voir toute les possibilités d'une future mise en œuvre réseau. Cisco Packet Tracer est un moyen d'apprentissage de la réalisation de divers réseaux et découvrir le fonctionnement des différents éléments constituants un réseau informatique.

La Figure V.1 est une image montrant l'interface principale du simulateur Cisco Packet Tracer :

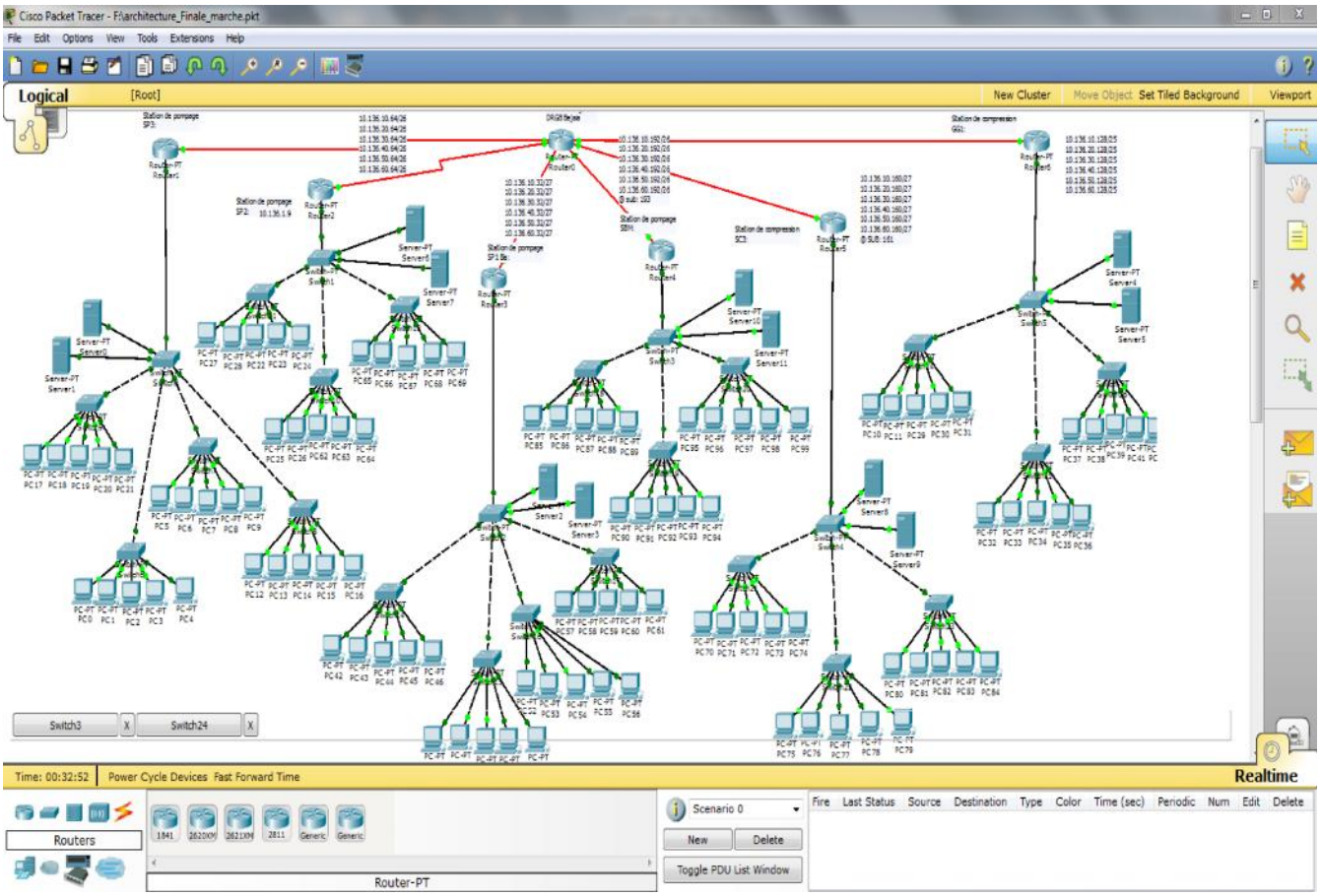

Figure V.1: Cisco Packet Tracer.

2. Interface commande de Packet Tracer :

Toutes les configurations des équipements du réseau, c'est au niveau de CLI (Command Language Inteface) quelles seront réalisées. CLI est une interface de simulateur Packet Tracer qui permet la configuration des équipements du réseau à l'aide d'un langage de commandes, c'est-à-dire qu'à partir des commandes introduite par l'utilisateur du logiciel, que la configuration est faite.

La Figure V.2 est l'interface CLI du Packet Tracer:

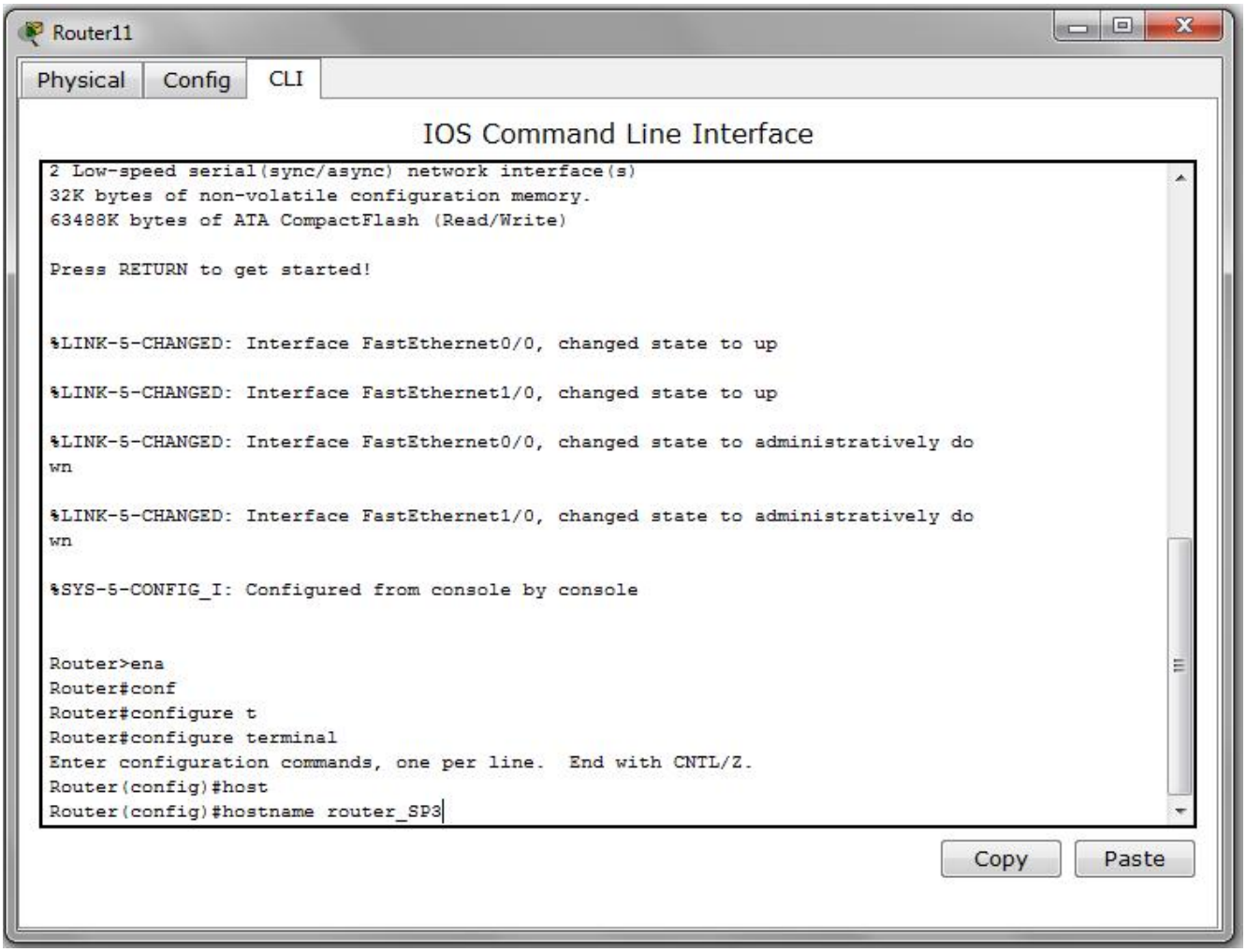

Figure V.2 : Interface CLI.

3. Configuration des équipements :

La configuration des équipements du réseau de la RTC Bejaia, est la configuration des commutateurs et les routeurs constituants les réseaux locaux des stations. En effet, une série de configurations sera réalisée à travers ces équipements, en montrant un exemple de chaque configuration.

3.1. Configuration des commutateurs :

Cette configuration contiendra un ensemble de points à configurer, en commençant d'abord, par une petite configuration des noms de chaque commutateur, ensuite configurer les différents VLANs existants, ainsi la configuration des interfaces du commutateur, en tenant compte bien sur, de l'ensemble des protocoles à implémenter, tel que VTP, Spanning-Tree et OSPF.

Pour la configuration du protocole OSPF, rappelant que les commutateurs de chaque LAN sont de niveau 3.Donc, supportent le routage. Prenant l'exemple du Switch Distribution du LAN SP3.

3.1.1. Configuration du Hostname :

Cette étape consiste à donner un nom significatif à l'ensemble des équipements constituant les LANs des stations. Par exemple, la nomination du commutateur Distribution de la station SP3, comme l'indique la Figure V.3 :

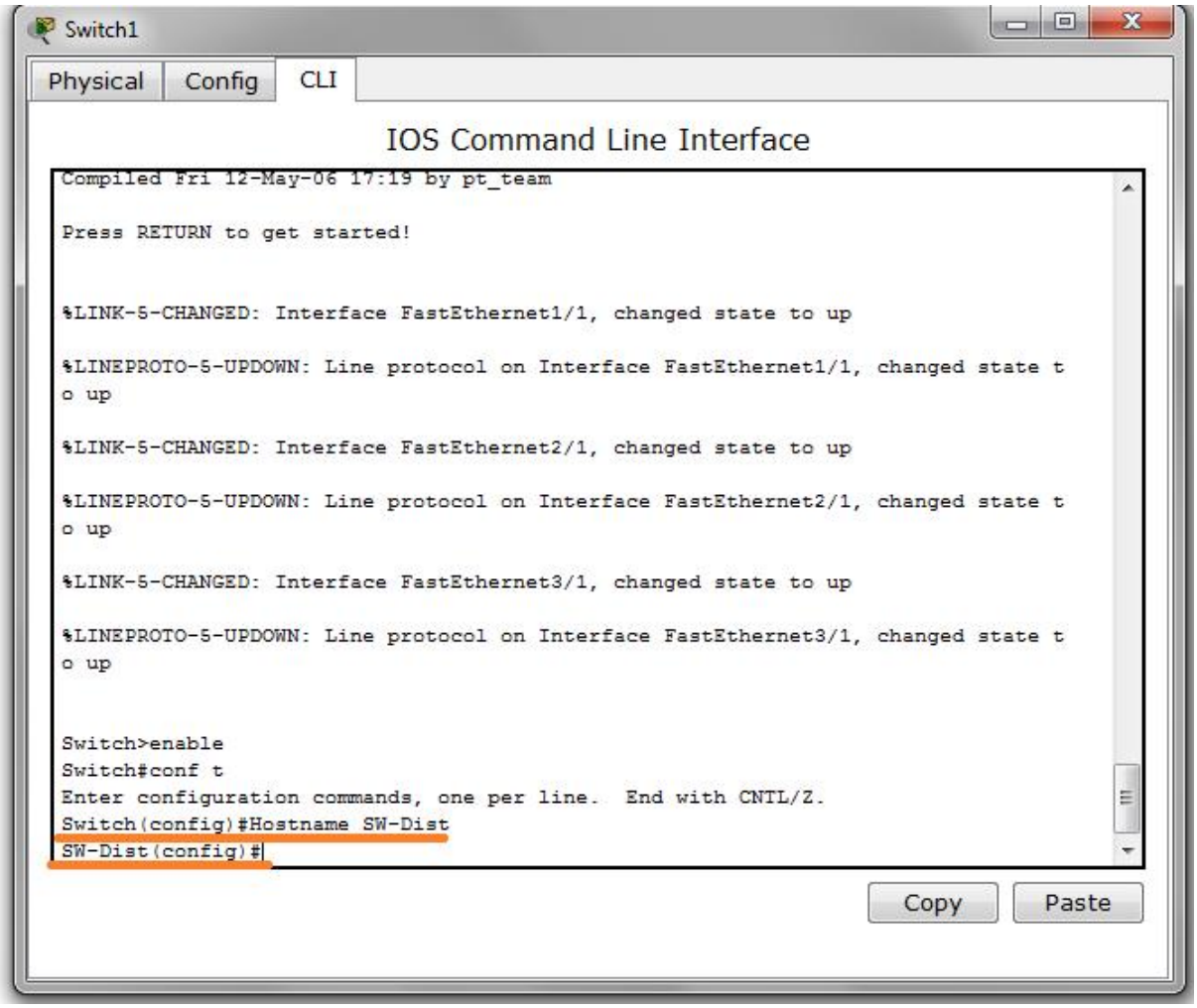

Figure V.3 : Nomination le Switch Distribution.

3.1.2. Configuration des VLANs :

La configuration des VLANs est faite au niveau des commutateurs Distribution dans chaque réseau local, comme le montre la Figure V.4 :

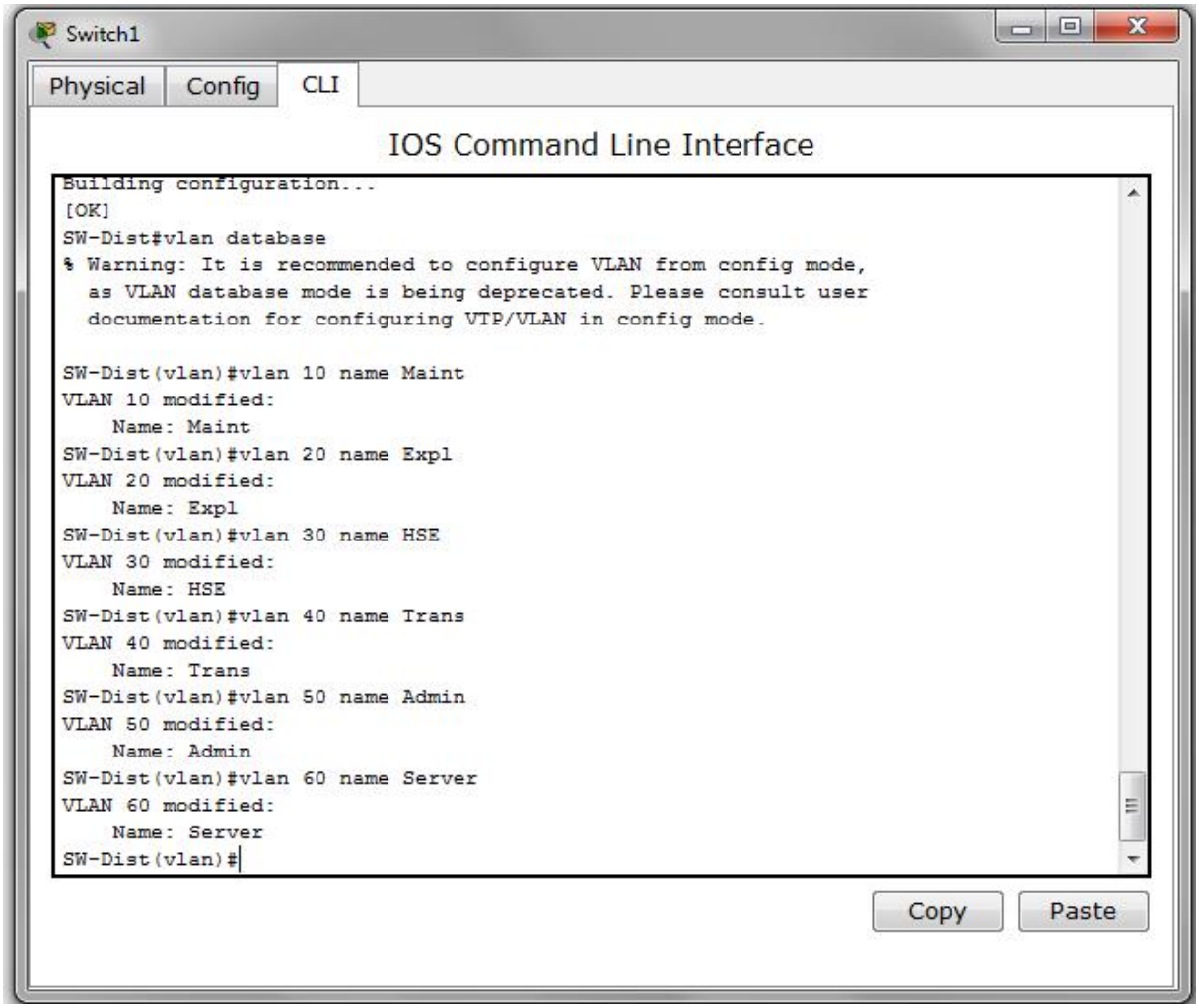

Figure V.4 : Création des VLANs.

3.1.3. Configuration du protocole VTP :

L'ensemble des commutateurs Distribution des LANs de la RTC Bejaia, seront configurés comme des Server-VTP. Donc, ce sont eux qui gèrent l'administration de l'ensemble des VLANs. Un nom de domaine est attribué, dans le cas présent c'est «SP3» en plus d'un mot de passe du domaine qui est « RTC ».

La Figure V.5 est un exemple de configuration VTP-Server :

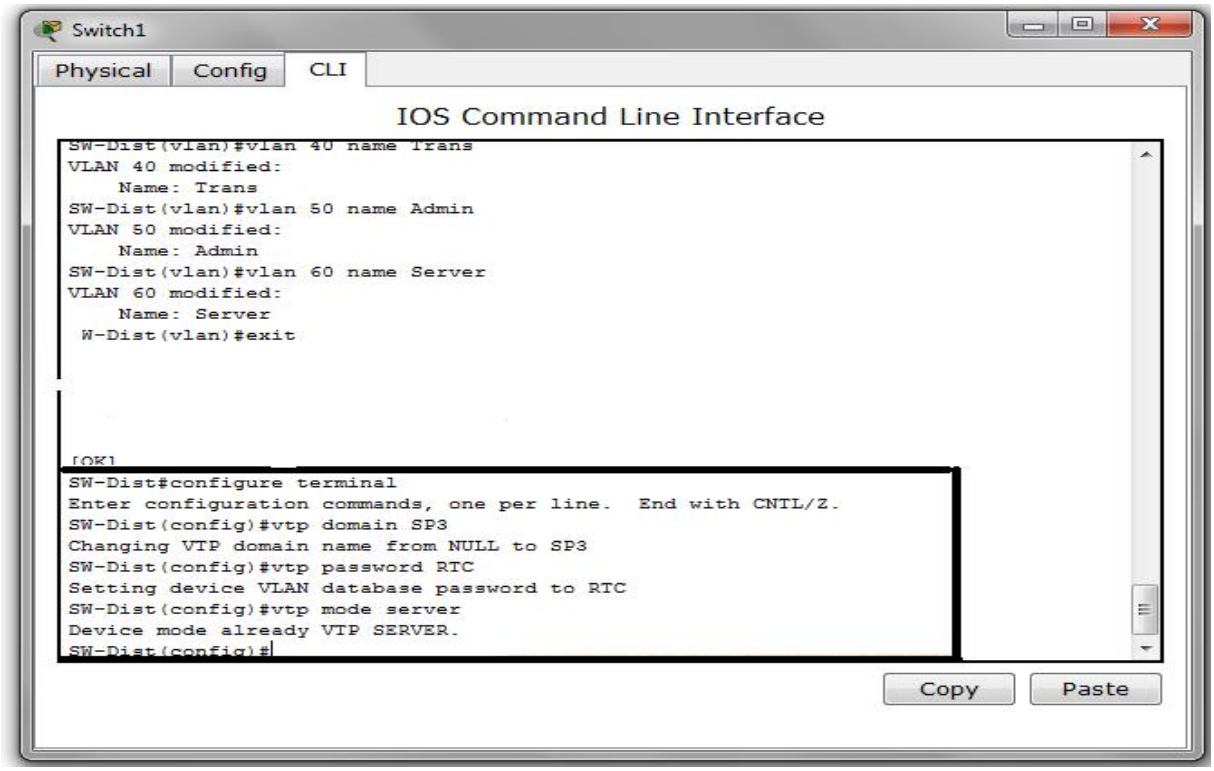

Figure V.5 : Configuration des VTP-Server.

Par ailleurs, la configuration des Client-VTP sera au niveau de tous les commutateurs Accès des LANs des stations, en respectant le même nom du domaine et mot de passe, comme le montre la Figure V.6 :

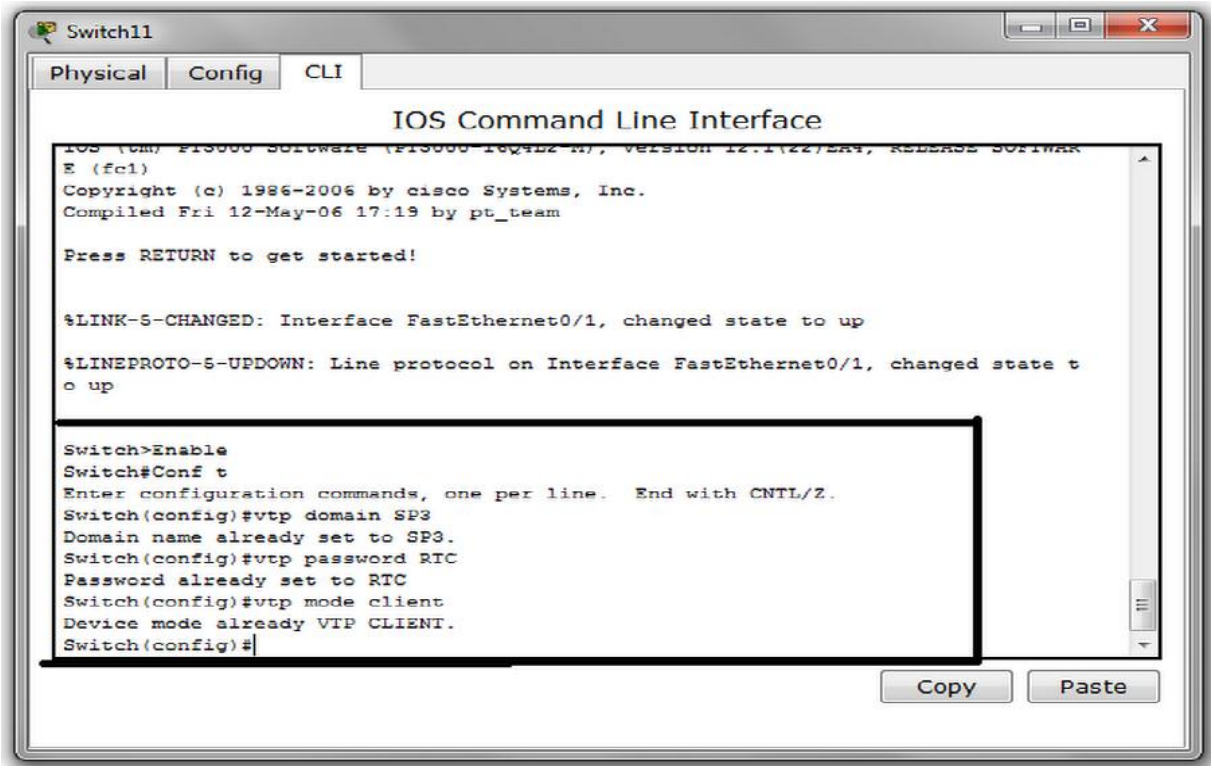

Figure V.6 : Configuration Client-VTP.

3.1.4. Configuration des interfaces VLAN :

La configuration des interfaces VLANs, est faite au niveau de chaque commutateur de chaque station, en donnant des adresses IP pour les VLANs natifs à ce stade.

La Figure V.7 illustre un exemple de configuration de l'interface VLAN :

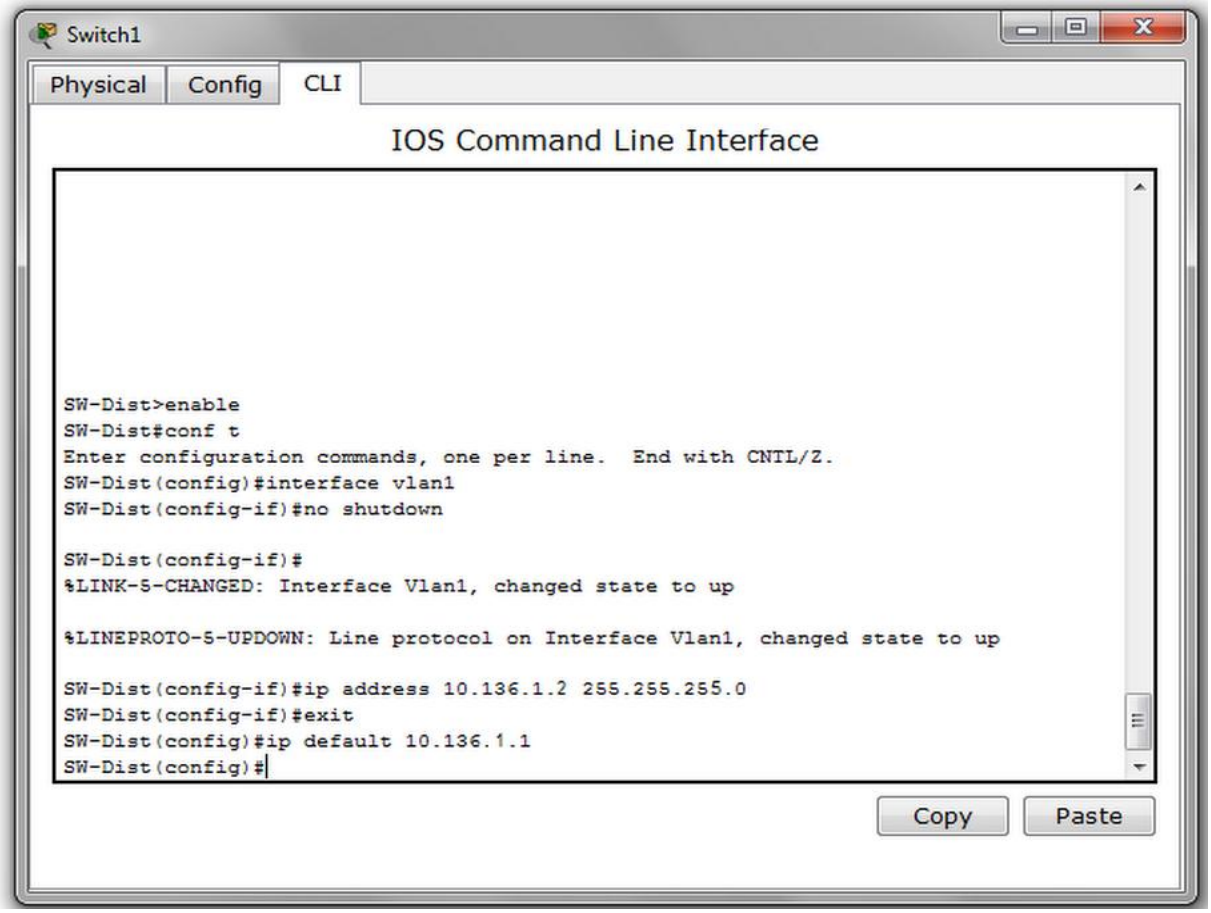

Figure V.7 : Configuration des interfaces VLANs.

3.1.5. Configuration des interfaces :

Les interfaces des équipements d'interconnexion à configurer en mode Trunk, sont toutes les interfaces existantes entre l'ensemble des commutateurs Accès et commutateur Distribution, ainsi celle du commutateur Distribution avec le routeur. Pour le commutateur Distribution de SP3, ce sont les interfaces reliées à l'ensemble des commutateurs Accès, ainsi au routeur. À vrai dire, les interfaces : Fa0/1, Fa1/1, Fa2/1, Fa3/1 et l'interface Fa4/1.

La Figure V.8 est exemple de configuration des liens Trunk :

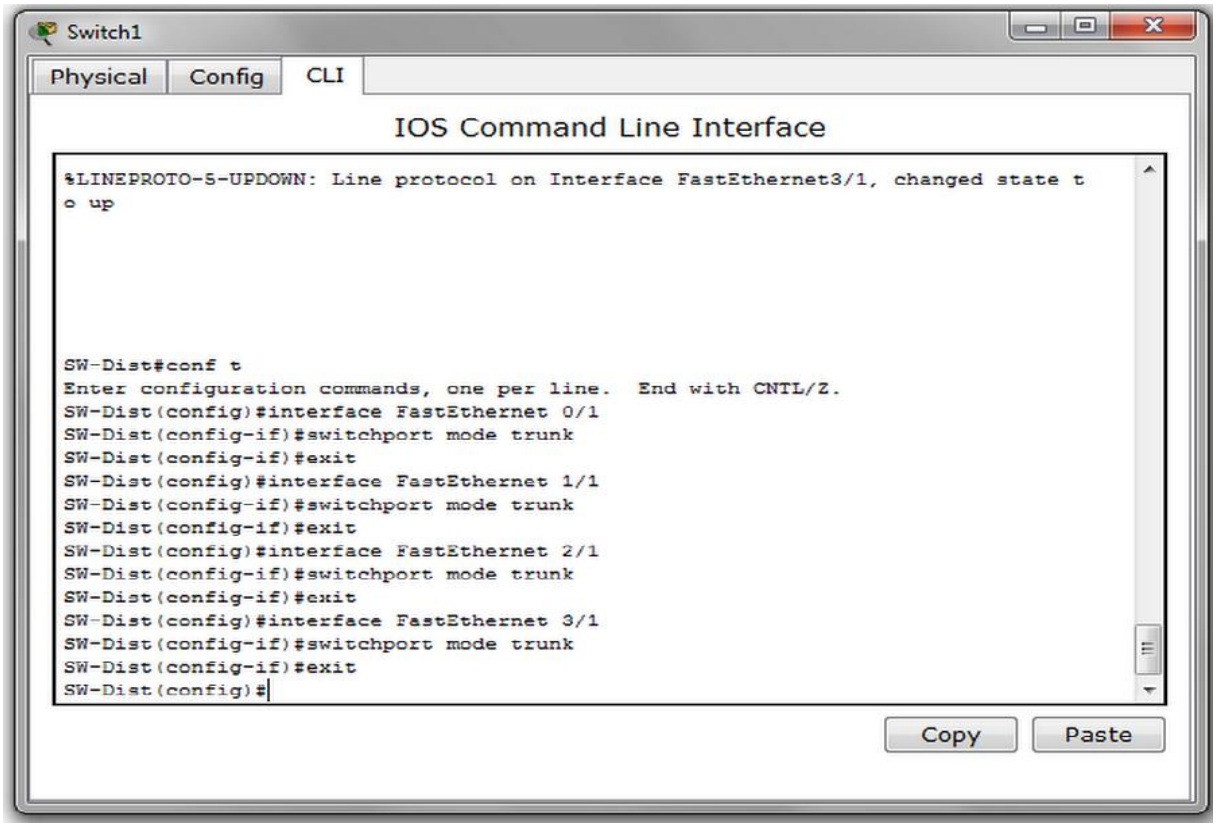

Figure V.8 : Configuration des liens trunk.

3.1.6. Attribution des ports des commutateurs aux VLANS :

C'est au niveau de chaque commutateur Accès, que les ports vont être assignés aux différents VLANs existés. En effet, chaque port d'un commutateur appartiendra à un VLAN donné.

La Figure V.9 montre l'attribution des ports de commutateur à des VLANs donnés :

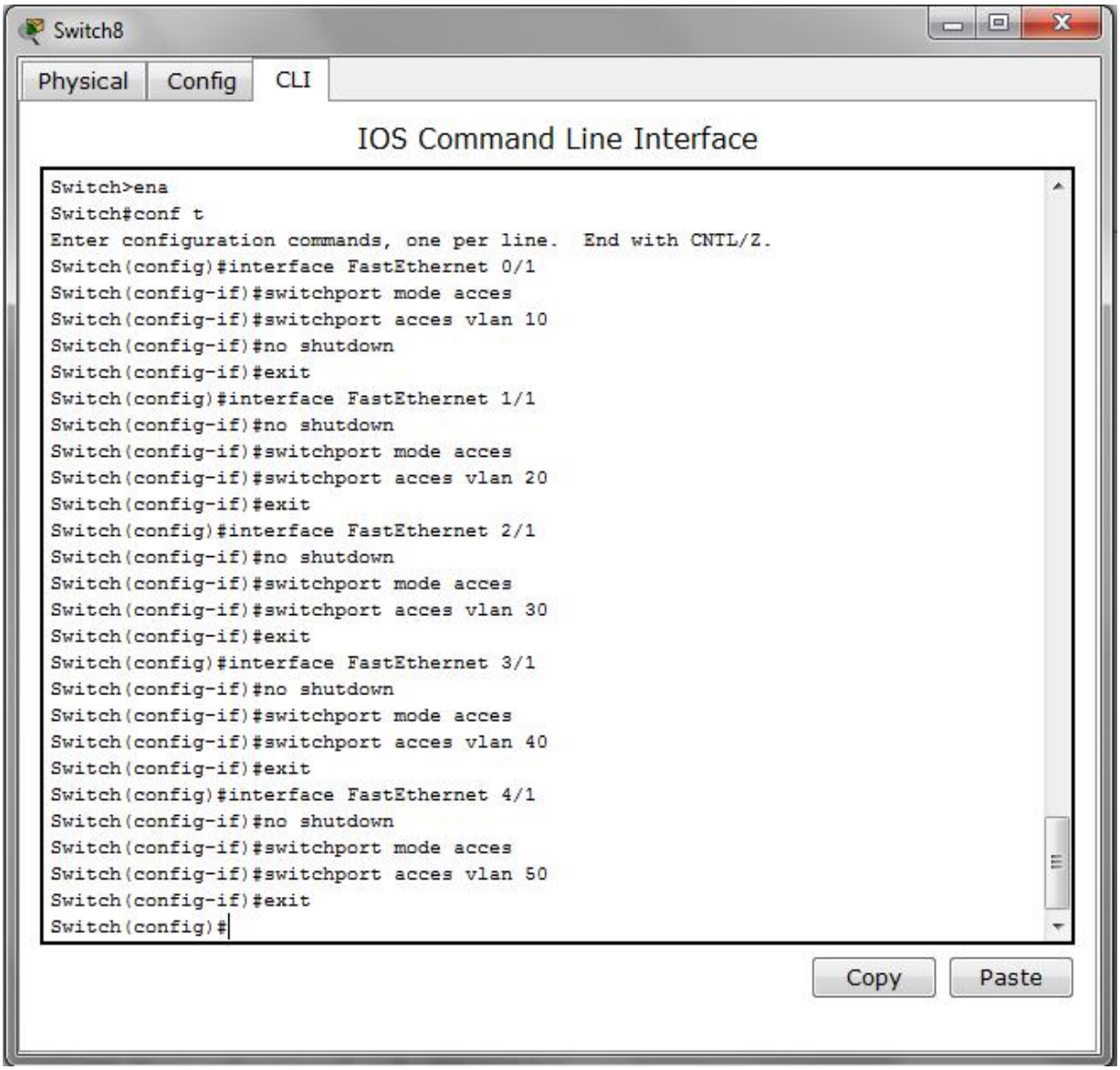

Figure V.9: Attribution des ports aux VLANs.

Par contre, pour les commutateurs Distribution, comme les deux serveurs sont connectés à ce dernier, le VLAN Server va être affecté au deux port de celui-ci. Comme le montre la Figure V.10 :

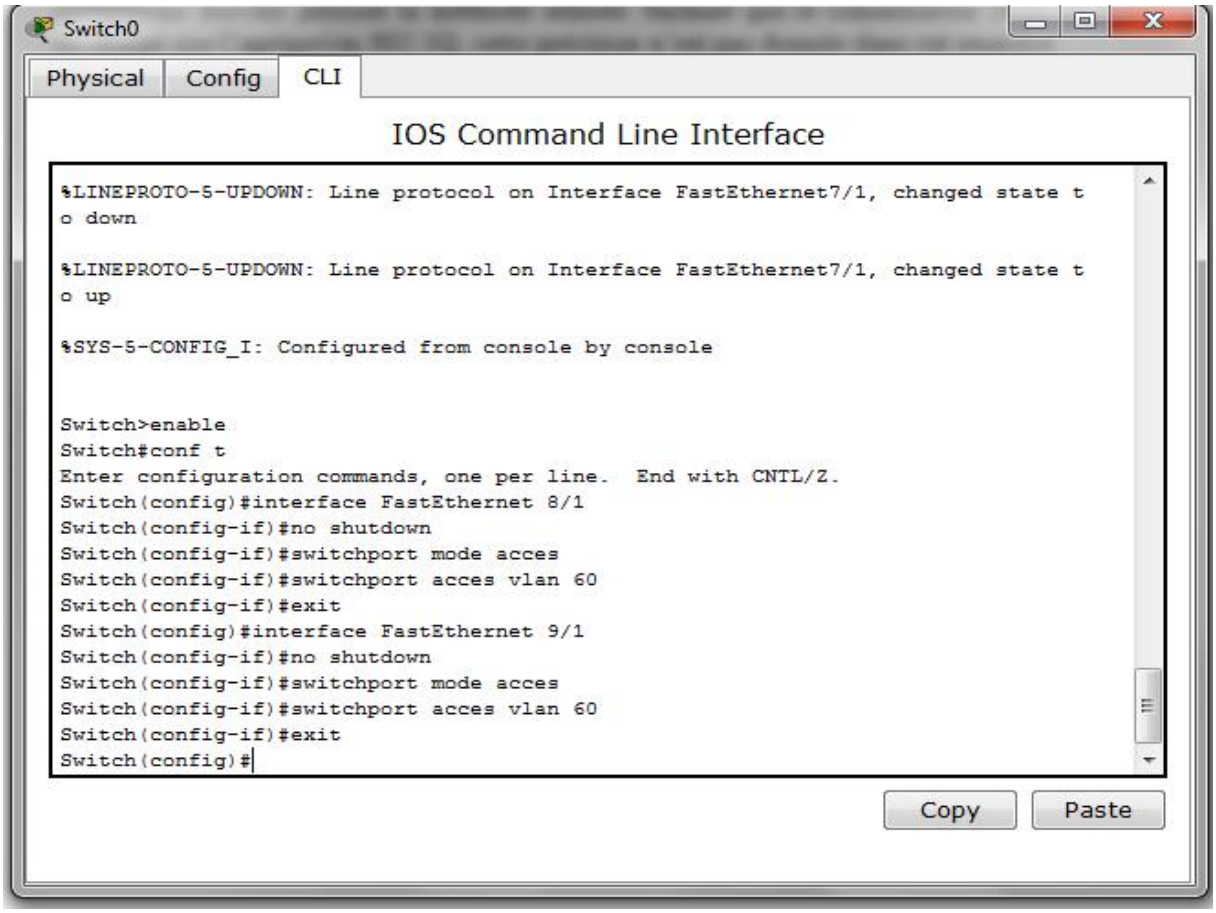

Figure V.10 : Attribution des ports au VLAN Server.

4. Configuration des routeurs :

Dans le cas des routeurs, la configuration consiste primordialement à configurer la communication entre-VLAN en subdivisant l'interface FastEthernet 0/0, celle reliée avec le commutateur Distribution, en un ensemble de sous interfaces suivant le nombre de VLAN existants. Finalement, reste à configurer le routage.

4.1. Subdivision de l'interface routeur-commutateur Distribution :

La subdivision de l'interface reliant le routeur et le commutateur Distribution, a pour but, d'accomplir la communication entre les différents VLANs (communication entre-VLAN). En effet, subdiviser l'interface en un nombre de sous interfaces, dépendant du nombre de VLAN qui existent, en leur affectant, ainsi, des adresse IP pour chacune d'elles.

La Figure V.11 illustre la manière avec laquelle la subdivision est faite :

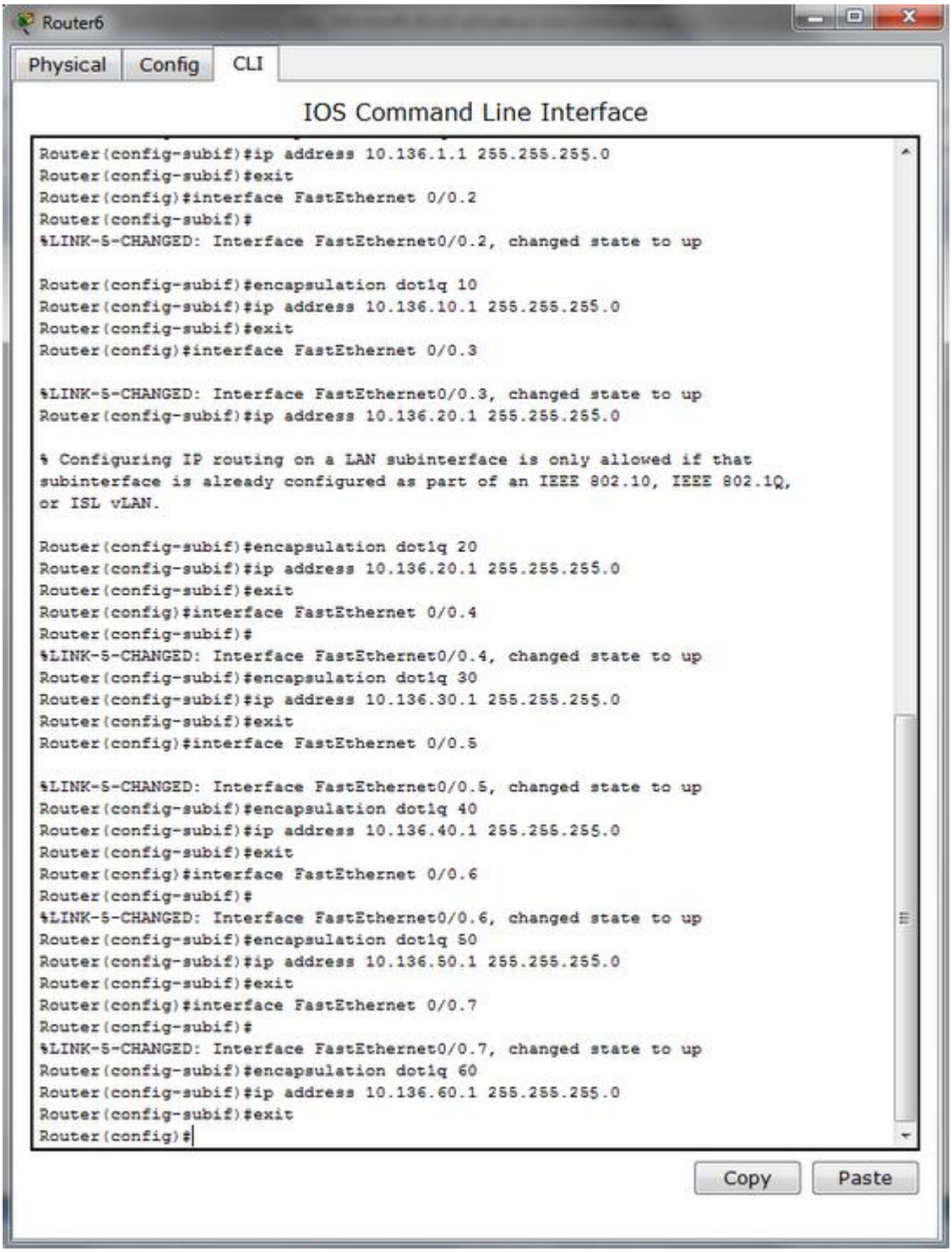

Figure V.11 : Subdivision de l'interface routeur.

4.2. Configuration des interfaces du routeur :

Les interfaces de chaque routeur doivent avoir une adresse IP pour qu'elles puissent communiquer avec les autres. La Figure V.12 montre la configuration des interfaces du routeur :

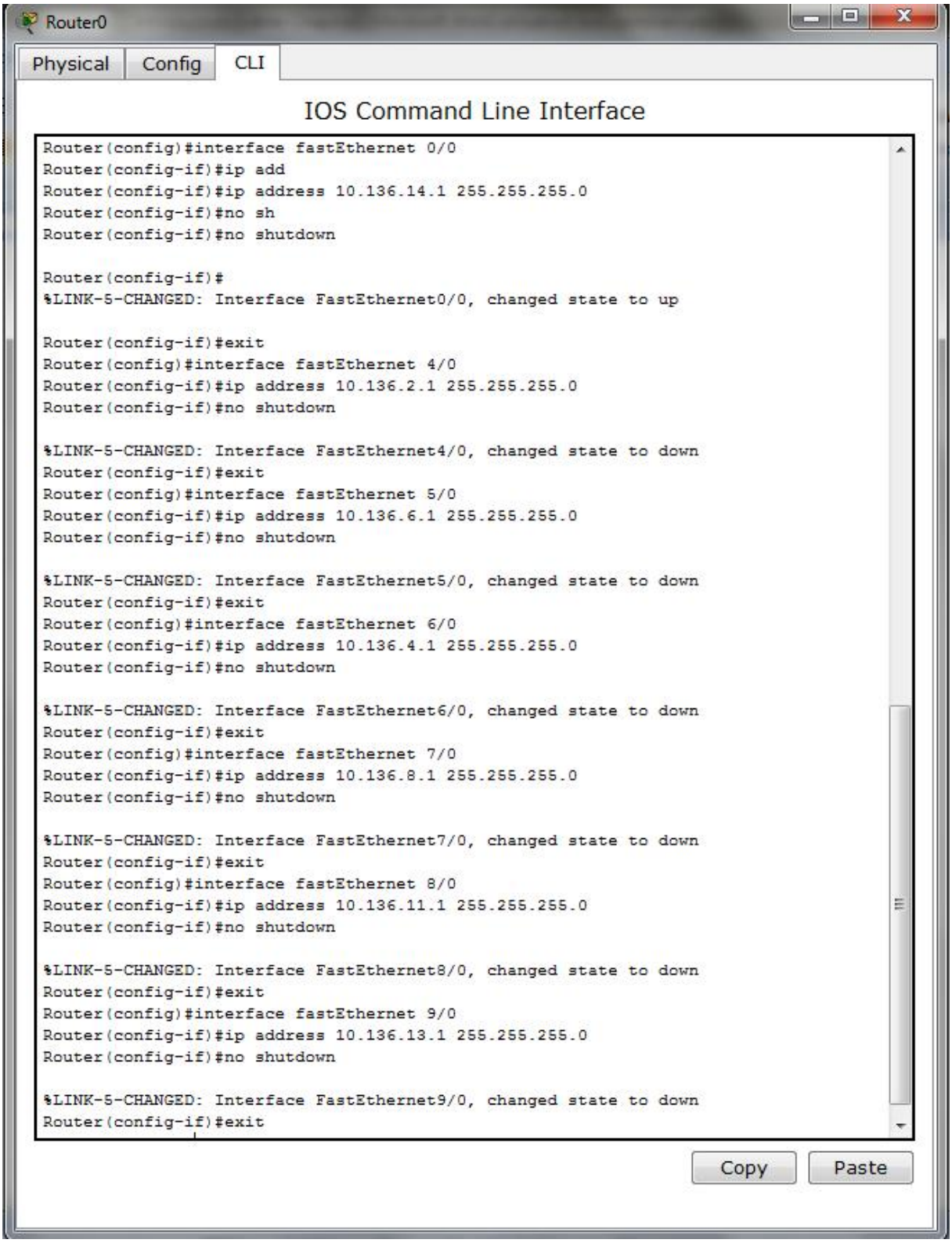

Figure V.12 : Configuration des interfaces routeur.

4.3. Configuration du routage :

Le routage consiste à déclarer au niveau de chaque routeur, les réseaux qui lui y sont directement connectés. Donc, pour chaque routeur, l'implémentation du protocole OSPF, est indispensable.

- ✓ Pour le routeur de la DRGB Bejaia :

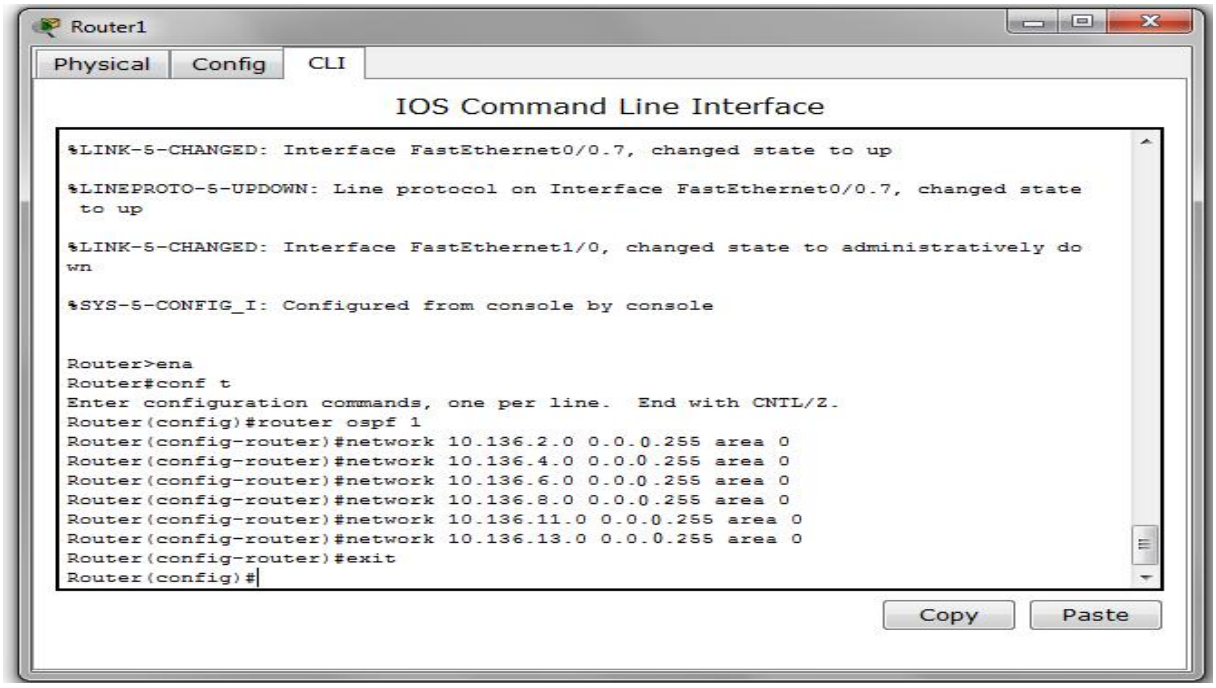

Figure V.13 : Routage au niveau du routeur DRGB.

- ✓ Pour le routeur de la station SP3 :

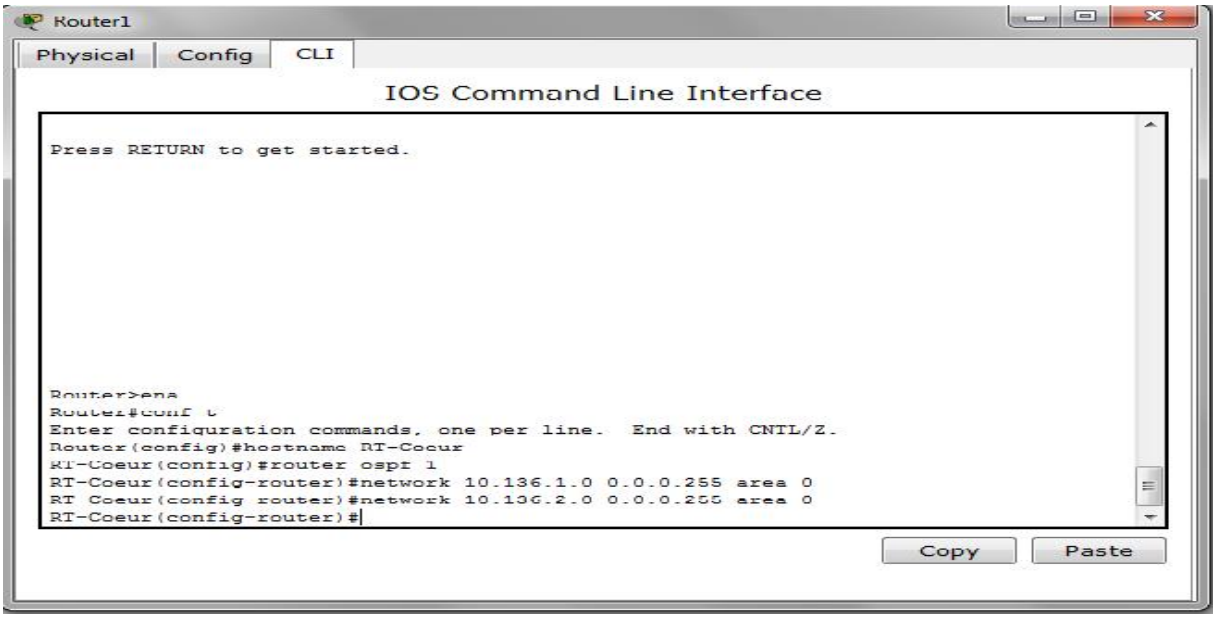

Figure V.14 : Routage au niveau du routeur SP3.

✓ Pour le routeur de la station SP1 Bis :

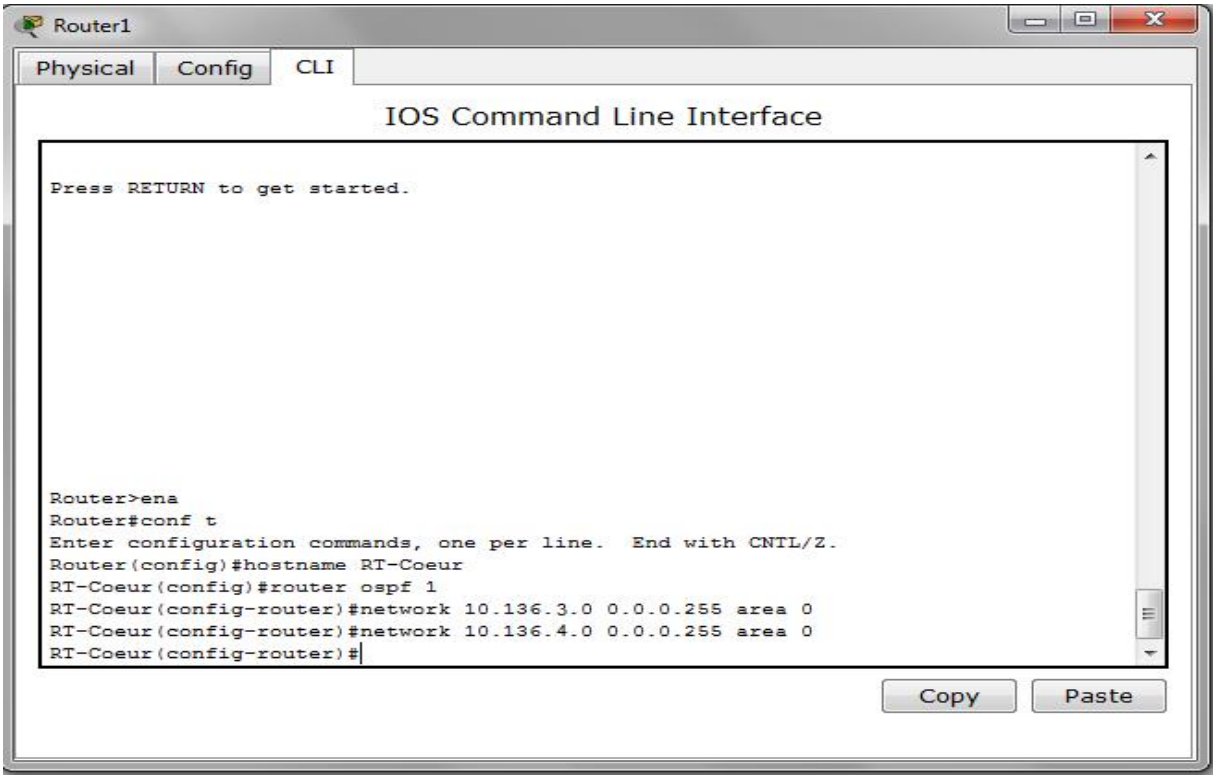

Figure V.15 : Routage au niveau du routeur SP1 Bis.

✓ Pour le routeur de la station SP2 :

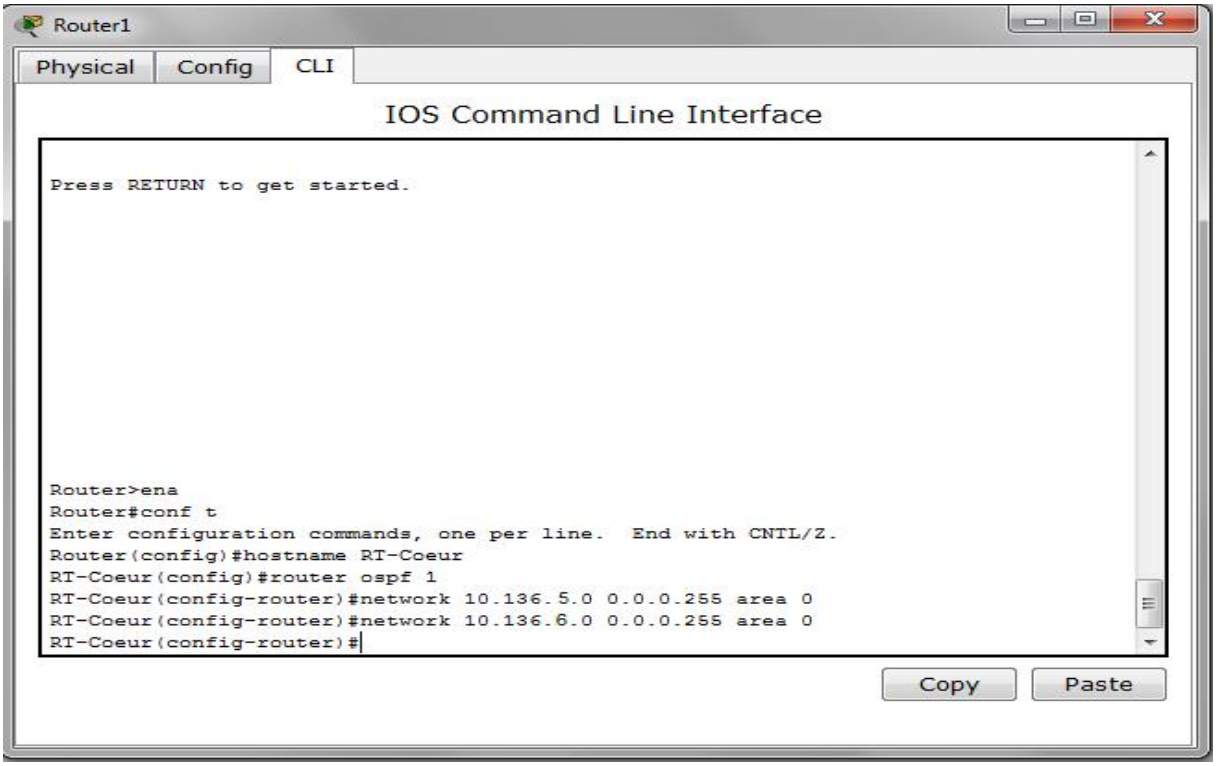

Figure V.16 : Routage au niveau du routeur SP2.

✓ Pour le routeur de la station SBM :

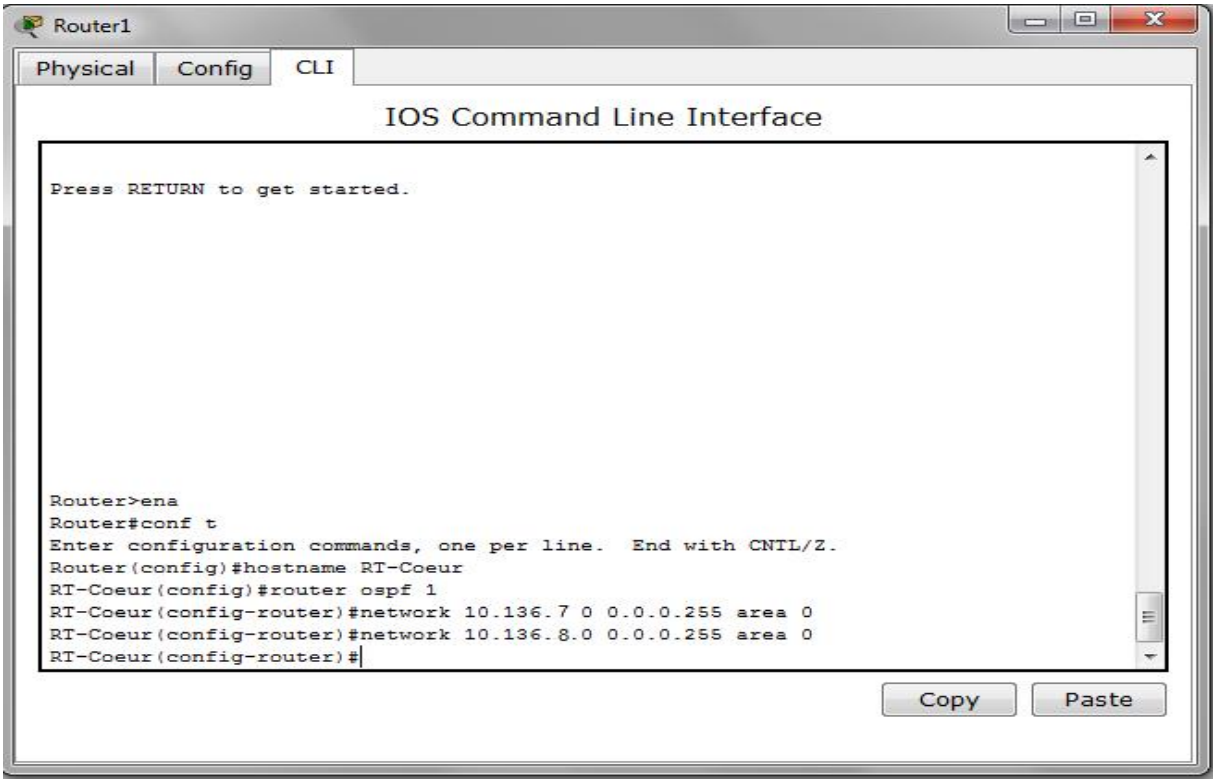

Figure V.17 : Routage au niveau du routeur SBM.

✓ Pour le routeur de la station SC3 :

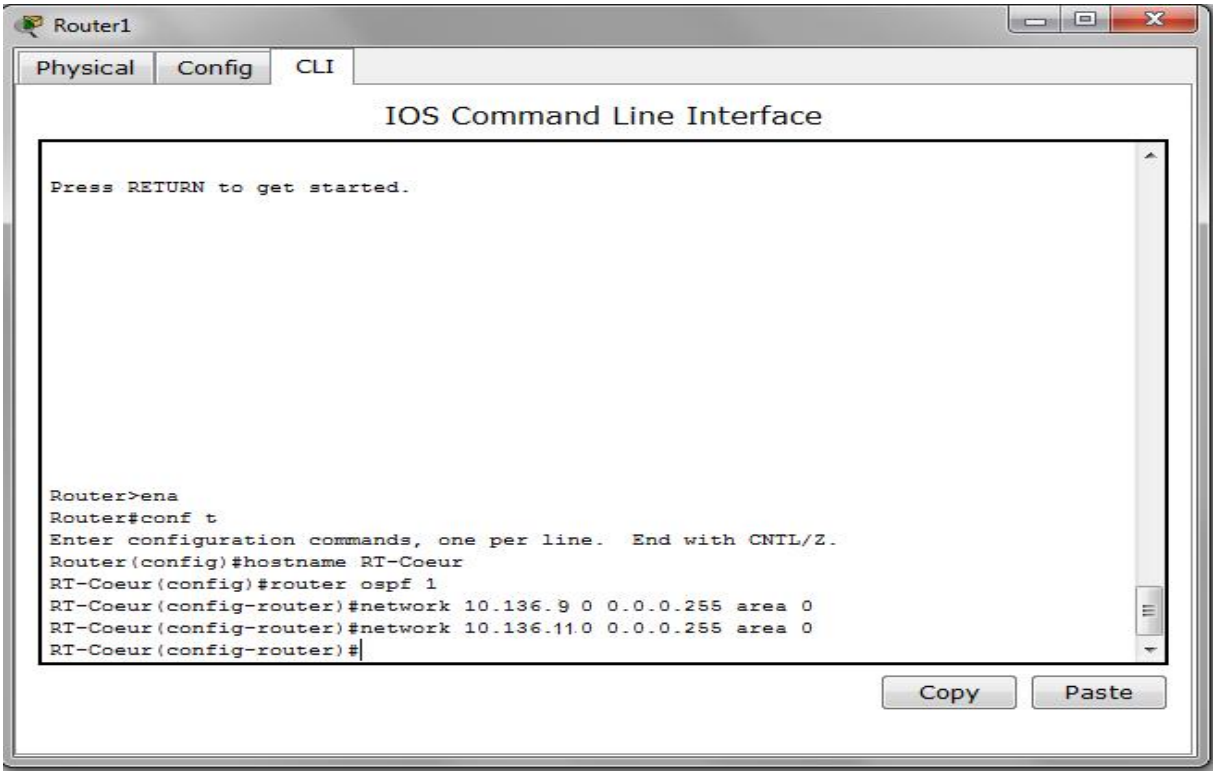

Figure V.18 : Routage au niveau du routeur SC3.

✓ Pour le routeur de la station GG1 :

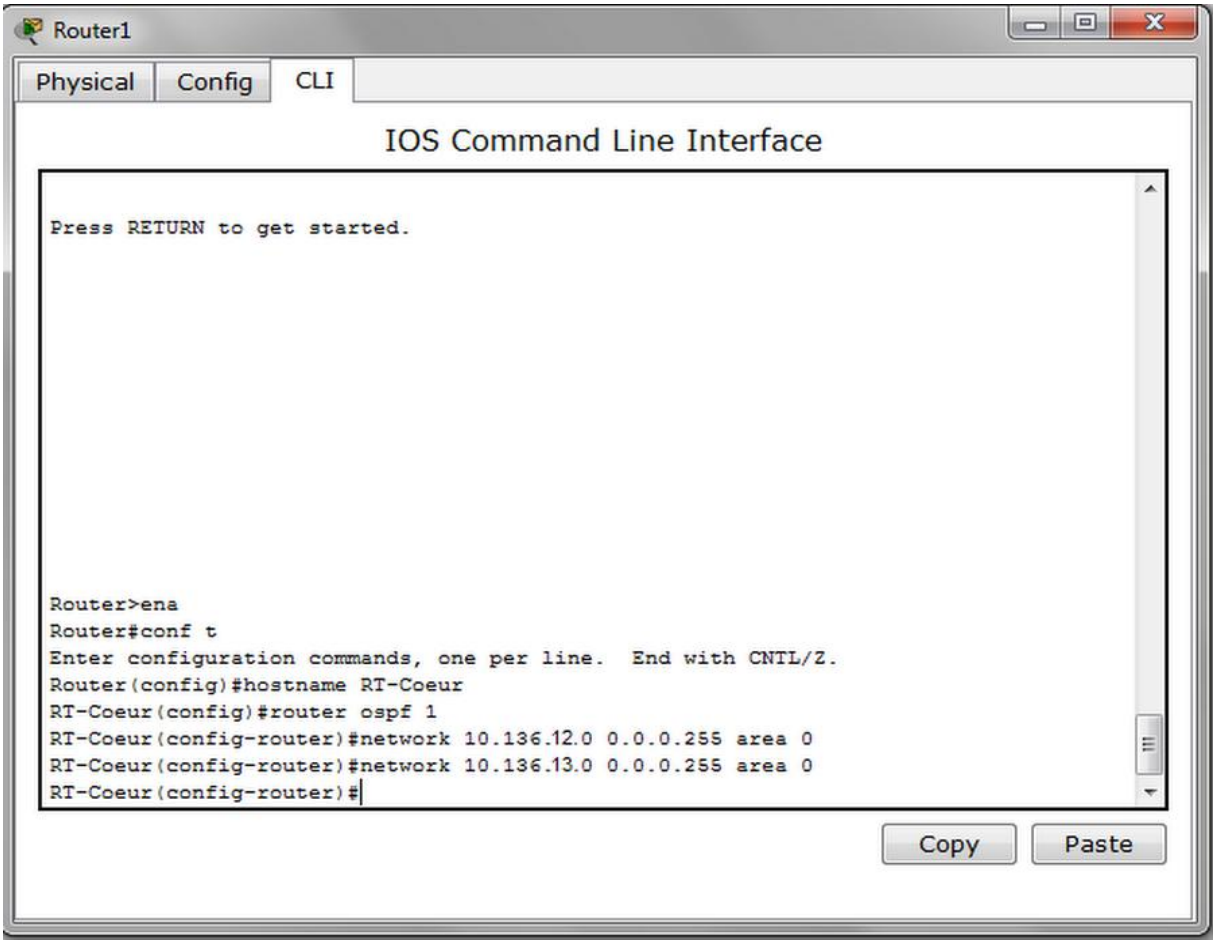

Figure V.19 : Routage au niveau du routeur GG1.

5. Configuration des PCs et des serveurs :

La configuration de l'ensemble des PCs et des serveurs, consiste à donner des adresses IP, des masques et des passerelles. En effet, pour attribuer des adresses IP, il faut que pour chaque PC ou serveur appartenant à un VLAN donné, cette adresse doit appartenir au même sous réseau que le VALN. Prenant l'exemple de configuration pour un PC et un serveur, et ça sera la même chose pour le reste.

✓ Pour les PCs :

La Figure V.20 montre l'attribution d'adresse au PC0 :

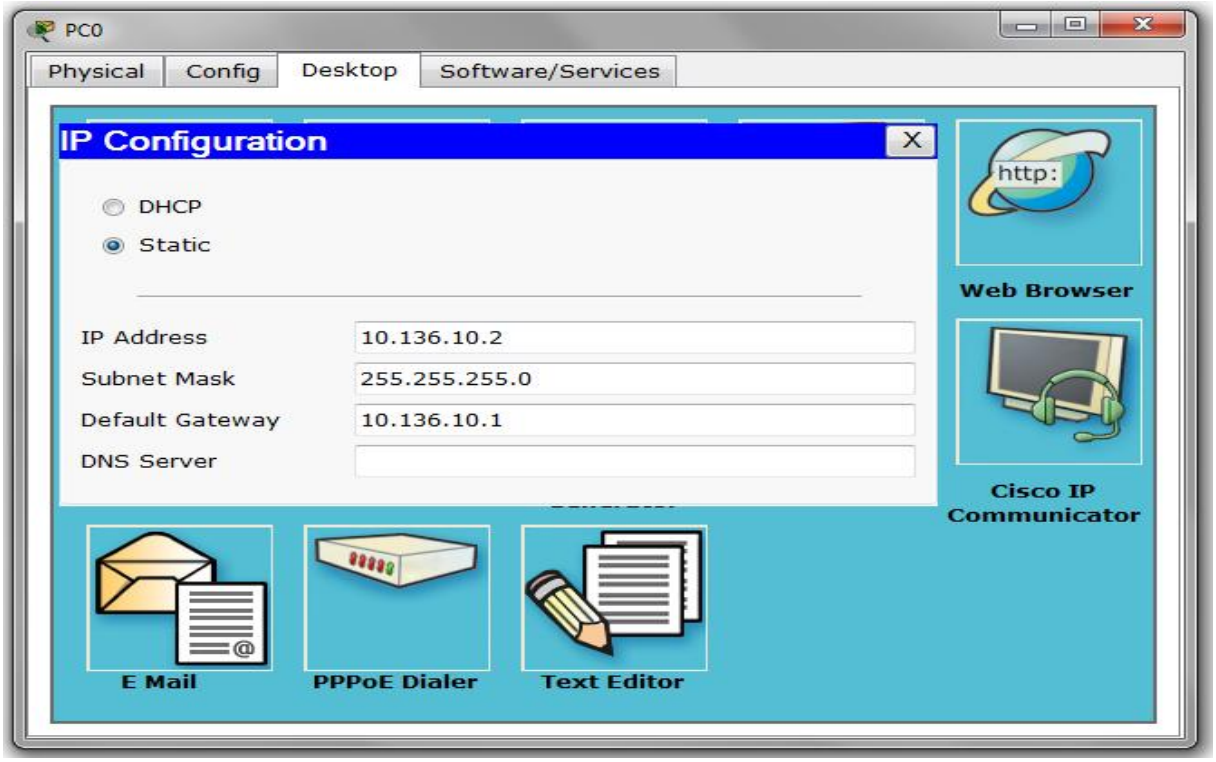

Figure V.20 : Attribution d'adresse IP aux PCs.

✓ Pour les serveurs :

La Figure V.21 montre l'adressage du Server0 :

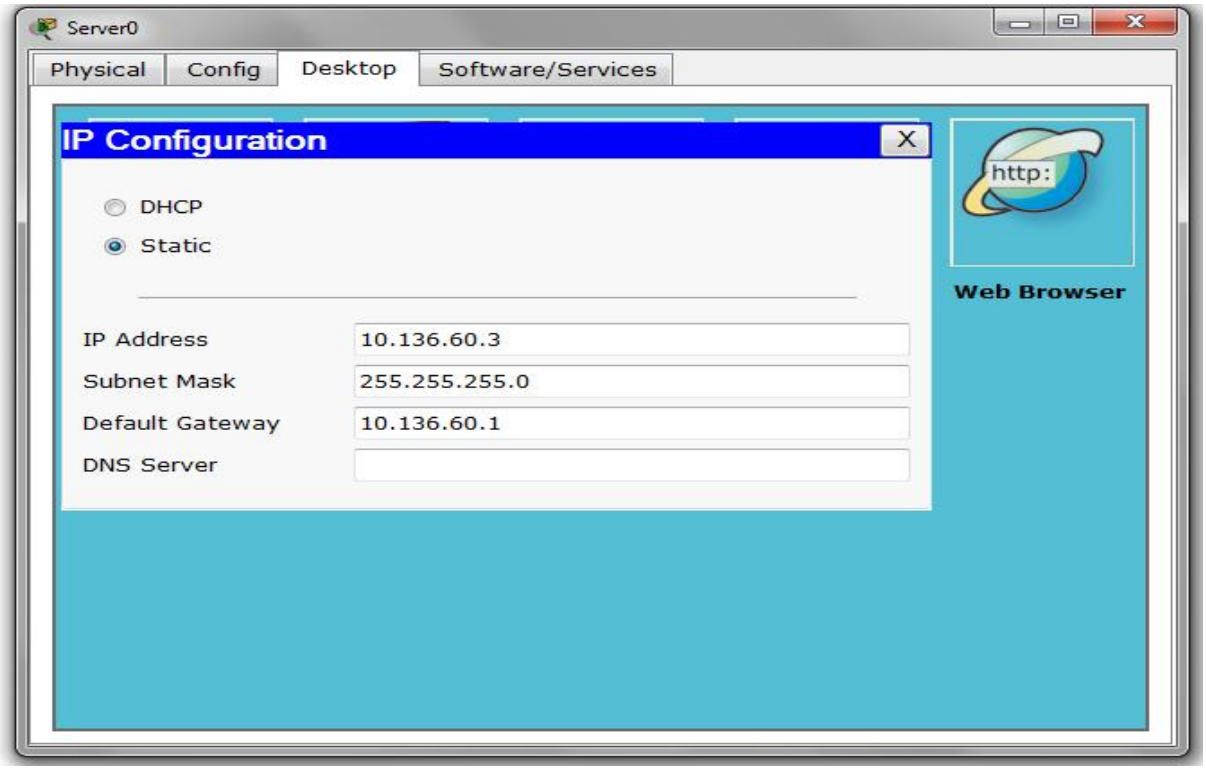

Figure V.21 : Attribution d'adresse aux serveurs.

6. Les tests de validation :

Dans cette partie, l'ensemble des tests de validation consiste à vérifier l'accessibilité de l'ensemble des équipements, en utilisant la commande « Ping » qui teste la réponse d'un équipement sur le réseau. Donc, si un équipement veut communiquer avec à un autre, le Ping, permet d'envoyer des paquets au destinataire. Si l'équipement récepteur reçoit ces paquets, donc, communication réussie. Sinon, cas échoué.

Les tests se font, entre les routeurs et les commutateurs, les équipements d'un même VLAN, les équipements des VLANs différents et les équipements des réseaux locaux distincts.

6.1. Vérifier la communication entre les équipements d'interconnexion :

- ✓ Commutateur Accès et commutateur Distribution :

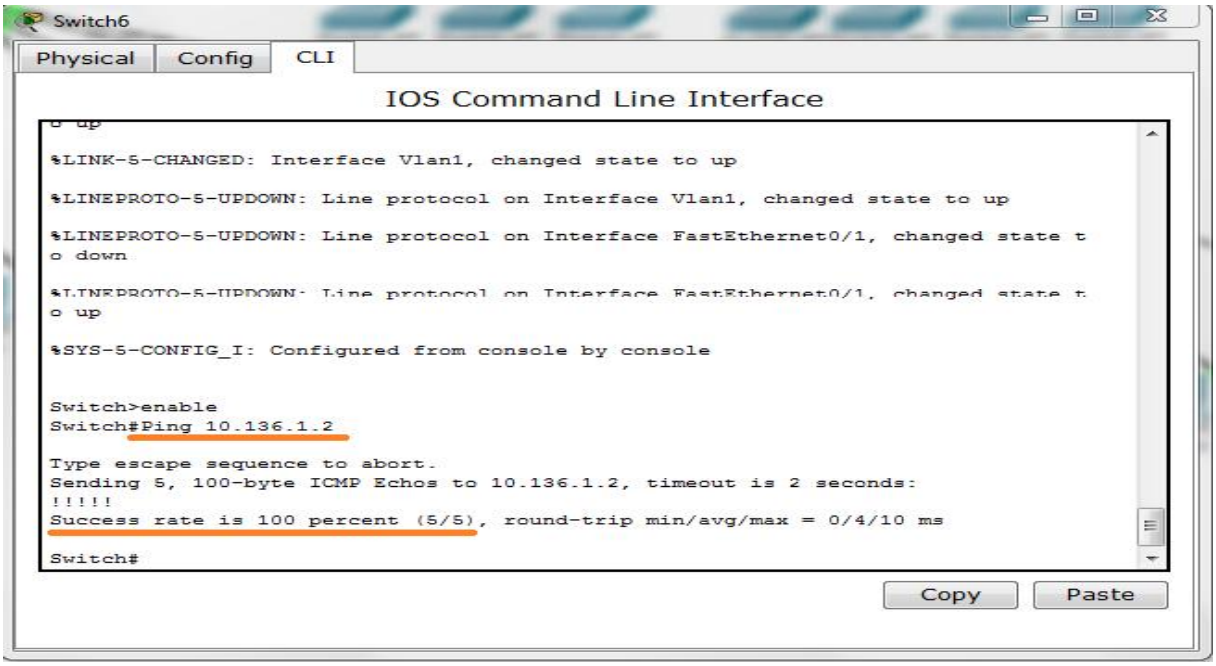

Figure V.22 : Test entre le Switch Accès et le Switch Distribution.

✓ Entre les commutateurs Accès :

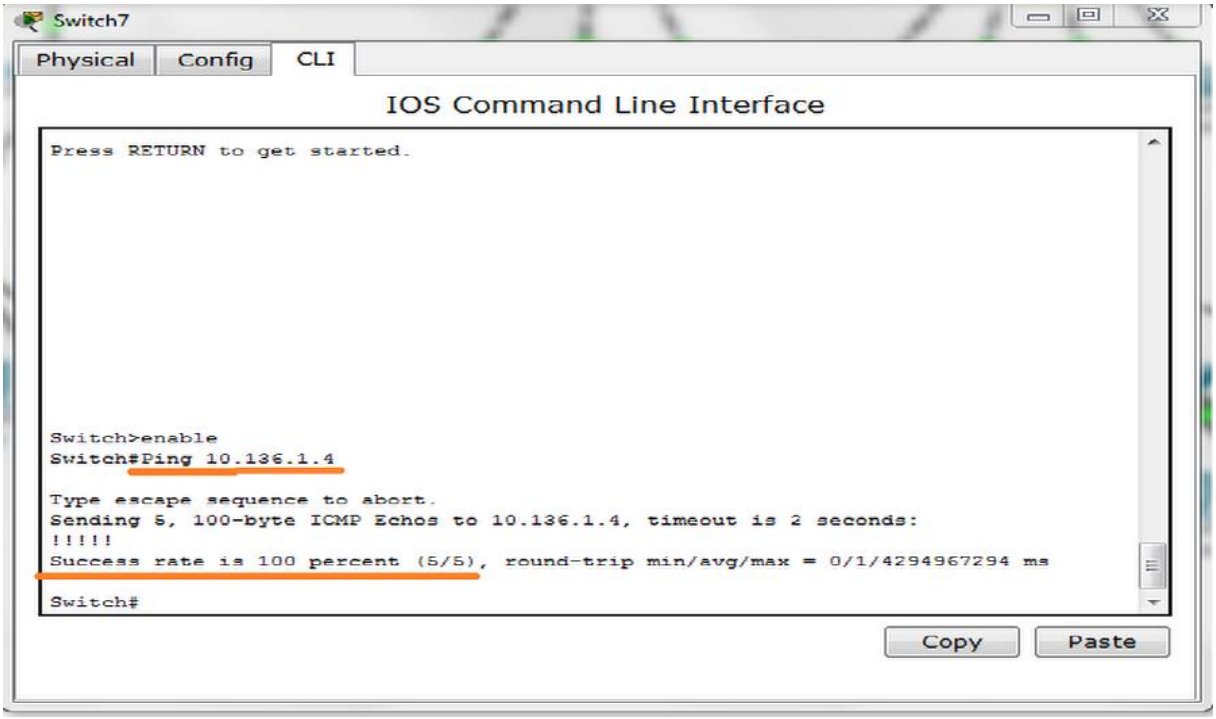

Figure V.23 : Test entre les Switchs Accès.

✓ Entre routeur et commutateur Distribution :

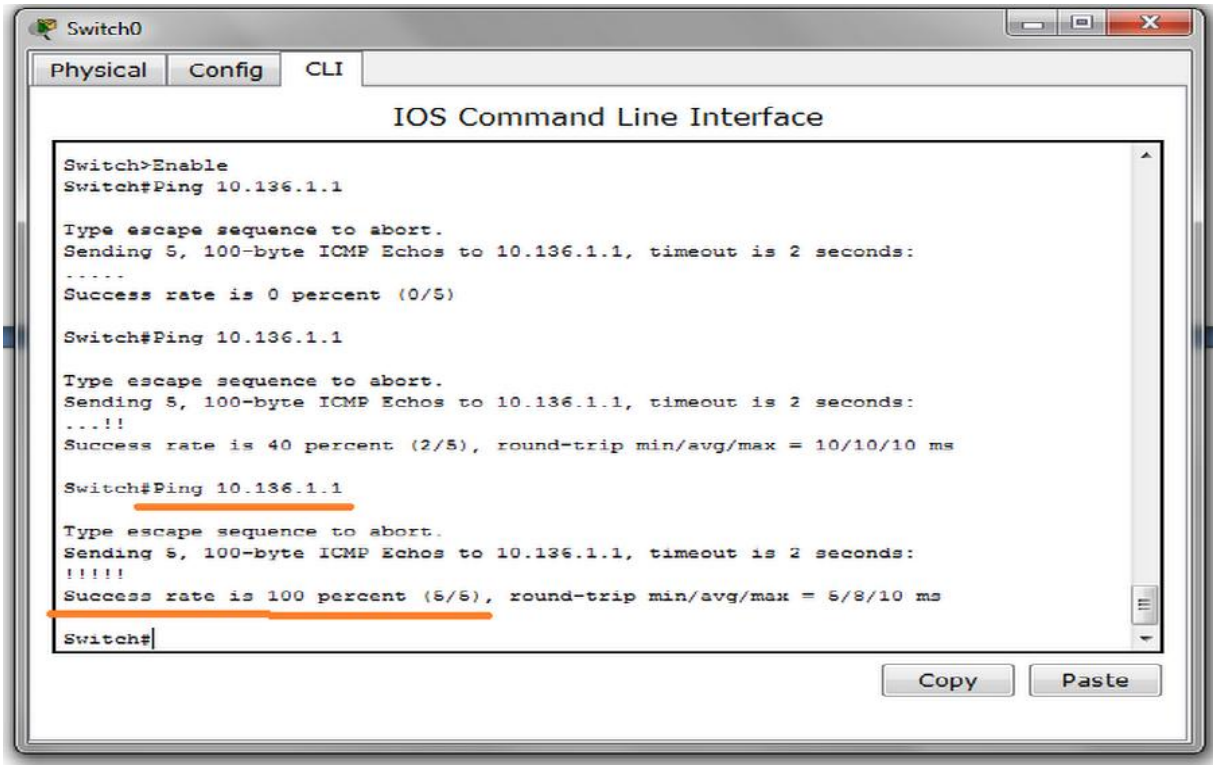

Figure V.24 : Test entre routeur et Switch Distribution.

✓ Test entre commutateur Accès et routeur :

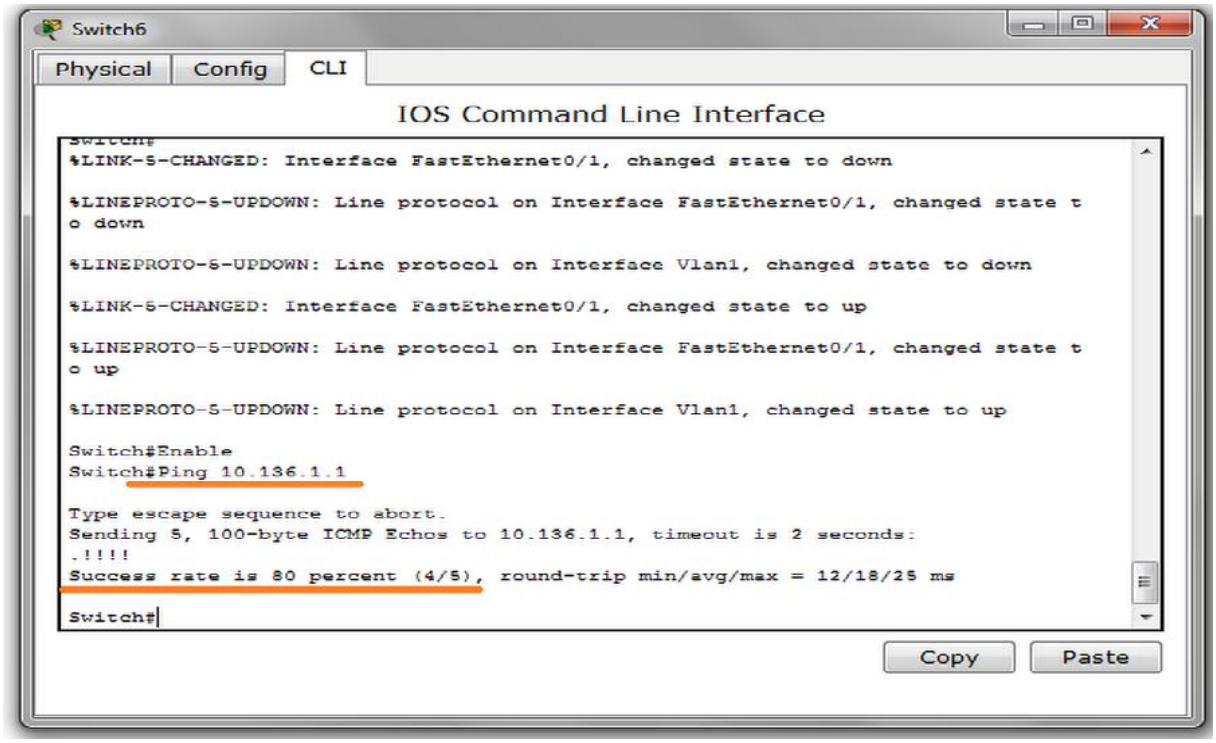

Figure V.25 : Test entre routeur et Switch Accès.

✓ Test entre les routeurs distants :

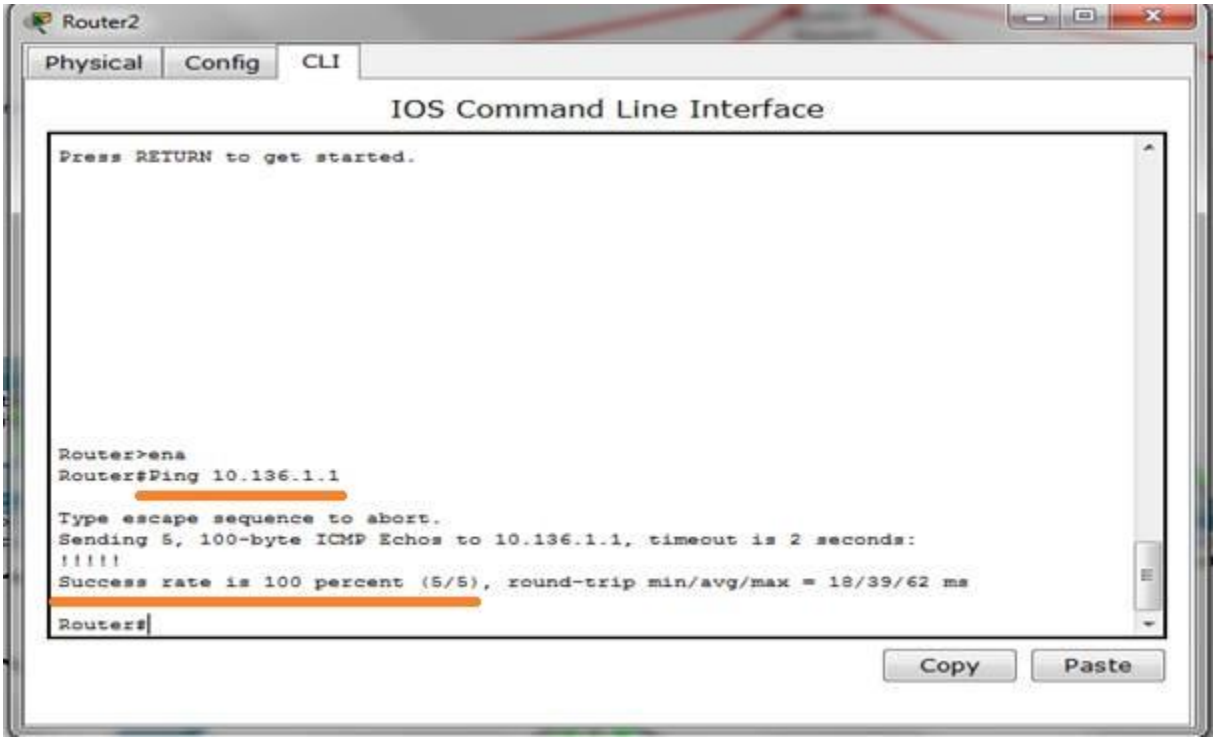

Figure V.26 : Test des routeurs distants.

6.2. Vérifier la communication entre les PCs :

- ✓ Test entre PC d'un même LAN et VLAN :

A ce stade, vérifiant l'accessibilité des équipements du même VLAN situés dans un réseau local commun. Depuis le PC0 (10.136.10.2), essayant d'accéder au PC5 (10.136.10.3), tel que, les deux se trouvent dans un même LAN et VLAN, mais dans des commutateurs Accès différent.

La Figure V.27 montre le succès du test effectué entre PC d'un même LAN et VLAN :

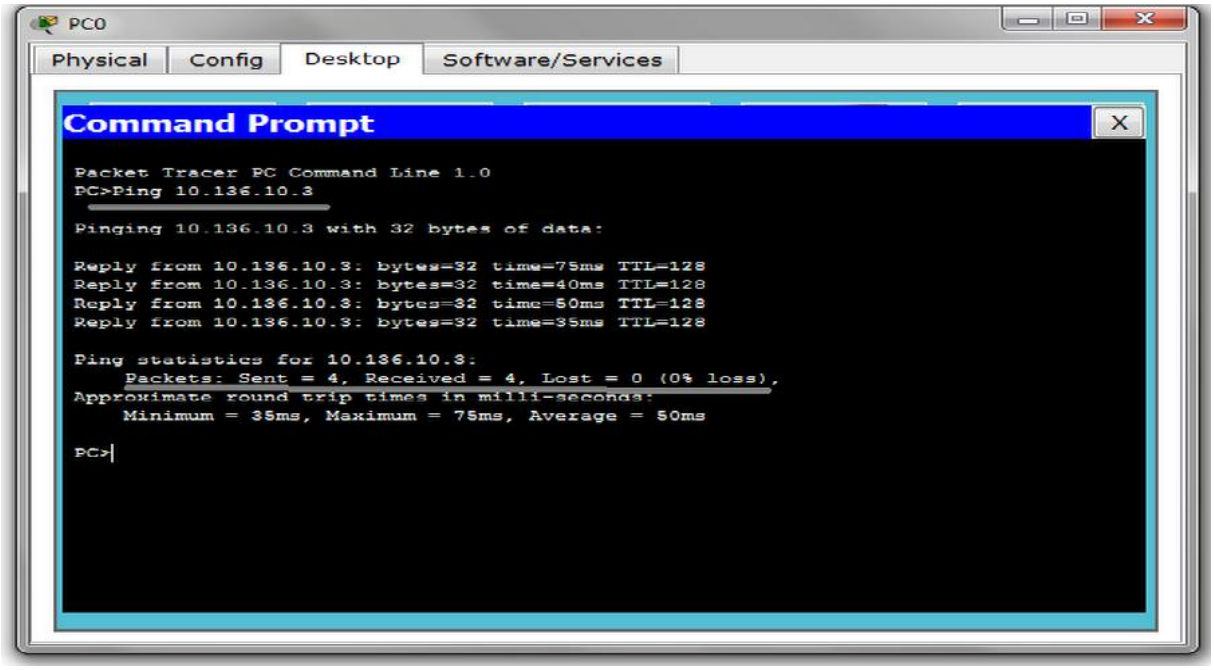

Figure V.27 : Test entre PC d'un même LAN et VLAN.

- ✓ Test entre PC d'un même LAN mais VLANs différents :

Vérifier l'accessibilité des différentes machines, qui se retrouvent dans un réseau local commun, mais dans des VLANs distincts. À partir du PC1 (10.136.20.2), essayant d'accéder au PC0 (10.136.10.2).

La Figure V.28 illustre le succès du test effectué entre PC d'un même LAN mais VLANs distincts :

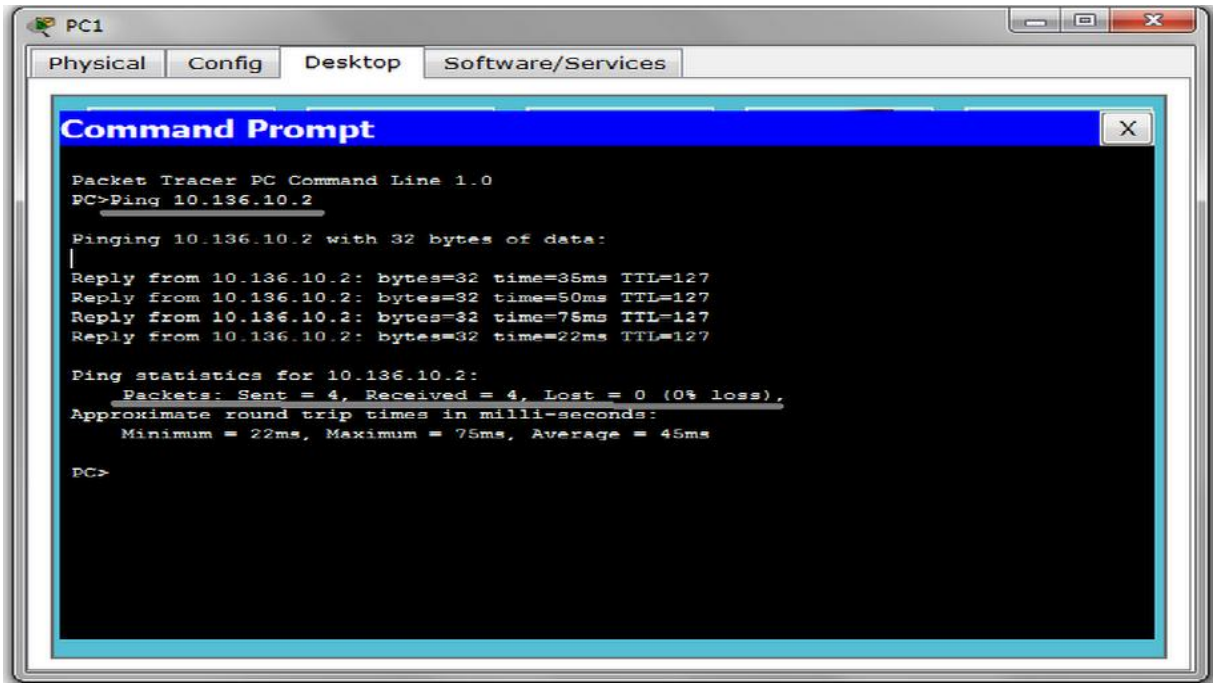

Figure V.28 : Test entre machines des VLANs distincts.

- ✓ Test entre PC de même VLAN mais LAN différent :

Dans ce cas de figure, testant la connectivité des PCs d'un même VLAN, entre les différents réseaux locaux des stations. À partir du PC9 (10.136.50.3) de LAN SP3, essayant d'accéder au PC36 (10.136.50.139) du LAN GG1. La Figure V.29 montre le succès du test effectué entre PC d'un même VLAN mais d'un LAN différent :

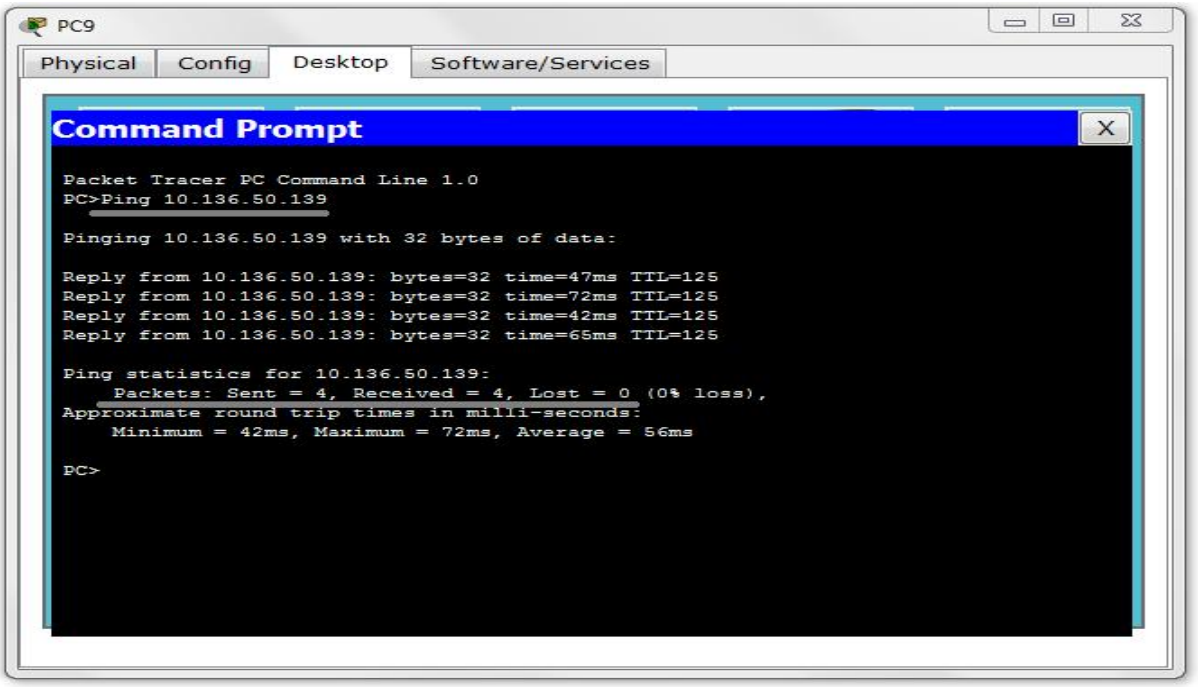

Figure V.29 : Test entre PC de même VLAN mais différent LAN.

- ✓ Test entre PC de différents VLAN et LAN :

Testant la connectivité des PCs de VLAN et LAN distincts. À partir du PC7 (10.136.30.3) de LAN SP3, essayant d'accéder au PC58 (10.136.20.39) du LAN SP1 Bis.

La Figure V.30 montre le succès du test effectué entre PC des différents VLAN et LAN :

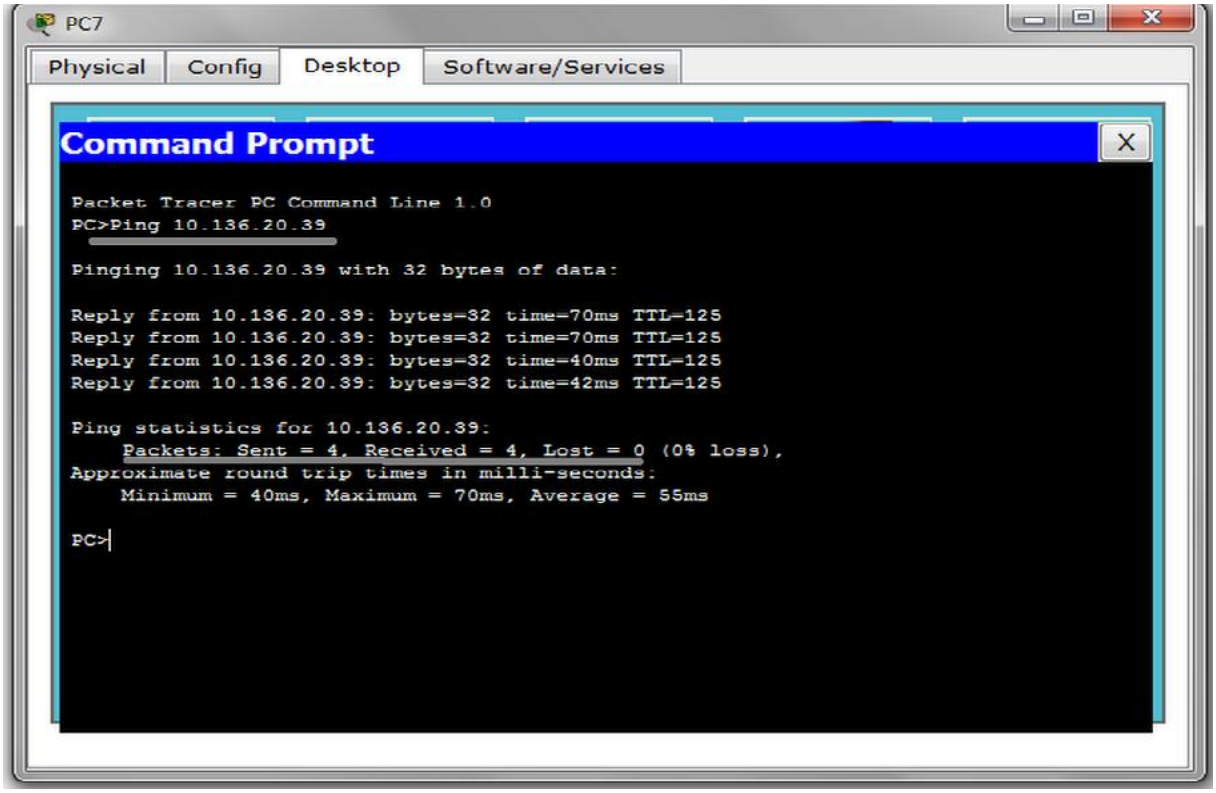

Figure V.30 : Test entre PC de VLAN et LAN différents.

Conclusion :

Ce chapitre est le fruit du travail. En effet, il portait sur l'ensemble des configurations réalisées au niveau du LAN étendu de la RTC Bejaia pour sa mise en marche. En configurant, chaque LAN d'une station et en assemblant tous les LANs distants, pour former un LAN étendu fonctionnel. Bien sur, en effectuant un ensemble de tests de validation entre les LANs distincts, afin de prouver l'efficacité des solutions.

Conclusion Générale et perspectives

Au terme de ce projet, il convient de dire que sa réalisation s'est révélée très enrichissante et bénéfique, en sens de domaine professionnel et formation, qui a permis d'acquérir de nombreuses connaissances en réseau informatique notamment en administration et optimisation des réseaux.

L'organisation des réseaux locaux des stations de la RTC Bejaia, ainsi leur interconnexion, était notre objectif durant tout ce projet. En effet, Nous avons tenté d'apporter une solution pour l'organisation de l'ensemble des réseaux locaux des stations constituants le LAN étendu de la RTC Bejaia. Donc, nous avons choisis une méthode de segmentation pour ces LANs, celle des VLANs, en créant des segments VLAN fonctionnels, c'est-à-dire, que suivant la méthode de regroupement par disposition des fonctions, que nous en organiser les LANs des stations, d'où la création d'un ensemble de réseaux locaux virtuels au sein d'un LAN. En plus, pour permettre la communication entre les différents LANs et la haute disponibilité du réseau, l'interconnexion de ces LANs distants, est primordial, en s'appuyant sur la notion du routage dynamique et implémentant un protocole efficace : OSPF. Permettant, ainsi, une communication d'un côté, entre les stations. D'un autre côté, entre les stations et la direction de Bejaia.

Pour la réalisation du travail, et après avoir bien étudiées et planifiées les solutions. Nous les avons implémentées, en donnant ainsi, une simulation à travers le simulateur Cisco Packet Trace. Pour la vérification de la validité du travail et pour affirmer que les objectifs initiaux, ont été bien visés, en réalisant un ensemble de tests de validation à travers ce LAN étendu.

Le travail permettra non seulement l'interconnexion des sites et la mise en place d'une communication plus efficace et plus sécurisée, mais aussi notre intégration dans le domaine professionnel et de savoir comment faire des analyses des cas.

Dans le futur, pour la continuité de notre travail, la prudence veut que l'on approfondisse l'étude, afin de compléter la solution. Nous aimerions définir des politiques de sécurité plus robuste et plus fiable, à savoir la mise en place des listes d'accès ACLs (Access Control List) ou mieux encore CBAC (Context-Based Access Control) afin de filtrer le trafic réseau passant par les routeurs. Les CBAC de Cisco fournissent un nouveau mécanisme de

filtrage basé sur l'état des connexions. Elles examinent non seulement les informations des couches réseau et transport, mais examinent aussi les informations de la couche application (comme ftp) pour apprendre et inspecter l'état des sessions TCP et UDP.

Donc, avoir un réseau mieux organisé en terme de segmentation, routage et sécurité.

Bibliographie

[1] : FENYÔ Alexandre, LE GUERN Frédéric, TARDIEU Samuel, *Raccorder son réseau d'entreprise a Internet : Notions de base des réseaux TCP/IP,* Eyrolles, Paris, 2006.

[2] : LLORENS Cédric, *Mesure de la sécurité « logique » d'un réseau d'un opérateur de télécommunication*, Thèse Doctorale, Ecole nationale Supérieure des Télécommunication, 2005.

[3] : PUJOLLE Guy, *Les Réseaux: Les réseaux IP*, 6ème Edition, Eyrolles, Saint-Germain, septembre 2007.

Webographie

[A] : BAPTISTE Wicht. *Introduction au réseau*, 03 Mars 2007, consulté le 02 Avril 2012, source < http://baptiste-wicht.developpez.com/tutoriel/reseau/introduction/>

[B] : BERNARD Adrien, et al., *Routage,* 06 Juin 2004, consulté le 08 Avril 20122,

source <http://www.techno-science.net/?onglet=glossaire&definition=3796>

[C] : DULAUNOY Alexandre, *Introduction à TCP/IP et aux routeurs de type IOS (Cisco) : Routage IP*, 19 Mai 2000, consulté le 10 Avril 2012, source

< http://www.foo.be/cours/cisco/cours-cisco.pdf>

[D] : ERON Eric, *Le routage*, Septembre 2004, consulté le 08 Avril 2012, source <http://www.frameip.com/routage/>

[E] : GATOUX Jean-Luc, *Le monde des réseaux : Routage statique ou dynamique*, 2005, consulté le 25 Mai 2012, source <http://www.gatoux.com/SECTION3/p4.php?PHPSESSID=65c5a61fcccf3485fd8ea2f6353c382b>

[F]: TANGUY Alexandre, *TOPOLOGIE RESEAU : Le modèle hiérarchique en 3 couches*, 3 Aout 2011, consulté le 11 Avril 2012, source < http://bibabox.fr/topologie-reseau-le-modele-hierarchique-en-3-couches/>

Annexe A1

A1.1. Principe de fonctionnement des VLANs :

Le principe des VLANs consiste à regrouper des machines dans un ou plusieurs segments quelque soit leur emplacement physique. Il existe 2 méthodes utilisées pour transmettre les informations des utilisateurs de manière logique entre VLANs:

Les deux techniques examinent la trame au moment de sa réception ou de son acheminement par le commutateur.

- ✓ Le filtrage des trames :
  Le filtrage des trames consiste à examiner les informations particulières à chaque trame (adresse MAC ou type de protocole de niveau 3). Une table de filtrage est alors élaborer pour chaque commutateur. Elle est réputée pour le contrôle administratif rigoureux grâce à l'examen des nombreux attributs de chaque trame. Cette méthode n'est pas très évolutive car chaque trame devra être vérifiée à l'aide d'une table de filtrage.

- ✓ L'identification (étiquetage) des trames :
  Conçu spécialement pour les communications inter-commutés à plusieurs VLANs, l'étiquetage consiste à marquer toutes les trames sortantes du commutateur avec le numéro du VLAN d'appartenance. Le commutateur suivant peut alors repérer les trames et les diriger vers le VLAN correspondant. Un identificateur unique est placé dans l'entête de chaque trame pendant qu'elle parcourt le backbone.
  L'identificateur est retiré avant que la trame ne quitte le commutateur pour des liaisons hors backbone (vers la station finale).Cette méthode demande peu de traitement et présente une faible charge administrative. Elle est spécifiée par la norme IEEE 802.1q qui privilégie cette technique en raison de son caractère évolutif

Annexe A2

A2.1. La norme 802.1Q

La norme 802.1q est née en 1998 pour répondre à un besoin de normalisation sur le transport des VLANs. La principale fonction de la norme est de transporter les VLANs sur le réseau, pour permettre à deux machines d'un même Vlan de communiquer à travers un nombre non définit d'équipement réseau.

Selon la norme IEEE 802.1Q, l'étiquetage de trames (méthode de distribution des ID de VLAN aux autres commutateurs) est la meilleure façon de mettre en œuvre des LAN virtuels.

La méthode d'étiquetage des trames VLAN a été développée spécialement pour les communications commutées. Cette méthode place un identificateur unique dans l'en-tête de chaque trame au moment où celle-ci est acheminée dans le backbone du réseau. L'identificateur est interprété et examiné par chaque commutateur avant tout broadcast ou transmission à d'autres commutateurs, routeurs ou équipements de station d'extrémité. Lorsque la trame quitte le backbone du réseau, le commutateur retire l'identificateur avant de transmettre la trame à la station d'extrémité cible.

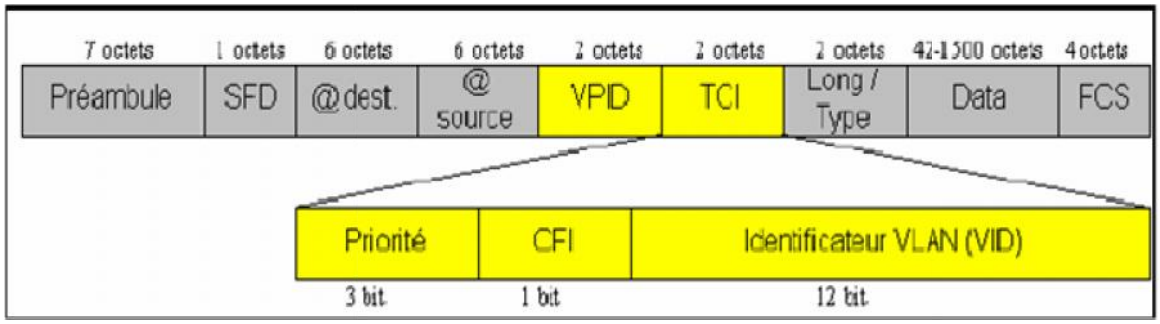

Figure A2.1 : Extension de la trame Ethernet modifiée par la norme 802.1Q.

A2.2 Description de la norme

Elle définit, en premier lieu, l'ajout de 2 octets dans la trame Ethernet. Ces deux octets ajoutent plusieurs champs pour répondre à plusieurs besoins. La norme définit alors sur la trame Ethernet le champ VPID à 0x8100 pour désigner la trame 802.1q.

- **Canonical Format Identifier (CFI) :** Un champ protocole définit sur 1 bit est prévu pour pouvoir utiliser le 802.1q aussi bien sur Ethernet que sur TokenRing.

- **Priorité:** 3 bits utilisés pour coder 8 niveaux de priorité (de 0 à 7). On se sert de ces 8 niveaux pour fixer la priorité des trames d'un VLAN par rapport à d'autres (exemple d'utilisation: nous favorisons un VLAN sur lequel on utilise la visioconférence (nécessitant beaucoup de bande passante) par rapport à un VLAN où l'on ne fait qu'envoyer et recevoir des mails**)**
- **VLAN ID (VID):** Le champ VID permet de fixer un identifiant sur 12 bits, c’est le champ d'identification du VLAN auquel appartient la trame.

Annexe A3

A3.1. Le protocole VTP (Virtual Trunking Protocol):

Le protocole VTP (VLAN Trunking Protocol) a été créé par Cisco pour résoudre des problèmes opérationnels dans des réseaux commutés contenant des VLAN. Cest un protocole propriétaire Cisco. Son rôle est de maintenir la cohérence de la configuration VLAN sur un domaine d'administration réseau commun. VTP est un protocole de messagerie qui utilise les trames d'agrégation de couche 2 pour gérer l'ajout, la suppression et l'attribution de nouveaux noms aux VLAN sur un domaine unique. De plus, VTP autorise les changements centralisés qui sont communiqués à tous les autres commutateurs du réseau.

A3.2. Les modes VTP :

Le protocole VTP dispose de trois modes de configuration sur des commutateurs :

- ✓ Mode *serveur* : il est possible de créer, modifier ou supprimer des VLANs et des les transmettre au domaine.

- ✓ Mode *client* : le Switch reçoit les mises à jour, les prend en compte et les transmet à ses voisins. Il ne peut pas faire de modification.

- ✓ Mode *transparent* : le Switch reçoit les mises à jour et les transmet à ses voisins sans les prendre en compte. Il peut créer, modifier ou supprimer ses propres VLANs mais ne les transmet pas.

A3.3. Configuration des modes VTP :

La configuration des commutateurs en différents modes VTP, est comme suit :

- ✓ Configuration en mode serveur :
  SW(config)#vtp domain nom-domaine
  SW(config)#vtp mode server

- ✓ Configuration en mode client :
  SW1(config)#vtp domain nom-domaine
  SW1(config)#vtp mode client

- ✓ Configuration en mode transparent:
  SW2(config)#vtp domain nom-domaine
  SW2(config)#vtp mode transpaent

Résumé

L'organisation des réseaux locaux, est un point important, qui nécessite une bonne étude concernant leur segmentation, afin de doter de LAN efficace en terme de performances et temps de réponse.

Communiquer entre les différents réseaux locaux constituants le réseau d'un organisme, est primordial, pour permettre un accomplissement des fonctions de cet organisme, ainsi que de profiter des services offerts par les réseaux informatiques entre les différents LANs.

L'objectif de ce projet, est de proposer un modèle pour l'organisation des réseaux locaux des stations constituants le LAN étendu de la RTC Bejaia (Région Transport Centre), en proposant un plan d'adressage pour chaque LAN d'une station, ainsi qu'une solution de routage pour permettre la communication entre les stations.

En pratique, les LANs sont segmentés par les VLANs, en adoptant la stratégie de VLAN fonctionnel pour regrouper les utilisateurs, et VLAN sécuritaire pour regrouper les serveurs existants dans cette société. En plus, une implémentation d'un routage dynamique suivant le protocole OSPF, pour l'ensemble des routeurs pour l'interconnexion des stations de la RTC Bejaia.

Mots clés : réseaux locaux, segmentation, adressage, routage, VLAN, OSPF.

Abstract

The organization of local networks, is an important point, which requires a good study on segmentation, in order to provide LAN-effective performance and response time. Communicate between different LANs.

the network components of an organism is essential to allow a discharge of the duties of this organization and take advantage of services offered by computer networks between different LANs.

The objective of this project is to propose a model for the organization of local networks of the extended LAN stations constituents of the RTC Bejaia (Region Travel Center), by proposing a plan for addressing each LAN station, and a routing solution for communication between stations.

In practice, the LANs are segmented by VLANs, adopting the strategy of functional VLANs group users, and secure VLAN to group existing server in this society. In addition, an implementation of a dynamic routing protocol OSPF according to the set of routers to interconnect the RTC stations Bejaia.

Key words: Local area networks, segmentation, addressing, routing, VLAN, OSPF.