REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A. MIRA – BEJAIA

Faculté de Technologie

Département de Génie Electrique

Filière : Electronique

Spécialité : Télécommunications

Projet de fin d'étude

En vue de l'obtention du diplôme de

MASTER

En Télécommunications

Thème

« Etude, Conception et Evaluation d'une Architecture MPLS/VPN Désignée pour une Infrastructure Operateur »

Présenté par :

M. MEGRI Hmanou
M. SALHI Noureddine

Encadré par :

Dr. ROUHA.M
Ing. AMRANI.Z

Membres du jury :

Prof. KHIREDDINE. A.K	Président
Prof. BERRAH.S	Examinateur

Année universitaire : 2014/2015

DÉDICACES

Je dédie ce modeste travail à mes très chers parents, pour leur soutien

et tous les efforts qu'on ma donnée le long de mon parcours et je

leurs souhaite bonne santé et longue vie.

Je dédie ce travail aussi à mes très chers frère et sœurs.

A tous les membres de ma famille.

A tous mes amis.

A tous mes amis de ma promotion Télécom.

A tous ceux et celles qui m'ont aidé de prés ou de loin.

Hmanou.M

DÉDICACES

Je dédie ce modeste travail

A ma grande et aimable famille

A mes chers et fidèles amis

A mes collègues télécom de la promotion 2014/2015

Nourdine

Remerciements

Au nom d'ALLAH le tout puissant et miséricordieux que

nous louons pour avoir guidé nos pas dans l'accomplissement de

*ce modeste travail. Merci à **ALLAH**.*

Nous remercions, nos deux promoteurs,

M. Mustapha ROUHA enseignant à l'université de Bejaia, M. Zoheir AMRANI Comme ingénieur à compagnie OTA,

pour leurs aide très appréciable caractérisée par

leurs disponibilité, leurs rigoureux encadrement et sans oublier leurs

précieux conseils.

Nos remerciements, également, sont destinés à

Mr. Zine Eddine Mohamed BELLAOUAR Chef d'équipe

et M. M'Hamed KHEDIM senior Manager à la compagnie OTA,

pour leur accueil et générosité durant la durée de stage pratique.

Nos remerciements les plus vifs s'adressent aussi aux membres de jury,

messieurs le président le professeur KHIREDDINE A.K et le professeur BERRAH.S de l'université de Bejaia d'avoir accepté

d'examiner et d'évaluer notre travail.

Nous exprimons également notre gratitude à tous les

professeurs et enseignants qui ont collaboré à notre formation

depuis notre premier cycle d'étude jusqu'à la fin de notre cycle

universitaire.

En fin, nous tenons à adresser nos sincères remercîments à nos

familles (parents, frères et sœurs) qui nous ont soutenu et

surtout supporté tout au long de nos études particulièrement

cette année.

Hmanou & Nourdine

Résumé

Résumé

La technologie IP (*Internet Protocol*) autrefois utilisée uniquement dans le cadre d'Internet est de nos jours le support de nombreuses autres applications dé-corrélées telle que la téléphonie ou encore la télévision. Cette multi utilisation du standard a entraîné une volonté de mutualisation au sein du cœur de réseau. Aujourd'hui, les fonctionnalités apportées par MPLS (*Multi Protocol Label Switching*) permettent une vitalisation des infrastructures de réseau IP sur un unique cœur, entraînant une complexité de la gestion de la ressource.

Dans ce travail, nous étudierons les possibilités actuelles de gestion de ce réseau mutualisé et nous proposerons l'adjonction d'un mécanisme de gestion IP/MPLS. Nous démontrerons les nombreuses possibilités offertes par ce nouveau système pour ainsi optimiser l'utilisation du réseau.

Notre approche dans ce mémoire, s'est de concevoir et de construire un cœur de réseau de type opérateur pour simuler un scénario réel qui véhicule les différents types de trafics (voix, données et vidéo).

Les résultats du mémoire sont présentés suivant le temps de simulation et la charge du réseau. Les résultats démontrent l'avantage de la performance des réseaux MPLS, par rapport aux réseaux IP traditionnelles.

Mots clés : *IP (Internet Protocol), MPLS (Multi Protocol Label Switching), Réseau, GNS3(Graphical Network Simulator).*

Abstract

IP technology once used only in the context of the Internet is today the support of many other de-correlated applications such as telephony or television. This multi-use standard resulted in a commitment to sharing within the network of heart. Today, the functionality provided by MPLS allow virtually IP network infrastructure on a single heart, causing complexity of the management of the resource.

In this work, we study the current possibilities of shared management of this network and we will propose the addition of an IP / MPLS management mechanism. We will demonstrate the many possibilities offered by this new system to optimize network utilization.

Our approach in this paper is to design and build a carrier-class network heart to simulate a real scenario that conveys the different types of traffic (voice, data and video).

The results are presented in memory of simulation time and network load. The results demonstrate the advantage of the performance of MPLS networks over traditional IP networks.

Keywords: *IP (Internet Protocol), MPLS (Multi Protocol Label Switching), Network, GNS3(Graphical Network Simulator).*

Liste des matières

TABLE DES MATIERES

CHAPITRE 2 : MULTI PROTOCOL LABEL SWITCHING (MPLS)

CHAPITRE 3 : CONCEPTION DU RESEAU MPLS REALISE

Liste des figures

Liste des figures

Liste des tableaux

Liste des tableaux

Liste des abréviations

Liste des abréviations

A

AD	**A**dministrative **D**istance
	Distance **A**dministrative
ARP	**A**ddress **R**esolution **P**rotocol
	Protocole de **R**ésolution d'**A**dresse
AS	**A**utonomous **S**ystem
	Système **A**utonome
ASN	**A**utonomous **S**ystem **N**umber
ATM	**A**synchrones **T**ransfert **M**ode
	Mode de **T**ransfert **A**synchrone
AToM	**A**ny **T**ransport **o**ver **MPLS**

B

BGP	**B**order **G**ateway **P**rotocol
BSS	**B**ase **S**ub **S**ystem

C

CIDR	**C**lassless **I**nter-**D**omain **R**outing
CR-LDP	**C**onstraint-based **R**outing **LDP**
CSMA/CD	**C**arrier **S**ense, **M**ultiple **A**ccess with **C**ollision **D**etection
CSPF	**C**onstrained **S**hortest **P**ath **F**irst

D

DCN	**D**ata **C**enter **N**etwork
DEC	**D**igital **E**quipment **C**orporation
DNS	**D**omain **N**ame **S**ystem
	Système de **N**oms de **D**omaine
DiffServ	**Diff**erentiated **Serv**ices

E

EXP	**Exp**érimental
EIGRP	**E**nhanced **I**nterior **G**ateway **R**outing **P**rotocol

F

FAI	**F**ournisseur d'**A**ccès **I**nternet
FEC	**F**orwarding **E**quivalent **C**lasses
	Classe d'**E**quivalence
FIB	**F**orwarding **I**nformation **B**ase
FTTH	**F**iber **T**o **T**he **H**ome
	Fibre **O**ptique **J**usqu'au **D**omicile

G

GLBP Gateway Load Balancing Protocol

GNS3 Graphical Network Simulator
Simulateur Graphique de Réseau

H

HSRP Hot Standby Routing Protocol

I

IANA Internet Assigned Numbers Authority

iBGP internal BGP

ICMP Internet Control Message Protocol

IEEE Institute of Electrical and Electronics Engineers

IGMP Internet Group Management Protocol

IGP Interior Gateway Protocol

IntServ Integrated Services

IOS Internetwork Operating System
Système d'Exploitation pour la Connexion des Réseaux

IP Internet Protocol

IPTV Internet Protocol TeleVision

IPv4 Internet Protocol Version 4

IPv6 Internet Protocol Version 6

IPX Internetwork Packet eXchange

ISIS Intermediate System to Intermediate System

L

LAN Local Area Network
RéseauLocal

LDP Label Distribution Protocol
Protocol de Distribution de Label

LER Label Edge Router

LFIB Label Forwarding Information Base

LIB Label Information Base

LLC Logical Link Control
Contrôle de la Liaison Logique

LSP Label Switched Path

LSR Label Switch Router

M

MAC Media Access Control
Contrôle d'Accès au Support

MAN Metropolitan Area Network

MD5 Message Digest 5

MP-BGP Multi Protocol Border Gateway Protocol

MPLS Multi Protocole Label Swiching
Multi Protocole à Commutation de Label

N

NAT	**N**etwork **A**ddress **T**ranslation
	Traduction d'**A**dresse **R**éseau
NetBT	**Net B**IOS over **TCP/IP**
NOC	**N**etwork **O**peration **C**enter
NSS	**N**etwork **S**ub **S**ystem

O

OSI	**O**pen **S**ystem **I**nterconnection
OSPF	**O**pen **S**hortest **P**ath **F**irst
OSS	**O**perating **S**ub **S**ystem
OTA	**O**rascom **T**elecom **A**lgérie

P

PIM	**P**rotocol **I**ndependent **M**ulticast

Q

QoS	**Q**uality **o**f **S**ervice
	Qualité **D**e **S**ervice

R

RFC	**R**equests **F**or **C**omments
	Demande **D**e **C**ommentaires
RIP	**R**outing **I**nformation **P**rotocol
	Protocole d'**I**nformation de **R**outage
RIPv1	**R**outing **I**nformation **P**rotocol **V**ersion 1
RIPv2	**R**outing **I**nformation **P**rotocol **V**ersion 2
RSVP	**R**e**S**er **V**ation **P**rotocol
RSVP-TE	**R**e**S**er**V**ation **P**rotocol-**T**raffic **E**ngineering
RTT	**R**ound-**T**rip **T**ime

S

SDH	**S**ynchronous **D**igital **H**ierarchy
	Hiérarchie **N**umérique **S**ynchrone
SLV	**S**ervice **L**evel **A**greement
SPF	**S**hortest **P**ath **F**irst

T

TCP/IP	**T**ransmission **I**nternet **P**rotocol/**I**nternet **P**rotocol
TCP	**T**ransmission **C**ontrol **P**rotocol
	Protocole de **C**ontrôle de **T**ransmissions
TDP	**T**ag **D**istribution **P**rotocol
TFTP	**T**rivial **F**ile **T**ransfer **P**rotocol
	Protocole **S**implifié de **T**ransfert de **F**ichiers

TTL	**T**ime **T**o **L**ive **D**urée de **V**ie

U

UDP	**U**ser **D**atagram **P**rotocol **P**rotocole de **D**atagramme **U**tilisateur

V

VCI	**V**irtual **C**hannel **I**dentifier
VLSM	**V**ariable **L**ength **S**ubnet **M**ask **M**asque de **S**ous-réseau à **L**ongueur **V**ariable
VOD	**V**ideo **O**n **D**emand **V**idéo à la **D**emande
VPI	**V**irtual **P**ath **I**dentifier
VPN	**V**irtual **P**rivate **N**etwork
VRF	**V**irtual **R**outing and **F**orwarding
VRRP	**V**irtual **R**outer **R**edundancy **P**rotocol **P**rotocole de **R**edondance de **R**outeur **V**irtuel

W

WAN	**W**ide **A**rea **N**etwork **R**éseau **E**tendu
WDM	**W**avelength **D**ivision **M**ultiplexing **M**ultiplexage en **L**ongueur d'**O**nde

Introduction Générale

Introduction générale

Avec l'accélération de l'utilisation d'Internet, on assiste à une convergence des secteurs de la téléphonie fixe, mobile, des données et du monde audiovisuel. Les réseaux supportant ces services sont historiquement séparés et leurs interactions sont possibles par l'intermédiaire des réseaux centraux. Cependant, une mutualisation de l'infrastructure physique est actuellement mise en œuvre tout en conservant une séparation protocolaire. Ce nouveau modèle entraîne une complexité de la gestion des cœurs de réseaux. En effet, ceux-ci sont soumis à des contraintes de disponibilité, de qualité ou de flexibilité.

La problématique réside alors dans l'optimisation des architectures. Ce problème peut ainsi être traité à la fois par une gestion des topologies adossée à une gestion protocolaire spécifique aux divers besoins. Les travaux de recherche se focalisent sur l'étude de la topologie tendent à améliorer la disponibilité, à contrarier les études protocolaires sont axées sur la qualité de service. Cependant, ces approches ne prennent pas vraiment en considération la flexibilité, eu égard à la diversité des flux transportés (Audio/visuel, Internet, Téléphonie, Données privées).

Le déploiement des réseaux à haut débit et le développement des technologies MPLS permettent la conception de réseaux multiservices capables de transporter aussi bien les flux de données que les flux temps réel (voix, vidéo). Ces nouveaux réseaux seront capables de satisfaire les exigences différentes des différents flux qu'ils transportent.

L'IETF (*Internet Engineering Task Force*) a ainsi défini le nouveau protocole MPLS avec deux objectifs principaux :

• Permettre un acheminement rapide des paquets IP en remplaçant la fonction de routage par une fonction de commutation beaucoup plus rapide. Ceci est possible grâce à la substitution des tables de routage classiques par des matrices de commutation beaucoup plus petites,

• Faciliter l'ingénierie réseau en fournissant aux opérateurs la maîtrise de l'acheminement des données, qui était très complexe avec les protocoles de routage classiques comme OSPF (*Open Shortest Path First*).

Le protocole MPLS, basé sur le changement de label, dérive directement de l'expérience acquise avec les réseaux ATM (*Asynchronous Transfer Mode*) (canaux virtuels, chemins virtuels). Les grandes innovations de MPLS par rapport au routage IP traditionnel sont la manipulation de tables de routage de bien plus petites tailles, des temps de commutation extrêmement rapides, des chemins (LSP (*Label Switched Path*)) par classe de service, l'ingénierie du trafic, une meilleure maîtrise de la qualité de service, des mécanismes de reroutage en cas de panne. MPLS, associé à des routeurs implémentant les mécanismes de différenciation de service (DiffServ (*Differentiated services*)) permet de traiter les flux séparément selon leurs caractéristiques (type de service, type d'application) par un routage plus précis et par le traitement différencié des paquets.

C'est cette double fonctionnalité qui permet une meilleure utilisation des ressources de bout en bout afin d'assurer la qualité de service requise par les applications.

Dans le cadre de ce mémoire de recherche, nous présentons l'architecture des réseaux IP et MPLS, en suite on parlera d'une mise en œuvre d'un réseau MPLS implémenté au sein d'un opérateur.

Le premier chapitre présente des généralités sur les réseaux IP. On définit leurs caractéristiques (couches, protocoles utilisés, routage et commutation).

Le deuxième chapitre est consacré pour la technologie MPLS. On décrit son architecture, ses mécanismes de fonctionnement et ses différentes applications.

Le troisième chapitre définit la conception de réseau MPLS implémenté. On détaille le plan d'adressage, le matériel et les protocoles utilisés.

Le quatrième chapitre décrit l'implémentation du réseau au sein de l'opérateur. On explique les différentes opérations faites ainsi des tests d'exécutions validant le projet réalisé.

Chapitre I

Généralités sur les réseaux

1.1 Introduction

L'évolution des besoins et des applications informatiques a conduit à l'acheminement, dans un même réseau des données informations traditionnelles, de la voix, de la vidéo, et autres flux sur IP. Les réseaux ont pour fonction de transporter des données d'une machine terminale vers une autre machine terminale. Les services qu'ils offrent font partie aujourd'hui de la vie courante des entreprises et administrations (banques, gestion, commerce, bases de données, recherche, etc.), et même chez de simples particuliers.

Dans ce chapitre, nous aborderons les fondements des réseaux informatiques, examinant ces propriétés en décrivant le fonctionnement des réseaux IP et l'évolution des technologies, ainsi que les principaux protocoles nécessaires à mettre en œuvre pour obtenir un réseau performant.

1.2 Qu'est-ce qu'un réseau?

Un réseau est un ensemble de matériels, de logiciels et d'équipements reliés entre eux, permettant le partage des données, des ressources et d'une connexion internet. Mais avec la convergence vers IP, plusieurs autres flux sont partagés sur le réseau informatique (Téléphonie sur IP, Vidéo sur IP, …etc.). Dès son origine, le réseau a été constitué par des liaisons formées en paires métalliques. Puis sont apparues dans le réseau d'accès, les liaisons en fibre optique et les liaisons radioélectriques. [1]

1.3 Classification des réseaux

Il existe plusieurs critères pour classifier les réseaux informatiques. Une classification (traditionnelle) est basée sur la notion d'étendue géographique (selon la distance). Une autre classification logique très utilisée se base sur la nature de communication entre les terminaux (Client / Client ou Client / Serveur). [1]

1.3.1 Réseau local LAN

La notion de réseau local LAN (***Local Area Network***) englobe un ensemble de techniques allant de celles nécessaires à la communication de plusieurs machines appartenant à une même organisation et reliés entre eux dans une petite aire géographique, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet). [2]

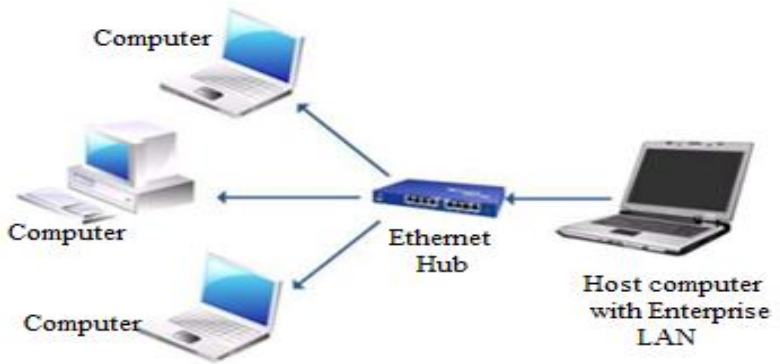


Figure 1.1 : Présentation d'un réseau local LAN

1.3.2 Réseau métropolitain MAN

Étendue de l'ordre d'une centaine de kilomètres, les MAN (***Metropolitan Area Network***) sont généralement utilisés pour fédérer les réseaux locaux ou assurer la desserte informatique de circonscriptions géographiques importantes (réseaux de campus). [2]

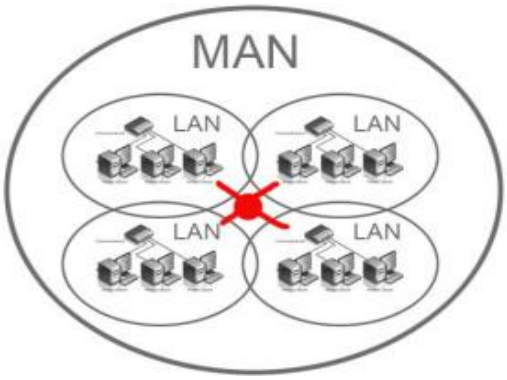


Figure 1.2 : Présentation d'un Réseau métropolitain MAN

1.3.3 Réseau WAN

Les WAN (***Wide Area Network***), sont destinés à transporter des données numériques sur des distances à l'échelle d'un pays, voire d'un continent ou de plusieurs continents. Lorsque ces réseaux appartiennent à des opérateurs, les services sont offerts à des abonnés contre une redevance.

Le réseau Internet n'a lui aucune existence propre, il est constitué d'un ensemble de réseaux d'opérateurs interconnectés entre eux (réseaux de réseaux). [2]

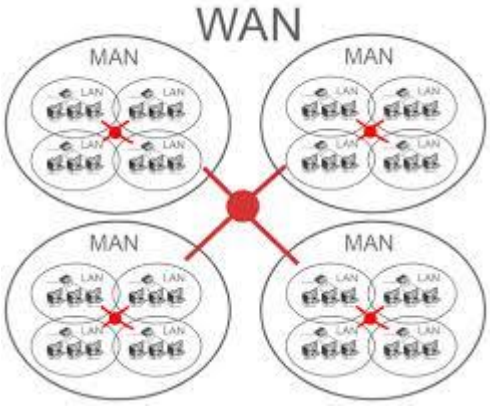


Figure 1.3 : Présentation d'un Réseau étendu WAN

Les réseaux informatiques peuvent être implémentés a partir des infrastructures via divers dispositifs et équipements, en utilisant plusieurs briques constitutives et des piles de protocoles qui se comprennent mutuellement, ou avec des combinaisons de médias et de couches de protocoles.

1.4 Équipements d'interconnexion d'un réseau

L'interconnexion des réseaux c'est la possibilité de faire dialoguer plusieurs sous réseaux initialement isolés, par l'intermédiaire de périphériques spécifiques: Répéteur, récepteur, concentrateur (Hub), pont (bridges), routeur, Commutateur (Switch), modem, Passerelle (Gateway), Vsat (*Very Small Aperture Terminal*) ....etc. Ils servent aussi à interconnecter les ordinateurs d'une organisation, d'un campus, d'un établissement scolaire, d'une entreprise. Il est parfois indispensable de les relier. Dans ce cas, des équipements spécifiques sont nécessaires. Lorsqu'il s'agit de deux réseaux de même type, il suffit de faire passer les trames de l'un vers l'autre.

Dans le cas de deux réseaux qui utilisent des protocoles différents, il est nécessaire de procéder à une conversion de protocole avant de transporter les trames (paquet des données) [3]

1.5 Les modèles d'interconnexion d'un réseau

Tous les applicatifs réseaux doivent pouvoir communiquer entre eux, quel que soit l'architecture ou la plate-forme utilisée. Pour cela, les opérations sur les réseaux ont été divisées en plusieurs phases de base, de manière à simplifier le portage des applicatifs sur toutes les plates-formes. C'est ce que l'on appelle le modèle en couche. plus souvent OSI (*Open System Interconnection*) et TCP/IP (*Transmission Internet Protocol/Internet Protocol*), Chaque couche résout un certain nombre de problèmes relatifs à la transmission de données, et fournit des services bien définis aux couches supérieures. [1]

1.5.1 Le modèle OSI

Défini en 1977, le modèle OSI (***Open System Interconnection***) découpe les communications réseaux en sept (07) niveaux, que l'on appelle également couches. Ces couches décrivent les fonctions nécessaires à la communication et la façon dont sont gérées ces communications. Par exemple, la couche 7 constitue la couche application qui gère le transfert des données entre programmes. La couche 1 (la base de l'édifice) s'occupe quant à elle de la couche physique et gère les connexions matérielles. [4]

Les couches du modèle OSI

- **La couche application :** La couche d'application fournit les protocoles et les fonctions nécessaires pour les applications clients. Il existe un nombre important de services fournis par la couche d'application. [4]
- **La couche présentation :** La couche de présentation gère la représentation des données. Un langage commun doit être utilisé pour une bonne compréhension entre les différents nœuds du réseau.
- **La couche session :** La couche de session gère les connexions entre les applications coopérants. Le modèle TCP/IP ne possède pas de couche de session car TCP fournit une grande partie des fonctionnalités de session. [4]
- **La couche transport** : La couche de transport offre des services supplémentaires par rapport à la couche réseau. Cette couche garantit l'intégrité des données. Son travail consiste à relier un sous-réseau non fiable à un réseau plus fiable. Dans le modèle TCP/IP, la fonction de la couche transport est assurée par TCP et par un protocole nommé UDP (*User Datagram Protocol*). [4]

- **La couche réseau** : La couche réseau gère les connexions entre les nœuds du réseau. Un routeur, par exemple, travaille au minimum dans cette couche. Dans le modèle TCP/IP, la fonction de la couche réseau est assurée par IP (IPv4 (*Internet Protocol version 4*) ou IPv6 (*Internet Protocol version 6*)). [4]
- **La couche liaison de données** : La couche liaison de données prend les données de la couche physique et fournit ses services à la couche réseau. Les bits reçus sont assemblés en trames (liaison possible : Ethernet, Frame Relay(*relai de trame*), X.25, PPP (*Point-to-Point Protocol*) , ATM). [4]
- **la couche physique :** La couche physique décrit les moyens mécaniques, électriques, fonctionnels et méthodologiques permettant d'activer, de gérer et de désactiver des connexions physiques pour la transmission de bits vers et depuis un périphérique réseau. [4]

1.5.2 Modèle TCP/IP

L'architecture TCP/IP (***Transmission Internet Protocol/Internet Protocol***) développé vers la fin des années 1970, a beaucoup évolué et évolue encore en fonction des innovations technologiques et des besoins des utilisateurs. Ce modèle a été créé afin de répondre à un problème pratique, alors que le modèle OSI correspond à une approche plus théorique, et a été développé plus tôt dans l'histoire des réseaux. Le modèle OSI est donc plus facile à comprendre, mais le modèle TCP/IP est le plus utilisé en pratique. Il est préférable d'avoir une connaissance du modèle OSI avant d'aborder TCP/IP, car les mêmes principes s'appliquent, mais sont plus simples à comprendre avec le modèle OSI. [5]

La figure suivante montre la différence entre le modèle OSI et TCP/IP.

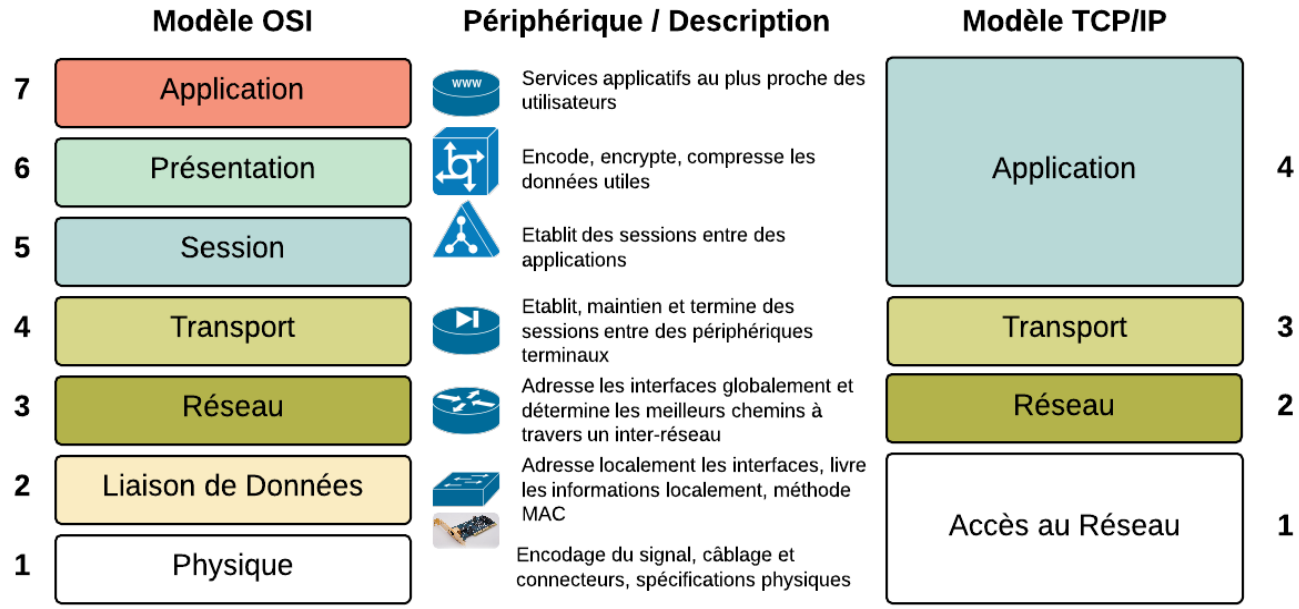


Figure 1.4 : La différence entre le modèle OSI et le TCP/IP

Les applications de réseau fonctionnent sur le modèle client/serveur. Sur la machine serveur un processus serveur traite les requêtes des clients, ces clients et serveurs dialoguent en échangeant des messages qui contiennent des requêtes et des réponses. Ce changement des messages nous conduit logiquement de cité particulièrement les protocoles veillant sur leurs bonnes communications.

1.5.2.1 TCP/UDP

TCP (***Transmission Control Protocol***) et UDP (***User Datagram Protocol***) sont les deux protocoles principaux dans la couche de transport. TCP et UDP utilisent IP comme couche réseau. TCP procure une couche de transport fiable, même si le service qu'il (IP) utilise ne l'est pas. TCP est orienté connexion, c'est-à-dire qu'il réalise une communication complète entre 2 points. Cela permet d'effectuer une communication client/serveur, par exemple, sans se préoccuper du chemin emprunté. UDP émet et reçoit des datagrammes. Cependant, contrairement à TCP, UDP n'est pas fiable et n'est pas orienté connexion. Il est utilisé pour les résolutions DNS (*Domain Name System*) et aussi pour TFTP (*Trivial File Transfer Protocol*). [4]

1.5.2.2 Le protocole IP

IP est le protocole principal de la couche réseau. Il est utilisé à la fois par TCP et UDP. Chaque bloc de données TCP, UDP, ICMP (*Internet Control Message Protocol*) et IGMP (*Internet Group Management Protocol*) qui circule sur le réseau est encapsulé dans l'IP. IP est non fiable et n'est pas orienté connexion. Par non fiable, nous voulons dire qu'il n'existe aucune garantie pour que le datagramme IP arrive à la destination. Si, par exemple, un datagramme IP arrive à un routeur saturé, le routeur efface le paquet et envoie un message ICMP "unreachabl" (inaccessible) à la source. La fiabilité d'une connexion doit être maintenue par TCP. "Pas orienté connexion", signifie que IP ne maintient aucune information d'état concernant les datagrammes successifs. Le trajet des datagrammes pour atteindre B à partir de A n'est peut-être pas le même. Les datagrammes peuvent également arriver dans le désordre par exemple. L'avantage majeur de cette technique du moindre effort, c'est la grande tolérance, notamment, vis-à-vis des pannes de l'infrastructure. [4]

1.6 L'adressage IP

Un des éléments essentiels d'IP est la couverture mondiale qu'assure le protocole. Ceci est fait grâce à une gestion d'adresses uniques. L'adressage IP permet d'identifier de façon unique une interface dans une machine connectée à un réseau. Une machine ayant plusieurs interfaces est communément appelée un routeur. Elle est capable de recevoir et de renvoyer des paquets de données par le biais de différentes interfaces. Elle utilise pour cela une table de routage qui, dans sa version la plus simple, contient un certain nombre d'adresses internet complètes ou sous forme de masques sous-réseaux, l'interface à utiliser pour atteindre chacune d'elles, et une ou plusieurs interfaces par défaut vers lesquelles envoyer les paquets d'adresse inconnues. Cette correspondance peut être enrichie d'un coût, appelé aussi métrique, servant aux protocoles de routage que nous verrons plus loin.il existe deux protocoles d'adressage en IP, le IPv4 et le IPv6. [6]

1.6.1 Le format des adresses IP

Les adresses IP sont composées de 4 octets. Par convention, on note ces adresses sous forme de 4 nombres décimaux de 0 à 255 séparés par des points. L'originalité de ce format d'adressage réside dans l'association de l'identification du réseau avec l'identification de l'hôte.

- La partie réseau est commune à l'ensemble des hôtes d'un même réseau,
- La partie hôte est unique à l'intérieur d'un même réseau.

Prenons le tableau suivant un exemple d'adresse IP pour en identifier les différentes parties :

Adresse complète	**192.168._ _1._ _1**
Masque réseau	255.255.255._ _0
Partie réseau	192.168._ _1._ _ _
Partie hôte	_ _ _._ _ _._ _ _._ _1
Adresse réseau	192.168._ _1._ _0
Adresse diffusion	192.168._ _1.255

Tableau 1.1 : Adresse IP 192.168.0.0

1.6.2 Les classes d'adresses

A l'origine, plusieurs groupes d'adresses ont été définis dans le but d'optimiser l'acheminement (ou le routage) des paquets entre les différents réseaux. Ces groupes ont été nommés classes d'adresses IP. Ces classes correspondent à des regroupements en réseaux de même taille. Les réseaux de la même classe ont le même nombre d'hôtes maximum. [6]

- **Classe A :**

Le premier octet à une valeur comprise entre 1 et 126, soit un bit de poids fort égal à 0. Ce premier octet désigne le numéro de réseau et les 3 autres correspondent à l'adresse de l'hôte. [6]

- **Classe B :**

Le premier octet à une valeur comprise entre 128 et 191, soit 2 bits de poids fort égaux à 10. Les 2 premiers octets désignent le numéro de réseau et les 2 autres correspondent à l'adresse de l'hôte. [6]

- **Classe C :**

Le premier octet à une valeur comprise entre 192 et 223, soit 3 bits de poids fort égaux à 110. Les 3 premiers octets désignent le numéro de réseau et le dernier correspond à l'adresse de l'hôte. [6]

- **Classe D :**

Le premier octet à une valeur comprise entre 224 et 239, soit 3 bits de poids fort égaux à 111. Il s'agit d'une zone d'adresses dédiées aux services de multidiffusion vers des groupes d'hôtes (host groups). [6]

- **Classe E :**

Le premier octet a une valeur comprise entre 240 et 255. Il s'agit d'une zone d'adresses réservées aux expérimentations. Ces adresses ne doivent pas être utilisées pour adresser des hôtes ou des groupes d'hôtes. [6]

voici le Tableau donnant un exemple pour l'espace d'adressage pour chaque classe :

Classe	Masque réseau	Adresse réseau	Nombre de réseaux	Nombre d'hôte par réseau
A	255.0.0.0	1.0.0.0 - 126.255.255.255	126	16777214
B	255.255.0.0	128.0.0.0 -191.255.255.255	16384	65534
C	255.255.255.0	192.0.0.0 - 223.255.255.255	2097152	254
D	240.0.0.0	224.0.0.0 - 239.255.255.255	adresses uniques	adresses uniques
E	Non défini	240.0.0.0 - 255.255.255.255	adresses uniques	adresses uniques

Tableau 1.2 : Espace d'adressage pour chaque classe

1.6.3 Le découpage des classes en sous-réseaux

Pour compenser les problèmes de distribution de l'espace d'adressage IP, la première solution utilisée a consisté à découper une classe d'adresses IP A, B ou C en sous-réseaux. Cette technique appelée subnetting a été formalisée en 1985 avec le document RFC950 (*Request for comments*). Si cette technique est ancienne, elle n'en est pas moins efficace face aux problèmes d'exploitation des réseaux contemporains. Il ne faut jamais oublier que le découpage en réseaux ou sous-réseaux permet de cloisonner les domaines de diffusion. Les avantages de ce cloisonnement de la diffusion réseau sont multiples. [6]

- Au quotidien, on évite l'engorgement des liens en limitant géographiquement les annonces de services faites par les serveurs de fichiers. Les services Microsoft basés sur netBT (*NetBIOS over TCP/IP*) sont particulièrement gourmands en diffusion réseau. En effet, bon nombre de tâches transparentes pour les utilisateurs supposent que les services travaillent à partir d'annonces générales sur le réseau. Sans ces annonces par diffusion, l'utilisateur doit désigner explicitement le service à utiliser. Le service d'impression est un bon exemple. [6]

- Il existe une quantité de vers et ou virus dont les mécanismes de propagation se basent sur une reconnaissance des cibles par diffusion. Le ver Sasser en est un exemple caractéristique. En segmentant un réseau en plusieurs domaines de diffusion, on limite naturellement la propagation de code malveillant. Le subnetting devient alors un élément de la panoplie des outils de sécurité. Pour illustrer le fonctionnement du découpage en sous-réseaux, on utilise le tableau suivant comme un exemple pratique. On reprend l'exemple de la classe C 192.168.1.0 dont le masque réseau est par définition 255.255.255.0. Sans découpage, le nombre d'hôtes maximum de ce réseau est de 254. Considérant qu'un domaine de diffusion unique pour 254 hôtes est trop important, on choisit de diviser l'espace d'adressage de cette adresse de classe C. On réserve 3 bits supplémentaires du 4ème octet en complétant le masque réseau. De cette façon on augmente la partie réseau de l'adresse IP et on diminue la partie hôte. [6]

Adresse	192.168. 1. 0	Plage d'adresses utilisables	Adresse de diffusion
Masque de réseau	255.255.255.224		
Sous-réseau 0	192.168. 1. 0	192.168.1. 1 - 192.168.1. 30	192.168.1. 31
Sous-réseau 1	192.168. 1. 32	192.168.1. 33 - 192.168.1. 62	192.168.1. 63
Sous-réseau 2	192.168. 1. 64	192.168.1. 65 - 192.168.1. 94	192.168.1. 95
Sous-réseau 3	192.168. 1. 96	192.168.1. 97 - 192.168.1.126	192.168.1.127
Sous-réseau 4	192.168. 1.128	192.168.1.129 - 192.168.1.158	192.168.1.159
Sous-réseau 5	192.168. 1.160	192.168.1.161 - 192.168.1.190	192.168.1.191
Sous-réseau 6	192.168. 1.192	192.168.1.193 - 192.168.1.222	192.168.1.223
Sous-réseau 7	192.168. 1.224	192.168.1.225 - 192.168.1.254	192.168.1.255

Tableau 1.3 : Adresse 192.168.1.0 avec subnetting sur 3 bits

Selon les termes du document RFC950, les sous-réseaux dont les bits de masque sont tous à 0 ou tous à 1 ne devaient pas être utilisés pour éviter les erreurs d'interprétation par les protocoles de routage dits classful comme RIPv1 (*Routing Information Protocol version 1*).

En effet, ces protocoles de routages de «première génération» ne véhiculaient aucune information sur le masque sachant que celui-ci était déterminé à partir de l'octet le plus à gauche. Dans notre exemple ci-dessus, il y avait confusion aux niveaux de l'adresse de réseau et de diffusion.

- L'adresse du sous-réseau 192.168.1.0 peut être considérée comme l'adresse réseau de 2 réseaux différents : celui avec le masque de classe C (255.255.255.0) et celui avec le masque complet après découpage en sous-réseaux (255.255.255.224).

- De la même façon, l'adresse de diffusion 192.168.1.255 est la même pour 2 réseaux différents: 192.168.1.0 ou 192.168.100.224. Depuis la publication du document RFC950, en 1985, les protocoles de routage qui servent à échanger les tables d'adresses de réseaux connectés entre routeurs ont évolué. Tous les protocoles contemporains sont conformes aux règles de routage inter-domaine sans classe (CIDR(*Classless Inter-Domain Routing*)). Les protocoles tels que RIPv2 (*Classless Inter-Domain Routing* 2) , OSPF et BGP (*Border Gateway Protocol*) intègrent le traitement des masques de sous-réseaux. Ils peuvent même regrouper ces sous-réseaux pour optimiser le nombre des entrées des tables de routage. Pour appuyer cet argument, le document RFC1878 de 1995 spécifie clairement que la pratique d'exclusion des sous-réseaux all-zeros (tous 0) et all-ones (tous 1) est obsolète. [6]

1.6.4 Le routage inter-domaine sans classe

Le routage inter-domaine sans classe ou Classless Inter-Domain Routing (CIDR 4) a été discuté par l'IETF à partir de 1992.

Certaines projections de croissance de l'Internet prévoyaient une saturation complète de l'espace d'adressage IP pour 1994 ou 1995.

L'utilisation de cette technique a débuté en 1994 après la publication de 4 documents RFC : RFC1517, RFC1518, RFC1519 etRFC1520.

La principale proposition du document RFC1519 publié en Septembre 1993 était de s'affranchir de la notion de classe en s'appuyant sur la notion de masque réseau dont l'utilisation était déjà très répandue à l'époque.

Le document RFC1519 permet aux administrateurs réseau d'aller au-delà du simple subnetting en donnant la capacité de faire du supernetting. En utilisant n'importe quel masque de sous-réseau ou masque de super-réseau possible, on ne se limite plus aux masques classiques des classes : 255.0.0.0, 255.255.0.0 et 255.255.255.0. Cette technique de supernetting associée au masque réseau de longueur variable (*Variable Length Subnet Mask* ou VLSM) a résolu les problèmes d'attribution de l'espace d'adressage IPv4 et d'accroissement des tables de routage de l'Internet.

Le problème d'attribution de l'espace d'adressage IPv4 a été diminué parce que l'Internet Assigned Numbers Authority n'a plus été contraint au déploiement d'espaces adresses «pleins» (classful). Au lieu d'avoir la moitié de l'espace d'adressage IPv4 réservé pour les grands réseaux massifs de classe A, cet espace a été découpé en tranches de plus petites tailles, plus faciles à utiliser. Le routage inter-domaine sans classe (CIDR), associé à la traduction d'adresses de réseau (NAT (*Network address translation*), document RFC1631de 1994), a permis au protocole IPv4 de survivre bien au-delà de la limite annoncée.

Le problème des tailles de table de routage a été également résolu à l'aide des techniques CIDR et VLSM. Le supernetting fournit aux administrateurs un masque unique pour représenter des réseaux multiples en une seule entrée de table de routage.

Par exemple, un fournisseur d'accès Internet (FAI) à qui on a assigné le réseau 94.20.0.0/16, peut attribuer des sous-réseaux à ses clients (94.20.1.0/24 à la société A, 94.20.2.0/24 à la société B, etc.) et publier l'adresse 94.20.0.0/16 dans les tables de routage pour représenter tous ses réseaux.

La technique de masque réseau de longueur variable (VLSM) permet à un client de n'acquérir que la moitié de cet espace, par exemple le réseau 94.20.0.0/23 attribue la plage d'adresses allant de 94.20.0.0 à 94.20.127.0. La plage 94.20.128.0 -94.20.254.0 peut être vendue à une autre société.

La capacité de synthétiser (summarize) de multiples sous-réseaux en une adresse et un masque de super réseau réduit significativement les tailles des tables de routage. Bien que ces tailles de tables augmentent encore, les capacités (mémoire et traitement) des équipements d'interconnexion modernes sont largement suffisantes pour gérer cette croissance. [6]

1.7 La commutation

Contrairement à un concentrateur, un commutateur ne diffuse pas les trames. Il met en relation les seuls postes concernés par l'échange. Avant de réémettre les trames, le commutateur vérifie que le support de communication est libre. Un commutateur évite donc les collisions au contraire d'un concentrateur. A chaque fois qu'un message lui parvient, le commutateur associe le port par lequel arrive la trame à l'adresse matérielle (adresse MAC (*Media Access Control*)) de l'émetteur de la trame. Ainsi après un certain nombre de trames, le commutateur connaît «l'emplacement» (c'est à dire le port de rattachement) des postes sur le réseau et peut les mettre en relation deux à deux. [3]

1.7.1 L'ethernet

La couche 2 la plus populaire est surement celle que l'on nomme abusivement "Ethernet", du nom du standard publié en 1982 par DEC (*Digital Equipment Corporation*), Intel Corp et Xerox. Cette technique repose sur une méthode d'accès et de contrôle dite CSMA/CD (*Carrier Sense, Multiple Access with Collision Detection*). Elle est devenue tellement populaire qu'on parle d'un câble Ethernet, d'une adresse Ethernet, d'une liaison Ethernet. . .

Plus tard l'IEEE sous l'instance de son comité 802, publia un ensemble de standards légèrement différents, les plus connus concernant la couche 2 sont 802.2 (Contrôle logique de la liaison – LLC7 (*Limited Liability Company 7*)) et 802.3 (CSMA/CD).

Dans le monde TCP/IP, l'encapsulation des datagrammes IP est décrite dans la RFC 894 [Hornig 1984] pour les réseaux Ethernet et dans la RFC 1042 [Postel et Reynolds 1988] pour les réseaux 802. [3]

1.7.2 Le protocole de résolution d'adresse ARP

ARP (***Address Resolution Protocol***), il est défini dans la RFC 826.

Le problème à résoudre est issu de la constatation qu'une adresse IP n'a de sens que pour la suite de protocole TCP/IP, celle-ci étant indépendante de la partie matérielle il faut avoir un moyen d'établir un lien entre ces deux constituants.

Sur une même liaison physique, Ethernet par exemple, deux machines peuvent communiquer si elles connaissent leurs adresses physiques respectives. On suppose qu'une machine connait sa propre adresse physique par un moyen qui n'est pas décrit ici (ne fait pas partie du protocole) [3]

Lors du premier échange entre 2 machines d'un même LAN, si les adresses physiques ne sont pas déjà connues, la solution à ce problème passe par l'usage du protocole ARP.

L'usage de l'ARP est complètement transparent pour l'utilisateur. [7]

1.8 Le routage

C'est l'opération qui permet d'acheminer les données dans la bonne voie.

1.8.1 Le routage statique

Le routage statique est un routage où chaque route a été saisie manuellement par l'administrateur. Il est utilisé dans les tous petits réseaux. Il est facile à gérer lorsque le nombre de routes reste limité. Lorsqu'une route est en panne, l'intervention de l'administrateur est obligatoire pour saisir une route de secours. [3]

1.8.2 Le routage dynamique

Le routage dynamique est un routage où les routes sont calculées et saisies grâce à un protocole de routage. Il est utilisé dans les plus grands réseaux. Il est plus difficile à mettre en place, mais plus facile à maintenir. Lorsqu'une route est en panne, il recalcule automatiquement un autre chemin. [3]

1.8.3 Les protocoles de routage dynamique

1.8.3.1 Le protocole RIP

C'est un protocole de routage IP de type ***vecteur distance*** basé sur l'algorithme de routage décentralisé Bellman-Ford. Il permet à chaque routeur de communiquer aux autres routeurs la métrique, c'est-à-dire la distance qui les sépare du réseau IP (le nombre de sauts qui les sépare, ou « hops » en anglais). Ainsi, lorsqu'un routeur reçoit un de ces messages, il incrémente cette distance de 1 et communique le message aux routeurs directement accessibles. Les routeurs peuvent donc conserver de cette façon la route optimale d'un message en stockant l'adresse du routeur suivant dans la table de routage de telle façon que le nombre de sauts pour atteindre un réseau soit minimal. [4]

Le fonctionnement

Le protocole RIP est le plus vieux protocole de routage dynamique, qui s'appuie sur l'échange d'information entre les routeurs adjacents. Chaque routeur connait le coût de ses propres liaisons, et diffuse ses informations aux autres routeurs qu'il connait. Ensuite les routeurs recalculent les meilleures routes, grâce aux informations reçues. [4]

1.8.3.2 Le protocole EIGRP

EIGRP (***Enhanced Interior Gateway Routing Protocol***) est un protocole de routage de type ***vecteur distance*** avancé (ou hybride selon les points de vue). Bien que son fonctionnement global ressemble très fort à un protocole de type « *distance vector* » il dispose d'une série de caractéristiques que l'on retrouve par exemple dans OSPF qui est un « ***link state*** protocol » (protocole ***d'état des liens***) comme l'établissement de relations d'adjacence.

Le fonctionnement

Tout d'abord, EIGRP fonctionne sur base d'un numéro de système autonome (« ***Autonomous System Number*** » ou « ASN »). C'est-à-dire qu'il pourra uniquement communiquer avec les routeurs où EIGRP est configuré pour le même ASN. Ensuite, une fois qu'on l'a activé sur une interface, que ce soit de manière dynamique ou statique, EIGRP tente de découvrir des voisins potentiels. pour cela, il y envoi des message « HELLO (bonjour) ». Lorsque deux routeurs reçoivent des messages HELLO l'un de l'autre, ils vérifient alors les conditions d'adjacence afin de décider si oui ou non ils deviendront des voisins EIGRP. Pour que deux routeurs deviennent voisins EIGRP il doivent remplir les conditions suivantes:

- Fonctionner dans le même AS (***Autonomous System***), donc être configuré avec le même ASN.
- Les deux routeurs doivent pouvoir s'envoyer et recevoir des paquets IP.
- Les interfaces doivent être configurées avec une adresse IP dans le même sous-réseau (subnet).
- L'interface concernée ne doit pas être configurée comme passive.
- Les valeurs K (valeurs qui définissent le calcul de la métrique) doivent correspondre.
- L'authentification EIGRP (si configurée) doit être passée avec succès. [4]

1.8.3.2 Protocole de Routage OSPF

Le protocole OSPF (***Open Shortest Path First***) est un protocole de routage à état de liens qui a été développé pour remplacer le protocole de routage à vecteur de distance RIP. Le protocole RIP était un protocole de routage acceptable au tout début des réseaux et d'Internet. Cependant, le fait que protocole RIP se basait uniquement sur le nombre de sauts comme seule métrique pour déterminer la meilleure route est rapidement devenu problématique. L'utilisation du nombre de sauts n'est pas adaptée aux réseaux de grande taille avec plusieurs chemins de vitesses variables. Le protocole OSPF présente des avantages considérables par rapport au protocole RIP car il offre une convergence plus rapide et s'adapte mieux aux réseaux de plus grande taille.

OSPF est un protocole de routage sans classe qui utilise le concept de zones pour son évolutivité.

Les caractéristiques de l'OSPF

Les caractéristiques du protocole OSPF incluent :

- **Sans classe** - Il est sans classe par conception, par conséquent, il prend en charge VLSM et CIDR.
- **Efficace** - Les changements de routage déclenchent des mises à jour de routage (pas de mises à jour régulières). Il utilise l'algorithme SPF (*Shortest Path First*) pour déterminer le meilleur chemin.

- **Convergence rapide** - Il diffuse rapidement les modifications apportées au réseau.

- **Évolutif** - Il fonctionne bien sur les petits et grands réseaux. Les routeurs peuvent être regroupés en zones pour prendre en charge un système hiérarchique.

- **Sécurisé**- Il prend en charge l'authentification MD5 (*Message Digest 5*). Une fois activés, les routeurs OSPF acceptent uniquement les mises à jour de routage chiffrées des homologues avec le même mot de passe pré-partagé.

La distance administrative (AD : ***Administrative Distance***) correspond à la fiabilité (ou préférence) de l'origine de la route. OSPF a une distance administrative par défaut de 110. [4]

1.8.3.3 Le protocole BGP

BGP (***Border Gateway Protocol***) est utilisé sur Internet pour le routage entre, par exemple, les différents systèmes autonomes OSPF. Ce protocole a été créé pour des besoins propres à Internet suite à la grande taille du réseau lui-même. [4]

1.9 L'évolution des technologies

La gestion des réseaux d'opérateurs devient de plus en plus complexe. En effet, la taille des réseaux qu'ils doivent gérer, combiner aux nombreuses contraintes techniques, législatives et commerciales les obligent à développer des solutions compliquées. Parmi ces contraintes techniques, nous pouvons mentionner l'acheminement rapide, la haute disponibilité, la répartition équilibrée du trafic, la qualité de service, la sécurité des investissements, la sécurisation des transactions... Ces contraintes rendent le routage difficile à réaliser. Pour cela, plusieurs solutions sont était normalisés. Parmi ces solutions, on trouve la technologie X25 et Frame Relay, dont on cite particulièrement l'ATM et surtout la technologie MPLS. [3]

1.9.1 La technologie ATM

Plus personne aujourd'hui ne peut contester le succès d'IP et de l'Internet. Le trafic continue sa progression géométrique à un rythme qui ne faiblit pas. Toutefois, ce succès n’est pas sans soulever des problèmes et des contraintes.

Une technologie réseau à longtemps répondue à nombre de ces contraintes, c'est l'ATM (***Asynchrones Transfert Mode***), l'ATM propose une technologie très différente d'Ethernet avec de la commutation de cellules, permettant de transporter plusieurs flottes de données par multiplexage de petites quantités de données. Chaque cellule porte un identificateur qui permet de savoir à quel flot elle appartient. La fonction de multiplexage est indépendante du support physique, ce qui permet à l'ATM d'utiliser tout type de support.

Malheureusement, cette technologie nécessite beaucoup d'énergie et lourde au cœur de réseau. Si ATM est approprié lorsque le trafic est constitué majoritairement de voix, il est inadapté lorsque le trafic est majoritairement constitue de données, ce qui est et sera de plus en plus le cas avec l'explosion du trafic où Les flux d'information sont dorénavant étendus, diversifiés, réversibles et accessibles. [3]

1.9.2 Convergence vers MPLS

Avant l'apparition de la technologie MPLS et des routeurs au débit du support physique, la réponse au problème des performances de routage des réseaux de routeurs consistait à superposer les réseaux IP aux réseaux ATM, ce qui créait une topologie virtuelle dans la couche ATM, dans laquelle tous les routeurs devenaient adjacents, et réduisant ainsi au minimum le nombre de sauts IP entre les routeurs. [3]

Toutefois, cette superposition IP/ATM présentait un inconvénient majeur : la nécessité de gérer l'explosion du nombre de connexions de circuit virtuel ATM nécessaires pour assurer un maillage complet des liaisons virtuelles entre les paires de routeurs. En effet, le nombre de circuits virtuels ATM nécessaires augmente comme le carré du nombre de routeurs connectés au nuage ATM.

Le pire fut atteint lorsque les réseaux IP eurent besoin d'augmenter leur bande passante ce que les réseaux ATM ne pouvaient leur fournir, il leur fallait des circuits à gigabits, alors que les circuits ATM étaient limités à des débits en raison des équipements.

Mais, avec le remplacement progressif des réseaux IP par les réseaux MPLS (qu'on détaillerons dans le deuxième chapitre) , les meilleures techniques des réseaux de routage et de commutation se trouvent réunies. Les réseaux MPLS sont capables de s'adapter aux besoins de forte croissance de l'internet, et de prendre la place de l'ATM en faisant face aux très grandes exigences du trafic professionnel.

De plus, les réseaux MPLS sont prêts pour la convergence des données, de la voix et de la vidéo sur IP. Il n'est donc pas surprenant que l'MPLS soit considéré par la majorité des opérateurs de réseau comme le réseau cible à long terme. [3]

1.10 Conclusion

Grasse a l'adressage IP et ces fonctionnalités le réseau a pu donner des services primordiales a communauté de la télécommunication. IP est un sigle très connu dans le domaine des réseaux, correspondant à toute une architecture.

L'apparition de découpage en sous-réseaux a permet la survie du réseau informatique malgré la saturation de ce dernier, les protocoles de routage dynamique tel que OSPF, EIGRP et BGP ont rendu la tâche plus au moins facile au ingénieurs de réseau.

Ce chapitre décrit l'architecture générale des réseaux informatique et les protocoles qui permettent à cet environnement de gérer les problèmes d'adressage, de routage et plus généralement tous les protocoles associés au protocole IP et se trouvant dans le niveau paquet.

Le prochain chapitre sera consacré à présenter et énumérer théoriquement la technologie MPLS.

Chapitre II

Multi Protocol Labels Switching (MPLS)

2.1 Introduction

Avec l'augmentation du débit des liens de communication et du nombre de routeur dans les Réseaux de communication, l'IETF a défini le nouveau protocole MPLS (***Multi Protocol Label Switching*** : ***commutation de label multi-protocole***) pour faire face au goulot d'étranglement induit par la complexité de la fonction de routage.

MPLS est une technique réseau dont le rôle principal est de combiner les concepts du routage IP de niveau 3, et les mécanismes de la commutation de niveau 2 telles que implémentée dans ATM ou Frame Relay. MPLS doit permettre d'améliorer le rapport performance/prix des équipements de routage, d'améliorer l'efficacité du routage (en particulier pour les grands réseaux) et d'enrichir les services de routage (les nouveaux services étant transparents pour les mécanismes de commutation de label, ils peuvent être déployés sans modification sur le cœur du réseau).

Les efforts de l'IETF portent aujourd'hui sur Ipv4. Cependant, la technique MPLS peut être étendue à de multiples protocoles (IPv6, IPX (*Internetwork Packet eXchange*), AppleTalk.. etc.). MPLS n'est en aucune façon restreint à une couche 2 spécifique et peut fonctionner sur tous les types de support permettant l'acheminement de paquets de niveau 3.

MPLS traite la commutation en mode connecté (basé sur les labels), les tables de commutation étant calculées à partir d'informations provenant des protocoles de routage IP ainsi que de protocoles de contrôle. MPLS peut être considéré comme une interface apportant à IP le mode connecté et qui utilise les services de niveau 2 (PPP, ATM, Ethernet, Frame Relay, SDH (*Synchronous Digital Hierarchy*) ...). La technique MPLS a été voulue par l'IETF relativement simple mais très modulaire et très efficace.

L'avantage majeur du protocole MPLS est qu'il permet un routage particulier pour chacun des LSP (*Label Switched Path*), appelés aussi tunnels MPLS, et donc permet d'associer un chemin (qui peut être différent du plus court chemin) à chaque groupe de flots considéré. La granularité du choix des routes est donc améliorée, ce qui permet une meilleure gestion de la QoS (*Quality of Service*) et surtout une ingénierie de trafic plus aisée. Mais les avantages de MPLS ne s'arrêtent pas à ces améliorations, MPLS permet aussi la création de réseaux privés virtuels VPN (***Virtual Private Network***) et est interopérable avec n'importe quelle couche de niveau 2. Il est possible aussi de déployer un réseau IP/MPLS sur des infrastructures sous-jacentes hétérogènes (SDH, Ethernet, ATM, WDM (*wavelength division multiplexing*),...).

En résumé, MPLS jouera un rôle important dans le routage, la commutation, et le passage des paquets à travers les réseaux de nouvelle génération, MPLS permet d'acheminer sur une unique infrastructure de différents types de trafic tout en respectant les contraintes de fonctionnement associées permettant la rencontre entre les besoins de service et les utilisateurs du réseau. [3.7.8]

La figure suivante, indique clairement l'enmplacement de protocole MPLS dans le modele OSI:

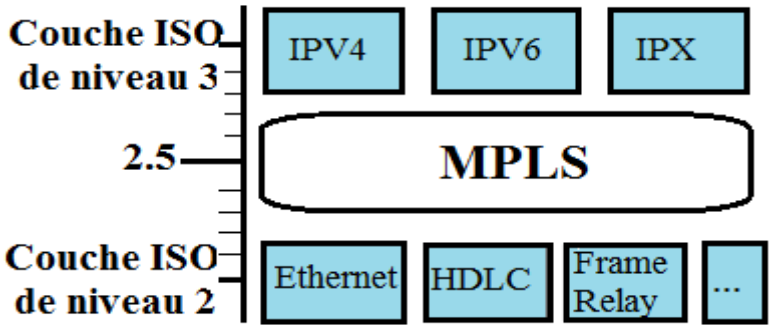


Figure 2.1: MPLS dans le modèle ISO

Nous allons, le long de ce ***deuxième (02) chapitre***, faire le tour de la technologie MPLS, nous commencerons par la présentation de ses Objectifs et missions, expliquant son principe de fonctionnement. Nous détaillerons ensuite les concepts relatifs aux labels et à leurs distributions, ainsi que d'autres détails relatifs à la technologie MPLS. Nous finirons par donner un aperçu des applications que MPLS permet de réaliser.

2.2 Objectifs de MPLS

L'un des objectifs initiaux était d'accroître la vitesse du traitement des datagrammes dans l'ensemble des équipements intermédiaires. Cette volonté, avec l'introduction des giga routeurs, est désormais passée au second plan. Depuis, l'aspect "fonctionnalité" a largement pris le dessus sur l'aspect "performance", avec notamment les motivations suivantes :

- Intégration IP/ATM.
- Création de VPN.
- Flexibilité : possibilité d'utiliser plusieurs types de media (ATM, FR (Frame Relay) , Ethernet, PPP, SDH). différentiel Services (DiffServ).
- Routage multicast.
- MPLS pourra assurer une transition facile vers l'Internet optique. MPLS n'étant pas lié à une technique de niveau 2 particulière, il peut être déployé sur des infrastructures hétérogènes (Ethernet, ATM, SDH, etc.). Avec la prise en charge de la gestion de contraintes sur la qualité de service. Avec la possibilité d'utiliser simultanément plusieurs protocoles de contrôle, MPLS peut faciliter l'utilisation de réseaux optiques en fonctionnant directement sur WDM.
- Traffic Engineering permettant de définir des chemins de routage explicites dans les réseaux IP (avec RSVP (*Resource ReSerVation Protocol*) ou CR-LDP (*Constraint-based Routing Label Distribution*)). L'ingénierie des flux est la faculté de pouvoir gérer les flux de données transportés au-dessus d'une infrastructure réseau. Aujourd'hui, cette ingénierie des flux est essentiellement faite à l'aide d'ATM, avec comme conséquence une grande complexité de gestion (en effet IP et ATM sont deux techniques réseaux totalement différentes, avec parfois des contraintes non compatibles). Avec l'intégration de cette fonctionnalité, MPLS va permettre une simplification radicale des réseaux.

MPLS est un mécanisme de transport de données basé sur la commutation d'étiquettes ou "labels", qui sont insérés à l'entrée du réseau MPLS et retirés à sa sortie. Les labels peuvent être associés à un chemin, une destination, une source, une application, un critère de qualité de service, etc. ou une combinaison de ces différents éléments. Autrement dit, le routage IP est considérablement enrichi sans pour autant voir ses performances dégradées (à partir du moment ou un datagramme est encapsulé, il est acheminé en utilisant les mécanismes de commutation de niveau 2). On peut imaginer qu'un des services les plus importants sera la possibilité de créer des réseaux privés virtuels (VPN) de niveau 3. Ainsi, des services de voix sur IP, de multicast ou d'hébergement de serveurs web pourront coexister sur une même infrastructure. La modularité de MPLS et la granularité des labels permettent tous les niveaux d'abstraction envisageables. [3]

2.3 Principe de fonctionnement de MPLS

La transmission des données s'effectue sur des chemins nommés LSP (***Label Switched Path***). Un LSP est une suite de références partant de la source et allant jusqu'à la destination, les LSPs sont établis avant la transmission des données. [7]

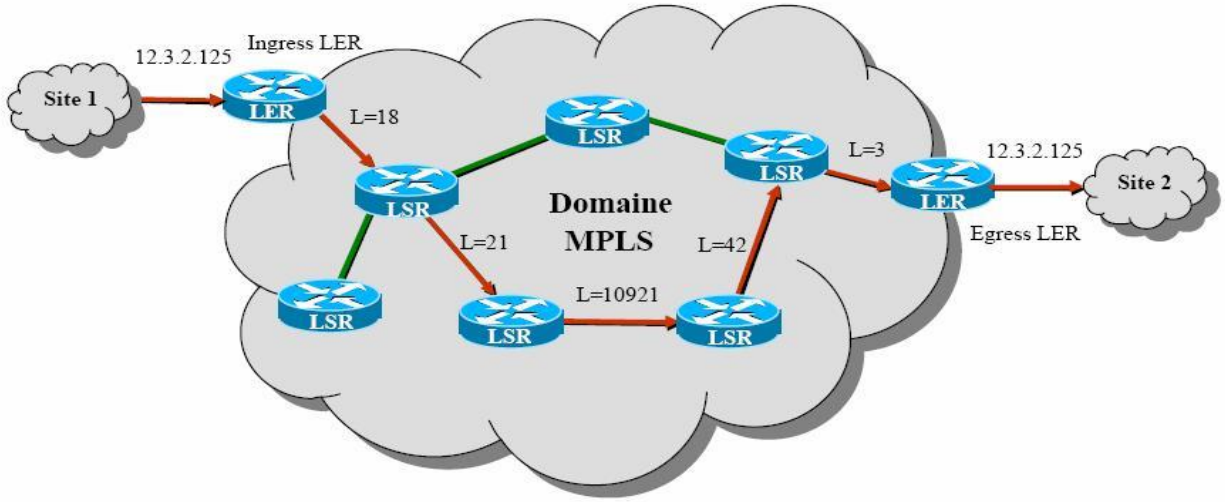


Figure 2.2: Exemple d'un réseau MPLS

Les nœuds (équipements) qui participent à la composition MPLS sont classifiés en LER (*Label Edge Router*) et LSR. Chacun pouvant avoir sa propre technique de commutation.

LSR *(Label Switch Router)* : Un LSR est un routeur dans le cœur du réseau qui participe à la mise en place du circuit virtuel par lequel les trames sont acheminées. Ses fonctions consistent en l'échange d'informations de routage, l'échange des labels, et l'acheminement des paquets.

LER *(Label Edge Router)* : Un LER est un nœud d'accès au réseau MPLS, qui peut avoir des ports multiples permettant d'accéder à plusieurs réseaux distincts. Les LER jouent un rôle important dans la mise en place des références. où Il existe deux types de LER :

- ***Ingress LER*** : c'est un routeur qui gère le trafic qui entre dans un réseau MPLS.
- ***Egress LER***: c'est un routeur qui gère le trafic qui sort d'un réseau MPLS.

Dans MPLS, le routage s'effectue par l'intermédiaire de classes d'équivalence, appelées FEC (***Forwarding Equivalence Class***). Une classe représente un flot ou un ensemble de flots ayant les mêmes propriétés, notamment le même préfixe dans l'adresse IP.

Toutes les trames d'une FEC sont traitées de la même manière dans les nœuds du réseau MPLS. Les trames sont introduites dans une FEC au nœud d'entrée et ne peuvent plus être distinguées à l'intérieur de la classe des autres flots.

Quand un paquet IP arrive à un ***ingress LER***, il sera associé à une ***FEC***. Puis, exactement comme dans le cas d'un routage IP classique, un protocole de routage sera mis en œuvre pour découvrir un chemin jusqu'à ***l'egress LER*** (Voir les flèches rouges dans Figure2.2). Mais à la différence d'un routage IP classique cette opération ne se réalise qu'une seule fois. Ensuite, tous les paquets appartenant à la même ***FEC*** seront acheminés suivant ce chemin qu'on appellera Label Switched Path ***(LSP)***. Un LSP est le chemin établi au travers d'un ou plusieurs LSRs pour rejoindre plusieurs LERs au sein d'un réseau MPLS, configuré uniquement via le mécanisme des labels, pour une FEC particulière. Il peut être établi statiquement ou dynamiquement. [1.7]

Ainsi on a eu la séparation entre fonction de routage et fonction de commutation : Le routage se fait uniquement à la première étape. Ensuite tous les paquets appartenant à la même FEC subiront une commutation simple à travers ce chemin découvert.

Pour que les LSR puissent commuter correctement les paquets, le Ingress LER affecte une étiquette appelée Label à ces paquets (label imposition ou label pushing). Ainsi, si on prend l'exemple de la figure 1.1, Le LSR1 saura en consultant sa table de commutation que tout paquet entrant ayant le label L=18 appartient à la FEC tel et donc doit être commuté sur une sortie tel en lui attribuant un nouveau label L=21 (label swapping). Cette opération de commutation sera exécuter par tous les LSR du LSP jusqu'à aboutir à l'Egress LER qui supprimera le label (label popping ou label disposition) et routera le paquet de nouveau dans le monde IP de façon traditionnelle, mais Comme les opérations de routage sont complexes et coûteuses, il est recommandé d'effectuer l'opération de dépilement sur le dernier LSR (***Penultimate node***) du LSP (avant-dernier nœud du LSP avant le LER) pour éviter de surcharger le LER inutilement.

Un Penultimate node est le routeur immédiat précédent le routeur LER de sortie pour un LSP donné au sein d'un réseau MPLS. C'est l'avant denier saut sur un LSP. Il joue un rôle particulier pour l'optimisation.

L'acheminement des paquets dans le domaine MPLS ne se fait donc pas à base d'adresse IP mais de label (commutation de label).

Il est claire qu'après la découverte de chemin (par le protocole de routage), il faut mettre en œuvre un protocole qui permet de distribuer les labels entre les LSR pour que ces derniers puissent constituer leurs tables de commutation et ainsi exécuter la commutation de label adéquate à chaque paquet entrant. Cette tâche est effectuée par ***"un protocole de distribution de label"*** tel que LDP (*Label Distribution Protocol*) ou RSVP-TE (*ReSerVation Protocol-Traffic Engineering*).

Les trois opérations fondamentales sur les labels (*Pushing/pousser, swapping/changer et popping*) sont tout ce qui est nécessaire pour MPLS. Le Label pushing/popping peut être le résultat d'une classification en FEC aussi complexe qu'on veut. Ainsi on aura placé toute la complexité aux extrémités du réseau MPLS alors que le cœur du réseau exécutera seulement la fonction simple de label swapping en consultant la table de commutation. [1.7]

2.4 Architecture MPLS

L'architecture MPLS supporte plusieurs protocoles que nous verrons lors de la description de label. Cela signifie que le mécanisme n'est pas lié à une couche de niveau 2 ou de niveau 3 particulière.

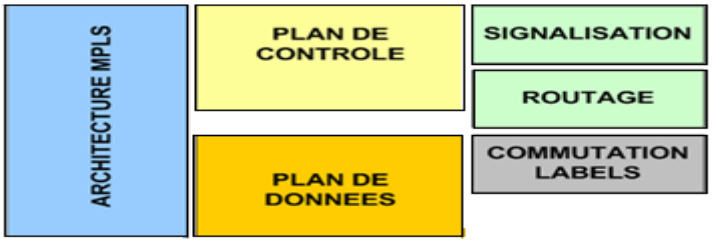


Figure 2.3: Architecture logique MPLS

le protocole MPLS est fondé sur deux plans principaux (regarder la figure 2.3) à savoir : le plan de contrôle et le plan de données. [1.7]

- **Le plan de contrôle** : chargé de gérer et maintenir les labels contenus dans chaque routeur du réseau MPLS. Ce plan de contrôle utilise des protocoles de routages classiques, tels que OSPF ou RIP (voir le chapitre 01) afin de créer la topologie des nœuds du réseau MPLS, ainsi que des protocoles spécialement développés pour le MPLS comme Label Distribution Protocol que nous étudierons par la suite.
- **Le plan de données** : contient le mécanisme de transmission des données et est complètement indépendant de la partie signalisation. Il utilise une table de commutation appelée ***Label Forwarding Information Base*** (LFIB) pour transférer les paquets labélisés avec les bons labels.

Exemple : de la figure 2.4

- Réception du label 17 pour les paquets à destination du 10.0.0.0/8.
- Génération d'un label 24 pour ces paquets et expédition de l'information aux autres routeurs.
- Insertion de l'information dans la LFIB.

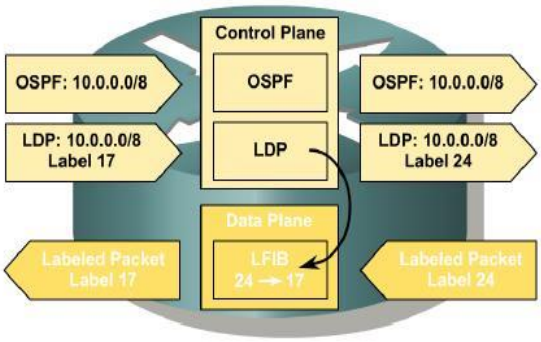


Figure 2.4: Structure fonctionnelle du routeur MPLS

Les nœuds de transfert (LSR) qui se comportent comme des commutateurs pour les flots de données utilisateur et comme des routeurs pour la signalisation, construisent trois bases d'information pour acheminer les paquets :

- **LIB** (***Label Information Base***) : C'est La première table construite par le routeur MPLS utilisée par LDP. Elle contient pour chaque sous-réseau IP la liste des labels affectés par les LSR voisins. il est possible de connaître les labels affectés à un sous-réseau par chaque LSR voisin et donc elle contient tous les chemins possibles pour atteindre la destination.
- **FIB** (***Forwarding Information Base***) : Appartient au plan de donnée, c'est la base de donnée utilisé pour acheminer les paquets non labellisé.
- **LFIB** (***Label Forwarding Information Base***) : A partir de la table LIB et de la table de routage IP, le routeur construit une table LFIB qui contient que les labels du meilleur prochain saut qui sera utilisée pour commuter les paquets labellisé. [1.7]

Fonctionnement

Un routeur effectue 4 étapes pour attribuer et distribuer les labels :

- Echange d'informations en utilisant l'IGP (*Interior Gateway Protocol*) comme OSPF, IS-IS (*Intermediate system to intermediate system*) ou EIGRP
- Les labels locaux sont générés. Un unique label est affecté à chaque destination IP contenu dans la table de routage et stocké dans la table appelée Label Information Base(LIB)
- Les labels locaux sont diffusés aux routeurs voisins pour être utilisés comme next-hop label. Stockage dans les tables FIB et LFIB
- Chaque LSR construit ses propres structures FIB, LFIB et LIB

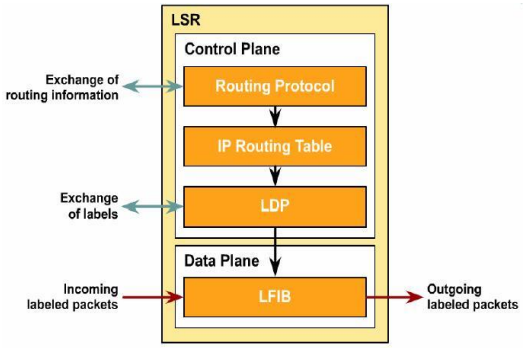


Figure 2.5 : Architecture de LRS

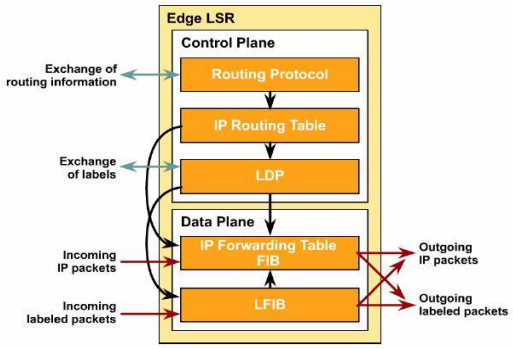


Figure 2.6 : Architecture de LER

Les technologies commutées demandent une référence (label) pour permettre aux blocs de données, que ce soit des trames, des paquets ou d'autres entités, d'avancer dans le réseau. [1.7]

2.5 Les labels

MPLS est un mécanisme de transport de données basé sur ***la commutation d'étiquettes ou "labels"***, qui sont insérés à l'entrée du réseau MPLS et retirés à sa sortie. [7]

2.5.1 Le label

Un label a une signification d'identificateur local d'une FEC entre 2 LSR adjacents et mappe le flux de trafic entre le LSR amont et le LSR aval. La figure 2.7, illustre la mise en œuvre des labels dans différentes technologies. Ainsi, MPLS fonctionne indépendamment des protocoles de niveau 2 (ATM, Frame Relay, etc.) et des protocoles de niveau 3 (IP, etc.). C'est ce qui lui vaut son nom de "Multi Protocol Label Switching". [1.7]

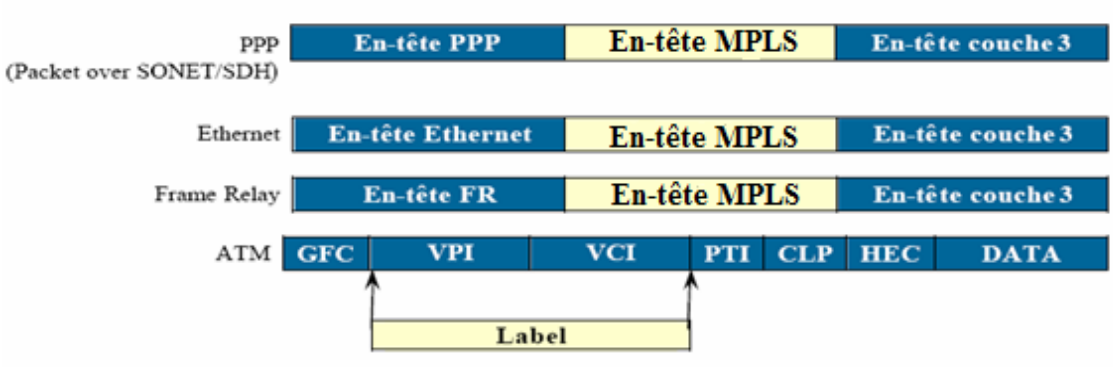


Figure 2.7: L'encapsulation MPLS dans différentes technologies

2.5.2 L'entête MPLS

Dans le cas ATM, MPLS utilise les champs VPI (*Virtual Path Identifier*) et VCI (*Virtual Channel Identifier*) comme étant un label MPLS. Dans les autres cas, MPLS insère un en-tête (***32 bits***) entre la couche 2 et la couche 3 appelés ***shim MPLS***. La figure 2.8 illustre le format d'un shim MPLS :

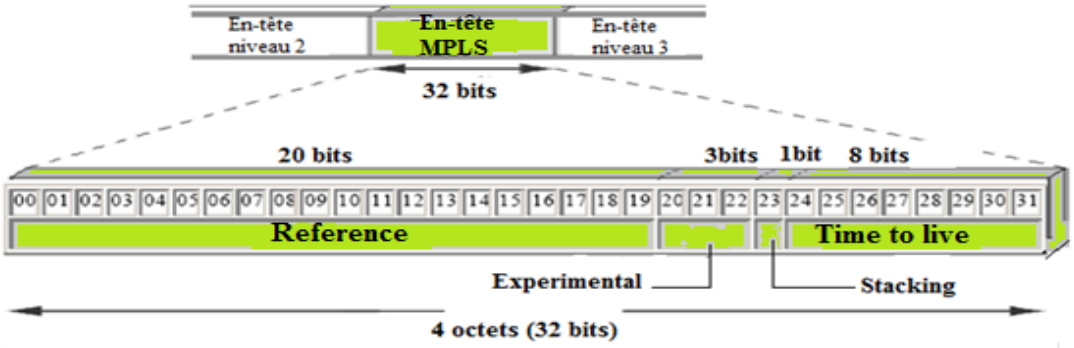


Figure 2.8: Introduction de références dans le label-switching

La référence (***label***) se trouve donc dans le champ appelé Shim MPLS, ou dérivation MPLS. Ce champ contient la référence elle-même ainsi qu'un champ de 3 bits appelé ***Expérimental*** (*EXP*) et destiné aux équipementiers, un bit appelé ***Stacking*** (*S*), qui permet d'empiler les références, c'est-à-dire de mettre plusieurs Shim MPLS de suite entre l'en-tête de niveau 2 et l'en-tête de niveau 3, et un dernier champ, dit ***Time To Live*** (*TTL*), sur 8 bits, qui définit le temps avant lequel le paquet est détruit. [7]

Schématisée à la Figure 2.8 l'entête MPLS dispose d'une longueur de 32 bits formée des champs suivants :

LABEL (***20 bits***) : Contient le label.

EXP (***3 bits***) : Initialement réservé pour une utilisation expérimentale. Actuellement, la plus part des implémentations utilise ce champ comme indicateur de ***QoS***. Généralement, c'est une copie du champ précédence (PPP) dans l'en-tête IP. En IP, la précédence définit la priorité d'un paquet (0 : priorité supérieure, 7 : priorité inférieure).

S (***1 bit***) : Indique s'il y a empilement de labels (il est en fait commun d'avoir plus qu'un label attaché à un paquet). Cette notion sera reprise dans le paragraphe suivant. Le bit S est à 1 lorsque le label se trouve au sommet de la pile, à 0 sinon.

TTL (***8 bits***) : Même signification que pour IP. Ce champ donne la limite supérieure au nombre de routeurs qu'un paquet peut traverser. Il limite la durée de vie du paquet. Il est initialisé à une certaine valeur, puis décrémenté de un par chaque routeur qui traite le paquet. Lorsque ce champ atteint 0, le paquet est rejeté. L'utilisation de ce champ évite les boucles de routage [7.13]

2.5.3 Pile de labels (*Label Stack*)

Comme on l'a déjà évoqué, il est commun d'avoir plus qu'un label attaché à un paquet. Ce concept s'appelle empilement de label. L'empilement de label permet en particulier d'associer plusieurs contrats de service à un flux au cours de sa traversée du réseau MPLS.

Les LSR de frontière de réseau (comme l'indique la figure 2.9), auront donc la responsabilité de pousser ou tirer la pile de labels pour désigner le niveau d'utilisation courant de label. [7.9]

Les applications suivantes l'exigent :

- MPLS VPN : MP-BGP (*Multi Protocol Border Gateway Protocol*) est utilisé pour propager un label secondaire en addition à celui propagé par TDP ou LDP.
- MPLS TE : MPLS TE utilise RSVP TE (*Ressource Reservation Protocol TE*) pour établir un tunnel LSP (*Label Switched Path*). RSVP TE propage aussi un label en addition de celui propagé par TDP (*Tag Distribution Protocol*) ou LDP. [7.9]

MPLS VPN et MPLS-TE parmi les applications majeures de la technologie MPLS qu'on verra prochainement.

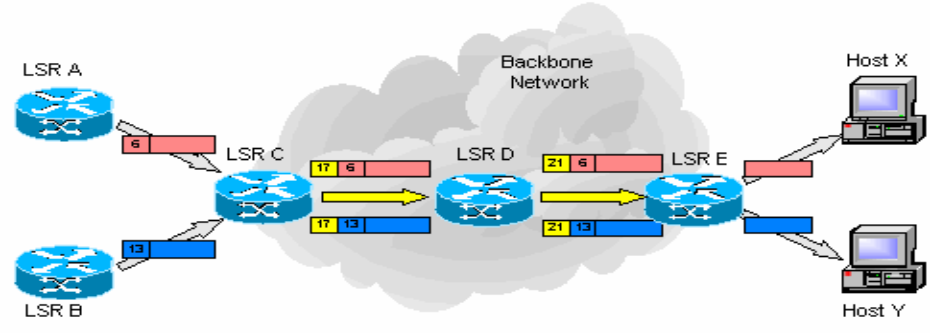


Figure2.9: Pile de labels

Le champ STACK permet d'identifier le classement du label dans la pile (voir la Figure 2.10), s'il est égal à 1 alors il s'agit du dernier label avant l'entête IP.

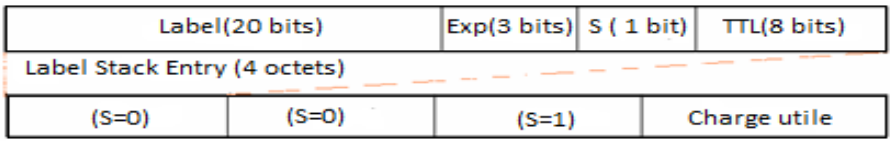


Figure 2.10: Exemple d'utilisation du champ STACK

2.5.4 Contrôle de distribution des labels

Il existe deux modes de contrôle de distribution des labels aux LSR voisins :

- ***Mode de contrôle ordonné (Ordered control mode) :***

Dans ce mode, un LSR associe un label à une FEC particulière, si :

- Il s'agit d'un Egress LER.
- L'assignation (l'association Label, FEC) a été reçue du LSR situé au saut suivant.

- ***Mode de contrôle indépendant (Independent control mode) :***

Dans ce mode, les LSR sont libres de communiquer les associations entre label et FEC à leurs voisins sans attendre de recevoir l'assignation du LSR situé au saut suivant.

Ainsi, un LSR peut diffuser un label pour une FEC, quand bien même il n'est pas prêt à communiquer sur ce label. [7.10]

2.5.5 Distribution et gestion des labels

La distribution des références s'effectuait par l'aval en remontant vers la station d'émission. dans la norme MPLS la distribution des références peut s'effectuer par l'aval (downstream) ou par l'amont (upstream). Dans le premier cas, le destinataire indique aux nœuds amont la valeur de la référence à mettre dans la table de commutation. Dans le second cas, le paquet arrive avec une référence, et le nœud met à jour sa table de commutation. [7.13]

- ***Descente systématique (unsolicited downstream) :***

Le LSR en aval envoie le label au LSR en amont de manière systématique (sans demande explicite), dans l'exemple de la figure 2.11, LSR C demande au LSR B d'utiliser le Label 53 Pour la destination 182.65.10/24. LSR B, à son tour, demande au LSR A d'utiliser le label 25 pour cette même destination.

Figure 2.11: Unsolicited downstream

Descente à la demande (Downstream-on-Demand)

Dans l'exemple de la figure suivante, le LSR en aval envoie le label au LSR précèdent uniquement s'il a reçu une requête. Et ceci même s'il a déjà généré un label pour la FEC en question. [7.10]

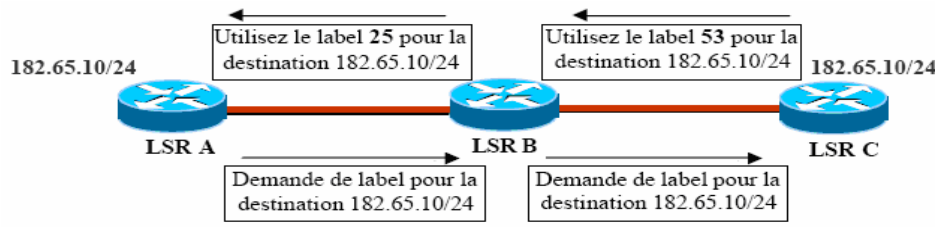


Figure 2.12 : Downstream-on-demand

2.5.6 Modes de rétention de label

Afin d'accélérer la convergence du réseau lors d'un changement de topologie (lien défectueux, dysfonctionnement d'un routeur), les LSR conservent dans leur table LIB la liste des labels annoncés pour chaque réseau IP par leurs voisins TDP, y compris de ceux n'étant pas les sauts suivants choisis par l'IGP. Ainsi, en cas de perte d'un lien ou d'un nœud, la sélection d'un nouveau label de sortie est immédiate : en effet, il suffit au routeur d'élire un nouveau saut et de sélectionner l'entrée correspondante dans la LIB, puis de mettre à jour la LFIB.

L'architecture MPLS prévoit deux politiques de rétention de labels : soit" **conservatif** "soit" **libéral** ".

- ***Mode de rétention conservatif*** : seul le label correspondant au meilleur bond est retenu et ignorent tous les autres, Ce mode nécessite peu de mémoire. En contrepartie, on aura une adaptation plus lente en cas d'erreur.
- ***Mode de rétention libéral*** : tous les labels transmis par les LSR adjacents pour un flux donné sont retenus. Ce mode permet un reroutage rapide en cas de problème car des labels alternatifs sont disponibles instantanément. En contrepartie, nécessite beaucoup de mémoire. [7.10]

2.5.7 Espace de labels (Label Space)

Les labels utilisés par un LSR pour l'assignation de labels à un FEC sont définis de deux façons:

Par plate-forme (per-platform label space ou global space) :

Dans ce cas, les valeurs de labels sont uniques dans tous les équipements LSR. Les labels sont alloués depuis un ensemble commun de labels : de la sorte, deux labels situés sur des interfaces distinctes possèdent des valeurs distinctes.

Par interface (per-interface label space) :

Les domaines de valeurs des labels sont associés à une interface. Plusieurs peuvent être définis. Dans ce cas, les valeurs de labels fournies sur des interfaces différentes peuvent être identiques. Il est clairement stipulé qu'un LSR peut utiliser une assignation de label par interface, à la condition express qu'il soit en mesure de distinguer l'interface depuis laquelle arrive le paquet. Il risque sinon de confondre deux paquets possédant le même label, mais issus d'interfaces différentes. [7.10]

2.5.8 Création des labels

Plusieurs méthodes sont utilisées pour la création des labels, en fonction des objectifs recherchés.

- ***Fondée sur la topologie (Topology-based) :*** Cette méthode engendre la création de labels à l'issue de l'exécution normale des processus de routages (comme OSPF ou BGP).
- ***Fondée sur les requêtes (Request-based) :*** Cette méthode de création de labels est déclenchée lors de l'exécution d'une requête de signalisation.

Les deux méthodes exposées sont des exemples d'assignation de labels établis à partir du modèle orienté contrôle, les labels sont assignés et distribués préalablement à l'arrivée des données de trafic de l'utilisateur.

Voici les principaux protocoles de distribution de labels envisagés :

- *TDP* ***(Tag Distribution Protocol)*** : Prédécesseur de LDP.
- *LDP* ***(Label Distribution Protocol)*** : Protocole créé spécifiquement.
- *PIM* ***(Protocol Independent Multicast)*** : Amélioration de PIM pour la distribution des labels.
- *CR-LDP* ***(Constraint-based Routing LDP)*** : Amélioration de LDP.
- *RSVP TE* ***(Ressource ReSerVation Protocol Traffic Engineering)*** : Amélioration de RSVP Les trois premières approches sont fondées sur la topologie (Topology-based). Les deux dernières approches sont fondées sur les requêtes (Request-based). Et ce sont ces deux protocoles de distribution de labels qui sont utilisés pour le MPLS Traffic Engineering. [7.10]

2.5.9 Fonctionnement de quelques protocoles de distribution de label

MPLS normalise plusieurs méthodes pour réaliser la distribution des références (Labels). La distribution indique que chaque nœud possède ses propres références et qu'il doit les mettre en correspondance avec les références de ses voisins. [7.9.11]

Le tableau ci-dessous présente quelques protocoles de distribution de labels et leurs modes de fonctionnements respectifs :

Protocole de distribution	Contrôle	Distribution	Conservation	Espace de label	Création
TDP et LDP	Unordered	Downstream unsolicited	Liberal	Per platform	Topology – based
TDP et LDP (avec ATM)	Ordered	Downstream on Demand	Conservative	Per interface	Topology-based
RSVP TE	Ordered	Downstream	Conservative	Per platform	Request-
CR-LDP	Unordered / Ordered	Downstream unsolicited Downstream onDemand	Liberal / Conservative	Per platform / Per interface	Request-based

Tableau 2.1: Mode de fonctionnement de quelques protocoles de distribution de label

2.6 Les protocoles de distribution de label

Les labels inclus dans les trames sont distribués en utilisant un protocole de signalisation. Le plus important de ces protocoles est LDP, mais on utilise aussi RSVP-TE et RC-LDP, éventuellement associé à un protocole de routage, comme BGP (*Border Gateway Protocol*) ou OSPF. Les trames acheminant les paquets IP transportent les labels de nœud en nœud. [7]

2.6.1 LDP

LDP (***Label Distribution Protocol***) est le protocole de distribution des références qui tend à devenir le standard le plus utilisé dans MPLS. Ce protocole tient compte des adresses unicast et multicast. Le routage est explicite et est géré par les nœuds de sortie. LDP est donc bidirectionnel et permet la découverte dynamique des nœuds adjacents (voir figure 2.13). Une fois que les 2 nœuds se sont découverts, ils établissent une session TCP qui agit comme un mécanisme de transport fiable des messages d'établissement de session TCP. [3.7]

Figure 2.13: Principe de fonctionnement d'un LDP

Les messages échangés entre les deux routeurs « LSR » lors d'une session « LDP » sont de types:

- ***Messages de découverte*** (discovery message) : recherche et maintien la connexion avec un - LSR - sur le réseau.
- ***Messages de session*** (session message) : établissement, maintien et cessation de sessions LDP.
- ***Messages d'avertissement*** (advertisement message) : Création, modification et suppression des correspondances entre FEC et labels.
- ***Messages de notification*** (notification message) : utilisés pour fournir des informations et signaler des erreurs.

Bien qu'LDP ait des limitations, il trouve sa compensation par le complément apporté par d'autres protocoles, parmi ces derniers nous allons insister sur les deux protocoles **RSVP-TE** et **CR-LDP**. Ceci nous conduit aux notions de routage dans MPLS. [3.7]

2.6.2 LE PROTOCOLE RSVP TE

RSVP-TE ***(Resource ReSerVation Protocol Traffic Engineering)*** est un protocole de signalisation destiné à réserver les ressources pour les flux de données des applications dans un réseau MPLS. Le protocole RSVP utilisait initialement un échange de messages pour réserver les ressources des flux IP à travers un réseau. Une version étendue de ce protocole RSVP-TE, en particulier pour permettre les tunnels de LSP, autorise actuellement RSVP à être utilisé pour distribuer des étiquettes MPLS.

RSVP est un protocole complètement séparé de la couche IP, qui utilise des datagrammes IP ou UDP (*User Datagram Protocol*) pour communiquer entre LSR. RSVP ne requiert pas la

maintenance nécessaire aux connexions TCP, mais doit néanmoins être capable de faire face à la perte de messages de contrôle. [9]

Les échanges d'informations nécessaires à l'établissement de LSP permettant les tunnels de LSP et utilisant RSVP sont décrits dans la figure suivante :

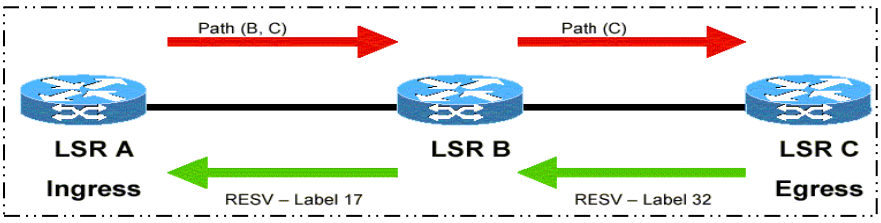


Figure 2.14: Etablissement LSP par RSVP-TE

Le fonctionnement de RSVP TE

RSVP TE est un mécanisme de signalisation utilisé pour réserver des ressources à travers un réseau. RSVP TE n'est pas un protocole de routage. Toute décision de routage est faite par IGP (*Interior Gateway Protocol*). Le seul travail de RSVP TE est de signaler et de maintenir la réservation de ressources à travers le réseau.

RSVP TE a trois fonctions de base :

1. L'établissement et la maintenance des chemins (*Path setup and maintenance*)
2. La suppression des chemins (*Path teardown*)
3. La signalisation des erreurs (*Error signalling*)

RSVP TE est un "*soft-state protocol*". Cela veut dire qu'il a besoin de rafraîchir périodiquement ses réservations dans le réseau. Ceci est différent des "*hard-state protocol*", qui signalent leurs requêtes une seule fois et puis supposent qu'elle reste maintenue jusqu'à sa résiliation explicite. Avec RSVP TE, une requête est résiliée si elle l'est explicitement du réseau par RSVP TE ou si la durée de réservation expire. [3.7.12]

Nous allons résumer le processus d'établissement des chemins avec l'exemple de la figure suivante :

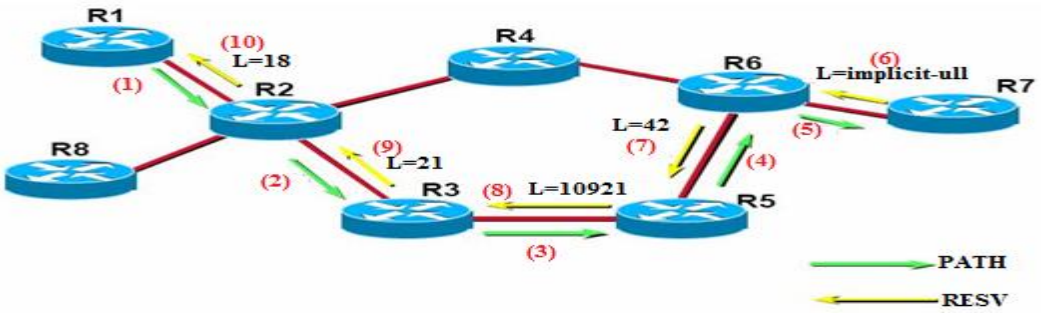


Figure 2.15: Path et Resv messages, lors de l'établissement de chemin

Supposant que R1 a déjà réalisé sa procédure CSPF (*Constrained Shortest Path First*) et a déjà décidé des besoins en bande passante qu'il veut réserver le long du chemin (R1→R2→R3→R5→R6→R7) :

(**1**) R1 envoie un Path message à R2. R2 reçoit le Path message, vérifie le format du message et la disponibilité de la bande passante demandée par R1. S'il y a un problème, R2 envoie un message d'erreur (PathErr) vers R1. Si tout se passe bien, on passe à l'étape(2)
(**2**) R2 envoie un Path message à R3. R3 fait les mêmes vérifications que dans l'étape (1)
(**3**) R3 envoie un Path message à R5. Réalisation des mêmes vérifications.
(**4**) R5 envoie un Path message à R6. Réalisation des mêmes vérifications.
(**5**) R6 envoie un Path message à R7. Réalisation des mêmes vérifications.
(**6**) R7 étant le tunnel tail, envoie un Resv message à R6. Ce Resv message contient le label que R7 veut voir dans les paquets de ce tunnel. Puisque R7 est le tail, il envoie un label= implicit-null=3.
(**7**) R6 envoie un Resv message à R5 et indique qu'il veut voir un incoming label 42 dans les paquets de ce tunnel. Ceci veut dire que quand R6 reçoit le label 42, il enlève ce label (à cause de l'implicit-null) et envoie le paquet vers R7.
(**8**) R5 envoie un Resv message à R3 et indique qu'il veut voir un incoming label 10921 dans les paquets de ce tunnel. Ceci veut dire que quand R5 reçoit un paquet de donnée avec le label 10921, il le change (swapping) en 42 et envoie le paquet vers R6.
(**9**) R3 envoie un Resv message à R2, en signalant le label 21.
(**10**) R2 envoie un Resv message à R1, en signalant le label 18 .

A ce stade, Le TE LSP est complètement établie entre R1 et R7. Le headend (R1) peut alors commencer à envoyer les données. [3.12]

2.6.3 Le protocole CR-LDP

CR-LDP ***(Constraint based Routing over Label Distribution Protocol)*** est une version étendue de LDP, où CR correspond à la notion de « routage basé sur les contraintes des LSP ». Tout comme LDP, CR-LDP utilise des sessions TCP entre les LSR, au cours desquelles il envoie les messages de distribution des étiquettes. Les échanges d'informations nécessaires à l'établissement des LSP utilisant CR-LDP sont décrits dans la figure 2.20 . Ceci permet en particulier à CR-LDP d'assurer une distribution fiable des messages de contrôle [3.9]

La gestion des réservations dans CR-LDP est très similaire à celle utilisée dans les réseaux ATM, Alors que RSVP TE utilise plutôt le modèle d'IntServ (*Integrated services*).

Il y a quatre catégories de message CR-LDP :

- ***Discovery messages :*** utilisés pour annoncer et maintenir la présence des LSR dans le réseau. Ceci est réalisé par l'envoie périodique de messages Hello.
- ***Session messages :*** utilisés pour établir, maintenir et libérer des sessions entre des voisins LDP**.**
- ***Advertisement messages :*** utilisés pour créer, changer et libérer des associations de FEC et LSP.
- ***Notification messages :*** utilisés pour véhiculer les informations de supervision.

Il y a deux sortes de Notification messages :

- *Error notifications :* utilisés pour signaler les erreurs fatales. Quand ces messages sont reçus, la session LDP est terminée et toutes les associations de labels correspondantes sont annulées.
- *Advisory notifications* : utilisés pour véhiculer des informations sur la session LDP. [7.9]

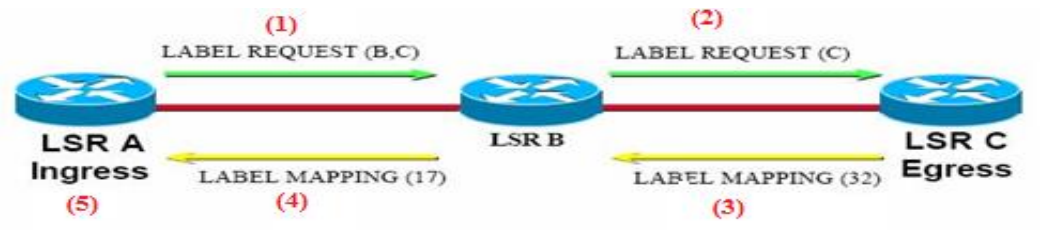


Figure 2.16 : Etablissement d'un CR-LDP LSP

(**1**) Ingress LSR A détermine qu'il a besoin d'établir un nouveau LSP vers LSR C en passant par LSR B. Pour cela, LSR A envoie à LSR B un LABEL_REQUEST message avec l'*explicit route* (B,C) et le détail des paramètres du trafic nécessaire pour cette nouvelle route.

(**2**) LSR B reçoit le LABEL_REQUEST message, réserve les ressources demandées, modifie l'*explicit route* dans le *LABEL_REQUEST message* et fait suivre le message à LSR C. Si nécessaire, LSR B peut réduire les réservations demandées dans le cas où les paramètres correspondant sont marqués négociables dans le *LABEL_REQUEST message.*

(**3**) LSR C détecte que c'est lui l'egress LSR. Il fait les mêmes activités de réservation et de négociation que LSR B. Il alloue un label pour le nouveau LSR et l'envoie à LSR B dans un *LABEL_MAPPING message.* Ce message contient aussi les détails des paramètres finaux du trafic pour ce LSP.

(**4**) LSR B reçoit le *LABEL_MAPPING message*, il finalise la réservation, alloue un label pour le LSP et met à jour sa table de labels. Ensuite, il envoie le nouveau label à LSR A dans un autre *LABEL_MAPPING message*.

(**5**) Le même processus se réalise dans LSR A. Mais vu que LSR A est l'ingress LSR, il n'aura pas à allouer un label. [12]

2.7 Le routage MPLS

Deux solutions d'implémentation des LSP sont possibles :

2.7.1 Implicit Routing

Le routage saut par saut (ou ***routage implicite***), où chaque paquet contenant un LSP choisit indépendamment le saut suivant pour une FEC de données et le ***routage explicite***, où le premier LSR détermine la liste des nœuds a suivre. [11]

La distribution implicite de labels aux LSR est réalisée grâce au protocole LDP (Label Distribution Protocol). LDP définit une suite de procédures et de messages utilisés par les LSR pour s'informer mutuellement du mapping entre les labels et le flux (Exemple dans la figure 2.22). Les labels sont spécifiés selon le chemin Hop By Hop défini par l'IGP (*Interior Gateway Protocol*) dans le réseau. Chaque nœud doit donc mettre en œuvre un protocole de routage de niveau 3, et les décisions de routage sont prises indépendamment les unes des autres. [7.12]

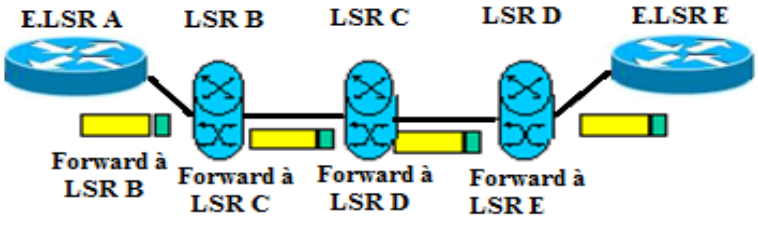


Figure 2.17: Implicit Routing: LSP HOP BY HOP

2.7.2 Explicit Routing

L'Explicit Routing est la solution MPLS pour faire du Traffic Engineering en imposant au réseau des contraintes sur les flux, du point source jusqu'au point destination. Ainsi, des routes autres que le plus court chemin peuvent être utilisées.

Les objectifs d'explicit Routing est le suivant :

- Utiliser efficacement les ressources du réseau
- Eviter les points de forte congestion en répartissant le trafic sur l'ensemble du réseau.

En effet, le plus court chemin déterminé par le routage classique IP pour atteindre une destination peut ne pas être le seul chemin possible et certains chemins alternatifs peuvent être sous-utilisés alors que le plus court chemin est sur utilisé. Dans l'Explicit Routing, le LSP n'est plus déterminé à chaque bond comme pour L'implicit Routing c'est l'ingress node qui choisit le chemin de bout en bout. Au niveau des LSR en cœur de réseau, seul le label MPLS est analysé (pas l'en-tête du datagramme IP). [7.11]

Un exemple d'Explicit Routing est représenté dans la figure suivante :

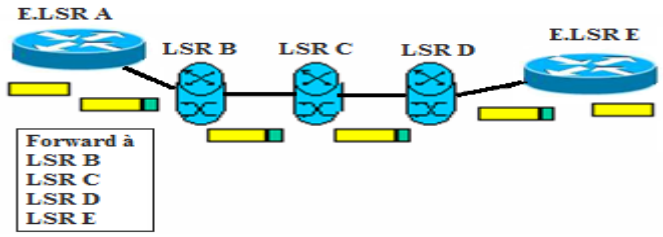


Figure 2.18: Explicit Routing LSP Route par la source

Le réseau détermine lui-même le chemin en suivant les étapes ci-dessous :

- Connaissance de l'état du réseau : topologie, bande passante réelle d'un lien, bande passante utilisée,
- Calcul d'un chemin répondant aux contraintes spécifiées.
- Envoi du trafic sur le chemin trouvé.
- Supervision de l'état des LSP et le transmet à l'IGP.
- Ré-optimisation des LSP quand nécessaire.
- Etablissement du ER-LSP (*Explicitly Routed LSP*). La source connaît le chemin complet de l'ingress node à l'egress node et c'est elle qui spécifie les LSR à l'intérieur du LSP.

Deux options de signalisation spécifiées pour l'établissement du LSP : RSVP ou CR-LDP:RSVP ne permet pas d'offrir du SLA (***Service Level Agreement***). Accord entre un client et un fournisseur sur le niveau de qualité de service offert par ce dernier car il repose sur le protocole UDP (non -orienté connexion)

CR-LDP est l'alternative à RSVP; il est jugé plus fiable dans la mesure où il met en œuvre TCP (orienté connexion). De plus, CR-LDP peut inter-fonctionner avec LDP et utilise les messages LDP pour signaler les différentes contraintes. Les fonctions de CR-LDP sont réalisées par des instructions matérielles ne nécessitant pas de fréquents rafraîchissements, contrairement à RSVP dont les fonctions sont réalisées par le logiciel nécessitant de fréquents messages de rafraîchissement. [7.11.13]

Les fonctions supportées par ER-LDP sont :

- ER-LSP de bout en bout.
- Strict / loose explicit routing : dans un LSP routé de manière " stricte ", chaque bond est spécifié. Une section du LSP peut être routée de manière " imprécise " lorsque sont introduits 2 LSR non directement connectés.
- Spécification d'une classe de service.
- Réservation de la bande passante.
- Route pinning : dans une section de ER-LSP routée de manière " imprécise ", les bonds sont sélectionnés selon une transmission bond par bond.
- ER-LSP préemption : établissement/maintien de priorité. [7.11]

2.8 Quelques applications d'MPLS

Il existe aujourd'hui des applications majeures de MPLS. Ces dernières supposent la mise en œuvre de composants adaptés aux fonctionnalités recherchées. L'implémentation de MPLS sera donc différente en fonction des objectifs recherchés. Cela se traduit principalement par une façon différente d'assigner et de distribuer les labels (Classification, protocoles de distribution de labels). Le principe d'acheminement des paquets fondé sur l'exploitation des labels étant le mécanisme de base commun à toutes les approches. [8]

Les applications les plus courantes du MPLS sont les suivantes :

Le Traffic Engineering

L'ingénierie de trafic est activée par des mécanismes MPLS permettant de diriger le trafic via un chemin spécifique, qui n'est pas nécessairement le chemin le moins coûteux. Les administrateurs de réseau peuvent mettre en œuvre des politiques visant à assurer une distribution optimale du trafic et à améliorer l'utilisation globale du réseau. [8.11]

Le support de la qualité de service

Avec la technologie MPLS, la QoS (***Quality of service***) est un élément crucial pour un réseau d'opérateur. En effet, l'opérateur doit pouvoir garantir à ses clients le transport de leurs flux en garantissant différentes contraintes, La qualité de service se décline principalement en quatre paramètres : débit, délai, gigue et perte. [7.8]

Les réseaux privés virtuels

VPN (***Virtual Private Network***) MPLS simplifient considérablement le déploiement des services par rapport aux VPN IP traditionnels. Lorsque le nombre de routes et de clients augmente, les VPN MPLS peuvent facilement monter en charge, tout en offrant le même niveau de confidentialité que les technologies de niveau 2. Ils peuvent également transporter des adresses IP non-uniques à travers un domaine public. Alors, le VPN résoudre deux problématiques essentielles a savoir :

- Assurer la confidentialité des données transportées.
- Prendre en charge des plans d'adressage privé, fréquemment identiques. [8.11]

La différentiation des services

Le modèle de différenciation des services semble être plus adéquat pour les réseaux multiservices tels que l'Internet. Ce modèle signifie en d'autres termes donner la priorité à une classe de service au dépend d'une autre classe au moment de congestion. Le modèle DiffServ (***Differentiated Services***) définit une approche totalement différente en comparaison avec le modèle IntServ (***Integrated Services***). Il ne nécessite ni une réservation de bout en bout ni signalisation. Il permet d'affecter chaque paquet à une classe de service. La complexité est reléguée dans les extrémités du réseau. Les services différenciés de l'architecture DiffServ permettent de diminuer substantiellement les informations d'état que chaque nœud du réseau doit mémoriser. [7.11]

La bande passante garantie

La bande passante garantie constitue une amélioration à forte valeur ajoutée par rapport aux mécanismes d'ingénierie de trafic traditionnels. MPLS permet aux fournisseurs de services d'allouer des largeurs de bande passante et des canaux garantis. La bande passante garantie permet également la comptabilité des ressources QoS (*qualité de service*) de manière à organiser le trafic 'prioritaire' et 'au mieux', tels que la voix et les données. [7.11]

Le reroutage rapide

Le reroutage rapide (*fast rerouting*) permet une reprise très rapide après la défaillance d'une liaison ou d'un nœud. Une telle rapidité de reprise empêche l'interruption des applications utilisateur ainsi que toute perte de données. [11]

Any Transport over

Ce service traduit l'indépendance de MPLS vis-à-vis des protocoles de couches 2 et 3. AToM (***Any Transport over MPLS***) est une application qui facilite le transport du trafic de couche 2, tel que Frame Relay, Ethernet, PPP et ATM, à travers un nuage MPLS. [8]

2.9 Conclusion

D'après l'étude de la technologie MPLS qui est faite le long de ce chapitre, nous avons pu constater les différentes fonctionnalités de la technique MPLS, les composantes qui forment ce réseau, l'acheminement des paquets IP tout à travers le réseau MPLS ainsi le concept de label, ses protocoles de distribution et la commutation à base de ces labels.

En résumé, le protocole MPLS fournit plusieurs services offrant une véritable valeur ajoutée aux performances de divers réseaux. Ceci est la raison qui a conduit les entreprises de choisir cette Puissante technologie.

Dans le but d'explorer les notions définies dans ce chapitre et le précédant, une implémentation d'un réseau qui exploite et montre les avantages de la technologie MPLS est élaborée dans les chapitres suivants.

Chapitre III

Conception du réseau MPLS réalisé

3.1 Introduction

La conception des réseaux est l'une des étapes essentielles permettant d'acquérir et de maîtriser des outils techniques et méthodologiques d'analyse, de conception, de planification, et d'administration de nombreux problèmes qui peuvent survenir au cours de réalisation d'un réseau.

Dans cette partie, nous allons présenter l'architecture du réseau MPLS mise en œuvre au niveau de l'opérateur mobile ***OTA*** (***DJEZZY***), et les besoins en termes d'équipements, en protocoles de redondances pour assurer la haute disponibilité de chaque niveau et liaison entre les composants de l'architecture du réseau.

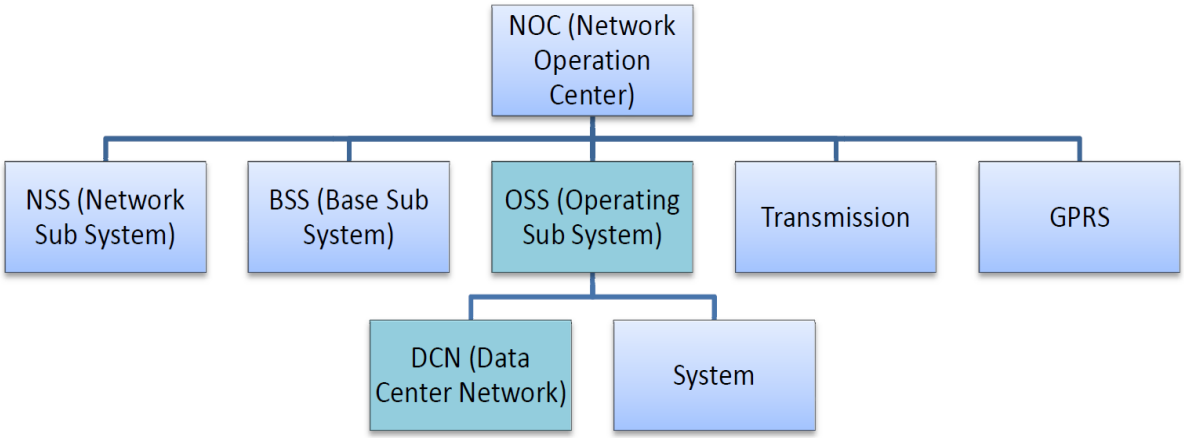
3.2 Entreprise d'accueil

3.2.1 Présentation de l'organisme d'accueil

OTA (***Optimum Telecom Algérie***) est un acteur majeur dans les télécom en Algérie, il compte plus de 18 millions d'abonnés pour l'année 2014 sur le territoire national.

C'est en juillet 2001 que le groupe OTA remporte la deuxième licence de téléphonie mobile en Algérie et ce pour le montant de 737 millions de Dollars. Fort d'un capital humain de plus de 4000 employés, et qui vient d'acquérir la licence 3G ($3^{ème}$ *Génération*) pour 3 milliard de Dinars.

3.2.2 Organigramme du NOC



Figue 3.1 : Organigramme du NOC

Le département NOC (***Network Operation Center***) est constitué de plusieurs services comme le montre l'organigramme, il est charge :

- Du contrôle des transactions.
- De la surveillance des incidents.
- De la charge d'un réseau local ou interconnecté.
- L'administration du réseau.
- La mise en œuvre des nouveaux services.
- l'administration des accès et de la bande passante.

3.2.3 OperationSub System

Ce sous-système assure la gestion et la supervision du réseau :

- Détection de panne.
- Mise en service de sites.
- Modification de paramétrage.
- Réalisation de statistiques.

3.2.4 Présentation du service DCN :

Est un site physique sur lequel se trouvent regroupés des équipements constituant du système d'information de l'entreprise (ordinateurs centraux, serveurs, baies de stockage, équipements réseaux et de télécommunications…).

C'est un service qui remplit les missions suivantes :

- Monitoring, assure le bon fonctionnement, configuration et administration des équipements IP/MPLS (routeurs, commutateurs, pare-feu, passerelles…).
- Assurer le support côté IP/MPLS pour les différents services.

3.3 Objectif de l'application

Cette application consiste à émuler un réseau IP/MPLS, avec un réseau cœur purement MPLS et des réseaux clients IP classique. Le but de telle phase dans ce projet est de cerner les failles à partir le design et raffiner le planning avant d'aller à la phase de déploiement sur un réseau opérationnel.

Vue que le réseau d'un opérateur est étendit et que l'émulation est faite sur un ordinateur simple (PC), le prototype réalisé a pour objectif principale de montrer le bon fonctionnement surtout au niveau réseau cœur, où agit la technologie MPLS et n'est pas tous le réseau.

3.4 Description de la maquette

La maquette suivante, représente l'architecture du réseau MPLS réalisé, en mettant en contact deux infrastructures : réseau cœur (***provider***) et réseau client (***customer***).

Tous les équipements du réseau sont reliés entre eux via des supports physique en cuivre.

3.4.1 Réseau cœur

Le contexte des réseaux désigne la partie qui supporte le gros trafic, en utilisant les technologies les plus rapides et une grande bande passante sur des distances importantes.

Ce cœur de réseau est construit par des fournisseurs (***provider***) et des bords fournisseurs (***provider edge***).

3.4.2 Réseau client

Les petits réseaux (internes à une entreprise ou à une région) joue un rôle de client vis-à-vis de l'infrastructure de l'opérateur (backbone). Dans notre cas, nos clients sont des simples demandeurs d'informations.

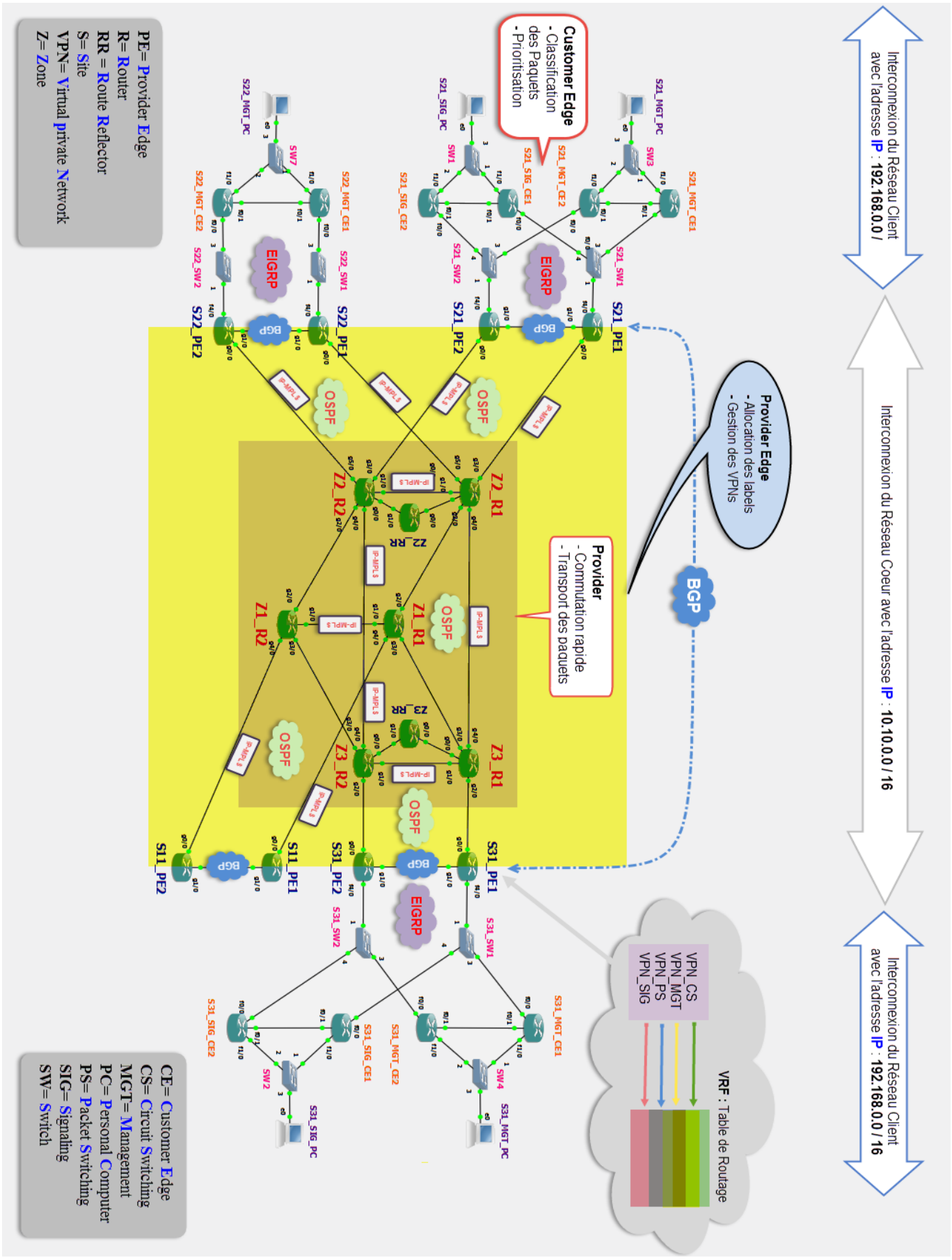


Figure 3.2 **Architecture du projet réalisé**

Notre réseau est édifié sur une architecture comprenant trois types de routeurs illustrés dans le tableau suivant :

Routeur	Zone 1	Zone 2	Zone 3
Des routeurs pour fournisseur (P, Provider)	* Z1_R1 * Z1_R2	* Z2_R1 * Z2_R2 * Z2_RR	* Z3_R1 * Z3_R2 * Z3_RR
Des routeurs pour fournisseur d'accès (PE, Provider Edge	* S11_PE1 * S11_PE2	* S21_PE1 * S21_PE2	* S31_PE1 * S31_PE2
Des routeurs pour l'accès d'abonnés (CE, Customer Edge		* S21_MGT_CE1 * S21_MGT_CE2 * S21_SIG_CE1 * S21_SIG_CE2 * S22 _MGT_CE1 * S22 _MGT_CE2	* S31_MGT_CE1 * S31_MGT_CE2 * S31_SIG_CE1 * S31_SIG_CE2
Note : Z = Zone, R= Routeur, RR = route reflectors (réflecteurs de route), S = Site, PE = Provider Edge, MGT = Management, CE = Customer Edge, SIG = Signaling.			

Tableau 3.1 : Type de routeurs utilisés

3.5 Equipements utilisés

Comme déjà vu dans le premier chapitre, les réseaux peuvent être constitués de divers catégories d'équipements à savoir : des routeurs, des commutateurs, des ponts ...etc.

Dans notre réseau, les équipements utilisés sont détaillés dans le tableau ci-dessous :

Equipement	Nombre	Modèle	Image IOS Cisco	Caractéristique
Routeurs	26	Cisco 7200	C7200-advipservicesk9-m), Version 12.4(2)	- Supporte la plate forme logicielle Cisco IOS - Liaison cuivre ou fibre - Supporte davantage d'instances VRF pour l'implémentation du protocole MPLS.
		Cisco 3745	C3745-adventerprisek9-m), Version 12.4(25	
Commutateur	11	Cisco Ethernet Switch		- Redirection de paquets et filtres non bloquants, pour une vitesse maximale - Autodétection des câbles droits et croisés.

Tableau 3.2 : Equipements utilisés

3.6 Protocoles de routage

Le tableau qui suit, indique les protocoles de routage utilisés dans le cadre de ce projet :

Protocole	But d'utilisation
OSPF	Assure le routage interne entre tous les routeurs ***P*** et ***PE***.
EIGRP	Utilise pour le routage du ***PE*** vers le end user.
MP-BGP	Configurer ente ***PE***, assure l'annoncement des routes des ***CE*** ainsi de les laisser séparés

Tableau 3.3 : Les protocoles de routage utilisés

3.7 Redondance

37.1 Redondance physique

Pour renforcer la haute disponibilité et la redondance de l'architecture de réseau, on était obligé de relier chaque routeur Provider (P1) à un deuxième routeur (P2) au niveau des différentes zones géographique (pour des raisons de sécurités), et faire de même avec les routeurs de bordure (PE) aussi les routeurs au niveau des clients (CE).

3.7.2 Réflecteurs de routes

Afin diminuer le nombre de sessions BGP, une extension appelée RR " route reflector" a été créée. Un seul routeur RR (avec un deuxième redondant) établit des sessions avec tous les autres routeurs PE de son groupe, ces derniers n'ont besoin que d'établir des connexions qu'avec le RR.

L'AS est divisé en groupes de routeurs (cluster) gérés par un route reflector, chaque RR a une session iBGP (*Internal BGP*) avec chacun de ses clients (PE) et leurs transfère ainsi les routes externes.

3.7.3 Redondance protocolaire

La redondance des éléments actifs du réseau permet de mettre en place des principes de haute disponibilités au sein d'un système d'information.

L'utilisation des protocoles de redondance permettant de gérer automatiquement les transitions, les répartitions de la charge ainsi que la tolérance de panne est fortement recommandée.

Les protocoles de redondance les plus utilisés sont : HSRP (***Hot Standby Routing Protocol***), VRRP (***Virtual Router Redundancy Protocol***), et le GLBP (***Gateway Load Balancing Protocol***).

Le protocole de redondance choisi dans notre projet est le HSRP.

Le protocole HSRP :

HSRP est un protocole propriétaire Cisco implémenté sur les routeurs et les commutateurs de niveau 3 permettant une continuité de service.

HSRP permet de mettre en place une passerelle réseau (virtuelle) hautement disponible, l'adresse IP de la passerelle est configuré sur deux routeurs, l'un des routeurs prendra un rôle «actif» et le second un «passif» ou «standby».

Le routeur primaire (actif) est élu par groupe au moyen d'une priorité, le second est considéré en standby, il assumera donc la tâche de transmettre les paquets à la place du primaire en cas de défaillance.

Le processus d'élection se déroule pendant la mise en place des liens, un fois le processus terminé, seul le routeur primaire (actif) va envoyer des messages multicast en UDP périodique à l'autre routeur afin de minimiser le trafic réseau.

Si ces messages ne sont plus reçus par le routeur secondaire (synonyme de défaillance), il devient immédiatement actif.

La figure d'après montre un exemple de protocole HSRP :

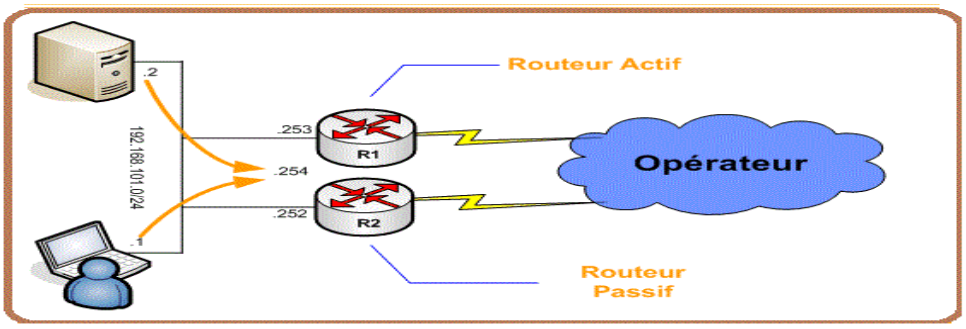


Figure 3.3 : Exemple de mise en place du protocole HSRP

3.8 Plan d'adressage

Pour l'affectation des adresses IP, on a utilisé l'adresse privée de classe A 10.10.0.0/16 pour le Backbone (réseau cœur) et l'adresse privée de classe C 192.168.0.0/16 pour la partie accès clients.

Pour une bonne distribution des adresses IP on fait appel à la techniques VLSM qui attribue des masques de longueur variable dans le but d'affaiblir le taux de gaspillage d'adresses.

Exemple : Comme l'indique la figure ci-dessous, la plage d'adresse réseau 10.10.0.0/24 sera scindé en 3 sous-réseaux comme suit :

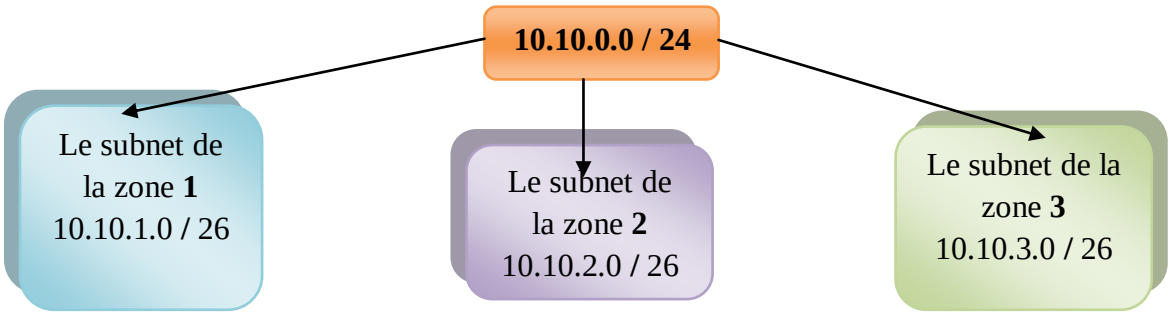


Figure 3.4 : Exemple de découpage en sous-réseaux d'une adresse IP

L'adresse réseau 192.168.0.0/16 sera divisée en sous-réseaux concernant la partie client (customer).

Le tableau suivant expose le plan d'adressage du projet global :

Router	Loopback	IP address	Mask	Interface	Description
Z1_R1	10.10.4.1	10.10.0.9	255.255.255.252	g1/0	To Z1_R2
		10.10.0.1	255.255.255.252	g2/0	To Z2_R1
		10.10.0.5	255.255.255.252	g3/0	To Z3_R1
		10.10.1.1	255.255.255.252	g4/0	To S11_PE1
Z1_R2	10.10.4.2	10.10.0.10	255.255.255.252	g1/0	To Z1_R1
		10.10.0.17	255.255.255.252	g2/0	To Z2_R2
		10.10.0.13	255.255.255.252	g3/0	To Z3_R2
		10.10.1.65	255.255.255.252	g4/0	To S11_PE2
Z2_R1	10.10.4.3	10.10.0.25	255.255.255.252	g1/0	To Z2_R2
		10.10.0.2	255.255.255.252	g2/0	To Z1_R1
		10.10.2.1	255.255.255.252	g3/0	To S21_PE1
		10.10.0.21	255.255.255.252	g4/0	To Z3_R1
		10.10.0.241	255.255.255.252	g0/0	To Z2_RR
Z2_R2	10.10.4.4	10.10.0.26	255.255.255.252	g1/0	To Z2_R1
		10.10.0.18	255.255.255.252	g2/0	To Z1_R2
		10.10.2.65	255.255.255.252	g3/0	To S21_PE2
		10.10.0.29	255.255.255.252	g4/0	To Z3_R2
		10.10.0.245	255.255.255.252	g0/0	To Z2_RR
Z3_R1	10.10.4.5	10.10.0.93	255.255.255.252	g1/0	To Z3_R2
		10.10.3.1	255.255.255.252	g2/0	To S31_PE1
		10.10.0.6	255.255.255.252	g3/0	To Z1_R1
		10.10.0.22	255.255.255.252	g4/0	To Z2_R1
		10.10.0.249	255.255.255.252	g0/0	To Z3_RR
Z3_R2	10.10.4.6	10.10.0.94	255.255.255.252	g1/0	To Z3_R1
		10.10.3.65	255.255.255.252	g2/0	To S31_PE2
		10.10.0.14	255.255.255.252	g3/0	To Z1_R2
		10.10.0.30	255.255.255.252	g4/0	To Z2_R2
		10.10.0.253	255.255.255.252	g0/0	To Z3_RR
S11_PE1	10.10.4.32	10.10.1.129	255.255.255.252	g1/0	To S11_PE2
		10.10.1.2	255.255.255.252	g0/0	To Z1_R1
S11_PE2	10.10.4.33	10.10.1.130	255.255.255.252	g1/0	To S11_PE1
		10.10.1.66	255.255.255.252	g0/0	To Z1_R2
S21_PE1	10.10.4.64	10.10.2.129	255.255.255.252	g1/0	To S21_PE2
		10.10.2.2	255.255.255.252	g0/0	To Z2_R1
S21_PE2	10.10.4.65	10.10.2.130	255.255.255.252	g1/0	To S21_PE2
		10.10.2.66	255.255.255.252	g0/0	To Z2_R2
S31_PE1	10.10.4.96	10.10.3.129	255.255.255.252	g1/0	To S31_PE2
		10.10.3.2	255.255.255.252	g0/0	To Z3_R1
S31_PE2	10.10.4.97	10.10.3.130	255.255.255.252	g1/0	To S31_PE2
		10.10.3.66	255.255.255.252	g0/0	To Z3_R2

Tableau 3.4 : Le plan d'adressage du projet réalisé

La suite de Tableau 3.4 :

Router	Loopback	IP address	Mask	Interface	Description
Z2_RR	10.10.4.30	10.10.0.242	255.255.255.252	g0/0	To Z2_R1
		10.10.0.246	255.255.255.252	g1/0	To Z2_R2
Z3_RR	10.10.4.31	10.10.0.250	255.255.255.252	g0/0	To Z3_R1
		10.10.0.254	255.255.255.252	g1/0	To Z3_R2
S21_MGT_CE1	/	192.168.20.2	255.255.255.252	Fa0/0	To S21_PE1
		192.168.20.9	255.255.255.252	Fa0/1	To S21_MGT_CE2
		192.168.20.130	255.255.255.128	Fa1/0	To S21_LAN_MGT
S21_MGT_CE2	/	192.168.20.6	255.255.255.252	Fa0/0	To S21_PE2
		192.168.20.10	255.255.255.252	Fa0/1	To S21_MGT_CE1
		192.168.20.131	255.255.255.128	Fa1/0	To S21_LAN_MGT
S21_SIG_CE1	/	192.168.20.2	255.255.255.252	Fa0/0	To S21_PE1
		192.168.20.9	255.255.255.252	Fa0/1	To S21_SIG_CE2
		192.168.20.130	255.255.255.128	Fa1/0	To S21_LAN_SIG
S21_SIG_CE2	/	192.168.20.6	255.255.255.252	Fa0/0	To S21_PE2
		192.168.20.10	255.255.255.252	Fa0/1	To S21_SIG_CE1
		192.168.20.131	255.255.255.128	Fa1/0	To S21_LAN_SIG
S31_MGT_CE1	/	192.168.30.2	255.255.255.252	Fa0/0	To S31_PE1
		192.168.30.9	255.255.255.252	Fa0/1	To S31_MGT_CE2
		192.168.30.130	255.255.255.128	Fa1/0	To S31_LAN_MGT
S31_MGT_CE2	/	192.168.30.6	255.255.255.252	Fa0/0	To S31_PE2
		192.168.30.10	255.255.255.252	Fa0/1	To S31_MGT_CE1
		192.168.30.131	255.255.255.128	Fa1/0	S31_LAN_MGT
S31_SIG_CE1	/	192.168.31.2	255.255.255.252	Fa0/0	To S31_PE1
		192.168.31.9	255.255.255.252	Fa0/1	To S31_SIG_CE2
		192.168.31.130	255.255.255.128	Fa1/0	To S31_LAN_SIG
S31_SIG_CE2	/	192.168.31.6	255.255.255.252	Fa0/0	To S31_PE1_
		192.168.31.10	255.255.255.252	Fa0/1	To S31_SIG_CE1
		192.168.31.131	255.255.255.128	Fa1/0	To S31_LAN_SIG

Tableau 3.4 : Le plan d'adressage du projet réalisé

Le tableau suivant indique l'attribution des adresses VRF aux routeurs Provider-Edge.

Router	Description	Subinterface	VLAN	IP address	Mask
S11_PE1	VPN_MGT	Fa4/0	100	192.168.10.1	255.255.255.252
S11_PE2	VPN_MGT	Fa4/0	100	192.168.10.5	255.255.255.252
S21_PE1	VPN_MGT	Fa4/0	100	192.168.10.1	255.255.255.252
	VPN_SIG	Fa4/0	200	192.168.10.1	255.255.255.252
S21_PE2	VPN_MGT	Fa4/0	100	192.168.10.5	255.255.255.252
	VPN_SIG	Fa4/0	200	192.168.10.5	255.255.255.252
S31_PE1	VPN_MGT	Fa4/0	100	192.168.10.1	255.255.255.252
	VPN_SIG	Fa4/0	200	192.168.10.1	255.255.255.252
S31_PE2	VPN_MGT	Fa4/0	100	192.168.10.5	255.255.255.252
	VPN_SIG	Fa4/0	200	192.168.10.5	255.255.255.252

Tableau 3.5 : L'attribution des adresses VRF aux routeurs Provider-Edge

3.9 Conclusion

Une bonne compréhension de l'environnement informatique aide à déterminer la portée du projet d'implémentation.

Cette conception permet de présenter une interprétation graphique sur le projet de façon prématurée, donc il reste que de travailler sur un simulateur graphique des réseaux. Et dans notre cas, la configuration des équipements a été réalisé à l'aide d'un émulateur appelé GNS3.

Chapitre IV

Implémentation et Test

4.1 Introduction

Ce chapitre est dédié pour des tests et validation des différentes configurations faites dans ce projet, pour bien dégager les avantages de cette nouvelle architecture, en utilisant le simulateur graphique « GNS3 version 1.2 ».

4.2 Présentation de simulateur GNS3

GNS3 (***Graphical Network Simulator***) est un logiciel libre très pratique pour maquetter un réseau, GNS3 permet de faire l'émulation et sert à reproduire une architecture physique ou logique complète avant la mise en production.

GNS3 permet de charger de véritable IOS Cisco des différents équipements, et de les utiliser en simulation complète sur un simple ordinateur. Par exemple, il permet d'avoir un routeur virtuel.

Il est composé des outils suivants :

- **Dynamips** : émulateur d'IOS Cisco.
- **Dynagen** : interface écrite en python (programme faisant la passerelle entre GNS3 et Dynamips) permettant l'interconnexion de plusieurs machines émulées.
- **Qemu** : émulateur de PC virtualisé.

4.3 Validation de Routage

Les protocoles de routage dynamique utilisés à savoir : OSPF, EIGRP, et BGP comportent deux aspects: l'annoncement des routes (advertisement) et la mise à jour (update) des tables de routage.

Faisant des tests de validation sur les différentes méthodes de routage et vérifiant la configuration des routeurs ainsi que la connectivité réseau.

4.3.1 Validation du protocole OSPF

La configuration OSPF consiste à déclarer sur chaque routeur Provider ou Provider Edge lesquelles des interfaces sont activées. Et la commande show ip route permet de visualiser les routes prises par le protocole OSPF. Après avoir fait les tests de vérification du routage interne (OSPF) effectuer avec succès au niveau des routeurs Providers. Prenant l'exemple sur le routeur ***Z1_R1*** de la zone une (01).

Remarque : Toutes les zones dont on parle tout le long de ce chapitre sont illustrées dans la maquette du projet réalisé.

Cette figure indique le test fait au niveau du routeur Provider Z1_R1 :

```
Z1_R1#show ip route ospf
    10.0.0.0/8 is variably subnetted, 41 subnets, 2 masks
O       10.10.4.4/32 [110/3] via 10.10.0.10, 00:00:13, GigabitEthernet1/0
                     [110/3] via 10.10.0.2, 00:00:13, GigabitEthernet2/0
O       10.10.4.5/32 [110/2] via 10.10.0.6, 00:00:13, GigabitEthernet3/0
O       10.10.4.6/32 [110/3] via 10.10.0.10, 00:00:13, GigabitEthernet1/0
                     [110/3] via 10.10.0.6, 00:00:13, GigabitEthernet3/0
O       10.10.2.0/30 [110/2] via 10.10.0.2, 00:00:13, GigabitEthernet2/0
O       10.10.3.0/30 [110/2] via 10.10.0.6, 00:00:13, GigabitEthernet3/0
O       10.10.4.2/32 [110/2] via 10.10.0.10, 00:00:13, GigabitEthernet1/0
O       10.10.2.4/30 [110/2] via 10.10.0.2, 00:00:13, GigabitEthernet2/0
O       10.10.4.3/32 [110/2] via 10.10.0.2, 00:00:13, GigabitEthernet2/0
O       10.10.0.12/30 [110/2] via 10.10.0.10, 00:00:13, GigabitEthernet1/0
O       10.10.0.16/30 [110/2] via 10.10.0.10, 00:00:13, GigabitEthernet1/0
O       10.10.0.20/30 [110/2] via 10.10.0.6, 00:00:13, GigabitEthernet3/0
                      [110/2] via 10.10.0.2, 00:00:13, GigabitEthernet2/0
O       10.10.0.24/30 [110/2] via 10.10.0.2, 00:00:13, GigabitEthernet2/0
O       10.10.4.30/32 [110/3] via 10.10.0.2, 00:00:13, GigabitEthernet2/0
O       10.10.4.31/32 [110/3] via 10.10.0.6, 00:00:13, GigabitEthernet3/0
O       10.10.0.28/30 [110/3] via 10.10.0.10, 00:00:13, GigabitEthernet1/0
                      [110/3] via 10.10.0.6, 00:00:13, GigabitEthernet3/0
                      [110/3] via 10.10.0.2, 00:00:13, GigabitEthernet2/0
O       10.10.4.32/32 [110/2] via 10.10.1.2, 00:00:13, GigabitEthernet4/0
O       10.10.4.33/32 [110/3] via 10.10.1.2, 00:00:13, GigabitEthernet4/0
                      [110/3] via 10.10.0.10, 00:00:13, GigabitEthernet1/0
O       10.10.1.64/30 [110/2] via 10.10.0.10, 00:00:31, GigabitEthernet1/0
O       10.10.2.64/30 [110/3] via 10.10.0.10, 00:00:32, GigabitEthernet1/0
                      [110/3] via 10.10.0.2, 00:00:32, GigabitEthernet2/0
O       10.10.3.64/30 [110/3] via 10.10.0.10, 00:00:33, GigabitEthernet1/0
                      [110/3] via 10.10.0.6, 00:00:33, GigabitEthernet3/0
O       10.10.4.64/32 [110/3] via 10.10.0.2, 00:00:33, GigabitEthernet2/0
O       10.10.4.65/32 [110/4] via 10.10.0.10, 00:00:33, GigabitEthernet1/0
                      [110/4] via 10.10.0.2, 00:00:33, GigabitEthernet2/0
O       10.10.4.66/32 [110/3] via 10.10.0.2, 00:00:33, GigabitEthernet2/0
O       10.10.2.68/30 [110/3] via 10.10.0.10, 00:00:33, GigabitEthernet1/0
                      [110/3] via 10.10.0.2, 00:00:33, GigabitEthernet2/0
O       10.10.4.67/32 [110/4] via 10.10.0.10, 00:00:34, GigabitEthernet1/0
                      [110/4] via 10.10.0.2, 00:00:34, GigabitEthernet2/0
O       10.10.0.92/30 [110/2] via 10.10.0.6, 00:00:34, GigabitEthernet3/0
O       10.10.4.96/32 [110/3] via 10.10.0.6, 00:00:34, GigabitEthernet3/0
O       10.10.4.97/32 [110/4] via 10.10.0.6, 00:00:34, GigabitEthernet3/0
O       10.10.1.128/30 [110/2] via 10.10.1.2, 00:00:35, GigabitEthernet4/0
O       10.10.2.128/30 [110/3] via 10.10.0.2, 00:00:35, GigabitEthernet2/0
O       10.10.3.128/30 [110/3] via 10.10.0.6, 00:00:35, GigabitEthernet3/0
O       10.10.2.132/30 [110/3] via 10.10.0.2, 00:00:35, GigabitEthernet2/0
O       10.10.0.240/30 [110/2] via 10.10.0.2, 00:00:35, GigabitEthernet2/0
O       10.10.0.244/30 [110/3] via 10.10.0.10, 00:00:35, GigabitEthernet1/0
                       [110/3] via 10.10.0.2, 00:00:35, GigabitEthernet2/0
O       10.10.0.248/30 [110/2] via 10.10.0.6, 00:00:36, GigabitEthernet3/0
O       10.10.0.252/30 [110/3] via 10.10.0.10, 00:00:36, GigabitEthernet1/0
                       [110/3] via 10.10.0.6, 00:00:36, GigabitEthernet3/0
Z1_R1#
```

Figure 4.1 : Test réussi de routage OSPF du Provider Z1_R1

La vérification du routage interne (OSPF) du Provider Edge est examinée par exemple sur le routeur ***S21_PE2*** de la zone deux (02), comme l'indique la figure suivante :

```
S21_PE2#show ip route ospf
    10.0.0.0/8 is variably subnetted, 41 subnets, 2 masks
O       10.10.4.4/32 [110/2] via 10.10.2.65, 02:05:05, GigabitEthernet0/0
O       10.10.0.0/30 [110/3] via 10.10.2.129, 02:05:05, GigabitEthernet1/0
                     [110/3] via 10.10.2.65, 02:05:05, GigabitEthernet0/0
O       10.10.4.5/32 [110/4] via 10.10.2.129, 02:05:05, GigabitEthernet1/0
                     [110/4] via 10.10.2.65, 02:05:05, GigabitEthernet0/0
O       10.10.1.0/30 [110/4] via 10.10.2.129, 02:05:05, GigabitEthernet1/0
                     [110/4] via 10.10.2.65, 02:05:05, GigabitEthernet0/0
O       10.10.4.6/32 [110/3] via 10.10.2.65, 02:05:05, GigabitEthernet0/0
O       10.10.2.0/30 [110/2] via 10.10.2.129, 02:05:05, GigabitEthernet1/0
O       10.10.3.0/30 [110/4] via 10.10.2.129, 02:05:05, GigabitEthernet1/0
                     [110/4] via 10.10.2.65, 02:05:05, GigabitEthernet0/0
O       10.10.0.4/30 [110/4] via 10.10.2.129, 02:05:05, GigabitEthernet1/0
                     [110/4] via 10.10.2.65, 02:05:05, GigabitEthernet0/0
O       10.10.4.1/32 [110/4] via 10.10.2.129, 02:05:05, GigabitEthernet1/0
                     [110/4] via 10.10.2.65, 02:05:05, GigabitEthernet0/0
O       10.10.4.2/32 [110/3] via 10.10.2.65, 02:05:05, GigabitEthernet0/0
O       10.10.2.4/30 [110/3] via 10.10.2.129, 02:05:05, GigabitEthernet1/0
                     [110/3] via 10.10.2.65, 02:05:05, GigabitEthernet0/0
O       10.10.4.3/32 [110/3] via 10.10.2.129, 02:05:05, GigabitEthernet1/0
                     [110/3] via 10.10.2.65, 02:05:05, GigabitEthernet0/0
O       10.10.0.8/30 [110/3] via 10.10.2.65, 02:05:05, GigabitEthernet0/0
O       10.10.0.12/30 [110/3] via 10.10.2.65, 02:05:05, GigabitEthernet0/0
O       10.10.0.16/30 [110/2] via 10.10.2.65, 02:05:05, GigabitEthernet0/0
O       10.10.0.20/30 [110/3] via 10.10.2.129, 02:05:06, GigabitEthernet1/0
                      [110/3] via 10.10.2.65, 02:05:06, GigabitEthernet0/0
O       10.10.0.24/30 [110/2] via 10.10.2.65, 02:05:06, GigabitEthernet0/0
O       10.10.4.30/32 [110/3] via 10.10.2.65, 02:05:06, GigabitEthernet0/0
O       10.10.4.31/32 [110/4] via 10.10.2.65, 02:05:06, GigabitEthernet0/0
O       10.10.0.28/30 [110/2] via 10.10.2.65, 02:05:06, GigabitEthernet0/0
O       10.10.4.32/32 [110/5] via 10.10.2.129, 02:05:06, GigabitEthernet1/0
                      [110/5] via 10.10.2.65, 02:05:06, GigabitEthernet0/0
O       10.10.4.33/32 [110/4] via 10.10.2.65, 02:05:06, GigabitEthernet0/0
O       10.10.1.64/30 [110/3] via 10.10.2.65, 02:05:06, GigabitEthernet0/0
O       10.10.3.64/30 [110/3] via 10.10.2.65, 02:05:06, GigabitEthernet0/0
O       10.10.4.64/32 [110/2] via 10.10.2.129, 02:05:06, GigabitEthernet1/0
O       10.10.4.66/32 [110/4] via 10.10.2.129, 02:05:06, GigabitEthernet1/0
                      [110/4] via 10.10.2.65, 02:05:06, GigabitEthernet0/0
O       10.10.2.68/30 [110/2] via 10.10.2.65, 02:05:06, GigabitEthernet0/0
O       10.10.4.67/32 [110/3] via 10.10.2.65, 02:05:06, GigabitEthernet0/0
O       10.10.0.92/30 [110/3] via 10.10.2.65, 02:05:06, GigabitEthernet0/0
O       10.10.4.96/32 [110/5] via 10.10.2.129, 02:05:06, GigabitEthernet1/0
                      [110/5] via 10.10.2.65, 02:05:06, GigabitEthernet0/0
O       10.10.4.97/32 [110/6] via 10.10.2.129, 02:05:06, GigabitEthernet1/0
                      [110/6] via 10.10.2.65, 02:05:06, GigabitEthernet0/0
O       10.10.1.128/30 [110/4] via 10.10.2.65, 02:05:06, GigabitEthernet0/0
O       10.10.3.128/30 [110/5] via 10.10.2.129, 02:05:06, GigabitEthernet1/0
                       [110/5] via 10.10.2.65, 02:05:06, GigabitEthernet0/0
O       10.10.2.132/30 [110/3] via 10.10.2.65, 02:05:07, GigabitEthernet0/0
O       10.10.0.240/30 [110/3] via 10.10.2.129, 02:05:07, GigabitEthernet1/0
                       [110/3] via 10.10.2.65, 02:05:07, GigabitEthernet0/0
O       10.10.0.244/30 [110/2] via 10.10.2.65, 02:05:07, GigabitEthernet0/0
O       10.10.0.248/30 [110/4] via 10.10.2.129, 02:05:07, GigabitEthernet1/0
                       [110/4] via 10.10.2.65, 02:05:07, GigabitEthernet0/0
```

Figure 4.2 : Test réussi de routage OSPF du Provider Edge S21_PE2

Commentaire OSPF : La validation OSPF dans ces deux tableaux donne les différentes routes sélectées par le protocole OSPF pour acheminer des paquets IP en précisant l'adresse IP destination ainsi le masque, via quelle interface…

Avec O = OSPF, 110 = AD (Administrative Distance) et le changement des chiffres qui sont devant l'AD indique la métrique.

Faisant maintenant un autre test, mais cette fois-ci, examinant le neighboring (voisinage) du protocole OSPF. Montrant comme exemple de validation du voisinage, les tests faits sur le Provider ***Z2_R1*** de la zone deux (02) et le Provider Edge ***S31_PE2*** de la zone trois (03).

Le test de validation du voisinage OSPF du Provider Z2_R1 est montré dans la figure suivante .

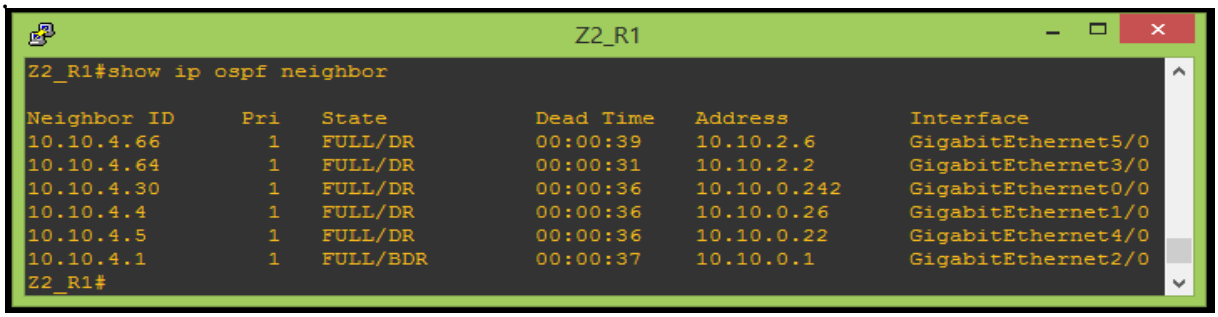


Figure 4.3 : Validation de voisinage OSPF du Provider Z2_R1

La figure suivante montre le test de vérification du voisinage OSPF qui a été fait sur le Provider Edge S31_PE1.

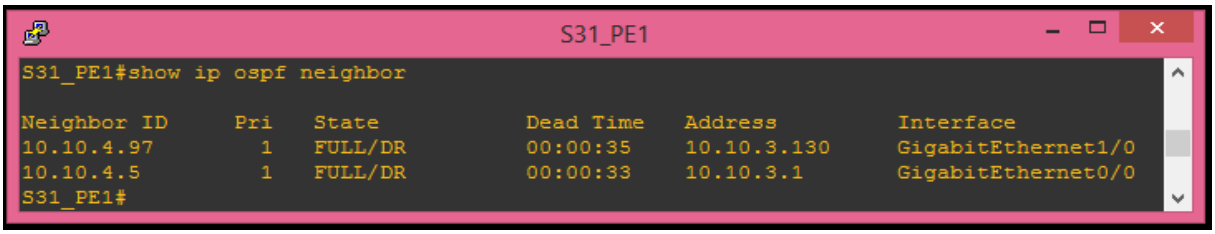


Figure 4.4 : Validation de voisinage OSPF du Provider Edge S31_PE1

Commentaire du voisinage OSPF: les deux figures examinent la validation de voisinage de protocole OSPF en spécifiant identificateur de voisinage, le temps d'établissement, l'adresse de destination ainsi l'interface appropriée…

4.3.2 Validation de protocole BGP

Ce protocole de routage extérieur prend en compte des informations de type qualité de service, coût, ... etc. Ces informations interviennent pour autoriser ou non le passage d'un client. Deux routeurs BGP deviennent voisins après avoir établi une connexion TCP entre eux. La connexion TCP est essentielle pour que les deux routeurs homologues commencent à échanger des mises à jour de routage.

BGP neighboring est configuré dans les Providers Edge et les routes réflecteurs, en faisant par exemple le même test de validation au niveau du routeur Provider Edge ***S22_PE2*** de la zone deux (02) ainsi que le routeur route réflecteur ***Z3_RR*** de la zone trois (03).

La vérification du voisinage BGP du routeur route réflecteur Z3_RR est indiqué dans la figure suivante :

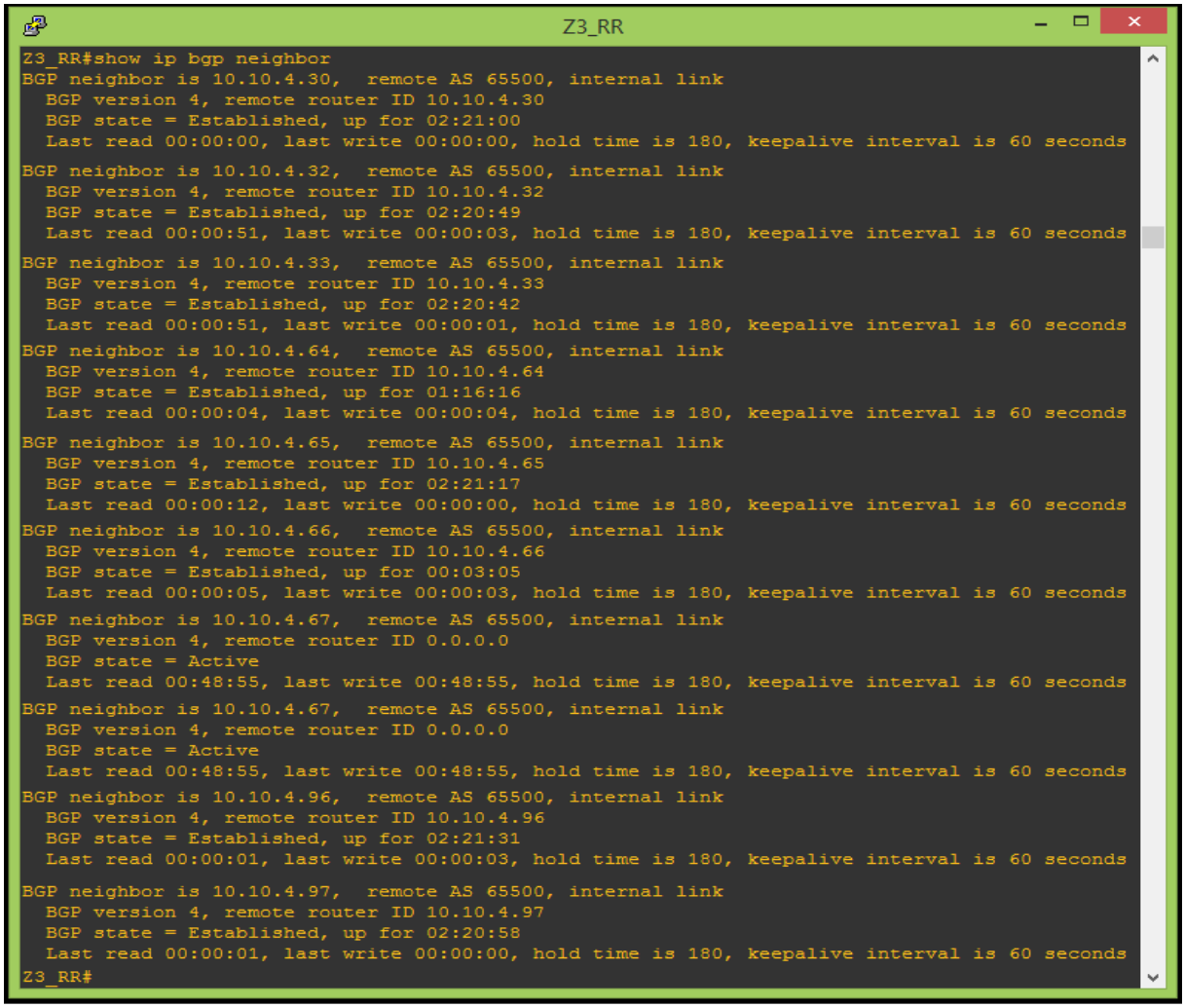


Figure 4.5 : Validation de voisinage BGP du route réflecteurs Z3_RR

Le test de validation du voisinage BGP du Provider Edge S22_PE2 est illustré dans la figure suivante :

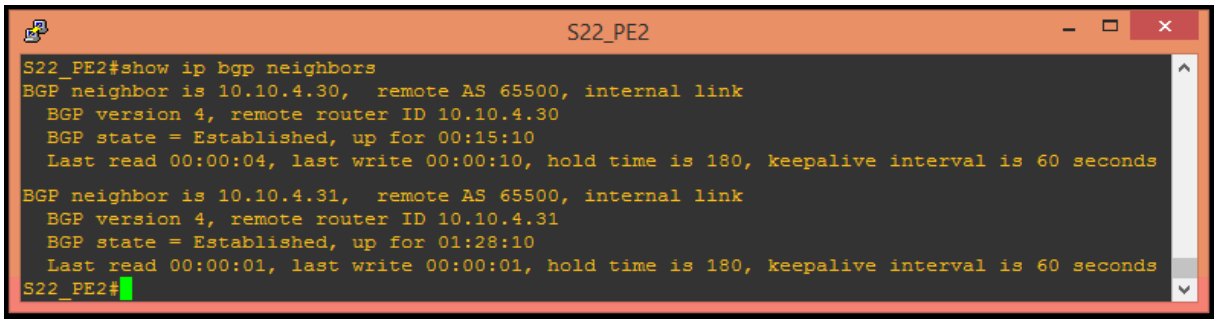


Figure 4.6 : Validation de voisinage BGP du Provider Edge S22_PE2

Commentaire BGP :la validation de voisinage illustrée dans les deux tableaux précédents définit l'adresse de voisinage BGP, numéro de l'AS (système autonome), le type de liaison (interne ou externe), la version BGP, l'identificateur réseau, l'état de BGP…

4.3.3 Validation de protocole EIGRP

Le protocole de routage EIGRP est configuré particulièrement au niveau d'interconnexion Provider Edge et les Customers Edge (réseaux clients) suite à sa possibilité de s'adapter au changement des topologies. Faisant alors deux tests de confirmation sur le bon fonctionnement de EIGRP, prenant comme exemple à tester : le routeur Customer Edge ***S21_MGT_CE1*** de la zone deux (02) et le routeur Customer Edge ***S31_SIG_CE2*** de la zone trois (03).

Le test de validation de routage EIGRP du routeur Customer Edge S21_MGT_CE1 est illustré dans la figure suivante :

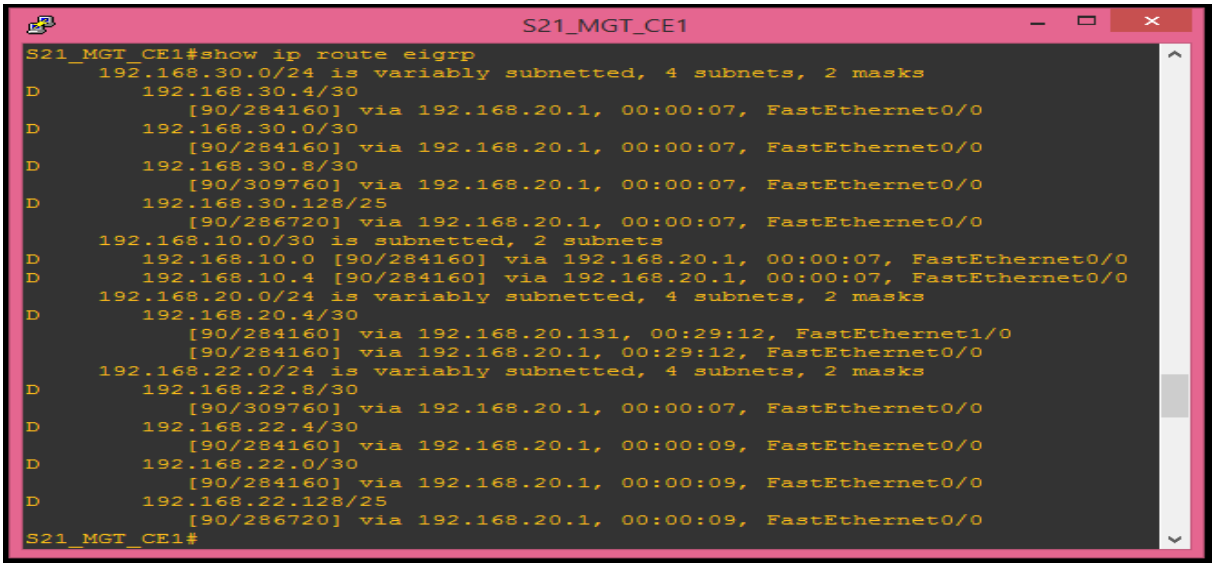


Figure 4.7 : Validation de routage EIGRP du Customer S21_MGT_CE1

La vérification de routage EIGRP du Customer Edge S31_SIG_CE2 est indiquée dans la figure suivante :

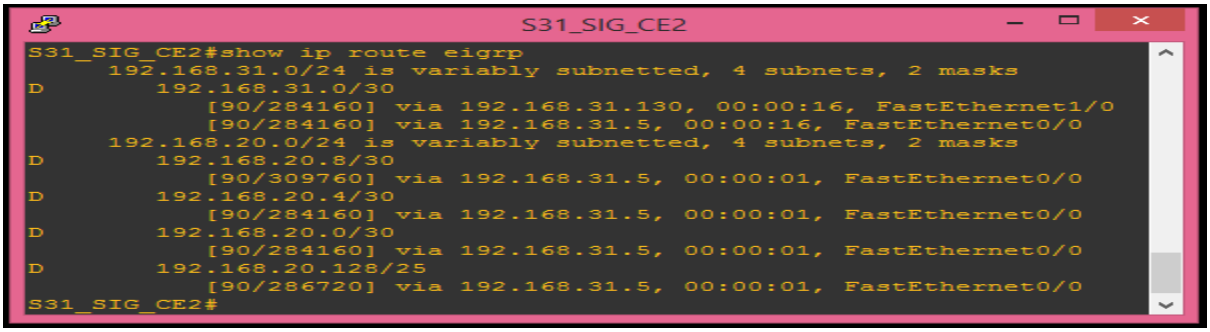


Figure 4.8 : Validation de routage EIGRP du Customer S31_SIG_CE2

Commentaire EIGRP: la validation EIGRP dans ces deux figures définit différentes routes sélectées par le protocole EIGRP en précisant le réseau configuré, le nombre de subnets (sous-réseaux), la distance administrative, l'adresse IP et l'interface appropriée…

Examinant maintenant le neighboring (voisinage) du protocole EIGRP. Montrant comme exemple de validation du voisinage, les tests faits sur le routeur Customer Edge ***S21_SIG_CE1*** de la zone deux (02) et le routeur Customer Edge ***S31_MGT_CE1*** de la zone trois (03).

Le test de validation de neighboring EIGRP du routeur Customer Edge S21_SIG_CE1 est montré dans la figure suivante :

Figure 4.9 : Validation de voisinage EIGRP du Customer Edge S21_SIG_CE1

La vérification du voisinage EIGRP du routeur Customer Edge S31_MGT_CE1 est indiquée dans la figure suivante :

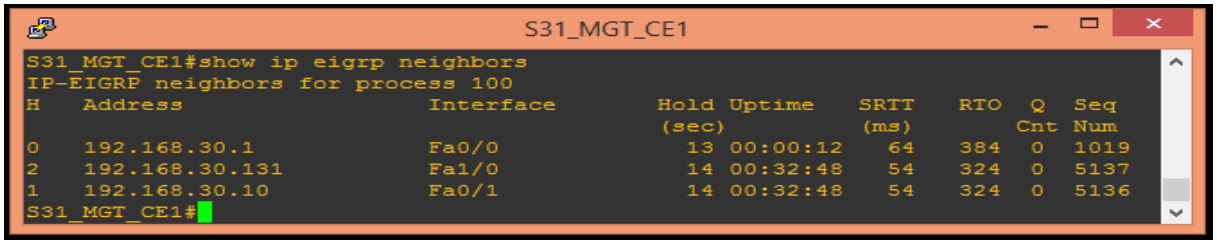


Figure 4.10 : Validation de voisinage EIGRP du Customer Edge S31_MGT_CE1

Commentaire du voisinage EIGRP: le voisinage EIGRP dans les figures précédentes détermine l'interface de l'adresse IP, la durée d'établissement, le numéro de séquence…

4.4 Validation MPLS

Faisant des tests de validation du bon fonctionnement du voisinage MPLS. en prenant comme exemple: deux routeurs Provider : ***Z2_R1*** de la zone 02 et ***Z3_R2*** de la zone 03, et deux routeurs Provider Edge : ***S21_PE2*** de la zone 02 et ***S31_PE1*** de la zone 03.

4.4.1 Voisinage MPLS Provider

La figure suivante montre la validation du voisinage MPLS du routeur Provider Z2_R1 :

```
Z2_R1#show mpls ldp neighbor
  Peer LDP Ident: 10.10.4.66:0; Local LDP Ident 10.10.4.3:0
    TCP connection: 10.10.4.66.62207 - 10.10.4.3.646
    State: Oper; Msgs sent/rcvd: 124/131; Downstream
    Up time: 01:11:41
    LDP discovery sources:
     GigabitEthernet5/0, Src IP addr: 10.10.2.6
    Addresses bound to peer LDP Ident:
     10.10.2.6    10.10.4.66    10.10.2.133
  Peer LDP Ident: 10.10.4.4:0; Local LDP Ident 10.10.4.3:0
    TCP connection: 10.10.4.4.27947 - 10.10.4.3.646
    State: Oper; Msgs sent/rcvd: 127/120; Downstream
    Up time: 01:11:37
    LDP discovery sources:
     GigabitEthernet1/0, Src IP addr: 10.10.0.26
    Addresses bound to peer LDP Ident:
     10.10.0.245    10.10.0.26    10.10.4.4    10.10.0.18
     10.10.2.65    10.10.0.29    10.10.2.69
  Peer LDP Ident: 10.10.4.64:0; Local LDP Ident 10.10.4.3:0
    TCP connection: 10.10.4.64.11897 - 10.10.4.3.646
    State: Oper; Msgs sent/rcvd: 124/130; Downstream
    Up time: 01:11:37
    LDP discovery sources:
     GigabitEthernet3/0, Src IP addr: 10.10.2.2
    Addresses bound to peer LDP Ident:
     10.10.2.2    10.10.4.64    10.10.2.129
  Peer LDP Ident: 10.10.4.5:0; Local LDP Ident 10.10.4.3:0
    TCP connection: 10.10.4.5.21250 - 10.10.4.3.646
    State: Oper; Msgs sent/rcvd: 128/127; Downstream
    Up time: 01:13:55
    LDP discovery sources:
     GigabitEthernet4/0, Src IP addr: 10.10.0.22
    Addresses bound to peer LDP Ident:
     10.10.0.249    10.10.0.93    10.10.4.5    10.10.3.1
     10.10.0.6    10.10.0.22
  Peer LDP Ident: 10.10.4.1:0; Local LDP Ident 10.10.4.3:0
    TCP connection: 10.10.4.1.646 - 10.10.4.3.27744
    State: Oper; Msgs sent/rcvd: 128/119; Downstream
    Up time: 01:14:05
    LDP discovery sources:
     GigabitEthernet2/0, Src IP addr: 10.10.0.1
    Addresses bound to peer LDP Ident:
     10.10.0.9    10.10.4.1    10.10.0.1    10.10.0.5
     10.10.1.1
Z2_R1#
```

Figure 4.11 : Test réussi de voisinage MPLS du Provider Z2_R1

Le test de validation du voisinage MPLS du routeur Provider Z3_R2 est illustré dans la figure suivante :

```
Z3_R2
Z3_R2#show mpls ldp neighbor
    Peer LDP Ident: 10.10.4.5:0; Local LDP Ident 10.10.4.6:0
        TCP connection: 10.10.4.5.646 - 10.10.4.6.20026
        State: Oper; Msgs sent/rcvd: 198/212; Downstream
        Up time: 02:16:18
        LDP discovery sources:
          GigabitEthernet1/0, Src IP addr: 10.10.0.93
        Addresses bound to peer LDP Ident:
          10.10.0.249      10.10.0.93       10.10.4.5        10.10.3.1
          10.10.0.6        10.10.0.22
    Peer LDP Ident: 10.10.4.2:0; Local LDP Ident 10.10.4.6:0
        TCP connection: 10.10.4.2.646 - 10.10.4.6.54316
        State: Oper; Msgs sent/rcvd: 197/194; Downstream
        Up time: 02:15:54
        LDP discovery sources:
          GigabitEthernet3/0, Src IP addr: 10.10.0.13
        Addresses bound to peer LDP Ident:
          10.10.0.10       10.10.4.2        10.10.0.17       10.10.0.13
          10.10.1.65
    Peer LDP Ident: 10.10.4.4:0; Local LDP Ident 10.10.4.6:0
        TCP connection: 10.10.4.4.646 - 10.10.4.6.15757
        State: Oper; Msgs sent/rcvd: 200/205; Downstream
        Up time: 02:15:44
        LDP discovery sources:
          GigabitEthernet4/0, Src IP addr: 10.10.0.29
        Addresses bound to peer LDP Ident:
          10.10.0.245      10.10.0.26       10.10.4.4        10.10.0.18
          10.10.2.65       10.10.0.29       10.10.2.69
Z3_R2#
```

Figure 4.12 : Test réussi de voisinage MPLS du Provider Z3_R2

4.4.2 Voisinage MPLS Provider Edge

La figure suivante montre la validation du voisinage MPLS du routeur Provider Edge S21_PE2:

Figure 4.13 : Test réussi de voisinage MPLS du Provider Edge S21_PE2

Le test de validation du voisinage MPLS du routeur Provider Edge S31_PE1 est illustré dans la figure suivante :

Figure 4.14 : Test réussi de voisinage MPLS du Provider Edge S31_PE

Le test de validation du voisinage MPLS du routeur Provider Edge S31_PE1 est illustré dans la figure suivante :

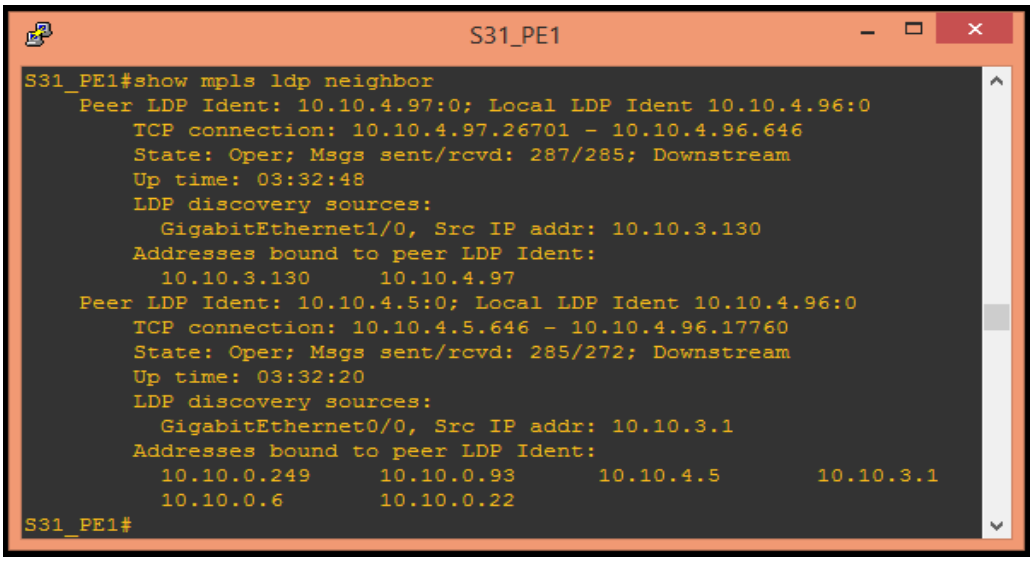


Figure 4.15 : Test réussi de voisinage MPLS du Provider Edge S31_PE1

Commentaire du voisinage MPLS: dans la validation MPLS on distingue sur les cinq figures précédentes qu'il définit la paire d'identifiant LDP, identifiant LDP local, la connexion TCP, le taux de paquets transmis, LDP découvert source, interface de l'adresse IP source, la liaison de l'identifiant LDP…

4.5 Fixation des labels MPLS

Faisant des tests montrant la fixation des labels. en prenant comme exemple: le routeur Provider : ***Z2_R1*** et le routeur Provider Edge : ***S21_PE1*** de la zone 02. ces deux tests sont illustrés, par ordre dans les deux figures suivantes :

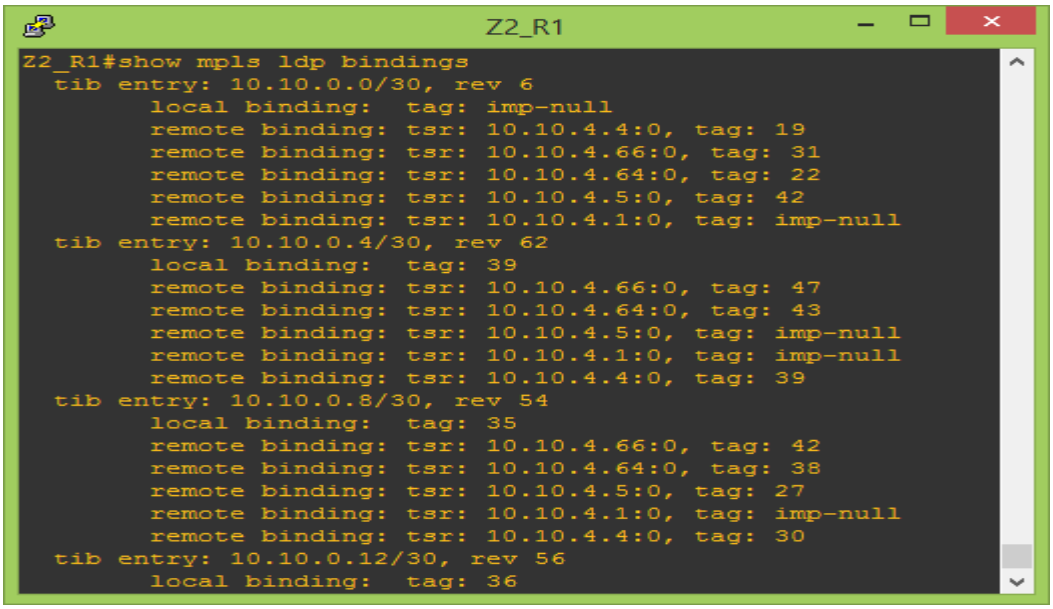


Figure 4.16 : Fixation des labels au niveau du Provider Z2_R1

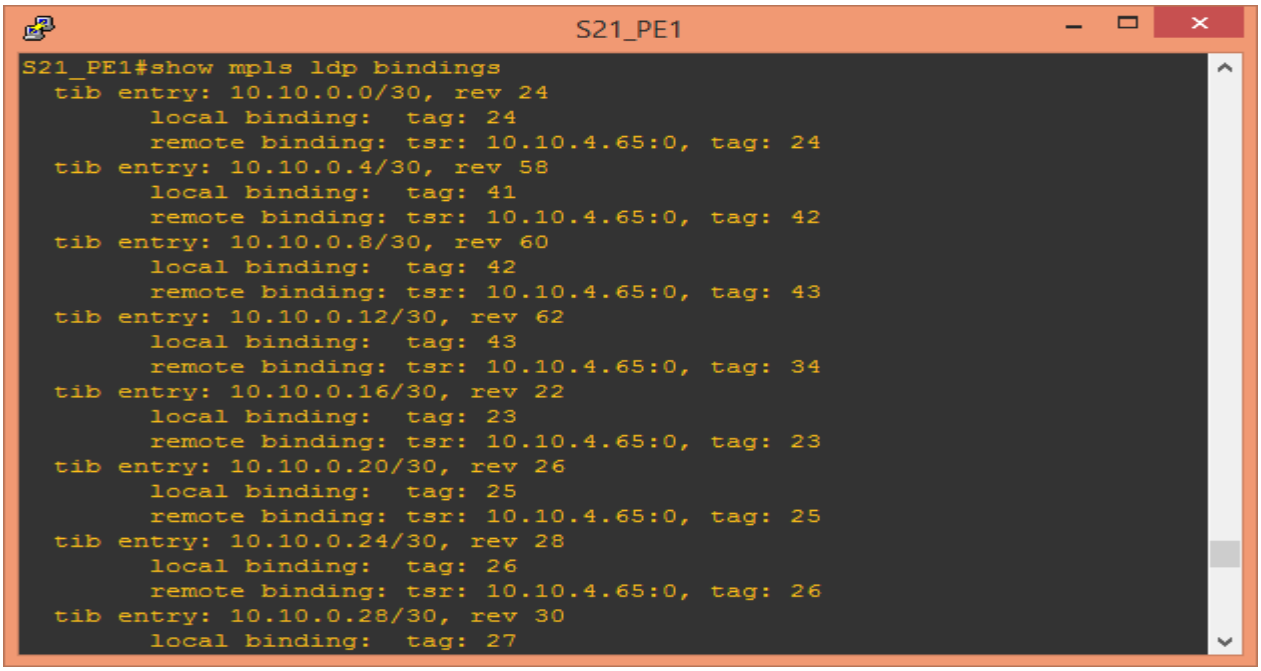


Figure 4.17 : Fixation des labels au niveau du Provider Edge S21_PE1

Commentaire sur l'allocation des labels MPLS : les figures précédentes montre la fixation des labels, en illustrant la LIB d'entrée (l'écran affiche tib d'entrée, par ce que c'est un nom propriétaire de Cisco), le nombre de révisions (rev), la fixation locale et lointaine ainsi que le numéro de label alloué (tag).....

4.6 Validation de la connectivité

Pour dire que la connectivité d'un réseau est vérifiée, il faut faire deux tests de validation à savoir : la commande ping et la commande trace route.

4.6.1 La commande ping

Ping est le nom d'une commande informatique permettant de tester la connectivité vers une autre machine à travers un réseau IP. La commande mesure également le temps mis pour recevoir une réponse, appelé **RTT**: ***round-trip time*** (temps aller-retour).

Ping est une requête ICMP et attend une réponse (echo, echo replay). L'envoi est répété pour des fins statistiques : déterminer le taux de paquets perdus et le délai moyen de réponse. Si d'autres messages ICMP sont reçus de la part de routeurs intermédiaires, ils sont affichés à l'écran. Le paramètre TTL (***Time to Live***) indique le nombre maximal de routeurs intermédiaires à traverser pour atteindre la cible.

Un délai élevé et variable, ou un taux de paquets perdus non nul, peut s'expliquer par un problème de congestion dans le réseau, un problème de qualité sur un lien ou un problème de performance affectant le système cible [14]

Dans notre cas, pour tester la connectivité du réseau, on écrit donc la commande suivante : ***ping*** suivi d'adresse ***IP*** de la machine ciblée.

4.6.1.1 Ping Intra Région

Ping intra région confirme la communication entre deux machines dans une même région, alors faisant un exemple de test de connectivité entre l'ordinateur ***S21_MGT_PC*** et l'ordinateur ***S22_MGT_PC*** dans la même région (zone), qui est la zone deux (02).

La figure ci-dessous, montre un exemple de test ping réussi de l'adresse IP : 192.168.22.150/25 de l'ordinateur S22_MGT_PC depuis l'ordinateur S21_MGT_PC, qui a à son tour l'adresse IP 192.168.20.150/25.

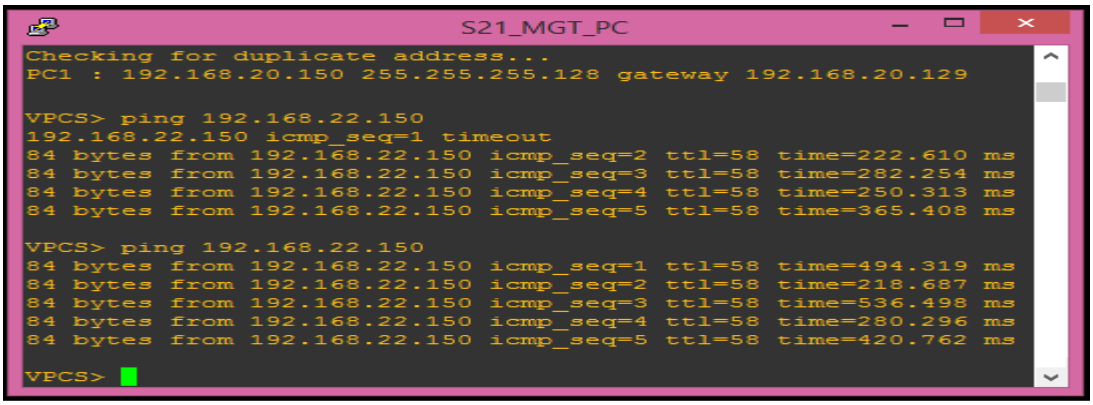


Figure 4.18 : Ping intra région réussi entre S21_MGT_PC et S22_MGT_PC

4.6.1.2 Ping Inter Région

Ping inter région est un test de validation de la connectivité entre deux machines dans deux régions différentes, alors faisant un test de connectivité entre l'ordinateur ***S21_MGT_PC*** de la zone deux (02) et l'ordinateur ***S31_MGT_PC*** de la zone trois (03). La figure qui suit montre l'exemple d'un test ping réussi de l'adresse IP : 192.168.30.150/25 de l'ordinateur S31_MGT_PC depuis l'ordinateur S21_MGT_PC configuré avec l'adresse IP : 192.168.20.150/25.

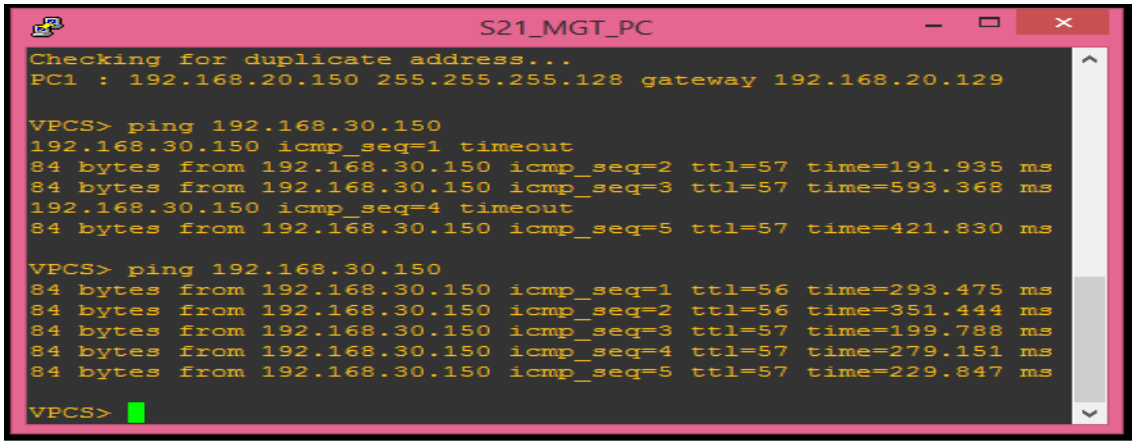


Figure 4.19 : Ping inter région réussi entre S21_MGT_PC et S31_MGT_PC

Faisant maintenant un autre test inverse, cela veut dire faisant un test ping de l'adresse IP : 192.168.20.150/25 de l'ordinateur ***S21_MGT_PC*** depuis l'ordinateur ***S31_MGT_PC*** configuré avec l'adresse IP : 192.168.30.150/25.

La figure d'après illustre ce test inversé.

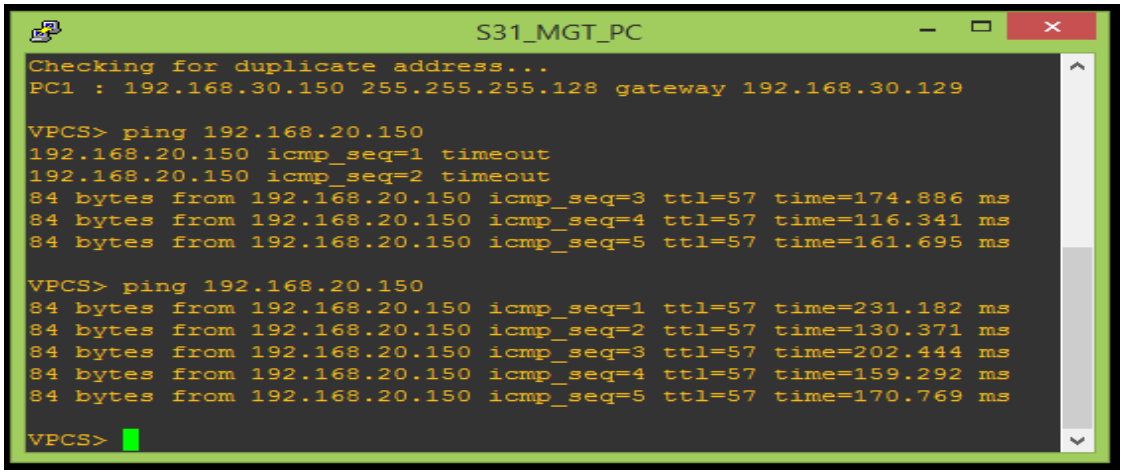


Figure 4.20 : Ping inter région réussi entre S31_MGT_PC et S21_MGT_PC

Et voilà, ça ping sans aucun problème, ce qui est le cas avec tous les autres terminaux, à savoir les PC du Customer, les routeurs Provider et les routeurs Provider Edge.

4.6.2 Test Trace route

Trace route (ou tracert) est un programme utilitaire qui permet de suivre les chemins qu'un paquet de données (paquet IP) va prendre pour aller de la machine locale à une autre machine connectée au réseau IP. Les paquets IP sont acheminés vers la destination en passant d'un routeur à un autre. Chaque routeur examine sa table de routage pour déterminer le routeur suivant. Trace route va permettre d'identifier les routeurs empruntés, indiquer le délai entre chacun des routeurs et les éventuelles pertes de paquets. Ces informations seront utiles pour diagnostiquer des problèmes de routage, comme des boucles, pour déterminer s'il y a de la congestion ou un autre problème sur un des liens vers la destination.

Le principe de fonctionnement de Trace route consiste à envoyer des paquets UDP (certaines versions peuvent aussi utiliser TCP ou bien ICMP Request) avec un paramètre Time-To-Live (TTL) de plus en plus grand (en commençant à 1). Chaque routeur qui reçoit un paquet IP en décrémente le TTL avant de le transmettre. Lorsque le TTL atteint 0, le routeur émet un paquet ICMP d'erreur Time to live exceeded (excédé) vers la source. Trace route découvre ainsi les routeurs de proche en proche [14]

Dans notre cas, pour tester cette commande de trace route, on écrit donc la commande suivante : ***trace*** suivi d'adresse ***IP*** de la machine ciblée.

4.6.2.1 Trace route Intra Région

Trace route intra région est une commande qui montre les chemins traversés par les multiples communications entre deux machines dans une même région, alors testant cette commande par exemple, entre l'ordinateur ***S21_MGT_PC*** et l'ordinateur ***S22_MGT _PC*** qui sont dans la même région (la zone 02).

La figure suivante montre l'exemple du test trace route réussi de l'adresse IP : 192.168.20.150/25 de l'ordinateur S21_MGT_PC vers l'ordinateur S22_MGT_PC avec l'adresse IP : 192.168.22.150/25.

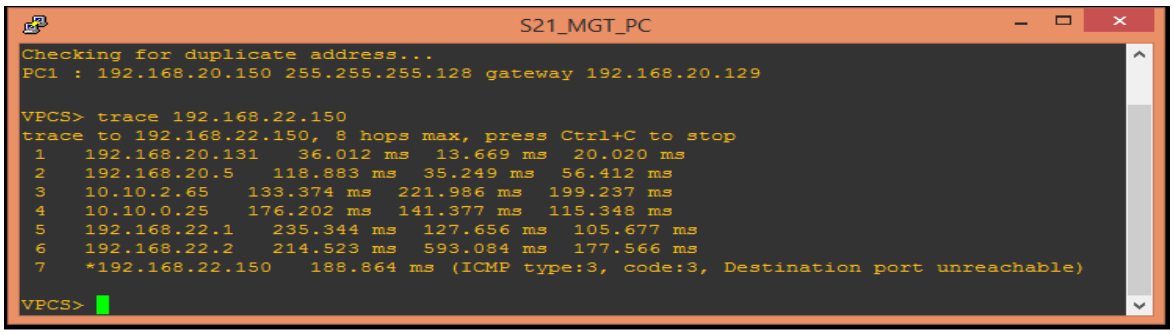


Figure 4.21 : Trace route intra région de S21_MGT_PC vers S22_MGT_PC

4.6.2.2 Trace route Inter Région

Trace route inter région contrairement à l'intra région, est une commande qui montre les chemins traversés par les multiples communications entre deux machines dans deux régions distinctes, alors testant cette commande entre deux ordinateurs, prenant l'exemple de la machine ***S21_MGT_PC*** de la zone deux (02) et la machine ***S31_MGT_PC*** de la zone trois (03).

La figure ci-dessous montre l'exemple du test trace route réussi de l'adresse IP : 192.168.20.150/25 de l'ordinateur S21_MGT_PC vers l'ordinateur S31_MGT_PC configuré avec l'adresse IP : 192.168.30.150/25.

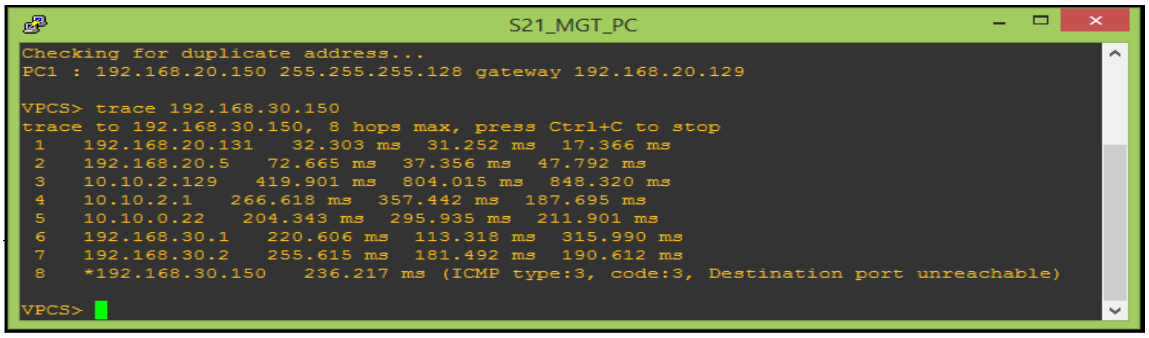


Figure 4.22 : Trace route inter région de S21_MGT_PC vers S31_MGT_PC

La prochaine figure montre le test inverse, c'est-à-dire, à partir de l'ordinateur ***S31_SIG_PC*** situé dans la zone trois (03) vers l'ordinateur ***S21_MGT_PC*** de la zone deux (02).

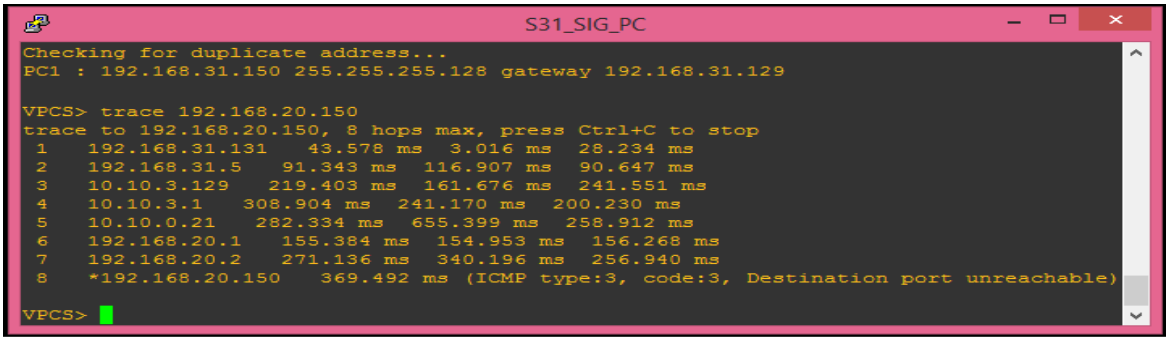


Figure 4.23 :Trace route inter région de S31_SIG_PC vers S21_MGT_PC

4.7 Validation de la redondance

Les tests qui suit, montrent le bon fonctionnement de la redondance et la fiabilité du réseau implémenté.

Alors recommençant le test de connectivité entre l'ordinateur ***S21_MGT_PC*** de la zone deux (02) et l'ordinateur ***S31_MGT_PC*** de la zone trois (03). Mais cette fois-ci, en suspendant les routeurs principaux Z2_R1 et Z2_RR de la zone 02, cette suspension est indiquée dans la figure suivante.

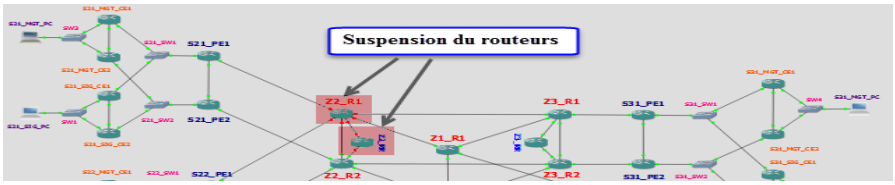


Figure 4.24 : Suspension des routeurs de base Z2_R1 et Z2_RR

La figure qui suit montre le test ping réussi de l'adresse IP : 192.168.30.150/25 de l'ordinateur S31_MGT_PC depuis l'ordinateur S21_MGT_PC configuré avec l'adresse IP : 192.168.20.150/25.

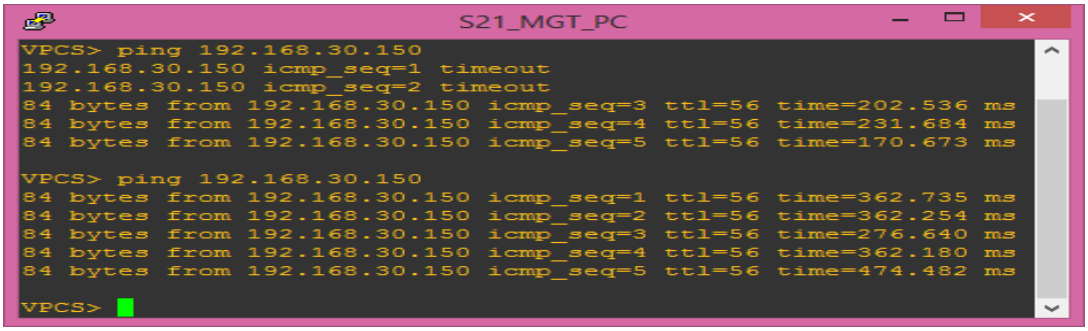


Figure 4.25 : Ping réussi entre S21_MGT_PC et S31_MGT_PC malgré la suspension

Malgré que les deux routeurs de base Z2_R1 et Z2_RR sont éteints, ceux qui sont en standby, c'est-a-dire les routeurs Z2_R2 et Z2_RR ont repris la relève. Et cela montre le bon fonctionnement de la redondance, ce qui garanti la fiabilité et la haute disponibilité du réseau.

4.8 Conclusion

On se basant toujours sur le logiciel d'émulation GNS3 dans ce chapitre pour valider notre travail. Pour ce but, des vérifications de routages, MPLS labels alloués, de connectivités, des chemins empruntés, la fiabilité ainsi que la redondance sont faites.

Finalement, vu à la validation du ce projet, cette nouvelle architecture est prête à être déployer au niveau de divers opérateurs de réseau.

Conclusion Générale

Conclusion générale

Dans ce mémoire, nous avons présentés nos travaux orientés sur la problématique de mutualisation de ressources dans le cadre de réseau d'opérateurs de transport mutualisé. Cette problématique résulte une volonté de fournir d'une part un maximum de bande passante à chaque client et d'autre part de disposer d'une qualité et d'une disponibilité maximale sur l'ensemble du réseau.

En effet, la demande de bande passante est en constante augmentation. De plus l'avènement des accès FTTH (Fiber To The Home) pour l'Internet, la 3G pour la téléphonie mobile, et de la vidéo haute définition entraîne une pression supplémentaire sur les coûts. Les opérateurs cherchent alors à en limiter les répercussions sur les utilisateurs en optimisant leurs infrastructures. Les travaux de recherche se focalisent alors sur l'optimisation des cœurs de réseaux afin d'en limiter le surdimensionnement.

Dans le cadre d'une recherche de réponse à cette problématique, nous avons tout d'abord montré les possibilités offertes par les méthodes classiques dans les réseaux IP. Celles-ci s'attachent à un routage classique soit dans le cœur de réseau ou dans des réseaux locaux.

Dans un second temps, nous avons étudié l'impact de la technologie MPLS sur les réseaux d'opérateurs, où on peut citer par exemple la qualité de service, ingénierie de trafic et la sécurité de réseau. Ces exemples témoignent parfaitement du bénéfice apporté par ce protocole.

Désormais tous les opérateurs commencent à utiliser les réseaux MPLS, car la tendance des réseaux de communications consiste à faire converger les réseaux de voix, données, multimédia en un réseau unique basé sur les paquets IP. Du fait que le protocole MPLS apporte des services IP ainsi que de la convergence des réseaux, le protocole MPLS a certainement un bel avenir devant lui.

Bibliographie

Bibliographie

Bibliographie

[1] Mohamed El Amine GHEFIR « Planification, ingénierie des réseaux de nouvelle génération » Thèse de Magister -2013- Université Abou Bekr Belkaid, Tlemcen.

[2] Claude Servin «" Aide-mémoire de Réseaux et Télécom"» Livre -2004-2009- -2012- Paris- Edition Dunod.

[3] Claude Servin «" Réseaux et Télécoms" Préface de Jean-Pierre Arnaud » Livre -2003- Edition Dunod.

[4] Pascal Urien «"cours réseaux" » Université de ParisTech -2011- France.

[5] http://www.memoireonline.com/03/11/4293/Mise-en-oeuvre-dun-coeur-de-reseau-IPMPLS.html (Site internet).

[6] David Gauchard « Simulation Hybride des Réseaux IP-DiffServ-MPLS Multi-services sur Environnement d'Exécution Distribuée »Thèse de doctorat -2003- Toulouse III, France.

[7] Guy Pujolle «"Les Réseaux" Avec la collaboration de Olivier Salvatori et la contribution de Jacques Nozick » Livre -2008- 6ème Edition Eyrolles.

[8] Oussama FOUDHAILI « Analyse des performances de MPLS en terme de "Traffic Engineering" dans un réseau multiservice », Projet fin d'étude d'ingénierie Tunis -2010- de l'école supérieur des communications de tuni.

[9] Mohamed Anouar RACHDI « Optimisation des ressources de réseaux hétérogènes avec cœur de réseau MPLS » Thèse de Doctorat -2007- l'Institut National des Sciences Appliquées de Toulouse, France.

[10] http://www-igm.univ-mlv.fr/ (Site internet).

[11] http://www.frameip.com/mpls/ (Site internet).

[12] http://www.httr.ups-tlse.fr/pedagogie/cours/tcp-ip/rsvp/ (Site internet).

[13] Mohand Yazid SAIDI « Méthodes de contrôle distribué du placement de LSP de secours pour la protection des communications unicast et multicast dans un réseau MPLS » Thèse de Doctorat -2008- l'Université de Rennes 1, France.

[14] http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-irp/13730 ext-ping-trace.html. (Site internet).